JOINT
CYBERSECURITY
ADVISORY

TLP:CLEAR

Co-Authored by:

Product ID: AA25-203A

July 22, 2025

#StopRansomware: Interlock

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

- Prevent initial access by implementing domain name system (DNS) filtering and web access firewalls, and training users to spot social engineering attempts.
- Mitigate known vulnerabilities by ensuring operating systems, software, and firmware are patched and up to date.
- Segment networks to restrict lateral movement from initial infected devices and other devices in the same organization.
- Implement identity, credential, and access management (ICAM) policies across the organization and then require multifactor authentication (MFA) for all services to the extent possible.

Summary

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

The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), Department of Health and Human Services (HHS), and Multi-State Information Sharing and Analysis Center (MS-ISAC)—hereafter referred to as "the authoring agencies"—are releasing this joint advisory to

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.

disseminate known Interlock ransomware IOCs and TTPs identified through FBI investigations (as recently as June 2025) and trusted third-party reporting.

The Interlock ransomware variant was first observed in late September 2024, targeting various business, critical infrastructure, and other organizations in North America and Europe. FBI maintains these actors target their victims based on opportunity, and their activity is financially motivated. FBI is aware of Interlock ransomware encryptors designed for both Windows and Linux operating systems; these encryptors have been observed encrypting virtual machines (VMs) across both operating systems. FBI observed actors obtaining initial access via drive-by download from compromised legitimate websites, which is an uncommon method among ransomware groups. Actors were also observed using the ClickFix social engineering technique for initial access, in which victims are tricked into executing a malicious payload under the guise of fixing an issue on the victim's system. Actors then use various methods for discovery, credential access, and lateral movement to spread to other systems on the network.

Interlock actors employ a double extortion model in which actors encrypt systems after exfiltrating data, which increases pressure on victims to pay the ransom to both get their data decrypted and prevent it from being leaked.

FBI, CISA, HHS, and MS-ISAC encourage organizations to implement the recommendations in the **Mitigations** section of this advisory to reduce the likelihood and impact of Interlock ransomware incidents.

For a downloadable copy of IOCs, see:

- AA25-203A STIX XML (63KB)
- AA25-203A STIX JSON (57KB)

Technical Details

Note: This advisory uses the MITRE ATT&CK® Matrix for Enterprise framework, version 17. See the **MITRE ATT&CK Tactics and Techniques** section of this advisory for tables mapped to the threat actors' activity.

Overview

Since September 2024, Interlock ransomware actors have impacted a wide range of businesses and critical infrastructure sectors in North America and Europe. These actors are opportunistic and financially motivated in nature and employ tactics to infiltrate and disrupt the victim's ability to provide their essential services.

Interlock actors leverage a double extortion model, in which they both encrypt and exfiltrate victim data. Ransom notes do not include an initial ransom demand or payment instructions; instead, victims are provided with a unique code and are instructed to contact the ransomware group via a `.onion` URL through the Tor browser. To date, Interlock actors have been observed encrypting VMs, leaving hosts, workstations, and physical servers unaffected; however, this does not mean they will not expand to these systems in the future. To counter Interlock actors' threat to VMs, enterprise defenders should implement robust endpoint detection and response (EDR) tooling and capabilities.

The authoring agencies are aware of emerging open-source reporting detailing similarities between the Rhysida and Interlock ransomware variants.[1] For additional information on Rhysida ransomware, see the joint advisory, #StopRansomware: Rhysida Ransomware.

Initial Access

FBI has observed Interlock actors obtaining initial access [TA0001] via drive-by download [T1189] from compromised legitimate websites, an atypical method for ransomware actors. Interlock ransomware methods for initial access have previously disguised malicious payloads as fake Google Chrome or Microsoft Edge browser updates, though a cybersecurity company recently reported a shift to payload filenames masquerading as updates for common security software (see **Table 3** and **Table 4** for a list of filenames).[2]

In some instances, FBI has observed Interlock actors using the ClickFix social engineering technique, in which unsuspecting users are prompted to execute a malicious payload by clicking a fake Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) [T1189]. The CAPTCHA contains instructions for users to open the Windows Run window, paste the clipboard contents, and then execute a malicious Base64-encoded PowerShell process [T1204.004].[3]

Note: This ClickFix technique has been used in several other malware campaigns, including Lumma Stealer and DarkGate.[4]

Execution and Persistence

Based on FBI investigations, the fake Google Chrome browser executable functions as a remote access trojan (RAT) [T1105] designed to execute a PowerShell script [T1059.001] that drops a file into the Windows Startup folder. From there, the file is designed to run the RAT every time the victim logs in [T1547.001], establishing persistence [TA0003].

