JOINT
CYBERSECURITY
ADVISORY

Product ID: AA22-335A

December 1, 2022

#StopRansomware: Cuba Ransomware

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.

Actions to take today to mitigate cyber threats from ransomware:

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

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) are releasing this joint CSA to disseminate known Cuba ransomware IOCs and TTPs associated with Cuba ransomware actors identified through FBI investigations, third-party reporting, and open-source reporting. This advisory updates the December 2021 FBI Flash: Indicators of Compromise Associated with Cuba Ransomware.

Note: While this ransomware is known by industry as "Cuba ransomware," there is no indication Cuba ransomware actors have any connection or affiliation with the Republic of Cuba.

Since the release of the December 2021 FBI Flash, the number of U.S. entities compromised by Cuba ransomware has doubled, with ransoms demanded and paid on the increase.

This year, Cuba ransomware actors have added to their TTPs, and third-party and open-source reports have identified a possible link between Cuba ransomware actors, RomCom Remote Access Trojan (RAT) actors, and Industrial Spy ransomware actors.

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

To report suspicious or criminal activity related to information found in this joint Cybersecurity Advisory, contact your local FBI field office at fbi.gov/contact-us/field-offices. 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. To request incident response resources or technical assistance related to these threats, contact CISA at Report@cisa.dhs.gov.

TECHNICAL DETAILS

Overview

Since the December 2021 release of FBI Flash: Indicators of Compromise Associated with Cuba Ransomware, FBI has observed Cuba ransomware actors continuing to target U.S. entities in the following five critical infrastructure sectors: Financial Services, Government Facilities, Healthcare and Public Health, Critical Manufacturing, and Information Technology. As of August 2022, FBI has identified that Cuba ransomware actors have:

- Compromised over 100 entities worldwide.
- Demanded over 145 million U.S. Dollars (USD) and received over 60 million USD in ransom payments.

Cuba Ransomware Actors' Tactics, Techniques, and Procedures

As previously reported by FBI, Cuba ransomware actors have leveraged the following techniques to gain initial access into dozens of entities in multiple critical infrastructure sectors:

- Known vulnerabilities in commercial software [T1190]
- Phishing campaigns [T1566]
- Compromised credentials [T1078]
- Legitimate remote desktop protocol (RDP) tools [T1563.002]

After gaining initial access, the actors distributed Cuba ransomware on compromised systems through Hancitor—a loader known for dropping or executing stealers, such as Remote Access Trojans (RATs) and other types of ransomware, onto victims' networks.

Since spring 2022, Cuba ransomware actors have modified their TTPs and tools to interact with compromised networks and extort payments from victims.[1],[2]

Cuba ransomware actors have exploited known vulnerabilities and weaknesses and have used tools to elevate privileges on compromised systems. According to Palo Alto Networks Unit 42,[2] Cuba ransomware actors have:

- Exploited CVE-2022-24521 in the Windows Common Log File System (CLFS) driver to steal system tokens and elevate privileges.
- Used a PowerShell script to identify and target service accounts for their associated Active Directory Kerberos ticket. The actors then collected and cracked the Kerberos tickets offline via Kerberoasting [T1558.003].
- Used a tool, called KerberCache, to extract cached Kerberos tickets from a host's Local Security Authority Server Service (LSASS) memory [T1003.001].
- Used a tool to exploit CVE-2020-1472 (also known as "ZeroLogon") to gain Domain Administrative privileges [T1068]. This tool and its intrusion attempts have been reportedly related to Hancitor and Qbot.

According to Palo Alto Networks Unit 42, Cuba ransomware actors use tools to evade detection while moving laterally through compromised environments before executing Cuba ransomware. Specifically, the actors, "leveraged a dropper that writes a kernel driver to the file system called

`ApcHelper.sys`. This targets and terminates security products. The dropper was not signed; however, the kernel driver was signed using the certificate found in the LAPSUS NVIDIA leak." [T1562.001].[2]

In addition to deploying ransomware, the actors have used “double extortion” techniques, in which they exfiltrate victim data, and (1) demand a ransom payment to decrypt it and, (2) threaten to publicly release it if a ransom payment is not made.[2]

Cuba Ransomware Link to RomCom and Industrial Spy Marketplace

Since spring 2022, third-party and open-source reports have identified an apparent link between Cuba ransomware actors, RomCom RAT actors, and Industrial Spy ransomware actors:

