
HAFNIUM – ÜBERWACHUNG IHRER SYSTEME

Schritt-für-Schritt-Anleitung zur Überwachung Ihrer Systeme nach einer möglichen Infektion durch Hafnium
Stand: Version 1.1, 24.03.2021, 01:00

SACHVERHALT

Microsoft hat am 3. März 2021 sogenannte “Out-of-Band” Updates für Exchange Server veröffentlicht. “Out of Band” bedeutet, dass die Patche von Microsoft als wichtig angesehen werden und sofort installiert werden sollten. Mit dem Update werden vier kritische Schwachstellen geschlossen, die bereits für Angriffe verwendet werden und die Angreifer die Möglichkeit bieten, vertrauliche Daten abzugreifen oder Schadsoftware zu installieren.

HINWEIS: Im Folgenden werden die aktuell verfügbaren Informationen genutzt um eine mögliche Vorgehensweise zum Überwachen der Systeme zu definieren. Das Dokument wird laufend aktualisiert. Bitte achten Sie daher auch auf weitere Veröffentlichungen unter

<https://research.hisolutions.com/hafnium>

ÜBERWACHEN DER SYSTEME MITTELS THOR LITE / LOKI

Da die Schwachstellen bereits durch mehrere unterschiedliche Gruppen ausgenutzt werden, reicht es aktuell nicht aus, nur nach einer bestimmten Malware oder Webshell zu suchen. Aus diesem Grund hat das BSI eine Übersicht veröffentlicht¹ welche weiteren Analysen auf den Systemen durchgeführt werden sollten. Zur Vereinfachung der Anwendung haben wir uns entschlossen Ihnen eine Hilfestellung bei der Nutzung des Thor-Lite Scanner² zu geben, welches ebenfalls in der Hilfe des BSI erwähnt wurde.

Thor Lite ist eine kostenfreie Version des kommerziellen Thor Scanners. Es existiert auch eine Open-Source-Variante, der Loki Scanner³, der keine Registrierung erfordert. Die Nutzung von Thor Lite ist für Sie kostenfrei sofern Sie sich zum Newsletter des Anbieters anmelden. Sofern Sie dies nicht wünschen können Sie alle folgenden Schritte auf mit dem Loki Scanner durchführen. Dieser nutzt die gleichen Suchmechanismen ist jedoch langsamer. Er kann jedoch genau wie der Thor Lite Scanner genutzt werden.

¹ <https://bsi.bund.de/exchange-schwachstellen>

² <https://www.nextron-systems.com/thor-lite/>

³ <https://github.com/Neo23x0/Loki>



TLP:WHITE



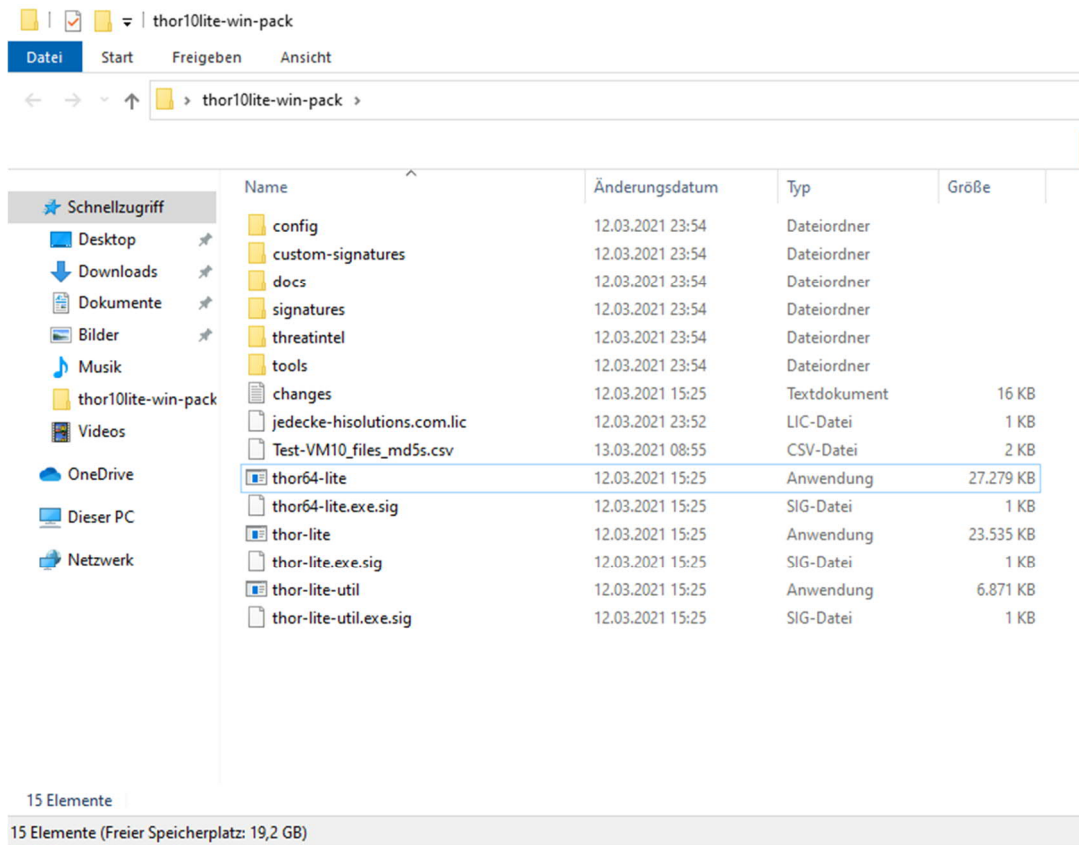
HiSolutions AG
Schloßstraße 1
12163 Berlin

