
THOR Manual

Nextron Systems GmbH

Apr 17, 2024

CONTENTS:

1	What is THOR?	1
1.1	Package	2
2	Requirements	3
2.1	Operating Systems	3
2.2	Update Servers	4
3	Before You Begin	5
3.1	Add License File	5
3.2	Upgrade THOR and Update The Signatures	8
3.3	Define an Antivirus / EDR Exclusion	9
3.4	Choose The Right THOR Variant	10
3.5	Choose The Right Architecture	13
3.6	Choose The Right Command Line Flags	13
3.7	Add Command Line Completions (optional)	13
3.8	Verify Public Key Signatures (optional)	14
4	Deployment	15
4.1	Licensing	15
4.2	Network Share (Windows)	21
4.3	ASGARD Management Center (Windows, Linux, macOS)	23
4.4	Ansible (Linux)	24
4.5	THOR Thunderstorm Service	27
4.6	THOR Remote	33
4.7	Distribute to Offline Networks / Field Offices	35
4.8	System Load Considerations	36
5	Scan	37
5.1	Quick Start	37
5.2	Often Used Parameters	38
5.3	Parameters possibly relevant for your Use Case	38
5.4	Risky Flags	38
5.5	Lesser Known But Useful Flags	39
5.6	Help and Debugging	39
5.7	Examples	39
5.8	Run a Scan with Specific Modules	41
5.9	Select or filter Signatures during Initialization	41
5.10	PE-Sieve Integration	42
5.11	Multi-Threading	42
6	Scan Modes	45

6.1	Modules	46
6.2	Features	51
7	Special Scan Modes	57
7.1	Lab Scanning	57
7.2	Lookback Mode	60
7.3	Drop Zone Mode	60
7.4	Image File Scan Mode	62
7.5	DeepDive	62
7.6	Eventlog Analysis	63
7.7	MFT Analysis	64
8	Analysis	65
8.1	ASGARD Analysis Cockpit	65
8.2	Splunk	65
8.3	THOR Util Report Feature	67
8.4	Log Analysis Manual	67
9	Configuration	69
9.1	Scan Templates	69
9.2	CPU Limit (--cpulimit)	70
9.3	Maximum File Size	71
9.4	Exclude Elements	72
10	Output Options	75
10.1	Scan Output	75
10.2	Syslog or TCP/UDP Output	80
10.3	Encrypted Output Files	81
11	Update	83
11.1	Update Locations	83
11.2	Update Server Information	83
12	Custom Signatures	85
12.1	Simple IOCs	85
12.2	Rules	90
12.3	STIX IOCs	97
12.4	Enhance YARA Rules with THOR Specific Attributes	99
13	Other Topics	107
13.1	License Retrieval	107
13.2	Evidence Collection	108
13.3	Resource Control	111
13.4	Scoring System	112
13.5	Action on Match	115
13.6	THOR DB	117
13.7	Archive Scan	118
14	Command Line Options	119
14.1	Scan Options	119
14.2	Scan Modes	120
14.3	Resource Options	121
14.4	Special Scan Modes	122
14.5	Thor Thunderstorm Service	122
14.6	License Retrieval	123

14.7	Active Modules	123
14.8	Module Extras	124
14.9	Active Features	125
14.10	Feature Extras	126
14.11	Output Options	126
14.12	ThorDB	128
14.13	Syslog	128
14.14	Reporting and Actions	128
14.15	THOR Remote	129
14.16	Automatic Collection of Suspicious Files (Bifrost)	129
14.17	VirusTotal Integration	129
14.18	Debugging and Info	130
15	Debugging	131
15.1	Collecting a Diagnostics Pack	131
15.2	Debugging Examples	131
15.3	Finding Bottlenecks	132
15.4	Most Frequent Causes of Missing Alerts	133
15.5	Most Frequent Causes of Frozen Scans	134
15.6	Most Frequent Causes of Failed Scans	135
15.7	Help Us With The Debugging	136
16	Analysis and Info	141
16.1	Log Analysis Manual	141
16.2	VALHALLA Rule Lookup	141
16.3	Rule List Output	141
17	Use Cases	145
17.1	Disk Image Analysis	145
17.2	Memory Image Analysis with Volatility	146
17.3	Scanning a Fileserver	148
18	Known Issues	151
18.1	THOR#003: No rules with DEEPSCAN tag found	151
18.2	THOR#002: THOR in Lab-Mode does not scan network or external drives	152
18.3	THOR#001: Could not parse sigma logsources	153
19	Links and References	155
19.1	Open Source License Acknowledgements	155
20	Changelog	169
20.1	THOR 10.7 (Techpreview)	169
20.2	THOR 10.6 (Stable)	174
20.3	THOR 10.5 (Legacy)	179
20.4	THOR 10.4	185
20.5	THOR 10.3	185
20.6	THOR 10.2	186
20.7	THOR 10.1	189
20.8	THOR 10.0	191
21	Indices and tables	193

WHAT IS THOR?

THOR is a portable scanner for attacker tools and activity on suspicious or compromised server systems.

It covers a big set of basic checks and in deep analysis of the local event log, registry and file system. THOR aims to be a sensitive auditor noticing files and behavior traces a common Antivirus may have missed. An integrated "Scoring System" enables THOR to rate elements based on numerous characteristics to give hints on unknown malware.

THOR can be easily expanded to handle individual, client-specific attack patterns (e.g. the detection of specific malware files or certain log entries on the basis of a forensic analysis).

It is a portable and agent-less "APT Scanner".

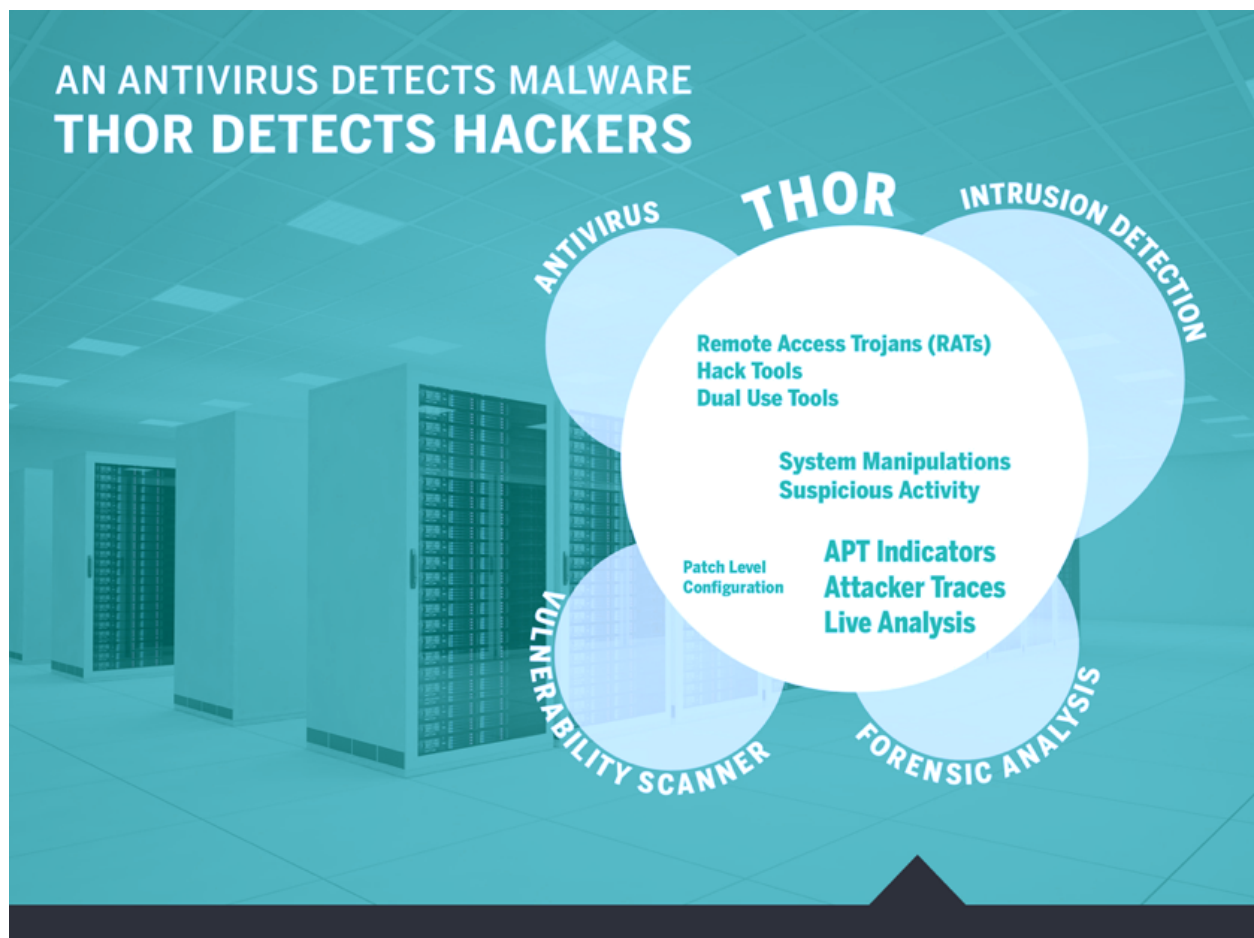


Fig. 1: THOR Coverage and Comparison to Antivirus and Intrusion Detection

The key features are:

- Scans for hack tools and attacker activity (with multiple detection mechanisms)
- Portable – no installation required
- Runs on Windows, Linux and macOS platforms without any prerequisites
- Adaptable to the specific tools and activity of new APT cases
- Scoring System – providing a way to detect previously unknown software
- Several Export Formats – Syslog (JSON/Key-Value/CEF), HTML, TXT, JSON, CSV
- Throttling of the scan process to reduce the system load to a minimum

1.1 Package

The THOR Package includes the following files and directories:

	Files/Directories
THOR Binaries	thor.exe and thor64.exe , for 32-bit and 64-bit systems respectively
THOR Utility	thor-util.exe , Helper tool for updates, encryption, report generation, signature verification and other tasks – see THOR Util Manual
Configuration Files	In subfolder <code>./config</code> - (directory-excludes.cfg , sigma.yml , false_positive_filters.cfg)
Main Signature Database	In subfolder <code>./signatures</code>
Custom Signatures and Threat Intel IOCs	In subfolder <code>./custom-signatures</code>
THOR Changelog	changes.log
Additional Tools	In subfolder <code>./tools</code> - EXE packers and the Bifrost server script
THOR Manuals	In subfolder <code>./docs</code>

REQUIREMENTS

THOR runs in any Windows, Linux and macOS environment without any further requirements. Everything needed is already included in the program package.

To use the full potential of THOR, you should execute it with administrative privileges - `LOCAL_SYSTEM` on Windows and `root` on Linux/macOS systems.

2.1 Operating Systems

The following operating systems and their versions are the **minimum requirements** to run THOR. Any newer version will also work with THOR.

Linux	Windows	macOS
RHEL/CentOS 6	Windows 7 x86/x64	macOS 10.14 (Mojave)
SuSE SLES 11	Windows Server 2008 R2	macOS 11 (Intel)
Ubuntu 16 LTS		macOS 11 (ARM, Apple M1)
Debian 9		

2.1.1 Legacy Systems

These versions are scannable with THOR Legacy. The legacy version of THOR is usually running on those systems, but if you encounter any problems, we will not be able to fix them. Contact us for details on how to download and use THOR Legacy.

OS	Architecture	Support
Windows Server 2008	x86 and x64	yes
Windows Server 2003 SP2	x86 and x64	limited
Windows Server 2003 SP1	x86 and x64	limited
Windows Server 2003	x86 and x64	limited
Windows XP SP3	x86 and x64	limited
Windows XP SP2	x86 and x64	limited

2.1.2 THOR for AIX

We offer a special version for AIX. Currently only a small number of versions are supported. We are extensively testing THOR on AIX 7.2 with Power7/Power8. THOR for AIX will not run on older versions of AIX. If you are running a newer version and are interested in THOR for AIX, we can always provide a test license to verify if everything is working as expected.

2.1.3 Unsupported

- VMWare ESX - <https://kb.vmware.com/s/article/1036544>
- many others

If you need to perform an analysis on unsupported operating systems or architectures, contact us for a solution using [THOR Thunderstorm](#) and [Thunderstorm collectors](#).

We have productive setups with our customers involving the file collection from:

- SPARC Solaris
- RHEL Linux 4
- Citrix Netscaler
- ICS environments with Windows XP embedded systems (planned)
- VMWare ESX (see this [blog post](#))

2.2 Update Servers

To download the newest updates for THOR and our signatures, you need an active internet connection. The endpoint performing the update needs to reach our update servers to do this.

For a detailed and up to date list of our update and licensing servers, please visit <https://www.nexttron-systems.com/hosts/>.

Hint: You do not need an active internet connection to scan an endpoint. This is only needed if you want to update to the latest THOR and signature versions. There are special licenses for special circumstances, for example when the licensed system does not have internet access.

BEFORE YOU BEGIN

Before you begin to use THOR for the first time, you should read through this section to get a better understanding of what is needed to use THOR.

In the following chapters you should learn how THOR works.

3.1 Add License File

Place a valid license file into the THOR program folder. THOR checks the program folder and all sub folder for valid license files (*.lic). Alternatively, you can specify a specific path with `--licensepath <path>`.

Tip: THOR is also able to fetch licenses from our licensing portal or a local ASGARD Management Center. Please see chapter [License Retrieval](#) for more information about license retrieval.

3.1.1 Generate a License

You can generate a valid license in our [customer portal](#).

Navigate to **Contracts & Licenses > My Contracts** and choose the correct Contract Type to generate a new license. You can use **THOR Workstation** or **THOR Server & Workstation** as the License Type.

Here is an Overview of which type of license you need to use:

- THOR Workstation
 - Host-based THOR scanner license for Windows workstations and macOS only. Not usable on Windows servers or Linux systems, regardless of their actual usage (e.g. Linux Desktop systems). Usage on legacy systems, such as Windows XP, requires the **legacy** option.
- THOR Server & Workstation
 - Host-based THOR scanner license for scans on all end systems, workstations, servers, Windows, Linux, and macOS. Usage on legacy systems, like Windows 2003 or Windows 2008 before R2, requires the **legacy** option.

Click on the green Plus icon of your contract and fill all the mandatory fields. After clicking on **Check Hostnames**, you can issue the license if all the hostnames are unique and valid.

For the license generation it is necessary to use the hostname of the system which will run THOR. On Windows system you should use the `computername` as hostname during license creation:

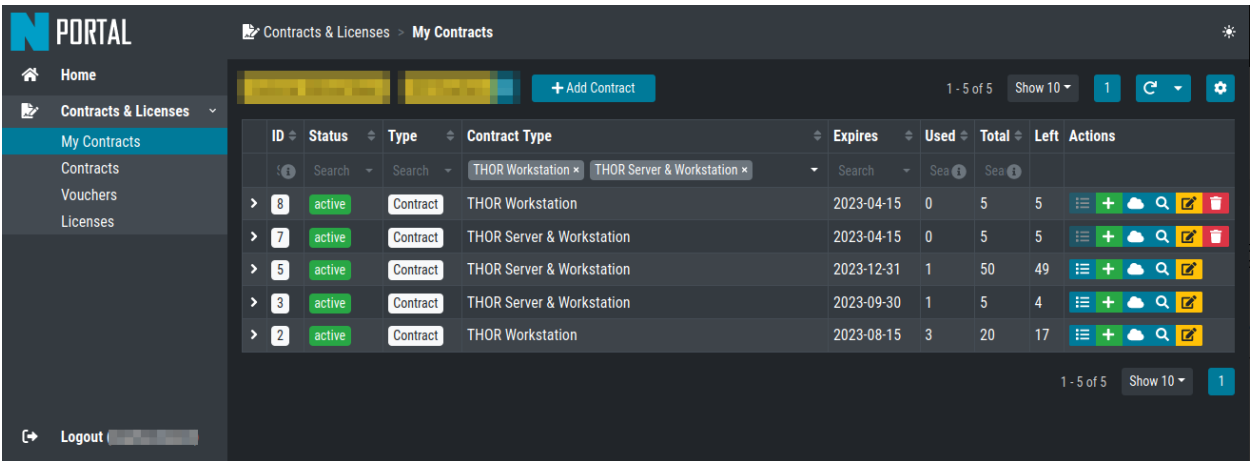


Fig. 1: Contract Overview in the Portal

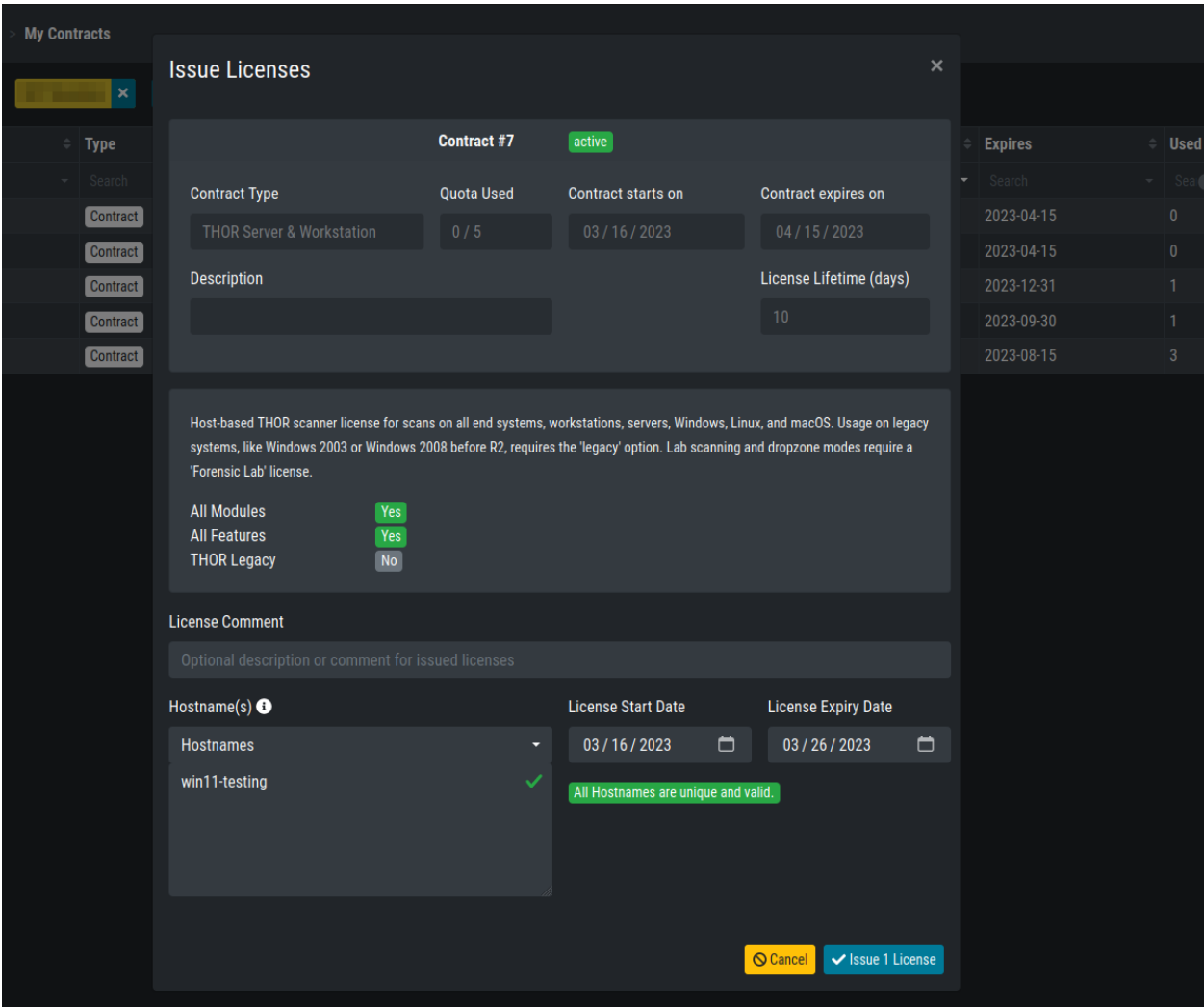


Fig. 2: Generate a License in the Portal

```
C:\Users\nextron>echo %COMPUTERNAME%
WIN11-TESTING
```

On Linux use the hostname command:

```
nextron@unix:~$ hostname
unix
```

On macOS use the following command:

```
MacBook:~ nextron$ sysctl kern.hostname
MacBook
```

Some more remarks regarding the hostname values:

- Use only the hostname of a FQDN (**master1** of **master1.internal.net**)
- The casing of the letters doesn't matter (case-insensitive)
- We do not store the hostnames anywhere in our portal

After you issued your license, your browser will forward you to the Licenses section of the portal. You will be able to see all the issued licenses for the contract you just used earlier. You can either download a single License, a License Bundle, which contains all the selected licenses in one zip file, or a Software + License Bundle, which contains the correct THOR version plus your license(s). If you want to see all your issued licenses for all of your contracts, you can remove the filter on the top which says Contract : xyz.

The screenshot displays the 'Licenses' section of the THOR Portal. The top navigation bar includes 'Home', 'Contracts & Licenses', 'My Contracts', 'Contracts', 'Vouchers', and 'Licenses'. The main content area shows a table of licenses for Contract #8, which is active. The table has columns for Created, Status, Contract Type, Contract ID, License Begins, License Expires, and Actions. Below the table, there is a detailed view of Contract #8, showing its type (THOR Workstation), quota used (1/5), start and end dates, and license lifetime (7 days). At the bottom, there are checkboxes for All Modules, All Features, and THOR Legacy, all of which are checked.

Created	Status	Contract Type	Contract ID	License Begins	License Expires	Actions
2023-03-16 11:02:53	active	THOR Workstation	8	2023-03-16	2023-03-23	[Download] [Bundle]

Contract #8 active

Contract Type	Quota Used	Contract starts on	Contract expires on
THOR Workstation	1 / 5	03 / 16 / 2023	04 / 15 / 2023

Description: [Text Box] License Lifetime (days): 7

All Modules: Yes
All Features: Yes
THOR Legacy: No

Fig. 3: Licenses Overview in the Portal

3.1.2 About License Files

THOR processes its program folder and all sub folders in search for a valid license file with a `.lic` extension, and picks the first valid license it can find.

This change has been made to facilitate the rollout using the new host based license model.

You can now generate licenses for a big set of systems, store all the licenses as `thor-system1.lic`, `this-system2.lic` and so on in a sub folder `./licenses` and transfer the THOR program folder with the "licenses" sub folder to all the different systems, for which you have generated licenses and just run the `thor.exe` executable.

3.2 Upgrade THOR and Update The Signatures

Run the following command to update THOR and its signatures:

Windows:

```
C:\nexttron\thor>thor-util.exe upgrade
Jan 10 09:24:20 win11-testing THOR_UTIL: Info: Read configuration from C:\nexttron\thor\
→config\thor-util.yml

      _____
     /_  _/ // /  _ \  _ \ / // /_  _/  _/ /
    / // _ / // / , _/ / // / // / _/ // /_
   /_ / // _ \ /_ / | | \_ _/ /_ / _/ _/

Copyright by Nextron Systems GmbH, 2021
v1.10.6+thor10.6.19

Jan 10 09:24:20 win11-testing THOR_UTIL: Info: Starting Upgrade Process
Jan 10 09:24:20 win11-testing THOR_UTIL: Info: License file found OWNER: Rick Roll TYPE:
→client STARTS: 2022/08/09 EXPIRES: 2023/08/09
Jan 10 09:24:20 win11-testing THOR_UTIL: Info: Downloading 'thor-win'
Jan 10 09:24:20 win11-testing THOR_UTIL: Info: Downloading from: https://update1.nexttron-
→systems.com/getupdate.php?full=1&lic=00000000000000000000000000000000&product=thor10-
→win&thorupgrader=1.10.6%2Bthor10.6.19&thorversion=10.6.19&upgrade_only=1
Jan 10 09:24:20 win11-testing THOR_UTIL: Info: already up-to-date
Jan 10 09:24:20 win11-testing THOR_UTIL: Info: THOR 10 detected, also updating
→signatures ...
Jan 10 09:24:20 win11-testing THOR_UTIL: Info: Starting Upgrade Process
Jan 10 09:24:20 win11-testing THOR_UTIL: Info: License file found OWNER: Rick Roll TYPE:
→client STARTS: 2022/08/09 EXPIRES: 2023/08/09
Jan 10 09:24:21 win11-testing THOR_UTIL: Info: Downloading 'signatures'
Jan 10 09:24:21 win11-testing THOR_UTIL: Info: Downloading from: https://update1.nexttron-
→systems.com/getupdate.php?full=1&lic=00000000000000000000000000000000&
→product=signatures&thorupgrader=1.10.6%2Bthor10.6.19&thorversion=23.1.5-122954&upgrade_
→only=1
Jan 10 09:24:21 win11-testing THOR_UTIL: Info: downloaded package as zip
Jan 10 09:24:28 win11-testing THOR_UTIL: Info: Successfully upgraded from Signatures 23.
→1.5-122954 to Signatures 23.1.9-153938
```

Linux:

```

nextron@unix:~/Documents/thor$ ./thor-util upgrade
Jan 10 09:33:10 unix THOR_UTIL: Info: Read configuration from /home/nextron/Documents/
↳ thor/config/thor-util.yml

      _____
     /_  _/ // /  _ \  _ \ / // /_  _/  _/ /
    / // _ / // / , _ / // / // /_ // /_
   /_ / // / \____/ _/ | | \____/ // / ____/

Copyright by Nextron Systems GmbH, 2021
v1.10.6+thor10.6.19

Jan 10 09:33:10 unix THOR_UTIL: Info: Starting Upgrade Process
Jan 10 09:33:10 unix THOR_UTIL: Info: License file found OWNER: Rick Roll TYPE: client_
↳ STARTS: 2023/01/10 EXPIRES: 2023/08/14
Jan 10 09:33:10 unix THOR_UTIL: Info: Downloading 'thor-linux'
Jan 10 09:33:10 unix THOR_UTIL: Info: Downloading from: https://update1.nextron-systems.
↳ com/getupdate.php?full=1&lic=00000000000000000000000000000000&product=thor10-linux&
↳ thorupgrader=1.10.6%2Bthor10.6.19&thorversion=10.6.19&upgrade_only=1
Jan 10 09:33:11 unix THOR_UTIL: Info: already up-to-date
Jan 10 09:33:11 unix THOR_UTIL: Info: THOR 10 detected, also updating signatures ...
Jan 10 09:33:11 unix THOR_UTIL: Info: Starting Upgrade Process
Jan 10 09:33:11 unix THOR_UTIL: Info: License file found OWNER: Rick Roll TYPE: client_
↳ STARTS: 2023/01/10 EXPIRES: 2023/08/14
Jan 10 09:33:11 unix THOR_UTIL: Info: Downloading 'signatures'
Jan 10 09:33:11 unix THOR_UTIL: Info: Downloading from: https://update1.nextron-systems.
↳ com/getupdate.php?full=1&lic=00000000000000000000000000000000&product=signatures&
↳ thorupgrader=1.10.6%2Bthor10.6.19&thorversion=23.1.9-153938&upgrade_only=1
Jan 10 09:33:11 unix THOR_UTIL: Info: already up-to-date

```

It is **important** that you update THOR after you have downloaded it from the customer portal, since the packages do not contain the newest signature files. (caused by internal integrity checks)

Note: The upgrade requires a valid license for the host that performs the update. If you don't want to use a license for that host, ask us for a **silent license**, which can be used for all kinds of testing purposes and also allows to update THOR and its signatures.

3.3 Define an Antivirus / EDR Exclusion

Since THOR accesses different process memories and probes for malicious Mutex, Named Pipes and Event values, it is recommended to exclude THOR from Antivirus / EDR scanning.

The Antivirus exclusion could also lead to a significant runtime reduction, since access to processes memory and files will not get intercepted anymore.

Note: We see massive runtime changes with Windows Defender since April 2021 (+50-100%). It is highly recommended to exclude THOR from scanning when using Windows Defender.

The quickest way to add an exclusion on a single system is with the following command (change the path in -ExclusionProcess accordingly).

Windows command line:

```
C:\Users\nextron>powershell -ep bypass -Command "Add-MpPreference -ExclusionProcess 'c:\temp\thor\thor64.exe'"
```

PowerShell:

```
PS C:\Users\nextron> Add-MpPreference -ExclusionProcess 'c:\temp\thor\thor64.exe'
```

For more information visit <https://docs.microsoft.com>.

3.3.1 A Note on SentinelOne

The process memory of systems running SentinelOne is polluted with suspicious strings. The most prevalent false positive is related to the keyword "ReflectiveLoader", but any other rule can match as well.

It is unclear what SentinelOne does to the process memory of many system processes. We cannot exclude these signatures from the scan. Be aware that the results from the "ProcessCheck" module on a system running SentinelOne can contain many false positives.

3.3.2 A Note on McAfee

It is not an easy task to define exclusions for THOR in all the different services when running McAfee products. You have to exclude the process in different sections (AV, EDR, On-Access). We've compiled a list of exclusions for our ASGARD customers, which you can find [here](#).

3.4 Choose The Right THOR Variant

We offer THOR in different variants.

- THOR
- THOR TechPreview
- THOR Legacy (limited support and compatibility)

3.4.1 THOR

The default version of THOR is the most stable version, intensively tested and without any broadly tested performance and detection tweaks.

The default version should be used for:

- Scan sweeps on hundreds or thousands of systems
- Continuous compromise assessments on hundreds or thousands of systems
- Systems with high requirements on stability

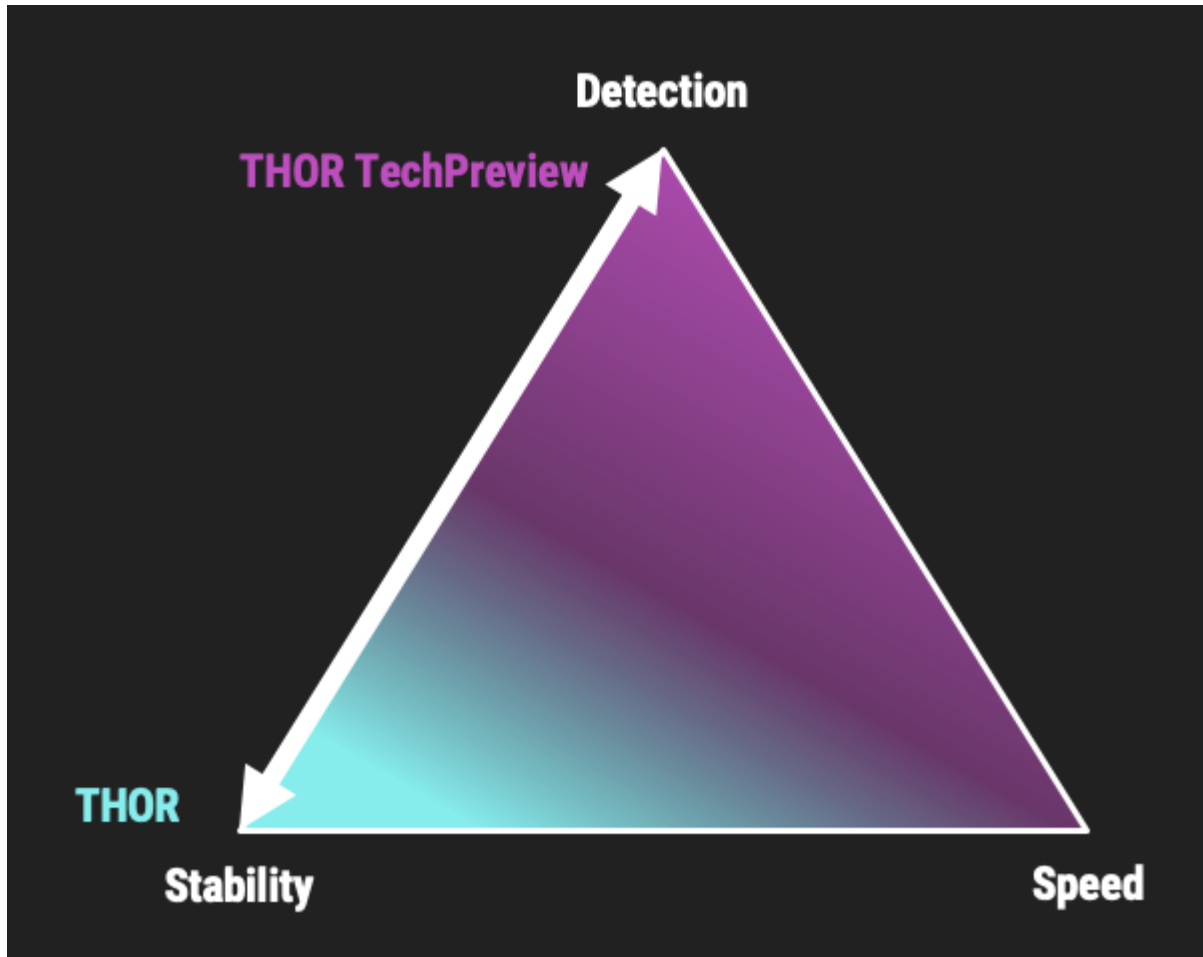


Fig. 4: THOR Default and TechPreview Focus

3.4.2 THOR TechPreview

The TechPreview version is focussed on detection and speed. This [blog post](#) contains more information on the differences.

The TechPreview version should be used for:

- Digital forensic lab scanning
- Dropzone mode scanning
- Image scanning
- THOR Thunderstorm setups
- Single system live forensics on systems that don't have highest priority on stability

You can find the information on how to get the TechPreview version in the [THOR Util manual](#).

3.4.3 THOR Legacy

THOR Legacy is a stripped down version that includes all modules that can be used on outdated operating systems. This [blog post](#) contains more information on the legacy version.

The legacy version lacks:

- Diagnostic features of THOR Util
- UPX unpacking
- ADS scanning
- Module: Process scanning
- Module: Eventlog scanning
- Module: THOR Thunderstorm
- Module: ETW Watcher
- Module: Task scheduler
- HTML report generation

Note: We only offer limited support for this version, since we cannot guarantee a successful stable scan on platforms that have already been deprecated.

To use THOR Legacy, you need a special license. Contact sales to get more information regarding Legacy licenses.

To download THOR Legacy, you can either download it directly from our portal (recommended; continue at step 5), or follow these steps:

1. Download a normal THOR package (non-legacy)
2. Use thor-util to download THOR Legacy:
`thor-util.exe download --legacy -t thor10-win`
3. You will get a zip file with the following name:
`thor-win-10.6.20_<date>-<time>.zip`
4. The content of this zip file should be as follows:

```

25K Feb 13 16:24 changes.log
4.0K Feb 13 16:24 config
4.0K Feb 13 16:24 custom-signatures
4.0K May 22 16:48 docs
4.0K May 22 16:48 signatures
27M Feb 13 16:24 thor64-legacy.exe
256 Feb 13 16:24 thor64-legacy.exe.sig
23M Feb 13 16:24 thor-legacy.exe
256 Feb 13 16:24 thor-legacy.exe.sig
5.7M Feb 13 16:24 thor-legacy-util.exe
256 Feb 13 16:24 thor-legacy-util.exe.sig
4.0K Feb 13 16:24 tools

```

5. You can now transfer this package to your Legacy system. Please do an upgrade before you start using this:

```
thor-legacy-util.exe upgrade
```

```
thor-legacy-util.exe update
```

6. Place your Legacy license inside this folder and start using THOR Legacy

3.5 Choose The Right Architecture

You will find a 32 and 64 bit version of the executable in the program folder. Never run the 32bit version of THOR named `thor.exe` on 64bit system. The 32bit version has some limitations that the 64bit version doesn't have (memory usage, sees different folders on disk and registry versions).

Make sure to run the correct binary for your target architecture.

3.6 Choose The Right Command Line Flags

The recommended way to run THOR has already been put into the default. So, the recommended way to start a THOR is without any command line flags.

However, special circumstances can lead to different requirements and thus a different set of command line flags. See chapter [Scan](#) for often used flags.

3.7 Add Command Line Completions (optional)

Since version 10.7.15, THOR offers shell completions for browsing the flags. These completions can be generated by using:

```
thor-linux-64 --completions <bash/zsh/fish/powershell>
```

This generates a snippet for the specified shell that can be loaded for the current terminal using the following command, depending on your shell:

- bash:

- ```
source <(thor-linux-64 --completions bash)
```
- zsh:

```
source <(thor-linux-64 --completions zsh)
```
  - fish:

```
thor-linux-64 --completions fish | source
```
  - PowerShell:

```
thor64.exe --completions powershell | Out-String | Invoke-Expression
```

## 3.8 Verify Public Key Signatures (optional)

You can verify the executable files in the THOR package with

- their digital signature (PE signature) issued by "Nextron Systems GmbH"
- thor-util's "verify" feature
- openssl verifying the integrity of executables manually

Find more information on THOR Util in its dedicated [online manual](#).

---

**Hint:** THOR Util automatically verifies the signatures of the contained binaries in an update package and exits if one or more signatures cannot be verified. You don't have to check them manually unless you distrust the THOR Util itself. In this case, you can use the public key published on [our web page](#).

---

After downloading the public key the signatures can be manually verified with the following command:

```
C:\Users\nextron>openssl dgst -sha256 -verify <Path to public key .pem> -signature <Path to signature .sig> <Path to the executable>
```

Example Windows:

```
C:\Users\nextron>openssl dgst -sha256 -verify codesign.pem -signature thor64.exe.sig thor64.exe
Verified OK
```

Example Linux:

```
user@unix:~/thor$ openssl sha256 -verify codesign.pem -signature thor-linux.sig thor-linux
Verified OK
```

## DEPLOYMENT

This chapter lists different ways to deploy THOR in an environment. Most of these methods are OS specific.

### 4.1 Licensing

In almost any method of deployment, the provision of valid licenses for the scanners on the endpoints is a core issue. Every license is limited to a certain host name. The only exception are the rare and relatively expensive "Incident Response" licenses.

In all other cases, a valid license has to be generated before a scan run.

There are numerous options to retrieve a valid license for a host.

With ASGARD:

- use an ASGARD Agent
- download THOR package with license from ASGARD's Downloads section
- generate licenses in ASGARD's web GUI under Licensing > Generate Licenses
- use THOR's `--asgard` and `--asgard-token` parameters to retrieve a license
- use ASGARD's API to retrieve a license manually

Without ASGARD:

- generate a license in the web GUI of the [customer portal](#)
- use THOR's `--portal-key` and `--portal-contracts` parameters to retrieve a license from the customer portal
- use the Customer Portal's API to retrieve a license manually

Some of the options are described in more detail in the following two chapters.

#### 4.1.1 Retrieve Valid License From ASGARD

##### Use THOR's `--asgard` and `--asgard-token` parameters

In ASGARD 2.5+ you're able to configure a download token to limit the download of THOR packages and licenses to clients with knowledge of this token. The token is a protection that no one without knowledge of that token can intentionally exceed your license quota limit or retrieve a THOR package without authorization.

The download token can be configured in the Downloads section of you ASGARD server.

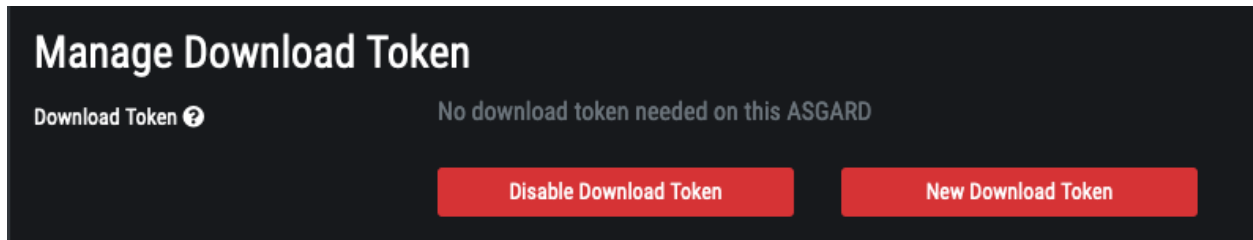


Fig. 1: Downloads &gt; Download Token Configuration

You can retrieve an appropriate THOR license at the scan start using the built-in `--asgard` and `--asgard-token` parameters.

```
C:\temp\thor>thor64.exe --asgard my-asgard.internal
```

```
C:\temp\thor>thor64.exe --asgard my-asgard.internal --asgard-token_
↪OCU92GW1Cy0JLzaHkGrim1v200_ZkHPu0A
```

If everything works as expected, you'll see an INFO level message in the output that looks like:

```
Info: Init License file found LICENSE: my-asgard.internal OWNER: Master ASGARD: ACME Inc_
↪TYPE: Workstation STARTS: 2021/06/18 EXPIRES: 2022/06/18 SCANNER: All Scanners VALID:_
↪true REASON:
```

### Use ASGARD's API to retrieve a license manually

You can also script the license retrieval from a local ASGARD server by using the API. The help box in ASGARD's Licensing > Generate License section shows curl requests that can be used to retrieve licenses from your ASGARD server.

All you need is:

- Hostname
- System Type (server or workstation)

---

**Hint:** Linux is always using the server license type

---

If there is uncertainty it's recommended to generate server type licenses which are more expensive but run on both system types.

For example: To retrieve a valid license for the servers named SRV001 and SRV002 you can use the following command:

```
nexttron@unix:~$ curl -XPOST "https://my-asgard.internal:8443/api/v0/licensing/issue?
↪token=0JCBAq4VGLjrCes2k4ACQ0zg0AxAoz01" -o licenses.zip -d "type=server" -d
↪"hostnames=SRV001" -d "hostnames=SRV002" ... -d "hostnames=hostnameN"
```

If you can't use curl and want to retrieve a license as part of a bigger PowerShell script, you can use the following code snippet to help you with the retrieval.

```
1 # License retrieval script
2 # Florian Roth, June 2021
```

(continues on next page)

### Generate Licenses via API

Licenses can be generated and downloaded via License API.

Run THOR with License from ASGARD:

```
thor64.exe --asgard [redacted] nexttron-systems.com" --asgard-token
[redacted] ...
```

Generate Server License(s) with **curl**:

```
curl -XPOST "https://[redacted]nexttron-systems.com:8443/api/v0/licensing/issue?
token=[redacted] -o licenses.zip -d "type=server" -d
"hostnames=hostname1" -d "hostnames=hostname2" ... -d "hostnames=hostnameN"
```

Generate Workstation License(s) with **curl**:

```
curl -XPOST "https://[redacted]nexttron-systems.com:8443/api/v0/licensing/issue?
token=[redacted] -o licenses.zip -d "type=workstation" -d
"hostnames=hostname1" -d "hostnames=hostname2" ... -d "hostnames=hostnameN"
```

Download all License(s) with **curl**:

```
curl -XGET "https://[redacted]nexttron-systems.com:8443/api/v0/licensing/download-all?
token=[redacted] -o licenses.zip
```

**i** The license generation via API is restricted by a Download Token that can be configured or disabled [here](#).

Fig. 2: Licensing &gt; Generate Licenses

(continued from previous page)

```

3
4 # ASGARD URL
5 $AsgardURL = "https://asgard.nextron-systems.com:8443/api/v0/licensing/issue"
6 $Token = ""
7 $LicenseFile = "licenses.zip"
8 $OutputPath = ".\"
9 $ExtractLicenses = $True
10
11 # Config
12 # Ignore Self-signed certificates
13 [System.Net.ServicePointManager]::ServerCertificateValidationCallback = {$true}
14 # Set current working directory for .NET as well
15 [Environment]::CurrentDirectory = (Get-Location -PSProvider FileSystem).ProviderPath
16
17 # Web Client
18 [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
19 $WebClient = New-Object System.Net.WebClient
20 if ($Token) {
21 $AsgardURL = [string]::Format("{0}?token={1}", $AsgardURL, $Token)
22 }
23 Write-Host "Using URL: $AsgardURL"
24
25 # Hostname
26 $Hostname = $env:COMPUTERNAME
27
28 # License Type
29 $LicenseType = "server"
30 $OsInfo = Get-CimInstance -ClassName Win32_OperatingSystem
31 if ($OsInfo.ProductType -eq 1) {
32 $LicenseType = "workstation"
33 }
34
35 # Proxy Support
36 $WebClient.Proxy = [System.Net.WebRequest]::DefaultWebProxy
37 $WebClient.Proxy.Credentials = [System.Net.CredentialCache]::DefaultNetworkCredentials
38
39 # Prepare request
40 $postData=New-Object System.Collections.Specialized.NameValueCollection
41 $postData.Add('hostnames',$Hostname)
42 $postData.Add('type',$LicenseType)
43 Write-Host "Requesting license for HOST: $Hostname TYPE: $LicenseType"
44
45 # Request license
46 try {
47 $Response = $WebClient.UploadValues($AsgardURL, $postData)
48 # HTTP Errors
49 } catch [System.Net.WebException] {
50 Write-Host "The following error occurred: $_"
51 $Response = $_.Exception.Response
52 # 403
53 if ([int]$Response.StatusCode -eq 403) {
54 Write-Host "This can be caused by a missing download token."

```

(continues on next page)



(continued from previous page)

```

55 }
56 break
57 }
58 [System.IO.File]::WriteAllBytes($LicenseFile, $Response);
59
60 # Extract licenses
61 if ($ExtractLicenses) {
62 Add-Type -AssemblyName System.IO.Compression.FileSystem
63 try {
64 [System.IO.Compression.ZipFile]::ExtractToDirectory($LicenseFile, $OutputPath)
65 } catch {
66 Write-Host "The following error occurred: $_"
67 }
68 Remove-Item -Path $LicenseFile
69 }

```

Check the ASGARD helper scripts section in [our Github repo](#) for more scripts and snippets.

## 4.1.2 Retrieve Valid License From Customer Portal

### Use THOR's `--portal-key` and `--portal-contracts` parameters to retrieve a license

To retrieve a licenses from the customer portal, you need a portal key. The portal key (API key) can be configured in the `My Settings > API Key` section of the [customer portal](#).

**Important:** API functionality needs to be activated by Nextron. Please contact support/sales to activate the API functionality.