- According to Palo Alto Networks Unit 42, Cuba ransomware actors began using RomCom malware, a custom RAT, for command and control (C2).[2]
- Cuba ransomware actors may also be leveraging Industrial Spy ransomware. According to third-party reporting, suspected Cuba ransomware actors compromised a foreign healthcare company. The threat actors deployed Industrial Spy ransomware, which shares distinct similarities in configuration to Cuba ransomware. Before deploying the ransomware, the actors moved laterally using Impacket and deployed the RomCom RAT and Meterpreter Reverse Shell HTTP/HTTPS proxy via a C2 server [T1090].
- Cuba ransomware actors initially used their leak site to sell stolen data; however, around May 2022, the actors began selling their data on Industrial Spy’s online market for selling stolen data.[2]

RomCom actors have targeted foreign military organizations, IT companies, food brokers and manufacturers.[3][4] The actors copied legitimate HTML code from public-facing webpages, modified the code, and then incorporated it in spoofed domains [T1584.001], which allowed the RomCom actors to:

- Host counterfeit Trojanized applications for
  - SolarWinds Network Performance Monitor (NPM),
  - KeePass password manager,
  - PDF Reader Pro, (by PDF Technologies, Inc., not an Adobe Acrobat or Reader product), and
  - Advanced IP Scanner software;
- Deploy the RomCom RAT as the final stage.

INDICATORS OF COMPROMISE

See tables 1 through 5 for Cuba ransomware IOCs that FBI obtained during threat response investigations as of late August 2022. In addition to these tables, see the publications in the References section below for aid in detecting possible exploitation or compromise.

Note: For IOCs as of early November 2021, see FBI Flash: Indicators of Compromise Associated with Cuba Ransomware.

Table 1: Cuba Ransomware Associated Files and Hashes, as of Late August 2022

File Name	File Path	File Hash
netping.dll	c:\windows\temp	SHA256: f1103e627311e73d5f29e877243e7ca203292f9419303c661aec57745eb4f26c
shar.bat		MD5: 4c32ef0836a0af7025e97c6253054bca SHA256: a7c207b9b83648f69d6387780b1168e2f1eabd23ae6e162dd700ae8112f8b96c
Psexesvc.exe		SHA256: 141b2190f51397dbd0dfde0e3904b264c91b6f81febc823ff0c33da980b69944
1.bat		
216155s.dll		
23246s.bat		SHA256: 02a733920c7e69469164316e3e96850d55fca9f5f9d19a241fad906466ec8ae8
23246s.dll		SHA256: 0cf6399db55d40bc790a399c6bbded375f5a278dc57a143e4b21ea3f402f551f
23246st.dll		SHA256: f5db51115fa0c910262828d0943171d640b4748e51c9a140d06ea81ae6ea1710
259238e.exe		
31-100.bat		
3184.bat		
3184.dll		
45.dll		SHA256: 857f28b8fe31cf5db6d45d909547b151a66532951f26cda5f3320d2d4461b583
4ca736d.exe		
62e2e37.exe		
64.235.39.82		
64s.dll		
7z.sfx		
7zCon.sfx		
7-zip.chm		
82.ps1		

File Name	File Path	File Hash
9479.bat		SHA256: 08eb4366fc0722696edb03981f00778701266a2e57c40cd2e9d765bf8b0a34d0
9479p.bat		SHA256: f8144fa96c036a8204c7bc285e295f9cd2d1deb0379e39ee8a8414531104dc4a
9479p.ps1		SHA256: 88d13669a994d2e04ec0a9940f07ab8aab8563eb845a9c13f2b0fec497df5b17
a.exe		MD5: 03c835b684b21ded9a4ab285e4f686a3 SHA1: eaced2fcfdcbf3dca4dd77333aaab055345f3ab4 SHA256: 0f385cc69a93abeaf84994e7887cb173e889d309a515b55b2205805bdfe468a3 SHA256: 0d5e3483299242bf504bd3780487f66f2ec4f48a7b38baa6c6bc8ba16e4fb605 SHA256: 7e00bfb622072f53733074795ab581cf6d1a8b4fc269a50919dda6350209913c SHA256: af4523186fe4a5e2833bbbe14939d8c3bd352a47a2f77592d8adcb569621ce02
a220.bat		
a220.dll		SHA256: 8a3d71c668574ad6e7406d3227ba5adc5a230dd3057edddc4d0ec5f8134d76c3
a82.exe		SHA256: 4306c5d152cdd86f3506f91633ef3ae7d8cf0dd25f3e37bec43423c4742f4c42
a91.exe		SHA256: 3d4502066a338e19df58aa4936c37427feecce9ab8d43abff4a7367643ae39ce
a99.exe		SHA256: f538b035c3de87f9f8294bec272c1182f90832a4e86db1e47cbb1ab26c9f3a0b
aa.exe		
aa2.exe		
aaa.stage.16549040.dns.alleivice.com		

