THREAT ACTOR PROFILE: GUNRA

Ransomware-as-a-Service (RaaS) Group

Threat Actor	Gunra
Also Known As	Gunra Ransomware
Type	Ransomware-as-a-Service (RaaS)
Active Since	April 2025
Motivation	Financial Gain — Double extortion (data theft + encryption), ransom demands
Risk Level	**HIGH**

2 March 2026 | Version 1.0 | NyxLab Threat Intelligence

1. Threat Actor History & Background

Gunra is a ransomware operation that first emerged in April 2025, with the earliest known sample compiled on April 10, 2025. The group's Data Leak Site (DLS) appeared on the Tor network shortly after, with the first victim posted on April 23, 2025. Gunra operates a double-extortion model — exfiltrating victim data before encrypting systems, then threatening public disclosure on their DLS if ransom demands are not met. The group typically issues a 5-day ultimatum for victims to begin negotiations.

Gunra's ransomware is built upon the leaked Conti v2 source code, which was publicly released in February 2022 by a Ukrainian researcher protesting the Conti group's pro-Russian stance during the Russia-Ukraine conflict. While Gunra reuses Conti's codebase as a foundation, the group has no confirmed organisational ties to the defunct Conti operation. This is evidenced by inherited artifacts such as the ransom note filename 'R3ADM3.txt' and the log file 'CONTI_LOG.txt', both carried over from the original Conti code. Initial samples also showed code overlaps with the Akira ransomware family, though newer Gunra builds from mid-2025 onward contain independently developed code not directly copied from other known variants.

In January 2026, Gunra launched a formal Ransomware-as-a-Service (RaaS) affiliate program on the RAMP dark web forum. CloudSEK researchers infiltrated the program via HUMINT operations and published a full technical dissection of the locker in January 2026. The RaaS program provides affiliates with cross-platform ransomware builders (Windows, Linux, ESXi, and NAS), a management panel for generating customised lockers, and detailed operator documentation. This lowered the barrier to entry and signalled an intent to scale operations.

Gunra's infrastructure has evolved significantly over its operational lifespan. The negotiation portal has undergone three major iterations: an initial WhatsApp-themed interface (April–May 2025), a dedicated client login portal with ReCaptcha protection (May–June 2025), and a WordPress-based real-time chat system using the Heartbeat API (late 2025 onward). The group briefly operated a clearnet DLS at datapub[.]news (registered June 7, 2025) before it was taken offline. Handler roles within the negotiation infrastructure include colour-coded designations such as 'Manager', 'redManager', 'BLACK MANAGER', and 'WHITE HANDLER', suggesting a team-based operation with specialised roles.

As of February 2026, Gunra has claimed more than 20 victims across Latin America, Asia, Europe, and the Middle East. Ransom demands have ranged from tens of thousands to $20 million, with documented negotiations showing significant reductions (e.g., a $20M demand reduced to $70K for one Colombian victim).

2. Victimology

Gunra targets a diverse range of sectors and geographies, consistent with an opportunistic, financially motivated ransomware operation rather than a state-directed campaign. The group's more than 20 confirmed victims span manufacturing, healthcare, business services, retail, technology, finance, education, and government sectors.

Based on public DLS postings, Gunra's geographic focus has primarily centred on Latin America and Asia, with additional activity observed across Europe, the Middle East, and North America.

The group does not appear to have a preferred sector. This sector diversity is consistent with opportunistic targeting, likely driven by accessible initial footholds (stolen credentials, successful phishing) rather than strategic sector focus.

Ransom demands vary considerably, from tens of thousands to $20 million, suggesting the group adjusts demands based on perceived victim revenue. Data exfiltration volumes have reached up to 13.2 TB in a single incident (SGI Seoul Guarantee Insurance). The following timeline summarises confirmed victims based on the group's DLS postings.

