2025. 12

AhnLab

2025 Threat Landscape
2026 Outlook

Overview

Contents

Overview

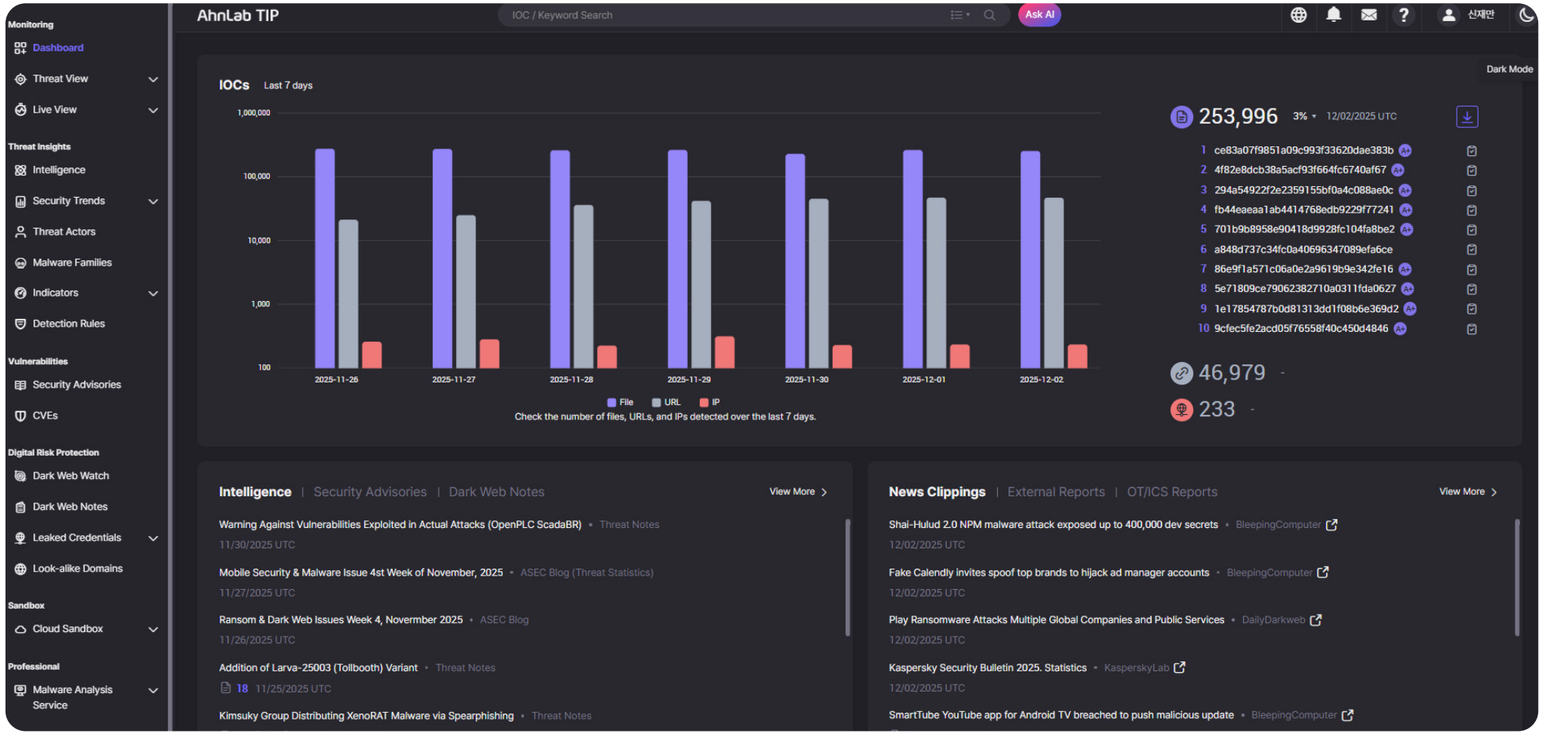
Intro

This report examines major security issues and trends from Q4 2024 to Q3 2025 and presents an outlook on cyber threats expected in 2026, based on our analysis provided through AhnLab TIP.

Our threat intelligence platform, AhnLab TIP collects, analyzes, and triages diverse threat information, including malware, security incidents, threat actors, vulnerabilities, indicators of compromise (IoCs), and security news. It enables customers to develop security strategies and make informed decisions based on actionable threat intelligence.

You can find further details on AhnLab TIP on our website and the AhnLab TIP portal.

→ Visit our website
→ Visit AhnLab TIP portal



[Image] AhnLab TIP dashboard

Overview

Our Threat Intelligence in Numbers

2,258
Threat Intelligence Articles

Over the past year, we published 2,258 pieces of content on the "Intelligence" menu on AhnLab TIP.

- **ASEC Notes**: Rapid delivery of the latest threat intelligence
- **Dark Web Notes**: Providing high-risk info identified in dark web
- **ASEC Blog**: Quick analysis of emerging threats
- **Trend Report**: Analyzing the trend of malware, phishing, etc.
- **Analysis Report**: Analysis into APTs, incidents, and others

661
Security Advisories

Security advisories provide rapid information on software vulnerabilities and high-risk issues, along with recommended mitigation measures.

Tens of Thousands IoCs Daily
30% - Our Exclusive IoCs

We provide thousands to tens of thousands of IoCs—such as malicious files, URLs, IPs, and domains—each day, enabling customers to leverage them for threat response.

We operate one of the largest threat detection sensor networks, and **approximately 30% of IoCs are AhnLab exclusive, which cannot be found on OSINT sources.**

404 – Threat Actors
1,051 – Malware Families

We continuously track threat actors and malware families and provide analytical intelligence through AhnLab TIP.

The Threat Actors section offers detailed profiles of threat groups, along with associated TTPs, IoCs, and recent news articles.

The Malware Families section provides information on malware groups classified by characteristics, techniques, creators, etc.

2,216
News Clippings

We deliver security news and technical documents published by major media outlets and cybersecurity vendors. Each news article includes related IoCs, allowing security teams to use them for incident response.

2,970 – External Reports
19,679 – Social Media Content

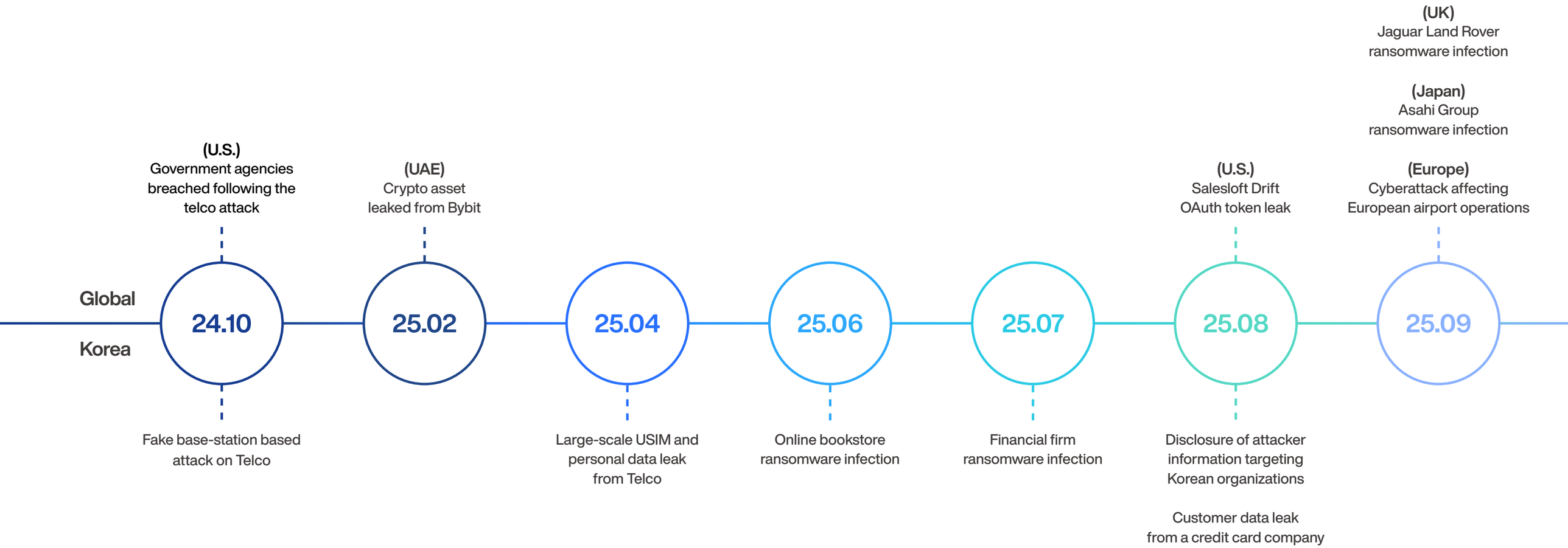
We provide curated security reports and trends from security vendors, industry experts, and articles on X (formerly Twitter). These also include related IoCs to help customers identify threats and support their swift response.

2025 Threat Landscape

- → Major Incident
- → Threat Actor Trend
  - Dark Web Top 8
  - APT Group
- → Ransomware Trend
  - Major Activities Top 10
  - Target Industries
  - Target Countries
- → Other Threat Trend
  - Malware Top 9
  - Attack Techniques Top 10
  - Vulnerabilities Top 10
  - Mobile Threats Top 6
- → Statistics
  - Cyber Attack Type

2025 Threat Landscape

Major Incident



2025 Threat Landscape

Major Incident: Global

2024.10. Government Agencies Breached After the U.S. Telco Attack

Salt Typhoon breached at least 8 major U.S. telecom providers, gaining access to wiretap systems and sensitive communications infrastructure.

They exploited vulnerabilities in Ivanti VPN(CVE-2023-46805, CVE-2024-21887), Fortinet EMS(CVE-2023-48788), Sophos Firewall(CVE-2022-3236), and Microsoft Exchange ProxyLogon. Evidence indicates that the compromised networks were used to monitor communications of U.S. government agencies and to access court-authorized wiretap data.

The group maintained long-term stealth access using backdoors such as GhostSpider, SnappyBee, and Masol RAT. Several government websites were also reported to have been affected.

2025.02. Crypto Assets Worth $1.5 Billion Leaked from Bybit

The Dubai-based crypto exchange Bybit suffered a major breach in which approximately $1.5 billion worth of crypto asset was stolen, an incident believed to be linked to Lazarus.

The attackers targeted the process of transferring funds from cold wallets to hot wallets. They compromised internal developer systems or manipulated the signing interface of the Safe Wallet platform to forge multisig transactions. The attackers injected malicious JavaScript into the signing host and spoofed legitimate wallet addresses, ultimately redirecting assets to the attackers' wallets. Stolen assets included ETH and stETH. Bybit launched compensation programs in response to the attack.

2025.08. Salesloft Drift, Data Exposed Due to OAuth Token Leak

Salesloft's Drift AI chatbot was compromised, leading to the leakage of OAuth tokens and the theft of customer data of more than 700 companies, including Salesforce.

Attackers first breached Salesloft's GitHub account and obtained internal code. They then moved into Drift's AWS environment to harvest OAuth tokens, subsequently used to access Salesforce instances and extract customer data. Adversaries also collected AWS keys, passwords, and Snowflake tokens. Salesforce and Salesloft removed the Drift app from AppExchange, blocked all connections, notified affected companies, and invalidated tokens.

Key Takeaways

- Salt Typhoon access wiretap and communications systems through the telecom provider attack.
- Attacks attributed to Lazarus leaked 1.5 billion USD worth of cryptocurrency from Bybit.
- OAuth token leak exposes data from 700+ companies due to Salesloft Drift AI breach.

2025 Threat Landscape

Major Incident: Global

2025.09. Asahi Infected by Ransomware

Japan's Asahi Group suffered a ransomware attack by Qilin, disrupting production and logistics systems across 30 factories nationwide.

Attackers encrypted Asahi's IT systems, exfiltrated data, and demanded ransom. Production and shipments of major products stopped, while customer service and ordering systems went offline. Qilin, a ransomware-as-a-service (RaaS) group, uses Golang and Rust based ransomware and double-extortion tactics. Asahi has been working with external experts on recovery, and partial operations resumed in early October.

2025.09. JLR Hit by Ransomware

Jaguar Land Rover (JLR) was hit by a ransomware attack attributed to Scattered Spider and Lapsus$, stopping worldwide production.

Adversaries disabled JLR's internal IT systems, disrupting major plants in the UK and global production lines for more than 5 weeks. Over 30k employees and 200k workers across the supply chain were affected. The total damage is estimated at GBP 1.9B.

JLR reported no customer data exposure, but delays in production caused significant financial impact. The UK government issued a GBP 1.5B emergency loan guarantee to support recovery.

2025.09. European Airports Disrupted by Ransomware

European airports experienced major disruptions after a ransomware attack on Collins Aerospace's MUSE software, which supports functions such as airport e-check-in, baggage processing, and boarding pass issuance. The incident caused hundreds of flight delays and cancellations at major airports, including Heathrow, Brussels, Berlin, and Dublin.

Attackers are believed to have gained access through Collins Aerospace's data center in Europe. Some systems were reinfected during recovery, causing extended outages and forcing passengers to rely on manual check-in.

Key Takeaways

- Qilin ransomware attack disrupted Asahi Group's systems at 30 plants nationwide.
- Ransomware attack stops JLR production for over 5 weeks causing GBP 1.9B damage.
- Ransomware attack on Collins Aerospace caused major flight delays and cancellations.

2025 Threat Landscape

Major Incident: South Korea

2024.10. A Telco Hit by Fake Base-Station Attacks Involving Data Theft

A fake base-station attack targeting a telco exposed personal data of approximately 22k customers and causing unauthorized small-payment charges for 368 victims.

Beginning in October 2024, attackers forced cell phones to connect to fake base stations, stole IMSI data, and used cloned devices with authentication bypass to conduct payment fraud.

Police seized several suspects and equipment. The government launched a joint investigation, and the telecom provider blocked new femtocells, tightened payment limits, expanded USIM protection, and compensated affected users.

2025.04. Large-scale USIM and Personal Data Leak from a Telco

A Korean telecom provider suffered a major breach exposing the data of about 23 million customers. The leaked data included phone numbers, IMSI/IMEI, and USIM authentication keys, raising concerns about SIM swapping and identity theft.

The attack involved the Linux-based BPFDoor backdoor, which uses kernel-level packet filtering to evade detection and activates only upon receiving specific magic packets. Attackers exploited web shells and RCE vulnerabilities to access internal systems and then installed BPFDoor on HSS servers to steal USIM data.

2025.06. Ransomware Causing Service Outage at Online Bookstore

South Korea's largest online bookstore and ticketing platform was hit by a ransomware that disabled its website and mobile app for 4 days. Attackers encrypted internal files and administrator accounts, locking the entire system and demanding ransom.

About 20 million users were unable to purchase books, reserve event tickets, or access community services, and several concerts and fan meetings were canceled or postponed.

Key Takeaways

- Fake base-station attack on a telecom provider caused customer data leakage and payment fraud.
- A telco suffered BPFDoor backdoor attack, leaking data of 23 million customers.
- Online bookstore was hit by ransomware - its website and mobile application were disabled for four days.

2025 Threat Landscape

Major Incident: South Korea

2025.07. Service Outage of Financial Firm Due to Ransomware

A financial firm suffered a major cyberattack after being infected with the Gunra ransomware, which disabled its IT systems. Attackers accessed the network through the SSH port of the SSL VPN appliance, escalated privileges, and deployed the ransomware.

Gunra uses ChaCha8 and RSA encryption to selectively encrypt key files and append the .ENCRT extension. The attack disrupted core financial services, including loan guarantees and mobile activations, forcing some branches to switch to manual operations. Financial Security Institute developed a recovery tool and helped the victim to restore its systems.

2025.08. Information on “APT Down” Disclosed

A report titled “APT Down: The North Korea Files,” released at DEF CON 33, detailed the activities of an APT group targeting South Korea. Based on 8.9GB of data recovered from a hacker workstation, the report examines long-term intrusions into Korean government agencies, media and telecom companies.