File Name	File Path	File Hash
add2.exe		
advapi32.dll		
agent.13.ps1		
agent.bat		SHA256: fd87ca28899823b37b2c239fbbd236c555bcab7768d67203f86d37ede19dd975
agent.dll		
agent13.bat		
agent13.ps1		SHA256: 1817cc163482eb21308adbd43fb6be57fcb5ff11fd74b344469190bb48d8163b
agent64.bin		SHA256: bff4dd37febd5465e0091d9ea68006be475c0191bd8c7a79a44fbf4b99544ef1
agsyst121.bat		
agsyst121.dll		
all.bat		SHA256: ecefd9bb8b3783a81ab934b44eb3d84df5e58f0289f089ef6760264352cf878a
all.dll		SHA256: db3b1f224aec1a7c58946d819d729d0903751d1867113aae5cca87e38c653cf4
anet.exe		SHA1: 241ce8af441db2d61f3eb7852f434642739a6cc3 SHA256: 74fbf3cc44dd070bd5cb87ca2eed03e1bbeec4fec644a25621052f0a73abbe84 SHA256: b160bd46b6efc6d79bfb76cf3eeacca2300050248969decba139e9e1cbeebf53 SHA256: f869e8fbd8aa1f037ad862cf6e8bbbf797ff49556fb100f2197be4ee196a89ae
App.exe		
appnetwork.exe		
AppVClient.man		
aswSP_arPot2		
aus.exe		SHA256: 0c2ffed470e954d2bf22807ba52c1ffd1ecce15779c0afdf15c292e3444cf674 SHA256: 310afba59ab8e1bda3ef750a64bf39133e15c89e8c7cf4ac65ee463b26b136ba

File Name	File Path	File Hash
av.bat		SHA256: b5d202456ac2ce7d1285b9c0e2e5b7ddc03da1cbca51b5da98d9ad72e7f773b8
c2.ps1		
c2.ps1		
cdzehhlzcwvzcmcr.aspx		
check.exe		
checkk.exe		
checkk.txt		SHA256: 1f842f84750048bb44843c277edeaa8469697e97c4dbf8dc571ec552266bec9f
client32.exe		
comctl32 .dll		
comp2.ps1		
comps2.ps1		
cqyrrxzhumiklndm.aspx		
defendercontrol.exe		
ff.exe		SHA256: 1b943afac4f476d523310b8e3afe7bca761b8cbaa9ea2b9f01237ca4652fc834
File __agsyst121.dll		
File __aswArPot.sys		
File __s9239.dll		
File_agsyst121.dll		
File_aswArPot.sys		
File_s9239.dll		
ga.exe		
gdi32 .dll		
geumspbgvvytqrih.aspx		
IObit UNLOCKER.exe		
kavsa32.exe		MD5: 236f5de8620a6255f9003d054f08574b SHA1: 9b546bd99272cf4689194d698c830a2510194722
kavsyst32.exe		
kernel32.dll		
komar.bat		SHA256: B9AFE016DBDBA389000B01CE7645E7EEA1B0A50827CDED1CBAA48FBC715197BB
komar.dll		
komar121.bat		
komar121.dll		

