Tactics, Techniques, and Procedures (TTPs) Used by HAFNIUM to Target Microsoft Exchange Servers

picussecurity.com/resource/blog/ttps-hafnium-microsoft-exchange-servers

Tactics, Techniques, and Procedures (TTPs) Used by HAFNIUM to Target Microsoft Exchange Servers
BLOG POST
Read Now
PICUS

Keep up to date with latest blog posts

Executive Summary

Microsoft released four out-of-band security updates on March 2, 2021 [1]. The usual reason for releasing an out-of-band update is the appearance of active and widespread exploitation of a 0-day vulnerability. In this case, these updates address 0-day vulnerabilities affecting Microsoft Exchange Server products that allow threat actors to read sensitive information in emails, take control of the target server, collect and exfiltrate data from the compromised server, and move laterally to other systems in the network.

The threat group that exploits Microsoft Exchange Server vulnerabilities is dubbed HAFNIUM by Microsoft [2] and the attack campaign is named Operation Exchange Marauder by Volexity [3]. Although the HAFNIUM threat group primarily targets defense, higher education, and health sectors in the United States, these zero-days affect unpatched Microsoft Exchange Servers worldwide. For example, The European Banking Authority (EBA) has announced that it has been the subject of a cyber-attack against its Microsoft Exchange Servers [4]. As another example, an incident due to these vulnerabilities is reported in Denmark [5].

In this article, we analyzed Tactics, Techniques, and Procedures (TTPs) utilized by the HAFNIUM threat actor to understand their attack methods and the impact of this breach. We also give mitigation and detection suggestions and relevant IOCs for this cyber attack campaign.

Key Findings

- Timeline: The attack campaign was detected first in January 2021 [3]. Microsoft released updates on March 2, 2021, and Volexity and Microsoft published blog posts on the same day. The European Banking Authority (EBA) announced the breach on March 7, 2021.
- Prevalence: The attack campaign has the potential to affect thousands of public and private organizations.
- Attack Lifecycle: Attack starts with reconnaissance of vulnerable Exchange servers and resumes with exploiting a vulnerability (CVE-2021-26855) to exploit other vulnerabilities (CVE-2021-26857, CVE-2021-26858, CVE-2021-27065). Then, the adversary uploads web shells using these vulnerabilities and executes malicious commands with uploaded web shells. In the post-exploitation phase, the adversary collects and exfiltrates data, dumps credentials, and moves laterally.
- Impact: Threat actors read sensitive information in mailboxes of users, compromise the victim server, dump local credentials, add user accounts, dump Active Directory database (NTDS.DIT), and move laterally to other systems in the network.
- Exploitability: Exploits are available, and all of the vulnerabilities are being exploited by adversaries. Exploits can be run remotely and do not require authentication.
- Priority: Security teams must treat them with the highest priority.
- Affected Versions: Microsoft Exchange 2019, 2016, 2013, 2010
- Mitigation: Microsoft Exchange Servers must be patched as soon as possible.
- Interim Mitigations: If you are unable to patch Exchange servers, implement IIS rewrite rules provided by Microsoft and disable UM, ECP, VDir, and OAB VDir Services [6].
- Detection: Scan Exchange server logs and paths for released IOCs. You can use Sigma/QRadar/Splunk/Arcsight detection rules released by Picus.

Vulnerabilities and Affected Exchange Servers

The Exploited Zero-Day Vulnerabilities and Their Impacts

Currently, the following vulnerabilities are exploited by adversaries:

CVE	Impact	Vulnerability Type	CVSS 3.0 Base Score
CVE-2021-26855 [7]	Gain access to mailboxes, read the full contents.	SSRF (Server-Side Request Forgery)	9.1 Critical
CVE-2021-26857 [8]	Arbitrary code execution as SYSTEM user, compromise the system	Insecure Deserialization	7.8 High

CVE-2021-26858 [9]	Arbitrary code execution, compromise the system	Post-Authentication Arbitrary File Write	7.8 High
CVE-2021-27065 [10]	Arbitrary code execution, compromise the system	Post-Authentication Arbitrary File Write	7.8 High

