ultraviolet

THREAT ADVISORY

Gunra Ransomware Group Targeting Vulnerable Fortinet Devices

Services Performed By:
UltraViolet Cyber TIDE Team
tide@uvcyber.com

Published Date:
August 12, 2026
TLP:GREEN

Executive Snapshot

CISA, the FBI, NSA, DC3, the U.S. Secret Service, and South Korea's National Police Agency issued a joint advisory this week warning that Gunra ransomware actors are actively targeting critical infrastructure worldwide. Gunra is a double-extortion ransomware-as-a-service operation built on leaked Conti source code that first appeared in spring 2025 and has since expanded into a structured affiliate program recruiting financially motivated criminals through dark web forums.

The group primarily gains initial access by exploiting two long-known Fortinet FortiOS/FortiProxy authentication bypass flaws, both of which have sat in CISA's Known Exploited Vulnerabilities catalog for over a year yet remain unpatched at many organizations. Once inside, affiliates hijack VPN and virtual desktop infrastructure, defeat multi-factor authentication, and combine data theft with encryption before threatening public leaks.

- Patch Fortinet FortiOS/FortiProxy devices now as two known flaws remain actively exploited over a year after disclosure
- Don't rely on MFA alone; always verify authentication files and portals haven't been tampered with
- Keep backups offline and immutable as Gunra deletes them before and after encrypting
- Watch for overnight activity and unusual credential access, which are key signs of Gunra's tradecraft
- Assume you're a target regardless of region and be mindful that healthcare, finance, government, and manufacturing are all in scope

TIDE Team Analysis

Gunra represents a maturing ransomware-as-a-service model that lowers the technical bar for affiliates while still achieving sophisticated outcomes against hardened targets. Built on Conti's leaked codebase, the malware supports both Windows and Linux payloads and uses fast stream ciphers capable of encrypting very large datasets quickly. Since formalizing its affiliate program in early 2026, Gunra has provided partners with a management console, a configurable builder, and structured documentation, functionally commoditizing ransomware deployment for less experienced criminals.

Gunra follows a double-extortion model, meaning affiliates both steal a victim's data and encrypt their systems. This gives them two separate points of leverage: victims face operational disruption from encrypted files and the threat of stolen data being published on a leak site if payment isn't made within five to seven days, even if they can restore from backup.

The group's initial access technique relies on patching gaps rather than novel exploitation. CVE-2024-55591 is a critical authentication bypass flaw in FortiOS and FortiProxy that grants attackers super-admin privileges on affected devices, while CVE-2025-24472 is a related high-severity authentication bypass impacting the same products. Both vulnerabilities were disclosed and patched over a year ago, yet Gunra continues to find unpatched, internet-facing instances still exposed.

What distinguishes Gunra operationally is its systematic targeting of identity infrastructure. Affiliates have manipulated SSL-VPN traffic-control features to intercept credentials and session cookies from users authenticating to a corporate VDI portal, then used those stolen sessions to impersonate legitimate users. In at least one case, they altered authentication-processing files so a Gunra-chosen one-time password value would always succeed, neutralizing MFA rather than bypassing it just once.

ADVERSARY PROFILE

Gunra

Golden Community

ALSO GUNRA, Gunra Ransomware Group

ATTRIBUTION	**Unattributed,** Not attributed to a specific agency or unit
ACTIVE SINCE	2025 (1+ years)
MOTIVES	**Financial gain** **Data extortion** **Data extortion**
INDUSTRIES	healthcare and public health, financial services, government services and facilities, manufacturing, and professional and nonprofit services.
COUNTRIES	South Korea, Brazil, Spain, Thailand, and Hong Kong.

NOTABLE TTPs

01	Exploiting known vulnerabilities in internet-facing Fortinet FortiOS and FortiProxy appliances for initial access
02	Hijacking SSL-VPN traffic control functionality to intercept credentials and session cookies
03	Tampering with VDI authentication files to enable a static one-time password and bypass multi-factor authentication
04	Using Impacket tools such as psexec.py, smbclient.py, and secretsdump.py for lateral movement and credential dumping
05	Exploiting default or dormant administrative accounts on SSL-VPN appliances
06	Stealing symmetric encryption keys from access control servers to decrypt stored enterprise credentials
07	Exfiltrating data to Microsoft OneDrive, SharePoint, and the MEGA file-sharing service before encryption
08	Deleting backups at primary and disaster recovery sites before and after deploying ransomware

Additional tradecraft includes exploiting default or dormant administrative accounts, harvesting a symmetric encryption key from an access-control server to decrypt stored enterprise credentials, and using Impacket utilities for SMB-based lateral movement and credential dumping. The group operates mainly overnight, clears logs and command history, exfiltrates data via a custom executable and the MEGA file-sharing service, and deletes backups at both primary and disaster-recovery sites before and after encryption.

