CYBLE®

ASIA AND PACIFIC THREAT LANDSCAPE

Q1 2026

January to March

TABLE OF CONTENT

Executive Summary

Cyble's Asia and Pacific Threat Landscape Report brings to light specific cyber threat activity targeting countries in the Asia and Pacific region in the first quarter of 2026.

A sharp escalation in cyber activity was observed, with ransomware, compromised access sales, data breaches, vulnerability exploitation, and hacktivist campaigns all occurring at significant scale. A total of 277 major cyber incidents were observed during the quarter, highlighting a region facing sustained pressure from financially motivated cybercriminals, opportunistic access brokers, state-aligned actors, and politically motivated groups.

Ransomware remained the most disruptive threat vector, accounting for **238 recorded attacks**. Activity was heavily concentrated among a small number of groups, led by The Gentlemen, which alone accounted for nearly one in four incidents, followed by Qilin and INC Ransom. **India recorded the highest number of attacks**, narrowly ahead of Thailand, while Taiwan, Japan, and Singapore also featured prominently. Manufacturing and IT & ITES emerged as the most targeted industries, reflecting attackers' continued focus on sectors where downtime creates immediate leverage and ransom pressure. A notable trend during the quarter was the repeated targeting of the same organizations by multiple ransomware groups, indicating rapid victim recycling once weaknesses become visible.

The **underground market for compromised access** also remained active, with threat actors selling unauthorized entry into enterprise environments across the region. Retail and Professional Services organizations were the most targeted, driven by the monetization value of customer data, payment information, and privileged corporate systems. Several listings involved access to high-value organizations in India, Indonesia, and the Philippines, underscoring how initial access brokers continue to fuel downstream ransomware, espionage, and fraud operations.

Data breaches and leak activity reflected a parallel threat stream, with government and law enforcement entities facing the highest volume of incidents, followed by retail, education, media, and IT sectors. Threat actors continued to trade both newly stolen and recycled historical datasets, often containing personally identifiable information, credentials, and internal business records. This reinforces the need for organizations to distinguish genuine breaches from reputational extortion campaigns built around previously exposed data.

The quarter also demonstrated how **critical vulnerabilities and zero-days are being weaponized faster than ever**. High-severity flaws affecting enterprise management platforms, network appliances, collaboration tools, and cloud-connected infrastructure were actively exploited. The Ivanti Endpoint Manager Mobile zero-day exemplified attacker preference for technologies that provide privileged, scalable access into corporate environments. These trends confirm that delayed patching, exposed management interfaces, and inadequate segmentation remain major enterprise risks across the region.

At the same time, **hacktivism surged across Southeast Asia**, with hundreds of campaigns involving website defacements, DDoS attacks, leaked data, and nationalist messaging. Government agencies, telecommunications providers, BFSI institutions, and educational entities were among the most common targets. While many operations were low sophistication, their volume and symbolic targeting amplified reputational and operational disruption.

Overall, Q1 2026 reveals a region confronting a **multi-layered cyber threat environment**: ransomware groups monetizing weak defenses, access brokers enabling larger attacks, state-linked actors pursuing persistence, and hacktivists exploiting geopolitical tensions. For defenders, the priorities are clear—accelerated patch management, stronger identity controls, third-party risk governance, continuous monitoring, rapid incident response readiness, and resilience planning for repeat attacks. Organizations that move quickly from reactive security to continuous exposure management will be best positioned to withstand the evolving threat landscape in the quarters ahead.

Key Highlights

What the Numbers Say

277
Total number of cyber incidents observed.

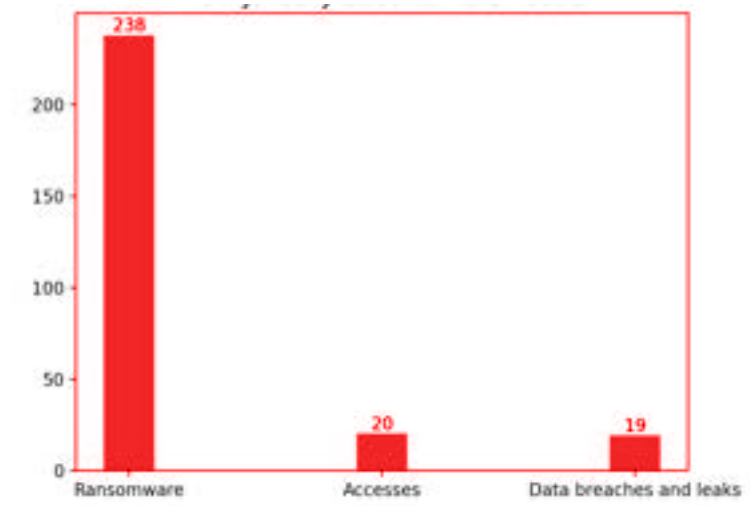


Fig 1: Cyber incidents in Europe in Q1 2026 (Source: Cyble Vision)

24%
"The Gentleman" group was the most active threat actor with 1 in every 4 attacks.

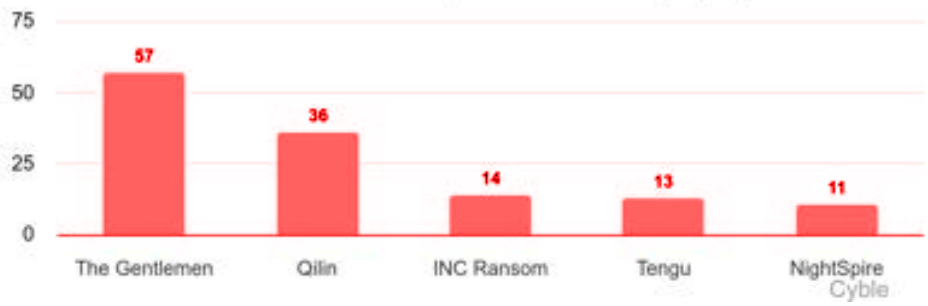


Fig 2: Five most active ransomware actors in APAC for Q1 2026 (Source: Cyble Vision)

India

With 45 attacks, India narrowly edged past Thailand for most attacked country.

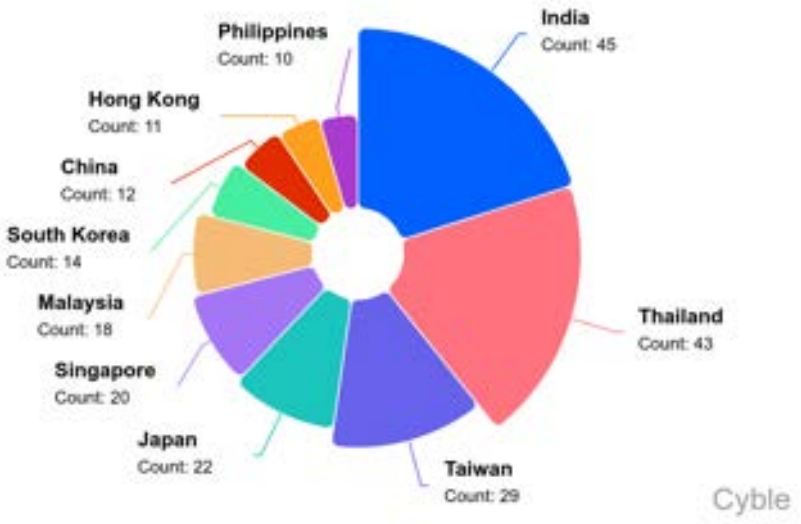


Fig 3: Top countries targeted by ransomware actors in APAC Q1 2026 (Source: Cyble Vision)

21%

Government sector faced highest number of data breaches while education was second best.

