JOINT
CYBERSECURITY ADVISORY

TLP:CLEAR

Product ID: AA26-293A

Co-Authored by:

#StopRansomware: SafePay Ransomware

Publication: October 20, 2026

U.S. Federal Bureau of Investigation
U.S. Cybersecurity and Infrastructure Security Agency
U.S. Secret Service
Germany's Landeskriminalamt Rheinland-Pfalz
United Kingdom's National Crime Agency
United Kingdom's North West Regional Organised Crime Unit

To report suspicious or criminal activity related to information found in this joint Cybersecurity Advisory, contact the FBI's Internet Crime Complaint Center (IC3), your local FBI field office, and/or CISA's 24/7 Operations Center at contact@cisa.dhs.gov or 1-844-Say-CISA (1-844-729-2472). 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 distributed as TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no forseeable 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 Traffic Light Protocol (TLP) Definitions and Usage.

Advisory at a Glance

Title	#StopRansomware: SafePay Ransomware
Original Publication	October 20, 2026
Executive Summary	This advisory details recent activity by the SafePay ransomware group. SafePay actors have been highly active since August 2024, targeting businesses and critical infrastructure across North America, South America, Europe, and Australia. SafePay actors typically gain access to networks by stealing or guessing passwords, exploiting vulnerabilities in security systems, and using phishing tactics. Once inside the network, SafePay actors establish control by creating new accounts or taking over existing ones. They then use legitimate system tools to move through the network, identify valuable files, and disable security protections to avoid detection. Next, they encrypt the victim's files, making them inaccessible, and leave a ransom note demanding payment in cryptocurrency. This advisory urges organizations to follow recommended security measures to reduce the risk and impact of SafePay ransomware attacks.
Affected Products	▪ CVE-2020-3259 [Common Weakness Enumeration (CWE)-200: Exposure of Sensitive Information to an Unauthorized Actor] ▪ CVE-2023-20269 [CWE-288: Authentication Bypass Using an Alternate Path or Channel] ▪ CVE-2023-27532 [CWE-306: Missing Authentication for Critical Function] ▪ CVE-2024-40711 [CWE-502: Deserialization of Untrusted Data] ▪ CVE-2024-40766 [CWE-284: Improper Access Control]
Key Actions	▪ **Regularly patch and update systems,** especially firewalls, and other edge devices. ▪ **Implement Zero Trust Principle.** ▪ **Restrict administrative tools and privileges** to necessary users only. ▪ Strengthen account security by **implementing identity, credential, and access management (ICAM) policies and multifactor authentication (MFA).**
Indicators of Compromise	For a downloadable copy of indicators of compromise, see: ▪ AA26-293A STIX XML (40KB), AA26-293A STIX JSON (38KB)
Intended Audience	**Organizations:** Government; Federal Civilian Executive Branch (FCEB); State, Local, Tribal, and Territorial (SLTT); Critical Infrastructure **Roles:** Defensive cybersecurity analysts, vulnerability analysts, security systems managers, and operational technology (OT) owners and operators

Table of Contents

Advisory at a Glance 2
Introduction 4
Technical Details 4
Initial Access 4
Execution, Persistence, Stealth, and Defense Impairment 5
Privilege Escalation 5
Lateral Movement 5
Collection, Exfiltration, and Impact 5
Leveraged Tools 6
Indicators of Compromise 7
MITRE ATT&CK Tactics and Techniques 11
Incident Response 14
Mitigations 15
Validate Security Controls 17
Resources 17
Reporting 18
Disclaimer 19
Version History 19

Introduction

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.

The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), United States Secret Service (USSS), Germany's Landeskriminalamt Rheinland-Pfalz, the United Kingdom's National Crime Agency, and the United Kingdom's North West Regional Organised Crime Unit—hereafter referred to as the authoring agencies—are releasing this joint advisory to disseminate known SafePay ransomware TTPs and IOCs identified through FBI, USSS, and Landeskriminalamt Rheinland-Pfalz investigations as recently as August 2026.

Since August 2024, SafePay ransomware group's operations have affected a wide range of businesses and critical infrastructure in North America, South America, Europe, and Australia. SafePay ransomware was among the most active ransomware groups in 2026. The SafePay threat actors have impacted at least 600 separate victims from multiple critical infrastructure sectors.

