THOR Cloud Microsoft Defender ATP Documentation

Nextron Systems GmbH

May 04, 2021

CONTENTS:

CHAPTER

ONE

REQUIREMENTS

1.1 Supported Operating Systems

The operating systems are limited to the set that supports the Microsoft Defender ATP "Live Response" feature. As of the date of this guide it is limited to Windows 10 workstations and Windows 2019 server systems.

Windows 10

- Version 1909 or later
- Version 1903 with KB4515384
- Version 1809 (RS 5) with KB4537818
- Version 1803 (RS 4) with KB4537795
- Version 1709 (RS 3) with KB4537816

Windows Server 2019 - Only applicable for Public preview

- Version 1903 or (with KB4515384) later
- Version 1809 (with KB4537818)

For a current version of the list of supported operating systems, check the following page:

https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/live-response

1.2 Enable „Live Response" Feature

You need to enable the live response capability in the "Advanced Features" settings page for Workstations and Servers.

https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/advanced-features

1.3 Hardware Requirements

The hardware requirements reflect the scan settings of a default scan.

Minimum	Recommended
1 CPU Cores 1 GB of RAM 100MB of temporary disk space	2 CPU cores or more 8 GB of RAM or more

Table 1 - Hardware Requirements

Note: THOR uses between 160 and 300 MB of main memory during the investigation, but there are conditions in which the memory usage can exceed this range for a short time. On very weak end systems, enable "soft" mode in THOR Seeds config section.

1.4 Network Connections

1.4.1 On Investigated Workstation

cloud.nextron-systems.com 443/tcp

(note: this FQDN resolves to multiple IP addresses)

1.4.2 Web Proxies

Web proxies are supported albeit not fully tested. THOR Seed, the script that retrieves a license and the temporary THOR scanner package is proxy aware and should use the local proxy configuration.

CHAPTER

TWO

RETRIEVE AND CONFIGURE THOR SEED

2.1 Download THOR Seed using Voucher Trials

Trial users receive a link that leads to a web page, which lists the attributes of the voucher rial including start date, expiration date, the life time of each license and quota statistics.

You have to read and accept the EULA and check the box to enable the download links.

2.2 Download THOR Seed in Customer Portal

Every applicable contract in our customer portal shows a certain button in the "Actions" column, which leads you to a THOR Seed download page.

The THOR Seed download page lists all attributes of the contract including the total quota, used licenses and the lifetime of each license. (see the FAQ section at the end of this document for more details on the terms)

2.3 Configure THOR Seed (Optional)

THOR Seed is the PowerShell script that retrieves THOR packages with a valid license for the end system on which it was started, executes a THOR scan and cleans up afterwards.

You can find more information on Github:
https://github.com/NextronSystems/nextron-helper-scripts/tree/master/thor-seed

The version that you've retrieved from our customer portal already contains a token that is connected with you voucher trial or contract. It is also configured to use our cloud systems to retrieve THOR packages. (users of the ASGARD platform can also use an on-premise ASGARD server to retrieve package from that local system)

