india

cyber_ threat

report {2026}

SEQRITE

Foreword

It gives me great pride to present the India Cyber Threat Report 2026, a comprehensive analysis from Seqrite Labs, India's largest malware analysis centre, monitoring over 8 million endpoints. The past year has been shaped by global political tensions, accelerated digital adoption, and the growing role of artificial intelligence in both innovation and threat creation.

No sector and no state in India are immune to cyberattacks. As the digital ecosystem expands, fraud and scams have emerged as universal concerns. In response, we launched AntiFraud.AI, India's first predictive fraud prevention platform, using behavioural analytics to protect citizens against digital financial fraud.

Our annual Cybersecurity Maturity Survey, with participation from over 180 organisations, highlighted gaps in predictive threat detection, incident response readiness, and data privacy governance. Guided by these insights, we strengthened our enterprise offerings, including Seqrite Data Privacy, to help organisations anticipate threats, safeguard sensitive data, and meet regulatory requirements. We also launched Seqrite Threat Intelligence, Seqrite Malware Analysis Platform, and Seqrite Intelligent Assistant, as well as a deep dive into the threat landscape and partaking in agentic-AI capabilities. This year, we further unveil Ransomware Recovery as a Service and Digital Risk Protection Service which will enable organisations to move from reactive cybersecurity to strategic cyber resilience, protecting their digital footprint, safeguarding their brand reputation, and ensuring uninterrupted operations. At the core of these solutions is AI driven intelligence, powered by our patented GoDeep.AI technology. Last year, we received our ninth patent, reflecting our commitment to innovation. Our products continue to achieve the highest scores from AVLab Poland and AV-TEST certifications, validating their effectiveness.

Adversaries are evolving rapidly, utilizing automation and generative AI to adapt in real-time. The report highlights rising risks from AI-generated phishing, cloud identity compromise, and data integrity manipulation. It emphasizes predictive defense, AI-powered threat correlation, zero-trust identity management, ransomware resilience, and cross-industry collaboration as pillars for strengthening digital defenses. In all we do, we remain true to our core purpose to innovate, simplify, and secure the digital ecosystem for citizens and enterprises alike.

Quick Heal Technologies Limited continues to represent India on the global cybersecurity stage, collaborating with the US NIST-NCCoE's data classification initiatives. As the first Indian cybersecurity-focused company to join the United States Artificial Intelligence Safety Institute Consortium, we advance responsible AI development and safer global digital ecosystems.

Our teams defend the nation's digital frontiers with vigilance and expertise. I invite you to explore this report's findings, predictions, and recommendations. Together, we can create a secure, trusted, and resilient digital future for India.

Dr. Kailash Katkar

Chairman and Managing Director
Quick Heal Technologies Ltd

Foreword

I am pleased to welcome you to the 2026 Seqrite Threat Report, an in-depth analysis of India's evolving cyber landscape. The past year has been one of unprecedented complexity; it was a year that witnessed a war with our neighbouring country, as well as the emergence of a parallel cyber conflict that tested the strength and resilience of our digital infrastructure.

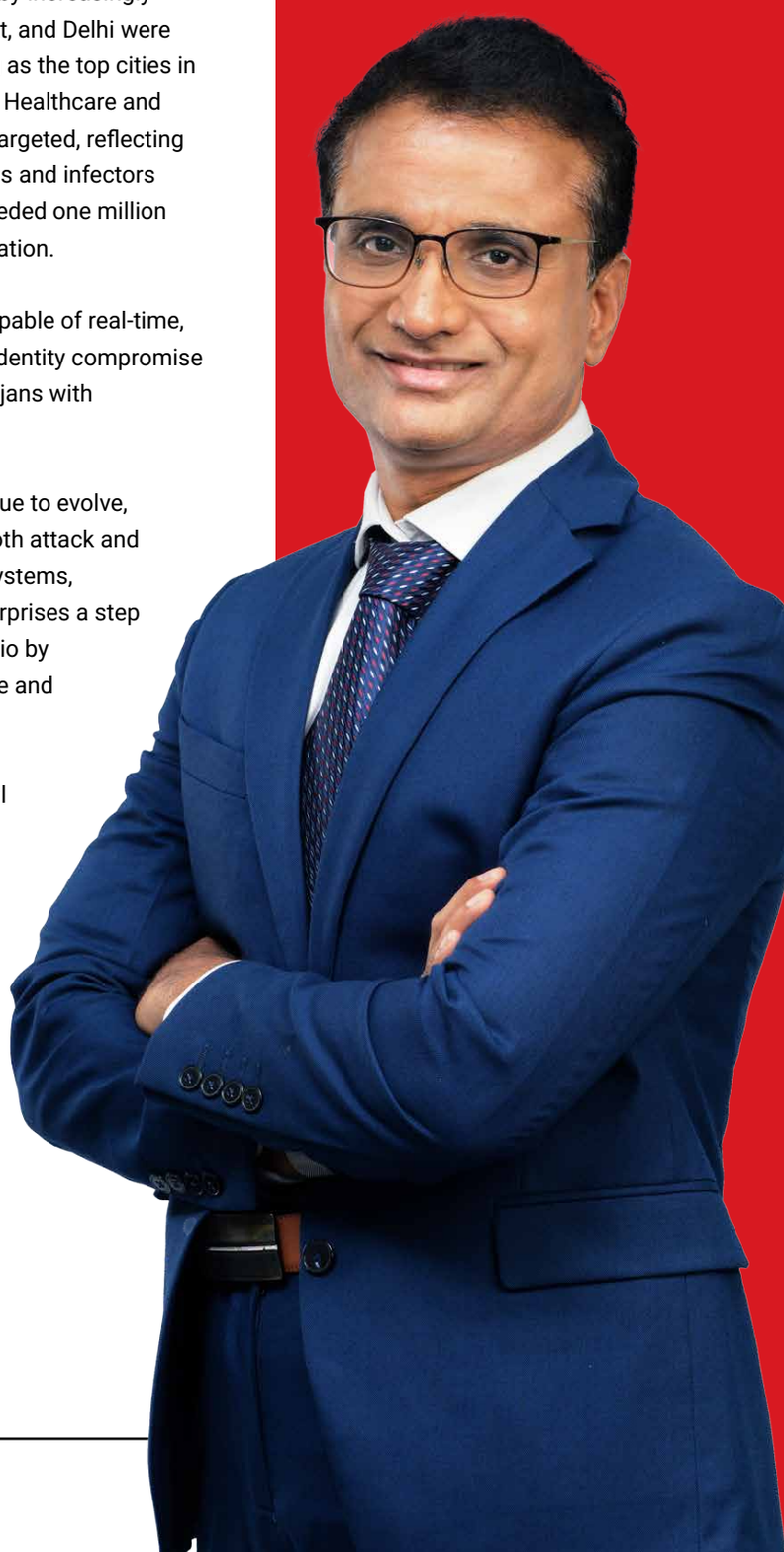
Hence, the country has witnessed a significant surge in cyber incidents, reflecting both the rapid pace of digital adoption and the growing sophistication of adversaries. Seqrite Labs, India's largest malware analysis centre monitoring over 8 million endpoints, has tracked and analysed this surge, providing actionable intelligence to enterprises, government institutions, and citizens.

Our findings indicate that India's cyber threat landscape is being shaped by increasingly automated, AI-assisted, and cross-platform attacks. Maharashtra, Gujarat, and Delhi were the most affected states, with Mumbai, New Delhi, and Kolkata emerging as the top cities in terms of incident density. Across various industries, including Education, Healthcare and Pharmaceuticals, and Manufacturing, these sectors remained the most targeted, reflecting both their economic and societal criticality. We also observed that Trojans and infectors together formed nearly 70 percent of all attacks, while ransomware exceeded one million detections, driven by double extortion campaigns and supply chain infiltration.

Among the alarming trends of 2025, AI-assisted phishing frameworks capable of real-time, contextual responses and the weaponization of OAuth tokens for cloud identity compromise stood out, alongside modular malware that combines remote access Trojans with automation, signalling the industrialization of cybercrime in India.

As we look ahead to 2026 and beyond, the threat environment will continue to evolve, becoming faster, smarter, and more adaptive. Generative AI will shape both attack and defense, hybrid and cloud-native surfaces will expand, and trust-based systems, including digital identities, will come under greater scrutiny. To keep enterprises a step ahead of evolving threats, Seqrite this year further strengthens its portfolio by launching two new services including Ransomware Recovery as a Service and Digital Risk Protection Service, which will help enterprises safeguard operational uptime and brand reputation by combining rapid post-attack recovery with proactive identification and neutralization of external digital threats. In addition, Seqrite Labs remains committed to equipping organisations with predictive intelligence, AI-powered defense capabilities, and actionable insights to help safeguard digital assets and preserve trust.

This report is an invitation to all stakeholders, including enterprises, policymakers, and citizens, to understand the evolving threats, recognise their implications, and engage in collective, proactive cybersecurity practices.

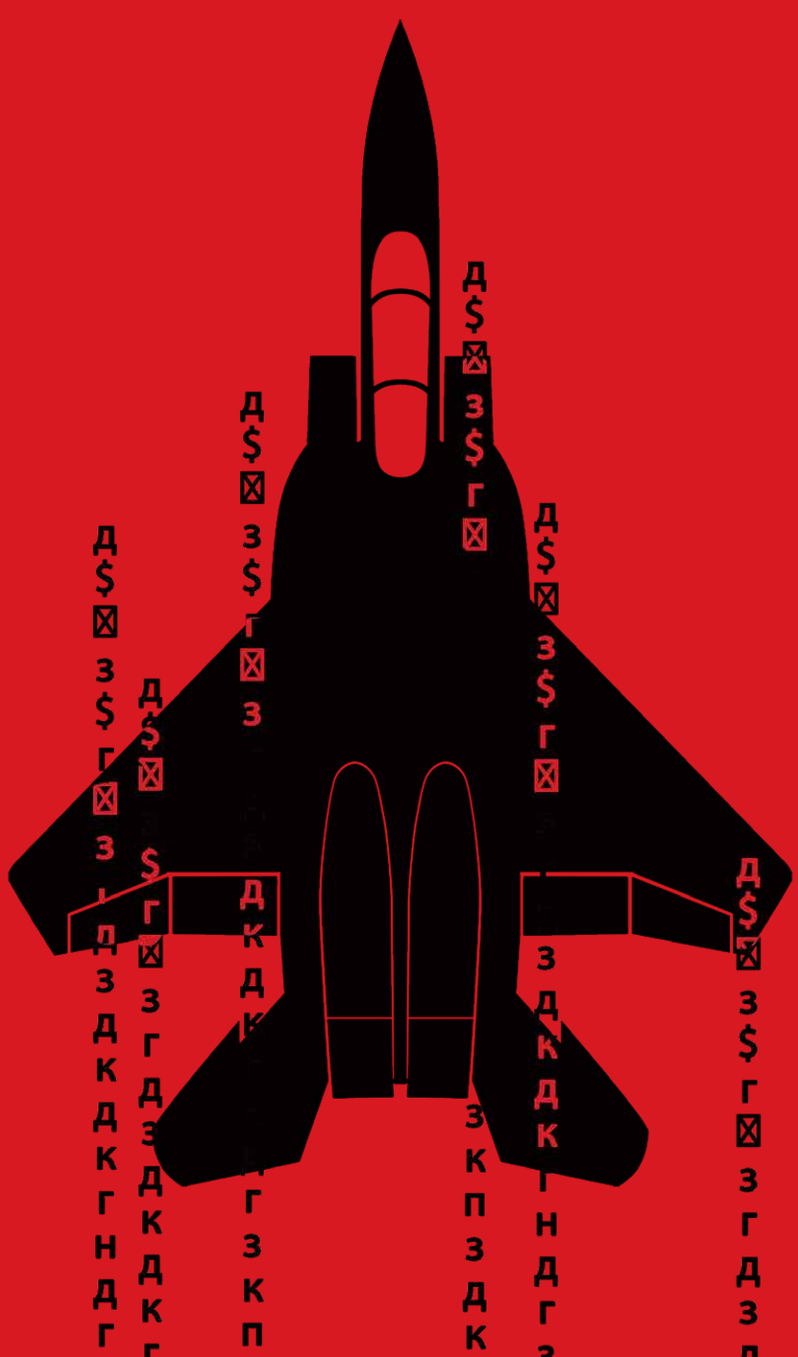


Dr. Sanjay Katkar

Joint Managing Director
Quick Heal Technologies Ltd.

Index

/{ executive **summary** };



Between October 2024 and September 2025, Seqrite's unified threat telemetry recorded 265.52 million detections across more than 8 million endpoints in India — ***averaging 505 detections every minute.*** This staggering volume underscores the relentless and adaptive nature of cyber threats targeting Indian enterprises, driven by a blend of legacy malware, fileless intrusions, AI-assisted phishing, and ransomware-as-a-service (RaaS) operations.

Behaviour-based technologies such as Next-Gen Antivirus (NGAV) and Anti-Ransomware (ARW) engines identified over 34 million anomalous detections, proving their value as the predictive defense layer against fileless and unknown attacks. Meanwhile, signature-based detections exceeded 230 million, highlighting that despite advances in evasion, traditional malware distribution remains a core component of India's cybercrime economy. The malware ecosystem remained dominated by Trojans (43%), File Infectors (35%), and Potentially Unwanted Applications (6%), reflecting adversaries' continued success through social engineering, cracked software, and legacy vulnerabilities.

Emerging threats such as cryptojacking and fileless persistence showcased a pivot toward stealth and sustained monetization, rather than overt disruption.

Ransomware, although accounting for less than 1% of total detections, had the highest strategic and financial impact. Activity peaked in January 2025, with 185 incidents and 113,000 detections, driven by campaigns like Xelera and Weaxor.

From an industry standpoint, the Education, Healthcare, and Manufacturing sectors together accounted for nearly 47% of all detections, underscoring how resource constraints, legacy infrastructure, and open collaboration networks continue to attract large-scale attacks.

On the geographical front, Maharashtra, Gujarat, and Delhi topped the list of affected states, while Mumbai, New Delhi, and Kolkata emerged as the most targeted cities — a reflection of dense financial, political, and industrial activity zones.

Globally connected ransomware groups such as Qilin, Akira, Cl0p, and Babuk2 dominated Indian campaigns, while hacktivist entities like Cyber Error System and INDOHAXSEC leveraged geopolitical flashpoints to launch DDoS, phishing, and defacement operations under banners like Operation Sindoor. This convergence of cybercrime and hacktivism marks a growing trend toward hybrid cyber warfare, where financial, political, and ideological motives overlap.

On the exploitation front, network-based attacks targeting WordPress Plugins, Apache Tomcat, and SysAid reflected continued exploitation of poor patch hygiene, while LNK-based host exploits reaffirmed that simple vectors remain devastatingly effective in unmanaged environments.

Emerging attack surfaces such as AI frameworks (Langflow) and cloud consoles indicate a shift toward targeting development and automation layers, signaling the beginning of AI stack exploitation.
The year also witnessed 25 major global and regional cyber campaigns, including Operation Sindoor, GrassCall, and Weaxor, revealing sophisticated supply-chain infiltration, phishing deception, and data extortion tactics. Additionally, the surge in zero-day weaponization from Oracle E-Business Suite to Cisco IOS demonstrates that patch latency remains one of the most exploited weaknesses across enterprises.

Looking ahead, Seqrite forecasts that 2026 will usher in the era of cognitive intrusions, where adversaries leverage AI to automate reconnaissance, deception, and persistence. *The threat battlefield will evolve from code-based to context-aware attacks, demanding defenses that are predictive, autonomous, and intelligence-led.*

KEY HIGHLIGHTS

265.52M DETECTIONS

across over 8 million endpoints were recorded averaging 505 detections every minute.

EDUCATION, HEALTHCARE MANUFACTURING

Sectors recorded 12.5 million detections, accounting for 47% of total volume.

Most affected states:

MAHARASHTRA *36.1M*

GUJARAT *24.1M*

DELHI *15.4M*

TROJANS *(~88.4M)*, FILE INFECTORS *(~71.1M)*

dominated, together making up nearly 70% of all malware detections.

BEHAVIOUR BASED DETECTIONS (NGAV + ANTI-RANSOMWARE)

blocked ~34M advanced threats, including fileless and encryption-based attacks.

CRYPTOJACKING DETECTIONS *(~6.5M)*

outpaced Ransomware (~0.81M), indicating a shift toward stealth monetization.

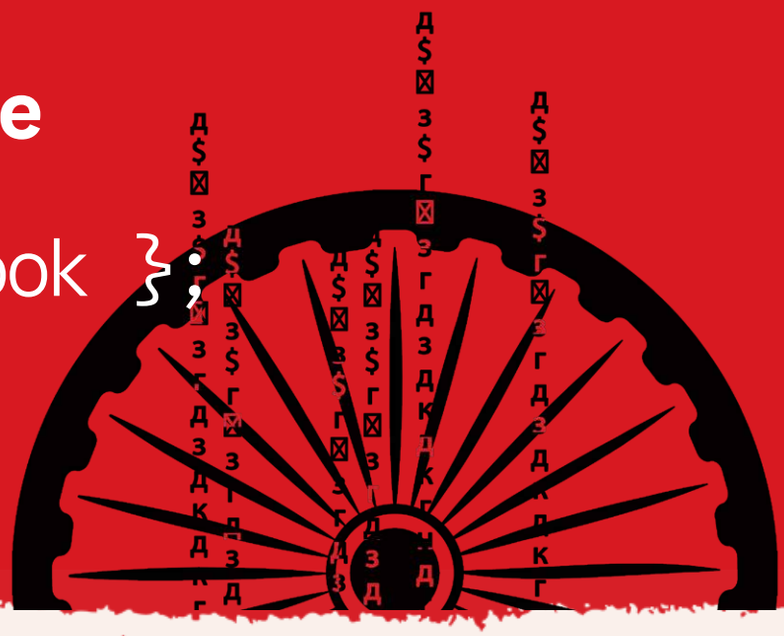
RANSOMWARE ACTIVITY PEAKED IN JAN

2025 with 185 incidents and 113,000 detections, led by Xelera and Weaxor campaigns.

NETWORK-BASED EXPLOITS EXCEEDED *9.2 MILLION* SCANS,

targeting WordPress, Apache Tomcat, and SysAid systems.

/{ india under **cyber siege** the 2025 threat outlook };



Between October 2024 and September 2025, Seqrite's unified telemetry recorded an astounding 265.52 million detections over 8 million endpoints, translating to nearly 727,000 detections per day or around 505 detections every minute.

This data reflects the unrelenting pace and sophistication of cyberattacks targeting Indian organisations, driven by a mix of legacy exploits, fileless malware, and evolving ransomware campaigns.

Yearly Detection Overview

Detection volumes remained consistently high throughout the 12-month period, fluctuating between 17.6 million and 23.1 million detections per month.

Peaks were observed in October 2024 and January 2025, coinciding with major ransomware and phishing activity, while a steady plateau from April to August reflected sustained but controlled intrusion attempts.
This consistency suggests that India's threat ecosystem has shifted from episodic outbreaks to continuous, automation-driven attack patterns.

Threat actors are no longer waiting for opportunities. They are constantly scanning, exploiting, and monetizing digital weaknesses.

Behaviour-Based Detections: *The Predictive Shield*

Behavioural analytics — powered by Next-Gen Antivirus (NGAV) and Anti-Ransomware (ARW) technologies identified over 34 million detections during the year.

These detections focused on identifying anomalous execution, encryption activity, and fileless intrusion techniques, often bypassing traditional signature-based models.

BEHAVIOUR BASED DETECTIONS The Predictive Shield

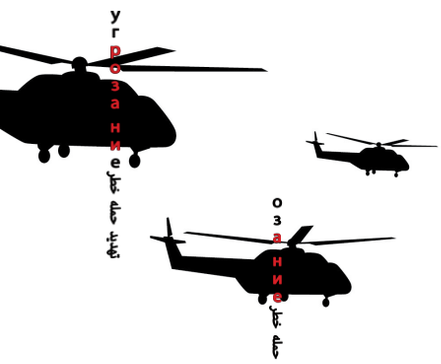
Behaviour-based detections saw notable spikes during Q1 2025, correlating with heightened ransomware activity and large-scale phishing-to-ransomware conversion chains.

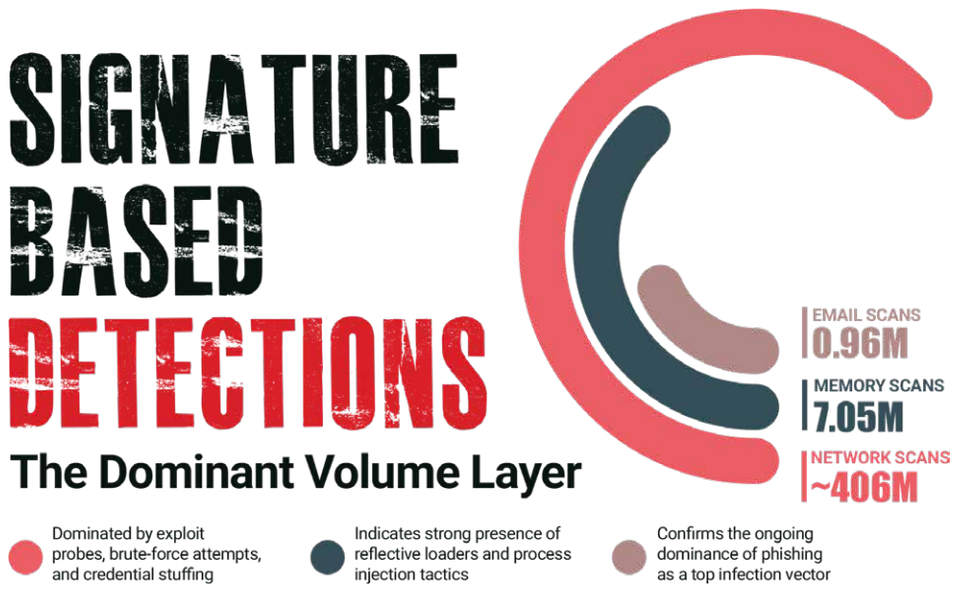
This clearly indicates that proactive behavioural layers now form the first line of defense against emerging and unknown threats.

Signature-Based Detections: *The Dominant Volume Layer*

Signature-based detections encompassing network, memory, and email scans accounted for the majority of observed threat activity, exceeding 415 million detections.

While traditional in nature, these detections remain crucial in catching mass malware distribution, brute-force network intrusions, and exploit-driven attacks.



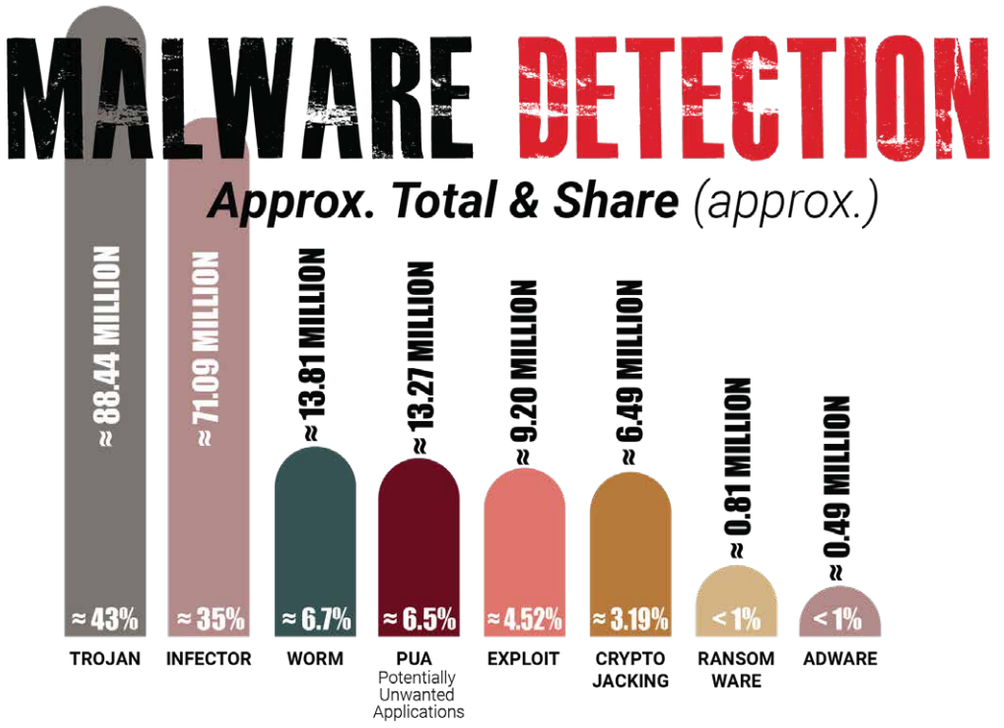


Network scanning remained the most exploited entry point, accounting for more than 90% of total detections underscoring that exposed, unpatched systems continue to be the weakest link in enterprise security posture.

/{ the state of
| **malware in**
| **india** };

The malware ecosystem remained heavily skewed toward high-volume, low-complexity threats such as Trojans, Infectors, and Worms. Together, these accounted for over 65% of all detections, underscoring how adversaries continue to rely on social engineering, cracked software, and legacy vulnerabilities to compromise systems at scale.

While overall detection volumes stayed steady across the year, newer monetization-driven campaigns, particularly cryptojacking signalled a shift towards stealthy, profit-centric cybercrime.



