Threat Actor Profile: Interlock Ransomware

Aug 10, 2026

WHITE

View Alert

Executive Summary

Interlock Ransomware is an opportunistic, financially motivated threat actor that emerged in late 2024. Operating as a closed group rather than a Ransomware-as-a-Service (RaaS) model, Interlock employs a double-extortion strategy—exfiltrating sensitive data and encrypting systems, then threatening their target/victims to leak the stolen data on their Tor-based Worldwide Secrets Blog if a ransom is not paid.

They are particularly notable for utilizing atypical initial access vectors for ransomware groups, such as drive-by downloads and the ClickFix social engineering technique, which tricks users into manually executing malicious scripts.

Figure 1. Interlock Ransomware Branding

Additional Info

Status: Active

Motive: Financial Gain

Threat Actor Class: Cybercriminal

Threat Actor Type: Opportunistic / Human-Operated Ransomware Group

Health Sector Impact

The chart below illustrates the number of Interlock ransomware attacks or claims across various sectors from 2025 to 2026 (by far). Although the chart shows Education having a higher raw number of attacks, the health sector still ranks among the top 4 sectors targeted by the ransomware group. Additionally, the impact on the health sector is often considered disproportionately significant due to the sensitive nature of the data and its potential effects on patient care.

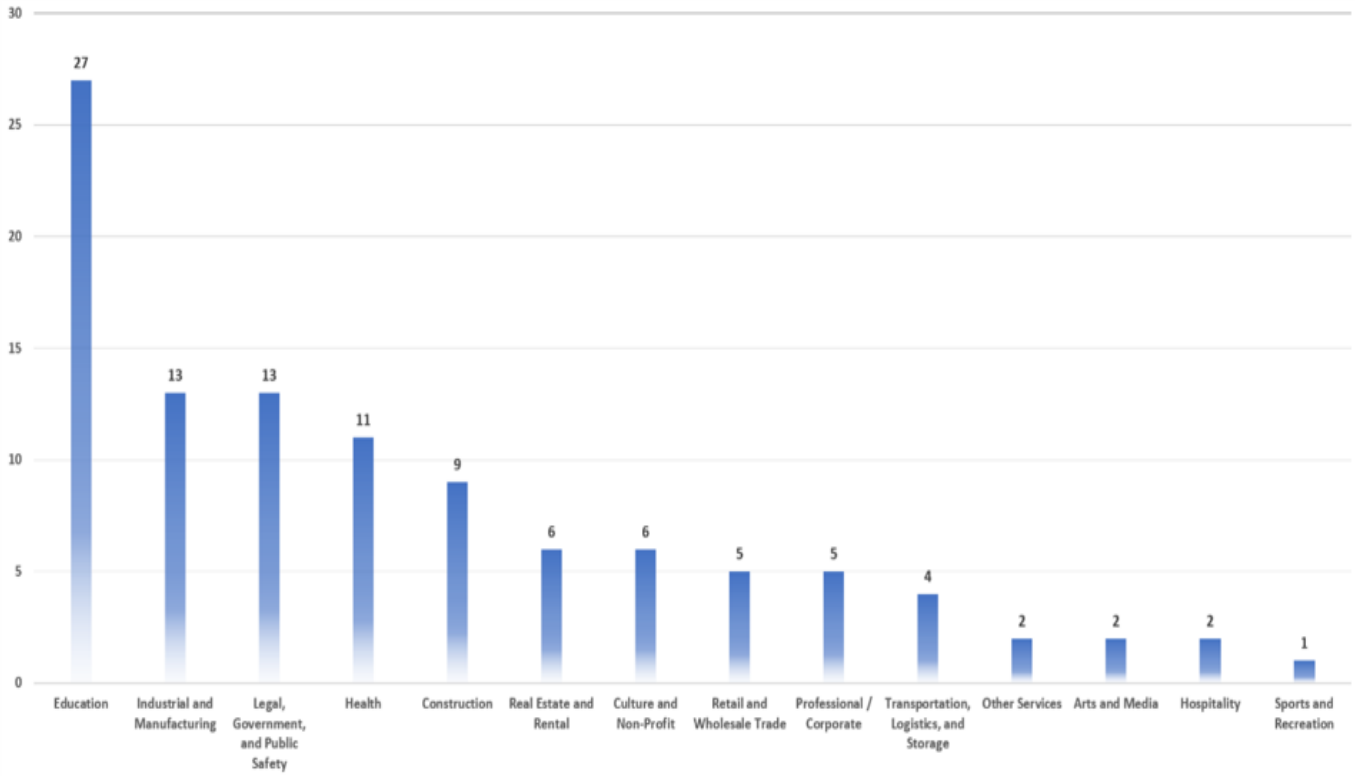

Figure 2. Interlock Claims: Health Sector Victims – 2025 to 2026 (By Far) (Source: Health-ISAC / eCrime)

Overview

The evolution of **Interlock ransomware** from its early origins as **Chaya_002** into a mature, double-extortion ransomware group involves significant growth in capabilities and operational maturity.

The group emerged as an unknown, financially motivated actor of medium sophistication in September 2024. A few months later, security researchers initially labeled their early intrusions as **Chaya_002**, which was later identified as a Traffic Distribution System (TDS) that would become a key element in Interlock's ransomware operations. During this phase, their primary capability was a basic PowerShell backdoor focused on credential theft, and they utilized opportunistic targeting on a limited scale. They used a TDS to target local news, small businesses, and community forum websites to serve malicious JavaScript. This script triggered fake update or application error prompts for software like Chrome and Teams.

The name **Interlock** came to light in October 2024, raising suspicions that an organized group was running the ransomware operation.

Meanwhile, in February 2025, the group expanded its social engineering tactics to impersonate remote connectivity software, such as FortiClient VPN and Cisco AnyConnect. The group is considered an active, maturing threat group, not just a one-off variant, demonstrating iterative improvements to their tooling and targeting since their emergence. In one year, they transformed from an unknown entity developing an infostealing Remote Access Trojan (RAT) into an emergency-level threat.

