Exchange servers under siege from at least 10 APT groups

By Matthieu FaouThomas DupuyMathieu Tartare

Archived: 2026-04-05 18:57:56 UTC

On 2021-03-02, Microsoft released out-of-band patches for Microsoft Exchange Server 2013, 2016 and 2019. These security updates fixed a pre-authentication remote code execution (RCE) vulnerability chain (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065) that allows an attacker to take over any reachable Exchange server, without even knowing any valid account credentials. We have already detected webshells on more than 5,000 email servers as of the time of writing, and according to public sources, several important organizations, such as the European Banking Authority, suffered from this attack.

ESET customers are advised to read the following articles for information related to ESET products:
A Microsoft Exchange saga: How is ESET technology protecting business customers post-exploitation? (ESET Corporate Blog)
Microsoft Exchange vulnerabilities discovered and exploited in-the-wild (ESET Customer Advisory)
Does ESET protect me from the Hafnium zero-day exploit in Microsoft Exchange? (ESET Knowledgebase)

These vulnerabilities were first discovered by Orange Tsai, a well-known vulnerability researcher, who reported them to Microsoft on 2021-01-05. However, according to a blogpost by Volexity, in-the-wild exploitation had already started on 2021-01-03. Thus, if these dates are correct, the vulnerabilities were either independently discovered by two different vulnerability research teams or that information about the vulnerabilities was somehow obtained by a malicious entity. Microsoft also published a blogpost about the early activity of Hafnium.

On 2021-02-28, we noticed that the vulnerabilities were used by other threat actors, starting with Tick and quickly joined by LuckyMouse, Calypso and the Winnti Group. This suggests that multiple threat actors gained access to the details of the vulnerabilities before the release of the patch, which means we can discard the possibility that they built an exploit by reverse engineering Microsoft updates.

READ NEXT: Prime targets: Governments shouldn't go it alone on cybersecurity

Finally, the day after the release of the patch, we started to see many more threat actors (including Tonto Team and Mikroceen) scanning and compromising Exchange servers en masse. Interestingly, all of them are APT groups interested in espionage, except for one outlier (DLTMiner), which is linked to a known cryptomining campaign. A summary of the timeline is shown in Figure 1.