Trojans

The Prime Infection Driver (~ 88.44M Detections)

Trojans represented the single largest malware family, contributing roughly four in every ten infections.

They acted as the initial payload in multistage campaigns, enabling credential theft, data exfiltration, or ransomware deployment. Dominant variants such as W32.Pioneer.CZ1, Trojan.Agent, and W32.Expiro.R3 leveraged phishing attachments, weaponized documents, and compromised websites.

Trojans continue to serve as the backbone of cybercrime operations due to their adaptability and modular design.

Infectors

Persistent Legacy Threats (~ 71.09M Detections)

File-infecting malware remained the second-largest category, reflecting continued exposure in unpatched Windows environments and older endpoint infrastructures.

Infectors modify legitimate executables to ensure reinfection and persistence, often spreading through USB drives and shared folders. Despite improved behavioural detection, their endurance highlights slow patch adoption and outdated software ecosystems in several sectors.

Worms

Enduring Network Pests (~ 13.81M Detections)

Worms continued exploiting SMB and AutoRun vulnerabilities, particularly in education, manufacturing, and small business networks. Their ability to propagate laterally and reactivate after cleaning makes them a persistent concern for unmanaged and legacy systems.

PUAs

Hidden Gateways for Intrusion (~ 13.27M Detections)

PUAs accounted for nearly one in every fifteen detections, reflecting widespread presence across both home and enterprise endpoints. While often dismissed as low-risk, these applications act as launchpads for credential stealers, adware, and miners. Most originate from cracked utilities, fake browser extensions, or deceptive installers, blurring the boundary between nuisanceware and active threats.

Exploits

From Mass Attacks to Targeted Intrusions (~ 9.20M Detections)

Exploits contributed a smaller share of detections but posed a significant strategic risk. Attackers increasingly targeted specific web servers, email gateways, and ERP systems rather than launching broad exploit-kit campaigns. This shift toward precision reflects the evolution of exploitation tactics from opportunistic compromise to controlled entry for APT operations.

Cryptojacking

The Silent Profit Engine (~ 6.49M Detections)

Cryptojacking emerged as one of the fastest-growing categories, with detections nearing five million. Adversaries hijacked compute power to mine Monero and PKT coins, primarily by exploiting RDP, Docker, or cloud misconfigurations. Its stealthy nature causing performance degradation rather than data loss makes it a profitable, low-noise alternative to ransomware.

Ransomware

Low Frequency, High Impact (~ 0.81M Detections)

Ransomware volume remained relatively small, but the impact per incident was severe. Modern strains like Weaxor, Xelera, and WantToCry used multi-extortion tactics, combining encryption, data theft, and public leaks. Most infections originated from Trojans or credential abuse, demonstrating ransomware's evolution into a post-compromise weapon rather than a random payload.

Adware

Declining but Widespread (~ 0.49M Detections)

Adware showed the steepest decline, partly due to stronger browser protection and mobile OS security. However, millions of detections still originated from malvertising networks and bundled installers.

While relatively benign, adware contributes to alert fatigue and can conceal more serious payloads within telemetry data.

/{ malware
| **warranting**
attention };

W32.Expiro.R3

File Infector | High

A legacy yet highly destructive file infector that targets executable files (both 32-bit and 64-bit). It spreads through cracked software and removable drives, and once active, it modifies application files, spreads through network drives, and can execute remote commands, allowing large-scale propagation across networks.

Trojan.KillAv.DR

Trojan | High

A Trojan known for disabling antivirus processes (“Kill AV”). It spreads through malicious email attachments or compromised sites and often disguises itself with legitimate Windows icons. Once executed, it can steal system and network information and deliver additional payloads such as spyware or remote access tools.

Trojan.Floxif.E5

Trojan | High

Distributed through infected USB drives and bundled software installers (notably a tampered version of CCleaner). It collects user and system details including unique IDs and MAC addresses, and transmits them to command-and-control servers, acting as both a data stealer and downloader for further infections.

Worm.Autoit.Sohanad.S

Worm | High

A self-replicating worm that spreads rapidly through messaging apps, removable drives, and network shares. It disguises itself as a Windows folder icon (.exe), tricking users into execution, after which it replicates to all connected drives enabling fast, uncontrolled spread in local networks.

W32.Brontok.Q

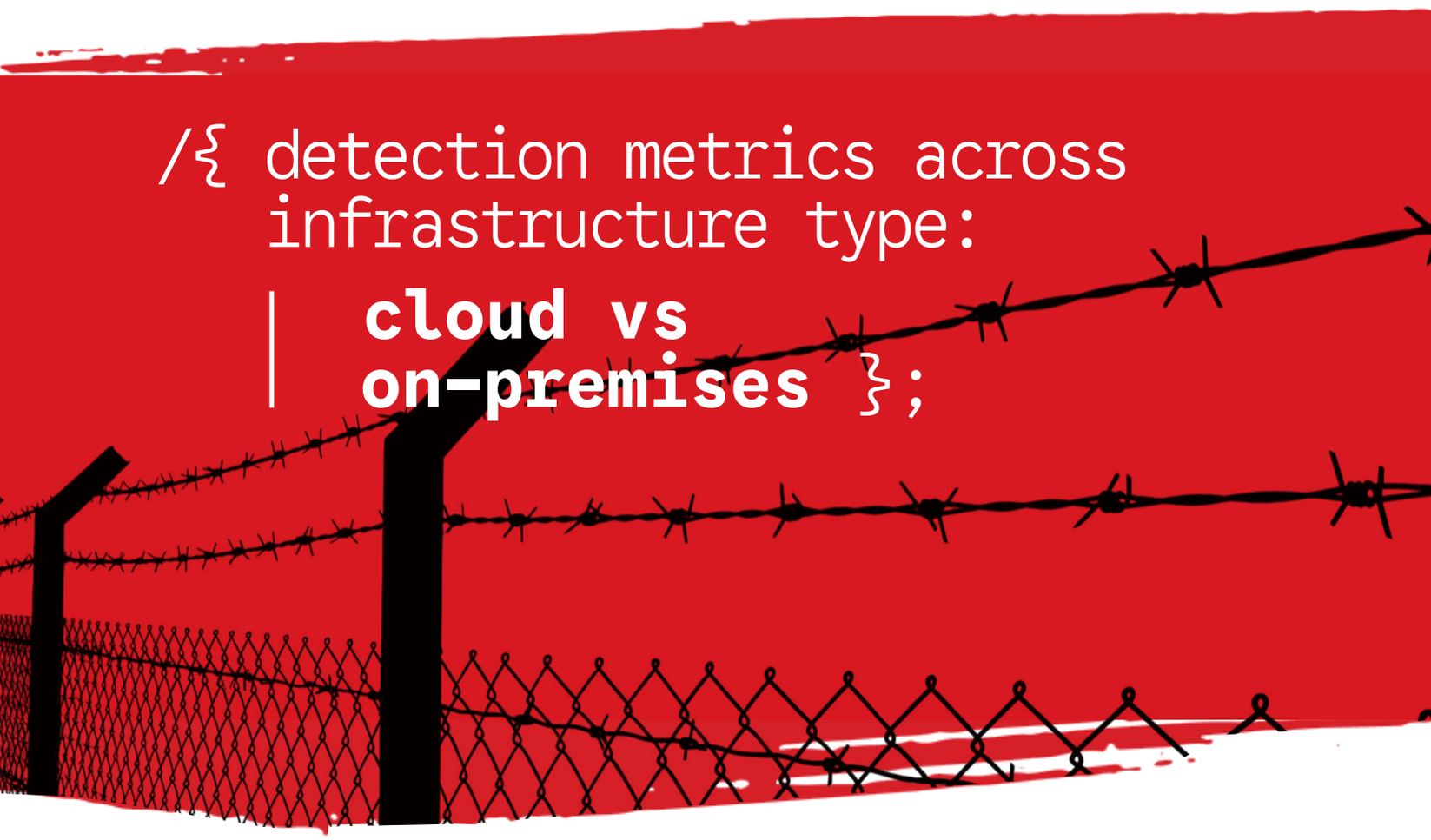
Worm | Medium

A resilient worm transmitted through infected USB devices and email attachments. It disables security tools, alters system settings, and modifies the HOSTS file to block access to security websites. Though older, it remains active in networks with weak endpoint protection.

Trojan.NSIS.Miner.SD

Trojan/Cryptominer | High

A resource-abusing Trojan that installs through malicious freeware or compromised websites. It secretly uses system resources for cryptocurrency mining (e.g., Bitcoin), heavily degrading performance. Additionally, it modifies system files, opens backdoors, and enables further malware infiltration.



Seqrite's telemetry data highlights a clear distinction between detection trends across cloud and on-premise environments, underscoring differences in adoption, exposure, and risk density.

Over the 12-month period, detections across cloud and on-prem infrastructures revealed that while cloud adoption is steadily increasing, on-prem systems remain the dominant source of threats due to legacy dependencies and broader endpoint bases.

	AVG ENDPOINTS	AVG ACTIVE CUSTOMERS	AVG MONTHLY DETECTIONS	SHARE OF TOTAL DETECTIONS
CLOUD	~5.6L	~6k	~0.33M	9%
ON-PREM	~19L	~23k	~3.5M	91%

KEY INSIGHTS

ON-PREM REMAINS THE PRIMARY TARGET

On-premises environments account for 91% of all detections, driven by a much larger endpoint base (~19 lakh), legacy systems, and higher exposure to automated attacks.

CLOUD SHOWS LOWER VOLUME BUT DIFFERENT RISKS

Cloud contributes only 9% of detections, supported by stronger native security controls, but faces more targeted threats such as identity misuse, OAuth abuse, and API exploitation. and unmanaged devices remain the primary attack surface.

ENDPOINT VISIBILITY ALONE IS NOT ENOUGH FOR CLOUD

Many cloud intrusions bypass traditional malware vectors and therefore do not surface in endpoint detection logs, making configuration drift, identity misuse, and access monitoring critical.

HYBRID ENVIRONMENTS NEED UNIFIED, AI-DRIVEN DEFENSE

With high-volume threat activity on-prem (~3.5M monthly detections) and stealthy, identity-centric cloud attacks, enterprises require integrated visibility and AI-powered security to close the gap.

Ransomware activity through FY25 revealed a clear pattern — a sharp escalation in the early months, steady containment mid-year, and a resurgence toward the close of the fiscal period.

The telemetry highlights how adversaries continuously evolved tactics, transitioning from mass-scale attacks to precision-targeted campaigns.

- **Early 2025:** *The Apex of Ransomware Activity*

  January 2025 recorded the highest surge, with 185 incidents and over 113,000 detections, representing a major ransomware wave driven by campaigns such as Xelera and Weaxor.

  Attackers leveraged large phishing infrastructures, cracked software, and malicious loaders to propagate payloads at scale, exploiting weak patch hygiene and credential reuse.

- **Mid-Year:** *Stabilization Through Proactive Containment*

  February through April saw a gradual decline in detections from 74,000 to 69,000 per month signaling effective containment through behavioural and anti-ransomware controls.

  Despite the reduction, incident volumes remained steady, underscoring the persistent probing nature of ransomware operators testing endpoint and network defenses.

- **May 2025:** *Tactical Shift to Targeted Intrusions*

  A distinct inflection was observed in May, with 126 incidents but comparatively lower detections (~57,000). This mismatch indicates low-volume, high-impact enterprise-focused intrusions, where attackers infiltrated environments through supply-chain or remote service vectors before triggering encryption.

- **Late 2025:** *Variant Recycling and Renewed Activity*

  August and September marked another climb, with detections exceeding 60,000 per month and incidents rising to 107. The activity corresponds to the re-emergence of retooled ransomware families, leveraging old exploits and stolen credentials, a trend consistent with post-compromise persistence tactics.

KEY INSIGHTS

1. **Sustained Threat Pressure:** Ransomware remained one of the most consistent and financially motivated threats across the year, with continuous detection events despite intermittent declines.

2. **Behavioural Defense Effectiveness:** The incident-to-detection ratio averaged 1:700, demonstrating that early-stage behavioural and heuristic layers successfully disrupted most encryption attempts.

3. **Shift to Enterprise-Grade Targets:** The spike in incidents during May points to strategic targeting of high-value environments over indiscriminate mass campaigns.

4. **Persistent Scanning Activity:** Even during quieter months, detections never dropped below 55,000 - confirming that adversaries maintained ongoing network reconnaissance and payload testing.

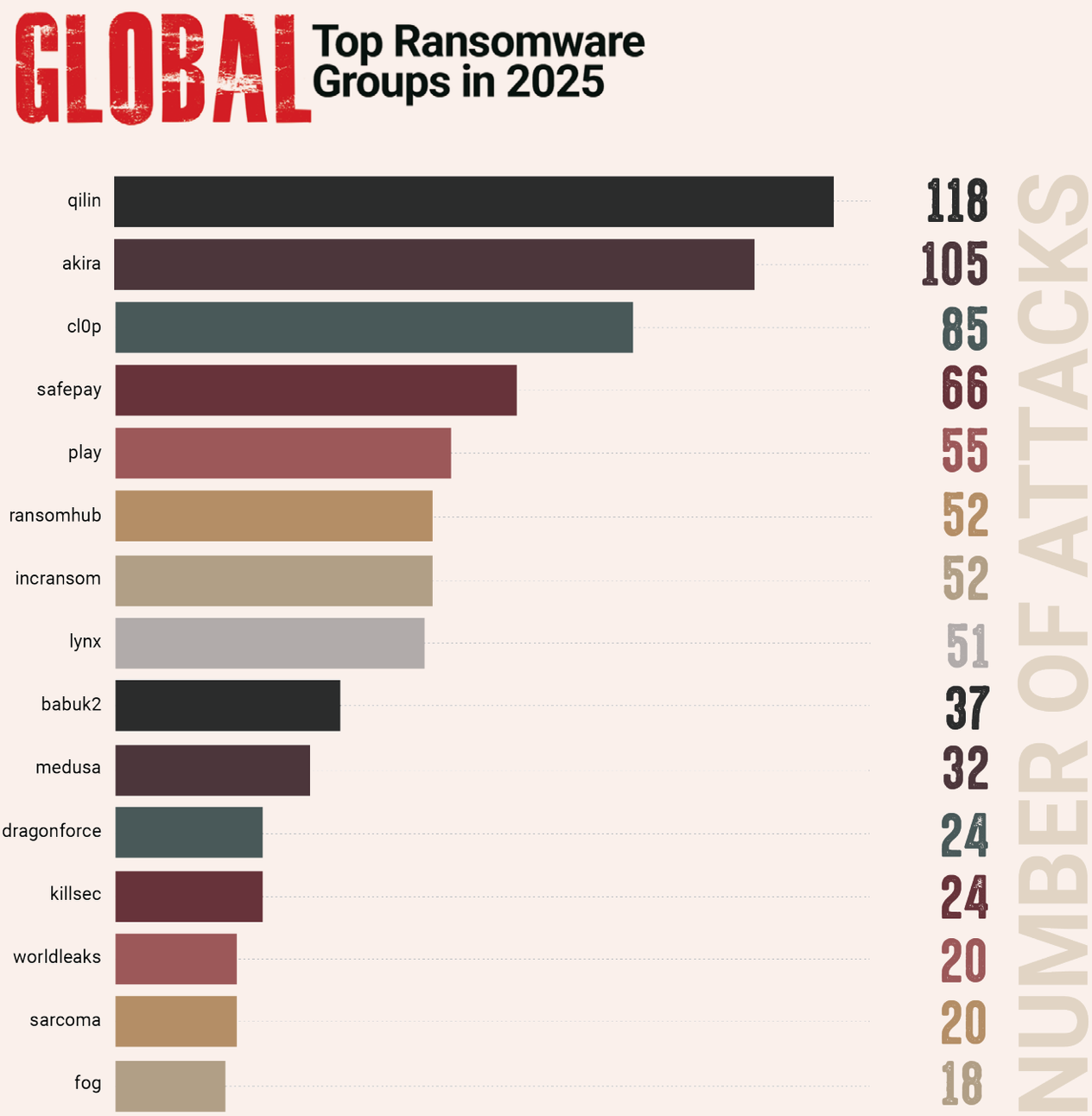
5. **Resilient Defense Posture:** By late 2025, defenses matured to intercept ransomware across pre-encryption and lateral movement stages, reflecting stronger response automation and visibility across infrastructures.

/{ top
ransomware &
hacktivist
groups
2025 };

The Human Faces Behind Automation: *Mapping the Global and Indian Threat Ecosystem*

Following the surge in ransomware detections and incidents in 2025, Seqrite Labs traced the operational footprints of major ransomware and hacktivist groups that shaped the global and Indian threat landscape.

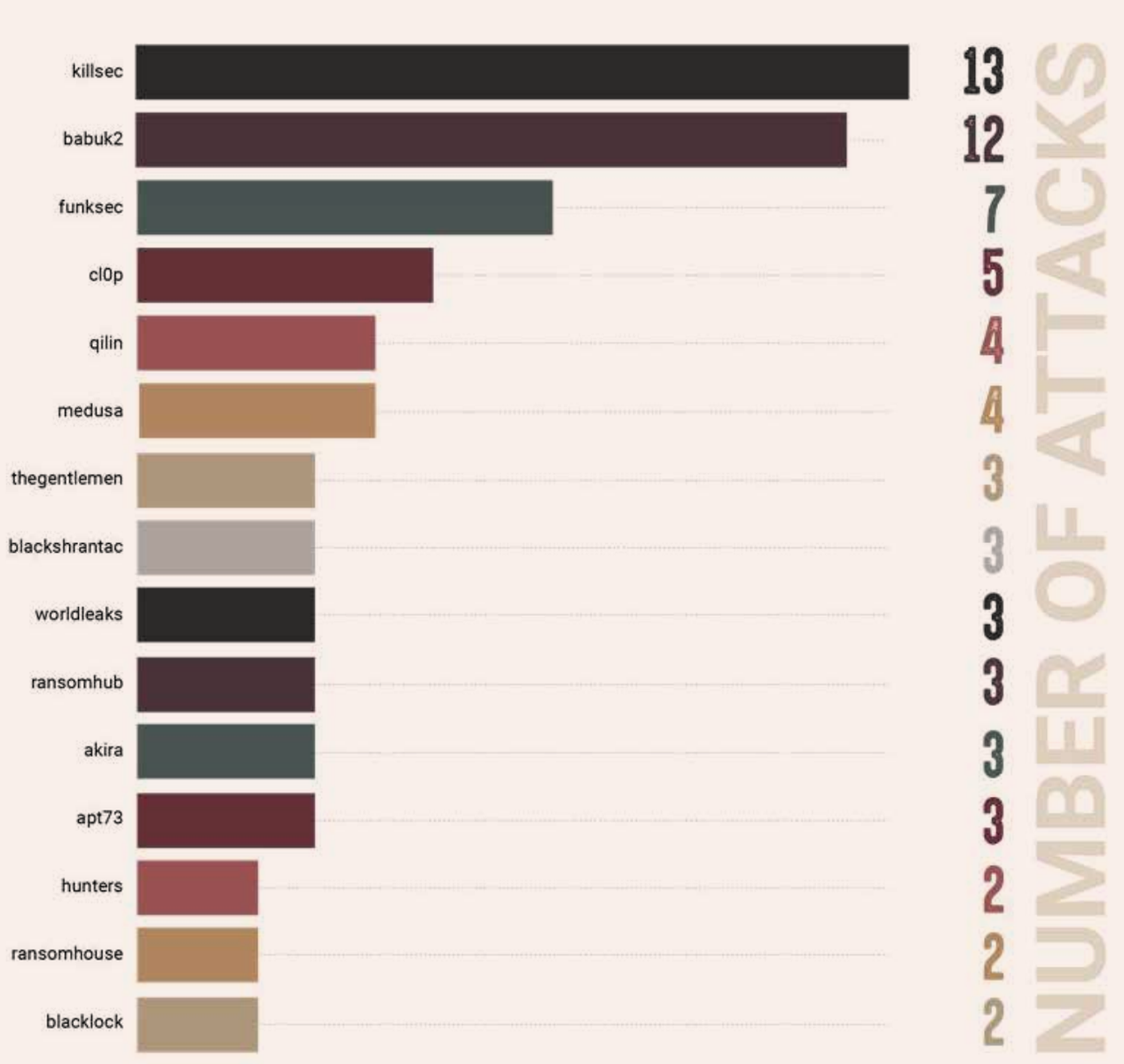
The data reveals an increasingly industrialized ecosystem — where ransomware syndicates operate like businesses, and hacktivist groups exploit geopolitical tensions to amplify chaos and influence public discourse.



2025 marked the consolidation of ransomware-as-a-service (RaaS) operations, with Qilin, Akira, and Cl0p dominating globally. These groups shifted tactics from mass encryption to data extortion and cloud compromise, often using OAuth and API abuse for lateral movement.

Groups like Play and Ransomhub leveraged automation and AI for faster reconnaissance and adaptive encryption payloads. Emerging players like Incransom and Lynx illustrated how smaller affiliates are rapidly scaling through shared tooling and leaked RaaS infrastructure.

INDIA Top Ransomware Groups in 2025



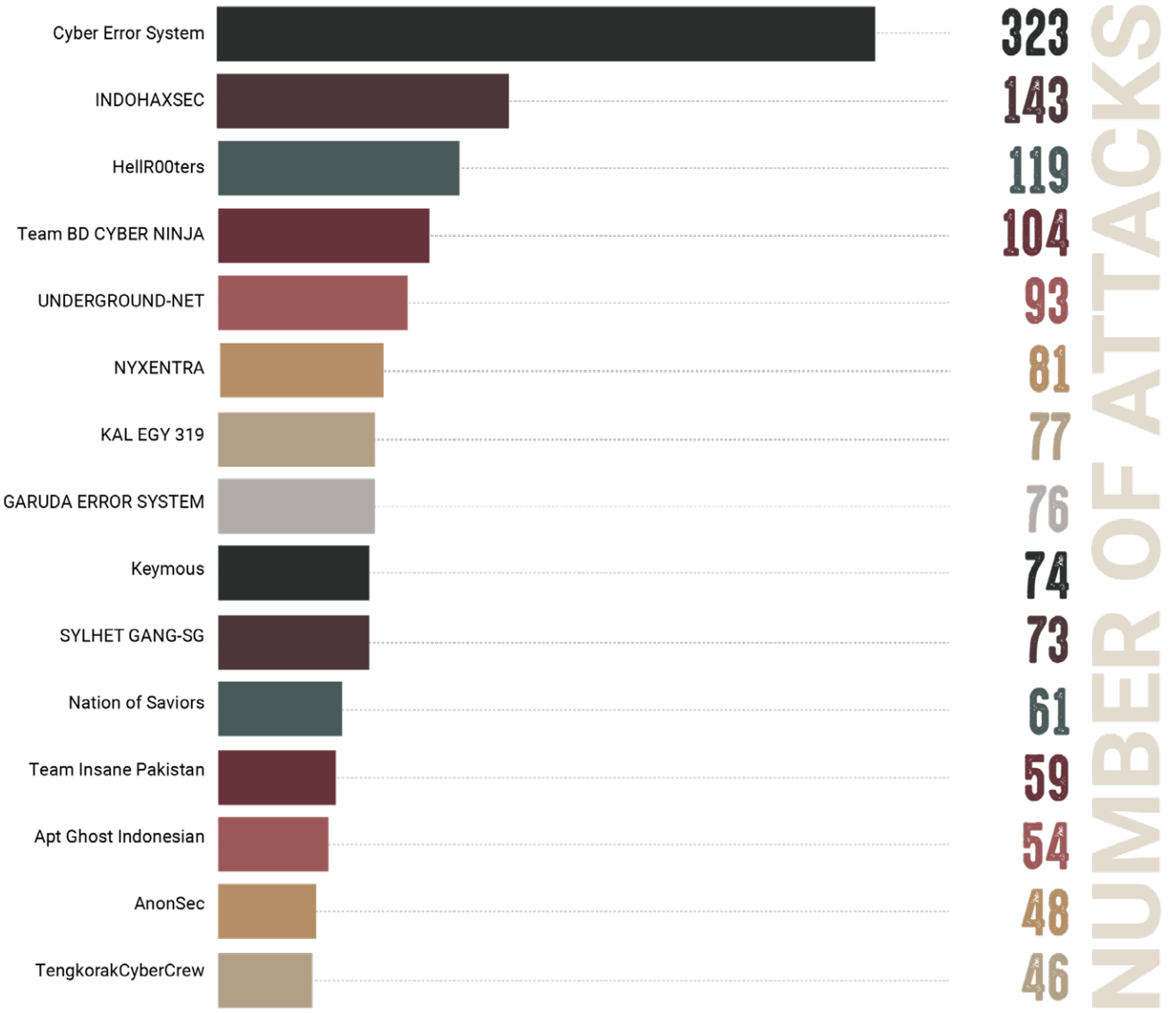
India's ransomware landscape reflects global-to-local spillover — where international syndicates operate through localized affiliates and regionalized campaigns.

Groups like KillSec and Babuk2 were especially active against BFSI, healthcare, and manufacturing, exploiting remote desktop exposure and supply chain vulnerabilities.

New entrants such as FunkSec and TheGentlemen targeted SMBs and educational institutions, leveraging phishing and infector hybrids.

The data underscores how India is increasingly part of the global ransomware economy, not just a peripheral target.

