Research-driven insights to build a safer digital society

Security Navigator 2026

orange

Cyberdefense | Editions

Foreword

The cybersecurity landscape is evolving rapidly, shaped by innovative adversaries, geopolitical tensions, technological advances, and significant social changes. As we look toward 2026, one thing is clear: anticipation, resilience, and collective action are essential to securing our digital future. In this context, Orange Cyberdefense is pleased to share the findings from our research and global operations in our Security Navigator 2026.

Over the past year, our analysis has highlighted major shifts in the threat environment. Cybercriminals, driven mainly by financial gain, have increased their focus on extortion, scams, and unpatched vulnerabilities, using methods that are becoming more organized and efficient. Recorded extortion incidents have risen by 45%, with small and medium-sized businesses (SMBs) increasingly affected. This trend reveals both their heightened vulnerability and the broader economic risks involved, as these companies are a critical component of the economy. Hacktivism, once primarily ideological, has become more closely tied to geopolitical agendas. Last year we found that 96% of a particular Russian-aligned hacktivist group's actions targeted Europe. This underlines the impact of hacktivism on regions involved in geopolitical conflicts.

These developments reinforce an important reality: cybersecurity has become a societal issue. Protecting SMEs is not optional, it is essential to achieve economic stability and national resilience. This responsibility requires trusted and sovereign cybersecurity capabilities, built on robust threat analysis.

For several years, Orange Cyberdefense has been investing in the development of its own Cyber Threat Intelligence, designed to be both accurate and adapted to the local context of its clients, while continually expanding data sources and improving our ability to anticipate emerging threats.

The malicious use of artificial intelligence, including automated phishing, deepfakes, and the exploitation of vulnerabilities, is also accelerating. As adversaries adopt AI to scale their operations, the need for consistent protection and response become increasingly urgent. These attacks are no longer isolated; they form part of a broader, global challenge. The integration of AI into essential systems also introduces new weaknesses, expanding the attack surface. While AI may advance defensive capabilities, it also creates fresh risks, making the security and reliability of AI itself a strategic priority. Defensive AI must be auditable, secure, controllable, and trustworthy.

Beyond AI, another major shift is already emerging; quantum computing. This technology has the potential to transform encryption and data protection, but it may also render current cryptographic standards insufficient. Just as AI has required us to rethink our strategies, quantum computing will challenge the foundations of digital trust and demand greater foresight and adaptability.

In this context of rapid and complex change, we are grateful for the trust our clients place in us to help protect what matters most. We remain committed to applying our expertise, using reliable, advanced technologies to safeguard their business and contribute to a safer digital environment. Thank you for your continued trust. We invite you to explore our Security Navigator 2026 and draw on its insights to support your security decisions in the year ahead.

Hugues Foulon

Directeur Exécutif,
CEO Orange Cyberdefense

You can return to this page using this icon!

Table of Contents

The Themes That Shaped the Year

Charl van der Walt - Head of Security Research

State Actors and Critical Infrastructure

- **Night Dragon (mid-2000s onward):** A China-linked campaign against energy and defense firms globally illustrated the move from opportunistic hacking to long-dwell, state-sponsored industrial espionage[1].
- **Volt Typhoon Botnet Disruption (Jan 2024):** The U.S. government announced a court-authorized operation to dismantle a botnet of compromised routers used by the Chinese state-sponsored group Volt Typhoon in pre-positioning within U.S. critical infrastructure[2].
- **Salt Typhoon Telecom Breaches (Oct 2024):** A global compromise of major telecom networks, attributed to the Chinese-linked group Salt Typhoon, exposed how state actors could access the communications of government officials and a multitude of civilians[3].
- **U.S. Advisory on Critical Infrastructure Targeting (Feb 2024):** The U.S. and allied agencies issue a joint advisory declaring that Volt Typhoon had compromised IT networks across communications, energy, transport and water sectors, marking a milestone in recognizing state cyber power as a strategic threat[4].

The Salt Typhoon operation is an expansive state-sponsored intrusion campaign into global telecommunications infrastructure that emerged publicly in late 2024. U.S. officials confirm that the campaign affected at least nine major U.S. telecom firms, as well as several network operators world-wide. Compromises enabled hackers to access court-authorized wiretap gateways, geolocate multitudes of users, and record phone calls. Salt Typhoon remains active, with investigations indicating that the campaign spans 80+ countries and targets beyond telecoms, including satellite operators and defense-connected networks[5].

The campaign revealed a continued shift in state behavior, achieved by a classic network intrusion playbook. The attackers infiltrated critical infrastructure and telecom networks worldwide by exploiting known vulnerabilities, then methodically established long-term, covert access. Anyone involved in offensive security work in 90s and 2000s would readily recognize the well-understood patterns of network intrusion they deployed, yet the scale and state backing make this campaign significant.

The Salt Typhoon attackers gained access through vulnerable network edge devices, specifically internet-facing routers, VPN gateways, and firewalls. Despite being a bona-fide Advanced Persistent Threat (APT), no zero-day exploits were identified[6].

Two of the exploited vulnerabilities were Ivanti VPN gateway flaws disclosed in early 2024 and another was a Palo Alto Networks firewall bug first observed in April 2024. Older, known issues in Cisco router software were also exploited. All of these were publicly disclosed vulnerabilities with patches available[7].

Salt Typhoon's operatives executed a classic intrusion playbook: exploit exposed entry points, establish persistent control over infrastructure, steal credentials, and pivot[8]. After breaching the perimeter, the intruders deployed classic hacking tricks like changing network device configurations to ensure persistence, which allowed them to maintain long-term access without detection. Next, they harvested credentials, captured authentication traffic to obtain high-privilege credentials. With valid admin passwords in hand, the attackers could move laterally across connected systems at will. None of these tactics are new or unexpected[9]. The shock was in the breadth and patience of the operation, which has impacted hundreds of organizations over the past few years.

The MITRE foundation describes Salt Typhoon as a "People's Republic of China (PRC) state-backed actor that has been active since at least 2019"[10]. But the actor is also an example of how cyber operations have become a standard instrument of state power globally. Not only by China, but by many countries, as a routine element of competition and conflict as "a standard tool of statecraft and warfighting" on par with traditional military assets. Nations like Israel, Russia, North Korea and Iran likewise integrate cyber intrusions into their statecraft for espionage, coercion, and battlefield preparation, as do most western countries[11]. The Belfer Center National Cyber Power Index (NCPI) reported in 2022 that major cyber powers in the world were the USA, China, and Russia, but the UK, Netherlands, France, Iran, Republic of Korea and even Vietnam also made the top 10 list[12]. Indeed, an October 2025 advisory by China CERT (CN-CERT) describes a major network attack executed by the American National Security Agency (NSA) against the Chinese National Time-Keeping Center[13].

We are living through an era in which cyber power is a key instrument of statecraft for many nations[14].

The long-term penetration of telecom backbones and critical networks by Salt Typhoon also suggests that state-sponsored hacking is increasingly focused on pre-positioning assets inside foreign infrastructure and silently gathering strategic intelligence. It is part of a broader paradigm in which many governments harness cyber espionage as a regular practice of international statecraft, and defenders must assume that determined foreign actors are actively probing and infiltrating systems.

Salt Typhoon also prompts us to adopt an "assume-breach" mentality and embrace zero-trust architecture as standard practice. We must sadly operate under the assumption that intruders may already be inside our networks or will eventually find a way in. This means continuously verifying every user, device, and connection as if it were untrusted, no matter its location or credentials. A compromise of one router or vendor should not grant an attacker unfettered access across an enterprise. Strict identity verification, least-privilege access controls, and internal network segmentation are essential to contain breaches when they occur. Moreover, Salt Typhoon's persistence shows that modern defense is as much about resilience - detection, investigation and recovery - as it is about prevention. This means increased focus on continuous monitoring, threat hunting, cross-sector intelligence sharing, and rigorous incident response planning.

But beyond the immediate technical impacts, campaigns like Salt Typhoon inflict more subtle damage by undermining confidence in the security of critical systems. The revelation that hackers accessed the core routers of telecom providers and even compromised lawful intercept systems erodes public and institutional trust and has a profound psychological impact. The unprecedented guidance urging officials to adopt end-to-end encrypted messaging (because their regular phone communications were presumably compromised) sent a clear signal that the integrity of telecom networks could no longer be taken for granted[15]. Ironically, this US government advisory coincides with the proposed European Union "Chat Control" law, which would require the scanning of private digital communications, including encrypted messages, to detect harmful content, thus undermining the security of communication tools like Signal[16]. The UK's Online Safety Bill is already law, bringing with it the prospect that tech firms are forced to scan people's messages - ostensibly for child abuse content[17].

By sowing doubt about whether citizens and organizations can rely on essential infrastructure, such a loss of trust is itself a strategic win for adversaries. A dilution of trust can strain alliances, damage the credibility of institutions, and scare the public, thus achieving effects far beyond the theft of data.

Preserving trust in the digital systems that underpin society is therefore not just an IT issue but a national security imperative.

Maintaining Trust

It should therefore be clear that the pervasive technical debt and apparent complacency that enabled the Salt Typhoon breaches are no longer tolerable in an era of active state cyber threats. The accumulation of vulnerabilities for the sake of expediency has proven catastrophic. An insistence on security Return On Investment (ROI), focus on compliance, and naive delegation to IT, can simply no longer be considered acceptable. Leadership must treat cybersecurity as a core operational priority, not an optional expense.

Salt Typhoon's legacy should be a collective resolve to harden the digital backbone of our societies. Earning and maintaining confidence in our digital environments will require leadership to address long-standing technical debt, treat cybersecurity as a mission-critical and societal imperative, and redesign defenses around principles of zero trust and resilience.

- **Dillon Peens** - Advisory Associate

AI: Workhorse, Weapon or Weakness?

- **June 12, 2025:** Researchers publish details of "CVE-2025-32711" zero-click prompt injection vulnerability (EchoLeak) in Microsoft 365 Copilot, one of the first known zero-click attacks that exploited an AI agent[18].
- **August 28, 2025:** Researchers at NYU Tandon School of Engineering publish findings suggesting that large-language-models (LLMs) can autonomously carry out full ransomware attack chains[19].
- **2024 / 2025:** OpenAI reports that more than 60 malicious operations and networks had been disrupted after misusing its models for malware creation, phishing activity and disinformation campaigns[20][21].
- **2024-2025:** Reports reveal that Anthropic burned approximately US $5.6 billion in 2024 while earning between US $400-600 million in revenue[22].
- **November 13, 2025:** Anthropic describes an AI-orchestrated campaign by a Chinese state-sponsored group that manipulated its Claude Code agent to conduct largely automated reconnaissance and intrusion attempts against about thirty global targets[23].

The cybersecurity implications of generative and agentic artificial intelligence have become a defining concern for the industry. The question is no longer whether AI will reshape the security landscape but how profoundly it will alter the relationship between attacker and defender. We continue to assert that (at least for the short term) the efficiencies offered by GenAIs will benefit attackers more than defenders[24].

The offensive potential of AI has already been demonstrated, albeit with limited real impact on the threat landscape. State-aligned actors from China, Iran, and Russia have used large language models to create phishing content, debug malware, and generate convincing disinformation[25]. OpenAI has documented more than twenty campaigns over the past year that misused ChatGPT for such malicious purposes[26]. Cyber extortion groups have also integrated AI into their operations. The Black Basta collective reportedly used ChatGPT to rewrite malicious code, craft emails in multiple languages, and test malware performance[27]. Meanwhile, researchers at New York University have shown that large language models are theoretically capable of executing complete ransomware attack sequences autonomously[28].

As we predicted in last year's report, AI has itself bloated the attack surface with an expanding layer of vulnerabilities that stretches from model inputs to integrations, data pipelines, and vendor ecosystems. Each model, plugin, and integration becomes a new point of exposure. The "EchoLeak" campaign against Microsoft 365 Copilot revealed how a carefully crafted email could deliver malicious instructions to an embedded AI assistant, leading to silent data exfiltration[29]. This occurs because modern language models process all input as context and thus do not distinguish between commands and content. The result is a fundamental vulnerability known as prompt injection (or "LLM scope violation"), which we must understand as an architectural flaw rather than a bug or configuration error[30]. Unsurprisingly, recent reports described AI browsers as "home to a host of known and unknown cybersecurity risks"[31].

The surrounding infrastructure magnifies this risk. The Salesloft-Drift breach in 2025, in which attackers exploited OAuth tokens for an AI-integrated chatbot, showed how third-party AI services can become conduits for large-scale compromise[32]. Each connected agent extends a company's digital footprint in unpredictable ways.

When an AI tool holds privileged access to customer data, code repositories, or communication channels, its compromise can escalate a single intrusion into a systemic breach. In effect, AI has become an additional form of connective tissue within enterprise systems that adversaries are already learning to manipulate.

At the same time, agentic AI is promising to transform defensive capabilities. AI systems can analyze information, act autonomously, and adapt to feedback. OpenAI's newly released Aardvark project is a notable early example[33]. Aardvark can audit code repositories, identify vulnerabilities, and suggest patches without direct human input. It represents a shift toward AI that does not merely assist analysts but participates in defense. But at this early stage its true efficacy, reliability, and resilience against adversarial manipulation remain to be proven. A recent report from Empirical Security for example argues that AI "are not yet a viable replacement for purpose-built tools in vulnerability exploitation prediction."[34] Moreover, as organizations adopt such tools, they will also need to secure them as carefully as any other critical infrastructure.

Business and geopolitical risks amplify these technical challenges. The economics of AI remain unstable, with many companies operating at enormous losses. As Wicus Ross argues later in this report, the tech industry's current investment into AI seems very unlikely to pay off. Anthropic's reported $5.6 billion in operational spending during 2024 exemplifies this imbalance[35]. Should market consolidation or investor retrenchment occur, enterprises relying on unviable vendors may find their AI tools unsupported or abruptly withdrawn. Meanwhile, in the context of widespread concerns about national sovereignty, the geopolitics of AI are creating new assymetries. The platforms and clouds that host major AI models threaten to become instruments of state influence, particularly in the competition between the United States, China, Europe and Gulf states[36]. Dependence on a single nation's technology stack introduces exposure, not only to cyber risk but also to regulatory and diplomatic disruption.

AI must therefore be approached as both an opportunity and a potential liability. It may eventually strengthen security operations[37] but could also weaken them if poorly implemented or insufficiently governed. The challenge is not simply to counter the risk from attackers using AI, but to ensure that defenders adopt it safely, deliberately, and with a clear understanding of its limits.

AI integration across modern systems makes it inseparable from the rest of the attack surface. It can be poisoned through its data, manipulated through its prompts, hijacked through its integrations, or subverted through its autonomy. Security leaders should therefore treat every AI model and agent as a privileged asset requiring dedicated controls, audit trails, and monitoring.

AI in the hands of attackers is a problem and AI in the hands of defenders is a potential solution. But AI as an infrastructure layer embedded in everything from code review to customer interaction is a long-term risk that demands serious consideration.

The future of cybersecurity may depend, not only on how effectively AI can protect us but on how well we protect the AI itself, and how well we can protect ourselves from the AI.

Hacktivism and the Blurring Threatscape

- **7 April 2025:** Attackers seized control of the Bremanger dam in Norway, opened floodgates, and released 500 litres of water per second for four hours. Later attributed to Russian hackers by Norway's security service[38].
- **7 May 2025:** The National Cyber Security Center (UK) report that the pro-Russian hacktivist group NoName057(16) had claimed a three-day DDoS campaign against several UK public sector websites[39].
- **17 June 2025:** Predatory Sparrow claim to have destroyed data at the Iranian state-owned Bank Sepah, causing outages for customers[40].
- **16 July 2025:** Europol announce the global "Operation Eastwood" disrupted the infrastructure of NoName057(16), marking a coordinated law-enforcement action against a hacktivist network[41].
- **14 August 2025:** Norway's intelligence service publicly attribute the dam intrusion and rising threat of pro-Russian cyber actors to the event.
- **29 October 2025:** The Canadian Center for Cyber Security alerts that hacktivist groups had breached water, energy and agricultural OT/ICS systems in Canada, manipulating water pressure and manipulating temperature and humidity levels[42].

As we've previously reported, hacktivism has entered its "establishment" era. Once a form of digital protest directed against institutions of power, it has evolved into a complex ecosystem of state-aligned and ideologically driven actors that often serve as informal extensions of geopolitical influence. The term "hacktivism" itself today conceals more than it reveals. It no longer refers simply to fringe collectives with political messages, but to distributed, collaborative and often state-tolerated movements capable of real-world disruption and wide-spread cognitive manipulation.

This evolution matters because it disrupts how security professionals classify and respond to threats. The boundaries between hackers, activists, and state actors are dissolving. Groups such as NoName057(16) and Killnet operate independently, but in support of their host states, attacking adversarial governments and institutions while maintaining plausible deniability for their state beneficiaries. They may act without clear coordination but align ideologically with state agendas. These actors are both patriots and proxy, unconstrained by the legal, strategic, diplomatic, or reputational limits that restrict government operators. They are motivated by ideology and attention, not profit, and they thrive on any form of visibility.

Recent events illustrate the implications of this shift. Distributed-denial-of-service operations remain the most visible form of hacktivism, yet the targets and intent are changing. Campaigns by pro-Russian groups in 2025 disrupted British public services and European infrastructure, not for ransom or data theft but to broadcast political narratives and erode confidence in institutions[43]. More concerning are incidents that blur into the physical world. In Norway, attackers remotely manipulated a valve at the Bremanger dam, prompting fears of cyber-physical escalation[44]. Around the same time, a Russian-aligned group claimed access to a water-utility system (though that later proved to a security honeypot)[45].

More recently, Canadian authorities have reported that hacktivist groups breached critical infrastructure, including water, energy and agricultural sites[46]. The attacks involved tampering with pressure valves at a water facility, manipulating an automated tank gauge at an oil and gas company and exploiting temperature and humidity levels at a grain silo on a farm. The symbolism of these incidents is as potent as the technical impact. Demonstrating reach into critical systems, even when the damage is contained, catalyzes exactly the kind of panicked narratives the actors desire.

The goals of hacktivism have shifted from technical disruption to cognitive persuasion. The Canadian Center for Cyber Security has warned[47], as we predicted previously, that industrial control systems exposed to the internet are increasingly abused for performative attacks that aim to attract attention rather than cause material harm. The spectacle itself is the weapon. Contemporary state-aligned hacktivists operate in the cognitive domain, seeking to broadly influence perception rather than achieve specific technical objectives. Their operations exploit the psychology of fear and outrage as much as the mechanics of intrusion. Every breach claim, verified or not, becomes a story amplified through sympathetic media channels and social networks.

This new threat class is stretching our traditional paradigms for defense. Firstly, security strategies require businesses to consider how they can work together to collectively protect their environments and societies, rather than just themselves. Law enforcement also faces challenges. Operations like Europol's takedown of NoName057(16) infrastructure in mid-2025 disrupted activity and illustrated encouraging commitment and capability[48]. The group, on the other hand, dismissed the law enforcement operation on its Telegram channel, discounting "all this nonsense of foreign special services" and reaffirming its commitment to support Russia[49]. Sanctions and arrests may be less of a deterrent to actors who see their actions as patriotic duty or ideological service. Even coordinated state responses struggle against a decentralized ecosystem of volunteers and influencers who can re-form faster than bureaucracies can act. This new environment demands a reconceptualization of deterrence and defense.

The risk is twofold. First, the risk of serious cyber-physical attacks is growing. While most hacktivist incidents remain low impact, the "addiction" of hacktivist groups to increased visibility and impact suggests they will continue to seek bigger and bolder opportunities. The growing familiarity of such groups with industrial and operational technology increases the likelihood of genuine harm. Attacks that were once digital graffiti could, by accident or intent, evolve into events with physical consequences. Second, the convergence of criminal, ideological, and state interests creates a synergy between information operations and infrastructure attacks. The target is no longer a single system but the public mind: to exhaust trust, polarize societies, and reshape narratives.

Defending against this class of threat requires more than technical resilience, it demands a societal approach. Companies and governments must acknowledge that the target is often collective cohesion and confidence. Keeping a website online during a DDoS attack does not sufficiently address the wider objective of undermining civic or institutional legitimacy. Collaboration between public and private sectors must therefore extend beyond incident response into coordinated communication, education, and cognitive defense. The challenge is not only to secure systems but to preserve the coherence of the societies that depend on them.

Hacktivists, Criminals And Everything in Between

Hacktivism has always reflected its political moment. In its establishment era it mirrors a world where conflict is constant, boundaries are porous, and narratives are as contested as territory. For security leaders, this is no longer a technical nuisance to be filtered or patched away. It is a strategic threat that must be met with shared awareness, cross-sector coordination, and a recognition that cyber security is inseparable from societal security.

- **Bjørn Kristian Rasmussen**
  CTO Orange Cyberdefense Norway

Supply Chain Weaknesses

- **March 6, 2025:** The European Cyber Resilience Act (CRA) is poised to reshape the security requirements for all hardware and software products within the EU[50].
- **March 26, 2020:** Software updates from SolarWinds' Orion platform contains malicious code (the "Sunburst" backdoor) and affected thousands of organizations[51].
- **July 19, 2025:** Microsoft publicly report that on-premises SharePoint Servers versions were under active attack via a critical zero-day vulnerability. Large-scale exploitation follows[52].
- **August 8-18, 2025:** OAuth token-theft campaign via Salesloft's Drift integration compromised several organizations' Salesforce and Google Workspace data[53].
- **August 21, 2025:** Official advisory by Salesloft describing a security issue with the Drift OAuth integration[54].
- **September 15-16, 2025:** Shai-Hulud worm in the NPM ecosystem compromised hundreds of packages and demonstrated automated propagation across software supply dependencies[55].
- **September 23, 2025:** Advisory from CISA (U.S. Cybersecurity & Infrastructure Security Agency) declaring a "widespread supply chain compromise impacting NPM ecosystem[56]."
- **October 8, 2025:** The GlassWorm self-propagating worm uses invisible Unicode to spread through the OpenVSX marketplace, harvesting credentials and turning infected machines into proxy nodes[57].
- **October 15, 2025:** F5 discloses that a nation-state actor had breached its systems and exfiltrated source code and information about undisclosed vulnerabilities[58].

The idea of supply chain security has become central to modern cybersecurity, yet the term itself hides a dangerous oversimplification. What we call a "supply chain" is not a line of discrete, manageable links, but a dense web of interdependence. Each company, library, and service depends on countless others, and a single point of failure can reverberate across the entire digital ecosystem.

The notion of security as something confined within organizational boundaries is obsolete. In reality, no entity's cybersecurity is isolated. Every business's security depends on its suppliers, customers, and the open-source projects it builds into its technology stack.

This web of dependency transforms individual weaknesses into ecosystem-wide risks. Attackers exploit these interconnections strategically, targeting key nodes where compromise can cascade outward. The SolarWinds attack in 2020 remains an early and dramatic example: by inserting malicious code into a widely used IT management tool, attackers gained potential access to thousands of organizations, including U.S. federal agencies[59].

That same dynamic continues today, with attackers seeking leverage points that deliver outsized results. As we describe later in this report, the cyber extortion actor Cl0p has built a reputation for its large-scale attacks targeting commonly used file transfer platforms, through which they chalk up hundreds of victims. Cl0p was active again during the first quarter of 2025, with mass exploitation of the Cleo vulnerability[60]. That single event accounted for around 18% of all cyber extortion victims recorded during Q1 of this year.

The "Shai-Hulud" NPM incident in 2025 epitomized this vulnerability in the open-source world[61]. By compromising a single developer's account, attackers infected over 180 widely used packages on NPM and GitHub, harvesting API keys and tokens through malicious workflows before automatically spreading to new projects[62]. Each installation of an affected package triggered a fresh infection. What began as a breach of one maintainer rippled across hundreds of projects and organizations that depended on those packages.

Fortunately, developers reacted quickly and the infected packages were removed within hours, which considerably limited the impact. But the incident reminds us that even the smallest node in the ecosystem can be a gateway for mass compromise.

A similar lesson emerged from the Salesloft-Drift OAuth breach later this year. Attackers exploited an integration between two legitimate SaaS platforms to steal OAuth tokens and gain access to hundreds of downstream organizations' Salesforce and Google Workspace environments[63]. No single customer was hacked directly; instead, attackers leveraged the trust relationships that connected these systems. The breach revealed how fragile cloud interconnectivity has become. In the current era of cloud platforms, APIs, and AI-driven automation, token and credential security is no longer a technical afterthought but a strategic imperative.

When such "supply chain" incidents occur, the damage is rarely contained. Research shows that organizations affected indirectly by third-party breaches suffer higher losses than those targeted directly. The Cyentia Institute found that multi-party "ripple events" impose median losses more than ten times higher than typical single-party breaches[64]. These costs represent economic externalities. As the UK's The National Cyber Security Center recently argued, "There is often a misalignment between those who bear the costs of insecurities (that is, end users and wider society) and the technology providers who are best positioned to 'bake in' security"[65]. The original source of the breach rarely bears the full burden. The financial and reputational impact radiates outward, falling on firms and individuals who may have had no visibility or control over the original weakness.

Adversaries understand that the supply chain offers an irresistible target. Nation-state actors and cybercriminals alike are investing in exploiting these connections as efficient entry points. In one recent case, a U.S. telecommunications intermediary with access to multiple major carriers was quietly infiltrated by a nation-state actor for nearly a year[66]. Such incidents confirm that systemic interdependence is now both an economic and geopolitical vulnerability.

Governments have persuaded businesses to respond by tightening compliance requirements across their supply networks, insisting that vendors demonstrate baseline security maturity before contracts are signed. Such measures have some value. One significant UK wealth management business reports that achieving Cyber Essentials Plus compliance across their partnership network has helped them to reduce cyber security incidents by approximately 80%[67].

But compliance alone cannot contain a systemic problem. Do third-party audits or vendor questionnaires really reach into the deeper layers of their technology stacks, open-source libraries, cloud APIs, and shared digital infrastructure like DNS and CDNs? A compliance checklist cannot capture the full complexity of interdependence.

Ultimately, organizations must internalize that supply chain security is not an abstract compliance function but a direct operational risk. Threat models should account for supplier compromise, procurement policies should reward demonstrable security, and monitoring systems should include visibility into third-party failures. Security "fundamentals" like least-privilege access, credential hygiene, integrity verification, and active dependency monitoring remain essential to reduce the blast radius when a supplier is breached.

But true resilience relies on us strengthening the weakest links. For example, many of the open-source components that underpin modern software are maintained by small teams or individual volunteers. Supporting these maintainers with funding, code review services, or security automation, tools or intelligence could yield far more systemic benefit than just imposing more paperwork on their users.

Similarly, liability must be re-examined. When a negligent vendor exposes the ecosystem to catastrophic loss, accountability should align with the source of the harm. Fair and transparent liability models could incentivize better security practices across the web of participants.

Initiatives like Software Bills of Materials (SBOMs) and sector-wide information sharing can help illuminate shared dependencies, but addressing the systemic risk from interdependence requires us to take collective action.

In Europe, the Cyber Resilience Act (CRA) entered into force on 10 December 2024, with its full obligations scheduled to apply from 11 December 2027. The legislation mandates that all "products with digital elements" be designed, developed and maintained with cybersecurity by design. It requires documentation like SBOMs, impose vulnerability-monitoring and describes obligations regarding updates. Software suppliers will face much stricter security obligations, procurement standards across the EU will shift toward CRA compliance, and global vendors who wish to access the EU market will have to adopt higher supply-chain and software-security hygiene.

Chained to Suppliers

Collaboration among vendors, governments, and organizations can transform interdependence from a weakness into a foundation for resilience. In this context, security becomes an ecosystem investment. Securing the web of interdependence demands that each organization, whether large or small, recognizes its role in maintaining the integrity of the whole.

- **Charl van der Walt** - Head of Security Research

Inside-Out. The Remote Worker Threat

- **March, 2024:** The National Security Division (U.S.) and FBI launch the DPRK RevGen: Domestic Enabler Initiative to counter remote worker scams[68].
- **September 12, 2024:** U.K. government publish a public advisory to warn UK businesses of the threat of DPKR nationals posing as remote IT workers[69].
- **December 12, 2024:** U.S. DOJ announces legal actions against 14 North Korean nationals indicted for remote IT worker fraud that generated $88m over six years[70].
- **April 1, 2025:** Google Threat Intelligence Group publish a report on IT worker scams intensifying across Europe[71].
- **June 30,2 025:** U.S. DOJ launches coordinated nationwide action dismantling an IT worker fraud network that stole over 80 US citizens identities, infiltrated hundreds of U.S. and caused at least $3m in losses[72].
- **July 24, 2025:** American woman sentenced to prison for helping North Korean IT workers obtain jobs at 309 US companies and managing a laptop farm[73].

In July 2024 security vendor KnowBe4 described an incident in which a malicious actor attempted to access their network via a fake persona that applied for a software development role and was hired remotely. “We sent them their Mac workstation, and the moment it was received, it immediately started to load malware.”[74]

Remote IT worker fraud schemes, typically linked to the Democratic People’s Republic of Korea (DPRK), have evolved into a significant and persistent security concern for organizations worldwide. Initially regarded as a limited sanction-evasion tactic, these schemes have matured into a coordinated activity designed both to generate revenue, and to establish a technical foothold in corporate environments. The growing number of related incidents, sanctions, and public advisories released in the past year illustrates the systemic nature of this growing threat.

In June 2025, the U.S. Department of Justice announced several coordinated cases related to hundreds of North Korean nationals that fraudulently obtained remote employment with U.S. organizations[75]. The U.S. Department of the Treasury reported similar findings, estimating that the illicit revenue earned ran to hundreds of millions of dollars[76], with an average earning of $300,000 annually per worker. Several public advisories in multiple countries and an FBI reward notice for $5 million illustrate just how serious the threat has become[77]. A recent report states that nearly a third (27%) of the targeted entities are not based in the U.S. and that this threat is slowly expanding towards other industries[78]. The scam has been facilitated by the growth of remote work over the past few years. Companies have increasingly relied on virtual recruitment and outsourced verification processes, creating opportunities for falsified identities to bypass traditional screening processes.

The primary driver of these schemes is financial, as North Korea reportedly continues to seek alternative methods to fund itself. The remote employment of skilled IT professionals, often operating from China, Russia, or Southeast Asia, provides a stable and relatively low-risk source of income to the regime.

Beyond revenue generation, these infiltrations have strategic, political, and operational implications. Once embedded within an organization, fraudulent workers may gain access to sensitive intellectual property and internal infrastructure[79]. This access can facilitate data theft, the introduction of malicious code for disruption or extortion purposes[80], or the creation of latent access points for future exploitation.

Investigations reports show that DPRK IT workers operate through well-structured networks supported by facilitators and brokers[81]. These intermediaries supply stolen or falsified identity documents, and in some cases, even legitimate identities obtained in exchange for financial compensation. They also support the financial and technical logistics of the operations - managing salary flows by routing payments through cryptocurrency wallets, establishing shell companies, and maintaining technical infrastructure like “laptop farms”[82], which enable workers to appear geographically consistent with their assumed identities[83]. The offenders frequently rely on synthetic personas[84], combining elements of real and fabricated identity information. This enables multiple simultaneous applications for remote roles while shielding them from background screening. In most instances, deep-fake technologies are used in interview processes. These methods produce obscure financial trails and protect the offenders from appearing in law enforcement notices.

The operational consequences of hiring fraudulent IT workers extend well beyond potential data loss and extortion. Companies that unknowingly employ these individuals may be violating international sanctions, exposing themselves to legal and financial penalties. The U.S. government has made clear that such employment constitutes a breach of sanctions law regardless of intent[85].

Despite falling for the fake employee, KnowBe4 avoided real harms because their technical controls detected malicious actions. But mitigating the issue requires a combination of governance, procedural, and technical measures.

The first and most critical step is strengthening identity verification during and after recruitment. For example, human resources departments and hiring managers can be trained to recognize indicators of deception during virtual interviews. A robust zero-trust approach also goes a long way: diligently implement “least privilege” throughout the organization, assume a breach has happened or will happen, and authenticate and authorize every transaction[86].

Payment processes should incorporate due diligence to ensure that funds are not transferred to high-risk jurisdictions or unverified accounts, including cryptocurrency wallets.

The remote worker threat emerges from a range of systemic factors, including increased remote work after COVID, continued cost pressures on businesses, growing unemployment and tech worker disenchantment, and of course the emergence of GenAI[100]. At the organizational level, the challenge thus extends beyond technical safeguards.

Governance and Intelligence Beat Fragmentation

> **Remote worker schemes exploit the gaps between human resources, compliance, and cybersecurity functions. Addressing this fragmentation requires integrated governance frameworks that align recruitment procedures and insider-threat management. Security teams should also maintain information-sharing relationships with industry peers and national authorities to identify recurring indicators across sectors.**
>
> - **Zohra Hamila** - Security Researcher

Cyber Extortion Is Still the Big Gorilla

- **20 March 2024:** The Bundeskriminalamt (BKA, German Federal Criminal Police) together with Frankfurt's ZIT cyber-unit conducted a takedown of the darknet marketplace "Nemesis Market", seizing infrastructure in Germany and Lithuania[87].
- **30 May 2024:** Authorities participating in Operation ENDGAME announce arrests of four suspects in Ukraine and Armenia, the takedown of internet servers and control of domains tied to botnets[88].
- **December 2024:** The Cl0p ransomware gang launched a major campaign exploiting a zero-day vulnerability in Cleo managed file-transfer software, leading to hundreds of victims[89].
- **14 January 2025:** The UK Home Office publishes a consultation paper proposing a targeted ban on ransomware payments by all UK public sector bodies and critical national infrastructure and introducing mandatory incident-reporting for ransomware events[90].
- **19-22 May 2025:** : In the latest phase of Operation ENDGAME, law-enforcement agencies dismantle servers, neutralize domains, and issue arrest warrants for 20 suspects[91].
- **June 2025:** A follow-up to Operation ENDGAME results in additional actions and detentions targeting successor groups and affiliates of initial-access ecosystems[92].
- **22 July 2025:** The UK government announces its formal intention to ban public-bodies from paying ransoms, and to legislate for mandatory reporting of incidents and payments[93].
- **11 August 2025:** The US Department of Justice announces a coordinated disruption of the ransomware group BlackSuit (Royal), involving multiple countries[94].

We report this year that cyber extortion attacks have expanded to nearly every region and every size of business. Small and medium enterprises have become more impacted than large businesses. Where large firms in developed economies previously dominated statistics, victims this year include firms in countries added to our extortion datasets for the first time. The entry costs for attackers have plummeted thanks to commoditization of ransomware-as-a-service, initial access brokers and cryptocurrency-enabled monetization. A single vulnerability in commonly used software can yield hundreds or thousands of victims overnight, as seen when Cl0p exploited another file-transfer platform to trigger the largest quarterly level of victims we've ever recorded[95].

Our data shows not only more victims, but also more actors. The victims-per-actor ratio has increased, suggesting that extortion groups are operating at greater scale and with greater reuse of infrastructure.

Three Key Trends Became Clear This Year

One, despite years of focus and substantial investment in defensive controls, the number of victims continues to rise[96]. Ransomware and extortion attacks now represent a dominant share of cyber incidents, accounting for more than a third of losses and exhibiting growth measured in multiples since the late 2010s[97].

Two, the techniques used by threat actors are in many cases well known, straightforward, and theoretically avoidable[98]. Phishing, stolen credentials, unpatched systems and misconfigurations feature prominently in breach post-mortems. Yet these attacks persist and succeed, even when the theoretical controls exist. This points to a deeper problem than individual technical weakness.

Three, the ecosystem behind these attacks is evolving rapidly. Our reporting shows that the cyber extortion ecosystem has matured into a decentralized, professionalized network of affiliates, service-providers and facilitators, using the lowest cost, highest leverage vectors available. While we report that law enforcement and governments are responding more assertively, they must overcome jurisdictional fragmentation, safe-haven states and an adversary that shifts shape and label constantly.

The fact that many of the techniques used in Cy-X compromises are familiar, predictable and defeatable, yet somehow remain effective, requires urgent reflection. The recent breach at a major aerospace company, in which attackers accessed a server with old credentials, stole data and followed up with a second ransomware team on the same system, illustrates how basic processes can fail at multiple layers[99]. If we know how to patch, how to secure credential access, how to maintain offline backups, and how to train staff, then why do firms keep falling victim? The explanation may consider three broad theories.

Firstly, many organizations simply adopt security technologies or controls that are inexpensive, unwieldy, or poorly aligned with their context. The tools may be in theory but fail in practice. Secondly, maybe the adoption rate of basic cyber-hygiene practices remains patchy, especially among smaller firms and in developing economies. This leaves a wide attack surface still to be exploited. Finally, we may have placed too much faith in preventing breaches, when today's environment also demands robust detection, response and recovery capabilities.

Clearly, every organization must assume it is a target and prepare accordingly. Prevention remains essential, but so too does resilience through detection, incident response and recovery. Table-top exercises, live-fire rehearsal of recovery from backup systems and transparent post-breach introspection must become standard business practice. But business cannot individually repel this implacable adversary.

If technical controls are crumbling under the continuous assault, perhaps international regulators and law enforcement can stem the tide. Governments and law enforcement agencies certainly are responding to the scourge, and there are signs of progress. As the unique data shared in this report shows, publicly reported operations against cyber extortion have increased every year since 2021. Several major jurisdictions now participate regularly in multinational takedowns, arrests and indictments. However, despite the increased volume of actions, the Cy-X ecosystem remains resilient. Cy-X brands strategically fragment, rebrand and redeploy rapidly, often replacing a disrupted group with new operations. Some states tolerate or even shield domestic cyber-criminals, creating safe havens that thwart global efforts[101].

The net effect is that law enforcement action alone, while necessary, cannot tip the balance without significantly improved coordination, sustained pressure and the elimination of safe havens.

As long as the economics of extortion remain attractive, as long as criminals remain immune to prosecution, and as long as illicit funds can continue to flow, attackers will continue to strike. It's become clear that turning the tide on this epidemic will require a willingness to rethink our assumptions and take bold collective action.

To begin, we must treat cyber extortion as a societal threat, not simply a business problem. Critical infrastructure, healthcare, supply chains, and smaller firms are all at risk, and the social and economic consequences extend far beyond individual balance sheets. The threat could even be considered an act of international aggression, in that some groups operate with the permission and support of their host states.

The other systemic elements that enable crime to flourish also need to be reviewed, including the flow of illicit funds via cryptocurrency exchanges and the relative pros and cons of cyber insurance and ransom negotiators.

Finally, ransom payments must be considered afresh as a national security issue, rather than as an individual cost vs impact business decision. Some governments are already debating legal bans on ransom payments[102], supported by mandatory incident reporting and in some cases potentially victim support[103]. This debate cannot be considered settled, however.

Keeping the Hydra in Check

A wholly new form of collaboration is required that is more reminiscent of a war-time society, in which a mutual adversary and shared goals surface a unique and authentic form of public-private partnership.

Cyber extortion is not a niche threat that will fade. It is a systemic challenge that will continue to grow unless we change how we think, defend, respond and collaborate. We have the technical knowledge and the policy tools. The challenge is to achieve collective execution at scale, global coordination and the political will to treat this threat as the societal hazard it has become.

- **Charl van der Walt** - Head of Security Research

Technology, Politics and Digital Sovereignty

- **August 2024:** the Salt Typhoon Chinese-linked campaign compromises multiple telecom providers and accesses metadata, wire-tap systems and core network infrastructure[104].
- **30 December 2024:** The U.S. Department of the Treasury confirms a state-sponsored breach via a remote-support vendor, attributed to Chinese APTs[105].
- **February 2025:** A report by the Center for Strategic and International Studies (CSIS) indicates Chinese cyber-espionage surged by ~150% in 2024, targeting sectors such as telecom, manufacturing and media[106].
- **April 2025:** The European Union Agency for Cybersecurity (ENISA) launched the European Vulnerability Database (EUVD) to provide a region-wide vulnerability repository and enhance awareness and tracking of flaws.
- **14 June 2025:** Denmark's Ministry of Digital Affairs announces a migration from Microsoft Office / Windows toward Linux / LibreOffice for sovereignty reasons[107].
- **8 July 2025:** The European Commission publishes the "Open Source Way to EU Digital Sovereignty & Competitiveness" roadmap, formalising policy support for open-source in Europe[108].
- **16 July 2025:** The UK National Cyber Security Center (NCSC) announce its "Vulnerability Research Initiative" to collaborate with external experts on detecting and mitigating software flaws[109].
- **25 August 2025:** The Linux Foundation Europe publishes "The World of Open Source Europe Report 2025," emphasising open-source as a strategic priority for Europe's digital sovereignty[110].

All technology is political, and as global political tensions intensify, the political nature of technology has become more visible and consequential. The tools and systems that underpin modern economies have become extensions of national power. States and other actors now use technology as an asset, a weapon, a target, a platform, and a lever for political or strategic ends. The result is that cybersecurity can no longer be treated as a purely technical discipline. It exists in a world where infrastructure, markets, and alliances are shaped by ideological conflict and economic rivalry. Security professionals must now factor these realities into their understanding of risk and resilience.

Over the past year, cyberspace has grown more militarized. State-aligned hackers have gravitated from espionage to pre-positioning for conflict. China-linked Volt Typhoon campaign reportedly infiltrated American critical infrastructure not only to collect intelligence but to seek persistence in case of future confrontation with the United States[111]. The later Salt Typhoon operation compromised telecom networks and exfiltrated vast troves of data across several different countries[112]. These incidents reveal that national infrastructures like power grids and communications systems have become battlegrounds in a cyber cold war.

The fragility of infrastructure extends beyond software. Undersea cables, satellites, and other physical components of the digital ecosystem have all been shown to be vulnerable. Investigations have tied several cable cuts in the Baltic Sea and near Taiwan to deliberate interference by state-linked vessels[113]. Meanwhile, research has revealed that a significant proportion of satellite transmissions, including commercial and military data, remain unencrypted and easily intercepted with consumer equipment[114]. The interdependence of systems means that a single incident can cascade across borders and industries, magnifying political tensions and economic loss.

Active conflicts in the war against Ukraine and the conflict in the Middle East have illustrated how geopolitical violence spills into cyberspace. Cyber operations now accompany war almost as predictably as propaganda and sanctions. Russian attacks on NATO networks and Western businesses have increased markedly since the invasion of Ukraine[115], and Iranian groups sympathetic to Hamas have conducted coordinated campaigns against Israeli and Western targets[116]. These operations often reach beyond governments to affect private enterprises and civil infrastructure. State-aligned hacktivist groups - state-aligned and sometimes state-supported - target banks, schools, hospitals and logistics firms to amplify fear or signal allegiance. Their motives are ideological rather than financial, yet the effects like service disruption, data loss, and reputational harm are similar to those of traditional cybercrime. For businesses, it means that political events anywhere in the world can create local and immediate security consequences.

The political environment also shapes how states regulate and control technology. Digital sovereignty has become a central concern for governments and businesses seeking to insulate themselves from foreign influence. Across Europe, debates between Paris and Berlin reveal competing visions of sovereignty, the former favouring autonomy and self-sufficiency, the latter supporting openness tempered by alliances[117]. This divergence mirrors a broader fragmentation of the regulatory landscape. The United States, European Union, China, and Russia each impose different expectations on how data is handled, how platforms are governed, and who can provide critical infrastructure. The result is a patchwork of legal and ideological boundaries that complicate global operations. For multinational companies, compliance now demands geopolitical literacy as much as legal diligence.

One of the most complicated domains is data sovereignty. The U.S. CLOUD Act and FISA section 702[118] grant American authorities access to data held by U.S. companies anywhere in the world, including on servers located in Europe. Microsoft has acknowledged that it cannot absolutely prevent such access, even for European customers[119]. This admission has reinforced European scepticism toward U.S. cloud providers and spurred the development of local alternatives.

The dilemma is that European institutions depend on American cybersecurity capabilities and intelligence yet also fear their extraterritorial reach. The question is no longer purely technical but political. Whose laws and values govern the digital spaces we inhabit?

Trade conflicts compound this problem. Bans on Chinese hardware, sanctions on software vendors, and export controls on semiconductors are reshaping global supply chains. Western states are removing Huawei and ZTE equipment from telecom networks[120], while China has imposed export restrictions on materials vital to chip production. Each action triggers new vulnerabilities and costs. Businesses must now assess not only the reliability of a vendor but also the geopolitical stability and extraterritorial laws of the vendor's home country. A product's origin has become a security attribute in itself.

As our previous research on this theme describes, developments over the last year have also exposed the world's continued reliance on U.S. leadership in cybersecurity[121]. For decades, American institutions have maintained the databases, intelligence networks, and enforcement mechanisms that underpin global cyber defense. Programs such as the Common Vulnerabilities and Exposures catalog (CVE) and the Known Exploited Vulnerabilities list (KEV) are indispensable to defenders across the globe. Yet political change in Washington can alter these commitments overnight. In 2025, directives within the U.S. government reportedly instructed analysts to reduce attention on Russian cyber threats, prompting concern among allies that long-standing cooperation could erode[122]. Such episodes remind us that the security of one region can hinge on the political will of another.

Governments are also expanding their surveillance powers in the name of safety and morality. The "Chat Control" legislation proposed in Europe to require scanning of encrypted messages for illegal content may weaken privacy and create new systemic vulnerabilities[123]. However, in October 2025, Germany publicly announced that it would not support the proposed text[124]. Similar age-verification and monitoring laws are emerging in the UK and elsewhere[125]. These initiatives blur the line between security and freedom, forcing CISOs to reconcile compliance with ethical responsibility. From the Snowden revelations[126] to Microsoft's compliance with politically motivated U.S. orders against the International Criminal Court[127], the history of state access to private data reveals how easily technical infrastructure can become an instrument of power abuse. Building systems that limit unnecessary data collection and preserve encryption is therefore not only good practice but a moral imperative.

The explosion of GenAI adds another layer of complexity. AI promises efficiency and insight but also deepens dependency on a handful of global platforms. Most large-scale AI technology is controlled by U.S. or Chinese firms. Adopting these services may bring short-term gains but may also entangle users in the political and economic priorities of those powers. As Wicus Ross explains elsewhere in this report, the economic sustainability of the AI industry is also uncertain. Analysts warn of speculative excess reminiscent of the dot-com bubble[128], with massive capital inflows and little measurable return on investment. For CISOs, the prudent course is measured experimentation, ensuring that enthusiasm for productivity does not create new exposures or dependencies.

In this environment, the role of the CISO has changed. Managing cybersecurity now means managing political, legal, and ethical risk. It demands awareness of how state policy, ideology, and global trade affect the organization's security posture. Technology choices are value choices.

The decision to use one cloud platform over another may express alignment with a particular system of laws, a particular vision of privacy, or a particular interpretation of freedom. CISOs must guide their boards and executives through these choices with both technical expertise and moral clarity.

Collective defense is part of this responsibility. No organization can secure itself alone. Interdependence across suppliers, service providers, and infrastructure means that resilience must be built through collaboration. Information sharing, joint exercises, and support for open standards and technologies are essential. By distributing control, the open-source movement reduces single points of failure and opportunity for political capture. Some European governments are already adopting open-source systems to regain autonomy. The state of Schleswig-Holstein in Germany and public institutions in Denmark are migrating from Microsoft products to Linux and LibreOffice, citing sovereignty and transparency[129] and the city of Lyon in France is also taking the leap to replace the Microsoft Office suite "in order to no longer be dependent on US software solutions and acquire true digital sovereignty"[130].

Plotting Borders in Cyber

Cyberspace is now a political domain as much as a technical one. The boundaries that once separated national security from corporate security, or public policy from private enterprise, have dissolving. Every organization is entangled in the geopolitical web that defines the digital age. Recognizing this reality is the first step toward resilience. The task for today's security leaders is to manage not only threats but also the political and ethical implications of their tools, suppliers, and alliances. In doing so, they can help ensure that technology serves human interests rather than only the ambitions of power.

- **Charl van der Walt** - Head of Security Research

CVE in Crisis-Will It Survive, and Should It?

- **April 15-16, 2025:** A warning is issued that the funding contract for the MITRE Corporation-managed CVE Program would expire on April 16, potentially ceasing new CVE assignments[131].
- **April 16, 2025:** The Cybersecurity and Infrastructure Security Agency (CISA) executes a last-minute extension of the CVE programme contract, averting immediate shutdown of CVE operations[132].
- **April 2025:** Orange Cyberdefense publishes paper on European technology sovereignty and security in light of a shifting world order[133].
- **May 13, 2025:** The European Vulnerability Database (EUVD), managed by ENISA, is launched to offer a complementary vulnerability tracking system aligned with European digital-sovereignty goals[134].
- **August 07, 2025:** Orange Cyberdefense article on the implications of the EUVD on Binding Hook[135].

For over two decades, the Common Vulnerabilities and Exposures (CVE) program has served as the universal index for software flaws. It provides the common language through which the security industry identifies, catalogues, and discusses vulnerabilities. Much like an index in libraries, CVE brings order and classification to an overwhelming universe of defects[136]. Yet the very ubiquity of this system has made it both indispensable and restrictive. Over the last year its fragility has become visible.

Its dominance may also be constraining how defenders think about risk itself.

Modern cybersecurity remains overwhelmed with vulnerabilities. Exploitation of vulnerabilities was cited as the initial access vector in approximately 20% of confirmed breaches in the 2025 DBIR[137]. The total number of unique CVEs has now exceeded 300,000, yet only a small fraction are ever exploited in the wild (Orange Cyberdefense, 2024). Organizations cannot hope to patch them all, and studies show that many address fewer than one fifth of known vulnerabilities each month. The CVE ecosystem simply produces more information than defenders can meaningfully act upon, and that should give us pause for thought.

The CVE catalogue is coordinated by MITRE and sustained through a network of numbering authorities that submit and score entries. It is a remarkable achievement of global cooperation, but it is also a fragile bureaucracy. In early 2025, funding shortfalls almost shut down the programme, leaving the industry at risk of disruption to its shared reference system[138]. Around the same time, a backlog at the National Vulnerability Database delayed the enrichment of tens of thousands of CVEs, causing real anxiety for defenders who rely on that data for patch prioritisation[139]. When a single public database can cause such widespread disruption, it may reveal an unhealthy systemic dependence.

As we wrote for Binding Hook, Europe's creation of the European Vulnerabilities Database (EUVD) in mid-2025 can be read as a strategic response to that dependence[140]. Managed by ENISA and designed to complement CVE, the EUVD aggregates data from national and open sources to improve visibility into software risk.

Beyond just creating redundancy, EUVD reflects Europe's broader concern with digital sovereignty and diversification. Similar projects already exist elsewhere, such as China's CNNVD[141] and Japan's NVD[142]. The problem, however, is not only operational. CVE defines vulnerabilities, not risk. It tells us what exists, not what matters. The overwhelming flow of new entries keeps defenders trapped in a reactive cycle, constantly patching, triaging, and chasing the next identifier. This may be useful for threat communication and mitigation, but it is not the same as reducing risk. Risk arises from the interaction of threats, vulnerabilities, and impacts. A more strategic approach begins by defining an architecture and process that results in a tolerable level of risk, and then considers where vulnerability data can most effectively guide intervention. The CVE feed is a means to that end, not the end itself.

