# THOR with Microsoft Defender for Endpoint

**Nextron Systems GmbH**

**Oct 08, 2025**

# CONTENTS:

This documentation is intended to provide guidance on how to use THOR with Microsoft Defender for Endpoint. We will provide a few different ways download and execute THOR on your endpoints via Microsoft Defender for Endpoint.

CHAPTER

ONE

# REQUIREMENTS

## 1.1 Supported Operating Systems

The operating systems are limited to the set that supports the Microsoft Defender for Endpoint "Live Response" feature.

Table 1: Table 1 - Supported Operating Systems

| Operating System | Version |
|---|---|
| **Windows 10 & 11** | Version 1909 or later |
| | Version 1903 with KB4515384 |
| | Version 1809 (RS 5) with with KB4537818 |
| | Version 1803 (RS 4) with KB4537795 |
| | Version 1709 (RS 3) with KB4537816 |
| **macOS** | Minimum required version: 101.43.84. Supported for Intel-based and ARM-based macOS devices. |
| **Linux** | Minimum required version: 101.45.13 |
| **Windows Server 2012** | R2 with KB5005292 |
| **Windows Server 2016** | with KB5005292 |
| **Windows Server 2019** | Version 1903 or (with KB4515384) later |
| | Version 1809 (with KB4537818) |
| **Windows Server 2022** | |

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

## 1.2 Enable "Live Response" Feature

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

Additionally, you need to change the Live response unsigned script execution option in the same page, which allows you to run unsigned[1] scripts in a live response session.

**Hint**

We recommend that you sign your scripts with a code signing certificate to avoid the need to change this setting.

[1] thor-seed.ps1 is an unsigned powershell script

## 1.3 Hardware Requirements

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

Table 2: Table 2 - Hardware Requirements

| Minimum | Recommended |
|---|---|
| 1 CPU Core | 2+ CPU Cores |
| 1 GB of RAM | 8+ GB of RAM |
| 100 MB of temporary Disk Space | |

**Hint**

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

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

### 1.4.1 On Investigated Workstations

Table 3: Table 3 - Remote Hosts

| Variant | Remote Host | Port |
|---|---|---|
| THOR Seed | cloud.nextron-systems.com | 443/tcp |
| THOR Cloud | thor-cloud.nextron-services.com | 443/tcp |

**Hint**

Above FQDNs resolve to multiple IP addresses. See https://www.nextron-systems.com/hosts/.

### 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

# THOR SEED

This section focuses on our powershell script `thor-seed.ps1`. THOR Seed is a script which can be configured to retrieve THOR and a valid license from different sources, and execute a THOR scan.

If you want to use the "Live Response" feature in conjunction with THOR on any other Operating System than Windows, you can use *THOR Cloud*, or create your own scripts.

**Hint**

THOR Seed is only available as a powershell script, hence it can only be executed on Windows systems.

## 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 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 "Cloud" 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

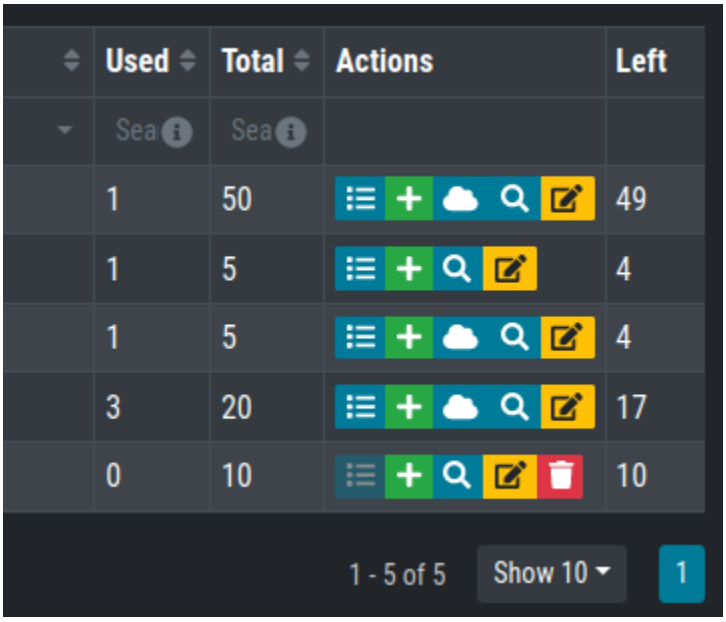


Fig. 2: Button that leads to the THOR Seed download page

### 2.3.1 Modify the Default Configuration

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

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

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.

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.

