Scan for HAFNIUM Exploitation Evidence with THOR Lite

nextron-systems.com/2021/03/06/scan-for-hafnium-exploitation-evidence-with-thor-lite

March 6, 2021

Since we’ve heard from partners and friends about many non-profit organisations affected by the Exchange server vulnerability, we’ve decided to transfer many detection rules from our commercial scanner into the free community version.

If you haven’t heard of THOR or THOR Lite before, I’d recommend reading the product page of at least THOR Lite.

TLDR: It’s a forensic scanner with the focus on traces of hacking activity, configuration backdoors, file anomalies and other things that an Antivirus often misses like web shells or the output of hack tools that has been left over by the attackers. It is portable and doesn’t require an installation.

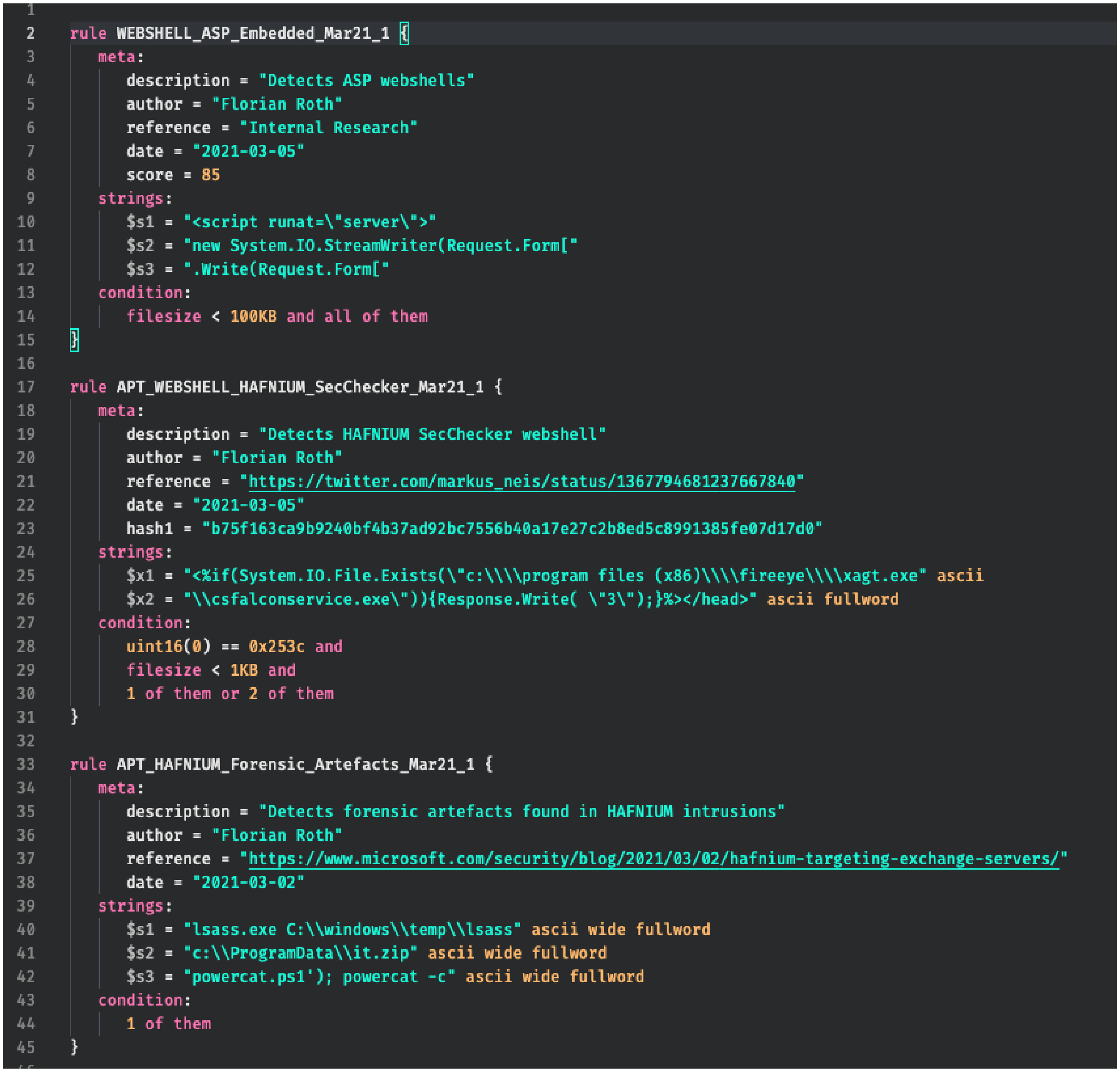
What we did to improve THOR Lite

We’ve added many of the signature that we also sell with THOR and the VALHALLA rule feed to the Open Source repository. Fellow researchers provided additional YARA signatures for some webshell types and traces in log files.