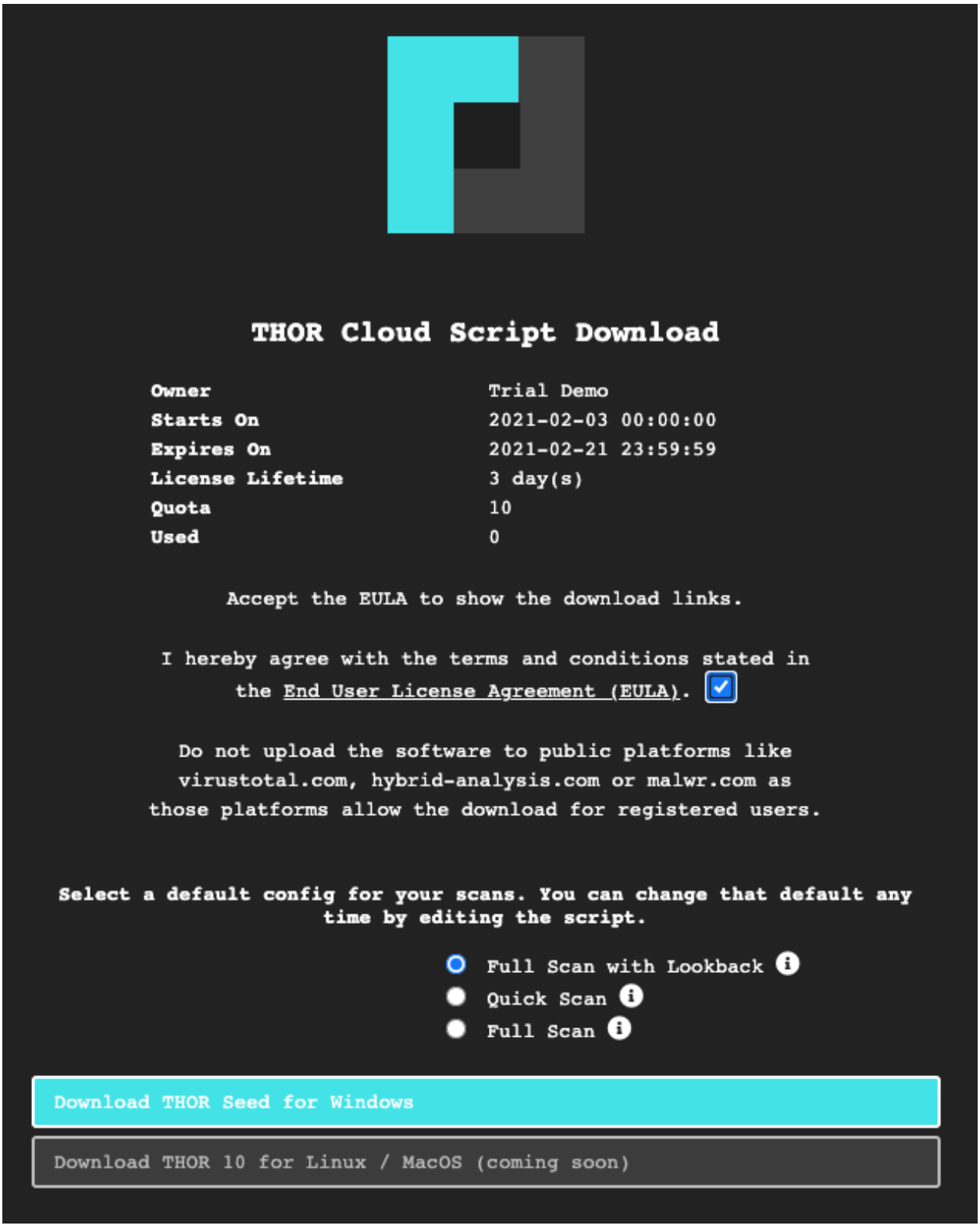


Fig. 1: THOR Cloud Voucher Trial

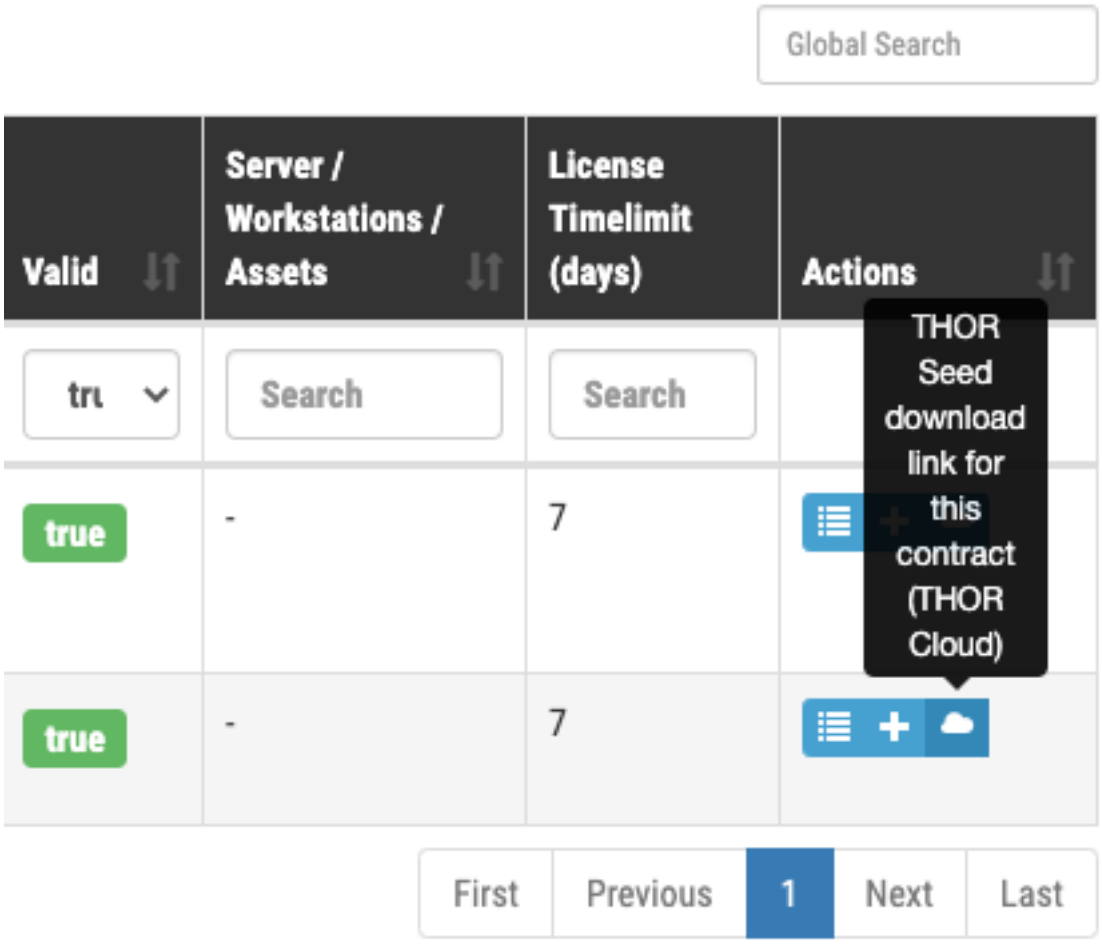


Fig. 2: Button that leads to the THOR Seed download page

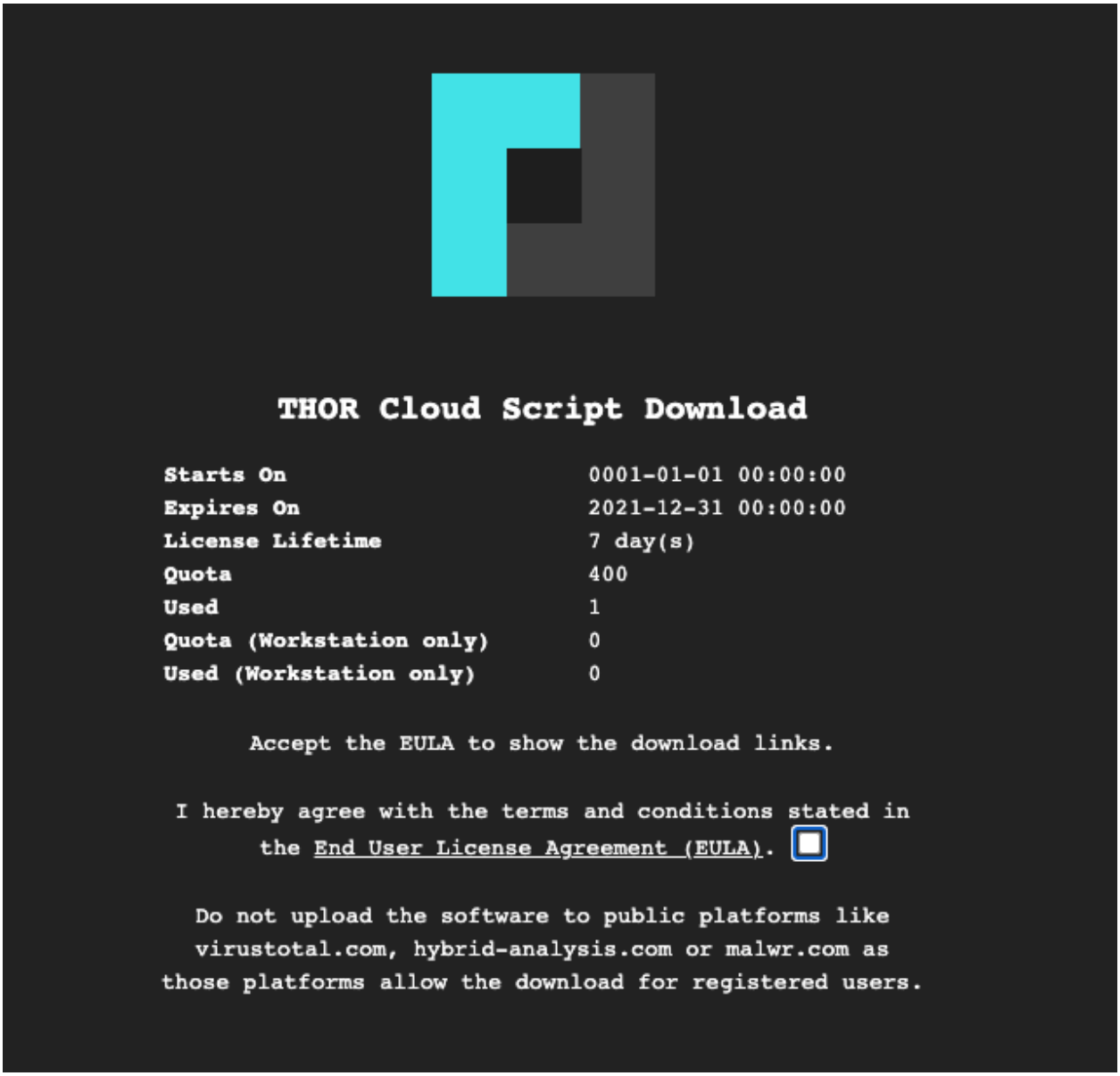


Fig. 3: THOR Seed Download Page

2.3.1 Modify the Default Configuration

In the section "PRESET CONFIGS" you can modify or choose different scan options.

```
159
160   # PRESET CONFIGS
161
162   # FULL with Lookback
163   # Preset template for a complete scan with a lookback of 2 days
164   # Run time: 40 minutes to 6 hours
165   # Specifics:
166   #   - runs all default modules
167   #   - only scans elements that have been changed or created within the last 14 days
168   #   - applies Sigma rules
169   # cloudconf: [!]PresetConfig_FullLookback [Full Scan with Lookback] Performs a full disk scan with all modules but
      only checks elements changed or created within the last 14 days - best for SOC response to suspicious events (5 to
      20 min)
170   $PresetConfig_FullLookback = @"
171   rebase-dir: $($OutputPath)  # Path to store all output files (default: script location)
172   nosoft: true           # Don't trottle the scan, even on single core systems
173   global-lookback: true  # Apply lookback to all possible modules
174   lookback: 14           # Log and Eventlog look back time in days
175   # cpulimit: 70         # Limit the CPU usage of the scan
176   sigma: true            # Activate Sigma scanning on Eventlogs
177   nofserrors: true       # Don't print an error for non-existing directories selected in quick scan
178   nocsv: true            # Don't create CSV output file with all suspicious files
179   noscanid: true         # Don't print a scan ID at the end of each line (only useful in SIEM import use cases)
