#StopRansomware: Ghost (Cring) Ransomware | CISA

Published: 2025-02-19 · Archived: 2026-04-06 00:56:19 UTC

1. Maintain regular system backups stored separately from the source systems which cannot be altered or encrypted by potentially compromised network devices [CPG 2.R].
2. Patch known vulnerabilities by applying timely security updates to operating systems, software, and firmware within a risk-informed timeframe [CPG 2.F].
3. Common Vulnerabilities and Exposures (CVE): CVE-2018-13379, CVE-2010-2861, CVE-2009-3960, CVE-2021-34473, CVE-2021-34523, CVE-2021-31207.
4. Segment networks to restrict lateral movement from initial infected devices and other devices in the same organization [CPG 2.F].
5. Require Phishing-Resistant MFA for access to all privileged accounts and email services accounts.

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), and the Multi-State Information Sharing and Analysis Center (MS-ISAC) are releasing this joint advisory to disseminate known Ghost (Cring)—(“Ghost”)—ransomware IOCs and TTPs identified through FBI investigation as recently as January 2025.

Beginning early 2021, Ghost actors began attacking victims whose internet facing services ran outdated versions of software and firmware. This indiscriminate targeting of networks containing vulnerabilities has led to the compromise of organizations across more than 70 countries, including organizations in China. Ghost actors, located in China, conduct these widespread attacks for financial gain. Affected victims include critical infrastructure, schools and universities, healthcare, government networks, religious institutions, technology and manufacturing companies, and numerous small- and medium-sized businesses.

Ghost actors rotate their ransomware executable payloads, switch file extensions for encrypted files, modify ransom note text, and use numerous ransom email addresses, which has led to variable attribution of this group over time. Names associated with this group include Ghost, Cring, Crypt3r, Phantom, Strike, Hello, Wickrme, HsHarada, and Rapture. Samples of ransomware files Ghost used during attacks are: Cring.exe, Ghost.exe, ElysiumO.exe, and Locker.exe.

Ghost actors use publicly available code to exploit Common Vulnerabilities and Exposures (CVEs) and gain access to internet facing servers. Ghost actors exploit well known vulnerabilities and target networks where available patches have not been applied.

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

Download the PDF version of this report:

For a downloadable copy of IOCs, see:

Technical Details

Note: This advisory uses the MITRE ATT&CK® Matrix for Enterprise framework, version 16.1. See the **MITRE ATT&CK Tactics and Techniques** section of this advisory for a table of the threat actors’ activity mapped to MITRE ATT&CK tactics and techniques.

Initial Access

The FBI has observed Ghost actors obtaining initial access to networks by exploiting public facing applications that are associated with multiple CVEs [T1190]. Their methodology includes leveraging vulnerabilities in Fortinet FortiOS appliances (CVE-2018-13379), servers running Adobe ColdFusion (CVE-2010-2861 and CVE-2009-3960), Microsoft SharePoint (CVE-2019-0604), and Microsoft Exchange (CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207—commonly referred to as the ProxyShell attack chain).

Execution

Ghost actors have been observed uploading a web shell [T1505.003] to a compromised server and leveraging Windows Command Prompt [T1059.003] and/or PowerShell [T1059.001] to download and execute Cobalt Strike Beacon malware [T1105] that is then implanted on victim systems. Despite Ghost actors' malicious implementation, Cobalt Strike is a commercially available adversary simulation tool often used for the purposes of testing an organization's security controls.

Persistence

Persistence is not a major focus for Ghost actors, as they typically only spend a few days on victim networks. In multiple instances, they have been observed proceeding from initial compromise to the deployment of ransomware within the same day. However, Ghost actors sporadically create new local [T1136.001] and domain accounts [T1136.002] and change passwords for existing accounts [T1098]. In 2024, Ghost actors were observed deploying web shells [T1505.003] on victim web servers.

Privilege Escalation

Ghost actors often rely on built in Cobalt Strike functions to steal process tokens running under the SYSTEM user context to impersonate the SYSTEM user, often for the purpose of running Beacon a second time with elevated privileges [T1134.001].