Why It Matters

This activity matters because it shows patch debt on perimeter devices, not novel exploits, is driving major ransomware losses against critical infrastructure. Both Fortinet vulnerabilities were disclosed and patched over a year ago, yet they are still yielding successful intrusions today. This gap underscores that vulnerability management and asset visibility, especially for internet-facing appliances like VPNs and firewalls, remain a primary enabler for well-resourced RaaS operations. It also signals that attackers don't need zero-days to succeed; they simply need organizations to be slow to patch. For stakeholders, this reframes "known" vulnerabilities as an ongoing operational risk rather than a solved problem once a patch exists.

The MFA-bypass technique is especially significant because it undermines a control many organizations treat as a definitive safeguard. If authentication files on VDI or SSL-VPN portals can be silently modified so that attacker-chosen credentials are always accepted, MFA alone cannot be assumed to stop account takeover. This matters to stakeholders because breach notification obligations, cyber insurance terms, and customer assurances often lean heavily on the presence of MFA as evidence of due diligence. Gunra's approach shows that the mere existence of MFA doesn't guarantee its integrity, which has implications for how confidently organizations and their boards can rely on that control during risk assessments or after an incident.

The systematic deletion of backups before and after encryption also raises the stakes for business continuity and disaster recovery planning. By deliberately targeting both primary and disaster-recovery backup locations, Gunra affiliates aim to remove the safety net organizations rely on to avoid paying ransoms or enduring prolonged outages. This directly affects recovery time objectives, insurance claims, and the overall calculus victims face when deciding whether to negotiate. Stakeholders responsible for continuity planning should recognize that backup availability can no longer be assumed once an intrusion has occurred undetected for any length of time.

Finally, while Gunra's victim base has skewed heavily toward Asia-Pacific, South America, and Europe so far, with only a small number of confirmed North American victims, the sector spread, healthcare, financial services, government, and manufacturing, shows a targeting model that is opportunistic rather than tied to any single region. Combined with a growing affiliate program actively recruiting new operators, this suggests North American organizations should not read the current victim geography as a reason for complacency. This carries direct implications for operational continuity, regulatory reporting obligations, and public safety, particularly for healthcare and government entities where service disruption can affect the public directly rather than just the organization's bottom line.

How to Respond

- **Patch and inventory internet-facing Fortinet appliances immediately.** Prioritize remediation of the two known exploited Fortinet vulnerabilities, and confirm no unmanaged or forgotten devices remain exposed to the internet.
- **Harden VPN and VDI authentication pathways.** Monitor for unauthorized changes to authentication-processing files, disable or rotate default and dormant administrative accounts, and treat unexpected OTP acceptance patterns as a high-priority alert.
- **Protect identity and credential stores.** Restrict and monitor access to systems holding encryption keys or credential databases, and limit the blast radius of credential-dumping attempts through tiered administration and segmentation.
- **Make backups immutable and offline.** Store backups in a physically or logically separate environment from production and disaster-recovery infrastructure so they cannot be deleted alongside primary systems during an attack.
- **Watch for lateral movement and off-hours activity.** Deploy detections for Impacket-style SMB tooling, unusual overnight administrative activity, log clearing, and large data transfers to cloud storage or file-sharing services like MEGA.

What UltraViolet Cyber is Doing

- Tracking new CVEs and high impact vulnerabilities, analyzing and deploying public Proof-Of-Concept code against custom built targets.
- Proactively enabling custom detections based on the collected artifacts, tactics, techniques, and procedures identified in this activity.
- Performing hypothesis driven threat hunts based on threat actor behavior and artifacts. UVCyber customers will be informed of the results through secure channels.
- Parsing available victim dump data for any social, financial, business, or technical relations to UVCyber Clients and partner organizations.
- Aggregating threat intelligence from myriad sources and applying the most up-to-date knowledge to proactive threat hunting and response.

About UltraViolet Cyber

UltraViolet Cyber is a leading tech-enabled managed security services provider, delivering unparalleled cybersecurity expertise that fills technology and talent gaps across Global 2000 and Federal Government customers. Founded and operated by security practitioners from the national intelligence community, UltraViolet Cyber connects offensive security, application security, detection and response, and security engineering to deliver a differentiated approach to cybersecurity operations. Transforming customers' security programs, UltraViolet Cyber's flagship security-as-a-service solution, UV Lens, removes complex operational silos, replacing them with integrated security capabilities. UltraViolet is headquartered in McLean, Virginia with technology centers across the world.

443.351.7630 / info@uvcyber.com | UltraViolet Cyber | @uv_cyber

---