Attackers exploit this error in perspective. As John Lambert observed, defenders think in lists, while attackers think in graphs[143]. Networks are not static inventories but dynamic systems of interconnections. A single vulnerable node can offer an attacker lateral movement through an entire enterprise. Focusing narrowly on the pipe dream of enumerating and patching vulnerabilities without addressing architecture and segmentation is therefore an exercise in diminishing returns. Security leaders must invest in reducing attack surfaces, enforcing segmentation, and improving the baseline quality of deployed systems. Concepts such as immutability and ephemerality, e.g. deploying short-lived, automatically renewed infrastructure, illustrate how engineering choices can remove whole classes of vulnerability.

For CISOs and practitioners, CVE remains an essential tool for coordination and communication, but it should not define strategy. Security teams must prioritize architectural resilience over vulnerability management, and demand better software security, transparency and standardization from vendors. Begin with a coherent model for systemic risk reduction, then decide if and how CVE data supports that model. Allowing the catalogue to dictate priorities reverses the logic of defense.

A Vulnerable System

The events of 2025 exposed the fragility of a system that has long served as the heartbeat of cybersecurity and surfaced broader conversations about redundancy and independence. CVE should remain our universal Dewey Decimal System, but it must not be the only lens through which we consider the issue of vulnerabilities and security.

- **Charl van der Walt** - Head of Security Research

Security Technologies Are the Front Line

- **January 2024:** Attackers exploit two zero-day vulnerabilities in Ivanti Connect Secure VPN (CVE-2023-46805 and CVE-2024-21887) to gain unauthorised access and enable session hijacking to bypass multi-factor authentication[144].
- **2024:** The Google Threat Intelligence Group track approximately 75 exploited zero-day vulnerabilities, of which more than one-third targeted network and security appliances (VPNs, firewalls, edge gear)[145].
- **23 October 2024:** The Cyber Resilience Act (CRA) is formally adopted by the European Parliament and the Council of the European Union, establishing horizontal cybersecurity requirements for "products with digital elements" including obligations for vulnerability reporting and lifecycle security[146].
- **August 9, 2025:** F5 Networks first detects unauthorized persistent access in its internal development systems for the BIG-IP product line[147].
- **10 September 2025:** The UK Government publishes a briefing on the cyber resilience of national digital infrastructure, emphasizing that vendors supplying critical systems may often have weaker cybersecurity and calling for stronger regulation[148].
- **September 25, 2025:** Cisco Systems release security advisories for three flaws in its Secure VPN/Firewall lines that are being actively exploited[149].
- **October 15, 2025:** The Cybersecurity and Infrastructure Security Agency (CISA) issues Emergency Directive ED-26-01 requiring U.S. federal agencies to patch or isolate affected F5 devices[150].
- **October 20, 2025:** Analysis by security-monitoring groups reports that more than 266,000 internet-connected F5 BIG-IP instances remained potentially exposed following the breach, presenting an "imminent threat"[151].

In recent years the cybersecurity industry has matured into a vast market, yet security technology itself has become a common conduit for compromise. Perimeter-security devices like virtual private networks, firewalls and other edge appliances are under sustained attack. According to Google Threat Intelligence Group, in 2024 alone nearly one in three exploited zero-day vulnerabilities targeted network and security appliances[152]. A 2025 report from Mandiant found that the four most-frequently exploited vulnerabilities in 2024 came from edge devices such as VPNs, firewalls and routers[153]. Further, insurers report that enterprises deploying ASA-class devices from vendors such as Cisco Systems or firewalls from Fortinet face several-fold higher claim rates[154].

These technologies represent the first line of defense for many enterprises, but their frequent compromise transforms that line into an attack surface. Perimeter devices have become a frequent vector of initial access.

Incidents at vendors themselves during 2024 and 2025 have further diminished industry trust. In mid-October 2025, F5 Networks disclosed a breach by a nation-state actor that maintained extended access to its engineering systems, stole source code for its BIG-IP appliances and internal vulnerability documentation[155]. The UK National Cyber Security Center responded by issuing an advisory and advising customers to inventory, patch or isolate F5 devices[156].

In another case, Cisco reported that state-sponsored actors had subverted its Adaptive Security Appliance hardware to monitor government networks[157]. And many still remember that in February 2024 CISA mandated US federal agencies to "disconnect all instances of Ivanti Connect Secure and Ivanti Policy Secure solution products from agency networks" in response to an exploitable vulnerability[158].

The recurrence of security incidents, vulnerabilities and compromises points to systemic issues. Analysis disclosed during the last year reveals that codebases still include "90s-era" flaws, suggesting that product development, testing and vendor-ecosystem practices are failing us. The problem is not simply that products contain bugs but that the vulnerability lifecycle, from discovery to mitigation, is fragmented and disorganized. Vendors release patches on ad-hoc schedules, severity ratings vary between suppliers, while advisory formats and channels differ (RSS feeds, email lists, portals). This inconsistency forces every new CVE to trigger emergency patch cycles, scanning, asset-mapping, prioritization meetings and often unplanned downtime. Enterprises bear the cost of each patch event, not just in monetary terms, but also in operational risk.

As the economic and geopolitical landscape continues to shift, vendor provenance is also a strategic concern. The dominance of U.S.-based providers subjects enterprise customers outside the United States to export regulation, law-enforcement reach and supply-chain dependencies. As the concept of digital sovereignty gains traction in Europe, European and open-source security solutions offer potential alternatives. Open-source software can facilitate inspection, control and independence, while European vendors may align better with regional policy and regulatory frameworks. Supporting these initiatives is not a panacea but forms part of a diverse defense strategy that hedges geopolitical and vendor-lock-in risk while also nurturing an alternative security technology ecosystem outside centers like the USA, Israel and China.

Change Requirement

Organizations and CISOs must therefore push for change. Vendors must adhere to higher standards and demonstrate secure development, rigorous testing, clear vulnerability reporting and clear transparent advisories. Organizations should incorporate European or open-source security products where practical, demand that dominant vendors improve hygiene, transparency and accountability, and develop vulnerability management capabilities that prioritize these technologies as primary attack vectors. Ultimately, resilience will emerge beyond blind trust in perimeter devices when disciplined vendor governance, diversified toolchains, and rigorous scrutiny are enforced.

- **Charl van der Walt** - Head of Security Research

Key data of the year: Intelligence and operations

Threat Detection Data: A Global View on the Analysis

As always, we strive to provide a global overview of what we are seeing in our incident data with the aim being to highlight trends that can also be applied to the global threat landscape. To facilitate this, a broad data set is collected from across all of the operational teams within Orange Cyberdefense including our CyberSOCs across 15 locations globally.

This time our analysis is based on 11 months' worth of Managed Threat Detection Services data, from 1st October 2024 to 31st August 2025. We will revert to 12-month periods again in future reports.

There has been a significant shift in the distribution between internal and external incidents this year, with incidents originating internally having increased from a 48% share in last year's report to now make up 57% of incidents, which is a 17% increase in terms of incident numbers.

Misuse and hacking are the most prominent threat actions, but incidents classed as misuse have again seen a significant increase up to 45% from 29% last year, this again follows on the back of the increase in incidents originating internally. Hacking incidents have remained at their previous level; however, malware incidents have decreased to around a third of the number reported last year, and social incidents have declined severely, now being reported in less than 1% of incidents compared with 13% in last year's report.

End user devices are still the most impacted assets but have increased significantly from 39% last year. Again, this is in line with the increase in incidents originating internally.

These two shifts appear to be driven in large part by an ongoing evolution towards Extended Detection and Response tools (XDR) as the primary driver for threat detection. XDR in general (and some products in particular) note and highlight "unauthorized" activity more aggressively than perimeter or network detections. Beyond that, many of our clients are growing via acquisition and thus deploying more XDR to endpoints. Finally, we believe that - as they mature in security - our clients are increasingly focused on detecting and preventing policy violations on user endpoints.

Incidents impacting accounts have increased slightly from last year's 12% and are now the second highest impacted asset. Incidents impacting servers have seen another slight decrease this year while network impacting incidents have again remained at a similar level to last year.

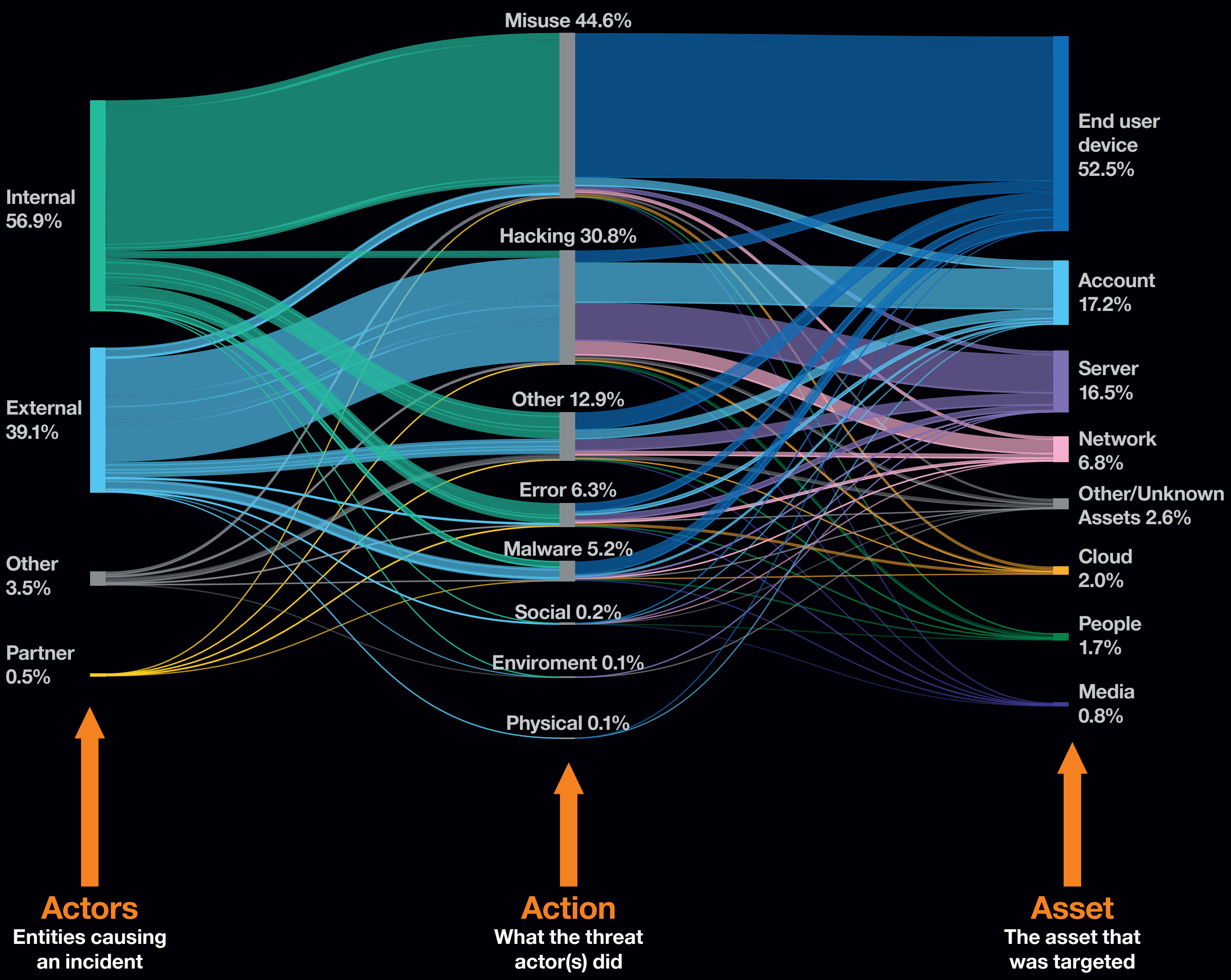
We are seeing the same pattern as last year with another large increase in confirmed incidents originating from internal users and impacting end-user devices. This, especially when coupled with the high number of misuse incidents, illustrates that organizations have become especially cognizant of the threat from within, be that intentional or accidental. We believe this indicates that our clients are focusing on, and responding to, endpoint security violations proportionally more, and not that other forms of incident are occurring less.

Threat Detection Data

Carl Morris - Senior Security Researcher

About the Data

- Total number of incidents: 139,373 over 11 months (a 3% increase when compared with 135,225 over 12 months in 2024)
- Analyzed period from October 2024 to August 2025 (11 months)
- Of these incidents, 19,053 (13.67%) were confirmed as True Positive incidents, an 8% decrease compared to Security Navigator 2025. However, not all clients include VERIS categories.
- Data sources: including Endpoint / eXtended Detection and Response (EDR / XDR), Network Detection and Response and SIEM platforms, as well as enriched incident data from Orange Cyberdefense Core Fusion platform



Events, Incidents, Confirmed Incidents

We log an event that has met certain conditions and is thus considered an Indicator of Compromise, Attack or Vulnerability. An Incident is when this logged Event, or several Events, are correlated or flagged for investigation by a human - our security analysts.

True Legitimate incidents are incidents that were raised but after consultation with the customer proved to be legitimate activity. Incidents are categorized as false positive when a false alarm is raised.

Because individual SOCs or Clients may have slightly different approaches to defining Incident status, we simplify these categories to confirmed and other in parts of this report.

An Incident is considered confirmed when, with the help of the customer or at the discretion of the analyst, we can determine that security was indeed compromised. At this point the incident is also categorized. We sometimes refer to these confirmed incidents in this report as true positives.

Totals

A total of 139,373 incidents were evaluated in this year's dataset, which represents a ~3% increase over the previous year. True positives account for 19,053 incidents, or 13.67% of the total. The balance of incidents (~86%) is comprised of 11.65% true legitimates, 67.81% false positives, and 6.87% of incidents not categorized.

As in previous years, we can calculate the number of incidents relative to our client base. For this year's dataset, we record an average of 12.3 confirmed incidents per month per client for the past 11 months. These are events that have been raised by a detection technology, triaged, confirmed and categorized by a trained analyst, raised with the customer, investigated and finally confirmed as "real".

The number of confirmed incidents per month per client is higher when evaluating only "mature" clients that have been using our CyberSOC service for the past 3 years or more.

The chart below demonstrates how detections have changed for established clients who have stayed with us for 36 months or more. There is a clear steady growth in the total number of incidents, which can be attributed to improved tooling, technology, and detection engineering. We note that the increase also correlates with the increased adoption of Endpoint Detection and Response (EDR) and Extended Detection and Response tools (XDR).

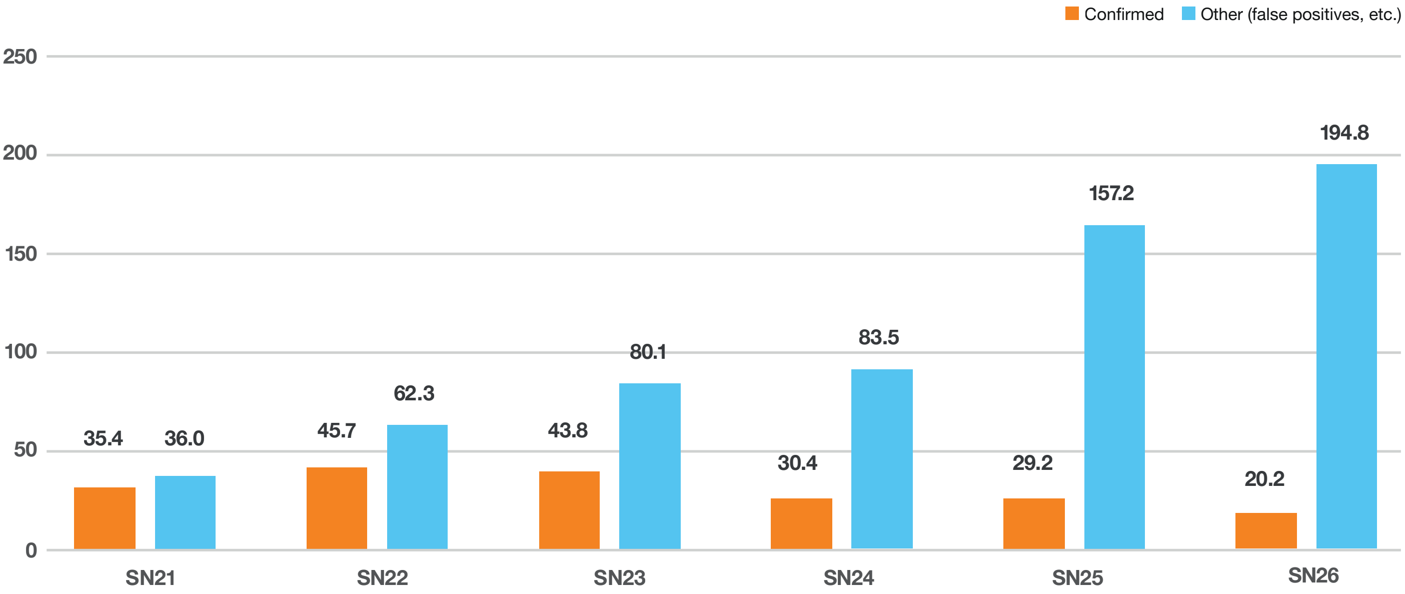
As one cybersoc analyst explained to us when discussing a client:

> **The customer's EDR tool of choice is very trigger-happy in general, especially when it comes to Potentially Unwanted Programs (PUP) and otherwise legitimate software.**
>
> **David Hörnsten** - Lead Security Analyst, CyberSOC

However, the number of "confirmed incidents" has steadily reduced because of improvements to triage and analysis processes but especially customer communication, feedback and understanding.

Incidents per Month

per Client for Clients Older Than 36 Months



Incidents by Priority

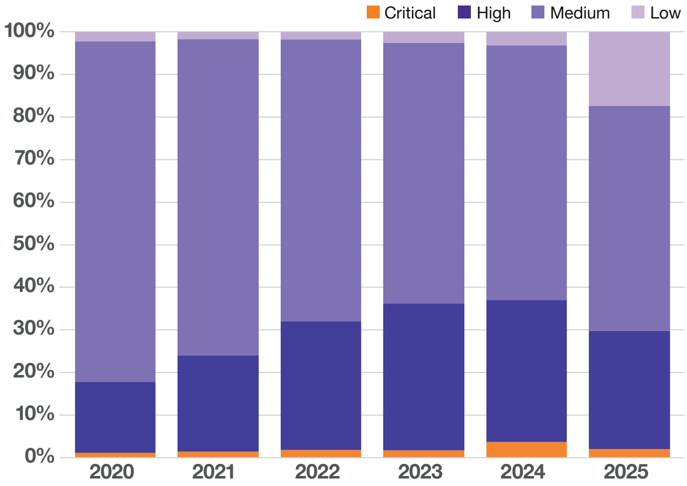
Alongside a reduction in the total number of incidents reported per client, we also note an improvement in incident granularity, as reflected by an increased diversity in incident priorities.

In 2020 97% of all incidents were classified as priority 2 or 3. In this year's data those moderate classifications account for only 80% of all confirmed incidents. In other words, analysts are able (and willing) to make stronger assertions that incidents are either very high, or very low, priority. Indeed, the proportion of incidents ranked as "Priority 1" doubled between 2020 and 2025.

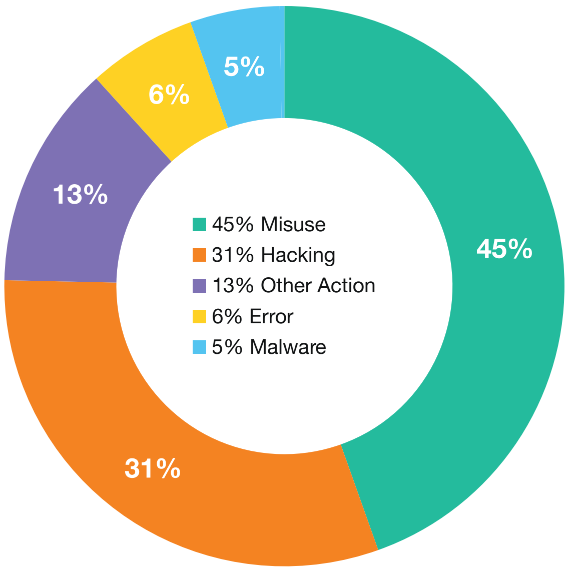
In a similar vein to last year, we have again seen the percentage of threat actions labeled misuse increase significantly rising from 29% to 45%, now far surpassing hacking which made up 31%, a slight increase on last year's 29%.

If we drill down into the threat actions, we can see that the top 3 positions retain the same order of actions. However there has been a considerable jump with the unapproved (misuse) threat action going from ~25% to ~43%, whilst both web attack (hacking) and phishing/spear-phishing (hacking) in turn saw slight decreases.

Incident Priority by Year



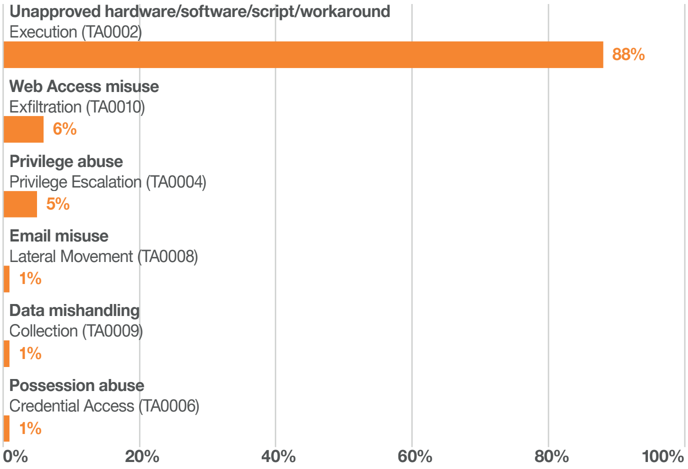
Incidents by Threat Action



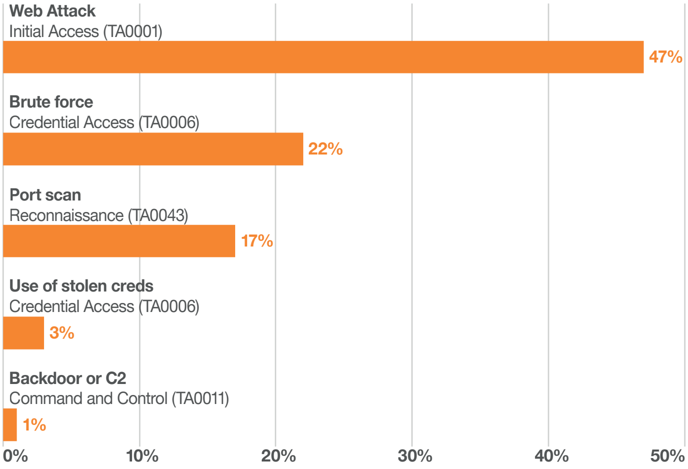
Actions Impacting "Accounts":

ATT&CK Tactic	Action	%
Initial Access (TA0001)	Phishing/Spear-Phishing	27%
Credential Access (TA0006)	Brute force	20%
Credential Access (TA0006)	Hacking	5%
Execution (TA0002)	Unapproved hardware/ software/script/workaround	5%
Credential Access (TA0006)	Use of stolen creds	4%
Privilege Escalation (TA0004)	Privilege abuse	3%
Initial Access (TA0001)	Spam (Social)	3%
Initial Access (TA0001)	Web Attack	2%
Exfiltration (TA0010)	Web Access misuse	2%
Privilege Escalation (TA0004)	Misuse	2%
Initial Access (TA0001)	Social	1%
Lateral Movement (TA0008)	Email misuse	1%
Initial Access (TA0001)	Hacking	1%
Execution (TA0002)	Misuse	1%

Most Prominent "Misuse" Actions:

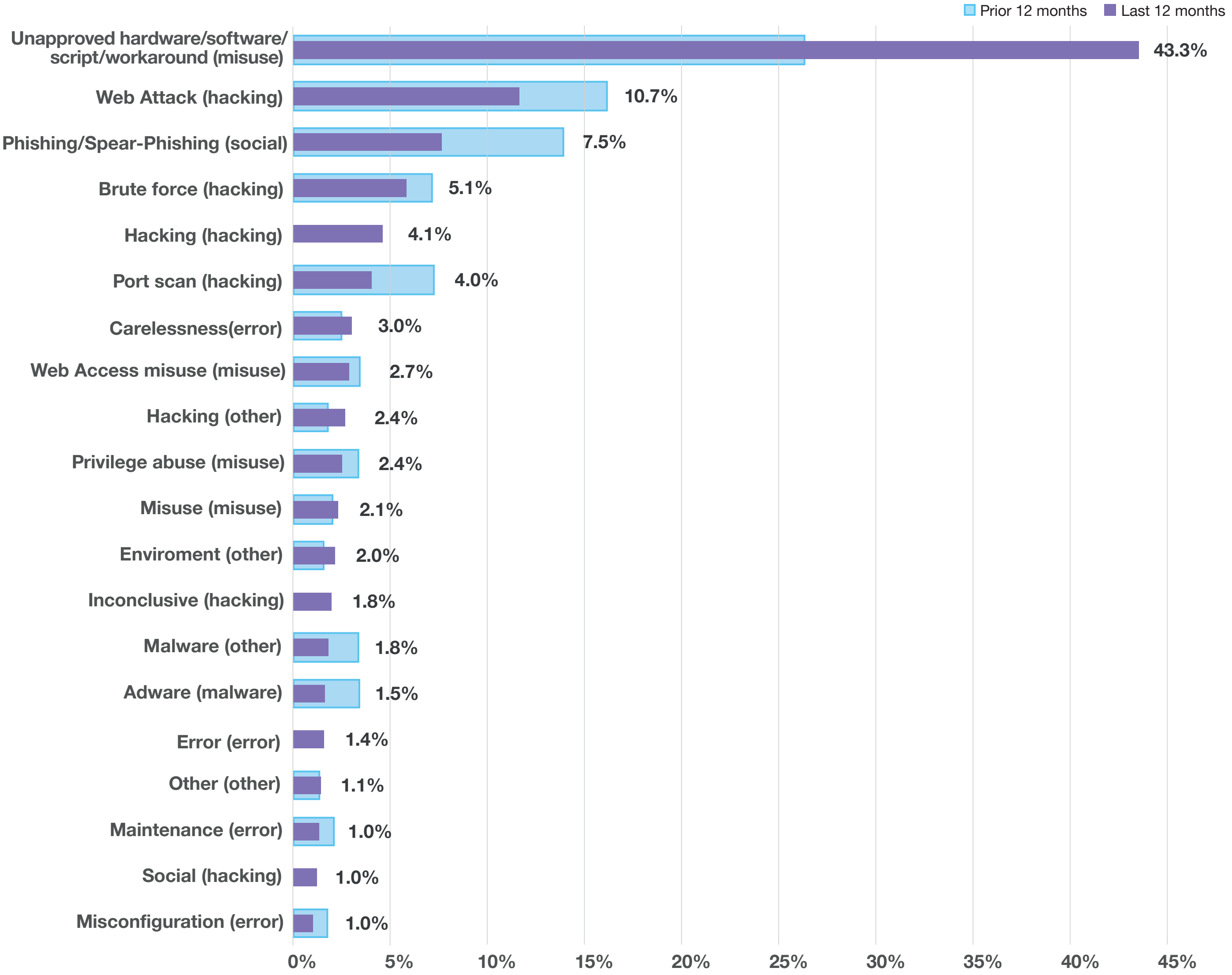


Most Prominent "Hacking" Actions:



Threat Action in Detail

Top 20 Threat Action and Threat Action Level 2 Combined

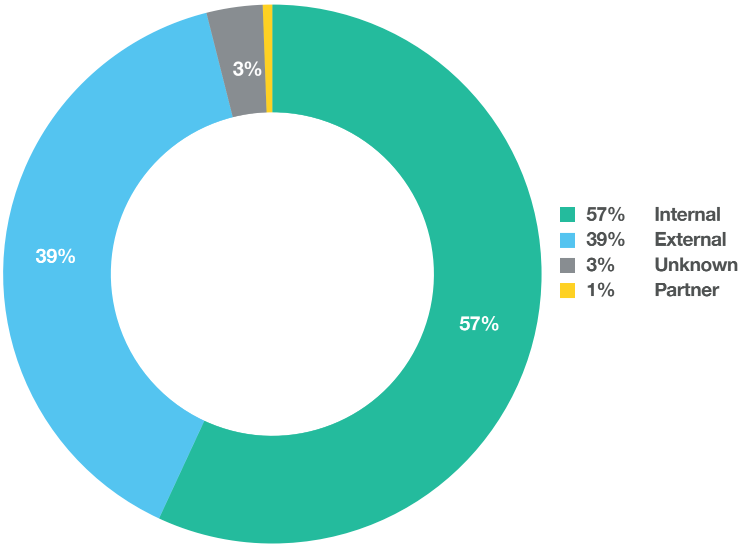


Threat Actions Summary

An important observation is that yet again the incidents associated with misuse actions have notably increased. Due to the majority of these incidents originating from internal actors and primarily impacting end user devices then an easy assumption to make is that these incidents are solely down to users' negligence, disregarding of policies or direct malicious intent. However, this increase could also be attributed to an improved maturity and security posture resulting in organizations implementing tighter security controls and restrictions on endpoints resulting in a "clean up" process whilst devices become compliant.

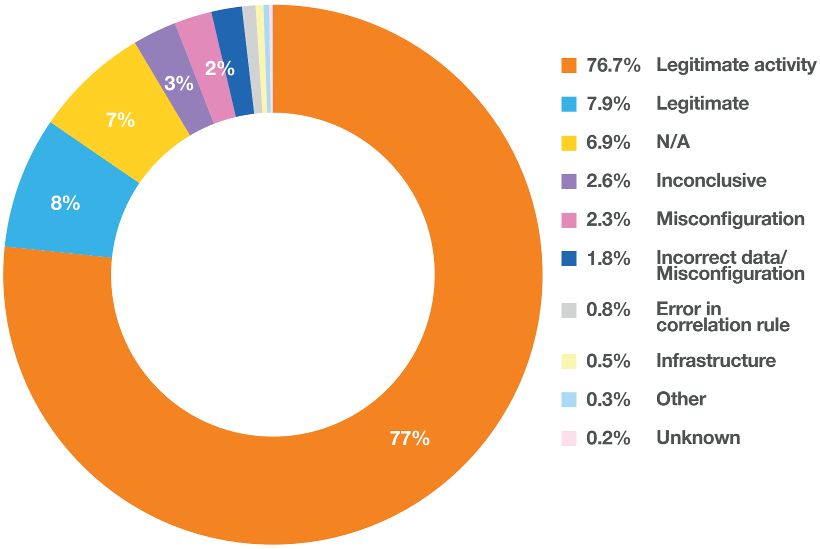
- **Carl Morris** - Senior Security Researcher

Incident Sources



False Positive Types

Incidents That Raised An Alert But Turned Out To Be Harmless



Incident Sources

In recent years we have seen swings back and forth in terms of the ratio of external and internal sources of incidents, with last year seeing them essentially neck and neck. This year though there seems to be a discernible trend with internal sources increasing again at a similar rate to last year, from 47% to 57%, at the same time external sources dropped from 48% to 39%.

Incident Targets

The continued growth of end user devices being the impacted asset, up from 36% last year to 52%, is in line with the increases in the misuse threat action and internal source and is to be expected. Of note though is the increase in the account asset jumping from 10% to 17%. This likely reflects how credentials and identity access have become an efficient way for attackers to gain and monetise access, driven by cloud adoption, phishing success, and the prominence of BEC.

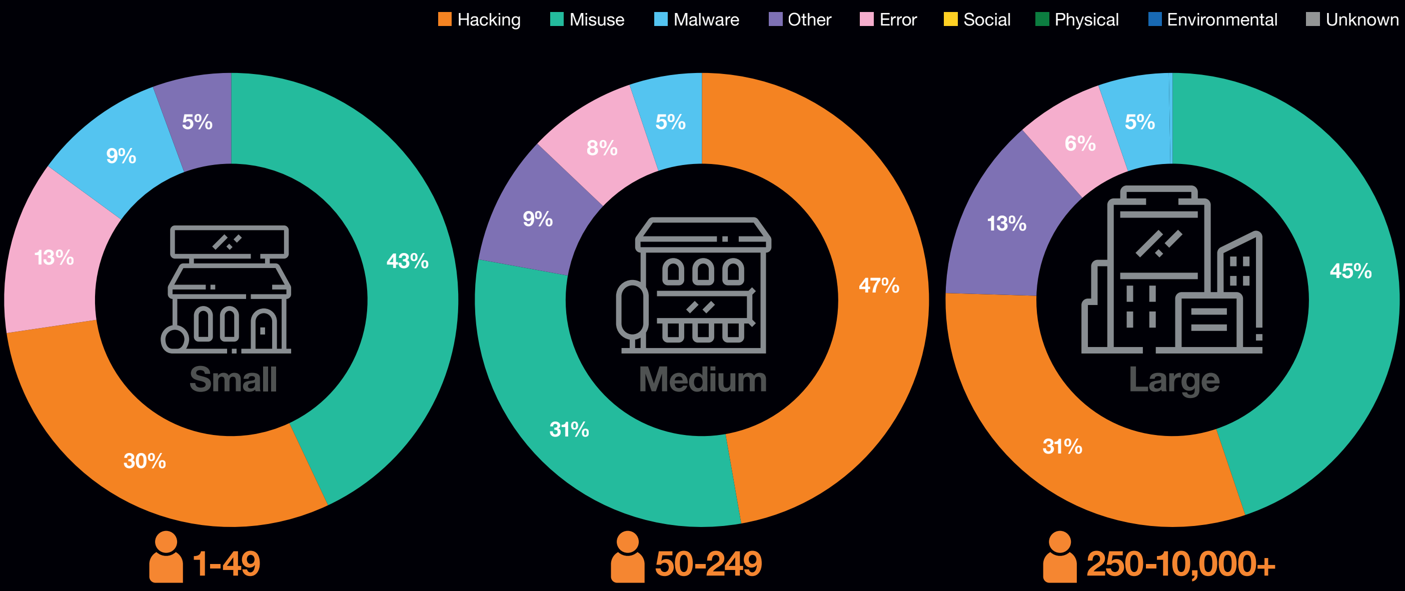
False Positives

Our research shows yet again that false positives primarily occur when everyday user activity is mistaken for a threat. Security systems are designed to detect suspicious behavior, but everyday activity such as logging in from a new location, downloading large volumes of data or installing a new application can sometimes look malicious. These legitimate activities may then trigger detection rules and generate unnecessary alerts. False positives underline the challenge of creating detection methods that are sharp enough to catch real threats while avoiding excessive alarms for routine activity.

Incidents by Business Size

Small and large businesses are more likely to be hit by cybersecurity incidents involving misuse because of how internal access works at their scale. Small companies have fewer resources and less restrictive policies which tends to mean employees have more access and permissions than they necessarily require, this then increases the likelihood of genuine mistakes or malicious activity occurring. In larger organizations, the sheer number of employees, contractors, and systems increases the chance that insider misuse can slip past even strong security measures. Medium-sized businesses, on the other hand, are more often targeted by hacking. They usually hold more valuable assets than small firms but don't always have the advanced defenses or dedicated security teams that larger enterprises do, making them especially vulnerable to outside attacks.

Threat Actions by Business Sizes



Following the pattern already established earlier in this report misuse incidents are still the most prevalent for small businesses, although their percentage share did drop slightly when compared to Security Navigator 2025, from 48% to 43%. Hacking remained second but increased to 30%, error and malware again are 3rd and 4th highest but swap places compared to last year and social does not feature at all this year.

Bucking the trend somewhat the top incident type for medium businesses is hacking with 47%, a significant increase on the 32% reported in Security Navigator 2025. The misuse incident category dropped to second but still saw a slight increase from 27% to 31%. As with small businesses the social incident category didn't feature this year.

Whilst both misuse and hacking have increased their share again, misuse had the most dramatic increase rising from 29% in Security Navigator 2025 to 45% this year, hacking went from 29% to 31%. This suggests an increased maturity on behalf of clients. Incidents categorized as malware notably decreased from 16% to 5%, as did social which dropped from 11% to 0.2%.

Mean Time To Resolve

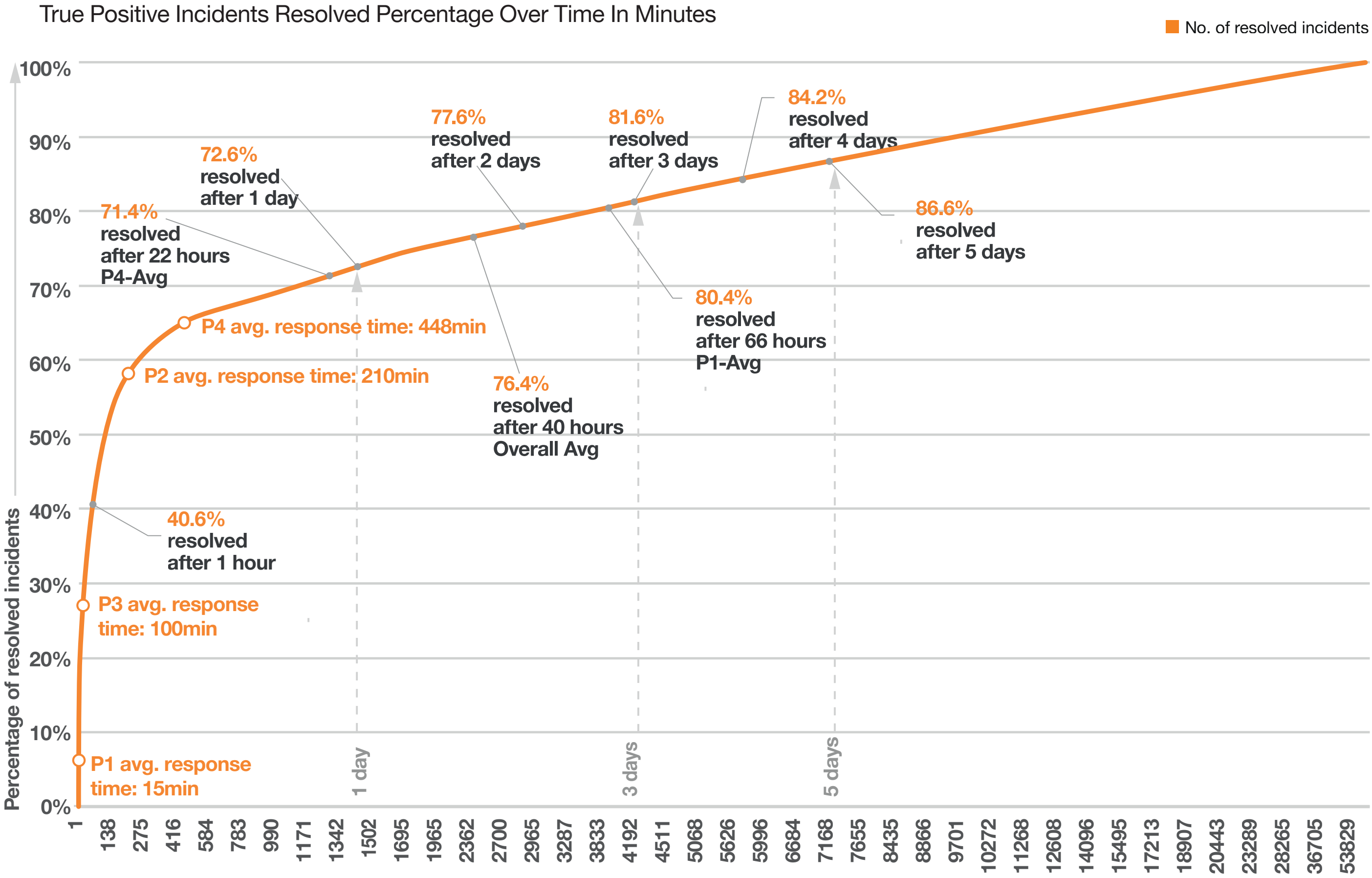
This year we are again able to include Mean Time To Resolve (MTTR) statistics in this report. In our operation we record the time it takes in minutes from when an alert is raised, through triage, analysis and reporting, to when it can be categorized and closed with the approval of the client. MTTR is a prickly metric and can easily mislead. We've taken a page from the Cyentia playbook and opted to present our data in the form of a "survival analysis", which is illustrated below[159]. The criticism laid against MTTR is that it can be opaque.

Since an uneven distribution of MTTR values, especially those on a "long tail", can easily skew the mean, it must be expressed in a transparent manner. Using "survival analysis" goes beyond the mean and median and allows us to present a full and transparent view of MTTR performance.

This year we also included the mean time to respond in addition to the mean time to resolve. Mean time to respond indicates the average time it takes an analyst to assess and provide initial feedback to a client. The mean time to resolve is the average time it takes to assess, triage, contain, mitigate and working with the client to ultimately resolve this issue.

Mean Time to Resolve (MTTR)

True Positive Incidents Resolved Percentage Over Time In Minutes



Summary:

- 40.6% of True Positive incidents are confirmed and resolved within an hour of being raised.
- 72.6% are confirmed and resolved within a day.
- On average, Priority 1 incidents are confirmed and resolved 66 hours after the initial alert was received. Incident priority can only be determined during the course of the investigation and is confirmed when the incident is closed.
- 86.6% of incidents are confirmed and resolved within 5 days.
- Priority 1 incidents were responded to in 15 minutes on average.
- The average response time for a Priority 2 incident is 3.5 hours. Priority 2's mean time to respond is abnormally high and is influenced by one extreme case that significantly increases the average. If adjusted priority 2's mean time to respond decreases to 63 minutes from 210 minutes.
- Incidents rated as Priority 3 were responded to in a little over 1.5 hours on average.
- Priority 4 incidents had an average response time of 7.5 hours.

Threat Detection Data for Small and Medium Businesses

Charl van der Walt - Head of Security Research

Introduction

The analysis presented here draws on operational data from Orange Cyberdefense's Micro-SOC-a service developed specifically for small and medium-sized enterprises (SMEs). One of the service models orients around the deployment, management, and monitoring of Endpoint and Extended Detection & Response (EDR/XDR) technologies, using automation and analyst triage to detect, classify, and respond to threats. Between September 2024 and September 2025, our operational teams handled incidents from 1,943 SME clients, collectively covering 1.5 million monitored endpoints and generating 1.63 million resolved incidents, of which 835,640 (51%) were confirmed as true positives. The median number of endpoints per client was 230. On average, each client experienced 204 incidents per month, including 105 true positives. This dataset offers an unprecedented look into the operational realities of cybersecurity at SME scale-where detection volumes rival enterprise levels, but teams, budgets, and resilience are far smaller.

Key Takeaways

Prioritize Signal Quality Over Quantity

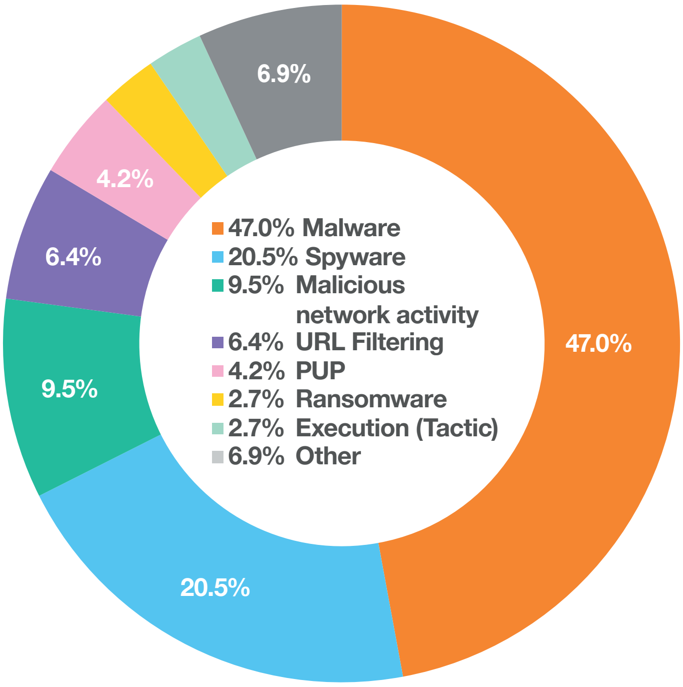
The Micro-SOC data shows that roughly half of all security alerts are false positives. For smaller security teams already stretched thin, this level of noise can consume limited analyst attention and delay the investigation of genuine compromises.

Our data shows that true-positive ratios vary dramatically between different vendors detection platforms, ranging from 67 percent on the high end to 24 percent on the low end. Not all platforms perform the same - both in detection efficacy and false positive ratios - so careful vendor evaluation and tuning may outweigh tool proliferation.

For the SME IT leadership, the challenge is to move from quantity to quality-to focus on the clarity and reliability of detection rather than the number of tools deployed. This means demanding transparency from vendors and managed service providers on true-positive/false-positive ratios, mean-time-to-validate, and automation accuracy, and adjusting service-level expectations accordingly.

Practical steps include establishing joint tuning sessions with the MSSP or MDR provider, reviewing alert classification thresholds quarterly, and insisting that tools provide contextual enrichment (MITRE ATT&CK mapping, behavioral correlation) to distinguish noise from real risk. For SMEs, where each security hire counts, improving signal quality is not a technical optimization-it's an existential efficiency strategy.

True Positive Findings by Classification



Focus on Core Hygiene: Malware Containment and Patch Discipline

Our data suggests that SMEs face an an incident per endpoint every two months, with one true-positive per endpoint roughly every four months. Around 70 percent of confirmed incidents were malware-related, with "generic malware," "cryptominers," and "Trojans" the most common detections, while a further 26 percent involved known software vulnerabilities.

This suggests that SMEs continue to wrestle with opportunistic, commoditized cybercrime campaigns that rely on weak patching or exposed endpoints rather than sophisticated intrusion tactics. The fundamentals remain the Achilles' heel.

SME leaders should therefore channel scarce budgets toward foundational hygiene controls. Ensuring automated patching across all assets, enforcing strong password and MFA policies, and maintaining up-to-date endpoint agents will neutralize most of the attack vectors represented in the data.

Leverage Managed Services Strategically

The Micro-SOC dataset demonstrates the dual power and limitation of automation: 85 percent of incidents were resolved within one hour with the aid of platforms, orchestration and automation, yet the most complex cases took up to five days to close. Despite automation, serious incidents still require real skill, experience, curiousity and persistence to resolve.

This contrast illustrates that while automation effectively handles routine detections, human oversight remains essential for nuanced or multi-stage intrusions. For SMEs that rely on an MSSP or MDR provider as their de facto SOC, this dependency must be actively managed, not assumed.

A strategic approach means establishing clear joint operating procedures with the service provider: defining escalation paths, communication windows, and decision rights for incident containment. SMEs should insist on visibility into unresolved or recurring incident types and review resolution times, automation coverage, and analyst interventions. By engaging with the MSSP or MDR provider as a collaborative partner SMEs can help ensure that responses are prioritized according to real business impact.

Our data here and elsewhere has shown that automation can close the majority of incidents quickly, but it is informed and empowered human partnership that turns outsourced detection into genuine protection. Even a single designated "incident liaison" who understands the provider's processes can drastically improve coordination.

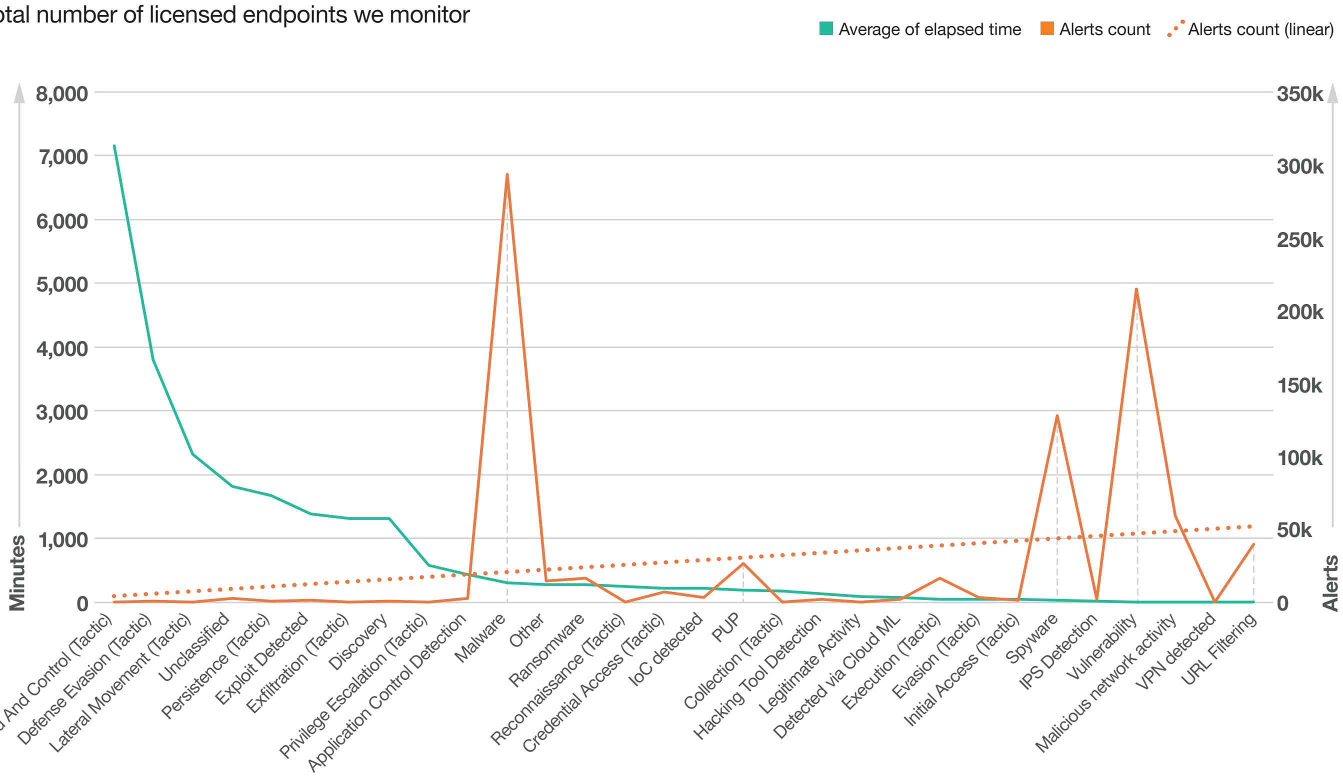
Summary

The Micro-SOC data depicts the reality of cyber defense at SME scale: enterprise-level alert volume, but limited human and financial capacity. Core hygiene like strong authentication, malware prevention and patch discipline remain the highest-yield investments, but SMEs also need to optimize for signal quality by tuning tools and demanding measurable detection accuracy.

Managed Security Services need to be approached as a collaboration, not delegation by building visibility, governance, and partnership into every SOC relationship.

Average Time to Resolve by Incident Category

Total number of licensed endpoints we monitor



Time To Resolve Main Findings:

- 85% of all incidents are resolved and closed within the 1st hour after the alarm is raised.
- 90% of incidents are resolved after 4 hours.
- By 72 hours 95% of all incidents have been resolved.
- 4% of issues analyzed remained unresolved during the period in our dataset.

Vulnerability Scanning Data

- **Wicus Ross** - Senior Security Researcher

About the Data

- **Unique assets:** 60,837
- **Unique findings:** 1,289,451
- **Analyzed period:** October 2024 to September 2025
- **Data sources:**
  Scan findings from external web facing assets and internal network equipment, servers, desktops, printers, etc.

The Orange Cyberdefense vulnerability operations centers (VOC) record a wide range of impactful vulnerability scanning findings on client assets. These findings provide a glimpse into the reality that vulnerability management teams face.