Ghost actors have been observed using multiple open-source tools in an attempt at privilege escalation through exploitation [T1068] such as "SharpZeroLogon ," "SharpGPPPass," "BadPotato ," and "GodPotato ." These privilege escalation tools would not generally be used by individuals with legitimate access and credentials.

See **Table 1** for a descriptive listing of tools.

Credential Access

Ghost actors use the built in Cobalt Strike function "hashdump" or Mimikatz [T1003] to collect passwords and/or password hashes to aid them with unauthorized logins and privilege escalation or to pivot to other victim devices.

Defense Evasion

Ghost actors used their access through Cobalt Strike to display a list of running processes [T1057] to determine which antivirus software [T1518.001] is running so that it can be disabled [T1562.001]. Ghost frequently runs a command to disable Windows Defender on network connected devices. Options used in this command are: Set-MpPreference -DisableRealtimeMonitoring 1 -DisableIntrusionPreventionSystem 1 -DisableBehaviorMonitoring 1 -DisableScriptScanning 1 -DisableIOAVProtection 1 -EnableControlledFolderAccess Disabled -MAPSReporting Disabled -SubmitSamplesConsent NeverSend.

Discovery

Ghost actors have been observed using other built-in Cobalt Strike commands for domain account discovery [T1087.002], open-source tools such as "SharpShares " for network share discovery [T1135], and "Ladon 911 " and "SharpNBTScan " for remote systems discovery [T1018]. Network administrators would be unlikely to use these tools for network share or remote systems discovery.

Lateral Movement

Ghost actors used elevated access and Windows Management Instrumentation Command-Line (WMIC) [T1047] to run PowerShell commands on additional systems on the victim network— often for the purpose of initiating additional Cobalt Strike Beacon infections. The associated encoded string is a base 64 PowerShell command that always begins with: powershell -nop -w hidden -encodedcommand JABzAD0ATgBlAHcALQBPAGIAagBlAGMAdAAgAEkATwAuAE0AZQBtAG8AcgB5AFMAdAByAGUAYQBtACgALABbAEMAbwBuAHYAZQI][T1564.003].

This string decodes to "$s=New-Object IO.MemoryStream(,[Convert]::FromBase64String("" and is involved with the execution of Cobalt Strike in memory on the target machine.

In cases where lateral movement attempts are unsuccessful, Ghost actors have been observed abandoning an attack on a victim.

Exfiltration

Ghost ransom notes often claim exfiltrated data will be sold if a ransom is not paid. However, Ghost actors do not frequently exfiltrate a significant amount of information or files, such as intellectual property or personally identifiable information (PII), that would cause significant harm to victims if leaked. The FBI has observed limited downloading of data to Cobalt Strike Team Servers [T1041]. Victims and other trusted third parties have reported limited uses of Mega.nz [T1567.002

] and installed web shells for similar limited data exfiltration. **Note:** The typical data exfiltration is less than hundreds of gigabytes of data.

Command and Control

Ghost actors rely heavily on Cobalt Strike Beacon malware and Cobalt Strike Team Servers for command and control (C2) operations, which function using hypertext transfer protocol (HTTP) and hypertext transfer protocol secure (HTTPS) [T1071.001]. Ghost rarely registers domains associated with their C2 servers. Instead, connections made to a uniform resource identifier (URI) of a C2 server, for the purpose of downloading and executing Beacon malware, directly reference the C2 server's IP address. For example, http://xxx.xxx.xxx.xxx:80/Google.com where xxx.xxx.xxx.xxx represents the C2 server's IP address.

For email communication with victims, Ghost actors use legitimate email services that include traffic encryption features. [T1573] Some examples of emails services that Ghost actors have been observed using are Tutanota, Skiff, ProtonMail, Onionmail, and Mailfence.

Note: Table 2 contains a list of Ghost ransom email addresses.

