BLACKFOG®

Threat Intelligence Brief

FOCUS	SECTOR
Scattered Spider	Insurance

Stopping Scattered Spider: BlackFog's Resilient Defense

Who is Scattered Spider?

Scattered Spider (aka UNC3944 or Octo Tempest) is one of the most dangerous cybercrime groups targeting the insurance sector today. Using sophisticated social engineering and post-exploitation techniques, including MFA bypass and living-off-the-land tactics, they infiltrate organizations undetected and steal sensitive data for extortion. Their methods are especially effective against traditional, signature-based defenses.

A New Target: Insurance Sector in the Crosshairs

Following a wave of high-profile attacks on retail organizations, Scattered Spider has now shifted its focus to the insurance industry. Threat intelligence analysts quickly detected this pivot, observing that the same advanced techniques, used successfully in retail breaches, are now being applied to U.S. insurance firms. In a public alert issued in June, Google's Mandiant Threat Intelligence Chief, John Hultquist, emphasized the urgency: "We are now seeing incidents in the insurance industry."

This one-sector-at-a-time strategy signals a targeted campaign approach, requiring insurers to elevate their cyber defenses against this highly adaptive and persistent threat actor.

Confirmed Breaches Signal a Coordinated Campaign

Within days of the public warning about Scattered Spider's shift toward the insurance sector, multiple U.S. insurance companies reported disruptive cyber incidents.

Philadelphia Insurance Companies (PHLY) disclosed unauthorized access, leading to sustained system outages during containment efforts.

Erie Insurance reported business disruption, later confirming in an SEC filing that it had suffered a cyber incident requiring extensive remediation.

Meanwhile, Aflac, the largest supplemental insurer in the U.S., acknowledged a separate breach. Although operations were not interrupted and ransomware was not deployed, Aflac confirmed that threat actors may have accessed personal and health information of clients and employees. The company stated that the intrusion was part of a broader cybercrime campaign targeting insurers, carried out by a highly sophisticated threat group. Investigators have since noted that the tactics and tradecraft closely align with Scattered Spider, including simultaneous multi-target attacks and a focus on data exfiltration rather than system encryption.

How BlackFog Mitigates the Risk

Stops Data Theft Before It Starts

BlackFog's anti data exfiltration (ADX) technology blocks unauthorized outbound data transfers in real-time, preventing Scattered Spider from monetizing breaches through extortion.

Detects Stealthy Movement in Real-Time

BlackFog uses AI driven behavioral analytics to identify abnormal patterns such as privilege escalation and lateral movement - techniques central to Scattered Spider's attack playbook.

Cuts Off Command & Control

With geo-fencing and dynamic IP/domain blocking, BlackFog prevents malware from communicating with external command infrastructure, neutralizing threats mid-attack.

Stays Ahead of Signatureless Threats

BlackFog's non-signature-based detection protects against fileless malware and zero-day exploits that evade traditional perimeter defense and antivirus tools.

BlackFog vs Scattered Spider

Threat Vector	Scattered Spider Tactic	BlackFog Countermeasure
Initial access + social engineering	MFA bypass, identity compromise	AI based behavioral monitoring + Geo/IP filtering
Lateral movement	PsExec, PowerShell, RDP	Behavioral anomaly detection, real-time traffic control
Data exfiltration	Zip + exfil via cloud, FTP, DNS	Anti data exfiltration (ADX) – BlackFog's specialty
Command & control	Dynamic IPs, domain fronting	Real-time IP/domain blocking, geo-fencing
Regulatory pressure on insurers	Breach disclosure, ransomware payouts	vCISO services, compliance reporting, forensic support

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