JOINT
CYBERSECURITY ADVISORY

TLP:CLEAR

Product ID: AA26-222A

Co-Authored by:

#StopRansomware: Gunra Ransomware

Publication: August 10, 2026

U.S. Federal Bureau of Investigation
U.S. Cybersecurity and Infrastructure Security Agency
U.S. Department of Defense Cyber Crime Center
U.S. National Security Agency
U.S. Secret Service
Republic of Korea's National Police Agency

To report suspicious or criminal activity related to information found in this joint Cybersecurity Advisory, contact the FBI's Internet Crime Complaint Center (IC3), your local FBI field office, your local USSS field office, and/or CISA's 24/7 Operations Center at contact@cisa.dhs.gov or 1-844-Say-CISA (1-844-729-2472). 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. For NSA-client cybersecurity guidance inquiries, contact CybersecurityReports@nsa.gov.

Advisory at a Glance

Title	#StopRansomware: Gunra Ransomware
Original Publication	August 10, 2026
Executive Summary	Gunra is a ransomware-as-a-service (RaaS) used by affiliates to target government, critical infrastructure, and other organizations. The Gunra ransomware variant first appeared in 2025 and expanded to RaaS operations in 2026. The actors leverage a double-extortion model, both encrypting data and threatening to publish exfiltrated data to a dedicated leak site (DLS) if the ransom is not paid. This advisory provides technical details of the activity, as well as tailored detection and mitigation guidance to protect at-risk organizations from Gunra.
Key Actions	▪ **Prioritize patching known exploited vulnerabilities in internet-facing systems**, including virtual private network (VPN) gateways and remote desktop protocol (RDP)-exposed infrastructure. ▪ **Implement and test offline, immutable backups** stored in a physically separate, segmented location to ensure recoverability without ransom payment. ▪ **Segment networks** to restrict lateral movement from an initially compromised device to other systems in the organization.
Indicators of Compromise	For a downloadable copy of indicators of compromise, see: ▪ AA26-222A STIX XML (55KB) ▪ AA26-222A STIX JSON (62 KB)
Intended Audience	**Organizations:** Government, Critical Infrastructure **Sectors:** Healthcare and public health, financial services and insurance, critical manufacturing and construction, transportation systems and logistics, government services and facilities, utilities, academia, media and communications, retail, and professional and nonprofit services. **Roles:** Cybersecurity architects, defensive cybersecurity analysts, vulnerability analysts, systems administrators, and security systems managers.

Table of Contents

Introduction

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 Defense Cyber Crime Center (DC3), National Security Agency (NSA), U.S. Secret Service (USSS), and Republic of Korea's National Police Agency (KNPA)—hereafter referred to as "the authoring agencies"—are releasing this joint advisory to alert organizations to the emerging Gunra ransomware threat and to provide detection and mitigation guidance.

Gunra first emerged in April 2025 as a sophisticated double-extortion ransomware variant derived from the leaked Conti[1] ransomware source code. As of early 2026, Gunra expanded its operations through a structured ransomware-as-a-service (RaaS) affiliate program advertised on dark web forums to financially motivated cybercriminals. Gunra actors demand ransom via a customized, Tor-based negotiation portal and threaten to publish exfiltrated data on a dedicated leak site (DLS) if victims do not comply.

Gunra victims observed on the actors' DLS span organizations across multiple sectors in the Americas, Europe, Middle East, Africa, and the Asia-Pacific.[2] These sectors include:

- Healthcare and public health
- Financial services and insurance
- Critical manufacturing and construction
- Transportation systems and logistics
- Government services and facilities
- Utilities
- Academia
- Media and communications
- Retail
- Professional and nonprofit services

The authoring agencies encourage organizations to implement the recommendations in the **Mitigations** section of this advisory to mitigate cyber threats related to Gunra ransomware, including:

- **Prioritizing patching known exploited vulnerabilities** in internet-facing systems, including virtual private network (VPN) gateways and remote desktop protocol (RDP)-exposed infrastructure.
- **Implementing and testing offline, immutable backups** stored in a physically separate, segmented location to ensure recoverability without ransom payment.
- **Segmenting networks** to restrict lateral movement from an initially compromised device to other systems in the organization.

For a downloadable copy of IOCs, see:

- AA26-222A STIX XML (55KB)
- AA26-222A STIX JSON (62 KB)

Technical Details

Note: This advisory uses the MITRE ATT&CK® Matrix for Enterprise framework, version 19.1. 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.