180   nothordb: true         # Don't create a local SQLite database for differential analysis of multiple scans
181   "@
182
```

Fig. 4: Configuration Presets

THOR Seed already includes good presets that can just be "selected" further below in the section.

```
220
221   # SELECT YOU CONFIG
222   # Select your preset config
223   # Choose between: $PresetConfig_Full, $PresetConfig_Quick, $PresetConfig_FullLookback
224   $PresetConfig = $PresetConfig_FullLookback
225
```

Fig. 5: Preset Selection

A list of all options can be found here: https://github.com/NextronSystems/nextron-helper-scripts/tree/master/thor-help

The THOR manual contains a complete description of most of these features and can downloaded from the "Downloads" section in the Nextron customer portal.

2.3.2 Define False Positive Filters

THOR Seed also includes a section in which you could include false positive statements (separated by new line) and defined as regular expressions.

```
226   # False Positive Filters
227   $UseFalsePositiveFilters = $True
228   # The following new line separated false positive filters get
229   # applied to all log lines as regex values.
230   $PresetFalsePositiveFilters = @"
231   Could not get files of directory
232   Signature file is older than 60 days
233   \\Our-Custom-Software\\v1.[0-9]+\\
234   "@
```

Fig. 6: False Positive filters

It's important to use escaping as it is used in regular expressions to escape e.g., back slashes, periods, dollar and asterisk characters. The expression is applied to a full log line. The THOR manual has more information on these filters and a list of examples.

CHAPTER

THREE

START A THOR SCAN

3.1 Start a Live Response Session

You find different locations in Microsoft Defender Security Center that allow you to initiate a Live Response session.

