THOR Util Manual

Nextron Systems GmbH

Apr 02, 2024

CONTENTS:

CHAPTER ONE

WHAT IS THOR UTIL?

THOR Util is the swiss-army knife with many maintenance features like update, download and license fetching. But it also supports executable signature verification, custom signature encryption, report generation and diagnostics for troubleshooting THOR scans.

CHAPTER

TWO

UPGRADE (UPGRADE) AND UPDATES (UPDATE)

You can download updates for THOR with `thor-util.exe` (Windows) or `thor-util` (Linux, macOS).

Running `thor-util --help` shows three options that seem to have a very similar meaning: "upgrade", "update" and "download".

The difference is that the "download" option downloads a full pack with all config files while the "upgrade" option fetches a full package but excludes the config files to avoid accidental overwrites of local config files (like: `thor.yml`, `falsepositive_filters.cfg`, etc.).

The "update" option retrieves only the newest signature pack (not the program files).

Option	Description
upgrade	Get new program files and signatures
update	Get new signatures
download	Get new program files, signatures and config files

If you have a full program package present, you should use the "upgrade" option.

Every other option has its own help. You can see the help of each option with

```
user@unix:~/thor$ ./thor-util *option* --help
```

The following examples show different upgrade methods.

```
C:\thor>thor-util.exe upgrade
C:\thor>thor-util.exe upgrade -a https://proxy.company.net:8080
C:\thor>thor-util.exe upgrade -a https://proxy.company.net:8080 -n dom\\user -p password
C:\thor>thor-util.exe upgrade -a https://proxy.local:8080 --ntlm -n dom\\user -p password
```

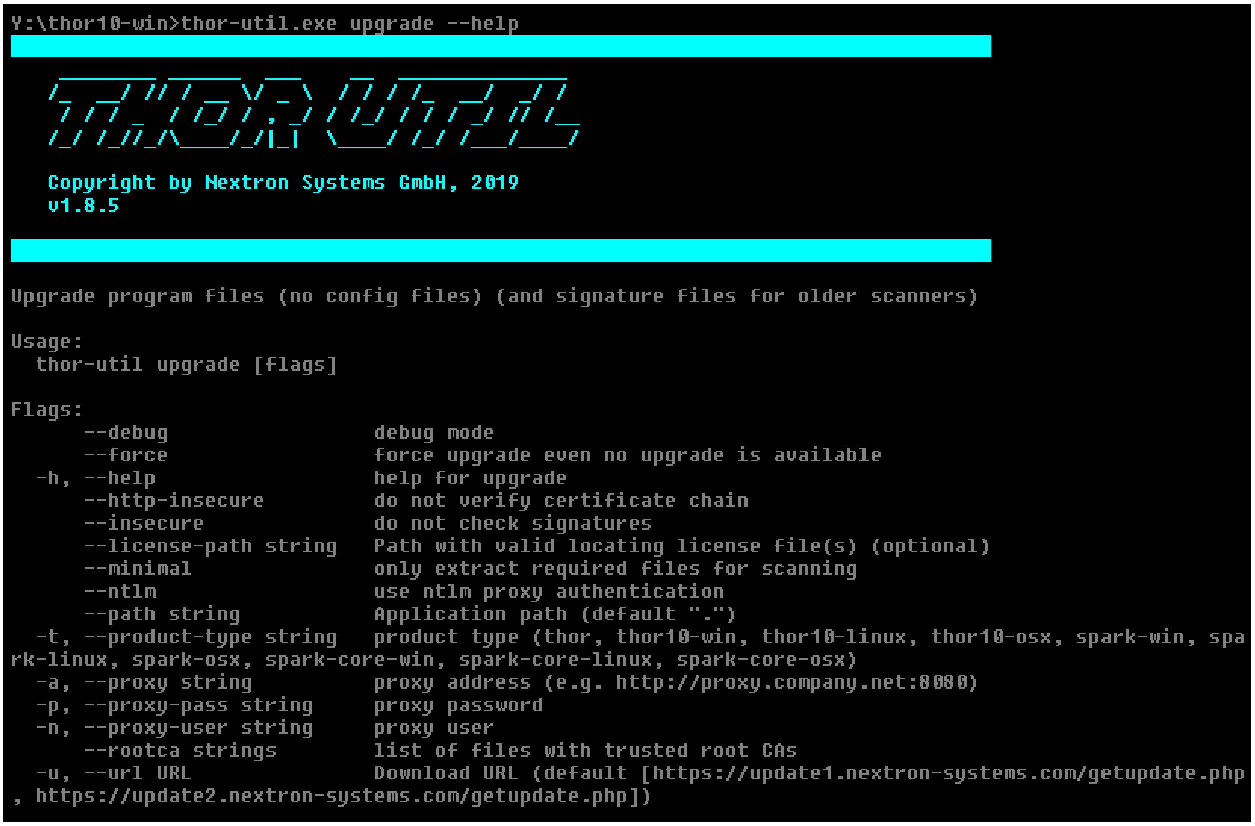
2.1 THOR TechPreview Version

To upgrade your current version to the TechPreview version, use the following command:

```
C:\thor>thor-util.exe upgrade --techpreview
```

You can find more information on the TechPreview version here.

