JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

TLP:CLEAR

Product ID: AA23-263A

September 20, 2023

#StopRansomware: Snatch 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 malicious cyber activity:

- Secure and closely monitor Remote Desktop Protocol (RDP).
- Maintain offline backups of data.
- Enable and enforce phishing-resistant multifactor authentication (MFA).

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) are releasing this joint CSA to disseminate known ransomware IOCs and TTPs associated with the Snatch ransomware variant identified through FBI investigations as recently as June 1, 2023.

Since mid-2021, Snatch threat actors have consistently evolved their tactics to take advantage of current trends in the cybercriminal space and leveraged successes of other ransomware variants' operations. Snatch threat actors have targeted a wide range of critical infrastructure sectors including the Defense Industrial Base (DIB), Food and Agriculture, and Information Technology sectors. Snatch threat actors conduct ransomware operations involving data exfiltration and double extortion. After data exfiltration often involving direct communications with victims demanding ransom, Snatch threat actors may threaten victims with double extortion, where the victims' data will be posted on Snatch's extortion blog if the ransom goes unpaid.

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

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.

TECHNICAL DETAILS

Note: This advisory uses the MITRE ATT&CK for Enterprise framework, version 13. 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.

First appearing in 2018, Snatch operates a ransomware-as-a-service (RaaS) model and claimed their first U.S.-based victim in 2019. Originally, the group was referred to as Team Truniger, based on the nickname of a key group member, Truniger, who previously operated as a GandCrab affiliate. Snatch threat actors use a customized ransomware variant notable for rebooting devices into Safe Mode [T1562.009], enabling the ransomware to circumvent detection by antivirus or endpoint protection, and then encrypting files when few services are running.

Snatch threat actors have been observed purchasing previously stolen data from other ransomware variants in an attempt to further exploit victims into paying a ransom to avoid having their data released on Snatch's extortion blog. **Note:** Since November 2021, an extortion site operating under the name Snatch served as a clearinghouse for data exfiltrated or stolen from victim companies on Clearnet and TOR hosted by a bulletproof hosting service. In August 2023, individuals claiming to be associated with the blog gave a media interview claiming the blog was not associated with Snatch ransomware and "none of our targets has been attacked by Ransomware Snatch…", despite multiple confirmed Snatch victims' data appearing on the blog alongside victims associated with other ransomware groups, notably Nokoyawa and Conti.[1]

Initial Access and Persistence

Snatch threat actors employ several different methods to gain access to and maintain persistence on a victim's network. Snatch affiliates primarily rely on exploiting weaknesses in Remote Desktop Protocol (RDP) [T1133] for brute-forcing and gaining administrator credentials to victims' networks [T1110.001]. In some instances, Snatch affiliates have sought out compromised credentials from criminal forums/marketplaces [T1078].

Snatch threat actors gain persistence on a victim's network by compromising an administrator account [T1078.002] and establishing connections over port `443` [T1071.001] to a command and control (C2) server located on a Russian bulletproof hosting service [T1583.003]. Per IP traffic from event logs provided by recent victims, Snatch threat actors initiated RDP connections from a Russian bulletproof hosting service and through other virtual private network (VPN) services [T1133].

Data Discovery and Lateral Movement

Snatch threat actors were observed using different TTPs to discover data, move laterally, and search for data to exfiltrate. Snatch threat actors use `sc.exe` to configure, query, stop, start, delete, and add system services using the Windows Command line. In addition to `sc.exe`, Snatch threat actors also use tools such as Metasploit and Cobalt Strike [S0154].

Prior to deploying the ransomware, Snatch threat actors were observed spending up to three months on a victim's system. Within this timeframe, Snatch threat actors exploited the victim's network

[T1590], moving laterally across the victim's network with RDP [T1021.001] for the largest possible deployment of ransomware and searching for files and folders [T1005] for data exfiltration [TA0010] followed by file encryption [T1486].

Defense Evasion and Execution

During the early stages of ransomware deployment, Snatch threat actors attempt to disable antivirus software [T1562.001] and run an executable as a file named `safe.exe` or some variation thereof. In recent victims, the ransomware executable's name consisted of a string of hexadecimal characters which match the `SHA-256` hash of the file in an effort to defeat rule-based detection [T1036]. Upon initiation, the Snatch ransomware payload queries and modifies registry keys [T1012][T1112], uses various native Windows tools to enumerate the system [T1569.002], finds processes [T1057], and creates benign processes to execute Windows batch (`.bat`) files [T1059.003]. In some instances, the program attempts to remove all the volume shadow copies from a system [T1490]. After the execution of the batch files, the executable removes the batch files from the victim's filesystem [T1070.004].