The authoring agencies encourage organizations to implement the recommendations in the **Mitigations** section of this advisory to reduce the likelihood and impact of SafePay ransomware incidents.

For a downloadable copy of IOCs, see:

- AA26-293A STIX XML (40KB)
- AA26-293A STIX JSON (38KB)

Technical Details

Note: This advisory uses the MITRE ATT&CK® Matrix for Enterprise framework, version 20. See **MITRE ATT&CK Tactics and Techniques** section of this advisory for a table of the threat actors' activity mapped to MITRE ATT&CK tactics and techniques.

Initial Access

The FBI, USSS, and cybersecurity researchers observed SafePay threat actors obtaining initial access [TA0001] to organizations through various means, including credential exposure, implementing brute force password attacks [T1110], and exploiting virtual private network (VPN) access. SafePay threat actors use the IP addresses of the VPN provider "Mullvad" to attain initial access—specifically, SafePay threat actors use phished account profiles to access victim networks to exploit the following known Common Vulnerabilities and Exposures (CVEs) for edge device products:

- CVE-2020-3259 [Common Weakness Enumeration (CWE)-200: Exposure of Sensitive Information to an Unauthorized Actor]
- CVE-2023-20269 [CWE-288: Authentication Bypass Using an Alternate Path or Channel]

Additionally, the authoring agencies observed SafePay threat actors exploiting the following vulnerabilities across internet-exposed systems [T1190] for initial access through automated scripts:

- CVE-2023-27532 [CWE-306: Missing Authentication for Critical Function]
- CVE-2024-40711 [CWE-502: Deserialization of Untrusted Data]
- CVE-2024-40766 [CWE-284: Improper Access Control]

Execution, Persistence, Stealth, and Defense Impairment

After SafePay threat actors gain access to a victim network, they establish persistence by gaining administrative privileges on existing accounts [T1098], or on newly created accounts [T1136], using built-in administrative tools consistent with living off the land (LOTL) techniques. Once SafePay threat actors establish a foothold in a victim's network, they use LOTL binaries (LOLBins) [T1218], such as PsExec [T1021.002] and Windows Remote Management (WinRM) [T1021.006], to execute commands on remote systems. In several instances, SafePay threat actors used `ShareFinder.ps1`—a PowerShell script function used for enumerating network file shares in Windows Active Directory environments—to identify valuable assets for exfiltration [T1059.001, T1059.003]. Additionally, SafePay threat actors used `SharpShares.exe`, a tool used to identify and enumerate network file shares.

As SafePay threat actors prepare for lateral movement, they commonly disable security software [T1685] to avoid detection. In some cases, the threat actors changed the passwords of system users, making valid logins impossible. SafePay threat actors have also been observed using software packing or virtual machine software protection to conceal their code [T1027.002].

Privilege Escalation

The authoring agencies observed SafePay threat actors using a User Account Control (UAC) Bypass Privilege Escalation technique [T1548.002] that creates an elevated process through a specified component object model, enabling the execution of malicious commands or binaries [T1059]. SafePay threat actors have also been observed using token impersonation methods [T1134.001].

Lateral Movement

To pivot laterally through a network and identify files for exfiltration [TA0010] and encryption, SafePay threat actors use legitimate tools like PsExec, WinRM, and Remote Management and Monitoring [T1569.002] software. They also employ Remote Desktop Protocol (RDP) [T1021.001, T1133] to expand their presence within the compromised network [T1021]. As SafePay threat actors move laterally through a network, they look for credentials to gain admin access and will create accounts, if needed.

Collection, Exfiltration, and Impact

SafePay threat actors use legitimate tools, such as FileZilla, 7-Zip, RClone, and WinRAR to compress files and collect data [T1560.001], and WinSCP and RClone to facilitate the exfiltration of data [T1048] from the compromised network to actor-controlled accounts. In some instances, SafePay threat actors use OneDrive to exfiltrate data [T1567]. In other instances, the SafePay threat actors installed legitimate remote desktop tools like AnyDesk or TeamViewer on the victim's systems. SafePay threat actors use these tools to transfer ransomware and other software onto a victim's system. Additionally, SafePay threat actors

halt the Volume Shadow Copy Service and reset Network Attached Storage containing victim backup data to initial factory settings to inhibit system recovery attempts [T1490].

