High-Tech Crime Trends Report 2025

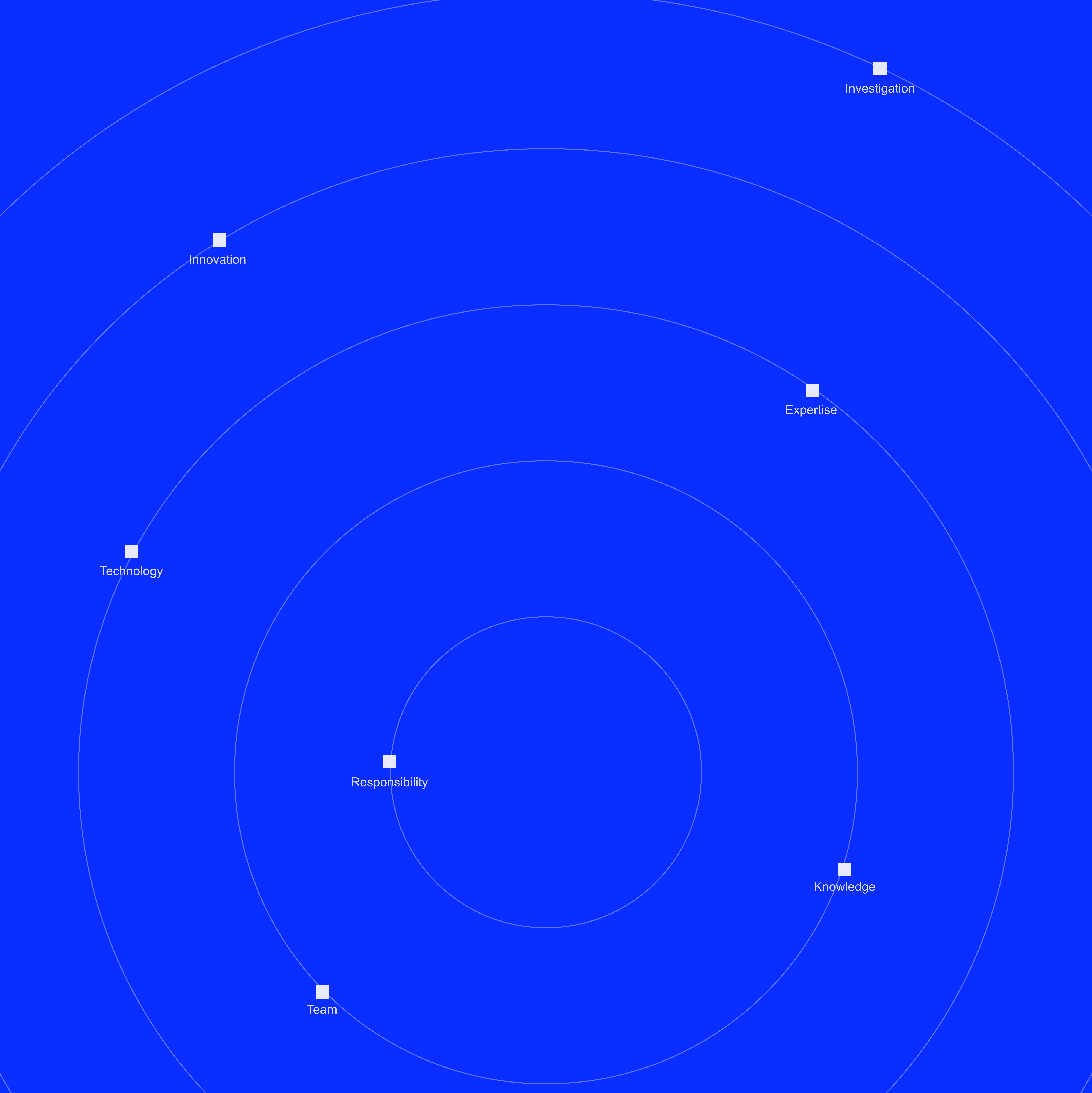
GROUP-IB

Fight against
cybercrime

Table of content

Methodology

Group-IB's High-Tech Crime Trends report is an annual, data-driven analysis of the evolving cybercrime landscape. Leveraging its Glocal Vision—a combination of deep local threat intelligence and a global analytical perspective—Group-IB delivers actionable insights that help organizations worldwide strengthen their cybersecurity posture. The report is built on proprietary research, intelligence gathering, and real-world cybercrime investigations. Group-IB experts, stationed across key cybercrime hotspots, track threat actors using unique tools that monitor dark web forums, dedicated leak sites (DLS), and underground marketplaces. Each year, our researchers identify and confirm trends in advanced persistent threats (APT), hacktivist activity, ransomware operations, initial access brokers (IABs), compromised hosts, data leaks, phishing, and scams. By mapping observed attacks to the MITRE ATT&CK framework and analyzing cybercriminal tactics, techniques, and procedures (TTPs), Group-IB not only provides a retrospective view of past cyber threats but also forecasts future risks with a high degree of accuracy. This predictive approach has been validated since the report's inception in 2012, making it an essential resource for businesses, governments, and cybersecurity teams worldwide.



Welcome to Group-IB’s High-Tech Crime Trends Report 2025

Welcome to Group-IB's High-Tech Crime Trends Report 2025

Dmitry Volkov
Chief Executive Officer,
Group-IB

The 2024 cyber threat landscape fortified the urgency of Group-IB's mission - to fight against cybercrime. Ransomware attacks saw an increase of 10% over 2023, with renewed attacks on the manufacturing, real estate, and professional services. Advanced Persistent Threats (APTs) grew more elusive, executing increasingly sophisticated campaigns that has increasingly focused on Europe and the Middle East and Africa. Financial losses from cybercrime reached staggering levels, while the number of data leaks and fraud incidents rose sharply. Perhaps most strikingly, artificial intelligence (AI) emerged as a double-edged sword, empowering defenders while simultaneously equipping attackers with new capabilities.

In the past year, our relentless commitment to fighting cybercrime delivered significant results, with notable achievements in dismantling cybercriminal networks and supporting investigations worldwide. Group-IB contributed to eight operations with local and international law enforcement agencies across more than 60 countries, enabling the arrests of key threat actors behind some of the most sophisticated attacks, and the disruption of their criminal networks. Together, we demonstrated that decisive action and global cooperation can bring meaningful progress.

As we turn our focus to 2025, the cybersecurity landscape will grow even more dynamic. Ransomware and APT tactics will evolve, pushing defenders to adopt increasingly proactive, intelligence-driven approaches. A fragmented global environment will amplify the importance of robust threat intelligence, while regulatory and technological shifts will shape how we adapt to emerging risks. Though these challenges are significant, they bring opportunities for innovation, and collaboration, and redefine how we continue to fight against cybercrime.

Yet, the path forward is not without its obstacles. The growing trend of deglobalization complicates the fight against cybercrime. Cross-border investigations and intelligence sharing are increasingly constrained by jurisdictional divides, creating gaps that cybercriminals are quick to exploit.

To counter these challenges, unified efforts and strategic investments are indispensable. For cybersecurity leaders, the priority must be on building robust, adaptive defenses and integrating threat intelligence into every layer of their operations. For governments and law enforcement agencies, collaboration across jurisdictions and support for private-public partnerships will be critical to dismantling transnational cybercriminal networks and safeguarding societies worldwide.

This year marks the 21st anniversary of Group-IB - a milestone we've marked as our "Age of Discovery". Over two decades, we have remained steadfast in our mission to protect the digital realm, fortified by the trust and confidence of our clients, partners, and law enforcement agencies. As we look to 2025 and beyond, we are committed to deeper collaboration, sharper innovation, and unwavering dedication to the fight against cybercrime.

Thank you for your partnership on this journey. Together, we can build a safer digital future.

Executive Summary

The Group-IB High-Tech Crime Trends Report 2025 presents a comprehensive analysis of the evolving cyber threat landscape and its impact on industries worldwide. The report highlights the significant rise in cybercrime activities, including ransomware, advanced persistent threats (APTs), data leaks, and financial fraud, with a particular emphasis on the growing role of artificial intelligence in both cyber defense and cyberattacks.

Cybercrime in 2024: A year of cybercriminal escalation

The past year witnessed a dramatic surge in cyber threats, emphasizing the urgency of proactive cybersecurity measures. Ransomware attacks increased by 10% compared to 2023, with targeted strikes on manufacturing, real estate, and professional services. Advanced Persistent Threats (APTs) became more elusive, leveraging increasingly sophisticated tactics, techniques, and procedures (TTPs) to breach networks, conduct cyber espionage, and steal critical data. The financial impact of cybercrime reached unprecedented levels, with sharp rises in fraud incidents and data breaches. At the same time, artificial intelligence (AI) became a double-edged sword, empowering cybersecurity professionals with automation and threat detection capabilities while simultaneously enabling cybercriminals to develop more advanced attacks.

In response to the escalating cyber threat landscape, Group-IB intensified its global fight against cybercrime. The company actively contributed to eight major law enforcement operations across more than 60 countries, resulting in the arrests of 1,221 cybercriminals and the dismantling of over 207,000 malicious infrastructures. These operations played a crucial role in disrupting large-scale cybercriminal networks, underscoring the importance of collaboration between private cybersecurity firms and international law enforcement agencies.

Key cybersecurity threats in 2025

Ransomware continues to be one of the most pervasive cyber threats, with the Ransomware-as-a-Service (RaaS) model fueling its rapid expansion through its affiliate networks. Ransomware operators have refined their methods, focusing not only on encryption but also on data exfiltration and extortion. Dedicated Leak Sites (DLS) saw a 10% increase in 2024, highlighting the growing trend of cybercriminals publishing stolen data when ransom demands are not met.

Advanced Persistent Threats (APTs) continue to be a major concern, particularly as geopolitical tensions intensify. State-sponsored actors have significantly escalated their activities, with Europe, the Middle East and Africa becoming primary targets for cyber espionage campaigns. Groups such as APT28, Lazarus, and Dark Halo have demonstrated in the past year of their ability to exploit vulnerabilities in enterprise software, cloud environments, and supply chain networks to gain long-term access to sensitive data.

Cybercriminal infrastructure has expanded dramatically, with phishing attacks increasing by 22% year-on-year. Group-IB identified more than 80,000 phishing websites in 2024, with the logistics, travel, and internet services industries emerging as primary targets. Cybercriminals have increasingly adopted sophisticated social engineering tactics, crafting highly convincing fake websites and fraudulent communications to deceive users into divulging their credentials. In parallel, scam operations have grown in scale and complexity, affecting a wide range of industries, including financial services, logistics, and telecommunications.

Initial Access Brokers (IABs) have also gained prominence, offering access to compromised corporate networks on underground forums. The number of IAB listings saw an increase of 15% year-on-year, with North America, Europe, and Latin America experiencing the most significant rise.

Data breaches and dark web activity remain a significant challenge, with cybercriminals leveraging stolen credentials to infiltrate corporate networks and personal accounts. In 2024 alone, more than 6.4 billion records were leaked, including email addresses, passwords, and financial data. Underground Clouds of Logs (UCL) have become a key component of the cybercrime economy, allowing threat actors to acquire vast amounts of compromised data at minimal cost. The increasing availability of such data fuels further cyberattacks, reinforcing the need for stronger cybersecurity practices across all sectors.

Challenges Ahead: Deglobalization and the growing complexities of cybercrime

The increasing trend of deglobalization is making cross-border cybercrime investigations more difficult, as legal and jurisdictional barriers hinder intelligence sharing and international collaboration. Cybercriminals are taking advantage of these gaps, leveraging anonymized infrastructure, cryptocurrencies, and decentralized financial systems to evade law enforcement. Additionally, artificial intelligence is accelerating the sophistication of cyberattacks, with AI-powered phishing, deepfake-based social engineering, and adaptive malware becoming more prevalent. The rapid expansion of cloud computing, remote work, and IoT devices has further widened the attack surface, exposing businesses and critical infrastructure to more complex and large-scale cyber threats. Many organizations continue to struggle with implementing effective cybersecurity strategies, leaving vulnerabilities that attackers are quick to exploit.

The way forward: Strengthening global cybersecurity

To counter these evolving threats, organizations must adopt intelligence-driven security strategies that incorporate real-time threat intelligence, AI-powered defense mechanisms, and proactive security frameworks. Strengthening cybersecurity awareness and training is essential, as phishing and social engineering remain key attack vectors. Businesses must implement robust security measures, such as multi-factor authentication, endpoint detection and response (EDR), and zero-trust architectures to enhance their resilience. Public-private collaboration is crucial in dismantling transnational cybercriminal networks, with governments and law enforcement agencies needing to work closely with cybersecurity firms to enhance intelligence sharing and regulatory enforcement. As cybercrime continues to evolve, strategic investments, global cooperation, and adaptive security approaches will be key to building a safer and more secure cyberspace for businesses and society at large.

Interconnectivity of cybercrime and geopolitics

GROUP-IB

Deglobalization & geopolitical tension

New techniques

01 ClickFix

02 Extended attributes attack

03 Nearest neighbour attack

Target telco: New tactics for espionage and disruption

Undersea cable disruption in Europe & Africa

Steatite network disruption in Ukraine

Infiltration of US government wiretap systems

European region

45.31% share of all attacks

Most active threat actors:

APT28	Dark Halo
Gamaredon	Core WereWolf
Cloud Atlas	Sticky WereWolf

Middle East and Africa

23.05% share of all attacks

Most active threat actors:

OilRig	RocketKitten
MuddyWatter	APT33

Asia-Pacific region

21.88% share of all attacks

Most active threat actors:

DarkPink	APT37
APT10	OceanLotus
Lazarus	

Increased state-sponsored threat actor activity, with

58% compared to 2023

828 cyberattacks in 2024

15.5% of all attacks Government and military

Growth of hacktivism

Distributed-Denial-of-Service (DDoS) is the main activity.

The most powerful attack in 5.6Tbps UDP

Asia-Pacific region is the most attacked region, with India as the #1 target

Top 10 hacktivist groups:

DDOSIA	Tengkorak Cyber Crew
ETHERSEC TEAM CYBER	DarkStormTeam
RipperSec	IT ARMY of Ukraine
SYLHET GANG-SG	Lulz Security Agency
THE ANONYMOUS BD	Indonesia anonymous

Surge in data leaks

due to state sponsored threat actors and hacktivist attacks

Top 3 countries from which data was leakes:

- United States
- Russia
- India

In 2024, 1,107 new instances of data being leaked into the public domain

Data leaks contribute to fraud

Surge in fraud

Web phishing and scams grow by

22% compared to 2023

38% of scams target the travel industry

Artificial intelligence-driven fraud

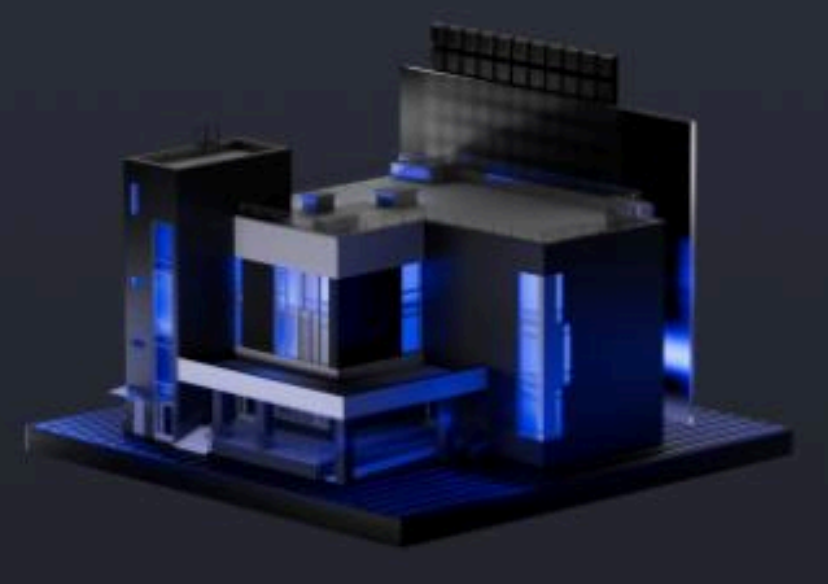
Voice and video deepfakes for scams

Banking trojans for Android and iOS to capture photo, video in order to create deepfakes

Know-Your Customer (KYC) bypass.

GoldFactory malware family with focus on Asia-Pacific

Widespread impact globally



200+ Indonesian government agencies paralyzed after attack on data center

140 hospitals (Ascension) across 19 states suffered a ransomware attack that severely disrupted its operations

186 state department websites have been shut down for 60 hours due to malware

Growth of cybercrime

Underground Clouds of Logs (UCL) keep growing for initial access

56.8% of access acquired by Ransomware-as-a-Service groups

25% by Advanced Persistent Threat groups

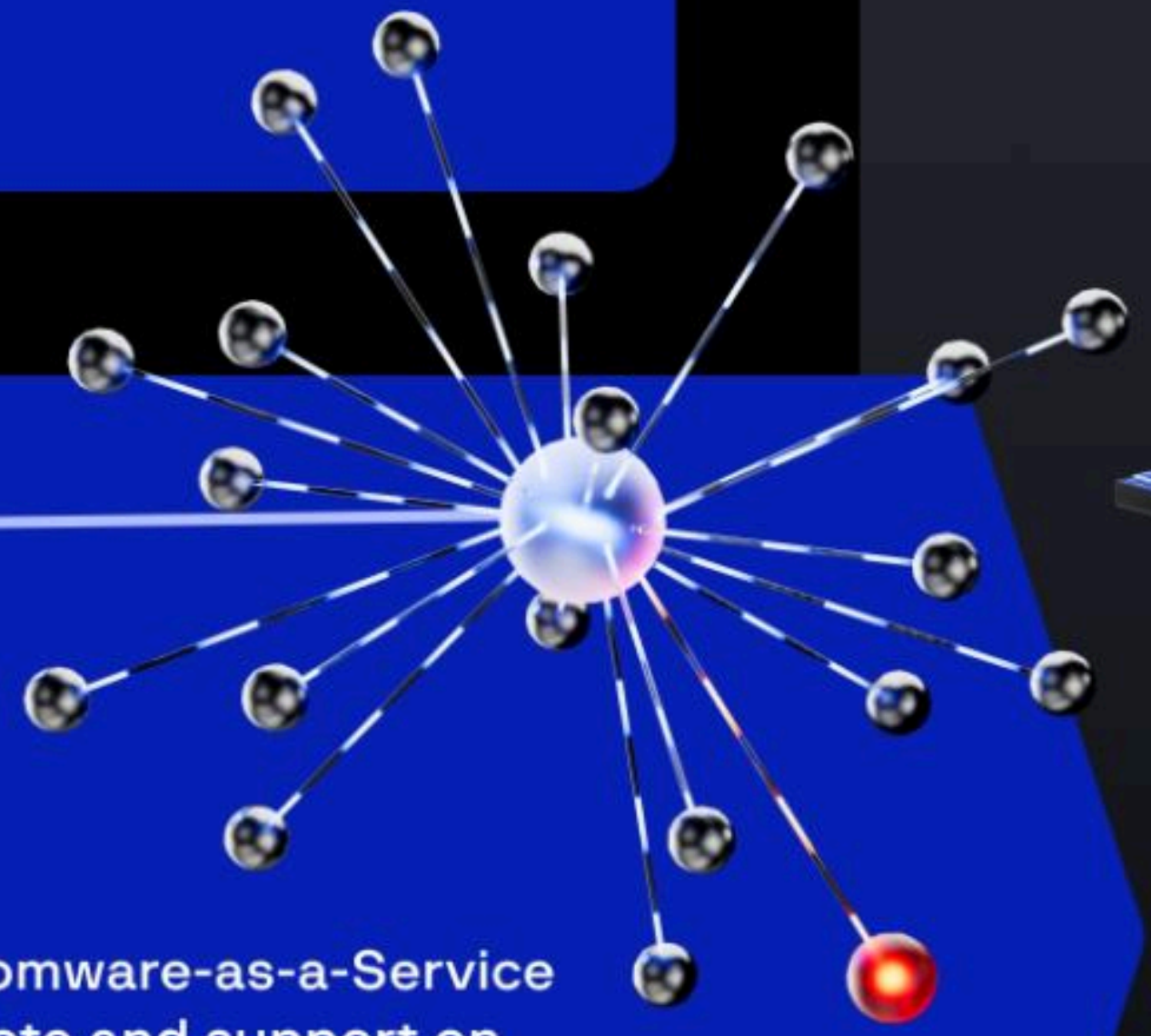
39 new Ransomware-as-a-Service groups — 44% over 2023

5,066 attacks published on DLSs in 2024 — 10% over 2023

The United States is the most attacked

48.53% of total number of attacks

3,055 Initial Access Brokers (IABs), instances of access — 15% over 2023



Ransomware-as-a-Service promote and support on 19 dark web forums

RAMP forum the most popular

About Group-IB

1550+	Successful high-tech crime investigations
400+	Employees
600+	Enterprise customers
60	Countries
$1 bln	Saved by our client companies through our technologies
#1	Incident Response Retainer
120+	Patents and applications
11	Unique Digital Crime Resistance Centers

Global partnerships

INTERPOL

EUROPOL

AFRIPOL

Recognized by top industry experts

FORRESTER

Aite Novarica

kuppingercole ANALYSTS

Gartner

IDC

FROST & SULLIVAN

Contributions to Law Enforcement Operations in 2024

Group-IB has been a firm advocate in private and public partnerships to combat the growing threat of cybercrime, and it is committed to enhancing global cybersecurity through strategic partnerships and collaborations with law enforcement agencies, both locally and internationally.

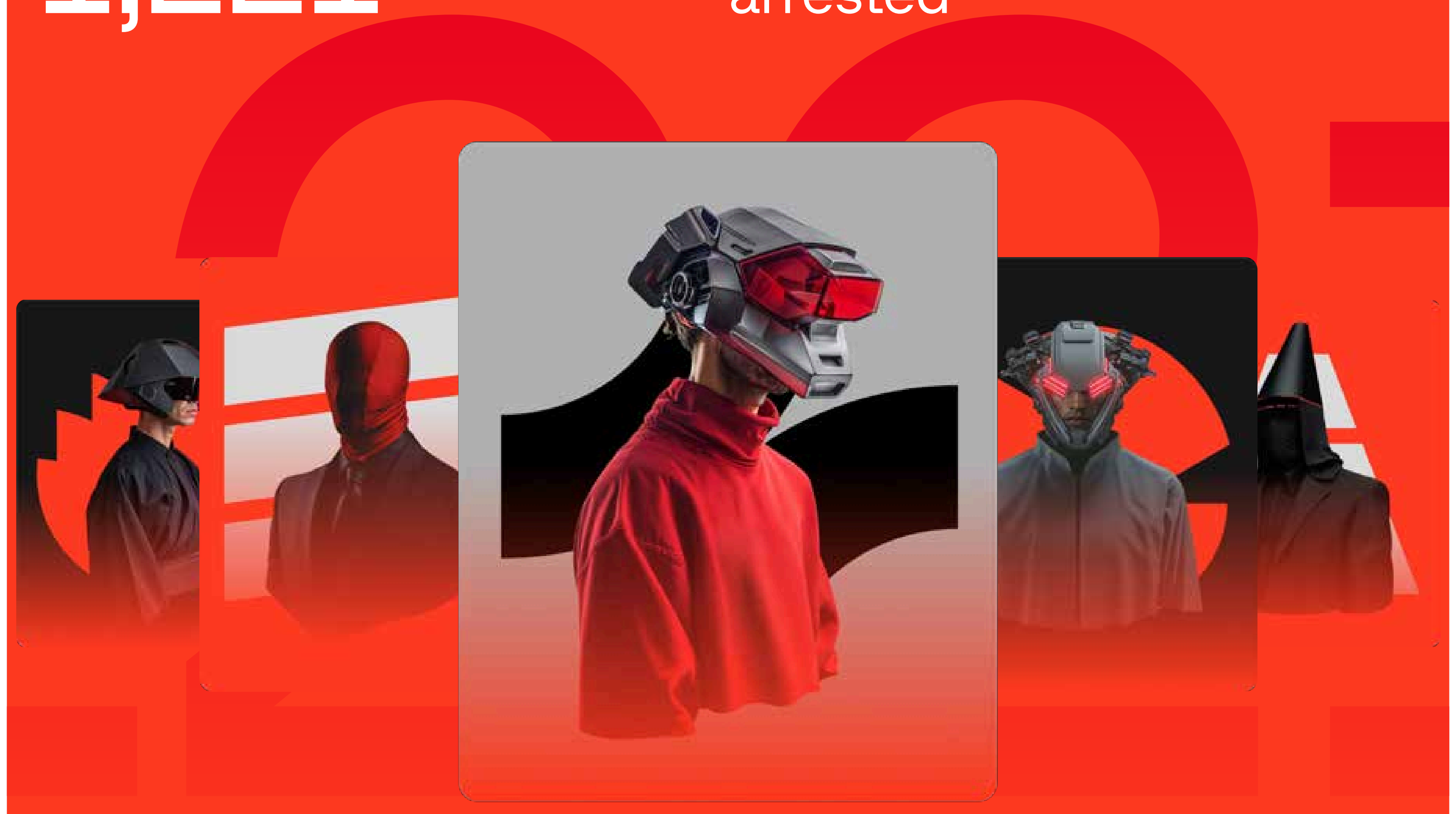
In 2024, Group-IB contributed mission critical data and investigative research that supported eight local and international law enforcement operations. By leveraging its expertise in threat intelligence, digital forensics, and cybercrime investigations, Group-IB continues to play a crucial role in assisting authorities in combating cyber threats and criminal activities.

8

Total Number of Law Enforcement Operations

1,221

Cybercriminals arrested



207,442

Dismantled malicious infrastructure (resources)

522,484

Estimated number of victims

$222 mln

Total estimated financial losses (in USD$)

Timeline

2024

Operation Synergia

Malware Phishing Ransomware

February

Operation Synergia, an INTERPOL-led initiative involving 60 law enforcement agencies across 50+ countries, targeted transnational cybercrime from September to November 2023. Group-IB identified over 2,400 malicious IPs linked to phishing, ransomware, and malware, sharing intelligence for coordinated action. The operation dismantled 70% of identified C2 servers and arrested 31 individuals, with 70 more suspects identified. Key efforts included takedowns in Europe, Asia-Pacific, Africa, and the Middle East. Highlights included Hong Kong and Singapore removing 239 servers and African nations arresting four suspects, while Kuwait supported victims and mitigated impacts.

Grandoreiro Malware

Malware Phishing

March

Group-IB assisted INTERPOL and Brazilian authorities in dismantling the Grandoreiro banking trojan operation, which defrauded victims of over €3.5 million since 2017. Spread via phishing emails, the malware allowed criminals to control victims' bank accounts and launder stolen funds. Between 2020 and 2022, Brazil and Spain collected malware samples and, with Group-IB's analysis, identified the malware's infrastructure and linked it to suspects. By August 2023, coordinated efforts led to house searches across five Brazilian states, resulting in five arrests. Authorities seized assets, dismantling the group's operations and recovering stolen funds.

LabHost

LabHost Phishing

April

Group-IB participated in a coordinated global takedown operation against prominent Canadian Phishing-as-a-Service (PhaaS) provider LabHost, which has led to the arrest of 37 suspects across the United Kingdom and around the world by law enforcement agencies. As part of the operation, Group-IB also conducted an extensive analysis of LabHost's criminal history and infrastructure, including insights into LabHost's administrative platform and the services it provides to its purported user base which exceeds 2,000 subscribers worldwide, who illegally obtained around 480,000 card numbers, 64,000 pin numbers, and over 1 million passwords from victims used for websites and other online services, according to law enforcement agencies.

Timeline

2024

Operation Distanthill

Phishing Remote Access Trojan

June

Group-IB supported "Operation DISTANTHILL," a joint effort by Singapore, Hong Kong, and Malaysian police to dismantle cyber fraud syndicates behind a 2023 Android Remote Access Trojan (RAT) campaign. Group-IB's analysis revealed over 250 phishing pages, C2 servers linked to 100+ malware samples, and insights into the syndicate's network. The campaign defrauded 4,000+ victims across Southeast Asia, including 1,899 cases in Singapore, with losses exceeding US$25 million.

Operation Kaerb

Phishing iOS

September

Group-IB supported "Operation Kaerb," an international effort led by Europol and Ameripol, in partnership with law enforcement and judicial authorities from Europe and Latin America, resulting in the arrest of 17 cybercriminals across Argentina, Chile, Colombia, Ecuador, Peru, and Spain. The operation dismantled the iServer phishing-as-a-service platform, active for five years, which targeted over 1.2 million mobile phones and defrauded approximately 483,000 victims worldwide. Among those arrested was the platform's administrator, an Argentinian national. The operation, conducted between September 10 and 17, 2024, marked a significant blow against global phishing operations targeting mobile users.

Operation Contender 2.0

Phishing Scams Business Email Compromise Impersonation

October

Group-IB contributed intelligence to INTERPOL's "Operation Contender 2.0," targeting cybercriminal syndicates in Africa. Led by INTERPOL's African Joint Operation against Cybercrime (AFJOC), the initiative combats threats like romance scams, business email compromise, and phishing. In April 2024, Nigerian police arrested two individuals behind a romance scam affecting a Finnish victim, while Côte d'Ivoire authorities apprehended six suspects linked to a phishing scam targeting Swiss citizens, causing $1.4 million in losses. The scammers used fake payment sites and impersonated customer service agents, with over 260 Swiss reports leading to their identification.

Timeline 2024

Operation Synergia II

Malware Phishing Ransomware

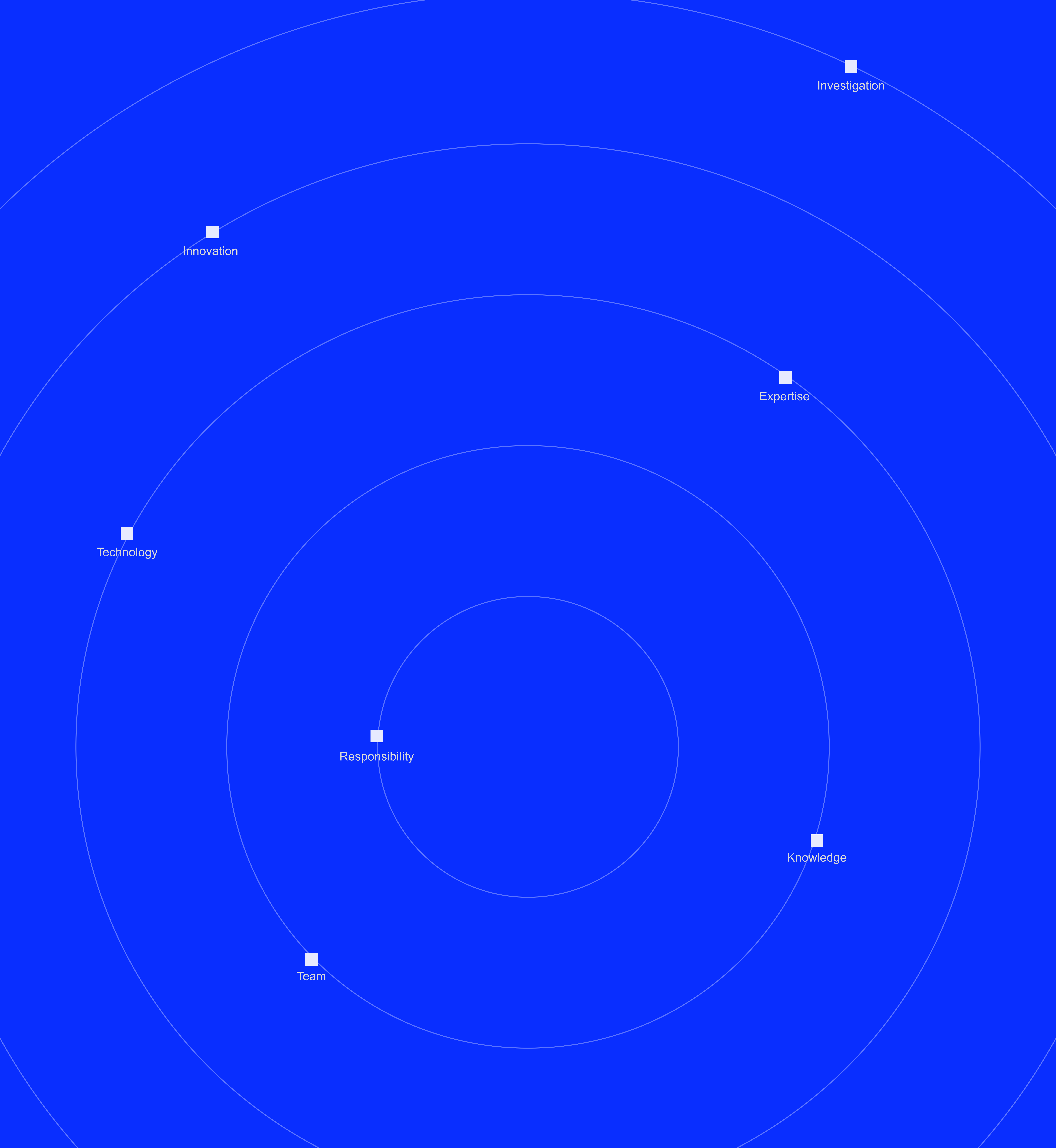
November

Group-IB supported "Operation Synergia II," an INTERPOL-led initiative involving 95 countries to combat phishing, ransomware, and malware attacks. The operation dismantled 22,000 malicious servers, seized 59 servers and 43 electronic devices, and led to 41 arrests, with 65 suspects under investigation. Group-IB analysts identified over 2,500 IPs linked to 5,000 phishing sites and 1,300 IPs tied to malware activities across 84 countries. In total, approximately 30,000 suspicious IPs were uncovered, significantly disrupting global cybercrime infrastructure.

Operation Serengeti

Business Email Compromise Data Stealers Distributed Denial of Service Phishing Ransomware Extortion

Group-IB participated in "Operation Serengeti," a two-month INTERPOL and AFRIPOL-led initiative targeting cybercrime across Africa. Conducted from September 2 to October 31, 2024, the operation led to 1,006 arrests, dismantled 134,089 malicious infrastructures, and identified over 35,000 victims with global losses nearing $193 million. Group-IB uncovered 10,000 Distributed Denial of Service (DDoS] attacks, 3,000 phishing domains, and data-stealer activities linked to African servers, contributing to actionable plans for dismantling cybercriminal networks. The operation disrupted ransomware, business email compromise, digital extortion, and online scams across the region.



Investigation

Innovation

Expertise

Technology

Responsibility

Knowledge

Team

Chapter 1: Global Cyber Threats

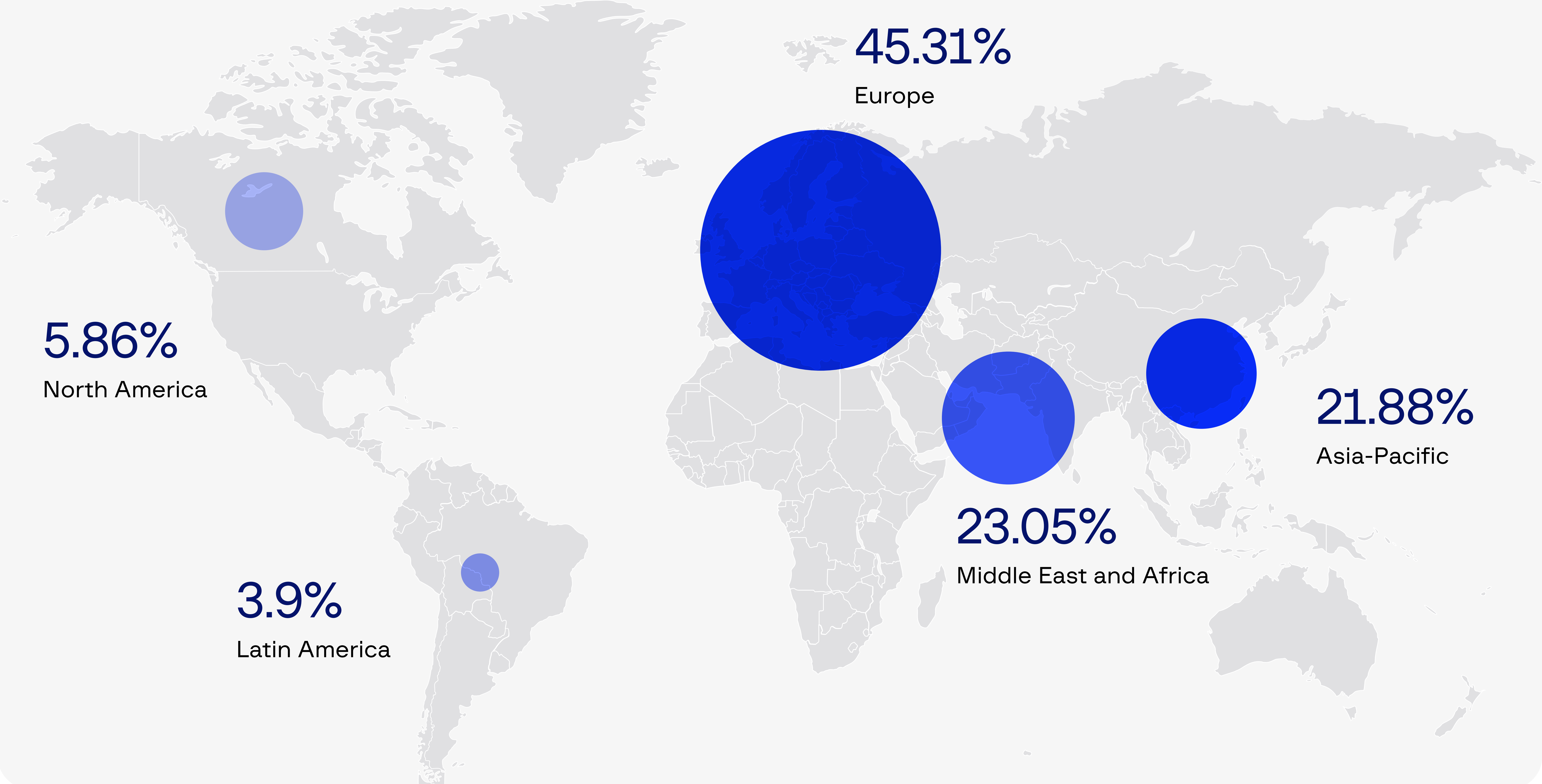
Advanced persistent threats

Advanced Persistent Threats (APTs) are long-term, targeted cyberattacks typically carried out by highly skilled and organized state-sponsored or financially motivated threat actors. These attackers aim to infiltrate a specific network or system and maintain unauthorized access for extended periods, gathering sensitive information or causing disruption. Unlike traditional cyberattacks, APTs are stealthy and carefully executed, with a focus on persistence and evasion of detection.

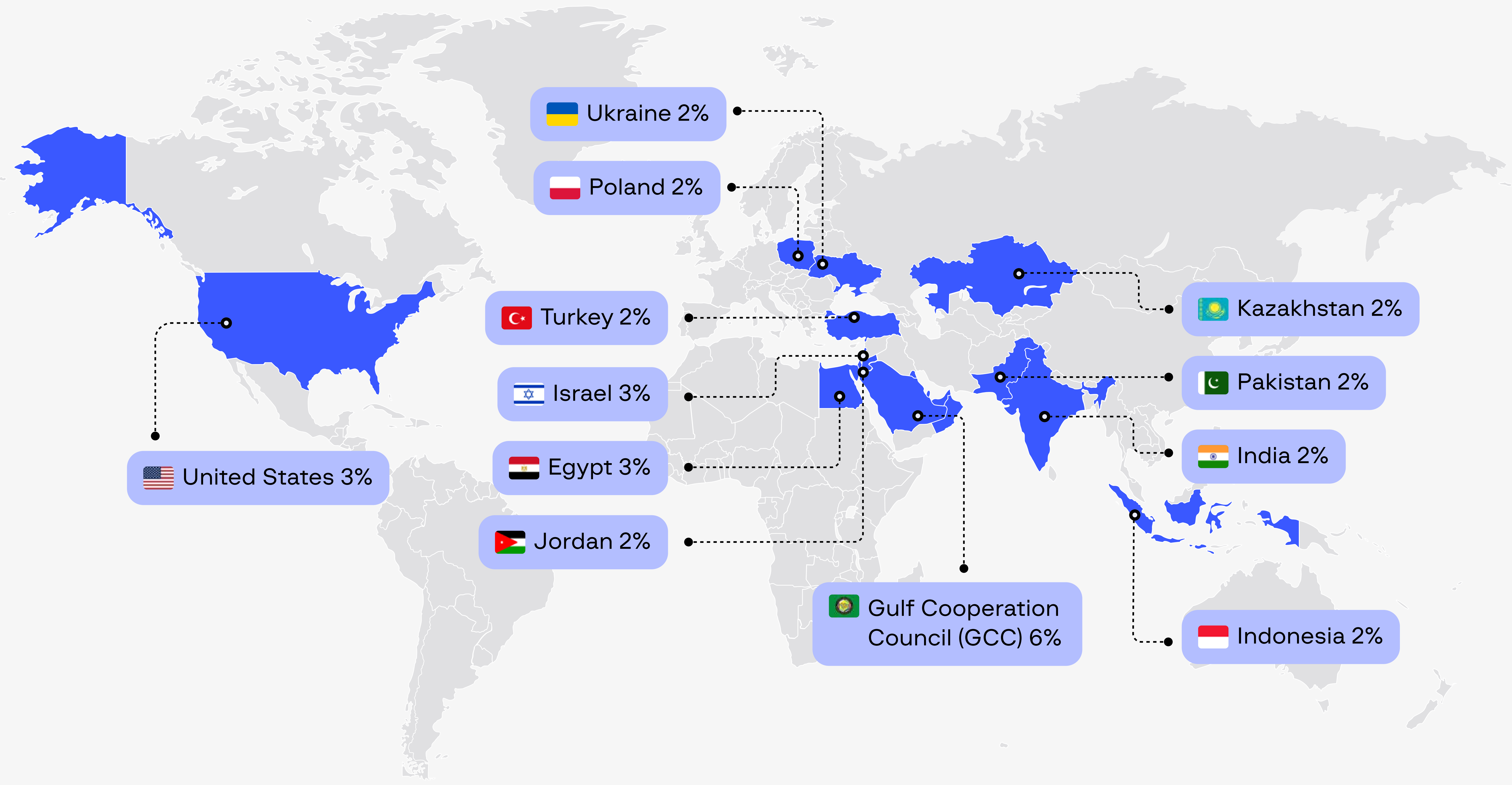
In 2024, Group-IB's Threat Intelligence team detected 828 cyberattacks attributed to APTs, an increase of 58% compared to 2023. State-sponsored actors have intensified their attacks on Europe (+18.24%) and the Middle East and Africa (+4.27%) regions in the past year, largely due to the ongoing political conflicts between Russia and Ukraine in Europe, as well as the tensions between Israel and the State of Palestine. These conflicts not only draw in various international stakeholders but also create an environment where cyber operations are used as tools of influence, disruption, and espionage, prompting state actors to exploit the geopolitical instability for their strategic objectives.

APTs have increasingly targeted specific industries, with the government and military sector being the most affected, accounting for 15.5% of attacks. This focus is driven by the sensitive information held by these industries, which can provide strategic advantages in geopolitical conflicts. The manufacturing sector (4.8%) is targeted due to potential disruption of supply chains and collection of trade secrets. Financial services (3.80%) are attacked for access to financial data and to create economic instability. The information technology sector (3.50%) is crucial for modern economies, making it a strategic target for exploiting vulnerabilities. Lastly, the science and engineering sector (2.30%) is targeted for its research capabilities, with state actors seeking to steal technological innovations.

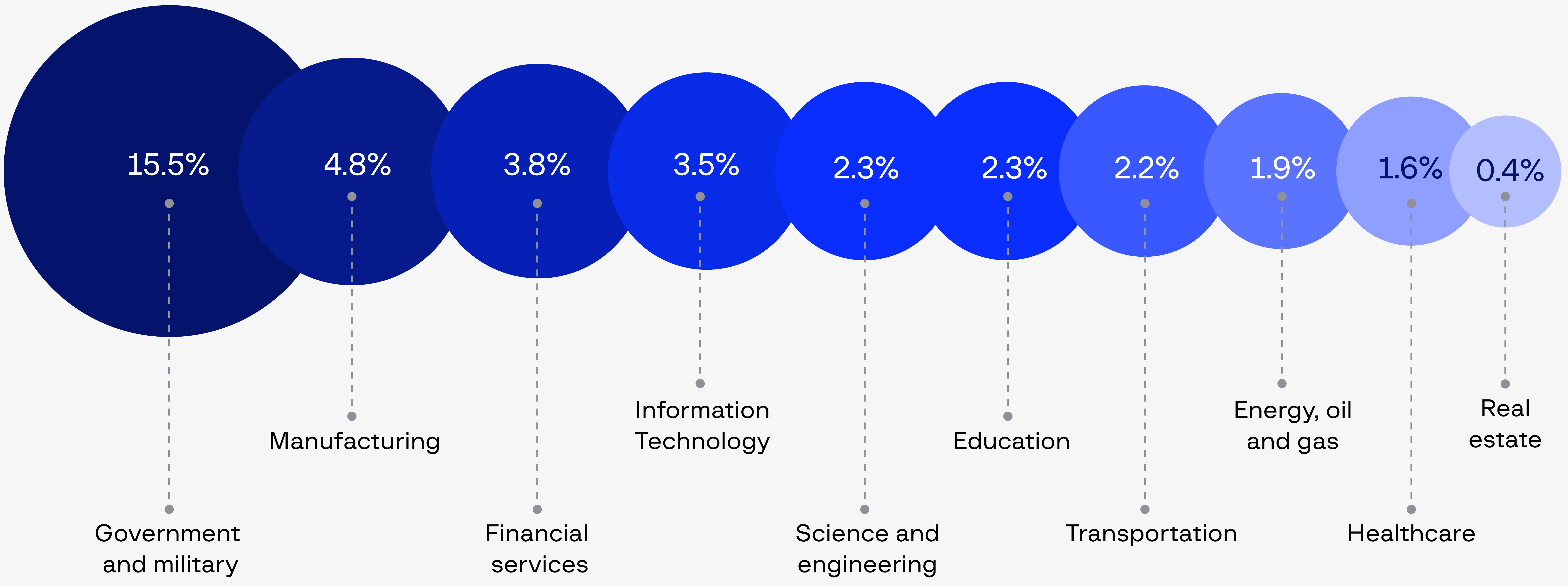
Global Distribution of cyberattacks conducted by APTs by region in 2024



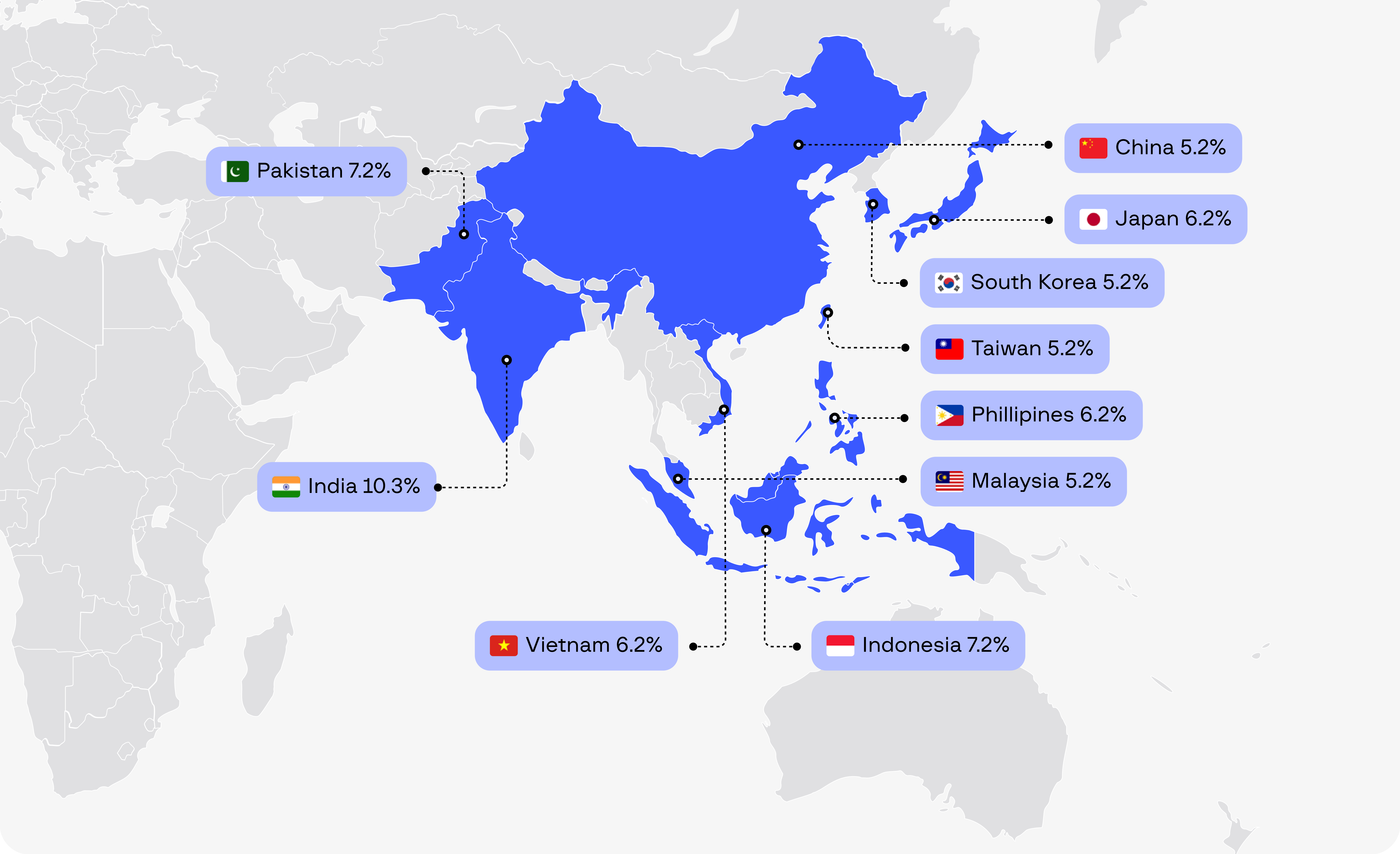
Global Top jurisdictions attacked by state sponsored threat actors



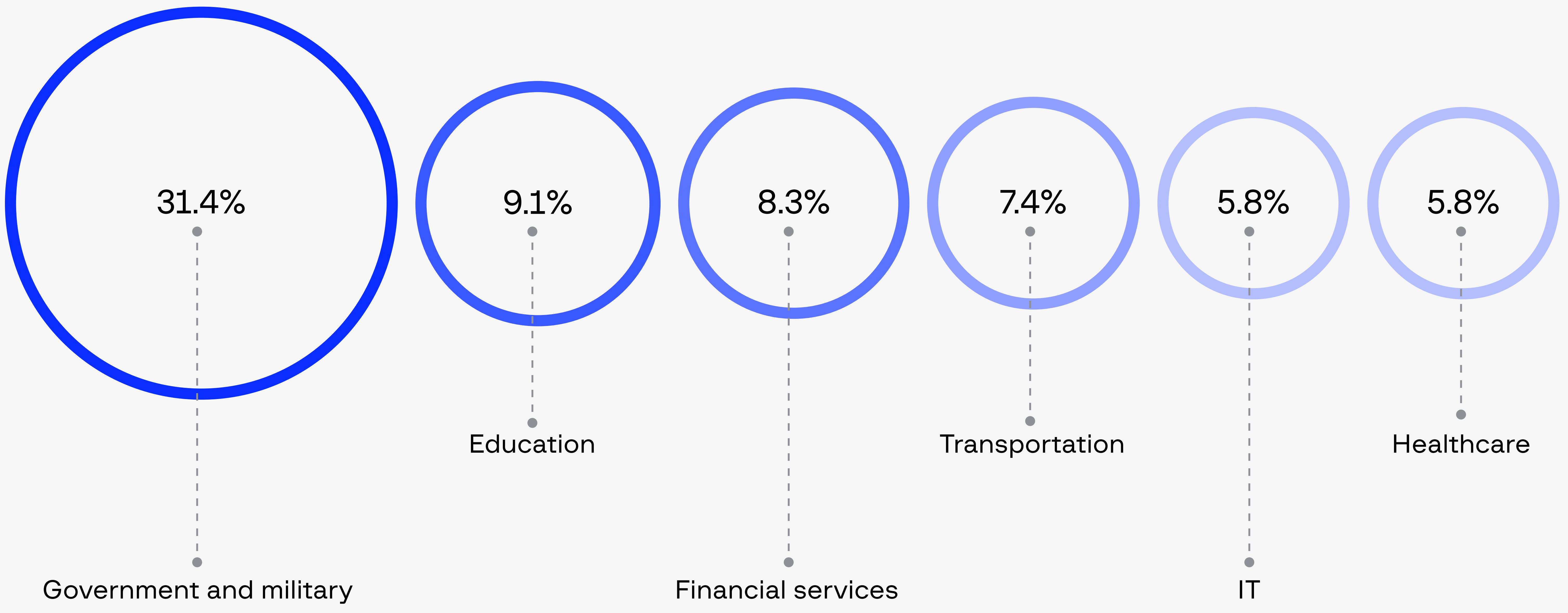
Global Top 10 industries targeted by APTs in 2024



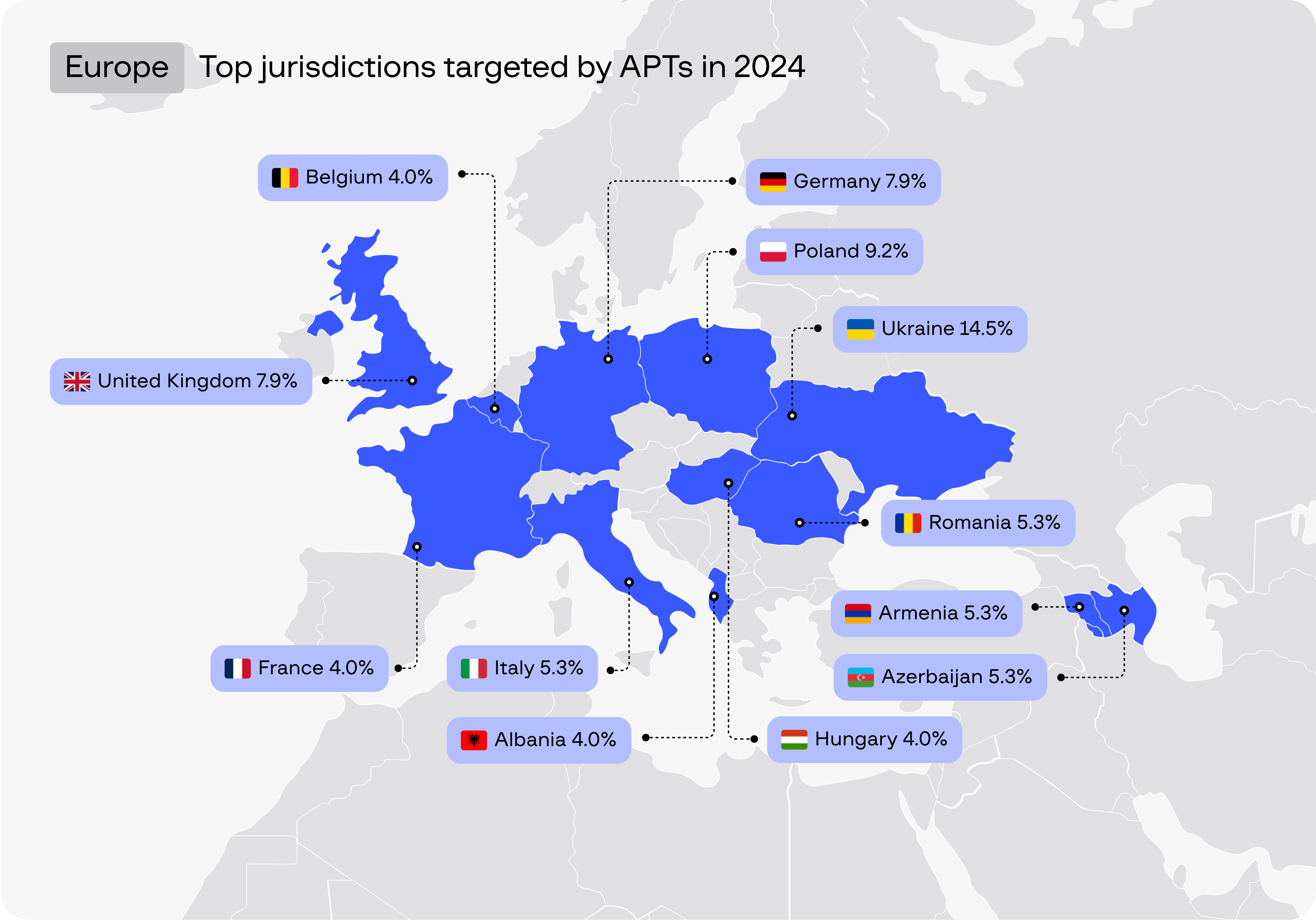
Asia-Pacific Top jurisdictions targeted by APTs in 2024



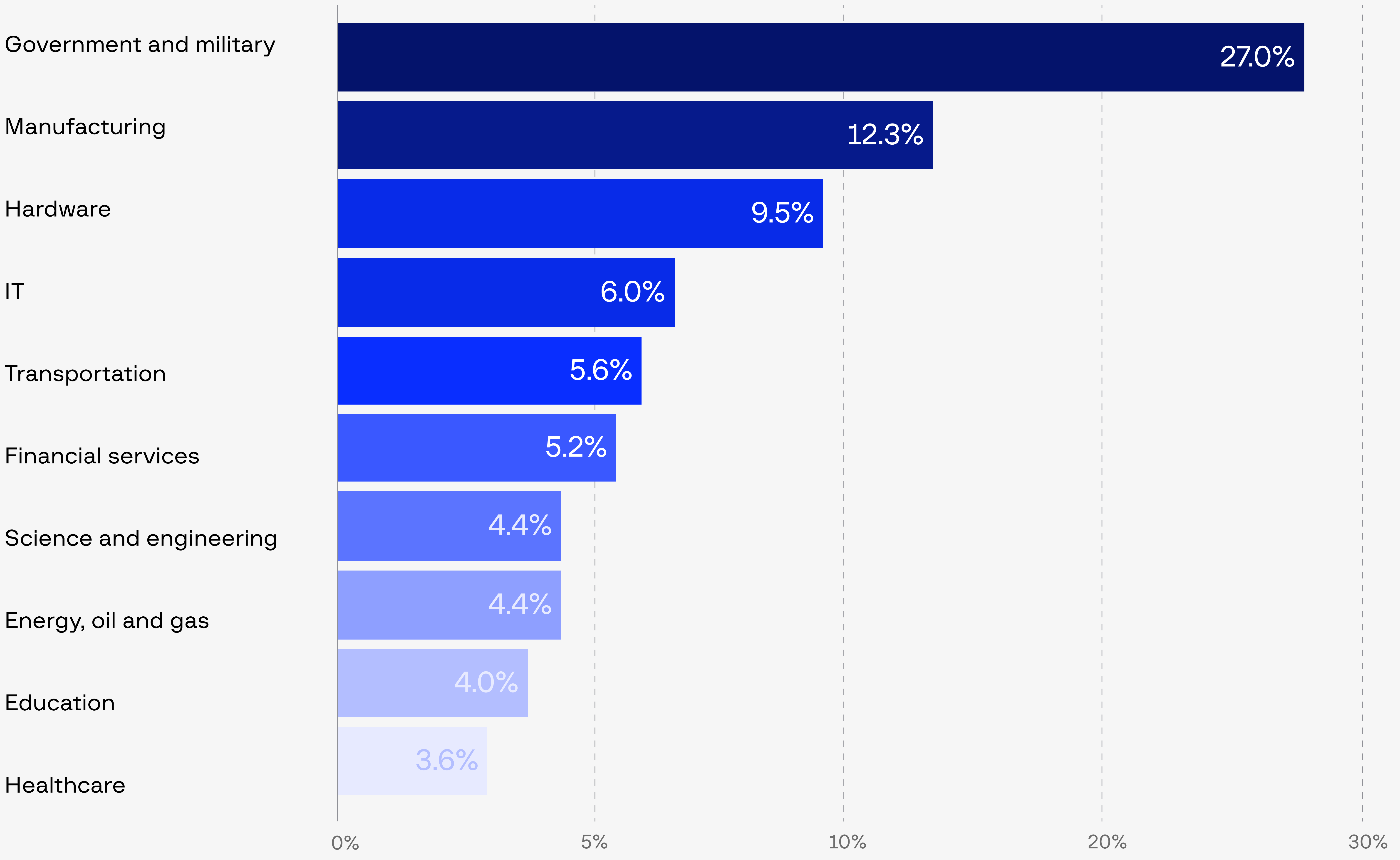
Asia-Pacific Top industries targeted by APTs in 2024



