JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

TLP: CLEAR

Product ID: AA23-061A

March 2, 2023

#StopRansomware: BlackSuit (Royal) Ransomware

Summary

Note: This joint Cybersecurity Advisory 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.

Actions for Organizations to Take Today to Mitigate Cyber Threats Related to BlackSuit Ransomware Activity

- Prioritize remediating known exploited vulnerabilities.
- Train users to recognize and report phishing attempts.
- Enable and enforce multifactor authentication.

Note: This advisory, originally published March 2, 2023, has been updated twice:

- **November 13, 2023:** The advisory was updated to share new Royal TTPs and IOCs.
- **August 7, 2024:** The advisory was updated to notify network defenders of the rebrand of "Royal" ransomware actors to "BlackSuit." The update includes new TTPs, IOCs, and detection methods related to BlackSuit ransomware. "Royal" was updated to "BlackSuit" throughout unless referring to legacy Royal activity. Updates and new content are noted.

(New August 7, 2024) The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) are releasing this joint advisory to disseminate known BlackSuit ransomware IOCs and TTPs identified through FBI threat response activities and third-party reporting as recently as of July 2024. BlackSuit ransomware is the evolution of the ransomware previously identified as Royal

To report suspicious or criminal activity related to information found in this joint Cybersecurity Advisory, contact your local FBI field office or CISA's 24/7 Operations Center at Report@cisa.gov or (888) 282-0870. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact.

This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see http://www.cisa.gov/tlp.

ransomware, which was used from approximately September 2022 through June 2023. BlackSuit shares numerous coding similarities with Royal ransomware and has exhibited improved capabilities.

(Updated August 7, 2024) BlackSuit conducts data exfiltration and extortion prior to encryption and then publishes victim data to a leak site if a ransom is not paid. Phishing emails are among the most successful vectors for initial access by BlackSuit threat actors. After gaining access to victims' networks, BlackSuit actors disable antivirus software and exfiltrate large amounts of data before ultimately deploying the ransomware and encrypting the systems.

(Updated August 7, 2024) Ransom demands have typically ranged from approximately $1 million to $10 million USD, with payment demanded in Bitcoin. BlackSuit actors have demanded over $500 million USD in total and the largest individual ransom demand was $60 million. BlackSuit actors have exhibited a willingness to negotiate payment amounts. Ransom amounts are not part of the initial ransom note, but require direct interaction with the threat actor via a `.onion` URL (reachable through the Tor browser) provided after encryption. Recently, an uptick was observed in the number of instances where victims received telephonic or email communications from BlackSuit actors regarding the compromise and ransom. BlackSuit uses a leak site to publish victim data based on non-payment.

FBI and CISA encourage organizations to implement the recommendations found in the Mitigations section of this CSA to reduce the likelihood and impact of ransomware incidents.

For a downloadable copy of IOCs, see:

- AA23-061A STIX XML (NOV 2023 Update)
- AA23-061A STIX JSON (NOV 2023 Update)
- AA23-061A STIX XML (BlackSuit) *(New August 7, 2024)*
- AA23-061A STIX JSON (BlackSuit) *(New August 7, 2024)*

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

BlackSuit uses a unique partial encryption approach that allows the threat actor to choose a specific percentage of data in a file to encrypt. This approach allows the actor to lower the encryption percentage for larger files, which helps evade detection, and also significantly improves ransomware speed.[1] In addition to encrypting files, BlackSuit actors also engage in double extortion tactics in which they threaten to publicly release the exfiltrated data if the victim does not pay the ransom.

BlackSuit actors gain initial access to victim networks in several ways, including:

- **Phishing.** According to third-party reporting, BlackSuit actors most commonly gain initial access to victim networks via phishing emails [T1566].

  - According to open source reporting, victims have unknowingly installed malware that delivers BlackSuit ransomware after receiving phishing emails containing malicious PDF documents [T1566.001] and malvertising [T1566.002].[2]
- **Remote Desktop Protocol (RDP).** The second most common vector (around 13.3% of incidents) BlackSuit actors use for initial access is RDP compromise [T1021.001].
- **Public-facing applications.** FBI has observed BlackSuit actors gain initial access through exploiting vulnerable public-facing applications [T1190].
- **Brokers.** Reports from trusted third-party sources indicate that BlackSuit actors may leverage initial access brokers to gain initial access and source traffic by harvesting virtual private network (VPN) credentials from stealer logs [T1650].

Command and Control

Once BlackSuit actors gain access to a network, they communicate with command and control (C2) infrastructure and download multiple tools [T1105]. Legitimate Windows software is repurposed by BlackSuit actors to strengthen their foothold within the victim's network. Ransomware operators often use open source projects to aid their intrusion activities.

Historically, Royal actors were observed leveraging `Chisel`, Secure Shell (SSH) client, PuTTY, OpenSSH, and MobaXterm [T1572], to communicate with their C2 infrastructure.

Lateral Movement and Persistence

(Updated August 7, 2024) Historically, Royal threat actors used RDP and legitimate operating system (OS) diagnostic tools to move laterally across a network [T1021.001]. BlackSuit actors used RDP and PsExec as well but also use SMB [T1021.001] to move laterally. In one confirmed case, BlackSuit actors used a legitimate admin account [T1078] to remotely log on to the domain controller via SMB. Once on the domain controller, the threat actor deactivated antivirus software [T1562.001] by modifying Group Policy Objects [T1484.001].

(Updated August 7, 2024) FBI observed BlackSuit actors using legitimate remote monitoring and management (RMM) software, to maintain persistence in victim networks [T1133].

(New August 7, 2024) BlackSuit actors use SystemBC and Gootloader malware to load additional tools and maintain persistence.

Discovery and Credential Access

(New August 7, 2024) BlackSuit actors have been observed using SharpShares and SoftPerfect NetWorx to enumerate victim networks. The publicly available credential stealing tool Mimikatz and password harvesting tools from Nirsoft have also been found on victim systems. Tools such as PowerTool and GMER are often used to kill system processes.

Exfiltration

BlackSuit actors exfiltrate data from victim networks by repurposing legitimate cyber penetration testing tools, such as Cobalt Strike, and malware tools/derivatives, such as Ursnif/Gozi, for data aggregation and

exfiltration. According to third-party reporting, BlackSuit actors' first hop in exfiltration and other operations is usually a U.S. IP address.