Date	Campaign / Target	Details
Feb 27, 2026	**Neo Derm Group Ltd.**	Based in Hong Kong. Data posted to Gunra DLS.
Dec 29, 2025	**INHA University**	Education sector, South Korea. 14-hour homepage disruption, personal information leak confirmed. University filed criminal complaint with National Police Agency Cyber Terror Investigation Unit. Data posted to Gunra DLS.
Oct 01, 2025	**miraense.com**	Business services sector, Brazil. Corporate data exfiltrated and posted to Gunra DLS after failed ransom negotiations.
Sep 10, 2025	**Hwacheon**	Manufacturing sector, South Korea. Industrial machinery manufacturer. 265 GB of data exfiltrated and posted to Gunra DLS.
Sep 03, 2025	**Samwha Capacitor Group**	Technology / semiconductor manufacturing sector, South Korea. Corporate and manufacturing data compromised.
Aug 18, 2025	**Justicia Penal Militar**	Government sector, Colombia. Sensitive government data exfiltrated. Ransom demand reportedly reduced from $20M to $70K during negotiations.
Aug 18, 2025	**SEGUROS AMÉRICA**	Insurance agents, brokers and services sector, Nicaragua. Insurance and client data compromised.
Aug 18, 2025	**Seoul Guarantee Insurance**	Finance sector, Vietnam. S2W reported 13.2 TB of data exfiltrated (‘pure compressed Oracle database’). Multi-day operational shutdown, with handwritten guarantee certificates issued for urgent cases.
Jun 06, 2025	**ACCS Le Groupe**	Business services / IT solutions sector, Canada. Corporate data exfiltrated and posted to DLS.

Jun 05, 2025	**American Hospital Dubai**	Healthcare sector, United Arab Emirates. Gunra claimed 450 million patient records (~4 TB uncompressed) from Cerner Millennium database (Oracle Health EHR). VMware vSphere infrastructure and EMC Unity storage compromised. 3-day deadline issued.
May 26, 2025	**Olho D'Agua**	Food and kindred products / retail sector, Brazil. Corporate data exfiltrated.
May 24, 2025	**Anjos Ramos**	Business services / legal sector, Brazil. Legal firm data compromised.
May 22, 2025	**Adria Grupa**	Business services sector, Croatia. Corporate data exfiltrated and posted to DLS.
May 17, 2025	**MG Chemicals**	Chemicals and allied products / manufacturing sector, Canada. Industrial and corporate data compromised.
May 12, 2025	**Grupo Jorge Batista**	Retail sector, Brazil. Corporate data exfiltrated.
May 04, 2025	**Tomoku**	Retail sector, Japan. Corporate data compromised and posted to DLS.
Apr 28, 2025	**Bioprofarma Bagó**	Retail / pharmaceutical sector, Argentina. Corporate data exfiltrated.
Apr 27, 2025	**KLINGER ITALY**	Manufacturing sector (level gauge/valve manufacturer), Italy. Breach data contained a ConnectWise remote access tool (Net-Admin-Supporto-Remoto-ClientSetup.exe) with 42 AV detections, suggesting pre-existing compromise or planted malware.
Apr 23, 2025	**Varela Hermanos**	Retail sector, Panama. Among the earliest Gunra victims, posted shortly after DLS launch.
Apr 23, 2025	**Dar Al Teb**	Healthcare sector, Egypt. Medical and patient data compromised.
Apr 23, 2025	**Shinko Shoji**	Technology sector, Japan. Among the first victims posted to the Gunra DLS upon its launch.

3. Associations & Affiliations

Leaked Conti v2 Source Code — *Code Lineage (NOT Organisational)*

Gunra's ransomware is built on the publicly leaked Conti v2 source code, released in February 2022 by a Ukrainian researcher. This is a code lineage relationship, not an organisational affiliation — the Conti group itself dissolved in mid-2022, and the leaked source has since been adopted by numerous unrelated operations. Inherited artifacts include the ransom note filename 'R3ADM3.txt', the log file 'CONTI_LOG.txt', and identical WMI queries for shadow copy deletion. Initial Gunra samples also exhibited code overlaps with the Akira ransomware family, though newer builds from mid-2025 onward contain independently developed code. Several other active ransomware families (Black Basta, Royal/BlackSuit, Akira) similarly derive from the same leaked codebase, representing parallel evolution rather than coordinated operations.

RAMP Dark Web Forum — *RaaS Affiliate Recruitment Platform*

In January 2026, Gunra launched a formal Ransomware-as-a-Service (RaaS) affiliate program on the RAMP dark web forum, a well-known cybercriminal marketplace for ransomware operator recruitment. The programme provides affiliates with cross-platform ransomware builders supporting Windows, Linux, ESXi, and NAS environments across x86 and ARM architectures. A management panel enables immediate locker generation, and a PDF operator guide documents the programme structure. Communication with prospective affiliates is conducted via Tox. CloudSEK researchers successfully infiltrated the programme in January 2026 and published a technical dissection of the locker obtained from the panel.

