Cyberdefense

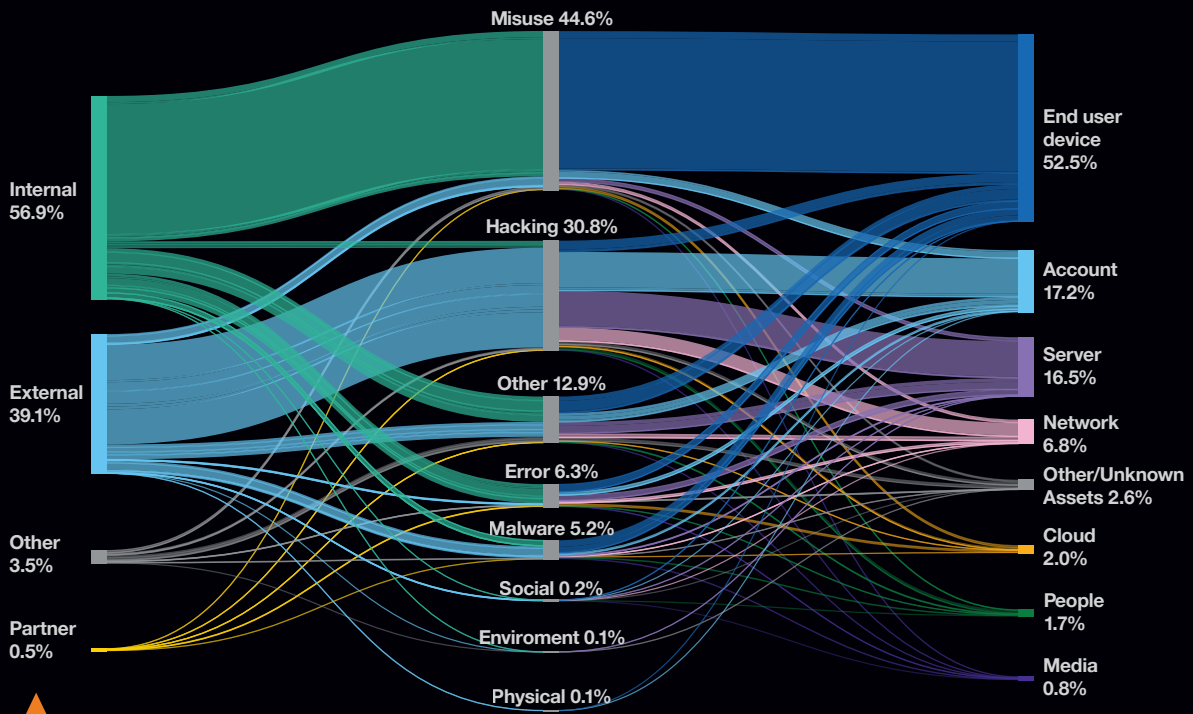
Security Navigator 2026

Research Summary

Key Data on Cybersecurity

- Orange Cyberdefense has built proprietary cyber threat intelligence capabilities over several years, leveraging our own and partner sources across 160 countries. **Our security operations centers detected 139,373 potential incidents, of which 19,053 were confirmed as true positive.**
- We are proud to share this year the **7th edition of our Security Navigator**. The past years allowed us to consolidate our analysis methods as well as put underlying threat trends into perspective. This report aims to help CISOs and security experts to refine their security strategy.
- **This research summary includes samples of the data and analysis in the Security Navigator 2026 report**