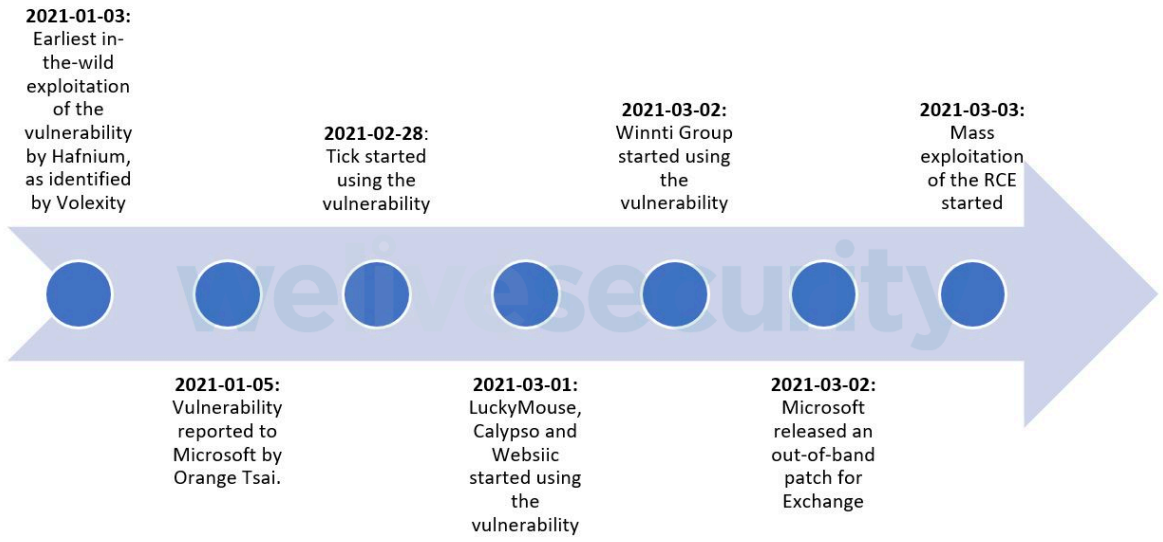

Figure 1. Timeline of important events

Exploitation statistics

For the past few days, ESET researchers have been monitoring closely the number of webshell detections for these exploits. At the date of publication, we had observed more than 5,000 unique servers in over 115 countries where webshells were flagged. These numbers utilize ESET telemetry and are (obviously) not complete. Figure 2 illustrates these detections before and after the patch from Microsoft.

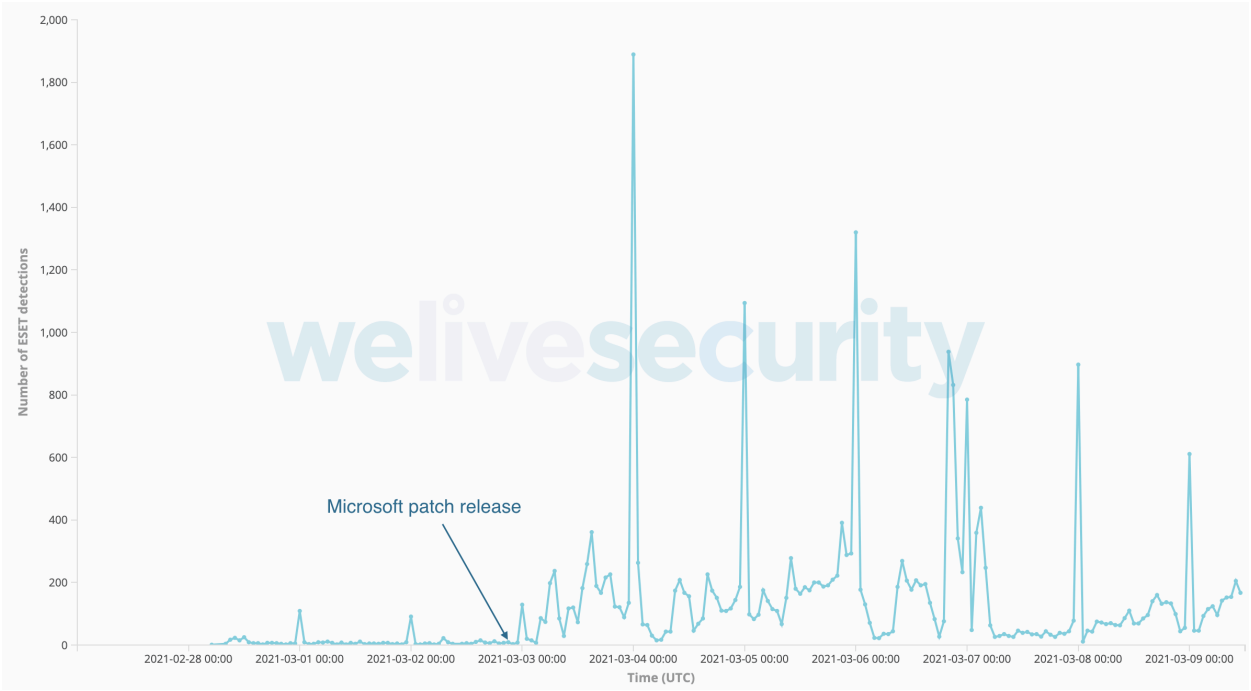

Figure 2. ESET detection of the webshells dropped via CVE-2021-26855 (hourly)

The heatmap in Figure 3 shows the geographical distribution of the webshell detections, according to ESET telemetry. Due to mass exploitation, it is likely that it represents the distribution of vulnerable Exchange servers around the world on which ESET security products are installed.

