Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

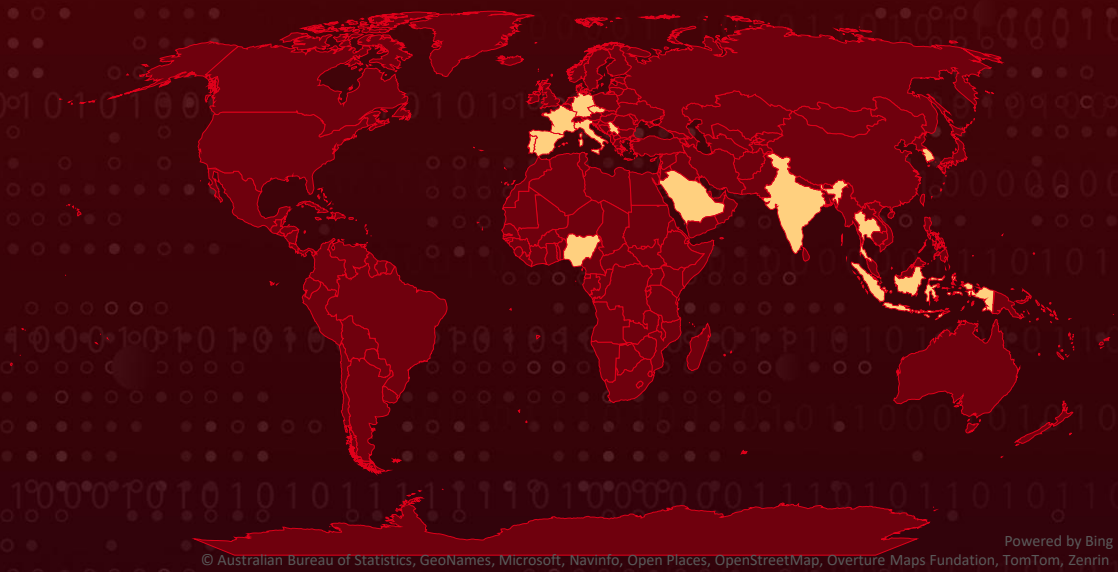
Panzer: New Cross-Platform RaaS Claims Global Victims in Its First Month

Date of Publication	Admiralty Code	TA Number
September 11, 2026	B1	TA2026267

Summary

First Seen: August 5, 2026
Targeted Regions: Spain, Portugal, France, Saudi Arabia, Germany, Indonesia, Serbia, Italy, South Korea, Czech Republic, India, Thailand, Nigeria
Targeted Platforms: Windows, Linux, VMware ESXi, FreeBSD
Targeted Industries: Technology, Manufacturing, Government, Food Production, Energy & Utilities, Education, Retail & E-Commerce, Telecommunications, Construction & Engineering, Media, Gaming
Malware: Panzer ransomware
Attack: Panzer is a newly emerged Ransomware-as-a-Service operation whose dedicated leak site was first observed active on August 5, 2026. Within its first month the group listed 20+ claimed victims across 10+ countries, pairing data theft with file encryption in a double-extortion model and pressuring victims through a Tor leak site with countdown timers. The operation advertises cross-platform payloads for Windows, Linux, VMware ESXi and FreeBSD, with the ESXi build posing the greatest risk since a compromised hypervisor allows encryption of many virtual machines in a single action. Panzer runs a semi-open affiliate programme with Tox-based screening, an 80/20 revenue split favouring affiliates, and a fully featured dashboard for build management, negotiation and leak publication. No encryptor sample has been publicly analysed and no file hashes or network infrastructure have been verified; the only public indicators are the leak-site onion address and affiliate Tox ID, initial access vectors remain unconfirmed, and all victim listings remain attacker claims except one publicly confirmed incident.

Attack Regions



Attack Details

#1

Panzer is a newly emerged Ransomware-as-a-Service operation whose dedicated data leak site was first observed active on August 5, 2026. Within its first month the group listed 20+ claimed victims across 10+ countries, pairing data theft with file encryption in a double-extortion model. Listed organisations span technology, manufacturing, government, agriculture, energy, education, retail, telecommunications and media, with technology and manufacturing the most affected sectors, and are distributed across Thailand, Italy, Indonesia, Serbia, Curaçao, South Korea, Spain, the Czech Republic, Germany, Nigeria and Switzerland. The breadth of geography and industry indicates opportunistic, affiliate-driven targeting rather than a focused campaign, and almost all of the listings remain attacker claims.

#2

The operation advertises cross-platform payloads for Windows, Linux, VMware ESXi and FreeBSD, with builds supporting more than fifteen customisable commands, anti-detection features and a control panel providing real-time monitoring of execution results. The ESXi capability is its most consequential advertised feature, since a compromised hypervisor can allow encryption of many virtual machines in a single action, converting a localised intrusion into an enterprise-wide outage, while Linux and FreeBSD support extends reach into mixed server estates.