Adversaries used phishing, certificate theft, and lateral movement, with evidence indicating joint North Korean and Chinese operations. The Korean government launched responses through relevant agencies. **AhnLab released our own analysis report uncovering their cyber attack campaigns.**

2025.08. Customer Data Leakage from a Credit Card Company

A credit card company experienced a major breach affecting 2.97 million customers, including 280k whose sensitive payment data, such as card number, expiration date, CVC, and PIN was exposed. Attackers installed malware and web shells on the online payment server and used them to exfiltrate 200GB amount of data.

The company offered card reissuance, fee waivers, full compensation and pledged KRW 110 billion for security over the next five years.

Key Takeaways

- A financial firm was infected by Gunra ransomware but successful recovered.
- Long-term intrusions by APT Down into Korean government and enterprise networks were revealed.
- A credit card company suffered a security breach, exposing personal data of 2.97 million customers.

2025 Threat Landscape

Threat Actor Trend – Dark Web Top 8

AhnLab continuously tracks cyber threat issues on the dark web and shares the analysis through AhnLab TIP. Below are adversary insights identified from the dark web over the past year.

1. Ransomware Fragmentation and Rise of Small Groups

In 2025, the ransomware landscape underwent significant structural changes. Major groups like LockBit were heavily weakened due to concentrated law enforcement efforts, and RansomHub halted its official activity because of internal conflicts.

As a result, over 40 small and newly formed groups emerged. The ecosystem previously dominated by several major groups has shifted toward a structure involving Akira, Qilin, Play, Gunra, and others. These small groups reuse leaked LockBit 3.0 and Conti code and operate with their own branding. Their negotiation strategies tend to be more aggressive and unpredictable than those of larger groups. Some groups do not provide decryption tools, worsening the overall damage.

The ransomware ecosystem is shifting from centralized to decentralized structures, and as IoC-based detection reaches its limitations, existing defense strategies must be redesigned.

2. RaaS and White-Label–Based Ransomware Cartels

A major trend in 2025 is the emergence of ransomware cartels based on white-label models. **Under this model, central platforms deliver encryption tools, data-exfiltration infrastructure, and negotiation tools, while affiliates execute attacks under independent brands and pay only 20% of profits.** This is considerably more favorable than the earlier RaaS model sharing of 30–40% of profits. Groups like Global Group and Anubis have expanded this model throughout the ransomware ecosystem.

Attackers can conduct attacks in a franchise-like structure without requiring technical expertise or infrastructure, lowering the entry barrier. Consequently, both attack frequency and variety have increased, making it harder to identify attack groups based solely on the attacker's brand.

Key Takeaways

- Ransomware fragmentation caused by weakened major operators has led to the emergence of many small groups
- White-label ransomware cartels offer favorable revenue structures and enable franchise-style attack execution

2025 Threat Landscape

Threat Actor Trend – Dark Web Top 8

3. APT and Ransomware Partnership

In 2025, **state-sponsored APT groups began merging into the ransomware ecosystem,** blurring the boundary between nation-state cyber operations and profit-driven cybercrime

Microsoft reported that the North Korean state-sponsored APT Moonstone Sleet began distributing the Russia-linked Qilin ransomware instead of its own FakePenny ransomware. Another case showed the North Korean group Andariel deploying the Play ransomware after installing the DTrack backdoor. **This indicates a division of roles in which APT groups carry out initial intrusion, while RaaS affiliates handle the extortion phase.**

The combination of APT's advanced intrusion capabilities and RaaS's efficient extortion mechanisms can significantly increase success rates and damage. It also complicates defensive analysis and raises the risk of sanctioned states exploiting these operations as a source of profit.

4. Impact of Joint Investigation

In 2025, global law-enforcement cooperation had a significant impact on the cybercrime ecosystem. **Operation Endgame, launched in May 2024, expanded into its second phase in May 2025, targeting major malicious infrastructure such as DanaBot, Qakbot, and Trickbot.**

During May 2025, authorities dismantled 300 servers and 650 domains, issued arrest warrants for 20 cybercriminals, and seized about USD 4.05 million worth of cryptocurrency, bringing total seizures to about USD 24.53 million. BreachForums admins and five XSS forum operators were also arrested, **delivering a major blow to dark web infrastructure and contributing to the collapse of major ransomware groups such as LockBit and RansomHub.**

5. Conflict within Ransomware Gangs

In 2025, the ransomware ecosystem suffered significant damage as internal trust collapsed. One of the most notable incidents occurred in May, when **LockBit's admin panel was hacked, exposing 60,000 Bitcoin address records, 208 negotiation chat logs between victims and affiliates, and affiliate account information.** Qilin and Black Basta also had internal tools and chat logs leaked, revealing their operational methods to competitors.

Victims often paid ransom but received nonfunctional decryption tools, or in many cases, received nothing at all. As a result, affiliates grew distrustful of core operators, choosing to act independently or switch to competing groups. This internal split has fueled the rise of small ransomware groups.

Key Takeaways

- Convergence of APTs and ransomware – APTs conduct initial intrusion while ransomware groups handle extortion.
- International joint operations targeting the cybercrime ecosystem – collapse of LockBit, RansomHub, and others.
- Cross-group breaches and internal splits within ransomware groups leading to the rise of small ransomware gangs.

2025 Threat Landscape

Threat Actor Trend – Dark Web Top 8

6. Evolving Supply Chain Attacks

In 2025, supply chain attacks became more sophisticated and larger in scale compared to 2024. They expanded beyond software to cloud services, MSPs, and security solution providers. A notable example is CLOP's exploitation of a zero-day vulnerability in the Cleo MFT platform. Last January, with a single attack, they carried out a large-scale operation, infiltrating 182 companies simultaneously. In addition, the exploitation of Oracle EBS vulnerabilities by CLOP has increased. CISA officially warned of the risk of cascading compromises caused by leaked Oracle Cloud credentials.

DragonForce and Scattered Spider directly targeted cloud MSPs, exploiting a SimpleHelp vulnerability and using social engineering to deceive IT administrators and obtain remote access, resulting in a "chain supply-chain attack" that simultaneously affected numerous customer organizations via a single MSP breach.

7. Instability of Dark Web Ecosystem

In 2025, the dark web ecosystem became more unstable than ever. The ecosystem fell into chaos as attacks among criminal groups became commonplace, on top of the usual conflict between law enforcement and cybercriminals.

In March, DragonForce hacked the rival RansomHub's data leak site (DLS). In April, it defaced the DLS of BlackLock and Mamona, leaking internal chat logs and backend settings. Researchers reported that DragonForce exploited vulnerabilities in AI-generated backend code used by rival groups. Interestingly, Everest and LockBit were defaced with the same message—"Don't do crime CRIME IS BAD xoxo from Prague"—which suggests a coordinated attack targeting threat groups.

8. Surge in Hacktivist Campaigns

In 2025, geopolitical conflicts intensified in cyberspace. NoName057(16), a pro-Russian hacktivist group, continued its attacks on NATO countries, while Dark Storm Team hit NATO's power infrastructure to cause physical damage. On the opposing side, IT Army Ukraine launched DDoS attacks against the Russian telecom provider UIS, resulting in service outages for 72 hours.

In the Middle East, hacktivist activity increased as the Iran–Israel war escalated. Holy League and 313 Team attacked Israeli hospitals and central banks. The #OpIsrael 2025 campaign announced large-scale cyberattacks, and some medical institutions were hit by DDoS attacks. In addition, during the India–Pakistan conflict, the Indian Cyber Force claimed that they hacked Pakistan's banks and National Police Bureau.

Key Takeaways

- Supply chain attacks expanding beyond SW to cloud and MSPs – a single company breach impacts many customers.
- DragonForce hacked the DLS of its rival RansomHub – indicating organized attacks between threat groups.
- Surge in hacktivist activity across Russia vs Ukraine+NATO, Iran–Israel, and India–Pakistan conflicts.

2025 Threat Landscape

Threat Actor Trend – APT: Overview

In 2025, North Korean APTs remained highly active, continuing the trend from 2024. The most frequently mentioned group was Lazarus, with 31 reported incidents. Because Lazarus consists of multiple affiliates, the number of mentions was higher. The count may vary depending on how those affiliates are categorized. Kimsuky followed with 27 incidents, and TA-RedAnt was mentioned 17 times.

APTs China and Russia were also active. Mustang Panda had 11 mentions, APT28 and Gamaredon each had 10. APT activity from India and Pakistan also remained steady, likely **influenced by escalating geopolitical tensions.** Pakistan's Transparent Tribe stood out with 17 reports. By country, North Korea topped the list with 86 reports. China followed with 27, then Russia and India with 18 each, and Pakistan with 17. Iran had 9, while other countries collectively accounted for 32 reports—indicating a wide range of state-backed activity in the global threat landscape. Fewer public reports do not always reflect lower activity levels. Some APT groups operate covertly, leaving little evidence, and attacks on government institutions are sometimes withheld for policy reasons.

	APTs	10/24	11/24	12/24	01/25	02/25	03/25	04/25	05/25	06/25	07/25	08/25	09/25
North Korea (86)	Andariel	2		1	1	1							
	Kimsuky	3	4	6	2	2	2			2	2	2	2
	Konni	2					2	1	1				
	Lazarus	5	2	2	4	3	4	1		2	2	4	2
	TA-RedAnt	2	1		2	1	4		1		2	3	1
China (27)	APT41	1	1					1	1	1	1	1	
	MirrorFace		2		1		1	1					
	Mustang Panda				2	2		3		1			3
	Salt Typhoon		1			1			1	1			
Russia (18)	APT28	2	1						3	1	2		1
	Gamaredon			4			1	1			1	1	
Iran (9)	Charming Kitten		2	1					1				
	MuddyWater		1			1					1	1	1
India (18)	Bitter	1	1	1					1	1		1	
	SideWinder	1					1		2			1	2
	Viceroy Tiger	1	1		1	1					1		
Pakistan (17)	Transparent Tribe		1	1			1	1	4	4	2	3	

[Table] Monthly Activities of State-Sponsored APTs (Oct 2024 – Sep 2025)

2025 Threat Landscape

Threat Actor Trend – APT: Overview

APT groups mainly operate in regions marked by geopolitical conflict, such as South Korea–North Korea, India–Pakistan, China–Southeast Asia, Russia–Ukraine, and Israel–Iran. **They target high-value entities, including government, military, finance, energy, telecommunications, education, and NGOs.**

Email-based spear-phishing remains the primary method of initial intrusion. Malicious attachments are commonly delivered in file formats such as LNK, ISO, MSC, PDF, CHM, and ZIP. Attackers use social engineering to disguise lures as fake job offers, policy documents, security alerts, or official notices, employing tailored bait documents and events to deceive victims.

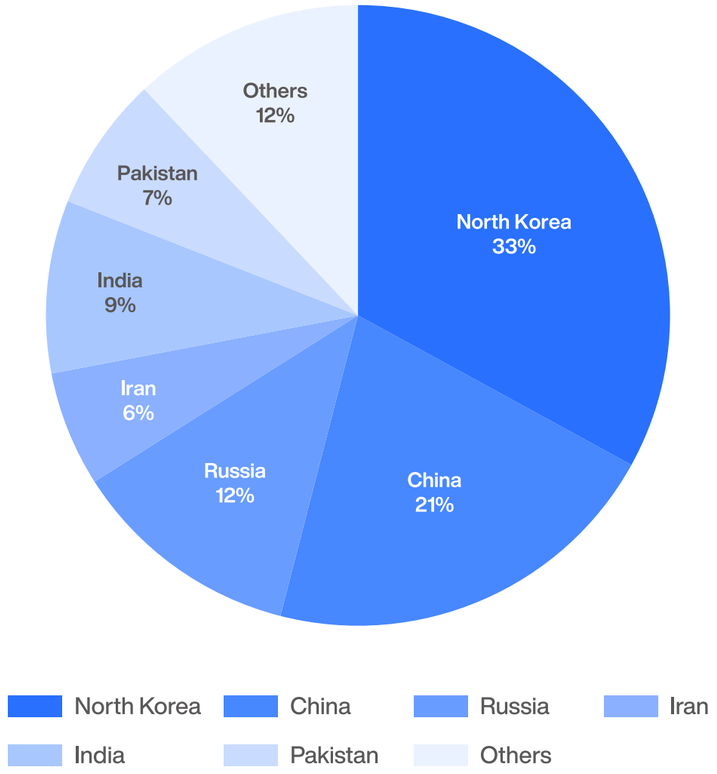
APT groups deploy a mix of malware and legitimate tools. These include remote access tools, backdoors, keyloggers, and information stealers. PowerShell, VBS, batch scripts, and open-source utilities such as Sliver and Mimikatz are also used. To support cross-platform campaigns, malware targeting Windows, Linux, macOS, and Android is adapted to the situation.

APTs are also armed with advanced techniques to maintain persistence and evade detection.

- Task scheduler and registry registration
- Service and COM hijacking
- User Account Control (UAC) bypass
- Fileless execution
- DLL sideloading
- JPEG steganography
- VM and sandbox evasion
- Log deletion

They leverage legitimate platforms and cloud infrastructure, such as GitHub, Dropbox, Google Drive, Telegram, and Outlook for C2 communications and data exfiltration. They also hide their activities using DNS, DoH, TOR, and VPNs.

Recent techniques include AI-generated deepfakes, MFA bypass (AiTM, OTP theft), supply chain attacks, watering hole attacks, IoT device intrusions, large-scale attack automation, and others. They also combine open-source tools with custom-developed malware.

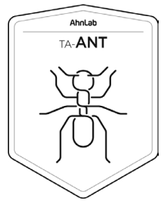


[Image] Proportion of APT Group Activities by Country (Oct 2024 – Sep 2025)

2025 Threat Landscape

Threat Actor Trend – APT: North Korea

North Korean APT groups pursue financial gain and information collection by targeting sectors such as politics, finance, and cryptocurrency.
They are known for using sophisticated techniques including spear-phishing, supply chain attacks, multi-platform malware, privilege escalation, and MFA bypass.



North Korea

Kimsuky

In 2025, Kimsuky conducted highly advanced cyberattacks against various countries and industries. **They used spear-phishing disguised as lecture invitations or interview requests to distribute ISO, LNK, and MSC files.** Notable tactics included MSC phishing hosted on Google Drive and abuse of VbsEdit signatures.

Newly observed were multi-stage attacks using GitHub, Facebook, and Telegram, as well as AI-generated fake IDs. They also strengthened remote access using malware such as PebbleDash, RDP Wrapper, and proxy malware. In attacks on Japan, a variant of AsyncRAT was used.

Kimsuky consists of multiple affiliates. Larva-24005 used Kimalogger to collect keystrokes. Larva-24009 carried out LNK-based attacks using QuasarRAT and UltraVNC. Larva-25001 delivered LNK files disguised as documents to infect targets with malware, including HttpSpy and Memload.

Andariel

Andariel has continued financially motivated attacks across multiple countries. Despite being indicted by the U.S. Department of Justice in 2024, the group remained active. **It previously targeted U.S. private companies by deploying the Preft and Nukebot backdoors.** Open-source tools like Sliver, Chisel, and PuTTY were utilized, along with keyloggers and Mimikatz for credential theft. The group also distributed ransomware via the Play ransomware infrastructure.

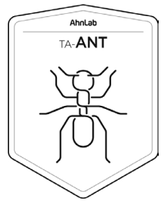
In South Korea, it deployed ModeLoader and SmallTiger malware against asset management and document centralization solutions. Long-term persistence was achieved through RDP access and hidden account creation. They also installed web shells by exploiting Apache Tomcat vulnerabilities and scanned internal networks using Advanced Port Scanner. Notably, they escalated low-privilege accounts to admin level using RID hijacking and added backdoor accounts with the CreateHiddenAccount tool. They also executed remote commands using PsExec and modified the SAM registry via REGINI, demonstrating sophisticated lateral movement. In addition, they stole a certificate from a South Korean cybersecurity company and signed malware with it to exploit trust.

Key Takeaways

- Kimsuky spreads malware via spear-phishing, using spoofed domains and malicious documents
- Kimsuky runs multiple affiliates enabling broader attacks
- Andariel infiltrated U.S. companies using backdoors
- Andariel deployed ransomware via Play's infrastructure

2025 Threat Landscape

Threat Actor Trend – APT: North Korea



North Korea

Konni

Konni conducted LNK-based spear-phishing attacks against high-value targets, including Ukraine. These attacks employed social engineering themes like tax and market analysis and executed malicious payloads via PowerShell and AutoIt. A key tactic involved embedding disguised shortcut files within ZIP archives to trigger multi-stage loaders when opened.

