



Threat Landscape Update

Three obstacles to navigate going forward

Bjørn Rasmussen, CTO Norway

28. April 2026



Agenda

3. Vulnerabilities

Industry trends and data
from our frontline operations



1. Cy-X

Cyber extortion and
the ransomware
threat landscape



2. Geopolitics

Hacktivism and other
state-aligned activities



\$whoami

- CTO for Orange Cyberdefense Norway
- GIAC certified CTI analyst
- 12+ years police & military service
 - NATO military operations
Afghanistan & Balkans
Combat engineer
 - Norwegian NCIS (Kripos)
National Cybercrime Centre
Investigating organized crime
and cyberattacks



1

Cy-X

**Cyber extortion and
the ransomware
threat landscape**



Methods & terminology

What we see, what we don't, and what we call it

All Cyber Extortion (Cy-X) attacks



Who's the "actor"?

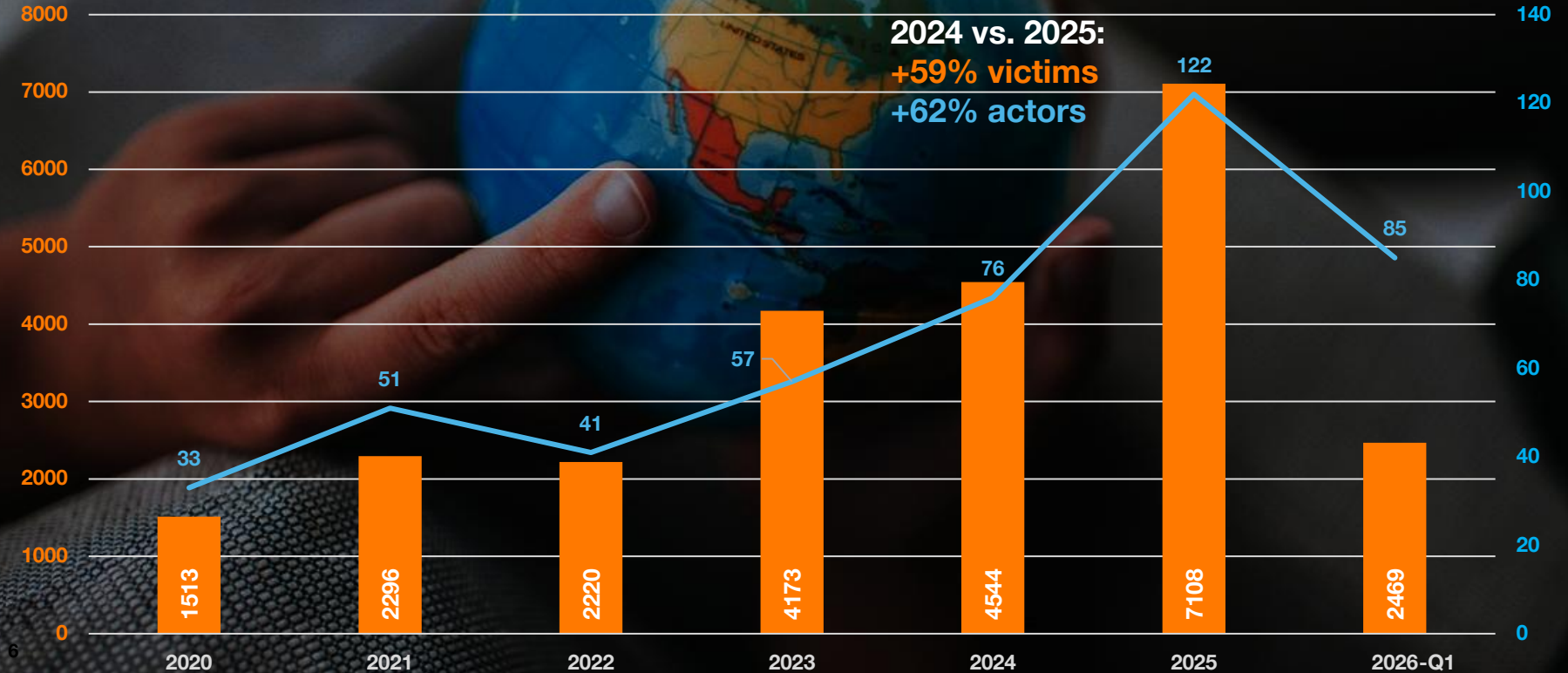


Cy-X Annual Global Development

Victims and Actors Count Observed on Leak Sites

n=23,654

n=244



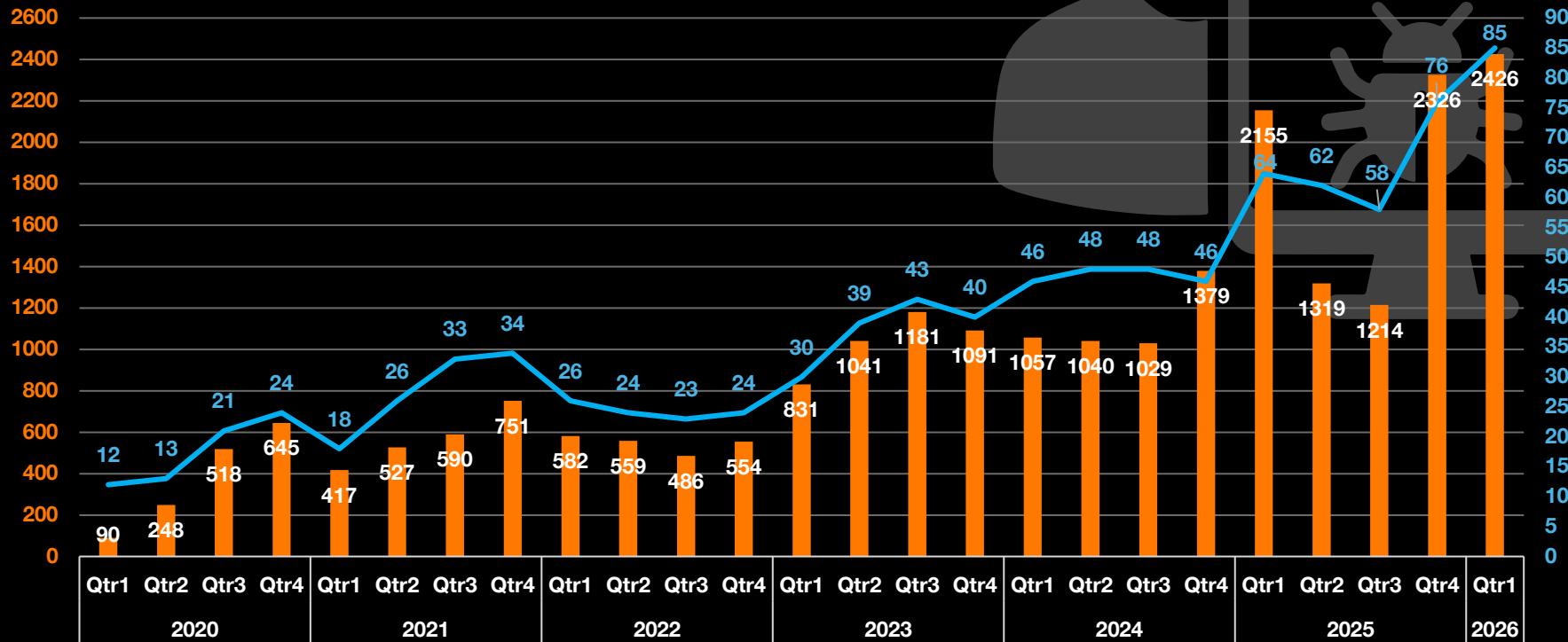
Cy-X Quarterly Analysis

Victims and Actors Count Observed on Leak Sites

n=23,654