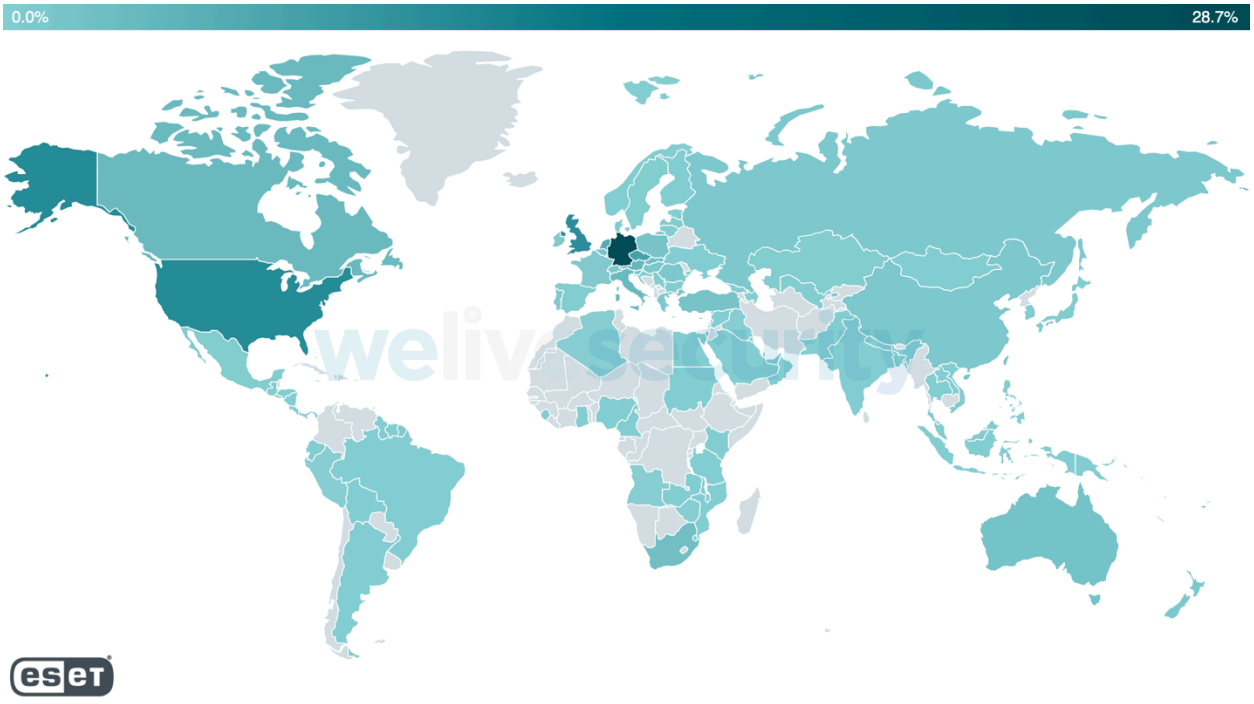

Figure 3. Proportion of webshell detections by country (2021-02-28 to 2021-03-09)

From RCE to webshells to backdoors

We have identified more than 10 different threat actors that likely leveraged the recent Microsoft Exchange RCE in order to install implants on victims' email servers.

Our analysis is based on email servers on which we found webshells in Offline Address Book (OAB) configuration files, which is a specific technique used in the exploitation of the RCE vulnerability and has already been detailed in a Unit 42 blogpost. Unfortunately, we cannot discount the possibility that some threat actors might have hijacked the webshells dropped by other groups rather than directly using the exploit.

Once the vulnerability had been exploited and the webshell was in place, we observed attempts to install additional malware through it. We also noticed in some cases that several threat actors were targeting the same organization.

Tick

On 2021-02-28, Tick (also known as Bronze Butler) compromised the webserver of a company based in East Asia that provides IT services. This means that the group likely had access to the exploit prior to the patch's release – in this case at least two days before.

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

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

We then observed a Delphi backdoor, highly similar to previous Delphi implants used by the group. C&C addresses used by this backdoor are www.averyspace[.]net and www.komdsecko[.]net.