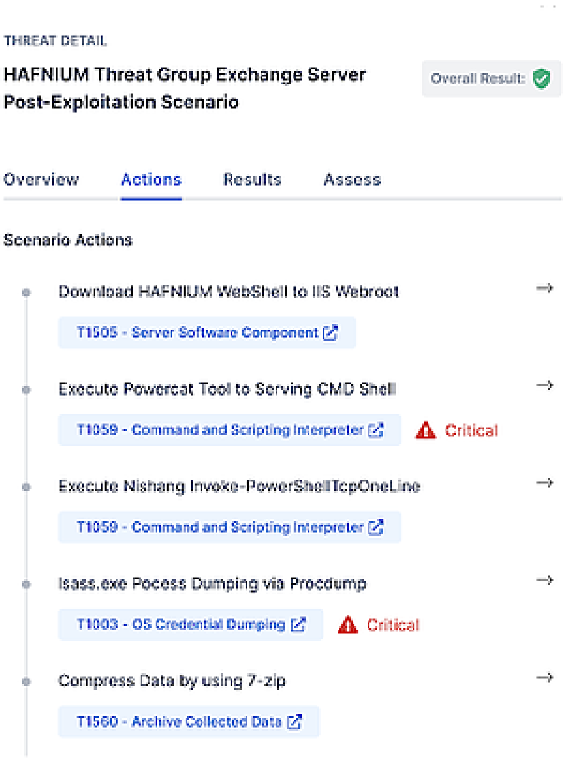
Although CVSS 3.0 score of the CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065 vulnerabilities is “7.8 High”, not “Critical”, when chained with the vulnerability CVE-2021-26855, these vulnerabilities enable the attacker to compromise the target Exchange server.

Affected Microsoft Exchange Server Versions

Version	Status	Mitigation
Exchange 2019	Affected (all CVEs)	Immediately deploy the updates.
Exchange 2016	Affected (all CVEs)	Immediately deploy the updates.
Exchange 2013	Affected (all CVEs)	Immediately deploy the updates.
Exchange 2010	Affected (CVE-2021-26857)	Immediately deploy the updates.
Exchange 2007	Unknown, stated as ”not believed to be affected” by Microsoft [1].	Unsupported version by Microsoft. Upgrade to a supported version.
Exchange 2003	Unknown, stated as ”not believed to be affected” by Microsoft [1].	Unsupported version by Microsoft. Upgrade to a supported version.
Exchange Online / Office 365	Not Affected	

Tactics, Techniques, and Procedures (TTPs) utilized by HAFNIUM

HAFNIUM uses 11 of 14 tactics in the MITRE ATT&CK framework. You can create an adversary emulation plan using techniques and sub-techniques given below to validate your security controls against the HAFNIUM threat group. Picus Threat database includes an APT adversary emulation scenario for HAFNIUM along with 700+ other attack scenarios and 10000+ network and endpoint attack emulations. Some actions of the HAFNIUM adversary emulation scenario in Picus is shown below.



HAFNIUM Threat Group Exchange Server Post-Exploitation Scenario

Scenario Actions

- Download HAFNIUM WebShell to IIS Webroot →
  T1505 - Server Software Component
- Execute Powercat Tool to Serving CMD Shell →
  T1059 - Command and Scripting Interpreter ⚠ Critical
- Execute Nishang Invoke-PowerShellTcpOneLine →
  T1059 - Command and Scripting Interpreter
- lsass.exe Pocess Dumping via Procdump →
  T1003 - OS Credential Dumping ⚠ Critical
- Compress Data by using 7-zip →
  T1560 - Archive Collected Data

1. Reconnaissance

The Reconnaissance tactic of the MITRE ATT&CK framework includes techniques involving adversaries to collect information actively and passively before compromising a victim [11]. Attackers use this information to use in other phases of the attack lifecycle, such as Initial Access as used by HAFNIUM.

1.1 MITRE ATT&CK T1592.002 Gather Victim Host Information: Software

The HAFNIUM threat actor determines whether an Exchange server is running on the machine, and if so, which version is running [1]. Adversaries collect information about installed software on a victim machine, which may be used for targeting [12].

2. Resource Development

The Resource Development tactic includes techniques involving adversaries to create, purchase, or compromise resources such as infrastructure, accounts, or capabilities [13]. They develop these resources before compromising the victim and leverage them to utilize in other phases, such as using leased Virtual Private Servers to support Command and Control.