FBI also observed instances in which Interlock actors executed a PowerShell command designed to establish persistence via a Windows Registry key modification [T1547.001]. To do so, Interlock actors used a PowerShell command [T1059.001] designed to add a run key value named “Chrome Updater” [T1036.005] that uses a specific log file as an argument upon user login.

Reconnaissance

To facilitate reconnaissance, a PowerShell script executes a series of commands [T1059.001] designed to gather information on victim machines (see **Table 1**).

Table 1. PowerShell Commands for Reconnaissance

PowerShell Command	Description
WindowsIdentity.GetCurrent()	Returns a WindowsIdentity object that represents the current Windows user [T1033].

PowerShell Command	Description
systeminfo	Displays detailed configuration information [T1082] about a computer and its operating system, including operating system configuration, security information, product ID, and hardware properties.
tasklist/svc	Lists unabridged service information [T1007] for each process currently running on the local computer.
Get-Service	Gets objects that represent the services [T1007] on a computer, including running and stopped services.
Get-PSDrive	Gets the drives [T1082] in the current session, such as: ▪ Windows logical drives on the computer, including drives mapped to network shares. ▪ Drives exposed by PowerShell providers. ▪ Session-specified temporary drives and persistent mapped network drives.
arp -a	Displays and modifies entries in the Address Resolution Protocol (ARP) cache table [T1016], which contains entries on the IPv4 and IPv6 addresses on host endpoints.

Command and Control

FBI observed Interlock actors using command and control (C2) [TA0011] applications like Cobalt Strike and SystemBC. Interlock actors also used Interlock RAT[5] and NodeSnake RAT (as of March 2025)[6] for C2 and executing commands.

Credential Access, Lateral Movement, and Privilege Escalation

FBI observed that once Interlock actors establish remote control of a compromised system, they use a series of PowerShell commands to download a credential stealer (`cht.exe`) [TA0006] and keylogger binary (`klg.dll`) [T1056.001][T1105]. According to open source reporting, the credential stealer collects login information and associated URLs for victims' online accounts [T1555.003], while the keylogger dynamic link library (DLL) logs users' keystrokes in a file named `conhost.txt` [T1036.005].[7] As of February 2025, private cybersecurity analysts also observed Interlock ransomware infections executing different versions of information stealers [TA0006], including Lumma Stealer[8] and Berserk Stealer, to harvest credentials for lateral movement and privilege escalation [T1078].[9]

Interlock actors leverage compromised credentials and Remote Desktop Protocol (RDP)[10] [T1021.001] to move between systems. They also use tools like AnyDesk to enable remote connectivity and PuTTY to assist with lateral movement [T1219].[11] In addition to stealing users' online credentials, Interlock actors have compromised domain administrator accounts (possibly by using a Kerberoasting attack [T1558.003]).[12] to gain additional privileges [T1078.002].

Collection and Exfiltration

Interlock actors leverage Azure Storage Explorer (`StorageExplorer.exe`) to navigate victims' Microsoft Azure Storage accounts [T1530] prior to exfiltrating data. According to open source reporting, Interlock actors execute AzCopy to exfiltrate data by uploading it to the Azure storage blob [T1567.002].[13] Interlock actors also exfiltrate data over file transfer tools, including WinSCP [T1048].

Impact

Following data exfiltration, Interlock actors deploy the encryption binary as a 64-bit executable named `conhost.exe` [T1486] [T1036.005]. FBI has observed Interlock ransomware encryptors for both Windows and Linux operating systems. Encryptors are designed to encrypt files using a combined Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA) algorithm. In addition, cybersecurity researchers have identified Interlock ransomware samples using a FreeBSD ELF encryptor [T1486], a departure from usual Linux encryptors designed for VMware ESXi servers and VMs.[14]

A cybersecurity company identified a DLL binary named `tmp41.wasd`—executed after encryption using `rundll32.exe` [T1218.011]—which uses the `remove()` function to delete the encryption binary [T1070.004];[15] on Linux machines, the encryptor uses a similar technique to execute the `removeme` function.