Findings are not just software vulnerabilities described by Common Vulnerabilities and Exposures (CVE), but also misconfigurations, default credentials, and more. A finding is identified by a scanning engine that uses heuristics, proprietary fingerprinting techniques, or well-known behaviors to determine potentially unwanted exposures. These detections may be imperfect and are influenced by various factors in the environment, potentially distorting findings. False positives are infrequent and are confirmed only when the scanning vendor cannot verify the impact after the original finding is challenged.

Terminology

We will use “unique assets” and “unique findings” throughout this section. Unique findings are always associated with an asset, and the unique asset is associated with a client.

Unique assets are defined in terms of Client, Asset Name, IP Address and Host Type.

A unique finding is defined in terms of a unique asset, with the addition of the ‘Finding Name’ and details assigned by the scanning engine.

Findings by Severity

The average severity and total severity distribution of findings for Security Navigator 2026 follow a similar trend to what was reported in the previous year. The most notable change is for findings rated medium, which recorded the most significant decrease while findings rated critical, high, or low increased.

Findings severities are defined as:

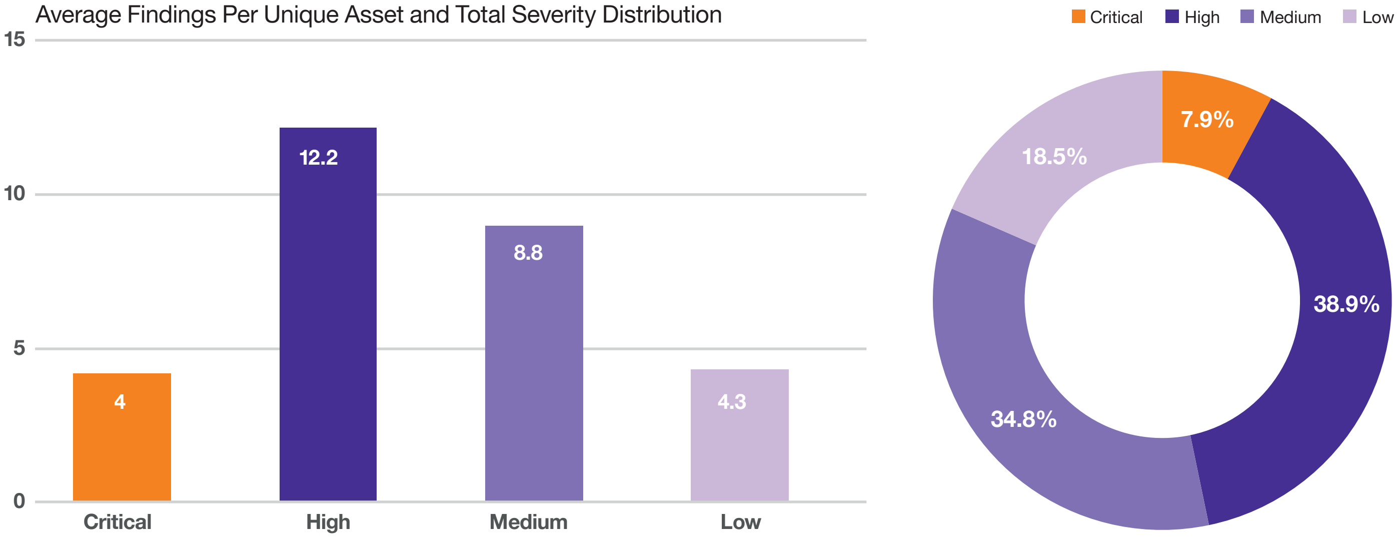
- Critical: Attackers can easily gain control of a host and this could potentially allow lateral movement.
- High: Attacks can use this vulnerability to obtain access to the host.
- Medium: Attackers can read contents of sensitive information on the impacted host. This may assist with gaining access to that host, for example direct file level access and directory browsing access.
- Low: Sensitive information about the host can assist an attacker to better target known vulnerabilities specific to the exposed host or service.
- Informational: Details of the system or service is divulged to attackers that can use this as part of their reconnaissance to find other possible associated weaknesses.

These finding fluctuations are unpredictable and a feature of the complex systems that attackers and defenders both operated in. This results in an evolving attack surface that continues to expand. Our data sheds light on the way our clients respond to the growing volume of vulnerabilities while also balancing growing business demands.

The average number of medium-rated findings per unique asset decreased by 1.49 from 10.37 previously to 8.8. Medium-rated findings also decreased from 40.65% previously to 34.79% now as a total share of all finding severities.

Severity of Findings

Average Findings Per Unique Asset and Total Severity Distribution



At the same time the average findings per unique asset rated critical and high increase from 3.72 and 11.14 previously to 4 and 12.22 respectively. As a result, the total share of severity for findings rated critical and high increased from 7% and 37% previously to 8% and 39% respectively. The increase in these numbers may not appear to be much, but findings of these severity ratings do require more attention from teams and will detract from other tasks. Findings associated with easily exploitable or actively used vulnerabilities can create extra pressure, especially with the continuous threat of cyber extortion or ransomware looming.

The growth of the average low severity finding per unique asset from 3.88 to 4.3 translated into the largest increase of total severity share, from 15% to 19%. Although the average findings per unique asset seem to have increased slightly, it is nowhere near the high average numbers reported in Security Navigator 2024. The change in the shape of findings, specifically the increase in critical and high rated severities, is indicative of the importance of proactive vulnerability management, as described in the Security Navigator 2025 chapter titled "Beyond vulnerability management". Eliminating classes of vulnerabilities can only be achieved through adapting systems to new methodologies and architectures.

Age of Findings

It seems that organizations continue to struggle with eliminating vulnerabilities in their environments. This is evident by the increasing age of findings across the severity spectrum. This could also be ascribed to possible accepted risks that are managed within an agreed framework.

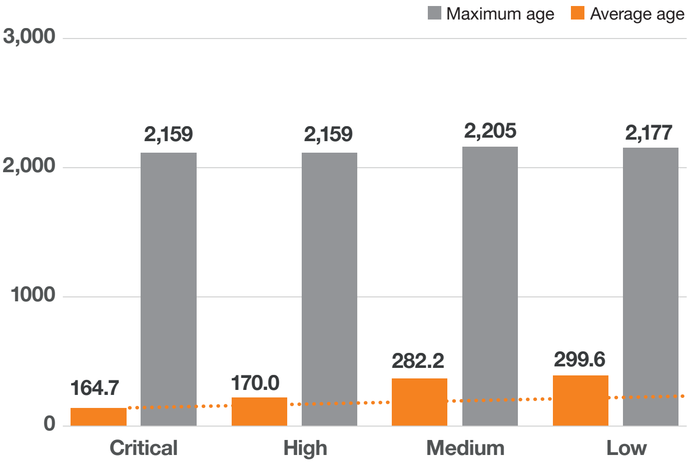
The increasing age of findings in environments has been a recurring theme for the past two years, and this year is no exception. Previously we highlighted an outlier, an account in the Retail and Trade industry, that skewed the maximum age. This outlier is still present in this year's dataset, but with a relatively lower maximum age. This could mean that findings associated with this extreme age have been remediated or the assets with the troublesome findings have been removed. Removing this outlier with all its associated findings from the dataset does slightly increase the average age of findings for findings rated high, medium or low. This suggests that this outlier also has findings of much younger age in addition to the long-lived findings.

Examining the dataset without the outlier surfaces a similar historic trend, namely that the maximum age of all findings reaches a consistent ceiling (2,159 to 2,205 days). The maximum age recorded for all findings also increases by approximately 350 days over the previous (1,855 previously compared with 2,205 now). As observed in the past, this means that findings continue to linger in environments for extended periods growing the long tail of findings in our dataset.

Almost 79% all VOC findings are 1 year old or younger; 56% of all VOC findings are 180 days old or younger, while 19% of all findings are less than 30 days old. Just over 65% of all findings within the 180-day window are older than 30 days. The majority of new findings therefore live for as long as six months, but patching teams are apparently working hard to keep these within a certain acceptable range.

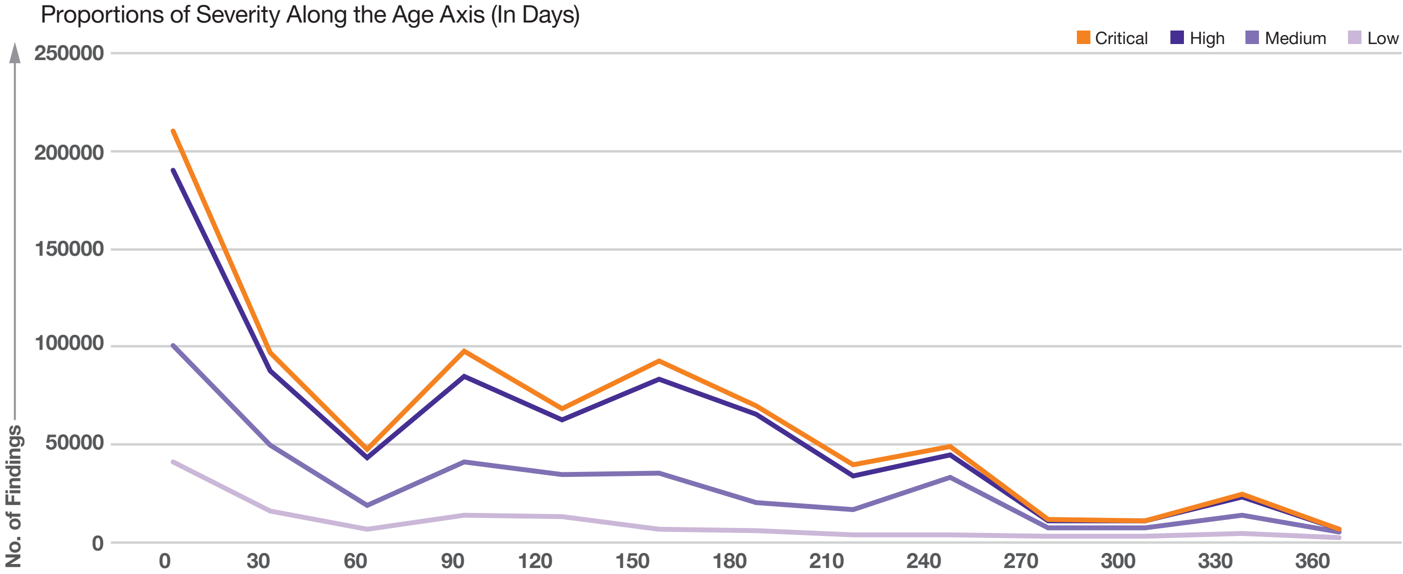
Age of Findings

Average and Maxium of Vulnerabilities Found in Days

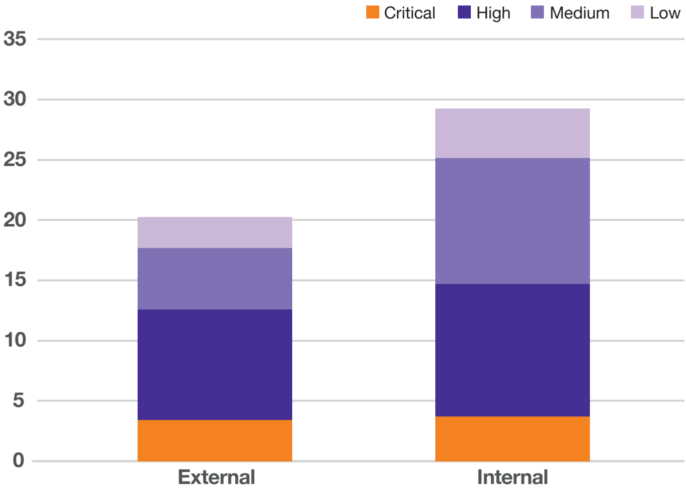


Severity Over Time

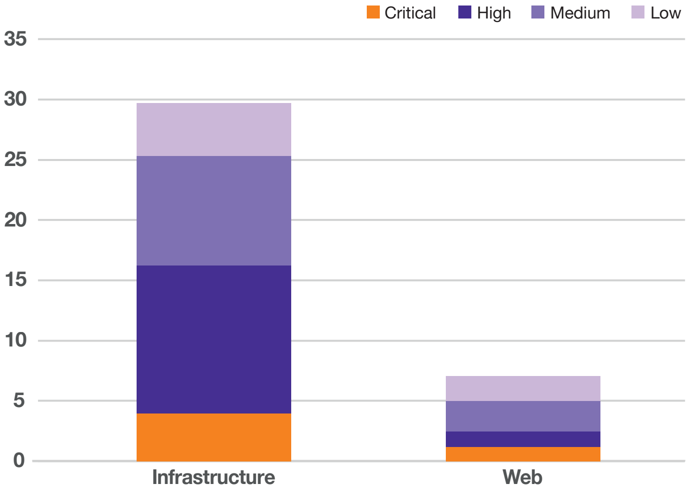
Proportions of Severity Along the Age Axis (In Days)



Finding Severity by Target Exposure



Finding Severity by Target Type



Operating System Exposure

In Security Navigator 2025 emphasis was placed on the relatively larger number of findings rated "high", especially for assets classified as "external" to the organization. This year the average number of severities rated high decreased to 9.01 from 10.5. Average findings for assets classified as external decreased slightly, but the average findings for assets classified as internal remained about the same. This is rather different from our previous report where we reported a sharp rise in average findings per target.

The average findings per target type for web and infrastructure recorded a slight change compared with figures observed in 2025. Infrastructure saw a slight increase (2.5%) in the average number of findings per asset. Contrary assets labeled as target type "web" decreased 15% in the number of average findings per severity. This decrease might seem like a major improvement, but we should bear in mind that the actual numbers are small, and any change is exaggerated when expressed in percentage terms.

The relatively noticeable difference in the average number of findings between the various asset classes is perhaps down to their nature or purpose. External web-facing services will generally be exposed to greater threat of exploitation compared with internally hosted services that are protected by the typical firewall or network router. Does this say anything about the effectiveness of the classical castle and moat approach to cybersecurity? If that is the case, then within those castle walls lies much greater potential for mischief.

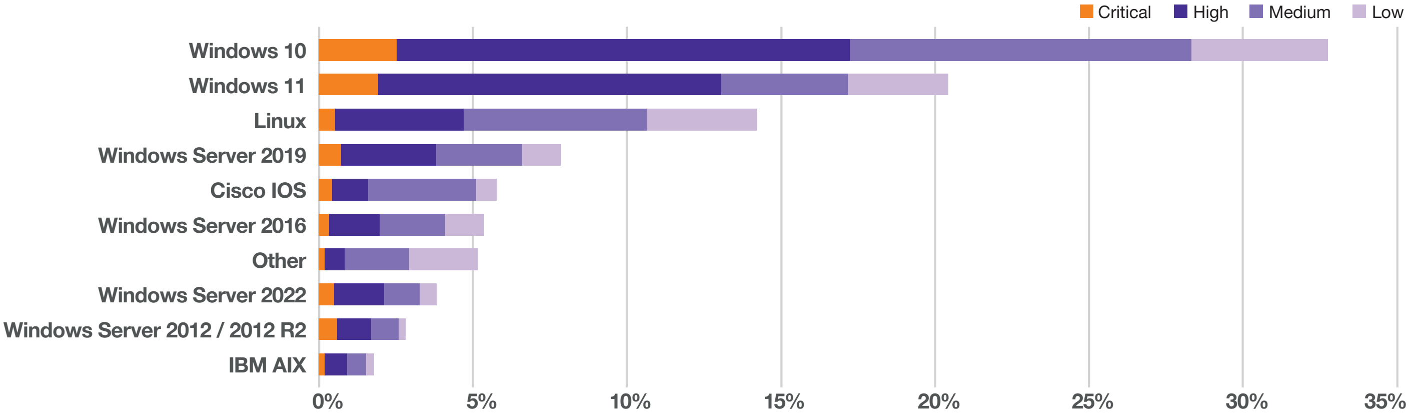
When examining the top 10 operating systems (OSs) in terms of proportion of findings, Microsoft Windows desktop and server OSs stand out, with assets running Windows 10 and 11 ranking as the largest contributors. Windows Server only represents 20% of findings, whereas Windows 10 and 11 together represent 53% of all findings. Assets identified as Linux OS claim a combined 14% of findings.

The picture does not change much when only focusing on findings with a severity rating of critical or high. Assets associated with Windows Server claim a combined share of 20.02% of findings rated critical or high. Windows 10 and 11's share increases to 63% of all findings in the top 10 comparison. For the same comparison, Linux accounts for 10% of findings rated critical or high.

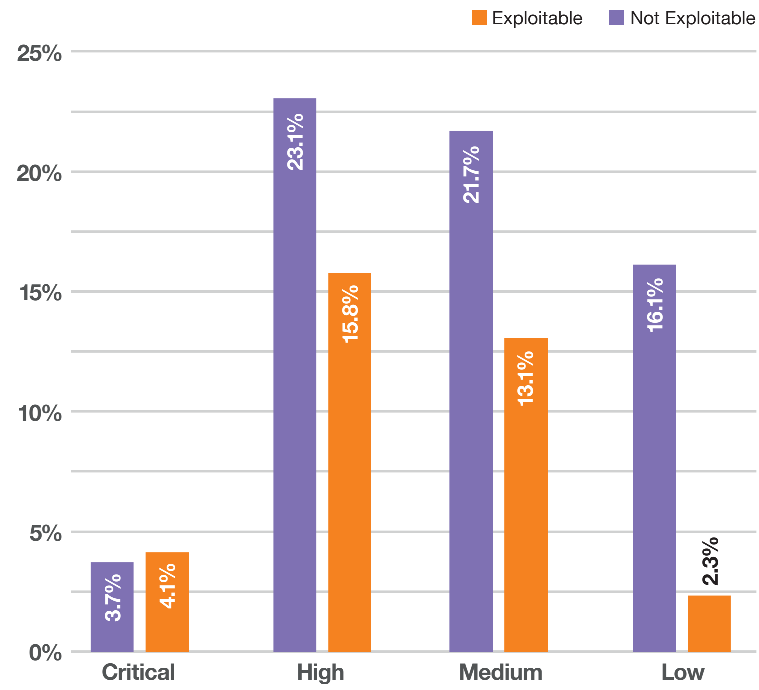
Does Windows 10 and Window 11 represent the soft underbelly of the enterprise?

Proportion of Findings Severity by OS-Top 10

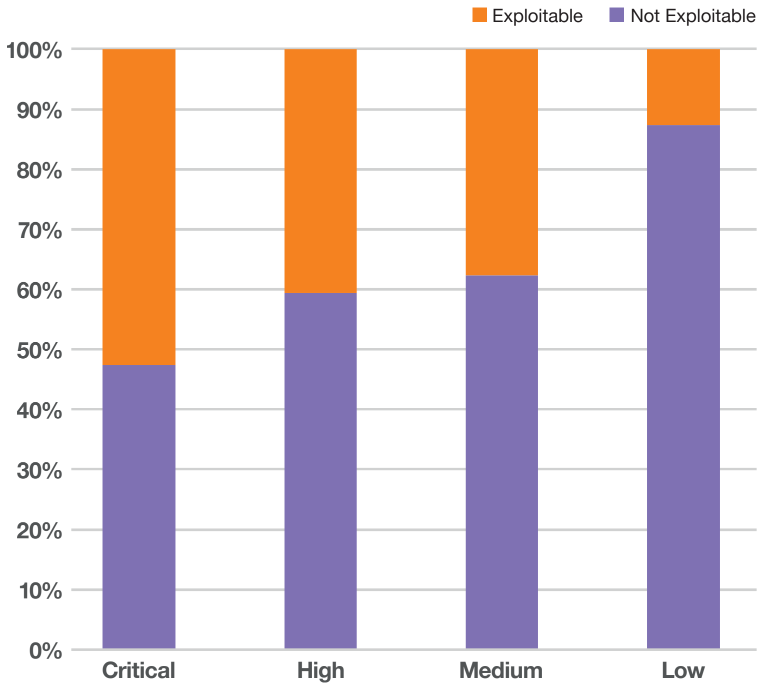
Sorted by Sum of Percentage of Total Findings



Exploitablity per Finding Severity



Proportion Of Exploitablity per Finding Severity



Exploitability

A different angle can be explored by considering findings that are potentially exploitable. The determination of whether a finding is exploitable or not is provided by the various scanning engines using their own proprietary threat intelligence. This “exploitable” status is merely a judgement call by the scanning engine and may require specific conditions before said findings could be leveraged successfully in reality. Conversely, many findings rated low or medium on their own would not yield any effective exploit, but successfully chaining some of these together may upset some people. The “exploitability” datapoint should therefore be taken with a grain of salt.

Most findings-or 65%-are considered not exploitable. The remaining 35% are considered exploitable. Low (2%) and medium (13%) findings together account for approximately the same proportion of exploitable findings as those rated high (16 %).

Critical findings are the only category where the proportion of exploitable findings is higher than the proportion that’s not exploitable.

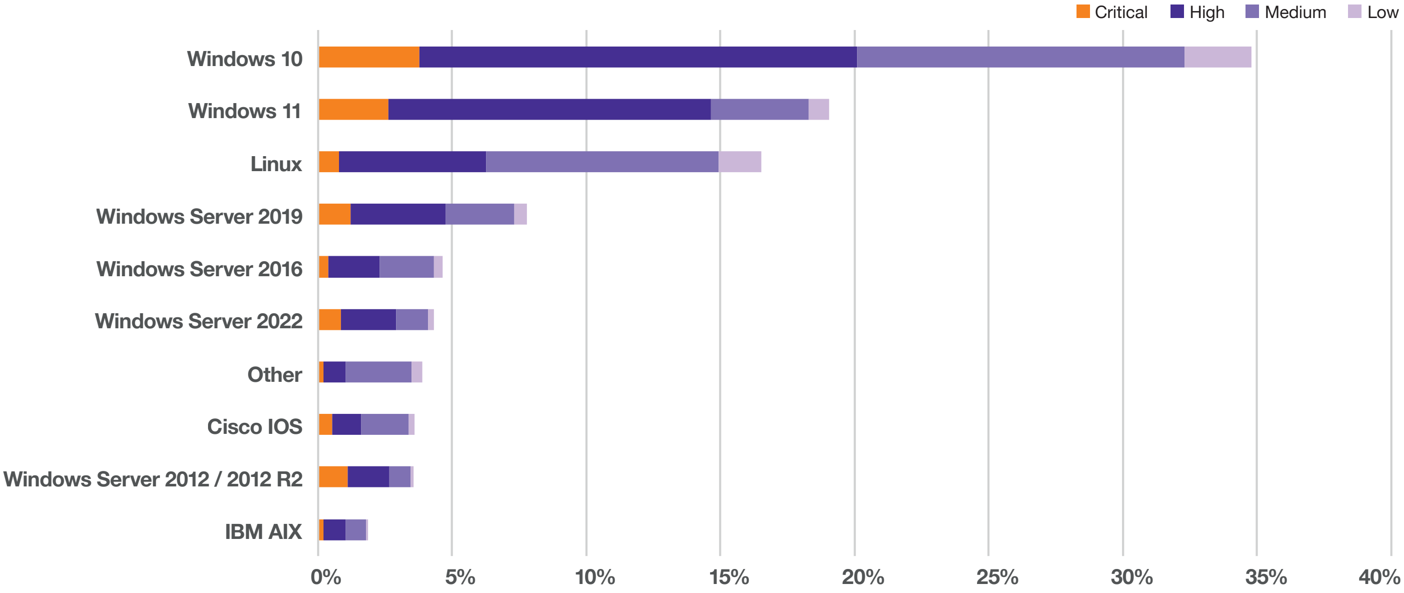
Exploitability in Operating Systems

Findings considered exploitable in terms of OS classification reveal a picture that resembles our prior findings regarding operating systems. Windows 10 and Windows 11 once again standout with 36% of findings considered exploitable. Similarly, the Windows Server 2019 findings considered exploitable account for 36% of all findings for the group of Windows Server editions. Linux has a higher proportion of exploitable findings, with 41% considered exploitable. Linux does however have a slightly lower number of exploitable findings compared to all Windows Server types combined, with a ratio of 1.23 exploitable Windows Server findings for every 1 exploitable finding on Linux.

Windows 10 ranks first out of the top 10 OSs for the proportion of findings considered exploitable. This must be a serious warning for organizations that still plan to use Windows 10 in the future as Microsoft has ended general support for Windows 10 on 14 October 2025[160]. The percentage is calculated as a share of all exploitable findings in the top 10. Linux’s share of exploitable findings is considerably higher than each edition of Windows Server separately, but Windows Server as a group nudge just ahead as suggested earlier.

Proportion of Exploitable Findings per Severity by OS-Top 10

Sorted by Sum of Percentage of Total Exploitable Findings



> Locating and remediating vulnerabilities pertaining to unpatched software or insecure configurations remain a persistent challenge for cybersecurity and IT teams. Modern IT environments create powerful yet complex ecosystems that often introduce new and persistent security risks.
>
> A small group of major vendors supplies most of today's IT infrastructure, but size offers no immunity to flaws: no system is entirely secure or error-free. Technology users must therefore demand higher standards and insist on products that are secure by design.
>
> It is time for system designers and administrators to urgently reimagine both information and security architectures to address entire classes of weaknesses, not just individual flaws.
>
> - **Tim Overgaard** - Vulnerability Management Technical Lead

The Hidden Cost Of Vulnerabilities in Security Products

▪ **Charl van der Walt** - Head of Security Research

Background: Managing Vulnerabilities

In addition to data from vulnerability scanning, we can draw insight from operational data gathered by Orange Cyberdefense's global SOC (Security Operations Center) teams between January 2023 and October 2025. Over this period, analysts logged 19,125 tickets related to vulnerability advisories affecting 25 different security vendors, including firewalls, VPNs, and other perimeter defense technologies. Each ticket generated multiple actions, or "tasks," whose time investment was carefully recorded, enabling an empirical view of the operational load imposed by vulnerability management for perimeter security technologies.

The data reveals a steadily rising burden: the number of vulnerability-related tasks increased by 14% month to month since 2023, while the average time per client per month remains around 3-4 hours despite process and automation gains. This body of evidence provides a unique, ground-level perspective on how defensive technologies themselves are contributing to systemic cybersecurity strain.

Treat Security Products as Critical Assets

The report reveals an uncomfortable paradox: The very technologies designed to protect networks are increasingly becoming primary attack surfaces.

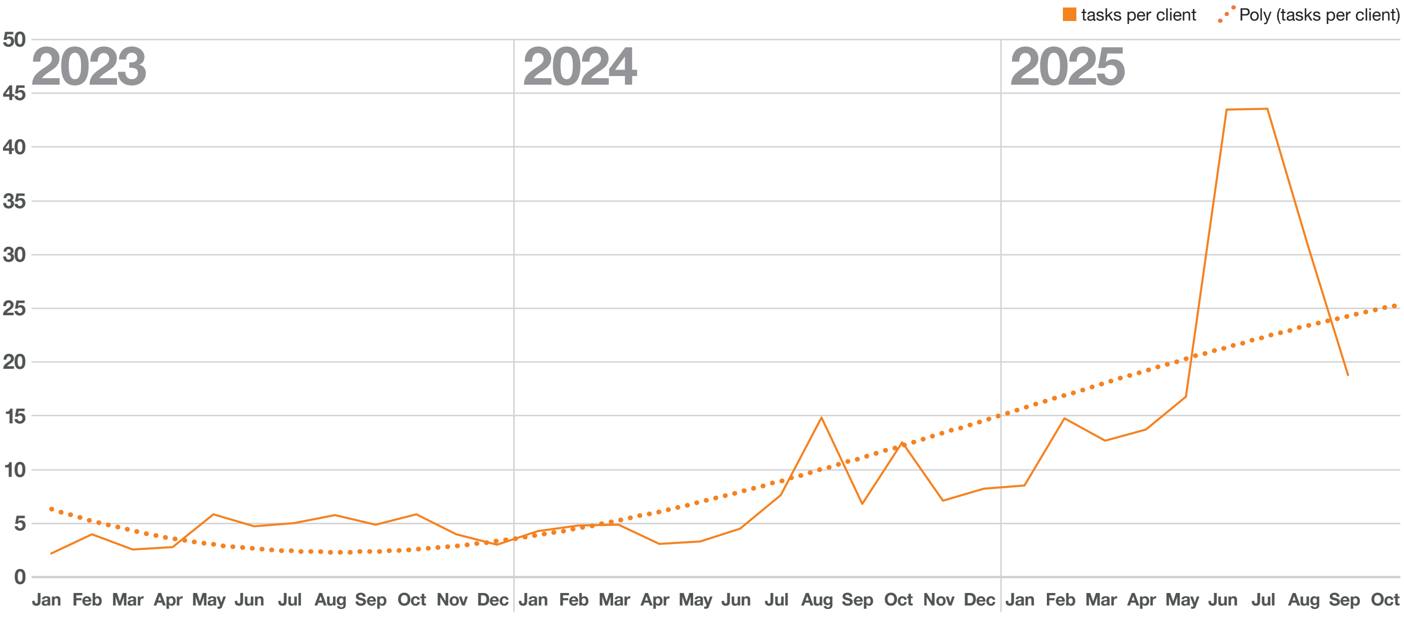
Perimeter devices such as firewalls and VPNs are not merely targets of opportunity but have become chosen points of entry for ransomware and state-sponsored actors. Vulnerabilities in these systems are often exploited almost immediately upon disclosure, leaving minimal window for defenders to respond.

For CISOs, this demands a mental and procedural shift. Security products must be managed not as inherently trustworthy controls but as high-value, high-exposure assets within enterprise threat models.

By treating these devices as attack surfaces rather than unquestioned barriers, organizations can reduce the likelihood that a breach will originate from within their defensive infrastructure itself.

This mindset should extend to procurement and vendor management. When evaluating new security tools, CISOs must weigh not only detection efficacy and feature set but also historical vulnerability posture, disclosure discipline, and patch responsiveness. The goal is to make discoverability, transparency and manageability defining criteria for technology acquisition, not just functionality or brand reputation.

Tickets vs. Vulnerabilities on Clients



Budget for the Hidden Cost of Vulnerability Management

The data shows that the operational load of vulnerability management is rising relentlessly: despite process improvements, our expert teams are required to perform an average of ~10 vulnerability-related tasks per client per month at an average investment of ~4 hours per client per month. This represents a “hidden tax” on cybersecurity which is an unbudgeted operational burden consuming scarce analyst time, extending mean-time-to-remediation, and inflating the total cost of ownership for defensive technologies.

For CISOs, this insight translates directly into budgeting and workforce planning. Investment models can underestimate the manpower required to maintain “securely configured” environments. The reality, shown by SOC data, is that vulnerability response in security tools competes directly with other mission-critical activities like incident response and detection engineering. CISOs should therefore explicitly model and fund vulnerability-management overhead as a recurring operational cost, not an exception.

Ticket automation, patch verification workflows, and vulnerability intelligence feeds can help teams reclaim analyst time and reduce burnout. But ultimately, this shift acknowledges that the cost of staying secure is not static. Whether to develop internal capabilities, or budget for appropriate outsourcing, sustained, realistic funding is critical to long-term resilience.

Demand Greater Vendor Transparency and Standardization

In the face of a relentless onslaught of vulnerabilities and attacks, our SOCs are encumbered by inconsistent advisory formats across vendors, divergent severity ratings, incomplete disclosure details, and licensing barriers that can impede timely remediation.

These structural and commercial inconsistencies slow automation, confuse prioritization, and amplify enterprise exposure to risk. CISOs are therefore urged to advocate for new standards of transparency and accountability in their vendor relationships with measurable procurement and governance criteria.

Vendors should be called upon to publish advisories in machine-readable formats (such as CSAF), align CVSS scoring, reference CISA KEV inclusion or EPSS, and provide unambiguous patch timelines. The UK NCSCs Software Security Code of Practice offers a useful guide to supplier negotiations resources to ensure providers are complying with the Code to deliver software that is secure and resilient[161].

Where possible, customers and MSSPs should coordinate to develop shared playbooks for vulnerability assessment and mitigation, ensuring that intelligence and patch workflows are synchronized.

Our data and experience points to an industry-wide failure in securing its own defensive technologies. Rectifying this will require precisely the kind of cross-stakeholder transparency and consistency that only customer pressure can produce. By demanding these standards collectively through industry associations, Information Sharing and Analysis Centres (ISACs), or vendor alliances, security leaders can help reduce the systemic friction that currently burdens SOCs and enterprise patching team.

Summary for Security Leaders:

Vulnerabilities in defensive technologies are eroding trust in the very systems designed to protect enterprises, while the operational load required to maintain them is escalating.

Security leaders must therefore treat defensive tools as assets, budget realistically for their upkeep, and demand far greater vendor transparency.

- **Charl van der Walt** - Head of Security Research

Cyber Extortion (Cy-X) Monitoring Data

▪ **Diana Selck-Paulsson** - Senior Security Researcher

Since January 2020, 18,943 victim organizations were observed on leak sites. These leaks are from 191 distinct Cy-X brands. The timeframe we consider for our annual analysis is always between October of the previous year to the end of September of the current year, providing us a 12-month overview of current cyber extortion trends.

Between October 2024 and September 2025, a total of 6,142 victims were documented, linked to 91 distinct Cy-X brands. This equates to a 44.5% increase in victims since last year's report.

The first quarter of 2025 was particularly active, driven largely by Cl0p's mass exploitation of the Cleo vulnerability. First observed in 2019, Cl0p quickly built a reputation for its large scale attacks, primarily targeting file transfer platforms. The group has previously claimed numerous victims, with its most notable campaigns leveraging vulnerabilities in the Accellion (2020), SolarWinds (2021), GoAnywhere (2023) and MOVEit (2023) solutions. This illustrates how a single vulnerability in widely used software can dramatically shape the criminal ecosystem, creating a surge of opportunistic attacks. In this case, that single event accounted for around 18% of all victims recorded during Q1.

Cy-X Over the Years

We observe a continuing upward trend in the number of Cy-X victims. As can be seen below, our 2025 data only includes the first 9 months of the year but has already exceeded the full year numbers from 2024. The number of victims has increased more than threefold since 2020 (from 1,497 to 4,685), while the number of distinct actors nearly tripled (from 33 to 89), reflecting the sustained expansion and diversification of this threat. We need to acknowledge, however, that some of the increase in actors might simply be the same actors operating under new brands.

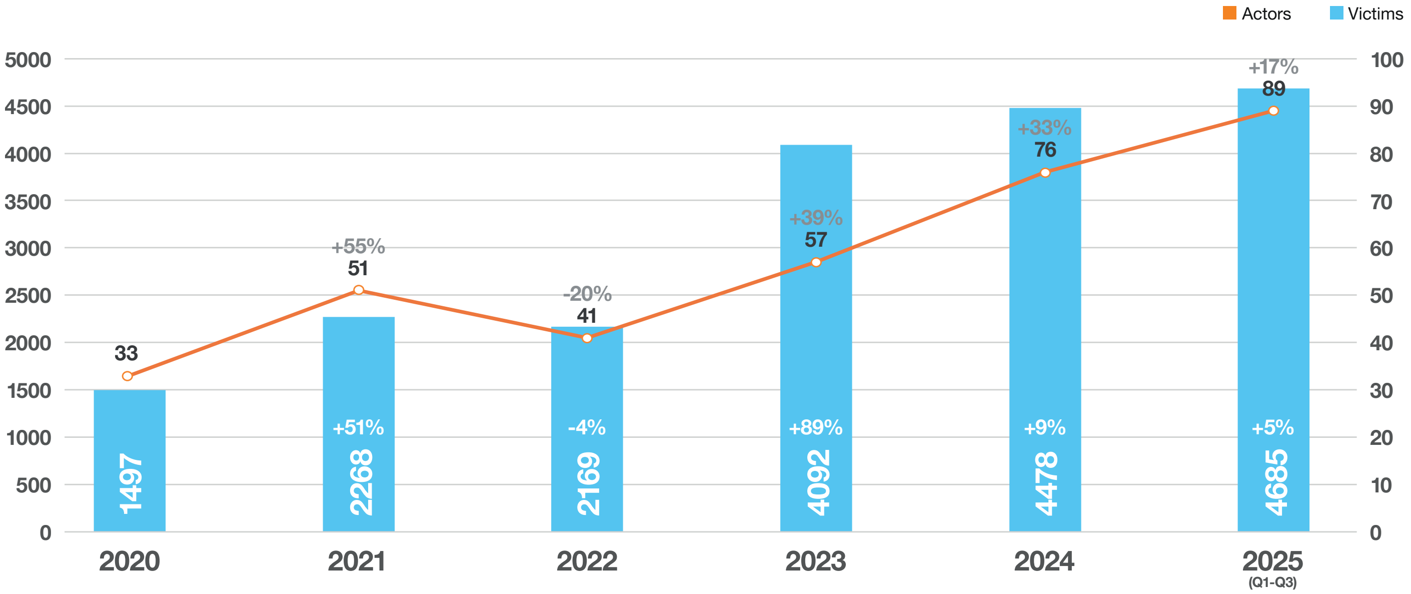
The obvious 2022 dip corresponds to the start of the war against Ukraine and collapse of the Conti ransomware collective, one of the most organized and influential groups until that year. After declaring support for Russia, Conti experienced a major internal leak that exposed its infrastructure, communications, and affiliates, leading to its dissolution. This incident fragmented the Cy-X ecosystem, as former members dispersed into smaller or rebranded entities (e.g., Black Basta, Royal, Quantum, Karakurt), temporarily reducing coordination and thus visibility in victim reporting. A re-emergence and diversification phase followed in 2023, characterized by a sharp resurgence in both victim and actor counts. Successor groups built upon Conti's operational legacy, that have been seen contributing to a more fragmented yet prolific ecosystem that expanded its scope while maintaining high activity levels.

Operational efficiency has also increased 18% over time, with the victims-per-actor ratio rising from approximately 45 in 2020 to 53 in 2025. This could suggest a growing industrialization through shared infrastructure, affiliate programs, and tool reuse.

Finally, the 2024-2025 period indicates relative stabilization.

Cy-X Over Time

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



Threat Actor Analysis

The current landscape is marked by a fundamental structural shift at the actor level. Whereas previous years were defined by single dominant groups like Conti in 2022 or LockBit through 2023 & 2024, the period between October 2024 and September 2025 demonstrates a transition toward a more decentralized balance of power. Multiple highly active groups now operate at volumes that previously only one collective could achieve. This year Qilin (600 victims), Akira (550), Cl0p (473), RansomHub (471), and Play (407) together represent a new era in which several actors sustain comparable, large-scale operational output.

Qilin and Akira are the most prevalent Cy-X actors in Europe when evaluated by number of victims, which increased 324% and 168% respectively since the previous period.

This development suggests both a fragmentation and professionalization of the Cy-X ecosystem. Rather than signaling decline, the dissolution of previously dominant groups like LockBit3, Black Basta, and BianLian has resulted in the redistribution of activity across multiple successor or emergent actors. We are observing a continuously adaptive and decentralized threat environment, where law enforcement action, internal fragmentation, or shifting affiliate allegiances rapidly surface different actors without reducing overall impact.

Basic TTPs

Threat actors have varied means of gaining access to environments. The general theme remains, don't reinvent the wheel if what you have works. Phishing in all its forms remains a tactic that has proven to be successful repeatedly. Account compromise is another frequently cited tactic that involves the reuse of credentials, brute forcing credentials, or simply buying stolen credentials off the dark web. Exploitation of vulnerabilities in public facing APIs, security solutions such as VPNs and firewalls, communication and managed file transfer services are all part of the game.

Cl0p is known for its exploitation of public-facing APIs, and some intrusions are also linked to phishing.

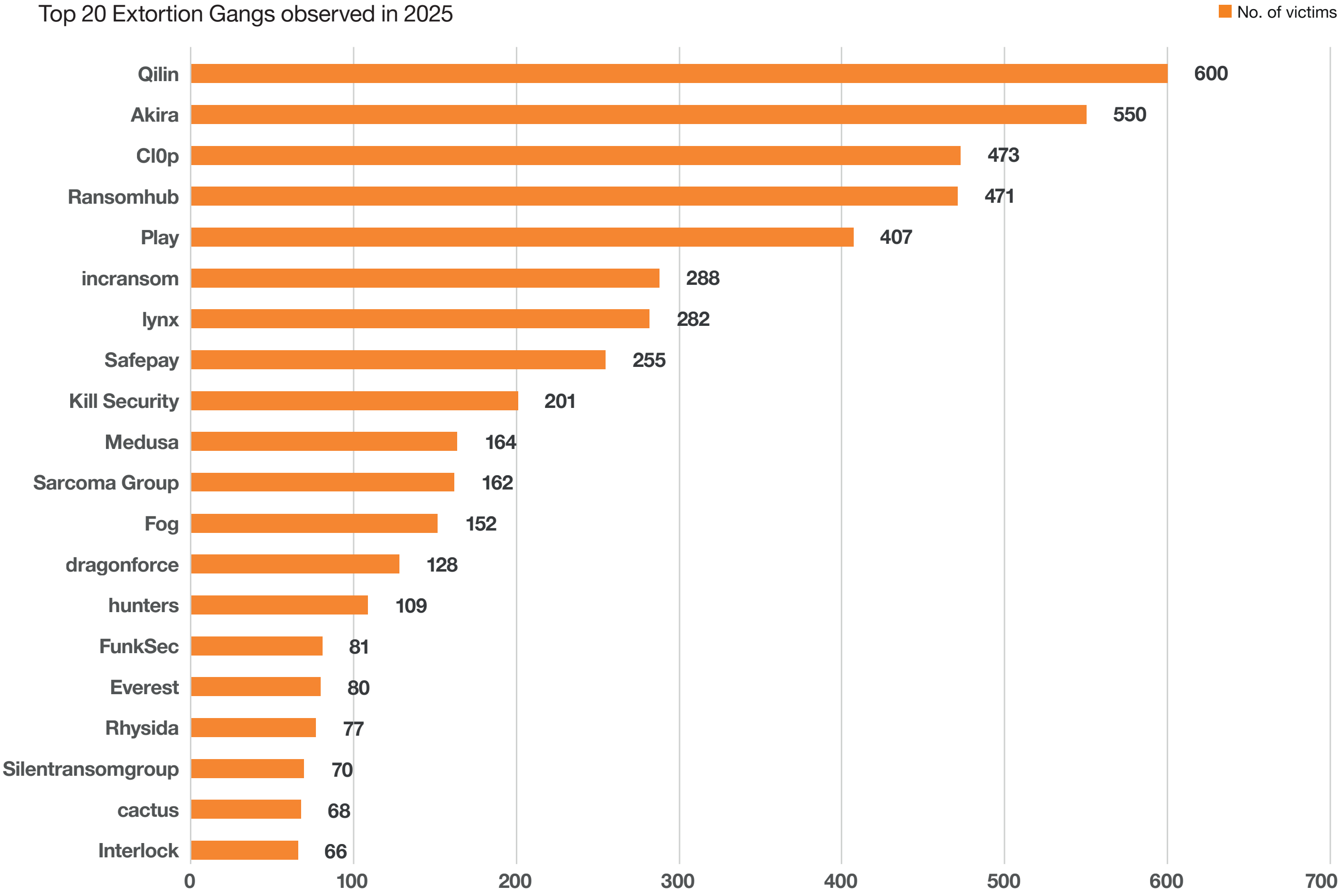
Qilin's TTPs include phishing with spear phishing specifically mentioned. It also includes gaining access by exploiting public-facing applications and using valid accounts.

Incransom follows with initial access vectors including valid accounts, phishing, as well as exploiting public facing applications such as firewalls and VPN services.

The now-defunct Ransomhub was known to gain initial access through spear-phishing, exploiting vulnerabilities in internet facing applications, and password spraying.

Most Active Cy-X Actors

Top 20 Extortion Gangs observed in 2025



Business Size

Organizations of all sizes have been affected by Cy-X attacks over the past year. In this analysis, business size is classified according to the OECD standard: Small businesses are defined as those with 1-49 employees, medium-sized businesses range from 50 to 249 employees, and large organizations have 250 or more employees.

Small organizations were the most affected, followed by medium-sized and large enterprises but as in previous years, the distribution across business sizes remains relatively even.

When normalizing growth rates against the overall 44% increase in total victims, the data reveals a clear shift. Small businesses (+12%) and medium-sized organizations (+5%) grew faster than the overall trend, indicating a proportional increase in their share of total victims. By contrast, large organizations (-17%) expanded more slowly, resulting in a relative decline in the proportion of victims. This pattern implies that the ecosystem's expansion in 2025 disproportionately affected small and mid-sized firms.

Which Groups Attack Which Business Sizes?

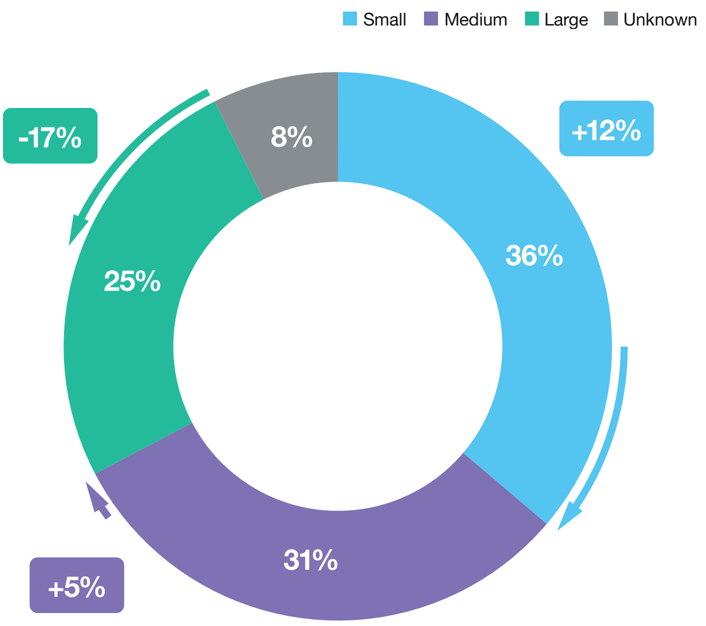
The business size versus actor table below reveals diverse impacts across the ten most active extortion groups. Qilin exhibits the highest overall activity, with a concentration on small and medium-sized enterprises, suggesting a high-volume, mid-tier strategy.

Akira and Play similarly primarily impact medium-sized firms, suggesting either strategic selection or opportunistic targeting. Safepay and Kill Security proportionally impact more smaller business. By contrast, Cl0p and Ransomhub demonstrate a balanced distribution across all business size categories. This suggests broader technical reach, consistent with their history of mass exploitation campaigns that impact organizations of various sizes.

Finally, Cl0p and Medusa claim the highest proportion of large businesss across their victims.

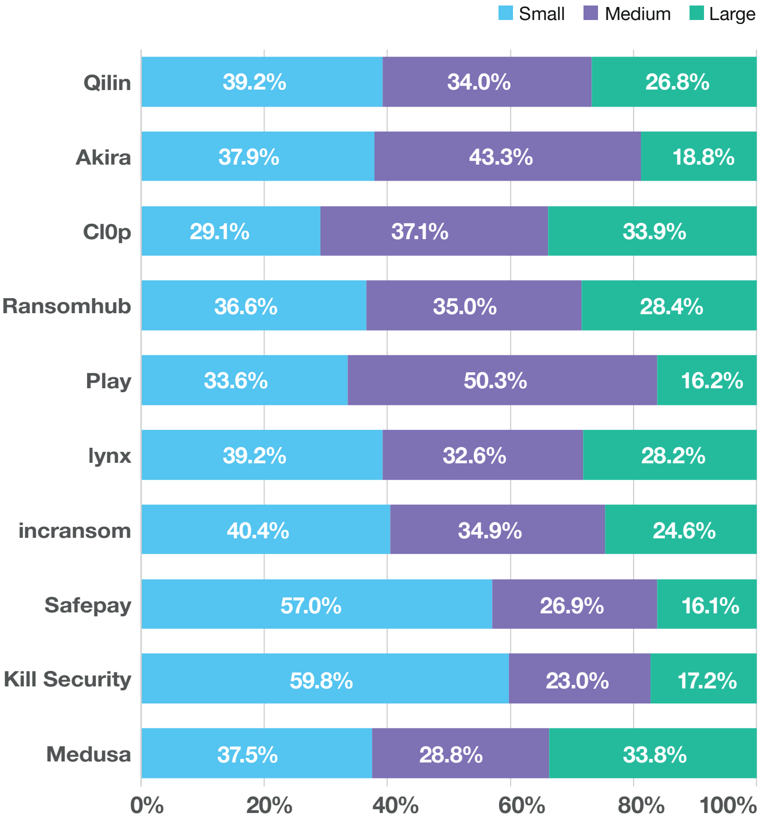
Actor	Small	Medium	Large
Qilin	221	192	151
Akira	198	226	98
Cl0p	128	163	149
Ransomhub	157	150	122
Play	135	202	65
lynx	107	89	77
incransom	110	95	67
Safepay	138	65	39
Kill Security	104	40	30
Medusa	60	46	54

Proportion of Victims by Size



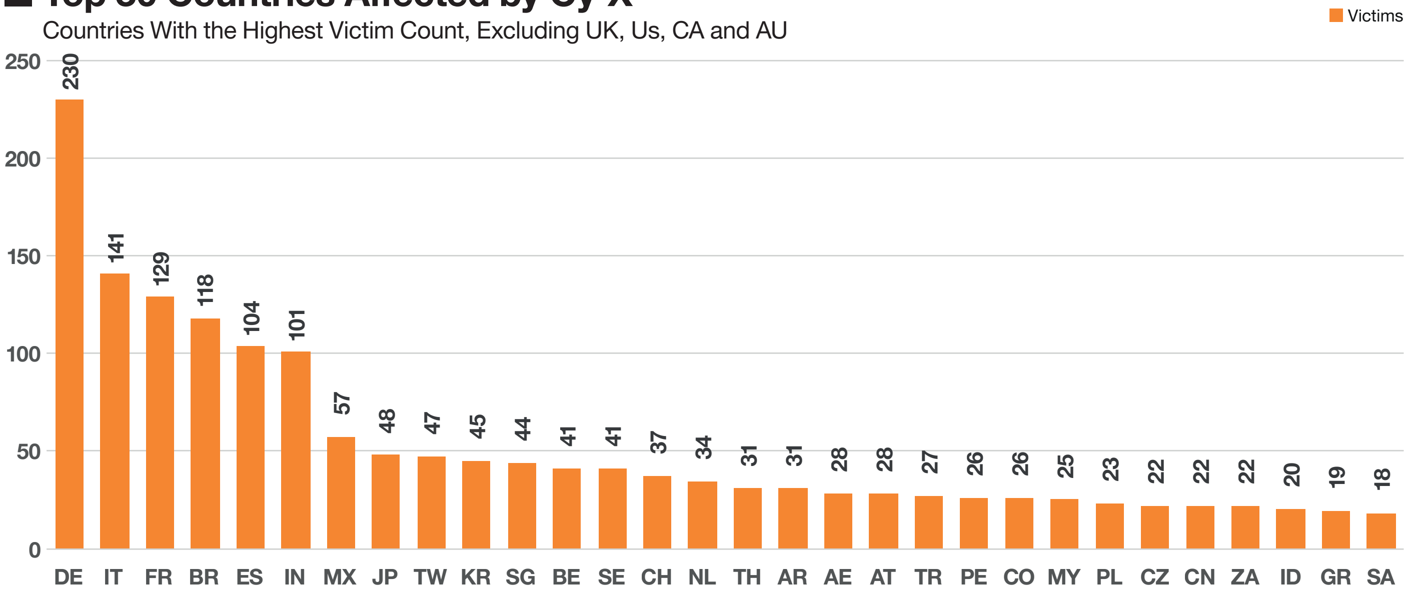
Victim Size by Actor

Top 10 Actors by Business Size in Order of Total Number of Victims
S = 1-49, M = 50-249, L = 250+



Top 30 Countries Affected by Cy-X

Countries With the Highest Victim Count, Excluding UK, Us, CA and AU



Regional Analysis

The United States and Canada collectively remains the most heavily impacted region, with 3,780 victims recorded in the past 12 months - an increase of 56%. The continued dominance of this region as the primary victim of extortion is likely due to its economic density, advanced digital development and the predominance of English as a business language. Europe (901 victims, +19%) remains the second most affected region, while Latin America (+60%) and East Asia excluding China (+82%) recorded some of the highest proportional increases.

