Threat Actor Economics

Understanding the Business of Cybercrime

ISSA NoVA Chapter Meeting

SUREFIRE CYBER

Agenda

- The Threat Actor Ecosystem
- The Merchants
- Ransomware-as-a-Service & Evolution of Extortion Tactics
- How Threat Actors Choose Targets
- The Ecosystem Beyond Ransomware
- Strategic Threat Intelligence & Turning Patterns into Defense
- Being Proactive & Turning Attacker Patterns into Defense
- Key Takeaways

The Ecosystem

Not lone wolves. An interconnected marketplace of independent criminal vendors.

What Is the Threat Actor Ecosystem?

Shared tools. Underground forums. Overlapping infrastructure. Fluid networks of collaboration.

THE MARKETPLACE

- Dark web forums, Telegram channels, and invite-only platforms where criminal vendors advertise, transact, and build reputations.
- 92% of major marketplaces operate escrow and dispute resolution systems that mirror legitimate e-commerce.

THE VENDORS

- Independent criminal specialists, each selling a distinct product or service: malware, stolen credentials, network access, ransomware platforms, laundering services.
- No membership required to buy.

THE SCALE

- Dark web markets generated $2B+ in 2024. 3.2M daily Tor users.
- 500% increase in credential logs on dark forums.
- A mature, global underground economy.

The Merchants

Each operates independently and sells to any buyer willing to pay, regardless of group affiliation

Malware Developers
- Build and sell ransomware, stealers, RATs, encryptors, loaders as-a-service subscriptions
- Sell subscriptions from $90-$600+/month

Infostealer Operators
- Run campaigns against targets to harvest credentials at scale.
- Provide a market to sell stealer logs on dark
- $1-$100+ per log

Initial Access Brokers
- Breach victim networks, sell access.
- Buyer(s): ransomware operators to nation-states, BEC threat actors).
- $500-$3,000+ per listing

RaaS Operators
Build and license ransomware platforms. Recruit affiliates. Take ~30-40% of all ransom revenue collected by their network

Ransomware Affiliates
Execute attacks using purchased access and licensed ransomware. Independent operators who can earn ~60-70% of ransom collected

Crypto Laundering Services
Financial infrastructure with layered exchange services that convert ransom payments into untraceable funds

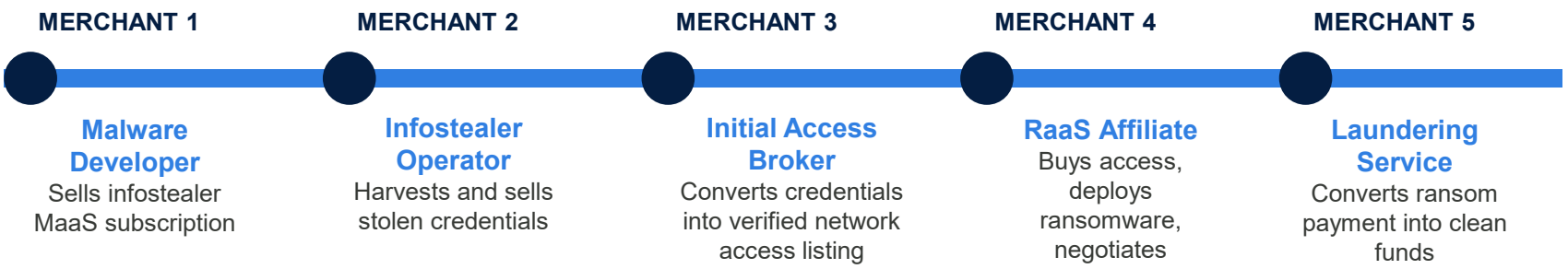
Cross-Merchant Commerce

Merchants transact independently across group lines. No shared membership required.

Infostealer operators sell credential logs	Buyers include IABs, BEC operators, and fraud actors. Stealer logs sell for $1-$100+ per record on auto-shops like Russian Market
IABs sell verified network access	Ransomware affiliates, BEC operators, and nation-state actors are all buyers. One IAB listing can be purchased by multiple unrelated threat actors
RaaS operators recruit and license to affiliates	Affiliates are independent contractors. The same affiliate may work for multiple competing RaaS operators simultaneously. No exclusivity.
Nation-state actors transact with criminal merchants	North Korea’s Jumpy Pisces acted as an IAB for the Play ransomware group. Criminal and state infrastructure now uses the same bulletproof hosting providers.

