#StopRansomware: Black Basta

cisa.gov/news-events/cybersecurity-advisories/aa24-131a

Actions for critical infrastructure organizations to take today to mitigate cyber threats from ransomware:

1. Install updates for operating systems, software, and firmware as soon as they are released.
2. Require phishing-resistant MFA for as many services as possible.
3. Train users to recognize and report phishing attempts.

SUMMARY

***Note**: This joint Cybersecurity Advisory (CSA) is part of an ongoing #StopRansomware effort to publish advisories for network defenders that detail various ransomware variants and ransomware threat actors. These #StopRansomware advisories include recently and historically observed tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help organizations protect against ransomware. Visit stopransomware.gov to see all #StopRansomware advisories and to learn more about other ransomware threats and no-cost resources.*

The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), Department of Health and Human Services (HHS), and Multi-State Information Sharing and Analysis Center (MS-ISAC) (hereafter referred to as the authoring organizations) are releasing this joint CSA to provide information on Black Basta, a ransomware variant whose actors have encrypted and stolen data from at least 12 out of 16 critical infrastructure sectors, including the Healthcare and Public Health (HPH) Sector.

This joint CSA provides TTPs and IOCs obtained from FBI investigations and third-party reporting. Black Basta is considered a ransomware-as-a-service (RaaS) variant and was first identified in April 2022. Black Basta affiliates have impacted a wide range of businesses and critical infrastructure in North America, Europe, and Australia. As of May 2024, Black Basta affiliates have impacted over 500 organizations globally.

Black Basta affiliates use common initial access techniques—such as phishing and exploiting known vulnerabilities—and then employ a double-extortion model, both encrypting systems and exfiltrating data. Ransom notes do not generally include an initial ransom demand or payment instructions. Instead, the notes provide victims with a unique code and instructs them to contact the ransomware group via a `.onion` URL (reachable through the Tor browser). Typically, the ransom notes give victims between 10 and 12 days to pay the ransom before the ransomware group publishes their data on the Black Basta TOR site, Basta News.

Healthcare organizations are attractive targets for cybercrime actors due to their size, technological dependence, access to personal health information, and unique impacts from patient care disruptions. The authoring organizations urge HPH Sector and all critical infrastructure organizations to apply the recommendations in the Mitigations section of this CSA to reduce the likelihood of compromise from Black Basta and other ransomware attacks. Victims of ransomware should report the incident to their local FBI field office or CISA (see the Reporting section for contact information).

Download the PDF version of this report:

AA24-131A #StopRansomware: Black Basta (PDF, 613.49 KB)
For a downloadable copy of IOCs, see:

AA24-131A STIX XML (XML, 237.45 KB)
AA24-131A STIX JSON (JSON, 180.78 KB)

TECHNICAL DETAILS

Note: This advisory uses the MITRE ATT&CK for Enterprise framework, version 15. See the MITRE ATT&CK Tactics and Techniques section for a table of the threat actors' activity mapped to MITRE ATT&CK® tactics and techniques. For assistance with mapping malicious cyber activity to the MITRE ATT&CK framework, see CISA and MITRE ATT&CK's Best Practices for MITRE ATT&CK Mapping and CISA's Decider Tool.

Initial Access

Black Basta affiliates primarily use spearphishing [T1566] to obtain initial access. According to cybersecurity researchers, affiliates have also used Qakbot during initial access.[1]

Starting in February 2024, Black Basta affiliates began exploiting ConnectWise vulnerability CVE-2024-1709 [CWE-288] [T1190]. In some instances, affiliates have been observed abusing valid credentials [T1078].

Discovery and Execution

Black Basta affiliates use tools such as SoftPerfect network scanner (`netscan.exe`) to conduct network scanning. Cybersecurity researchers have observed affiliates conducting reconnaissance using utilities with innocuous file names such as `Intel` or `Dell`, left in the root drive `C:\` [T1036].[1]

Lateral Movement

Black Basta affiliates use tools such as BITSAdmin and PsExec, along with Remote Desktop Protocol (RDP), for lateral movement. Some affiliates also use tools like Splashtop, Screen Connect, and Cobalt Strike beacons to assist with remote access and lateral movement.

