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 Angreifern 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 veröffentlicht[1] 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 herunterzuladen[2].

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

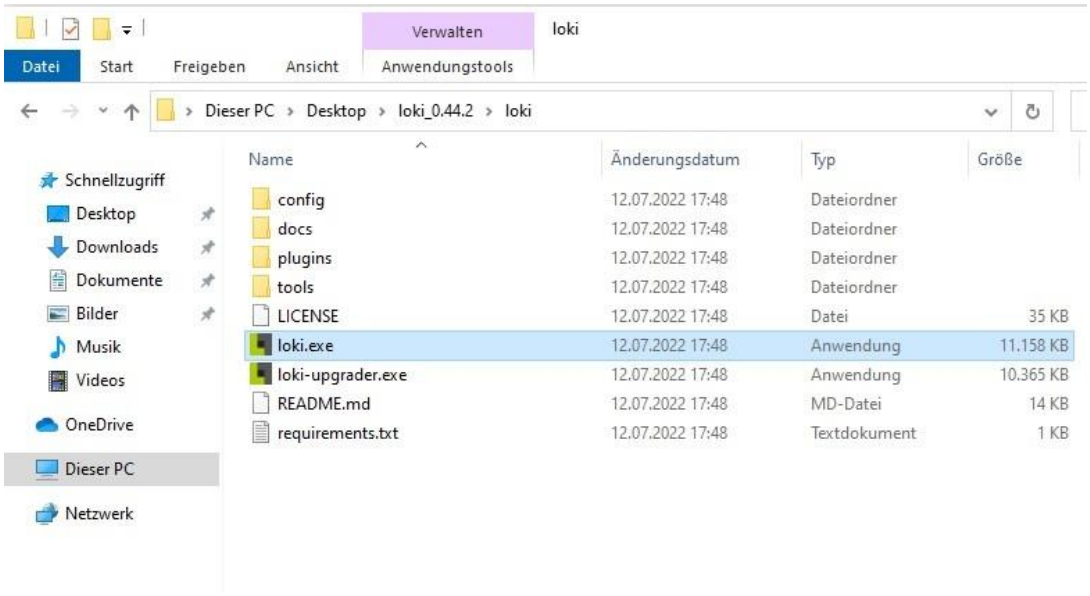
[1] https://bsi.bund.de/exchange-schwachstellen
[2] https://github.com/Neo23x0/Loki

TLP:WHITE

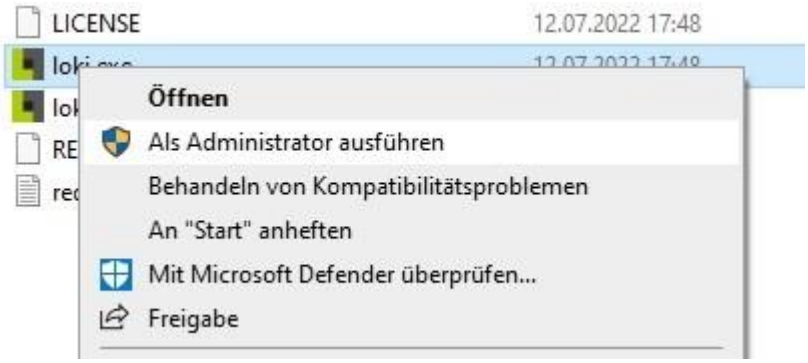
HiSolutions AG
Schloßstraße 1
12163 Berlin