Only a few rules haven’t been published with THOR Lite in order to keep some detection logic secret. (creative ways to detect the compiled ASP.NET DLLs)

YARA rules, filename IOCs and hash IOCs provided by Microsoft and Volexity are also already included.

We estimate the coverage provided by the open source rules and IOCs to be around 95%.

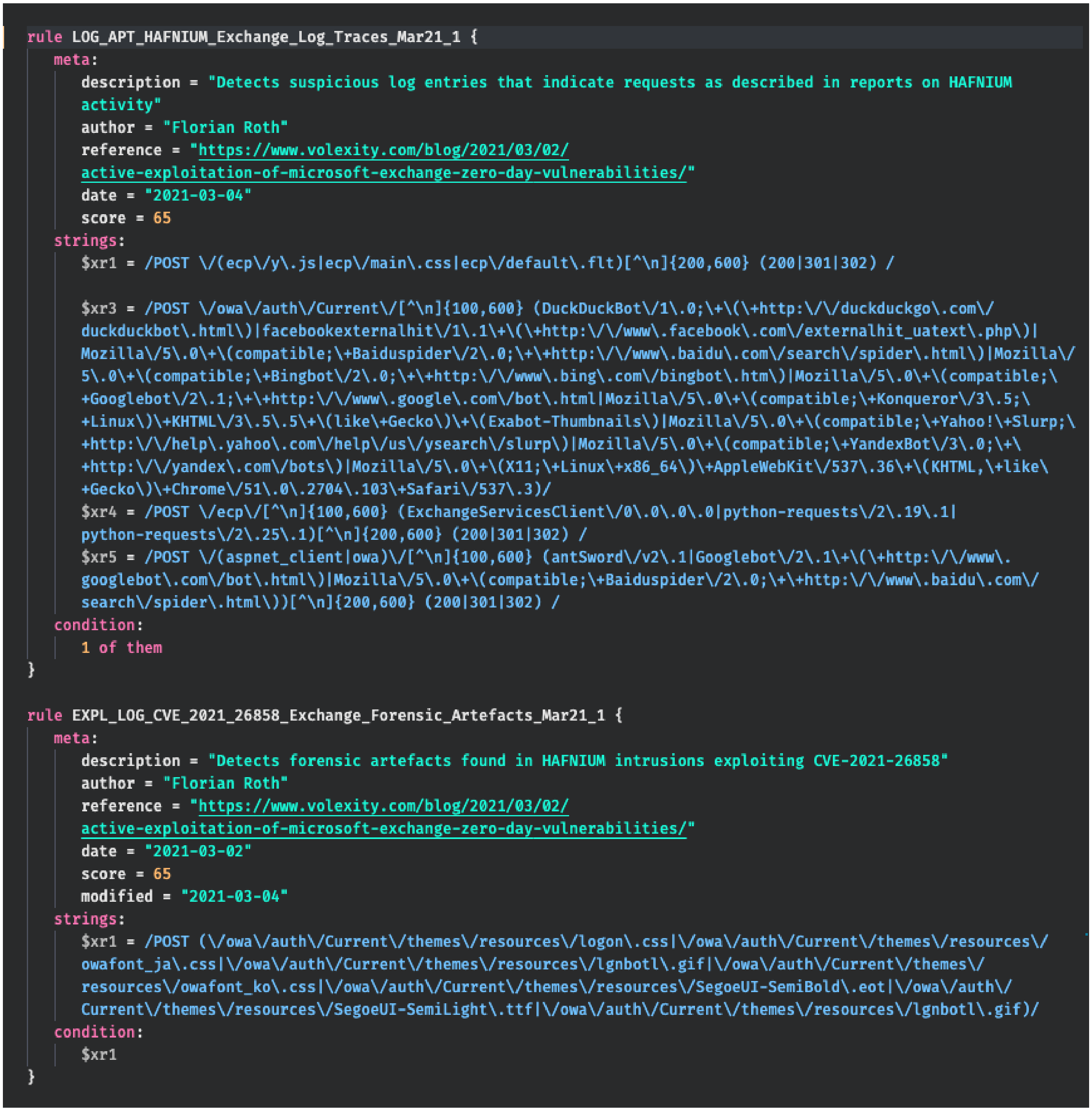


```
rule WEBSHELL_ASP_Embedded_Mar21_1 {
   meta:
      description = "Detects ASP webshells"
      author = "Florian Roth"
      reference = "Internal Research"
      date = "2021-03-05"
      score = 85
   strings:
      $s1 = "<script runat=\"server\">"
      $s2 = "new System.IO.StreamWriter(Request.Form["
      $s3 = ".Write(Request.Form["
   condition:
      filesize < 100KB and all of them
}

rule APT_WEBSHELL_HAFNIUM_SecChecker_Mar21_1 {
   meta:
      description = "Detects HAFNIUM SecChecker webshell"
      author = "Florian Roth"
      reference = "https://twitter.com/markus_neis/status/1367794681237667840"
      date = "2021-03-05"
      hash1 = "b75f163ca9b9240bf4b37ad92bc7556b40a17e27c2b8ed5c8991385fe07d17d0"
   strings:
      $x1 = "<%if(System.IO.File.Exists(\"c:\\\\program files (x86)\\\\fireeye\\\\xagt.exe" ascii
      $x2 = "\\csfalconservice.exe\")){Response.Write( \"3\");}%></head>" ascii fullword
   condition:
      uint16(0) == 0x253c and
      filesize < 1KB and
      1 of them or 2 of them
}

rule APT_HAFNIUM_Forensic_Artefacts_Mar21_1 {
   meta:
      description = "Detects forensic artefacts found in HAFNIUM intrusions"
      author = "Florian Roth"
      reference = "https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/"
      date = "2021-03-02"
   strings:
      $s1 = "lsass.exe C:\\windows\\temp\\lsass" ascii wide fullword
      $s2 = "c:\\ProgramData\\it.zip" ascii wide fullword
      $s3 = "powercat.ps1'); powercat -c" ascii wide fullword
   condition:
      1 of them
}
```