Privilege Escalation and Lateral Movement

Black Basta affiliates use credential scraping tools like Mimikatz for privilege escalation. According to cybersecurity researchers, Black Basta affiliates have also exploited ZeroLogon (CVE-2020-1472, [CWE-330]), NoPac (CVE-2021-42278 [CWE-20] and CVE-2021-42287 [CWE-269]), and PrintNightmare (CVE-2021-34527, [CWE-269]) vulnerabilities for local and Windows Active Domain privilege escalation [T1068].[1], [2]

Exfiltration and Encryption

Black Basta affiliates use RClone to facilitate data exfiltration prior to encryption. Prior to exfiltration, cybersecurity researchers have observed Black Basta affiliates using PowerShell [T1059.001] to disable antivirus products, and in some instances, deploying a tool called Backstab, designed to disable endpoint detection and response (EDR) tooling [T1562.001].[3] Once antivirus programs are terminated, a ChaCha20 algorithm with an RSA-4096 public key fully encrypts files [T1486]. A `.basta` or otherwise random file extension is added to file names and a ransom note titled `readme.txt` is left on the compromised system.[4] To further inhibit system recovery, affiliates use the `vssadmin.exe` program to delete volume shadow copies [T1490].[5]

Leveraged Tools

See Table 1 for publicly available tools and applications used by Black Basta affiliates. This includes legitimate tools repurposed for their operations.

Disclaimer: Use of these tools and applications should not be attributed as malicious without analytical evidence to support threat actor use and/or control.

Tool Name	Description
BITSAdmin	A command-line utility that manages downloads/uploads between a client and server by using the Background Intelligent Transfer Service (BITS) to perform asynchronous file transfers.
Cobalt Strike	A penetration testing tool used by security professions to test the security of networks and systems. Black Basta affiliates have used it to assist with lateral movement and file execution.
Mimikatz	A tool that allows users to view and save authentication credentials such as Kerberos tickets. Black Basta affiliates have used it to aid in privilege escalation.
PSExec	A tool designed to run programs and execute commands on remote systems.
PowerShell	A cross-platform task automation solution made up of a command-line shell, a scripting language, and a configuration management framework, which runs on Windows, Linux, and macOS.
RClone	A command line program used to sync files with cloud storage services such as Mega.
SoftPerfect	A network scanner (`netscan.exe`) used to ping computers, scan ports, discover shared folders, and retrieve information about network devices via Windows Management Instrumentation (WMI), Simple Network Management Protocol (SNMP), HTTP, Secure Shell (SSH) and PowerShell. It also scans for remote services, registry, files, and performance counters.
ScreenConnect	Remote support, access, and meeting software that allows users to control devices remotely over the internet.
Splashtop	Remote desktop software that allows remote access to devices for support, access, and collaboration.
WinSCP	Windows Secure Copy is a free and open source SSH File Transfer Protocol, File Transfer Protocol, WebDAV, Amazon S3, and secure copy protocol client. Black Basta affiliates have used it to transfer data from a compromised network to actor-controlled accounts.

Table 1: Tools Used by Black Basta Affiliates

MITRE ATT&CK TACTICS AND TECHNIQUES

See Tables 2–6 for all referenced threat actor tactics and techniques in this advisory.

Technique Title	ID	Use
Phishing	T1566	Black Basta affiliates have used spearphishing emails to obtain initial access.
Exploit Public-Facing Application	T1190	Black Basta affiliates have exploited ConnectWise vulnerability CVE-2024-1709 to obtain initial access.

Table 2: Black Basta ATT&CK Techniques for Initial Access

Technique Title	ID	Use
Exploitation for Privilege Escalation	T1068	Black Basta affiliates have used credential scraping tools like Mimikatz, Zerologon, NoPac and PrintNightmare for privilege escalation.

Table 3: Black Basta ATT&CK Techniques for Privilege Escalation

Technique Title	ID	Use
Masquerading	T1036	Black Basta affiliates have conducted reconnaissance using utilities with innocuous file names, such as `Intel` or `Dell`, to evade detection.
Impair Defenses: Disable or Modify Tools	T1562.001	Black Basta affiliates have deployed a tool called Backstab to disable endpoint detection and response (EDR) tooling. Black Basta affiliates have used PowerShell to disable antivirus products.

Table 4: Black Basta ATT&CK Techniques for Defense Evasion

Technique Title	ID	Use
Command and Scripting Interpreter: PowerShell	T1059.001	Black Basta affiliates have used PowerShell to disable antivirus products.