n=244

Distinct Count of Victim Distinct Count of Actor

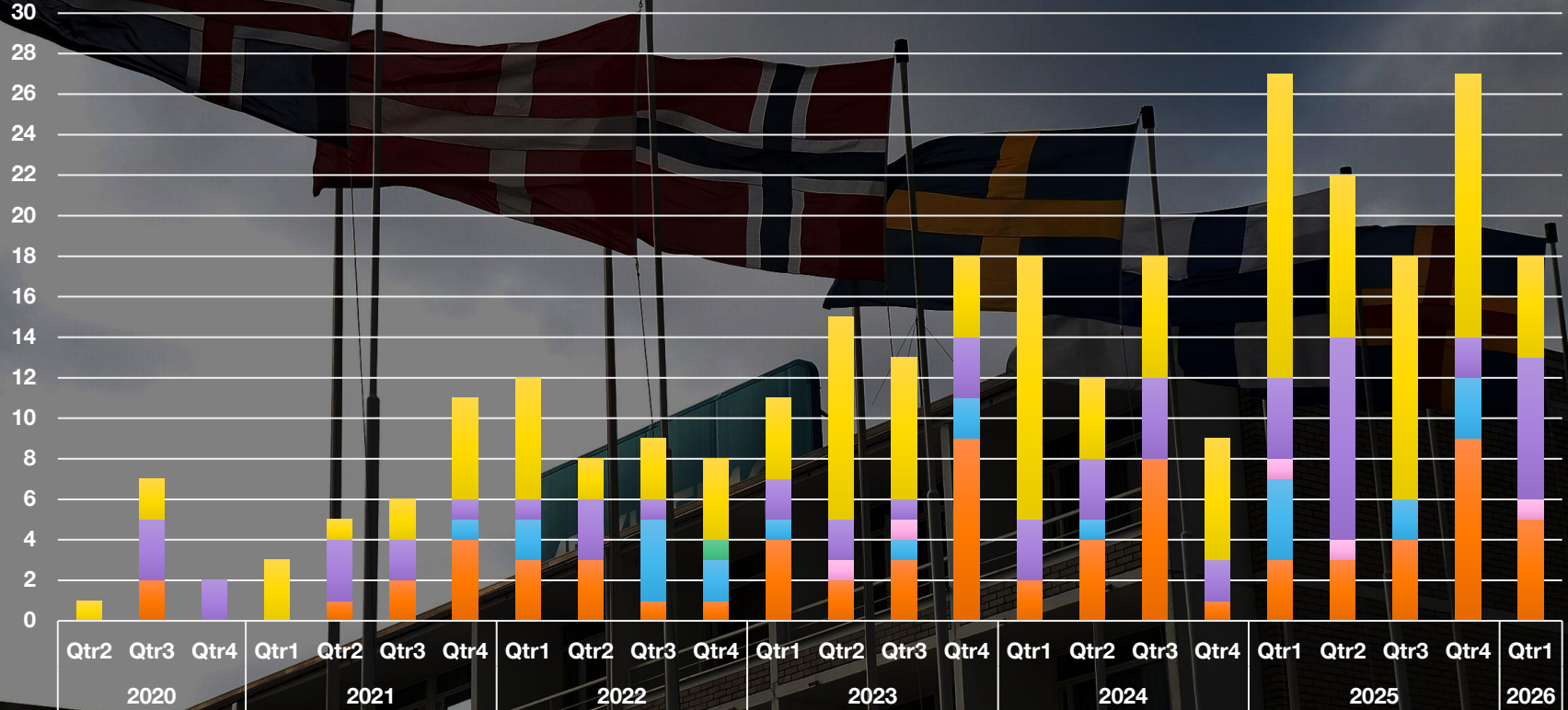


Cy-X Nordic overview

Total victims based in the Nordics

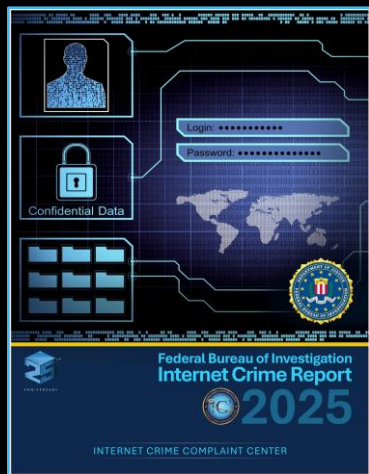
n=298

DK FI GL IS NO SE



Cybercrime Trends Q1-2026

Cy-X & ransomware

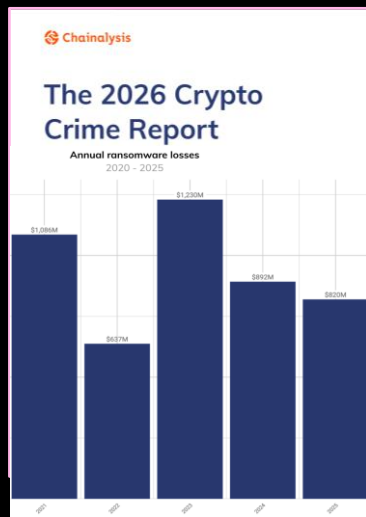


Cybercrime losses up 26% to \$20.9 billion

- According to FBI IC3 annual Internet Crime Report.
- BEC, investment-, and tech support scams caused the highest losses.
- Of cyberthreats reported to the IC3 in 2025, 36% were ransomware incidents, and 39% were data breaches.
- The IC3 identified 63 new ransomware variants.

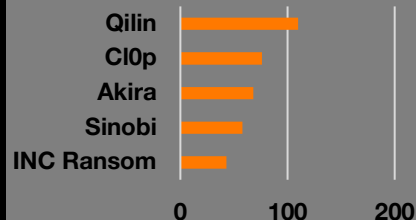
Ransomware payments stagnate

- \$820M in ransom payments in 2025 an 8% decline from 2024.
- Quote eCrime.ch data, showing record-high +50% YoY increase in claimed ransomware victims since 2024 (close to our +59%).
- Divergence between ransom payments and number of victims:
 - ✓ RaaS fragmentation, SMB shift
 - ✓ Poor code (ie. VolkLocker)
 - ✓ Law enforcement actions
 - ✓ CSIRT & regulatory pressure

