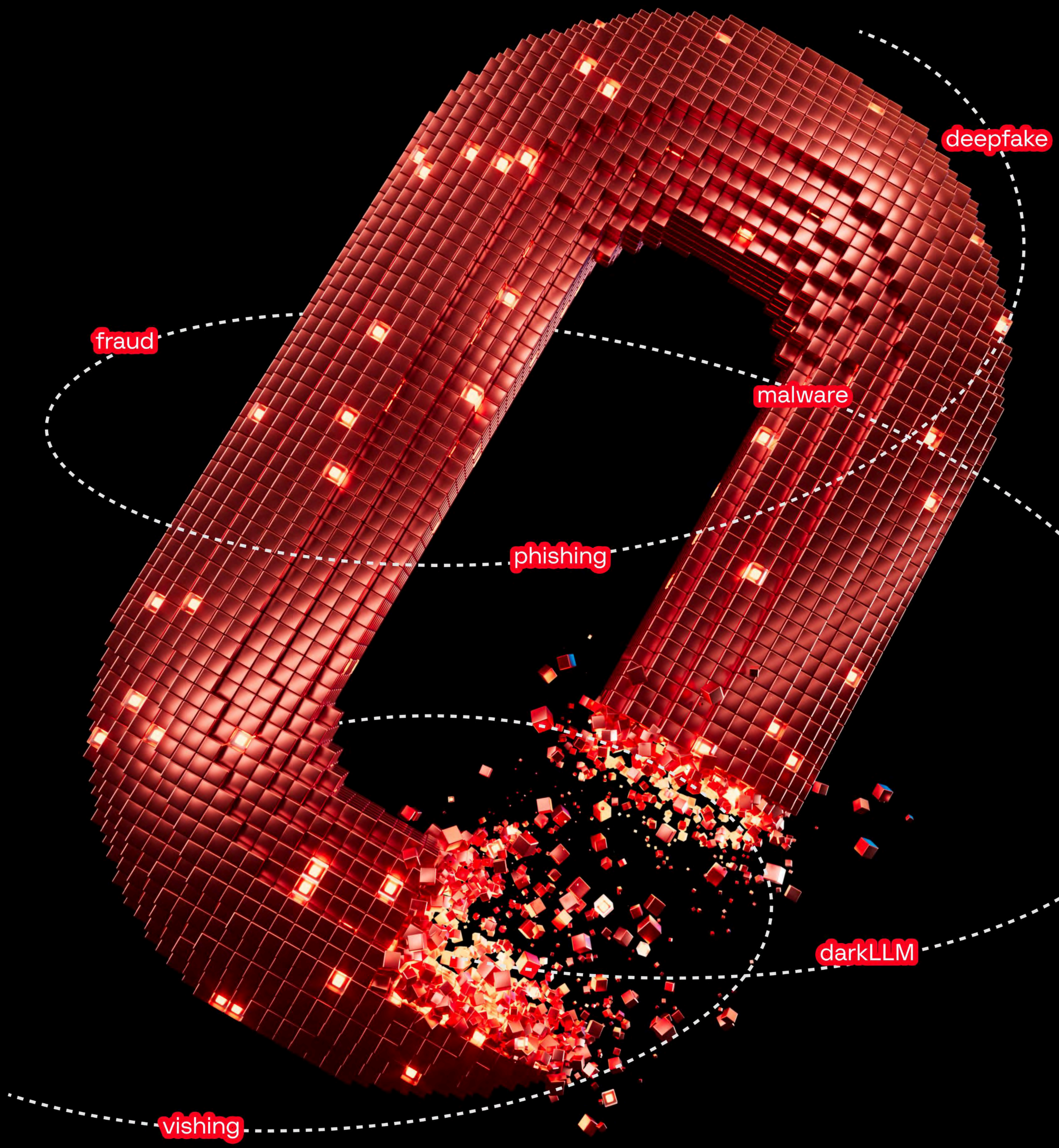
GROUP-IB



High Tech Crime Trends Report 2026

The Age of Supply Chain Attacks

GROUP-IB.COM

Table of content

Introduction

Welcome to Group-IB's High-Tech Crime Trends Report 2026 03

Executive Summary 04
At a Glance: Threat Actors and Malware Mentioned Within This Report 08
Methodology 09
Contributions to Law Enforcement Operations in 2025 10

Chapter 01

The Age of Supply Chain Attacks: The Crisis of Trust Deepens 13

The Fragility of Open-Source Ecosystems 15
The Rise of Malicious Extensions 17
Phishing-Driven Identity Compromise in the Supply Chain 20
The Evolution of Social Engineering in Supply Chain Attacks 28
Data Breaches as a Supply Chain Attack Multiplier 34
From Access to Extortion: The Industrialization of the Ransomware Supply Chain 41
Advanced Persistent Threats: Converging Motives, Strategic Narratives, and Technological Superiority 56

Chapter 02

Key Threat Actors and Malware 58

Group-IB Threat Intelligence Portal 59
Supply Chain-Focused Threat Actors 60

Chapter 03

2026 Cyber Forecast and Recommendations 66

AI-Assisted Code Generation: Innovation with Hidden Supply Chain Risks 67
The API Wild West: Unchecked Integrations Expanding the Attack Surface 68
Artificial Intelligence in the Middle: The Rising Threat to Authentication 69
AI-Driven Malware: The Next Evolution in Autonomous Cyber Threats 70
Agentic Extortion: The Next Stage of Ransomware Evolution 71
Crypto and Stablecoins: Financial Innovation or Expanding Cyber Vulnerability 72
The Psychological Power Behind Modern Phone Scams 73
Secure-by-Sovereignty, Exposed-by-Design 74
Wearable Devices: An Emerging Vector of Data Exposure 75

Welcome to Group-IB's High-Tech Crime Trends Report 2026

Dmitry Volkov
Chief Executive Officer, Group-IB

Cybercrime is no longer defined by isolated breaches. Today, supply chain cyber attacks form interconnected ecosystems where trust, access, and data continuously reinforce one another. As organizations become more digitally interdependent, attackers increasingly target upstream vendors and service providers to achieve scale, speed, and stealth.

By compromising software providers, managed service partners, and other trusted third parties, adversaries can bypass perimeter defenses and inherit trusted access to entire customer networks. A single compromised supplier can now expose dozens or even hundreds of downstream organizations.

This access is amplified by the rapid growth of data leaks. Stolen credentials, source code, API keys, and internal communications provide attackers with deep insight into trusted relationships and business workflows. Combined with brokered access, leaked data enables highly targeted intrusion, impersonation, and fraud campaigns that blend into legitimate activity.

These elements converge into multi-vector attacks. Compromised vendors are used to launch phishing and business email compromise. Trusted platforms are abused to distribute malware or manipulate transactions. Identity compromise opens the door to financial systems, procurement processes, and customer accounts. Intrusion feeds fraud, fraud generates new data, and that data fuels further attacks.

This cycle has transformed cybercrime into an industrialized operation and exposed the limits of perimeter-focused defense. Organizations must understand how access is obtained, how data is weaponized, and how attacks propagate across ecosystems before damage occurs.

Group-IB addresses this challenge through predictive intelligence and cyber fraud fusion. By correlating initial access activity, emerging data leaks, behavioral anomalies, and cross-industry fraud signals, we help organizations anticipate weak links, disrupt attack chains early, and prevent cascading supply chain compromise.

We invite you to explore the insights in this report and join us in shaping a more proactive approach to defeating high-tech crime.

Executive Summary

The Group-IB High-Tech Crime Trends 2026 Report examines how supply chain attacks have emerged as a defining force in today's cyber threat landscape. Rather than targeting organizations in isolation, attackers increasingly exploit software dependencies, third-party providers, and trusted digital ecosystems to gain wide-reaching access. The report details how these indirect attack paths are reshaping risk across industries, accelerating the spread of compromise, and magnifying the operational and financial consequences of modern cyber incidents.

The Interconnected Nature of Modern Supply Chain Attacks

Cybercrime has evolved into a landscape where **supply chain attacks form the connective tissue between otherwise distinct threats.** What appear to be separate incidents—phishing, ransomware, data breaches, malicious software, or insider abuse—are increasingly stages of the same supply chain-driven attack ecosystem, all exploiting trust as the primary attack surface.

Modern supply chain attacks are built on **inherited access**. By compromising upstream vendors, open-source maintainers, SaaS platforms, browser extensions, or managed service providers, attackers gain legitimate entry points that quietly extend across hundreds or thousands of downstream organizations. A single compromise can trigger a domino effect, enabling attackers to move laterally across customers, partners, and platforms while remaining embedded in trusted workflows.

These attack types are no longer independent. Open-source package compromise feeds malware distribution and credential theft. Phishing and OAuth abuse enable identity compromise that unlocks SaaS and CI/CD environments. Data breaches supply the credentials, context, and relationships needed to refine impersonation and lateral movement. Ransomware and extortion arrive later in the chain, capitalizing on access and intelligence gathered earlier. Each stage strengthens the next, creating a self-reinforcing cycle of supply chain exploitation.

Identity sits at the center of this convergence. Stolen tokens, API keys, service accounts, and even synthetic human identities act as portable supply chain access, allowing attackers to blend in as trusted users or insiders for extended periods. Once inside, attackers reuse legitimate integrations and permissions to spread across interconnected environments without triggering traditional defenses.

As a result, supply chain attacks now unify cybercrime and state activity. Criminal groups and state-aligned actors increasingly leverage the same supply chain weaknesses, tools, and access brokers, blurring attribution and amplifying systemic risk. The true danger lies not in any single attack, but in how these interconnected techniques combine—turning isolated compromises into widespread, cascading failures across entire digital ecosystems.

The Interconnectivity and Impact of Supply Chain Attacks

2025 saw an escalation in the abuse of trusted vendor access that triggered a cascading impact across supply chains, impacting hundreds of organizations and millions of users worldwide.

Main Supply Chain Attack Targets in 2025

- Upstream vendors
- Open-source maintainers
- SaaS platforms
- Browser extensions
- Managed Service Providers

Triggering a Domino Effect

Oracle breach caused by legacy environment exploit

6 mln users

~128K unique domains

Drift/Salesloft/ Salesforce token abuse

700+ organizations worldwide impacted via compromised OAuth tokens

Fintech firm Marquis ransomware attack

70+ financial institutions sensitive data compromised

Shai-hulud NPM self-propagating worms. Compromise impact

100 mln downloads

800+ npm packages

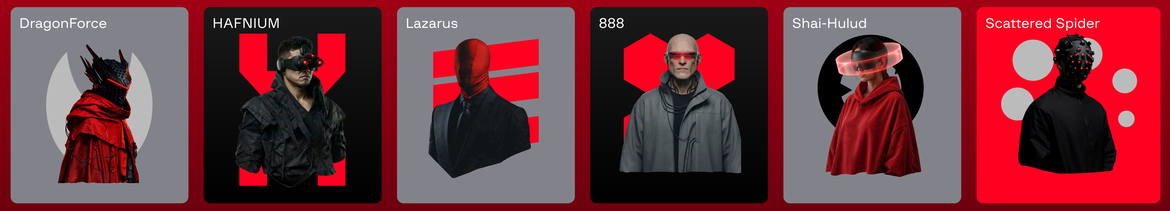
Top Techniques Used to Attack Upstream Vendors

- Token hijacking
- Compromised third-party integrations & API keys
- Developer / maintainer targeting
- Synthetic insiders / deepfake-enabled impersonation
- Malicious package injection

Evolution of Social Engineering Through Artificial Intelligence

Mass phishing	→ Hyper-personalized lures
Impersonation	→ Deepfake-enabled trust attacks
Fake accounts	→ Synthetic identities
Manual ops	→ Autonomous scam workflows
Persuasion	→ On-demand malware delivery

Top Supply Chain-Focused Cybercriminals



Transformation of the Cybercrime Ecosystem

Initial Access Brokers

Public IAB listings declined

27%

shifting high-value deals into private channels

High-value access is sold directly to ransomware operators

Access is increasingly sold as

- Tokens
- SaaS admin
- Integration footholds

not just VPN/RDP

Phishing

Automated SpaaS + AI-driven lures turned phishing into **an always-on, adaptive delivery layer**

Focus shifted from passwords → **to identity, tokens, and consent theft**

Ransomware

Fewer new RaaS programs

-17.9%

but overall activity continued to expand

Operations moved from "single victim" → **to vendor/ MSP-scale extortion**

AI-assisted ransomware moved from experimental → **to affiliate-ready**

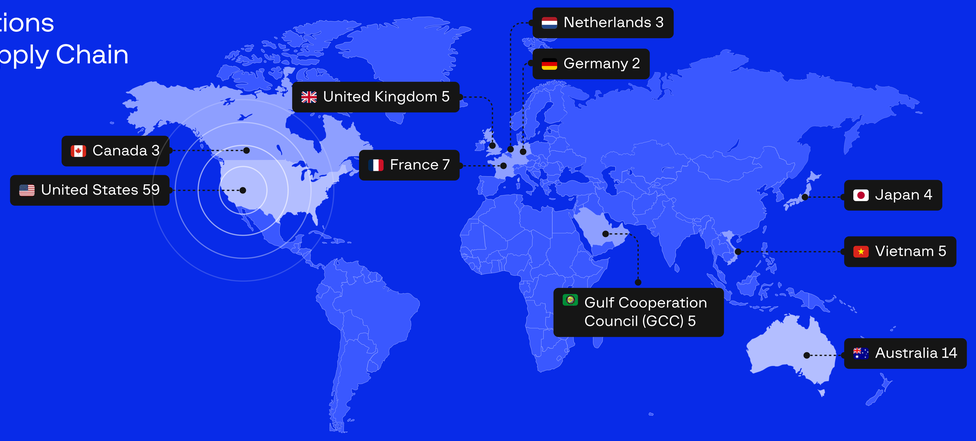
Advanced Persistent Threats

Identity simulation enables stealthy access and hybrid espionage-for-profit

Attribution is increasingly used as political signaling, not purely forensics

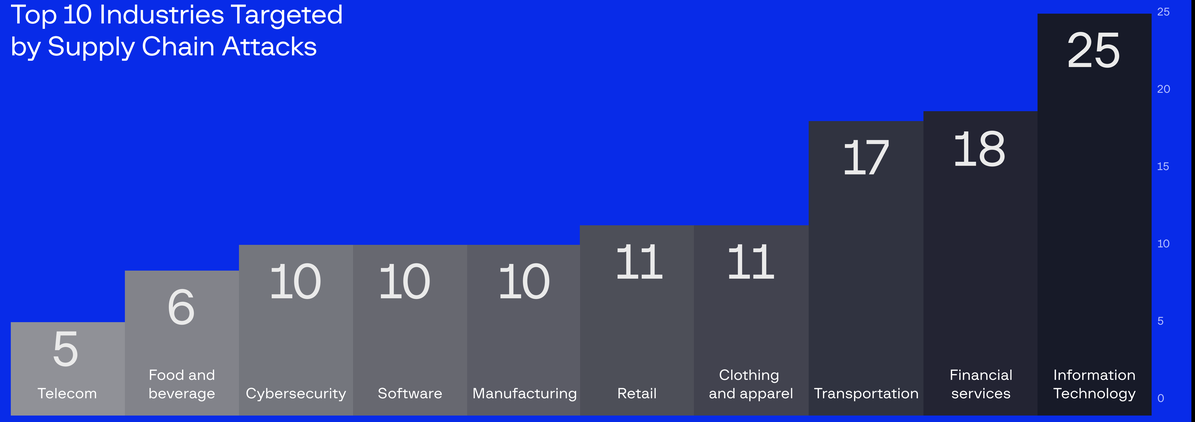
Nation-state groups increasingly mix espionage with financial gain and strategic disruption

Top 10 Jurisdictions Targeted by Supply Chain Attacks



2025

Top 10 Industries Targeted by Supply Chain Attacks



The Threat Landscape Ahead: Where Supply Chain Risk Is Headed

As organizations move toward 2026, the supply chain threat landscape will be defined by **acceleration, automation, and invisibility**. Attackers are no longer experimenting with supply chain compromise—they are industrializing it as the most efficient path to asymmetric impact.

AI-assisted tooling will dramatically compress attack timelines. Threat actors will autonomously identify weak maintainers, exposed OAuth scopes, vulnerable vendors, and misconfigured integrations at machine speed. Open-source repositories, browser extension marketplaces, CI/CD pipelines, and SaaS ecosystems will be continuously scanned, poisoned, and re-poisoned, shrinking the window between initial compromise and downstream exploitation from weeks to hours—or minutes.

Identity will become the dominant choke point. OAuth tokens, API keys, service accounts, and synthetic human identities will increasingly replace traditional malware as primary intrusion mechanisms. Because these access paths are legitimate by design, attackers will blend into normal business operations, extending dwell time and evading detection. Insider-style access—whether through stolen tokens or fabricated employees—will become the default model for long-term infiltration.

Multi-tenant and integration-centric breaches will also accelerate. Platforms that aggregate trust—CRM, ERP, HR, marketing automation, MSP tooling, and developer services—will be prioritized as high-impact targets. A single compromised integration or vendor account will increasingly expose hundreds of downstream organizations at once, transforming localized failures into systemic events.

Ransomware and extortion will further specialize along supply chain lines as access brokers, ransomware operators, and data brokers converge into tightly coordinated ecosystems. Rather than targeting end victims directly, attackers will focus upstream, where disruption produces cascading financial, operational, and reputational damage across entire industries.

At the geopolitical level, state-aligned and criminal threats will continue to merge. Nation-state actors will exploit commercial supply chains to obscure attribution, while cybercriminals adopt espionage-grade techniques. The most dangerous attacks ahead will not be the loudest, but the most trusted—embedded deep within digital ecosystems long before detection.

Mitigating and Countering Supply Chain Attacks

Defending against modern supply chain attacks requires a fundamental shift in how organizations define and protect their attack surface. Supply chain security can no longer be treated as a compliance exercise or vendor checklist; it must become a core security discipline.

Trust must be continuously verified rather than assumed. Software dependencies, browser extensions, APIs, OAuth applications, and third-party integrations should be treated as untrusted by default and monitored throughout their lifecycle. This demands visibility into how trust is granted, inherited, and abused—not just periodic risk assessments.

Identity must be secured as critical infrastructure. Defensive strategies must extend beyond user credentials to include OAuth tokens, service principals, API keys, CI/CD secrets, and machine identities. Continuous token monitoring, rapid revocation, strict scope control, and behavioral anomaly detection are essential to preventing silent lateral movement across interconnected platforms.

Organizations must gain end-to-end visibility into their digital supply chains, including open-source dependencies, SaaS integrations, MSP access paths, and browser environments. Early detection of weak signals—such as token misuse, developer environment compromise, stealer-log exposure, or anomalous SaaS behavior—is often the only opportunity to stop a cascading, multi-victim incident.

Upstream providers must assume they are prime targets. Software publishers, SaaS vendors, and service providers need to harden CI/CD pipelines, enforce mandatory code signing, implement strict OAuth governance, and continuously monitor privileged accounts. Downstream organizations must treat vendor security posture as an extension of their own risk.

Finally, incident response must evolve to reflect ecosystem-level reality. Future breaches will span vendors, customers, and partners simultaneously. Response planning, legal coordination, communications, and recovery strategies must be designed for multi-party impact.

The organizations that succeed will be those that stop defending isolated systems and start securing trust itself—across every relationship, identity, and dependency that powers their digital ecosystem.

At a Glance: Threat Actors and Malware Mentioned Within This Report

Group-IB customers may click on the following names of the threat actors and malware below for detailed analysis and information of the threat actors and malware prescribed within this report, via Group-IB's Threat Intelligence portal.

Supply Chain Focused Threat Actors

Scattered Spider 60

Lazarus 61

HAFNIUM 62

Shai-Hulud 63

888 64

DragonForce 65

Methodology

Group-IB's High-Tech Crime Trends report is an annual, intelligence-led assessment of how cybercrime is evolving—and where it is heading next. Grounded in the company's Glocal Vision, the report fuses deep, on-the-ground regional intelligence with global analytical modeling to move beyond situational awareness toward forward-looking risk insight.

Built on proprietary research, predictive intelligence, and real-world investigations, the report draws from Group-IB's presence in key cybercrime hubs worldwide. Analysts use specialized tooling to monitor dark web forums, dedicated leak sites (DLS), underground marketplaces, and criminal infrastructure, enabling early detection of emerging campaigns and shifts in attacker behavior.

Each year, researchers identify, validate, and correlate activity across advanced persistent threats (APTs), ransomware ecosystems, hacktivist operations, initial access brokers (IABs), compromised hosts, data leaks, phishing, and fraud schemes. By mapping observed activity to the MITRE ATT&CK framework and analyzing adversary tactics, techniques, and procedures (TTPs), the report connects isolated incidents into broader operational patterns.

This analytical foundation enables predictive intelligence: anticipating how threat actors will adapt, which attack paths are likely to scale, and where future risk will concentrate. Continuously refined and validated since 2012, this approach transforms historical threat data into actionable forecasts—making the report a trusted strategic resource for law enforcement agencies, enterprises, governments, and cybersecurity teams worldwide.

All technical information provided in this publication is shared solely for defensive cybersecurity and research purposes. Group-IB does not endorse or permit any unauthorized or offensive use of the information contained herein. The data and conclusions represent Group-IB's analytical assessment based on available evidence and are intended to help organizations detect, prevent, and respond to cyber threats.

Group-IB expressly disclaims liability for any misuse of the information provided. Organizations and readers are encouraged to apply this intelligence responsibly and in compliance with all applicable laws and regulations. This publication may reference legitimate third-party services such as Telegram and others, solely to illustrate cases where threat actors have abused or misused these platforms.

Contributions to Law Enforcement Operations in 2025

Since its inception, Group-IB has a strong advocate of private-public partnerships to combat the rising threat of cybercrime. The company is committed to strengthening global cybersecurity through close collaboration with law enforcement agencies worldwide.

In 2025, Group-IB supported 52 local and international law enforcement agencies across 6 operations globally by providing mission-critical data and investigative research. Through its network of Digital Crime Resistance Centers (DCRCs) strategically located across key regions, Group-IB can rapidly respond to investigative requests, delivering timely threat intelligence, digital forensics, and cybercrime expertise. This regional presence enables swift, coordinated action with authorities to disrupt cyber threats and dismantle criminal networks, reinforcing Group-IB's commitment to building a safer digital world.

52

Law enforcement agencies supported in 2025

1,809

Cybercriminals arrested as a result of Group-IB's contributions

310,643

Total number of victims of cybercriminal activities confirmed by law enforcement

Law enforcement operations per region in 2025

Malicious infrastructure and resources dismantled

34,838

Estimated total financial losses

due to cybercriminal activities | by cybercriminals

US$100M+

Timeline

2025

Arrest of ALTDOS

Region: Asia-Pacific **Agencies:** Singapore Police Force, Royal Thai Police

Cybercrime: Data leak, Cyber extortion

February

Group-IB aided Royal Thai Police and the Singapore Police Force in arresting a cybercriminal responsible for 90+ data leaks, including 65 in APAC, totaling 13TB of stolen data. Using aliases ALTDOS, DESORDEN, GHOSTR, and 0mid16B, he targeted industries like healthcare, finance, e-commerce, and logistics. His methods included SQL injection (sqlmap), exploiting vulnerable RDP servers, and deploying cracked CobaltStrike beacons for control. Unique tactics involved directly notifying victims' customers to pressure payments.

Operation Red Card

Region: Middle East and Africa **Agency:** INTERPOL

Cybercrime: Fraud, Scam, Phishing, Malware

Group-IB provided critical threat intelligence for Operation Red Card, which led to 306 arrests across seven African countries. The crackdown targeted banking, investment, and messaging app scams, impacting more than 5,000 victims. Nigerian police detained 130 suspects, seizing 26 vehicles, 16 houses, and 39 land plots, with some participants potentially coerced into the schemes. South African authorities dismantled a SIM box fraud network, seizing over 1,000 SIM cards, while Rwandan scammers stole US$305,000 through social engineering, with US$103,043 recovered.

Operation Secure

Region: Asia-Pacific **Agency:** INTERPOL

Cybercrime: Infostealer, Malware

April

Operation Secure dismantled a cybercriminal network using infostealer malware such as Lumma, Risepro, and META Stealer, which compromised data of more than 216,000 potential victims. Group-IB provided intelligence on command-and-control infrastructure, dark web, and Telegram accounts linked to malware distribution and stolen data sales. The operation led to 32 arrests, seizure of 41 servers holding over 100GB of data, and takedown of more than 20,000 malicious IPs/domains. Tactics included phishing, online fraud, and social media scams. Vietnamese police arrested 18 suspects, while Sri Lanka and Nauru authorities apprehended 14, identifying around 40 victims.

Timeline

2025

Operation Serengeti 2.0

Region: Middle East and Africa **Agency:** INTERPOL

Cybercrime: Ransomware, Scam, Business Email Compromise

August

Group-IB provided crucial threat intelligence and training for Operation Serengeti 2.0, sharing insights on cryptocurrency scams, business email compromise (BEC) infrastructure, and malicious networks. The operation led to 1,209 arrests across Africa, the dismantling of 11,432 malicious networks, and recovery of US$97.4 million, protecting nearly 88,000 victims. Highlights included Angola shutting down 25 illegal crypto-mining centers worth over US$37 million, Zambia disrupting a US$300 million investment scam, and Côte d'Ivoire stopping a US$1.6 million inheritance scam.

Operation Contender 3.0

Region: Middle East and Africa **Agency:** INTERPOL

Cybercrime: Scam, Sextortion

September

Leveraging Group-IB's investigative intelligence, law enforcement in 14 countries arrested 260 suspects and seized 1,235 devices linked to 81 cybercriminal infrastructures behind romance scams and sextortion schemes, which defrauded 1,463 victims of nearly US$2.8 million. Group-IB's High-Tech Crime Investigations team also traced the perpetrators' interactions and payment data, helping investigators follow financial flows and strengthen attribution.

Operation Big Bang

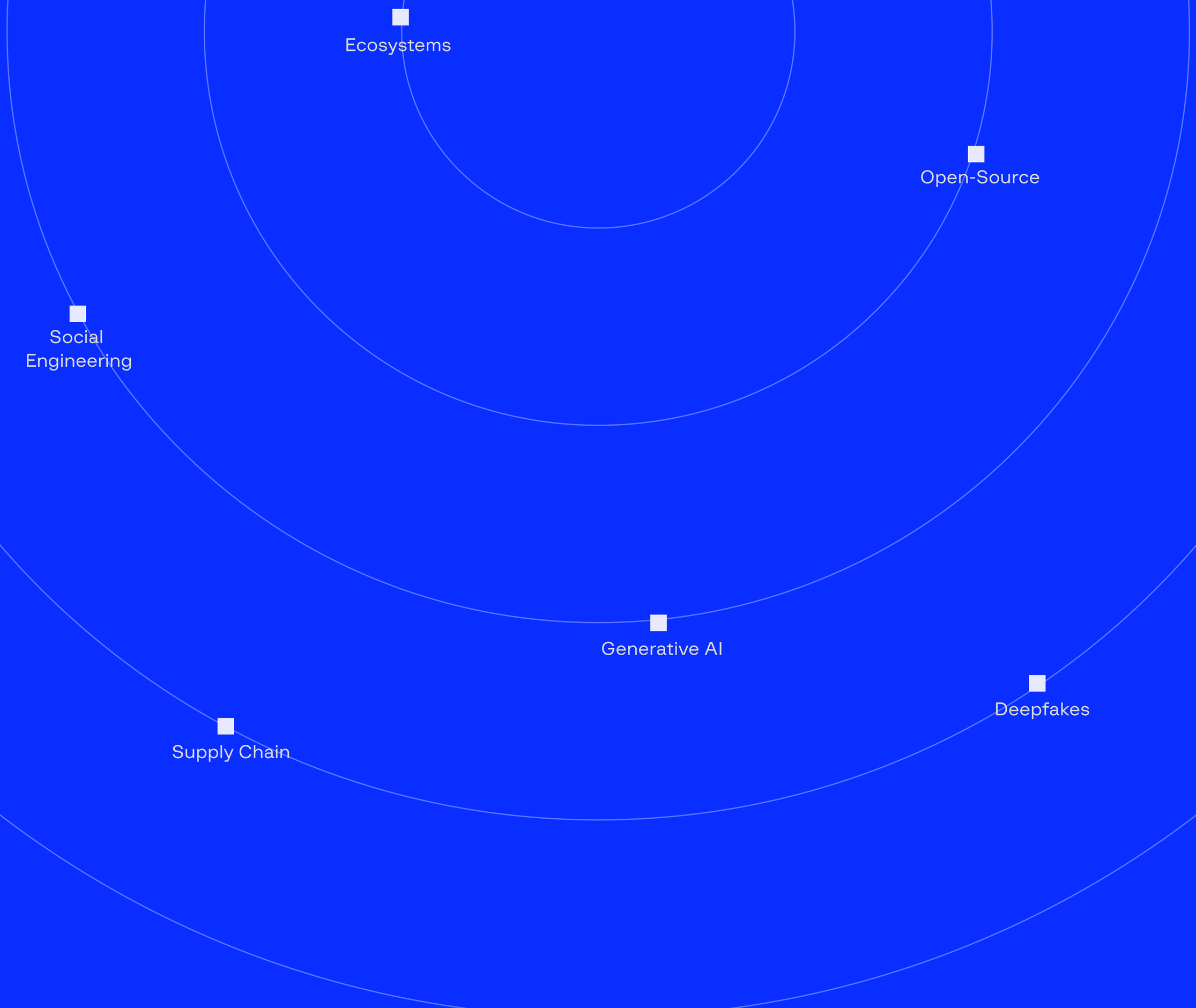
Region: Europe **Agency:** Guardia Civil (Spain)

Cybercrime: Phishing, Malware, Cybercrime-as-a-Service

October

Group-IB assisted the Spanish Guardia Civil in arresting a 25-year-old Brazilian national known as "GoogleXCoder," the mastermind behind the "GXC Team" Crime-as-a-Service (CaaS) ecosystem. Discovered by Group-IB in 2023, the syndicate developed and sold AI-powered phishing kits, Android malware, and voice-based scam tools to cybercriminals operating across Europe and the Americas. Through its investigation, Group-IB mapped the group's infrastructure, uncovering more than 250 phishing sites and nine Android malware strains, and provided intelligence that enabled coordinated law enforcement raids across six Spanish cities. The joint operation dismantled the CaaS network, seized its critical infrastructure, and recovered stolen cryptocurrency assets.

Chapter 1: The Age of Supply Chain Attacks: The Crisis of Trust Deepens



2025 marked a pivotal shift in the global threat landscape. What was once considered a hypothetical “worst-case scenario” — the compromise of software supply chains, third-party vendors, and even critical development infrastructure — has become disturbingly routine. This year proved that **trust itself has become the most exploited vulnerability.**

From open-source ecosystems and SaaS platforms to browser extensions and CI/CD pipelines, attackers have found increasingly effective ways to weaponize trust — not just within corporate systems, but among end users as well. A single compromise in the supply chain carries the potential to silently reach thousands of downstream victims.

At the heart of this shift is the erosion of confidence — not only among defenders and CISOs, but among everyday users who unknowingly install compromised software, trust malicious extensions, or interact with spoofed government services. As the boundaries between user and enterprise blur, stolen identities, and behavioral data harvested from trusted platforms can now be reused in highly targeted attacks.

Artificial Intelligence has accelerated this transformation. In 2025, we observed how AI-powered tooling lowered the barrier to entry for threat actors — enabling faster creation of phishing kits, more convincing impersonation, and scalable abuse of open-source software, authentication flows, and browser environments. AI didn’t invent supply chain attacks, but it made them cheaper, faster, and harder to detect.

