

Outsmart cybercrime with clear, actionable intel

The problem

Cybercriminals aren't just opportunistic. They're organized, persistent and constantly evolving tactics to **maximize impact and profit**. From ransomware cartels to info stealers, many groups now work like agile global businesses, with clear roles, global reach and technical sophistication. **Ransomware revenues keep climbing** as extortion becomes more targeted and aggressive. In this reality, security teams need more than simple indicators of compromise. They need **deep, contextual intelligence** on how these groups operate, what they're after and how to stop them before real damage is done.

256 DAYS

average time for an organization to fully recover from a ransomware attack

Source: Forrester: 2024 Ransomware Breach Benchmarks, By Industry

50%

year-over-year rise in ransomware attacks (2025)

Source: ESET analyses of data leak sites

15% MORE DESTRUCTIVE

ransomware attacks vs. other types of breaches

Source: Forrester: 2024 Ransomware Benchmarks, By Region

The solution

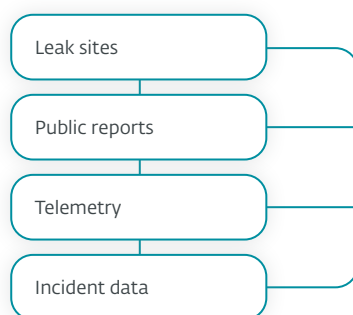
ESET THREAT INTELLIGENCE eCRIME REPORTS

ESET Threat Intelligence eCrime Reports **cut through the noise** with intelligence that's **built for action**. Each report gives you a clear picture of **how cybercriminal groups operate**, from their tooling and infrastructure to their monetization playbooks. You get insights that help you disrupt their business, not just detect their malware. Backed by ESET's global research teams, this intelligence is grounded in real-world telemetry, deep technical analysis and direct monitoring of underground activity. It's not just data – it's a **strategic advantage**.

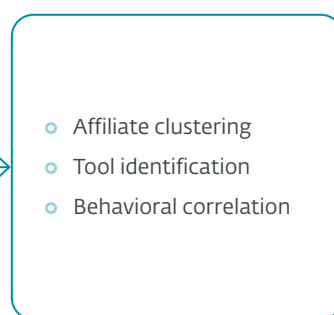
HOW IT WORKS

Instead of focusing on big-name RaaS groups and high-level overviews, we dissect the affiliates themselves – the actual criminals behind the attacks.

DATA SOURCES



ANALYSIS



OUTPUTS



WHAT SETS ESET eCRIME REPORTS APART

Proactive defense

Gain intel not just into eCrime groups, but into the affiliates who actually run the attacks. See how they work and anticipate their next moves – allowing you to stay one step ahead.

Operational efficiency

Use clear, curated insights from real incidents to cut through the noise. Make it easier for your team to detect threats, respond faster and focus hunts where it matters most.

Exclusive visibility

Go beyond public threat feeds with deeper insight into monetization tactics, infrastructure and affiliate behavior in practice – all backed by ESET's global telemetry and research.

What's in ESET Threat Intelligence eCrime Reports

Type of access	What's in the reports	eCrime Reports	eCrime Reports Advanced
Activity Summary MONTHLY	- Latest ransomware and infostealer campaigns distilled into clear, strategic insights - Who is targeted, how attacks unfold, what went wrong - Key lessons, IOCs and guidance to strengthen resilience	✓	✓
Technical Analysis PERIODICALLY	- Deep dives into specific threat actors (e.g. FIN7) - Full attack chain: initial access to data theft - Attacker tactics, tools, infrastructure, MITRE ATT&CK® mapping, IOCs	✓	✓
Monthly Digest MONTHLY	- Executive-ready overview of recent ransomware/infostealer activity - Key trends, notable incidents, emerging threats - Helps leadership assess risk and set priorities without technical complexity	✓	✓
eCrime feed	- Fresh and curated IOCs on ransomware gangs, their affiliates and infostealer campaigns - Available in the standard STIX/TAXII format	✓	✓
ESET LiveAI	- Uses eCrime insights to answer threat-related questions - Helps interpret incidents and attacker behavior - Makes threat intelligence instantly accessible for teams and decision-makers	✗	✓
Access to MISP server	- Direct integration with curated threat intelligence - Automatic IOC ingestion to enrich defenses - Streamlines workflows, speeds detection and supports incident response	✗	✓