Hive Pro

Threat Level

Red

CISA: AA26-222A

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

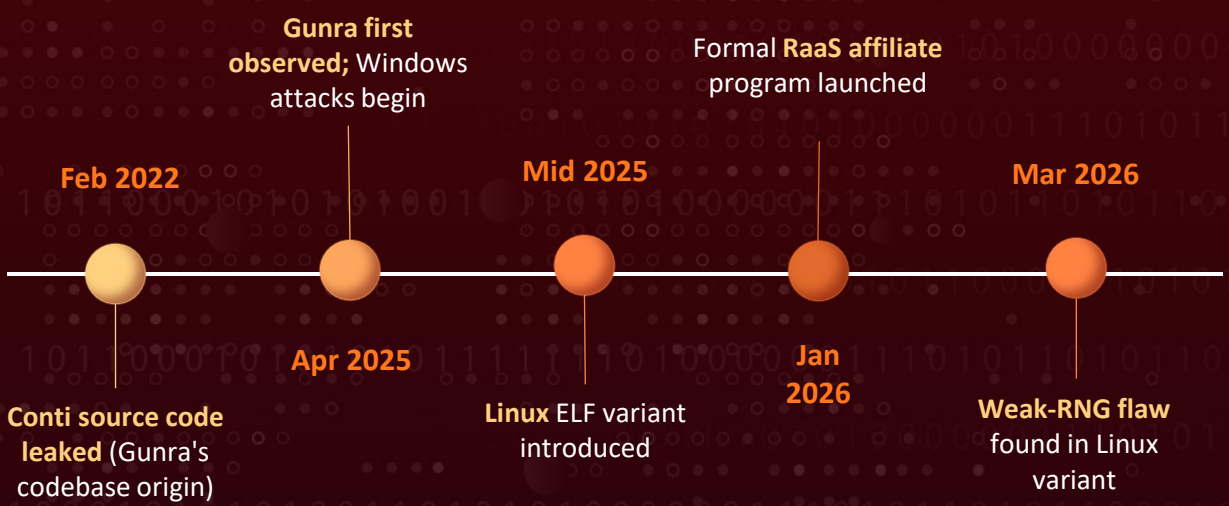
Gunra Ransomware Evolves into Full RaaS Operation Targeting Global Critical Infrastructure