This trend represents more than just a shift in adversary tactics — it signals a paradigm change in how cybercrime operates. Trust in the software and services we rely on daily is now a strategic liability if left unchecked.

Trust is no longer implicit — it must be verified, monitored, and secured continuously.

In this part, we break down the core threats that defined 2025 and explain how they will shape the attack surface of 2026. From phishing-as-a-service and evolving ransomware ecosystems to the exploitation of open-source software, third-party integrations, and the browser extensions, we outline how attackers are rewriting the rules — and why defenders must respond in kind.

The Fragility of Open-Source Ecosystems

A defining characteristic of supply chain threats in 2025 was the significant increase in attacks targeting open-source package ecosystems — specifically npm, PyPI, and others. These platforms serve as critical infrastructure for global software development, yet their decentralized and trust-based nature makes them highly susceptible to exploitation.

Several prominent examples:

- An example from early 2025 involved a campaign targeting Ethereum developers via npm. More than 20 malicious packages were uploaded using typosquatting tactics, mimicking legitimate Hardhat plugins. These packages were designed to exfiltrate sensitive information such as private keys, wallet credentials, and API tokens during installation. Since the compromise occurred during the development stage, the risk extended to production environments, creating downstream vulnerabilities in deployed services.

- On September 8, 2025, a threat actor compromised the NPM account of developer Josh Junon, known as “qix,” through a highly targeted phishing campaign impersonating NPM Support. The phishing link redirected victims to a cloned NPM login page. Once credentials were entered, the attacker gained full access to the victim’s NPM account. With this access, the actor modified 20 popular NPM packages inserting a JavaScript clipper into their source code. The malware monitored browser and app activity for cryptocurrency wallet interactions, replacing copied or used wallet addresses with attacker-controlled ones. It could detect and replace Bitcoin (BTC), Ethereum (ETH), Solana (SOL), Tron (TRX), Litecoin (LTC), and Bitcoin Cash (BCH) addresses, effectively diverting funds without user awareness.

  Discover how Group-IB’s Business Email Protection (BEP) could prevent an NPM supply chain compromise by detecting the initial phishing email that led to the developer’s infection.

- Later in September 2025, a more disruptive campaign emerged with the discovery of the Shai-Hulud worm. This malware initially compromised over **180 npm packages**, including widely used libraries like tinycolor. The worm propagated via stolen maintainer tokens and malicious preinstall scripts, enabling automated infection of additional packages upon installation. The worm’s speed and reach demonstrated how a single breach in open-source infrastructure could lead to widespread compromise.

- In November 2025, a second wave—dubbed Shai-Hulud 2.0—expanded the campaign’s reach dramatically. This iteration leveraged credentials harvested in the first wave to compromise near **800 packages**. This variant introduced a preinstall-phase payload, increasing exposure across developer machines and CI/CD environments. The malware was designed to exfiltrate GitHub tokens, npm credentials, session cookies, and local project files, uploading them to attacker-controlled GitHub repositories for persistence and further spread. If valid tokens were not found, a destructive payload triggered, corrupting local files to disrupt developer workflows.

- One of the most persistent APT groups abusing the npm ecosystem is Lazarus Group, which has repeatedly used malicious packages to deliver custom malware such as BeaverTail and InvisibleFerret. These tools are designed to steal cryptocurrency and sensitive user data, often targeting developers and blockchain-related organizations. Lazarus's activity highlights how nation-state actors increasingly exploit open-source platforms for targeted, financially motivated campaigns under the guise of routine development tools.

Output

These incidents demonstrate how open-source ecosystems have evolved into a critical attack surface — not just for opportunistic actors, but for highly organized campaigns capable of delivering multi-stage malware at scale. The trust-based nature of package management systems, combined with limited validation and widespread dependency chains, has amplified the blast radius of even a single compromise.

Future attack updates 2026

Threat actors can further aggravate this threat by using AI. AI could autonomously discover vulnerable maintainers, generate malicious packages, and orchestrate registry-wide attacks at machine speed. The barrier has dropped from needing a coordinated team of expert cybercriminals to a single operator who understands how to prompt an AI system.

This is no longer theoretical. In 2025, we already observed an S1ngularity campaign where the malware leveraged AI command-line tools (including Claude, Gemini, and Q) to aid in their reconnaissance efforts, and then exfiltrated the stolen data to publicly accessible attacker-created repositories within victims' GitHub accounts. With tooling improving and more models becoming accessible, such attacks are expected to proliferate rapidly in 2026, driving a new wave of automated supply chain compromise.

Countermove

In response, the industry is gradually moving toward stronger safeguards, including mandatory Software Bill of Materials (SBOMs), runtime dependency scanning, reproducible builds, secure development lifecycles (SDL), enforced package signing, and tighter controls on repository mirroring to reduce cross-ecosystem contamination.

The Rise of Malicious Extensions

Over the past three years, browser extensions have emerged as a persistent blind spot in enterprise and consumer security. Designed to operate with elevated privileges inside the browser, malicious extensions offer attackers direct access to session data, credentials, payment information, and national IDs — all before the data leaves the user's machine. Our analysis has uncovered extension frameworks capable of injecting code, intercepting POST requests, and tracking user activity across tabs and sessions.

In 2025, we observed a clear uptick in supply chain attacks abusing the browser ecosystem, particularly via trojanized or backdoored Chrome extensions. The growing number of campaigns demonstrates that browser extension abuse is no longer opportunistic — it is systematic, scalable, and increasingly integrated into broader financial and credential theft operations.

Several prominent examples:

$8.5 million

stolen via trojanized version of the extension

- One of the most damaging incidents occurred in December, 2025, when a malicious version of the Trust Wallet Chrome Extension (v2.68) was published to the Chrome Web Store outside of the vendor's standard release process. The trojanized version granted attackers access to sensitive wallet data and enabled unauthorized transactions directly from user accounts. Trust Wallet later confirmed that **2,520 wallets** were affected, with approximately **$8.5 million in assets stolen**. The stolen funds were traced to 17 attacker-controlled wallet addresses, highlighting how a single compromised extension in an official marketplace can trigger large-scale financial losses.

>2.6 million users

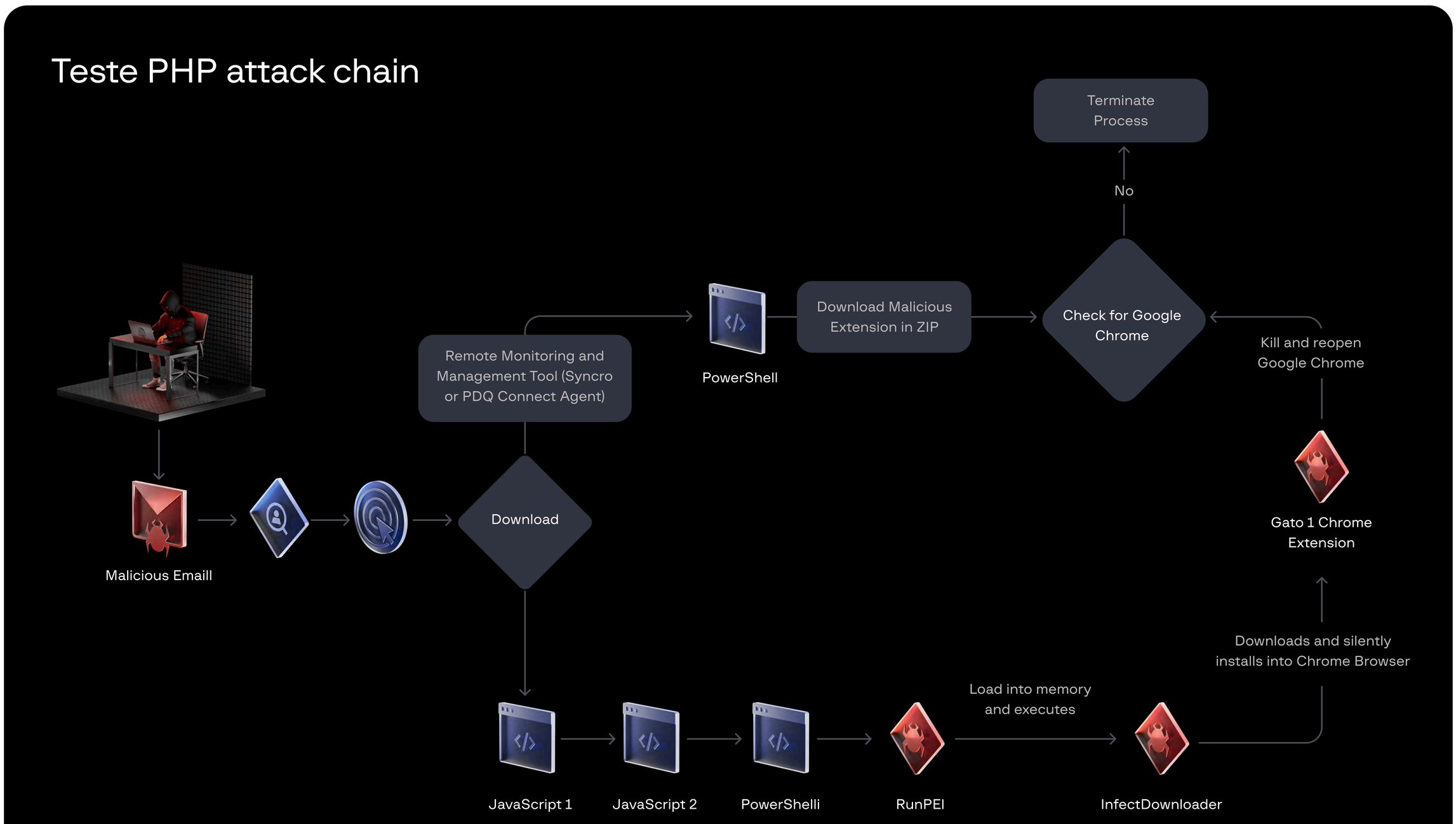
were affected across all compromised extensions

- A similarly impactful case unfolded on December 24, 2024, when Cyberhaven fell victim to a sophisticated phishing attack that compromised their Chrome extension, ultimately affecting around **400,000 users**. The attack began when a company admin received a phishing email claiming that Cyberhaven's extension violated Chrome Web Store policies. The admin was redirected to a malicious OAuth consent screen, granting the attacker access to manage the extension. With this access, the attacker uploaded a trojanized version of the legitimate extension, embedding code that targeted Facebook access tokens, business credentials, and AI and ad platform accounts. The Cyberhaven compromise was later linked to a broader campaign that tampered with over 35 Chrome extensions, impacting a combined user base of **more than 2.6 million**. This case illustrates how targeted phishing and OAuth abuse can turn even trusted browser tools into scalable attack vectors.

In parallel with high-profile global incidents, **Group-IB's threat intelligence operations** revealed **a significant uptick in malicious browser extension activity originating from Latin America**. A notable example is the **intrusion set dubbed** Teste PHP (Group-IB's name), first identified in **June 2025**, which has remained consistently active throughout the year.

This financially motivated activity targets **C-level executives** and **finance/HR departments** across industries, including banking and cryptocurrency platforms. The group primarily operates in **Portuguese- and Spanish-speaking countries,** such as **Brazil, Portugal, Chile, and Spain**.

Their campaigns rely on malspam delivery, leading to the download of **Remote Monitoring and Management (RMM)** tools and malicious extensions, including the **Gato1 Chrome Extension**. The goal is to steal credentials and gain unauthorized access to banking portals and financial services.



Despite frequent changes in **infrastructure** and **TTPs**, recurring patterns are observable: the same spammer infrastructure, malicious links embedded in email bodies, ZIP archives containing malicious extensions, PowerShell execution for payload deployment, and predictable infection flow — regardless of whether the initial vector is an RMM tool or obfuscated JavaScript.

These campaigns show that **browser-based compromise**, especially via extensions, is not only a problem of global scope but also a **regionalized and rapidly evolving threat vector** tailored to local targets and languages.

Output	Malicious browser extensions have matured into a scalable, evasive threat vector, capable of bypassing traditional endpoint and email defenses. In 2025, we saw widespread abuse of legitimate distribution channels (like the Chrome Web Store), targeted phishing of extension developers, and regionally tailored campaigns. These operations allowed attackers to harvest sensitive data, hijack sessions, and conduct financial fraud at scale.
Future attack updates 2026	We expect attackers to increase focus on supply chain infiltration via browser plugins, combining phishing, OAuth abuse, and automated extension deployment. A continued rise in global exploitation of this under-regulated vector is likely, driven by low technical barriers and high access rewards such as credentials, cookies, and full session hijack. AI-powered targeting and broader integration with IAB operations may further escalate the threat landscape.
Countermove	To address the growing exploitation of browser extensions, organizations must adopt a zero-trust approach to browser ecosystems, treating all extensions as potential threats. This includes enforcing strict allowlisting, minimizing permissions, and monitoring browser activity on endpoints — especially for high-risk user groups. Strengthening upstream defenses through secure development practices, OAuth restrictions, and hardened CI/CD pipelines is equally critical. As attackers exploit gaps in visibility and trust, centralized extension control, real-time monitoring, and rapid incident response capabilities will be essential to reduce risk and contain future abuse.

Phishing-Driven Identity Compromise in the Supply Chain

While phishing and social engineering attacks remain the primary initial access vector for supply chain attacks, **token compromise became far more visible and consistently observed in 2025**. In multiple incidents, one stolen OAuth token granted attackers entry into interconnected customer tenants, third-party services, or CI/CD pipelines. This enabled large-scale data exfiltration—spanning environment variables, cloud access keys, and embedded credentials stored in internal tooling—and allowed adversaries to pivot laterally, escalate privileges, and even tamper with application logic at scale. Rather than targeting individual users, attackers focused on **high-trust integrations**, transforming identity compromise into a multiplier for systemic breach.

This shift was fueled by the evolution of phishing and social engineering into a **data-driven, automated ecosystem**, powered by generative AI and attacker-specific LLMs. No longer constrained to bulk email spam, modern phishing campaigns scraped public data, replicated internal writing styles, and delivered hyper-personalized lures that convincingly impersonated trusted partners, vendors, and internal stakeholders. As a result, the boundary between legitimate business communication and malicious activity became increasingly difficult to distinguish, especially within complex supply chains.

A critical enabler of these attacks was the **abuse of OAuth and SSO workflows**. Threat actors routinely redirect victims through legitimate authentication flows to obtain OAuth tokens via phishing or social engineering. Unlike traditional credential theft, OAuth token compromise allows attackers to bypass multifactor authentication and gain legitimate, persistent access to cloud services, collaboration platforms, or CI/CD systems, often with elevated scopes or inherited permissions.

Adding to this complexity, deepfakes, mobile messaging platforms, and fake support agents added new layers of realism, further exploiting trust within distributed vendor ecosystems. As AI continues to lower the technical barrier to entry, defenders now face a surge of unique, automated attacks that not only exploit human trust, but to **hijack identity as a pathway into the supply chain itself.**

Below are several case studies Group-IB analyzed in 2025 that illustrate the evolving use of AI in phishing and scam operations, as well as common OAuth compromise scenarios that enabled downstream and supply chain-wide impact.

Example 1 OAuth Hijacking via Phishing-as-a-Service – Tycoon2FA

In 2025, Group-IB continued monitoring the Tycoon2FA — a sophisticated Phishing-as-a-Service (PhaaS) offering that has significantly lowered the barrier for carrying out adversary-in-the-middle (AiTM) attacks designed to bypass multi-factor authentication (MFA). First observed in late 2023, Tycoon2FA enables cybercriminals to intercept valid session tokens and cookies from Microsoft 365 and Gmail users, effectively allowing full session hijacking without password reuse or direct credential compromise.

Phishing campaigns powered by Tycoon2FA typically begin with an email lure containing a PDF or HTML attachment. These documents embed links like:

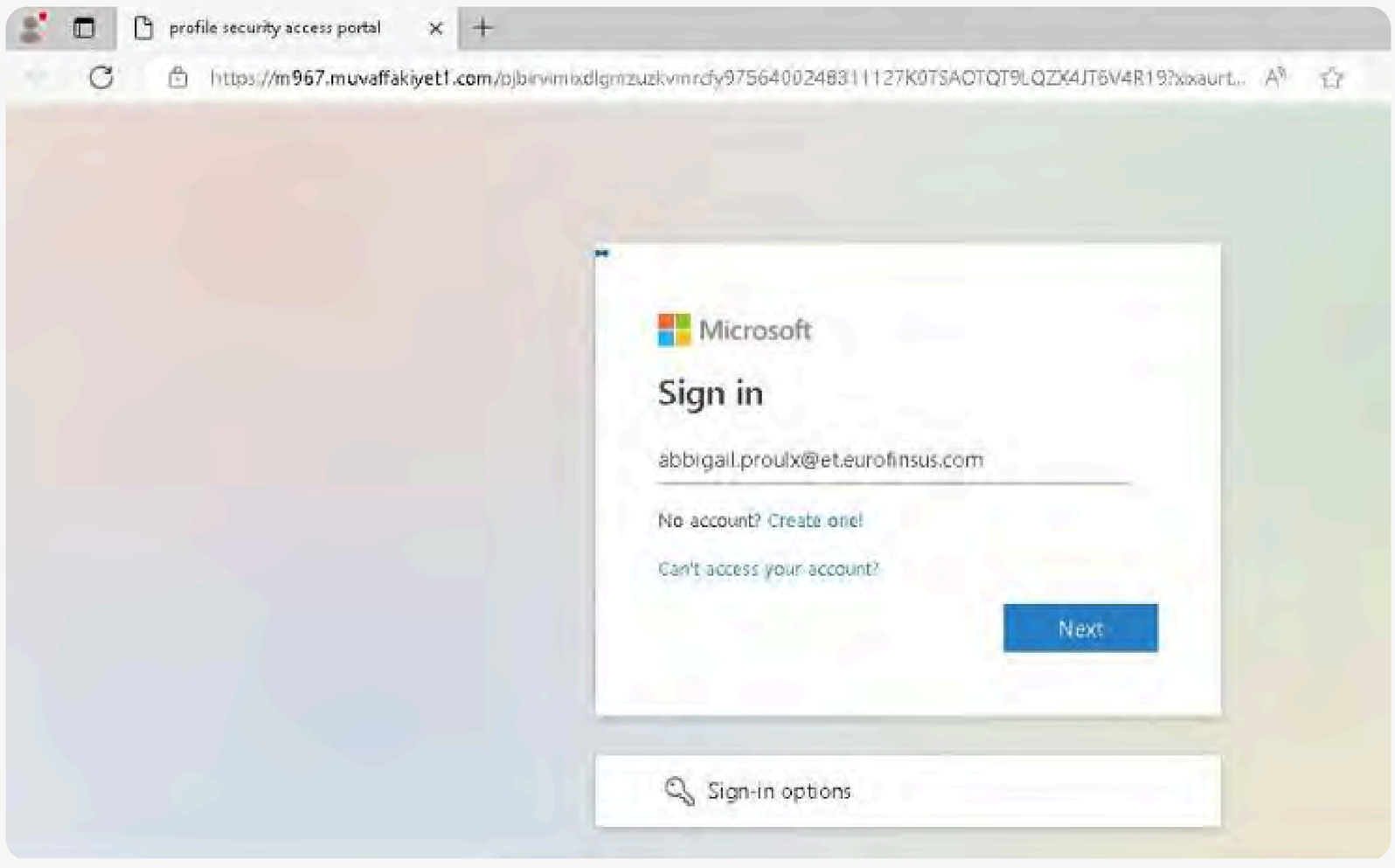
```
hxxps://malicious-domain[.]com/cllascio.php?token=XYZ
```

This tokenized URL identifies the specific campaign and victim. When clicked, the target is directed to a fake login page. The attack unfolds in real-time as follows:

01 The link loads obfuscated JavaScript that renders a fake but convincing login interface.

02 Once the victim enters their credentials and 2FA code, a POST request sends this data, along with session cookies and browser fingerprinting information, to the attacker's server.

03 These details are stored and immediately usable to hijack the session, bypassing MFA entirely.



A screenshot of a fake Microsoft 365 login page

Example 2 Autonomous Malspam Agents and Spam-as-a-Service

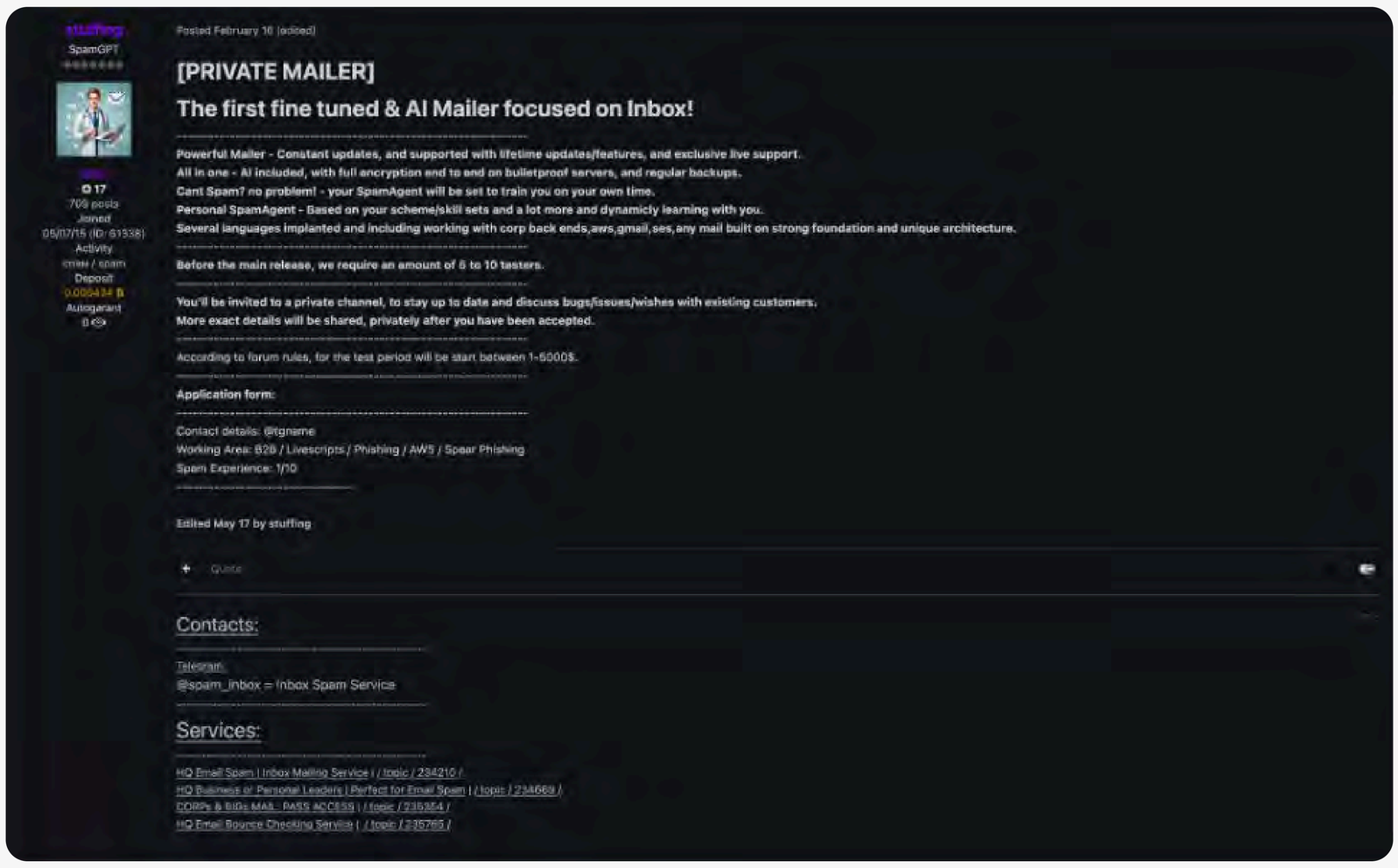
In 2025, malicious spam operations entered a new phase of automation. Traditionally dependent on SMTP-based bulk delivery and semi-manual scripting, malspam infrastructure is now being augmented with generative AI. Criminal actors increasingly deploy open-source LLMs to dynamically alter email content—adjusting HTML tags, rewriting text, and even modifying embedded images—to evade spam filters and enhance personalization.

The primary use cases include phishing, scam lures, and initial malware delivery. At least three AI-powered malspam tools are known to be active, with new variants emerging rapidly.

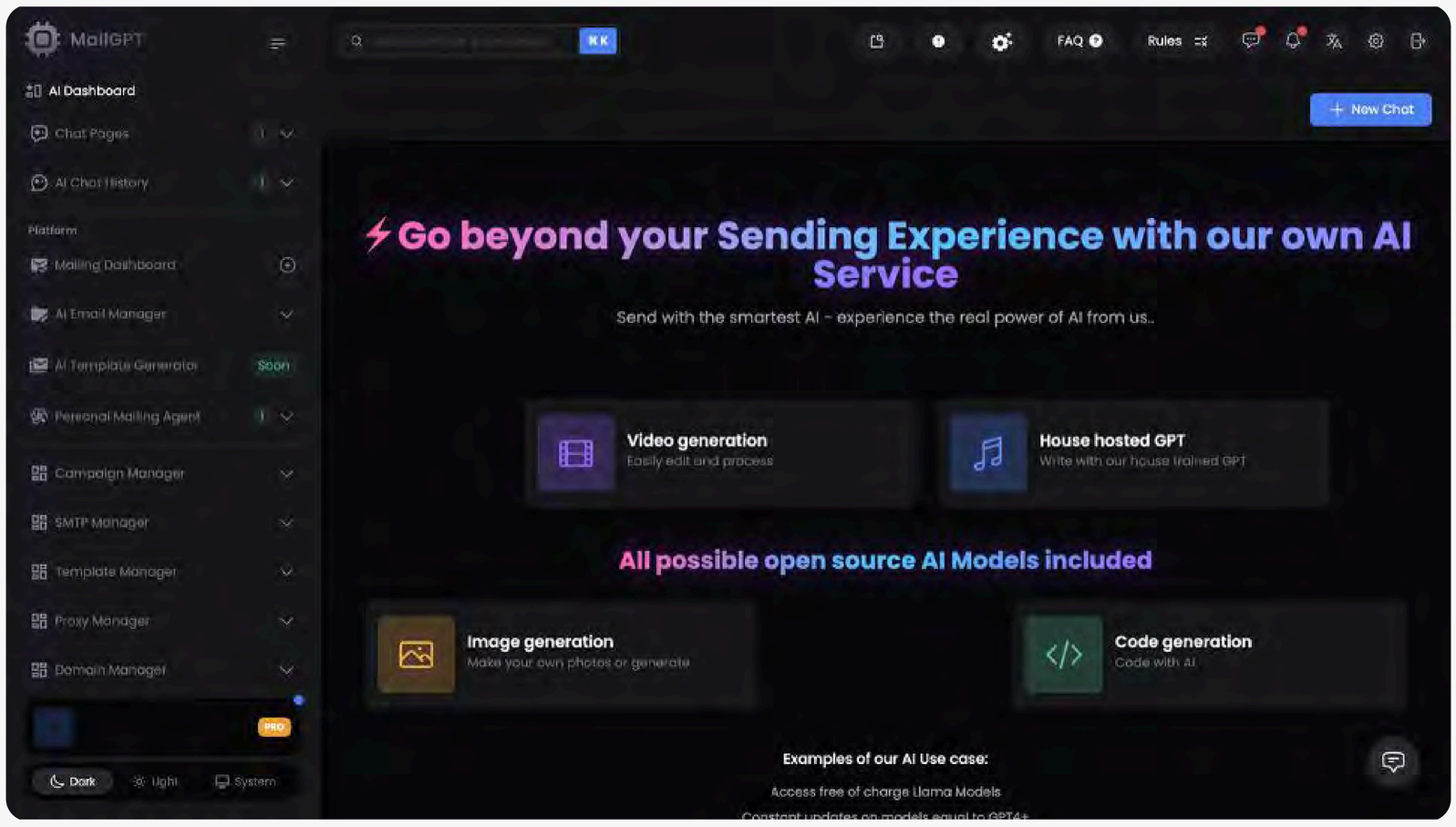
Notably, Group-IB discovered **SpamGPT**, an underground "Spam-as-a-Service" offering claiming to function as a fully autonomous spam agent. It leverages jailbroken models such as DeepSeek R1 and Qwen-2.5 to drive adaptive campaign logic. Key features include:

- End-to-end spam campaign automation via SMTP/Proxy/IMAP integration
- Screenshot-based email generation with AI-assisted segmentation and rewriting
- Custom-trained GPTs tailored to specific countries, schemes, and verticals
- Inbox testing and redirect validation in real time, including AWS/cracked corp setups

This reflects a growing trend toward fully autonomous, scalable malspam operations that reduce technical barriers and increase campaign effectiveness.



A screenshot of a post promoting a fully autonomous spam agent in a dark web forum



A screenshot of the interface of the fully autonomous spam agent

More information on the proliferation and abuse of AI in cybercrime in our Weaponized AI: Inside The Criminal Ecosystem Fueling The Fifth Wave of Cybercrime report.

Example 3 Phishing Page Generation with Generative AI – The Case of Xanders

In mid-2025, Group-IB identified an ongoing phishing campaign by a threat actor known as Xanders, believed to originate from Nigeria, targeting organizations in Malaysia. The actor used email lures leading to phishing pages designed to mimic file-sharing services. Victims were prompted to "log in" to access shared files, with stolen credentials exfiltrated via Telegram bots.