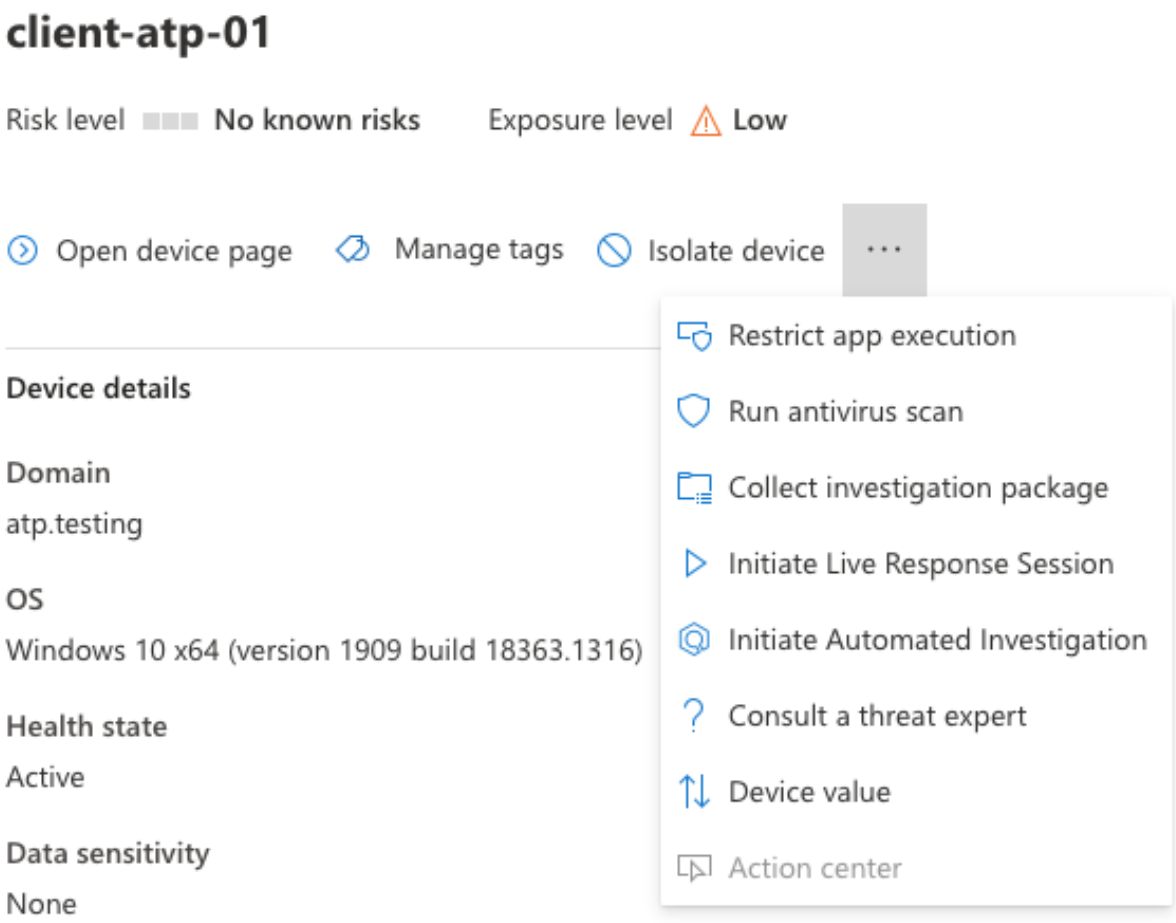


Fig. 1: Initiate Live Response Session

3.2 Upload THOR Seed

Use the button in the upper right corner of the window to upload "thor-seed.ps1" into the Live Response script library.

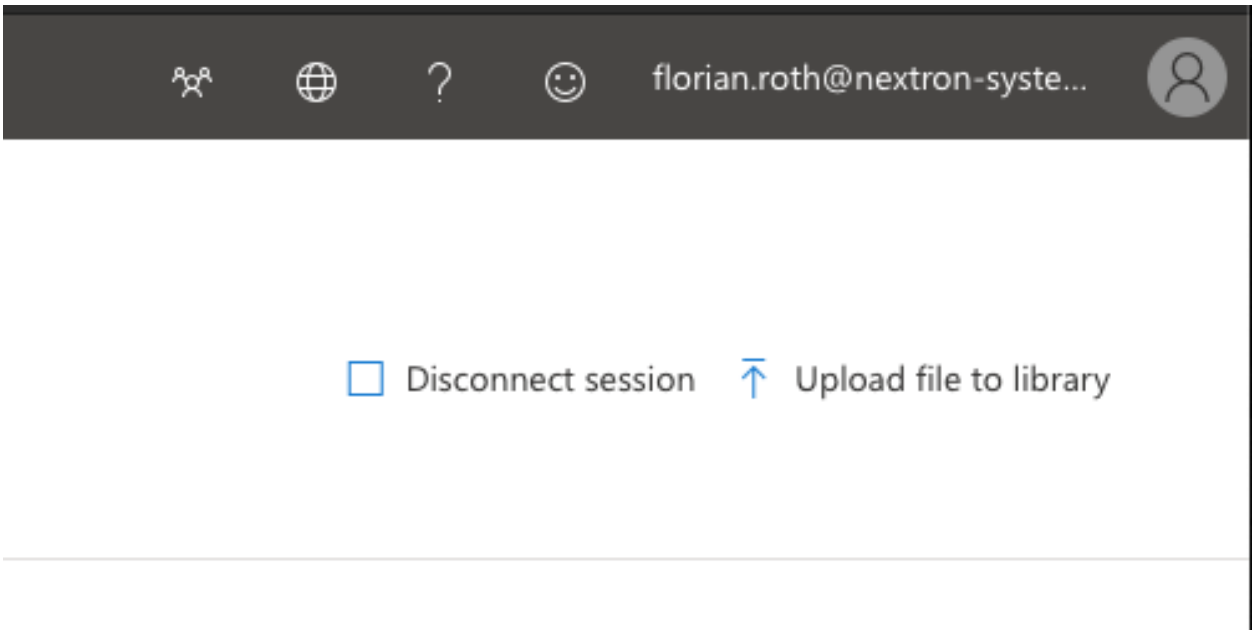


Fig. 2: Upload Button

Make sure to check "Overwrite file" to replace an older version of THOR Seed in your library.