Tick is an APT group active since as early as 2008 and targeting organizations primarily based in Japan but also in South Korea, Russia and Singapore amongst others. Its main objective seems to be intellectual property and classified information theft. It makes use of various proprietary malware such as Daserf, xxmm and Datper as well as open source RATs such as

Lilith. Tick is among the APT groups now having access to the ShadowPad backdoor, which was used during Operation ENTRADE documented by Trend Micro.

LuckyMouse

On 2021-03-01, LuckyMouse compromised the email server of a governmental entity in the Middle East, which means this APT group likely had access to the exploit at least one day before the patch release, when it was still a zero day.

LuckyMouse operators started by dropping the Nbtscan tool in C:\programdata\, then installed a variant of the ReGeorg webshell and issued a GET request to http://34.90.207[.]23/ip using curl. Finally, they attempted to install their SysUpdate (aka Soldier) modular backdoor that uses the aforementioned IP address as its C&C server.

LuckyMouse, also known as APT27 and Emissary Panda, is a cyberespionage group known to have breached multiple government networks in Central Asia and the Middle East but also transnational organizations such as International Civil Aviation Organization (ICAO) in 2016. It uses various custom malware families such as HyperBro and SysUpdate.

Calypso

On 2021-03-01, Calypso compromised the email servers of governmental entities in the Middle East and in South America, which means the group likely had access to the exploit as a zero day, like LuckyMouse and Tick. In the following days, Calypso operators targeted additional servers of governmental entities and private companies in Africa, Asia and Europe using the exploit.

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

As part of these attacks, two different backdoors were observed: a variant of PlugX specific to the group (Win32/Korplug.ED) and a custom backdoor that we detect as Win32/Agent.UFX (known as Whitebird in a Dr.Web report). These tools are loaded using DLL search-order hijacking against legitimate executables (also dropped by the attackers):

- netcfg.exe (SHA-1: 1349EF10BDD4FE58D6014C1043CBBC2E3BB19CC5) using a malicious DLL named netcfg.dll (SHA-1: EB8D39CE08B32A07B7D847F6C29F4471CD8264F2)
- CLNTCON.exe (SHA-1: B423BEA76F996BF2F69DCC9E75097635D7B7A7AA) using a malicious DLL named SRVCON.OCX (SHA-1: 30DD3076EC9ABB13C15053234C436406B88FB2B9)
- iPAQDetetion2.exe (SHA-1: C5D8FEC2C34572F5F2BD4F6B04B75E973FDFEA32) using a malicious DLL named rapi.dll (SHA-1: 4F0EA31A363CFE0D2BBB4A0B4C5D558A87D8683E)

The backdoors were configured to connect to the same C&C servers: yolkish[.]com and rawfuns[.]com.

Finally, we also observed a variant of a tool known as Mimikat_ssp that is available on GitHub.

Calypso (which is also tied to XPATH) is a cyberespionage group targeting governmental institutions in Central Asia, the Middle East, South America and Asia. Its main implant is a variant of the PlugX RAT.

Websiic

Starting 2021-03-01, ESET researchers observed a new cluster of activity we have named Websiic, targeting seven email servers belonging to private companies (in the domains of IT, telecommunications and engineering) in Asia and a governmental body in Eastern Europe. As observed in the cases above, the operators behind this cluster likely had access to the exploit before the patch's release.

This cluster was identified by the presence of a loader as its first stage, generally named google.log or google.aspx, and an encrypted configuration file, generally named access.log. The loader stops a specific service identified in the config and creates a new entry under the Windows service registry HKLM\SYSTEM\CurrentControlSet\Services\<servicename>\Parameters (the service's filename is provided by the config). It sets two keys ServiceDll and ServiceMain. The first one contains the path to a DLL while the latter contains the export to call (INIT in this case). Finally, it restarts the service that was stopped at the outset.