Konni relied on a WordPress-based C2 setup to distribute multiple RATs. It maintained persistence by evading Avast antivirus, enabling startup folder autoruns, creating hidden directories, and registering registry keys. Large batches of malware samples were generated and distributed over time, using payloads with layered obfuscation and encryption to evade detection.

On the social engineering front, attacks targeted the South Korean and Ukrainian government institutions. They forged sender details using PHPMailer, and bundled malicious scripts with trusted documents to gain user trust. Beyond info-stealing, Konni's operations included system control, credential theft, and reconnaissance, all aimed at long-term infiltration.

Lazarus

Lazarus expanded its operations across finance, IT, and defense. **They developed numerous multi-platform malware variants that support macOS and Linux.** New backdoors and info-stealers were introduced using the Electron and Tauri frameworks. Their malware, InvisibleFerret, BeaverTail, OtterCookie, CookiePlus, and FrostyFerret, perform keylogging, clipboard monitoring, and theft of browser cache and crypto wallet data. Supply chain attacks and watering hole techniques were particularly prominent.

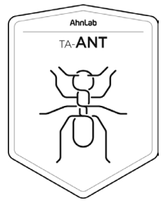
In South Korea, at least six industrial organizations were compromised via the Operation SyncHole campaign, exploiting software vulnerabilities. The group also infected developers and companies by distributing malicious packages through open-source platforms such as npm, PyPI, and GitHub. Social engineering tactics evolved, incorporating fake interview campaigns like ClickFix & ClickFake Interview, along with more sophisticated psychological manipulation techniques. Technically, Lazarus employed advanced evasion and persistence techniques such as multi-stage obfuscation, JPEG steganography, fileless execution, DLL sideloading, and TxF-based process doppelganging.

Key Takeaways

- Konni focused on LNK-based spear-phishing attacks
- Konni distributed various RATs via WordPress-based C2
- Lazarus developed multi-platform malware supporting macOS and Linux
- In South Korea, Lazarus breached at least six organizations through Operation SyncHole exploiting software vulnerabilities.

2025 Threat Landscape

Threat Actor Trend – APT: North Korea



North Korea

TA-RedAnt

TA-RedAnt expanded its cyber operations into East Asia, South Asia, the Middle East, and Europe. It targeted various industries, including politics, defense, finance, healthcare and energy. The group comprises several affiliates, such as ScarCruft (APT37), SideWinder, Transparent Tribe (APT36), and UNC3886 (Fire Ant).

TA-RedAnt employed diverse techniques including spear-phishing, watering hole attacks, and malicious files (PDF, ISO, LNK), as well as trojanized installers and compressed files (EGG, ZIP), cloud-based links, and Github/Dropbox-based C2. They are armed with advanced stealth and persistence tactics, such as JPEG steganography, fileless execution, and DLL sideloading.

Newly identified techniques include Rust-based backdoors (Rustonotto, CHILLYCHINO), VCD ransomware, PubNub/Ably messaging C2 channels, LLM-based malware (LAMEHUG), MFA bypass (AitM, OTP theft), and AI-generated image and voice manipulation, as well as Python code obfuscation. There has also been a notable increase in multi-platform attacks, including the use of .desktop files in Linux and payload delivery via Google Drive.

Their social engineering has evolved significantly, employing impersonation of real people, fake academic events and newsletters, group chats on messengers, and emails without links to avoid suspicion. Its capabilities in attack automation and detection evasion have also advanced. Techniques include disguising malware as legitimate files or signed software, using cloud or trusted servers for C2, multi-stage decoding and obfuscation, and hiding payloads in temp folders with self-deletion.

TA-RedAnt has leveraged a wide array of tools and malware to steal credentials, system info, crypto assets, documents, audio, and USB/MTP data. **In some incidents, it deployed ransomware to financially damage victim organizations.** The group is expected to remain a persistent and evolving global threat.

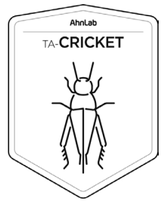
Key Takeaways

- TA-RedAnt targeted politics, defense, and energy sectors.
- They use spear-phishing, trojanized installers, and cloud-based C2
- They enhance stealth with JPEG steganography, fileless execution, and DLL sideloading.
- TA-RedAnt deployed ransomware in some cases, causing financial damage.

2025 Threat Landscape

Threat Actor Trend – APT: China

Chinese APT groups conduct long-term, strategic information gathering and surveillance operations against government, military, and industrial targets. They leverage advanced techniques, including zero-day exploits, supply chain attacks, multi-platform malware, and cloud infrastructure abuse, while strengthening detection evasion.



China

APT41

APT41 sustained sophisticated attacks targeting global government entities and key industries. Its operations included the TOUGHPROGRESS campaign abusing Google Calendar, ClickOnce-based OneClick attacks, and the RunnerBeacon backdoor targeting government, energy, and finance sectors. They also deployed reconnaissance tools and encrypted web shells against Japanese firms while simultaneously targeting the IT infrastructure of African governments. **In July 2024, they exploited a zero-day in Fortinet's FortiClient to extract post-authentication credentials from memory.**

To evade detection, APT41 leveraged WordPress C2, encrypted HTTPS, and TLS disguise techniques. To automate attacks, they generated and distributed large volumes of malicious samples over time. It simultaneously conducted supply chain attacks and mobile platform intrusions. APT41 distributed customized malicious apps on iOS and Android to steal data and hijacked cloud accounts to move into corporate networks. Its social engineering strategies reflected victims' language and culture, and evidence suggests AI-powered tools were used to mass-produce phishing content.

MirrorFace

MirrorFace has extended its attacks from Japan to diplomatic institutions in Taiwan, India, and Europe. They carried out initial intrusion via spear-phishing emails and OneDrive links, delivering ZIP files containing ROAMINGMOUSE macro documents, shortcut files, and SFX executables. Zero-day vulnerabilities in SSL VPN and file storage services (CVE-2023-28461, CVE-2023-27997) were exploited to breach systems, with MirrorStealer, Lodeinfo, and Cobalt Strike used for credential theft and AD server infiltration. MirrorFace deployed updated versions of the ANEL backdoor along with new strains such as NOOPDOOR and NOOPLDR. Attack automation involved PowerShell and WMI-based execution, while evasion techniques included Base64/HEX encoding, UAC bypass, sandbox evasion, and WMI abuse.

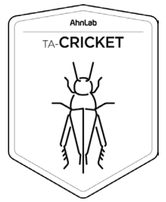
It also conducted phishing campaigns tailored to Japanese politicians and journalists. Cloud services and CDNs were used to disguise traffic as legitimate. Japanese police warned that their activities are highly likely to be part of an organized intelligence-gathering effort.

Key Takeaways

- APT41 exploited a zero-day vulnerability to extract FortiClient credentials.
- They evaded detection via WordPress-based C2, encrypted HTTPS traffic, and TLS obfuscation.
- MirrorFace attempted initial access via spear-phishing and zero-day exploitation.
- They launched phishing campaigns against Japanese politicians and journalists.

2025 Threat Landscape

Threat Actor Trend – APT: China



China

Mustang Panda

Mustang Panda broadened its attacks across Southeast and Northeast Asia, Europe, and South America, targeting governments, military, and NGOs. **Spear-phishing emails and malicious documents in LNK, CHM, OneNote, PDF, HTML, and ISO formats were used for initial infiltration.** Attack techniques included HTML smuggling, USB worms (SnakeDisk), and cloud-based phishing.

Their malware utilized PlugX, TONESHELL, Bookworm, PUBLOAD, MQsTTang, CCoreDoor, and ShadowPad, as well as new tools such as StarProxy, PAKLOG/CorKLOG, SplatCloak, and Yokai. These enabled lateral movement, keylogging, bypassing EDR, and USB-based spread. Evasion techniques featured DLL injection using trusted processes (e.g., MAVInject.exe), reflective DLL injection via WriteProcessMemory, traffic masking via FakeTLS and TLS-like headers, and payload delivery via cloud platforms like Cloudflare CDN and Google Drive. Social engineering relied on current events such as Taiwan's election, Mongolian floods, ASEAN meetings, and Tibetan events. Additional techniques were WebSocket C2, AES/DES-based encryption layers, and Kavach OTP theft for MFA evasion.

Salt Typhoon

Salt Typhoon conducted long-term surveillance and info-gathering operations targeting telcos, governments, and military in the United States, Asia, the Middle East, and Africa. They conducted initial access by exploiting known vulnerabilities in exposed servers and network appliances (e.g., CVE-2018-0171, CVE-2023-20198). Lateral movement within networks involved WMIC.exe and PSEXEC.exe. For privilege escalation in AD servers, they used Kerberos ticket manipulation and Pass-the-Hash. To evade detection, they intensified their use of Living-off-the-Land (LOTL) tactics by abusing legitimate administrative tools.

Salt Typhoon primarily used GHOSTSPIDER, SNAPPYBEE, and MASOL RAT. GHOSTSPIDER featured a modular design and TLS encryption, making analysis difficult. SNAPPYBEE exfiltrated data via cloud API calls, while MASOL RAT combined fileless execution with PowerShell obfuscation to evade detection. In May 2025, they exploited a zero-day (CVE-2025-3928) in the Commvault Metallic SaaS platform to breach Microsoft 365. They also leveraged techniques, such as C2 concealment via ShadowPad.

Key Takeaways

- Mustang Panda used spear-phishing and malicious documents for initial access, leveraging HTML smuggling.
- They leveraged reused tools and newly developed stealth techniques.
- Salt Typhoon exploited exposed server and network vulnerabilities to gain access.
- They leveraged advanced tactics, including LOTL for evasion, and traffic disguise.

2025 Threat Landscape

Threat Actor Trend – APT: Russia

Russia

Russian APT groups leverage geopolitical tensions to launch sustained, organized attacks on government institutions. They use tactics like phishing, hiding C2 in cloud, and fileless execution for defense evasion. They run tailored campaigns to pursue psychological warfare and political influence. Beyond data theft, they aim to disrupt national infrastructure.

APT28

APT28 pursue long-term cyberattacks against government and technology sectors in Ukraine, NATO countries, and Eastern Europe. They leveraged geopolitical conflict to conduct phishing campaigns with lures referencing the Russia–Ukraine war and NATO summits. For initial access, they conducted email phishing and exploitation of CVE-2023-38831, CVE-2023-23397, and email server vulnerabilities in Outlook, Roundcube, and Zimbra.

APT28 used LLM-based malware (LAMEHUG) to automate commands and gather intelligence. They reinforced persistence via MFA bypass (AiTM), COM hijacking, and UAC bypass. Google Drive and other cloud services were exploited to hide C2 communications. Python scripts paired with PowerShell obfuscation enabled mass generation of malicious samples. HeadLace, GooseEgg, and MASEPIE were among the identified malware, supporting credential theft, lateral movement, and network surveillance. They utilized Cobalt Strike and Sliver to build a sophisticated attack chain, with additional techniques like HTML smuggling, fileless execution, and JPEG steganography

Gamaredon

Gamaredon executed advanced spear-phishing and info-gathering operations against Ukraine and Russian-speaking people. They performed initial access by using malicious LNK, HTA, and XHTML that ran PowerShell malware to collect system data and retrieve payloads. To bypass detection, they utilized Cloudflare Tunnels and DNS over HTTPS (DoH). Python scripts were combined with PowerShell obfuscation to automate attacks. Their new malware (GammaDrop, GammaLoad, and GammaSteel) carried out obfuscation, registry concealment, and USB weaponization.

Gamaredon also reinforced mobile platform attacks. They used Android surveillance malware such as BoneSpy and PlainGnome to target Russian-speaking people. Some malware disguised themselves as Samsung Knox to infiltrate enterprises. These malicious apps collected call logs, messages, and location data, and remotely controlled cameras and microphones. In 2025, the group conducted a PowerShell-based data theft against Western troops stationed in Ukraine. These operations go beyond simple espionage, combining military and diplomatic intelligence gathering with psychological warfare. They are suspected to be linked to the 18th Center of Information Security under Russia's FSB.

Key Takeaways

- APT28 used Russia-Ukraine conflict lures in phishing attacks.
- They introduced LAMEHUG, an LLM-based malware, to automate their campaigns.
- Gamaredon used advanced malware that conducts obfuscation and USB weaponization.
- Their mobile attacks using Android spyware target Russian-speaking people.

2025 Threat Landscape

Threat Actor Trend – APT: Iran

Iranian APTs conduct long-term attacks against governments and media agencies, mainly in the Middle East and Europe. They use techniques such as spear-phishing, HTML smuggling, fileless execution, MFA bypass, and OTP theft. By combining Android malware with AI-generated phishing content, they have expanded their attacks to mobile devices.

Iran

Charming Kitten

Charming Kitten carried out attacks targeting governments and media agencies, mainly in the Middle East and Europe. For initial access, they utilized social-engineering-based phishing and the distribution of malicious documents. **They have also added a new multi-stage loading method that combines LNK files and PowerShell.** They hid malware through steganography inside JPEG images and actively used fileless execution techniques to evade detection.

Charming Kitten bypassed authentication through MFA bypass and OTP theft techniques, and operated AiTM (Adversary-in-the-Middle)–based phishing websites to hijack sessions in real time. Their cloud-based C2 communication disguised itself as normal traffic by using Dropbox, Google Drive, and the Telegram API. They also evaded network detection by combining TLS encryption with DNS over HTTPS (DoH). Their malware (POWERSTATS, NokNok, and CharmPower) provide keylogging, browser cookie theft, and system information collection capabilities.

MuddyWater

MuddyWater continued its attacks targeting governments, telcos, and industrial organizations in the Middle East, Europe, and South Asia. **The group actively used Living-off-the-Land (LOTL) techniques, conducting initial access and command execution with legitimate tools such as PowerShell and MSHTA.** They distributed malicious LNK files through spear-phishing emails and combined normal documents with malicious scripts to evade detection. MuddyWater expanded C2 communications using open-source tools, including Ligolo, SimpleHelp, and Venom Proxy. They also utilized the BugSleep (MuddyRot) backdoor to replace the existing Atera RMM, and combined Python scripts with PowerShell obfuscation to automate attacks. Fileless execution and in-memory malware loading were also key aspects of their operations.

Their MuddyC2Go, BugSleep, and SimpleHelp RAT carried out credential theft, keylogging, and reconnaissance. They hid C2 traffic using DNS over HTTPS (DoH) and TLS encryption, and delivered payloads through cloud services such as Google Drive and Dropbox. Their infrastructure leveraged watering hole tactics using CDNs and legitimate websites.

Key Takeaways

- Charming Kitten deployed phishing attacks using social engineering tactics, with a new LNK and PowerShell-based multi-stage loader.
- They evaded authentication systems using MFA bypass and OTP theft.
- MuddyWater used LOTL techniques to gain initial access and execute commands.
- They expanded C2 communications using open-source tools, enabling lateral movement through VPNs.

2025 Threat Landscape

Threat Actor Trend – APT: India

Indian APTs conduct persistent attacks targeting government institutions in South Asia and the Middle East. They have been conducting multi-platform attacks using Android malware and enhancing their social-engineering techniques by leveraging AI-generated phishing content.

India

Bitter

Bitter continuously targeted government entities in South Asia and the Middle East. They achieved initial access through email attacks using malicious documents and LNK files. **The group enhanced its evasion capabilities by newly employing HTML smuggling and PowerShell-based malware.** Bitter combined legitimate documents with malicious scripts to gain victim trust and concealed payloads using multi-stage loading techniques.

Bitter expanded into mobile attacks using Android malware that stole financial data, messages, and location info, and enabled remote control of the camera and microphone. C2 traffic was disguised via Google Drive, Dropbox, and Telegram API, with TLS and DNS over HTTPS (DoH) used to evade network detection. They bypassed MFA using AiTM phishing and OTP theft. The group relied on AridViper variants, BitterRAT, and VajraSpy for keylogging, cookie theft, and system reconnaissance. Bitter automated attacks with Python scripts and PowerShell obfuscation and used phishing emails mimicking government, diplomatic, and military documents to deceive targets.

