TLP:WHITE

Bundesamt
für Sicherheit in der
Informationstechnik

# Microsoft Exchange Schwachstellen

CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065

# Detektion und Reaktion

*Version 2.4, Stand 19.03.2021*

# Änderungshistorie

| *Version* | *Datum* | *Name* | *Beschreibung* |
|---|---|---|---|
| Initiale Version v1.0 | 08.03.2021 | Bundesamt für Sicherheit in der Informationstechnik | Ergänzende Informationen zur BSI Warnmeldung. |
| v1.1 – v1.4 | 09.03.2021 | Bundesamt für Sicherheit in der Informationstechnik | Ergänzungen zu Detektionsmöglichkeiten, Korrekturen bei URLs, Aufnahme weiterer Quellen sowie Hinweis auf ACS-Seite zu APT-Dokumenten. |
| v2.0 | 10.03.2021 | Bundesamt für Sicherheit in der Informationstechnik | Aufnahme weiterer Detektionsmöglichkeiten sowie Hinweise zur forensischen Sicherung und Datenschutz. |
| v2.1 | 11.03.2021 | Bundesamt für Sicherheit in der Informationstechnik | Verweis auf neue Berichte sowie Hinweis auf ZAC. |
| v2.2 | 12.03.2021 | Bundesamt für Sicherheit in der Informationstechnik | Hinweise zu Ransomware, Update der YARA-Regel. |
| v2.3 | 16.03.2021 | Bundesamt für Sicherheit in der Informationstechnik | Hinweise zu geänderten Verzeichnisrechten, Exchange On-premises Mitigation Tool (EOMT), weitere Quellen. |
| v2.4 | 19.03.2021 | Bundesamt für Sicherheit in der Informationstechnik | Powercat-Link aufgrund von Antivirus-Erkennungen verschleiert, exklusiver Webshell-Zugriff durch Angreifende, Beschreibung weiterer nachgeladener Payloads. |

**ⓘ Hinweis**

Auf Grund der fortlaufenden Entwicklungen und Erkenntnisse des BSI wird dieses Dokument laufend aktualisiert und angepasst. Bitte achten Sie darauf, immer die aktuellste Version zu nutzen.

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Internet: https://www.bsi.bund.de
Service-Center (Telefon): 0800 2741000
Service-Center (E-Mail): service-center@bsi.bund.de
Einen Vorfall melden: https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/IT-Sicherheitsvorfall/Unternehmen/Online-Meldung/online-meldung_node.html
Für die Zielgruppen und Partner des BSI gelten darüber hinaus die üblichen Meldewege.

# Inhalt

# 1 Die Intention der Angreifenden

Aktuell werden die Exchange-Schwachstellen von mehreren Tätergruppen ausgenutzt, die laut öffentlicher Berichte von Sicherheitsfirmen in der Vergangenheit mit Informationsbeschaffung in Verbindung gebracht wurden. Ziele waren damals Think-Tanks, Universitäten und Nicht-Regierungs-Organisationen sowie Kanzleien und Rüstungsfirmen. Die betroffenen Organisationen waren in der Regel in Nordamerika ansässig und sind bis dahin offenbar sehr gezielt ausgesucht worden (vgl. z.B. [Mic2021a]).

Spätestens seit Bekanntwerden der Schwachstellen hat sich das Verhalten der Angreifenden jedoch stark geändert. Nun werden die Exploits **massenhaft gegen Tausende von Zielen eingesetzt - offenbar weltweit.**

Es ist bisher unklar, ob die geänderte Vorgehensweise auch mit geänderten Intentionen und Zielen einhergeht. Es ist denkbar, dass das Ziel weiterhin Informationsbeschaffung ist und die Exploits mit maximaler Wirkung eingesetzt werden sollten, bevor Sicherheitsteams weltweit Patches einspielen können. In diesem Fall wird nur ein Bruchteil der kompromittierten Organisationen für die Angreifenden interessant sein - sie benötigen aber zunächst Zeit, um ihre Opfer zu triagieren. Aber auch das Szenario, dass die Angreifenden die Exploits nun finanziell motiviert verwenden und in späteren Schritten relativ großflächig Ransomware oder Ähnliches nachladen, erscheint plausibel (vgl. z.B. auch [CIS2021b]).

Auf Basis der derzeitigen Informationslage kann keines der genannten Szenarien eindeutig bestätigt werden. Man darf jedoch davon ausgehen, dass Sicherheitsfirmen und Medien zeitnah berichten werden, sobald sichtbare Effekte wie Ransomware festgestellt werden.

