Gen Threat Report Q2/2025

Key highlights

Gen | norton Avast LifeLock by norton MoneyLion

This quarter, Gen Threat Labs shines a light on PharmaFraud - a network of fake online pharmacies stealing people's data and money. Avast released free decryptor to combat the first AI-built ransomware while we saw tech support scams spreading on Facebook.

PharmaFraud: Fake pharmacies, real danger

1M

fake pharmacy attacks blocked

5,000+

fake sites linked to cyber gang MediPhantom

Thousands of slick-looking online pharmacies are actually run by one giant cybercrime network: MediPhantom. These sites prey on people looking for medications quickly, discreetly or at a lower cost. But, unfortunately, they are putting themselves, their identities and their bank accounts at serious risk.

Most targeted drugs:

- Erectile dysfunction pills
- Weight-loss meds
- Antibiotics

Tactics used:

- Malicious code in real medical sites
- AI-generated fake health blogs and reviews
- Search engine manipulation

Gen

Red flags:

- Crypto-only payments and unsecured checkouts
- Prescription drugs without proof of prescription
- Too-good-to-be-true prices

FunkSec: AI meets ransomware

The big picture:

- First known ransomware crew to **openly use generative AI**
- Asked for just 0.1 Bitcoin, but attacked schools, child protection orgs, retailers and more
- Gen built a **free decryptor** (distributed through Avast) to help victims recover without paying

Why it matters:

Cybercriminals are moving faster with AI. But good tech and global teamwork can still outsmart them.

Gen

The perfect crime? Why Facebook is a top weapon for cybercriminals

Facebook continues to be a hotbed for cyber scams, supporting massive spikes in both financial fraud (+340%) and tech support scams (14% of all Facebook threats) in the last quarter.

Why it matters:

Facebook is where your mom, your neighbor and your local teacher hang out online. When scams flood platforms like Facebook, they're not targeting corporations, they're targeting **ordinary people**. Everyday users are being tricked by **deepfake videos**, fake legal help pages and fraudulent investment opportunities, all looking deceptively real. The impact is personal: lost savings, stolen identities and a growing sense that it's getting harder to tell what's real online.

Facebook tech support scams:

- 14% of Facebook threats
- Fake messenger-style pop-ups asking people to fix their machines
- Locked browsers and fake call support prompts

Gen

Fast facts.
What to watch.

3 must-know stats

- 16 billion leaked credentials are still circulating
- 317% rise in malicious push notifications
- 100+ ransomware victims hit by AI-assisted malware in just 3 months

Trends to watch

1. **Cybercrime is scaling like a business:** Global teams. Big data. Branding. Even live-chat support.
2. **AI is now a criminal co-pilot:** Phishing templates, malware builds, social engineering, it's speeding everything up.
3. **Disruption ≠ Deletion:** Takedowns help, but criminals adapt fast. Malware like Lumma keeps coming.

Threat Category	Q2/2025 Surge
Financial Scams	▲ +340%
Sextortion Scams	▲ +100%
Data Breaches	▲ +21%
Malicious Push Notifications	▲ +317%
Remote Access Attacks (RATs)	▲ +62%
Breached Emails	▲ +16%

Gen

Threat	Gen's Response
AI-powered Ransomware	Discovered cryptographic flaw in FunkSec, launched **free decryptor**
PharmaFraud Scams	1M fake pharmacy attacks blocked
Facebook Scams	Blocked messenger-style tech support scams and deepfake finance baits

Read the full Q2/2025 Threat Report

Gen