SECURONIX™

Securonix Threat Research:

On HAFNIUM/ CHOPPERWAVE Exchange Server Attacks Detection Using Security Analytics - Securonix Security Advisory (SSA)

Oleg Kolesnikov, Den Iuzvyk
Securonix Threat Research Team
Created: March 3, 2021
Last Updated: March 18, 2021, v0.02

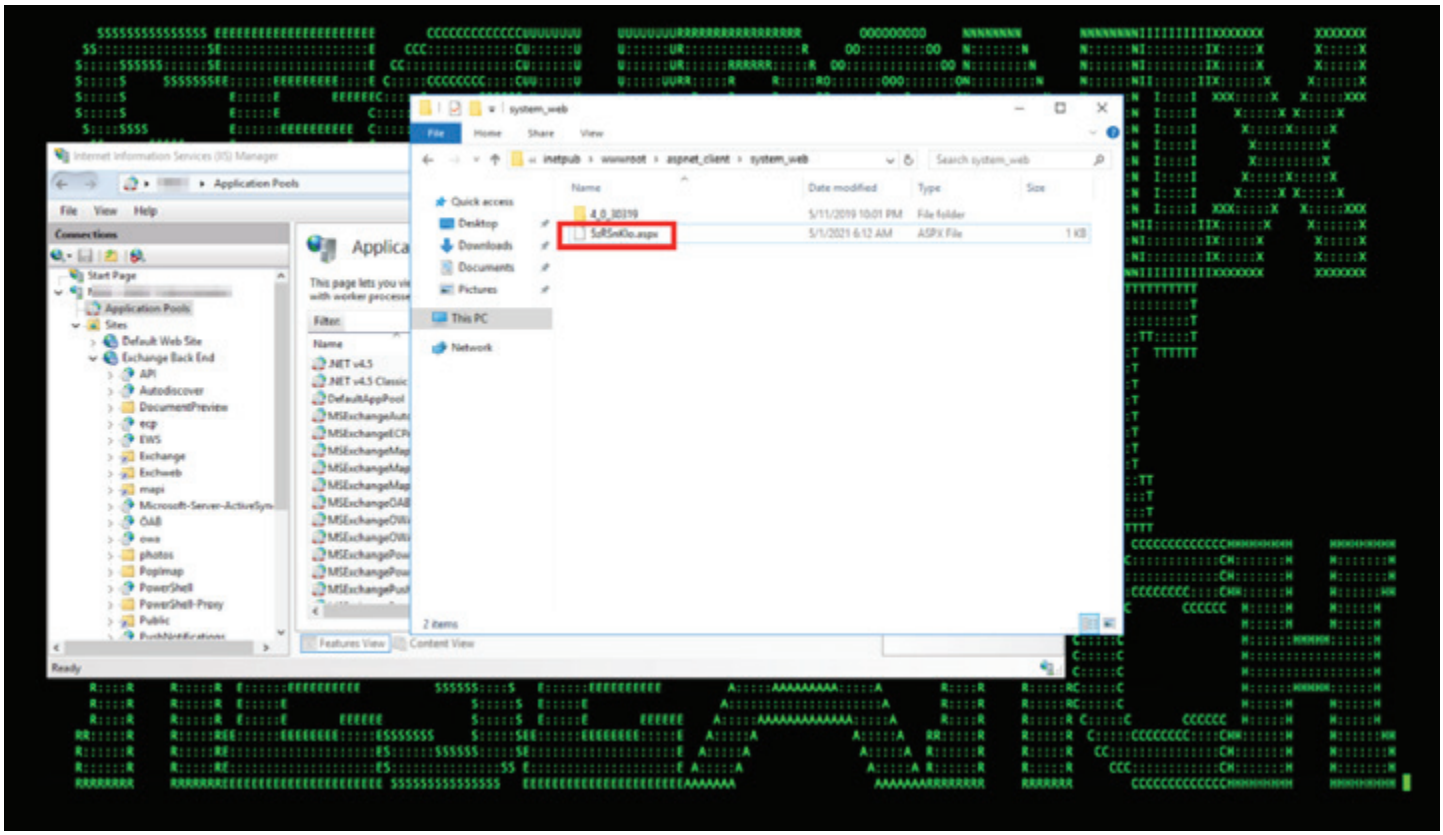

Figure 1: Example of HAFNIUM Webshell On a Victim's Host

Introduction

The Securonix Threat Research (STR) team is actively monitoring, investigating, and proactively hunting for the critical ongoing HAFNIUM (tracked by STR as CHOPPERWAVE) attacks and the related malicious activity. We are also tracking cryptomining implants and ransomware operator placement attempts of the DearCry/DoejoCrypt, a ransomware payload, and the other implants [1,2,4].

The summary below includes some of the key details we observed about these high-profile attacks and our recommendations on what Securonix predictive indicators/security analytics to use to increase the chances of detecting both the known/future variants of the attacks and related post-breach activity.

Figure 2: Publicly available HAFNIUM/Exchange Exploit in Action

Summary

- **Synopsis:** The HAFNIUM/CHOPPERWAVE exchange server exploits involved a group of malicious threat actors leveraging four different zero-day exploits to place .aspx implants/webshells on a large number of Exchange servers exposed online (see Figure 2). Some of the implants placed on the servers were never used.

- The significance of these attacks is not only manifested in the number of victims that were exploited successfully, but also the fact that many of the Exchange servers exploited had some form of a security tool/AV/EDR solution running, and many of the tools were effectively bypassed by the attackers.

- Note: this is not to say the security tools are not useful, many of them are very effective, but this is a good example showing that preventing some of these attacks can be a non-trivial problem and detection is never guaranteed, especially for unknown attacks, so it is best not to rely on a single security tool for your detection, and instead use multiple security tools/diversify your telemetry to increase the chances of detecting such attacks) [2];