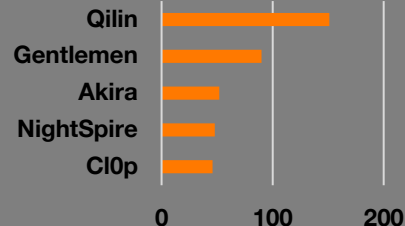


Top 5 Cy-X groups per month by claimed victims

January total: 703 victims



February total: 838 victims



March total: 928 victims



2

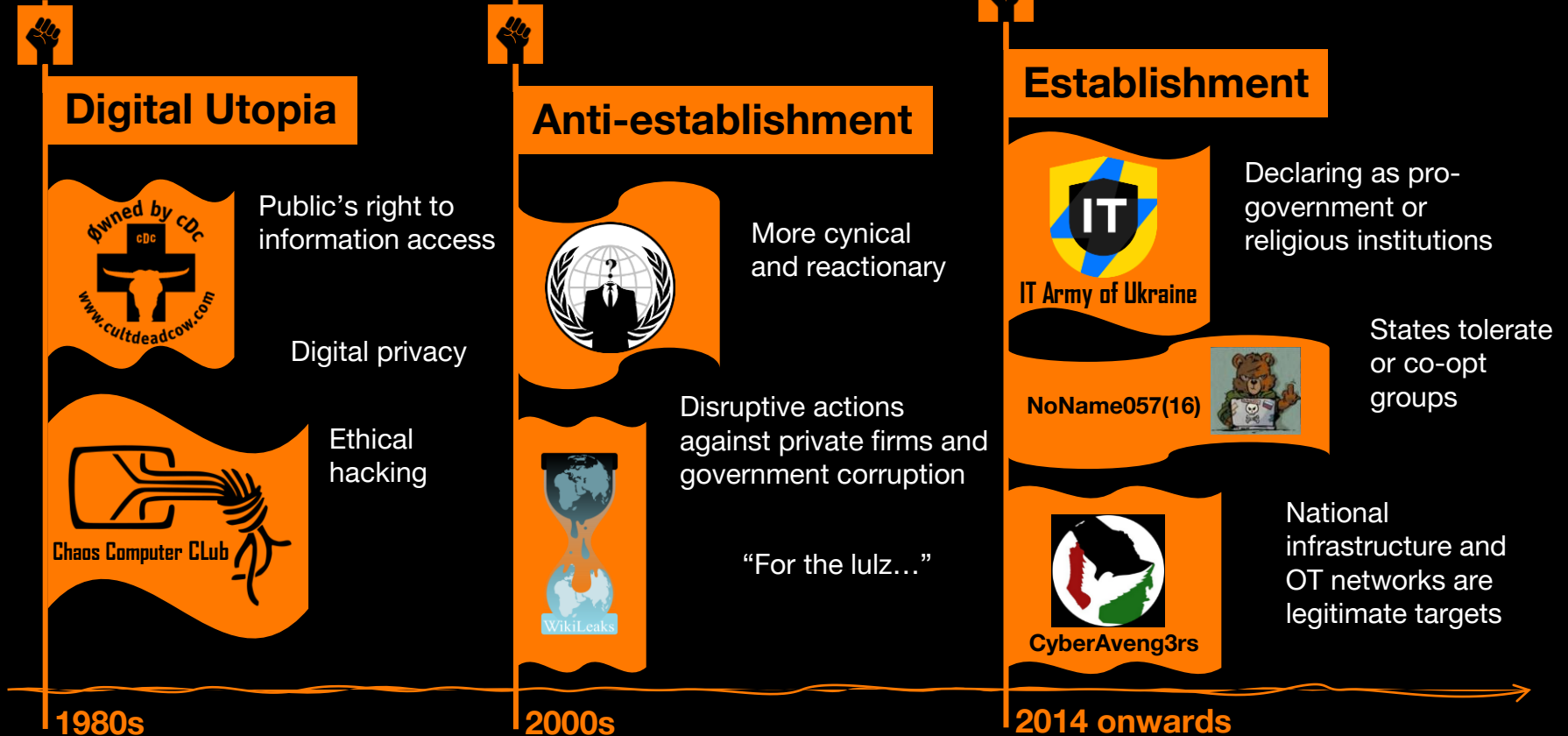
Geopolitics

Hacktivism and other
state-aligned activities

FISH
ON
FRIDAYS

Past development

The Three Eras of Hacktivism



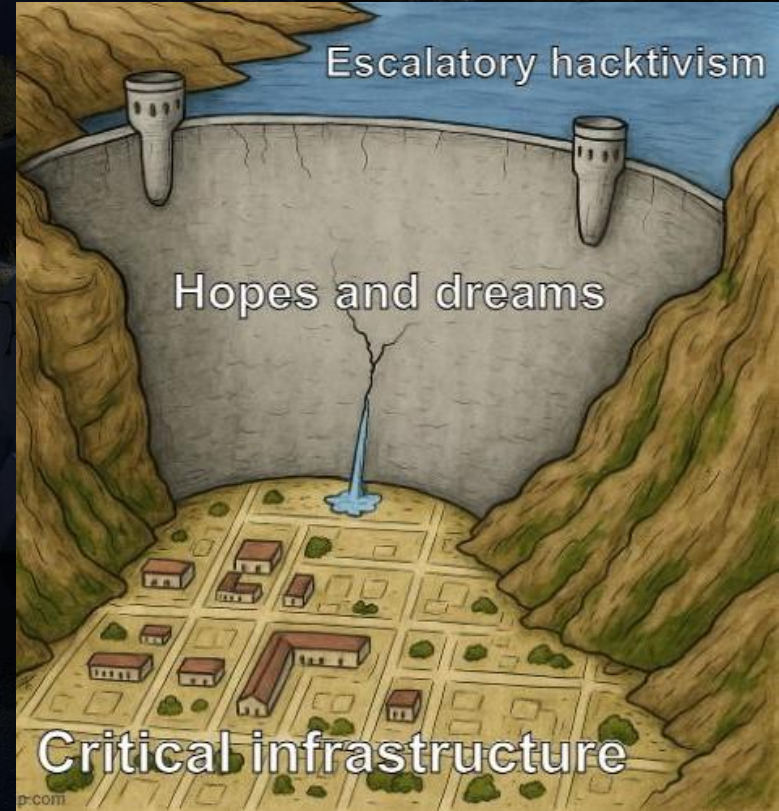
Escalatory Hacktivism

Targeting Critical National Infrastructure

- Norway, April 2025:
 - ✓ web-exposed panel w/weak pw
 - ✓ Discovered after 4 hours ~20k L «flooding»
 - ✓ Pro-russian «Z-alliance»
 - ✓ 3 min. Telegram video.
 - ✓ Case dismissed August 2025
- Sweden, mid-2025:
 - ✓ Attempted hack of thermal power plant
 - ✓ Swedish government attributed to pro-russian hackvist with ties to Russian intelligence

These groups are unconstrained by diplomacy in the way states are, and unconstrained by ROI in the way cybercriminals are.
This is going to get worse.

Ric Derbyshire (2025)
Principal Security Researcher
Orange Cyberdefense



Response

Accountability

For national security policymakers, knowing who is to blame can be more important than who did it

Jason Healy (2011)
Senior Research Scholar,
Columbia University Research

”

Emergence of state-aligned hacktivism make attribution even more difficult