DONOT Loader & Lumma Stealer — *Attack Chain Tooling*

Gunra's attack chain incorporates the DONOT Loader, an embedded loader stub within the ransomware binary responsible for payload decryption and execution through obfuscated API resolution and XOR-based decoding routines. The group also utilises Lumma Stealer for data exfiltration during the pre-encryption phase. For data staging and exfiltration, Gunra employs FTP servers, AWS S3 buckets, SFTP servers, and the Bash Upload service (bashupload[.]com). Group-IB obtained AWS S3 credentials used by the group during Tox negotiations, confirming this cloud-based exfiltration approach.

ChaCha20+RSA Encryption Family — *Shared Encryption Architecture*

Gunra uses a ChaCha20 stream cipher combined with RSA-4096 public key encryption — a hybrid encryption architecture shared by multiple modern ransomware families including Black Basta, Rhysida, Akira, Qilin/Agenda, Royal/BlackSuit, and DoNex/DarkRace. This convergence reflects industry-wide adoption of a proven encryption design rather than coordination between groups. Gunra's Windows variant uses BCryptGenRandom for secure key generation, while the Linux variant has a critical implementation flaw using time()-seeded rand(), making encrypted data recoverable via brute-force of only 256 byte values.

4. Tactics, Techniques & Procedures (TTPs)

Gunra employs a multi-stage attack chain centred on initial access via spear-phishing or stolen credentials, followed by data exfiltration and system-wide encryption. The ransomware incorporates an embedded DONOT Loader stub for payload delivery, uses ChaCha20+RSA-4096 hybrid encryption, and systematically deletes Volume Shadow Copies to inhibit recovery. The group operates a double-extortion model with a Tor-based Data Leak Site and negotiation infrastructure. Gunra's initial access techniques deserve particular attention — they heavily rely on Microsoft-themed phishing emails and credentials obtained from initial access brokers or infostealer logs (victims may have had prior infostealer compromises). This section covers both the MITRE ATT&CK; mapping and analysis of their recent operational tradecraft.

Recent Attack Analysis

Initial Access — Leaked Credentials & VPN Compromise

A significant initial access vector for Gunra involves the use of leaked or stolen credentials to authenticate directly into victims' VPN infrastructure. These credentials are typically sourced from infostealer logs or purchased from initial access brokers (IABs) on dark web forums.

Alpha Hunt reported that 25% of Gunra victims had domain credentials previously compromised by infostealers, indicating the group actively leverages pre-existing credential exposure to gain initial footholds. VPN access provides attackers with direct, authenticated entry into internal networks, bypassing perimeter defences entirely.

Once inside via VPN, the group deploys a custom lateral movement tool and uses WMI for network propagation, PsExec for remote execution, and SMB shares for ransomware staging across servers.

Initial Access — Spear-Phishing Campaigns

Gunra's second primary initial access vector is spear-phishing emails impersonating Microsoft security notifications. Documented phishing emails use subject lines such as 'Microsoft account security info verification'. Malicious attachments delivered through these emails trigger the embedded DONOT Loader within the Gunra binary.

Once inside, the group follows the same post-compromise playbook — deploying a custom lateral movement tool, using WMI for network propagation, PsExec for remote execution, and SMB shares for ransomware staging across servers.

Double Extortion via Tor DLS & Negotiation Infrastructure

Gunra operates a structured double-extortion programme with dedicated Tor infrastructure for both public shaming and private negotiation.

(1) Data Leak Site (DLS): The primary DLS at gunrabxbig445sjqa535uaymzerj6fp4nwc6ngc2xughf2pedjdhk4ad[.]onion publishes victim data with searchable industry verticals.

(2) Negotiation Portals: Victims receive a Client ID and Password in the R3ADM3.txt ransom note to access Tor-based chat portals. The infrastructure has evolved through three iterations — WhatsApp-themed (April–May 2025), ReCaptcha-protected client login (May–June 2025), and WordPress-based real-time chat with Heartbeat API (late 2025).

(3) Exfiltration Infrastructure: Data is staged via FTP servers, AWS S3 buckets, SFTP, and the Bash Upload service before being published on the DLS.