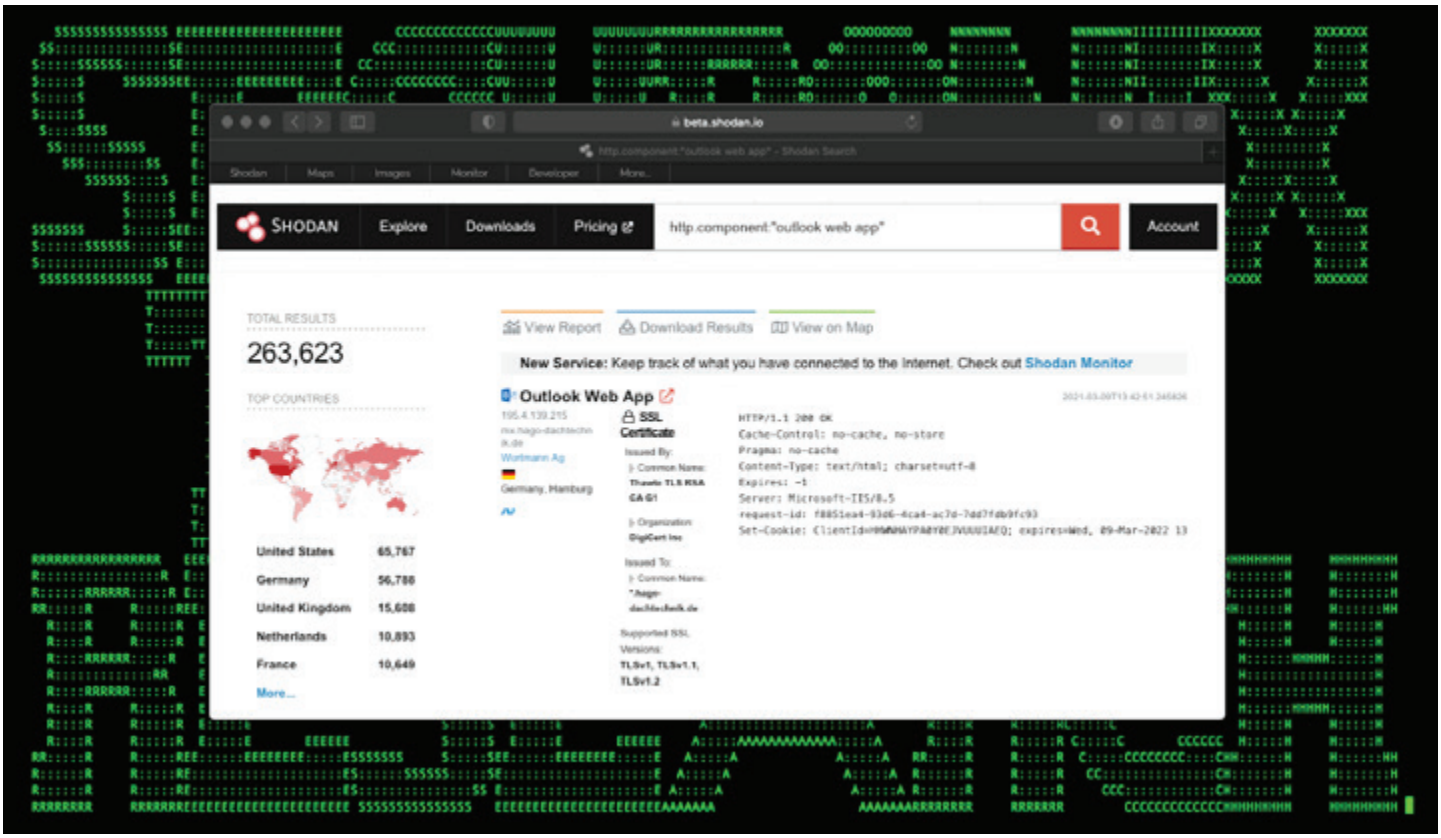

Figure 3: Examples of some of the potentially vulnerable Exchange servers (Credit: Shodan)

- **Attack vector(s):** The attacks began by early January 2021 and leveraged a combination of four different zero-day exploits (now available publicly - see Figure 2):
    - CVE-2021-26855
    - CVE-2021-26857
    - CVE-2021-26858
    - CVE-2021-27065

Impact: According to Shodan, over 250,000 potentially vulnerable Exchange servers worldwide are impacted with over 60,000 in the US (See Figure 3). Exchange 2013, 2016, and 2019 are impacted, Exchange 2010 are only impacted by CVE-2021-26857.

Some relevant attack artifacts - highlights: Some of the malicious payloads observed are well-known webshells, such as China Chopper. These web shells typically involve the use of command lines that contain certain fixed strings, e.g., "[s]&cd&echo [e]" and others as reported by some researchers [7].