Encrypted files are appended with either a `.interlock` or `.1nt3rlock` file extension, alongside a ransom note titled `!__README__!.txt` delivered via group policy object (GPO). Interlock actors use a double-extortion model [T1657], encrypting systems after exfiltrating data. The ransom note provides each victim with a unique code and instructions to contact the ransomware actors via a `.onion` URL.

Interlock actors do not leave an initial ransom demand or payment instructions on compromised networks, and do not relay this information until contacted by the victim. The actors instruct victims to make ransom payments in Bitcoin to cryptocurrency wallet addresses provided by the actors. The actors threaten to publish the victim's exfiltrated data to their leak site on the Tor network unless the victim pays the ransom demand; the actors have previously followed through on this threat.[16]

Leveraged Tools

See **Table 2** for publicly available tools and applications used by Interlock ransomware actors. This includes legitimate tools repurposed for their operations.

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

Table 2. Tools Used by Interlock Ransomware Actors

Tool Name	Description
AnyDesk	A common legitimate remote monitoring and management (RMM) tool maliciously used by Interlock actors to obtain remote access and maintain persistence. AnyDesk also supports remote file transfer.

Tool Name	Description
Cobalt Strike	A penetration testing tool used by security professionals to test the security of networks and systems.
PowerShell	A cross-platform task automation solution made up of a command-line shell, a scripting language, and a configuration management framework, which runs on Windows, Linux, and macOS.
PSExec	A tool designed to run programs and execute commands on remote systems.
PuTTY.exe	An open source file transfer application commonly used to remotely connect to systems via Secure Shell (SSH). PuTTY also supports file transfer protocols like Secure File Transfer Protocol (SFTP) and Secure Copy Protocol (SCP).
ScreenConnect	A remote support, access, and meeting software that allows users to control devices remotely over the internet. CISA observed Interlock actors using a cracked version of this software in at least one incident. These versions may be standalone versions not connecting to ScreenConnect's official cloud domains (domains available upon request from ConnectWise).
SystemBC	Enables Interlock actors to compromise systems, run commands, download malicious payloads, and act as a proxy tool to the actors' C2 servers.
Windows Console Host	Windows Console Host (`conhost.exe`) manages the user interface for command-line applications in Windows, including Command Prompt and PowerShell.
WinSCP	A free and open source SSH File Transfer Protocol (FTP), WebDAV, Amazon S3, and secure copy protocol client.

Leveraged Files

See **Table 3** and **Table 4** for files used by Interlock ransomware actors. These were obtained from FBI investigations as recently as June 2025.

Disclaimer: Some of the hashes are for legitimate tools and applications and should not be attributed as malicious without analytical evidence to support threat actor use and/or control. The authoring agencies recommend organizations investigate or vet these hashes prior to taking action, such as blocking.

Table 3. Files Used by Interlock Ransomware Actors (SHA-256)

File Name	Hash
1.ps1	fba4883bf4f73aa48a957d894051d78e0085ecc3170b1ff50e61ccec6aeee2cd

