Microsoft Exchange Zero Day’s – Mitigations and Detections.

blueteamblog.com/microsoft-exchange-zero-days-mitigations-and-detections

March 6, 2021

By Auth or / March 6, 2021 / Uncategorized
No Comments

This post will aim to explain what the Microsoft Zero Day’s are, and then provide all mitigation and detection advice which I am aware of so far. It will be updated every day, if and when new information is available.

If you feel like I miss anything important here, or made any mistakes; please DM me at https://twitter.com/blueteamblog and ill update the post.

All companies / researchers etc will be credited throughout the post.

Post Updated 12th March –

See further details on each point throughout the post.

It has been discovered on the 12th of March, that since the 9th of March; ransomware named DoejoCrypt aka DearCry has been targeting vulnerable Exchange Servers. A separate section has been created within the blog post for that, with the following details so far.

- Bleeping Computer and TheRecord articles.
- 3 Yara rules.
- MalwareBazaar Link.
- James Quinn Analysis and AppAnyRun Run.
- DearCry hashes from MSTIC.

Other Updates

- Further IOCs from BadPackets and THEDFIRReport
- Added updated Splunk Blog Post

Post Updated 11th March –

See further details on each point throughout the post.

- Microsoft had changed the links for their NMAP and IOC check script. Have added the new link.
- Added updated Elastic blog post which contains new TTPs.
- Added new IOC's from DFIRReport and KyleHanslovan from Huntress Labs.

Post Updated 10th March –

See further details on each point throughout the post.

- Added ESET post "Exchange servers under siege from at least 10 APT groups". Added IOCs from this post to the IOC section.
- Added available samples of the ESET analysis about Exchange vulnerabilities used by Chinese APT.
- Added DomainTools post "Examining Exchange Exploitation and its Lessons for Defenders"
- Added GreyNoise GNQL query for devices crawling the Internet for Microsoft OWA instances, minus known-benign hosts.
- Added detection advice that scheduled tasks similar to the "Sapphire Pigeon" tasks on non-Exchange hosts are being seen on the same network as a compromised Exchange server.
- Added detection advice that looks for hard coded elements from Exchange POC exploit code.
- Added Azure Sentinel detection that looks for Exchange Auditing being disabled.

Post Updated 9th March –

See further details on each point throughout the post.

- Added further IP's which are known to be targeting the vulnerabilities.
- Added link to video of technical showcase of some post exploitation techniques.
- Added link to Victim Notification Website. Businesses can check via email or IP, but only discloses to people with a provable association with the victim.
- Added link to TrueSec blog post, in particular in relation to the Post Explotation section.
- Added Sigma rule based on TrueSec's findings.
- Added another query for Azure Sentinel / Defender for detecting exchange exploitation.
- Added VirusTotal search for HAFNIUM webshell uploads.
- Added detection advice to use externaldata operator in Azure Sentinel.
- Added Microsoft Safety Scanner link.
- Added SIGMA rules to detect HAFNIUM Exchange Exploitation Activity and Suspicious Service Binary Directory.
- Added link to RedCanary blog.

Post Updated 8th March –

See further details on each point throughout the post.

- Added KrebsOnSecurity timeline of the Exchange hacks, and when companies reported the issues to Microsoft.
- Added hashes of known good exchange files.
- Added 2 webshell samples which match hashes mentioned in Microsoft's HAFNIUM report.
- Added List of known suspect / bad IPs targeting Exchange vulnerabilities.
- Added detection advice for when you are checking POST requests.
- Fixed missing Elastic detection's link.
- Added sysmon config for Exchange Servers.

Post Updated 7th March –

See further details on each point throughout the post.

- Added queries for Azure Sentinel (Sysmon) and M365D to detect anomalous network connections made by the servers.
- Added Elastic detection's.
- Added update that you need to re-scan any Exchange systems you previously scanned with Microsoft's nmap NSE script (http-vuln-cve2021-26855.nse)

What are the Exchange Zero Days?