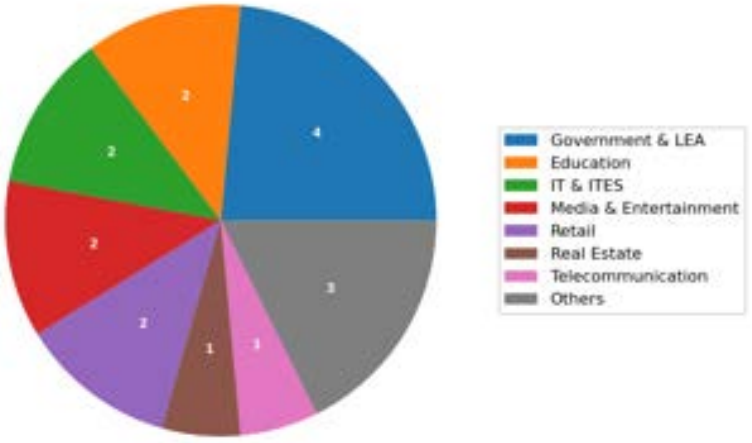


Fig 4: Sector-wise targets of ransomware actors (Source: Cyble Vision)

Major Asia and Pacific Cyber Incidents: Q1 2026

Date Reported	Threat Actor	Claimed Activity and Targets
Jan 4, 2026	**Unidentified**	**Cloud provider:** Targeted exploitation of misconfigured bucket permissions; leaked internal metadata for several high-growth startups in SE Asia.
Jan 15, 2026	**FriendlyDealer**	**Regional App Users (India/Vietnam):** Mass distribution of 1,500+ fake app store replicas; used to harvest banking credentials and 2FA tokens via high-fidelity UI impersonation.
Jan 29, 2026	**Lazarus Group**	Japanese Crypto Exchange: A "recovery denial" attack where data wasn't just encrypted but strategically corrupted to prevent restoration from backups; $45M in assets impacted.
Feb 8, 2026	**ShinyHunters**	**Phishing-led breach of 900,000 records;** focused on identity harvesting rather than immediate financial theft.
Mar 5, 2026	**Volt Typhoon**	**Critical Infrastructure (Southeast Asia):** Discovered "living off the land" (LotL) persistence in several regional power grids; no immediate disruption, but evidence of long-term espionage.
Mar 14, 2026	**Unidentified**	**University Research Systems:** 1.2 million records exposed, including driver's licenses and health research data, via a sophisticated ransomware pivot.
Mar 21, 2026	**Supply Chain (SaaS)**	**Regional E-commerce Aggregator:** Stolen OAuth tokens allowed attackers to bypass MFA and move laterally into hundreds of downstream merchant accounts.

Threat Assessment

1. **The "Trust Surface" Shift**
   Attackers in APAC are increasingly ignoring traditional technical exploits in favor of UI-based social engineering.

- Identity Hijacking: 79% of organizations in the region reported an increase in cyber-enabled fraud and phishing. The focus has moved from email to messaging app hijacking (Signal/ WhatsApp) by impersonating "Security Bots" to steal verification codes.
- App Store Impersonation: Campaigns like FriendlyDealer represent a new class of threat where the UI itself is the payload, exploiting user trust in platform design rather than software bugs.

2. **AI: The Double-Edged Sword**

APAC leads the world in AI adoption for defense, yet it faces the most significant AI-driven risk.

- Rapid Adoption: 75% of regional organizations have processes to assess the security of AI tools prior to deployment—trailing only North America.
- Data Leakage Anxiety: Data leaks are the #1 concern linked to Generative AI in the region (42% vs. 34% globally), specifically regarding how internal LLMs might inadvertently expose sensitive PII.

3. **Geopolitical Fragmentation**

Cybersecurity in APAC is inextricably linked to geopolitical friction.

- Sovereignty Dilemma: Deepening fragmentation is forcing countries to rethink their dependence on international undersea cables and cloud providers, leading to a rise in "Sovereign Cloud" initiatives.
- LotL Persistence: State-backed groups are moving away from noisy ransomware toward quiet, persistent access in virtualization stacks and network appliances to ensure long-term espionage capabilities.

4. **The Resilience Paradox**

While 47% of APAC organizations are confident in their national response capabilities (above the global average), 57% cite insufficient skills as their primary barrier to achieving true resilience. This gap is being filled by a heavy reliance on Managed Security Service Providers (MSSPs) to handle Continuous Threat Exposure Management (CTEM).

Initial Accesses on Sale

Analysis of the Overall Threat Activity

CRIL observed 20 incidents involving the sale of compromised access between January and March 2026.

The Retail and Professional Services sectors were the most frequently targeted, each accounting for 25% of the incidents and collectively representing half of all observed compromises. This significant concentration indicates a deliberate focus by threat actors on industries with high-value data.

The targeting of Retail organizations likely aims to acquire customer PII and payment card information for financial fraud, while compromising Professional Services firms provides access to sensitive client data, intellectual property, and strategic information that can be leveraged for extortion or corporate espionage.

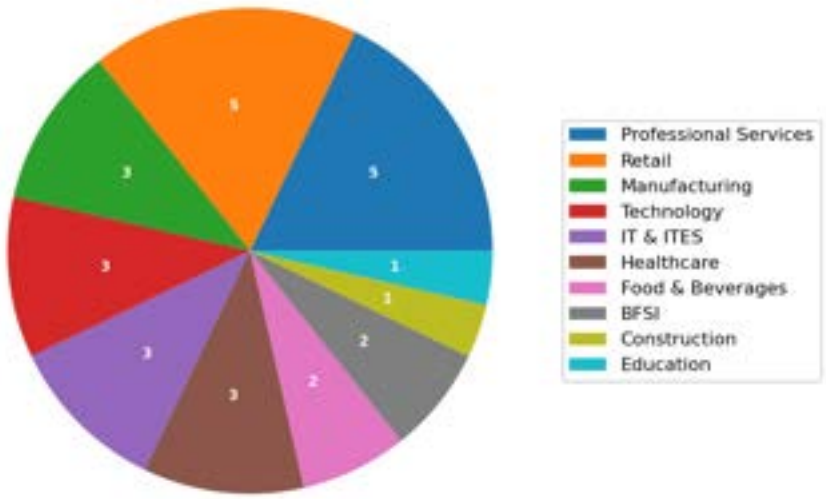


Fig 5: Compromised accesses across APAC industries in Q1 2026 (Source: Cyble Vision)

During the first quarter of 2026, the compromised access market was led by a small number of prolific threat actors. The most active entity was ‘sanguine’, who was responsible for six separate advertisements.

Following ‘sanguine’ in activity were ‘karuhunters’ and ‘redpin’, with four and three posts, respectively. These top three actors collectively accounted for 65% of all observed posts, indicating a market structure dominated by a few key players.

While several other actors were observed making single posts, the significant concentration of activity suggests that a core group of suppliers is responsible for most of the access offerings in this landscape.

