Hive Pro

Threat Level

Red

HiveForce Labs

# THREAT ADVISORY

## ATTACK REPORT

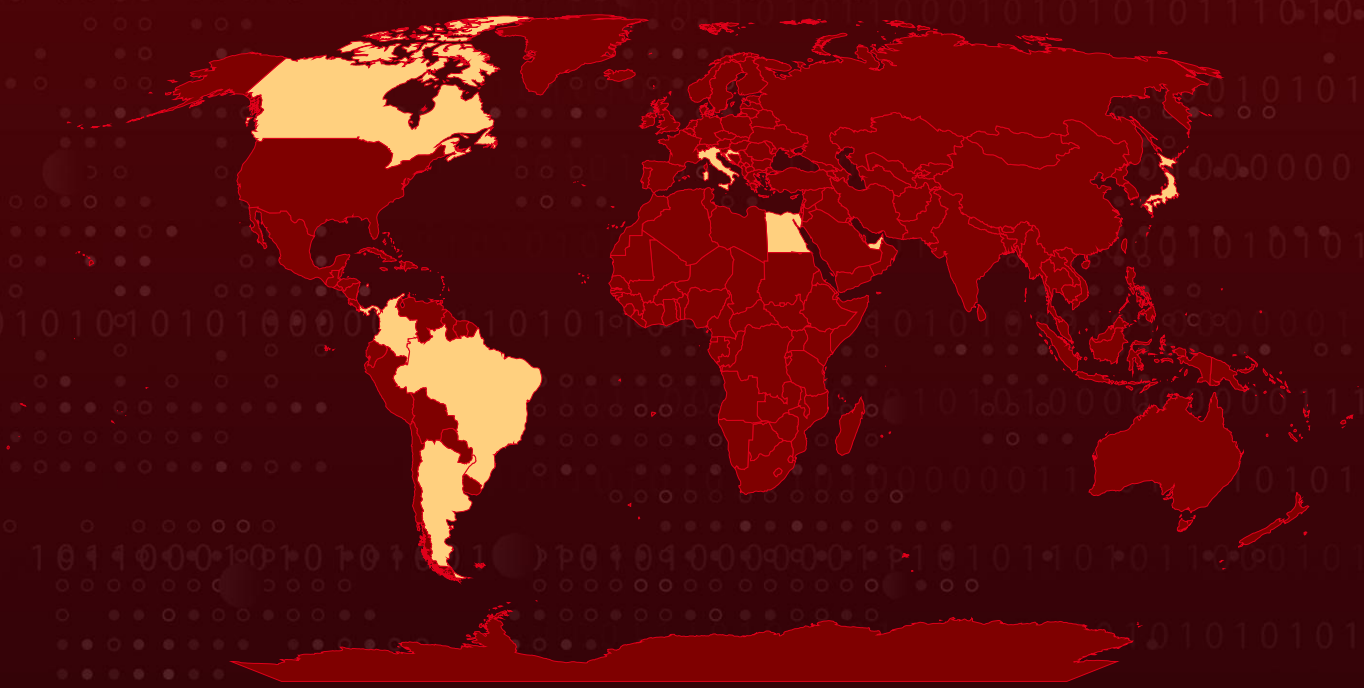
# Gunra Ransomware's Five-Day Deadline Strategy Fuels Panic


| Date of Publication | Admiralty Code | TA Number |
| --- | --- | --- |
| June 18, 2025 | A1 | TA2025193 |

# Summary

**First Seen:** April 2025
**Malware:** Gunra Ransomware
**Targeted Countries:** United Arab Emirates, Colombia, Canada, Brazil, Croatia, Japan, Italy, Egypt, Panama, Argentina
**Targeted Industries:** Business Services & Consulting, Construction, Consumer Services, Electronics, Food & Beverage, Healthcare, Legal, Manufacturing, Pharmaceuticals, Real Estate, Technology, Retail, Transportation, Government
**Affected Platform:** Windows
**Attack**: Gunra ransomware, a malware strain written in C/C++, is quickly making headlines for its aggressive double-extortion tactics. Built on the leaked Conti ransomware source code, it has compromised approximately 13 high-profile organizations worldwide since its emergence in April 2025.