### Weitere Informationen zu Angriffen / Medienberichte

Am 10.03.2021 veröffentlichte die Sicherheitsfirma ESET Research einen Blogbeitrag (siehe [FTD2021]), in dem darüber berichtet wird, dass die Exchange-Schwachstellen von mindestens 10 verschiedenen APT-Gruppen massenhaft ausgenutzt werden (bzw. zum Teil schon vor Veröffentlichung der Out-of-Band Patches von Microsoft ausgenutzt wurden). Laut ESET handelt es sich dabei mit Ausnahme von DLTMiner (einer Gruppe, die mit Kryptomining in Verbindung gebracht wird) ausschließlich um solche APT-Gruppen, die im Kontext der Informationsbeschaffung gesehen werden (dazu zählen z.B. Tick, LuckyMouse, Calypso, Tonto Team, Mikroceen oder auch Winnti). Im nachfolgenden Abschnitt 1.1 sowie in Kapitel 4 „Wie kann ich weitere Aktivitäten detektieren?“ finden Sie weitergehende Informationen.

**Neue Informationen zu Ransomware**

Am 11.03.2021 berichtete Bleeping Computer über eine mögliche **Ransomware** namens **DearCry (Ransom:Win32/DoejoCrypt.A)**, welche unter Umständen die Microsoft Exchange Schwachstellen auf Servern ausnutzt, um sich zu verbreiten (siehe [Abr2021]). Am 12.03.2021 bestätigte das Microsoft Security Intelligence Team via Twitter[1], dass die Ransomware manuell nach initialer Ausnutzung der Microsoft Exchange Schwachstellen eingesetzt wird (siehe [MSI2021]).

**Eine großflächige automatisierte Ausnutzung kann zwar derzeit noch nicht beobachtet werden, dies könnte sich jedoch schnell ändern – insbesondere, wenn genaue Beschreibungen von Angriffswegen und funktionsfähige PoC-Skripte veröffentlicht werden**.

In Kapitel 5 „Weitere Hinweise“ finden Sie daher weitere wichtige Hinweise zum Thema Ransomware.

[1] “We have detected and are now blocking a new family of ransomware being used after an initial compromise of unpatched on-premises Exchange Servers. Microsoft protects against this threat known as Ransom:Win32/DoejoCrypt.A, and also as DearCry.”

## 1.1 APT-Gruppen im Kontext der MS Exchange Schwachstellen

**ⓘ Hinweis**

Wie bereits beschrieben, berichtete die Sicherheitsfirma ESET Research in einem Blogbeitrag davon, mehrere APT-Gruppen im Zusammenhang mit den MS Exchange Schwachstellen beobachtet zu haben. Die nachfolgende Tabelle zeigt übersichtlich alle in [FTD2021] genannten Informationen zu den APT-Gruppen. Davon erscheinen insbesondere die beiden letzten Einträge relevant, da Aktivitäten von diesen beiden Gruppen verstärkt auch in Deutschland beobachtet werden konnten.

| Gruppe | Typische Zielregionen | Typische Sektoren | Typische Malware | Zugang zu Exploits |
|---|---|---|---|---|
| Hafnium | Nordamerika | ThinkTanks, NGOs, Rüstung, Kanzleien, Corona-Forschung | Mist | Vor Bekanntwerden |
| Tick/ BronzeButler | Ostasien, Russland | u.a. IT | Datper, Daserf, xxmm, Lilith, ShadowPad | Vor Bekanntwerden |
| LuckyMouse/ APT27/ EmissaryPanda | Zentralasien, Mittlerer Osten, | Behörden, intern. Organisationen | SysUpdate/ Soldier, HyperBro | Vor Bekanntwerden |
| Tonto Team/ Karma Panda/ Cactus Pete | Osteuropa, Asien | Regierung, IT | ShadowPad, Bisonal | Nach dem Patch |
| Calypso | Zentralasien, Mittlerer Osten, Südamerika, später auch Afrika, Asien, Europa | Regierungen, ungenannte Wirtschafts-sektoren | PlugX, Whitebird/ Agent.UFX | Vor Bekanntwerden |
| Mikroceen/ Vicious Panda | Zentralasien | Regierungen, Telkos | Mikroceen RAT | Nach dem Patch |
| „Winnti“-Nutzer | Ostasien | Chemie, Gesundheit, Telkos, Energie, Spiele | PlugX, Winnti v4 | Vor Bekanntwerden |
| Websiic | Asien, Osteuropa | IT, Telko, Maschinenbau, Regierungen | Eigener Loader | Vor Bekanntwerden |
| **DLTMiner** | **weltweit** | **ungezielt** | **CryptoMiner** | **Nach dem Patch** |
| **Unbekannte Gruppe** | **u.a. Deutschland** | **großflächig** | **CobaltStrike** | **Nach dem Patch** |