Sidewinder

SideWinder expanded their attacks against government, energy, and education sectors across South Asia, Southeast Asia, and the Middle East. **They developed various modules, including USB worms, keyloggers, and data stealers, centered around the WarHawk malware family.** SideWinder enhanced detection evasion through a combination of multi-stage loading and fileless execution. **They gained initial access via spear-phishing emails, delivering malicious LNK files and leveraging HTML smuggling techniques.**

SideWinder evaded detection using PowerShell obfuscation, DLL sideloading, and TxF-based Process Doppelganging. They masked C2 communication using Cloudflare CDN and Google Drive, while combining TLS encryption with DNS over HTTPS (DoH) to avoid detection. Their malware (WarHawk, SideWinder RAT, and SplatCloak) enabled keylogging, cookie theft, and system reconnaissance. Social engineering tactics evolved to impersonation, fake academic events, and group chats. Attackers built trust through multi-step email exchanges, automated campaigns using AI-generated phishing content.

Key Takeaways

- Bitter used HTML smuggling and PowerShell malware for enhanced evasion.
- Their Android apps stole financial data, messages, locations, and enabled remote camera/mic access.
- SideWinder built WarHawk-based modules with USB worms, keyloggers, and data stealers.
- Their social engineering included impersonation, fake events, and group chats.

2025 Threat Landscape

Threat Actor Trend – APT: Pakistan and Others

Pakistani APTs have targeted government, military, and education sectors across India, Pakistan, the Middle East, and Africa. Their Evasion techniques include MFA bypass and WebSocket-based C2, along with payload concealment via cloud infrastructure and steganography. They enhanced social engineering technique through tailored phishing and AI-generated content.

Pakistan

Transparent Tribe

Transparent Tribe continued targeting government, military, and education sectors across India, Pakistan, the Middle East, and Africa. **They used multiple RATs (CapraRAT, CrimsonRAT, ObliqueRAT) to simultaneously compromise Windows, Linux, and Android systems.** Their evasion techniques leverage WebSocket-based C2, MFA bypass via Kavach OTP theft, and real-time session hijacking using AiTM phishing sites.

Transparent Tribe actively utilized cloud infrastructure, expanding C2 communication through Google Drive, Slack, and Telegram APIs. They evaded network detection using a combination of TLS encryption and DNS over HTTPS (DoH). In addition to CrimsonRAT, CapraRAT, and ObliqueRAT, they deployed Android malware disguised as legitimate apps. Their social engineering techniques involved tailored lures, such as fake diplomatic documents and academic invitations, paired with multi-stage email exchanges to build trust. They attempted to automate their campaigns by using AI-generated phishing content.

Others

Miscellaneous APT groups exhibit complex and varied behavior that defies national attribution. They target a wide range of sectors (government, defense, finance, telecom, education, and NGOs) across Asia, the Middle East, Europe, and the Americas. **Initial access typically involves social engineering-based spear-phishing with diverse document formats, followed by multi-stage script-based payloads like PowerShell.** They actively use cloud and open-source infrastructure, frequently leveraging GitHub, Dropbox, Google Drive, and Telegram for C2. **Their malware, written in Rust, Go, and Python, enable multi-platform attacks across Windows, Linux, macOS, and Android.**

Advanced evasion techniques encompass obfuscation, encryption, fileless execution, DLL sideloading, COM hijacking, log wiping, and timestamp manipulation. New methods such as LLM-based malware (e.g., LAMEHUG), ClickFix, HTML smuggling, MFA bypass, and session cookie theft have also emerged. Some groups hijack other actors' infrastructure or employ false flag operations to create confusion.

Key Takeaways

- Transparent Tribe deployed multiple RATs to target Windows, Linux, and Android platforms
- They expanded C2 operations and evaded detection using cloud-based infrastructure.
- Other APTs commonly used social engineering and diverse document formats for initial access.
- These groups launched multi-platform attacks via malware developed in various languages.

2025 Threat Landscape

Ransomware Trend

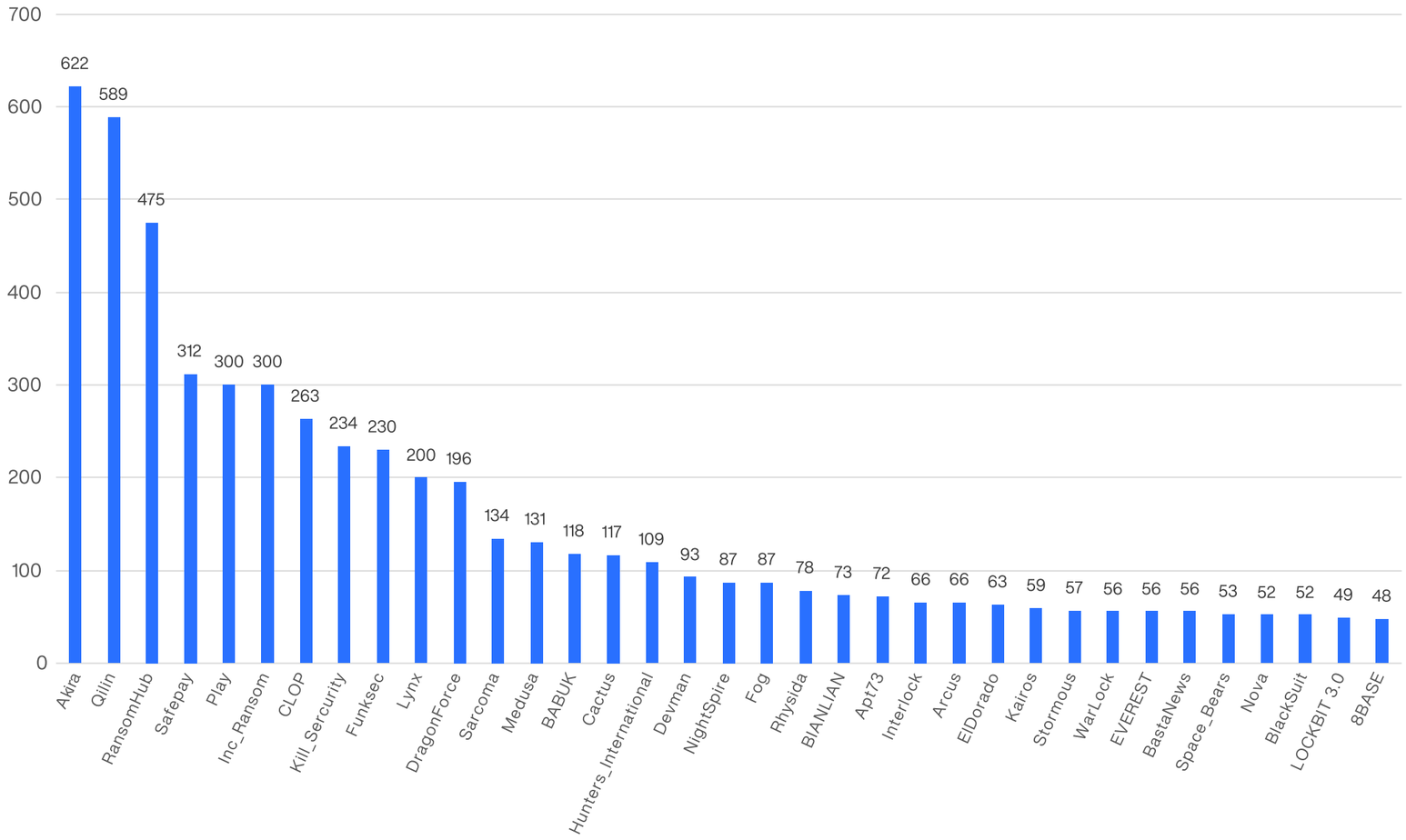
Overview

The ransomware ecosystem expanded rapidly in 2025, growing by 38%. Despite law-enforcement actions, the number of active groups increased by 26% to 96, accelerating fragmentation across the ecosystem.

There were also significant shifts in group rankings by attack volume. **Akira recorded 622 incidents and moved from 4th to 1st place.** Qilin rose from 11th to 2nd with 589 incidents, and CLOP climbed from 43rd to 7th. LockBit, which ranked 1st in 2024, dropped out of the top 30 after Operation Cronos.

North Korea linked Andariel and Moonstone Sleet deployed Play and Qilin ransomware, **highlighting how state-backed actors are increasingly joining RaaS cartels.** This shift represents a new model for generating revenue and evading international sanctions.

Number of Victim Companies by Ransomware Group in 2025



2025 Threat Landscape

Ransomware Trend

Enforcement Actions and Limitations

Law enforcement efforts against ransomware increased this year, but the overall impact remained limited. LockBit, disrupted by Operation Cronos, resurfaced as LockBit 5.0 and adopted more aggressive tactics, targeting major infrastructure such as nuclear and thermal power plants.

RansomHub abruptly shut down in April, despite leading 2024 in attack volume. DragonForce claimed to absorb the group, but RansomHub accused DragonForce of cooperating with law enforcement, exposing internal friction.

Former RansomHub affiliates shifted to Qilin, DragonForce, and Lynx, reshaping the landscape and demonstrating the resilience of the RaaS ecosystem.

Major Attack Tactics

Ransomware actors have shifted toward triple extortion, adding pressure by contacting victims' customers and partners in addition to encrypting and stealing data. This method has been widely used in healthcare and finance to maximize reputational damage.

Another notable change is the move from zero-day attacks to one-day exploits. CLOP compromised 400 organizations through a Cleo MFT zero-day, and Akira exploited a SonicWall SSL VPN vulnerability. As a result, MFT platforms and VPN appliances have become major attack vectors.

Outlook

Ransomware is expected to advance through AI-driven automation and LLM-based tactics, along with an increase in non-encryption, data-theft attacks. Cooperation between state-sponsored actors and criminal groups is also likely to grow, as shown by recent North Korean activity.

Defending against these threats requires a multi-layered approach, that includes zero trust, MFA for VPN/RDP, secured hypervisors such as VMware ESXi, and micro-segmentation to limit impact. Threat intelligence-driven 24/7 monitoring is vital for early detection, using the 18-day gap between IAB sales and intrusions. Physically isolated and immutable backups also remain essential.

Key Takeaways

- Major ransomware groups have weakened, but the RaaS ecosystem remains resilient.
- Ransomware tactics have shifted to triple extortion, adding more pressure to victims.
- Evolving threats require multi-layered defenses - zero trust, MFA, threat intel-driven monitoring, etc.

2025 Threat Landscape

Ransomware Trend – Major Activities Top 10

1. Gunra - Financial Sector Intrusion

Gunra is a newly discovered ransomware group identified in April 2025, targeting South Korea, Japan, Brazil, Turkey, and Taiwan. Notably, the U.S. was not among the affected countries. Gunra is built on the Conti v2 source code.

Its most distinctive characteristic is an extremely short negotiation window of only 5 days, which creates strong pressure on victims. The group also maintains a structured operation on the dark web, including a WhatsApp-style negotiation portal operated by dedicated staff.

Gunra operates on both Windows and Linux, with its Linux variant supporting up to 100 concurrent encryption threads. The Linux version uses ChaCha20 encryption, but weaknesses were found in its implementation allowing the Korean insurance company to successfully decrypt the affected data.

2. Qilin - Solidifying Its Dominance

Qilin, which had no recorded activity in South Korea and Japan in 2024, became one of the most active groups in both countries in 2025. It swiftly replaced RansomHub, absorbing its former affiliates. **In Korea, it launched the "Korean Leak" campaign, attacking 29 small asset managers through supply chain breaches.**

Moonstone Sleet, a North Korea linked actor, began distributing Qilin ransomware in February, signaling Qilin's evolution into a state-sponsored group. In September, Qilin formed a cartel with DragonForce and LockBit to strengthen its market dominance.

3. Play - Joining with Andariel

In October 2024, Play ransomware was identified working with Andariel, a North Korea-backed group, marking **the first state actor to leverage a RaaS infrastructure.** After infiltrating victims in May using Sliver C2 and Dtrack backdoor, Andariel deployed Play ransomware in September.

In the first half of 2025, the FBI reported around 900 victims of Play ransomware. North Korea has used ransomware as a funding mechanism since WannaCry, and its collaboration with Play is viewed as a new strategy to circumvent international sanctions.

Key Takeaways

- Gunra ransomware supports both Windows and Linux – a weakness was found in the encryption of its Linux version.
- North Korea-backed Moonstone Sleet has evolved into a state-sponsored threat group, distributing Qilin ransomware.
- Play ransomware collaborates with North Korea's Andariel – the first case of a state-backed group leveraging RaaS.

2025 Threat Landscape

Ransomware Trend – Major Activities Top 10

4. Akira - Exploiting SSL VPN

Akira showed steady growth throughout 2025, becoming the most active ransomware group. It shifted from sporadic mass leaks in 2024 to smaller, regular leaks in Q1 2025.

I**ts most notable campaign activity started in July, launching global attacks on SonicWall SSL VPN devices by exploiting CVE-2024-40766.** By August, U.S. organizations reported sequential network scanning, lateral movement, privilege escalation, and data exfiltration.

Akira is highly specialized in VMware ESXi and can perform extensive encryption in cloud environments. It also released a new Rust-based variant, Akira v2, featuring advanced obfuscation, PowerTool abuse, log deletion, and multiple EDR evasion techniques. Targeting manufacturing, education, and healthcare, Akira solidified its position as one of leading ransomware gangs

5. Lynx – Targeting Manufacturers

Lynx emerged in July 2024 by rebranding INC ransomware. Its number of victims surged from 96 in January 2025 to 300 by August. In June, the group adopted a multi-brand strategy under the name Sinobi. **Its operations focused on manufacturing and construction, with the U.S. accounting for 60% of all victims.**

In January, Lynx attacked a U.S. law firm, stealing sensitive client data, and in December, it disrupted a Romanian energy provider. Although Lynx claims to be an ethical hacking group, it in fact employs double extortion and carries out opportunistic and indiscriminate attacks.

6. LockBit – Coming Back as v5.0

LockBit, disrupted by Operation Cronos in February 2024, announced its return as LockBit 5.0 in September 2025. **The new version strengthened its cross-platform strategy on Windows, Linux, and VMware ESXi,** and adopted advanced anti-analysis techniques like DLL reflection loading and ETW patching.

LockBit 5.0 explicitly allowed affiliates to attack critical infrastructure including nuclear and thermal power plants, which they had previously avoided.

Key Takeaways

- Akira ransomware exploits vulnerabilities in SonicWall SSL VPN devices to launch global-scale attacks.
- Lynx targets manufacturing and construction industries – the U.S. accounts for 60% of all affected countries.
- LockBit 5.0 strengthens its cross-platform strategy, targeting Windows, Linux, and VMware ESXi.

2025 Threat Landscape

Ransomware Trend – Major Activities Top 10

7. DragonForce – Cartel Formation

DragonForce, which appeared in late 2023, declared a ransomware cartel in March 2025 to reshape the ecosystem. **It introduced a white-label model that allows affiliates to use its infrastructure under their own brands,** offering 80% profit shares, large-scale storage, 24/7 monitoring, and blogs and file servers. In April 2025, DragonForce claimed to have absorbed RansomHub's infrastructure. However, RansomHub accused DragonForce of cooperating with law enforcement.

8. CLOP – A Return with Cleo MFT Attack

CLOP dramatically returned in Q1 2025, exploiting two Cleo MFT zero-days (CVE-2024-50623, CVE-2024-55956). Cleo patched the first flaw in October, but CLOP bypassed the fix in November and found a second vulnerability in December, compromising about 400 organizations. Building on its 2023 MOVEit campaign, CLOP demonstrated strong expertise in exploiting MFT platforms. It began publishing victims alphabetically in January, with several hundred victims in total.

9. RansomHub – Rise and Fall of the King

RansomHub remained the most active group through Q1 2025, offering 90% profit share to affiliates and breaching over 210 organizations. Its operations abruptly stopped on April 1. **The collapse triggered a major reshuffle, with hundreds of affiliates migrating to Qilin, DragonForce, and Lynx.** It was the largest structural shift since LockBit after Operation Cronos in 2024. It underscored the volatility and adaptability of the ransomware ecosystem.