3.3 Run THOR Seed

After uploading THOR Seed to the Live Response script library, you can start the script with the "run" command.

3.4 Interrupted THOR Seed Sessions

Microsoft Defender Security Center allows scripts a run time of a maximum of 30 minutes and then terminates the script. However, the sub process "thor64.exe" is still running.

3.4.1 Check the Scan Status

In THOR Seed versions before v0.18, it was difficult to get the scan status of THOR in the background or find the log files that THOR produces during the scan and the HTML report that is generated at the end of the scan.

Users can check of THOR is still running with

```
processes -name thor64.exe
```

Since THOR Seed version 0.18 you just run thor-seed.ps1 again and will see the information that THOR is still running, where to find the current log file and the last 3 log lines of that file.

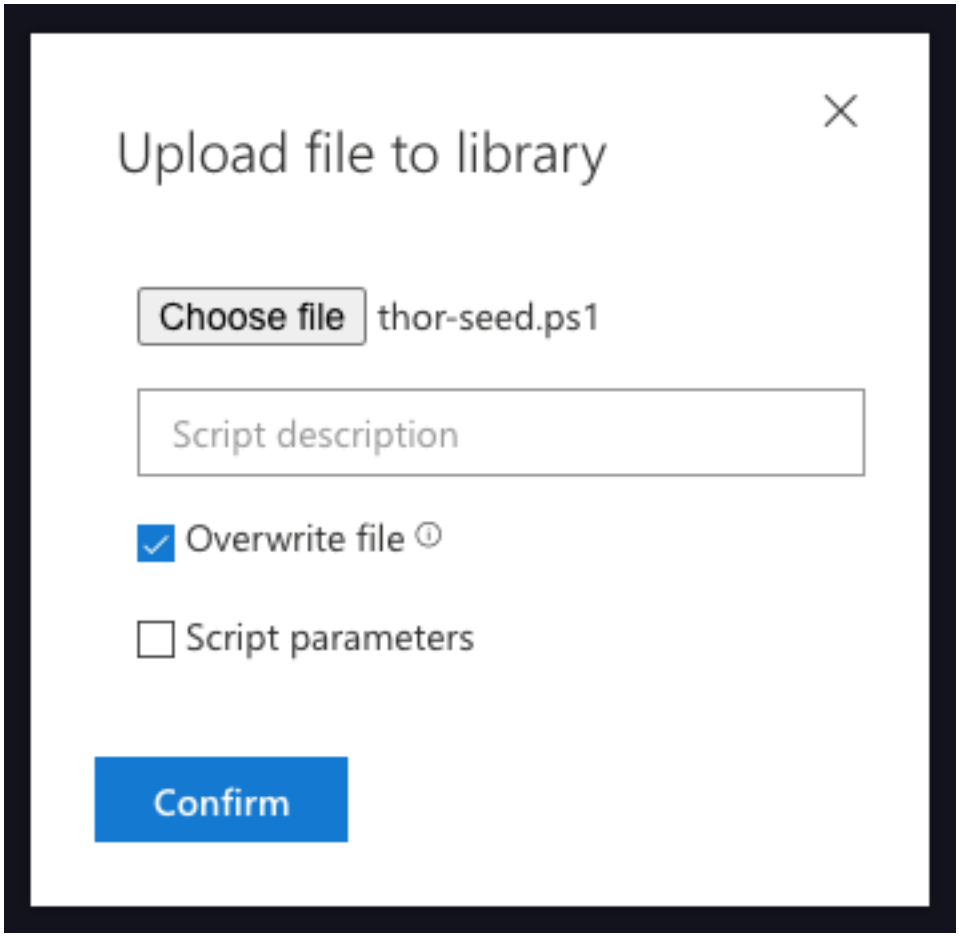


Fig. 3: Upload THOR Seed

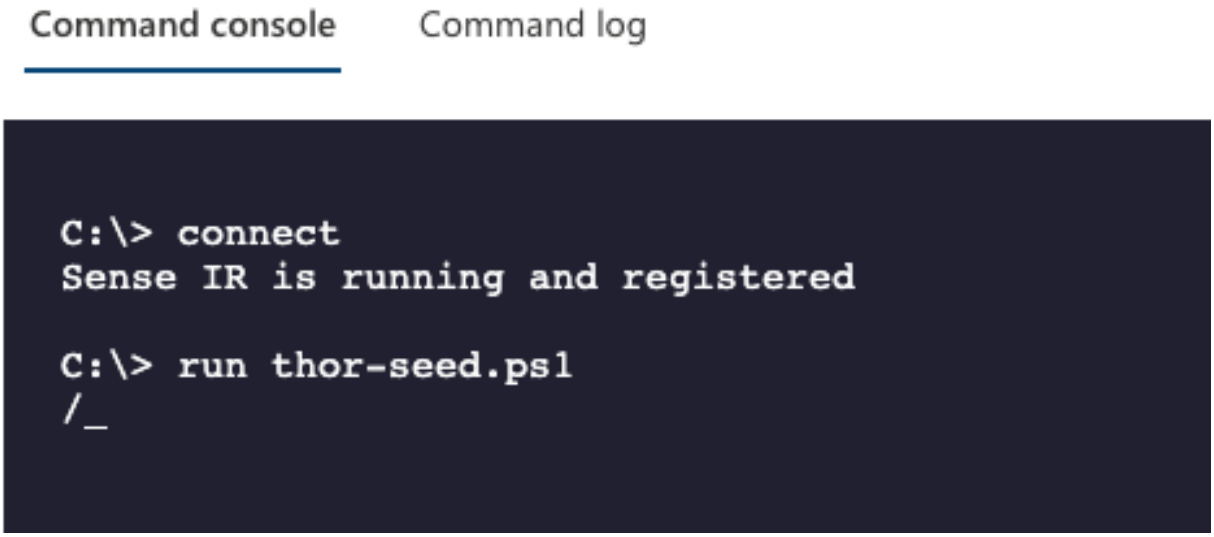


Fig. 4: Run thor-seed.ps1 in Live Response session

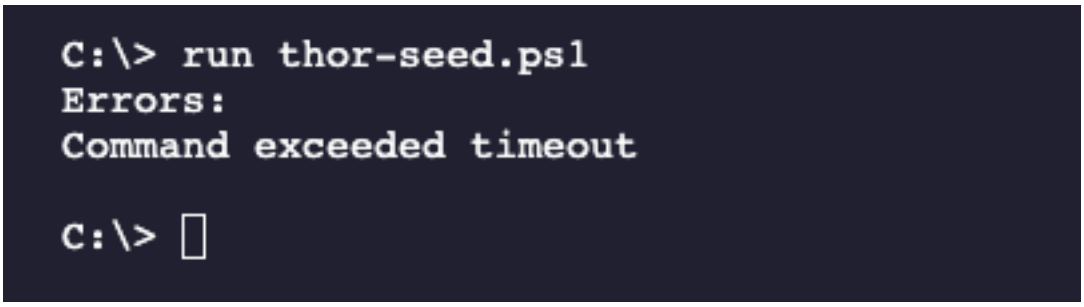


Fig. 5: Interrupted scan due to exceeded timeout

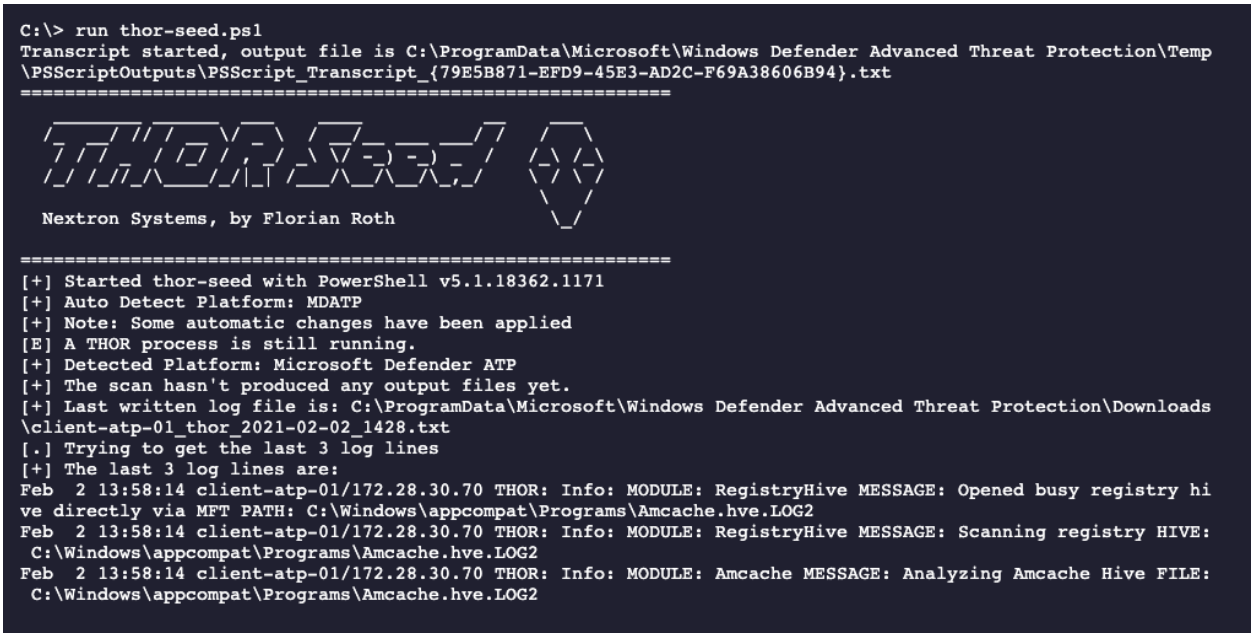


Fig. 6: THOR Seed start while THOR is still running

You can run the script as often as you like to get an information on the current status of the scan. A normal scan takes between 20 and 180 minutes to complete.

3.4.2 Detect a Finished Scan

The moment that you run "thor-seed.ps1" while "thor64.exe" has finished its job in the background, you get a listing of all generated log files and HTML reports in the output directory and commands to download them and remove them from the end system.

It shows a list of three actions to proceed:

1. Retrieve the available log files and HTML reports