Table 5: Black Basta ATT&CK Techniques for Execution

Technique Title	ID	Use
Inhibit System Recovery	T1490	Black Basta affiliates have used the vssadmin.exe program to delete shadow copies.
Data Encrypted for Impact	T1486	Black Basta affiliates have used a public key to fully encrypt files.

Table 6: Black Basta ATT&CK Techniques for Impact

INDICATORS OF COMPROMISE

See Table 7 for IOCs obtained from FBI investigations.

Hash	Description
0112e3b20872760dda5f658f6b546c85f126e803e27f0577b294f335ffa5a298	rclone.exe
d3683beca3a40574e5fd68d30451137e4a8bbaca8c428ebb781d565d6a70385e	Winscp.exe
88c8b472108e0d79d16a1634499c1b45048a10a38ee799054414613cc9dccccc	DLL
58ddbea084ce18cfb3439219ebcf2fc5c1605d2f6271610b1c7af77b8d0484bd	DLL
39939eacfbc20a2607064994497e3e886c90cd97b25926478434f46c95bd8ead	DLL
5b2178c7a0fd69ab00cef041f446e04098bbb397946eda3f6755f9d94d53c221	DLL
51eb749d6cbd08baf9d43c2f83abd9d4d86eb5206f62ba43b768251a98ce9d3e	DLL
d15bfbc181aac8ce9faa05c2063ef4695c09b718596f43edc81ca02ef03110d1	DLL
5942143614d8ed34567ea472c2b819777edd25c00b3e1b13b1ae98d7f9e28d43	DLL
05ebae760340fe44362ab7c8f70b2d89d6c9ba9b9ee8a9f747b2f19d326c3431	DLL
a7b36482ba5bca7a143a795074c432ed627d6afa5bc64de97fa660faa852f1a6	DLL
86a4dd6be867846b251460d2a0874e6413589878d27f2c4482b54cec134cc737	DLL
07117c02a09410f47a326b52c7f17407e63ba5e6ff97277446efc75b862d2799	DLL
96339a7e87ffce6ced247feb9b4cb7c05b83ca315976a9522155bad726b8e5be	ELF
1c1b2d7f790750d60a14bd661dae5c5565f00c6ca7d03d062adcecda807e1779	ELF
360c9c8f0a62010d455f35588ef27817ad35c715a5f291e43449ce6cb1986b98	ELF
0554eb2ffa3582b000d558b6950ec60e876f1259c41acff2eac47ab78a53e94a	EXE

Hash	Description
9a55f55886285eef7ffabdd55c0232d1458175b1d868c03d3e304ce7d98980bc	EXE
62e63388953bb30669b403867a3ac2c8130332cf78133f7fd4a7f23cdc939087	EXE
7ad4324ea241782ea859af12094f89f9a182236542627e95b6416c8fb9757c59	EXE
350ba7fca67721c74385faff083914ecdd66ef107a765dfb7ac08b38d5c9c0bd	EXE
90ba27750a04d1308115fa6a90f36503398a8f528c974c5adc07ae8a6cd630e7	EXE
fafaff3d665b26b5c057e64b4238980589deb0dff0501497ac50be1bc91b3e08	EXE
acb60f0dd19a9a26aaaefd3326db8c28f546b6b0182ed2dcc23170bcb0af6d8f	EXE
d73f6e240766ddd6c3c16eff8db50794ab8ab95c6a616d4ab2bc96780f13464d	EXE
f039eaaced72618eaba699d2985f9e10d252ac5fe85d609c217b45bc8c3614f4	EXE
723d1cf3d74fb3ce95a77ed9dff257a78c8af8e67a82963230dd073781074224	EXE
ae7c868713e1d02b4db60128c651eb1e3f6a33c02544cc4cb57c3aa6c6581b6e	EXE
fff35c2da67eef6f1a10c585b427ac32e7f06f4e4460542207abcd62264e435f	EXE
df5b004be71717362e6b1ad22072f9ee4113b95b5d78c496a90857977a9fb415	EXE
462bbb8fd7be98129aa73efa91e2d88fa9cafc7b47431b8227d1957f5d0c8ba7	EXE
3c50f6369f0938f42d47db29a1f398e754acb2a8d96fd4b366246ac2ccbe250a	EXE
5d2204f3a20e163120f52a2e3595db19890050b2faa96c6cba6b094b0a52b0aa	EXE
37a5cd265f7f555f2fe320a68d70553b7aa9601981212921d1ac2c114e662004	EXE
3090a37e591554d7406107df87b3dc21bda059df0bc66244e8abef6a5678af35	EXE
17879ed48c2a2e324d4f5175112f51b75f4a8ab100b8833c82e6ddb7cd817f20	EXE
42f05f5d4a2617b7ae0bc601dd6c053bf974f9a337a8fcc51f9338b108811b78	EXE
882019d1024778e13841db975d5e60aaae1482fcf86ba669e819a68ce980d7d3	EXE
e28188e516db1bda9015c30de59a2e91996b67c2e2b44989a6b0f562577fd757	EXE
0a8297b274aeab986d6336b395b39b3af1bb00464cf5735d1ecdb506fef9098e	EXE
69192821f8ce4561cf9c9cb494a133584179116cb2e7409bea3e18901a1ca944	EXE
3337a7a9ccdd06acdd6e3cf4af40d871172d0a0e96fc48787b574ac93689622a	EXE
17205c43189c22dfcb278f5cc45c2562f622b0b6280dcd43cc1d3c274095eb90	EXE
b32daf27aa392d26bdf5faafbaae6b21cd6c918d461ff59f548a73d447a96dd9	EXE