Targeting of OT and critical national infrastructure may indicate a turn of pace

Most new regulations (NIS2) asymmetrically impact system owners over vendors



CERT analysis: State-aligned activities in 2026-Q1

China



- **Mustang Panda** targeting government and energy entities in Europe with **LOTUSLITE** and **PDFSIDER** malware.
- **UNC2814** targeting telco operators and government organizations in **40+ countries** using **GRIDTIDE** backdoor, GoogleSheets for C2 traffic.
- Palo Alto report 70 orgs in **37+ countries** targeted by **TGR-STA-1030** throughout 2025.



Trending sectors

government, energy, telco, technology,

Russia



- Attempted destructive attack with novel malware **DynoWiper** against Poland's energy grid attributed to **Sandworm**.
- Russian **Storm-1516** targets Germany and France with **anti-Ukraine propaganda** to undermine support.
- Russia restricts the use of **Telegram** and **WhatsApp** to promote **Max**.



Trending sectors

government, defense, energy, transportation

Iran



- **No drastic change** of cyber activity amid ongoing US-Israel-Iran conflict per 31.3.
- **Very limited spillover** to countries outside of the region.
- **Pro-Iranian hacktivism increase**; unverified data leak claims, overstated DDoS and a few wiper malware attacks.
- **Handala** hacks of Stryker MDM and FBI Director's email is somewhat noteworthy.