10. Increase in Attacks Targeting Japan

Japan saw a 217% year-over-year rise in ransomware attacks from October 2024 to September 2025. Qilin recorded the most incidents, followed by Lynx, Nightspire, RansomHub, and Akira, mainly targeting SMBs with weak security.

A new group, Kawa4096 appeared in June, breaching two organizations with KaWaLocker. The ransomware uses Salsa20 encryption, multithreading, and filename hashing, with version 2.0 in July adding further enhancements. Manufacturing was the most affected sector, and small businesses made up most victims.

Key Takeaways

- DragonForce introduces a white-label model - affiliates operate under their brand while leveraging its infrastructure.
- CLOP ransomware exploits a zero-day vulnerability in Cleo MFT solutions – compromising around 400 organizations.
- Ransomware attacks on Japan surge by 217% – manufacturing and SMBs suffered the greatest impact.

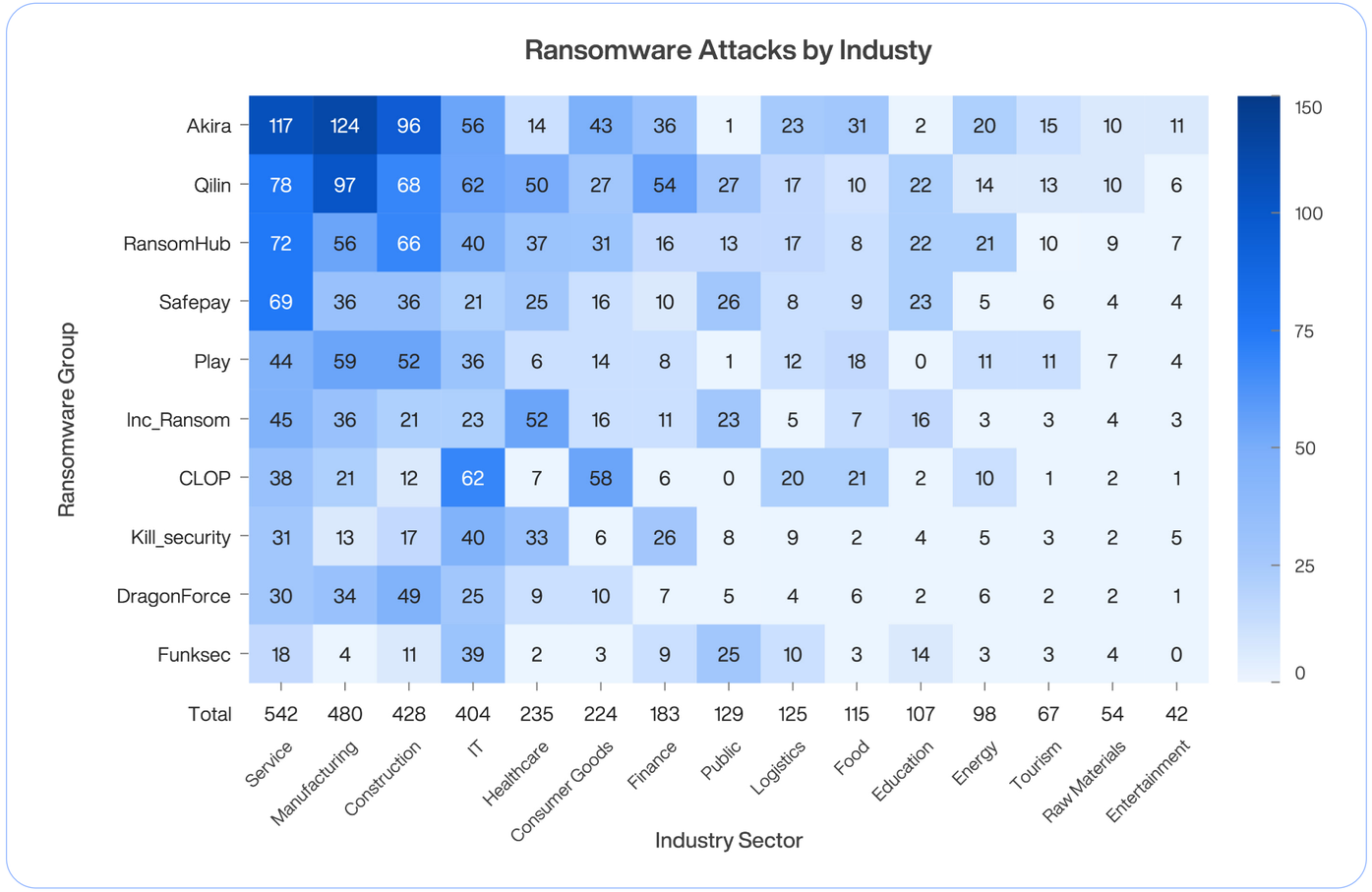
2025 Threat Landscape

Ransomware – Target Industries

Ransomware attacks show that service, manufacturing, construction, and IT sectors were the primary targets. **The biggest shift was the service sector becoming the most affected,** driven by higher digital dependence after COVID-19 and immediate revenue loss when systems go down.

Manufacturing and construction sectors remained major targets. Manufacturers saw a broader attack surface due to smart-factory and supply-chain systems. Production shutdowns cause direct financial losses, increasing the likelihood of ransom payment. Construction also faced heavy targeting, as project delays often lead to penalties and legal disputes. IT companies continued to be hit because of the large volumes of customer data they manage.

The most concerning trend was the sharp rise in attacks on healthcare. Although long considered off-limits, that barrier collapsed in 2025. BlackCat, for instance, reemerged after being dismantled in 2024 and lifted its ban on hospital attacks, actively encouraging them. Because delays threaten patient safety and breaches expose highly sensitive data, healthcare has become a high-profit target. In contrast, food and tourism saw far fewer incidents due to lower digital dependency.



[Image] Ransomware Attacks by Industry (Oct 2024 – Sep 2025)

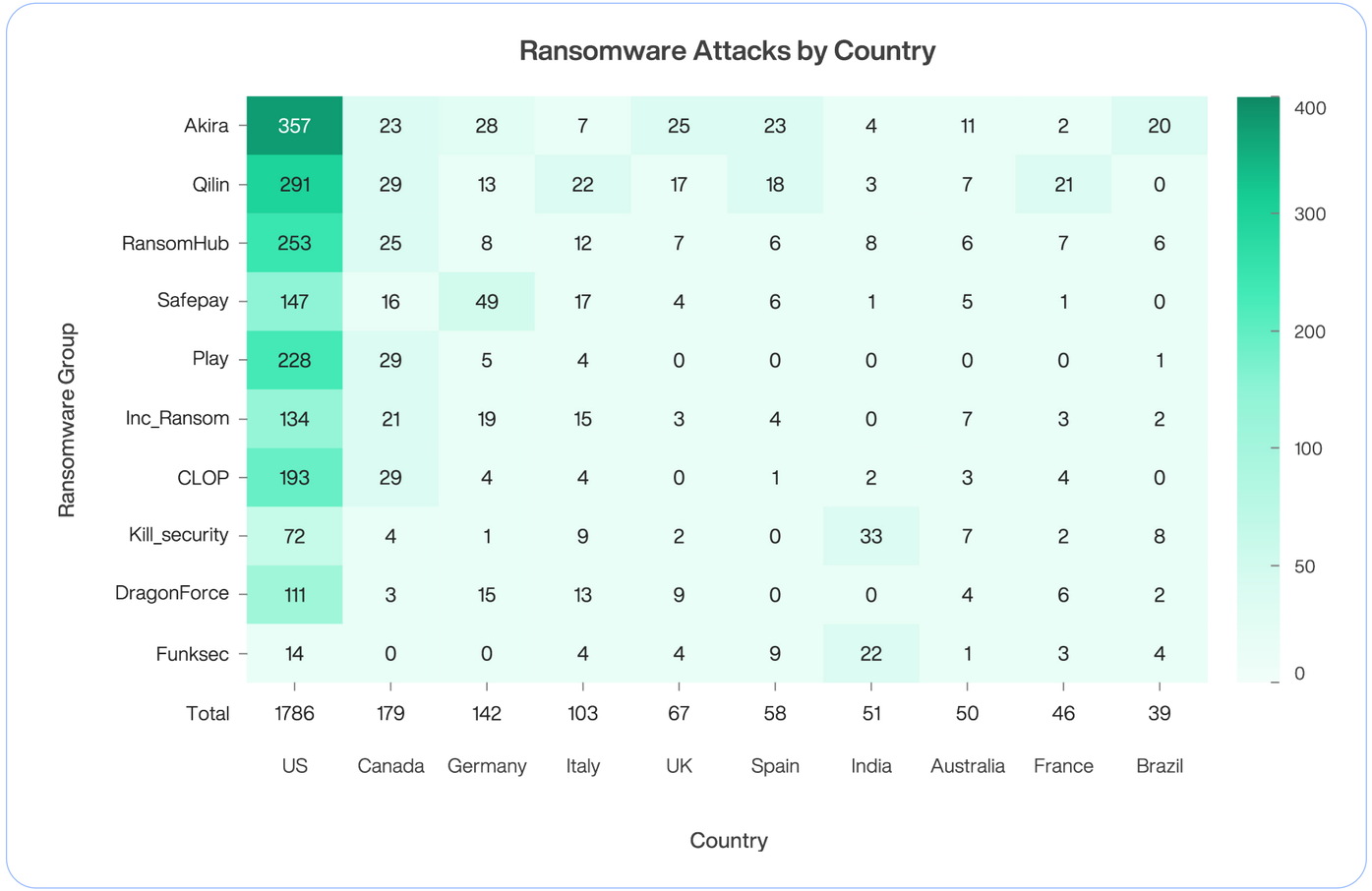
2025 Threat Landscape

Ransomware – Target Countries (Global)

The United States remained the most targeted country for ransomware in 2025. **Akira and Qilin maintained steady activity, while RansomHub continued targeting U.S. organizations until its shutdown in April.** As the world's largest economy, the U.S. concentrates high-value industries such as IT, healthcare, and finance. Large volumes of data stored in the cloud also make it a prime target for data theft and multi-stage extortion.

The diversification of attack patterns in Europe and Asia was also notable. Germany was heavily affected by Safepay and Akira, especially through data-extortion attacks. France and the UK experienced continuous pressure as well. **In Asia, India emerged as a key target as Kill_Security and Funksec expanded operations in the region.** Canada also remained heavily affected due to economic and structural similarities with the U.S.

In Europe, Qilin and Akira carried out sustained attacks on Spain and Italy, while in South America, Brazil faced concentrated attacks from Akira. In the Asia-Pacific region, Australia and Japan were the primary targets. The United States and its allies responded with coordinated investigations and sanctions against ransomware groups, but attackers continue to exploit jurisdictional gaps and evade enforcement by operating through infrastructure overseas.



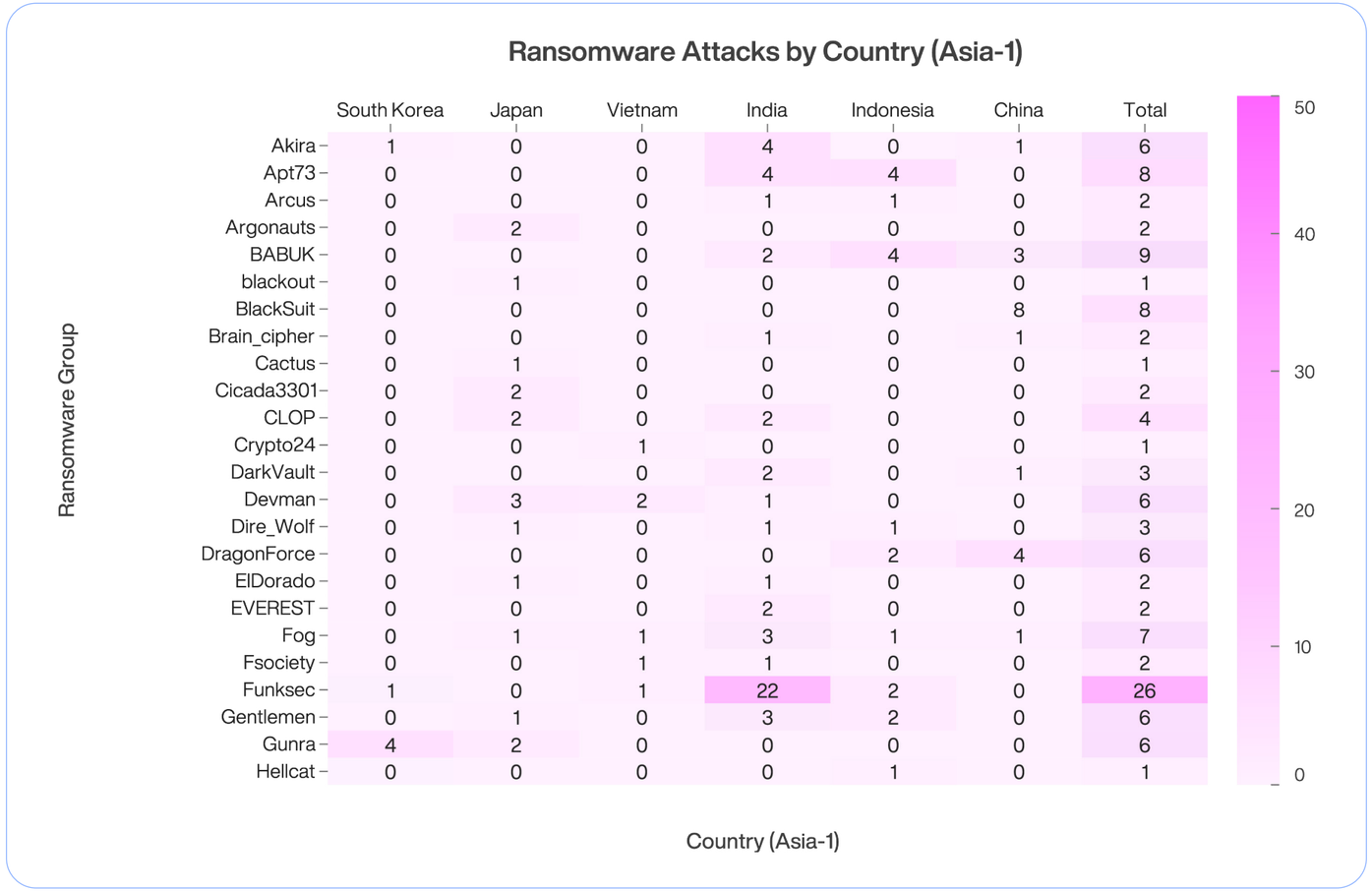
[Image] Ransomware Attacks by Country (Oct 2024 – Sep 2025)

2025 Threat Landscape

Ransomware – Target Countries (Asia 1)

Across Asian countries in 2025, **India became the primary target, overtaking Japan**. Taiwan, South Korea, and Japan recorded similar numbers of incidents, while the overall case count rose sharply from the previous year.

Threat concentration differed across countries. **South Korea and China showed a high level of activity from only a few dominant groups. In contrast, Japan and Indonesia displayed a broader and more distributed threat landscape,** which requires preparing for a wider range of intrusion tactics.