Feds Warn Health, Other Sectors of Interlock Threats

In July 2025, a coalition of U.S. agencies, including the FBI, CISA (Cybersecurity and Infrastructure Security Agency), HHS (Department of Health and Human Services), and MS-ISAC (Multi-State Information Sharing and Analysis Center), released a joint cybersecurity advisory, which aimed to warn organizations about the escalating threat and provided actionable intelligence.

In the same month, Health-ISAC released an advisory after observing that, of 51 Interlock attacks across all sectors since the group appeared in the last quarter of 2024, 7 have targeted the health sector.

Victimology

Interlock is an opportunistic threat actor, meaning they target organizations based on vulnerabilities and access rather than focusing on specific sectors. However, their successful attacks have shown a clear pattern of impacting critical infrastructure.

Prioritized Sectors: While opportunistic, they have a notable track record of impacting Health, Education, Manufacturing, Industrial, Legal, Government, and Construction.

Primary Targets: They target a wide range of organizations, from local governments to large healthcare providers and critical infrastructure entities.

Geographic Focus: Primarily North America (especially the United States) and Europe.

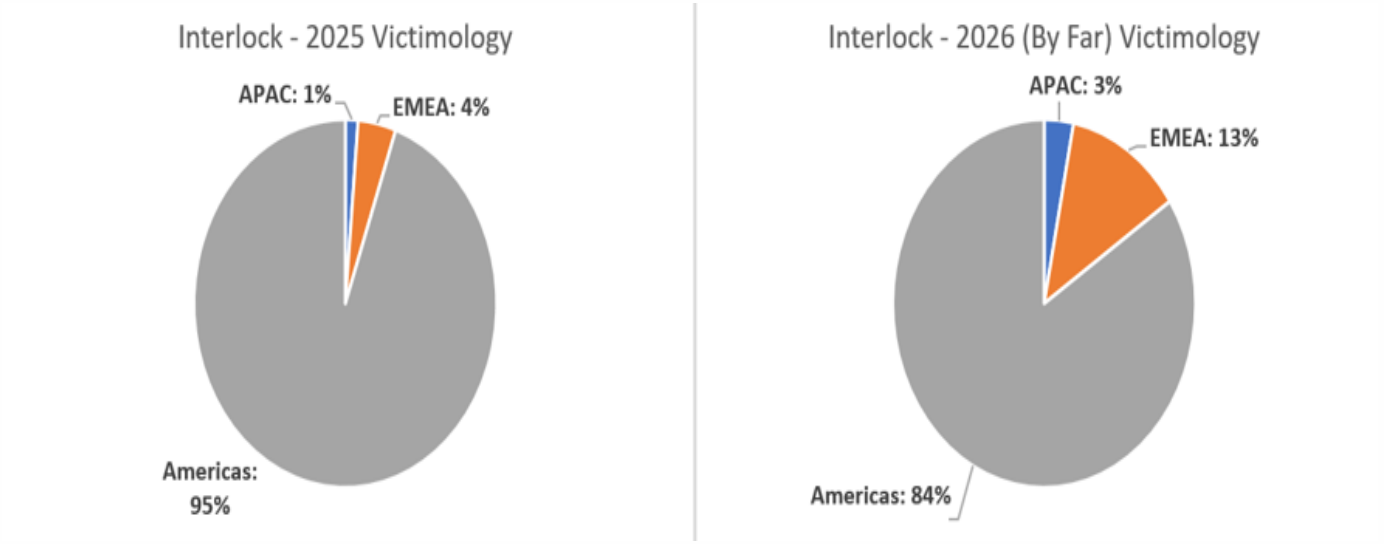

Figure 3. Interlock: 2025 to 2026 (By Far) Victims' Data (Source: Health-ISAC / eCrime)