# 2 Vorbemerkungen zur Detektion

**☝ Wichtiger Hinweis**

Da bei auffälligen Funden ggf. tiefergehende forensische Analysen notwendig werden, empfiehlt es sich, bereits vor der Suche eine Gesamtsicherung des Exchange-Servers durchzuführen. Zusätzlich sollten zumindest die Event-Logs des Domain Controllers gesichert werden. (Hinweis: Um Security-Logs des Domain Controllers länger vorzuhalten, können die Event-Logs auch mit Hilfe von Bordmitteln archiviert werden).

Zudem empfiehlt es sich, das Logging für die Firewall (zumindest für den/die Exchange Server) sowie für Powershell auf dem/den Exchange-Server/n sowie auf dem/den DC/s zu intensivieren. Stellen Sie dabei sicher, dass ggf. ältere Logdaten nicht überschrieben werden.

**ⓘ Hinweise zu möglichen Meldepflichten und Strafanzeige**

Beachten Sie, dass etwaige Funde auf eine Kompromittierung hinweisen, aufgrund derer entsprechende **Meldepflichten** zu **beachten** sein könnten **(z.B. nach Art. 33 DSGVO, BSIG, usw.).** Zum Beispiel könnten personenbezogene Daten abgeflossen sein, da die Angreifenden zumindest theoretisch Zugriff auf die Postfächer hatten. Prüfen Sie die Situation daher im Zweifelsfall gemeinsam mit Ihrem/Ihrer Datenschutzbeauftragten, um ggf. rechtzeitig (binnen 72 Stunden) die zuständige Aufsichtsbehörde (den/die Landesdatenschutzbeauftragte/n) zu informieren.

Sollten Sie aufgrund etwaiger Funde von einer Kompromittierung ausgehen (z.B. aufgrund weiterer Malware-Funde), empfiehlt das BSI zudem **Strafanzeige bei der für Sie zuständigen Polizei** zu **stellen**. Das Bundeskriminalamt bzw. die zuständigen Landeskriminalämter haben für diese Zwecke Anlaufstellen eingerichtet (Zentralen Ansprechstellen Cybercrime für die Wirtschaft (ZAC)), die Opfern von Cyber-Straftaten beratend zur Seite stehen und bei einer Anzeige unterstützen (Weitere Informationen finden Sie hier: https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/IT-Sicherheitsvorfall/Unternehmen/Kontakt-zur-Polizei/kontakt-zur-polizei_node.html).

# 3 Wie kann ich erkennen, ob ich betroffen bin?

Die Schwachstellen erlauben es Angreifenden, auch ohne Credentials, **Mails von beliebigen Postfächern auszulesen, beliebige Dateien auf dem Exchange-Server (oder auf Freigaben mit der Identität des System-Benutzers des Exchange-Servers) zu schreiben** und **eigenen Code auf dem Exchange-Server im Kontext des System-Benutzers auszuführen**. Auf diese drei Möglichkeiten sollte demnach geprüft werden. Dafür eignen sich die im Folgenden beschriebenen Methoden.

**ⓘ Hinweis**

Die im Folgenden beschriebenen Methoden lassen sich zum Teil automatisiert durch Skripte und geeignete Software überprüfen. Dazu zählen z.B.:

- **Microsoft Test Skript:** https://github.com/microsoft/CSS-Exchange/tree/main/Security
  Das Tool enthält alle IOCs, die in dem Microsoft Blogpost beschrieben werden:
  https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/
  *Hinweis: Achten Sie darauf immer die neueste Version des Skripts zu verwenden, da Microsoft bereits mehrere Updates veröffentlicht hat.*

- **Microsoft Support Emergency Response Tool (MSERT):** Microsoft Defender hat den Microsoft Safety Scanner (MSERT.exe) aktualisiert, um mögliche Ausnutzungen der Microsoft Exchange Schwachstellen zu detektieren. Das Tool kann von Administratoren **für Server** genutzt werden, **die nicht von Microsoft Defender geschützt werden** (Hinweis: Das Tool muss mit dem Argument „/N“ gestartet werden, wenn eventuelle Funde nicht direkt gelöscht werden sollen: msert.exe /N): https://msrc-blog.microsoft.com/2021/03/05/microsoft-exchange-server-vulnerabilities-mitigations-march-2021/

- Am 15.03.2021 hat **Microsoft** unter dem zuvor genannten Link das **Exchange On-premises Mitigation Tool (EOMT)** bereitgestellt, dass das o. g. MSERT enthält. **Es dient nicht als Ersatz für die Sicherheitsupdates, kann jedoch bis zur Installation dieser zum Einsatz kommen.** Auch die Suche nach Webshells und weiteren Infektionen ist weiter zwingend notwendig, sonst droht ein späteres Nachladen weiterer Schadprogramme (z. B. Ransomware).