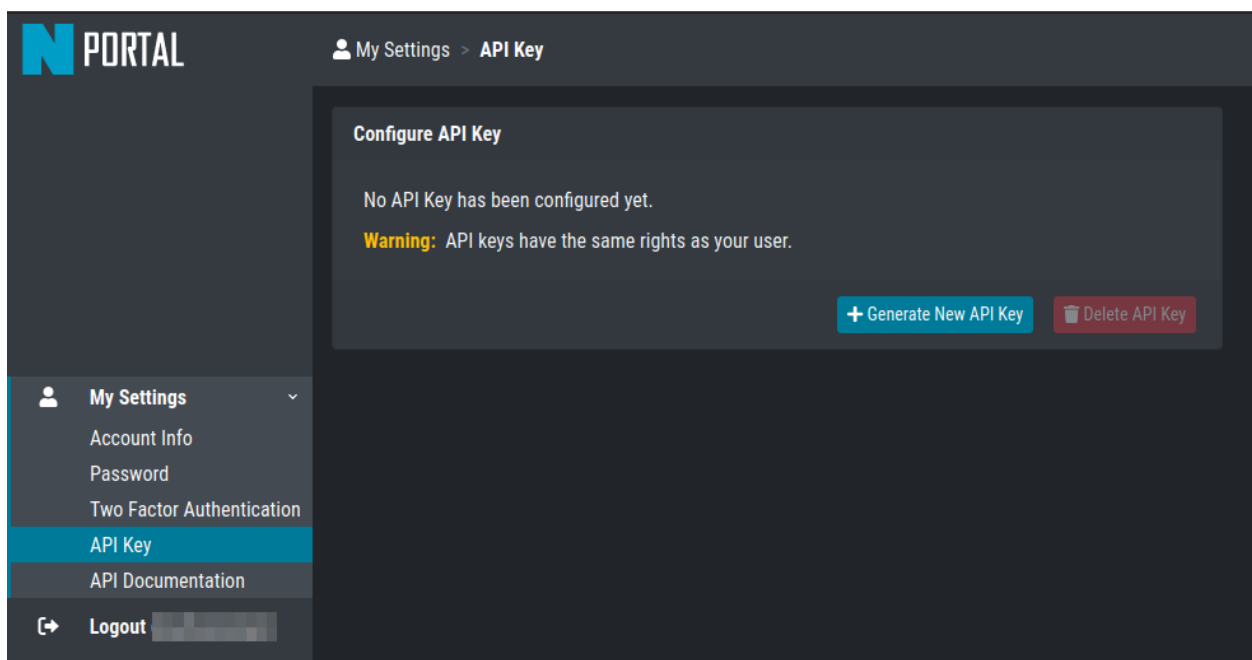


Fig. 3: My Settings > API Key

You can retrieve an appropriate THOR license at the scan start using the built-in `--portal-key` and `--portal-contracts` parameters. The `--portal-contracts` parameter is optional. It can be used to take licenses from a specific contract in case you have more than one and want to use a specific one. If none is set, THOR will automatically retrieve licenses from a contract of the right type. (e.g. retrieve workstation license from the first still valid contract that has workstation licenses available)

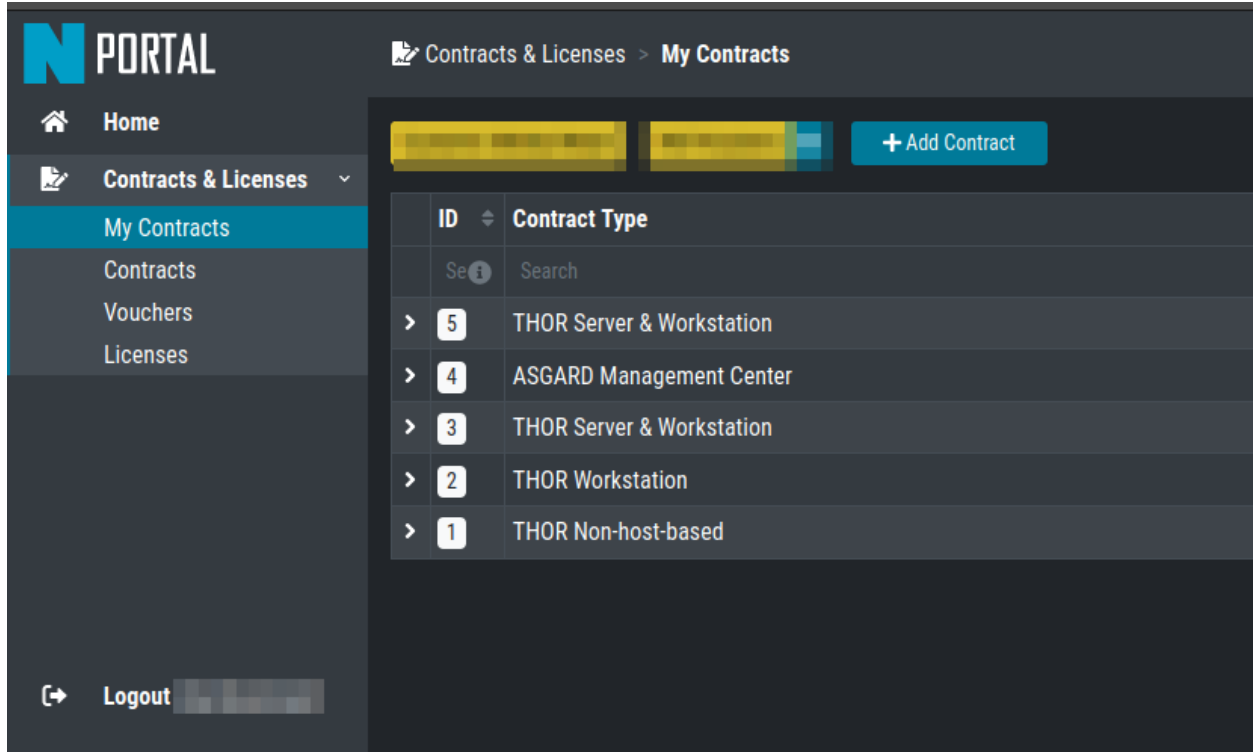


Fig. 4: Contract IDs in Customer Portal

You can then use the parameters as shown in the following examples:

```
C:\temp\thor>thor64.exe --portal-key IY5Y36thrt7h1775tt1ygfuyIadmGzZJmVk32lXcud4
```

```
C:\temp\thor>thor64.exe --portal-key IY5Y36thrt7h1775tt1ygfuyIadmGzZJmVk32lXcud4 --
portal-contracts 3,5
```

If everything works as expected, you'll see an **INFO** level message in the output that looks like:

```
Info License file found LICENSE: portal.nextron-systems.com OWNER: ACME Inc TYPE:
Workstation STARTS: 2021/06/23 EXPIRES: 2021/06/30 SCANNER: All Scanners VALID: true
REASON:
```

You can specify a proxy by setting the `HTTP_PROXY` and `HTTPS_PROXY` environment variables, e.g. to `my-proxy.internal:3000`.

Username and password can be specified as part of the proxy URL as `http://username:password@host:port/`.

## Use the Customer Portal's API to retrieve a license manually

This is a bit more complicated as we've decided long ago that our customer portal will never contain personal or otherwise relatable information and this includes any kind of hostnames - not even in memory. Therefore it's necessary to generate a HMAC SHA1 hash of the lowercased hostname on the client side and include only the hash in the request to our customer portal.

This command generates a HMAC SHA1 of the current host you're working on. If you'd like to generate a license for a different host, simply replace the first part of the command with `echo -n "mycustomname"`.

```
nexttron@unix:~$ echo -n "$(hostname -s)" | tr '[:upper:]' '[:lower:]' | openssl dgst -
↳ binary -sha1 -mac hmac -macopt
↳ hexkey:b190dd4a98456999b6d9c7e4e1ac1f231b978c3e7652898d7db2fcdede34613dbc7909c9fc8b3177bb904871b8b7fc
↳ | base64 | tr '/+' '_-' | tr -d '='
```

The values needed for a successful request are:

- `$CONTRACT` = contract id (set to 0 for automatic selection)
- `$TYPE` = [server/client]
- `$HASH` = the hash generated from the hostname in the previous step
- `$APIKEY` = the API from the User Settings section in the customer portal

```
nexttron@unix:~$ curl -XPOST https://portal.nexttron-systems.com/api/public/contracts/
↳ issue/$CONTRACT/$TYPE/$HASH?download=1 -H "Authorization: $APIKEY" -o license.lic
```

A valid license is an encrypted blob of at least 800 bytes. You can check the content of the license for possible error message that came back from the server using `xxd`.

```
nexttron@unix:~$ xxd license.lic
```

If you find a **Error: HTTP-401** in the file, than you've most likely used an invalid API key.

## 4.2 Network Share (Windows)

THOR is a lightweight tool that can be deployed in many different ways. It does not require installation and leaves only a few temporary files on the target system.

A lightweight deployment option provides the THOR program folder on a read-only network share and makes it accessible from all systems within the network. Systems in DMZ networks can be scanned manually by transferring a THOR program package to the system and run it from the command line. The locally written log files have the same format as the Syslog messages sent to remote SIEM systems and can be mixed without any problem.

We often recommend triggering the scan via "Scheduled Task" distributed to the systems via GPO or PsExec. The servers access the file share at a given time, pull THOR into memory and start the scan process. You can either mount the network share and run THOR from there or access it directly via its UNC path (e.g. `\\server\share\thor.exe` or `\\server\share\thor64.exe`).

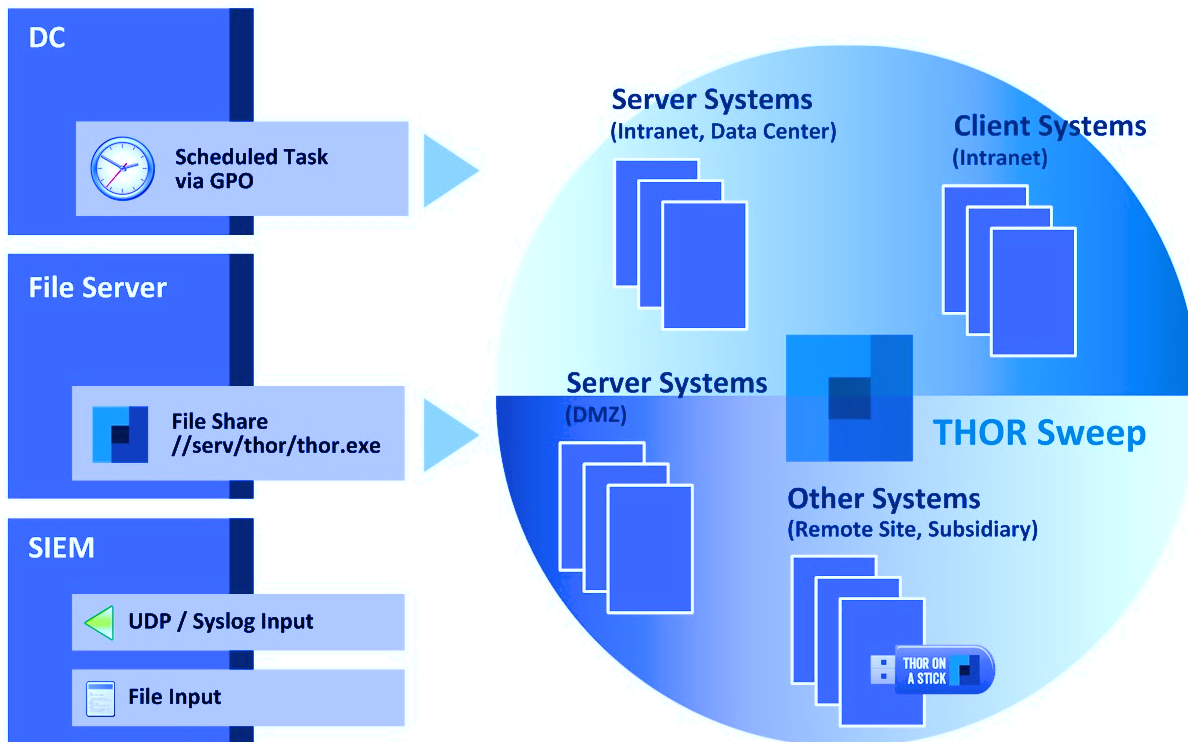


Fig. 5: Deployment via Network Share

#### 4.2.1 Place THOR on a Network Share

A good way to run THOR on multiple systems is by defining a "Scheduled Task" using your Windows domain's group policy functionality.

The preferred way to run THOR on a remote system is by providing a network share on which the extracted THOR package resides. You can use this directory as the output directory but it is recommended to create another share with write permissions especially for the HTML and TXT result files. The share that holds the THOR program folder should be read-only. The various output files must be disabled or defined in different locations in order to avoid write-access errors.

The necessary steps are:

1. Create a network share and extract the THOR package into the root of the share, i.e. `\\fileserver\thor\`
2. Find the "thor\_remote.bat" batch file, which can be found in the "tools" sub folder, place it directly in the root of the program folder and adjust it to your needs.
  - set the network share UNC path
  - set the parameters for the THOR run (see [Scan](#))

You should then test the setting like this:

1. Connect to a remote system (Remote Desktop), which you would like to scan
2. Start a command line "as Administrator" (right click > Run as Administrator)
3. Run the following command, which is going to mount a network drive, run THOR and disconnect the previously mounted drive: `\\fileserver\thor\thor_remote.bat`

After a successful test run, you decide on how to invoke the script on the network drive. The following chapters list different options.

### 4.2.2 Create a Scheduled Task via GPO

In a Windows Domain environment, you can create a Scheduled Task and distribute this Scheduled Task via GPO. This Scheduled Task would invoke the batch file on the network share and runs THOR. Make sure that the respective user account has the rights to mount the configured network share.

You can find more information here:

<https://technet.microsoft.com/en-us/library/cc725745.aspx>

### 4.2.3 Create a Scheduled Task via PsExec

This method uses Sysinternals PsExec and a list of target systems to connect and create a Scheduled Task via the command line. This could look like the following example:

```
C:\temp\thor>psexec \\server1 -u domain/admin -p pass schtasks /create /tn "THOR Run" /
→ tr "\\server\share\thor_remote.bat" /sc ONCE /st 08:00:00 /ru DOMAIN\FUadmin /rp_
→ password
```

### 4.2.4 Start THOR on the Remote System via WMIC

THOR can be started on a remote system via "wmic" using a file share that serves the THOR package and is readable by the user that executes the scan.

```
C:\temp\thor> wmic /node:10.0.2.10 /user:MYDOM\scanadmin process call create "cmd.exe /c_
→ \\server\thor10\thor.exe"
```

## 4.3 ASGARD Management Center (Windows, Linux, macOS)

ASGARD is the central management platform for THOR scans. It manages distributed THOR scans on thousands of systems, collects, forwards and analyses logs. Furthermore, ASGARD can control and execute complex response tasks if needed.

ASGARD comes in two variations: While ASGARD Management Center features scan control and response functions, ASGARD Analysis Cockpit can be used to analyze large amounts of scan logs through an integrated base-lining and case management.

The hardened, Linux-based ASGARD appliance is a powerful, solid and scalable response platform with agents for Windows, Linux and macOS. It provides essential response features like the collection of files, directories and main memory, remote file system browsing and other counteractive measures.

It features templates for scan runs and lets you plan and schedule distributed sweeps with the lowest impact on system resources. Other services are:

- **Quarantine Service** - file quarantine via Bifrost protocol
- **Update Service** - automatic updates for THOR scanners
- **License Service** - central registration and sub license generation

- **Asset Management Service** - central inventory and status dashboard
- **IOC Management** – manage and scan with custom IOC and YARA rule sets
- **Evidence Collection** – collect evidences (files and memory) from asset

| ASGARD Query | Hostname   | First Seen          | Last Seen         | OS      | Last Scan Completed |
|--------------|------------|---------------------|-------------------|---------|---------------------|
| > [icon]     | [redacted] | 2021-10-29 18:16:54 | a few seconds ago | Windows | 2023-03-10 14:41:04 |
| > [icon]     | [redacted] | 2021-10-29 18:05:02 | a few seconds ago | Linux   | 2023-03-04 19:25:41 |
| > [icon]     | [redacted] | 2021-10-29 18:02:05 | a few seconds ago | Linux   | 2022-11-08 10:53:52 |
| > [icon]     | [redacted] | 2021-10-29 17:56:24 | a few seconds ago | Linux   | 2022-10-18 16:16:34 |
| > [icon]     | [redacted] | 2021-10-29 17:53:19 | a few seconds ago | Linux   | 2023-03-04 19:32:43 |
| > [icon]     | [redacted] | 2021-10-29 17:25:51 | a few seconds ago | Linux   | 2022-10-21 08:54:11 |
| > [icon]     | [redacted] | 2021-10-29 16:57:30 | a few seconds ago | Linux   | 2022-10-20 16:22:49 |
| > [icon]     | [redacted] | 2021-10-29 16:51:51 | a few seconds ago | Linux   | 2023-03-04 19:38:47 |
| > [icon]     | [redacted] | 2021-10-29 16:24:40 | a few seconds ago | Windows | 2023-03-10 14:39:32 |
| > [icon]     | [redacted] | 2021-10-29 16:04:02 | a few seconds ago | Windows | 2023-03-10 14:38:02 |
| > [icon]     | [redacted] | 2021-10-29 15:29:25 | a few seconds ago | Windows | 2023-03-10 14:37:18 |
| > [icon]     | [redacted] | 2021-10-29 15:16:24 | a few seconds ago | Windows | 2023-03-10 14:44:54 |
| > [icon]     | [redacted] | 2021-10-29 14:47:19 | a few seconds ago | Windows | 2023-03-10 14:42:10 |
| > [icon]     | [redacted] | 2021-10-29 14:35:42 | a few seconds ago | Windows | 2023-03-10 14:45:24 |
| > [icon]     | [redacted] | 2021-10-29 14:31:16 | a few seconds ago | Windows | 2023-03-10 14:45:31 |
| > [icon]     | [redacted] | 2021-10-29 14:20:11 | a few seconds ago | Windows | 2023-03-10 14:40:10 |

Fig. 6: ASgard Management Center

## 4.4 Ansible (Linux)

### 4.4.1 Distribute Run with Ansible

In practice it is crucial to execute THOR on many servers in a network. A possible way to achieve this is described within this paper, taking into account that the footprint on the target should be minimal and that the procedure should not depend on the used Linux Distribution.

| Status    | Description                                 | Arguments                                                                                              | Hostname | Module         | Status |
|-----------|---------------------------------------------|--------------------------------------------------------------------------------------------------------|----------|----------------|--------|
| Completed | Remote Console                              |                                                                                                        |          | Remote Console | 202    |
| Completed | Remote Console                              |                                                                                                        |          | Remote Console | 202    |
| Error     | Remote Console                              |                                                                                                        |          | Remote Console | 202    |
| Completed | Test PS                                     | PowerShell.exe -ExecutionPolicy Bypass -command "Get-Process   tee process.txt   select ID, Name, CPU" |          | Playbook       | 202    |
|           |                                             | PowerShell.exe -ExecutionPolicy Bypass -command "Get-LocalUser   tee LocalUser.txt"                    |          |                | 11:    |
|           |                                             | PowerShell.exe -ExecutionPolicy Bypass -command "Get-LocalGroup   tee LocalGroup.txt"                  |          |                |        |
| Completed | Create Thor 10 Memory and CPU Graph (Linux) |                                                                                                        |          | Playbook       | 202    |

Fig. 7: ASGARD Response

#### 4.4.2 Ansible

The software Ansible (<https://www.ansible.com>) is a solution to perform tasks distributed over a network on different targets. An Open Source Version is available as well as a version with commercial support for enterprises. Ansible uses SSH to connect to the target hosts and performs a defined set of tasks on them called playbooks. Per default it uses keys for authentication, but this can be setup differently. Please refer to the official documentation for other methods of authentication. The tasks and the targets can be customized using host groups. The host groups may be used to separate different Linux distributions. The other steps may remain the same. Within the playbook any command line option may be customized for the given scenario.

Ansible does parallelization of the tasks by itself. The default amount of parallel executions is five and can be configured using the `-f` or `--forks` parameter when starting the playbooks.

#### 4.4.3 Execute THOR using Ansible

The following section will show how to use an Ansible playbook to execute THOR on multiple Linux systems.

It will perform following steps on each system:

- Create a temporary folder
- Mount a RAM drive using the folder as mount point
- Copy THOR to this RAM drive
- Execute THOR
- Unmount the RAM drive
- Delete the temporary folder

#### 4.4.4 Inventory File

First it is needed to define a list of hosts to execute THOR on. This is done by setting up a YAML file with the hostnames or IP addresses of the hosts. This file is later used with the `-i` parameter in the `ansible-playbook` command. A simple version of this could look like following:

```

host1.com
host2.com
132.123.213.111
```

To learn more about Ansible inventory files and how to use them, please refer to the official documentation:

[https://docs.ansible.com/ansible/latest/user\\_guide/intro\\_inventory.html](https://docs.ansible.com/ansible/latest/user_guide/intro_inventory.html)

#### 4.4.5 Ansible Playbook Template

```
1 ---
2 - hosts: all
3 #remote_user: root become: true tasks:
4 - name: Create folder for temporary RAM drive
5 command: mkdir /mnt/temp_ram creates=/mnt/temp_ram
6 - name: Create THOR RAM drive on target
7 command: mount -t ramfs -o size=60M ramfs /mnt/temp_ram/ ignore_warnings: true
8 - name: Copy THOR to RAM drive
9 copy: src=../thor-linux-pack/ dest=/mnt/temp_ram/ ignore_warnings: true
10 - name: Make THOR Executeable
11 file: path=/mnt/temp_ram/thor-x64 state=touch mode="0555"
12 - name: Execute THOR
13 command: /mnt/temp_ram/thor64 -l /mnt/temp_ram/thor.txt creates=/mnt/temp_ram/thor.html
14 - name: Fetch Log file
15 fetch: src=/mnt/temp_ram/thor.txt dest=../thoransible-output/{{inventory_hostname}}/thor.
16 ↪txt flat=true
17 - name: Unmount temporary RAM drive
18 mount:
19 path: /mnt/temp_ram
20 state: unmounted
21 - name: check Mount
22 command: mount
23 - name: Delete folder for temporary RAM drive
24 command: rmdir /mnt/temp_ram/
```

#### 4.4.6 Usage of THOR's Ansible playbook

Copy the playbook in the main directory of THOR. After this is done it can be started as follows:

```
nexttron@unix:~$ ansible-playbook -f <number_of_parallel_executions> -i <inventory_file> ↪
↪thorplaybook.yml
```

After the playbook finished running the scans, the output of each system can be found in the **thoransible**-output directory located at the parent directory of THOR. Therefore it is important that the user starting `ansible-playbook` has the required rights to write in this directory.



### 4.4.7 Adjust THOR's Command Line Parameters

Per default this playbook will only start THOR with the parameter that defines the output log file. This can be changed in the playbook in the "Execute THOR"-Task. However, it should be kept in mind, that changing the output log file is not recommended, since the later tasks of the playbook depend on this.

## 4.5 THOR Thunderstorm Service

The command line flag `--thunderstorm` starts THOR as a RESTful web service on a given network interface and port. This service receives samples and returns a scan result.

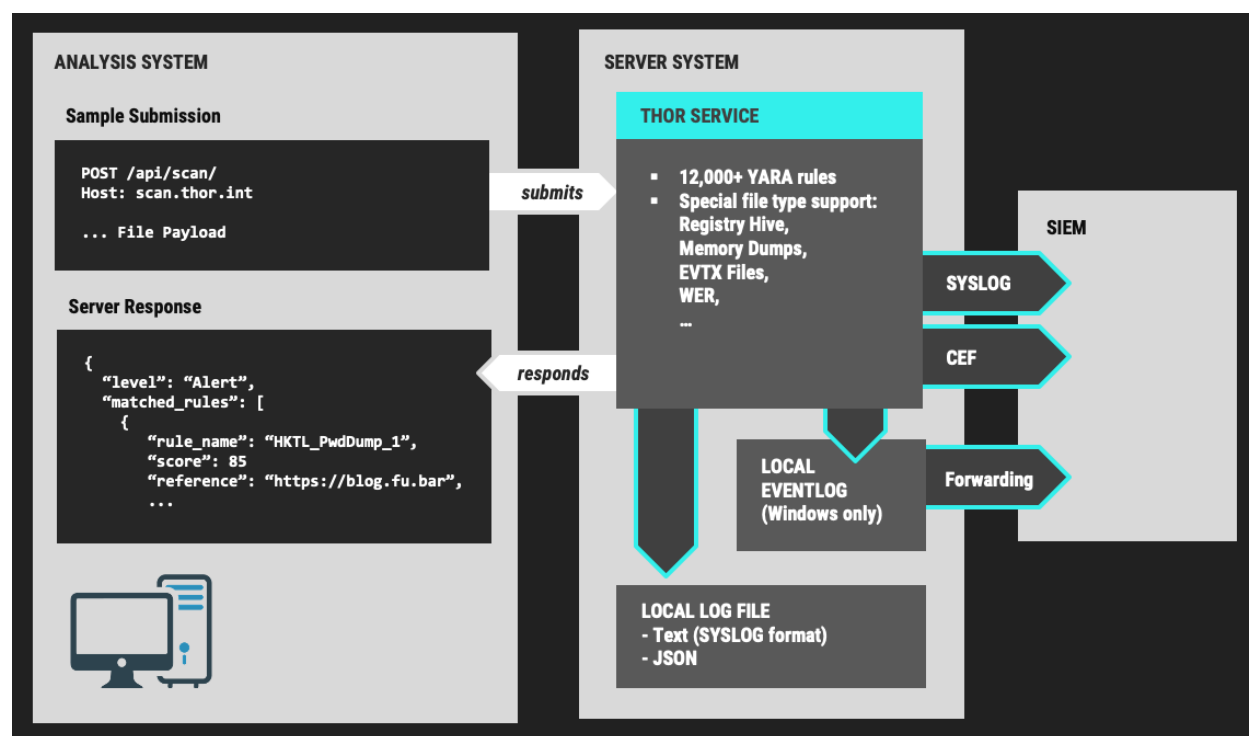


Fig. 8: THOR Thunderstorm Overview

The service can be started in two scan modes:

- Pure YARA
- Full-Featured

In the pure YARA mode (`--pure-yara`) THOR Thunderstorm only applies the 13,000 internal and all custom YARA rules to the submitted samples. It's lightweight and fast.

The full-featured mode is the default. In this mode Thunderstorm also parses and analyses Windows Eventlogs (EVTX), registry hives, memory dumps, Windows error reports (WER) and more. It's not just a YARA scan, but a full forensic processing.

Under normal circumstances, we recommend using the full-featured mode, since most files are not of a type that triggers an intense parsing function, the processing speed should be similar to the "pure-yara" mode.

It is recommended to use "pure-yara" mode in cases in which:

- huge forensic artefacts (EVTX or memory dump files) appear on the source systems and overload the Thunderstorm service
- deeper forensic parsing, IOC matching or other internal THOR checks aren't needed or wanted

The following table contains all THOR Thunderstorm related command line flags:

| Parameter                         | Values             | Function                                                                                                                                                                                                                                                    |
|-----------------------------------|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>--thunderstorm</b>             |                    | Watch and scan all files sent to a specific port (see <b>--server-port</b> ). Disables resource checks and quick mode, activate intense mode, disable ThorDB and apply IOCs platform independently                                                          |
| <b>--server-host</b>              | ip-address         | IP address that THOR's server should bind to (default 127.0.0.1)                                                                                                                                                                                            |
| <b>--server-port</b>              | port number        | TCP port that THOR's server should bind to (default 8080)                                                                                                                                                                                                   |
| <b>--server-cert</b>              | .crt location      | TLS certificate that THOR's server should use. If left empty, TLS is not used                                                                                                                                                                               |
| <b>--server-key</b>               | .key location      | Private key for the TLS certificate that THOR's server should use. Required if <b>--server-cert</b> is specified                                                                                                                                            |
| <b>--pure-yara</b>                |                    | Apply only YARA signatures (no IOCs or other programmatical checks)                                                                                                                                                                                         |
| <b>--server-upload-dir</b>        | upload-directory   | Path to a temporary directory where THOR drops uploaded files. Only relevant for Windows and MacOS. On Linux, THOR stores files in in-memory files. (default /tmp/thor-uploads)                                                                             |
| <b>--server-result-cache-size</b> | number of results  | Size of the cache that is used to store results of asynchronous requests temporarily. If set to 0, the cache is disabled and asynchronous results are not stored. (default 10000)                                                                           |
| <b>--server-store-samples</b>     | all/malicious/none | Sets whether samples should be stored permanently in the folder specified with <b>--server-upload-dir</b> . Specify <b>all</b> to store all samples, or <b>malicious</b> to store only samples that generated a warning or an alert. (default <b>none</b> ) |
| <b>--sync-only-threads</b>        | number of threads  | Number of threads reserved for synchronous requests (only needed in environments in which users use both synchronous and asynchronous mode of transmission)                                                                                                 |
| <b>--threads</b>                  | number of threads  | Number of threads that the Thunderstorm service should use (default: number of detected CPU cores)                                                                                                                                                          |

### 4.5.1 Service License Type

To run THOR in Thunderstorm service mode, you need a special license type named "Service License" that allows this mode of operation.

After the launch of THOR Thunderstorm, we may allow other license types to run THOR in service mode for a limited period of time, so that customers can test the service and its integration into other solutions.

### 4.5.2 Thunderstorm Collectors

### 4.5.3 Thunderstorm API Client

We provide a free and open source command line client written in Python to communicate with the Thunderstorm service.

<https://github.com/NextronSystems/thunderstormAPI>

It can be installed with:

```
nexttron@unix:~$ pip install thunderstormAPI
```

### 4.5.4 Thunderstorm API Documentation

An API documentation is integrated into the web service.

Simply visit the service URL, e.g.: <http://my-server:8080/>

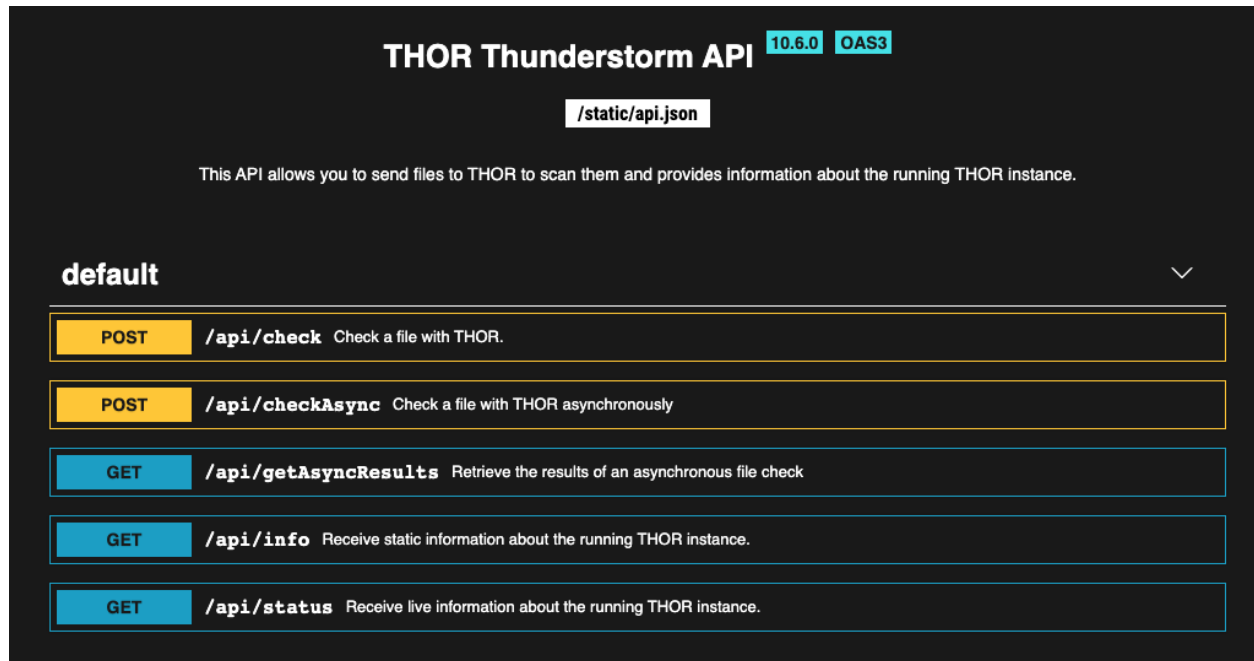


Fig. 9: Thunderstorm API documentation

### 4.5.5 Server Installer Script for Linux

A script that facilitates the installation on Linux systems can be found in our github repository.

<https://github.com/NextronSystems/nextron-helper-scripts/blob/master/thunderstorm/thunderstorm-installer.sh>

The installation of a full THOR Thunderstorm server requires only two steps.

1. Download and place a THOR Service license file in the current working directory
2. Run the following command

```
nexttron@unix:~$ wget -O - https://raw.githubusercontent.com/NextronSystems/nextron-helper-scripts/master/thunderstorm/thunderstorm-installer.sh | bash
```

**Warning:** Please inspect scripts from the internet before executing them!

Everything else will automatically be handled by the installer script. It even supports an “uninstall” flag to remove all files and folders from the system to get the system clean again after a successful proof-of-concept.

After the installation, the configuration file is located in `/etc/thunderstorm`.

The log file of the service can be found in `/var/log/thunderstorm`.

### 4.5.6 Thunderstorm Update

The Thunderstorm service gets updated just as THOR does. Use "thor-util update" to update signatures or "thor-util upgrade" to update binaries and signatures. The service has to be stopped during the updates.

Update signatures:

```
nexttron@unix:~$ thor-util update
```

Upgrade signatures:

```
nexttron@unix:~$ thor-util upgrade
```

See the [THOR Util Manual](#) manual for details on how to use these functions.

### Thunderstorm Update Script

The Thunderstorm installer script for Linux automatically places an updater script in the PATH of the server system.

<https://github.com/NextronSystems/nextron-helper-scripts/tree/master/thunderstorm>

Update binaries and signatures:

```
nexttron@unix:~$ thunderstorm-update
```

Stop service, update binaries and signatures, restart service:

```
nexttron@unix:~$ thunderstorm-update full
```

```
root@ygdrasil:/mnt/workspace/thunderstorm-installer# ./thunderstorm-setup.sh
=====
 _/__
 /_\
 /_\
 v0.1.2

THOR Thunderstorm Service Installer
Florian Roth, September 2020
=====

The script will make the following changes to your system:
 1. Install THOR into /opt/nextron/thunderstorm
 2. Drops a base configuration into /etc/thunderstorm
 3. Create a log directory /var/log/thunderstorm for log files of the service
 4. Create a user named 'thunderstorm' for the new service
 5. Create a new service named 'thor-thunderstorm'

You can uninstall THOR Thunderstorm with './thunderstorm-installer uninstall'

Are you ready to install THOR Thunderstorm? y
Started Thunderstorm Installer - version 0.1.2
Writing logfile to ./Thunderstorm_Installer_ygdrasil_20200904.log
HOSTNAME: ygdrasil
IP: 172.17.0.1 10.0.2.27
OS: BUG_REPORT_URL="https://bugs.debian.org/";HOME_URL="https://www.debian.org/";ID=debian
ME="Debian GNU/Linux 10 (buster)";SUPPORT_URL="https://www.debian.org/support";VERSION="10";
VERSION_ID="10";
ISSUE: Debian GNU/Linux 10 \n \l
KERNEL: Linux ygdrasil 4.19.0-8-amd64 #1 SMP Debian 4.19.98-1+deb10u1 (2020-04-27) x86_64
Checking the required utilities ...
All required utilities found.
Searching for license file in current folder ...
Found license file 9-20200409-020000-1.lic
Evaluated license hash: 8b7e4e6a10368d55a1720e54650b455f
Creating new directory '/opt/nextron/thunderstorm' ...
Creating new user 'thunderstorm' ...
Adding system user `thunderstorm' (UID 117) ...
```

Fig. 10: Thunderstorm Service Installer

### 4.5.7 Source Identification

The log file generated by THOR Thunderstorm doesn't contain the current host as hostname in each line. By default, it contains the sending source's FQDN or IP address if a name cannot be resolved using the locally configured DNS server.

However, every source can set a “source” value in the request and overwrite the automatically evaluated hostname. This way users can use custom values that are evaluated or set on the sending on the end system.

```
nexttron@unix:~$ curl -X POST "http://myserver:8080/api/check?source=test" -F
 ↪ "file=@sample.exe"
```

### 4.5.8 Synchronous and Asynchronous Mode

It is also important to mention that THOR Thunderstorm supports two ways to submit samples, a synchronous and an asynchronous mode.

The default is synchronous submission. In this mode, the sender waits for the scan result, which can be empty in case of no detection or contains match elements in cases in which a threat could be identified.

In asynchronous mode, the submitter doesn't wait for the scan result but always gets a send receipt with an id, which can just be discarded or used to query the service at a later point in time. This mode is best for use cases in which the submitter doesn't need to know the scan results and batch submission should be as fast as possible.

|                                  | Synchronous                            | Asynchronous                                |
|----------------------------------|----------------------------------------|---------------------------------------------|
| Server API Endpoint              | /api/check                             | /api/checkAsync                             |
| ThunderstormAPI Client Parameter |                                        | --asyn                                      |
| Advantage                        | Returns Scan Result                    | Faster submission                           |
| Disadvantage                     | Client waits for result of each sample | No immediate scan result on the client side |

In asynchronous mode, the Thunderstorm service keeps the samples in a queue on disk and processes them one by one as soon as a thread has time to scan them. The number of files in this queue can be queried at the status endpoint **/api/status** and checked on the landing page of the web GUI.

In environments in which the Thunderstorm service is used to handle synchronous and asynchronous requests at the same time, it is possible that all threads are busy processing cached asynchronous samples and not more synchronous requests are possible.

In this case use the **--sync-only-threads** flag to reserve a number of threads for synchronous requests. (e.g. **--threads 40 --sync-only-threads 10**)

### 4.5.9 Performance Tests

Performance tests showed the differences between the two submission modes.

In Synchronous mode, sample transmission and server processing take exactly the same time since the client always waits for the scan result. In asynchronous mode, the sample transmission takes much less time, but the processing on the server takes a bit longer, since the sever caches the samples on disk.

|                     | Synchronous | Asynchronous |
|---------------------|-------------|--------------|
| Client Transmission | 40 minutes  | 18 minutes   |
| Server Processing   |             | 46 minutes   |
| Total time          | 40 minutes  | 46 minutes   |

### 4.5.10 SSL/TLS

We do not recommend the use of SSL/TLS since it impacts the submission performance. In cases in which you transfer files through networks with IDS/IPS appliances, the submission in an SSL/TLS protected tunnel prevents IDS alerts and connection resets by the IPS.

Depending on the average size of the samples, the submission frequency and the number of different sources that submit samples, the transmission could take up to twice as much time.

Note: The thunderstormAPI client doesn't verify the server's certificate by default as in this special case, secrecy isn't important. The main goal of the SSL/TLS encryption is an obscured method to transport potentially malicious samples over network segments that could be monitored by IDS/IPS systems. You can activate certificate checks with the `--verify` command line flag or `verify` parameter in API library's method respectively.

## 4.6 THOR Remote

THOR Remote is a quick method to distribute THOR in a Windows environment. It has been developed during an incident response and can be considered as a clever hack that makes use of PsExec to push and execute THOR with certain parameters on remote systems.

Requirements:

- Administrative Domain Windows user account with access rights on the target systems
- Reachability of the target systems (Windows Ports):
  - 135/tcp for SCM (Service Management)
  - 445/tcp for SMB (Mounting)
- A list of target systems

Advantages:

- Agent-less
- Comfortable scanning without scripting
- Quick results (useful in incident response scenarios)

Disadvantages:

- Requires reachability of Windows ports
- User credentials remain on the target system if it is used with explicit credentials (NTLM Auth) and the users doesn't already use an account that has access rights on target systems (Kerberos Auth)

### 4.6.1 Usage

A list of parameters used with the remote scanning function can be found in the help screen.

```
> Flags for THOR Remote:
--remote strings Target host (use multiple --remote <host> statements for a set of hosts)
--remote-debug Debug Mode for THOR Remote
--remote-dir string Upload THOR to this remote directory (default "C:\\WINDOWS\\TEMP\\thor10-remote")
--remote-password string Password to be used to authenticate against host
--remote-prompt Prompt for password
--remote-rate int Number of seconds to wait between scan starts (default 30)
--remote-user string Username (alternatively use windows integrated authentication)
--remote-workers int Number of concurrent scans (default 25)
```

Fig. 11: THOR Remote Usage

As you can see, a list of target hosts can be provided with the help of the new YAML config files. See [chapter Configuration](#) for more details.

A YAML file with a list of hosts looks like this:

```
remote:
- winatl001.dom.int
- winatl002.dom.int
- winnyk001.dom2.int
```

You can then use that file with:

```
C:\nexttron\thor>thor64.exe -t targets.yml
```

### 4.6.2 THOR Remote Licensing

Valid licenses for all target systems are required. Place them in the program folder or any sub folder within the program directory (e.g. ./licenses). In case of incident response licenses, just place that single license in the program folder.

You don't need a valid license for the system that runs THOR's remote scanning feature (the source system of the scans, e.g. admin workstation).

---

**Hint:** You can pair THOR Remote with the [License Retrieval](#) options available within THOR, to make deployment easier.

---

### 4.6.3 Output

The generated log files are collected and written to the folder ./remote-logs

The "THOR Remote" function has its own interface, which allows you to view the progress of the scans, view and scroll through the log files of the different remote systems.



```

+-----+-----+
| Hosts | THOR Events of dc-2016.testing |
+-----+-----+
client-win10.testing	Info: Report End Time: Thu Aug 8 12:55:02 2019
dc-2016.testing	Info: Report Scan took 0 hours 0 mins 4 secs
unknown.testing	Notice: Report Thor Scan finished TIME: Thu Aug 8 12:55:02 2019 ALERTS: 0 WARNINGS: 0 NOTICES: 0...
	Info: ThorDB Successfully closed ThorDB
	ok
+-----+-----+	
Console	
+-----+-----+	
Info: Remote The following remotes will be scanned HOSTS: client-win10.testing dc-2016.testing	
unknown.testing	
Info: Remote Mounting share HOST: client-win10.testing USER: MOUNT: \\client-win10.testing\c$	
+-----+-----+

+-----+-----+
| Status | Hosts |
+-----+-----+
Pending 0	Info: Remote Starting THOR service HOST: dc-2016.testing
Running 0	Info: Remote Deleting THOR service HOST: dc-2016.testing
Completed 2	Info: Remote Deleting THOR pioneer service HOST: dc-2016.testing
Failed 1	Info: Remote Deleting THOR directory HOST: dc-2016.testing PATH:
	\\dc-2016.testing\c$\WINDOWS\TEMP\thor10-remote
+-----+-----+	
Keybindings	Info: Remote Unmounting share HOST: dc-2016.testing MOUNT: \\dc-2016.testing\IPC$
C-c, q Exit	Info: Remote Unmounting share HOST: dc-2016.testing MOUNT: \\dc-2016.testing\c$
Right Next Host	Info: Remote Successfully scanned remote HOST: dc-2016.testing
Left Previous...	Info: Remote Mounting share HOST: unknown.testing USER: MOUNT: \\unknown.testing\c$
+-----+-----+

```

Fig. 12: THOR Remote Interface

## 4.6.4 Issues

### System Error 5 occurred – Access Denied

See: <https://helgeklein.com/blog/2011/08/access-denied-trying-to-connect-to-administrative-shares-on-windows-7/>

### Running THOR from a Network Share

THOR must reside on the local file system of the source system. Don't run it from a mounted network share. This could lead to the following error:

```
CreateFile .: The system cannot find the path specified.
```

## 4.7 Distribute to Offline Networks / Field Offices

The quickest and most simple way to run THOR is by providing the ZIP archive to the colleagues in the remote location, letting them run the THOR executable and collect the report files afterwards.

The most usable format in this use case is the HTML report if only a few reports have to be analyzed. If the number of collected reports is high, we recommend using ASGARD Analysis Cockpit or Splunk with the free App and Add-on.

ASGARD Analysis Cockpit: <https://portal.nextron-systems.com/webshop/downloads>

THOR APT Scanner App: <https://splunkbase.splunk.com/app/3717/>

THOR Add-On: <https://splunkbase.splunk.com/app/3718/>

## 4.8 System Load Considerations

We recommend staging the THOR Run in order to avoid resource bottlenecks (network or on VMware host systems). Especially during the THOR start, program files and signatures get pulled over the network, which is about 30 MB per system. Additionally, the modules, which take only a few seconds or minutes to complete, run first so that the load is higher during the first 10 to 15 minutes of the scan.

It is therefore recommended to define sets of systems that will run at the same time and let other systems start at intervals of an hour.

It is typically no problem to start a big set of physical machines at the same time. But if you start a scan on numerous virtual guests or on remote locations connected through slow WAN lines, you should define smaller scan groups.

## SCAN

This chapter is a quick introduction on how to run a THOR scan and how to personalize scans to better fit your environment and expectations.

Please note, the command line arguments are used to fine tune your scans and yield potentially better results for your use cases.

There is no "one fits all" command line argument, but we designed THOR to cover the broadest area with minimal impact in the default operating mode. Default in this case means no additional command line arguments.

### 5.1 Quick Start

Follow these steps to complete your first THOR scan

1. Make sure you've read the *Before You Begin* guide
2. Open a command line as administrative user
  - a. Administrator on Windows
  - b. root on Linux and macOS
3. Navigate to the folder in which you've extracted the THOR package and placed the license file(s)
4. Start THOR on your command line
  - a. `thor64.exe` on 64-bit Windows systems
  - b. `thor.exe` on 32-bit Windows systems
  - c. `thor-linux-64` on x86-64 Linux systems
  - d. `thor-linux` on i386 Linux systems
  - e. `thor-macos` on macOS
5. Wait until the scan has completed (this can take between 20 and 180 minutes)
6. When the scan is finished, check the text log and HTML report in the THOR program directory

## 5.2 Often Used Parameters

| Parameter               | Description                                                                                                     |
|-------------------------|-----------------------------------------------------------------------------------------------------------------|
| <b>--soft</b>           | Reduce CPU usage, skip all checks that can consume a lot of memory (even if only for a few seconds)             |
| <b>--quick</b>          | Perform a quick scan (skips Eventlog and checks only the most relevant folders); see <a href="#">Scan Modes</a> |
| <b>-e target-folder</b> | Write all output files to the given folder                                                                      |

## 5.3 Parameters possibly relevant for your Use Case

| Parameter                                | Description                                                                                                                                                                                                                                                         |
|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>-c, --cpulimit integer</b>            | Instruct THOR to pause all scanning if the systems CPU load is higher than the value specified.<br>Please see <a href="#">CPU Limit (--cpulimit)</a> for more information.                                                                                          |
| <b>--allhds</b>                          | By default THOR scans only the C: partition on Windows machines and other files/folders only<br>in cases in which some reference points to a different partition (e.g. configured web root of IIS is on D:\inetpub, registered service runs from D:\vendor\service) |
| <b>--lookback days -- globallookback</b> | Only check the elements changed or created during the last X days in all available modules (reduces the scan duration significantly)                                                                                                                                |

## 5.4 Risky Flags

This list contains flags that should better be avoided unless you know exactly what you're doing.

| Parameter              | Description                                                                                            |
|------------------------|--------------------------------------------------------------------------------------------------------|
| <b>--intense</b>       | long runtime, stability issues due to disabled resource control                                        |
| <b>--c2-in-memory</b>  | many false positives on user workstations (especially browser memory)                                  |
| <b>--alldrives</b>     | long runtime, stability issues due to scan on network drives or other remote file systems              |
| <b>--mft</b>           | stability issues due to high memory usage                                                              |
| <b>--dump-procs</b>    | stability issues, possibly high disk space usage (free disk space checks are implemented but may fail) |
| <b>--full-registry</b> | longer runtime, low positive impact                                                                    |

## 5.5 Lesser Known But Useful Flags

This list contains flags that are often used by analysts to tweak the scan in useful ways.

| Parameter                         | Description                                                                          |
|-----------------------------------|--------------------------------------------------------------------------------------|
| <b>--allreasons</b>               | Show all reasons that led to a certain score                                         |
| <b>--printshim</b>                | Print all available SHIM cache entries into the log                                  |
| <b>--utc</b>                      | Print all timestamps in UTC (helpful when creating timelines)                        |
| <b>--string-context num-chars</b> | Number of characters preceeding and following the string match to show in the output |

## 5.6 Help and Debugging

You can use the following parameters help you to understand THOR and the output better.

| Parameter         | Description                                     |
|-------------------|-------------------------------------------------|
| <b>--debug</b>    | Get debug information if errors occur           |
| <b>--help</b>     | Get a help with the most important scan options |
| <b>--fullhelp</b> | Get a help with all scan options                |

## 5.7 Examples

### 5.7.1 Logging to a Network Share

The following command creates a plaintext log file on a share called "rep" on system "sys" if the user running the command has the respective access rights on the share.

```
thor64.exe --nohtml --nocsv -l \\sys\rep\%COMPUTERNAME%_thor.txt
```

### 5.7.2 Logging to Syslog Server

The following command instructs THOR to log to a remote syslog server only.

```
thor64.exe --nohtml --nocsv --nolog -s syslog.server.net
```

### 5.7.3 Scan Run on a Single Directory

```
thor64.exe --lab -p C:\ProgramData
thor64.exe --lab -p I:\mounted_image\disk1
```

---

**Important:** This feature requires a [forensic lab license](#) type which is meant to be used in forensic labs.

---

You can imitate a lab scan without a lab license with these command line flags:

```
thor64.exe -a Filescan --intense --norescontrol --nosoft --cross-platform -p C:\
↳ProgramData
```

### 5.7.4 Save the result files to a different directory

```
thor64.exe -s 10.1.5.14 -e Z:\
```

### 5.7.5 Only scan the last 7 days of the Windows Eventlog and log files on disk

```
thor64.exe --lookback 7
```

### 5.7.6 Scan System with Defaults and Make a Surface Scan

By default, the surface scan (DeepDive) applies all YARA rules in `./custom-signatures` folder. In this example, all output files are written to a network share.

```
thor64.exe --deepdivecustom -e \\server\share\thor_output\
```

### 5.7.7 Intense Scan and DeepDive on a Mounted Image

The following are two examples on how to scan a mounted image on Windows and Linux.

