THOR Util Manual Documentation

Nextron Systems GmbH

May 04, 2021

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 and report generation.

CHAPTER

TWO

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.

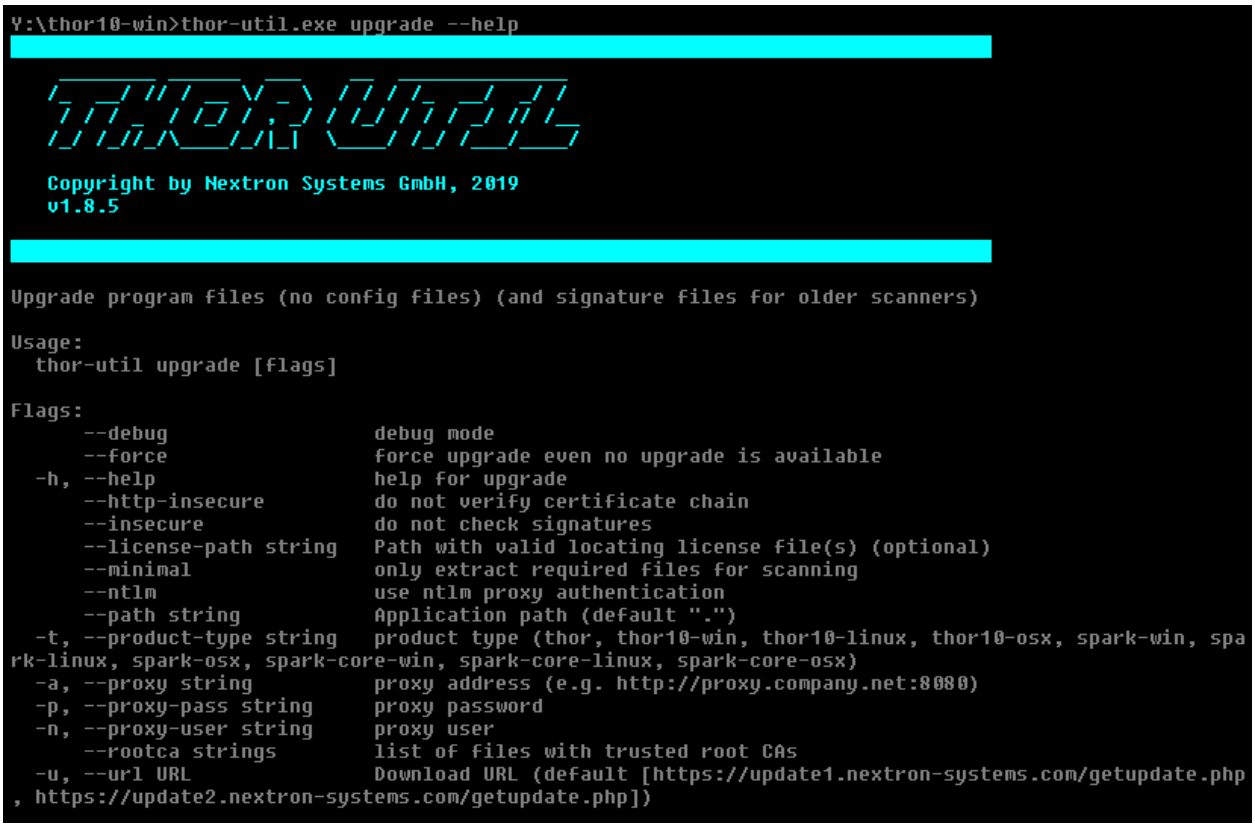

Fig. 1: THOR-util Upgrade Help

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

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.

```
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.

CHAPTER

FOUR

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.

CHAPTER