Following exfiltration, SafePay threat actors encrypt files [T1486] using a sophisticated hybrid encryption scheme to lock data. This involves combining a ChaCha20 stream cipher with an RSA public-key cryptosystem for a fast and secure key exchange. This multilayered approach customizes encryption methods based on file type and size and enables full or partial encryption. Data encrypted with the SafePay ransomware variant (appended with `.SafePay`) cannot be recovered without the decryption key. SafePay threat actors hold the encrypted data for ransom and typically demand a subset of company revenue in cryptocurrency in exchange for decryption software. SafePay threat actors leave a ransom note on the victim's system, typically on the desktop or root directory, advising them that SafePay locked their system and to reach out over a chat portal at a TOR `.onion` website link with a victim ID as the login. To put pressure on the victim, a representative makes phone calls on behalf of the ransomware group. If the victim does not pay, SafePay posts the exfiltrated data to their SafePay leak website, which is linked in the ransom note. Following encryption, SafePay may delete itself from the victim's filesystem [T1070.004].

Leveraged Tools

Table 1 lists publicly available tools and applications used by SafePay threat actors, including legitimate tools repurposed for their operations.
Note: These tools and applications should not be attributed as malicious without analytical evidence to support threat actor use and/or control.

Table 1. Tools Leveraged by SafePay Threat Actors

Tool Name	Description
7-Zip	An open source software that enables users to compress various file formats. SafePay threat actors maliciously use 7-Zip for data packaging and movement.
FileZilla	An open source client that enables users to transfer files between servers. SafePay threat actors use FileZilla maliciously for data exfiltration.
Mimikatz	A credential dumper that enables users to view and save authentication credentials, such as Kerberos tickets [T1550.002]. SafePay threat actors use Mimikatz for password exfiltration.
PowerShell	A cross-platform task automation solution used for various malicious activities, including command execution. It is composed of a command-line shell, a scripting language, and a configuration management framework—which runs on Windows, Linux, and macOS.
PsExec	A tool designed to run programs that SafePay threat actors use to execute commands on remote systems.

Tool Name	Description
RClone	A legitimate command-line program used to sync files with cloud storage services, such as Mega. SafePay threat actors maliciously use RClone for data packaging and movement.
ScreenConnect	A remote support, access, and meeting software that allows users to control devices remotely over the internet. SafePay threat actors use ScreenConnect for persistence and access.
ShareFinder.ps1	A PowerShell script used to scan an Active Directory network for shared folders. SafePay threat actors use `ShareFinder.ps1` for exfiltration hunting.
WinRAR	Archive utility used to split compromised data into segments and to compress [T1560.001] files into a `.RAR` format prior to exfiltration. SafePay threat actors use WinRAR for data packaging and movement.
WinRM	A Windows-based protocol designed to facilitate remote management and automation. SafePay threat actors use WinRM for command execution.
AnyDesk and TeamViewer	Legitimate remote desktop tool used for accessing and controlling computers over the internet. SafePay threat actors use AnyDesk and TeamViewer to transfer malware to the victim's system.
AcronisDiskDirector	A legitimate disk management tool.
SharpShares.exe	A network scanning tool used for host discovery and enumeration.
NetExec	A legitimate network assessment tool to enumerate systems, validate credentials, and manage remote operations across private networks.
Backblaze	A command-line tool for file management within Backblaze B2 cloud storage. SafePay threat actors executed commands via `b2.exe` to exfiltrate a victim's data.

Indicators of Compromise

Table 2 through **Table 5** list IOCs associated with SafePay ransomware that allowed for the identification of malicious activity.

Disclaimer: The authoring agencies recommend organizations investigate or verify IP addresses prior to taking action, such as blocking. These IOCs were observed between November 2024 and August 2026.

Table 2. IP Addresses

IP Address	Description
104.26.2[.]223	SafePay victim intrusion
140.82.114[.]4	SafePay victim intrusion
185.199.108[.]133	SafePay victim intrusion
77.37.49[.]40	SafePay victim intrusion
173.194.194[.]94	Hosting victim data
167.235.225[.]149	Client login panels
5.255.11[.]134	Used in exfiltration
88.119.167[.]239	soc.dll command and control
37.10.71[.]188	Used in exfiltration

Table 3. Malicious Files

Note: Some of these files are legitimate tools. The authoring organizations recommend organizations investigate or verify tool use prior to taking action, such as blocking.