Table 7: Malicious Files Associated with Black Basta Ransomware

See Tables 8–11 for IOCs obtained from trusted third-party reporting.

Disclaimer: The authoring organizations recommend network defenders investigate or vet IP addresses prior to taking action, such as blocking, as many cyber actors are known to change IP addresses, sometimes daily, and some IP addresses may host valid domains.

IP Address	Description
66.249.66[.]18	0gpw.588027fa.dns.realbumblebee[.]net, dns.trailshop[.]net, dns.artspathgroupe[.]net
66.249.66[.]18	my.2a91c002002.588027fa.dns.realbumblebee[.]net
66.249.66[.]18	fy9.39d9030e5d3a8e2352daae2f4cd3c417b36f64c6644a783b9629147a1.afd8b8a4615358e0313bad8c544a1af0d8efcec0e8
95.181.173[.]227	adslsdfdsfmo[.]world
	fy9.36c44903529fa273afff3c9b7ef323432e223d22ae1d625c4a3957d57.015c16eff32356bf566c4fd3590c6ff9b2f6e8c587444
207.126.152[.]242	xkpal.d6597fa.dns.blocktoday.net nuher.3577125d2a75f6a277fc5714ff536c5c6af5283d928a66daad6825b9a.7aaf8bba88534e88ec89251c57b01b322c7f52c7f

IP Address	Description
72.14.196[.]50	.rasapool[.]net, dns.trailshop[.]net
72.14.196[.]192	.rasapool[.]net
72.14.196[.]2	.rasapool[.]net
72.14.196[.]226	.rasapool[.]net
46.161.27[.]151	
207.126.152[.]242	nuher.1d67bbcf4.456d87aa6.2d84dfba.dns.specialdrills[.]com
185.219.221[.]136	
64.176.219[.]106	
5.78.115[.]67	your-server[.]de
207.126.152[.]242	xkpal.1a4a64b6.dns.blocktoday[.]net
46.8.16[.]77	
185.7.214[.]79	VPN Server
185.220.100[.]240	Tor exit
107.189.30[.]69	Tor exit
5.183.130[.]92	
185.220.101[.]149	Tor exit
188.130.218[.]39	
188.130.137[.]181	
46.8.10[.]134	
155.138.246[.]122	
80.239.207[.]200	winklen[.]ch
183.181.86[.]147	Xserver[.]jp
34.149.120[.]3	
104.21.40[.]72	
34.250.161[.]149	
88.198.198[.]90	your-server[.]de; literoved[.]ru
151.101.130[.]159	
35.244.153[.]44	
35.212.86[.]55	
34.251.163[.]236	
34.160.81[.]203	
34.149.36[.]179	
104.21.26[.]145	
83.243.40[.]10	
35.227.194[.]51	
35.190.31[.]54	
34.120.190[.]48	
116.203.186[.]178	
34.160.17[.]71	