info@hisolutions.com
www.hisolutions.com

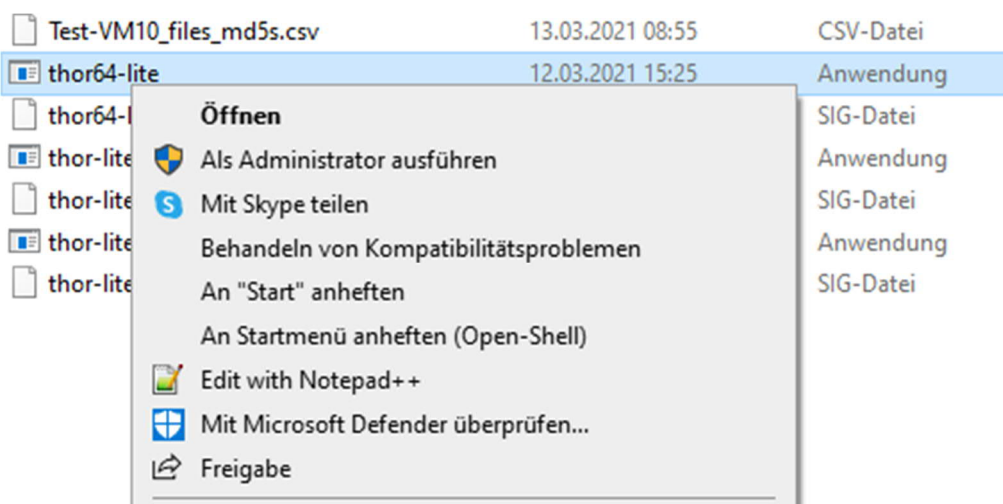
+49 30 533 289-0
+49 30 533 289-900

Nach erfolgreicher Anmeldung erhalten Sie einen Link zum Laden des Programms für Microsoft Windows (andere Betriebssysteme wie Linux und Mac werden auch angeboten, sind aber im aktuellen Fall nicht relevant).