FIVE

CUSTOM SIGNATURE ENCRYPTION (ENCRYPT)

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

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

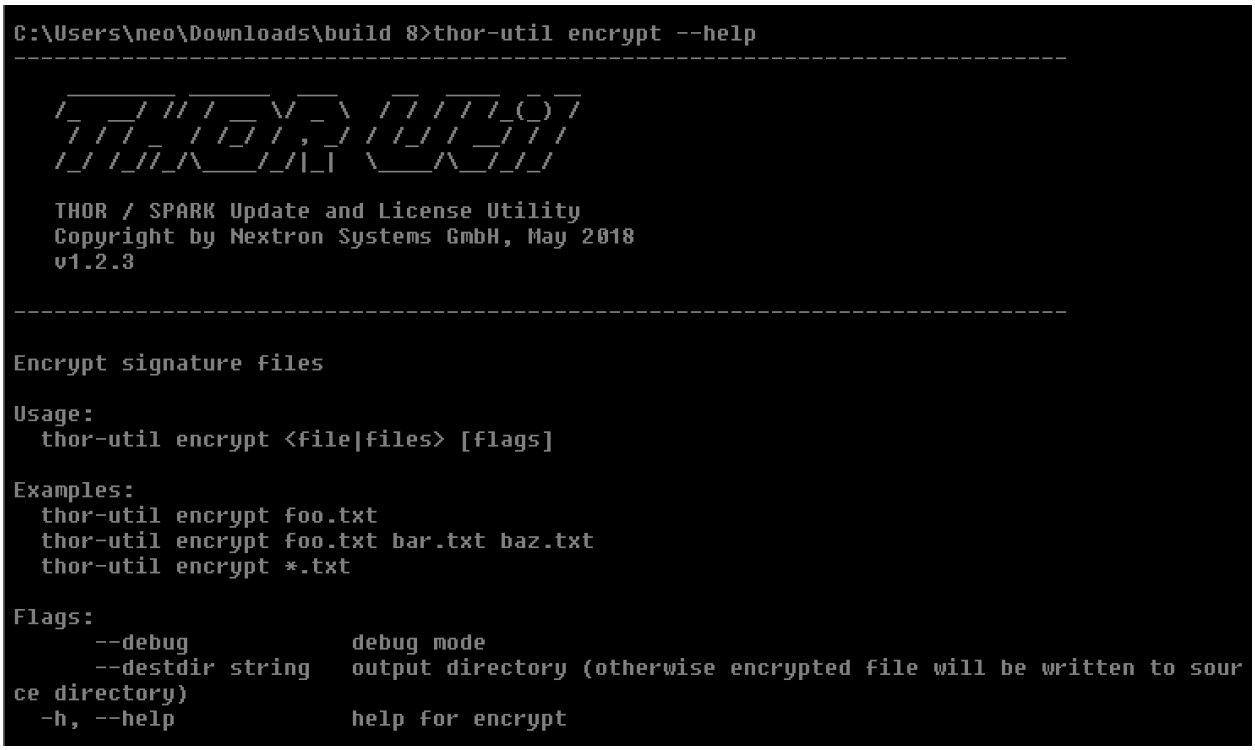

Fig. 1: THOR Util's Encrypt Feature Help

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

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

CHAPTER

SIX

REPORT GENERATION (REPORT)

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

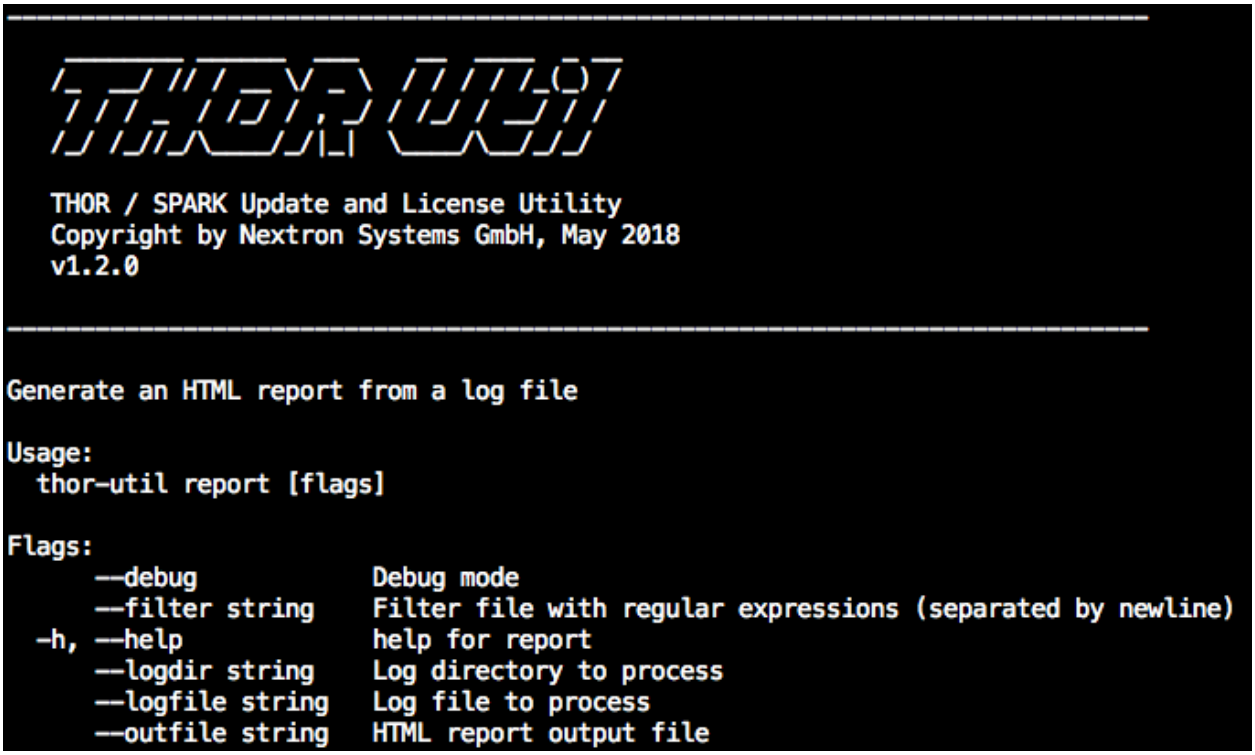

Fig. 1: THOR Util's report generation functions