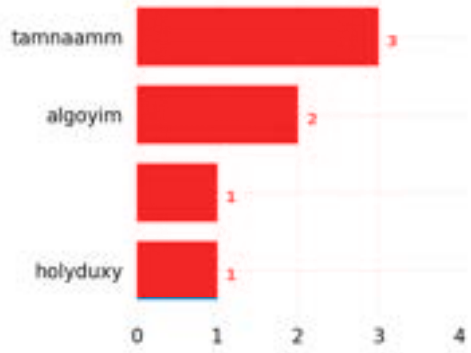


Fig 6: Active threat actors selling compromised access (Source: Cyble Vision)

Notable Accesses on Sale

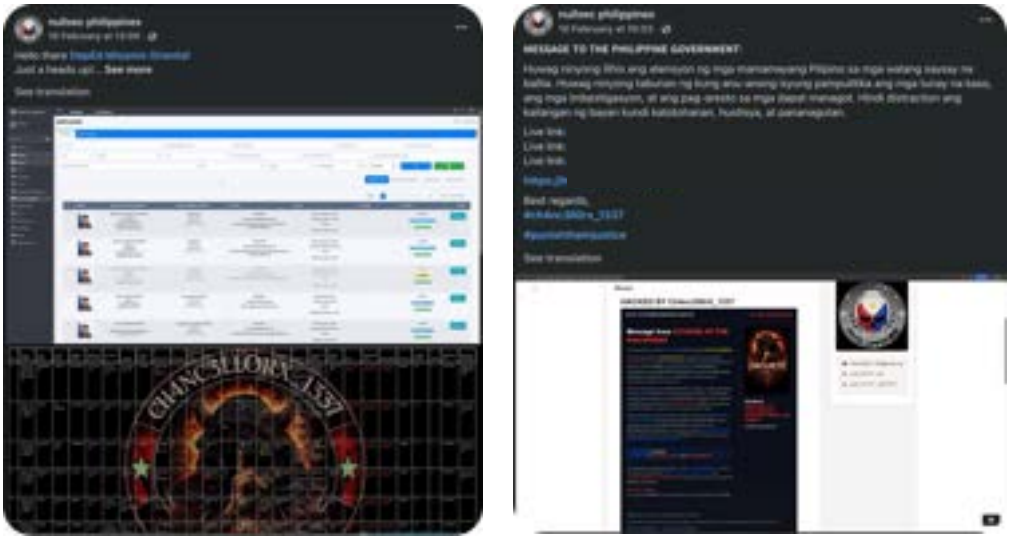
Alleged Philippines GAB Database Leak

In February, the threat actor 'r3dpin' leaked a database allegedly stolen from the Philippines Games and Amusement Board (GAB). The actor claimed to have obtained the data via a LandBank Payment API endpoint, and the compromise was later validated by the discovery of a web shell on a GAB subdomain. The investigation revealed the compromised infrastructure, managed by a third-party developer, suffered from multiple critical security exposures. These included an open directory that likely served as the data exfiltration point, a publicly exposed Microsoft SQL Server, and an accessible PESONET 2.0 Production system, indicating a significant risk to the nation's financial infrastructure.

(Source: Cyble Vision)

NullSec Philippines Targets Philippine Government and Education Sectors

In February, the hacktivist group NullSec Philippines claimed responsibility for unauthorized access and web defacement activities targeting Philippine government and education entities. The group shared screenshots indicating an internal webpage was compromised and defaced with the message "HACKED BY Ch4nc3ll0rX_1337". NullSec Philippines also alleged unauthorized access to the education department and the office for student affairs, where shared evidence suggested they accessed employee records and internal library management systems. Screenshots of compromised databases indicated that personal and employment details were exposed. The group framed the attacks as a protest against alleged government corruption, using hashtags such as #punishtheinjustice.



(Source: Cyble Vision)

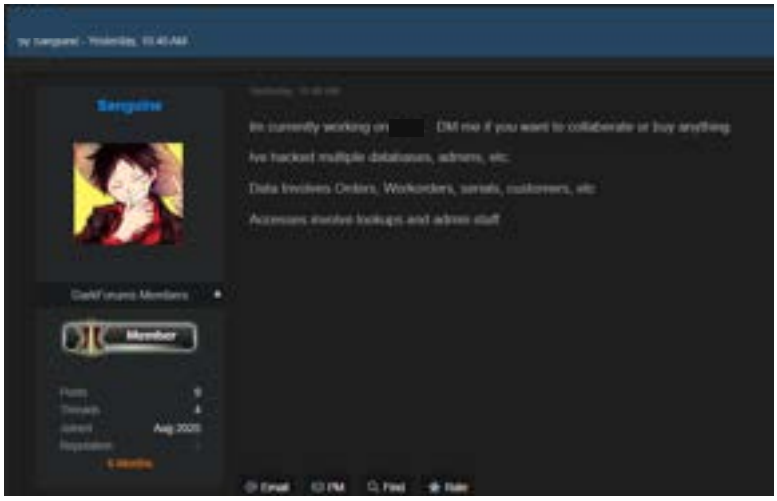
Unauthorized Access to Billion Dollar Indian Construction Firm for Sale

In March, the threat actor 'XSSRAT' advertised the sale of unauthorized access to an undisclosed construction company in India on the DarkForums cybercrime forum. The actor claimed the company has a revenue of US$1 billion and offered administrator-level privileges to its database for US$1,500. The post alleged that the access would compromise over 44 GB of data and included a screenshot from MySQL Workbench as a proof-of-concept, although the database names were masked.

(Source: Cyble Vision)

Threat Actor Claims Unauthorized Access to Computer-making Giants

In February, the threat actor "Sanguine" posted on the DarkForums cybercrime forum claiming to have compromised systems belonging to major technology manufacturers. The actor alleged access to multiple databases and administrative systems containing customer orders, work orders, serial numbers, and other customer information. Sanguine also offered administrative access and stolen data related to Asia region logistics operations, citing unspecified vulnerabilities. The threat actor did not provide any proof-of-compromise to support the assertions, and therefore, the claims remained unconfirmed at the time of reporting.



(Source: Cyble Vision)

Access to Indonesian Platform and 14.6 Million Records for Sale

In late January, the threat actor "KaruHunters" advertised the unauthorized access to a database belonging to LinkUMKM, an Indonesian digital platform. The advertisement, posted on the English-language cybercrime forum DarkForums, claimed the database contained 14,621,156 user records. To support their claims, the threat actor shared proof of access via a Telegram channel. The access was offered as a one-time sale for US$500, with instructions for interested buyers to establish private contact.

(Source: Cyble Vision)

Data Breaches and Leaks

Analysis of the Overall Threat Activity

Cyble Research and Intelligence Labs (CRIL) observed 19 incidents related to data breaches and leaks impacting the region in Q1 2026.

The Government and Law Enforcement (LEA) sector was the most frequently targeted, accounting for 4 incidents, which represents approximately 21% of all observed breaches. A secondary cluster of attacks was directed at the Media & Entertainment, IT & ITES, Retail, and Education sectors, each representing just over 10% of the incidents.

The targeting of government and LEA entities likely stems from threat actors' interest in acquiring sensitive citizen PII, intelligence data, and official communications for espionage or disruption. Attacks on the other prominent sectors are typically driven by the pursuit of large volumes of customer data, financial information, and intellectual property for monetization on dark web forums.

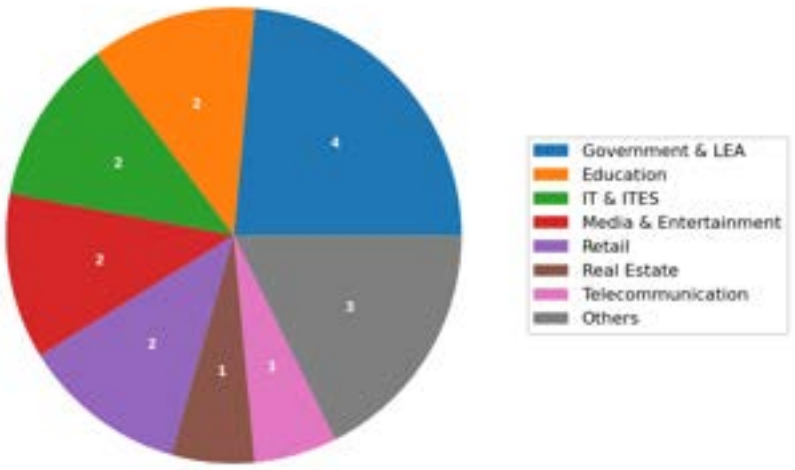


Fig 7: Industry-wise data breaches across APAC (Source: Cyble Vision)

Analysis of threat actor activity in Q1 2026 indicates that the threat actor 'jxq09' was the most active when it came to data breach and leak posts. The actor was responsible for three separate incidents.

The actors 'pixelphreak' and 'crowstealer' were also notably active, each associated with two distinct breach disclosures. The remaining activity was highly fragmented, distributed across ten different actors, each responsible for a single post.