Filename	Hash
C:\Users\Public\Audio\Jun.exe	b6a4f4097367d9c124f51154d8750ea036a812d5badde0baf9c5f183bb53dd24
C:\Users\Public\Audio\esx.zip	
C:\Users\Public\Audio\7zG.exe	f21240e0bf9f0a391d514e34d4fa24ecb997d939379d2260ebce7c693e55f061
C:\Users\Public\Audio\7z.dll	
C:\Users\Public\db_Usr.sql	8501e14ee6ee142122746333b936c9ab0fc541328f37b5612b6804e6cdc2c2c6
C:\Users\Public\Audio\db_Usr.sql	
C:\Users\Public\Audio\hv2.ps1	
C:\Users\Public\7zG.exe	
C:\Users\Public\7z.dll	
C:\Users\Public\BitLogic.dll	
C:\Users\Public\NetApp.exe	4c897334e6391e7a2fa3cbcbf773d5a4
C:\Users\Public\DataSoft.exe	2642ec377c0cee3235571832cb472870
C:\Users\Public\BitData.exe	b3fe23dd4701ed00d79c03043b0b952e
C:\Users\Public\DigitalText.dll	
C:\Users\Public\GeniusMesh.exe	
\Device\Mup\ {redacted}\C$\Users\Public\Music\PROCEXP.sys	
\Device\Mup\ {redacted}\C$\Users\Public\Music\DumpNParse86.exe	
\Device\Mup\ {redacted}\C$\Users\Public\Music\POSTDump.exe	
\Device\Mup\ {redacted}\C$\Users\Public\Music\DumpNParse.exe	
C:\Users\Public\socksps.ps1	
C:\Users\Public\Thief.exe	034b5fe047920b2ae9493451623633b14a85176f5eea0c7aadc110ea1730ee79
C:\Users\All Users\{redacted}\GWT.ps1 C:\Program Files\MonitorIT\GWT.ps1	8C68B2A794BA3D148CAE91BDF9C8D357289752A94118B5558418A36D95A5A45F
Winx86.exe **Comment:** alias for cmd.exe	
C:\Users\Public\eucr.exe	3c65da7f7bfdaf9acc6445abbedd9c4e927d37bb9e3629f34afc338058680407
C:\Windows\DS_c1.dll	808c96cb90b7de7792a827c6946ff48123802959635a23bf9d98478ae6a259f9
C:\Windows\DS_c1.dll	3a8fc07cadc08eeb8be342452636a754158403c3d4ebff379a4ae66f8298d9a6
C:\Windows\DS_c1.dll	4ac69411ed124da06ad66ee8bfbcea2f593b5b199a2c38496e1ee24f9d04f34a
C:\Windows\DS_c1.dll	819cb9bcf62be7666db5666a693524070b0df589c58309b067191b30480b0c3a
C:\Windows\DS_c1.dll	c26a5cb62a78c467cc6b6867c7093fbb7b1a96d92121d4d6c3f0557ef9c881e0
C:\Windows\DS_c1.dll	d503090431fdd99c9df3451d9b73c5737c79eda6eb80c148b8dc71e84623401f
*\instructions_read_me.txt	

Table 9: File Indicators

Domain	Date/Time (UTC)/Time (UTC)
trailshop[.]net	5/8/2024 6:37
realbumblebee[.]net	5/8/2024 6:37
recentbee[.]net	5/8/2024 6:37
investrealtydom[.]net	5/8/2024 6:37
webnubee[.]com	5/8/2024 6:37
artspathgroup[.]net	5/8/2024 6:37
buyblocknow[.]com	5/8/2024 6:37
currentbee[.]net	5/8/2024 6:37
modernbeem[.]net	5/8/2024 6:37
startupbusiness24[.]net	5/8/2024 6:37
magentoengineers[.]com	5/8/2024 6:37
childrensdolls[.]com	5/8/2024 6:37
myfinancialexperts[.]com	5/8/2024 6:37
limitedtoday[.]com	5/8/2024 6:37
kekeoamigo[.]com	5/8/2024 6:37
nebraska-lawyers[.]com	5/8/2024 6:37
tomlawcenter[.]com	5/8/2024 6:37
thesmartcloudusa[.]com	5/8/2024 6:37
rasapool[.]net	5/8/2024 6:37
artspathgroupe[.]net	5/8/2024 6:37
specialdrills[.]com	5/8/2024 6:37
thetrailbig[.]net	5/8/2024 6:37
consulheartinc[.]com	3/22/2024 15:35
otxcosmeticscare[.]com	3/15/2024 10:14
otxcarecosmetics[.]com	3/15/2024 10:14
artstrailman[.]com	3/15/2024 10:14
ontexcare[.]com	3/15/2024 10:14
trackgroup[.]net	3/15/2024 10:14
businessprofessionalllc[.]com	3/15/2024 10:14
securecloudmanage[.]com	3/7/2024 10:42
oneblackwood[.]com	3/7/2024 10:42
buygreenstudio[.]com	3/7/2024 10:42
startupbuss[.]com	3/7/2024 10:42
onedogsclub[.]com	3/4/2024 18:26
wipresolutions[.]com	3/4/2024 18:26
recentbeelive[.]com	3/4/2024 18:26
trailcocompany[.]com	3/4/2024 18:26
trailcosolutions[.]com	3/4/2024 18:26
artstrailreviews[.]com	3/4/2024 18:26