Top Hacktivist Groups Targeting INDIA



Hacktivism in 2025 evolved from symbolic website defacements to coordinated psychological and influence operations. Leading groups such as Cyber Error System, INDOHAXSEC, and HellR00ters orchestrated large-scale DDoS, phishing, and defacement attacks on Indian government and media entities, often timed around geopolitical flashpoints.

Their campaigns blended propaganda, misinformation, and digital disruption, reflecting a new phase of cyber activism intertwined with geopolitics. Notably, the activity spike during Operation Sindoor highlighted hacktivism's transition from nuisance-level attacks to strategic cyber offensives with real-world impact.

STRATEGIC TAKEAWAYS

RANSOM-WARE ECOSYSTEM

Now an organized economy with affiliate networks, revenue sharing, and service-based operations (RaaS).

INDIA'S GROWING DIGITAL FOOTPRINT

Makes it a lucrative ransomware frontier, with both local and global groups exploiting hybrid infrastructures.

HACKTIVISM HAS MATURED

into cyber influence warfare, blurring lines between political protest, state-sponsored disinformation, and cybercrime.

DEFENSIVE POSTURE

must evolve...

toward predictive intelligence, attribution-driven detection, and cross-sector information sharing to disrupt these ecosystems early.

/{ network-based **exploits** };

Network exploitation remained a dominant intrusion vector through 2025, reflecting a concerning mix of poor patch hygiene, expanding attack surfaces, and rapid weaponization of newly disclosed vulnerabilities. Seqrite telemetry revealed that attackers actively targeted internet-facing applications such as CMS platforms, middleware, and administrative consoles, with exploit traffic often automated through botnets and mass-scan tools.

Top Network Exploits Observed

WordPress Plugins Exploitation: *The New CMS Epidemic*

- **Total affected customers:** 3,075
- **Detection count:** 394
- **Vulnerability:** CVE-2025-3102 – SureTriggers/OttoKit Authentication Bypass
- Attackers leveraged missing validation in authentication tokens to create rogue admin accounts, leading to full site takeover, defacement, and SEO poisoning.
- This campaign was largely automated, with exploit traffic originating from botnets leveraging compromised VPS nodes and targeting Indian SMEs and content-hosting providers.

Langflow RCE: *AI Development Environments Under Fire*

- **Total affected customers:** 2,861
- **Detection count:** 12
- **Vulnerability:** CVE-2025-3248 – Unauthenticated RCE through API endpoint
- Exploitation attempts involved Python exec() abuse, granting full code execution through unsecured /api/v1/validate/code endpoints.
- The appearance of this CVE in active telemetry marks the first wave of AI stack–oriented attacks, signaling that developer and ML infrastructure are becoming valuable targets for reconnaissance and persistence.

Apache Tomcat Exploitation: *Persistent Entry through Middleware*

- **Total affected customers:** 234
- **Detection count:** 97
- **Vulnerability:** CVE-2025-24813 – Path Equivalence / Partial PUT Exploit
- **Attackers exploited writable servlet paths** to overwrite serialized objects, deploy webshells, and establish persistence within application servers. These intrusions align with tactics used by APT actors and cybercrime groups focusing on data theft and internal pivoting from compromised middleware.

SysAid XXE Exploit: *Targeting IT Management Consoles*

- **Total affected customers**: 225
- **Detection count:** 57
- **Vulnerability:** CVE-2025-2775 – XML External Entity Injection
- **Adversaries exploited /mdm/checkin and /serverurl endpoints** to read system files and escalate privileges. Given SysAid's privileged position in IT infrastructure, successful exploitation provides attackers with network-wide administrative access.

MailEnable XSS: *Phishing Through Infrastructure*

- **Total affected customers:** 245
- **Detection count:** 40
- **Vulnerability:** CVE-2025-44148 – Reflected XSS (failure.aspx)
- Exploits used crafted URLs to inject JavaScript into admin sessions, leading to session hijacking and malicious redirects. While older in nature, MailEnable's wide usage across self-hosted enterprise mail servers keeps it a consistent target for exploit recycling.

KEY TAKEAWAYS

- HTTP-based exploitation is now a dominant attack vector, driven by automated reconnaissance and public exploit kits.
- CMS platforms like WordPress remain persistently vulnerable, serving as a convenient entry point into corporate and government networks.
- Middleware and DevOps tools (Tomcat, Langflow, SysAid) represent high-value targets, bridging application and infrastructure layers for lateral movement.
- The expansion of exploit activity into AI ecosystems marks a major evolution in threat targeting for 2026 and beyond.
- Network defense must shift toward continuous exposure management, real-time patch orchestration, and behavioural network detection to counter this new era of stealth exploitation.

/{ host-based exploits };

A surge in LNK-based exploits dominated host-level detections this year, revealing how attackers continue to exploit simple Windows shortcut vulnerabilities to achieve code execution, persistence, and lateral movement. Over 8 million detections were recorded, with LNK.Cmd.Exploit.F leading due to its ability to self-propagate across USBs and shared drives. These exploits thrive in environments with weak removable media controls, legacy systems, and user-driven file interactions, making them a persistent challenge for enterprises.

HOST-BASED EXPLOITS

MALWARE	DETECTIONS	UNIQUE CUSTOMERS AFFECTED
LNK.Cmd.Exploit.F	5,169,490	42,072
LNK.Exploit.Gen	2,335,153	76,929
LNK.Exploit.Cpl.Gen	412,279	14,421
LNK.USB.Exploit	117,991	14,262
HTML/IFrame_Exploit.CE	41,909	601

LNK.Cmd.Exploit.F

The most widespread host exploit, capable of autonomously spreading through removable drives, shared folders, and emails. It executes malicious code when users open or preview infected shortcut files, often installing secondary malware and causing rapid propagation across internal networks.

LNK.Exploit.Gen

A generic Windows shortcut exploit that triggers arbitrary code when parsed. It is widely distributed through phishing campaigns and compromised archives, enabling attackers to deploy payloads or escalate privileges with minimal user interaction.

LNK.Exploit.Cpl.Gen

Abuses Control Panel shortcut (.CPL) handling flaws to execute hidden payloads. Often used to gain persistence or deploy backdoors, allowing attackers to maintain long-term footholds within enterprise networks.

LNK.USB.Exploit

Targets USB autorun behaviours to infect hosts when removable media is accessed. It spreads silently across devices and is commonly observed in controlled or isolated environments where network security tools have limited visibility.

HTML/IFrame_Exploit.CE

A browser-based exploit using malicious HTML or iFrame injections to execute drive-by payloads. It takes advantage of outdated browser plugins or unpatched vulnerabilities, enabling silent compromise during routine browsing.

RECOMMENDED ACTIONS

HARDEN ENDPOINT AND USB CONTROLS

Disable Windows autorun features and restrict .LNK and .CPL execution from removable or shared drives. Enforce device control policies to prevent unauthorised USB usage.

IMPLEMENT APPLICATION ALLOWLISTING

Allow only trusted executables to run. Block unknown or unsigned binaries, especially those launched through explorer or shortcut parsing.

PROACTIVE THREAT HUNTING AND MONITORING

Regularly scan for LNK-related artifacts and suspicious explorer-launched processes. Monitor network shares for abnormal file creation or replication activity.

UPDATE LEGACY SYSTEMS AND PATCHES

Apply security updates that fix known shortcut parsing flaws (e.g., CVE-2010-2568) to eliminate long-standing exploit vectors.

BUILD USER AWARENESS

Educate employees about risks associated with unknown USB drives, phishing attachments, and shortcut-based files to minimize accidental infections.

/{ android threat **landscape** };

1. Lured and Compromised: *The Rise of Digital Honey Traps*

Digital honey traps have become a powerful social engineering tool where attackers build emotional connections over social media, WhatsApp, or dating apps to extract sensitive information. These profiles are often AI-generated, complete with realistic photos and crafted backstories. Conversations typically begin casually, then shift toward personal bonding, and finally, subtle probing for workplace details, internal documents, or private media.

In several Indian cases, personnel from the Army, paramilitary forces, and defense research units were targeted through such tactics. Victims were manipulated into sharing operational details or compromising information, which attackers later used for blackmail or coercion. The danger of honey traps lies in the fact that no malware is required. The breach occurs purely through trust exploitation. Raising awareness and encouraging quick reporting remain the strongest defenses.

Medium

Government, Defense, Intelligence

India, Asia-Pacific

2. ‘NextGen mParivahan’ Malware *Returns with Enhanced Stealth*

A more sophisticated version of the fake “NextGen mParivahan” malware resurfaced alongside the app’s rebranding. Attackers send SMS messages about pending traffic challans, complete with vehicle numbers and violation codes, directing users to download a malicious APK. The fake app looks identical to the real government interface, making detection difficult for average users.

Once installed, it requests invasive permissions, hides its icon, and silently collects device notifications, SMS, and sensitive user’s data. It also shows a fake challan-payment page to steal UPI or card details. The malware relies on encrypted communication and dynamically generated C2 addresses, allowing it to bypass traditional detection methods. These campaigns highlight the growing trend of government-service impersonation for fraud and identity theft.
Seqrite Labs Detection: Android.Dropper

High | India

3. High-Security Registration Plate (HSRP) Scam

The HSRP scam targets vehicle owners by mimicking official booking portals and promoting them through Google ads, SMS alerts, and WhatsApp forwards. These fake sites look authentic, asking users to enter vehicle information and make online payments for plate installation.

Some campaigns now include links to “HSRP verification apps” that request access to SMS or call data, enabling OTP theft and unauthorised UPI transactions. Victims lose money upfront and unknowingly expose personal information such as RC numbers, addresses, and phone details, and this data is later used for additional fraud. The scam’s success relies on urgency messaging (“final notice”, “fine imposed”) and the lack of verification from users.

Seqrite blocks malicious URLs linked to this scam.

Medium | India

4. SparkKitty Spyware

SparkKitty is a cross-platform spyware family found embedded inside modified versions of gaming apps, TikTok clones, and adult-content apps popular in Southeast Asia. Users often download these apps from third-party stores, unaware that the embedded code silently extracts photos, device information, and app tokens once installed.

The spyware operates quietly in the background, sending stolen data to remote servers through encrypted channels. Unlike targeted espionage malware, SparkKitty operates broadly, collecting large volumes of personal media from infected devices. Its presence in apps that sometimes pass basic store checks suggests an increased risk from malicious SDKs and developer-side compromise.

Seqrite Labs Detection: Android.SparkKitty

High | Southeast Asia, China

5. Evolving Android Banking Trojans *Pose Serious Financial Threats*

Banking Trojans on Android grew significantly more advanced during the year.
OctoV2 spreads through phishing pages disguised as AI or productivity apps and abuses Accessibility permissions to read screens, stream activity, and perform on-device fraud. Zanubis, originally spotted in Latin America, continues to evolve into a full device-control Trojan that locks screens and captures banking credentials while posing as legitimate service apps.

The most sophisticated, TsarBot, impersonates Google Play Services and uses precise overlay screens to steal banking logins, credit-card details, and OTPs. It communicates through WebSockets, allowing attackers to execute real-time transactions. These Trojans are part of organized, monetization-driven ecosystems that target global users and rely heavily on social engineering for installation.

Seqrite Labs Detection: Android.Banker

High | Global

/{ top zero-day threats 2025 };

2025 marked a surge in zero-day weaponization across enterprise, network, and endpoint ecosystems. Threat actors including ransomware and extortion groups — exploited critical flaws within days of disclosure. These attacks underscored the urgent need for faster patch cycles, application isolation, and continuous threat-hunting across hybrid infrastructures.

1. Oracle E-Business Suite *(CVE-2025-61882)*

A critical unauthenticated RCE flaw exploited by CL0P-linked actors to compromise ERP servers, steal business data, and issue extortion demands.

IMPACT: Complete system takeover, database exposure, and lateral movement inside finance and HR networks.

ACTION: Patch immediately; restrict public access to EBS; review logs for unusual commands or outbound transfers.

2. Microsoft Windows Core *(CVE-2025-59230 / 24990 / 47827)*

Multiple Windows zero-days patched in October 2025 after confirmed in-the-wild exploitation.

IMPACT: Privilege escalation and remote execution across enterprise endpoints — enabling domain compromise.

ACTION: Deploy the October updates enterprise-wide; verify no deferred patching; hunt for new admin accounts or scheduled tasks.

3. Cisco SNMP "Zero Disco" *(CVE-2025-20352)*

A remote-code flaw in Cisco IOS/XE devices used to implant rootkits for long-term persistence & network monitoring.

IMPACT: Network-level compromise allowing traffic interception and covert C2 channels.

ACTION: Patch and restrict SNMP; validate firmware integrity; monitor for rogue outbound traffic from network devices.

4. 7-Zip Symbolic-Link Vulnerabilities *(CVE-2025-11001 & 11002)*

Two archive-parsing flaws enabling malicious ZIP files to overwrite system files and execute code.

IMPACT: Endpoint compromise through user-interaction or automated file extraction.

ACTION: Upgrade 7-Zip across all systems; disable auto-extraction on servers; reinforce user awareness on malicious attachments.

5. Adobe AEM Forms *(CVE-2025-54253)*

An OGNL injection bug allowing pre-authentication code execution; leveraged in ransomware intrusions.

IMPACT: Full control of web servers hosting digital forms and portals; potential internal pivot.

ACTION: Patch AEM immediately; restrict admin access; scan for webshells and unknown uploads.

STRATEGIC OBSERVATIONS

ZERO-DAY
Exploitation
now begins within a week of disclosure.

ATTACKERS TARGET
Business platforms
(ERP, CMS, network firmware), not just endpoints. infrastructures.

PATCHING LATENCY
remains the most exploited weakness.

ORGANISA-TIONS
with strong threat-hunting and asset visibility
contained breaches fastest.

LEADERSHIP PRIORITIES

FOCUS AREA	OBJECTIVE	OUTCOME
Accelerated Patching	Apply critical fixes within 5 days of disclosure	Reduced exposure window
Network Segmentation	Isolate admin & application tiers	Contain lateral movement
Threat Hunting	Retrospective review post-patch	Early detection of persistence
Vendor Oversight	Track CISA KEV & vendor advisories	Up-to-date posture
Executive Metrics	Measure Mean Time to Remediate (MTTR)	Board-level risk visibility

/{ geographical hotspots };

Top 10 States With the Highest Malware Detection

RANK	STATE	DETECTIONS in millions	SHARE
1	MAHARASHTRA	36.13	24.31%
2	GUJARAT	24.13	16.24%
3	DELHI NCR	15.41	10.37%
4	WEST BENGAL	14.35	9.66%
5	UTTAR PRADESH	13.94	9.38%
6	KARNATAKA	11.64	7.83%
7	TAMIL NADU	7.51	5.05%
8	MADHYA PRADESH	7.33	4.93%
9	RAJASTHAN	6.8	4.58%
10	TELANGANA	6.59	4.43%

1. Maharashtra *36.13M detections*

Maharashtra registers the highest threat activity, supported by one of India's largest digital estates, including 556K+ engineering & manufacturing units, 1.5M+ healthcare entities, 473K+ IT & software units, and 765K+ education institutions, creating unmatched adversarial exposure.

2. Gujarat *24.13M detections*

Gujarat's elevated threat levels reflect its massive industrial backbone, comprising millions of manufacturing, engineering, chemical, and textile units, forming dense endpoint clusters frequently targeted by automated and supply-chain-oriented attacks.

3. Delhi (NCR) *15.41M detections*

Delhi's position is anchored in its high-value concentration of 231K+ education entities, 20.9K+ media organisations, 65K+ financial services units, and critical government infrastructure, making it continuously attractive for threat actors.

4. West Bengal *14.35M detections*

West Bengal's threat density is driven by its exceptionally large Energy & Utilities sector (159,983 units), Media & Entertainment (192,077 units), major government networks, and public-service institutions that are recurrent targets.

5. Uttar Pradesh *13.94M detections*

Uttar Pradesh reports high detections due to its broad endpoint distribution across 1.14M+ misc. businesses, 163K+ education units, 71K+ IT entities, 111K+ healthcare units, and expansive government services.

6. Karnataka *11.64M detections*

Karnataka's threat profile correlates with its massive IT & software ecosystem (65,714 units), 225K+ engineering & manufacturing units, and 329K+ education organisations, with Bengaluru's digital-first environment amplifying exposure.

7. Tamil Nadu *7.51M detections*

Tamil Nadu's detections stem from robust industrial networks including 18.9K automotive units, 142K engineering & manufacturing units, 62K consumer goods entities, and 68K real-estate and construction organisations.

8. Madhya Pradesh *7.33M detections*

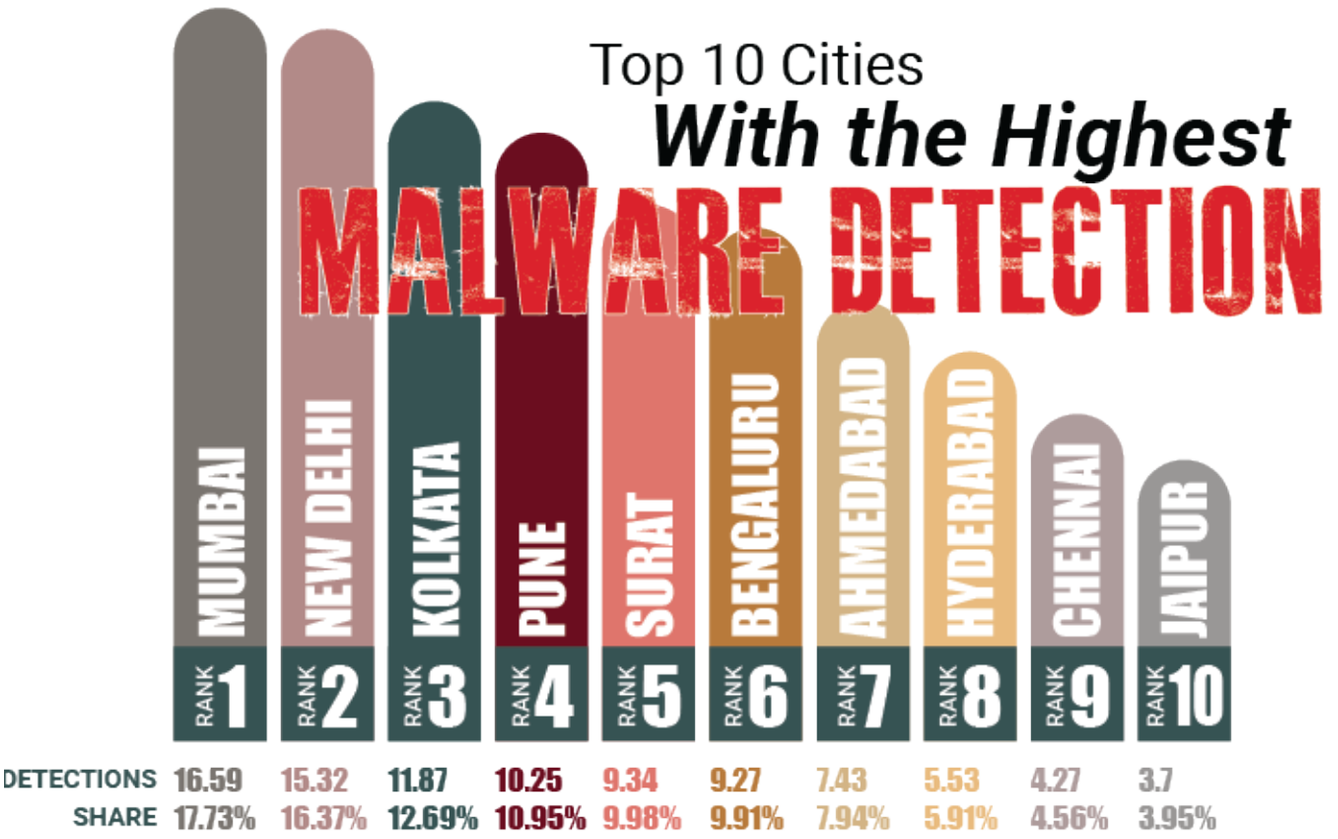
Madhya Pradesh maintains high activity through 106K+ engineering & manufacturing units, 36K+ healthcare entities, 43K+ education units, and 36K+ logistics & transportation organisations, contributing to broad digital exposure.

9. Rajasthan *6.80M detections*

Rajasthan's threat landscape is shaped by its extensive public-sector services, large education systems, and expanding manufacturing and construction footprints, driving significant endpoint presence.

10. Telangana *6.59M detections*

Telangana's exposure is driven by very large healthcare & life sciences clusters (232,863 units), 259K+ education entities, and 182K+ engineering & manufacturing units, alongside Hyderabad's expanding IT infrastructure.



1. Mumbai

India's financial capital with dense BFSI, media, and enterprise networks makes it the most targeted

2. New Delhi

High concentration of government, public-sector, and critical infrastructure drives sustained threat activity

3. Kolkata

Large public-sector institutions, utilities, and media ecosystems attract continuous intrusion attempts.

4. Pune

Major IT, R&D, education, and manufacturing clusters create a wide and diverse attack surface.

5. Surat

Massive textile and SME manufacturing hubs lead to dense endpoint presence vulnerable to automated attacks.

6. Bengaluru

India's tech hub with thousands of IT firms and startups creates high-value digital exposure.

7. Ahmedabad

Strong industrial base across textile, chemical, and manufacturing sectors attracts threat actors.

8. Hyderabad

Large healthcare, life sciences, and IT ecosystems make it a lucrative target for data-driven attacks

9. Chennai

Automotive, manufacturing, and retail supply chains contribute to sustained malware activity.

10. Jaipur

Rapidly growing digital adoption across education, SMEs, and government services increases exposure.

/{ industry insights };

Top 10 Most AFFECTED INDUSTRIES

RANK	INDUSTRY	DETECTIONS	SHARE
01	Education & Training	4,924,679	18.45%
02	Healthcare & Pharmaceuticals	3,799,177	14.24%
03	Engineering & Manufacturing	3,794,114	14.22%
04	Government	2,882,393	10.80%
05	Information Technology & Software	2,761,738	10.35%
06	Metals, Mining & Materials	1,234,218	4.62%
07	Financial Services	1,163,772	4.36%
08	Construction & Real Estate	918,061	3.44%
09	Consumer Goods & Retail	918,061	3.44%
10	Energy & Utilities	609,119	2.28%

1. Education & Training *4.92M detections (18.45%)*

Education remained the most targeted sector. Attackers exploited unpatched systems, shared Wi-Fi networks, and poorly secured research infrastructure. Frequent use of Trojan.Pioneer.CZ1 and W32.Expiro.R3 malware families indicates large-scale credential theft, coin-mining, and data exfiltration campaigns across universities and training institutions.

2. Healthcare & Pharmaceuticals *3.79M detections (14.24%)*

Healthcare continued to face relentless exploitation, driven by data-rich hospital networks and patient management systems. Malware such as W32.Expiro.R3 and Trojan.Eqtonex were observed compromising EHR platforms, while RAT-based intrusions indicated sustained espionage efforts targeting pharma R&D data and clinical trials.

3. Engineering & Manufacturing *3.79M detections (14.22%)*

Manufacturing and industrial units saw a spike in malware-laced CAD tools, spear-phishing campaigns, and lateral movement through SMB exploits. Nsis.Bitmin, Trojan.Shadowbrokers, and KillAv.DR families dominated detections, underscoring the vulnerability of production and design systems integrated with legacy OT assets.

4. Government *2.88M detections (10.80%)*

The government sector was consistently targeted by state-backed APT campaigns and ransomware groups. Malware such as LNK.HoudRAT.47401 and Eqtonex facilitated espionage, file exfiltration, and disruption of e-governance portals. Increased APT activity points toward strategic intelligence collection and digital disruption motives.

5. Information Technology & Software *2.76M detections (10.35%)*

The IT sector, serving as a backbone for India's digital economy, faced high malware activity, especially fileless and loader-based attacks.

Infections driven by W32.Mofksys.A4, Trojan.GenericPMF variants, and Miner.SD reveal a trend toward supply-chain infiltration and payload staging on developer endpoints.

6. Metals, Mining & Materials *1.23M detections (4.62%)*

This sector witnessed targeted intrusions focused on industrial design theft, production data compromise, and OT system exploitation.

Trojan.Eqtonex and PMF.S3146672 were primary threats, often delivered through phishing or compromised ERP environments.

7. Financial Services *1.16M detections (4.36%)*

Financial institutions faced ongoing threats from credential stealers, banking Trojans, and fake update campaigns. Detections of Trojan.CryptRI, Risktool.Bitcoinminer, and Infostealer variants underline the persistence of financially motivated cybercrime targeting digital banking systems and fintech platforms.

8. Construction & Real Estate – *918K detections (2.80%)*

Construction and real estate saw social engineering-based intrusions leveraging fake tenders and invoice attachments. Malware such as Trojan.KillAv.DR and Hacktool.Keygen were prevalent, indicating a shift toward industrial espionage and financial fraud campaigns.

9. Consumer Goods & Retail – *918K detections (2.28%)*

Retail and consumer goods industries continued to attract attackers through point-of-sale (POS) malware, phishing, and credential-harvesting loaders. Detections suggest exploitation of e-commerce APIs, misconfigured databases, and weakly protected vendor systems.