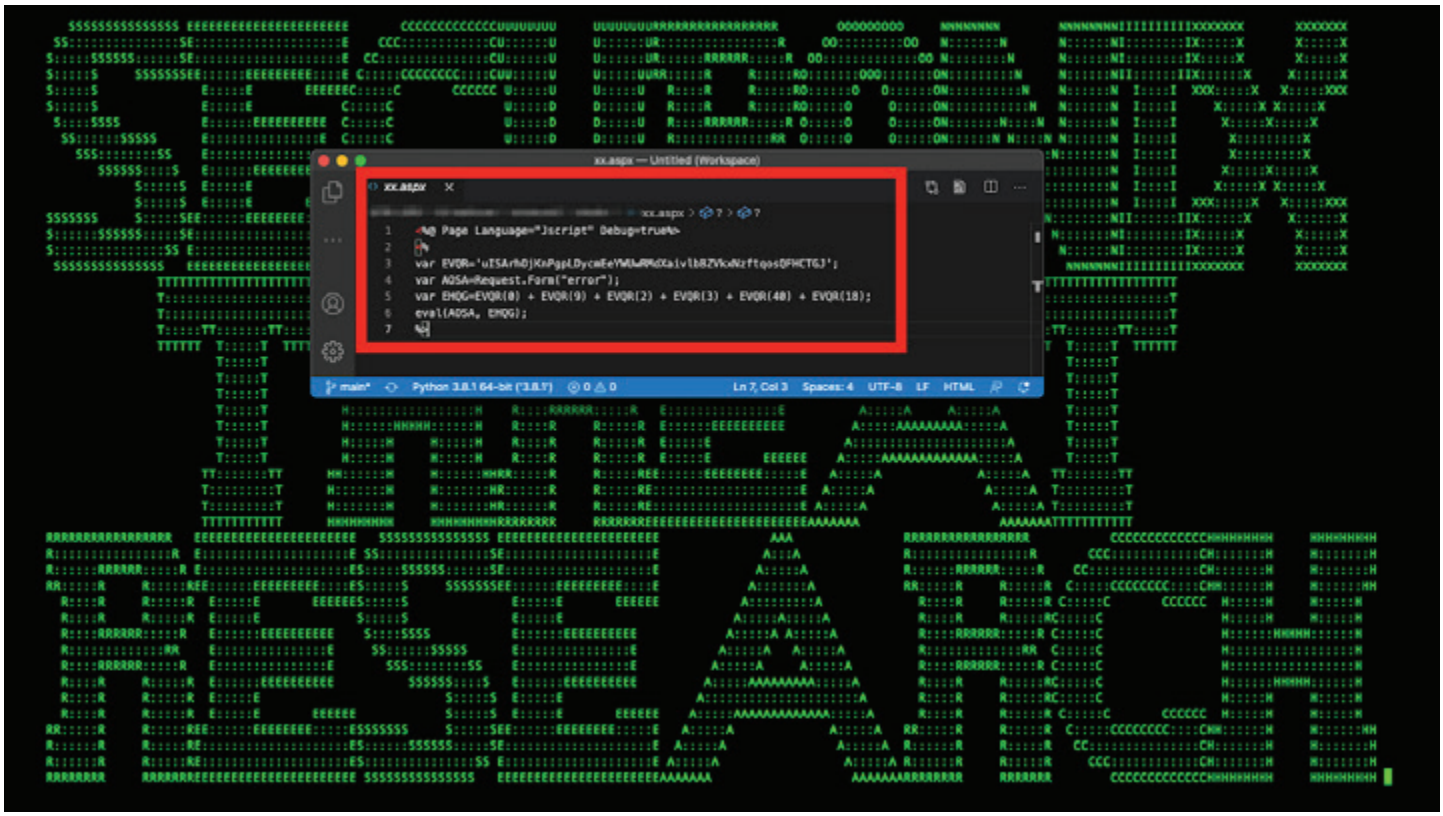

Figure 4: Example of one of webshells used by HAFNIUM

Critical HAFNIUM/CHOPPERWAVE Attacks - Blue Team Highlights

Update 3/18/2021: The HAFNIUM attackers have been active for some time now, therefore it is critical to shift focus to post-exploitation activity/potential compromised user account monitoring instead of compromised instance triaging/monitoring/response. Move to implementing detection and response capabilities to identify the future variants of such malicious threats in your environment. To help you identify future variants, we've shared examples of relevant hunting queries and detection use cases in the 'Detection' section below.

Below are some of the technical observations that can help blue teams better detect the malicious activity associated with the HAFNIUM/CHOPPERWAVE attacks:

- We have been observing the attackers dropping a large number of webshells. This was likely an attempt to "seed" the victim environments in anticipation of an upcoming Microsoft patch. The webshells can potentially allow the attackers to take advantage of the victim environments later. There are already reported attempts that attackers tried to leverage their access, including crypto mining and ransomware placement (See Figure 8).

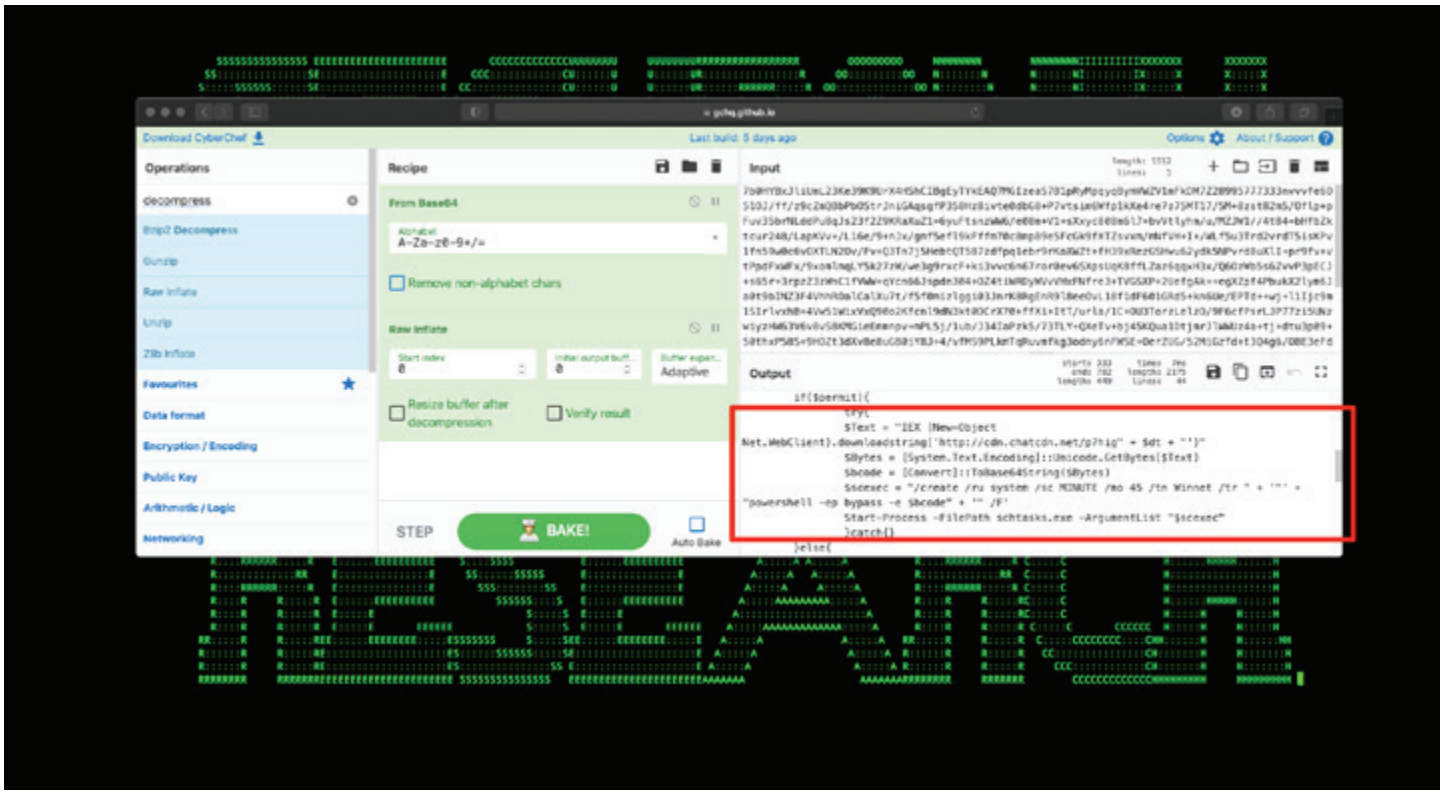

Figure 5: Multi-stage powershell code/persistence

- Some of the exploits mentioned targeting the Exchange servers are publicly available (see Figure 2), and there are multiple malicious threat actors (MTA) observed that have been involved in the exploitation activity, so for some victims multiple different webshells were observed to be installed (see Figure 4);

- The post-exploitation activity appears to be different for different types of webshells installed. For some of the webshells, the post-exploitation activity involved may look like, e.g., commands to make Exchange user and group changes:

  cmd.exe /c cd /d “C:\\inetpub\\wwwroot\\aspnet_client\\system_web”&net group “Exchange Organization administrators” administrator /del /domain&echo [S]&cd&echo [E] [6]

- There appears to be a significant amount of post-exploitation activity involving the use of multi-stage payloads with encoded powershell code, so monitoring powershell-related log sources can help detect some of the attack variants (See Figure 5).