MITRE ATT&CK: Mapping

Initial Access

ID	Technique	Context
T1566.001	Spearphishing Attachment	Microsoft-themed phishing emails with subject 'Microsoft account security info verification' delivering malicious attachments
T1078	Valid Accounts	Stolen credentials purchased from initial access brokers; victims may have had prior infostealer compromises a common pattern in ransomware operations

Execution

ID	Technique	Context
T1204	User Execution	Victim executes malicious attachment from phishing email, triggering embedded DONOT Loader within the Gunra binary
T1047	Windows Management Instrumentation	WMI used for shadow copy enumeration (SELECT * FROM Win32_ShadowCopy) and deletion, as well as network propagation
T1129	Shared Modules	Dynamic shared module loading for runtime payload execution and API resolution

Persistence

ID	Technique	Context
T1176	Software Extensions	Software extension abuse for persistent access and session monitoring
T1542.003	Bootkit	Pre-OS boot persistence mechanisms to survive system reinstalls
T1574.002	DLL Side-Loading	DLL side-loading for maintaining persistent access via legitimate binary hijacking

Privilege Escalation

ID	Technique	Context
T1548	Abuse Elevation Control Mechanism	Elevation of privilege through control mechanism abuse
T1055	Process Injection	Code injection into running processes for privilege escalation and defence evasion

Defense Evasion

ID	Technique	Context
T1027	Obfuscated Files or Information	XOR and Base64 encoding for string obfuscation; all strings encrypted at rest and decrypted at runtime; dynamic API resolution prevents static analysis

T1027.002	Software Packing	Packed executables with LTCG (Link-Time Code Generation) optimisation to evade signature-based detection
T1014	Rootkit	Rootkit techniques for deep system concealment and persistence
T1036	Masquerading	Process and file name masquerading to blend with legitimate system activity
T1564.001	Hidden Files and Directories	Hidden file and directory operations to conceal malicious artifacts
T1574	Hijack Execution Flow	Execution flow manipulation through DLL side-loading and hijacking

Credential Access

ID	Technique	Context
T1555	Credentials from Password Stores	Harvesting credentials from browser password stores and system keychains
T1555.003	Credentials from Web Browsers	Extraction of saved credentials from web browsers via Lumma Stealer
T1539	Steal Web Session Cookie	Web session cookie theft for authenticated access to victim web services
T1552.001	Credentials In Files	Searching for credentials stored in configuration files, scripts, and documents

Discovery

ID	Technique	Context
T1082	System Information Discovery	System enumeration via GetNativeSystemInfo API to determine CPU core count for threading optimisation; WMI queries for system profiling
T1057	Process Discovery	Running process enumeration via GetCurrentProcess; IsDebuggerPresent for anti-analysis checks
T1083	File and Directory Discovery	Recursive file system scanning across drives A-Z using FindFirstFileW/FindNextFileW/FindFirstFileExW/FindNextFileExW APIs
T1518	Software Discovery	Enumeration of installed software and security tools to identify defensive controls

Collection

ID	Technique	Context
T1119	Automated Collection	Automated data collection routines targeting documents, databases, images, and archives prior to encryption
T1005	Data from Local System	Systematic collection of corporate data, patient records, financial databases, and personal information from local systems
T1185	Browser Session Hijacking	Active browser session hijacking for access to authenticated web applications and cloud services

Command and Control		
ID	**Technique**	**Context**
`T1090`	**Proxy**	Tor-based communication channels for DLS operations and victim negotiation portals
`T1071`	**Application Layer Protocol**	HTTP/HTTPS-based C2 communication; WordPress Heartbeat API used in latest negotiation portal for real-time messaging

Exfiltration		
ID	**Technique**	**Context**
`T1048`	**Exfiltration Over Alternative Protocol**	Data exfiltrated via FTP servers, AWS S3 buckets, SFTP servers, and the Bash Upload service (bashupload[.]com)

Impact		
ID	**Technique**	**Context**
`T1486`	**Data Encrypted for Impact**	ChaCha20 (20-round) + RSA-4096 hybrid encryption; per-file unique 32-byte key + 12-byte nonce via BCryptGenRandom; 1 MB chunk processing; files renamed with .ENCRT extension
`T1490`	**Inhibit System Recovery**	Volume Shadow Copy deletion via WMIC — 60+ shadow copies targeted using 'wmic.exe shadowcopy where ID={GUID} delete'; identical WMI query pattern to Conti, LockBit 4.0, and VanHelsing
`T1496`	**Resource Hijacking**	Multi-threaded encryption consuming system resources; thread pool matches CPU logical core count ×2 via GetNativeSystemInfo; ~52 MB/s encryption throughput

5. Indicators of Compromise (IoCs)

Key Identified Malware Hashes (by Family)