Closer examination of the phishing kits revealed several technical indicators suggesting the use of generative AI. Most notably, the HTML code of the pages included **instructional comments** typical of AI-generated content, reinforcing suspicions that tools like large language models were used to build them.

```
// Simulate credential validation
async function validateCredentials(email, password) {
    // In a real application, you would make an API call to your backend
    const validEmails = ['team1@company.com', 'team2@company.com', 'team3@company.com'];
    const validPassword = 'SecurePassword123';

    return validEmails.includes(email) && password === validPassword;
}
```

A screenshot of the HTML code of the phishing kits deployed by the threat actor known as Xanders, with instructional comments that is believed to be AI-generated content

Furthermore, the phishing pages used a permissive and unconventional email validation regex—

```
/^[^\s@]+@[^\s@]+\.[^\s@]+$/
```

—commonly generated by LLMs in response to general prompts. This pattern would allow invalid strings like “#@$.&” to pass as valid emails, something a human developer would typically avoid.

```
// Basic email format validation
function validateEmailFormat(email) {
    const re = /^[^\s@]+@[^\s@]+\.[^\s@]+$/;
    return re.test(email);
```

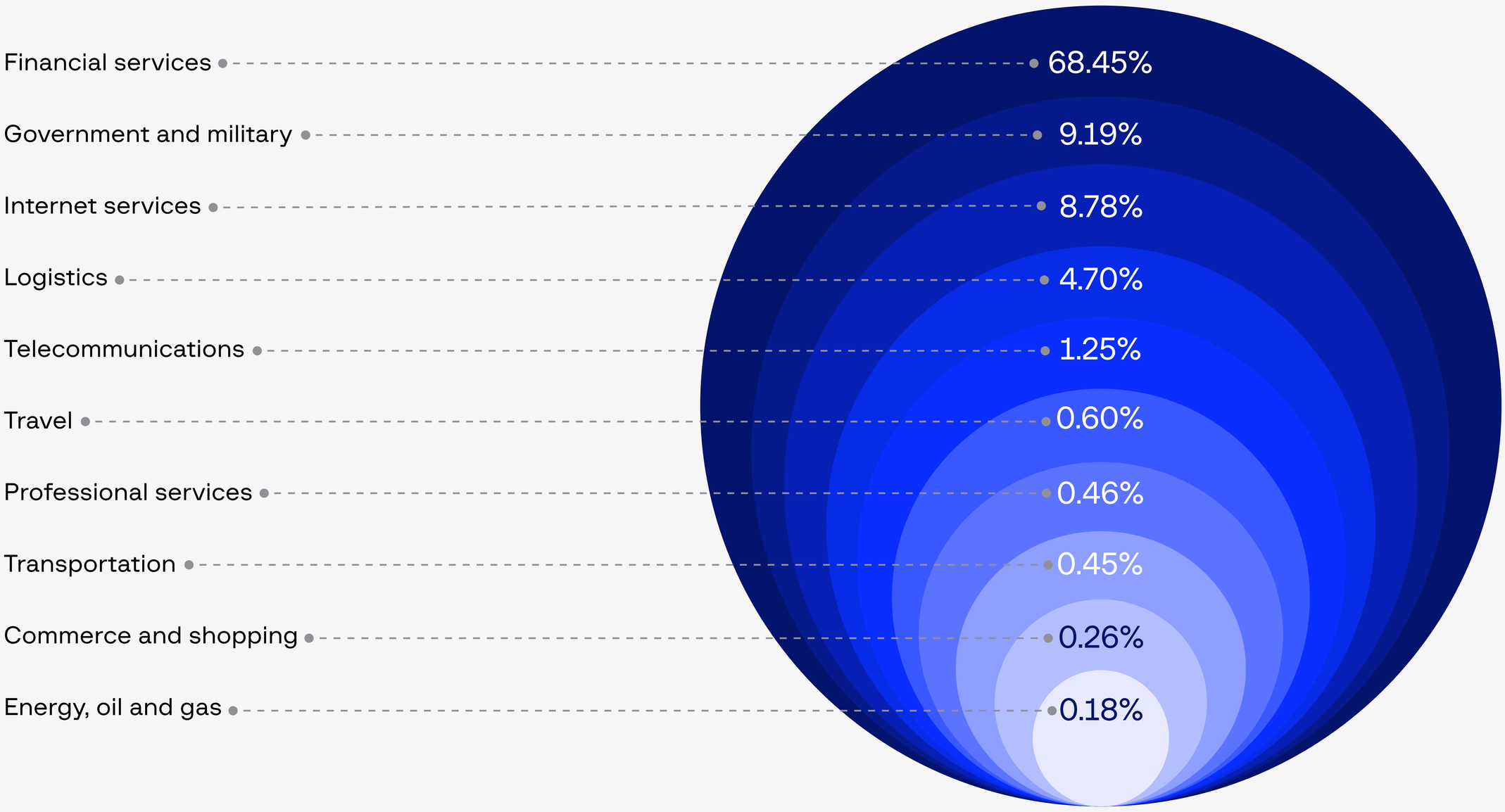
```
// Validate email
function validateEmail() {
    const email = emailInput.value.trim();
    const emailRegex = /^[^\s@]+@[^\s@]+\.[^\s@]+$/;
```

Identical regex pattern used for email validation. A snippet from a phishing page (top)in this campaign compared with AI generated code (bottom).

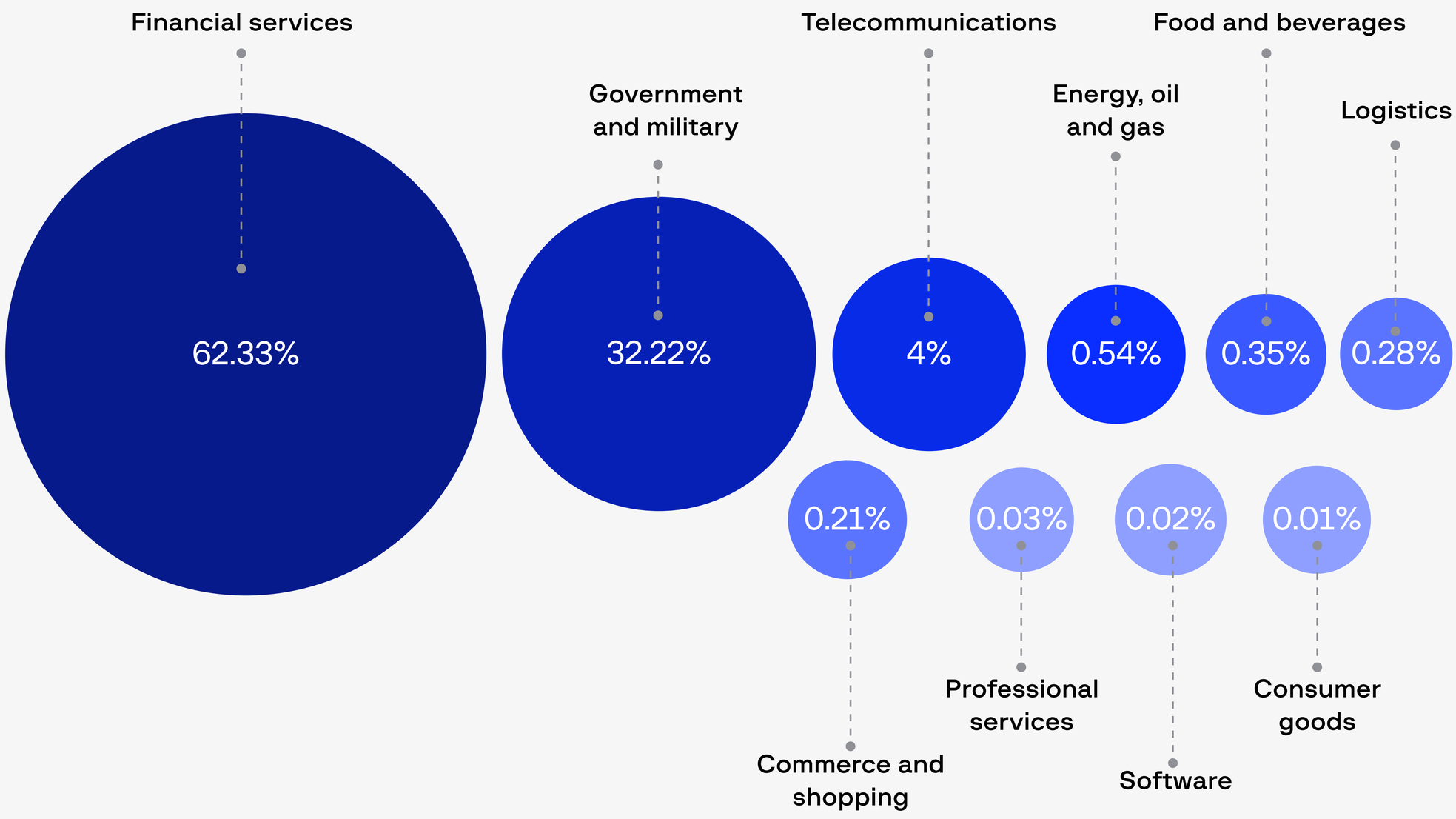
Testing with various AI tools (ChatGPT, Gemini, Vercel_v0, etc.) showed Vercel_v0 generated HTML most closely matching the phishing kits observed in this campaign. Its permissiveness and structural similarities strongly suggest that it may have been used to produce the pages. This case illustrates how low-skill actors are now able to generate functional phishing infrastructure using freely available AI tools, significantly lowering the barrier to entry.

Phishing Attacks in 2025

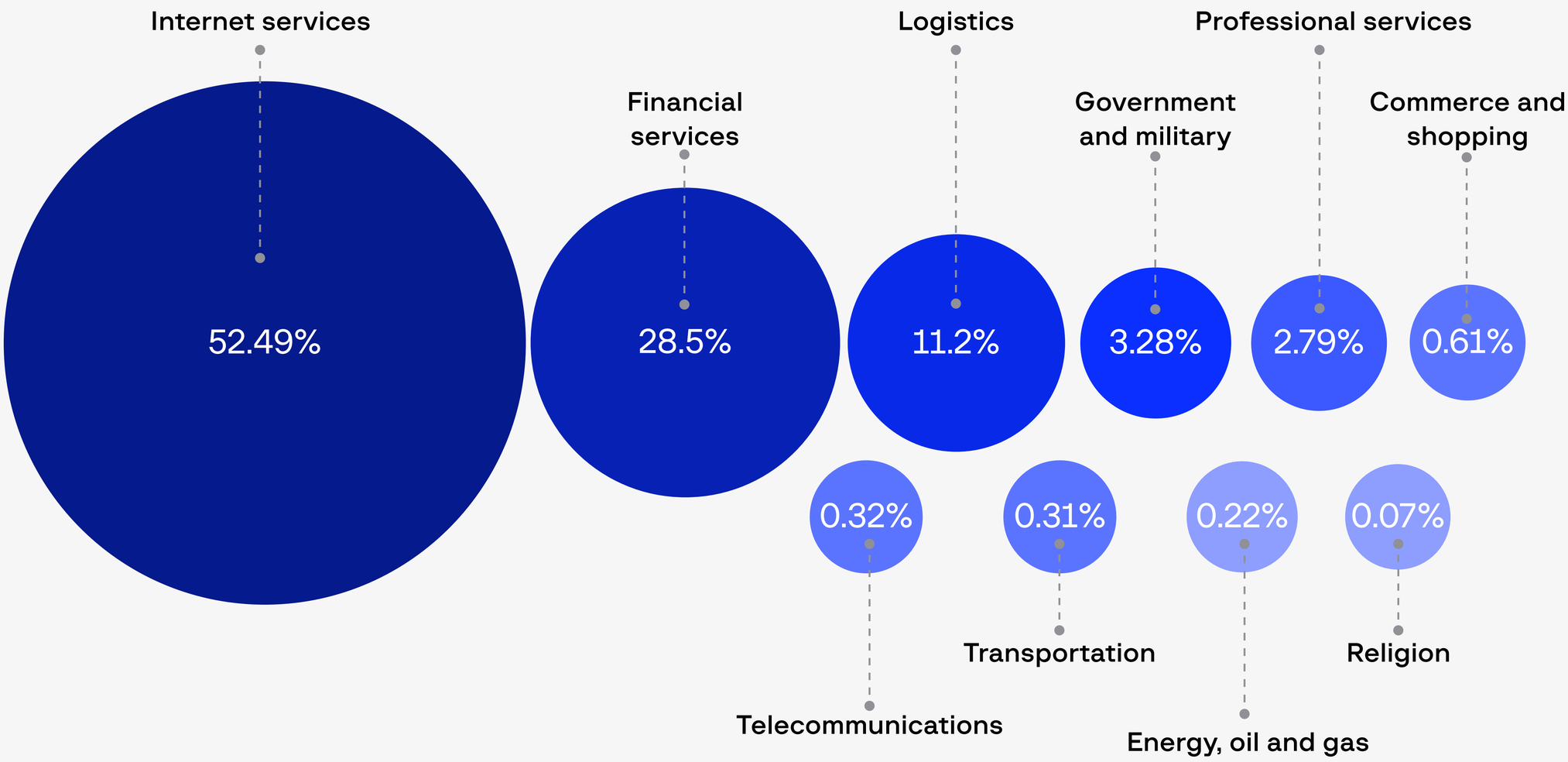
Global Top 10 Industries Targeted by Phishing Attacks in 2025



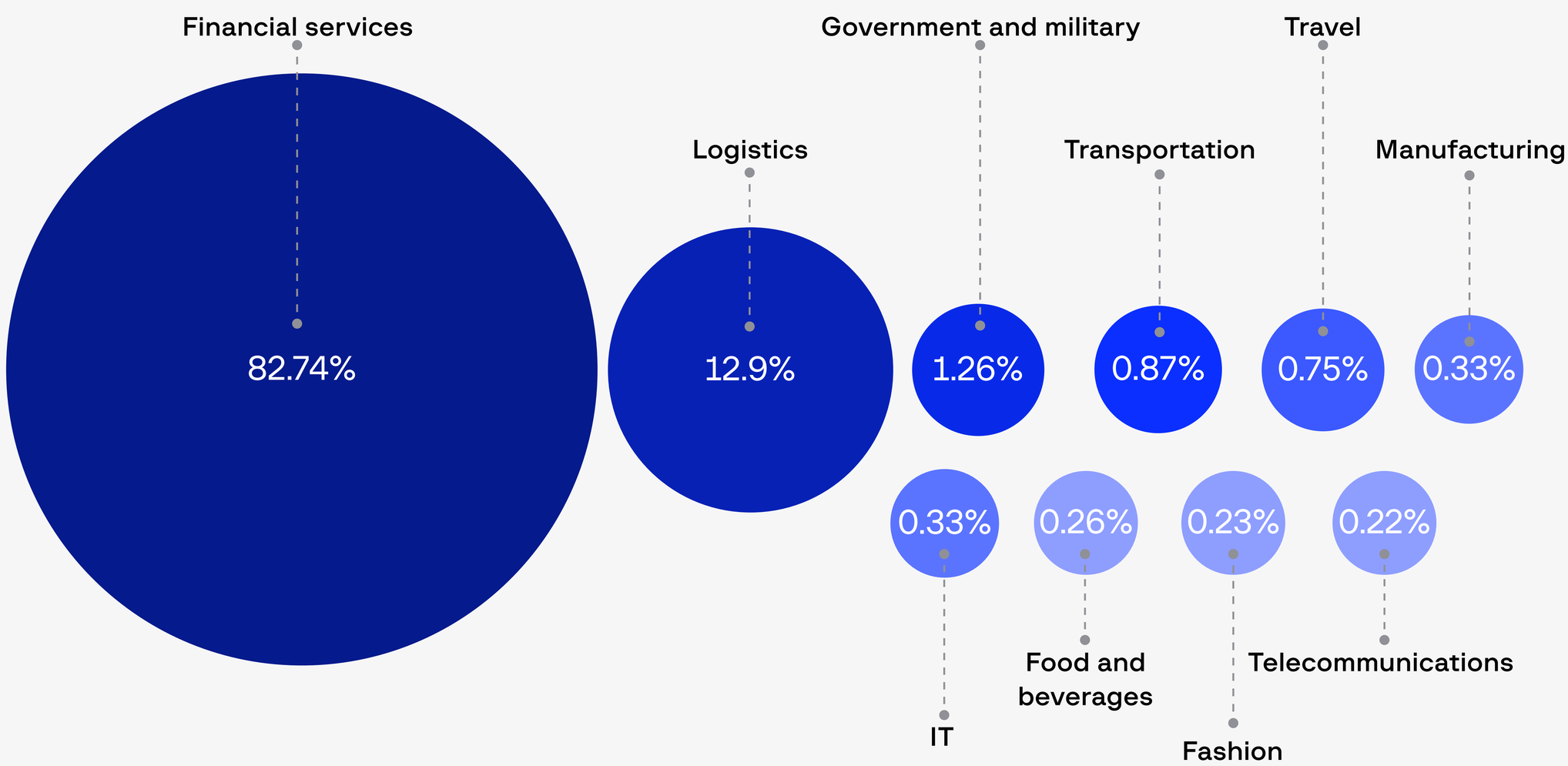
Asia-Pacific Top 10 Industries Targeted by Phishing Attacks in 2025



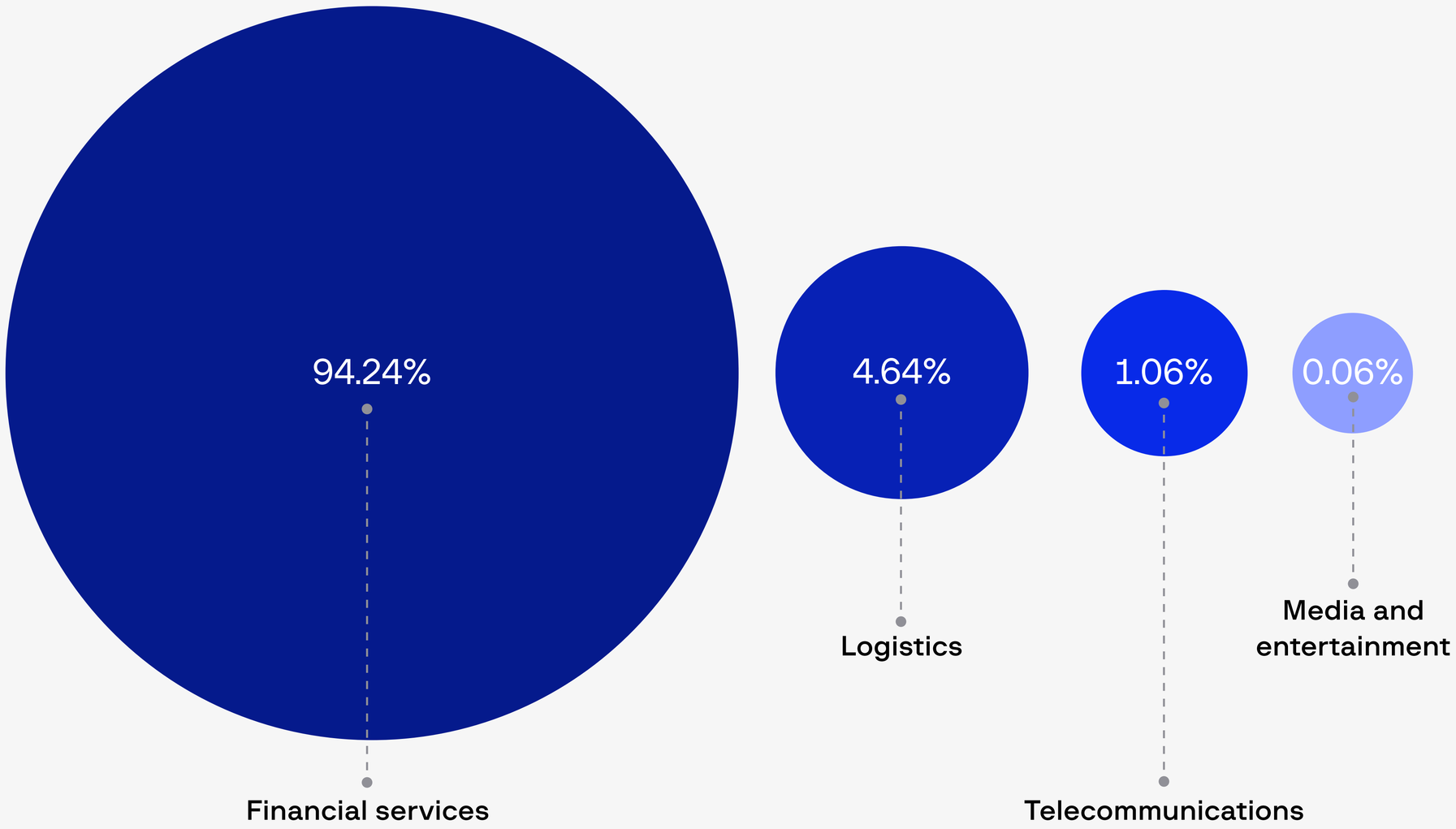
Middle-East & Africa Top 10 Industries Targeted by Phishing Attacks in 2025



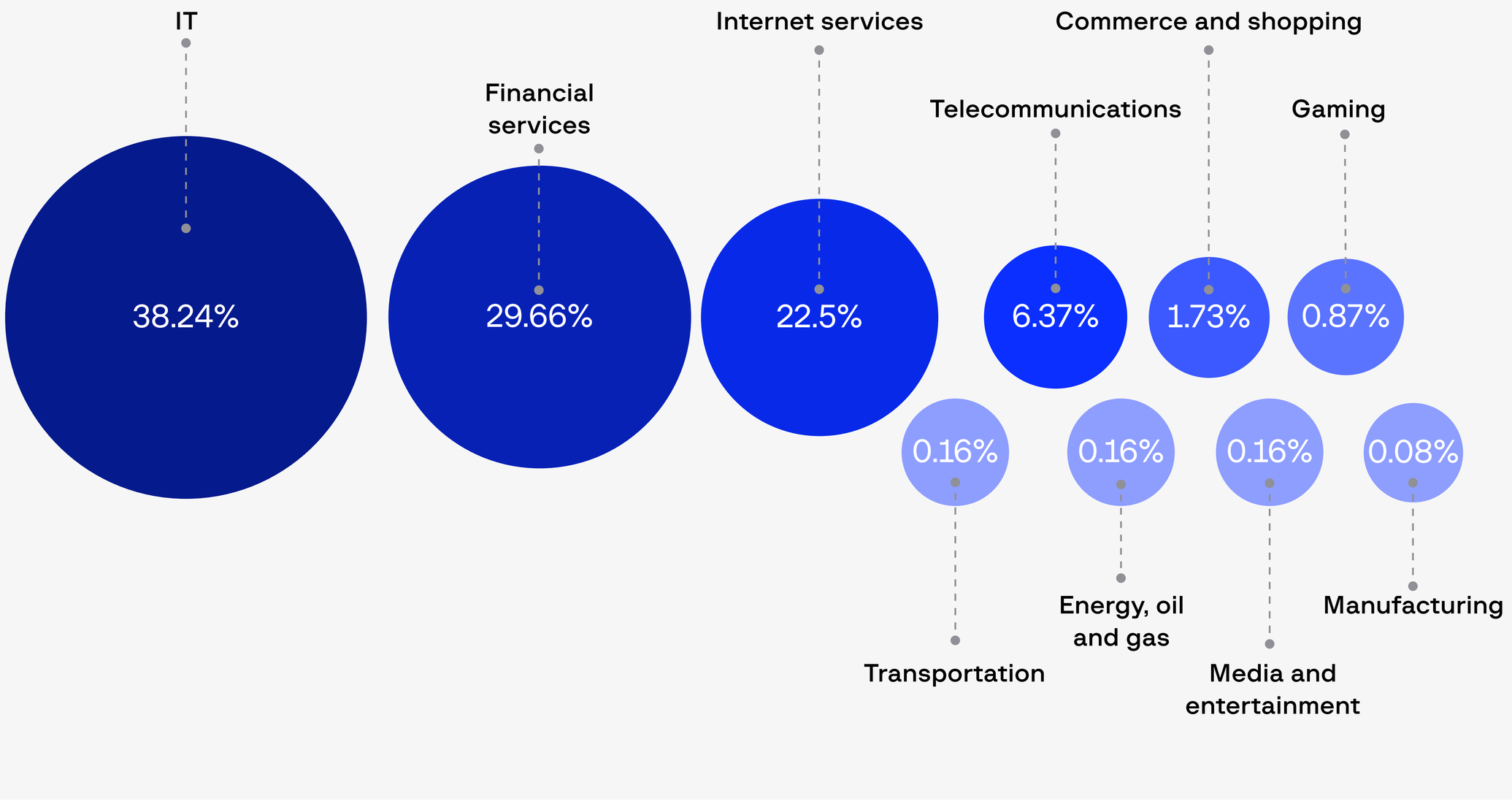
Europe Top 10 Industries Targeted by Phishing Attacks in 2025



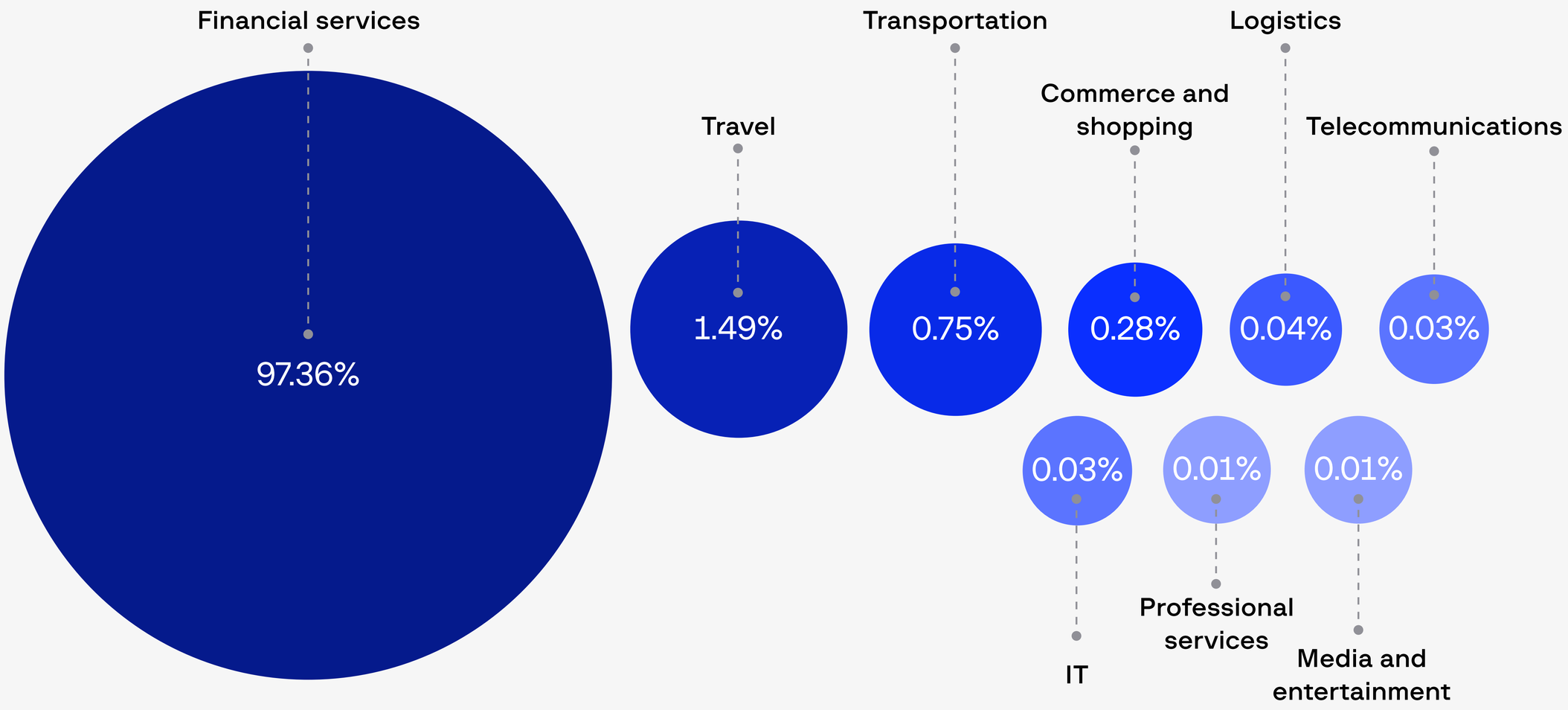
Central Asia Top Industries Targeted by Phishing Attacks in 2025



North America Top 10 Industries Targeted by Phishing Attacks in 2025



Latin America Top Industries Targeted by Phishing Attacks in 2025



The Evolution of Social Engineering in Supply Chain Attacks

Identity, Simulated: Deepfakes, Voice Spoofing, and the Rise of Insider Threats

In 2025, the weaponization of synthetic media evolved into a direct supply chain threat, transforming impersonation into a scalable mechanism for gaining trusted access across interconnected organizations. What once required manual effort and basic scripting has now evolved into industrialized impersonation driven by generative AI. Scam operations and intrusion operations now increasingly leverage AI-driven call center platforms that integrate SIP telephony, text-to-speech models, and fraud scenario orchestration into a single automated interface. These systems can now convincingly impersonate voices, simulate emotional cues, and adapt responses in real-time, dramatically increasing the effectiveness and scalability of voice phishing and social engineering against vendors, partners, and internal service providers embedded in the supply chain.

Lawrence Wong posted a tweet about the launch of the new project.

The story about Lawrence Wong's new project in the news broadcast.

A screenshot of an AI-generated deepfake video of Lawrence Wong, Prime Minister of Singapore, that was used in the Immediate Era fraud exposed by Group-IB.

At the same time, the underground economy supporting synthetic identities has expanded beyond short-term fraud into long-term access operations. Group-IB observed a growing market for impersonation toolkits, including cloned voices, deepfake avatars, and biometric datasets, available for as little as $5. These toolkits are increasingly used to facilitate long-term infiltration, not merely deception. AI-generated personas, complete with fabricated resumes, social media profiles, and pre-recorded interviews, are being deployed to gain employment in legitimate companies. Once employed, these synthetic “employees” operate as insider threats with access to internal systems, sensitive data, and third-party integrations. This evolution blurs the line between external and internal risk and trusted insiders within the supply chain. Rather than breaching through technical exploits, threat actors can now enter organizations by exploiting human trust, assuming legitimate roles that grant access to upstream and downstream systems. In complex vendor ecosystems, a single synthetic identity can enable lateral movement into partner environments, shared platforms, or customer networks. This marks a paradigm shift in identity abuse, where the supply chain compromise is no longer solely driven by vulnerabilities or exposed credentials, but by fabricated “humans” embedded directly into the operations of trusted organizations.

North Korean IT Workers as Synthetic Insiders

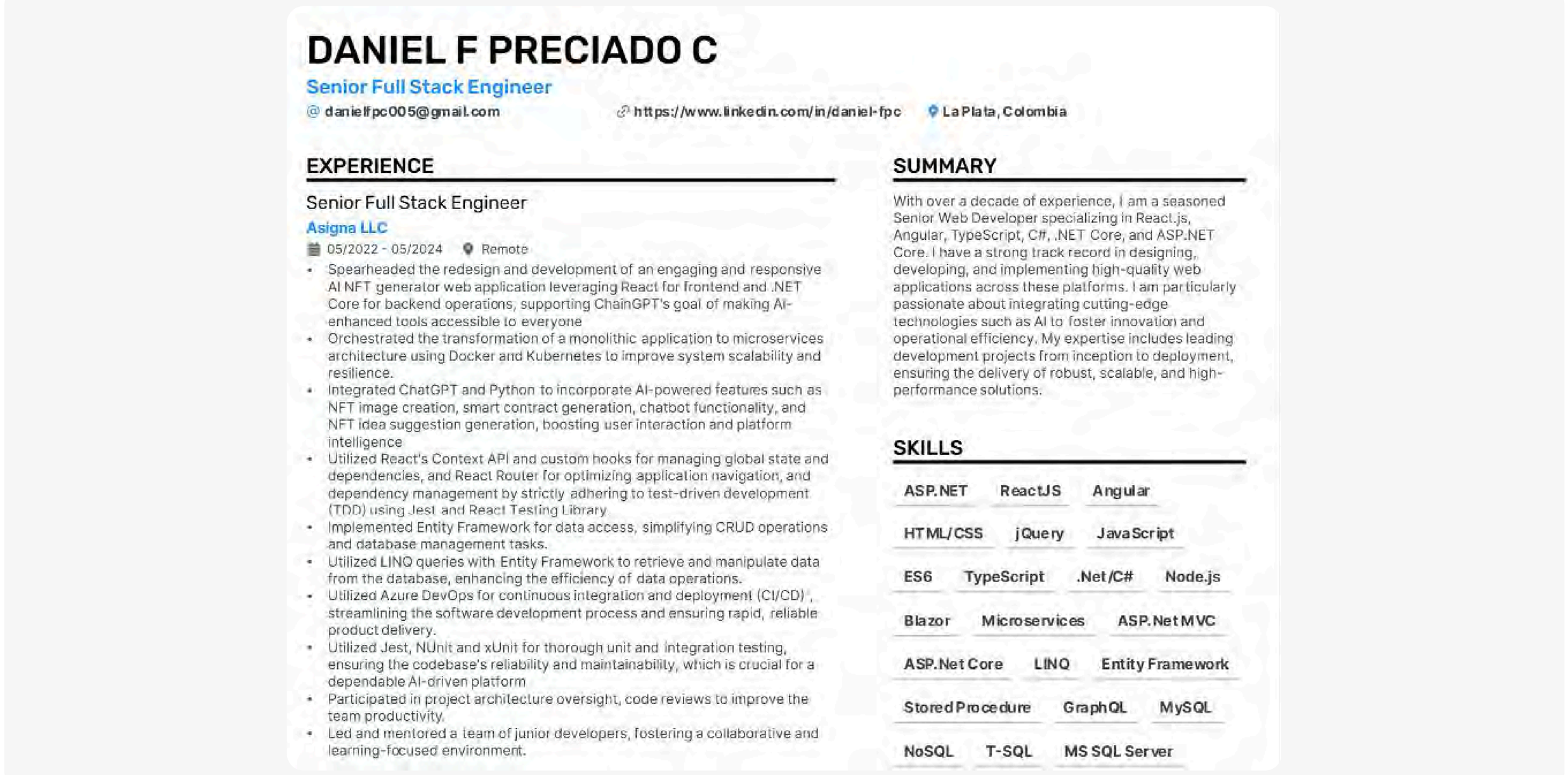
Among the most sophisticated examples of identity simulation in 2025 was the large-scale deployment of fake IT professionals by North Korean state-backed actors, identified under aliases such as Wagemole / Jasper Sleet / DPRK IT Workers. These operatives posed as remote developers, complete with fabricated identities, resumes, LinkedIn profiles, and even deepfaked video interviews, all tailored to pass corporate vetting processes.