## Attack Regions



# Attack Details

**#1** Gunra ransomware surfaced in April 2025, a malware strain written in C/C++. It draws heavily from the leaked source code of the Conti ransomware group. Gunra operates using double-extortion tactics, encrypting victims' data while exfiltrating sensitive files to blackmail organizations with the threat of public exposure.

**#2** The ransomware typically infiltrates systems through phishing campaigns and exploit kits. It collects critical data, disables recovery mechanisms by deleting shadow copies through Windows Management Instrumentation (WMI), and deploys obfuscation with anti-debugging techniques to evade security tools.

**#3** Gunra encrypts files and appends a ".ENCRT" extension to each filename. A ransom note titled "R3ADM3.txt" appears in every affected directory, providing payment instructions and a deadline for compliance. Victims usually receive a five-day response window, with negotiations conducted through anonymous Tor-based portals.

**#4** In recent weeks, Gunra targeted a healthcare organization in the UAE, adding the institution to its ransom site and threatening to leak a database reportedly containing records of 450 million patients. The group claiming to have stolen a large cache of highly sensitive data allegedly includes personal identification records, credit card information, Emirates ID numbers, patient health records, and internal communications.

**#5** The initial breach was disclosed on June 4, 2025. Shortly after, Gunra announced it had exfiltrated 4 terabytes of uncompressed patient data and warned of a mass data release if ransom demands were not met. The ongoing attack highlights Gunra's aggressive strategy and capability to compromise high-value targets while remaining difficult to detect and contain.

# Recommendations

**Optimize and Fine-Tune EDR Detection for Ransomware Behaviors:** Review and enhance EDR detection rules to specifically monitor for behaviors linked to Gunra ransomware. Focus on detecting process enumeration, system information gathering, and debugger checks using the IsDebuggerPresent API. Configure alerts for abnormal file encryption activity, especially files with ".ENCRT" extensions, and monitor WMI abuse targeting shadow copies and service controls.

**Implement the 3-2-1 Backup Rule:** Maintain three total copies of your data, with two backups stored on different devices and one backup kept offsite or in the cloud. This ensures redundancy and protects against data loss from ransomware attacks.

**Backup & Recovery Preparedness:** Maintain offline, immutable, and regularly tested backups. Ensure recovery time objectives (RTOs) and recovery point objectives (RPOs) meet business continuity requirements in the event of ransomware deployment.

## Potential MITRE ATT&CK TTPs

| | | | |
|---|---|---|---|
| TA0001 Initial Access | TA0002 Execution | TA0003 Persistence | TA0005 Defense Evasion |
| TA0007 Discovery | TA0009 Collection | TA0011 Command and Control | TA0010 Exfiltration |
| TA0040 Impact | T1566 Phishing | T1129 Shared Modules | T1176 Software Extensions |
| T1542 Pre-OS Boot | T1542.003 Bootkit | T1574 Hijack Execution Flow | T1574.001 DLL |
| T1055 Process Injection | T1548 Abuse Elevation Control Mechanism | T1014 Rootkit | T1564 Hide Artifacts |
| T1564.001 Hidden Files and Directories | T1518 Software Discovery | T1490 Inhibit System Recovery | T1486 Data Encrypted for Impact |
| T1185 Browser Session Hijacking | T1047 Windows Management Instrumentation | T1005 Data from Local System | T1090 Proxy |
| T1083 File and Directory Discovery | T1082 System Information Discovery | T1071 Application Layer Protocol | T1518.001 Security Software Discovery |
| T1057 Process Discovery | T1036 Masquerading | T1027 Obfuscated Files or Information | T1070 Indicator Removal |