10. Energy & Utilities – *609K detections (2.9%)*

The energy sector recorded steady but significant threats linked to W32.Sality and Eqtonex variants, hinting at adversaries probing critical power and oil infrastructure. Attacks mainly focused on data reconnaissance and lateral movement, emphasizing the need for continuous OT-IT convergence security.

KEY TAKEAWAYS

EDUCATION, HEALTHCARE, & MANUFACTURING

together contribute over 47% of all detections, underlining their critical exposure.

GOVERNMENT & IT SECTORS

remain under dual pressure from espionage-driven APTs and commodity malware.

ENERGY, FINANCE, & INFRASTRUCTURE

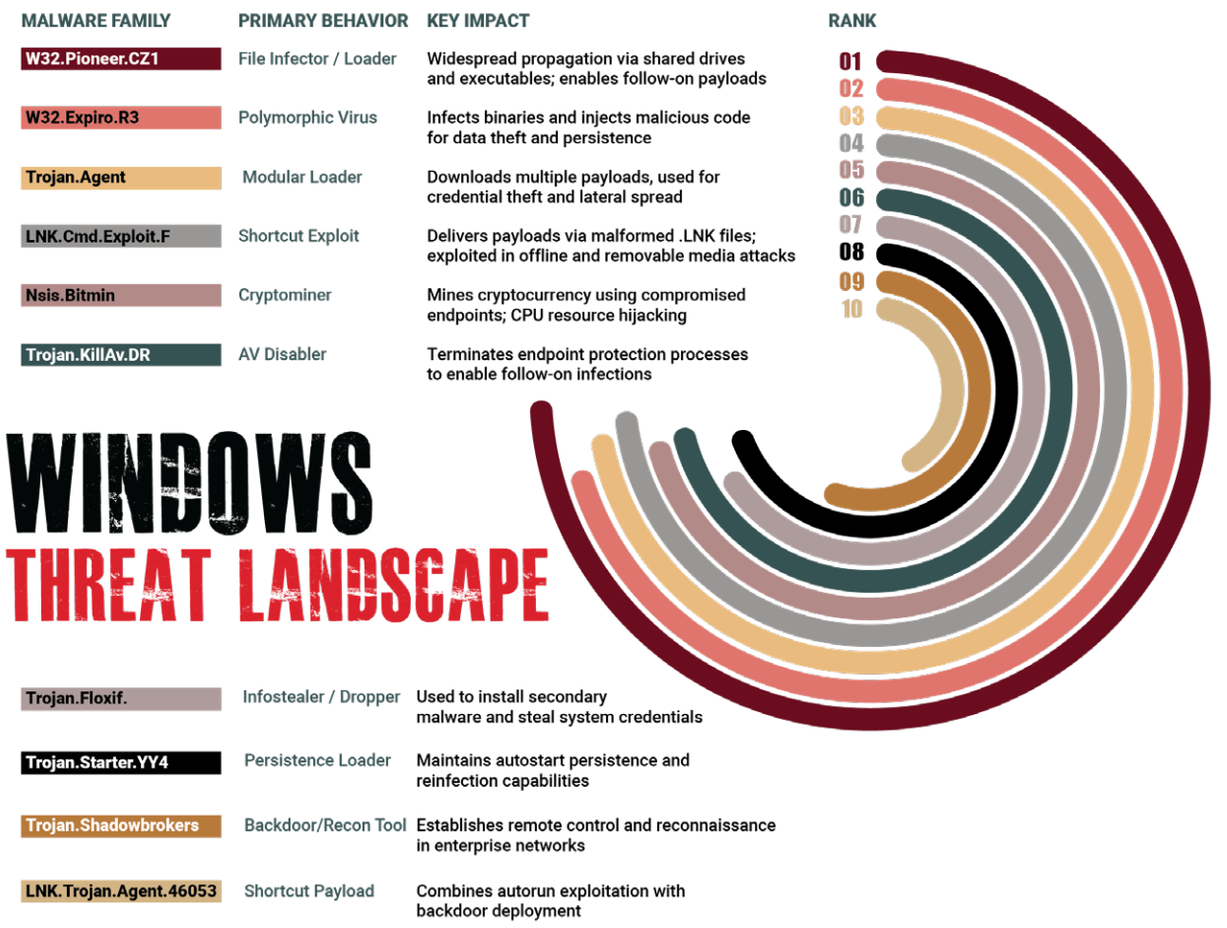
industries are witnessing cross-domain attack convergence — where traditional IT malware targets OT and supply-chain endpoints.

MALWARE-AS-A-SERVICE (MaaS) & AI-ASSISTED PHISHING

are accelerating infection rates across both high-value and mid-tier enterprises.

/{ windows
| **threat**
landscape };

The Windows malware ecosystem in 2025 continued to evolve — not through new malware families, but through the reinvention of old ones. Seqrite's telemetry reveals that legacy malware such as W32.Pioneer.CZ1, W32.Expiro.R3, Trojan.Agent, and LNK.Cmd.Exploit.F remains dominant, accounting for the bulk of detections. These families have endured for years, but their latest variants exhibit increased automation, stealth, and persistence, making them harder to eradicate across enterprise networks and hybrid work setups.



MALWARE FAMILY	PRIMARY BEHAVIOR	KEY IMPACT	RANK
W32.Pioneer.CZ1	File Infector / Loader	Widespread propagation via shared drives and executables; enables follow-on payloads	01
W32.Expiro.R3	Polymorphic Virus	Infects binaries and injects malicious code for data theft and persistence	02
Trojan.Agent	Modular Loader	Downloads multiple payloads, used for credential theft and lateral spread	03
LNK.Cmd.Exploit.F	Shortcut Exploit	Delivers payloads via malformed .LNK files; exploited in offline and removable media attacks	04
Nsis.Bitmin	Cryptominer	Mines cryptocurrency using compromised endpoints; CPU resource hijacking	05
Trojan.KillAv.DR	AV Disabler	Terminates endpoint protection processes to enable follow-on infections	06
Trojan.Floxif.	Infostealer / Dropper	Used to install secondary malware and steal system credentials	07
Trojan.Starter.YY4	Persistence Loader	Maintains autostart persistence and reinfection capabilities	08
Trojan.Shadowbrokers	Backdoor/Recon Tool	Establishes remote control and reconnaissance in enterprise networks	09
LNK.Trojan.Agent.46053	Shortcut Payload	Combines autorun exploitation with backdoor deployment	10

KEY THREAT INSIGHTS

1. Legacy Persistence, Modern Stealth

Despite being over a decade old, file infectors such as Pioneer.CZ1 and Expiro.R3 continue to dominate detections, reflecting ongoing gaps in patch hygiene and endpoint segmentation. Modern variants incorporate obfuscation and anti-sandbox techniques, turning simple file infectors into resilient loaders capable of evading first-generation antivirus detection.

2. Shortcut and Autorun Exploits Re-emerge

LNK.Cmd.Exploit.F and related trojans showed strong, recurring activity across multiple quarters. These infections thrive in hybrid work environments where USB drives and offline data transfers remain common. They underline a low-tech but highly effective intrusion tactic that continues to bypass network-layer defenses.

3. Cryptomining Quietly Expands

Nsis.Bitmin and Trojan.NSIS.Miner.SD represented the stealthier monetization vector of 2025. Attackers now deploy miners that automatically adapt CPU usage to avoid detection. The combination of miner payloads and compromised enterprise compute resources suggests monetization-driven persistence campaigns running parallel to espionage or ransomware operations.

4. Modular Trojans Become the Norm

Families like Trojan.Agent, Trojan.Floxif.E5, and Trojan.KillAv.DR demonstrate modular evolution—each designed to deploy, disable, or adapt. Once a system is compromised, these trojans establish persistence, disable protections, and act as conduits for ransomware or espionage modules, effectively turning endpoints into multi-purpose launchpads.

5. A Blended Threat Environment

Across 2024–2025, the data reveals a convergence of traditional malware, cryptominers, and backdoor implants. Attackers increasingly reuse known codebases, wrapping them in modern evasion frameworks, resulting in familiar signatures but far more capable behaviour.

2025 TAKEAWAYS

- Legacy malware remains dominant, proving that attackers prioritize reliability and reach over novelty.
- Shortcut-based and autorun infections surged, underscoring the ongoing importance of USB security and removable drive control.
- Cryptomining and stealth monetization replaced visible ransomware spikes, highlighting attackers' preference for silent profit.
- Trojans evolved into modular ecosystems, enabling persistent infiltration and multi-stage payload delivery.
- The Windows threat landscape in India remains a mix of the old and the adaptive, demanding continuous visibility, behavioural analysis, and faster patch cycles to reduce reinfection risk.

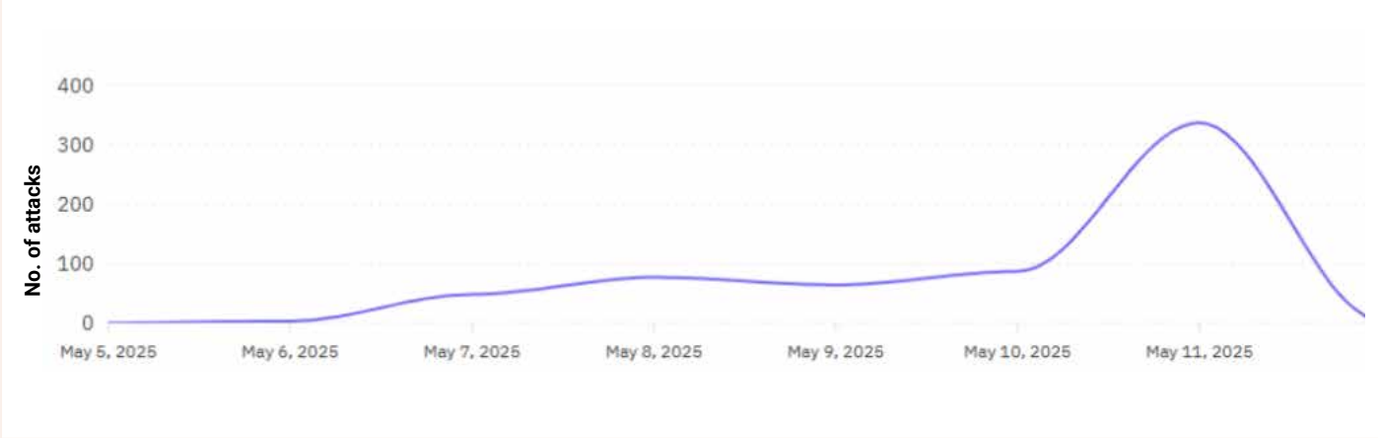
/{ major | **cyber campaigns** of 2025 };

Operation Sindoor

Anatomy of a Digital Siege

Uncovered by Seqrite Labs, Operation Sindoor exposed a coordinated campaign involving state-sponsored APT36 and SideCopy groups, working alongside hacktivist collectives. The operation blended cyber espionage, data theft, and digital disruption, representing a new phase of hybrid warfare targeting India's critical sectors. Attackers used spear-phishing emails, spoofed government domains, and malware-laced lure files to infiltrate defense and government IT systems. The introduction of Ares RAT, a modular and evasive remote access tool, enabled persistent surveillance and data exfiltration. Simultaneously, hacktivist groups launched defacements, DDoS attacks, and data leaks, amplifying impact through Telegram channels under banners like #OpIndia and #OperationSindoor.

High | **India** | **Government, Defense, Intelligence, IT, Healthcare, Telecom, Education**



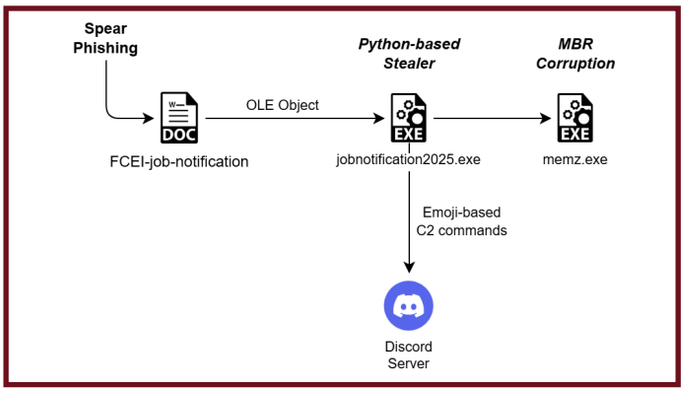
XELERA Ransomware Campaign

Fake Food Corporation of India Job Offers Targeting Tech Aspirants

Cybercriminals are once again exploiting the aspirations of India's young tech professionals, this time using fake government job offers to deliver a sophisticated ransomware campaign. Attackers posed as the Food Corporation of India (FCI) and circulated deceptive job descriptions and application documents that secretly deployed XELERA ransomware.

Victims received a malicious document titled FCEI-job-notification.doc, containing a PyInstaller-packed executable named jobnotification2025.exe. Upon execution, the malware connected to a Discord-based command-and-control (C2) server to steal data and receive commands, while simultaneously encrypting files and demanding ransom payments in Litecoin.

Beyond encryption, XELERA disrupted infected systems by terminating Windows Explorer processes unless a decoy file was open, and it downloaded a destructive MBR-corrupting Trojan (MEMZ.exe) that rendered systems unbootable. It also changed wallpapers, deleted files, flooded desktops with ransom notes, altered window titles, and used Text-to-



Speech to broadcast ransom demands.

This campaign demonstrates how attackers now combine fake job offers, Python-based malware, and Discord-based controls to evade detection and target vulnerable job seekers.

Seqrite Labs Detection: OLE.Ransom.49280.GC, Ransom.Variant.Xelera

High

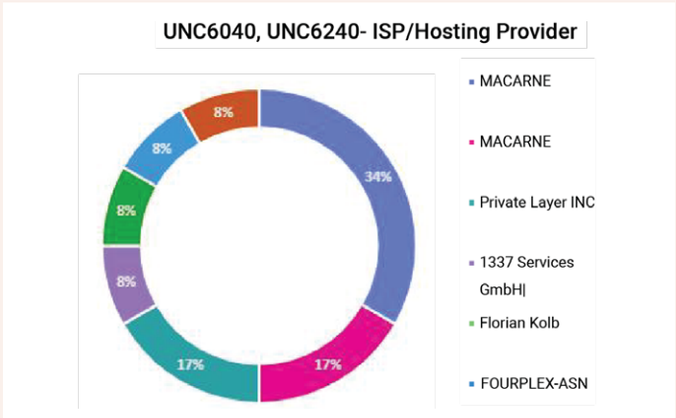
India

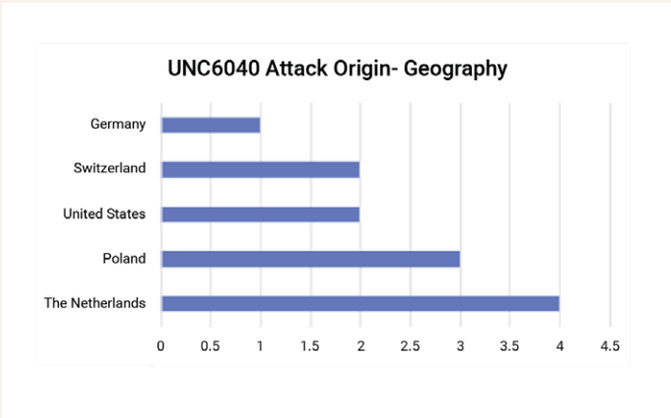
Google Salesforce Breach

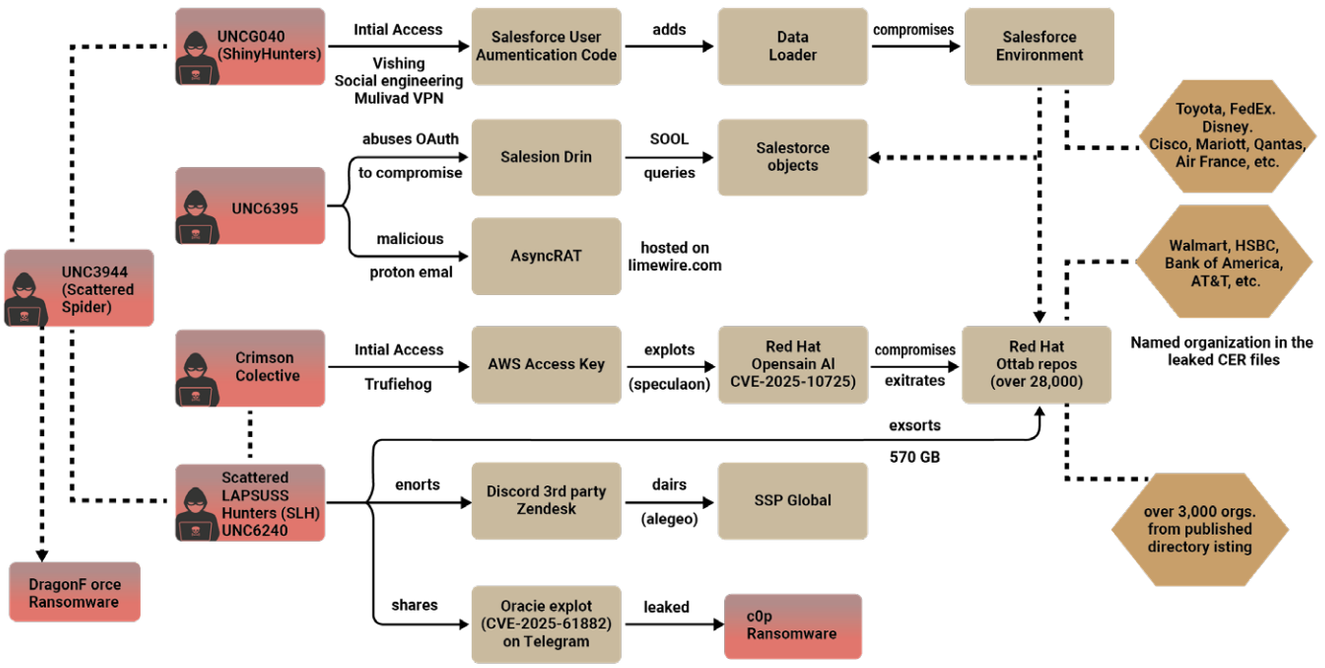
A Deep Dive into the Chain and Extent of the Compromise

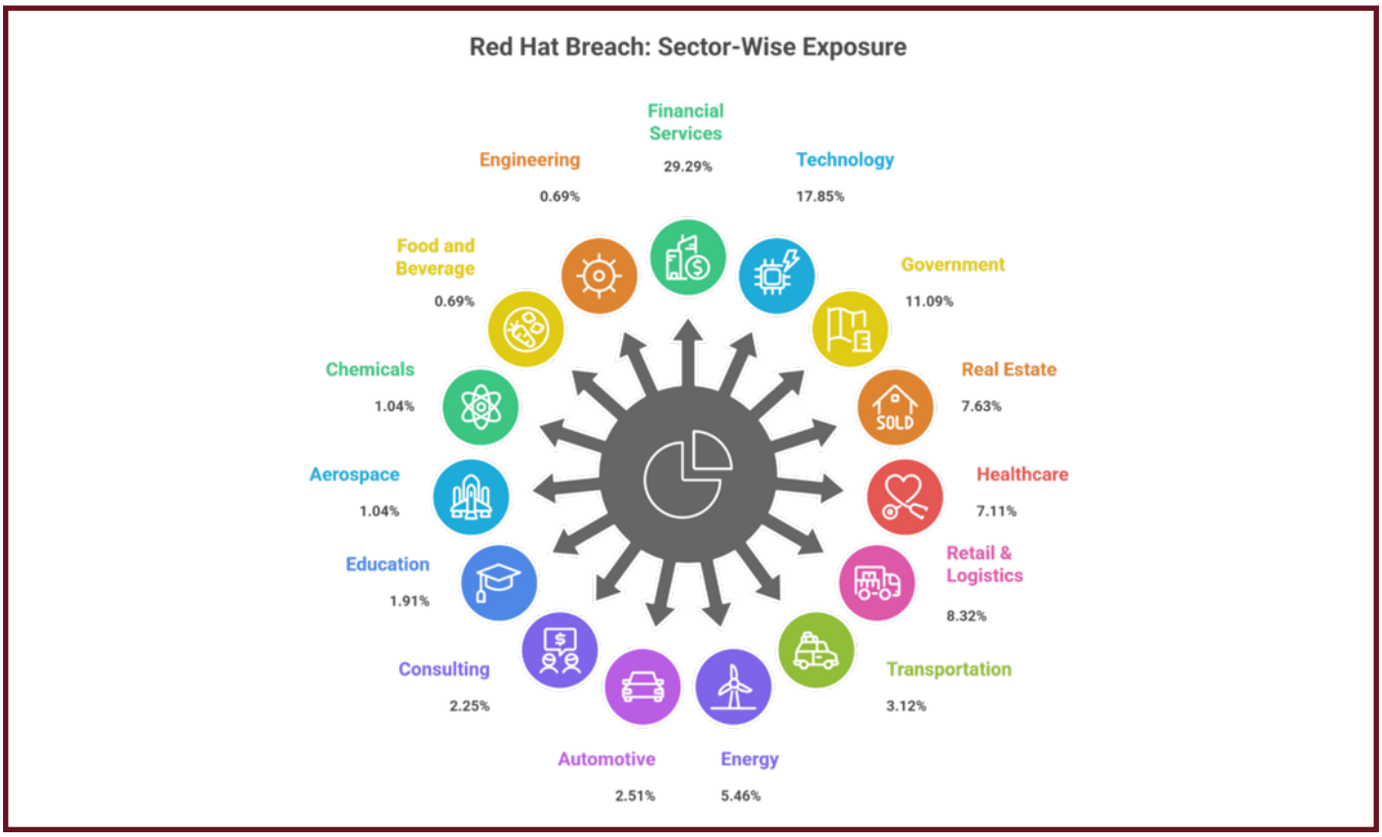
In June 2025, Google's internal Salesforce system was breached in a well-planned cyber-extortion campaign conducted by groups UNC6040 and UNC6240, linked to the ShinyHunters collective. Attackers impersonated Google IT staff in vishing attacks, tricking an employee into approving a malicious OAuth application.

The compromised access was then exploited using custom Python scripts mimicking Salesforce's DataLoader API to extract massive datasets including business contacts, emails, and phone numbers while masking their activity through Mullvad VPN and TOR.






UNCG040 (ShinyHunters)
Intial Access
Vishing
Social engineering
Mulivad VPN
Salesforce User Aumentication Code
adds
Data Loader
compromises
Salesforce Environment
Toyota, FedEx. Disney. Cisco, Mariott, Qantas, Air France, etc.
UNC6395
abuses OAuth
to compromise
Salesion Drin
SOOL
queries
Salestorce objects
malicious
proton emal
AsyncRAT
hosted on limewire.com
Walmart, HSBC, Bank of America, AT&T, etc.
UNC3944 (Scattered Spider)
Named organization in the leaked CER files
Crimson Colective
Intial Access
Trufiehog
AWS Access Key
explots
(speculaon)
Red Hat Opensain Al CVE-2025-10725)
compromises
exitrates
Red Hat Ottab repos (over 28,000)
exsorts
570 GB
Scattered LAPSUSS Hunters (SLH) UNC6240
enorts
Discord 3rd party Zendesk
dairs
(alegeo)
SSP Global
over 3,000 orgs. from published directory isting
DragonF orce Ransomware
shares
Oracie explot (CVE-2025-61882) on Telegram
leaked
c0p Ransomware


Red Hat Breach: Sector-Wise Exposure
Financial Services
29.29%
Technology
17.85%
Government
11.09%
Real Estate
7.63%
Healthcare
7.11%
Retail & Logistics
8.32%
Transportation
3.12%
Energy
5.46%
Automotive
2.51%
Consulting
2.25%
Education
1.91%
Aerospace
1.04%
Chemicals
1.04%
Food and Beverage
0.69%
Engineering
0.69%
SOLD

Subsequently, a related attack by UNC6395 exploited Salesloft Drift AI integrations, leveraging stolen OAuth tokens and SOQL queries to read Salesforce objects like user accounts and cases. The attackers sought AWS keys, Snowflake tokens, and sensitive credentials for lateral attacks or resale.

This campaign reveals the rising trend of OAuth abuse and voice-based social engineering.
Enterprises must enforce strict OAuth governance, monitor API activity, and strengthen zero-trust identity policies.

High

Education, IT, Financial Services

India

Unveiling Swan Vector APT

Targeting Taiwan and Japan with Varied DLL Implants

Swan Vector, a multi-stage APT campaign, targeted educational and mechanical engineering institutions across Taiwan and Japan in May 2025. The threat employed malicious RAR/ZIP packages with .LNK shortcuts, fake resumes, and payment-related lures.

