REASEARCH ON MS EXCHANGE EXPLOITATION

CVE-2021-26855

CVE-2021-26857

CVE-2021-26858

CVE-2021-27065

B.G Maduranga Chandrasena

MS19810874

INTRODUCTION

On March 2, 2021, Microsoft delivered four out-of-band security reports. The typical justification for delivering an out-of-band update is the presence of dynamic and boundless abuse of a 0-day attack. For this situation, these updates address a 0-day attack influencing Microsoft Exchange Server items that permit dangerous threat actors to peruse valuable data in E-mails, assume responsibility for the objective worker, gather and exfiltrate information from the target system.

The dangerous bunch that abuses Microsoft Exchange Server weaknesses is named HAFNIUM by Microsoft [2] and the assault crusade is named Operation Exchange Marauder by Volexity [3]. Albeit the HAFNIUM danger bunch principally targets protection, advanced education, and wellbeing areas in the United States, these zero-days influence unpatched Microsoft Exchange Servers around the world. For instance, The European Banking Authority (EBA) has declared that it has been the subject of a digital assault against its Microsoft Exchange Servers [4]. As another model, an occurrence because of these weaknesses is accounted for in Denmark [5].

WHAT IS HAFNIUM?

HAFNIUM targets many institutions in the United States across various industry areas, including infectious disease research, law offices, advanced education foundations, Security contractors, strategic thought groups, and NGOs.

Hafnium is a newly identified cyber attack group that is thought to be responsible for other attacks on servers connected to the Internet, they used open-source framework like Covenant & gained access to victim systems, after that usually uploading data to data exchange sites like MEGA. The group is believed to be in China (which is difficult to attribute, especially according to international intelligence and many security researchers who find them difficult to locate).

This research paper consists of Procedures and Techniques used by the HAFNIUM attackers to comprehend their assault strategies and the effect of this exchange security attack campaign.

IDENTIFIED VULNERABILITY

- **CVE-2021-26855 [7]:-** Get full access to MAILBOXES and read their contents
  Vulnerability Type:- Server Side Request Forgey

- **CVE-2021-26857 [8]:-** Discretionary code execution as SYSTEM account, attack to the system
  Vulnerability Type:- Insecure Deserialization

- **CVE-2021-26858 [9]:-** Discretionary code execution as SYSTEM account, attack to the system
  Vulnerability Type:- Post Authentication Arbitrary File Write

- **CVE-2021-27065 [10]:-** Discretionary code execution as SYSTEM account, attack to the system.
  Vulnerability Type:- Post Authentication Arbitrary File Write

IMPACTED PRODUCTS & VERSIONS

- **Exchange 2019/2016/2013** are affected by aforesaid all CVEs and mitigation technique stated as to immediately apply the updates
- **Exchange 2010** affected only from CVE-2021-26857 and deploying exchange update is the mitigation technique.
- **Exchange 2007/2003** are outdated products and Microsoft no longer provides support for those products[1]. Mitigation techniques are stated to update the current exchange servers to the supported version.
- **Office 365 is** not affected by these CVEs.

ANALYSIS

HAFNIUM utilizes eleven of fourteen strategies in the MITRE ATT&CK structure. Below are the tactics that are used by the HAFNIUM.

1. **Reconnaissance**

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

Attackers have gathered information about the MS Exchange server. They looked at whether the server runs MS Exchange server or not. If there is such a server running, they collect information about version [1] and installed other software that may be applied for targeting.

2. **Resource Development**

In these tactics, HAFNIUM attackers include techniques to build, buy or compromise information assets, like accounts or capabilities[13]. HAFNIUM builds these assets before attacking the client's system and leverage uses them for other stages, like using leased VPS support to rum cmdlets and control.

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

VPSs used by HAFNIUM in the USA to perform their attacking campaign[1] the HAFNIUM hires VPS to prevent them from being pursued[14]. Through VPS services they have taken the opportunity to expedite the provision modification and closure of the infrastructure.

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

The HAFNIUM team used the following tools to hack the MS exchange. These are the tools used for other cyber attacks. They can be usually commercial/ closed or open-source software.

3. **Initial Access**

Technological methods that are threat actors used to the primary level breach of the network, exploiting exposures on internet faced web servers.

3.1. MITRE ATT&CK T1190 Exploit Internet-Facing Softwares

Threat actors used exploitable vulnerabilities in victims web servers to gain host access[17]

HAFNIUM team exploits CVE-2021-26855/ CVE-2021-26857/ CVE-2021-26858/ CVE-2021-27065. They gained initial access to web-facing MS Exchange servers.

4. **Execution**

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

HAFNIUM team used ChinaChopper[18] web shell to execute the command using windows cmd.exe on the victim's server.

5. Persistence

This technique used by the HAFNIUM team to enter to the system to perform tasks like restart the system, credential management, find fetched vulnerabilities[19]

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

HAFNIUMs used web shells, scripts installed on the webserver as a backdoor to constitute persistency on the attacked server[29]. They used SIMPLESHARP, SPORTSBALL, ChinaChopper, AspxSpy.