#### Mounted as Drive Z

```
thor64.exe --lab --deepdive -p Z:\
```

#### Mounted as /mnt

```
thor64.exe --lab --deepdive -p /mnt
```

---

**Important:** Lab scanning mode requires a [forensic lab license](#) type, which is meant to be used in forensic labs.

---

### 5.7.8 Scan Multiple Paths

```
thor64.exe --lab -p C:\\ D:\\webapps E:\\inetpub
```

---

**Hint:** non-existent directories will be automatically skipped

---

### 5.7.9 Scan All Hard Drives (Windows Only)

```
thor64.exe --allhds
```

### 5.7.10 Don't Scan Recursively

To instruct THOR to scan a folder non-recursively use the `:NOWALK` suffix.

```
thor64.exe -a FileScan -p C:\Windows\System32:NOWALK
```

## 5.8 Run a Scan with Specific Modules

With the parameter `-a` you can run a single module or select a set of modules that you'd like to run. All available modules can be found in the section *Scan Module Names*.

Run a Rootkit check only:

```
thor64.exe -a Rootkit
```

Run the Eventlog and file system scan:

```
thor64.exe -a Eventlog -a Filescan
```

## 5.9 Select or filter Signatures during Initialization

THOR 10.7.8 introduces the `Init Selector` and `Init Filter` functionalities, allowing users to fine-tune and customize their scanning process for improved accuracy and efficiency.

You can use these flags to limit the signature set to a certain campaign, threat or threat actor.

The filter values are applied to:

- Rule name
- Tags
- Description

Here are some examples:

```
thor64.exe --init-selector ProxyShell
```

You can pass multiple selector keywords separated by comma:

```
thor64.exe --init-selector RANSOM,Lockbit
```

Or filter a set of signatures that only cause false positives in your environment:

```
thor64.exe --init-filter AutoIt
```

It is important to note that while these features offer flexibility and customization, we recommend utilizing a limited signature set only for specific use cases. This approach is particularly suitable when scanning exclusively for indicators related to a specific campaign. By understanding the proper utilization of Init Selectors and Init Filters, users can optimize their scanning process and effectively identify targeted threats.

The main advantages of a reduced signature set are:

- improved scan speed
- lower memory usage

## 5.10 PE-Sieve Integration

THOR integrates [PE-Sieve](#), an open-source tool by @hasherezade to check for malware masquerading as benevolent processes.

PE-Sieve can be activated by using the `--processintegrity` flag. It runs on Windows as part of the ProcessCheck module and is capable of detecting advanced techniques such as Process Doppelganging.

When investigating infections, you can also raise the sensitivity of the integrated PE-Sieve beyond the default with `--full-proc-integrity` (at the cost of possible false positives).

THOR reports PE-Sieve results as follows:

| Findings          | THOR's Reporting Level |
|-------------------|------------------------|
| Replaced PE File  | Warning                |
| Implanted PE File | Warning                |
| Unreachable File  | Notice                 |
| Patched           | Notice                 |
| IAT Hooked        | Notice                 |
| Others            | No Output in THOR      |

See the [PE-Sieve documentation](#) for more details on these values.

## 5.11 Multi-Threading

Starting from version 10.6, THOR supports scanning a system with multiple threads in parallel, allowing for a significant increase in speed in exchange for a higher CPU usage.

To use this feature, use the `--threads` flag which allows you to specify THOR's number of parallel threads.

When using the `--lab` (Lab Scanning), `--dropzone` (sample drop zone) or `--thunderstorm` (Thunderstorm) command line flags, THOR will default to using as many threads as the system has CPU cores; otherwise, THOR will still default to running with a single thread.

---

**Note:** The above listed modes are only available with the "Lab", "Thunderstorm" and "Incident Response" license type.

---



### 5.11.1 Enabled Modules

Not all modules support multi-threading. It is currently supported for:

- Filescan
- RegistryChecks
- Eventlog
- Thunderstorm (Thunderstorm License needed)
- Dropzone (Lab License needed)



## SCAN MODES

You can select between six different scan modes in THOR:

- **Default**

We recommend using the default scan mode for all sweeping activities. Scans take from one to six hours, depending on the partition size and number of interesting files.

In default mode, THOR automatically chooses the "**Soft**" mode if the system has only limited CPU and RAM resources.

There's a special "Lab Scanning" (`--lab`) method described in section [Lab Scanning](#), which disables many limitations and allows to scan mounted images in a Lab scenario, even with multiple THOR instances on a single Workstation.

---

**Note:** "Lab Scanning" requires a special forensic license.

---

- **Quick** `--quick`

This mode is the fastest one and oriented on the "Pareto Principle", covering 80% of the modules and checks in 20% of the normal scan time. In "quick" mode, THOR skips elements that have not been created or modified within the last 2 days in the "Eventlog", "Registry" and "Filescan" modules. A set of 40+ predefined directories will still be checked completely (e.g. AppData, Recycler, System32). "Quick" mode is known to be the "preventive" scan mode – less intense and very fast.

Themed scan modes:

- **Soft** `--soft` - force disable with `--nosoft`

This mode disables all modules and checks that could be risky for system stability. It is automatically activated on (more details in chapter [Automatic Soft Mode](#)):

- Systems with only a single CPU core
- Systems with less than 1024 MB of RAM

- **Lab Scan** `--lab`

This mode scans only the file system and disables all other modules. (see [Lab Scanning](#) for more details and flags used in this scan mode)

Example:

```
user@unix:~/thor$./thor64 --lab -p /mnt/image_c/
```

- **Intense** `--intense`

This mode is meant for system scanning in a non-productive or lab environment. It disables several speed optimizations and enables time-consuming extra checks for best detection results. Be careful with this mode on database servers, as this could corrupt your database due to the high load of the server. Snapshots/backups are advised before using this mode.

- **Difference --diff**

The Diff Mode looks for a last scan and last finished modules in the local THOR DB and scans only elements on disk that have been changed or created since the last scan start. This mode applies shortcuts to the "Filesystem", "Eventlog" and "Registry" modules. Diff scans are typically the shortest scans but require a completed previous scan. This scan mode is also susceptible to the so-called "Timestomping".

These scan modes can also be combined, e.g. for `--soft --diff`, though not all combinations may make sense, e.g. `--soft --intense`.

The following tables give an overview on the active modules and features in the different scan modes. The [Modules](#) section lists all available modules, whereas the [Features](#) section lists only features that are handled differently in the different scan modes.

## 6.1 Modules

Modules are standalone jobs, which are being executed one after the other by THOR. Those modules are invoking one job, for example the File System Scan module will scan your file system, or the User Account Check will scan your system for user accounts. Modules can invoke one or multiple [Features](#), which we will explain further down in this section.

### 6.1.1 OS Module Overview

| Module                   | Windows   | Linux                  | MacOS                           |
|--------------------------|-----------|------------------------|---------------------------------|
| File System Scan         | Supported | Supported              | Supported                       |
| Registry Scan            | Supported | Not Supported          | Not Supported                   |
| SHIM Cache Scan          | Supported | Not Supported          | Not Supported                   |
| Mutex Check              | Supported | Not Supported          | Not Supported                   |
| Named Pipes Check        | Supported | Not Supported          | Not Supported                   |
| DNS Cache Check          | Supported | Supported              | Supported                       |
| Hotfix Check             | Supported | Not Supported          | Not Supported                   |
| Hosts File Check         | Supported | Supported              | Supported                       |
| Firewall Config Check    | Supported | Supported              | Not Supported                   |
| Network Share Check      | Supported | Not Supported          | Not Supported                   |
| Logged In Check          | Supported | Supported              | Supported                       |
| Process Check            | Supported | Supported <sup>1</sup> | Supported <sup>Page 47, 1</sup> |
| Service Check            | Supported | Supported              | Not Supported                   |
| Autoruns Check           | Supported | Supported              | Supported                       |
| Rootkit Check            | Supported | Supported              | Not Supported                   |
| LSA Sessions Analysis    | Supported | Not Supported          | Not Supported                   |
| User Account Check       | Supported | Supported              | Supported                       |
| User Profile Check       | Supported | Supported              | Supported                       |
| Network Sessions Check   | Supported | Not Supported          | Not Supported                   |
| Scheduled Tasks Analysis | Supported | Not Supported          | Not Supported                   |
| WMI Startup Check        | Supported | Not Supported          | Not Supported                   |
| At Entries Check         | Supported | Not Supported          | Not Supported                   |

continues on next page

Table 1 – continued from previous page

| Module                      | Windows       | Linux         | MacOS         |
|-----------------------------|---------------|---------------|---------------|
| MFT Analysis                | Supported     | Not Supported | Not Supported |
| Eventlog Analysis           | Supported     | Not Supported | Not Supported |
| KnowledgeDB Check           | Not Supported | Not Supported | Supported     |
| Environment Variables Check | Supported     | Supported     | Supported     |
| Crontab Check               | Not Supported | Supported     | Not Supported |
| Integrity Check             | Not Supported | Supported     | Not Supported |
| Event Check                 | Supported     | Not Supported | Not Supported |
| ETW Watcher                 | Supported     | Not Supported | Not Supported |

**Hint:** For a list of module names and how to turn them off, please see [Scan Module Names](#)

## 6.1.2 Scan Mode Overview

| Module                   | Normal                        | Quick    | Soft                 | Intense |
|--------------------------|-------------------------------|----------|----------------------|---------|
| File System Scan         |                               | Reduced  |                      |         |
| Registry Scan            |                               |          |                      |         |
| SHIM Cache Scan          |                               |          |                      |         |
| Mutex Check              |                               |          | Disabled             |         |
| Named Pipes Check        |                               |          |                      |         |
| DNS Cache Check          |                               |          |                      |         |
| Hotfix Check             |                               | Disabled |                      |         |
| Hosts File Check         |                               |          | Disabled             |         |
| Firewall Config Check    |                               | Disabled | Disabled             |         |
| Network Share Check      |                               |          | Disabled             |         |
| Logged In Check          | Enabled <sup>2</sup>          |          | Disabled             |         |
| Process Check            |                               |          | Reduced <sup>3</sup> |         |
| Service Check            |                               |          |                      |         |
| Autoruns Check           |                               |          |                      |         |
| Rootkit Check            |                               |          |                      |         |
| LSA Sessions Analysis    |                               |          | Disabled             |         |
| User Account Check       | Enabled <sup>Page 48, 2</sup> |          |                      |         |
| User Profile Check       | Enabled <sup>Page 48, 2</sup> | Disabled |                      |         |
| Network Sessions Check   | Enabled <sup>Page 48, 2</sup> |          | Disabled             |         |
| Scheduled Tasks Analysis |                               |          |                      |         |
| WMI Startup Check        |                               |          |                      |         |
| At Entries Check         |                               |          |                      |         |
| MFT Analysis             | Disabled                      | Disabled | Disabled             | Enabled |
| Eventlog Analysis        |                               | Disabled |                      |         |

continues on next page

<sup>1</sup> No process memory scan with YARA rules

Table 2 – continued from previous page

| Module                      | Normal | Quick | Soft | Intense |
|-----------------------------|--------|-------|------|---------|
| KnowledgeDB Check           |        |       |      |         |
| Environment Variables Check |        |       |      |         |
| Crontab Check               |        |       |      |         |
| Integrity Check             |        |       |      |         |
| Event Check                 |        |       |      |         |
| ETW Watcher                 |        |       |      |         |

### 6.1.3 Scan Module Names

| Scan Mode                   | Module Name     | Disable Module      |
|-----------------------------|-----------------|---------------------|
| File System Scan            | Filescan        | --nofilesystem      |
| Registry Scan               | RegistryChecks  | --noreg             |
| SHIM Cache Scan             | SHIMCache       | --noshimcache       |
| Mutex Check                 | Mutex           | --nomutex           |
| Named Pipes Check           | Pipes           | --nopipes           |
| DNS Cache Check             | DNSCache        | --nodnscache        |
| Hotfix Check                | HotfixCheck     | --nohotfixes        |
| Hosts File Check            | Hosts           | --nohosts           |
| Firewall Config Check       | Firewall        | --nofirewall        |
| Network Share Check         | NetworkShares   | --nonetworkshares   |
| Logged In Check             | LoggedIn        | --nologons          |
| Process Check               | ProcessCheck    | --noproc            |
| Service Check               | ServiceCheck    | --noservices        |
| Autoruns Check              | Autoruns        | --noautoruns        |
| Rootkit Check               | Rootkit         | --norootkits        |
| LSA Sessions Analysis       | LSASessions     | --nolsasessions     |
| User Account Check          | Users           | --nouers            |
| User Profile Check          | UserDir         | --noprofiles        |
| Network Sessions Check      | NetworkSessions | --nonetworksessions |
| Scheduled Tasks Analysis    | ScheduledTasks  | --notasks           |
| WMI Startup Check           | WMIStartup      | --nowmi             |
| At Entries Check            | AtJobs          | --noatjobs          |
| MFT Analysis                | MFT             | --nomft             |
| Eventlog Analysis           | Eventlog        | --noeventlog        |
| KnowledgeDB Check           | KnowledgeDB     | --noknowledgedb     |
| Environment Variables Check | EnvCheck        | --noenv             |
| Crontab Check               | Cron            |                     |
| Integrity Check             | Integritycheck  | --nointegritycheck  |
| Event Check                 | Events          | --noevents          |
| ETW Watcher                 | EtwWatcher      | --noetwwatcher      |

<sup>2</sup> Disabled on Domain Controllers

<sup>3</sup> No process memory scan with YARA rules



## 6.1.4 Scan Module Explanation

| Module             | Explanation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Filescan           | Events reported by the <b>FileScan</b> module typically originate from the file system scan. But due to the "Message Enrichment" feature, other modules that include events with full "file path" strings may also produce events of this type (e.g. module SHIMCache, Eventlog).                                                                                                                                                                                                           |
| SHIMcache          | The <b>SHIM Cache</b> or AppCompatCache (Application Compatibility Cache) is a special Registry cache containing valuable information, because the cache tracks metadata for binary files that were executed.                                                                                                                                                                                                                                                                               |
| Autoruns           | The <b>Autoruns</b> module makes use of the command line version of SysInternals Autoruns. It parses the tools output and integrates the output in each log message.                                                                                                                                                                                                                                                                                                                        |
| LogScan            | The <b>LogScan</b> module processes *.log files found on disk line by line (It performs some checks to avoid scanning files that are not ASCII log files, but something else that uses the *.log extension). Each log line is checked with all file name and keyword IOCs and scanned with the "keyword" and "log" type YARA rules.                                                                                                                                                         |
| GroupsXML          | The <b>GroupsXML</b> module is a module that reports on critical security issues related to decryptable passwords in group policy files, that are readable for anyone within a Windows Domain.                                                                                                                                                                                                                                                                                              |
| Registry           | <b>Registry</b> matches can be caused by different signature types: File name IOCs, keywords or YARA signatures matches.                                                                                                                                                                                                                                                                                                                                                                    |
| WMIPersistence     | It is difficult to detect malicious <b>WMIPersistence</b> objects. The detection methods are based on whitelists and a blacklist with keywords from APT reports. The whitelists are extended every time our analysts detect false positives in a customer's environment. The black lists are extended every time an APT report states a certain WMI persistence method with specific event filer or event file name.                                                                        |
| VulnerabilityCheck | The <b>VulnerabilityCheck</b> module is limited to a few vulnerabilities that are known to be exploited by various threat groups. The vulnerability checks focus on vulnerabilities that are used for lateral movement or weaknesses which allow an attacker to easily achieve persistence without using any kind of software as backdoor. Note: There are vulnerabilities covered by YARA rules and reported in other modules. The YARA rules that detect vulnerabilities start with VUL_. |
| LoggedIn           | The <b>LoggedIn</b> module analyses all currently logged in users and analyses their names.                                                                                                                                                                                                                                                                                                                                                                                                 |
| ProcessCheck       | Different checks are performed in the <b>ProcessCheck</b> module. Some of them check the process characteristics such as parent/child relations, process priorities and executable file locations for anomalies. Other checks evaluate the processes network connections and YARA checks match on the process memory.                                                                                                                                                                       |
| HotfixCheck        | The <b>HotFixCheck</b> module analyses the installed hotfixes on the end system.                                                                                                                                                                                                                                                                                                                                                                                                            |
| RunKeyCheck        | The <b>RunKeyCheck</b> module processes entries in the RUN Key.                                                                                                                                                                                                                                                                                                                                                                                                                             |
| AmCache            | The <b>AmCache</b> module processes entries in the AmCache of the system. In contrast to the SHIMCache entries, AmCache entries contain a SHA1 hash value that can be used to determine the exact program that was executed on the end system.                                                                                                                                                                                                                                              |
| Firewall           | The <b>Firewall</b> module evaluates all local Windows firewall rules and tries to detect suspicious entries by using white- and blacklists.                                                                                                                                                                                                                                                                                                                                                |
| ServiceCheck       | The <b>ServiceCheck</b> module evaluates all registered local Windows services. It detects suspicious service entries by different anomaly checks, blacklisted keywords and reports file path anomalies.                                                                                                                                                                                                                                                                                    |
| DNSCache           | The <b>DNSCache</b> module evaluates the entries of the local DNS cache. It compares the entries with known C2 servers and reports suspicious entries based on some regular expression checks.                                                                                                                                                                                                                                                                                              |
| Hosts              | The <b>Hosts</b> module evaluates the entries in the local hosts file.                                                                                                                                                                                                                                                                                                                                                                                                                      |
| WMIShutdown        | The <b>WMIShutdown</b> module uses different WMI queries to retrieve information on elements that could be used for persistence. It is very likely that findings by this module also appear in other modules (e.g. <b>Autoruns</b> ) in a different form, because it just uses a different method to look at the same elements.                                                                                                                                                             |
| CommandCheck       | The <b>CommandCheck</b> module is a meta module that analyses full command lines (path, executable, parameters) in different modules.                                                                                                                                                                                                                                                                                                                                                       |
| ProcessHandles     | The <b>ProcessHandles</b> module is a sub module of the <b>ProcessCheck</b> module that analyses the handles of each process. The module makes use of the SysInternals <code>handle.exe</code> tool that can be placed in the <code>./tools</code> sub folder.                                                                                                                                                                                                                              |



## 6.2 Features

Features are being invoked by *Modules* and provide further Details about an item. For example, the File System Scan might find a .zip file during a scan and invoke the Archive Scan feature. The Archive Scan feature in return will extract the zip file and scan all the items in it.

Another example would be the Eventlog Analysis Module, which might invoke the Sigma Scan feature on certain eventlog entries.

---

**Hint:** Please see chapter *Archive Scan* for a list of supported archive formats.

---

## 6.2.1 Feature Scan Mode Overview

| Feature                                   | Normal               | Quick    | Soft     | Intense |
|-------------------------------------------|----------------------|----------|----------|---------|
| Sigma Scan                                | Disabled             | Disabled | Disabled | Enabled |
| EXE Decompression <sup>5</sup>            | Enabled              | Enabled  | Disabled | Enabled |
| Archive Scan                              | Enabled              | Enabled  | Enabled  | Enabled |
| Double Pulsar Check <sup>Page 52, 5</sup> | Enabled              | Enabled  | Disabled | Enabled |
| Groups XML Analysis                       | Enabled              | Enabled  | Enabled  | Enabled |
| Vulnerability Check                       | Enabled              | Enabled  | Enabled  | Enabled |
| Web Server Dir Scan                       | Enabled              | Disabled | Enabled  | Enabled |
| WMI Persistence                           | Enabled              | Enabled  | Enabled  | Enabled |
| Registry Hive Scan                        | Enabled <sup>4</sup> | Enabled  | Enabled  | Enabled |
| AmCache Analysis                          | Enabled              | Enabled  | Enabled  | Enabled |
| Process Handle Check                      | Enabled              | Enabled  | Enabled  | Enabled |
| Process Connections Check                 | Enabled              | Enabled  | Enabled  | Enabled |
| Windows Error Report (WER)                | Enabled              | Enabled  | Enabled  | Enabled |
| Windows At Job File Analysis              | Enabled              | Enabled  | Enabled  | Enabled |
| EVTX File Scanning                        | Enabled              | Disabled | Enabled  | Enabled |
| Prefetch Library Scanning                 | Enabled              | Enabled  | Enabled  | Enabled |
| Memory Dump DeepDive                      | Disabled             | Disabled | Disabled | Enabled |
| Text Log File Scanning                    | Enabled              | Disabled | Enabled  | Enabled |
| Shellbag Entry Analysis                   | Enabled              | Enabled  | Enabled  | Enabled |
| Authorized Key File Analysis              | Enabled              | Enabled  | Enabled  | Enabled |
| Bifrost File Upload                       | Enabled              | Enabled  | Enabled  | Enabled |
| Malicious Domain Check                    | Enabled              | Enabled  | Enabled  | Enabled |
| File Scan                                 | Enabled              | Enabled  | Enabled  | Enabled |
| Cobalt Strike Beacon Parsing              | Enabled              | Enabled  | Enabled  | Enabled |
| Process Integrity Check <sup>5</sup>      | Disabled             | Disabled | Disabled | Enabled |
| SHIM Cache Analysis                       | Enabled              | Enabled  | Enabled  | Enabled |
| ETL File Scanning <sup>5</sup>            | Enabled              | Enabled  | Enabled  | Enabled |

<sup>5</sup> Only supported on Windows

<sup>4</sup> Disabled on Domain Controllers

### 6.2.2 Feature caller list

The following table gives an overview of THOR's features and how they are called by the different modules and other features.

| Feature                      | Callers                        |
|------------------------------|--------------------------------|
| Sigma Scan                   | Eventlog, Log file scanning    |
| EXE Decompression            | File Scan                      |
| Archive Scan                 | File Scan                      |
| Double Pulsar Check          | Rootkit Check                  |
| Groups XML Analysis          | File Scan                      |
| Vulnerability Check          | File Scan                      |
| Web Server Dir Scan          | Process Check                  |
| WMI Persistence              | File Scan                      |
| Registry Hive Scan           | File Scan                      |
| AmCache Analysis             | File Scan                      |
| Process Handle Check         | Process Check                  |
| Process Memory Check         | Process Check                  |
| Process Connections Check    | Process Check                  |
| Windows Error Report (WER)   | File Scan                      |
| Windows At Job File Analysis | File Scan                      |
| EVTX File Scanning           | File Scan                      |
| Prefetch Library Scanning    | File Scan                      |
| Memory Dump DeepDive         | File Scan                      |
| Text Log File Scanning       | File Scan                      |
| Shellbag Entry Analysis      | Registry Hive Scan             |
| Authorized Key File Analysis | File Scan                      |
| Bifrost File Upload          | File Scan                      |
| Malicious Domain Check       | File Scan                      |
| File Scan                    | Most modules and features      |
| Cobalt Strike Beacon Parsing | File Scan, Process Check       |
| Process Integrity Check      | Process Check                  |
| SHIM Cache Analysis          | SHIM Cache Scan, Registry Hive |
| ETL File Scanning            | File Scan                      |

### 6.2.3 Feature selectors

Since THOR 10.7, some features in THOR are triggered by YARA rules.

When a (meta or generic) YARA rule with a specific tag matches on a file, the corresponding feature is started and parses the file.

The standard signatures contain a number of rules with these tags, but if required, you can add additional rules with these tags as custom signatures.

| Tag                | Feature        | Applied regardless of Filesize limit |
|--------------------|----------------|--------------------------------------|
| AMCACHE            | Amcache        | no                                   |
| ZIPARCHIVE         | Archive        | no                                   |
| RARARCHIVE         | Archive        | no                                   |
| TARARCHIVE         | Archive        | no                                   |
| TARGZARCHIVE       | Archive        | no                                   |
| TARBZ2ARCHIVE      | Archive        | no                                   |
| CABARCHIVE         | Archive        | no                                   |
| GZIPCOMPRESSEDFILE | Archive        | no                                   |
| SEVENZIPARCHIVE    | Archive        | no                                   |
| ATJOBS             | AtJobs         | yes                                  |
| AUDITLOG           | Auditlog       | yes                                  |
| AUTHORIZEDKEYS     | AuthorizedKeys | yes                                  |
| EMAILFILE          | EmailParser    | no                                   |
| ETL                | ETL            | yes                                  |
| EVTX               | EVTX           | yes                                  |
| UPX                | ExeDecompress  | no                                   |
| WINRAR             | ExeDecompress  | no                                   |
| LNK                | LinkScan       | yes                                  |
| LOGSCAN            | LogScan        | yes                                  |
| MFT                | MftFile        | yes                                  |
| OLE                | OleScan        | no                                   |
| PREFETCH           | Prefetch       | yes                                  |
| REGISTRYHIVE       | RegistryHive   | yes                                  |
| UNESCAPE           | Unescaper      | no                                   |
| WER                | WER            | yes                                  |
| WMIPERSISTENCE     | WMIPersistence | yes                                  |

## 6.2.4 Feature names

| Feature                                                                     | Feature Name       | Disable Feature                                                                            |
|-----------------------------------------------------------------------------|--------------------|--------------------------------------------------------------------------------------------|
| Use a persistent database for holding information across scans              | ThorDB             | --nothordb                                                                                 |
| Scan with Sigma signatures                                                  | Sigma              | <b>THOR 10.6</b> per default disabled, use --sigma to enable<br><b>THOR 10.7</b> --nosigma |
| Scan log file (identified by .log extension or location) entries one by one | LogScan            | --nologscan                                                                                |
| Check files, processes or blobs with YARA                                   | Yara               |                                                                                            |
| Check files with STIX                                                       | Stix               | --nostix                                                                                   |
| Extract files contained in archives                                         | Archive            | --noarchive                                                                                |
| Scan files contained in archives                                            | ArchiveScan        | --noarchive                                                                                |
| Run checks for known C2 Domains                                             | C2                 | --noc2                                                                                     |
| Analyze process handles                                                     | ProcessHandles     | --noprochandle                                                                             |
| Analyze process connections                                                 | ProcessConnections | --noproconnections                                                                         |
| Analyze entries in Amcache files                                            | Amcache            | --noamcache                                                                                |
| Parse and analyze registry hives                                            | RegistryHive       | --noregistryhive                                                                           |

continues on next page

Table 4 – continued from previous page

| Feature                                                                              | Feature Name       | Disable Feature                                      |
|--------------------------------------------------------------------------------------|--------------------|------------------------------------------------------|
| Decompress and scan UPX or SFX packed portable executables                           | ExeDecompress      | --noexedecompress                                    |
| Analyze web directories that were found in process handles                           | WebdirScan         | --nowebdirscan                                       |
| Search for configuration file vulnerabilities (e.g. weak Tomcat passwords)           | VulnerabilityCheck | --novulnerabilitycheck                               |
| Parse Windows prefetch directories                                                   | Prefetch           | --noprefetch                                         |
| Parse groups.xml files (for AD permissions) and search for vulnerabilities           | GroupsXML          | --nogroupsxml                                        |
| Parse WMI Persistence directories                                                    | WMIPersistence     | --nowmipersistence                                   |
| Parse and analyze LNK files                                                          | Lnk                | --nolnk                                              |
| Check Knowledge DB on Mac OS                                                         | KnowledgeDB        | --noknowledgedb                                      |
| Parse .wer crash dump files                                                          | WER                | --nower                                              |
| Parse EVTX eventlogs and scan the contained log entries                              | EVTX               | --noevtX                                             |
| Analyze authorized_keys SSH files                                                    | AuthorizedKeys     | --noauthorizedkeys                                   |
| Parse and analyze .eml Email files                                                   | Eml                | --noeml                                              |
| Parse Windows Event Trace Logging files and scan the contained logs                  | ETL                | --noetl                                              |
| Parse jobs files scheduled with the 'at' tool                                        | AtJobs             | --noatjobs                                           |
| Upload suspicious files to a server running the Bifrost 2 quarantine service         | Bifrost2           | per default disabled, use --bifrost2Server to enable |
| Scan multiple entries as a single block                                              | BulkScan           | can't be disabled                                    |
| Disable cpulimit check                                                               | CPULimit           | --nocpulimit                                         |
| Run filename IOC, keyword IOC, and YARA rules on a chunk of data                     | CheckString        | can't be disabled                                    |
| Parse crontab files and analyze their entries                                        | CronParser         | can't be disabled                                    |
| Check for DoublePulsar Backdoor in the rootkit module                                | DoublePulsar       | --nodoublepulsar                                     |
| Gather additional information (like hashes, owner, timestamps, ...) about file paths | EnrichFileInfo     | can't be disabled                                    |
| Apply filename IOCs                                                                  | FilenameIOCs       | can't be disabled                                    |
| Scan files and similar objects                                                       | Filescan           | can't be disabled                                    |
| Apply keyword IOCs                                                                   | KeywordIOCs        | can't be disabled                                    |
| Log information during a THOR run                                                    | Logger             | can't be disabled                                    |
| Detect a file's type based on its first bytes                                        | MagicHeader        | can't be disabled                                    |
| Parse OLE files (e.g. old MS office documents, or MS Office macros)                  | OLE                | can't be disabled                                    |
| Parse additional information from a detected CobaltStrike beacon                     | ParseCobaltStrike  | can't be disabled                                    |
| Keep and display information about THOR's current activity                           | ProgressTracker    | can't be disabled                                    |

continues on next page

Table 4 – continued from previous page

| Feature                                                                           | Feature Name     | Disable Feature                                        |
|-----------------------------------------------------------------------------------|------------------|--------------------------------------------------------|
| Parse additional information from files in a Windows recycle bin                  | RecycleBin       | can't be disabled                                      |
| Check whether the system is running out of RAM, and end THOR, if this is the case | Rescontrol       | --norescontrol                                         |
| Parse SHIM Caches from registry and analyze their entries                         | SHIMCache        | --noshimcache                                          |
| React to interrupts from outside THOR in a controlled manner                      | SignalHandler    | can't be disabled                                      |
| Look for unencrypted TeamViewer passwords in registry hives                       | TeamViewer       | can't be disabled                                      |
| Add additional information from Virustotal to detected files                      | VirusTotal       | per default disabled, use --vtkey to enable            |
| Run a user defined command for detected files                                     | Action           | per default disabled, use --action_command to enable   |
| Write a detailed output file with information about all scanned elements          | AuditTrail       | per default disabled, use --audit-trail to enable      |
| Scan memory dump files in chunks                                                  | DumpScan         | per default disabled, use --dumpscan to enable         |
| Scan processes with PE-Sieve to check for process integrity (Windows only)        | ProcessIntegrity | per default disabled, use --processintegrity to enable |

## SPECIAL SCAN MODES

This section describes special purpose scan modes that change THOR's mode of operation or activate particular features. Some of these modes need a special license which is highlighted in the **note** box. If you have any questions regarding pricing of those licenses, please contact our sales department at [sales@nextron-systems.com](mailto:sales@nextron-systems.com)

### 7.1 Lab Scanning

Lab scanning mode that is activated with `--lab` (formerly `--fsonly`). It is used to scan mounted forensic images or a single directory on a forensic workstation. All resource control functions are disabled and intense mode is activated by default.

The `--lab` parameter automatically activates the following other options:

- intense (scan every file intensively regardless of its extension or magic header)
- norescontrol (do not limit system resources or interrupt scan on low memory)
- nosoft (do not automatically activate soft mode on systems with single core CPUs or low memory)
- nodoublecheck (do not check for other THOR instances on the same system and do not interrupt scan if another instance has been found)
- multi-threading (it automatically sets the number of threads to use to the number of CPU cores found on the workstation)

The chapter *Use Cases* contains some use cases in which this scan mode is used. You may find the guides useful.

---

**Note:** If you run multiple THOR scans with multi-threading on a single system, resource usage will rise quickly since it scales per thread.

Consider using `--threads` to reduce the number of threads that each THOR scan uses, e.g. `--threads 4` if running 4 scans on a 16 core system.

---

### 7.1.1 Forensic Lab License

The scan of mounted disk or memory images is a use case that we call "lab scanning". It requires a [forensic lab license](#) which is meant to be used in corporate digital forensic labs.

All other license types are meant for other use cases. (usually live system scanning) You can get a similar but not an equally thorough scan using the following command line flags

```
C:\nexttron\thor>thor64.exe -a Filescan --intense --norescontrol --cross-platform -p path-
↪to-scan
```

Without a valid lab license, you cannot use multiple instances of THOR on a single system or switch into multi-threaded scanning. The features mentioned in the following sub chapters are also limited to a lab license.

[This article](#) explains that advantages of a lab licenses.

### 7.1.2 Virtual Drive Mapping

Since THOR enriches messages with more details, it could be problematic to scan a mounted drive "s:", which has originally been a partition "c:" on the source system of the image.

E.g. The analyst has mounted a partition "C:" from a source system to drive "F:" on the forensic lab workstation. A SHIMCache entry points to C:\temp\mk.exe. THOR would look at location C:\temp\mk.exe for that file and couldn't find anything, since that file doesn't exist on the forensic lab workstation.

Virtual drive mapping allows you to virtually map that drive to its original name. The syntax is as follows:

```
--virtual-map current-location:original-location
```

Some examples:

A original partition "C:" from the source system has been mounted to drive "F:" on the forensic lab workstation:

```
--virtual-map F:C
```

A original mount point "/" has been mounted to "/mnt/image1" on a Linux forensic lab workstation:

```
--virtual-map /mnt/image1:/
```

A Windows image of drive "C:" mounted to "/mnt/image1" on a Linux forensic lab workstation:

```
--virtual-map /mnt/image1:C
```

---

**Note:** This feature requires a [forensic lab license](#) type, which is meant to be used in forensic labs.

---



### 7.1.3 Hostname Replacement in Logs

The parameter `-j` can be used to set the hostname used in the log files to a given identifier instead of using the current workstation's name in all output files. If you don't use this flag, all log files generated on that forensic lab workstation would contain the name of the forensic lab workstation as the source.

You should use the name of the host from which the image has been retrieved as the value for that parameter.

```
-j orig-hostname
```

### 7.1.4 Artefact Collector

THOR 10.7.8 introduces the **Artefact Collector** module. The purpose of this module is to be able to quickly collect and archive system artifacts into a single ZIP via THOR. It can be activated via `--collector` (running the collector module at the end of a THOR run) or `--collector-only` (only running the collector module) and uses `:hostname:_collector.zip` as output path for the ZIP archive per default. The default ZIP archive path can be changed with `--collector-output <path>`. The ZIP archive includes all found artifacts and a special file called `collector.log` containing logging information for the module execution (e.g. timestamps, hashes, filesize, ...)

The artifacts which are collected per default (GLOB patterns) can be seen with `--collector-print-config`. To change the default settings use `--collector-config <file>`.

---

**Tip:** Pipe the output of `--collector-print-config` to a file and use a modified version of it.

---

For testing the collector config you can use `--collector-dry-run` - this only prints the artifacts which would be collected to stdout - no output ZIP archive will be created. It is also possible to limit the artifact size via the `--collector-max-filesize` flag.

If run on Windows, the collector module will parse the MFT and collect files based on the extracted information. This allows the collection of all files including special files like \$UsnJrnl. The downside of MFT parsing is that it takes a bit longer. If you do not care about special files and want to speed up the collection process, use `--collector-no-mft`.

All flags can be found in the THOR full help (`--fullhelp`).

---

**Note:** A special license called **THOR Deep Forensics** is needed to use the **Artefact Collector** feature.

---

### 7.1.5 Examples

#### THOR Lab Scanning Example

A full command line of a THOR scan started in a lab environment would look like this:

```
C:\nexttron\thor>thor64.exe --lab -p S:\ --virtual-map S:C -j WKS001 -e C:\reports
```

It instructs THOR to scan the mounted partition S: in lab scanning mode, maps the current partition "S:" to a virtual drive "C:", replaces the hostname with "WKS001" in the outputs and saves every output file (text log, HTML, CSV) to a reports folder named C:\reports.

---

**Note:** This feature requires a **forensic lab license** type which is meant to be used in forensic labs.

---

### Artefact Collector Example

The command line of a THOR scan in collector-only mode would like this:

```
C:\nexttron\thor>thor.exe --collector-only
```

If you want THOR to run in its "classic" way and afterwards collect artifacts, use:

```
C:\nexttron\thor>thor.exe <normal-THOR-flags> --collector
```

---

**Note:** This feature requires a [forensic lab license](#) type which is meant to be used in forensic labs.

---

## 7.2 Lookback Mode

The `--lookback` option allows you to restrict the Eventlog and log file scan to a given amount of days. E.g. by using `--lookback 3` you instruct THOR to check only the log entries that have been created in the last 3 days.

In THOR v10.5 we've extended this feature to include all applicable modules, including "FileScan", "Registry", "Services", "Registry Hives" and "EVTX Scan".

By setting the flags `--all-module-lookback --lookback 2` you instruct THOR to scan only elements that have been created or modified during the last 2 days. This reduces the scan duration significantly.

This scan mode is perfect for quick scans to verify SIEM related events and is used by default in THOR Cloud's settings for executions via Microsoft Defender ATP.

## 7.3 Drop Zone Mode

The drop zone mode allows you to define a folder on your local hard drive that is monitored for changes. If a new file is created in that folder, THOR scans this file and writes a log message if suspicious indicators have been found. The optional parameter `--dropdelete` can be used to remove the dropped file once it has been scanned. Example:

```
C:\thor>thor64.exe --dropzone -p C:\dropzone
```

**Warning:** If another process writes a file to the drop zone, this is prone to a race condition: THOR might read the file when no or not all data has been written yet.

For consistent scan results, move files from another folder to the dropzone.

---

**Note:** This feature requires a [forensic lab license](#) or [Thunderstorm license](#) which are meant to be used in forensic labs.

---

### 7.3.1 Drop Zone Mode Output

We designed the drop zone mode to show only relevant output (Notice, Warning or Alert) after the initialization to reduce clutter on the screen. This might look like no files are being scanned, which is actually not the case. To see if files are being scanned, you can do one of the following two options.

You can drop the [EICAR test file](#) into the defined dropzone to test if findings are shown properly:

```
> 1/1 > Running module 'Dropzone'
Info Starting module
Info Watching the following directory for changes PATH: C:\dropzone
Info Successfully started watcher
Notice Suspicious file found
FILE: eicar.com.txt EXT: .txt SCORE: 40 TYPE: UNKNOWN
SIZE: 68
MD5: 44d88612fea8a8f36de82e1278abb02f
SHA1: 3395856c81f2b7382dee72602f798b642f14140
SHA256: 275a021bbf6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f FIRSTBYTES: 58354f2150254041505b345c505a58353428505e / X501P%AP[4]PZX54(P*
CREATED: Tue Nov 22 11:31:56.861 2022 MODIFIED: Tue Nov 22 11:31:57.009 2022 ACCESSED: Tue Nov 22 11:31:57.012 2022 PERMISSIONS: BUILTIN\Administrators:F / BUILTIN\Users:R / NT AUTHORITY\Authenticated Users:G / NT AUTHORITY\SYSTEM:F / OWNER:
REASON: 1: YARA rule SUSP_Just_EICAR / Just an EICAR test file - this is boring stuff SUBSCORE_1: 40 REF_1: http://2016.eicar.org/85-0-Download.html SIGTYPE_1: Internal MATCHED_1: Str1: "X501P%AP[4]PZX54(P*)ZCC7)$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$HHH" at 0x0 RULEDATE_1: 2019-03-24 TAGS_1: FILE, SUSP RULENAME_1: SUSP_Just_EICAR AUTHOR_1: Florian Roth REASONS_COUNT: 1
Notice Suspicious file found
FILE: eicar.com.txt EXT: .txt SCORE: 40 TYPE: UNKNOWN
SIZE: 68
MD5: 44d88612fea8a8f36de82e1278abb02f
SHA1: 3395856c81f2b7382dee72602f798b642f14140
SHA256: 275a021bbf6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f FIRSTBYTES: 58354f2150254041505b345c505a58353428505e / X501P%AP[4]PZX54(P*
CREATED: Tue Nov 22 11:31:56.861 2022 MODIFIED: Tue Nov 22 11:31:57.009 2022 ACCESSED: Tue Nov 22 11:31:57.012 2022 PERMISSIONS: BUILTIN\Administrators:F / BUILTIN\Users:R / NT AUTHORITY\Authenticated Users:G / NT AUTHORITY\SYSTEM:F / OWNER:
REASON: 1: YARA rule SUSP_Just_EICAR / Just an EICAR test file - this is boring stuff SUBSCORE_1: 40 REF_1: http://2016.eicar.org/85-0-Download.html SIGTYPE_1: Internal MATCHED_1: Str1: "X501P%AP[4]PZX54(P*)ZCC7)$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$HHH" at 0x0 RULEDATE_1: 2019-03-24 TAGS_1: FILE, SUSP RULENAME_1: SUSP_Just_EICAR AUTHOR_1: Florian Roth REASONS_COUNT: 1
Worker 04: idle
```

Or you can print all output with `--printall` - this might clutter the output:

```
> 1/1 > Running module 'Dropzone'
Info Starting module
Info Watching the following directory for changes PATH: C:\dropzone
Info Successfully started watcher
Info Scanning file
FILE: C:\dropzone\test.exe ORIGINAL_NAME: test.exe
Info Scanning file
FILE: C:\dropzone\Everything-1.4.1.1017.x64-Setup.exe ORIGINAL_NAME: Everything-1.4.1.1017.x64-Setup.exe
Info Scanning file
FILE: C:\dropzone\Everything-1.4.1.1022.x64-Setup.exe ORIGINAL_NAME: Everything-1.4.1.1022.x64-Setup.exe
Info Scanning file
FILE: C:\dropzone\Everything-1.4.1.1022.x86-Setup.exe ORIGINAL_NAME: Everything-1.4.1.1022.x86-Setup.exe
Info Scanning file
FILE: C:\dropzone\ChromeSetup.exe ORIGINAL_NAME: ChromeSetup.exe
Info Scanning file
FILE: C:\dropzone\LibreOffice_7.4.1_Win_x64.msi ORIGINAL_NAME: LibreOffice_7.4.1_Win_x64.msi
Info Scanning file
FILE: C:\dropzone\LibreOffice_7.4.1_Win_x64.msi ORIGINAL_NAME: LibreOffice_7.4.1_Win_x64.msi
Info Scanning file
FILE: C:\dropzone\Firefox Installer.exe ORIGINAL_NAME: Firefox Installer.exe
Info Scanning file
FILE: C:\dropzone\npp.8.4.5.Installer.x64.exe ORIGINAL_NAME: npp.8.4.5.Installer.x64.exe
Info Scanning file
FILE: C:\dropzone\Sysmon.zip ORIGINAL_NAME: Sysmon.zip
Info Scanning file
FILE: C:\dropzone\test ORIGINAL_NAME: test
Info Scanning file
FILE: ORIGINAL_NAME: LibreOffice_7.4.1_Win_x64.msi\macros
Info Scanning file
FILE: ORIGINAL_NAME: Sysmon.zip\Sysmon.exe
Info Scanning file
FILE: C:\dropzone\test.exe ORIGINAL_NAME: test.exe
Info Scanning file
FILE: ORIGINAL_NAME: Sysmon.zip\Sysmon64.exe
Info Scanning file
FILE: ORIGINAL_NAME: Sysmon.zip\Eula.txt
Worker 06: idle
```

## 7.4 Image File Scan Mode

The image file scan mode has a misleading name. It isn't meant to be used for forensic image scanning but for the scan of un-mountable images or memory dumps only. If you have a forensic image of a remote system, it is always recommended to mount the image as a Windows drive and scan it using the Lab Scanning (--lab) mode.

The Image File Scan mode performs a deep dive on a given data file. Therefore, the file type, structure or size of that file is not relevant. The DeepDive module processes the file in overlapping 3 Megabyte chunks and checks these chunks using the given YARA rule base only (including custom YARA signatures).

The only suitable use case is the scan of a memory dump using your own YARA signatures placed in the "./custom-signatures/yara" sub folder.

```
C:\nexttron\thor>thor.exe -m systemX123.mem -j systemX123 -e C:\reports
```

---

**Note:** This feature requires a [forensic lab license](#) type which is meant to be used in forensic labs.

---

## 7.5 DeepDive

The DeepDive module allows a surface scan of a given memory dump.

This check processes every byte of the memory dump.

DeepDive is not recommended for triage sweeps in a whole network as it generates more false positives than a normal file system scan. This is mainly caused by the fact that chunks of data read from the dump are processed regardless of their corresponding file's type, name or extension. It processes Antivirus signatures, pagefile contents and other data that may trigger an alert.

In the current stage of development, the DeepDive check parses out every executable file and applies all included Yara signatures. A positive match is reported according to the score as "Notice", "Warning" or "Alert".

There are some disadvantages linked with the DeepDive detection engine:

- The file name cannot be extracted from the raw executable code
- The file path of the reported sample is unknown

THOR uses other attributes to report these findings:

- Offsets
  - THOR reports the location on the disk, so that forensic investigators are able to check and extract the file from an image of the hard drive.
- Restore
  - THOR is able to restore the whole file to a given directory. It uses the system's NetBIOS name, rule name, the score and the offset to create a file name for the extracted file.

As a side effect of this dissection all the embedded executables in other file formats like RTF or PDF are detected regardless of their way of concealment.

To perform a surface scan, use the "--image\_file" option. To restore all detected files to a restore directory additionally use the "-r directory" option.

| Option              | Description                                                                                      |
|---------------------|--------------------------------------------------------------------------------------------------|
| <b>--image_file</b> | Activate DeepDive for a specific image file, i.e. <code>--image_file C:\\tmp\\memory.hdmp</code> |
| <b>-r directory</b> | Recovery directory for files found by DeepDive                                                   |

## 7.6 Eventlog Analysis

The Eventlog scan mode allows scanning certain Windows Eventlogs.

In intense mode, all Eventlogs are scanned. In normal or soft mode, the following Eventlogs are scanned:

- System
- Application
- Security
- Windows PowerShell
- Microsoft-Windows-AppLocker/EXE and DLL
- Microsoft-Windows-AppLocker/MSI and Script
- Microsoft-Windows-CodeIntegrity/Operational
- Microsoft-Windows-DeviceGuard/Operational
- Microsoft-Windows-Folder Redirection/Operational
- Microsoft-Windows-PowerShell/Operational
- Microsoft-Windows-Sysmon/Operational
- Microsoft-Windows-Security-Mitigations/KernelMode
- Microsoft-Windows-Shell-Core/Operational
- Microsoft-Windows-SmbClient/Security
- Microsoft-Windows-SMBServer/Security
- Microsoft-Windows-TaskScheduler/Operational
- Microsoft-Windows-WMI-Activity/Operational
- Microsoft-Windows-Windows Defender/Operational
- Microsoft-Windows-Windows Firewall With Advanced Security/Firewall
- Microsoft-Windows-WinINet-Config/ProxyConfigChanged
- Microsoft-Windows-VHDMP-Operational
- Microsoft-Windows-WLAN-AutoConfig/Operational
- Microsoft-Windows-Winlogon/Operational
- Microsoft-Windows-UniversalTelemetryClient/Operational

The parameter `-n` works like the `-p` parameter in the Filesystem module. It takes the target Eventlog as parameter, which is the Windows Eventlog's full name.

```
C:\nexttron\thor>thor64.exe -a Eventlog -n "Microsoft-Windows-Sysmon/Operational"
```

From THOR 10.7.13 onwards, `-n` can also be used to scan all event logs by using `-n *`.

You can get the full name of a Windows Eventlog by right clicking the Eventlog in Windows Event Viewer and selecting "Properties".