The attack chain unfolded in four stages:

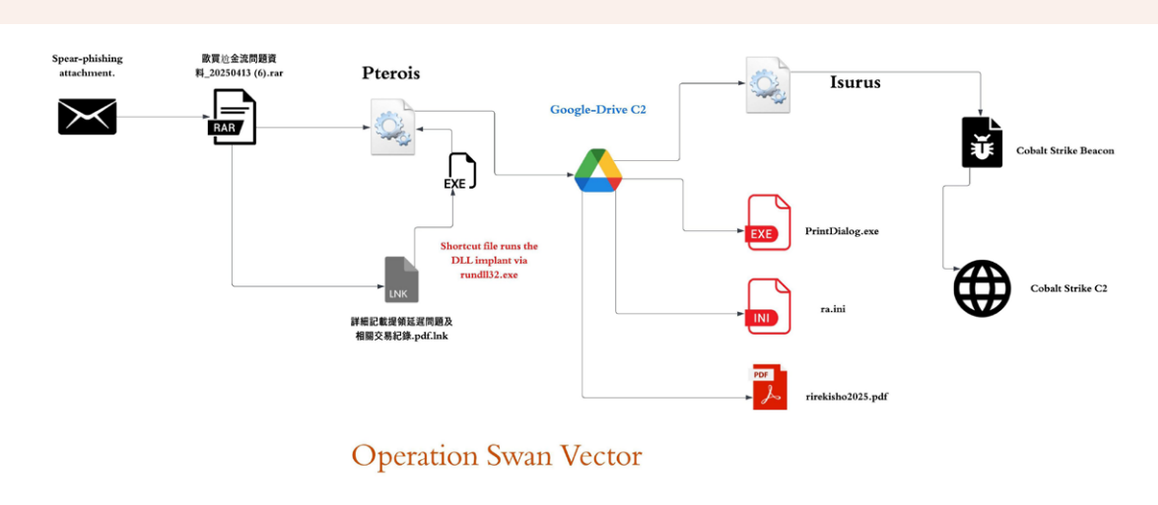
- LNK launches rundll32.exe to execute a malicious DLL (Pterois).
- Pterois resolves APIs via hashed lookups and abuses timer objects for stealth.
- A second DLL (Isurus) decrypts shellcode from configuration files using RC4 and executes it via syscall-based in-memory loading.
- A Cobalt Strike beacon establishes long-term remote control.
- These sophisticated techniques — DLL sideloading, Google Drive abuse, export-table hashing — show meticulous OPSEC and stealth.

Seqrite Labs Detection: Trojan.Pterois.S36007342, Trojan.49524.GC, Trojan.49518.GC

High

Education, Engineering

Taiwan, Japan



Operation Swan Vector

Goodbye HTA, Hello MSI

New TTPs and Clusters of an APT Driven by Multi-Platform Attacks

The SideCopy APT group, linked to Pakistan, has evolved its infection strategy — shifting from HTA-based to MSI (Microsoft Installer)-based attacks since December 2024.

The group expanded its focus to include Railways, Oil & Gas, External Affairs, and Defense Ministries.

New infection chains used malicious MSI installers and .pdf.lnk shortcuts, employing DLL sideloading, reflective loading, and open-source RATs like Xeno RAT, Spark RAT, and CurlBack.

One cluster targeted Linux systems with Go-based binaries, while others retained HTA-based delivery with encrypted resources.

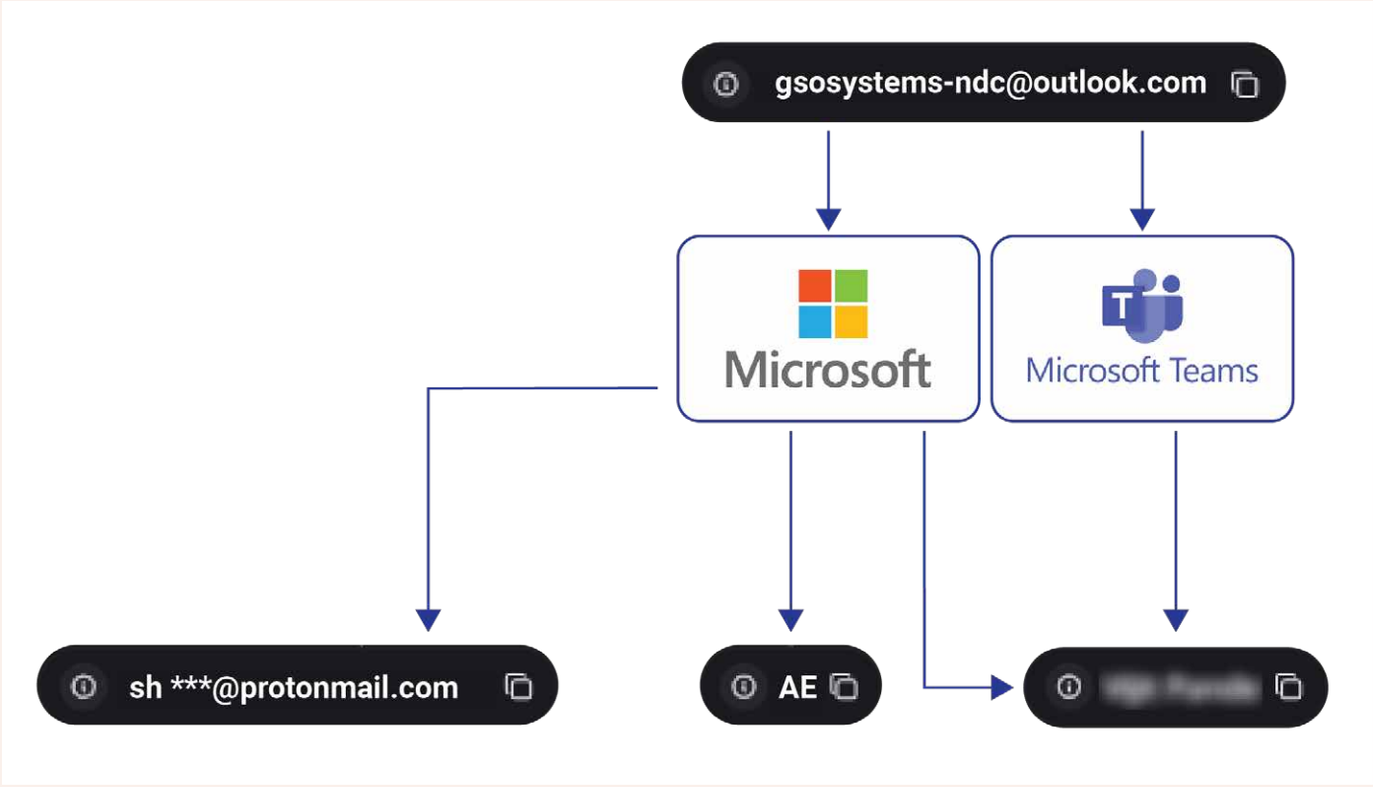
Attackers impersonated officials, cloned e-governance domains, and even compromised the National Hydrology Project's legitimate site to host payloads.

Seqrite Labs Detection: LNK.SideCopy.49245.Gen, HTA.SideCopy.49247.Gen

High

Defense, Railways, Oil & Gas, Education

India



Operation HollowQuill

Malware Delivered into Russian R&D Networks via Research Decoy PDFs

Operation HollowQuill targeted the Baltic State Technical University (BSTU) in Russia using malicious research invitation PDFs. The infection chain began with a .NET-based dropper deploying a Golang shellcode loader into the OneDrive process via APC injection, finally loading a Cobalt Strike beacon.

The dropper ensured persistence through Windows Startup shortcuts and evaded detection with anti-analysis checks.

Domains like phpsymfony[.]com were used for C2 communication, disguised with legitimate user agents.

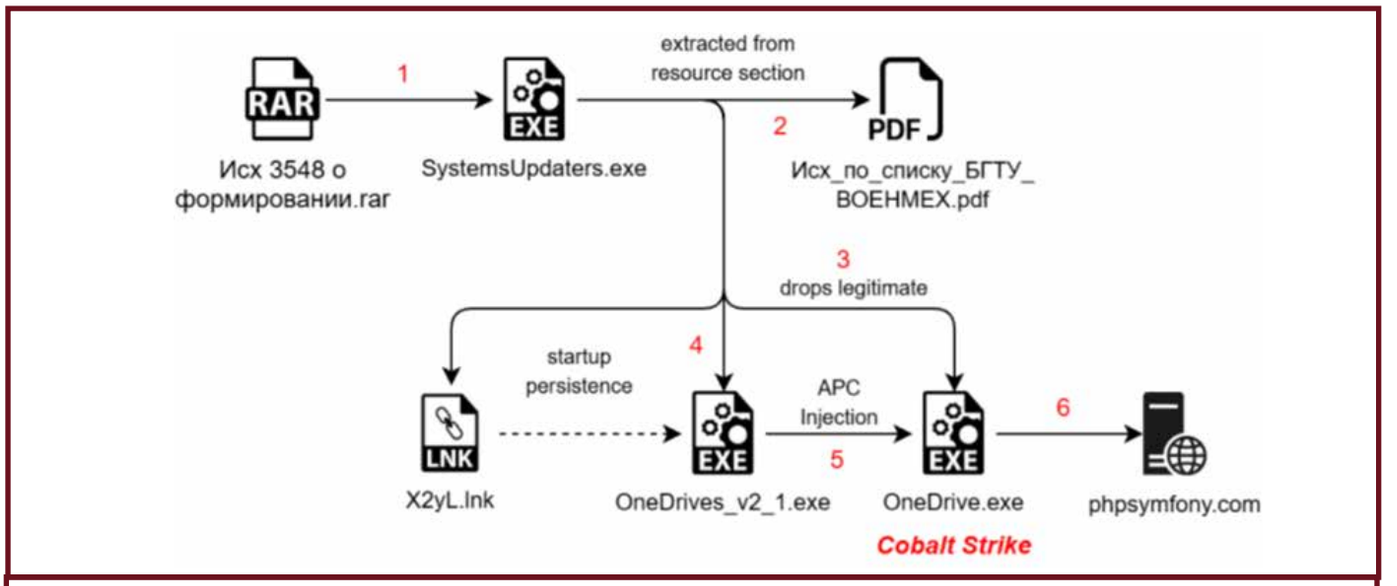
Analysts traced multiple payloads through Go build IDs, uncovering shared infrastructure with AsyncRAT campaigns pointing to a persistent, well-funded actor targeting strategic research institutions.

Seqrite Labs Detection: Trojan.Ghanarava

Medium

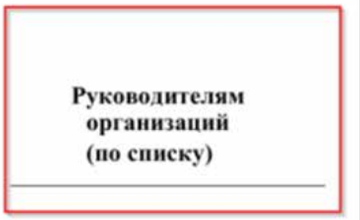
R & D, Education

Russia



МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова»
(БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова)

Санкт-Петербург, 190005, 1-я Красноармейская ул., д. 1
Тел.: (812) 316-2394, Факс: (812) 490-0591
E-mail: komdep@bstu.spb.su. www.voenmeh.ru
ИНН 7809003047
16.12.2024 № 3/548



Руководителям организаций
(по списку)

Weaxor

Rebranded Mallox Ransomware with a Unique Payload Delivery Method

Weaxor, a rebranded Mallox ransomware, specifically targets Microsoft SQL (MSSQL) servers. Attackers exploit weak credentials to run hidden PowerShell commands via sqlps.exe, which downloads two heavily obfuscated payloads encoded in Base64 and XOR.

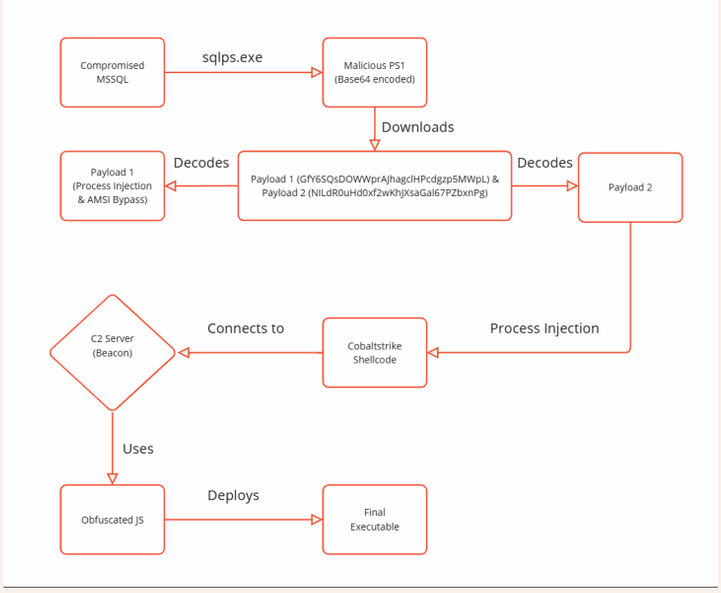
The attack includes AMSI bypass, process injection, and Cobalt Strike beacon deployment. Once the beacon connects to its C2 servers, the final ransomware payload encrypts files, appending the .rox extension and demanding ransom through TOR links.

Seqrite Labs Detection: Weaxor.Ransomware.49258.GC

High

Technology, Financial Institutions

India, China



Unmasking GrassCall Campaign

The Hackers Behind Job Recruitment Cyber Scams

The GrassCall campaign exploited global job seekers by posing as recruiters for crypto and Web3 roles. Victims were contacted on job boards, redirected to Telegram, and asked to download “video interview” software like VibeCall.exe, which installed the Rhadamanthys stealer on Windows or AMOS Stealer on macOS.

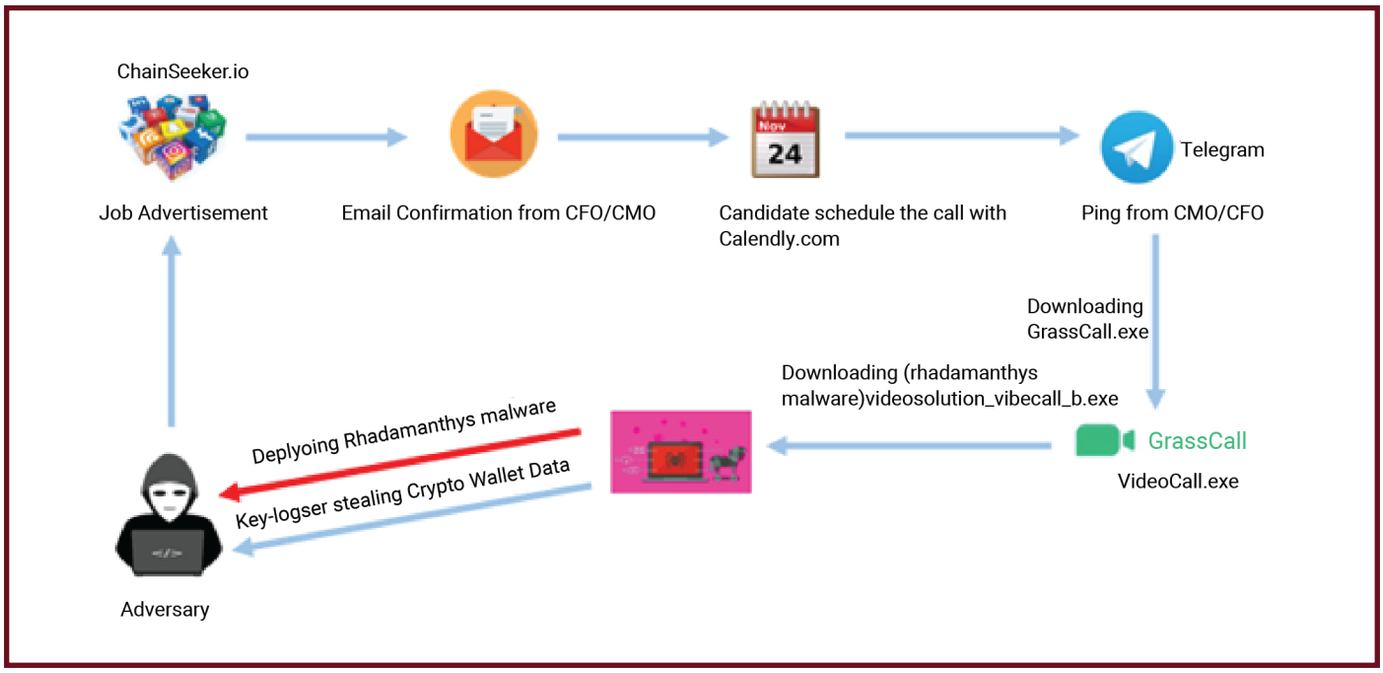
The malware exfiltrated credentials, cryptocurrency wallets, and browser data. GrassCall exemplifies the social engineering evolution blending fake corporate infrastructure, realistic UX design, and cross-platform trojans.

Seqrite Labs Detection: Trojan.GrassCallCiR, Trojan.Rhadamanth

High

Job Seekers

Global



SnakeKeylogger

A Multistage Info Stealer Malware Campaign

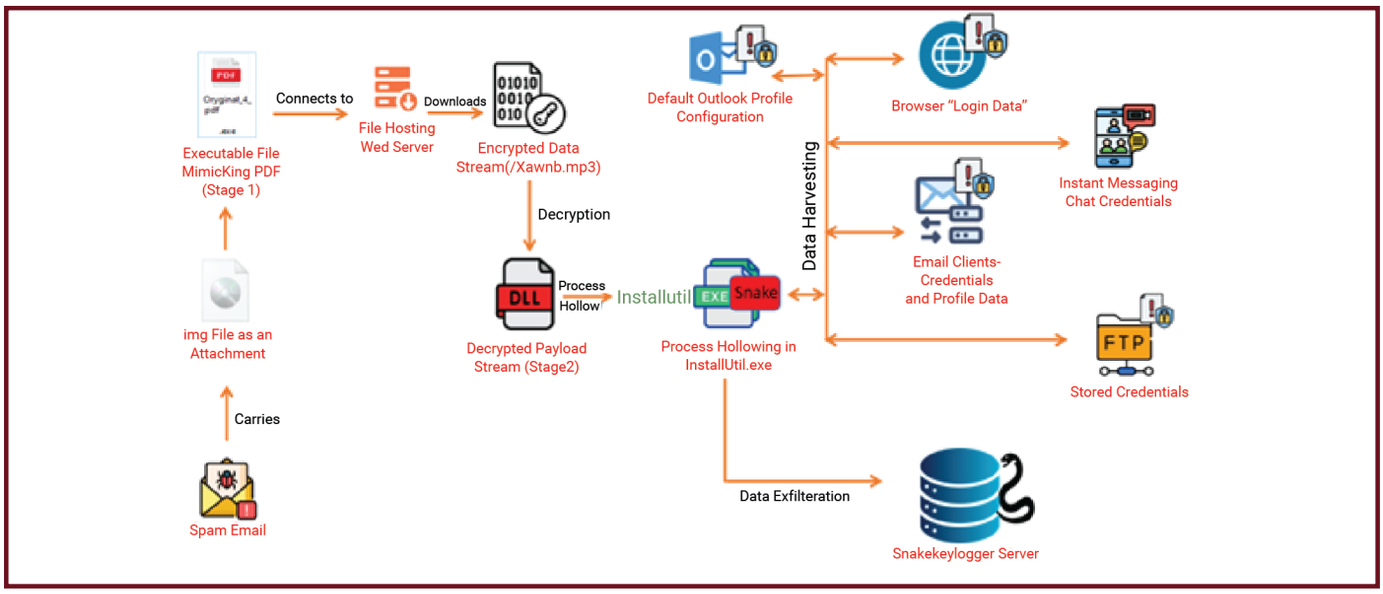
Seqrite identified a multi-stage SnakeKeylogger campaign spreading via .img attachments. Once opened, an executable masquerading as a PDF downloaded obfuscated payloads from an Apache server, decrypted in-memory to bypass AV detection.

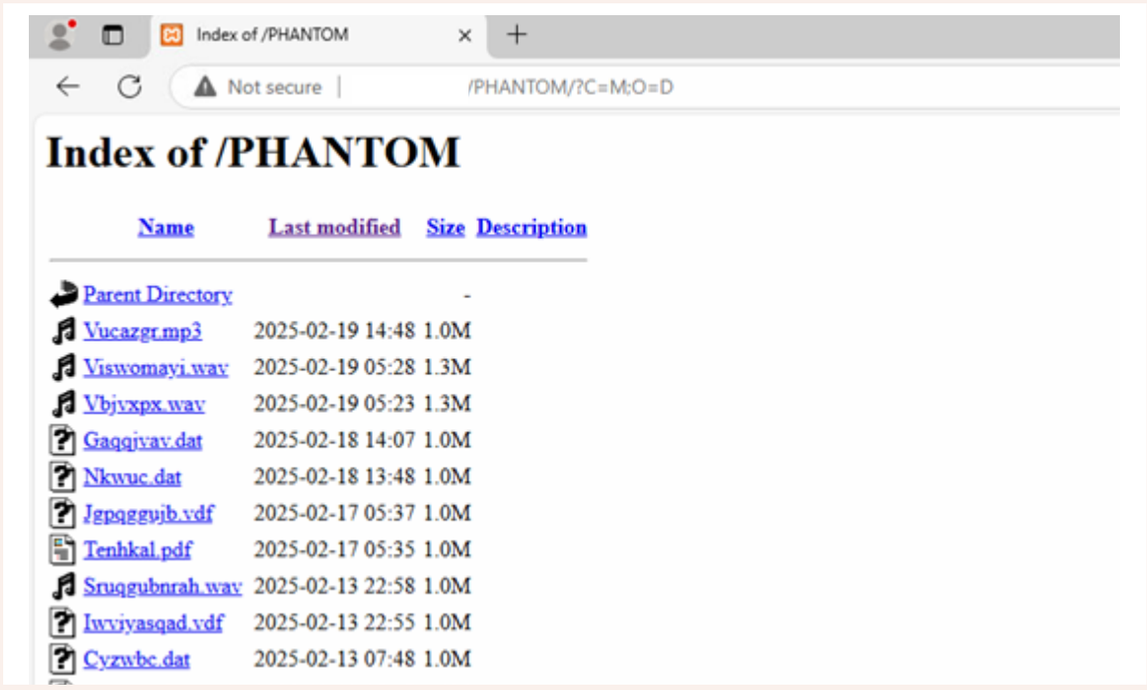
The second-stage payload used InstallUtil.exe process hollowing, executing SnakeKeylogger to harvest credentials, FTP logins, and Wi-Fi details. The malware's in-memory decryption, delegate injection, and rotating payload directories indicate Malware-as-a-Service distribution.

Seqrite Labs Detection: Downldr.Snakeloggr.S35164149

High

Windows Users





Exposed SMB

The Hidden Risk Behind 'WantToCry' Ransomware Attacks

The WantToCry ransomware exploits misconfigured SMB services, brute-forcing credentials to remotely encrypt drives and NAS devices.

Files are appended with .want_to_cry, and ransom notes direct victims to Telegram and Tox channels.
Because encryption occurs remotely without leaving local traces, traditional AVs often fail to detect early stages. Organisations must harden SMB/FTP/RPC configurations, disable public access, and monitor for brute-force anomalies.
Seqrite Labs Detection: HEUR:Trojan.Win32.EncrSD

High
Global

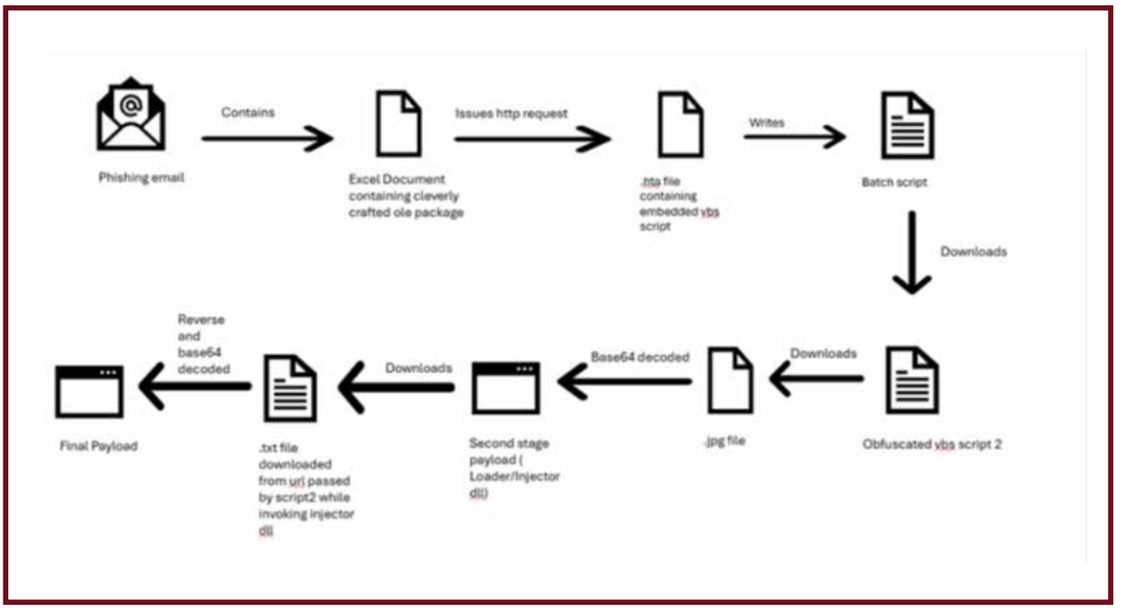
New Steganographic Campaign

Distributing Multiple Malware

The StegoCampaign (SteganoAmor) resurfaced in 2025, distributing Remcos, AsyncRAT, VIPKeylogger, Xworm, and AgentTesla.