## 2.4 Start a Live Response Session

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

## 2.5 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.

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

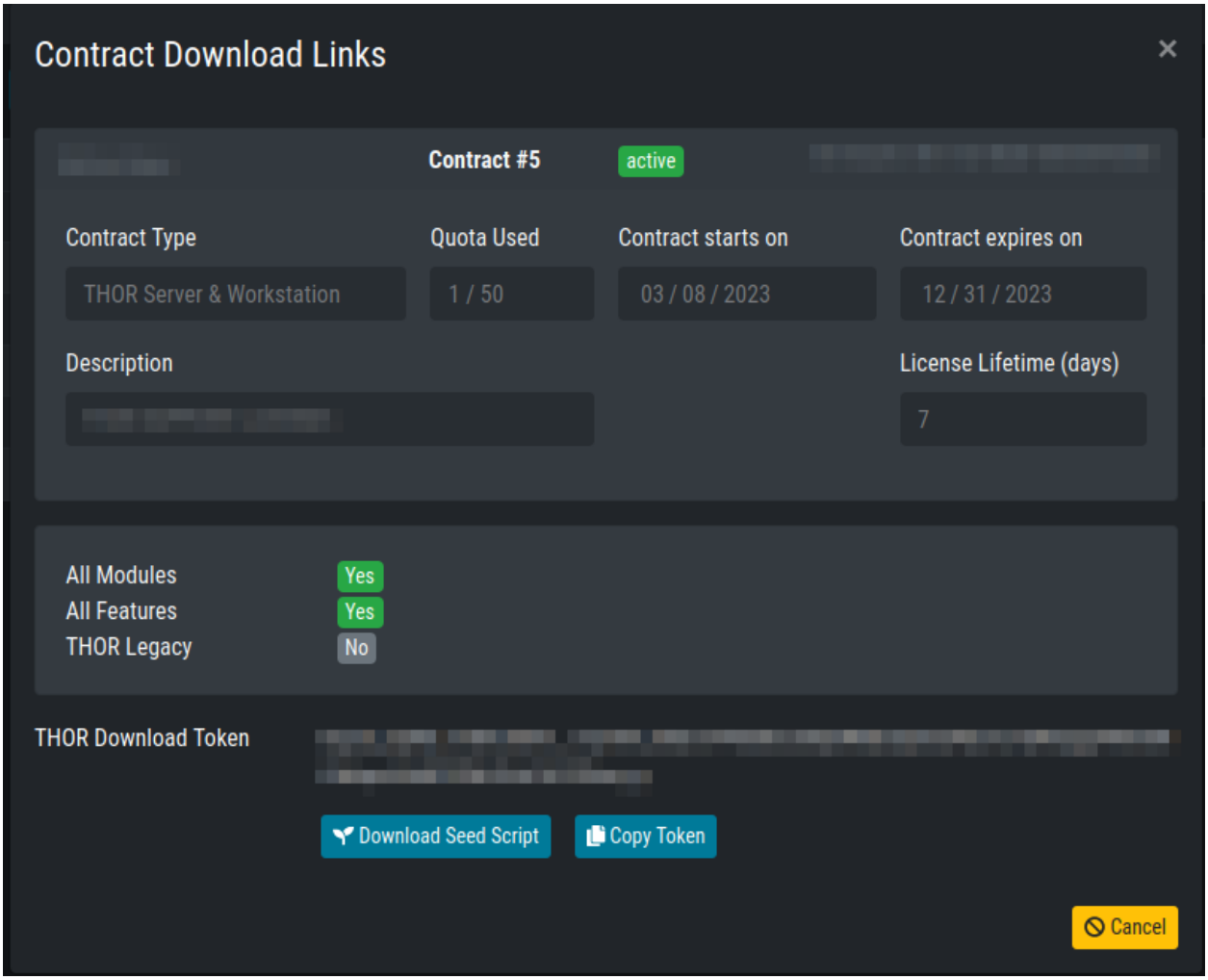


Fig. 3: THOR Seed Download Page

```
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

```
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

```
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

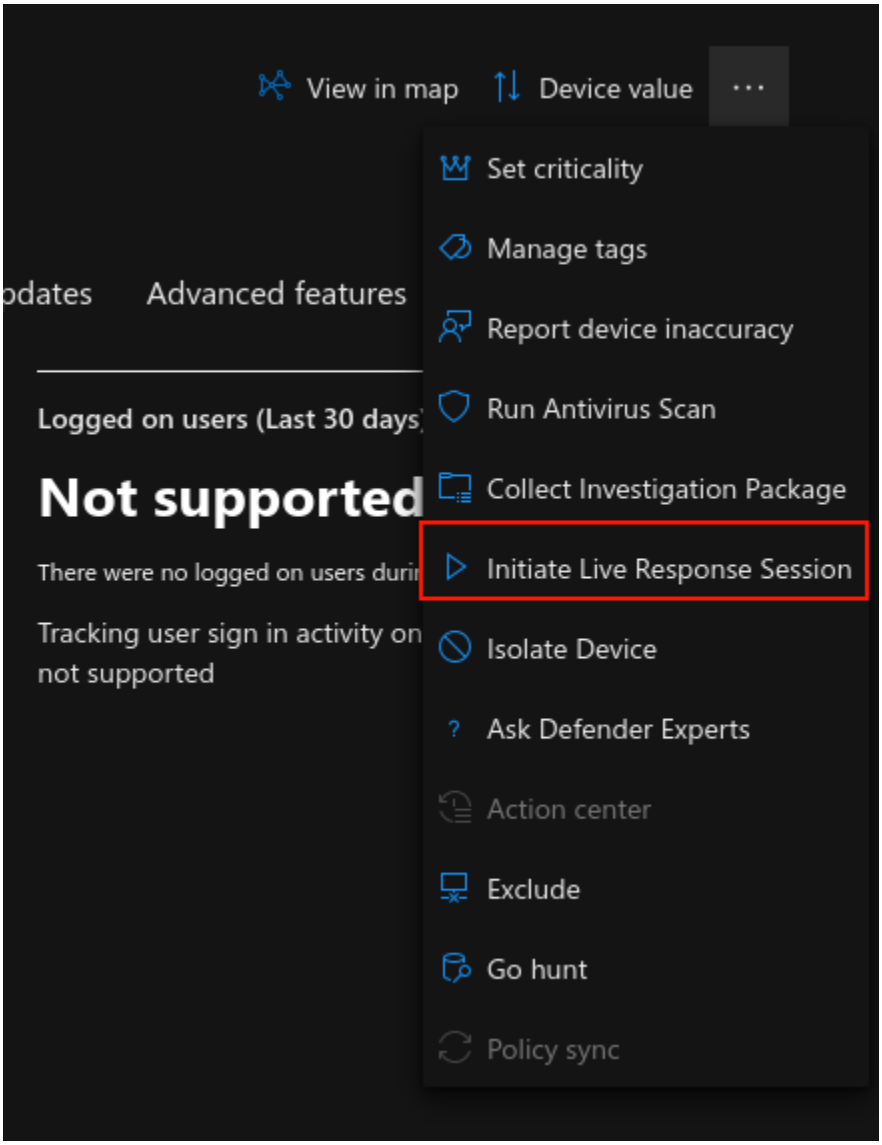


Fig. 7: Initiate Live Response Session

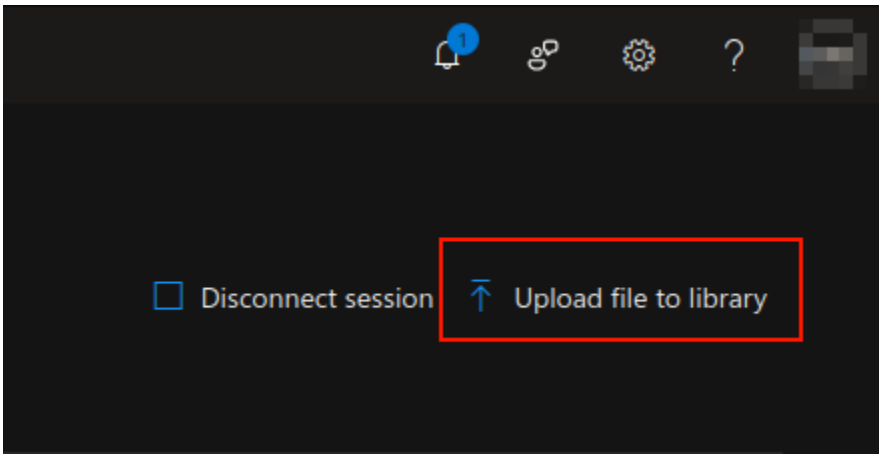


Fig. 8: Upload Button

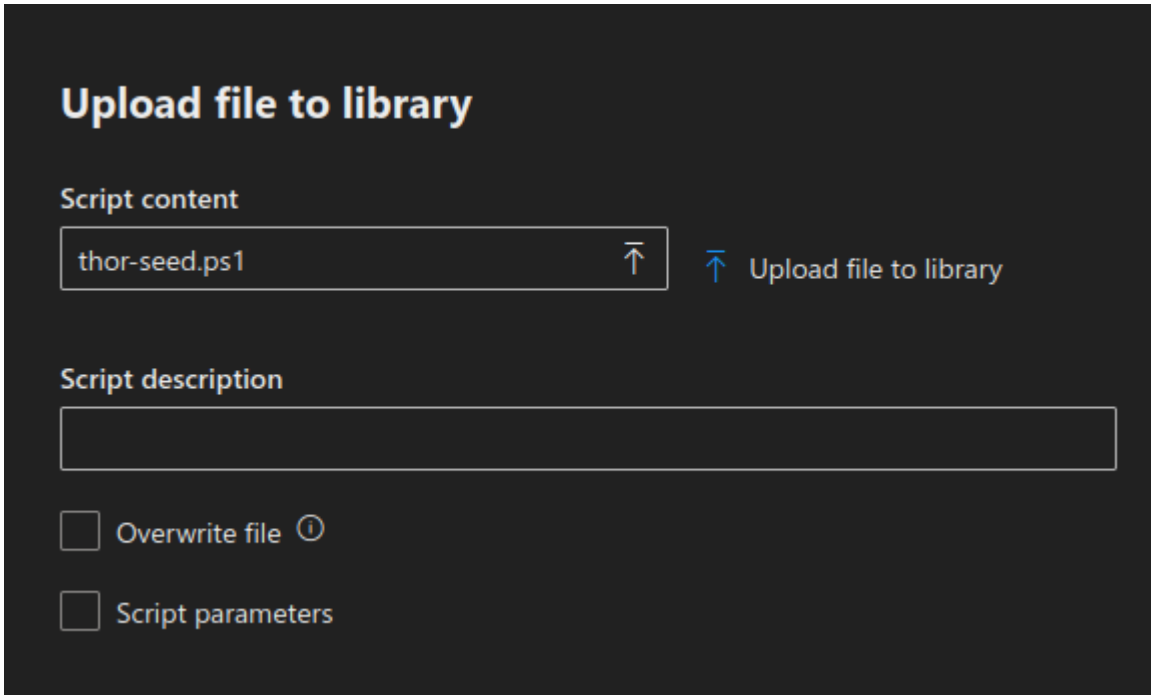


Fig. 9: Upload THOR Seed

## 2.6 Run THOR Seed

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

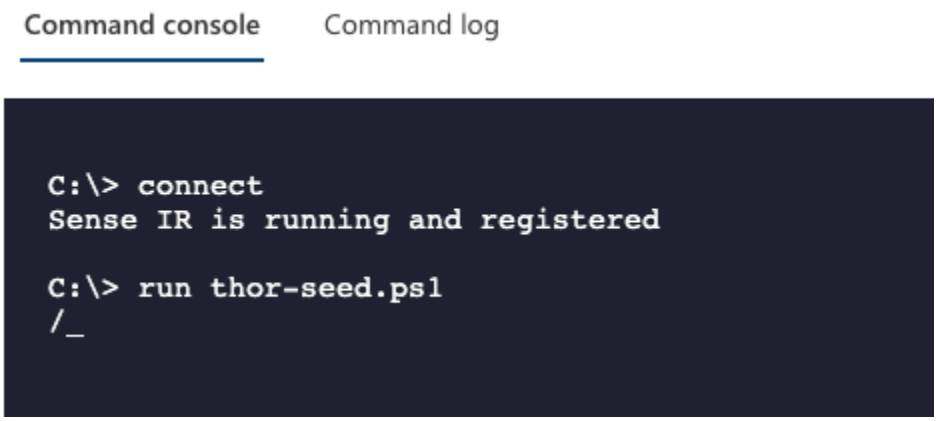


Fig. 10: Run thor-seed.ps1 in Live Response session

## 2.7 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.

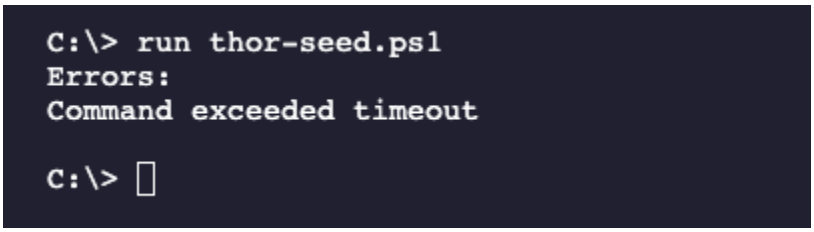


Fig. 11: Interrupted scan due to exceeded timeout

### 2.7.1 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