C:\inetpub\wwwroot\aspnet_client\system_web\lCK4sMeJ.aspx	Bitdefender
C:\inetpub\wwwroot\aspnet_client\system_web\M2gRp7Zo.aspx	Cylance OPTICS, Cylance
C:\inetpub\wwwroot\aspnet_client\system_web\rYa8Rnhx.aspx	Webroot
C:\inetpub\wwwroot\aspnet_client\system_web\bLt32SQG.aspx	Webroot
C:\inetpub\wwwroot\aspnet_client\system_web\Vd0fUyxN.aspx	
C:\inetpub\wwwroot\aspnet_client\system_web\yFu5T8JV.aspx	Cylance
C:\inetpub\wwwroot\aspnet_client\system_web\hjmQWreC.aspx	Webroot
C:\inetpub\wwwroot\aspnet_client\system_web\gwVPU69R.aspx	Windows Defender
C:\inetpub\wwwroot\aspnet_client\system_web\XJrBqeul.aspx	Webroot
C:\inetpub\wwwroot\aspnet_client\system_web\1DOyENMK.aspx	Windows Defender, RocketCyber
C:\inetpub\wwwroot\aspnet_client\system_web\LX9pWi4u.aspx	Symantec, Trend Micro
C:\inetpub\wwwroot\aspnet_client\system_web\Gt9KNFaZM.aspx	Perch
C:\inetpub\wwwroot\aspnet_client\system_web\FU7WfSK.aspx	
C:\inetpub\wwwroot\aspnet_client\system_web\l95DGqbQ.aspx	Windows Defender, Webroot
C:\inetpub\wwwroot\aspnet_client\system_web\SBx3mpCE.aspx	ESET
C:\inetpub\wwwroot\aspnet_client\system_web\jFabdYwZ.aspx	Windows Defender, SentinelOne
C:\inetpub\wwwroot\aspnet_client\system_web\comHG5Iz.aspx	Cylance, Windows Defender
C:\inetpub\wwwroot\aspnet_client\system_web\hNp1PEB7.aspx	Webroot, Bitdefender
C:\inetpub\wwwroot\aspnet_client\system_web\sKPt5Zml.aspx	SentinelOne, ThreatLocker
C:\inetpub\wwwroot\aspnet_client\system_web\qNKd61vE.aspx	Webroot
C:\inetpub\wwwroot\aspnet_client\system_web\YZ3Pn1yB.aspx	ESET, Webroot
C:\inetpub\wwwroot\aspnet_client\system_web\8tzybc6a.aspx	Webroot
C:\inetpub\wwwroot\aspnet_client\system_web\NVTGrgH0.aspx	Windows Defender
C:\inetpub\wwwroot\aspnet_client\system_web\CX47ujQS.aspx	Cylance, Cylance OPTICS
C:\inetpub\wwwroot\aspnet_client\system_web\Tx2tWFMb.aspx	Cylance OPTICS, Cylance
C:\inetpub\wwwroot\aspnet_client\system_web\6zOVlhZf.aspx	Webroot
C:\inetpub\wwwroot\aspnet_client\system_web\5fxzdtAl.aspx	
C:\inetpub\wwwroot\aspnet_client\system_web\C05E6dYt.aspx	Cylance
C:\inetpub\wwwroot\aspnet_client\system_web\0x9pzh86.aspx	Webroot
C:\inetpub\wwwroot\aspnet_client\system_web\zuFLEONY.aspx	Webroot, Windows Defender
C:\inetpub\wwwroot\aspnet_client\system_web\K5SHo6MQ.aspx	
C:\inetpub\wwwroot\aspnet_client\system_web\KLMV9StC.aspx	Sophos, RocketCyber
C:\inetpub\wwwroot\aspnet_client\system_web\x638MRKj.aspx	SentinelOne
C:\inetpub\wwwroot\aspnet_client\system_web\MvR1xZ3o.aspx	Webroot, Bitdefender
C:\inetpub\wwwroot\aspnet_client\system_web\GnTEiDtw.aspx	Windows Defender, Trend Micro
C:\inetpub\wwwroot\aspnet_client\system_web\mPOtfnwB.aspx	ThreatTrack Security
C:\inetpub\wwwroot\aspnet_client\system_web\9vKjdUnK.aspx	CrowdStrike, Windows Defender