Overview

The FBI originally observed Gunra ransomware in April 2025. The threat actors quickly established a DLS on the Tor network to list victims and publish exfiltrated data. As of January 2026, Gunra launched a formal RaaS affiliate program on dark web forums, providing affiliates with access to a management panel, a configurable ransomware builder, cross-platform locker payloads, and structured affiliate documentation.[3] The FBI observed the group adopting new branding aliases (notably operating under the name Golden Community) to support this expansion. Gunra has further commercialized its platform by actively recruiting penetration testers and ethical hackers to serve as initial access brokers, offering a share of the ransom profits in exchange for enterprise network access.

Based on FBI observations, Gunra actors use a traditional double-extortion model, exfiltrating sensitive victim data prior to encryption and threatening to publish the leaked data on their DLS unless the ransom is paid. Victims receive a ransom note in every affected directory guiding them to a Tor-based negotiation portal where they are assigned a Client ID and an initial password. Subsequently, victims receive instructions to contact the Gunra actors via qTox (an encrypted messaging application) to negotiate ransom payments within five to seven days. If the ransom is not paid, Gunra actors threaten to sell victim data on the DLS.

Gunra ransomware appears to be based on, or significantly influenced by, the Conti ransomware source code leaked in 2022.[4] Initially, Gunra actors' campaigns focused on Windows environments; reporting in mid-2025 indicated the group introduced a Linux variant and moved toward broader cross-platform targeting. [5]

Initial Access

The FBI observed Gunra actors obtaining initial access [TA0001] primarily through the exploitation of known vulnerabilities in internet-facing devices [T1190], including firewall and VPN appliances. The FBI observed exploits based on the following Common Vulnerabilities and Exposures (CVEs):

- CVE-2024-55591 [CWE-288: Authentication Bypass Using an Alternate Path or Channel]: Authentication bypass vulnerability affecting specific FortiOS and FortiProxy versions (see CVE record for more details).
- CVE-2025-24472 [CWE-288: Authentication Bypass Using an Alternate Path or Channel]: Authentication bypass vulnerability affecting specific FortiOS and FortiProxy versions (see CVE record for more details).

Additionally, for initial access, KNPA observed Gunra actors exploit credential-exposure and Secure Shell (SSH) access control vulnerabilities in internet-facing VPN gateways to gain unauthorized remote access.

Execution

Gunra's Windows encryptor relies on native operating system (OS) application programming interfaces (APIs) to drive both execution and targeted encryption activity. The binary uses the `FindFirstFileW`/`FindNextFileW` API calls [T1106] to enumerate files and directories on all accessible drive letters (A through Z), enabling comprehensive traversal of the file system prior to encryption of victim data.

Persistence, Privilege Escalation, Lateral Movement, and Command and Control

Gunra actors regularly exploit Impacket libraries `psexec.py` and `smbclient.py` to move laterally across victim networks using the Server Message Block (SMB) protocol [T1021.002].

KPNA observed that against one victim, Gunra actors gained access to an administrator account for a secure socket layer (SSL)-VPN appliance [T1133] by exploiting default credentials when account lockout controls were not present [T1078.001][T1078.002]. The actors subsequently downloaded OpenSSH (an SSH tunneling tool) [T1105] from an external attacker-controlled server to establish connections between compromised systems and maintain persistence in the victim's environment [T1572].

After gaining access to an internet-connected workstation used by a network administrator, Gunra actors accessed the SSL-VPN administrative web console and identified an unused account that had access to both the internet-facing and internal corporate networks. The actors modified the account configuration to bypass the mandatory password change requirement enforced on the account and subsequently leveraged it for malicious activities [T1098].

Using stolen session information, Gunra actors gained initial access to the internal virtual desktop infrastructure (VDI) environment and conducted lateral movement via RDP [T1021.001]. The actors pivoted to multiple critical systems, including the VDI authentication web server, the internal Active Directory (AD) server, and virtual desktops assigned to IT personnel.

Credential Access

The FBI observed multiple instances of Gunra actors using `secretsdump.py` (another Impacket library) to conduct OS credential dumping [T1003.003] against compromised domain controllers to extract password hashes of user accounts from the NT Directory Services (NTDS) file. This enabled pass-the-hash [T1550.002] or pass-the-ticket [T1550.003] attacks for lateral movement into other privileged systems.