One Attack, Five Merchants

A single ransomware incident can involve five independent criminal vendors who may never communicate directly



None of these five merchants need to know each other. The underground marketplace connects them through anonymous, reputation-rated transactions. Ransomware execution can begin within 48 hours of credentials appearing in an underground market.

Ransomware-as-a-Service

Cybercrime operates like a modern franchise

DEVELOPERS

Build ransomware, maintain infrastructure, leak sites

AFFILIATES

Breach networks, deploy malware, negotiate ransoms

REVENUE SPLIT

60-70% to affiliates, 30-40% to operators

Evolution of RaaS & Extortion Tactics

2019-2020

Maze

Pioneered double extortion

2019-2022

REvil/Sodinokibi

$100M+ annual revenue claimed

2019-Present

LockBit

2,000+ victims, $120M collected

2021-2024

BlackCat/ALPHV

First Rust-based ransomware

2023-Present

Qilin

Most active group in late 2025

Pre-2019

Single Extortion

Big Game Hunting encrypted files and demanded ransom for decryption keys

Nov 2019

Double Extortion

Steal data first, threaten to leak if unpaid

2021+

Triple Extortion

DDoS & targeting client's/partners

2024+

Data-Only

Skip encryption entirely, pure extortion

The Shift to Data Theft-Only

11x

Increase in data-only extortion attacks

Nov 2024 to Nov 2025

57.6%

of extortion cases involved data theft without encryption

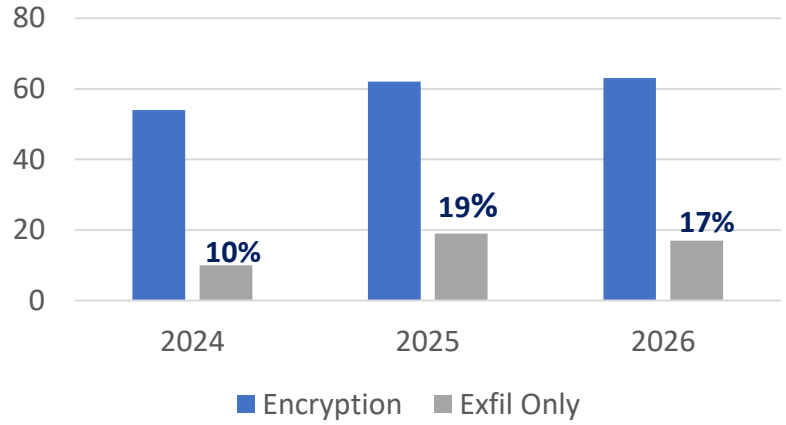
Full Year 2025

Why? Better backups mean encryption alone doesn't guarantee payment

Source: Arctic Wolf 2026 Threat Report, Resilience Insurance

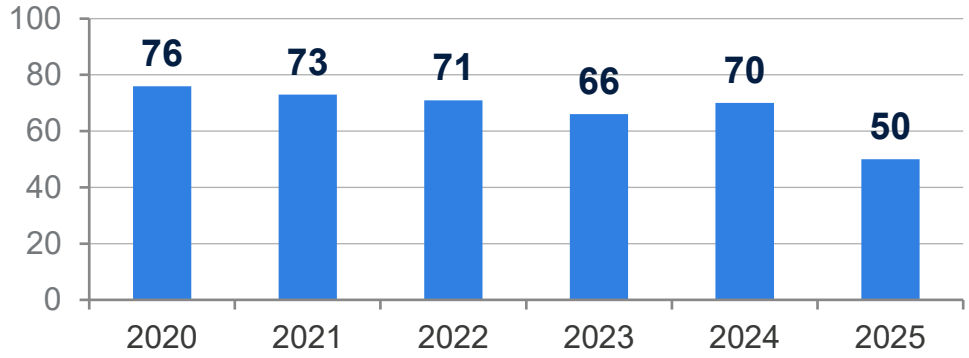
Encryption Is Declining

Surefire Cyber Exfiltration Only



Source: Surefire Cyber Data

Broader Market Exfiltration Only



Source: Sophos State of Ransomware Reports 2020-2025

How Threat Actors Choose Targets

Revenue Thresholds

US: $5M+ | EU: $20M+ | Other: $40M+

Geographic Preference

US (47%), Canada (37%), Australia (37%), EU (31%)