Hint: To make the TechPreview version persistent, consider adding it to your THOR Util configuration file (`thor-util.yml`). Please see *TechPreview configuration*.



```
Y:\thor10-win>thor-util.exe upgrade --help

     _______ _______ ____     __  ___________
   /_  __/ // /  __ \/ _ \   / / / /_  __/  _/ /
    / / / _  / /_/ / ,  _/ / /_/ / / / / _/ // /__
   /_/ /_//_/\____/_/|_|   \____/ /_/ /___/____/

   Copyright by Nextron Systems GmbH, 2019
   v1.8.5


Upgrade program files (no config files) (and signature files for older scanners)

Usage:
  thor-util upgrade [flags]

Flags:
      --debug                 debug mode
      --force                 force upgrade even no upgrade is available
  -h, --help                  help for upgrade
      --http-insecure         do not verify certificate chain
      --insecure              do not check signatures
      --license-path string   Path with valid locating license file(s) (optional)
      --minimal               only extract required files for scanning
      --ntlm                  use ntlm proxy authentication
      --path string           Application path (default ".")
  -t, --product-type string   product type (thor, thor10-win, thor10-linux, thor10-osx, spark-win, spa
rk-linux, spark-osx, spark-core-win, spark-core-linux, spark-core-osx)
  -a, --proxy string          proxy address (e.g. http://proxy.company.net:8080)
  -p, --proxy-pass string     proxy password
  -n, --proxy-user string     proxy user
      --rootca strings        list of files with trusted root CAs
  -u, --url URL               Download URL (default [https://update1.nextron-systems.com/getupdate.php
, https://update2.nextron-systems.com/getupdate.php])
```

Fig. 1: THOR-util Upgrade Help

2.2 Update Locations

When using the full version of THOR, the following servers are used as update mirrors and should be accessible via HTTPS:

```
update1.nextron-systems.com
update2.nextron-systems.com
```

When using THOR Lite, the following server is used instead and should be accessible:

```
update-lite.nextron-systems.com
```

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

2.3 SigDev Signatures

Usually it takes our internal testing 1-2 days to verify the quality of new rules. In rare cases in which a new and severe threat has been discovered it could make sense to use the newest and untested signatures that are still in our testing process. (e.g. new vulnerability and public proof-of-concept code)

