Rapid7's InsightIDR Enables Detection And Response to Microsoft Exchange Zero-Day

blog.rapid7.com/2021/03/03/rapid7s-insightidr-enables-detection-and-response-to-microsoft-exchange-0-day

Andrew Christian March 3, 2021

Last updated at Thu, 18 Mar 2021 13:34:41 GMT

Starting February 27, 2021, Rapid7 has observed a notable increase in the exploitation of Microsoft Exchange through existing detections in InsightIDR's Attacker Behavior Analytics (ABA). The Managed Detection and Response (MDR) identified multiple, related compromises in the past 72 hours. In most cases, the attacker is uploading an "eval" webshell, commonly referred to as a "chopper" or "China chopper". With this foothold, the attacker would then upload and execute tools, often for the purpose of stealing credentials. Further investigative efforts have identified overlap in attacker techniques and infrastructure.

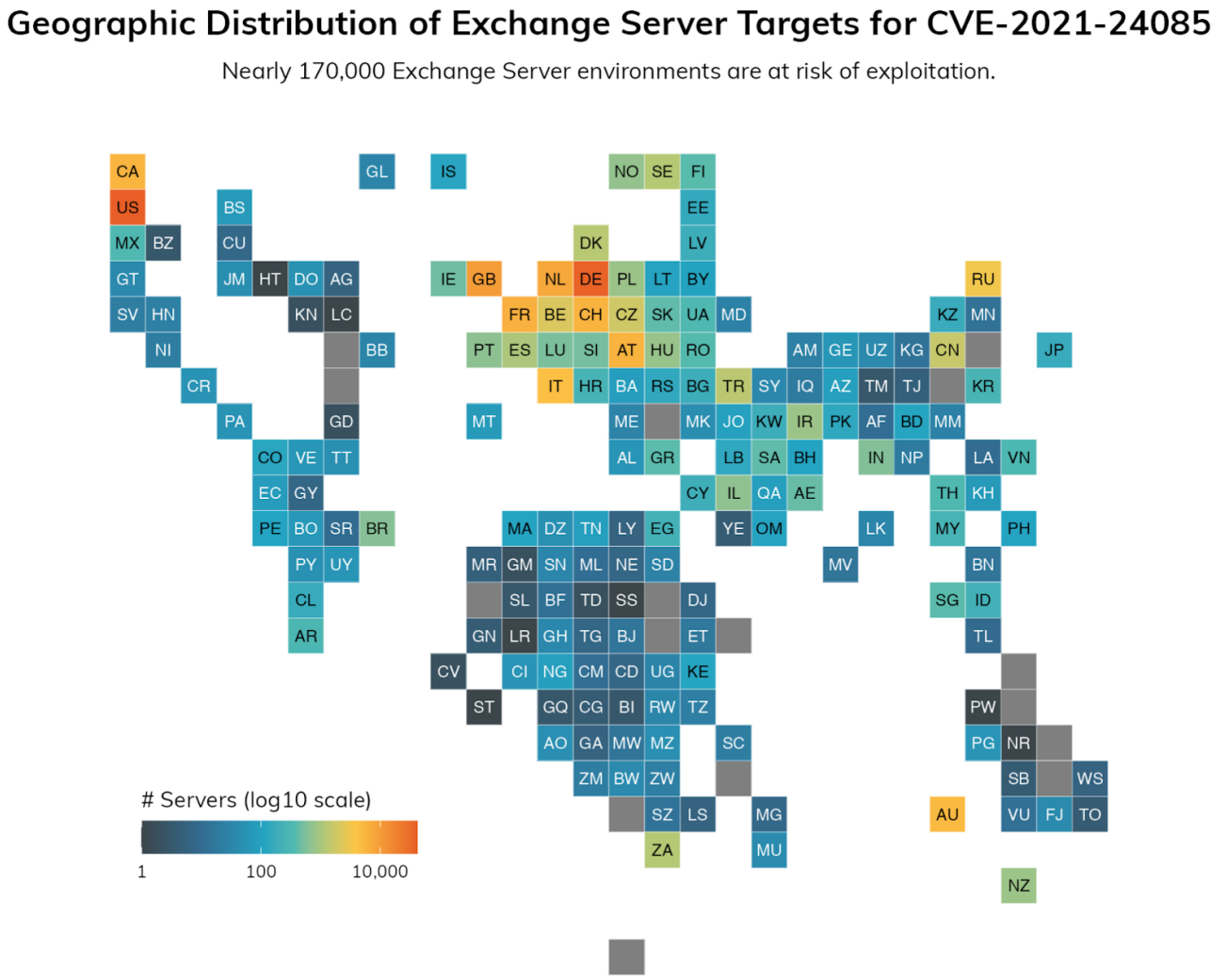
Summary

At close to midnight UTC on February 27, 2021, Managed Detection and Response SOC analysts began observing alerts for the following ABA detections in InsightIDR:

- Attacker Tool - China Chopper Webshell Executing Commands
- Attacker Technique - ProcDump Used Against LSASS

Upon further inspection of Enhanced Endpoint Telemetry data produced by InsightAgent, Rapid7 analysts identified that attackers had successfully compromised several systems and noted that they were all on-premise Microsoft Exchange servers with web services accessible to the public Internet. Exposing web services to the public internet is a common practice for customers with on-premise instances of Microsoft Exchange to provide their users with email services over the web through Outlook Web Access (OWA).

Using Project Sonar, Rapid7's Labs team was able to identify how target-rich an environment attackers have to work with: Nearly 170,000 servers vulnerable to a different recent Exchange CVE (for which proof-of-concept exploit code is readily available) were exposed to the public internet.



With the compromise identified, our team of Customer Advisors alerted our customers to this activity. Meanwhile, our analysts quickly began performing deeper inspection of the logs uploaded to InsightIDR along with collecting additional forensic information directly from the compromised endpoints. Within a very short period of time, our analysts were able to identify how the attackers were executing commands, where they were coming from, and what tools they were using. This information allowed Rapid7 to provide proactive, actionable steps to