Trending sectors

Defense, government, healthcare

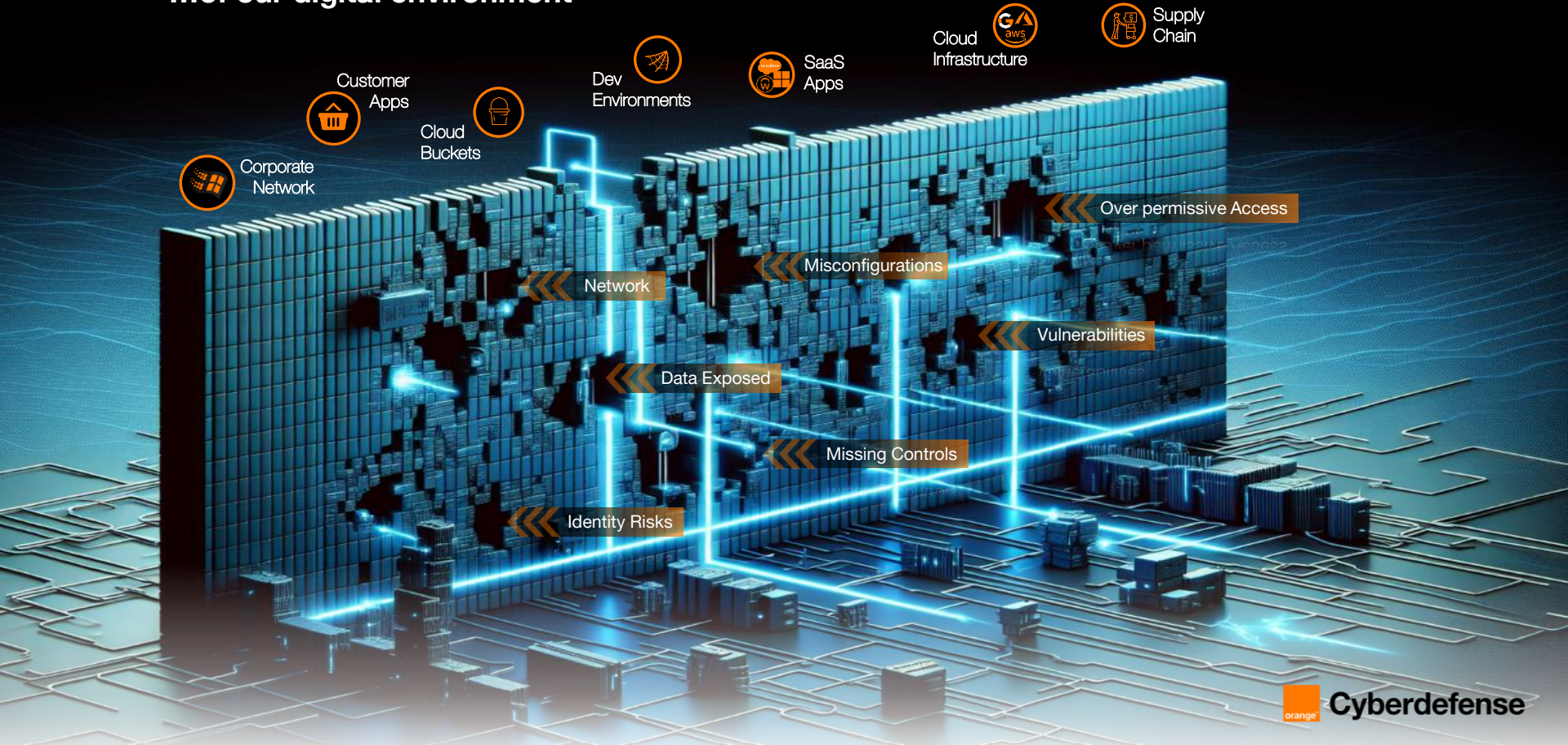
3

Vulnerabilities

Industry trends and
data from the frontlines

Complexity

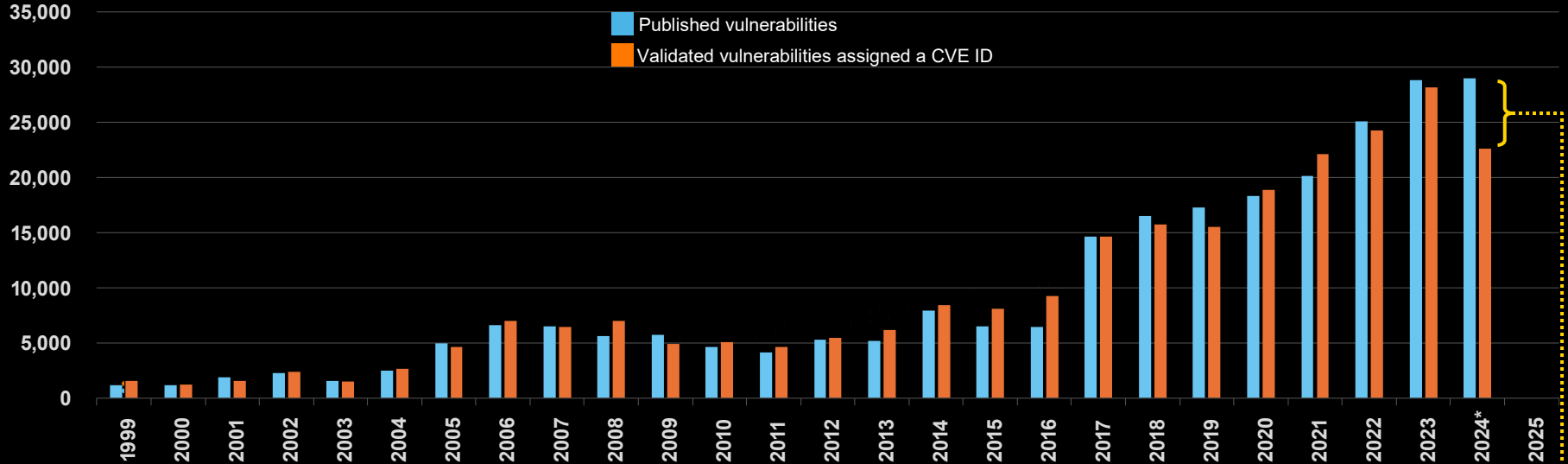
...of our digital environment



Backlog

...with global standards providers

US National Vulnerability Database per September 2024:



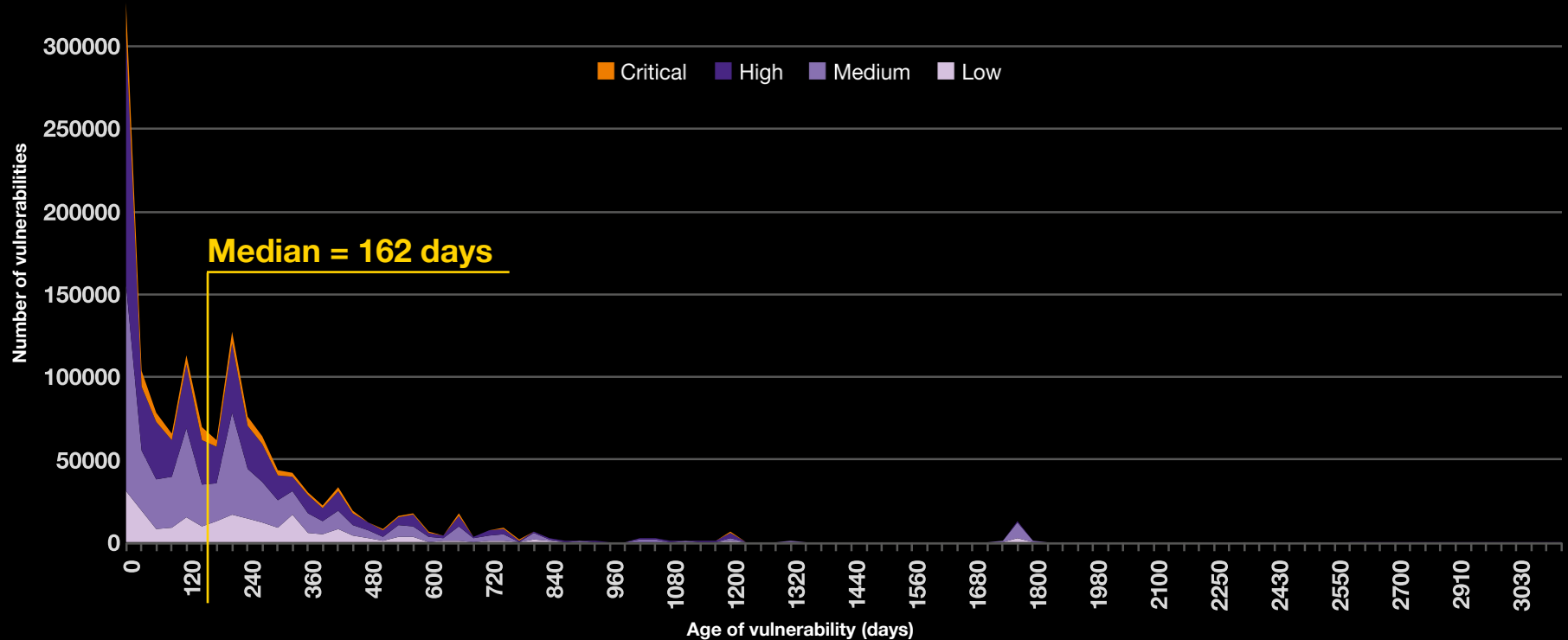
All time total: ~265,000 CVEs (>6% exploited)

2024 backlog: 18,167 CVEs

Backlog

...in vulnerability patching

Orange Cyberdefense 1 year of scannings (2024) ► 68 509 assets | 1 337 797 findings



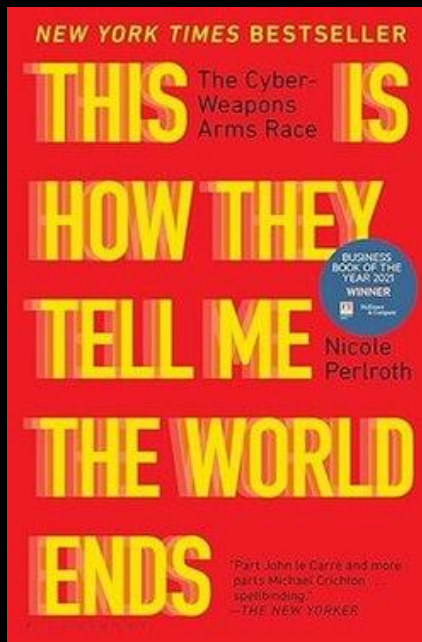
Market demand

...for vulnerability exploits, especially in security products



“We offer rewards from \$10,000 - \$7,000,000 for full exploit chains or previously unreported capabilities”

2017: Grey market for zero-day vulnerability exploits



2021: «Cyberweapons arms race»

NSM

NCSC anbefaler å erstatte SSLVPN/WebVPN med sikrere alternativer

Publisert: 15.05.2024 Oppdatert: 03.09.2024

Årsaken er gjentakende utnyttelse av sårbarheter. Overgang til anbefalt tiltak bør være på plass innen utgangen av 2025. For virksomheter underlagt sikkerhetsloven bør det skje før utgangen av 2024.