Impact and Encryption

Ghost actors use Cring.exe, Ghost.exe, ElysiumO.exe, and Locker.exe, which are all ransomware executables that share similar functionality. Ghost variants can be used to encrypt specific directories or the entire system's storage [T1486]. The nature of executables' operability is based on command line arguments used when executing the ransomware file. Various file extensions and system folders are excluded during the encryption process to avoid encrypting files that would render targeted devices inoperable.

These ransomware payloads clear Windows Event Logs [T1070.001], disable the Volume Shadow Copy Service, and delete shadow copies to inhibit system recovery attempts [T1490]. Data encrypted with Ghost ransomware variants cannot be recovered without the decryption key. Ghost actors hold the encrypted data for ransom and typically demand anywhere from tens to hundreds of thousands of dollars in cryptocurrency in exchange for decryption software [T1486].

The impact of Ghost ransomware activity varies widely on a victim-to-victim basis. Ghost actors tend to move to other targets when confronted with hardened systems, such as those where proper network segmentation prevents lateral moment to other devices.

Indicators of Compromise (IOC)

Table 1 lists several tools and applications Ghost actors have used for their operations. The use of these tools and applications on a network should be investigated further.

Note: Authors of these tools generally state that they should not be used in illegal activity.

Table 1: Tools Leveraged by Ghost Actors

Name	Description	Source
Cobalt Strike	Cobalt Strike is penetration testing software. Ghost actors use an unauthorized version of Cobalt Strike.	N/A
IOX	Open-source proxy, used to establish a reverse proxy to a Ghost C2 server from an internal victim device.	github[.]com/EddieIvan01/iox
SharpShares.exe	SharpShares.exe is used to enumerate accessible network shares in a domain. Ghost actors use this primarily for host discovery.	github[.]com/mitchmoser/SharpShares
SharpZeroLogon.exe	SharpZeroLogon.exe attempts to exploit CVE-2020-1472 and is run against a target Domain Controller.	github[.]com/leitosama/SharpZeroLogon
SharpGPPPass.exe	SharpGPPPass.exe attempts to exploit CVE-2014-1812 and targets XML files created through Group Policy Preferences that may contain passwords.	N/A
SpnDump.exe	SpnDump.exe is used to list service principal name identifiers, which Ghost	N/A

Name	Description	Source
	actors use for service and hostname enumeration.	
NBT.exe	A compiled version of SharpNBTScan, a NetBIOS scanner. Ghost actors use this tool for hostname and IP address enumeration.	github[.]com/BronzeTicket/SharpNBTScan
BadPotato.exe	BadPotato.exe is an exploitation tool used for privilege escalation.	github[.]com/BeichenDream/BadPotato
God.exe	God.exe is a compiled version of GodPotato and is used for privilege escalation.	github[.]com/BeichenDream/GodPotato
HFS (HTTP File Server)	A portable web server program that Ghost actors use to host files for remote access and exfiltration.	rejitto[.]com/hfs
Ladon 911	A multifunctional scanning and exploitation tool, often used by Ghost actors with the MS17010 option to scan for SMB vulnerabilities associated with CVE-2017-0143 and CVE-2017-0144.	github[.]com/k8gege/Ladon
Web Shell	A backdoor installed on a web server that allows for the execution of commands and facilitates persistent access.	Slight variation of github[.]com/BeichenDream/Chunk-Proxy/blob/main/proxy.aspx

Table 2: MD5 File Hashes Associated with Ghost Ransomware Activity

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

Ransom Email Addresses

Table 3 is a subset of ransom email addresses that have been included in Ghost ransom notes.

Table 3: Ransom Email Addresses

Email Addresses

Email Addresses		
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

Ransom Notes

Starting approximately in August 2024, Ghost actors began using TOX IDs in ransom notes as an alternative method for communicating with victims. For example: EFE31926F41889DBF6588F27A2EC3A2D7DEF7D2E9E0A1DEFD39B976A49C11F0E19E03998DBDA and E83CD54EAAB0F31040D855E1ED993E2AC92652FF8E8742D3901580339D135C6EBCD71002885B.