   get file "C:\ProgramData\Microsoft\Windows Defender Advanced…
2. Use the following command to clean-up the output directory
   run thor-seed.ps1 -parameters "-Cleanup"
3. Start a new THOR scan with
   run thor-seed.ps1

```
C:\> run thor-seed.ps1
Transcript started, output file is C:\ProgramData\Microsoft\Windows Defender Advanced Threat Protecti
on\Temp\PSScriptOutputs\PSScript_Transcript_{8890739E-DC5D-4432-92BA-A5DAD211BE42}.txt
===========================================================
   ________ ______  ___    ____          __   ___
  /_  __/ // / __ \/ _ \  / __/__ ___ ___/ /  /   \
   / / / _  / /_/ / , _/ _\ \/ -_) -_) _  /  /_\ /_\
  /_/ /_//_/\____/_/|_| /___/\__/\__/\_,_/   \ / \ /
                                              \   /
  Nextron Systems, by Florian Roth             \_/

===========================================================
[+] Started thor-seed with PowerShell v5.1.18362.1171
[+] Auto Detect Platform: MDATP
[+] Note: Some automatic changes have been applied
[+] Detected Platform: Microsoft Defender ATP
[E] Cannot start new THOR scan as long as old report files are present
A.) Retrieve the logs and reports needed
    getfile "C:\ProgramData\Microsoft\Windows Defender Advanced Threat Protection\Downloads\client-at
p-01_thor_2021-02-02_1817.txt"
    getfile "C:\ProgramData\Microsoft\Windows Defender Advanced Threat Protection\Downloads\client-at
p-01_thor_2021-02-02_1817.html"
B.) Use the following command to cleanup the output directory and remove all previous reports
    run thor-seed.ps1 -parameters "-Cleanup"
C.) Run THOR Seed again
    run thor-seed.ps1


C:\> _
```

Fig. 7: THOR Seed run shows previously finished scan

3.5 Retrieve the Results

The output of THOR Seed already contains the right commands to download a report after the scan has finished.