C:\inetpub\wwwroot\aspnet_client\system_web\c2TUqNrx.aspx	Perch, Webroot
C:\inetpub\wwwroot\aspnet_client\system_web\pOTZwYgq.aspx	Cylance
C:\inetpub\wwwroot\aspnet_client\system_web\ZKS7YlnF.aspx	Webroot
C:\inetpub\wwwroot\aspnet_client\system_web\7H3kSz5g.aspx	Webroot, Windows Defender
C:\inetpub\wwwroot\aspnet_client\system_web\lA3rFekt.aspx	Webroot
C:\inetpub\wwwroot\aspnet_client\system_web\HF25QZvy.aspx	Malwarebytes, Webroot, Windows Defender
C:\inetpub\wwwroot\aspnet_client\system_web\FT89Vd3u.aspx	Malwarebytes, Webroot, Windows Defender
C:\inetpub\wwwroot\aspnet_client\system_web\70CJOw4i.aspx	Malwarebytes, Webroot
C:\inetpub\wwwroot\aspnet_client\system_web\9llwg2aX.aspx	Malwarebytes, Webroot
C:\inetpub\wwwroot\aspnet_client\system_web\kxvetqGR.aspx	
C:\inetpub\wwwroot\aspnet_client\system_web\caVZQkJF.aspx	Webroot
C:\inetpub\wwwroot\aspnet_client\system_web\VkvLJFXT.aspx	Webroot
C:\inetpub\wwwroot\aspnet_client\system_web\bkZj3nPX.aspx	Webroot
C:\inetpub\wwwroot\aspnet_client\system_web\0cvxSJy9.aspx	Webroot, CrowdStrike
C:\inetpub\wwwroot\aspnet_client\system_web\DCXrMji2.aspx	ThreatTrack Security, Webroot, Windows Defender
C:\inetpub\wwwroot\aspnet_client\system_web\Q3ep9hZW.aspx	Bitdefender, Windows Defender
C:\inetpub\wwwroot\aspnet_client\system_web\D8NTsC4w.aspx	Bitdefender, Windows Defender
C:\inetpub\wwwroot\aspnet_client\system_web\aXnJTHkd.aspx	Bitdefender
C:\inetpub\wwwroot\aspnet_client\system_web\VEuswX4o.aspx	Webroot
C:\inetpub\wwwroot\aspnet_client\system_web\Hf6koiAg.aspx	McAfee
C:\inetpub\wwwroot\aspnet_client\system_web\iH3FogCE.aspx	
C:\inetpub\wwwroot\aspnet_client\system_web\SebmlUrd.aspx	Sophos
C:\inetpub\wwwroot\aspnet_client\system_web\ZI1DzdL8.aspx	
C:\inetpub\wwwroot\aspnet_client\system_web\9vMTSpW.aspx	Webroot
C:\inetpub\wwwroot\aspnet_client\system_web\i5UHAcd32.aspx	Malwarebytes, Webroot
C:\inetpub\wwwroot\aspnet_client\system_web\z36OZseJ.aspx	Webroot
C:\inetpub\wwwroot\aspnet_client\system_web\2NRugkpf.aspx	Cylance, Windows Defender
C:\inetpub\wwwroot\aspnet_client\HttpProxy.aspx	Carbon Black
C:\inetpub\wwwroot\aspnet_client\system_web\Atiky8GL.aspx	CrowdStrike
C:\inetpub\wwwroot\aspnet_client\system_web\XhOHA2Z1.aspx	CrowdStrike, Windows Defender
C:\inetpub\wwwroot\aspnet_client\HttpProxy.aspx	Bitdefender
C:\inetpub\wwwroot\aspnet_client\supp0rt.aspx	Bitdefender
C:\inetpub\wwwroot\aspnet_client\HttpProxy.aspx	Bitdefender
C:\inetpub\wwwroot\aspnet_client\HttpProxy.aspx	Bitdefender
C:\inetpub\wwwroot\aspnet_client\system_web\qFmgfyuB.aspx	
C:\inetpub\wwwroot\aspnet_client\supp0rt.aspx	SentinelOne, Bitdefender
C:\inetpub\wwwroot\aspnet_client\system_web\LGgpxTsQ.aspx	ThreatLocker, Cylance

Figure 6: Malicious implants/webshells deployed as part of the massive Exchange server attack campaign [5]

- Different persistence mechanisms were used for different victims. For example, in some of the reported variants, the persistence was accomplished through the use of Scheduled Tasks (MITRE ATT&CK T1053) executed with the name of "Winnet" and SYSTEM privileges.
- The attackers attempted to dump credentials using different methods, including direct lsass dumps via native comsvcs.dll using rundll32 for additional covertness. [8]:

  powershell rundll32.exe c:\windows\system32\comsvcs.dll MiniDump 520 c:\inetpub\wwwroot\aspnet_client\[...].tmp.dmp full

- This is typically followed by internal recon, archiving, and exfiltrating the stolen data:

  makecab c:\inetpub\wwwroot\aspnet_client\[...].tmp.dmp c:\inetpub\wwwroot\aspnet_client\[...].dmp.zip

  dsquery * -limit 0 -filter objectCategory=person -attr * -uco c:\inetpub\wwwroot\aspnet_client\[...].tmp

- Attackers used different initial discovery approaches and tools which need to be factored into the detection strategy. For instance, one of such tools observed was customized PingCastle (https://github.com/vletoux/pingcastle/blob/master/Scanners/ms17_010scanner.cs).
- There are variants of attacks that involved multiple stagers (see Figure 7).

Detection - Sample Spotter Search Queries - HAFNIUM/ProxyLogon Exchange Servers Attacks Malicious Activity

Below are a few examples of the Spotter queries to assist with initial threat hunting/retrohunting and identifying some possible post-exploitation attack behaviors based on the details above.

Note: Because of the rapidly changing attack landscape, the recommendation is not to rely on static IOAs/queries and to implement the use cases/predictive indicators for the best possible protection (see next section).

Web server/IIS
rg_functionality = “Web Server” AND message CONTAINS “Set-” AND message CONTAINS “VirtualDirectory”

Scheduled tasks
rg_functionality = “Endpoint Management Systems” and baseeventid=1 and destinationprocessname=”schtasks.exe” and resourcecustomfield1 contains “powershell”

Powershell
rg_functionality = “Microsoft Windows Powershell” and baseeventid=4104 and (message contains “Get-MessageTrackingLog” or message contains “MailboxExportRequest”)
rg_functionality = “Microsoft Windows Powershell” and baseeventid=4104 and message contains “Remove-MailboxExportRequest” and message contains “-Confirm:$False”
rg_functionality = “Microsoft Windows Powershell” and baseeventid=4104 and message contains “ComObject” and message contains “Schedule.Service”

Covert Exchange Mailbox Export
rg_functionality = “Microsoft Windows Powershell” AND baseeventid = “4104” AND (message CONTAINS “Microsoft.Exchange.Management.Powershell.Snapin” OR message CONTAINS “New-MailboxExportRequest”)