our customers to thwart the attack . Additionally, our analysts worked jointly with our Threat Intelligence and Detection Engineering (TIDE) team to review the collected data for the purpose of immediately developing and deploying additional detections for customers.

Three days later, on March 2, 2021, Microsoft acknowledged and released information on the exploitation of 0-day vulnerabilities in Microsoft Exchange by an actor they refer to as "hafnium." They also released patches for Microsoft Exchange 2013, 2016 and 2019 (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065, as well as others).

Despite this vulnerability being unknown to the public, Rapid7 was able to identify the attacker's presence on systems to help defend against the use of these 0-day exploits with our Attacker Behavior Analytics library.

Rapid7 recommends that everyone running Microsoft Exchange apply these patches immediately as they are being exploited in the wild by a sophisticated adversary.

Technical Analysis of Attacker Activity

1. Automated scanning to discover vulnerable Exchange servers from the following DigitalOcean IP addresses:

- 165.232.154.116
- 157.230.221.198
- 161.35.45.41

2. Analysis of Internet Information Services (IIS) logs shows a POST request is then made from the scanning DigitalOcean IP to multiple paths and files:

- /ecp/y.js
- /rpc/
- /owa/auth/signon.aspx
- /aspnet_client/system_web/<random_name>.aspx
- IIS Path ex: /aspnet_client/system_web/TInpB9PE.aspx
- File system path ex: C:\inetpub\wwwroot\aspnet_client\system_web\TInpB9PE.aspx
- /aspnet_client/aspnet_iisstart.aspx
- File system path: C:\inetpub\wwwroot\aspnet_client\aspx_iisstart.aspx
- /aspnet_client/aspx_client.aspx
- File system path: C:\inetpub\wwwroot\aspnet_client\aspx_client.aspx
- /aspnet_client/aspnet.aspx
- File system path: C:\inetpub\wwwroot\aspnet_client\aspnet.aspx

In some cases, additional dynamic link libraries (DLLs) and compiled aspx files are created shortly after the webshells are first interacted with via POST requests in the following locations:

- C:\Windows\Microsoft.NET\Framework64\<version>\Temporary ASP.NET Files\root\
- C:\Windows\Microsoft.NET\Framework64\<version>\Temporary ASP.NET Files\owa\

3. Next, a command executes, attempting to delete the “Administrator” from the “Exchange Organization administrators” group:

> cmd /c cd /d C:\\inetpub\\wwwroot\\aspnet_client\\system_web&net group "Exchange Organization administrators" administrator /del /domain&echo [S]&cd&echo [E]

4. With the command executed, and the webshell successfully uploaded, interaction with the webshell will begin from a different IP.