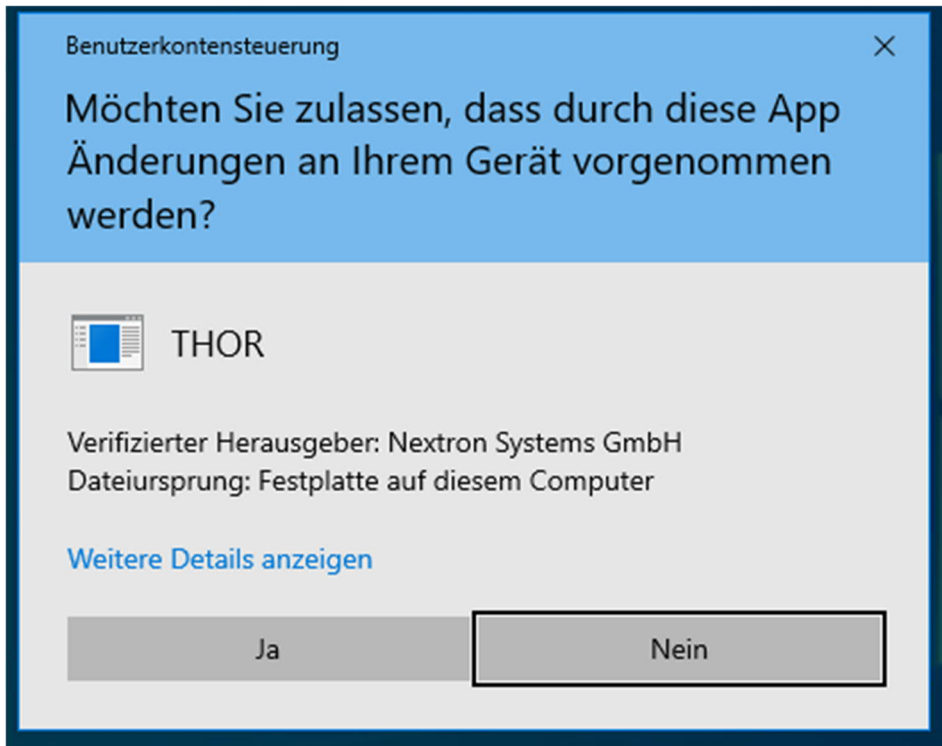
Laden Sie sich das Programm am besten auf einen USB Stick, entpacken dieses dort und kopieren die Lizenzdatei (Diese haben Sie per E-Mail erhalten und sie hat die Endung .lic) ebenfalls in das entpackte Verzeichnis:



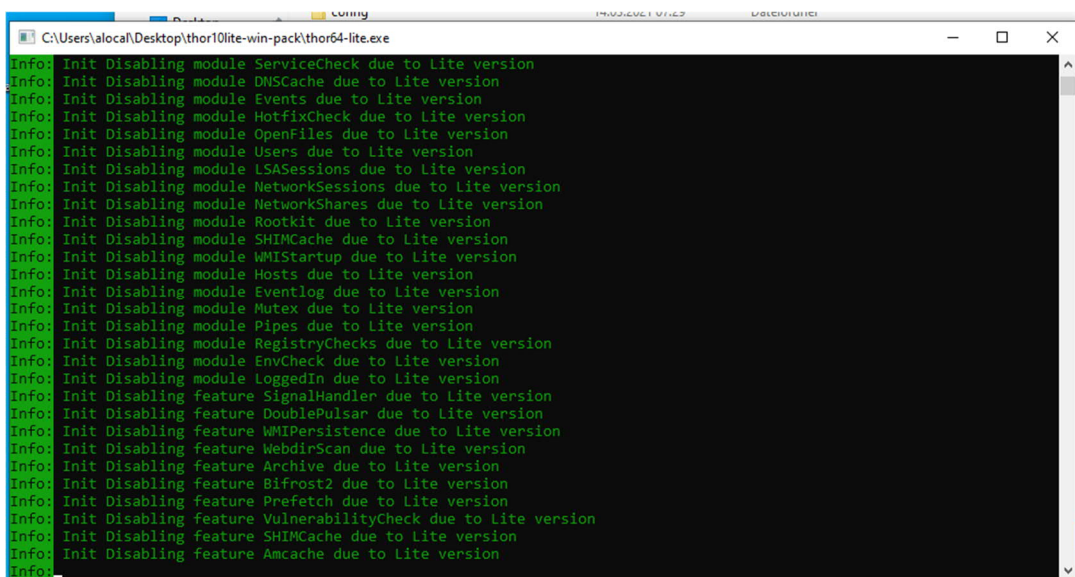
Klicken Sie mit der rechten Maustaste auf die Datei „thor64-lite“ und führen Sie die Datei als Administrator aus:



Sie werden aufgefordert, die Nutzung des Programms zuzulassen. Dies müssen Sie für einen vollständigen Scan bejahen.