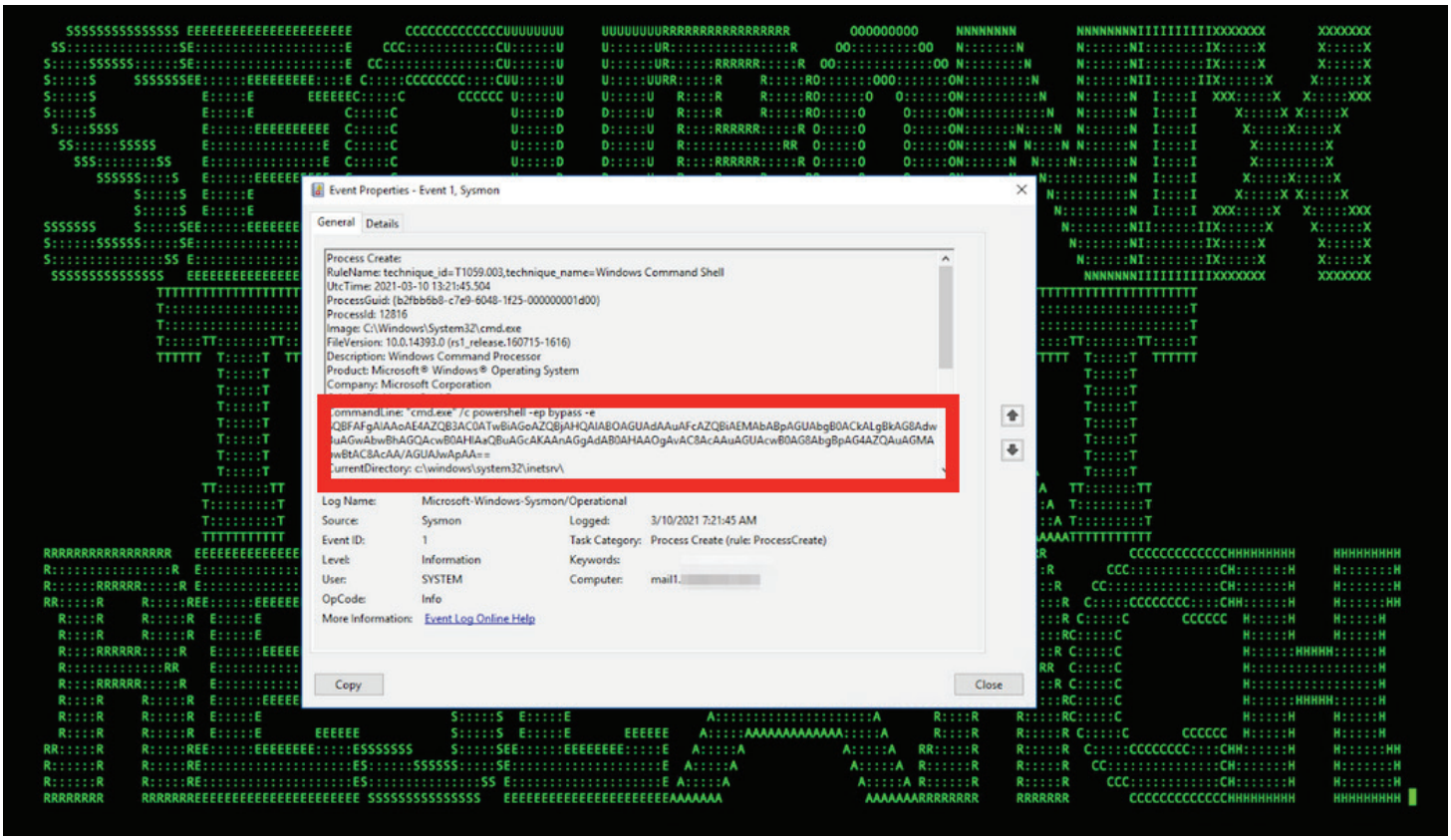

Figure 7: One of stagers used by HAFNIUM/Exchange attacks in logs

Endpoint
# Chopper artifacts
rg_functionality = “Endpoint Management Systems” AND baseeventid = “1” AND destinationprocessname ENDS WITH “cmd.exe” AND resourcecustomfield1 CONTAINS “echo [S]&cd&echo [E]”
# Bitsadmin staging
rg_functionality = “Endpoint Management Systems” and baseeventid=1 and destinationprocessname=”bitsadmin.exe” and resourcecustomfield1 contains “getfile” and resourcecustomfield1 contains “rawreturn”

# NTDS.dit via LOLBINS ntdsutil.exe/diskshadow.exe
rg_functionality = “Endpoint Management Systems” and baseeventid=1 and (destinationprocessname=”ntdsutil.exe” or destinationprocessname=”diskshadow.exe”)

rg_functionality = “Endpoint Management Systems” AND baseeventid = “11” AND (filepath CONTAINS “inetpub\wwwroot” OR filepath CONTAINS “FrontEnd\HttpProxy”) AND (filepath ENDS

WITH ".aspx" OR filepath ENDS WITH ".dll" OR filepath ENDS WITH ".asmx" OR filepath ENDS WITH ".asax") | rare filepath

# Minidump via comsvcs
rg_functionality = "Endpoint Management Systems" AND baseeventid = "1" AND destinationprocessname ENDS WITH "rundll32.exe" AND resourcecustomfield1 CONTAINS "comsvcs.dll" AND resourcecustomfield1 CONTAINS "minidump"

# covertness
rg_functionality = "Endpoint Management Systems" AND baseeventid = "1" AND (sourceprocessname ENDS WITH "UMWorkerProcess.exe" OR sourceprocessname ENDS WITH "UMService.exe") AND ((destinationprocessname NOT ENDS WITH "werfault.exe" OR destinationprocessname NOT ENDS WITH "wermgr.exe"))

# w3wp activity
rg_functionality = "Endpoint Management Systems" AND baseeventid = "1" AND sourceprocessname ENDS WITH "w3wp.exe" | rare destinationprocessname

rg_functionality = "Endpoint Management Systems" AND baseeventid = "1" AND sourceprocessname ENDS WITH "w3wp.exe" AND resourcecustomfield2 CONTAINS "MSExchange" AND resourcecustomfield2 CONTAINS "AppPool" AND (destinationprocessname ENDS WITH "cmd.exe" OR destinationprocessname ENDS WITH "powershell.exe" OR destinationprocessname ENDS WITH "pwsh.exe")

rg_functionality = "Endpoint Management Systems" AND baseeventid = "1" AND destinationprocessname ENDS WITH "procdump.exe" AND resourcecustomfield1 CONTAINS " -ma "

rg_functionality = "Endpoint Management Systems" AND baseeventid = "1" AND resourcecustomfield1 CONTAINS "vssadmin" AND resourcecustomfield1 CONTAINS "Temp__ output"

rg_functionality = "Endpoint Management Systems" AND baseeventid = "1" AND filepath CONTAINS "ProgramData\VSPerfMon"

rg_functionality = "Endpoint Management Systems" AND baseeventid = "11" AND (destinationprocessname = "umworkerprocess.exe" OR destinationprocessname = "UMService.exe") AND (resourcecustomfield5 ENDS WITH ".php" OR resourcecustomfield5 ENDS WITH ".jsp" OR resourcecustomfield5 ENDS WITH ".js" OR resourcecustomfield5 ENDS WITH ".aspx" OR resourcecustomfield5 ENDS WITH ".asmx" OR resourcecustomfield5 ENDS WITH ".asax" OR resourcecustomfield5 ENDS WITH ".cfm" OR resourcecustomfield5 ENDS WITH ".shtml")