2.1 MITRE ATT&CK T1583.003 Acquire Infrastructure: Virtual Private Server

HAFNIUM uses leased Virtual Private Servers (VPSs) in the United States to operate its threat campaign [1]. Adversaries rent VPSs to make it difficult to bind operations back to them physically [14]. They are also enabled to swiftly provision, modify, and shut down their infrastructure through VPSs.

2.2 MITRE ATT&CK T1588.002 Obtain Capabilities: Tool

Adversaries obtain tools in cyberattacks to support their operations [15]. These tools can be free or commercial, open or closed source. The HAFNIUM threat group uses the following tools to help its post-compromise behaviors.

Tool	Description
Procdump	`Procdump` is a command-line utility that is a part of the Microsoft Sysinternals suite. Although its primary purpose is monitoring an application for CPU spikes and generating crash dumps to determine the cause of the spike, it can be used to dump the memory of a process [16].
Nishang	`Nishang` is a collection of scripts and payloads which using PowerShell for penetration testing and red teaming. It can be categorized as a PowerShell post-exploitation framework [17]. Copy-VSS PowerShell script of Nishang can be used to copy the SAM file and dump credentials [16]. Advanced Persistent Threat (APT) groups are heavily using Nishang in their operations [17].
PowerCat	`PowerCat` is an open-source PowerShell script that can read and write data across network connections like the famous Netcat tool [18].
PsExec	`PsExec` is a legitimate Microsoft tool and a part of Windows Sysinternals utilities [19]. PsExec can execute commands and binaries on remote systems and download or upload a file over a network share. Attackers like Nefilim and LockerGoga ransomware gangs utilize PsExec for lateral movement [20] [21].
Covenant	`Covenant` is an open-source Command and Control (C2) framework written in .NET [22].
SIMPLESEESHARP	`SIMPLESEESHARP` is a simple ASPX web shell used by the HAFNIUM to write additional files to disk, such as the SPORTSBALL web shell [3].
SPORTSBALL	`SPORTSBALL` is a more extensive web shell used by HAFNIUM to upload files or execute commands on the system [3].
China Chopper	`China Chopper` is a web shell that provides access back into the victim system and is used by several threat groups [23].
ASPXSPY	`ASPXSpy` is a publicly available web shell used by several threat groups, such as Threat Group 3390 [24].
7-Zip	HAFNIUM uses 7-Zip to compress data to be exfiltrated.

Winrar	HAFNIUM uses WinRar to compress data prior to exfiltration.
Exchange Snap-ins	HAFNIUM uses Exchange PowerShell snap-ins to export data in mailboxes [2].

3. Initial Access

The Initial Access tactic includes techniques used by attackers to gain an initial foothold within a network, such as exploiting vulnerabilities on public-facing web servers [25].

3.1 MITRE ATT&CK T1190 Exploit Public-Facing Application

Adversaries exploit vulnerabilities in Internet-facing software, such as web servers, to gain access to the host [26]. HAFNIUM exploits CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065 vulnerabilities in the Internet-facing and vulnerable Microsoft Exchange servers for initial access [2] [3].

4. Execution

4.1 T1059.003 Command and Scripting Interpreter: Windows Command Shell

Web shells used by the HAFNIUM threat group, such as China Chopper [27], allow adversaries to execute commands on the victim server using Windows Command Shell (cmd.exe), the primary command prompt on Windows systems.

- Enroll in the free “MITRE ATT&CK Windows Command Shell” course in Purple Academy to learn how adversaries operate Windows Command Shell in their attacks and red and blue team exercises.
- Read our blog post about the Windows Command Shell (Command Line Interface) technique.

5. Persistence

The Persistence tactic consists of techniques used by adversaries to maintain their foothold across system restarts, changed credentials, or patched vulnerabilities [28].

5.1 MITRE ATT&CK T1505.003 Server Software Component: Web Shell

Adversaries use web shells, web scripts placed on web servers, as backdoors to establish persistency on the target server [29]. HAFNIUM utilize the following web shells as mentioned in the “T1588.002 Obtain Capabilities: Tool” technique:

- SIMPLESEESHARP
- SPORTSBALL
- China Chopper
- ASPXSPY

5.2 MITRE ATT&CK T1136.002 Create Account: Domain Account

Adversaries, such as HAFNIUM, add new domain accounts and grant privileges to these accounts to maintain access in the future [3].