(New August 7, 2024) BlackSuit actors also use RClone and Brute Ratel for exfiltration.

Encryption

Before starting the encryption process, BlackSuit actors:

- Use Windows Restart Manager to determine whether targeted files are currently in use or blocked by other applications [T1486].[1]
- Use Windows Volume Shadow Copy service (`vssadmin.exe`) to delete shadow copies to inhibit system recovery.[1]

FBI has found numerous batch (`.bat`) files on impacted systems which are typically transferred as an encrypted 7zip file. Batch files create a new admin user [T1078.002], force a group policy update, set pertinent registry keys to auto-extract [T1119] and execute the ransomware, monitor the encryption process, and delete files upon completion—including Application, System, and Security event logs [T1070.001]. Registry Keys created can be modified and deleted to enable persistence on the victim's system.

Malicious files have been found in victim networks in the following directories:

- `C:\Temp\`
- `C:\Users\<user>\AppData\Roaming\`
- `C:\Users\<users>\`
- `C:\ProgramData\`

`Root C:\` directory has also served as a storage location for malicious files. BlackSuit actors have been observed using legitimate software and open source tools during ransomware operations.

Indicators of Compromise (IOC)

See **Table 1** through **Table 5** for Royal ransomware IOCs obtained by FBI during threat response activities as of January 2023.

(New November 13, 2023) See **Table 6** and **Table 7** for Royal and BlackSuit Ransomware IOCs as of June 2023. See Table 8 for a list of legitimate software used by Royal and BlackSuit threat actors identified through FBI investigations as of June 2023.

(New August 7, 2024) See **Table 9** through **Table 15** for BlackSuit ransomware IOCs obtained by FBI during threat response activities as of July 2024 and **Figure 1** for a sample ransom note.

Disclaimer: Some of the observed IP addresses are several years old. FBI and CISA recommend vetting or investigating these IP addresses prior to taking forward-looking action, such as blocking.

Royal IOCs as of January 2023

Table 1: Royal Ransomware Associated Files as of January 2023

IOC	Description
.royal	Encrypted file extension
README.TXT	Ransom note

Table 2: Royal Ransomware Associated IP addresses as of January 2023

Malicious IP	Last Observed Activity
102.157.44[.]105	November 2022
105.158.118[.]241	November 2022
105.69.155[.]85	November 2022
113.169.187[.]159	November 2022
134.35.9[.]209	November 2022
139.195.43[.]166	November 2022
139.60.161[.]213	November 2022
148.213.109[.]165	November 2022
163.182.177[.]80	November 2022
181.141.3[.]126	November 2022
181.164.194[.]228	November 2022
185.143.223[.]69	November 2022
186.64.67[.]6	November 2022
186.86.212[.]138	November 2022
190.193.180[.]228	November 2022
196.70.77[.]11	November 2022

Malicious IP	Last Observed Activity
197.11.134[.]255	November 2022
197.158.89[.]85	November 2022
197.204.247[.]7	November 2022
197.207.181[.]147	November 2022
197.207.218[.]27	November 2022
197.94.67[.]207	November 2022
23.111.114[.]52	November 2022
41.100.55[.]97	November 2022
41.107.77[.]67	November 2022
41.109.11[.]80	November 2022
41.251.121[.]35	November 2022
41.97.65[.]51	November 2022
42.189.12[.]36	November 2022
45.227.251[.]167	November 2022
5.44.42[.]20	November 2022
61.166.221[.]46	November 2022
68.83.169[.]91	November 2022
81.184.181[.]215	November 2022
82.12.196[.]197	November 2022
98.143.70[.]147	November 2022
140.82.48[.]158	December 2022
147.135.36[.]162	December 2022

Malicious IP	Last Observed Activity
147.135.11[.]223	December 2022
152.89.247[.]50	December 2022
172.64.80[.]1	December 2022
179.43.167[.]10	December 2022
185.7.214[.]218	December 2022
193.149.176[.]157	December 2022
193.235.146[.]104	December 2022
209.141.36[.]116	December 2022
45.61.136[.]47	December 2022
45.8.158[.]104	December 2022
5.181.234[.]58	December 2022
5.188.86[.]195	December 2022
77.73.133[.]84	December 2022
89.108.65[.]136	December 2022
94.232.41[.]105	December 2022
47.87.229[.]39	January 2023

Table 3: Royal Ransomware Associated Domains as of January 2023

Malicious Domain	Last Observed Activity
sombrat[.]com	October 2022
gororama[.]com	November 2022
softeruplive[.]com	November 2022
altocloudzone[.]live	December 2022

Malicious Domain	Last Observed Activity
ciborkumari[.]xyz	December 2022
myappearinc[.]com	December 2022
parkerpublic[.]com	December 2022
pastebin.mozilla[.]org/Z54Vudf9/raw	December 2022
tumbleproperty[.]com	December 2022
myappearinc[.]com/acquire/draft/c7lh0s5jv	January 2023

Table 4: Tools Used by Royal Operators

Tool	SHA256
AV tamper	8A983042278BC5897DBCDD54D1D7E3143F8B7EAD553B5A4713E30DEFFDA16375
TCP/UDP Tunnel over HTTP (Chisel)	8a99353662ccae117d2bb22efd8c43d7169060450be413af763e8ad7522d2451
Ursnif/Gozi	be030e685536eb38ba1fec1c90e90a4165f6641c8dc39291db1d23f4ee9fa0b1
Exfil	B8C4AEC31C134ADBDBE8AAD65D2BCB21CFE62D299696A23ADD9AA1DE082C6E20
Remote Access (AnyDesk)	4a9dde3979c2343c024c6eeeddff7639be301826dd637c006074e04a1e4e9fe7
PowerShell Toolkit Downloader	4cd00234b18e04dcd745cc81bb928c8451f6601affb5fa45f20bb11bfb5383ce
PsExec (Microsoft Sysinternals)	08c6e20b1785d4ec4e3f9956931d992377963580b4b2c6579fd9930e08882b1c
Keep Host Unlocked (Don't Sleep)	f8cff7082a936912baf2124d42ed82403c75c87cb160553a7df862f8d81809ee
Ransomware Executable	d47d4b52e75e8cf3b11ea171163a66c06d1792227c1cf7ca49d7df60804a1681

