BLACKFOG®

Threat Intelligence Brief

FOCUS	SECTOR
Akira Ransomware	Manufacturing, Education, Information Technology, Healthcare, Financial Services, Critical Infrastructure

Stopping Akira Through BlackFog's Prevention-First Strategy

Who Is Akira?

Akira is a ransomware-as-a-service (RaaS) operation that has matured significantly since its emergence in 2023. According to CISA's November 13, 2025, joint advisory, Akira threat-actors have expanded capabilities, including targeting virtual machine hypervisors and cloud backup systems, as well as increased the scale of attacks.

As of late September 2025, Akira is estimated to have netted approximately US $244 million in ransom payments, and impacted hundreds of organizations across multiple continents. Akira is linked to, or shares infrastructure with, other cybercrime groups such as Storm 1567, Howling Scorpius, Punk Spider, and possibly the legacy Conti group.

Key Threat Characteristics

Primary Targets: While Akira often targets small and medium-sized businesses (SMBs), the new guidance emphasises that larger entities and critical infrastructure organizations are increasingly at-risk including manufacturing, education, IT, healthcare, finance, food and agriculture.

Attack Vectors And Observed Tactics

- Initial access via exposed services such as VPNs, backup servers, and hypervisors, along with stolen credentials, especially where MFA is missing.
- Targets virtualization platforms, including Nutanix AHV encryption observed in June 2025, expanding beyond VMware ESXi and Hyper-V.
- Exploits known vulnerabilities, including SonicWall CVE-2024-40766 and Veeam CVE-2023-27532 and CVE-2024-40711.
- Uses credential abuse, lateral movement tools like Mimikatz and SharpDomainSpray, and legitimate remote access tools such as AnyDesk and LogMeIn.
- Uses double extortion, combining data theft, encryption, and threats to publish stolen data.

How BlackFog Mitigates Akira Ransomware

Prevention-first strategy designed for advanced adversaries:

- **Anti Data Exfiltration (ADX):** Blocks outbound transfers of data even when encrypted or disguised, cutting off the double extortion channel.
- **Behavioral Detection & Anomaly Monitoring:** Detects unusual activities such as bulk VM image encryption, hypervisor attacks, credential harvesting, and misuse of administration tools.
- **Edge-Device & Backup Protection:** Focuses on securing vulnerable appliances (VPNs, hypervisors, backup servers) by integrating backup deletion protection.
- **Rapid Incident Response & Containment:** Enables quick isolation of infected systems, forensic readiness.

Akira vs BlackFog Countermeasures

Threat Vector	Akira's Tactic	BlackFog Countermeasure
Initial Access	Exploited VPN/back-up vulnerabilities, stolen credentials	Harden external access, enforce phishing-resistant MFA
Virtualisation & Backup Assault	Encryption of VM disk files (e.g., Nutanix AHV), backup deletion	Monitor VM/backup changes, enforce offline immutable backups
Lateral Movement & Persistence	Use of legitimate remote tools, credential dumping, domain account creation	Behavioral alerting, privilege monitoring, anomaly detection
Data Exfiltration & Double Extortion	Data theft followed by encryption and leak threats	ADX enforcement, blocking of unauthorized transfers, logging
Multi-Sector Targeting	Wide-ranging impact across infrastructure, manufacturing, IT, healthcare	Cross-sector readiness, tailored incident response & risk modelling

Recommended Actions (per CISA & BlackFog)

- Ensure multi-factor authentication (MFA) is enforced, especially on remote access, VPNs, and backup systems.
- Prioritize remediation of known exploited vulnerabilities and maintain patching cadence for hypervisors, VPNs, backup appliances.
- Maintain regular offline, tested backups and ensure backups are immutable and disconnected from network during normal operations.
- Monitor and alert for unusual activity around virtualization platforms, backup servers, and administrative tools.
- Develop and test an incident response plan specific to large-scale ransomware events, including VM restoration and data recovery.
- Conduct staff training on phishing awareness, remote access risks, and insider threat indicators.
- Report any suspected intrusion or ransomware incident to local law enforcement (e.g., FBI) or relevant agency immediately. Early detection can reduce severe outcomes.

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

MSP Today Product of the Year 2025 · Cybersecurity Breakthrough Award · Fortress Cyber Security Award · teiss Awards 2025 · Globee Awards · Cyber Security Excellence Awards Winner

Follow us:

Contact us for a demo

Start your free trial

Visit blackfog.com