File Name	File Path	File Hash
komar2.ps1		SHA256: 61971d3cbf88d6658e5209de443e212100afc8f033057d9a4e79000f6f0f7cc4
komar64.dll		SHA256: 8E64BACAF40110547B334EADCB0792BDC891D7AE298FBFFF1367125797B6036B
mfcappk32.exe		
newpass.ps1		SHA256: c646199a9799b6158de419b1b7e36b46c7b7413d6c35bffaeaa8700b2dcc427
npalll.exe		SHA256: bd270853db17f94c2b8e4bd9fa089756a147ed45cbc44d6c2b0c78f361978906
ole32.dll		
oleaut32.dll		
open.bat		SHA256: 2EB3EF8A7A2C498E87F3820510752043B20CBE35B0CBD9AF3F69E8B8FE482676
open.exe		
pass.ps1		SHA256: 0afed8d1b7c36008de188c20d7f0e2283251a174261547aab7fb56e31d767666
pdfdecrypt.exe		
powerview.ps1		
prt3389.bat		SHA256: e0d89c88378dcb1b6c9ce2d2820f8d773613402998b8dcdb024858010dec72ed
ra.ps1		SHA256: 571f8db67d463ae80098edc7a1a0cad59153ce6592e42d370a45df46f18a4ad8
rg1.exe		
Rg2.exe		
rundll32		
s64174.bat		SHA256: 10a5612044599128981cb41d71d7390c15e7a2a0c2848ad751c3da1cbec510a2 SHA256: 1807549af1c8fdc5b04c564f4026e41790c554f339514d326f8b55cb7b9b4f79
s64174.dll		
s9239.bat		
s9239.dll		
shell32.dll		
stel.exe		
syskav64.exe		

File Name	File Path	File Hash
sysra64,exe		
systav332.bat		SHA256: 01242b35b6def71e42cc985e97d618e2fabd616b16d23f7081d575364d09ca74
TC-9.22a.2019.3.exe		
TeamViewer.exe		
testDLL.dll		
tug4rigd.dll		SHA256: 952b34f6370294c5a0bb122febfaa80612fef1f32eddd48a3d0556c4286b7474
UpdateNotificationPipeline.002.etl		
user32.dll		
v1.bat		
v2.bat		
v3.bat		
veeamp.exe		SHA256: 9aa1f37517458d635eae4f9b43cb4770880ea0ee171e7e4ad155bbdee0cbe732
version.dll		
vlhqbgvudfnirmzx.aspx		
wininet.dll		
wlog.exe		
wpeqawzp.sys		
y3lcx345.dll		
zero.exe		SHA256: 3a8b7c1fe9bd9451c0a51e4122605efc98e7e4e13ed117139a13e4749e211ed0

Table 2: Cuba Ransomware Associated Email Addresses, as of Late August 2022

Email Provider	Email Addresses
Cuba-supp[.]**com**	admin@cuba-supp[.]com
Encryption-support[.]**com**	admin@encryption-support[.]com
Mail.supports24[.]**net**	inbox@mail.supports24[.]net

Table 3: Cuba Ransomware Associated Jabber Address, as of Late August 2022

cuba_support@exploit[.]im

Table 4: IP Addresses Associated with Cuba Ransomware, as of Late August 2022

Note: *Some of these observed IP addresses are more than a year old. FBI and CISA recommend vetting or investigating these IP addresses prior to taking forward-looking action such as blocking.*

193.23.244[.]244	144.172.83[.]13	216.45.55[.]30
94.103.9[.]79	149.255.35[.]131	217.79.43[.]148
192.137.101[.]46	154.35.175[.]225	222.252.53[.]33
92.222.172[.]39	159.203.70[.]39	23.227.198[.]246
92.222.172[.]172	171.25.193[.]9	31.184.192[.]44
10.13.102[.]1	185.153.199[.]169	37.120.247[.]39
10.13.102[.]58	192.137.100[.]96	37.44.253[.]21
10.133.78[.]41	192.137.100[.]98	38.108.119[.]121
10.14.100[.]20	192.137.101[.]205	45.164.21[.]13
103.114.163[.]197	193.34.167[.]17	45.32.229[.]66
103.27.203[.]197	194.109.206[.]212	45.86.162[.]34
104.217.8[.]100	195.54.160[.]149	45.91.83[.]176
107.189.10[.]143	199.58.81[.]140	64.52.169[.]174
108.170.31[.]115	204.13.164[.]118	64.235.39[.]82
128.31.0[.]34	209.76.253[.]84	79.141.169[.]220
128.31.0[.]39	212.192.241[.]230	84.17.52[.]135
131.188.40[.]189	213.32.39[.]43	86.59.21[.]38
141.98.87[.]124	216.45.55[.]3	