Tool	SHA256
Windows Command Line (NirCmd)	216047C048BF1DCBF031CF24BD5E0F263994A5DF60B23089E393033D17257CB5
System Management (NSudo)	19896A23D7B054625C2F6B1EE1551A0DA68AD25CDDBB24510A3B74578418E618
AV tamper	8A983042278BC5897DBCDD54D1D7E3143F8B7EAD553B5A4713E30DEFFDA16375
TCP/UDP Tunnel over HTTP (Chisel)	8a99353662ccae117d2bb22efd8c43d7169060450be413af763e8ad7522d2451
Ursnif/Gozi	be030e685536eb38ba1fec1c90e90a4165f6641c8dc39291db1d23f4ee9fa0b1
Exfil	B8C4AEC31C134ADBDBE8AAD65D2BCB21CFE62D299696A23ADD9AA1DE082C6E20
Remote Access (AnyDesk)	4a9dde3979c2343c024c6eeeddff7639be301826dd637c006074e04a1e4e9fe7
PowerShell Toolkit Downloader	4cd00234b18e04dcd745cc81bb928c8451f6601affb5fa45f20bb11bfb5383ce
PsExec (Microsoft Sysinternals)	08c6e20b1785d4ec4e3f9956931d992377963580b4b2c6579fd9930e08882b1c
Keep Host Unlocked (Don’t Sleep)	f8cff7082a936912baf2124d42ed82403c75c87cb160553a7df862f8d81809ee
Ransomware Executable	d47d4b52e75e8cf3b11ea171163a66c06d1792227c1cf7ca49d7df60804a1681
Windows Command Line (NirCmd)	216047C048BF1DCBF031CF24BD5E0F263994A5DF60B23089E393033D17257CB5
System Management (NSudo)	19896A23D7B054625C2F6B1EE1551A0DA68AD25CDDBB24510A3B74578418E618

Table 5: Batch Script Tools Used by Royal Operators

File name	Hash Value
2.bat	585b05b290d241a249af93b1896a9474128da969
3.bat	41a79f83f8b00ac7a9dd06e1e225d64d95d29b1d
4.bat	a84ed0f3c46b01d66510ccc9b1fc1e07af005c60
8.bat	c96154690f60a8e1f2271242e458029014ffe30a
kl.bat	65dc04f3f75deb3b287cca3138d9d0ec36b8bea0
gp.bat	82f1f72f4b1bfd7cc8afbe6d170686b1066049bc7e5863b51aa15ccc5c841f58
r.bat	74d81ef0be02899a177d7ff6374d699b634c70275b3292dbc67e577b5f6a3f3c
runanddelete.bat	342B398647073159DFA8A7D36510171F731B760089A546E96FBB8A292791EFEE

Royal and BlackSuit IOCs as of June 2023 (New November 13, 2023)

Table 6: Royal Ransomware Associated Files, Tools, and Hashes as of June 2023

Name	Description or SHA 256 Hash Value
C:\Users\Public\conhost.exe client 149.28.73.161:443 R:149.28.73.161:43657:socks	Executed on the victim's machine, uses a Chisel client to tunnel traffic through port 443 instead of port 43657.
royal_w	Encryption extension
%PROGRAMDATA%	Ransomware Filepath
%TEMP%\execute.bat	
InstallerV20.8.msi	
windows_encryptor.exe	85087f28a84205e344d7e8e06979e6622fab0cfe1759fd24e38cd0390bca5fa6
%PROGRAMDATA%\wine.exe	5b08c02c141eab94a40b56240a26cab7ff07e9a6e760dfde8b8b053a3526f0e6

Name	Description or SHA 256 Hash Value
%USERPROFILE%\Downloads\run1.bat	bc609cf53dde126b766d35b5bcf0a530c24d91fe23633dad6c2c59fd1843f781
%USERPROFILE%\Downloads\run2.bat	13c25164791d3436cf2efbc410caec6b6dd6978d7e83c4766917630e24e1af10
%USERPROFILE%\Downloads\run3.bat	2b93206d7a36cccdf7d7596b90ead301b2ff7e9a96359f39b6ba31bb13d11f45
%USERPROFILE%\Downloads\run4.bat	84e1efbed6bb7720caea6720a8bff7cd93b5d42fb1d71ef8031bfd3897ed4435
%USERPROFILE%\Downloads\sc.bat	e0dbe3a2d07ee10731b68a142c65db077cfb88e5ec5c8415e548d3ede40e7ffc
%USERPROFILE%\Downloads\sr.bat	34a98f2b54ebab999f218b0990665485eb2bb74babdf7e714cc10a306616b00c
runanddelete.bat	342b398647073159dfa8a7d36510171f731b760089a546e96fbb8a292791efee
scripttodo.ps1 (94.232.41.105)	4cd00234b18e04dcd745cc81bb928c8451f6601affb5fa45f20bb11bfb5383ce
dontsleep.exe	f8cff7082a936912baf2124d42ed82403c75c87cb160553a7df862f8d81809ee
wstart.exe	d47d4b52e75e8cf3b11ea171163a66c06d1792227c1cf7ca49d7df60804a1681
InstallerV8.1.ms	3e6e2e0de75896033d91dfd07550c478590ca4cd4598004d9e19246e8a09cb97
shutdowni.bat	8a983042278bc5897dbcdd54d1d7e3143f8b7ead553b5a4713e30deffda16375
f827.exe	5654f32a4f0f2e900a35761e8caf7ef0c50ee7800e0a3b19354b571bc6876f61
d2ef5.exe	be030e685536eb38ba1fec1c90e90a4165f6641c8dc39291db1d23f4ee9fa0b1

Name	Description or SHA 256 Hash Value
f24dc8ea.msi	91605641a4c7e859b7071a9841d1cd154b9027e6a58c20ec4cadafeaf47c9055
defw10.bat	fb638dba20e5fec72f5501d7e0627b302834ec5eaf331dd999763ee925cbc0f9
ll.exe	f0197bd7ccd568c523df9c7d9afcbac222f14d344312322c04c92e7968859726
Royal Ransomware Hash	b987f738a1e185f71e358b02cafa5fe56a4e3457df3b587d6b40e9c9de1da410
b34v2.dll	a51b1f1f0636bff199c0f87e2bb300d42e06698b
1.exe	d93f1ef533e6b8c95330ba0962e3670eaf94a026
34.dll	9e19afc15c5781e8a89a75607578760aabad8e65
ll.exe	9a92b147cad814bfbd4632b6034b8abf8d84b1a5
Royal Ransomware Hash	a4ef01d55e55cebdd37ba71c28b0c448a9c833c0

Table 7: BlackSuit Ransomware Associated Files, Tools, and Hashes as of June 2023

IP Address	MD5 Hash Value
sys32.exe	30cc7724be4a09d5bcd9254197af05e9fab76455
esxi_encryptor	861793c4e0d4a92844994b640cc6bc3e20944a73

BlackSuit threat actors have been observed using legitimate software and open source tools during ransomware operations. Threat actors have been observed using open source network tunneling tools such as Chisel and Cloudflared, as well as Secure Shell (SSH) Client, OpenSSH, and MobaXterm to establish SSH connections. The publicly available credential stealing tool Mimikatz and password harvesting tools from Nirsoft have also been found on victim systems. Legitimate RMM tools have also been observed as backdoor access vectors. Some legitimate software and open source tools can be found in Table 8.