The Snatch ransomware executable appends a series of hexadecimal characters to each file and folder name it encrypts—unique to each infection—and leaves behind a text file titled `HOW TO RESTORE YOUR FILES.TXT` in each folder. Snatch threat actors communicate with their victims through email and the Tox communication platform based on identifiers left in ransom notes or through their extortion blog. Since November 2021, some victims reported receiving a spoofed call from an unknown female who claimed association with Snatch and directed them to the group's extortion site. In some instances, Snatch victims had a different ransomware variant deployed on their systems, but received a ransom note from Snatch threat actors. As a result, the victims' data is posted on the ransomware blog involving the different ransomware variant and on the Snatch threat actors' extortion blog.

Indicators of Compromise (IOCs)

The Snatch IOCs detailed in this section were obtained through FBI investigations from September 2022 through June 2023.

Email Domains and Addresses

Since 2019, Snatch threat actors have used numerous email addresses to email victims. Email addresses used by Snatch threat actors are random but usually originate from one of the following domains listed in Tables 1 and 2:

Table 1: Malicious Email Domains Observed in Use by Snatch Threat Actors

Email Domains
sezname[.]cz
cock[.]li
airmail[.]cc

Table 2 shows a list of legitimate email domains offering encrypted email services that have been used by Snatch threat actors. These email domains are all publicly available and legal. The use of these email domains by a threat actor should not be attributed to the email domains, absent specific articulable facts tending to show they are used at the direction or under the control of a threat actor.

Table 2: Legitimate Email Domains Observed in Use by Snatch Threat Actors

Email Domains
tutanota[.]com / tutamail[.]com / tuta[.]io
mail[.]fr
keemail[.]me
protonmail[.]com / proton[.]me
swisscows[.]email

The email addresses listed in Table 3 were reported by recent victims.

Table 3: Snatch's Email Addresses Reported by Recent Victims

Email Addresses
sn.tchnews.top@protonmail[.]me
funny385@swisscows[.]email
funny385@proton[.]me
russellrspeck@seznam[.]cz
russellrspeck@protonmail[.]com
Mailz13MoraleS@proton[.]me
datasto100@tutanota[.]com
snatch.vip@protonmail[.]com

TOX Messaging IDs

TOX Messaging IDs
CAB3D74D1DADE95B52928E4D9DFC003FF5ADB2E082F59377D049A91952E8BB3B419DB2FA9D3F
7229828E766B9058D329B2B4BC0EDDD11612CBCCFA4811532CABC76ACF703074E0D1501F8418
83E6E3CFEC0E4C8E7F7B6E01F6E86CF70AE8D4E75A59126A2C52FE9F568B4072CA78EF2B3C97
0FF26770BFAEAD95194506E6970CC1C395B04159038D785DE316F05CE6DE67324C6038727A58 **NOTE:** According to ransom notes, this is a "Customer service" TOX to reach out to if the original TOX ID does not respond.

Folder Creation

Folder Creation
C:\$SysReset

Filenames with Associated SHA-256 Hashes

Filenames	SHA-256
qesbdksdvnotrjnexutx.bat	0965cb8ee38adedd9ba06bdad9220a35890c2df0e4c78d0559cd6da653bf740f
eqbglqcngblqnl.bat	1fbdb97893d09d59575c3ef95df3c929fe6b6ddf1b273283e4efadf94cdc802d
safe.exe	5950b4e27554585123d7fca44e83169375c6001201e3bf26e57d079437e70bcd
safe.exe	7018240d67fd11847c7f9737eaaae45794b37a5c27ffd02beaacaf6ae13352b3
safe.exe	28e82f28d0b9eb6a53d22983e21a9505ada925ebb61382fabebd76b8c4acff7c
safe.exe	fc31043b5f079ce88385883668eeebba76a62f77954a960fb03bf46f47dbb066
DefenderControl.exe	a201f7f81277e28c0bdd680427b979aee70e42e8a98c67f11e7c83d02f8fe7ae