For one victim, Gunra actors manipulated the network traffic control functionality of an SSL-VPN appliance to collect credentials and session information transmitted by users authenticating to a corporate VDI authentication portal [T1040]. The actors then used stolen session cookies to conduct session hijacking [T1539], impersonating legitimate users to gain access to the internal network.

For the same victim, the Gunra actors modified authentication processing files on the corporate VDI authentication portal server to allow successful authentication when a specific, Gunra-designated one time password (OTP) value was entered, thereby enabling the continuous bypass of multi-factor authentication (MFA) [T1556.006].

Additionally, the actors accessed a Hiware system access control server via SSH from a compromised virtual desktop and stole a symmetric encryption key stored on the server. The stolen key enabled the actors to decrypt passwords for enterprise server accounts stored within the database [T1555] and perform credential dumping of credentials associated with all enterprise servers [T1003].

Stealth, Defense Impairment, and Discovery

Gunra employs multiple stealth and defense impairment techniques to hinder detection and analysis. While active within victim networks, Gunra actors typically attempt to mask their presence by deleting system/network access logs [T1685] and clearing command history [T1070.003]. Additionally, to evade administrator detection, Gunra actors primarily conduct malicious activities and internal infrastructure reconnaissance [T1049] during late-night and early-morning hours (10:00 p.m. – 06:00 a.m.) [T1678].

The ransomware binary is self-contained and performs full volume encryption without observable network indicators (e.g., domain name system, HTTP).[6] The Windows binary includes the `IsDebuggerPresent` API [T1622], which defends against reverse engineering by detecting if the application is being run in a debugger.[7]

To avoid dedicating encryption resources to non-critical files, the binary includes filtering logic to exclude common system directories (e.g., `C:\Windows`, `C:\Program Files`, `C:\Program Files (x86)`) from the file system reconnaissance [T1679]. For files that pass the initial filter, the binary checks against a second set of filter rules that exclude file extensions related to system-critical files (e.g., `.exe`, `.dll`, `.sys`). Files with extensions consistent with user data (e.g., documents, databases, images, archives) are approved and added to the work queue for data encryption.[8]

Prior to encryption, Gunra performs file and directory discovery across all accessible drive letters (A through Z) to identify victim data for targeting [T1083].[9]

Collection and Exfiltration

Prior to data encryption, Gunra actors collect sensitive victim data as part of their double-extortion strategy. The FBI observed actors collecting files from victims that included business-critical documents, databases, personally identifiable information (PII), and internal email communications [TA0009][T1114]. Gunra actors' custom support for filtering redundant system files during initial discovery/file system reconnaissance streamlines the actors' collection of user-specific data from local victim machines [T1005].

The FBI observed Gunra actors use a malicious executable (`main.exe`) to exfiltrate victim data from Microsoft OneDrive and SharePoint [T1530]. For at least one known Gunra victim, the actors generated compressed archives with sensitive data [T1560] and exfiltrated the archives to the file-sharing service Mega [T1567]; the volume of exfiltrated data ranged up to tens of terabytes.[10]

In addition to collecting business-critical documents, the KNPA identified a victim case in which Gunra actors connected to the VDI environments of IT personnel and collected sensitive documents containing system and network configuration information [T1005]. The actors then leveraged enterprise server credentials stolen from a system access control server to deploy ransomware to encrypt key assets, including database servers and network attached storage (NAS) systems [T1486].

The FBI observed several common open source tools on Gunra infrastructure that Gunra actors use to facilitate collection and exfiltration of data, including 7-Zip, RClone, and FileZilla [T1048] (see **Leveraged Tools** for a full list of tools used maliciously by Gunra actors).

Impact

Gunra's double-extortion model relies on both data exfiltration and data encryption for optimal success. The binary achieves high speed file encryption of entire file systems by leveraging a multi-threaded architecture that supports parallel encryption of multiple files simultaneously using strong ChaCha20 + RSA-4096 encryption [T1486]. Upon successful encryption of a file, the binary renames the encrypted file with the file extension `.ENCRT`. Gunra also used the `.CRYPT` file extension in one documented sample from July 2025.[11]

After the binary completes the encryption process for all files in a specific directory, Gunra actors write a static ransom note named `R3ADM3.txt` to the directory. To avoid unnecessary overhead, the binary also contains logic to prevent encryption of the ransom notes (`R3ADM3.txt`) and re-encryption of already encrypted files (`.ENCRT`).[12]

In their ransom notes, Gunra actors typically demand that victims initiate negotiation discussions within five to seven days via a Tor-based negotiation portal or qTox, or risk having their data leaked on Gunra's DLS. The FBI observed Gunra actors attempting to communicate directly with management staff at victim companies via email to solicit ransom payments with limited success. Gunra actors instructed victims to send ransom payments to specific cryptocurrency wallet addresses [T1657] and generally started negotiations at arbitrarily high ransom amounts (over tens of millions in US dollars).

