
THOR Util Manual Documentation

Nexttron Systems GmbH

Apr 08, 2021

CONTENTS:

1	What is THOR Util?	1
2	Upgrade (upgrade) and Updates (update)	3
2.1	THOR TechPreview Version	3
2.2	Update Locations	5
2.3	Update Server Information	5
3	Download Packages (download)	7
3.1	THOR TechPreview Version	7
3.2	THOR Legacy Version	7
4	Install Packages (install)	9
5	Custom Signature Encryption (encrypt)	11
6	Report Generation (report)	13
7	Verify Binaries (verify)	15
8	License Retrieval (license)	17
9	Decrypt Reports and Log Files (decrypt)	19
10	Log Conversion (logconvert)	21
11	Indices and tables	23

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 and report generation.

UPGRADE (UPGRADE) AND UPDATES (UPDATE)

You can download updates for THOR and SPARK 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 only works with THOR 10 and retrieves only the newest signature pack.

Option	Description	Program
upgrade	Get new program files and signatures	THOR 8, SPARK, THOR 10
update	Get new signatures	THOR 10
download	Get new program files, signatures and config files	THOR 8, SPARK, THOR 10

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

```
thor-util *option* --help
```

The following two examples show different upgrade methods.

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

```
thor-util.exe upgrade --techpreview
```

You can find more information on the TechPreview version [here](#).

```
V:\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, spark-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

The following servers are used as update mirrors and should be accessible via HTTPS:

update1.nextron-systems.com

update2.nextron-systems.com

2.3 Update Server Information

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

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




Product	Filename	Type	Version	Date	MD5
THOR8 	thor8-latest.pack	PROD	8.42.1	12. Dec 2017	5d69d2d2fa65aecebb9f7afa0d2f2d84
	thor8-pack.zip	PROD	unavailable	12. Dec 2017	3d6b502fd656ed14d20ded4e3606b6de
	thor8-latest-dev.pack	DEV	8.42.10	08. Jan 2018	1158cd6cd8d21bfd49a99f9d2c0eb6be
	thor8-pack-dev.zip	DEV	unavailable	08. Jan 2018	e0a14a01a871b62852d5a5a8d208362d
Product	Filename	Type	Version	Date	MD5
SPARK 	spark-linux-latest.pack	PROD	1.8.4	16. Oct 2017	77440eb8cbbb28b76cf808b425ba49cd
	spark-linux-pack.zip	PROD	unavailable	16. Oct 2017	746897a9c5ecb1b349938fa02c22d50b
	spark-osx-pack.zip	PROD	unavailable	26. Apr 2017	26282dcbfec4a50fc00c11ffc2fac5c8
	spark-win-latest.pack	PROD	1.8.4	16. Oct 2017	91eafb0bfe0d5f9ec870dfaae18104f6
	spark-win-pack.zip	PROD	unavailable	16. Oct 2017	db15a9ecdaedc75e1f367ebb7cf6c984
	spark-linux-latest-dev.pack	DEV	1.8.6	21. Nov 2017	1bc8bd3b9409dad3501ebd0a2786aad3
	spark-linux-pack-dev.zip	DEV	unavailable	21. Nov 2017	652d77be9b2c54f2c5c73fc0757d4362
	spark-macosx-latest-dev.pack	DEV	1.8.6	14. Dec 2017	f76b2f856fdd36a134af627034fa69b1
	spark-macosx-pack-dev.zip	DEV	unavailable	14. Dec 2017	7036c1558ab275194662eec61ad89d77
	spark-win-latest-dev.pack	DEV	1.8.6	21. Nov 2017	cc9f3f94862d90e94f9f80f2d1d2e203
	spark-win-pack-dev.zip	DEV	unavailable	21. Nov 2017	2f557c6da1501360b6182b5e90c08380
Product	Filename	Type	Version	Date	MD5
ASGARD 	asgard-installer.zip	PROD	1.1.5	17. Nov 2017	d1f632b5e672ad3e1afc15f464066627

Fig. 2: Update server information

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.

```
thor-util.exe download -t thor10-win
```

3.1 THOR TechPreview Version

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

```
thor-util.exe download -t thor10-win --techpreview
```

You can find more information on the TechPreview version [here](#).

3.2 THOR Legacy Version

To download the Legacy version, which is usable on windows XP, Vista, 2003 and 2008, use the following command line flag.

```
thor-util.exe download -t thor10-win --legacy
```

You can find more information on the Legacy version [here](#).

Important: The THOR Legacy version is not supported.

INSTALL PACKAGES (INSTALL)

The “install” feature is only used to install previously downloaded packages using the “download” feature and often used on systems without Internet connection.