We even have translated the Sigma rules used in THOR into YARA rules in order to enable the detection of these patterns in THOR Lite (as THOR Lite doesn't allow Sigma scanning but can apply these rules in the available 'Logscan' module).



```
rule LOG_APT_HAFNIUM_Exchange_Log_Traces_Mar21_1 {
   meta:
      description = "Detects suspicious log entries that indicate requests as described in reports on HAFNIUM
      activity"
      author = "Florian Roth"
      reference = "https://www.volexity.com/blog/2021/03/02/
      active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/"
      date = "2021-03-04"
      score = 65
   strings:
      $xr1 = /POST \/(ecp\/y\.js|ecp\/main\.css|ecp\/default\.flt)[^\n]{200,600} (200|301|302) /

      $xr3 = /POST \/owa\/auth\/Current\/[^\n]{100,600} (DuckDuckBot\/1\.0;\+\(\+http:\/\/duckduckgo\.com\/
      duckduckbot\.html\)|facebookexternalhit\/1\.1\+\(\+http:\/\/www\.facebook\.com\/externalhit_uatext\.php\)|
      Mozilla\/5\.0\+\(compatible;\+Baiduspider\/2\.0;\+\+http:\/\/www\.baidu\.com\/search\/spider\.html\)|Mozilla\/
      5\.0\+\(compatible;\+Bingbot\/2\.0;\+\+http:\/\/www\.bing\.com\/bingbot\.htm\)|Mozilla\/5\.0\+\(compatible;\
      +Googlebot\/2\.1;\+\+http:\/\/www\.google\.com\/bot\.html|Mozilla\/5\.0\+\(compatible;\+Konqueror\/3\.5;\
      +Linux\)\+KHTML\/3\.5\.5\+\(like\+Gecko\)\+\(Exabot-Thumbnails\)|Mozilla\/5\.0\+\(compatible;\+Yahoo!\+Slurp;\
      +http:\/\/help\.yahoo\.com\/help\/us\/ysearch\/slurp\)|Mozilla\/5\.0\+\(compatible;\+YandexBot\/3\.0;\+\
      +http:\/\/yandex\.com\/bots\)|Mozilla\/5\.0\+\(X11;\+Linux\+x86_64\)\+AppleWebKit\/537\.36\+\(KHTML,\+like\
      +Gecko\)\+Chrome\/51\.0\.2704\.103\+Safari\/537\.3)/
      $xr4 = /POST \/ecp\/[^\n]{100,600} (ExchangeServicesClient\/0\.0\.0\.0|python-requests\/2\.19\.1|
      python-requests\/2\.25\.1)[^\n]{200,600} (200|301|302) /
      $xr5 = /POST \/(aspnet_client|owa)\/[^\n]{100,600} (antSword\/v2\.1|Googlebot\/2\.1\+\(\+http:\/\/www\.
      googlebot\.com\/bot\.html\)|Mozilla\/5\.0\+\(compatible;\+Baiduspider\/2\.0;\+\+http:\/\/www\.baidu\.com\/
      search\/spider\.html\))[^\n]{200,600} (200|301|302) /
   condition:
      1 of them
}

rule EXPL_LOG_CVE_2021_26858_Exchange_Forensic_Artefacts_Mar21_1 {
   meta:
      description = "Detects forensic artefacts found in HAFNIUM intrusions exploiting CVE-2021-26858"
      author = "Florian Roth"
      reference = "https://www.volexity.com/blog/2021/03/02/
      active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/"
      date = "2021-03-02"
      score = 65
      modified = "2021-03-04"
   strings:
      $xr1 = /POST (\/owa\/auth\/Current\/themes\/resources\/logon\.css|\/owa\/auth\/Current\/themes\/resources\/
      owafont_ja\.css|\/owa\/auth\/Current\/themes\/resources\/lgnbotl\.gif|\/owa\/auth\/Current\/themes\/
      resources\/owafont_ko\.css|\/owa\/auth\/Current\/themes\/resources\/SegoeUI-SemiBold\.eot|\/owa\/auth\/
      Current\/themes\/resources\/SegoeUI-SemiLight\.ttf|\/owa\/auth\/Current\/themes\/resources\/lgnbotl\.gif)/
   condition:
      $xr1
}
```