If Gunra victims do not negotiate or pay ransom, the actors publicly disclose the victims on their DLS and offer a preview of victims' leaked data. This preview typically includes a directory listing of a victim's exposed OneDrive and SharePoint files, but not the content of the files. Between June and July of 2025, Gunra actors operated a clearnet mirror of their Tor-based DLS at domain `datapub.news`. By March 2026, Gunra had moved their original Tor-based DLS to a different `.onion` address. On Gunra's current Tor-based DLS, the actors advertise the sale of datasets from specific victims and instruct interested parties to contact them via qTox for more information.

To increase the likelihood of ransom payment and prevent system recovery [T1490], Gunra actors also used Windows Management Instrumentation (WMI) [T1047] to initiate deletion of volume shadow copies prior to encryption, as demonstrated in the following example [T1059.003]:[13]

```
cmd.exe /c C:\Windows\System32\wbem\WMIC.exe shadowcopy where "ID='{guid of shadowcopy}'" delete
```

Additionally, against one Gunra victim, Gunra actors deleted backup and archived data stored on backup infrastructure at both the primary data center and disaster recovery center before and after the ransomware deployment [T1490].

Leveraged Tools

Table 1 lists publicly available tools and applications used by Gunra ransomware actors. If network defenders identify use of these tools on their network, they should investigate further to determine possible malicious activity.

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 1. Tools Used by Gunra Ransomware Actors

Tool Name	Description
FileZilla	Open source, cross-platform File Transfer Protocol (FTP) application that supports file transfers between devices and remote servers.
Amass	Open source reconnaissance tool for network mapping and information gathering.
RClone	Open source command-line program designed to manage files in cloud storage.
Sliver	Penetration testing toolset that allows remote command and control of systems.
7-Zip	Open source, cross-platform file archiver utility.
WinRAR	Open source file archiver utility for Microsoft Windows.
DBeaver	Open source database management tool for managing Structured Query Language (SQL) databases like MySQL, MariaDB, PostgreSQL, SQLite, etc.
Slack	Cloud-based team communication and collaboration platform.
Microsoft Visual Studio Code	Open source extendable source code editor.
MobaXterm	Windows application with support for multiple remote computing protocols, including SSH, X11, RDP, virtual network computing (VNC), FTP, etc.
AnyDesk	Common, legitimate remote monitoring and management (RMM) tool that can be used by a cyber actor to obtain remote access and maintain persistence. AnyDesk also supports remote file transfer.
Google Remote Desktop	Web-based remote desktop software tool developed by Google that runs on a proprietary Google protocol.

Tool Name	Description
Mimikatz	Post-exploitation tool that allows users to access and exfiltrate authentication credentials from Windows systems.
Impacket	Suite of networking utilities, including `smbclient`, `psexec`, `secretsdump`, etc. Gunra utilized several tools from this suite.

Indicators of Compromise

Table 2 lists IP addresses and domains associated with Gunra ransomware infrastructure since early 2025.

Disclaimer: Observed IP addresses/domains may be historical in nature. The authoring agencies recommend organizations investigate or vet these IP addresses prior to taking action, such as blocking.

Table 2. IP Addresses/Domains

IP Address/Domain	First Seen	Last Seen
23.239.119[.]2	July 2025	Nov. 6, 2025
23.239.119[.]3	July 2025	Nov. 6, 2025
23.239.119[.]4	July 2025	Nov. 6, 2025
23.239.119[.]5	July 2025	Nov. 6, 2025
23.239.119[.]6	July 2025	Nov. 6, 2025
86.54.28[.]216	June 7, 2025	July 23, 2025
103.125.234[.]14	Nov. 2025	Dec. 2025
70.36.99[.]82	Nov. 2025	Dec. 2025
211.21.210[.]181	Nov. 2025	Dec. 2025
123.184.143[.]105	Nov. 2025	Dec. 2025
182.204.21[.]240	Nov. 2025	Dec. 2025
182.204.16[.]112	Nov. 2025	Dec. 2025
123.244.187[.]144	Nov. 2025	Dec. 2025