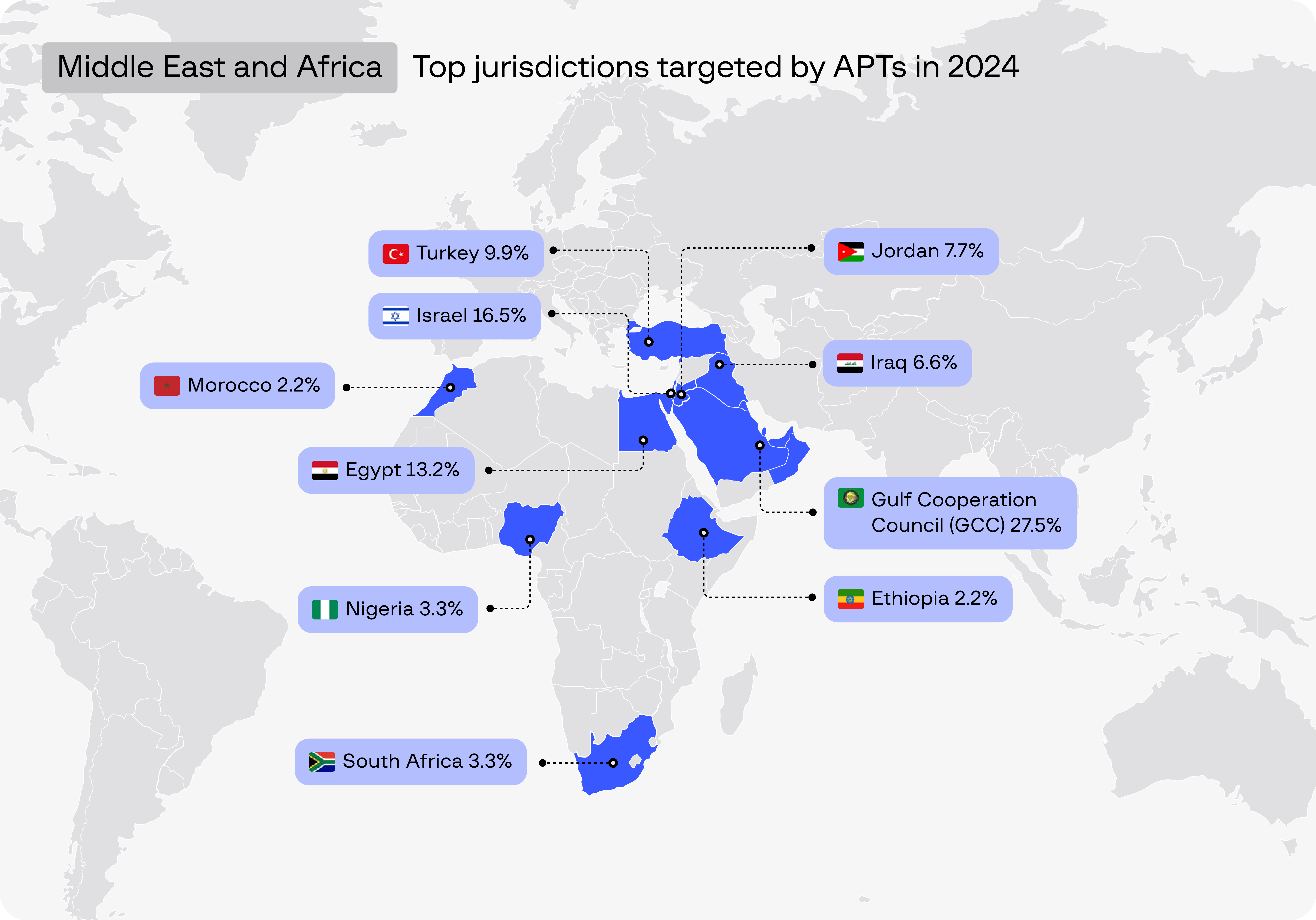
Europe Top jurisdictions targeted by APTs in 2024



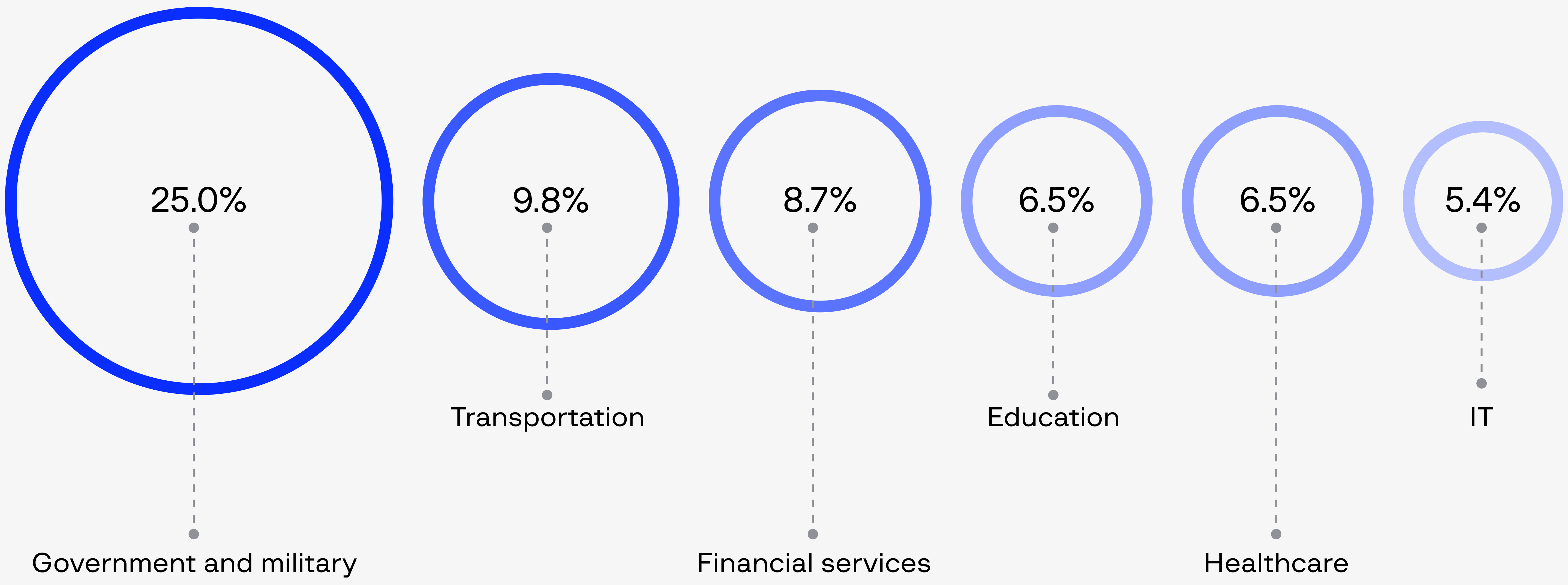
Europe Top industries targeted by APTs in 2024



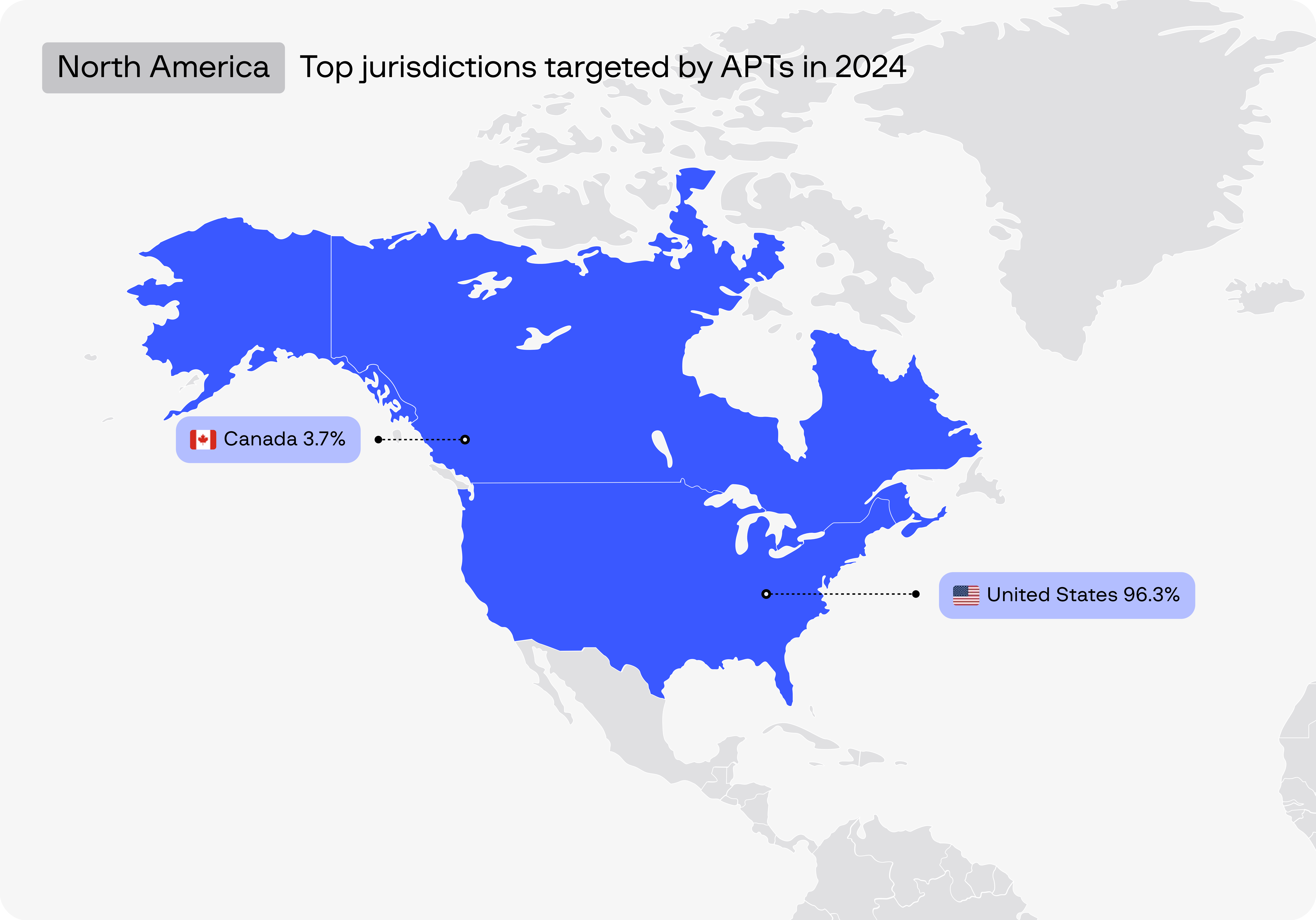
Middle East and Africa Top jurisdictions targeted by APTs in 2024



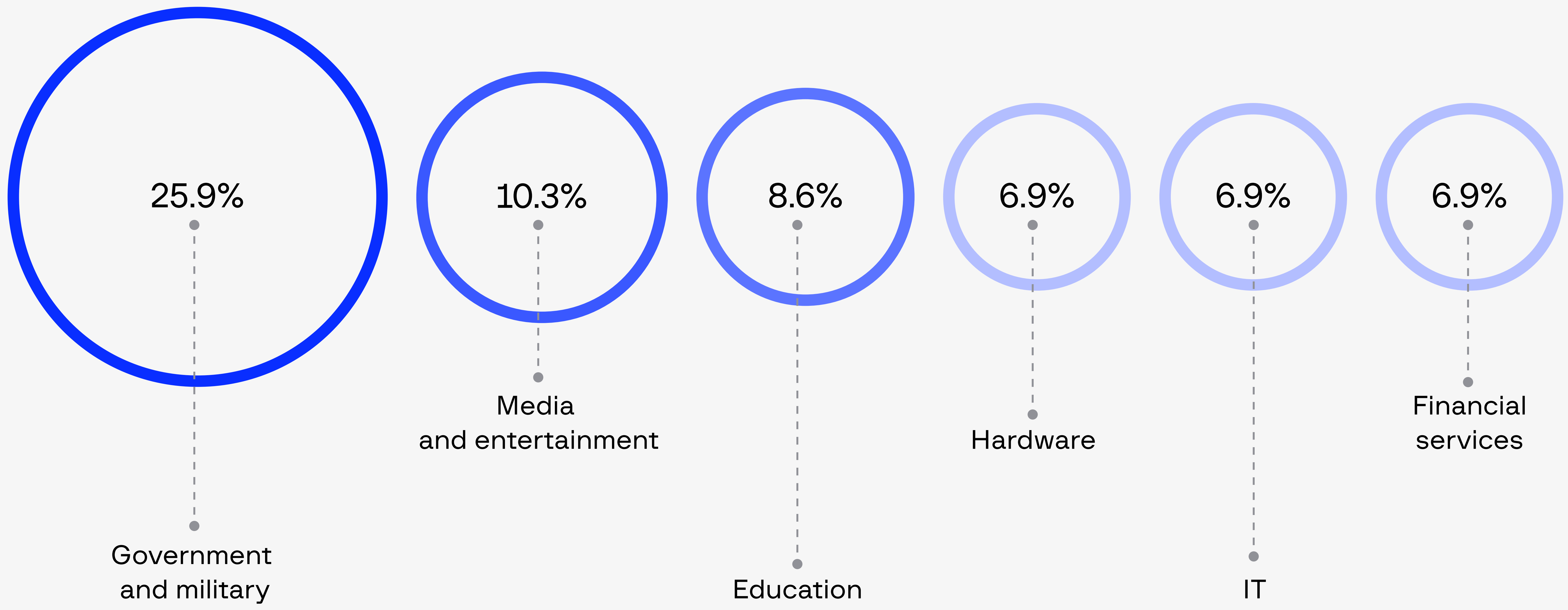
Middle East and Africa Top industries targeted by APTs in 2024



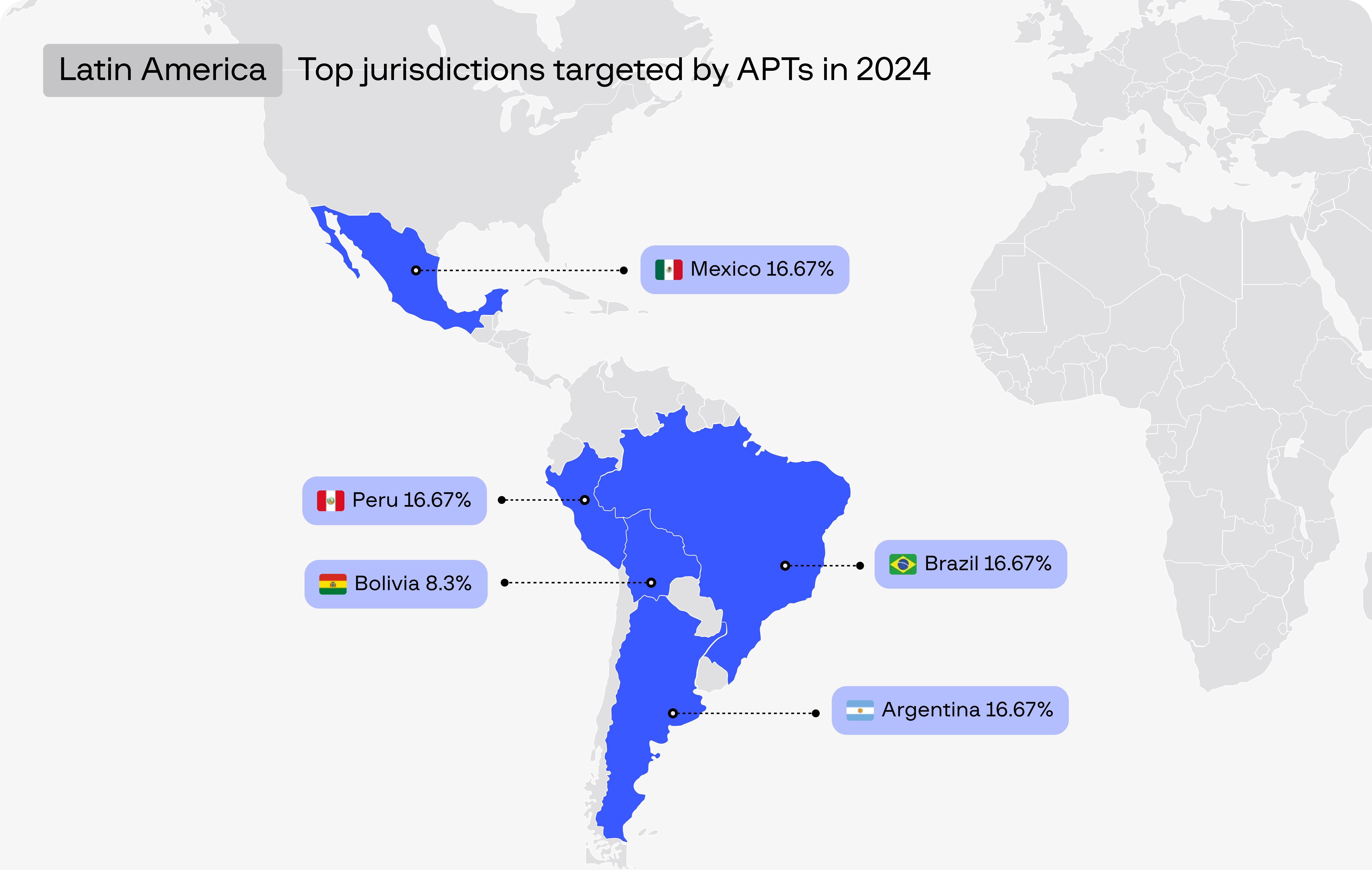
North America Top jurisdictions targeted by APTs in 2024



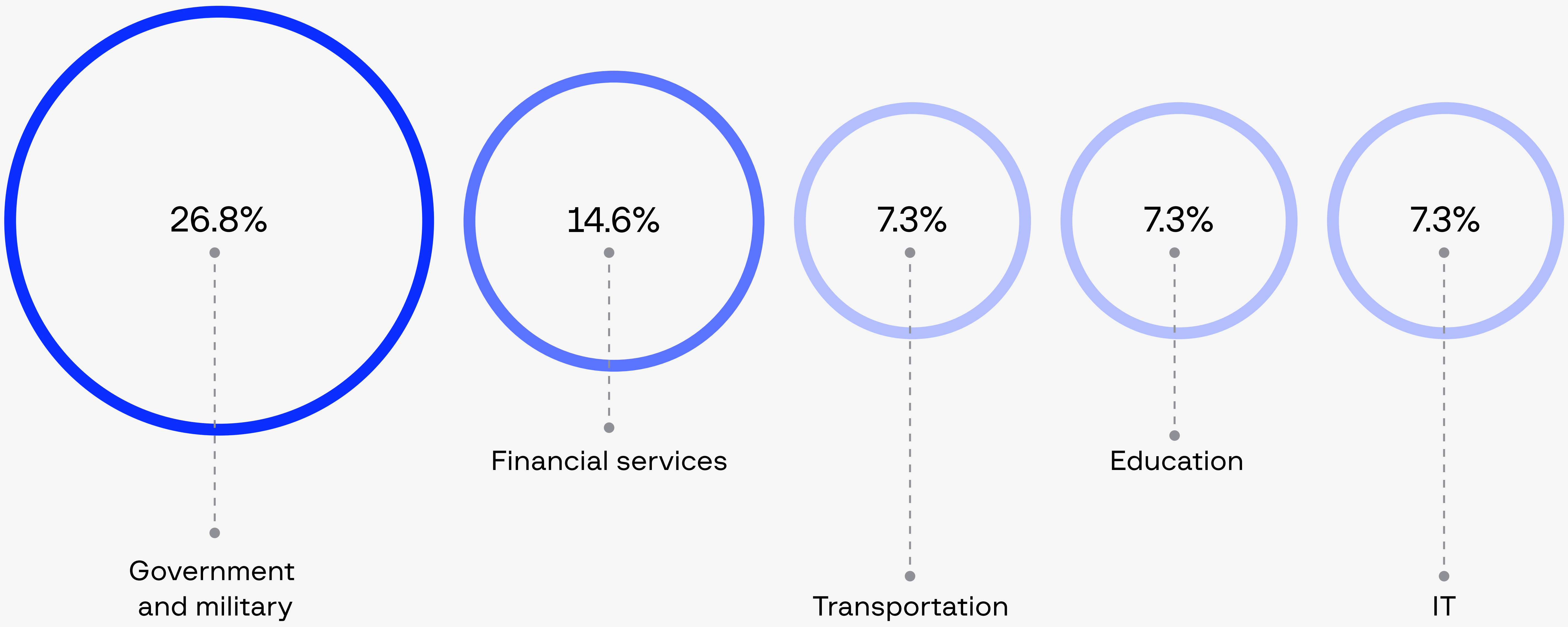
North America Top industries targeted by APTs in 2024



Latin America Top jurisdictions targeted by APTs in 2024



Latin America Top industries targeted by APTs in 2024



Most prolific APTs based on number of observed attacks

Malware
AI-Driven Threats
Ransomware
Dark Web Dangers
Scam
Fraud
Data Stealers
Phishing
Extortion

Dark Pink

Alleged attribution
Unknown

Scope
Asia-Pacific, Europe

First seen
2021

ABOUT

Dark Pink is the name given by Group-IB to a new wave of APT attacks targeting the APAC region. At this time, Group-IB cannot attribute the campaign to any known threat actor or country.

Early research into Dark Pink reveals that the attackers employ a unique set of tactics, techniques, and procedures rarely used by previously known APT groups. They utilize a custom toolkit designed to steal confidential documents from government and military networks. Notably, Dark Pink can infect USB devices connected to compromised computers and access messaging applications on infected machines.

In 2024, Group-IB observed the group updating its tools—including new custom tools, CogProBot and DPinkVenom—as well as refining its methods of Trojan communication and data exfiltration via Slack channels. These developments indicate that Dark Pink remains active and is investing significant effort into concealing its operations.

ALIASES

APT-LY-1005, Saaiwc Group

TOP TACTICS

- Phishing (T1566)
- Steal Application Access Token (T1528)
- Command and Scripting Interpreter → PowerShell (T1059.001)
- Event Triggered Execution → Windows Management Instrumentation Event Subscription (T1546.003)
- Hijack Execution Flow → DLL Side-Loading (T1574.002)
- Credentials from Password Stores → Credentials from Web Browsers (T1555.003)
- Archive Collected Data → Archive via Utility (T1560.001)
- Scheduled Task/Job → Scheduled Task (T1053.005)

INDUSTRY FOCUS

- Religion
- Non profit
- Universities
- Government and military

APT28

Alleged attribution
Russia

Scope
Worldwide

First seen
2004

ABOUT

The APT28 hacking group has a long history of hacking. Its members are Russian-speaking, and most of its attacks have targeted political and military institutions, with a smaller percentage aimed at media and sports organizations.

APT28 employs various tactics, including spearphishing emails, malware distribution via websites disguised as news sources, and exploiting zero-day vulnerabilities. In 2024, analysts observed the group adopting new techniques, such as abusing the search-ms protocol and WebDAV servers to deploy malware, as well as leveraging reCAPTCHA phishing (ClickFix) to evade detection.

ALIASES

Fancy Bear, Sednit group, Sofacy, Pawn Storm, Strontium, Tsar Team, TG-4127, TAG-0700, Swallowtail, IRON TWILIGHT, Group 74, SNAKEMACKEREL, SectorC01, ITG05, APT-C-20, SIG40, Walleye, Fighting Ursa, TA422, BlueDelta, Forest Blizzard, Blue Athena, FROZENLAKE

TOP TACTICS

- Phishing (T1556)
- Exploitation for Client Execution (T1203)
- Command and Scripting Interpreter → PowerShell (T1059.001)
- Obfuscated Files or Information (T1027)
- Indicator Removal → File Deletion (T1070.004

INDUSTRY FOCUS

- Advertising
- Content and publishing
- Education
- Data and analytics
- Energy
- Financial services
- Government and military
- Healthcare
- Manufacturing
- Information technology
- Media and entertainment
- Sports
- Natural resources
- Non profit
- Sales and marketing
- Science and engineering
- Telecommunications
- Transportation
- Travel and tourism

Cloud Atlas

Alleged attribution
Ukraine

Scope
Asia, Europe

First seen
2007

ABOUT

Cloud Atlas is a cyber-espionage group that conducts highly targeted attacks on critical infrastructure across various regions and political conflicts. Despite years of activity, its tactics, techniques, and procedures (TTPs) have remained largely unchanged, relying on phishing emails with trojanized documents for malware delivery.

Initially focused on Russia, Cloud Atlas has since expanded its operations globally. The group employs advanced identity cloaking and deploys clean, sophisticated malware, indicating strong backing. Its arsenal includes malware targeting Android, BlackBerry, and Apple iOS devices.

ALIASES

Inception, Inception Framework, Oxygen, ATK 116, RedOctober, Hive0097, Clean Ursa, Cloud Werewolf

TOP TACTICS

- Phishing → Spearphishing Attachment (T1566.001)
- User Execution → Malicious File (T1204.002)
- Boot or Logon Autostart Execution → Registry Run Keys / Startup Folder (T1547.001)
- Template Injection (T1221)
- Ingress Tool Transfer (T1105)
- System Information Discovery (T1082)

INDUSTRY FOCUS

- Aerospace
- Community and lifestyle
- Energy
- Financial services
- Government and military
- Manufacturing
- Lending and investments
- Natural resources
- Transportation

Dark Halo

Alleged attribution
Unknown

Scope
Europe, Americas

First seen
2019

ABOUT

Dark Halo has been active since late 2019, conducting cyber-espionage operations. The group has compromised organizations worldwide through a supply chain attack involving a trojanized update file for the SolarWinds Orion Platform.

In 2024, Dark Halo launched a series of highly targeted spear-phishing campaigns against individuals in government, academia, defense, non-governmental organizations, and other sectors. Notably, the group employed a signed RDP configuration file as a novel access vector to infiltrate targets' devices.

Earlier in 2024, reports linked Dark Halo to the TeamViewer attack. Findings suggest the group exploited a compromised employee account to access and copy employee directory data, including names, corporate contact details, and encrypted employee passwords from TeamViewer's internal corporate IT environment.

ALIASES

UNC2452, SolarStorm, StellarParticle, NobleBaron, IRON RITUAL, UNC3004, UNC2652, Solar Phoenix , DarkHalo, Nobellium, TA421, BlueBravo, Midnight Blizzard, Blue Dev 5

TOP TACTICS

- Process Discovery (T1057)
- Account Manipulation (T1098)
- Hijack Execution Flow → DLL Side-Loading (T1574.002)
- Command and Scripting Interpreter → Windows Command Shell (T1059.003)
- Hijack Execution Flow → DLL Side-Loading (T1574.002)
- Exfiltration Over Web Service: Exfiltration to Cloud Storage (T1567.002)
- Exploit Public-Facing Application (T1190)

INDUSTRY FOCUS

- Agriculture and farming
- Biotechnology
- Education
- Commerce and shopping
- Energy
- Transportation
- Consumer electronics
- Financial services
- Gaming
- Food and beverage
- Government and military
- Healthcare
- Information technology
- Internet services
- Manufacturing
- Media and entertainment
- Telecommunications
- Real estate
- Travel and tourism
- Sales and marketing
- Software

APT10

Alleged attribution
China

Scope
Worldwide

First seen
2006

ABOUT

APT10 operates as part of a broader cyber-espionage initiative. Rather than acting independently, APT10 plays a key role in Operation Cloud Hopper, a campaign that infiltrates Managed Service Providers (MSPs) to gain access to their clients' networks.

Known for intellectual property theft, the group primarily targets sensitive business and technological data. APT10 also gained significant attention for Operation Soft Cell, a prolonged attack on global telecommunications providers.

In 2024, APT10 evolved its tactics, techniques, and procedures (TTPs), deploying various backdoor malware—LODEINFO, NOOPDOOR, and Cobalt Strike—to expand its operations into Japan, Taiwan, India, and Africa.

ALIASES

MenuPass, DustStorm, Red Apollo, CVNX, HOGFISH, Stone Panda, POTASSIUM, Cloud Hopper, BRONZE RIVERSIDE, CTG-5938, ITG01, Cicada, TA429, GALLIUM, Soft Cell, Alloy Taurus, Granite Taurus, Red Moros, MirrorFace, Earth Kasha

TOP TACTICS

- Phishing → Spearphishing Attachment (T1566.001)
- Windows Management Instrumentation (T1047)
- Hijack Execution Flow → DLL Side-Loading (T1574.002)
- Indicator Removal → File Deletion (T1070.004)
- OS Credential Dumping (T1003)
- Ingress Tool Transfer (T1105)
- File and Directory Discovery (T1083)

INDUSTRY FOCUS

- Aerospace
- Commerce and shopping
- Education
- Data and analytics
- Consumer electronics
- Electronics
- Energy
- Financial services
- Government and military
- Healthcare
- Information technology
- Manufacturing
- Media and entertainment
- Natural resources
- Non profit
- Professional services
- Real estate
- Religion
- Telecommunications
- Transportation
- Travel and tourism

Lazarus

Alleged attribution
North Korea

Scope
Worldwide

First seen
2007

ABOUT

The Lazarus Group, first identified in cyberattacks against the South Korean government, is a notorious hacking organization linked to major global incidents. These include the 2014 attack on Sony Pictures Entertainment, the $81 million heist from Bangladesh Bank in 2016, and the compromise of multiple Polish banks in 2017.

With the onset of the COVID-19 pandemic, Lazarus shifted its focus to pharmaceutical companies. Using spear-phishing techniques, members impersonated health officials, sending employees malicious links to infiltrate their systems.

In recent years, Lazarus has intensified its attacks on cryptocurrency services, amassing approximately $1.3 billion in stolen funds from crypto-related hacks in 2024.

ALIASES

Dark Seoul Gang, HIDDEN COBRA, Guardians of Peace, APT38, APT-C-26, Labyrinth Chollima, Zinc, Bluenoroff, Stardust Chollima, BeagleBoyz, Labyrinth Chollima , TA444, UNC2970, Temp.Hermit, UNC577, Diamond Sleet, Sapphire Sleet, CL-STA-0240, CL-STA-0241, Citrine Sleet

TOP TACTICS

- Phishing (T1566)
- Command and Scripting Interpreter (T1059)
- User System Information Discovery (T1082)
- User Execution (T1204)
- Process Injection (T1055)
- Obfuscated Files or Information (T1027)
- Application Layer Protocol (T1071)

INDUSTRY FOCUS

- Aerospace
- Commerce and shopping
- Education
- Energy
- Financial services
- Gaming
- IT
- Government and military
- Manufacturing
- Real estate
- Media and entertainment
- Telecommunications
- Transportation
- Travel and tourism

Gamaredon

Alleged attribution
Russia

Scope
Europe, Asia

First seen
2013

ABOUT

While Ukrainian governmental institutions remain Gamaredon's primary focus, researchers have observed that since the 2022 conflict, the group has also attempted attacks on Ukraine's NATO allies, including Bulgaria, Latvia, Lithuania, and Poland.

Gamaredon primarily relies on spear-phishing campaigns, delivering weaponized Word documents and infected USB drives designed to spread within targeted organizations. To maintain persistence, the group deploys multiple lightweight downloaders and backdoors simultaneously.

Although its tools are technically unsophisticated, Gamaredon frequently updates and modifies them to evade detection. In 2024, alongside existing malware such as GammaLoad, Pteranodon, and GammaSteel, the group introduced Android spyware tools BoneSpy and PlainGnome, further expanding its capabilities.

ALIASES

Primitive Bear, SectorC08, Armageddon, Shuckworm, BlueOtso, ACTINIUM, DEV-0157, Winterflouder, APT-C-53, Trident Ursa, UAC-0010, Aqua Blizzard

TOP TACTICS

- Input Capture (T1056)
- Application Layer Protocol (T1071)
- Command and Scripting Interpreter → Visual Basic (T1059.005)
- Boot or Logon Autostart Execution → Registry Run Keys / Startup Folder (T1547.001)
- Input Capture (T1056)
- Scheduled Task/Job (T1053)
- Obfuscated Files or Information → Software Packing (T1027.002)
- Phishing → Spearphishing Attachment (T1566.001)

INDUSTRY FOCUS

- Healthcare
- Energy
- Financial services
- Government and military
- Non profit
- Universities
- Travel and tourism
- Telecommunications

APT37

Alleged attribution
North Korea

Scope
Europe, Asia-Pacific

First seen
2012

ABOUT

APT37 primarily targets both public and private sectors in South Korea, focusing on intelligence gathering to support North Korea's military, political, and economic strategies. The group relies on spear phishing, strategic web compromises, and torrent file sharing as initial infection methods. It is also highly adept at rapidly incorporating newly discovered vulnerabilities into its arsenal.

For command-and-control (C2) operations, APT37 utilizes a mix of compromised servers, messaging platforms, cloud services, and social networks to distribute malware and evade detection. In 2024, the group exploited the Zero-Day vulnerability (CVE-2024-38178) in an in-the-wild attack against specific organizations in South Korea.

ALIASES

ScarCruft, Reaper, Group123, TEMP.Reaper, Geumseong121, Hermit, Venus 121, Red Eyes, Thallium, Ricochet Chollima, ATK 4, InkySquid, Moldy Pisces, Earth Kitsune, APT-C-28, OSMIUM, Opal Sleet

TOP TACTICS

- Exploit Public-Facing Application (T1190)
- Phishing → Spearphishing Attachment (T1566.001)
- Command and Scripting Interpreter → Windows Command Shell (T1059.003)
- Process Injection (T1055)
- Application Layer Protocol (T1071)
- System Binary Proxy Execution (T1218)
- Obfuscated Files or Information (T1027)

INDUSTRY FOCUS

- Content and publishing
- Financial services
- Government and military
- Media and entertainment
- Science and engineering

Ocean Lotus

Alleged attribution
Vietnam

Scope
Asia-Pacific

First seen
2009

ABOUT

OceanLotus has primarily targeted Vietnamese bloggers and conducted focused attacks in Vietnam and adjacent countries that reflect Vietnam's interests. Researchers have noted the group's long-term operational cycles, with active phases following extensive preparation.

Specializing in cyber espionage, intelligence gathering, and intellectual property theft, OceanLotus employs phishing emails sent from addresses resembling potential victims, as well as watering hole attacks, which compromise legitimate websites to infect visitors.

In 2024, analysts observed a shift in focus toward China and Hong Kong. The group frequently disguised its malware as Chinese software, which, when launched, executed multiple shellcodes, ultimately delivering KSRAT or Cobalt Strike as the final payload.

ALIASES

Cobalt Kitty, SeaLotus, APT-C-00, APT32, SectorF01

TOP TACTICS

Phishing (T1566) | Modify Registry (T1112) | Phishing → Spearphishing Attachment (T1566.001) | System Information Discovery (T1082) | Application Layer Protocol (T1071)

INDUSTRY FOCUS

Agriculture and farming | Content and publishing | Energy | Education | Financial services | Government and military | IT | Manufacturing | Real estate | Mining | Travel and tourism | Telecommunications | Transportation

Oilrig

Alleged attribution
Iran

Scope
Scope: Worldwide

First seen
2014

ABOUT

OilRig conducts cyber-espionage campaigns primarily targeting organizations in the Middle East and the United States.

Their attacks often begin with spear-phishing emails, which are typically disguised as job applications or business-related documents, and they frequently exploit vulnerabilities to gain initial access. Over time, OilRig's operations have evolved, showing increasing sophistication and adaptability.

The group has adopted DNS-based exfiltration techniques to avoid detection, leveraged legitimate system tools to blend in with normal activity (a technique known as living-off-the-land), and developed modular, custom-built malware frameworks that are easily adaptable for various operations.

OilRig's activities have caused significant disruptions, including the theft of sensitive data, operational downtime, and financial losses. Their evolving tactics, modular malware, and strategic targeting make them a persistent threat, emphasizing the importance of robust cybersecurity defenses and proactive threat intelligence efforts.

ALIASES

Twisted Kitten, Crumbus, APT34, Cobalt Gypsy, Helix Kitten, Chrysene, TA452, GreenBug, nobody.gu3st, Evasive Serpens , IRN2, Hazel Sandstorm, EUROPIUM, Crambus, ITG13, Yellow Maero, ATK40, DEV-0861, G0049, Scarred Manticore, Storm-0861

TOP TACTICS

Exploit Public-Facing Application (T1190) | Command and Scripting Interpreter (T1059) | Scheduled Task/Job (T1053) | Phishing (T1566) | System Information Discovery (T1082) | Application Layer Protocol (T1071) | Ingress Tool Transfer (T1105)

INDUSTRY FOCUS

Aerospace | Education | Energy | Mining | Financial services | Government and military | IT | Telecommunications | Transportation | Healthcare

Muddy Water

Alleged attribution
Iran

Scope
Scope: Worldwide

First seen
2017

ABOUT

MuddyWater, also known by aliases TA450 and Seedworm, is a sophisticated threat actor group that has been operating since at least 2017. The group's primary motivation is espionage and intelligence gathering.

MuddyWater targets a variety of industries, including government, telecommunications, energy, and critical infrastructure, with a particular focus on the Middle East, South Asia, and NATO-affiliated countries.

ALIASES

TEMP.Zagros, Seedworm, Static Kitten, SectorD02, TA450, Boggy Serpens, MERCURY, Mango Sandstorm, Earth Vetala, Mercury, Cobalt Ulster, ATK51, T-APT-14, Yellow Nix

TOP TACTICS

- Command and Scripting Interpreter (T1059)
- Command and Scripting Interpreter → PowerShell (T1059.001)
- Scheduled Task/Job (T1053)
- Phishing (T1566)
- Phishing → Spearphishing Attachment (T1566.001)
- Boot or Logon Autostart Execution (T1547)

INDUSTRY FOCUS

- Financial services
- Education
- Financial services
- Transportation
- Government and military
- IT
- Healthcare

Sticky Werewolf

Alleged attribution
Ukraine

Scope
Europe

First seen
2023

ABOUT

Sticky Werewolf is a newly emerged cybercriminal group that primarily utilizes widely available commercial tools, which are relatively easy to detect and block. Despite this, the group has achieved notable success, having been active since at least April 2023 and conducting over 30 attacks to date.

Initial reports suggest that Sticky Werewolf is targeting public organizations, research centers, pharmaceutical companies, and the aerospace and defense sectors in Russia and Belarus. Their infection methods involve a complex chain of files and scripts, ultimately leading to the deployment of commonly used remote access malware.

ALIASES

Unknown

TOP TACTICS

- User Execution (T1204)
- User Execution → Malicious File (T1204.002)
- User Execution → Malicious Link (T1204.001)
- Stage Capabilities → Upload Malware (T1608.001)
- Obtain Capabilities → Malware (T1588.001)

INDUSTRY FOCUS

- Aerospace
- Biotechnology
- Energy
- Government and military
- Financial services
- Hardware
- Healthcare
- Manufacturing
- Religion

APT33

Alleged attribution
Iran

Scope
Middle East, Americas, Europe

First seen
2011

ABOUT

APT33 is an Iranian state-sponsored cyber threat actor linked to the Islamic Revolutionary Guard Corps (IRGC) and the Nasr Institute; a key entity associated with Iran's cyber warfare efforts. Active since at least 2011, the group has transitioned from using custom-built malware to a more adaptable approach, incorporating publicly available remote access tools (RATs) alongside highly specialized custom backdoors. Its activities are aligned with Iranian state interests in espionage, cyber sabotage, and strategic intelligence gathering. APT33 is especially interested in sectors where sensitive technologies and critical infrastructures are involved. APT33 is known for its destructive operations like Shamoon in Saudi Arabia. They are also known to perform password spray attacks to gain access to targets of interest. Their most recent malware arsenal consists of Tickler, TURNEDUP, and FalseFont. Public tools such as NanoCore RAT, PupyRAT, PoshC2, and others have been observed in the group's operations.

ALIASES

Shamoon, VOLATILE KITTEN, Magic Hound, Timberworm, MAGNALLIUM, Elfin, HOLMIUM, NewsBeef, TA451, Peach Sandstorm, Refined Kitten

TOP TACTICS

- Boot or Logon Autostart Execution (T1547)
- Command and Scripting Interpreter (T1059)
- Password Spraying (T1110.003)
- Phishing (T1566)
- Credential API Hooking (T1056.004)
- Obfuscated Files or Information (T1027)

INDUSTRY FOCUS

- Aerospace
- Defense
- Government
- Energy and Petrochemicals
- Critical Infrastructure
- Education
- High-tech industries

Core Werewolf

Alleged attribution
Unknown

Scope
Asia, Europe

First seen
2021

ABOUT

Core Werewolf is a cyberespionage group that actively targets Russian organizations linked to the military-industrial complex and critical information infrastructure. The group was first identified in August 2021. In March 2024, Core Werewolf attacked a Russian research institute involved in weapons development, and in early April, it targeted a Russian defense plant. The group uses UltraVNC software in its campaigns to facilitate its attacks.

ALIASES

PseudoGamaredon, Awaken Likho

TOP TACTICS

- Phishing (T1566)
- Access Token Manipulation (T1134)
- Scheduled Task/Job → Scheduled Task (T1053.005)
- User Execution → Malicious File (T1204.002)
- Virtualization/Sandbox Evasion → Time Based Evasion (T1497.003)
- Remote Services → VNC (T1021.005)
- Remote Access Software (T1219)

INDUSTRY FOCUS

- Government and military
- Manufacturing

Rocket Kitten

Alleged attribution
Iran

Scope
Middle East, America, Europe

First seen
2010

ABOUT

Rocket Kitten is a state-sponsored threat actor attributed to Iran. Initially identified by FireEye as the Ajax Security Team, the group appears to have formed as early as 2010 through the activities of hacker personas such as “Cair3x” and “HUrr!c4nE!”. By 2012, it shifted focus to targeting Iran's political opponents, and by 2013–2014, it began executing malware-based cyberespionage campaigns under the moniker Rocket Kitten.

Over time, overlapping infrastructure, tools, objectives, and personnel have led researchers, including those at Group-IB, to conclude that Rocket Kitten and Charming Kitten are essentially the same group—albeit with some evolution in their lineup and capabilities. Recent research has identified emerging malware variants and enhanced operational tactics, suggesting that Rocket Kitten is continually refining its arsenal.

The group is primarily motivated by intelligence gathering, with operations focused on surveillance and espionage. Rocket Kitten employs a variety of custom-built malware and public command-and-control (C2) frameworks. Notably, they have used the Mythic C2 framework, and their custom-built malware includes the MediaPl backdoor, BellaCiao, BellaCPP, and Cyclops. Their shift from .NET (BellaCiao) to C++ (BellaCPP) and Golang (Cyclops), along with the incorporation of advanced defense evasion techniques, reflects their technical maturation over time.

ALIASES

APT35, Ajax Security Team, Charming Kitten, Flying Kitten, PHOSPHOROUS, Educated Manticore, Mint Sandstorm, Group 26, Parastoo, iKittens, Group 83, Newscaster

TOP TACTICS

- Registry Run Keys / Startup Folder (T1547.001)
- Exploit Public-Facing Application (T1190)
- Phishing (T1566)
- Input Capture (T1056)
- Application Layer Protocol (T1071)

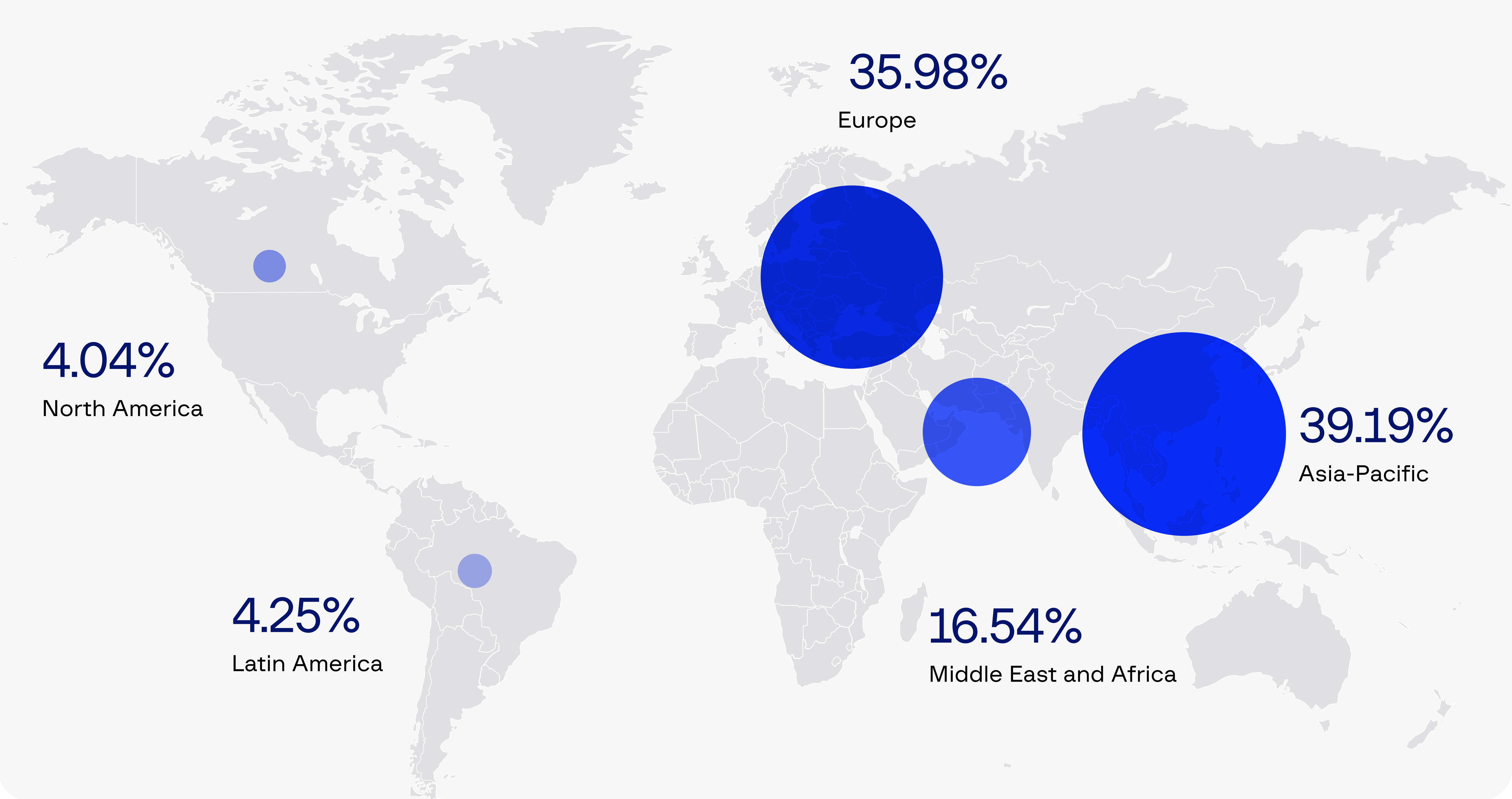
INDUSTRY FOCUS

- Government agencies
- Energy
- Defense sectors
- Think tanks and academic institutions
- Media organizations
- Human rights groups
- Telecommunications

Hacktivism

Hacktivism (a combination of the terms “hacking” and “activism”) is a hacker activity performed with political or social purposes, such as drawing attention to conflict or promoting specific ideas. The primary goal of hacktivism is to inflict reputational damage on opponents or disable their resources. Common attack methods include DDoS attacks to render resources inaccessible, defacing websites to promote the group’s ideas or positions, and publishing compromised data to cause reputational harm. Unlike financially motivated or pro-state threat actors, hacktivists work publicly. They are active on social networks and some groups have their own websites. These resources contain information about the group’s principles and goals, reports about attacks that have taken place, tools for carrying out attacks, and more. Hacktivists also use social networks to coordinate their campaigns.

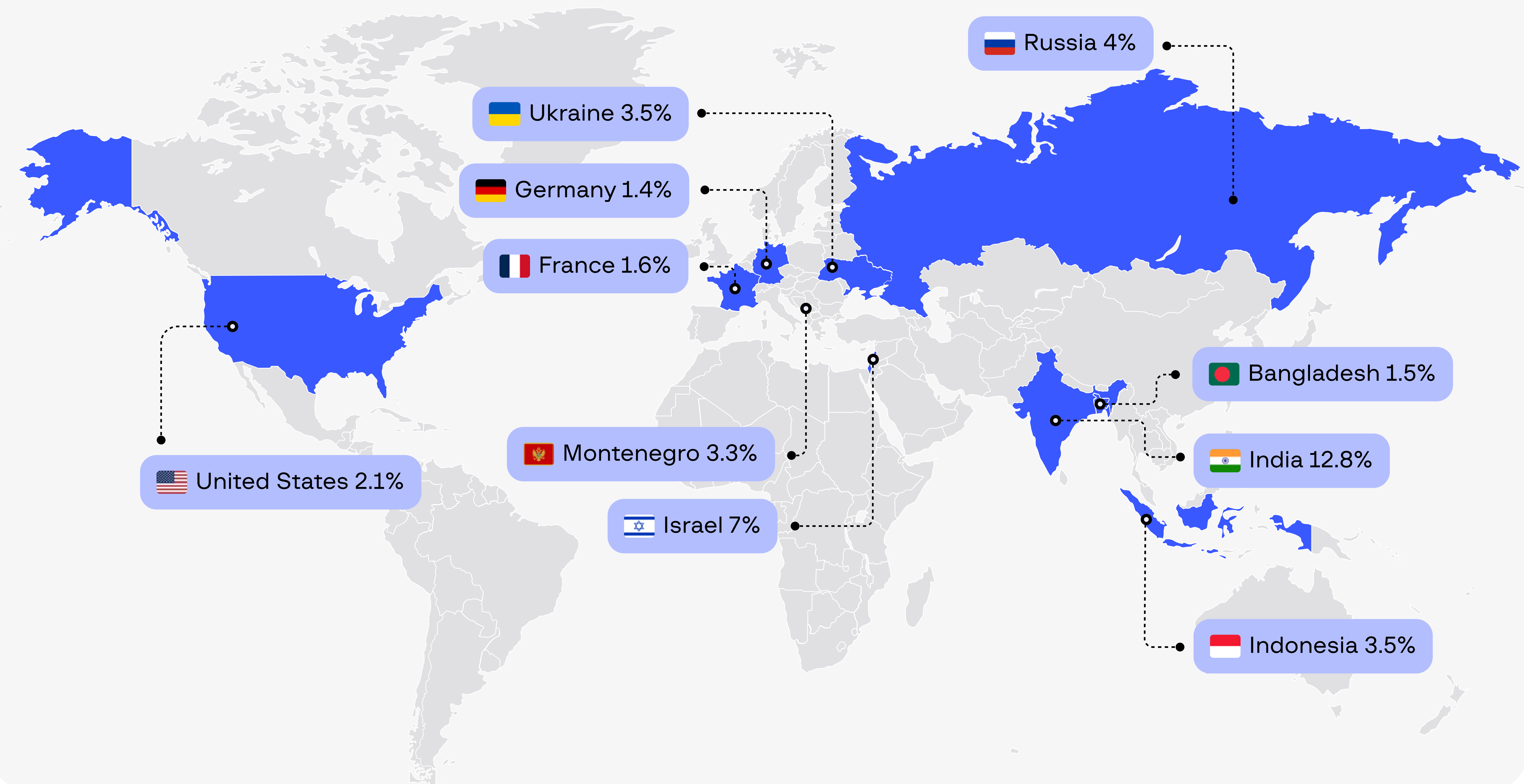
Global Distribution of hacktivist attacks by region in 2024



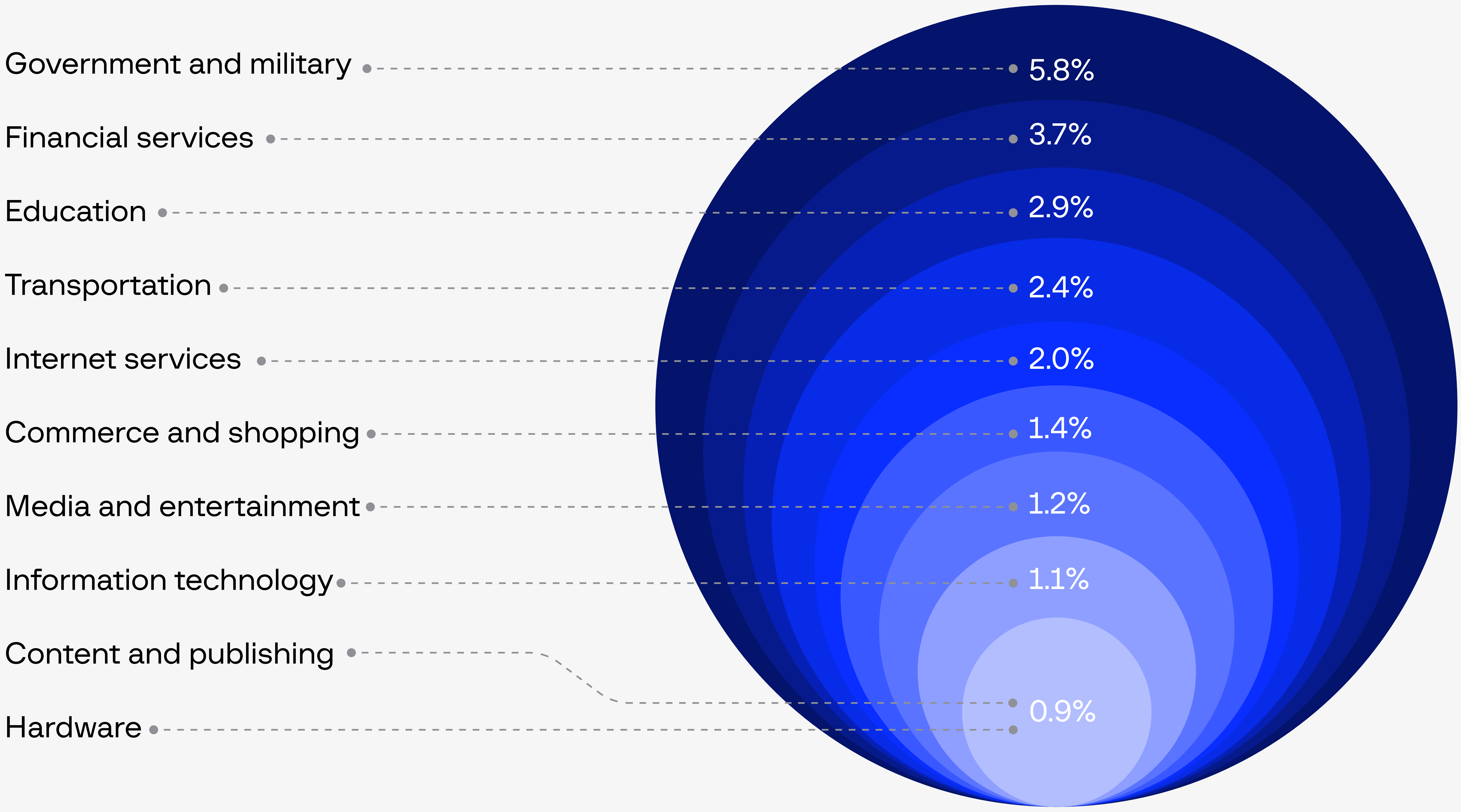
Most hacktivist groups operate with a political agenda, particularly in the context of ongoing conflicts such as those between Israel and Palestine and Russia and Ukraine. These groups often target not only the countries directly involved in the conflicts but also nations that are perceived as supportive of them.

Notably, India has emerged as a leading target for hacktivist attacks. This trend can be attributed to several factors, including regional tensions between India and its neighboring countries. Additionally, India has frequently been targeted by pro-Palestinian hacktivist groups due to its diplomatic stance and increasingly close relationship with Israel. The presence of various Indian hacktivist groups that actively attack organizations supporting Palestine further exacerbates the situation, making India a prime target for retaliatory cyberattacks.

Global Top jurisdictions targeted by hacktivists in 2024



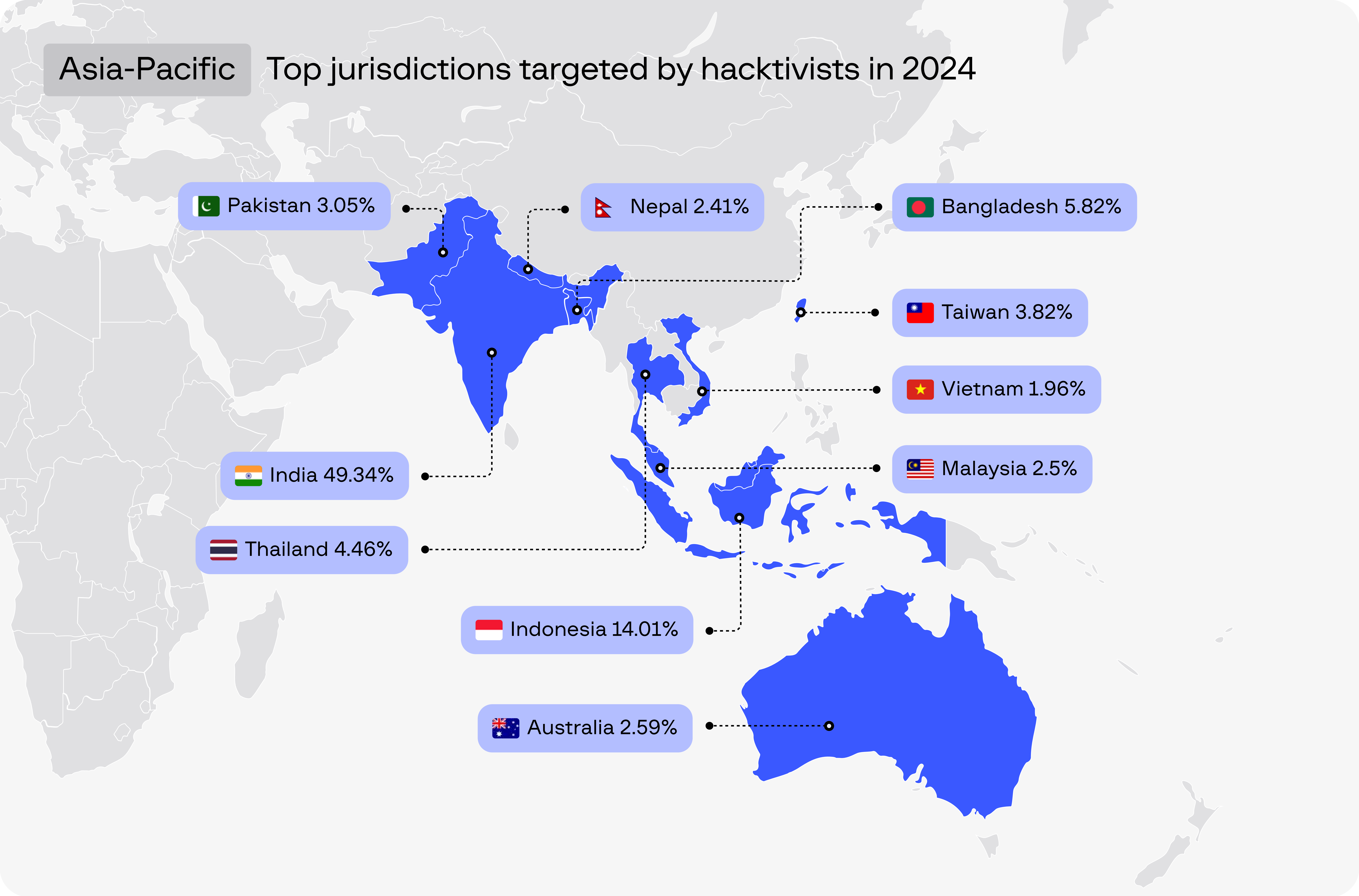
Global Top 10 industries targeted by hacktivists in 2024



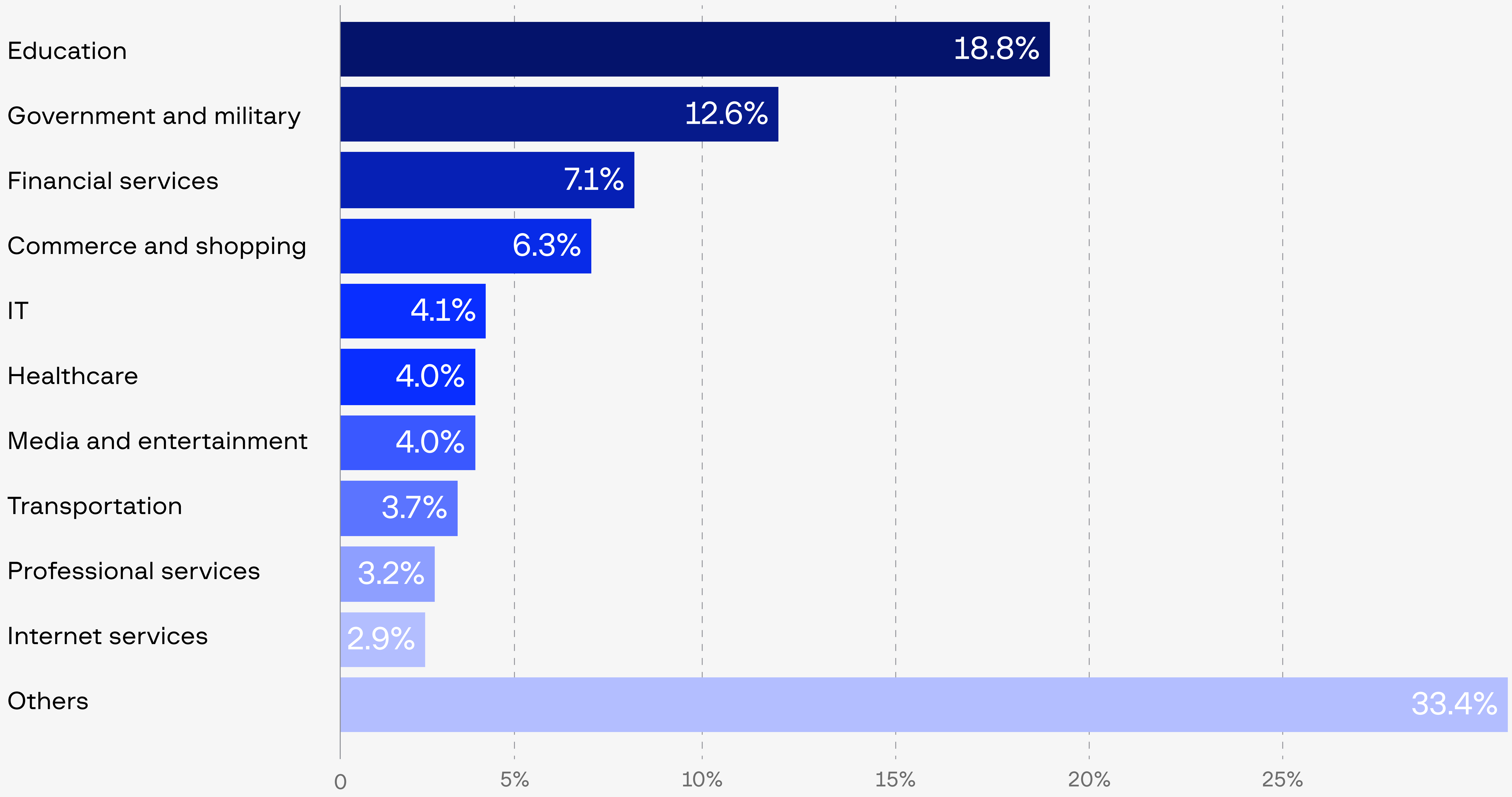
Hacktivists typically operate with a political agenda, which often leads them to target government entities and financial services as their primary focus. These sectors are seen as symbols of authority and economic power, making them attractive targets for hacktivist groups seeking to make a statement or provoke change.