Filenames	SHA-256
PRETTYOCEANApplicationdrs.bi	6992aaad3c47b938309fc1e6f37179eb51f028536f8afc02e4986312e29220c0
Setup.exe	510e9fa38a08d446189c34fe6125295f410b36f00aceb65e7b4508e9d7c4e1d1
WRSA.exe	ed0fd61bf82660a69f5bfe0e66457cfe56d66dd2b310e9e97657c37779aef65d
ghnhfglwaplf.bat	2155a029a024a2ffa4eff9108ac15c7db527ca1c8f89ccfd94cc3a70b77cfc57
nllraq.bat	251427c578eaa814f07037fbe6e388b3bc86ed3800d7887c9d24e7b94176e30d
ygariiwfenmqteiwcr.bat	3295f5029f9c9549a584fa13bc6c25520b4ff9a4b2feb1d9e935cc9e4e0f0924
bsfyqgqeauegwyfvtp.bat	6c9d8c577dddf9cc480f330617e263a6ee4461651b4dec1f7215bda77df911e7
rgibdcghzwpk.bat	84e1476c6b21531de62bbac67e52ab2ac14aa7a30f504ecf33e6b62aa33d1fe5
pxyicmajjlqrtgcnhi.bat	a80c7fe1f88cf24ad4c55910a9f2189f1eedad25d7d0fd53dbfe6bdd68912a84
evhgpp.bat	b998a8c15cc19c8c31c89b30f692a40b14d7a6c09233eb976c07f19a84eccb40
eqbglqcngblqnl.bat	1fbdb97893d09d59575c3ef95df3c929fe6b6ddf1b273283e4efadf94cdc802d
qesbdksdvnotrjnexutx.bat	0965cb8ee38adedd9ba06bdad9220a35890c2df0e4c78d0559cd6da653bf740f
HOW TO RESTORE YOUR FILES.TXT	

Filenames with Associated SHA-1 Hashes

Filenames	SHA-1
safe.exe	c8a0060290715f266c89a21480fed08133ea2614

Commands Used by Snatch Threat Actors

Commands
wmiadap.exe /F /T /R
%windir%\System32\svchost.eve –k WerSvcGroup
conhost.exe 0xFFFFFFFF -ForceV1
vssadmin delete shadows /all /quiet
bcdedit.exe /set {current} safeboot minimal
REG ADD HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\VSS /VE /T REG_SZ /F /D Service
REG ADD HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\mXoRpcSsx /VE /T REG_SZ /F /D Service
REG QUERY HKLM\SYSTEM\CurrentControlSet\Control /v SystemStartOptions
%CONHOST% "1088015358-1778111623-1306428145949291561678876491840500802412316031-33820320
"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --flag-switches-begin --flag-switches-end --no-startup-window /prefetch:5
cmd /d /c cmd /d /c cmd /d /c start " " C:\Users\grade1\AppData\Local\PRETTYOCEANluvApplication\PRETTYOCEANApplicationidf.bi.

Registry Keys

Registry Keys
HKLM\SOFTWARE\Microsoft\Windows Media Player NSS\3.0\Servers\D8B548F0-E306-4B2B-BD82-25DAC3208786\FriendlyName

HKU\S-1-5-21-4270068108-2931534202-3907561125-1001\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached\{ED50FC29-B964-48A9-AFB3-15EBB9B97F36} {ADD8BA80-002B-11D0-8F0F-00C04FD7D062} 0xFFFF

System Log Changes

Source	Message
TerminalServices-RemoteConnectionManager	Remote session from client name exceeded the maximum allowed failed logon attempts. The session was forcibly terminated.
Microsoft-Windows-Windows Firewall With Advanced Security%4Firewall	A rule was added (Event 2004) or modified (Event 2005) in the Windows Defender Firewall exception list. All rules included action “Allow” and rule name included “File and Printer Sharing”
Microsoft-Windows-Windows Firewall With Advanced Security%4Firewall	A Windows Defender Firewall setting was changed in private, public, and domain profile with type “Enable Windows Defender Firewall” and value of “no”.
Microsoft-Windows-TaskScheduler%4Operational	Instance of process C:\Windows\svchost.exe. (Incorrect file location, should be C:\Windows\System32\svchost.exe)

Mutexes Created

Mutexes Created
\Sessions\1\BaseNamedObjects\gcc-shmem-tdm2-fc_key
\Sessions\1\BaseNamedObjects\gcc-shmem-tdm2-sjlj_once
\Sessions\1\BaseNamedObjects\gcc-shmem-tdm2-use_fc_key
gcc-shmem-tdm2-fc_key
gcc-hmem-tdm2-sjlj_once
gcc-shmem-tdm2-use_fc_key

MITRE ATT&CK TACTICS AND TECHNIQUES

See Tables 4-16 for all referenced threat actor tactics and techniques in this advisory.

Table 4: Snatch Threat Actors ATT&CK Techniques for Enterprise – Reconnaissance

Technique Title	ID	Use
Gather Victim Network Information	T1590	Snatch threat actors may gather information about the victim's networks that can be used during targeting.