Sector Avoidance

47% avoid healthcare/education, 37% avoid government

CIS Blocklist

Russia, Ukraine, Belarus, Kazakhstan never targeted

2025 Attack Distribution

Industry (Surefire Cyber)

Professional Services **19%**

Healthcare **17%**

Manufacturing **11%**

Public Administration **8%**

Education **6%**

Industry (Broader Market)

Manufacturing **21%**

Healthcare **18%**

Professional Services **12%**

Financial Services **10%**

Retail **11%**

By Business Size

Most Targeted:

51-200 employees

$5M-$25M revenue

SMBs can't afford downtime and often pay to survive

Beyond Ransomware

The Broader Cybercrime Economy

$16.6 billion in reported losses in 2024 alone

FBI IC3 2024 Annual Report

Business Email Compromise

The quiet giant of cybercrime no malware required

$8.5B

in losses over 3 years (2022-2024)

FBI IC3

How It Works

1. Compromise email via social engineering/phishing
2. Monitor conversations for payment threads
3. Hijack thread, impersonate trusted party
4. Redirect wire transfers to criminal accounts

18%	$166,000	+15%
Involve financial loss	Average loss	increase in BEC attacks (2025)

Source: FBI IC3 2024 Report and Surefire Cyber Data

Using Threat Intelligence

Move from reactive to proactive

TACTICAL

IOCs, malware hashes, C2 domains, known exploited CVEs

OPERATIONAL

TTPs, affiliate behaviors, initial access methods, tooling

STRATEGIC

Targeting trends, economic drivers, group motivations

Focus resources on what matters to YOUR organization

Turning Patterns into Defense

External remote access (59% of attacks)	→	Secure RDP, enforce MFA on VPN
Exploited vulnerabilities (32%)	→	Prioritize KEV catalog patching
Compromised credentials (23%)	→	Credential monitoring, password policies
Phishing/malicious email (37%)	→	User training, email security
Data exfiltration before encryption	→	DLP, network segmentation, monitoring

Industry Response

Organizations are getting better at defense and recovery

82%

have disaster recovery plans

62%

use immutable backups

87%

refuse to pay ransoms

53%

recover within one week

Payment rates declining: 13% in 2026, 16% in 2025 and 17% in 2024

Proactive Steps

Key actions your organization can take today

Backup Strategy

3-2-1-1-0 rule for all business critical and sensitive data

Identity Security

Phishing-resistant MFA on all external access

Vulnerability Management

Prioritize CISA KEV catalog

Network Segmentation

Limit lateral movement capabilities

Detection & Response

24/7 monitoring, defined IR playbook

User Training

Phishing simulations, reporting culture

Key Takeaways

- Ransomware is a mature business with sophisticated economics
- Data theft alone is now enough for extortion encryption optional
- BEC, infostealers, and IABs fuel the broader ecosystem
- Attackers target based on revenue, geography, and sector
- Better backups and response are reducing payment rates
- Threat intelligence enables proactive, not just reactive defense

Questions?