Malspam emails delivered benign-looking .jpg files embedding final payloads through steganography, effectively bypassing content filters.
Seqrite Labs Detection: Backdoor.Remcos, Trojan.LoaderCiR

High
Global



Demystifying PKT and Monero Cryptocurrency

Deployed on MSSQL Servers

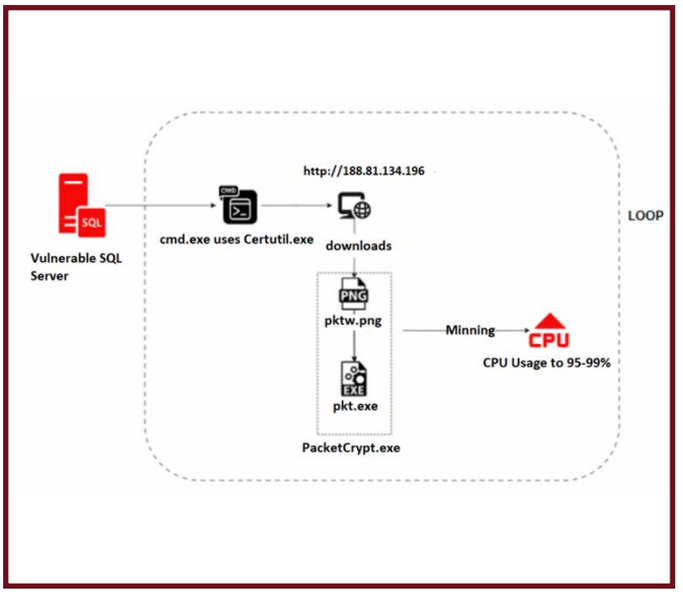
Seqrite discovered PKT Classic and Monero mining operations hijacking SQL servers via certutil-based payload downloads. Attackers deployed PacketCrypt mining tools through Base64 PowerShell commands and Themida-packed binaries.

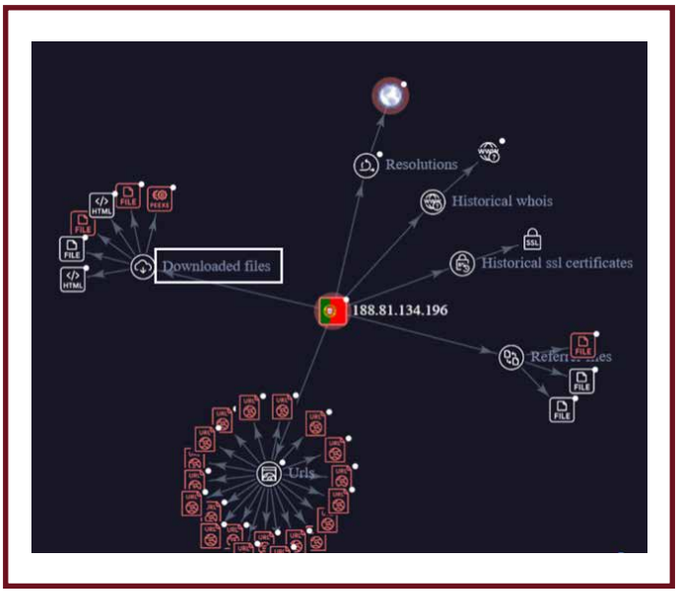
The campaign illustrated creative abuse of server resources for covert crypto-mining and bandwidth theft.

Seqrite Labs Detection: Trojan.Alevaul

High

India





Threat Actors Targeting US Tax-Session

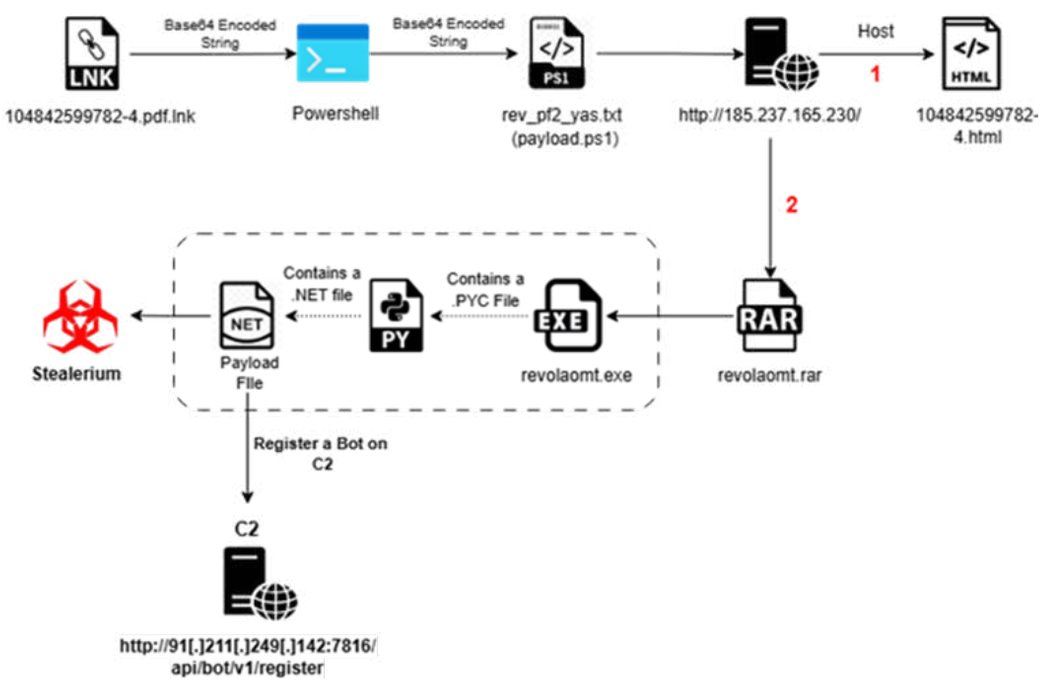
with Stealerium Infostealer

Phishing campaigns during the U.S. tax season distributed LNK-based payloads disguised as IRS forms. The attack involved nested Base64 PowerShell commands downloading a PyInstaller executable that dropped Stealerium v1.0.35, exfiltrating credentials and browser data.

Seqrite Labs Detection: Trojan.Win32.PH

Low

United States



Unveiling Silent Lynx APT

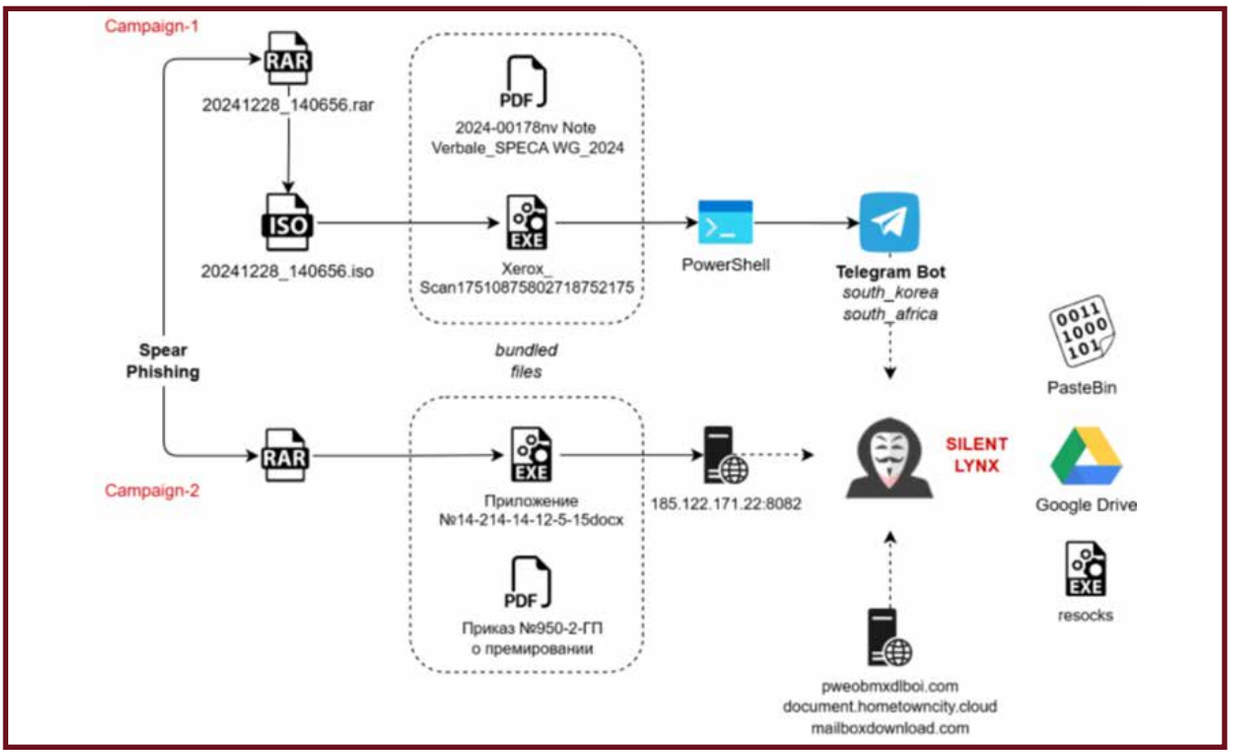
Targeting Entities Across Kyrgyzstan

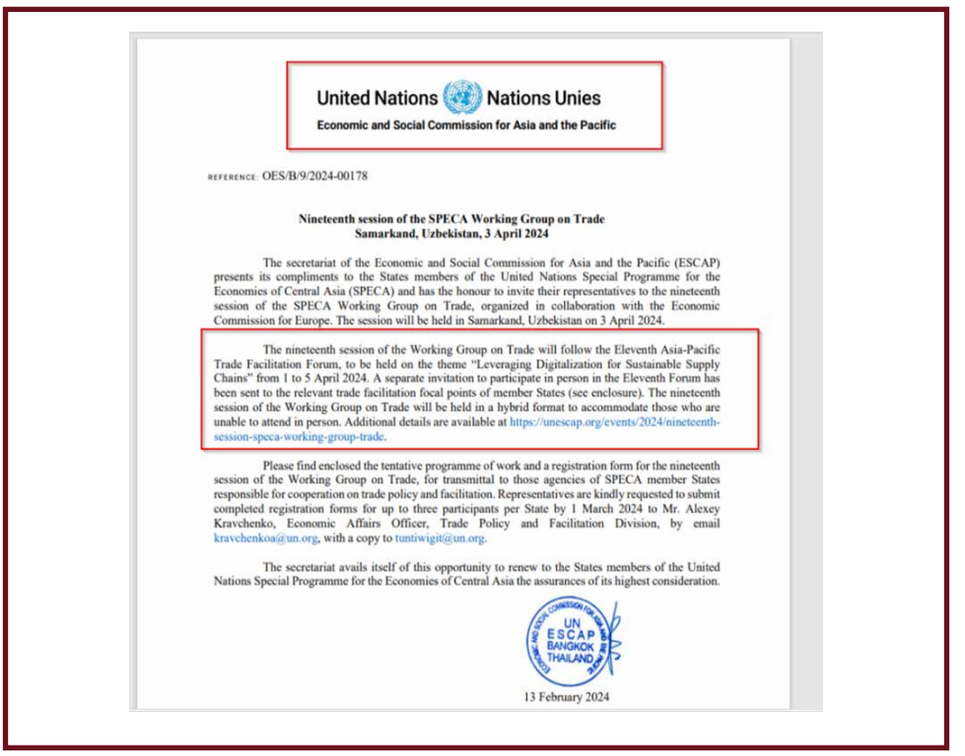
The Silent Lynx APT targeted Kyrgyzstan's National Bank and Ministry of Finance using RAR attachments with C++ loaders and Golang reverse shells. The campaigns used Telegram bots for C2, and Google Drive for payload delivery. Attribution suggests overlap with YoroTrooper operations from Kazakhstan.

Seqrite Labs Detection: Trojan.SLynx

Medium

Kyrgyzstan





United Nations Nations Unies

Economic and Social Commission for Asia and the Pacific

REFERENCE: OES/B/9/2024-00178

Nineteenth session of the SPECA Working Group on Trade
Samarkand, Uzbekistan, 3 April 2024

The secretariat of the Economic and Social Commission for Asia and the Pacific (ESCAP) presents its compliments to the States members of the United Nations Special Programme for the Economies of Central Asia (SPECA) and has the honour to invite their representatives to the nineteenth session of the SPECA Working Group on Trade, organized in collaboration with the Economic Commission for Europe. The session will be held in Samarkand, Uzbekistan on 3 April 2024.

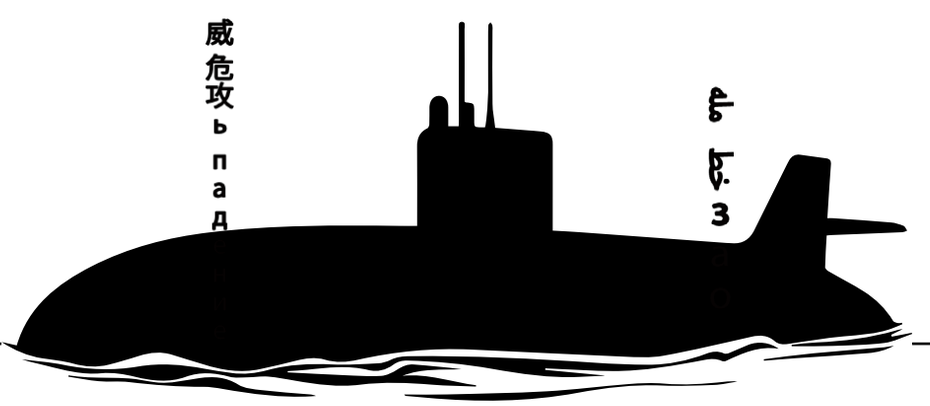
The nineteenth session of the Working Group on Trade will follow the Eleventh Asia-Pacific Trade Facilitation Forum, to be held on the theme "Leveraging Digitalization for Sustainable Supply Chains" from 1 to 5 April 2024. A separate invitation to participate in person in the Eleventh Forum has been sent to the relevant trade facilitation focal points of member States (see enclosure). The nineteenth session of the Working Group on Trade will be held in a hybrid format to accommodate those who are unable to attend in person. Additional details are available at https://unescap.org/events/2024/nineteenth-session-speca-working-group-trade.

Please find enclosed the tentative programme of work and a registration form for the nineteenth session of the Working Group on Trade, for transmittal to those agencies of SPECA member States responsible for cooperation on trade policy and facilitation. Representatives are kindly requested to submit completed registration forms for up to three participants per State by 1 March 2024 to Mr. Alexey Kravchenko, Economic Affairs Officer, Trade Policy and Facilitation Division, by email kravchenkoa@un.org, with a copy to tuntiwigit@un.org.

The secretariat avails itself of this opportunity to renew to the States members of the United Nations Special Programme for the Economies of Central Asia the assurances of its highest consideration.

UN ESCAP BANGKOK THAILAND

13 February 2024



Unmasking the SVG Threat

How Hackers Use Vector Graphics for Phishing Attacks

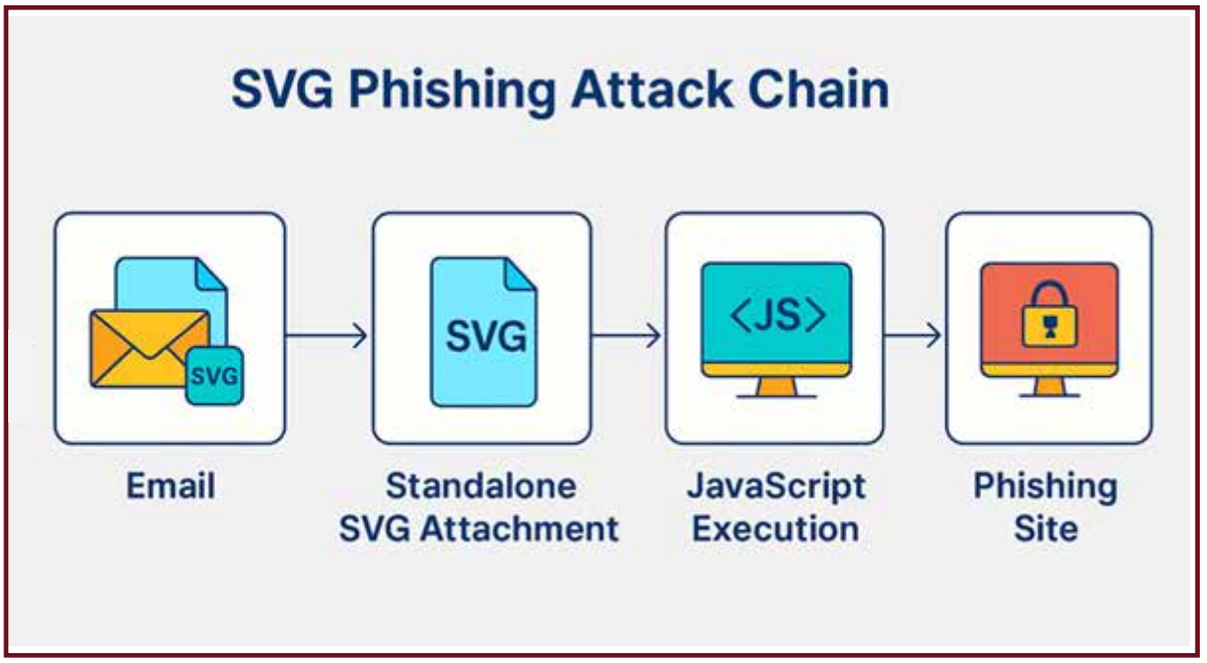
Attackers weaponized SVG files to deliver phishing redirects using embedded JavaScript. When opened in browsers, SVGs silently executed scripts that redirected users to fake Office 365 credential pages.

Seqrite Labs Detection: Xml.Trojan.49854.GC

Medium

BFSI, Healthcare, Telecom

India, EU, United States



False GPS Signals

Disrupt Aircraft Navigation in India

Multiple flights reported sudden GPS inconsistencies caused by spoofed GNSS signals during landing approaches. Authorities are investigating unidentified external sources. Spoofing is far more dangerous than jamming because it feeds credible but false navigation data, risking incorrect positioning, approach deviation, and reduced situational awareness.

High

Aviation

India

Fake CAPTCHA Lures Victims

Lumma Stealer Abuses Clipboard and PowerShell

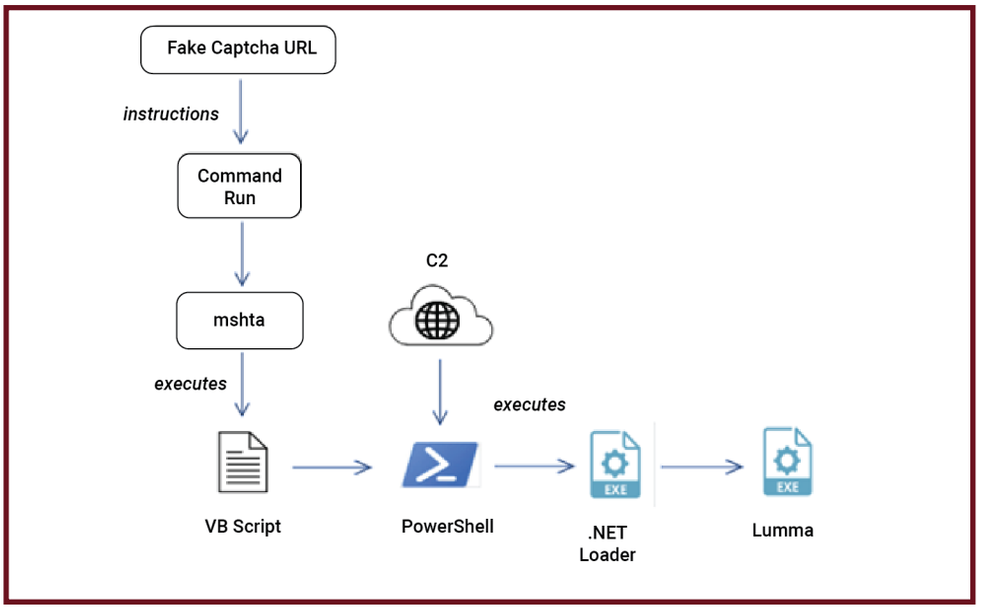
Attackers deployed fake Cloudflare CAPTCHA pages that tricked users into pasting malicious commands copied to their clipboard.

The payload downloaded Lumma Stealer, which harvested clipboard contents, screenshots, and credentials while using hash-based API resolution and anti-sandbox checks.

Seqrite Labs Detection: Trojan.LummaStealerCiR

High

Global



Plague

A Silent PAM-Based Backdoor Threatening Linux Authentication Layers

Plague is a stealthy Linux backdoor that embeds directly into the Pluggable Authentication Module (PAM) stack to bypass login security and grant persistent attacker access. Unlike traditional Linux malware, it integrates within trusted authentication routines, enabling invisible privilege escalation without relying on external binaries or network callbacks. The backdoor uses static passwords, multi-layered obfuscation, and anti-sandbox logic to evade detection, while sanitizing session traces and redirecting logs to /dev/null. Its advanced design allows it to survive system updates, remain undetected in forensic scans, and persist long-term in enterprise and cloud environments.

Medium

Linux-based systems, Enterprise servers, Cloud infrastructure

Global

ZuRu Malware

Weaponizing macOS Developer Tools for Stealthy Persistence

The ZuRu malware resurfaced in 2025, targeting macOS users through a tampered version of the legitimate Termius SSH client. The compromised app embeds malicious code in its helper process, allowing it to run silently while appearing legitimate. Once executed, it downloads a Khepri RAT variant as a second-stage payload, enabling full remote control, file theft, and command execution. ZuRu maintains persistence via LaunchDaemon tasks, disguises network communication as DNS traffic, and uses a custom signature to evade macOS security checks. Its abuse of trusted developer tools underscores a growing threat to developer ecosystems and unmanaged macOS environments.

High

Apple and Mac OS

Global

XCSSET Malware

Targeting Apple Developers

XCSSET is a macOS-specific malware that infects Xcode development environments to spread malicious payloads. By injecting code into project build phases, it ensures execution whenever a developer compiles code. The malware steals browser data, credentials, and session tokens, and disables macOS security updates to maintain persistence. Using modified tools like HackBrowserData and persistence via LaunchDaemons and Git repositories, XCSSET remains hidden across shared developer projects. It poses significant risk to software supply chains, especially where Xcode projects are reused or distributed among teams.

Medium

Apple and Mac OS

Global

Masslogger Fileless Variant

Spreads via .VBE, Hides in Registry

Seqrite Labs identified a fileless variant of Masslogger, a credential-stealing malware that operates entirely from Windows Registry without writing files to disk. Delivered via phishing emails containing .VBE scripts, it loads multiple encoded stages into memory using PowerShell SendKeys automation. The final payload injects into legitimate processes like AddInProcess32.exe to steal browser credentials, email logins, clipboard data, and screenshots. With geo-targeted variants and multi-channel exfiltration through FTP, SMTP, and Telegram, this variant exemplifies modern fileless persistence and anti-forensic evasion.

Medium

Enterprise Windows Users

Global

Exploit Targeting SAP NetWeaver Development Server

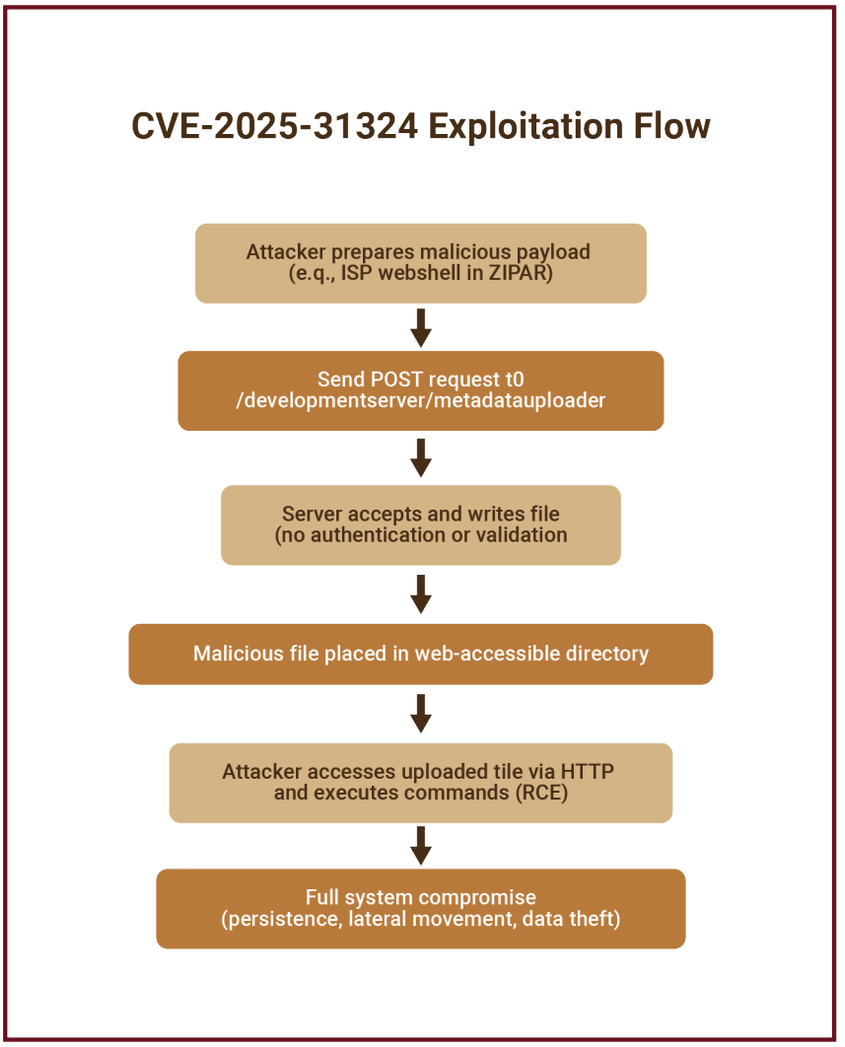
Mass RCE Attacks (CVE-2025-31324)

A critical remote code execution (RCE) flaw in SAP NetWeaver Development Server is being weaponized globally. Attackers exploit the insecure metadata uploader endpoint to upload malicious ZIP/JAR files, gaining persistent access and deploying JSP web shells. Since mid-2025, groups like LAPSUS$ Hunters and ShinyHunters have automated the exploit, leading to mass compromises across manufacturing, telecom, and retail sectors. In many cases, attackers dropped the Auto-Color Linux backdoor, enabling lateral movement and data exfiltration from ERP systems. Over 1,200 SAP servers are confirmed exposed, highlighting a widespread enterprise-level threat to mission-critical infrastructure.