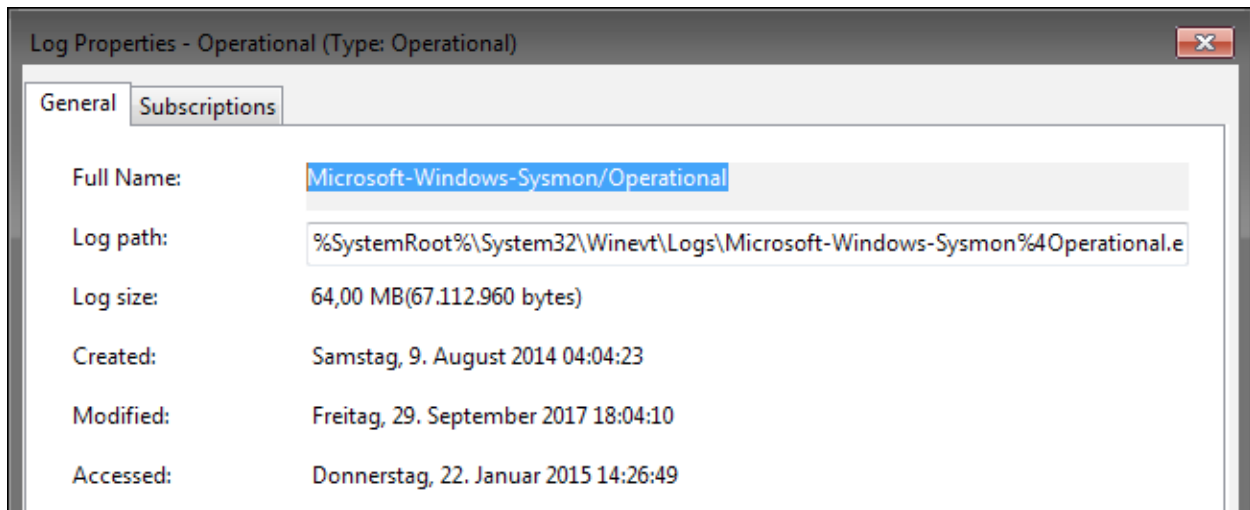


Fig. 1: Windows Eventlog Properties

The `-n` parameter can also be used to restrict the Eventlog scanning to certain Eventlogs. The following command will start a default THOR scan and instructs the Eventlog module to scan only the "Security" and "System" Eventlog.

```
C:\nexttron\thor>thor64.exe -n Security -n System
```

## 7.7 MFT Analysis

The MFT analysis module reads the "Master File Table" (MFT) of a partition and parses its contents. The MFT analysis takes a significant amount of time and is only active in "intense" scan mode by default.

You can activate MFT analysis in any mode by using `--mft`.

The way THOR handles the MFT Analysis can be influenced by the following parameters:

| Option                       | Description                                                                                          |
|------------------------------|------------------------------------------------------------------------------------------------------|
| <code>--mft</code>           | Activate MFT analysis                                                                                |
| <code>--nomft</code>         | Do not perform any MFT analysis whatsoever (only useful in combination with <code>--intense</code> ) |
| <code>--maxmftsize MB</code> | The maximum MFT size in Megabytes to process (default: 200 MB)                                       |

## **ANALYSIS**

This chapter explains the possibilities for collecting and analyzing THOR logs.

### **8.1 ASGARD Analysis Cockpit**

The ANALYSIS COCKPIT is the central platform for analyzing THOR logs. It can be used in an environment where scans are controlled by ASGARD Management Center and can also be used where THOR is executed manually or controlled by third party solutions. It is available as a virtual appliance on VMWare and also as a dedicated hardware appliance.

THOR can also be seen or used as hunting solution, it is optimized to avoid false negatives – meaning optimized to not miss an indicator of compromise. On the other side this clearly leads to more anomalies and false positives being reported.

In a scenario where you scan your infrastructure frequently you would either be seeing the same anomalies again and again or you would need to create many rules to filter out these anomalies in order to save analysis time.

The ANALYSIS COCKPIT is designed to facilitate this process and help you generate these rules automatically, so that you can set your baseline-filters after the first scan. After setting the first baseline it is now easy to focus on relevant Alerts and Warnings as only differences between the first and second scans are shown.

The ANALYSIS COCKPIT comes with an integrated and highly configurable ticketing system that helps organizing your analysis workflow. Furthermore, the ANALYSIS COCKPIT comes with a rule based alert forwarding and SIEM integration that makes it easy for your organization to react quickly on new incidents.

### **8.2 Splunk**

We offer a THOR Splunk App and Add-on via the official Splunk App Store. This App helps you to extract the event fields and provides dashboards to get a better overview on distributed runs on multiple systems.

THOR APT Scanner App: <https://splunkbase.splunk.com/app/3717/>

THOR Add-On: <https://splunkbase.splunk.com/app/3718/>

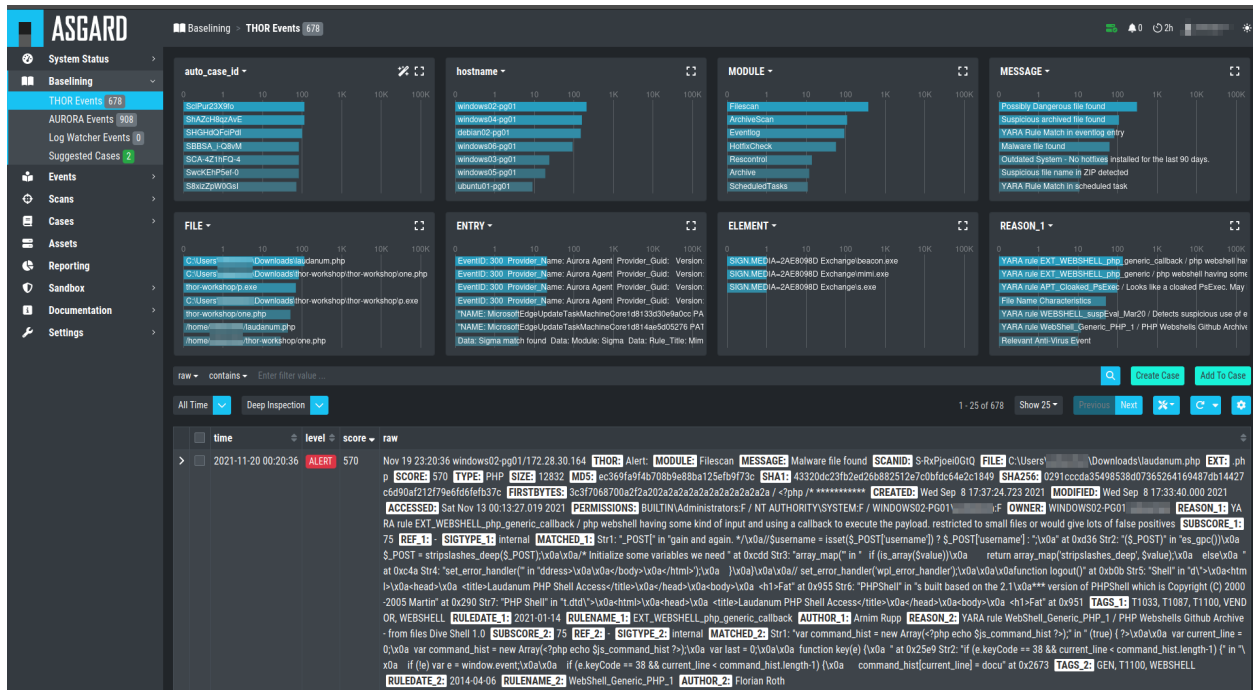


Fig. 1: Analysis Cockpit View

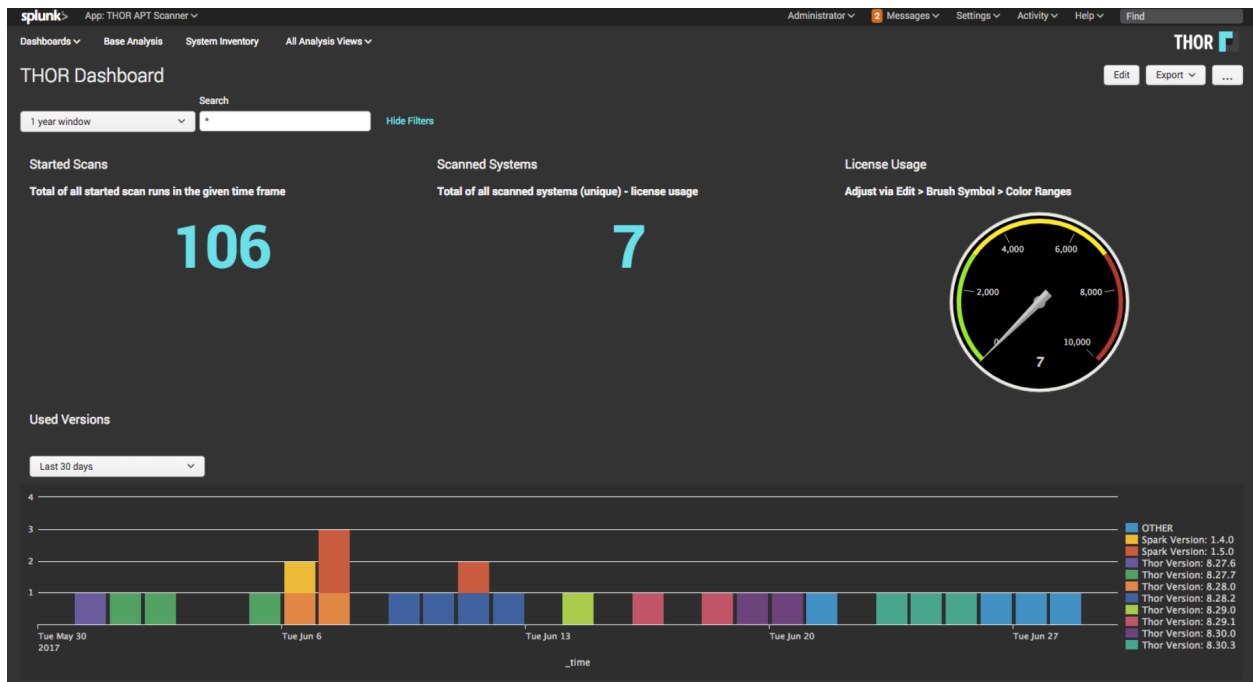


Fig. 2: THOR Splunk App (free)



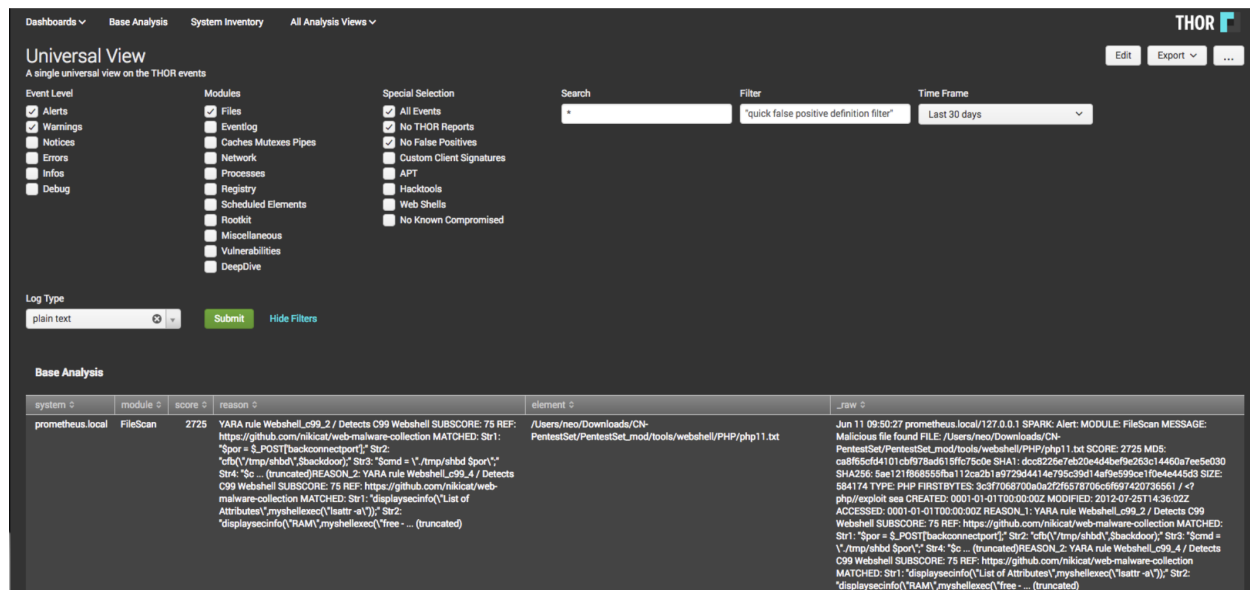


Fig. 3: Splunk THOR App Universal View

## 8.3 THOR Util Report Feature

THOR Util provides a feature called "report" that creates HTML reports from text logs of one or more scanned systems.

Find more information about this feature on our website or the separate THOR Util manual.

<https://www.nextron-systems.com/2018/06/20/thor-util-with-html-report-generation/>

## 8.4 Log Analysis Manual

We have written a detailed Log Analysis Manual which:

- Explains how to analyze THOR logs
- Contains example logs
- Lists potential false positives you might encounter
- And how different attributes are to be evaluated

<https://log-analysis-manual.nextron-systems.com/>

file:///C:/nexttron/thor/report.htm

| Scan Information |   |    |      |   | Modules        |     | Statistics         |                                                                                            |  |  |
|------------------|---|----|------|---|----------------|-----|--------------------|--------------------------------------------------------------------------------------------|--|--|
|                  | 1 | 32 | 1519 |   | Autoruns       | 8   | Alerts             | 0                                                                                          |  |  |
|                  |   | 18 | 130  | 3 | EVTX           | 1   | Warnings           | 37                                                                                         |  |  |
|                  | 4 | 7  | 252  | 2 | Eventlog       | 117 | Notice             | 1224                                                                                       |  |  |
|                  |   | 37 | 1467 |   | Filescan       | 77  | Info               | 58224                                                                                      |  |  |
|                  | 1 | 24 | 1478 |   | LogScan        | 2   | Errors             | 57                                                                                         |  |  |
|                  |   | 24 | 1471 |   | Loggedin       | 82  | Help               |                                                                                            |  |  |
|                  |   | 15 | 1405 | 3 | ProcessCheck   | 4   | Shortcuts          | Use Ctrl+I (Windows/Linux) or ⌘+I (macOS) to return to the top of the page                 |  |  |
|                  |   | 15 | 1414 |   | ProcessDiff    | 493 | Filters            | You can provide a file (-filter file) with regular expressions to suppress false positives |  |  |
|                  |   | 21 | 1462 | 1 | ProcessHandles | 4   | Hint 1             | Select text and use the context menu to filter / select / lookup strings                   |  |  |
|                  |   | 4  | 270  | 2 | RegistryHive   | 8   | Hint 2             | Click on a module to filter for all events from that module.                               |  |  |
|                  |   | 29 | 1489 |   | SHIMCache      | 16  |                    |                                                                                            |  |  |
|                  | 1 | 28 | 1532 |   | ServiceCheck   | 332 |                    |                                                                                            |  |  |
|                  | 1 | 27 | 1537 |   | UserDir        | 1   |                    |                                                                                            |  |  |
|                  |   | 29 | 1483 |   | Users          | 36  |                    |                                                                                            |  |  |
|                  |   | 41 | 1459 |   | WMIStartup     | 35  | No filters applied |                                                                                            |  |  |
|                  |   | 8  | 82   | 2 |                |     |                    |                                                                                            |  |  |
|                  |   | 27 | 1537 |   |                |     |                    |                                                                                            |  |  |
|                  |   | 42 | 1445 |   |                |     |                    |                                                                                            |  |  |
|                  |   | 8  | 80   | 3 |                |     |                    |                                                                                            |  |  |
|                  |   | 9  | 35   |   |                |     |                    |                                                                                            |  |  |
|                  |   | 34 | 1471 | 2 |                |     |                    |                                                                                            |  |  |
|                  |   | 36 | 1512 |   |                |     |                    |                                                                                            |  |  |
|                  |   | 6  | 76   | 2 |                |     |                    |                                                                                            |  |  |

Fig. 4: THOR Util's Report Output

## CONFIGURATION

### 9.1 Scan Templates

THOR 10 accepts config files (called "templates") in YAML format. They reflect all command options to make them flexible and their use as comfortable as possible.

This means that every parameter set via command line can be provided in the form of a config file. You can even combine several of these config files in a single scan run.

#### 9.1.1 Default Template

By default, THOR only applies the file named `thor.yml` in the `./config` sub folder. Other config files can be applied using the `-t` command line parameter.

#### 9.1.2 Apply Custom Scan Templates

The following command line provides a custom scan template named `mythor.yml`.

```
C:\nexttron\thor>thor.exe -t mythor.yml
```

#### 9.1.3 Example Templates

The default config `thor.yml` in the `./config` folder has the following content.

Content of THOR's Default Config `thor.yml`:

```
1 # This is the default config for THOR
2 # Terminate THOR if he runs longer than 72 hours
3 max_runtime: 72
4 # Minimum score to report is 40
5 min: 40
6 # Skip files bigger than 120000000 bytes
7 max_file_size: 120000000
8 # Skip files bigger than 300000000 bytes in intense mode (--fsonly, --intense)
9 max_file_size_intense: 300000000
10 # Limit THOR's CPU usage to 95%
11 cpulimit: 95
12 # The minimum amount of free physical memory to proceed (in MB)
13 minmem: 50
```

(continues on next page)

(continued from previous page)

```

14 # Truncate THOR's field values after 2048 characters
15 truncate: 2048

```

Content of Config File `mythor.yml`:

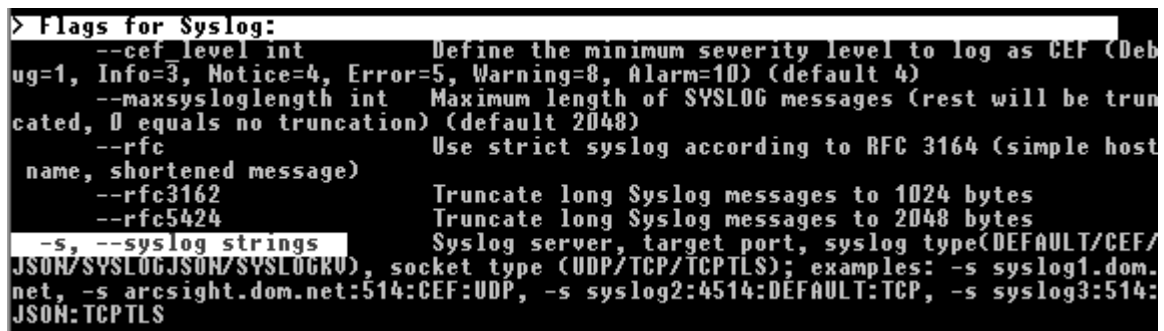
```

1 resume: true
2 cpulimit: 40
3 intense: true
4 max_file_size: 7500000
5 syslog:
6 - foo.nextron
7 - bar.nextron:514:TCP

```

The default scan template is always applied first. Custom templates can then overwrite settings in the default template. In the example above, the `cpulimit` and `max_file_size` parameters are overwritten by the custom template.

As you can see in the example file, you have to use the long form of the command line parameter (e.g. `syslog`) and not the short form (e.g. `-s`) in the template files. The long forms can be looked up in the command line help using `--help`.



```

> Flags for Syslog:
--cef_level int Define the minimum severity level to log as CEF (Debug=1, Info=3, Notice=4, Error=5, Warning=8, Alarm=10) (default 4)
--maxsysloglength int Maximum length of SYSLOG messages (rest will be truncated, 0 equals no truncation) (default 2048)
--rfc Use strict syslog according to RFC 3164 (simple host name, shortened message)
--rfc3162 Truncate long Syslog messages to 1024 bytes
--rfc5424 Truncate long Syslog messages to 2048 bytes
-s, --syslog strings Syslog server, target port, syslog type(DEFAULT/CEF/JSON/SYSLOGJSON/SYSLOGKRV), socket type (UDP/TCP/TCP/TLS); examples: -s syslog1.dom.net, -s arcsight.dom.net:514:CEF:UDP, -s syslog2:4514:DEFAULT:TCP, -s syslog3:514:JSON:TCP/TLS

```

Fig. 1: Lookup command line parameter long forms using `-help`

## 9.2 CPU Limit (`--cpulimit`)

Since the `--cpulimit` behavior can cause some confusion, we will explain the functionality of it a bit more in detail here.

This argument will take an integer (default 95; minimum 15), which represents the maximum CPU load at which THOR will be actively scanning. The value can be seen as percentage of the systems maximum CPU load.

This can be helpful to reduce the load on server systems with real-time services, or to reduce the noise produced by fans in laptops.

The specified value instructs THOR to pause (all scanning), if the load of the systems CPU is higher than the `cpulimit`. One example would be, if a user is doing something CPU intensive, and THOR is running at the same time, THOR will pause and wait until the CPU load drops below the `cpulimit` before continuing.

To illustrate this a bit, please see the table below:

Table 1: --cpulimit 40

| Total CPU load of system                   | THOR status |
|--------------------------------------------|-------------|
| 20 %                                       | running     |
| 80 % (user is running CPU intensive tools) | paused/idle |
| 30 %                                       | running     |

---

**Hint:** A tool like `top` might show values greater than 100% for a running THOR process. Please see `Irix Mode` in the man page of `top`: <https://man7.org/linux/man-pages/man1/top.1.html>

---

## 9.3 Maximum File Size

The default maximum file size for deeper investigations (hash calculation and YARA scanning) is 30 MB. The maximum file size for the `-intense` scan mode is 100 MB.

You can adjust the values in `./config/thor.yml`. This file does not get overwritten by an update or upgrade.

Special scan features like the EVTX or Memory Dump scan ignore these limits.

Features that obey the file size limit:

- YARA Matching
- Hash calculation
- STIX IOC application
- ArchiveScan

Features that ignore the file size limit:

- LogScan
- RegistryHive scanning
- EVTX scanning
- DeepDive on memory dumps (selected by `.dmp` and magic headers)
- Filename IOCs
- YARA meta rules (only check the first 100 bytes of a file and all meta data)

If the `--intense` flag is used, a different file size limit is applied.

The only exception is `ArchiveScan` (e.g. ZIP file analysis) that has no file size limit in intense scan.

### 9.3.1 Chunk Size in DeepDive

The chunk size in DeepDive module is set to the value defined as **maximum file size**. DeepDive uses overlapping chunks of this size for YARA rule scanning.

Example: If the maximum file size is set to a default of 12 MB, DeepDive use the following chunks in its scan to apply the YARA rule set:

```
Chunk 1: Offset 0 - 12
Chunk 2: Offset 6 - 18
Chunk 3: Offset 12 - 24
Chunk 4: Offset 18 - 30
```

## 9.4 Exclude Elements

### 9.4.1 Files and Directories

You may use the file `directory-excludes.cfg` to exclude directories and files(! The name of the config file is misleading) from the scan.

THOR will not scan the contents of these directories. This `directory-excludes.cfg` config is meant to avoid scanning sensitive files like databases or directories with a lot of content. If you want to suppress false positives that are generated in these directories, please see the following chapter and how to suppress them by using `false_positive_filters.cfg`.

The exclusion file contains regular expressions that are applied to each scanned element. Each element consists of the file path and file name (e.g. `C:\IBM\temp_tools\custom.exe`). If one of the defined expressions matches, the element is excluded. Exclusions can be defined for a full element name, at the beginning at the end or somewhere in the element name.

**Note:** If used in combination with flags like `--virtual-map` that change the original path on the filesystem, the exclusions are applied to the real path on the filesystem, not the original path.

For example, when using `--virtual-map F:C` and scanning a file located at `F:\Windows\explorer.exe`, THOR will check if `F:\Windows\explorer.exe` is excluded, not if `C:\Windows\explorer.exe` is excluded.

As the configured exclusions are treated as regular expressions, special characters must be masqueraded by backslash. This applies at least for: `[]\^$. \ | ? * + ( ) -`

| Element to exclude                                        | Possible solution                          |
|-----------------------------------------------------------|--------------------------------------------|
| <code>C:\IBM\temp_tools\custom.exe</code>                 | <code>C:\\IBM\\temp_tools\\</code>         |
| Log folder of the tool "hpsm" regardless on the partition | <code>\\HPSM\\log\\</code>                 |
| Every file with the extension .nsf                        | <code>\\.nsf\$</code>                      |
| THOR custom signatures                                    | <code>\\THOR\\custom\\-signatures\\</code> |
| SQL database                                              | <code>/var/lib/mysql/</code>               |

## 9.4.2 Eventlogs

Eventlog sources can be excluded as whole in "**eventlog-excludes.cfg**". The file holds one expression per line and applies them as regular expression on the name of the Eventlog. (e.g. Microsoft-Windows-Windows Defender/Operational)

| Element to exclude                             | Possible solution  |
|------------------------------------------------|--------------------|
| Windows PowerShell                             | Windows PowerShell |
| Microsoft-Windows-Windows Defender/Operational | Windows Defender   |

## 9.4.3 Registry

Registry paths/keys can be excluded in **registry-excludes.cfg**. The file holds one expression per line and applies them as regular expression on each registry key. (e.g. "Software\WOW6432Node"). Don't include the root of the key, e.g. HKLM.

| Element to exclude                                                                          | Exclude Definition                         |
|---------------------------------------------------------------------------------------------|--------------------------------------------|
| HKEY_LOCAL_MACHINE\Software\Wow6432Node\Symantec\Symantec Endpoint Protection\AV\Exclusions | Symantec Endpoint Protection\AV\Exclusions |

## 9.4.4 False Positives

The false positive filters work like the directory/file excludes. A regular expression is applied to the **full** event, excluding the event header (e.g. Sep 14 12:07:07 some-hostname/192.168.0.20).

E.g. if you want to Exclude all messages that contain the string Trojan\_Buzus\_dev you just add this string to the **false\_positive\_filters.cfg** file. The file works with regular expressions so you could also define something like chinese\_(charcode|keyboard).

## 9.4.5 Filter Verification

If you are unsure about the filters you just set, we recommend a test run on a certain directory that matches the criteria.

You can start a short test run on a certain directory with:

```
C:\nexttron\thor>thor.exe -a FileScan --intense -p C:\\TestDir
```

## 9.4.6 Personal Information

THOR features an option named **--brd** that allows to filter the output messages and replace all known locations and fields that can contain user names or user ids with the value **ANONYMIZED\_BY\_THOR**.

What it does is:

- Replace all "USER" and "OWNER" field values of all modules with the anonymized string value
- Replaced the subfolder names of C:\Users and C:\Documents and Settings with the anonymized string value

There is no guarantee that all user IDs will be removed by the filter, as they may appear in the most unexpected locations, but in most cases this approach is sufficient to comply with data protection requirements.



## OUTPUT OPTIONS

### 10.1 Scan Output

THOR creates several files during and at the end of the scan.

- **Real Time**
  - the text log file is written during the scan process. Also the SYSLOG output is sent in real-time to one or more remote systems.
- **End of Scan**
  - the full HTML report and CSV file with all file scan elements reported as suspicious are written at the end of the scan.

You can define different formatting options for each the FILE and the SYSLOG output.

#### 10.1.1 Placeholders

Two placeholders can be used in command line parameters to facilitate the use of parameter on different operating systems.

- :hostname:
- :time:

These can be used in command line parameters and scan templates across all platforms.

```
C:\thor>thor64.exe -a FileScan -p S:\\ -o :hostname:_:time:.csv
```

#### 10.1.2 Log File Output (.txt)

The standard log file is written by default.

- **--nolog**
  - Don't create a log file
- **--logfile filename**
  - Set a filename for the log file

The log file's format aligns with the format of SYSLOG messages. This way it can easily be imported to most SIEM or log analysis systems.

### 10.1.3 CSV Output (.csv)

The CSV output is an optional legacy output file without much details. It contains only “Filescan” module findings and consist of 3 columns, file hash, file path and score.

CSV File Output:

```
1 c926bf384319e40506e3d6e409dc856e,C:\PowerZure.ps1,140
2 62160f1a71507e35ebf104a660d92794,C:\f.bat,180
3 c926bf384319e40506e3d6e409dc856e,C:\ntds.dit,50
4 c926bf384319e40506e3d6e409dc856e,C:\temp\ntds.zip|ntds.dit,140
5 36a93511fc0e2e967bc5ced6a5bc36a6,C:\temp\ntds.zip,50
6 44b34aac3135dcb03ababac5f7767a55,C:\temp\windows-hardening.bat,60
```

Be aware that archives with matches show up as “archive.zip|file-with-finding.js” (pipe separator) in the second column.

If you need more columns in that CSV, consider processing the JSON output instead. To do this, you can use `thor-util` to convert logs from one format to the other:

<https://thor-util-manual.nextron-systems.com/en/latest/usage/log-conversion.html>

### 10.1.4 CSV Stats

The CSV stats file is an optional output file that contains only the scan statistics. It contains a single line with:

Hostname, scan start, scan end, THOR version, used command line flags, number of alerts, number of warnings, number of notices and number of errors

CSV Stats Output:

```
HYPERION,2021-02-17 17:01:25,2021-02-17 17:01:28,10.6.2,--lab -p C:temp -o HYPERION:time:.csv --
csvstats,5,2,3,0
```

### 10.1.5 JSON Output (.json)

The JSON output file can be configured with these options:

- **--json** (deprecated since THOR 10.7, use `--jsonv2`)
  - Create a JSON output file
- **--jsonv2** (THOR >= 10.7)
  - Use the JSON v2 format, which is easier to parse than the old v1 format.
  - This can be used with `--jsonfile`.
- **--jsonfile filename**
  - Log file for JSON output. If no value is specified, defaults to `:hostname:_thor_:time:.json`.
- **--cmdjson**
  - Print JSON format into the command line (e.g. used with Splunk scripted input)
- **--syslog [syslogtarget]:[port]:SYSLOGJSON**
  - Send syslog messages with JSON formatting

### 10.1.6 Key Value Output

THOR provides the option to create a "Key/Value" pair output that simplifies the SIEM integration.

By using the "**--keyval**" option you get the text and syslog output transformed as shown in the following example. The command line output stays untouched by this setting.

There are three different Key Value Pair Formatting flags:

- **--keyval**
  - Write key/value pairs to the log file
- **--cmdkeyval**
  - Print key/value pairs in the command line (e.g. used with Splunk scripted input)
- **--syslog [syslogtarget]:[port]:SYSLOGKV**
  - Send syslog messages with proper key/value formatting

#### Default - Without "--keyval" parameter

```
Jul 10 09:08:47 PROMETHEUS/10.0.2.15 THOR: Alert: MODULE: SHIMCache MESSAGE: Malware name
found in Shim Cache Entry ENTRY: C:\Users\neo\Desktop\ncat.exe KEYWORD: \ncat.exe DATE: 07/29/13
05:16:04 TYPE: system HIVEFILE: None EXTRAS: N/A N/A True
```

#### Key/Value Pairs - With "--keyval" parameter

```
Jul 10 09:07:59 PROMETHEUS/10.0.2.15 THOR : Alert: MODULE="SHIMCache" MESSAGE="Malware
name found in Shim Cache Entry" ENTRY="C:\Users\neo\Desktop\ncat.exe" KEYWORD="\ncat.exe"
DATE="07/29/13 05:16:04" TYPE="system" HIVEFILE="None" EXTRAS="N/A N/A True"
```

### 10.1.7 Audit trail

Audit trail output is available starting from THOR 10.8.

It contains different output from the other output options. Usually, THOR only prints elements (e.g. files, or registry entries) that have been matched on by some signature. Audit trail mode, on the other hand, contains `_all_` scanned elements, even those that THOR considers inconspicuous, as well as their (known) connections to each other.

This information can be used to visualize these elements, and help with grouping suspicious elements or laterally finding more suspicious elements.

**Warning:** Audit trail output comes with an overhead since THOR usually does not calculate all the information contained in the audit trail.

## Output format

Audit trail output is a gzipped JSON file. The file can be specified with `--audit-trail my-target-file.json.gz`.

The file contains newline delimited JSON, where each contained JSON object follows the following schema:

```
{
 "id": "string",
 "details": {
 "...": "...",
 },
 "timestamps": {
 "...": "...",
 },
 "reasons": [
 {
 "summary": "string",
 "score": "int",
 "...": "...",
 }
],
 "references": [
 {
 "target-id": "string"
 }
]
}
```

- `id` contains a unique ID for the element that was matched on
- `details` contains the element that was matched on
- `timestamps` contains all timestamps found within this element
- `reasons` contains a list of signatures that matched on this element
- `references` contains a list of IDs of other elements that this element referred to in some way

### 10.1.8 Timestamps

Timestamp in all modules are using the **ANSI C** format:

```
Mon Jan 2 15:04:05 2006
Mon Mar 19 09:04:05 2018
```

<https://go.dev/src/time/format.go>

## UTC

The `--utc` parameter allows to use UTC in all timestamps.

## RFC3339 Time Stamps

The parameter `--rfc3339` generates time stamps for UTC time in the format described in RFC 3339. In contrast to the default time stamps RFC 3339 timestamps include a year and look like this:

```
2017-02-31T23:59:60Z
```

### 10.1.9 SCAN ID

The former parameter `-i`, which has been used for so-called case IDs (CID) has been repurposed to allow users to set a certain scan ID (SCANID) that appears in every log line.

The scan ID helps SIEM and analysis systems to correlate the scan lines from multiple scans on a single host. Otherwise it would be very difficult to answer the following questions:

- How many scans completed successfully on a certain endpoint?
- Which scan on a certain endpoint terminated during the scan run?

If no parameter is set, THOR will automatically generate a random scan ID, which starts with an S- and contains the following characters: a-zA-Z0-9\_-

#### Example ScanIDs

```
S-Rooa61RfuM
S-0vRKu-1_p7A
```

Users can overwrite the scan ID with `-i myscanid` to assign the logs of multiple scan runs to a single logical scan, e.g. if multiple partitions of a system get scanned in the lab in different scan runs, but should be shown as a single scan in Analysis Cockpit or your SIEM of choice.

In a log line, it looks like (set newlines for readability):

```
Jul 10 09:08:47 PROMETHEUS/10.0.2.15 THOR: Alert:
MODULE: SHIMCache
SCANID: S-r4GhEhEiIRg
MESSAGE: Malware name found in Shim Cache Entry
ENTRY: C:\Users\neo\Desktop\ncat.exe
KEYWORD: \\ncat\.exe
DATE: 07/29/13 05:16:04
TYPE: system
HIVEFILE: None
EXTRAS: N/A N/A True
```

## Custom Scan ID Prefix

Since THOR version 10.5 you are able to set your custom prefix by using `--scanid-prefix`. The fixed character "S" can be replaced with any custom string. This allows users to set an identifier for a group of scans that can be grouped together in a SIEM or Analysis Cockpit.

## 10.2 Syslog or TCP/UDP Output

### 10.2.1 Target Definition

THOR version 10 comes with a very flexible Syslog target definition. You can define as many targets as you like and give them different ports, protocols and formats.

For example, if you want to send the THOR log entries to a Syslog server and an ArcSight SIEM at the same time, you just have to define two log targets with different formats.

```
C:\nexttron\thor>thor.exe -s syslog1.server.net -s arcsight.server.net:514:CEF
```

The definition consists of 4 elements:

| System | : | Port | : | Type | : | Protocol |
|--------|---|------|---|------|---|----------|
|--------|---|------|---|------|---|----------|

The available options for each element are:

```
(target ip):(target port):(DEFAULT/CEF/JSON/SYSLOGJSON/SYSLOGKV):(UDP/TCP/TCPTLS)
```

The available type field values require an explication:

| Option     | Format                                              |
|------------|-----------------------------------------------------|
| DEFAULT    | standard THOR log format                            |
| CEF        | Common Event Format (ArcSight)                      |
| JSON       | Raw JSON                                            |
| SYSLOGJSON | encoded and escaped single line JSON                |
| SYSLOGKV   | syslog messages that contain strict key/value pairs |

There are default values, which do not have to be defined explicitly:

```
(your target system ip):514:DEFAULT:UDP
```

Sending Syslog to a target on a port that differs from the default port 514/udp looks like this:

```
--syslog 10.0.0.4:2514
```

Sending Syslog to a receiving server using an SSL/TLS encrypted TCP connection:

```
--syslog 10.0.0.4:6514:DEFAULT:TCPTLS
```

You can define as many targets as you like.

An often used combination sends JSON formatted messages to a certain UDP port:

```
--syslog 10.0.0.4:5444:JSON:UDP
```

## 10.2.2 Common Event Format (CEF)

THOR supports the CEF format for easy integration into ArcSight SIEM systems. The CEF mapping is applied to a log line if the syslog target has the CEF format set, e.g.:

```
C:\nexttron\thor>thor.exe -s syslog1.server.local:514:CEF
```

## 10.2.3 Local Syslog

If your Linux system is already configured to forward syslog messages, you might just want to write to your local syslog and use the existing system configuration to forward the events. This can be achieved by using the `--local-syslog` flag.

THOR logs to the `local0` facility, which is not being written to a file by default on every Linux distribution. By default Debian derivatives log it to `/var/log/syslog`; Others such as Red Hat do not. To enable writing `local0` messages to a file a syslog configuration for `rsyslog` (e.g. `/etc/rsyslog.conf`) could look like:

```
THOR --local-syslog destination
local0.* -/var/log/thor
```

Do not forget to restart the syslog daemon (e.g. `systemctl restart rsyslog.service`).

You then either add that file in your syslog forwarding configuration or write to a file that is already forwarded instead.

## 10.3 Encrypted Output Files

THOR allows to encrypt the output files of each scan using the `--encrypt` parameter. A second parameter `--pubkey` can be used to specify a public key to use. The public key must be an RSA key of 1024, 2048 or 4096 bit size in PEM format.

```
C:\nexttron\thor>thor64.exe --encrypt --pubkey mykey.pub
```

If you don't specify a public key, THOR uses a default key. The private key for this default key is stored in "thor-util", which can be used to decrypt output files encrypted with the default key.

```
nexttron@unix:~$ thor-util decrypt file.txt
```

For more information on "thor-util" see the separate [THOR Util manual](#).





You can download updates for THOR with "thor-util".

Running `thor-util --help` shows two options that look very similar:

- **upgrade** : program and signature updates
- **update** : signature updates only

For more information on "thor-util" see the separate [THOR Util manual](#).

## 11.1 Update Locations

The following servers are used as update mirrors and should be accessible via HTTPS (443/tcp):

- [update1.nexttron-systems.com](https://update1.nexttron-systems.com)
- [update2.nexttron-systems.com](https://update2.nexttron-systems.com)

## 11.2 Update Server Information

You can get information on the available update packages on this site:

<https://update1.nexttron-systems.com/info.php>



## CUSTOM SIGNATURES

THOR checks the contents of the `./custom-signatures` folder and processes every file in this folder. The file extension determines the type of signature (e.g. a simple IOC file, a YARA rule or a Sigma rule). For some signature types, string tags in the file names are used to further distinguish the signatures.

For example, a file named `my-c2-iocs.txt` will be initialized as a file containing simple IOC indicators with C2 server information.

Internally the regex `\Wc2\W` is used to detect the tag, so `mysource-c2-iocs.txt` and `dec15-batch1-c2-indicators.txt` would be detected correctly, whereas `filenameiocs.txt` or `myc2iocs.txt` would not be detected.

If you do not wish to place your custom IOCs on potentially compromised systems during an engagements, you can use `thor-util` to encrypting custom signatures. This is described in detail in the [THOR Util manual](#)

### 12.1 Simple IOCs

Simple IOC files are basically CSV files that include the IOC and comments. Simple IOC files must have the extension `.txt`. encrypted simple IOC files must have the extension `.dat`.

The following tags for simple IOCs are currently supported:

- **"c2" or "domains"**
  - for IP addresses and hostnames
- **"filename" or "filenames"**
  - for filenames
- **"hash" or "hashes"**
  - for MD5, SHA1 or SHA256 hashes or (since THOR 10.7.6) Imphashes
- **"keyword" or "keywords"**
  - for string-based keywords
- **"trusted-hash" or "trusted-hashes" or "falsepositive-hash" or "falsepositive-hashes"**
  - for hashes that you trust
- **"handles"**
  - for malicious Mutex / Events
- **"pipes" or "pipe"**
  - for Named Pipes

| Tag/String in File Name | Example                                    |
|-------------------------|--------------------------------------------|
| c2                      | misp- <b>c2</b> -domains-iocs.txt          |
| filename                | Case-UX22- <b>filename</b> -iocs.txt       |
| filenames               | Malicious- <b>filenames</b> -unitX.txt     |
| hash                    | op-aura- <b>hash</b> -iocs.txt             |
| hashes                  | int-misp- <b>hashes</b> .txt               |
| keyword                 | Incident-22- <b>keyword</b> .txt           |
| keywords                | <b>keywords</b> -incident-3389.txt         |
| trusted-hash            | my- <b>trusted-hashes</b> .dat (encrypted) |
| handles                 | Operation-fallout- <b>handles</b> .txt     |
| pipes                   | incident-22-named- <b>pipes</b> .txt       |

**Hint:** You can find IOC examples in the directory `custom-signatures/iocs/templates` of THOR. This should help you to create your own simple IOC files.

For a list of Features/Modules which are used by the different *Simple IOCs*, please see the table below.

| Name            | Type    | Filename | Keyword | Named Pipe | Handle | Hash | C2  |
|-----------------|---------|----------|---------|------------|--------|------|-----|
| Amcache         | Feature | Yes      | Yes     | No         | No     | Yes  | No  |
| Archive         | Feature | Yes      | No      | No         | No     | Yes  | No  |
| AtJobs          | Feature | Yes      | Yes     | No         | No     | No   | No  |
| AtJobs          | Module  | Yes      | Yes     | No         | No     | No   | No  |
| AuthorizedKeys  | Feature | Yes      | Yes     | No         | No     | No   | No  |
| Autoruns        | Module  | Yes      | No      | No         | No     | Yes  | No  |
| Cron            | Module  | Yes      | Yes     | No         | No     | No   | No  |
| DeepDive        | Module  | No       | No      | No         | No     | No   | No  |
| DNSSCache       | Module  | No       | No      | No         | No     | No   | Yes |
| DumpScan        | Feature | No       | No      | No         | No     | No   | No  |
| Eml             | Feature | Yes      | No      | No         | No     | Yes  | No  |
| Env             | Module  | Yes      | Yes     | No         | No     | No   | No  |
| ETL             | Feature | Yes      | Yes     | No         | No     | No   | No  |
| Eventlog        | Module  | Yes      | Yes     | No         | No     | No   | No  |
| Events          | Module  | Yes      | Yes     | No         | Yes    | No   | No  |
| EVTX            | Feature | Yes      | Yes     | No         | No     | No   | No  |
| FileScan        | Feature | Yes      | No      | No         | No     | Yes  | No  |
| FileScan        | Module  | Yes      | No      | No         | No     | Yes  | No  |
| Firewall        | Module  | No       | No      | No         | No     | No   | Yes |
| Hosts           | Module  | No       | Yes     | No         | No     | No   | Yes |
| KnowledgeDB     | Module  | No       | Yes     | No         | No     | No   | No  |
| Lnk             | Feature | Yes      | Yes     | No         | No     | No   | No  |
| LoggedIn        | Module  | No       | No      | No         | No     | No   | No  |
| LogScan         | Feature | Yes      | Yes     | No         | No     | No   | No  |
| LSASessions     | Module  | No       | Yes     | No         | No     | No   | No  |
| MFT             | Module  | Yes      | Yes     | No         | No     | No   | No  |
| Mutex           | Module  | Yes      | Yes     | No         | Yes    | No   | No  |
| NetworkSessions | Module  | No       | Yes     | No         | No     | No   | No  |
| NetworkShares   | Module  | No       | Yes     | No         | No     | No   | No  |
| OLE             | Feature | Yes      | No      | No         | No     | No   | No  |
| Pipes           | Module  | No       | Yes     | Yes        | No     | No   | No  |

continues on next page

Table 1 – continued from previous page

| Name               | Type    | Filename | Keyword | Named Pipe | Handle | Hash | C2  |
|--------------------|---------|----------|---------|------------|--------|------|-----|
| Prefetch           | Feature | Yes      | No      | No         | No     | No   | No  |
| ProcessCheck       | Module  | Yes      | Yes     | No         | Yes    | No   | Yes |
| ProcessConnections | Feature | Yes      | Yes     | No         | No     | No   | Yes |
| ProcessHandles     | Feature | Yes      | Yes     | No         | Yes    | No   | No  |
| Profiles           | Module  | No       | Yes     | No         | No     | No   | No  |
| RegistryChecks     | Module  | Yes      | Yes     | No         | No     | No   | No  |
| RegistryHive       | Feature | Yes      | Yes     | No         | No     | No   | No  |
| ServiceCheck       | Module  | Yes      | Yes     | No         | No     | No   | No  |
| SHIMCache          | Feature | Yes      | Yes     | No         | No     | No   | No  |
| SHIMCache          | Module  | Yes      | Yes     | No         | No     | No   | No  |
| TaskScheduler      | Module  | Yes      | Yes     | No         | No     | No   | No  |
| Users              | Module  | Yes      | Yes     | No         | No     | No   | No  |
| WER                | Feature | Yes      | No      | No         | No     | No   | No  |
| WMIPersistence     | Feature | Yes      | Yes     | No         | No     | No   | No  |
| WMIStartup         | Module  | No       | Yes     | No         | No     | No   | No  |

### 12.1.1 Hashes

Files with the string `hash` or `hashes` in their filename get initialized as hash IOC sets. Either you are assigning a custom score to your hashes, or you do not assign a score at all, in which case the match will default to a score of 100.

The first column contains your MD5, SHA1 or SHA256 hash or (since THOR 10.7.6) an Imphash. The second column contains your comment, if you do not use any scoring. If you choose to use your own scoring (example below on line 2), the score goes into the second column and the comment into the third. Columns are separated by a semicolon and hashes are applied case-insensitively. Scoring and comments are optional.

Listing 1: custom-hashes-iocs.txt

```
1 0c2674c3a97c53082187d930efb645c2;DEEP PANDA Sakula Malware - http://goo.gl/R3e6eG
2 f05b1ee9e2f6ab704b8919d5071becbce6f9d0f9d0ba32a460c41d5272134abe;50;Vulnerable Lenovo
 ↪Diagnostics Driver - https://github.com/alfarom256/CVE-2022-3699/tree/main
```

### 12.1.2 File Name IOCs

Filename IOC files allow you to define IOCs based on filename and filepath using regular expressions. You can add or reduce the total score of a file element during the scan with a positive (e.g. "40") or negative score (e.g. "-30").

While this can also be used to define false positives, or reduce the score of well-known files and locations, it gives you all the flexibility to add scores according to your needs.

Filename IOCs are case insensitive if they don't use any special regex characters (such as `*`, `.`, `[`, `...`). Otherwise, they are case sensitive by default, but can be set as case insensitive by using `(?i)` anywhere in the regex.

Listing 2: custom-filename-iocs.txt

```
1 # Ncat Example
2 \\bin\\nc\\.exe;-20
```

If you know that administrators in your organization use `PsExec.exe` in a folder named `Sysinternals`, but any other location should be reported as suspicious you could define the following statements:

Listing 3: psexec-filename-ioc.txt

```
1 # PsExec
2 \\PsExec\.exe;60
3 \\SysInternals\\PsExec\.exe;-60
```

This following example represents the 3<sup>rd</sup> generation filename IOC format introduced with THOR version 8.30 and SPARK version 1.5, which is now the recommended form to define such signatures.