Domain	Date/Time (UTC)/Time (UTC)
usaglobalnews[.]com	2/15/2024 5:56
topglobaltv[.]com	2/15/2024 5:56
startupmartec[.]net	2/15/2024 5:56
technologgies[.]com	1/2/2024 18:16
jenshol[.]com	1/2/2024 18:16
simorten[.]com	1/2/2024 18:16
investmentgblog[.]net	1/2/2024 18:16
protectionek[.]com	1/2/2024 18:16

Table 10: Known Black Basta Cobalt Strike Domains

airbusco[.]net
allcompanycenter[.]com
animalsfast[.]net
audsystemecll[.]net
auuditoe[.]com
bluenetworking[.]net
brendonline[.]com
businesforhome[.]com
caspercan[.]com
clearsystemwo[.]net
cloudworldst[.]net
constrtionfirst[.]com
erihudeg[.]com
garbagemoval[.]com
gartenlofti[.]com
getfnewsolutions[.]com
getfnewssolutions[.]com
investmendvisor[.]net
investmentrealtyhp[.]net
ionoslaba[.]com
jessvisser[.]com
karmafisker[.]com
kolinileas[.]com
maluisepaul[.]com
masterunix[.]net
monitor-websystem[.]net
monitorsystem[.]net
mytrailinvest[.]net
prettyanimals[.]net

reelsysmoona[.]net
seohomee[.]com
septcntr[.]com
softradar[.]net
startupbizaud[.]net
startuptechnologyw[.]net
steamteamdev[.]net
stockinvestlab[.]net
taskthebox[.]net
trailgroupl[.]net
treeauwin[.]net
unitedfrom[.]com
unougn[.]com
wardeli[.]com
welausystem[.]net
wellsystemte[.]net
withclier[.]com

Table 11: Suspected Black Basta Domains

MITIGATIONS

The authoring organizations recommend all critical infrastructure organizations implement the mitigations below to improve your organization's cybersecurity posture based on Black Basta's activity. These mitigations align with the Cross-Sector Cybersecurity Performance Goals (CPGs) developed by CISA and the National Institute of Standards and Technology (NIST). The CPGs provide a minimum set of practices and protections that CISA and NIST recommend all organizations implement. CISA and NIST based the CPGs on existing cybersecurity frameworks and guidance to protect against the most common and impactful threats, tactics, techniques, and procedures. Visit CISA's Cross-Sector Cybersecurity Performance Goals for more information on the CPGs, including additional recommended baseline protections.

- **Install updates for operating systems, software, and firmware as soon as they are released** [CPG 1.E]. Prioritize updating Known Exploited Vulnerabilities (KEV).
- **Require phishing-resistant multi-factor authentication (MFA)** [CPG 2.H] for as many services as possible.
- **Implement recommendations, including training users to recognize and report phishing attempts** [CPG 2.I], from joint Phishing Guidance: Stopping the Attack Cycle at Phase One.
- **Secure remote access software** by applying mitigations from joint Guide to Securing Remote Access Software.
- **Make backups of critical systems and device configurations** [CPG 2.R] to enable devices to be repaired and restored.
- **Apply mitigations from the joint #StopRansomware Guide**.

The authoring organizations also recommend network defenders of HPH Sector and other critical infrastructure organizations to reference CISA's Mitigation Guide: Healthcare and Public Health (HPH) Sector and HHS's HPH Cybersecurity Performance Goals, which provide best practices to combat pervasive cyber threats against organizations. Recommendations include the following:

- **Asset Management and Security**: Cybersecurity professionals should identify and understand all relationships or interdependencies, functionality of each asset, what it exposes, and what software is running to ensure critical data and systems are protected appropriately. HPH Sector organizations should ensure electronic PHI (ePHI) is protected and compliant with the Health Insurance Portability and Accountability Act (HIPAA). Organizations can complete asset inventories using active scans, passive processes, or a combination of both techniques.
- **Email Security and Phishing Prevention**: Organizations should install modern anti-malware software and automatically update signatures where possible. For additional guidance, see CISA's Enhance Email and Web Security Guide.
    - **Check for embedded or spoofed hyperlinks**: Validate the URL of the link matches the text of the link itself. This can be achieved by hovering your cursor over the link to view the URL of the website to be accessed.