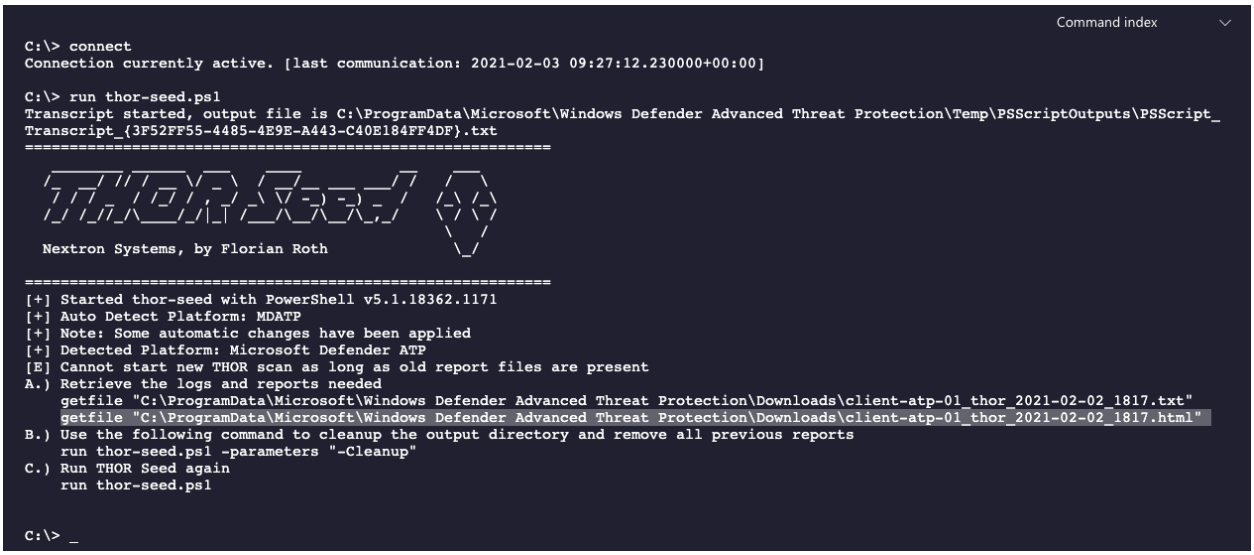


Fig. 8: THOR Seed output on a system with finished scan

Simply copy and paste the full "getfile" command line to retrieve the HTML report.

```
getfile "C:\\ProgramData\\Microsoft\\Windows Defender Advanced Threat Protection\\
↪Downloads\\client-atp-01\_thor\_2021-02-02\_1817.html"
```

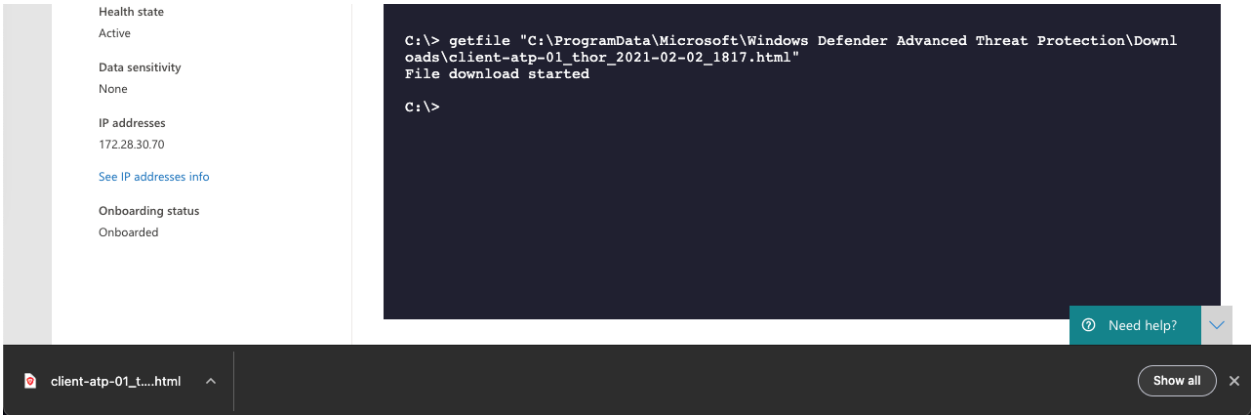
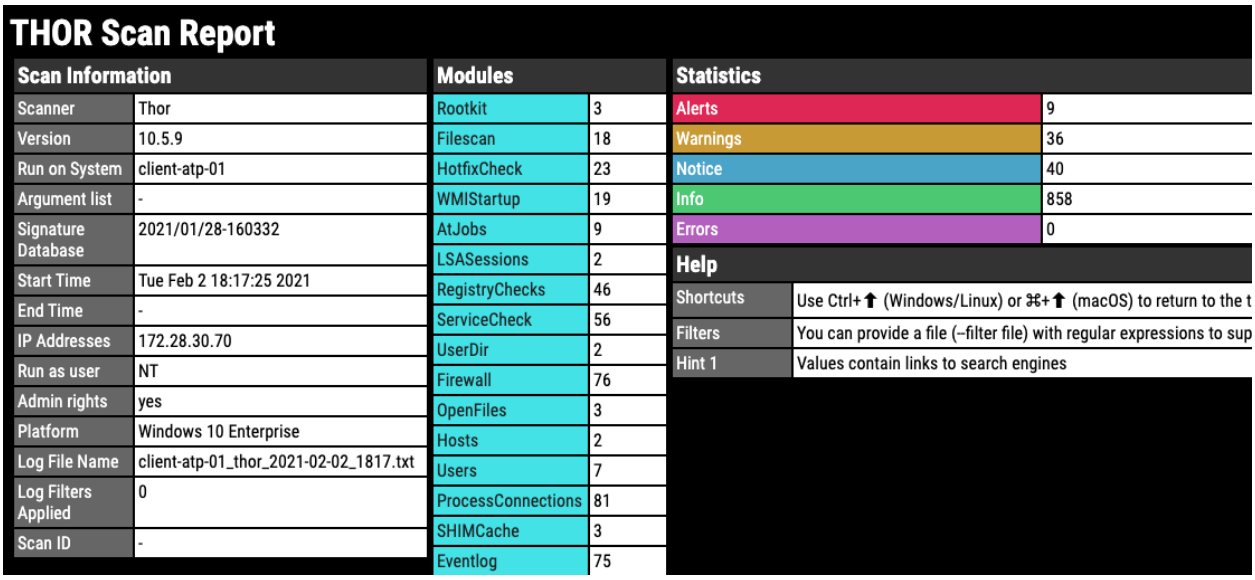