```
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

PROMETHEUS	476	119	26	553	1
TRINITY	14	40	21	127	1
ALPHA	0	15	19	148	1
PROMETHEUS	0	1	18	140	1
PROMETHEUS	1	0	6	13	0
prometheus.local	15	4	15	30	0
metusalem	16	4	8	37	0

Modules

ArchiveCheck	24
Log	1
PESieve	1
DeepDive	61
Autoruns	427
LogScan	491
VulnerabilityCheck	5
Registry	455
Filescan	185
Amcache	4
SHIMCache	18
FileScan	2
RegistryChecks	18
ProcessCheck	52

Statistics

Alerts	522
Warnings	183
Notice	113
Info	1048
Errors	4

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

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:** 08966ce743aa1cbed0874933e104ef7b913188ecd8f0c679f7d8378516c51da2 **SIZE:** 562688 **TYPE:** UNKNOWN **FIRSTBYTES:** 4d5a900003000000040000000ffff0000b8000000 / 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

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.

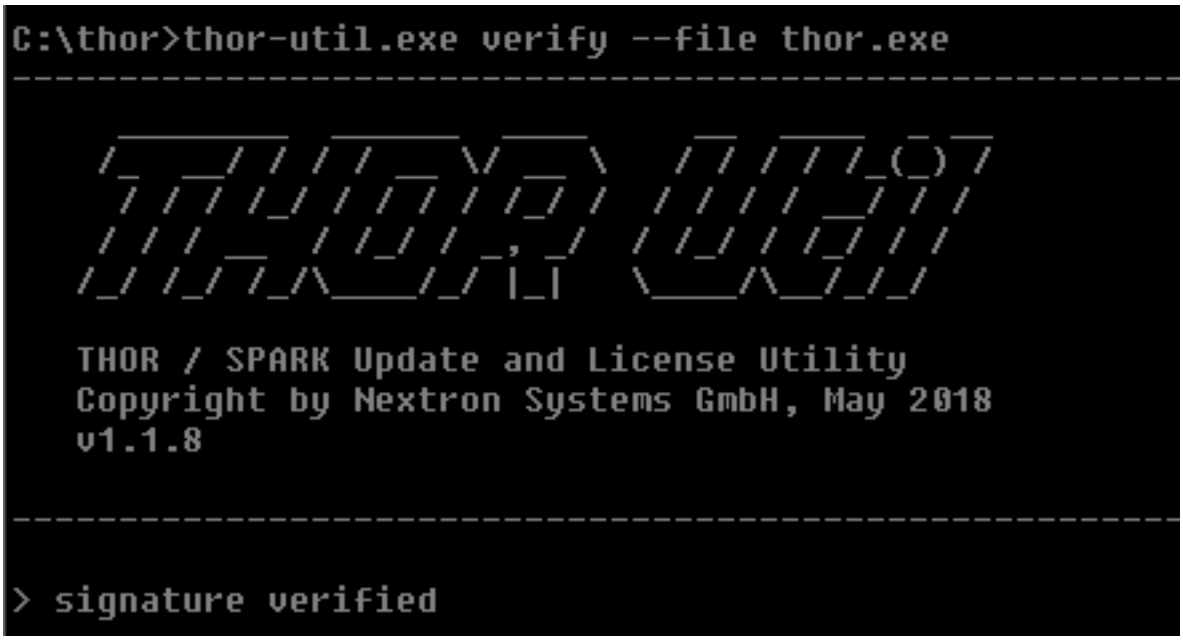

Fig. 1: Verify thor.exe signature using THOR Util

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:

```
openssl dgst -sha256 -verify nextronCode.pem -signature thor-util.sig thor-util
```