Cyber extortion is continuing to globalize beyond the traditional transatlantic corridor. West Asia (+45%), the Caribbean region (+100%), and South Asia excluding India (+120%), though smaller in absolute numbers, demonstrate emerging regional exposure and growing threat actor reach.

A notable finding is the geographic diversification of victims, with newly impacted countries emerging across nearly all regions. For this report, we added 35 countries where victims were not previously observed in the past 5 years. Africa experienced the largest expansion, with 10 countries added to the dataset for the first time, followed by Europe (5), the Caribbean (4), and Southeast Asia (4). As we have cautioned previously, this demonstrates that extortion activity is no longer confined to established geographies and economies but is increasingly reaching previously peripheral or lower visibility victims. The inclusion of new countries across regions like Oceania, Central Asia, and West Asia further underscores this.

The data therefore points to a widening global footprint, where the traditional concentration in North America, the UK, and Europe coexists with a growing penetration into the rest of the world.

Victims at Country Level

Excluding the typically most-impacted Anglophone countries (see above), the distribution of impacted nations highlights the growing prominence of continental Europe and emerging economies among the victims. Germany (230 victims), Italy (141), and France (129) lead the list. Meanwhile, Brazil (118), India (104), and Mexico (57) stand out as leading targets in the Global South. East Asian and Southeast Asian economies such as Japan (48), Taiwan (47), and Singapore (44) also recorded substantial victim activity.

Overall, the data indicates that while Cy-X operations remain concentrated in large, advanced Anglophone economies, there is clear geographic broadening toward middle-income and high-growth regions, consistent with the ecosystem's wider global expansion observed in 2025.

Business Sizes per Region

The overall trend toward growth in small and medium-sized businesses outlined earlier speaks to the tremendous volume the United States of America (US) contributes in terms of Cy-X victim count. Small businesses (+91%) in the US are taking most of the Cy-X actor heat by nearly doubling and breaking through the four-digit ceiling mark in reaching 1,327 victims. There are more victims in the small business sector in the US than there are victims in all the business sizes in Europe and the UK combined. Medium sized businesses (+61%) in the US may not have grown by as much but also reached a new high of 1,214 victims. The two US business sizes represents a significant part of the overall victim count.

In Europe small businesses are impacted the most in terms of volume, but the large (+25%) and medium (+32%) sized businesses are growing much faster compared to smaller businesses (+7%) in terms of victim count.

The impact of Cy-X on German businesses is increasing. The Cy-X victim count was up for all business sizes in Germany. The victim count for large businesses (+110%) more than doubled, whileh its small business (+54%) also experienced a significant increase in number of victims.

The victim count for Italy has remained constant with minor movements in business sizes. Even then Italy is only second after Germany in terms of victim count in Europe.

The number of victims recorded for large businesses (+59%) associated with France also experienced a significant increase, while small businesses (-8%) experience a proportional decrease.

The United Kingdom (UK) is one of the few countries that experienced a decline in observed victims, with large business (-57%) pushing the overall numbers down, even though small business' (+34%) experienced noteworthy increase.

The Nordics region is experiencing a growth in the number of victims, especially in small business size category, for example, Sweden's small businesses (+188%) experienced what seems like a significant increase, but this is from a relatively small base growing from 8 to 23 victims. Denmark overall is experiencing a decline in victim counts, most prominently in the small (-86%) and medium (-58%) sized business categories. Norway is relatively flat compared to the previous year.

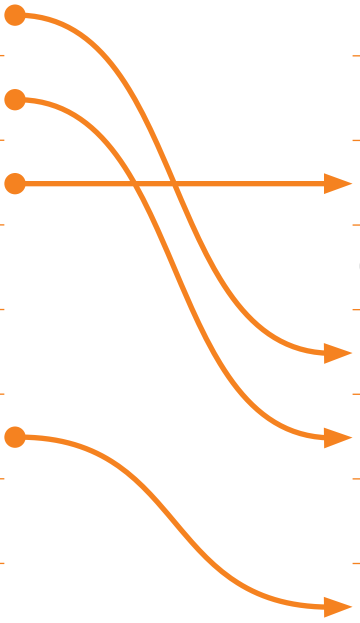
Africa experiences an increase in victim numbers with small businesses (+83%) leading the charge, followed by modest increase in medium sized businesses (+21%).

Does the GDP Affect the Victimology?

The graphic below illustrates the number of victims per country relative to each country's 2024 Gross Domestic Product (GDP) in US$ billion. While the U.S. records the highest number of victims in total, it is only the 25th most impacted relative to its GDP. Great Britain ranks 29th on this basis, and Canada at 16th. On the other end of the scale, for countries with at least 10 victims, Lebanon is the 6th most impacted relative to its GDP. Relatively small countries like Jamaica, the Cayman Islands and Thailand emerge as heavily impacted relative to their GDP. Among the larger, developed countries, Canada emerges as the most impacted relative to GDP (16th), above the USA and Great Britain. In Europe, Italy and Belgium emerge as more impacted than their contemporaries, relative to their economic size.

A full breakdown of victims per GDP is shown at the bottom of the page for the 50 countries most impacted on this scale.

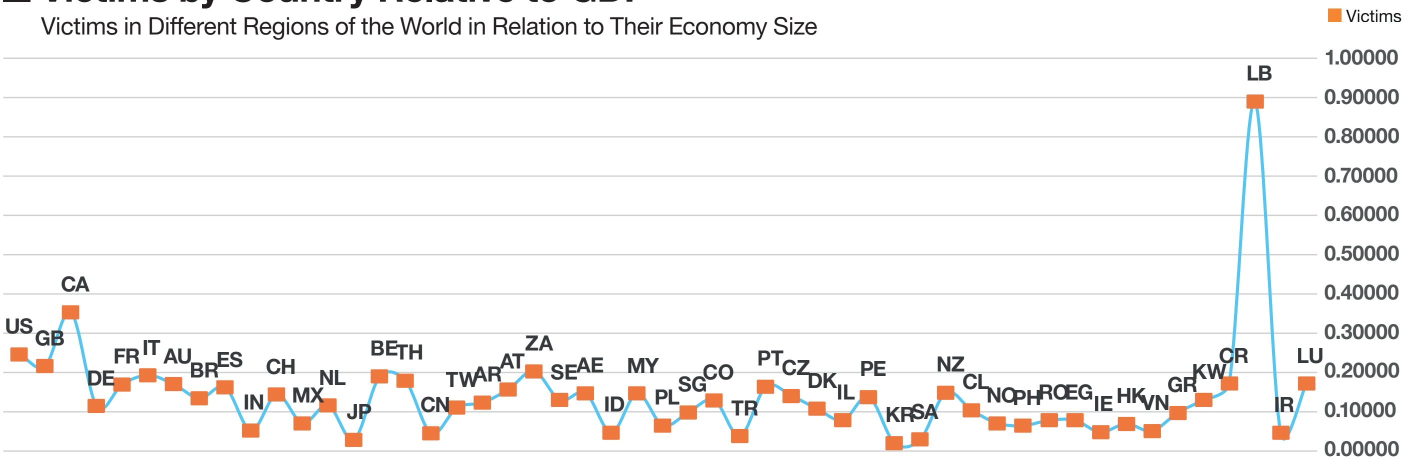
Country	Total Victims	Victims Ranking
USA	7321	1
Great Britain	803	2
Canada	798	3
Germany	561	4
France	550	5
Italy	467	6
Australia	308	7
Brazil	294	8
Spain	285	9
India	234	10



Country	GDP	Total vs. GDP
Lebanon	20,08	0,90
Jamaica	21,41	0,51
Canada	2230	0,36
Cyprus	38,74	0,28
USA	29184	0,25
Great Britain	3644	0,22
South Africa	410,34	0,21
Italy	2373	0,20
Belgium	684,86	0,19
Thailand	546,22	0,18

Victims by Country Relative to GDP

Victims in Different Regions of the World in Relation to Their Economy Size



Cy-X Perspectives for Regions

The number of Cy-X victims in the European region grew 19.5% compared to the previous period. In terms of business size, the victim counts for large, medium, and small business increased 24.7%, 32.1% and 7.2% respectively. The victim counts for organizations that could not be classified in terms of business size increased by 23.6%.

The number of victims per business size can be adjusted by allocating the victims from the “unknown” business size category to each business size based on their share of total victims excluding the unknown victim count. With this method the new increase of victims for each business size in Europe is now 25.5%, 32.9%, and 7.9% for victims classified as large, medium, or small businesses respectively.

The victim count per business size as a share of the region’s total victim count is mostly concentrated in small businesses (40.7%) and large and medium business splits the difference nearly equally.

Qilin and Akira are the most prevalent Cy-X actors when evaluated on number of victims and increased 324.0% and 168.0% respectively since the previous period. Other noteworthy Cy-X groups include incransom, Safepay, Sarcoma Group, Ransomhub, and Fog. The demise of LockBit3 and Blackcat (ALPHV) gave way to a more fragmented cyber extortion landscape breathing new life into this unrelenting threat.

Germany

Germany ranks first in Europe in terms of victim count and is the country with the biggest growth in terms of Cy-X victims at 57.7%. All victim counts across all business sizes increased in relation to previously recorded numbers. Victims classified as large grew by 110.0%, and 116.4% when adjusted. Small businesses have the largest share of victim counts, 44.5%, and the adjusted victim count is even greater at 58.1%. The adjusted victim counts for victims classified as medium sized businesses increased by 20.6%.

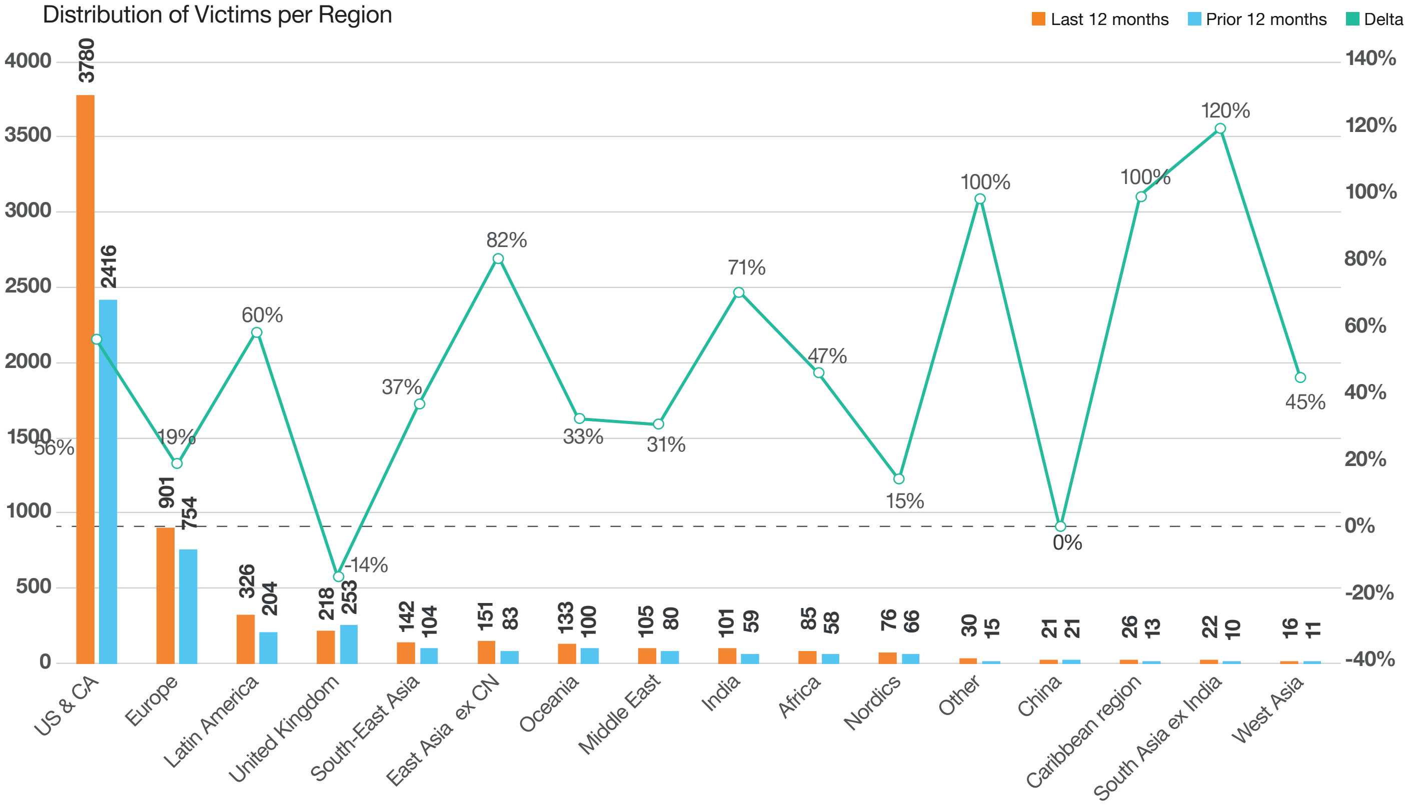
The most active Cy-X groups in terms of observed victim count in Germany are Safepay, incransom, Akira, Qilin, and Sarcoma Group with 126 victims between them. Fog, Incransom, Qilin, and Akira grew the most when comparing observed victim count, but the growth came of low single digit numbers to low 10s and 20s, which exaggerate the respective percentage numbers.

Italy

Italy ranks second in total number of victims (141) in Europe. Italy’s victim count for the period decreased, albeit only by 0.7%. Small businesses received some relief as the observed number of victims in that sector decreased by 12.7% (adjusted). Victims classified as small business represents 50.0% of victims associated with Italy. The remaining victims classified as large and medium represent 24.2% and 25.8% of the adjusted volume. As far as Cy-X groups go, Sarcoma Group, Akira, and Qilin account for 38.0% of the observed victim count for the period.

Regional Shift in Cy-X Victim Count

Distribution of Victims per Region



Belgium

Belgium experienced a decline of 10.9% in the number of observed Cy-X victims. Belgium's total victim count of 87 is relatively smaller than that of Germany (230) or UK (218) but is closer to that of France (129). The Cy-X groups Fog, Ransomhub, Qilin, and Sarcoma Group were observed with the largest number of victims observed for Belgium.

Medium sized businesses in Belgium have the largest adjusted share of victims (39.5%), followed by small (34.2%) and large (26.3%) business. The number of victims classed as medium sized businesses increased the most in terms of adjusted growth (24.7%). The number of victims classified as large business declined by 39.0%, while the number of victims classified as small business declined by 8.5%.

France

The observed Cy-X victim counts in France grew by 10.3%, ranking France third in Europe in terms of total victim count for the period. Large businesses seem to have taken most of the hit as the adjusted number of victims classified as large businesses increased 53.6%. The opposite was observed for victims classified as small with an adjusted victim count that declined 10.8%. The adjusted number of victims for medium sized businesses remained at the same level as before. The overall adjusted share of victims per business size is 38.4%, 28.6%, and 33.0% for large, medium, and small respectively. The most prolific Cy-X groups in France are Qilin (19.4%) and Ransomhub (7.8%). Qilin grew by 525%, claiming 25 victims.

United Kingdom (UK)

The UK is another country that experienced a decline of 13.8% in the number of Cy-X victims. The top five active Cy-X actors, listed in descending order based on victim count, are Qilin, incransom, Ransomhub, Medusa, and Akira. Qilin's victim count increased threefold compared with the prior 12 months. The takedown of LockBit 3.0 seems to have played a big role in reducing the victim count.

By business size, UK victims classified as large, or medium experienced the biggest benefit in the decline of observed Cy-X victims. The adjusted number of victims for large and medium victims dropped by 57.2% and 9.2%, respectively. The largest concentration of victims is now in small businesses with 49.4% of the adjusted share, compared to 17.0 % for large and 33.5% for medium sized businesses.

The Nordics region

The Nordics region experienced a 15.2% increase in the number of victims. The adjusted share of victims associated by business size resembles that of Italy with 49.3% attributed to victims classified as small. The increase in victim count for small businesses was almost 63.0%. The medium sized business category saw 23.9% fewer victims while the large business category increased by 10.2% in terms of adjusted victim count.

Africa

Africa once again experienced an increase in victim count and grew by 46.6%. The small business size category experienced an increase of 107.3% in the number of victims (adjusted). The large and medium business categories increased by 25.2% and 37.3% respectively. The number of victims in the large business category accounts for 44.3% of the victims, while medium's share of the adjusted count is 24.3%. This leaves 31.4% in the small business size category. Kill Security is the only group that managed double digits for observed victim count, followed by Ransomhub, FunkSec, and Qilin in high-to-mid single digit victims count. The balance of victims is shared between 41 other Cy-X groups.

> **The number of Cy-X victims in the European region grew 19.5% compared to the previous period.**
>
> **The victim count per business size as a share of the region's total victim count is mostly concentrated in small businesses (40.7%), and large and medium business splits the difference nearly equally.**
>
> - **Zohra Hamila** - Security Researcher

World Watch Data: Advisories of the Year

- **Zohra Hamila** - Security Researcher

About the Data

- **Period:** October 2024 to September 2025
- **413 World Watch advisories** delivered
- **Themes:** threats, vulnerabilities, breaches, news
- **Category distribution:** Vulnerabilities 31%, Cybercrime 30%, Nation-State 20%, Geopolitics 6%, Technical 5%, Other 8%

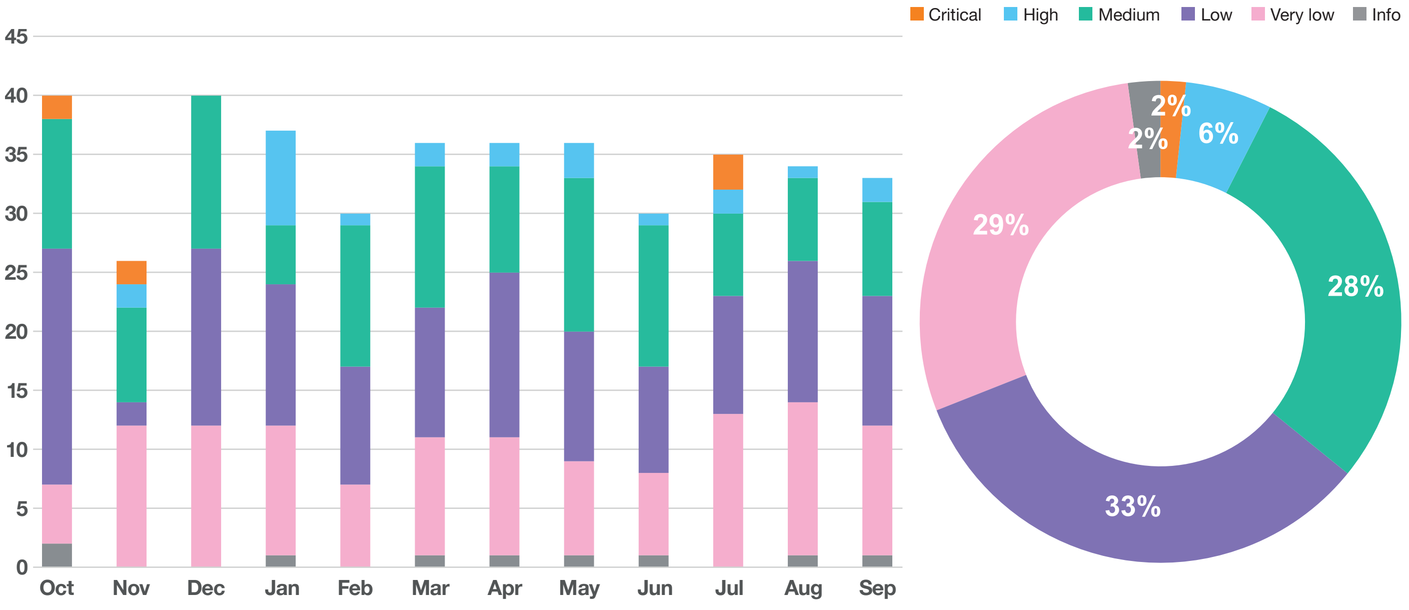
This chapter outlines some of the main developments that have shaped the cyber threat landscape over the past year. The main themes we chose to explore include:

- The persistence of cyber operations in the long-running conflict in Eastern Europe, marked by increased hacktivism and the shift in Ukraine's response.
- Notable Advanced Persistent Threat (APT) campaigns reflecting continued strategic espionage objectives.
- The extensive use of supply chain and deceptive techniques, through the NPM package infection chain, and ClickFix and Fake CAPTCHA campaigns.
- We will give light to some of the research done by the World Watch team over the past year.
- Last but not least, we will take a closer look at Scattered Spider, a highly active threat actor known for its agility, targeted operations, and use of social engineering techniques against third-party service providers and organizations.

> **Modern cybersecurity operations are a bit like meteorology - they involve ingesting and processing a huge amount of information from diverse sources. These various data points are used by security teams to make minute-by-minute decisions on how to spend time and resources efficiently. The right decision keeps the organization out of the rain and saves precious time, money, and reputation.**
>
> **Our World Watch service works on behalf of the customer to collect, analyze, prioritize, contextualize, and summarize the essential threat and vulnerability intelligence and provide actionable insights that any organization needs to make informed decisions and take appropriate actions.**
>
> - **Mael Sarp** - Threat Intelligence Team Leader

World Watch Advisories by Severity

Criticality of Advisories (New and Updated) Over Time



Long-Running Conflicts

Themes: Hacktivism, Nation-state, Geopolitics

Nation-state hacktivism | 5 advisories

Following last year's World Watch section titled Long-Running Conflicts, this year is marked by a series of events that shape the face of the geopolitical scene.

One of the main ongoing conflicts is the war against Ukraine. Since the start of the war in February 2022, hacktivism has surged, impacting organizations through Distributed Denial of Service (DDoS) attacks, defacements, and disinformation campaigns. In last year's Security Navigator, we reported on a notorious pro-Russian hacktivist group that alone claimed over 6,000 attacks between August 2022 and August 2024. As such groups thrive on public attention, we maintain our decision not to name the group. From early on, the group announced that any country liaising and working against Russia's interests would become a target of their DDoS attacks[162], in particular those that support Ukraine.

In October 2024, several government websites in Belgium were made inaccessible after the Belgian government pledged to provide military resources to Ukraine. Several media outlets were also targeted in anticipation of the country's municipal and provincial elections scheduled for October 13, 2024[163] . Japan was also hit by the group after the Russian Federation's Ministry of Foreign Affairs expressed concerns regarding Japan's increase in military resources and its involvement in military exercises sponsored by the United States[164].

More attacks followed, targeting both Ukraine directly and its allies including several NATO members[165]. The focus was disrupting critical sectors such as government, energy, finance, transport, and digital infrastructure. To counter this growing threat, Europol led "Operation Eastwood"[166] in July 2025, a major law enforcement action involving 19 European countries and the US. The operation resulted in the dismantling of the hacktivist group's core infrastructure, the takedown of servers, and several arrests. However, the group resurfaced just a week after and released a new ideological manifesto, calling for a "Time of Retribution". They proceeded to launch new waves of DDoS campaigns against organizations and states across Europe[167].

Ukraine hacks back | 6 advisories

Several pro-Ukraine hacktivist and state-sponsored groups reciprocated by launching their own cyber-attacks against Russia.

Reports show that Ukraine has significantly increased its capabilities since the start of the conflict-both kinetic, with the support of allies-but also on the digital and cyberwarfare domain. This is visible through a sharp increase in cyber-attacks led by Ukraine's military intelligence agency (HUR). In collaboration with volunteer civilian hackers, HUR has targeted several high-profile Russian entities in the private and public sector over the past months.

By means of those attacks, which Russia has partially acknowledged, Ukraine makes a point to bring this war into the Russian territory, moving the conflict from a purely kinetic plane to a digital and cognitive one.

In the cyber domain, attacks during the summer of 2025 included distributed denial of service against the Russian airline Aeroflot[168] and the compromise of the major drone manufacturer Gaskar Group[169] among others.

State-Aligned APT Espionage Campaigns

Geopolitics, Nation-state, Cybercrime

Salt Typhoon | 8 advisories

Following a series of breaches in 2024 targeting major U.S. internet and telecommunications providers, including Verizon, AT&T, and Lumen, the Chinese-state aligned Salt Typhoon group continued its global cyber espionage campaign during 2025. Not long before the 2025 U.S. presidential election, the group shifted its focus to prominent U.S. political figures, creating national political turmoil and raising concerns over election interference[170].

However, Salt Typhoon's activity is not confined to the United States. The group has impacted organizations across critical sectors globally, including government, telecommunications, universities and critical infrastructure[171]. The group is known to exploit exposed network edge devices, including Cisco routers and products from Ivanti and Palo Alto Networks[172].

These operations ultimately prompted the United States Department of the Treasury's Office of Foreign Assets Control (OFAC) to publish a press release in January 2025 announcing sanctions[173] against a Sichuan-based cybersecurity company allegedly linked to the group and its actions.

The FBI also announced a reward[174] in response to the group's escalating operations, seeking information leading to the identification or disruption of the group. The Five Eyes intelligence alliance alongside several European nations and Japan also issued a joint cybersecurity advisory[175] last September, signaling a coordinated international effort to counter People's Republic of China (PRC) sponsored threats, which includes Salt Typhoon. Despite the sanctions and increased scrutiny, Salt Typhoon remains active and continues to target telcos and internet providers worldwide.

● October

10/09-Initial: Microsoft Patch Tuesday: several 0-days, 2 exploited in the wild

10/10-Initial: Multiple financially motivated threat actors rely on ClickFix-like social engineering campaigns to distribute malware

10/29-Updated: Salt Typhoon spies on US presidential candidates following telco hack

● November

11/13-Initial: Chinese APT BrazenBamboo exploits an unpatched 0-day in FortiClient Windows VPN

● December

12/16-Update 2: Updated-New CVE assigned to Cleo MFT vulnerability, Cl0p claims responsibility for data-theft attacks

12/27-Update 6: Critical vulnerabilities in Palo Alto PAN-OS Web Management Interface, exploited in the wild

2025

● January

01/08-Initial: New 0-day in Ivanti's Connect/Policy Secure and Neurons for ZTA, limited exploitation / CVE-2025-0282, CVE-2025-0283

01/13-Initial: Threat actors exploit a probably 0-day in exposed management consoles of Fortinet FortiGate firewalls

Void Blizzard | 1 advisory

First identified in May 2025 but active since 2024, Void Blizzard (also known as Laundry Bear) is a Russian state-sponsored cyber espionage group targeting organizations of strategic interest to Russia[176], including in Ukraine and NATO member states. The group focuses on sectors including government, defense, transportation, healthcare, media, and NGOs[177].

In May 2025, the Dutch intelligence services blamed this group for several attacks from September 2024[178] targeting Dutch organizations and the Dutch National Police. This attack resulted in the theft of professional contact details that were potentially used to compromise other governmental organizations. The group reportedly gained access via session hijacking[179], likely using authentication cookies stolen through an infostealer and possibly obtained from criminal marketplaces.

Throughout 2025, Void Blizzard conducted opportunistic intrusions using password spraying, credential phishing, and stolen authentication tokens, usually leveraging living-off-the-land (LOTL) techniques. In a campaign conducted in April 2025, the group posed as organizers of the European Defense and Security Summit[180], sending emails containing PDFs with malicious QR codes linking to Evilginx-based phishing pages on typo-squatted domains.

The group also abuses cloud APIs such as Microsoft Graph and Exchange Online and then proceeds to automate the bulk collection of data, including email, files, and Teams conversations[181].

While some of its methods overlap with APT28 (aka Fancy Bear), Dutch authorities treat Void Blizzard as a distinct distinct actor[182].

Deceptive Techniques And Supply Chain Compromise

Themes: Hacktivism, Nation-state, Geopolitics

ClickFix and fake CAPTCHA | 4 advisories

ClickFix and fake CAPTCHA are social engineering techniques where users are presented with deceptive pop-ups in the form of fake error messages, or CAPTCHA challenges. The user is then prompted to copy and paste a command into PowerShell or via the command line interface. In the FileFix variant, the command would be executed using the Windows File Explorer address bar or via a browser file dialog. The technique is aimed at getting the user to download and run a malicious executable, ultimately giving remote access to the attackers.

Since 2024, large widespread campaigns using these lures have been used to deliver a wide range of payloads. Examples of these payloads include Lumma, SectopRAT, DarkGate, NetSupport RAT, Emmenhtal, XWorm, Vidar, VenomRAT, AsyncRAT, and DanaBot[183].

Our CERT and CyberSOC teams have been tracking several threat actors and clusters behind these operations, such as ClearFake, Storm-1865, and state-backed Advanced Persistent Threats (APT) including Kimsuky, MuddyWater/Static Kitten, and APT28. The initial step in the infection chain is to drive the users to lure pages using diverse methods: malvertising, forum and social media spamming, search engine optimization (SEO) poisoning, compromised legitimate sites, or phishing/spear-phishing emails containing malicious HTML attachments.

NPM compromise campaigns | 4 advisories

Among the most visible software supply chain incidents of 2025 are infected packages delivered via the NPM (Node Package Manager) repository, used to gain initial access and which unfolded through multiple coordinated campaigns.

In July 2025, malicious code was injected into five widely used JavaScript libraries hosted on NPM[184], the largest distribution platform for Node.js packages. The breach originated from a phishing attack that compromised a maintainer's computer, enabling the attacker to push a new version of the packages containing "Scavenger Loader" malware[185].

In August, two malicious packages delivering SilentSync[186] were discovered on the Python Package Index (PyPi). This Python-based remote access trojan (RAT) targeted Windows systems and enabled attackers to execute remote code, steal browser data (credentials, cookies, history), capture screenshots, and communicate with command-and-control (C2) servers over HTTP.

In September, another large-scale attack struck the JavaScript ecosystem[187]. After a sophisticated phishing email tricked a prominent developer into resetting a two-factor authentication, the attacker compromised 18 of its popular packages, collectively downloaded over two billion times weekly. The injected code specifically targeted cryptocurrency and Web3 transactions, silently intercepting blockchain activity (Ethereum, Bitcoin, Solana, Tron) in browsers. It tampered with wallets; rewriting payment addresses to redirect funds to attacker-controlled addresses[188].

February

02/21-Initial: Horizon3 details four critical vulnerabilities in Ivanti Endpoint Manager

02/24-Update 28: North Korean APT Lazarus carries out largest cryptocurrency heist in history with $1.46 billion stolen

March

03/17-Initial: Supply chain attack targets popular GitHub Action "tj-actions" used in 23,000 repositories

03/21-Update 1: Widespread adoption of ClickFix and fake CAPTCHA lures to distribute commodity malware

April

04/07-Update 2: ClickFix technique remains active, new variant FileFix observed in the wild

04/28-Initial: ReliaQuest reveals critical 0-day in SAP NetWeaver systems exploited in the wild / CVE-2025-31324

May

05/13-Update 1: Multiple threat actors exploit SAP NetWeaver, vendor fixes additional vulnerability CVE-2025-42999) / CVE_2025-31324

A week later, researchers observed a new and highly sophisticated worm named Shai-Hulud, affecting both NPM packages and GitHub accounts. The infection chain began with the compromise of a developer[189], allowing attackers to tamper with 38 packages. Though the infected versions were available for a few hours only, the worm's self-propagating nature dramatically amplified the attack potential.

Upon execution, Shai-Hulud scanned the compromised environment for secrets using legitimate tools such as TruffleHog, queried cloud metadata endpoints in public clouds for credentials and API keys, and exfiltrated that data using GitHub Actions. In parallel, the worm traversed accessible GitHub repositories, turning private repositories public and injecting the malicious workflow into all of them[190].

By mid-September, nearly 500 NPM packages[191] were impacted by this campaign, highlighting the scale and severity of recent supply-chain attacks and the increasing risks facing third-party and open-source ecosystems.

A Brief Look Into This Year's Research Themes

The World Watch team, part of the Orange Cyberdefense CERT, regularly conducts in-depth investigations to provide insights into today's threats. By breaking down complex threat elements and turning the research findings into actionable intelligence, the World Watch team plays a key role in the global CTI community.

To Read More About Our Publications:

CERT Blog:
https://www.orangecyberdefense.com/global/blog/cert-news

CERT Threat Research:
https://research.cert.orangecyberdefense.com/

Github:
https://github.com/cert-orangecyberdefense

Sorillus

- **Authors: Marine Pichon, Alexis Bonnefoi**
- **Supported by our IR, reverse engineering and MTD teams**
- **170 IOCs shared**

Sorillus RAT, also known as SambaSpy and Ratty RAT[192], first appeared in 2019. It was leveraged in malicious campaigns targeting European organizations based in Spain, Portugal, Italy, France, Belgium and the Netherlands. Likely emanating from Brazilian Portuguese-speaking threat actors, this infection chain cluster relies on invoice-themed phishing for initial access using multi-language-based lures.

Read more: https://www.orangecyberdefense.com/global/blog/cert-news/from-sambaspy-to-sorillus-dancing-through-a-multi-language-phishing-campaign-in-europe

MintsLoader

- **Author: Simon Vernin**
- **96 IOCs shared**

MintsLoader is a JavaScript/PowerShell loader that was first detailed by OCD in 2024. This malware was observed in distribution campaigns from July to October 2024. It primarily delivers malicious RAT or infostealer payloads such as AsyncRAT and Vidar through phishing emails, targeting organizations in Europe (Spain, Italy, Poland, etc.). A new version of the malware has been detected in June 2025 in campaigns using fake invoices lures.

Read more: https://github.com/cert-orangecyberdefense/cti/blob/main/mintsloader/2025-07-04-IoCs.md

Metappenzeller

- **Author: World Watch, CSIRT, CyberSOC teams**
- **9 IOCs shared**

Since early September 2025, the Orange Cyberdefense teams have detected ongoing campaigns impersonating Meta, Appsheet and Paypal. The campaigns are initiated from legitimate email addresses, containing lures targeting corporate sales, marketing, and legal teams. Active since December 2024, our teams track these campaigns under the name Metappenzeller.

Read more: https://github.com/cert-orangecyberdefense/cti/blob/main/Metappenzeller/20250922-InitialReport.md

June

06/30-Update 1: ReliaQuest identified in the wild malicious activity affecting NetScaler, possibly through CitrixBleed2 vulnerability

July

07/04-Update 2: ClickFix technique remains active, new variant FileFix observed in the wild

07/21-Initial: Critical 0-day vulnerability chain, affecting SharePoint actively and massively exploited / CVE-2025-53770 and CVE-2025-53771

August

08/04-Update 4: NoName057(16) resurfaces after Operation Eastwood, claims new attacks

08/27-Initial: 0-day CVE-2025-7775 in Citrix NetScaler exploited in the wild, two additional flaws patched

September

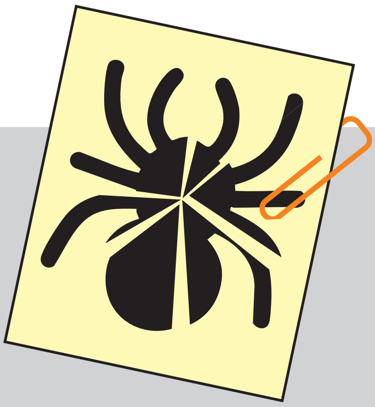
09/17-Initial: Crowdstrike and 186 other JavaScript libraries impacted by massive "worming" NPM supply chain attack

09/30-Initial: Chinese threat actor UNC5174 exploited a 0-day since October 2024 in VMware Tools & Aria / CVE-2025-41244

Scattered Spider snapshot- Profile, Methods & 2025 Attacks

Scattered Spider was formed around May 2022 and stands out today as one of the most active threat actors, responsible for several major attacks on global companies. Initially operating in the credential theft and SIM-swapping resale domains, the group has shifted its focus towards ransomware operations. Their attacks usually begin with social engineering and phishing techniques, often impersonating employees or IT support staff to gain initial access. Characterized by a decentralized and loosely affiliated structure[201], the group demonstrates high levels of operational agility and persistence.

Scattered Spider's evolution reflects several defining trends in today's threat landscape, including the opportunistic and decentralized nature of cybercrime, and the exploitation of humans, third-parties, open-source solutions and AI. These themes are further developed in our PEST chapter.



Threat Actor profile:

Scattered Spider

Aliases	UNC3944, Octo Tempest, Storm-0875, Muddled Libra, StarFraud, Oktapus, Scatter Swine
Estimated Inception	Around May 2022
Organizational structure	Loose affiliation among members, no rigid hierarchy, fluid membership
Member profile	Young, English-speaking (U.S./U.K.), sometimes teenagers[193]
Primary vectors	Social engineering, spear / phishing, vishing, help desk impersonation, employee impersonation, SMS, push bombing, Multi-Factor Authentication fatigue and takeover
Persistence / lateral movement	Use of legitimate Remote Monitoring and Management tools, hacking Endpoint Detection and Response, fallback backdoors, disabling security, using multiple access tools
Evasion & adaptation	Frequent TTP changes, dynamic response to defense efforts, joining / infiltrating incident calls to adapt (through Microsoft Teams, Microsoft Exchange or Slack)[194]
Malware / Tools	AveMaria, Raccoon, Vidar, custom Spectre RAT, use of legitimate tools TeamViewer, AnyDesk, Splashtop, FleetDeck, Level.io, Tailscale, etc.
Financial schema	Initially credentials theft and SIM swapping, resale then ransomware with double extortion (data theft + encryption)
Target sectors	Telecom, MSSPs, third party solutions and service providers, critical infrastructure, airlines, commercial sector
Affiliations	Connection with RaaS groups (ALPHV/BlackCat, RansomHub, DragonForce), potential member of The Com network
Law enforcement actions	Arrests of some prominent members (American and British citizens), seizures of crypto assets, prosecutorial actions, joint international authorities public advisories[195]
Notable attacks	▪ **MGM Resorts International (US):** hospitality and casinos in 2022. ▪ **Caesars Entertainment (US):** hospitality and casinos in 2022. ▪ **Transport for London (UK):** transport, August 2024[196]. ▪ **US Federal Court System (US):** government, 2024-2025[197]. ▪ **Hawaiian Airlines (US)-alleged:** airline, June 2025[198]. ▪ **Allianz Life (US):** insurance, July 2025[199]. ▪ **Salesforce (US):** cloud-based CRM platform, June 2025[200].

Industry Comparisons

▪ **Wicus Ross** - Senior Security Researcher

Cy-X Industry Analysis

The distribution of industries impacted by Cyber Extortion (Cy-X) (Cy-X) is heavily concentrated around a few dominant sectors. Manufacturing (1,228 victims) and Professional, Scientific, and Technical Services (1,179) together account for nearly 40% of all observed cases, indicating sustained impacts on production and knowledge-based industries. These are followed by Wholesale Trade (436), Construction (397), and Health Care and Social Assistance (383), which collectively reflect a secondary tier of high-risk sectors.

The concentration across these categories highlights a persistent impact on industries central to supply chains, infrastructure, and essential services. It may also reflect sector-specific vulnerabilities. For instance, Manufacturing and Wholesale Trade often operate with legacy systems and extensive third-party dependencies, while Construction remains a particularly exposed yet underexamined sector due to its fragmented project-based operations and reliance on subcontractors.

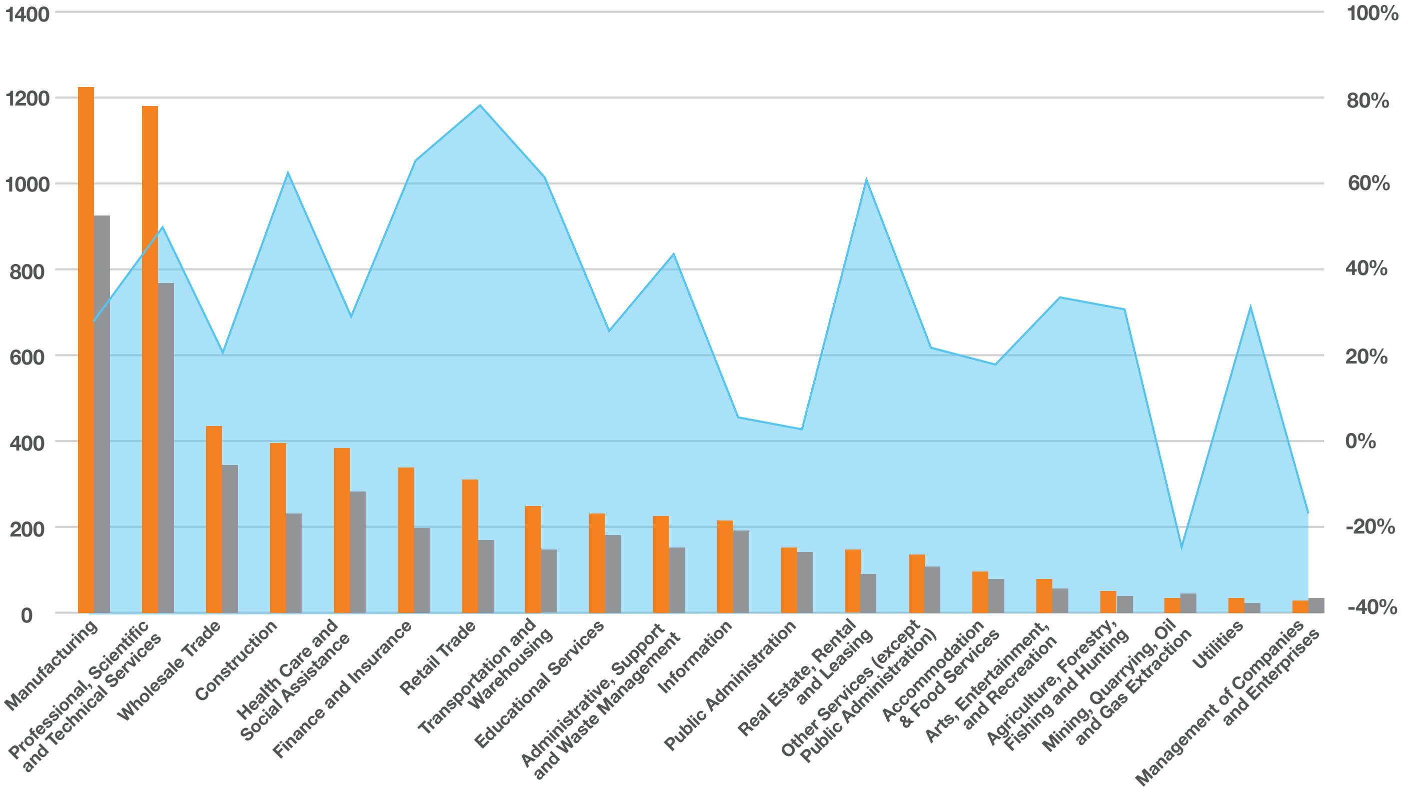
While we don't have sufficient data to comment on the Wholesale industry, we do note from our data that businesses in the manufacturing and construction industry rank 3rd-worst 5th-worst out of 14 sectors assessed in key vulnerability management metrics. Such structural characteristics may create more fertile ground for opportunistic intrusion, positioning these industries as persistent victims within an increasingly interconnected threat landscape.

> **The total number of Cy-X victims increased across nearly all industries, but with particularly sharp rises in some sectors. 2025 continued the growth trend already seen in the broader dataset, but again the distribution has shifted. This may indicate evolving actor priorities, but it is still too soon to be certain.**
>
> ▪ **Diana Selck-Paulsson** - Senior Security Researcher

We observe increases in affected and less-affected sectors. Manufacturing (+32%, 1,228 victims) and Professional, Scientific, and Technical Services (+54%, 1,179 victims) remain the most impacted industries. The largest relative increases occurred in Retail Trade (+84%), Finance and Insurance (71%), Health Care and Social Assistance (+69%), and Transportation and Warehousing (+67%).

Cy-X Victims Across Industries

Distribution and Shift Since 2024



We can consider this trend further by looking at the behaviors of individual brands. Note that a brief discussion of tactics, techniques, and procedures are present in the Cyber Extortion data analysis chapter under the heading “Threat Actors”.

Cl0p impacted Transportation and Warehousing and Retail Trade the most with 69 and 57 victims respectively. The incransom brand has little to no concern about its impact on victims in the Health Care and Social Assistance industry with 64 victims compared with Cl0p’s 1. Following this trend, Qilin accounts for 40 victims in Health Care and Social Assistance, 25 victims in Retail Trade, and 18 victims in Transport and Warehousing. Ransomhub, which is considered inactive since end April 2025, had managed to amass 32 victims in Health Care and Social Assistance since October 2024. During the same time Ransomhub also impacted 20 victims in Retail and Trade and 14 victims in Transportation and Warehousing.

The increase in Finance and Insurance occurred mostly in the USA and the Republic of Korea (KR). Most prominent actors in this sector are Silentransomgroup, Akira, Qilin, and Ransomhub. Specifically for Finance and Insurance, the Republic of Korea accumulated 29 victims after seeing no victims previously. Qilin claimed nearly all victims (27) in this industry in KR. What stood out was how similar the Qilin announcements were for these victims. It was as if they had a template that they followed by just swapping out the victim’s name and incremented a counter. These announcements spanned over a matter of 14 days from middle September 2025. This is very peculiar and might point to a common platform or a common service provider that was compromised. Supply chain compromises are common these days and it could explain the large batch of similar looking victims.

If cyber extortion actors are so prevalent and if this activity only represents the tip of the proverbial iceberg, then we should expect to see a large amount of activity in our clients’ environments that point to external actors. However, this is not the case as noted in our Threat Detection chapter that highlights an increase in confirmed incidents related to internal actors. The increased deployment of EDR/XDR tools brought a magnifying glass to activity on end user devices. All industries recorded a relatively higher number of false positives, some more than others. Higher coverage in terms of security solutions does not seem to correlate to more or fewer incidents. The function of the number of incidents is more related to the type of solutions.

Hidden among the confirmed incidents are activities related to external actors trying to gain access to some system. The share of incidents associated with “hacking”, “malware”, and “social engineering” threat actions should point to this. After all, Cy-X actors are using tactics and techniques that work. For example, high profile cyberattacks in the United Kingdom (UK) impacted major retailers and a large motor vehicle manufacturer[202][203]. Information on these attacks is sparse with no official explanation of how these attacks played out. From the scant details and speculation, we can assert that attackers gained initial access through manipulation of people and not necessarily hacking outright.

In our dataset we see few incidents classified as “social engineering”, with Administrative and Support and Waste Management and Remediation Services having the highest share. If there is little evidence of social engineering, does that imply that what is recorded are the residual effects of phishing which manifests as misuse impacting end user devices?

As noted in the World Watch chapter, attacks such as ClickFix manipulate the user into executing commands that open the door to attackers. These attacks are effective since it plays out in the blind spot of popular detection tools. However, the over zealousness of detection tools that report legitimate actions as malicious does increase the overall false positive count as experienced by the manufacturing, finance, and retail industries. The balance between what is malicious and what is normal is where social engineering pushes the boundaries of security architectures.

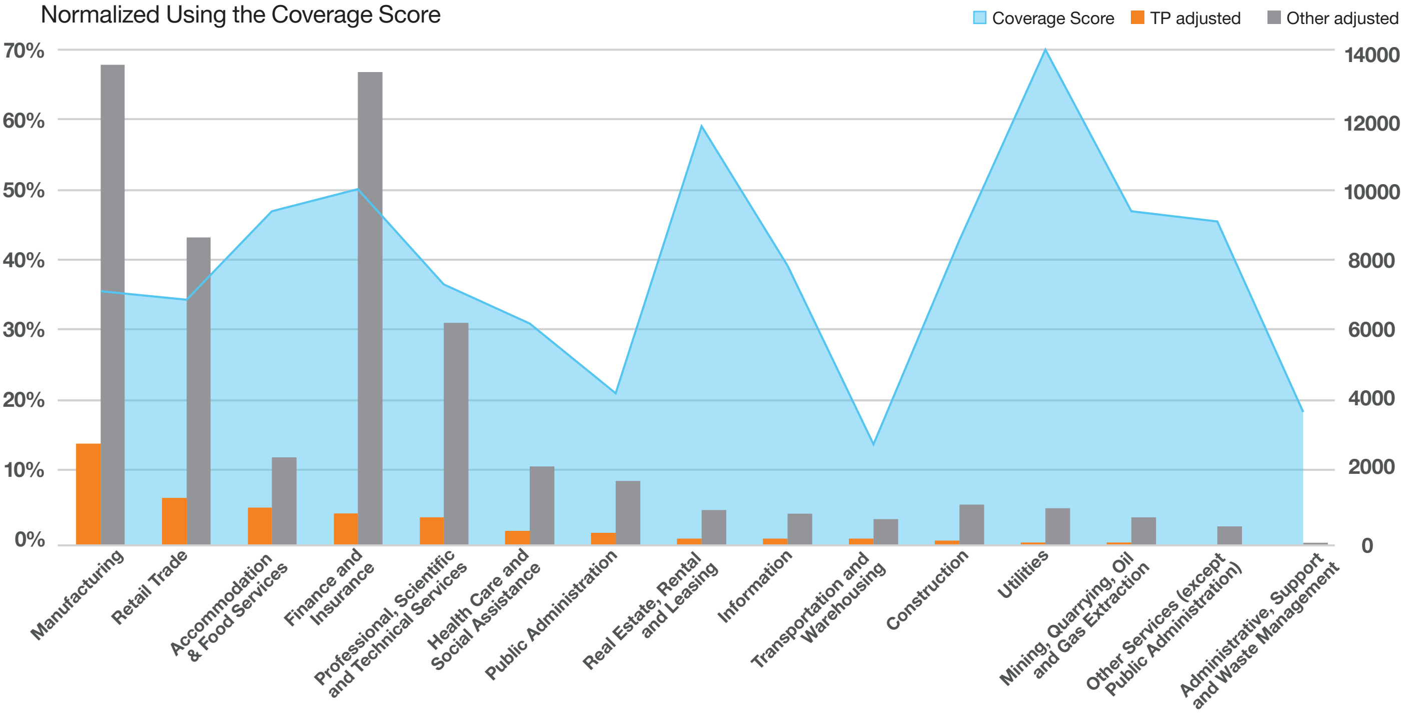
The number of findings in terms of vulnerabilities, whether it's a misconfiguration or is a missing patch, remains on average at the same level as in the previous period. Businesses across industries are remediating and responding to findings as fast as they can.

Some industries such as Public Administration do sit on several findings that are more serious on average than other industries. One would expect to see businesses with fewer assets to reduce their overall number of findings. Industries like Information and Accommodation and Food Services still manage average numbers of findings that are close to the overall average even with relatively fewer assets.