Fig. 9: HTML Report Download in Browser



THOR Scan Report

Scan Information	
Scanner	Thor
Version	10.5.9
Run on System	client-atp-01
Argument list	-
Signature Database	2021/01/28-160332
Start Time	Tue Feb 2 18:17:25 2021
End Time	-
IP Addresses	172.28.30.70
Run as user	NT
Admin rights	yes
Platform	Windows 10 Enterprise
Log File Name	client-atp-01_thor_2021-02-02_1817.txt
Log Filters Applied	0
Scan ID	-

Modules	
Rootkit	3
Filescan	18
HotfixCheck	23
WMIStartup	19
AtJobs	9
LSASessions	2
RegistryChecks	46
ServiceCheck	56
UserDir	2
Firewall	76
OpenFiles	3
Hosts	2
Users	7
ProcessConnections	81
SHIMCache	3
Eventlog	75

Statistics	
Alerts	9
Warnings	36
Notice	40
Info	858
Errors	0

Help	
Shortcuts	Use Ctrl+⬆ (Windows/Linux) or ⌘+⬆ (macOS) to return to the t
Filters	You can provide a file (--filter file) with regular expressions to sup
Hint 1	Values contain links to search engines

Fig. 10: THOR HTML Report

3.6 Cleanup

In order to run another THOR scan, you have to remove all previous log files and HTML reports using the following command:

```
run thor-seed.ps1 -parameters "-Cleanup"
```

After removing the text logs and HTML reports you can start a new scan on this end system.

CHAPTER

FOUR

FAQS

4.1 Why does my scan suddenly terminate?

Live response applies a rather disadvantages timeout for PowerShell scripts run within a Live Response session, which is 30 minutes by default. If a scan takes longer to complete, it gets terminated.

We recommend

- using scan settings that allow the scan to terminate within 30 minutes
- increasing the timeout to a higher value in future versions of Microsoft Defender ATP

Since version 0.18 of THOR Seed, this situation gets handled automatically. Just run thor-seed.ps1 another time to get information on the thor64.exe process that still runs in the background. It will show you information on the log file and print commands that you can use to download the log file and HTML report once THOR finished its work.

4.2 Why can't I see a progress indicator?

The scripting environment doesn't give us the opportunity to report back any status information before the script terminates. All output written to STDOUT and STDERR will be returned at the end of the script execution although it appears earlier.

Unfortunately, it is not possible to return information before the scan terminates.

4.3 I cannot start a new THOR scan due to old log files?

Simply run a cleanup before starting a new scan.

```
run thor-seed.ps1 -parameters "-Cleanup"
```

4.4 I can't start a scan and get the error "THOR already running", why?

It is possible that you've interrupted a previous script run with CTRL+C and got back to the shell. In Live Response, sub processes started by scripts running from the script library don't get killed on CTRL+C.

It is highly likely that a THOR scan is still running in the background without you knowing.

Since version 0.18 of THOR Seed, this situation gets handled automatically. Just run thor-seed.ps1 another time to get information on the thor64.exe process that still runs in the background. It will show you information on the log file and print commands that you can use to download the log file and HTML report once THOR finished its work.

4.5 Does each scan use up one of my licenses?

Once you generate a license for a system, this license has a certain lifetime (e.g. 48 hours). You can start as many scans within that lifetime without using a new license from your quota.

THOR doesn't stop if the scan takes longer than the license lifetime.

If you start a new scan on a system that has be scanned in the past and the old license is expired, a new license will be generated and count against the quota.

4.6 Can I use my own IOCs and YARA signatures with THOR Seed?

Not yet but we'll add an option to the THOR Seed PowerShell script to download and use a ZIP archive with custom IOCs and YARA signatures from a user defined location.

CHAPTER

FIVE

LINKS AND REFERENCES

THOR Cloud Integration Into Microsoft Defender ATP Web Page

https://www.nextron-systems.com/thor-cloud/microsoft-defender-atp/

Webinar with Patriot Consulting

https://www.nextron-systems.com/2020/06/19/webinar-mitigating-persistent-threats-using-microsoft-defender-atp-and-thor/

First Complete PoC with Microsoft Defender ATP

https://www.nextron-systems.com/2020/01/07/thor-integration-into-windows-defender-atp/

THOR Seed Github Page

https://github.com/NextronSystems/nextron-helper-scripts/tree/master/thor-seed

CHAPTER

SIX

INDICES AND TABLES

- search