MITRE ATT&CK Tactics and Techniques

See **Table 4 to Table 13** for all referenced threat actor tactics and techniques in this advisory. For assistance with mapping malicious cyber activity to the MITRE ATT&CK framework, version 16.1, see CISA and MITRE ATT&CK's Best Practices for MITRE ATT&CK Mapping and CISA's Decider Tool.

Table 4: Initial Access

Technique Title	ID	Use
Exploit Public-Facing Application	T1190	Ghost actors exploit multiple vulnerabilities in public-facing systems to gain initial access to servers.

Table 5: Execution

Technique Title	ID	Use
Windows Management Instrumentation	T1047	Ghost actors abuse WMI to run PowerShell scripts on other devices, resulting in their infection with Cobalt Strike Beacon malware.
PowerShell	T1059.001	Ghost actors use PowerShell for various functions including to deploy Cobalt Strike.
Windows Command Shell	T1059.003	Ghost actors use the Windows Command Shell to download malicious content on to victim servers.

Table 6: Persistence

Technique Title	ID	Use
Account Manipulation	T1098	Ghost actors change passwords for already established accounts.
Local Account	T1136.001	Ghost actors create new accounts or makes modifications to local accounts.
Domain Account	T1136.002	Ghost actors create new accounts or makes modifications to domain accounts.
Web Shell	T1505.003	Ghost actors upload web shells to victim servers to gain access and for persistence.

Table 7: Privilege Escalation

Technique Title	ID	Use

Technique Title	ID	Use
Exploitation for Privilege Escalation	T1068	Ghost actors use a suite of open source tools in an attempt to gain elevated privileges through exploitation of vulnerabilities.
Token Impersonation/Theft	T1134.001	Ghost actors use Cobalt Strike to steal process tokens of processes running at a higher privilege.

Table 8: Defense Evasion

Technique Title	ID	Use
Application Layer Protocol: Web Protocols	T1071.001	Ghost actors use HTTP and HTTPS protocols while conducting C2 operations.
Impair Defenses: Disable or Modify Tools	T1562.001	Ghost actors disable antivirus products.
Hidden Window	T1564.003	Ghost actors use PowerShell to conceal malicious content within legitimate appearing command windows.

Table 9: Credential Access

Technique Title	ID	Use
OS Credential Dumping	T1003	Ghost actors use Mimikatz and the Cobalt Strike “hashdump” command to collect passwords and password hashes.

Table 10: Discovery

Technique Title	ID	Use
Remote System Discovery	T1018	Ghost actors use tools like Ladon 911 and ShapNBTScan for remote systems discovery.
Process Discovery	T1057	Ghost actors run a ps command to list running processes on an infected device.
Domain Account Discovery	T1087.002	Ghost actors run commands such as net group “Domain Admins” /domain to discover a list of domain administrator accounts.
Network Share Discovery	T1135	Ghost actors use various tools for network share discovery for the purpose of host enumeration.
Software Discovery	T1518	Ghost actors use their access to determine which antivirus software is running.
Security Software Discovery	T1518.001	Ghost actors run Cobalt Strike to enumerate running antivirus software.

Table 11: Exfiltration

Technique Title	ID	Use
Exfiltration Over C2 Channel	T1041	Ghost actors use both web shells and Cobalt Strike to exfiltrate limited data.
Exfiltration to Cloud Storage	T1567.002	Ghost actors sometimes use legitimate cloud storage providers such as Mega.nz for malicious exfiltration operations.

Table 12: Command and Control

Technique Title	ID	Use
Web Protocols	T1071.001	Ghost actors use Cobalt Strike Beacon malware and Cobalt Strike Team Servers which communicate over HTTP and HTTPS.
Ingress Tool Transfer	T1105	Ghost actors use Cobalt Strike Beacon malware to deliver ransomware payloads to victim servers.
Standard Encoding	T1132.001	Ghost actors use PowerShell commands to encode network traffic which reduces their likelihood of being detected during lateral movement.
Encrypted Channel	T1573	Ghost actors use encrypted email platforms to facilitate communications.

