BLACKFOG®

Threat Intelligence Brief

FOCUS	SECTOR
INC Ransom	Healthcare, Professional Services, Government, Critical Infrastructure

Confronting INC Ransom
BlackFog's Prevention-First Strategy for Affiliate-Driven Ransomware

Who Is INC Ransom?

INC Ransom is a financially motivated ransomware-as-a-service (RaaS) operation that emerged in mid-2023 and is also tracked as Tarnished Scorpion and GOLD IONIC. Its affiliate model allows multiple intrusion crews to use INC ransomware tooling and infrastructure, while the core operation handles extortion and ransom payment workflows. Authorities say the group has compromised organizations worldwide since 2023 and has been increasingly observed targeting Australia, New Zealand, and Pacific Island states since early 2025. INC affiliates use double extortion: they steal sensitive data, encrypt files, and then threaten to publish the stolen material on a Tor-based data leak site if the victim refuses to pay. The advisory notes the group tends to pursue high-value entities handling sensitive information, with recent activity showing a focus on the healthcare sector.

A New Regional Focus

Critical Networks in the Crosshairs: A joint advisory from the Australian Cyber Security Centre (ACSC), CERT Tonga, and New Zealand's National Cyber Security Centre (NCSC) warns that INC Ransom and its affiliate network pose a threat to networks across Australia, New Zealand, and the Pacific island states. The warning highlights ongoing ransomware and data-extortion activity affecting organizations across the region, including healthcare providers, government-linked environments, and professional services entities. The guidance is notable because it ties INC Ransom to a broader affiliate-enabled campaign model that can scale across regional targets. Authorities emphasize the group commonly relies on compromised credentials, known vulnerabilities in unpatched internet-facing systems, and access purchased from initial access brokers to gain footholds inside victim environments.

Evolving TTPs: What Makes INC Dangerous

INC Ransom affiliates typically gain initial access through spear-phishing, exploitation of unpatched internet-facing devices, or the use of valid credentials purchased from initial access brokers. After establishing access, they create new privileged accounts, move laterally through victim networks, and prepare data for theft before launching encryption. For exfiltration and staging, the joint advisory says INC actors abuse legitimate tools such as 7-Zip and WinRAR to compress sensitive data and rclone to move it out of the environment. That blend of legitimate utilities and ransomware tradecraft makes detection harder for traditional signature-based tools, especially in organizations with limited visibility into outbound traffic and privileged account behavior. Authorities also note INC Ransom's tactics overlap with other RaaS ecosystems, including Lynx and operations such as Nemty, Karma, and Nokoyawa, suggesting an adaptable affiliate ecosystem rather than a single rigid playbook, increasing the likelihood of variation by victim, sector, and region.

BlackFog's Real-Time Defense For Risk Mitigation

- **Stops data theft before it starts:** BlackFog's anti data exfiltration (ADX) technology is aligned to the INC Ransom model. Because INC affiliates steal sensitive information before encryption and rely on leak site publication for pressure, blocking unauthorized outbound transfers can disrupt the most profitable stage of the attack, especially where actors abuse tools like rclone and compressed archives.
- **Detects suspicious privilege escalation in real-time:** The advisory highlights the creation of administrator-level accounts and lateral movement after compromise. BlackFog's behavioral analytics help identify abnormal authentication activity, privilege escalation, and suspicious account creation patterns before attackers broaden control of the environment.
- **Cuts off living-off-the-land exfiltration:** Because INC affiliates rely on legitimate software for compression and exfiltration, conventional malware-centric defenses may miss key stages. BlackFog's prevention-first approach helps expose and stop suspicious outbound behavior even when the utilities appear benign.
- **Reduces exposure across critical networks:** The latest regional guidance focuses on healthcare and critical network operators in Australia, New Zealand, and the Pacific. BlackFog's non-signature-based protections, data exfiltration controls, and rapid containment capabilities are suited for organizations that cannot afford prolonged disruption or exposure of regulated data.

BlackFog Vs INC Ransom

Threat Vector	INC Ransom Tactic	BlackFog Countermeasure
Initial Access	Spear-phishing, exploited internet-facing systems, purchased credentials	Behavioral detection, access anomaly monitoring, exposure reduction
Privilege Escalation	Creation of new admin accounts, compromised account abuse	Privileged account monitoring, real-time anomaly detection
Lateral Movement	Movement across victim networks after foothold	Behavioral analytics, traffic control, rapid containment
Data Exfiltration	7-Zip, WinRAR, rclone, leak-site extortion	Anti data exfiltration (ADX)
Ransom & Extortion	Encryption plus Tor-based data leak pressure	Data loss prevention, incident containment, forensic readiness

BLACKFOG®

Why BlackFog?

In a cyber landscape increasingly shaped by human-operated threats, organizations need more than reactive alerts, they need 24/7 real-time prevention. BlackFog delivers exactly that.

With its unique anti data exfiltration (ADX) technology, AI based behavioral threat detection, and dynamic blocking capabilities, BlackFog helps organizations prevent breaches by ensuring unauthorized data never leaves the network.

For organizations with lean internal teams, BlackFog's vCISO services provide expert leadership, streamlined incident response, and compliance-ready reporting, all tailored to the demands of that specific industry.

Ready to Learn More?

Visit blackfog.com or contact us at sales@blackfog.com

Award-winning Technology

Follow us:

Contact us for a demo

Start your free trial

Visit blackfog.com