Filename	Description
1 - Copy.bat	A batch script likely used to copy, stage, or move files during lateral movement or data collection.
CCleaner.exe/ CCleaner64.exe	A legitimate system utility; however, it is suspicious if deployed in enterprise environments for file cleanup or anti-forensics.
CCleaner*.exe / *.dll	A file used for potential masquerading or abuse of CCleaner components for execution or persistence.
dcsync.exe	A tool used to perform DCSync operations to extract Active Directory credentials; high-confidence credential theft activity.
domains.txt	An output file likely containing enumerated domain information.
DYRasWtb.exe	A suspected malicious executable.
libsmb2.dll	A library associated with Server Message Block (SMB) communication; may support lateral movement or file transfer.

Filename	Description
Libwa*.dll	A suspicious library set; likely part of a custom toolset or malware framework; requires further analysis.
License.txt	A benign file that may accompany tool packages or be used for masquerading. In one instance, it accompanied the tool “S.P_Network Scanner.”
locker.dll	A potential ransomware or encryption-related component.
netscan.exe	A network scanning tool used for host discovery and enumeration.
netscan.lic / netscan.xml	Output or configuration files associated with network scanning activity.
netscanNEW.zip	Archive file potentially used to stage or transfer scanning tools.
nltest.exe	Legitimate Windows tool used for domain trust enumeration; suspicious when used outside admin workflows.
oui.txt	A MAC address vendor lookup output—network reconnaissance artifact.
ping.txt	An output file from network connectivity testing.
portable.dat	A potential configuration or staging file (context-dependent).
scan.xml	An output file from scanning/enumeration tools.
sharefinder.ps1	A PowerShell script used to enumerate network shares (reconnaissance).
Socks.exe	A tool used to establish SOCKS proxy for tunneling traffic.
Socks_werfault.exe	A binary likely masquerading to blend with Windows processes.
subs.txt	A possible staging file or list of targets/data for exfiltration.
svchost.exe	A legitimate Windows process; suspicious if located outside System32 or used for masquerading.
wa_3rd_party_host_*.exe	A file of suspicious binaries—likely part of SafePay threat actor toolset or masquerading components.
winrar.exe	A legitimate archiving tool frequently used for data staging prior to exfiltration.

Filename	Description
AnyDesk.exe	A legitimate remote desktop tool for accessing and controlling computers over the internet; most of the time it is used to transfer malware to a victim's system.
SharpShares.exe	A network scanning tool used for host discovery and enumeration.
AcronisDiskDirector-12.5 / acro.exe / DiskDirector.exe / Acronis.exe	A legitimate disk management tool.
b2.exe	A command-line tool for data exfiltration to Backblaze B2 cloud storage.
nxc.exe	The executable for NetExec, a legitimate network assessment tool used to enumerate systems, validate credentials, and manage remote operations across private networks.

Table 4. SHA-1 Hash Values

Hash	File/Description
07353237350c35d6dc2c8f143b649cd07c71f62b	1.exe (ransomware binary)
b498a2683640c983bb069fa2ea9e67cef4a3797d	Locker.dll PE32 executable
BBFED53E3BB1F306F4DA97D995CF4AE5B73AD081	locker.dll
d711a5af5aed48a3b36b98f4fcf52809aebef7a2	nxc

Table 5. SHA-256 Hash Files

Hash	File/Description
921df888aaabcd828a3723f4c9f5fe8b8379c6b7067d16b2ea10152300417eae	soc.dll
6c1d36df94ebe367823e73ba33cfb4f40756a5e8ee1e30e8f0ae55d47e220a6a	RunPE bundled DLL
e79608cf1d6b51324c14bef8883054c1238ed5f080222cc464810e6e14adc346	Injected PE
327b8b61eb446cc4f710771e44484f62b804ae3d262b57a56575053e2df67917	locker.dll PE32 executable

Hash	File/Description
a0dc80a37eb7e2716c02a94adc8df9baedec192a77bde31669faed228d9ff526	locker.dll
BBDD3620A67AEDEC4B9A68B2C9CC880B6631215E129816AEA19902A6F4BC6F41	SharpShares.exe

The following are IOC hostnames:

- WIN-SBOE3CPNAL
- WIN-3IUUOFVTQAR
- WIN-DK18BI83M0S
- WIN-I1HRRJHCEIV

MITRE ATT&CK Tactics and Techniques

See **Table 6** through **Table 16** for all referenced threat actor tactics and techniques in this advisory. 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.