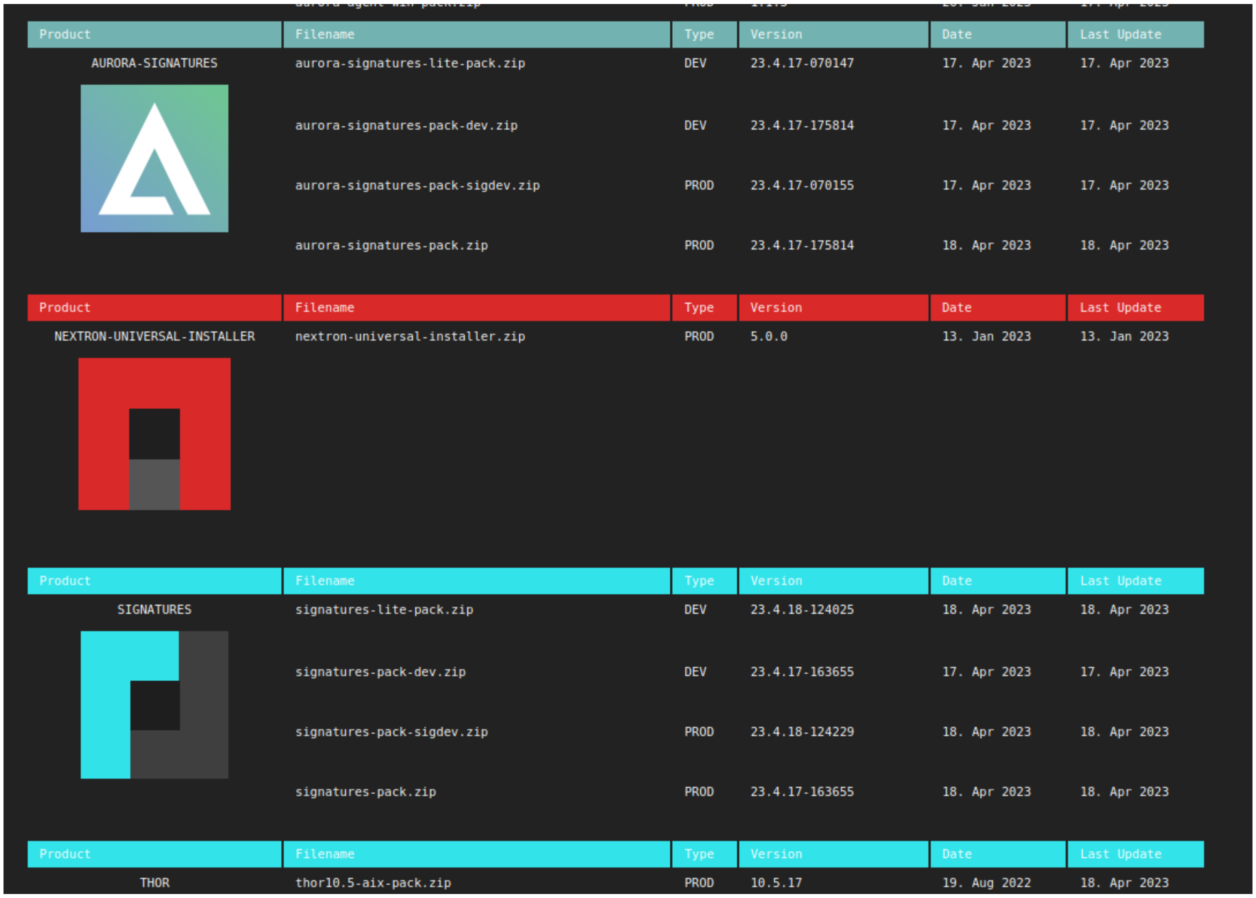
To retrieve the newest and untested signatures you can use the `thor-util.exe update --sigdev` flag.

To reset the signature set to the latest stable version use `thor-util.exe update --force`. (retrieve the stable set and enforce the download even if the current set is newer)

2.4 Update Server Information

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

https://update1.nextron-systems.com/info.php



```
                              aurora-agent-win-pack.zip                            PROD   1.1.3                     20. Jan 2023   17. Apr 2023
Product                       Filename                                             Type   Version                   Date           Last Update
      AURORA-SIGNATURES       aurora-signatures-lite-pack.zip                      DEV    23.4.17-070147            17. Apr 2023   17. Apr 2023

                              aurora-signatures-pack-dev.zip                       DEV    23.4.17-175814            17. Apr 2023   17. Apr 2023

                              aurora-signatures-pack-sigdev.zip                    PROD   23.4.17-070155            17. Apr 2023   17. Apr 2023

                              aurora-signatures-pack.zip                           PROD   23.4.17-175814            18. Apr 2023   18. Apr 2023

Product                       Filename                                             Type   Version                   Date           Last Update
  NEXTRON-UNIVERSAL-INSTALLER nextron-universal-installer.zip                      PROD   5.0.0                     13. Jan 2023   13. Jan 2023

Product                       Filename                                             Type   Version                   Date           Last Update
         SIGNATURES           signatures-lite-pack.zip                             DEV    23.4.18-124025            18. Apr 2023   18. Apr 2023

                              signatures-pack-dev.zip                              DEV    23.4.17-163655            17. Apr 2023   17. Apr 2023

                              signatures-pack-sigdev.zip                           PROD   23.4.18-124229            18. Apr 2023   18. Apr 2023

                              signatures-pack.zip                                  PROD   23.4.17-163655            18. Apr 2023   18. Apr 2023

Product                       Filename                                             Type   Version                   Date           Last Update
            THOR              thor10.5-aix-pack.zip                                PROD   10.5.17                   19. Aug 2022   18. Apr 2023
```

Fig. 2: Update server information

CHAPTER

THREE

DOWNLOAD PACKAGES (DOWNLOAD)

Using the “download” flag you can download any of the scanner packages for Windows, Linux and macOS.

This option is especially useful in cases in which you have to download the updates on an Internet connected machine and bring them to a system without Internet access.

```
C:\thor>thor-util.exe download -t thor10-win
```

3.1 THOR TechPreview Version

To download the TechPreview version, use the following command line flag.

```
C:\thor>thor-util.exe download -t thor10-win --techpreview
```

You can find more information on the TechPreview version here.