File Name	Hash
advanced_port_scanner.exe	4b036cc9930bb42454172f888b8fde1087797fc0c9d31ab546748bd2496bd3e5
Aisa.exe	18a507bf1c533aad8e6f2a2b023fbbcac02a477e8f05b095ee29b52b90d47421
AnyDesk.exe	1a70f4eef11fbecb721b9bab1c9ff43a8c4cd7b2cafef08c033c77070c6fe069
autoservice.dll	a4069aa29628e64ea63b4fb3e29d16dcc368c5add304358a47097eedafbbb565
Autostart.exe	d535bdc9970a3c6f7ebf0b229c695082a73eaeaf35a63cd8a0e7e6e3ceb22795
cht	FAFCD5404A992850FFCFFEE46221F9B2FF716006AECB637B80E5CD5AA112D79C
cht.exe	C20BABA26EBB596DE14B403B9F78DDC3C13CE9870EEA332476AC2C1DD582AA07
cleanup.dll (SystemBC)	1845a910dcde8c6e45ad2e0c48439e5ab8bbbeb731f2af11a1b7bbab3bfe0127
conhost	44887125aa2df864226421ee694d51e5535d8c6f70e327e9bcb366e43fd892c1
conhost.dll	a70af759e38219ca3a7f7645f3e103b13c9fb1db6d13b68f3d468b7987540ddf
conhost.dll	96babe53d6569ee3b4d8fc09c2a6557e49ebc2ed1b965abda0f7f51378557eb1
difxepi.dll (SystemBC)	1845a910dcde8c6e45ad2e0c48439e5ab8bbbeb731f2af11a1b7bbab3bfe0127
iexplore.exe	d0c1662ce239e4d288048c0e3324ec52962f6ddda77da0cb7af9c1d9c2f1e2eb
klg.dll	A4F0B68052E8DA9A80B70407A92400C6A5DEF19717E0240AC608612476E1137E
!!!OPEN_ME!!!.txt	68A49D5A097E3850F3BB572BAF2B75A8E158DADB70BADDC205C2628A9B660E7A
processhacker-2.39-bin.zip	88f26f3721076f74996f8518469d98bf9be0eaee5b9eccc72867ebfc25ea4e83
PsExec.exe	078163d5c16f64caa5a14784323fd51451b8c831c73396b967b4e35e6879937b
putty.exe	7a43789216ce242524e321d2222fa50820a532e29175e0a2e685459a19e09069
puttyportable.exe	97931d2e2e449ac3691eb526f6f60e2f828de89074bdac07bd7dbdfd51af9fa0
PuTTYPortable.zip	ff7ad2376ae01e4b3f1e1d7ae630f87b8262b5c11bc5d953e1ac34ffe81401b5

File Name	Hash
qrpce91.exe.asd	64a0ab00d90682b1807c5d7da1a4ae67cde4c5757fc7d995d8f126f0ec8ae983
ScreenConnect.ClientService.exe	2814b33ce81d2d2e528bb1ed4290d665569f112c9be54e65abca50c41314d462
SophosendpointAgent.exe	f51b3d054995803d04a754ea3ff7d31823fab654393e8054b227092580be43db
SophosScaner.exe	dfb5ba578b81f05593c047f2c822eeb03785aecffb1504dcb7f8357e898b5024
Starship.exe	94bf0aba5f9f32b9c35e8dfc70afd8a35621ed6ef084453dc1b10719ae72f8e2
start	28c3c50d115d2b8ffc7ba0a8de9572fbe307907aaae3a486aabd8c0266e9426f
start.exe	70bb799557da5ac4f18093decc60c96c13359e30f246683815a512d7f9824c8f
StorageExplorer.exe	73a9a1e38ff40908bcc15df2954246883dadfb991f3c74f6c514b4cffdabde66
Sysmon.sys	1d04e33009bcd017898b9e1387e40b5c04279c02ebc110f12e4a724ccdb9e4fb
upd_2327991.exe	7b9e12e3561285181634ab32015eb653ab5e5cfa157dd16cdd327104b258c332
webujgd.lnk	70EE22D394E107FBB807D86D187C216AD66B8537EDC67931559A8AEF18F6B5B3
WinSCP-6.3.5-Setup.exe	8eb7e3e8f3ee31d382359a8a232c984bdaa130584cad11683749026e5df1fdc3
Proxy Tool	e4d6fe517cdf3790dfa51c62457f5acd8cb961ab1f083de37b15fd2fddeb9b8f
Encryptor	e86bb8361c436be94b0901e5b39db9b6666134f23cce1e5581421c2981405cb1
Encryptor	c733d85f445004c9d6918f7c09a1e0d38a8f3b37ad825cd544b865dba36a1ba6
Encryptor	28c3c50d115d2b8ffc7ba0a8de9572fbe307907aaae3a486aabd8c0266e9426f

Table 4. Files Used by Interlock Ransomware Actors (SHA-1)