Table 6. Initial Access

Technique Title	ID	Use
External Remote Services	T1133	SafePay threat actors use external remote services, such as VPNs or other tools, to externally connect to an internal network.
Exploit Public-Facing Application	T1190	SafePay threat actors attempt to exploit a vulnerability within a system to gain access. Common vulnerabilities include software bugs, glitches, or misconfigurations.

Table 7. Execution

Technique Title	ID	Use
Command and Scripting Interpreter: PowerShell	T1059.001	SafePay threat actors use PowerShell, an interactive command-line interface and scripting environment contained within Windows, to identify code within a targeted network.
Command and Scripting Interpreter: Windows Command Shell	T1059.003	SafePay threat actors use the Windows command shell prompt to gain control of a component on a system that requires specific permissions depending on the command executed.

Technique Title	ID	Use
System Services: Service Execution	T1569.002	SafePay threat actors use tools, such as PsExec, to execute commands on remote systems.
Command and Scripting Interpreter	T1059	SafePay threat actors use Windows UAC to elevate a program's privileges, enabling the execution of malicious commands or binaries.

Table 8. Persistence

Technique Title	ID	Use
Account Manipulation	T1098	SafePay threat actors establish persistence by gaining administrative privileges on existing accounts.

Table 9. Privilege Escalation

Technique Title	ID	Use
Abuse Elevation Control Mechanism: Bypass User Account Control	T1548.002	SafePay threat actors use Windows UAC to elevate a program's privileges and execute a task on an administrator-level permission scale.

Table 10. Stealth

Technique Title	ID	Use
Obfuscated Files or Information: Software Packing	T1027.002	SafePay threat actors use software packing to conceal malicious code by means of encrypting an executable to avoid detection.
Indicator Removal: File Deletion	T1070.004	SafePay threat actors delete files associated with the intrusion activity to minimize their digital footprint and obfuscate malicious activities.
System Binary Proxy Execution	T1218	SafePay threat actors proxy the execution of malicious content with a trusted binary, often a Microsoft-signed file, to bypass signature-based network defenses.

Table 11. Defense Impairment

Technique Title	ID	Use
Disable or Modify Tools	T1685	SafePay threat actors disable security features, modify or delete registry keys or configuration files to impair functionality, and disable updates such as security patches on a system or network.

Table 12. Credential Access

Technique Title	ID	Use
Brute Force	T1110	SafePay threat actors gain access to accounts by implementing brute force password attacks.

Table 13. Lateral Movement

Technique Title	ID	Use
Remote Services: Remote Desktop Protocol	T1021.001	SafePay threat actors gain access to a valid account using RDP and typically disable cybersecurity features, such as Windows Defender, while using LOLBins.
Remote Services: SMB/Windows Admin Shares	T1021.002	SafePay threat actors gain access to a valid account using SMB to enable lateral movement throughout a network.
Remote Services	T1021	SafePay threat actors employ remote services to expand their presence within the compromised network.
Remote Services: Windows Remote Management	T1021.006	SafePay threat actors use tools, such as WinRM, to execute commands on remote systems.

Table 14. Collection

Technique Title	ID	Use
Archive Collected Data: Archive via Utility	T1560.001	SafePay threat actors use utilities to compress or encrypt collected data prior to exfiltration to change the format of the data to one compatible for transportation.
Archive Collected Data: Archive via Library	T1560.002	SafePay threat actors use credential dumpers, such as Mimikatz, for password exfiltration.

Table 15. Exfiltration

Technique Title	ID	Use
Exfiltration Over Alternative Protocol	T1048	SafePay threat actors exfiltrate data over an alternative protocol, including file transfer protocol, simple mail transfer protocol, HTTP/S, domain name system, SMB, or another network protocol variation that is not the main or current command and control channel.
Exfiltration Over Web Service	T1567	SafePay threat actors exfiltrate data over web services, such as OneDrive.