In case you have been hiding under a rock this past week (I wouldn't blame you), here is a breakdown of what they are. You may also hear people referring to the Exchange Zero Days as:

- HAFNIUM (Original threat group who exploited the zero days, named by Microsoft)
- Operation Exchange Marauder (Name given to the initial attack by Volexity, the company who first identified the zero days)

From the original Microsoft post (I highly recommend reading this whole article) –

CVE-2021-26855 is a server-side request forgery (SSRF) vulnerability in Exchange which allowed 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. Insecure deserialization is where 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 is a post-authentication arbitrary file write vulnerability in Exchange. If HAFNIUM could authenticate with the Exchange server then they could use this vulnerability 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.

CVE-2021-27065 is a post-authentication arbitrary file write vulnerability in Exchange. If HAFNIUM could authenticate with the Exchange server then they could use this vulnerability 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.

It is important to note that these vulnerabilities exist on Microsoft Exchange Server, and does not affect Microsoft Exchange Online users.

Further reading

There is further information about the zero days at Volexity's original post and also at the Mandiant Managed Defence post.

A site named proxylogon.com has also been created. This is for CVE-2021-26855 and is then chained with CVE-2021-27065 which allows unauthenticated attackers to execute code on remote systems. The site shows an example of the exploit in action.

Brian Krebs (KrebsOnSecurity) has released a basic timeline of the Exchange mass hack. This includes a timeline of when companies first noted the issues to Microsoft, until the present date.

Post Exploitation Activities

After exploiting the above vulnerabilities, there have been a number of post exploitation actions seen.

> **As per the Microsoft post, the following post exploitation activities were seen from the HAFNIUM group, after they dropped a webshell using the above vulnerabilities.**

Using Procdump to dump the LSASS process memory

Using 7-Zip to compress stolen data into ZIP files for exfiltration

Adding and using Exchange PowerShell snap-ins to export mailbox data

Using the Nishang Invoke-PowerShellTcpOneLine reverse shell

Downloading PowerCat from GitHub, then using it to open a connection to a remote server

Downloaded the Exchange offline address book from compromised systems.

> **As per the Volexity post, the following post exploitation activities have been seen.**

rundll32 C:\windows\system32\comsvcs.dll / MiniDump lsass.dmp – Dump process memory of lsass.exe to obtain credentials

PsExec – Windows Sysinternals tool used to execute commands on remote systems

ProcDump – Windows Sysinternals tool to dump process memory

WinRar – Command Line Utility Used archive data exfiltration

Webshells (ASPX and PHP) – Used to allow command execution or network proxying via external websites

Domain Account User Addition – Leveraged by attackers to add their own user account and grant it privileges to provide access in the future

> **As per the Mandiant post, the following additional activity was seen.**

net group "Exchange Organization administrators" administrator /del /domain.

This command attempts to delete the administrator user from the Exchange Organizations administrators group, beginning with the Domain Controller in the current domain. If the system is in a single-system domain, it will execute on the local computer.

> **Please take your time to read the Post-Exploitation Analysis section of this report from Huntress Labs**. There is an in depth write-up originating from the execution of a command that was detected and stopped by Windows Defender. The thread then goes on until the attacker drops Mimikatz.
>
> **Please take your time to read the Post Exploitation section of this report from TrueSec**. It has a number of new post exploitation activities which have not been noted in other posts as of yet.
>
> **Please take your time to read this post from ESET** – "Exchange servers under siege from at least 10 APT groups" . It contains details of 10 threat groups using the exploits and behaviors they are known to exhibit.
>
> **Please take your time to read this post from DomainTools** – "Examining Exchange Exploitation and its Lessons for Defenders". It contains a good write up especially in relation to attribution and detection.

DoejoCrypt aka DearCry Ransomware

Please continue to read information below before reading this section, if you have not done so already. On the 9th of March, Ransomware named #DoejoCrypt aka #DearCry has started to target Exchange Servers via the exploits mentioned in this blog.

There are number of well written, informative articles on the ransomware targeting Exchange Servers so far –

- BleepingComputer article
- TheRecord article
- Twitter thread from Sophos explaining DearCry

DoejoCrypt / Dearcry samples are available at Malware Bazaar.

Thanks to James Quinn (who added some of the above samples to Malware Bazaar) for sharing the following :

- Notes on the samples he found
- AppAnyRun Run

As shared by Pete Bryan, the MSTIC feed has been updated. It includes some hashes related to DearCry ransomware seen exploiting the Exchange vulnerabilities.