Table 8: Legitimate Files and Tools Used by Royal and BlackSuit Ransomware

Name	Description or SHA 256 Hash Value
C:\Program Files\OpenSSH\ssh-agent.exe C:\Program Files\OpenSSH\sshd.exe	SSH Client
%USERPROFILE%\Downloads\WinRAR.exe	Compression tool
%APPDATA%\MobaXterm\	Toolbox for remote computing
\Program Files (x86)\Mobatek\	Toolbox for remote computing
\Program Files (x86)\Mobatek\MobaXterm\	Toolbox for remote computing
b34v2.dll	ColbaltStrike Beacon
34.dll	CobaltStrike Beacon
mimikatz.exe	Mimikatz credential harvester
dialuppass.exe	Nirsoft password harvesting utility
iepv.exe	Nirsoft password harvesting utility
mailpv.exe	Nirsoft password harvesting utility
netpass.exe	Nirsoft password harvesting utility
routerpassview.exe	Nirsoft password harvesting utility
AdFind.exe	ADFind tool
LogMeIn	Remote access tool
Atera	Remote access tool
C:\Program Files\Eraser\Eraser.exe	Anti-Forensics Tool used by TA
advanced_ip_scanner.exe	Reconnaissance Tool used by TA
conhost.exe (chisel_windows_1_7_7.exe)	b9ef2e948a9b49a6930fc190b22cbdb3571579d37a4de56564e41a2ef736767b

Name	Description or SHA 256 Hash Value
%USERPROFILE%\Downloads\svvhost.exe \Users\Administrator\AppData\Local\Temp \cloudflared.exe	c429719a45ca14f52513fe55320ebc49433c729a0d22234 79d9d43597eab39fa
nircmd.exe	216047c048bf1dcbf031cf24bd5e0f263994a5df60b23089e 393033d17257cb5
nsudo.exe	19896a23d7b054625c2f6b1ee1551a0da68ad25cddbb245 10a3b74578418e618

IOCs as of July 2024 (New August 7, 2024)

Disclaimer: Several of these observed IP addresses were first observed as early as 2023, although the most recent are from July of 2024 and have been historically linked to BlackSuit (formerly known as Royal) Ransomware. IP addresses in this advisory were maliciously used during the time range highlighted below, and may have been used for legitimate purposes outside of that time span. FBI and CISA recommend these IP addresses be investigated or vetted by organizations prior to taking action, such as blocking.

Table 9: Malicious URL (s) associated with BlackSuit Ransomware

URL Association	Malicious URLs
URLs from malicious PowerShell on P0, potentially `debug.ps1`	https://1tvnews[.]af/xmlrpc.php https://avpvuurwerk[.]nl/xmlrpc.php https://beautyhabits[.]gr/xmlrpc.php https://interpolyaris[.]ru/xmlrpc.php https://libertygospeltracts[.]com/xmlrpc.php https://oldtimertreffen-rethem[.]de/xmlrpc.php https://parencyivf[.]com/xmlrpc.php https://pikaluna[.]com/xmlrpc.php https://stroeck[.]at/xmlrpc.php
URL associated to BRC4 / Brute Ratel	megupdate[.]com
URLs associated to Exfiltration	mystuff[.]bublup[.]com backblaze[.]com api[.]backblazeb2[.]com

URL Association	Malicious URLs
URL associated to Cobalt Strike C2	provincial-gaiters-gw[.]aws-use1[.]cloud-ara[.]tyk[.]io
URL associated to Initial Access Download	zoommanager[.]com

Table 10: BlackSuit Ransomware Associated Files and Hash Values

Filename	Hash Value – SHA-256	Description
1.exe	af9f95497b8503af1a399bc6f070c3bbeabc5aeecd8c09bca80495831ae71e61	Encryptor
PowerTool64.exe		Hacktool
aaa.exe	C4A2227CD8D85128EAFEF8EE2298AA105DA892C8B0F37405667C2D1647C35C46	Encryptor
aaa.exe	8d16a23d5a5630502b09c33fbc571d2261c6c98fecc3a79a1e1129354f930d0a	
Wen.exe	01ce9cfebb29596d0ab7c99e8dbadf1a8409750b183e6bf73e0de021b365be13	
etmc.exe	a0a4a99948e12309f54911264261d96f0e40d5fd695bab82e95fbc1f9024482e	
svchost.exe	9bbc9784ce3c818a127debfe710ec6ce21e7c9dd0daf4e30b8506a6dba533db4	Data Exfiltration Tool – Renamed version of `RClone.exe`
locker_N1uYkmEsfoHmT4lK66trUjBuy5gyAj7n.ex_	146335b1be627318ac09476f0c8f8e6e027805e6077673f72d6dce1677a24c78	
socks32.exe	9493b512d7d15510ebee5b300c55b67f9f2ff1dda64bddc99ba8ba5024113300	
C:\users\Administrator\AppData\Local\msa.ps1		SystemBC backdoor
%APPDATA%\Zoom\Alternative Workplace Strategies.js	E813F8FAF3AA2EB20E285596413F5088B2D7FD153FE9F72F3FF45735D0FDDCED	Gootloader infection