More information regarding the activity and tools deployed by such threat actors can be found on Group-IB's Threat Intelligence portal.

Their tactics demonstrate a mature model of identity abuse and insider threat creation. From our monitoring, we've identified several recurring patterns in their setup:

01 Fake Identities & Employment History

- Use of fabricated resumes, false national identities, and even invented personalities.
- Theft and repurposing of legitimate employment documents and profiles.
- Creation of entire fake digital footprints to appear credible to employers.



DANIEL F PRECIADO C

Senior Full Stack Engineer

@ danielfpc005@gmail.com https://www.linkedin.com/in/daniel-fpc La Plata, Colombia

EXPERIENCE

Senior Full Stack Engineer

Asigna LLC

05/2022 - 05/2024 Remote

- Spearheaded the redesign and development of an engaging and responsive AI NFT generator web application leveraging React for frontend and .NET Core for backend operations, supporting ChainGPT's goal of making AI-enhanced tools accessible to everyone
- Orchestrated the transformation of a monolithic application to microservices architecture using Docker and Kubernetes to improve system scalability and resilience.
- Integrated ChatGPT and Python to incorporate AI-powered features such as NFT image creation, smart contract generation, chatbot functionality, and NFT idea suggestion generation, boosting user interaction and platform intelligence
- Utilized React's Context API and custom hooks for managing global state and dependencies, and React Router for optimizing application navigation, and dependency management by strictly adhering to test-driven development (TDD) using Jest and React Testing Library
- Implemented Entity Framework for data access, simplifying CRUD operations and database management tasks.
- Utilized LINQ queries with Entity Framework to retrieve and manipulate data from the database, enhancing the efficiency of data operations.
- Utilized Azure DevOps for continuous integration and deployment (CI/CD), streamlining the software development process and ensuring rapid, reliable product delivery.
- Utilized Jest, NUnit and xUnit for thorough unit and integration testing, ensuring the codebase's reliability and maintainability, which is crucial for a dependable AI-driven platform
- Participated in project architecture oversight, code reviews to improve the team productivity.
- Led and mentored a team of junior developers, fostering a collaborative and learning-focused environment.

SUMMARY

With over a decade of experience, I am a seasoned Senior Web Developer specializing in React.js, Angular, TypeScript, C#, .NET Core, and ASP.NET Core. I have a strong track record in designing, developing, and implementing high-quality web applications across these platforms. I am particularly passionate about integrating cutting-edge technologies such as AI to foster innovation and operational efficiency. My expertise includes leading development projects from inception to deployment, ensuring the delivery of robust, scalable, and high-performance solutions.

SKILLS

ASP.NET ReactJS Angular HTML/CSS jQuery JavaScript ES6 TypeScript .Net/C# Node.js Blazor Microservices ASP.Net MVC ASP.Net Core LINQ Entity Framework Stored Procedure GraphQL MySQL NoSQL T-SQL MS SQL Server

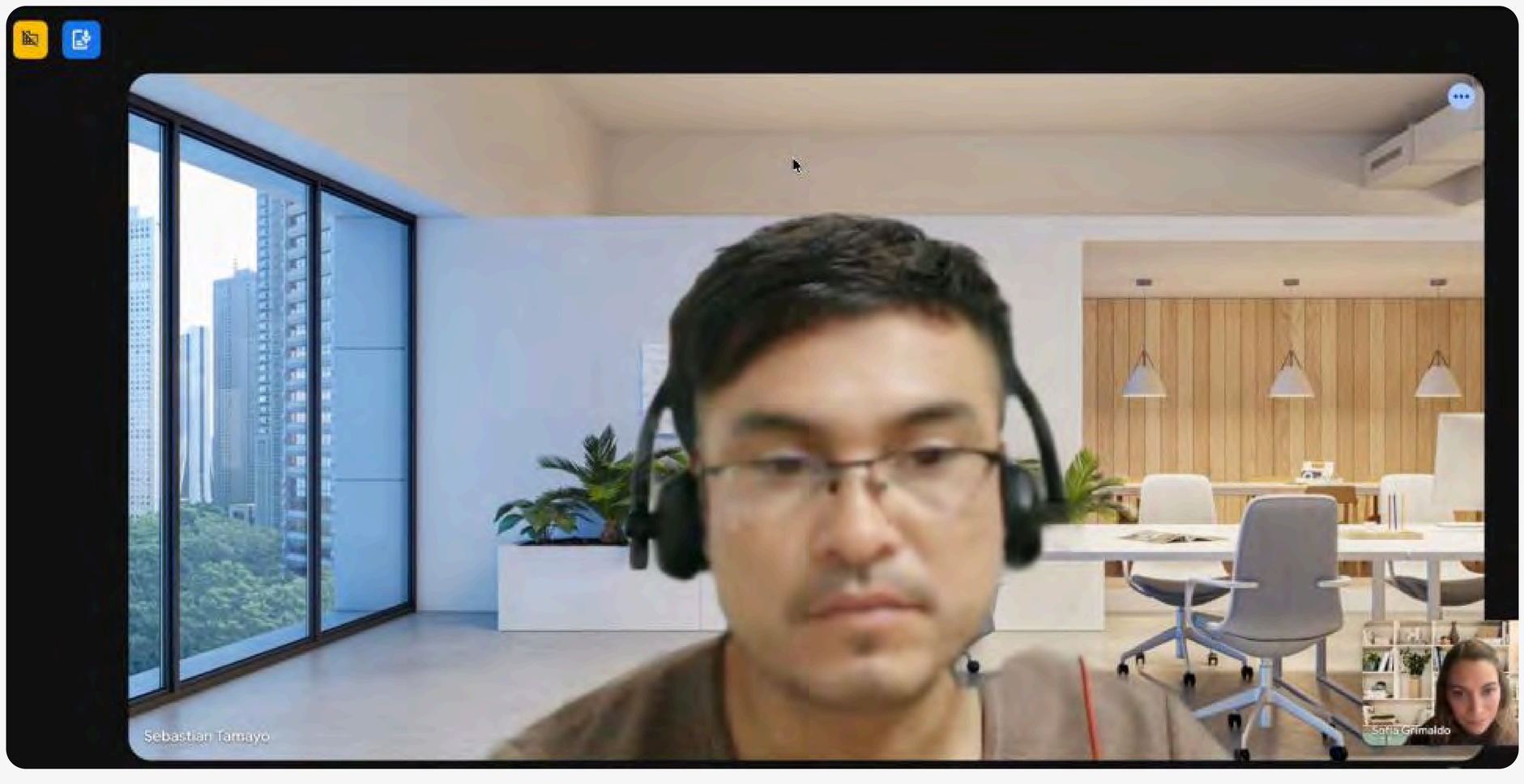
A screenshot of a fabricated resume used by a DPRK IT Worker, impersonating a job applicant

02 Hiring local co-conspirators

- Buying real-world documents (and person itself on salary) from non-IT individuals to pass local hiring checks.
- Receive and manage corporate devices in so-called laptop farms. This enables centralized control and persistent access to the internal environments of multiple organizations under the guise of legitimate remote work.
- Install remote access tools on corporate devices.
- Create and manage front companies which gives workers an appearance of being affiliated with a legitimate company.
- Use local residency status to acquire/maintain local bank accounts or local money transfer services to launder revenue.

03 Use of AI and Deepfake Tools

- AI-generated or enhanced photos to make professional-looking profile pictures.
- AI-assisted image manipulation to forge identity documents.
- Voice-changing software used during interviews and video calls to mask regional accents.
- Face-swapping software to impersonate someone else during video calls.



A screenshot of a video interview, where a North Korean IT worker impersonates an applicant.

04 Evasion & Deception

- Workers avoid detection by using VPNs, remote infrastructure, false locations, and rented phone numbers.
- Communication conducted through anonymized platforms or through ghost employees (“rented” real person).
- Often apply for roles across various freelance platforms or remote job boards.

05 Objectives & Impact

- Primary goal: Generate foreign currency for the North Korean government, likely funnelled through state-controlled entities.
- Secondary goal: Potential for insider access and espionage, depending on employer and access level.
- There have also been a minority of cases where workers exfiltrated sensitive information for extortion. Such incidents are likely to be opportunistic in nature.
- Risks to companies include data leakage, unauthorized access, financial fraud, and regulatory violations (e.g., sanctions evasion).

06 Notable Characteristics

- Actors are often technically skilled and capable of passing technical interviews.
- They prioritize long-term employment, blending into development teams and collecting salaries.
- Some are linked to cybercriminal markets and may contribute to broader DPRK cyber operations, like cooperation with Lazarus for delivering BeaverTail infostealers and OtterCookie backdoors.

This type of operation blends identity fraud, deep social engineering, and long-term infiltration. It's a clear demonstration of how synthetic identities—both digital and physical—are being industrialized to bypass traditional trust-based hiring and access models.

Output

Impersonation-based attacks matured into a strategic threat vector in 2025. The widespread availability of generative AI lowered the entry barrier for creating convincing voice and video deepfakes, while synthetic identities enabled long-term infiltration of organizations. Threat actors combined these tools with compromised/rented/generated accounts, real-world documentation, and remote access setups to operate as embedded insider threats - undetected for months or to get a big quick profit.

Countermove

Effective mitigation of synthetic identity and insider threats requires a security pipeline that starts with robust pre-employment vetting: verifying candidate digital presence across developer ecosystems, conducting mandatory real-time video interviews with facial liveness detection, and validating resume claims via credential checks and contribution analysis. During onboarding, organizations should perform device attestation and baseline behavioral profiling. Post-access, technical controls must include continuous monitoring of remote endpoints for unauthorized tooling (e.g., RMM platforms, tunneling software), geolocation/IP inconsistencies, and signs of scripted interaction or automation. Role-based access should be tightly scoped and escalated only after contextual review. Behavioral analytics can help surface anomalies such as uniform work hours across time zones, excessive background activity, or lateral exploration outside job scope. Over time, organizations should invest in internal upskilling and reduce reliance on external or freelance labor in roles with persistent access or elevated privileges.

Data Breaches as a Supply Chain Attack Multiplier

The year 2025 marked a turning point in how data breaches are conducted, monetized. While previous years were often defined by a handful of large, isolated leaks, the breaches of 2025 revealed a strategic shift: threat actors moved upstream, targeting individual organizations to compromise third-party vendors, SaaS platforms, and integration layers that serve as trust anchors for thousands of downstream customers.

This shift introduced a new kind of breach logic entirely. Rather than breaching one target for single payoff, threat actors began targeting service providers whose privileged access could cascade across hundreds of client environments. OAuth tokens, and misconfigured partner access became prime attack vectors. In many cases, a single compromised account or vendor system enabled attackers to move laterally, exfiltrating data, delivering malicious updates, or abusing trusted contact lists to conduct fraud at scale.

As a result, data breaches in 2025 were no longer isolated security failures; they became supply chain events with compounding impact. A breach at one node reverberated across partners, customers, and platforms, amplifying both operational disruption and financial risk far beyond the original victim.
This evolution also transformed how leaks are shared and sold. In April 2025, BreachForums, one of the most prominent underground leak forums, was shut down once again, triggering disruption across the leak-as-a-service ecosystem. While some actors disappeared or moved underground, others seized the opportunity: new channels emerged, old sellers migrated, and even previously untrusted forums like DarkForums evolved into active hubs for breach data, essentially becoming a scaled-down replacement for BreachForums.

In this section, we explore how the supply chain breach model matured in 2025, the incidents that shaped it, and why the breach economy is no longer about one leak, but many victims.

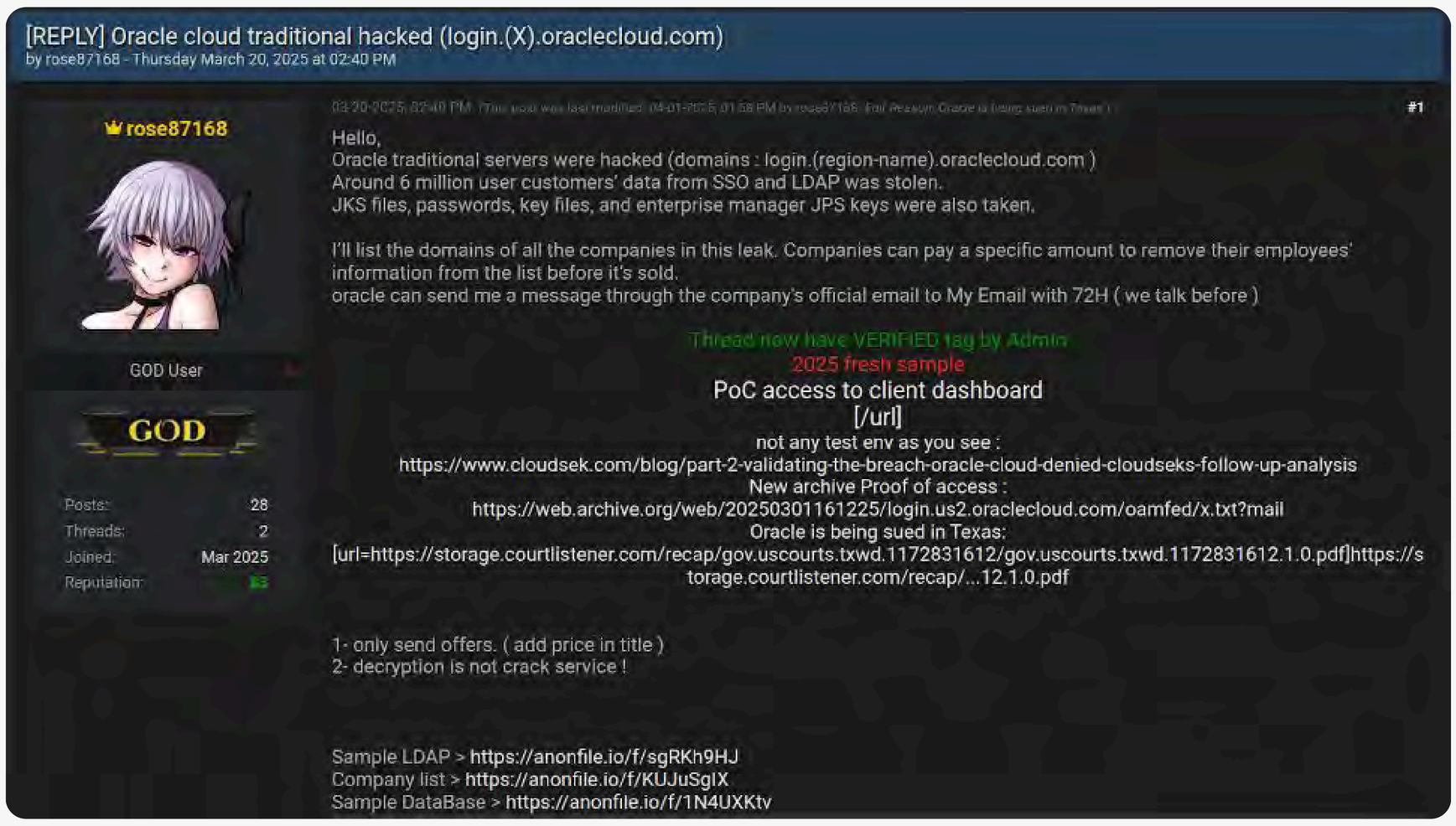
Example 1 Oracle Cloud Breach by 'rose87168'

In March 2025, a threat actor known as **rose87168** claimed responsibility for a breach of Oracle's legacy cloud infrastructure, specifically

```
login.<REGION>.oraclecloud[.]com
```

The actor stated they had obtained data on approximately **6 million users**, including:

- Encrypted SSO passwords
- LDAP hashed credentials
- Java Keystore (JKS) files
- Key files
- Enterprise Manager JPS keys
- Additional user metadata



A screenshot of a post by rose87168 claiming responsibility for a breach of Oracle's legacy cloud infrastructure

According to the attacker, access was gained by exploiting a **known Java vulnerability** in Oracle's **Gen 1 (Cloud Classic)** environment — infrastructure that Oracle reported as "legacy" and no longer in active use, though evidence suggests the attacker was present in the system as early as **January 2025**.

Oracle privately notified affected clients and emphasized that its Gen 2 infrastructure was not impacted, while confirming that the FBI and CrowdStrike had been engaged in the investigation.

Group-IB Threat Intelligence analysts established contact with **rose87168** and were able to **obtain and analyze samples** of the stolen data, as detailed in this Threat Intelligence report. Based on our assessment:

- The actor shared **two user data** files containing more than **1,700 unique domains** (the total number of unique domains from the list previously published by the attacker is 128,465 unique domains).

- The sample included user data such as names, email addresses, job titles, hashed passwords (SHA-1/SHA-256), phone numbers, manager relationships, login attempts, account status flags, and more.

- Importantly, **timestamps** such as `USR_UPDATE` showed that at least part of the data was current as of **February 26, 2025**, confirming recent access.

- Cross-referencing revealed that a number of email addresses from the sample were compromised in public stealer logs. These stealer logs recorded attempts by these users to log into various websites with Oracle domains. This indirectly indicates that the users from the sample may indeed be Oracle customers.

While the attacker initially advertised the breach on a leak forum, and some data samples were later shared in the public domain and media for independent analysis, the full dataset was never comprehensively published. According to the actor, a portion of the data obtained by Group-IB had not been shared with journalists, researchers, or made publicly available, indicating a selective disclosure strategy.

This case underscores how even legacy infrastructure at a widely trusted vendor like Oracle can serve as an entry point for multi-tenant exposure. Although the affected systems were positioned as non-production, the leaked credentials, integration points, and user metadata could be used to facilitate downstream exploitation — including supply chain pivoting, credential stuffing, and trusted phishing operations.

Given the size of Oracle's customer base and the attention the incident attracted across underground forums and media, this breach became a focal point for both threat actors and defenders in early 2025, and may have contributed to the broader enforcement pressure that culminated in the shutdown of BreachForums in April 2025.

Example 2 Salesloft–Drift–Salesforce Compromise and the OAuth Breach Chain

In one of the more complex and cascading breaches of 2025, unknown threat actors exploited OAuth tokens to move laterally across multiple integrated systems — starting with Salesloft's Drift chatbot and extending into Salesforce and other connected platforms. The incident highlights how compromised third-party integrations can serve as **multipliers** in modern supply chain attacks, enabling attackers to exfiltrate data from multiple environments using a single point of access.

Timeline and Key Facts

March–June 2025

Threat actor gains access to Salesloft's GitHub repositories, adds a guest user, and establishes initial workflows. Reconnaissance observed in both Salesloft and Drift environments.

Access to Drift's AWS environment enables attackers to extract OAuth tokens associated with customer integrations.

August 8–18

Attackers use the tokens to access sensitive data across connected Salesforce environments, including:

- Account metadata
- Support case content
- AWS credentials
- Snowflake tokens
- User passwords and internal notes

August 20

Salesloft and Salesforce jointly revoke all active OAuth tokens and remove Drift from AppExchange.

August 26

Google Threat Intelligence Group (GTIG) issues public warning that the breach extends beyond Salesforce and advises clients to assume token compromise across multiple platforms.

August 28

GTIG reveals that a subset of Google Workspace accounts integrated with Drift were also accessed. Further alerts extend to Slack, AWS, and other services.

Early September

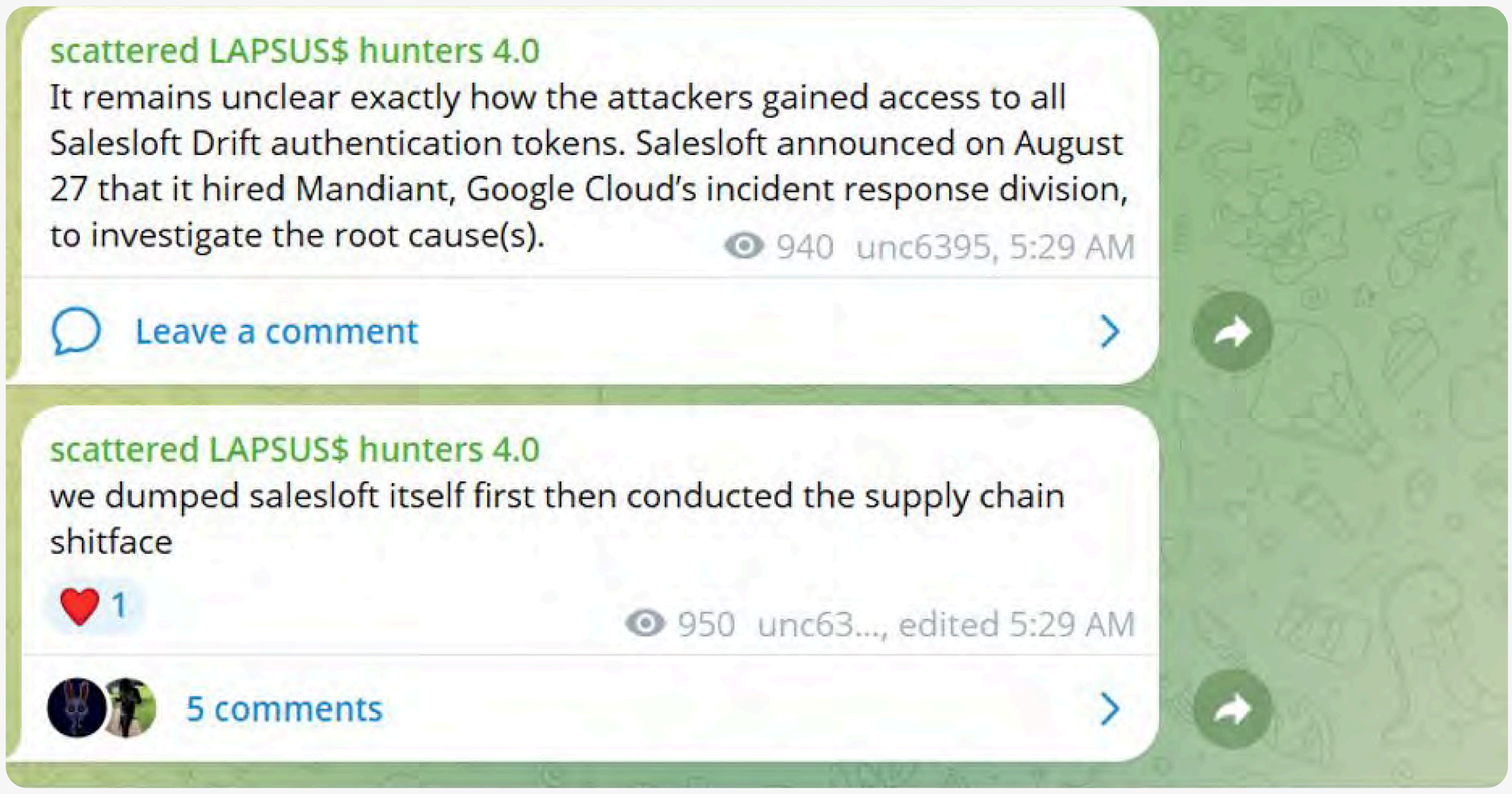
Salesloft announces temporary suspension of Drift to conduct security review.

September 8

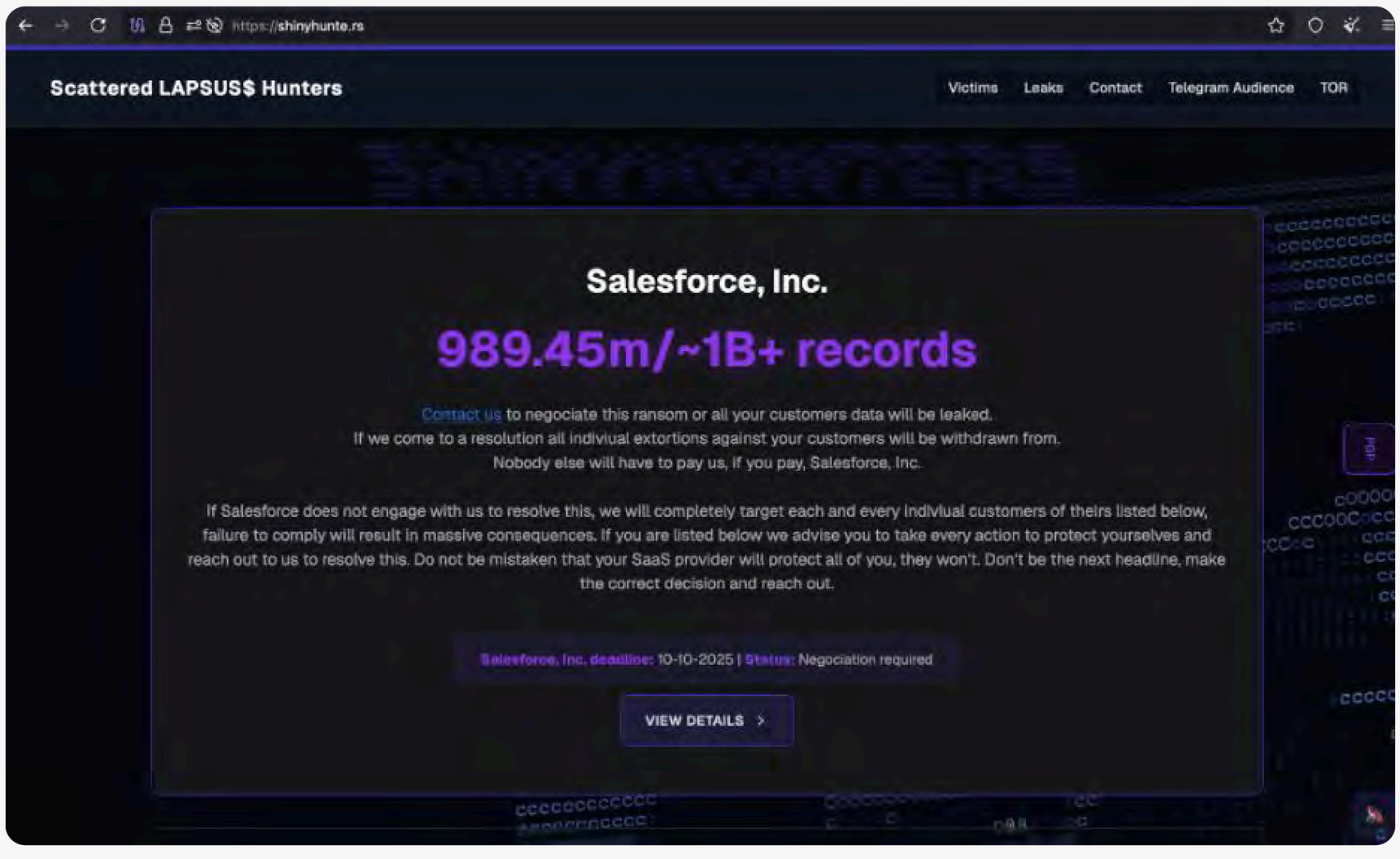
Integration between Salesloft and Salesforce is restored after remediation.

Attribution and Impact

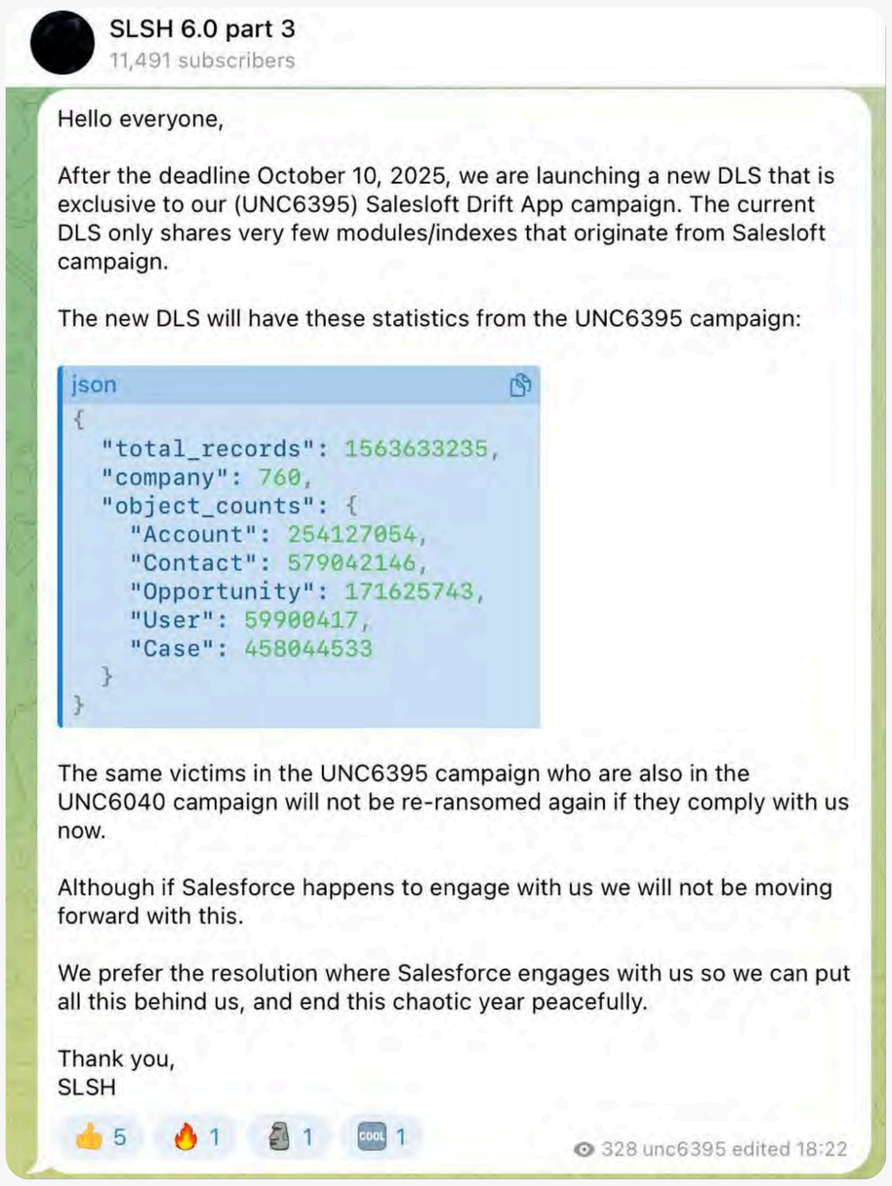
Attribution for this breach remains inconclusive. While members of the Telegram channel "ShinyHunters / Scattered Spider / Lapsus" aka SLSH posted messages indirectly claiming responsibility, no direct technical links were established. The analysis attributes the activity to UNC6395.