While the loader was deployed on all victims from this cluster, the second stage (also a loader) was observed on the computer of only one of the victims and was located in C:\Program Files\Common Files\microsoft shared\WMI\iiswmi.dll. The DLL has an export named INIT that contains the main logic and uses the same XOR encryption loop as well as the same technique to dynamically resolve the Windows API names as seen in the first stage. It loads the following DLL %COMMONPROGRAMFILES%\System\websvc.dll with an argument extracted from the registry key HKLM\SOFTWARE\Classes\Interface\{6FD0637B-85C6-D3A9-CCE9-65A3F73ADED9}. Unfortunately, the lack of indicators matching previously known threat actors prevents us from drawing any conclusions or a reasonable hypothesis as to the group behind these attacks.

Seven victims were flagged by the presence of the first loader and at one of them, the second loader was identified. We have not currently tied any known threat actor to Websiic. A recent article from GTSC also briefly describes the same cluster.

Winnti Group

Starting 2021-03-02, a few hours before Microsoft released the patch, the Winnti Group (also known as BARIUM or APT41) compromised the email servers of an oil company and a construction equipment company both based in East Asia. This indicates that this APT group also had access to the exploit prior to the patch release.

The attackers started by dropping webshells at the following locations, depending on the victim:

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

At one of the compromised victims we observed a PlugX RAT sample (also known as Korplug) with C&C domain mm.portomnail[.]com and back.rooter.tk. Note that mm.portomnail[.]com was previously used by the Winnti Group with ShadowPad and the Winnti malware. On the same machine, during the same timeframe, we also observed some malware, not yet fully analyzed, using 139.162.123[.]108 as its C&C address but at the time of writing we don't know whether this is related to the Exchange compromise or not.

At the second victim, we observed a loader that is highly similar to previous Winnti v4 malware loaders such as that mentioned in our white paper on the arsenal of the Winnti Group. Like that Winnti v4 loader, this loader is used to decrypt an encrypted payload from disk and execute it using the following command:

srv64.exe <Decryption_Key> <Encrypted_Payload_Filename>

where <Decryption_key> is the decryption key used to decrypt the payload stored in <Encrypted_Payload_Filename>. Once executed, this loader drops a malicious DLL at the following location:

C:\Windows\system32\oci.dll

This malicious DLL shares multiple similarities with a previous Winnti implant documented by Trend Micro as well as the Spyder backdoor recently documented by DrWeb and that we have observed being used by the Winnti Group in the past. The C&C address used by this implant is 161.129.64[.]124:443.

Additionally, we observed various Mimikatz and password dumping tools.

The Winnti Group, active since at least 2012, is responsible for high-profile supply-chain attacks against the video game and software industries, leading to the distribution of trojanized software (such as CCleaner, ASUS LiveUpdate and multiple video games) that is then used to compromise more victims. It is also known for having compromised various targets in multiple different verticals such as healthcare and education.

Tonto Team

On 2021-03-03, Tonto Team (also known as CactusPete) compromised the email servers of a procurement company and of a consulting company specialized in software development and cybersecurity, both based in Eastern Europe.

In that case, the attacker used C:\inetpub\wwwroot\aspnet_client\dukybySSSS.aspx for the first-stage webshell.

The attacker then used PowerShell to download their payloads from 77.83.159[.]15. Those payloads consist of a 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 C&C address being used by ShadowPad here is lab.symantecsafe[.]org and the communication protocol is HTTPS.

In addition to ShadowPad, the attacker also made use of a variant of the Bisonal RAT highly similar to a Bisonal variant that was previously used during Operation Bitter Biscuit attributed to Tonto Team.

On one of the compromised machines, the attacker used an LSAS dumper that was also previously used by Tonto Team.

Tonto Team is an APT group active since at least 2009 and targeting governments and institutions mostly based in Russia, Japan and Mongolia. For more than ten years, Tonto Team has been using the Bisonal RAT. Tonto Team is one of the APT groups that now has access to the ShadowPad backdoor.