Filename	Hash Value – SHA-256	Description
C:\Users\Public\socks.ps1	25A6F82936134A6C5C0066F382530B9D6BF2C8DA6FEAFE028F166B1A9D7283CF	PowerShell Backdoor
HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Run (Value == socks_powershell)		Executes socks.ps1 on reboot
share$.zip	e3d7c012040962acd66f395d1c5c5f73f305aa1058f2111e8e37d9cb213b80c4	Contains `_COPY.bat`, `PsExec.exe`, `etmc.exe`, and `_EXEC.bat` to deploy encryptor (`etmc.exe`) across environment using domain admin credentials
socss.exe	C798B2690C5F16EB2917A679AF3117CFE9C7060FA8BC84FFC3159338EF33508E	Malware
qq.exe	3c8c1b1f53e0767b7291bb1ae605ffa62a93e9c8cc783e4ca47ac84b48320d59	
gomer.exe		A renamed executable of GMER used for defense evasion
288-csrss.exe	ee6ec2810910c6d2a2957f041edd1e39dca4266a1cc8009ae6d7315aba9196f5	
372-winlogon.exe	68c57daed0e5899c49b827042bcf3bbeba33b524bd83315a44d889721664dc34	
776-svchost.exe	bbb7404419f91f82cedfec915931a9339f04165b27d8878d63827c9ee421ed62	
Exe.exe, aaaa.exe, qq.exe	338228a3e79f3993abc102cbac2ff253c84965213d59ac30892538cdd9b0a22b	Ransomware file
Mwntv.sys	6332f189cc71df646ff0f1b9b02a005c9ebda3fe7b9712976660746913b030de	Potential Tool Ingress

Filename	Hash Value – SHA-256	Description
Un_A.exe		Malicious binary for attempting to disable/uninstall security software
Un_B.erxe		Malicious binary for attempting to disable/uninstall security software

Table 11: Batch Script Tools Used by BlackSuit Ransomware Operators and Hash Values

Filename	Description	Hash Value – SHA-256
2.bat	Batch Script to copy and execute encryptor	3041dfc13f356c2f0133a9c11a258f87cb7de1e17bc435e9b623d74bc5e1c6be
C:\share$_EXEC.bat	Execute encrypter	8F87A1542EE790623896BBAAB933D1883484DE02A7B3D65D6C791D50173A923D
fstart.bat	A batch script used to enable remote services, perform anti-forensics, and enable clear-text passwords in memory	
NLA.bat	A batch script used to disable Network Level Authentication (NLA) for Remote Desktop Services (RDS)	
av.bat	A batch script that searches for presence of an application and uninstalls it	
systeminfo.bat	A batch script used for system enumeration	
mv.bat	A batch script used to move the PsExec executable and delete the netscan executable	

Table 12: IP addresses from BlackSuit Ransomware Deployments (from November 2023 to July 2024)

IP Address	Time Range of Use	Description
4.231.128[.]59	July 2024	IP associated to reverse lookup from `Socss.exe`
2.18.121[.]83	July 2024	IP associated to reverse lookup from `Socss.exe`
40.126.31[.]73	July 2024	IP associated to reverse lookup from `Socss.exe`
20.114.59[.]183	July 2024	IP associated to reverse lookup from `Socss.exe`
20.242.39[.]171	July 2024	IP associated to reverse lookup from `Socss.exe`
93.184.221[.]240	July 2024	IP associated to reverse lookup from `Socss.exe`
2.18.121[.]197	July 2024	IP associated to reverse lookup from `Socss.exe`
52.111.229[.]19	July 2024	IP associated to reverse lookup from `Socss.exe`
217.20.59[.]36	July 2024	IP associated to reverse lookup from `Socss.exe`
40.79.189[.]58	July 2024	IP associated to reverse lookup from `Socss.exe`
143[.]244[.]146[.]183:443	May 2024	Unknown C2 – potential SOCKS Proxy
45[.]141[.]87[.]218:9000	May 2024	Arechclient2 Backdoor/SecTopRAT
45[.]141[.]87[.]218:443	May 2024	Arechclient2 Backdoor/SecTopRAT
184.174.96[.]16	May 2024	Associated with download of the binary `vm.dll`
89.251.22[.]32	May 2024	Cobalt Strike
135.148.67[.]84	May 2024	Resolves to domain `turnovercheck[.]com`
180.131.145[.]85	May 2024	Associated with malicious PowerShell execution
180.131.145[.]61	May 2024	SystemBC Command & Control
138.199.53[.]226	Feb 2024	
184.166.211[.]74	Feb 2024	
185.190.24[.]103	Feb 2024	

IP Address	Time Range of Use	Description
5.181.234[.]58	Feb 2024	
137.220.61[.]94	Nov – Feb 2024	connecting outbound from `Socss.exe`
193.37.69[.]116	Nov – Jan 2024	Associated with exfiltration
144.202.120[.]122	Nov 2023	`socks1.ps1` backdoor; SystemBC Backdoor C2; `www.recruitment-interview[.]org` (C2 SystemBC)
104.21.58[.]219:443	Nov 2023	Cobalt Strike
141.98.80[.]181:80	Nov 2023	Cobalt Strike
144.202.120[.]122:433	Nov 2023	PowerShell Reverse Proxy
155.138.150[.]236:8088	Nov 2023	PowerShell Reverse Proxy
140.82.18[.]48	Nov 2023	
141.98.80[.]181	Nov 2023	
44.202.120[.]122	Nov 2023	
45.76.225[.]156	Nov 2023	

Table 13: Legitimate Files and Tools Used by Black Suit Ransomware (1 of 3)

File name	Hash Value – SHA-256	Description
share.exe	f02af8ffc37d1874b971307fdec80e33e583b56d9ebabda78a4b8ad038bc3bf0	Cobalt Strike
181.exe	b028eaa0ec452c6844881dc34be813834813a40591b89ea9a57dd4fb4084e477	Cobalt Strike – File name
222wqc.exe	ae724dce252c7b05a84bc264993172cf86950d22744b5e3a1b15ba645d9d3733	Cobalt Strike
gmer.exe		GMER / Rootkit Hunter
PowerTool64.exe		PowerTool64 for hacking