Sobald das Programm das erste Mal ausgeführt wird, lädt es automatisch die aktuellen Signaturen zum Überprüfen Ihrer Systeme herunter. Bitte beachten Sie, dass Ihr System hierzu Zugriff auf das Internet benötigt. Sollte dies nicht der Fall sein, so starten Sie den Scanner zuerst auf einem PC/Laptop mit Internet Zugriff um die aktuelle Signaturen zu laden. Der Scanner prüft nun selbstständig ihr System



```
C:\Users\alocal\Desktop\thor10lite-win-pack\thor64-lite.exe
0000ffff000b000000
[Info] ProcessCheck Process info PID: 8696 PPID: 712 PARENT: NAME: svchost.exe OWNER: NT-AUTORITÄT\SYSTEM COMMAND: C:\WI
NDOWS\system32\svchost.exe -k netsvcs -p -s Appinfo PATH: C:\WINDOWS\system32\svchost.exe
CREATED: Sat Mar 13 03:16:19 2021
MD5: F586835082f632dc8d9404d83bc16316 CONNECTION_COUNT: 0 LISTEN_PORTS: FILE_1: C:\WINDOWS\system32\svchost.exe EXISTS_
1: yes CREATED_1: Wed Mar 3 09:25:16 2021 MD5_1: F586835082f632dc8d9404d83bc16316 SHA1_1: 010db07461e45b41c886192df6fd4
25ba8d42d82 SHA256_1: 643ec58e82e0272c97c2a59f6020970d881af19c0ad5029db9c958c13b6558c7 FIRSTBYTES_1: 4d5a90000300000040
0000ffff000b000000
[Info] ProcessCheck Process info PID: 1280 PPID: 712 PARENT: NAME: svchost.exe OWNER: NT-AUTORITÄT\Lokaler Dienst COMMAN
D: C:\WINDOWS\system32\svchost.exe -k LocalService -p -s LicenseManager PATH: C:\WINDOWS\system32\svchost.exe
CREATED: Sat Mar 13 03:30:13 2021
MD5: F586835082f632dc8d9404d83bc16316 CONNECTION_COUNT: 0 LISTEN_PORTS: FILE_1: C:\WINDOWS\system32\svchost.exe EXISTS_
1: yes CREATED_1: Wed Mar 3 09:25:16 2021 MD5_1: F586835082f632dc8d9404d83bc16316 SHA1_1: 010db07461e45b41c886192df6fd4
25ba8d42d82 SHA256_1: 643ec58e82e0272c97c2a59f6020970d881af19c0ad5029db9c958c13b6558c7 FIRSTBYTES_1: 4d5a90000300000040
0000ffff000b000000
[Info] ProcessCheck Process info PID: 3228 PPID: 712 PARENT: NAME: svchost.exe OWNER: NT-AUTORITÄT\Lokaler Dienst COMMAN
D: C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s lmhosts PATH: C:\WINDOWS\system32\svchost.exe
CREATED: Sat Mar 13 07:23:28 2021
MD5: F586835082f632dc8d9404d83bc16316 CONNECTION_COUNT: 0 LISTEN_PORTS: FILE_1: C:\WINDOWS\system32\svchost.exe EXISTS_
1: yes CREATED_1: Wed Mar 3 09:25:16 2021 MD5_1: F586835082f632dc8d9404d83bc16316 SHA1_1: 010db07461e45b41c886192df6fd4
25ba8d42d82 SHA256_1: 643ec58e82e0272c97c2a59f6020970d881af19c0ad5029db9c958c13b6558c7 FIRSTBYTES_1: 4d5a90000300000040
0000ffff000b000000
[Info] ProcessCheck Process info PID: 2136 PPID: 712 PARENT: NAME: svchost.exe OWNER: NT-AUTORITÄT\SYSTEM COMMAND: C:\WI
NDOWS\system32\svchost.exe -k WbioSvcGroup -s WbioSrvc PATH: C:\WINDOWS\system32\svchost.exe
CREATED: Sat Mar 13 07:23:34 2021
MD5: F586835082f632dc8d9404d83bc16316 CONNECTION_COUNT: 0 LISTEN_PORTS: FILE_1: C:\WINDOWS\system32\svchost.exe EXISTS_
1: yes CREATED_1: Wed Mar 3 09:25:16 2021 MD5_1: F586835082f632dc8d9404d83bc16316 SHA1_1: 010db07461e45b41c886192df6fd4
25ba8d42d82 SHA256_1: 643ec58e82e0272c97c2a59f6020970d881af19c0ad5029db9c958c13b6558c7 FIRSTBYTES_1: 4d5a90000300000040
0000ffff000b000000
```