```
C:\> 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.

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.

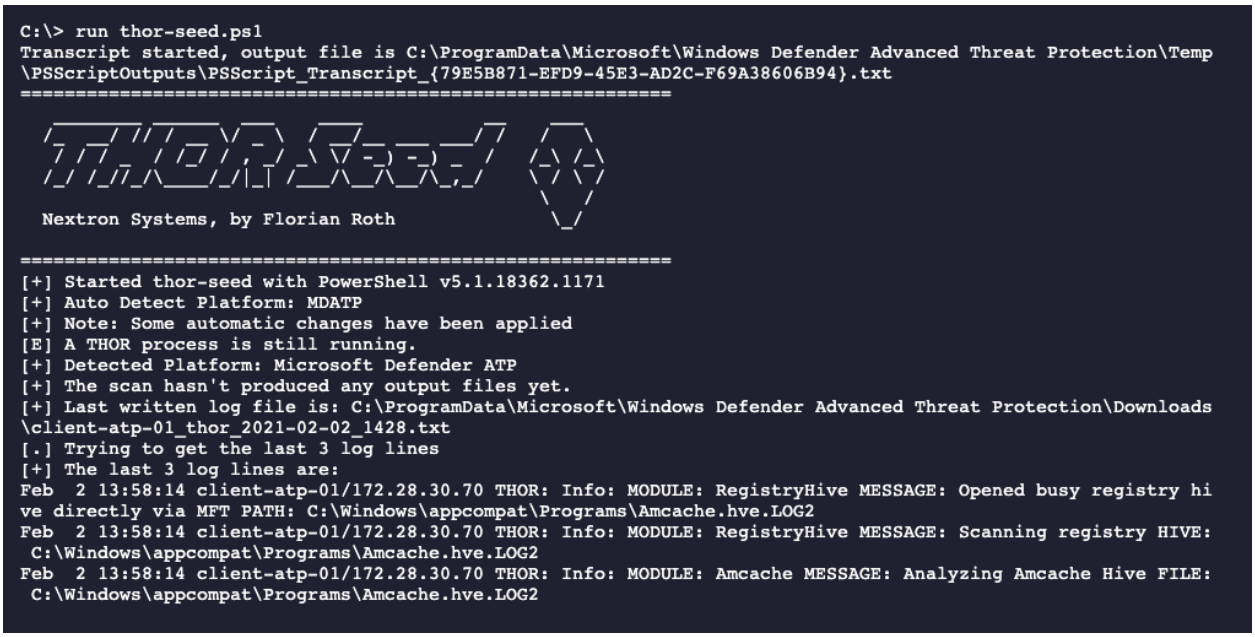


Fig. 12: THOR Seed start while THOR is still running

### 2.7.2 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

```
C:\> get file "C:\ProgramData\Microsoft\Windows Defender Advanced...
```

2. Use the following command to clean-up the output directory

```
C:\> run thor-seed.ps1 -parameters "-Cleanup"
```

3. Start a new THOR scan with

```
C:\> run thor-seed.ps1
```

## 2.8 Retrieve the Results

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

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

```
C:\> getfile "C:\ProgramData\Microsoft\Windows Defender Advanced Threat Protection\
↪Downloads\client-atp-01_thor_2021-02-02_1817.html"
```