CHAPTER

FOUR

INSTALL PACKAGES (INSTALL)

The "install" feature is only used to install previously downloaded packages.

The packages can be downloaded

- using the "download" function in THOR Util
- using the displayed URL that is shown during update or upgrade procedures

It is often used to update THOR program folders on systems without Internet access.

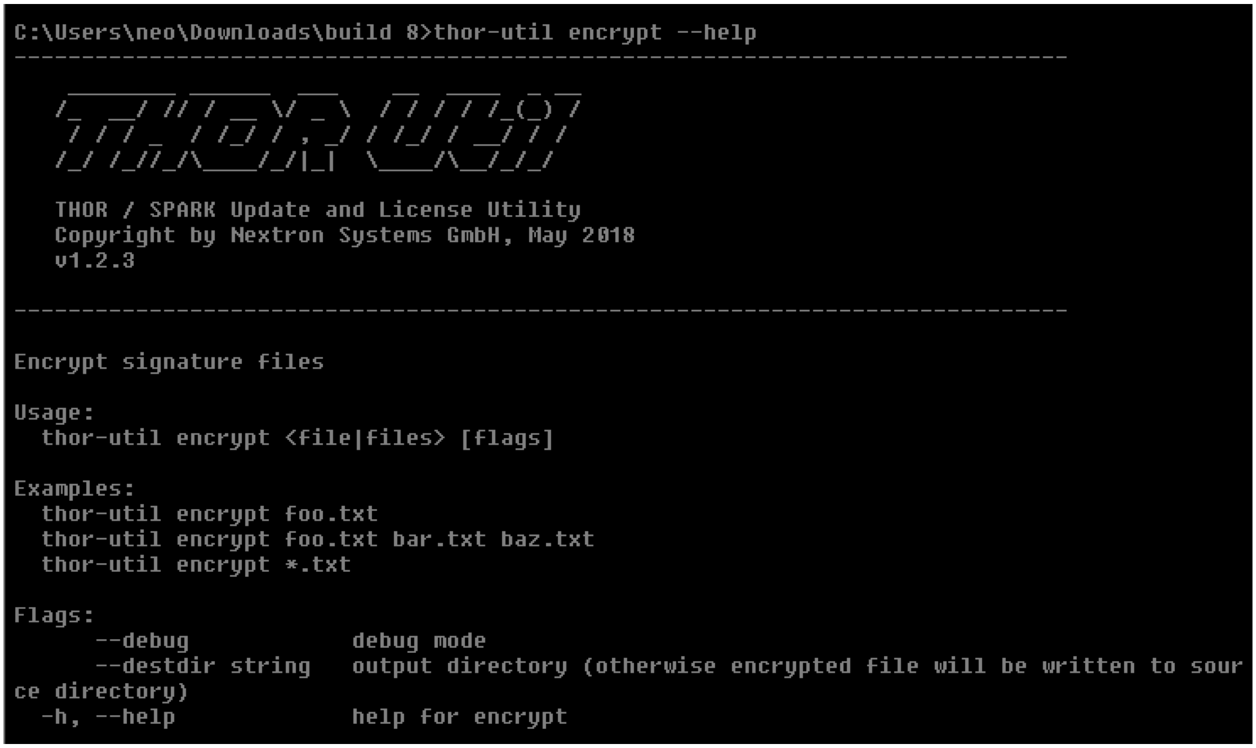
CHAPTER

FIVE

CUSTOM SIGNATURE ENCRYPTION (ENCRYPT)

You can encrypt the YARA signatures and IOC files with the help of THOR-Util's "encrypt" feature.

```
C:\thor>thor-util.exe encrypt --help
```



```
C:\Users\neo\Downloads\build 8>thor-util encrypt --help
------------------------------------------------------------------------------

    ________ ______  ____     __  _____ _ ___
   /_  __/ // / __ \/ __ \   / / / / /_(_) /
    / / / _  / /_/ / , _/  / /_/ / __/ / /
   /_/ /_//_/\____/_/|_|   \____/\__/_/_/

   THOR / SPARK Update and License Utility
   Copyright by Nextron Systems GmbH, May 2018
   v1.2.3

------------------------------------------------------------------------------

Encrypt signature files

Usage:
  thor-util encrypt <file|files> [flags]

Examples:
  thor-util encrypt foo.txt
  thor-util encrypt foo.txt bar.txt baz.txt
  thor-util encrypt *.txt

Flags:
      --debug            debug mode
      --destdir string   output directory (otherwise encrypted file will be written to sour
ce directory)
  -h, --help             help for encrypt
```