Unattributed ShadowPad activity

Starting 2021-03-03, we observed the compromise of email servers at a software development company based in East Asia and a real estate company based in the Middle East where ShadowPad was dropped by the attacker and that we were not able to conclusively attribute to any known groups at the time of writing.

The attackers used C:\inetpub\wwwroot\aspnet_client\discover.aspx and C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\RedirSuiteServerProxy.aspx as first-stage webshells and dropped ShadowPad at the following locations:

- C:\Windows\Help\mui\0109\mscoree.dll
- C:\mscoree.dll

One of the ShadowPad samples uses soft.mssysinfo[.]xyz as its C&C address using the HTTPS protocol while the second sample uses ns.rtechs[.]org using the DNS protocol, which is less common.

The ShadowPad backdoor is a modular backdoor that was exclusive to the Winnti Group until the end of 2019. To the best of our knowledge, ShadowPad is now used by at least five additional groups: Tick, Tonto Team, KeyBoy, IceFog and TA428.

The “Opera” Cobalt Strike

On 2021-03-03 at 04:23 AM UTC, just a few hours after the patch was released, we noticed that another set of malicious activities had started. At this point we don’t know if these threat actors had access to the exploit beforehand or reverse engineered the patch. This corresponds to indicators that were published on Twitter and by FireEye, but we haven’t been able to link this set to any group we are already tracking.

From 2021-03-03 to 2021-03-05, ESET telemetry shows this activity targeting around 650 servers, mostly in the US, Germany, the UK and other European countries. Interestingly, this threat actor was consistent in the naming and location of their first-stage webshell, always using <Exchange_install_directory>\FrontEnd\HttpProxy\owa\auth\RedirSuiteServerProxy.aspx.

Then on a few selected machines, they executed a PowerShell script, shown in Figure 4, to download additional components from 86.105.18[.]116. The final payload is Cobalt Strike, which uses the same IP address for its C&C server. Cobalt Strike is loaded via DLL search-order hijacking against a legitimate Opera executable named opera_browser.exe (SHA-1: AB5AAA34200A3DD2276A20102AB9D7596FDB9A83) using a DLL named opera_browser.dll (SHA-1: 02886F9DAA13F7D9855855048C54F1D6B1231B0A) that decrypts and loads a shellcode from opera_browser.png (SHA-1: 2886F9DAA13F7D9855855048C54F1D6B1231B0A). We noticed that 89.34.111[.]11 was also used to distribute malicious files.

Figure 4. PowerShell script used to download Cobalt Strike

IIS backdoors

Starting 2021-03-03, we observed that on four email servers located in Asia and South America, webshells were used to install so-called IIS backdoors.

We identified two different malware families:

- 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 as part of several incidents against Taiwanese governmental agencies.

Mikroceen

On 2021-03-04, the Mikroceen APT group compromised the Exchange server of a utility company in Central Asia, which is the region it mainly targets.

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 and C:\inetpub\wwwroot\aspnet_client\log_error_9e23efc3.aspx. Then, they downloaded a payload we could not recover from http://46.30.188[.]60/webengine4.dll. We were not able to tie those first steps to Mikroceen with high confidence, but these indicators appeared only on the specific server where we saw the Mikroceen backdoors a few hours after.

A few hours later, a Mikroceen RAT was dropped in C:\Users\Public\Downloads\service.exe. Its C&C server is 172.105.18[.]72. Then, this RAT dropped additional tools such as Mimikatz (in C:\users\public\alg.exe), Mimikat_ssp (in

C:\users\public\Dump.exe) and a custom proxy (in c:\Users\Public\calcx.exe). The latter was executed with the following command line (exposing another attacker-controlled IP address):

calcx.exe 300 194.68.44[.]19 c:\users\public\1.log <private IP>:3128

The Mikroceen APT group (aka Vicious Panda) is a threat actor operating since at least 2017. It mainly targets governmental institutions and telcos in Central Asia, Russia and Mongolia. It uses a custom backdoor we've named Mikroceen RAT.