This landscape suggests that while a small number of actors like 'jxq09' play a more consistent role in publicizing data compromises, the broader ecosystem is populated by a diverse and opportunistic collection of individuals or groups participating in data leak activities.

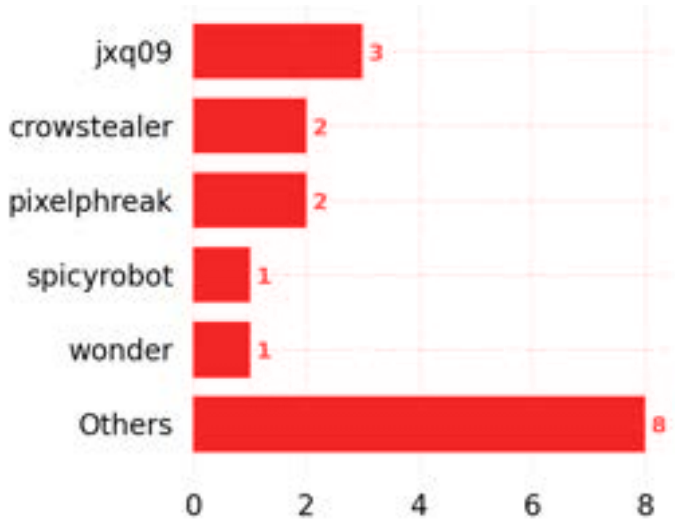


Fig 8: Active threat actors selling breached data of APAC entities (Source: Cyble Vision)

Prominent threat actors active during the first quarter of 2026 demonstrated a distinct operational focus on the Asia region. The actor 'jxq09' was observed in a sustained campaign from early February to early March, specifically targeting the Real Estate and Retail sectors within Japan, indicating a likely financial motivation.

Concurrently, the threat actor 'SpicyRobot' engaged in a more condensed, week-long burst of activity in late February concentrated on targets within China.

Collectively, the profiles of these top actors reveal a pattern of targeted, country-specific campaigns directed at commercial entities in East Asia.

Notable Data Breaches and Leaks

Over 209,000 Vietnamese travel platform Customer Records Leaked on Cybercrime Forum

In January, the threat actor "Solonik" leaked a database on the DarkForums cybercrime forum, allegedly stolen from the Vietnamese travel platform. The dataset reportedly originates from the company's customer relationship management (CRM) system and contains 209,759 verified know-your-customer (KYC) records. The exposed personal information includes full names, Citizen Identity Card numbers, mobile phone numbers, dates of birth, and complete residential addresses.

(Source: Cyble Vision)

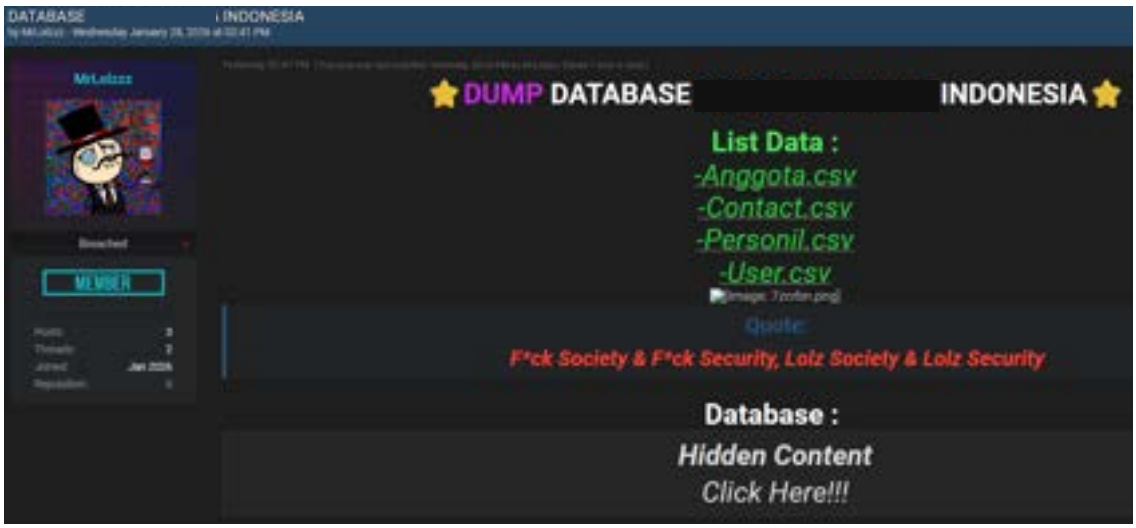
Indian AI Firm Source Code for Sale on Cybercrime Forum

In January, the threat actor '888,' a moderator on the DarkForums cybercrime forum, advertised the sale of source code allegedly stolen from an Indian technology and software development firm. The advertised data purportedly contained a complete Node.js backend project named "Canada Study Backend," which includes sensitive configuration files for databases and cloud services, API route handlers, business logic controllers, and database models. The detailed file structure listed by the threat actor suggests the exposure of proprietary code related to the management of admins, agents, students, orders, and leads, revealing the application's internal architecture and operational logic.

(Source: Cyble Vision)

Threat Actor Exaggerates Claims in Leak of Public Worker Data

In late January, the threat actor 'MrLolzzz' posted on the BreachForums cybercrime forum, claiming to have breached a community organization for workers of the Indonesian state-owned energy company. The actor offered a database allegedly containing four CSV files with member data, contact information, personnel records, and user data. However, analysis revealed that the leaked data was sourced from the organization's publicly accessible website. The incident did not involve an actual compromise of the company's systems; instead, the threat actor reposted publicly available information while exaggerating their claims to present it as a significant data breach.



(Source: Cyble Vision)

Threat Actor Leaks Historical Data Allegedly from Indian Travel and Tourism-based Company

In early January, the threat actor Solonik posted on the DarkForums cybercrime forum, claiming to have leaked a database from the Indian online travel platform.

The threat actor alleged the database contained approximately 6 million user records in CSV format, including personally identifiable information (PII) such as names, email addresses, phone numbers, genders, and physical addresses. While sample records were provided to support the claim, analysis revealed that the data was from a previously known historical leak and had already been indexed. The claim of a new data breach is therefore considered improbable.

(Source: Cyble Vision)

Bangladeshi Retail Giant's Alleged Breached Data of 3.5 Million Users for Sale

In January, a threat actor identified as "bitcoin" posted on the BreachStars cybercrime forum, offering for sale a database allegedly exfiltrated from a prominent Bangladeshi fashion and lifestyle retailer.

The actor claimed the dataset contains over 3.5 million customer records and simultaneously offered administrative panel access, granting full control over the compromised information. Sample data revealed the potential exposure of sensitive personally identifiable information (PII), including customer identification numbers, full names, email addresses, phone numbers, postal codes, dates of birth, gender, and employee discount OTP fields. The seller instructed potential buyers to initiate contact privately.

(Source: Cyble Vision)

Ransomware Attacks

Cyble Research and Intelligence Labs (CRIL) observed 238 ransomware attacks during the first quarter of 2026, indicating a highly active and aggressive threat landscape. With 45 attacks, India was the most attacked country in the APAC. As compared to Q1 2025, which saw only 17 attacks, this is a 165% jump in volume, and a 55% rise in comparison to the last quarter (Q4 2025).

India was closely followed at the second place by Thailand. The semi-conductor and technology hubs of the world, Taiwan and Japan, along with Singapore closed the top five list of most attacked countries in the Asia and Pacific region.