Gunra Ransomware — Primary Windows Samples (SHA-256)

```
854e5f77f788bbbe6e224195e115c749172cd12302afca370d4f9e3d53d005fd
a82e496b7b5279cb6b93393ec167dd3f50aff1557366784b25f9e51cb23689d9
6d25d5c988a8cda3837dff5f294cbc25c97aea48dde1a74cba71a2439cab0a11
5530363373dfe8fa474c9394184d2c56a0682c6a178d6f1c3536a1a3796dff42
91f8fc7a3290611e28a35a403fd815554d9d856006cc2ee91ccdb64057ae53b0
944a1a411abb97f9ae547099c4834beb49de0745740ba450efb747bd62d8d83b
76f13279f2ea05c8895394f57b71716847857d2beac269272375ce8a71c80e40
```

Gunra RaaS Locker & Operator Guide (SHA-256)

```
75e5621756e9d19efeac2bcbb2ac4711fb85243c03b0a19c05b18e31a780691e (RaaS Locker Sample)
25c8cb27947042de89d634b3e260e614e5b1425a89494fa4e4295bcabfa8ee48 (Operator Guide PDF)
```

Gunra Ransomware — Linux Variant (SHA-256)

```
22c47ec98718ab243f2f474170366a1780368e084d1bf6adcd60450a9289e4be (ELF64, compiled Jul 16, 2025)
```

Gunra Lateral Movement Tool (SHA-256)

```
6d59bb6a9874b9b03ce6ab998def5b93f68dadedccad9b14433840c2c5c3a34e
```

Tor Infrastructure & Communication Channels

gunrabxbig445sjqa535uaymzerj6fp4nwc6ngc2xughf2pedjdhk4ad[.]onion (Primary DLS)	nsnhzysbntsqdwpys6mhml33muccsvterxewh5rkbmcab7bg2ttevjqd[.]onion
apdk7hpbbquomgoxbhutegxco6btrz2ara3x2weqnx65tt45ba3sclyd[.]onion	2bw7r32r5eshwk2h7uekj3lwzorxds2jyhyzqyilphid3r27x5hsf4yd[.]onion (Backend)
jzbhtsuwysslrzi2n5is3gmzsyh6ayhm7jt3xowldhk7rej4dqqubxqd[.]onion (Negotiation v2)	r3tkfu3h7sx4k6n7mr7ranuk5godwz7vlgvv2dk2fs2cbma5nailigad[.]onion (Backend API)
a00f105546345756@proton[.]me (Contact Email)	6449a3c1e612168526@proton[.]me (Contact Email)
ilovemycubscout@gmail[.]com (Registration Email)	

Infrastructure IP Addresses

86.54.28[.]216			

Additional Indicators (Tox ID, Mutex, File Artifacts)

Tox ID: 2507312EC10BB44ED9DAA04E3C5C27E8C13154649B1A02E73ACFAE1681EE0208D05133A8FB22

Mutex: kjsidugiaadf99439

Mutex: 34adfwefadf99439

Ransom Note: R3ADM3.txt

Log File: CONTI_LOG.txt

Encrypted Extension: .ENCRT

Process Name: gunraransome.exe

PDB Path: D:\wrk\tool\encrypter\x64\Debug\encrypter.pdb

Keystore Pattern: {sha256_hash}.keystore

AWS Access Key ID: AKIAXZQFPG6GBV2HKMRD

Additional File Hashes (SHA-256)

6d59bb6a9874b9b03ce6ab998def5b93f68dadedccad9b14433840c2c5c3a34e (Lateral Movement Tool)
22c47ec98718ab243f2f474170366a1780368e084d1bf6adcd60450a9289e4be (Linux ELF Variant)
75e5621756e9d19efeac2bcbb2ac4711fb85243c03b0a19c05b18e31a780691e (RaaS Locker)
25c8cb27947042de89d634b3e260e614e5b1425a89494fa4e4295bcabfa8ee48 (Operator Guide PDF)

Additional File Hashes (MD5)

9a7c0adedc4c68760e49274700218507
0339269cef32f7af77ce9700ce7bf2e2
3178501218c7edaef82b73ae83cb4d91
7dd26568049fac1b87f676ecfaac9ba0
92e11df03725e29d963d44508d41a8dd
94b68826818ffe8ceb88884d644ad4fc
acecebd48355f14caf26fcd6ce7b5dcd
1aa9a959ff49196580b0f00e0620eb80
969e45903c37717bd40a2fdeee6a4f2a
8d5a8c443e728f693c5c13f8b5453e20
ae6f61c0fc092233abf666643d88d0f3
f6664f4e77b7bcc59772cd359fdf271c
4c0e74e9f94dff611226cd1619cb1e1d
e57b130718373f6ba9b37f39ca1d7e3d