Table 13: Impact

Technique Title	ID	Use

Technique Title	ID	Use
Data Encrypted for Impact	T1486	Ghost actors use ransomware variants Cring.exe, Ghost.exe, ElysiumO.exe, and Locker.exe to encrypt victim files for ransom.
Inhibit System Recovery	T1490	Ghost actors delete volume shadow copies.

Mitigations

The FBI, CISA, and MS-ISAC recommend organizations reference their #StopRansomware Guide and implement the mitigations below to improve cybersecurity posture on the basis of the Ghost ransomware activity. These mitigations align with the Cross-Sector Cybersecurity Performance Goals (CPGs) developed by CISA and the National Institute of Standards and Technology (NIST). The CPGs provide a minimum set of practices and protections that CISA and NIST recommend all organizations implement. CISA and NIST based the CPGs on existing cybersecurity frameworks and guidance to protect against the most common and impactful threats, tactics, techniques, and procedures. Visit CISA's CPGs webpage for more information on the CPGs, including additional recommended baseline protections.

- **Maintain regular system backups** that are known-good and stored offline or are segmented from source systems [CPG 2.R]. Ghost ransomware victims whose backups were unaffected by the ransomware attack were often able to restore operations without needing to contact Ghost actors or pay a ransom.
- **Patch known vulnerabilities by** applying timely security updates to operating systems, software, and firmware within a risk-informed timeframe [CPG 1.E].
- **Segment networks to restrict lateral movement from initial infected devices and other devices in the same organization [CPG 2.F].**
- **Require Phishing-Resistant MFA for access to all privileged accounts and email services accounts.**
- **Train users to recognize phishing attempts.**
- **Monitor for unauthorized use of PowerShell. Ghost actors leverage PowerShell for malicious purposes, although it is often a helpful tool that is used by administrators and defenders to manage system resources. For more information, visit NSA and CISA's joint guidance on PowerShell best practices.**
    - Implement the principle of least privilege when granting permissions so that employees who require access to PowerShell are aligned with organizational business requirements.
- **Implement allowlisting** for applications, scripts, and network traffic to prevent unauthorized execution and access [CPG 3.A].
- **Identify, alert on, and investigate abnormal network activity. Ransomware activity generates unusual network traffic across all phases of the attack chain. This includes running scans to discover other network connected devices, running commands to list, add, or alter administrator accounts, using PowerShell to download and execute remote programs, and running scripts not usually seen on a network. Organizations that can successfully identify and investigate this activity are better able to interrupt malicious activity before ransomware is executed [CPG 3.A].**
    - Ghost actors run a significant number of commands, scripts, and programs that IT administrators would have no legitimate reason for running. Victims who have identified and responded to this unusual behavior have successfully prevented Ghost ransomware attacks.
- **Limit exposure of services by disabling unused ports** such as, RDP 3398, FTP 21, and SMB 445, and restricting access to essential services through securely configured VPNs or firewalls.
- **Enhance email security** by implementing advanced filtering, blocking malicious attachments, and enabling DMARC, DKIM, and SPF to prevent spoofing [CPG 2.M].

Validate Security Controls

In addition to applying mitigations, the FBI, CISA, and MS-ISAC recommend exercising, testing, and validating your organization's security program against the threat behaviors mapped to the MITRE ATT&CK for Enterprise framework in this advisory.

To get started:

1. Select an ATT&CK technique described in this advisory (see **Table 3** to **Table 13**).
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.

Reporting

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

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

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

The FBI, CISA, and MS-ISAC do not encourage paying ransom as payment does not guarantee victim files will be recovered. Furthermore, payment may also embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities. Regardless of whether you or your organization have decided to pay the ransom, the FBI and CISA urge you to promptly report ransomware incidents to 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 (report@cisa.gov✉) or by calling 1-844-Say-CISA (1-844-729-2472).

Disclaimer

The information in this report is being provided "as is" for informational purposes only. The FBI, CISA, and MS-ISAC do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by the FBI, CISA, and the MS-ISAC.

Version History

February 19, 2025: Initial version.