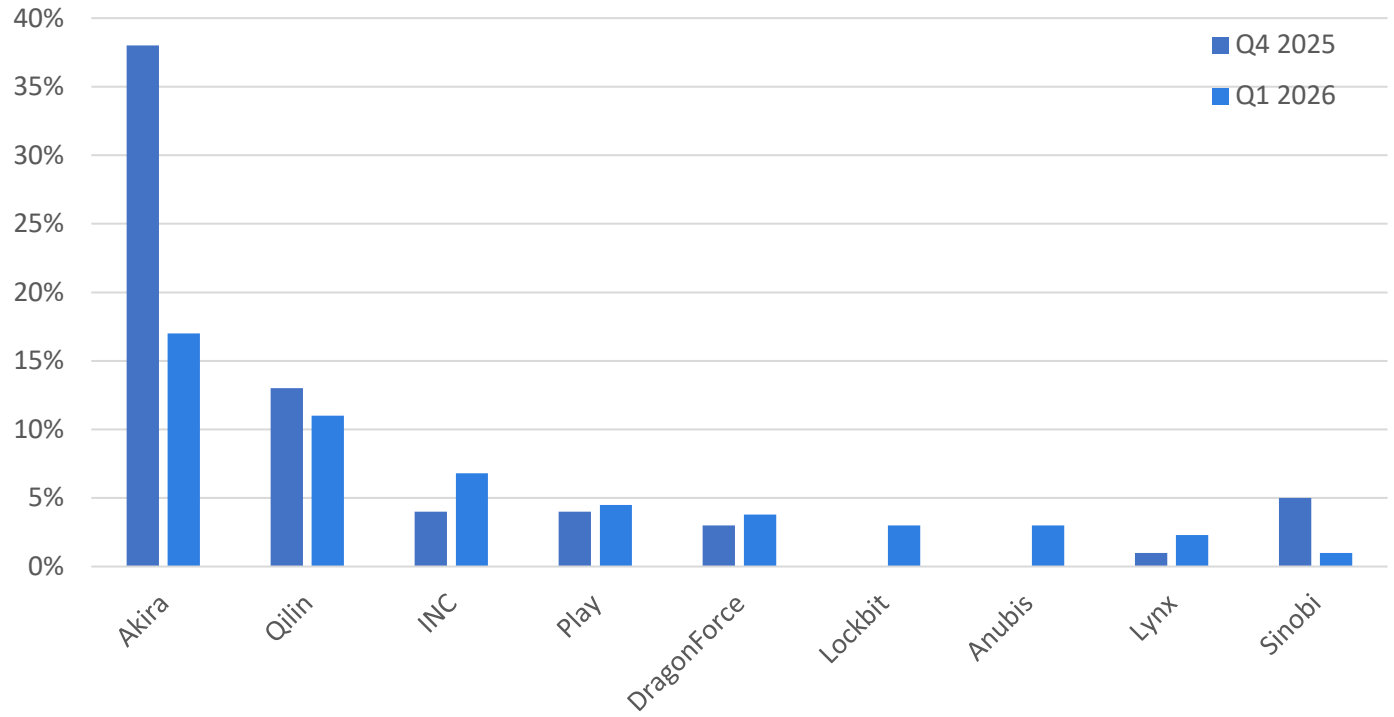
SUREFIRE CYBER

www.surefirecyber.com

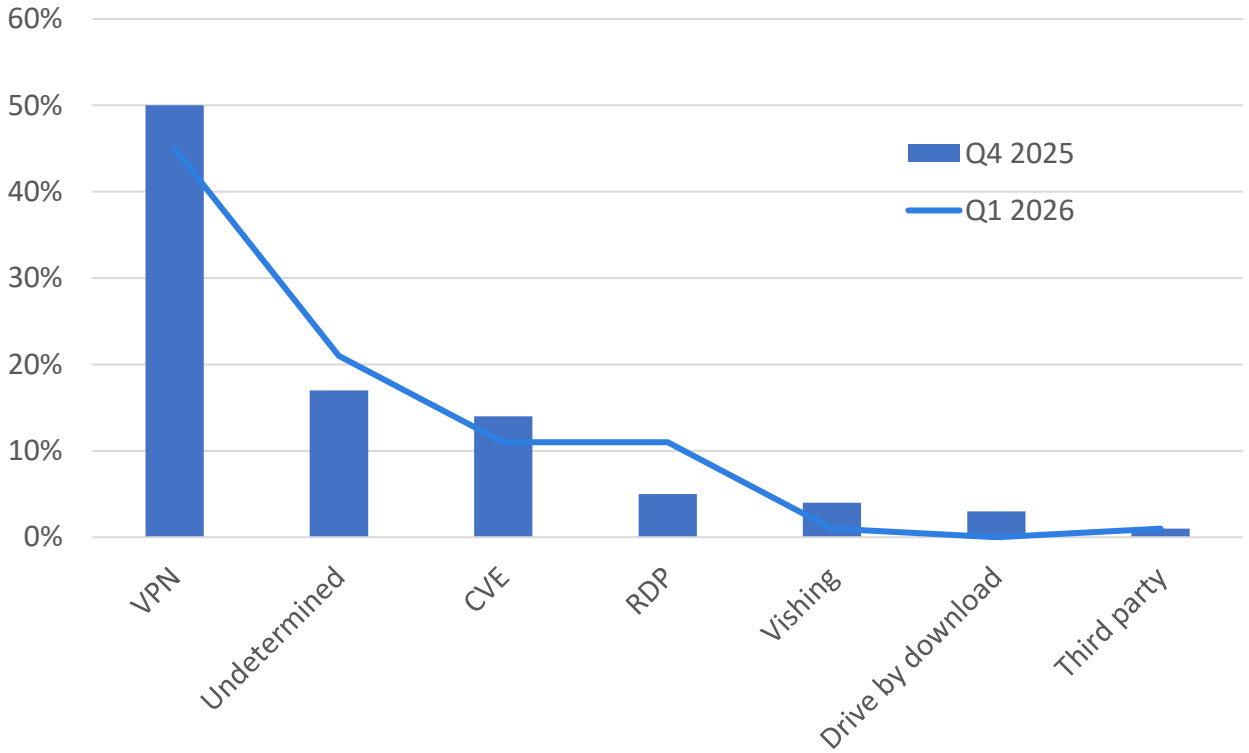
Appendix

Surefire Cyber Data Highlights

