U.S. Coast Guard Cyber Command

Maritime Cyber Alert

Information Sharing Protocol: **TLP:CLEAR** (https://www.us-cert.gov/tlp)

April 29, 2026

INC Ransom

Summary

Coast Guard Cyber Command (CGCYBER) is drawing attention to the threat posed by the INC Ransom group, which has demonstrated the capability to target the U.S. Marine Transportation System (MTS) using sophisticated tactics, techniques, and procedures (TTPs). This threat actor gains initial access by exploiting unpatched public-facing applications and through targeted phishing campaigns. Once a foothold is established, the threat actor moves laterally using legitimate network administration tools, attempting to escalate privileges and disable security controls. Ultimately, INC Ransom appears to be a financially motivated group that employs a 'double extortion' model, exfiltrating sensitive data prior to encryption and demanding payment for both data decryption and the non-disclosure of stolen information.

Background

INC Ransom has been active since at least mid-2023, compromising organizations worldwide with a focus on entities in the United States and Europe. Financial gain is their primary motivation for ransomware attacks across industries including critical infrastructure, healthcare, education, and government. While no joint cybersecurity advisory has been issued for this specific group, their tactics, techniques, and procedures (TTPs) are well-documented by government-sponsored organizations like the CISA-sponsored MITRE ATT&CK® framework, which tracks their activities under designation G1032.

Once inside a network, their operational playbook relies heavily on "living off the land" techniques to evade detection. They use native command-line interpreters to execute payloads and leverage legitimate remote access utilities to pivot between hosts. Key tactics include harvesting account credentials from system memory with credential dumping tools while simultaneously disabling endpoint security solutions. In the final stage before encryption, the group exfiltrates large volumes of data using third-party cloud synchronization tools, allowing their activity to blend with normal network traffic.

Targeted Applications & Systems

The systems and the associated Common Vulnerabilities and Exposures (CVEs) exploited by INC Ransom include:

- Citrix NetScaler (ADC & Gateway) appliances (CVE-2023-3519)
- User credentials harvested via targeted phishing campaigns
- Initial Access through exploitation of CVEs on public facing applications

CGCYBER Cyber Protection Teams (CPTs) have observed malicious actors exploiting public facing systems through unpatched vulnerabilities in the MTS. The second most common CVE that CGCYBER CPTs detected in 2023 was found on internet-facing servers, creating a significant vulnerability and entry point for malicious cyber actors. In addition, it was found that INC Ransom actors often operate in environments using the Microsoft 365 application suite. In 2024, CGCYBER CPTs found that 80% of MTS mission partners relied upon the Microsoft 365 application suite for business operations.[1] These findings highlight an increased threat to the MTS due to similar vulnerabilities between MTS entities and known victims of the INC Ransom group.

Threat Actor Tactics:

Below are the MITRE ATT&CK techniques utilized by INC Ransom (Techniques - Enterprise | MITRE ATT&CK®).

T1190: Exploit Public-Facing Application

- INC Ransom has exploited known vulnerabilities including CVE-2023-3519 in Citrix NetScaler for initial access.

T1562.001: Impair Defenses - Disable or Modify Tool

- INC Ransom can use SystemSettingsAdminFlows.exe, a native Windows utility, to disable Windows Defender.

T1059.003: Command and Scripting Interpreter – Windows Command Shell

- INC Ransom has used cmd.exe to launch malicious payloads.

T1070.004: Indicator Removal – File Deletion

- INC Ransom has uninstalled tools from compromised endpoints after use.

T1105: Ingress Tool Transfer

- INC Ransom has downloaded tools to compromised servers including Advanced IP Scanner.

T1570: Lateral Tool Transfer

- INC Ransom has used a rapid succession of copy commands to install a file encryption executable across multiple endpoints within compromised infrastructure.

T1036.005: Masquerading - Match Legitimate Resource Name or Location

- INC Ransom has named a PsExec executable, winupd, to mimic a legitimate Windows update file.

T1003: OS Credential Dumping

[1] "2024 Cyber Trends and Insights in the Marine Environment" 2024 Cyber Trends in the Marine Environment

- Ghost actors use “hashdump” or Mimikatz through Cobalt Strike to collect passwords and hashes for unauthorized logins and privilege escalation.

T1057, T1518.001 & T1562.001: Process Discovery, Security Software Discovery & Disable or Modify Tools

- Ghost actors use Cobalt Strike to list running processes, determine the antivirus software, and then disable it to evade detection in victim networks.