Table 5: Cuba Bitcoin Wallets Receiving Payments, as of Late August 2022

bc1q4vr25xkth35qslenqwd7aw020w85qrvlrhv7hc
bc1q5uc0fdnz0ve5pg4nl4upa9ly586t6wmnghfe7x
bc1q6rsj3cn37dngypu5kad9gdw5ykhctpwhjvun3z
bc1q6zkemtyyrre2mkk23g93zyq98ygrygvx7z2q0t
bc1q9cj0n9k2m282x0nzj6lhqjvhkkd4h95sewek83
bc1qaselp9nhejc3safcq3vn5wautx6w33x0llk7dl
bc1qc48q628t93xwzljtvurpqhcvahvesadpwqtsza
bc1qgsuf5m9tgxuv4ylxcmx8eeqn3wmlmu7f49zkus
bc1qhpepeeh7hlz5jvrp50uhkz59lhakcfvme0w9qh
bc1qjep0vx2lap93455p7h29unruvr05cs242mrcah
bc1qr9l0gcl0nvmngap6ueyy5gqdwvm34kdmtevjyx
bc1qs3lv77udkap2enxv928x59yuact5df4t95rsqr
bc1qyd05q2m5qt3nwpd3gcqkyer0gspqx5p6evcf7h
bc1qzz7xweq8ee2j35tq6r5m687kctq9huskt50edv
bc1qvpk8ksl3my6kjezjss9p28cqj4dmpmmjx5yl3y
bc1qhtwfcysclc7pck2y3vmjtpzkaezhcm6perc99x
bc1qft3s53ur5uq5ru6sl3zyr247dpr55mnggwucd3
bc1qp7h9fszlqxjwyfhv0upparnsgx56x7v7wfx4x7
bc1q4vr25xkth35qslenqwd7aw020w85qrvlrhv7hc
bc1q5uc0fdnz0ve5pg4nl4upa9ly586t6wmnghfe7x
bc1q6rsj3cn37dngypu5kad9gdw5ykhctpwhjvun3z
bc1q6zkemtyyrre2mkk23g93zyq98ygrygvx7z2q0t
bc1q9cj0n9k2m282x0nzj6lhqjvhkkd4h95sewek83
bc1qaselp9nhejc3safcq3vn5wautx6w33x0llk7dl
bc1qc48q628t93xwzljtvurpqhcvahvesadpwqtsza
bc1qgsuf5m9tgxuv4ylxcmx8eeqn3wmlmu7f49zkus
bc1qhpepeeh7hlz5jvrp50uhkz59lhakcfvme0w9qh
bc1qjep0vx2lap93455p7h29unruvr05cs242mrcah
bc1qr9l0gcl0nvmngap6ueyy5gqdwvm34kdmtevjyx
bc1qs3lv77udkap2enxv928x59yuact5df4t95rsqr
bc1qyd05q2m5qt3nwpd3gcqkyer0gspqx5p6evcf7h
bc1qzz7xweq8ee2j35tq6r5m687kctq9huskt50edv

See figure 1 for an example of a Cuba ransomware note.

Greetings! Unfortunately we have to report that your company were compromised. All your files were
encrypted and you can't restore them without our private key. Trying to restore it without our help may
cause complete loss of your data. Also we researched whole your corporate network and downloaded all
your sensitive data to our servers. If we will not get any contact from you in the next 3 days we will public
it in our news site.
You can find it there (https[:]// cuba4ikm4jakjgmkeztyawtdgr2xymvy6nvgw5cglswg3si76icnqd.onion/)
Tor Browser is needed (https[:]//www.torproject.org/download/)
Also we respect your work and time and we are open for communication.
In that case we are ready to discuss recovering your files and work. We can grant absolute privacy and compliance with agreements by our side.
Also we can provide all necessary evidence to confirm performance of our products and statements.
Feel free to contact us with quTox (https[:]//tox.chat/download.html)

Our ToxID:
37790E2D198DFD20C9D2887D4EF7C3E2951888424801926898 64DCCA3C8BD808A18956768271

Alternative method is email: inbox@mail.supports24[.]net

Mark your messages with your personal ID:

Figure 1: Sample Cuba Ransom Note 2, as of late August 2022

Additional resources to detect possible exploitation or compromise:

- Palo Alto Networks blog: Novel News on Cuba Ransomware: Greetings from Tropical Scorpius
- BlackBerry blog: RomCom Threat Actor Abuses KeePass and SolarWinds to Target Ukraine and Potentially the United Kingdom
- BlackBerry blog: Unattributed RomCom Threat Actor Spoofing Popular Apps Now Hits Ukrainian Militaries

MITRE ATT&CK TECHNIQUES

Cuba ransomware actors use the ATT&CK techniques listed in Table 6. **Note:** For details on TTPs listed in the table, see FBI Flash Indicators of Compromise Associated with Cuba Ransomware.