A number of Yara rules are available to detect DearCry / DoejoCrypt.

Sebdraven – Yara rule link.

Florian Roth / Nils Kuhnert – Yara rule link.

Reversing Labs – Yara rule link.

Mitigations and Detections

The below list is all the knowledge I have so far gathered for Mitigations and Detections against / for CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 and CVE-2021-27065. This also includes some detections for known post exploitation tactics.

Microsoft

Microsoft Vulnerability Mitigation's

Importantly, this tells you –

- How to install the security update (**This does not evict an attacker if they have already compromised the system**). It is also worth noting that if you are installing the upgrades manually, you **must** run the update from the elevated command prompt. If you are running an older CU then what the patch will accept, you must upgrade to at least the required CU as stated above then apply the patch.
- If you see unexpected behaviors or your upgrade fails, please go to this link which advises how to troubleshoot.
- If you are unsure of the patch levels of your Exchange Servers, use this script from Microsoft.
- Interim mitigation's if you are unable to patch Exchange Server 2013/16/19. This includes what they mitigate and potential impact. (**These do not fully protect against the attacks. As above, does not evict an attacker if they have already compromised the system)**

Microsoft have also provided the following –

- All Microsoft scripts (NMAP script to identify if your systems are vulnerable to Exchange zero days and Powershell script to check Windows event logs and Exchange logs for IOCs.) can now be found at this link.
- Microsoft Safety Scanner designed to find and remove malware from Windows computers. Simply download it and run a scan on Exchange Servers to find malware and try to reverse changes made by identified threats.

CheckMyOWA – Victim Notification Site

Thanks to Allison Nixon for sharing this

CheckMyOWA is a site from Unit221b. In the words of Allison "***Re: The recent mass Exchange hacks, we're releasing a victim notification website. Can check via email or IP, but only discloses to people with a provable association with the victim. Target audience is small businesses who haven't already been made aware.***"

Check out the site here.

Volexity

Within the Volexity post they have a large list of indicators that it is recommended you search for. I am not going to include them all here, as the list is too long. Please go to the post and review the **Indicators of Compromise** section and ensure you check for them all.

Mandiant Managed Defense

Mandiant Advisory

Mandiant advise checking the following –

- Child processes of C:\Windows\System32\inetsrv\w3wp.exe on Exchange Servers, particularly cmd.exe.
- Files written to the system by w3wp.exe or UMWorkerProcess.exe.
- ASPX files owned by the SYSTEM user
- New, unexpected compiled ASPX files in the Temporary ASP.NET Files directory

- Reconnaissance, vulnerability-testing requests to the following resources from an external IP address:
  - /rpc/ directory
  - /ecp/DDI/DDIService.svc/SetObject
  - Non-existent resources
  - With suspicious or spoofed HTTP User-Agents
- Unexpected or suspicious Exchange PowerShell SnapIn requests to export mailboxes

They also advise preserving the following artifacts for forensic analysis:

- At least 14 days of HTTP web logs from the inetpub\Logs\LogFiles directories (include logs from all subdirectories)
- The contents of the Exchange Web Server (also found within the inetpub folder)
- At least 14 days of Exchange Control Panel (ECP) logs, located in Program Files\Microsoft\Exchange Server\v15\Logging\ECP\Server
- Microsoft Windows event logs

Red Canary

Red Canary Intel have released a fantastic post which contains.

- The different clusters of threat activity they are seeing
- The detection analytics they used to detect them
- The simple remediation steps you can take to start to remove this activity from your environment if you find it, whether you're a single administrator or a mature security team.

Cisco Talos

Cisco Talos Advisory

Cisco Talos have released a number of Snort rules which can detect / block the behavior as follows –

- CVE-2021-26857 — 57233-57234
- CVE-2021-26855 — 57241-57244
- CVE-2021-26858 & CVE-2021-27065 — 57245-57246
- CVE-2021-24085 — 57251
- CVE-2021-27065 — 57252-57253
- Html.Webshell.Hafnium — 57235-57240

There is also a ClamAV signature – Win.ASP.MSExchangeExploit

They importantly point out "*All organisations using the affected software should prevent external access to port 443 on Exchange Servers, or set up a VPN to provide external access to port 443. This will ensure that only authenticated and authorized users can connect to this service. However, this action will only protect against the initial step of the attack.*"

CISA

CISA Advisory

On top of the above recommendations from Cisco, the following advice from CISA is also important –

- Block external access to on-premise Exchange:
  - Restrict external access to OWA URL: `/owa/`.
  - Restrict external access to Exchange Admin Center (EAC) aka Exchange Control Panel (ECP) URL: `/ecp/`.
- Disconnect vulnerable Exchange servers from the internet until a patch can be applied.