Included IOCs and YARA Rules

- YARA – Hafnium samples and forensic evidence – apt_hafnium.yar
- YARA – Exploitation in log files – apt_hafnium_log_sigs.yar
- Hash IOCs – hash-iocs.txt
- Filename IOCs – filename-iocs.txt

Getting Started

We offer THOR Lite for free. All we require is a newsletter subscription. (side note: we've never sent a newsletter to that list so far. This will be the first blog post that will be sent to all subscribers)

Just visit the download page, subscribe, receive a license file and download links to download the scanner package.

After the download you place the license file sent to you in a separate email into the extracted program folder and should immediately update the signatures with the following command:

```
thor-lite-util.exe update
```

If you want to use a web proxy to connect to the Internet, use the following command to get a help for the "update" command.

```
thor-lite-util.exe update --help
```

If you are already a user of THOR Lite, make sure to use at least signature set version "21.3.6-090007".

Specific Recommendations

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)

How Can I Help

- Please provide feedback on false positives. Include all information that you're allowed to share, e.g. file name, file hash, rule name or the full log line with all confidential information removed. Use the issues section on Github or send an email to rules@nextron-systems.com.

- Please help us cover false negatives. If you’ve found a webshell or forensic evidence that THOR Lite wasn’t able to detect, please provide that evidence and we add coverage for everyone in the community to use. (open source YARA rule usable in any scanner including LOKI and THOR Lite)

FAQs

Where can I find help?

Please first check the documentation, which is provided as PDF in the ./docs sub folder. It’s written for THOR, but many chapters also apply to THOR Lite.

You can report THOR Lite issues on Github.

How can I scan unsupported Windows version?

We provide a legacy version of THOR to scan outdated Windows version (2003, 2008) for our customers only. Sorry. You can find information on pricing in the license packs section.

How can I provide samples that haven’t been detected?

Please add information about them to a new issue on Github or send them to rules@nextron-systems.com.

I’ve subscribed to the Newsletter but didn’t get an email with a license file or the download links. What can I do?

The response emails sometimes get classified as SPAM. Please check your junk mail folder. In 100% of the cases in which subscribers didn’t get a corresponding email, this was the reason.