6. Defense Evasion

Defense evasion consists of techniques that are used by adversaries to avoid detection by security controls.

6.1 T1036.005 Masquerading: Match Legitimate Name or Location

Adversaries may masquerade names/locations of their artifacts as identical or similar names/locations of legitimate files to evade monitoring and detection [30]. HAFNIUM masquerade names of deployed web shells as identical or similar names of legitimate files, such as log.aspx, logout.aspx, default.aspx, errorPage.aspx, and server.aspx. You can find the list of used web shell filenames in the Indicators of Compromise (IoC) list at the end of this article.

- Enroll in the free and practical “MITRE ATT&CK Masquerading” course in Purple Academy to learn all sub-techniques of this technique with red and blue team exercises:
- Read our blog post about the Masquerading technique.

7. Credential Access

The Credential Access tactic includes techniques used by adversaries to steal account usernames and passwords.

7.1 MITRE ATT&CK T1003.001 - OS Credential Dumping: LSASS Memory

There are many information sources targeted by attackers to dump credentials. As one of them, The Local Security Authority Subsystem Service (LSASS) stores credentials of the logged-in users in memory to provide seamless access to network resources without re-entering their credentials [16]. Adversaries interact with the lsass.exe process and dump its memory to obtain credentials. Several methods and tools can be utilized to dump credentials in memory. The HAFNIUM threat actor uses Procdump to dump the LSASS process memory and gather credentials. An example ProcDump command to dump credentials in this given below:

```
C:\temp>procdump.exe -accepteula -ma lsass.exe lsass.dmp
```

7.2 T1003.003 OS Credential Dumping: NTDS

HAFNIUM creates and steals copies of the NTDS.dit file using deployed web shells [3]. The NTDS.dit file is the Active Directory Domain Services (AD DS) database that contains AD data, including information about user objects, groups, and group membership. NTDS.dit database also includes the password hashes for all users in the domain.

- Enroll in the free “MITRE ATT&CK OS Credential Dumping” course in Purple Academy to learn 11 ways for credential dumping with practical red team exercises:
- Read our blog post about the OS Credential Dumping technique.

8. Lateral Movement

The Lateral Movement tactic includes techniques that are used by adversaries to access and control remote systems (lateral movement) on the target network [31].

8.1 MITRE ATT&CK T1021.002 - Remote Services: SMB/Windows Admin Shares

Hafnium uses PsExec to move laterally through the target environment [3]. PsExec is a legitimate Windows SysInternals tool used by attackers to run commands on the remote system by leveraging network shares or valid accounts [32].

9. Collection

The Collection tactic consists of techniques used by adversaries to gather the information that is relevant to their objectives.

9.1 MITRE ATT&CK T1560.001 - Archive Collected Data: Archive via Utility

Adversaries may use several utilities such as 7-Zip, WinRAR, and WinZip to compress or encrypt data before exfiltration [33]. Among these utilities, HAFNIUM uses WinRar and 7-Zip to compress data to be exfiltrated.

9.2. MITRE ATT&CK T1114.002 - Email Collection: Remote Email Collection

Adversaries may access external-facing Exchange services to access emails and collect sensitive information by leveraging valid accounts, access tokens, or remote exploits [34]. HAFNIUM adds and uses Exchange PowerShell snap-ins to export data in mailboxes [2].

10. Command and Control

The Command and Control (C2) tactic consists of techniques used by adversaries to communicate with compromised systems within a victim network [35].

10.1 MITRE ATT&CK T1071.001 - Application Layer Protocol: Web Protocols

The HAFNIUM threat group communicates with deployed web shells using application-layer web protocols (HTTP/HTTPS). Adversaries use these protocols for C2 to avoid detection and network filtering [36].

11. Exfiltration

11.1 MITRE ATT&CK T1567.002 - Exfiltration Over Web Service: Exfiltration to Cloud Storage

Adversaries may exfiltrate data to cloud storage that allows upload, modify and retrieve files. HAFNIUM exfiltrates collected data to cloud file sharing like MEGA.io [2].