Table 16. Impact

Technique Title	ID	Use
Data Encrypted for Impact	T1486	SafePay threat actors encrypt data on targeted systems to disrupt access to a particular system or network service. They then demand a ransom payment in exchange for a decryption key.
Inhibit System Recovery	T1490	SafePay threat actors disable services designed to assist in recovery of a corrupted system. In some cases, SafePay threat actors deleted all network-attached backups of company data.

Incident Response

If a potential compromise is detected, but ransomware actors have not (yet) encrypted items, organizations should take the following actions:

1. **Determine which hosts were compromised and isolate them** by quarantining or taking them offline.
2. **Initiate threat hunting activities to scope the intrusion**. Collect and review relevant artifacts, logs, and other data to identify threat actor TTPs, compromised devices and accounts, a timeline of activity, etc.
3. **Report the suspected compromise** to the FBI and other agencies as appropriate (if located within the U.K., report the compromise to Report Fraud or local police force) (see the **Reporting** section for contact information).
4. **Apply eviction countermeasures**, including those listed below, to contain the incident and eradicate the threat actor from the network (**Note:** Start applying countermeasures after collecting enough threat hunting data to inform effective countermeasure selection; this will likely overlap with threat hunting activities).
    a. Use CISA's Eviction Strategies Tool to assemble countermeasures for a systematic eviction plan—the tool comprises **Playbook-NG** (a web application) and **COUN7ER** (a database of post-compromise countermeasures mapped to adversary TTPs).

i. Use Playbook-NG and COUN7ER together to assemble a systematic eviction plan, or playbook, that leverages distinct countermeasures to contain and evict cyber threat actors. The playbook features a list of recommended response actions based on threat actor TTPs and includes each action's intended outcome, preparatory steps, and associated risks. For more information, see CISA's Eviction Strategies Tool fact sheet.

5. **Harden the network to prevent additional malicious activity** (see **Mitigations** for guidance).

If compromise is detected and items have been encrypted, see the "Ransomware and Data Extortion Response Checklist" in CISA's joint #StopRansomware Guide.

Mitigations

The authoring agencies recommend organizations implement the mitigations below to improve their cybersecurity posture on the basis of the threat actors' 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 CPGs webpage for more information on the CPGs, including additional recommended baseline protections.

Organizations should implement the following mitigations:

- **Prioritize remediating known exploited vulnerabilities (KEVs) and keep all operating systems, software, and firmware up to date**, as timely patching is one of the most efficient and cost-effective steps an organization can take to minimize its exposure to cybersecurity threats; specifically, prioritize patching KEVs in internet-facing systems. [CPG 2.B].
  - Additionally, using Binding Operational Directive 26-04 offers a framework for patch prioritization based on technology type and steps for forensics triage. Under its implementation guidance, it offers guidance and steps to perform forensic triage for severe vulnerability cases.
- **Implement identity, credential, and access management (ICAM) policies across the organization and require MFA** for all services to the greatest extent possible—particularly for webmail, VPNs, and accounts that access critical systems [CPG 3.F].
- **Require all accounts** with password logins (e.g., service accounts, admin accounts, and domain admin accounts) to comply with NIST's digital identity guidelines; require employees to use long passwords and consider not requiring recurring password changes, as these can weaken security [CPG 3.B].
  - Use longer passwords consisting of at least 15 characters and no more than 64 characters in length.
  - Store passwords in a hashed format using industry-recognized password managers.
  - Add password user "salts" to shared login credentials.
  - Avoid reusing passwords [CPG 3.C].
  - Implement multiple failed login attempt account lockouts [CPG 3.E].