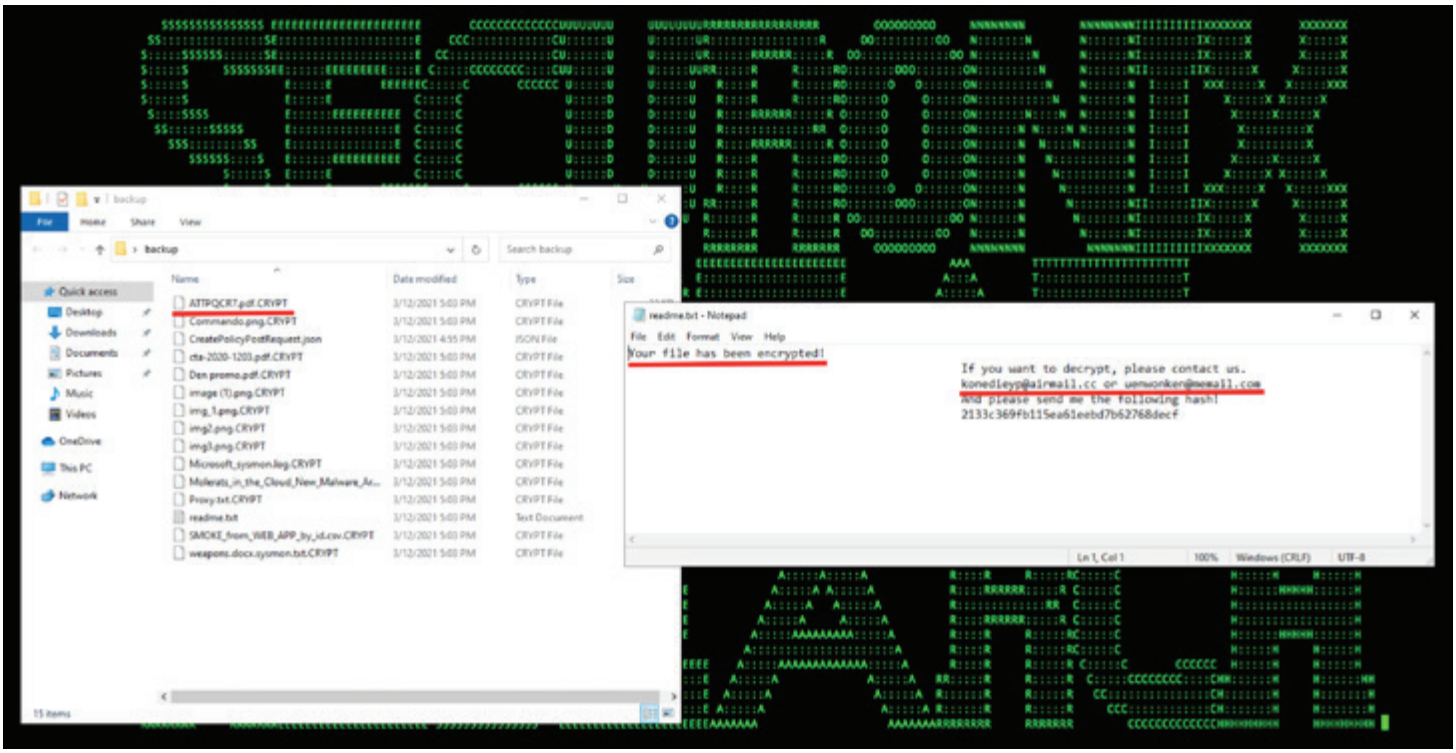

Figure 8: DearCry Ransomware Implant Leveraging HAFNIUM/Exchange exploit

(rg_functionality = “Microsoft Windows” OR rg_functionality = “Endpoint Management Systems”) AND (baseeventid = “1” OR baseeventid = “4688”) AND (sourceprocessname = “UMService.exe” OR sourceprocessname = “umworkerprocess.exe”)

((baseeventid = “1” OR baseeventid = “4688”) AND (rg_functionality = “Microsoft Windows” OR rg_functionality = “Endpoint Management Systems”) AND (destinationprocessname = “cmd.exe” OR destinationprocessname = “powershell.exe” OR destinationprocessname = “powershell_ise.exe”) AND (resourcecustomfield1 CONTAINS “System.Net.Sockets.TCPClient”))
((baseeventid = “1” OR baseeventid = “4688”) AND (rg_functionality = “Microsoft Windows” OR rg_functionality = “Endpoint Management Systems”) AND (destinationprocessname = “cmd.exe” OR destinationprocessname = “powershell.exe” OR destinationprocessname = “powershell_ise.exe”)

AND (resourcecustomfield1 CONTAINS “powercat.ps1”))

((rg_functionality = “Web Server” OR rg_functionality = “Web Proxy”) AND (requesturl CONTAINS “/owa/auth/Current/themes/resources”) AND (requestmethod = “POST”))

((rg_functionality = “Web Server” OR rg_functionality = “Web Proxy”) AND (requesturl CONTAINS “/owa/auth/Current” OR requesturl CONTAINS “/ecp/default.flt” OR requesturl CONTAINS “/ecp/main.css”) AND (requestmethod = “POST”))

Mitigation and Prevention - Securonix Recommendations

Here are our recommendations to help customers prevent and/or mitigate the attacks:

1. Follow the mitigation/response guidance in the CISA advisory: https://us-cert.cisa.gov/ncas/alerts/aa21-062a
2. Apply the patches released by Microsoft - https://techcommunity.microsoft.com/t5/exchange-team-blog/released-march-2021-exchange-server-security-updates/ba-p/2175901
3. Run the latest Microsoft Support Emergency Response Tool https://github.com/microsoft/CSS-Exchange/blob/main/Security/Defender-MSERT-Guidance.md checks
4. Assume your Exchange servers are breached even if you applied the Microsoft patch in a timely manner. Then, retro-hunt for possible signs of compromise from at least Jan 1, 2021 onwards.
5. If you have not already, backup any data stored on your Exchange servers immediately and closely review the baselines in the context of your environment - https://github.com/microsoft/CSS-Exchange/blob/main/Security/src/Baselines/baseline_15.0.1044.25.csv
6. Review your third-party vendor ecosystem for possible collateral damage. The presence of this vulnerability, within your third-party vendor ecosystem, can pose a threat to your environment(s) as well.
7. Restrict web access to your Exchange Servers to only trusted, internal IPs, and/or place it behind a 2FA VPN which can only be accessed by authenticated clients. Disable Outlook Web Access and related public-facing ports, if feasible.