Date of Publication	Admiralty Code	TA Number
August 14, 2026	A1	TA2026233

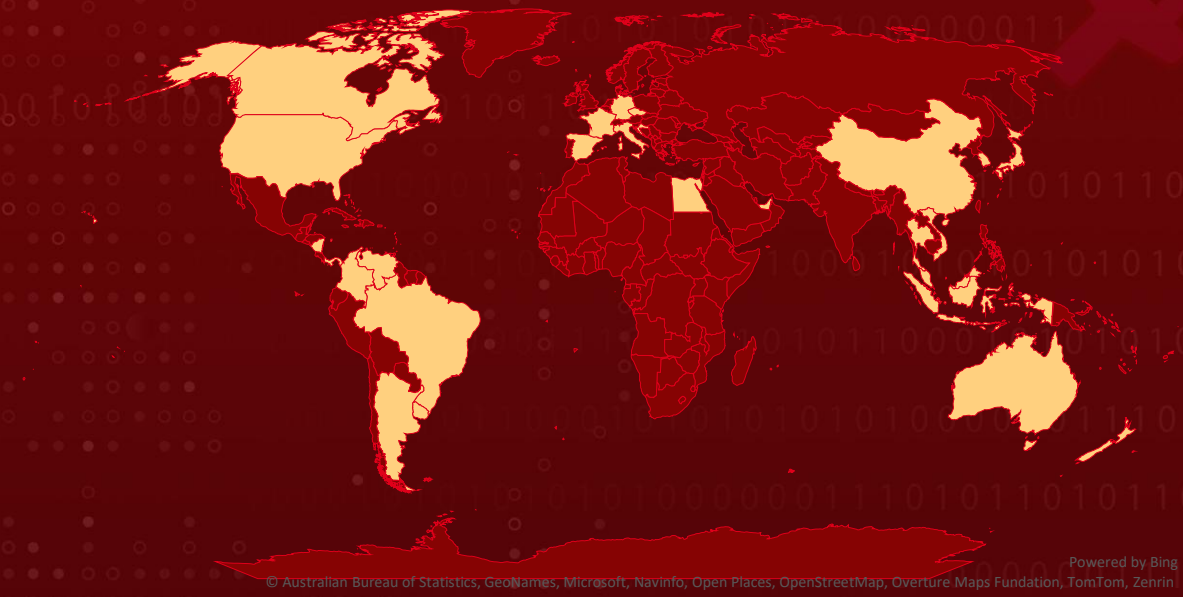
Summary

First Seen: April 2025
Targeted Countries: United States, Canada, Brazil, Argentina, Uruguay, Venezuela, Colombia, Nicaragua, Panama, Bahamas, Spain, France, Germany, Italy, Czech Republic, Croatia, United Arab Emirates, Egypt, South Korea, Japan, China, Thailand, Hong Kong, Singapore, Malaysia, Vietnam, Indonesia, New Zealand, Australia
Targeted Platforms: Windows and Linux
Targeted Products: Fortinet FortiOS, Fortinet FortiProxy, SSL-VPN appliances, Virtual Desktop Infrastructure (VDI) authentication portals, Microsoft OneDrive, Microsoft SharePoint, Hiware system access control servers, domain controllers, database servers, Network Attached Storage (NAS) systems
Targeted Industries: 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
Malware: Gunra Ransomware (aka Golden Community)
Attack: Gunra is a Conti-derived ransomware-as-a-service operation that emerged in April 2025 and formalized its dark-web affiliate program in January 2026, also operating as "Golden Community." Affiliates gain access by exploiting FortiOS/FortiProxy authentication-bypass flaws (CVE-2024-55591, CVE-2025-24472) to create persistent superuser accounts, then move laterally via Impacket over SMB, dump NTDS credentials, and tamper with VDI authentication files to bypass MFA. Under a double-extortion model, they exfiltrate up to tens of terabytes to Mega before deploying a multi-threaded ChaCha20 + RSA-4096 encryptor that appends the .ENCRT extension and drops the R3ADM3.txt note, with a five-to-seven-day deadline before leak-site publication.

Ransomware Timeline



Attack Regions



Targeted Non-Targeted

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-55591	Fortinet FortiOS and FortiProxy Authentication Bypass Vulnerability	Fortinet FortiOS	✓	✓	✓
CVE-2025-24472	Fortinet FortiOS and FortiProxy Authentication Bypass Vulnerability	Fortinet FortiOS and FortiProxy Office	✗	✓	✓

Attack Details

#1

Gunra is a double-extortion ransomware operation first observed in April 2025 and derived from the leaked Conti ransomware source code, initially deployed against Windows environments. In mid-2025 the operators introduced a Linux variant, extending the operation to cross-platform campaigns. As of January 2026, Gunra expanded its operations through a structured ransomware-as-a-service affiliate program advertised on dark web forums, providing affiliates with a management panel, a configurable ransomware builder, cross-platform locker payloads, and structured affiliate documentation. During this expansion the operation was also observed operating under the alias "Golden Community.“

#2

The threat actors obtain initial access primarily by exploiting vulnerabilities in internet-facing security appliances. The authoring agencies attribute intrusions to exploitation of CVE-2024-55591 and CVE-2025-24472, authentication-bypass flaws in FortiOS and FortiProxy that the operators leverage to create persistent super-user accounts on compromised appliances. The operators additionally abuse exposed credentials and weak SSH access controls on internet-facing VPN gateways to establish remote access.

#3

Following intrusion, Gunra affiliates operate a data-theft-first playbook, exfiltrating sensitive data prior to encryptor deployment. The locker employs a hybrid encryption scheme combining ChaCha20 for high-speed file encryption with RSA-4096 key wrapping, and is capable of encrypting very large data volumes within a limited timeframe. Victims are directed to a Tor-based negotiation portal, and the actors threaten to publish exfiltrated data on a dedicated leak site if the ransom is not paid. Individual incidents have reportedly involved exfiltration of tens of terabytes and ransom demands exceeding tens of millions of dollars.