Ransomware Group	South Korea	Japan	Vietnam	India	Indonesia	China	Total
Akira	1	0	0	4	0	1	6
Apt73	0	0	0	4	4	0	8
Arcus	0	0	0	1	1	0	2
Argonauts	0	2	0	0	0	0	2
BABUK	0	0	0	2	4	3	9
blackout	0	1	0	0	0	0	1
BlackSuit	0	0	0	0	0	8	8
Brain_cipher	0	0	0	1	0	1	2
Cactus	0	1	0	0	0	0	1
Cicada3301	0	2	0	0	0	0	2
CLOP	0	2	0	2	0	0	4
Crypto24	0	0	1	0	0	0	1
DarkVault	0	0	0	2	0	1	3
Devman	0	3	2	1	0	0	6
Dire_Wolf	0	1	0	1	1	0	3
DragonForce	0	0	0	0	2	4	6
ElDorado	0	1	0	1	0	0	2
EVEREST	0	0	0	2	0	0	2
Fog	0	1	1	3	1	1	7
Fsociety	0	0	1	1	0	0	2
Funksec	1	0	1	22	2	0	26
Gentlemen	0	1	0	3	2	0	6
Gunra	4	2	0	0	0	0	6
Hellcat	0	0	0	0	1	0	1

[Image] Ransomware Attacks by Country – Asia (Oct 2024 – Sep 2025, 1/2)

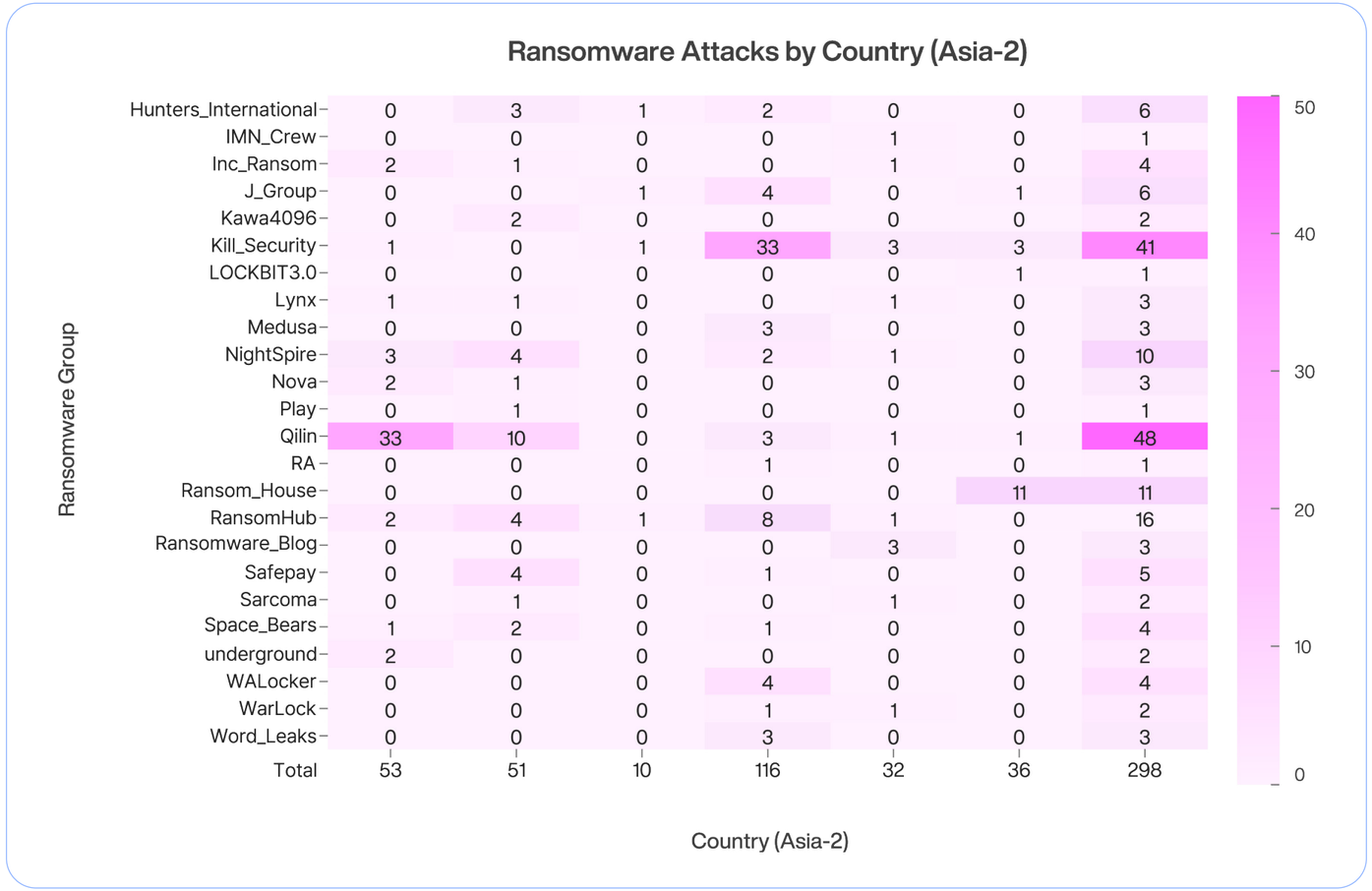
2025 Threat Landscape

Ransomware – Target Countries (Asia 2)

Qilin was the most active actor in Asia this year, with particularly concentrated operations in South Korea and Japan. Its surge in South Korea came from a supply chain breach in which the group compromised an IT service provider. Through that access, it simultaneously impacted several asset management firms. Kill_Security followed as the next most active group, showing a strong focus on India.

Ransomware activity across Asia in 2025 can be summarized by three key patterns: **an overall increase in incident volume, a shift in primary targets from Japan to India, and clear differences in threat-group concentration by country.**

With attacks continuing across South Korea, India, Japan, and other Asian nations, sustained monitoring and stronger security controls are essential. Organizations must also adapt their response strategies to reflect the evolving tactics of major threat groups such as Qilin and Kill_Security, which reorganized after the collapse of RansomHub.



[Image] Ransomware Attacks by Country – Asia (Oct 2024 – Sep 2025, 2/2)

2025 Threat Landscape

Other Threat Trend – Malware Top 9

In 2025, we witnessed various types of malware, with notable attacks targeting telcos, finance, and Linux infrastructure. Threat actors utilized ransomware and malware to exploit authentication mechanisms. New malware linked to North Korean APTs was identified, while existing families remained in steady circulation.

1. BPFDoor, a Stealthy Intruder Targeting Telcos

BPFDoor is a backdoor targeting Linux systems. It abuses the BPF network filtering to evade monitoring and gain access to internal systems.

It becomes active upon receiving specific packets. It communicates using network protocols to receive external commands and exfiltrate data. It masquerades as legitimate processes, duplicates files and deletes the originals to minimize traces, and attempts memory-based execution via the /dev/shm path. In 2025, BPFDoor was used in a campaign that breached the South Korean telco. The attack compromised customer authentication servers, highlighting the need for industry-wide security assessments.

2. Qilin Ransomware Attacking Financial Firms

Unlike other ransomware written in C, **Qilin is developed in Rust and supports both Windows and Linux.** While typical ransomware encrypts files once, it encrypts the file three times on Linux. It also has features for backup deletion and recovery disruption. Highly organized, Qilin offers legal and PR support to affiliates.

Qilin attacked South Korean asset management companies. It attacked a cloud server shared by multiple firms and leaked data onto the dark web.

3. Gunra Ransomware, Recovered without Negotiation

Gunra is known to use the source code of Conti. Supporting both Windows and Linux, it selectively encrypts only a victim's critical assets to maximize operational disruption.

Gunra launched consecutive attacks against South Korean organizations and leaked data onto the dark web. **Analysts discovered a structural flaw in the encryption key generation of its Linux variant.** Thus, one of the victims was able to extract the decryption key and recover its data.

Key Takeaways

- BPFDoor only activates upon receiving specific packets and exfiltrates data.
- Qilin is developed in Rust and supports Windows and Linux – attacking Korean financial firms
- Gunra's Linux variant contains a structural flaw in key generation, which allows for decryption.

2025 Threat Landscape

Other Threat Trend – Malware Top 9

4. Plague Malware Exploiting Linux Authentication

Plague malware intercepts the login process on Linux to steal user account credentials. It runs automatically at system boot and captures ID/PW entered during SSH or terminal logins.

Linux systems validate logins via PAM authentication. Plague exploits the LD_PRELOAD technique to insert itself ahead of legitimate authentication. As a result, the malware silently intercepts login credentials before the system processes them.

It deletes login records and alters system settings to ensure persistence across reboots. Recent variants have evolved with enhanced stealth and detection-evasion capabilities.

5. Malware Spreading via USBs

USB malware still remains effective. **There were cases of coinminers spreading through infected USBs.**

Attackers hide LNK files on the compromised USB. When a user executes them, a PowerShell script installs the XMRig. The malware communicates with PostgreSQL to send and receive commands, having a more sophisticated communication structure than typical malware, which enables external control and monitoring of mining activity. It also downloads malicious files from GitHub and uses the run key of the Windows Registry for persistence, ensuring auto-execution after reboot and continuous mining.

6. Infostealer Disguised as Fake Ads

Attackers display Facebook ads disguised as well-known exchanges like Binance. When users click the ads, they are redirected to a fake website and prompted to download an installer.msi. The file checks whether the victim environment meets the attacker-defined conditions, and then registers a scheduler to download and run an infostealer payload.

Users outside the target are redirected to normal websites to evade detection. Simply visiting the URL does not result in infection. The malware retrieves additional payloads via PowerShell and collects sensitive data, including system information and browser-stored data.

Key Takeaways

- Plague malware intercepts the login process on Linux to steal user account credentials.
- Coinminers spread via infected USBs – hiding malware on the compromised device
- Fake Facebook ads disguised as exchanges > website redirection > downloading malware

2025 Threat Landscape

Other Threat Trend – Malware Top 9

7. Proxyware Sharing the Victim's Network Resources

A malware abusing Proxyware has emerged as a significant cyber threat. **Attackers install Proxyware without user consent, covertly sharing the victim's network resources.** Numerous cases of this "proxyjacking" have been identified, where attackers generate revenue through unauthorized bandwidth usage.

It is often distributed alongside the Mimo coinminer or automatically installed during freeware installations through advertising pages. Victims experience degraded system performance and network speed.

Attackers complicate detections as Proxyware maintains continuous communication with external servers and allocates resources according to attacker-defined rules. It is similar to cryptojacking, but it exploits network bandwidth rather than CPU resources.

8. BeaverTail and Tropidoor, Phishing Campaign by Lazarus

Lazarus actively utilizes BeaverTail and Tropidoor malware by distributing them via job recruitment phishing emails. Attackers impersonate legitimate companies and target developers or IT professionals, embedding Bitbucket links that contain malicious projects to initiate infections.

BeaverTail is an infostealer that collects browser-stored credentials and crypto-wallet data. Tropidoor is a backdoor that enables long-term intrusion through system information gathering, command execution, and screen capture.

9. EndRAT, Kimsuky's New Malware

EndRAT is a new AutoIt-based remote access trojan (RAT) used by Kimsuky since July 2025.

It contains the unique communication identifiers "endServer9688" and "endClient9688". It is typically distributed by enticing victims to execute LNK files. It was also observed being delivered through an MSI installer disguised as a program called "Stress Clear." Its use of AutoIt scripts, execution conditions, and specific strings within its communication protocol set it apart from previously known malware used by the group.

Key Takeaways

- Attackers install Proxyware without user consent and covertly share the victim's network resources.
- Lazarus has launched phishing campaigns against IT professionals by using BeaverTail and Tropidoor malware.
- Kimsuky began using a new "EndRAT" using AutoIt scripts and unique communication identifiers.

2025 Threat Landscape

Other Threat Trend – Attack Techniques Top 10

1. Software Supply Chain Attack

Attackers infiltrated open-source package repositories (such as npm and PyPI) or tampered with libraries and developer tools to spread malware through updates and installations. These attacks compromised development and CI/CD environments, resulting in source code theft, backdoor insertion, and credential collection. Notably, multiple incidents in 2025 exploited trusted code-signing and automated deployment, posing a serious threat to the integrity and reliability of the broader open-source ecosystem.

2. Credential Theft and MFA Evasion (T1078)

Attackers obtain valid accounts to infiltrate VPN, SSO, and cloud services. **To bypass MFA, they use proxy-based authentication-in-the-middle tools such as EvilProxy or trigger repeated authentication prompts on user devices to induce accidental approval.** APT29 and Scattered Spider have leveraged these techniques to remain hidden and expand their foothold within networks.

3. Cloud Attack and Repatriation

Cloud repatriation moves cloud workloads back on-premises to optimize costs, improve performance or meet regulations. **The lack of built-in cloud security controls can pose risks, including misconfigurations and inadequate security settings.** Cloud services are experiencing growing incidents involving OAuth token theft and credential abuse, which enable lateral movement and privilege escalation.

4. AI and LLM-Powered Attack

Attackers leverage AI and LLMs to automate malware generation, detection evasion, phishing content creation, and deepfake production. This has increased both the efficiency and sophistication of attacks, making them difficult to block with traditional detection techniques. Automated tools also enable rapid design and deployment of large-scale targeted attacks, reducing defenders' response time.

Top 10 Attack Techniques

1. Software Supply Chain Attack
2. Credential Theft and MFA Evasion
3. Cloud Attack and Repatriation
4. AI and LLM-Powered Attack
5. Remote Access and Breach
6. MoTW Bypass and ZIP Exploits
7. Cloud-based C2
8. Phishing Email Attachment
9. DLL Search Order Hijacking
10. Living Off the Land

2025 Threat Landscape

Other Threat Trend – Attack Techniques Top 10

5. Remote Access and Breach (T1133)

There are various infiltration attempts through remote access via RDP, VPN, and VDI. Vulnerabilities in firewalls and VPNs at the perimeter are major entry points. Attackers gain initial access through exposed ports, weak credentials, and insecure authentication. They move laterally inside the network by hijacking SSO sessions and bypassing authentication. Zero-day vulnerabilities in Ivanti, Fortinet, Cisco, and Palo Alto Networks appliances have been widely exploited in APT campaigns.

6. MoTW Bypass and ZIP Exploits (T1553.005)

Attackers continue to evade Windows' Mark of the Web (MoTW) security feature. **They bypass MoTW by using ISO or ZIP files to prevent MoTW from being applied to internal files. They manipulate LNK file structures and exploit the 7-ZIP vulnerability (CVE-2025-0411) to remove MoTW,** allowing malicious files to run without alerts. As a result, users open malicious files without recognizing the risk, which can lead to account compromise or ransomware infection.

7. Cloud-based C2 (T1071.001)

Attackers are increasingly using web services and cloud platforms—such as GitHub, Google Drive, and Telegram—for C2 communication. By disguising themselves as normal network traffic, they make it difficult for firewalls and IDS to detect malicious behavior. In 2024, CloudSorcerer hid encrypted commands on GitHub and communicated with compromised systems through the Microsoft Graph API and Yandex Cloud. Gamaredon, Kimsuky, and PteroBox also employ this technique.

8. Phishing Email Attachment (T1566.001)

Attackers employ social-engineering-based spear-phishing as a primary intrusion method. Malicious attachments commonly include LNK, CHM, ZIP, and RAR files; some have shifted to using malicious URLs and QR codes. They also use ClickFix technique, inducing users to click, enter credentials, or install malicious files, enabling internal network access and credential theft. MuddyWater and Konni have been using the email attachment for lateral movement.

9. DLL Search Order Hijacking (T1574.001) DLL Side Loading (T1574.002)

DLL search order hijacking manipulates the Windows DLL loading sequence to load a malicious DLL instead of a legitimate one. It is abused for privilege escalation, remote code execution, and persistence. It has been observed in ShadowPad ransomware campaigns and the exploitation of the vulnerability in NI LabVIEW (CVE-2025-2630). Attackers place malicious DLLs in vulnerable directories to maintain privileges while evading detection.

10. Living Off the Land (T1059)

Attackers use "Living Off the Land (LOTL)" techniques, leveraging legitimate Windows tools such as PowerShell and WMI. This technique allows them to evade antivirus and EDR by masking malicious activity within trusted processes. According to Microsoft, China-linked APTs, including Volt Typhoon, used wmic, netsh, and PowerShell in their campaigns targeting U.S. infrastructure to gain privileges, collect credentials, and conduct network reconnaissance.

2025 Threat Landscape

Other Threat Trend – Vulnerabilities Top 10

1. Ivanti Connect Secure VPN (CVE-2024-21887, CVE-2025-22457)

Ivanti Connect Secure VPN's authentication bypass vulnerability (CVE-2023-46805) and command injection flaw (CVE-2024-21887) have remained prime targets for attackers. UNC5221, an APT group, exploited an overflow–based remote code execution vulnerability disclosed in April 2025 (CVE-2025-22457). Attackers leveraged these flaws to deploy web shells and backdoors, infiltrating governments and financial institutions.

2. FortiOS and FortiProxy (CVE-2025-24472)

In early 2025, an authentication bypass vulnerability in FortiOS and FortiProxy (CVE-2025-24472) was disclosed, allowing **attackers to obtain super-admin privileges and full control over targeted networks.** Multiple incidents were reported in which the vulnerability was exploited during the initial intrusion stage, resulting in severe damage to large enterprises and financial institutions. Attack attempts surged sharply following the release of the vulnerability PoC.