- **Microsoft IOC Feed:** Microsoft veröffentlicht bekannte Hashes und maliziöse Dateipfade in einem eigenen Feed. Die Daten sind in JSON und CSV erhältlich:
  https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/Sample%20Data/Feeds/MSTICIoCs-ExchangeServerVulnerabilitiesDisclosedMarch2021.csv und
  https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/Sample%20Data/Feeds/MSTICIoCs-ExchangeServerVulnerabilitiesDisclosedMarch2021.json

- **MISP:** Organisationen, die in einem Malware Information Sharing Portal (MISP) Verbund angeschlossen sind, finden im MISP-Event "HAFNIUM - Mass attack on Microsoft Exchange Servers" (UUID: b7636c3e-a515-436b-a646-5ebd750df006) weitere Informationen.

- **Sigma**: Das Sigma Team hat eine Regel veröffentlicht, welche zur Detektion der Exchange Schwachstellen genutzt werden kann:
  https://github.com/SigmaHQ/sigma/blob/master/rules/web/web_exchange_exploitation_hafnium.yml

- **YARA:** Siehe [Rot2021a], [Rot2021b] und [Rup2021]. Als Alternative können auch die Yara Scanner Thor Lite[2] (https://www.nextron-systems.com/thor-lite/) oder Loki (https://github.com/Neo23x0/Loki) genutzt werden
- ~~**CERT.LV Detektions-Skript für Webshells:** Das lettische CERT hat ebenfalls ein eigenes Skript veröffentlicht, mit welchem nach Webshells im Kontext Hafnium gesucht werden kann: https://github.com/cert-lv/exchange_webshell_detection~~ Projekt eingestellt mit Verweis auf Microsoft MSERT (siehe oben)
- **Logsuche mit Bordmitteln:** Eric Capuano hat einige Beispielaufrufe bereitgestellt, die zur ersten schnellen Suche in Logs genutzt werden können: https://gist.github.com/ecapuano/13386852fb80beac4561f2bed569095e
- **Veränderte Verzeichnisberechtigungen:** Frank Zöchling stellt veränderte Verzeichnisberechtigungen nach erfolgreichen Exchange-Server Kompromittierung dar, die bei der Installation von Exchange-Updates zu Fehlermeldungen führen können. Bei geänderten Verzeichnisrechten ist von einer erfolgreichen Kompromittierung auszugehen: https://www.frankysweb.de/hafnium-veraenderte-verzeichnisberechtigungen-verhindern-update/
- Eine **deutschsprachige Übersicht der Exchange Schwachstellen, Sicherheitsupdates, Such- und Mitigationsmaßnahmen** findet sich zudem unter: https://www.msxfaq.de/exchange/update/hafnium-exploit.htm

## 3.1 Auslesen von E-Mails mittels CVE-2021-26855

Die Ausnutzung der o.a. Schwachstelle kann mittels Log-Einträgen nachvollzogen werden. Im Fall von Outlook on the Web/Outlook Web App (OWA) nutzen die Täter **POST-Anfragen auf statische Inhalte** unter dem Pfad /owa/auth/Current/themes/resources. Mit speziell präparierten SOAP-Payloads ist es den Tätern dann möglich, E-Mails ohne Authentifizierung zu exfiltrieren.

## 3.2 Auffälligkeiten in den ECP Server Logs

Hinweise für die Ausnutzung der Remote Code Execution Schwachstelle können sich in den **Exchange Control Panel (ECP) Server Logs** befinden (in der Regel finden Sie die Logs unter <exchange install path>\Logging\ECP\Server\), da die Ausnutzung im Kontext des Set-OabVirtualDirectory ExchangePowerShell cmdlet stattzufinden scheint [Vol2021].

Es empfiehlt sich daher nach dem **String** S:CMD=Set-OabVirtualDirectory.ExternalUrl='" zu suchen (*Hinweis: Der String könnte so oder so ähnlich aussehen*). Insbesondere die Zeichenfolge „script“ innerhalb eines solchen Log-Eintrags könnte auf die Ausnutzung der Schwachstelle CVE-2021-27065 hindeuten.