Table 6: Cuba Ransomware Actors ATT&CK Techniques for Enterprise

Resource Development		
Technique Title	**ID**	**Use**
Compromise Infrastructure: Domains	T1584.001	Cuba ransomware actors use compromised networks to conduct their operations.
Initial Access		
Technique Title	**ID**	**Use**
Valid Accounts	T1078	Cuba ransomware actors have been known to use compromised credentials to get into a victim's network.
External Remote Services	T1133	Cuba ransomware actors may leverage external-facing remote services to gain initial access to a victim's network.
Exploit Public-Facing Application	T1190	Cuba ransomware actors are known to exploit vulnerabilities in public-facing systems.
Phishing	T1566	Cuba ransomware actors have sent phishing emails to obtain initial access to systems.
Execution		
Technique Title	**ID**	**Use**
Command and Scripting Interpreter: PowerShell	T1059.001	Cuba ransomware actors have used PowerShell to escalate privileges.
Software Deployment Tools	T1072	Cuba ransomware actors use Hancitor as a tool to spread malicious files throughout a victim's network.

Privilege Escalation		
Technique Title	**ID**	**Use**
Exploitation for Privilege Escalation	T1068	Cuba ransomware actors have exploited ZeroLogon to gain administrator privileges.[2]
Defense Evasion		
Technique Title	**ID**	**Use**
Impair Defenses: Disable or Modify Tools	T1562.001	Cuba ransomware actors leveraged a loader that disables security tools within the victim network.
Lateral Movement		
Technique Title	**ID**	**Use**
Remote Services Session: RDP Hijacking	T1563.002	Cuba ransomware actors used RDP sessions to move laterally.
Credential Access		
Technique Title	**ID**	**Use**
Credential Dumping: LSASS Memory	T1003.001	Cuba ransomware actors use LSASS memory to retrieve stored compromised credentials.
Steal or Forge Kerberos Tickets: Kerberoasting	T1558.003	Cuba ransomware actors used the Kerberoasting technique to identify service accounts linked to active directory.[2]
Command and Control		
Technique Title	**ID**	**Use**
Proxy: Manipulate Command and Control Communications	T1090	Industrial Spy ransomware actors use HTTP/HTTPS proxy via a C2 server to direct traffic to avoid direct connection. [2]

MITIGATIONS

FBI and CISA recommend network defenders apply the following mitigations to limit potential adversarial use of common system and network discovery techniques and to reduce the risk of compromise by Cuba ransomware:

- **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.
- **Require multifactor authentication** for all services to the extent possible, particularly for webmail, virtual private networks, and accounts that access critical systems.
- **Keep all operating systems, software, and firmware up to date.** 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 SonicWall firewall vulnerabilities and known exploited vulnerabilities in internet-facing systems. **Note:** SonicWall maintains a vulnerability list that includes Advisory ID, CVE, and mitigation. Their list can be found at psirt.global.sonicwall.com/vuln-list.
- **Segment networks** 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.** 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.

- **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.**
- **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). JIT sets a network-wide policy 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. 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.

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.
- No-cost cyber hygiene services: Cyber Hygiene Services and Ransomware Readiness Assessment.

REPORTING

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

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, FBI and

CISA urge you to promptly report ransomware incidents immediately. Report to a local FBI Field Office, or CISA at us-cert.cisa.gov/report.

DISCLAIMER

The information in this report is being provided “as is” for informational purposes only. FBI and CISA do not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by FBI or CISA.

ACKNOWLEDGEMENTS

FBI and CISA would like to thank BlackBerry, ESET, The National Cyber-Forensics and Training Alliance (NCFTA), and Palo Alto Networks for their contributions to this CSA.

REFERENCES

[1] Palo Alto Networks: Tropical Scorpius
[2] Palo Alto Networks: Novel News on Cuba Ransomware - Greetings From Tropical Scorpius
[3] BlackBerry: Unattributed RomCom Threat Actor Spoofing Popular Apps Now Hits Ukrainian Militaries
[4] BlackBerry: RomCom Threat Actor Abuses KeePass and SolarWinds to Target Ukraine and Potentially the United Kingdom