| | |
|---|---|
| T1027.002<br>Software Packing | T1070.004<br>File Deletion |

## Indicators of Compromise (IOCs)

| TYPE | VALUE |
|---|---|
| Filename | gunraransome.exe,<br>R3ADM3.txt |
| MD5 | 9a7c0adedc4c68760e49274700218507 |
| SHA1 | 77b294117cb818df701f03dc8be39ed9a361a038 |
| SHA256 | 854e5f77f788bbbe6e224195e115c749172cd12302afca370d4f9e3d53d005fd |
| Tox ID | 2507312EC10BB44ED9DAA04E3C5C27E8C13154649B1A02E73ACFAE1681EE0208D05133A8FB22 |
| TOR Address | gunrabxbig445sjqa535uaymzerj6fp4nwc6ngc2xughf2pedjdhk4ad[.]onion,<br>apdk7hpbbquomgoxbhutegxco6btrz2ara3x2weqnx65tt45ba3sclyd[.]onion,<br>jzbhtsuwysslrzi2n5is3gmzsyh6ayhm7jt3xowldhk7rej4dqqubxqd[.]onion |

## Recent Breaches

https://www.accslegroupe.ca/
https://www.ahdubai.com/
https://www.aguasolhodagua.com.br/
https://anjosramos.com.br/
https://adria-grupa.hr/
http://www.justiciamilitar.gov.co/home
https://www.supersolidaria.gov.co/
https://mgchemicals.com/
https://vendasjb.com/
https://www.klinger.it/
https://www.shinkocorp.co.jp/
https://daralteb.com/
https://www.varelahermanos.com/

## References

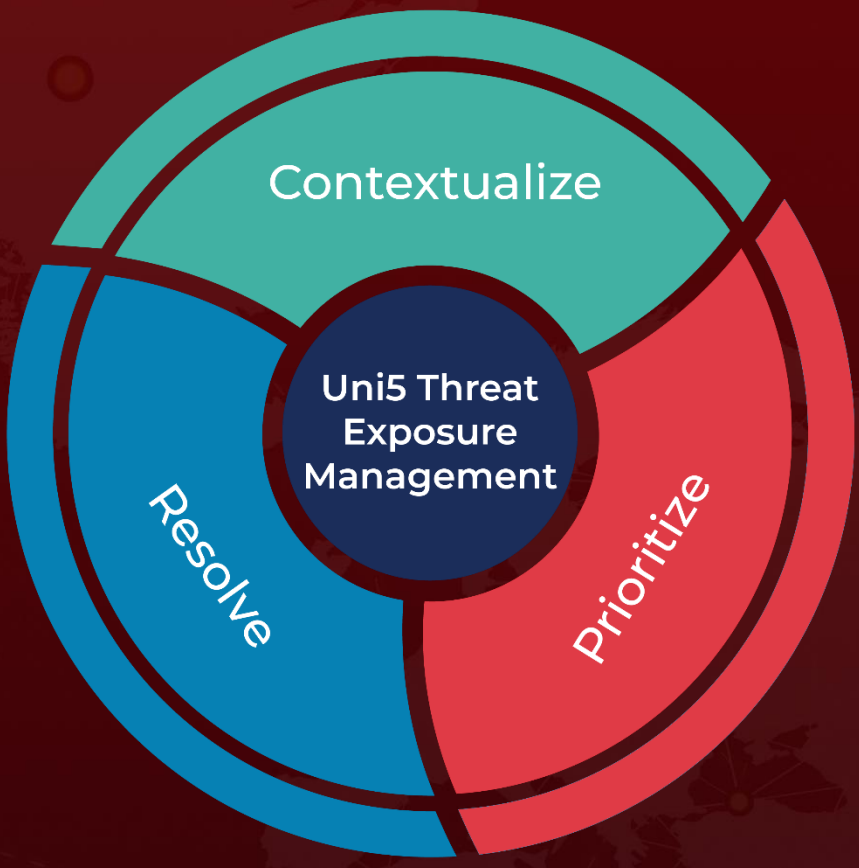
https://www.cyfirma.com/research/gunra-ransomware-a-brief-analysis/

https://databreaches.net/2025/06/04/ransomware-group-gunra-claims-to-have-exfiltrated-450-million-patient-records-from-american-hospital-dubai/

# What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.




REPORT GENERATED ON

**June 18, 2025 • 6:30 AM**



More at www.hivepro.com