#4

Gunra targeting spans multiple sectors across the Americas, Europe, the Middle East, Africa, and the Asia-Pacific, including healthcare, financial services, government, manufacturing, transportation, utilities, and retail. Leak-site-listed victims (attacker-claimed) are concentrated in South Korea, Brazil, Spain, Thailand, and Hong Kong, with only limited North American exposure reported to date.

Recommendations

Patch Fortinet FortiOS and FortiProxy Immediately: Apply vendor patches for CVE-2024-55591 and CVE-2025-24472 on all internet-facing FortiGate firewalls and FortiProxy appliances and treat both as KEV-priority items; until patched, restrict management interfaces to trusted management networks and disable HTTP/HTTPS administrative access from the internet.

Deploy Detection Content for the Gunra Encryptor: Alert on creation of files with .ENCRT extensions, appearance of R3ADM3.txt files, high-volume file rename bursts, and companion .keystore file creation, and monitor for the file hashes and executables listed in the Indicators of Compromise section.

Eliminate Default Credentials and Enforce Account Lockout on SSL-VPN Appliances: Rotate every factory-default credential on SSL-VPN and VPN gateway appliances, enforce account lockout thresholds on administrative accounts, disable or delete unused accounts in the administrative web console, and remove configuration options that permit bypass of mandatory password change requirements.

Detect and Block Impacket Tooling on the Internal Network: Deploy detection logic for the Impacket suite (psexec.py, smbclient.py, secretsdump.py) including named-pipe artifacts, service creation over SMB, and anomalous authentication against domain controllers, and alert on unexpected NTDS.dit or SYSTEM/SECURITY hive access.

Protect Symmetric Keys on Access Control Servers: Store symmetric encryption keys used by system access control platforms such as Hiware in hardware security modules or protected keystores rather than on the server file system, restrict SSH access to these servers to jump hosts only, and monitor for credential store access anomalies from virtual desktops.

Maintain Offline, Immutable, Segmented Backups: Keep at least one copy of sensitive data in offline, immutable storage that is physically separate from the primary environment and the disaster recovery site, restrict backup infrastructure credentials to dedicated privileged access workstations, and regularly test full restoration to confirm recoverability without ransom payment.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Execution	T1047: Windows Management Instrumentation	
	T1106: Native API	
	T1059: Command and Scripting Interpreter	T1059.003: Windows Command Shell
Persistence	T1098: Account Manipulation	
	T1133: External Remote Services	
Privilege Escalation	T1078: Valid Accounts	T1078.001: Default Accounts
		T1078.002: Domain Accounts
Defense Evasion	T1622: Debugger Evasion	
	T1070: Indicator Removal	T1070.003: Clear Command History
	T1678: Delay Execution	
	T1679: Selective Exclusion	
	T1685: Disable or Modify Tools	

Tactic	Technique	Sub-technique
Credential Access	T1003: OS Credential Dumping	T1003.003: NTDS
	T1040: Network Sniffing	
	T1539: Steal Web Session Cookie	
	T1555: Credentials from Password Stores	
	T1556: Modify Authentication Process	T1556.006: Multi-Factor Authentication
Discovery	T1083: File and Directory Discovery	
	T1049: System Network Connections Discovery	
Lateral Movement	T1021: Remote Services	T1021.001: Remote Desktop Protocol
		T1021.002: SMB/Windows Admin Shares
	T1550: Use Alternate Authentication Material	T1550.002: Pass the Hash
		T1550.003: Pass the Ticket

