
HAFNIUM – ÜBERWACHUNG IHRER SYSTEME

Schritt-für-Schritt-Anleitung zur Überwachung Ihrer Systeme nach einer möglichen Infektion durch Hafnium
Stand: Version 1.2, 02.08.2022

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 bei Bedarf weiter aktualisiert. Bitte achten Sie daher auch auf weitere Veröffentlichungen unter

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

ÜBERWACHEN DER SYSTEME MITTELS 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 Loki Scanner zu geben, welches ebenfalls in der Hilfe des BSI erwähnt wurde.

Der Loki Scanner ist eine Open-Source-Variante des kommerziellen Thor Scanners, erfordert keine Registrierung und ist auch für die kommerzielle Nutzung kostenlos herunterzuladen².

Laden Sie sich das Programm am besten auf einen USB Stick und entpacken Sie es dort:

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

² <https://github.com/Neo23x0/Loki>



TLP:WHITE

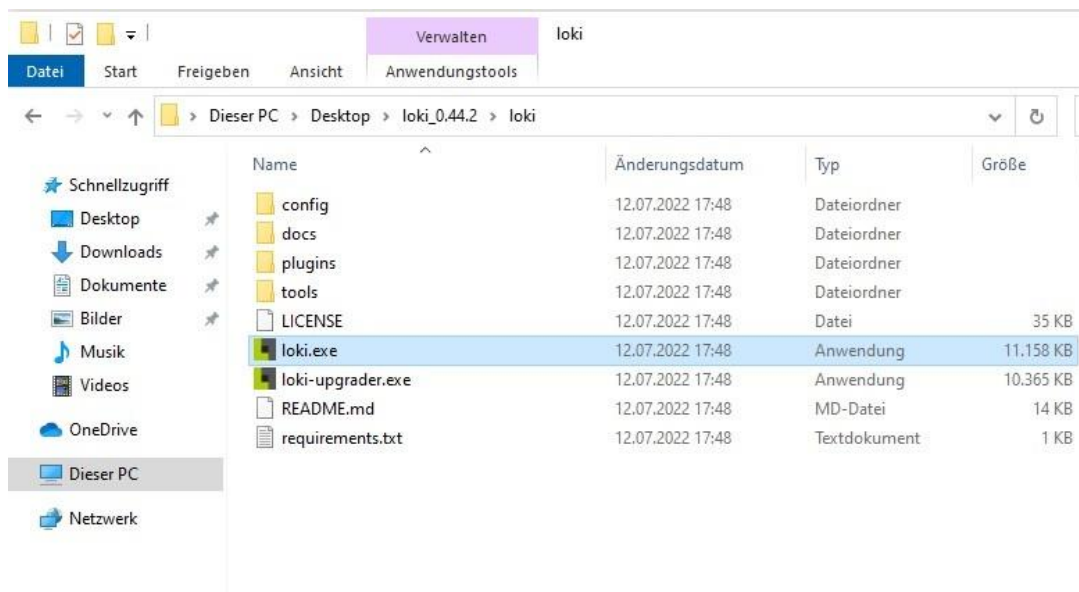


HiSolutions AG

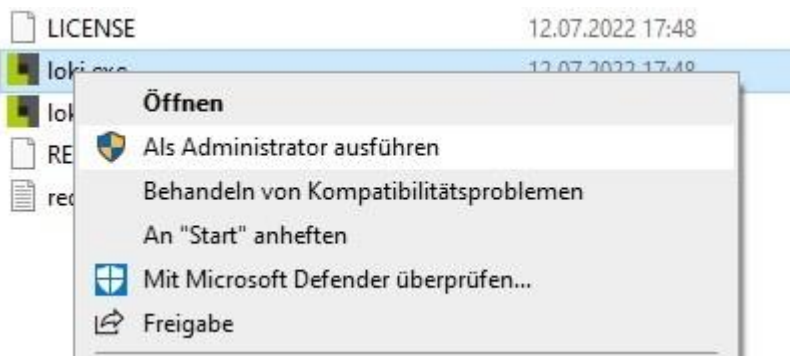
Schloßstraße 1
12163 Berlin

info@hisolutions.com
www.hisolutions.com

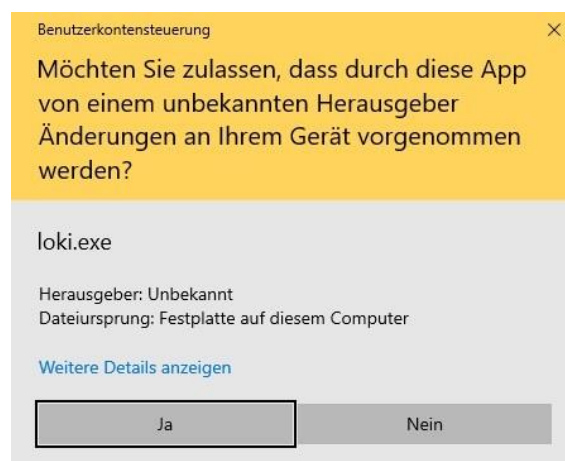
+49 30 533 289-0
+49 30 533 289-900



Klicken Sie mit der rechten Maustaste auf die Datei „loki.exe“ und führen Sie die Datei als Administrator aus:



Sie werden (je nach Konfiguration des untersuchten Systems ggf. mehrfach) 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.