- **Access Management**: Phishing-resistant MFA completes the same process but removes 'people' from the equation to help thwart social engineering scams and targeted phishing attacks that may have been successful using traditional MFA. The two main forms of phishing-resistant MFA are FIDO/Web Authentication (WebAuthn) authentication and Public Key Infrastructure (PKI)-based authentication. Prioritize phishing-resistant MFA on accounts with the highest risk, such as privileged administrative accounts on key assets. For additional information on phishing-resistant MFA, see CISA's Implementing Phishing-Resistant MFA Guide.
- **Vulnerability Management and Assessment**: Once vulnerabilities are identified across your environment, evaluate and prioritize to appropriately deal with the posed risks according to your organization's risk strategy. To assist with prioritization, it is essential to:
    - **Map your assets to business-critical functions.** For vulnerability remediation, prioritize assets that are most critical for ongoing operations or which, if affected, could impact your organization's business continuity, sensitive PII (or PHI) security, reputation, or financial position.
    - **Use threat intelligence information.** For remediation, prioritize vulnerabilities actively exploited by threat actors. To assist, leverage CISA's KEV Catalog and other threat intelligence feeds.
    - **Leverage prioritization methodologies, ratings, and scores**. The Common Vulnerability Scoring System (CVSS) assesses the technical severity of vulnerabilities. The Exploit Prediction Scoring System (EPSS) measures the likelihood of exploitation and can help with deciding which vulnerabilities to prioritize. CISA's Stakeholder-Specific Vulnerability Categorization (SSVC) methodology leverages decision trees to prioritize relevant vulnerabilities into four decisions, Track, Track*, Attend, and Act based on exploitation status, technical impact, mission prevalence, and impacts to safety and public-wellbeing.

VALIDATE SECURITY CONTROLS

In addition to applying mitigations, the authoring organizations recommend exercising, testing, and validating your organization's security program against the threat behaviors mapped to the MITRE ATT&CK for Enterprise framework in this advisory. The authoring organizations recommend testing your existing security controls inventory to assess how they perform against the ATT&CK techniques described in this advisory.

To get started:

1. Select an ATT&CK technique described in this advisory (see Tables 2-6).
2. Align your security technologies against the technique.
3. Test your technologies against the technique.
4. Analyze your detection and prevention technologies' performance.
5. Repeat the process for all security technologies to obtain a set of comprehensive performance data.
6. Tune your security program, including people, processes, and technologies, based on the data generated by this process.

The authoring organizations recommend continually testing your security program, at scale, in a production environment to ensure optimal performance against the MITRE ATT&CK techniques identified in this advisory.

REFERENCES

REPORTING

Your organization has no obligation to respond or provide information back to FBI in response to this joint CSA. If, after reviewing the information provided, your organization decides to provide information to FBI, reporting must be consistent with applicable state and federal laws.

FBI is interested in any information that can be shared, to include boundary logs showing communication to and from foreign IP addresses, a sample ransom note, communications with threat actors, Bitcoin wallet information, decryptor files, and/or a benign sample of an encrypted file.

Additional details of interest include: a targeted company point of contact, status and scope of infection, estimated loss, operational impact, transaction IDs, date of infection, date detected, initial attack vector, and host- and network-based indicators.

FBI, CISA, and HHS do not encourage paying ransom as payment does not guarantee victim files will be recovered. Furthermore, payment may also embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities. Regardless of whether you or your organization have decided to pay the ransom, FBI and CISA urge you to promptly report ransomware incidents to FBI's Internet Crime Complain Center (IC3), a local FBI Field Office, or CISA via the agency's Incident Reporting System or its 24/7 Operations Center (report@cisa.gov or by calling 1-844-Say-CISA [1-844-729-2472]).

DISCLAIMER

The information in this report is being provided "as is" for informational purposes only. FBI, CISA, HHS, and MS-ISAC do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by FBI, CISA, HHS, and MS-ISAC.

VERSION HISTORY

May 10, 2024: Initial version.

This product is provided subject to this Notification and this Privacy & Use policy.