File name	Hash Value – SHA-256	Description
Psexesvc.exe	141b2190f51397dbd0dfde0e3904b264c91b6f81febc823ff0c33da980b69944	Sysinternals
Socks5.ps1 Socks.ps1	25a6f82936134a6c5c0066f382530b9d6bf2c8da6feafe028f166b1a9d7283cf	PowerShell Reverse Proxy
netscan.exe		A network reconnaissance tool
3iSDtcX.exe	e87512ea12288acec611cf8e995c4ced3971d9e35c0c5dcfd9ee17c9e3ed913d	Putty suite
File.exe	f805dafb3c0b7e18aa7d8c96db8e8d4e9301ff619622d1aecc8080e0ecd9ebbe	Putty.exe. Possibly used for C2
Mwntv.sys	6332f189cc71df646ff0f1b9b02a005c9ebda3fe7b9712976660746913b030de	Potential Tool Ingress
AnyDesk	1cdafbe519f60aaadb4a92e266fff709129f86f0c9ee595c45499c66092e0499	Potential remote access tool
ScreenConnect	420db40d26d309d3dba3245abb91207f1bca050530545a8048f856e5840d22a2	Potential remote access tool
SharpShares.exe		Enumerate network shares
Networx.exe		Bandwidth utilization

Table 14: Legitimate Files and Tools Used by Black Suit Ransomware (2 of 3)

Filename	Hash Value – SHA-1	Description
181[.]exe	790d40cd16fb458bf99e3600bce29eca06d40b56	Cobalt Strike – Host name

Table 15: Legitimate Files and Tools Used by Black Suit Ransomware (3 of 3)

Filename	File Path	Description
Anydesk.exe	C:\Program Files(x86)\AnyDesk\AnyDesk.exe	Remote Monitoring and Management (RMM) Tool

Filename	File Path	Description
ehorus_display.exe	C:\Program Files\ehorus_agent\ehorus_display\ehorus_display.exe	RMM Tool
ehorus_launcher.exe	C:\Program Files\ehorus_agent\ehorus_launcher.exe	RMM Tool

Table 16: Domain(s) associated to BlackSuit Ransomware

Domain Name	Description
Abbeymathiass[.]com	Cobalt Strike C2
Mail.abbeymathiass[.]com	Cobalt Strike C2
Store.abbeymathiass[.]com	Cobalt Strike C2
https://file[.]io/ScPd1KcJTtxO	Associated with download of the binary disabler.exe by threat actors
Mail.turnovercheck[.]com	Cobalt Strike C2
Store.turnovercheck[.]com	Cobalt Strike C2
turnovercheck[.]com	Cobalt Strike C2
Hourlyprofitstore[.]com	Cobalt Strike
IPs and Domains for downloads / C2 / exfiltration of communication	https://protect-us.mimecast[.]com/s/A2PyC31xN5IpzR0XUvzaAj?domain=5.181.157.8 https://protect-us.mimecast[.]com/s/CcsrC4xyO7fBK73ztjNfPl?domain=5.181.234.58 https://protect-us.mimecast[.]com/s/NwueC5yzP5IZLW4MuIfSrc?domain=137.220.61.94 https://protect-us.mimecast[.]com/s/T3InC2kwM5hpzEOVU9S5zn?domain=147.135.36.162 https://protect-us.mimecast[.]com/s/teBrC1wvL8iMNE56tXga0n?domain=147.135.11.223

Table 17: BlackSuit Ransomware Note and Hash Value

File Name	Hash Value	Description
readme.BlackSuit.txt	1743494f803bbcbd11150a4a8b7a2c5faba1223da607f67d24b18ca2d95d5ba3	Ransomware note

Ransom Note (New August 7, 2024)

Figure 1 shows the observed BlackSuit ransom notes delivered to victims.

> Your safety service did a really poor job of protecting your files against our professionals.
>
> Extortioner named BlackSuit has attacked your system.
>
> As a result all your essential files were encrypted and saved at a secure server for further use and publishing on the Web into the public realm.
>
> Now we have all your files like: financial reports, intellectual property, accounting, law actions and complaints, personal files and so on and so forth.
>
> We are able to solve this problem in one touch.
>
> We (BlackSuit) are ready to give you an opportunity to get all the things back if you agree to make a deal with us.
>
> You have a chance to get rid of all possible financial, legal, insurance and many others risks and problems for a quite small compensation.
>
> You can have a safety review of your systems.
>
> All your files will be decrypted, your data will be reset, your systems will stay in safe.
>
> Contact us through TOR browser using the link:

Figure 1. BlackSuit Ransom Note

MITRE ATT&CK Tactics and Techniques

See **Table 18** through **Table 23** for all referenced threat actor tactics and techniques in this advisory, as well as corresponding detection and/or mitigation recommendations. For additional mitigations, see the Mitigations section.

Table 18: BlackSuit Actors ATT&CK Techniques for Resource Development

Technique Title	ID	Use
Acquire Access	T1650	BlackSuit actors may leverage brokers in support of gaining initial access.

Table 19: Cyber Threat Actors ATT&CK Techniques for Initial Access

Technique Title	ID	Use
Remote Services: Remote Desktop Protocol	T1021.001	BlacSuit actors use RDP compromise as secondary initial access vector.
External Remote Services	T1133	BlackSuit actors gain initial access through a variety of RMM software.
Exploit Public Facing Application	T1190	BlackSuit actors gain initial access through public-facing applications.
Phishing	T1566	BlackSuit actors most commonly gain initial access to victim networks via phishing.
Phishing: Spear phishing Attachment	T1566.001	BlackSuit actors used malicious PDF document attachments in phishing campaigns.
Phishing: Spear phishing Link	T1566.002	The actors gain initial access using malvertising links via emails and public-facing sites.

Table 20: Cyber Threat Actors ATT&CK Techniques for Privilege Escalation

Technique Title	ID	Use
(New August 7, 2024) Valid Accounts	T1078	BlackSuit actors used a legitimate admin account to gain access privileges to the domain controller.
Valid Accounts: Domain Accounts	T1078.002	BlackSuit actors used encrypted files to create new admin user accounts.

Table 21: Cyber Threat Actors ATT&CK Techniques for Defense Evasion

Technique Title	ID	Use
Remote Services: Remote Desktop Protocol	T1021.001	BlackSuit actors used valid accounts to move laterally through the domain controller using RDP.
Indicator Removal: Clear Windows Event Logs	T1070.001	BlackSuit actors deleted shadow files and system and security logs after exfiltration.
Automated Collection	T1119	BlackSuit actors used registry keys to auto-extract and collect files.

Technique Title	ID	Use
Domain Policy Modification: Group Policy Modification	T1484.001	BlackSuit actors modified Group Policy Objects to subvert antivirus protocols.
Impair Defenses: Disable or Modify Tools	T1562.001	BlackSuit actors deactivated antivirus protocols.