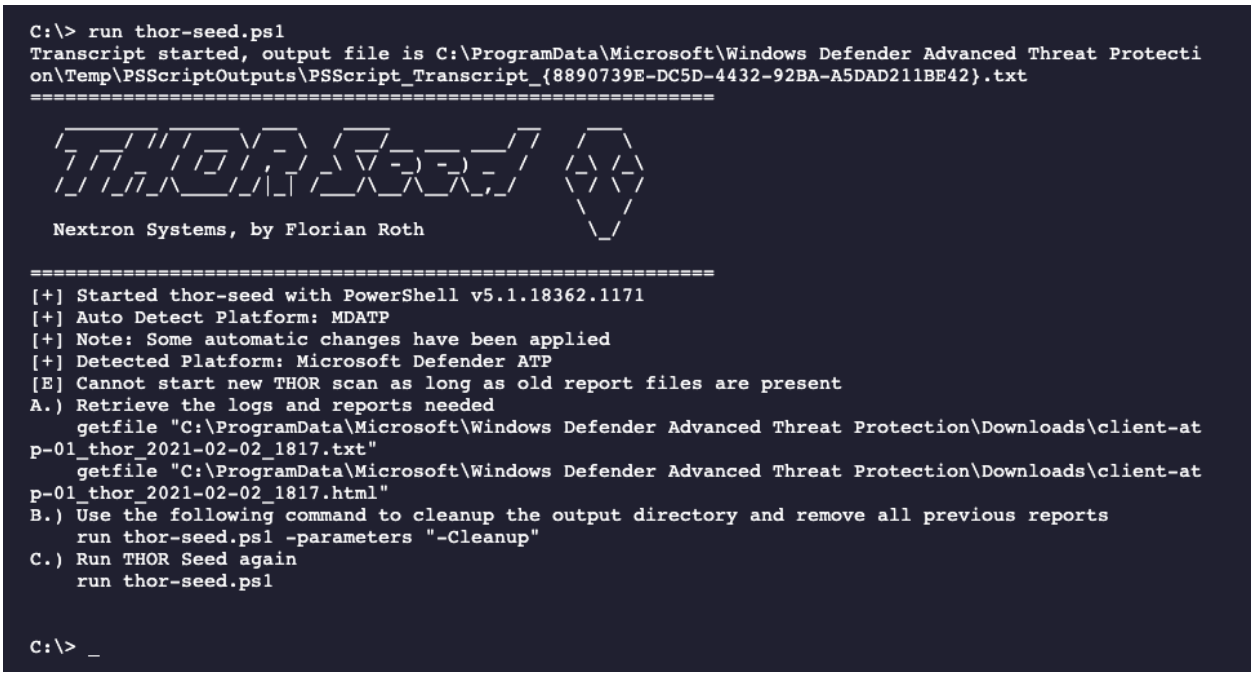


Fig. 13: THOR Seed run shows previously finished scan

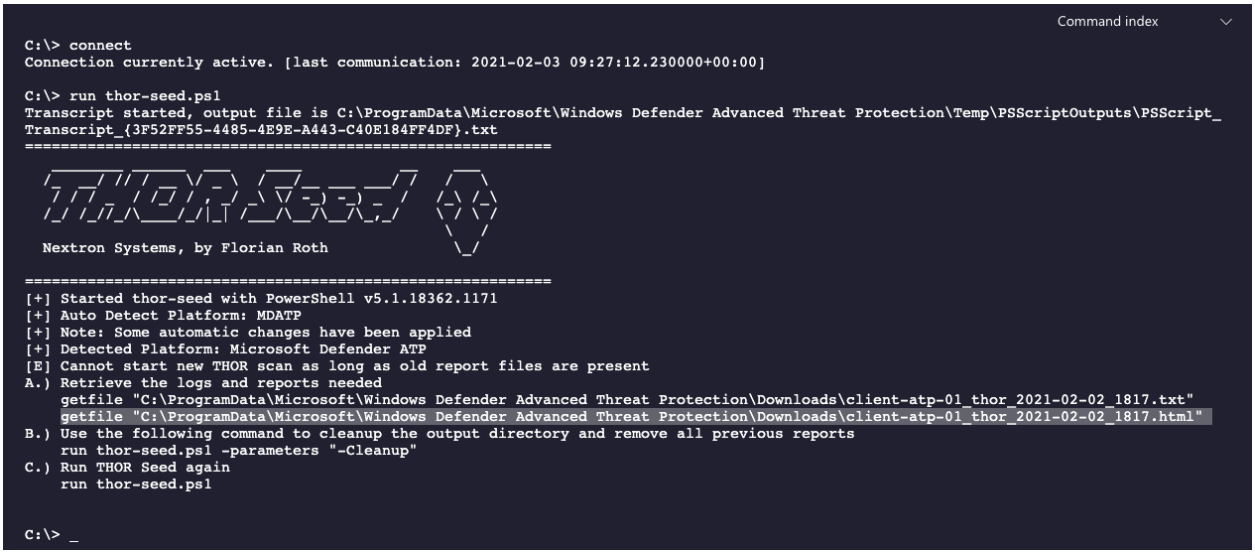


Fig. 14: THOR Seed output on a system with finished scan

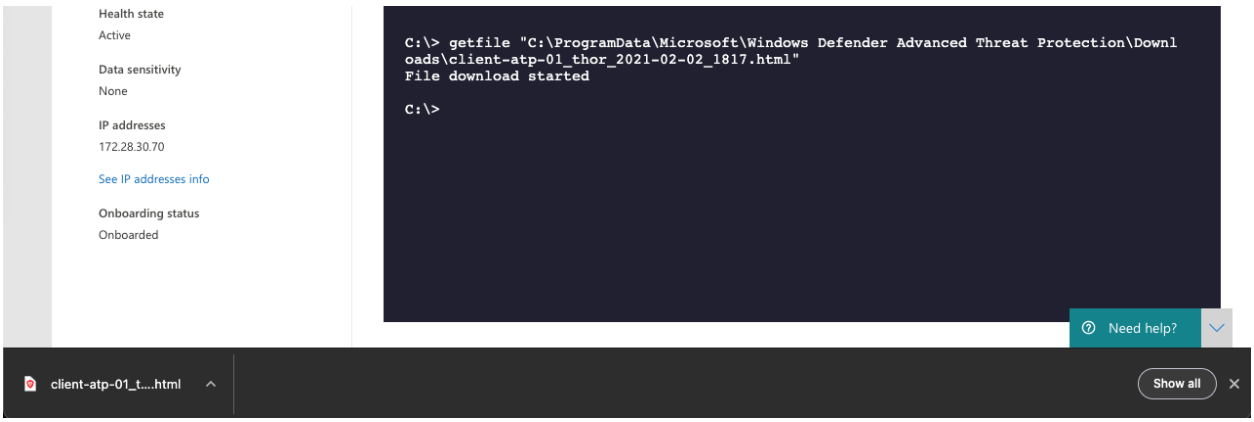


Fig. 15: HTML Report Download in Browser

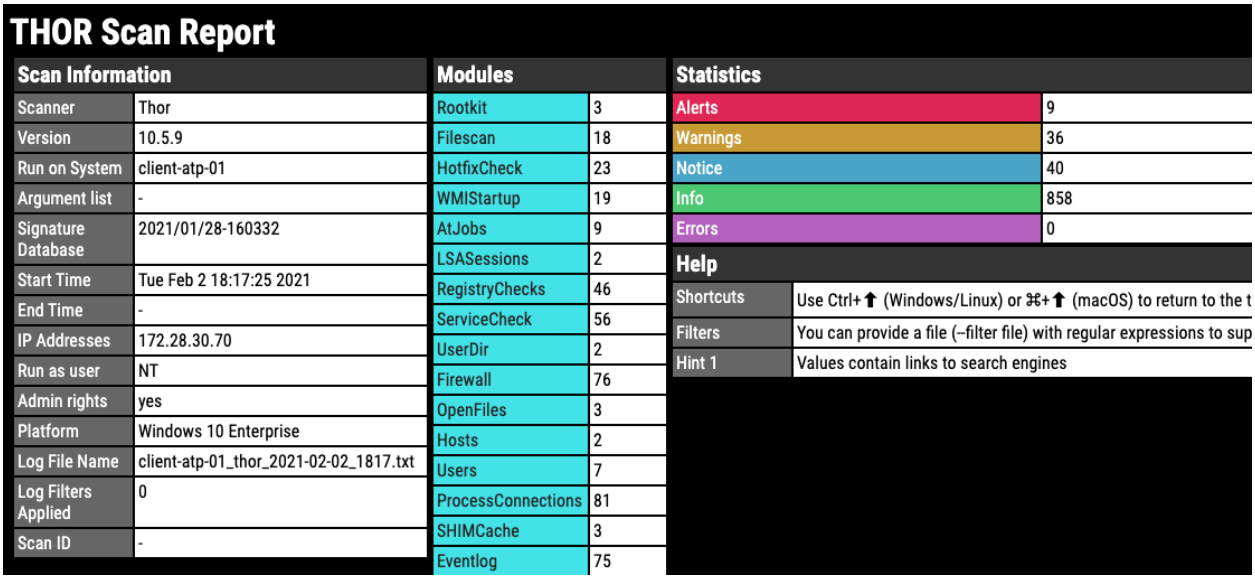


Fig. 16: THOR HTML Report

## 2.9 Cleanup

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

```
C:\> 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

THREE

# THOR CLOUD

This section focuses on our online platform `THOR Cloud`.

THOR Cloud eliminates the need for on-premise systems for licensing and scanner package downloads. With THOR Cloud, all you need is a small yet powerful tool known as the THOR Cloud launcher. Simply bring it to your endpoint or allow end users to download and execute it themselves.