CHAPTER

EIGHT

LICENSE RETRIEVAL (LICENSE)

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

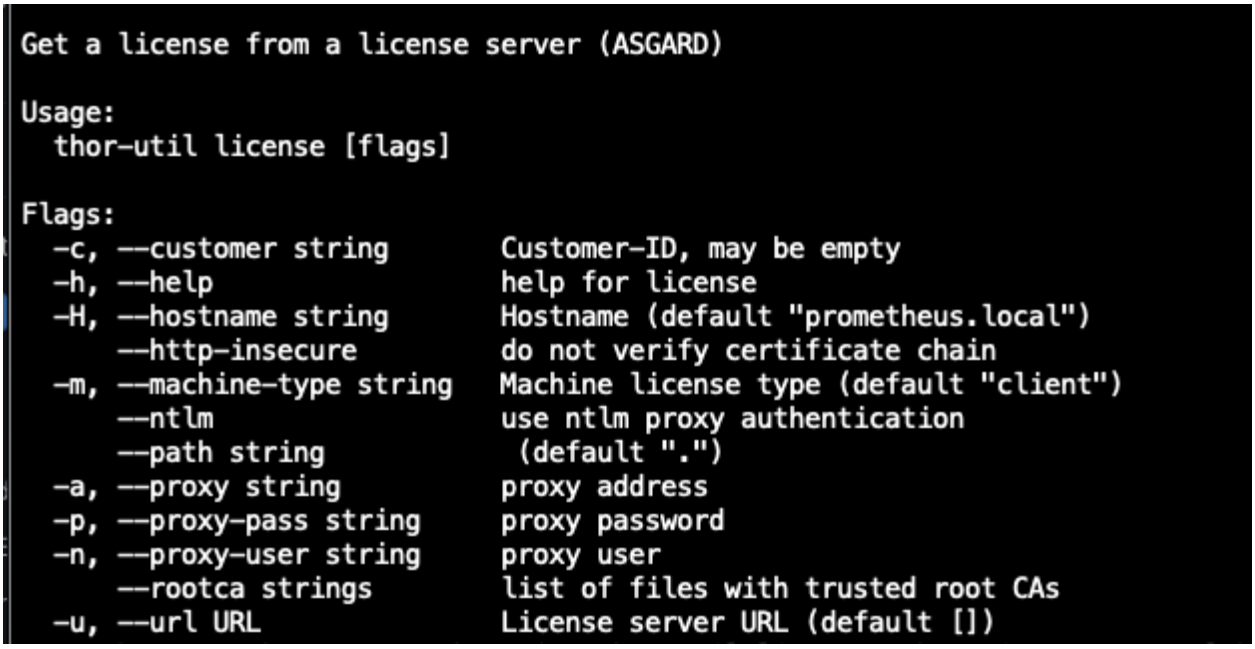

Fig. 1: THOR Util's license generation feature

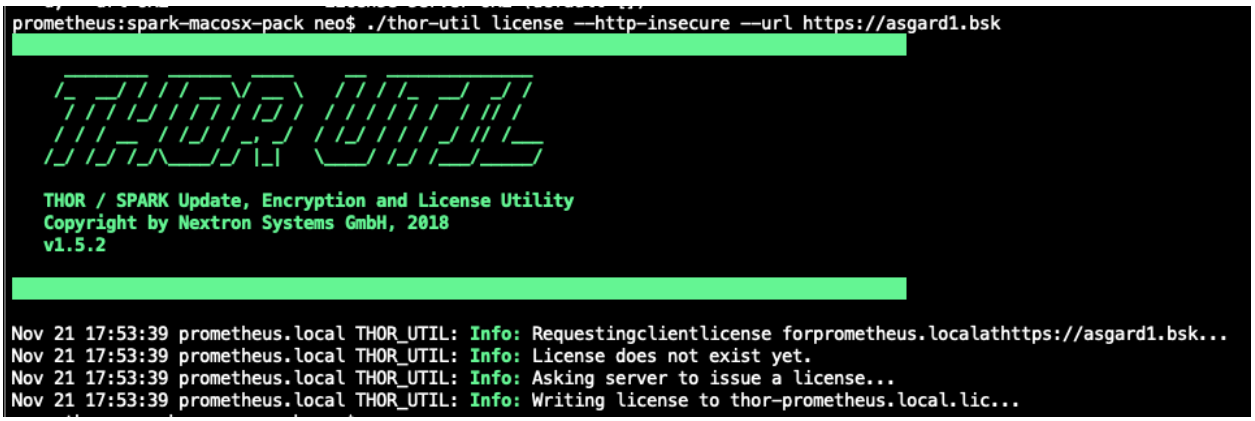

Fig. 2: License retrieval from an ASGARD server

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

CHAPTER

NINE

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

CHAPTER

TEN

LOG CONVERSION (LOGCONVERT)