It contains three fields:

- Column 1: Regex
- Column 2: Score
- Column 3: False Positive Regex

The False Positive Regex statement is only evaluated if the Regex statement in column 1 matched.

```
\\PsExec\.exe;60;\\SysInternals\\
```

We use this new format internally to describe abnormal locations of system files like

```
[C-Zc-z]:\\|\\\\\\\\\\\\\\\\.\\{1,40}\\svchost\\.exe;65;(?!)(HKCR\\|
Applications|System32|system32|SYSTEM32|winsxs|WinSxS|SysWOW64|SysWow64|syswow64|SYSNATIVE|Sysnative|
%system32%)\\
```

You could also score down directories with many false positives reported as "Notices" or "Warnings" like this:

```
\\directory_with_many_false_positives\\;-30
```

### 12.1.3 Keyword IOCs

The keyword-based IOC files contain plaintext strings that are matched against the console output of THOR. Not all console output is being used for those IOCs, you can find the full list here: [Simple IOCs Modules](#).

One use case would be to have different strings which you encountered in Scheduled Tasks within Windows. Usually THOR will output all the Scheduled Tasks as **Info**, so this can help to look for specific things throughout the whole THOR scan.

Every line is treated as case-sensitive string. A comment can be specified with a line starting with a # and applies to all following IOCs until another comment is encountered.

Keyword IOCs are case sensitive.

Listing 4: custom-keyword-iocs.txt

```
1 # Evil strings from our case
2 sekurlsa::logonpasswords
3 failed to create Service 'GAMEOVER'
4 kiwi.eo.oe
```

### 12.1.4 C2 IOCs

C2 IOC files specify remote servers which are known to be malicious. This can include:

- Domain names
- FQDNs
- Single IPs
- IP address ranges in CIDR notation

These IOCs are applied to the connections of examined processes and can optionally be used to search process memory.

Each IOC must be placed on a single line. A comment can be specified with a line starting with a # and applies to all following IOCs until another comment is encountered. A score for the IOC can optionally be specified after the IOC, separated by a ;, it defaults to 100 if none is specified.

Listing 5: custom-c2-domains.txt

```
1 # Case 44 C2 Server
2 mastermind.eu
3 googleaccountservices.com
4 89.22.123.12
5 someotherdomain.biz;80
```

### 12.1.5 Mutex or Event Values

Custom mutex or event values can be provided in a file that contains the “handles” keyword in its filename. The entries can be string or regular expression values. The entries are applied to the processes handles as “equals” if no unescaped special regex characters are used, otherwise they are applied as “contains” (though a regex can, of course, specify its match position by using ^ and/or \$).

You can decide if you want to set a scope by using Global\\ or BaseNamedObjects\\ as a prefix. If you decide to use none, your expression will be applied to any scope. Mutex and event IOCs are case sensitive.

Listing 6: custom-mutex-iocs.txt

```

1 Global\\mymaliciousmutex;Operation Fallout - RAT Mutex
2 Global\\WMI_CONNECTION_RECV;Flame Event https://bit.ly/2KjUTuP
3 Dwm-[a-f0-9]{4}-ApiPort-[a-f0-9]{4};Chinese campaign malware June 19

```

### 12.1.6 Named Pipes

Custom named pipe values can be provided in a file that contains the "pipes" keyword in its filename. The entries should be regular expressions that match the malicious named pipes. The `\\\\.\\pipe\\` prefix should not be part of the entry. The IOCs are applied to the pipes as "equals" if no unescaped special regex characters are used, otherwise they are applied as "contains" (though a regex can, of course, specify its match position by using `^` and/or `$`).

Optionally, a score can be added as 2nd field. If none is present, it defaults to 100. Named Pipe IOCs are case insensitive.

Listing 7: custom-named-pipes-iocs.txt

```

1 # Incident Response Engagement
2 MyMaliciousNamedPipe;Malicious pipe used by known RAT
3 MyInteresting[a-z]+Pipe;50;Interesting pipe we have seen in new malware

```

## 12.2 Rules

There are different types of rules you can use to write your own custom rules. This chapter will explain all the methods you can use to achieve this.

For a list of Features/Modules which are used by *Sigma Rules*, *Generic YARA Rules* and *Specific YARA Rules*, please see the table below.

| Name           | Type    | Keyword rules | Log rules | Registry rules | Generic rules | Sigma Rules |
|----------------|---------|---------------|-----------|----------------|---------------|-------------|
| Amcache        | Feature | Yes           | No        | No             | No            | No          |
| Archive        | Feature | No            | No        | No             | Yes           | No          |
| AtJobs         | Feature | Yes           | No        | No             | No            | No          |
| AtJobs         | Module  | Yes           | No        | No             | No            | No          |
| AuthorizedKeys | Feature | Yes           | No        | No             | No            | No          |
| Autoruns       | Module  | No            | No        | No             | No            | No          |
| Cron           | Module  | Yes           | No        | No             | No            | No          |
| DeepDive       | Module  | No            | No        | No             | Yes           | No          |
| DNSSCache      | Module  | No            | No        | No             | No            | No          |
| DumpScan       | Feature | No            | No        | No             | Yes           | No          |
| Eml            | Feature | No            | No        | No             | Yes           | No          |
| Env            | Module  | Yes           | No        | No             | No            | No          |
| ETL            | Feature | Yes           | Yes       | No             | No            | Yes         |
| Eventlog       | Module  | Yes           | Yes       | No             | No            | Yes         |
| Events         | Module  | Yes           | No        | No             | No            | No          |
| EVTX           | Feature | Yes           | Yes       | No             | No            | Yes         |
| FileScan       | Feature | No            | No        | No             | Yes           | No          |
| FileScan       | Module  | No            | No        | No             | Yes           | No          |
| Firewall       | Module  | No            | No        | No             | No            | No          |

continues on next page



Table 2 – continued from previous page

| Name               | Type    | Keyword rules | Log rules | Registry rules | Generic rules | Sigma Rules |
|--------------------|---------|---------------|-----------|----------------|---------------|-------------|
| Hosts              | Module  | No            | No        | No             | No            | No          |
| KnowledgeDB        | Module  | No            | No        | No             | No            | No          |
| Lnk                | Feature | Yes           | No        | No             | No            | No          |
| LoggedIn           | Module  | No            | No        | No             | No            | No          |
| LogScan            | Feature | Yes           | Yes       | No             | No            | Yes         |
| LSASessions        | Module  | No            | No        | No             | No            | No          |
| MFT                | Module  | Yes           | No        | No             | No            | No          |
| Mutex              | Module  | Yes           | No        | No             | No            | No          |
| NetworkSessions    | Module  | No            | No        | No             | No            | No          |
| NetworkShares      | Module  | No            | No        | No             | No            | No          |
| OLE                | Feature | No            | No        | No             | Yes           | No          |
| Pipes              | Module  | No            | No        | No             | No            | No          |
| Prefetch           | Feature | No            | No        | No             | No            | No          |
| ProcessCheck       | Module  | Yes           | No        | No             | No            | Yes         |
| ProcessConnections | Feature | Yes           | No        | No             | No            | No          |
| ProcessHandles     | Feature | Yes           | No        | No             | No            | No          |
| Profiles           | Module  | No            | No        | No             | No            | No          |
| RegistryChecks     | Module  | Yes           | No        | Yes            | No            | No          |
| RegistryHive       | Feature | Yes           | No        | Yes            | No            | No          |
| ServiceCheck       | Module  | Yes           | No        | No             | No            | No          |
| SHIMCache          | Feature | Yes           | No        | No             | No            | No          |
| SHIMCache          | Module  | Yes           | No        | No             | No            | No          |
| TaskScheduler      | Module  | Yes           | No        | No             | No            | No          |
| Users              | Module  | Yes           | No        | No             | No            | No          |
| WER                | Feature | No            | No        | No             | No            | No          |
| WMIPersistence     | Feature | Yes           | No        | No             | No            | No          |
| WMIShutdown        | Module  | No            | No        | No             | No            | No          |

### 12.2.1 Sigma Rules

Sigma is a generic rule format for detections on log data. Sigma is for log data, what Snort is for network packets and YARA is for files.

THOR applies Sigma rules to Windows Eventlogs and log files on disk (.log). By default, THOR ships with the public Sigma rule set, which is maintained by the community at <https://github.com/SigmaHQ/sigma>.

To activate Sigma scanning, you have to use the `--sigma` command line option or perform an `--intense` scan. Sigma scanning is not activated by default. This behavior may change in the future.

By default only the results of Sigma rules of level critical and high are shown. If called with the `--intense` flag, medium level rules are applied as well.

Custom Sigma rules must have the `.yaml` extension for unencrypted sigma rules and the `.ymls` extension for encrypted sigma rules.

```

Eventlog System
Alert Eventlog critical Sigma match on Eventlog SCORE: 170 EVENT_ID: 7045 EVENT_
EVENT_LEVEL: Information EVENT_TIME: 2017-06-18T07:10:06Z
EVENT_MESSAGE: A service was installed in the system. Service Name: WCESERVICE
testing\wce\wce.exe -S Service Type: user mode service Service Start Type: dem
t: LocalSystem
REASON_1: Malicious Service Installations SUBSCORE_1: 100 DESC_1: Detects known
ls that only appear in cases of lateral movement, credential dumping and other s
REASON_2: Malicious Service Install SUBSCORE_2: 70 DESC_2: This method detects w
licious services in the Windows System Eventlog

```

Fig. 1: Example Sigma match on Windows Eventlog

## Sigma Examples

Perform a scan with the Sigma rules on the different local Windows Eventlogs (-a Eventlog)

```
C:\tools\thor>thor64.exe -a Eventlog --sigma
```

Perform a scan with the Sigma rules on logs of Linux systems (-a LogScan) only

```
C:\tools\thor>thor64 -a Filesystem -p /var/log -sigma
```

### 12.2.2 YARA Rules

THOR allows you include your own custom YARA rules. YARA rules must have the **.yar** extension for plain text YARA rules and the **.yas** extension for encrypted YARA rules. (the rules can be encrypted using THOR Util)

Custom YARA rules have to be saved to the **.\custom-signatures\yara** folder. In order to apply only custom YARA rules and IOCs, use the **--customonly** flag.

There are two custom YARA rule types that you can define in THOR:

- Generic Rules
- Specific Rules

#### Generic YARA Rules

All YARA rules which do not contain any specific tag (see *Specific YARA Rules*) are considered generic YARA rules.

The generic YARA rules are applied to the following elements:

- Files  
THOR applies the Yara rules to all files that are smaller than the size limit set in the **thor.yml** and matches specific rules. *Additional Attributes* are available.
- Process Memory  
THOR scans the process memory of all processes with a working set memory size up to a certain limit. This limit can be altered by the **"--max\_process\_size"** parameter.
- Data Chunks  
The rules are applied to the data chunks read during the DeepDive scan. DeepDive only reports and restores chunks if the score level of the rule is high enough to cause at least a warning.

The following table shows in which modules the Generic YARA rules are applied to content.

| Applied in Module                | Examples                                    |
|----------------------------------|---------------------------------------------|
| Filescan, ProcessCheck, DeepDive | incident-feb17.yar<br>misp-3345-samples.yar |

## Specific YARA Rules

The specific YARA rules contain certain tags in their filename to differentiate them further:

- Registry Keys  
Tag: **'registry'**  
Rules are applied to a whole key with all of its values. See *THOR YARA Rules for Registry Detection* for more details.
- Log Files  
Tag: **'log'**  
Rules are applied to each log entry. See *THOR YARA Rules for Log Detection* for more details.
- Process Memory  
Tag: **'process'** or **'memory'**  
Rules are applied to process memory only.
- All String Checks  
Tag: **'keyword'**  
Rules are applied to all string checks in many different modules.
- Metadata Checks (since THOR 10.6)  
Tag: **'meta'**  
Rules are applied to all files without exception, including directories, symlinks and the like, but can only access the THOR specific external variables (see *Additional Attributes*) and the first 2048 bytes of the file.  
Since THOR 10.6.8: If a metadata rule has the special tag DEEPSCAN, THOR will perform a YARA scan on the full file with the default rule set (see *Generic YARA Rules*).  
Since THOR 10.7: Symlinks now have their target as the content.  
Since THOR 10.8: Directories now have their directory listing (as file names, separated by newlines) as the content.

The following table shows in which modules the specific YARA rules are applied to content.

| Tag in File Name | Applied in Module                                                                                                                                     | Examples                               |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------|
| registry         | RegistryChecks, RegistryHive                                                                                                                          | incident-feb17- <b>registry</b> .yar   |
| log              | Eventlog, Logscan, EVT_X                                                                                                                              | general- <b>log</b> -strings.yar       |
| process          | ProcessCheck (only on process memory)                                                                                                                 | case-a23- <b>process</b> -rules.yar    |
| keyword          | Mutex, Named Pipes, Eventlog, MFT, ProcessCheck (on all process handles), ProcessHandles, ServiceCheck, AtJobs, LogScan, AmCache, SHIMCache, Registry | misp-3345- <b>keyword</b> -extract.yar |
| meta             | Filescan                                                                                                                                              | <b>meta</b> -rules.yar                 |

## THOR YARA Rules for Registry Detection

THOR allows checking a complete registry path key/value pairs with Yara rules. To accomplish this, THOR composes a string from the key/value pairs of a registry key path and formats them as shown in the following screenshot.

```

YARA CHECK ON REGISTRY KEY CONTENT:

CMI-CreateHive{D43B12B8-09B5-40DB-B4F6-F6DFEB78DAEC}\Software\Microsoft\Windows\CurrentVersion\Internet Settings
\Zones\4;(default);
CMI-CreateHive{D43B12B8-09B5-40DB-B4F6-F6DFEB78DAEC}\Software\Microsoft\Windows\CurrentVersion\Internet Settings
\Zones\4;DisplayName;Restricted sites
CMI-CreateHive{D43B12B8-09B5-40DB-B4F6-F6DFEB78DAEC}\Software\Microsoft\Windows\CurrentVersion\Internet Settings
\Zones\4;PMDisplayName;Restricted sites [Protected Mode]
CMI-CreateHive{D43B12B8-09B5-40DB-B4F6-F6DFEB78DAEC}\Software\Microsoft\Windows\CurrentVersion\Internet Settings
\Zones\4;Description;This zone contains Web sites that could potentially damage your computer or data.
CMI-CreateHive{D43B12B8-09B5-40DB-B4F6-F6DFEB78DAEC}\Software\Microsoft\Windows\CurrentVersion\Internet Settings
\Zones\4;Icon;inetcpl.cpl#00004481
CMI-CreateHive{D43B12B8-09B5-40DB-B4F6-F6DFEB78DAEC}\Software\Microsoft\Windows\CurrentVersion\Internet Settings
\Zones\4;LowIcon;inetcpl.cpl#005426

Warning: Suspicious file name in Registry Value detected STRING: C:\TEMP\gsecdump.exe PATTERN: gsecdump\..exe KEY
: CMI-CreateHive{D43B12B8-09B5-40DB-B4F6-F6DFEB78DAEC}\Software\Microsoft\Windows\CurrentVersion\Run HIVE: C:\Us
ers\trinity\NTUSER.DAT
Alarm: Malicious registry key found KEY: CMI-CreateHive{D43B12B8-09B5-40DB-B4F6-F6DFEB78DAEC}\Software\Microsoft
\Windows\CurrentVersion\Run NAME: xyz VALUE: evil.exe HIVE: C:\Users\trinity\NTUSER.DAT DESC: Test
YARA CHECK ON REGISTRY KEY CONTENT:

CMI-CreateHive{D43B12B8-09B5-40DB-B4F6-F6DFEB78DAEC}\Software\Microsoft\Windows\CurrentVersion\Run;THOR Test;C:\
\TEMP\gsecdump.exe
CMI-CreateHive{D43B12B8-09B5-40DB-B4F6-F6DFEB78DAEC}\Software\Microsoft\Windows\CurrentVersion\Run;xyz;evil.exe

```

Fig. 2: Composed strings from registry key/value pairs

The composed format is:

```
KEYPATH;KEY;VALUE\n
KEYPATH;KEY;VALUE\n
KEYPATH;KEY;VALUE\n
```

### Registry Base Names

Please notice that strings like HKEY\_LOCAL\_MACHINE, HKLM, HKCU, HKEY\_CURRENT\_CONFIG are **not** part of the key path that your YARA rules are applied to. They depend on the analyzed hive and should not be in the strings that you define in your rules.

Values are formatted as follows:

- REG\_BINARY values are hex encoded with upper case.
- REG\_MULTI\_SZ values are printed with \\0 separating the multiple strings.
- Numeric values are printed normally (with base 10; e.g., use 32 for REG\_DWORD 0x00000020).
- String values are printed normally.

This means that you can write a Yara rule that looks like this (remember to escape all backslashes):

```
rule Registry_DarkComet {
 meta:
 description = "DarkComet Registry Keys"
 strings:
```

(continues on next page)

(continued from previous page)

```

 $a1 = "LEGACY_MY_DRIVERLINKNAME_TEST;NextInstance"
 $a2 = "\\Microsoft\\Windows\\CurrentVersion\\Run;MicroUpdate"
 $a3 = "Path;Value;4D5A00000001" # REG_BINARY value
 $a4 = "Shell\\Open;Command;explorer.exe\\0comet.exe" # REG_MULTI_SZ value
 $a5 = ";Type;32" # REG_DWORD 0x00000020
condition:
 1 of them
}

```

Remember that you have to use the keyword **registry** in the file name in order to initialize the YARA rule file as registry rule set (e.g. "**registry\_exe\_in\_value.yar**").

Registry scanning uses bulk scanning. See *Bulk Scanning* for more details.

## THOR YARA Rules for Log Detection

YARA Rules for logs are applied as follows:

- For text logs, each line is passed to the YARA rules.
- For Windows Event Logs, each event is serialized as follows for the YARA rules: Key1: Value1 Key2: Value2 ... where each key / value pair is an entry in EventData or UserData in the XML representation of the event.

Log (both text log and event log) scanning uses bulk scanning. See *Bulk Scanning* for more details.

Remember that you have to use the keyword **log** in the file name in order to initialize the YARA rule file as registry rule set (e.g. **my\_log\_rule.yar**).

## How to Create YARA Rules

Using the UNIX "string" command on Linux systems or in a CYGWIN environment enables you to extract specific strings from your sample base and write your own rules within minutes. Use "**string -el**" to also extract the UNICODE strings from the executable.

A useful Yara Rule Generator called "yarGen" provided by our developers can be downloaded from Github. It takes a target directory as input and generates rules for all files in this directory and so called "super rules" if characteristics from different files can be used to generate a single rule to match them all. (<https://github.com/Neo23x0/yarGen>)

Another project to mention is the "Yara Generator", which creates a single Yara rule from one or multiple malware samples. Placing several malware files of the same family in the directory that gets analyzed by the generator will lead to a signature that matches all descendants of that family. (<https://github.com/Xen0ph0n/YaraGenerator>)

We recommend testing the Yara rule with the "yara" binary before including it into THOR because THOR does not provide a useful debugging mechanism for Yara rules. The Yara binary can be downloaded from the developers' website (<https://github.com/VirusTotal/yara>).

The best practice steps to generate a custom rule are:

1. Extract information from the malware sample (Strings, Byte Code, MD5 ...)
2. Create a new Yara rule file. It is important to:
  - a. Define a unique rule name – duplicates lead to errors
  - b. Give a description that you want to see when the signature matches

- c. Define an appropriate score (optional but useful in THOR, default is 75)
3. Check your rule by scanning the malware with the Yara binary from the project's website to verify a positive match
4. Check your rule by scanning the "Windows" or "Program Files" directory with the Yara binary from the project's website to detect possible false positives
5. Copy the file to the "/custom-signatures/yara" folder of THOR and start THOR to check if the rule integrates well and no error is thrown

There are some THOR specific add-ons you may use to enhance your rules.

Also see these articles on how to write "simple but sound" YARA rules:

<https://www.nextron-systems.com/2015/02/16/write-simple-sound-yara-rules/>

<https://www.nextron-systems.com/2015/10/17/how-to-write-simple-but-sound-yara-rules-part-2/>

## Typical Pitfalls

Some signatures - even the ones published by well-known vendors - cause problems on certain files. The most common source of trouble is the use of regular expressions with a variable length as shown in the following example. This APT1 rule published by the AlienVault team caused the Yara Binary as well as the THOR binary to run into a loop while checking certain malicious files. The reason why this happened is the string expression "\$gif1" which causes Yara to check for a "word character" of undefined length. Try to avoid regular expressions of undefined length and everything works fine.

AlienVault APT1 Rule: yara

```
1 rule APT1_WEBC2_TABLE {
2 meta:
3 author = "AlienVault Labs"
4 strings:
5 $msg1 = "Fail To Execute The Command" wide ascii
6 $msg2 = "Execute The Command Successfully" wide
7 $gif1 = /\w+\.gif/
8 $gif2 = "GIF89" wide ascii
9 condition:
10 3 of them
11 }
```

Copying your rule to the signatures directory may cause THOR to fail during rule initialization. If this happens you should check your rule again with the Yara binary. Usually this is caused by a duplicate rule name or syntactical errors.

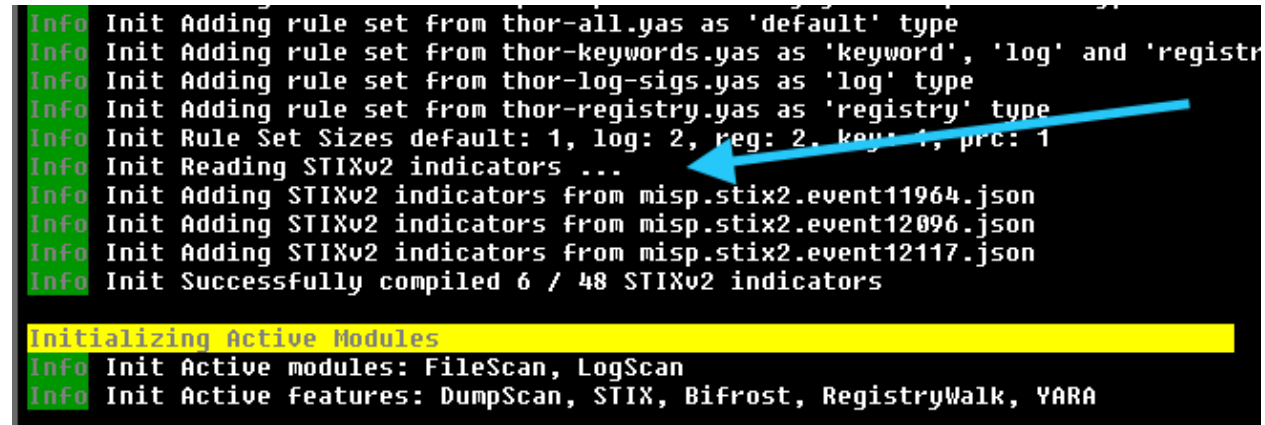
## YARA Rule Performance

We compiled a set of guidelines to improve the performance of YARA rules. By following these guidelines you avoid rules that cause many CPU cycles and hamper the scan process.

<https://gist.github.com/Neo23x0/e3d4e316d7441d9143c7>

## 12.3 STIX IOCs

THOR can read and apply IOCs provided in STIXv2 JSON files. They must have the `.json` extension for unencrypted STIXv2 files and the `.jsos` extension for encrypted STIXv2 files.



```

Info Init Adding rule set from thor-all.yas as 'default' type
Info Init Adding rule set from thor-keywords.yas as 'keyword', 'log' and 'registr
Info Init Adding rule set from thor-log-sigs.yas as 'log' type
Info Init Adding rule set from thor-registry.yas as 'registry' type
Info Init Rule Set Sizes default: 1, log: 2, reg: 2, key: 1, prc: 1
Info Init Reading STIXv2 indicators ...
Info Init Adding STIXv2 indicators from misp.stix2.event11964.json
Info Init Adding STIXv2 indicators from misp.stix2.event12096.json
Info Init Adding STIXv2 indicators from misp.stix2.event12117.json
Info Init Successfully compiled 6 / 48 STIXv2 indicators

Initializing Active Modules
Info Init Active modules: FileScan, LogScan
Info Init Active features: DumpScan, STIX, Bifrost, RegistryWalk, YARA

```

Fig. 3: STIXv2 Initialization during startup

The following observables are supported.

- file:name with
  - =
  - !=
  - LIKE
  - MATCHES
- file:parent\_directory\_ref.path with
  - =
  - !=
  - LIKE
  - MATCHES
- file:hashes.sha-256 / file:hashes.sha256 with
  - =
  - !=
- file:hashes.sha-1 / file:hashes.sha1 with
  - =
  - !=
- file:hashes.md-5 / file:hashes.md5 with
  - =
  - !=
- file:size with
  - <

- <=
- >
- >=
- =
- !=
- file:created with
  - <
  - <=
  - >
  - >=
  - =
  - !=
- file:modified with
  - <
  - <=
  - >
  - >=
  - =
  - !=
- file:accessed with
  - <
  - <=
  - >
  - >=
  - =
  - !=
- win-registry-key:key with
  - =
  - !=
  - **LIKE**
  - **MATCHES**
- win-registry-key:values.name with
  - =
  - !=
  - **LIKE**
  - **MATCHES**



- win-registry-key:values.data with with
  - =
  - !=
  - LIKE
  - MATCHES
- win-registry-key:values.modified\_time with
  - <
  - <=
  - >
  - >=
  - =
  - !=

### 12.3.1 STIX v1

STIX version 1 is not supported.

## 12.4 Enhance YARA Rules with THOR Specific Attributes

The following listing shows a typical YARA rule with the three main sections "meta", "strings" and "condition". The YARA Rule Manual which can be downloaded as PDF from the developer's website and is bundled with the THOR binary is a very useful guide and reference to get a function and keyword overview and build your own rules based on the YARA standard.

The "meta" section contains all types of meta information and can be extended freely to include own attributes. The "strings" section lists strings, regular expressions or hex string to identify the malware or hack tool. The condition section defines the condition on which the rule generates a "match". It can combine various strings and handles keywords like "not" or "all of them".

Simple Yara Rule:

```

1 rule simple_demo_rule_1 {
2 meta:
3 description = "Demo Rule"
4 strings:
5 $s1 = "EICAR-STANDARD-ANTIVIRUS-TEST-FILE"
6 condition:
7 $s1
8 }
```

The following listing shows a more complex rule that includes a lot of keywords used in typical rules included in the rule set.

Complex Yara Rule:

```
1 rule complex_demo_rule_1 {
2 meta:
3 description = "Demo Rule"
4 strings:
5 $a1 = "EICAR-STANDARD-ANTIVIRUS-TEST-FILE"
6 $a2 = "li0n" fullword
7 $a3 = /msupdate\.(exe|dll)/ nocase
8 $a4 = { 00 45 9A ?? 00 00 00 AA }
9 $fp = "MSWORD"
10 condition:
11 1 of ($a*) and not $fp
12 }
```

The example above shows the most common keywords used in our THOR rule set. These keywords are included in the YARA standard. The rule does not contain any THOR specific expressions.

Yara provides a lot of functionality but lacks some mayor attributes that are required to describe an indicator of compromise (IOC) defined in other standards as i.e. OpenIOC entirely. Yara's signature description aims to detect any kind of string or byte code within a file but is not able to match on meta data attributes like file names, file path, extensions and so on.

THOR adds functionality to overcome these limitations.

### 12.4.1 Score

THOR makes use of the possibility to extend the Meta information section by adding a new parameter called "score".

This parameter is the essential value of the scoring system, which enables THOR to increment a total score for an object and generate a message of the appropriate level according to the final score.

Every time a signature matches the value of the score attribute is added to the total score of an object.

Yara Rule with THOR specific attribute "score":

```
1 rule demo_rule_score {
2 meta:
3 description = "Demo Rule"
4 score = 80
5 strings:
6 $a1 = "EICAR-STANDARD-ANTIVIRUS-TEST-FILE"
7 $a2 = "honkers" fullword
8 condition:
9 1 of them
10 }
```

Feel free to set your own "score" values in rules you create. If you don't define a "score" the rule gets a default score of 75.

The scoring system allows you to include ambiguous, low scoring rules that can't be used with other scanners, as they would generate to many false positives. If you noticed a string that is used in malware as well as legitimate files, just assign a low score or combine it with other attributes, which are used by THOR to enhance the functionality and are described in [Additional Attributes](#).

## 12.4.2 Additional Attributes

THOR allows using certain external variables in your generic and meta YARA rules. These external variables are:

- **filename**
  - single file name
  - Example: `cmd.exe`
- **filepath**
  - file path without file name
  - Example: `C:\temp`
- **extension**
  - file extension with a leading `.`, lower case
  - Example: `.exe`
- **filetype**
  - type of the file based on the magic header signatures (for a list of valid file types see: `./signatures/misc/file-type-signatures.cfg`)
  - Example: `EXE` or `ZIP`
- **timezone**
  - the system's time zone (see [https://golang.org/src/time/zoneinfo\\_abbrs\\_windows.go](https://golang.org/src/time/zoneinfo_abbrs_windows.go) for valid values)
- **language**
  - the systems language settings (see <https://docs.microsoft.com/en-us/windows/win32/intl/sort-order-identifiers>)
- **owner**
  - The file owner
  - Example: `NT-AUTHORITY\SYSTEM` on Windows
  - Example: `root` on Linux
- **group** (available since THOR 10.6.8)
  - The file group
  - Example: `root` on Linux
  - This variable is empty on Windows
- **filemode** (available since THOR 10.6)
  - file mode for this file (see <https://man7.org/linux/man-pages/man7/inode.7.html>, "The file type and mode").
  - On Windows, this variable will be an artificial approximation of a file mode since Windows is not POSIX compliant.
- **filesize**
  - The value contains the file size in bytes. It is provided directly by YARA and is not specific to THOR.

Yara Rule with THOR External Variable:

```

1 rule demo_rule_enhanced_attribute_1 {
2 meta:
3 description = "Demo Rule - Eicar"
4 strings:
5 $a1 = "EICAR-STANDARD-ANTIVIRUS-TEST-FILE"
6 condition:
7 $a1 and filename matches /eicar.com/
8 }

```

A more complex rule using several of the THOR external variables would look like the one in the following listing.

This rule matches to all files containing the EICAR string, having the name "eicar.com", "eicar.dll" or "eicar.exe" and a file size smaller 100byte.

Yara Rule with more complex THOR Enhanced Attributes.

```

1 rule demo_rule_enhanced_attribute_2 {
2 meta:
3 author = "F.Roth"
4 strings:
5 $a1 = "EICAR-STANDARD-ANTIVIRUS-TEST-FILE"
6 condition:
7 $a1 and filename matches /eicar\.(com|dll|exe)/ and filesize < 100
8 }

```

The following YARA rule shows a typical combination used in one of the client specific rule sets, which are integrated in THOR. The rule matches on .idx files that contain strings used in the Java Version of the VNC remote access tool. Without the enhancements made this wouldn't be possible as there would be no way to apply the rule only to a special type of extension.

Real Life Yara Rule:

```

1 rule HvS_Client_2_APT_Java_IDX_Content_hard {
2 meta:
3 description = "VNCViewer.jar Entry in Java IDX file"
4 strings:
5 $a1 = "vncviewer.jar"
6 $a2 = "vncviewer/VNCViewer.class"
7 condition:
8 1 of ($a*) and extension matches /\.idx/
9 }

```

### 12.4.3 Bulk Scanning

THOR scans registry and log entries in bulks since each YARA invocation has a relatively high overhead. This means that during the scan, the following happens:

- THOR gathers entries that need to be scanned.
- When sufficiently many entries are gathered, all of them are combined (separated by line breaks) and passed to YARA.
- If any YARA rule matches, each entry is scanned separately with YARA to determine whether any YARA rule matches for this specific entry.

One potential caveat of this is that false positive strings may prevent a rule from ever applying.

For example, consider this rule:

```

1 rule FakeMicrosoftStartupEntry {
2 strings:
3 $s1 = "Microsoft\\SomeRegistryKey;ShouldBeUsedOnlyByMicrosoft;"
4 $fp = "Windows\\System32"
5 condition:
6 $s1 and not $fp
7 }

```

This rule is meant to match if the specified registry key contains some DLL that is not in C:\Windows\System32. However, the false positive string may inadvertently match on other entries in the bulk, like here:

```

Path\to\Microsoft\SomeRegistryKey;ShouldBeUsedOnlyByMicrosoft;C:\evil.exe
...
Path\to\SomeOtherRegistryKey;Entry;C:\Windows\System32\explorer.exe
...

```

Because the rule does not apply to the bulk, THOR never scans the single elements and does not report any match. Therefore, be very careful with false positive strings with log or registry YARA rules.

A possible workaround for this issue is to define the false positive strings in ways that they can't match anywhere else, e.g. like this:

```

rule FakeMicrosoftStartupEntry {
 strings:
 $s1 = "Microsoft\\SomeRegistryKey;ShouldBeUsedOnlyByMicrosoft;"
 $fp = /Microsoft\\SomeRegistryKey;ShouldBeUsedOnlyByMicrosoft;[^\\n]{0,40}
 ↪Windows\\System32/
 condition:
 $s1 and not $fp
}

```

## 12.4.4 Restrict Yara Rule Matches

On top of the keyword based initialization you can restrict Yara rules to match on certain objects only. It is sometimes necessary to restrict rules that e.g. cause many false positives on process memory to file object detection only. Use the meta attribute "type" to define if the rule should apply to file objects or process memory only.

Apply rule in-memory only:

```

1 rule Malware_in_memory {
2 meta:
3 author = "Florian Roth"
4 description = "Think Tank Campaign"
5 type = "memory"
6 strings:
7 $s1 = "evilstring-inmemory-only"
8 condition:
9 1 of them
10 }

```

Apply rule on file objects only:

```
1 rule Malware_in_fileobject {
2 meta:
3 description = "Think Tank Campaign"
4 type = "file"
5 strings:
6 $s1 = "evilstring-infile-only"
7 condition:
8 1 of them
9 }
```

You can also decide if a rule should not match in "DeepDive" module by setting the "nodeepdive" attribute to "1".

Avoid DeepDive application:

```
1 rule Malware_avoid_DeepDive {
2 meta:
3 description = "Think Tank Campaign"
4 nodeepdive = 1
5 strings:
6 $s1 = "evilstring-not-deepdive"
7 condition:
8 1 of them
9 }
```

If you have problems with false positives caused by the specific YARA rules, try using the "limit" modifier in the meta data section of your YARA rule. Using the "limit" attribute, you can limit the scope of your rules to a certain module. (Important: Use the module name as stated in the log messages of the module, e.g. "ServiceCheck" and not "services")

E.g. if you have defined a malicious 'Mutex' named '\_evtx\_' in a rule and saved it to a file named "mutex-keyword.yar", the string "\_evtx\_" will be reported in all other modules to which the keyword rules are applied – e.g. during the Eventlog scan.

You can limit the scope of your rule by setting 'limit = "Mutex"' in the meta data section of the YARA rule.

Limits detection to the "Mutex" module:

```
1 rule Malicious_Mutex_Evtx {
2 meta:
3 description = "Detects malicious mutex EVTX"
4 limit = "Mutex"
5 strings:
6 $s1 = "_evtx_"
7 condition:
8 1 of them
9 }
```

Notes:

- the internal check in THOR against the module name is case-insensitive
- this "limit" parameter only applies to specific YARA rules (legacy reasons – will be normalized in a future THOR version)

## 12.4.5 False Positive Yara Rules

Yara rules that have the "falsepositive" flag set will cause a score reduction on the respective element by the value defined in the "score" attribute. Do not use a negative score value in YARA rules.

False Positive Rule:

```
1 rule FalsePositive_AVSig1 {
2 meta:
3 description = "Match on McAfee Signature Files"
4 falsepositive = 1
5 score = 50
6 strings:
7 $s1 = "%%McAfee-Signature%%"
8 condition:
9 1 of them
10 }
```





## OTHER TOPICS

### 13.1 License Retrieval

THOR allows for a more flexible way to fetch licenses, besides the classic way of placing a license file in the program folder. In this chapter we will show both available options for license retrieval.

It is important to know that those two options also work with *THOR Remote*. In this case, all licenses will be downloaded to the host which is running the initial THOR Remote command (the host running THOR Remote does not need a license).

---

**Important:** If you have already a valid THOR license for your host placed within THOR's program folder, no (new) license will be downloaded/issued from the remote locations.

---

#### 13.1.1 ASGARD License Retrieval

If you are having a local instance of the ASGARD Management Center installed and using its license pool for your THOR scans, you can use the `--asgard` flag to download a valid license. This flag also needs the `--asgard-token` flag to work. The Token can be found in the **Download** section of your ASGARD Management Center.

Example:

```
nexttron@unix:~/thor$./thor-linux-64 --asgard "my-asgard.local" --asgard-token "download-
↳ token"
[...SNIP...]
Info License file found LICENSE: my-asgard.local OWNER: John Doe TYPE: Server STARTS:
↳ 2023/08/30 EXPIRES: 2023/11/01 SCANNER: THOR VALID: true REASON:
```

The retrieved license will be placed in the program folder of THOR, so you can run THOR the next time without all the extra flags. The name of the license is `<hostname>.lic`. Rerunning the command will not issue a new license, but rather download the already valid license again from your ASGARD Management Center.

### 13.1.2 Nextron Portal License Retrieval

If you are using standalone packages of THOR, you can speed up the process of deploying THOR by using its `--portal-key` flag. This allows you to download a THOR license straight from the Licensing Portal, without the need to generate all the licenses and downloading them manually first. This is a good way to automate scanning.

The argument `--portal-key` is expecting one argument, which can be one of:

- The API key of your Portal user
- A download token for one of your contracts

When using an API key, THOR will grab the first available license from the contract with the lowest ID and issue one to your host. No new license will be issued if a valid license was found for the host. If no valid license was found, a new one will be issued. This also means that you should provide the `--portal-contracts` flag if you want to limit THOR to a specific contract(s) for issuing/downloading licenses.

Example:

```
nexttron@unix:~/thor$./thor-linux-64 --portal-key "my-api-key" --portal-contracts "3,5,
↪12,13"
...SNIP...
Info License file found LICENSE: portal.nextron-systems.com OWNER: Jane Doe TYPE: Server.
↪STARTS: 2023/03/10 EXPIRES: 2023/09/29 SCANNER: THOR VALID: true REASON:
```

The retrieved license will be placed in the program folder of THOR, so you can run THOR the next time without all the extra flags. The name of the license is `<hostname>.lic`. Rerunning the command will not issue a new license, but rather download the already valid license again from the portal.

**Attention:** If no valid license is found, a new one will be issued. This can be prevented with the `--portal-nonewlic` flag. If THOR can't find a valid license within the account/contracts, it will simply exit. This is a useful feature if you want to prevent over-issuing of licenses within your contracts.

## 13.2 Evidence Collection

### 13.2.1 Process Memory Dumps (`--dump-procs`)

Since THOR version 10.5 it supports process dumping to backup volatile malware information.

THOR on Windows creates a process dump of any process that is considered malicious. Maliciousness is determined as anything that triggers a warning or an alert.

Activate process memory dumping with `--dump-procs`.

This process dump can then be analyzed with standard tools later on to examine the found malware.

To prevent flooding the disk fully in case many dumps are created, old dumps of a process are overwritten if a new dump is generated. Also, THOR will not generate dumps by default if less than 5 GB disk space is available. This can be overwritten to always or never dump malicious processes.

Also note that THOR will never dump `lsass.exe` to prevent these dumps from potentially being used to extract passwords by any attackers.

```
Warning: ProcessCheck YARA rule match on process memory RULE: Example_Rule TAGS: DESC: Example rule to match a process SCORE: 75 REFERENCE: not set RULEDATE: 2019-05-14 PID: 5736 NAME: procexp64.exe CMD: "C:\Users\Max\Downloads\PROCEXP64.EXE" USER: DESKTOP-EEM5B52\Max MATCH_STRINGS: Str1: "procexp"
Info: ProcessCheck Successfully dumped process PID: 5736 PPID: 3320 PARENT: NAME: procexp64.exe OWNER: DESKTOP-EEM5B52\Max COMMAND: "C:\Users\Max\Downloads\PROCEXP64.EXE" PATH: C:\Users\Max\Downloads\PROCEXP64.EXE
CREATED: Mon May 11 14:27:58 2020
MD5: 7e7eaa8aebc4026be3b56b965b0d8947 CONNECTION_COUNT: 0 LISTEN_PORTS: FILE_1: C:\Users\Max\Downloads\PROCEXP64.EXE EXISTS_1: yes MD5_1: 7e7eaa8aebc4026be3b56b965b0d8947 SHA1_1: 57fe177df7e94ba8495e1885c9b5946fa4312df3 SHA256_1: aac11d3ff8661e14a6d7073e44f0d6ccabc436856af5faf10e761c57e8b42f71 FIRSTBYTES_1: 4d5a90000300000004000000ffff0000b8000000 DUMP_FILE: C:\ProgramData\thor\procexp64.exe.zip
Info: ProcessCheck Finished module TOOK: 0 hours 0 mins 9 secs
```

Fig. 1: Process dumping

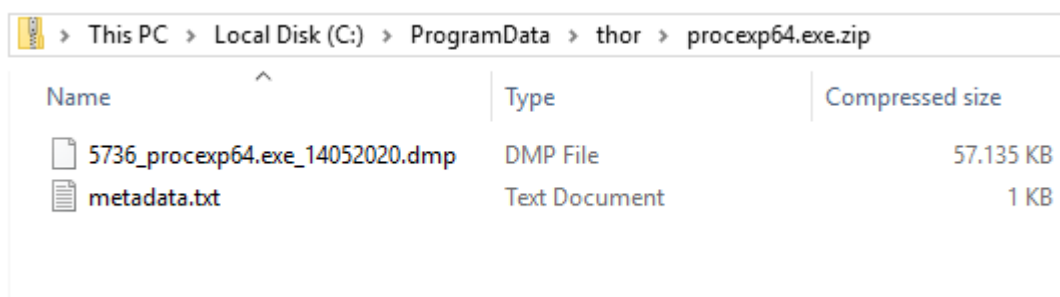


Fig. 2: Process dumps on disk

### 13.2.2 File Collection (Bifrost)

#### Bifrost v1 with Script-Based Server

The `./tools` folder in the program directory contains a simple Python based file collection server named Bifrost. The script is named `bifrost-server.py`.

You can run that script on any internal system with a Python script interpreter installed. By default, it uses port 1400/tcp for incoming connections but you can use any port you like.

Usage is:

```
nexttron@unix:~$ python ./bifrost-server.py -h
usage: bifrost-server.py [-h] [-d out-dir] [-i ip] [-p port]
```

Bifrost optional arguments:

```
-h, --help show this help message and exit
-d out-dir Quarantine directory
-i ip IP address to bind to
-p port Port to bind to (tcp, default 1400)
```

You can run the server script with:

```
nexttron@unix:~$ python ./bifrost-server.py
```

In order to send suspicious file to that server, you have to set some command line flags when running THOR, e.g.

```
C:\nexttron\thor>thor64.exe --bifrostServer myserver
```

A more complex statement setting a minimum score and custom port would look like this:

```
C:\nexttron\thor>thor64.exe --bifrostServer myserver --bifrost-port 8080 --bifrostLevel 80
```

THOR will then try to submit all samples with score equal or higher than 80 to a Bifrost service running on myserver port 8080/tcp.

### Bifrost v2 with ASGARD

Bifrost v2 cannot be used standalone yet. The required API Key is set by ASGARD v2 during initialization and is unknown to a THOR user.

You can activate the quarantine function via Bifrost v2 when creating a single or group scan via the ASGARD management interface.

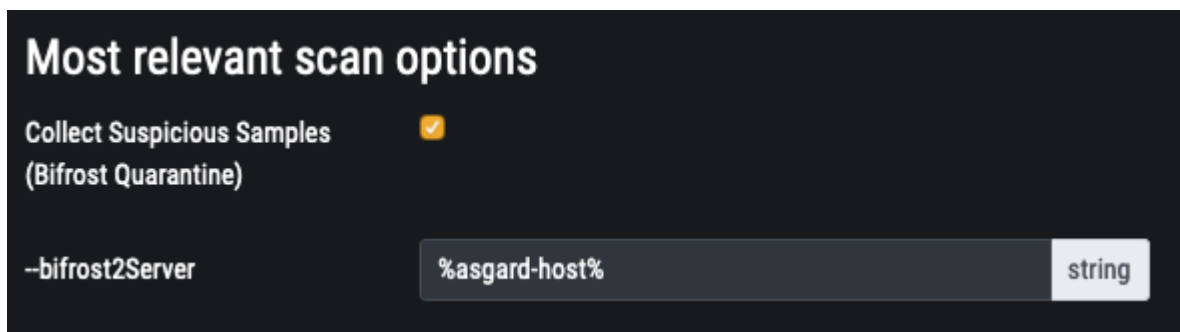


Fig. 3: Configure Quarantine via Bifrost in New Scan Dialogue

| ASGARD                                                           |         |                                          |                    |
|------------------------------------------------------------------|---------|------------------------------------------|--------------------|
| Bifrost Samples                                                  |         |                                          |                    |
| 40 Entries                                                       | Refresh | Column visibility                        |                    |
| SHA256                                                           | Type    | Affected Hosts                           | Filenames          |
| Search                                                           | Search  | Search                                   | Search             |
| b57bf397984545f419045391b56dcdf7b0bed8b6ee331b5c46cee35c92ffa13d | JSP     | server-001.de.sales.nexttron-systems.com | zehir4.asp.php.txt |
| 7d72ed0ef1b497619f12bc962512061d131c96cf9bccdd4a9a4345490e0a088c | JSP     | server-001.de.sales.nexttron-systems.com | zehir4.php         |
| ee256d7cc3ceb2bf3a1934d553cdd36e3fbde62a02b20a1b748a74e85d4dbd33 | PHP     | server-001.de.sales.nexttron-systems.com | safe0ver.php       |

Fig. 4: Collected File Evidence in ASGARD v2

## 13.3 Resource Control

THOR's internal resource control feature puts the system's stability and the responsiveness of running services first.

Resource control is active by default. You can deactivate it using **--norescontrol**.

Be advised that due to Resource Control, the THOR scan may terminate its completion. The scan gets terminated under the following conditions:

1. If the available physical memory drops below 60MB
2. If more than 60 MB of log data have been written (disk / syslog)

In this case, THOR switches in the "reduced-logging" mode in which it only transmits "Notices, Warnings and Alerts" and after another 4 MB of log data THOR terminates itself in order to prevent log flooding due to a high number of false positives

If the scan constantly terminates you should check what causes the performance issues or choose times with less workload (e.g. weekends, night). To debug such states, you can check the last warning that THOR generates before exiting the scan. It includes the top memory consumers that could have caused the memory exhaustion.

```
> 1/12 > Running module 'Autoruns'
Info: Autoruns Starting module
Warning: Rescontrol Available physical memory dropped below 60000 MB
Warning: Rescontrol Stopping THOR scan in order to avoid a memory outage (use --norescontrol to avoid this)
Error: Rescontrol Could not get process memory usage PID: 69018 ERROR: exit status 1
Notice: Rescontrol Process with high memory usage PID: 80897 NAME: plugin-container COMMAND: /Applications/Firefox.app/Contents/MacOS/plugin-container.app/Content
s/MacOS/plugin-container -childID 6 -isForBrowser -prefsLen 8985 -prefMapSize 182025 -sbStartup -sbLevel 3 -sbAllowAudio -sbAllowWindowServer -sbAppPath /Applicat
ions/Firefox.app -parentBuildID 20190516215225 -greomni /Applications/Firefox.app/Contents/Resources/omni.ja -appomni /Applications/Firefox.app/Contents/Resources
/browser/omni.ja -appdir /Applications/Firefox.app/Contents/Resources/browser -profile /Users/codehardt/Library/Application Support/Firefox/Profiles/a09ubvas.defa
ult 69020 gecko-crash-server-pipe.69020 org.mozilla.machname.1328547851 tab MEMORY_USAGE: 4.35%
Notice: Rescontrol Process with high memory usage PID: 17144 NAME: Sourcetree COMMAND: /Applications/Sourcetree.app/Contents/MacOS/Sourcetree MEMORY_USAGE: 2.95%
Notice: Rescontrol Process with high memory usage PID: 69020 NAME: firefox COMMAND: /Applications/Firefox.app/Contents/MacOS/firefox -foreground MEMORY_USAGE: 2.9
4%
```

Fig. 5: Resource Control Scan Termination

**Warning:** Deactivating Resource Control on systems with exhausted resources can put the system's stability at risk.

### 13.3.1 Automatic Soft Mode

Soft mode is automatically activated on systems with low hardware resources.