## 3.1 Download THOR Cloud Launcher Script

Once you logged into your THOR Cloud account, create a new Campaign or use an existing one. In the Campaign details, download the Launcher in the top right corner. You need to download the Script for your Operating System, as the Live Response feature only allows the execution of scripts.

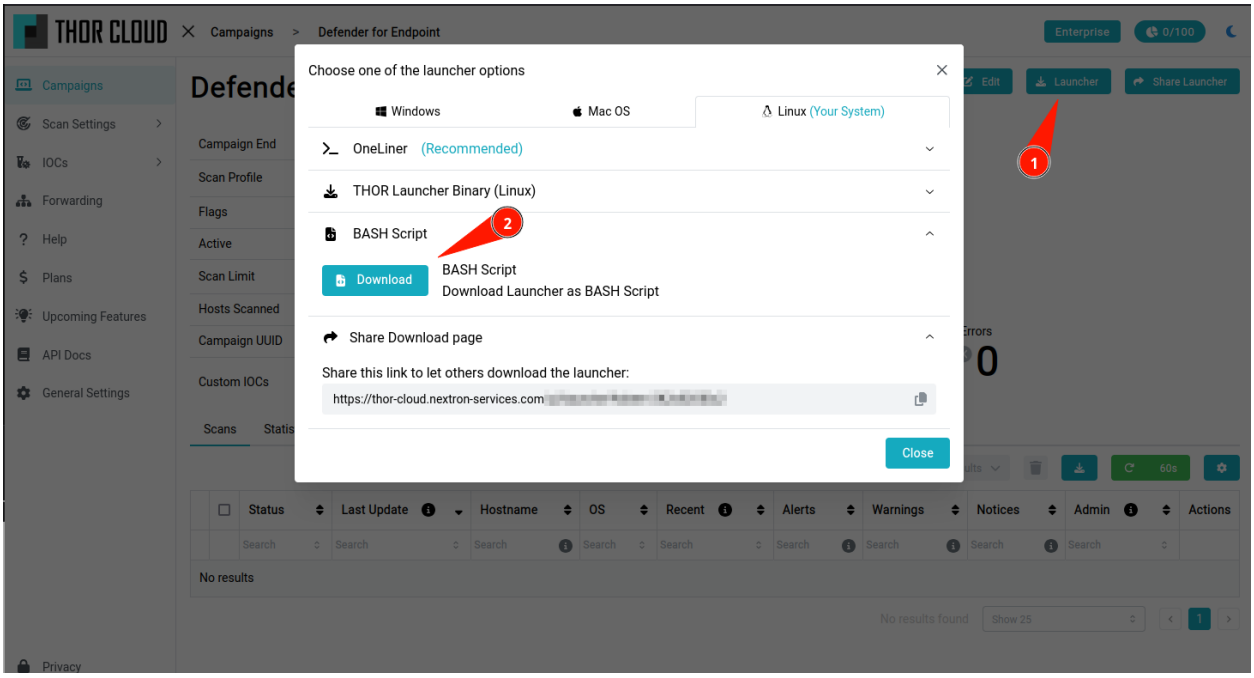


Fig. 1: Download the THOR Cloud Launcher Script

## 3.2 Start a Live Response Session

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

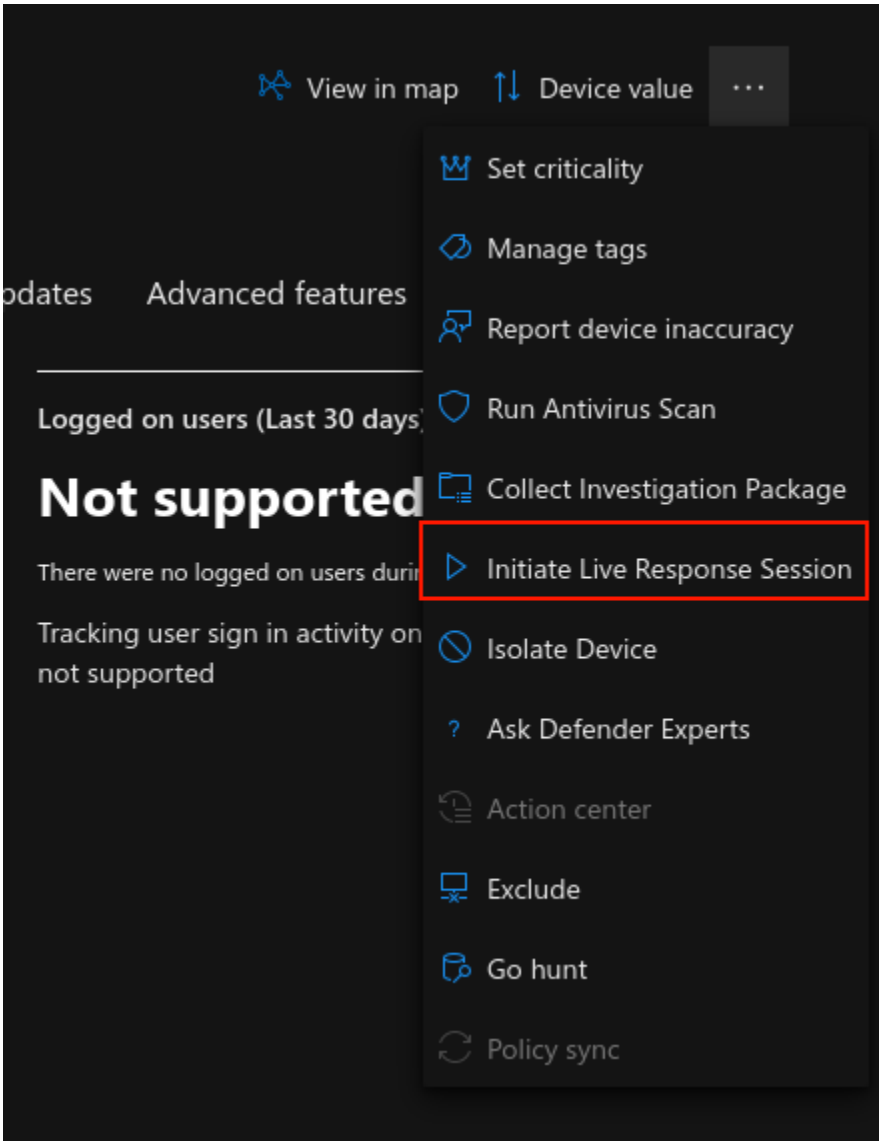


Fig. 2: Initiate Live Response Session

## 3.3 Upload THOR Cloud Launcher

Use the button in the upper right corner of the window to upload the THOR Cloud Launcher script into the Live Response script library.