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

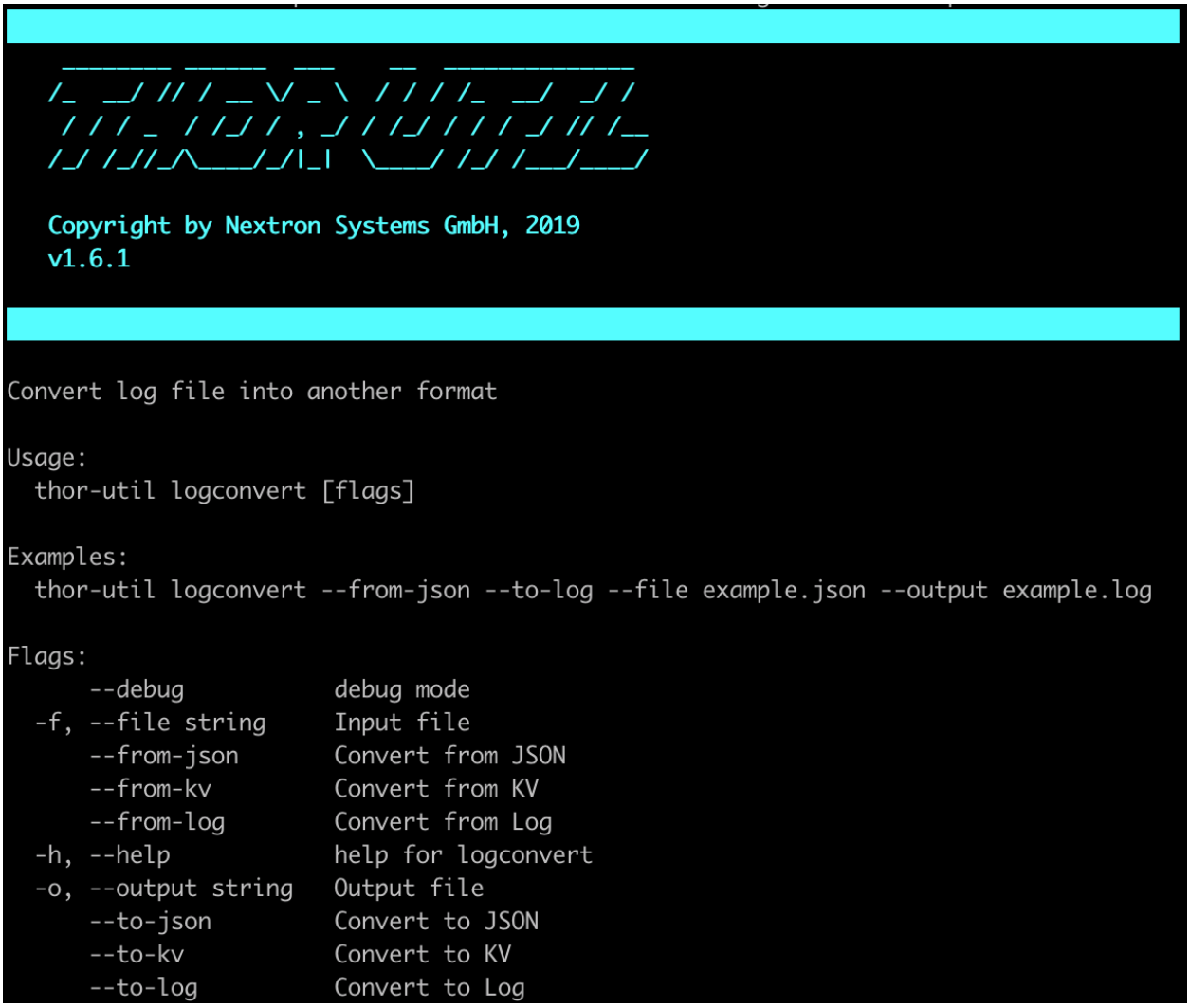

Fig. 1: Log Conversion Options

CHAPTER

ELEVEN

TEMPLATES

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

Within this file, parameters can be set in YAML form: Say, for example, that you always want to use an HTTP proxy. This can be specified in your configuration file with:

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

These default parameters can be overridden with command line flags.

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

```
./thor-util --help
```

CHAPTER

TWELVE

INDICES AND TABLES

- search