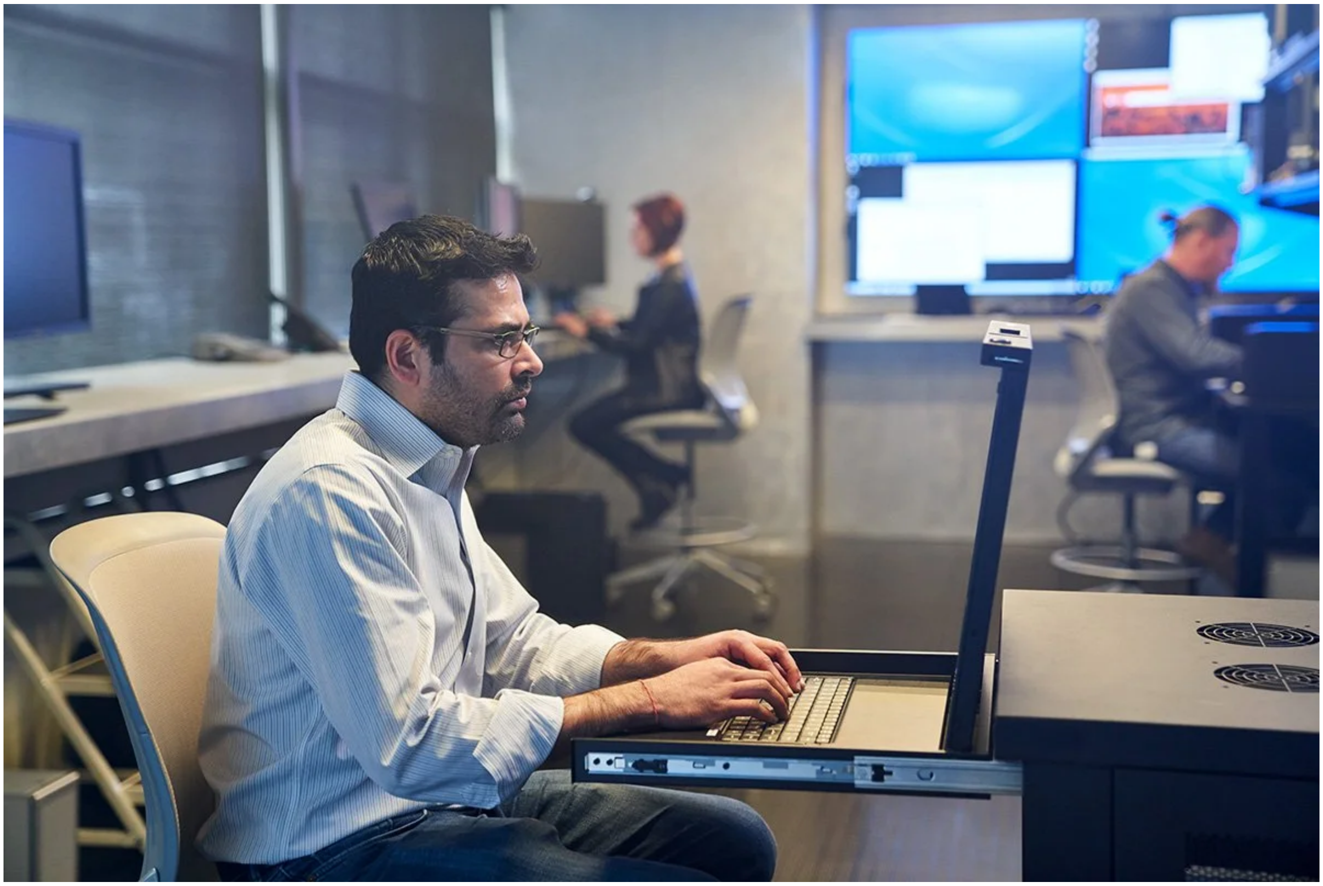
Mass exploitation of on-prem Exchange servers :(

reddit.com/r/msp/comments/lwmo5c/mass_exploitation_of_onprem_exchange_servers



level 1

Op · 1 yr. ago · edited 1 yr. ago*Locked*

2

Vendor Contributor

Update 16 - 03/12/2021 - 0458 ET

On Thursday afternoon (March 11th), security researcher Michael Gillespie reported ID Ransomware received a sudden increase in ransomware notices coming from IPs belonging to Microsoft Exchange servers. The encrypted files can be identified by their `.CRYPT` file extension and the file marker `DEARCRY!` (screenshot of the magic bytes). The ransom notice is named readme.txt and includes the following contact emails:

- konedieyp@airmail[.]cc
- uenwonken@memail[.]com

Microsoft has since confirmed this new family of ransomware is being used after the initial compromise of unpatched on-premises Exchange Servers. Microsoft Defender has received updates to detect this and may also be discoverable by the creation of a Service named `msupdate` according to James Quinn.