Table 22: Cyber Threat Actors ATT&CK Techniques for Command and Control

Technique Title	ID	Use
Ingress Tool Transfer	T1105	BlackSuit actors used C2 infrastructure to download multiple tools.
Protocol Tunneling	T1572	BlackSuit actors used an encrypted SSH tunnel to communicate within C2 infrastructure.

Table 23: Cyber Threat Actors ATT&CK Techniques for Impact

Technique Title	ID	Use
Data Encrypted for Impact	T1486	BlackSuit actors encrypted data to determine which files were being used or blocked by other applications.

Detection Methods

(New August 7, 2024) Please reference YARA rule below to aid in detecting BlackSuit activity. **Note:** The YARA rule is derived from FBI investigations and is not guaranteed to detect confirmed malicious activity.

```
private rule is_executable {

   condition:
      uint32(uint32(0x3C)) == 0x00004550

}

rule obfuscates_dlls {

         strings:

                  // Code for unscrambling names of true DLL imports
                  $code_load_obfuscated = {
                                                c6 84 24 ?? 00 00 00 ??
                                                c6 84 24 ?? 00 00 00 ??
                                                c6 84 24 ?? 00 00 00 ??
                                                c6 84 24 ?? 00 00 00 ??
```

```
                                                                        c6 84 24 ?? 00 00 00 ??
                                                                        c6 84 24 ?? 00 00 00 ??
                                                                        c6 84 24 ?? 00 00 00 ??
                                                                        c6 84 24 ?? 00 00 00 ??
                                                                }
                        // c6 84 24 ?? 00 00 00 ??          | MOV byte ptr [ESP + ??], ??

                $code_deobfuscate = { 99 f7 ?? 8d ?? ?? 99 f7 ?? 88}
                        // 99                                       | CDQ
                        // f7 ??                            | IDIV ??
                        // 8d ?? ??                                 | LEA ??, ??
                        // 99                                       | CDQ
                        // f7 ??                            | IDIV ??
                        // 88                                       | MOV

        condition:
                all of them

}
rule calls_rsa_function {

        strings:

                // Code for function calls using RSA key
                $code_rsa_function_1 = { 8d4c2410 6a?? 6a?? 51 6a?? 6a?? 6a?? 68???????? ffd0 }
                        // 8d 4c 24 10                      | LEA ECX, [esp + 0x10]
                        // 6a ??                            | PUSH ??
                        // 6a ??                            | PUSH ??
                        // 51                                       | PUSH ECX
                        // 6a ??                            | PUSH ??
                        // 6a ??                            | PUSH ??
                        // 6a ??                            | PUSH ??
                        // 68 ?? ?? ?? ??                   | PUSH (address of RSA string)
                        // ff d0                            | CALL EAX

                $code_rsa_function_2 = { 8d4c2410 6a?? 6a?? 51 56 6a?? 6a?? 68???????? ffd0 }
                        // 8d 4c 24 10                      | LEA ECX, [esp + 0x10]
                        // 6a ??                            | PUSH ??
                        // 6a ??                            | PUSH ??
                        // 51                                       | PUSH ECX
                        // 56                                       | PUSH ESI
                        // 6a ??                            | PUSH ??
                        // 6a ??                            | PUSH ??
                        // 68 ?? ?? ?? ??                   | PUSH (address of RSA string)
                        // ff d0                            | CALL EAX

        condition:
                any of them

}

rule xor_decoder_functions {

        strings:
```

```
                    // Functions 402e00 and 402f00 both appear to contain a xor-decoding loop

                    // 402e00
                    $code_xor_loop_1 = { 0f a4 ce ?? 0f ac d5 ?? c1 e1 ?? c1 ea ?? 0b cd 0b f2 99 33 c8 }
                              // 0f a4 ce ??                    | SHLD ESI, param_1, ??
                              // 0f ac d5 ??                    | SHRD EBP, EDX, ??
                              // c1 e1 ??                                | SHL param_1, ??
                              // c1 ea ??                                | SHR EDX, 0x19
                              // 0b cd                          | OR param_1, EBP
                              // 0b f2                          | OR ESI, EDX
                              // 99                                      | CDQ
                              // 33 c8                                   | XOR param_1, EAX

                    // 402f00
                    $code_xor_loop_2 = { 0f a4 ce ?? c1 ea ?? 0b f2 c1 e1 ?? 0b c8 0f be c3 8a 1f 99 33 c8 }
                              // 0f a4 ce ??                    | SHLD ESI, param_1, ??
                              // c1 ea ??                                | SHR EDX, ??
                              // 0b f2                          | OR ESI, EDX
                              // c1 e1 ??                                | SHL, param_1, ??
                              // 0b c8                          | OR param_1, EDX
                              // 0f be c3                                | MOVSX EAX, BL
                              // 8a 1f                          | BL, byte ptr [EDI]
                              // 99                                      | CDQ
                              // 33 c8                                   | XOR param_1, EAX

          condition:
             any of them

}

rule win_BlackSuit_manual {

   meta:
      author = "CVH - Raleigh"
      date = "2024-07-12"
      version = "1"
      description = "Detects win.BlackSuit. Rules were manually constructed and results should not be considered
conclusive."
      malpedia_reference = "https://malpedia.caad.fkie.fraunhofer.de/details/win.BlackSuit"

   strings:

                    // Somehow keeps this in plaintext, although in UTF-16
                    $string_readme = "readme.BlackSuit.txt" nocase wide ascii

                    // RSA key for encrypting AES encryption key present in plaintext
                    $string_rsa_key = "BEGIN RSA PUBLIC KEY" nocase wide ascii

                    // Unusual debug strings
                    $string_debug_1 = ".rdata$voltmd"
                    $string_debug_2 = ".rdata$zzzdbg"

                    // Relevant functions calls
                    $import_1 = "MultiByteToWideChar"
                    $import_2 = "EnterCriticalSection"
```

```
                $import_3 = "GetProcessHeap"



    condition:
            (is_executable and $string_readme)

                Or

                ($string_readme and

                        (obfuscates_dlls or calls_rsa_function or xor_decoder_functions)

                )

                or

                2 of (obfuscates_dlls, calls_rsa_function, xor_decoder_functions)

                or

                1 of (obfuscates_dlls, calls_rsa_function, xor_decoder_functions) and any of them

}
```

Mitigations

Network Defenders

The FBI and CISA recommend network defenders implement the mitigations below to improve your organization's cybersecurity posture based on BlackSuit actor'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.