A screenshot of a Telegram message from SLSH claiming responsibility for the data leak dump



A screenshot of a ransom note to Salesforce from SLSH



A screenshot of a Telegram message announcing the launch of a new Dedicated Leak Site (DLS) relating to the Salesforce breach

Regardless of attribution, the **impact is undeniable**. The attackers successfully leveraged Drift's integration layer to infiltrate **high-profile targets** including Palo Alto Networks, Cloudflare, Elastic, Workday, and others. The attackers also threatened to release data from up to 50 additional compromised organizations, several of which appeared to be linked to the Drift integration ecosystem.

This case exemplifies how OAuth token compromise via a third-party integration can enable multi-organizational intrusion at scale. A single OAuth credential tied to a chatbot integration became a launchpad for unauthorized access across CRMs, cloud environments, and communication tools, bypassing traditional authentication controls and impacting over 700 organizations.

When Supply Chain Breaches Become National and Global Economic Events

While the technical sophistication of supply chain attacks often dominates analysis, the financial and economic consequences of these incidents became impossible to ignore in 2025. A stark example is the cyberattack on Jaguar Land Rover, which was publicly claimed by actors associated with ShinyHunters / Scattered Spider / Lapsus.

Disclosed on September 1, 2025, the breach forced Jaguar Land Rover to halt assembly lines across the United Kingdom, Slovakia, Brazil, and India — triggering widespread disruption across manufacturing operations, supplier dependencies, and downstream logistics networks. What began as a cyber incident quickly escalated into a global supply chain disruption.

Jaguar Land Rover later confirmed that the incident resulted in £196 million (approximately $250 million) in direct losses, underscoring how cyber intrusions into digitally interconnected production environments can translate into immediate and material financial damage.

The impact extended beyond the company itself. According to the Bank of England, the U.K. economy grew by just 0.2% in Q3 2025, falling short of expectations. Among the contributing factors cited were weaker exports to the United States and supply chain disruptions linked to the Jaguar Land Rover cyberattack — highlighting how breaches affecting critical manufacturers can ripple outward, influencing national economic performance.

Taken together, the incident illustrates a defining reality of 2025: supply chain breaches are no longer confined to IT environments or corporate balance sheets. When trusted operational ecosystems are disrupted, the consequences can scale rapidly — from factory floors to national economies.

Output

2025 marks a shift in breach dynamics—from targeting isolated organizations to exploiting centralized third-party platforms to gain access to entire customer ecosystems. Attacks on SaaS providers exposed sensitive data and enabled downstream compromises of hundreds of integrated systems. The closure of major breach forums and the rise of fragmented leak spaces further complicated attribution and detection, signaling a maturing threat actor landscape that's more calculated, stealthy, and economically disruptive.

Future Attack Updates 2026

We anticipate a continued rise in multi-tenant breach attempts, where a single point of compromise in a cloud service or integration platform grants access to a wide array of customers. Attacks will likely expand into ERP, HR, and marketing automation ecosystems, especially those with deep cross-client access. Additionally, we expect further abuse of OAuth tokens, SSO misconfigurations, and plugin/integration systems as attackers focus on invisible pivots that evade perimeter detection. Leaked data will increasingly be used to launch targeted fraud, impersonation, and insider-style phishing across trusted communication channels.

Countermove

Organizations must now treat third-party vendors as extensions of their own attack surface. This means enforcing vendor risk scoring, zero-trust controls around integrations, and continuous token and API monitoring. SaaS providers, meanwhile, must improve OAuth token hygiene, implement integration access logs, and introduce granular permissioning and revocation flows. Strategic investments in supply chain threat modeling, automated dependency checks, and data flow visibility are no longer optional—they are foundational to modern security architecture.

From Access to Extortion: The Industrialization of the Ransomware Supply Chain

Ransomware activity in 2025 underwent a deep structural and psychological shift. After years of headline-grabbing attacks and coordinated law enforcement crackdowns, the ecosystem is now marked by paranoia, fragmentation, and retreat. As a result, we saw the ransomware landscape split into two distinct trajectories:

- On one side, a proliferation of smaller, agile groups emerged — often composed of former affiliates from big syndicates. These actors chose to operate independently or semi-cooperatively, trading notoriety for longevity. Many explicitly avoid formal partnership, viewing them as a liability rather than an advantage. Some of these groups intentionally remain in the shadows, limiting exposure and minimizing law-enforcement attention. They conduct operations within closed circles and refrain from publicly naming their ransomware strains. By contrast, groups such as **The Gentlemen** and **Devman** pursue the opposite strategy. They seek maximum visibility for their attacks, leveraging publicity and fear as force multipliers.

- On the other side, veteran actors like ClOp doubled down on operational maturity. Highly compartmentalized and suspicious of outsiders, they built “island-style” ransomware operations, where all critical access, tooling, and zero-day exploitation is handled internally or by contracted red-teamers. Rather than competing in noisy affiliate markets, these groups invest in vulnerability research, acquiring or discovering zero-day exploits to silently infiltrate high-value targets.

Additionally, ransomware operations matured into fully industrialized ecosystems — and Initial Access Brokers (IABs) became their critical suppliers. These brokers have moved far beyond selling RDPs on forums. Today, they operate closed-access marketplaces and sell high-quality, pre-filtered access directly to ransomware affiliates, often via private Telegram channels. We now observe clear segmentation between tiered access sales — where privileged or critical access is reserved for partners, while lower-value credentials trickle into public dark web markets.

Case Study 1

The Rise of Ex-Affiliates and Shrinking RaaS Ecosystem

The ransomware underground in 2025 has been gripped by a wave of fear, uncertainty, and doubt. High-profile disruptions, exit scams, and mounting law enforcement pressure have deeply eroded trust within Ransomware-as-a-Service (RaaS) programs. Once-reliable names—including NoEscape, BlackCat, and RansomHub—either collapsed or vanished.

The ransomware underground in 2025 has been gripped by a wave of fear, uncertainty, and doubt. High-profile disruptions, exit scams, and mounting law enforcement pressure have deeply eroded trust within Ransomware-as-a-Service (RaaS) programs. Once-reliable names—including NoEscape, BlackCat, and RansomHub—either collapsed or vanished.

This erosion of trust led to a significant operational shift: **former affiliates began launching their own ransomware operations** to reduce dependency on unreliable syndicates and minimize the risk of arrest. New players like VanHelsing (ex-RansomHub and Medusa affiliates), Devman (ex-Qilin, Conti and DragonForce affiliate), and The Gentlemen (ex-Qilin affiliate) emerged in 2025 as direct offshoots of disillusioned affiliates, now running smaller, private or semi-open RaaS platforms.

Ransomware operators have also turned against each other. In 2025, we observed intra-underground sabotage, with some groups hacking the infrastructure of their rivals or launching deception campaigns. The trust deficit is now so severe that even affiliate onboarding processes have become adversarial, requiring new levels of vetting and surveillance.

-17.9%
of new affiliate

Meanwhile, the total number of new affiliate programs dropped from **39 in 2024 to 32 in 2025, a 17.9% decrease**. While new groups continue to emerge, the net decline highlights a more cautious, fragmented market, where operators are prioritizing operational security over recruitment scale.

Frequency of New Ransomware Affiliate Programs Emerging in 2025

Date	Ransomware	Username	Forum
04.01.2025	Skibidi	Skibidi-RaaS	CryptBB
13.01.2025	-	Striker	CryptBB
14.01.2025	BlackLock	$$$	Ramp
29.01.2025	A1Project	ambassador	Ramp
23.02.2025	Anubis	superSonic	Ramp
28.02.2025	Mimic v.10	mr.Guram	Ramp
27.03.2025	VanHelsing	VanHelsingRAAS	Ramp
08.03.2025	Embargo	oknos	Ramp
11.03.2025	MAMONA R.I.P	$$$	Ramp
16.04.2025	Embargo	Embargo_supp	Ramp

Date	Ransomware	Username	Forum
16.04.2025	Scareface	ScarefaceServices	promarket
03.05.2025	Nova	Nova	BHF
25.05.2025	DeadDog	mangoour	Dread
26.05.2025	Nebu1a	Nebula000	Rutor
05.06.2025	Chaos	MikeMelton	Ramp
07.06.2025	Desolator	desperados_1337	Darknetarmy
19.06.2025	-	masterblackhat	Dread
25.06.2025	-	Ghost2n	Darkforums
26.06.2025	Global	$$$	Ramp
07.07.2025	Devman 2.0	-	-
19.07.2025	BQTlock RaaS	@ZeroDayx1	Telegram
07.08.2025	Angel RaaS	id7577978812	Telegram
03.09.2025	LockBit 5.0	-	-
12.09.2025	The Gentlemen	Zeta88	Ramp
30.09.2025	mimic_v2.0	onion13	Ramp
04.10.2025	CipherWolf	CipherWolf	dna.forum
13.10.2025	Kryptos	Kryptaveli	umbraforums
28.10.2025	Data Keeper	DataKeeper	darknetarmy
04.11.2025	Coinbase Cartel	g77	RAMP
01.12.2025	Nopyfy	Nopyfy	cryptbb
03.12.2025	cry0	cry0	RAMP
10.12.2025	Gunra	wmanager000	Exploit

Case Study 2

The Quiet Evolution of Access Sales

While Initial Access Brokers (IABs) were once known for selling compromised credentials and footholds on public forums, **2025 marked a significant shift toward closed-door operations**. Today, many brokers operate in vetted ransomware affiliate groups, selling **high-value access directly to ransomware operators**, bypassing the open underground economy altogether.

A prime example of this new model is the "ToyMaker" access broker, highlighted in a 2025 investigation by Cisco Talos. ToyMaker specializes in targeting critical infrastructure by exploiting public-facing servers, deploying a custom backdoor named **LAGTOY**, and harvesting credentials across victim environments. After several weeks of undetected access and reconnaissance, ToyMaker passes control to the CACTUS ransomware, which then executes the classic double extortion strategy: **data exfiltration, encryption, and extortion.**

The operation demonstrated a clear division of labor and planning:

- ToyMaker performs technical infiltration and persistence (via LAGTOY).
- After 3+ weeks of dwell time, CACTUS enters the network, escalates access, and deploys tools like AnyDesk and OpenSSH for lateral movement and payload delivery.
- Victims are then hit with ransom demands, while their stolen data is threatened with public release.

This type of exclusive, pre-arranged access sale underscores a broader market evolution: public access listings are shrinking. According to Group-IB monitoring:

3,055

publicly advertised access sales on dark web forums in 2024

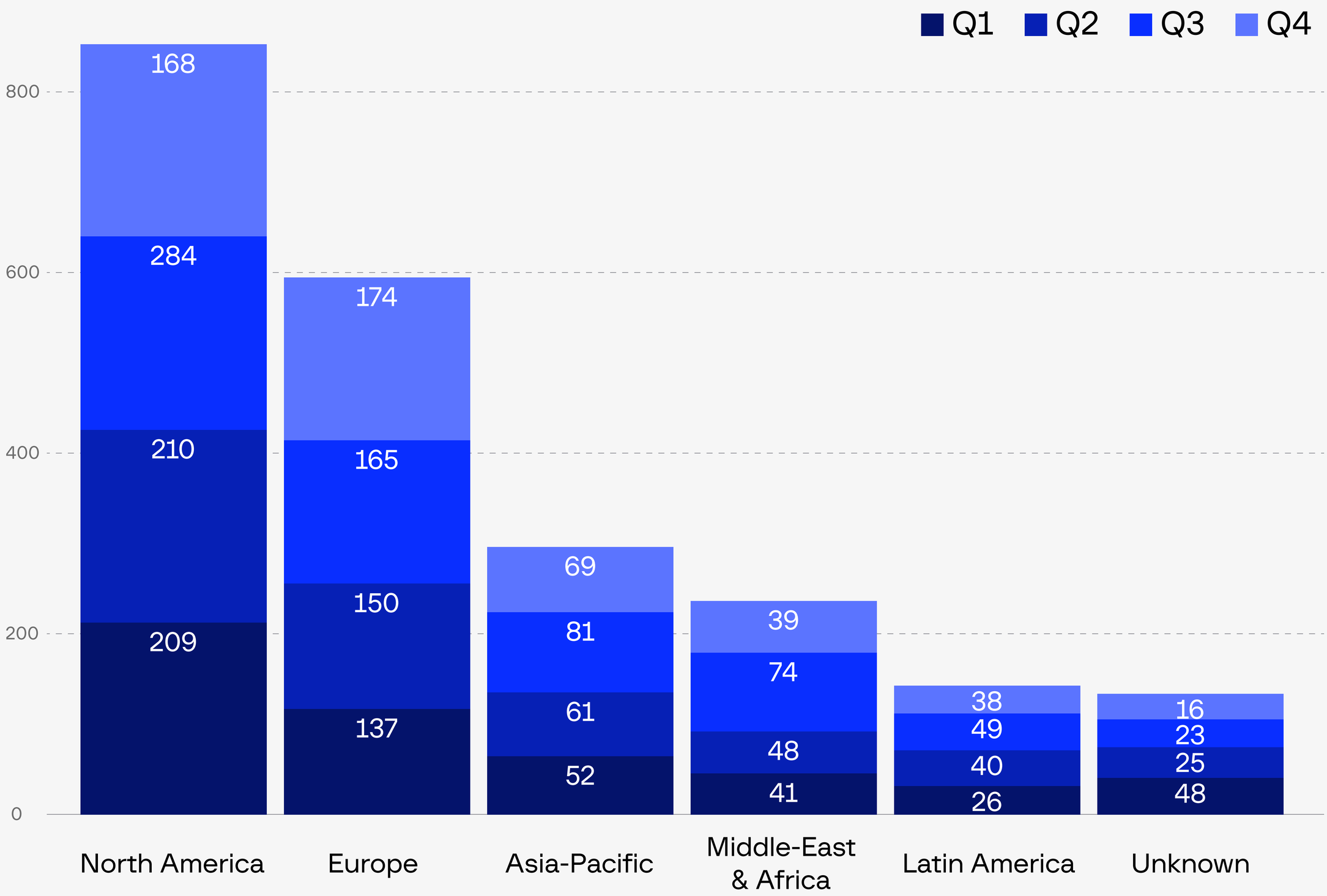
27.1%

this number dropped to 2,227 in 2025

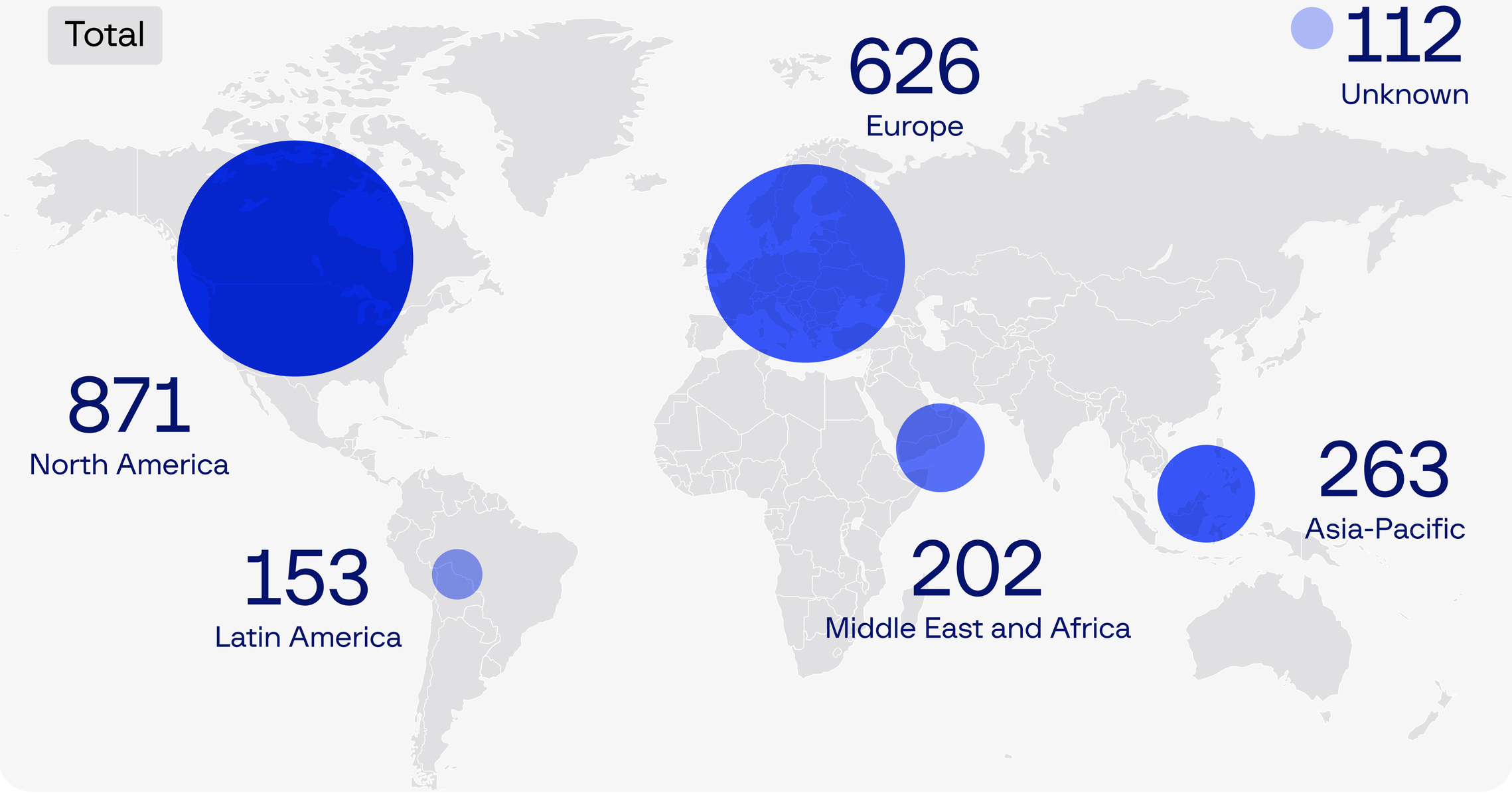
This decline doesn't indicate reduced activity—rather, it reflects increasing operational discipline. The most valuable access types (e.g., domain admin accounts, VPN panels, SaaS logins) are now **reserved for trusted ransomware partners** in closed channels, never reaching open markets. For defenders, this means that visibility into access sales is decreasing, even as the threat continues to scale in private.

Instances of corporate access detected and sold on the dark web by region in 2025

By region and quarter (Q1–Q4)



Total



Case Study 3

Ransomware Through the Supply Chain

In 2025, ransomware groups increasingly exploited trusted third-party providers to compromise multiple downstream organizations in a single stroke. These attacks bypassed direct perimeter defenses by targeting vendors with privileged integration or data access. Two key incidents demonstrate this shift:

01 DragonForce via MSP RMM Tool

In this case, a threat actor compromised a Managed Service Provider's (MSP) instance of SimpleHelp, a remote monitoring and management (RMM) tool. The attacker then used the legitimate RMM environment to:

- Push malicious installers to customer endpoints.
- Deploy DragonForce ransomware across multiple client machines.
- Gather configuration data from multiple customers, including hostnames, user accounts, and network connections.

This attack leveraged a centralized point of trust (the MSP) to pivot laterally into otherwise segmented customer environments.

02 Unknown ransomware → Marquis Software Solutions → Banks

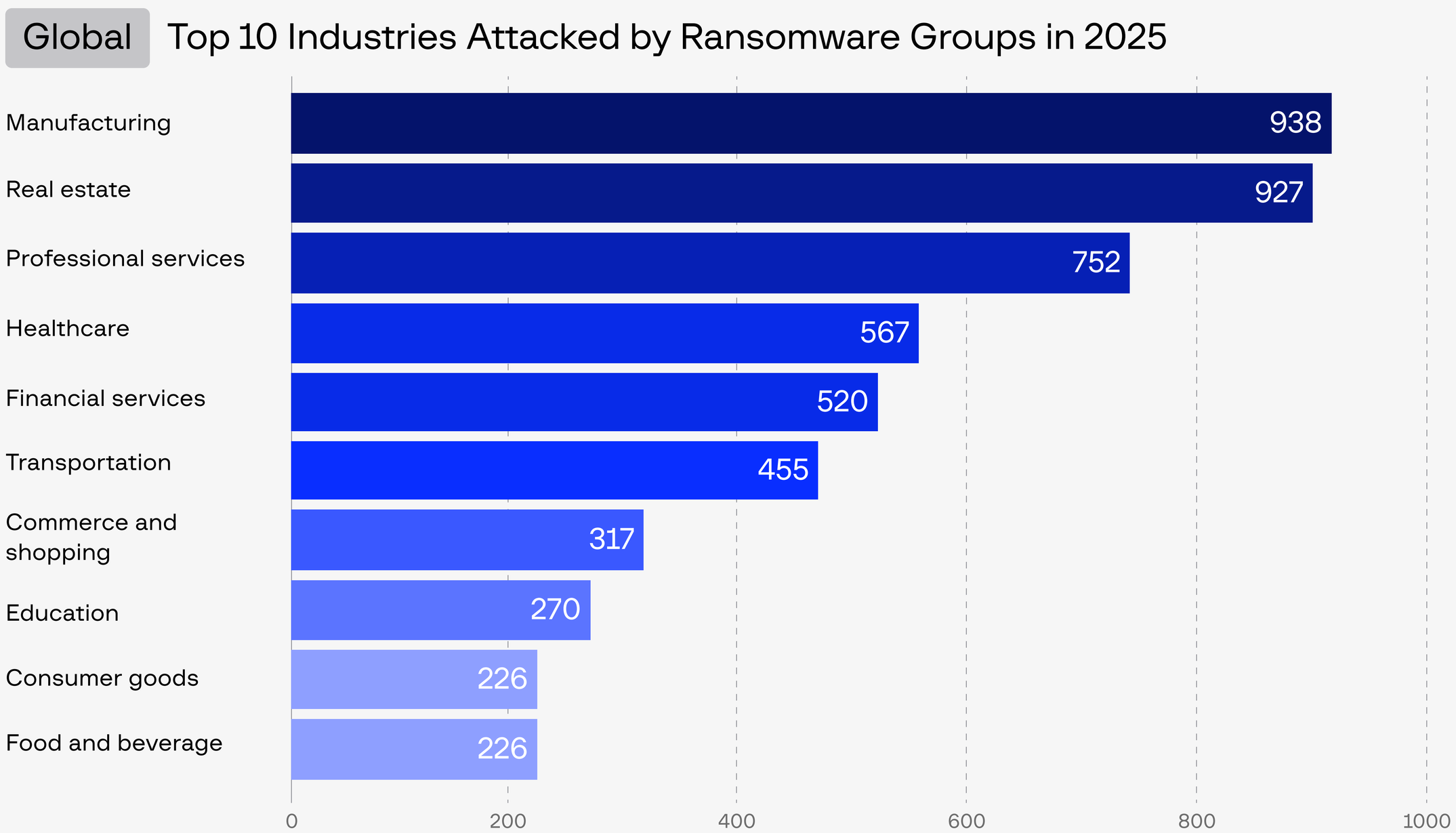
In August 2025, Marquis Software Solutions, a vendor for analytics and communications tools in the financial sector, suffered a ransomware attack. The intrusion originated from a vulnerability in a SonicWall firewall and led to the theft of sensitive data belonging to customers of Marquis' clients:

- VeraBank and Artisans' Bank confirmed that attackers stole personal data including names, SSNs, TINs, account numbers, and contact details.
- Over 37,000+ users were impacted at VeraBank; 32,000+ at Artisans' Bank.
- Based on compilations from state breach registries, the total number of affected individuals is estimated between **788,000 and 1.35 million**.
- **74 financial institutions** were ultimately notified that their customer data was caught up in the Marquis breach.
- Notably, the banks themselves were not breached — attackers exfiltrated data solely from Marquis Software's environment, underlining the power of vendor access.

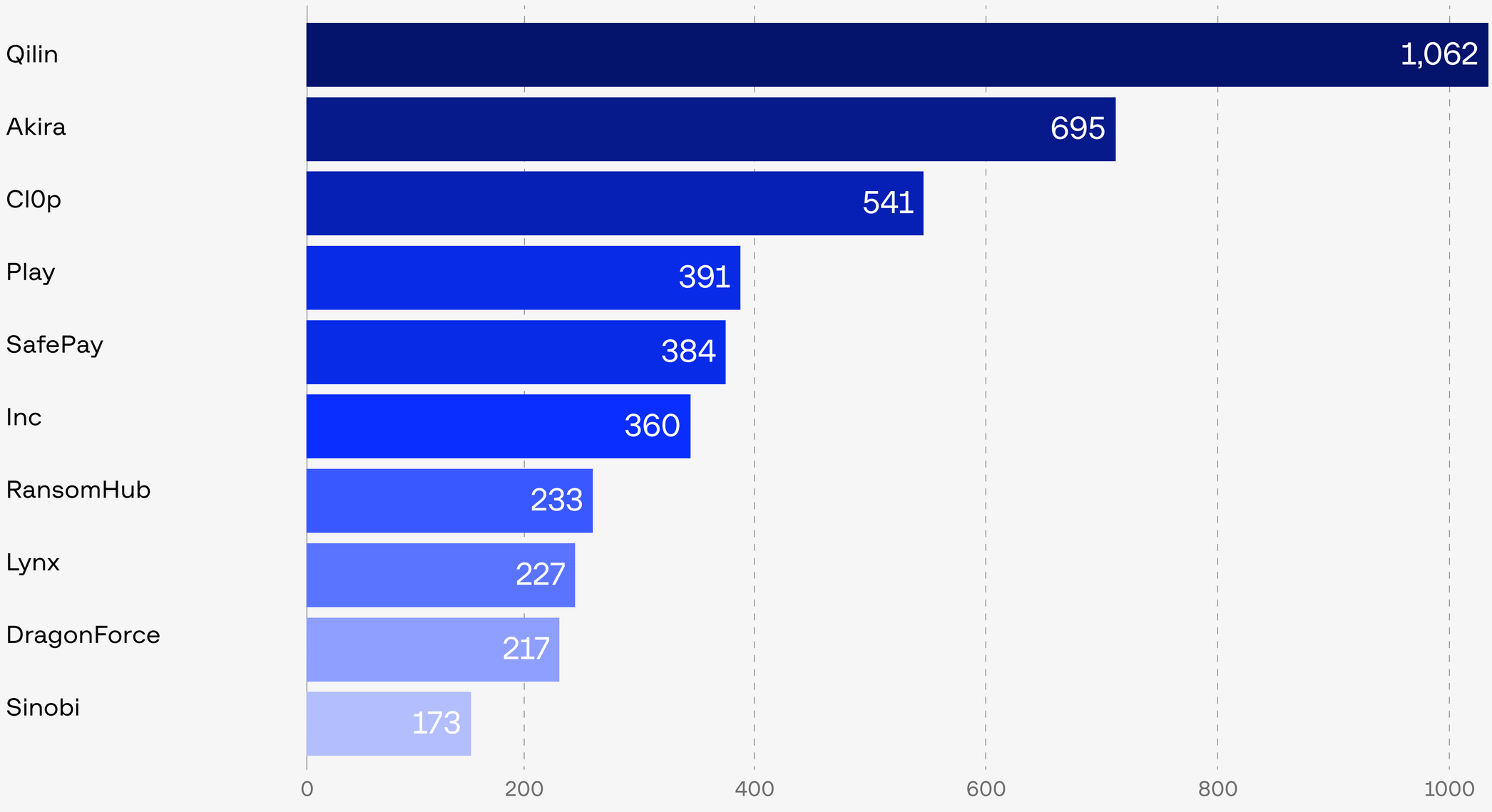
Distribution of Ransomware Attacks in 2025