Funnel: 139,373 incidents ▶ 19,053 confirmed security incidents



Actors
Entities causing an incident

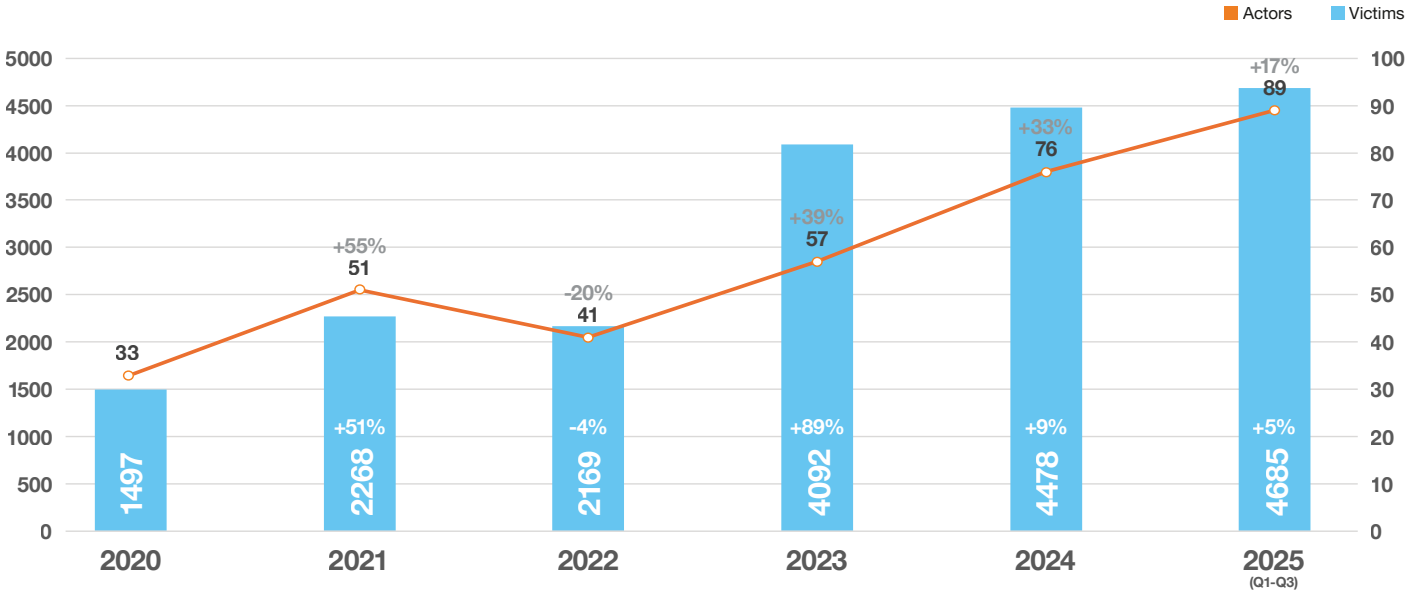
Action
What the threat actor(s) did

Asset
The asset that was targeted

Read the full story! Get your free copy of the Security Navigator on:
orangecyberdefense.com/navigator/

Cy-X Over Time

Victims and Actors Count Observed on Double-Extortion Leak Sites Since 2020



Key Findings and Topics:

Cyber extortion (Cy-X) has reached a new level. In just the first three quarters of 2025, there has already been a significant increase compared to the entire year of 2024. While the United States, Canada, and the UK remain the most affected countries, the trend is now spreading to smaller, non-English-speaking economies. The impact relative to GDP can be severe. By industry, retail and trade have set a dramatic record, with nearly an 80% increase in victims over the past 12 months, totaling approximately 300 victims in this sector in 2025.

Law enforcement efforts are intensifying, proving that cyber criminals are not beyond reach. It is an opportune moment for a criminological deep-dive. In a dedicated chapter, we examine for the first time what is known about apprehended cyber criminals. We explore which law enforcement actions were taken, who led and collaborated on these efforts, and what information is available about the demographics of those caught.

Steal now, decrypt later: Quantum computing is widely rumored to be the next major disruption in cybersecurity. We examine why this future technology is particularly relevant to encryption and highlight the potential challenges it may introduce. Additionally, we discuss practical steps for proactively addressing this issue and migrating to quantum-safe solutions, just as cybercriminals are already preparing for this new era.