info@hisolutions.com
www.hisolutions.com

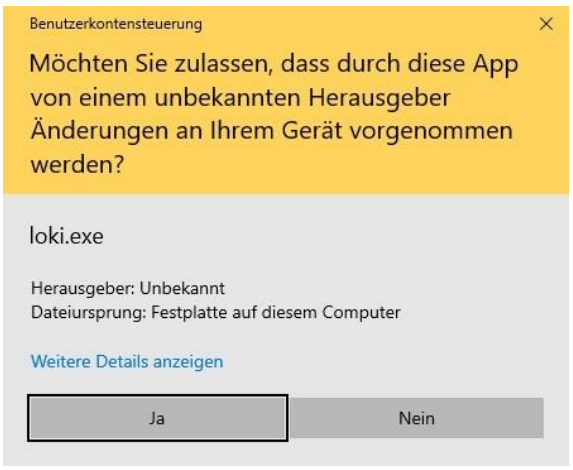
+49 30 533 289-0
+49 30 533 289-900



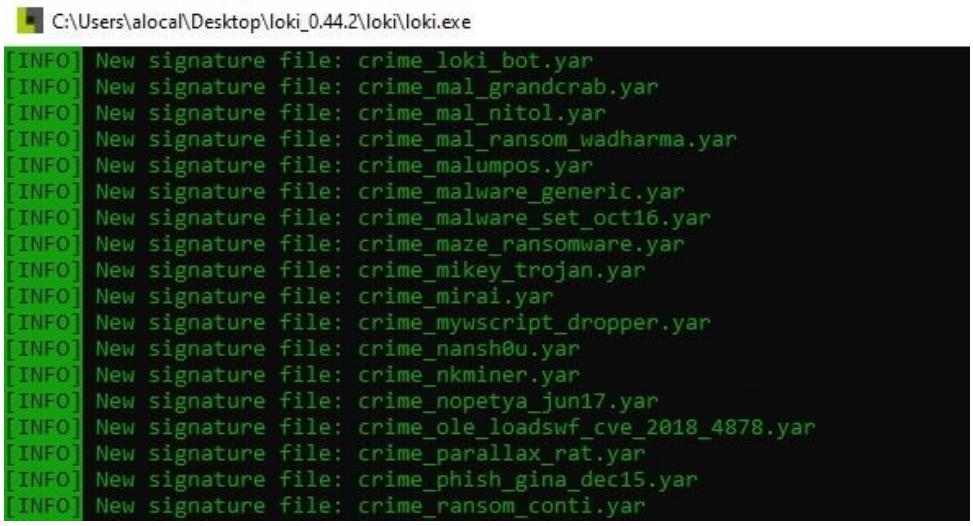
Klicken Sie mit der rechten Maustaste auf die Datei „loki.exe“ und führen Sie die Datei als Administrator aus:



Sie werden (je nach Konfiguration des untersuchten Systems ggf. mehrfach) aufgefordert, die Nutzung des Programms zuzulassen. Dies müssen Sie für einen vollständigen Scan bejahen.

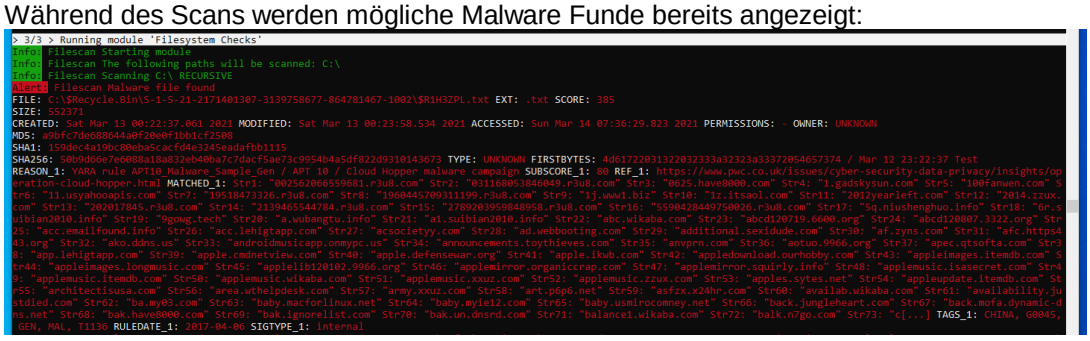


Sobald das Programm das erste Mal ausgeführt wird, lädt es automatisch die aktuellen Signaturen zum Überprüfen Ihrer Systeme herunter. Bitte beachten Sie, dass Ihr System hierzu Zugriff auf das Internet benötigt. Sollte dies nicht der Fall sein, so starten Sie den Scanner zuerst auf einem PC/Laptop mit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



Der Scanner prüft nun selbstständig ihr System:

Während des Scans werden mögliche Malware Funde bereits angezeigt:



TLP:WHITE

Bitte beachten Sie: Aufgrund der verwendeten Technologie kann es sein, das 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 (beispielweise 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 Videobotschaft[4] 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 tiefergreifende 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

[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