```
thor-util.exe encrypt --help
```

[illegible]

Fig. 1: THOR Util's Encrypt Feature Help

```
thor-util.exe encrypt ~/sigs/case14.yar
```

```
thor-util.exe encrypt ~/sigs/case14.yar ~/sigs/case14-hashes.txt
thor-util.exe encrypt ~/sigs/case14.*
```

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

```
thor-util report --logfile PROMETHEUS\_thor.log  
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/>

Scan Information						Modules		Statistics	
PROMETHEUS	476	119	26	553	1	ArchiveCheck	24	Alerts	522
TRINITY	14	40	21	127	1	Log	1	Warnings	183
ALPHA	0	15	19	148	1	PESieve	1	Notice	113
PROMETHEUS	0	1	18	140	1	DeepDive	61	Info	1048
PROMETHEUS	1	0	6	13	0	Autoruns	427	Errors	4
prometheus.local	15	4	15	30	0	LogScan	491	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 Some header elements contain links to the sections below Hint 2 Values contain links to search engines	
metusalem	16	4	8	37	0	VulnerabilityCheck	5		
						Registry	455		
						Filescan	185		
						Amcache	4		
						SHIMCache	18		
						FileScan	2		
						RegistryChecks	18		
						ProcessCheck	52		
Alerts									
Alert 1	PROMETHEUS	2018-06-12T13:00:15Z PROMETHEUS/10.0.2.4 MODULE: RegistryChecks MESSAGE: Malicious filename found SCORE: 80 DESC: FEIB Heist - BAE Report https://goo.gl/8LbqZ9 ELEMENT: USBSERV C:\Windows\Temp\bitsran.exe C:\Windows\Temp\bitsran.exe OBJECT: RUN Key							
Alert 2	PROMETHEUS	2018-06-12T08:15:32Z PROMETHEUS/10.0.2.4 MODULE: Filescan MESSAGE: Malicious file found FILE: C:\hp\Mailing_Oxford_Label.exe SCORE: 80 MD5: 520a6d1cbcc9cf642c625fe814c93c58 SHA1: fb517abb38e9ccc67de411d4f18a9446c11c0923 SHA256: 08966ce743aa1cbcd0874933e104ef7b913188ecd8f0c679f7d8378516c51da2 SIZE: 562688 TYPE: UNKNOWN FIRSTBYTES: 4d5a90000300000004000000ffff0000b8000000 / MZ CREATED: 2014-01-27T13:35:50Z MODIFIED: 2013-07-08T07:35:59Z ACCESSED: 2014-01-27T13:35:50Z EXT: .exe							

Fig. 2: HTML report generated by thor-util

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.

[illegible]

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

LICENSE RETRIEVAL (LICENSE)

This feature can be used to retrieve a license from a remote ASGARD server system.

```
Get a license from a license server (ASGARD)

Usage:
  thor-util license [flags]

Flags:
  -c, --customer string      Customer-ID, may be empty
  -h, --help                  help for license
  -H, --hostname string      Hostname (default "prometheus.local")
  --http-insecure             do not verify certificate chain
  -m, --machine-type string   Machine license type (default "client")
  --ntlm                      use ntlm proxy authentication
  --path string               (default ".")
  -a, --proxy string          proxy address
  -p, --proxy-pass string     proxy password
  -n, --proxy-user string     proxy user
  --rootca strings            list of files with trusted root CAs
  -u, --url URL               License server URL (default [])
```

Fig. 1: THOR Util's license generation feature

```
prometheus:spark-macosx-pack neo$ ./thor-util license --http-insecure --url https://asgard1.bsk...

THOR / SPARK Update, Encryption and License Utility
Copyright by Nextron Systems GmbH, 2018
v1.5.2

Nov 21 17:53:39 prometheus.local THOR_UTIL: Info: Requesting client license for prometheus.local at https://asgard1.bsk...
Nov 21 17:53:39 prometheus.local THOR_UTIL: Info: License does not exist yet.
Nov 21 17:53:39 prometheus.local THOR_UTIL: Info: Asking server to issue a license...
Nov 21 17:53:39 prometheus.local THOR_UTIL: Info: Writing license to thor-prometheus.local.lic...
```

Fig. 2: License retrieval from an ASGARD server

```
thor-util license --hostname machine1 server --url https://asgard1.bsk  
thor-util license --http-insecure --url https://asgard1.bsk
```

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 SPARK upon scan completion.

```
Decrypt log- and csv-files from THOR/SPARK

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

Examples:
  thor-util decrypt --keyfile /path/to/privatekey.pem scan-results.log

Flags:
  --debug          debug mode
  -h, --help       help for decrypt
  --privkey string RSA Private Key in PEM Format (privkey="<key>" or privkey="<file>")
```

Fig. 1: THOR Util's decryption feature options

The log conversion features allows to convert between Text and JSON format.

```

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:
  --debug          debug mode
  -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-json        Convert to JSON
  --to-kv          Convert to KV
  --to-log         Convert to Log

```

Fig. 1: Log Conversion Options

INDICES AND TABLES

- search