Während des Scans werden mögliche Malware Funde bereits angezeigt:

```
D:\373 > Running module 'filesystem Checks'
[Info] Filescan Scanning module
[Info] Filescan The following paths will be scanned: C:\
[Info] Filescan Scanning C:\ RECURSIVE
[Warning] Filescan Malware file found
FILE: C:\$Recycle.Bin\S-1-5-21-2171491307-3139758677-864701467-1002\SRH3ZPL.txt EXT: .txt SCORE: 385
SIZE: 552374
CREATED: Sat Mar 13 00:22:37.061 2021 MODIFIED: Sat Mar 13 00:23:58.534 2021 ACCESSED: Sun Mar 14 07:36:29.823 2021 PERMISSIONS: OWNER: UNKNOWN
MD5: a0c7d6d8044a0f0b0ef3b01cf2580
SHA1: f590e4a19bc88eb5c9fd4e3245eadaefb1115
SHA256: 50bb0d6e7e088a18a32eb40ba7c7dacf5ae73c9954b4a5df822d9310143673 TYPE: UNKNOWN FIRSTBYTES: 4d612203132203233a32323a3372054657374 / Mar 12 23:22:37 Test
REASON_1: VARA rule AP71B_Hatchup_Sample_Gen / AP7 10 / Cloud Hopper malware campaign SUBSCORE_1: 80 REF_1: https://www.pwc.co.uk/issues/cyber-security-data-privacy/insights/op
eration-cloud-hopper.html MATCHED_1: STR1: "000252080599081.r3ub.com" STR2: "0011608033400e1.r3ub.com" STR3: "0622.hay8000.com" STR4: "1.gadsky.com" STR5: "100fame.com" S
TR6: "11.usyahoop15.com" STR7: "1051847326.r3ub.com" STR8: "106044570931199.r3ub.com" STR9: "1j.www1.biz" STR10: "1z.itsaol.com" STR11: "2012yearleft.com" STR12: "2014.zxw.
com" STR13: "202017845.r3ub.com" STR14: "2139465544784.r3ub.com" STR15: "2780203959840958.r3ub.com" STR16: "5590420449750020.r3ub.com" STR17: "5q.nushenghuo.info" STR18: "6n.4
nidian2010.info" STR19: "6gwg.tech" STR20: "a.wubantu.info" STR21: "ai.suibian2010.info" STR22: "abc.wikaba.com" STR23: "abcd120719.6680.org" STR24: "abcd120887.3322.org" STR
25: "acc.emailfound.info" STR26: "acc.lehigtapp.com" STR27: "acc.party.com" STR28: "ad.webbooting.com" STR29: "additional.asxdata.com" STR30: "af.rjms.com" STR31: "af.hfz3p4
43.org" STR32: "ako.ddns.us" STR33: "androidmusicapp.omnycp.us" STR34: "announcements.toythieves.com" STR35: "anypnn.com" STR36: "aotuo.9966.org" STR37: "apex.qtssoft.com" STR
38: "app.lehigtapp.com" STR39: "apple.cdnnetview.com" STR40: "apple.defensewar.org" STR41: "apple.ikub.com" STR42: "appledownload.ourhobby.com" STR43: "appleimages.itemdb.com" S
TR44: "appleimages.longmusic.com" STR45: "applell120102.9966.org" STR46: "applemirror-organicrap.com" STR47: "applemirror-squirly.info" STR48: "applemusic.lease.net.com" STR4
9: "applemusic.itemdb.com" STR50: "applemusic.wikaba.com" STR51: "applemusic.xxuz.com" STR52: "applemusic.zxuz.com" STR53: "appleupdate.itemdb.com" STR
54: "appleupdate.itemdb.com" STR55: "architectuissusa.com" STR56: "area.uhelhelpdesk.com" STR57: "army.xxuz.com" STR58: "art.pdp.net" STR59: "asfzx.x24hr.com" STR60: "availab.wikaba.com" STR61: "availability.ju
stified.com" STR62: "bamy03.com" STR63: "baby.macforlinux.net" STR64: "baby.wyie12.com" STR65: "baby.usmircorney.net" STR66: "back.jungleheart.com" STR67: "back.mofa.dynamic.d
ns.net" STR68: "bak.faxv8000.com" STR69: "bak.ignoreslist.com" STR70: "bak.un.dnsrd.com" STR71: "balance1.wikaba.com" STR72: "bak.nrga.com" STR73: "c[...] TAGS_1: CHINA, 60045,
60046, 60047, 60048 RULEDATE: 1: 2017-04-09 SIGTYPE: 1: internal
```