6. NyxLab Recommendations

Gunra represents an active and escalating ransomware threat that has compromised more than 20 organisations across four continents since April 2025. The group's transition to a formal RaaS affiliate programme in January 2026 signals intent to scale operations significantly. Their double-extortion model demonstrates both capability and willingness to inflict maximum operational and reputational damage on victims.

Based on available intelligence, Gunra's initial access techniques are likely to involve: (1) leaked or stolen credentials used to access VPN infrastructure, often sourced from infostealer logs or initial access broker marketplaces; (2) spear-phishing emails impersonating Microsoft security notifications; and (3) exploitation of unpatched internet-facing applications. The prevalence of stolen credentials as an access vector — with 25% of victims having prior infostealer compromises — underscores the critical importance of credential hygiene, dark web monitoring, and VPN hardening. Once inside a network, the group moves quickly — deploying a custom lateral movement tool, exfiltrating data via FTP/S3/SFTP infrastructure, deleting Volume Shadow Copies via WMIC, and encrypting systems.

Based on these findings, NyxLab recommends the following actions to detect, hunt for, and mitigate Gunra-specific threats.

1. Patch & Harden External-Facing Services

Reduce the external attack surface by ensuring all internet-facing infrastructure is patched, hardened, and minimised.

- **VPN & Remote Access:** Ensure VPN appliances and remote access gateways are fully patched against known vulnerabilities. Disable split tunnelling where possible and enforce device compliance checks before granting VPN access. Restrict VPN access to only necessary users and services.
- **Edge Infrastructure:** Patch firewalls, routers, VPN concentrators, and file transfer appliances promptly. These devices are high-value targets due to their internet exposure and privileged network position.
- **Minimise Exposure:** Audit and reduce the number of services exposed to the internet. Remove unnecessary management interfaces, legacy portals, and unused applications. Only expose services that are strictly required for business operations.
- **Vulnerability Scanning:** Conduct regular external vulnerability scans and penetration testing to identify exploitable weaknesses before attackers do.

2. User Awareness & Phishing Resilience

Strengthen organisational resilience against phishing-based initial access, which is one of Gunra's primary attack vectors.

• **Phishing Awareness Training:** Conduct regular security awareness training for all staff.
• **Phishing Simulation Campaigns:** Run periodic phishing simulation exercises using lures that match Gunra's documented phishing templates. Track click rates and mandate additional training for repeat offenders.
• **Reporting Culture:** Encourage and simplify the process for employees to report suspicious emails. Establish a clear escalation path from user report to SOC investigation.
• **Email Security Controls:** Strengthen email gateway controls to detect and block Microsoft-themed spear-phishing emails. Implement DMARC, DKIM, and SPF enforcement to prevent domain spoofing.

3. SOC Detection & Threat Hunting

Implement SOC detection rules and conduct proactive threat hunting combining standard security monitoring with Gunra-specific indicators.

Email, Phishing & Cloud Identity Detection

• Review email gateway and email security products to ensure they can effectively identify and quarantine phishing emails. Gunra's initial access is likely to involve Microsoft-themed spear-phishing with malicious attachments.
• **Suspicious mailbox rules:** Alert on creation of new inbox rules that auto-forward, delete, or move emails to obscure folders (e.g., RSS Feeds) — a common post-compromise persistence technique to intercept security notifications and hide attacker activity.
• **MFA anomalies:** Alert on new MFA method registrations, particularly additions of new authenticator apps, phone numbers, or FIDO2 keys on accounts that did not initiate the request. Correlate with impossible travel or anomalous sign-in events.
• **New device enrolment:** Monitor for new devices joined to Azure AD / Entra ID or enrolled in MDM from unexpected locations. Alert on device registrations that do not match known corporate provisioning workflows.
• **Risky sign-in review:** Review cloud identity provider (Azure AD / Entra ID, Okta, Google Workspace) risky sign-in reports daily. Investigate sign-ins flagged for impossible travel, unfamiliar locations, anonymous IP addresses, or password spray patterns. Correlate with known Gunra victim credential exposure on dark web forums.