NCSC har over lengre tid observert og varslet om kritiske sårbarheter i VPN-løsninger som benytter Secure Socket Layer/Transport Layer Security (SSL/TLS), ofte kjent som SSLVPN, WebVPN eller klientens VPN.

Sårbarhetenes alvorlighetsgrad og aktørers gjentakende utnyttelse av denne typen sårbarheter gjør at NCSC anbefaler å erstatte løsninger for sikker fjernaksess som bruker SSL/TLS med sikrere alternativer. NCSC anbefaler Internet Protocol Security (IPsec) med Internet Key Exchange (IKEv2). Andre lands myndigheter har anbefalt tilsvarende.

Formålet med denne anbefalingen er å redusere sårbarhets- og angrepsflaten for sikker fjernaksess. Det er sannsynlig at det vil avdekkes nye nulldagssårbarheter i produktkategorien SSLVPN i fremtiden. Det må understrekes at løsninger som

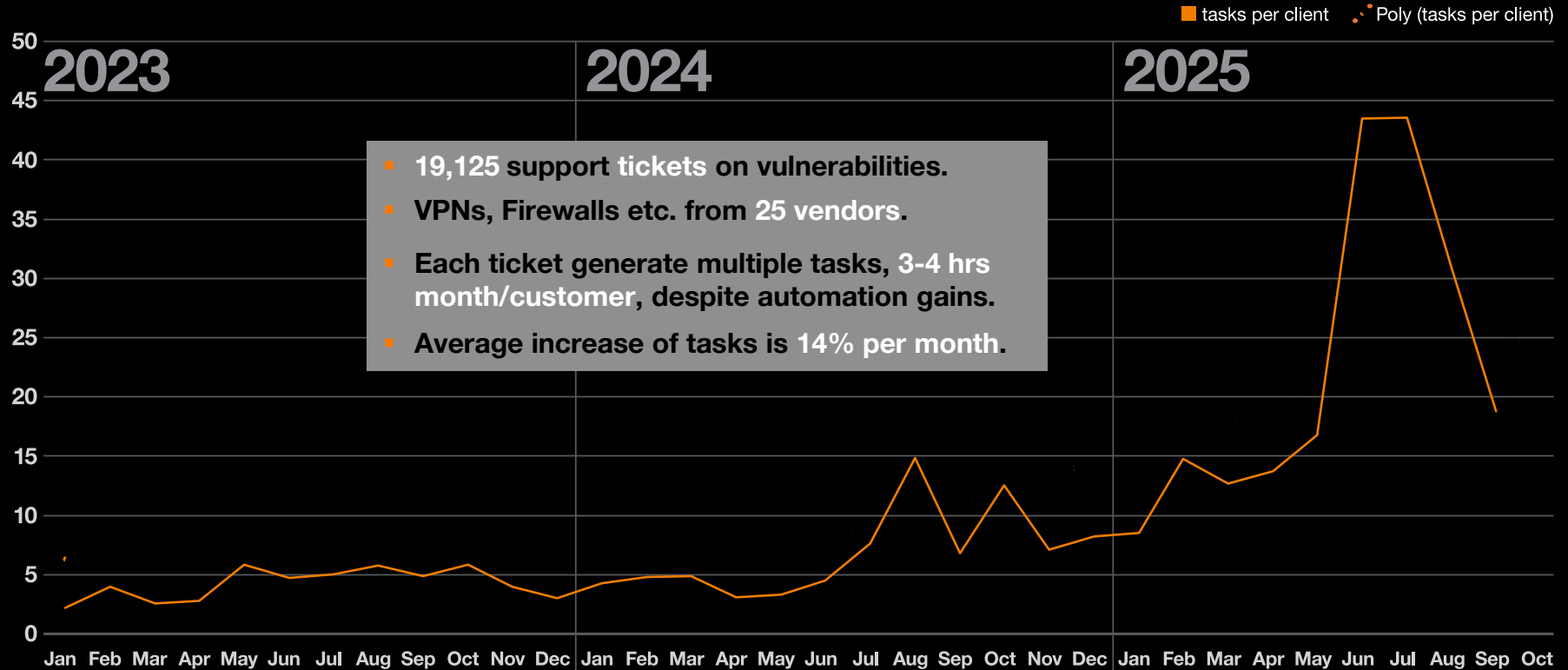
- Norwegian government: Stop using SSLVPN by 2026!
- Due to severe and repeated exploitation of vulnerabilities in VPN products



- 21.3% initial access via vulnerability exploitation (vs. 60% via phishing)
- 70% result in serious intrusions / malware (vs. 23% in phishing)