One of the following conditions activates soft mode:

- Less than 2 CPU cores
- Less than 1024 MB of RAM

In Soft mode several checks and features that could risk system's stability or could provoke an Antivirus or HIDS to intervene with the scanner are disabled. See *Scan Modes* for a complete overview.

## 13.4 Scoring System

The scoring system is one of THOR's most prominent features. Both YARA signatures and filename IOCs contain a score field. The score is an integer value that can be negative to reduce the score on elements that are prone to false positives.

Only YARA rules and Filename IOCs support a user defined score. But since you are able to write YARA rules for almost every module, the scoring system is very flexible.

The total score of an element determines the level/severity of the resulting log message.

Table 1: THOR <= 10.6

| Score | Level   | Condition                         |
|-------|---------|-----------------------------------|
| 40    | Notice  |                                   |
| 60    | Warning |                                   |
| 100   | Alert   | At least 1 sub score more than 75 |

Table 2: THOR >= 10.7

| Score | Level   | Condition                         |
|-------|---------|-----------------------------------|
| >= 40 | Notice  |                                   |
| >= 60 | Warning |                                   |
| > 80  | Alert   | At least 1 sub score more than 75 |

**Note:** As of THOR version 10.7, we reworked the scoring system to only use scores between 0 and 100. The score is a metric that expresses a combination of confidence and severity in percent. This means a finding with a score of 95 can be seen as a severe finding with a high confidence. Exceptions might be - as always - obvious false positives like unencrypted or in-memory AV signatures.

### 13.4.1 Scoring per Signature Type Match

| Type               | Score                                                                              |
|--------------------|------------------------------------------------------------------------------------|
| YARA match         | Defined in the meta data of the YARA rule as integer value (e.g. "score = 50")     |
| Filename IOC match | Defined in the 2 <sup>nd</sup> field of the CSV (e.g. <code>\\evil.exe;80</code> ) |
| Keyword IOC match  | "warning" level messages, see <a href="#">Default Scores</a>                       |
| C2 IOC match       | "warning" and "alert" level messages, see <a href="#">Default Scores</a>           |

### 13.4.2 Accumulated Scores

If an element has multiple sub-scores, all sub-scores will be accumulated and calculated into one final score. The following chapters show you how those scores are calculated.

#### THOR $\leq 10.6$

| Module                                                                                                                                      | Cumulated Scoring | Score                                                                                                                                                                                                                                                                              |
|---------------------------------------------------------------------------------------------------------------------------------------------|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• Filescan</li> <li>• Archive Scan</li> <li>• DeepDive</li> <li>• Prefetch</li> <li>• WER</li> </ul> | Yes               | Score is a sum of the scores of all "REASONS" (YARA matches, filename IOCs, other anomalies)<br><b>Note 1:</b> Only positive scores are shown by default<br><b>Note 2:</b> Only the top 2 reasons are shown by default (use <code>--allreasons</code> to show all positive scores) |
| All Other Modules                                                                                                                           | No                | Individual score of each signature match (YARA, filename IOC, keywords, C2)<br><b>Note 1:</b> This means that multiple matches for a single element are possible                                                                                                                   |

#### THOR $\geq 10.7$

Most modules and features summarize via reasons. Please keep in mind that only positive scores and the top two reasons are shown by default. You can use `--allreasons` to show all positive scores.

Reason scores are not added up for the total score. Instead, given a number of scores ( $s_0, s_1, \dots$ ) that are ordered descending. The total score is calculated with the following formula:

$$100 * (1 - (1 - s_0 / 100 / 2^0) * (1 - s_1 / 100 / 2^1) * (1 - s_2 / 100 / 2^2) * \dots)$$

This means, scores are "capped" at a maximum of 100, and multiple lower scores are weighted far less.

You can use python to calculate the score and try the formula. Please note that we use an example with five sub-scores and no sub-score higher than the threshold of 75 to turn classify this as an alert:

```
subscore0 = 1 - 70 / 100 / pow(2, 0)
subscore1 = 1 - 70 / 100 / pow(2, 1)
subscore2 = 1 - 50 / 100 / pow(2, 2)
subscore3 = 1 - 40 / 100 / pow(2, 3)
subscore4 = 1 - 40 / 100 / pow(2, 4)
score = 100 * (1 - (subscore0 * subscore1 * subscore2 * subscore3 * subscore4))
print(score)
84.195859375
```

### 13.4.3 Default Scores

If no score is set in an "alert" or "warning" message, THOR automatically appends a score that corresponds to the message level:

Table 3: THOR <= 10.6

| Level   | Score |
|---------|-------|
| Warning | 70    |
| Alert   | 100   |

Table 4: THOR >= 10.7

| Level   | Score |
|---------|-------|
| Warning | 60    |
| Alert   | 80    |

### 13.4.4 Exception: High total score with low sub scores

"Alerts" on file system elements are only generated if one of the sub scores is more than 75.

Before that change, multiple low scoring reasons had led to a score higher 100 and caused an "Alert" level message although not a single hard match was included in the "Reasons". A wrong extension, e.g. `.txt` for an executable, which is often used by employees to hand executables through tight mail filters, and a suspicious location, e.g. `C:\Temp\funprog.txt` caused an "Alert" level message.

Since version 8.27.2, one of the sub scores that pushes the total score over 100 has to be more than 75. (internally calculated as `"alert_level - 25"` because the user can adjust the alert level via the `--alert` parameter)

### 13.4.5 Exception: Filename IOC Matches

The "Filename IOC Check" is a sub check of the "String Check", which is applied to many elements, like Eventlog messages or Registry keys.

The function `checkString()` receives a string as input and returns possible matches.

The string is checked in multiple sub-checks against different signature lists. The most important sub-checks are `checkKeyword()` and `checkFilename()`.

While the `checkKeyword()` sub-check returns each individual match, the `checkFilename()` sub check accumulates the score of all matches and returns a single total score. It is possible that many different filename signatures have matched on that string but only one match with a total score is reported. This is an exception to the usual behavior where only the "FileScan" module accumulates scores.



## Filename IOC Matching in String Check Example

Imagine the following filename IOC signatures:

```
\\nmap.exe;70
\\bin\\nmap.exe;-30
```

and the following Keyword signature:

```
nmap.exe
```

The `checkString()` function receives the following string from the Eventlog scan module (here: a Sysmon Eventlog entry):

```
Process Create:
UtcTime: 20180110 10:22:25.277
ProcessGuid: {c1b49677e9615a5500000010bbc80702}
ProcessId: 3912
Image: C:\\Program Files\\Nmap\\bin\\nmap.exe
CommandLine: nmap.exe
CurrentDirectory: C:\\Windows\\system32\\
User: PROMETHEUS\\user1
LogonGuid: {c1b496771d725a5300000020d4232500}
LogonId: 0x2523d4
TerminalSessionId: 1
IntegrityLevel: High
Hashes: SHA1=F5DC12D658402900A2B01AF2F018D113619B96B8, MD5=9FEA051A9585F2A303D55745B4BF63AA
ParentProcessGuid: {c1b496771d745a530000001057452500}
ParentProcessId: 1036
ParentImage: C:\\Windows\\explorer.exe
ParentCommandLine: C:\\Windows\\Explorer.EXE
```

The `checkString()` function would create two messages: 1 "warning" for the keyword signature and 1 "notice" of the filename IOC signatures.

The keyword IOC matches in the `checkKeyword()` sub-check and `checkString()` returns a match, that generates a "Warning" level message that automatically receives a score of 75 (see [Default Scores](#)).

The filename IOCs would both match on the string in the `checkFilename()` sub-check and both scores would be summed up to a total score of 40 ( $70 + (-30) = 40$ ), which would generate a "Notice".

## 13.5 Action on Match

The action command allows you define a command that runs whenever THOR encounters a file during "Filescan" that has a certain total score or higher. The default score that triggers the action command (if set) is 40.

The most popular use case for the action command is sample collection.

### 13.5.1 Action Flags

| Parameter                      | Description                                                                                                                                                                       |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>--action_command string</b> | Run this command for each file that has a score greater than the score from --action_level                                                                                        |
| <b>--action_args strings</b>   | Arguments to pass to the command specified via --action_command. The placeholders %filename%, %filepath%, %file%, %ext%, %md5%, %score% and %date% are replaced at execution time |
| <b>--action_level int</b>      | Only run the command from --action_command for files with at least this score (default 40)                                                                                        |

### 13.5.2 Command Line Use

A typical use would be e.g. to copy a sample to a network share:

```
C:\Users\nextron>copy %filepath% \\server\share1
```

To instruct THOR to run this command, you need

```
C:\nextron\thor>thor64.exe --action_command copy --action_args %filepath% --action_args \
↪\server\share1
```

### 13.5.3 Use in a Config File

The ./config folder contains a template for a config file that uses the action commands.

Content of 'tmpl-action.yml':

```

1 # Action to perform if file has been detected with a score more than the defined 'action_
 ↪level'
2 # You may use all environment variables that are available on the system, i.e.
 ↪%COMPUTERNAME%.
3 # Further available meta vars are:
4 # %score% = Score
5 # %file% = Filename without extension
6 # %filename% = Basename
7 # %filepath% = Full path
8 # %ext% = Extension without dot
9 # %md5% = MD5 value
10 # %date% = Detection time stamp
11
12 action_level: 35
13 action_command: "copy"
14 action_args:
15 - "%filepath%"
16 - "\\VBOXSVR\Downloads\restore_files\%COMPUTERNAME%\%md5%\%file%\%ext%\%date%"

```

## 13.6 THOR DB

This simple SQLite database is created by default in the "%ProgramData%\thor" (Linux, macOS: /var/lib/thor/) directory as "thor10.db". You can deactivate THOR DB and all its features by using the `--nothordb` flag.

It stores persistent information over several scan runs:

- Scan State Information
  - This information is used to resume scan runs where they were stopped
- Delta Comparison
  - This detection feature allows to compare the result of a former module check with the current results and indicate suspicious changes between scan runs

The THOR DB related command line options are:

| Parameter                      | Description                                                                                                                                                                                                                     |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>--nothordb</code>        | Disables THOR DB completely. All related features will be disabled as well.                                                                                                                                                     |
| <code>--dbfile [string]</code> | Allows to define a location of the THOR database file. File names or path names are allowed. If a path is given, the database file <code>thor10.db</code> will be created in the directory. Environment variables are expanded. |
| <code>--resume</code>          | Resumes a previous scan (if scan state information is still available and the exact same command line arguments are used)                                                                                                       |
| <code>--resumeonly</code>      | Only resume a scan if a scan state is available. Do not run a full scan if no scan state can be found.                                                                                                                          |

### 13.6.1 Resume a Scan

THOR tries to resume a scan when you set the `--resume` parameter. Since THOR version 10.5 the resume state doesn't get tracked by default due to its significant performance implications. If you want to be able to resume a scan, you have to start scans with the `--resume` flag. If you start a scan and a previous resume state is present, then THOR is going to resume the interrupted scan.

It will only resume the previous scan if

1. You have started the scan with `--resume`
2. The argument list is exactly the same as in the first scan attempt
3. You haven't used the flag `--nothordb`
4. Scan state information is still available (could have been cleared by running THOR a second time without the `--resume` parameter)

You can always clear the resume state and discard an old state by running `thor.exe` once without using the `--resume` parameter.

### 13.6.2 Delta Comparison

The delta comparison feature allows comparing former scan results on a system with the current results, indicating changes in system configurations and system components.

Currently, the following scan modules feature the delta comparison check:

- Autoruns
  - THOR compares the output of the Autoruns module with the output of the last scan run. The Autoruns module does not only check "Autorun" locations but also elements like browser plugins, drivers, LSA providers, WMI objects and scheduled tasks.
- Services
  - The comparison detects new service entries and reports them.
- Hosts
  - New or changed entries in the "hosts" file could indicate system manipulations by attackers to block certain security functions or intercept connections.

## 13.7 Archive Scan

The Archive Scan feature supports the following archive types:

- ZIP
- RAR
- TAR
- TAR + GZIP (.tar.gz)
- TAR + BZIP2 (.tar.bz2)
- GZIP (THOR 10.7+)
- 7ZIP (THOR 10.7+)
- CAB (THOR 10.7+)

When scanning a file within any of these file types, THOR will append the path within the archive to the archive's own path for scan purposes (like filename IOCs or YARA rules). For example, an archive `C:\temp\test.zip` containing a file `path/in/zip.txt` will cause the simulated path to be `C:\temp\test.zip\path\in\zip.txt`.

## COMMAND LINE OPTIONS

This section lists all options that THOR TechPreview currently offers.

### 14.1 Scan Options

|                                |                                                                                                                                                                                                                                                                                                             |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>-t, --template string</b>   | Process default scan parameters from this YAML file                                                                                                                                                                                                                                                         |
| <b>--generate-config</b>       | Print a YAML config from the given parameters and exit                                                                                                                                                                                                                                                      |
| <b>-p, --path strings</b>      | Scan a specific file path. Define multiple paths by specifying this option multiple times. Append ':NOWALK' to the path for non-recursive scanning (default: only the system drive)                                                                                                                         |
| <b>--allhds</b>                | (Windows Only) Scan all local hard drives (default: only the system drive)                                                                                                                                                                                                                                  |
| <b>--alldrives</b>             | Scan all local drives, including network drives (default: only the system drive). Requires a Forensic Lab license.                                                                                                                                                                                          |
| <b>--max_file_size uint</b>    | Max. file size to check (larger files are ignored). Increasing this limit will also increase memory usage of THOR.                                                                                                                                                                                          |
| <b>--max_log_lines int</b>     | Maximum amount of lines to check in a log file before skipping the remaining lines                                                                                                                                                                                                                          |
| <b>--max_process_size uint</b> | Max process size to check (larger processes won't be scanned)                                                                                                                                                                                                                                               |
| <b>--max_runtime int</b>       | Maximum runtime in hours. THOR will stop once this time has run out. 0 means no maximum runtime.                                                                                                                                                                                                            |
| <b>--nodoublecheck</b>         | Don't check whether another THOR instance is running (e.g. in Lab use cases when several mounted images are scanned simultaneously on a single system) (requires a Forensic Lab license)                                                                                                                    |
| <b>-f, --epoch strings</b>     | <p>Specify a range of days with attacker activity as start and end date pairs.</p> <p>Files created/modified between these days (including the specified start, excluding the specified end) will receive an extra score.</p> <p>Example: -f 2009-10-09 -f 2009-10-10 marks the 09.10.2009 as relevant.</p> |
| <b>--epochscore int</b>        | Score to add for files that were created/modified on days with attacker activity (see --epoch parameter)                                                                                                                                                                                                    |
| <b>--insecure</b>              | Skip TLS host verification (insecure)                                                                                                                                                                                                                                                                       |

|                                   |                                                                                                  |
|-----------------------------------|--------------------------------------------------------------------------------------------------|
| <b>--ca strings</b>               | Root CA for host certificate verification during TLS handshakes                                  |
| <b>--cross-platform</b>           | Apply IOCs with path separators platform independently.                                          |
| <b>--require-admin</b>            | Terminate immediately if THOR is executed without administrator rights.                          |
| <b>--follow-symlinks</b>          | When encountering a symlink during the file scan that points to a directory, scan the directory. |
| <b>--max-recursion-depth uint</b> | Maximum depth of archives to scan                                                                |
| <b>--max-nested-objects uint</b>  | Maximum number of files per archive to scan                                                      |

## 14.2 Scan Modes

|                                   |                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>--quick</b>                    | <p>Activate a number of flags to speed up the scan at cost of some detection.</p> <p>This is equivalent to: <code>--noeventlog --nofirewall --nopfiles --nologscan --noevtx --nohotfixes --nomft --lookback 3 --lookback-modules filescan</code></p>                                                                                                                              |
| <b>--soft</b>                     | <p>Skip CPU and RAM intensive modules (Mutexes, Firewall, Logons, Network sessions and shares, LSA sessions, open files, hosts file), don't decompress executables and doesn't perform a DoublePulsar backdoor check, lower max CPU usage to 70% and set low priority for THOR.</p> <p>This mode activates automatically on systems with 1 CPU core or less than 1024 MB RAM.</p> |
| <b>--intense</b>                  | <p>Paranoid scan mode that disables all safe guards. Only use this mode in lab scanning scenarios. We don't recommend using this mode to live scan productive systems. (enables: memory intensive extra modules)</p>                                                                                                                                                              |
| <b>--diff</b>                     | <p>Set lookback time (see <code>--lookback</code>) for each module to the last time the module ran successfully and activates <code>--global-lookback</code>.</p> <p>Effectively, this means that only elements that changed since the last scan are examined. (only works if ThorDB has been active)</p>                                                                         |
| <b>--lookback int</b>             | <p>Specify how many past days shall be analyzed. Event log entries from before this point will be ignored. 0 means no limit</p>                                                                                                                                                                                                                                                   |
| <b>--global-lookback</b>          | <p>Apply Lookback to all modules that support it (not only Eventlog). See also <code>--lookback</code> and <code>--lookback-modules</code>.</p> <p>Warning: Timestomping or similar methods of antivirus evasion may result in elements not being examined.</p>                                                                                                                   |
| <b>--force-aptdir-lookback</b>    | <p>Enforce lookback application on all files in the FileScan module. By default, especially endangered directories ignore the lookback value.</p>                                                                                                                                                                                                                                 |
| <b>--lookback-modules strings</b> | <p>Apply Lookback to the given modules. See also <code>--lookback</code> and <code>--modules</code>.</p> <p>Warning: Timestomping or similar methods of antivirus evasion may result in elements not being examined.</p>                                                                                                                                                          |

|                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>--lab</b>                 | <p>Lab scan mode - scan only the file system, disable resource checks and quick mode, activate intense mode, disable ThorDB, apply IOCs platform independently and use all CPU cores.</p> <p>This option scans all drives by default, but is often used with -p to scan only a single path. Requires a Forensic Lab license.</p>                                                                                                                                                                                           |
| <b>--virtual-map strings</b> | <p>Rewrite found file paths to use a different prefix.</p> <p>This can be useful for mounted images, where the current location of files does not match the original location and therefore references might be out of date.</p> <p>Specify the original and current path as --virtual-map path/to/current/location:path/to/original/location.</p> <p>On Windows, drive names are also supported, e.g. specify --virtual-map F:C if the drive on F: was originally used as C:.</p> <p>Requires a Forensic Lab license.</p> |

## 14.3 Resource Options

|                              |                                                                                                                                                                  |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>-c, --cpulimit float</b>  | Limit CPU usage of THOR to this level (in percent). Minimum is 15%                                                                                               |
| <b>--nocpulimit</b>          | Disable cpulimit check                                                                                                                                           |
| <b>--nosoft</b>              | Disable automatic activation of soft mode (see --soft)                                                                                                           |
| <b>--norescontrol</b>        | Do not check whether the system is running out of resources. Use this option to enforce scans that have been canceled due to resource scarcity. (use with care!) |
| <b>--minmem uint</b>         | Cancel the running scan if the amount of free physical memory drops below this value (in MB)                                                                     |
| <b>--lowprio</b>             | Reduce the priority of the THOR process to a lower level                                                                                                         |
| <b>--verylowprio</b>         | Reduce the priority of the THOR process to a very low level                                                                                                      |
| <b>--lowioprio</b>           | Reduce the disk priority of the THOR process to a lower level                                                                                                    |
| <b>--nolowprio</b>           | Do not reduce the priority of the THOR process to a lower level due to soft mode (see --soft)                                                                    |
| <b>--nolockthread</b>        | Do not lock calls to C libraries to main thread (this may increase performance at the cost of memory usage)                                                      |
| <b>--yara-stack-size int</b> | Allocate this number of slots for the YARA stack. Default: 16384. Increasing this limit will allow you to use larger rules, albeit with more memory overhead.    |
| <b>--yara-timeout int</b>    | Cancel any YARA checks that take longer this amount of time (in seconds)                                                                                         |
| <b>--threads uint16</b>      | Run this amount of THOR threads in parallel. Requires a Forensic Lab license.                                                                                    |
| <b>--bulk-size uint</b>      | Check this amount of elements together, e.g. log lines or registry entries                                                                                       |

## 14.4 Special Scan Modes

- m, --image\_file string** Scan only the given single memory image / dump file (don't use for disk images, scan them mounted with --lab). Requires a Forensic Lab license.
- image-chunk-size uint** Scan image / dump files in chunks of this size
- r, --restore\_directory string** Restore PE files with YARA rule matches during the Deep-Dive into the given folder
- restore\_score int** Restore only chunks with a total match score higher than the given value
- dropzone** Watch and scan all files dropped to a certain directory (which must be passed with -p). Disable resource checks and quick mode, activate intense mode, disable ThorDB and apply IOCs platform independently. Requires a Forensic Lab license.
- dropdelete** Delete all files dropped to the drop zone after the scan.

## 14.5 Thor Thunderstorm Service

- thunderstorm** Watch and scan all files sent to a specific port (see --server-port). Disable resource checks and quick mode, activate intense mode, disable ThorDB and apply IOCs platform independently.
- server-upload-dir string** Path to a directory where THOR drops uploaded files.  
If this path does not exist, THOR tries to create it.
- server-host string** IP address that THOR's server should bind to.
- server-port uint16** TCP port that THOR's server should bind to.
- server-cert string** TLS certificate that THOR's server should use. If left empty, TLS is not used.
- server-key string** Private key for the TLS certificate that THOR's server should use. Required if --server-cert is specified.
- server-store-samples string** Sets whether samples should be stored permanently in the folder specified with --server-upload-dir.  
Specify "all" to store all samples, or "malicious" to store only samples that generated a warning or an alert.
- server-result-cache-size uint32** Size of the cache that is used to store results of asynchronous requests temporarily.  
If set to 0, the cache is disabled and asynchronous results are not stored.
- pure-yara** Only scan files using YARA signatures (disables all programmatic checks, STIX, Sigma, IOCs, as well as most features and modules)
- sync-only-threads uint16** Reserve this amount of THOR threads for synchronous requests
- force-max-file-size** Enforce the maximum file size even on files like registry hives or log files which are usually scanned despite size.



## 14.6 License Retrieval

- asgard string**      Hostname of the ASGARD server from which a license should be requested, e.g. asgard.my-company.internal
- asgard-token string**      Use this token to authenticate with the License API of the asgard server. The token can be found in the 'Downloads' or 'Licensing' section in the ASGARD. This requires ASGARD 2.5+.
- q, --license-path string**      Path containing the THOR license
- portal-key string**      Get a license for this host from portal.nexttron-systems.com using this API Key.  
  
This feature is only supported for host-based server / workstation contracts.
- portal-contracts ints**      Use these contracts for license generation. If no contract is specified, the portal selects a contract by itself. See --portal-key.
- portal-nonewlic**      Only use an existing license from the portal. If none exists, exit. See --portal-key.

## 14.7 Active Modules

- a, --module strings**      Activate the following modules only (Specify multiple modules with -a Module1 -a Module2 ... -a ModuleN).
- noprocs**      Do not analyze Processes
- nofilesystem**      Do not scan the file system
- noreg**      Do not analyze the registry
- nousers**      Do not analyze user accounts
- nologons**      Do not show currently logged in users
- noautoruns**      Do not analyse autorun elements
- noeventlog**      Do not analyse the eventlog
- norootkits**      Do not check for rootkits
- noevents**      Do not check for malicious events
- nodnscache**      Do not analyze the local DNS cache
- noenv**      Do not analyze environment variables
- nohosts**      Do not analyze the hosts file
- nomutex**      Do not check for malicious mutexes
- notasks**      Do not analyse scheduled tasks
- noservices**      Do not analyze services
- noprofiles**      Do not analyze profile directories
- noatjobs**      Do not analyze jobs scheduled with the 'at' tool
- nonetworksessions**      Do not analyze network sessions

|                           |                                                                      |
|---------------------------|----------------------------------------------------------------------|
| <b>--nonetworkshares</b>  | Do not analyze network shares                                        |
| <b>--noshimcache</b>      | Do not analyze SHIM Cache entries                                    |
| <b>--nohotfixes</b>       | Do not analyze Hotfixes                                              |
| <b>--nowmistartup</b>     | Do not analyze startup elements using WMI                            |
| <b>--nofirewall</b>       | Do not analyze the local Firewall                                    |
| <b>--nowmi</b>            | Disable all checks with WMI functions                                |
| <b>--nolsasessions</b>    | Do not analyze lsa sessions                                          |
| <b>--nomft</b>            | Do not analyze the drive's MFT (default, unless in intense mode)     |
| <b>--mft</b>              | Analyze the drive's MFT                                              |
| <b>--nopipes</b>          | Do not analyze named pipes                                           |
| <b>--noetwwatcher</b>     | Do not analyze ETW logs during THOR runtime                          |
| <b>--nointegritycheck</b> | Do not check with the package manager for package integrity on Linux |
| <b>--notimestamp</b>      | Disable timestamping detection                                       |

## 14.8 Module Extras

|                                      |                                                                                                                                               |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>--process ints</b>                | Process IDs to be scanned. Define multiple processes by specifying this option multiple times (default: all processes) (Module: ProcessCheck) |
| <b>--dump-procs</b>                  | Generate process dumps for suspicious or malicious processes (Module: ProcessCheck)                                                           |
| <b>--max-procdumps uint</b>          | Create at most this many process dumps (Module: ProcessCheck)                                                                                 |
| <b>--procdump-dir string</b>         | Store process dumps of suspicious processes in this directory (Module: ProcessCheck)                                                          |
| <b>-n, --eventlog-target strings</b> | Scan specific Eventlogs (e.g. 'Security' or 'Microsoft-Windows-Sysmon/Operational') (Module: Eventlog)                                        |
| <b>--nodoublepulsar</b>              | Do not check for DoublePulsar Backdoor (Module: Rootkit)                                                                                      |
| <b>--full-registry</b>               | Do not skip registry hives keys with less relevance (Module: Registry)                                                                        |
| <b>--noregwalk</b>                   | Do not scan the whole registry during the registry scan                                                                                       |
| <b>--showdeleted</b>                 | Show deleted files found in the MFT as 'info' messages.                                                                                       |
| <b>--allfiles</b>                    | Scan all files, even ones that are usually not interesting. Sets --max_file_size to 200MB unless specified otherwise.                         |
| <b>--ads</b>                         | Scan Alternate Data Streams for all files                                                                                                     |

## 14.9 Active Features

|                               |                                                                                                                                               |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>--nothordb</b>             | Do not use or create ThorDB database for holding scan information                                                                             |
| <b>--nosigma</b>              | Disable Sigma signatures                                                                                                                      |
| <b>--dumpscan</b>             | Scan memory dumps                                                                                                                             |
| <b>--nologscan</b>            | Do not scan log files (identified by .log extension or location)                                                                              |
| <b>--noyara</b>               | Disable checks with YARA                                                                                                                      |
| <b>--nostix</b>               | Disable checks with STIX                                                                                                                      |
| <b>--noarchive</b>            | Do not scan contents of archives                                                                                                              |
| <b>--noc2</b>                 | Disable checks for known C2 Domains                                                                                                           |
| <b>--noprochandles</b>        | Do not analyze process handles                                                                                                                |
| <b>--noproconnections</b>     | Do not analyze process connections                                                                                                            |
| <b>--noamcache</b>            | Do not analyze Amcache files                                                                                                                  |
| <b>--noregistryhive</b>       | Do not analyze Registry Hive files                                                                                                            |
| <b>--noexedecompress</b>      | Do not decompress and scan portable executables                                                                                               |
| <b>--nowebdirscan</b>         | Do not analyze web directories that were found in process handles                                                                             |
| <b>--novulnerabilitycheck</b> | Do not analyze system for vulnerabilities                                                                                                     |
| <b>--noprefetch</b>           | Do not analyze prefetch directory                                                                                                             |
| <b>--nogroupsxml</b>          | Do not analyze groups.xml                                                                                                                     |
| <b>--nowmipersistence</b>     | Do not check WMI Persistence                                                                                                                  |
| <b>--nolnk</b>                | Do not analyze LNK files                                                                                                                      |
| <b>--noknowledgedb</b>        | Do not check Knowledge DB on Mac OS                                                                                                           |
| <b>--nower</b>                | Do not analyze .wer files                                                                                                                     |
| <b>--noevtx</b>               | Do not analyze EVTX files                                                                                                                     |
| <b>--noauthorizedkeys</b>     | Do not analyze authorized_keys files                                                                                                          |
| <b>--noimphash</b>            | Do not calculate imphash for suspicious EXE files (Windows only)                                                                              |
| <b>--c2-in-memory</b>         | Apply C2 IOCs on process memory (not recommended unless you are willing to accept many false positives on browser and other process memories) |
| <b>--custom-c2-in-memory</b>  | Apply custom C2 IOCs on process memory                                                                                                        |
| <b>--noeml</b>                | Disable Email parser                                                                                                                          |
| <b>--noetl</b>                | Disable ETL parser                                                                                                                            |

## 14.10 Feature Extras

|                              |                                                                                                                                                             |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>--customonly</b>          | Use custom signatures only (disables all internal THOR signatures and detections)                                                                           |
| <b>--full-proc-integrity</b> | Increase sensitivity of --processintegrity for process impersonation detection. Likely to cause false positives, but also better at detecting real threats. |
| <b>--processintegrity</b>    | Run PE-Sieve to check for process integrity (Windows only)                                                                                                  |

## 14.11 Output Options

|                                        |                                                                                                                                         |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| <b>-l, --logfile string</b>            | Log file for text output                                                                                                                |
| <b>--htmlfile string</b>               | Log file for HTML output                                                                                                                |
| <b>--nolog</b>                         | Do not generate text or HTML log files                                                                                                  |
| <b>--nohtml</b>                        | Do not create an HTML report file                                                                                                       |
| <b>--appendlog</b>                     | Append text log to existing log instead of overwriting                                                                                  |
| <b>--keyval</b>                        | Format text and HTML log files with key value pairs to simplify the field extraction in SIEM systems (key='value')                      |
| <b>--jsonfile string</b>               | Log file for JSON output. If no value is specified, defaults to :hostname:_thor_:time:.json.                                            |
| <b>-o, --csvfile string</b>            | Generate a CSV containing MD5,Filepath,Score for all files with at least the minimum score                                              |
| <b>--nocsv</b>                         | Do not write a CSV of all mentioned files with MD5 hash (see --csvfile)                                                                 |
| <b>--stats-file string</b>             | Generate a CSV file containing the scan summary in a single line. If no value is specified, defaults to :hostname:_stats.csv.           |
| <b>-e, --rebase-dir string</b>         | Specify the output directory where all output files will be written. Defaults to the current working directory.                         |
| <b>--suppresspi</b>                    | Suppress all personal information in log outputs to comply with local data protection policies                                          |
| <b>--eventlog</b>                      | Log to windows application eventlog                                                                                                     |
| <b>-x, --min int</b>                   | Only report files with at least this score                                                                                              |
| <b>--allreasons</b>                    | Show all reasons why a match is considered dangerous (default: only the top 2 reasons are displayed)                                    |
| <b>--printshim</b>                     | Include all SHIM cache entries in the output as 'info' level messages                                                                   |
| <b>--printamcache</b>                  | Include all AmCache entries in the output as 'info' level messages                                                                      |
| <b>-j, --overwrite-hostname string</b> | Override the local hostname value with a static value (useful when scanning mounted images in the lab. Requires a Forensic Lab license. |
| <b>-i, --scanid string</b>             | Specify a scan identifier (useful to filter on the scan ID, should be unique)                                                           |

---

|                                   |                                                                                                                                                                          |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>--scanid-prefix string</b>     | Specify a prefix for the scan ID that is concatenated with a random ID if neither <b>--scanid</b> nor <b>--noscanid</b> are specified                                    |
| <b>--noscanid</b>                 | Do not automatically generate a scan identifier if none is specified                                                                                                     |
| <b>--silent</b>                   | Do not print anything to command line                                                                                                                                    |
| <b>--cmdjson</b>                  | Format command line output as JSON                                                                                                                                       |
| <b>--cmdkeyval</b>                | Use key-value pairs for command line output, see <b>--keyval</b>                                                                                                         |
| <b>--encrypt</b>                  | Encrypt the generated log files and the MD5 csv file                                                                                                                     |
| <b>--pubkey string</b>            | Use this RSA public key to encrypt the logfile and csvfile (see <b>--encrypt</b> ). Both <b>--pubkey="&lt;key&gt;"</b> and <b>--pubkey="&lt;file&gt;"</b> are supported. |
| <b>--nocolor</b>                  | Do not use ANSI escape sequences for colorized command line output                                                                                                       |
| <b>--genid</b>                    | Print a unique ID for each log message. Identical log messages will have the same ID.                                                                                    |
| <b>--print-rescontrol</b>         | Print THOR's resource threshold and usage when it is checked                                                                                                             |
| <b>--truncate int</b>             | Max. length per THOR value (0 = no truncation)                                                                                                                           |
| <b>--registry_depth_print int</b> | Don't print info messages when traversing registry keys at a higher depth than this                                                                                      |
| <b>--utc</b>                      | Print timestamps in UTC instead of local time zone                                                                                                                       |
| <b>--rfc3339</b>                  | Print timestamps in RFC3339 (YYYY-MM-DD'T'HH:mm:ss'Z') format                                                                                                            |
| <b>--reduced</b>                  | Reduced output mode - only warnings, alerts and errors will be printed                                                                                                   |
| <b>--printlicenses</b>            | Print all licenses to command line (default: only 10 licenses will be printed)                                                                                           |
| <b>--local-syslog</b>             | Print THOR events to local syslog                                                                                                                                        |
| <b>--showall</b>                  | Print rule matches even if that rule already matched more than 10 times.                                                                                                 |
| <b>--ascii</b>                    | Don't print non-ASCII characters to command line and log files                                                                                                           |
| <b>--string-context uint</b>      | When printing strings from YARA matches, include this many bytes surrounding the match                                                                                   |
| <b>--include-info-in-html</b>     | Include info messages in the HTML report                                                                                                                                 |
| <b>--audit-trail string</b>       | Output file for audit trail                                                                                                                                              |
| <b>--background string</b>        | Optimize font colors for given terminal background (options: default, light, dark)                                                                                       |

## 14.12 ThorDB

|                        |                                                                                                                                                               |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>--dbfile string</b> | Location of the thor.db file                                                                                                                                  |
| <b>--resumeonly</b>    | Don't start a new scan, only finish an interrupted one. If no interrupted scan exists, nothing is done.                                                       |
| <b>--resume</b>        | Store information while running that allows to resume an interrupted scan later. If a previous scan was interrupted, resume it instead of starting a new one. |

## 14.13 Syslog

|                              |                                                                                                                                                                                                                                                                                                                                               |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>-s, --syslog strings</b>  | Write output to the specified syslog server, format: server[:port[:syslogtype[:sockettype]]].<br><br>Supported syslog types: DEFAULT/CEF/JSON/SYSLOGJSON/SYSLOGKV<br><br>Supported socket types: UDP/TCP/TCPTLS<br><br>Examples: -s syslog1.dom.net, -s arcsight.dom.net:514:CEF:UDP, -s syslog2:4514:DEFAULT:TCP, -s syslog3:514:JSON:TCPTLS |
| <b>--rfc3164</b>             | Truncate long Syslog messages to 1024 bytes                                                                                                                                                                                                                                                                                                   |
| <b>--rfc5424</b>             | Truncate long Syslog messages to 2048 bytes                                                                                                                                                                                                                                                                                                   |
| <b>--rfc</b>                 | Use strict syslog according to RFC 3164 (simple host name, shortened message)                                                                                                                                                                                                                                                                 |
| <b>--maxsysloglength int</b> | Truncate Syslog messages to the given length (0 means no truncation)                                                                                                                                                                                                                                                                          |
| <b>--cef_level int</b>       | Define the minimum severity level to log to CEF syslogs (Debug=1, Info=3, Notice=4, Error=5, Warning=8, Alarm=10)                                                                                                                                                                                                                             |

## 14.14 Reporting and Actions

|                                |                                                                                                                                                                                           |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>--notice int</b>            | Minimum score on which a notice is generated                                                                                                                                              |
| <b>--warning int</b>           | Minimum score on which a warning is generated                                                                                                                                             |
| <b>--alert int</b>             | Minimum score on which an alert is generated                                                                                                                                              |
| <b>--action_command string</b> | Run this command for each file that has a score greater than the score from --action_level.                                                                                               |
| <b>--action_args strings</b>   | Arguments to pass to the command specified via --action_command.<br><br>The placeholders %filename%, %filepath%, %file%, %ext%, %md5%, %score% and %date% are replaced at execution time. |
| <b>--action_level int</b>      | Only run the command from --action_command for files with at least this score.                                                                                                            |
| <b>--nofserrors</b>            | Silently ignore filesystem errors                                                                                                                                                         |

## 14.15 THOR Remote

|                                 |                                                                                       |
|---------------------------------|---------------------------------------------------------------------------------------|
| <b>--remote strings</b>         | Target host (use multiple <b>--remote &lt;host&gt;</b> statements for a set of hosts) |
| <b>--remote-user string</b>     | Username (if not specified, windows integrated authentication is used)                |
| <b>--remote-password string</b> | Password to be used to authenticate against remote hosts                              |
| <b>--remote-prompt</b>          | Prompt for password for remote hosts                                                  |
| <b>--remote-debug</b>           | Debug Mode for THOR Remote                                                            |
| <b>--remote-dir string</b>      | Upload THOR to this remote directory                                                  |
| <b>--remote-workers int</b>     | Number of concurrent scans                                                            |
| <b>--remote-rate int</b>        | Number of seconds to wait between scan starts                                         |

## 14.16 Automatic Collection of Suspicious Files (Bifrost)

|                                |                                                                                                                                                                          |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>--bifrost2Server string</b> | Server running the Bifrost 2 quarantine service. THOR will upload all suspicious files to this server.<br><br>This flag is only usable when invoking THOR from ASGARD 2. |
| <b>--bifrost2Score int</b>     | Send all files with at least this score to the Bifrost 2 quarantine service.<br><br>This flag is only usable when invoking THOR from ASGARD 2.                           |

## 14.17 VirusTotal Integration

|                         |                                                                                                                                                                                    |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>--vtkey string</b>   | Virustotal API key for hash / sample uploads                                                                                                                                       |
| <b>--vtmode string</b>  | VirusTotal lookup mode (limited = hash lookups only, full = hash and sample uploads)                                                                                               |
| <b>--vtscore int</b>    | Minimum score for hash lookup / sample upload to VirusTotal                                                                                                                        |
| <b>--vtaccepteula</b>   | By specifying this option, you accept VirusTotal's EULA: <a href="https://www.virustotal.com/en/about/terms-of-service/">https://www.virustotal.com/en/about/terms-of-service/</a> |
| <b>--vtwaitforquota</b> | Wait if the VirusTotal API key quota is exceeded                                                                                                                                   |
| <b>--vtverbose</b>      | Show more information from VirusTotal                                                                                                                                              |

## 14.18 Debugging and Info

|                           |                                                     |
|---------------------------|-----------------------------------------------------|
| <b>--debug</b>            | Show Debugging Output                               |
| <b>--trace</b>            | Show Tracing Output                                 |
| <b>--printall</b>         | Print all files that are checked (noisy)            |
| <b>--print-signatures</b> | Show THOR Signatures and IOCs and exit              |
| <b>--version</b>          | Show THOR, signature and software versions and exit |
| <b>-h, --help</b>         | Show help for most important options and exit       |
| <b>--fullhelp</b>         | Show help for all options and exit                  |



## DEBUGGING

Most unexpected behavior can be debugged by using the parameter `--debug`.

If you ever encounter a situation in which:

- THOR doesn't produce an alert on a known malicious element
- THOR exits with an error
- THOR takes a long time or unexpected short time on elements

### 15.1 Collecting a Diagnostics Pack

THOR Util comes with the functionality to collect a diagnostics pack for THOR scans. This is helpful if a scan is taking more time as expected or if THOR exits unexpectedly. More details can be found in the [diagnostics](#) section of [THOR Util](#).

### 15.2 Debugging Examples

If you found the culprit for your problematic scan, try scanning that specific element with the `--debug` parameter set.

To run a scan only with certain modules only use the `--module` (short hand `-a`) command line switch (see [Scan Module Names](#) for a full list of module names):

```
C:\nexttron\thor>thor64.exe -a Mutex
C:\nexttron\thor>thor64.exe -a FileScan
C:\nexttron\thor>thor64.exe -a Eventlog
```

---

**Hint:** You can specify multiple modules:

```
C:\nexttron\thor>thor64.exe -a Mutex -a EnvCheck -a Users
```

---

You can try to reduce the scope of a module even further by using lookbacks

```
C:\nexttron\thor>thor64.exe -a Eventlog --lookback 3
C:\nexttron\thor>thor64.exe -a FileScan -p C:\Windows\System32 --globallookback --
↳lookback 1
```

To find out why a certain file couldn't be detected, use `--debug` with `--printall` and try to switch into `--intense` mode.

```
C:\nextron\thor>thor64.exe -a Filescan -p C:\testfolder --debug --printall
C:\nextron\thor>thor64.exe -a Filescan -p C:\testfolder --debug --printall --intense
```

If it has been detected in `--intense` mode but not in default mode, the file extension or the magic header is most likely the problem. You can adjust `max_file_size` in `./config/thor.yml` or add a magic header in `./signatures/misc/file-type-signatures.cfg`.

## 15.3 Finding Bottlenecks

You may get the error message `MODULE: RuntimeWatcher MESSAGE: Maximum runtime has exceeded, killing THOR` or encounter very slow/never-ending scans.

You can check the statistics table in `thor10.db` on the problematic endpoint after a scan to determine the last element or elements that took a long time to process.

We recommend using: <https://sqlitebrowser.org/>

The THOR DB is located at: `C:\ProgramData\thor\thor10.db`.

DB Browser for SQLite - C:\ProgramData\thor\thor10.db

File Edit View Tools Help

New Database Open Database Write Changes Revert Changes Open Project Save Project Attach Database Close Database

Database Structure Browse Data Edit Pragma Execute SQL

Table: stats

|    | module         | element                                         | started                           | duration |
|----|----------------|-------------------------------------------------|-----------------------------------|----------|
| 1  | RegistryChecks | SOFTWARE\Classes\WorkspaceRuntime.Workspace.1   | 2020-04-09 11:46:32.732851+00:00  | 0        |
| 2  | RegistryChecks | SOFTWARE\Classes\WorkspaceRuntime.Workspace     | 2020-04-09 11:46:32.7284332+00:00 | 0        |
| 3  | RegistryChecks | SOFTWARE\Classes\WorkspaceBrokerAx.Workspace... | 2020-04-09 11:46:32.7231963+00:00 | 0        |
| 4  | RegistryChecks | SOFTWARE\Classes\WorkspaceBrokerAx.Workspace... | 2020-04-09 11:46:32.7184094+00:00 | 0        |
| 5  | RegistryChecks | SOFTWARE\Classes\WorkspaceBroker.WorkspaceB...  | 2020-04-09 11:46:32.7129112+00:00 | 0        |
| 6  | RegistryChecks | SOFTWARE\Classes\WorkspaceBroker.WorkspaceB...  | 2020-04-09 11:46:32.7078139+00:00 | 0        |
| 7  | RegistryChecks | SOFTWARE\Classes\Workspace.ResTypeRegistry.1    | 2020-04-09 11:46:32.7035492+00:00 | 0        |
| 8  | RegistryChecks | SOFTWARE\Classes\Workspace.ResTypeRegistry      | 2020-04-09 11:46:32.6995246+00:00 | 0        |
| 9  | RegistryChecks | SOFTWARE\Classes\Workspace.PolicyProcessor.1    | 2020-04-09 11:46:32.6948404+00:00 | 0        |
| 10 | RegistryChecks | SOFTWARE\Classes\Workspace.PolicyProcessor      | 2020-04-09 11:46:32.6902687+00:00 | 0        |
| 11 | RegistryChecks | SOFTWARE\Classes\Workspace.Installer.1          | 2020-04-09 11:46:32.6847406+00:00 | 0        |
| 12 | RegistryChecks | SOFTWARE\Classes\Workspace.Installer            | 2020-04-09 11:46:32.6804795+00:00 | 0        |
| 13 | RegistryChecks | SOFTWARE\Classes\Wordpad.Document.1             | 2020-04-09 11:46:32.6754806+00:00 | 0        |
| 14 | RegistryChecks | SOFTWARE\Classes\WordAddin_RD.WordAddinRD.1     | 2020-04-09 11:46:32.6603448+00:00 | 0        |
| 15 | RegistryChecks | SOFTWARE\Classes\WordAddin_RD.WordAddinRD       | 2020-04-09 11:46:32.3211086+00:00 | 0        |
| 16 | RegistryChecks | SOFTWARE\Classes\WMVFile                        | 2020-04-09 11:46:32.3182644+00:00 | 0        |
| 17 | RegistryChecks | SOFTWARE\Classes\WMSDKNamespace.Namespac...     | 2020-04-09 11:46:32.3120948+00:00 | 0        |
| 18 | RegistryChecks | SOFTWARE\Classes\WMSDKNamespace.Namespac...     | 2020-04-09 11:46:32.3079582+00:00 | 0        |
| 19 | RegistryChecks | SOFTWARE\Classes\WMSDKMSBSourcePlugin.MSB...    | 2020-04-09 11:46:32.302025+00:00  | 0        |
| 20 | RegistryChecks | SOFTWARE\Classes\WMSDKMSBSourcePlugin.MSB...    | 2020-04-09 11:46:32.2981605+00:00 | 0        |
| 21 | RegistryChecks | SOFTWARE\Classes\WMSDKHTTPSourcePlugin.HT...    | 2020-04-09 11:46:32.2941111+00:00 | 0        |
| 22 | RegistryChecks | SOFTWARE\Classes\WMSDKHTTPSourcePlugin.HT...    | 2020-04-09 11:46:32.2892924+00:00 | 0        |
| 23 | RegistryChecks | SOFTWARE\Classes\WMSClientNetManager.ClientN... | 2020-04-09 11:46:32.2843999+00:00 | 0        |
| 24 | RegistryChecks | SOFTWARE\Classes\WMSClientNetManager.ClientN... | 2020-04-09 11:46:32.2793848+00:00 | 0        |

Edit Database Cell

Mode: Text

3712

Type of data currently in cell: Text / Numeric  
4 char(s)

Remote

Identity

Name Commit L

## 15.4 Most Frequent Causes of Missing Alerts

Below you can find the most frequent causes of missing alerts.