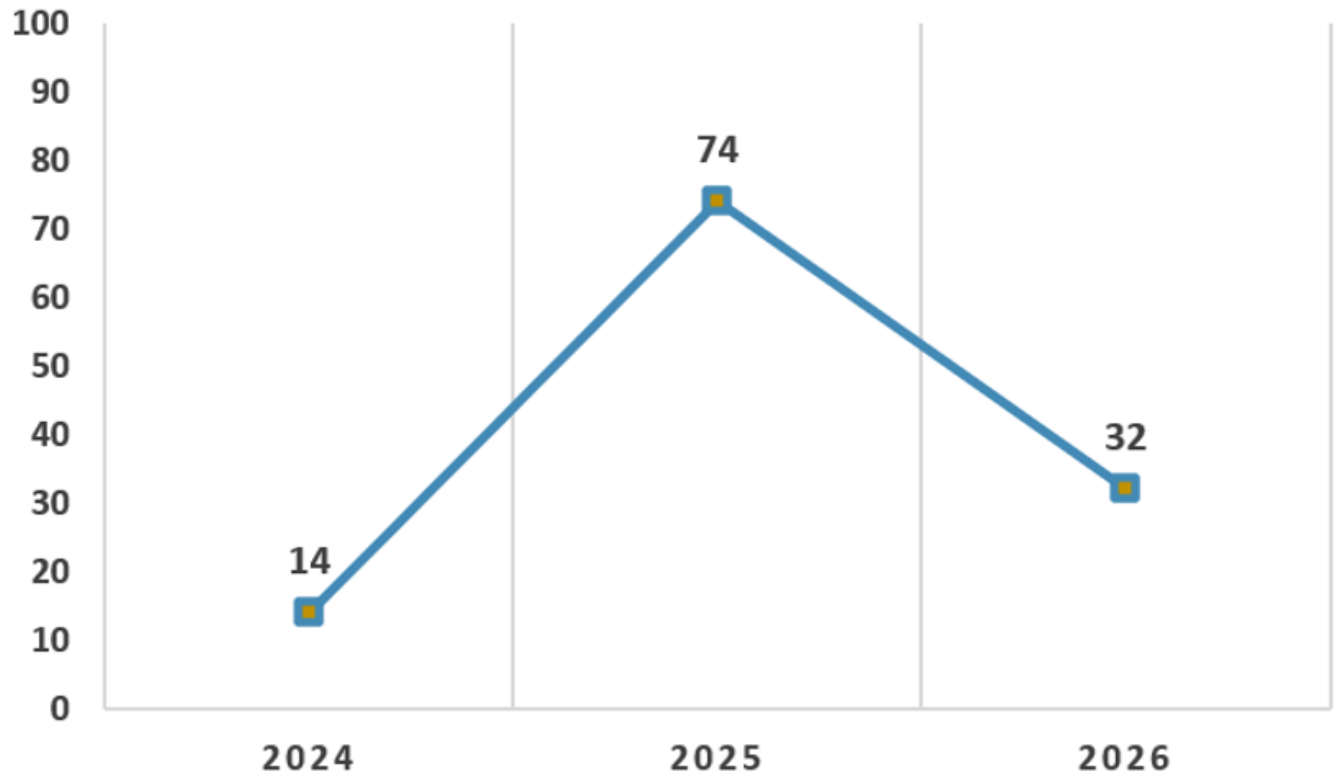

Figure 4. Interlock: Victimology Trend – 2024 to 2026 (By Far) (Source: Health-ISAC / eCrime)

Technical Analysis

Interlock's attack chain relies heavily on social engineering and deceptive delivery methods to establish an initial foothold, then employs stealthy tactics for network discovery and lateral movement.

- **Initial Access**
  - **Drive-by Downloads:** Compromising legitimate websites (often news or retail sites) to host malicious payloads disguised as software updates (i.e., Google Chrome, Microsoft Edge, FortiClient, Cisco AnyConnect).
  - **ClickFix Technique:** Tricking users into opening the Windows Run dialog and executing a malicious, Base64-encoded PowerShell script disguised as a CAPTCHA verification ("prove you are human") or a system alert.

- **Execution and Persistence**
    - **Malicious Payloads:** The fake executables often function as Remote Access Trojans (RATs) that execute embedded PowerShell scripts.
    - **Startup Folder:** Establishing persistence by dropping shortcut files (.lnk) or executable files into the Windows Startup folder.
    - **Registry Modification:** Modifying registry run keys (e.g., disguised as "Chrome Updater") to ensure execution upon user login.

- **Discovery and Credential Access**
    - **System Discovery:** Utilizing built-in commands like systeminfo, Get-PSDrive, tasklist /svc, and Get-Service to enumerate system details, logical drives, and active services (to identify security tools).
    - **Infostealers & Keyloggers:** Deploying secondary payloads, such as credential stealers (e.g., Lumma, Berserk) and keyloggers (often loaded via rundll32.exe), to harvest login credentials from web browsers and capture user input.
    - **Privilege Escalation:** Performing Kerberoasting attacks to steal Kerberos service tickets for high-privilege accounts.

- **Lateral Movement and Command & Control**
    - **Living off the Land:** Reusing harvested credentials to move stealthily across the network via Remote Desktop Protocol (RDP).
    - **Remote Access Tools:** Using legitimate tools like AnyDesk and PuTTY for remote connectivity and lateral movement.
    - **C2 Infrastructure:** Utilizing frameworks like Cobalt Strike and SystemBC, alongside custom RATs (Interlock RAT, NodeSnake RAT), communicating with attacker-controlled domains (e.g., via Cloudflare).

- **Exfiltration and Impact**
    - **Data Exfiltration:** Stealing sensitive data before encryption to leverage for extortion.
    - **Targeted Encryption:** Deploying encryptors specifically designed for Windows and Linux operating systems, with a noted focus on encrypting Virtual Machines (VMs) rather than physical hosts or workstations.

Common Arsenal

Interlock utilizes a mix of custom malware and legitimate dual-use tools:

- **Backdoors and RATs:** Interlock RAT, NodeSnake backdoor (written in multiple languages, including JavaScript, Java, and native C++), and PowerShell backdoors.
- **Command and Control (C2):** Cobalt Strike, SystemBC, and Cloudflare Tunnels.
- **Credential Theft:** Custom NTLM credential harvester DLLs.
- **Lateral Movement & Remote Access:** Legitimate tools such as AnyDesk, PuTTY, and ConnectWise ScreenConnect (delivered via malicious MSI installers).
- **Payload Delivery:** Custom crypter frameworks are used to package the ransomware payloads

Observables

Data Leak Channels:

- **Primary Data Leak Site (a.k.a. Worldwide Secrets Blog)** - hxxp://ebhmkoohccl45qesdbvrjqtyro2hmhkmh6vkyfyjjzfllm3ix72aqaid[.]onion
- **Support / Negotiation Portal** - hxxp://ebhmkoohccl45qesdbvrjqtyro2hmhkmh6vkyfyjjzfllm3ix72aqaid[.]onion/support/step[.]php

INTERLOCK

The Corporate Secrets They Never Wanted You to Se

News

Help

DATA LEAKS

94%

9.7 days

$4.45

About Us

We are INTERLOCK, a relentless collective that exposes the reck
protect their most critical assets: customer data and intellectual
vulnerabilities they leave wide open, delivering a harsh but nece
they can cut corners on security.

In 2024, the numbers speak for themselves: ransomware attacks
second quarter, with more than half of the world's top breaches
negligence. Corporations continue to mishandle sensitive inform
rooted in avoidable security flaws. This isn't just incompetence
show them the consequences of that carelessness.

We don't just want payment; we want accountability. Our action
behind weak defenses and half-measures: your data is only as s
protecting it. If you don't take data security seriously, we will on
price.
In this digital age, there's no excuse for complacency. When co
make them pay not just with ransoms, but with lessons they wo
standards they fail to uphold.