Age of findings tells us how fast teams are addressing these overall. Most findings are younger than a year, but there are some findings that accumulate and age beyond that. The Accommodation and Food Services, Health Care and Social assistance, and Public Administration industries overall accumulate findings that span multiple years on average. Retail Trade do have single instances where there are findings with extreme age, but this is localized to one client and is not symptomatic of all clients in Retail Trade.

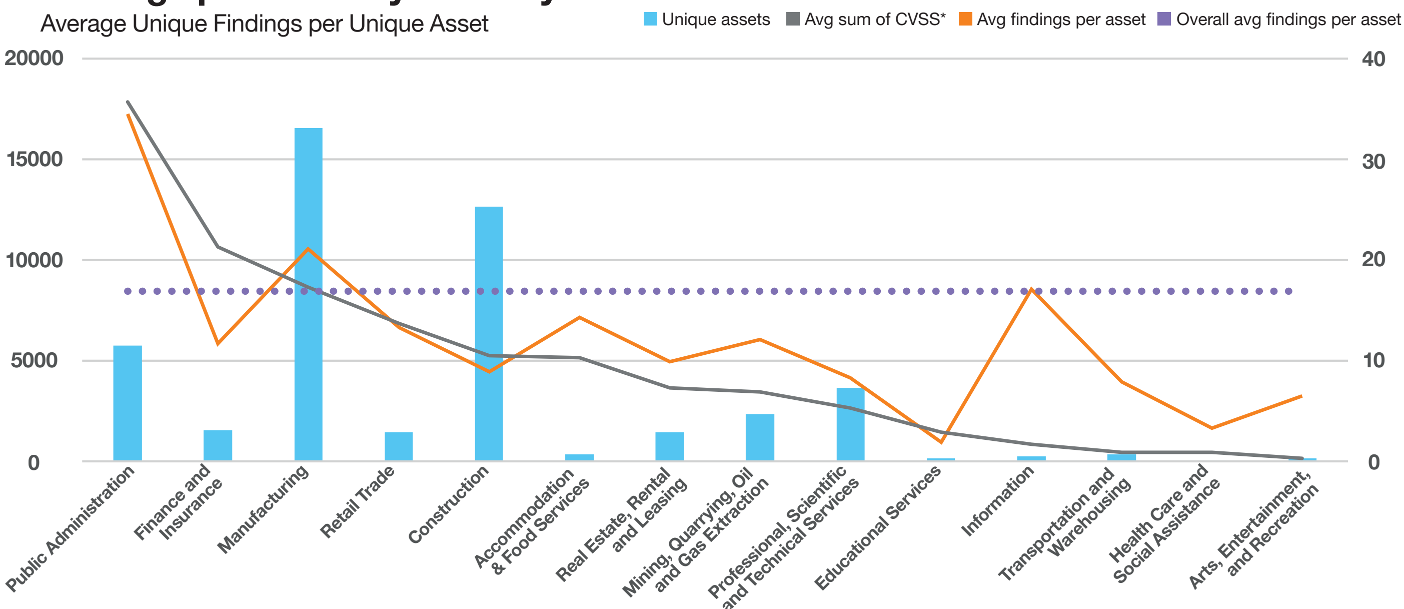
Detected Incidents by Industry

Normalized Using the Coverage Score



Findings per asset by industry

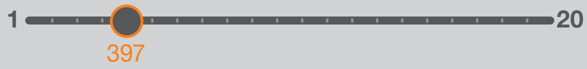
Average Unique Findings per Unique Asset



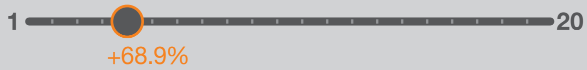
Industry Scorecard

Construction

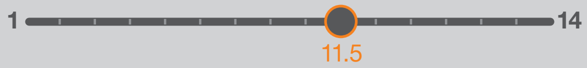
Cy-X Victim ranking (Avg: 292)



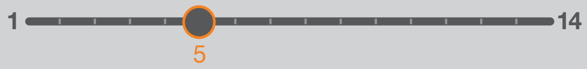
Cy-X Victim delta (Avg: +44.5%)



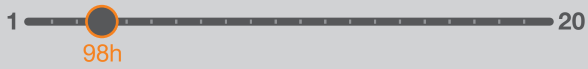
VOC: Findings per asset (Avg: 21.2 findings)



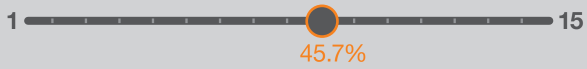
VOC: Total Vulnerability Score



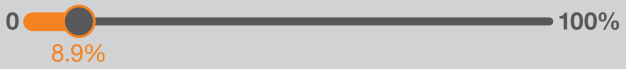
Threat Detection: Mean time to resolve (Avg: 40h)

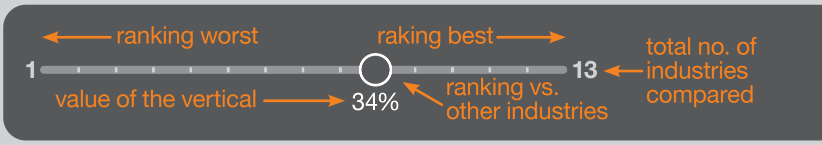


Threat Detection: Coverage (Avg: 42.1%)

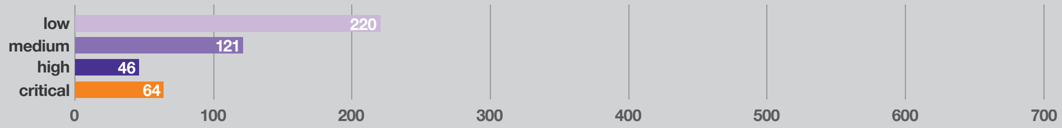


Threat Detection: True positives (Avg: 13.7%)

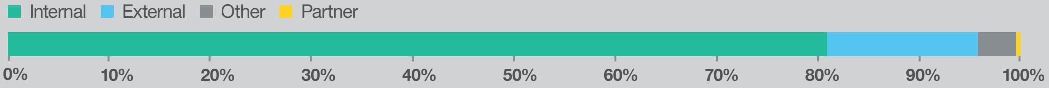



ranking worst
raking best
1
13
total no. of industries compared
value of the vertical
34%
ranking vs. other industries

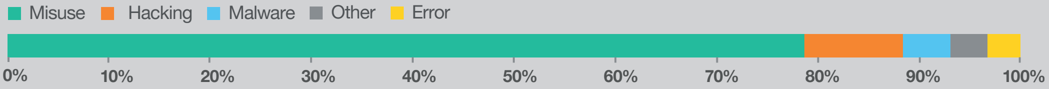
VOC: Finding age by severity (in days)



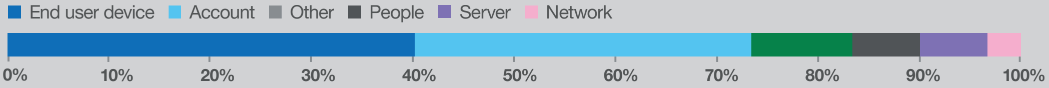
Threat Detection: Threat Actor



Threat Detection: Threat Action



Threat Detection: Impacted Asset



Summary

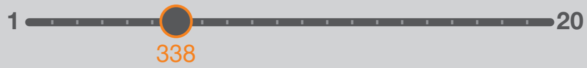
Construction is not one of the major industries - at least not in the USA - so we cannot explain the industry’s prominence in our victim data simply by its size. Cy-X victims from the construction industry grew 69% from last year, so the industry now ranks as the 4th most impacted.

Our clients in the construction industry appear to have improved some of their security posture, with the average vulnerability findings per asset dropping from 15.88 to 11.05 since last year. The average finding age of 104.69 days is one of the lowest, relative to the number of assets. Approximately 90% of findings are less than 12 months old, but nearly 60% of Construction-related findings are still classified as critical or high in severity. As with our clients in other industries, we believe a shift to EDR/XDR as a defense strategy is surfacing a significant number of detections that indicate internal user misbehavior, which does little to explain the increase in Cy-X victims. Nevertheless, 15% of all incidents we triage are classified as “external” and incidents classified as “hacking” account for 10% of the incidents we triage.

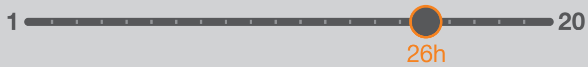
Industry Scorecard

Finance and Insurance

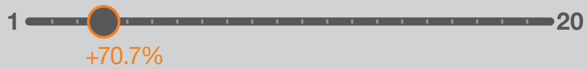
Cy-X Victim ranking (Avg: 292)



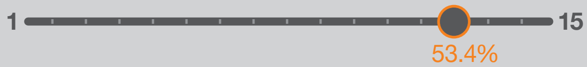
Threat Detection: Mean time to resolve (Avg: 40h)



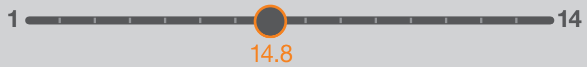
Cy-X Victim delta (Avg: +44.5%)



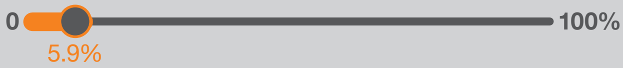
Threat Detection: Coverage (Avg: 42.1%)



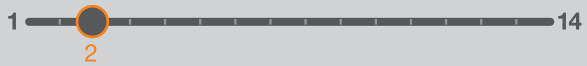
VOC: Findings per asset (Avg: 21.2 findings)

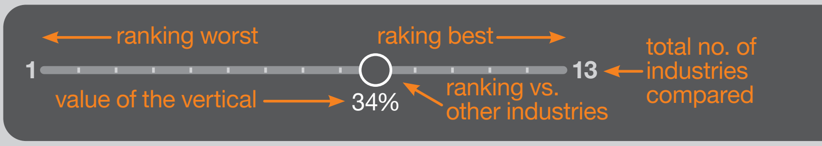


Threat Detection: True positives (Avg: 13.7%)

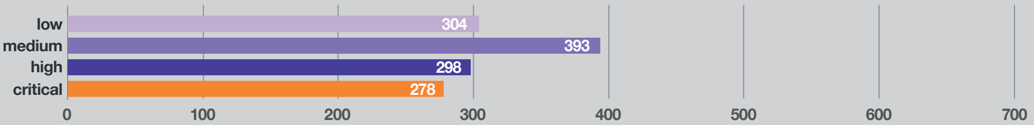


VOC: Total Vulnerability Score

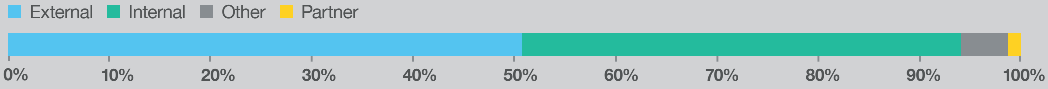



ranking worst
raking best
1
13
total no. of industries compared
value of the vertical
34%
ranking vs. other industries

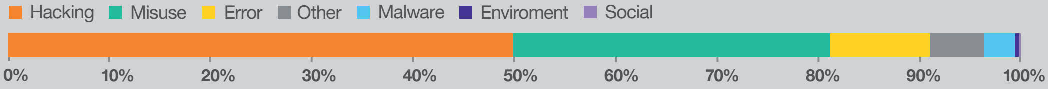
VOC: Finding age by severity (in days)



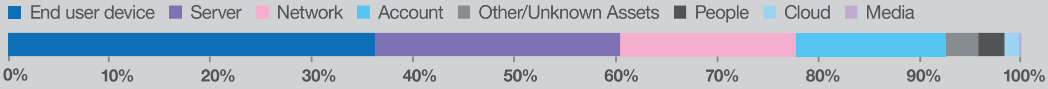
Threat Detection: Threat Actor



Threat Detection: Threat Action



Threat Detection: Impacted Asset



Summary

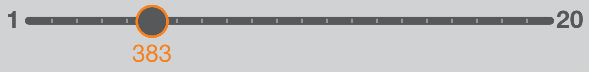
As one might expect, our clients in this industry tend to demonstrate higher levels of security maturity. The average MTTR of 26 hours is way below the overall average-indicative of fast feedback times leading to faster resolutions. Only 6% of incidents raised with us are confirmed as true positives-compared to Manufacturing and Retail Trade with 16% and 13% respectively. In line with other industries, “legitimate activity and applications” account for 89% of false positives.

Possibly reflecting a different set of security threats and priorities, the “hacking” action category is most prominent in this industry, accounting for 50% of incidents. Most of the “hacking” actions we triaged were linked to external actors. In terms of internal actors, misuse (28%) is the largest action and impacts end user devices (25%) most frequently. Our clients in Finance and Insurance demonstrate robust relatively effective vulnerability management practices also, with only about 15 vulnerability findings per unique asset. Nevertheless, the average age of vulnerabilities for our clients in this sector is still ~336 days. Approximately 82% of findings are less than a year old, but 46% of those findings are rated critical or high.

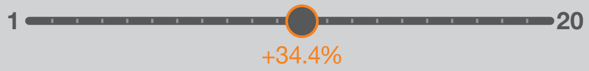
Industry Scorecard

Health Care and Social Assistance

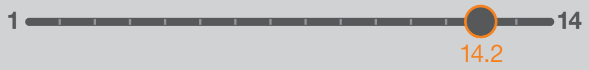
Cy-X Victim ranking (Avg: 292)



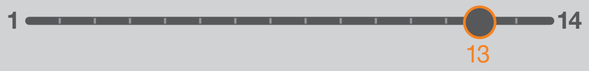
Cy-X Victim delta (Avg: +44.5%)



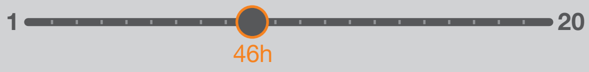
VOC: Findings per asset (Avg: 21.2 findings)



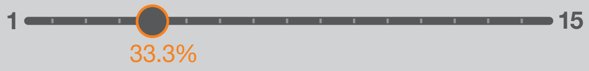
VOC: Total Vulnerability Score



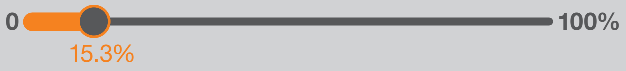
Threat Detection: Mean time to resolve (Avg: 40h)

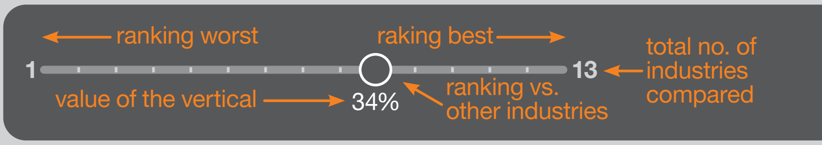


Threat Detection: Coverage (Avg: 42.1%)

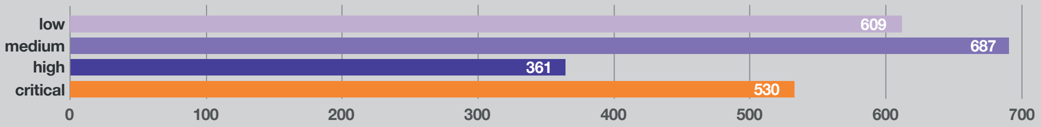


Threat Detection: True positives (Avg: 13.7%)

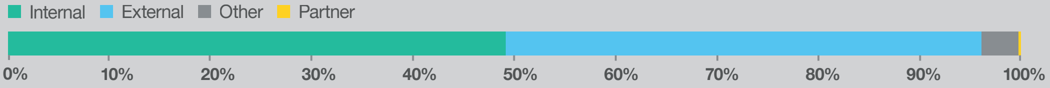



ranking worst
raking best
1
13
total no. of industries compared
value of the vertical
34%
ranking vs. other industries

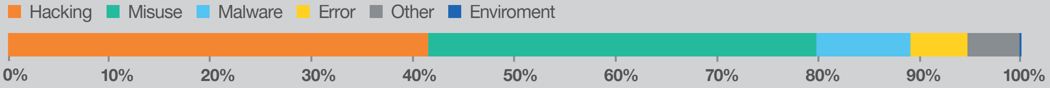
VOC: Finding age by severity (in days)



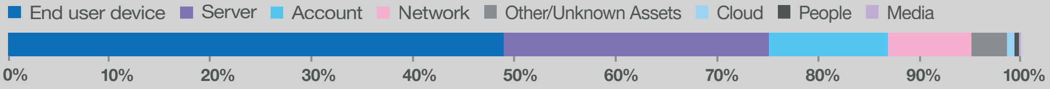
Threat Detection: Threat Actor



Threat Detection: Threat Action



Threat Detection: Impacted Asset



Summary

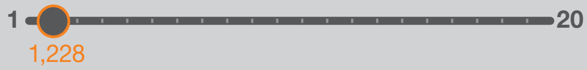
As we've previously reported, organizations in healthcare are now common victims of cyber extortion. Healthcare is also a large industry - the 4th biggest in the USA - yet it has previously been somewhat shielded from Cy-X by an apparent moral hesitation among threat actors. The incransom group has no apparent moral qualms with 64 victims this year, Qilin accounts for 40 victims and Ransomhub-inactive since end April 2025-still managed to amass 32. This sector is now the fifth most impacted.

For clients in this industry, we note that 40% of vulnerabilities we report are older than 1 year. Somewhat unusually, our detection teams classify the largest share of incidents (39%) triaged as "hacking". The hacking action is mostly associated with external threat actors that are impacting server assets. Still, incidents involving end user devices account for 49% of the total.

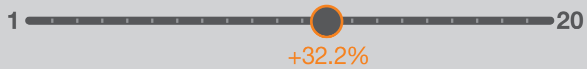
Industry Scorecard

Manufacturing

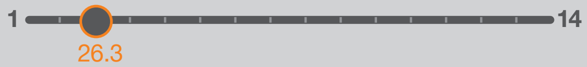
Cy-X Victim ranking (Avg: 292)



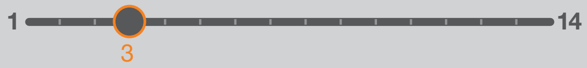
Cy-X Victim delta (Avg: +44.5%)



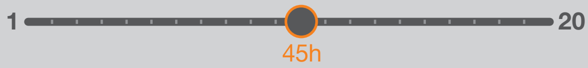
VOC: Findings per asset (Avg: 21.2 findings)



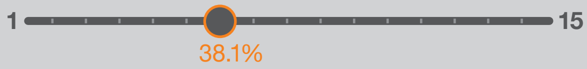
VOC: Total Vulnerability Score



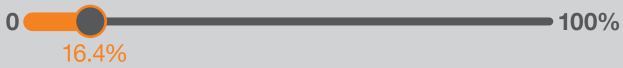
Threat Detection: Mean time to resolve (Avg: 40h)

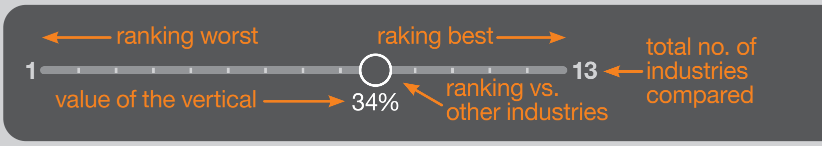


Threat Detection: Coverage (Avg: 42.1%)

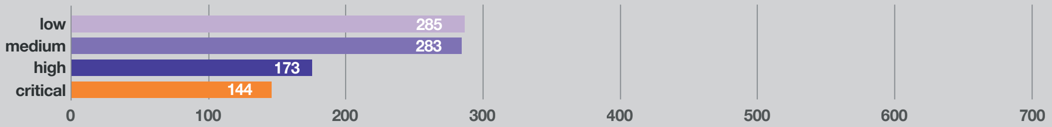


Threat Detection: True positives (Avg: 13.7%)

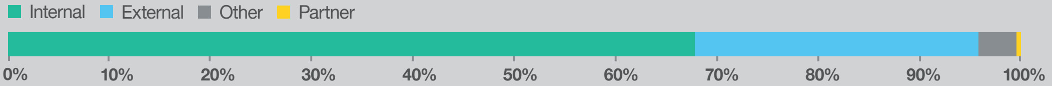



ranking worst
raking best
1
13
total no. of industries compared
value of the vertical
34%
ranking vs. other industries

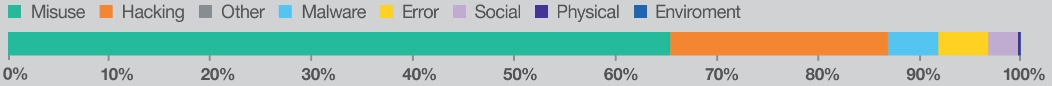
VOC: Finding age by severity (in days)



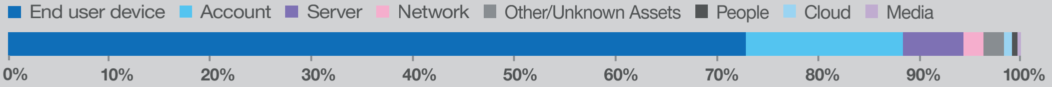
Threat Detection: Threat Actor



Threat Detection: Threat Action



Threat Detection: Impacted Asset



Summary

The Manufacturing industry accounts for approximately 11% of US GDP and is the third biggest industry in that country, so it's somewhat understandable that it should be heavily impacted. However, its size doesn't quite account for its prominence among Cy-X victims.

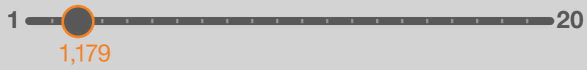
We do see indications in our threat detection data that businesses in this industry are heavily impacted - our clients in manufacturing record the highest number of confirmed incidents, even after adjusting the confirmed incidents using coverage.

As is generally the case, the incidents we detect and record within the industry are mostly internal actors (68%). Hacking alerts account for 22% of all detected incidents, and malware for only 5%. We believe this to be a function of detection technology behavior, rather than threat actor behavior.

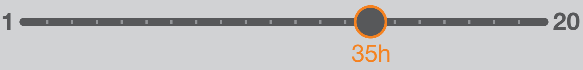
Industry Scorecard

Professional, Scientific and Technical Services

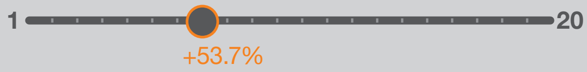
Cy-X Victim ranking (Avg: 292)



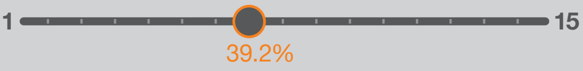
Threat Detection: Mean time to resolve (Avg: 40h)



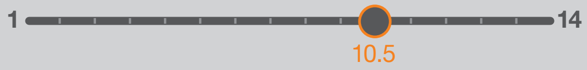
Cy-X Victim delta (Avg: +44.5%)



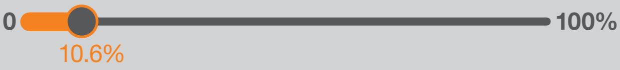
Threat Detection: Coverage (Avg: 42.1%)



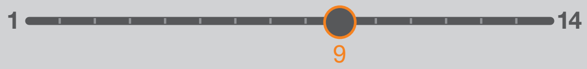
VOC: Findings per asset (Avg: 21.2 findings)

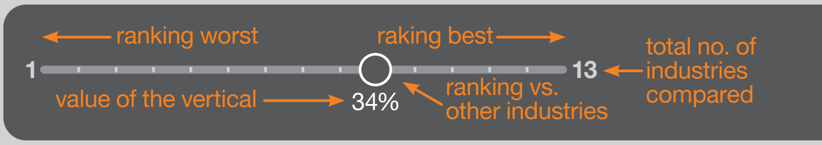


Threat Detection: True positives (Avg: 13.7%)

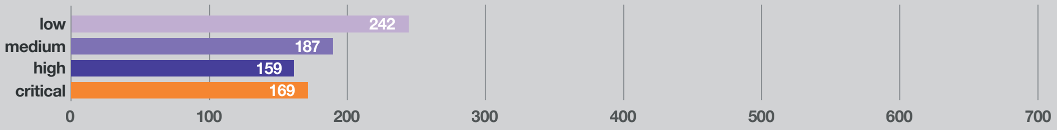


VOC: Total Vulnerability Score

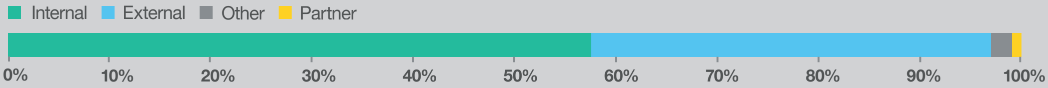



ranking worst
raking best
1
13
total no. of industries compared
value of the vertical
34%
ranking vs. other industries

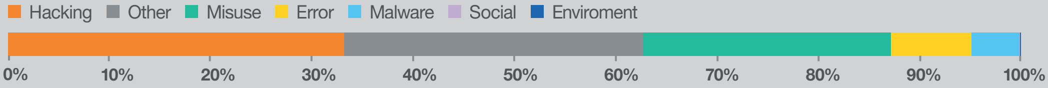
VOC: Finding age by severity (in days)



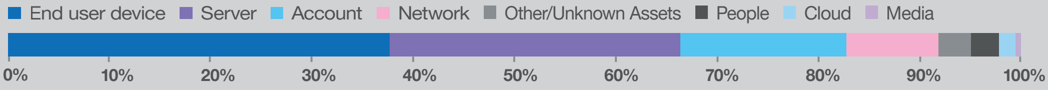
Threat Detection: Threat Actor



Threat Detection: Threat Action



Threat Detection: Impacted Asset



Summary

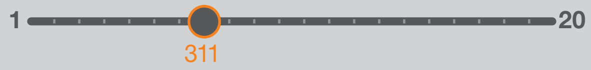
The number of Cy-X victims from this industry this year was 1,179-the second largest in our data. As Professional, Scientific, and Technical Services (PSTS) is considered the largest industry in the USA, this finding is somewhat predictable. But businesses in this sector do appear to face security challenges also. For example, our threat detection teams only consider 11% of incidents raised by detection technologies as confirmed true positives. Legitimate activity or applications account for 78.92% of false positives.

Our detection services for PSTS attribute 40% of incidents to external actors, down from the previous year's share of 53%. Incidents attributed to external actors and classified as "hacking "(31%) impact account (12%), server (9%), and network (7%) assets. Still, the MTTR for PSTS is just below the average at 35.4 hours Most vulnerability findings for clients in this section are aged 1 year or younger, with the bulk residing in findings rated medium (41%) and findings rated low (41%).

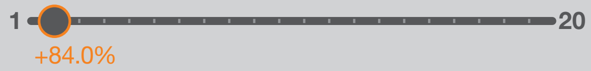
Industry Scorecard

Retail Trade

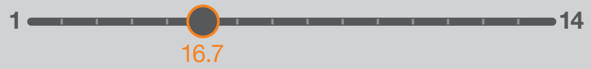
Cy-X Victim ranking (Avg: 292)



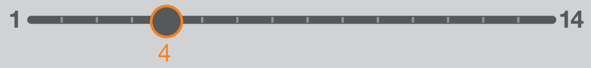
Cy-X Victim delta (Avg: +44.5%)



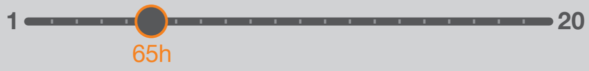
VOC: Findings per asset (Avg: 21.2 findings)



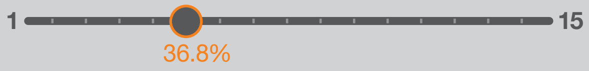
VOC: Total Vulnerability Score



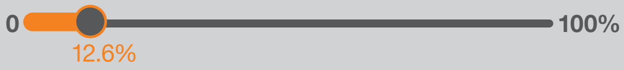
Threat Detection: Mean time to resolve (Avg: 40h)

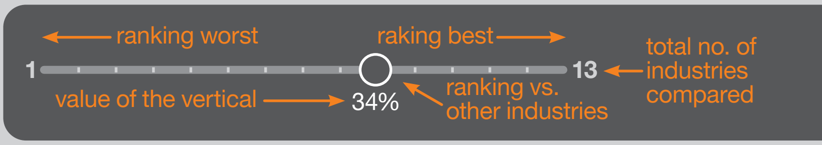


Threat Detection: Coverage (Avg: 42.1%)

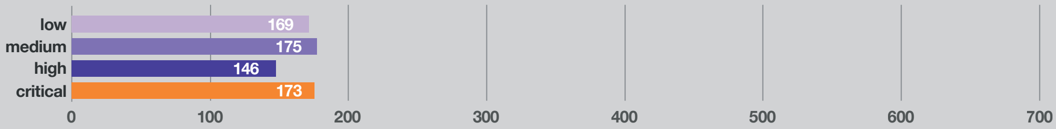


Threat Detection: True positives (Avg: 13.7%)

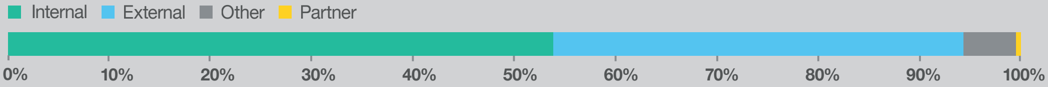



ranking worst
raking best
1
13
total no. of industries compared
value of the vertical
34%
ranking vs. other industries

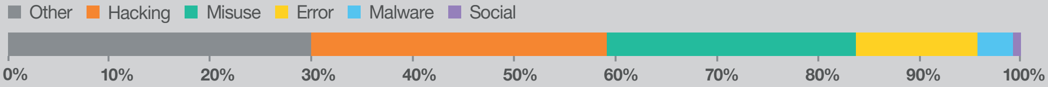
VOC: Finding age by severity (in days)



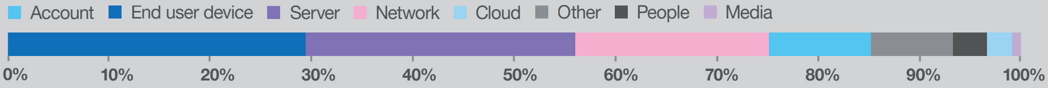
Threat Detection: Threat Actor



Threat Detection: Threat Action



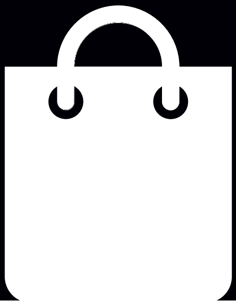
Threat Detection: Impacted Asset



Summary

Retail Trade is the 7th most impacted industry by Cy-X, with an increase of 84% in victims since last year- the largest increase of all industries. It's (coincidentally) considered to be the 7th largest industry in the USA. The actor Cl0p was responsible for 57 of those new victims, Qilin claimed 40, and Ransomhub took credit for another 20.

External threat actors are attributed in just over 40% of incidents, with one quarter of those classified as "hacking". For our clients in retail the average MTTR is 65 hours, well above average and among the highest overall. 13% of all incidents triaged are ultimately classified as confirmed true positives. Somewhat unusually, only 67% of false positives are categorized as legitimate activity or application, which is lower than most other industries. This speaks to how much each environment varies from the next.



Research Perspectives

Year of the Wood Dragon: Growth and Creativity With Intelligence and Honor

2025 ended the Chinese year of the Wood Dragon.

As every new year brings added threats and complexity, Orange Cyberdefense continues seek clarity for ourselves and our clients through extensive investment into cyber intelligence and research. Our research efforts are an effort to surface and propagate novel, authentic and meaningful perspectives on the pressing cybersecurity problems of the day. These perspectives can then drive better decision making by our leadership, product teams and operators. They also enable us to advise our clients better. Finally, we share our findings with security community generally as part of our broader effort to help build a safer digital society.

Our research efforts are informed by our diverse teams of experienced experts and by the datapoints generated from the products and services we deliver to clients. But good research doesn't begin with data. It begins by identifying the important questions. Successful research teams need the curiosity to identify and pursue fresh lines of investigation, the skills and data required to shed light on complex questions, and the structures and discipline to remain focused and consistent.
Our multi-disciplinary global research considers over a dozen themes and topics, from malware and threat actor analysis, through artificial intelligence and operational technology, to geopolitics and criminology.

Not all our research efforts produce meaningful results, but with perseverance and persistence a useful, considered perspective does begin to emerge. Viewed collectively, the diverse pieces of the puzzle we investigate begin to describe a cohesive view of the complex and dynamic environment we operate in.

In Chinese five elements philosophy, the Wood element signifies growth, vitality and creative potential, while in broader Chinese symbolism the Dragon stands for power, good fortune, intelligence and honor[204]. As we consider our research efforts over the past year, we note that wood characteristics like growth and creativity appear to be in tension with essential dragon attributes like intelligence and honor. We've needed to balance both preserve the safe digital society we're working for.

2025 was the Chinese year of the Wood Snake, associated with traits like wisdom, intelligence, intuition, and transformation. It was good year for sincere, strategic, and innovative research to anticipate and counter fundamental cyber risks and threats.

In the sections that follow, we offer a structured summary of some of the key themes that focused our research efforts and shaped our views regarding the dominant factors that are shaping the cybersecurity landscape.

PESTs in Cyberspace

Charl van der Walt - Head of Security Research

A Complex Landscape

The contemporary threat landscape is not a simple product of the whims or choices of criminal hackers and other threat actors. Instead, there is a diversity of actors - both benign and malicious - that have an influence. Those actors operate within a context that is in turn defined by the complex interactions between yet another set of systemic forces.

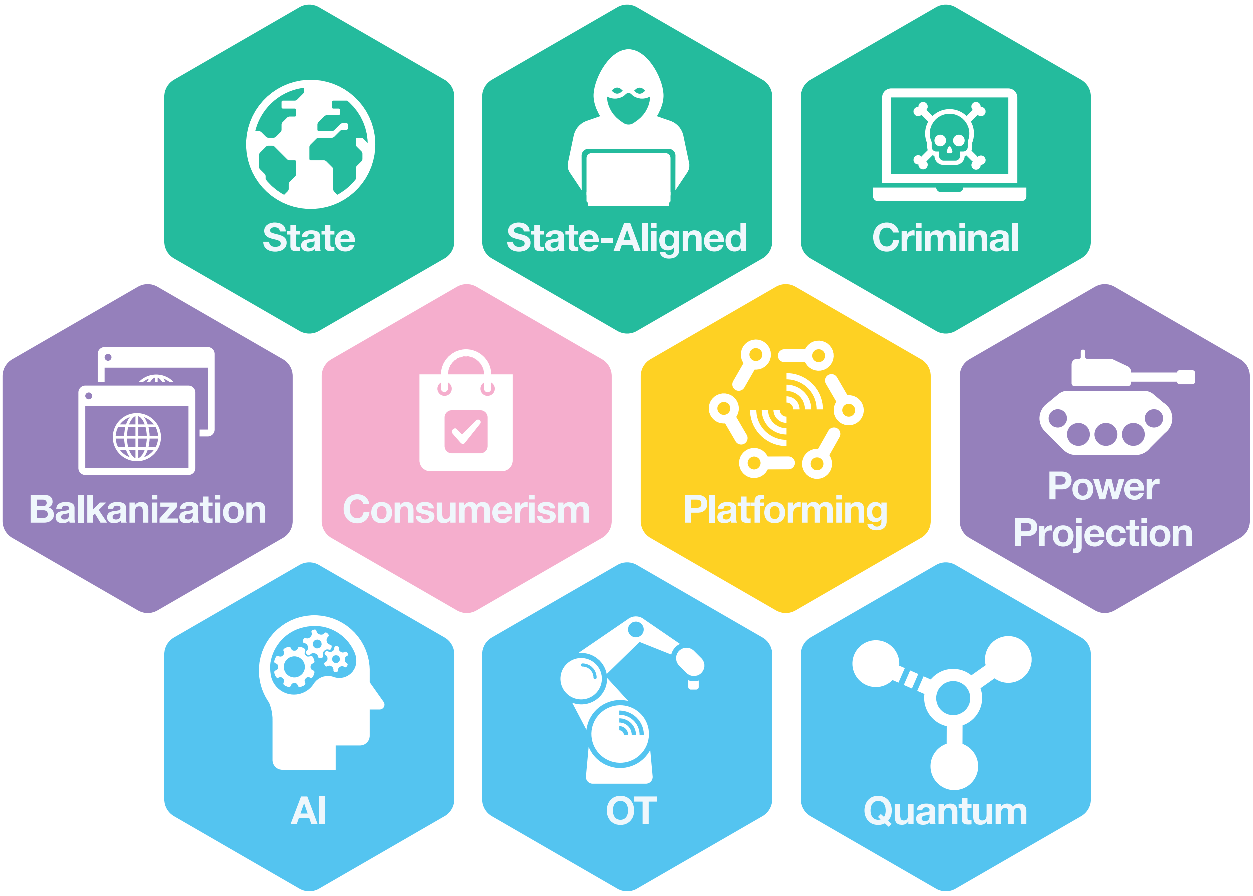
To understand the threat landscape, we must therefore consider all the systemic factors that shape it, as well as the actors that operate within it.

In our research efforts at Orange Cyberdefense, we apply a framework called PEST to help make sense of this complexity. The PEST framework is a strategic tool for assessing how Political, Economic, Social, and Technological external factors may influence operations and risks.

In this section we will summarize some of the work undertaken by our research and intelligence teams of the year past year. Each research area is summarized independently, but our work is approached and organized using the PEST framework to ensure that we are considering the full depth and breadth of the landscape.

Political, Economic, Sociocultural and Technological

From the myriad of factors that shape the landscape, in 2025 we have been most closely examining the following PEST factors.



Political Factors

The Political factors include regulatory changes, government policies, and institutional stability that affect an organization's external environment.

This year our research has focused on the following:

Power Projection via Technology

All technology is considered political, and is involved as a weapon, a target, or a lever in geopolitical conflict. As a political entity increases its reliance on technology platforms, it increases its exposure to technical power projection, enabling cyber and psychological operations, misinformation campaigns, and other forms of soft power projection.

This year our focus has centerd on the evolving relationship between Europe and its traditional ally the USA, with recent "America First" narratives reshaping global alliances and sparking anxiety in Europe as in the rest of the world.

Technological Autonomy & Alliances

The relative safety, peace and prosperity that much of the world has enjoyed since 1945 was not accidental. It emerged from the ashes of two world wars and the deliberate construction of a new global order. The United States of America set the terms of this new world.

The long peace under Pax Americana provided a stable foundation, but this year we note that foundation is shifting. Europe's deep strategic dependence on U.S.'s cybersecurity capabilities, from intelligence and infrastructure to frameworks and funding, is now being tested by changing American priorities and a more volatile global landscape. Those tectonic geopolitical changes are undermining trust, threatening the state of safety, and compelling European organizations to rethink security architectures and approaches at every level.

The Pax Americana is fading, and in 2025 the foundation on which the cybersecurity ecosystem has been built started changing in response.

Cyber Balkanization

Driven by the unfolding geopolitical chilling between the US and Europe, cyberspace is fragmenting along political, national, and ideological lines, driven by sovereignty concerns, tariff disputes, censorship, and data control policies.

Cyber balkanization is the geopolitical fragmentation of the internet-once envisioned as an open, borderless network - into national or bloc-aligned cyber domains, driven by technology dependencies, security imperatives, and political influence, echoing Cold War-era divides. In 2025, we've been observing the phenomenon accelerating, tracking a political reality that is already fundamentally reshaping.

As we have continued to observe this past year, 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.

Economic Factors

The economic factors include macroeconomic trends such as inflation, exchange rates, growth rates, and capital availability that directly or indirectly affect the shape of the cybersecurity landscape.

This year we highlight the following:

Platforming & Dependency Risks

Platform firms have become the prevailing business model in the digital era, particularly in cloud computing, AI, and multi-sided marketplaces. Platform offerings provide infrastructures, protocols, or ecosystems that mediate interactions and enforce rules between participants. Platform businesses dominate because of network effects, low marginal costs, and the ability to scale rapidly. Analysts now describe platforms as the "dominant" enterprise form of the 21st century. Driven in part by the explosion of AI businesses, 2025 saw this trend accelerate further. The dominance of platform firms, especially cloud providers and major AI models,has been indirectly reshaping geopolitical dynamics and cybersecurity in several ways.

First, as states, enterprises, and critical infrastructure systems become dependent on a few platform owners, those owners acquire leverage over economic continuity. This dependency amplifies systemic risk: if access is restricted or terms changed, entire national industries or critical services can be disrupted.

Second, that leverage degrades sovereignty. Platforms rooted in one jurisdiction can bring foreign legal, regulatory, or coercive constraints to bear on users in other states via data access mandates, export controls, or compliance obligations. Nations lose autonomous control over their data, digital infrastructure, and strategic compute capabilities, making them vulnerable to external pressure and influence.

Finally, the concentration of digital power translates into economic, political and military advantage. States that host or dominate global platforms can project influence via control of foundational digital layers, shaping standards, access, signal intelligence, or even offensive cyber capacities.

In 2025 we noticed platformization increasingly emerging as a central domain of power competition, where control over clouds, models, and data can equal control over economies, security, and politics.

AI & Data Concentration

The widespread adoption of AI, especially large language models (LLMs), further entrenches dependency on a small number of providers. Because training and operating these models requires immense compute resources, massive datasets, and sophisticated infrastructure, only a few firms can realistically sustain them, creating a de facto "control layer" over the most advanced AI capabilities.

This concentration magnifies external influence, as those firms can exercise sway through access restrictions, API pricing, or selective feature gating. For states and organizations relying on third-party AI systems, this opens paths for coercion, conditional access, or forced localization in effect giving those providers latent geopolitical power over data, computational sovereignty, and strategic autonomy.

In 2025 we observed concentrated AI infrastructure becoming a strategic asset or systemic vulnerability in geopolitical competition - a particular concern for European security leaders. Nations that host or regulate leading AI providers gain leverage in setting rules, enforcing standards, or controlling cross-border data flow. Europe fears that rival powers may resort to restricting access, instituting export controls, or competing to build local alternatives, thus exacerbating concerns regarding European digital sovereignty.

Socio-cultural Factors

The socio-cultural factors include the demographic shifts, cultural norms, public attitudes, and lifestyle changes that shape behavior and expectations. This year we highlight the following:

Consumerism & Technology Adoption

As has been the case for several years already, in 2025 consumer demand for smart devices & IoT systems, and advanced AI tools has accelerated adoption of platform offerings. As users increasingly rely on connected services, providers bundle functionality, data access, and convenience into cohesive platforms, making isolated tools or alternative architectures less attractive.

Consumer demand for cloud services has continued to grow while demand for generative AI tools surged, leaving many businesses feeling compelled to incorporate those technologies into their operations or offerings.

As more consumers, organizations, and device ecosystems adopt cloud + AI services, it reinforces the network effect and accelerates consolidation around dominant platforms.

Every new user, application, or dataset added to a provider increases its attractiveness for others, making it increasingly difficult to switch or adopt alternatives. In effect, consumer behavior that values convenience, integration, or performance has intensified lock-in dynamics and deepened dependence on a handful of device, cloud and AI providers.

Security Gaps & Strategic Foresight

For the past year, consumer demand and a panicked response by businesses have left security teams racing to catch up. As employees have adopted new cloud or AI tools, defenders have been forced into retroactive assessment and mitigation. Without an appropriate strategy and architecture, security has become a reactive patchwork.

2025 has surfaced a threshold between innovation and sovereignty, as nations and enterprises realize they must resist treating these technology choices as purely tactical. It has become imperative to transition from reactive adoption and ad hoc defense, to a strategic approach that balances consumer demand and tangible business benefit with a sombre assessment of the technical threats and strategic risks.

Technological Factors

The technological factors include rates of innovation, adoption of new technologies, and the diffusion of automation or digital tools into the environment.

The threat will always adapt to the evolution of technology, and this year we consider whether developments in Artificial Intelligence (AI), Operational Technology (OT) and Quantum Computing have a significant impact on the threat landscape.

Threat Actors

Within the context created by the diverse systemic factors described above, we propose that there are three broad groups of actors active in the landscape that defenders need to consider:

Criminal

Criminal actors are driven by profit and constrained by risk. They will focus on targets and techniques that provide the best Return on Investment (ROI) for the lowest risk.

State

State Actors are directed by national security (or economic security) and have significant budgets, but are constrained by manpower, national law, global norms and the risk of reciprocation or escalation.

State-aligned

This emergent actor class of state-aligned (or "Establishment-era"[205]) hacktivism is politically motivated but (historically) constrained by technical capabilities. Since these actors are not constrained by national laws, global norms, or fear of escalation, we can thus expect them to escalate to attacks with kinetic impacts-e.g., against operational technology-even outside domains in open conflict.

AI: Shaping Reality

▪ **Wicus Ross** - Senior Security Researcher

Artificial Intelligence

Generative AI is here to stay. Its influence will shape our world for decades, bringing innovation and progress alongside disruption and risk. But the same tools that empower us to create and discover could also cause serious harm and even catastrophe. To fully understand the risks posed by the emergence of GenAI, we need consider multiple aspects of the equation, including the economic viability of the products and vendors driving the evolution.

The Economic Engine Behind AI

GenAI's rise is driven by vast investment in companies developing frontier large language models (LLM) such as OpenAI, Anthropic, Perplexity, and xAI[206]. These firms attract billions of dollars and spur demand for specialized high-end computing hardware[207]. The resulting expansion of datacenters fuels further energy consumption worldwide[208][209].

AI datacenters consume immense power. xAI's Colossus AI supercomputer, which trained Grok3, relies on Tesla power banks to stabilize grid fluctuations[210]. Microsoft, facing similar strain, is investing in carbon-free nuclear energy to feed its power-hungry AI infrastructure until more efficient hardware arrives[211][212][213]. U.S. GDP growth for early 2025 was nearly flat, but sustained mainly by heavy investment in data centers and IT[214][215]. Such spending now represents 4% of U.S. GDP, which is a 92% increase for the period[216].

The phrase "a rising tide lifts all boats"[217] captures the optimism regarding a promised productivity boom it is hoped will justify these investments and externalities. Wharton researchers predict AI could lift global GDP by 1.5% by 2035, nearly 3% by 2055, and 3.7% by 2075[218], but Microsoft's CEO Satya Nadella argues that GenAI must boost global GDP by as much as 10% to justify the scale of current investment[219]. Only 14% of European firms use AI [220] compared with 78% globally[221] and 58% of U.S. small businesses[222], raising doubts about near-term returns. Growth may stall if adoption lags.

Reaching the 10% global GDP growth Nadella envisions [223] seems improbable.

The IMF forecasts real economic growth for 2025 around 3.3%, up from 3.2% in 2024[224] and the OECD projects only 3.3% worldwide and 2.8% for the U.S, while major European economies remain below 2.5%.

If current AI models fail to deliver on the promised economic miracle, perhaps the key lies with artificial general intelligence (AGI). Frequent breakthroughs [225][226][227][228] show LLMs improving in math, coding, and reasoning benchmarks, yet progress is slowing. As models approach their limits, the next major leap is expected from AGI.

DeepMind's Demis Hassabis defines AGI as human-level cognition, while Anthropic CEO Dario Amodei sees it as expert-level task performance within seconds. Amondei argues that nations controlling such "super AI" will gain lasting economic and military advantages, requiring billions of dollars and millions of specialized chips[229]. The U.S. is racing to reach that milestone ahead of China.

Amodei predicts AGI could arrive by 2026-27 [230], while Hassabis puts its odds at 50% by 2030.

Boosting real global GDP from 3.2% to 4.2% would require several trillion dollars in new output. A 1% rise in global growth requires the addition of the equivalent of a major nation's GDP to the world economy. If the required growth fails to materialize, the resultant crash may leave tech business bankrupt and users without access to technology or services. Can AI realistically deliver 5-10% growth amid slowing productivity and other economic headwinds?

The Future of Work and Agentic AI

One of the purported benefits is that AI will reshape workforces as employers adopt it for automation. The World Economic Forum's Future of Jobs 2025 report finds that 40% plan staff reductions through AI[231], displacing 92 million jobs but creating 170 million new ones by 2030. Wharton identifies office, finance, and technical roles as most vulnerable to AI-driven disruption.

This kind of game-changing automation hinges on the emergence of agentic AI.

"Agentic AI"[232] refers to autonomous systems driven by LLMs that plan, decide, and act with minimal human input. These agents can use tools and collaborate with other agents to achieve complex goals through dynamic interaction. For example, a traveler might ask an agentic AI to plan an entire overseas trip. The system queries specialized agents for flights, hotels, and restaurants, then summarizes and presents options that the user refines through natural-language conversation.

However, LLMs and agentic AI do more than automate tasks to displace human workers, they fundamentally change how we relate with computers.

Software Evolution and Security Implications

Andrej Karpathy argues that LLMs are a new kind of operating system [233], emerging from software's evolution from code-based "Software 1.0," to neural-network-driven "Software 2.0," to today's "Software 3.0," where natural-language prompts serve as executable programs interpreted by LLMs.

Natural language offers a powerful way to interface with machines, but it also invites ambiguity. LLMs depend on precise context and intent, yet humans are often vague, manipulative, or careless, making misinterpretation inevitable.

In the "Software 3.0" paradigm, LLMs execute loosely defined instructions whose stochastic, non-deterministic nature produces unpredictable outcomes.

According to George Dyson, this emergent behavior is "that which cannot be predicted through analysis at any level simpler than that of the system as a whole. Emergent behavior, by definition, is what's left after everything else has been explained."[234]

This "emergent behavior" poses risks for critical or sensitive workflows.

LLMs form the foundation of today's agentic AI ecosystem. When chained together, these services create vast, complex systems with unpredictable outcomes because LLMs treat natural language as both instructions and data. Combining the two in a single execution pipeline fuels emergent behavior.

When an autonomous system causes harm, accountability is unclear. Cybersecurity experts Dan Geer and Dave Aitel warn that today's frameworks - including NIST's Secure Software Development Framework and OWASP guidelines - rely on predictable, accountable human coders[235]. Those assumptions break down under agentic AI's speed, opacity, and autonomy.

What recourse exists when one of these autonomous systems produces unwanted results? Who decides fault, and can users expect compensation?

Malicious actors will inevitably seek and exploit such weaknesses for personal gain.

Attackers are already exploiting GenAI to craft convincing phishing messages and to generate synthetic voices and videos that deceive victims, according to multiple cybercrime reports[236][237][238].

Anthropic's threat intelligence team also reports that criminals are already weaponizing agentic AI to support multiple stages of complex cybercrime[239]. It further documents cases of North Korean IT workers using GenAI to fraudulently obtain and retain remote foreign jobs.

In August 2025, ESET revealed PromptLock, a ransomware prototype that used GenAI to conduct attacks[240], although it was later confirmed to be a research project demonstration[241][242]. Even so, the proof-of-concept signals how future attackers might weaponize GenAI more effectively.

AI's transformative promise is inseparable from its systemic and security risks. These emerge from the defining characteristics of the technology, which are also the characteristics on which the technology's great "promise" hinge.

It's a gamble. Besides the fact that the emergent risks and threats are complex and difficult to predict, the technology itself may never deliver the promised economy required to offset the costs. This complex equation calls for demanding governance and restraint to balance disruptive new paradigms and innovation.

Operational Technology

▪ **Dr. Ric Derbyshire** - Principal Security Researcher

Operational technology (OT) is used to control, automate, and monitor physical infrastructure. Although you may not see it, you're almost guaranteed to have utilized it in every day of modern life. It can be found in the large physical infrastructures you may expect, such as the treatment of wastewater and provision of drinking water; power generation, transmission, and distribution; and manufacturing. However, OT permeates deeper than that. You'll find it in datacenters, where it manages power, cooling, and environmental controls that keep servers running. It's in stadiums that rely on automated systems to move retractable roofs and manage lighting and crowd flow. It powers major attractions, operating the control systems behind rides, lifts, and moving structures. It's also embedded in transport infrastructure, coordinating bridge hydraulics, tunnel ventilation, and traffic systems that keep cities moving.