Other international agencies have been releasing advice regarding the zero days.
Catalin Cimpanu shared on Twitter this list of International advisories regarding the Exchange Zero days.

CERT Latvia

The Latvian CERT have released a powershell script to detect webshells dropped by the recent zero days onto exchange servers.

Nextron Systems

Nextron Systems have setup THOR Lite (a free forensics scanner) to scan for HAFNIUM indicators. See the blog post and usage instructions here.

This includes this YARA rule written by Joe Hannon from Microsoft that looks for HAFNIUM indicators.

Recon Infosec

OSQuery hunt to look for systems where the ProcDump EULA has been accepted. This is important as attackers are using Procdump to dump the LSASS process memory

Microsoft 365 Defender Hunting Queries

Microsoft have published a number of hunting queries, as follows.

- Reverse shell loaded using Nishang Invoke-PowerShellTcpOneLine technique
- Exchange Server IIS dropping web shells
- Procdump dumping LSASS credentials
- 7-ZIP used by attackers to prepare data for exfiltration
- Exchange PowerShell snap-in being loaded
- Powercat exploitation tool downloaded
- Exchange vulnerability creating web shells via UMWorkerProcess
- Exchange vulnerability launching subprocesses through UMWorkerProcess
- Base64-encoded Nishang commands for loading reverse shell

SIGMA Queries

Thanks to Florian Roth for sharing and creating these.

This includes two rules.

- HAFNIUM Exchange Exploitation Activity – Detects activity observed by different researchers to be HAFNIUM group acitivity (or related) on Exchange servers.
- Suspicious Service Binary Directory – Detects a service binary running in a suspicious directory.

Splunk Queries

Thanks to Jose Enrique Hernandez for sharing these on Twitter.

On the 12th of March, Splunk have released an updated blog post including further detection advice. Thanks to John Stoner for sharing this.

SOC Prime (SIEM detection's to translate to various languages)

Thanks to Ring3API for sharing these on Twitter. Free rules which can be converted to various SIEM languages.

Azure Sentinel (Sysmon) and M365D queries to detect anomalous network connections made by the servers.

Thanks to Mehmet Ergene for creating and sharing these.

Link to the query logic here.

Further Azure / Defender query to detect exploitation of Exchange vulnerabilities.

Thanks to James Quinn for creating and sharing these.

Link to the query logic here.

Elastic Queries / Write-Up

Thanks to Austin for sharing this.

This is the full write-up from elastic which I missed in my original blog post. It contains a number of detection logic's, see the **detection** section of the article.

On the 11th of March, Elastic have updated their post with the following –

Some TTP's include:

- Network enumeration/discovery
- Credential dumping of Windows Registry
- Leveraging makecab utility to compress files

Known Good Exchange Hashes

Thanks to John Lambert for sharing this.

- Hashes provided by Microsoft Exchange team.
- Hashes provided by NCCGroup

Sysmon Config

As shared by Emir Erdogan there is a Sysmon config file that can be used for your Exchange servers, to aid in detections.

Further Detection Ideas

These are detection ideas which I am gathering over time from twitter.