File Name	Hash
autorun.log	514946a8fc248de1ccf0dbeee2108a3b4d75b5f6
jar.jar	b625cc9e4024d09084e80a4a42ab7ccaa6afb61d

File Name	Hash
pack.jar	3703374c9622f74edc9c8e3a47a5d53007f7721e

MITRE ATT&CK Tactics and Techniques

See **Table 5** 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 5. Initial Access

Technique Title	ID	Use
Drive-By Compromise	T1189	Interlock actors obtain initial access by compromising a legitimate website that network users visit, or by disguising malicious payloads as fake browser updates or common security software, including the following:[17] ▪ FortiClient.exe ▪ Ivanti-Secure-Access-Client.exe ▪ GlobalProtect.exe ▪ Webex.exe ▪ AnyConnectVPN.exe ▪ Cisco-Secure-Client.exe ▪ zyzoom_antimalware.exe Interlock actors also gain access via the ClickFix social engineering technique, in which users are tricked into executing a malicious payload by clicking on a fake CAPTCHA that prompts users to execute a malicious PowerShell script.

Table 6. Execution

Technique Title	ID	Use
Command and Scripting Interpreter: PowerShell	T1059.001	Interlock actors implement PowerShell scripts to drop a malicious file into the Windows Startup folder. Interlock actors execute a PowerShell command for registry key modification. Interlock actors use a PowerShell script to execute a series of commands to facilitate reconnaissance.

Technique Title	ID	Use
User Execution: Malicious Copy and Paste	T1204.004	Via the ClickFix social engineering technique, users are tricked into clicking a fake CAPTCHA and prompted into executing a malicious Base64-encoded PowerShell process by following instructions to open a Windows Run window (Windows Button + R), pasting clipboard contents ("CTRL + V"), and then executing the malicious script ("Enter").

Table 7. Persistence

Technique Title	ID	Use
Boot or Logon Autostart Execution: Registry Run Keys/Startup Folder	T1547.001	Interlock actors establish persistence by adding a file into a Windows StartUp folder that executes a RAT every time a user logs in. Interlock actors also implement registry key modification by using a PowerShell command to add a run key value (named "Chrome Updater") that uses a log file as an argument every time a user logs in.

Table 8. Privilege Escalation

Technique Title	ID	Use
Valid Accounts: Domain Accounts	T1078.002	Interlock actors compromise domain administrator accounts to gain additional privileges.

Table 9. Defense Evasion

Technique Title	ID	Use
Defense Evasion	TA0005	Interlock actors execute the `removeme` function on Linux systems to delete the encryption binary for defense evasion.
Masquerading: Match Legitimate Resource Name or Location	T1036.005	Interlock actors disguise a malicious run key value by naming it "Chrome Updater"; the run key value uses a specific log file as an argument upon user login. Interlock actors disguise files of keystrokes logged by one of their credential stealers with a legitimate Windows filename: `conhost.txt`. Interlock actors disguise an encryption binary, a 64-bit executable, by giving it the same name as the legitimate Console Windows Host executable: `conhost.exe`

Technique Title	ID	Use
System Binary Proxy Execution: Rundll32	T1218.011	Interlock actors use `rundll32.exe` to proxy execution of a malicious DLL binary `tmp41.wasd`.
Indicator Removal: File Deletion	T1070.004	Interlock actors execute a DLL binary `tmp41.wasd` that uses the `remove()` function to delete their encryption binary for defense evasion.

Table 10. Credential Access

Technique Title	ID	Use
Credential Access	TA0006	Interlock actors download credential stealer `cht.exe` and execute other versions information stealers (including Lumma Stealer and Berserk Stealer) to harvest credentials.
Credentials from Password Stores: Credentials from Web Browsers	T1555.003	Interlock actors download a credential stealer that collects login information and associated URLs for victims' online accounts.
Input Capture	T1056	Interlock actors execute Lumma Stealer and Berserk Stealer information stealers on victim systems.
Input Capture: Keylogging	T1056.001	Interlock actors download `klg.dll`, a keylogger binary, onto compromised systems, where it logs users' keystrokes in a file named `conhost.txt`.
Steal or Forge Kerberos Tickets: Kerberoasting	T1558.003	Interlock actors possibly use a Kerberoasting attack to compromise domain administrator accounts.