At the heart of OT, you'll find some common technologies that bridge between the digital and physical. Programmable logic controllers (PLCs) are one of the more common assets that sense and actuate the physical world according to their configuration. Human machine interfaces (HMIs) allow operators to monitor the OT and the environment in which it's implemented, often with ways of facilitating interventions for engineers to have direct control. And more recently, the rise of the Industrial Internet of Things (IIoT) has made it possible to deploy more dispersed sensing, with connected devices sharing telemetry across networks and, in some cases, providing control.

Despite its clear criticality, OT continues to face an increasing number of outages due to cyber-attacks. Whether it's the persistent and pervasive onslaught of cyber extortion (Cy-X)[243] or the surging intent and capability of hacktivism[244], OT is not just reserved for the notorious "nation-state" adversaries it was once known to attract.

The most significant threat to OT remains indirect attacks on IT, typically ransomware, that cascade into operations. As IT/OT convergence permeates more organizations, these IT-borne incidents have become the primary driver of cyber-physical impact, fueled by the rise of ransomware-as-a-service and double extortion since 2020. This often occurs when OT dependencies within IT are affected during an attack, or when outages are self-inflicted out of caution or distrust in security controls and network architecture. However, while attacks on the IT are more frequent and therefore pose the most common threat, attacks deliberately targeting the OT with context-specific TTPs are where we see the most dangerous impacts. Using our dataset that has been presented in previous Security Navigator reports, we can isolate impacts unique to cyber-attacks that have included OT-specific TTPs. The results include manipulation of control, loss of safety, and damage to property. While less frequent, these are clearly much more impactful and therefore change the calculus of risk. Along with a threat asymmetry between IT and OT, we also have a similar defense asymmetry. Due to the ubiquity of IT and proliferation of ransomware targeting it, substantial resources have been spent on its defense. However, what about defending against those low-frequency, high-impact risks that OT faces? To begin with, how do we test whether we're vulnerable to them, particularly when OT production environments are so fragile?

To address this question, we recently concluded a piece of work with the Research Institute in Trustworthy Inter-connected Cyber-physical Systems (RITICS)[245]. In the work, we investigated the current challenges faced by OT penetration testing, and in doing so, provided recommendations on how it might be improved. The process included literature review, and interviews with practitioners and procurers.

The main challenge faced by OT penetration testing is that there are no public methodologies, and consequently no standardization at all. This causes knock-on consequences for procurers where they don't know what to expect from the results of a penetration test. Another related challenge is that of legacy IT penetration testing methods being applied to OT penetration testing. The scope-based, CVE-centric approach does not lend itself to producing useful findings. Instead, it results in reports that contain long lists of vulnerabilities, many of which are irrelevant in the context of the OT process. Conversely, OT lends itself to a more attack-narrative driven approach that guides the test in the direction of specific unacceptable impacts that have been identified in advance.

The skillset of penetration testers isn't seen as a challenge. In fact, the "hacker skills and mindset" are widely considered to be universal and transferable to any context. However, OT knowledge is often seen as lacking in OT penetration testers that have transitioned from a traditional IT cyber security background. To truly identify how sophisticated OT cyber-attacks may cause specific impacts during a penetration test, the testers need to be able to understand the industrial process and how it can be weaponized. This includes process comprehension, a tactic unique to OT cyber-attacks whereby the adversary gathers an understanding of:

- the underlying physical process,
- how the OT controls, automates, and monitors it,
- how the supporting network architecture is arranged,
- how cyber security controls are layered on top and
- how humans interact with every layer.

Culture is the final major challenge in OT penetration testing. Operators respond poorly to the connotation of "testing" their environment, seeing it as combative. Testing needs to be presented as a form of support for the operators' mission to prevent disruption, with a focus on safety. OT penetration testers that take this approach have a more productive relationships with the operators they work with.

As the OT security threat looms ever larger, Addressing these challenges requires short, medium, and long term responses.

In the short term, common guidance and baseline methods need to be established, supported by shared glossaries and catalogues of common physical consequences to improve clarity and consistency in OT testing. In the medium term, work should focus on developing better metrics for assessing OT vulnerabilities and integrating attack-narrative testing and process comprehension into standard methodologies. In the long term, research should embed OT testing within wider assurance frameworks and ensure it reflects real operational risk.

Together these measures represent a practical roadmap for strengthening OT penetration testing maturity and making results more actionable across industries.

You'll be able to read about our OT penetration testing study in more detail in 2026 with the publication of its associated paper.

Of course, penetration testing isn't all of cyber security, and solving its challenges in OT won't fix OT security as a whole. However, a more accurate emulation of adversary thinking, intent, and resultant TTPs will have a catalytic effect. Once we begin testing for the more relevant attack narratives, focusing on the OT process, with better relationships with operators, we can illuminate where we need to improve in other areas of OT security. From there, we can continue building on successes and look forward to a brighter, less dangerous cyber-physical future.

Post-Quantum Cryptography

▪ **Wicus Ross** - Senior Security Researcher

Cryptographic algorithms form the foundation of secure online communication, ensuring confidentiality, integrity, and authenticity. Much has improved since the 1990s. SSL has evolved into TLS to close vulnerabilities such as BEAST, POODLE, TLS 1.3 improved performance and tightened cipher-suite rules, and RFC 9325 established standards for secure configuration. Without these building blocks, the internet on which societies, businesses, and governments depend could not operate securely.

These foundations, however, may be facing a new threat. Quantum computing maybe represents an existential risk to the cryptographic systems that underpin digital trust. Modern cryptosystems resist nearly all known attacks, but advances in quantum computing threaten to overturn this resilience. The emergence of cryptographically relevant quantum computers (CRQCs) could make today's algorithms obsolete. For more on CRQC impacts and preparation strategies, see the article on PQC migration contributed by Dr. Mohammed Meziani.

Unlike classical computers that process bits as either 0 or 1, quantum computers use quantum bits (qubits) that can be both 0 and 1 simultaneously through a phenomenon called superposition. This ability lets quantum processors explore countless possible solutions simultaneously, rather than sequentially, enabling them to solve certain problems far faster. In some cases, they may solve problems that even the most powerful supercomputers still cannot. Quantum computers harness four fundamental principles of quantum mechanics:

- **Superposition:** A qubit can represent 1, 0, or both simultaneously, unlike classical bits with fixed binary states.
- **Entanglement:** Quantum particles can become so correlated that a change in one instantaneously affects the other.
- **Decoherence:** Quantum states degrade through interaction or measurement, collapsing into single, classically observable outcomes.
- **Interference:** Entangled states interact to create probabilistic variations that power quantum computation.

A quantum computer's capability is measured in qubits, or quantum bits, which exploit superposition and entanglement to solve problems beyond classical reach. Google's Willow chip, for example, operates with 105 qubits[246]. The greatest challenge for quantum computers is decoherence, which introduces noise and high error rates. The Willow chip mitigates this problem more effectively than others, thus achieving improved scalability as additional qubits are added.

Estimates from 2021 suggest that breaking RSA-2048 encryption would require about 6,190 logical qubits, or roughly 1.17 million physical qubits[247]. Gidney and Ekerå later calculated that 20 million qubits could perform the task in eight hours[248], before revising the estimate to a week[249] but with fewer than one million qubits. For comparison, the world's fastest classical supercomputer would need about 300 trillion years to achieve the same[250].

As of December 2024, Atom Computing's circuit-based processor boasts 1,180 qubits which makes it the leading known effort[251][252]. D-Wave's Advantage 2 boasts over 7,000 qubits[253] in the annealing processor category - an approach tailored to solve optimization problems by evolving a quantum system toward its lowest-energy (optimal) state. IBM plans to deliver a fault-tolerant machine by 2029 with 200 logical qubits and 100 million quantum gates[254]. Despite this progress, current hardware remains far below the million-qubit threshold required to compromise RSA-2048. A 2024 expert survey[255] placed a realistic timeline for a 24-hour quantum attack anywhere between today and 2035.

Because classical cryptography depends on difficult mathematical problems like factoring large primes or solving discrete logarithms, quantum algorithms such as Shor's can render it ineffective. Shor's algorithm allows factoring large integers (and solving discrete logarithms) within a finite time, thereby threatening the security of widely used public-key cryptosystems such as RSA and Elliptic Curve Cryptography[256]. This threat is the reason for the urgent attention on post-quantum cryptography (PQC).

To counter the quantum threat, new algorithms collectively known as post-quantum cryptography (PQC) have emerged. National authorities including NIST (US), NCSC (UK), ANSSI (France), and BSI (Germany) are developing standards and coordinating migration efforts[257]. The UK NCSC estimates that overall migration to PQC could take up to 10 years[258], but France, Germany, the Netherlands, the US, and the UK plan to deprecate RSA, ECDSA, EdDSA, DH, DSA, and ECDH by 2030 and ban them entirely by 2035[259].

This timeline affects every internet user. Browser and server developers must adopt PQC protocols as they did during the TLS transition[260]. Certificate authorities will need new standards, and virtually every connected device from servers and PCs to smart appliances and vehicles will require upgrades[261].

All sectors are exposed to the risk of weakened encryption. Financial institutions depend on cryptography to protect data and authenticate transactions and smart-card chips must be redesigned to meet PQC standards. The blockchain sector is especially impacted, since it fundamentally relies on digital signatures and hashes. Early projects like the Quantum Resistant Ledger (QRL)[262], Algorand[263], and Ethereum[264][265]are already testing PQC, but Bitcoin remains at risk since parts of its chain could be compromised[266][267]. Proposals are underway to make it quantum-resistant[268].

Major vendors such as Apple, Google, Microsoft, and Amazon AWS are embedding PQC algorithms into their operating systems, devices, and cloud platforms[269][270][271][272]. However, customers must update their own applications and systems to activate these protections.

Ultimately, every piece of critical infrastructure must be assessed against a realistic theat model.

Although not imminent, the transition to PQC has inspired both optimism and anxiety. Migration to PQC will differ for every organization, and many will temporarily run PQC and classical algorithms in parallel[273]. Transitioning existing systems is complex and risk-prone, requiring careful planning, coordination, and testing to avoid disruptions. Hence the emergence of “crypto agility”, the ability of a security system to rapidly replace cryptographic algorithms, keys or protocols in response to regulation, threats or new vulnerabilities. Because PQC methods are new and may surface future flaws, crypto agility is a characteristic rather than a project.

Preparing for this new reality demands that governments and businesses conduct quantum-risk assessments and allocate resources accordingly. Yet PQC projects must compete for funding, leaving smaller organizations and economies vulnerable to falling behind.

Leaders will need to embed crypto agility into their core policies[274]. Adaptation should not result from a specific threat, but form part of a broader strategy to strengthen organizational resilience.

Political, Economic and Sociocultural Factors

▪ **Charl van der Walt** - Head of Security Research

Cybersecurity in 2025 has been significantly shaped by the intersection of political, economic, sociocultural, and technological pressures. For European leaders, these forces converge in one critical question: how to make deliberate, strategic choices about the technologies and platforms on which our security, economies, society and sovereignty increasingly depend.

Geopolitics in Technology

All technology is now political, either as a weapon, a target, or a lever of influence. Technology enables technical power projection, cyber operations, misinformation campaigns, and new forms of soft power.

This reality is visible across the geopolitical spectrum. Conflicts such as Russia's war against Ukraine and the Middle East continue to demonstrate how cyberspace amplifies kinetic confrontation, while diplomatic crises across Africa-such as the dispute over Western Sahara-are also mirrored online. In 2025, another consequential shift has been the deteriorating relationship between Europe and the United States, as "America First" narratives redefine alliances and unsettle decades of trust that underpinned the post-war order.

The long peace under Pax Americana provided stability through U.S. leadership of the global security and technology ecosystem. Now that foundation is shifting. Europe's strategic dependence on U.S. cybersecurity technologies, intelligence, infrastructure, and funding is being tested by changing American priorities and a more volatile world. These tectonic changes are undermining trust and compelling European institutions (and the enterprises that rely on them) to rethink their architectures, procurement, and partnerships.

Digital Dependency- From Advantage to Exposure

Europe's modern success in digital transformation has been built upon deep integration with foreign platforms and providers. That integration has delivered efficiency and growth but also embedded a systemic asymmetry. As the political climate cools, dependence has become exposure, introducing new compliance, operational, and strategic risks.

According to the Eurostack report[275], over 80% of Europe's digital technologies are imported. U.S. companies dominate foundational tools, with Microsoft, Apple, and Google controlling over 90% of the European market for operating systems.

Just three U.S.-based firms-Amazon, Microsoft, and Google-account for nearly 70% of Europe's cloud infrastructure market and 70% of foundational AI models have been developed in the United States, with another 15% in China.

Meanwhile, China controls approximately 90% of the world's rare earth refining capacity-crucial for the production of everything from smartphones to wind turbines. And in terms of digital innovation investment, EU firms represent only 7% of global R&D spending in software and internet technologies, compared to 71% by U.S. firms and 15% by Chinese firms.

From a risk perspective, this vulnerability can be viewed through two lenses:

- **Compliance risk** arises from the EU's ongoing assessment of U.S. assurances that they can meet European legal standards on data protection and privacy. Should those assurances fail, EU data may no longer be lawfully stored or processed by U.S. companies. This is a transparent, consultative, and predictable legislative process, but one that could impact the entire Union.
- **Operational** risk emerges when U.S. technology companies are compelled to enforce U.S. government sanctions, potentially denying services to entities or individuals. The allegation that Microsoft denied email access to the International Criminal Court's chief prosecutor illustrates this risk . Such sanctions arise from U.S. national security mechanisms rather than judicial or congressional approval. They can be applied to individual employees, enacted with little warning, and lack public transparency, making them impossible to anticipate or mitigate in advance.

> **These dual risks demonstrate that technology procurement is no longer a purely operational consideration. It is a strategic act that must account for legal, political, and sovereignty implications.**
>
> ▪ **Bjørn Kristian Rasmussen**
> CTO Orange Cyberdefense Norway

A Strategic Imperative- From Dependency to Strategic Interdependence

Yet the goal for European leaders should not be isolationism. It should be to achieve strategic interdependence by developing the ability to choose partnerships voluntarily from a position of strength and trust. Achieving this balance requires autonomy in key technologies, diversification of intelligence and suppliers, and a disciplined approach to security architecture.

For business and cybersecurity leaders, this means:

- **Treat procurement as a security decision,** assessing vendors not only for technical capability but for geopolitical and legal exposure.
- **Evaluate and support open-source alternatives** wherever feasible, to enhance transparency, reduce vendor lock-in, and strengthen collective resilience through shared development and oversight.
- **Simplify and harden environments,** as each new dependency extends the attack surface and the supply chain.
- **Prioritize trustworthy intelligence** that is actionable and locally relevant, rather than relying solely on external or global feeds.

These measures allow organizations to move from reactive defense toward strategic foresight by building resilience through governance and planning, not only in systems.

Building Sovereign Capacity- The Eurostack Principle

Europe's pathway to sovereignty lies in federated, interoperable digital architecture.

The EuroStack embodies this direction. The initiative describes a vision for a technologically resilient Europe, presenting a comprehensive strategy to establish Europe's digital sovereignty[276]. It advocates for the development of a federated digital infrastructure encompassing cloud services, data governance, and artificial intelligence, rooted in European values and legal standards.

Key components of EuroStack include:

- **Federated cloud infrastructure:** developing interconnected cloud services that ensure data remains within EU jurisdictions. This approach aims to reduce dependency on non-European cloud providers and enhance data sovereignty.
- **Open-source platforms:** promoting the use of open-source software to enhance transparency, reduce vendor lock-in, and foster innovation. As of a few years ago, Europe had over 3 million open-source contributors, reportedly surpassing the United States in active participation . By leveraging Europe's strength in open-source communities, EuroStack proposes to build a resilient and collaborative digital ecosystem.
- **Investment in R&D:** allocating resources to research and development to drive innovation within the continent. The initiative calls for substantial investment, including the establishment of a European Sovereign Tech Fund to support homegrown technologies and reduce reliance on foreign solutions.

EuroStack describes a path via which Europe may begin to transition from a position of dependency to one of strategic autonomy. This shift would enable the continent to safeguard its democratic values, enhance cybersecurity, and ensure that its digital infrastructure aligns with its economic and societal objectives.

But the objective should not be to wall off Europe technologically. Rather it is to ensure that dependency becomes choice and not compulsion. Federated initiatives such as EuroStack and the ongoing European Union Cloud Services Scheme (EUCS) demonstrate how shared governance, transparency, and open protocols can strengthen the region's innovation ecosystem while reducing single-vendor lock-in.

Sovereignty, in this sense, is not isolationism; it is the freedom to engage globally on equitable terms. To innovate and interoperate without sacrificing control, compliance, or trust.

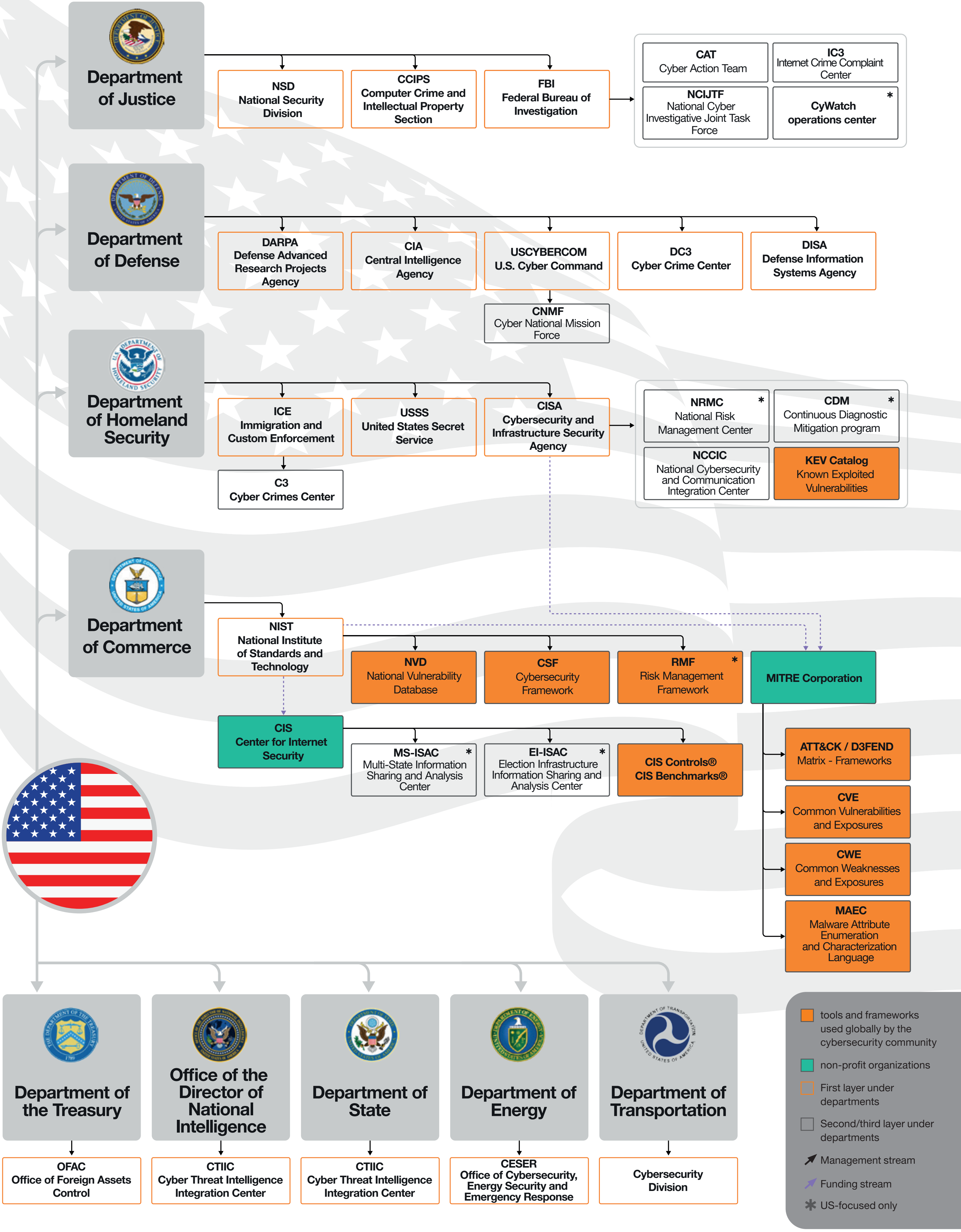
Leadership at the Intersection Of Innovation and Sovereignty

Europe now stands at a decisive crossroads. The forces of AI, cloud adoption, and global platformization that are driving innovation are also redefining sovereignty and security. Enterprises must navigate this tension between progress and dependence with deliberate strategy and foresight.

Security defenders are already feeling the strain. As employees and business units are influenced to adopt new AI or cloud tools, defenders are left scrambling to assess unplanned risks and configuration gaps introduced by technologies chosen without strategic oversight.

As 2025 surfaces this juncture between innovation and sovereignty, it's essential for enterprises to understand the drivers of change shaping today's cyber landscape. Future resilience will depend on a multi-faceted strategy combining foresight, planning, alliances, and investment in sovereign capacity.

Europe's security and prosperity now depend on treating technology choice as a strategic decision. Each adoption, integration, or partnership either reinforces autonomy or deepens dependency. The future will belong to those who can balance innovation with sovereignty, ensuring that Europe's digital transformation strengthens its values, freedom, trust, and resilience.



Department of Justice

NSD
National Security Division

CCIPS
Computer Crime and Intellectual Property Section

FBI
Federal Bureau of Investigation

CAT
Cyber Action Team

IC3
Internet Crime Complaint Center

NCIJTF
National Cyber Investigative Joint Task Force

CyWatch *
operations center

Department of Defense

DARPA
Defense Advanced Research Projects Agency

CIA
Central Intelligence Agency

USCYBERCOM
U.S. Cyber Command

CNMF
Cyber National Mission Force

DC3
Cyber Crime Center

DISA
Defense Information Systems Agency

Department of Homeland Security

ICE
Immigration and Custom Enforcement

C3
Cyber Crimes Center

USSS
United States Secret Service

CISA
Cybersecurity and Infrastructure Security Agency

NRMC *
National Risk Management Center

CDM *
Continuous Diagnostic Mitigation program

NCCIC
National Cybersecurity and Communication Integration Center

KEV Catalog
Known Exploited Vulnerabilities

Department of Commerce

NIST
National Institute of Standards and Technology

NVD
National Vulnerability Database

CSF
Cybersecurity Framework

RMF *
Risk Management Framework

MITRE Corporation

CIS
Center for Internet Security

MS-ISAC *
Multi-State Information Sharing and Analysis Center

EI-ISAC *
Election Infrastructure Information Sharing and Analysis Center

CIS Controls®
CIS Benchmarks®

ATT&CK / D3FEND
Matrix - Frameworks

CVE
Common Vulnerabilities and Exposures

CWE
Common Weaknesses and Exposures

MAEC
Malware Attribute Enumeration and Characterization Language

Department of the Treasury

OFAC
Office of Foreign Assets Control

Office of the Director of National Intelligence

CTIIC
Cyber Threat Intelligence Integration Center

Department of State

CTIIC
Cyber Threat Intelligence Integration Center

Department of Energy

CESER
Office of Cybersecurity, Energy Security and Emergency Response

Department of Transportation

Cybersecurity Division

🟧 tools and frameworks used globally by the cybersecurity community

🟩 non-profit organizations

□ First layer under departments

□ Second/third layer under departments

↗ Management stream

↗ Funding stream

✱ US-focused only

The Threat Actors

▪ **Zohra Hamila** - Security Researcher
▪ **Dr. Ric Derbyshire** - Principal Security Researcher

Cyber Criminals

In recent years, the cybercrime ecosystem has undergone significant transformation, not only in scale and diversity but also in its structure and identity. As conflicts, crises, and economic instability continue to increase globally, this reverberates in the digital underground space. Considering cybercrime as a detached component of the international landscape simply denies the contemporary reality of that ecosystem.

One of the most persistent misconceptions in the cybersecurity field is the assumption of a fixed, monolithic adversary. Threat actors are often defined as stable and coherent entities, with distinct tools and tactics. However, many of these groups are better described as loose affiliations of individuals, bound not by trust, hierarchy, or loyalty but by shared financial objectives achieved through pragmatic collaboration. Their operational agility turns attempts to label them into an underlying vulnerability for defenders, limiting the effect of prevention and response strategies. This challenge is emphasized when threat actors reorganize and rebrand.

This fluidity extends to motivation. In recent years, cybercrime activity has been increasingly influenced by geopolitical events, blurring the line between financial, political, and ideological drivers. While many cybercriminal groups pursue financial or ideological agendas, the actions of the states that host them inevitably draw them into the broader dynamics of the international scene. In addition, grey zones are emerging in which states tolerate, encourage and even involve civilians in cyber operations as seen in the war against Ukraine[277]. This challenges the traditional notions of sovereignty and attribution, showing that cyber defense can no longer be viewed purely as a matter of technical risk management. It requires a broader framework which includes strategic, cognitive, and geopolitical dimensions.

The commoditization of cybercrime “as a service” has drastically lowered the threshold to participate in these activities. This has been observed since 2020, with a steady increase in the number of new groups appearing in the Cy-X and hacktivist space. The development of the Crime-as-a-Service economy has enabled threat actors to launch impactful attacks supported by the growing availability of third-party services leveraged to outsource parts of their attacks: bulletproof hosting, money laundering, initial access brokers. This phenomenon is further amplified by the misuse of developing technologies such as cryptocurrencies[278] and AI. The combination of these elements does not only form fertile ground for opportunistic attacks, but it gives threat actors an edge in adapting defense and law enforcement efforts and exploiting emerging vulnerabilities.

State-Backed Actors

Since last year’s Security Navigator, state-linked cyber operations have remained active with a primary focus on intelligence collection and occasional disruptive actions used for signaling, amid a backdrop of information operations that vary widely in scale and intensity[279]. A clear pattern is long-term pre-positioning inside critical infrastructure using routine administrative tools and techniques that blend into normal activity.

Attack methods are concentrating around identity and the edge[280]. Recent reporting also describes stealthy backdoors placed on appliance and virtualization platforms to maintain access for many months without noisy malware[281]. In parallel, rapid exploitation of 0-day and n-day vulnerabilities in perimeter appliances remains common, and supplier and service-provider pathways continue to feature prominently in incident trends[282].

Targeting remains concentrated on government and telecommunications, with repeated activity against defense linked networks[283]. High tech sectors, notably semiconductors, also saw focused campaigns in 2025[284]. The seam between enterprise IT and OT in industrial environments remains a concern, with pivots into plant and field systems where monitoring is limited and safety constraints slow response. Blended operations that combine intrusion with information tactics continue to surface, including hack-and-leak activity aimed at shaping narratives[285]. Open reporting also indicates continued use of commercial spyware by government clients, with fresh forensic cases against journalists in 2025[286].

Attribution and response remain complicated because visibility varies by region, analysts don’t always agree on which intrusions belong to the same actor, and adversaries use deception. To avoid overreach, trend analysis benefits from cautious, multi-source corroboration, and clarity about confidence levels. Sanctions remain a primary diplomatic lever to impose costs for state-linked cyber activity, often paired with public attribution, indictments, export controls, and joint advisories[287].

This state-linked picture is only part of the landscape. Non-state actors and hacktivists increasingly operate alongside or in the wake of state campaigns.

Establishment Era State-Aligned Hacktivists

Hacktivism continued to embed itself firmly in the Establishment Era over the past year, which has been maturing since approximately 2019. The center of gravity is now aligned with host states and conflicts, with campaigns that target ideological opposition. This is the backdrop for what we have coined as “escalatory hacktivism”, where actors seek higher-impact moments and political relevance rather than protest “the establishment” itself[288].

DDoS continues for private and public sectors. Dark Storm Team claimed outages at X in March 2025, a reminder that platform-scale DDoS still earns attention[289]. Pro-Russia NoName057(16) ran multi-day waves against UK public bodies in May 2025, briefly knocking some services offline and highlighting persistent pressure on government surfaces[290]. We also saw more instances of cyber-physical intent translating into action. For example, on April 7, 2025, attackers remotely opened a valve at the Bremanger dam in Norway for several hours before operators intervened[291]. More recently, a Russian-aligned group boasted on Telegram about breaching what turned out to be Forescout’s water-utility honeypot[292].

Policy responses have not kept pace with the threat’s scale and speed. Sanctions, takedowns, and occasional arrests struggle to deter a dispersed ecosystem that includes state-tolerated volunteers and rebrand-ready crews. Europol’s Operation “Eastwood” degraded NoName057(16)’s DDoS infrastructure in July 2025[293]. Within a week, the group resumed claiming attacks; a Europol spokesperson said the aim was disruption rather than complete dismantlement[294].

Earlier in the year, we released research on the current state of escalatory hacktivism that concerns all the points above. In doing so we introduced the Cyber Impact-Alignment-Responsibility Spectrum (CIARS) to better interpret hacktivists. CIARS weighs the impact of hacktivist attacks, observable alignment with a host state, and any evidence of that state’s control or support. It can be seen below, but the full preprint is available online[295].

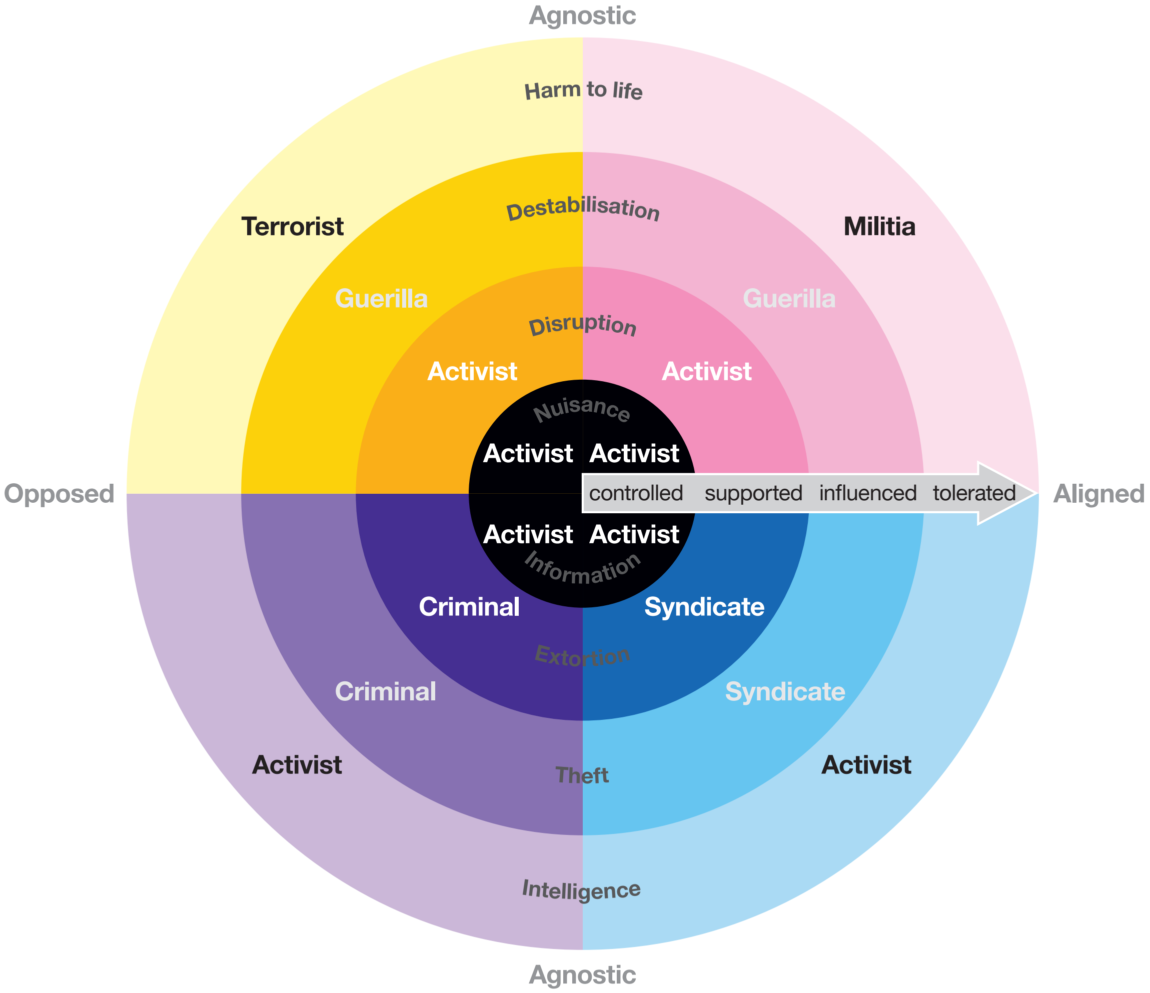
The concern is not just that hacktivism has escalated, but that it continues to do so. Capabilities remain limited yet are growing, and stated intent to disrupt operational technology increases the risk of future moves beyond click-ops. Three drivers are exacerbating escalatory hacktivism.

First, an attention race pushes groups to keep chasing the metaphorical cyber-dragon, competing for visibility and relevance, so each round demands a larger spectacle.

Second, widening conflicts draw hacktivists to target opposing states and their supporters, extending campaigns into allied countries and partners.

Third, hacktivists face fewer constraints than other threat actors. Even belligerent states weigh diplomatic cost, and cybercriminals consider return on investment and reputation. Hacktivists often do neither.

Together, these forces signal further escalation amid an environment increasingly characteristic of hybrid warfare in and through cyberspace. Countering escalatory hacktivism demands sustained, coordinated action from operators of essential services, national authorities, and international institutions.



Tracking the Fight Against Cybercrime

- Diana Selck-Paulsson - Senior Security Researcher
- Zohra Hamila - Security Researcher

Introduction

The growing sophistication and diversification of cybercrime has compelled law enforcement agencies worldwide to respond through increasingly coordinated and publicized actions. Yet, despite the visibility of these operations, there remains no comprehensive overview, to our knowledge, on how law enforcement is addressing cybercrime globally. Publicly available information is dispersed across agencies, jurisdictions, case-specific reporting (e.g. "Operation Endgame"[296]) and reporting formats, offering fragmented insights rather than a cohesive understanding of what types of crime are being targeted, what actions are taken, and who the offenders are. This results in isolated glimpses rather than a consistent global picture. Therefore, no publicly available summary exists that we are aware of that systematically aggregates information on law enforcement actions.

About the Data

To address this gap, this analysis introduces a systematically constructed dataset of 418 publicly announced law enforcement activities conducted between 2021 and mid-2025. The data was collected by Orange Cyberdefense intelligence teams, which continuously monitors and assesses cyber threats to identify emerging trends and the evolution of cyber incidents.

In our dataset each entry represents a verified law enforcement action collected from official announcements and media reports, then manually enriched by the Orange Cyberdefense Security Research Center team by cross-referencing each entry to include contextual and demographic details when available.

A central focus lies on the type of law enforcement action taken, such as arrests, extraditions, takedowns of illicit platforms, seizures, or sanctions. The type of illicit activity was also documented by noting which type of crime the law enforcement action addressed, e.g. Hacking, Distributed Denial of Service (DDoS) Attack, IT Worker Fraud or Cyber Extortion, and then translated into the actual criminal act of such attacks.

Type	Cybercrime Category (Criminal Act)
Hacking	Unauthorized Access / Intrusion
Distributed Denial-of-Service (DDoS) Attack	Unauthorized Disruption of Services
IT Worker Fraud	Insider Misuse of Access Privileges
Cyber Extortion	Demands for payment under threat of ICT[297] (incl. Ransomware)

The dataset also records the participating law enforcement agencies and countries, as well as offender characteristics such as nationality, age range, gender, and group affiliation. While the dataset is based on publicly available reporting, it nonetheless offers an empirical overview of global law enforcement efforts to counter cybercrime.

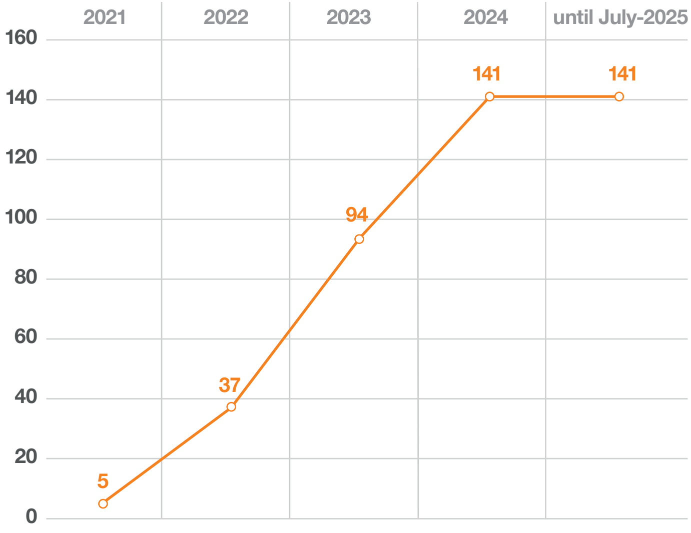
Limitations: Like all open-source datasets, this one has inherent limitations. It captures only publicly reported actions, reflecting the subset of offenders who have been identified, apprehended, or disrupted, rather than the full spectrum of cybercriminal activity. Furthermore, not all announcements include complete demographic information: age, gender, or nationality are sometimes unavailable.

From Crime to Response

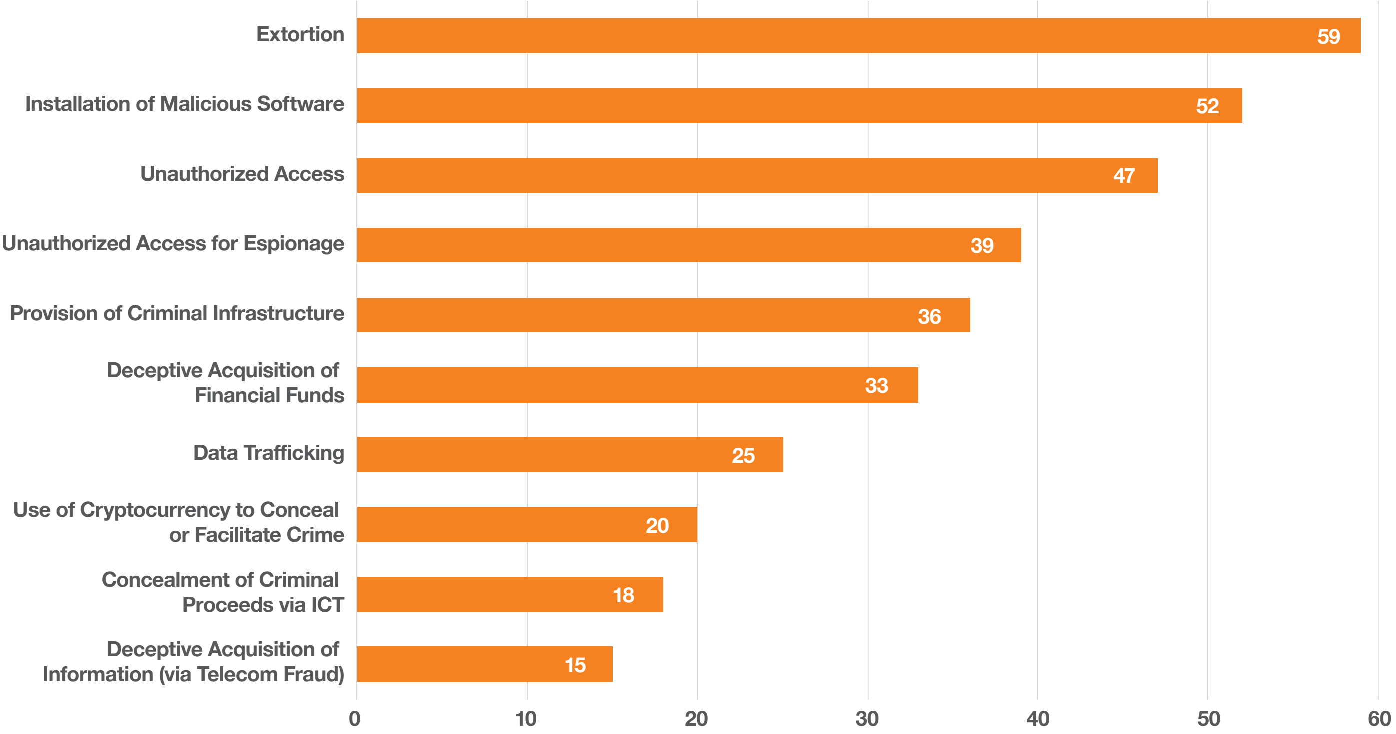
By analyzing how authorities respond through their actions, the types of crime addressed, and international collaborations, we gain a clearer understanding of who is driving global efforts to disrupt cybercrime and how these responses are shaping the broader security environment.

As can be seen below, our data shows a clear and steady increase in publicly announced law enforcement (law enforcement) actions targeting cybercrime between 2021 and mid-2025. The number of reported operations has grown each year. Notably in July 2025, the volume of law enforcement actions already matched 2024's total (141 cases). Thus, the year 2025 may see even higher numbers of recorded law enforcement actions to date once completed.

Law Enforcement Actions Over Time



Top 10 Criminal Acts Targeted by Law Enforcement



Which Criminal Acts Were Addressed?

This chart shows the top 10 criminal acts most frequently addressed by law enforcement in publicly reported operations.

The data reveals that Extortion (incl. Ransomware) is the most addressed criminal act, followed closely by Installation or Distribution of Malicious Software (Malware) and Unauthorized Access or Intrusion (Hacking). Together, these three categories dominate the landscape and illustrate law enforcement's continued focus on Cyber Extortion operations and the technical intrusions that enable them.

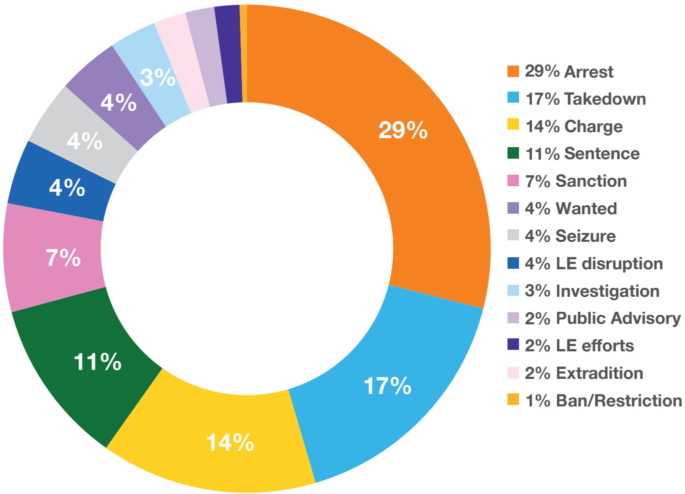
Other prominent criminal acts, including Unauthorized Access for Espionage (Cyber Espionage), Provision of Criminal Infrastructure (Dark Web Marketplace / Sites or Infrastructure and Hosting Services) and Deceptive Acquisition of Financial Assets (Fraud) suggest that authorities are also targeting the enablers and facilitators of cybercrime. While less frequent, offenses like Data/ Information Trafficking (Selling Stolen Goods (Data), Use of Cryptocurrency to Conceal or Facilitate Crime (Cryptocurrency Misuse), and Concealment of Criminal Proceeds via ICT (Money Laundering) reflect law enforcement's increasing attention to the financial transactions and laundering mechanisms that underpin cyber operations.

While financial gain remains a central driver of cyber offenses[298][299][300], the lines between motivations have become increasingly blurred, in some cases shifting in response to geopolitical events, as we have continuously been reporting on in the past two years[301][302]. Activities initially framed as financially motivated can quickly take on political or ideological dimensions. These fluid boundaries illustrate how financial, political, and cognitive motives increasingly coexist, challenging traditional distinctions between criminal and ideological cyber activity.

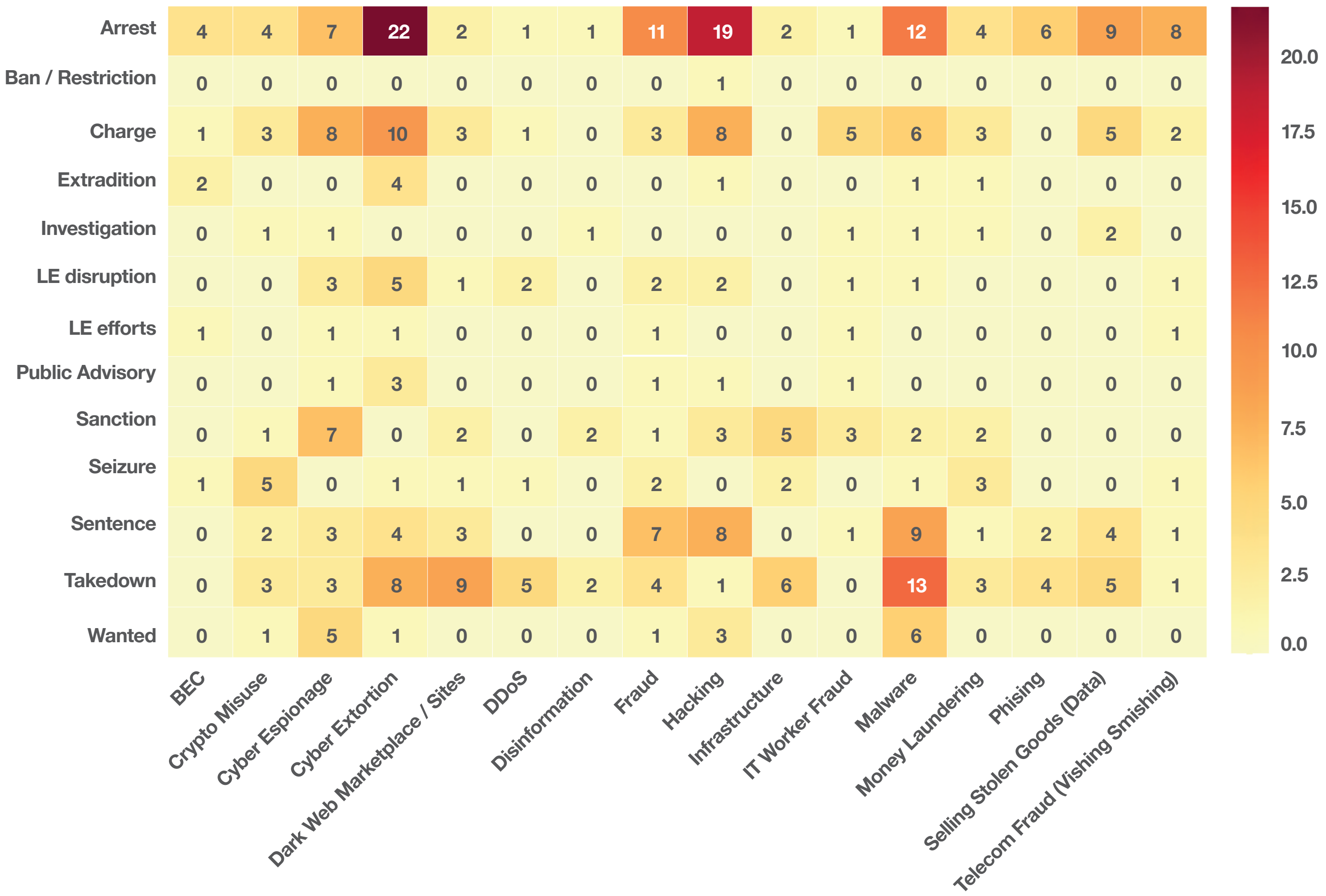
What Actions Were Taken by Law Enforcement?

Arrests account for the largest share (29%) of law enforcement actions, illustrating law enforcement's continued focus on individual accountability and prosecution. Takedowns (17%) and Charges (14%) indicate a strong emphasis on disrupting operational networks and bringing offenders to justice, and together represent nearly one-third of all activity. Complementary measures such as Sentences (11%), Sanctions (7%), and Seizures (4%) show that law enforcement is addressing both criminal actors and the economic infrastructure sustaining their activities. Specifically, sanctions have shown a steady increase over recent years and reflect a growing use of non-traditional enforcement mechanisms for the inclusion of economic and diplomatic tools within the law enforcement arsenal.

Types of Law Enforcement Actions



Law Enforcement Actions vs. Cybercrime Types



	BEC	Crypto Misuse	Cyber Espionage	Cyber Extortion	Dark Web Marketplace / Sites	DDoS	Disinformation	Fraud	Hacking	Infrastructure	IT Worker Fraud	Malware	Money Laundering	Phising	Selling Stolen Goods (Data)	Telecom Fraud (Vishing Smishing)
Arrest	4	4	7	22	2	1	1	11	19	2	1	12	4	6	9	8
Ban / Restriction	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
Charge	1	3	8	10	3	1	0	3	8	0	5	6	3	0	5	2
Extradition	2	0	0	4	0	0	0	0	1	0	0	1	1	0	0	0
Investigation	0	1	1	0	0	0	1	0	0	0	1	1	1	0	2	0
LE disruption	0	0	3	5	1	2	0	2	2	0	1	1	0	0	0	1
LE efforts	1	0	1	1	0	0	0	1	0	0	1	0	0	0	0	1
Public Advisory	0	0	1	3	0	0	0	1	1	0	1	0	0	0	0	0
Sanction	0	1	7	0	2	0	2	1	3	5	3	2	2	0	0	0
Seizure	1	5	0	1	1	1	0	2	0	2	0	1	3	0	0	1
Sentence	0	2	3	4	3	0	0	7	8	0	1	9	1	2	4	1
Takedown	0	3	3	8	9	5	2	4	1	6	0	13	3	4	5	1
Wanted	0	1	5	1	0	0	0	1	3	0	0	6	0	0	0	0

Actions like Investigations, wanted notices, and extraditions demonstrate cross-border cooperation and the procedural depth behind each publicized enforcement effort. Wanted notices represent a non-coercive enforcement measure focused on public identification and pursuit. They bridge the gap between investigation and arrest by facilitating cross-border coordination and sustaining pressure on suspects. Through public attribution, they also serve a deterrent function, signaling law enforcement capability and reach even when direct apprehension is not immediately possible.

If we combine the data showing the type of illicit activity addressed, with the type of law enforcement action, we can see that Arrests dominate across nearly all crime types, particularly Cyber Extortion (22) and Hacking (19).

Charges and Sentences are the next most frequent responses, which demonstrates that many cases progress through to judicial process. Cyber Extortion, Malware, Hacking, and Cyber Espionage attract the most diverse range of responses (including arrests, charges, sentences, sanctions).

Takedowns are strongly linked with Dark Web sites or marketplaces[303][304][305] and malware infrastructure[306][307][308] which makes sense given the operational logic behind such actions. These operations typically involve the coordinated dismantling of online infrastructure, such as servers, domains, or communication platforms that enable criminal activity. In the case of Dark Web Marketplaces, takedowns often include seizure of servers, arrests of administrators, and replacement of website landing pages with law enforcement banners, signaling control and deterrence. Sanctions appear primarily tied to Cyber Espionage and state-aligned operations, reflecting government-level actions rather than addressing individuals.