Security products are becoming preferred targets

...contributing to overall cybersecurity strain



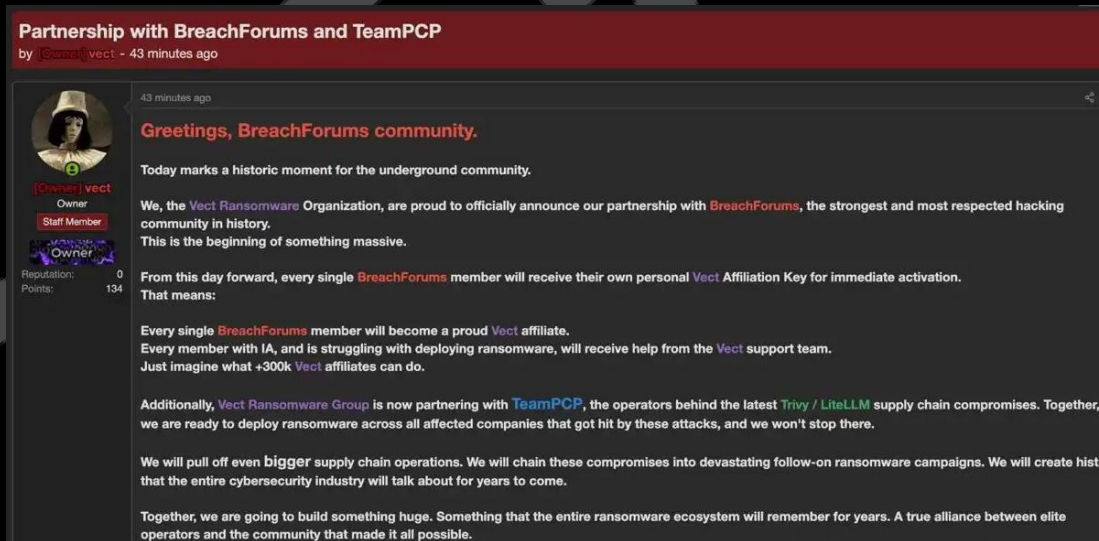
Vulnerability Trends Q1-2026

Supply Chain attacks on security and cloud apps

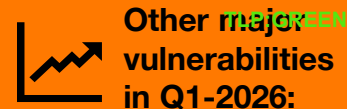


- TeamPCP announce collaboration with RaaS

- Alias: DeadCatx3, PCPcat, ShellForce, CanisterWorm
- Comprised Aqua Security's GitHub repos in March/April
- Supply-chain poisoning of Trivy, LiteLLM, Checkmarx, Telnix
- Trend since Q4-25 of hacking popular devs in NPM, GitHub, PyPI



1. orangepcyberdefense.com/no/blog/cert-news/critical-ivanti-epmm-zero-days-actively-exploited-what-organizations-need-to-know



- Critical Ivanti EPMM 0-days actively exploited¹ (CVE-2026-1281 and CVE-2026-1340).
- Cisco patch multiple flaws in Catalyst SD-WAN: CVE-2026-20127 exploited since 2023. Two linked flaws (CVE-2026-20128 and CVE-2026-20122) also being exploited.
- APT28 exploit 0-day in M365 (CVE-2026-21509) against Ukraine, Poland, Slovakia and Romania in Operation Neusplit.
- 2026-Q1 Microsoft Patch Tuesdays CVEs:
 - Jan: 114 reported, 1 exploited
 - Feb: 58 CVEs reported, 6 exploited
 - Mar: 8 CVEs reported, 0 exploited

GenAI and the vulnerability threat landscape

Summary and implications (per April 20th, 2026)

What?

- Mythos Preview: New Anthropic frontier LLM¹.
- Project Glasswing: Mythos early access to a group of software vendors for cybersecurity purposes².

So what?

- Vulnerabilities. Finding them. Making exploits. Creating, testing and deploying patches.
- From months/years to minutes/hours?
- Glasswing partners report vulnerabilities found in most major OS, open-source projects and SaaS applications.

What now?

- This isn't new (Opus 4.6 has similar capabilities).
- Possible GenAI lock-in for security vendors.
- Future price hikes? (inference is heavily subsidized).
- Continued monitoring. Anthropic tend to over-hype.

1. www-cdn.anthropic.com/8b8380204f74670be75e81c820ca8dda846ab289.pdf

2. www.anthropic.com/glasswing

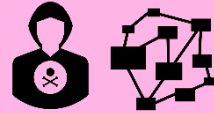
Defenders think in lists. Attackers think in graphs.

...as long as this is true, attackers win (John Lambert, 2014¹)



Start from the top of a never-ending list of vulnerability patches.

- Relying on general severity scores (i.e. CVSS and EPSS)



Start from wherever initial access is gained, then pivot to end target.

- Relying on navigating the **graph of security relationships**

Is it time for a crisis-mindset?

The conversations we should be having

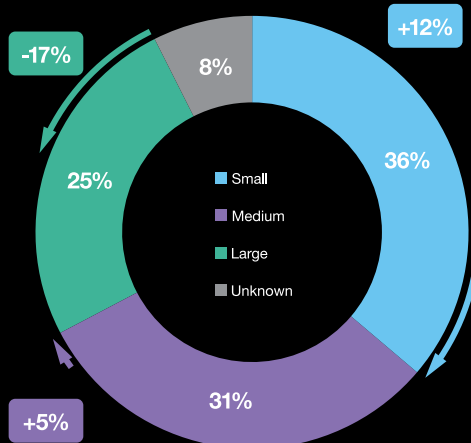
Different actors, single adversary

Distinctions between state-sponsored, criminal and hacktivist are blurring



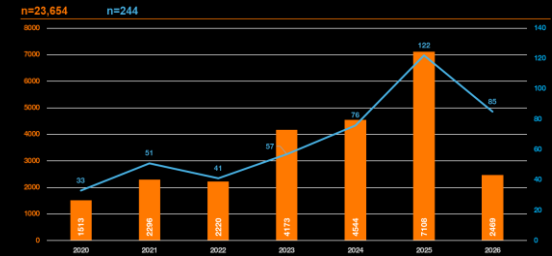
The victim is us

We see Cy-X victims in all countries and sectors, with increased targeting of small and medium businesses



The damage is real

Cyberattacks and geopolitics act as a cohesive pressure system against all levels of our trust-based society





Cyberdefense

Thanks!

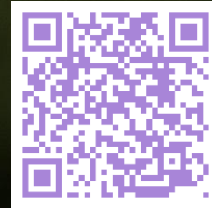
Questions?



Get
**Security
Navigator**



Get
**World
Watch**



Get
**Cybercrime
maps**



Get
**in
touch**