Gunra-Specific Process & Encryption Detection

• **Shadow copy deletion (T1490):** Alert on wmic.exe with 'shadowcopy' and 'delete' arguments. Gunra deletes 60+ shadow copies using: `cmd.exe /c C:\Windows\System32\wbem\WMIC.exe shadowcopy where "ID={GUID}" delete`. Also alert on vssadmin.exe delete shadows.
• **Ransom note detection:** Alert on creation of R3ADM3.txt across multiple directories — definitive Gunra indicator. Wazuh Rule ID 100601 (Level 15).
• **Encryption indicator:** Detect rapid creation of files with .ENCRT extension. Trend Micro query: `eventSubId:106 AND objectFilePath:/\.ENCRT$/`. Also alert on CONTI_LOG.txt creation.
• **Process detection:** Alert on execution of gunraransome.exe or unsigned executables with PDB path containing 'D:\wrk\tool\encrypter'. Monitor for mutex creation matching 'kjsidugiaadf99439' or '34adfwefadf99439'.
• **VSSVC.exe anomaly:** Alert on VSSVC.exe loading amsi.dll (Wazuh Rule 100602). Alert on CHXSmartScreen.exe loading urlmon.dll (Wazuh Rule 100603).

Lateral Movement Detection

• **PsExec detection:** Alert on creation of the PSEXESVC service (Sysmon Event ID 13 for registry, Event ID 7045 for service installation). Monitor for PsExec.exe or renamed variants executing on remote hosts — Gunra uses PsExec for lateral movement and ransomware staging across servers.

• **SMB lateral movement:** Monitor for anomalous SMB file transfers, particularly executable files (.exe, .dll) being written to ADMIN$ or C$ shares on multiple hosts in rapid succession. Alert on SMB connections from non-administrative workstations to server ADMIN$ shares.

• **WMI remote execution:** Alert on WMI process creation events (Event ID 4688) where the parent process is WmiPrvSE.exe on remote hosts, indicating WMI-based lateral command execution.

Suspicious Outbound Traffic & Exfiltration Monitoring

• **FTP/SFTP connections:** Alert on outbound FTP (port 21) and SFTP (port 22) connections to external IP addresses not on an approved whitelist. Gunra uses FTP servers for data exfiltration.

• **Large outbound data transfers:** Implement DLP alerts for outbound transfers exceeding defined thresholds (e.g., 500 MB in a single session or 2 GB cumulative within 24 hours). Gunra has exfiltrated up to 13.2 TB from a single victim.

• **Cloud storage exfiltration:** Monitor for outbound connections to cloud storage services (AWS S3, Bash Upload, SFTP) from hosts that do not normally communicate with these services. Alert on S3 API calls (PutObject, UploadPart) from unexpected endpoints.

• **Tor traffic:** Block and alert on outbound connections to known Tor entry and exit nodes. Gunra's entire C2 and DLS infrastructure operates on Tor.

• **Network IoC hunting:** Review DNS and proxy logs for connections to Gunra C2 IPs (86.54.28[.]216) and datapub[.]news (clearnet DLS).

IoC & Rule-Based Hunting

• Scan all endpoints for known Gunra file hashes (SHA-256, MD5) listed in the IoC section of this report. Prioritise: `854e5f77f788bbbe6e224195e115c749172cd12302afca370d4f9e3d53d005fd`

• Search for files with .ENCRT extension or R3ADM3.txt across all file shares and endpoints.

• Search for the PDB path string 'D:\wrk\tool\encrypter' in process memory dumps or on-disk binaries.

• Deploy the YARA rule for the embedded DONOT Loader stub (published by The Raven File) across endpoint protection platforms.

4. Attack Surface Management Scan

Perform a comprehensive external and internal attack surface assessment focused on Gunra's documented initial access vectors.

External Attack Surface

• **Credential Exposure Monitoring:** Conduct dark web monitoring for organisational credentials exposed via infostealer logs. Organisations with credentials exposed via infostealer logs are at heightened risk of being targeted. Mandate password resets for any exposed accounts and enforce MFA organisation-wide.

• **Ongoing External Surface Monitoring:** Implement continuous monitoring of the external attack surface for newly exposed services, misconfigurations, and emerging vulnerabilities. Track public proof-of-concept (PoC) exploit releases for technologies in use and prioritise patching accordingly. Gunra and similar opportunistic groups actively scan for low-hanging fruit — newly disclosed vulnerabilities with available PoCs are frequently weaponised within days of public disclosure.