- As shared by Samir – "Multiple instances of w3wp.exe with cmdline containing "MSExchange*AppPool" spawning WerFault.exe could be also an indicator of failed exploitation attempts."
- As shared by Joseph – "If you find you are compromised with the latest Exchange exploit, take moment and check for any new users is your domain that "appeared" after compromise. Try running this script to see- https://pastebin.com/raw/cr01VuCa"
- As shared by Kevin look for the following – "Large amounts of internal SMB traffic from Exchange Server. Also look for Scheduled task called Winnet on Exchange Server"
- As shared by Tyler be careful when checking your POST requests – "Anyone searching for/responding to Exchange attacks, one of the key indicators is POST to /ecp/<singleletter>.js. DO NOT JUST LOOK FOR singleletter!!!! Seeing a bunch going to /ecp/program.js!"
- As shared by Randy – "AzureSentinel pro tip: use the externaldata operator to grab IOC lists such as the one that Microsoft is maintaining for HAFNIUM indicators (https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/Sample%20Data/Feeds/MSTICIoCs-ExchangeServerVulnerabilitiesDisclosedMarch2021.csv…) and use those values in your KQL queries"
- As shared by John – "We haven't confirmed lateral movement, but interesting to see scheduled tasks similar to the "Sapphire Pigeon" tasks on non-Exchange hosts on the same network as a compromised Exchange server."
- As shared by Pete – "There are a few PoC scripts for Exchange exploits floating around (with varying validity) that people may be trying to use for opportunistic exploits. One of the PoCs has hard coded elements you can hunt for in logs" See further details in the twitter thread here.
- As shared by Huy – "A good use-case to alert on is, when someone is turning off Exchange auditing." There is a Sentinel detection for this here.

IOC List

There are numerous IOC's contained within the Microsoft and Volexity reports. Here are some extra's that I have came across. These are either hosting badness or attempting the exploits.

Bad Packets have shared the following:

- Active CVE-2021-21972 payload: http://www.lingx[.]club/javac
- Virus Total Link
- Exploit attempt source IP: 104.197.133(.)59

DFIR Report have shared the following:

Exchange proxylogon and file write exploit attempt coming from: 45.114.130[.]89 – EHOSTIDC (Japan)

Kyle Hanslovan has shared the following China Mobile IP addresses were used for exploitation and interacting with webshells as early as Feb 28.

- 182.239.124(.)180
- 182.239.123(.)241

TheDFIRReport has shared the following

172.105.174[.]117 scanning for the following Exchange webshells –

0QWYSEXe.aspx
aspnet_client.aspx
aspnettest.aspx
discover.aspx
error.aspx
help.aspx
HttpProxy.aspx
iispage.aspx
load.aspx
log.aspx
OutlookEN.aspx
shell.aspx
shellex.aspx
sol.aspx
supp0rt.aspx

From the ESET post above –

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

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
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

Arkbird has shared the available samples of the ESET analysis about Exchange vulnerabilities used by Chinese #APT.

Andrew Morris has shared a GNQL (Greynoise) query to search for devices crawling the Internet for Microsoft OWA instances, minus known-benign hosts.

cyb3rops (Florian Roth) has shared that a new webshell sample with hash mentioned in Microsoft's HAFNIUM report surfaced on Virustotal (upload from Turkey).

Huseyin Rencber has shared another webshell sample added to VirusTotal which matches another hash mentioned in Microsoft's HAFNIUM report.

BushidoToken shared that all HAFNIUM related uploads to VirusTotal can be found with this search.

MrR3boot (Daniel Card) has created a community list of known suspect / bad IPs which are targeting the Exchange vulnerabilities.

Further IOC's (May overlap with other links over time) –

- 188.166.162[.]201
- hxxp://p.estonine[.]com/p?e
- hxxp://cdn.chatcdn[.]net/p?low
- 112.66.255[.]71
- 86.105.18[.]116
- 77.61.36[.]169
- 165.232.154[.]116
- 157.230.221[.]198
- 104.248.49[.]97
- 161.35.76[.]1
- 139.59.56[.]239
- List of known Microsoft Exchange Incident "China Chopper" ASPX Webshell filenames from Huntress Labs.
- 183.136.225[.]46 – Checking for Exchange Servers vulnerable to CVE-2021-26855
- 104.225.219[.]16
- 159.89.95[.]163
- 198.50.168[.]176
- 45.154.2[.]94
- 34.87.113[.]30
- 185.173.235[.]172
- 185.173.235[.]54
- 185.65.134[.]165

If you find any broken links, think I am missing any important information or have made a mistake; DM me at https://twitter.com/blueteamblog. If I find more mitigations / detections, sections will be clearly updated; with timestamps.

Leave a Reply

Your email address will not be published. Required fields are marked *