Table 11. Discovery

Technique Title	ID	Use
System Owner/User Discovery	T1033	Interlock actors execute a PowerShell command `WindowsIdentity.GetCurrent()` on victim systems to retrieve a WindowsIdentity object that represents the current Windows user.

Technique Title	ID	Use
System Information Discovery	T1082	Interlock actors execute a PowerShell command `systeminfo` on victim systems to access detailed configuration information about the system, including OS configuration, security information, product ID, and hardware properties. Interlock actors execute a PowerShell command `Get-PSDrive` on victim systems to discover the drives in the current session, such as: ▪ Windows logical drives on the computer, including drives mapped to network shares. ▪ Drives exposed by PowerShell providers. ▪ Session-specified temporary drives and persistent mapped network drives.
System Service Discovery	T1007	Interlock actors execute a PowerShell command `tasklist /svc` on victim systems that lists service information for each process currently running on the system. Actors also execute a PowerShell command `Get-Service` on victim systems that retrieves objects that represent the services (including running and stopped services) on the system.
System Network Configuration Discovery	T1016	Interlock actors execute a PowerShell command `arp -a` on victim systems that displays and modifies entries in the Address Resolution Protocol (ARP) cache table (which contains entries on the IPv4 and IPv6 addresses on host endpoints).

Table 12. Lateral Movement

Technique Title	ID	Use
Valid Accounts	T1078	Interlock actors harvest and abuse valid credentials for lateral movement and privilege escalation.
Remote Services: Remote Desktop Protocol	T1021.001	Interlock actors use RDP and valid credentials to move laterally between systems.

Table 13. Collection

Technique Title	ID	Use
Data from Cloud Storage	T1530	Interlock actors use `StorageExplorer.exe`, the cloud storage solution Azure Storage Explorer, to explore Microsoft Azure Storage accounts.

Table 14. Command and Control

Technique Title	ID	Use
Command and Control	TA0011	Interlock actors use applications Cobalt Strike and SystemBC for C2.
Ingress Tool Transfer	T1105	Interlock actors use a fake Google Chrome or Microsoft Edge browser update to cause users to execute a RAT on the victimized system. Interlock actors download credential stealers (`cht.exe`) and keylogger binaries (`klg.dll`) once actors establish remote control of a compromised system.
Remote Access Tools	T1219	Interlock actors use legitimate remote access tools such as AnyDesk to enable remote connectivity and PuTTY to assist with lateral movement.

Table 15. Exfiltration

Technique Title	ID	Use
Exfiltration Over Web Service: Exfiltration to Cloud Storage	T1567.002	Interlock actors exfiltrate data to cloud storage by executing AzCopy to upload data to the Azure storage blob.
Exfiltration Over Alternative Protocol	T1048	Interlock actors use file transfer tools like WinSCP to exfiltrate data.

Table 16. Impact

Technique Title	ID	Use
Data Encrypted for Impact	T1486	Interlock actors encrypt victim data using a combined AES and RSA algorithm on compromised systems to interrupt availability to system and network resources. Actors code encryptors using C/C++. Interlock actors use encryptors for both Windows and Linux operating systems. Interlock actors also use a FreeBSD ELF encryptor to encrypt victim data.
Financial Theft	T1657	Interlock actors deliver a ransom note titled `!__README__!.txt` via a GPO which provides victims with instructions to use a `.onion` URL to contact the actors over the Tor network. Actors use a double-extortion model, both encrypting victim data and threatening release of victim data on their Tor network leak site if the ransom is not paid.

Mitigations

The authoring agencies recommend organizations implement the mitigations below to improve your organization's cybersecurity posture on the basis of the Interlock ransomware 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 and TTPs. Visit CISA's CPGs webpage for more information on the CPGs, including additional recommended baseline protections.

In addition to the below mitigations, Healthcare and Public Health (HPH) organizations should use HPH Sector CPGs to implement cybersecurity protections to address the most common threats and TTPs used against this sector.