Make sure to check "Overwrite file" to replace an older version of THOR Seed in your library if needed. Make sure you are using the correct script for your target OS.

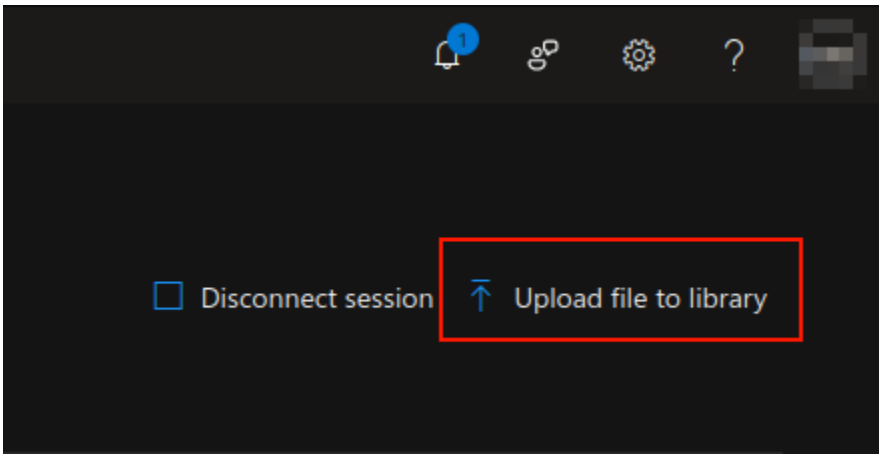


Fig. 3: Upload Button

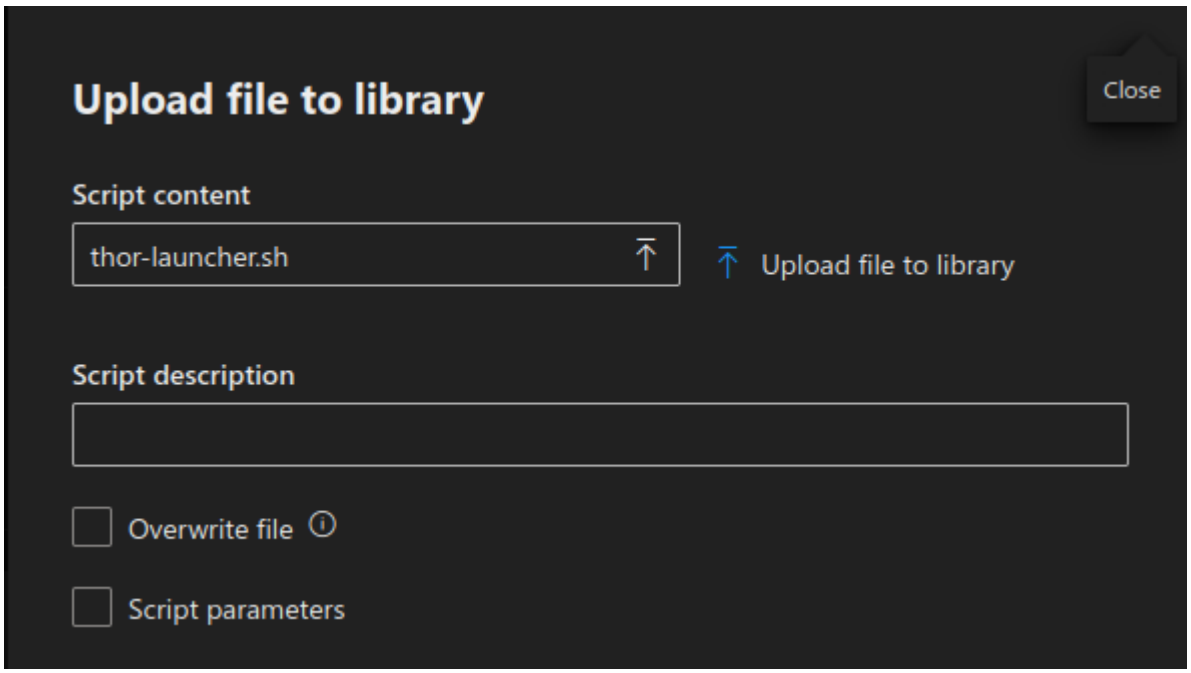


Fig. 4: Upload THOR Seed

## 3.4 Run THOR Cloud Launcher

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

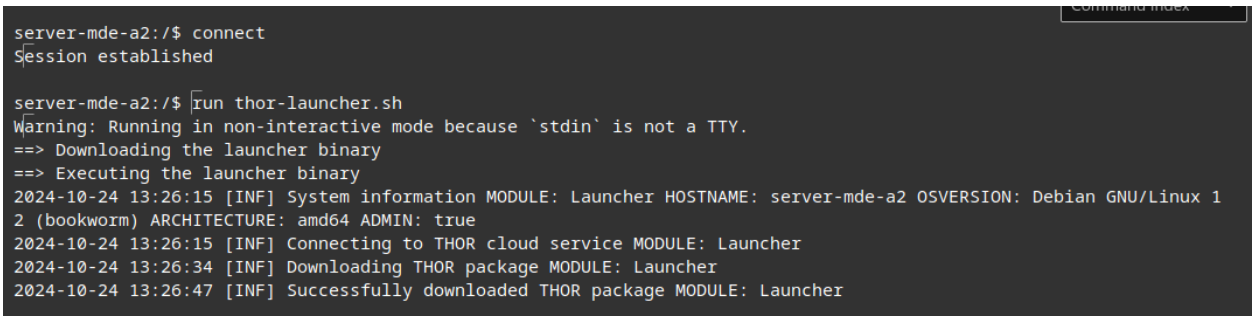


Fig. 5: Run thor-seed.sh in Live Response session on Linux

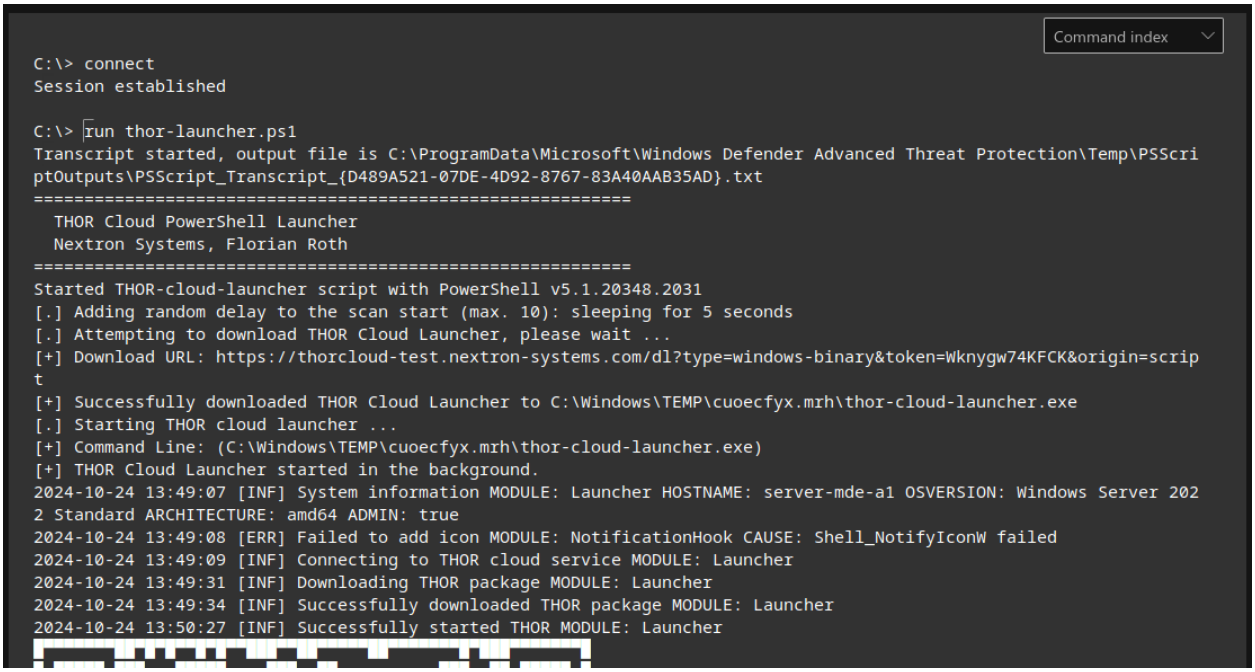


Fig. 6: Run thor-seed.ps1 in Live Response session on Windows

You can see the status of the running scan in your Campaign View:

You can close the Live Response Session if you want to, since the THOR process will continue to run in the background.