High

SAP ERP Environment

Global



Zero-Click AI Theft

"EchoLeak" Exploits Microsoft 365 Copilot for Data Exfiltration

The EchoLeak exploit (CVE-2025-32711) demonstrates how attackers can abuse AI assistants like Microsoft 365 Copilot to perform zero-click data theft. By embedding prompt injection payloads in emails, adversaries trigger Copilot to autonomously send sensitive data — such as emails, documents, and tokens — to attacker-controlled servers. This occurs without any user interaction, making detection nearly impossible. The exploit manipulates Copilot's trusted access to Outlook, OneDrive, and Teams, turning an AI assistant into an unintentional data exfiltration agent. EchoLeak marks the first recorded zero-click attack on an enterprise AI platform, exposing a critical new vector in AI-driven security ecosystems.

High

Enterprise Microsoft 365 Copilot Users

Global

Clickfix HijackLoader Campaign

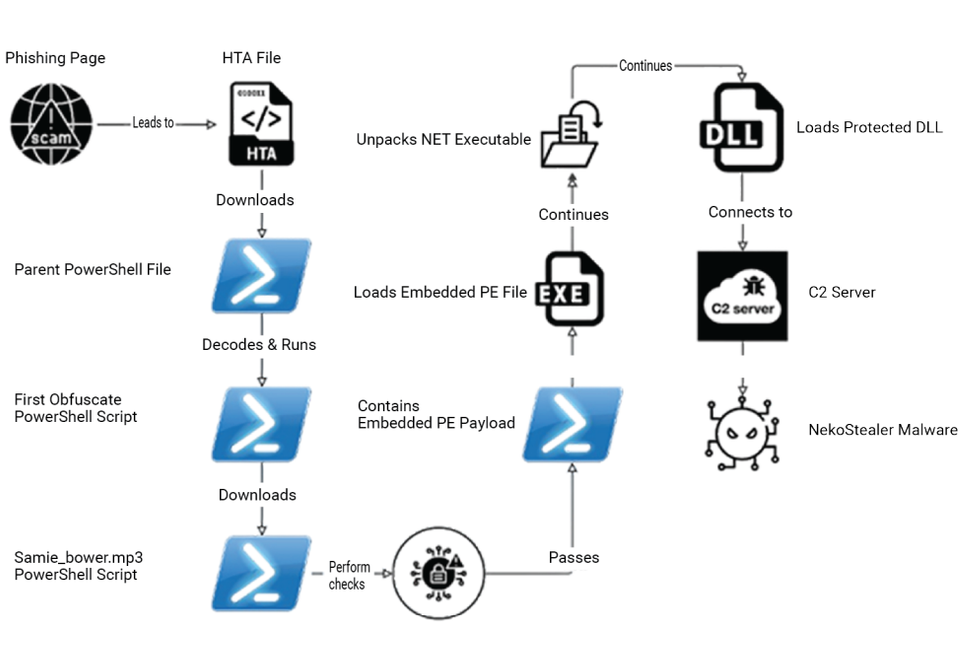
Phishing-Fueled Malware-as-a-Service Expansion

The Clickfix HijackLoader campaign illustrates the evolution of loader-based attacks in the cybercrime ecosystem. Distributed via malicious .msi installers on fake download sites and malvertising networks, it delivers HijackLoader, a modular loader capable of injecting payloads like DeerStealer. Used in financially motivated campaigns, HijackLoader is often part of Malware-as-a-Service ecosystems, where actors like TAG-150 and CastleLoader collaborate to deliver credential stealers and remote access tools. Its multi-stage execution and integration with external loaders highlight the growing commercialization and efficiency of malware delivery networks.

High

Financial Institutions

Europe, Middle East



Operation CargoTalon

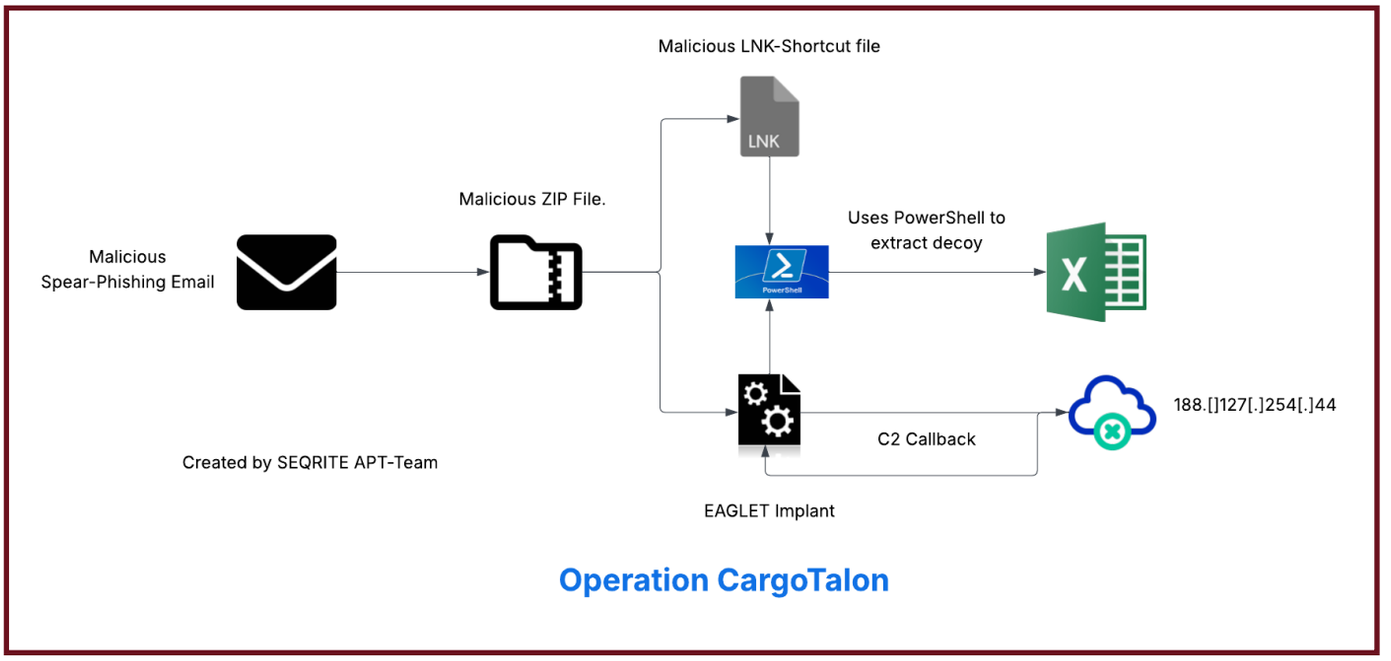
UNG0901 Targets Russian Aerospace & Defense

Operation CargoTalon (UNG0901) is a spear-phishing campaign aimed at the Russian aerospace and defense sector, using logistics-themed lures to deliver the EAGLET implant. The infection chain (Emai/ LNK/DLL/decoy XLS) relies on LOLBIN execution to deploy the implant while presenting a benign document. EAGLET acts as a lightweight HTTP C2 backdoor, capable of executing commands, downloading additional payloads, and exfiltrating files. Infrastructure overlaps link the campaign loosely to previously known threat clusters, suggesting an ongoing espionage operation targeting sensitive defense data.

Medium

Aerospace and Defense

Russia



WinRAR Vulnerabilities

Directory Traversal & NTFS ADS (CVE-2025-6218 & CVE-2025-8088)

Two severe flaws in WinRAR for Windows — CVE-2025-6218 and CVE-2025-8088 allow attackers to write malicious files outside extraction directories, enabling RCE and stealthy persistence. Threat actors including RomCom and Paper Werewolf (GOFFEE) have exploited these vulnerabilities in phishing campaigns. CVE-2025-6218 abuses directory traversal, while CVE-2025-8088 hides payloads in NTFS Alternate Data Streams, making them invisible to users. Exploitation enables auto-execution on login or side-loading by other processes, posing long-term risks to enterprise networks and individual users alike.

Medium

Enterprise Windows Users

Global

Political

Rising geopolitical tension with regional adversaries (notably China and Pakistan) has expanded the cyber espionage and disinformation threat vector.

State-aligned APT campaigns (e.g., TAG-38, SideWinder, Mustang Panda variants) are increasingly targeting Indian government, defense, and BFSI institutions to exfiltrate sensitive data.

India's growing cyber-sovereignty posture (National Cyber Security Strategy and Digital India initiative) pushes for indigenous cyber defense capabilities but also increases its visibility as a target.

CERT-In and NCIIPC mandates (6-hour breach reporting rule) reflect proactive regulatory oversight but have created compliance strain for private-sector entities.

STRATEGIC IMPLICATION

Cyber incidents may escalate into statecraft or economic coercion instruments, necessitating public–private threat intelligence sharing and attribution capabilities.

Economic

India's $4 trillion economy, driven by rapid digitization of BFSI, e-commerce, and fintech, has become highly data-dependent, expanding the attack surface.

Surge in ransomware and financial fraud especially targeting UPI, NEFT, and RTGS channels impacts both consumer trust and macroeconomic stability.

Cybercrime-as-a-Service (CaaS) models have lowered the entry barrier for financial threat actors, particularly in Tier-2 and Tier-3 cities.

Economic sanctions and supply chain decoupling have increased dependency on indigenous cybersecurity vendors and SOC outsourcing, creating uneven defense maturity.

STRATEGIC IMPLICATION

Financial and reputational losses from cybercrime could exceed ₹15,000 crore annually, threatening investor confidence in India's digital economy and fintech sector.

PEST
Anal

India Cyber Threat L

Social

Over 900 million internet users and instant payment adoption have made citizens both digital participants and potential attack vectors.

Low cyber hygiene awareness among rural and small-business populations fuels phishing, QR code scams, and fraudulent loan app incidents.

Growing public concern about data misuse (post-DPDPA) is increasing demand for privacy accountability in both private and public digital systems.

Cybercrime victimization narratives on social media accelerate misinformation and loss of institutional trust in banks and digital services.

STRATEGIC IMPLICATION

Cyber defense must include behavioral interventions such as public awareness, digital literacy, and financial fraud education alongside technical controls.

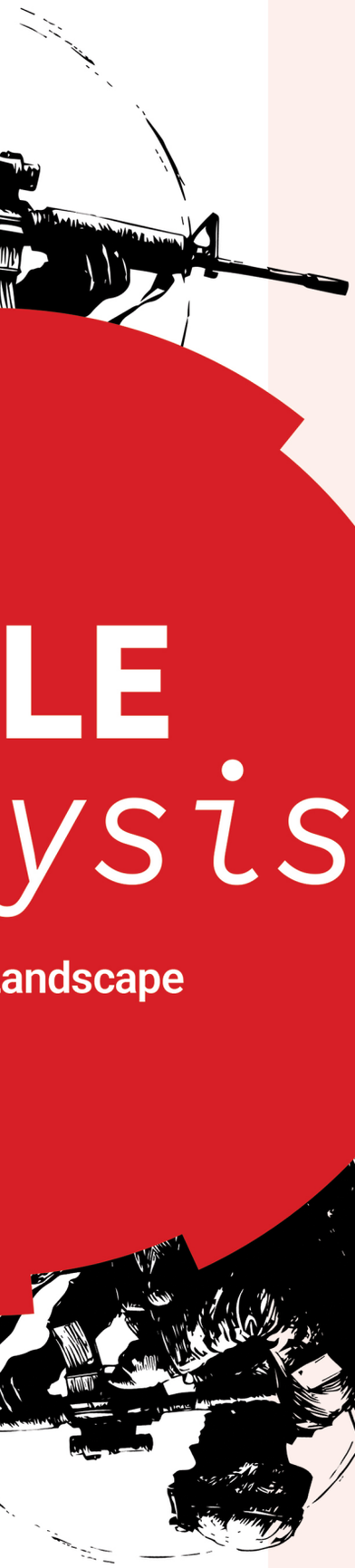
EXECUTIVE TAKEAWAYS

India's cyber landscape is shifting from reactive defense to regulatory-driven resilience.

BFSI, government, and telecom remain the core attack surfaces their compromise could cascade into systemic economic risk.

Future resilience depends on three pillars:

- National threat intelligence fusion (public–private sharing)
- Data sovereignty and compliance automation
- Resilient digital trust frameworks (AI-secure identity, Zero Trust, and privacy engineering).



LE
ysis
andscape

Technological

Expansion of cloud-first infrastructure, API-driven fintech ecosystems, and AI-powered digital banking introduces both agility and systemic exposure.

Increased use of AI/LLMs in phishing, fake KYC, and synthetic identity generation complicates detection.

Persistent legacy systems in public sector banks and cooperative institutions create patching and segmentation challenges.

Growth in IoT/OT convergence (ATM, insurance kiosks, smart branches) introduces lateral movement risks.

Adoption of Zero Trust and EDR/XDR technologies is accelerating, but small institutions lag in implementation.

STRATEGIC IMPLICATION
Technology modernization without secure architecture design amplifies risk; the focus should shift from perimeter defense to identity-centric resilience.

Legal, regulatory

The Digital Personal Data Protection Act (DPDPA 2023) establishes stringent obligations for breach reporting, data minimization, and consent management.

RBI IT Governance and Outsourcing Guidelines (2023) enforce strict third-party security controls for BFSI entities.

CERT-In 2022 directive mandates incident reporting within six hours, forcing tighter detection and response frameworks.

Emerging Digital India Act (DIA) aims to consolidate cybercrime prosecution, platform accountability, and AI regulation.

Enforcement maturity remains uneven across states and sectors; SMEs struggle to meet compliance without automation support.

STRATEGIC IMPLICATION
Legal risk is now operational risk. Non-compliance may trigger financial penalties and reputational damage equivalent to major data breaches.

Environmental

Rising climate-linked disruptions (heatwaves, floods) are impacting data center availability and disaster recovery readiness.

Push toward green data centers and sustainable IT operations creates new dependencies on distributed energy and IoT sensors—potential attack surfaces.

Hybrid work models and cloud service relocation during environmental events have led to ad hoc network exposures.

STRATEGIC IMPLICATION
Cyber resilience planning must integrate climate resilience ensuring critical financial infrastructure remains operational during physical or cyber disruptions.

SEQRITE

/{ industry **cybersecurity preparedness** survey };

KEY FINDINGS ACROSS CYBERSECURITY DOMAINS

Cyber Hygiene

Organisations continue strengthening their security culture, but gaps remain in foundational practices.

52.5% have higher maturity in defining and practicing cyber hygiene practices

13.3% of the participating organisations have yet to implement cyber hygiene practices

74% invest in cybersecurity culture through training and awareness

65% have defined and implemented security processes

Securing Assets

Asset visibility and lifecycle management remain a mixed issue.

75.7% have higher maturity in asset (hardware/ software/data, etc) protection

80.1% maintain an updated Configuration Management Database (CMDB)

39.8% still operate End-of-Life (EOL/EOS) systems

81.2% securely handle data during asset disposal

11.6% have no mechanism to secure assets

Data Security

Organisations have strengthened their data protection measures but still face challenges in managing the sensitive data lifecycle.

7.2% of the participants don't have any controls in protecting data

74.6% have their data classified

75.7% have data leakage controls

64.1% have secure data wipe processes

Malware Protection

The adoption of advanced malware defenses is high, although a small portion still relies on basic protection.

62% of the participants don't have any controls in protecting data

4.90% rely only on basic protection

86.7% use advanced malware protection technologies

Access Control

Identity and access governance continues to mature steadily.

47.5% have a proper access control mechanism for managing identity and ensuring only authorised access to the data

79.6% have defined workflows for access provisioning and revocation

75.7% follow best practices for credentials and password policies

Secure Configuration

Configuration hardening remains one of the weakest domains.

6.6% have not implemented any policies to protect their assets

47.5% enforce secure configurations based on best practices

Software Updates & Patch Management

Patch discipline varies significantly across organisations.

64.1% have implemented a patch management process

1.7% focus only on critical & essential updates

69.6% prioritize patches irrespective of severity

7.2% have no defined patch management process

Backup & Recovery

Backup hygiene shows strong adoption, but a small number remain unprepared.

78.5% have defined and implemented a backup strategy

2.8% securely handle data during asset disposal

83.4% restrict unauthorised access to backups

80.7% store backups offline

Incident Response

IR maturity reveals significant gaps in readiness and execution.

72.4% have a defined incident response process to detect & respond to threats

27.6% lack an incident management process

79.6% have employee awareness on IR

Security Process Management

Process effectiveness is inconsistent across organisations.

11% don't test their security processes

67.4% test processes regularly

39.2% never revisited processes after introduction

36.5% have defined processes but never tested

34.8% have partially defined and untested processes

Threat Exposure & Attack Patterns

A significant proportion of organisations reported facing attacks; social engineering remains the top attack vector.

56.9%
of participated organisations were unsure whether they had experienced a cyberattack

16.6%
reported experiencing a cyberattack at some point in the past 12 months

8.8%
reported facing multiple cyberattacks, occurring weekly or monthly

1.1%
experienced cyber-attacks very often

Most observed threat types

- **Social engineering (phishing/vishing/ smishing) – highest**
- **Malware attacks**
- **Web application attacks**
- **10% attributed to ransomware**
- **~6% linked to AI/ML-based attacks**
- **~5% supply chain attacks**
- **Spoofing attacks remain concerning**

Cyber Resiliency

Organisations demonstrate varying levels of resilience in the aftermath of an attack.

50.8%
reported no impact despite being targeted

9.4%
faced business disruption

7.7%
suffered data loss

5.5%
faced financial loss

3.8% suffered regulatory implications

Top 5 Challenges in Cybersecurity Adoption (2026)

Lack of knowledge/ experience	Lack of manpower/ skilled resources	Budget constraints	Lack of senior management support	Low priority within the organisation

Threat Intelligence Adoption

41.4% **of participated organisations consume threat intelligence (OSINT, commercial, or both) to support proactive cyber defense.**

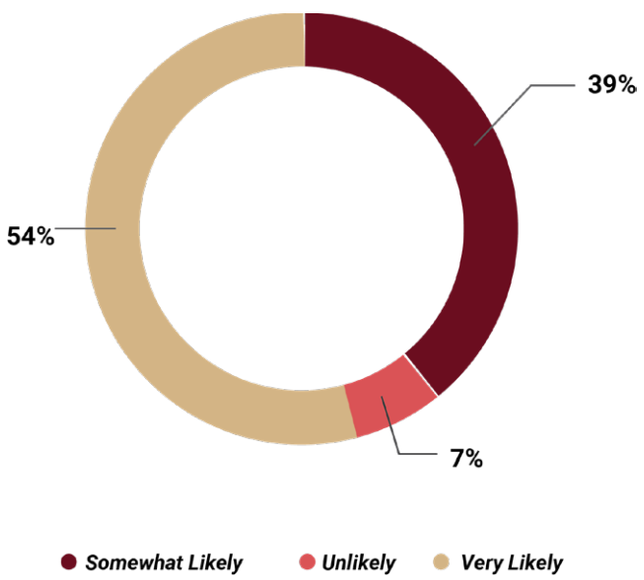
Attack Surface Monitoring

33.7% **of participated organisations continuously monitor their attack surface and take timely remedial actions.**

Top Priorities for Cyber Security Investment

1. Threat Detection & Response
2. Endpoint Security
3. Data Protection
4. Cloud Security
5. Employee Training

Adoption of AI for Cyber Threat Defense

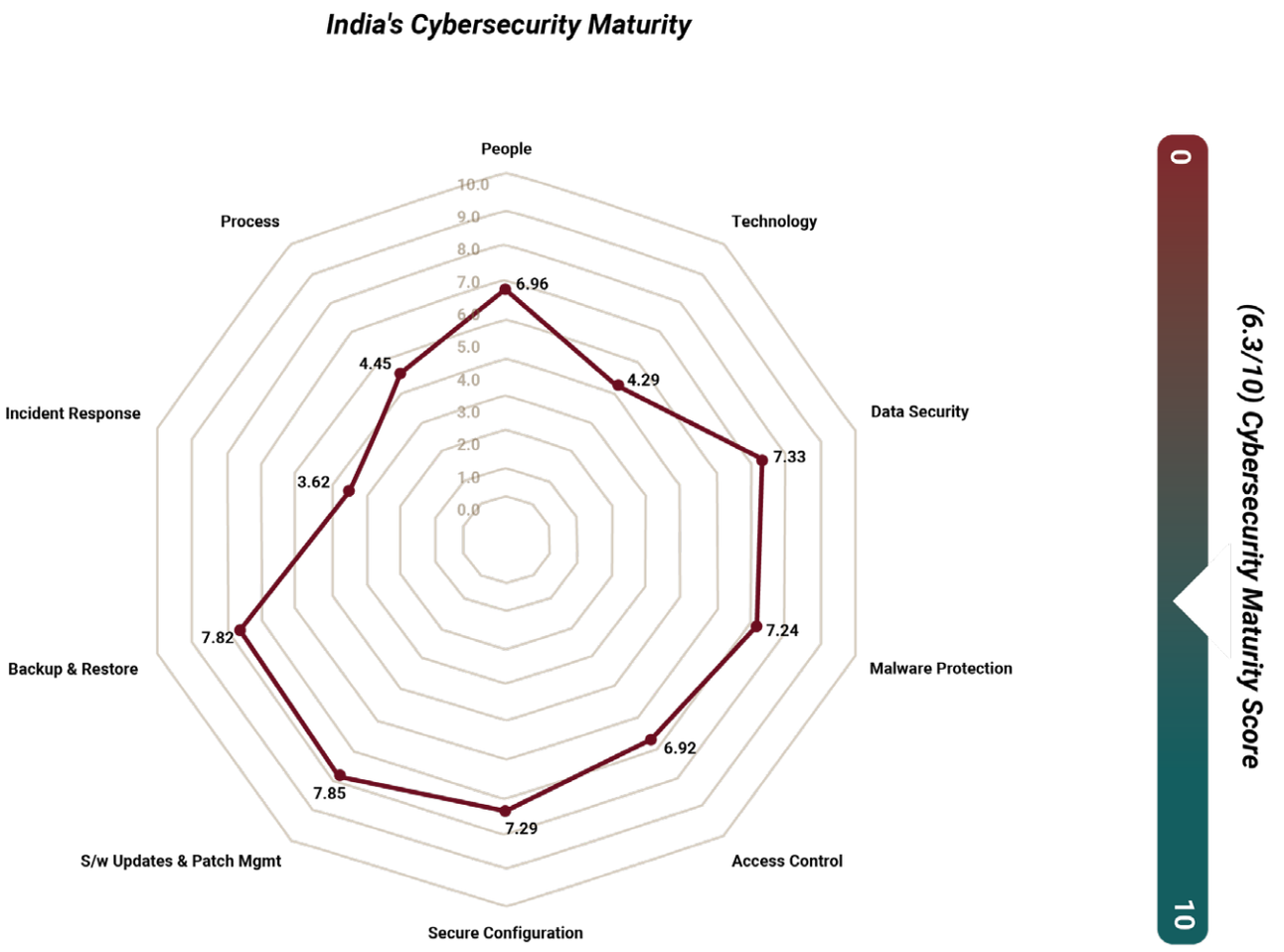


Cybersecurity Maturity Radar Map

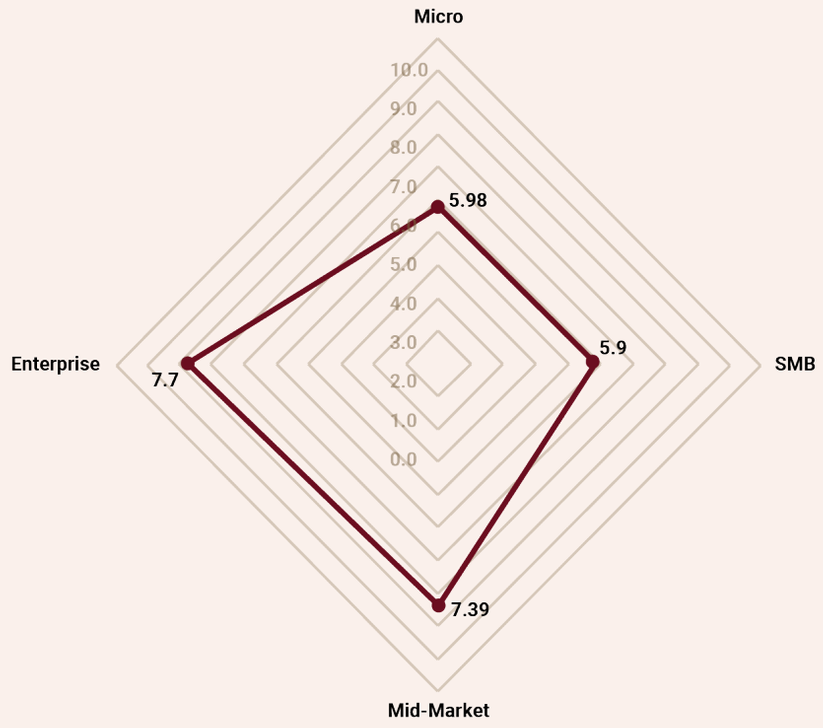
The Cybersecurity Maturity Radar Map offers a comprehensive snapshot of the current state of cybersecurity readiness. By evaluating critical areas such as incident response, malware protection, data security, and access control, the map effectively highlights both strengths and areas for improvement within the cybersecurity framework. Each axis on the radar corresponds to a specific category, with scores ranging from 0 to 10, providing a clear measure of maturity levels in those areas. Here's a detailed breakdown

People: Assesses staff awareness and training to address cybersecurity risks.
Process: Evaluates the strength and efficiency of cybersecurity management processes.
Technology: Measures the use of advanced tools to protect systems and data.
Data Security: Reviews mechanisms for safeguarding sensitive data against unauthorized access and breaches.
Malware Protection: Examines the ability to prevent, detect, and respond to malware threats.
Access Control: Evaluates the effectiveness of restricting access to systems and information.
Secure Configuration: Focuses on applying secure settings to reduce vulnerabilities.
Software Updates & Patches: Tracks efficiency in addressing known vulnerabilities through updates.
Backup & Restore: Assesses the reliability of backups and data recovery capabilities.
Incident Response: Measures readiness and effectiveness in managing security incidents.

