US Coast Guard Cyber Command
Maritime Cyber Alert

March 24, 2025

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

Ghost (Cring) Ransomware Group Targeting Critical Infrastructure

Summary:

Government agencies are observing ransomware attacks on critical infrastructure by Ghost (Cring) ransomware group that exploit vulnerabilities and use tactics similar to those seen in the Marine Transportation System (MTS) by Coast Guard Cyber Command (CGCYBER). Furthermore, CGCYBER has observed malicious actors continuing to execute ransomware attacks on the MTS with more devastating effects. Maritime companies and vessels commonly have Operational Technology (OT) systems that are segmented improperly and equipped with outdated software, posing a higher risk to the MTS. Awareness and implementation of mitigation recommendations can help maritime companies thwart the threat from Ghost actors.

Background:

Ghost ransomware group, located in China, has compromised organizations across more than 70 countries since 2021. Financial gain is their primary motivation for the widespread ransomware attacks on various industries including critical infrastructure, schools, healthcare, government, technology, manufacturing, and businesses.

Ghost actors often target internet facing servers by exploiting Common Vulnerabilities and Exposures (CVEs) that are unpatched. There are various payloads, file extensions, ransom notes, and email addresses used by Ghost actors causing inconsistent attribution of this group. Names associated with this group include Ghost, Cring, Crypt3r, Phantom, Strike, Hello, Wickrme, HsHarada, and Rapture.

The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and the Multi-State Information Sharing and Analysis Center (MS-ISAC) released a

joint cybersecurity advisory on February 19th, 2025, warning of Ghost Ransomware and providing recommended mitigations for companies.[1]

Targeted Applications & Systems

Ghost actors gain initial access to networks by exploiting CVEs on public facing applications. In 2024, while conducting Incident Response for MTS partners, CGCYBER Cyber Protection Teams (CPTs) observed malicious actors typically exploiting public facing systems through unpatched vulnerabilities. Furthermore, the second most common CVE that CGCYBER CPTs detected in 2023 was often found on internet facing servers.[2] These findings highlight an increased threat to the marine environment due to similar vulnerabilities between MTS companies and victims of the Ghost ransomware group.

The systems and the associated CVEs exploited by Ghost actors include:

- Fortinet FortiOS appliances (CVE-2018-13379)
- Servers running Adobe ColdFusion (CVE-2010-2861, CVE-2009-3960)
- Microsoft SharePoint (CVE-2019-0604)
- Microsoft Exchange (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207)

Fortinet, which has been targeted by Ghost actors, provides various security products for Managed Security Services Providers (MSSPs).[3] In 2024, CGCYBER CPTs found that 73% of MTS mission partners used MSSPs. Similarly, Ghost actors are targeting applications within 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.

Threat Actor Tactics:

Below are the tactics referenced by MITRE ATT&CK techniques, which are linked to these attacks (Techniques - Enterprise | MITRE ATT&CK®).

- **T1190: Exploit Public-Facing Application**
  - Threat actors obtain initial access via unpatched public facing web applications by exploiting CVEs.
  - CGCYBER has increasingly been able to exploit public facing applications in the last three years of assessing MTS partners networks including 12 instances in 2024.
- **T1505.003: Server Software Component – Web Shell**
  - Threat actors upload web scripts to compromised servers to establish persistence.
- **T1059.003 & T1059.001: Command and Scripting Interpreter – Windows Command Shell and PowerShell**

---

[1] "#StopRansomware: Ghost (Cring) Ransomware" February 19, 2025. #StopRansomware: Ghost (Cring) Ransomware | CISA

[2] "2023 Cyber Trends and Insights in the Marine Environment" 2023 Cyber Trends and Insights in the Marine Environment

[3] "Managed Security Services Providers" Managed Security Services - MSSP | Fortinet

    - Ghost actors use Command Prompt and PowerShell to download and execute Cobalt Strike Beacon malware.
- **T1105: Ingress Tool Transfer**
    - Used by actors to transfer tools and files from Cobalt Strike to be executed on target systems.
- **T1136.001**, **T1136.002 & T1098: Create Local Account, Create Domain Account & Account Manipulation**
    - Ghost actors occasionally create new local and domain accounts and changed existing account passwords.
- **T1505.003: Server Software Component – Web Shell**
    - Ghost actors deployed web shells on target web servers in 2024.
- **T1134.001: Access Token Manipulation – Token Impersonation/Theft**
    - Ghost actors impersonate the SYSTEM user by stealing process tokens using Cobalt Strike functions in order to run Beacon again with elevated privileges.
- **T1068: Exploitation for Privilege Escalation**
    - Ghost actors escalate privileges using open source tools.
- **T1003: OS Credential Dumping**
    - 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 process, determine the antivirus software, and then disable it to evade detection in victim networks.
- **T1087.002, T1135 & T1018: Domain Account Discovery, Network Share Discovery & Remote System Discovery**
    - Ghost Actors utilize Cobalt Strike commands for domain account discovery and open-source tools to discover network shares and remote systems.
- **T1047, T1132.001 & T1564.003**: **Windows Management Instrumentation, Standard Data Encoding & Hidden Window**
    - Ghost actors move laterally by using Windows Management Instrumentation command line for running commands on systems in the victim network. They then use Cobalt Strike to encode subsequent Beacon infections.
- **T1071.001: Application Layer Protocol – Web Protocols**
    - Ghost actors conduct command and control using Cobalt Strike malware and servers that function using HTTP and HTTPS.
- **T1573: Encrypted Channel**
    - While communicating via email with victims, Ghost actors use legitimate email services with encryption.
- **T1486**, **T1070.001 & T1490: Data Encrypted for Impact, Clear Windows Event Logs, Inhibit System Recovery**
    - Ghost Actors encrypt victim data using ransomware executables that clear Windows Event Logs and inhibit system recovery. They then hold the encrypted data for ransom in exchange for cryptocurrency.