IP Address/Domain	First Seen	Last Seen
182.204.39[.]118	Nov. 2025	Dec. 2025
67.43.53[.]10	Nov. 2025	Dec. 2025
123.246.37[.]108	Nov. 2025	Dec. 2025
91.201.66[.]146	Nov. 2025	Dec. 2025
Datapub[.]news	June 2025	July 2025
gunrabxbig445sjqa535uaymzerj6fp4nwc6ngc2xughf2pedjdhk4ad[.]onion	Apr. 2025	Feb. 2026
lgiil72vkmdtbc3qv4tyq6wedyjxqr2qd4ze7xl2cxgerdnymxj7soqd[.]onion	Mar. 2026	July 2026
nsnhzysbntsqdwpys6mhml33muccsvterxewh5rkbmcab7bg2ttevjqd[.]onion	Jan. 2026	Jan. 2026

Table 3 lists email addresses associated with Gunra actors.

Table 3. Gunra Email Addresses

Email Address	Description
a00f105546345756@proton[.]me	Ransom negotiation
4569f6322bc3b22e9@proton[.]me	Ransom negotiation
ilovemycubscout@gmail[.]com	Ransom negotiation
6449a3c1e612168526@proton[.]me	Ransom negotiation

The following qTox IDs are associated with Gunra actors:

- 2507312EC10BB44ED9DAA04E3C5C27E8C13154649B1A02E73ACFAE1681EE0208D05133A8FB22
- 0FE87CED0C611AE97E049C64288557F49E8271E91399E849328B078DA789A573031783235BEF
- 47829AF1C943D4C296C910706923AS199BDA4995B076ED9A9016F7DEF161D445DF00F13E6900
- 9500B1A73716BCF40745086F7184A33EA0141B7D3F852431C8FDD2E1E8FAF9277E9FDC117B47

Table 4 lists malicious files associated with Gunra ransomware.

Table 4. Malicious Files (SHA256)

Filename	Hash (SHA256)	Description
main.exe	2dc70a12d158d437e45a55b1d52f3d61c6082a1e1667573302ba3b62813e2751	Tool to exfil OneDrive and SharePoint
main.exe	834efe9b392c6c000877ea5613a079445affc16fe8af5997d68c55cafc95e5d1	Tool to exfil OneDrive and SharePoint
cryptor.exe	91f8fc7a3290611e28a35a403fd815554d9d856006cc2ee91ccdb64057ae53b0	Malicious executable
msmp.exe	a82e496b7b5279cb6b93393ec167dd3f50aff1557366784b25f9e51cb23689d9	Malicious executable

Table 5 lists malicious accounts created by Gunra actors to gain initial access to victim Fortinet devices.

Table 5. Malicious Fortinet User Accounts

Username	Details
forticloud-sync	CVE-2024-55591 and CVE-2025-24472 allow threat actors to exploit scheduled tasks on vulnerable FortiOS firewall devices to create a new, malicious persistent user forticloud-sync with super user privileges and a hard-coded password.

MITRE ATT&CK Tactics and Techniques

See Table 6 to Table 18 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 6. Initial Access

Technique Title	ID	Use
Exploit Public-Facing Application	T1190	Gunra actors exploited vulnerabilities in FortiGate firewall and SSL-VPN appliances to gain initial access to victim networks.

Table 7. Execution

Technique Title	ID	Use
Windows Management Instrumentation	T1047	The Gunra ransomware binary contained specific WMI commands to delete volume shadow copies on victim machines.
Native API	T1106	The Gunra ransomware binary utilized Native APIs (`FindFirstFileW`, `FindNextFileW`) for file system discovery.
Command and Scripting Interpreter: Windows Command Shell	T1059.003	Gunra actors executed commands via `cmd.exe` on Windows to initiate the WMI command.

Table 8. Persistence

Technique Title	ID	Use
Account Manipulation	T1098	Gunra actors gained access to an unused account for a victim network. They altered the account configuration to bypass the mandatory password change requirement, which allowed them to use the compromised account for subsequent malicious activities.
External Remote Services	T1133	Gunra actors used external-facing remote services in combination with an administrator account to gain access.