Detection – Securonix Behavior Analytics/Security Analytics

Here are some examples of some of the relevant Securonix behavior analytics/predictive indicators to increase the chances of early detection of the malicious activity associated with the SolarWinds/ECLIPSER MTA including potential future variants of attacks:

- Possible Webshell Creation In Rare Location Analytic
- China Chopper Web Shell Analytic

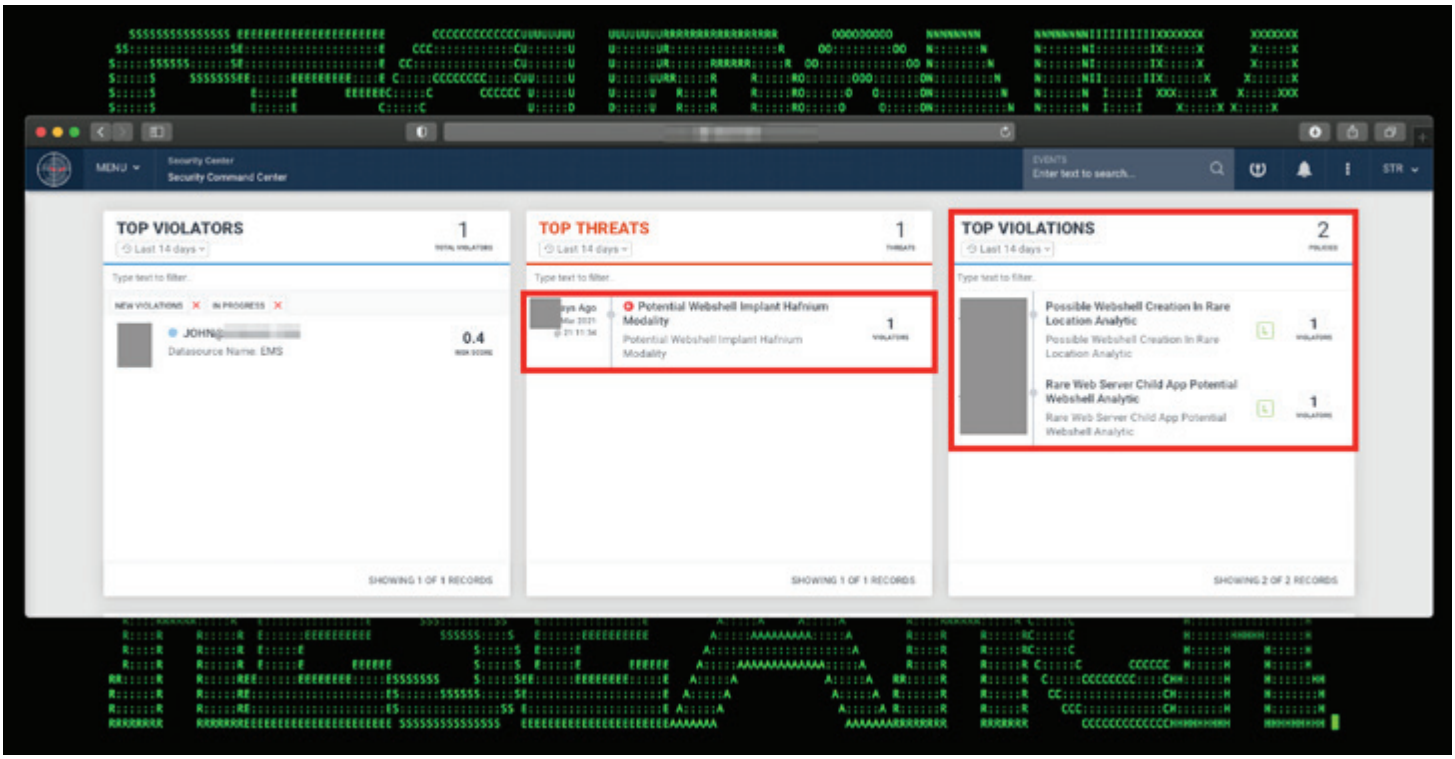

Figure 9: Example of malicious HAFNIUM activity detection in Securonix Labs

- Microsoft Exchange VirtualDirectory Modification Analytic
- Process Dump Using Service DLL CommandLine Analytic
- Microsoft Exchange Unified Messaging Service Suspicious Child Process Analytic
- Microsoft Exchange Suspicious Child Process Analytic
- Powershell Microsoft Exchange Snapin CommandLine Analytics
- Possible DearCry Ransomware File Encryption Analytic
- Potential HAFNIUM Malicious Group ASPX Page Attribute Changes Analytic,
- and a number of others, including EDR-SYM154-RUN, WEL-TAR45-RUN, WEL-TAR40-RUN, EDR-SYM79-ERI, and others.

References

1. [1] Microsoft Threat Intelligence Center (MSTIC). HAFNIUM targeting Exchange Servers with 0-day exploits. March 8, 2021. https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

2. [2] Oleg Kolesnikov. Threats from the Wild - Episode 1: Detecting Future Variants of Sunburst. March 11, 2021. https://www.securonix.com/securonix-threat-research-lab/

3. [3] Brain Krebs. At Least 30,000 U.S. Organizations Newly Hacked Via Holes in Microsoft's Email Software. March 5, 2021. https://krebsonsecurity.com/tag/hafnium/

4. [4] Cyberwire. DearCry ransomware hits vulnerable Exchange Servers. https://thecyberwire.com/newsletters/daily-briefing/10/48

5. [5] Kyle Hanslovan. Huntress. March 3, 2021. https://twitter.com/kylehanslovan?lang=en

6. [6] Unit42. Hunting for the Recent Attacks Targeting Microsoft Exchange. March 3, 2021.https://blog.paloaltonetworks.com/security-operations/attacks-targeting-microsoft-exchange/

7. [7] Tony Lee et al. Breaking Down the China Chopper Web Shell. https://www.fireeye.com/blog/threat-research/2013/08/breaking-down-the-china-chopper-web-shell-part-ii.html

8. [8] Lawrence Abrams. Bleeping Computer: Chile's bank regulator shares IOCs after Microsoft Exchange hack. March 17, 2021. https://www.bleepingcomputer.com/news/security/chiles-bank-regulator-shares-iocs-after-microsoft-exchange-hack/

About Securonix

Securonix is redefining SIEM for today's hybrid cloud, data-driven enterprise. Built on big data architecture, Securonix delivers SIEM, UEBA, SOAR, Security Data Lake, NTA, and vertical-specific applications as a pure SaaS solution with unlimited scalability and no infrastructure cost. Securonix reduces noise, prioritizes high fidelity alerts, and detects and responds to advanced insider and cyber threats with behavioral analytics technology that pioneered the UEBA category.

Contact Securonix

www.securonix.com
info@securonix.com | (310) 641-1000

0321


SECURONIX™