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

Create domain account on attacked system and they used this to assign privileges and access and allow accesses to use infrastructure.

6. Defense Evasion

To prevent pursued they modified names, locations as real names and locations[20].

6.1. T1036.005 Masquerading: Match Legitimate Name or Location

HAFNIUM modified names of deployed webshells similar to the real names like log.aspx/ logout.aspx/ default.aspx/ errorpage.aspx/ server.aspx

Below are the webshell filename that used by HAFNIUM. (in bold letters it stated the file path & then web shells)

\<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.

\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

7. Credential Access

This is used to steal user credentials (user names and the password)

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

HAFNIUM used LSASS (Local Security Authority Subsystem Services)to steal user names and passwords. This system is used to be store logged user's credentials[16]. They engage with the isass.exe and dump that process and used the procdump tool to dump isassprocess and retrieved user credentials.

7.2. T1003.003 OS Credential Dumping: NTDS

Using web shells HAFNIUM team steals the NTDS.dit file [3]. This is a DB file that active directory stored data and consist of user names, password & password hashes.

8. Lateral Movement

This technique used to manipulate hacked systems[21]

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

Using PsExec (that is genuine windows Sysinternals tool)[3] they run commands on the compromised system.

9. Collection

This consists of how attackers collect the data matched to their objectives.

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

Using data compression software's like WinZip/ 7-zip/ WinRAR to compress data.

HAFNIUM used 7-zip to compress steal data of compromised servers.

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

HAFNIUM accessed internet faced MS Exchange email servers and collect data by valid accounts leveraging access tokens/ exploits of remote tokens[22]

They exported data by adding Exchange PowerShell snap-ins[2].

10. Command and Control

Techniques that used by HAFNIUM to manipulate the systems in compromised victims network[23]

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

HAFNIUM group corresponds with deployed web shells using HTTP/ HTTPS. They utilize these HTTP/ HTTPS protocols to command and control to avoid pursued [24].

11. Exfiltration

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

HAFNIUMs may extract data and uploaded them to cloud storage sites like MEGA.io[2]

VENDOR-SPECIFIC PREVENTIONS

Below are some vender specific signatures against the HAFNIUM exploits and tools[24]

Major vendors are Check Point NGFW, Cisco Firepower, F5 BigIP ASM, Forcepoint NGFW, Fortinet AV/IPS/WAF/ WEB, McAfee NSP, Palo Alto Networks NGFW.

ThreatId:-

Name:- Backdoor used by HAFNIUM Threat Group .HTML File Download Variant-1

Signature ID :- 0A097FBC9

Signature Name:- Trojan.ASP.Agent.bh.TC.b

Engine:- TP

Vendor:- Checkpoint

ThreatId:-

Name:- Backdoor used by HAFNIUM Threat Group .HTML File Download Variant-1

Signature ID :- 10007108

Signature Name:- HTML/Agent.A121!tr

Engine:- virus

Vendor:- Fortigate

ThreatId:- CVE-2021-26855

Name:- Microsoft Exchange Server Unauthorized SSRF Vulnerability Variant-2

Signature ID :- 1.57241.4

Signature Name:- SERVER-WEBAPP Microsoft Exchange Server server-side request forgery attempt

Engine:- IPS

Vendor:- Snort

ThreatId:- CVE-2021-26855

Name:- Microsoft Exchange Server Unauthorized SSRF Vulnerability Variant-1

Signature ID :- 0x4528a400

Signature Name:- HTTP: Microsoft Exchange Server Remote Code Execution Vulnerability (CVE-2021-26855)

Engine:- Exploit

Vendor:- Mcafee

ThreatId:-

Name:- Backdoor used by HAFNIUM Threat Group. HTML File Download Variant-1

Signature ID:-

Signature Name:- File_Malware-Blocked

Engine:- FileRep

Vendor:- Forcepoint

TARGETED FILE PATHS.

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

Table 01. Targeted File Paths (Source:-MSRC)

SOLUTION

Microsoft has released security updates addressing these vulnerabilities, it is recommended to apply

these security updates as soon as possible to prevent vulnerability exploitation.

Additionally, Microsoft has released a list of indicators of compromise, it would be recommended

to check for the presence of these indicators and initiate incident response procedures in case they are present on the network.

REFERENCES

[1]M. Team, "On-Premises Exchange Server Vulnerabilities Resource Center – updated March 25, 2021 – Microsoft Security Response Center", Msrc-blog.microsoft.com, 2021. [Online]. Available: https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server/. [Accessed: 24- May- 2021].

[2]"HAFNIUM targeting Exchange Servers with 0-day exploits - Microsoft Security", Microsoft Security, 2021. [Online]. Available: https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/. [Accessed: 05- May- 2021].

[3]"Operation Exchange Marauder: Active Exploitation of Multiple Zero-Day Microsoft Exchange Vulnerabilities | Volexity", Volexity.com, 2021. [Online]. Available: https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/. [Accessed: 07- May- 2021].

[4]"Cyber-attack on the European Banking Authority - European Banking Authority", European Banking Authority, 2021. [Online]. Available:

https://www.eba.europa.eu/cyber-attack-european-banking-authority. [Accessed: 05- May- 2021].