#3

Panzer runs a semi-open affiliate programme, reportedly recruited via Russian-speaking cybercrime forums though this is not independently confirmed, with applicants screened through a Tox-based process before receiving dashboard access and monitored during their first month for signs of researcher or law-enforcement infiltration. Affiliates retain 80 percent of ransom proceeds while the platform collects 20 percent automatically on each payment, and accounts idle for more than seven days are deactivated. The panel offers balance tracking, build management, support tickets, team sub-accounts, per-build negotiation portals with integrated Bitcoin invoicing and a leak-publication workflow requiring team approval, and operational rules prohibit targeting CIS countries and organisations involving minors.

#4

All available information derives from the group's own advertising and leak-site postings. No encryptor sample has been publicly analysed, no verified file hashes, network infrastructure or malware samples exist, and the only public indicators are the leak-site onion address and affiliate Tox ID. Initial access vectors remain unconfirmed, and assessments linking the group to credential dumping, brute force, remote-service movement, security-tool tampering and exfiltration over alternative protocols are medium-to-low confidence.

Recommendations

Alert on and isolate hosts performing shadow copy deletion: Deploy detection rules for vssadmin delete shadows, wmic shadowcopy delete and bcdedit recoveryenabled no. Treat any execution on a server as imminent encryption: isolate the host automatically, preserve evidence and open an incident rather than a ticket.

Monitor the Panzer leak site and Tox recruitment channel: Add the published .onion leak-site address and affiliate Tox ID to threat-intelligence monitoring and alert on any connection attempts from internal assets. Because no file hashes, domains or IP addresses have been verified, do not rely on blocklists for this threat.

Hunt for unsanctioned RMM tooling and admin-share propagation: Baseline the approved remote-management stack and alert on ScreenConnect, AnyDesk or similar agents appearing outside change control, on PsExec service installations, on WmiPrvSE spawning child processes on servers, and on RMM execution combined with mass archive creation and admin-share activity within a compressed window.

Detect pre-exfiltration staging: Alert on archives larger than 100 MB appearing in user profiles or ProgramData, on rclone, 7-Zip, WinRAR, MEGA or anonymous file-transfer processes running on servers, and on large or unusual outbound transfers to non-corporate cloud storage. The 48-to-72-hour window between domain-level access and exfiltration is the most actionable interception point.

Extend EDR with tamper protection to Linux, FreeBSD and virtualization tiers: Deploy endpoint detection with tamper protection across every platform Panzer advertises a build for, and alert on service-stop attempts against EDR or antivirus agents, since impairment of security tooling is associated with this group.

Maintain immutable, cross-platform backups and test hypervisor-level recovery: Keep immutable, offline or air-gapped backups for Windows, Linux, ESXi and FreeBSD workloads held outside the virtual estate, and rehearse restoration against a hypervisor-level failure rather than a single file server, validating that recovery points predate any compromise.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Persistence	T1078: Valid Accounts	
	T1136: Create Account	
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
Command and Control	T1219: Remote Access Software	
Credential Access	T1003: OS Credential Dumping	
	T1110: Brute Force	
Discovery	T1046: Network Service Discovery	
Lateral Movement	T1021: Remote Services	
Defense Evasion	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
Collection	T1005: Data from Local System	
	T1560: Archive Collected Data	
Exfiltration	T1048: Exfiltration Over Alternative Protocol	
	T1567: Exfiltration Over Web Service	
Impact	T1486: Data Encrypted for Impact	
	T1490: Inhibit System Recovery	
	T1657: Financial Theft	

Indicators of Compromise (IOCs)

TYPE	VALUE
TOR Address	pnzruro7syvwvefx5mpo2fhzi4jftgquynsqf3vy5x3no57yp2iz4nyd[.]onion
Tox ID	8C3D96497A9438794F705C055FC2FD3059F6CF11FF51060EE55ED7F0679CFC7218825BD56CB1

Recent Breaches

https://aemet.es
https://aqualogus.pt
https://kafec.sa
https://hs-heilbronn.de
https://diskominfo.go.id
https://senvibe.com
https://vojvodina.gov.rs
https://nteitalia.it
https://frisianflag.com
https://jccm.es
https://doimocucine.com
https://dle.co.kr
https://sagasta.cz
https://alpine-electronics.eu
https://xpresstech.in
https://minorfood.com
https://siamoil.com
https://dailytrust.com
https://unsa.ac.id
https://festinagroup.com

References

https://andreafortuna.org/2026/09/07/panzer-ransomware-italian-victims/

https://cyberxtron.com/resources/blogs/panzer-ransomware-profile-of-an-emerging-double-extortion-operator-8102

https://www.kobaran.com/panzer-ransomware-emerges-as-a-full-affiliate-platform-before-any-sample-is-analyzed/

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

September 11, 2026 • 09:30 AM

More at www.hivepro.com