Update 15 - 03/11/2021 - 1504 ET

We are observing an uptick in post-exploitation activity. Many of these TTPs were previously disclosed in our March 9th Tradecraft Tuesday but the relevant slides can be found here:

- Opera Browser DLL Sideloading Services
- Cobalt Strike Loading from VSPerfMon Scheduled Tasks
- Sapphire Pigeon Activity Leading to Mimikatz
- PowerShell Based Lateral Movement Over SMB

With that said, there are some amazing blogs which highlight additional TTPs. We strongly suggest reading these resources:

- Elastic Blog Highlighting Collection of Network Recon Data
- TrustedSec Blog with Awesome Post-Exploitation Details
- ESET Diving into Multiple Reported Actors Exploiting This Situation

---

Update 14 - 03/11/2021 - 1413 ET

The last three days have been packed with mass analyzing verified intrusions of our partners. With this data, we've shared specific threat actor IOCs (not client data) with relevant Law Enforcement, CERTs, and national security organizations. For public organizations looking to do their own logging/monitoring/blocking/response, we feel comfortable sharing these observed exploit sources under TLP:WHITE. Huntress has direct evidence these IP addresses were used for exploitation and webshell interaction:

- 103.137.63.195, Mar 3
- 103.212.223.210, Mar 4
- 103.213.247.41, Mar 3
- 104.248.49.97, Feb 28

- 118.189.41.34, Mar 4
- 130.255.189.21, Mar 3
- 137.116.145.209, Mar 3
- 139.59.56.239, Mar 4
- 139.162.98.150, Mar 4
- 157.230.221.198, Feb 27
- 161.35.1.207, Feb 28
- 161.35.1.225, Feb 28
- 161.35.51.41, Feb 28
- 165.232.154.116, Feb 27
- 167.99.239.29, Feb 28
- 168.63.134.28, Mar 4
- 178.20.181.209, Mar 4
- 182.239.123.241, Feb 28
- 182.239.124.180, Mar 3
- 182.153.128.230, Mar 4
- 185.250.151.192, Mar 2

___

Update 13 - 03/08/2021 - 1610 ET

If interested, tomorrow on Tradecraft Tuesday (March 9 at 1300 ET) we will be covering the post-exploitation techniques we have observed. Everything from the web shells to the malware dropped.___

Update 12 - 03/06/2021 - 0632 ET

Yesterday we started seeing multiple partners' on-prem Exchange servers receive malicious scheduled tasks that executed a PowerShell downloader from `hxxp://p.estonine[.]com/p?e` . This server was hosted on Digital Ocean and resolved to IP address 188.166.162[.]201 and delivered a base64 encoded/compressed PowerShell script. Oddly enough, this PowerShell looked very similar to a previous coin miner campaign reported by Carbon Black in 2019. After reporting the incident to Digital Ocean (hosting) and NameCheap (registrar), we started digging into Layer 4 of the delivered payload. After deobfucating this (which produced Layer 5) we learned there were two Mimikatz DLLs (x86 and x64) embedded within the script which gets reflectively loaded/injected.

- 32bit - D58A41A393F4B9A406226689F29C7017CA20F788
- 64bit - FA8E53CB3497CBF81CFEE0DDBF171DE98B83211D

Stay vigilant because it looks like things may start to heat up 🔥

Update 11 - 03/05/2021 - 2319 ET

Brian Krebs' fantastic reporting estimates 30,000+ unique US organizations have been compromised. Many researchers beyond the Huntress team are scratching their heads on why did this incident escalated from the "limited and targeted" attacks observed by Volexity on Jan 6th, 2021 to this worldwide incident. Notable commenters include former CISA Director Chris Krebs and Microsoft's Hafnium blog has been updated with additional resources to aid those performing investigations.

Also of note is Microsoft has updated their CSS Exchange repo on Github with their own Nmap NSE to "detect whether the specified URL is vulnerable to the Exchange Server SSRF Vulnerability (CVE-2021-26855)." Folks have reported improved accuracy but warned a bug in Nmap could cause false inaccessibility errors. This is reportedly fixable by adding `--min-rtt-timeout 3` to Nmap's parameters. We recommend using this Microsoft version going forward to assist validating your patch status and will provide feedback if we discover better alternatives.

Update 10 - 03/05/2021 - 1704 ET

Just a quick update to our 1254 ET post.

We've confirmed the Nmap NSE script will display "potentially vulnerable" for both fully patched server AND servers with only the most recent CU level (which is still vulnerable). The script scrapes the OWA page to determine the version of Exchange. The OWA page only includes the version number as **major.minor.X** but you need **major.minor.X.Y** to confirm the fully patched version.

That said, the script is useful for finding unpatched versions quickly. Just be aware you need to verify the complete patch level for servers that have the most recent CU applied.

Also, the various Exchange registry keys, such as ClientAccessRole, are not completely reliable for patch verification. Here only the latest CU level version is reported, but patches to a CU do not appear to update the version number stored in the registry.

Update 9 - 03/05/2021 - 1254 ET

Tons of folks couldn't join the webinar yesterday so we want to more useful points:

- The internet is now mass scanning for these webshells
- Microsoft published a script to assist the detection of malicious Exchange activity
- The Nmap NSE to find vulnerable exchange boxes is not perfect (more on this shortly)
- Using the registry's exchange build data is not perfect (more on this shortly)

More community resources are starting to pour in, so we'd like to highlight them:

- NinjaRMM created great collection vendor knowledge. Check it out!
- Shodan has added some detection capabilities. Unsure if it has the same accuracy issues as the Nmap NSE released earlier this week.

Update 8 - 03/04/2021 - 1628 ET

Just finished the webinar and our team is in the process of sending the slides and recordings. In case you didn't make it, here's some of the most useful data

- List of Huntress Discovered "China Chopper" ASPX Webshell Filenames - 04 March
- PDF Version of the Presented Slides - 04 March
- Microsoft Emergency Patches - 02 March

Had to split this into two posts (hit the Reddit limit). See the older updates here.

88