Figure 5. Interlock: Data Leak Site - Overview, About Us, and Contact Information (Source: eCrime)

Encrypted File Extension:

- .interlock
- .interlocked
- .1nt3rlock

Ransom Note:

- !__README__!.txt
- !!_DO_THIS_FIRST_!!.txt
- !!!OPEN_ME!!!.txt
- OPEN_BEFORE_ANYTHING.txt

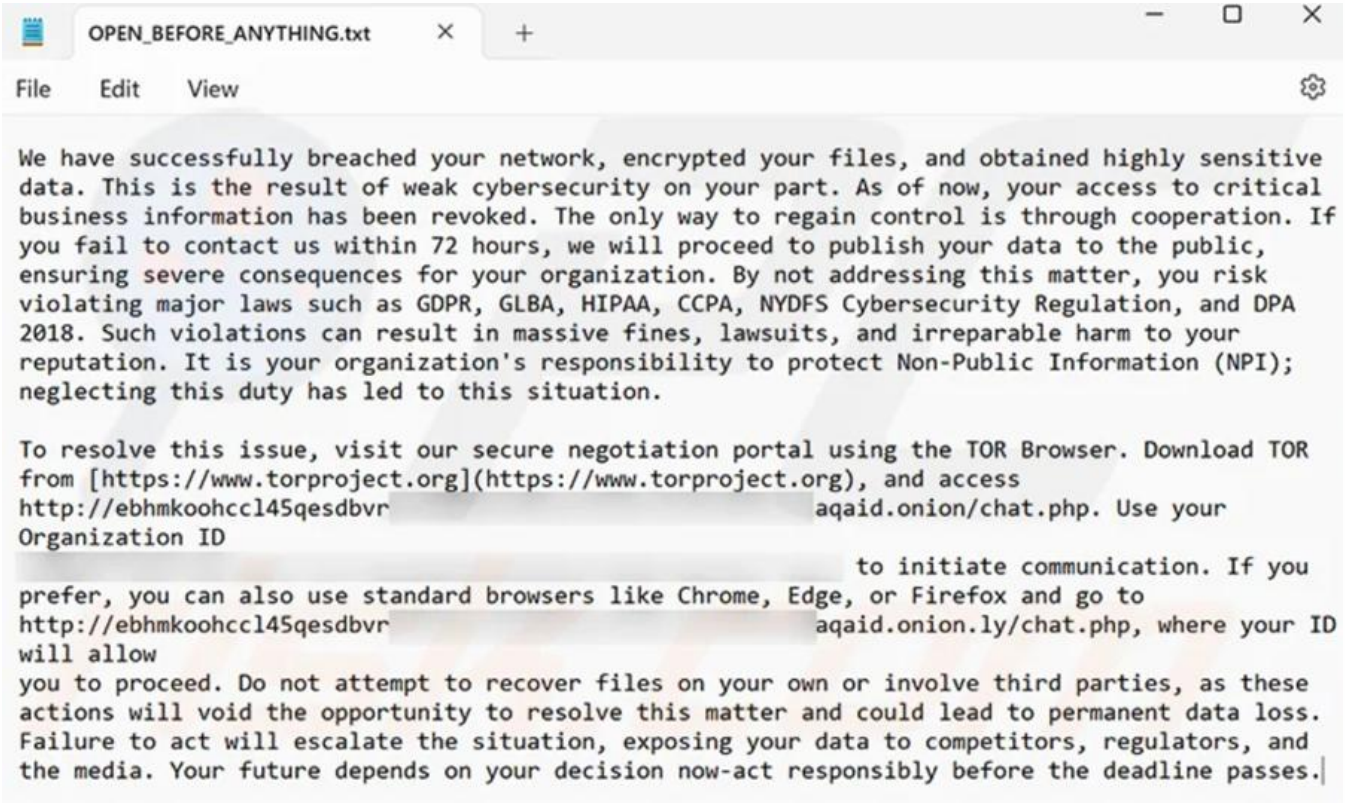

Figure 6. Interlock: Ransom Note Sample #1 (Source: PCRisk)

!_README_!.txt - Notepad

File Edit Format View Help

```
    INTERLOCK - CRITICAL SECURITY ALERT

To Whom It May Concern,
Your organization has experienced a serious security breach. Immediate action is required to mitigate further
risks. Here are the details:

    THE CURRENT SITUATION
- Your systems have been infiltrated by unauthorized entities.
- Key files have been encrypted and are now inaccessible to you.
- Sensitive data has been extracted and is in our possession.

    WHAT YOU NEED TO DO NOW
1. Contact us via our secure, anonymous platform listed below.
2. Follow all instructions to recover your encrypted data.

Access Point: http://ebhmkoo                                        .onion/support/step.php
Use your unique Company ID:

    DO NOT ATTEMPT:
- File alterations: Renaming, moving, or tampering with files will lead to irreversible damage.
- Third-party software: Using any recovery tools will corrupt the encryption keys, making recovery impossible.
- Reboots or shutdowns: System restarts may cause key damage. Proceed at your own risk.

    HOW DID THIS HAPPEN?
We identified vulnerabilities within your network and gained access to critical parts of your infrastructure. The
following data categories have been extracted and are now at risk:
- Personal records and client information
- Financial statements, contracts, and legal documents
- Internal communications
- Backups and business-critical files
We hold full copies of these files, and their future is in your hands.

    YOUR OPTIONS
#1. Ignore This Warning:
- In 96 hours, we will release or sell your sensitive data.
- Media outlets, regulators, and competitors will be notified.
- Your decryption keys will be destroyed, making recovery impossible.
- The financial and reputational damage could be catastrophic.

#2. Cooperate With Us:
- You will receive the only working decryption tool for your files.
- We will guarantee the secure deletion of all exfiltrated data.

    HOW DID THIS HAPPEN?
We identified vulnerabilities within your network and gained access to critical parts of your infrastructure. The
following data categories have been extracted and are now at risk:
- Personal records and client information
- Financial statements, contracts, and legal documents
- Internal communications
- Backups and business-critical files
We hold full copies of these files, and their future is in your hands.

    YOUR OPTIONS
#1. Ignore This Warning:
- In 96 hours, we will release or sell your sensitive data.
- Media outlets, regulators, and competitors will be notified.
- Your decryption keys will be destroyed, making recovery impossible.
- The financial and reputational damage could be catastrophic.

#2. Cooperate With Us:
- You will receive the only working decryption tool for your files.
- We will guarantee the secure deletion of all exfiltrated data.
- All traces of this incident will be erased from public and private records.
- A full security audit will be provided to prevent future breaches.

    FINAL REMINDER
Failure to act promptly will result in:
- Permanent loss of all encrypted data.
- Leakage of confidential information to the public, competitors, and authorities.
- Irreversible financial harm to your organization.

    CONTACT US SECURELY
1. Install the TOR browser via https://torproject.org
2. Visit our anonymous contact form at
http://ebhmkoo                                        .onion/support/step.php
3. Use your unique Company ID:
4. Review a sample of your compromised data for verification.
5. Use a VPN if TOR is restricted in your area.
```