Global Ransomware Attacks in 2025

Global Top 10 Industries Attacked by Ransomware Groups in 2025

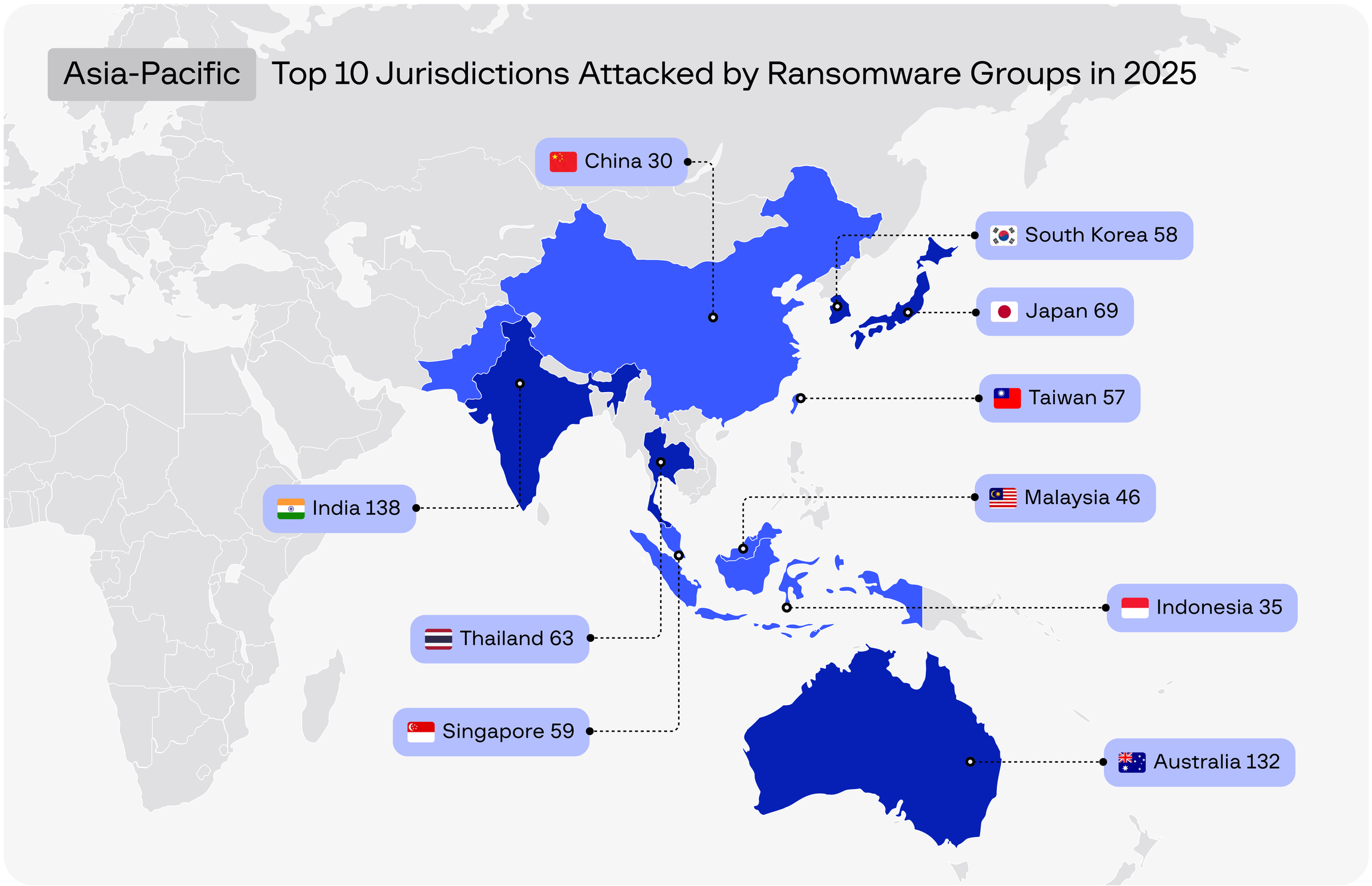


Global Top 10 Ransomware Groups by Number of Attacks in 2025

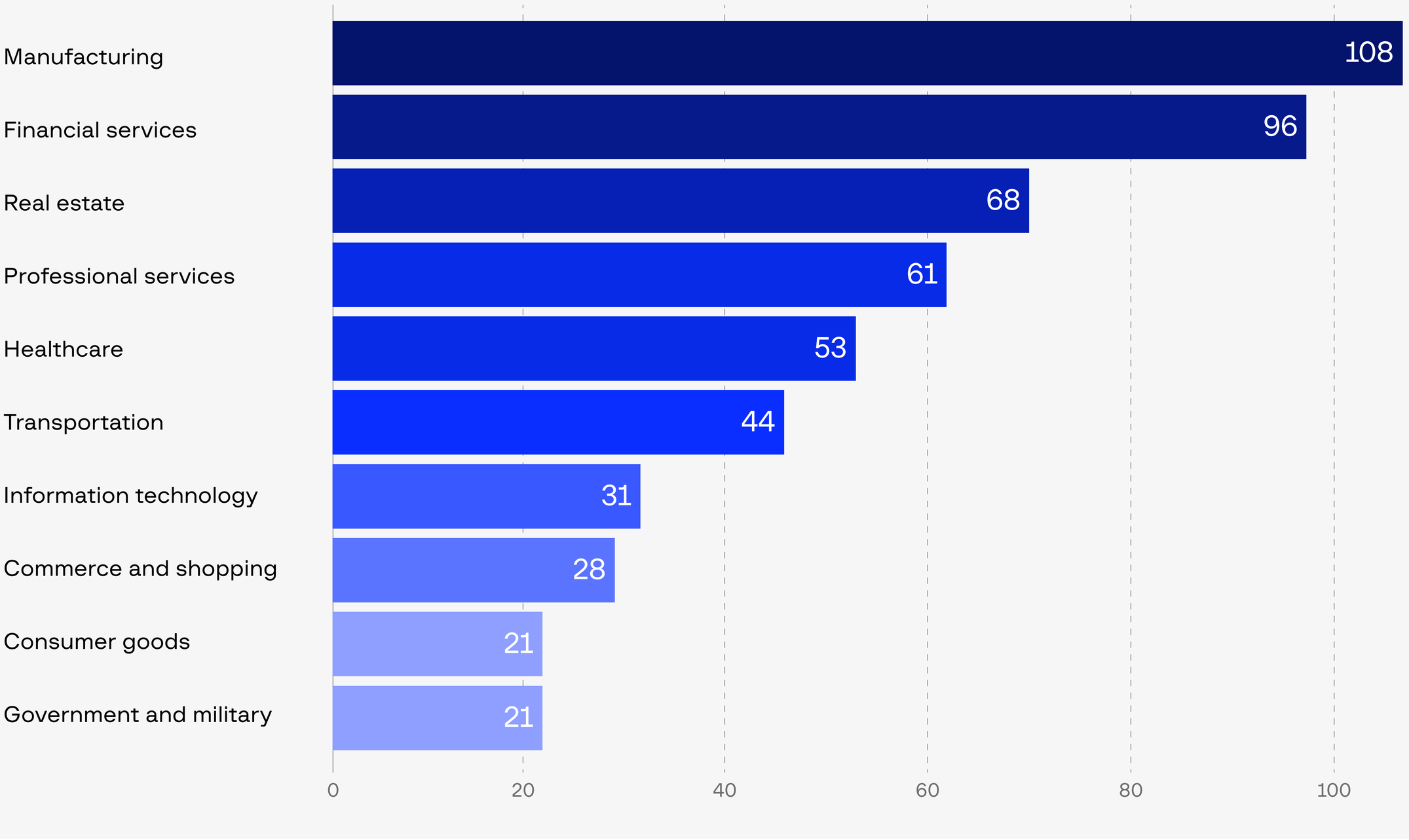


Asia-Pacific Ransomware Attacks in 2025

Asia-Pacific Top 10 Jurisdictions Attacked by Ransomware Groups in 2025

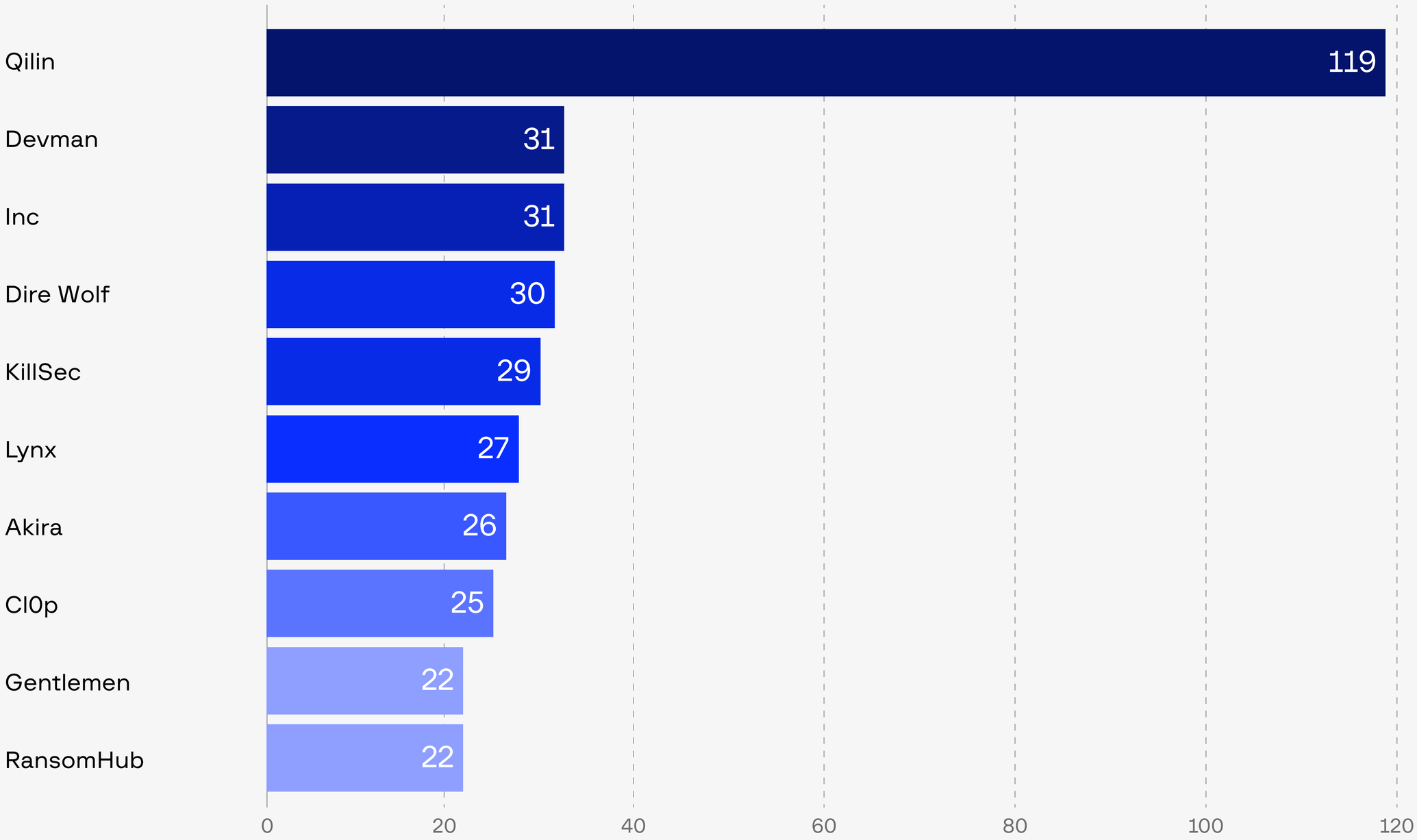


Asia-Pacific Top 10 Industries Attacked by Ransomware Groups in 2025



Asia-Pacific

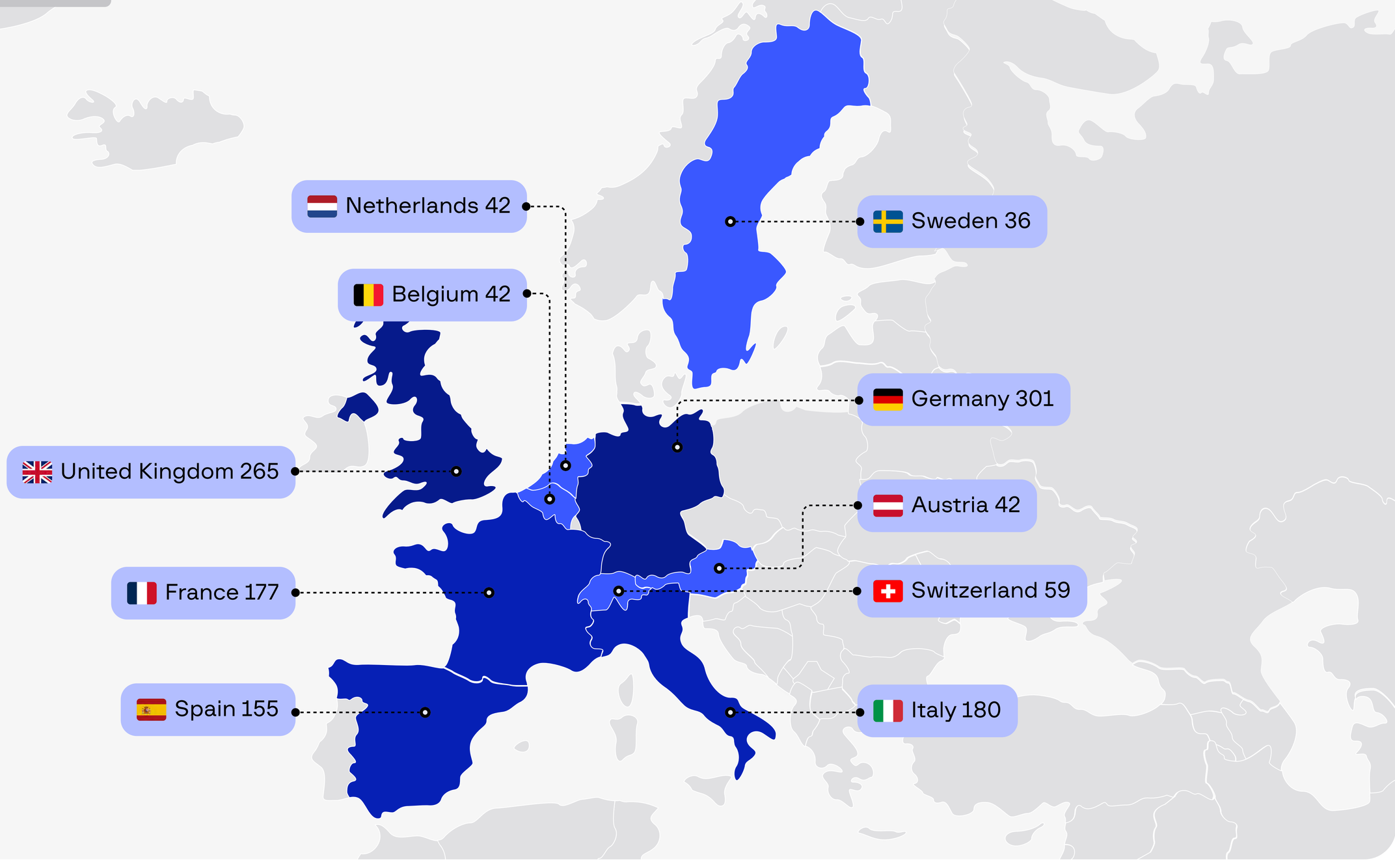
Top 10 Ransomware Groups by Number of Attacks in 2025



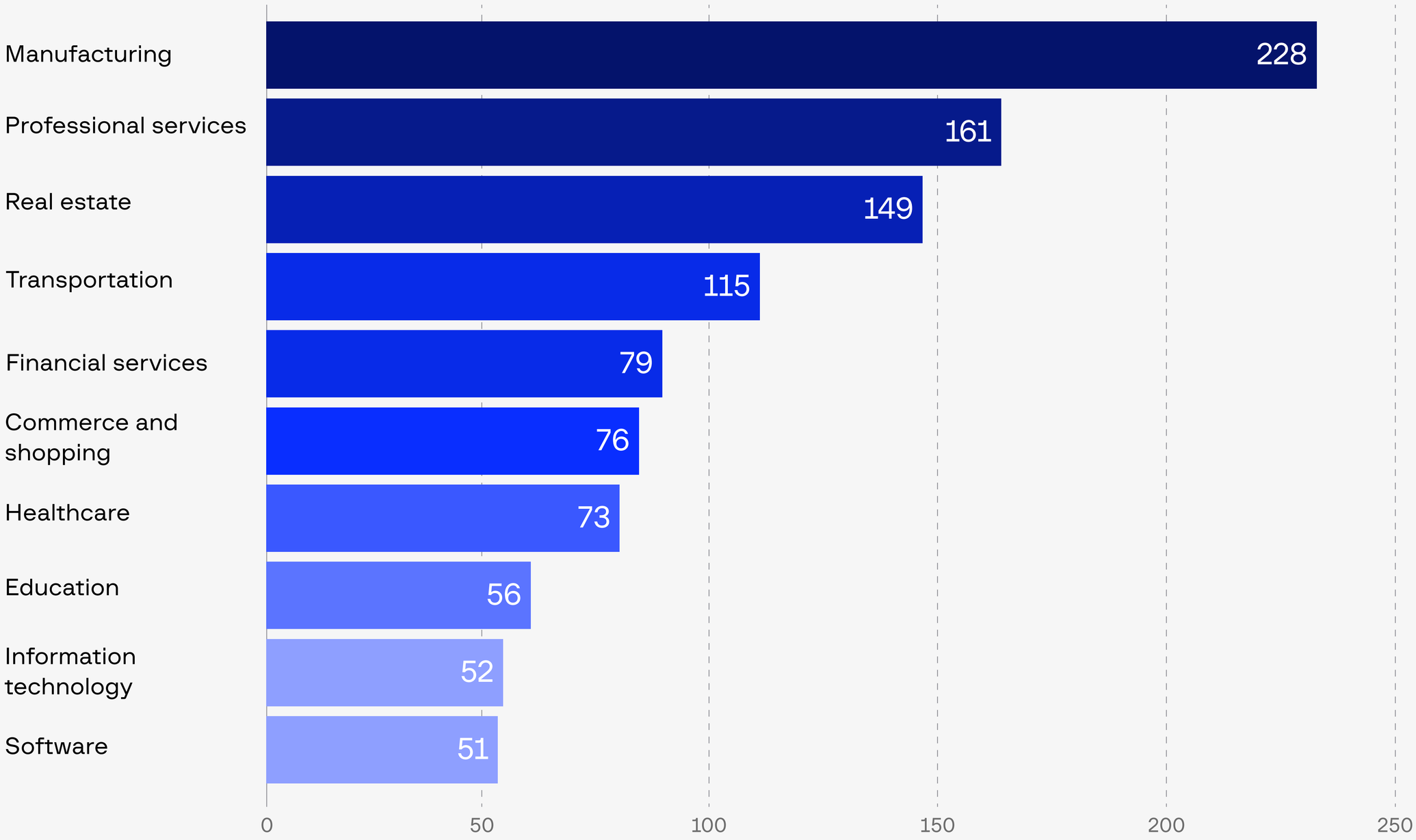
Europe Ransomware Attacks in 2025

Europe

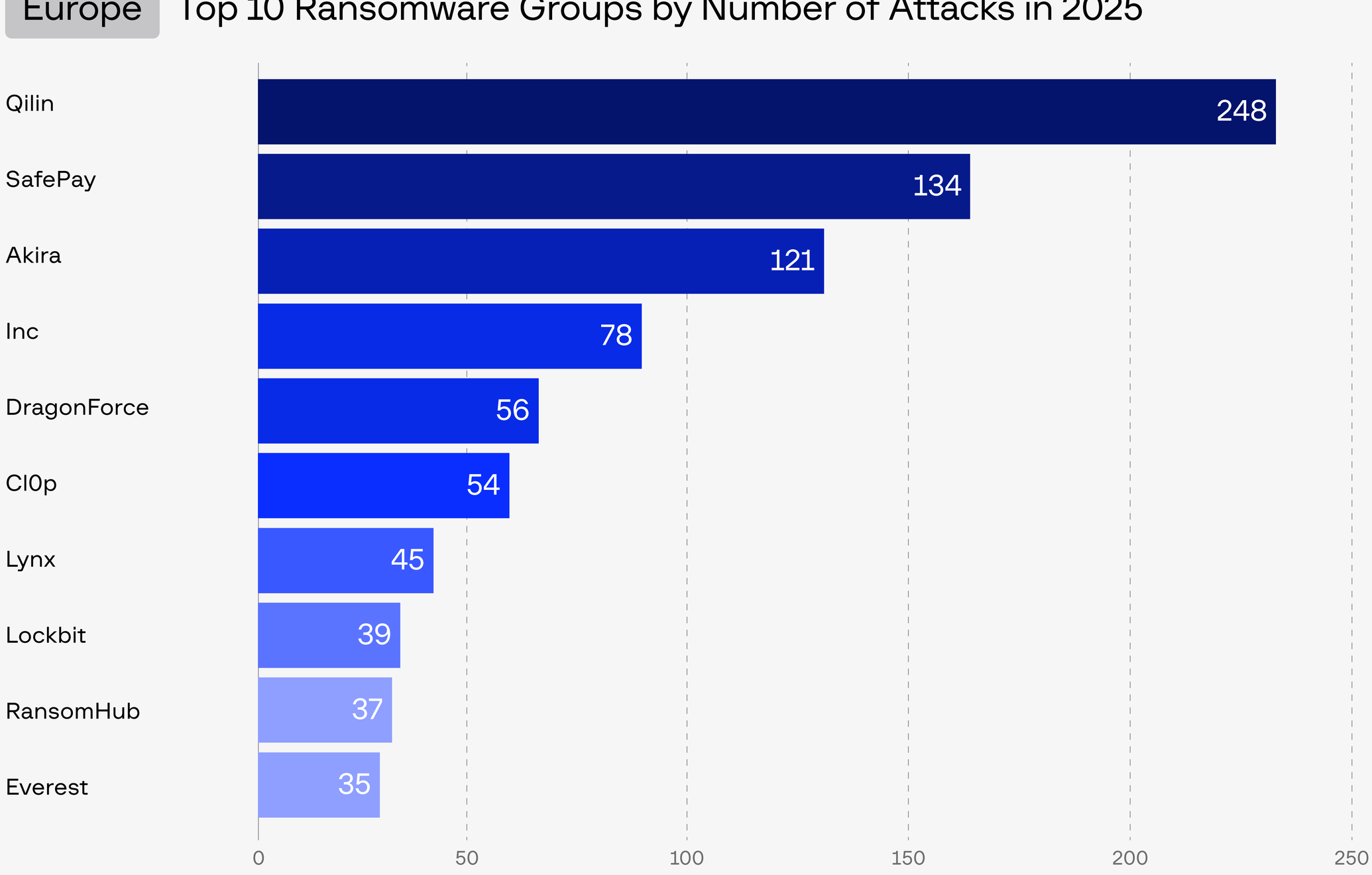
Top 10 Jurisdictions Attacked by Ransomware Groups in 2025



Europe Top 10 Industries Attacked by Ransomware Groups in 2025



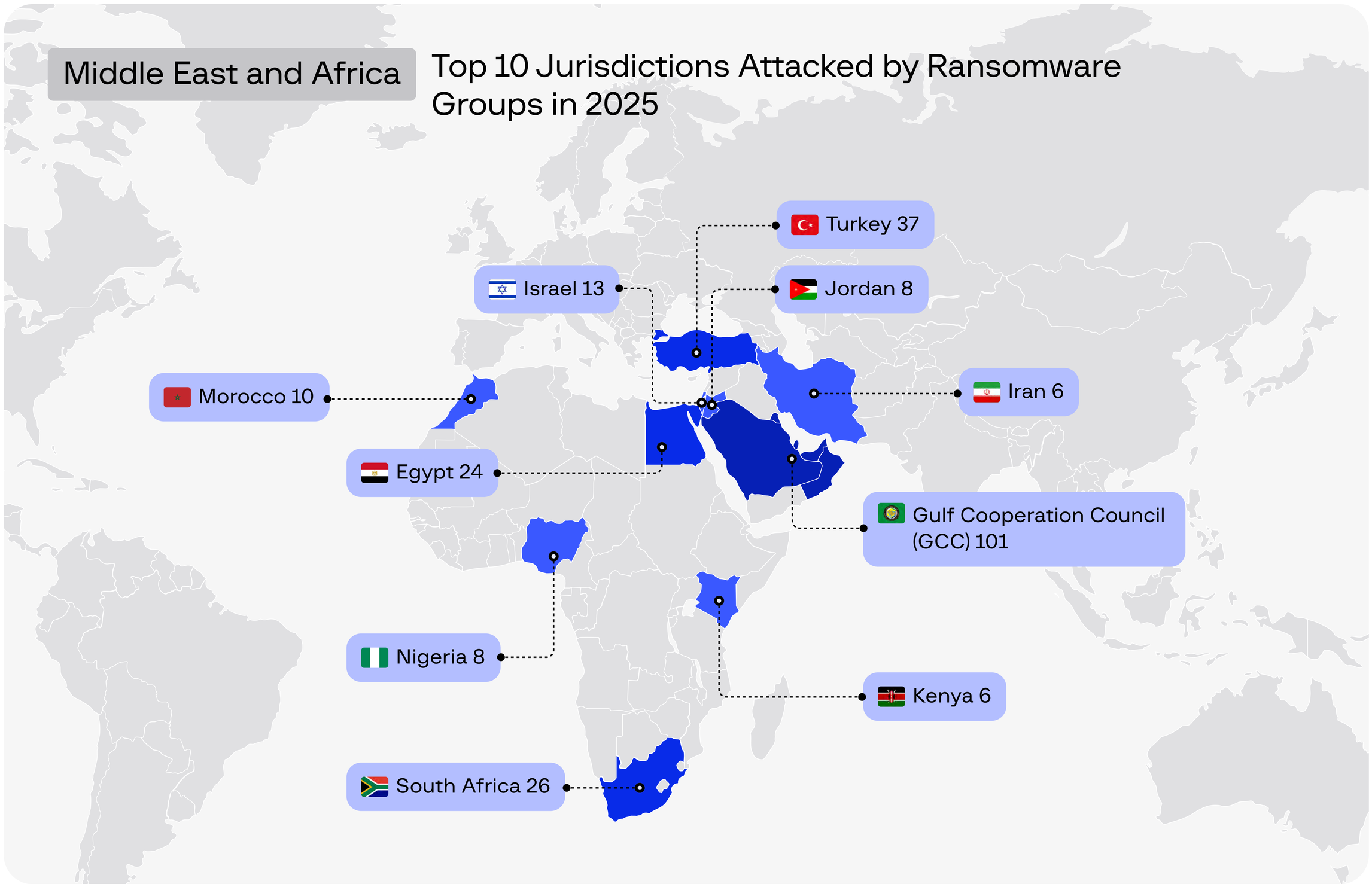
Europe Top 10 Ransomware Groups by Number of Attacks in 2025



Middle-East & Africa Ransomware Attacks in 2025

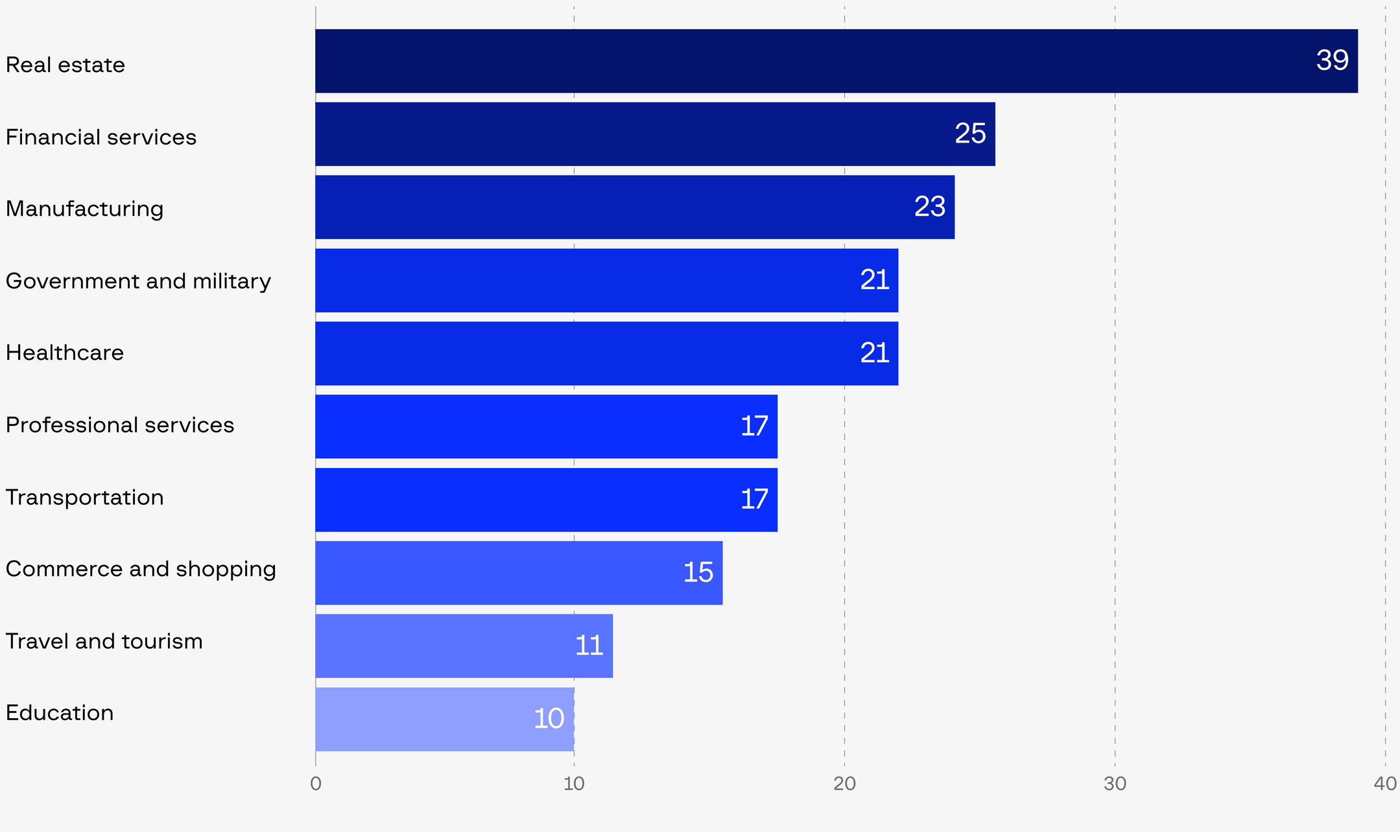
Middle East and Africa

Top 10 Jurisdictions Attacked by Ransomware Groups in 2025



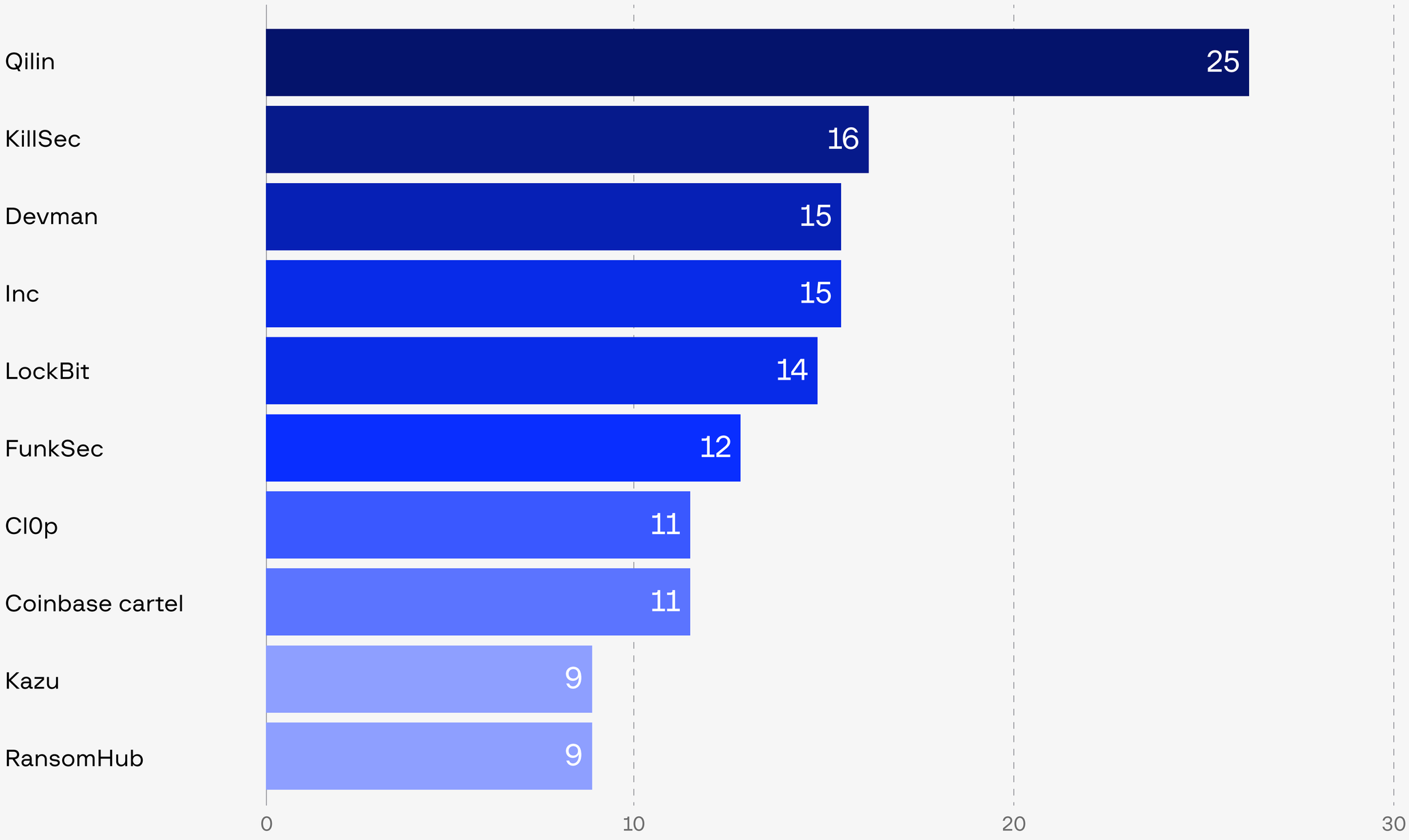
Middle East and Africa

Top 10 Industries Attacked by Ransomware Groups in 2025



Middle-East & Africa

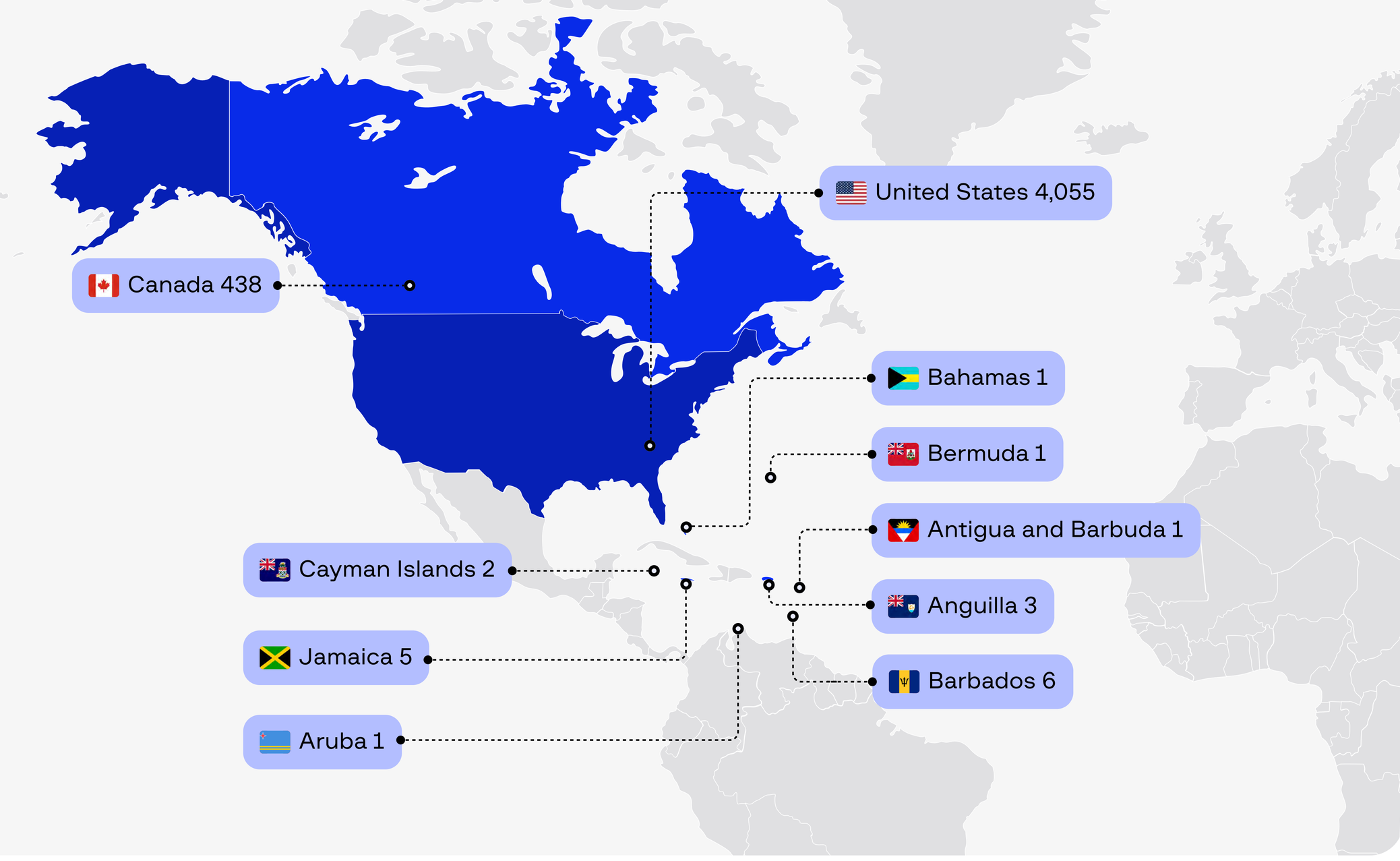
Top 10 Ransomware Groups by Number of Attacks in 2025