- **Implement a recovery plan** to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, and secure location (i.e., hard drive, storage device, the cloud).
- **Require all accounts** with password logins (e.g., service account, admin accounts, and domain admin accounts) to comply with National Institute for Standards and Technology (NIST) standards for developing and managing password policies.
    - Use longer passwords consisting of at least 8 characters and no more than 64 characters in length;
    - Store passwords in hashed format using industry-recognized password managers;
    - Add password user "salts" to shared login credentials;

  - Avoid reusing passwords;
  - Implement multiple failed login attempt account lockouts;
  - Disable password "hints;"
  - Refrain from requiring password changes more frequently than once per year.
  - **Note:** NIST guidance suggests favoring longer passwords instead of requiring regular and frequent password resets. Frequent password resets are more likely to result in users developing password "patterns" cyber criminals can easily decipher.
  - Require administrator credentials to install software.
- **Keep all operating systems, software, and firmware up to date** [CPG 1.E]**.** Timely patching is one of the most efficient and cost-effective steps an organization can take to minimize its exposure to cybersecurity threats. Prioritize patching known exploited vulnerabilities in internet-facing systems.
- **Require Phishing-Resistant multifactor authentication to administrator accounts** [CPG 2.H]**,** and require standard MFA for all services to the extent possible, particularly for webmail, virtual private networks, and accounts that access critical systems.
- **Segment networks** [CPG 2.F] to prevent the spread of ransomware. Network segmentation can help prevent the spread of ransomware by controlling traffic flows between—and access to—various subnetworks and by restricting adversary lateral movement.
- **Identify, detect, and investigate abnormal activity and potential traversal of the indicated ransomware with a networking monitoring tool** [CPG 3.A]**.** To aid in detecting the ransomware, implement a tool that logs and reports all network traffic, including lateral movement activity on a network. Endpoint detection and response (EDR) tools are particularly useful for detecting lateral connections as they have insight into common and uncommon network connections for each host.
- **Install, regularly update, and enable real time detection for antivirus** software on all hosts.
- **Implement Secure Logging Collection and Storage Practices** [CPG 2.T]**.** Learn more on logging best practices by referencing CISA's Logging Made Easy resources.
- **Review domain controllers, servers, workstations, and active directories** for new and/or unrecognized accounts.
- **Audit user accounts** with administrative privileges and configure access controls according to the principle of least privilege.
- **Disable unused ports.**
- **Implement and Enforce Email Security Policies** [CPG 2.M]**.**
- **Disable Macros by Default** [CPG 2.N]**.**
- **Consider adding an email banner to emails** received from outside your organization.
- **Disable hyperlinks in received emails.**

- **Implement time-based access for accounts set at the admin level and higher.** For example, the Just-in-Time (JIT) access method provisions privileged access when needed and can support enforcement of the principle of least privilege (as well as the Zero Trust model). This is a process where a network-wide policy is set in place to automatically disable admin accounts at the Active Directory level when the account is not in direct need. Individual users may submit their requests through an automated process that grants them access to a specified system for a set timeframe when they need to support the completion of a certain task.
- **Disable command-line and scripting activities and permissions.** Privilege escalation and lateral movement often depend on software utilities running from the command line. If threat actors are not able to run these tools, they will have difficulty escalating privileges and/or moving laterally.
- **Maintain offline backups of data, and regularly maintain backup and restoration [CPG 2.R].** By instituting this practice, the organization ensures they will not be severely interrupted, and/or only have irretrievable data.
- **Ensure all backup data is encrypted,** immutable (i.e., cannot be altered or deleted), and covers the entire organization's data infrastructure.

Software Manufacturers

The above mitigations apply to enterprises and critical infrastructure organizations with on-premises or hybrid environments. Recognizing that insecure software is the root cause of the majority of these flaws and that the responsibility should not be on the end user, CISA urges software manufacturers to implement the following to reduce the prevalence of <identified or exploited issues *(e.g.,* misconfigurations, weak passwords, and other weaknesses identified and exploited through the assessment team)>:

- **Embed security into product architecture** throughout the entire software development lifecycle (SDLC).
- **Mandate MFA, ideally phishing-resistant MFA, for privileged users** and make MFA a default, rather than opt-in, feature.

These mitigations align with tactics provided in the joint guide Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software. CISA urges software manufacturers to take ownership of improving the security outcomes of their customers by applying these and other secure by design tactics. By using secure by design tactics, software manufacturers can make their product lines secure "out of the box" without requiring customers to spend additional resources making configuration changes, purchasing security software and logs, monitoring, and making routine updates.

For more information on secure by design, see CISA's Secure by Design webpage.

Validate Security Controls

In addition to applying mitigations, the FBI and CISA 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 FBI and CISA 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 **Table 18 – Table 23**).

Align your security technologies against the technique.

Test your technologies against the technique.

Analyze your detection and prevention technologies' performance.

Repeat the process for all security technologies to obtain a set of comprehensive performance data.

Tune your security program, including people, processes, and technologies, based on the data generated by this process.

The FBI and CISA 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.

Resources

- Stopransomware.gov is a whole-of-government approach that gives one central location for ransomware resources and alerts.
- Resource to mitigate a ransomware attack: CISA-Multi-State Information Sharing and Analysis Center (MS-ISAC) Joint Ransomware Guide.
  Note: The joint Ransomware Guide provides preparation, prevention, and mitigation best practices as well as a ransomware response checklist.
- No-cost cyber hygiene services: Cyber Hygiene Services and Ransomware Readiness Assessment.

Reporting

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

The 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 BlackSuit 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.

The FBI and CISA 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, the FBI and CISA urge you to promptly report ransomware incidents to the 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

Your organization has no obligation to respond or provide information in response to this product. If, after reviewing the information provided, your organization decides to provide information to the authoring agencies, it must do so consistent with applicable state and federal law.

The information in this report is being provided "as is" for informational purposes only. FBI and CISA 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 and CISA.

Version History

January 31, 2023: Initial Release (Royal Ransomware)

November 13, 2023: First Update (Royal Ransomware)

August 7, 2024: Updated title from "Royal Ransomware" to "BlackSuit Ransomware"; updates noted throughout.