At-risk organizations should implement the following mitigations:

- **Prevent Interlock ransomware actors from obtaining initial access**:
  - **Implement domain name system (DNS) filtering** to block users from accessing malicious sites and applications.
  - **Implement web access firewalls** to mitigate and prevent unknown commands or process injection from malicious domains or websites.
  - **Train users** [CPG 2.I] to identify, avoid, and report **social engineering attempts**.
- **Implement a recovery plan** [CPG 5.A] to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, and secure location (e.g., hard drive, storage device, the cloud) [CPG 2.R].

- **Require all accounts** with password logins (e.g., service accounts, admin accounts, and domain admin accounts) to comply with NIST password standards.
  - Require employees to use long passwords [CPG 2.B] and consider not requiring recurring password changes, as these can weaken security.
- **Require MFA** [CPG 2.H] for all services to the extent possible, particularly for webmail, virtual private networks (VPNs), and accounts that access critical systems.
  - Implement ICAM policies across the organization as a precursor to MFA.
- **Keep all operating systems, software, and firmware up to date**; prioritize patching known exploited vulnerabilities in internet-facing systems [CPG 1.E].
  - Timely patching is efficient and cost effective for minimizing an organization's exposure to cybersecurity threats.
- **Implement robust EDR capabilities** on VMs, systems, and networks.
- **Segment networks** [CPG 2.F] to prevent the spread of ransomware.
  - Network segmentation can help prevent the spread of ransomware by controlling traffic flows between—and access to—various subnetworks and by restricting adversary lateral movement.
- **Identify, detect, and investigate abnormal activity and potential traversal of the indicated ransomware [CPG 3.A] with a networking monitoring tool [CPG 2.T].**
  - To aid in detecting ransomware, implement a tool that logs and reports all network traffic, including lateral movement activity on a network.
  - Implement EDR tools; these are useful for detecting lateral connections as they provide 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.
- **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 [CPG 2.E].
- **Disable unused ports**.
- **Consider adding an email banner to emails** received from outside of your organization [CPG 2.M].
- **Disable hyperlinks** in received emails.
- **Implement time-based access for accounts set at the admin level and higher;** for example, the just-in-time (JIT) access method provisions privileged access when needed and can support enforcement of the principle of least privilege (as well as the Zero Trust model):
  - This is a process where a network-wide policy is set in place to automatically disable admin accounts at the Active Directory level when the account is not in direct need.

- Individual users may submit their requests through an automated process that grants them access to a specified system for a set timeframe when they need to support the completion of a certain task.

- **Disable command line and scripting activities and permissions** [CPG 2.N].
  - Disabling software utilities that run from the command line makes it more difficult for threat actors to escalate privileges and move laterally.
- **Maintain offline backups of data** and regularly maintain backups and restorations [CPG 2.R]; this avoids severe service interruption and irretrievable data in the event of a compromise.
- **Ensure all backup data is encrypted, immutable** (i.e., cannot be altered or deleted), and covers the entire organization's data infrastructure [CPG 2.R].

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. The authoring agencies recommend testing your existing security controls inventory to assess how they perform against the ATT&CK techniques described in this advisory.

To get started:

1. Select an ATT&CK technique described in this advisory (see **Table 5** through **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: Whole-of-government, central location for ransomware resources and alerts.
- HHS Cyber Gateway: Contains key resources for HPH entities to bolster their cyber resilience.
- #StopRansomware Guide: Resource to mitigate a ransomware attack.
- Cyber Hygiene Services, Ransomware Readiness Assessment: CISA's no-cost cyber hygiene services.
- MS-ISAC Services: MS-ISAC's no-cost cybersecurity services for state, local, tribal, and territorial (SLTT) entities.

- Ransomware Defense-in-Depth: MS-ISAC guidance for SLTT entities to mitigate the threat of ransomware using a defense-in-depth strategy.
- Combatting Ransomware: MS-ISAC guidance on ransomware mitigation strategies aligned with recommendations from NIST and CSF.

Reporting

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

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

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

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, FBI and CISA urge you to promptly report ransomware incidents to FBI's Internet Crime Complain Center (IC3), a local FBI Field Office, or CISA via the agency's Incident Reporting System or its 24/7 Operations Center (contact@mail.cisa.dhs.gov) or by calling 1-844-Say-CISA (1-844-729-2472).

State, local, tribal, and territorial governments should report incidents to the MS-ISAC (SOC@cisecurity.org or 866-787-4722).