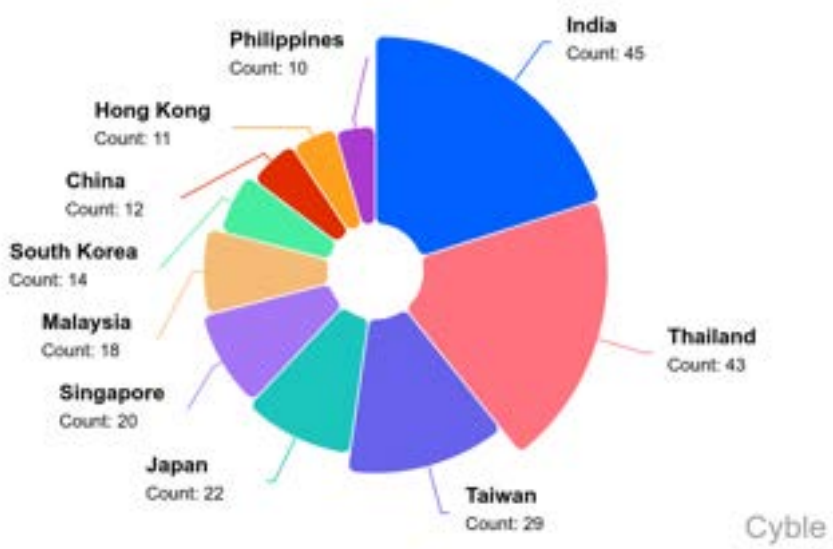


Fig 9: Active threat actors selling breached data of APAC entities (Source: Cyble Vision)

The period was characterized by the overwhelming dominance of a few prolific groups that were responsible for a significant portion of the total incidents. Analysis of victimology reveals that the Manufacturing and IT & ITES sectors bore the brunt of these attacks, which shows their vulnerability and attractiveness to cybercriminals. This quarter's activity indicates a dynamic and concentrated threat environment where strategic targeting and opportunistic attacks converge.

Dominant Groups

An analysis of the ransomware landscape reveals a significant concentration of activity among a few key players.

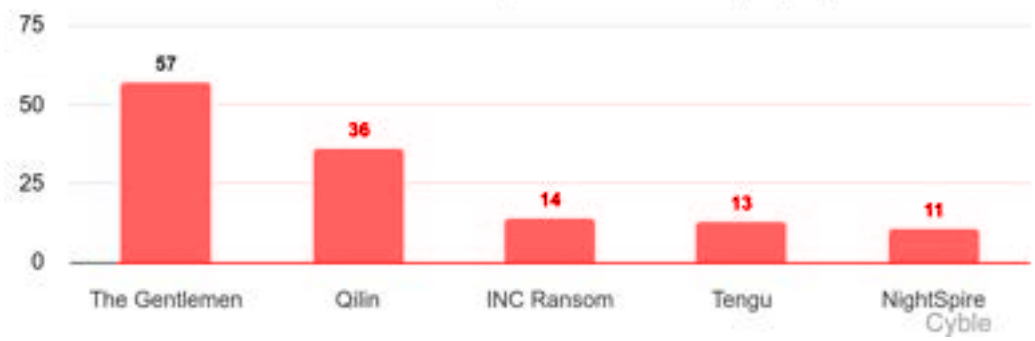


Fig 10: Top ransomware actors that targeted APAC in Q1 2026 (Source: Cyble Vision)

The "The Gentlemen" group was exceptionally prolific, accounting for 57 incidents, which constitutes approximately 24% of all observed attacks, which means nearly 1 in every 4 attacks. Although India was the most attacked country during the reporting period, The Gentleman group mainly remained focused on Thailand (20 attacks) and on its manufacturing and BFSI sector.

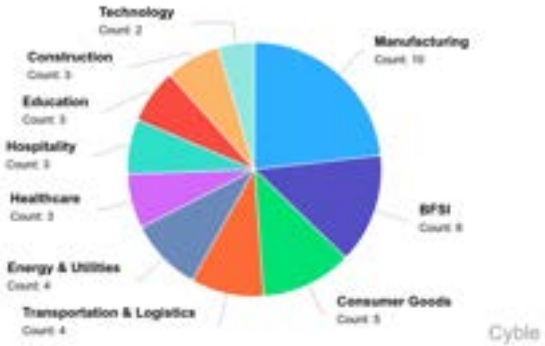


Fig 11: Industry-wise attacks by The Gentleman.

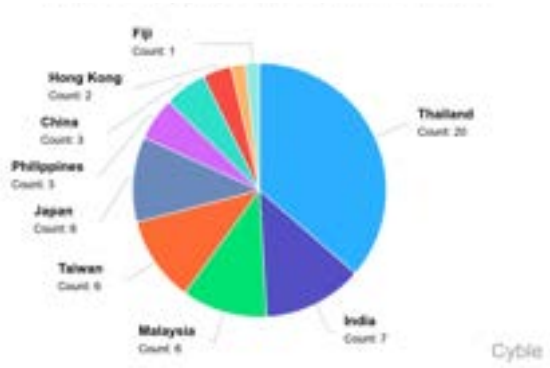


Fig 12: Country-wise attacks by The Gentleman.

Following at a distance but still highly active was the Qilin ransomware group, responsible for 36 attacks (15%). The INC Ransom group was the third most active, with 14 documented incidents.

Collectively, these top three groups were responsible for 107 attacks, representing a staggering 45% of the total ransomware activity this quarter, demonstrating their substantial impact and operational capacity within the cybercrime ecosystem.

Impact Analysis

The Manufacturing sector was the most heavily impacted industry during this quarter, suffering numerous attacks from a wide array of threat actors, including The Gentlemen, Qilin, and LockBit.

This was followed by the IT & ITES sector, which faced significant disruption from groups such as Tengu, Sinobi, and Qilin targeting technology service providers and software companies.

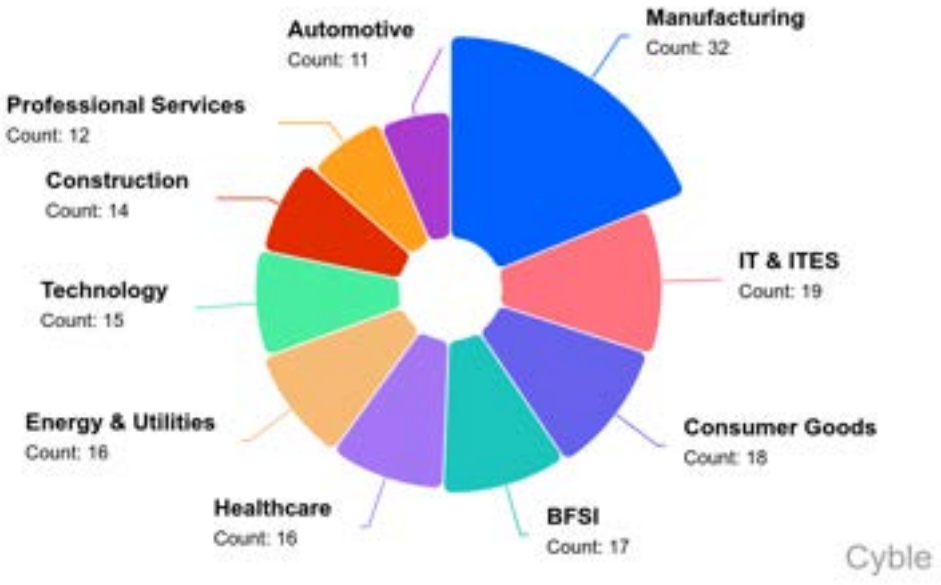


Fig 13: Sector-wise targets of ransomware actors in APAC (Source: Cyble Vision)

Other frequently targeted sectors include Professional Services, Healthcare, and Consumer Goods, each experiencing a high volume of attacks. This widespread targeting across critical and commercial sectors illustrates the indiscriminate and opportunistic nature of many ransomware campaigns, which prioritize vulnerable organizations regardless of their industry.

The spray-and-pray tactic was also very evident in India where all key sectors including, IT, Manufacturing, Healthcare, Professional Services, Automotive and BFSI were almost equally targeted.