DLTMiner

Starting 2021-03-05 at 02:53 AM UTC, we detected the deployment of PowerShell downloaders on multiple email servers that were previously targeted using these Exchange vulnerabilities.

The first PowerShell script downloads the next stage at the following address http://p.estonine[.]com/p?e. Previous articles from 2019 show similarities between this cluster and a cryptominer campaign. More details about the analysis can be found in Tencent and Carbon Black blogposts. A more recent Twitter post describes the various compromise steps.

We were unable to find any correlation in terms of webshells deployed on these servers. It is possible that this group is hijacking webshells previously installed by other threat groups.

Summary

Our ongoing research shows that not only Hafnium has been using the recent RCE vulnerability in Exchange, but that multiple APTs have access to the exploit, and some even did so prior to the patch release. It is still unclear how the distribution of the exploit happened, but it is inevitable that more and more threat actors, including ransomware operators, will have access to it sooner or later.

It is now clearly beyond prime time to patch all Exchange servers as soon as possible (see Microsoft guidance and apply special care in following the steps in the “About installation of these updates” section). Even those not directly exposed to the internet should be patched because an attacker with low, or unprivileged, access to your LAN can trivially exploit these vulnerabilities to raise their privileges while compromising an internal (and probably more sensitive) Exchange server, and then move laterally from it.

In case of compromise, one should remove webshells, change credentials and investigate for any additional malicious activity.

Finally, this is a very good reminder that complex applications such as Microsoft Exchange or SharePoint should not be open to the internet since, in case of mass exploitation, it is very hard, if not impossible, to patch in time.

For any inquiries, or to make sample submissions related to the subject, contact us at: threatintel@eset.com.

Indicators of Compromise (IoCs)

A plaintext list of Indicators of Compromise (IoCs) and a MISP event can be found in our GitHub repository.

Webshells

ESET detects the webshells used in these attacks as JS/Exploit.CVE-2021-26855.Webshell.A and JS/Exploit.CVE-2021-26855.Webshell.B.

The ASPX webshells are typically placed in these folders, using a large variety of filenames:

- C:\inetpub\wwwroot\aspnet_client\system_web\
- <Exchange install directory>\FrontEnd\HttpProxy\owa\auth\Current\themes\resources\
- <Exchange install directory>\FrontEnd\HttpProxy\owa\auth\

Malware files

SHA-1	ESET detection name	Details
30DD3076EC9ABB13C15053234C436406B88FB2B9	Win32/Korplug.RT	Calypso loader for Win32/Korplug.ED
EB8D39CE08B32A07B7D847F6C29F4471CD8264F2	Win32/Korplug.RU	Calypso loader for Win32/Korplug.ED
4F0EA31A363CFE0D2BBB4A0B4C5D558A87D8683E	Win32/Agent.ACUS	Calypso loader for Win32/Agent.UFX
2075D8E39B7D389F92FD97D97C41939F64822361	Win64/HackTool.Mimikat.A	Mimikat_ssp used by Calypso
02886F9DAA13F7D9855855048C54F1D6B1231B0A	Win32/Agent.ACUQ	Opera Cobalt Strike loader
123CF9013FA73C4E1F8F68905630C8B5B481FCE7	Win64/Mikroceen.AN	Mikroceen RAT
B873C80562A0D4C3D0F8507B7B8EC82C4DF9FB07	Win64/HackTool.Mimikat.A	Mimikat_ssp used by Mikroceen
59C507BCBEFCA2E894471EFBCD40B5AAD5BC4AC8	Win32/HackTool.Proxy.A	Proxy used by Mikroceen
3D5D32A62F770608B6567EC5D18424C24C3F5798	Win64/Kryptik.CHN	ShadowPad backdoor used by Tonto Team
AF421B1F5A08499E130D24F448F6D79F7C76AF2B	Win64/Riskware.LsassDumper.J	LSASS dumper used by Tonto Team
1DE8CBBF399CBC668B6DD6927CFEE06A7281CDA4	Win32/Agent.ACGZ	PlugX injector used by the Winnti Group
B8D7B850DC185160A24A3EE43606A9EF41D60E80	Win64/Winnti.DA	Winnti loader
33C7C049967F21DA0F1431A2D134F4F1DE9EC27E	Win64/HackTool.Mimikat.A	Mimikatz used by the Winnti Group
A0B86104E2D00B3E52BDA5808CCEED9842CE2CEA	Win64/HackTool.Mimikat.A	Mimikatz used by the Winnti Group
281FA52B967B08DBC1B51BAFBFBF7A258FF12E54	Win32/PSWTool.QuarksPwDump.E	Password dumper used by the Winnti Group