Tactic	Technique	Sub-technique
Collection	T1560: Archive Collected Data	
	T1530: Data from Cloud Storage	
	T1005: Data from Local System	
	T1114: Email Collection	
Command and Control	T1105: Ingress Tool Transfer	
	T1572: Protocol Tunneling	
Exfiltration	T1567: Exfiltration Over Web Service	
	T1048: Exfiltration Over Alternative Protocol	
Impact	T1486: Data Encrypted for Impact	
	T1657: Financial Theft	
	T1490: Inhibit System Recovery	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	75e5621756e9d19efeac2bcbb2ac4711fb85243c03b0a19c05b18e31a780691e, 25c8cb27947042de89d634b3e260e614e5b1425a89494fa4e4295bcabfa8ee48, 2dc70a12d158d437e45a55b1d52f3d61c6082a1e1667573302ba3b62813e2751, 834efe9b392c6c000877ea5613a079445affc16fe8af5997d68c55cafc95e5d1, 91f8fc7a3290611e28a35a403fd815554d9d856006cc2ee91ccdb64057ae53b0, a82e496b7b5279cb6b93393ec167dd3f50aff1557366784b25f9e51cb23689d9
SHA1	BB79502D301BA77745B7DBC5DF4269FC7B074CDA
MD5	E57b130718373f6ba9b37f39ca1d7e3d, 7DD26568049FAC1B87F676ECFAAC9BA0
IPv4	23[.]239[.]119[.]2, 23[.]239[.]119[.]3, 23[.]239[.]119[.]4, 23[.]239[.]119[.]5, 23[.]239[.]119[.]6, 86[.]54[.]28[.]216, 103[.]125[.]234[.]14, 70[.]36[.]99[.]82, 211[.]21[.]210[.]181, 123[.]184[.]143[.]105, 182[.]204[.]21[.]240, 182[.]204[.]16[.]112, 123[.]244[.]187[.]144, 182[.]204[.]39[.]118, 67[.]43[.]53[.]10, 123[.]246[.]37[.]108, 91[.]201[.]66[.]146
Domain	datapub[.]news

TYPE	VALUE
Emails	a00f105546345756[@]proton[.]me, 4569f6322bc3b22e9[@]proton[.]me, ilovemycubscout[@]gmail[.]com, 6449a3c1e612168526[@]proton[.]me
Filename	main.exe, cryptor.exe, msmp.exe, R3ADM3.txt
TOR Address	gunrabxbig445sjqa535uaymzerj6fp4nwc6ngc2xughf2pedjdhk4ad[.]onion, lgiil72vkmdtbc3qv4tyq6wedyjxqr2qd4ze7xl2cxgerdnymxj7soqd[.]onion, nsnhzysbntsqdwpys6mhml33muccsvterxewh5rkbmcab7bg2ttevjqd[.]onion
Tox ID	2507312EC10BB44ED9DAA04E3C5C27E8C13154649B1A02E73ACFAE1681EE0208D05133A8FB22, 0FE87CED0C611AE97E049C64288557F49E8271E91399E849328B078DA789A573031783235BEF, 47829AF1C943D4C296C910706923AS199BDA4995B076ED9A9016F7DEF161D445DF00F13E6900, 9500B1A73716BCF40745086F7184A33EA0141B7D3F852431C8FDD2E1E8FAF9277E9FDC117B47
Malicious Account	forticloud-sync

Recent Breaches

https://www.allcosmos.com
https://www.worldtube.co.kr
https://www.sakai-ssc.com
https://www.weilhotel.com
https://www.dissingerlaw.com
https://www.new-tiles.com
https://www.yuditec.com
https://www.segurospiramide.com
https://www.on-us.com
https://www.suarezyclavera.com.uy
https://www.grupomhe9.com.br
https://www.findyello.com
https://www.segroup.starempire.com
https://www.somafix.fr
https://www.kukjepharm.co.kr
https://www.neoderm.hk
https://www.aspships.com
https://www.tpt.co.th
https://www.incarfe.es
https://www.le-caillebotis-diamond.fr
https://www.ffgwm.com
https://www.envy-recycling.cz
https://www.ventilacionesnerual.com
https://www.nokair-bkksky.com
https://www.ericdavisdental.com
https://www.elezh.com
https://www.vintage-homestead.de
https://www.ipirangacontabil.com
https://www.cablematic.com
https://www.triotech.com
https://www.grupopyd.com

Patch Link

CVE-2024-55591 and CVE-2025-24472:

https://fortiguard.fortinet.com/psirt/FG-IR-24-535

References

https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-222a

https://www.cloudsek.com/blog/inside-gunra-raas-from-affiliate-recruitment-on-the-dark-web-to-full-technical-dissection-of-their-locker

https://socprime.com/active-threats/gunra-ransomware-uses-multithreaded-chacha20-encryption/

https://www.hivepro.com/threat-advisory/gunra-ransomwares-five-day-deadline-strategy-fuels-panic

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 Demo of **HivePro**.

REPORT GENERATED ON

August 14, 2026 • 05:20 AM

More at www.hivepro.com