C:\Users\alocal\Desktop\loki_0.44.2\loki\loki.exe

```
[INFO] New signature file: crime_loki_bot.yar
[INFO] New signature file: crime_mal_grandcrab.yar
[INFO] New signature file: crime_mal_nitol.yar
[INFO] New signature file: crime_mal_ransom_wadharma.yar
[INFO] New signature file: crime_malumpos.yar
[INFO] New signature file: crime_malware_generic.yar
[INFO] New signature file: crime_malware_set_oct16.yar
[INFO] New signature file: crime_maze_ransomware.yar
[INFO] New signature file: crime_mikey_trojan.yar
[INFO] New signature file: crime_mirai.yar
[INFO] New signature file: crime_mywscript_dropper.yar
[INFO] New signature file: crime_nanshou.yar
[INFO] New signature file: crime_nkminer.yar
[INFO] New signature file: crime_nopetya_jun17.yar
[INFO] New signature file: crime_ole_loadswf_cve_2018_4878.yar
[INFO] New signature file: crime_parallax_rat.yar
[INFO] New signature file: crime_phish_gina_dec15.yar
[INFO] New signature file: crime_ransom_conti.yar
```

Der Scanner prüft nun selbstständig ihr System:

```
C:\Users\alocal\Desktop\loki_0.44.2\loki\loki.exe
Schedule PATH: C:\WINDOWS\system32\svchost.exe
[INFO] PE-Sieve reported no anomalies PID: 1252 NAME: svchost.exe OWNER: SYSTEM CMD: C:\WINDOWS\system32\svchost.exe -k netsvcs -p -s Schedule PATH: C:\WINDOWS\system32\svchost.exe
[NOTICE] Listening process PID: 1252 NAME: svchost.exe COMMAND: C:\WINDOWS\system32\svchost.exe -k netsvcs -p -s Schedule IP: :: PORT: 49667
[NOTICE] Listening process PID: 1252 NAME: svchost.exe COMMAND: C:\WINDOWS\system32\svchost.exe -k netsvcs -p -s Schedule IP: 0.0.0.0 PORT: 49667
[INFO] Scanning Process PID: 1284 NAME: svchost.exe OWNER: Netzwerkdienst CMD: C:\WINDOWS\System32\svchost.exe -k NetworkService -p -s NlaSvc PATH: C:\WINDOWS\System32\svchost.exe
[INFO] PE-Sieve reported no anomalies PID: 1284 NAME: svchost.exe OWNER: Netzwerkdienst CMD: C:\WINDOWS\System32\svchost.exe -k NetworkService -p -s NlaSvc PATH: C:\WINDOWS\System32\svchost.exe
[INFO] Scanning Process PID: 1352 NAME: svchost.exe OWNER: SYSTEM CMD: C:\WINDOWS\system32\svchost.exe -k netsvcs -p -s ProfSvc PATH: C:\WINDOWS\system32\svchost.exe
[INFO] PE-Sieve reported no anomalies PID: 1352 NAME: svchost.exe OWNER: SYSTEM CMD: C:\WINDOWS\system32\svchost.exe -k netsvcs -p -s ProfSvc PATH: C:\WINDOWS\system32\svchost.exe
[INFO] Scanning Process PID: 1360 NAME: svchost.exe OWNER: Lokaler Dienst CMD: C:\WINDOWS\system32\svchost.exe -k LocalService -p -s EventSystem PATH: C:\WINDOWS\system32\svchost.exe
[INFO] PE-Sieve reported no anomalies PID: 1360 NAME: svchost.exe OWNER: Lokaler Dienst CMD: C:\WINDOWS\system32\svchost.exe -k LocalService -p -s EventSystem PATH: C:\WINDOWS\system32\svchost.exe
[INFO] Scanning Process PID: 1372 NAME: svchost.exe OWNER: SYSTEM CMD: C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s SysMain PATH: C:\WINDOWS\system32\svchost.exe
[INFO] PE-Sieve reported no anomalies PID: 1372 NAME: svchost.exe OWNER: SYSTEM CMD: C:\WINDOWS\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s SysMain PATH: C:\WINDOWS\system32\svchost.exe
[INFO] Scanning Process PID: 1392 NAME: svchost.exe OWNER: SYSTEM CMD: C:\WINDOWS\System32\svchost.exe -k netsvcs -p -s Themes PATH: C:\WINDOWS\System32\svchost.exe
[INFO] PE-Sieve reported no anomalies PID: 1392 NAME: svchost.exe OWNER: SYSTEM CMD: C:\WINDOWS\System32\svchost.exe -k netsvcs -p -s Themes PATH: C:\WINDOWS\System32\svchost.exe
[INFO] Scanning Process PID: 1520 NAME: svchost.exe OWNER: Lokaler Dienst CMD: C:\WINDOWS\System32\svchost.exe -k LocalService -p -s netprofm PATH: C:\WINDOWS\System32\svchost.exe
```