However, their activities are not limited to these industries alone. Hacktivists may also direct their attacks toward well-known or particularly vulnerable companies across various sectors. The primary objective of these attacks is to inflict damage, disrupt operations, or draw public attention to specific issues, rather than to achieve a particular outcome related to the industry itself.

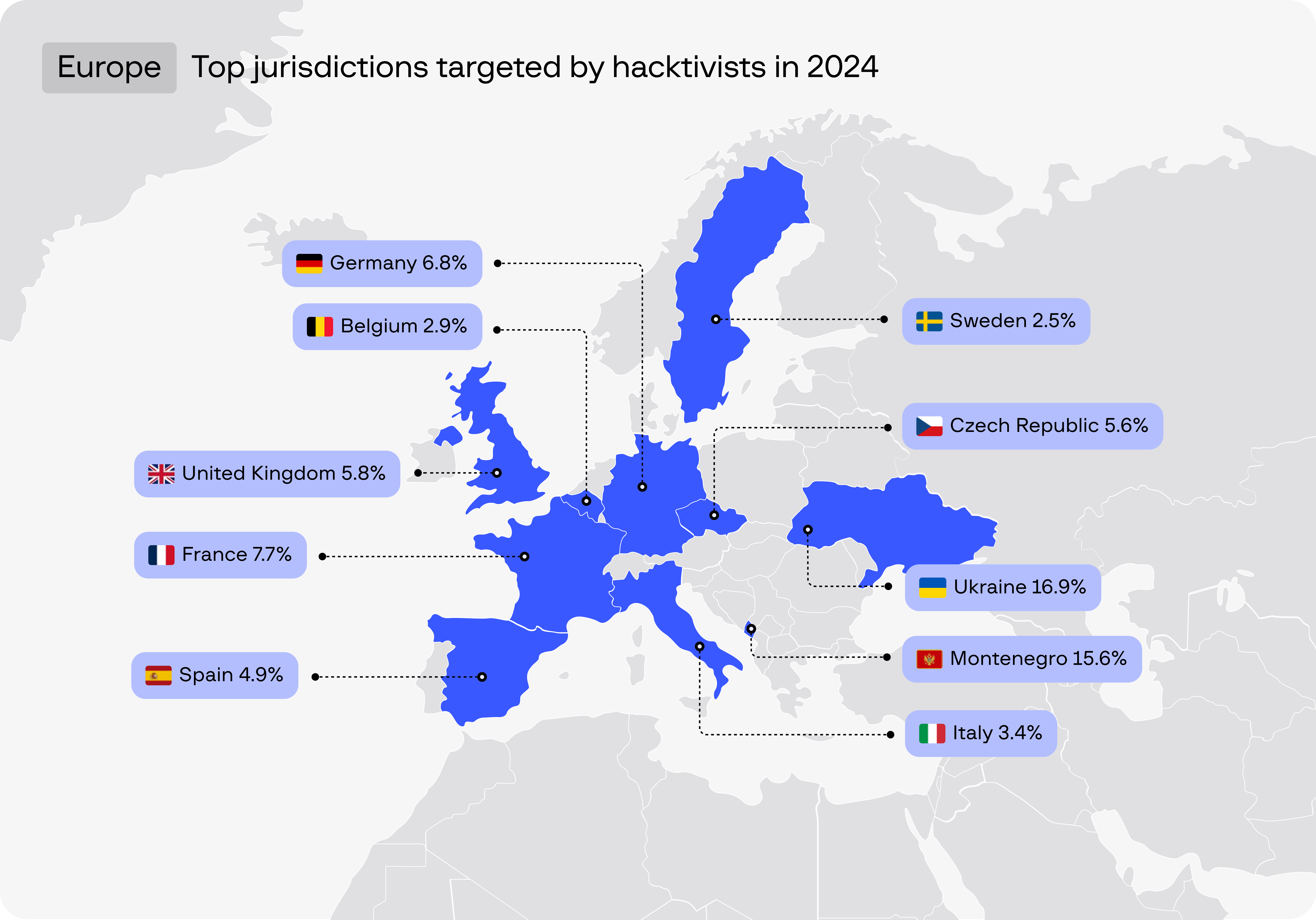
Asia-Pacific Top jurisdictions targeted by hacktivists in 2024



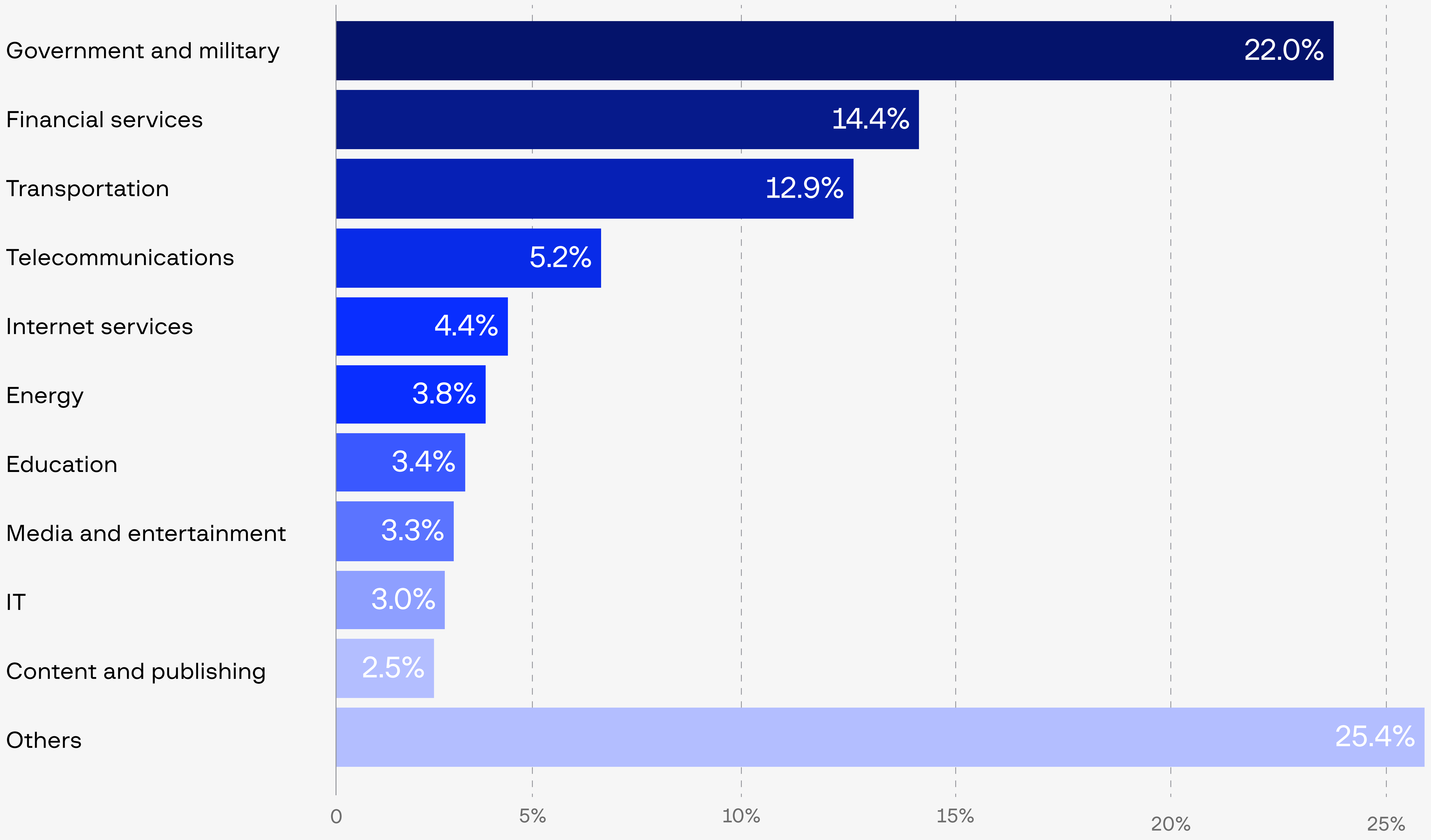
Asia-Pacific Top industries targeted by hacktivists in 2024



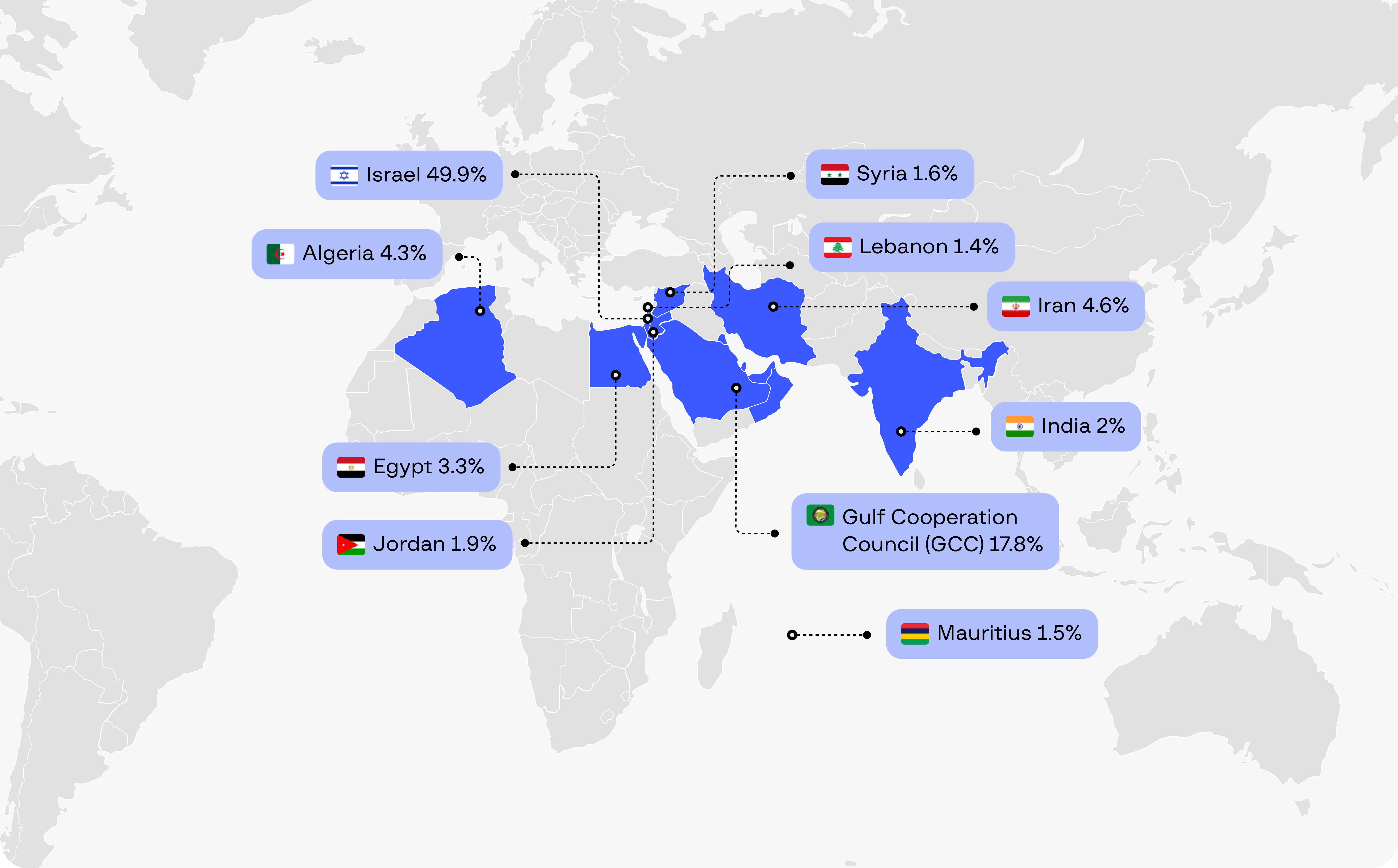
Europe Top jurisdictions targeted by hacktivists in 2024



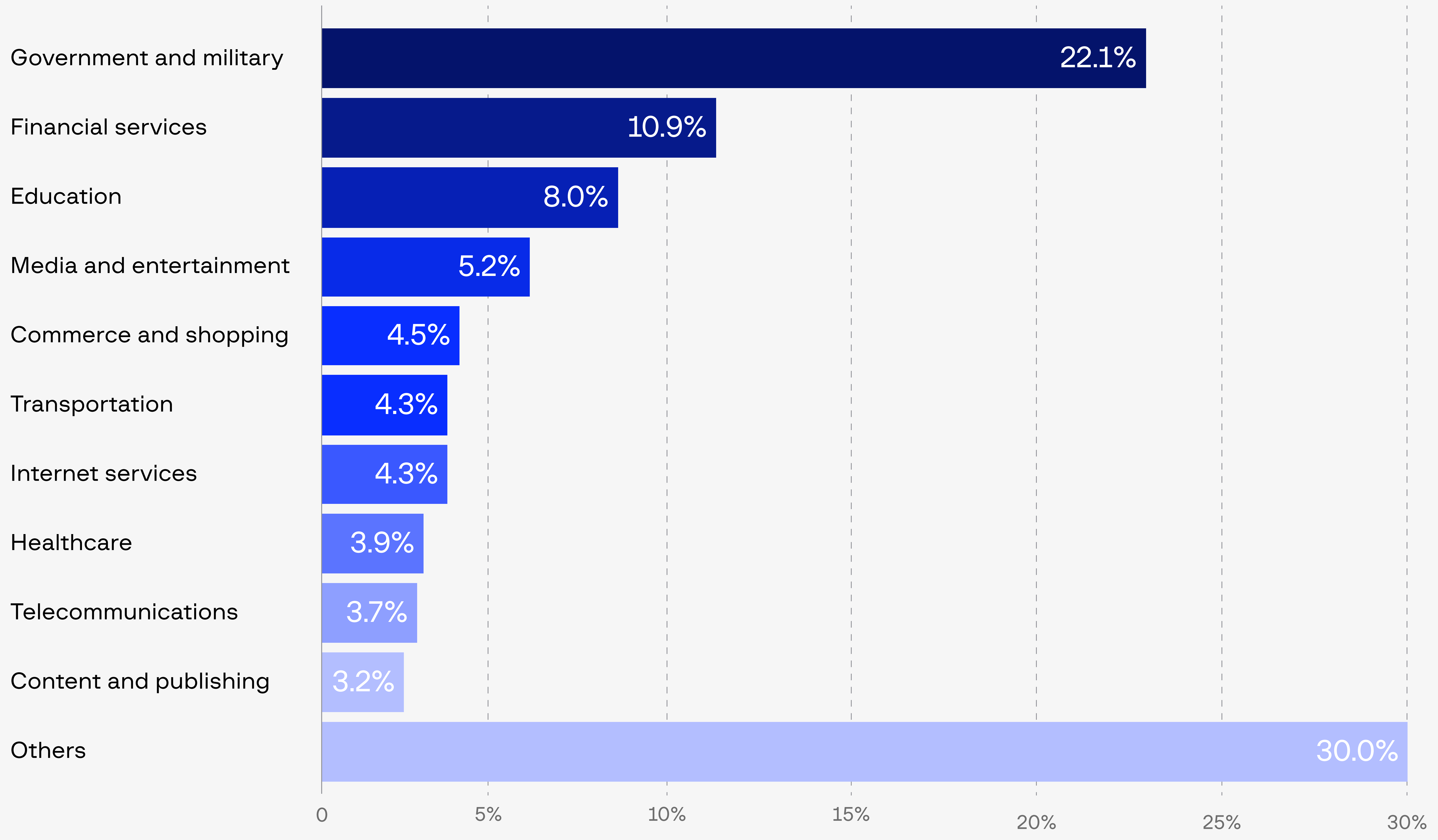
Europe Top industries targeted by hacktivists in 2024



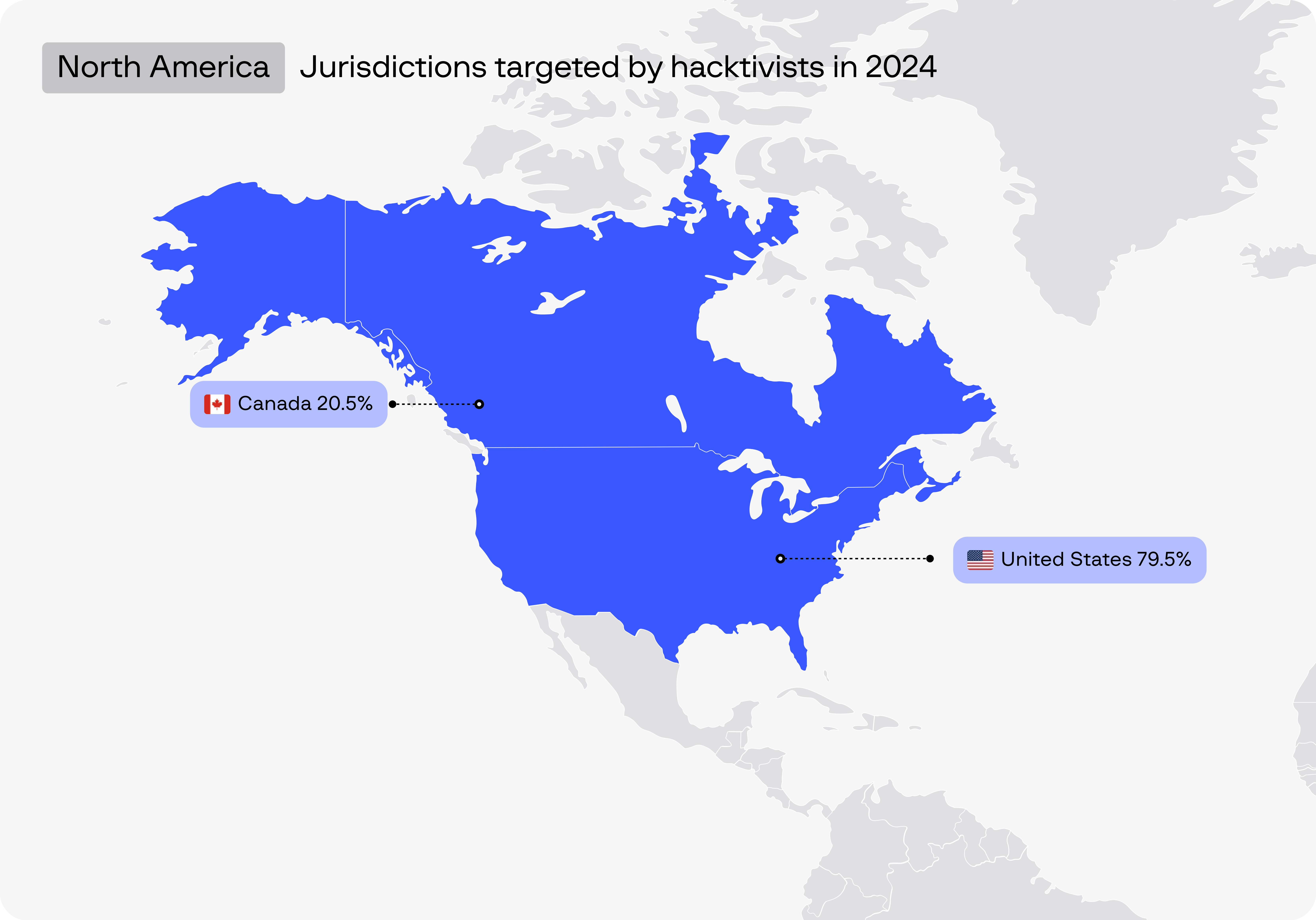
Middle East and Africa Top jurisdictions targeted by hacktivists in 2024



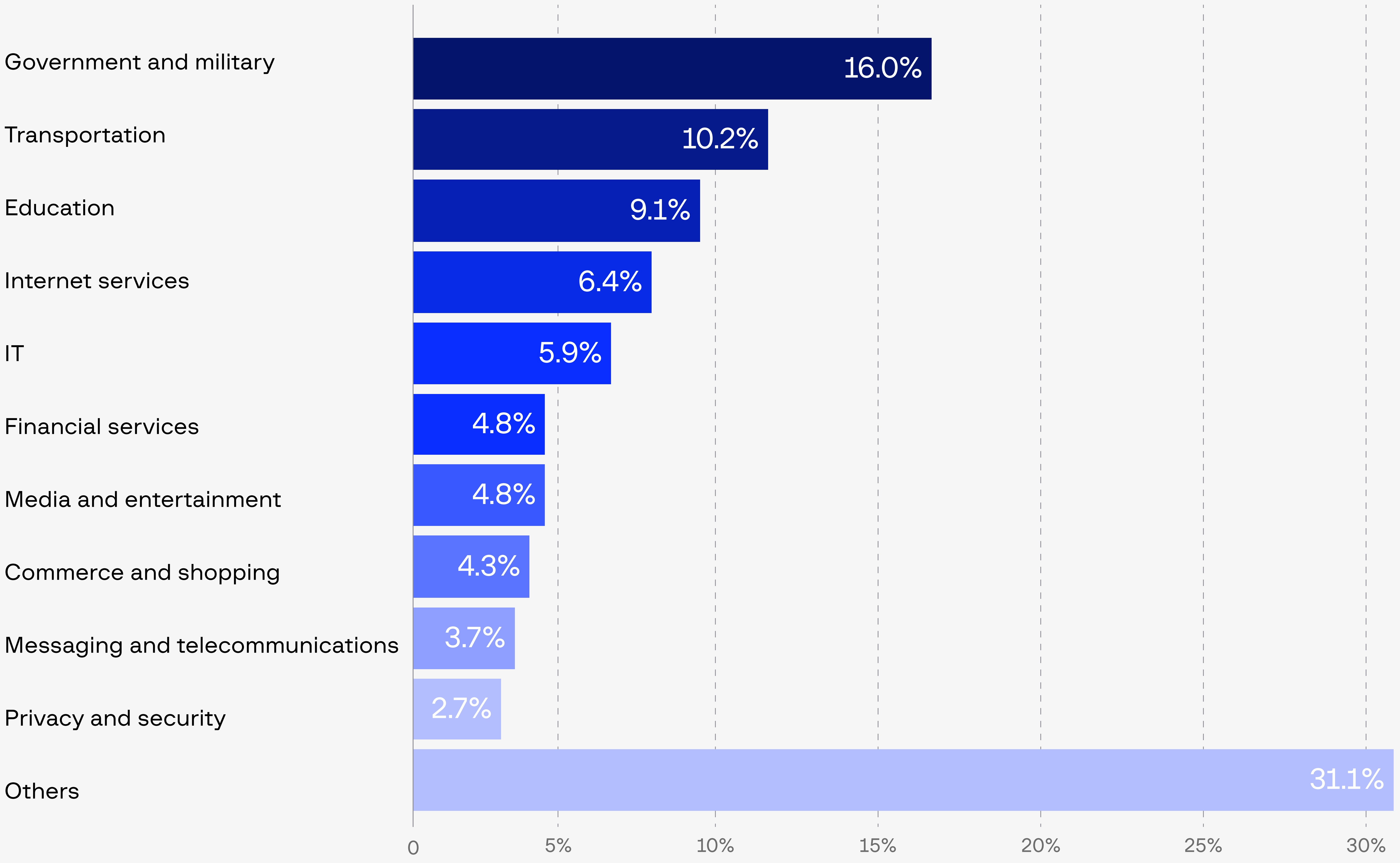
Middle East and Africa Top industries targeted by hacktivists in 2024



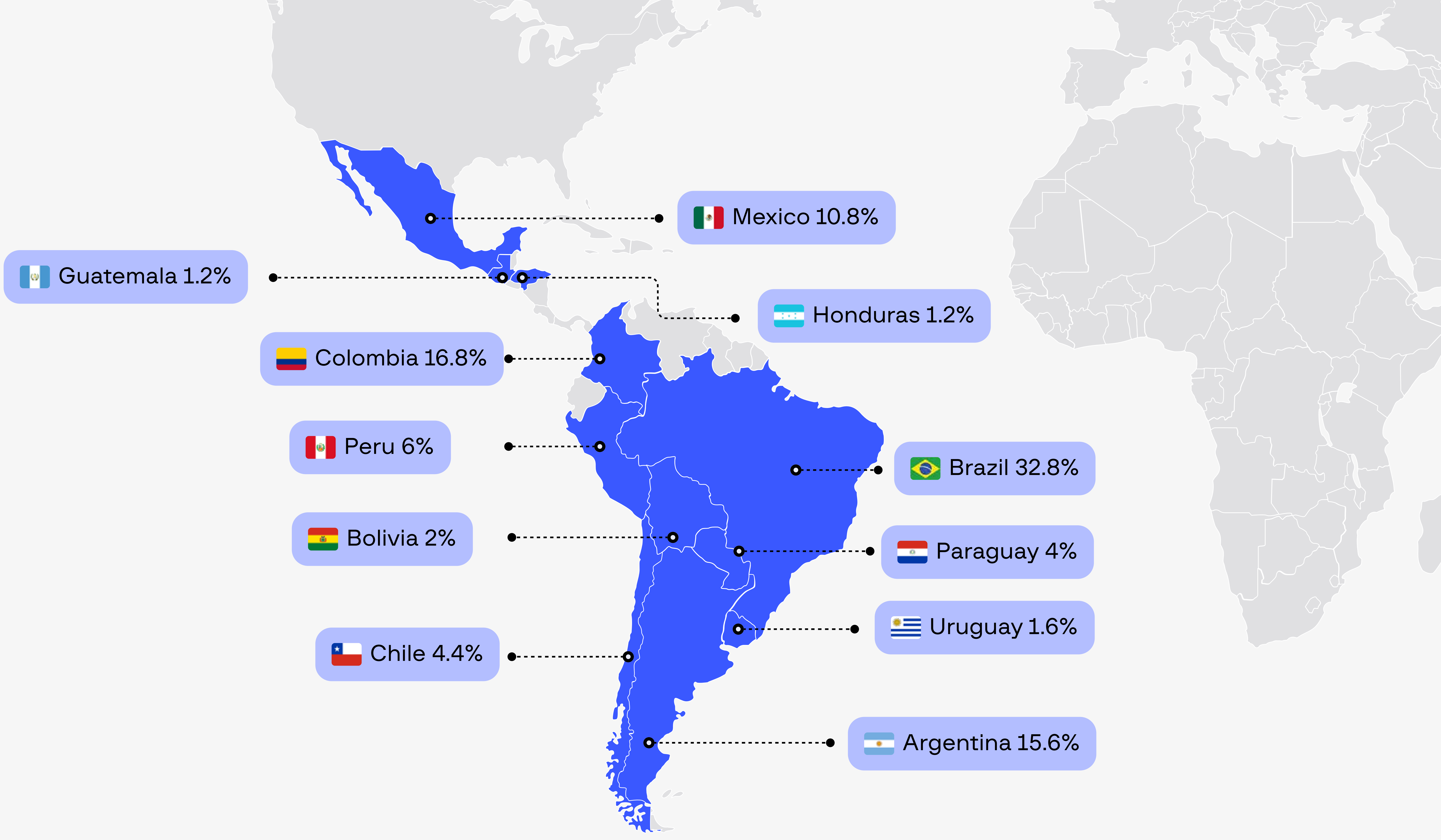
North America Jurisdictions targeted by hacktivists in 2024



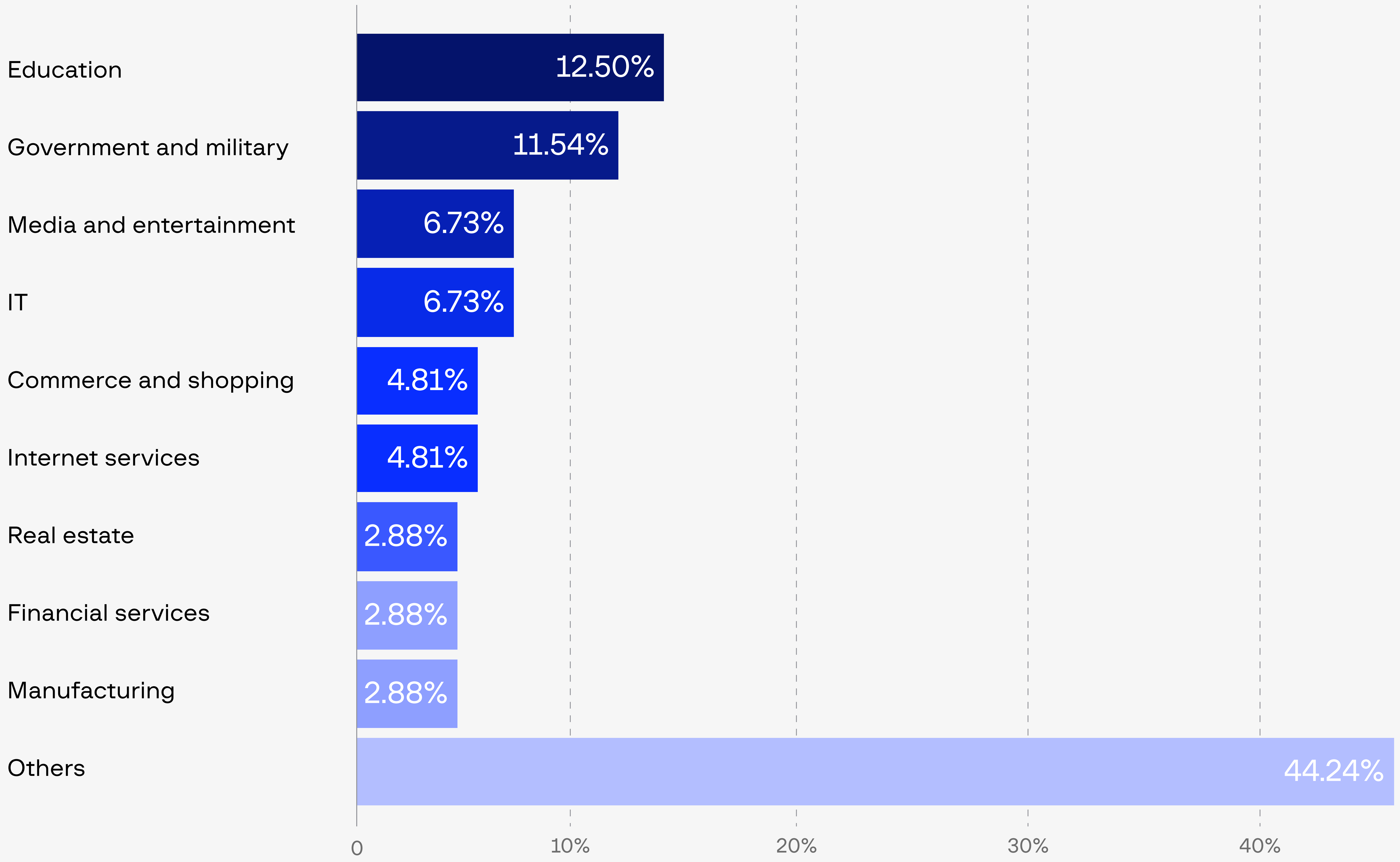
North America Top industries targeted by hacktivists in 2024



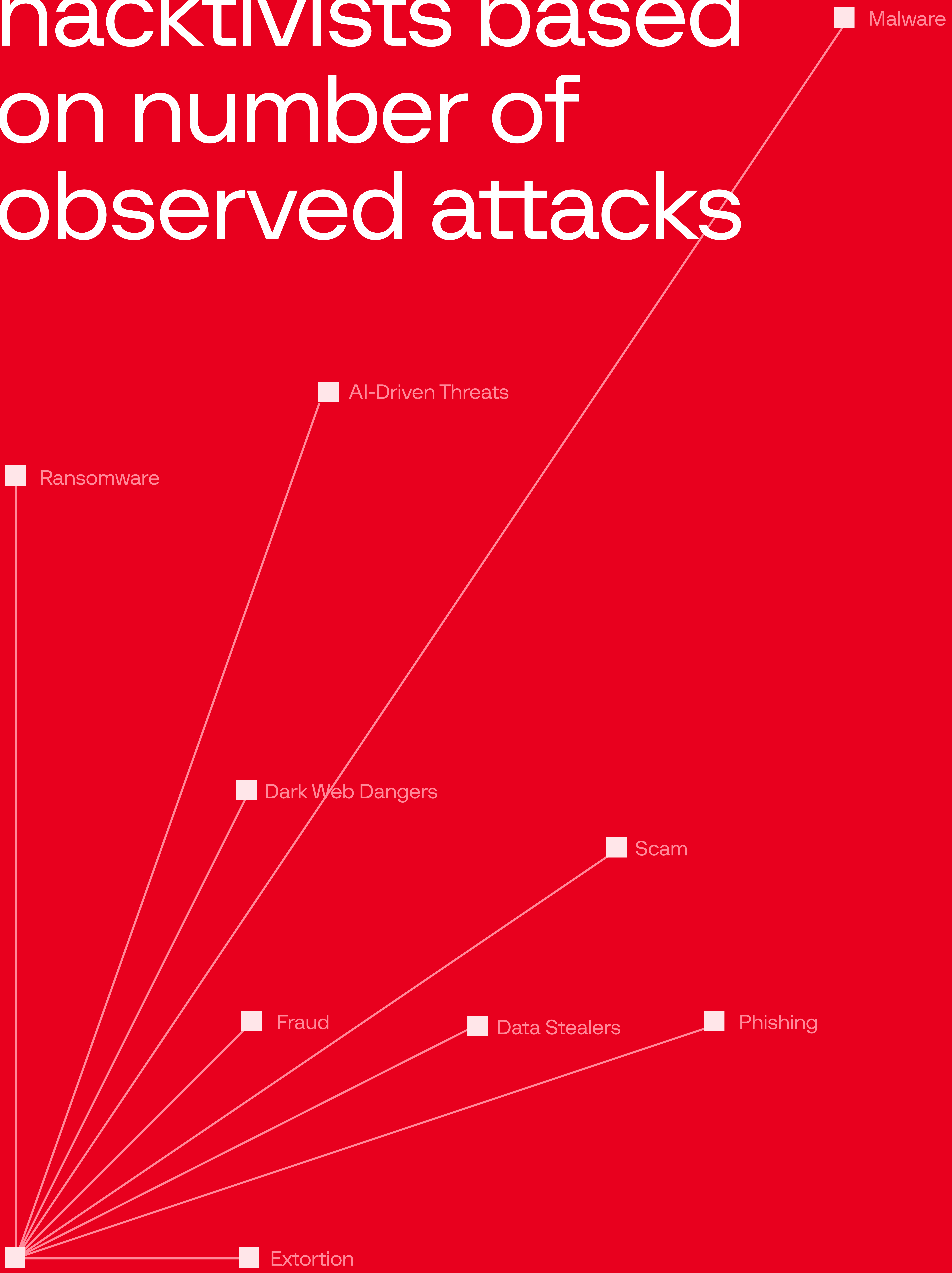
Latin America Top jurisdictions targeted by hacktivists in 2024



Latin America Top industries targeted by hacktivists in 2024



Most prolific hacktivists based on number of observed attacks



NoName 057(16)

Alleged attribution
Russia

Scope
Europe

First seen
2022

ABOUT

NONAME057(16) is a hacktivist group primarily recognized for its DDoS attacks, heavily relying on crowdsourcing. The group mainly targets government and financial institutions, with less frequent attacks on the healthcare and energy sectors. Positioning itself as pro-Russian, the group's activities are driven by political motives, particularly against information resources located in Europe. This is indirectly supported by posts on the group's Telegram channel. Prior to launching a new campaign, NONAME057(16) often shares a message in its Telegram channel accusing the target country, thereby justifying its forthcoming attack.

ALIASES

DDOSIA, DOSIA, NoName057

TOP TACTICS

Endpoint Denial of Service (T1499)
Network Denial of Service (T1498)
Defacement (T1491)

INDUSTRY FOCUS

Government and military · Financial services · Transportation · Internet services · Energy · Media and entertainment · Commerce and shopping · IT · Healthcare · Education · Real estate · Telecommunications · Professional services · Travel and tourism · Data and analytics

Ethersec Team Cyber

Alleged attribution
Indonesia

Scope
Worldwide

First seen
2024

ABOUT

ETHERSEC TEAM CYBER conducts attacks against companies and countries involved in the recent Israel and Palestine conflict. In addition, previous entities were targeted for no apparent reason other than data exfiltration. Their primary attacks involve website defacement and data leaks. They tend to publish all leaked data through their Telegram channels, sharing them as CSV files or Google Sheets. ETHERSEC TEAM CYBER uses publicly available Command & Control tooling when conducting their attacks. When performing website defacement, they were observed to share information on vulnerable websites for exploitation, more specifically exploiting URL parameters.

ALIASES

ethersecteam, ETHERSECPRIV

TOP TACTICS

Endpoint Denial of Service (T1499)
Defacement (T1491)

INDUSTRY FOCUS

Education · Healthcare · Government and military · Internet services · IT · Media and entertainment · Commerce and shopping · Science and engineering · Gaming · Manufacturing · Professional services · Travel and tourism · Consumer goods

Ripper Sec

Alleged attribution
Malaysia

Scope
Worldwide

First seen
2023

ABOUT

RipperSec is a Pro-Palestine hacktivist group which became active on June 17, 2023 in their Telegram channel @RipperSec. Performed attacks are mainly DDoS and Data Leak. In their Telegram channel the hacktivist group also forwards attacks and leaks from other groups. Based on the description of the channel, it could be assumed that the group is in collaboration with Nusantara @nusantaraMYID

ALIASES

RipperSec MY

TOP TACTICS

- Endpoint Denial of Service (T1499)
- Network Denial of Service (T1498)

INDUSTRY FOCUS

- Government and military
- Financial services
- Internet services
- Gaming
- Media and entertainment
- Education
- Commerce and shopping
- Hardware
- Food and beverage
- Real estate
- Healthcare
- IT
- Consumer goods

SYLHET GANG-SG

Alleged attribution
Bangladesh

Scope
India, Israel

First seen
2023

ABOUT

The Sylhet Gang is a religiously motivated hacktivist group involved in cyberactivism and hacking activities. While they have claimed responsibility for numerous DDoS attacks primarily targeting countries such as Israel and India, their operations extend worldwide. The group has been active on their Telegram channel, "SYLHET GANG-SG," since July 2023.

ALIASES

BlueFlame

TOP TACTICS

- Endpoint Denial of Service (T1499)
- Network Denial of Service (T1498)
- Defacement (T1491)
- Exfiltration Over Web Service (T1567)
- Exfiltration Over C2 Channel (T1041)
- Exfiltration Over Alternative Protocol (T1048)

INDUSTRY FOCUS

- Government and military
- Financial services
- Media and entertainment
- Content and publishing
- Education
- Internet services
- Transportation
- Data and analytics
- Real estate
- Commerce and shopping
- Agriculture and farming
- Design
- Community and lifestyle
- Manufacturing
- IT

THE ANONYMOUS BD

Alleged attribution
Bangladesh

Scope
India, Israel

First seen
2023

ABOUT

THE ANONYMOUS BD is a hacktivist group involved in cyberactivism and hacking activities. Since September 30, 2023, they have been active on their Telegram channel, @T_GRAY_Hacker. The group asserts on their channel that they target the resources of countries that support Israel.

ALIASES

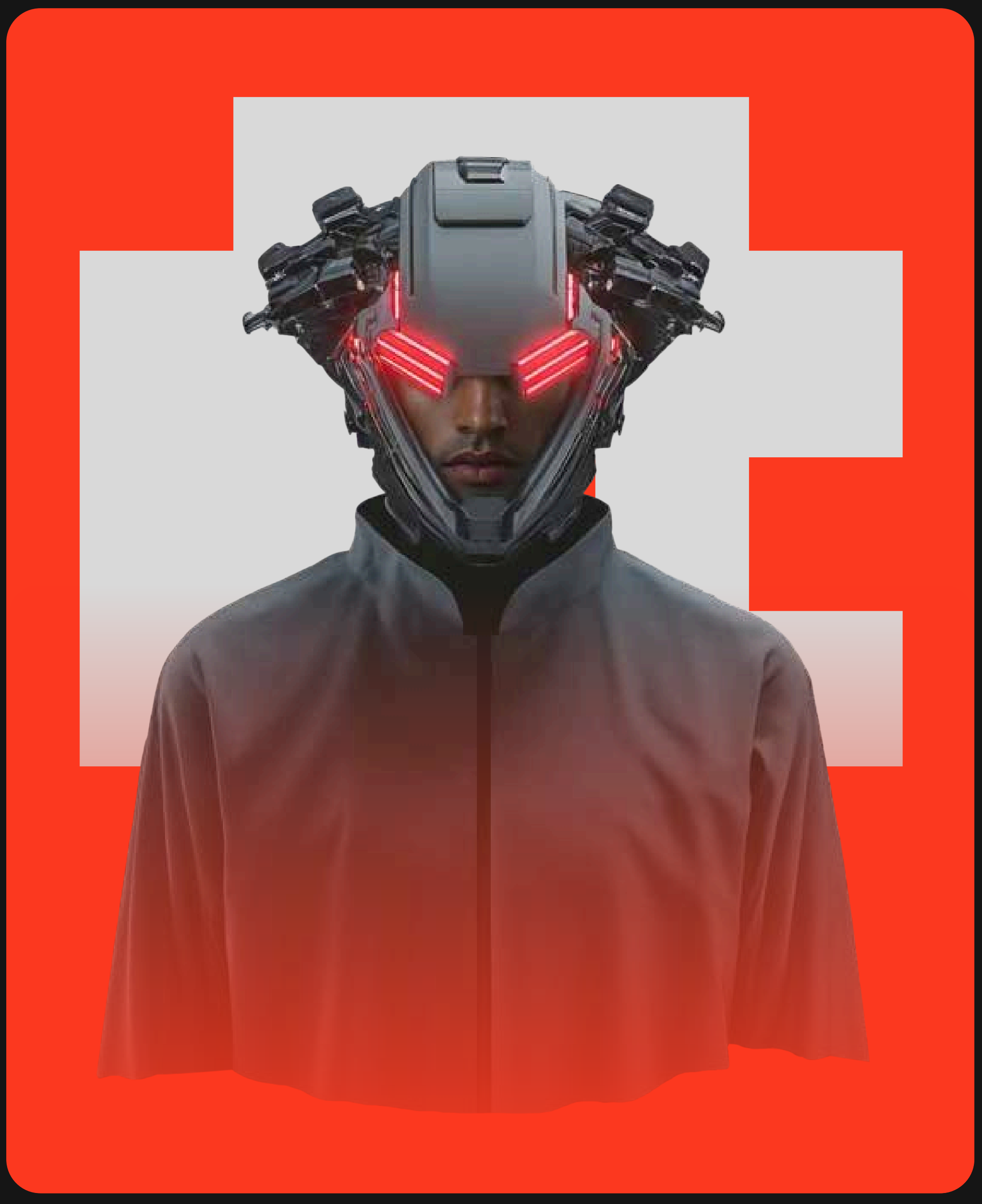
unknown

TOP TACTICS

- Endpoint Denial of Service (T1499)
- Network Denial of Service (T1498)
- Defacement (T1491)
- Exfiltration Over Web Service (T1567)
- Exfiltration Over C2 Channel (T1041)
- Exfiltration Over Alternative Protocol (T1048)

INDUSTRY FOCUS

- Internet services
- Consumer goods
- Financial services
- Education
- Data and analytics
- Government and military
- Healthcare
- Commerce and shopping
- Real estate
- Content and publishing
- Hardware
- Media and entertainment
- Professional services
- Community and lifestyle
- Events



Tengkorak Cyber Crew

Alleged attribution
Malaysia

Scope
India, Israel

First seen
2023

ABOUT

Tengkorak Cyber Crew is a hacktivist group that claims to engage in cyberactivism and hacking activities. While they have taken responsibility for numerous DDoS and web defacement attacks primarily targeting countries such as Israel and India in the wake of the Israeli-Palestinian conflict, their operations extend globally. The group has been active on Telegram and Discord since October 2023.

ALIASES

unknown

TOP TACTICS

- Endpoint Denial of Service (T1499)
- Network Denial of Service (T1498)
- Defacement (T1491)
- Exfiltration Over Web Service (T1567)

INDUSTRY FOCUS

- Internet services
- Media and entertainment
- Commerce and shopping
- Education
- Hardware
- Healthcare
- IT
- Software
- Community and lifestyle
- Financial services
- Gaming
- Science and engineering

DarkStorm Team

Alleged attribution
unknown

Scope
Israel, MEA

First seen
2023

ABOUT

DarkStorm Team is a relatively new hacktivist group that emerged in August 2023. Since its inception, the group has primarily targeted Israel. Additionally, DarkStorm Team has engaged in attacks that align with the activities of Eagle Cyber Crew and Team Herox. The group predominantly employs DDoS as its primary attack method; however, a message posted on their Telegram channel indicates that they also possess tools for defacement attacks and are open to offering their services for a fee.

ALIASES

unknown

TOP TACTICS

- Endpoint Denial of Service (T1499)
- Network Denial of Service (T1498)

INDUSTRY FOCUS

- Government and military
- Financial services
- Transportation
- Content and publishing
- Education
- Food and beverage
- Energy
- Media and entertainment
- Commerce and shopping
- Events
- Internet services
- Professional services

IT ARMY of Ukraine

Alleged attribution
Ukraine

Scope
Russia, Belarus, Montenegro

First seen
2022

ABOUT

The IT Army of Ukraine is a hacktivist group that was established on February 26, 2022, with the aim of targeting Russian and pro-Russian resources. They publish tasks for IT volunteers from around the globe on their Telegram channels. The group utilizes the IT ARMY KIT, their official application designed for operating systems with a graphical interface, which includes essential tools for conducting DDoS attacks.

ALIASES

it_army_of_ukraine, itaou

TOP TACTICS

- Endpoint Denial of Service (T1499)
- Network Denial of Service (T1498)

INDUSTRY FOCUS

- Government and military
- Financial services
- Transportation
- Content and publishing
- Education
- Food and beverage
- Energy
- Media and entertainment
- Commerce and shopping
- Events
- Internet services
- Professional services

Lulz Security Agency

Alleged attribution
Indonesia

Scope
India, Israel

First seen
2023

ABOUT

Lulz Security Agency is a hacktivist group that emerged in August 2023. They are recognized for their support of Palestine and their opposition to Israel and India. In August 2023, the group began operating independently through their Telegram channel, @lulzsecurityagency, where they have been sharing statements, leaks, defacements, and targets for DDoS attacks. The group's primary focus is on identifying and taking action against content and activities they perceive as conflicting with Islamic law, particularly in the realm of public media. This includes cyber campaigns aimed at exposing, disrupting, or countering such content.

ALIASES

unknown

TOP TACTICS

Endpoint Denial of Service (T1499)

INDUSTRY FOCUS

Telecommunications · Education · Internet services · Financial services · Real estate · Commerce and shopping · Consumer goods · Government and military · Professional services · Science and engineering · Travel and tourism

Indonesia Anonymous

Alleged attribution
Indonesia

Scope
Israel, Worldwide

First seen
2023

ABOUT

Indonesia Anonymous is a hacktivist group that participates in cyberactivism and hacking activities. The group has been active since September 18, 2023, on their Telegram channel, @ackedindonesi. On February 2, 2024, the username of their Telegram channel was changed @informasi_leak. They engage in DDoS attacks, defacements, and data leaks. Initially, the group acted against Israel, but later they expanded geography.

ALIASES

zalcyber, Rogojampi Hacktivist, ZALCYBER, RogojampiHacktivist

TOP TACTICS

Endpoint Denial of Service (T1499)
Defacement (T1491)
Exfiltration Over Web Service (T1567)

INDUSTRY FOCUS

Education · Internet services · Consumer goods · Commerce and shopping · Real estate · Transportation · Data and analytics · Financial services · Healthcare · IT · Professional services · Sales and marketing · Science and engineering

Ransomware / DLS

In today's digital landscape, ransomware has emerged as one of the most formidable threats facing companies across the globe. This malicious software not only encrypts critical data, rendering it inaccessible, but also demands hefty ransoms for its release, often leaving organizations in a precarious position. Moreover, ransomware has evolved into a sprawling underground industry, characterized by the emergence of Ransomware-as-a-Service (RaaS) affiliate programs, dedicated leak sites (DLS) that publicly expose stolen data, and the involvement of initial access brokers (IABs) who facilitate entry into targeted networks, creating a complex ecosystem that amplifies the threat and accessibility of these attacks for cybercriminals.

Affiliate or partner programs for cybercriminals, known as **Ransomware-as-a-Service (RaaS)**, consist of affiliates who join to execute specific roles within cybercriminal networks, primarily focusing on delivering and deploying ransomware in corporate environments. These programs have evolved significantly over the years. Initially, affiliates were selected based on their experience and access to corporate networks, but today, they operate more like large-scale enterprises.

In 2024, Group-IB identified **39 advertisements** for RaaS programs on dark web forums. In 2024, the number of offers looking for affiliates to join RaaS programs increased by **44%** compared to 2023.

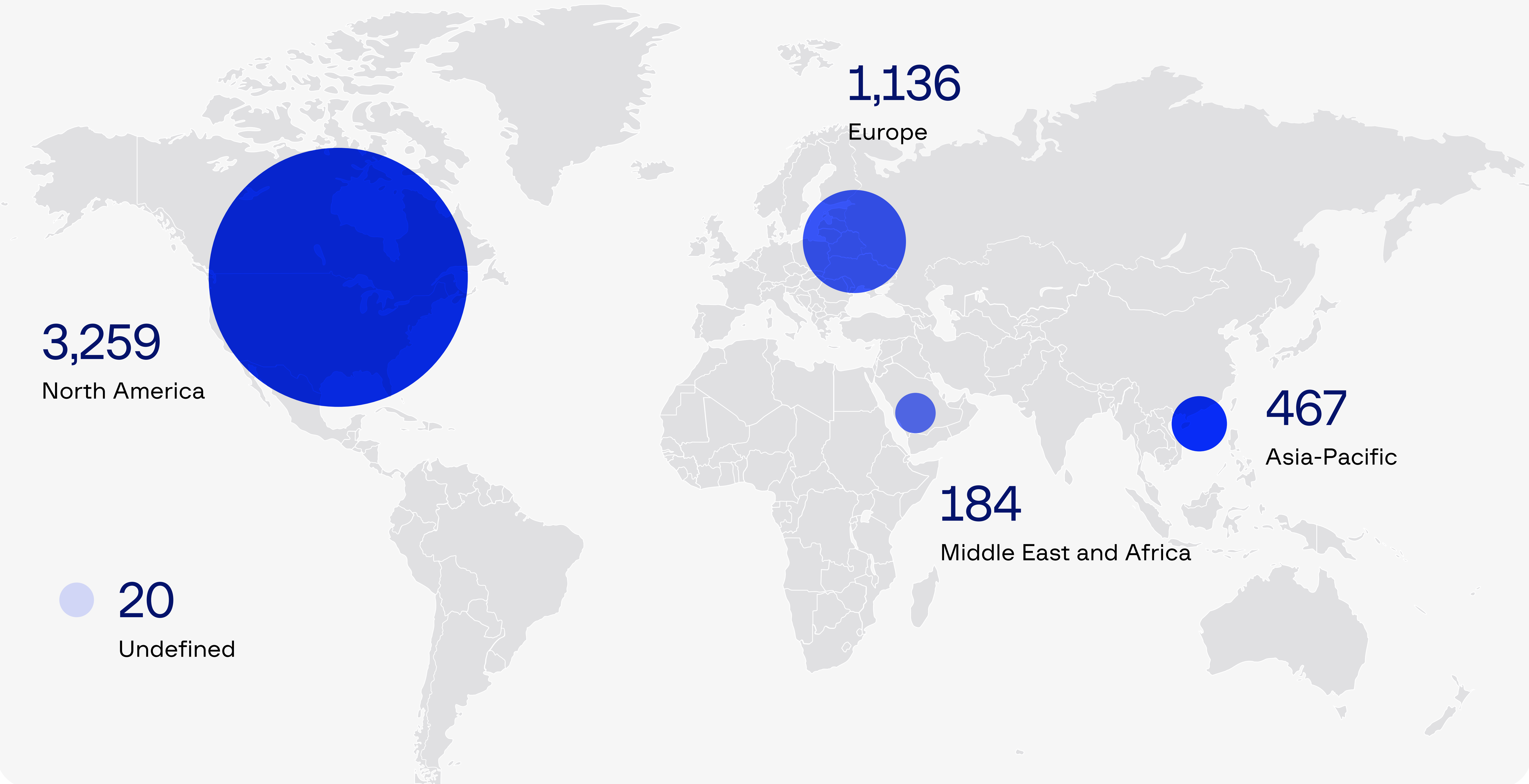
Date	Ransomware	Username	Forum
27.01.2024	TrapTight	SkyWalker	Breachforums
28.01.2024	Wing	blackhunt	RAMP
02.02.2024	RansomHub	koley	RAMP
07.02.2024	-	skz112	RAMP
07.02.2024	Cloak	wockstar	ufolabs
09.02.2024	Synapse	Simon128	RAMP
24.02.2024	Medusa	Medusa	RAMP
03.03.2024	Black Hunt 2.0	blackhunt	RAMP
11.03.2024	FLOCKER	Vtyaion	bestblackhatforum
18.04.2024	Apos	Bezzle	RAMP
24.04.2024	Psoglav	rtgtgth	RAMP

Date	Ransomware	Username	Forum
26.04.2024	Partn3rka	M3llstroy	Lolz
27.04.2024	Kadavro	angelbanker	Cracked.to
09.05.2024	Rape	rapelord	promarket.ws
25.05.2024	SpiderX	phant0m	onniforums
07.06.2024	-	FireWalker	RAMP
18.06.2024	Nevermore	TheShadowHacker	RAMP
24.06.2024	AzzaSec	AzzaSec	crackingx
26.06.2024	DragonForce	dragonforce	RAMP
27.06.2024	-	uliss	RAMP
28.06.2024	-	guccigan	RAMP
29.06.2024	Cicada3301	Cicada3301	RAMP
11.07.2024	Meow	MLeak	XSS
15.07.2024	-	skz112	RAMP
19.07.2024	-	uliss	RAMP
23.07.2024	-	realOnline	DarkMarkey
31.07.2024	VAULTLOCKER	VAULTLOCKER	CryptBB
08.08.2024	Lynx	silencer	RAMP
24.08.2024	Frid	halvdan130	Cracked
28.08.2024	-	obe1	Verifed
05.09.2024	InvaderX	InvaderX	RAMP
06.09.2024	-	FASTPRISONER	RAMP
24.10.2024	Bashe	-	Bashe
31.10.2024	PlayBoy	Kyley	RAMP

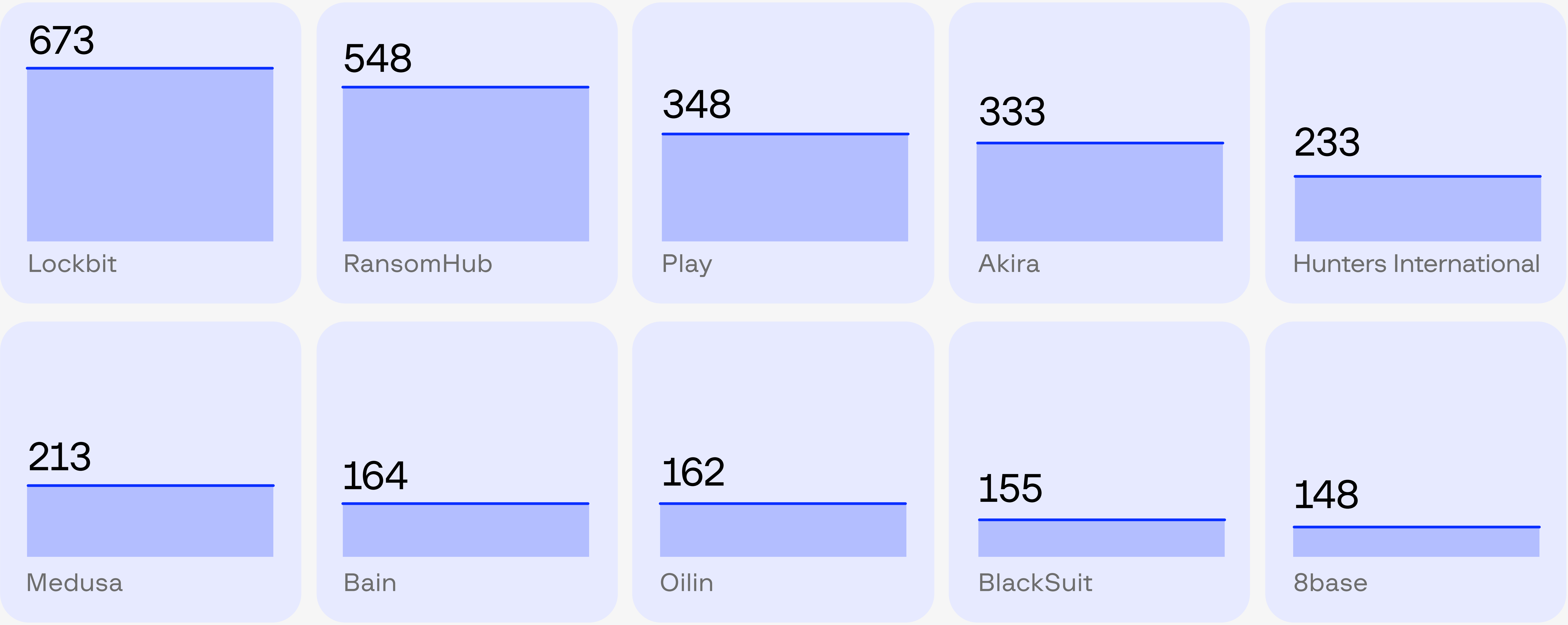
Date	Ransomware	Username	Forum
31.10.2024	Slivk	hotashell	Nulled
01.11.2024	DragonRansom	-	Telegram
06.11.2024	Hellborn	blackw0tch	Cracked
20.11.2024	rssmai	realOnline	Seopirat
19.12.2024	LockBit4.0	-	LockBit

A **dedicated leak site (DLS)** is a platform where data stolen from companies that refuse to pay a ransom is published. Group-IB specialists analyzed DLSs used by various ransomware groups and identified approximately **5,066 attacks** that were published on DLSs in 2024, an increase of **10%** over 2023, during which **4,583 attacks** were published. The number of total ransomware attacks worldwide is likely to be much larger, with probable instances of organizations paying the ransom or groups deciding not to go ahead with their threat of publishing data on a DLS.