Figure 7. Interlock: Ransom Note Sample #2 (Source: Fortinet)

Figure 8. Interlock: Sample Ransom Note and Encrypted Files (Source: Fortinet)

Indicators of Compromise

Category	Indicator	Context / Threat Detail
SHA-256	fba4883bf4f73aa48a957d894051d78e0085ecc3170b1ff50e61ccec6aeee2cd	PowerShell script, often used by Interlock during initial access or execution to download next-stage payloads or establish persistence.
SHA-256	4b036cc9930bb42454172f888b8fde1087797fc0c9d31ab546748bd2496bd3e5	Legitimate network

		scanning tool utilized by threat actors for network reconnaissance and discovery.
SHA-256	18a507bf1c533aad8e6f2a2b023fbbcac02a477e8f05b095ee29b52b90d47421	Malicious executable payload.
SHA-256	1a70f4eef11fbecb721b9bab1c9ff43a8c4cd7b2cafef08c033c77070c6fe069	A legitimate remote desktop application was abused by Interlock actors to establish remote connectivity and enable lateral movement across the network.
SHA-256	a4069aa29628e64ea63b4fb3e29d16dcc368c5add304358a47097eedafbbb565	Malicious dynamic link library (DLL) payload.
SHA-256	d535bdc9970a3c6f7ebf0b229c695082a73eaeaf35a63cd8a0e7e6e3ceb22795	Executable likely used to maintain persistence

		upon user login or system reboot.
SHA-256	fafcd5404a992850ffcffee46221f9b2ff716006aecb637b80e5cd5aa112d79c	Custom credential stealer binary downloaded via PowerShell to collect login information and associated URLs for victims' online accounts.
SHA-256	c20baba26ebb596de14b403b9f78ddc3c13ce9870eea332476ac2c1dd582aa07	Custom credential stealer binary downloaded via PowerShell to collect login information and associated URLs for victims' online accounts.

SHA-256	1845a910dcde8c6e45ad2e0c48439e5ab8bbbeb731f2af11a1b7bbab3bfe0127	Associated with SystemBC, a SOCKS5 proxy utility used by Interlock to establish Command and Control (C2) and obfuscate malicious network traffic.
SHA-256	44887125aa2df864226421ee694d51e5535d8c6f70e327e9bcb366e43fd892c1	Malicious files masquerading as a legitimate Windows process. Interlock frequently disguises its final ransomware encryptor payload as a file named conhost.exe.
SHA-256	a70af759e38219ca3a7f7645f3e103b13c9fb1db6d13b68f3d468b7987540ddf	Malicious files masquerading as a legitimate

		Windows process. Interlock frequently disguises its final ransomware encryptor payload as a file named conhost.exe.
SHA-256	96babe53d6569ee3b4d8fc09c2a6557e49ebc2ed1b965abda0f7f51378557eb1	Malicious files masquerading as a legitimate Windows process. Interlock frequently disguises its final ransomware encryptor payload as a file named conhost.exe.
SHA-256	d0c1662ce239e4d288048c0e3324ec52962f6ddda77da0cb7af9c1d9c2f1e2eb	Malicious payload or injected process masquerading as

		Internet Explorer.
SHA-256	a4f0b68052e8da9a80b70407a92400c6a5def19717e0240ac608612476e1137e	A custom keylogger dynamic link library (DLL), deployed to log users' keystrokes into a text file, facilitating credential access.
SHA-256	68a49d5a097e3850f3bb572baf2b75a8e158dadb70baddc205c2628a9b660e7a	Interlock's ransom note. Contains a unique victim identifier and instructions to contact the group via a Tor .onion URL for negotiation.
SHA-256	88f26f3721076f74996f8518469d98bf9be0eaee5b9eccc72867ebfc25ea4e83	Process Hacker archive. A legitimate administrative utility frequently

		abused by ransomware operators to terminate EDR/antivirus processes prior to encryption.
SHA-256	078163d5c16f64caa5a14784323fd51451b8c831c73396b967b4e35e6879937b	Microsoft Sysinternals tool, abused for execution and lateral movement across the network.
SHA-256	7a43789216ce242524e321d2222fa50820a532e29175e0a2e685459a19e09069	Legitimate SSH and Telnet client utilized by actors alongside compromised credentials to assist with lateral movement and remote connectivity.
SHA-256	97931d2e2e449ac3691eb526f6f60e2f828de89074bdac07bd7dbdfd51af9fa0	Legitimate SSH and

		Telnet client utilized by actors alongside compromised credentials to assist with lateral movement and remote connectivity.
SHA-256	ff7ad2376ae01e4b3f1e1d7ae630f87b8262b5c11bc5d953e1ac34ffe81401b5	Legitimate SSH and Telnet client utilized by actors alongside compromised credentials to assist with lateral movement and remote connectivity.
SHA-256	64a0ab00d90682b1807c5d7da1a4ae67cde4c5757fc7d995d8f126f0ec8ae983	Malicious executable payload.
SHA-256	2814b33ce81d2d2e528bb1ed4290d665569f112c9be54e65abca50c41314d462	Component of ConnectWise