## 3.3 Suche nach Webshells

Ein typisches Vorgehen der Täter ist es, mit Ausnutzung der RCE-Schwachstelle eine Webshell auf dem Server zu hinterlassen, um weitere Befehle auszuführen.

[2] https://www.nextron-systems.com/2021/03/06/scan-for-hafnium-exploitation-evidence-with-thor-lite/

**☝ Wichtiger Hinweis**

Durch die sehr breite Ausnutzung der Schwachstelle ist davon auszugehen, dass nicht nur die Webshells zum Einsatz kommen, über die kürzlich im Kontext der Gruppe Hafnium durch Microsoft und Volexity berichtet wurde.

**☝ Wichtiger Hinweis**

Sollten Sie bei den Analysen keine Webshells finden, so sollten Sie berücksichtigen, dass der Microsoft Defender bzw. andere AV-Lösungen eventuelle Funde bereits gelöscht haben könnten. Überprüfen Sie daher auch die zentralen Logs Ihres Virenscanners bzw. die Einträge in der Ereignisanzeige unter Microsoft\Windows\Windows-Defender\Operational (zu finden unterhalb von Anwendungs- und Dienstprotokoll in der Ereignisanzeige) auf Logeinträge mit den Event-IDs 1006 bzw. 1116.

**☝ Wichtiger Hinweis**

Neben der Erkennung und Entfernung von Webshells durch Antivirusprogramme können diese auch durch Angreifende gelöscht werden, um einen exklusiven Zugriff zu erlangen. Dem BSI liegen Hinweise vor, dass Angreifende zuvor abgelegte Webshells löschen und eine eigene Webshell versteckt als Systemdatei ablegen. Des Weiteren ist eine Anpassung der Rechte der OWA- und ECP-Verzeichnisse auf „nur lesen und ausführen“ zu beobachten, sodass nach der Umsetzung weitere Angreifende keinen Schadcode mehr ablegen können. Aufgrund von geänderten Verzeichnisrechten fehlgeschlagene Exchange-Updates können auf derartige Aktivitäten hindeuten.

Mindestens die folgenden Webshells wurden bereits im Zusammenhang mit der Ausnutzung der Exchange-Schwachstelle beobachtet:

- SIMPLESEESHARP
- SPORTSBALL
- China Chopper
- ASPXSPY
- reGeorg

Daher ist es sinnvoll, sowohl spezifisch als auch generisch nach Webshells zu suchen:

- Die YARA-Regeln unter [Rot2021b] helfen bei der Suche nach Webshells im Kontext Hafnium.
- Die YARA-Regeln unter [Rup2021] helfen bei der Suche nach generischen Webshells.

Im Zusammenhang mit den Exchange Schwachstellen sind zudem ASPX-Dateien in den folgenden Verzeichnissen und Unterverzeichnissen [Vol2021] auffällig[3]:

- \inetpub\wwwroot\aspnet_client\
- \<exchange install path>\FrontEnd\HttpProxy\ecp\auth\ *(lediglich TimeoutLogout.aspx ist legitim)*

[3] Die NCC Group hat ein GitHub Respository veröffentlicht, in dem sie die Hashwerte der Dateien in den Exchange-Installationsverzeichnissen aus den Installationspaketen zur Verfügung stellen, was ggf. als Abgleich für die Suche nach Webshells hilfreich sein kann: https://github.com/nccgroup/Cyber-Defence/tree/master/Intelligence/Exchange
(vgl. auch https://twitter.com/NCCGroupInfosec/status/1368466300515844096).

- \<exchange install path>\FrontEnd\HttpProxy\owa\auth\Current\
- \<exchange install path>\FrontEnd\HttpProxy\owa\auth\<Versionsnummer>\

Etwas aufwendiger ist die Suche in folgendem Verzeichnis, das bei einer Standard-Installation ASPX-Dateien enthält. Webshells können auch in diese legitimen Dateien eingefügt werden, indem eine einzige Zeile ergänzt wird.