You can reuse the Thor-Launcher scripts for other systems, as the only unique part is the Campaign ID. If you want to scan hosts within another campaign, make sure to use the script from the other campaign.

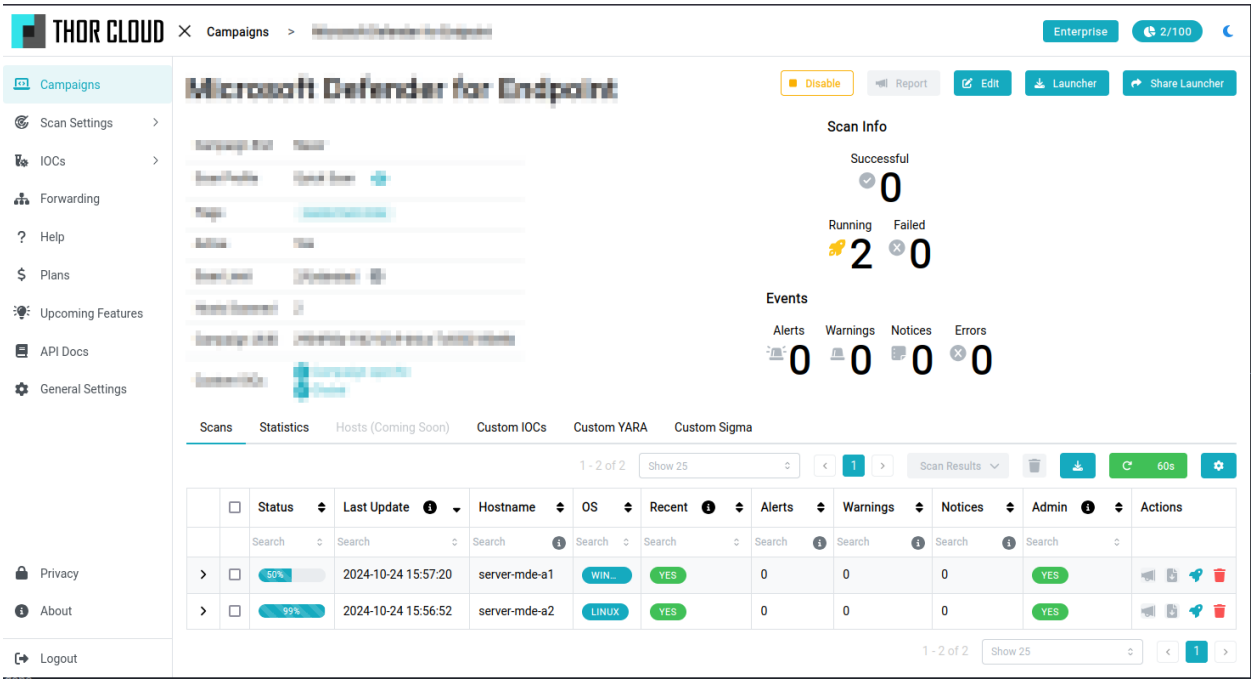


Fig. 7: Running THOR via Live Response on Linux

CHAPTER

# FOUR

# FAQS

## 4.1 THOR Seed

### 4.1.1 Scan is terminating

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.

If `thor64.exe` is still running when you start THOR seed, you will get information regarding the current scan.

If `thor64.exe` is finished, you will get some example commands to retrieve your files and clean up the reports of the previous scan.

### 4.1.2 No 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.

### 4.1.3 Old log files prevent new scan

Simply run a cleanup before starting a new scan.

