BLACKFOG®

Threat Intelligence Brief

FOCUS
Interlock Ransomware

CROSS-SECTOR
Manufacturing / Education / Healthcare

Taking Down Interlock Ransomware: BlackFog's Prevention First Approach

Who is Interlock?

Interlock, also referred to as Interlocker, is a ransomware variant which first appeared in September 2024. The financially motivated group has rapidly evolved from extortion-only tactics to full-scale ransomware deployment, known for its aggressive encryption and double extortion tactics and targeted attacks on critical infrastructure organizations.

Interlock often spreads through phishing emails, exploit kits, or compromised Remote Desktop Protocol (RDP) credentials. Once inside a network, it may attempt lateral movement to maximize damage. It has gained attention for the use of the increasingly popular ClickFix tactics, where users unknowingly execute a malicious payload by clicking a fake CAPTCHA pop up that instructs them to copy PowerShell code into Windows Run.

The advisory warned that after gaining access, Interlock actors are known to run remote access trojans (RATs) every time a user logs in, deploying command and control applications such as Cobalt Strike and SystemBC.

Notable Incidents and Tactics

CISA's July 2025 advisory warns of the following Interlock TTPs:

- Execution of obfuscated PowerShell commands for file staging and execution
- Manual lateral movement using compromised admin credentials
- Use of legitimate cloud storage services (e.g., Mega, Dropbox) for exfiltration
- Disabling Windows Defender, Microsoft Security Center, and registry protections
- Deployment of batch scripts to automate and maintain persistence

Organizations report encrypted file extensions like .interlock, making attribution clearer post-compromise.

Escalating Risks for the Healthcare Sector

The recent advisory issued by the FBI and CISA, jointly authored by the Department of Health and Human Services, and the MS-ISAC comes after a recent spate of attacks, orchestrated by Interlock, on the healthcare sector. The cybercrime group claimed responsibility for breaching DaVita, a Fortune 500 company specializing in kidney care, resulting in the theft and leak of 1.5 TB of data from their systems, as well as for hacking Kettering Health, a healthcare giant that operates over 120 outpatient facilities and employs more than 15,000 people. The group has also carried out a number of notable attacks on the education and manufacturing sector in recent months.

How BlackFog Mitigates the Risk

Stops Data Theft Before It Starts
BlackFog's anti data exfiltration (ADX) technology proactively blocks outbound data transfers, neutralizing Interlock's extortion mechanism.

Detects Suspicious Behavior in Real-Time
AI-driven analytics identify unusual behavior such as privilege escalation and remote execution, hallmarks of Interlock's manual post-exploitation techniques.

Cuts Off Command & Control
Geo-fencing and real-time domain blocking prevent Interlock from contacting leak sites or external infrastructure, disrupting the attack chain.

Defends Against Fileless and Living-off-the-Land Attacks
BlackFog provides non-signature-based protection against PowerShell, RDP abuse, and zero-day exploits, bypassing legacy antivirus systems.

BlackFog vs Interlock Ransomware

Threat Vector	Interlock Tactic	BlackFog Countermeasure
Initial Access	Phishing, malvertising, fake updates	Behavioral threat detection + malicious IP filtering
Lateral Movement	Manual admin exploitation via PsExec, RDP	Real-time anomaly detection, ADX policy enforcement
Data Exfiltration	Mega.nz, FTP, OneDrive uploads	Data exfiltration prevention (ADX)
Command & Control	Use of hidden cloud and Tor links	Real-time IP/domain blocking + geo-fencing
Security Tool Evasion	Disables Defender and logging features	Acts as another defense layer, stopping exfiltration even when other defenses are breached.

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