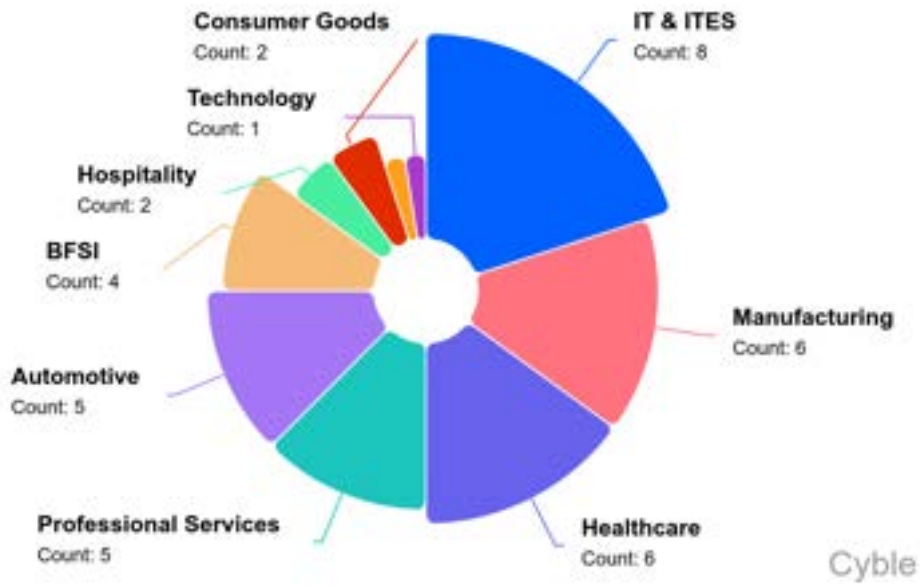


Fig 14: Sector-wise targets of ransomware actors in India (Source: Cyble Vision)

India also faced targeted attacks not just from regional leaders but other smaller actors that mainly concentrate on South-East Asia. The top five included, Sinobi, The Gentleman, Vect, Tengu and CL0P.

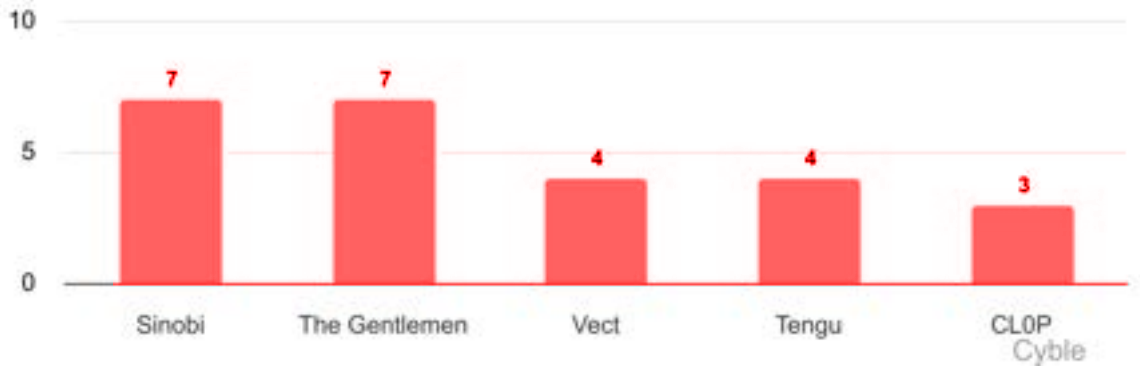


Fig 15: Top ransomware actors that targeted India in Q1 2026 (Source: Cyble Vision)

Notable Incidents and Trends

A notable trend observed this quarter was the targeting of the same organization by multiple, distinct ransomware groups. For instance, two Malaysian entities were listed as victims, both by Qilin and The Gentlemen, in separate incidents. This pattern suggests that once an organization's security posture is compromised or publicly identified as vulnerable, it becomes a prime target for subsequent attacks by other threat actors.

Furthermore, the data indicates the persistent activity of established groups like LockBit, which continued its operations targeting diverse sectors from Energy & Utilities to Government & Law Enforcement, alongside the high-volume campaigns from newer or rebranded entities like The Gentlemen.

The first quarter of 2026 was defined by a relentless pace of ransomware operations, dominated by the hyper-active "The Gentlemen" and Qilin groups. The sustained focus on critical sectors like Manufacturing highlights systemic vulnerabilities that threat actors continue to exploit for financial gain.

The trend of multiple groups victimizing the same entity calls for rapid remediation and security hardening following an initial breach. The primary threat stems from a diverse but top-heavy ecosystem where a handful of sophisticated and opportunistic groups can inflict widespread damage across a multitude of industries.

Vulnerability Intelligence

Known Exploited Vulnerabilities

The first quarter of 2026 demonstrated a significant and industry-agnostic trend of critical vulnerabilities, with a substantial number of CVEs scoring 9.0 or higher, indicating a landscape where severe, remotely exploitable flaws are prevalent.

The inclusion of these vulnerabilities in the CISA Known Exploited Vulnerabilities (KEV) catalog underscores their real-world exploitation by threat actors, making them immediate risks for organizations globally, irrespective of their region.

Notably, vendors such as SmarterTools, Solarwinds, and Cisco appeared multiple times, with critical vulnerabilities affecting widely used products like email servers, help desk software, and network management appliances.

For instance, a critical remote code execution vulnerability in Cisco's Secure Firewall Management Center (CVE-2026-20131) allows unauthenticated attackers to gain root access and has been actively exploited by ransomware groups.

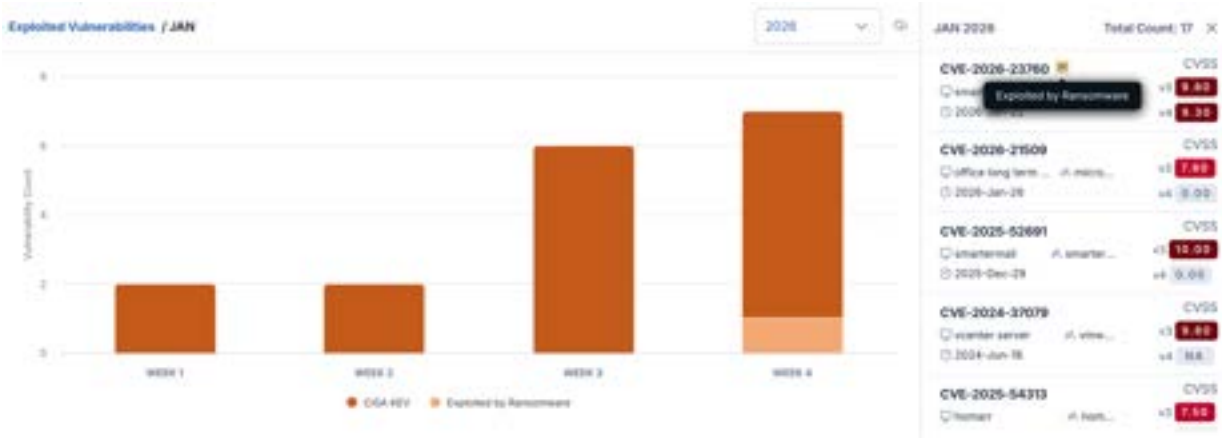


Fig 16: Vulnerabilities exploited in January 2026 (Source: Vulnerability Intelligence Module Cyble Vision)