> We have monitored interaction from 45.77.252[.]175

5. Following the POST request, multiple commands are executed on the asset:

a. Lsass.exe dumping using procdump64.exe and C:\Temp\update.exe (MD5: f557a178550733c229f1087f2396f782):

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

b. Reconnaissance commands:

- whoami.exe
- ping.exe
- tasklist.exe
- quser.exe
- query.exe

Indicators Of Compromise (IOCs)

Type	Value
IP Address	165.232.154.116
IP Address	157.230.221.198
IP Address	161.35.45.41
IP Address	45.77.252.175
IP Address	104.248.49[.]97
IP Address That Interacts with Uploaded Webshells	194.87.69[.]35
URL	/ecp/y.js

Type	Value
URL	/ecp/DDI/DDIService.svc/GetList
URL	/ecp/DDI/DDIService.svc/SetObject
URL	/owa/auth/errorEE.aspx
URL	/owa/auth/logon.aspx
URL	/owa/auth/errorFE.aspx
URL	/aspnet_client/aa.aspx
URL	/aspnet_client/iis
URL	/iistart.aaa
URL	/owa/iistart.aaa
User Agent	python-requests/2.25.1
User Agent	antSword/v2.1

References

Update: March 7, 2021

Microsoft published tools to help identify servers potentially compromised by HAFNIUM. Upon review of the checks within the tools, Rapid7 identified the following additional pre-existing detections within InsightIDR's Attacker Behavior Analytics that would have alerted customers to this malicious actor in their environment:

- Attacker Technique - PowerShell New-MailboxExportRequest (Created March 14, 2019)
- Attacker Technique - PowerShell Remove-MailboxExportRequest (Created Dec. 15, 2020)
- Attacker Technique - Compressing Mailbox With 7zip (Created Dec. 15, 2020)
- Attacker Technique - PowerShell Download Cradles (Created Jan. 3, 2019)

These previously existing detections are based on observed attacker behavior seen by our Incident Response (IR), Managed Detection and Response, and Threat Intelligence and Detection Engineering (TIDE) teams. Through continuous collaboration across the Detection and Response practice, we help ensure our clients continue to have coverage for the latest techniques being used by malicious actors.

Update March 18, 2021

Widespread exploitation of vulnerable on-premises Exchange servers is ongoing. Microsoft has released a "One-Click Exchange On-premises Mitigation Tool" (EOMT.ps1) that may be able to automate portions of both the detection and patching process. Microsoft has said the tool is intended "to help customers who do not have dedicated security or IT teams to apply these security updates...This new tool is designed as an interim mitigation for customers who are unfamiliar with the patch/update process or who have not yet applied the on-premises Exchange security update." They have tested the tool across Exchange Server 2013, 2016, and 2019 deployments. See Microsoft's blog on the tool for details and directions: https://msrc-blog.microsoft.com/2021/03/15/one-click-microsoft-exchange-on-premises-mitigation-tool-march-2021/

We continue to encourage on-premises Exchange Server users to prioritize patching and monitoring for indicators of compromise on an emergency basis.

We'd like to extend a huge thank-you to everyone who helped contribute to this blog post:

- *Robert Knapp*
- *Shazan Khaja*
- *Lih Wern Wong*
- *Tiffany Anders*
- *Andrew Iwamaye*
- *Rashmi Joshi*
- *Daniel Lydon*
- *Dan Kelly*
- *Carlo Anez Mazurco*
- *Eoin Miller*
- *Charlie Stafford*
- *The Rapid7 MVM Team*

Never miss a blog

Get the latest stories, expertise, and news about security today.