		ScreenConnect. A legitimate remote management tool abused by attackers for persistent remote access and lateral movement.
SHA-256	f51b3d054995803d04a754ea3ff7d31823fab654393e8054b227092580be43db	Malicious payloads masquerading as legitimate Sophos security software updates. Utilized in drive-by downloads to trick users into executing the initial payload.
SHA-256	dfb5ba578b81f05593c047f2c822eeb03785aecffb1504dcb7f8357e898b5024	Malicious payloads masquerading as legitimate Sophos security

		software updates. Utilized in drive-by downloads to trick users into executing the initial payload.
SHA-256	94bf0aba5f9f32b9c35e8dfc70afd8a35621ed6ef084453dc1b10719ae72f8e2	Malicious executable payload.
SHA-256	28c3c50d115d2b8ffc7ba0a8de9572fbe307907aaae3a486aabd8c0266e9426f	Executable frequently utilized in startup folders or scheduled tasks to ensure malware persistence.
SHA-256	70bb799557da5ac4f18093decc60c96c13359e30f246683815a512d7f9824c8f	Executable frequently utilized in startup folders or scheduled tasks to ensure malware persistence.

SHA-256	73a9a1e38ff40908bcc15df2954246883dadfb991f3c74f6c514b4cffdabde66	Legitimate Azure Storage Explorer tool leveraged to navigate victims' Microsoft Azure Storage environments prior to data exfiltration.
SHA-256	1d04e33009bcd017898b9e1387e40b5c04279c02ebc110f12e4a724ccdb9e4fb	Legitimate Microsoft Sysinternals driver; actors may abuse or tamper with logging drivers to evade detection.
SHA-256	7b9e12e3561285181634ab32015eb653ab5e5cfa157dd16cdd327104b258c332	Malicious payload, likely delivered under the guise of a software update (such as a fake Chrome or Edge

		update) during initial access.
SHA-256	70ee22d394e107fbb807d86d187c216ad66b8537edc67931559a8aef18f6b5b3	A Windows shortcut file; typically dropped into the Windows Startup folder to ensure a malicious payload (like a Remote Access Trojan) executes every time the victim logs in.
SHA-256	8eb7e3e8f3ee31d382359a8a232c984bdaa130584cad11683749026e5df1fdc3	A legitimate file transfer application, utilized to exfiltrate stolen data to an attacker-controlled infrastructure.
SHA-256	e4d6fe517cdf3790dfa51c62457f5acd8cb961ab1f083de37b15fd2fddeb9b8f	A tool used to route or

		obfuscate attacker traffic and maintain C2 connectivity.
SHA-256	e86bb8361c436be94b0901e5b39db9b6666134f23cce1e5581421c2981405cb1	FreeBSD Version - Ransomware payloads responsible for encrypting targeted systems (primarily Virtual Machines across Windows and Linux) and appending the .interlock extension.
SHA-256	c733d85f445004c9d6918f7c09a1e0d38a8f3b37ad825cd544b865dba36a1ba6	FreeBSD Version - Ransomware payloads responsible for encrypting targeted systems (primarily Virtual

		Machines across Windows and Linux) and appending the .interlock extension.
URL	f00a7652ad70ddb6871eeef5ece097e2cf68f3d9a6b7acfbffd33f82558ab50e	FreeBSD Version - Ransomware payloads responsible for encrypting targeted systems (primarily Virtual Machines across Windows and Linux) and appending the .interlock extension.
URL	a26f0a2da63a838161a7d335aaa5e4b314a232acc15dcabdb6f6dbec63cda642	Windows Version - Ransomware payloads responsible for encrypting targeted systems

		(primarily Virtual Machines across Windows and Linux) and appending the .interlock extension.
URL	e9ff4d40aeec2ff9d2886c7e7aea7634d8997a14ca3740645fd3101808cc187b	Backdoor malware allegedly found on the Interock ransomware victim's machine.
URL	7d750012afc9f680615fe3a23505f13ab738beef50cd92ebc864755af0775193	Backdoor malware allegedly found on the Interock ransomware victim's machine.
URL	6933141fbdcdcaa9e92d6586dd549ac1cb21583ba9a27aa23cf133ecfdf36ddf	Backdoor malware allegedly found on the Interock ransomware victim's machine.

IP Address	216.245.184[.]181	AS399629 - BitLaunch - Interlock's Backup IP Address used to host PowerShell backdoors for C2
IP Address	212.237.217[.]182	AS57043 - Hostkey B.v. - Interlock's Backup IP Address used to host PowerShell backdoors for C2
IP Address	168.119.96[.]41	AS24940 - Hetzner Online GmbH - Interlock's Backup IP Address used to host PowerShell backdoors for C2
Domain	Bronxy[.]cc	Interlock's domain for initial access

Domain	Basiclock[.]cc	Interlock's domain for initial access
Domain	fake-domain-1892572220[.]com	Interlock's domain for initial access
Email Address	interlock@2mail[.]co	Email address used by the Interlock for victim communication and extortion
Hex Bytes	92 01 88 fe	RC4-Encrypted Prefix used by Interlock during WebSocket Handshake
Hex Bytes	488b041f483345f04889041e	Hardcoded binary sequence used in the crypter decryption loop of the InterLock's toolset
URL	hxxp://ebhmkoohccl45qesdbvrjqtyro2hmhkmh6vkyfyjjzfllm3ix72aqaid[.]onion	Interlock's Primary Data Leak

		Site (a.k.a. Worldwide Secrets Blog)
URL	hxxp://ebhmkoohccl45qesdbvrjqtyro2hmhkmh6vkyfyjjzfllm3ix72aqaid[.]onion/support/step[.]php	Interlock's Support / Negotiation Portal
File Extension	.interlock	Interlock Encrypted File Extension
File Extension	.interlocked	Interlock Encrypted File Extension
File Extension	.1nt3rlock	Interlock Encrypted File Extension
Filename	!__README__!.txt	Interlock Ransom Note
Filename	!!_DO_THIS_FIRST_!!.txt	Interlock Ransom Note
Filename	!!!OPEN_ME!!!.txt	Interlock Ransom Note
Filename	OPEN_BEFORE_ANYTHING.txt	Interlock Ransom Note

Tactics, Techniques, and Procedures (TTPs)

Below is the consolidated table of the Tactics, Techniques, and Procedures (TTPs) mapped to the MITRE ATT&CK framework for Interlock ransomware operations.