- \<exchange install path>\FrontEnd\HttpProxy\owa\auth\
  (Dateien, die nicht mehr dem Stand der Standard-Installation entsprechen)

Bei Internet Information Service (IIS)-Webservern werden ASP-Dateien zu temporären Bibliotheken kompiliert. Die Dateien mit dem Namen app_web_[a-zA-Z0-9]{8}.dll können auch eine mögliche Webshell enthalten (siehe nachfolgende YARA-Regel).

```
rule Compiled_Webshell_Mar2021_1 {
   meta:
      description = "Triggers on temporary pe files containing strings commonly used in webshells."
      author = "Bundesamt fuer Sicherheit in der Informationstechnik"
      date = "2021-03-05"
      modified = "2021-03-12"
   strings:
      $x1 = /App_Web_[a-zA-Z0-9]{7,8}.dll/ ascii wide fullword

      $a1 = "~/aspnet_client/" ascii wide nocase
      $a2 = "~/auth/" ascii wide nocase

      $b1  = "JScriptEvaluate" ascii wide fullword

      $c1 = "get_Request" ascii wide fullword
      $c2 = "get_Files" ascii wide fullword
      $c3 = "get_Count" ascii wide fullword
      $c4 = "get_Item" ascii wide fullword
      $c5 = "get_Server" ascii wide fullword
   condition:
      uint16(0) == 0x5a4d and filesize > 5KB and filesize < 40KB and all of ($x*) and 1 of ($a*) and ( all of ($b*) or all of
($c*) )
}
```

## 3.4 Web Log User Agents

Volexity erwähnt auch einige User-Agents, die zwar nicht als eindeutige Indikatoren für eine Kompromittierung zu verstehen sind, jedoch als weitere Anhaltspunkte dienen können, wenn ein Kompromittierungsverdacht besteht [Vol2021].

**POST Requests zu den Dateien in den Ordnern unter /owa/auth/Current**

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/537.36

**Auffällige User-Agents im Kontext der Ausnutzung der /ecp/ URLs**

ExchangeServicesClient/0.0.0.0
python-requests/2.19.1
python-requests/2.25.1

(Hinweis: Hier wurden auch Post-Requests auf statische Ressourcen wie z.B. /ecp/y.js beobachtet)

**Auffällige User-Agents im Kontext des Post-Exploitation-Zugriffs auf Webshells**

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 )

# 4 Wie kann ich weitere Aktivitäten detektieren?

**☝ Wichtiger Hinweis**

Eine weitergehende Kompromittierung der Domäne ist durch die im Standard vorhandenen hohen Rechte der Exchange Server im Active Directory verhältnismäßig einfach möglich. **Es sollte auf eine weitergehende Kompromittierung des ADs bspw. mit den Rechten des Exchange Servers oder durch Hinzufügen von neuen Benutzern mit hochprivilegierten Rechten geprüft werden.**
Es ist möglich, dass die Active Directory Datenbank (ntds.dit) bspw. über ein nach außen verfügbares Exchange-Verzeichnis ausgeleitet wurde.

**Hinweis: Microsoft hat am 09.03.2021 auch Patches für eine kritische RCE-Schwachstelle (CVE-2021-26897, CVSS: 9.8) im DNS-Server veröffentlicht [Mic2021c]. Da DNS-Server oftmals auf dem AD betrieben werden, könnte diese Schwachstelle ausgenutzt werden, um vom Exchange Server aus Zugriff auf das AD zu erhalten. Das BSI empfiehlt daher dringend, entsprechende Patches zeitnah einzuspielen.**

**Dumpen von Credentials aus dem Speicher**

Die Angreifer verwenden u.a. Procdump, um den LSASS Prozessspeicher zu dumpen:

```
C:\windows\temp\procdump64 -accepteula -ma lsass.exe C:\windows\temp\lsass
```

Das Dumpen des LSASS Prozessspeichers via Procdump hinterlässt ein Artefakt in Form eines „EulaAccepted"-Eintrags mit dem Wert „1" in der Registry unter HKEY_USERS\<SID des verwendeten Benutzers>\Software\Sysinternals\ProcDump, welches auf dem betroffenen Server geprüft werden kann.

Laut [Vol2021] wurde der LSASS Prozessspeicher in manchen Fällen auch mit Hilfe von comsvcs.dll gedumpt, da comsvcs.dll als LOLBin nativ auf den Servern vorhanden ist:

```
rundll32 C:\windows\system32\comsvcs.dll / MiniDump lsass.dmp
```

Alternativ verwenden die Täter auch eine spezielle Variante von Mimikatz. Diese wurde mit dem Dateinamen CreateRemoteThreadTest.exe und dem SHA-256-Hash 173ac2a1f99fe616f5efa3a7cf72013ab42a68f7305e24ed795a98cb08046ee1 verwendet [Rap2021].

**Staging**

In einigen Fällen haben die Täter Daten, die sie stehlen wollen, per 7Zip in ZIP-Archiven zusammengefasst [Mic2021b]. Die Existenz unerwarteter ZIP-Dateien (mit meist kurzen Namen und in Verzeichnissen wie "ProgramData\" kann daher ein Hinweis auf Exfiltration sein.