Table 9. Privilege Escalation

Technique Title	ID	Use
Valid Accounts: Default Accounts	T1078.001	Gunra actors compromised an SSL-VPN appliance by exploiting default credentials and the absence of account lockout controls to obtain administrator access to the victim network device.
Valid Accounts: Domain Accounts	T1078.002	Gunra actors gained access to an administrator account for an SSL appliance.

Table 10. Stealth

Technique Title	ID	Use
Debugger Evasion	T1622	The Gunra ransomware Windows encryptor binary contained the `IsDebuggerPresent` API to defend against reverse engineering and debugging activity.

Technique Title	ID	Use
Indicator Removal: Clear Command History	T1070.003	Gunra actors cleared command history files on victim machines to prevent detection of their malicious activity.
Delay Execution	T1678	Gunra actors strategically timed their reconnaissance and malicious network activities to late night or early morning to avoid detection by the victim.
Selective Exclusion	T1679	The Gunra ransomware binary programmatically excludes certain directories and filetypes from encryption to ensure system critical files continue to function and that ransom notes are readable. In addition, the binary contains logic to prevent re-encryption of already Gunra-encrypted files.

Table 11. Defense Impairment

Technique Title	ID	Use
Disable or Modify Tools	T1685	Gunra actors cleared system/network logs on victim machines to prevent detection of their malicious activity.

Table 12. Credential Access

Technique Title	ID	Use
OS Credential Dumping: NTDS	T1003.003	Gunra actors used `secretsdump.py` on multiple victim domain controllers to extract password hashes for user accounts from the NTDS files.
Network Sniffing	T1040	Gunra actors abused SSL-VPN network traffic controls to capture users' VDI login credentials and session information in transit, effectively sniffing authentication traffic for a victim network.
Steal Web Session Cookie	T1539	Gunra actors captured legitimate VDI session data for a victim, which allowed them to steal and reuse session cookies to hijack active sessions and impersonate legitimate users on the internal victim network.
Credentials from Password Stores	T1555	From a compromised virtual desktop, Gunra actors accessed the Hiware access control server for a victim and stole its symmetric encryption key.

Technique Title	ID	Use
OS Credential Dumping	T1003	Gunra actors used a stolen symmetric encryption key from a Hiware system access control server to decrypt and dump stored enterprise server passwords.
Modify Authentication Process: Multi-Factor Authentication	T1556.006	Gunra actors altered files in a victim's VDI authentication server portal so that a specific attacker-chosen OTP always succeeded, creating a persistent backdoor that bypassed MFA.

Table 13. Discovery

Technique Title	ID	Use
File and Directory Discovery	T1083	The Gunra ransomware binary contains custom instructions to enumerate the complete directory structure of victim machines to identify user-data files and directories for encryption.
System Network Connections Discovery	T1049	Gunra actors enumerated active system network connections to map reachable internal infrastructure prior to ransomware deployment.

Table 14. Lateral Movement

Technique Title	ID	Use
Remote Services: Remote Desktop Protocol	T1021.001	Gunra actors used stolen VDI session information to access a victim's internal VDI environment, then moved laterally via RDP to access the victim's VDI authentication web server, internal AD server, and IT staff virtual desktops.
Remote Services: SMB/Windows Admin Shares	T1021.002	Gunra actors used SMB administrative shares with valid credentials to move laterally and deploy tools across compromised systems.
Use Alternate Authentication Material: Pass the Hash	T1550.002	Gunra actors used pass-the-hash methods to move laterally to privileged systems.
Use Alternate Authentication Material: Pass the Ticket	T1550.003	Gunra actors used pass-the-ticket methods to move laterally to privileged systems.

Table 15. Collection

Technique Title	ID	Use
Collection	TA0009	Gunra actors were observed collecting business-critical documents, databases, PII, and internal email communications.
Archive Collected Data	T1560	Gunra actors were observed utilizing tools such as 7-Zip, WinRAR, RClone, and others to copy and archive victim data for exfiltration.
Data from Cloud Storage	T1530	Gunra actors launched a malicious application (`main.exe`) that specifically targeted Microsoft Cloud Services (OneDrive and SharePoint) for data exfiltration.
Data from Local System	T1005	The Gunra ransomware binary recursed through the full directory structure of a compromised device to identify user-data files and directories for targeted exfiltration and subsequent encryption. In one instance, Gunra actors were observed collecting system and network configuration network information by connecting to the VDI environments of IT personnel.
Email Collection	T1114	Gunra actors collected internal email communications.