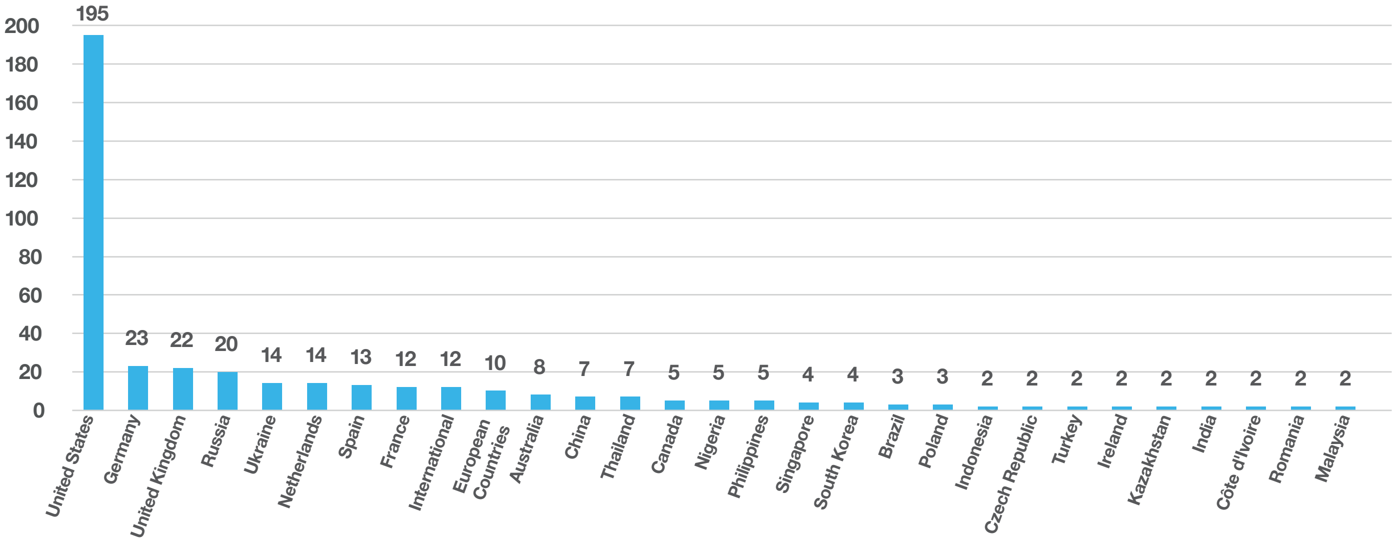
Which Countries Make The Most Effort To Disrupt Cybercrime?

The United States' global leadership in cyber law enforcement is demonstrated by its listing as the primary participant in nearly half of all actions (45%).

The second cluster, namely Germany, the United Kingdom, Russia, Ukraine, the Netherlands, Spain, and France, represents the core of global cyber enforcement capacity outside the U.S. Active EU member-state participation in Europol and Eurojust-led operations demonstrates the Union's emphasis on a joint, cross-border enforcement approach.

The presence of Russia and Ukraine near the top of this list is noteworthy. These states are frequently targets of global law enforcement actions but also conduct their own domestic prosecutions and counter-cybercrime operations, often involving politically sensitive cases. Entries such as International and European Countries reflect the role of multinational task forces where leadership attribution is shared. These include Europol-led takedowns, Interpol operations, and Five Eyes collaborations. In some cases, law enforcement announcements did not go into detail and only described these multinational actions by European nations or International ones, whenever countries were listed on their own, they were documented as such in our data.

Top 30 Countries Leading the Law Enforcement Action



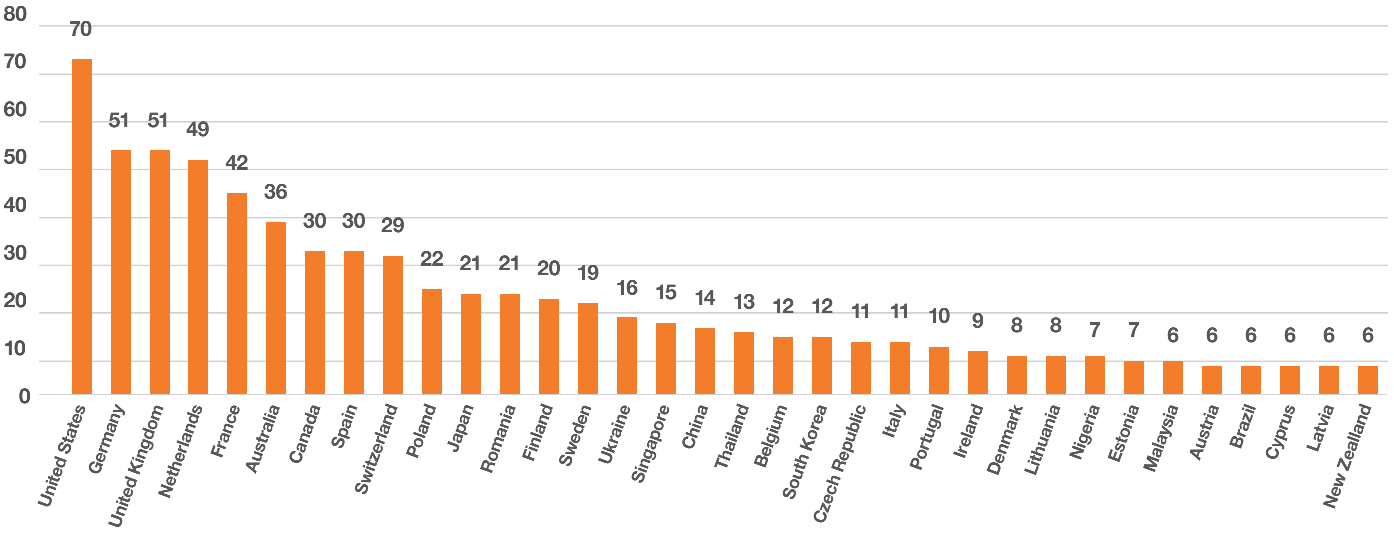
The Collaborative Landscape

While we studied the countries that lead a specific law enforcement action, we now dive into the secondary countries. Countries that followed the lead and assisted within their own capabilities in a law enforcement action. We call them collaborating countries. The United States again demonstrates its central role in global cyber enforcement, appearing as a secondary participant in 17% of all reported law enforcement actions. A strong European commitment follows, with Germany, the United Kingdom, the Netherlands, and France each involved in roughly 10-12% of collaborations. Australia and Canada stand out as core Five Eyes partners, maintaining consistent involvement in global operations.

Countries like Poland, Japan, Romania, Finland, Sweden, Ukraine, Singapore, China and Thailand occupy a mid-tier position in the collaboration landscape. They appear regularly in multinational operations but not at the same frequency as leading actors such as the United States, Germany, or the United Kingdom.

In summary, we see that the U.S. and Europe remain the central enforcement hubs, with overlapping involvement across most international disruption efforts. But countries from Asia, Africa, and Latin America increasingly participate and demonstrate the globalization of cyber law enforcement cooperations.

Top 30 Countries Collaborating in Law Enforcement Actions



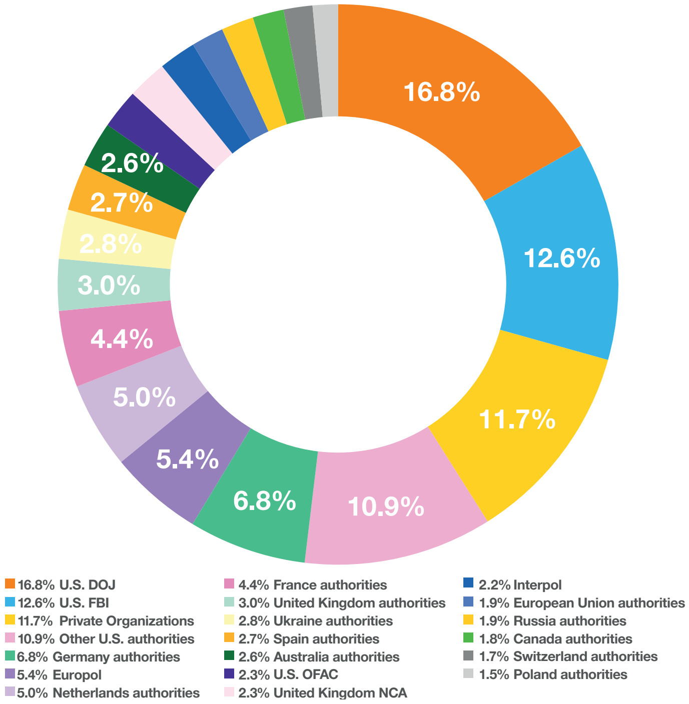
Who Are the Leading Institutions in Law Enforcement?

The distribution of participating national authorities naturally reflects the same geographic patterns observed in the country-level analysis.

A study of the top 20 institutions involved in reported law enforcement actions highlights the clear dominance of U.S. agencies. The U.S. Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI) lead by a wide margin, followed by private organizations, which appear as a major supporting actor in cybercrime disruption efforts. The presence of OFAC[309] further illustrates the integration of financial and political instruments into cybercrime responses.

The strong representation of private organizations among the leading entities is particularly noteworthy. In this dataset, private organizations rank among the top three most frequently mentioned participants. Across the 169 institutions analyzed, 74 distinct private entities were identified as supporting efforts in one way or another. This is a significant indicator of the expanding scale of public-private collaboration, which illustrates its growing importance in the fight against cybercrime.

Top 20 Law Enforcement Institutions



Who Are the Cybercriminals (That Got Caught)-and What Do We Know About Them?

Shifting focus from those working to counter cybercrime to the offenders themselves, consider the individuals behind these illicit operations. Law enforcement data reveals who is acting, what types of crimes are being investigated, and how international cooperation is organized. In contrast, offender data sheds light on who engages in these activities, where they originate, and the broader trends that emerge across the cybercrime landscape.

Offenders' Age

The age distribution of offenders in this dataset reveals notable distinctions from patterns traditionally observed in crime studies. Our data indicates that cyber offenders are not exclusively young adults, as conventional theories might suggest[310][311][312].

Foundational studies generally suggest that criminal behavior typically emerges in adolescence, peaks in the late teens or early adulthood, and declines sharply thereafter. This is due to developmental changes, reduced impulsivity, and stronger social bonds that come with age. Known as the Age-Crime Curve (ACC), this pattern describes the consistent relationship between age and the prevalence of offending across most forms of traditional crime[313][314][315].

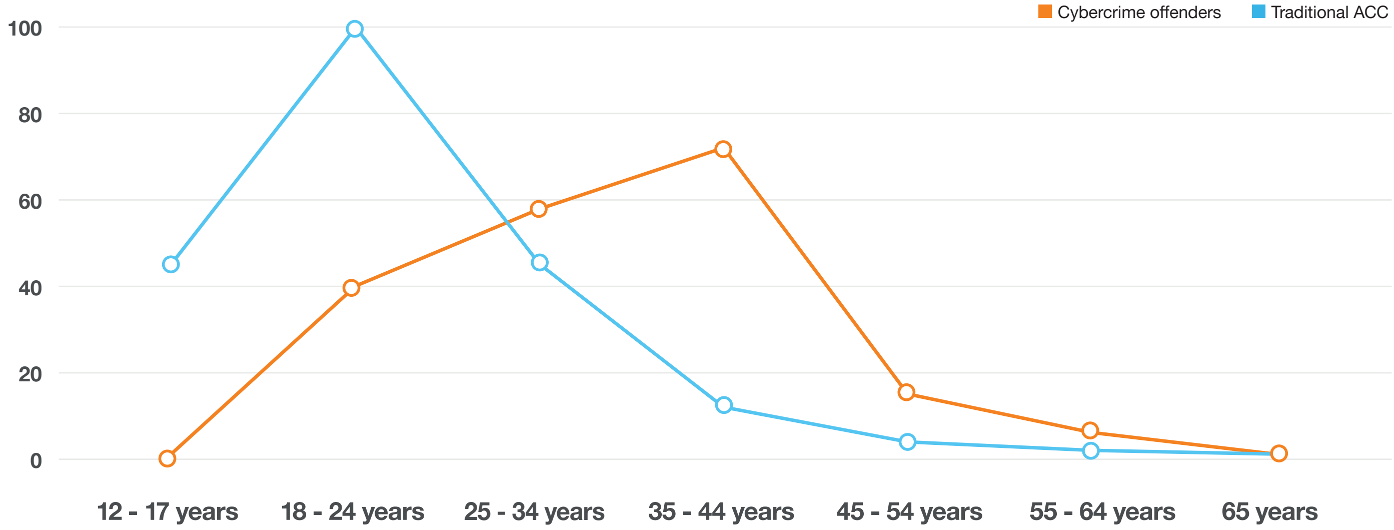
By contrast, the data considered here reveals more sustained criminal activity across adulthood and even into mid-life, which suggest that cybercrime might follow a different developmental pattern than traditional forms of engaging in crime.

More recent studies show a more nuanced picture by offense type, context, and measurement, suggesting that age-crime dynamics are no longer universal and might have changed, similar to our findings.

The United States Sentencing Commission (2024)[316] found that in federal crime cases involving child pornography, hacking, cryptocurrency, or dark-web tools, the median offender age rose from 30 to 34 years (2014-2021). By contrast, a study of 50 convicted romance-fraud offenders in Nigeria[317] found that 46% were aged 18-23 and 39% aged 23-28, and only 1% aged 34 and above, yielding a median age of 24 years, a profile consistent with the traditional ACC. Likewise, the UK Millennium Cohort Study[318] reported 5.6 % offending at 14, 3.8% at 17, and only ~1.1 % persisting committing crime, reflecting an adolescent peak followed by steep desistance. Hadzhidimova and Payne (2019)[319] found that among international cyber-offenders prosecuted in the U.S., the average age was 'slightly higher' than those in more generic samples, again suggesting that higher-visibility cybercrime cases tend to involve older actors.

As can be seen below, offenders considered here differ from the traditional age distribution. The prevalence of middle-aged offenders (35-44 years) indicates a form of criminal engagement that is deliberate and cognitively informed, rather than impulsive or situational.

Age Range Cybercrime Offenders (N=193) vs. Traditional Age Crime Curve



The Rational Choice Theory, developed by Clarke and Cornish (1985)[320], posits that offending is not purely impulsive or pathological, but the result of a reasoned, yet bounded, evaluation of risks, rewards, and situational factors. This finding thus suggests that many cyber offenders possess the maturity, technical competence, and life experience to make strategic decisions about their involvement in illicit activity. By observing that cyber offenders are showing a peak engagement in crime at age 35-44, one can assume that cyber offenders are capable of exercising a calculated evaluation of risks and rewards. They deliberately make decisions that afford them opportunities for profit, influence, or ideological impact, and outweigh perceived threats of detection or sanction.

Cybercrime Typologies Overall and Across Age Groups

The distribution across actors engaging in cybercrime activity by age group reveals notable variation in crime types across the lifespan.

It is noteworthy that some age groups are represented by very few cases, limiting possible interpretation. In our dataset (n=193 offenders with verified age data), the 35-44 age group accounts for 37%, followed by 25-34 years (30%), and 18-24 years (21%), together representing nearly 90% of all identified offenders. By contrast, younger (12-17 years) and older (55 years and above) groups each account for less than 5% of cases, making statistical analysis of those categories less meaningful.

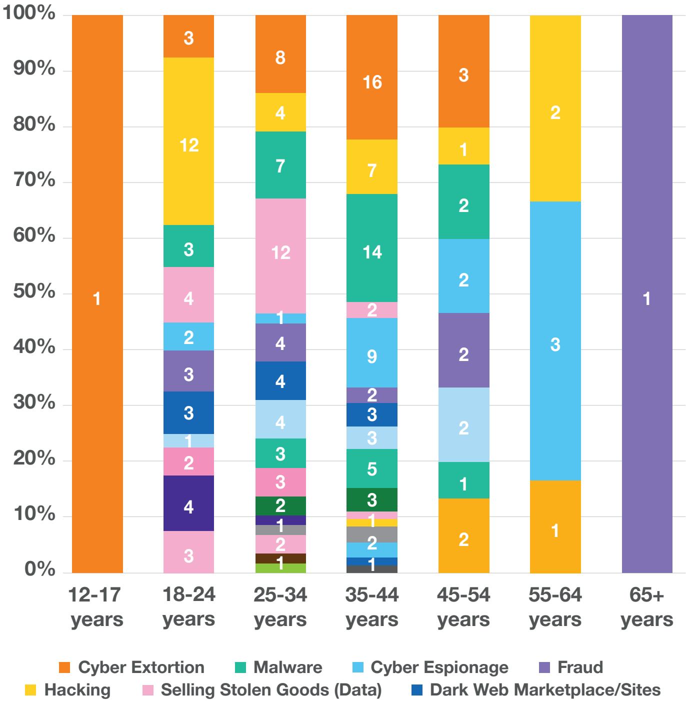
Accordingly, we will focus primarily on the three core age ranges (18-24, 25-34, and 35-44 years), where offender representation is most robust.

Among young adults (18-24 years), cyber offense appears highly diverse yet predominantly technically oriented. Hacking clearly dominates this cohort (30%), followed by Selling Stolen Goods (data) and DDoS attacks (10% each), activities that often rely on technical skill and may serve reputational or exploratory purposes rather than immediate financial gain. A secondary cluster of offenses-malware, fraud, telecom fraud, dark web marketplace activity, and cyber extortion (each 8%)-illustrates the experimental and multifaceted nature of this age group's engagement in cybercrime.

A shift becomes evident among offenders aged 25-34, where activities such as Selling Stolen Goods (Data) (21%), Cyber Extortion (14%), and Malware deployment (12%) dominate. This may indicate a move toward profit-motivated activities among actors of this age.

The trend intensifies with the 35-44 cohort, which is the largest group in this dataset showing the highest diversities of types. Within this group, Cyber Extortion (22%) is the dominant offense, followed by Malware (19%), Cyber Espionage (13%), Hacking (10%), and Money Laundering (7%). Together, these categories account for the vast majority of activities by this age group, potentially indicating a focus on high impact, financially, and politically significant actions.

Offender Age And Type of Cybercrime



Gender

The gender composition of identified offenders reveals a pronounced imbalance. Out of 280 offenders where genders were publicly shared, 255 (91%) were male, while only 25 (9%) were female. This distribution reflects a pattern commonly observed[321][322] where male offenders constitute the majority across most offense categories. Such disparity has been attributed to a combination of social, cultural, and situational factors that influence engagement in both conventional and cyber-enabled illicit activities. The findings are consistent with prior studies indicating that cyber offending, despite its technological context, continues to exhibit the gender asymmetry characteristic of broader criminal behavior trends.

Interestingly, gender distributions like this also mirror those observed within the legitimate cybersecurity workforce, where women account for only around 20-25% of professionals globally[323]. This parallel suggests that the gender imbalance in cyber offending may reflect broader structural dynamics within the digital domain itself, where access, participation, and representation remain heavily male-dominated despite growing awareness and inclusion efforts.

Nationality

The nationality of the offender was disclosed in 365 cases. The dataset contains offenders from 64 distinct nationalities, suggesting a wide geographical and cultural spread. Although nationality can provide valuable insight into the geographic and sociopolitical context of offenders, it offers only a partial view in an interconnected digital landscape.

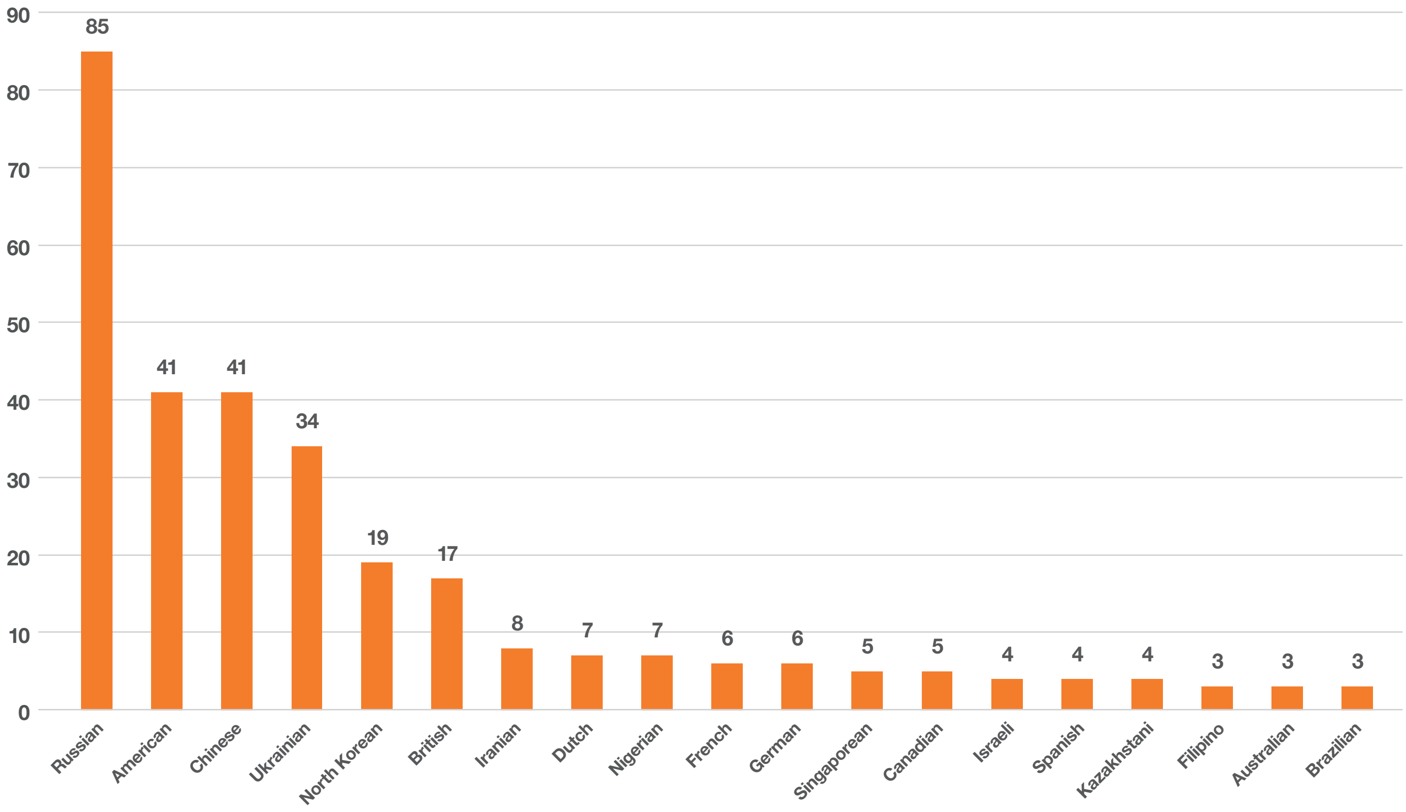
Given the transnational nature of the internet and the complex, fluid identities of actors operating across jurisdictions, nationality alone cannot reliably describe the true origin or alignment of cyber operators.

The distribution is heavily skewed toward a small number of countries. Russian nationals dominate the dataset, accounting for 85 individuals (23%), followed by American (11%), Chinese (11%), Ukrainian (9%), and North Korean (5%) offenders. Together, these five nationalities represent over half of all cases (58%). Noteworthy, one explanation for the relatively high number of American offenders could be explained by jurisdictional and reporting bias: U.S. authorities conduct and publicly disclose far more cybercrime prosecutions than most other countries, making American cases more visible in open data.

Offenders of British nationality (n=17) also represent a notable share of contributors. The involvement of Western nations shows two things: the continuous efforts and transparency they offer and at the same time that cyber operations and related offenses are not confined to states typically implicated in cybercriminal activity.

Beyond the top five, offenders represent many other nationalities including, the Dutch, French, German, Canadian, Australian, Singaporean, and more. However, we need to note that lower numerical representation does not necessarily correspond to lower levels of activity, but may instead reflect differences in detection, exposure, or attribution.

Top 20 Offender's Nationality



■ Key Takeaways

Taken together, the findings offer a dual perspective on the fight against cybercrime that examines both the offenders and the law enforcement actors working to counter them.

On the offender side, the data highlights persistent asymmetries. The overwhelming majority of identified offenders are male, reflecting trends widely observed in cybercrime research. Age data indicates that cyber offense is concentrated among adults in their mid-20s to mid-40s, with comparatively few cases involving younger or older individuals. Offense types vary across these age ranges, with younger offenders often engaged in technical and exploratory activities like hacking and DDoS attacks, while older cohorts were more frequently involved in profit-driven or complex operations such as cyber extortion, data theft, and malware deployment.

Nationality data show a strong concentration within a few groups, with Russian nationals alone accounting for nearly a quarter of cases. While nationality cannot fully describe the origins of cybercrime in an interconnected digital space, it provides useful insight into the sociopolitical and regional contexts in which offenders operate. The types of criminal acts most frequently prosecuted-such as cyber-enabled financial crime, extortion and ransomware, and unauthorized access-suggest that most cyber-criminal activities remain primarily financially motivated.

Analysis of 418 publicly reported law-enforcement actions (2021-mid-2025) shows an increasingly active and diversified global law enforcement response. The U.S. Department of Justice and FBI are the most visible, joined by leading European agencies like Europol, Germany's BKA, and authorities in the Netherlands and France. Participation from Ukraine, Russia, Australia, Singapore, Japan, and Nigeria illustrates how enforcement has become truly international. Private organizations also play a critical role: seventy-four private companies supported operations in some capacity, showing that public-private partnerships are now essential to ongoing disruption efforts.

TIBER-EU in Practice

Learnings From 16 Months of Dora Assessments

Elias Issa - Head of Red Team Operation

Introduction

A TIBER-EU exercise was performed for a European bank to assess and improve its cybersecurity posture.

The exercise was conducted over a period of 16 months, involving multiple teams, stakeholders, and complex scenarios. This article provides an overview of the exercise, its objectives, execution, key findings, and lessons learned.

TIBER-EU involves a combination of threat intelligence, ethical hacking, and organizational testing to identify vulnerabilities before malicious actors can exploit them.

Breakdown of Phases

The whole project took about 16 months and was divided into four main phases.

Key Stakeholders Involved

The exercise involved over 20 different stakeholders, each with specific responsibilities:

Tiber Cyber Team (TCT)

From the national central bank, they supervised the project and made sure everything was compliant.

White Team (WT)

The client supervisors, including key bank staff, who oversaw the exercise.

Threat Intelligence Team (TI)

Our team responsible for gathering intelligence on threat actors, analyzing their tactics, and designing realistic attack scenarios.

Red Team Provider (RT)

Our ethical hacking team tasked with executing simulated cyberattacks based on threat intelligence.

Blue Team (BT)

The bank's defense teams, both internal and external, unaware of the test until the end, to ensure authentic responses.

Phase 1: Preparation (4 months)

This phase involved close collaboration between the bank's leadership, the board of direction and regulators, to establish clear objectives, scope (flags to reach), and rules of engagement. The critical assets identified included:

- Active Directory (AD): The core system managing user identities and access rights.
- Online Banking Platform: The digital interface used by customers.
- Electronic Money Network: The infrastructure supporting money transactions.

The scope was carefully defined to avoid disrupting business operations while ensuring a realistic test. Moreover, the White Team composition was performed as well.

Phase 2: Targeted Threat Intelligence (3 months)

This phase involved the Threat Intelligence team to identify potential attack surfaces within the bank by analyzing the scoping document and the country's Generic Threat Landscape Report. Passive reconnaissance to gather publicly available information, such as leaked credentials and infrastructure details, were performed.

Based on this analysis, six tailored threat scenarios were developed. These scenarios reflect the tactics, motivations, and objectives of relevant threat actors, such as cybercriminal groups and state-sponsored entities and ensuring the attack simulations are realistic and aligned with current risks. From these scenarios, TCT and White Team selected three:

1. Ransomware group targeting Active Directory
2. Organized criminal group conducting financial fraud on online banking platforms
3. Foreign state actor APTs disrupting financial infrastructure

Phase 3: Red Team Test Phase (4 months)

Building on the threat scenarios, the Red Team developed multiple attack options for each one, based on the TTPs (Tactics, Techniques, and Procedures) of the selected threat actors.

Each scenario had three stages

- **IN:** Gaining initial access
- **THROUGH:** Moving laterally and escalating privileges
- **OUT:** Exfiltrating data or causing impact

Where appropriate, 'leg-ups' were used to simulate realistic attack progressions, with activities designed to mimic real adversaries' efforts. The approach aimed to test different layers of security controls, from perimeter defenses to internal detection mechanisms.

Throughout the simulations, our Red Team maintained stealth, closely mimicking the behavior and mindset of actual threat actors. The Blue Team's responses were continuously monitored and analyzed to identify detection gaps, procedural weaknesses, and areas for improvement. Key aspects during this phase included controlling risks, adhering to ethical principles, ensuring a realistic approach, and avoiding uncontrolled escalation to prevent any disruption to the bank's operations.

Phase 4: Closure and Analysis (2 months)

At the end, both the Red and Blue Teams wrote detailed reports about what they observed, how they responded, and their perspectives. The Blue Team's report mapped their responses against the Red Team's actions, providing valuable insights.

These reports helped understand attack paths, how well detection worked, and where responses could be improved.

A Purple Team phase played a key role here, working together to refine and create new detection rules. This process, including replay exercises and discussions, helped identify vulnerabilities, detection gaps, procedural issues, and unmonitored network areas.

Everything was compiled into a final report with a remediation plan.

Key Findings and Lessons Learned

The exercise provided valuable insights into the organization's cybersecurity, highlighting strengths and areas for improvement.

One major lesson was the importance of detection capabilities. Many alerts were delayed or missed due to incomplete logs. Most of the Red Team's activities went unnoticed by existing security tools and were only detected through manual rules, revealing gaps in automation.

We also learned that an alert was initially dismissed as a false positive by a junior analyst. However, a more experienced analyst with offensive expertise reviewed it and identified a critical vulnerability, which was part of the attack scenario. This shows the need for better training and strict procedures, including double-checking alerts. Combining the skills of analysts with offensive and defensive backgrounds is crucial to avoid missing important alerts.

During the exercise, all three main scenarios successfully achieved their objectives, demonstrating that the overall planning and execution were effective in testing the bank's resilience. However, some attack paths were detected, but this did not prevent the Red Team from reaching their goals (the "flags"). This shows that while detection works in certain areas, there is still room for improvement to cover all attack steps more effectively.

Furthermore, while treating an alert, the Blue Team said it looked like one of the threat actor we were simulating. This was particularly well received by the White Team, as it demonstrated that the Blue Team had a good understanding of the threat, and that the Red Team had effectively simulated the actor.

A significant IOC required advanced reverse engineering skills, leading to collaboration between the Blue Team and state-sponsored entities. This partnership helped analyze the threat and improve response processes, strengthening overall security.

Procedural issues, such as communication delays and information loss, made incident management more difficult. Some network segments were not monitored, highlighting the need to extend monitoring capabilities.

A key lesson was the gap between theory and reality. For example, when a workstation was isolated, the procedure was to provide a spare computer. However, in one case, no spare was available, causing delays.

Another challenge was the lack of clear ownership of security risks for critical systems, especially those managed by third parties. This can lead to overlooked vulnerabilities and hinder risk mitigation. The absence of a centralized asset database also made it harder to detect undocumented systems, slowing down incident response and increasing potential impacts.

The Blue Team also highlighted the need to improve coordination with the SOC on incident severity. It is important to clearly define and agree on what types of incidents should trigger alerts at different severity levels, to ensure the SOC responds appropriately and promptly to the most critical threats.

Finally, the Purple Team's collaboration was highly valuable. We worked on creating new, finely-tuned manual detection rules that produced no false positives, enabling reliable detection of specific stages of the attack kill chain. This ongoing cooperation demonstrated how continuous collaboration between offensive and defensive teams can significantly enhance detection capabilities and overall security posture.

Overall, regular testing, detailed reporting, and continuous improvement are vital to stay ahead of evolving threats.

Conclusion

The TIBER-EU exercise for the bank was a realistic and thorough simulation of today's cyber threats. Over 16 months, we identified key vulnerabilities, tested detection and response, and helped build a stronger cybersecurity culture.

By involving many stakeholders, using threat intelligence, and running sophisticated attack scenarios, the bank learned a lot about its resilience. The exercise met regulatory requirements under DORA and showed the bank's commitment to protecting its assets, customers, and reputation.

In a world where cyber threats keep changing, ongoing testing and improvement are crucial. The lessons from this project will help the bank stay resilient and ready for future challenges.

Electric Vehicle Charging Stations

as OT-IT Convergence Points

Thomas Zhang - Technical Delivery Manager

Imagine plugging in your EV only to unwittingly open a gateway to grid blackouts or data theft: welcome to the cybersecurity risks of charging stations, the Achilles' heel of smart cities. As operational technology (OT) converges with information technology (IT), these energy hubs become prime targets for cyber attacks. Hackers can remotely manipulate thousands of units, potentially causing urban grid collapses or mass vehicle data breaches.

This article explores this emerging risk, blending real-world events to reveal novel impacts from personal privacy erosion to national security threats. With IEA forecasting 25% EV market share in 2025, this critical topic demands urgent attention to protect the green energy future.

Charging Stations: A High-Risk OT-IT Frontier

At the core of modern EV charging stations is the seamless integration of OT and IT systems, a synergy that drives the efficiency of electric mobility while simultaneously exposing new vulnerabilities. OT refers to the hardware and software that manage physical processes, such as regulating voltage, distributing power and handling mechanical components in charging equipment. IT, on the other hand, oversees data-driven operations like user authentication, payment processing and data synchronization through cloud platforms and mobile applications.

This convergence is vividly illustrated in the IoT ecosystem of EV charging. IoT's role in EV infrastructure highlights the service as the connective tissue between OT and IT, facilitating real-time data exchange for advanced features like dynamic pricing, load balancing and vehicle-to-grid (V2G) communication. For example, a charging station might employ OT to deliver up to 350 kW of power while IT simultaneously transmits usage data to a central server for billing and analysis.

Yet, this integration forms a cyber-physical system where a compromise in one area can ripple into the other. Attackers could exploit known vulnerabilities in outdated software within connected apps, seizing control of OT functions and potentially bypass safety mechanisms and causing tangible harm. Drawing from expertise in industrial control systems, EV stations resemble miniaturized power substations, much like those in refineries or utilities. However, unlike these heavily secured sites, public chargers are often deployed in accessible urban settings. This makes them comparable to unsecured IoT devices dispersed across cities.

The scale of this infrastructure increases the stakes. As of mid-2025, the number of global public EV charging points had increased by 12% since 2024. This rapid expansion is being fueled by the expected sale of over 20 million EVs this year[324], resulting in the emergence of exploitable gaps.

Emerging Cybersecurity Risks: A Multifaceted Threat Landscape

The cybersecurity risks at OT-IT convergence points in EV charging span a broad spectrum, from data interception to large scale disruptions. Threats can be categorizes into these key areas:: communication protocols, supply chain and physical access points. Communication protocols, particularly the Open Charge Point Protocol (OCPP), are a frequent weak link. In 2024, researchers identified multiple zero-day vulnerabilities in OCPP[325], enabling unauthorized access to charging management systems. Such flaws could allow attackers to halt charging sessions, manipulate billing, or deploy malware to connected vehicles. For instance, CVE-2024-25998[326] exemplifies an unauthenticated command injection vulnerability in devices like the Phoenix Contact CHARX SEC-3100. This flaw arises from improper input validation in the OCPP service, particularly during the handling of Update Firmware messages. An attacker can craft a malicious payload that injects arbitrary commands into the system's shell, potentially executing code with limited privileges. This often involves exploiting unescaped user inputs in protocol fields, such as file paths or parameters in the firmware update process. This leads to modifications in runtime configurations or even persistent changes to system files like those in the /etc or /var directories. In practice, patching requires rigorous sanitization of all incoming OCPP messages and implementing strict allowlisting for command parameters to prevent such injections.

Supply chain vulnerabilities further complicate the picture, as charging hardware often relies on components from a global network of suppliers, creating opportunities for embedded malware or backdoors. This risk is heightened by the modular nature of EV chargers, where third-party firmware, chips, or software libraries can be compromised during manufacturing or distribution. For example, attackers might insert malicious code into bootloader firmware or communication modules, turning stations into persistent threats capable of exfiltrating data or awaiting activation for coordinated attacks. Unverified supply chain elements, like off-the-shelf microcontrollers from unvetted vendors, can introduce flaws similar to those in broader attacks, such as the SolarWinds incident[327] adapted to EV ecosystems. A single tainted component could propagate malware across fleets and bypass initial security scans and enable remote control over power delivery or data flows.

Physical tampering issues add layers of complexity. Hardware implantation and firmware tampering allow malicious actors to physically interface with devices, inject malware, or alter code to gain persistent control over the system. For example, attackers can implant keyloggers or small wireless transmitters (like cellular modules or Bluetooth devices) into charging station interfaces. Public USB ports at chargers were already flagged by the FBI in 2023 for malware risks and persist as entry points[328].

Real-World Incidents: Lessons From the Frontlines

Real-world examples bring these risks into sharp focus, demonstrating how theoretical vulnerabilities translate into practical disruptions. In 2023, researchers demonstrated the BrokenWire attack[329], which enables hackers to wirelessly disrupt the Combined Charging System (CCS) used in EV charging. They may induce electromagnetic interference on the control pilot signal, causing ongoing charging sessions to abort abruptly and potentially stranding vehicles mid-process. More recently, there were at least 30 major publicly reported cyberattacks on the automotive industry in 2024, including one specifically targeting EV charging infrastructure in Lithuania[330], according to the research.

At the Black Hat USA conference in 2025, a demonstration showcased how EV charger vulnerabilities could cause cable overheating, raising fire hazards, as covered in Vicone's blog[331]. Similarly, a March 2025 Nature article proposed detection methods for attacks on Electric Vehicle Supply Equipment (EVSE)[332] after simulations revealed malware propagation from chargers to vehicles.

An additional perspective comes from data privacy concerns.. Compared to traditional IT services, EV charging stations often require a broader range of vehicle-related data, such as vehicle identification numbers (VINs), geographic locations and charging histories. This can heighten public concerns over increased data exposure and privacy risks.

For instance, Digital Charging Solutions experienced a data breach in 2025[333], compromising customer information, although the company claimed that only a limited set of names and email addresses were affected. This event shows that cyber attacks targeting critical energy and mobility systems are not only escalating in frequency but also in potential impact..

Impacts: From Personal Privacy to National Security

The consequences of these risks extend far beyond immediate technical failures, affecting individuals, economies and wider societies. On a personal scale, data breaches undermine privacy by allowing attackers to harvest location data from charging apps to enable tracking, stalking, or identity theft.

Economically, outages can cripple operations for fleets and businesses. A widespread disruption could strand commuters and disrupt supply chains, incurring billions in losses. For smart cities embracing EVs as cornerstones of sustainable transport, such vulnerabilities could erode public trust and slow the transition to green energy.

At the national level, grid attacks represent significant security threats. In regions with low-inertia grids dominated by renewables, manipulated chargers might induce instability. Geopolitically, adversaries could exploit EV infrastructure to sabotage economies, like past pipeline hacks.

Mitigation Strategies: Best Practices Should Be Followed

Addressing these challenges demands a multifaceted strategy, starting with foundational security measures. Key best practices include:

Identity Authentication

Implement multi-factor authentication (MFA) and single sign-on (SSO) to verify users, vehicles and backend systems, using digital certificates for secure plug-and-charge. This prevents unauthorized access and mitigates weak credential risks in IT-OT environments.

SOC Monitoring

Deploy security operations centers with real-time monitoring tools to identify unusual patterns like traffic spikes or unauthorized connections. Integrate intrusion detection systems (IDS) and security information and event management (SIEM) for proactive threat response in charging networks.

Vulnerability Management

Embed security requirements into the design during development by adhering to standards like ISO/SAE 21434[334]. In operations, conduct regular assessments and establish coordinated disclosure mechanisms with suppliers, including timely firmware updates to address exploits in EV chargers and software.

Physical Security

Use lock, video surveillance and access audit at sites to prevent tampering exposing network interfaces. Combine with endpoint protection against blended attacks, following public EV station guidelines for resilience.

Future Outlook: Securing the Green Horizon

Looking ahead, the IEA projects 150 million new charging points by 2030[335], necessitating scalable security innovations. Emerging technologies like post-quantum cryptography and blockchain for V2G transactions could transform defenses, offering robust protection against sophisticated attacks.

There are still challenges to overcome, such as balancing user convenience with stringent security, mitigating supply chain risks and harmonizing global standards. However, by learning from past incidents and embedding proactive measures, the industry can turn these convergence points from liabilities into strengths.

In essence, EV charging stations embody the dual nature of progress: promise intertwined with peril. Through vigilant innovation and cross-sector collaboration, we can fortify this infrastructure, paving the way for a secure and sustainable electric future.

Strategies and Challenges for

Post-Quantum Migration

Mohammed Meziani - Senior IT Security Consultant

Quantum Waiting Game: "Steal It Today, Break It in a Decade"

Cryptography is the backbone of digital trust, but the looming era of quantum computing threatens its foundations.

Harnessing quantum physics, future quantum machines will effortlessly break the mathematical encryption schemes that protect data today. Though current prototypes[336] are not quite there yet because they fundamentally lack the scale and error-correction capability required to successfully execute complex quantum algorithms. However, the prospect of a mature, cryptographically relevant quantum computer (CRQC) is alarming. Such a machine could potentially break modern encryption in a matter of minutes, likely by 2030 to 2035.

To combat the looming quantum computing threat, our cryptography must evolve immediately. This is why Post-Quantum Cryptography (PQC)[337] is being introduced as a solution. PQC provides new cryptographic algorithms designed to withstand attacks from both today's classical computers and future quantum machines.

Furthermore, patient adversaries are employing a "Harvest Now, Decrypt Later" (HNDL) strategy. They are quietly accumulating encrypted data with the intention of decrypting it later using quantum computers. Any data requiring long-term security, such as trade secrets or classified designs, is vulnerable because its lifespan will inevitably outlive its current encryption. Therefore, it is crucial that organizations must begin planning their PQC migration now, ensuring that data encrypted today remains secure against future quantum-enabled decryption attacks.

A Step-By-Step Guide To Future-Proofing With PQC

PQC migration is a complex process that spans the entire organization and potentially reaches deep into its security architecture. This massive transition is complicated by the current state of industry planning. There is still a lack of consensus in technical literature regarding common steps or uniform terminology for migration strategies. Without a common language, companies find it difficult to effectively compare, adopt, or coordinate the most suitable migration strategies.

Our research concludes that the following strategy offers an effective, universal framework that can be adapted to suit any organization [338] [339] [340] [341] [342] [343] [344].

At this stage, it is important to emphasize that a migration team must be established for each migration. This team should consist of cryptography and cyber security experts and managers from the software system or infrastructure being migrated. The team will drive the migration process forward and ensure its completion.

Step 1 (Preparation)

This phase establishes the scope and leadership for the PQC migration process. Key activities include assessing the relevance and urgency of PQC, appointing a program lead, aligning stakeholders on clear goals, and initiating conversations with vendors to determine migration needs.

Step 2 (Diagnosis)

This phase involves a thorough evaluation of the current cybersecurity posture to establish a comprehensive security baseline. Key activities include documenting all cryptographic assets, categorizing data based on their confidential lifespan, identifying suppliers of cryptographic tools to evaluate their PQC readiness, and conducting a formal risk assessment to generate a prioritized asset list based on principles such as Mosca's theorem[345].

Step 3 (Planning)

Once the urgency and scope are determined, this phase focuses on the "how" and "when". It focuses on the migration strategy, creating a comprehensive business and technical plan and timeline based on the urgency and scope determined in previous steps. Key activities involve appointing a dedicated migration manager to oversee the process and conducting a comprehensive cost estimate for the entire migration.

Step 4 (Execution)

This critical phase involves executing the plan to establish a quantum-safe environment through careful technical implementation. Key activities include maintaining backward compatibility via a hybrid cryptographic approach, implementing recommended PQC primitives for key exchange and signatures, adjusting key sizes, and integrating cryptographic agility to ensure rapid adaptation with minimal service disruption.

Step 5 (Continuous Monitoring and Update)

This final phase focuses on continuous vigilance after migration, recognizing the dynamic cryptographic landscape. Key activities include routinely reviewing and updating the cryptographic inventory, conducting regular reviews of emerging threats to PQC schemes, performing proactive security audits and vulnerability assessments, and staying updated on the latest PQC advances to ensure timely system and software updates.

Addressing Key Challenges: A Practical Checklist

To ensure a successful PQC migration, organizations must proactively identify and mitigate key obstacles that could hinder progress. They must recognize that the transition involves navigating three interdependent categories of challenges.

Organizational Challenges

These non-technical obstacles relate to people, strategic planning, internal governance, and coordination across the wider ecosystem, often complicated by a lack of urgency or qualified personnel.

PQC Challenges

These stem directly from the immaturity of the new technology. Although we now have initial standards, such as ML-KEM and its implementation in protocols like TLS, a lack of standardization for a complete suite of algorithms and uncertainty in selecting and testing reliable PQC solutions remain major hurdles. The main issue is the lack of specific implementation guidelines, such as how to effectively deploy hybridization or agility mechanisms.

Code and Documentation Challenges

These are technical hurdles caused by the inherent rigidity of existing IT infrastructure (legacy systems), the need for extensive code modification, and the complexity of implementing secure cryptographic changes.

The following breaks down the major obstacles to a successful PQC migration and offers solutions for each. Each obstacle falls under one of the previously established challenge categories. See references [347] and [348] for a more comprehensive discussion of additional obstacles.

Lack of Urgency and Business Case (Organizational)

- **Problem:** The quantum threat seems distant, making it challenging to establish the sense of urgency and budget approval from leadership.
- **Solution:** Organizations can use tools like Mosca's Theorem[346] to quantify their vulnerability and take inventory of cryptographic assets to improve current cybersecurity regardless of the quantum timeline.

Internal Knowledge and Skills Deficit (Organizational)

- **Problem:** Lack of internal knowledge about quantum-based threats, and shortage of qualified personnel to implement new PQC solutions.
- **Solution:** Launch training initiatives for IT and management. Engage external PQC consultants to design the strategy and knowledge transfer.

Internal Governance and Planning (Organizational)

- **Problem:** Absence of PQC governance and a fully articulated transition plan, leading to ineffective task prioritization and operational inefficiencies.
- **Solution:** Appoint a PQC migration manager or steering committee to mandate a cryptographic inventory for risk-based migration prioritization.

Ecosystem and Coordination Failures (Organizational)

- Problem: Lack of ecosystem engagement, unclear governance, and limited collaboration hamper the PQC transition.
- Solution: Proactively manage vendor relationships and join industry forums to share knowledge, collaborate, and influence standards development.

Regulatory Voids (Organizational):

- **Problem:** Existing regulations (e.g. NIS2 and DORA) mandate the use of state-of-the-art cryptography while new PQC-specific laws are pending.
- **Solution:** Adopt recent PQC standards proactively for critical systems to meet the "state-of-the-art" requirement. Leverage EUCC certification and monitor ETSI/OpenSSL for implementation guidance.

Uncertain Selection Criteria (PQC):

- **Problem:** Organizations struggle to decide between an all-at-once or phased hybrid approach to replacing PQC, as they lack clear criteria.
- **Solution:** Default to a hybrid PQC model to gain operational knowledge, and minimize complications before committing to a full replacement strategy.

Security and Reliability Concerns (PQC):

- **Problem:** Uncertainty about the maturity and security of PQC algorithms, organizations must balance present-day protection and future resilience.
- **Solution:** Use a hybrid PQC approach with a staged rollout. Begin with non-critical areas before expanding to ensure the solution is stable and reliable.

Rigidity of Legacy Systems (Code and Documentation):

- **Problem:** Legacy systems inflexibility. This is exacerbated in resource-constrained devices, e.g. IoT and smart cards, which lack the memory and power necessary for larger PQC keys and intense computations.
- **Solution:** Replace hardware to accommodate PQC demands. If this is not feasible, implement lightweight, optimized PQC libraries.

Ecosystem Interdependency (Code and Documentation):

- **Problem:** The interconnected nature of the Public Key Infrastructure (PKI) means that a PQC transition affects all involved parties, including standards bodies, hardware/software vendors, and certificate authorities (CAs).
- **Solution:** Collaborate with suppliers and CAs, participate in industry and regulatory groups (e.g., NIST, CISA, ENISA, ETSI, ANSSI, NCSC and BSI), and map all third-party component dependencies.

Lack of Certified and Approved Components (Code and Documentation):

- **Problem:** Limited availability of certified components (eg HSMs) from vendors, especially in regulated sectors such as finance and government.
- **Solution:** During procurement, organizations must mandate FIPS 140-3 or EUCC validation for PQC-capable hardware, while beginning software-level migration (e.g., TLS/SSH) in parallel.

Lack of Agility (Code and Documentation):

- **Problem:** Current systems are cryptographically inflexible requiring adaptation to new threats or evolving standards slow and complex due to the need for intricate code changes.
- **Solution:** Prioritize cryptographic agility by designing new systems that allow for algorithm swapping via simple configuration and centralized key and certificate support.

Key Takeaways

Urgency of Migration: Act immediately! The deadline is now. The time for waiting for CRQC is over. Organizations must start preparing and migrating their data immediately to ensure its long-term security.

Establish Foundational Priorities: Strategic efforts must focus on developing a clear, actionable strategy for planning and executing the PQC transition smoothly.

Foster United Collaboration: The PQC transition demands a unified effort to address the collective security challenge. This requires actively sharing lessons learned and collaborating across industries, governments, and academia.

Embed Hybrid Cryptography and Cryptographic Agility: The ability to rapidly and seamlessly combine, modify or swap cryptographic primitives must be adopted as the cornerstone of the new security posture to adapt to future advances in quantum-safe standards.

Acknowledge Interdependent Challenges: The success of any PQC migration hinges on recognizing that the transition involves navigating several interdependent categories of challenges.

Security Predictions

- **Tatiana Chamis-Brown** - SVP Global Strategic Marketing
- **Vivien Mura** - Global CTO

Cyber Attacks Become a Mainstream Disruption to Daily Life

For many people outside of the cyber security industry, cyber attacks may still be an abstract concept, and a far-away event to their daily lives. But what we have seen this year is a much wider impact of cyber attacks, disrupting the daily routines of millions at once. In 2025 alone, we have seen several instances of collective impact.

In March 2025, a third-party provider managing an IT platform for multiple Italian transport companies suffered a data breach which subsequently led to ticketing systems being paralysed for two days, impacting several thousand commuters.

Multiple UK retailers were hit by cyber attacks In April, May and June that incapacitated their ecommerce and payments processing systems. Some had to suspend online orders and accepting contactless payments in their stores for 46 days.

Travellers at London, Brussels and Berlin airports suffered delays, queues and cancelled flights in September due to an attack on an airport supplier which disrupted check-in and boarding systems. The disruption lasted days, with over 160 flights cancelled. With back-up and recovery systems lacking, one airport resorted to pen and paper at check-in.

We expect recent cases of sector-wise impacts, especially those driven by vulnerabilities in industry-specific software, will drive an increased focus on third-party risk management. Adoption of risk quantification approaches overlayed with traditional assessments will enable more effective prioritization and acceleration of critical security investments.

We also expect further focus on other supply chain risks with the introduction of the Cyber Resilience Act (CRA) in 2027. This will impose security requirements for digital products and services, aimed at reducing systemic vulnerabilities by embedding security-by-design practices and formalizing vulnerability disclosure obligations.