Fig. 1: THOR Util's Encrypt Feature Help

As target for the encrypt command, you can use a single file, a list of files or wildcards.

```
C:\thor>thor-util.exe encrypt ~/sigs/case14.yar
C:\thor> hor-util.exe encrypt ~/sigs/case14.yar ~/sigs/case14-hashes.txt
C:\thor>thor-util.exe encrypt ~/sigs/case14.\*
```

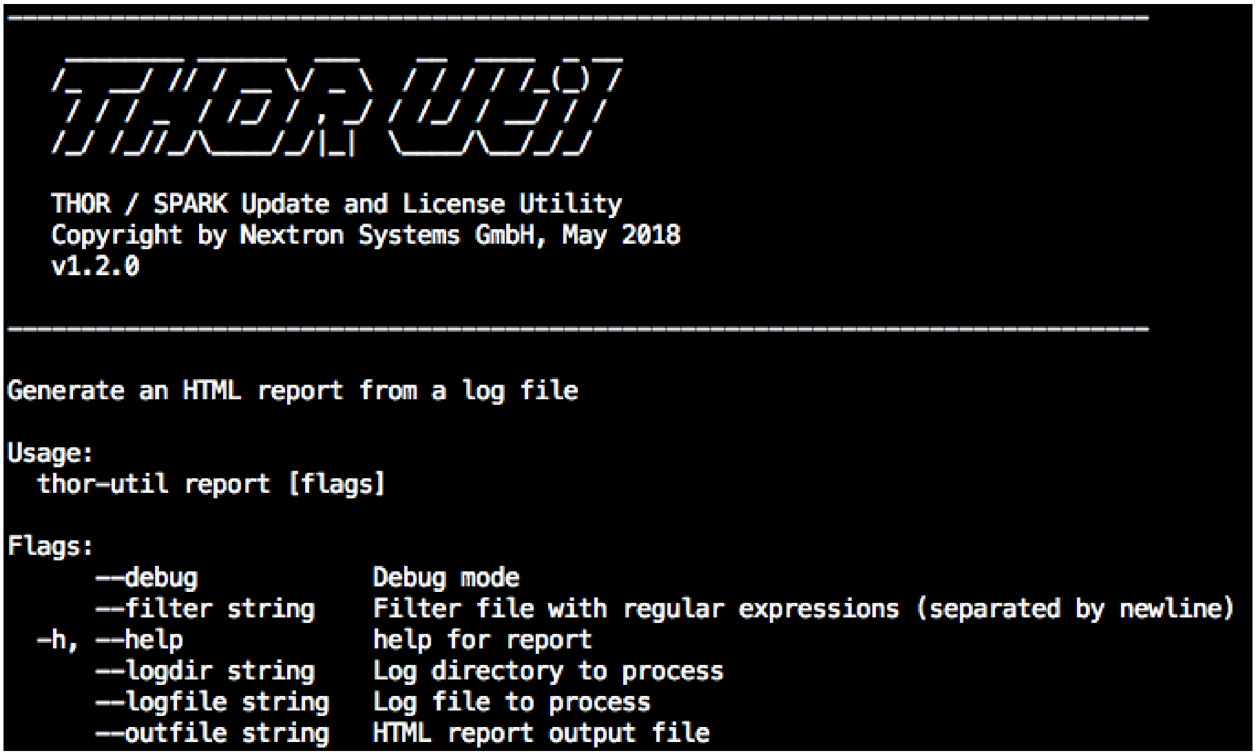
It will automatically detect the type of the signature based on its extension.

File Type	Clear Text Extension	Extension of Encrypted File
IOC File	.txt	.dat
YARA Rule	.yar, .yara, .yac (compiled YARA)	.yas
Sigma	.yml, .yaml	.yms
STIXv2	.json	.jsos

Place the encrypted IOC files in the `./custom-signatures` sub folder in the program directory and the encrypted YARA rules in the `./custom-signatures/yara` sub folder.

REPORT GENERATION (REPORT)

Using the `--report` flag, you can generate HTML report from plain text log files.



