BRIEF FOCUS · GUNRA · RANSOMWARE

Gunra Ransomware: Why Stopping Data Exfiltration Matters Before Encryption Begins

> A joint advisory from the FBI, CISA, DC3, NSA, U.S. Secret Service and the Republic of Korea National Police Agency details an emerging ransomware-as-a-service operation built on double extortion. Business-critical data, in one case tens of terabytes, is stolen before encryption ever begins.

THREAT ACTOR	MODEL	PLATFORMS	ADVISORY
Gunra (first observed April 2025)	**Ransomware-as-a-Service Double extortion**	**Windows Linux (mid-2025)**	**FBI · CISA · DC3 NSA · USSS · KNPA Aug 10, 2026**

SECTORS AT RISK

Government · Critical Infrastructure · Healthcare · Financial Services

THE ACTOR

Who Is Gunra?

On August 10, 2026, the FBI, CISA, Department of Defense Cyber Crime Center (DC3), NSA, and U.S. Secret Service, alongside the Republic of Korea National Police Agency, issued a joint Cybersecurity Advisory warning organizations about the emerging Gunra ransomware threat. The advisory highlights attacks against government, critical infrastructure, and other organizations worldwide and details the group's evolving tactics, techniques, and procedures.

First observed by the FBI in April 2025, Gunra has since expanded into a ransomware-as-a-service (RaaS) operation that uses double extortion, stealing sensitive information before encrypting systems and threatening to publish the data if victims refuse to pay. Initially focused on Windows environments, Gunra introduced a Linux variant in mid-2025 and moved toward broader cross-platform targeting.

DATA THEFT BEFORE ENCRYPTION

Exfiltration Is Central To Gunra's Strategy

Gunra actors collect business-critical documents, databases, personally identifiable information, and internal email before deploying ransomware. The FBI has observed a malicious tool designed specifically to steal data from Microsoft OneDrive and SharePoint.

In one known incident, attackers compressed sensitive information and transferred it to the MEGA file-sharing service, with stolen data reaching tens of terabytes.

Gunra infrastructure has also been associated with legitimate tools including 7-Zip, RClone, and FileZilla.

This focus on data theft means organizations may face significant exposure even if encrypted systems can ultimately be restored.

THREAT SNAPSHOT

APR 2025
First observed by the FBI, before expanding into a RaaS operation

10s of TB
Stolen data transferred to MEGA in a single known incident

2 CVEs
Authentication bypass flaws named in the joint advisory

EVOLVING TTPS

What Makes Gunra Dangerous

Gunra actors primarily gain access by exploiting vulnerabilities in internet-facing firewall and VPN appliances. The joint advisory highlights CVE-2024-55591 and CVE-2025-24472, authentication bypass flaws affecting certain FortiOS and FortiProxy versions.

Once inside, attackers have used Impacket tools including psexec.py and smbclient.py for lateral movement over SMB. Investigators also documented abuse of default VPN administrator credentials, SSH tunneling for persistence, stolen session information, and RDP access to critical systems.

Before encryption, Gunra actors have used WMI to delete Windows volume shadow copies and have deleted backup and archived data from backup infrastructure, limiting recovery options.

The combination of compromised credentials, legitimate administrative utilities, cloud services, and cross-platform ransomware makes Gunra difficult for traditional signature-based defenses to contain.

TOOLS AND SERVICES OBSERVED IN GUNRA ACTIVITY

OneDrive · SharePoint · MEGA · 7-Zip · RClone · FileZilla · Impacket · psexec.py · smbclient.py · WMI · FortiOS · FortiProxy

THE BLACKFOG PERSPECTIVE

BlackFog's Real-Time Defense For Risk Mitigation

Stops data theft before encryption
BlackFog's anti data exfiltration (ADX) technology directly addresses Gunra's double-extortion model. By preventing unauthorized outbound transfers, organizations can disrupt the stage of the attack that gives Gunra its greatest leverage.

Cuts off cloud and file-transfer exfiltration
Gunra has targeted OneDrive and SharePoint and used services and utilities such as MEGA, RClone, and FileZilla. BlackFog monitors outbound data movement and blocks suspicious transfers, even where legitimate applications are being abused.

Identifies abnormal behavior in real-time
Gunra affiliates use compromised accounts, SMB, RDP, SSH tunneling, and legitimate administrative tools to move through victim environments. Behavioral analytics help identify anomalous activity before attackers broaden their access.

Reduces exposure before ransomware deployment
Gunra may spend significant time gathering credentials, collecting data, and targeting backups before encryption begins. BlackFog's prevention-first approach focuses on stopping malicious activity earlier in the attack chain.

SIDE BY SIDE

BlackFog Vs Gunra Ransomware

THREAT VECTOR	GUNRA TACTIC	BLACKFOG COUNTERMEASURE
Initial Access	Exploited internet-facing VPN and firewall systems, compromised credentials	Behavioral detection, access anomaly monitoring, exposure reduction
Lateral Movement	Impacket, SMB, RDP, SSH tunneling	Behavioral analytics, traffic control, rapid containment
Data Collection	OneDrive, SharePoint, compressed archives, sensitive business data	Behavioral monitoring, sensitive data protection
Data Exfiltration	MEGA, RClone, FileZilla, cloud services	**Anti data exfiltration (ADX)**
Ransom & Extortion	Encryption, deletion of shadow copies and backup data, leak-site pressure	Data loss prevention, incident containment, forensic readiness

ABOUT BLACKFOG

Real-Time, On-Device, Data Exfiltration Prevention

BlackFog helps organizations reduce modern cyber risk by stopping data exfiltration, the common factor behind ransomware, insider threats, zero day attacks, and Shadow AI exposure. Our anti data exfiltration (ADX) platform delivers real-time, on-device prevention. It stops sensitive data from leaving endpoints and networks without authorization and blocks ransomware communication, data theft, and AI driven leakage before damage occurs. By focusing on prevention instead of just detection, BlackFog helps organizations strengthen compliance, protect privacy, and improve operational resilience.