Tactics	Technique ID	Technique Name	Procedures / Observables
Initial Access	**T1189**	Drive-by Compromise	Compromising legitimate websites (like news or community forums) to host malicious payloads disguised as fake software updates (e.g., Google Chrome, FortiClient, Cisco AnyConnect, Sophos).
Initial Access	**T1204.004**	User Execution: Malicious Copy and Paste	Utilizing the ClickFix social engineering technique. Victims are presented with a fake CAPTCHA or alert, tricking them into copying and pasting a malicious, Base64-encoded PowerShell script into the Windows Run dialog.
Execution	**T1059.001**	Command and Scripting Interpreter: PowerShell	Heavily relying on PowerShell scripts to download first-stage backdoors (like Interlock RAT), perform system reconnaissance, and establish persistence mechanisms.
Execution	**T1218.011**	System Binary Proxy Execution: Rundll32	Using rundll32.exe to indirectly execute malicious dynamic link library (DLL) payloads (such as klg.dll and autoservice.dll) to bypass security controls.
Persistence	**T1547.001**	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Dropping malicious shortcut files (e.g., webujgd.lnk) into the Windows Startup folder or modifying registry run keys (often disguised as Chrome Updater). Also observed creating scheduled tasks named TaskSystem.

Privilege Escalation	**T1558.003**	Steal or Forge Kerberos Tickets: Kerberoasting	Performing Kerberoasting attacks to obtain Kerberos service tickets associated with high-privilege domain accounts, allowing actors to escalate to Domain Administrator.
Defense Evasion	**T1036.005**	Masquerading: Match Legitimate Name or Location	Disguising malicious executables and DLLs as legitimate system processes. For example, naming their final encryptor or keylogger tools conhost.exe or conhost.dll, and saving keylog data to conhost.txt.
Defense Evasion	**T1070.004**	Indicator Removal: File Deletion	Utilizing functions like remove() within DLLs or native Linux commands to delete the ransomware binary immediately following encryption to reduce forensic evidence.
Credential Access	**T1555.003**	Credentials from Web Browsers	Deploying commercial information stealers (such as Lumma Stealer and Berserk Stealer) and custom binaries (cht.exe) to harvest login credentials and session tokens from web browsers.
Credential Access	**T1056.001**	Input Capture: Keylogging	Deploying custom keyloggers (e.g., klg.dll) to record keystrokes and capture sensitive user input, saving the output to hidden text files.
Discovery	**T1082**	System Information Discovery	Utilizing native commands like systeminfo and PowerShell cmdlets like Get-PSDrive to collect comprehensive details about the operating system, hardware, and attached logical drives.
Discovery	**T1007**	System Service Discovery	Running commands such as tasklist /svc and Get-Service to enumerate active services on a host, specifically searching for running EDR, antivirus, or monitoring tools.
Discovery	**T1016**	System Network Configuration Discovery	Utilizing the arp -a command to inspect the system's ARP cache, aiding the attackers in mapping internal network IP addresses for lateral movement.

Lateral Movement	**T1021.001**	Remote Services: Remote Desktop Protocol (RDP)	Utilizing previously harvested valid credentials to authenticate over RDP, allowing for stealthy lateral movement across the victim's internal network.
Lateral Movement	**T1219**	Remote Access Software	Leveraging legitimate dual-use remote access tools like AnyDesk, PuTTY, and ConnectWise ScreenConnect to maintain persistent remote connectivity to infected hosts.
Command and Control	**T1105**	Ingress Tool Transfer	Using initial access PowerShell scripts to download subsequent C2 and post-exploitation frameworks, including Cobalt Strike, SystemBC, and custom RATs (Interlock RAT, NodeSnake).
Command and Control	**T1090**	Proxy	Utilizing SystemBC (a SOCKS5 proxy utility via cleanup.dll or difxepi.dll) and dynamically generated Cloudflare Tunnels (using trycloudflare[.]com subdomains) to obfuscate and route malicious C2 traffic.
Exfiltration	**T1530**	Data from Cloud Storage	Utilizing tools such as Azure Storage Explorer (StorageExplorer.exe) to browse and access victims' cloud storage environments to identify valuable data prior to exfiltration.
Exfiltration	**T1048**	Exfiltration Over Alternative Protocol	Using legitimate file transfer applications like WinSCP (WinSCP-6.3.5-Setup.exe) to siphon stolen data out of the network to an attacker-controlled infrastructure.
Impact	**T1486**	Data Encrypted for Impact	Deploying custom encryptors (often targeting Virtual Machines running Windows, Linux, and FreeBSD). Files are encrypted using AES+RSA, appended with the .interlock or .1nt3rlock extension, and ransom notes (e.g., !!!OPEN_ME!!!.txt or !__README__!.txt) are distributed.

Recommendations

- **User Training & Awareness**
    - **Educate on ClickFix:** Train employees to recognize and report the "ClickFix" technique. Ensure they know never to copy and paste code into the Windows Run dialog or PowerShell console, especially when prompted by supposed CAPTCHA verifications or website errors.
    - **Prevent Drive-By Downloads:** Warn staff about the dangers of downloading unexpected software or browser updates (e.g., Chrome, Edge, FortiClient) from pop-ups or unverified third-party websites.