3. PAN-OS and GlobalProtect (CVE-2024-0012)

Palo Alto Networks **PAN-OS vulnerabilities (CVE-2024-0012, CVE-2025-0108) were chained with a privilege-escalation flaw (CVE-2024-9474) and an authenticated file-read vulnerability (CVE-2025-0111) to obtain root privileges, modify configurations, and access sensitive data.** The zero-day vulnerability in GlobalProtect (CVE-2024-3400) was exploited to facilitate remote shell establishment and lateral movement within internal networks.

4. Cisco ASA and Firepower (CVE-2025-20333, CVE-2025-20362)

Zero-day and N-day vulnerabilities exploited by ArcaneDoor were discovered in Cisco ASA and Firepower. CVE-2025-20333 enables remote code execution through a VPN web server flaw, while CVE-2025-20362 allows invalid access to restricted URLs. CISA instructed federal agencies to identify affected assets, collect forensic data, and conduct patches. Cisco also confirmed persistence techniques involving the manipulation of ROMMON and the boot chain.

Top 10 Vulnerabilities

1. Ivanti Connect Secure VPN
2. FortiOS and FortiProxy
3. PAN-OS and GlobalProtect
4. Cisco ASA and Firepower
5. File Transmission Program
6. Sitecore RCE
7. Web Browser Zero-Day
8. Android Privilege Escalation
9. File Compression Software
10. Open-Source SW Supply Chain

2025 Threat Landscape

Other Threat Trend – Vulnerabilities Top 10

5. File Transmission Program (MOVEit, Cleo)

Remote code execution and authentication-bypass vulnerabilities were identified in MFT products, including Cleo Harmony and VLTrader. CLOP ransomware actors leveraged them to compromise multiple organizations.

CVE-2024-50623 enables remote code execution by abusing unrestricted file upload and download capabilities. CVE-2024-55956 allows unauthenticated command execution by manipulating the Autorun directory configuration. MOVEit Transfer's CVE-2024-5806, a SFTP authentication flaw, also allowed authentication bypass. As a result, Safe Wallet's frontend assets were compromised, and funds were stolen. The FBI attributed this to North Korean threat actor TraderTraitor.

6. Sitecore RCE (CVE-2025-534690)

The ViewState deserialization vulnerability in Sitecore (CVE-2025-534690) enables remote code execution without prior authentication. The root cause was the reuse of sample machineKey values in an older deployment guide. Evidence of exploitation began appearing in late 2024, and an official advisory was released in September 2025.

Attackers gained initial access through internet-exposed Sitecore instances, then deployed remote shells and conducted system and domain reconnaissance, credential collection, and lateral movement. They exfiltrated sensitive data, including configuration files and secret keys.

7. Web Browser Zero-Day

(Chrome: CVE-2024-4947, Firefox CVE-2024-9680)

Zero-day vulnerabilities in web browsers have been exploited in real-world attacks. **The Chrome V8 engine vulnerability (CVE-2024-4947) enables code execution by visiting a crafted webpage.** Lazarus-affiliated threat actors have exploited it in campaigns targeting the financial sector. RomCom, the Russian APT group, exploited Firefox's use-after-free vulnerability (CVE-2024-9680) to deploy backdoors during espionage campaigns across Europe and North America. These vulnerabilities have been leveraged in attack chains involving credential theft, payload execution, and the establishment of persistence.

Key Takeaways

- MFT products (Cleo Harmony and VLTrader) had remote code execution and authentication-bypass vulnerabilities.
- The ViewState deserialization vulnerability in Sitecore appeared due to the reuse of old machineKey values.
- The Chrome V8 engine vulnerability enables code execution by just visiting a specially crafted webpage.

2025 Threat Landscape

Other Threat Trend – Vulnerabilities Top 10

8. Android Privilege Escalation
(Android CVE-2025-38352)

Threat actors have exploited the Android vulnerability (CVE-2025-38352) for local privilege escalation, enabling malicious apps to expand their device permissions. In several observed cases, it was chained with web browser zero-day vulnerabilities: after initial device compromise, attackers stole credentials and executed additional payloads. With elevated privileges, malicious apps can modify system settings, access sensitive data, and disable security features. These techniques pose significant risks in targeted mobile attacks, potentially leading to financial theft or espionage.

9. File Compression Software
(CVE-2025-0411, CVE-2025-8088)

Attackers are increasingly exploiting vulnerabilities in compression programs as part of their intrusion workflows. Notably, 7-Zip and WinRAR have been targeted in real-world attacks. **The 7-Zip MoTW bypass vulnerability (CVE-2025-0411) was leveraged by Russian threat actors to distribute SmokeLoader against Ukrainian government agencies and private organizations.** WinRAR was found to contain path search vulnerabilities (CVE-2025-6128, CVE-2025-8088). In particular, RomCom has exploited CVE-2025-8088 in attacks targeting logistics, manufacturing, financial, and defense companies across Europe and Canada.

10. Open-Source Software Supply Chain
(ex: npm package)

A series of supply chain attacks compromised open-source maintainers' accounts by injecting malware into libraries such as JavaScript npm packages. In September 2025, multiple npm packages were breached following phishing attacks and token theft. PyPI issued an official warning about phishing campaigns directed at developers, highlighting the risk of account takeover. In the container ecosystem, numerous Docker Hub images contained the XZ backdoor. In the Rust ecosystem, a malicious crate designed to steal wallet keys was identified and immediately removed.

Key Takeaways

- Attackers exploited the Android vulnerability for privilege escalation - malicious apps expanding device permissions.
- Russian threat actors have exploited the 7-Zip MoTW bypass vulnerability to compromise the Ukrainian government.
- A series of supply chain attacks compromised open-source maintainers' accounts by injecting malware into libraries.

2025 Threat Landscape

Other Threat Trend – Mobile Threat Top 6

1. Social Engineering and Mobile Scams

In 2025, mobile-focused crimes leveraging social engineering techniques have evolved. **Attackers tailor malicious apps to trending social issues and impersonate telcos, AI applications, and even government agencies to attract victims' attention.** Numerous scam apps have also been observed that disguise themselves as investment opportunities—such as meme stocks or IPOs—to build trust and lure victims into fraudulent investment schemes. These apps promise high returns and persuade victims to install malicious apps.

Victims are shown manipulated profit figures within the app. When they attempt to withdraw their money, attackers refuse under various pretexts and eventually disappear. Additionally, "sextortion" apps continue to surface: attackers entice victims to install apps supposedly enabling private conversations, then steal contact lists, photos, and other sensitive data, later using them to extort payment under threats of exposure.

2. Malicious Apps with New Features

Malicious apps are leveraging Android's HCE (Host Card Emulation) to intercept NFC communication. Known as "NGate," this app not only intercepts NFC traffic but also displays fake screens to steal user credentials. These apps capture NFC data exchanged when interacting with NFC-enabled devices and transmit it to attackers, who then use the data to perform unauthorized ATM withdrawals and other fraudulent activities. Also, new apps have emerged that target crypto assets by exploiting OCR (Optical Character Recognition) libraries. Attackers exploit users who store mnemonic phrases as images when backing up their crypto wallets. They use OCR to analyze, extract, and steal mnemonic phrases and other data embedded in images.

3. More Malicious Apps in App Stores

Various malicious apps are emerging even in official app stores - banking credential stealers (Banker), high-interest loan scams (SpyLoan), cryptocurrency-theft malware (SparkCat, SparkKitty), hidden advertisement loaders (HiddenAds), and investment fraud apps (ScamFX).

In particular, a banking malware has evolved to evade app-store security screening. **Instead of embedding malicious features directly, attackers now register apps that appear valid, then execute malicious payloads after installation.** Some apps activate features only under specific conditions, considering environments, regions and languages.

Key Takeaways

- Social-engineering – Attackers use decoy apps impersonating telcos, AI apps, and governments to lure victims.
- New malicious apps leverage Android's HCE to intercept NFC communication and steal sensitive data.
- Attackers register valid-looking apps on app stores, then execute malicious payloads after installation.

2025 Threat Landscape

Other Threat Trend – Mobile Threat Top 6

4. Zero-Day Vulnerability Exploitations

In addition to CVEs, we have seen more attacks exploiting unreported vulnerabilities. Because these flaws are unknown before disclosure, attackers leverage them as zero-days to distribute malicious apps. Victims remain exposed until security patches are released.

A notable example is the Pixnapping vulnerability. By exploiting this flaw, attackers can extract pixel data on certain Android devices running versions 13 to 16; they exploit semi-transparent overlays to steal sensitive data such as MFA codes. Another case is CVE-2024-43093, an elevation-of-privilege vulnerability that exploits “Contacts Directory” to automatically launch apps without user interaction. This allows malicious apps to activate harmful features in the background.

5. Spy Apps from North Korea

North Korean threat actors continue to distribute spy apps to steal sensitive data. These apps masquerade as utility apps—such as file managers or software updaters—with interfaces and features crafted to appear fully legitimate.

Attackers employ techniques including code obfuscation, encryption, dynamic loading, and conditional execution to hinder analysis. The apps communicate with C2 servers to receive commands and exfiltrate stolen data. Some C2s have even hosted crypto-phishing pages, indicating that these operations are expanding into crypto-asset theft as well.

6. Distribution of Infected Devices

There are Android smartphones, set-top boxes, and others being distributed with malware (Mirai and HiddenAds variants) preinstalled even before leaving the manufacturer. The malware operates in the background without the user’s awareness, potentially causing increased network traffic, battery drain, and personal data leakage.

Malicious USB cables also continue to surface. These cables contain embedded chipsets that abuse data-transfer features, enabling unauthorized file access, command execution, and data theft on connected devices.

Key Takeaways

- Beyond CVEs, attackers are increasingly leveraging unreported vulnerabilities in mobile platforms.
- North Korean threat actors disguise spy apps as utilities to keep themselves hidden and steal critical data.
- Some smartphones and set-top boxes have been found to contain malware at the manufacturing stage.

2025 Threat Landscape

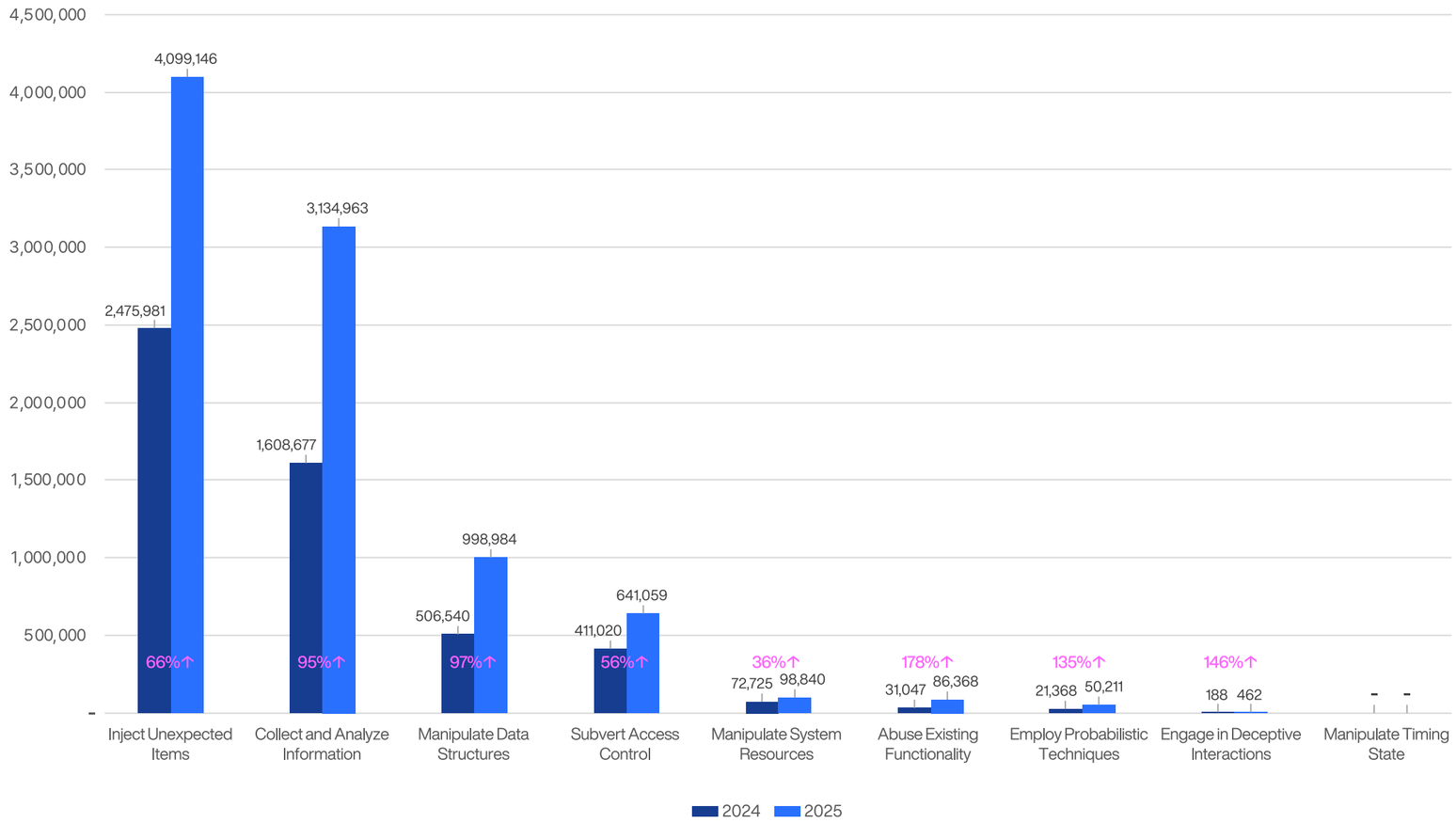
Statistics – Cyber Attack Types

Our incident response unit, the Computer Emergency Response Team (CERT), publishes a monthly report that analyzes ongoing cyber threat trends. Based on these reports, we have summarized the statistics for cyberattack types in 2025.

In 2025, the total number of detected attacks increased by 78% year-over-year. All attack categories saw double-digit growth, with some increasing by more than 100%. This is attributed to advancement of AI-driven attacks, expansion of cloud, and widespread exploitation of supply chain vulnerabilities.

The most prevalent attack type was “inject Unexpected Items”, maintaining its top position from 2024. This was followed by Collect and Analyze Information, Manipulate Data Structures, Subvert Access Control, and Manipulate System Resources.

2025 Cyber Attack Type Stats



2025 Threat Landscape

Statistics – Cyber Attack Type Glossary

1. Inject Unexpected Items

It is a technique in which adversaries manipulate a system by supplying abnormal or unexpected data through input interfaces. This occurs due to insufficient input validation or poor input-handling logic. The system may perform abnormal behavior, bypass security controls, or leak sensitive data.

2. Collect and Analyze Information

This technique involves **attackers actively querying or passively observing a target system to gather and analyze information.** They collect details such as system configurations and user accounts to design future attack paths or identify potential vulnerabilities. It is typically used prior to initial intrusion.

3. Manipulate Data Structures

It deliberately **alters internal data structures within a system, disrupting data-processing flows.** By tampering with the data structure, attackers can trigger abnormal outcomes. Such manipulation not only causes unexpected errors but also compromises the integrity and reliability of the data.

4. Subvert Access Control

This attack technique involves **bypassing or disabling access-control mechanisms to obtain unauthorized privileges and improperly access system resources.** By gaining administrative or elevated user privileges, attackers can access sensitive data or manipulate critical functions.

5. Manipulate System Resources

This technique **exhausts a victim's system resources to degrade performance or deplete available capacity.** As resources are consumed, the system becomes unable to provide normal services, leading to slower responses or complete freezes. Prolonged resource exhaustion can result in DoS-like impact.

6. Abuse Existing Functionality

This technique **abuses normal features of a system or application** to cause harm, without adding new code. Instead, attackers use existing functionality for malicious purposes. For example, they may use a customer service file-upload feature to deliver malicious file or to expose internal data.