### 15.4.1 THOR didn't scan file due to file size restrictions

**Solution:** Use the `--max_file_size` parameter or set it permanently in the config file `./config/thor.yml`.

```
C:\nexttron\thor>thor64.exe --max_file_size 206233600 # setting max file size to 100 MB
```

Listing 1: Default thor.yml

```

1 # This is the default config for THOR
2 # Skip files bigger than 31457280 bytes
3 max_file_size: 31457280
4 # Skip files bigger than 209715200 bytes in intense mode (--lab, --intense)
5 max_file_size_intense: 209715200
6 # Terminate THOR if he runs longer than 168 hours
7 max_runtime: 168
8 # Limit THOR's CPU usage to 95%
9 cpulimit: 95
10 # The minimum amount of free physical memory to proceed (in MB)
11 minmem: 50
12 # Minimum score to report is 40
13 min: 40
14 # Truncate THOR's field values after 2048 characters
15 truncate: 2048

```

### 15.4.2 THOR didn't scan the file due to a skipped deeper inspection

This can be caused by two reasons:

The magic header of that file is not in the list of interesting magic headers (see `./signatures/misc/file-type-signatures.cfg`) AND file doesn't have a relevant file extension:

```
.asp, .vbs, .ps, .ps1, .rar, .tmp, .bas, .bat, .chm, .cmd, .com, .cpl, .crt, .dll,
.exe, .hta, .js, .lnk, .msc, .ocx, .pcd, .pif, .pot, .pdf, .reg, .scr, .sct, .sys,
.url, .vb, .vbe, .vbs, .wsc, .wsf, .wsh, .ct, .t, .input, .war, .jsp, .php, .asp,
.aspx, .doc, .docx, .pdf, .xls, .xlsx, .ppt, .pptx, .tmp, .log, .dump, .pwd, .w,
.txt, .conf, .cfg, .conf, .config, .psd1, .psm1, .ps1xml, .clixml, .psc1, .pssc,
.pl, .www, .rdp, .jar, .docm, .ace, .job, .temp, .plg, .asm
```

**Solution:** Use an intense scanning mode for that folder (`--intense`) or add the magic header to `file-type-signatures.cfg`

**Warning:** This file gets overwritten with an update; Intense scanning mode threatens the scan and system stability!

### 15.4.3 THOR fails to initialize custom rules with the correct type

It happens very often that users that prepare custom IOCs or YARA rules forget to include the correct keyword in the filename of the IOC or YARA rule file.

The correct use of keywords is described in the chapters *Simple IOCs* for IOCs and *Specific YARA Rules* for YARA rules.

A wrong or missing keyword leads to situations in which a file that contains YARA rules that are meant to be applied to log files, but doesn't contain a "log" keyword in its filename.

You can review a correct initialization in the command line output or log file.

Info Adding rule set from my-log-rules.yar as 'log' type

Using the keyword **c2** for C2 IOCs in a filename should result in a line like the following:

Info Reading iocs from /tmp/thor10/custom-signatures/iocs/my-c2-iocs.txt as 'domains' ↵  
↪ type

## 15.5 Most Frequent Causes of Frozen Scans

Whenever THOR stops or pauses without any traceback or panic message and no error messages.

Usually the following sources are responsible (descending order, by frequency):

1. An *Antivirus or EDR suspends THOR* (>98%)
2. A "paused" command line window due to *Windows Quick Edit Mode* (<1%)
3. A *Constant High System Load* that causes THOR to stay back and wait for an idling CPU (<1%)
4. *The Perception of a Stalled Scan*, which is actually running (<1%)

### 15.5.1 Antivirus or EDR suspends THOR

In more than 98% of the cases, an Antivirus or EDR is responsible for a stalled process. Especially McAfee AV/EDR is a well-known source of issues. This is caused by the different dialogues in which exceptions have to be defined and the fact certain kinds of blocks cannot be found in any logs.

If a THOR scans stalls in one of these modules, an Antivirus or EDR interaction is highly likely:

- Mutex
- Events
- NamedPipes
- ShimCache
- ProcessCheck

**Solution:** Review all possible exclusions in your AV / EDR and add the THOR folder to the exclusion list

## 15.5.2 Windows Quick Edit Mode

Since Windows 10, the Windows command line window has the so-called "Quick Edit Mode" enabled by default. This mode causes a behavior that can lead to a paused THOR scan process. Whenever a user switches the active windows from the cmd.exe to a different application, e.g. Windows Explorer, and clicks back into the command line window, the running process automatically gets suspended. A user has to press "Enter" to resume the suspended process. As the progress indicator of THOR isn't always changing, this could lead to the impression that the scan paused by itself.

See [this StackOverflow post](#) for more details.

**Solution:** Press "Enter" in the command line window

## 15.5.3 Constant High System Load

Since THOR automatically sets a low process priority a scan can slow down to a level that appears to be paused or suspended on systems that are under a constant high load.

**Solution:** You can avoid this behaviour by using the `--nolowprio` flag. Be aware that scans on a system with a constant high CPU load take longer than on other systems and could slow down the processes that would otherwise take all the CPU capacity.

## 15.5.4 The Perception of a Stalled Scan

Under certain circumstances the scan may appear stalled but is still running. You can always interrupt a scan using CTRL+C that brings THOR into the interrupt menu in which you can see the currently scanned element. In case of the "FileScan" module, this is a file or folder. In case of the "EventLog" module, this is an event with an ID. If you resume the scan by pressing "C" and interrupt it again a few minutes later, you should see another element in the interrupt menu.

If THOR still processes the same element for several hours, we recommend checking that element (size, format, access rights, location).

**Solution:** Check progress using the interrupt menu (CTRL+C)

# 15.6 Most Frequent Causes of Failed Scans

The following examples are the most frequent causes of a failed scan.

## 15.6.1 External Processes Terminating THOR

Whenever THOR dies without any traceback or panic message and no error message in the log file, an external process terminated the THOR process.

Usually the four following sources are responsible (descending order, by frequency):

1. Antivirus or EDR killed the THOR process
2. A user killed the THOR process
3. A management solution that noticed a high CPU load caused by the THOR process killed it
4. Attackers killed the THOR process

---

**Note:** A process termination that always happens at the same element is a sign for an Antivirus or EDR detection.

---

## 15.6.2 Insufficient Free Memory

If the system you are trying to scan runs out of free memory, you will encounter the following message in your scan log:

```
fatal error: out of memory
```

Probable causes:

1. Other processes consume a lot of memory
2. THOR's scanning of certain elements requires a lot of memory
3. You've set ulimit values that are too restrictive
4. You are using the wrong THOR version for your architecture
5. You've activated a feature that consumes a lot of memory (e.g. `--mft` or `--intense`)

Whenever THOR recognizes a low amount of free memory, it checks the top three memory consumers on the system and includes them in the log message, before exiting the scan.

You could try running THOR in Soft Mode (`--soft`), which will deactivate modules and features that require a lot of memory.

Using the 32bit binary of THOR named `thor.exe` on a 64bit system can lead to interrupted scans with the above error message. The 32bit binary is not able to address as much memory as the 64bit version. Always make sure to use the correct THOR version for the respective architecture.

Several `ulimits` might cause THOR to terminate if they are too restrictive, including:

- locked-in-memory size
- address space
- number of open file descriptors
- maximum data size

If you are certain your machine has sufficient RAM, check your ulimits with `ulimit -a` and try to rerun the scan with increased limits, if necessary. The [man page](#) for the ulimits configuration size gives a full overview over the limits and how to persistently modify them.

## 15.7 Help Us With The Debugging

If you cannot find the source of a problem, please contact us using the [support@nexttron-systems.com](mailto:support@nexttron-systems.com) email address.

You can help us find and debug the problem as quickly as possible by providing the following information.

### 15.7.1 Which THOR version do you use?

Tell us the exact THOR version you are using:

1. For which operating system (Windows, Linux, macOS, AIX)
2. For which architecture (32bit, 64bit)

Run `thor --version` and copy the resulting text into the email.

On Windows:

```
C:\thor>thor64.exe --version
THOR 10.6.6
Build bea8066 (2021-04-27 14:32:40)
YARA 4.0.5
PE-Sieve 0.2.8.5
OpenSSL 1.1.1j
Signature Database 2021/05/03-150936
Sigma Database 0.19.1-1749-g2f12c5c5
```

On Linux:

```
user@desktop:~$./thor-linux-64 --version
THOR 10.6.6
Build bea8066 (2021-04-27 14:32:40)
YARA 4.0.5
PE-Sieve 0.2.8.5
OpenSSL 1.1.1j
Signature Database 2021/05/03-150936
Sigma Database 0.19.1-1749-g2f12c5c5
```

On macOS:

```
user@macos:~$./thor-macosx --version
THOR 10.6.6
Build bea8066 (2021-04-27 14:32:40)
YARA 4.0.5
PE-Sieve 0.2.8.5
OpenSSL 1.1.1j
Signature Database 2021/05/03-150936
Sigma Database 0.19.1-1749-g2f12c5c5
```

### 15.7.2 What is the target platform that THOR fails on?

Please provide the output of the following commands.

On Windows:

```
C:\Users\user>systeminfo > systeminfo.txt
```

On Linux:

```
user@desktop:~$ uname -a
```

On macOS:

```
user@macos:~$ system_profiler -detailLevel mini > system_profile.txt
```

### 15.7.3 Which command line arguments do you use?

Please provide a complete list of command line arguments that you've used when the error occurred.

```
C:\thor>thor64.exe --quick -e D:\logs -p C:\Windows\System32
```

### 15.7.4 Provide the log of a scan with the --debug flag

The most important element is a scan log of a scan with the --debug flag used.

The easiest way is to run the scan exactly as you've run it when the problem occurred adding the --debug command line flag.

```
C:\thor>thor64.exe --quick -e D:\logs -p C:\Windows\System32 --debug
```

If you're able to pinpoint the error to a certain module, you could limit the scan to that module to get to the problematic element more quickly.

```
C:\thor>thor64.exe -a Rootkit --debug
```

After the scan you will find the normal text log (\*.txt) in the program folder. It is okay to replace confidential information like the hostname or IP addresses.

Note: The debug log files can be pretty big, so please compress the file before submitting it to us. Normal log files have a size between 1 and 4 MB. Scans started with the --debug flag typically have sizes of 30-200 MB. The compression ratio is typically between 2-4%, so a compressed file shouldn't be larger than 10 MB.

### 15.7.5 Provide a Screenshot (Optional)

Sometimes errors lead to panics of the executables, which causes the situation in which relevant log lines don't appear in the log file. In these cases, please also create a screenshot of a panic shown in the command line window.

### 15.7.6 Provide the THOR database (Optional)

The *THOR DB* helps us debug situations in which the THOR scan timed out or didn't complete at all. It contains statistics on the run time of all used modules and the durations of all folders up to the second folder level from the root of a partition. (e.g. C:\Windows\SysWow64).

The default location of that file is:

- Windows: C:\ProgramData\thor\thor10.db
- Linux/macOS: /var/lib/thor/thor10.db

Please provide that file in situations in which:

- THOR exceeded its maximum run time
- THOR froze and didn't complete a scan for days
- THOR scans take too long for the selected scan targets



### 15.7.7 Further Notes

- If the files are too big to send, even after compression, please contact us and you'll receive a file upload link that you can use
- If a certain file or element (eventlog, registry hive) caused the issue, please check if you can provide that file or element for our analysis, as those files can contain sensitive information.



## ANALYSIS AND INFO

### 16.1 Log Analysis Manual

You can find our Log Analysis Manual online:

<https://log-analysis-manual.nexttron-systems.com>

This will help to process the events generated by THOR.

### 16.2 VALHALLA Rule Lookup

The new rule info pages allow you to get more information on a certain rule. You can find all the meta data, as well as past rule matches and previous antivirus verdicts. A second tab contains statistics. You can also report false positives that you've encountered with that rule using the button in the tab bar.

Note that the rule info lookups in the web GUI are rate limited. If you query rule infos too often, you get blocked.

The rule info pages can be access using this URL scheme:

[https://valhalla.nexttron-systems.com/info/rule/RULE\\_NAME](https://valhalla.nexttron-systems.com/info/rule/RULE_NAME)


For example:

[https://valhalla.nexttron-systems.com/info/rule/HKTL\\_Empire\\_ShellCodeRDI\\_Dec19\\_1](https://valhalla.nexttron-systems.com/info/rule/HKTL_Empire_ShellCodeRDI_Dec19_1)

### 16.3 Rule List Output

By using the `--print-signatures` flag, you can get a list of all initialized YARA and Sigma rules.

This information can also be printed machine readable as JSON by using the `--print-signatures-json` flag.


**VALHALLA**  
SUPERCHARGE YOUR DETECTION

## HKTL\_Empire\_ShellCodeRDI\_Dec19\_1

Info
Statistics
Report False Positive

### Rule Info

|                    |                                                                                                                                                                               |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name               | HKTL_Empire_ShellCodeRDI_Dec19_1                                                                                                                                              |
| Author             | Florian Roth                                                                                                                                                                  |
| Description        | Detects Empire shellcode RDI                                                                                                                                                  |
| Score              | 75                                                                                                                                                                            |
| Reference          | <a href="https://github.com/BC-SECURITY/Empire/">https://github.com/BC-SECURITY/Empire/</a>                                                                                   |
| Date               | 2019-12-09                                                                                                                                                                    |
| Minimum Yara       | 1.7                                                                                                                                                                           |
| Rule Hash          | da9a57d689dbb4ea1d7bf1ae9229025f                                                                                                                                              |
| Tags               | [HKTL]                                                                                                                                                                        |
| Required Modules   | []                                                                                                                                                                            |
| Av Ratio           | 44.59                                                                                                                                                                         |
| Virustotal Matches | <a href="https://www.virustotal.com/gui/search/hktl_empire_shellcoderdi_dec19_1/comments">https://www.virustotal.com/gui/search/hktl_empire_shellcoderdi_dec19_1/comments</a> |

### Antivirus Verdicts

| Rating                    | Number of Samples |
|---------------------------|-------------------|
| Malicious (>= 10 engines) | 66                |
| Suspicious (< 10 engines) | 15                |
| Clean (0 engines)         | 0                 |

### Rule Matches

| Timestamp           | Positives | Total | Hash                                                             | VT Link |
|---------------------|-----------|-------|------------------------------------------------------------------|---------|
| 2020-05-10 13:45:29 | 10        | 59    | 497ff4d9f4b8b24d7aaf37b06b53ea7efe753b6581c5e9b0d982e63ec7bca72f | >       |
| 2020-05-09 23:05:27 | 11        | 59    | 7d19e0e8e3920366a22460a92245b8d3983be1d361a8248ab2c8c5f7f53c7fb4 | >       |
| 2020-05-02 02:42:59 | 3         | 73    | 485fcc6c4a64bc63a7a9312ae92f69c4123aec81fb9d637f320111798f92dab  | >       |
| 2020-04-24 01:59:27 | 10        | 58    | 5b07014032ff99616f49b08af009ba5a74d7abe2cc49903b5dbd80fff5271678 | >       |
| 2020-04-23 20:50:34 | 28        | 67    | bff921b96bd5541e5cd393684f4f2626b6b0f6a606ff7c3a2cdef878b2c16eda | >       |
| 2020-04-19 01:15:18 | 29        | 70    | 4d120187bb417b65c553c181fc17520ac7b1912ef9f458efb5b5e9cb682cf79c | >       |
| 2020-04-17 17:56:11 | 9         | 55    | 5efae2d2cb84adbc68ef14dc326735d5a357eefb4be6009f468066a4645f2b38 | >       |
| 2020-04-17 14:58:28 | 49        | 72    | 6b5a437399030a758f4fbac6d20eaa76ca917c11737b30fd527c53491d9ac579 | >       |
| 2020-04-17 14:11:25 | 21        | 72    | 6c80375edb554b570e2b4a5bc5e3236d2eeb0a9bf7319b7cd976aeeba2a3077e | >       |

Fig. 1: Rule Info Page

```
TYPE: YARA RULE: APT_Sakabota_Malware_Sep19_1 DESCRIPTION: Detects Sakabota malware RULE_DATE: 2019-09-26 REFERENCE: https://unit42.paloaltonetworks.com/xhunt-campaign-attacks-on-kuwait-shipping-and-transportation-organizations/ AUTHOR: Florian Roth
TYPE: YARA RULE: APT_KEYBOY_Malware_Sep19_1 DESCRIPTION: Detects KEYBOY malware RULE_DATE: 2019-09-27 REFERENCE: https://twitter.com/stvemillertime/status/1177623076151779329 AUTHOR: Florian Roth
TYPE: YARA RULE: APT_MAL_NK_Kimsuky_Sep19_1 DESCRIPTION: Detects Kimsuky malware RULE_DATE: 2019-09-30 REFERENCE: https://twitter.com/cyberwar_15/status/1178529821573279744 AUTHOR: Florian Roth
TYPE: YARA RULE: APT_MAL_NK_Kimsuky_PS1_Sep19_2 DESCRIPTION: Detects Kimsuky PowerShell malware helper RULE_DATE: 2019-09-30 REFERENCE: https://twitter.com/cyberwar_15/status/1178529821573279744 AUTHOR: Florian Roth
TYPE: YARA RULE: APT_MAL_Lazarus_Sep19_1 DESCRIPTION: Detects Lazarus malware RULE_DATE: 2019-09-30 REFERENCE: https://twitter.com/KseProso/status/1178580006047539200 AUTHOR: Florian Roth
TYPE: YARA RULE: APT_NATO_Lamberts_Strings DESCRIPTION: Detects strings from Lamberts malware samples RULE_DATE: 2019-09-30 REFERENCE: https://ti.qianxin.com/blog/articles/network-weapons-of-cia/ AUTHOR: Florian Roth
```

Fig. 2: Rule List Output



## USE CASES

This chapter contains use cases that users often asked for.

### 17.1 Disk Image Analysis

---

**Hint:** A lot of functions in this chapter require a **forensic lab** or **lab** license. This license is geared towards forensic experts. Forensic Lab Licenses are a special license type with more functionality.

---

THOR, as a scanner, does not mount disk images to a certain drive on your forensic workstation. You have to use 3rd party tools for that task. Please see *Arsenal Image Mounter (AIM)* and *FTKImager* for Windows or *Dissect* for Linux to get an overview of potential tools to use. Other tools should also work.

First, you mount the image to a certain drive/path with your preferred tool. Afterwards you can use THOR in the lab scanning mode to analyze the mounted image.

The following example shows a recommended set of parameters, scanning a mounted image of a host named **WKS0001** on drive **S:\** of your forensic Windows workstation.

```
C:\thor>thor64.exe --lab --virtual-map S:C -j WKS0001 -p S:\
```

The following example shows the same parameters for a Linux forensic workstation. The drive is mounted to **/mnt/image/fs/sysvol/**.

```
nextron@unix:~/thor$./thor-linux-64 --lab --virtual-map /mnt/image/fs/sysvol/:C -j WKS0001 -p /mnt/image/fs/sysvol/
```

The **--lab** parameter will apply several internal flags (e.g. enables intense mode to scan every file, enables multi-threading, disables resource control, removes all limitations). The **--virtual-map** parameter maps every file found in elements of that image to the original drive letter and allows the message enrichment to work correctly. The **-j HOSTNAME** parameter can be used to write every log line with the hostname of the original system and not with that of the forensic workstation.

You find more information on the scan parameters in the chapter *Lab Scanning*.

---

**Hint:** This [blog post](#) mentions different ways to use commercial or built-in tools to mount and scan VMDK images.

---

### 17.1.1 Arsenal Image Mounter (AIM)

We recommend using [Arsenal Image Mounter](#).

In case you plan to use an automated setup in which you use scripts to automatically process images, you could try to use the command-line of AIM, please see the `aim_cli.exe` within the program folder for more help.

### 17.1.2 FTKImager

Alternatively, you can use the tool [FTKImager](#) to mount your image.

---

**Note:** We recommend using Arsenal Image Mounter to mount your images, since we observed better performance during our internal tests.

---

### 17.1.3 Dissect

Dissect is an incident response framework build from various parsers and implementations of file formats. Tying this all together, Dissect allows you to work with tools named `target-query` and `target-shell` to quickly gain access to forensic artefacts, such as Runkeys, Prefetch files, and Windows Event Logs, just to name a few!

You can find the tool here: <https://github.com/fox-it/dissect>

For instructions on how to mount a disk image, you can find information here: <https://docs.dissect.tools/en/latest/tools/target-mount.html>

## 17.2 Memory Image Analysis with Volatility

In this use case, we show a way to run a THOR scan on a full memory image of a target system.

In volatility, we first evaluate the right profile for a memory image. You can use the `imageinfo` command or select one manually from the list that is show when you run `vol.py --info`.

```
user@linux:~$ vol.py -f win10-lab1.mem imageinfo

Volatility Foundation Volatility Framework 2.6.1
INFO : volatility.debug : Determining profile based on KDBG search...
 Suggested Profile(s) : Win10x64_19041
 AS Layer1 : SkipDuplicatesAMD64PagedMemory (Kernel AS)
 AS Layer2 : FileAddressSpace (/mnt/downloads/mem-dumps/win10-lab1.
↪ mem)
 PAE type : No PAE
 DTB : 0x1aa002L
 KDBG : 0xf8005aa00b20L
 Number of Processors : 2
 Image Type (Service Pack) : 0
 KPCR for CPU 0 : 0xffffffff80055ec0000L
 KPCR for CPU 1 : 0xffff8500313c0000L
 KUSER_SHARED_DATA : 0xffffffff780000000000L
 Image date and time : 2021-06-15 08:25:08 UTC+0000
 Image local date and time : 2021-06-15 10:25:08 +0200
```



We then create a directory that will store all our process memory images.

```
user@linux:~$ mkdir procs
```

Now we can extract all process memory images and save them to the new directory.

```
user@linux:~$ vol.py -f win10-lab1.mem --profile=Win10x64_19041 memdump -D procs/
```

```
Volatility Foundation Volatility Framework 2.6.1

Writing System [4] to 4.dmp

Writing Registry [92] to 92.dmp

Writing smss.exe [348] to 348.dmp

Writing csrss.exe [440] to 440.dmp

Writing wininit.exe [512] to 512.dmp

Writing csrss.exe [520] to 520.dmp

Writing winlogon.exe [608] to 608.dmp

Writing services.exe [624] to 624.dmp

Writing lsass.exe [656] to 656.dmp

Writing fontdrvhost.ex [748] to 748.dmp
```

We recommend saving that output for mapping purposes, since THOR will only report the file names upon a YARA rule match, e.g. 748.dmp, and not the name of the executable fontdrvhost.exe.

Using THOR, we can now scan the extracted process memory images.

```
user@linux:~$./thor-linux-64 --lab -p /mnt/mem-dumps/procs/
```

Without a valid lab license, we can simulate that behaviour using the following command (see [Lab Scanning](#) for more details and flags used in lab scan mode):

```
user@linux:~$./thor-linux-64 -a Filescan --intense -p /mnt/mem-dumps/procs/
```

The output of such a scan will look like this

```
[?] Worker 01: /mnt/mem-dumps/procs/3812.dmp [-----]
↪Progress: 286 MB
[?] Worker 01: /mnt/mem-dumps/procs/3812.dmp [-----]
↪Progress: 343 MB
Alert YARA Score Rule Match
 TARGET: /mnt/mem-dumps/procs/3812.dmp
 TYPE: file
 NAME: SUSP_Encoded_UA_Mozilla
 SCORE: 50
 DESCRIPTION: Detects encoded keyword - User-Agent: Mozilla/
 SIGTYPE: internal
```

(continues on next page)

(continued from previous page)

```

CHUNK_OFFSET: 3660000000
TAGS: SUSP, T1027
MATCHING_STRINGS: Str1: "VzZXItQWdlbnQ6IE1vemlsbGEv" in
↪ "dDBRMDONClVzZXItQWdlbnQ6IE1vemlsbGEvNS4wIChjb2" at 0x1672eacc
MODIFIED: Tue Jun 15 11:38:13 2021
CHANGED: Tue Jun 15 11:38:13 2021
TARGET_SIZE: 610324480
[?] Worker 01: /mnt/mem-dumps/procs/3812.dmp [-----]
↪]Progress: 400 MB
[?] Worker 01: /mnt/mem-dumps/procs/3812.dmp [-----]
↪]Progress: 457 MB

```

The match includes an offset, e.g. `CHUNK_OFFSET: 3660000000`, and a matching string, e.g. `Str1: "VzZXItQWdlbnQ6IE1vemlsbGEv"` which help you to locate the correct section in the dump file using a hex editor for further analysis.

## 17.3 Scanning a Fileserver

The recommendation for scanning a fileserver is running THOR directly on the system. If that is not possible, because the operating system of the fileserver is not supported by THOR, we recommend a dedicated system to perform a filescan on the shares. The system should have at least 2 CPU cores and 2 GB of RAM.

The recommended flags to run THOR are:

```
C:\temp\thor>thor64.exe --module Filescan --alldrives --path X: --path Y: --path Z:
```

**Note:** The `--alldrives` flag is only available with a lab license

If needed or desired, the scan can be adapted using the following flags. In general, the following options are not recommended but can help in special scenarios.

- `--resume`
  - If a previous scan failed (e.g. because of a exceeded max. runtime) the scan can be resumed, if the same flags (and additional the resume flag) are used to start the scan.
- `--max-runtime 0`
  - Default is 7 days. Change this value if your scans need more time.
- `--path \\fileserver01\shareA`
  - If permissions allow anonymous access, the shares can be accessed using the UNC path and do not need to be mounted.
- `--nosoft`
  - If your scanning system has too little system resources, the softmode is automatically enabled. This flag prevents that.
- `--all-module--lookback --lookback 8`
  - Only scans files that were modified within the last 8 days. Faster scan time but vulnerable to timestamping attacks.
- `--diff`

- Only scans new files or files that were modified since the last scan. Faster scan time but vulnerable to timestomping attacks. THOR DB is needed for diff, so cannot be used in combination with `--nothordb`.
- `--max_file_size` ?????
  - Maximum file size In bytes. The default is 20 MB. If you need to scan bigger files, you might need to increase the maximum file size.
- `--no<feature>`
  - Disable features like scanning eventlog files (`--noevt`), if your share contains files that trigger special feature checks of THOR, that are not desired. Please see [Scan Module Names](#) and [Feature names](#) for a list of module/feature names and the respective command line argument to disable them.
- `--allfiles`
  - Scan all files, independent of file extensions or magic headers. Use `--max_file_size_intense` instead of `--max_file_size`. (Caution: This will increase the scan time drastically!)

If the share is not accessible anonymously, you need to mount the shares using valid user credentials. This has to be done before the scan and access granted to the user running the THOR scan. If you use ASGARD to launch THOR the user performing the scan is `NT AUTHORITY\SYSTEM`.

The usage of diff and lookback are generally not recommended, but can be used if your fileshare scan does not finish in the timeframe you desire. Another option is to use multiple dedicated systems to run scans on the fileserver shares in parallel.



## KNOWN ISSUES

### 18.1 THOR#003: No rules with DEEPSCAN tag found

| Introduced Version | Fixed Version |
|--------------------|---------------|
| N/A                | N/A           |

This error is caused by a missing signature set. Usually the user just copied the THOR executable and forgot to copy the whole program folder including the `./signatures` folder. The error message means that none of THOR's own signatures could be found. These signatures also include the so-called DEEPSCAN signatures. THOR reports that not a single one of these signatures could be found, which results in very limited scan capabilities.

You can see that this is the case by inspecting your scan results:

```
THOR: Warning: MODULE: Init MESSAGE: No rules with DEEPSCAN tag found.
 THOR won't scan any files with YARA rules. Please ensure that you use
 up-to-date signatures. SCANID: S-Qpw5dDmEBaw
THOR: Info: MODULE: Init MESSAGE: Successfully compiled 0 custom default
 YARA rules SCANID: S-Qpw5dDmEBaw TYPE: YARA
```

You can also see during the initialization process of THOR, that no YARA rules are compiled:

```
C:\nexttron\thor>thor64.exe
[...]

> Reading YARA signatures and IOC files ...
Info Successfully compiled 0 default YARA rules TYPE: YARA
Info Successfully compiled 0 log YARA rules TYPE: YARA
Info Successfully compiled 0 registry YARA rules TYPE: YARA
Info Successfully compiled 0 keyword YARA rules TYPE: YARA
Info Successfully compiled 0 process YARA rules TYPE: YARA
Info Successfully compiled 0 meta YARA rules TYPE: YARA
Warning No rules with DEEPSCAN tag found. THOR won't scan any files with YARA rules.
 Please ensure that you use up-to-date signatures.
Info Successfully compiled 0 custom default YARA rules TYPE: YARA
Info Skip sigma initialization, use '--sigma' flag to scan with sigma
Info Successfully compiled 0 STIXv2 indicators (skipped 0 indicators) TYPE: STIX
Info Successfully compiled 0 keyword ioc strings TYPE: IOC
Info Successfully compiled 0 filename ioc strings and 0 filename ioc regexs TYPE: IOC
Info Successfully compiled 0 malware and 0 false positive hashes TYPE: IOC
```

(continues on next page)

(continued from previous page)

```
Info Successfully compiled 0 file type signatures TYPE: IOC
Info Successfully compiled 0 malware domains TYPE: IOC
Info Successfully compiled 0 malicious handles and 0 regex malicious handles TYPE: IOC
Info Successfully compiled 0 named pipe ioc strings and 0 named pipe ioc regexs TYPE: IOC
Warning No file type signatures compiled, file type detection can't be done.
 Because of this, many files won't be scanned.
[...]
```

### 18.1.1 THOR#003: Solution

Make sure that you have the `./signatures` folder in your THOR program folder and that it contains at least the following files:

- `./signatures/yara/thor-all.yas`
- `./signatures/yara/thor-deepscan-selectors.yasx`
- `./signatures/yara/thor-expensive.yase`
- `./signatures/yara/thor-keywords.yas`
- `./signatures/yara/thor-log-sigs.yas`
- `./signatures/yara/thor-meta.yas`
- `./signatures/yara/thor-process-memory-sigs.yas`
- `./signatures/yara/thor-registry.yas`

## 18.2 THOR#002: THOR in Lab-Mode does not scan network or external drives

| Introduced Version | Fixed Version                                         |
|--------------------|-------------------------------------------------------|
| N/A                | <code>&gt;=10.6.16</code><br><code>&gt;=10.7.3</code> |

If running a command like `thor64.exe --lab -p Z:\myshare` THOR will not currently scan the path. Normally the `--alldrives` flag should be implicitly activated in Lab-mode.

---

**Note:** The `--alldrives` flag is only available with a lab license

---

### 18.2.1 THOR#002: Workaround

You have to add the `--alldrives` flag on your own. E.g.

```
C:\thor>thor64.exe --lab -p Z:\myshare --alldrives
```

## 18.3 THOR#001: Could not parse sigma logsources

| Introduced Version | Fixed Version |
|--------------------|---------------|
| N/A                | N/A           |

```
Error could not parse sigma log sources
FILE: config\sigma.yml ERROR: no logsources element found
```

The issue occurs only for very old THOR installations that at one time had the template file `config\templ-sigma.yml` named `config\sigma.yml`.

### 18.3.1 THOR#001: Workaround

The error can be ignored and the THOR scan will run as expected. To prevent the error message from showing, remove `config\sigma.yml` or use a newly downloaded THOR package.





## LINKS AND REFERENCES

THOR Website: <https://www.nexttron-systems.com/thor/>

Nexttron Customer Portal: <https://portal.nexttron-systems.com>

Nexttron Software Update Status: <https://update1.nexttron-systems.com/info.php>

YARA Documentation: <https://yara.readthedocs.io/>

yarGen - YARA Rule Generator: <https://github.com/Neo23x0/yarGen/>

THOR APT Scanner App and Add-on v2: <https://splunkbase.splunk.com/app/3717/> and <https://splunkbase.splunk.com/app/3718/>

Sigma Project: <https://github.com/Neo23x0/sigma>

### 19.1 Open Source License Acknowledgements

List of third-party software components used by THOR 10 with open source licensing requirements.

#### 19.1.1 golang.org

Copyright (c) 2009 The Go Authors  
Licensed under BSD-3 License

#### 19.1.2 OpenSSL

Copyright (c) OpenSSL  
Licensed under OpenSSL license (<https://www.openssl.org/source/license.html>)

### 19.1.3 YARA

Copyright (c) 2007-2016 The YARA Authors  
Licensed under BSD-3 License

### 19.1.4 [github.com/Azure/go-ntlmssp](https://github.com/Azure/go-ntlmssp)

Copyright (c) 2016 Microsoft  
Licensed under MIT License

### 19.1.5 [github.com/botherder/go-autoruns](https://github.com/botherder/go-autoruns)

modified as [github.com/Codehardt/go-autoruns](https://github.com/Codehardt/go-autoruns)  
Copyright (c) 2018 Claudio Guarnieri  
Licensed under MIT License

### 19.1.6 [github.com/omarghader/pefile-go](https://github.com/omarghader/pefile-go)

modified as [github.com/Codehardt/go-pefile](https://github.com/Codehardt/go-pefile)  
Copyright (c) 2004-2015 Ero Carrera  
Licensed under MIT License

### 19.1.7 Copyright (c) 2018 Marcel Gebhardt

[github.com/Codehardt/go-cpulimit](https://github.com/Codehardt/go-cpulimit)  
[github.com/Codehardt/go-handle](https://github.com/Codehardt/go-handle)  
[github.com/Codehardt/go-ntlm-proxy-auth](https://github.com/Codehardt/go-ntlm-proxy-auth)  
[github.com/Codehardt/go-osversion](https://github.com/Codehardt/go-osversion)  
[github.com/Codehardt/go-priority](https://github.com/Codehardt/go-priority)  
[github.com/Codehardt/go-taskscheduler](https://github.com/Codehardt/go-taskscheduler)  
Licensed under MIT License

### 19.1.8 Copyright (c) 2018 Samuel Melrose

[github.com/Codehardt/go-win64api](https://github.com/Codehardt/go-win64api)  
[github.com/iamacarpet/go-win64api](https://github.com/iamacarpet/go-win64api)  
Licensed under MIT License

### **19.1.9 Copyright (c) 2011, Evan Shaw <edsrzf@gmail.com>**

github.com/Codehardt/mmap-go  
github.com/ncw/mmap-go  
Licensed under BSD-3 License

### **19.1.10 github.com/StackExchange/wmi**

Copyright (c) 2013 Stack Exchange  
Licensed under MIT License

### **19.1.11 Copyright (c) 2018-2020 velocidex**

github.com/Velocidex/ordereddict  
github.com/Velocidex/regparser  
github.com/secDre4mer/regparser  
www.velocidex.com/golang/go-ntfs  
www.velocidex.com/golang/evtx  
github.com/Velocidex/evtx  
Licensed under Apache License 2.0

### **19.1.12 github.com/andrewkroh/sys**

Copyright (c) 2009 The Go Authors

### **19.1.13 github.com/bothorder/go-files**

Copyright (c) 2018 Nex  
Licensed under MIT License

### **19.1.14 github.com/coreos/go-systemd/v22**

(no copyright notes found)  
Licensed under Apache License 2.0

### **19.1.15 github.com/dsnet/compress**

Copyright (c) 2015, Joe Tsai and The Go Authors  
Licensed under BSD-3 License

### **19.1.16 [github.com/dustin/go-humanize](https://github.com/dustin/go-humanize)**

Copyright (c) 2005-2008 Dustin Sallings <[dustin@spy.net](mailto:dustin@spy.net)>  
Licensed under MIT License

### **19.1.17 Copyright (c) 2014-2020 Elasticsearch BV**

[github.com/elastic/beats](https://github.com/elastic/beats)  
[github.com/elastic/go-ucfg](https://github.com/elastic/go-ucfg)  
[github.com/elastic/go-sysinfo](https://github.com/elastic/go-sysinfo)  
Licensed under Apache License 2.0

### **19.1.18 [github.com/fatih/color](https://github.com/fatih/color)**

Copyright (c) 2013 Fatih Arslan  
Licensed under MIT License

### **19.1.19 [github.com/fsnotify/fsnotify](https://github.com/fsnotify/fsnotify)**

Copyright (c) 2012 The Go Authors  
Copyright (c) 2012 fsnotify Authors  
Licensed under BSD-3 License

### **19.1.20 Copyright (c) 2015 Zack Guo**

[github.com/gizak/termui/v3](https://github.com/gizak/termui/v3)  
[github.com/gizak/termui/v3/widgets](https://github.com/gizak/termui/v3/widgets)  
[github.com/gizak/termui/v3/drawille](https://github.com/gizak/termui/v3/drawille)  
Licensed under MIT License

### **19.1.21 [github.com/go-ole/go-ole](https://github.com/go-ole/go-ole)**

Copyright (c) 2013-2017 Yasuhiro Matsumoto, <[matt.n.jp@gmail.com](mailto:matt.n.jp@gmail.com)>  
Licensed under MIT License

### **19.1.22 [github.com/godbus/dbus](https://github.com/godbus/dbus)**

Copyright (c) 2013, Georg Reinke (<[guelfey@gmail.com](mailto:guelfey@gmail.com)>), Google  
Licensed under BSD-2 License

### 19.1.23 [github.com/gofrs/uuid](https://github.com/gofrs/uuid)

Copyright (C) 2013-2018 by Maxim Bubliss <b@codemonkey.ru>  
Licensed under MIT License

### 19.1.24 [github.com/google/pprof](https://github.com/google/pprof)

(no copyright notes found)  
Licensed under Apache License 2.0

### 19.1.25 [github.com/golang/snappy](https://github.com/golang/snappy)

Copyright (c) 2011 The Snappy-Go Authors  
Licensed under BSD-3 License

### 19.1.26 Copyright (c) 2010-2012 The w32 Authors

[github.com/gonutz/w32](https://github.com/gonutz/w32)  
[github.com/shirou/w32](https://github.com/shirou/w32)  
[github.com/AllenDang/w32](https://github.com/AllenDang/w32)  
Licensed under MIT License

### 19.1.27 Licensed under Mozilla Public License 2.0

[github.com/hashicorp/go-multierror](https://github.com/hashicorp/go-multierror)  
[github.com/hashicorp/golang-lru](https://github.com/hashicorp/golang-lru)  
[github.com/hashicorp/errwrap](https://github.com/hashicorp/errwrap)  
(no copyright notes found)

### 19.1.28 [github.com/hillu/go-yara/v4](https://github.com/hillu/go-yara/v4)

Copyright (c) 2015-2020 Hilko Bengen <bengen@hilluzination.de>  
Licensed under BSD-2 License

### 19.1.29 [github.com/inconshreveable/mousetrap](https://github.com/inconshreveable/mousetrap)

Copyright (c) 2014 Alan Shreve  
Licensed under Apache License 2.0

### **19.1.30 [github.com/joeshaw/multierror](https://github.com/joeshaw/multierror)**

Copyright (c) 2014 Joe Shaw  
Licensed under MIT License

### **19.1.31 [github.com/kardianos/service](https://github.com/kardianos/service)**

Copyright (c) 2015 Daniel Theophanes  
Licensed under zlib License

### **19.1.32 [github.com/marcsauter/single](https://github.com/marcsauter/single)**

Copyright (c) 2018 Marc Sauter  
Licensed under MIT License

### **19.1.33 Copyright (c) Yasuhiro MATSUMOTO <[mattn.jp@gmail.com](mailto:mattn.jp@gmail.com)>**

[github.com/mattn/go-colorable](https://github.com/mattn/go-colorable)  
[github.com/mattn/go-isatty](https://github.com/mattn/go-isatty)  
[github.com/mattn/go-runewidth](https://github.com/mattn/go-runewidth)  
[github.com/mattn/go-shellwords](https://github.com/mattn/go-shellwords)  
[github.com/mattn/go-sqlite3](https://github.com/mattn/go-sqlite3)  
Licensed under MIT License

### **19.1.34 [github.com/mitchellh/go-wordwrap](https://github.com/mitchellh/go-wordwrap)**

Copyright (c) 2014 Mitchell Hashimoto  
Licensed under MIT License

### **19.1.35 [github.com/mholt/archiver](https://github.com/mholt/archiver)**

Copyright (c) 2016 Matthew Holt  
Licensed under MIT License

### **19.1.36 [github.com/nsf/termbox-go](https://github.com/nsf/termbox-go)**

Copyright (C) 2012 termbox-go authors  
Licensed under MIT License

**19.1.37 [github.com/nwaples/rardecode](https://github.com/nwaples/rardecode)**

Copyright (c) 2015 Nicholas Waples  
Licensed under BSD-2 License

**19.1.38 [github.com/pierrec/lz4](https://github.com/pierrec/lz4)**

Copyright (c) 2015 Pierre Curto  
Licensed under BSD-3 License

**19.1.39 Copyright (c) Dave Cheney <dave@cheney.net>**

[github.com/pkg/errors](https://github.com/pkg/errors)  
[github.com/pkg/profile](https://github.com/pkg/profile)  
Licensed under BSD-2 License

**19.1.40 [github.com/pytimer/win-netstat](https://github.com/pytimer/win-netstat)**

Copyright (c) 2018 pytimer  
Licensed under MIT License

**19.1.41 [github.com/sebdah/goldie](https://github.com/sebdah/goldie)**

Copyright 2016 Sebastian Dahlgren <sebastian.dahlgren@gmail.com>  
Licensed under MIT License

**19.1.42 [github.com/shirou/gopsutil](https://github.com/shirou/gopsutil)**

Copyright (c) 2014 WAKAYAMA Shirou  
Copyright (c) 2009 The Go Authors  
Licensed under BSD License

**19.1.43 Copyright (c) 2016 SmartyStreets, LLC**

[github.com/smartystreets/goconvey](https://github.com/smartystreets/goconvey)  
[github.com/smartystreets/assertions](https://github.com/smartystreets/assertions)  
Licensed under MIT License

#### **19.1.44 [github.com/spf13/cobra](https://github.com/spf13/cobra)**

(no copyright notes found)

Licensed under Apache License 2.0

#### **19.1.45 [github.com/spf13/pflag](https://github.com/spf13/pflag)**

Copyright (c) 2012 Alex Ogier

Copyright (c) 2012 The Go Authors

Licensed under BSD-3 License

#### **19.1.46 [github.com/stretchr/testify](https://github.com/stretchr/testify)**

Copyright (c) 2012-2018 Mat Ryer and Tyler Bunnell

Licensed under MIT License

#### **19.1.47 [github.com/xi2/xz](https://github.com/xi2/xz)**

(no license and copyright notes found)

#### **19.1.48 Copyright (c) 2016-2017 Uber Technologies, Inc.**

[go.uber.org/atomic](https://go.uber.org/atomic)

[go.uber.org/multierr](https://go.uber.org/multierr)

Licensed under MIT License

#### **19.1.49 [go.uber.org/zap](https://go.uber.org/zap)**

Copyright (c) 2016-2017 Uber Technologies, Inc.

Licensed under MIT License

#### **19.1.50 Copyright (c) 2009 The Go Authors**

[golang.org/x/arch](https://golang.org/x/arch)

[golang.org/x/crypto](https://golang.org/x/crypto)

[golang.org/x/sys](https://golang.org/x/sys)

[golang.org/x/exp](https://golang.org/x/exp)

[golang.org/x/net](https://golang.org/x/net)

[golang.org/x/oauth2](https://golang.org/x/oauth2)

[golang.org/x/term](https://golang.org/x/term)

[golang.org/x/time](https://golang.org/x/time)

[golang.org/x/tools](https://golang.org/x/tools)

[golang.org/x/sync](https://golang.org/x/sync)

Licensed under BSD-3 License



### **19.1.51 gopkg.in/ini.v1**

Copyright (c) 2014 Unknwon  
Licensed under Apache License 2.0

### **19.1.52 gopkg.in/natefinch/npipes.v2**

Copyright (c) 2013 npipes authors  
Licensed under MIT License

### **19.1.53 Copyright 2011-2016 Canonical Ltd.**

gopkg.in/yaml.v2  
gopkg.in/yaml.v3  
Licensed under Apache License 2.0

### **19.1.54 howett.net/plist**

Copyright (c) 2013, Dustin L. Howett  
Copyright (c) 2012 The Go Authors  
Licensed under BSD-3 License

### **19.1.55 github.com/willballenthin/shellbags**

(no copyright notes found)  
Licensed under Apache License 2.0

### **19.1.56 go.opencensus.io**

(no copyright notes found)  
Licensed under Apache License 2.0

### **19.1.57 cloud.google.com/go**

(no copyright notes found)  
Licensed under Apache License 2.0

### 19.1.58 Copyright (c) 2015 Chzyer

github.com/chzyer/logex  
github.com/chzyer/readline  
github.com/chzyer/test  
Licensed under MIT License

### 19.1.59 github.com/ianlancetaylor/demangle

Copyright (c) 2015 The Go Authors  
Licensed under BSD-3 License

### 19.1.60 github.com/jstemmer/go-junit-report

Copyright (c) 2012 Joel Stemmer  
Licensed under MIT License

### 19.1.61 Google Go modules

google.golang.org/api  
google.golang.org/appengine  
google.golang.org/genproto  
google.golang.org/grpc  
(no copyright notes found)  
Licensed under Apache License 2.0

### 19.1.62 Copyright (c) 2018 The Go Authors

google.golang.org/protobuf  
github.com/golang/protobuf  
Licensed under BSD-3 License

### 19.1.63 github.com/golang/groupcache

(no copyright notes found)  
Licensed under Apache License 2.0

**19.1.64 [github.com/google/go-cmp](https://github.com/google/go-cmp)**

Copyright (c) 2017 The Go Authors  
Licensed under BSD-3 License

**19.1.65 <https://github.com/hasherezade/pe-sieve>**

Copyright (c) 2017-2020, @hasherezade  
Licensed under BSD 2-Clause License

**19.1.66 <https://github.com/hasherezade/libpeconv>**

Copyright (c) 2017-2019, hasherezade (@hasherezade)  
Licensed under BSD 2-Clause License

**19.1.67 <https://github.com/parsiya/golnk>**

(no copyright notes found)  
Licensed under Apache License 2.0

**19.1.68 <https://github.com/olekukonko/tablewriter>**

Copyright (C) 2014 by Oleku Konko  
Licensed under MIT License

**19.1.69 [github.com/frankban/quicktest](https://github.com/frankban/quicktest)**

Copyright (c) 2017 Canonical Ltd.  
Licensed under MIT License

**19.1.70 [github.com/niemeyer/pretty](https://github.com/niemeyer/pretty)**

Copyright 2012 Keith Rarick  
Licensed under MIT License

### 19.1.71 [github.com/prometheus/procfs](https://github.com/prometheus/procfs)

(no copyright notes found)

Licensed under Apache License 2.0

### 19.1.72 Beats

<https://github.com/secDre4mer/beats>

<https://github.com/elastic/beats>

Licensed by Elasticsearch B.V.

Licensed under Apache License 2.0

### 19.1.73 <https://github.com/ulikunitz/xz>

Copyright (c) 2014-2020 Ulrich Kunitz

Licensed under BSD 2-Clause "Simplified" License

### 19.1.74 [go.elastic.co/ecszap](https://go.elastic.co/ecszap)

Copyright 2020 Elastic and contributors

Licensed under Apache License 2.0

### 19.1.75 [gopkg.in/check.v1](https://gopkg.in/check.v1)

Copyright (c) 2010-2013 Gustavo Niemeyer <[gustavo@niemeyer.net](mailto:gustavo@niemeyer.net)>

Licensed under BSD 2-Clause "Simplified" License

### 19.1.76 [github.com/gopherjs/gopherjs](https://github.com/gopherjs/gopherjs)

Copyright (c) 2013 Richard Musiol

Licensed under BSD 2-Clause "Simplified" License

### 19.1.77 [github.com/kr/text](https://github.com/kr/text)

Copyright 2012 Keith Rarick

Licensed under MIT License

### **19.1.78 Copyright (c) 2016 Mark Bates**

github.com/gobuffalo/envy  
github.com/gobuffalo/packr  
github.com/gobuffalo/packr/v2  
Licensed under MIT License

### **19.1.79 github.com/karrick/godirwalk**

Copyright (c) 2017, Karrick McDermott  
Licensed under BSD 2-Clause License

### **19.1.80 github.com/rogppe/go-internal**

Copyright (c) 2018 The Go Authors  
Licensed under BSD 3-Clause "New" License

### **19.1.81 github.com/sirupsen/logrus**

Copyright (c) 2014 Simon Eskildsen  
Licensed under MIT License

### **19.1.82 github.com/Workiva/go-datastructures**

(no copyright notes found)  
Licensed under Apache License 2.0

### **19.1.83 github.com/swagger-api/swagger-ui**

Copyright 2020 SmartBear Software Inc.  
Licensed under Apache License 2.0

### **19.1.84 github.com/cheggaaa/pb/v3**

Copyright (c) 2012-2015, Sergey Cherepanov  
Licensed under BSD 3-Clause "New" License

### **19.1.85 [github.com/magefile/mage](https://github.com/magefile/mage)**

Copyright 2017 the Mage authors  
Licensed under Apache License 2.0

### **19.1.86 [github.com/secDre4mer/go-parseflags](https://github.com/secDre4mer/go-parseflags)**

(no copyright notes found)  
Licensed under BSD 3-Clause "New" License

### **19.1.87 [github.com/secDre4mer/go-inject](https://github.com/secDre4mer/go-inject)**

Copyright (c) 2021 secDre4mer  
Licensed under MIT License

## CHANGELOG

In this chapter you can find all the changes of THOR. Current version naming can be found in the index below.