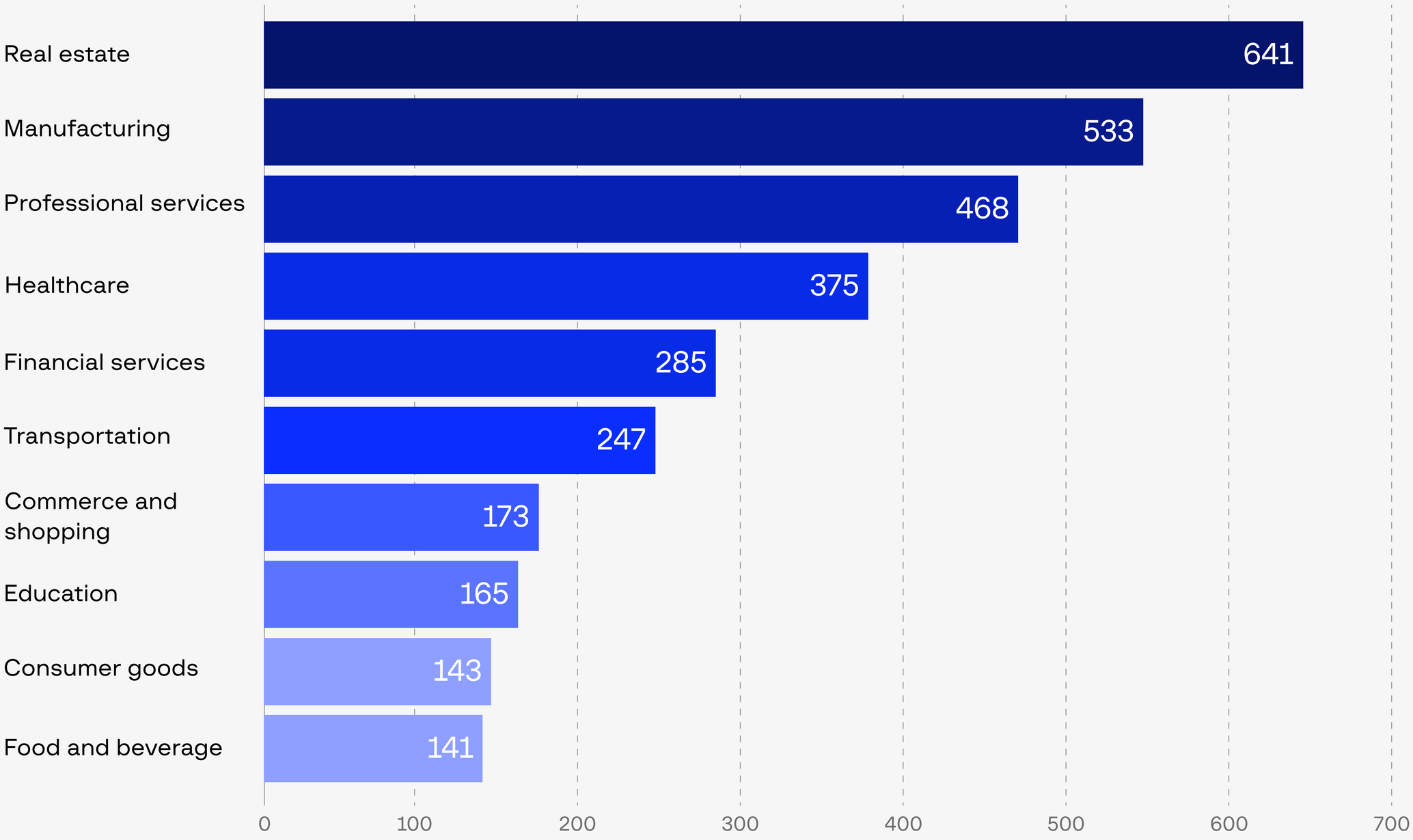
North America Ransomware Attacks in 2025

North America

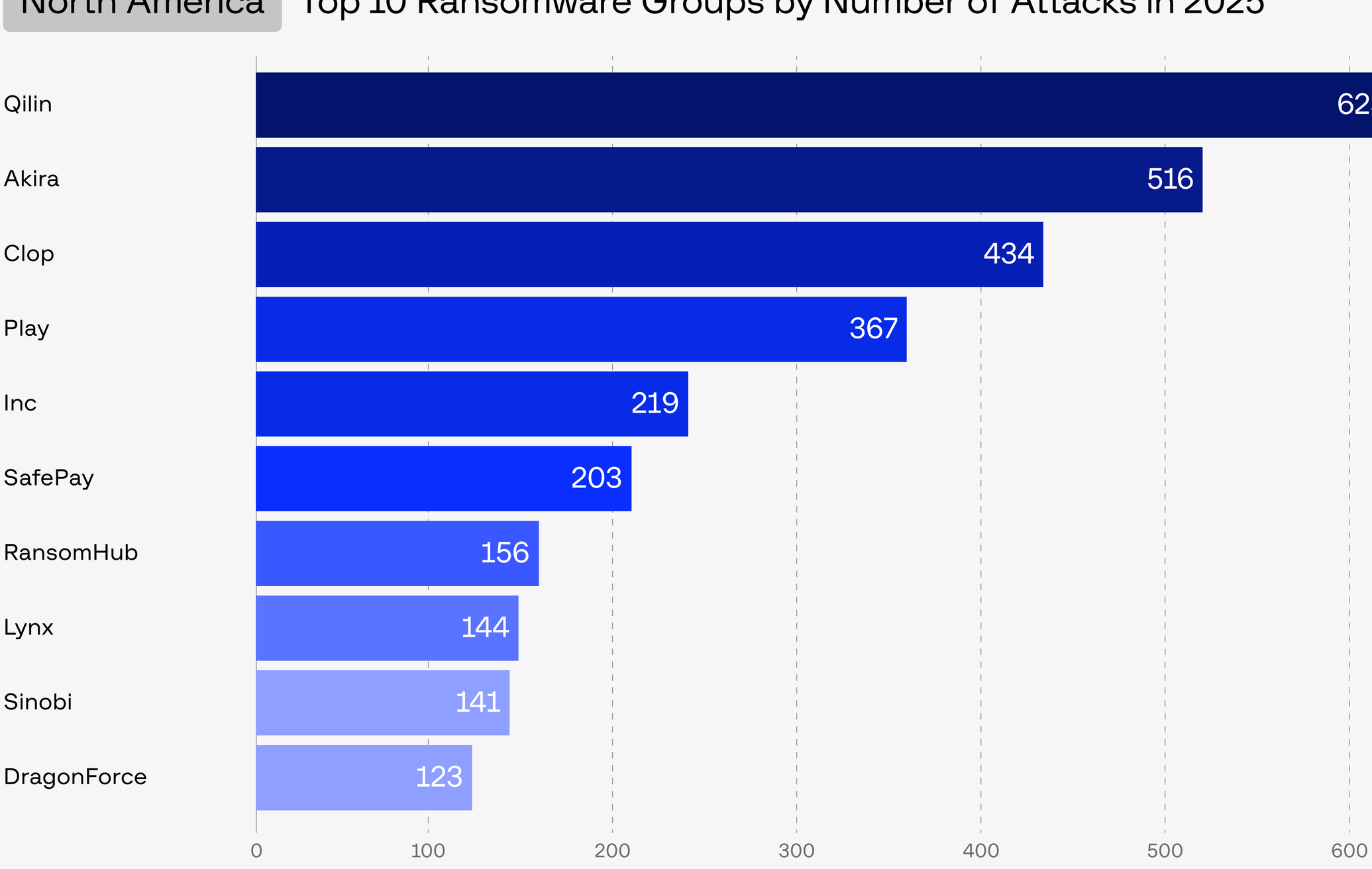
Top 10 Jurisdictions Attacked by Ransomware Groups in 2025



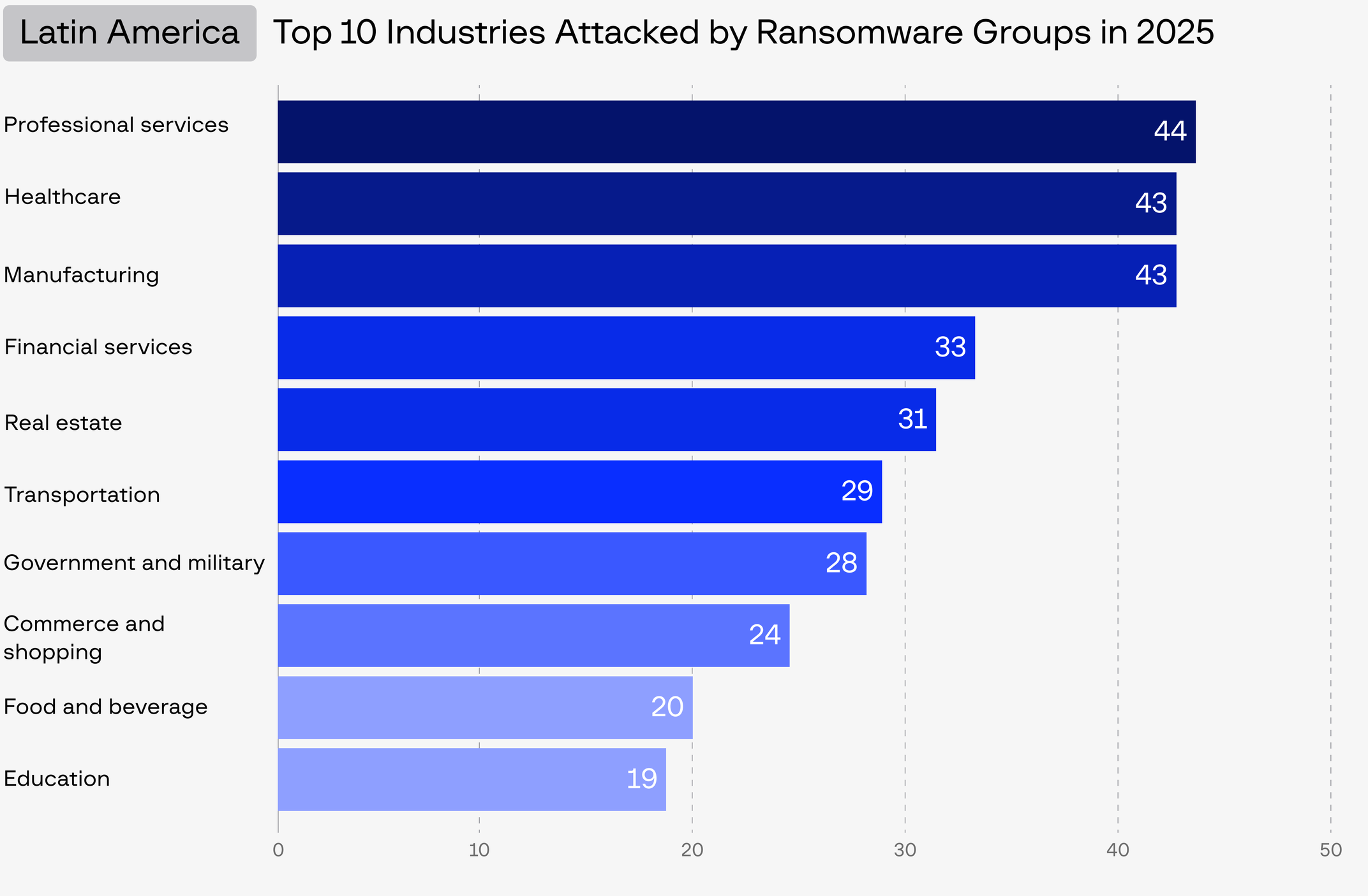
North America Top 10 Industries Attacked by Ransomware Groups in 2025



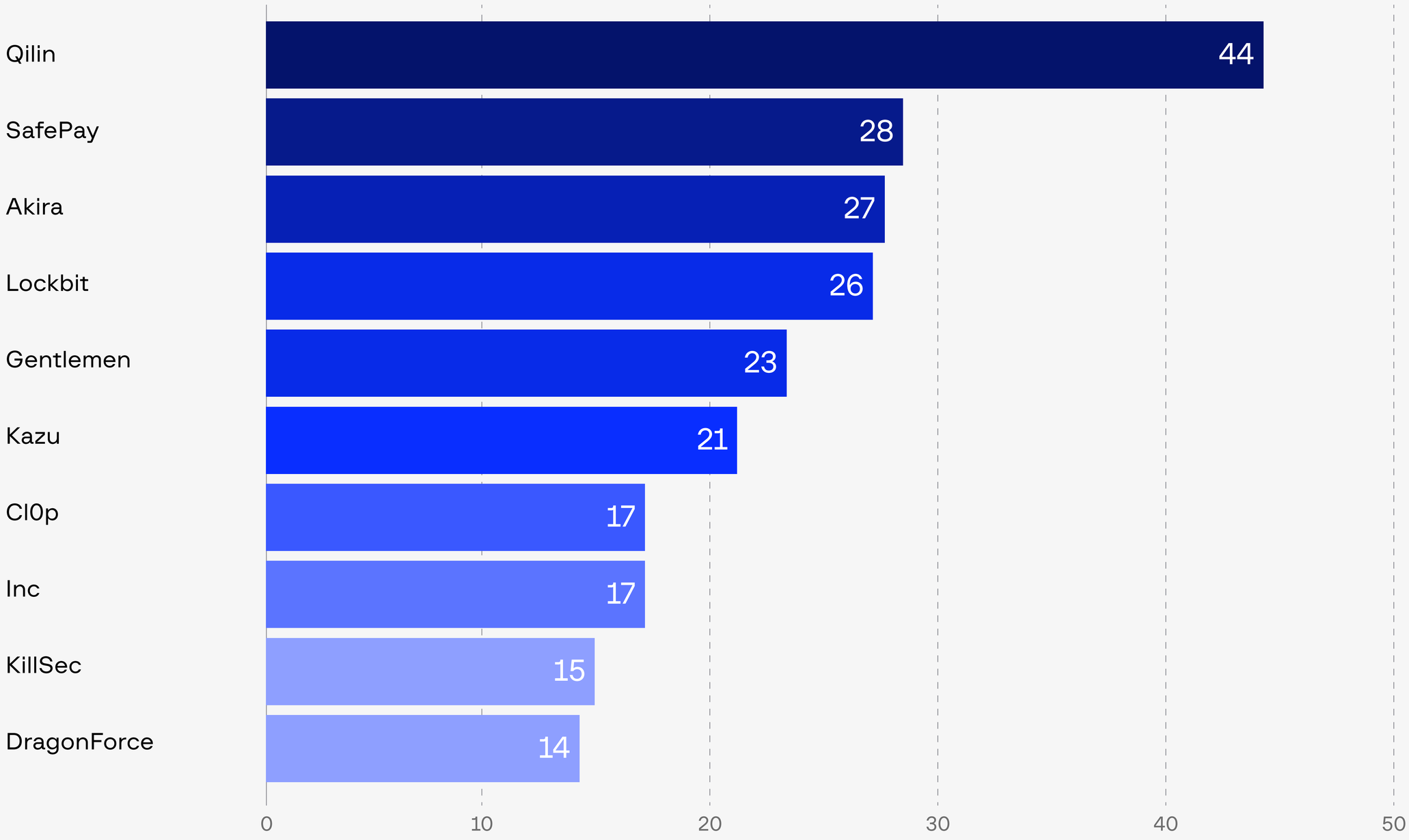
North America Top 10 Ransomware Groups by Number of Attacks in 2025



Latin America Ransomware Attacks in 2025



Latin America Top 10 Ransomware Groups by Number of Attacks in 2025



Output

Ransomware in 2025 evolved into a modular supply chain operation. Former affiliates splintered into smaller RaaS programs to avoid exposure, while high-value access shifted to closed channels, fueling exclusive ransomware deals. IABs now operate as structured suppliers, integrating directly into the early stages of extortion workflows. Supply chain abuse — including attacks via MSPs and SaaS platforms — became a preferred method for scalable impact with minimal initial intrusion.

Future attack updates 2026

We expect further fragmentation of ransomware operators and convergence between access brokers and encryption actors. Supply chain intrusions will grow, targeting integration points to bypass edge defenses. AI-assisted reconnaissance and credential reuse across SaaS ecosystems will reduce attack latency and expand scope.

Countermove

To reduce the impact of organized ransomware operations and evolving IAB ecosystems, defenders should prioritize zero-trust architectures, continuous session monitoring, and behavioral anomaly detection to identify early-stage access abuse. Security programs must enforce strong segmentation, implement strict access controls on remote admin tools, and continuously audit privileged accounts. Proactive mitigation also includes real-time IAB intelligence monitoring, sandbox testing for lateral movement, and endpoint detection for persistence tools commonly used in ransomware post-exploitation. Immutable backups, rapid patch cycles, and container/network microsegmentation should be standard in high-risk environments.

Advanced Persistent Threats: Converging Motives, Strategic Narratives, and Technological Superiority

In 2025, Advanced Persistent Threat (APT) activity revealed several transformative trends that reshaped how we understand and track state-linked cyber operations:

Convergence of Financial and Political Objectives

The traditional boundary between financially motivated operations and state-directed espionage has all but vanished, as nation-linked threat actors increasingly blend profit, disruption, and intelligence collection within the same operations.

North Korean–aligned groups continued large-scale cryptocurrency theft targeting financial and virtual asset infrastructure, at times escalating from data exfiltration to ransomware deployment to generate secondary revenue. Russian-linked APTs combined destructive capabilities with ransomware tooling to disrupt operational technology environments, particularly across critical sectors, while Chinese threat actors sustained long-term access to U.S. utilities, telecommunications, and water systems—behavior consistent with strategic contingency positioning. At the same time, Western actors were observed conducting deeply embedded operations within foreign state and technology organizations to harvest intellectual property and strategic intelligence.

Attribution as a Geopolitical Weapon

Public attribution of cyberattacks is no longer merely a tool for defensive transparency. In 2025, it became a calculated geopolitical lever. Several governments led waves of high-profile attribution campaigns that emphasized narrative dominance over technical forensics, with announcements that were rapid, tightly coordinated, and amplified through the media. This shift signaled that messaging, deterrence, and political legitimacy now carry as much weight as evidentiary rigor, transforming attribution into a performative act that shapes alliances, policy decisions, and public perception alongside incident response.

Early Adoption of Advanced Offensive Capabilities

APT actors remained at the forefront of technical innovation, often piloting or industrializing techniques before they appeared in broader cybercrime. As previously discussed, this included the integration of generative AI to enhance phishing, impersonation, and large-scale information processing, as well as the systematic abuse of software supply chains, leveraging compromised dependencies, open-source projects, and third-party integrations to embed quietly within trusted environments. State-aligned groups also drove the early adoption of open-source ecosystem exploitation, pioneering methods that were later replicated and scaled by financially motivated threat actors.

Output	The APT landscape in 2025 became structurally more complex: attackers blurred the lines between espionage and monetization, while defenders faced increased difficulty distinguishing political signaling from actionable threat intelligence. The result — a more ambiguous, adversarial, and fast-evolving threat environment.
Future Attack Updates 2026	Geopolitical tensions will increasingly externalize into cyberspace, where state-aligned actors will proxy attacks through criminal groups or vendors, targeting private sector infrastructure to achieve policy goals. Strategic attribution will become harder: actors will intentionally mix TTPs, hijack open-source tooling, and plant misleading artifacts. Attribution will no longer be just about technical evidence —it must factor in geopolitical timing, narrative control, and psychological operations. The battleground will shift to utility providers, critical SaaS links, and embedded access chains.
Countermove	Defenders must treat attribution with skepticism and apply structured adversary intelligence frameworks to distinguish technical indicators from narrative spin. Prioritize behavior-based detections over IOC-heavy workflows. Expand threat modeling to include both financially and geopolitically motivated scenarios. Invest in hardening third-party exposure, secure-by-design principles for software, and red team-informed detection engineering to keep pace with APT tradecraft.

Chapter 2: Key Threats in 2026

The global cyber threat landscape is increasingly defined by adversaries that exploit trust rather than attack systems directly. Supply chain attacks, in particular, have become a favored strategy, allowing attackers to compromise software, services, and dependencies that are widely trusted and broadly deployed.

By abusing development pipelines, third-party relationships, and update mechanisms, these threats can evade traditional defenses and achieve scale from a single point of entry. Malicious activity is often designed to blend into normal operations, enabling long-term persistence and delayed impact across multiple organizations.

Understanding these tactics is critical to identifying the threat actors and malware that matter most in 2026. As digital ecosystems grow more interconnected, organizations must assume supply chain risk is inevitable and prioritize visibility, verification, and resilience across their entire technology stack.

Group-IB Threat Intelligence Portal

Group-IB customers can access our Threat Intelligence portal for more information by clicking on the respective threat actor or malware names that target the supply chain, within the following sections.

Supply Chain-Focused Threat Actors

Scattered Spider

Language
English

First seen
May 2022

About

Scattered Spider is a financially motivated cybercriminal threat cluster, long known for SMS-swapping and large-scale vishing campaigns. While attribution debates persist regarding whether this activity represents a single group or multiple related clusters, this reporting treats the activity under a single umbrella: Scattered Spider.

In 2025, the group significantly were focused toward supply-chain-enabled intrusions, with a particular emphasis on compromising corporate Salesforce environments. The primary objective of these campaigns is large-scale data exfiltration from Salesforce instances followed by extortion. Targets are predominantly English-speaking branches of multinational organizations.

Group-IB Threat Intelligence team identified phishing campaigns abusing Salesforce and cryptocurrency wallet brands, we assess medium confidence in Scattered Spider's involvement. Victimology analysis shows a clear focus on senior, high-impact corporate roles (e.g., SVP, CFO/ Treasurer, Heads of Digital Product), consistent with the objective of harvesting privileged SaaS credentials.

Aliases

Storm-0875 | Muddled Libra | UNC3944 | Scattered LAPSUS$ Hunters

Skillset

Phishing | Vishing | SMS-swapping | Supply-Chain | Trojanized applications

Toolset

STONESTOP | POORTRY | FakeOkta.Beta | FakeOkta.Gamma | FakeCitrix.Gamma | FakeOkta.Alpha | SpectreRAT | ALPHV | Mimikatz | AnyDesk | AMOS | Vidar | Meduza stealer | TeamViewer | FakeMicrosoft.Zeta | FakeOkta.Zeta

Targeted Industries

Artificial intelligence | Blockchain | Clothing and apparel | Consumer electronics | Consumer goods | Data and analytics | Design | Education | Energy | Financial services | Food and beverage | Gaming | Healthcare | Information technology | Internet services | Lending and investments | Manufacturing | Media and entertainment | Messaging and telecommunications | Non profit | Payments | Privacy and security | Professional services | Retail, Retirement | Sales and marketing | Software | Transportation | Travel and tourism | Video streaming | Web hosting

Targeted Countries

United States | Australia | Canada | France | United Kingdom | Vietnam | Germany | India | Netherlands | Sweden | Singapore | Belgium | Switzerland | Czech Republic | Denmark | Ireland | Italy | Japan | South Korea | Luxembourg | Mexico | Thailand | Taiwan

Motivation

Data theft | Financial gain

Modus Operandi

Scattered Spider conducts targeted vishing campaigns in which operators impersonate internal IT support staff. During interactions with employees, the attackers directly request user credentials and MFA codes to authenticate into Salesforce environments. In some cases, victims are instructed to enter connection codes to authorize access through a modified version of the Salesforce Data Loader application.

In another campaign, attackers gained access to Salesloft's GitHub repositories, added a guest user, and established initial workflows. Reconnaissance activity was observed in both Salesloft and Drift environments.

Access to Drift's AWS environment enabled the attackers to extract OAuth tokens associated with customer integrations. These tokens were used to access sensitive data across connected Salesforce environments, including account metadata, support case content, AWS credentials, Snowflake tokens, user passwords, and internal notes. By abusing trusted third-party integrations, the attackers were able to pivot into multiple high-profile downstream targets. A similar case later happened with Gainsight (Salesforce AppExchange partner).

Lazarus

Language
Korean

First seen
January 2007

ABOUT

Lazarus is a notorious hacking organization of Masked Actors, known as an advanced persistent threat (APT) group. With links to North Korea, it's been tied to many high-profile cyberattacks, including 2014's Sony Pictures hack and 2017's WannaCry ransomware attack. Just like its biblical namesake, Lazarus has a habit of disappearing and re-emerging under new identities to evade detection.

In 2025, the group significantly escalated its focus on software supply chain compromise, particularly through the abuse of malicious npm packages. Additionally, the group carried out a $1.5 billion hack of Bybit this year, which was caused by malicious code originating from Safe{Wallet}'s infrastructure.

These campaigns primarily targeted software developers and cryptocurrency-related organizations, with the objective of stealing credentials, sensitive data, and cryptocurrency assets to generate revenue for the DPRK regime.

Aliases

Dark Seoul Gang | HIDDEN COBRA | Guardians of Peace | APT38 | APT-C-26 | Zinc | Bluenoroff | Stardust Chollima | BeagleBoyz | TA444

Skillset

Typosquatting and brand impersonation | Custom malware development | Social engineering | Open-Source ecosystem abuse | Cryptocurrency data harvesting

Toolset (2025)

ThreatNeedle | RustyAttr | BeaverTail | CivetQ | InvisibleFerret | PondRAT | ThemeForestRAT | SIMPLESEA | SimplexTea | GolangGhost | Tropidoor | PylangGhost | NimDoor | FlexibleFerret | OtterCookie | Agamemnon | Manuscrypt | wAgent | MISTPEN

Targeted Industries

Crypto | Energy & Utilities | Government | Science & Engineering | Software & IT

Targeted Countries

Global

Motivation

Data theft | Financial gain | Espionage

Modus Operandi

Lazarus abuses the open-source ecosystem by publishing malicious npm packages that typosquat or mimic popular libraries, including names resembling widely used dependencies such as is-buffer, eslint, redux, socket, and react-related packages. Victims are infected during routine dependency installation.

Malicious packages commonly deploy BeaverTail, a JavaScript-based stealer and loader capable of harvesting browser data, credentials, and cryptocurrency wallet information (for example, Solana and Exodus). In later stages, some packages install the InvisibleFerret Python backdoor, enabling persistent access, file exfiltration, and screen capture.

In parallel, Lazarus uses social engineering to increase infection rates, creating fake developer personas on platforms such as LinkedIn and GitHub to lure targets into work with trojanized repositories. Across multiple waves in 2025, dozens of malicious packages were identified, ranging from low-download developer tools to highly popular libraries. Some campaigns leveraged crypto-clipping techniques to directly steal digital assets at scale.

HAFNIUM

Language
Chinese

First seen
January 2021

About

HAFNIUM is a cyber-espionage threat actor specializing in trusted-relationship and cloud supply chain compromises. In 2025, HAFNIUM was observed abusing stolen API keys and credentials associated with privileged access management (PAM), cloud application providers, and cloud data management platforms. Abuse of these credentials enabled the threat actor to access downstream customer environments belonging to the initially compromised organizations.

Once in possession of valid API keys, HAFNIUM leveraged this access to conduct reconnaissance and data collection within downstream tenants using administrative-level privileges. Victims of this downstream activity observed to date were primarily organizations within state and local government and the IT sector.

Aliases

Murky Panda | Silk Typhoon | G0125 | Red Dev 13

Skillset

Internet-facing service compromise | Vulnerabilities development | Lateral movement | Privilege escalation | Supply-Chain

Toolset

Neo-reGeorg | CloudedHope | China Chopper | ASPXSpy | Covenant | Mimikatz | ProcDump | Psexec | Nishang | PowerCat | 7-Zip | Godzilla Webshell | Tarrask | Ligolo

Targeted Industries

Financial services | Government and military | Education | Energy | Telecommunications | Healthcare | Information technology | Internet services | Non profit | Professional services | Aerospace

Targeted Countries

Global

Motivation

Data theft | Espionage

Modus Operandi

HAFNIUM gains initial access through exploitation of zero-day and n-day vulnerabilities in internet-facing services, as well as via compromised credentials. In January 2025, the group exploited a zero-day vulnerability in Ivanti Pulse Connect VPN (CVE-2025-0282).

After compromise, the actor abuses stolen API keys to access downstream customer environments of the initially compromised organization. Using administrative access, HAFNIUM conducts reconnaissance and data collection.

Post-compromise activity includes resetting default admin accounts via API access, deploying web shells, creating additional users, and clearing logs. The group later pivots from on-premises to cloud environments by dumping Active Directory data, harvesting credentials, and targeting Entra Connect (AADConnect) servers.

HAFNIUM abuses service principals and OAuth applications with elevated permissions to exfiltrate email and file data via Microsoft Graph and Exchange Web Services, including by adding attacker-controlled credentials to existing applications or creating new ones designed to blend into the environment.

Shai-Hulud

Language
N/A

First seen
August 2025

About

Shai-Hulud and S1ngularity are two related, sophisticated supply chain attacks that targeted the npm (Node Package Manager) ecosystem during 2025, specializing in stealing developer credentials, sensitive data, and, in the case of Shai-Hulud, exhibiting self-propagating "worm" behavior (designed to self-propagate).