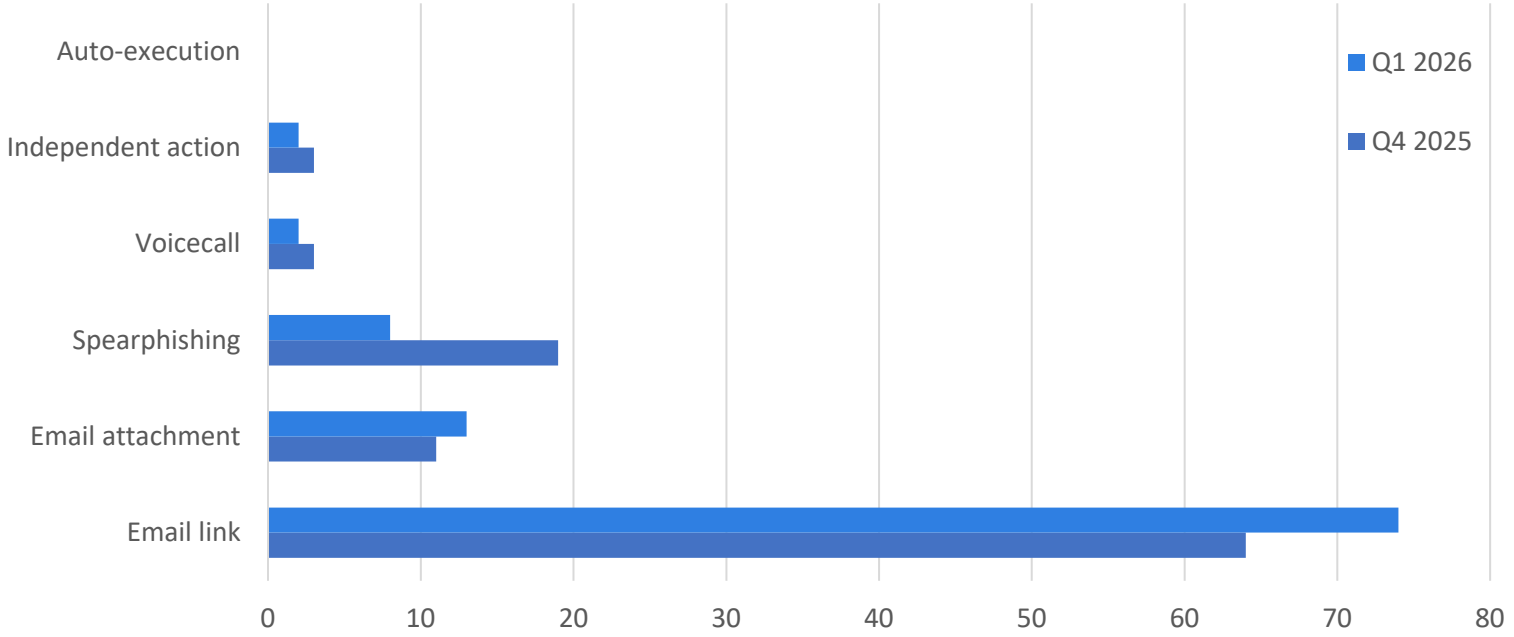
Threat Actor Activity Q4 2025 to Q1 2026



Root Point of Compromise



Business Email Compromise (BEC) Initial Access



BEC Financial Loss