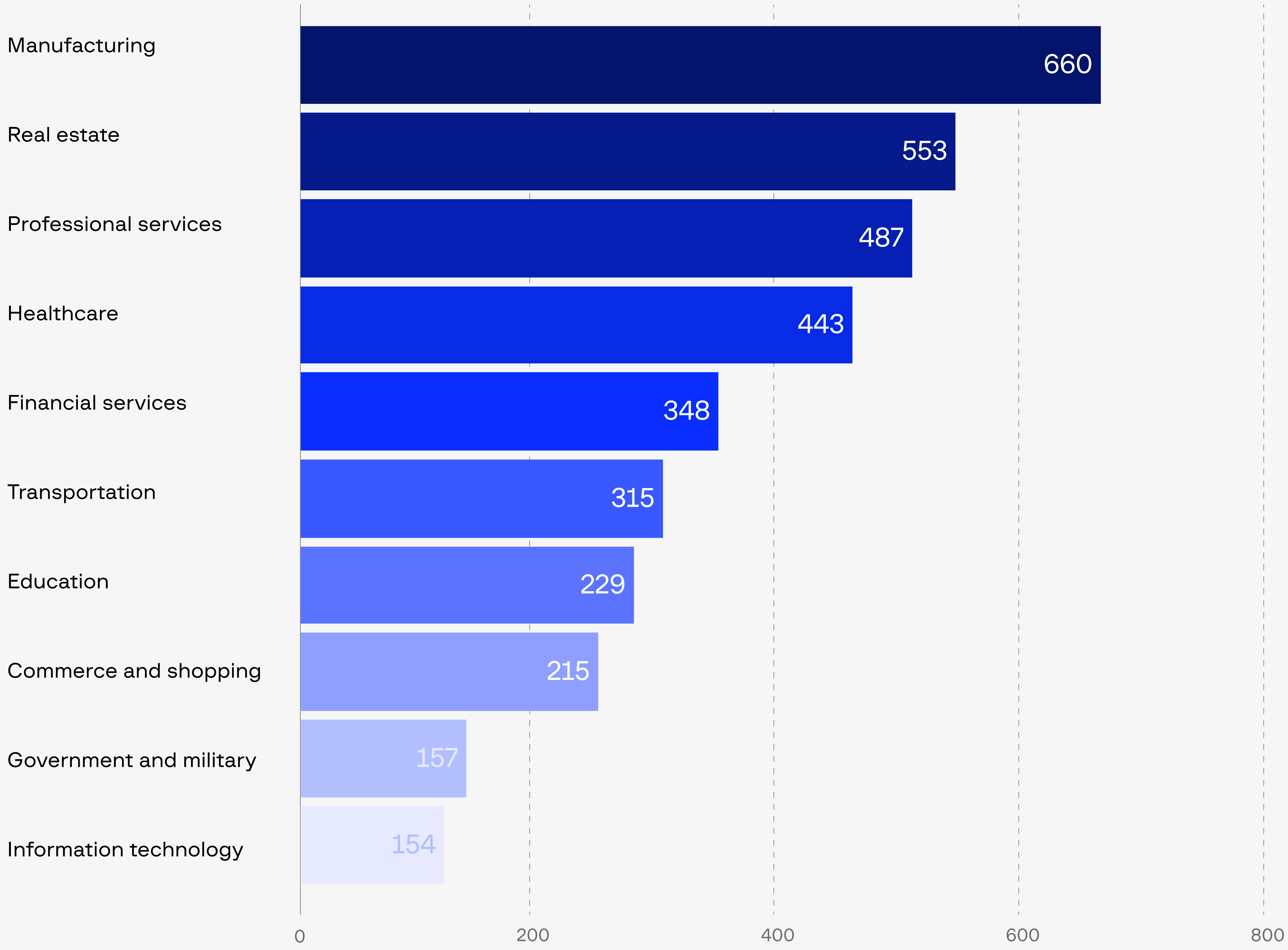
Global Distribution of ransomware attacks by region in 2024



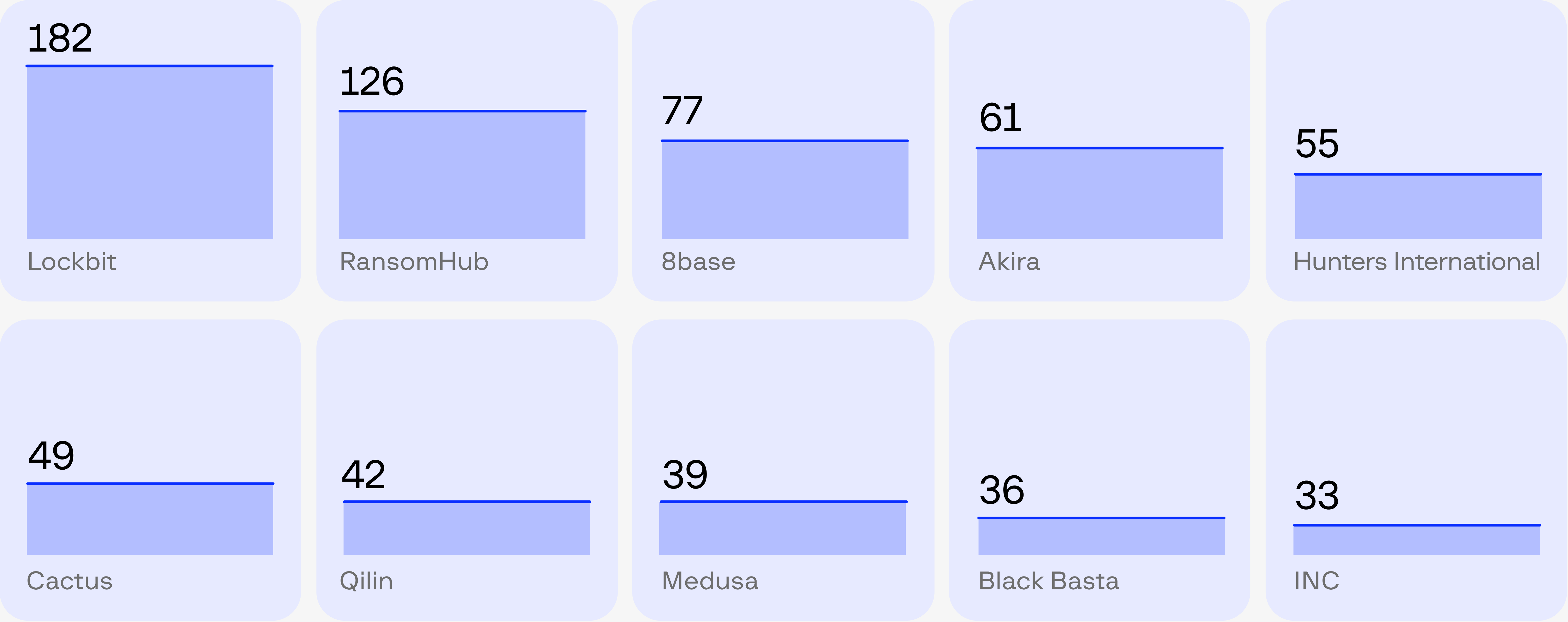
Global Top 10 ransomware groups by number of attacks in 2024



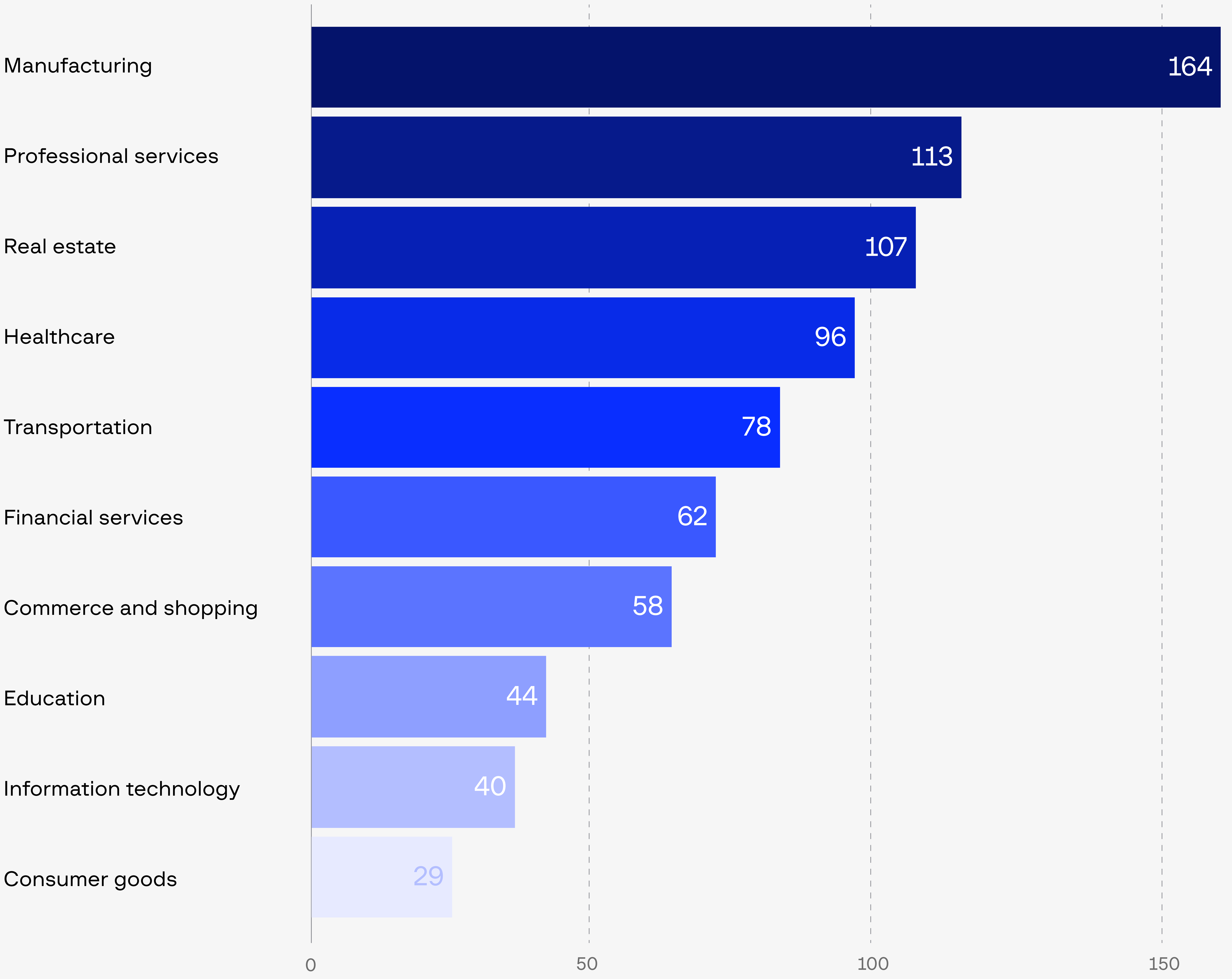
Global Top industries targeted by ransomware groups



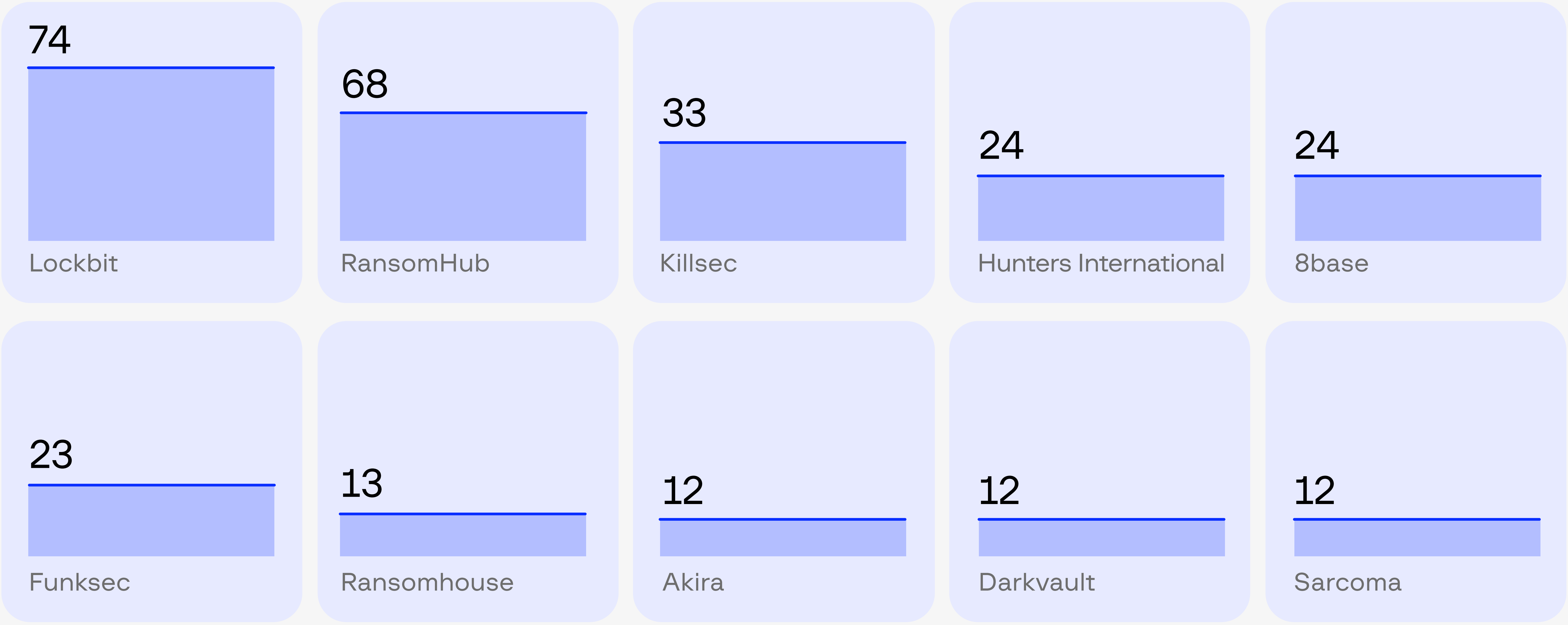
Europe Top 10 ransomware groups by number of attacks in 2024



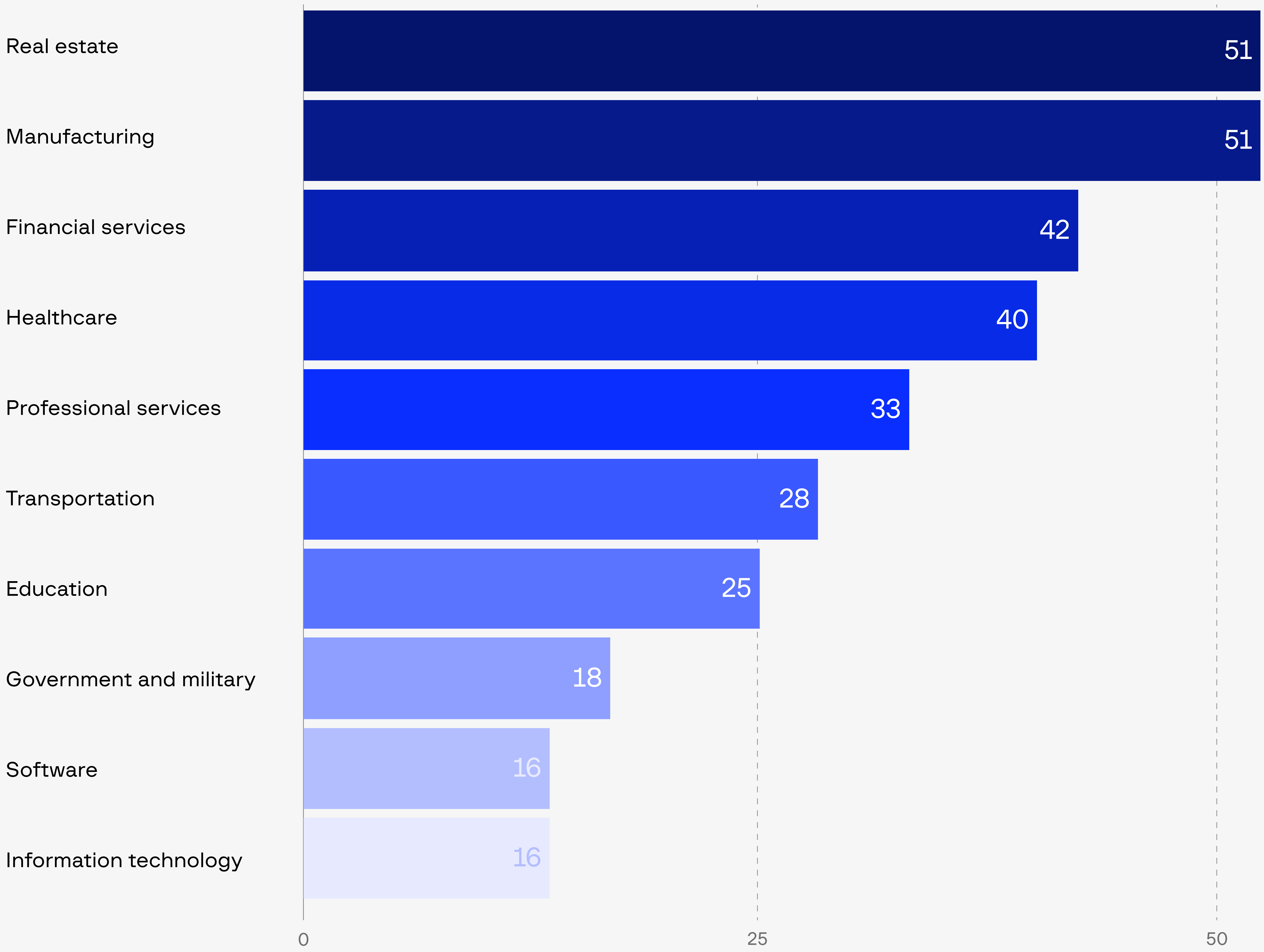
Europe Top 10 industries targeted by ransomware in 2024



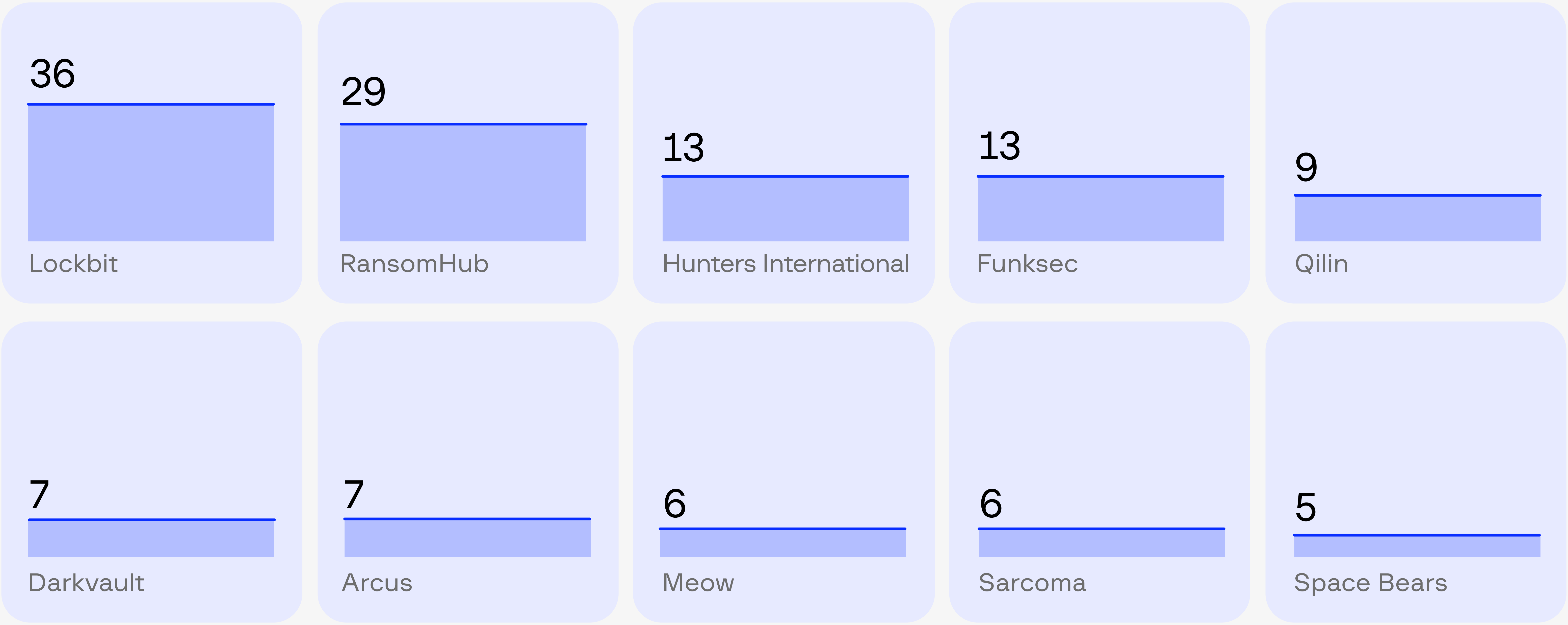
Asia-Pacific Top 10 ransomware groups by number of attacks in 2024



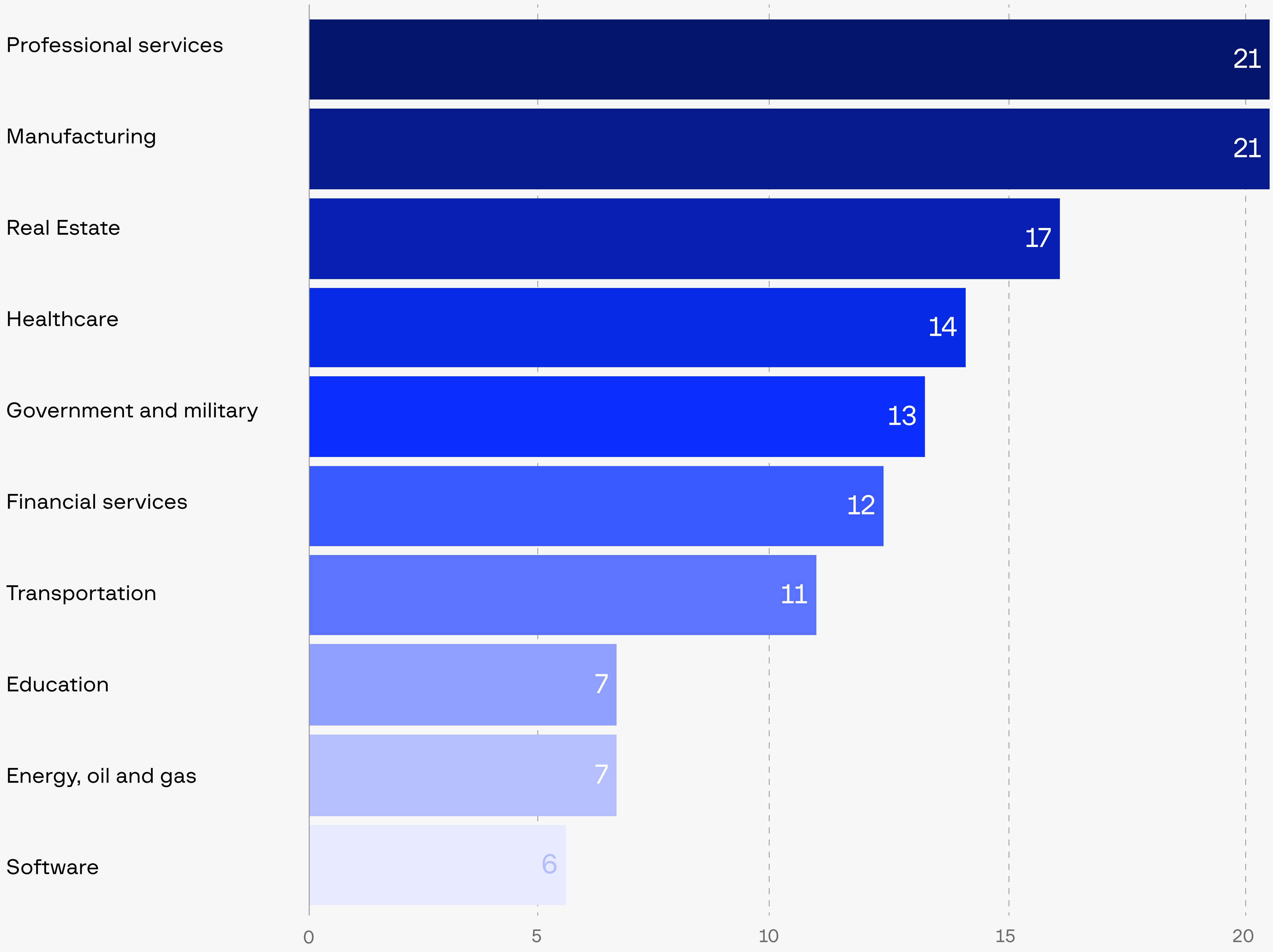
Asia-Pacific Top 10 industries targeted by ransomware in 2024



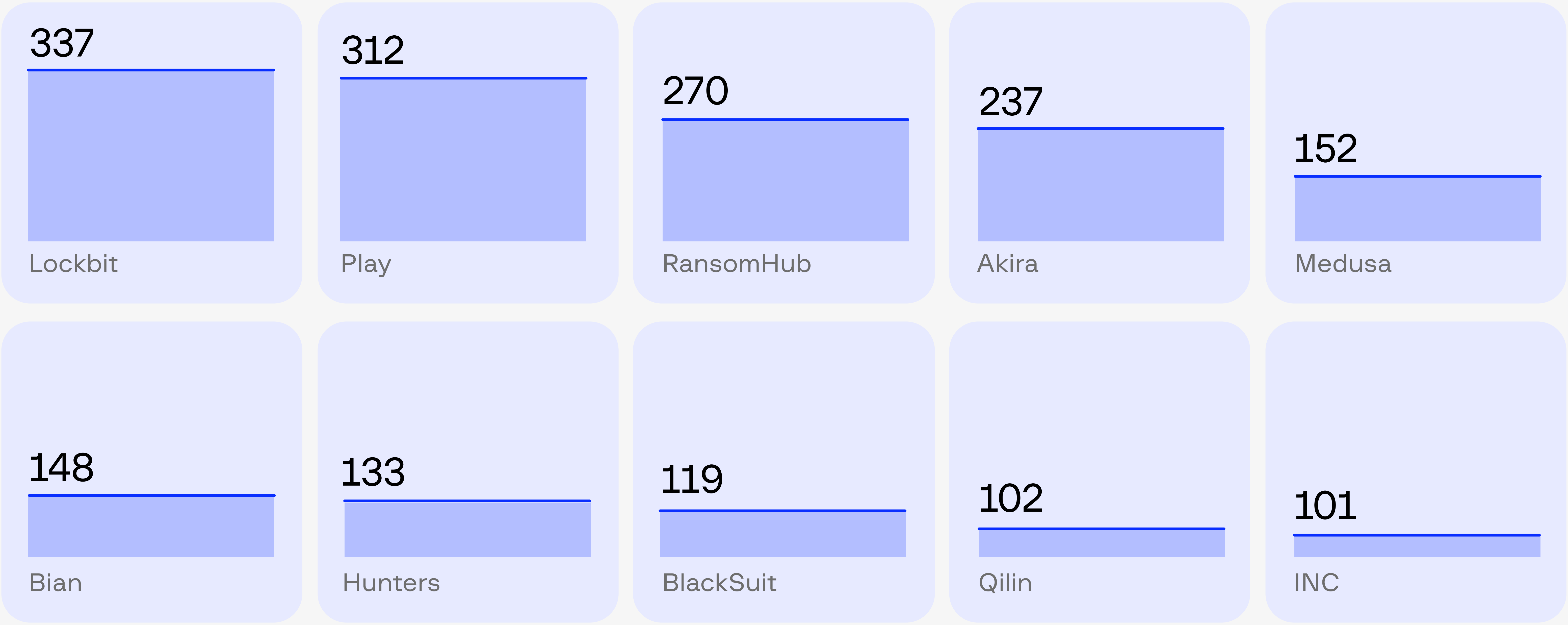
Middle East and Africa Top 10 ransomware groups by number of attacks in 2024



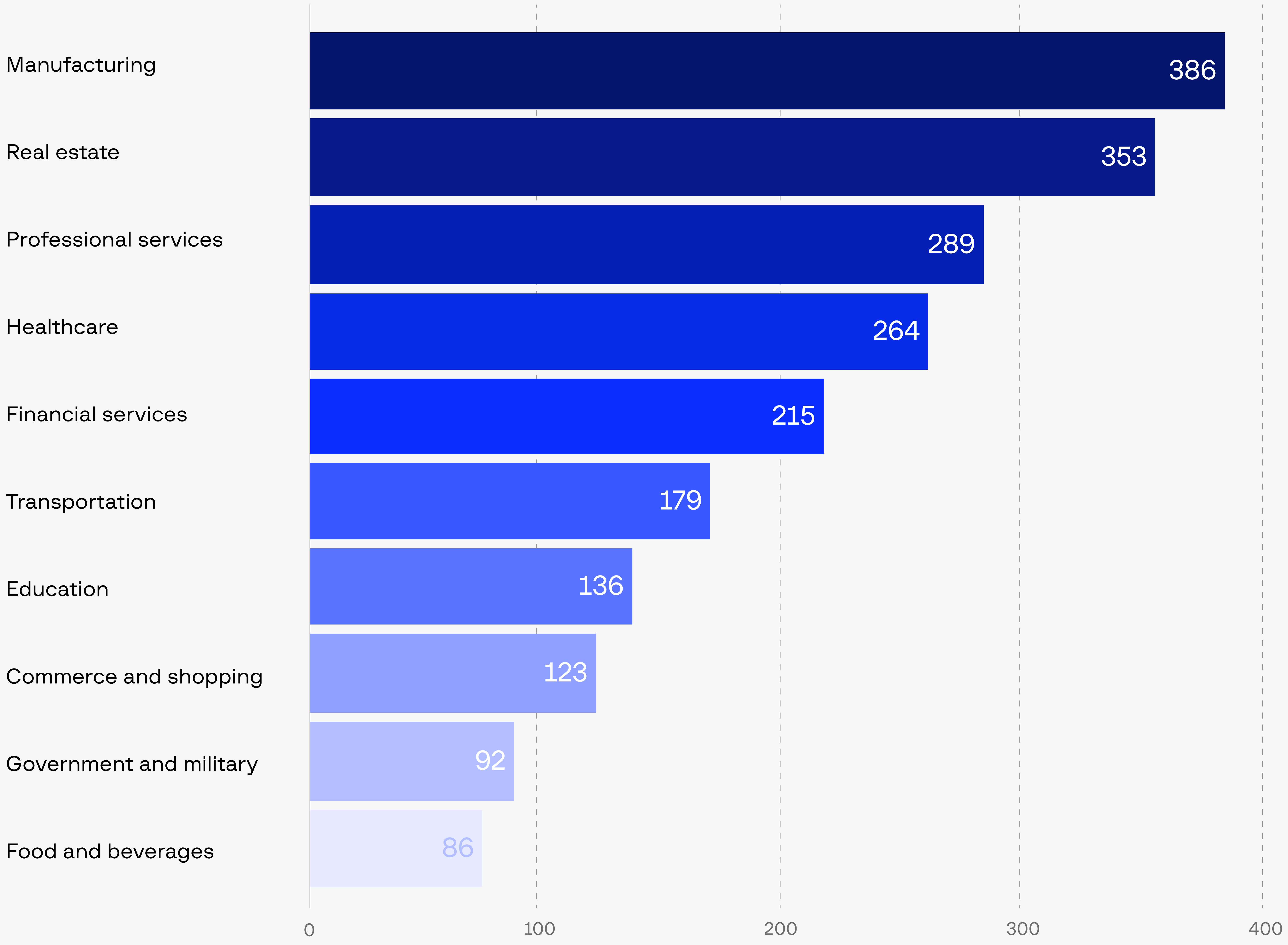
Middle East and Africa Top 10 industries targeted by ransomware in 2024



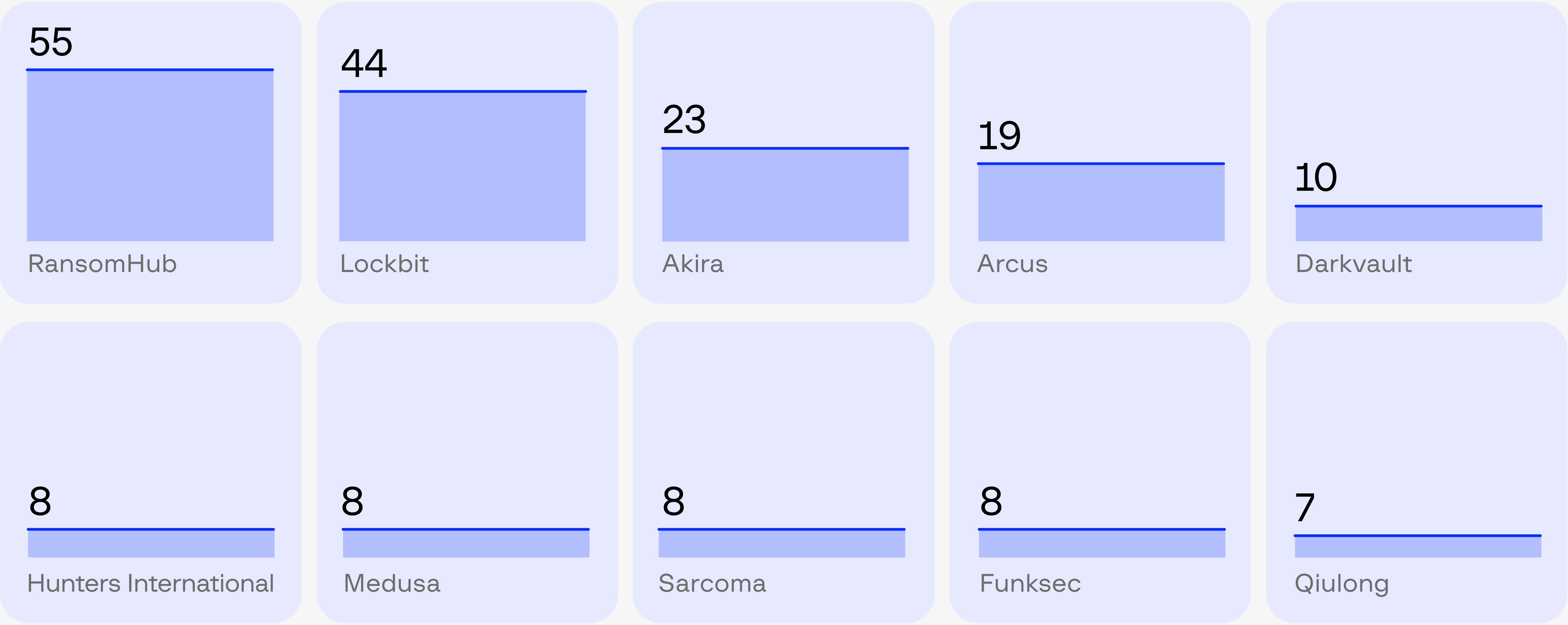
North America Top 10 ransomware groups by number of attacks in 2024



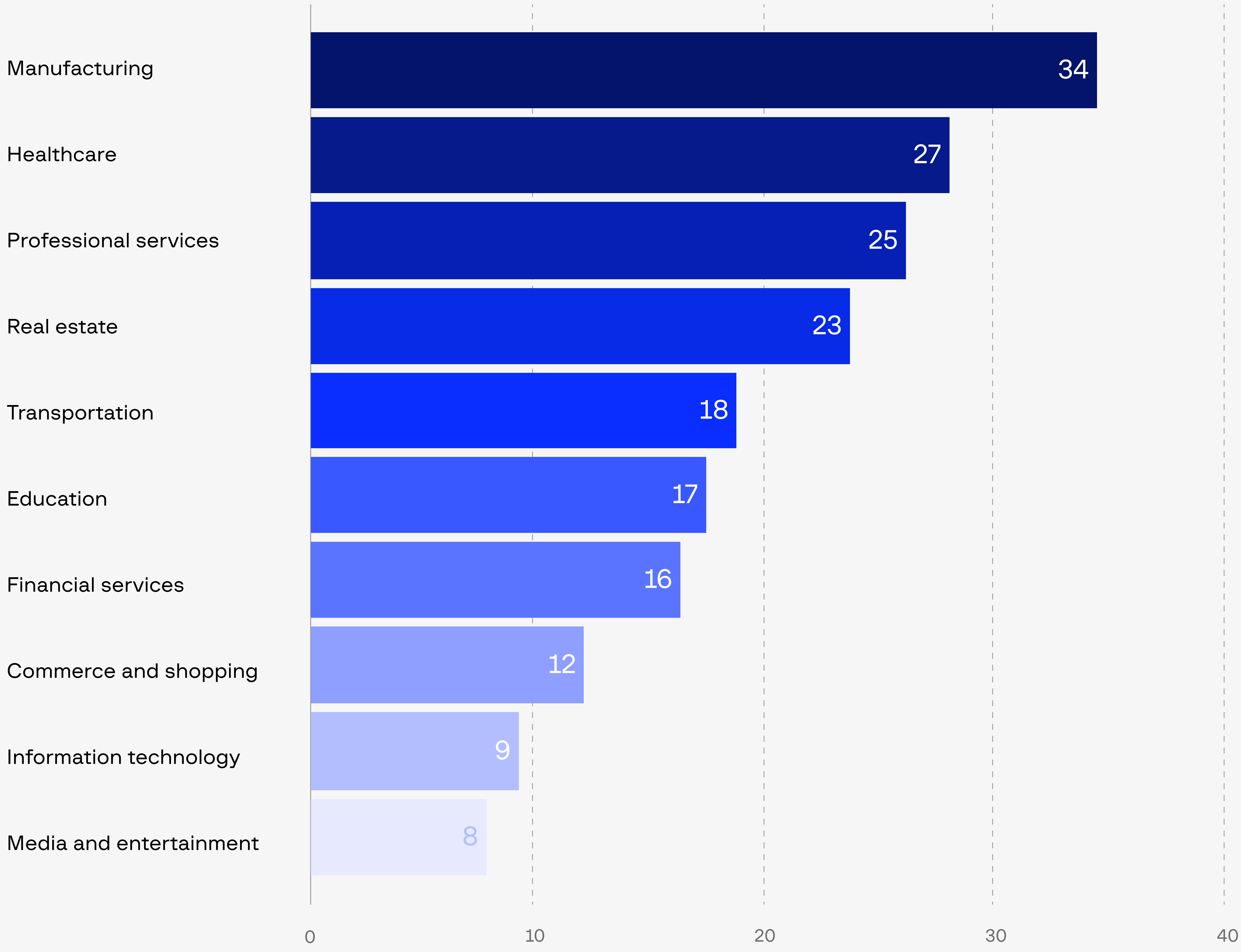
North America Top 10 industries targeted by ransomware in 2024



Latin-America Top 10 ransomware groups by number of attacks in 2024



Latin-America Top 10 industries targeted by ransomware in 2024



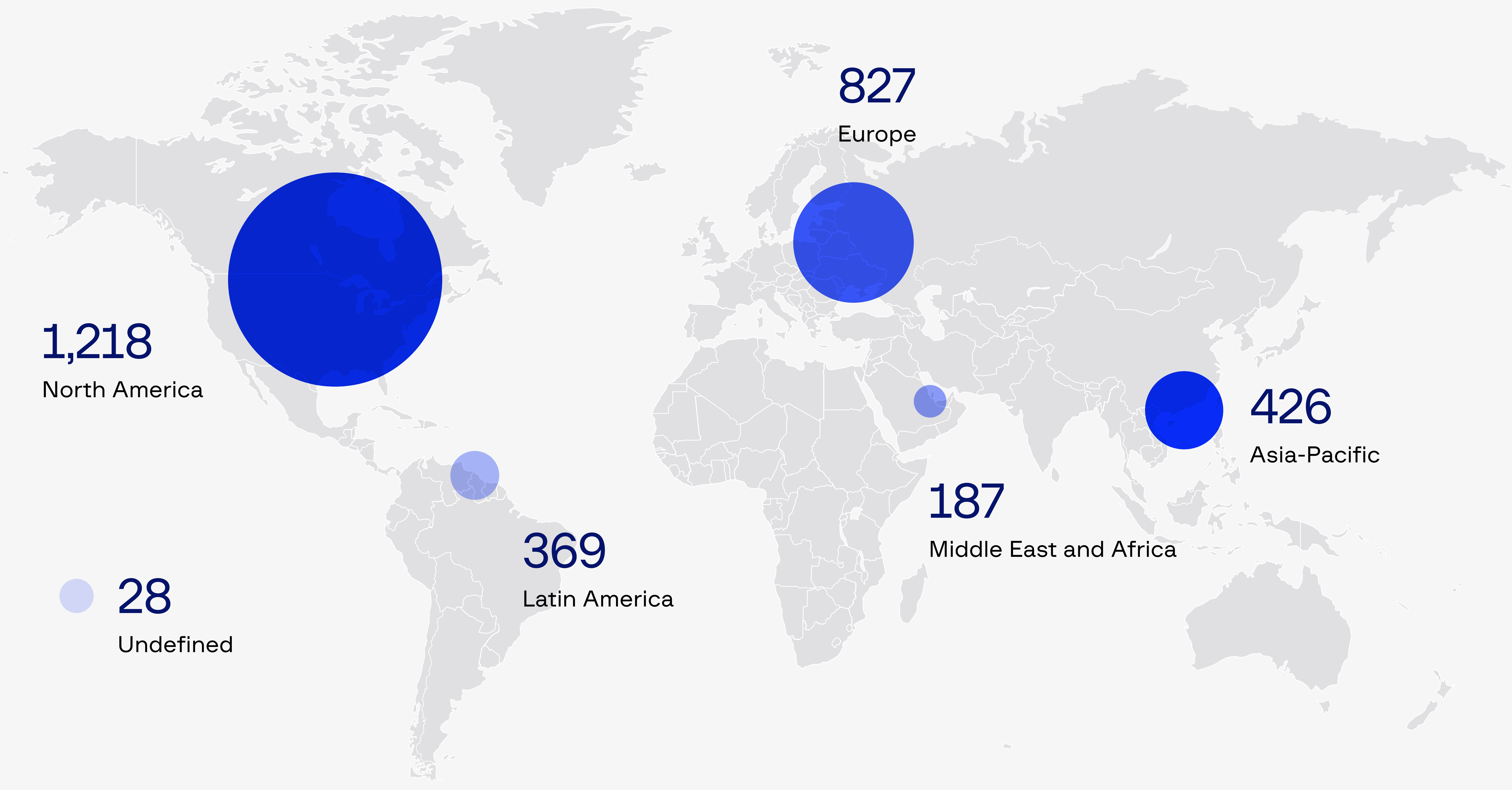
Initial Access Brokers

Initial Access Brokers (IABs) are threat actors who gain access to corporate computer systems and then sell the access on the dark web. The initial access to a company's system could potentially result in data theft, corporate espionage, or malware installed in the infrastructure for various other malicious purposes.

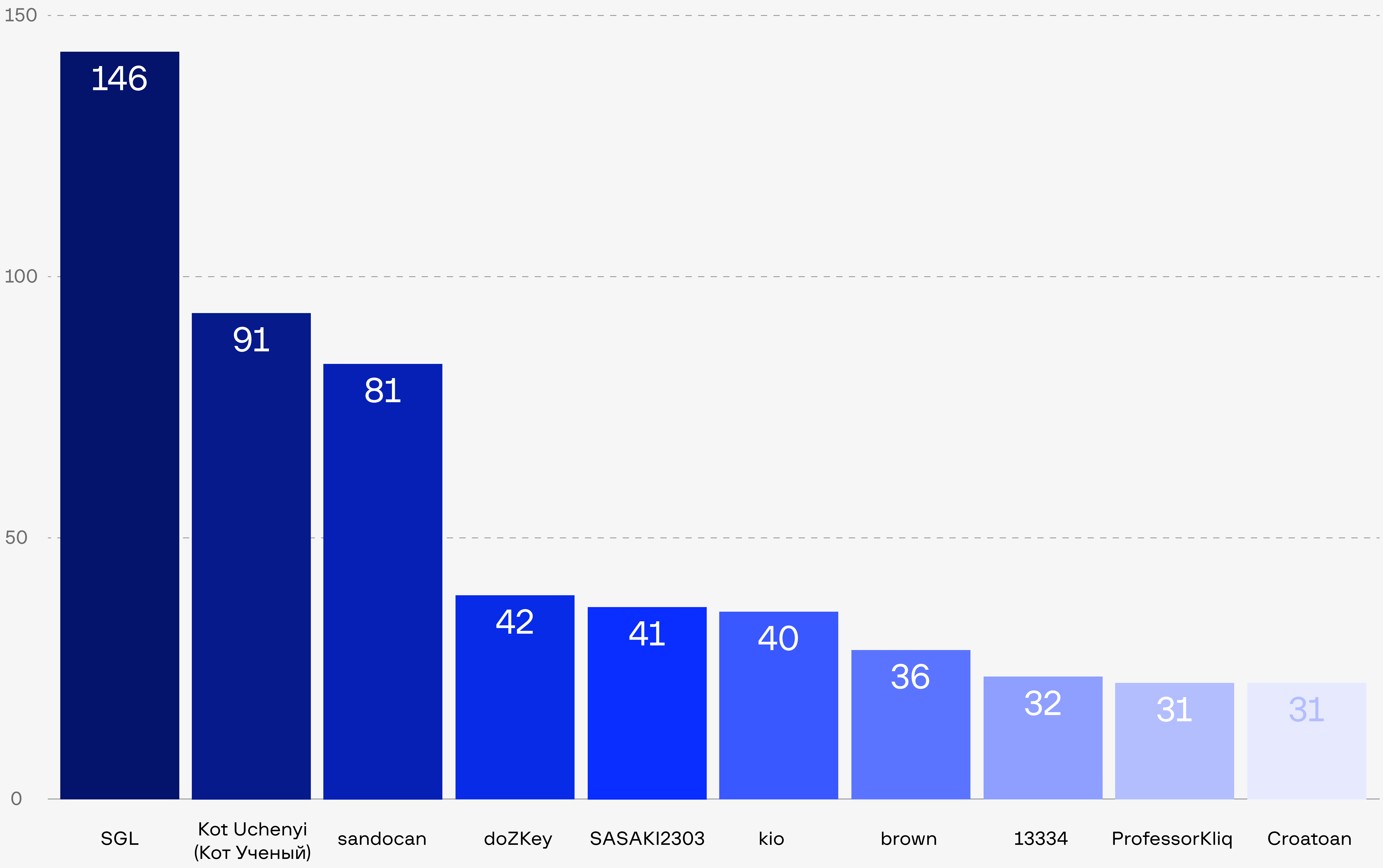
Over the course of 2024, Group-IB detected a total of 3,055 instances of access to corporate computer systems for sale on the dark web, a 15% increase over 2023 (2,646). The overall surge is exacerbated by 1,218 instances from North America, an increase of 43% compared to 2023. This trend is also reflected in the rise in other regions including Europe (32%) and Latin-America (41%), while the number of instances in the Asia-Pacific and Middle East and Africa regions remain broadly similar to the previous year.

The leading sellers of initial access on the dark web are SGL, Kot Ucheniy or Wise Cat (Кот Ученый in Russian), and sandocan with detected instances for sale totaling 146, 91, and 81, respectively.

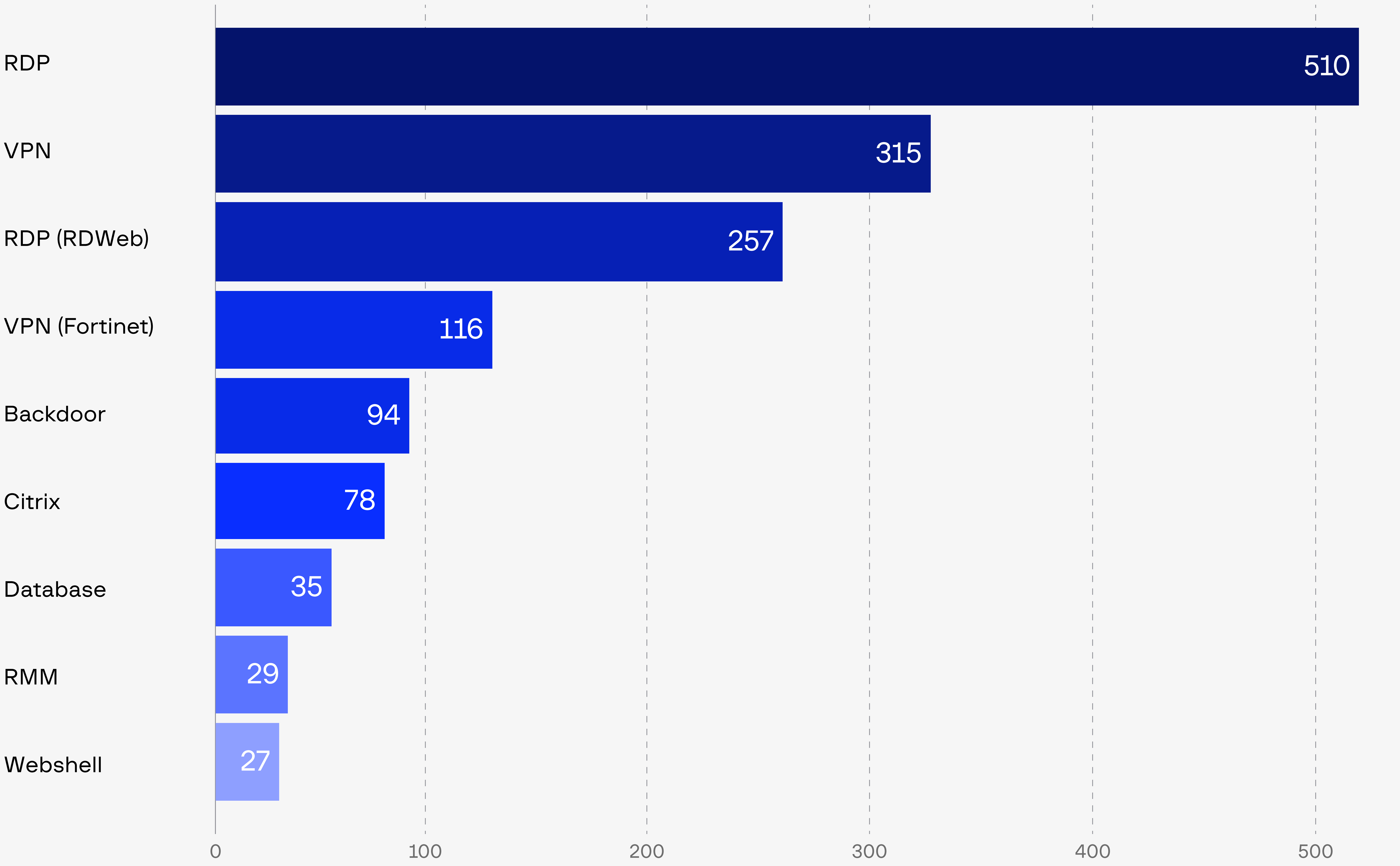
Global Instances of corporate access detected and sold on the dark web by region in 2024



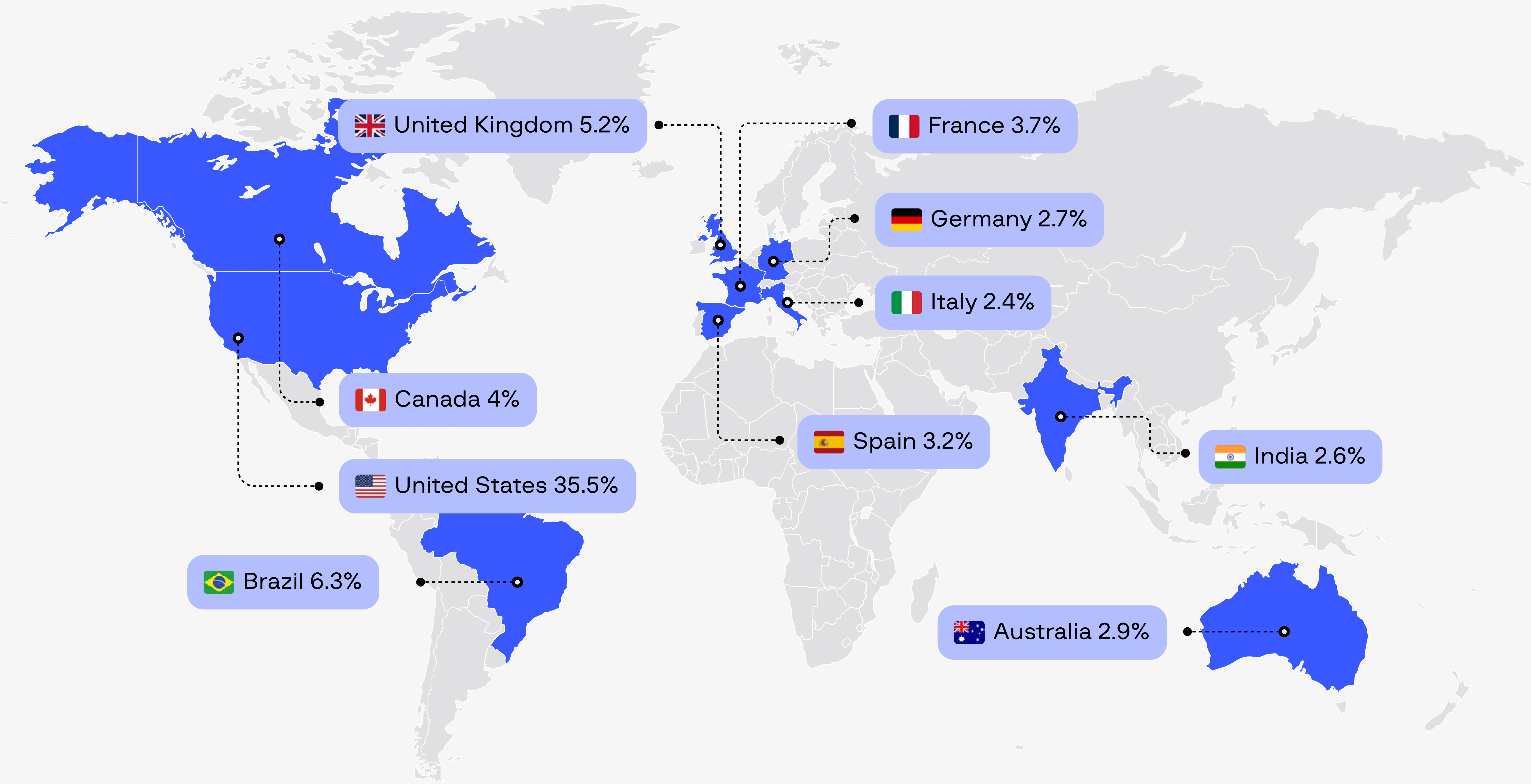
Top-10 initial access sellers by number of instances on sale



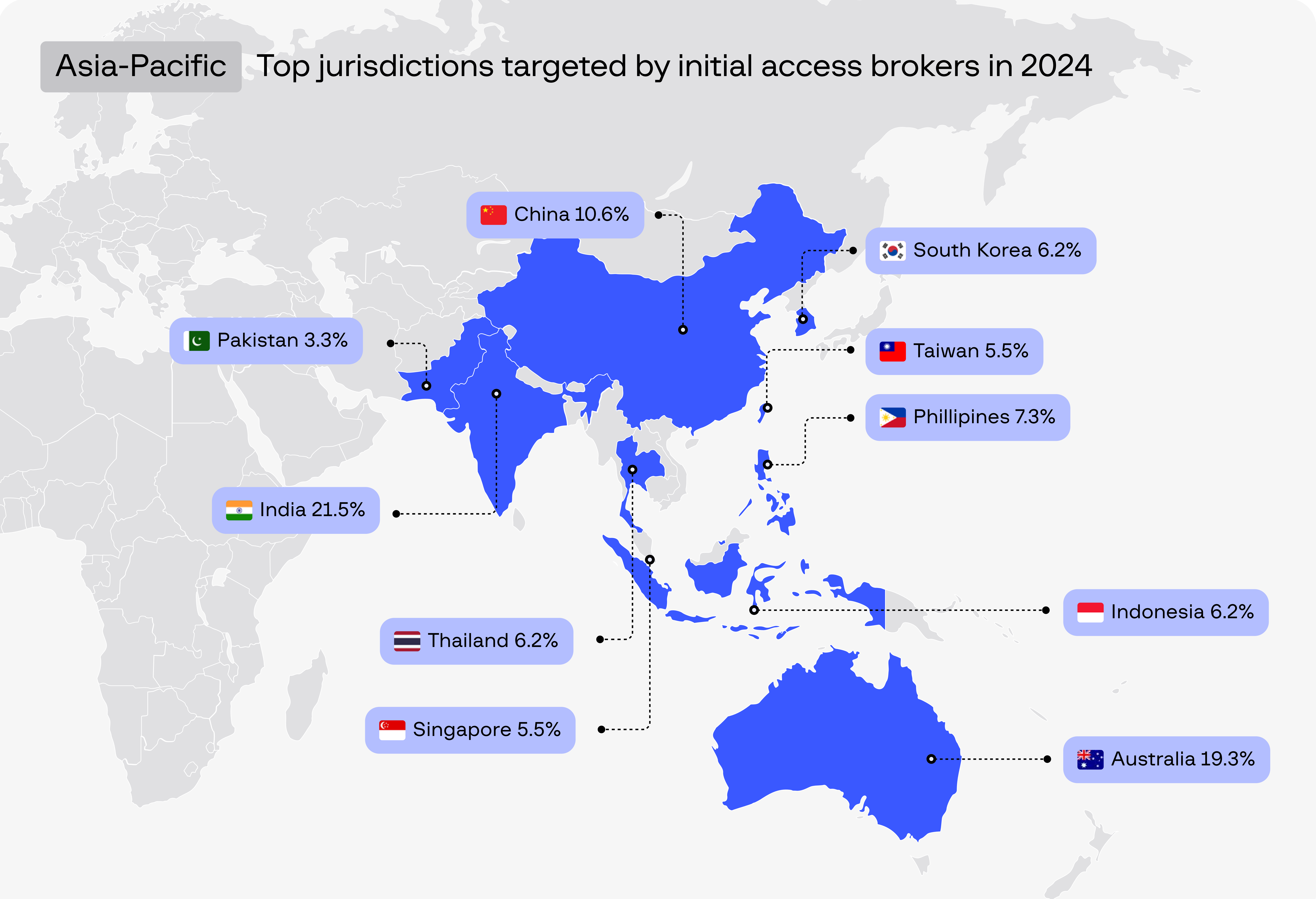
Top types of initial access sold



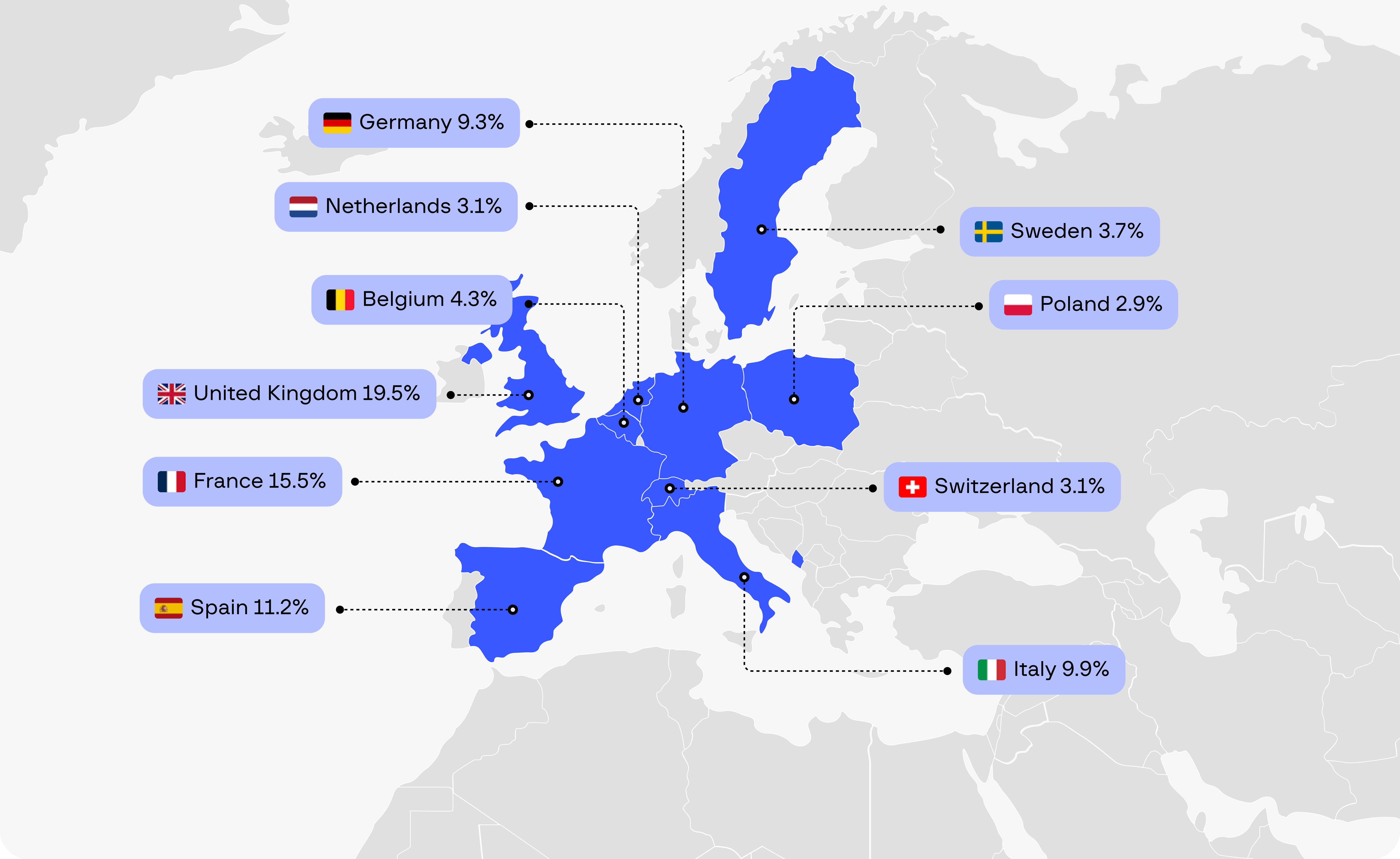
Global Top 10 jurisdictions targeted by initial access brokers in 2024