7. Employ Probabilistic Techniques

This technique **probes system weaknesses and gradually increases the probability of a successful compromise.** A common example is brute force, in which attackers guess passwords repeatedly. It is particularly effective against systems with weak encryption or authentication mechanisms.

8. Engage in Deceptive Interactions

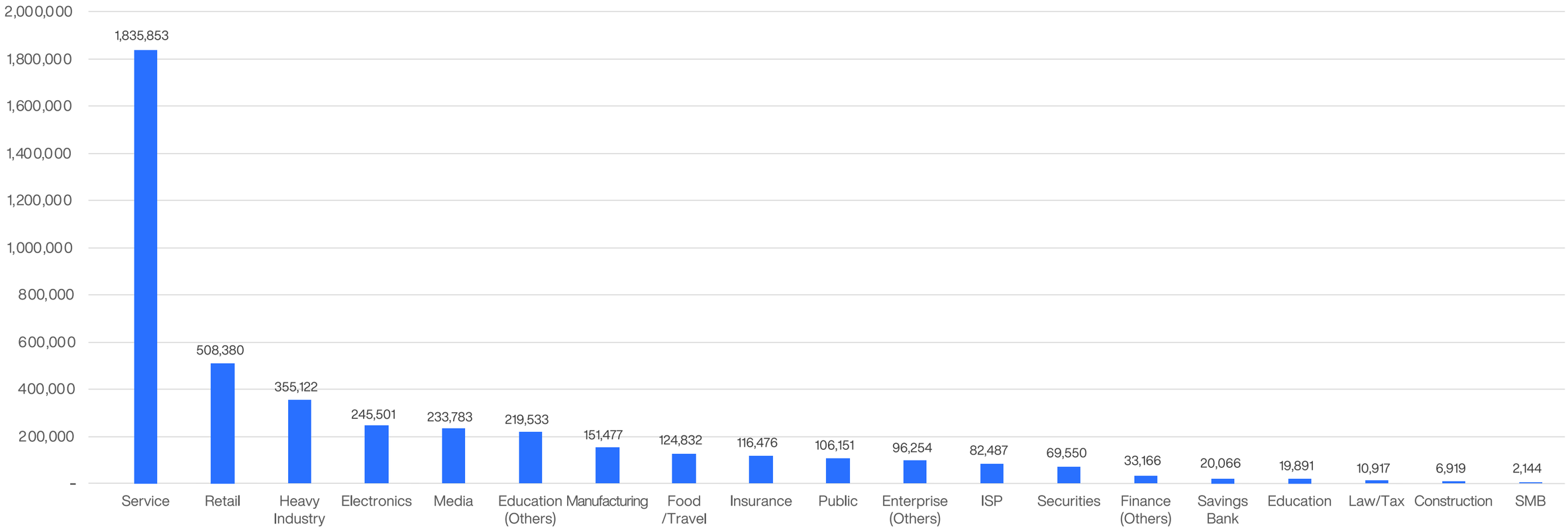
This technique **conceals the attacker's identity and intent during interactions with systems,** delivering misleading data to achieve a desired outcome. Common examples include phishing emails and fake websites. Attackers deceive users into entering sensitive data or downloading malicious files.

2025 Threat Landscape

Statistics – Cyber Attack Frequency per Industry

In the 2025 2H, the service sector recorded the highest number of attacks with 1,835,853 incidents, followed by retail (508,380), heavy industry (355,122), and electronics (245,501).

2025 2H – Cyber Attack Frequency per Industry



2025 Threat Landscape

Statistics – Cyber Attack Type per Industry

2025 2H – Cyber Attack Type per Industry

	Inject Unexpected Items	Collect and Analyze Information	Manipulate Data Structures	Subvert Access Control	Manipulate System Resource
Service	43%	33%	12%	9%	1%
Retail	37%	50%	7%	3%	1%
Heavy Industry	51%	34%	8%	3%	1%
Electronics	48%	14%	20%	12%	1%
Media	38%	40%	9%	10%	2%
Education (Others)	28%	62%	6%	3%	1%
Manufacturing	48%	37%	11%	2%	1%
Food/Travel	41%	48%	6%	5%	0%
Insurance	30%	62%	4%	4%	0%
Public	40%	45%	7%	5%	1%
Enterprise (Others)	50%	41%	6%	2%	0%
ISP	38%	53%	6%	3%	0%
Securities	53%	30%	9%	3%	4%
Finance (Others)	44%	39%	12%	3%	1%
Savings Bank	41%	36%	10%	8%	0%
Education	49%	42%	6%	3%	1%
Law/Tax	50%	29%	13%	6%	0%
Construction	35%	51%	8%	4%	1%
SMB	80%	1%	9%	3%	0.0%

2026 Outlook

→ 2026 Outlook Top 5

1. Explosive Growth of AI-Driven Cyber Attacks
2. Organized and Diversified Ransomware Operations
3. Supply Chain Attacks Targeting Open-Source Ecosystems
4. Evolving Campaigns Against National Infrastructure
5. Surge in Cyber Attacks on Linux Systems

2026 Outlook

1. Explosive Growth of AI-Driven Cyber Attacks

→ Learn more about our AI-powered security strategies

AI-Driven Tailored Campaigns

In 2026, we expect a surge of adaptive AI-driven attacks, capable of analyzing a victim's environment in real-time and generating tailored malware. AI can produce numerous code variants to evade detection, enabling attackers to bypass traditional security controls. The importance of behavioral detection and dynamic analysis will grow significantly beyond static detection technologies.

Evolving deepfakes are will enable real-time phishing through realistic impersonations of a victim's voice or face during video or phone calls. As campaigns continue to improve, it will become increasingly difficult for victims to identify fake synthetic voices that attempt to steal critical data.

Also, AI-powered scam automation is expected to accelerate. Attackers will mass-generate fake websites, chatbots, and online stores capable of interacting convincingly with victims. We expect to see much larger volumes of automated and nearly indistinguishable AI phishing campaigns in 2026.

In addition, AI will contribute to the development of new hacking techniques. By identifying vulnerabilities and analyzing behavioral patterns, AI may uncover previously unknown security flaws that can be weaponized for zero-day attacks. Ultimately, the use of AI by attackers will lower the barrier to entry for hacking while ncreasing both the frequency and precision of attacks.

Sophisticated Attacks Targeting AI Models

Attacks targeting AI models are also expected to grow. Key techniques include prompt injection & data poisoning, prompt leakage, and model inversion. Attackers may inject malicious inputs into chatbots and AI models or manipulate training data to trigger a malfunction or data disclosure. Such attacks fundamentally undermine the integrity of AI-based systems and security solutions.

Attackers will also attempt to steal AI prompts. If prompts are exposed—such as through code-sharing platforms like GitHub—adversaries can exploit them to distort AI behavior. As AI adoption increases, safeguarding prompts and protecting associated data will become a critical security priority.

Furthermore, attackers can perform model inversion by issuing repeated queries to analyze how a model operates and extract information about its training data. By examining model responses, they can infer internal structures and leak sensitive data. Threat actors are expected to increasingly use this technique against vulnerable AI models to expand their attacks.

Key Takeaways

- There will be an increase in AI-based malware, deepfakes, automated scams, and zero-day vulnerability exploitations.
- Techniques such as prompt injection, prompt leakage, and model inversion will become more sophisticated.

2026 Outlook

2. Organized and Diversified Ransomware Operations

→ Learn more about our unified security approach to anti-ransomware.

Ransomware Fragmentation and Cartel Formation

In 2025, major ransomware groups such as LockBit and RansomHub saw their influence weaken or their operations cease. However, this did not lead to a decline in the overall ransomware ecosystem. **The weakening of large groups triggered the emergence of numerous new and smaller groups—including Akira, Qilin, Play, and Gunra.** As observed in 2025, these new groups are actively conducting cyber attacks, and this reshaped ransomware landscape is expected to persist into 2026.

Collaboration between APT groups and ransomware operators, along with the cartelization of RaaS, is expected to intensify in 2026. Centralized platforms offering attack infrastructure, tooling, and services—combined with revenue-sharing models where affiliates receive 80% and operators take 20%—have become well established within the ransomware economy. APT-ransomware partnerships, observed in 2025, are likely to grow further amid escalating geopolitical tensions.

As a result, defenders will face a broader and more frequent stream of intrusions, increasing the complexity of security operations. The further fragmentation of the ransomware ecosystem and the rise of inter-group collaboration will also make attribution more challenging.

Growth in SMB-Targeted Attacks

A key trend of the 2025 ransomware landscape is the lowered barrier to entry and increased diversification of attack methods. For financially motivated actors, targeting large enterprises—which yield higher potential payouts per incident—remains a rational strategy. Conglomerates are expected to remain primary targets in 2026 as well.

However, in an environment where adversaries can easily execute diverse attacks, **ransomware campaigns against small and medium-sized businesses (SMBs) are projected to rise sharply.** Attackers can continuously create new ransomware strains and variants, and SMBs—often lacking comprehensive multilayer security—are more likely to be successfully compromised.

In 2025, some threat actors actually shifted away from large enterprises in favor of SMBs. Smaller organizations must remain vigilant against targeted intrusions and social-engineering tactics. They must also assume that similar attacks may recur at any time.

Key Takeaways

- Ransomware remains a core criminal revenue model – Even as group names change, attack volumes will rise.
- Adversaries are precisely targeting beyond file encryption to databases, backup solutions, and VMs.
- With ransomware becoming easier to deploy, attacks against SMBs with weaker security postures are expected to grow.

2026 Outlook

3. Supply Chain Attacks Targeting Open-Source Ecosystems

→ Discover how we safeguard open-source ecosystems with zero trust strategy.

Exploiting Open-Source for Bigger Damage

In 2025, supply chain attacks targeting open-source package registries surged. Large volumes of malicious packages spread across ecosystems, and numerous incidents involved leaked developer passwords and CI/CD tokens. Given that modern software development relies on open-source components for more than 90%, a single compromised package can trigger cascading impacts.

These threats are expected to intensify in 2026. **Attackers are likely to refine techniques that harvest sensitive data during installation or within CI pipelines to trigger chain infections.** A combination of techniques—such as typosquatting, account takeover, and dependency confusion attacks—is expected to be used more frequently and in more sophisticated ways.

For organizations exposed to such supply chain risks, **the top priority is achieving visibility across the entire pipeline by continuously monitoring open-source usage and data flows.** This visibility enables rapid response when vulnerabilities arise, minimizing damage and improving resilience.

Beyond Software to Cloud and Hardware

In 2025, supply chain attacks expanded beyond software to include cloud services, managed service providers (MSPs), and even cybersecurity vendors. For example, DragonForce and Scattered Spider targeted cloud MSPs and launched campaigns impacting their customers simultaneously.

We have also seen supply chain attacks extended from software into hardware. Some Android-based smartphones, set-top boxes, and other devices were found to contain malware before leaving the manufacturer. If these devices are mass-distributed, the scale of damage is beyond imagination.

Consequently, we expect adversaries to target software, cloud services, and hardware in 2026 to pursue maximum impact. As supply chain attacks transcend national borders, multinational cooperation and a unified supply-chain security framework will be needed more than ever.

Key Takeaways

- Open-source is essential to software development, but its openness and dependency make it attractive for attackers.
- Securing open-source usage requires end-to-end visibility and control across the entire pipeline.
- In 2026, supply chain attacks are expected to span all domains - software, cloud, and hardware.

2026 Outlook

4. Evolving Campaigns Against National Infrastructure

→ Learn more about how our market-leading CPS protection platform secures key industries.

Striking Core Industries (Geo-Political Tension)

According to our analysis, nearly half of ransomware attacks targeted critical infrastructures such as manufacturing, healthcare, and energy in 2025. These sectors attract adversaries due to the high likelihood of ransom payment to avoid operational downtime and the value of their data.

When we look at the industrial cyber-attack trend, the service sector has suffered the most damage, driven by rapid digital transformation. Manufacturing experienced a surge in attacks as the smart factory expanded. Also, the healthcare sector continued to be targeted; medical institutions, where disruptions can directly impact patient safety, have become high-value targets. This trend of infrastructure-focused attacks is expected to continue into 2026.

Sectors projected to see increased attacks next year include rail, maritime, aviation, and telecommunications. As digitization advances, port and vessel management, aircraft control and airport security systems may become viable attack targets. Telecommunications networks, which connect governments, enterprises, and the public will see escalated attacks in 2026.

While most attackers remain financially motivated, some state-sponsored threat actors are expected to launch attacks driven by geopolitical tensions. As international conflicts persist, cyberattacks against critical infrastructure are likely to become increasingly sophisticated.

Taking Advantage of Industrial Digitalization

The keyword underlying infrastructure attacks is “digitalization.” As industrial digital transformation accelerates, once isolated OT networks are being connected to external interfaces and the attack surface is expanding, providing attackers with new opportunities to strike.

The most significant shift driven by industrial digitalization is the transition from traditional OT to Cyber-Physical Systems (CPS). As air-gapped OT environments gain more external connectivity, security must now encompass IT, IoT, and cloud services. In modern smart-manufacturing environments, a diverse array of IoT and other advanced devices can already be observed.

As a result, attack techniques targeting CPS environments are becoming more sophisticated.
A common tactic involves initially compromising the IT domain, then moving laterally into OT networks. Also, we are seeing more malware and ransomware specifically designed to target OT environments. CPS-targeted campaigns are expected to grow not only in 2026 but also well into the future.

Key Takeaways

- Industrial digitalization and geopolitical tensions are driving CPS-level threats against national critical infrastructure.
- Robust backup systems, recovery procedures, and incident-response drills will be required to achieve cyber resilience.

2026 Outlook

5. Surge in Cyber Attacks on Linux Systems

→ Discover how we protect Linux systems with our cross-domain security strategy.

More Vulnerabilities, More Advanced Attacks

According to our research, adversaries launched 12,000 attacks against 176 Linux systems in June 2025 alone. Although monthly volumes vary, an average of over 100 Linux systems experience thousands—sometimes over ten thousand—attacks every month. These attacks include DDoS bot, coin miners, backdoors, and ransomware. Linux vulnerabilities number in the thousands, and more than 60,000 new Linux-targeting malware samples were identified in just the first half of 2025. **The number of Linux attacks, vulnerabilities, and malware is all expected to increase in 2026.**

For example, in 2025, the Linux servers of a major Korean telco were compromised by the Linux-based BPFDoor, leaking personal data of 23 million customers. The threat actor infiltrated internal systems through a web shell and remote-code-execution (RCE) vulnerabilities, installed BPFDoor on HSS servers, and exfiltrated USIM data. **In 2026, we expect national infrastructure to remain a major target, and Linux servers will face increasing pressure as part of that broader trend.**

Adversaries are eyeing Linux servers because they are connected to numerous client PCs and store a wide range of business-critical data. Also, major cloud environments—AWS, Microsoft Azure, and Google Cloud—as well as container platforms such as Docker and Kubernetes, all rely on Linux as their foundation. It means that **a breach of a single Linux system may put hundreds of virtual machines and containers at risk.**

Attackers are also shifting their focus from guest operating systems to the hypervisor layer itself. In June 2025, Akira ransomware encrypted Nutanix AHV (Acropolis Hypervisor) virtual machine disk files, extending its reach beyond VMware ESXi and Hyper-V. A single compromise can disable hundreds of virtual machines within hours, significantly amplifying attack efficiency. With ransomware and other Linux-targeting malware on the rise, the risk of severe business disruption is increasing.

Defenders cannot address these advanced Linux-focused attacks with fragmented security measures. Attacks originate across multiple domains while new and variant malware continue to emerge. **As a result, the importance of unified security architectures will continue to grow, providing dynamic protection across all layers of the business.**

Key Takeaways

- Attacks targeting Linux systems will increase, and a single intrusion can compromise hundreds of devices and VMs.
- Organizations should design a unified security architecture to effectively address Linux threats across all domains.

AhnLab

© AhnLab, Inc. (Headquarter)

220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do 13493, Korea

Tel: +82-31-722-8000 | Fax: +82-31-722-8901 | Business Inquiries: global.sales@ahnlab.com

Website: https://www.ahnlab.com/en | LinkedIn: www.linkedIn.com/company/ahnlab-inc. | YouTube: https://www.youtube.com/@AhnLabGlobal