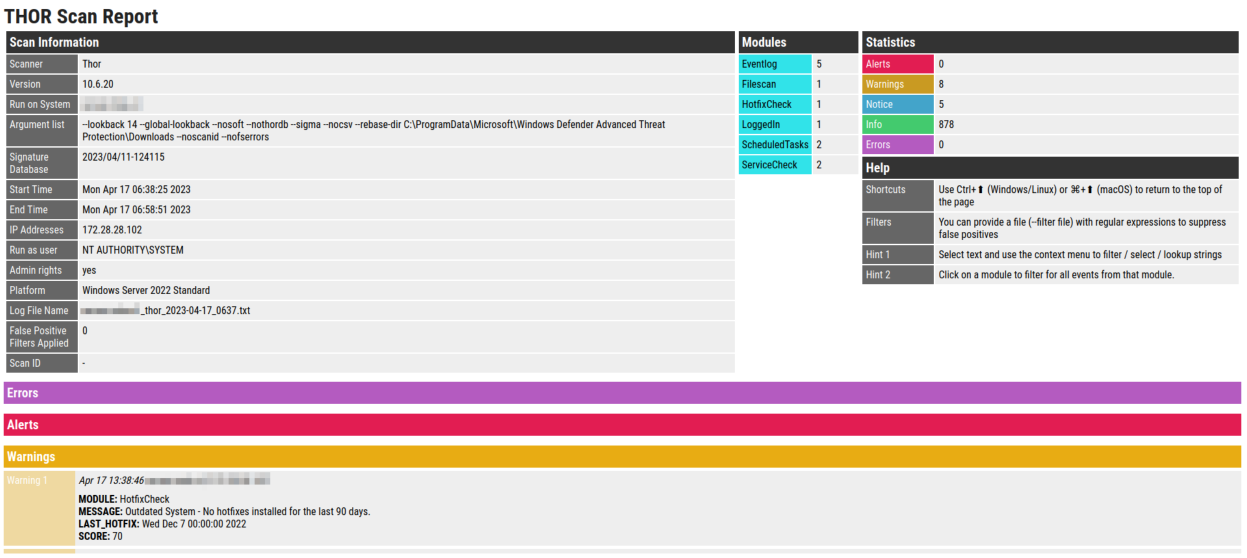
```
------------------------------------------------------------------------------

   THOR / SPARK Update and License Utility
   Copyright by Nextron Systems GmbH, May 2018
   v1.2.0

------------------------------------------------------------------------------

Generate an HTML report from a log file

Usage:
  thor-util report [flags]

Flags:
      --debug            Debug mode
      --filter string    Filter file with regular expressions (separated by newline)
  -h, --help             help for report
      --logdir string    Log directory to process
      --logfile string   Log file to process
      --outfile string   HTML report output file
```

Fig. 1: THOR Util's report generation functions

```
user@unix:~/thor$ ./thor-util report --logfile system-xyz_thor.log
user@unix:~/thor$ ./thor-util report --logdir ./logs
```

See this blog post for details:

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



THOR Scan Report

Scan Information	
Scanner	Thor
Version	10.6.20
Run on System	[redacted]
Argument list	--lookback 14 --global-lookback --nosoft --nothordb --sigma --nocsv --rebase-dir C:\ProgramData\Microsoft\Windows Defender Advanced Threat Protection\Downloads --noscanid --nofserrors
Signature Database	2023/04/11-124115
Start Time	Mon Apr 17 06:38:25 2023
End Time	Mon Apr 17 06:58:51 2023
IP Addresses	172.28.28.102
Run as user	NT AUTHORITY\SYSTEM
Admin rights	yes
Platform	Windows Server 2022 Standard
Log File Name	[redacted]_thor_2023-04-17_0637.txt
False Positive Filters Applied	0
Scan ID	-

Modules	
Eventlog	5
Filescan	1
HotfixCheck	1
LoggedIn	1
ScheduledTasks	2
ServiceCheck	2

Statistics	
Alerts	0
Warnings	8
Notice	5
Info	878
Errors	0

Help	
Shortcuts	Use Ctrl+⬆ (Windows/Linux) or ⌘+⬆ (macOS) to return to the top of the page
Filters	You can provide a file (--filter file) with regular expressions to suppress false positives
Hint 1	Select text and use the context menu to filter / select / lookup strings
Hint 2	Click on a module to filter for all events from that module.

Errors

Alerts

Warnings

Warning 1

Apr 17 13:38:46 [redacted]

MODULE: HotfixCheck
MESSAGE: Outdated System - No hotfixes installed for the last 90 days.
LAST_HOTFIX: Wed Dec 7 00:00:00 2022
SCORE: 70

Fig. 2: HTML report generated by thor-util

CHAPTER

SEVEN

VERIFY BINARIES (VERIFY)

This feature allows to verify the authenticity of the included binaries. The signature verification is based on a public key encryption algorithm and requires the `*.sig` files that are shipped with the packages.