5. Endpoint Hardening & Recovery Preparedness

Implement targeted endpoint controls to reduce Gunra's encryption impact and ensure rapid recovery capability.

Backup & Recovery

• Maintain regular offline and immutable backups tested for restoration. Gunra specifically targets Volume Shadow Copies (60+ deletions per execution), making online backups insufficient.
• Ensure backup infrastructure is network-segmented and not accessible via the same credentials used for domain administration.
• Test ransomware recovery procedures quarterly, including restoration from immutable backups.

Application Control

• Enforce application allowlisting via AppLocker or Windows Defender Application Control (WDAC) to prevent execution from user-writable directories (AppData, Temp, Downloads).
• Block execution of unsigned executables matching Gunra's 194.50 KB file size profile where feasible.

Network Segmentation

• Segment critical infrastructure to limit lateral movement capability. Gunra uses PsExec, SMB shares, and WMI for network propagation.
• Restrict administrative credential usage across network segments to prevent credential reuse-based lateral movement.

Phishing-Resistant MFA & Identity Hardening

• **Deploy phishing-resistant MFA:** Enforce FIDO2 security keys or passkey-based authentication for all privileged and high-risk accounts. Traditional SMS/OTP-based MFA can be bypassed via real-time phishing proxies — phishing-resistant MFA eliminates this risk. Given Gunra's primary reliance on spear-phishing for initial access, this is the single most effective control to prevent compromise.
• **Conditional access policies:** Implement conditional access rules requiring compliant/managed devices for access to corporate resources. Block sign-ins from unmanaged devices, anonymous proxies, and high-risk locations.
• **Token protection:** Enable token binding and continuous access evaluation (CAE) to prevent stolen session token reuse. Revoke refresh tokens immediately upon detection of anomalous sign-in activity.
• **Phishing simulation:** Conduct regular phishing simulation campaigns targeting all staff, with emphasis on Microsoft-themed lures matching Gunra's documented phishing templates. Track click rates and mandate additional training for repeat offenders.

References

[1] **Trend Micro — Gunra Ransomware: Exploring Its Linux Variant**
https://www.trendmicro.com/en_us/research/25/g/gunra-ransomware-linux-variant.html

[2] **Broadcom — Gunra Ransomware Protection Bulletin**
https://www.broadcom.com/support/security-center/protection-bulletin/gunra-ransomware

[3] **Wazuh — Detecting Gunra Ransomware with Wazuh**
https://wazuh.com/blog/detecting-gunra-ransomware-with-wazuh/

[4] **S2W — Gunra Targeting South Korean Financial Institutions**
https://s2w.inc/en/resource/detail/890

[5] **ASEC (AhnLab) — Gunra Ransomware Emerges with New DLS**
https://asec.ahnlab.com/en/89206/

[6] **ASEC (AhnLab) — Linux Variant Cryptographic Weakness Analysis**
https://asec.ahnlab.com/en/90791/

[7] **Ampcus Cyber — Gunra Ransomware Strikes American Hospital Dubai**
https://www.ampcuscyber.com/shadowopsintel/gunra-ransomware-strikes-american-hospital-dubai/

[8] **CloudSEK — Inside Gunra RaaS: From Affiliate Recruitment to Full Technical Dissection**
https://www.cloudsek.com/blog/inside-gunra-raas-from-affiliate-recruitment-on-the-dark-web-to-full-technical-dissection-of-their-locker

[9] **The Raven File — Gunra Ransomware: What You Don't Know**
https://theravenfile.com/2025/09/23/gunra-ransomware-what-you-dont-know/

[10] **CYFIRMA — Gunra Ransomware: A Brief Analysis**
https://www.cyfirma.com/research/gunra-ransomware-a-brief-analysis/

[11] **PolySwarm — Gunra Ransomware**
https://blog.polyswarm.io/gunra-ransomware

[12] **Alpha Hunt — Gunra: Conti-Derived Double-Extortion Threat**
https://blog.alphahunt.io/gunra-ransomware-conti-derived-double-extortion-threat-targeting-global-critical-sectors/

[13] **SOC Prime — Detect Gunra Ransomware**
https://socprime.com/blog/detect-gunra-ransomware/

[14] **Lumu — Advisory Alert: Gunra Ransomware 5-Day Ultimatum**
https://lumu.io/blog/advisory-alert-gunra-ransomware-5day-ultimatum/