Table 5: Snatch Threat Actors ATT&CK Techniques for Enterprise – Resource Development

Technique Title	ID	Use
Acquire Infrastructure: Virtual Private Server	T1583.003	Snatch threat actors may rent Virtual Private Servers (VPSs) that can be used during targeting. Snatch threat actors acquire infrastructure from VPS service providers that are known for renting VPSs with minimal registration information, allowing for more anonymous acquisitions of infrastructure.

Table 6: Snatch Threat Actors ATT&CK Techniques for Enterprise – Initial Access

Technique Title	ID	Use
Valid Accounts	T1078	Snatch threat actors use compromised user credentials from criminal forums/marketplaces to gain access and maintain persistence on a victim's network.
External Remote Services	T1133	Snatch threat actors exploit weaknesses in RDP to perform brute forcing and gain administrator credentials for a victim's network. Snatch threat actors use VPN services to connect to a victim's network.

Table 7: Snatch Threat Actors ATT&CK Techniques for Enterprise – Execution

Technique Title	ID	Use
Command and Scripting Interpreter: Windows Command Shell	T1059.003	Snatch threat actors may use batch files (`.bat`) during ransomware execution and data discovery.
System Services: Service Execution	T1569.002	Snatch threat actors may leverage various Windows tools to enumerate systems on the victim's network. Snatch ransomware used `sc.exe`.

Table 8: Snatch Threat Actors ATT&CK Techniques for Enterprise – Persistence

Technique Title	ID	Use
Valid Accounts: Domain Accounts	T1078.002	Snatch threat actors compromise domain accounts to maintain persistence on a victim's network.

Table 9: Snatch Threat Actors ATT&CK Techniques for Enterprise – Defense Evasion

Technique Title	ID	Use
Masquerading	T1036	Snatch threat actors have the ransomware executable match the `SHA-256` hash of a legitimate file to avoid rule-based detection.
Indicator Removal: File Deletion	T1070.004	Snatch threat actors delete batch files from a victim's filesystem once execution is complete.
Modify Registry	T1112	Snatch threat actors modify Windows Registry keys to aid in persistence and execution.
Impair Defenses: Disable or Modify Tools	T1562.001	Snatch threat actors have attempted to disable a system's antivirus program to enable persistence and ransomware execution.
Impair Defenses: Safe Mode Boot	T1562.009	Snatch threat actors abuse Windows Safe Mode to circumvent detection by antivirus or

		endpoint protection and encrypt files when few services are running.

Table 10: Snatch Threat Actors ATT&CK Techniques for Enterprise – Credential Access

Technique Title	ID	Use
Brute Force: Password Guessing	T1110.001	Snatch threat actors use brute force to obtain administrator credentials for a victim's network.

Table 11: Snatch Threat Actors ATT&CK Techniques for Enterprise – Discovery

Technique Title	ID	Use
Query Registry	T1012	Snatch threat actors may interact with the Windows Registry to gather information about the system, configuration, and installed software.
Process Discovery	T1057	Snatch threat actors search for information about running processes on a system.

Table 12: Snatch Threat Actors ATT&CK Techniques for Enterprise – Lateral Movement

Technique Title	ID	Use
Remote Services: Remote Desktop Protocol	T1021.001	Snatch threat actors may use Valid Accounts to log into a computer using the Remote Desktop Protocol.

Table 13: Snatch Threat Actors ATT&CK Techniques for Enterprise – Collection

Technique Title	ID	Use
Data from Local System	T1005	Snatch threat actors search systems to find files and folders of interest prior to exfiltration.

Table 14: Snatch Threat Actors ATT&CK Techniques for Enterprise – Command and Control

Technique Title	ID	Use
Application Layer Protocols: Web Protocols	T1071.001	Snatch threat actors establish connections over port 443 to blend C2 traffic in with other web traffic.

Table 15: Snatch Threat Actors ATT&CK Techniques for Enterprise – Exfiltration

Technique Title	ID	Use
Exfiltration	TA0010	Snatch threat actors use exfiltration techniques to steal data from a victim's network.

Table 16: Snatch Threat Actors ATT&CK Techniques for Enterprise – Impact

Technique Title	ID	Use
Data Encrypted for Impact	T1486	Snatch threat actors encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources.
Inhibit System Recovery	T1490	Snatch threat actors delete all volume shadow copies from a victim's filesystem to inhibit system recovery.

MITIGATIONS

The FBI and CISA recommend organizations implement the mitigations below to improve your organization's cybersecurity posture on the basis of the Snatch threat 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.