A Multifaceted Threat

An increasingly violent multifaceted threat, with an increased risk of severe attacks in Europe in 2026.

Cyber threats are becoming more multifaceted, exploiting vulnerabilities arising from new digital practices, taking advantage of the fragility of small businesses, and combining reputation attacks with cyber assaults: all executed with increasing speed. This trend is likely to intensify. Cybercriminal organizations will continue to evolve to maintain resilience, maximize profits, and industrialize their attack methods through "as-a-service" models. Consequently, small and medium-sized businesses, local authorities, and associations are expected to see a rise in extortion cases.

Escalating international tensions are creating conditions for an increase in espionage, sabotage, and destabilization attacks. Democratic processes such as presidential elections in Europe could serve as opportunities for a rise in information manipulation.

Furthermore, we can anticipate an increase of cyberattacks targeting critical infrastructure systems such as telecommunications, transportation, and energy supply. Past incidents, like geographically lateralized supply chain attacks (e.g., NotPetya), could recur and state attackers will likely continue to target perimeter-security companies to increase their intrusion opportunities. Additionally, with the evolution of mobile networks and the convergence of IT and OT environments combined with the increasing robotization of industry, there is a growing risk of targeting physical systems for ideological reasons, including industrial connected objects.

Automation Is at the Heart

In the coming years, automation will be at the heart of the evolution of our digital society and will increase risks but also provide opportunities to better protect. The balance will be the main indicator of cybersecurity success.

The trend toward using AI agents to enhance automation within companies and digital life was confirmed in 2025. Despite ongoing uncertainties regarding profitability, this trend is expected to continue, with significant implications for skills retention and employees' ability to effectively utilize these new technologies to maintain competitiveness. Indeed, in addition to the possibilities offered by LLMs for processing information, AI will gradually allow anyone to automate most repetitive tasks with a minimum of human-machine interfaces and without technical expertise.

What we are experiencing is not just a technological shift but also a psychological and societal one: humans may gradually accept AI to perform tasks traditionally carried out by people, such as payments, personal data management, sensitive operations on production lines, and physical system control. Recent advances, particularly in reducing AI hallucinations, facilitate the transfer of control from humans to machines.

As a result, we must anticipate increased interest from attackers in exploiting vulnerabilities within AI systems, at the application level or in the AI model itself, either to access information or to carry out unauthorized actions. Fortunately, technical and technological solutions already exist, and cybersecurity is benefiting from similar progress. Automated execution of complex investigative or corrective actions, requiring high privileges (administration practices, vulnerability remediation, active threat hunting, mitigation), may become more widespread.

The challenge will be to strike a balance between allowing human expertise to verify and approve these actions and ensuring maximum responsiveness, especially as vulnerability exploitation accelerates. We can expect the average time between discovering a critical vulnerability and its exploitation to continue decreasing, with new records likely in the coming months. The implementation of the Cyber Resilience Act in Europe will help better manage risks associated with digital product vulnerabilities on the market.

Generative AI as Target and Threat

Feared in 2025, the risks linked to the accessibility and deployment of generative and agentic AI will materialize more clearly in 2026.

In 2025, cybersecurity experts revealed new offensive uses of AI, notably the use of generative AI to create deployable ransomware scripts that are difficult to detect. By 2026, we can expect to see an increase in such exploits, aiming to automate entire kill chains, leveraging vulnerabilities exploitation and unscripted attack paths.

Moreover, the performance of generative AI models accessible online is likely to enhance fraud and social engineering techniques, such as deepfakes or deep voice impersonations.

More generally, attackers of all levels will necessarily have gained skills in the use of AI, which will have consequences on the speed of execution of attacks but also on the volume of sophisticated attacks. We anticipate a drastic increase in disinformation and reputational attacks, made possible by the accessibility of high-performance AI-powered content generation solutions and by anonymization and dissemination methods borrowed from the cyber domain (bots, impersonations, etc.). This major phenomenon in our society raises the question of an evolution of European cybersecurity doctrine to better combat the hybrid nature of attacks in the cyberspace.

Innovation for Good and Bad

CISOs will have to make choices in the face of complexity: new paradigms, cooperation and planning are the clues.

In this context, the responsibility of cybersecurity actors to ensure a trustworthy society will continue to grow. Particularly in Europe, private sector players, institutions, and cybersecurity authorities across member states will need to collaborate more closely to face increasingly complex and aggressive threats. The Cyber Solidarity Act has laid the groundwork for such cooperation, but it remains the responsibility of stakeholders to unite. European nations will also need to look into new cyber defense doctrine that accounts for the hybrid nature of modern threats.

CISOs will have to manage increasing complexity with tighter budgets but more regulatory leverage and technological solutions. On a strategic level, meeting regulatory requirements and addressing threats on a constant budget will require aligning compliance and risk management objectives, and planning operations. On a technical level, automating defense mechanisms (such as vulnerability discovery and incident response), behavioral detection, supply chain monitoring, and crisis preparedness are essential strategies. Additionally, cyber partners will likely interface their AI systems to enable real-time cooperation. Innovation will remain a key pillar in countering the creativity of attackers.

Increased accountability As Breaches Lead to CEO Pay Cuts

Boards are tightening up accountability from Executives overseeing organizations that suffered breaches. CISOs and CIOs are no longer alone in facing the legal, reputational and financial accountability for cyber incidents.

Following the recent example from Quantas Airways-whose CEO and team had their bonus decreased as a penalty for the incident that breached the personal data of millions of customers- we believe Executive penalties will become an increased common practice. This, accelerated by regulatory and investor scrutiny, will ultimately drive greater Executive engagement and sponsorship of organizations' cyber security programs and investments.

The feedback from our customer CISOs also echoes that Boards have rapidly matured in their knowledge and governance of cyber risks. Boards are increasingly expecting CISOs to advise on corporate cyber risk on a recurrent basis, and to share relevant cyber threat intelligence and advisory specific to their organization and industry vertical.

They are proactively questioning the security of new technology adoption, the cyber security implication of geopolitical dynamics and the impacts of regulations across the geographies where the organization operates. They want to ensure they have the insight and knowledge to effectively perform their role in the oversight of corporate security programs and investments. We expect Board cyber maturity to continue to continue improve over the coming years, enabling more effective governance of organizational cyber risks.

What Have We Learned?

How to summarize another hectic year? In 2025, three key phenomena stand out: attackers weaponized AI, vulnerabilities were exploited at record speed, and Europe moved to the center of the cyber chessboard. Here's what changed—and why it matters to security leaders and practitioners.

AI, a Triple-Edged Sword

In 2025, AI has extended its reach in the cyber space.

Threat groups —criminal and state-backed— adopted AI into their tactics, techniques, and procedures (TTPs). Phishing is now fluent and error free. Malware development sped up, with examples like Chinese actor UTA0388 using AI to develop the GOVERSHELL malware. Social engineering traps grew more convincing as AI-powered impersonation tools became accessible to all.

AI isn't just a weapon—it's also a new attack surface which organizations need to protect with security for AI solutions. Over the summer, the "Drift" AI module linked to Salesloft was compromised. This resulted in the theft of Salesforce data from several hundred organizations—including multiple security vendors, leading to a supply chain attack.

In response, defenders have stepped up their game. A new wave of AI-first security tools has entered the market— intelligent triage that deduplicates and filters noisy tickets; analyst copilots that summarize logs, suggest queries, and draft playbooks; phishing/brand abuse detection across text, images, and URLs. The result: fewer false positives, faster investigations, clearer, auditable actions—while humans still approve high impact steps.

Vulnerability Exploits Landed Faster and Broader

Cybercriminals are exploiting vulnerabilities at an unprecedented pace. The urgency to patch and manage vulnerabilities has never been greater. Throughout 2025, widely exploited flaws in Microsoft SharePoint, Oracle E-Business Suite, Ivanti, and F5 devices underscored that vulnerabilities remain a primary entry point for intruders.

A notable example is the Salt Typhoon cyber-espionage campaign targeting several telecom providers. The group allegedly leveraged unpatched network device vulnerabilities to maintain long term access, evading detection with traffic obfuscation, using covert channels, and log manipulation. The broader geopolitical backdrop included state sponsored espionage against U.S. targets – up to high profile individuals such as the U.S. Presidential candidates - aimed at intelligence gathering and asserting technological dominance in an international power struggle.

This relentless pace of exploitation emphasizes the importance of continuous monitoring, rapid patching, and a proactive vulnerability management strategy, as provided through Continuous Threat Exposure Management (CTEM) services. In a landscape where attackers are increasingly precise and swift, organizations must stay vigilant to prevent breaches.

Europe in the Crosshairs: Building Autonomy

Europe remains a fertile ground for cyber activity. It is both a prime target for state-sponsored actors and cybercriminals, and a region where hacktivist groups are particularly active. Russian aligned group NoName057(16) continued daily DDoS cyberattacks against European NATO aligned countries. A stark warning came from Norway: authorities attributed a dam breach to Russia, where adversaries seized control and caused water to flow undetected for four hours—a wake-up call highlighting the urgent need for Europeans to bolster the defense of their critical infrastructure. Meanwhile, reports suggest North Korean cyber operatives pretending to be remote IT workers are shifting focus from U.S. targets to European organizations, likely in response to increased U.S. countermeasures.

Against this backdrop, Europe must prioritize the development of independent technology capabilities to safeguard its digital future. Recent signals and policy shifts have raised concerns about the stability and robustness of relying on foreign technology. Beyond policy signals, concrete steps include the EU Vulnerability Database (EUVD), which consolidates a list of vulnerabilities with unique identifiers in real time. It is intended to reduce dependency on the U.S. based CVE database by MITRE —whose funding was jeopardized during the early days of the new U.S. government administration.

Building on this momentum, Europe should continue to expand and strengthen its security capabilities, fostering innovation and collaboration across member states to build a resilient and autonomous digital ecosystem.

Sara Puigvert

Executive Vice President Global Operations
Orange Cyberdefense

Sources

[1] https://en.wikipedia.org/wiki/Night_Dragon_Operation

[2] https://www.justice.gov/archives/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical

[3] https://www.reuters.com/technology/cybersecurity/us-adds-9th-telcom-list-companies-hacked-by-chinese-backed-salt-typhoon-2024-12-27/

[4] https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

[5] https://www.nextgov.com/cybersecurity/2025/08/salt-typhoon-hackers-targeted-over-80-countries-fbi-says/407719/

[6] https://www.secpod.com/blog/stealth-in-the-storm-breaking-down-salt-typhoons-global-cyber-campaign

[7] https://media.defense.gov/2025/Aug/22/2003786665/-1/-1/0/CSA_COUNTERING_CHINA_STATE_ACTORS_COMPROMISE_OF_NETWORKS.PDF

[8] https://media.defense.gov/2025/Aug/22/2003786665/-1/-1/0/CSA_COUNTERING_CHINA_STATE_ACTORS_COMPROMISE_OF_NETWORKS.PDF

[9] https://www.atlanticcouncil.org/content-series/cybersecurity-policy-and-strategy/the-eight-body-problem-exploring-the-implications-of-salt-typhoon

[10] https://attack.mitre.org/groups/G1045/

[11] https://www.belfercenter.org/publication/national-cyber-power-index-2022

[12] https://www.belfercenter.org/publication/national-cyber-power-index-2022

[13] https://docs.google.com/document/d/1gk1fDLKrN3m5jOSk7QbpGL1SBcLvrm0FTN3H-5ZJZcY/

[14] https://warontherocks.com/2025/10/the-things-that-bedevil-u-s-cyber-power/

[15] https://www.bleepingcomputer.com/news/security/cisa-urges-switch-to-signal-like-encrypted-messaging-apps-after-telecom-hacks/

[16] https://en.wikipedia.org/wiki/Regulation_to_Prevent_and_Combat_Child_Sexual_Abuse

[17] https://www.opendemocracy.net/en/digitaliberties/online-safety-act-bill-uk-government-encryption-privacy-ofcom/

[18] https://arxiv.org/html/2509.10540

[19] https://engineering.nyu.edu/news/large-language-models-can-execute-complete-ransomware-attacks-autonomously-nyu-tandon-research

[20] https://openai.com/global-affairs/disrupting-malicious-uses-of-ai-october-2025/

[21] https://openai.com/global-affairs/an-update-on-disrupting-deceptive-uses-of-ai/

[22] https://www.wheresyoured.at/costs/

[23] https://www.anthropic.com/news/disrupting-AI-espionage

[24] https://rdi.berkeley.edu/frontier-ai-impact-on-cybersecurity/

[25] https://time.com/7321098/ai-2026-midterm-elections/

[26] https://openai.com/global-affairs/an-update-on-disrupting-deceptive-uses-of-ai

[27] https://www.trellix.com/blogs/research/analysis-of-black-basta-ransomware-chat-leaks

[28] https://engineering.nyu.edu/news/large-language-models-can-execute-complete-ransomware-attacks-autonomously-nyu-tandon-research

[29] https://www.aim.security/post/when-public-prompts-turn-into-local-shells-rce-in-cursor-via-mcp-auto-start

[30] https://www.schneier.com/blog/archives/2025/10/agentic-ais-ooda-loop-problem.html

[31] https://www.theverge.com/report/810083/ai-browser-cybersecurity-problems

[32] https://cybersecuritynews.com/salesloft-drift-data-breaches

[33] https://openai.com/index/introducing-aardvark

[34] https://www.forbes.com/councils/forbestechcouncil/2025/08/28/why-llms-arent-ready-for-predicting-vulnerability-exploitation/

[35] https://www.wheresyoured.at/costs/

[36] https://warontherocks.com/2025/10/silicon-statecraft-how-u-s-gulf-ai-deals-project-power

[37] https://danielmiessler.com/blog/will-ai-help-moreattackers-defenders

[38] https://www.reuters.com/technology/norway-spy-chief-blames-russian-hackers-dam-sabotage-april-2025-08-13/

[39] https://www.theguardian.com/technology/2025/may/07/pro-russian-hackers-claim-to-have-targeted-several-uk-websites

[40] https://www.reuters.com/world/middle-east/suspected-israeli-hackers-claim-destroy-data-irans-bank-sepah-2025-06-17/

[41] https://www.europol.europa.eu/media-press/newsroom/news/global-operation-targets-noname05716-pro-russian-cybercrime-network

[42] https://www.cyber.gc.ca/en/alerts-advisories/al25-016-internet-accessible-industrial-control-systems-ics-abused-hacktivists

[43] https://www.thehackacademy.com/news/pro-russian-hacktivists-launch-ddos-blitz-on-uk-councils-and-agencies-but-impact-remains-limited/

[44] https://www.bleepingcomputer.com/news/security/pro-russian-hackers-blamed-for-water-dam-sabotage-in-norway/

[45] https://www.forescout.com/blog/anatomy-of-a-hacktivist-attack-russian-aligned-group-targets-otics/

[46] https://www.cyber.gc.ca/en/alerts-advisories/al25-016-internet-accessible-industrial-control-systems-ics-abused-hacktivists

[47] https://www.cyber.gc.ca/en/alerts-advisories/al25-016-internet-accessible-industrial-control-systems-ics-abused-hacktivists

[48] https://www.europol.europa.eu/media-press/newsroom/news/global-operation-targets-noname05716-pro-russian-cybercrime-network

[49] https://www.recordedfuture.com/research/anatomy-of-ddosia

[50] https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

[51] https://www.fortinet.com/resources/cyberglossary/solarwinds-cyber-attack

[52] https://krebsonsecurity.com/2025/07/microsoft-fix-targets-attacks-on-sharepoint-zero-day/

[53] https://cloud.google.com/blog/topics/threat-intelligence/data-theft-salesforce-instances-via-salesloft-drift

[54] https://trust.salesloft.com/?uid=Drift/Salesforce+Security+Notification

[55] https://www.wiz.io/blog/shai-hulud-npm-supply-chain-attack

[56] https://www.cisa.gov/news-events/alerts/2025/09/23/widespread-supply-chain-compromise-impacting-npm-ecosystem

[57] https://www.koi.ai/blog/glassworm-first-self-propagating-worm-using-invisible-code-hits-openvsx-marketplace

[58] https://my.f5.com/manage/s/article/K000154696

[59] https://www.reuters.com/legal/government/us-sec-solarwinds-reach-preliminary-deal-end-breach-lawsuit-2025-07-02/

[60] https://www.bleepingcomputer.com/news/security/Cl0p-ransomware-claims-responsibility-for-cleo-data-theft-attacks/

[61] https://www.aikido.dev/blog/s1ngularity-nx-attackers-strike-again

[62] https://www.cisa.gov/news-events/alerts/2025/09/23/widespread-supply-chain-compromise-impacting-npm-ecosystem

[63] https://thehackernews.com/2025/08/salesloft-oauth-breach-via-drift-ai.html

[64] https://www.linkedin.com/pulse/your-third-partys-breach-costs-much-own-cyentia-institute-zuyhf

[65] https://www.ncsc.gov.uk/pdfs/blog-post/sausages-incentives-rewarding-resilient-technology-future.pdf

[66] https://www.reuters.com/business/media-telecom/us-company-with-access-biggest-telecom-firms-uncovers-breach-by-nation-state-2025-10-29

[67] https://dataconnect.co.uk/resources/insights/cyber-essentials-scheme/how-st-jamess-place-used-cyber-essentials-to-dramatically-reduce-supply-chain-risks/

[68] https://www.justice.gov/archives/opa/pr/justice-department-announces-arrest-premises-search-and-seizures-multiple-website-domains

[69] https://www.gov.uk/government/publications/north-korean-it-workers-advisory-signs-to-watch-for

[70] https://www.justice.gov/opa/pr/fourteen-north-korean-nationals-indicted-carrying-out-multi-year-fraudulent-information

[71] https://cloud.google.com/blog/topics/threat-intelligence/dprk-it-workers-expanding-scope-scale/

[72] https://www.justice.gov/opa/pr/justice-department-announces-coordinated-nationwide-actions-combat-north-korean-remote

[73] https://www.justice.gov/opa/pr/arizona-woman-sentenced-17m-information-technology-worker-fraud-scheme-generated-revenue

[74] https://blog.knowbe4.com/how-a-north-korean-fake-it-worker-tried-to-infiltrate-us

[75] https://cybersecuritynews.com/u-s-doj-announces-nationwide-actions/

[76] https://home.treasury.gov/news/press-releases/sb0205

[77] https://www.fbi.gov/wanted/cyber/dprk-it-workers

[78] https://www.okta.com/en-se/newsroom/articles/north-korea-s-it-workers-expand-beyond-us-big-tech

[79] https://www.reuters.com/legal/government/doj-announces-arrest-indictments-north-korean-it-worker-scheme-2025-06-30/

[80] https://www.bbc.com/news/articles/ce8vedz4yk7o

[81] https://www.bbc.com/news/articles/c15wk77zxngo

[82] https://www.justice.gov/opa/pr/arizona-woman-sentenced-17m-information-technology-worker-fraud-scheme-generated-revenue

[83] https://www.reuters.com/legal/government/doj-announces-arrest-indictments-north-korean-it-worker-scheme-2025-06-30/

[84] https://unit42.paloaltonetworks.com/north-korean-synthetic-identity-creation/

[85] https://www.justice.gov/usao-dc/pr/charges-and-seizures-brought-fraud-scheme-aimed-denying-revenue-workers-associated-north

[86] https://www.orangecyberdefense.com/uk/zero-trust

[87] https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2024/Presse2024/240321_PM_Nemesis_Market.html

[88] https://thehackernews.com/2025/05/300-servers-and-35m-seized-as-europol.html

[89] https://thehackernews.com/2024/12/cleo-file-transfer-vulnerability-under.html

[90] https://www.ncsc.gov.uk/news/your-say-proposals-to-counter-ransomware

[91] https://www.europol.europa.eu/media-press/newsroom/news/operation-endgame-strikes-again-ransomware-kill-chain-broken-its-source

[92] https://eucrim.eu/news/operation-endgame-targets-initial-access-malware/

[93] https://www.gov.uk/government/news/uk-to-lead-crackdown-on-cyber-criminals-with-ransomware-measures

[94] https://www.justice.gov/opa/pr/justice-department-announces-coordinated-disruption-actions-against-blacksuit-royal

[95] https://blog.checkpoint.com/research/the-state-of-ransomware-in-the-first-quarter-of-2025-a-126-increase-in-ransomware-yoy/

[96] https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

[97] https://www.cyentia.com/iris-ransomware/

[98] https://www.cyentia.com/wp-content/uploads/2024/08/IRIS_Ransomware.pdf

[99] https://www.bankinfosecurity.com/more-collins-aerospace-hacking-fallout-a-29848

[100] https://www.bloomberg.com/news/features/2025-07-24/north-korea-infiltrated-america-by-taking-remote-us-it-jobs

[101] https://assets.recordedfuture.com/insikt-report-pdfs/2025/cta-ru-2025-1022.pdf

[102] https://assets.publishing.service.gov.uk/media/6899a4ddad0cbc0e276431e3/Government_Response_Ransomware_proposals_to_increase_incident_reporting_and_reduce_payments_to_criminals.pdf

[103] https://www.gov.uk/government/consultations/ransomware-proposals-to-increase-incident-reporting-and-reduce-payments-to-criminals/ransomware-legislative-proposals-reducing-payments-to-cyber-criminals-and-increasing-incident-reporting-accessible

[104] https://www.nextgov.com/cybersecurity/2025/06/us-agencies-assessed-chinese-telecom-hackers-likely-hit-data-center-and-residential-internet-providers/405920/

[105] https://www.politico.com/news/2024/12/30/treasury-breached-chinese-hackers-cybersecurity-00196140

[106] https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

[107] https://www.windowscentral.com/software-apps/windows-11/its-the-year-of-linux-at-least-for-denmark-heres-why-the-countrys-government-is-dumping-windows-and-office-365

[108] https://digital-strategy.ec.europa.eu/en/news/thematic-roadmap-open-source-and-inputs-common-trust-principles

[109] https://www.bankinfosecurity.com/uk-ncsc-announces-software-vulnerability-initiative-a-2899

[110] https://tech.eu/2025/08/25/the-world-of-open-source-europe-report-2025-mapping-trends-challenges-and-the-push-for-digital-sovereignty/

[111] https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/

[112] https://therecord.media/allied-spy-agencies-blame-chinese-companies-salt-typhoon

[113] https://www.theguardian.com/technology/2025/jul/17/risk-undersea-cable-attacks-backed-russia-china-likely-rise-report-warns

[114] https://www.wired.com/story/satellites-are-leaking-the-worlds-secrets-calls-texts-military-and-corporate-data/

[115] https://www.theguardian.com/world/2025/oct/16/russian-cyber-attacks-against-nato-states-up-by-25-in-a-year-analysis-finds

[116] https://www.microsoft.com/en-us/security/security-insider/threat-landscape/iran-surges-cyber-enabled-influence-operations-in-support-of-hamas

[117] https://www.eunews.it/en/2025/10/24/berlin-and-paris-diverging-visions-of-digital-sovereignty-at-the-european-council/

[118] https://www.intel.gov/foreign-intelligence-surveillance-act/fisa-section-702

[119] https://www.forbes.com/sites/emmawoollacott/2025/07/22/microsoft-cant-keep-eu-data-safe-from-us-authorities/

[120] https://www.washingtonpost.com/technology/2025/10/30/tp-link-proposed-ban-commerce-department/

[121] https://www.orangecyberdefense.com/fileadmin/general/pdf/WP_Europe_Cyber_Dilemma.pdf

[122] https://www.theguardian.com/us-news/2025/feb/28/trump-russia-hacking-cybersecurity

[123] https://www.euronews.com/my-europe/2025/09/11/fact-check-is-the-eu-about-to-start-scanning-your-text-messages

[124] https://www.lemonde.fr/pixels/article/2025/10/31/chat-control-le-projet-europeen-de-surveillance-des-messageries-largement-abandonne_6650578_4408996.html

[125] https://www.theguardian.com/technology/2025/jul/24/what-are-the-new-uk-online-safety-rules-and-how-will-they-be-enforced

[126] https://en.wikipedia.org/wiki/Edward_Snowden

[127] https://apnews.com/article/icc-trump-sanctions-karim-khan-court-a4b4c02751ab84c09718b1b95cbd5db3

[128] https://www.businessinsider.com/bill-gates-ai-bubble-similar-dot-com-bubble-2025-10

[129] https://arstechnica.com/information-technology/2024/04/german-state-gov-ditching-windows-for-linux-30k-workers-migrating/

[130] https://www.lyon.fr/actualite/action-municipale/la-ville-de-lyon-renforce-sa-souverainete-numerique

[131] https://krebsonsecurity.com/2025/04/funding-expires-for-key-cyber-vulnerability-database

[132] https://www.cybersecuritydive.com/news/cisa-extend-funding-cve/745531/

[133] https://www.orangecyberdefense.com/be/hot-topics/sovereignty-trusted-security-resilience

[134] https://www.computerweekly.com/news/366623995/Enisa-launches-European-vulnerability-database

[135] https://bindinghook.com/why-europes-new-vulnerability-database-matters-more-than-you-think/

[136] https://www.zdnet.com/article/why-the-cve-database-for-tracking-security-flaws-nearly-went-dark-and-what-happens-next/

[137] https://www.verizon.com/business/resources/reports/dbir/

[138] https://krebsonsecurity.com/2025/04/funding-expires-for-key-cyber-vulnerability-database/

[139] https://www.forbes.com/sites/kateoflahertyuk/2025/04/16/cve-program-funding-cut-what-it-means-and-what-to-do-next/

[140] https://bindinghook.com/why-europes-new-vulnerability-database-matters-more-than-you-think/

[141] https://en.wikipedia.org/wiki/China_National_Vulnerability_Database

[142] https://jvn.jp/en/

[143] https://medium.com/@johnlatwc/defenders-mindset-319854d10aaa

[144] https://www.volexity.com/blog/2024/01/10/active-exploitation-of-two-zero-day-vulnerabilities-in-ivanti-connect-secure-vpn/

[145] https://cloud.google.com/blog/topics/threat-intelligence/2024-zero-day-trends?hl=en

[146] https://en.wikipedia.org/wiki/Cyber_Resilience_Act

[147] https://my.f5.com/manage/s/article/K000154696

[148] https://researchbriefings.files.parliament.uk/documents/POST-PN-0753/POST-PN-0753.pdf

[149] https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-webvpn-z5xP8EUB

[150] https://www.cisa.gov/news-events/alerts/2025/10/15/cisa-directs-federal-agencies-mitigate-vulnerabilities-f5-devices

[151] https://www.bleepingcomputer.com/news/security/over-266-000-f5-big-ip-instances-exposed-to-remote-attacks/

[152] https://www.csoonline.com/article/4074945/network-security-devices-endanger-orgs-with-90s-era-flaws.html

[153] https://cyberscoop.com/mandiant-m-trends-2025

[154] https://www.coalitioninc.com/blog/cyber-insurance/2024-cyber-claims-report

[155] https://firecompass.com/f5-big-ip-source-code-and-vulnerabilities-breach

[156] https://www.ncsc.gov.uk/news/confirmed-compromise-f5-network

[157] https://www.reuters.com/technology/cybersecurity/cisco-says-hackers-subverted-its-security-devices-spy-governments-2024-04-24

[158] https://www.cisa.gov/news-events/directives/supplemental-direction-v1-ed-24-01-mitigate-ivanti-connect-secure-and-ivanti-policy-secure

[159] https://www.cyentia.com/why-your-mttr-is-probably-bogus/

[160] https://support.microsoft.com/en-gb/windows/windows-10-support-has-ended-on-october-14-2025-2ca8b313-1946-43d3-b55c-2b95b107f281

[161] https://www.ncsc.gov.uk/section/software-security-code-of-practice

[162] https://www.eurojust.europa.eu/news/hacktivist-group-responsible-cyberattacks-critical-infrastructure-europe-taken-down

[163] https://www.politico.eu/article/pro-russian-hackers-target-belgium-websites-media-elections-noname057-flemish-parliament/

[164] https://therecord.media/japan-political-party-hit-by-cyberattack-pro-russian-hackers

[165] https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025.pdf

[166] https://www.europol.europa.eu/media-press/newsroom/news/global-operation-targets-noname05716-pro-russian-cybercrime-network

[167] https://yle.fi/a/74-20184917

[168] https://www.reuters.com/en/pro-ukrainian-hackers-claim-massive-cyberattack-russias-aeroflot-2025-07-28/

[169] https://therecord.media/ukraine-hackers-claim-attack-russia-gaskar-group-drone-maker

[170] https://www.theguardian.com/world/2024/dec/13/democrats-republicans-condemn-salt-typhoon-hack

[171] https://www.ncsc.gov.uk/news/uk-allies-expose-china-tech-companies-enabling-cyber-campaign

[172] https://thehackernews.com/2025/08/salt-typhoon-exploits-cisco-ivanti-palo.html

[173] https://home.treasury.gov/news/press-releases/jy2792

[174] https://www.ic3.gov/PSA/2025/PSA250424-2

[175] https://www.cisa.gov/sites/default/files/2025-09/CSA_COUNTERING_CHINA_STATE_ACTORS_COMPROMISE_OF_NETWORKS.pdf

[176] https://www.aivd.nl/documenten/publicaties/2025/05/27/aivd-en-mivd-onderkennen-nieuwe-russische-cyberactor

[177] https://www.microsoft.com/en-us/security/blog/2025/05/27/new-russia-affiliated-actor-void-blizzard-targets-critical-sectors-for-espionage/

[178] https://www.defensie.nl/actueel/nieuws/2025/05/27/onbekende-russische-groep-achter-hacks-nederlandse-doelen

[179] https://therecord.media/laundry-bear-void-blizzard-russia-hackers-netherlands

[180] https://www.microsoft.com/en-us/security/blog/2025/05/27/new-russia-affiliated-actor-void-blizzard-targets-critical-sectors-for-espionage/

[181] https://therecord.media/laundry-bear-void-blizzard-russia-hackers-netherlands

[182] https://www.aivd.nl/documenten/publicaties/2025/05/27/aivd-en-mivd-onderkennen-nieuwe-russische-cyberactor

[183] https://www.csa.gov.sg/alerts-and-advisories/alerts/al-2025-068

[184] https://github.com/prettier/eslint-config-prettier/issues/339#issuecomment-3090304490

[185] https://invokere.com/posts/2025/07/scavenger-malware-distributed-via-eslint-config-prettier-npm-package-supply-chain-compromise/

[186] https://www.zscaler.com/blogs/security-research/malicious-pypi-packages-deliver-silentsync-rat

[187] https://www.infosecurity-magazine.com/news/npm-supply-chain-attack-averted/

[188] https://www.aikido.dev/blog/npm-debug-and-chalk-packages-compromised

[189] https://bsky.app/profile/scooper.bsky.social/post/3lywfjqhf7s23

[190] https://www.aikido.dev/blog/s1ngularity-nx-attackers-strike-again

[191] https://socket.dev/blog/tinycolor-supply-chain-attack-affects-40-packages

[192] https://www.fortinet.com/blog/threat-research/multilayered-email-attack-how-a-pdf-invoice-and-geofencing-led-to-rat-malware

[193] https://www.safebreach.com/blog/scattered-spider/

[194] https://flashpoint.io/blog/scattered-spider-threat-profile/

[195] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a

[196] https://therecord.media/transport-for-london-cyberattack

[197] https://www.justice.gov/opa/pr/united-kingdom-national-charged-connection-multiple-cyber-attacks-including-critical

[198] https://www.reuters.com/business/hawaiian-airlines-hit-by-cyber-attack-2025-06-26/

[199] https://therecord.media/millions-impacted-by-data-breaches-insurance-car-dealership-software

[200] https://therecord.media/salesforce-scattered-spider-extortion-site

[201] https://therecord.media/scattered-spider-targeting-snowflake-access-data-exfiltration

[202] https://www.reuters.com/business/retail-consumer/ms-co-op-cyberattackers-duped-it-help-desks-into-resetting-passwords-says-report-2025-05-06/

[203] https://www.cnbc.com/2025/10/29/jaguar-land-rover-cyberattack-holds-ominous-lesson-for-british-firms.html

[204] https://www.facebook.com/Saint.Louis.Art.Museum/posts/today-begins-the-year-of-the-wood-dragon-for-the-chinese-new-year-according-to-c/777304421104188/

[205] https://www.orangecyberdefense.com/de/white-papers/security-navigator-2025

[206] https://fortune.com/2025/08/01/openai-funding-oversubscribed-early-investors-new-partners-dragoneer/

[207] https://www.investopedia.com/nvidia-stock-price-levels-to-watch-after-chip-giant-usd100-billion-deal-with-openai-11815140

[208] https://www.msn.com/en-us/money/other/microsoft-forecasts-show-data-center-crunch-persisting-into-2026/ar-AA1Oao9q

[209] https://content.knightfrank.com/research/2960/documents/en/data-centers-global-forecast-report-2025-11877.pdf

[210] https://www.tomshardware.com/desktops/servers/first-in-depth-look-at-elon-musks-100-000-gpu-ai-cluster-xai-colossus-reveals-its-secrets

[211] https://www.bbc.com/news/articles/cx25v2d7zexo

[212] https://www.nature.com/articles/d41586-024-03162-2

[213] https://penncapital-star.com/economy/microsoft-describes-three-mile-island-plant-as-a-once-in-a-lifetime-opportunity/

[214] https://www.bea.gov/news/2025/gross-domestic-product-2nd-quarter-2025-third-estimate-gdp-industry-corporate-profits

[215] https://x.com/jasonfurman/status/1971995367202775284

[216] https://fortune.com/2025/10/07/data-centers-gdp-growth-zero-first-half-2025-jason-furman-harvard-economist/

[217] https://en.wikipedia.org/wiki/A_rising_tide_lifts_all_boats

[218] https://budgetmodel.wharton.upenn.edu/issues/2025/9/8/projected-impact-of-generative-ai-on-future-productivity-growth

[219] https://www.youtube.com/watch?v=4GLSzuYXh6w

[220] https://www.politico.eu/article/europe-business-barely-use-artificial-intelligence-brussels-fix/

[221] https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai

[222] https://www.uschamber.com/technology/artificial-intelligence/u-s-chambers-latest-empowering-small-business-report-shows-majority-of-businesses-in-all-50-states-are-embracing-ai

[223] https://www.oecd.org/en/about/news/press-releases/2024/12/economic-outlook-global-growth-to-remain-resilient-in-2025-and-2026-despite-significant-risks.html

[224] https://www.imf.org/external/datamapper/profile/WEOWORLD

[225] https://huggingface.co/spaces/lmarena-ai/chatbot-arena-leaderboard

[226] https://llm-stats.com/

[227] https://www.vellum.ai/llm-leaderboard

[228] https://aider.chat/docs/leaderboards/

[229] https://darioamodei.com/on-deepseek-and-export-controls

[230] https://www.youtube.com/watch?v=4poqjZlM8Lo

[231] https://www.weforum.org/publications/the-future-of-jobs-report-2025/digest/

[232] https://aws.amazon.com/what-is/agentic-ai/

[233] https://www.youtube.com/watch?v=LCEmiRjPEtQ

[234] George Dyson, Darwin Among the Machines, Addison-Wesley, 1997

[235] https://www.lawfaremedia.org/article/ai-and-secure-code-generation

[236] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/deepfake-it-til-you-make-it-a-comprehensive-view-of-the-new-ai-criminal-toolset

[237] https://www.weforum.org/stories/2025/02/deepfake-ai-cybercrime-arup/

[238] https://www.group-ib.com/blog/ai-cybercrime-usecases/

[239] https://www.anthropic.com/news/detecting-countering-misuse-aug-2025

[240] https://www.eset.com/us/about/newsroom/research/eset-discovers-promptlock-the-first-ai-powered-ransomware/?srsltid=AfmBOoqwxT-tNXx-l3j8X-3C2-QAA2oTQFqTUDz3ZYRp7hnMBqgsKtyl5

[241] https://cyberscoop.com/ai-ransomware-promptlock-nyu-behind-code-discovered-by-security-researchers/

[242] https://arxiv.org/html/2508.20444v1

[243] https://www.reuters.com/en/jlrs-uk-factory-stoppage-cyber-attack-stretches-three-weeks-2025-09-16

[244] https://therecord.media/norway-police-suspect-pro-russian-hackers-dam-sabotage

[245] https://ritics.org/

[246] https://blog.google/technology/research/google-willow-quantum-chip/

[247] https://research.kudelskisecurity.com/2021/08/24/quantum-attack-resource-estimate-using-shors-algorithm-to-break-rsa-vs-dh-dsa-vs-ecc/

[248] https://quantum-journal.org/papers/q-2021-04-15-433/

[249] https://arxiv.org/html/2505.15917v1

[250] https://blog.acmvit.in/quantum-timebomb?x-host=blog.acmvit.in#:~300%20trillion%20years

[251] https://arstechnica.com/science/2023/10/atom-computing-is-the-first-to-announce-a-1000-qubit-quantum-computer/

[252] https://en.wikipedia.org/wiki/List_of_quantum_processors

[253] https://www.dwavesys.com/company/newsroom/press-release/d-wave-announces-1-200-qubit-advantage2-prototype-in-new-lower-noise-fabrication-stack-demonstrating-20x-faster-time-to-solution-on-important-class-of-hard-optimization-problems/

[254] https://www.ibm.com/quantum/blog/large-scale-ftqc

[255] https://globalriskinstitute.org/publication/2024-quantum-threat-timeline-report/

[256] https://www.fortinet.com/resources/cyberglossary/shors-grovers-algorithms

[257] https://pqcc.org/international-pqc-requirements/

[258] https://www.ncsc.gov.uk/guidance/pqc-migration-timelines

[259] https://quant-x-sec.com/whitepapers/The%20Financial%20Market%E2%80%99s%20Transition%20to%20Post-Quantum%20Cryptography_%20Print_May%202025.pdf

[260] https://www.digicert.com/blog/evolution-of-ssl

[261] https://www.gsma.com/newsroom/wp-content/uploads//PQC-Guidelines-for-Telco-Use-Cases-Executive-Summary.pdf

[262] https://www.theqrl.org/a-visionary-future-proof-blockchain-with-unparalleled-security/

[263] https://algorand.co/technology/post-quantum

[264] https://www.btq.com/blog/ethereums-roadmap-post-quantum-cryptography

[265] https://ethereum.org/roadmap/future-proofing/

[266] https://www.deloitte.com/nl/en/services/consulting-risk/perspectives/quantum-computers-and-the-bitcoin-blockchain.html

[267] https://bernardmarr.com/will-quantum-computing-kill-bitcoin/

[268] https://bitcoinwiki.org/wiki/bitcoin-improvement-proposals

[269] https://support.apple.com/en-us/122756

[270] https://techcommunity.microsoft.com/blog/microsoft-security-blog/post-quantum-cryptography-comes-to-windows-insiders-and-linux/4413803

[271] https://cloud.google.com/security/resources/post-quantum-cryptography

[272] https://aws.amazon.com/security/post-quantum-cryptography/

[273] https://www.encryptionconsulting.com/current-landscape-of-post-quantum-cryptography-migration/#:~:text=This%20hybrid%20approach%20delivers%20the%20best%20of%20both%20worlds%3A%20the%20reliability%20of%20established%20classical%20methods%20with%20the%20resilience%20of%20quantum%2Dsafe%20algorithms.

[274] https://www.weforum.org/publications/quantum-readiness-toolkit-building-a-quantum-secure-economy/

[275] https://www.euro-stack.info/

[276] https://www.euro-stack.info

[277] https://therecord.media/ukraine-takes-steps-dedicated-cyber-force

[278] https://www.coe.int/en/web/cybercrime/-/cybersee-in-cooperation-with-cepol-strengthen-regional-law-enforcement-capabilities-on-illegal-use-of-virtual-assets-and-asset-recovery

[279] https://therecord.media/ukraine-takes-steps-dedicated-cyber-force

[280] https://www.microsoft.com/en-us/security/blog/2025/02/13/storm-2372-conducts-device-code-phishing-campaign/

[281] https://cloud.google.com/blog/topics/threat-intelligence/brickstorm-espionage-campaign

[282] https://services.google.com/fh/files/misc/m-trends-2025-en.pdf

[283] https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a

[284] https://www.proofpoint.com/us/blog/threat-insight/phish-china-aligned-espionage-actors-ramp-up-taiwan-semiconductor-targeting

[285] https://www.justice.gov/archives/opa/pr/three-irgc-cyber-actors-indicted-hack-and-leak-operation-designed-influence-2024-us

[286] https://securitylab.amnesty.org/latest/2025/03/journalists-targeted-with-pegasus-spyware/

[287] https://www.consilium.europa.eu/en/press/press-releases/2025/01/27/cyber-attacks-three-individuals-added-to-eu-sanctions-list-for-malicious-cyber-activities-against-estonia

[288] https://cloud.google.com/blog/topics/threat-intelligence/global-revival-of-hacktivism/

[289] https://www.wired.com/story/x-ddos-attack-march-2025

[290] https://www.theguardian.com/technology/2025/may/07/pro-russian-hackers-claim-to-have-targeted-several-uk-websites

[291] https://www.reuters.com/technology/norway-spy-chief-blames-russian-hackers-dam-sabotage-april-2025-08-13/

[292] https://www.forescout.com/blog/anatomy-of-a-hacktivist-attack-russian-aligned-group-targets-otics/

[293] https://apnews.com/article/42d98dabdc0182dac4bd4c80d880cdb4

[294] https://nltimes.nl/2025/08/08/pro-russian-hacker-group-active-ever-europol-takedown

[295] https://arxiv.org/pdf/2509.05104

[296] https://www.europol.europa.eu/operations-services-and-innovation/operations/operation-endgame

[297] ICT-Information and Communication technology

[298] https://www.verizon.com/business/resources/reports/2025-dbir-executive-summary.pdf

[299] https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

[300] https://securitydelta.nl/media/com_hsd/report/690/document/ENISA-Threat-Landscape-2024.pdf

[301] https://www.orangecyberdefense.com/global/white-papers/security-navigator-2024

[302] https://www.orangecyberdefense.com/se/security-navigator

[303] https://www.justice.gov/archives/opa/pr/criminal-marketplace-disrupted-international-cyber-operation

[304] https://www.europol.europa.eu/media-press/newsroom/news/global-coalition-takes-down-new-criminal-communication-platform

[305] https://www.politie.nl/nieuws/2024/oktober/8/11-internationale-actie-tegen-werelds-grootste-darkweb-markt-bohemia-cannabia.html

[306] https://www.europol.europa.eu/media-press/newsroom/news/takedown-of-sms-based-flubot-spyware-infecting-android-phones

[307] https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2023/Presse2023/231220_PM_Darknet_Kingdom_Market.html

[308] https://www.europol.europa.eu/media-press/newsroom/news/largest-ever-operation-against-botnets-hits-dropper-malware-ecosystem

[309] The Office of Foreign Assets Control (“OFAC”) of the US Department of the Treasury

[310] Farrington, D. P. (1986). Age and crime. In M. Tonry & N. Morris (Eds.), Crime and Justice: An Annual Review of Research (Vol. 7, pp. 189-250). University of Chicago Press.

[311] Hirschi, T., & Gottfredson, M. (1983). Age and the explanation of crime. American Journal of Sociology, 89(3), 552-584.

[312] Moffitt, T. E. (1993). Adolescence-limited and life-course-persistent antisocial behavior: A developmental taxonomy. Psychological Review, 100(4), 674-701.

[313] https://www.verizon.com/business/resources/reports/2025-dbir-executive-summary.pdf

[314] https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

[315] https://www.orangecyberdefense.com/global/white-papers/security-navigator-2024

[316] United States Sentencing Commission. (2024). Cyber technology in federal crime. Washington, DC: USSC. Retrieved from https://www.ussc.gov/sites/default/files/pdf/research-and-publications/research-publications/2024/202409_cyber-technology.pdf

[317] Soares, A. B., & Lazarus, S. (2024). Examining fifty cases of convicted online romance-fraud offenders. London School of Economics. Retrieved from https://eprints.lse.ac.uk/126265/

[318] Maras, T., Kiernan, A., Broadhurst, R., & Steffensmeier, D. (2024). Predictors and pathways in middle adolescence: Examining the longitudinal stability of cyber-offending between ages 14 and 17. United Kingdom Millennium Cohort Study. Retrieved from https://www.researchgate.net/publication/390328879_Predictors_and_Pathways_in_Middle_Adolescence_Examining_the_Longitudinal_Stability_of_Cyber_Offending_Between_Ages_14_and_17

[319] Hadzhidimova, L. I., & Payne, B. K. (2019). The profile of the international cyber offender in the U.S. International Journal of Cybersecurity Intelligence & Cybercrime, 2(1), 40-55. https://doi.org/10.52306/0201041YNGG5534

[320] Clarke, R. V., & Cornish, D. B. (1985). Modeling offenders' decisions: A framework for research and policy. In M. Tonry & N. Morris (Eds.), Crime and Justice: An Annual Review of Research (Vol. 6, pp. 147-185). University of Chicago Press.

[321] Donner, C. M. (2016). The Gender Gap and Cybercrime: An Examination of College Students' Online Offending. Victims & Offenders, 11(4), 556-577. https://doi.org/10.1080/15564886.2016.1173157

[322] Hutchings, A., & Chua, Y. T. (2017). Gendering cybercrime. In T. J. Holt (Ed.), Cybercrime through an interdisciplinary lens (pp. 167-188). Routledge. https://www.cl.cam.ac.uk/~ah793/papers/2017gendering_cybercrime.pdf

[323] https://www.isc2.org/Insights/2025/03/Women-Comprise-22-percent-of-the-Cybersecurity-Workforce

[324] https://iea.blob.core.windows.net/assets/0aa4762f-c1cb-4495-987a-25945d6de5e8/GlobalEVOutlook2025.pdf

[325] https://upstream.auto/cybersecurity-risks-ev-charging-ecosystem/

[326] https://www.cve.org/CVERecord?id=CVE-2024-25998

[327] https://www.orangecyberdefense.com/global/white-papers/winds-of-change-causes-and-implications-of-the-solarwinds-compromise

[328] https://en.wikipedia.org/wiki/Juice_jacking

[329] https://www.ndss-symposium.org/ndss-paper/brokenwire-wireless-disruption-of-ccs-electric-vehicle-charging/

[330] https://konbriefing.com/en-topics/cyber-attacks-2024-ind-automotive.html

[331] https://vicone.com/blog/electric-vehicle-charger-security-risks-how-vulnerabilities-could-lead-to-fire-hazards

[332] https://www.nature.com/articles/s41598-025-92895-9

[333] https://digitalchargingsolutions.com/en/data-update/

[334] https://www.iso.org/standard/70918.html

[335] https://www.iea.org/reports/global-ev-outlook-2025/electric-vehicle-charging

[336] Swayne, M. (2025, August 11). From Quantum Computing Roadmaps: A Look at The Maps And Predictions of Major Quantum Players: https://thequantuminsider.com/2025/05/16/quantum-computing-roadmaps-a-look-at-the-maps-and-predictions-of-major-quantum-players/

[337] Simran Tinani, U. W. (2025, April 16). From Post-Quantum Cryptography: A Comprehensive Guide: https://www.cnlab.ch/fileadmin/documents/Publikationen/2025/Post-Quantum_Cryptography_-__A_Comprehensive_Guide.pdf

[338] ETSI. (2020, August 11). From Migration strategies and recommendations to Quantum Safe schemes: https://www.etsi.org/newsroom/press-releases/1805-2020-08-etsi-releases-migration-strategies-and-recommendations-for-quantum-safe-schemes

[339] NCSC. (2025, March 20). From Timelines for migration to post-quantum cryptography: https://www.ncsc.gov.uk/guidance/pqc-migration-timelines

[340] Joshi, H. (2025, August 6). From Enterprise Guide to PQC Migration: https://www.encryptionconsulting.com/enterprise-guide-to-pqc-migration/

[341] NIST. (2024, February 20). From Migration to Post-Quantum Cryptography: Preparation for Considering the Implementation and Adoption of Quantum Safe Cryptography: https://csrc.nist.gov/pubs/sp/1800/38/iprd-(1)

[342] CCC. (2019, September 16). From Identifying Research Challenges in Post Quantum Cryptography Migration and Cryptographic Agility: https://arxiv.org/abs/1909.07353

[343] CISA. (2023, August 21). From Quantum-Readiness: Migration to Post-Quantum Cryptography: https://www.cisa.gov/resources-tools/resources/quantum-readiness-migration-post-quantum-cryptography

[344] BSI. (2022, May 18). From Quantum-safe cryptography - fundamentals, current developments and recommendations: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.html

[345] Mosca, M. (2018). Cybersecurity in an Era with Quantum Computers: Will We Be Ready? IEEE Security & Privacy, 38-41.

[346] Mosca, M. (2018). Cybersecurity in an Era with Quantum Computers: Will We Be Ready? IEEE Security & Privacy, 38-41.

[347] CCC. (2019, September 16). From Identifying Research Challenges in Post Quantum Cryptography Migration and Cryptographic Agility: https://arxiv.org/abs/1909.07353

[348] NXP. (2024). Post-Quantum Cryptographic Migration Challenges for Embedded Devices: https://www.nxp.com/docs/en/white-paper/POSTQUANCOMPWPA4.pdf

Disclaimer

All content in this report, including text, graphics, logos, icons and images, is the property of Orange Cyberdefense and is protected by copyright and/or other works of authorship laws. The content may be used as a resource, stating clear references. Any other use, in particular including reproduction, modification, distribution, transmission, republication, display or performance of the content is strictly prohibited, unless written consent is given.

The use of any part of this report in (i) data mining or data crawling or (ii) training generative artificial intelligence (AI) and large language model (LLM) technologies to generate content any kind of content is expressly prohibited, unless written consent is given.

Orange Cyberdefense makes this report available on an "as-is" basis with no guarantees of completeness, accuracy, usefulness, timeliness or any warranty of any kind. The information contained in this report is general in nature. Opinions and conclusions presented reflect judgment at the time of publication and may change at any time. Orange Cyberdefense assumes no responsibility or liability for errors, omissions or for the results obtained from the use of the information. If you have specific security concerns, please contact Orange Cyberdefense via https://orangecyberdefense.com/global/contact/ for more detailed analysis and security consulting services.

Orange Cyberdefense:
Leading European Excellence in Cybersecurity

Orange Cyberdefense is a leading European partner for cybersecurity services. Backed by over 30 years of expertise developed within the Orange Group, we independently deliver intelligence-led solutions across managed services, consulting and systems integration, helping organizations anticipate, prevent and respond to cyber threats at any time.

With 36 Security Operations Centers worldwide and a team of 3,200 experts across 12 countries, including our in-house CERT, Orange Cyberdefense provides comprehensive, innovative, and integrated cybersecurity solutions supported by AI and tailored for businesses, from SMEs to large enterprises and critical national infrastructures. Our guiding principle is to build a safer digital society for all placing people at the heart of what we do.

By combining deep human competence, strong local presence, with carefully selected technology, we deliver solutions that help you stay ahead of evolving threats.

Our multidisciplinary cybersecurity specialists work across all cyber domains to support the growth and resilience of more than 50,000 organizations worldwide, so you can focus on what matters most: your business, your people, your clients.

We deliver engineered cybersecurity solutions powered by ThreatMap, our proprietary cyber threat intelligence, enabling you to identify emerging threats early, strengthen your strategy, and take decisive action.

This work is reinforced by our Security Research Center, a dedicated unit that identifies, tracks, analyzes, and communicates significant developments in the threat landscape. We share what we learn to help strengthen collective cyber resilience.

www.orangecyberdefense.com