Fig. 1: Verify thor.exe signature using THOR Util

To verify the integrity of THOR Util, download the public key used for the verification on Nextrons Website: https://www.nextron-systems.com/pki/ The public key can be then used with the following command to verify the integrity of `thor-util`:

on Windows:

```
C:\thor>openssl dgst -sha256 -verify codesign.pem -signature thor-util.exe.sig thor-util.exe
```

on Linux:

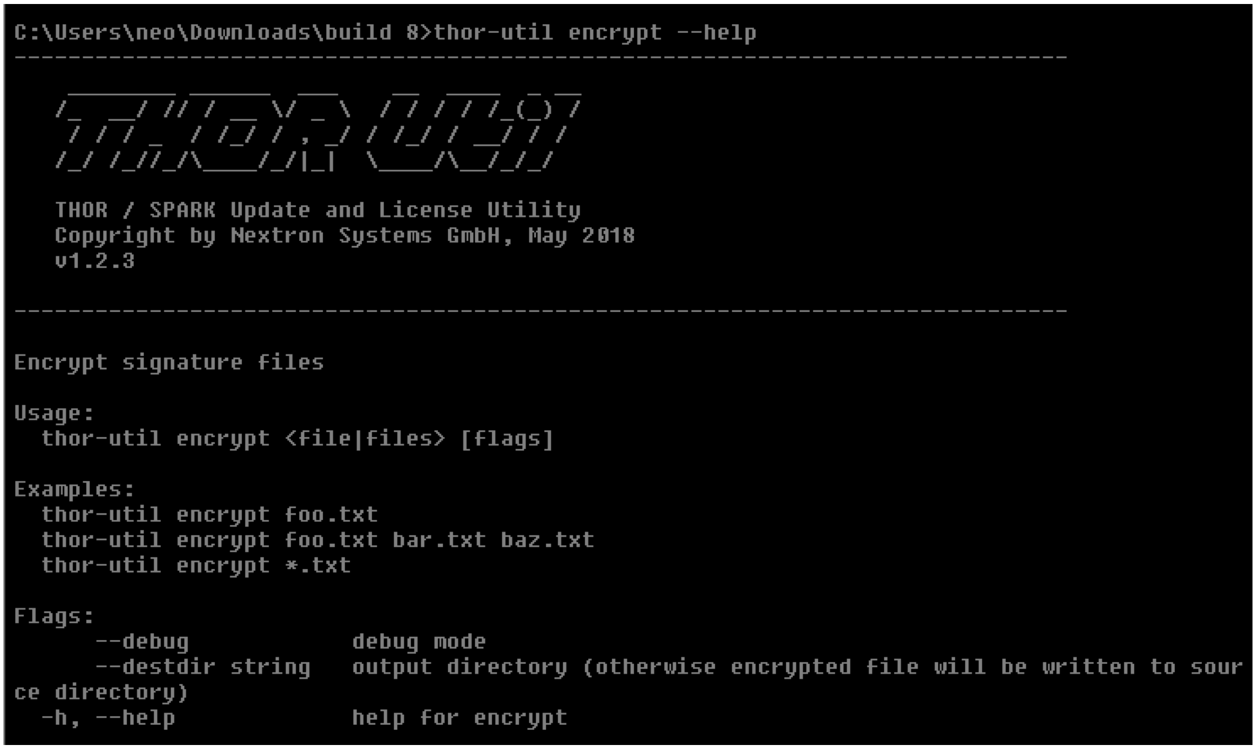
```
C:\thor>openssl dgst -sha256 -verify codesign.pem -signature thor-util.sig thor-util
```

CHAPTER

EIGHT

DECRYPT REPORTS AND LOG FILES (DECRYPT)

This feature can be used to decrypt HTML reports or text log files that have previously been encrypted by THOR upon scan completion.



```
C:\Users\neo\Downloads\build 8>thor-util encrypt --help
------------------------------------------------------------------------------
    ________ ______  ___   __  ____  _ __
   /_  __/ // / __ \/ _ \  / / / / /_(_) /
    / / / _  / /_/ / , _/ / /_/ / __/ / /
   /_/ /_//_/\____/_/|_|  \____/\__/_/_/

   THOR / SPARK Update and License Utility
   Copyright by Nextron Systems GmbH, May 2018
   v1.2.3

------------------------------------------------------------------------------

Encrypt signature files

Usage:
  thor-util encrypt <file|files> [flags]

Examples:
  thor-util encrypt foo.txt
  thor-util encrypt foo.txt bar.txt baz.txt
  thor-util encrypt *.txt

Flags:
      --debug            debug mode
      --destdir string   output directory (otherwise encrypted file will be written to sour
ce directory)
  -h, --help             help for encrypt
```

Fig. 1: THOR Util's decryption feature options

CHAPTER

NINE

LOG CONVERSION (LOGCONVERT)

The log conversion features allows you to convert THOR Logs between different formats. You can chose whatever format fits your needs the most:

Format	Convert From	Convert To
Log[1]	Yes	Yes
JSON	Yes	Yes
Key-Value	No[2]	Yes
CSV	No	Yes
ZIP CSV	No	Yes

```
C:\nextron\thor>thor-util.exe logconvert --help
    ________ ______  ___    __  ______________
   /_  __/ // / __ \/ _ \  / / / /_  __/  _/ /
    / / / _  / /_/ / , _/ / /_/ / / / _/ // /__
   /_/ /_//_/\____/_/|_|  \____/ /_/ /___/____/

   Copyright by Nextron Systems GmbH, 2023
   v1.11.0+thor10.7.6

Convert log file into another format

Usage:
  thor-util logconvert [flags]

Examples:
  thor-util logconvert --from-json --to-log --file example.json --output example.log

Flags:
  -f, --file string     Input file
      --from-json       Convert from JSON
      --from-kv         Convert from KV
      --from-log        Convert from Log
  -h, --help            help for logconvert
  -o, --output string   Output file
      --to-csv          Convert to CSV
      --to-csv-zip      Convert to ZIP containing one CSV log per module
```

(continues on next page)

[1] This is the default THOR log format `<hostname>_timestamp.txt`.

[2] The help menu shows the flag is existing, but this is not implemented yet.

(continued from previous page)

```
      --to-json          Convert to JSON
      --to-kv            Convert to KV
      --to-log           Convert to Log
```

Note: The feature to convert logs into CSV and CSV-zip was introduced in THOR Util Version 1.11.0

9.1 Conversion Examples

Here you can find some examples on how to convert logs to different formats.

Your command should always follow the same structure of a `--from` format, as well as a `--to` format. Additionally, you also need to instruct which file is your input file `-f` and which should be your output file `-o`.

```
user@unix:~/thor$ ./thor-util logconvert --from-log --to-json -f thor.txt -o thor-
↪converted.json
user@unix:~/thor$ ./thor-util logconvert --from-log --to-csv -f thor.txt -o thor-
↪converted.csv
user@unix:~/thor$ ./thor-util logconvert --from-json --to-log -f thor.json -o thor-
↪converted.log
user@unix:~/thor$ ./thor-util logconvert --from-log --to-csv -f thor.txt -o thor-
↪converted.csv
user@unix:~/thor$ ./thor-util logconvert --from-log --to-csv-zip -f thor.txt -o thor-
↪converted.zip
```

CHAPTER

TEN

TEMPLATES

THOR Util reads a default configuration from `config/thor-util.yml`.

Within this file, default parameters can be set in YAML form.

These default parameters can be overwritten with command line flags.

All global flags for THOR Util are supported in the configuration file. These flags can be shown with:

```
user@unix:~/thor$ ./thor-util --help
```

10.1 Proxy configuration

If you want to use a specific HTTP proxy, this can be specified in your configuration file with:

```
proxy: http://myproxy:8080
```

10.2 TechPreview configuration

If you always want to download the latest TechPreview instead of the standard THOR version, add:

```
techpreview: True
```

CHAPTER

ELEVEN

DIAGNOSTICS

If THOR does not behave like it should, e.g. using more resources than you expected, taking more time with the scan as usual or unexpectedly exits with a generic error, you can create a diagnostics pack for our support to help in troubleshooting the issue.

This can be done using THOR Util's diagnostics command.

```
C:\thor>thor-util.exe help diagnostics

Create diagnostics pack

Usage:
  thor-util diagnostics [flags]

Flags:
  -h, --help        help for diagnostics
  --output string   File to write diagnostics pack to (default "[...]\diagnostics.zip")
  --run             Rerun last THOR scan with debug logging before collecting␣
↪diagnostics pack
```

By default the `diagnostics.zip` file is put in THOR's working directory. The location is printed on the commandline in the end of the data collection and can be changed using the `--output` flag.

11.1 Get diagnostics of a running THOR scan

The generally preferred method of collecting THOR diagnostics is to run THOR Util's diagnostics command directly when the issue is occurring.

```
C:\thor>thor-util.exe diagnostics
```

11.2 Get diagnostics of a finished THOR scan

If the THOR run is already finished, you can also use the diagnostics command like above with reduced information being collected.

Another possibility is to use the `--run` flag to rerun the last THOR scan. In addition to conveniently rerunning the scan, THOR Util can now watch over the THOR process for interrupting signals from other processes (e.g. anti virus) which greatly helps in determining if anti virus exclusions for THOR are applied correctly or not. Using the `--run` flag should be the preferred method if THOR is exiting unexpectedly.

```
C:\thor>thor-util.exe diagnostics --run
```

CHAPTER

TWELVE

INDICES AND TABLES

- search