These mitigations apply to all stakeholders. The authoring agencies recommend that software manufactures incorporate secure-by-design and -default principles and tactics into their software development practices for hardening software against ransomware attacks (e.g., to prevent threat actors from using Safe Mode to evade detection and file encryption), thus strengthening the secure posture for their customers.

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

- **Reduce threat of malicious actors** using remote access tools by:
  - **Auditing remote access tools** on your network to identify currently used and/or authorized software.
  - **Reviewing logs for execution of remote access software** to detect abnormal use of programs running as a portable executable [CPG 2.T].
  - **Using security software** to detect instances of remote access software being loaded only in memory.
  - **Requiring authorized remote access solutions** to be used only from within your network over approved remote access solutions, such as virtual private networks (VPNs) or virtual desktop interfaces (VDIs).
  - **Blocking both inbound and outbound connections** on common remote access software ports and protocols at the network perimeter.
- **Implement application controls** to manage and control execution of software, including allowlisting remote access programs.
  - Application controls should prevent installation and execution of portable versions of unauthorized remote access and other software. A properly configured application allowlisting solution will block any unlisted application execution. Allowlisting is important because antivirus solutions may fail to detect the execution of malicious portable executables when the files use any combination of compression, encryption, or obfuscation.
- **Strictly limit the use of RDP and other remote desktop services**. If RDP is necessary, rigorously apply best practices, for example [CPG 2.W]:
  - Audit the network for systems using RDP.
  - Close unused RDP ports.
  - Enforce account lockouts after a specified number of attempts.

  - Apply phishing-resistant multifactor authentication (MFA).
  - Log RDP login attempts.
- **Disable command-line and scripting** activities and permissions [CPG 2.N].
- **Review domain controllers, servers, workstations, and active directories** for new and/or unrecognized accounts [CPG 4.C].
- **Audit user accounts with administrative privileges** and configure access controls according to the principle of least privilege (PoLP) [CPG 2.E].
- **Reduce the threat of credential compromise** via the following:
  - **Place domain admin accounts in the protected users' group** to prevent caching of password hashes locally.
  - Refrain from storing plaintext credentials in scripts.
- **Implement time-based access for accounts** set at the admin level and higher [CPG 2.A, 2.E].

In addition, the authoring authorities of this CSA recommend network defenders apply the following mitigations to limit potential adversarial use of common system and network discovery techniques, and to reduce the impact and risk of compromise by ransomware or data extortion actors:

- **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).
- **Maintain offline backups of data** and regularly maintain backup and restoration (daily or weekly at minimum). By instituting this practice, an organization limits the severity of disruption to its business practices [CPG 2.R].
- **Require all accounts** with password logins (e.g., service account, admin accounts, and domain admin accounts) **to comply** with NIST's standards for developing and managing password policies.
  - Use longer passwords consisting of at least eight characters and no more than 64 characters in length [CPG 2.B].
  - Store passwords in hashed format using industry-recognized password managers.
  - Add password user "salts" to shared login credentials.
  - Avoid reusing passwords [CPG 2.C].
  - Implement multiple failed login attempt account lockouts [CPG 2.G].
  - 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 phishing-resistant multifactor authentication (MFA)** for all services to the extent possible, particularly for webmail, virtual private networks (VPNs), and accounts that access critical systems [CPG 2.H].
- **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 known exploited vulnerabilities in internet-facing systems [CPG 1.E].

- **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 [CPG 2.F].
- **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 and activity, including lateral movement, 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 [CPG 3.A].
- **Install, regularly update, and enable real time detection for antivirus software** on all hosts.
- **Disable unused ports and protocols** [CPG 2.V].
- **Consider adding an email banner to emails** received from outside your organization [CPG 2.M].
- **Disable hyperlinks** in received emails.
- **Ensure all backup data is encrypted, immutable** (i.e., ensure backup data cannot be altered or deleted), and covers the entire organization's data infrastructure [CPG 2.K, 2.L, 2.R].

VALIDATE SECURITY CONTROLS

In addition to applying mitigations, 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. 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 Tables 4-16).
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.

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

REPORTING

The FBI is seeking any information that can be shared, to include boundary logs showing communication to and from IP addresses, a sample ransom note, communications with Snatch threat actors, Bitcoin wallet information, decryptor files, and/or a benign sample of an encrypted file. The FBI and CISA strongly discourage 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 Internet Crime Complaint Center (IC3) at ic3.gov, a local FBI Field Office, or to CISA at report@cisa.gov or (888) 282-0870.

REFERENCES

[1] DataBreaches.net

DISCLAIMER

The information in this report is being provided “as is” for informational purposes only. FBI and CISA do not endorse any commercial entity, 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.

VERSION HISTORY

September 20, 2023: Initial version.