**Nachladen von Tools**

Vereinzelt haben die Täter PowerCat von Github heruntergeladen und verwendet. Es kann daher geprüft werden, ob die URL hXXps://raw[.]githubusercontent[.]com/besimorhino/powercat/master/powercat[.]ps1 (für die Suche hXXps gegen https austauschen sowie die eckigen Klammern entfernen) in den Log-Daten auftaucht. Falls PowerCat nicht von den Administratoren selbst verwendet wird, kann geprüft werden, ob die Datei powercat.ps1 auf dem System vorhanden ist.

Außerdem wurden Varianten von den „Invoke-TheHash“ Powershell-Skripten von Kevin Robertson (https://github.com/Kevin-Robertson/Invoke-TheHash) beobachtet, die mit zuvor ausgespähten NTLM-Hashes via Windows Management Instrumentation (WMI) und Server Message Block (SMB) Protokoll Code ausführen können.

**Umbenennen von cmd.exe**

Bei Bedarf haben die Täter die cmd.exe in "ProgramData\" kopiert und ggf. umbenannt.

**DLL-Side-Loading**

Um weitere Backdoors zu installieren, verwenden die Täter DLL-Side-Loading. Zu diesem Zweck wird eine legitime Anwendung (wie z.B. AppLaunch.exe) in einen kurzen Dateinamen umbenannt und zusammen mit einer maliziösen DLL in ein Verzeichnis wie "ProgramData\" kopiert. Die Existenz einer unerwarteten Datei mit zweistelligem Dateinamen und .exe-Dateiendung zusammen mit einer DLL kann also ein Hinweis auf Aktivität der Täter sein.

**Scheduled Tasks**

[Grö2021] nennen die Möglichkeit, dass von Angreifenden auch Scheduled Tasks gesetzt worden sein könnten, um Persistenz zu erlangen. Es empfiehlt sich daher, alle gesetzten Scheduled Tasks seit November 2020 auf Legitimität zu überprüfen (bzw. die Task Scheduler Logs zu überprüfen).

**APT Aktivitäten**

[FTD2021] nennen in ihrem Blogeintrag eine Vielzahl von IOCs, die Sie zur Suche nach möglichen Spuren verwenden können.

Mit Bezug auf [FTD2021] finden Organisationen, die in einem Malware Information Sharing Portal (MISP) Verbund angeschlossen sind, im MISP-Event "Exchange servers under siege from at least 10 APT groups (OSINT)" (UUID: 5ef60b0d-a198-4216-93c5-4b12748294ae) gesammelt alle IOCs.

# 5 Weitere Hinweise

**Weitere spezifische Hinweise**

Weitere sehr detaillierte Hinweise (auf Englisch) finden sich auch unter [Blu2021], [Ham2021], [Fir2021], [Exu2021] und [CIS2021a], [CIS2021b].

**Weitere generische Hinweise**

Viele weitere generische Hinweise zum Umgang mit IT-Sicherheitsvorfällen finden Sie auch auf der Webseite des BSI: https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/Kritische-Infrastrukturen-und-meldepflichtige-Unternehmen/kritische-infrastrukturen-und-meldepflichtige-unternehmen.html?nn=133608&cms_pos=1

Viele weitere Hinweise zur Detektion von Advanced Persistent Threats sowie zur Reaktion bei Hinweisen auf eine Kompromittierung finden Sie darüber hinaus auch in den nachfolgend aufgeführten BSI-Publikationen:

**TLP:AMBER Advanced Persistent Threats – Teil 3 Detektion**
**Technische und organisatorische Maßnahmen für die Vorfallsbearbeitung**
*Anlassbezogene und akute Hilfestellungen,* BSI 2021

**TLP:WHITE, in Teilen TLP:AMBER Advanced Persistent Threats – Teil 4 Reaktion**
**Technische und organisatorische Maßnahmen für die Vorfallsbearbeitung**
*Anlassbezogene und akute Hilfestellungen,* BSI 2021

**TLP:GREEN Advanced Persistent Threats – Teil 5 Reaktion**
**Strategische Maßnahmen zur Reaktion für das Management**
*Wo zieht man im Angriffsfall rote Linien?,* BSI 2021

**ⓘ Hinweis**

Weitere Informationen zu den genannten APT-Dokumenten finden Sie unter:

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Gefaehrdungen/APT/apt.html

**Bitte beachten Sie, dass die Dokumente aufgrund der Einstufung z.T. nur über den internen Bereich der ACS bzw. nur im internen INSI-Bereich der ACS verfügbar sind.**