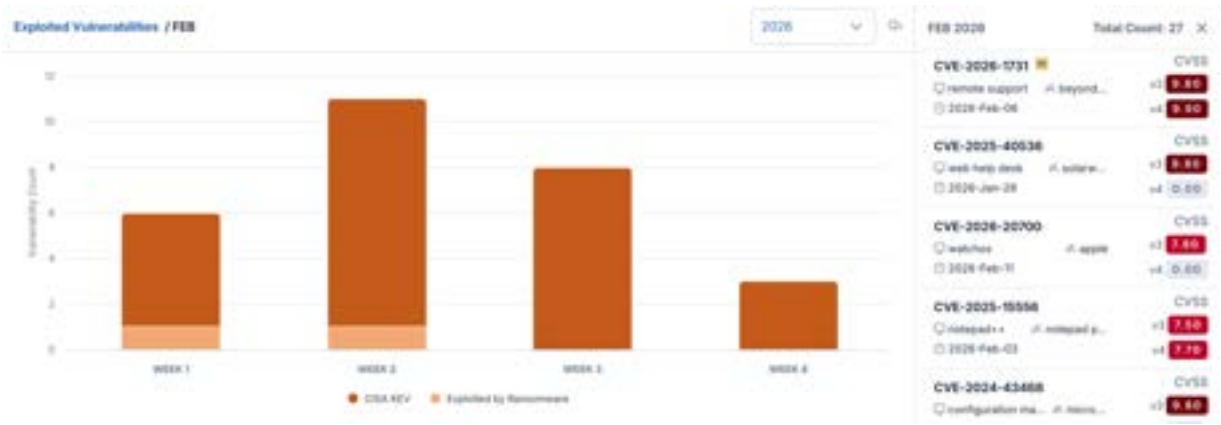


Fig 17: Vulnerabilities exploited in February 2026 (Source: Vulnerability Intelligence Module Cyble Vision)

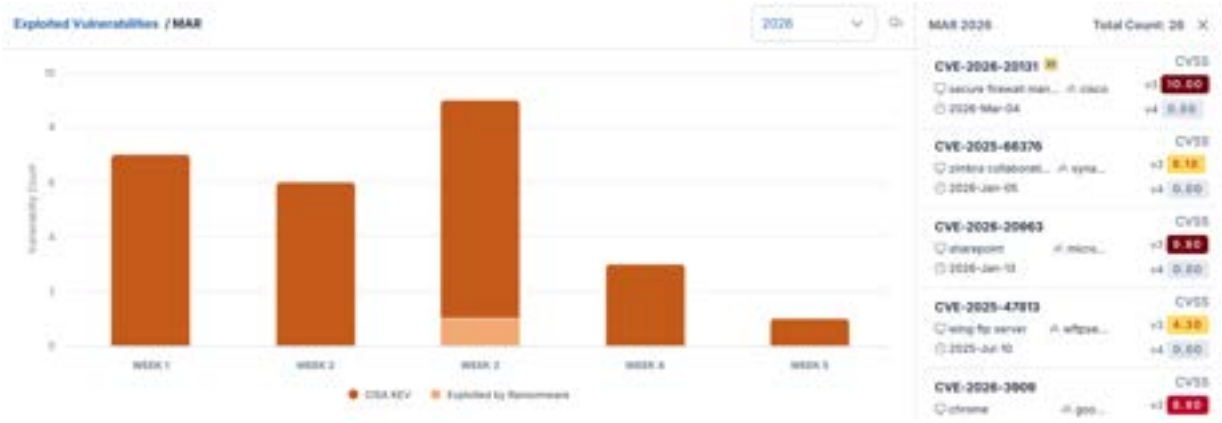


Fig 18: Vulnerabilities exploited in March 2026 (Source: Vulnerability Intelligence Module Cyble Vision)

Similarly, a zero-day vulnerability in Dell's RecoverPoint for Virtual Machines (CVE-2026-22769) with a CVSS score of 10.0 was exploited by a suspected state-sponsored threat actor to achieve persistent access and deploy malware.

The persistent targeting of edge infrastructure and enterprise management platforms calls for patching these known exploited vulnerabilities on priority. To mitigate these threats, organizations should focus on immediate patching, network segmentation to limit lateral movement, and continuous monitoring for indicators of compromise.

CVE ID	Product	Vendor	CVSS(V3)
CVE-2025-37164	Oneview	Hpe	9.8
CVE-2026-20045	Unified Communications Manager	Cisco	9.8
CVE-2024-37079	Cloud Foundation	Vmware	9.8
CVE-2025-52691	Smartermail	Smartertools	10
CVE-2026-24061	Inetutils	Gnu	9.8
CVE-2026-23760	Smartermail	Smartertools	9.8
CVE-2026-24858	Fortianalyzer	Fortinet	9.8
CVE-2026-1281	Endpoint Manager Mobile	Ivanti	9.8
CVE-2019-19006	Freepbx	Sangoma	9.8
CVE-2025-40551	Web Help Desk	Solarwinds	9.8
CVE-2025-11953	Metro Development Server	Metro Development Server	9.8
CVE-2026-24423	Smartermail	Smartertools	9.8
CVE-2025-40536	Web Help Desk	Solarwinds	9.8
CVE-2024-43468	System Center Configuration Manager	Microsoft	9.8
CVE-2026-1731	Remote Support Privileged Remote Access	Beyondtrust	9.8
CVE-2020-7796	Zimbra Collaboration Suite	Synacor	9.8
CVE-2021-22175	Gitlab	Gitlab	9.8
CVE-2026-22769	Recoverpoint For Virtual Machines	Dell	10
CVE-2026-20127	Catalyst Sd Wan Manager	Cisco	10
CVE-2017-7921	Ds 2Cd2032 I Firmware	Hikvision	9.8
CVE-2021-22681	Factorytalk Services Platform	Rockwellautomation	9.8
CVE-2025-26399	Web Help Desk	Solarwinds	9.8
CVE-2026-20963	Sharepoint Server	Microsoft	9.8
CVE-2026-20131	Secure Firewall Management Center	Cisco	10
CVE-2025-32432	Cms	Craft	10
CVE-2025-54068	Livewire	Livewire	9.8
CVE-2026-33017	Langflow	Langflow Ai	9.8
CVE-2025-53521	Big Ip Apm	F5	9.8
CVE-2026-3055	Netscaler Application Delivery Controller	Citrix	9.8

Zero-Day Vulnerabilities

The threat landscape from January to March 2026 was characterized by a concentration of high-impact vulnerabilities, all of which were industry- and region-agnostic.

The most notable of these was CVE-2026-1340, a critical zero-day code injection vulnerability in Ivanti's Endpoint Manager Mobile (EPMM) with a CVSS score of 9.8. Its active exploitation by threat actors for unauthenticated remote code execution highlights the significant and immediate risk to enterprises using such platforms.

This incident continues a clear trend of attackers targeting enterprise management platforms and other edge infrastructure to gain initial access to corporate networks. Overall, the complete absence of moderate or low-severity vulnerabilities indicates a strategic focus by adversaries on developing exploits for flaws that promise the most significant impact.

CVE ID	Product	Vendor	CVSS(V3)
CVE-2026-1340	Endpoint Manager Mobile	Ivanti	9.8

Hacktivism

Hacktivism Landscape

The first quarter of 2026 was characterized by a high volume of hacktivist activity, primarily driven by a coalition of threat groups with apparent regional and nationalistic motivations, particularly from Southeast Asia.

Prominent channels and collectives observed leading these campaigns included EXECUTOR NETWORK CO LTD, BROTHEROOD CAPUNG INDONESIA (B.C.I) PRIVATE, Malaysia Hacktivist - Official, and Group Spider Team. Their primary tactics consisted of website defacements, Distributed Denial-of-Service (DDoS) attacks, and the dissemination of sensitive information, with CRIL observing approximately 498 posts related to data leaks and dumps during this period.

The scope of these operations was extensive and largely indiscriminate, impacting nearly 3,600 unique domains. Targets spanned a wide array of sectors, including Government & LEA, BFSI, Technology, and Telecommunication, affecting both public and private entities.

