Scan for HAFNIUM Exploitation Evidence with THOR Lite

By Florian Roth

Published: 2026-03-30 · Archived: 2026-04-05 14:40:00 UTC

Exclude Mailbox Folders

We recommend excluding the mailboxes from the scan by adding the following lines to the file ./config/directory-excludes.cfg

```
\\(MDBDATA|Mailbox|Mailbox Database)\\
```

Scanning this directory would just slow down the scan and – according to all available reports – wouldn't be necessary to produce relevant findings.

Exchange on Drives Other than C:

If your Exchange server isn't installed on drive C:, use the "–allhds" flag.

```
thor64-lite.exe --allhds
```

Otherwise just run a standard scan without flags.

Antivirus Exclusion

Since THOR Lite doesn't provide modules for "Rootkit" detection or problematic modules like "Mutex" or "NamedPipes", you shouldn't have problems scanning systems without an Antivirus exclusion filter.

All YARA rules are included in a compressed and encrypted form so that an Antivirus shouldn't trigger on clear text signatures as it is the case for most of the other YARA scanners including LOKI.

However, since some realtime engines check every file that THOR Lite has "touched" during its scan, an Antivirus exclusion can increase the scan speed by ~30% and avoid any interference (blocked access to some files etc.).

Scanning a Subset Only

You could run a scan on a subset only and skip other system folders. If you have a good picture of the location of the Exchange folder and all relevant sub directories (log files, owa web service folders), you could run a selective scan using the following command.

```
thor64-lite.exe -a Filescan -p "C:\Program Files\Microsoft\Exchange Server"
```

However, we do not know if all relevant forensic evidence can be found in that folder.

Intense Mode

Don't use the "–intense" flag or use it only in cases in which it is okay for the scan to take 12+ hours to complete and system stability isn't a concern – which is almost never the case. The "–intense" flag is meant for lab scenarios or use cases in which a maximum detection rate is very important. Warning: That flag disables all system resource monitoring safe guards that we've integrated into THOR.

Lab Scans

Test the scan on samples that you've collected using the following commands:

```
thor64-lite.exe -a Filescan -p D:\collected-samples
```

```
thor64-lite.exe --fsonly -p D:\collected-samples
```

The first command reflects the scan mode that is used during a default scan with all modules. The second command starts THOR in "lab scanning" mode, which scans samples regardless of their extension and magic header. If you discover samples that get detected only in lab scanning mode, please let us know. (see "How Can I Help" below)