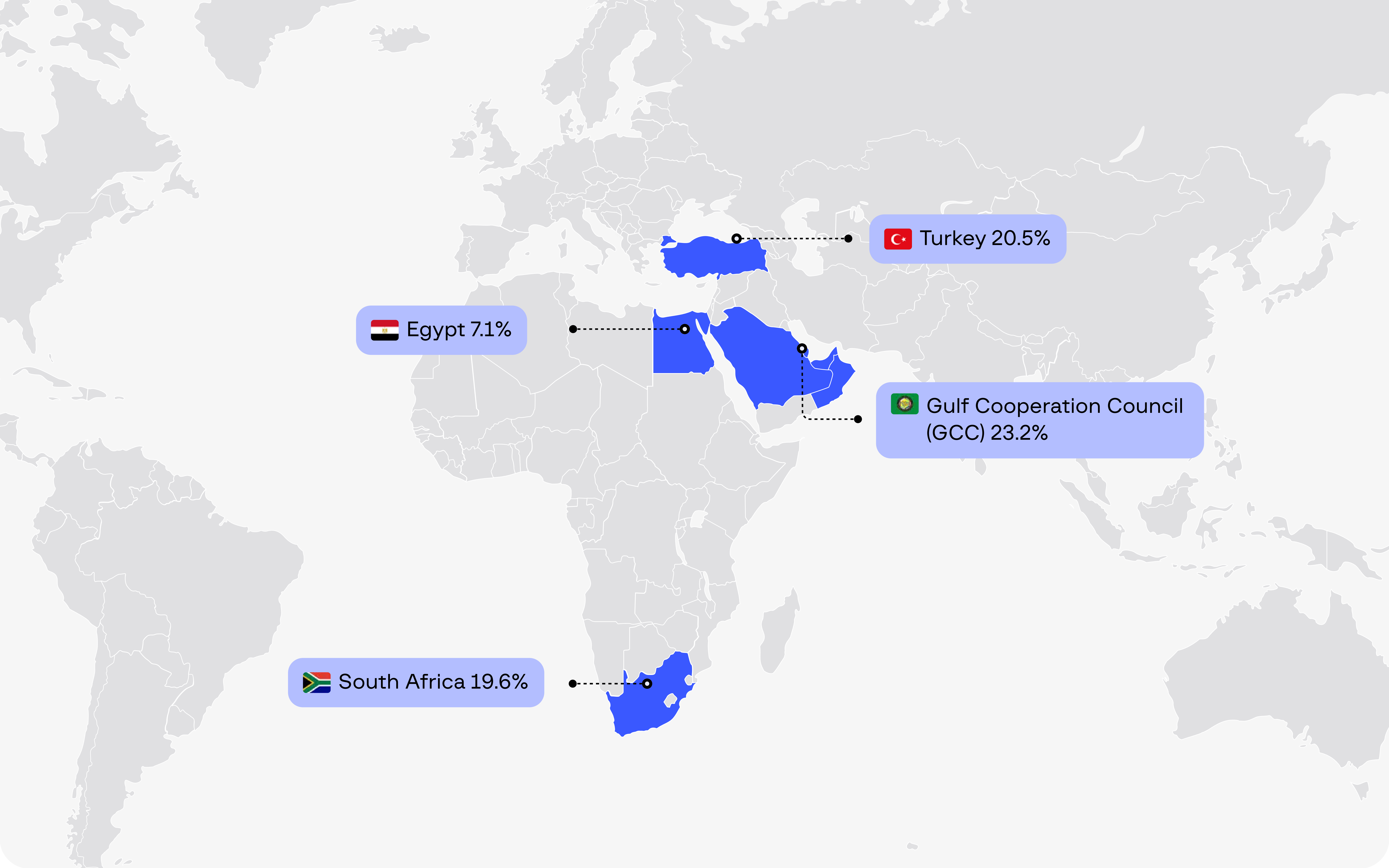
Asia-Pacific Top jurisdictions targeted by initial access brokers in 2024



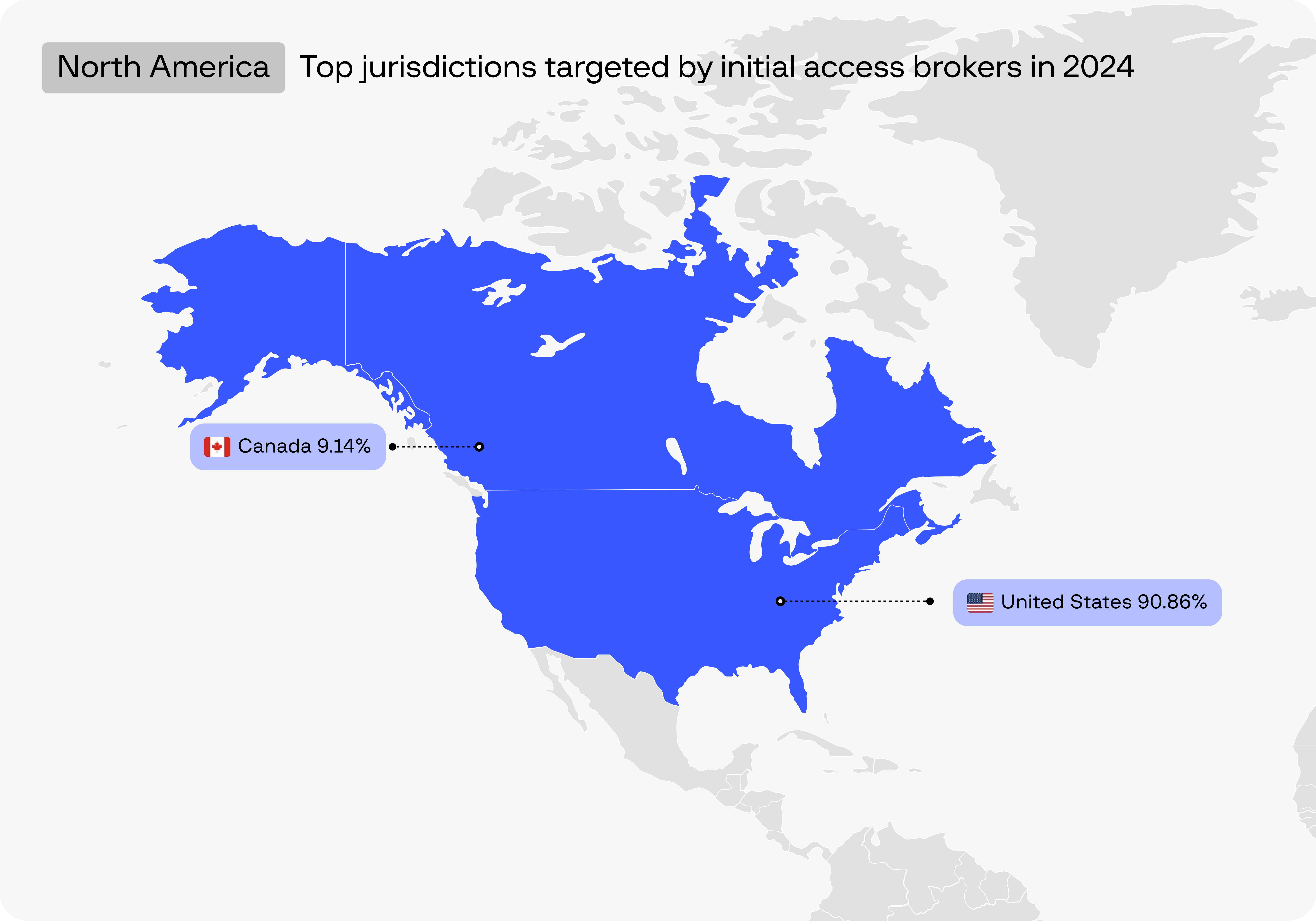
Europe Top jurisdictions targeted by initial access brokers in 2024



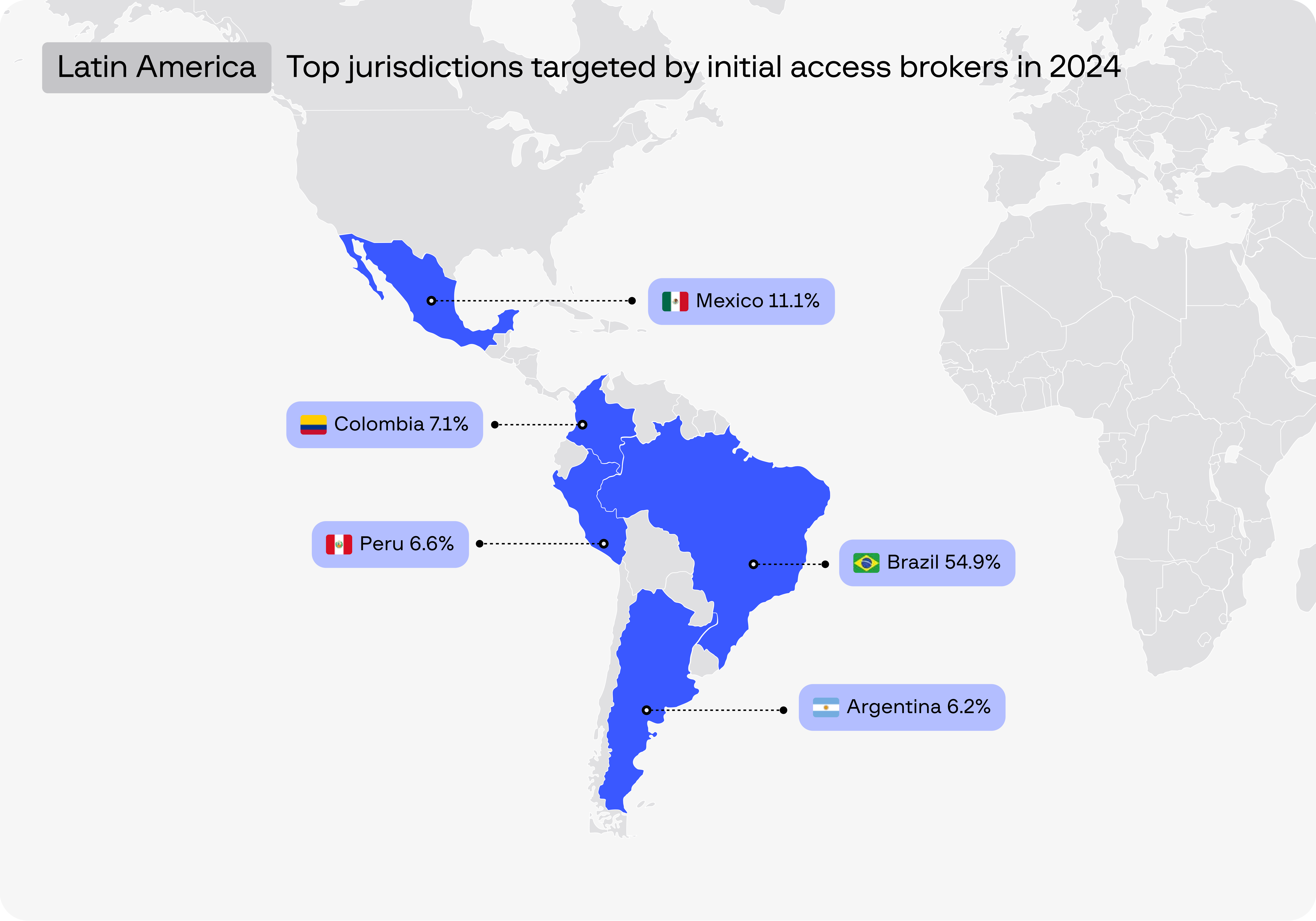
Middle East and Africa Top jurisdictions targeted by initial access brokers in 2024



North America Top jurisdictions targeted by initial access brokers in 2024



Latin America Top jurisdictions targeted by initial access brokers in 2024

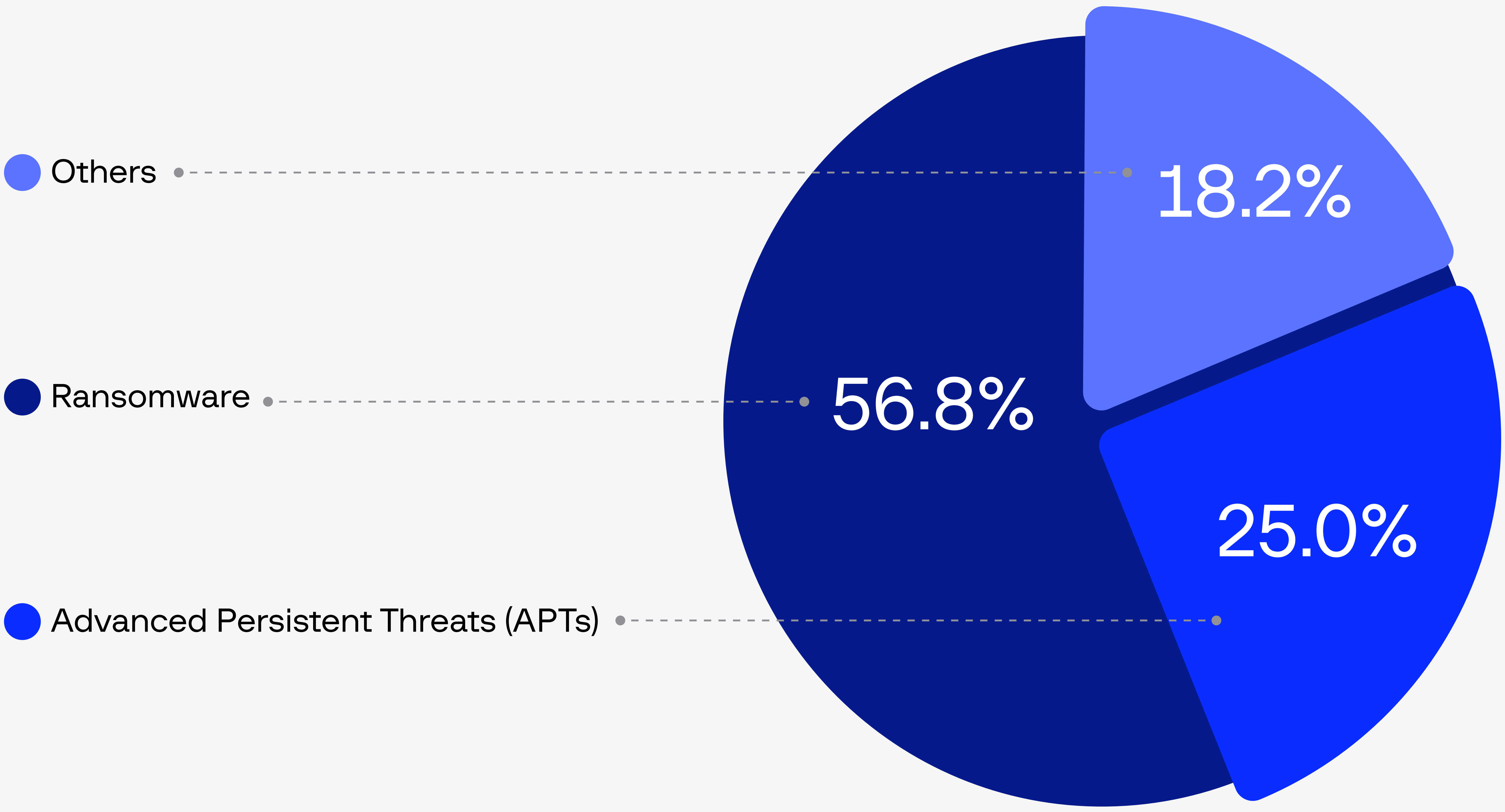


Compromised hosts

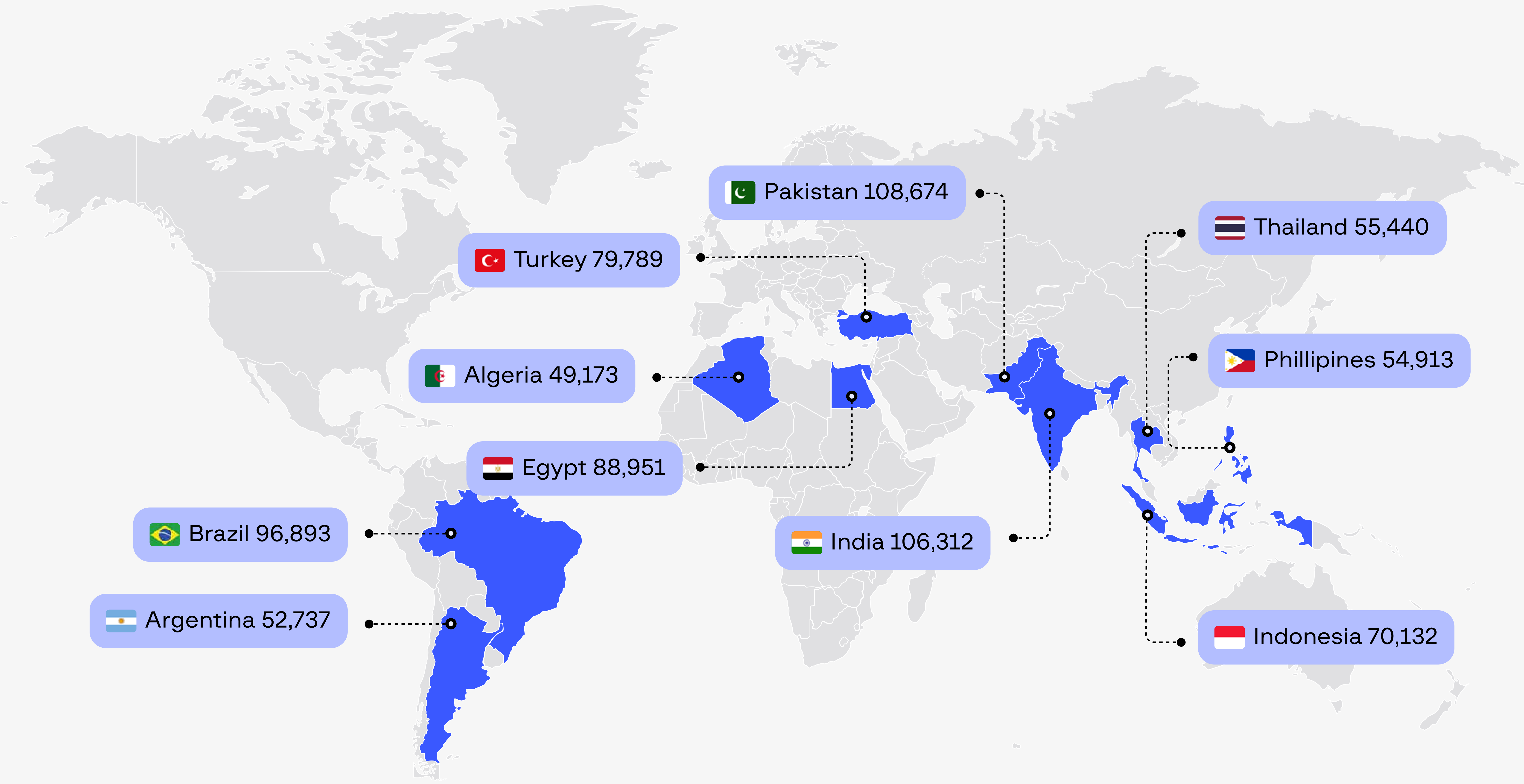
Credentials and sensitive data from compromised devices are often sold on the dark web, serving as initial vectors for ransomware operators, state-sponsored attackers, and other malicious actors. Underground Clouds of Logs (UCL) are a key source of compromised confidential information, primarily acquired through information-stealer malware. These services, often available for a nominal fee or even free, provide less-skilled threat actors with initial access to valuable data without requiring them to employ more complex cybercriminal techniques such as phishing or exploiting public-facing applications.

By utilizing UCL services, cybercriminals can focus on identifying valid accounts for internal services or legitimate credentials to access external remote services, depending on their targeted organization. Hosts infected with information stealers, particularly those involving users with corporate access, can serve as entry points for organized attacks against corporate networks.

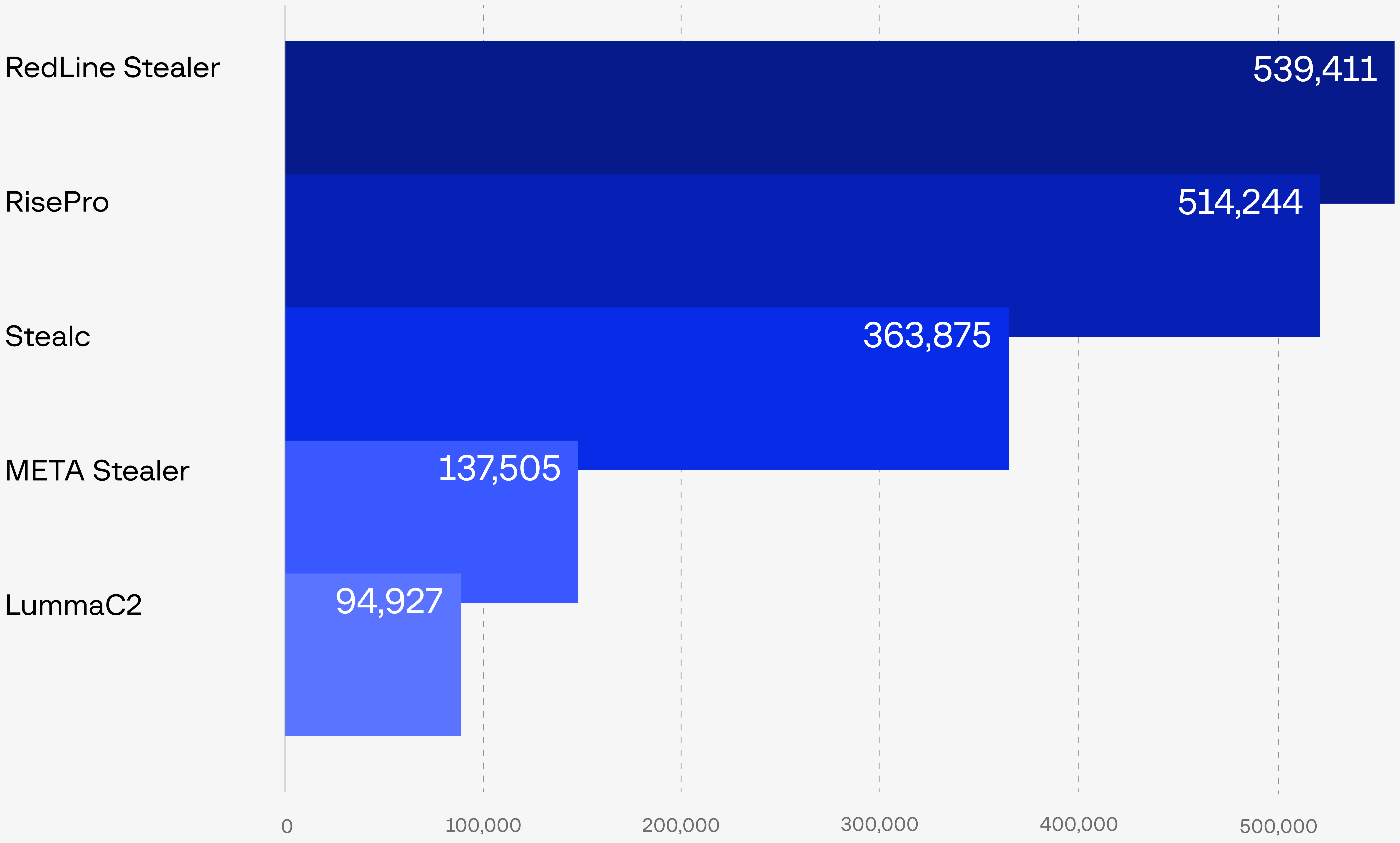
Usage of valid accounts for initial access by threat actor



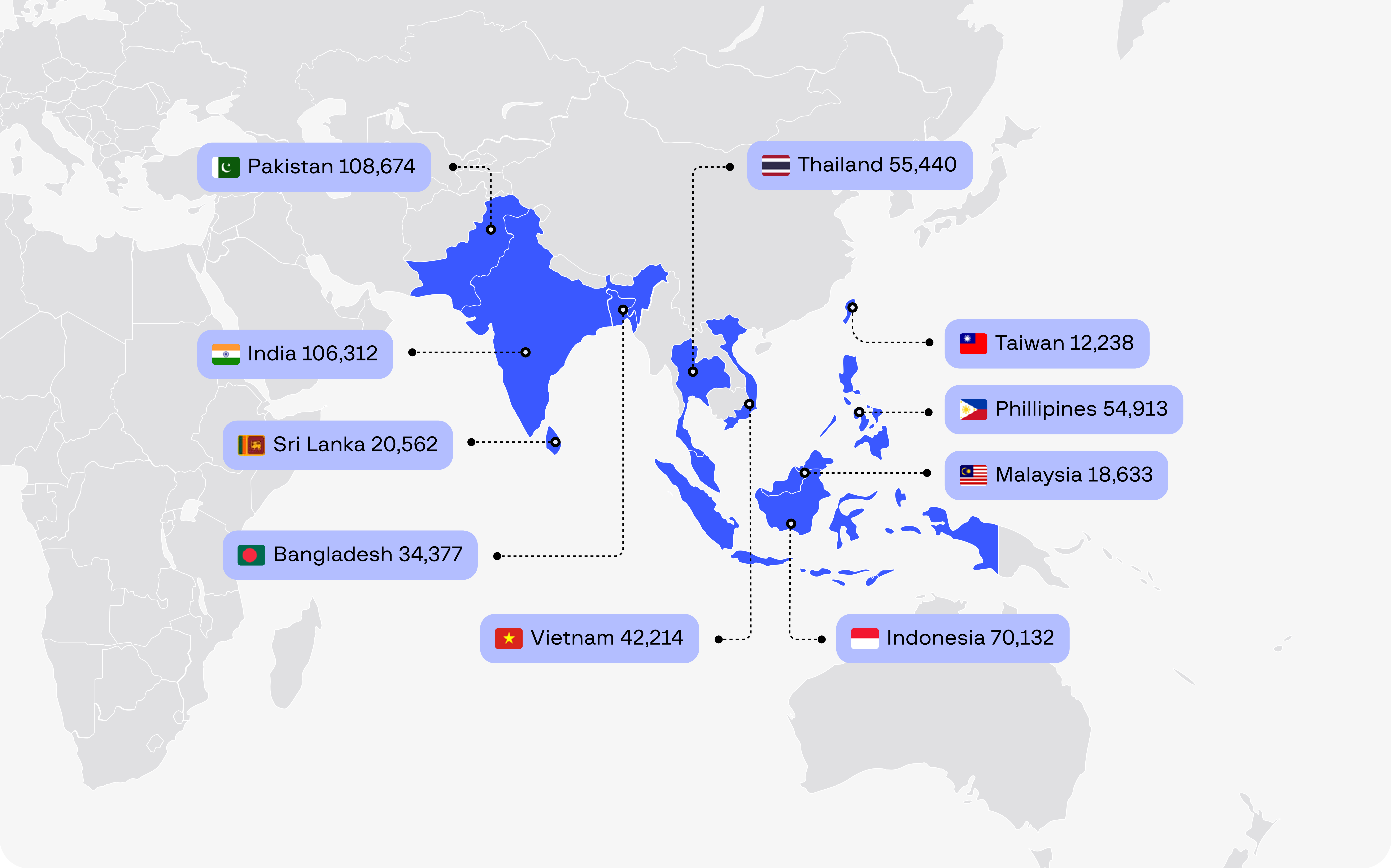
Global Top 10 jurisdictions by number of compromised hosts observed



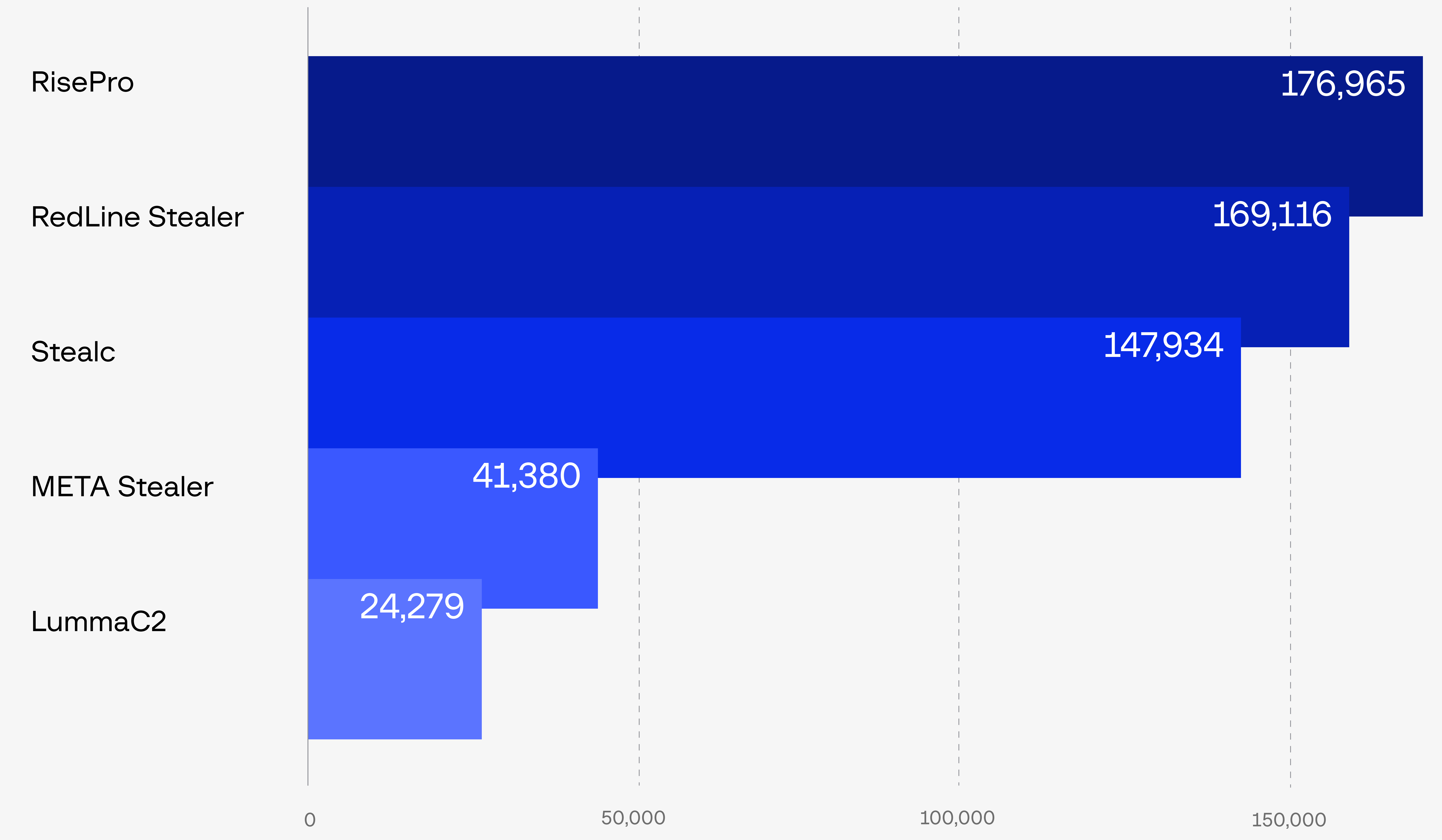
Global Top 5 stealers by number of compromised hosts in 2024



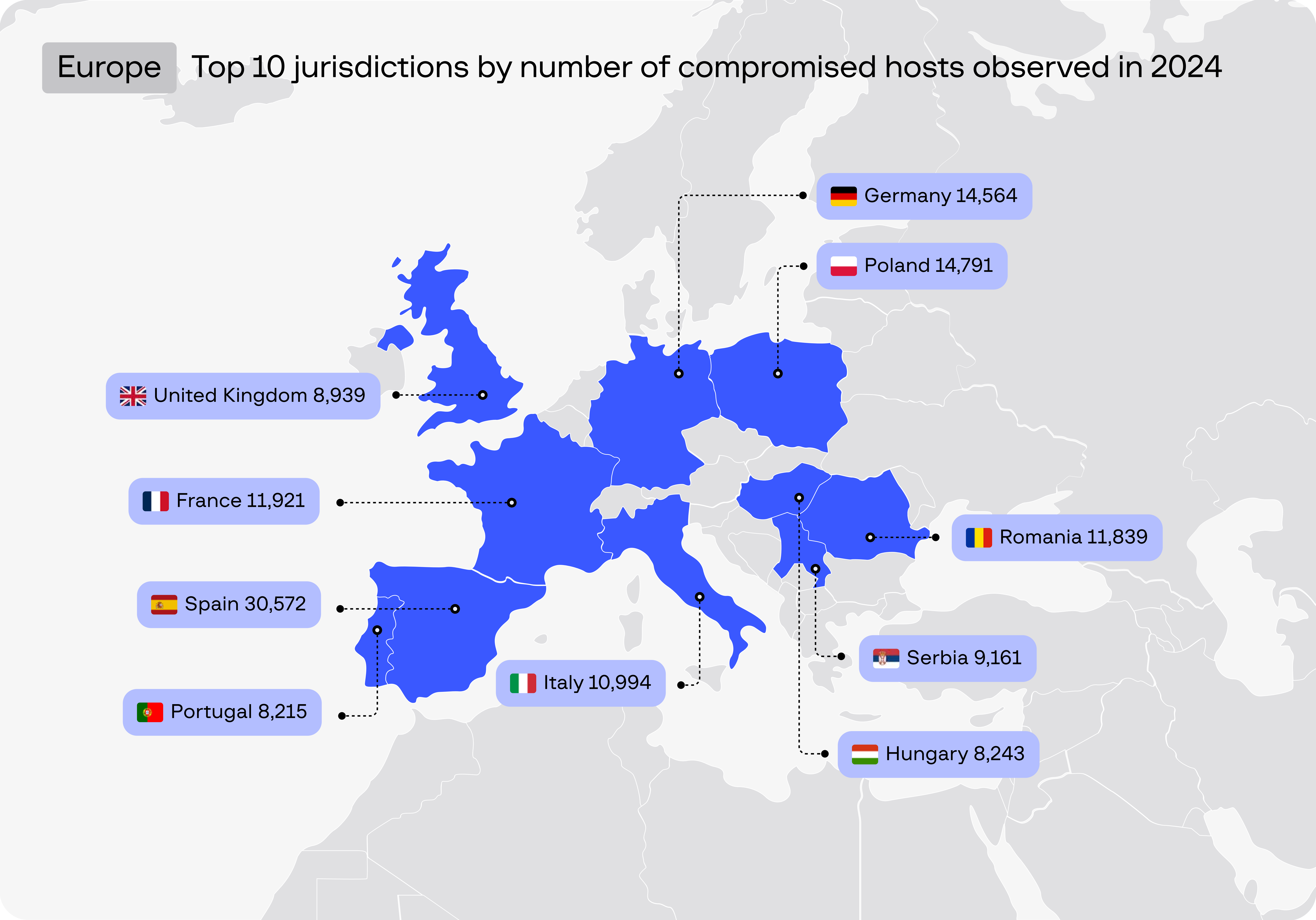
Asia-Pacific Top 10 jurisdictions by number of compromised hosts observed in 2024



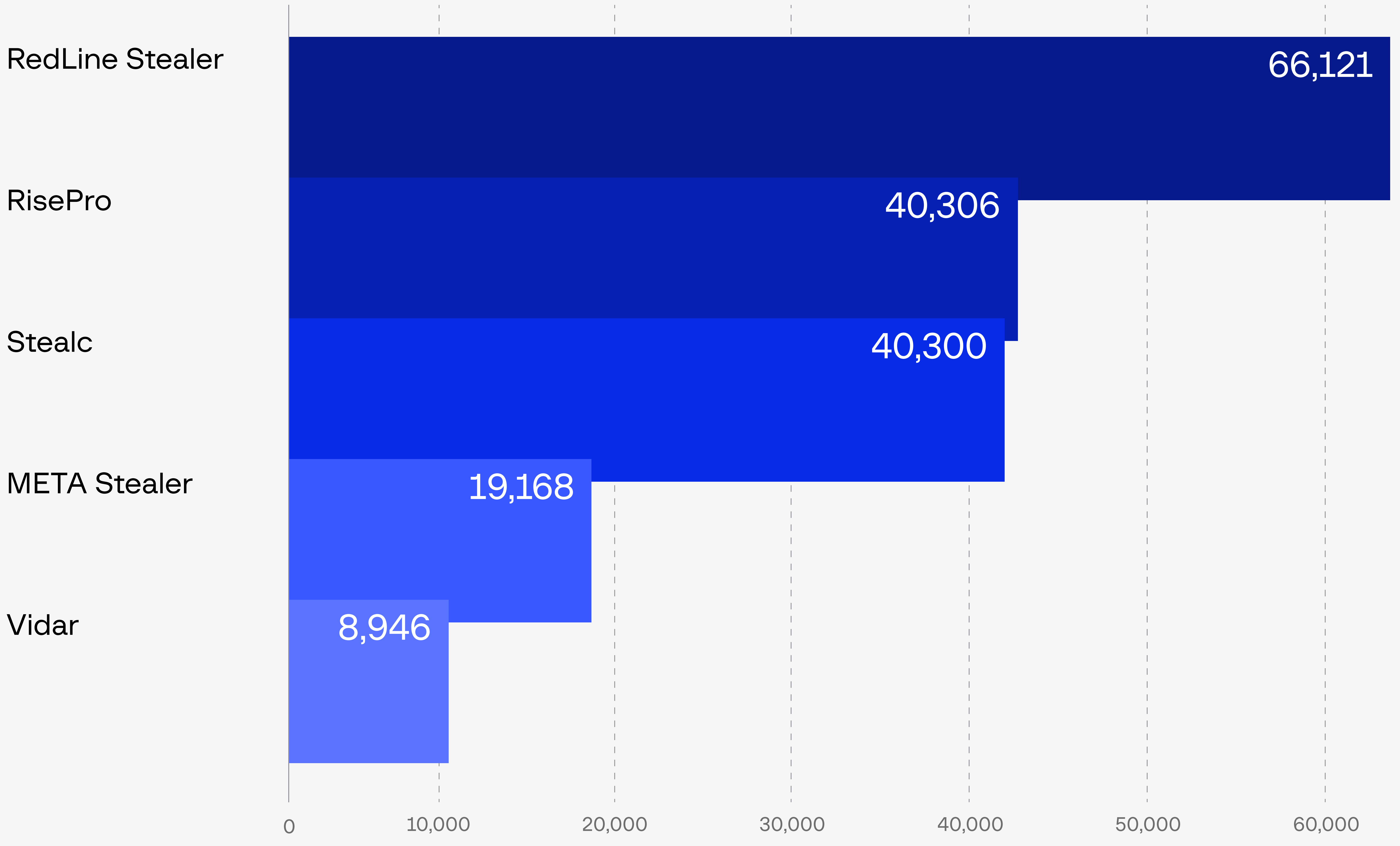
Asia-Pacific Top 5 stealers by number of compromised hosts observed in 2024



Europe Top 10 jurisdictions by number of compromised hosts observed in 2024

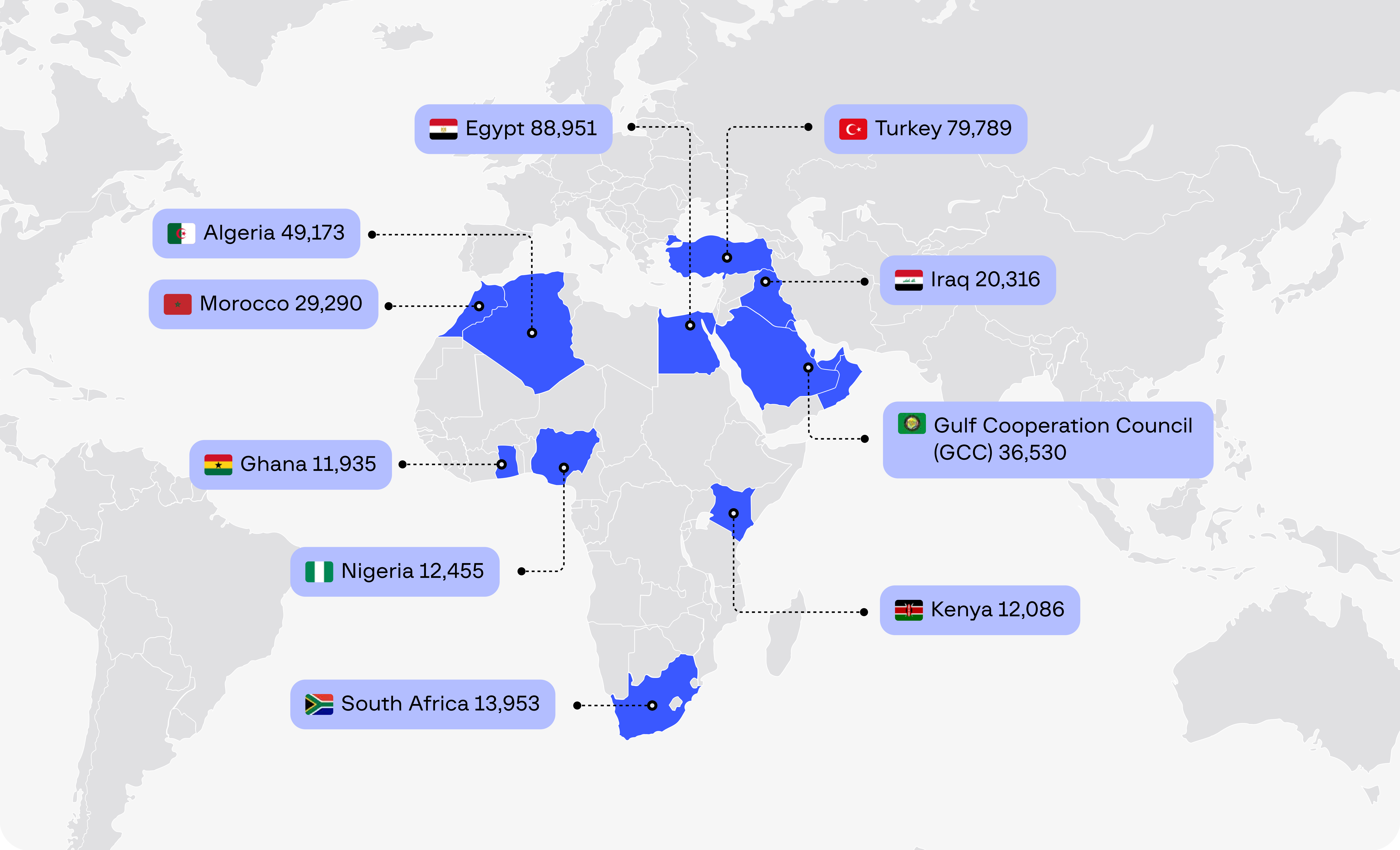


Europe Top 5 stealers by number of compromised hosts observed in 2024



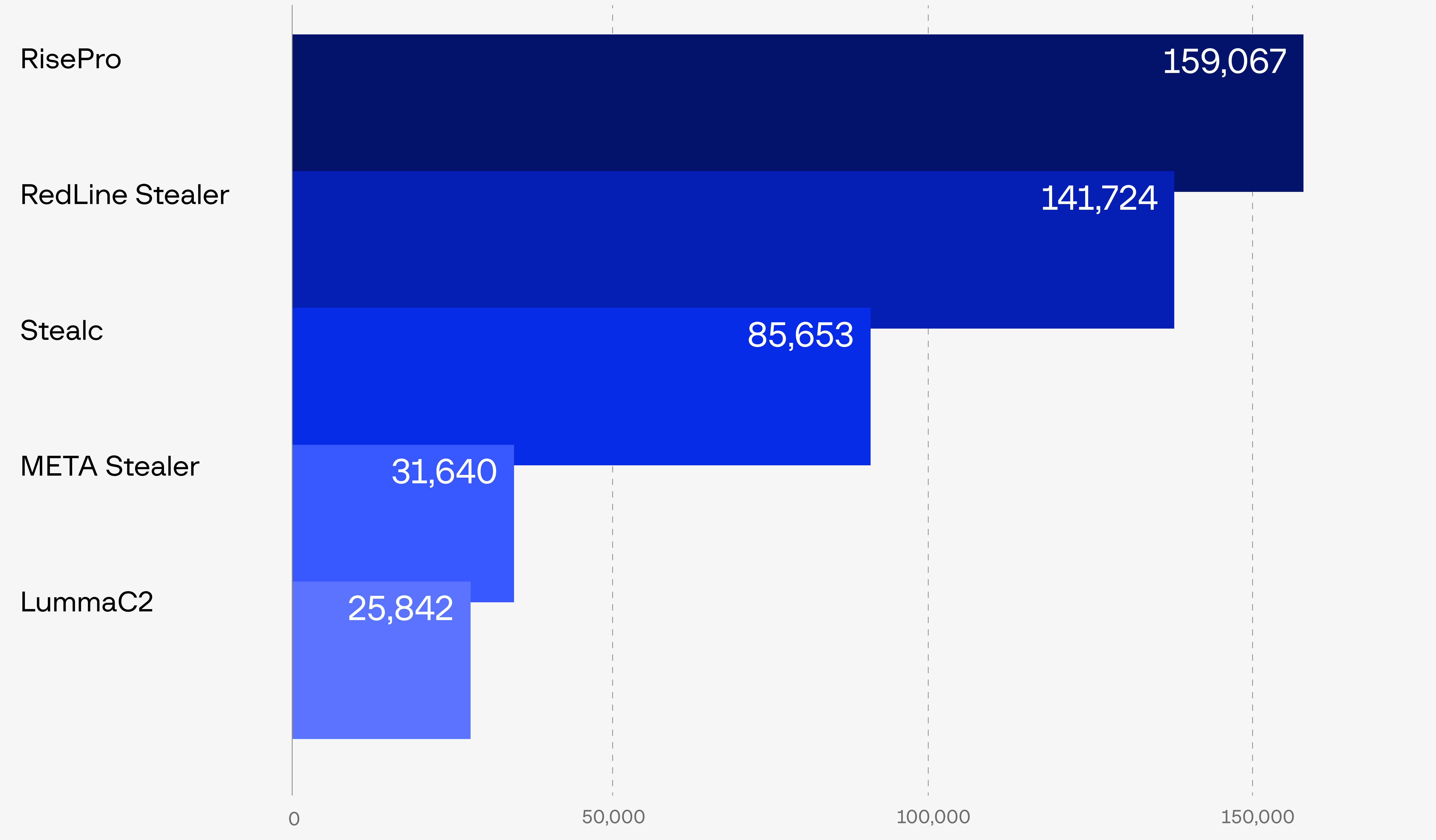
Middle East and Africa

Top 10 jurisdictions by number of compromised hosts observed in 2024

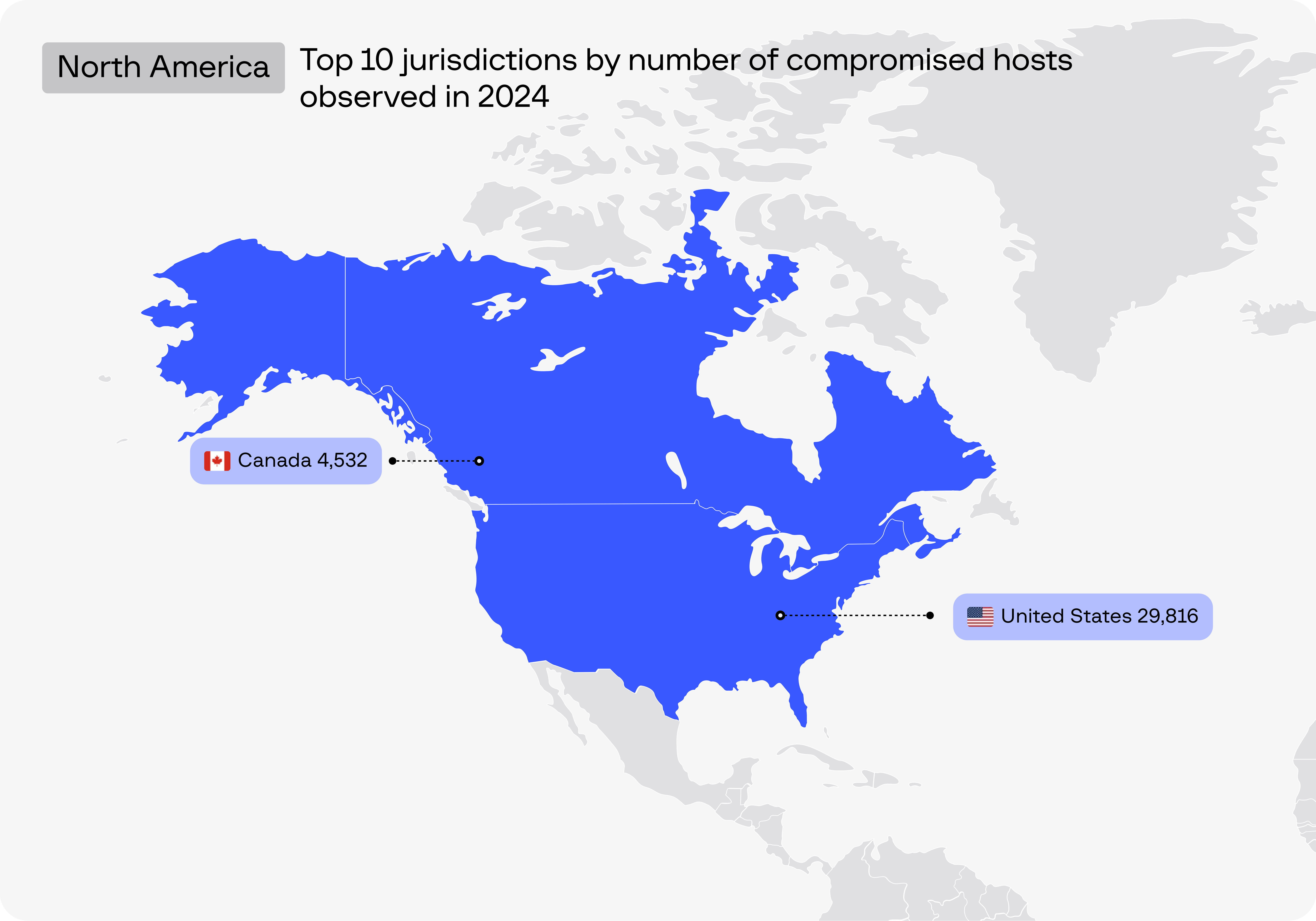


Middle East and Africa

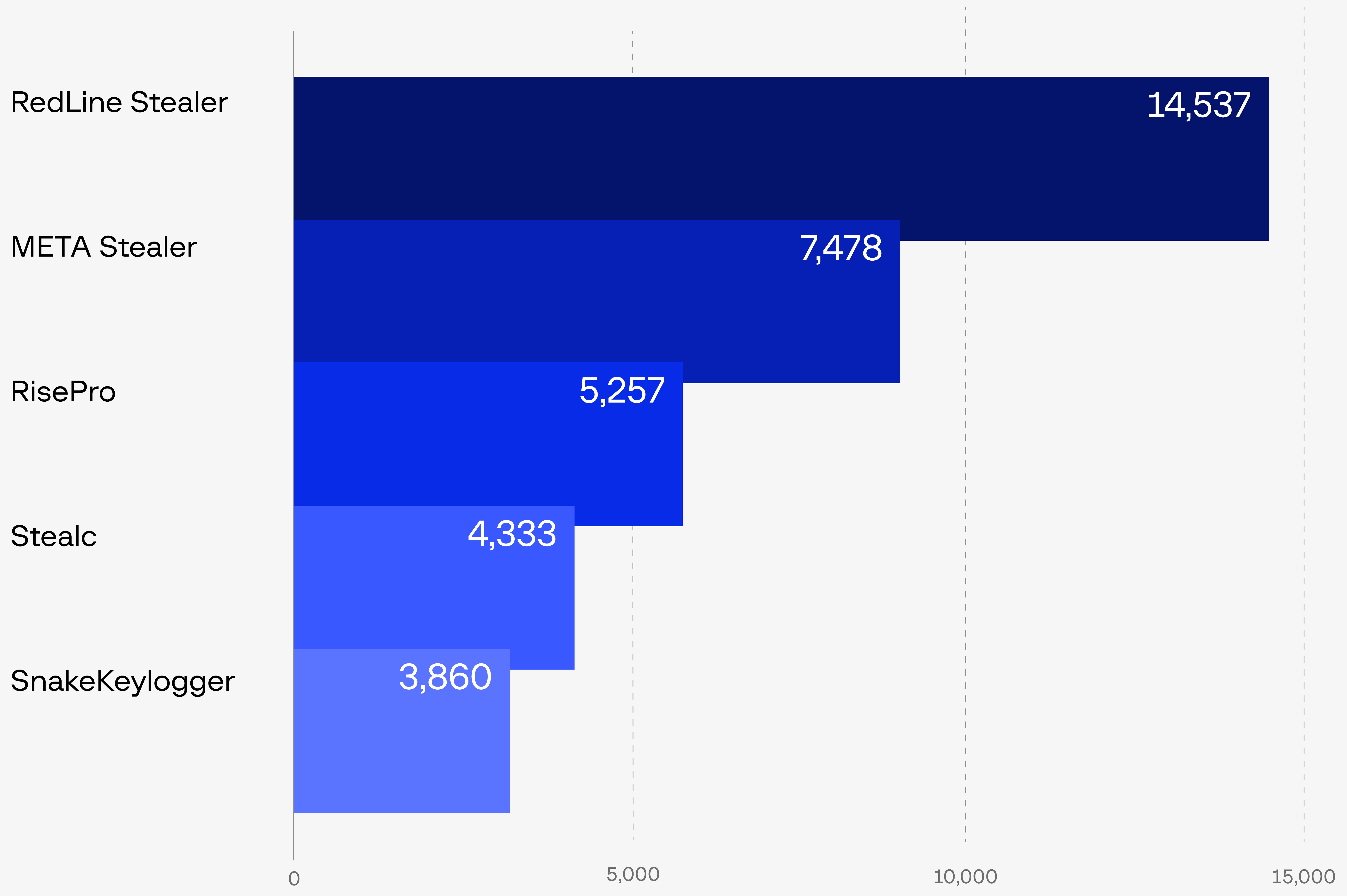
Top 5 stealers by number of compromised hosts observed in 2024



North America Top 10 jurisdictions by number of compromised hosts observed in 2024

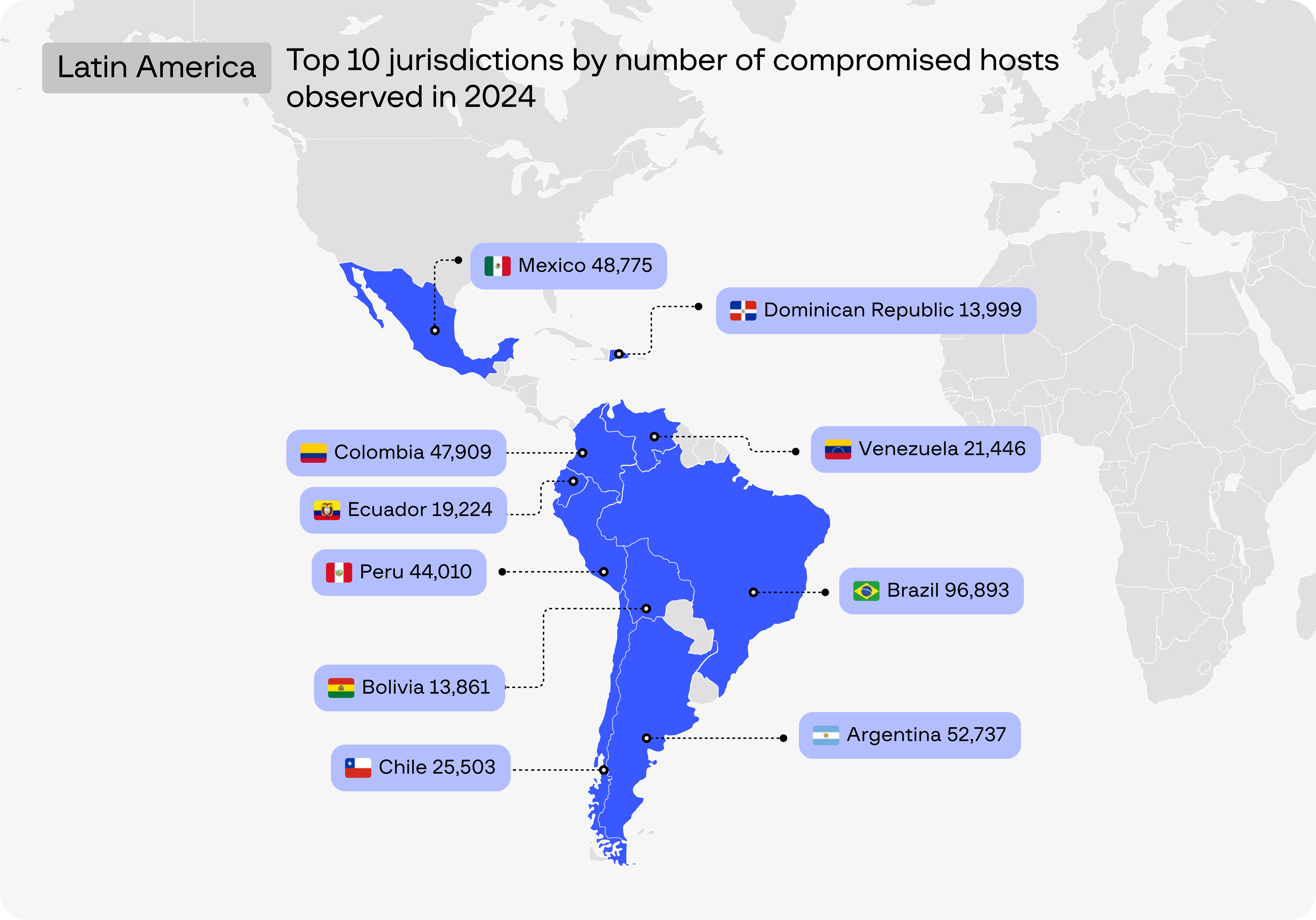


North America Top 5 stealers by number of compromised hosts observed in 2024



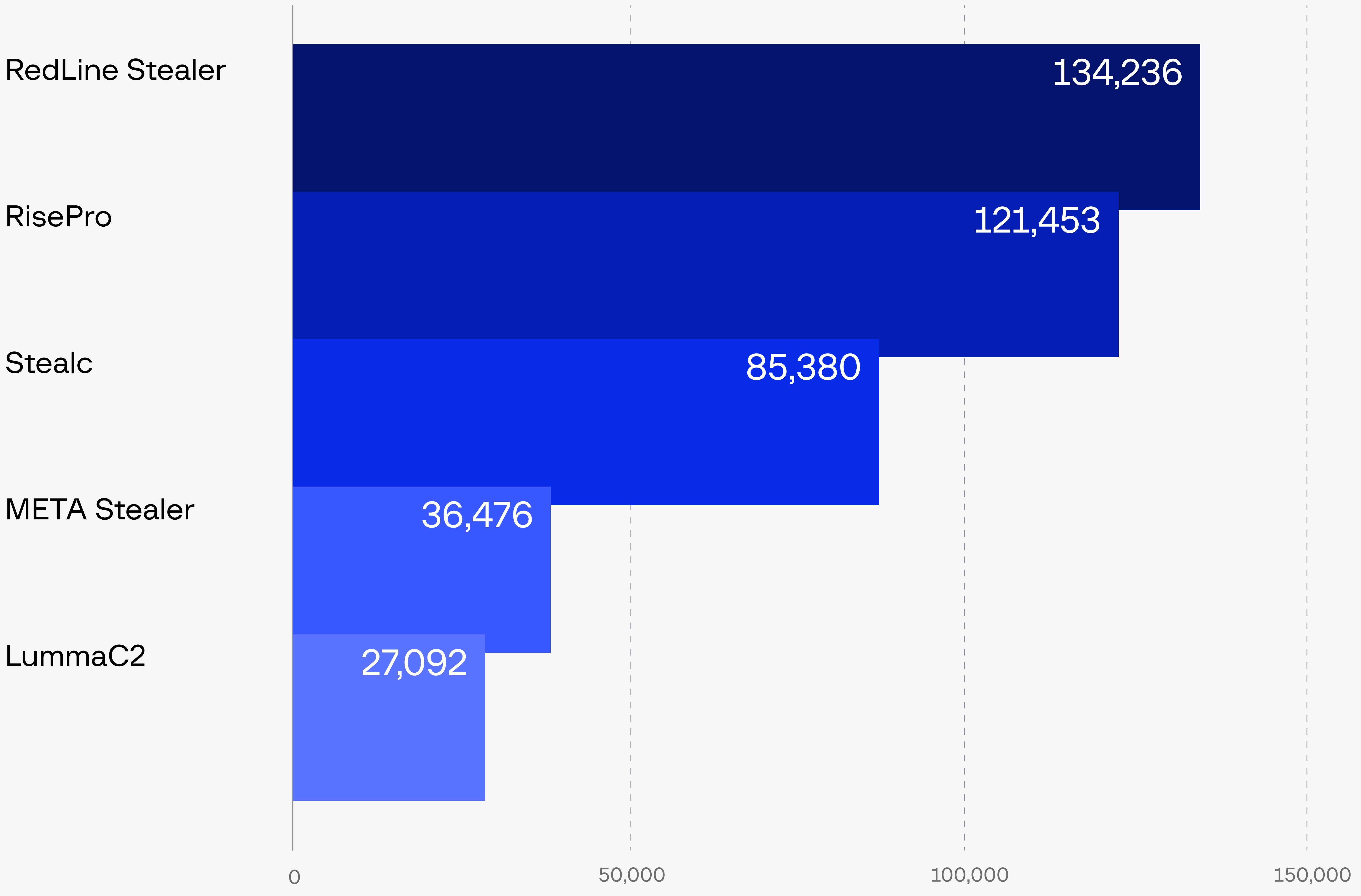
Latin America

Top 10 jurisdictions by number of compromised hosts observed in 2024



Latin America

Top 5 stealers by number of compromised hosts observed in 2024



Top information stealers of 2024

Malware
AI-Driven Threats
Ransomware
Dark Web Dangers
Scam
Fraud
Data Stealers
Phishing
Extortion

RedLine Stealer

Platform
Windows

First seen
2020

ABOUT

Redline Stealer emerged on underground forums in early 2020 and is available for purchase either as a standalone version or through a subscription model. It is designed to extract sensitive information from web browsers, including saved credentials, autocomplete data, and credit card details.
When executed on a target machine, Redline also collects system inventory data, such as the username, location information, hardware specifications, and details about the installed security software.