```
C:\> run thor-seed.ps1 -parameters "-Cleanup"
```

### 4.1.4 THOR alreay running error

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.

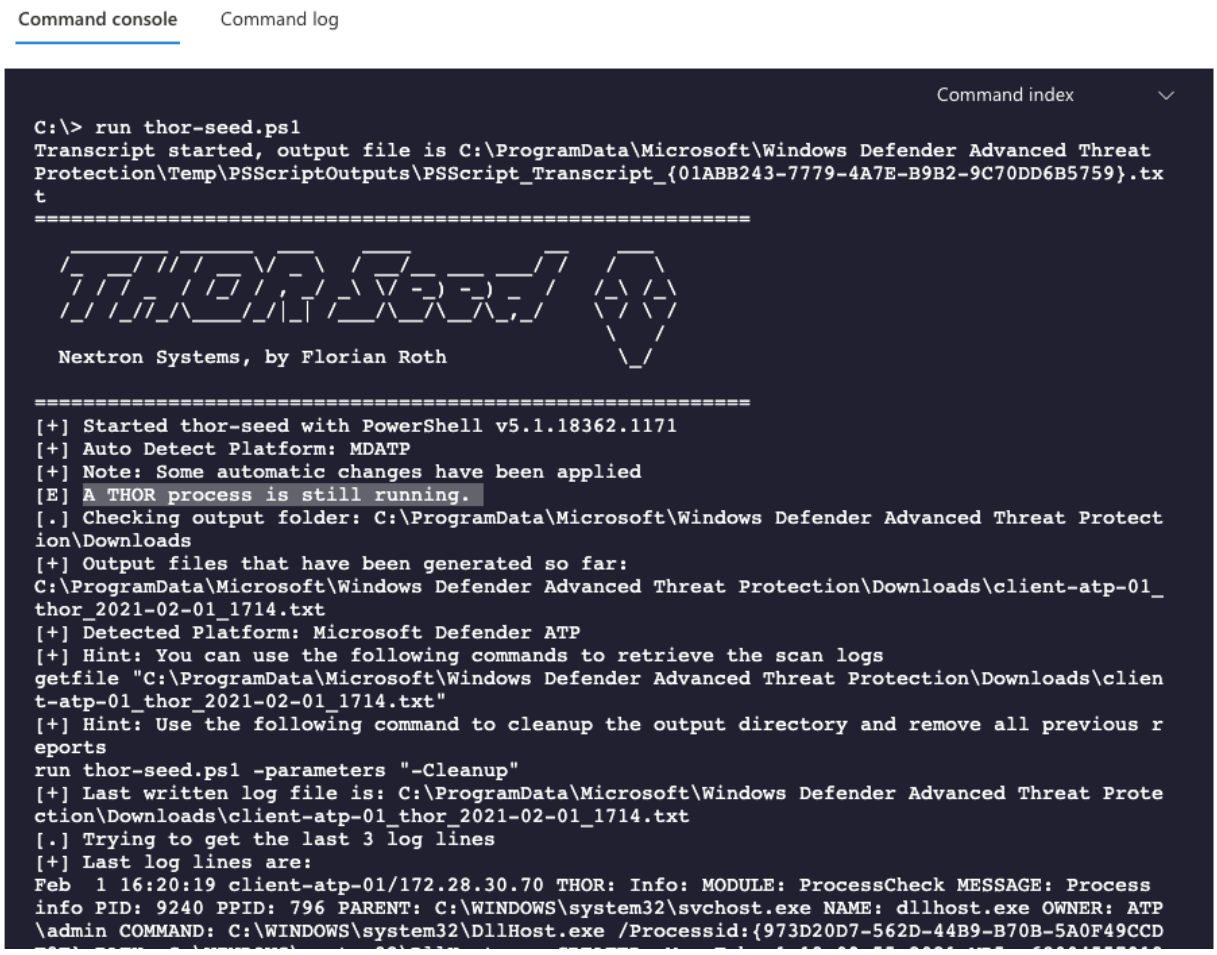


Fig. 1: THOR Seed after timeout

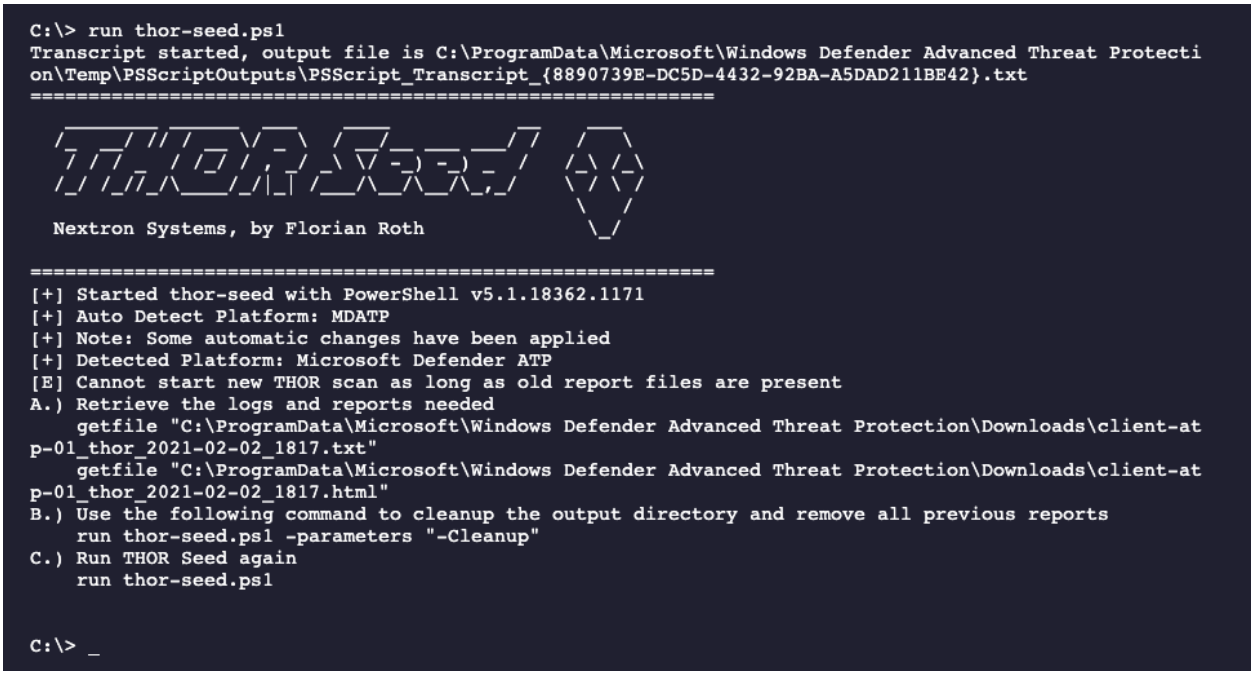


Fig. 2: THOR Seed after finished scan

### 4.1.5 THOR Seed is using multiple Licenses

In certain configurations, THOR Seed might use multiple licenses, even though you only issued a scan on one endpoint. This is due to the fact that Defender for Endpoint might be configured to execute certain files upon detection in a sandbox. The problem with this is that the sandbox is actually issuing a license from our portal, which can't be reused by the customer. To circumvent this, you have a few options:

- Define Exclusions for the `thor-seed.ps1` script (When adding exclusions, make sure you're excluding the script from both **cloud protection** and **behavioral analysis (sandbox)** .)
- Sign your version of the `thor-seed.ps1` script with a code signing certificate
- Make sure your on premise proxy does not use sandboxing, or set an exclusion

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