[5]"Please leave an exploit after the beep", Dubex.dk, 2021. [Online]. Available: https://www.dubex.dk/aktuelt/nyheder/please-leave-an-exploit-after-the-beep. [Accessed: 02- May- 2021].

[6]M. Team, "Microsoft Exchange Server Vulnerabilities Mitigations – updated March 15, 2021 – Microsoft Security Response Center", Msrc-blog.microsoft.com, 2021. [Online]. Available: https://msrc-blog.microsoft.com/2021/03/05/microsoft-exchange-server-vulnerabilities-mitigations-march-2021/. [Accessed: 06- May- 2021].

[7]"Security Update Guide - Microsoft Security Response Center", Msrc.microsoft.com, 2021. [Online]. Available: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26855. [Accessed: 06- May- 2021].

[8]"Security Update Guide - Microsoft Security Response Center", Msrc.microsoft.com, 2021. [Online]. Available: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26857. [Accessed: 08- May- 2021].

[9]"Security Update Guide - Microsoft Security Response Center", Msrc.microsoft.com, 2021. [Online]. Available: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26858. [Accessed: 09- May- 2021].

[10]"Security Update Guide - Microsoft Security Response Center", Msrc.microsoft.com, 2021. [Online]. Available: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-27065. [Accessed: 07- May- 2021].

[11]"Reconnaissance, Tactic TA0043 - Enterprise | MITRE ATT&CK®", Attack.mitre.org, 2021. [Online]. Available: https://attack.mitre.org/tactics/TA0043/. [Accessed: 09- May- 2021].

[12]"Gather Victim Host Information: Software, Sub-technique T1592.002 - Enterprise | MITRE ATT&CK®", Attack.mitre.org, 2021. [Online]. Available: https://attack.mitre.org/techniques/T1592/002/. [Accessed: 08- May- 2021].

[13]"Resource Development, Tactic TA0042 - Enterprise | MITRE ATT&CK®", Attack.mitre.org, 2021. [Online]. Available: https://attack.mitre.org/tactics/TA0042/. [Accessed: 11- May- 2021].

[14]"Acquire Infrastructure: Virtual Private Server, Sub-technique T1583.003 - Enterprise | MITRE ATT&CK®", Attack.mitre.org, 2021. [Online]. Available: https://attack.mitre.org/techniques/T1583/003/. [Accessed: 09- May- 2021].

[15]"Obtain Capabilities: Tool, Sub-technique T1588.002 - Enterprise | MITRE ATT&CK®", Attack.mitre.org, 2021. [Online]. Available: https://attack.mitre.org/techniques/T1588/002/. [Accessed: 10- May- 2021].

[16]"MITRE ATT&CK T1003 Credential Dumping", Picussecurity.com, 2021. [Online]. Available: https://www.picussecurity.com/resource/blog/picus-10-critical-mitre-attck-techniques-t1003-credential-dumping?hsLang=en-gb. [Accessed: 07- May- 2021].

[17]"Exploit Public-Facing Application, Technique T1190 - Enterprise | MITRE ATT&CK®", Attack.mitre.org, 2021. [Online]. Available: https://attack.mitre.org/techniques/T1190/. [Accessed: 05- May- 2021].

[18]"China Chopper, Software S0020 | MITRE ATT&CK®", Attack.mitre.org, 2021. [Online]. Available: https://attack.mitre.org/software/S0020/. [Accessed: 10- May- 2021].

[19]"Persistence, Tactic TA0003 - Enterprise | MITRE ATT&CK®", Attack.mitre.org, 2021. [Online]. Available: https://attack.mitre.org/tactics/TA0003/. [Accessed: 10- May- 2021].

[20]"MITRE ATT&CK T1036 Masquerading", Picussecurity.com, 2021. [Online]. Available: https://www.picussecurity.com/resource/blog/picus-10-critical-mitre-attck-techniques-t1036-masquerading?hsLang=en-gb. [Accessed: 10- May- 2021].

[21]"Lateral Movement, Tactic TA0008 - Enterprise | MITRE ATT&CK®", Attack.mitre.org, 2021. [Online]. Available: https://attack.mitre.org/tactics/TA0008/. [Accessed: 24- May- 2021].

[22]"Email Collection: Remote Email Collection, Sub-technique T1114.002 - Enterprise | MITRE ATT&CK®", Attack.mitre.org, 2021. [Online]. Available: https://attack.mitre.org/techniques/T1114/002/. [Accessed: 08- May- 2021].

[23]"Command and Control, Tactic TA0011 - Enterprise | MITRE ATT&CK®", Attack.mitre.org, 2021. [Online]. Available: https://attack.mitre.org/tactics/TA0011/. [Accessed: 10- May- 2021].

[24]"Application Layer Protocol: Web Protocols, Sub-technique T1071.001 - Enterprise | MITRE ATT&CK®", Attack.mitre.org, 2021. [Online]. Available: https://attack.mitre.org/techniques/T1071/001/. [Accessed: 11- May- 2021].