Table 16. Command and Control

Technique Title	ID	Use
Ingress Tool Transfer	T1105	After obtaining admin access to a victim's SSL-VPN appliance, Gunra actors downloaded an SSH tunneling tool from an external server to create and maintain persistent tunnel connections to compromised systems in the victim's network.
Protocol Tunneling	T1572	Gunra actors used an SSH tunneling tool to establish connections and maintain persistence between compromised systems.

Table 17. Exfiltration

Technique Title	ID	Use
Exfiltration Over Web Service	T1567	Gunra actors were observed archiving victim data and exfiltrating it over the file-sharing service Mega.
Exfiltration Over Alternative Protocol	T1048	Gunra actors used Filezilla software to exfiltrate data over FTP.

Table 18. Impact

Technique Title	ID	Use
Data Encrypted for Impact	T1486	Gunra actors encrypt victim data using combined ChaCha20 + RSA-4096 algorithms to prevent victim access to critical business files. Gunra encryptors are available for Windows and Linux, increasing the potential attack surface within a victim network. In one instance, Gunra actors encrypted key assets that included database servers and NAS systems.
Financial Theft	T1657	Under the double-extortion model, Gunra actors demand ransom payment through a ransom note (`R34DM3.txt`) in cryptocurrency. The note instructs victims to make the payment to prevent public leaks of their sensitive business data and acquire decryption keys to unlock encrypted files on compromised systems.
Inhibit System Recovery	T1490	To augment encryption of critical data on victim networks and prevent system recovery, Gunra actors disable backup features, such as volume shadow copies. In one instance, Gunra actors prevented restoration from backups by deleting backup and archived data stored at the primary data center and disaster recovery center.

Incident Response

If a potential compromise is detected, but ransomware actors have not (yet) encrypted items, organizations should take the following actions:

1. **Determine which hosts were compromised and isolate them** by quarantining or taking them offline.
    a. **If the incident involves a Gunra Linux variant, preserve encrypted files, file timestamps, ransom notes, and relevant system logs.**
        i. As of March 2026, researchers identified a weakness in the Gunra ransomware's Linux Executable and Linkable Format (ELF) variants (appended with `.GNRA`); the encryption keys use a weak pseudorandom number generator (PRNG) seeded with the predictable system `srand(time(NULL))`.[14] Defenders may leverage this to mathematically reconstruct the keys using file timestamps and recover files without paying the ransom.
2. **Initiate threat hunting activities to scope the intrusion.** Collect and review relevant artifacts, logs, and other data to identify threat actor TTPs, compromised devices and accounts, a timeline of activity, etc. Responders should consider:
    a. Reviewing logs of network appliances (e.g., edge devices) to audit actions associated with privileged users to identify anomalous activity.
    b. Collecting copies of ransom notes to identify current threat actor communication platforms.

c. Auditing the creation of new files (particularly archives) to determine possible pre- or post-exfiltration activity.

3. **Report the compromise** to the FBI and other agencies as appropriate (see **Reporting** for contact information).
4. **Apply eviction countermeasures**, including those listed below, to contain the incident and eradicate the threat actor from the network (**Note:** Start applying countermeasures after collecting enough threat hunting data to inform effective countermeasure selection; this will likely overlap with threat hunting activities).
   a. Identify and disable malicious, actor-controlled accounts.
   b. Identify and secure legitimate, privileged accounts.
   c. Use CISA's Eviction Strategies Tool to assemble countermeasures for a systematic eviction plan—the tool comprises **Playbook-NG** (a web application) and **COUN7ER** (a database of post-compromise countermeasures mapped to adversary TTPs).
      i. Use Playbook-NG and COUN7ER together to assemble a systematic eviction plan, or playbook, that leverages distinct countermeasures to contain and evict cyber threat actors. The playbook features a list of recommended response actions based on threat actor TTPs and includes each action's intended outcome, preparatory steps, and associated risks. For more information, see CISA's Eviction Strategies Tool Fact Sheet.
5. **Harden the network to prevent additional malicious activity** (see **Mitigations** for guidance).

If compromise is detected and items have been encrypted, see the "Ransomware and Data Extortion Response Checklist" in CISA's joint #StopRansomware Guide.