SHA-1	ESET detection name	Details
46F44B1760FF1DBAB6AAD44DEB1D68BEE0E714EA	Win64/Shadowpad.E	Unattributed ShadowPad
195FC90AEE3917C94730888986E34A195C12EA78	Win64/Shadowpad.E	Unattributed ShadowPad
29D8DEDCF19A8691B4A3839B805730DDA9D0B87C	PowerShell/TrojanDownloader.Agent.CEK	DLTMiner
20546C5A38191D1080B4EE8ADF1E54876BEDFB9E	PowerShell/TrojanDownloader.Agent.CEK	DLTMiner
84F4AEAB426CE01334FD2DA3A11D981F6D9DCABB	Win64/Agent.AKS	Websiic
9AFA2AFB838CAF2748D09D013D8004809D48D3E4	Win64/Agent.AKS	Websiic
3ED18FBE06D6EF2C8332DB70A3221A00F7251D55	Win64/Agent.AKT	Websiic
AA9BA493CB9E9FA6F9599C513EDBCBEE84ECECD6	Win64/Agent.IG	IIS Backoor

C&C servers

IP address / domain	Details
34.90.207[.]23	LuckyMouse SysUpdate C&C server
yolkish[.]com	Calypso C&C server
rawfuns[.]com	Calypso C&C server
86.105.18[.]116	“Opera Cobalt Strike” C&C & distribution server
89.34.111[.]11	“Opera Cobalt Strike” distribution server
172.105.18[.]72	Mikroceen RAT C&C server
194.68.44[.]19	Mikroceen proxy C&C server
www.averyspace[.]net	Tick Delphi backdoor C&C server
www.komdsecko[.]net	Tick Delphi backdoor C&C server
77.83.159[.]15	Tonto Team distribution server
lab.symantecsafe[.]org	Tonto Team ShadowPad C&C server
mm.portomnail[.]com	Winnti Group PlugX C&C server
back.rooter[.]tk	Winnti Group PlugX C&C server
161.129.64[.]124	Winnti malware C&C server
ns.rtechs[.]org	Unclassified ShadowPad C&C server
soft.mssysinfo[.]xyz	Unclassified ShadowPad C&C server
p.estonine[.]com	DLTMiner C&C server

MITRE ATT&CK techniques

Note 1: This table was built using version 8 of the MITRE ATT&CK framework.

Note 2: This table includes techniques covering the exploitation of the vulnerability and the webshell's deployment.

Tactic	ID	Name	Description
Reconnaissance	T1595	Active Scanning	Attackers are scanning the internet in order to find vulnerable Microsoft Exchange servers.
Resource Development	T1587.004	Develop Capabilities: Exploits	Attackers developed or acquired exploits for CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065.
Initial Access	T1190	Exploit Public-Facing Application	Attackers exploited vulnerabilities in Microsoft Exchange 2013, 2016 and 2019 (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065) to gain a foothold on the email servers.
Execution	T1203	Exploitation for Client Execution	Attackers exploited vulnerabilities in Microsoft Exchange 2013, 2016 and 2019 (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065) to drop an ASPX webshell on the compromised email servers.
Persistence	T1505.003	Server Software Component: Web Shell	Attackers installed China Chopper ASPX webshells in IIS or Exchange folders reachable from the internet.