- **Access & Identity Management**
    - **Enforce Phishing-Resistant MFA:** Require Multi-Factor Authentication for all remote access, including VPNs, Webmail, and Remote Desktop Protocol (RDP), to mitigate the impact of stolen credentials.
    - **Audit Remote Access Tools:** Audit your environment for legitimate remote management software (like **AnyDesk, ConnectWise ScreenConnect, and PuTTY**). Uninstall any unauthorized tools, as Interlock heavily abuses these for lateral movement.
    - **Mitigate Kerberoasting:** Implement the principle of least privilege and use strong, complex passwords for service accounts to make Kerberoasting attacks significantly more difficult to crack offline.

- **Endpoint & Network Security**
    - **Restrict PowerShell:** Configure PowerShell execution policies, enable Constrained Language Mode (CLM), and turn on Script Block Logging (Event ID 4104) to monitor and restrict the execution of Interlock's initial access scripts.
    - **Harden EDR Solutions:** Ensure your Endpoint Detection and Response (EDR) tools are properly configured with anti-tampering features enabled to prevent attackers from disabling them using tools like Process Hacker or vulnerable drivers.
    - **Implement DNS Filtering:** Use DNS filtering and web proxies to block access to known malicious domains and prevent the initial drive-by download payloads from reaching your network.

    - **Monitor Tunneling Services:** Inspect network traffic for unexpected WebSocket connections and block or strictly alert on unauthorized traffic to cloud tunneling services, particularly **Cloudflare Tunnels** (trycloudflare[.]com), which Interlock uses for Command and Control (C2).

- **Infrastructure & Data Protection**
    - **Secure Virtual Environments:** Interlock specifically targets Virtual Machines (VMs). Harden your ESXi and Hyper-V environments by keeping hypervisors fully patched, restricting access to management interfaces, and using dedicated administrative workstations.
    - **Maintain Immutable Backups:** Implement a robust backup strategy that includes offline, encrypted, and immutable backups. This ensures you can restore critical operations without paying a ransom, directly countering their double-extortion tactics.

Detection Opportunities – YARA Rules

```
rule APT_Interlock_RAT_PowerShell_Backdoor {
  meta:
    description = "Detects the Interlock RAT PowerShell backdoor used in initial access and C2"
    author = "Sekoia.io"
    date = "2025-04-16"
    malware_family = "Interlock RAT / NodeSnake"
    reference = "Sekoia.io Threat Intelligence"

  strings:
    // Known C2 path indicator used by Interlock
    $c2_path = "path: '/init1234'" ascii wide nocase

    // System reconnaissance commands frequently used by the group
    $recon_1 = "Get-PSDrive -PSProvider FileSystem" ascii wide nocase
    $recon_2 = "tasklist /svc" ascii wide nocase
    $recon_3 = "systeminfo" ascii wide nocase

    // Base64 execution patterns associated with ClickFix
    $b64_exec_1 = "[Convert]::FromBase64String(" ascii wide nocase
    $b64_exec_2 = "powershell.exe -e" ascii wide nocase
    $b64_exec_3 = "powershell -enc" ascii wide nocase
```

```
  condition:
    ($c2_path) or
    (all of ($recon_*) and any of ($b64_exec_*))
}

rule Mal_Interlock_Crypter_Decryption_Loop {
  meta:
    description = "Detects the hex byte pattern of the custom crypter decryption loop used by
Interlock ransomware"
    author = "Jay Villanueva"
    date = "2026-08-05"
    malware_family = "Interlock Ransomware"

  strings:
    // Hex byte pattern identified in Interlock crypter decryption loops
    $hex_pattern = { 48 8b 04 1f 48 33 45 f0 48 89 04 1e }

  condition:
    $hex_pattern
}

rule Mal_Interlock_Ransomware_Artifacts {
  meta:
    description = "Detects strings and artifacts associated with the final Interlock ransomware
encryptor"
    author = "Jay Villanueva"
    date = "2026-08-05"
    malware_family = "Interlock Ransomware"

  strings:
    // Ransom note file names
    $note_1 = "!__README__!.txt" ascii wide
    $note_2 = "!!_DO_THIS_FIRST_!!.txt" ascii wide
    $note_3 = "!!!OPEN_ME!!!.txt" ascii wide

    // Encrypted file extensions
    $ext_1 = ".interlock" ascii wide
    $ext_2 = ".1nt3rlock" ascii wide
    $ext_3 = ".interlocked" ascii wide
```

```
    // Known Onion/Tor URL patterns used by Interlock
    $onion_site = "ebhmkoohccl45qesdbvrjqtyro2hmhkmh6vkyfyjjzfllm3ix72aqaid[.]onion" ascii
wide

    // EDR Evasion / Log clearing artifacts
    $evasion_1 = "wevtapi.dll" ascii wide nocase
    $evasion_2 = "processhacker" ascii wide nocase

  condition:
    uint16(0) == 0x5A4D and // MZ header (Windows executable)
    (
      any of ($note_*) and
      any of ($ext_*) and
      $onion_site
    )
}
```

Note: For the URLs (specifically the TOR-based URLs / Onion Sites), please make sure to fang them before using/deploying the YARA rule(s).

<hr size=1 width="100%" align=center>

Alert Id	3f74d271
Category	Finished Intelligence Reports
References	cisa cyware health-isac cyware 1 picussecurity cyware 2 cyware 3 fortinet cyware 4 pcrisk cyware 5 cyware 6
Tags	Interlock, Interlock Ransomware, Threat Actor Profile

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments
Please email us at toc@h-isac.org

Please provide your feedback

Like Dislike

Download the App
Available on iOS, Android and Web

Download on the App Store Get it on Google Play

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**
Health-ISAC is an invite only platform. Please DO NOT forward this email to anyone. If you are not supposed to receive this email, please report to **toc@h-isac.org**

--
You received this message because you are subscribed to the Google Groups "TLP Green - Health-ISAC Partners" group.
To unsubscribe from this group and stop receiving emails from it, send an email to health-isac-partners+unsubscribe@h-isac.org.
To view this discussion visit https://groups.google.com/a/h-isac.org/d/msgid/health-isac-partners/0100019fea9d6dd8-2afb00e6-8812-433d-a29e-b060b5b52692-000000%40email.amazonses.com.