Mitigations

The authoring agencies recommend organizations implement the mitigations below to improve your organization's cybersecurity posture on the basis of Gunra actor 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.

- **Prioritize patching known exploited vulnerabilities** [CPG 2.B] **and the CVEs in this advisory** in internet-facing systems—including VPN gateways and RDP-exposed infrastructure—and keep all OSs, software, and firmware up to date to support this.
- **Implement a recovery plan** 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 3.I, 3.O, 1.C].
- **Review domain controllers, servers, workstations, and active directories** for new and/or unrecognized accounts [CPG 2.A, 2.E].

- **Audit user accounts with administrative privileges and configure access controls** according to the principle of least privilege [CPG 3.G].
- **Segment networks** [CPG 3.I] 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.
- **Require MFA** for all services to the extent possible, particularly for webmail, VPNs, and accounts that access critical systems [CPG 3.F].
- **Disable command-line and scripting activities and permissions.** Privilege escalation and lateral movement often depend on software utilities running from the command line. If threat actors are not able to run these tools, they will have difficulty escalating privileges and/or moving laterally [CPG 3.G, 3.M].

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 6** to **Table 18**).
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.
- #StopRansomware Guide: Resource to mitigate a ransomware attack.
- Cyber Hygiene Services, Ransomware Readiness Assessment: CISA's no-cost cyber hygiene services.
- USSS's Preparing for a Cyber Incident: Outlines basic steps an organization can take before, during, and after a cyber incident.

Reporting

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

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

South Korean organizations: Report cybersecurity incidents to KNPA via the online cybercrime reporting system or by calling 112.

Disclaimer

The information in this report is being provided "as is" for informational purposes only. CISA and co-sealers 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 CISA and co-sealers.

Version History

August 10, 2026: Initial version.

Notes

[1] For information on historical Conti ransomware activity, see CISA and FBI's Conti Ransomware advisory.

[2] Breakglass Intelligence, "Gunra Ransomware's Linux Variant Has a Fatal Flaw: time()-Seeded rand() Makes Encrypted Files Recoverable Without Paying," Breakglass Intelligence, March 12, 2026, https://intel.breakglass.tech/post/gunra-ransomware-s-linux-variant-has-a-fatal-flaw-time-seeded-rand-makes-encrypted-files-recoverable-without-paying; Jeffrey Francis Bonaobra, Melvin Singwa, Emmanuel Panopio "Gunra Ransomware Group Unveils Efficient Linux Variant," Trend Micro, July 29, 2025, https://www.trendmicro.com/en_us/research/25/g/gunra-ransomware-linux-variant.html; and CYFIRMA, "Gunra Ransomware – A Brief Analysis," CYFIRMA, May 3, 2025, https://www.cyfirma.com/research/gunra-ransomware-a-brief-analysis/.

[3] CloudSEK, "Inside Gunra RaaS: From Affiliate Recruitment on the Dark Web to Full Technical Dissection of their Locker," CloudSEK, February 11, 2026, https://www.cloudsek.com/blog/inside-gunra-raas-from-affiliate-recruitment-on-the-dark-web-to-full-technical-dissection-of-their-locker.

[4] CYFIRMA, "Gunra Ransomware – A Brief Analysis"; and Breakglass Intelligence, "Gunra Ransomware's Linux Variant Has a Fatal Flaw."

[5] Bonaobra, "Gunra Ransomware Group Unveils Efficient Linux Variant"; and CloudSEK, "Inside Gunra RaaS."

[6] CloudSEK, "Inside Gunra RaaS."

[7] CYFIRMA, "Gunra Ransomware – A Brief Analysis."

[8] CloudSEK, "Inside Gunra RaaS."

[9] CloudSEK, "Inside Gunra RaaS."

[10] Bonaobra, "Gunra Ransomware Group Unveils Efficient Linux Variant."

[11] VirusTotal, "VirusTotal - File - 91f8fc7a3290611e28a35a403fd815554d9d856006cc2ee91ccdb64057ae53b0," *VirusTotal*, https://www.virustotal.com/gui/file/91f8fc7a3290611e28a35a403fd815554d9d856006cc2ee91ccdb64057ae53b0/details.

[12] CloudSEK, "Inside Gunra RaaS."

[13] CYFIRMA, "Gunra Ransomware – A Brief Analysis."

[14] Breakglass Intelligence, "Gunra Ransomware's Linux Variant Has a Fatal Flaw."