HPH Sector organizations should report incidents to FBI or CISA but also can reach out to HHS at HHScyber@hhs.gov for cyber incident support focused on mitigating adverse patient impacts.

Disclaimer

The information in this report is being provided "as is" for informational purposes only. The authoring agencies 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 favor by the authoring agencies.

Acknowledgements

Cisco Talos contributed to this advisory.

Version History

July 22, 2025: Initial version.

Notes

---

[1] Elio Biasiotto, et. al., "Unwrapping the Emerging Interlock Ransomware Attack," *Talos Intelligence* (blog), *Cisco Talos*, last modified November 7, 2024, https://blog.talosintelligence.com/emerging-interlock-ransomware/.
[2] Sekoia Threat Detection and Research team, "Interlock Ransomware Evolving Under the Radar," *Sekoia* (blog), *Sekoia*, last modified April 16, 2025, https://blog.sekoia.io/interlock-ransomware-evolving-under-the-radar/.
[3] Yashvi Shah and Vignesh Dhatchanamoorthy, "ClickFix Deception: A Social Engineering Tactic to Deploy Malware," *McAfee Labs* (blog), *McAfee*, last modified June 11, 2024, https://www.mcafee.com/blogs/other-blogs/mcafee-labs/clickfix-deception-a-social-engineering-tactic-to-deploy-malware/ and "HC3 Sector Alert: ClickFix Attacks," Health Sector Cybersecurity Coordination Center, Department of Health and Human Services, last modified October 29, 2024, https://www.hhs.gov/sites/default/files/clickfix-attacks-sector-alert-tlpclear.pdf.
[4] Shah, "ClickFix Deception: A Social Engineering Tactic to Deploy Malware."
[5] Sekoia Threat Detection and Research team, "Interlock Ransomware Evolving Under the Radar."
[6] Bill Toulas, "Interlock Ransomware Gang Deploys New NodeSnake RAT on Universities," *Bleeping Computer*, May 28, 2025, https://www.bleepingcomputer.com/news/security/interlock-ransomware-gang-deploys-new-nodesnake-rat-on-universities/.
[7] Biasiotto, "Unwrapping the Emerging Interlock Ransomware Attack."
[8] International law-enforcement and Microsoft took down the Lumma Stealer malware in May 2025 by seizing internet domains the actors used to distribute the malware to actors and taking down domains that hosted the malware's infrastructure. For more information, see Tara Seals, "Lumma Stealer Takedown Reveals Sprawling Operation," *Dark Reading,* May 21, 2025, https://www.darkreading.com/cybersecurity-operations/lumma-stealer-takedown-sprawling-operation, and Steven Masada, "Disrupting Lumma Stealer: Microsoft Leads Global Action Against Favored Cybercrime Tool," *Microsoft On the Issues* (blog), *Microsoft*, last modified May 21, 2025, https://blogs.microsoft.com/on-the-issues/2025/05/21/microsoft-leads-global-action-against-favored-cybercrime-tool/.
[9] Sekoia Threat Detection and Research team, "Interlock Ransomware Evolving Under the Radar."
[10] Biasiotto, "Unwrapping the Emerging Interlock Ransomware Attack."
[11] Biasiotto, "Unwrapping the Emerging Interlock Ransomware Attack."
[12] Biasiotto, "Unwrapping the Emerging Interlock Ransomware Attack."
[13] Biasiotto, "Unwrapping the Emerging Interlock Ransomware Attack."
[14] Lawrence Abrams, "Meet Interlock — The New Ransomware Targeting FreeBSD Servers," *Bleeping Computer*, November 3, 2024, https://www.bleepingcomputer.com/news/security/meet-interlock-the-new-ransomware-targeting-freebsd-servers/.

[15] Biasiotto, "Unwrapping the Emerging Interlock Ransomware Attack."
[16] Graham Cluley, "Interlock Ransomware: What You Need to Know," *Fortra* (blog), *Fortra*, last modified May 30, 2025, https://www.tripwire.com/state-of-security/interlock-ransomware-what-you-need-know.
[17] Sekoia Threat Detection and Research team, "Interlock Ransomware Evolving Under the Radar."