### 20.1 THOR 10.7 (Techpreview)

#### 20.1.1 THOR Version 10.7.14

| Type    | Description                                                                                                                                                                        |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Feature | New <code>--max-reasons</code> flag to limit the shown number of reasons per message. This flag replaces <code>--allreasons</code> , which will still work, but is now deprecated. |
| Bugfix  | Fix an issue where the 32-bit version of THOR for Linux crashed when loading the signatures                                                                                        |
| Bugfix  | Fix an issue where large <code>/etc/hosts</code> files could cause extremely long scan times                                                                                       |
| Bugfix  | Fix an issue where entries in <code>/etc/hosts</code> that mapped multiple hostnames to the same IP address could cause hard-to-read log entries                                   |

#### 20.1.2 THOR Version 10.7.13

| Type    | Description                                                                                                     |
|---------|-----------------------------------------------------------------------------------------------------------------|
| Feature | New <code>--max-hits</code> flag to limit the number of hits per IOC or YARA rule                               |
| Feature | <code>--eventlog-target</code> now supports '*' as a target                                                     |
| Change  | Memory dump files are now scanned with process memory YARA rules rather than the default YARA rules             |
| Change  | Update to Golang v1.20.13                                                                                       |
| Bugfix  | <code>--lab --collector</code> now activates the artifact collector, as intended                                |
| Bugfix  | Fix an issue where THOR could crash during initialization                                                       |
| Bugfix  | Dataless files on MacOS are now ignored                                                                         |
| Bugfix  | Fix an issue where some network drives on Linux were scanned even if <code>--alldrives</code> was not activated |
| Bugfix  | Fix an issue where THOR for Linux could crash in the 'Crontab' module                                           |
| Bugfix  | Fix an issue where some eventlogs could cause a crash in the 'Eventlog' module                                  |
| Bugfix  | Fix an issue where, if an error occurred when reading a file, incorrect file hashes were displayed              |

### 20.1.3 THOR Version 10.7.12

| Type   | Description                                                             |
|--------|-------------------------------------------------------------------------|
| Bugfix | Fix an issue where a high number of mutexes could cause a crash in THOR |

### 20.1.4 THOR Version 10.7.11

| Type   | Description                                                                  |
|--------|------------------------------------------------------------------------------|
| Bugfix | Fix an issue where THOR could hang when scanning specific processes on Linux |

### 20.1.5 THOR Version 10.7.10

| Type    | Description                                                                                                                                                   |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Feature | New <code>--nommap</code> flag to disable memory mapping in features                                                                                          |
| Change  | Remove action feature due to potential abusability                                                                                                            |
| Change  | Update to Golang v1.20.10                                                                                                                                     |
| Change  | SFX RAR executables are now extracted using the Archive feature instead of the ExeDecompress feature, which allows access to the filenames within the archive |
| Bugfix  | Fix an issue where too many open handles on a system could cause a crash                                                                                      |
| Bugfix  | Fix an issue where a scan exit due to the Rescontrol could cause a deadlock                                                                                   |
| Bugfix  | Ensure that data is truncated, even if match strings are unusually large                                                                                      |
| Bugfix  | Fix an issue where the EtwWatcher could crash when finishing                                                                                                  |

### 20.1.6 THOR 10.7.9

| Type   | Description                                                                                                                       |
|--------|-----------------------------------------------------------------------------------------------------------------------------------|
| Change | CPU limit now applies only to full system CPU usage, not only THOR (reverts a change made in 10.7.4)                              |
| Change | If THOR is cancelled by the Rescontrol feature, the information is now displayed as an Error instead of a Warning                 |
| Change | Standardized logging of matches on processes                                                                                      |
| Change | Update to Golang v1.20.6                                                                                                          |
| Change | Update to YARA v4.3.2                                                                                                             |
| Bugfix | Fixed an issue where simultaneous write access from another process to a file that THOR scanned could cause the THOR scan to fail |
| Bugfix | Fixed an issue where old Windows systems could incorrectly be displayed as unpatched                                              |
| Bugfix | Fixed an issue where 'thor-util update' could remove the file type signatures                                                     |



## 20.1.7 THOR 10.7.8

| Type    | Description                                                                                                                                                                                                                                                                             |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Feature | (via THOR Util) log conversion to CSV is now possible                                                                                                                                                                                                                                   |
| Feature | New Artifact Collector module, which allows collection of forensic artifacts from the current system into a ZIP file                                                                                                                                                                    |
| Feature | New <code>--print-signatures-json</code> flag for JSON output of current signatures                                                                                                                                                                                                     |
| Feature | New <code>--init-selector</code> and <code>--init-filter</code> flags which allow the user to load only a subset of the normal signatures                                                                                                                                               |
| Change  | When using <code>--encrypt</code> , log files are now encrypted as they are written during the THOR scan. This prevents temporary log files, but also makes generation of HTML reports afterwards impossible. Use THOR Util instead to generate HTML reports after decrypting the logs. |
| Change  | Display matches on reverse lookup IP addresses in a better way                                                                                                                                                                                                                          |
| Change  | Update to Golang v1.20.5                                                                                                                                                                                                                                                                |
| Change  | Update to OpenSSL 3.0.9                                                                                                                                                                                                                                                                 |
| Bugfix  | Display error messages correctly in JSON logs                                                                                                                                                                                                                                           |
| Bugfix  | On Linux, don't skip directories with children where <code>lstat()</code> fails                                                                                                                                                                                                         |

## 20.1.8 THOR 10.7.7

| Type   | Description                                                                       |
|--------|-----------------------------------------------------------------------------------|
| Change | THOR Lite licenses with Sigma now also have the Eventlog and EVTX modules enabled |

## 20.1.9 THOR 10.7.6

| Type    | Description                                                                                                                                                                                                                       |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Feature | Add <code>--minimum-sigma-level</code> to specify which Sigma rules should trigger a finding. This defaults to high and is reduced to medium in intense mode, which is the current behaviour.                                     |
| Feature | Add <code>--audit-trail</code> for detailed log output of THOR scan trails. This feature is experimental so far, and the output and output format may yet change.                                                                 |
| Feature | Add <code>--background</code> to adjust THOR log level colors to specific backgrounds. Currently, optimizeds for dark and light backgrounds are available.                                                                        |
| Feature | Add <code>--jsonv2</code> which changes the JSON output to better reflect the structure of the log entry, with substructures now properly representing parts of the log entry. This also affects Thunderstorm responses when set. |
| Change  | Increased default value for <code>--yara-stack-size</code> to 32768                                                                                                                                                               |
| Change  | Standardized logging of filename IOC related reasons                                                                                                                                                                              |
| Change  | Update to Golang v1.20.2                                                                                                                                                                                                          |
| Bugfix  | Fix an issue where THOR scans failed due to a perceived symlink loop in the scan path                                                                                                                                             |

## 20.1.10 THOR 10.7.5

| Type    | Description                                                                                                                   |
|---------|-------------------------------------------------------------------------------------------------------------------------------|
| Feature | Add new ETL feature for parsing ETL files                                                                                     |
| Feature | Add <code>--vtkey</code> , <code>--vtmode</code> , and <code>--vtaccepteula</code> flag for integration of VirusTotal in THOR |
| Feature | Improve progress reports when scanning complex files                                                                          |
| Feature | Support Sigma scans with THOR Lite for specific licenses                                                                      |
| Change  | Unify logging fields for many filename IOC, keyword IOC and YARA matches                                                      |
| Change  | Unify logging fields for many messages in the NetworkShares module                                                            |
| Change  | Update to Golang v1.19.5                                                                                                      |
| Change  | Upgrade PE-Sieve to v0.3.5                                                                                                    |
| Change  | <code>--print-signatures</code> now silences the normal initialization output                                                 |
| Change  | Use <code>mimalloc</code> for YARA allocations on Linux and MacOS                                                             |
| Change  | Scanning network paths now requires a Lab license                                                                             |
| Bugfix  | Reduce log level for corrupt <code>/etc/passwd</code> entries from Notice to Info                                             |
| Bugfix  | Identify packed samples correctly with <code>--customonly</code> set                                                          |

## 20.1.11 THOR 10.7.4

| Type    | Description                                                                                                                                                            |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Feature | New OLE feature for extraction of Office macros                                                                                                                        |
| Feature | ExeDecompress feature is now also supported on Linux                                                                                                                   |
| Feature | Added <code>--lowioprio</code> flag for lowered IO priority                                                                                                            |
| Change  | Update to Golang v1.19.2                                                                                                                                               |
| Change  | CPU limit now applies only to THOR's CPU usage, not the the complete system                                                                                            |
| Change  | Windows Access Groups (e.g. in file permissions) are now always displayed in English                                                                                   |
| Change  | Modified the scoring formula to further reduce the impact of multiple subscores on the full score. As compensation, the default threshold for alerts has been reduced. |
| Bugfix  | .lnk file processing with <code>--virtual-map</code> no longer causes link targets to be scanned without applying the virtual mapping                                  |
| Bugfix  | Access faults while reading memory mapped files no longer cause THOR to crash                                                                                          |
| Bugfix  | Panics on opening an archive are now handled properly                                                                                                                  |

### 20.1.12 THOR 10.7.3

| Type    | Description                                                                                                                                                                                                          |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Feature | Meta rule matches with 'FORCE' tag will now cause THOR to ignore the maximum file size for that file                                                                                                                 |
| Feature | Improved matching behaviour of YARA rules on bulks. Scans on bulks (but not scans on single bulk elements) will now use a different YARA ruleset where common false positive constructs (e.g. filesize) are removed. |
| Feature | Improved performance in cases where a rule or IOC matched on a bulk                                                                                                                                                  |
| Feature | Improved memory usage and performance of HTML report generation                                                                                                                                                      |
| Feature | THOR now issues a Notice or Warning for Office connection cache entries                                                                                                                                              |
| Feature | THOR now scans archives (e.g. ZIP files) recursively. This changes how matches in subfiles of archives are reported.                                                                                                 |
| Feature | Added '.cab' support in the 'Archive' feature                                                                                                                                                                        |
| Feature | Added '.gz' support in the 'Archive' feature                                                                                                                                                                         |
| Feature | Added '.7z' support in the 'Archive' feature                                                                                                                                                                         |
| Feature | Added new 'EML' feature for scanning .eml files                                                                                                                                                                      |
| Change  | Increase amount of bytes scanned by meta rules to 2048                                                                                                                                                               |
| Change  | THOR now prefers reading files via memory maps over using the file read API                                                                                                                                          |
| Bugfix  | Improved performance of Sigma rule loading                                                                                                                                                                           |
| Bugfix  | Fixed a bug where THOR scanned some files multiple times, possibly resulting in a loop                                                                                                                               |

### 20.1.13 THOR 10.7.2

| Type    | Description                                              |
|---------|----------------------------------------------------------|
| Feature | Process memory checks are now enabled on Linux and MacOS |
| Feature | Added a check on Linux for deleted executables           |
| Feature | UTF-16 Log files are now parsed correctly                |
| Change  | Upgrade YARA to v4.2.1                                   |

### 20.1.14 THOR 10.7.1

| Type    | Description                                                                                                          |
|---------|----------------------------------------------------------------------------------------------------------------------|
| Feature | Sigma rules are now applied to running processes on the system                                                       |
| Feature | New command line option '-follow-symlinks' that causes the FileScan module to follow symlinks.                       |
| Feature | Checking e.g. log lines from a file with YARA will now set the THOR external variables like 'filepath' appropriately |
| Feature | THOR now shows modules names where string matches were found if a YARA rule matches on process memory                |
| Feature | THOR now shows a warning if low rlimits are detected                                                                 |
| Change  | THOR will now scan processes even in soft mode, with a maximum process size of 250MB.                                |
| Change  | --max_file_size_intense is now deprecated. Instead, --max_file_size should be used.                                  |
| Change  | --virtual-map now supports mounts in subpaths on Windows, e.g. as --virtual-map G:\mount:C                           |
| Change  | Upgrade PE-Sieve to v0.3.3                                                                                           |
| Change  | Filescan progress report for folders without subfolders was improved                                                 |

## 20.1.15 THOR 10.7.0

| Type    | Description                                                                                                     |
|---------|-----------------------------------------------------------------------------------------------------------------|
| Feature | Mark files with names close to common Windows executables as suspicious                                         |
| Feature | Change how score is added to avoid cases where scores added up to absurd values                                 |
| Feature | Support scanning alternate data streams with <code>--ads</code>                                                 |
| Feature | Check environment variables of processes                                                                        |
| Change  | THOR now terminates if a positional argument was specified since none are expected                              |
| Fix     | Scan files written to the Dropzone only once the write is complete (or does not continue for at least 1 second) |

## 20.2 THOR 10.6 (Stable)

### 20.2.1 THOR Version 10.6.24

| Type   | Description                                                                                                  |
|--------|--------------------------------------------------------------------------------------------------------------|
| Bugfix | Fix an issue where <code>--lowprio</code> and <code>--verylowprio</code> were not working correctly on Linux |

### 20.2.2 THOR Version 10.6.23

| Type   | Description                                                                                 |
|--------|---------------------------------------------------------------------------------------------|
| Bugfix | Fix an issue where unicode characters in file names could cause panics                      |
| Bugfix | Fix an issue where corrupt archive files could cause panics                                 |
| Bugfix | Fix an issue where the 32-bit version of THOR for Linux crashed when loading the signatures |
| Bugfix | Fix an issue where the NetworkShares module incorrectly reported an error                   |

### 20.2.3 THOR 10.6.22

| Type   | Description                                                                                                                                                   |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Change | SFX RAR executables are now extracted using the Archive feature instead of the ExeDecompress feature, which allows access to the filenames within the archive |
| Change | Remove action feature due to potential abusability.                                                                                                           |
| Change | Update to Golang v1.20.8                                                                                                                                      |
| Change | Update to OpenSSL v1.1.1w                                                                                                                                     |
| Change | Update to YARA v4.3.2                                                                                                                                         |
| Bugfix | Fix an issue where registry values with new lines could lead to messages missing information about the registry key                                           |

## 20.2.4 THOR 10.6.21

| Type    | Description                                                                                                                  |
|---------|------------------------------------------------------------------------------------------------------------------------------|
| Feature | Add SIGTYPE fields to Sigma matches                                                                                          |
| Feature | Add TYPE fields to reasons                                                                                                   |
| Change  | Update to Golang v1.19.9                                                                                                     |
| Change  | Terminate early when an invalid flag is used in the THOR template file                                                       |
| Change  | Report YARA matches in the DeepDive feature with reasons                                                                     |
| Change  | Increase default YARA stack size to 32768                                                                                    |
| Bugfix  | Don't report filename matches on nonexistent files when resolving the file name from a reference using environment variables |

## 20.2.5 THOR 10.6.20

| Type    | Description                                                                           |
|---------|---------------------------------------------------------------------------------------|
| Feature | Add a warning when running on MacOS without full disk access                          |
| Change  | Update to Golang v1.19.5                                                              |
| Bugfix  | Improve trace output for decompressing EXE files                                      |
| Bugfix  | Exclude MacOS directories used to for cloud storage unless '--alldrives' is specified |
| Bugfix  | Set rule date in '--print-signatures' output to modified date, if available           |
| Bugfix  | Check if file is located remotely before trying to read file stats                    |

## 20.2.6 THOR 10.6.19

| Type   | Description                                                                      |
|--------|----------------------------------------------------------------------------------|
| Change | Update to Golang v1.19.2                                                         |
| Bugfix | Fixed an issue where scans were not properly resumed                             |
| Bugfix | Fixed an issue that caused ASGARD to download THOR even if it was cached locally |

## 20.2.7 THOR 10.6.18

| Type   | Description                                             |
|--------|---------------------------------------------------------|
| Change | Removed some exclusions where archives were not scanned |

## 20.2.8 THOR 10.6.17

| Type   | Description                                            |
|--------|--------------------------------------------------------|
| Change | Errors now appear as the first section in HTML reports |
| Change | Update to YARA v4.2.3                                  |
| Change | Update to Golang v1.18.5                               |

## 20.2.9 THOR 10.6.16

| Type    | Description                                                                                  |
|---------|----------------------------------------------------------------------------------------------|
| Feature | Show Office Connection Cache entries                                                         |
| Change  | Show informational message when downloading a license from Portal or ASGARD                  |
| Change  | Update to Golang v1.18.3                                                                     |
| Change  | Update to YARA v4.2.1                                                                        |
| Change  | Improved HTML report generation performance and HTML report UI                               |
| Change  | Registry YARA rules are now loaded on other platforms than Windows as well (for image scans) |
| Bugfix  | Added MATCHED_STRINGS field to filename IOC matches to improve visibility for complex IOCs   |
| Bugfix  | Fixed an issue where Sigma rules could use a large amount of memory during initialization    |
| Bugfix  | Fixed an issue where Linux services were incorrectly reported as group writable              |
| Bugfix  | Corrected the signature type (custom or internal) for C2 IOC matches on memory               |

## 20.2.10 THOR 10.6.15

| Type    | Description                                                                                                          |
|---------|----------------------------------------------------------------------------------------------------------------------|
| Feature | Added a new 'diagnostics' command for THOR Util that collects information about a hanging or terminated THOR process |
| Feature | Custom process exclude regexps can now be specified in 'config/process-excludes.cfg'                                 |
| Bugfix  | Log messages about suspicious services are now correctly logged as belonging to the 'ServiceCheck' module            |
| Bugfix  | Process excludes are now handled more stringently, and accesses on excluded processes are less intrusive             |
| Bugfix  | Scan end time no longer sometimes misses from the HTML report                                                        |
| Change  | Matches from deprecated sigma rules are no longer shown                                                              |
| Change  | Upgrade of the sigma matching engine from v1 to v2                                                                   |
| Change  | Update to Golang v1.17.9                                                                                             |
| Change  | Update to PE-Sieve v0.3.3                                                                                            |
| Change  | Default maximum file size increased to 30 MB (200 MB for intense mode)                                               |

### 20.2.11 THOR 10.6.14

| Type   | Description                                              |
|--------|----------------------------------------------------------|
| Bugfix | The Bifrost 2 server option is again available in ASGARD |

### 20.2.12 THOR 10.6.13

| Type   | Description                                                                                                                                           |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| Bugfix | Some YARA rules were not applied correctly on unpacked files                                                                                          |
| Bugfix | Catch panics that could occur when unpacking certain RAR files                                                                                        |
| Bugfix | THOR no longer attempts to access files that are not local (e.g. OneDrive files) when they are referenced from elsewhere unless '--alldrives' is used |

### 20.2.13 THOR 10.6.12

| Type    | Description                                                                                        |
|---------|----------------------------------------------------------------------------------------------------|
| Feature | Executing 32 bit THOR on a 64 bit Windows system now causes a warning                              |
| Feature | Hash IOCs may now have an optional score (default is 100, as before)                               |
| Change  | Disable RarVM support                                                                              |
| Change  | Change colors for some log levels to improve readability in specific terminals                     |
| Change  | THOR Util can no longer download licenses from ASGARD, use THOR instead                            |
| Change  | THOR now terminates if the internal signatures can't be loaded                                     |
| Change  | Intrusive process actions that require process memory access are now skipped on excluded processes |
| Change  | THOR Lite Util no longer supports '--force' for upgrades and updates                               |
| Change  | Update to Golang v1.16.13                                                                          |
| Bugfix  | Process dumps are now created with secure access rights                                            |

### 20.2.14 THOR 10.6.11

| Type    | Description                                    |
|---------|------------------------------------------------|
| Feature | Support Apple M1                               |
| Feature | Save resume state on system shutdown or logoff |
| Change  | Upgrade PE-Sieve to v0.3.1                     |
| Change  | Upgrade OpenSSL to v1.1.11                     |

## 20.2.15 THOR 10.6.10

| Type   | Description                                      |
|--------|--------------------------------------------------|
| Change | Update to Golang v1.16.7                         |
| Bugfix | Show process details for PPL processes correctly |

## 20.2.16 THOR 10.6.9

| Type    | Description                                                                      |
|---------|----------------------------------------------------------------------------------|
| Feature | Print rule authors for YARA rule matches                                         |
| Feature | Check environment variables for other processes                                  |
| Feature | Use Administrator rights on Windows, if available                                |
| Change  | Upgrade PE-Sieve to v0.3.0                                                       |
| Fix     | Handle UTF-16 output in string matches better                                    |
| Fix     | Improve progress estimation for Eventlog module                                  |
| Fix     | Skip non-local files on Windows (from e.g. OneDrive) unless '--alldrives' is set |

## 20.2.17 THOR 10.6.8

| Type    | Description                                                                                                                                                                                                                                                                         |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Feature | Analyze ETW logs in the background for CobaltStrike beacon characteristics. This can be disabled with '--noetwwatcher'.                                                                                                                                                             |
| Feature | Check IP forwarding on Linux as part of the Firewall module.                                                                                                                                                                                                                        |
| Feature | Analyze authorized_keys files that are found. This feature can be disabled with '--noauthorizedkeys'.                                                                                                                                                                               |
| Feature | Support metadata YARA rules which are applied to all files, but can only access the first 100 bytes of the file. These files must contain the "meta" word in their filename. If a Metadata YARA rule with the DEEPSCAN tag matches, a full YARA scan on the file will be triggered. |
| Feature | Add the "group" external variable to YARA rules for non-Windows scans.                                                                                                                                                                                                              |
| Change  | Upgrade YARA to v4.1.1                                                                                                                                                                                                                                                              |
| Change  | Print more timestamps for deep dive targets                                                                                                                                                                                                                                         |
| Change  | Disable global YARA rules since they could impact THOR's internal rules                                                                                                                                                                                                             |
| Fix     | Handle a bug where THOR froze when calculating the hash of a file opened via the MFT                                                                                                                                                                                                |

## 20.2.18 THOR 10.6.7

| Type   | Description                                           |
|--------|-------------------------------------------------------|
| Bugfix | Apply cross platform IOCs correctly if '--lab' is set |
| Bugfix | Don't scan specific files twice if '--lab' is set     |



## 20.2.19 THOR 10.6.6

| Type     | Description                                                                                                                                              |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Upstream | Merge current changes from THOR 10.5.16                                                                                                                  |
| Feature  | Scanning for symlinks and irregular files with Filename IOCs                                                                                             |
| Feature  | YARA Meta rules (filename needs to contain the word meta) which are applied on all files, but which only can access the first 100 Bytes of the file      |
| Feature  | Improve Scheduled Task parsing and give a notice if a task's binary does not exist                                                                       |
| Feature  | Parse Cobalt Strike beacon configurations and return basic information about them                                                                        |
| Feature  | New command line option '--allfiles' that includes file types and locations that are usually not interesting. This is a subset of what '--intense' does. |
| Change   | Upgrade PE-Sieve to v0.2.9.6                                                                                                                             |
| Change   | Disable quick edit mode for a Windows console while THOR is running in it                                                                                |
| Change   | Update to Golang 1.15.11                                                                                                                                 |
| Bugfix   | Fix some issues with using THOR Util templates                                                                                                           |

## 20.2.20 THOR 10.6.5

| Type     | Description                                                                                                      |
|----------|------------------------------------------------------------------------------------------------------------------|
| Upstream | Merge changes from THOR 10.5.15                                                                                  |
| Change   | Multithreading and virtual mapping have been restricted to Forensic Lab and Incident Response license types      |
| Change   | THOR TechPreview packages now contain a THOR Util configuration file to default to the Tech-Preview on upgrades. |

## 20.3 THOR 10.5 (Legacy)

### 20.3.1 THOR 10.5.18

| Type   | Description                                                    |
|--------|----------------------------------------------------------------|
| Change | Remove outdated content from the tools folder in THOR packages |
| Bugfix | Exclude THOR logs from being detected by THOR                  |

### 20.3.2 THOR 10.5.17

| Type    | Description                                                                                         |
|---------|-----------------------------------------------------------------------------------------------------|
| Feature | Authors of YARA rules are now included in match outputs                                             |
| Change  | Update PE-Sieve to v0.2.9.6                                                                         |
| Change  | Global YARA rules now cause an error since they can inadvertently affect THOR's internal signatures |
| Change  | Some modules were removed on specific platforms (especially on MacOS and AIX) that only held dummy  |
| Change  | Add EVTX 3.2 support                                                                                |
| Bugfix  | Print Eventlog timestamps in local timezone, unless '--utc' is used                                 |

### 20.3.3 THOR 10.5.16

| Type   | Description                                   |
|--------|-----------------------------------------------|
| Change | Upgrade PE-Sieve to v0.2.9.5                  |
| Change | Upgrade OpenSSL to 1.1.1j                     |
| Bugfix | Ensure THOR honors low CPU limits correctly   |
| Bugfix | Correct loading for some named pipe IOC files |
| Bugfix | Incorrect formatting for JSON syslog output   |

### 20.3.4 THOR 10.5.15

| Type    | Description                                                                                                                                   |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| Feature | Add support for a THOR Util configuration file. This file allows setting a default configuration (e.g. to always upgrade to the TechPreview). |
| Change  | Notarize THOR for MacOS                                                                                                                       |

### 20.3.5 THOR 10.5.14

| Type    | Description                                                                                                                                                        |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Feature | Scan all event logs if '--intense' was specified                                                                                                                   |
| Feature | Allow fetching the signatures in development by using '--sigdev' with thor-util update                                                                             |
| Change  | Add info resource to THOR Windows files                                                                                                                            |
| Change  | Refactor bulk scanning to have less memory allocated / released to reduce memory usage volatility                                                                  |
| Change  | Let THOR Util default to its own directory for THOR and license paths (same behaviour as THOR already has)                                                         |
| Change  | Check YARA / IOC filename indicators (like log, registry, keyword) with word boundaries                                                                            |
| Change  | Add additional event logs to list scanned by default                                                                                                               |
| Change  | Don't allow a downgrade in THOR Util unless '--force' is specified                                                                                                 |
| Change  | Update to Golang 1.15.10                                                                                                                                           |
| Change  | Specific options (dropzone mode, deep dive mode, fsonly, nodoublecheck, hostname rewrite) have been restricted to Forensic Lab and Incident Response license types |
| Bugfix  | Add checks for improved handling of corrupted registry hives                                                                                                       |
| Bugfix  | Clarify some messages of THOR Util                                                                                                                                 |
| Bugfix  | Apply excludes with OS path separators with '--cross-platform'                                                                                                     |

### 20.3.6 THOR 10.5.13

| Type   | Description                                                  |
|--------|--------------------------------------------------------------|
| Change | Minor directory exclusion adjustments for Microsoft Exchange |

### 20.3.7 THOR 10.5.12

| Type   | Description                                                   |
|--------|---------------------------------------------------------------|
| Bugfix | Remove some directory excludes specific to Microsoft Exchange |

### 20.3.8 THOR 10.5.11

| Type    | Description                                                                       |
|---------|-----------------------------------------------------------------------------------|
| Feature | Make bulk scan size manually configurable with '--bulk-size'                      |
| Change  | Disable 60 MB log size limit if debugging (with '--debug' or '--trace') is active |

### 20.3.9 THOR 10.5.10

| Type    | Description                                                                                                               |
|---------|---------------------------------------------------------------------------------------------------------------------------|
| Feature | Suppress rule matches on log files after the same rule matched 10 times or more, this can be deactivated with '--showall' |
| Feature | Add a context menu for filtering to the HTML reports                                                                      |
| Feature | Add support for NFTables firewalls on Linux                                                                               |
| Feature | Add a field 'SIGTYPE' to messages which displays whether an IOC or YARA rule is custom or built-in                        |
| Feature | Reuse previous Scan ID if a scan is resumed                                                                               |
| Feature | Add additional information to files detected in a Windows recycle bin (original file name, deletion time)                 |
| Change  | Limit file enrichment to 10 files per message                                                                             |
| Change  | Name automatically generated YARA rules for C2 domains after the domain rather than after a counter                       |
| Change  | Reduce score of a C2 match with a YARA rule by 30                                                                         |
| Change  | Upgrade to YARA 4.0.5                                                                                                     |
| Change  | Make matching of C2 IOCs on process memory optional, it can be enabled with '--c2-in-memory'                              |
| Bugfix  | Deduplicate listen ports per process                                                                                      |
| Bugfix  | Improve permission vulnerability check for Linux services                                                                 |
| Bugfix  | Skip specific registry hives where THOR could behave unstable                                                             |

### 20.3.10 THOR 10.5.9

| Type    | Description                                                                               |
|---------|-------------------------------------------------------------------------------------------|
| Feature | Apply C2 checks to log scans                                                              |
| Change  | Increase the default maximum runtime to 1 week                                            |
| Change  | Apply special scan features on files even if those files exceed the maximum file size set |
| Bugfix  | Remove several false positives on process memory of Antivirus products                    |
| Bugfix  | Fix an issue where THOR Remote could freeze if too many remote scans were started         |
| Bugfix  | Fix an issue where packed files weren't unpacked completely before being scanned          |

### 20.3.11 THOR 10.5.8

| Type   | Description                                               |
|--------|-----------------------------------------------------------|
| Bugfix | Print time of currently analyzed event in Eventlog module |

### 20.3.12 THOR 10.5.7

| Type   | Description                                                                                                                                                                            |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Change | Upgrade to Golang 1.14.7                                                                                                                                                               |
| Change | Catch Panics in a Module to leave other modules unaffected                                                                                                                             |
| Change | Disable support for licenses using an obsolete encryption method                                                                                                                       |
| Bugfix | Extend output in a specific Events module message                                                                                                                                      |
| Bugfix | New parameter '--max_process_size' that limits the size of processes that THOR scans with YARA rules. Default value is 500 MB. THOR memory usage increases as this value is increased. |

### 20.3.13 THOR 10.5.6

| Type   | Description                                                          |
|--------|----------------------------------------------------------------------|
| Bugfix | Catch possible panic during Amcache parsing                          |
| Bugfix | Catch possible panic if the Application Eventlog could not be opened |

### 20.3.14 THOR 10.5.5

| Type   | Description                                                             |
|--------|-------------------------------------------------------------------------|
| Change | Exchange signing certificate for newer                                  |
| Bugfix | Check Registry Hive entries in the same format as Live Registry entries |
| Bugfix | Check UserData elements in EVTX files                                   |

### 20.3.15 THOR 10.5.4

| Type    | Description                                                                                                            |
|---------|------------------------------------------------------------------------------------------------------------------------|
| Feature | Support download of Tech Previews in Thor-Util                                                                         |
| Feature | Support license download from ASGARD 2.5+ with '--asgard-token'                                                        |
| Bugfix  | Terminate if started with '--resumeonly' and no previous scan with the same context existed                            |
| Bugfix  | Calculate the context that '--resume' used to check for previous scans differently, excluding elements prone to change |

### 20.3.16 THOR 10.5.3

| Type   | Description                                                |
|--------|------------------------------------------------------------|
| Bugfix | Catch Panic when handling specific Registry Hives on disk. |

### 20.3.17 THOR 10.5.2

| Type   | Description                                                                                                                |
|--------|----------------------------------------------------------------------------------------------------------------------------|
| Bugfix | Disable PE-Sieve by default to follow up on some rare issues. It can be enabled with '--process-integrity' or '--intense'. |

### 20.3.18 THOR 10.5.1

| Type    | Description                                                                                                       |
|---------|-------------------------------------------------------------------------------------------------------------------|
| Feature | Generate process dumps of suspicious processes (for now Windows only) when '--procdumps' is specified             |
| Feature | New command line option '--procdump-dir' to control where process dumps are stored                                |
| Feature | Integrate parser for Windows LNK files                                                                            |
| Feature | New command line option '--image-chunk-size' to set the size of chunks when scanning image files                  |
| Feature | New command line option '--generate-config' to create a configuration file for THOR based on command line options |
| Feature | Open busy registry hives using a raw disk image and the MFT                                                       |
| Feature | On interactive interrupts, show progress and a menu to continue or abort the scan                                 |
| Feature | Support new IOC file for named pipes on Windows                                                                   |
| Feature | Detect files with uncommon / unlikely timestamps (timestomping)                                                   |
| Change  | Reduce log level for open port messages to Info                                                                   |
| Change  | Extend '--all-module-lookback' to Registry Hive files and EVTX log files, rename it to '--global-lookback'        |
| Change  | Update used YARA to 4.0.1                                                                                         |
| Change  | Print last scanned element when maximum runtime is exceeded                                                       |
| Bugfix  | Don't stop HTML log generation on encountering certain uncommon log lines                                         |

### 20.3.19 THOR 10.5.0

| Type    | Description                                                                                                                               |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------|
| Feature | New PowerShell script to download and run Thor easily                                                                                     |
| Feature | Execute PE-Sieve at runtime to discover processes with malicious sections, sensitivity can be raised further with '--full-proc-integrity' |
| Feature | New command line option '--scanid-prefix' to set a custom Scan ID prefix                                                                  |
| Feature | New command line option '--print-signatures' to print metadata to all YARA and Sigma signatures                                           |
| Feature | New command line option '--all-module-lookback' that applies lookback to the Filesystem, Registry, and Services modules as well           |
| Feature | Make score for Handle IOCs customizable                                                                                                   |
| Feature | New command line option '--ascii' to exclude non-ASCII characters from the logs                                                           |
| Change  | Check open files without using an external 'lsuf' executable on Unix platforms                                                            |
| Change  | Update descriptions for most command line options                                                                                         |
| Change  | Print non-ASCII strings in matches as hex sequences                                                                                       |
| Change  | Include time (in addition to the date) in default log file name                                                                           |

## 20.4 THOR 10.4

### 20.4.1 THOR 10.4.2

| Type    | Description                                                                                    |
|---------|------------------------------------------------------------------------------------------------|
| Feature | Store resume information only if '--resume' is set to improve performance                      |
| Feature | New command line option '--portal-key' to download a license at start time                     |
| Feature | New command line option '--yara-max-strings-per-rule' to increase the supported number of IOCs |
| Feature | New command line option '--nofserrors' to suppress filesystem errors                           |
| Feature | Print integrated revision of the sigma rules at startup                                        |
| Feature | Include Scan ID in HTML report synopsis                                                        |
| Change  | Apply suspicious locations platform independently                                              |
| Bugfix  | Don't stop HTML log generation on encountering certain uncommon log lines                      |
| Bugfix  | Remove anonymization on non-personal accounts like Default                                     |
| Bugfix  | Apply Signatures for Windows Handles more precisely                                            |
| Bugfix  | Remove a False Positive that could occur in the DNS cache                                      |
| Bugfix  | Increase the supported number of IOCs massively beyond the default 10000.                      |
| Bugfix  | Fix a panic related to incorrectly formatted /etc/passwd files on Linux.                       |

### 20.4.2 THOR 10.4.1

| Type   | Description                                        |
|--------|----------------------------------------------------|
| Bugfix | Filescan panic on WER (Windows Error Report) files |

### 20.4.3 THOR 10.4.0

| Type    | Description                                        |
|---------|----------------------------------------------------|
| Feature | Added Bifrost 2 gRPC support for upcoming ASGARD 2 |
| Feature | EmoCheck in FileScan module                        |
| Feature | TeamViewer password detection and decryption       |

## 20.5 THOR 10.3

### 20.5.1 THOR 10.3.1

| Type   | Description                                                 |
|--------|-------------------------------------------------------------|
| Bugfix | Files mentioned in Archivescan do not show up in CSV export |

## 20.5.2 THOR 10.3.0

| Type    | Description                                                                            |
|---------|----------------------------------------------------------------------------------------|
| Feature | Iterate over process handles (files, events, mutants) natively without external tools  |
| Feature | Automatically set a random Scan ID that will be added to each log line                 |
| Feature | Log to local syslog with '--local-syslog' (Linux and macOS only)                       |
| Feature | SHIMCache entries will be scanned in Registry Hive files, too                          |
| Feature | Do not skip registry paths with low relevance by using '--fullregistry' or '--intense' |
| Feature | New license type 'Silent' for rollout / deployment testing                             |
| Feature | Cross-platform filename IOCs in '--fsonly' mode (or with flag '--cross-platform')      |
| Feature | New exclude configurations 'registry-excludes.cfg' and 'eventlog-excludes.cfg'         |
| Feature | Enrich process information for event and mutant handles                                |
| Feature | Apply regexes on event and mutant handles                                              |
| Feature | Added few more eventlog targets                                                        |
| Feature | New flag '--process <pid>' to scan a specific process                                  |
| Change  | Added comment to users' last logon date                                                |
| Change  | Enrich file information in process check output                                        |
| Change  | New flag '--max_file_size_intense' to set max file size for intense mode separately    |
| Change  | Removed flag '--buffer_size'. THOR's buffer will now be as big as '--max_file_size'    |
| Change  | Added YARA rules' date to match output                                                 |
| Change  | Upgraded THOR Util to 1.9.8                                                            |
| Change  | Wordings in flag descriptions                                                          |
| Change  | Duplicates in IOCs will be filtered automatically                                      |
| Bugfix  | '-j <hostname>' will also rewrite names of THOR's logfiles                             |
| Bugfix  | Fixed sporadically missing start- and endtime in html report                           |
| Bugfix  | Fixed off-by-one error for '--maxloglines' flag                                        |
| Bugfix  | Skip directory junctions when scanning remotely mounted windows ntfs partitions        |
| Bugfix  | Fixed interaction of relevant file extensions and some file types                      |

## 20.6 THOR 10.2

### 20.6.1 THOR 10.2.11

| Type    | Description                                                   |
|---------|---------------------------------------------------------------|
| Feature | Sigma modifiers "startswith" and "endswith" are now supported |

### 20.6.2 THOR 10.2.10

| Type   | Description                                                  |
|--------|--------------------------------------------------------------|
| Bugfix | Empty values for "(Default)" keys names in Registry matching |



### 20.6.3 THOR 10.2.9

| Type   | Description                                                                                                                      |
|--------|----------------------------------------------------------------------------------------------------------------------------------|
| Change | Removed legacy files (sfx, bat)                                                                                                  |
| Change | Removed fix skip of "SOFTWAREClasses" Registry key                                                                               |
| Bugfix | custom IOC initialization used different keywords than described in documentation ("c2" > "domain", "trusted" > "falsepositive") |

### 20.6.4 THOR 10.2.8

| Type   | Description                                            |
|--------|--------------------------------------------------------|
| Change | Increased default max. file size from 4.5 MB to 6.5 MB |
| Bugfix | Fixed a bug in sigma scoring system                    |

### 20.6.5 THOR 10.2.7

| Type   | Description                                                                                                                              |
|--------|------------------------------------------------------------------------------------------------------------------------------------------|
| Change | Dropped max filesize check for many types in intense scan mode (--intense / --fsonly) including memory dumps, registry hives, EVTX files |
| Change | Added PKZIP and MS Office PK header to headers eligible for archive scan                                                                 |
| Change | Added file name, file path, hostname and channel to matches on events found in EVTX files                                                |

### 20.6.6 THOR 10.2.6

| Type   | Description                                         |
|--------|-----------------------------------------------------|
| Change | Improvements to MESSAGE field (better descriptions) |

### 20.6.7 THOR 10.2.5

| Type   | Description                                               |
|--------|-----------------------------------------------------------|
| Change | List available modules if selected module is unknown      |
| Change | Increased log window size for thor events in thor remote  |
| Change | Print reasons for invalid licenses                        |
| Change | Sigma rules will be muted if they matched too often       |
| Change | Event IOCs will be applied on Mutex checks and vice versa |

## 20.6.8 THOR 10.2.4

| Type   | Description                                                        |
|--------|--------------------------------------------------------------------|
| Bugfix | Fixed logic error in lsasessions' kerberos ticket life time checks |

## 20.6.9 THOR 10.2.3

| Type   | Description                                                                                              |
|--------|----------------------------------------------------------------------------------------------------------|
| Change | Removed THOR Remote warning that a file could not be collected, which doesn't exist                      |
| Change | Low sigma rules will not be printed anymore, medium sigma rules will only be printed in '--intense' mode |

## 20.6.10 THOR 10.2.2

| Type    | Description                                                  |
|---------|--------------------------------------------------------------|
| Feature | New module 'Events' that checks for malicious Windows events |

## 20.6.11 THOR 10.2.1

| Type    | Description                                                                 |
|---------|-----------------------------------------------------------------------------|
| Feature | New ThorDB table 'stats', which contains scan duration of scan elements     |
| Feature | New output mode '--reduced' to reduce output to warnings, alerts and errors |
| Change  | Files can be scanned multiple times in Dropzone mode                        |

## 20.6.12 THOR 10.2.0

| Type   | Description                                                                       |
|--------|-----------------------------------------------------------------------------------|
| Change | Upgraded YARA to 3.11.0                                                           |
| Change | Extended output of '--version' command                                            |
| Change | Added ExecFlag to SHIMCache output                                                |
| Change | Apply YARA on WMI Event Filters                                                   |
| Change | Passing new external YARA variables 'timezone' and 'language' to registry ruleset |

## 20.7 THOR 10.1

### 20.7.1 THOR 10.1.9

| Type   | Description                                                                                 |
|--------|---------------------------------------------------------------------------------------------|
| Change | Made YARA more robust - YARA rules will now compile even if there is a duplicate identifier |
| Change | Made Sigma more robust - Sigma rules will now compile even if a rule is corrupt             |
| Change | Removed challenge-response for trial licenses that are host-based                           |
| Change | Updated file types that will trigger a warning if cloaked                                   |

### 20.7.2 THOR 10.1.8

| Type   | Description                                      |
|--------|--------------------------------------------------|
| Change | Reverting case-insensitive filename IOC checking |
| Docs   | New manual (fixed broken references)             |

### 20.7.3 THOR 10.1.7

| Type   | Description                                 |
|--------|---------------------------------------------|
| Change | Crash reports are not truncated anymore     |
| Bugfix | Improved stability of ScheduledTasks module |

### 20.7.4 THOR 10.1.6

| Type   | Description                       |
|--------|-----------------------------------|
| Change | Improved Sigma initialization     |
| Change | Improved THOR Lite initialization |

### 20.7.5 THOR 10.1.5

| Type    | Description                     |
|---------|---------------------------------|
| Feature | THOR Lite (replaces SPARK Core) |

## 20.7.6 THOR 10.1.4

| Type   | Description                                                                        |
|--------|------------------------------------------------------------------------------------|
| Change | Add <code>https://</code> protocol to ' <code>--bifrost2Server</code> ' if missing |

## 20.7.7 THOR 10.1.3

| Type    | Description                                                                                         |
|---------|-----------------------------------------------------------------------------------------------------|
| Feature | New flag ' <code>--bifrost2Ignore &lt;pattern&gt;</code> ' to specify ignore patterns for Bifrost 2 |

## 20.7.8 THOR 10.1.2

| Type   | Description                                      |
|--------|--------------------------------------------------|
| Change | Wordings in ' <code>--help</code> ' section      |
| Bugfix | Fixed THOR crash when scanning corrupt EVTX file |

## 20.7.9 THOR 10.1.1

| Type    | Description                                                                                            |
|---------|--------------------------------------------------------------------------------------------------------|
| Feature | New flags ' <code>--ca &lt;path&gt;</code> ' and ' <code>--insecure</code> ' for tls host verification |
| Feature | HTTP proxy support for Bifrost 2 and license generation with ASGARD                                    |

## 20.7.10 THOR 10.1.0

| Type    | Description                                                      |
|---------|------------------------------------------------------------------|
| Feature | THOR Remote for Windows                                          |
| Feature | Bifrost 2                                                        |
| Feature | Sigma value modifiers (contains, base64, re, ...)                |
| Bugfix  | Fixed file descriptor leak in PE imphash calculation             |
| Bugfix  | Fixed "has admin rights" output when running with different EUID |
| Bugfix  | Wrong eventtime in WER module output                             |

## 20.8 THOR 10.0

### 20.8.1 THOR 10.0.14

| Type   | Description                                                       |
|--------|-------------------------------------------------------------------|
| Bugfix | Ignore filepaths of archives when scanning the contents with YARA |

### 20.8.2 THOR 10.0.13

| Type   | Description                                              |
|--------|----------------------------------------------------------|
| Bugfix | Fixes in exclusions and firewall indicator regex filters |

### 20.8.3 THOR 10.0.12

| Type   | Description                                |
|--------|--------------------------------------------|
| Bugfix | Fixed obfuscated exclusion and apt presets |

### 20.8.4 THOR 10.0.11

| Type   | Description                        |
|--------|------------------------------------|
| Change | ZEUS port detection regex adjusted |

### 20.8.5 THOR 10.0.10

| Type   | Description                            |
|--------|----------------------------------------|
| Change | More process excludes (OneDrive issue) |

### 20.8.6 THOR 10.0.9

| Type   | Description                                                 |
|--------|-------------------------------------------------------------|
| Change | Adjusted process excludes list (Windows Defender, OneDrive) |

## 20.8.7 THOR 10.0.8

| Type   | Description                                                           |
|--------|-----------------------------------------------------------------------|
| Change | Adjusted suspicious locations to avoid some SHIMCache false positives |

## 20.8.8 THOR 10.0.7

| Type   | Description                                                                                     |
|--------|-------------------------------------------------------------------------------------------------|
| Bugfix | Eventlog module deactivation disfunctional ( <code>--noeventlog</code> , <code>--quick</code> ) |

## 20.8.9 THOR 10.0.6

| Type    | Description                                                                                                                                                                                                                                                                         |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Feature | Linux and MacOS support                                                                                                                                                                                                                                                             |
| Feature | Scan eventlog and logfiles with Sigma                                                                                                                                                                                                                                               |
| Feature | STIX v2 in various checks and modules                                                                                                                                                                                                                                               |
| Feature | Log to JSON file, send JSON via UDP/TCP                                                                                                                                                                                                                                             |
| Feature | Scan templates '-t <template-file>' that holds preset command line arguments                                                                                                                                                                                                        |
| Feature | Get license from ASGARD with ' <code>--asgard &lt;host&gt;</code> '                                                                                                                                                                                                                 |
| Change  | Update signatures with <i>thor-util update</i>                                                                                                                                                                                                                                      |
| Change  | Upgrade scanner with <i>thor-util upgrade</i>                                                                                                                                                                                                                                       |
| Change  | Changed programming language from Python to Golang                                                                                                                                                                                                                                  |
| Change  | Configure actions with command line arguments ' <code>--action-command &lt;cmd&gt;</code> ', ' <code>--action-args &lt;argN&gt;</code> ' and ' <code>--action-level &lt;level&gt;</code> '                                                                                          |
| Change  | Encrypt (RSA) scan results with ' <code>--encrypt</code> ', use custom key (or key file) with ' <code>--pubkey &lt;key file&gt;</code> '                                                                                                                                            |
| Change  | Removed obsolete 'thor-upgrade.exe' tool                                                                                                                                                                                                                                            |
| Change  | THOR doesn't require SYSINTERNALS 'autorunsc.exe' in tools directory anymore                                                                                                                                                                                                        |
| Change  | Removed obsolete fast mode ' <code>--fast</code> '                                                                                                                                                                                                                                  |
| Change  | Command line arguments with multiple values can not be appended anymore, they require a key in front of each value<br>Example: ' <code>-p &lt;path1&gt; -p &lt;path2&gt; ... -p &lt;pathN&gt;</code> ' instead of ' <code>-p &lt;path1&gt; &lt;path2&gt; ... &lt;pathN&gt;</code> ' |
| Change  | Short command line arguments with more than one character were removed. E.g. ' <code>-em &lt;days&gt;</code> ', use ' <code>--lookback &lt;days&gt;</code> ' instead                                                                                                                |
| Change  | Removed log caching in ThorDB                                                                                                                                                                                                                                                       |

## INDICES AND TABLES

- search