Bitte beachten Sie: Aufgrund der verwendeten Technologie kann es sein, dass die angezeigten Alarme sogenannte False-Positives sind. In der Medizin wäre dies der Fall, wenn „Der Patient ist gesund, aber der Test hat ihn fälschlicherweise als krank eingestuft.“⁴ Sofern Sie unter Betreuung durch die HiSolutions AG sind, werden unsere Fallbetreuer mögliche Funde mit Ihnen besprechen. Andernfalls besprechen Sie Ihre Ergebnisse bitte mit einem qualifizierten IT-Dienstleister.

Hierzu erhalten Sie am Ende des Scans einen Bericht als HTML Datei (beispielsweise Test-VM10_thor_2021-03-13_0026.html) oder im Falle einer Prüfung mit Loki eine Text Datei (beispielsweise Test-VM10_thor_2021-03-13_0026.txt).

Wichtiger Hinweis: Bitte führen Sie die Überprüfung mindestens auf den folgenden Systemen aus:

- Exchange Server
- Active Directory Server
- Auf aus dem Backup eingespielten Systemen

⁴ https://de.wikipedia.org/wiki/Beurteilung_eines_bin%C3%A4ren_Klassifikators



ÜBERWACHEN DER SYSTEME MITTELS CHECKLISTEN

Wie bereits das BSI in Ihrer Videobotschaft⁵ dargelegt hat, gibt es nicht „das“ System zur Überwachung des Active Directories. Auch uns ist bewusst, dass es hierfür keine vollständige Lösung geben kann.

Um Ihnen jedoch trotzdem zu helfen, wollen wir Ihnen im Folgenden einige Tipps und Tricks geben, mit denen Sie selber zu einem gewissen Maß feststellen können, ob eine tiefgreifende Infiltration stattgefunden hat.

Sie sollten auf jeden Fall ihr Active Directory näher überprüfen. Eine mögliche Vorgehensweise hat Microsoft zur Verfügung gestellt.⁶

Zudem sollten Sie sicherstellen, dass Ihre Logfiles mindestens bis Anfang März (lieber länger zurück) vorhanden sind und sicher abgelegt sind. Windows überschreibt regelmäßig die Logfiles, so dass diese im schlimmsten Fall nur wenige Stunden zurückreichen. Passen Sie daher bitte die „Log Retention Policy“ und die „Maximum Log Size“ an, um mehr Daten zu speichern. Sofern die Daten bereits überschrieben worden sind, finden sich oft noch ältere Daten in Backups.

Es ist aktuell zusätzlich ratsam, die Logdaten täglich auf ein externen Medium wie eine USB-Festplatte oder einen USB-Stick zu sichern.

Dauer der Überwachung

Wir empfehlen die Beobachtung der Systeme gemäß diesen Empfehlungen für einen Zeitraum von 12 Monaten. In der Vergangenheit haben wir häufig 'Ruhezeiten' (nach initialer Kompromittierung bis zum eigentlichen Angriff) von 2-4 Monaten, in einigen Fällen aber auch bis zu 9 Monaten gesehen.

Prüfen Sie in der nächsten Zeit regelmäßig die folgenden Seiten auf neue Hinweise:

- <https://research.hisolutions.com/hafnium>
- <https://bsi.bund.de/exchange-schwachstellen>

Dieses Werk ist lizenziert unter einer [Creative Commons Namensnennung - Weitergabe unter gleichen Bedingungen 4.0 International Lizenz](#).

⁵ <https://www.youtube.com/watch?v=QcqRRc-VoB0>

⁶ <https://docs.microsoft.com/de-de/windows-server/identity/ad-ds/plan/security-best-practices/monitoring-active-directory-for-signs-of-compromise>

