BLACKFOG®

Threat Intelligence Brief

FOCUS	CROSS-SECTOR
The Com	Tech / Telecom / FinTech / Social

Understanding The Com: A New Cybercrime Model

Who is The Com?

The Com is a decentralized global cybercrime subculture, primarily composed of English-speaking actors aged 11-25. Operated via Discord, Telegram, and private forums, it comprises loosely affiliated subsets, notably Hacker Com, IRL Com, and Extortion Com, with fluid memberships and diverse motivations including financial gain, notoriety, and ideological satisfaction.

Notable subsets:

- **Hacker Com** focuses on technical crime: ransomware, phishing, SIM swapping, IP theft, malware development, and account compromise.
- **IRL Com** enables physical violence-for-hire, extortion, and coercion linked to online disputes.
- **Extortion Com** targets vulnerable individuals, particularly minors, using doxxing, blackmail, and CSAM coercion.

Tie to Scattered Spider and RaaS Ecosystems

Security analysts have identified Scattered Spider (a.k.a. UNC3944 / Octo Tempest / 0ktapus) as an operational evolution of the Hacker Com faction, with shared TTPs and infrastructure dating back to notable breaches at companies like HubSpot, Twilio, Cloudflare, Riot Games, Coinbase, Reddit, and MGM.

Scattered Spider has expanded into ransomware deployment, often as an affiliate deploying ALPHV/BlackCat-based payloads. The group's criminal infrastructure includes access brokering, social engineering, and targeted phishing designed to facilitate human-operated ransomware attacks.

Evolving Threat Profile

Tactics, Techniques & Procedures

- Initial Access & Credential Access
- Spear-phishing, social-engineered password resets of helpdesk/admin accounts.
- SIM-swapping and VoIP techniques enable account takeover and lateral privilege gain.

Modular, Burnable Toolkits

- Direct deployment of customized malware drop loaders and "burner" payloads built to evade behavioural and signature-based EDR detection.

Access Brokering Economy

- Initial access sold within cells or to ransomware affiliates and state-linked actors.
- Ecosystem model: multiple adversaries buy into the same network intrusion for different monetization objectives.

Ransomware & Double Extortion Deployments

- Scattered Spider affiliates deploy BlackCat/ALPHV payloads and other malware variants.
- Data theft precedes encryption, maximizing pressure through reputational and regulatory risk.

Real-World Violence as Leverage

- IRL Com subsets coordinate threats, kidnapping, or extortion to coerce victims or brag within the network.

How BlackFog Counters The Com Ecosystem

Real-Time Threat Prevention for Dynamic Cybercrime Cells

Threat Vector	Observed Tactics	BlackFog Countermeasure
Initial Access	Phishing; SIM/xSIM fraud; helpdesk compromise	Behavioral AI; SaaS gateway monitoring; anomaly detection
Credential Abuse	VoIP spoofing; SIM swap; insider mediation	Account monitoring; MFA enforcement; SIM/fraud alerts
Modular & Burn Malware	One-time loaders; burner malware	Zero-trust process isolation; digital signatures enforced
Access Brokering Activity	Compromised network resale; multi-affiliate intrusions	Network segmentation; lateral access alerting; isolation
Ransomware Deployment	BlackCat/ALPHV affiliates; double extortion	Anti data exfiltration (ADX); execution disruption policies
Real-World Coercion	Violent extortion or physical threats linked to online disputes	Incident escalation alerts; collaboration with law enforcement

Final Takeaway

The Com represents the new face of disruptive cybercrime - fluid, adaptable, and ominously collaborative. Threat actors span everything from technical hackers to online-turned-IRL attackers. Their evolution into ransomware operations like Scattered Spider demands defenses built for cross-vector threats and stealth-first tactics.

BlackFog's prevention-centric solution empowers organizations to defend against these ever-evolving, ecosystem-driven threats.

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 2024

2024 FORTRESS CYBER SECURITY AWARD

teiss Awards 2025

GLOBEE AWARDS

CYBER SECURITY EXCELLENCE AWARDS WINNER 2023

Follow us:

Contact us for a demo

Start your free trial

Visit blackfog.com