Mitigation Measures:

CGCYBER recommends MTS partners implement the mitigations below which align with the joint cybersecurity advisory mitigations from the FBI, CISA, and MS-ISAC.

- **Maintain regular system backups**
  - CGCYBER observed a company with insufficient backups causing inability to recover data after a ransomware attack.
- **Patch known vulnerabilities**
  - CGCYBER has regularly found CVEs on partner networks, demonstrating lack of regular software updates. Most 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 ransomware attack taking place on a vessel due to connection to the company network. However, this attack did not impact OT onboard the vessel because of proper segmentation of 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.
- **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**

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.

Appendix A: IOCs

Ghost Actor Tool IOCs

Tool	Source
Cobalt Strike	N/A
I0X	github[.]com/EddieIvan01/iox
SharpShares.exe	github[.]com/mitchmoser/SharpShares
SharpZeroLogon.exe	github[.]com/leitosama/SharpZeroLogon
SharpGPPPass.exe	N/A
SpnDump.exe	N/A
NBT.exe	github[.]com/BronzeTicket/SharpNBTScan
BadPotato.exe	github[.]com/BeichenDream/BadPotato
God.exe	github[.]com/BeichenDream/GodPotato
HFS (HTTP File Server	rejitto[.]com/hfs
Ladon 911	github[.]com/k8gege/Ladon
Web Shell	Slight variation of github[.]com/BeichenDream/ChunkProxy/blob/main/proxy.aspx

Ghost File IOCs

File Name	MD5 File Hash
Cring.exe	c5d712f82d5d37bb284acd4468ab3533
Ghost.exe	34b3009590ec2d361f07cac320671410 d9c019182d88290e5489cdf3b607f982
ElysiumO.exe	29e44e8994197bdb0c2be6fc5dfc15c2 c9e35b5c1dc8856da25965b385a26ec4 d1c5e7b8e937625891707f8b4b594314
Locker.exe	ef6a213f59f3fbee2894bd6734bbaed2
iex.txt, pro.txt (I0X)	ac58a214ce7deb3a578c10b97f93d9c3
x86.log (I0X)	c3b8f6d102393b4542e9f951c9435255 0a5c4ad3ec240fbfd00bdc1d36bd54eb
sp.txt (I0X)	ff52fdf84448277b1bc121f592f753c5
main.txt (I0X)	a2fd181f57548c215ac6891d000ec6b9
isx.txt (I0X)	625bd7275e1892eac50a22f8b4a6355d
sock.txt (I0X)	db38ef2e3d4d8cb785df48f458b35090

Ransom Email Address IOCs

asauribe@tutanota.com	ghostbackup@skiff.com	rainbowforever@tutanota.com
cringghost@skiff.com	ghosts1337@skiff.com	retryit1998@mailfence.com
crptbackup@skiff.com	ghosts1337@tuta.io	retryit1998@tutamail.com
d3crypt@onionmail.org	ghostsbackup@skiff.com	rsacrpthelp@skiff.com
d3svc@tuta.io	hsharada@skiff.com	rsahelp@protonmail.com
eternalnightmare@tutanota.com	just4money@tutanota.com	sdghost@onionmail.org
evilcorp@skiff.com	kellyreiff@tutanota.com	shadowghost@skiff.com
fileunlock@onionmail.org	kev1npt@tuta.io	shadowghosts@tutanota.com
fortihooks@protonmail.com	lockhelp1998@skiff.com	summerkiller@mailfence.com
genesis1337@tutanota.com	r.heisler@skiff.com	summerkiller@tutanota.com

ghost1998@tutamail.com	rainbowforever@skiff.com	webroothooks@tutanota.com

References:

"#StopRansomware: Ghost (Cring) Ransomware" February 19, 2025. #StopRansomware: Ghost (Cring) Ransomware | CISA

"2023 Cyber Trends and Insights in the Marine Environment" 2023 Cyber Trends and Insights in the Marine Environment

"Managed Security Services Providers" Managed Security Services - MSSP | Fortinet