Vulnerabilities are concerning on their own, but vulnerabilities within security products are especially alarming. Analysts at Orange Cyberdefense's global security operations center (SOC) recorded 19,125 tickets related to vulnerability advisories affecting 25 different security vendors, including firewalls, VPNs, and other perimeter defense technologies. Each ticket triggered multiple follow-up actions, or "tasks." Since 2023, the number of tasks has increased by 14% month over month, placing a significant burden on security teams.

Technology dependency and geopolitics: Today, all technology has become inherently political. It can be a weapon, a target, or a tool of influence. Technology enables political power projection, cyber operations, misinformation campaigns, and new forms of soft power. This dynamic is evident across the geopolitical landscape. Ongoing conflicts, such as Russia's war against Ukraine and those in the Middle East, continue to demonstrate how cyberspace amplifies and extends traditional forms of confrontation.

Read the full story! Get your free copy of the Security Navigator on: orangecyberdefense.com/navigator/

1. Political Factors

- **Power Projection & Balkanization:** Increasing reliance on technology platforms enhances power projection capabilities, enabling cyber and psychological operations, misinformation campaigns, and soft power exertion.
- **Cyber Balkanization:** Cyberspace is fragmenting along political, national, and ideological lines, driven by sovereignty concerns, censorship, and data control policies.
- **Technological Autonomy & Alliances:** Nations with limited indigenous tech capabilities face pressures to form alliances with dominant cyber powers, risking loss of autonomy and fostering a divided cyberspace aligned with superpowers.

2. Economic Factors

- **Platforming & Dependency Risks:** Dominance of platform businesses (cloud providers, AI models) risks market monopolization, creating dependencies that threaten economic stability and geopolitical leverage.
- **AI & Data Concentration:** The adoption of AI, especially large language models (LLMs), amplifies dependency on major providers, raising concerns over external influence and control.

3. Sociocultural Factors

- **Consumerism & Technology Adoption:** Growing consumer demand for advanced technologies (smart devices, LLMs, IoT) drives rapid adoption, often without comprehensive security considerations.
- **Security Gaps & Strategic Foresight:** The push for innovation necessitates a balanced approach, integrating strategic foresight, alliances, and resilience to mitigate risks associated with consumer-driven technology proliferation.

4. Technological Factors

- **Evolving Threats & Technologies:** Threat landscapes evolve alongside technological advancements such as AI, OT, and quantum computing.
- **AI & Generative Models:** AI accelerates threat capabilities, expanding attack surfaces and benefiting attackers more than defenders.
- **OT/IoT & Industry 4.0:** Increased connectivity in industrial environments introduces vulnerabilities not just in individual devices but in process understanding and manipulation, often underestimated in current security paradigms.

5. Threat Actors & Behavioral Dynamics

- **Criminal Actors:** Driven by profit, constrained by risk, focusing on extortion, scams, and crypto theft. Future trends depend on regulatory and law enforcement effectiveness.
- **State Actors:** Motivated by national/economic interests, engaging in espionage, psy-ops, and soft-power campaigns, with increasing impact driven by geopolitical developments.
- **State-Aligned Hacktivists:** Politically motivated, constrained by capabilities but escalating DDoS, leak, and cognitive attacks, potentially leading to kinetic impacts outside traditional domains.

About Orange Cyberdefense

Orange Cyberdefense is the Orange Group's entity dedicated to cybersecurity. It has 8,700 customers worldwide. As Europe's leading cybersecurity service provider, we strive to protect freedom and build a safer digital society. Our services capabilities draw their strength from research and intelligence, which allows us to offer our clients unparalleled knowledge of current and emerging threats. With 25 years of experience in the field of information security, 3,000 experts, 18 SOCs and 14 CyberSOCs spread around the world, we know how to address the global and local issues of our customers. We protect them across the entire threat lifecycle in more than 160 countries.

For more information check www.orangecyberdefense.com!