Recent iterations of Redline have added features that enable the theft of cryptocurrency. Additionally, the malware appears to target FTP and instant messaging clients, with capabilities to upload and download files, execute commands, and periodically transmit data about the compromised system.

TOP TACTICS

- Event Triggered Execution→Screensaver (T1546.002)
- Access Token Manipulation (T1134)
- Process Injection (T1055)
- Virtualization/Sandbox Evasion (T1497)
- System Information Discovery (T1082)

THREAT ACTORS

danon1488 plymouth Tdska
Malsmoke Vasy Grek TA551
Hive LAPSUSS EZCube Royal, Cyclops
Lazarus Sticky Werewolf vn5socks REDGlade
jokeadvert Narketing 163

RisePro

Platform
Windows

First seen
2020

ABOUT

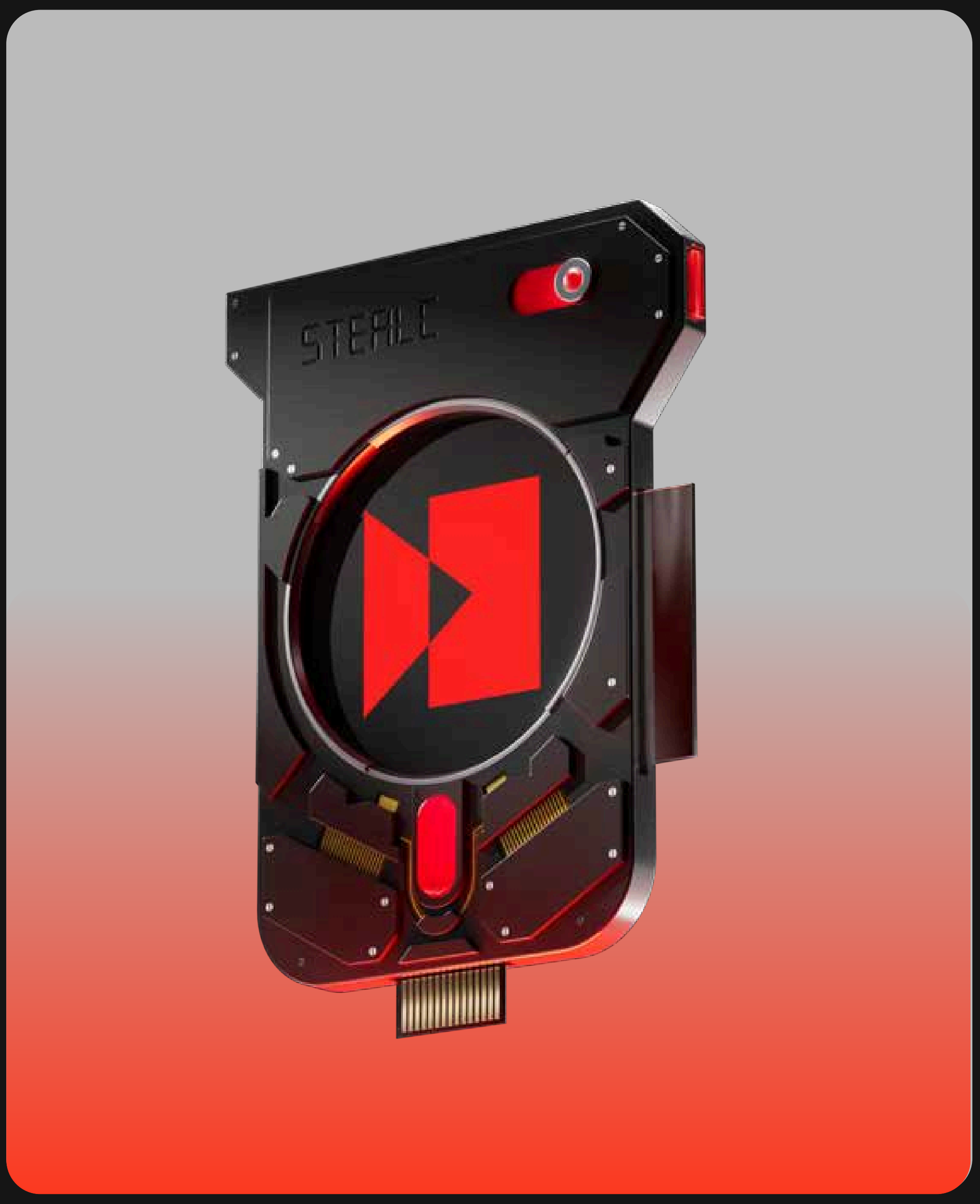
RisePro Stealer malware has been sold as Malware-as-a-Service (MaaS) by the threat actor known as RiseHub since February 2020. The stealer possesses several notable features.
It includes an HVNC module that allows covert, full-system access, enabling cybercriminals to conduct fraudulent activities while bypassing anti-fraud mechanisms. Additionally, Rise ro offers data exfiltration capabilities, collecting data from 45 Chromium-based browsers, 9 Quantum-based browsers, over 200 types of cryptocurrency wallets, and various applications such as FTP, VPN, and gaming platforms.
On February 24, 2024, the builder, command-and-control panel, and server components of RisePro Stealer were compromised and leaked.

TOP TACTICS

- Access Token Manipulation (T1134)
- Impair Defenses→Disable or Modify Tools (T1562.001)
- Obfuscated Files or Information→Software Packing (T1027.002)
- Virtualization/Sandbox Evasion (T1497)
- System Information Discovery (T1082)
- Application Layer Protocol→Web Protocols (T1071.001)

THREAT ACTORS

RiseHub InfectionHub



Stealc

Platform
Windows

First seen
2023

ABOUT

Stealc is an information-stealing malware developed using techniques and structures similar to other stealers such as Vidar, Raccoon, Mars, and RedLine. Attackers leverage stolen accounts to upload YouTube videos that instruct viewers on how to install cracked software for free, while also providing a malicious link.

This link directs victims to a "cracked software catalog" website, where the malicious payload, containing the Steal infostealer, is embedded in a downloadable file. When victims download and extract the archive, they are prompted to execute the "setup.exe" file. Upon execution, Steal establishes communication with its Command and Control (C2) server.

TOP TACTICS

- Access Token Manipulation (T1134)
- Impair Defenses→Disable or Modify Tools (T1562.001)
- Obfuscated Files or Information→Software Packing (T1027.002)
- Virtualization/Sandbox Evasion (T1497)
- System Information Discovery (T1082)
- Application Laver Protocol→Web Protocols (T1071.001)

THREAT ACTORS

- plymouth
- InfectionHub

META stealer

Platform
Windows

First seen
2022

ABOUT

META Stealer is a fork of the notorious Redline Stealer that emerged in March 2022. Unlike its predecessor, META has been modified to specifically target CIS nations, in addition to the standard capabilities of Redline, which is an unusual characteristic for malware within Russian-speaking communities.

This new information-stealing malware quickly gained traction following the discontinuation of Raccoon Stealer. Developed by a Russian-speaking creator, META is actively promoted within those communities.

TOP TACTICS

- Obfuscated Files or Information→Software Packing (T1027.002)
- Virtualization/Sandbox Evasion (T1497)
- System Time Discovery (T1124)
- Application Layer Protocol→Web Protocols (T1071.001)
- Scheduled Task/Job→Scheduled Task (T1053.005)

THREAT ACTORS

- Sticky Werewolf
- _META_
- Vasy Grek
- LuckyBogdan
- ReaverBits

Lumma C2

Platform
Windows

First seen
2022

ABOUT

LummaC2 is a stealer malware written in the C programming language and has been marketed as Malware-as-a-Service on Russian underground forums by the threat actor known as Shamel since December 2022. This malware specifically targets cryptocurrency and two-factor authentication (2FA) extensions, extracting data from both Chromium and Mozilla-based browsers.

It features a built-in File Grabber that operates through low-level system calls, and it is claimed to be capable of stealing data from 60 different cryptocurrency and 2FA browser extensions. All interactions with the operating system are conducted through a low-level wrapper written in assembly language, using only manual syscalls.

The decryption process is handled server-side, meaning all data transmitted by the stealer is decrypted on the server. Additionally, it retains the ability to collect logs in the control panel even after a subscription has ended.

TOP TACTICS

- Indicator Removal (T1070)
- Web Service One→Way Communication (T1102.003)
- Process Injection→Portable Executable Injection (T1055.002)
- Scheduled Task/Job→Scheduled Task (T1053.005)
- Hide Artifacts→Hidden Files and Directories (T1564.001)
- System Binary Proxy Execution (T1218)
- File and Directory Discovery (T1083)
- Unsecured Credentials→Credentials in Registry (T1552.002)

THREAT ACTORS

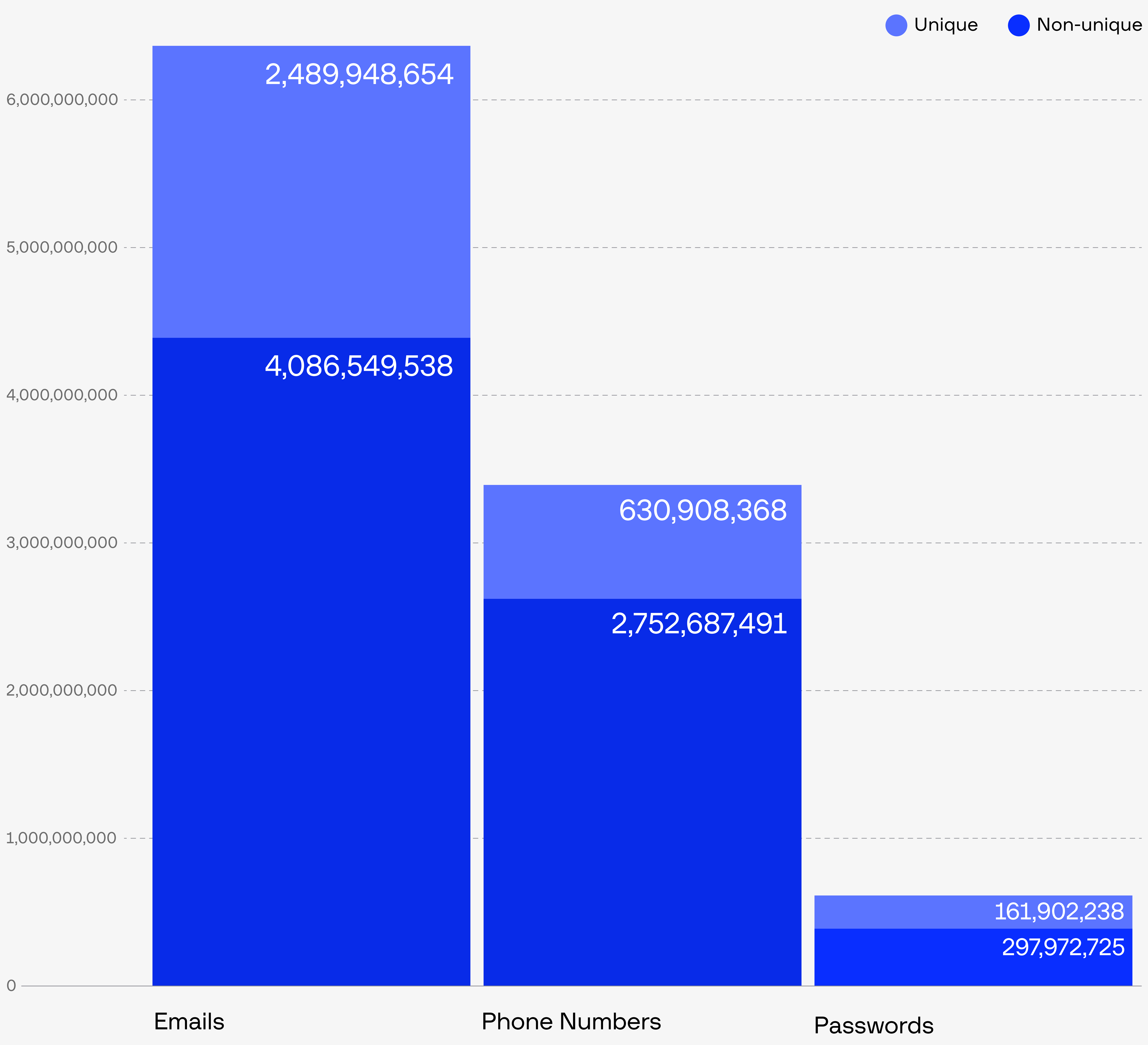
- WDS-Landings
- LuckyBogdan
- CoralRaider
- InfectionHub
- RansomHub
- ClickFix-Anc

Data leaks

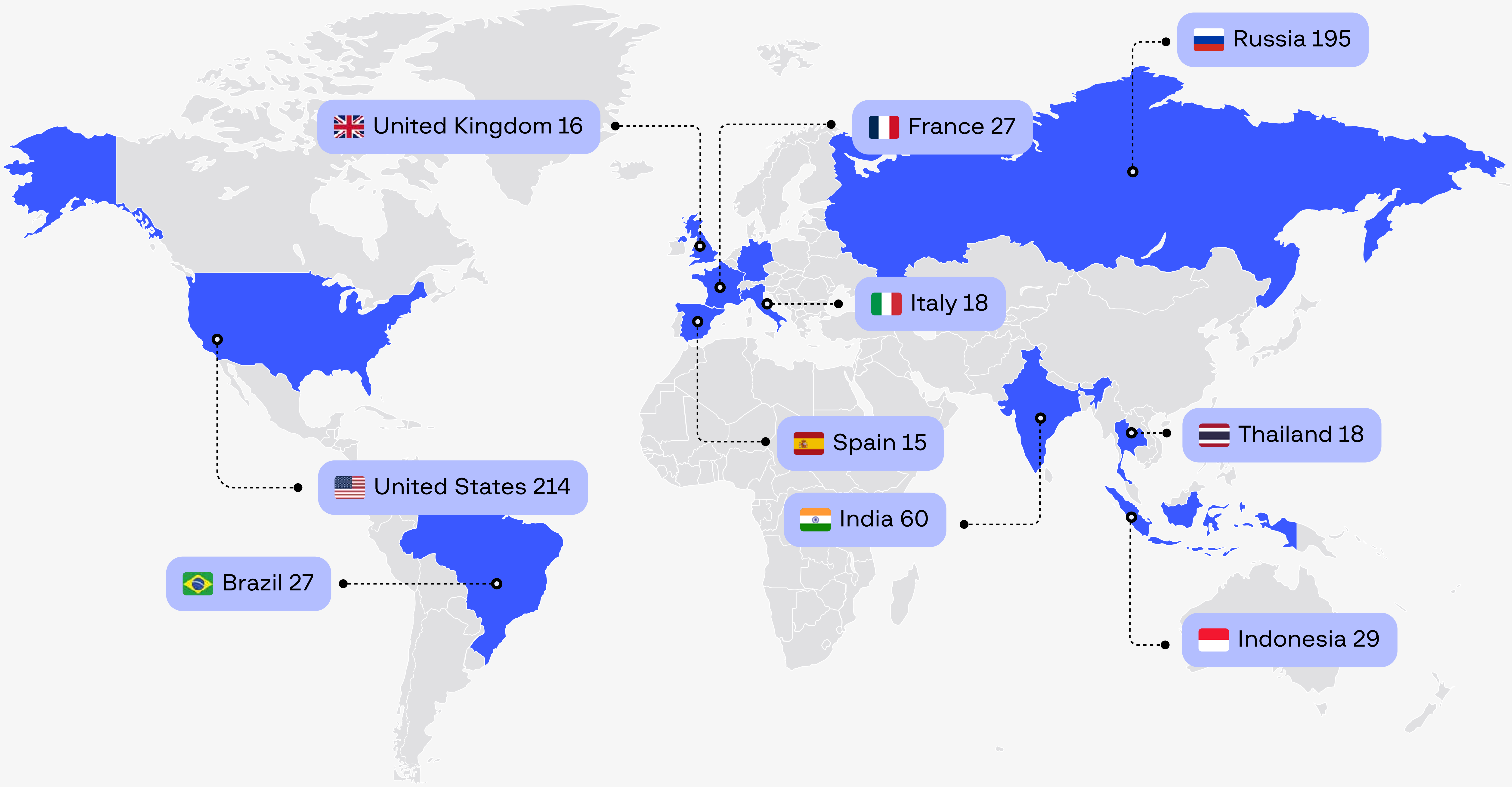
In 2024, 1,107 new instances of data being leaked into the public domain were detected worldwide. These incidents resulted in the compromise of more than 6.4 billion user data strings.

Among the leaked data, email addresses, phone numbers, and passwords pose the highest risk, as they can be exploited by threat actors for various types of attacks. Of all the leaked data, more than 6.5 billion entries contained email addresses, with nearly 2.5 billion being unique. More than 3.3 billion entries contained phone numbers, with nearly 631 million being unique. In total 460-million passwords were leaked, of which 162-million were unique.

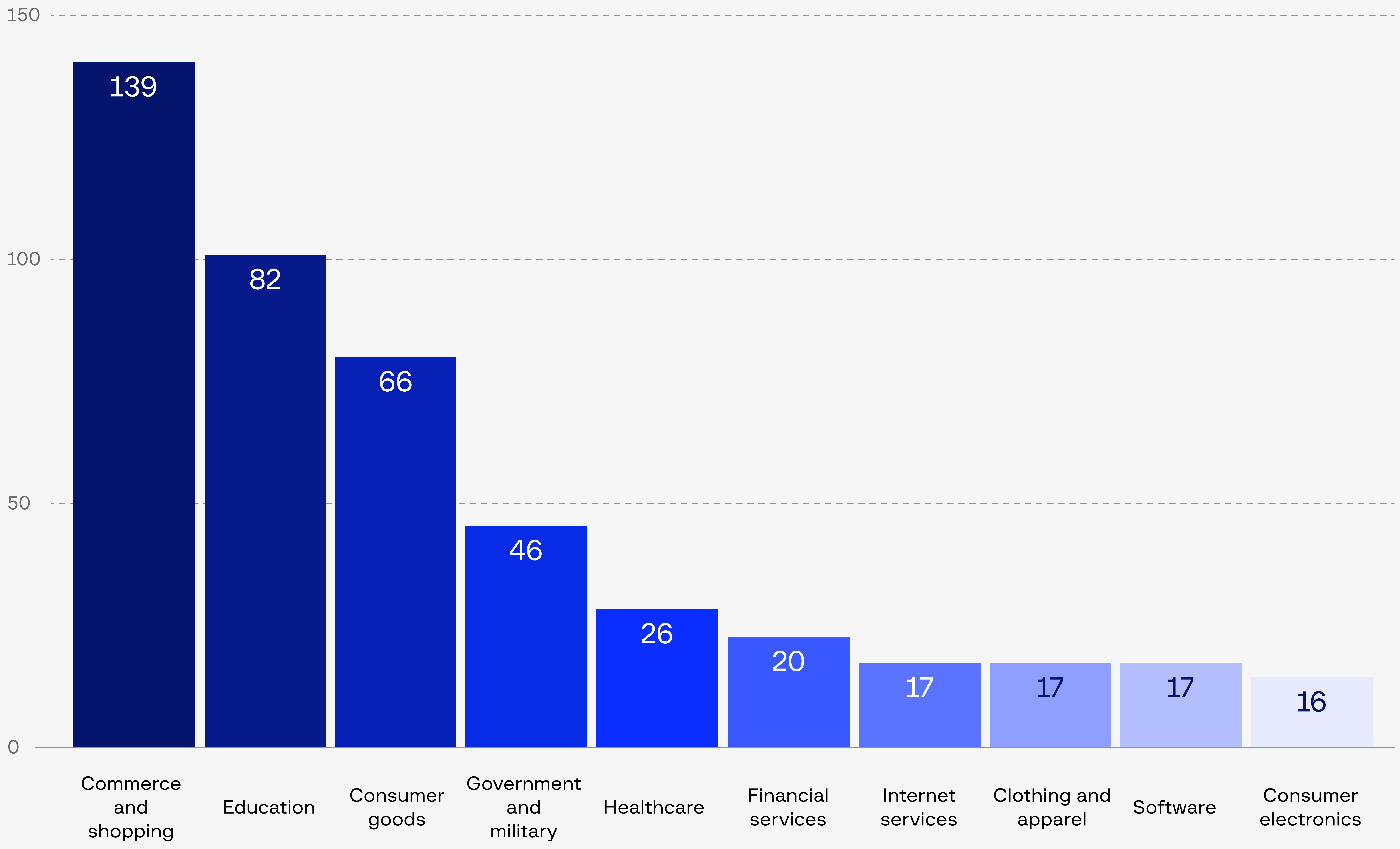
Global Leaks by data type sold on the dark web in 2024



Global Top 10 jurisdictions with reported data leaks in 2024



Global Top 10 Industries impacted by data leaks in 2024



Phishing

Phishing remains one of the most pervasive and damaging cyber threats, with attackers using deceptive emails, fake websites, and fraudulent messages to steal sensitive information. In 2024, Group-IB detected more than 80,000 phishing websites, marking a 22% increase over the previous year.

Over the past year, logistics, travel, and internet services were the top three industries targeted, accounting for 25.3%, 20.4%, and 16.4% of phishing web-sites, respectively.

The logistics industry is particularly vulnerable to phishing attacks due to its reliance on digital communication and the sensitive information exchanged during shipping and delivery processes. Cybercriminals often create fake websites that mimic legitimate logistics companies, enticing victims to enter their personal information or payment details.

The travel sector is another prime target for phishing attacks, especially during peak travel seasons when consumers are actively booking flights and accommodations. Attackers frequently set up fraudulent websites that appear to offer attractive travel deals or booking confirmations.

As reliance on internet services grows, so does the opportunity for cybercriminals to exploit this sector. Phishing websites often impersonate popular online platforms, tricking users into entering their login credentials or personal information.

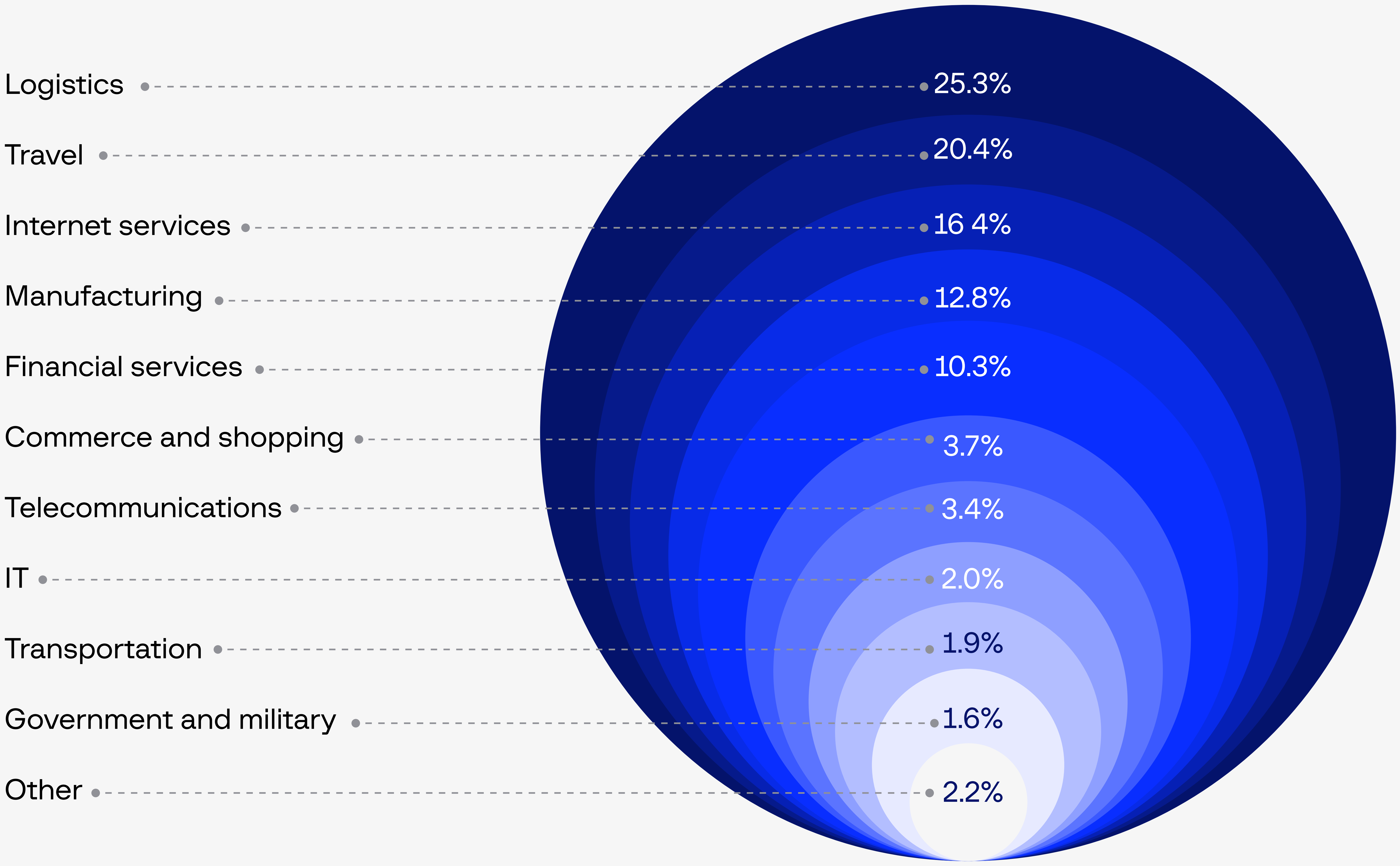
It is essential to note that we calculated only direct phishing attacks. If we included indirect phishing attacks, financial services would rank at the top, as many phishing schemes ultimately lead victims to fraudulent banking sites.

In 2024, the tactics employed by attackers have seen minor changes. The availability of deepfake technology and the proliferation of related services have enabled individuals with limited technical skills to create high-quality deepfakes using just a small voice sample or a single photograph.

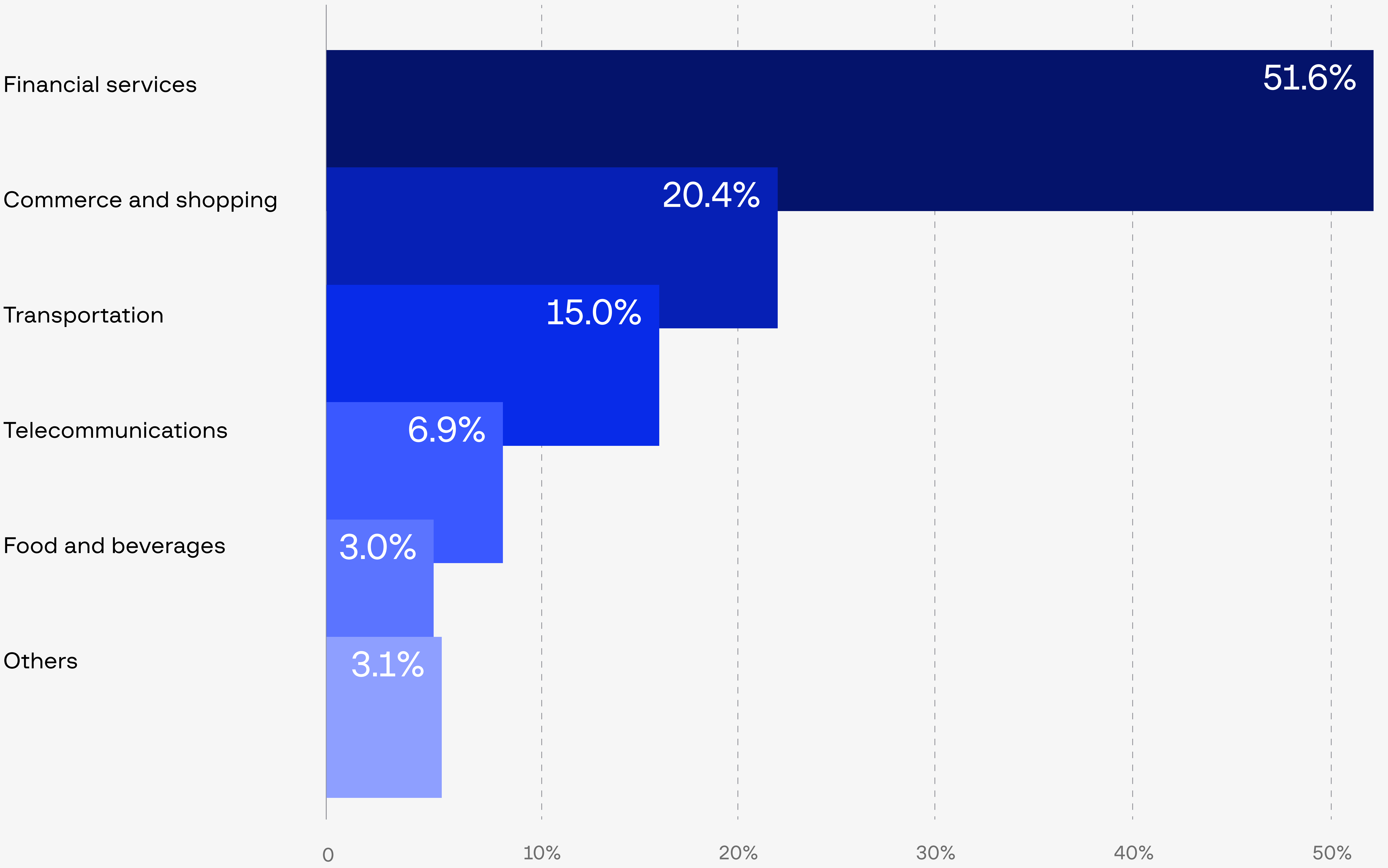
Moreover, many attackers use services for automated generation of deepfakes, with specialized bots available on platforms like Telegram that facilitate the creation of fake audio or video for a fee. It is possible to simply select a celebrity and a text overlay, which is then voiced by a fake celebrity. Subscription prices for these services vary, with the average cost for a one-day subscription around $13.

Criminals also have increasingly focused on techniques to evade detection. A growing number of attackers are honing their efforts to target specific user groups, thereby restricting access to phishing pages for users not included in the attack. User validity is assessed through methods such as HTTP referer checks, IP range restrictions (which can be limited to specific providers), and the verification of user data (email, phone number, ID number) at the initial stage. This information is then compared against an existing victim database before redirecting users to the phishing form. Additionally, attackers are implementing measures to hinder manual site analysis, including prohibiting code viewing and detecting the use of Developer Tools.

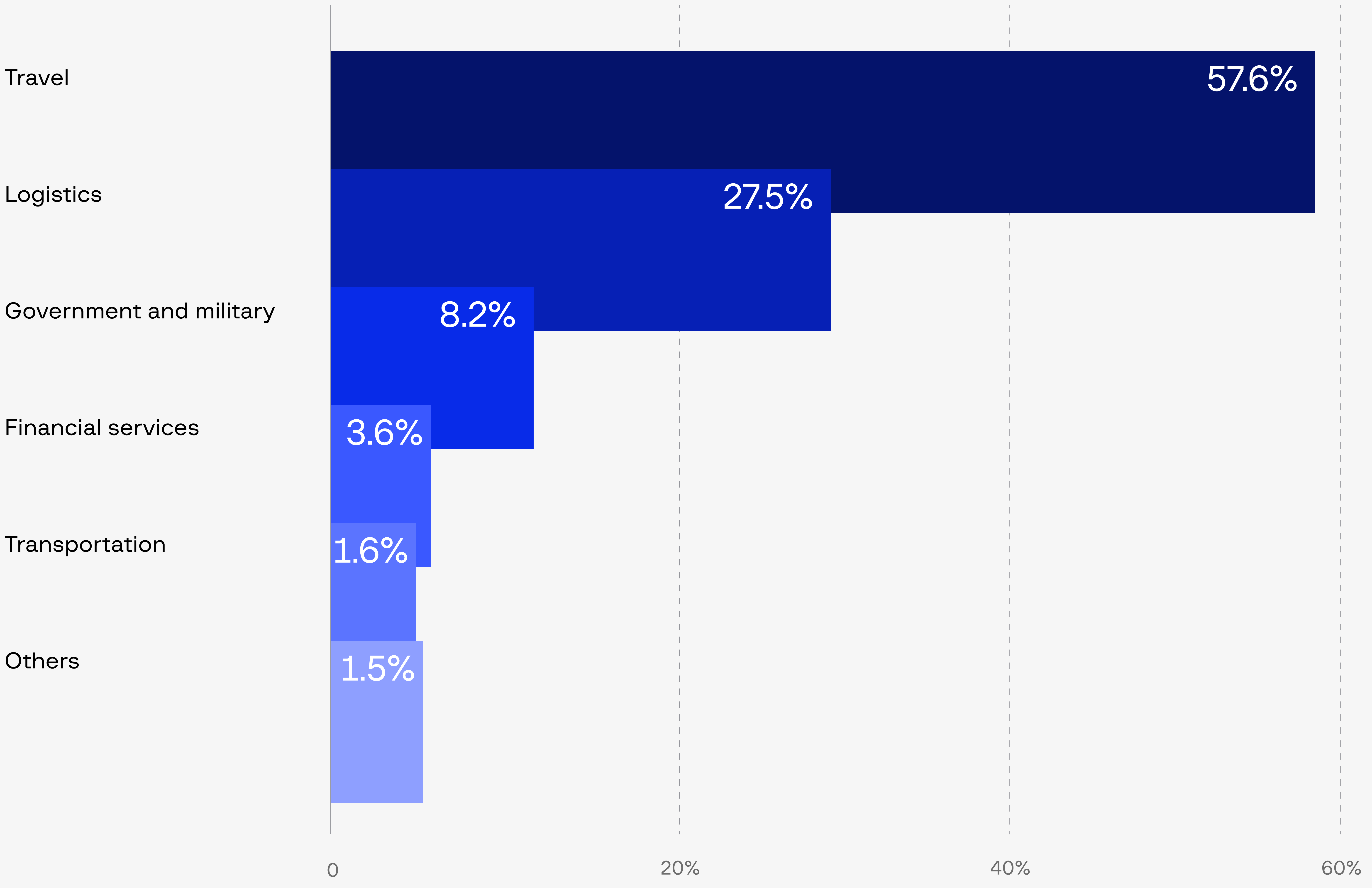
Global Top 10 industries targeted by phishing attacks in 2024



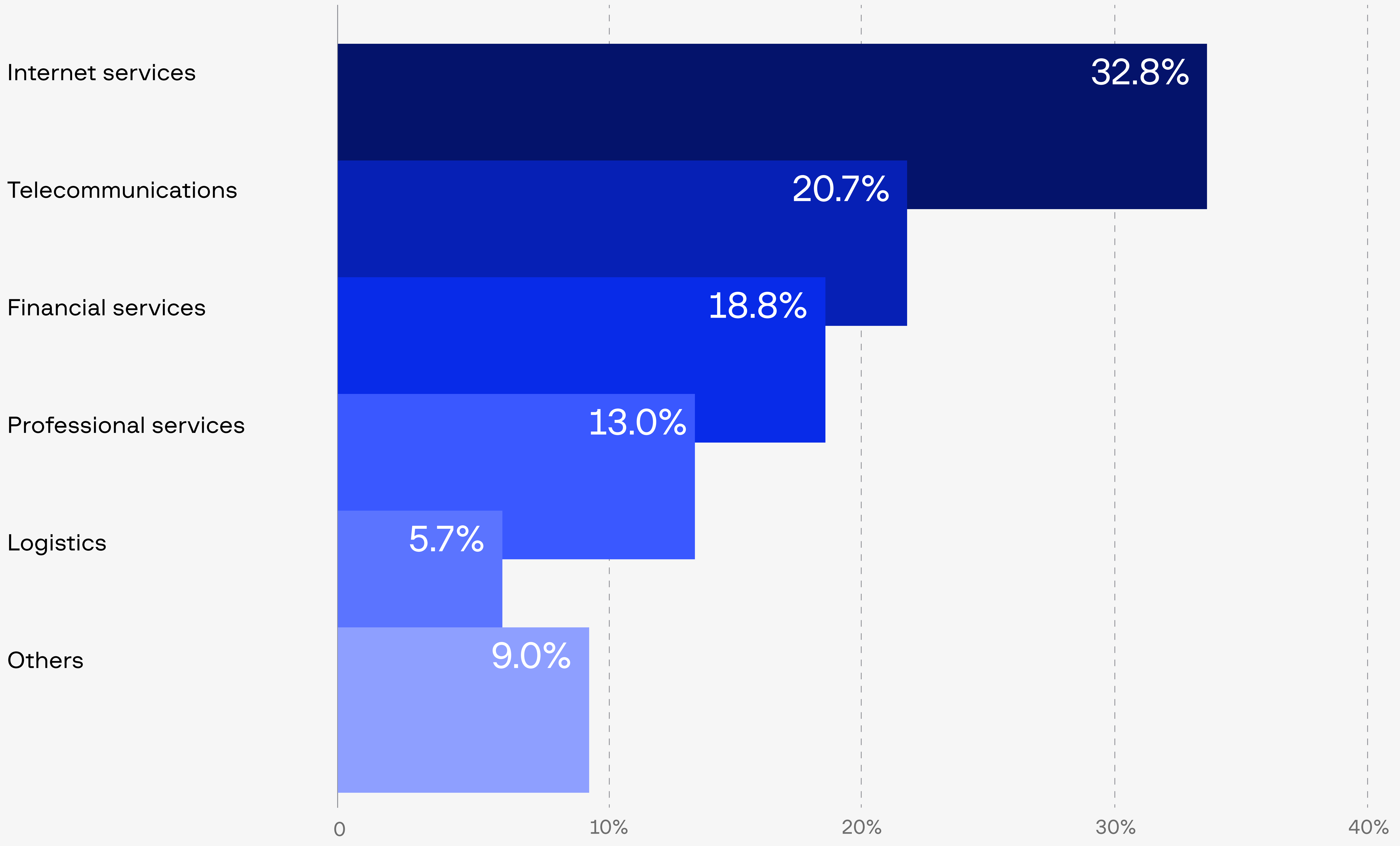
Asia-Pacific Top industries targeted by phishing attacks in 2024



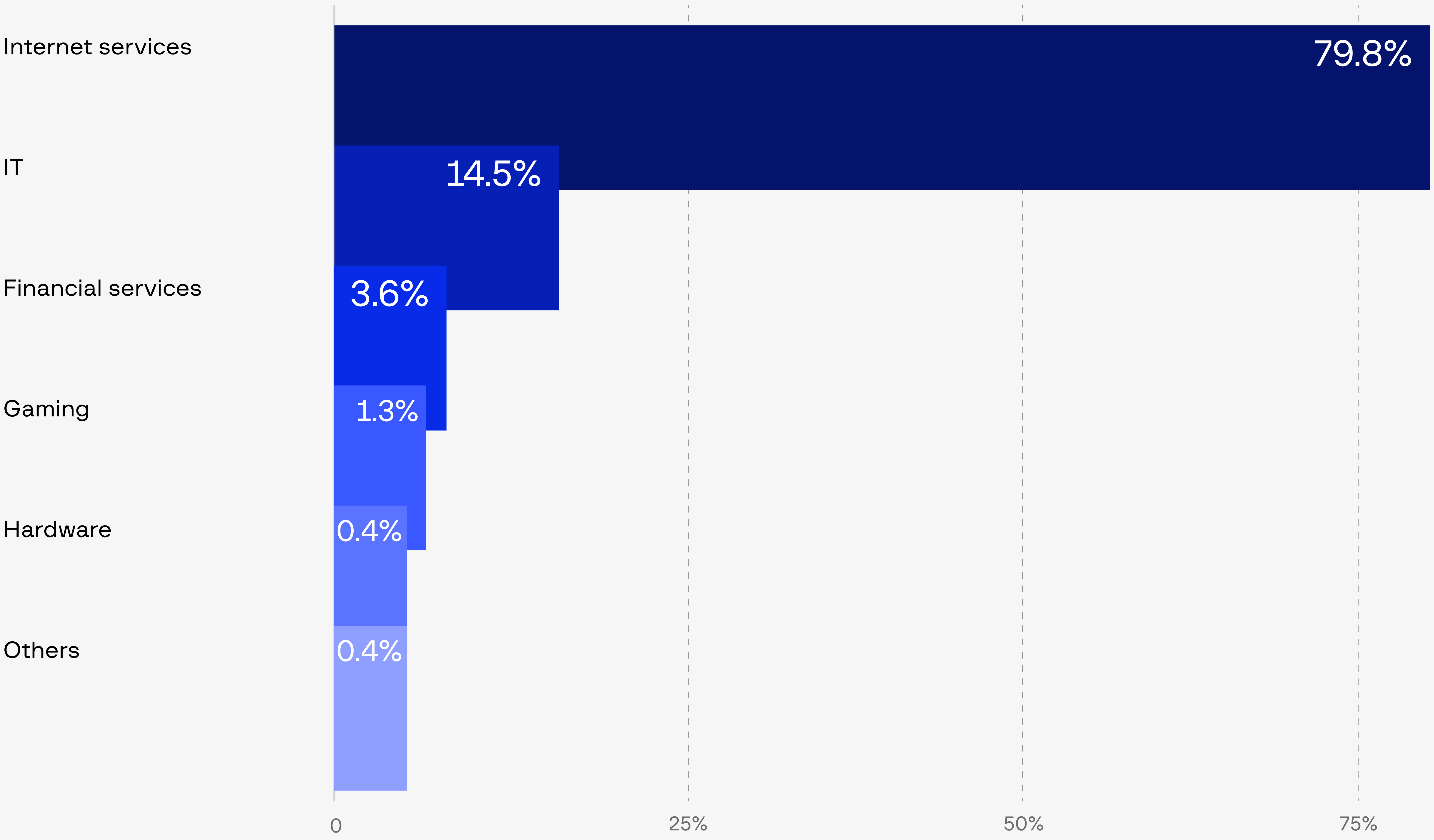
Europe Top industries targeted by phishing attacks in 2024



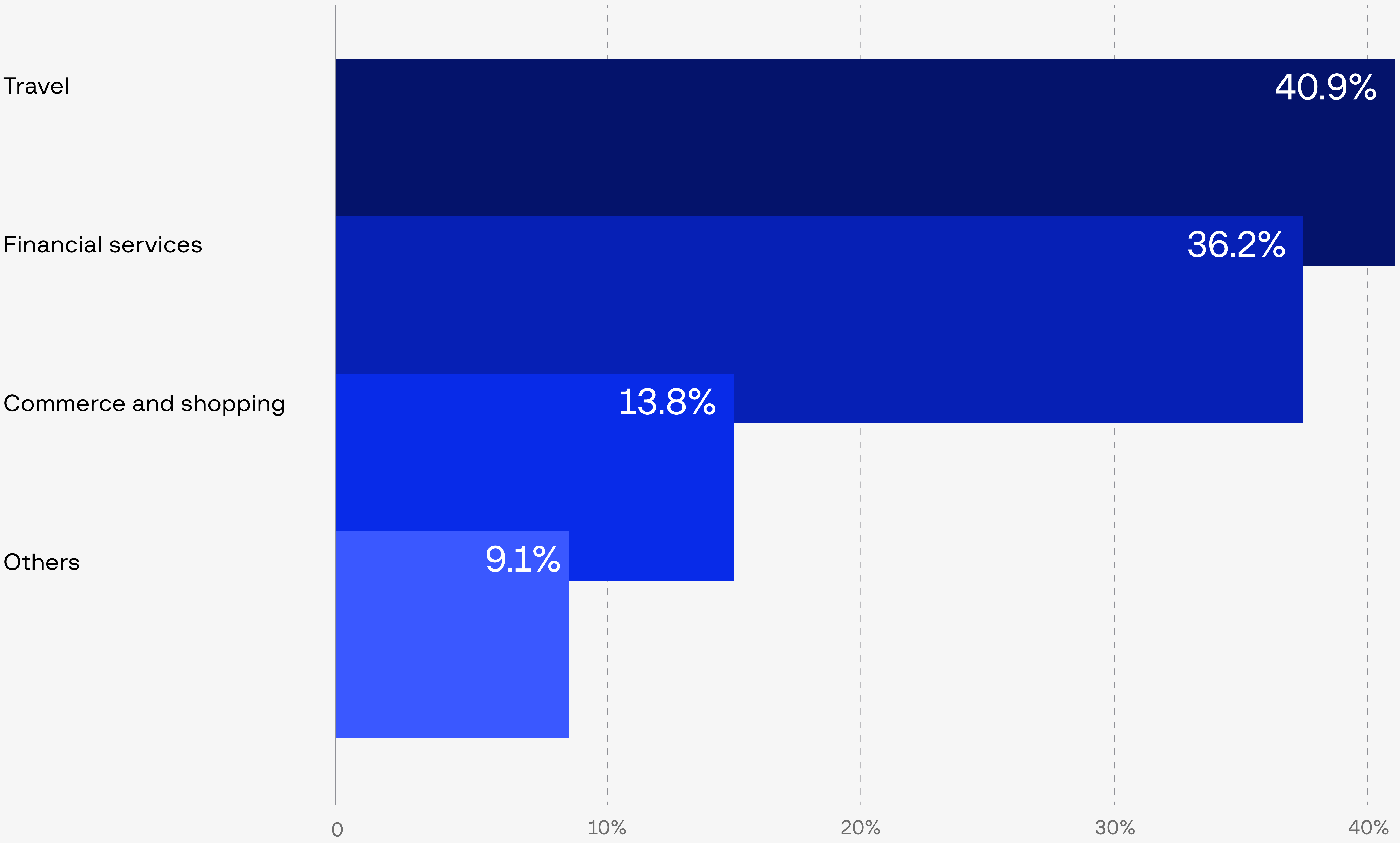
Middle East and Africa Top industries targeted by phishing attacks in 2024



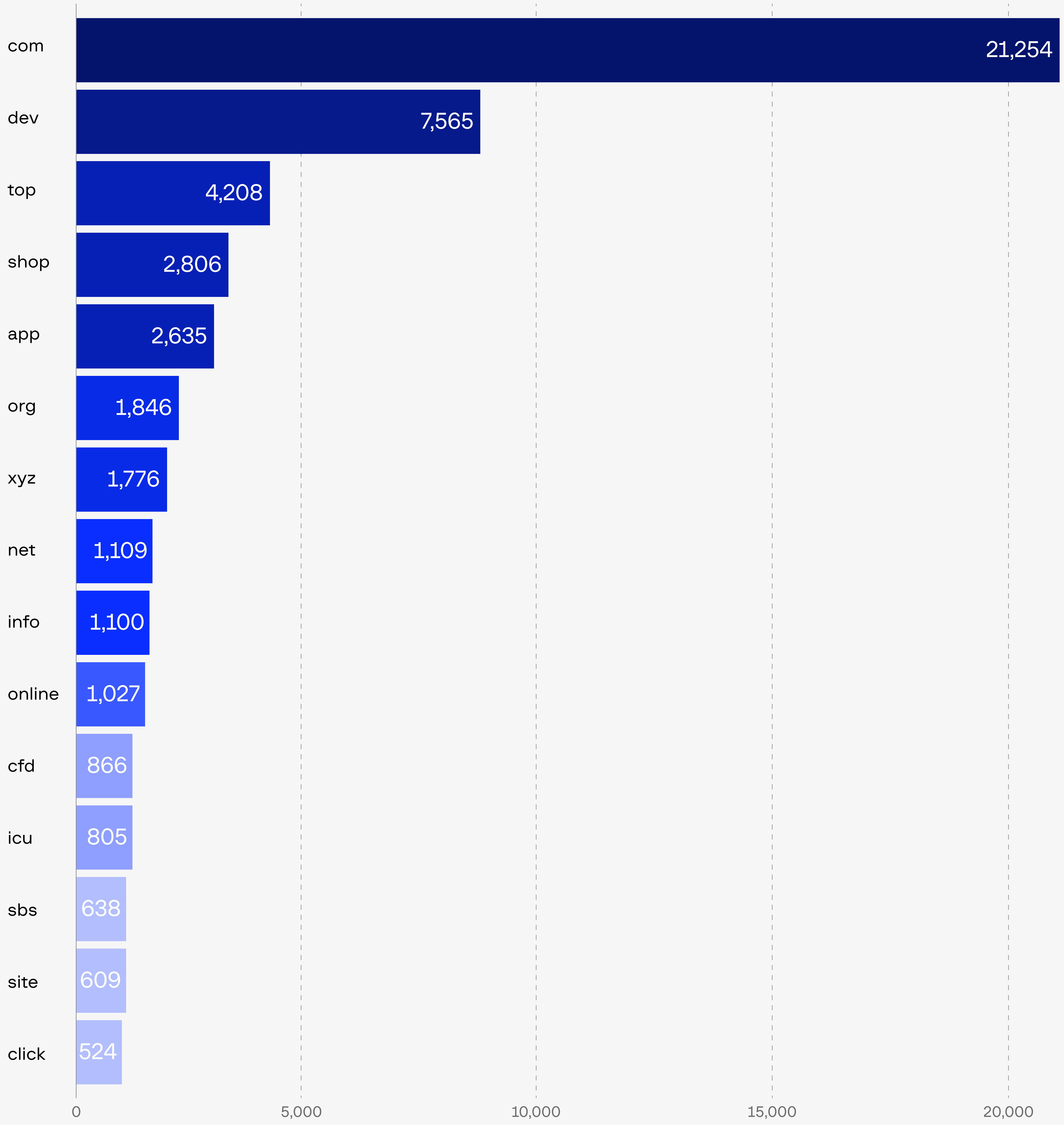
North America Top industries targeted by phishing attacks in 2024



Latin America Top industries targeted by phishing attacks in 2024



Global Top generic TLDs for phishing resources



Statistics for 2024 indicate that the .com Top Level Domain (TLD) remains the most commonly used domain for phishing attacks. Historically, it has been the most recognized and widely utilized TLD, which gives phishing sites a deceptive appearance of legitimacy. Users are accustomed to .com addresses, making them less suspicious and more likely to trust these sites. This familiarity significantly increases the likelihood of victims falling for phishing attempts.

Scams

Scams rely on exploiting the emotions and urgency of its victims in order to steal personal or financial information, often impersonating the name and likeness of popular legitimate brands in order to deceive their targets. Common examples of fraudulent resources include:

Investment scams

Fraudsters promise high returns on investments in fake cryptocurrency or stock opportunities.

Romance scams

Scammers create fake profiles on dating sites to build emotional connections and solicit money.

Delivery scams

Scammers impersonate legitimate delivery companies to trick victims into providing personal information or payment for nonexistent packages

Tech support scams

Scammers pose as technical support representatives to gain access to victims' computers and personal data.

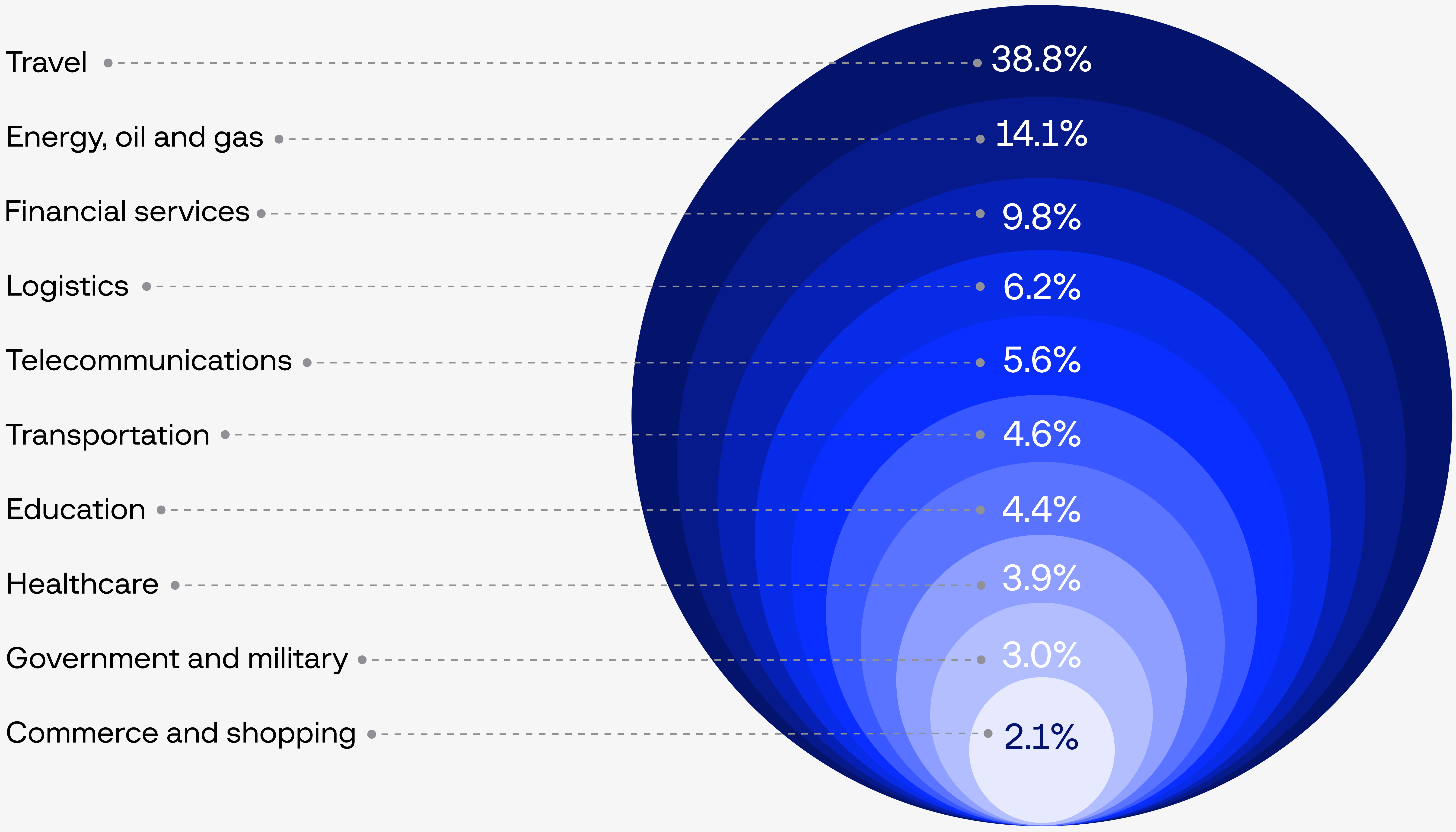
Lottery or prize scams

Victims are informed they've won a prize but must pay fees to claim it.

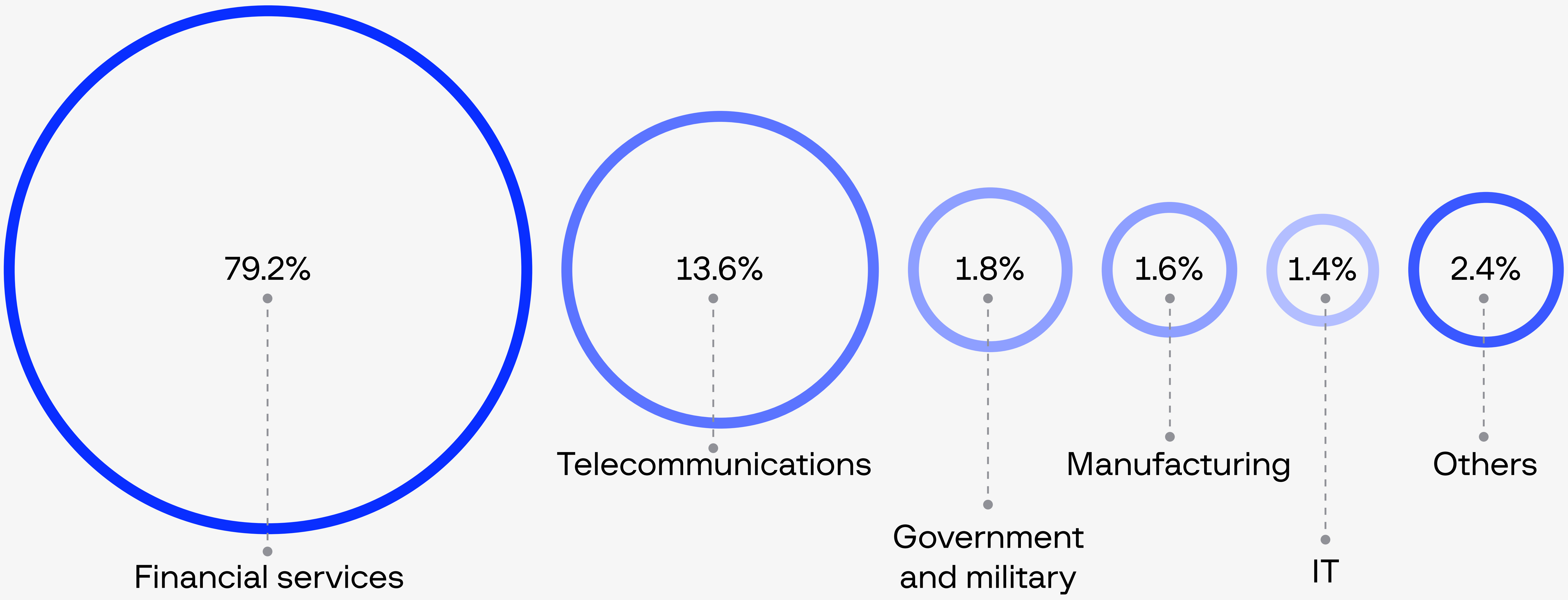
In 2024, Group-IB detected more than 200,000 fraudulent resources, marking a 22% increase year-on-year, with nearly 39% of observed scams targeting the travel industry. These scams often exploit periods of high demand, primarily targeting customers of popular apartment and hotel booking platforms as well as ticket purchasing aggregators.

Other industries, including energy, financial services, logistics, and telecommunications, accounted for over 35% of the scams detected in 2024. The logistics sector remains a major concern, as it has historically been a prime target for scammers, exemplified by the notorious Classiscam scheme.