Countermeasures by Picus

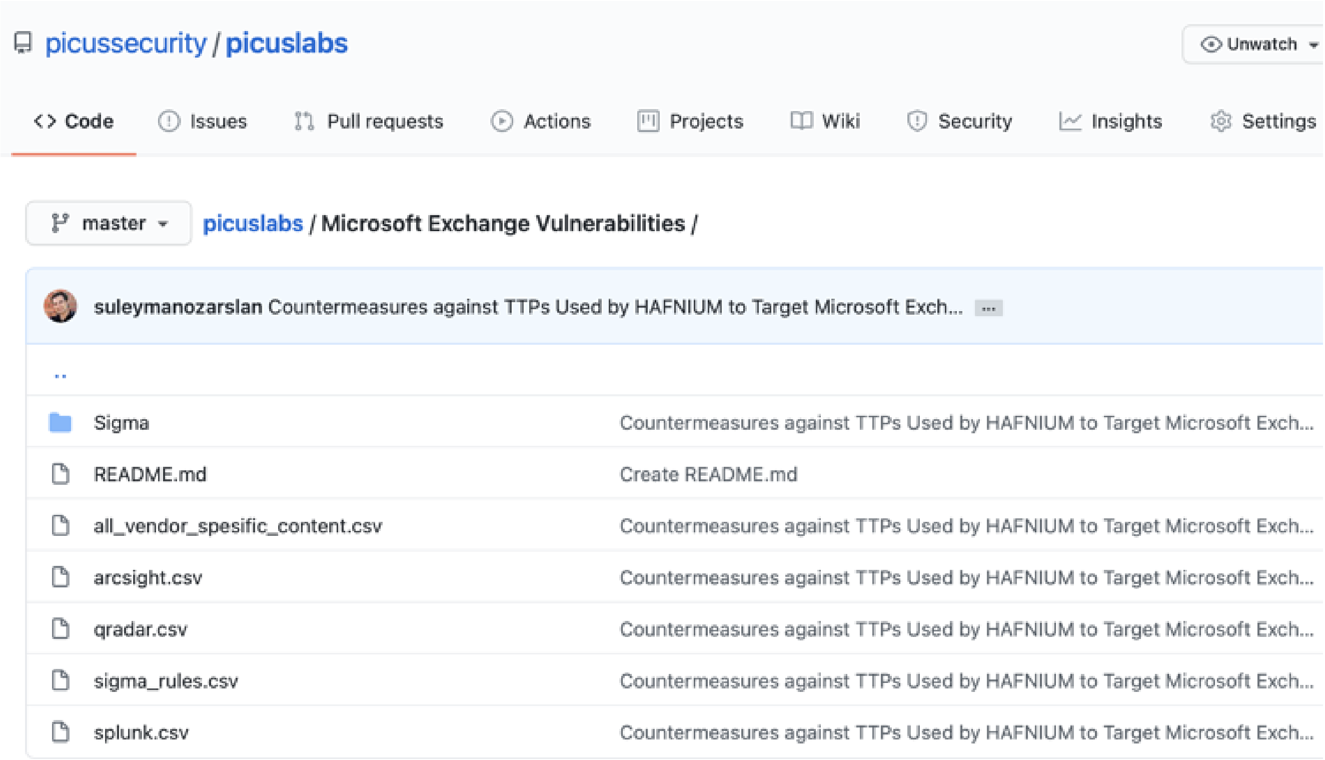
Built on technology alliances, Picus Mitigation Library delivers immediate value by providing mitigation insights in Network Security, Endpoint Detection and Response, and Security Information and Event Management categories. The Picus Threat Library includes most of the stolen tools in this breach, and the Picus Mitigation Library contains actionable mitigation recommendations and detection rules against them. Picus Labs' Red Team and Blue Teams are working on the missing tools and adding them and their techniques to our libraries.

So this means, Picus users have already assessed their cyber defense against most of the stolen red team tools and their attack techniques. And, they fixed the identified gaps using actionable recommendations provided by the Picus platform. We decided to share these actionable recommendations with the community in this article to help defend against these tools.