  - Disable password "hints."
  - Refrain from requiring password changes more frequently than once per year.
    Note: NIST guidance suggests favoring longer passwords instead of requiring frequent password resets. Frequent password resets are more likely to result in users developing password patterns cyber threat actors can easily decipher.
- **Maintain offline backups of data and regularly test and maintain backup and restoration processes** [CPG 3.O]; implementing this practice helps organizations avoid severe operational interruptions and prevents scenarios in which data is irretrievable.
- **Ensure all backup data is encrypted, immutable** (i.e., cannot be altered or deleted), and covers the entire organization's data infrastructure [CPG 3.K].
- **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 (e.g., hard drives, storage devices, or the cloud) [CPG 3.I, 3.O, 1.C].
- **Segment networks** to prevent the spread of ransomware, as network segmentation can help control traffic flows between, and access to, various subnetworks and restrict adversary lateral movement [CPG 3.I].
- **Identify, detect, and investigate abnormal activity and potential traversal of the indicated ransomware with a network monitoring tool** [CPG 4.B].
  - To aid in detecting 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.
- **Filter network traffic** by preventing unknown or untrusted origins from accessing remote services on internal systems—this prevents threat actors from directly connecting to remote access services that they have established for persistence.
- **Review domain controllers, servers, workstations, and Active Directories** for new, unactive and/or unrecognized accounts.
- **Disable unused ports**.
- **Consider adding an email banner to emails received from outside of your organization.**
- **Audit user accounts** with administrative privileges and configure access controls according to the principle of least privilege [CPG 3.G].
- **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 Maturity 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,** since privilege escalation and lateral movement often depend on software utilities running from the command line; if threat actors cannot run these tools, they will have difficulty escalating privileges and moving laterally [CPG 3.M].

These mitigations align with principles 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 implementing secure by design tactics, software manufacturers can make their product lines secure "out of the box" without requiring customers to make additional configuration changes, purchasing product security add-in software and logs, monitoring, and making frequent security updates.

Validate Security Controls

In addition to applying mitigations, the authoring agencies 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.

To get started:

1. Select an ATT&CK technique described in this advisory (see **Table 6** to **Table 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.

The authoring agencies 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 provides one central location for ransomware resources and alerts.
- CISA's #StopRansomware Guide provides organizations with comprehensive best practices to mitigate the risk of ransomware attacks.

- CISA's Known Exploited Vulnerabilities Catalog is an authoritative resource for organizations to support improvement of their patch management best practices.
- CISA's Multifactor Authentication webpage provides best practices for network defenders to mitigate threats to accounts and systems that use MFA.
- CISA's Cyber Hygiene Services help organizations reduce the risk of a successful cyberattack.
- USSS's Preparing for a Cyber Incident outlines basic steps an organization can take before, during, and after a cyber incident.
- CISA's Cyber Security Evaluation Tool (CSET) provides a systematic, disciplined, and repeatable approach for evaluating an organization's security posture; see Downloading and Installing CSET for step-by-step guidance to help your organization evaluate cybersecurity practices on your networks.
- CISA's Ransomware Risk Assessment helps assess an organization's ability to counteract a ransomware infection.
- Department of Health and Human Services' Cybersecurity Performance Goals is a resource to help healthcare organizations implement high-impact cybersecurity practices.
- CISA's Binding Operational Directive 26-04: Prioritizing Security Updates Based on Risk and its implementation guidance
- CISA's CI Fortify: Strengthening Resilience Across Critical Infrastructure
- CISA's Eviction Strategies Tool enables incident response teams to quickly turn observed behaviors into remediation plans
- U.K.'s National Cyber Security Centre
- U.K.'s National Crime Agency

Reporting

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

The FBI and other authoring agencies are interested in any information, to include boundary logs showing communication to and from foreign IP addresses, a sample ransom note, communications with threat actors, Bitcoin wallet information, decryptor files, and/or a benign sample of an encrypted file.

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

The authoring agencies 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 Complaint Center (IC3), a local FBI field office, a local USSS Field Office, or CISA via the agency's Incident Reporting System or its 24/7 Operations Center (contact@cisa.dhs.gov) or by calling 1-844-Say-CISA (1-844-729-2472).

In the U.K., report incidents of a cybercrime or fraud at the UK's Home for Reporting Cyber Crime & Fraud or 0300-123-2040, your local police force, or use the non-emergency number 101.

Disclaimer

The information in this report is being provided "as is" for informational purposes only. CISA and the FBI/USSS 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 the FBI, CISA, or USSS.

The authoring agencies recognize that infrastructure used for malicious activity may be hosted on cloud or virtualized platforms where IP addresses can be dynamically or temporarily assigned. As a result, an address associated with malicious activity at one point in time may later be reassigned to benign services. Accordingly, these indicators should be interpreted as historically observed infrastructure within the activity window and should be corroborated with current network telemetry or additional intelligence sources when used for defensive or investigative purposes.

Version History

October 20, 2026: Initial version.