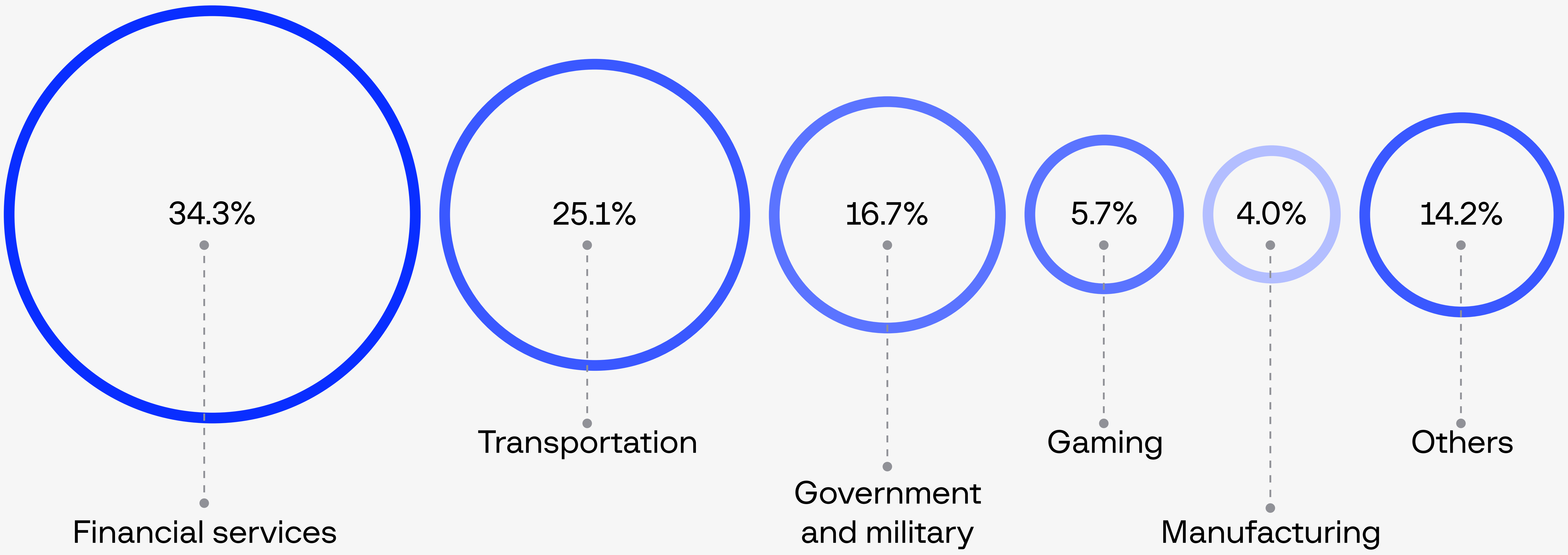
Global Top industries where scam resources were detected in 2024



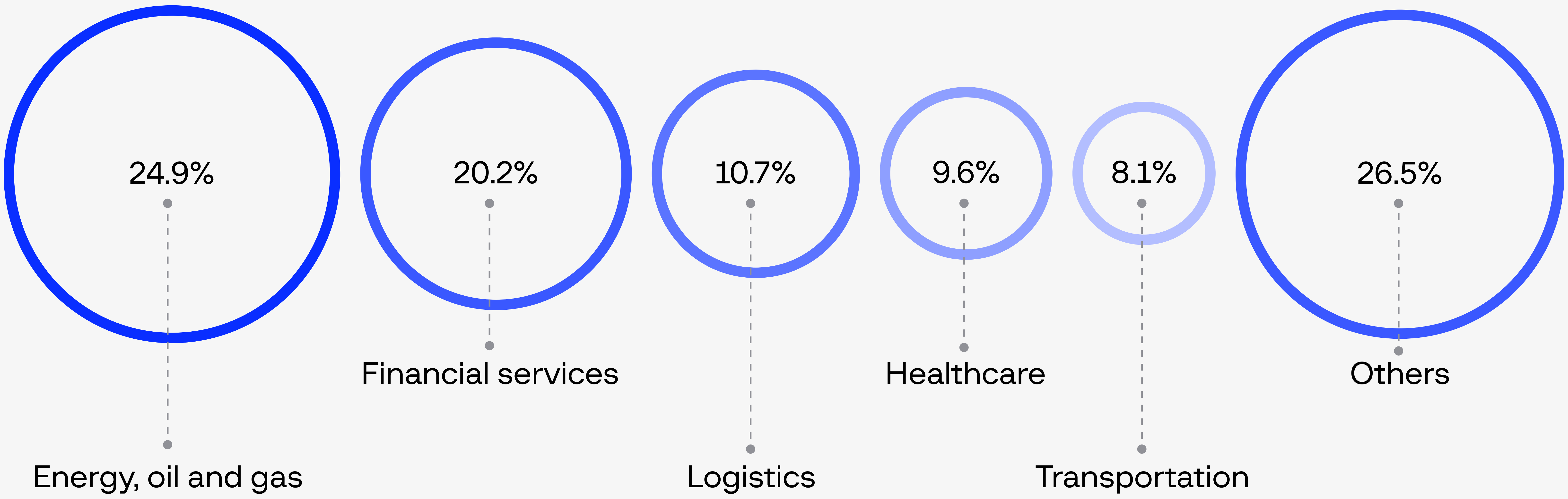
Asia-Pacific Top industries targeted by scams in 2024



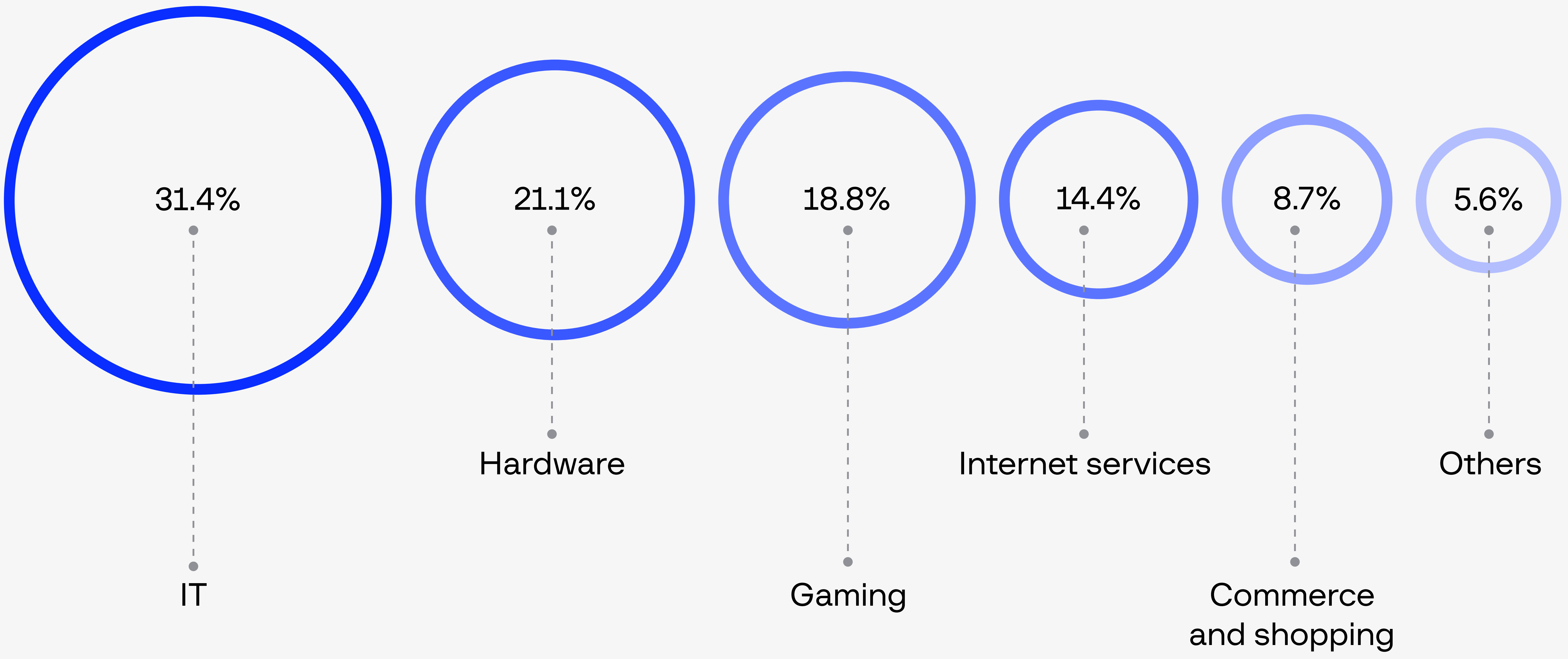
Europe Top industries targeted by scams in 2024



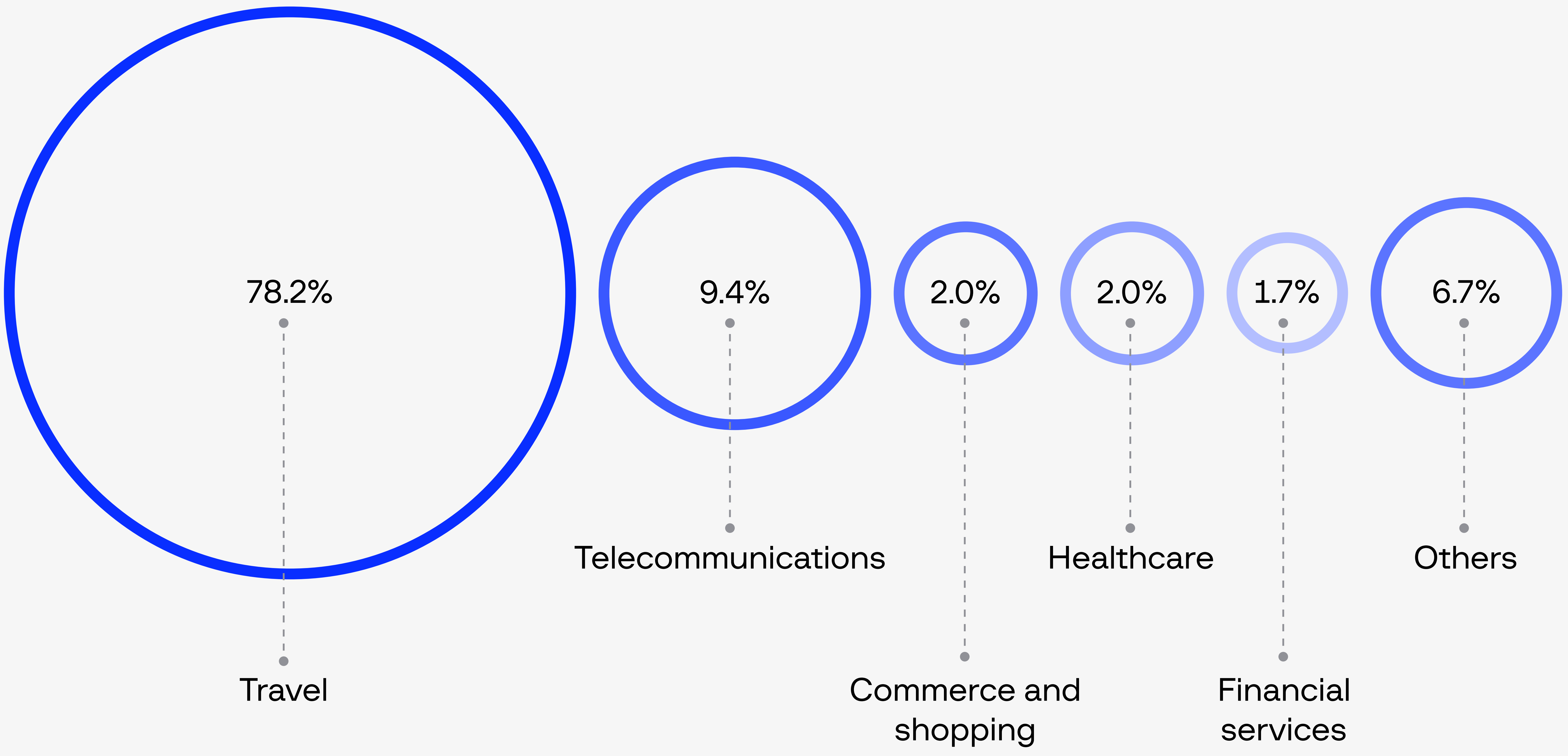
Middle East and Africa Top industries targeted by scams in 2024



North America Top industries targeted by scams in 2024



Latin America Top industries targeted by scams in 2024



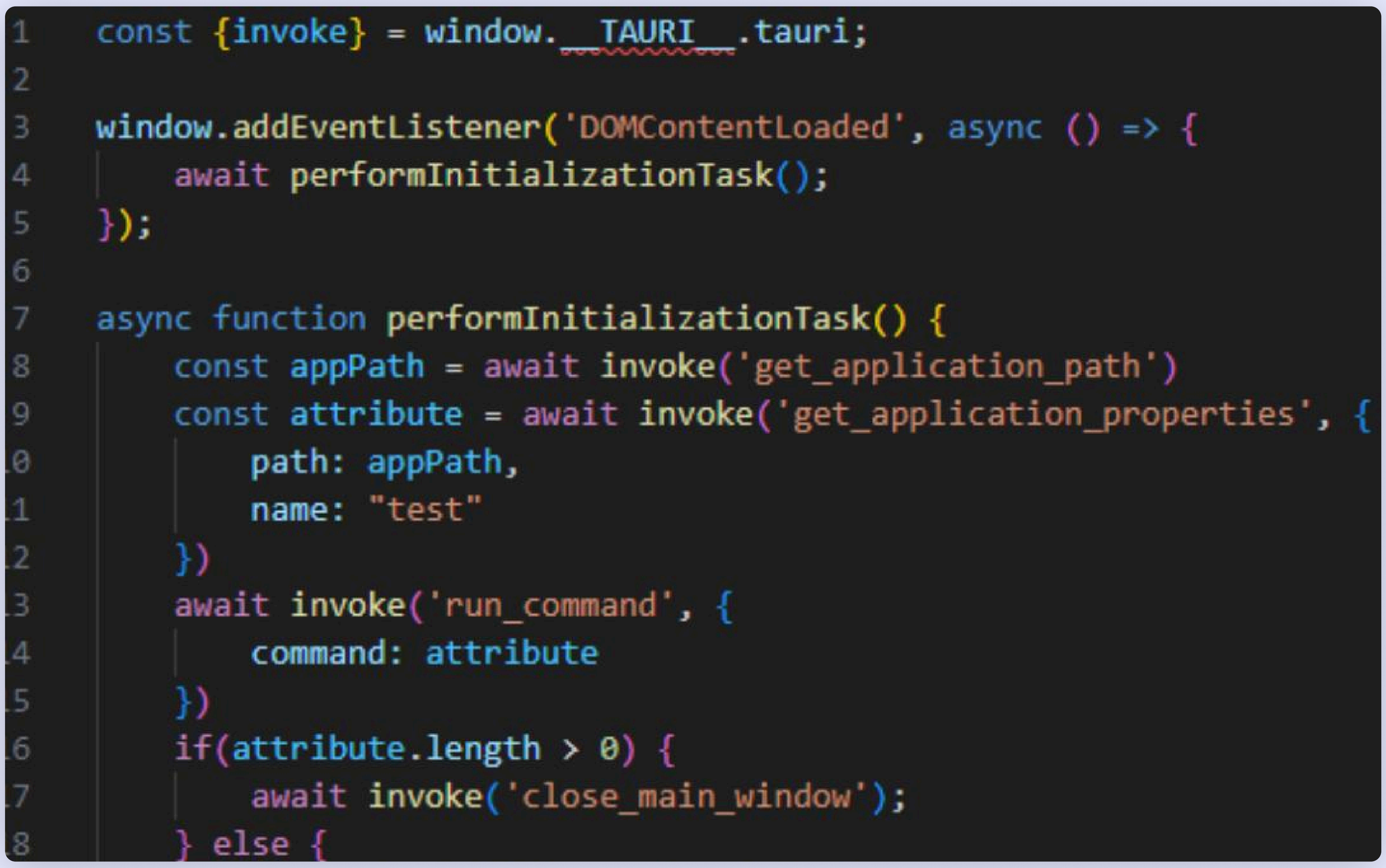
Top Tactics, Techniques and Procedures employed by threat actors in 2024

Tactics, Techniques, and Procedures (TTPs), describe the methods threat actors use to conduct cyberattacks. Tactics refer to the overall objectives of an attack, such as gaining initial access or exfiltrating data. Techniques are the specific ways attackers achieve their goals, like phishing or exploiting vulnerabilities. Procedures detail the exact steps and tools used to execute an attack.

In the current threat landscape, ordinary users, including employees and government officials, represent a significant target for cyberattacks. Phishing remains the most common initial attack vector, with threat actors employing various techniques to manipulate users into disclosing sensitive information. A concerning trend is the increasing preference for social engineering tactics, where attackers lure victims into executing malicious code, as this method is often more straightforward and effective than identifying and exploiting software vulnerabilities. Among the various types of cyberattacks, ransomware poses one of the most severe impacts, capable of incapacitating organizations and necessitating substantial ransoms for data recovery.

Notable new techniques by threat actors in 2024

Extended attributes attack

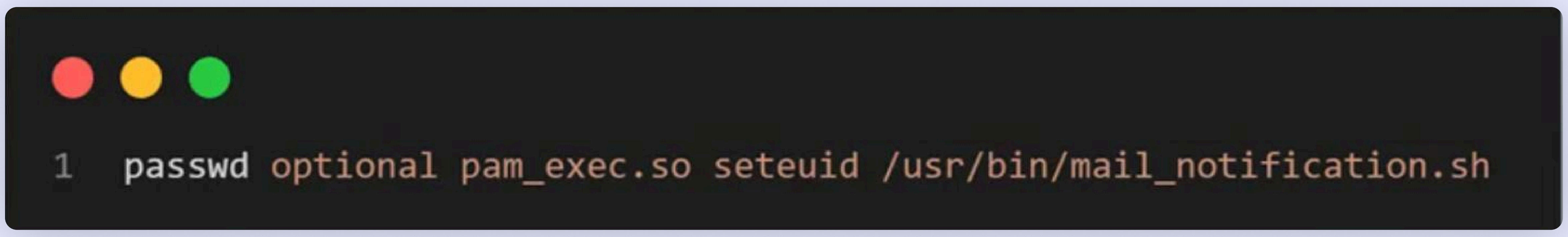


```
const {invoke} = window.__TAURI__.tauri;

window.addEventListener('DOMContentLoaded', async () => {
    await performInitializationTask();
});

async function performInitializationTask() {
    const appPath = await invoke('get_application_path')
    const attribute = await invoke('get_application_properties', {
        path: appPath,
        name: "test"
    })
    await invoke('run_command', {
        command: attribute
    })
    if(attribute.length > 0) {
        await invoke('close_main_window');
    } else {
```

This attack exploits Extended Attributes (EAs), metadata associated with files and directories in various file systems. The threat actor defines a custom extended attribute labeled "test". An application built on the Tauri framework then attempts to render an HTML webpage through a WebView, which loads a suspicious JavaScript file, "preload.js". Using the "get_application_properties" function, the application retrieves content from the "test" attribute and passes it to "run_command", where a shell script is executed, leading to potential system compromise.

Nearest neighbour attack

This technique exploits nearby Wi-Fi networks to enable remote infiltration of an organization's infrastructure. The threat actor conducts credential stuffing attacks to compromise at least two neighboring Wi-Fi networks. Once access is obtained, the attacker leverages the stolen credentials to penetrate the organization's network.

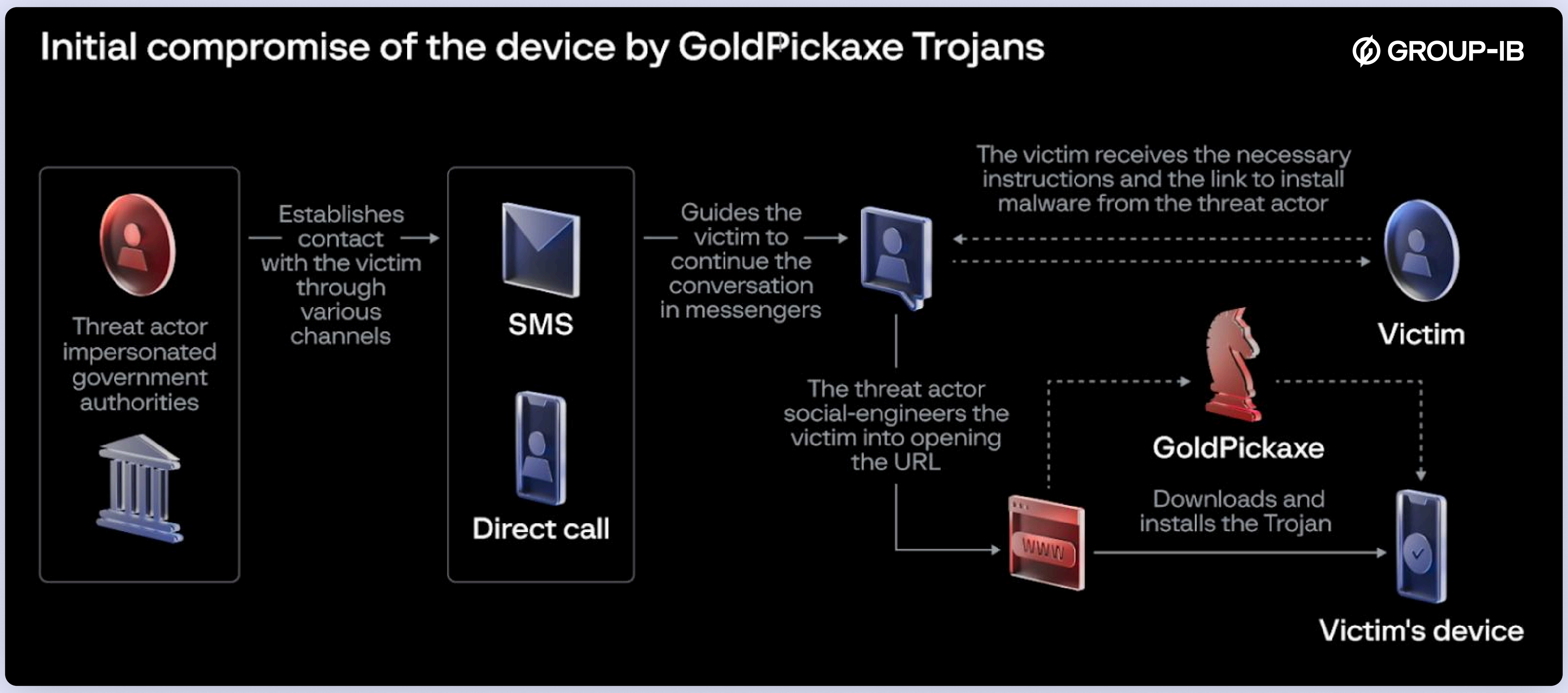


```
passwd optional pam_exec.so seteuid /usr/bin/mail_notification.sh
```

Pluggable authentication module (PAM) attack

The pluggable authentication module (PAM) is a modular framework built on shared libraries that manages user authentication and authorization across various Linux applications. A newly identified technique involves the use of the pam_exec module to obtain a privileged shell on a host, thereby granting the threat actor persistent access.

Face-stealing trojan



Initial compromise of the device by GoldPickaxe Trojans

GROUP-IB
Threat actor impersonated government authorities
Establishes contact with the victim through various channels
SMS
Direct call
Guides the victim to continue the conversation in messengers
The victim receives the necessary instructions and the link to install malware from the threat actor
Victim
The threat actor social-engineers the victim into opening the URL
WWW
GoldPickaxe
Downloads and installs the Trojan
Victim's device

The first iOS Trojan specifically designed to harvest facial recognition data for unauthorized access to bank accounts has emerged. Named GoldPickaxe.iOS, this malware is capable of collecting facial recognition data, identity documents, and intercepting SMS messages.

ClickFix

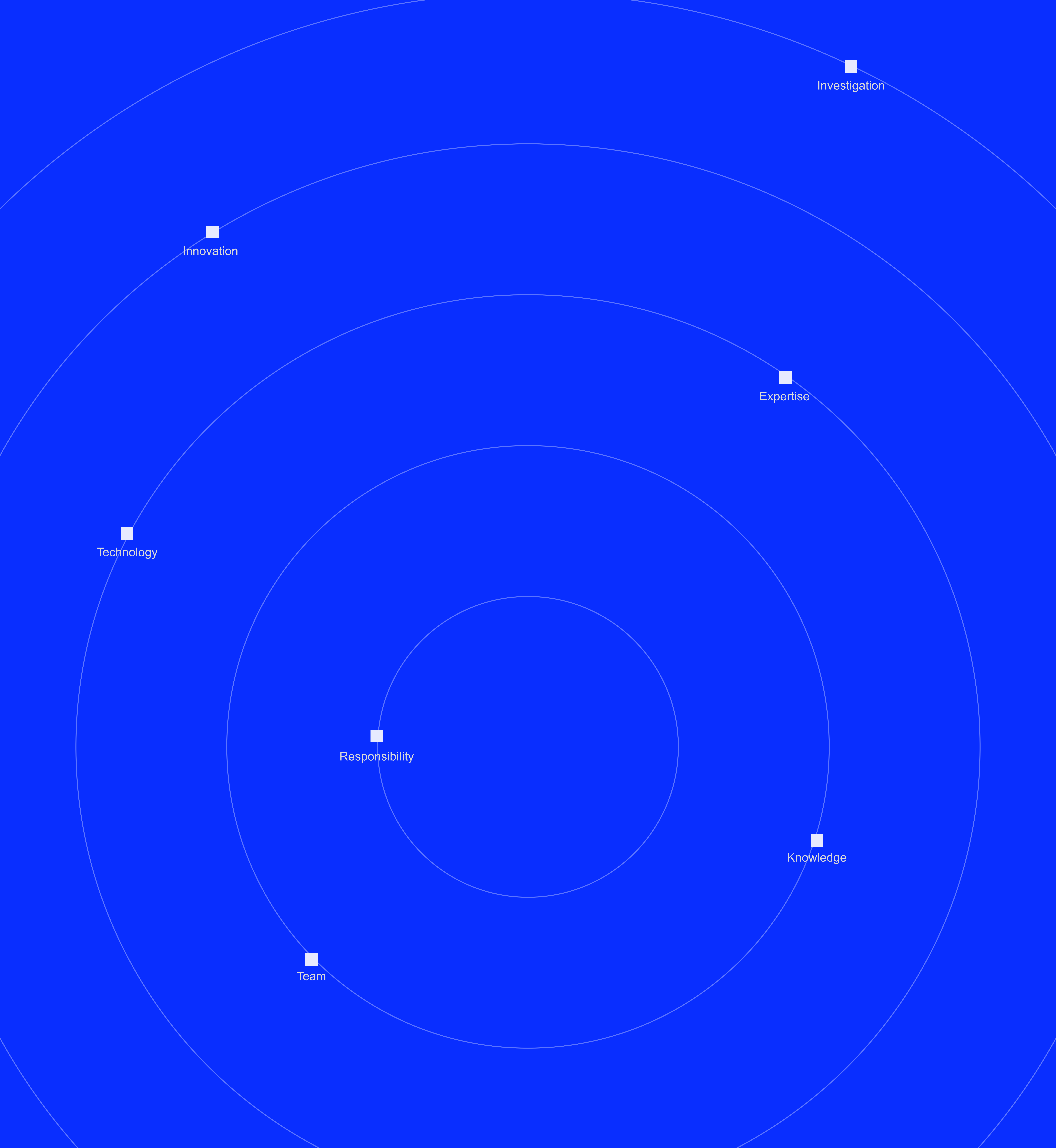
This infection chain manipulates users into unintentionally executing malware by presenting deceptive pop-ups that prompt actions to continue browsing. These pop-ups display messages such as **"Fix It"** or **"I am not a robot."** When clicked, a malicious PowerShell script is automatically copied to the clipboard. Users are then tricked into pasting the script into the **RUN** dialog (Windows Key + R), unknowingly executing the malware. This technique effectively enlists users in the infection process, allowing attackers to deploy malware with minimal resistance.

Most popular tactics and techniques used by threat actors

The most popular tactics and techniques used by threat actors, as monitored and observed by Group-IB, include:

Tactic	Technique	Technique/Sub-Technique ID	%
Initial Access	Phishing → Spearphishing Attachment	T1566.001	20.5
	Phishing	T1566	19.4
	Phishing → Spearphishing Link	T1566.002	14.5
Execution	User Execution/Malicious File	T1204.002	16.6
	Command and Scripting Interpreter	T1059	12.3
	User Execution	T1204	10.0
Persistence	Scheduled Task/Job → Scheduled Task	T1053.005	14.1
	Boot or Logon Autostart Execution → Registry Run Keys / Startup Folder	T1547.001	12.6
	Scheduled Task/Job	T1053	8.7
Privilege Escalation	Scheduled Task/Job → Scheduled Task	T1053.005	12.1
	Boot or Logon Autostart Execution → Registry Run Keys / Startup Folder	T1547.001	10.9
	Scheduled Task/Job	T1053	7.5
Defense Evasion	Obfuscated Files or Information	T1027	8.8
	Deobfuscate/Decode Files or Information	T1140	5.0
	Indicator Removal → File Deletion	T1070.004	4.9
Credential Access	Credentials from Password Stores → Credentials from Web Browsers	T1555.003	13.5
	Input Capture → Keylogging	T1056.001	9.2
	Unsecured Credentials → Credentials In Files	T1552.001	9.0

Tactic	Technique	Technique/Sub-Technique ID	%
Discovery	System Information Discovery	T1082	14.1
	File and Directory Discovery	T1083	9.2
	Process Discovery	T1057	8.2
Lateral Movement	Remote Services	T1021	23.9
	Remote Services → Remote Desktop Protocol	T1021.001	14.7
	Remote Services → SMB/Windows Admin Shares	T1021.002	12.7
Collection	Data from Local System	T1005	12.6
	Screen Capture	T1113	12.6
	Input Capture → Keylogging	T1056.001	10.4
Command-and-Control	Application Layer Protocol → Web Protocols	T1071.001	20.3
	Application Layer Protocol	T1071	15.3
	Ingress Tool Transfer	T1105	10.4
Exfiltration	Exfiltration Over Web Service	T1567	37.8
	Exfiltration Over C2 Channel	T1041	32.6
	Exfiltration Over Alternative Protocol	T1048	25.3
Impact	Data Encrypted for Impact	T1486	60.3
	Endpoint Denial of Service	T1499	28.3
	Network Denial of Service	T1498	6.2



Chapter 2: Key Threats and Trends

Key threat actors to look out for in 2025

Notorious cybercriminal groups have continued to evolve, executing high-profile attacks and refining their tactics, techniques, and procedures (TTPs). From sophisticated ransomware operations to targeted phishing campaigns, these threat actors have demonstrated a relentless ability to adapt and refine their methods, posing significant challenges to organizations worldwide.

LabHost

Regions
Worldwide

Industries
Multiple

LabHost has emerged as one of the most notorious platforms in the cybercriminal world, offering Phishing-as-a-Service (PhaaS) and enabling large-scale, automated phishing campaigns. Group-IB's Threat Intelligence team first identified LabHost in 2021, with its operations gaining significant traction in 2024. In early 2024, Group-IB observed a surge in phishing URLs targeting INTERAC, a Canadian payment service, which led to a deeper investigation into the broader LabHost ecosystem. This investigation revealed a well-organized structure designed to facilitate a variety of cybercrime activities.

The LabHost ecosystem includes multiple interlinked services: LabHost, the core PhaaS platform; LabCVV, a marketplace for stolen credit card data; LabSend, a SMS/MMS spam delivery system; and LabRefund, a Telegram channel where cybercriminals share methods for exploiting stolen data. These services work in tandem to simplify the execution of phishing attacks and lower the skill threshold required for attackers, increasing the scale and frequency of phishing incidents.

LabHost enables criminals to rent VPS servers and auto-deploy phishing websites within minutes, using a simple portal. Attackers can then generate links to these phishing sites, which are distributed to victims via the LabSend service—an SMS spam tool controlled through an Android application. Once victims open the phishing link, they are guided through a series of pre-defined attack scenarios to steal sensitive data such as credit card numbers, CVVs, and personally identifiable information. The LabRat module further enables attackers to manually guide victims, even capturing 2FA codes.

The widespread use of LabHost represents a new threat vector, with its ability to automate and streamline phishing operations making it a significant cybersecurity risk. Group-IB's research highlights the growing sophistication of these campaigns, which continue to evolve and pose serious challenges for organizations worldwide.

January

UNC5221

Regions
North America

Industries
Government and Military

The widespread compromise of VPN devices, particularly those used by critical infrastructure organizations, poses a significant security risk and underscores the potential for espionage and disruption.

In January 2024, Ivanti disclosed the mass exploitation of two high-severity zero-day vulnerabilities in its widely deployed Connect Secure VPN products. Researchers reported thousands of compromised Ivanti VPN devices, with victims including the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and MITRE, a prominent federally funded research and development organization.

Mandiant, a Google Cloud-owned cybersecurity firm, attributed the exploitation primarily to UNC5221, a group linked to China. Their research suggests that the group's malicious activity began as early as December 2023, indicating a potential window of vulnerability before the public disclosure.

Dark Halo

Regions
North America

Industries
Technology

State-sponsored cyber espionage remains a persistent threat, with high-value organizations frequently targeted by advanced threat actors. In January 2024, Microsoft disclosed a significant security breach, revealing that a had successfully exfiltrated emails from its senior leadership team, as well as employees within its cybersecurity and legal departments. The attack was attributed to Midnight Blizzard (in Group-IB gradation Dark Halo). The exfiltration of sensitive emails represents a serious intelligence loss for Microsoft, underscoring the ongoing challenge of defending against sophisticated cyber espionage campaigns.

Boolka

Regions:
Worldwide

Industries:
Multiple

In January 2024, during an analysis of infrastructure used by ShadowSyndicate, Group-IB Threat Intelligence analysts detected a landing page designed to distribute the BMANAGER modular trojan, created by a threat actor known as Boolka. Further investigation revealed that this landing page was a test run for a malware delivery platform based on the BeEF framework. Since at least 2022, the threat actor behind this campaign has been conducting opportunistic SQL injection attacks against websites in multiple countries. Over the past three years, Boolka has been infecting vulnerable websites with malicious JavaScript capable of intercepting any data entered on compromised pages.

In March 2024, Group-IB Threat Intelligence analysts observed the first use of Boolka's malware delivery platform in the wild. Given the significant overlap between the list of websites infected with Boolka's form-stealing JavaScript and those serving the BeEF payload, it is likely that the threat actor employed the same infection approach tested in the early stages of their activity.

In the analyzed cases, Boolka's BeEF-based malware delivery platform was used to distribute a downloader for the BMANAGER trojan.

February

ALPHV (BlackCat)

Regions
North America

Industries
Healthcare

The February 2024 ransomware attack on Change Healthcare, a subsidiary of UnitedHealth Group, caused widespread disruption to more than 100 critical healthcare functions, including claims processing and prescription management. The attack was attributed to the ALPHV (BlackCat) group, a notorious ransomware operator. In response, UnitedHealth Group issued $8.5 billion in loans to support affected healthcare providers, with $3.2 billion repaid by October 2024. The total financial impact of the incident was estimated at $2.87 billion for the year, highlighting the severe economic and operational consequences of cyberattacks on the healthcare sector.

RansomHub

Regions
Worldwide

Industries
Multiple

RansomHub, which launched its affiliate program in February 2024, has actively recruited former affiliates from the Scattered Spider group and enables collaboration with other Ransomware-as-a-Service (RaaS) operations.

Against the backdrop of increased pressure from law enforcement agencies and a high number of operations targeting the LockBit group, we assume that RansomHub will take the lead in the number of attacks in 2025. As of now, according to global statistics (based on DLS data), it ranks second, and in some specific regions, it has already surpassed LockBit in the number of compromised organizations.

The ransomware developed by RansomHub targets Windows, Linux, and ESXi systems, with the ability to self-propagate within internal networks. It employs tactics such as disabling network interfaces and initiating Safe Mode on Windows systems before encryption. The most common attack vector is through publicly accessible Remote Desktop Protocol (RDP) services on Windows servers that lack multi-factor authentication.

RansomHub exfiltrates data by archiving and transferring it to remote file shares using tools like rclone to Mega. To obscure their tracks, attackers revoke access tokens for Mega after data transfer. Group-IB has observed exfiltrations exceeding 150 GB in a single instance, creating noticeable spikes in network traffic that may indicate ongoing data theft.

Lazarus

Regions
APAC

Industries
Finance

The largest cryptocurrency heist of 2024 was carried out by the North Korean state-sponsored group Lazarus, which stole $308 million in cryptocurrency from the Japanese platform DMM in May, according to the FBI.

In March 2024, a North Korean cyber actor posed as a recruiter on LinkedIn to target an employee at Ginco, a Japan-based cryptocurrency wallet company. The attacker tricked the employee into executing a malicious Python script from a GitHub page, leading to their compromise.

By mid-May 2024, hackers exploited session cookies to impersonate the victim and gain access to Ginco's communications system. Later, in May 2024, they likely manipulated a legitimate transaction request by a DMM employee, leading to the theft of 4,502.9 BTC ($308M). The stolen funds were later transferred to Lazarus-controlled wallets.

The FBI, in collaboration with the U.S. Defense Department and Japan's National Police Agency, confirmed Lazarus' involvement. This incident highlights the increasing sophistication of North Korean cyber operations and their reliance on cryptocurrency theft as a key revenue source for the regime. The scale of the attack underscores the vulnerabilities of cryptocurrency platforms to advanced cyber threats and the ongoing challenges in tracking and recovering stolen digital assets.

DMM Bitcoin announced in December 2024, that it was going out of business, unable to continue operation after its losses in May. It plans to pass over customers' deposits to SBI VC Trade, a cryptocurrency exchange unit of SBI Holdings, by March 2025.

Eldorado

Regions
Worldwide

Industries
Multiple

In March 2024, an advertisement for a new affiliate program appeared on the ransomware forum “RAMP.” The post promoted the availability of a locker and loader, while also seeking pentesters to join the team. Group-IB analysts infiltrated the Eldorado group and discovered that the group's representative was a Russian speaker. The ransomware builder required the domain administrator's password or NTLM (Windows New Technology LAN Manager) hash, along with other parameters, to generate ransomware samples.

The Eldorado group possesses two versions of the malware—one for Windows and another for Linux. This development is unique, as it does not rely on previously published ransomware builder sources. For context, on September 21, 2022, the builder for LockBit 3.0 ransomware was leaked, enabling various threat actors to create their own versions and conduct numerous high-profile attacks using its encryption and evasion techniques. Similarly, the Babuk ransomware source code was leaked on September 1, 2021, leading to the creation of multiple ransomware strains by different groups to exploit and exfiltrate data from targeted networks. Notable examples of these include the LIMPOPO (also known as SOCOTRA, FORMOSA, SEXi) ransomware group, BabLock ransomware, and Estate ransomware.

The Eldorado ransomware is built using Golang for cross-platform capabilities. It employs ChaCha20 for file encryption and RSA-OAEP (Rivest-Shamir-Adleman Optimal Asymmetric Encryption Padding) for key encryption. Additionally, it is capable of encrypting files on shared networks using the Server Message Block (SMB) protocol. Customization during the build process includes key parameters such as target networks, company names, ransom note content, and administrator credentials.

April

ShinyHunters

Regions
Worldwide

Industries
Finance, Internet

In April 2024, a series of significant data breaches impacted numerous major enterprises after the threat actor ShinyHunters compromised high-profile Snowflake cloud database accounts. These breaches exposed vast quantities of personal data.

Santander disclosed that the bank details of 30 million customers, along with information on current and some former employees, were stolen. The compromised data included 28 million credit card numbers, 6 million account numbers, and sensitive HR information pertaining to Santander staff.

Ticketmaster suffered what was, at the time, the largest data breach on record, with the credentials of 530 million live music fans compromised.

These incidents highlight the risks associated with cloud-based data storage and the potential for widespread impact when such systems are breached. They underscore the need for robust security measures to protect sensitive information in cloud environments.

Ansgar

Regions
North America

Industries
Healthcare

In April 2024, MediSecure, an Australian electronic prescription provider, suffered a significant cyberattack resulting in the theft of approximately 6.5 terabytes of sensitive data. The compromised information included names, addresses, email addresses, phone numbers, insurance details, prescription information, and login credentials.

The threat actor, identifying as Ansgar, reportedly offered the stolen data for sale for $50,000, providing screenshots as proof of the breach.

This incident raises serious concerns about the security of patient data within the healthcare system and the potential for identity theft and other malicious use of the stolen information. The scale of the data breach, along with the offer to sell the data, underscores the growing targeting of healthcare organizations by cybercriminals.

May

LockBit

Regions
North America

Industries
Government and military

In late May 2024, the City of Wichita, Kansas, confirmed a significant cyberattack that disrupted essential city services. Unauthorized access to the city's network led to the encryption of critical systems with malware, prompting officials to isolate the affected systems in an effort to contain the spread.

The LockBit ransomware group claimed responsibility for the attack, which caused widespread disruptions, including payment processing failures and airport delays, demonstrating the far-reaching impact on municipal operations.

While the city acknowledged receiving a ransom demand, it emphasized its commitment to cooperating with law enforcement in the ongoing investigation. The city has prioritized collaboration with authorities over meeting the attackers' demands.

Ajina

Regions
Central Asia

Industries
Finance

In May 2024, Group-IB analysts uncovered suspicious activity targeting bank customers in Central Asia. The threat actors were distributing malicious Android malware designed to steal users' personal and banking information, with the potential to intercept two-factor authentication (2FA) messages.

During the investigation, Group-IB discovered APK files masquerading as legitimate applications for payments, banking, deliveries, and other daily functions. These malicious files were being spread across Telegram channels.

Group-IB analyzed approximately 1,400 unique samples of Android malware and identified variations between different versions of the same malware strain.

The attackers appear to operate with a network of affiliates motivated by financial gain, spreading Android banker malware to target everyday users. Analysis of the file names, sample distribution methods, and other activities suggests that the attackers possess a cultural familiarity with the region in which they are operating.

The campaign has since evolved, expanding beyond its initial target region and impacting victims in other countries.

GoldFactory

Regions
APAC

Industries
Finance

In May 2024, Group-IB uncovered the first iOS Trojan designed to harvest facial recognition data for unauthorized access to bank accounts, which they have dubbed GoldPickaxe.iOS. The GoldPickaxe family, which includes versions for both iOS and Android, is based on the GoldDigger Android Trojan and features regular updates aimed at enhancing its capabilities and evading detection.

GoldPickaxe.iOS is capable of collecting facial recognition data, identity documents, and intercepting SMS. Its Android counterpart shares similar functionalities but also includes additional features typical of Android Trojans. To exploit the stolen biometric data, the threat actor utilizes AI-driven face-swapping services to create deepfakes. This combination of biometric data, ID documents, and SMS interception enables cybercriminals to gain unauthorized access to victims' bank accounts—introducing a new method of monetary theft previously unseen by Group-IB researchers in other fraud schemes.

GoldPickaxe.iOS employs a notable distribution method. Initially, the threat actor utilized Apple's mobile application testing platform, TestFlight, to distribute the malware. After the malicious app was removed from TestFlight, the attacker adopted a more sophisticated approach by using a multi-stage social engineering scheme to persuade victims to install a Mobile Device Management (MDM) profile, granting the attacker complete control over the victim's device.

Group-IB has attributed this entire threat cluster to a single threat actor, codenamed GoldFactory, which has developed a sophisticated suite of mobile banking malware.

The victims of these attacks are predominantly located in the Asia-Pacific (APAC) region, with evidence suggesting a particular focus on Vietnam and Thailand. However, there are emerging indications that GoldFactory may expand its operations beyond these two countries. Group-IB has notified the brands that were impersonated by GoldFactory's Trojans.

CraxsRat

Regions
APAC

Industries
Finance

Since April 2023, a series of scams involving fake Android apps have targeted Singapore, deploying banking trojans to harvest victims' credentials, steal personal information, and gain control over their devices. In this specific campaign, threat actors leveraged phishing websites to distribute fake apps disguised as well-known brands. The abuse of popular brands and the use of Android trojans disguised as legitimate-looking apps have become a notable trend in cybercriminal activity in recent years.

As part of the scam, cybercriminals lured victims through fraudulent advertisements for services or products. Users were then prompted to download fake Android apps under the pretense of making a payment or placing an order.

Group-IB's High-Tech Crime Investigation team has been actively analyzing these early campaigns. Initially, the fake Android apps were detected as Spymax by most antivirus products. However, deeper analysis of the code revealed that these apps were, in fact, Remote Access Trojans (RATs) built using Craxs RAT.

Spymax is a mobile RAT originally developed in 2019 by the threat actor known as ✶ s c я є α м. After its source code was leaked in 2020, multiple cybercriminals customized the software for their own purposes. One such actor, EVLF, developed his own malware variant, Craxs RAT, using the leaked code. As of April 2023, EVLF continued to advertise new versions of Craxs RAT on his Telegram channel.

During the investigation into the Singapore phishing campaign using Craxs RAT, Group-IB identified at least 10 different brands exploited by threat actors. These ranged from online shopping platforms and an anti-scam center to a pet grooming salon and a dumpling shop, among others. In each case, victims were tricked into downloading and installing the fraudulent Android app, allowing attackers to take control of their devices.

Expansion into Malaysia

In May 2024, Group-IB received a request from a Malaysia-based financial organization to investigate a malware sample targeting its clients across the Asia-Pacific region.

One victim encountered a phishing website impersonating a well-known local food brand, which prompted them to download an app to place an order. Within five minutes of installing the app, the victim's credentials were stolen, and within 20 minutes, unauthorized fund withdrawals occurred from the victim's bank account.

June

Qilin

Regions
Europe

Industries
Healthcare

In June 2024, a $50 million ransomware attack targeted Synnovis, a pathology partnership providing specialist blood tests for several London NHS Trusts, including Guy's and St Thomas' and King's College Hospital. Ciaran Martin, former head of the UK's National Cyber Security Centre, suggested that the attack was likely carried out by Qilin, a Russian cybercriminal group.

Qilin, which has been active since 2022 and is known for its Ransomware-as-a-Service (RaaS) operations, is suspected of being behind the attack. Group-IB's 2023 infiltration of the group revealed their typical attack vector: spear phishing campaigns targeting insiders to gain initial access to victim networks, often by tricking them into sharing credentials or installing malware.

The attack on Synnovis, which affected critical blood transfusion services, underscores the severe risks ransomware poses to healthcare infrastructure and highlights the potential for widespread disruption to essential medical services.

BlackSuit

Regions
North America

Industries
Technology

In June 2024, CDK Global, a major US-based software provider serving the automotive industry, was targeted by a significant ransomware attack. First reported on June 18th, the incident occurred when an employee inadvertently downloaded malware, leading to the encryption of critical files and systems.

The BlackSuit ransomware group, believed to be affiliated with threat actors from Eastern Europe and Russia, claimed responsibility for the attack. Initially, the attackers demanded a ransom of $10 million, which later escalated to over $50 million, reflecting the increasingly aggressive tactics used by ransomware operators.

The attack caused substantial disruption to CDK Global's operations, affecting dealerships and potentially disrupting downstream processes within the automotive industry that rely on their software.

Cicada3301

Regions
Europe, North America

Industries
Multiple

Since its discovery in June 2024, the Cicada3301 Ransomware-as-a-Service (RaaS) group has been actively targeting businesses across numerous critical sectors. Between June and October 2024, the group leaked stolen data from 30 organizations via its dedicated leak sites (DLS), with 24 of these incidents affecting victims in the United States and the United Kingdom.

Group-IB recently gained access to the Cicada3301 ransomware affiliate panel, providing valuable insight into the group’s operations.

The ransomware is written in Rust, supporting a variety of platforms, including Windows, Linux, ESXi, and NAS, and even extends to less common architectures like PowerPC.

Cicada3301 operates an affiliate program, recruiting penetration testers (pentesters) and access brokers. Affiliates receive a 20% commission and gain access to a feature-rich, web-based panel for managing ransom negotiations.

The ransomware uses ChaCha20 and RSA encryption, with configurable modes (Full, Fast, Auto), allowing both full and partial file encryption to optimize the speed and impact of the attacks.

The group's destructive capabilities include shutting down virtual machines on ESXi and Hyper-V, terminating processes and services, deleting shadow copies, and encrypting network shares to maximize disruption.

Brain Cipher

Regions
Worldwide

Industries
Government and military

On 20 June 2024, a major ransomware attack targeted an Indonesian data center, crippling approximately 210 critical national and local government services, including customs and immigration. The attack caused significant delays for travelers at airports. The threat actor, Brain Cipher, initially demanded a ransom of US$8 million but later published the decryptor for free.

Brain Cipher ransom notes were found in connection with LockBit malware samples. Furthermore, there are notable similarities between the style and content of Brain Cipher’s ransom notes and those of the SenSayQ ransomware group. Both groups' TOR websites utilize similar technologies and scripts.

The contact email addresses associated with SenSayQ, EstateRansomware, and another unnamed ransomware group overlap. Traces of the EstateRansomware group were first identified in April 2024, raising the possibility that the individuals behind Brain Cipher and EstateRansomware could be the same. The tactics, techniques, and procedures of EstateRansomware were previously described by Group-IB.

In July 2024, attacks with similar ransom notes were carried out under the name RebornRansomware.

July

Rhysida

Regions
North America

Industries
Government and military

In July 2024, the City of Columbus, Ohio, was targeted by a major ransomware attack attributed to the Rhysida ransomware group. The attackers claimed to have exfiltrated 6.5 terabytes of data from the city's systems, including highly sensitive information such as emergency services data and access to city surveillance camera feeds. Subsequent data breach filings confirmed that the personal information of over 500,000 current and former residents was compromised.

This breach led to a high-profile lawsuit, emphasizing the complex legal landscape surrounding municipal cybersecurity incidents and the growing accountability of local governments for data protection. The attack underscores the vulnerability of critical city infrastructure to ransomware and the potential for large-scale data breaches with severe consequences for residents.

Lazarus

Regions
Worldwide

Industries
Multiple

Lazarus continues to push forward with its cyber campaign in 2024. The Beaver Fever trend has persisted into the year, with the Lazarus-led Contagious Interview campaign continuing to cause widespread disruption. This campaign begins with a fake job interview, deceiving job seekers into downloading and executing a Node.js project that contains the BeaverTail malware. BeaverTail then deploys a Python backdoor known as InvisibleFerret.

Originally identified by PANW researchers as JavaScript malware in November 2023, BeaverTail was later discovered in a native macOS version in July 2024. In mid-August 2024, Group-IB researchers detected a fraudulent Windows video conferencing application impersonating a legitimate one, which was subsequently confirmed to be BeaverTail following analysis.

As part of its ongoing research, Group-IB identified additional malicious repositories newly hosted on code-sharing platforms, all associated with Lazarus malware. The team also discovered a Python variant of BeaverTail with expanded capabilities, dubbed CivetQ.

DragonForce

Regions
Worldwide

Industries
Manufacturing, Real Estate, and Transportation

Discovered in August 2023, the DragonForce ransomware group has been actively targeting organizations across multiple industries. Initially leveraging a variant of a leaked LockBit 3.0 builder, the group expanded its attack arsenal in July 2024 by introducing its own ransomware variant.

DragonForce operates a Ransomware-as-a-Service (RaaS) affiliate program, offering affiliates access to two ransomware variants: a modified LockBit 3.0 variant and a ContiV3-derived variant. While initially claimed as original, the latter was found to be based on repurposed Conti code. The group employs double extortion tactics, encrypting victim data and threatening to leak stolen information unless a ransom is paid.

Launched on June 26, 2024, the affiliate program offers affiliates 80% of ransom payments, along with tools for attack management and automation. Affiliates can generate customized ransomware samples with options to disable security features, configure encryption parameters, and personalize ransom notes.

The group employs the “Bring Your Own Vulnerable Driver” (BYOVD) technique in its Conti-based variant to disable security processes and evade detection. Additionally, DragonForce clears Windows Event Logs post-encryption to hinder forensic investigations and obscure its activities.

Between August 2023 and August 2024, DragonForce targeted 82 victims, primarily in the manufacturing, real estate, and transportation sectors. Its ransomware payload incorporates advanced encryption techniques and anti-analysis countermeasures.

The group also utilizes the SystemBC backdoor for persistence, Mimikatz and Cobalt Strike for credential harvesting, and Cobalt Strike for lateral movement. Network scanning tools, such as SoftPerfect Network Scanner, are used to map networks and facilitate ransomware propagation.

TeamTNT

Regions
Europe, APAC

Industries
Crypto

In 2024, TeamTNT intensified attacks on Virtual Private Server (VPS) cloud infrastructures, particularly CentOS systems. Their campaigns begin with SSH brute-force attacks, exploiting weak credentials to gain access. Once inside, they deploy malicious scripts to disable security features, delete logs, and modify system files, making detection difficult.

A key objective of these attacks is hijacking system resources for cryptocurrency mining. The malware kills existing miners, removes Docker containers, and updates DNS settings to Google's servers. To maintain stealth, TeamTNT installs the Diamorphine rootkit, which grants root privileges and hides their presence. They further secure control by modifying file attributes, creating a backdoor user, and erasing command history.

Group-IB has observed that TeamTNT is expanding beyond CentOS, now targeting misconfigured Docker APIs and Kubernetes environments. The group has developed techniques to scan for exposed credentials and use legitimate cloud monitoring tools to gather intelligence on compromised systems (source: group-ib.com). These advancements reflect their growing sophistication and ability to exploit cloud infrastructure at scale.

The increasing complexity of TeamTNT's attacks highlights the urgent need for stronger cloud security. Organizations should enforce multi-factor authentication, regularly audit system configurations, and implement continuous monitoring to detect and mitigate threats proactively.

Salt Typhoon

Regions
North America

Industries
Telecommunications

In late 2024, China-linked hacking group Salt Typhoon attacked major U.S. telecom companies. As many as eight telecoms firms have been identified as victims including Verizon, AT&T, and others. Authorities are investigating the data breaches, which may have impacted national security.

Notable cybersecurity events

The past year has been a pivotal period for cybersecurity, marked by significant events that have shaped the threat landscape, from critical incidents, high-profile data breaches, large-scale cyberattacks, to the arrests of notable cybercriminals. 2024 also saw the emergence of new techniques, tactics, and procedures (TTPs) adopted by threat actors, along with the discovery and exploitation of critical vulnerabilities. The following events illuminate the evolving threat landscape and their implications for organizations worldwide.

Transportation

Transport for London breach and disruption

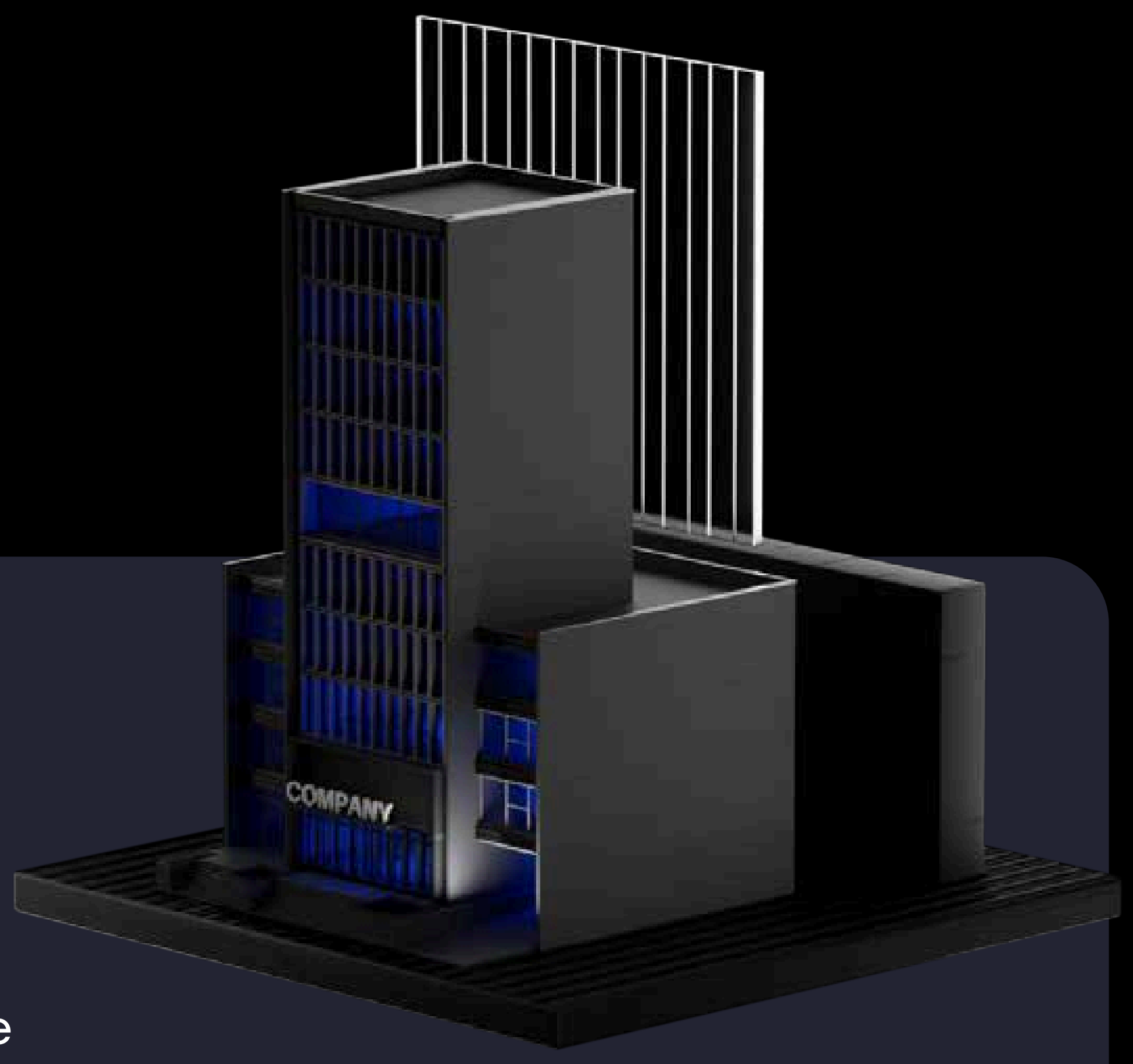
Regions
Europe

Industries
Transportation

In September 2024, Transport for London (TfL) reported a sophisticated and aggressive cyberattack that severely disrupted its digital services, though core transport operations, including buses and trains, remained unaffected. The attack impacted key customer-facing systems, including online and app-based Oyster card registration and the processing of refunds for contactless pay-as-you-go journeys.

Critically, the breach exposed the bank details of approximately 5,000 customers, along with employee passwords. The financial impact has been substantial, exceeding £30 million, with over £5 million allocated to incident response, investigation, and cybersecurity enhancements in the three months following the attack.

This incident underscores the vulnerability of critical infrastructure providers like TfL to cyber threats and highlights the significant financial and operational disruptions that can occur, even when core services continue to function.



Dell Technologies data breach

Regions
Worldwide

Industries
Technology

Dell Technologies in May said 49 million customer records were stolen in a data breach, including names, addresses, hardware bought, services rendered, and order information.

ScreenConnect software vulnerability

Regions
Worldwide

Industries
Technology

In February 2024, ConnectWise, a vendor of managed service provider (MSP) tools, disclosed two critical vulnerabilities (CVE-2024-1709 and CVE-2024-1708) in its widely used ScreenConnect software. ScreenConnect is a crucial tool for MSPs, enabling remote access to client devices for IT support. The vulnerabilities, including an authentication bypass flaw (CVSS 10), allowed attackers to potentially gain administrative privileges.

In late February 2024, Huntress researchers reported that over 8,800 servers were still unpatched and running vulnerable versions of ScreenConnect. They also demonstrated a proof-of-concept exploit capable of bypassing authentication on these unpatched servers, highlighting the urgent need for MSPs to update to the patched version.

XZ Utils backdoor vulnerability

Regions
Worldwide

Industries
Technology

In March 2024, a critical backdoor was discovered in XZ Utils, a widely used open-source data compression toolset based on the LZMA algorithm, affecting a broad range of Linux distributions. The backdoor was uncovered by Microsoft developer Andres Freund during a routine code review and poses a severe supply chain risk.

The backdoor, likely present for an unknown period prior to its discovery, allowed attackers to compromise systems by injecting malicious code into the SSH daemon. This vulnerability enabled remote attackers to execute arbitrary code, granting them complete control over affected machines. The potential impact is extensive, including data theft, ransomware deployment, and the creation of botnets. Given the widespread use of XZ Utils across servers, desktops, and embedded devices, this vulnerability is of significant concern.

Internet Services

Trello data leak

Regions
Worldwide

Industries
Internet services

About 15 million users of the Trello productivity platform had their details shared online in July, costing the company up to US$10 million in damages.

On July 16, 2024, a threat actor with the nickname "emo" on the breachforums forum published the API scraped database of Trello. In January 2024, the threat actor offered this scraped database for sale. The scraped database contains 15,182,079 records including usernames, names, and email addresses among other data. Notably, the attacker used a list of previously compromised email addresses, sending a request to see if the email address was registered on Trello.

Internet Archive data leak

Regions
Worldwide

Industries
Internet services

In September 2023, the Internet Archive, a prominent non-profit digital library providing free access to digitized materials, was targeted by a series of cyberattacks that resulted in the exposure of over 31 million files. The compromised data included sensitive information such as email addresses and usernames. Attackers exfiltrated a 6.4GB SQL database file, marking a significant data breach.

This incident raises serious concerns about the security of user data stored by non-profit organizations, highlighting the critical need for robust cybersecurity measures, even for entities with a public service mission. The scale of the breach, which affected millions of users, underscores the risk of identity theft and the potential malicious use of the stolen information.

ClickFix social engineering technique

Regions
Worldwide

Industries
Internet services

In June 2024, a new and particularly insidious social engineering technique known as ClickFix emerged. This method quickly gained traction among various threat actors, who exploit it to lure individuals into executing malicious PowerShell commands that ultimately lead to malware infections.

The ClickFix technique is characterized by its ability to exploit user trust through the presentation of fake error messages that mimic legitimate system notifications. These messages can originate from multiple sources.

Upon encountering a ClickFix dialog box, users are presented with instructions that appear to guide them in resolving a purported issue. The instructions may lead to one of two outcomes:

Automatic Execution:

In some instances, the ClickFix technique is designed to automatically copy and paste a malicious script into the PowerShell terminal or the Windows Run dialog box. This action results in the execution of the malicious code without any user intervention.

Manual Execution:

Alternatively, users may receive detailed instructions prompting them to manually open PowerShell and paste a provided command. This method relies on user compliance to execute the malicious script, thereby facilitating the malware download.