Countermeasures with Open-source Sigma and Snort Rules

Picus Labs Blue Team develops, tests, and verifies detection rules as SIGMA, a generic and open signature format for SIEM products, based on threats developed by Picus Labs Red Team. Also, Blue Team simulates these threats against Snort IPS, an open-source Intrusion Prevention System, and then analyzes the results and maps with the right signatures.

In this section, you can find the SIGMA rules and Snort signatures to defend against TTPs used by HAFNIUM to target Microsoft Exchange Servers. The SIGMA rule names and Snort signature categories are below as a list, but detailed information about these contents are published in Picus Labs' Github repository:



picussecurity / picuslabs

picuslabs / Microsoft Exchange Vulnerabilities /

suleymanozarslan Countermeasures against TTPs Used by HAFNIUM to Target Microsoft Exch...

..

Sigma	Countermeasures against TTPs Used by HAFNIUM to Target Microsoft Exch...
README.md	Create README.md
all_vendor_spesific_content.csv	Countermeasures against TTPs Used by HAFNIUM to Target Microsoft Exch...
arcsight.csv	Countermeasures against TTPs Used by HAFNIUM to Target Microsoft Exch...
qradar.csv	Countermeasures against TTPs Used by HAFNIUM to Target Microsoft Exch...
sigma_rules.csv	Countermeasures against TTPs Used by HAFNIUM to Target Microsoft Exch...
splunk.csv	Countermeasures against TTPs Used by HAFNIUM to Target Microsoft Exch...

SIGMA Rules:

- Process Dumping via Procdump
- Remote Command Execution via Powercat
- Suspicious ASPX File Creation
- Suspicious PowerShell Invoke Expression Usage
- TCP Connection Creating via PowerShell Script
- Data Collection with 7z.exe via Commandline

Snort Rules:

Signature Id	SignatureName
1.2017260.10	ET WEB_SERVER WebShell Generic - ASP File Uploaded
1.57241.4	SERVER-WEBAPP Microsoft Exchange Server server side request forgery attempt
1.57242.4	SERVER-WEBAPP Microsoft Exchange Server server side request forgery attempt
1.57244.4	SERVER-WEBAPP Microsoft Exchange Server server side request forgery attempt
1.2017260.10	ET WEB_SERVER WebShell Generic - ASP File Uploaded
1.2017260.10	ET WEB_SERVER WebShell Generic - ASP File Uploaded

Countermeasures with QRadar, Splunk, Carbon Black, and ArcSight

Picus is working with SIEM and EDR vendors in a Technical Alliance Partnership program. Picus Labs Blue Team develops SIEM (IBM QRadar, Splunk, Micro Focus ArcSight) and EDR (VMware Carbon Black) specific detection rules based on the SIGMA rules defined in the chapter above. Following the development, they test and analyze the results on each vendor environment and finalize the rules with the specific product's query language.

In this section, you can find the IBM QRadar, Splunk, Micro Focus ArcSight, and VMware Carbon Black rules to defend against the HAFNIUM threat group. You can find these rules in Picus Labs' Github repository.

Vendor-Specific Prevention Signatures

Picus is also working with network security vendors through its Technical Alliance Partnership (TAP) program. Picus Labs Blue Team simulates the threats developed by Picus Labs Red Team against TAP vendor environments and then analyzes the results and maps with the right signatures to eliminate F/P issues.

In this section, you can find the vendor-specific network prevention signatures to defend against exploits and tools used by HAFNIUM to target Microsoft Exchange Servers. The vendor and product names are given in the below list, but detailed information about these signatures is published in Picus Labs' Github repository.

- Check Point NGFW
- Cisco Firepower
- F5 BigIP ASM
- Forcepoint NGFW
- Fortinet AV, IPS, WAF, WEB
- McAfee NSP
- Palo Alto Networks NGFW
- Snort IPS

Indicators of Compromise

Targeted File Paths

During authentication bypass, the threat actors send HTTP POST requests to image (.gif), JavaScript (.js), cascading style sheet (.css), and font (ttf, eot) files used by Outlook Web Access (OWA). The following table shows the list of known file paths targeted by the POST requests:

Folder	Files
/owa/auth/Current/themes/resources/	lgnbotl.gif, lgnbotl.gif, logon.css, owafont_ja.css, owafont_ko.css, SegoeUI-SemiBold.eot, SegoeUI-SemiLight.ttf
/ecp/	Default.flt, main.css, <single char>.js

User-agents

Adversaries used the following “non-standard” user-agents in POST requests:

User-Agent
antSword/v2.1
DuckDuckBot/1.0;+(+http://duckduckgo.com/duckduckbot.html)
ExchangeServicesClient/0.0.0.0
facebookexternalhit/1.1+(+http://www.facebook.com/externalhit_uatext.php)
Googlebot/2.1+(+http://www.googlebot.com/bot.html)
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
python-requests/2.19.1
python-requests/2.25.1

Web Shells

Adversaries upload web shells to the following paths. Bear in mind that there may be other web shells with different file names in these folders. So, search for any new or modified ASPX files in these folders and their subfolders.

Folder	Web Shell Files
\<exchange_install_path>\FrontEnd\HttpProxy\owa\auth\	8Lw7tAhF9i1pJnRo.aspx, a.aspx, authhead.aspx, bob.aspx, default.aspx, errorPage.aspx, errorPages.aspx, fatal-erro.aspx, log.aspx, logg.aspx, logout.aspx, one.aspx, one1.aspx, OutlookZH.aspx, shel.aspx, shel2.aspx, shel90.aspx.
\<exchange_install_path>\FrontEnd\HttpProxy\owa\auth\current\	one1.aspx
\<exchange_install_path>\FrontEnd\HttpProxy\OAB	log.aspx
\inetpub\wwwroot\aspnet_client\	aspnet_client.aspx, aspnet_iisstart.aspx, aspnet_pages.aspx, aspnet_www.aspx, default1.aspx, discover.aspx, errorcheck.aspx, HttpProxy.aspx, iispage.aspx, OutlookEN.aspx, s.aspx, Server.aspx, session.aspx, shell.aspx, supp0rt.aspx, xclkmcfldfi948398430fdjkfdkj.aspx, xx.aspx
\inetpub\wwwroot\aspnet_client\system_web\	log.aspx
\<exchange_install_path>\FrontEnd\HttpProxy\ecp\auth\	log.aspx

Command and Control IP Addresses

Connected IP Addresses
103.77.192.219
104.140.114.110
104.250.191.110
108.61.246.56

149.28.14.163
157.230.221.198
167.99.168.251
185.250.151.72
192.81.208.169
203.160.69.66
211.56.98.146
5.254.43.18
80.92.205.81

SHA256 Hashes of Web Shells

SHA256 Hashes
511df0e2df9bfa5521b588cc4bb5f8c5a321801b803394ebc493db1ef3c78fa1
b75f163ca9b9240bf4b37ad92bc7556b40a17e27c2b8ed5c8991385fe07d17d0
4edc7770464a14f54d17f36dc9d0fe854f68b346b27b35a6f5839adf1f13f8ea
811157f9c7003ba8d17b45eb3cf09bef2cecd2701cedb675274949296a6a183d
65149e036fff06026d80ac9ad4d156332822dc93142cf1a122b1841ec8de34b5
b75f163ca9b9240bf4b37ad92bc7556b40a17e27c2b8ed5c8991385fe07d17d0
097549cf7d0f76f0d99edf8b2d91c60977fd6a96e4b8c3c94b0b1733dc026d3e
2b6f1ebb2208e93ade4a6424555d6a8341fd6d9f60c25e44afe11008f5c1aad1

65149e036fff06026d80ac9ad4d156332822dc93142cf1a122b1841ec8de34b5
511df0e2df9bfa5521b588cc4bb5f8c5a321801b803394ebc493db1ef3c78fa1
4edc7770464a14f54d17f36dc9d0fe854f68b346b27b35a6f5839adf1f13f8ea
811157f9c7003ba8d17b45eb3cf09bef2cecd2701cedb675274949296a6a183d
1631a90eb5395c4e19c7dbcbf611bbe6444ff312eb7937e286e4637cb9e72944

References:

[1] MSRC Team, “Multiple Security Updates Released for Exchange Server – updated March 8, 2021.” https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server/.