**Weitere Hinweise zu Ransomware**

Das BSI stellt Ihnen auf der BSI-Webseite sowie auf den Webseiten der Allianz für Cybersicherheit vielfältige Informationen zum Thema Ransomware zur Verfügung:

https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Informationen-und-Empfehlungen/Empfehlungen-nach-Gefaehrdungen/Ransomware/ransomware_node.html

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Schadprogramme/Ransomware/ransomware_node.html

# Literaturverzeichnis

**Abr2021** Lawrence Abrams, Ransomware now attacks Microsoft Exchange servers with ProxyLogon exploits, https://www.bleepingcomputer.com/news/security/ransomware-now-attacks-microsoft-exchange-servers-with-proxylogon-exploits/

**Blu2021** Blue Team Blog, Microsoft Exchange Zero Day's – Mitigations and Detections, https://blueteamblog.com/microsoft-exchange-zero-days-mitigations-and-detections

**CIS2021a** Cybersecurity & Infrastructure Security Agency (CISA), Alert (AA21-062A) Mitigate Microsoft Exchange Server Vulnerabilities, https://us-cert.cisa.gov/ncas/alerts/aa21-062a

**CIS2021b** Cybersecurity & Infrastructure Security Agency (CISA), Remediating Microsoft Exchange Vulnerabilities, https://us-cert.cisa.gov/remediating-microsoft-exchange-vulnerabilities

**Exu201** Exupdatestepbystep, https://exupdatestepbystep.azurewebsites.net/

**FTD2021** Matthieu Faou, Mathieu Tartare, Thomas Dupuy, WeliveSecurity by ESET, Exchange Server under siege from at least 10 APT groups, https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/

**Fir2021** FireEye, Threat Research: Detection and Response to Exploitation of Microsoft Exchange Zero-Day Vulnerabilities, https://www.fireeye.com/blog/threat-research/2021/03/detection-response-to-exploitation-of-microsoft-exchange-zero-day-vulnerabilities.html

**Grö2021** Rasmus Grönlund, Tracking Microsoft Exchange Zero-Day ProxyLogon and HAFNIUM, https://blog.truesec.com/2021/03/07/exchange-zero-day-proxylogon-and-hafnium/

**Ham2021** John Hammond, Rapid Response: Mass Exploitation of On-Prem Exchange Servers, https://www.huntress.com/blog/rapid-response-mass-exploitation-of-on-prem-exchange-servers

**Mic2021a** Microsoft, New nation-state cyberattacks, https://blogs.microsoft.com/on-the-issues/2021/03/02/new-nation-state-cyberattacks/

**Mic2021b** Microsoft, HAFNIUM targeting Exchange Servers with 0-day exploits, https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

**Mic2021c** Microsoft, Windows DNS Server Remote Code Execution Vulnerability, https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26897

**MSI2021** Microsoft Security Intelligence via Twitter, https://twitter.com/MsftSecIntel/status/1370236539427459076?s=19

**Rap2021** Rapid7, https://blog.rapid7.com/2021/03/03/rapid7s-insightidr-enables-detection-and-response-to-microsoft-exchange-0-day/

**Rot2021a** Florian Roth, apt_hafnium_log_sigs.yar, https://github.com/Neo23x0/signature-base/blob/master/yara/apt_hafnium_log_sigs.yar

**Rot2021b** Florian Roth, apt_hafnium.yar, https://github.com/Neo23x0/signature-base/blob/master/yara/apt_hafnium.yar

**Rup2021** Arnim Rupp, gen_webshells.yar, https://github.com/Neo23x0/signature-base/blob/master/yara/gen_webshells.yar

**Vol2021** Volexity, Operation Exchange Marauder: Active Exploitation of Multiple Zero-Day Microsoft Exchange Vulnerabilities, https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/

# Abkürzungsverzeichnis

| | |
|---|---|
| **AD** | Active Directory |
| **APT** | Advanced Persistent Threat |
| **BSI** | Bundesamt für Sicherheit in der Informationstechnik |
| **DLL** | Dynamic Link Library |
| **ECP** | Exchange Control Panel |
| **IIS** | Internet Information Service |
| **IOC** | Indicators of Compromise |
| **MISP** | Malware Information Sharing Platform |
| **OWA** | Outlook Web App |
| **PoC** | Proof of Concept |
| **RCE** | Remote Code Execution |
| **SMB** | Server Message Block |
| **WMI** | Windows Management Instrumentation |