The attack chain usually concludes with the deployment of the different stealers such as Vidar, CStealer, AMOS, DarkGate, Emmenthal, StealC, Rhadamanthys, Atomic, Lumma. However, threat actors may also introduce additional malware, such as remote access trojans (RATs) like AsyncRAT and worms like XWorm.

Since August 2024, the Group-IB Threat Intelligence (TI) team has researched and actively monitored the ClickFix technique in the wild. At its core, the ClickFix infection chain operates by deceiving users into taking an action to continue browsing the internet. Pop-ups are shown with dialog requiring the user to press on buttons like "Fix It" or "I am not a robot". Once clicked, a malicious powershell script is automatically copied to the user's clipboard. Users are then deceived into pasting the script into the RUN dialog after pressing Windows key + R, thereby executing the malware without their knowledge. This technique facilitates the infection process, enabling attackers to deploy the malware with direct help of users.

When users click the button on these webpages, a malicious PowerShell script is copied to their clipboard, and additional instructions are displayed to prompt execution. The website uses JavaScript to automatically copy the script without any user interaction.

This technique has been adopted by many cybercriminals, and even APT groups to lure their victims and infect them with their desired malware. Cybercriminals have primarily used this method to distribute infostealers including Lumma, Vidar, CStealer, AMOS, DarkGate, Emmenthal, and others.

Fortinet Azure SharePoint server breach

Regions
Worldwide

Industries
Internet services

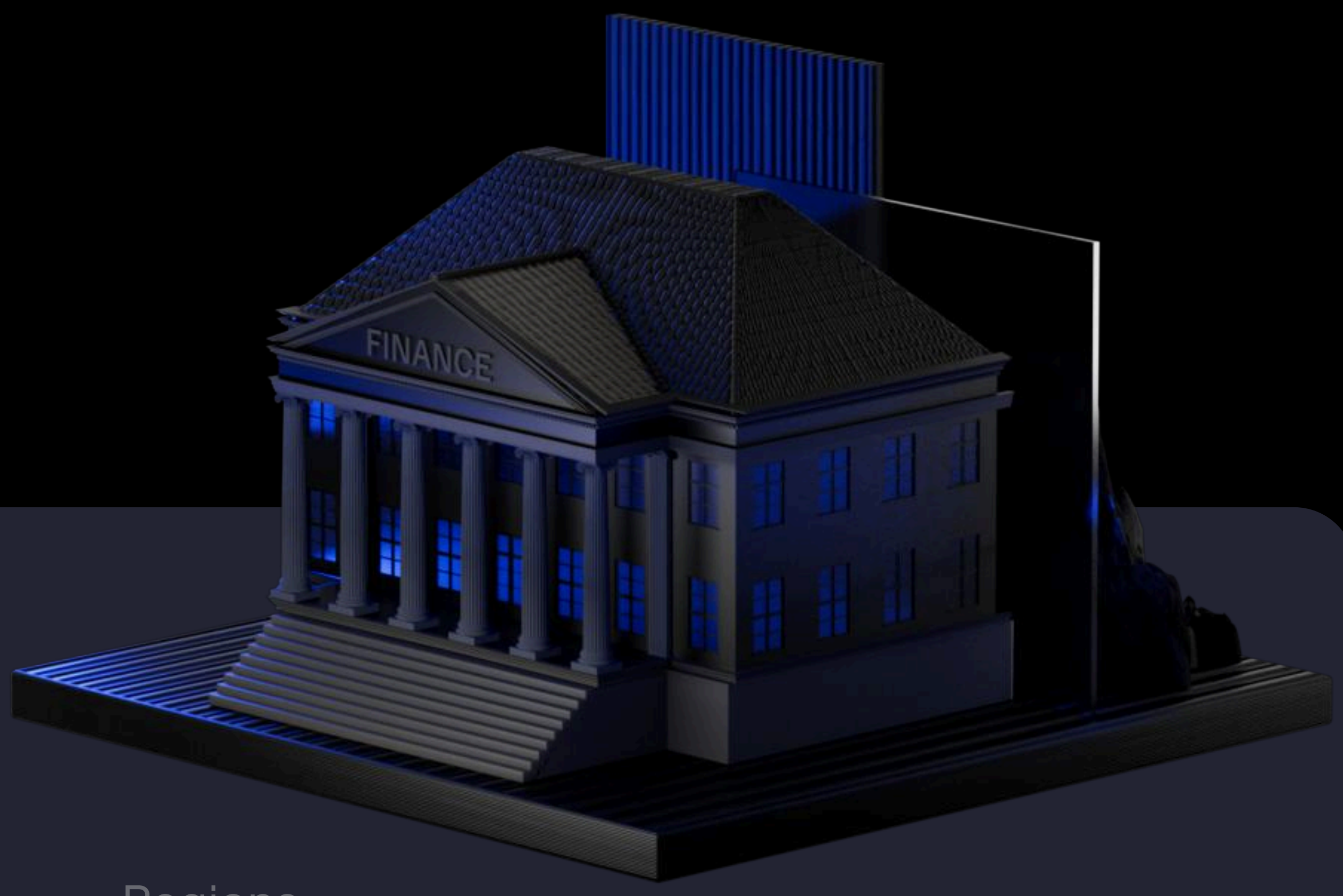
On September 12, 2024, an attacker, using the newly created Breachforums account "FortiBitch," claimed responsibility for the theft of 440 gigabytes of data from cybersecurity company Fortinet's Azure Sharepoint server. The attacker indicated an intention to ransom the stolen data but mentioned that Fortinet refused to comply with the demand. The attacker posted a URL to an S3 Bucket server where the stolen data was allegedly uploaded.

On September 13, 2024, the server hosting the Fortinet data leak was taken down, with the attacker reporting that the server was offline due to its extremely low bandwidth, preventing any data from being downloaded during its brief availability. The attacker promised to republish the data through another method.

As of October 11, 2024, the attacker has remained inactive on the forum since September 13, and no other individual has managed to download or republish the data. The hacker community on Breachforums offered a reward for anyone who could republish the stolen data, but as of now, it has not been shared by anyone.

Fortinet has since confirmed the breach in a public statement.

Finance



Deepfake financial fraud in Indonesia

Regions
Worldwide

Industries
Finance

In August 2024, a prominent Indonesian financial institution reported a deepfake fraud incident within its mobile application, prompting a comprehensive investigation by Group-IB.

Despite implementing robust, multi-layered security measures — including anti-emulation, anti-virtual environments, anti-hooking mechanisms, and Real-Time Application Self-Protection (RASP) — attackers successfully bypassed biometric verification using AI-generated deepfake images.

Fraudsters obtained victims' IDs through malware, social media, and dark web sources, then altered facial features, clothing, and hairstyles to manipulate identity verification systems. This allowed them to bypass digital Know Your Customer (KYC) procedures, including facial recognition and liveness detection, and fraudulently access financial services.

Group-IB's investigation uncovered over 1,100 deepfake fraud attempts targeting the institution's loan application process. The increasing use of deepfake technology in financial fraud poses severe risks, with estimated losses in Indonesia alone reaching $138.5 million USD. Beyond financial damage, these attacks threaten personal security, institutional trust, and national stability.

This incident highlights a significant shift in cybercriminal tactics, as AI-powered tools enable fraudsters to circumvent traditional security measures with alarming efficiency.

ATM attacks

Regions
Worldwide

Industries
Finance

In 2024, a renewed surge in ATM-related cyber threats was observed, with various groups employing different tactics to achieve a common goal—illicit financial gain. Group-IB identified three key cases highlighting this trend.

Michelangelo and the Sale of FASTCash 2.0 Source Code

A cybercriminal known as Michelangelo surfaced on a dark web forum, claiming to be selling the FASTCash 2.0 source code. He alleged that he had acquired it through a partnership with the original developer, who had previously sold the malware to multiple groups, including Lazarus.

Through interactions with the threat actor, Group-IB obtained intelligence on the malware, now identified as Renaski Proc. This trojan is designed to compromise payment processing servers, intercept ISO8583 messages, and manipulate them to approve fraudulent transactions. Renaski Proc has variants for both Windows and IBM AIX. Delivered as a DLL file, it is injected into legitimate processes to evade detection and facilitate unauthorized transactions.

Lazarus Expands FASTCash with a Linux Variant

The North Korean threat group Lazarus has been observed using a Linux variant of the well-known FASTCash malware as part of a financially motivated campaign. This malware is deployed on payment switches within compromised networks that process card transactions, enabling unauthorized ATM cash withdrawals.

Previously, FASTCash was documented in IBM AIX (FASTCash for UNIX) and Microsoft Windows (FASTCash for Windows). The discovery of a Linux variant expands the known capabilities of this malware family, highlighting Lazarus's continued evolution in targeting financial institutions.

UNC1945's Physical Attack Using a Raspberry Pi

Group-IB's Incident Response team detected the presence of UNC1945 within a financial institution in Indonesia. During the investigation, a Raspberry Pi device was found connected to a switch behind an ATM, directly linked to the ATM network segment.

Although the full impact could not be determined, evidence suggests that the attackers were detected before they could complete their fraudulent withdrawals. This case represents a unique and unconventional method of infiltrating a financial organization's network, blending physical and cyber tactics.

Crowdstrike global outage

Regions
Worldwide

Industries
All

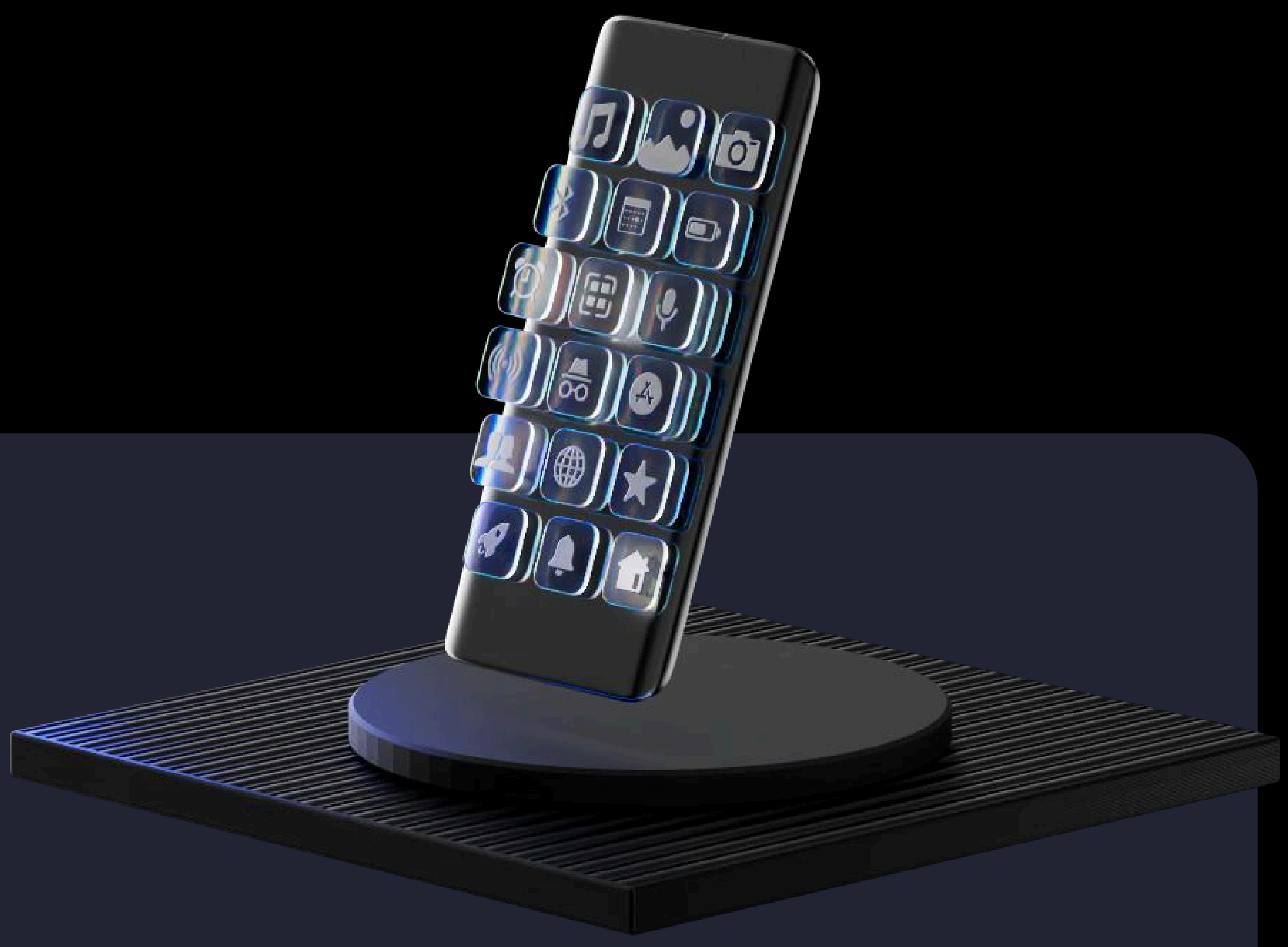
The most globally disruptive incident this year was not a direct cyberattack but rather a widespread failure linked to a malfunction in endpoint detection and response (EDR) software for Windows systems. The Crowdstrike outage led to a cascading disruption across multiple industries worldwide.

The event, now widely discussed in cybersecurity circles, stemmed from insufficient patch testing prior to deployment and a heavy reliance on a single security solution. The malfunction acted as a single point of failure for numerous organizations worldwide. For example, the outage caused disruption to banks, utilities, media, TV, cellular and internet providers. Civil aviation authorities in many countries announced the suspension of flights due to this incident.

Additionally, cybercriminals were quick to exploit the situation, launching phishing campaigns, registering fraudulent domains, and spreading malware. Many impersonated support services, using the IT disruptions as a pretext to deceive victims. Despite legitimate recovery efforts, the widespread nature of the issue created opportunities for cyber fraud.

Beyond the immediate impact, the incident has broader regulatory implications for frameworks like Europe's NIS2 Directive and DORA Regulation, which emphasize operational resilience, supply chain security, and incident response. The disruptions caused by this failure highlight key vulnerabilities that organizations will need to address to align with these compliance requirements.

Mobile services



Fake mobile Android trading and dating apps

Regions
Worldwide

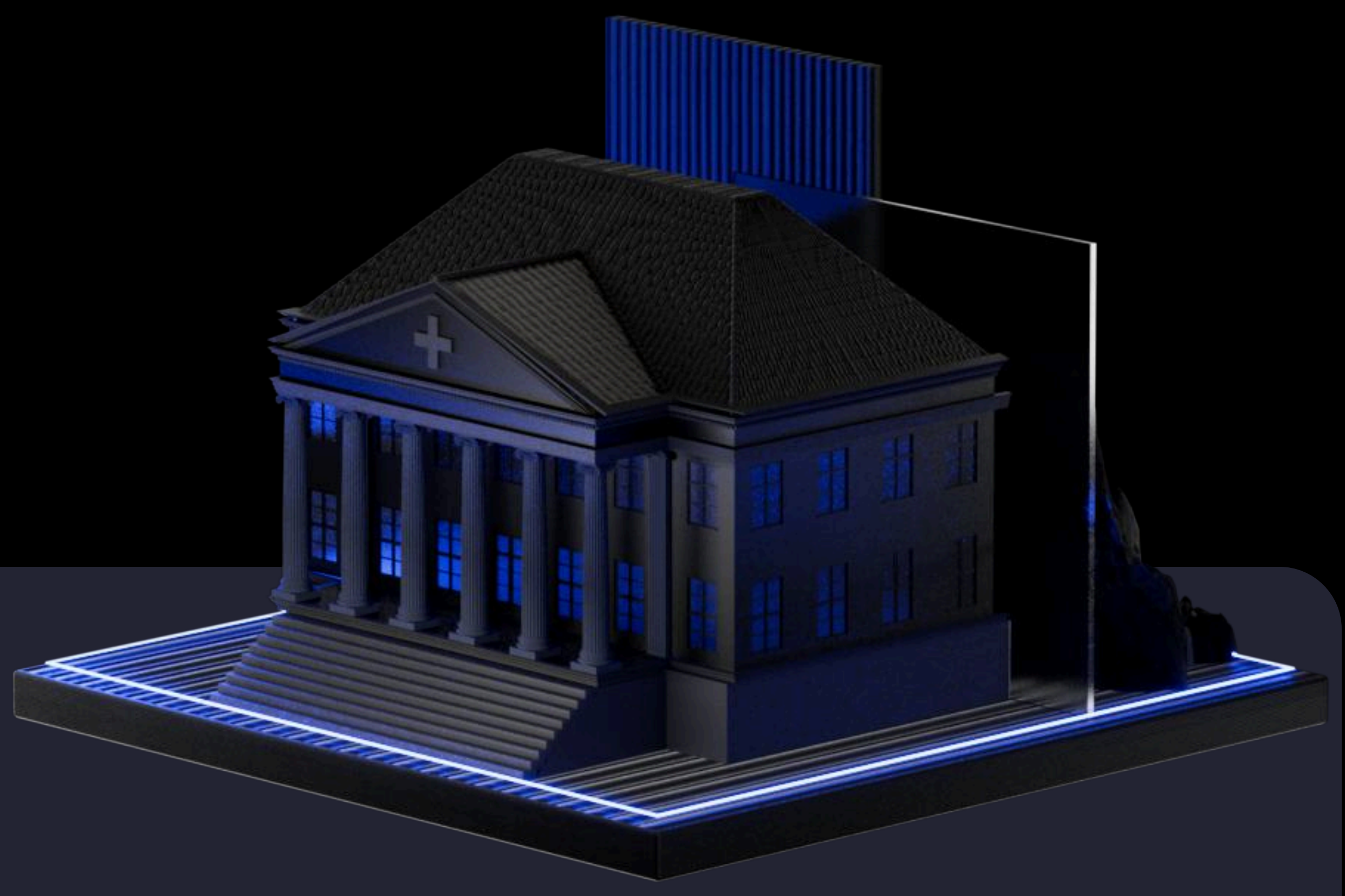
Industries
Mobile services

Since May 2024, Group-IB analysts have observed a surge in fake mobile trading applications targeting victims globally. Developed using the UniApp Framework, these apps primarily target Android devices, with some variants also infiltrating the Google Play Store and Apple App Store. A notable iOS version, disguised as a mathematical tool, required an invitation code for access, indicating targeted attacks.

Cybercriminals exploit dating apps and social engineering tactics to lure victims into funding fraudulent trading accounts, ultimately stealing their money. Once trust is established, victims are prompted to upload personal identification documents and make deposits. After these apps were removed from official app stores, attackers shifted to phishing websites, using enterprise developer profiles to distribute fake iOS versions.

These scams have been detected across the Asia Pacific, Europe, the Middle East, and Africa, demonstrating their widespread reach. The use of trusted app stores and web-based applications makes detection more difficult. Users are advised to thoroughly verify trading platforms before sharing personal information or making financial transactions.

Healthcare



Ascension ransomware attack

Regions
North America

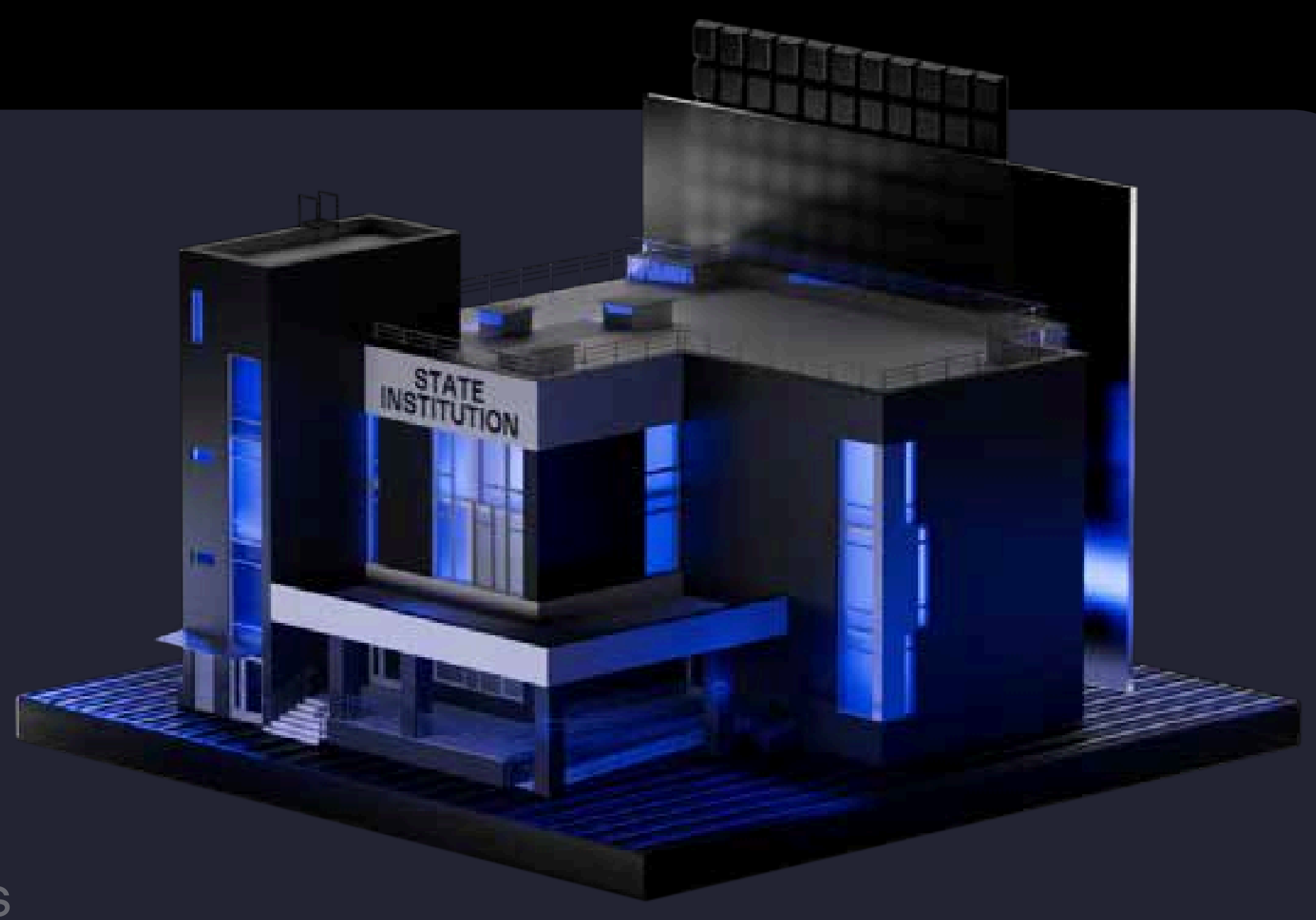
Industries
Healthcare

In May 2024, Ascension, one of the largest U.S. health systems—comprising approximately 140 hospitals across 19 states—suffered a ransomware attack that severely disrupted its operations. For over two weeks, staff were forced to rely on manual procedures due to widespread system outages.

Ascension reported a net loss of $1.1 billion for 2024, attributing a significant portion of this loss to the cyberattack's impact. This incident highlights the healthcare sector's growing vulnerability to ransomware attacks, where operational disruptions can severely affect patient care and institutional stability.

The attack also reflects a broader trend of cybercriminals increasingly targeting critical infrastructure, leveraging disruption as a powerful bargaining tool. It serves as a stark reminder of the urgent need to strengthen cybersecurity defenses in healthcare, where the stakes extend beyond financial losses to patient safety and public trust.

Government and military



UK Ministry of Defence's payroll system leak

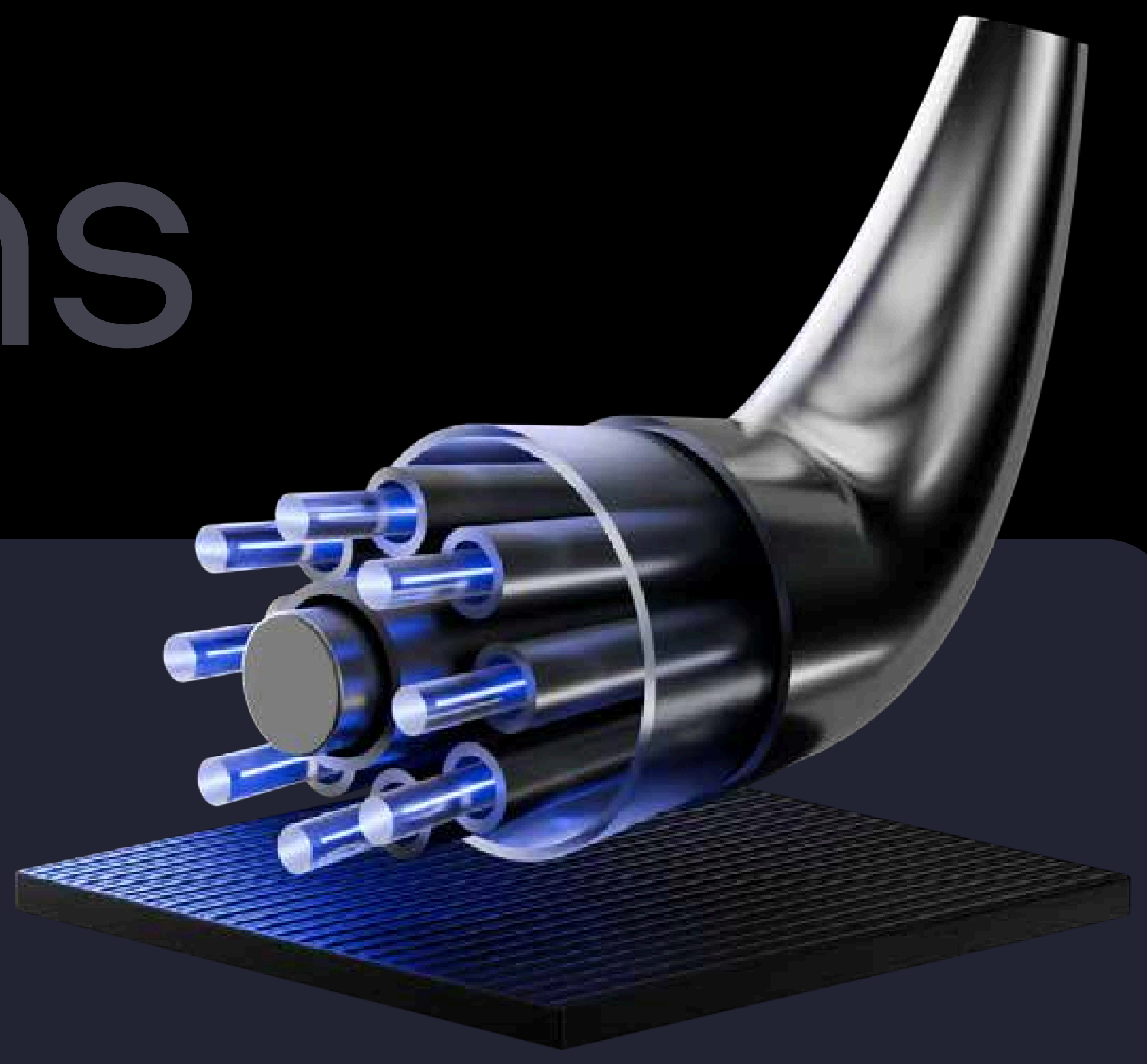
Regions
Europe

Industries
Government and military

In May 2024, a cyberattack on the UK Ministry of Defence's payroll system significantly impacted the cybersecurity landscape, exposing the sensitive personal information of 270,000 current and former military personnel. The breach raised serious concerns about the vulnerability of critical national infrastructure and underscored the urgent need for stricter supply chain security practices, particularly when working with third-party vendors handling sensitive data such as payroll information.

Initial reports suggest the attack may have been orchestrated by a state-affiliated threat actor using advanced persistence techniques to evade detection, further amplifying the severity of the breach.

Telecommunications



Submarine telecommunications cables disruptions

Regions
Europe, Africa

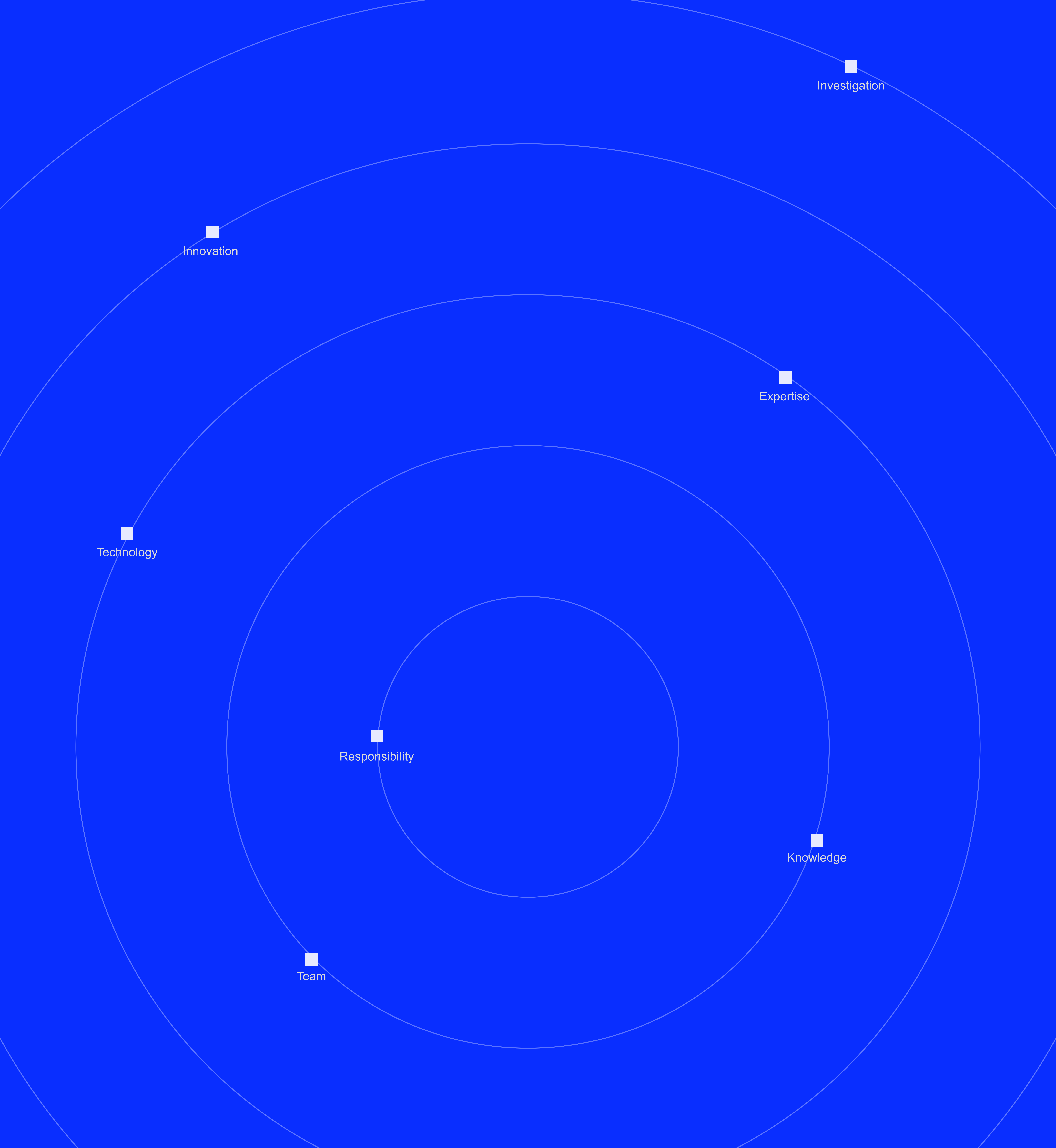
Industries
Telecommunications

Submarine telecommunications cables power over 99% of global data exchange, yet they remain vulnerable to natural disasters, aging infrastructure, and human activities like fishing and anchoring. The International Cable Protection Committee (ICPC) reports 150–200 faults annually, requiring around three repairs per week.

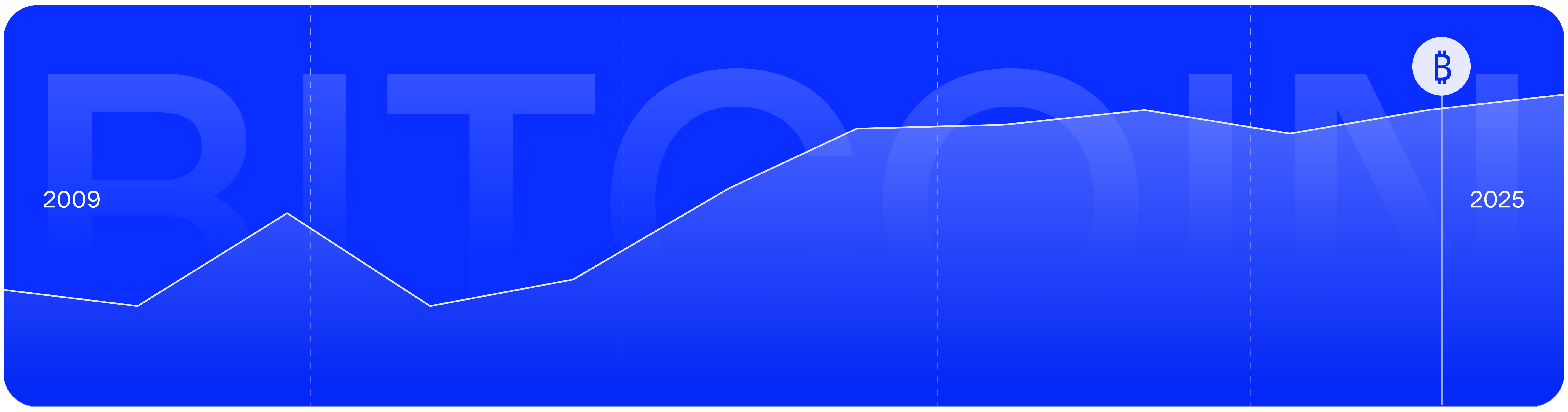
A growing concern is sabotage by rival nations. In February, four major cables—AAE-1, Seacom, EIG, and TGN—were severed in the Red Sea, disrupting internet access for over 100 million people across West and North Africa and affecting 70% of data traffic between Europe and Asia. The damage was likely caused by an intentional anchor drag.

More recently, on November 17, 2024, the BCS East-West Interlink cable between Lithuania and Sweden and the C-Lion1 cable between Finland and Germany were severed, disrupting telecom services in both countries.

In response to rising threats, the United Nations established its first advisory body for subsea cable resilience on November 29, managed by the International Telecommunication Union (ITU). This initiative aims to enhance the security and stability of critical global communications infrastructure.



Chapter 3: Forecasts & Recommendations



01 Growth of bitcoin & cryptocurrencies

As more countries, including major economies, recognize the national interest in developing cryptocurrencies, we are witnessing an explosive growth in this digital asset class. In 2025 and the foreseeable future, we expect broader adoption of cryptocurrencies, particularly among cybercriminals seeking to legitimize their earnings. As they amass wealth through ransomware attacks, data breaches, and other illicit activities, these criminals will likely look for ways to convert their digital gains into legitimate assets. This could lead to increased use of cryptocurrency exchanges and services that facilitate the conversion of crypto to fiat currency. However, with growing regulatory scrutiny, they may encounter more challenges in finding safe avenues for laundering their funds.

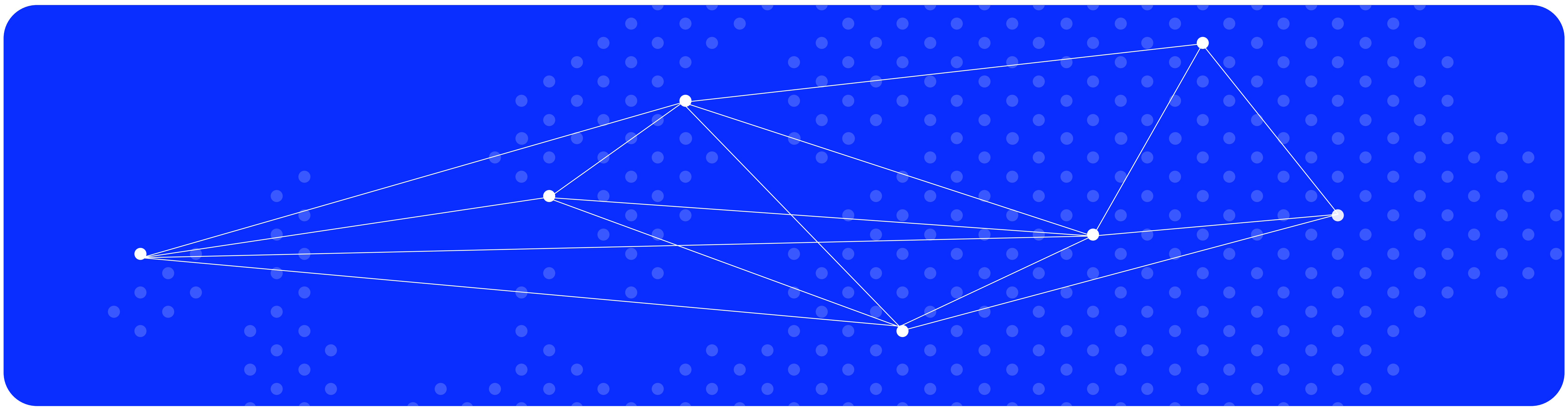
On the other hand, the rise of Decentralized Finance (DeFi) platforms, which offer decentralized lending, borrowing, and trading services, introduces new security challenges. These platforms may provide cybercriminals with opportunities to obscure their transactions, making it even more difficult for law enforcement to trace illicit funds. As a result, organizations will need to adopt enhanced monitoring capabilities and develop robust strategies to detect and mitigate risks associated with cryptocurrency transactions.

Moreover, the rising interest in cryptocurrencies will likely give rise to an increase in scam projects targeting unsuspecting investors. As the market expands, so too does the opportunity for fraudsters to exploit the lack of regulation and oversight in certain areas.

It is essential for cryptocurrency platforms to undergo a security audit to assess every aspect of their environment, including the blockchain network, website, application, and smart contracts for underlying risks.

Establishing strong defenses against Anti-Money Laundering (AML) risks are crucial. Group-IB Fraud Protection (FP) helps detect illegitimate accounts and account takeovers that could be exploited for fraud. It enables tracking individual scammers, mapping relationships, and identifying mule activity across different accounts to uncover fraud networks.

Many crypto-related threats and fraud schemes involve brand impersonation, which requires real-time and effective detection. With Group-IB Digital Risk Protection (DRP), you can monitor, identify, and take down brand abuse targeting your company, including phishing domains, fraudulent websites, fake social media accounts, deceptive advertisements, and counterfeit mobile apps.



02 Deglobalization on the Internet

The trend of deglobalization of the internet is expected to shift the web from a unified, borderless open space to a patchwork of controlled regional internets, reshaping the future of the cybersecurity landscape. This is particularly evident as countries like Russia implement stringent regulations over their local internet segments. By attacking anonymity, cracking down on VPN usage, and preparing to block foreign services, these regulations are likely to create a more controlled and monitored internet environment.

On the other hand, we may see a significant decrease in the number of amateur scammers who rely on the internet's anonymity to conduct their activities. The increased difficulty in operating anonymously could deter many low-level cybercriminals, leading to a decline in opportunistic scams and phishing attacks. However, it's important to note that Advanced Persistent Threats (APTs) are unlikely to be significantly affected by these regulations. APTs, often state-sponsored or highly organized groups, will continue to operate with sophisticated techniques and resources, adapting to the changing landscape.

Moreover, other countries may follow suit, seeking to create their own highly regulated internet ecosystems that are partially separated from the global World Wide Web. This fragmentation could lead to a patchwork of regulations, making it increasingly challenging for organizations to navigate compliance and security requirements across different jurisdictions. Companies will need to invest in robust cybersecurity measures and stay informed about the evolving regulatory landscape to protect their operations and data.

This trend has both positive and negative implications for cybersecurity at national, corporate, and individual levels. As a consequence, cybercriminals may be forced to adapt their tactics, potentially leading to a decline in certain types of scams in heavily regulated regions. However, this could also push some threat actors to operate in less regulated environments, creating new hotspots for cybercrime. Organizations will need to stay vigilant and adapt their cybersecurity strategies to navigate this evolving landscape.

To effectively navigate the evolving cybersecurity landscape, organizations should monitor global cyber threats, particularly in less regulated regions and emerging hotspots, while considering data localization strategies to ensure compliance and security through the use of local data centers and partnerships with cybersecurity firms that adopt a “glocal” approach, blending global reach with in-depth knowledge of regional threat landscapes.

Establishing collaborations with local law enforcement and cybersecurity agencies is essential for staying informed about regional threats and participating in information-sharing initiatives. Additionally, organizations must continuously update their compliance frameworks to align with local laws on data protection and cybersecurity. Investing in advanced threat detection systems will enhance the ability to identify sophisticated threats, while also preparing for increased regulatory scrutiny by ensuring transparency in cybersecurity practices and compliance reporting will help build trust with customers and partners.

03 Messaging apps regulations & the migration of threat actors

Messaging platforms have become one of the primary communication channels for both users and organizations, posing significant cybersecurity risks due to the exchange of sensitive data. However, with increasing scrutiny on platforms like Telegram, we can expect a shift in how threat actors communicate and coordinate their activities. As governments implement regulations to curb illegal activities on these platforms, cybercriminals may seek refuge in alternative communication channels.

This migration could lead to a resurgence of activity on dark forums and encrypted messaging services like Signal. These platforms offer a higher degree of anonymity and security, making them attractive options for threat actors seeking to evade detection.

As a result, organizations will need to enhance their threat intelligence capabilities to monitor these emerging channels. Understanding the dynamics of these platforms and the communities within them will be crucial for identifying potential threats and mitigating risks. Additionally, organizations should consider investing in advanced analytics and machine learning tools to detect communication patterns that may indicate malicious intent.

Social Media Monitoring should be an essential part of digital businesses to identify risks in time. Businesses can enable it with Group-IB Threat Intelligence which helps users scour the dark web for concrete evidence of illegal mentions, data leaks, and other potential attacks. It also provides unique insights into the top threat actors active in their region and industry, their proclivity of targeting them, as well as the tools, techniques, frequency of use, and infrastructure they rely on.

It deeply analyzes the dark web content, including discreet usernames, aliases, and historical activity data of threat actors, to build a comprehensive threat profile. By correlating various posts in underground forums, it uncovers hidden connections between threat actors — exposing the complete scope and extent of their activities.

04 Changes in ransomware ecosystems

The recent law enforcement operations targeting cybercrime, particularly ransomware, had a profound impact on the global ransomware ecosystem in 2024. Key events such as Operation Cronos, Operation Endgame, Operation Morpheus, and Operation Magnus have demonstrated a concerted effort by authorities to dismantle criminal networks. International collaboration against ransomware,such as the Counter Ransomware Initiative—bringing together over 60 countries and organizations, including INTERPOL—further reinforces global efforts to combat ransomware and enhance coordinated responses. The arrest of individuals associated with groups such as Scattered Spider in 2024 further emphasizes the importance of this crackdown. Additionally, the exit scams carried out by ALPHV and NoEscape have undermined confidence among ransomware operators, leading to uncertainty within the community.

As a result, we may witness a notable shift in the ransomware tactics. There is growing concern of an increase in attacks targeting healthcare and critical infrastructure, as these sectors may be perceived as vulnerable and high-impact targets. Furthermore, governmental entities, including local agencies, may face similar threats, with attackers looking to exploit perceived weaknesses in public sector cybersecurity.

The ransomware landscape may also see a transformation in extortion methods. Some groups may move away from double extortion—where data is both encrypted and threatened with public release—to extortion-only attacks. This could lead to a diversification of tactics and the rise of new ransomware and extortion methods in 2025, as criminals adapt to the changing environment and seek to evade law enforcement scrutiny.

Evaluating the impact of these developments remains challenging. Although discussions in the U.S. Congress have highlighted concerns about hostile foreign cyber actors, the anticipated decrease in companies disclosing ransomware incidents on data leak sites (DLS) has not materialized. Additionally, despite expectations of a decline in ransom payments, high-profile cases—such as Black Suit demanding $25 million and Dark Angel seeking $75 million—indicate that the financial stakes in ransomware attacks remain high.

The resilience of cybercriminals, coupled with the emergence of new groups, suggests that the threat of ransomware will continue to evolve, necessitating ongoing vigilance and adaptation from both law enforcement and organizations at risk. Leveraging an advanced, real-time threat detection and response technology that comprehensively covers your infrastructure is advised. Group-IB Managed Extended Detection and Response (MXDR) identifies ransomware indicators across your managed endpoints, email, web, and network, issuing automated responses while your team analyzes further mitigation actions.

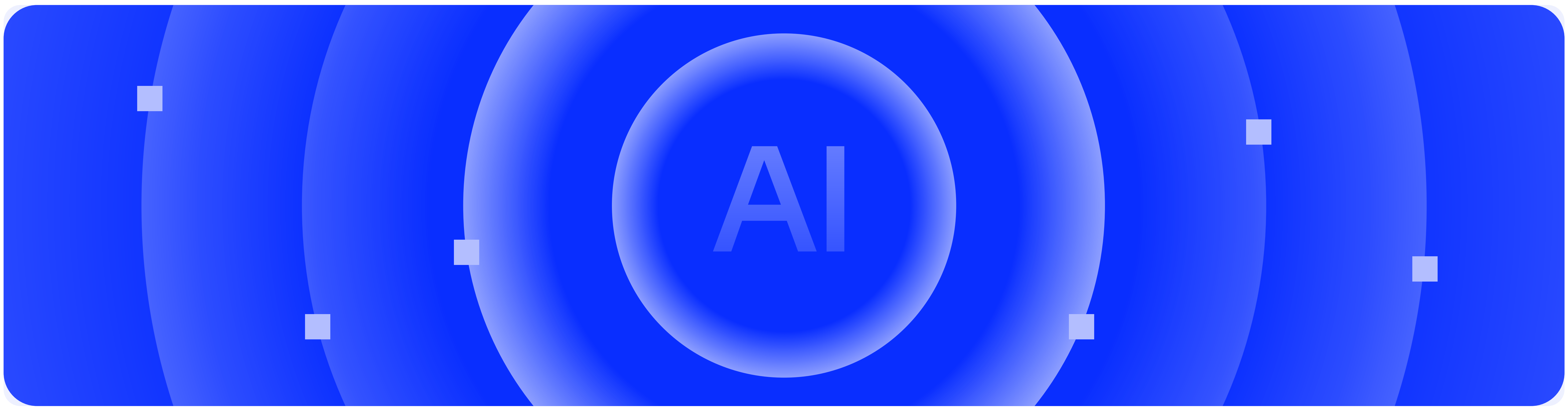
Having an Incident Response Retainer ensures your business is best prepared if ransomware strikes. With experienced professionals by your side, you can enable a swift and effective response to mitigate damage, collect forensic evidence, and recover data.

05 United Nations Cybercrime convention

The adoption of the UN Cybercrime convention in December 2024 represents a landmark step in global efforts to combat cybercrime. As the first comprehensive international treaty on this issue, the Convention provides a framework for nations to enhance their ability to prevent, investigate, and prosecute cybercrime, as well as to strengthen international cooperation in sharing electronic evidence for serious offenses. While its immediate impact may be limited, it establishes a foundation for greater standardization in cybersecurity practices worldwide. But even as nations work toward standardized cybersecurity practices, cybercriminals may be forced to adapt before stricter regulations take effect. However, some threat actors may exploit legal frameworks to operate under the guise of legitimacy.

To navigate the evolving regulatory landscape, cybersecurity organizations must integrate legal awareness into their operations. Training incident response teams on relevant laws and permissible actions will improve their ability to prevent attacks and collaborate with information intermediaries. This is especially valuable within a Digital Risk Protection framework.

Building regional cybersecurity alliances among businesses, governments, and academic institutions can facilitate knowledge sharing and strengthen collective defenses. Additionally, investing in real-time tracking tools for regulatory updates will help organizations remain compliant and responsive to emerging threats. By adopting these strategies, cybersecurity companies can align with legal requirements while enhancing protection for their assets and clients.



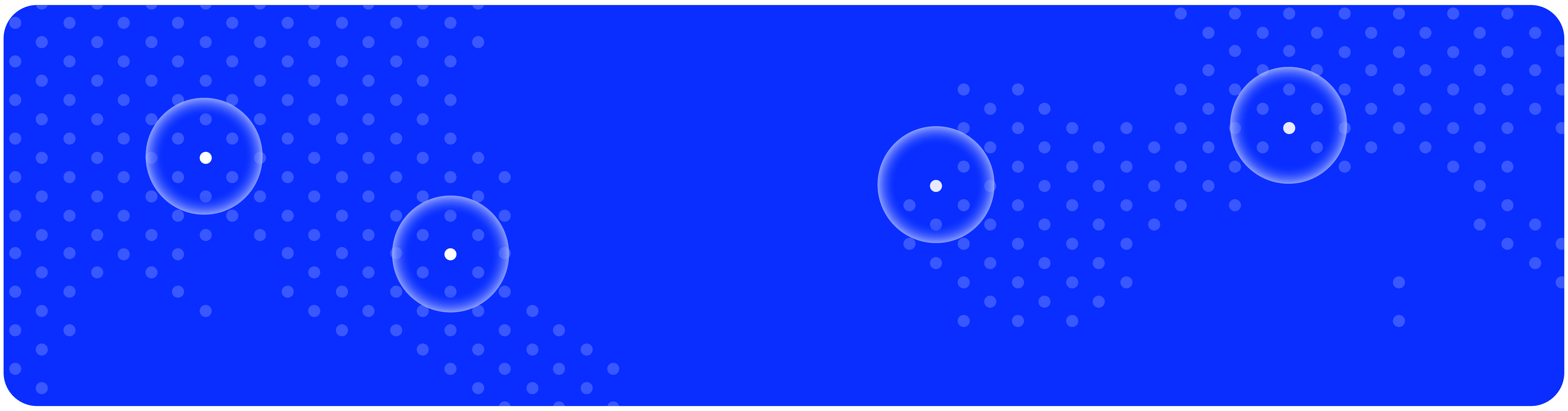
06 Misuse of artificial intelligence for attacks

As AI technology advances, its role in cyberattacks is expected to grow significantly by 2025. Cybercriminals will likely exploit AI to develop sophisticated attacks, including deepfake technology, which enables realistic impersonations to bypass security measures and access sensitive data.

Malicious AI-driven systems pose a major threat, automating phishing campaigns, vulnerability scanning, and coordinated attacks on critical infrastructure. As AI tools become more accessible, cybercrime will escalate in frequency and severity.

To counter these threats, organizations must adopt AI-powered cybersecurity solutions, such as advanced threat detection, anomaly detection, and automated response systems. A "security by design" approach is essential, as AI systems, with their extensive access, are prime targets for attacks. Businesses should conduct specialized AI security audits and implement deepfake detection tools while training employees to recognize manipulated content.

Embedding security measures into AI development and deployment will help safeguard assets and maintain operational integrity in an increasingly AI-driven world. Learn more in our Cybersecurity X AI e-guide.



07 Rising political tensions and the emergence of cyber wars

The rising geopolitical tensions are fueling an increase of state-sanctioned cyber warfare, with nations seeking to assert their influence and protect or further their national interests. In 2025, we can expect a surge in state-sponsored cyberattacks targeting critical infrastructure, government systems, and private enterprises.

In this environment, some nations, or coalitions of countries, may choose to deglobalize their digital infrastructure, creating isolated networks that are less susceptible to foreign interference. While this fragmentation of the internet could result in a patchwork of national networks—each with its own regulations and security protocols—aims to reduce foreign cyber threats, it could complicate international relations and pose significant challenges for organizations operating across borders.

As countries invest in their own cybersecurity capabilities, we may see an increase in the development of homegrown technologies and services, which could potentially lead to a decline in reliance on foreign software and hardware, as nations prioritize national security over global collaboration. However, these efforts of deglobalization could introduce opportunities for cybercriminals, who may exploit the vulnerabilities inherent in less mature domestic technologies.

It is important to recognize that attacks can take place not only in the cyber realm but also in the physical domain. We can anticipate various forms of sabotage targeting key infrastructure, such as cable cuts, orchestrated power outages, assaults on data centers, and disruptions to satellite operations. In light of these threats, governments are likely to prioritize the development and deployment of physical measures for threat detection and prevention. This may include implementing critical infrastructure monitoring systems utilizing drones and AI technologies, establishing redundant infrastructure, and enhancing armed security for a greater number of critical nodes.

In this context, cybersecurity companies, particularly those with access to critical infrastructure, must also prioritize the physical security of their servers and employees. This includes conducting thorough risk assessments to identify vulnerabilities in physical security measures and implementing robust protocols to safeguard against potential breaches. Additionally, fostering a culture of security awareness among employees can help ensure that everyone is vigilant and prepared to respond to physical threats. By integrating physical security considerations into their overall cybersecurity strategy, organizations can create a more resilient defense against the evolving landscape of threats that span both cyber and physical domains.

08 Involvement of tech manufacturers in government attacks

As political tensions escalate, there is a growing concern that popular software and device manufacturers may become unwitting participants in government-led cyberattacks. This could occur through various means, including the introduction of backdoors, exploitation of zero-day vulnerabilities, or compromises by adversaries.

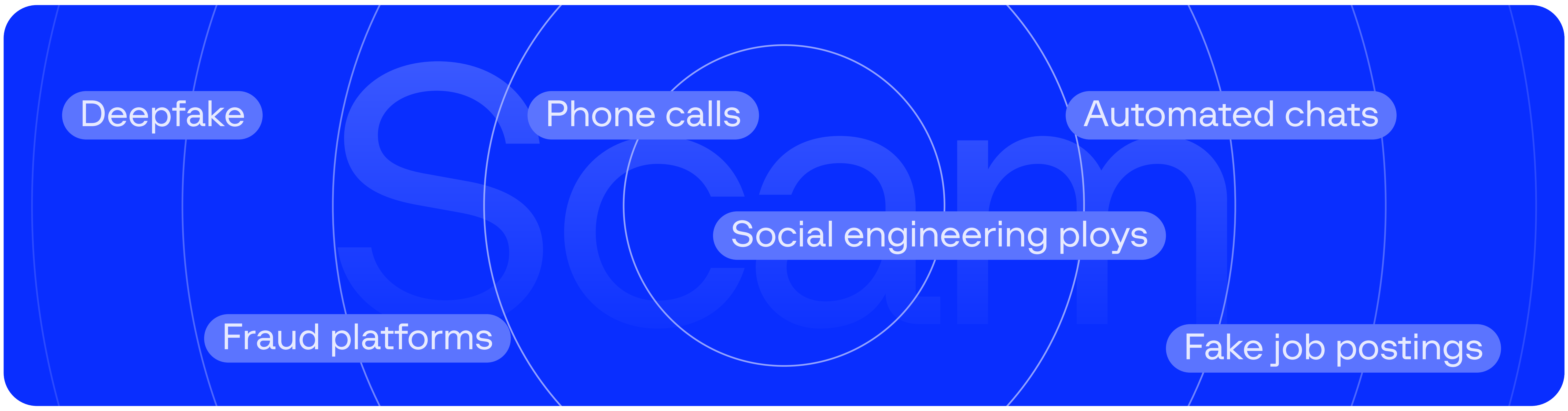
For instance, if a government were to mandate that a software provider include backdoors for surveillance purposes, this could expose users to significant risks. Such actions could lead to widespread vulnerabilities that cybercriminals could exploit, undermining the security of millions of users. Additionally, if these backdoors were discovered, the reputational damage to the software provider could be severe, resulting in a loss of trust among consumers and businesses alike.

Moreover, the potential for adversaries to compromise popular software or devices raises serious concerns about supply chain security. If a widely used application or device is found to have been manipulated by a foreign adversary, the fallout could be catastrophic, leading to data breaches, financial losses, and even national security threats.

As the involvement of software and device producers in government attacks becomes more apparent, we can expect a significant backlash from consumers and businesses. The exposure of these relationships could lead to a loss of reputation for affected companies, resulting in decreased user trust and potential financial repercussions.

Organizations that rely on these compromised services may find themselves in a precarious position, facing increased scrutiny and pressure to enhance their cybersecurity measures. This could lead to a shift in consumer behavior, with users seeking alternatives that prioritize privacy and security over convenience.

In response to these challenges, companies will need to adopt a proactive approach to cybersecurity, focusing on transparency and accountability. This may involve conducting regular security audits, engaging in third-party assessments, and communicating openly with users about potential risks and vulnerabilities.



09 Shapeshifting and hyper-scaling fraud

AI's influence is seen across all cyber activities, and assumingly, fraudsters are finding innovative ways to exploit it for scam automation, marketing, and distribution. Deepfake technology, social engineering ploys, automated chats, emails, and phone calls are now part of advanced scams to create even more convincing fraud platforms, online affiliate programs, and fabricated identities and credentials to deceive and defraud victims.

A growing component of the scam ecosystem is scam call centers. Once confined to less developed regions due to limited legislative power and lax enforcement, these centers are forming an illegal global economy. Crime networks' financial schemes now either involve individuals directly—through trafficking to scamming compounds—or indirectly, by luring people into fraudulent activities through fake job postings, pig butchering schemes, and other scam-related content.

Increasing scams have reportedly caused double-digit billion losses. To capitalize on this opportunity, cybercriminals have extended their operations to other regions, such as the Middle East, Eastern Europe, Latin America, West Africa, and the United States.

They are likely to emerge in mature economies in the future, with greater access to potential targets. Potential vulnerabilities such as exploitable legal measures, enforcement mechanisms, and evolving tactics based on the complexity of mature systems may further the growth.

The need to build an effective defense against fraud and scam threats is immediate, and it goes beyond siloed defenses. It involves building a collective shield through intelligence sharing among financial institutions – including fraud schemes, mule accounts, detection logic, and effective counterstrategies. Such collaboration ensures that banks protect their clients and ensures international collaboration to identify scams and means of disinformation.

Group-IB continuously upgrades its patented Fraud Protection solution to defend against emerging fraud schemes. We empower our customers and industries with targeted fraud intelligence across the entire kill chain, built into the solution.

In one of its previous reports, Gartner recognized Group-IB as one of the only two vendors providing organizations with the capability to identify Tactics, Techniques, and Procedures (TTPs) used by fraudsters early in the Cyber Fraud Attack Chain.

That said, identity authentication also remains critical for businesses to stopping fraud early in its tracks. Group-IB Fraud Protection facilitates this through multifactorial verification – behavioral biometrics, device fingerprinting, anti-money laundering (AML) systems, and more. These checks also help in compliance reporting, risk scoring, and enhanced internal and external threat detection, among other use cases.

10 Cloud targeting

Everything is moving to the cloud. Businesses are leveraging the efficiency, extensive data exchange capabilities, and virtually limitless potential of cloud and multi-cloud environments to collaborate and grow. However, this transition also attracts attackers who increasingly target cloud infrastructures by creating malicious services and launching effective phishing campaigns to infiltrate cloud environments.

Common challenges such as data migration vulnerabilities, network security misconfigurations, insecure APIs, access management flaws, and weak encryption practices only amplify these risks. Lax security in configuring, accessing, and managing cloud infrastructure can leave your organization more exposed than secure, making cloud protection essential.

It is advised to constantly run cloud infrastructure audits, use automated monitoring tools to identify vulnerabilities in the environment, and implement strict hygiene measures company-wide to prevent threats such as cloud jacking, privacy concerns, and more aggressive threats such as ransomware.

To mitigate the security risks associated with serverless environments, infrastructure providers—such as AWS, Azure, or Google Cloud—and businesses can benefit from the expertise of leading cybersecurity service providers. For example, Group-IB's current partnership with AWS focuses on countering threats like phishing, email scams, user account fraud, payment fraud, malicious bots, mobile Trojans, and more. These threats are detected and prevented effectively through real-time monitoring and analysis of user behavior across multiple sources.

11 Identity-based attacks call for adaptive verification

Linking every online interaction to the real user behind it has become critical to ensuring the integrity and security of the digital trade. Identity exploitation is a growing concern, and current security practices fail to curb it.

A common practice of people reusing passwords across multiple accounts increases the risk of data leaks and exposed credentials.

Exploiting weaknesses in authentication methods is another form of identity exploitation. Authentication via Google, Microsoft, and other identity providers uses an SSO-based login mechanism, where attackers only need to bypass a single verification layer by obtaining credentials through advanced phishing or malware attacks.

Once credentials are compromised, attackers can impersonate users across various platforms, and even two-factor authentication (2FA) may not prevent this. This facilitates the creation of fake accounts, cross-IDP impersonation, and multi-access attacks.

As adversaries increasingly exploit systems to fulfill malicious objectives, verification mechanisms must evolve to counter modern identity-based attacks, fraud, and social engineering threats. Adaptive verification is the successive development in authentication, surpassing MFA (multi-factor authentication) and 2FA (two-factor authentication). This advanced method authenticates runtime users based on risk factors like location, device integrity, and behavior patterns.

With the rise of synthetic identity fraud, media manipulation, and exploits targeting system vulnerabilities, adopting multifactorial verification protocols might become a norm—especially in critical sectors such as banking and finance.

To keep pace with the momentum, Group-IB Fraud Protection offers risk-based authentication, ensuring precise user verification by assessing multiple parameters. These measures significantly reduce the risk of identity exploitation.

Fight Against Cybercrime

GROUP-IB