Während des Scans werden mögliche Malware Funde bereits angezeigt:

```
> 3/3 > Running module "filesystem Checks"
[INFO] Filescan Starting 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-1-5-21-2171401307-3139758677-864781467-18021\SR1H3ZPL.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 07:36:29.023 2021 PERMISSIONS: OWNER: UNKNOWN
MD5: 409174e030444091091f1b11f2580
SHA1: 1590de44a19c8b8e5cacf4462450ad9fb1115
SHA256: 9b0d06e7e0e88a18a32eb40ba7c7dacf5e73c9954b4a5df822d9310143673 TYPE: UNKNOWN FIRSTBYTES: 4d6172203132283233a32323a3372054657374 / Mar 12 23:22:37 Test
REASON: 1: YARA rule APITB_Malware_Sample_Gen / API 10 / Cloud Hopper malware campaign SUBSCORE: 1 80 REF_1: https://www.pwc.co.uk/issues/cyber-security/data-privacy/insights/op
ration-cloud-hopper.html MATCHED: 14 Str1: "8025208059981.r3u8.com" Str2: "00116089334444.r3u8.com" Str3: "0025208059981.r3u8.com" Str4: "1-gbidskyun.com" Str5: "100famen.com" S
tr6: "11-usyahoop15.com" Str7: "10518475326.r3u8.com" Str8: "1960445709311109.r3u8.com" Str9: "1j.www1.biz" Str10: "1r.itsaol.com" Str11: "2812yearleft.com" Str12: "2014.szuk
.com" Str13: "202017845.r3u8.com" Str14: "2139465544784.r3u8.com" Str15: "278920395848958.r3u8.com" Str16: "5590428449750026.r3u8.com" Str17: "5q.niushenghuo.info" Str18: "6n.s
hibian2010.info" Str19: "9gong.tech" Str20: "a.wubangtu.info" Str21: "a1.suibian2010.info" Str22: "abc.wikaba.com" Str23: "abcd120719.6680.org" Str24: "abcd120807.3322.org" Str
25: "accsmallfound.info" Str26: "acc.lehigtapp.com" Str27: "acc.lehigtapp.com" Str28: "acc.lehigtapp.com" Str29: "additional.exp1ude.com" Str30: "af-fjms.com" Str31: "afe.http4
3.org" Str32: "ako.ddns.us" Str33: "androidmiscapp.ommypc.us" Str34: "announcements.toythieves.com" Str35: "anypn.com" Str36: "aotuo.9006.org" Str37: "apcc.qtssofta.com" Str3
8: "app.lehigtapp.com" Str39: "apple.cmdnetvow.com" Str40: "apple.defensewar.org" Str41: "apple.ikub.com" Str42: "appledownload.ourhobby.com" Str43: "appleimages.itemdb.com" S
tr44: "appleimages.longmusic.com" Str45: "applellid120102.9966.org" Str46: "appleliron.organicrap.com" Str47: "appleliron.squirrel.info" Str48: "applemusic.isasecret.com" Str4
9: "applemusic.itemdb.com" Str50: "applemusic.wikaba.com" Str51: "applemusic.xuxu.com" Str52: "applemusic.zxux.com" Str53: "apples.aytes.net" Str54: "appleupdate.itemdb.com" Str
55: "anchiackissusa.com" Str56: "area.uwtheipdsk.com" Str57: "army.xxuz.com" Str58: "ant.ppp.net" Str59: "asfzx.x24h.com" Str60: "availab.wikaba.com" Str61: "availabilitty.ju
stled.com" Str62: "ba.my83.com" Str63: "baby.macronlinux.net" Str64: "baby.myle12.com" Str65: "baby.usmircomey.net" Str66: "back.jungleheart.com" Str67: "back.mofa.dynamic.d
ns.net" Str68: "bak.hayeb880.com" Str69: "bak.lignonist.com" Str70: "bak.un.dnsrd.com" Str71: "balance1.wikaba.com" Str72: "bak.n7go.com" Str73: "c[...] TAGS_1: CHINA, G0045,
G01, MAL, T1526 RULEDATE: 1 2017-04-06 SIGTYPE: 1: iremrel
```



TLP:WHITE

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/die Patientin ist gesund, aber der Test hat ihn bzw. sie fälschlicherweise als krank eingestuft.“³. Sofern Sie unter Betreuung durch die HiSolutions AG sind, werden unsere Fallbetreuerinnen und 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 TXT-Datei (beispielsweise loki_TEST-VM10_2022-07-13_16-52-01.txt).

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

- Exchange Server
- Active Directory Server
- Aus dem Backup eingespielte Systeme

³ https://de.wikipedia.org/wiki/Beurteilung_eines_bin%C3%A4ren_Klassifikators



ÜBERWACHEN DER SYSTEME MITTELS CHECKLISTEN

Wie bereits das BSI in Ihrer Videobotschaft⁴ 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.⁵

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](#).

⁴ <https://www.youtube.com/watch?v=QcqRRc-VoB0>

⁵ <https://docs.microsoft.com/de-de/windows-server/identity/ad-ds/plan/security-best-practices/monitoring-active-directory-for-signs-of-compromise>