[2] Microsoft Threat Intelligence Center (MSTIC), Microsoft 365 Defender Threat Intelligence Team, and Microsoft 365 Security, “HAFNIUM targeting Exchange Servers with 0-day exploits,” 02-Mar-2021. https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/.

[3] “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/.

[4] “Cyber-attack on the European Banking Authority - European Banking Authority,” 07-Mar-2021. https://www.eba.europa.eu/cyber-attack-european-banking-authority.

[5] “Please leave an exploit after the beep.” https://www.dubex.dk/aktuelt/nyheder/please-leave-an-exploit-after-the-beep.

[6] MSRC Team, “Microsoft Exchange Server Vulnerabilities Mitigations – updated March 6, 2021.” https://msrc-blog.microsoft.com/2021/03/05/microsoft-exchange-server-vulnerabilities-mitigations-march-2021/.

[7] “Security Update Guide - Microsoft Security Response Center.” https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26855.

[8] “Security Update Guide - Microsoft Security Response Center.” https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26857.

[9] “Security Update Guide - Microsoft Security Response Center.” https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26858.

[10] “Security Update Guide - Microsoft Security Response Center.” https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-27065.

[11] “Reconnaissance.” https://attack.mitre.org/tactics/TA0043/.

[12] “Gather Victim Host Information: Software.” https://attack.mitre.org/techniques/T1592/002/.

[13] “Resource Development.” https://attack.mitre.org/tactics/TA0042/.

[14] “Acquire Infrastructure: Virtual Private Server.” https://attack.mitre.org/techniques/T1583/003/.

[15] “Obtain Capabilities: Tool.” https://attack.mitre.org/techniques/T1588/002/.

[16] S. Özarslan, “MITRE ATT&CK T1003 Credential Dumping.” https://www.picussecurity.com/resource/blog/picus-10-critical-mitre-attck-techniques-t1003-credential-dumping.

[17] S. Özarslan, “MITRE ATT&CK T1086 PowerShell.” https://www.picussecurity.com/resource/blog/picus-10-critical-mitre-attck-techniques-t1086-powershell.

[18] besimorhino, “besimorhino/powercat.” https://github.com/besimorhino/powercat.

[19] markruss, “PsExec - Windows Sysinternals.” https://docs.microsoft.com/en-us/sysinternals/downloads/psexec.

[20] S. Özarslan, “How to Beat Nefilim Ransomware Attacks.” https://www.picussecurity.com/resource/blog/how-to-beat-nefilim-ransomware-attacks.

[21] S. Özarslan, “The Ransomware Resurgence Led By LockerGoga.” https://www.picussecurity.com/resource/blog/locker-goga.

[22] cobbr, “cobbr/Covenant.” https://github.com/cobbr/Covenant.

[23] “China Chopper.” https://attack.mitre.org/software/S0020/.

[24] SecureWorks Counter Threat Unit Threat Intelligence, “Threat Group-3390 Targets Organizations for Cyberespionage.” https://www.secureworks.com/research/threat-group-3390-targets-organizations-for-cyberespionage.

[25] “Initial Access.” https://attack.mitre.org/tactics/TA0001/.

[26] “Exploit Public-Facing Application.” https://attack.mitre.org/techniques/T1190/.

[27] “China Chopper.” https://attack.mitre.org/software/S0020/.

[28] “Persistence.” https://attack.mitre.org/tactics/TA0003/.

[29] “Server Software Component: Web Shell.” https://attack.mitre.org/techniques/T1505/003/.

[30] S. Özarslan, “MITRE ATT&CK T1036 Masquerading.” https://www.picussecurity.com/resource/blog/picus-10-critical-mitre-attck-techniques-t1036-masquerading.

[31] “Lateral Movement.” https://attack.mitre.org/tactics/TA0008/.
[32] “Remote Services: SMB/Windows Admin Shares.” https://attack.mitre.org/techniques/T1021/002/.

[33] “Archive Collected Data: Archive via Utility.” https://attack.mitre.org/techniques/T1560/001/.

[34] “Email Collection: Remote Email Collection.” https://attack.mitre.org/techniques/T1114/002/.

[35] “Command and Control.” https://attack.mitre.org/tactics/TA0011/.

[36] “Application Layer Protocol: Web Protocols.” https://attack.mitre.org/techniques/T1071/001/.