T1087.002, T1135 & T1046: Domain Account Discovery, Network Share Discovery & Network Service Discovery

- INC Ransom has scanned for domain admin accounts in compromised environments.
- INC Ransom has used NETSCAN.EXE for internal reconnaissance.
- INC Ransom has used Internet Explorer to view folders on other systems.

T1588.002: Obtain Capabilities - Tool

- INC Ransom has acquired and used several tools including MegaSync, AnyDesk, esentutl and PsExec.

T1071: Application Layer Protocol

- INC Ransom has used valid accounts over Remote Desktop Protocol (RDP) to connect to targeted systems.

T1069.002: Permission Groups – Domain Groups

- INC Ransom has enumerated domain groups on targeted hosts.

T1560.001: Archive Collected Data – Archive via Utility

- INC Ransom has used 7-Zip and WinRAR to archive collected data prior to exfiltration.

T1486: Data Encrypted for Impact

- INC Ransom has used ransomware to encrypt victim's data.

T1074: Data staged

- INC Ransom has staged data on compromised hosts prior to exfiltration.

T1657: Financial Theft

- INC Ransom has stolen and encrypted victim's data in order to extort payment for keeping it private or decrypting it.

T1566: Phishing

- INC Ransom has used phishing to gain initial access.

T1219.001: Remote Services: Remote Desktop Protocol

- INC Ransom has RDP to move laterally.

T1049: System Network Connections Discovery

- INC Ransom has used RDP to test network connections.

T1569.002: System Services – Service Execution

- INC Ransom has run a file encryption executable via Service Control Manager/7045;winupd,%SystemRoot%\winupd.exe,user mode service, demand start ,LocalSystem.

T1537 : Transfer Data to Cloud Account

- INC Ransom has used Megasync to exfiltrate data to the cloud

Mitigation Measures

CGCYBER recommends MTS partners implement the mitigations below which align with operational insights from CISA, FBI, and the Intelligence Community.[2]

Maintain regular system backups

- CGCYBER observed a company with insufficient backups causing an inability to recover data after a ransomware attack.

Patch known vulnerabilities

- CGCYBER has regularly found CVEs on partner networks, demonstrating a lack of regular software updates. Most Operational Technology (OT) networks assessed by CGCYBER in 2024 ran unsupported software and legacy hardware including End of Life Operating Systems.

Ensure proper network segmentation

- Improper network segmentation was CGCYBER's top finding in OT assessments from 2024.
- Modern vessels and port OT systems are at greater risk of impact from cyber incidents due to increasing interconnectivity. This is evidenced by a 2024 ransomware attack taking place on a vessel due to its connection to the company network. However, this attack did not impact OT onboard the vessel because of proper segmentation of Information Technology (IT) and OT, demonstrating the significance of proper segmentation.

Require phishing-resistant Multi-Factor Authentication (MFA)

- Only 37% of partners assessed by CGCYBER in 2024 used MFA and for around half of these, MFA was bypassed through phishing campaigns.[3]

Enhance email security

- Implement advanced filtering, block malicious attachments, and prevent spoofing

Disable unused ports

- Such as RDP 3398, FTP 21, and SMB 45

Utilize endpoint and detection response (EDR) on systems

- This will alert network defenders of possible malicious activity

Monitor unauthorized use of PowerShell and implement allowlisting

- This will prevent unauthorized access and execution of scripts, applications, and network traffic.
- Conduct user training to help identify phishing attempts. This will reduce the risk of credential compromise and accidental malware infection by enabling users to recognize and report things like malicious emails.

Resources

If your organization has any questions related to this alert, please contact the U.S. Coast Guard at: maritimecyber@uscg.mil, or for immediate assistance call the Coast Guard Cyber Command 24x7 Watch at **202-372-2904**.

- INC Ransom, GOLD IONIC, Group G1032 | MITRE ATT&CK®
- Stop Ransomware | CISA

[2] "How Can I Protect Against Ransomware?" How Can I Protect Against Ransomware? | CISA

[3] "2024 Cyber Trends and Insights in the Marine Environment" 2024 Cyber Trends in the Marine Environment

Appendix A: IOCs

INC Ransom IOCs

Tools
Cobalt Strike
Mimikatz
NETSCAN.EXE
MegaSync
AnyDesk
Essentutl
PsExec
7-Zip
WinRAR
SystemSettingsAdminFlows.exe
Hashdump

Malware
winupd.exe

References

"INC Ransom" October 28, 2024. INC Ransom, GOLD IONIC, Group G1032 | MITRE ATT&CK®

"How Can I Protect Against Ransomware?" How Can I Protect Against Ransomware? | CISA

"2024 Cyber Trends and Insights in the Marine Environment" 2024 Cyber Trends in the Marine Environment