FIA AGENCY GC

In Q1 2026, the 'FIA AGENCY GC' channel functioned as a hub for geopolitical commentary and cyber activity with a strong focus on the Indian subcontinent. The group's activities primarily consisted of information operations, disseminating news and OSINT-style analysis on military and political events involving India, Pakistan, and Bangladesh. The channel also engaged in cyberattacks, directly claiming responsibility for defacing dozens of Indian websites, primarily in the media and commercial sectors.

Furthermore, it acted as an aggregator for other hacktivist groups, sharing third-party claims of DDoS attacks and system compromises targeting government, aviation, and telecommunications infrastructure in India, Pakistan, and Bangladesh. The channel also frequently posted personally identifiable information, including phone numbers and names, of individuals from these three nationalities. The stated motivations for these activities were consistently nationalistic, with actions framed as retaliation or defense of Indian interests.

Webshell Market

The 'Webshell Market' channel functions primarily as a cybercrime marketplace operated by actors with a stated Indonesian affiliation, focusing on the commercial sale of illicit tools, data, and access. During this period, the channel's main offerings included webshell and cPanel access to a wide range of compromised websites, with a notable concentration of victims located in India across various industries.

The actors also advertised the sale of large databases, including one allegedly containing the personal and financial information of 23 million Chinese bank customers and several others purportedly from global cryptocurrency exchanges.

Additionally, the group marketed custom hacking and intelligence-gathering tools, such as DDoS-for-hire services, an automated exploitation bot named 'XENPAIBOT', and an OSINT tool specifically for reconnaissance on Malaysian individuals. The activities are exclusively financial in nature, with goods and services priced in both Indonesian Rupiah and US Dollars.

EXECUTOR NETWORK CO LTD

The Indonesian threat group 'EXECUTOR NETWORK CO LTD' operates as a commercial provider of cybercrime services and a marketplace for related tools. Their primary offering is the 'Executor Stresser' DDoS-for-hire service, which is advertised as capable of launching both Layer 4 (botnet) and Layer 7 (API) attacks with methods such as 'exec-flash,' 'killnet,' and 'browser,' claiming to bypass security measures like Cloudflare's. The group's channel is also used to sell illicit infrastructure, including Virtual Private Servers (VPS) with Indonesian and US-based IPs, and compromised accounts for services like AWS and Digital Ocean.

In addition to these commercial activities, the group disseminates leaked data, such as documents from the Indonesian entity PT Prisma Multi Sinergi, and shares free scripts for various malicious acts including defacement and doxing. Their operations suggest a financial motivation, functioning within a broader Indonesian cybercriminal ecosystem that uses shared resources like a "Blacklist Scammer" channel for community regulation.

BROTHEROOD CAPUNG INDONESIA (B.C.I) PRIVATE

The Indonesian hacktivist group 'BROTHEROOD CAPUNG INDONESIA (B.C.I) PRIVATE' focused primarily on cyberattacks against domestic entities, with a pronounced emphasis on data breaches targeting the Indonesian government. The group claimed responsibility for and shared multiple large-scale data leaks, allegedly containing millions of records of Indonesian citizens, provincial government employees, and data from the Ministry of Manpower and the Ministry of Health. In addition to data exfiltration, B.C.I conducted Distributed Denial-of-Service (DDoS) attacks against Indonesian government and educational websites, and members posted evidence of website defacements targeting local government portals. The channel also served as a hub for sharing allegedly compromised login credentials for various Indonesian government services. Posts indicate affiliations and coordinated activities with other Indonesian hacktivist crews, including 'Jakarta Ghost Digital' and 'Babayo Eror System'.

Jav4nyM0uzCorp [Public]

During the observation period, the 'Jav4nyM0uzCorp [Public]' channel primarily operated as a marketplace for cybercriminal tools rather than a platform for claiming specific hacktivist attacks. The group's focus was the advertisement and sale of a hacking tool named "XENPAIBOT," which was marketed with capabilities for automated web application attacks, including web scanning, shell uploads, CVE exploitation, and brute-forcing credentials for platforms like WordPress, Joomla, Moodle, and cPanel.

The group's motivations appear to be financial, with tools priced in both Indonesian Rupiah and US Dollars. Secondary activities observed on the channel included doxing and public shaming of Indonesian individuals accused of being scammers, suggesting the group's activities and disputes are largely concentrated within the Indonesian cybercriminal community.

Conclusion

The first quarter of 2026 revealed a highly active and concentrated threat landscape where a few prolific groups dominated across multiple attack vectors.

Ransomware activity was exceptionally high, with groups like “The Gentlemen” and Qilin responsible for nearly half of all incidents, primarily targeting the Manufacturing and IT sectors.

Similarly, the initial access market was led by a small number of actors such as ‘sanguine’, who focused on compromising Retail and Professional Services firms.

A significant trend was the rapid exploitation of critical zero-day vulnerabilities in widely used enterprise software, which facilitated sophisticated state-aligned cyber-espionage campaigns using advanced tactics like kernel-mode rootkits and AI-generated malware.

Concurrently, hacktivism surged, driven by nationalistically motivated groups from Southeast Asia conducting widespread DDoS attacks and data leaks, underscoring a period defined by targeted, high-impact campaigns from a concentrated set of opportunistic and sophisticated threat actors.

Industry Recognition

Cyble's capabilities are highly praised by global analysts, industry critics, and cybersecurity leaders

Gartner

Cyble Recognized in **Three Gartner® Hype Cycle™ Reports** for the **Second Consecutive Year 2025, TechScape 2025 & More**

FROST & SULLIVAN

Cyble Named Leader in Frost Radar™ Cyber Threat Intelligence 2024

Y Combinator

Cyble featured among AI startups backed by Y Combinator (YC) 2025

FORRESTER®

Cyble Recognized in Forrester's **External Threat Intelligence** Service Providers Landscape, **Q1 2026 report**

QKS Group
SPARK Matrix™ 2025
LEADER

Cyble Named as a Leader in Digital Threat Intelligence Management

AMERICA'S BEST STARTUP EMPLOYERS Forbes 2026

Recognized as one of America's Best Startup Employers by Forbes

Cyble Secures Four Prestigious Honors at the 2026 Global Infosec Awards

Gartner Peer Insights.

Ranked No. 1 among the top Security Threat Intelligence Providers.

4.8/5

Cyble Named in America's Greatest Startup Workplaces 2025, By Newsweek

Cyble Wins Three Top InfoSec Innovator 2025 Awards

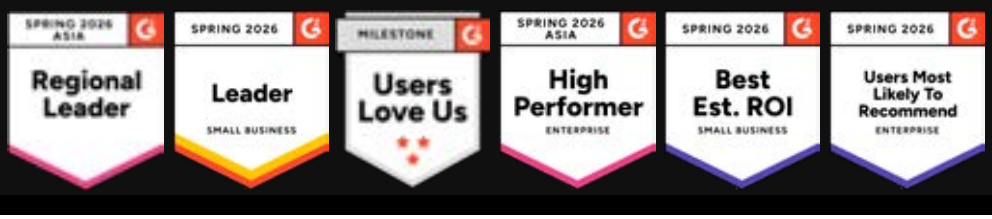
G2

Named a leader in the G2 Grid for Dark Web Monitoring and Threat Intelligence

2026 WINNER CYBER SECURITY EXCELLENCE AWARDS

BEST SOFTWARE 2026 Top 50

Cyble Sets a New Benchmark With **40 Badges in G2 Spring 2026 Report** — Its Highest Ever



OUR INVESTORS

BLACKBIRD · KING RIVER · SUMMIT PEAK · Singtel innov8 · BizLabs · Y Combinator · SPIDER CAPITAL · svb Silicon Valley Bank

10080 North Wolfe Road, Suite SW3-200, Cupertino, CA 95014 | contact@cyble.com | +1 888 673 2067


Stay Ahead of the Next Threat
REQUEST YOUR DEMO NOW!
Experience the power of predictive security with Cyble.