While S1ngularity was focused on manual distribution and only Nx packages, the first wave of Shai-Hulud was less selective and tried to reach as many packages as possible, starting with the package initiated by @ctrl/tinycolor, which receives more than two million weekly downloads. The next wave, "Second Coming," significantly expanded the scope of the campaign, temporarily compromising popular projects associated with Zapier, ENS Domains, PostHog, Postman, and others.

Aliases

S1ngularity

Skillset

Malware development | NPM | Supply-Chain | Open-Source ecosystem abuse | Lateral movement

Toolset

TruffleHog | SHA1Hulud | Runner.Listener

Targeted Industries

All

Targeted Countries

Global

Motivation

Financial gain | Data theft | Data destruction

Modus Operandi

Shai-Hulud operates through malicious npm packages that execute during the post-install phase. The malware harvests developer secrets, including npm tokens, GitHub tokens, cookies, and local workspace data, and exfiltrates them to attacker-controlled GitHub repositories.

The malware exhibits worm-like self-propagation behavior. When valid npm tokens are discovered in the execution environment, the malware automatically publishes malicious versions of any npm packages accessible to those credentials, enabling rapid lateral spread across the npm ecosystem.

Later variants introduced execution during the preinstall phase, significantly expanding exposure across developer workstations and CI/CD pipelines by triggering earlier dependency installation workflows.

If no valid GitHub or npm tokens are present, the malware executes a destructive payload, deleting local files instead of exfiltrating data.

888

Language
N/A

First seen
August 2023

About

888 is an individual threat actor active on underground forums, primarily specializing in the sale of stolen databases. In addition to data sales, the actor also advertises and sells unauthorized access to corporate environments, including access to software companies with cloud and development infrastructure such as AWS S3, Jira, Bitbucket, and MySQL.

In 2025, several incidents linked to 888 demonstrated how a single initial compromise can cascade into multiple downstream intrusions. In one case, Group-IB identified that the actor compromised a software development company responsible for maintaining a centralized ERP platform used by an education-sector organization, resulting in secondary exposure of the platform's customer.

In another instance, 888 published multiple forum posts claiming access to source code from several companies within the same country. Subsequent analysis indicated that the source code exfiltration could have occurred through a shared contractor, specifically a digital design company servicing these organizations.

Aliases

N/A

Skillset

SQL | Valid accounts | Active Scanning | Supply-Chain

Toolset

N/A

Targeted Industries

Software | Commerce and shopping | Consumer electronics | Education | Financial services | Healthcare | Electrical distribution | Food and beverage | Government and military | Information technology | Manufacturing | Media and entertainment | Professional services | Software | Automotive

Modus Operandi

888 gains initial access to organizations and leverages that access to pivot through trusted contractor and service-provider relationships. Compromised environments are monetized either through direct sale of stolen databases or by selling ongoing access to internal systems and development resources.

The actor likely identifies exposed or weakly protected services through scanning, then leverages valid credentials—either compromised, reused, or obtained from third parties—to access internal systems.

Targeted Countries

India | Jordan | South Korea | United Arab Emirates | Brazil | Switzerland | Egypt | Malaysia | Philippines | Saudi Arabia | Thailand | Vietnam

Motivation

Financial gain | Data theft

Dragon Force

Languages
English, Russian

First seen
August 2023

ABOUT

DragonForce is a ransomware group active since 2023, operating under a Ransomware-as-a-Service (RaaS) model. Initially associated with politically motivated attacks, the group later pivoted to financially motivated extortion campaigns and has since established itself as a notable ransomware operator.

DragonForce runs an affiliate program that provides infrastructure, tooling, and customizable ransomware payloads for Windows, Linux, ESXi, and NAS systems. The group places strong emphasis on supply chain attacks, particularly targeting Managed Service Providers (MSPs) to gain access to multiple downstream client environments through a single intrusion.

Aliases

DragonForce Ransomware

Skillset

Ransomware development
RDP and VPN-based intrusion
Privilege Escalation
PowerShell
Double-Extortion Tactics
Living off the Land
BYOVD
ESXi

Toolset

SystemBC
Cobalt Strike
DragonForce Black
Mimikatz
AdFind
SoftPerfect Network Scanner
SimpleHelp

Targeted Industries

All

Targeted Countries

United States
United Kingdom
Germany
Australia
Canada
Italy
Argentina
Switzerland
France
Spain
New Zealand
United Arab Emirates
Saudi Arabia
China
Dominican Republic
Ireland
Puerto Rico
Sweden
Singapore
Brazil
South Africa
Belgium
Colombia
India
Malaysia
Bulgaria
Costa Rica
Curacao
Egypt
Hong Kong
Japan
Portugal
Palau
Czech Republic
Guatemala
Indonesia
Lebanon
Norway
Slovakia
Taiwan
Vietnam
Denmark
British Indian Ocean Territory
Iran
Mexico
El Salvador
Venezuela

Motivation

Financial gain

Modus Operandi

In May 2025, the group exploited multiple vulnerabilities in SimpleHelp RMM (CVE-2024-57726, CVE-2024-57727, CVE-2024-57728), enabling unauthorized access to MSP environments.

Once an MSP's RMM infrastructure is compromised, attackers leverage administrative access to deploy malicious installers, execute commands, and distribute ransomware across downstream customer networks. This approach allows DragonForce to scale attacks efficiently and impact multiple organizations simultaneously.

DragonForce employs a double-extortion model, combining ransomware deployment with prior data exfiltration from both the MSP and affected clients. Affiliates are supported with ransomware variants derived from LockBit 3.0 and Conti v3, alongside automation tools and configuration options to tailor encryption behavior and ransom notes.

Some affiliates activities commonly includes credential harvesting and lateral movement using SystemBC, Mimikatz, and Cobalt Strike, as well as network reconnaissance to identify and propagate to high-value systems before encryption.

Chapter 3: 2026 Cyber Forecast and Recommendations

Expertise

Artificial Intelligence

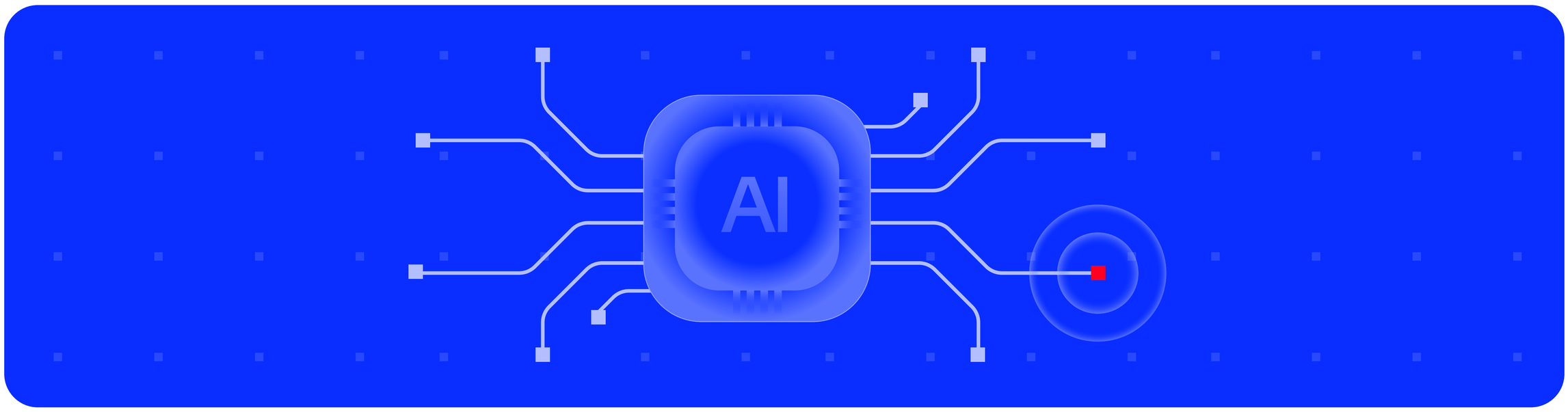
Agentic Extortion

AI-Driven Malware

Crypto and Stablecoins

AI-Assisted Code Generation

Wearable Devices



3.1 AI-Assisted Code Generation: Innovation with Hidden Supply Chain Risks

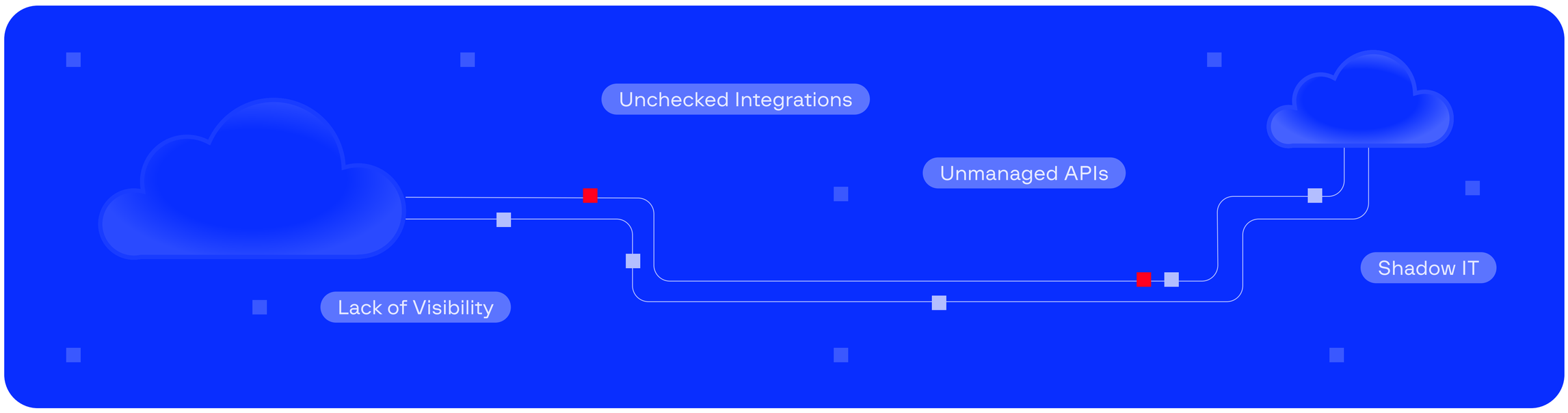
AI-driven tools are rapidly reshaping software development. Code generation has reached a level where developers increasingly trust automated output, accelerating delivery cycles and reducing traditional code review rigor. As a result, more generated code flows directly into production environments with minimal validation.

This growing reliance introduces significant supply chain vulnerabilities. Threat actors have long sought to embed covert backdoors and malicious functionality into widely used libraries and software components. With AI-based coding systems now handling larger portions of development activity, nation-state and organized cybercriminal groups may attempt to manipulate these tools to introduce vulnerabilities at scale.

The convergence of expanded adoption and reduced scrutiny presents an attractive target. For adversaries, AI-assisted development represents a scalable pathway to compromise systems and infiltrate development pipelines, an opportunity that is unlikely to go unnoticed.

Countermove

As a growing share of enterprise production code becomes partly or fully AI-generated, intelligence-informed risk decisions must begin before deployment, within development pipelines, not only at the SOC or incident response level. Organizations should align Threat Intelligence with modern SDLC practices, tracking adversary activity targeting developer tools, open-source tools, and AI model manipulation to inform preventive controls across CI/CD workflows. Security testing must also evolve to keep up with models, prompts, and dependencies as SecDevOps moves to AI-assisted development. By enabling greater scrutiny and continuous verification in AI developments, compromise risk can be significantly reduced preemptively.



3.2 The API Wild West: Unchecked Integrations Expanding the Attack Surface

Modern organizations are rapidly extending digital capabilities through cloud and API ecosystems. These interconnected environments deliver speed, scalability, and decentralized operations that drive growth. Yet without proper governance, the same technologies can become critical points of exposure.

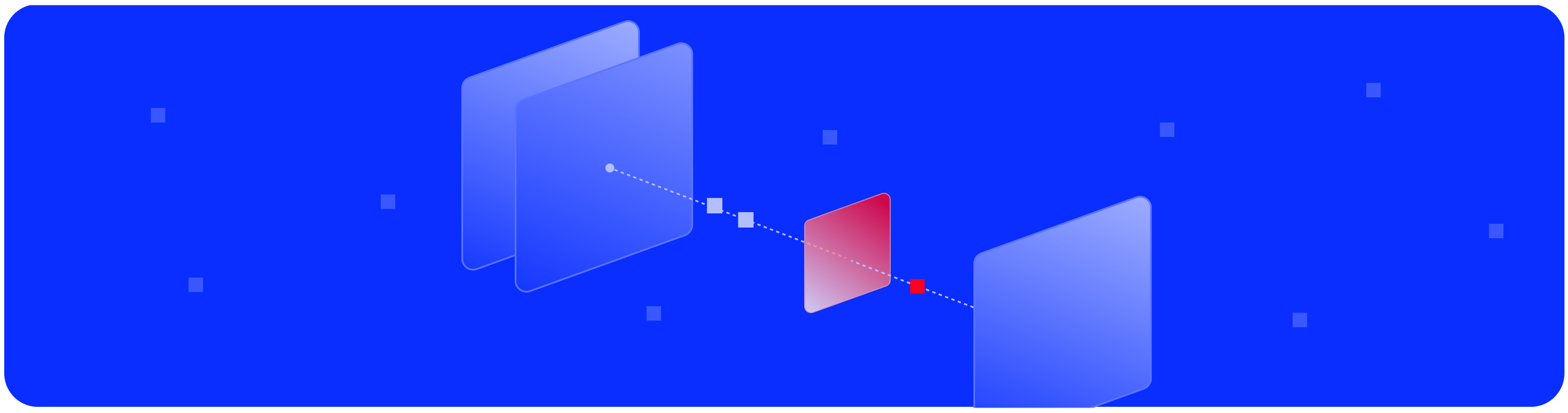
Legacy IT architectures were never designed to manage vast and continuously active integrations. APIs now exchange data across clouds, SaaS platforms, business partners, and internal systems at all times, often without centralized oversight.

This surge in unmanaged connectivity has created security blind spots. Poorly secured SaaS to cloud integrations and untracked APIs are merging into a sprawling attack surface that weakens visibility, posture management, and compliance. These hidden pathways offer threat actors easy opportunities for targeted intrusions, lateral movement, and sensitive data exfiltration.

As organizations adopt more multi-cloud, automated, and serverless architectures, API-centric risks are expected to intensify. By 2026 and beyond, Shadow IT is projected to fully evolve into cloud-native and API-driven ecosystems, where critical workloads and data flows may operate completely outside IT's view.

Countermove

To reduce the risks of unmanaged APIs, shadow IT, and cloud environment vulnerabilities, organizations need better cloud visibility and control with Cloud Security Posture Management (CSPM), threat intelligence context, and behavior-based detection solutions.



3.3

Artificial Intelligence in the Middle: The Rising Threat to Authentication

In today's digital ecosystem, identity authentication serves as the core layer of security. Multi-factor authentication (MFA), biometrics, passwordless systems, and other verification measures are designed to ensure that only legitimate users can access protected environments. However, adversaries are increasingly targeting this trust model by hijacking identities to initiate and sustain damaging attacks. One key tactic driving this trend is the Adversary-in-the-Middle (AiTM) attack.

AiTM frameworks are gaining traction across the cybercriminal community. These attacks enable threat actors not only to steal login credentials but also to exploit the ongoing authenticated access users maintain across devices, applications, and platforms. In their current form, such operations often demand a considerable amount of manual work — managing active sessions, ensuring persistence, and continuously bypassing authentication safeguards.

By 2026, this threat is expected to escalate significantly. With AI embedded into AiTM frameworks, cybercriminals will be able to automate large-scale session hijacking and credential harvesting. These autonomous attack systems will rapidly adapt to changes in authentication defenses, making verification tools increasingly ineffective.

As artificial intelligence moves to the center of identity exploitation, security teams will face a fast-evolving and highly automated threat that challenges the very basis of digital trust.

Countermove

Organizations need to move from credentials and point-in-time authentication checks toward continuous behavioural inspection. This allows them to identify hijacked or automated access even when credentials appear valid. Therefore, behaviour-based fraud protection and bot protection solutions are becoming critical for defense against such threats.

3.4

AI-Driven Malware: The Next Evolution in Autonomous Cyber Threats

Malware has continuously evolved, taking on more sophisticated and persistent forms that challenge even the most advanced cybersecurity defenses. Historically, most malicious software required manual interaction for execution and spread, but that landscape is shifting rapidly.

The integration of artificial intelligence (AI) is enabling a new generation of autonomous, self-propagating malware. These emerging threats are expected to mimic worm-like characteristics, allowing compromised systems to act as active broadcasters of infection rather than simple endpoints.

Although self-spreading malware is not new, past incidents underscore the significant damage potential. WannaCry exploited a Windows vulnerability to trigger a global outbreak within hours. NotPetya demonstrated the dual utility of malware in both ransomware operations and destructive cyberwarfare. Mirai leveraged insecure Internet-of-Things devices to launch massive distributed denial-of-service (DDoS) attacks. These attacks caused billions of dollars in losses, largely because threat actors successfully automated propagation across vast digital environments.

Looking ahead in 2026, there will be an increase in experimentation with AI-assisted automation across parts of the cyber kill chain, particularly in reconnaissance, evasion, modularity, and social engineering. As cybercriminals embrace AI-powered automation, the risk of the first truly AI-driven worm epidemic remains a possibility, representing a shift that will redefine how cybersecurity teams must detect, respond to, and contain malware outbreaks.

Countermove

To address faster, more automated, AI-assisted attacks, organizations need stronger predictive capabilities and pre-emptive actions that can not only operate at machine speed but also help stay a step ahead by anticipating emerging attack techniques.

3.5

Agentic Extortion: The Next Stage of Ransomware Evolution

Ransomware has intensified from a purely technological menace into a calculated psychological weapon. The shift from mass data theft to targeted single, double, and even triple extortion attacks shows how far threat actors are willing to go, including coercing insiders to maximize leverage. Ransomware-as-a-Service (RaaS) has further industrialized cybercrime by enabling a mature underground economy of developers, operators, and affiliates with a shared goal of maximizing impact while reducing operational effort.

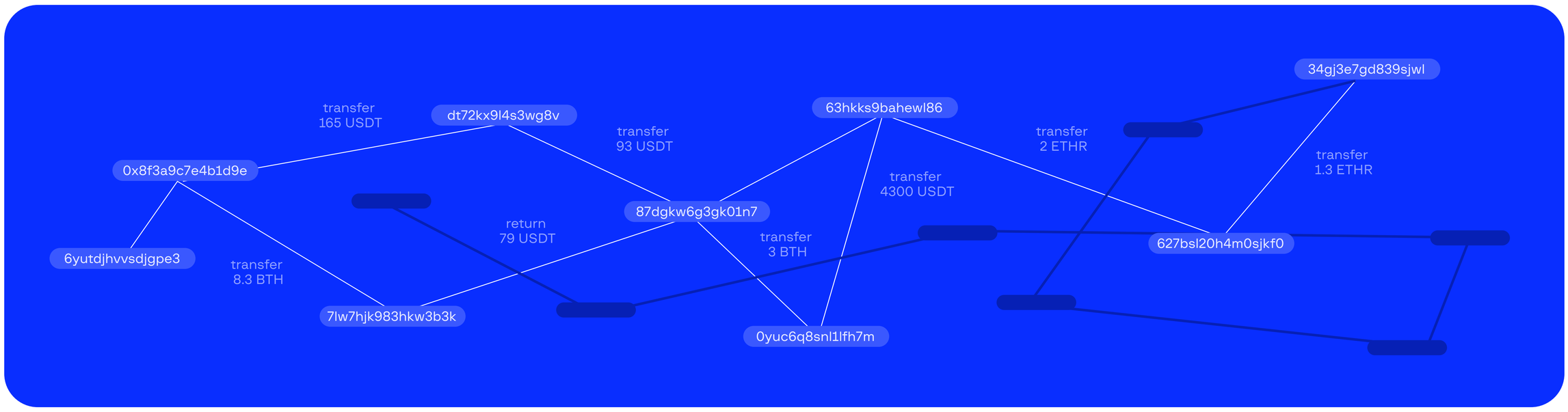
By 2026 and beyond, AI-led innovation is projected to significantly reshape the ransomware landscape. Criminal groups are expected to deploy autonomous AI agents to accelerate attacks once initial access is secured in a target environment. These intelligent agents are likely to become a core part of RaaS offerings, granting even low-skilled attackers access to advanced automated capabilities.

Substantial automation already exists across the ransomware kill chain. Threat actors rapidly encrypt servers and virtual environments, destroy backups, automate lateral movement, and disable security technologies such as Extended Detection and Response (EDR). AI-driven agents will amplify these tactics, enabling ransomware campaigns to scale faster, execute with greater precision, and outpace defenders by dramatically shrinking detection and response windows.

As ransomware evolves into agentic extortion, organizations should expect more dynamic, efficient, and psychologically aggressive attacks designed to pressure victims into quick compliance.

Countermove

As attackers compress their execution timelines and enable more agentic and automated ransomware operations, defenders need AI-based and threat-intelligence-driven detection to spot intrusion signals early, combined with automated response, containment, and pre-emptive actions that operate not just in real-time speed, but machine speed.



3.6

Crypto and Stablecoins: Financial Innovation or Expanding Cyber Vulnerability

Traditional financial institutions are rapidly integrating crypto rails and stablecoins to modernize payment systems and meet rising expectations for instant, transparent, and always-available value transfers across customers and institutions. Yet as this transformation accelerates, significant risks are advancing alongside it.

Global financial systems already face massive challenges from both fiat and crypto laundering. Trillions of dollars move illicitly through legitimate banking channels each year, and these figures are poised to increase as adoption of digital assets grows.

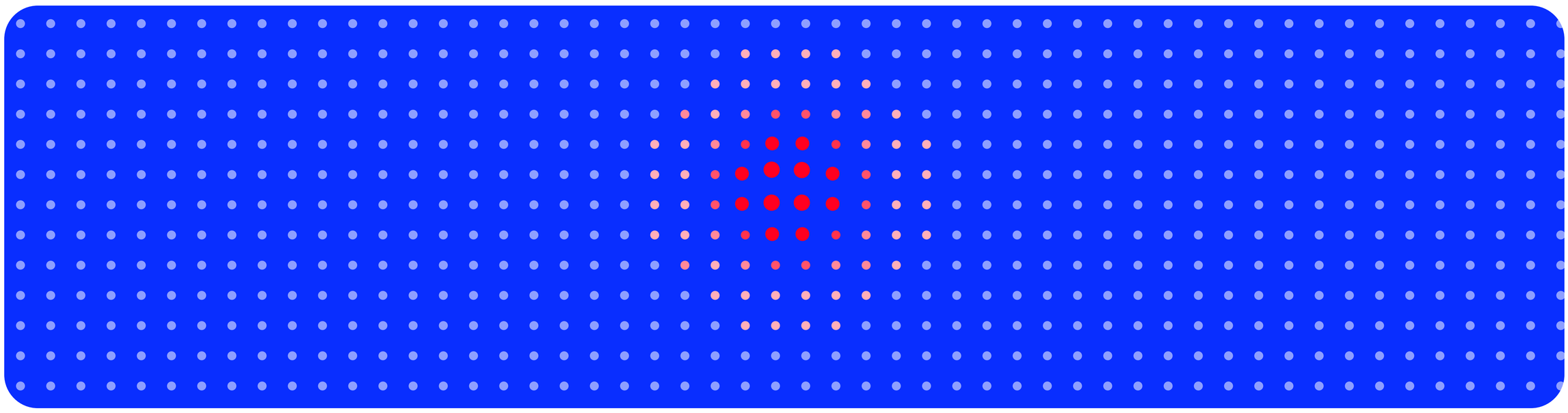
The tokenization of assets and deeper integration into crypto ecosystems will open the door for new and highly sophisticated fraud models. Criminal organizations are expected to intensify investment in automation and obfuscation technologies, enabling more seamless layering of funds and evasion of compliance controls. Increased exploitation of decentralized finance (DeFi), malicious smart contract toolkits, AI-assisted laundering bots, and techniques designed to erase transactional traceability will become more prevalent.

Beyond existing identity and authentication fraud challenges within the financial sector, crypto and stablecoins are set to play a larger role in fueling cybercrime economies. As banks move toward crypto-enabled infrastructure, striking the right balance between innovation and security will become crucial to preventing widespread financial exploitation.

Countermove

Crypto-enabled fraud is increasingly merging with traditional cybercrime. To respond, security teams need to fuse cyber and fraud controls (Threat Intelligence, Digital Risk Protection, and Fraud Protection) to identify coordinated activity across infrastructure, accounts, and network flows.

At the same time, adversaries do not operate either in fiat or crypto environments; they move fluidly between both. Organizations need controls capable of detecting fraud and money laundering activity across traditional and crypto financial systems.



3.7

The Psychological Power Behind Modern Phone Scams

Phone scams increasingly rely on psychological manipulation rather than purely technical deception. Many individuals believe they would never comply when confronted with a suspicious request, yet fear, urgency, and perceived authority often override rational decision-making in high-pressure moments.

These schemes are becoming more intrusive, more persuasive, and far more difficult to resist. Awareness alone is rarely enough to prevent victims from being coerced into dangerous actions.

In several regions, criminals no longer focus on harvesting card details, one-time passwords, or small payments, as these methods are losing effectiveness. Instead, social engineering techniques have advanced to a point where scammers can pressure victims into taking out substantial loans or liquidating major assets, including cars, apartments, or homes. This evolution reflects a shift toward high-reward, psychologically driven fraud as low-effort tactics become less profitable.

As these strategies continue to scale, the threat of phone scams will increasingly center on exploiting human emotion, not technology, making prevention far more complex.

Countermove

Phone scams succeed because they manipulate human behaviour, not just systems. Therefore, banks need to immediately shift to behaviour-based antifraud solutions that detect threats based on interactions and not just static rules or known scam indicators.

Additionally, these scams often operate in coordinated networks, targeting multiple victims using the same tactics. To disrupt them effectively, banks should rely on a real-time cyber fraud intelligence-sharing platform for collective visibility and to exchange indicators of active scams across regions and financial ecosystems.

3.8 Secure-by-Sovereignty, Exposed-by-Design

As digital sovereignty becomes a priority across many regions, data localization mandates are accelerating. These measures require data to be stored, processed, and shared strictly within national or regional borders. While this strengthens local control and compliance, it also creates unintended challenges for cybersecurity.

Regionalizing data can restrict the global visibility needed to combat wide-scale, coordinated threat campaigns. Cybercriminals operate without borders, rapidly shifting infrastructure and tactics worldwide, yet defenders increasingly face constraints that limit detection and response to a local perspective.

This raises a critical question: how can organizations and governments understand the full scale and intent of modern attack operations when their security insights are confined to regional boundaries?

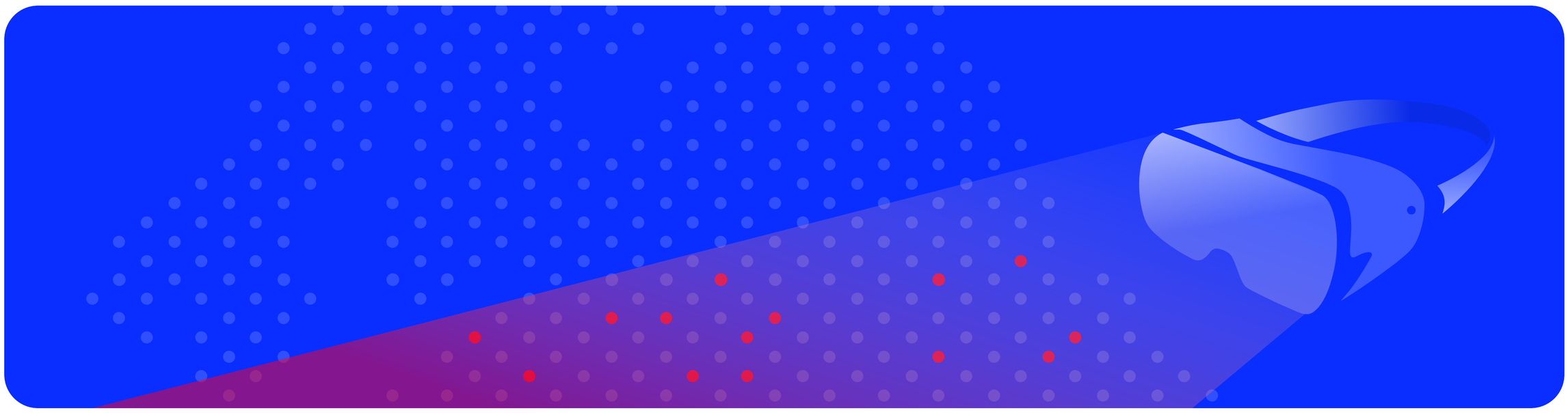
Group-IB has addressed this gap through a distributed network of Digital Crime Resistance Centers (DCRCs) designed to empower regional defense while leveraging a global ecosystem of threat intelligence. This model provides access to comprehensive insights on emerging threats, adversary tactics, techniques, and procedures (TTPs), and underground activity that influences attacks across borders.

Importantly, Group-IB's approach avoids transferring sensitive or regulated customer data. Instead, it relies on secure threat indicators and anonymized intelligence signals to strengthen detection and response. This ensures adherence to data localization and privacy laws while maintaining the global perspective required to counter internationally driven cybercrime.

Countermove

As digital sovereignty increasingly influences today's cybersecurity operations, organizations must not allow localization and compliance boundaries to become intelligence-sharing deterrents. There is a need for security models that deliver global threat visibility without violating regional data regulations. Group-IB addresses this gap through a distributed network of Digital Crime Resistance Centers (DCRCs) designed to empower regional defense while leveraging a global ecosystem of threat intelligence. This model provides access to comprehensive insights on emerging threats, adversary tactics, techniques, and procedures (TTPs), and underground activity that influences attacks across borders.

Importantly, Group-IB's approach avoids transferring sensitive or regulated customer data. Instead, it relies on secure threat indicators and anonymized intelligence signals to strengthen detection and response. This ensures adherence to data localization and privacy laws while maintaining the global perspective required to counter internationally driven cybercrime.



3.9

Wearable Devices: An Emerging Vector of Data Exposure

The concept of data capture is now moving beyond the digital space into the physical world, where security controls have far less visibility and impact. Wearable devices today can capture video, audio, and contextual data, allowing sensitive information displayed on a screen to be viewed and recorded without generating a digital record. When sensitive information is captured directly through the human eye through wearables operating in plain sight, the challenge becomes far harder to address.

Traditional privacy controls, such as screenshot blocking, privacy filters, or session monitoring, no longer apply. This shifts data loss and exfiltration from a technical problem to a behavioral and physical security challenge.

Countermove

Wearable devices introduce non-digital, unregulated avenues of data consumption and exposure. Therefore, traditional controls need to pivot to manage this challenge. Businesses must integrate physical, behavioral, and policy-based controls into their data protection programs. Data loss can occur at any time during a visual exposure, mandating restrictions and governance around wearable devices, especially in high-risk or sensitive industries. Parallely, detection and response must evolve beyond network- and endpoint-based approaches to include behavioral monitoring, contextual intelligence (for risk-awareness, not necessarily surveillance), capable of identifying nuanced, non-technical indicators of risks.

About Group-IB

1600+

Successful high-tech crime investigations

550+

Employees

600+

Enterprise customers

60

Countries

$1 bln+

Saved by our client companies through our technologies

#1

Incident Response Retainer

* According to Cybersecurity Excellence Awards

147+

Patents and applications

11

Unique Digital Crime Resistance Centers

Global partnerships

INTERPOL

EUROPOL

AFRIPOL

Recognized by top industry experts

FORRESTER®

datos INSIGHTS

kuppingercole ANALYSTS

Gartner®

IDC

FROST & SULLIVAN

Fight Against Cybercrime

GROUP-IB