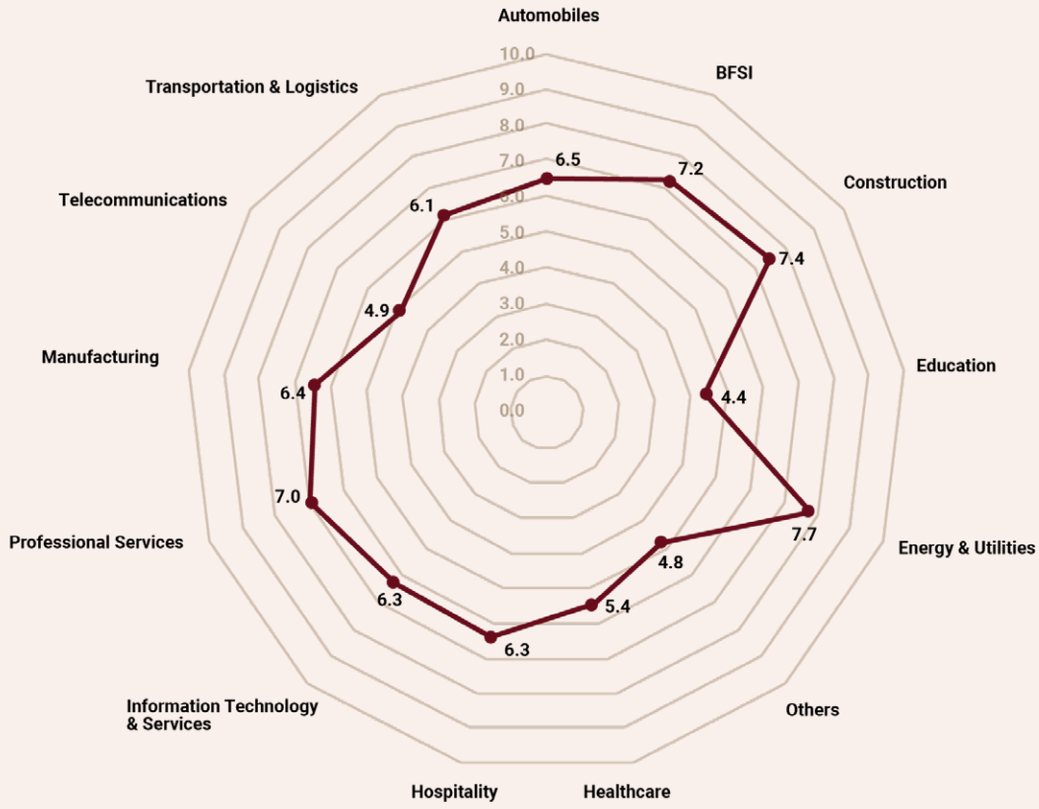
For the analysed sample size, the maturity score stands at 6.3/10, indicating a moderate level of maturity with room for improvement.



Segment-wise Maturity



Industry-wise Maturity



EVALUATION PARAMETERS

Cyber Hygiene

evaluates how well organisations build a security-first culture through employee awareness, responsible behaviour, and regular training. The goal is to understand how effectively employees function as the first line of defense and how consistently security practices are followed across daily operations.

Securing Assets

assesses the organisation's ability to identify, track, and protect all hardware and software assets through accurate inventories, updated CMDBs, secure disposal, and removal of EOL/EOS systems. The purpose is to measure asset visibility and assess how effectively organisations mitigate exposure and safeguard their infrastructure.

Data Security

evaluates the protection of sensitive and business-critical information through data classification, leakage controls, encryption, and secure data wipe processes. The goal is to determine how effectively organisations preserve confidentiality, integrity, and availability while preventing unauthorised access or leakage.

Malware Protection

examines the deployment of advanced anti-malware tools, scanning practices, firewall usage, and restrictions on unauthorised or unsafe software. This helps assess how prepared organisations are to defend against malware, ransomware, and modern attack vectors.

Access Control

reviews how organisations manage identities, privileges, and authentication through role-based access, provisioning workflows, strong password practices, and restricted admin usage. The aim is to evaluate the strength of controls that prevent unauthorised access to systems and data.

Secure Configuration

focuses on system hardening practices, removal of default or weak settings, disabling unused features, and adherence to industry baselines such as CIS standards. The goal is to understand how effectively organisations minimize misconfigurations — a leading cause of security incidents.

Software Updates & Patch Management

evaluate the consistency and completeness of deploying patches and updates across environments, including prioritization and structured processes. This aims to measure how well organisations mitigate known vulnerabilities before they are exploited.

Backup & Recovery

assess the implementation of reliable, protected, and offline backup strategies covering critical systems and cloud environments. The purpose is to understand the organisation's capability to restore operations quickly and maintain continuity during disruptions or cyber incidents.

Incident Response

assesses the presence of defined processes, employee awareness, and readiness to detect, respond to, and recover from an incident. The goal is to determine how effectively organisations can limit the impact and restore normal operations during cyberattacks.

Security Process Management

reviews how regularly organisations test, update, and validate their cybersecurity processes. The objective is to assess whether organisations continuously strengthen their security posture and adapt to evolving threats through ongoing governance and improvement.

/{ threat | **forecast 2026** the age of cognitive intrusions };

RETROSPECTIVE ACCURACY
PREDICTIONS THAT SHAPED 2025

YEAR	PREDICTIONS MADE	VERIFIED	ACCURACY
2025	20	14	70%

Key Themes Confirmed

AI-driven threats, ransomware evolution,
supply chain compromise, insider risk, cyber warfare

Seqrite's 2025 threat forecasts achieved a 70% validation rate, accurately anticipating the surge in AI-powered attacks, hybrid warfare operations (Operation Sindoor), and the evolution of ransomware into data-extortion ecosystems.

The global threat surface expanded faster than defenses driven by AI adoption, geopolitical friction, and systemic dependency on digital ecosystems.

2026 THE YEAR CYBER THREATS BECOME COGNITIVE AND COVERT

AI Trust Manipulation PREDICTED TREND Poisoning the Well – Direct Attacks on AI Models	**Social Engineering 2.0** PREDICTED TREND Hyper-Personalized AI Phishing & Mobile Banking Malware	**Statecraft by AI** PREDICTED TREND AI-Enhanced APTs and Strategic Deception	**Exploit Acceleration** PREDICTED TREND Zero-Day & Supply Chain Weaponization	**Hidden File Vectors** PREDICTED TREND SVG File Abuse in Stealth Attacks
Ransomware Reinvented PREDICTED TREND AI-Driven RAT Orchestration in Ransomware	**Persistent Encryption Campaigns** PREDICTED TREND Multi-Stage, Stealth-Oriented Ransomware	**Endpoint Neutralization** PREDICTED TREND EDR Freeze & Kernel Suspension Exploits	**Fileless Persistence** PREDICTED TREND WMI Abuse for Remote Control & Stealth	**Mobile Evasion** PREDICTED TREND Malware Adapting to Google's New App Rules
Contactless Fraud PREDICTED TREND NFC Relay & Token Hijacking in Payments	**Digital Activism 2.0** PREDICTED TREND Hybrid Hacktivism in Geopolitical Conflicts	**Cybercrime Evolution** PREDICTED TREND Fragmented Underground Ecosystems	**Dual-Use Tools** PREDICTED TREND Weaponizing Legitimate System Utilities	**Identity at Risk** PREDICTED TREND Credential Abuse & Identity-Based Attacks

KEY PREDICTIONS

- **Poisoning the Well:** *Direct Attacks on AI Systems*

  As critical sectors increasingly adopt AI for decision-making—medical imaging, credit scoring, industrial control, fraud detection—attackers will target AI lifecycles directly. By inserting biased, mislabeled, or strategically crafted samples into training data, adversaries can distort model behaviour, implant logic-based backdoors, or trigger dangerous misclassifications at runtime.

  These compromises can persist for months due to the opaque nature of AI pipelines. Organisations will need integrity checks, adversarial testing frameworks, and secure training environments to maintain trust in AI systems.

- **AI-Powered Deception:** *Hyper-Personalized Social Engineering*

  AI will make social engineering almost indistinguishable from legitimate interaction. Attackers will construct "digital twins" of victims' contacts mimicking writing styles, speech patterns, and even video presence. This mirrors early-stage impersonation patterns seen in campaigns like GrassCall, where staged conversations were used to deliver malware.

  In 2026, these techniques will merge with AI-enhanced mobile banking malware capable of auto-filling credentials, bypassing biometrics, and executing fraud autonomously. Enterprises must adopt phishing-resistant MFA and continuous user authentication to counter the precision of AI-driven deception.

- **The Rise of Cognitive APTs:** *AI-Enhanced Strategic Deception*

  State-backed APT groups and organized cybercriminal syndicates will integrate AI into reconnaissance, vulnerability discovery, lateral movement, and real-time payload adaptation. Operations resembling Operation Sindoor, which combined espionage, psychological operations, and false attribution signals, foreshadow how AI will amplify misdirection and obfuscation.

  AI-enabled APTs will autonomously refine their TTPs, mutate malware, and spoof the behavioural patterns of rival groups, further complicating attribution and response.

- **Zero-Days at Machine Speed:** *Exploit and Supply Chain Attacks*

  Exploit development cycles will compress dramatically due to AI-assisted vulnerability research. Attacks on high-value systems like SAP NetWeaver (CVE-2025-31324), Oracle EBS, and archive parsing vulnerabilities (e.g., 7-Zip CVEs) already demonstrate how quickly adversaries exploit weaknesses.

  In 2026, supply chain compromise—CI/CD pipelines, SDKs, container registries, and cloud integrations—will remain the most efficient pathway to large-scale infiltration. Organisations must adopt automated patch orchestration, software bill of materials (SBOM) visibility, and hardened build systems.

- **The Hidden Canvas:** *SVG File Abuse*

  SVG files—frequently treated as harmless assets—will emerge as powerful malware carriers. Recent cases involving Xml.Trojan-embedded SVG payloads preview how attackers embed JavaScript or redirection logic inside vector graphics.

With creative teams, marketing workflows, and AI design tools increasingly exchanging SVG files, attackers will use them to infiltrate automated pipelines and collaboration systems, bypassing traditional filters and sandboxing.

- **AI-Led Ransomware:** *Autonomous RAT Deployment*

  Ransomware operators will deploy AI-based orchestration engines capable of autonomously mapping network topologies, selecting RAT payloads, evolving anti-analysis behaviour, and performing adaptive privilege escalation. Early versions of automated delivery chains—such as the Weaxor ransomware SQL-based RAT deployment—hint at what fully autonomous ransomware operations may look like in 2026.

  These attacks will mimic legitimate processes, rotate execution behaviour, and reduce detection windows to minutes.

- **Ransomware 2.0:** *Multi-Stage, Stealth-Oriented Campaigns*

  Ransomware attacks will increasingly unfold as multi-phase operations rather than single-event encryptions. Campaigns like Xelera and Weaxor, which combined reconnaissance, data theft, C2 beaconing, and eventual encryption, reflect this shift.

  In 2026, ransomware will operate with extended dwell time, using memory injection, sandbox evasion, and multi-stage loaders to remain invisible until final impact. Data theft, financial fraud, lateral movement, and crypto-mining will often precede encryption.

- **Ghosted Defenses:** *EDR Freeze & Kernel-Level Suspension*

  Attackers will target endpoint security directly using thread suspension, dump manipulation (e.g., WerFault, MiniDump), and vulnerable driver exploitation. While this tactic did not appear widely in the 2025 dataset, it aligns with increased abuse of kernel-level components for stealth persistence.

  In 2026, these attacks will allow malware to operate on “healthy-looking” systems where EDR is running but silently neutralized. Continuous telemetry validation and strict driver policies will be essential

- **Living Off WMI:** *Fileless Persistence and Remote Control*

  Fileless attacks will continue to rise, with adversaries increasingly weaponizing WMI for persistence, stealthy command execution, and lateral movement. Campaigns similar to the Masslogger fileless variant, which used registry-only payloads and PowerShell execution, show how attackers avoid leaving artifacts.

  In 2026, permanent WMI event subscriptions and remote WMI RPC calls will become high-signal indicators of compromise, requiring SOCs to baseline and monitor WMI behaviour.

- **Adaptive Mobile Threats:** *Bypassing Google’s App Rules*

  Google’s enforcement of verified-developer requirements for all sideloaded apps will reshape Android malware delivery. Threat actors will increasingly purchase or compromise verified developer identities to push malicious apps through trusted channels.

  The fake NextGen mParivahan malware campaign demonstrates how attackers already mimic trusted services. As verification tightens, adversaries will pivot to Progressive Web Apps (PWAs), malicious ads, and outdated devices outside enforcement coverage.

- **NFC Exploitation:** *The Next Wave of Contactless Fraud*

  With global expansion of tap-and-pay services, NFC-based attacks will scale. Attackers will exploit compromised Android devices as relay nodes, intercepting HCE tokens and manipulating transactions in real time.

  Although the 2025 dataset did not observe direct NFC fraud, the pattern of credential-stealing mobile malware suggests a high potential for evolution in 2026.

- **Hybrid Hacktivism:** *Statecraft in the Digital Age*

  Hacktivism is evolving into a geopolitical instrument, blending cyberattacks with disinformation campaigns. Groups linked to operations like Operation Sindoor and emerging hacktivist clusters show how "volunteer" groups engage in state-aligned narratives while maintaining plausible deniability.

  In 2026, expect coordinated DDoS attacks, data leaks, deepfake propaganda, and symbolic disruptions of critical infrastructure tied to political timelines.

- **The Fragmented Underground:** *Cybercrime Without Borders*

  The cybercrime ecosystem will fracture into small, decentralized cells as large ransomware groups face shutdowns. Campaigns spreading across variant families—KillSec, FunkSec, Lynx, StegoCampaign loaders, and HijackLoader (ClickFix)—already signal distributed specialization.

  Access brokers, exploit developers, and data extortion operators will collaborate in modular, service-based structures, making takedowns harder and reconstitution faster.

- **Dual-Use Exploitation:** *Weaponizing Legitimate Tools*

  Ransomware actors will increasingly rely on living-off-the-land binaries, signed drivers, and low-level utilities to neutralize EDR. Examples like Weaxor's use of sqlps.exe, Masslogger's InstallUtil.exe abuse, and WantToCry's SMB-based lateral movement reflect this pattern.

  In 2026, AI will assist attackers in selecting the least-detectable pathways, including kernel rootkits, cloud admin APIs, and syscalls that bypass user-mode monitoring.

- **Identity as the New Battlefield:** *Credential Abuse at Scale*

  Identity will remain the most valuable target. Credential-stealing campaigns—such as Stealerium, SnakeKeylogger, and OAuth abuse during the Google Salesforce breach—show how attackers bypass perimeter defenses entirely by impersonating legitimate users.

  With widespread adoption of SSO, federated identity models, and cloud-native access, a single compromised identity could unlock entire enterprise environments. Identity threat detection, privileged access controls, and continuous authentication will define future defense strategies.

/{ recommendations & | **beyond 2026** from reactive defense to cognitive resilience };

1. Prioritize Predictive Intelligence

By 2026, attacks will no longer depend solely on exploits but on deception and adaptive behaviour. rganizations must integrate AI-driven threat prediction, anomaly detection, and telemetry correlation to anticipate attacks before impact. Invest in cross-layer visibility — endpoints, cloud, identity, and network — to identify behavioural deviations in real time.

2. Accelerate Patch Orchestration

Vulnerability-to-exploit time has compressed from weeks to days. Automated patch orchestration, vulnerability prioritization, and virtual patching through EDR/XDR must become standard across hybrid infrastructures.

3. Reinforce Identity as the New Perimeter

Identity will remain the primary attack vector. Adopt Zero Trust principles, enforce strong MFA, and continuously monitor for credential replay, token abuse, and privilege escalation.

4. Harden the AI Layer

AI models, copilots, and data pipelines are emerging as new breach surfaces. Implement AI security governance, model integrity validation, and adversarial data testing to prevent prompt injection and model poisoning attacks.

5. Advance to Autonomous Detection and Response

Move from manual SOC triage to autonomous security operations powered by GenAI and context-aware correlation. Integrating tools like Seqrite's Intelligent Assistant (SIA) can enhance decision support, triage efficiency, and analyst productivity.

6. Build Cyber Resilience Frameworks

Accept that compromise is inevitable; containment and continuity define maturity.
Develop cyber crisis playbooks, simulate breach drills, and measure Mean Time to Remediate (MTTR) as a board-level KPI.

7. Strengthen Ecosystem Collaboration

Cybercrime today is borderless. Enterprises must collaborate across industry ISACs, government CERTs, and global intelligence exchanges to share IoCs, TTPs, and defense playbooks in near real time.

8. Secure the Human Element

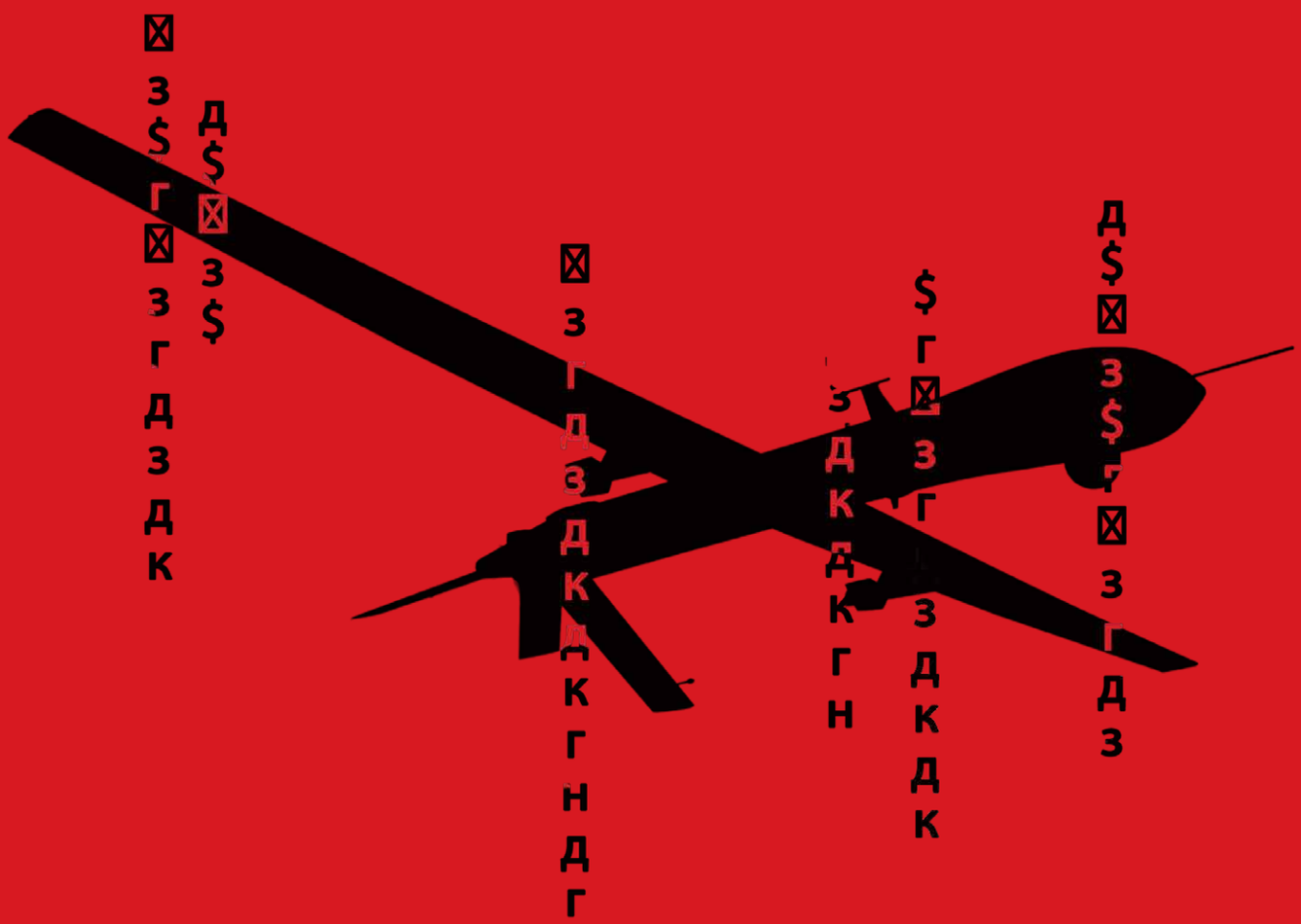
Despite AI's dominance, social engineering remains the attacker's most effective weapon. Embed continuous cyber awareness, phishing simulations, and behaviour-driven access policies to reduce human error.

9. Defend Against the New Frontier – Cognitive Threats

2026 will usher in AI-augmented adversaries capable of autonomous reconnaissance and deception.
Defenders must match this evolution with AI-augmented defense, ensuring every layer — from SOC to endpoint — can detect and respond dynamically.

The next frontier of cybersecurity will not be defined by who has more tools, but who adapts faster.

As threat actors evolve into cognitive adversaries, capable of mimicking users and weaponizing AI platforms, India's cybersecurity strategy must focus on resilience, adaptability, and intelligence.
The coming year will test the readiness of enterprises to embrace autonomous protection, predictive defense, and human-machine collaboration in real time. Only those who see cyber defense not as a cost, but as a strategic differentiator, will thrive in the digital future.



/{ expert
    quotes };

"The future of security lies beyond the device, our new mission is safeguarding the lifeblood of the digital enterprise: data. As India accelerates into an AI-driven, cloud-native economy, the old guard of endpoint-centric controls must yield to a dynamic, data-centric security vision. Leadership is not just about protecting resources, but about shaping a culture where data protection is woven into every decision, partnership, and innovation. Building digital trust for tomorrow demands an unwavering commitment to resilient, intelligent, and ethical data stewardship. This is the paradigm shift that will secure India's digital ambitions for generations to come."

PRAVEEN KUMAR

CISO, Nykaa

"In BFSI sector, the threat landscape is unforgiving. Cybercriminals know that trust is our most valuable currency, and they target it relentlessly. Over the last year, we have seen sophisticated fraud schemes, account takeovers, and ransomware campaigns aimed directly at disrupting financial stability. **For us, cybersecurity is no longer a back-office function, it is core to customer confidence and regulatory compliance.** The future will belong to institutions that can combine real-time fraud detection with proactive intelligence, ensuring security and trust go hand in hand."

C. SHERMUGADURAI

CISO, Tamil Nadu Mercantile Bank (TMB)

"The insights from the India Cyber Threat Report 2026 mirror the realities we face in engineering, construction & manufacturing. As IT and OT environments merge, even small security gaps can trigger large-scale operational disruptions. Our priority today is ensuring visibility across industrial networks, tightening access controls, and predicting anomalies before they halt production & operations. **Cybersecurity has become a key enabler for business because in engineering & construction industry, every minute of uptime counts & reliability of platforms is of paramount importance"**

UDAY DESHPANDE

CISO, Larsen & Toubro

"As enterprises embrace cloud, mobility, and connected devices, the attack surface is expanding faster than security teams can cover it. Our traditional models built for fixed perimeters no longer apply. Security must move closer to identity, data, and behaviour wherever they reside. The concept of a 'secure boundary' has become entirely digital. This shift has also transformed how attacks are launched — with adversaries now using AI to scale, automate, and adapt. Defending against AI-driven threats requires AI-driven defense: security built to match the speed and intelligence of the attackers themselves."

ASHISH ADHVARYU

VP & Delivery Head - Cyber Security Practice, Infosys

"In BFSI sector, the threat landscape is unforgiving. Cybercriminals know that trust is our most valuable currency, and they target it relentlessly. Over the last year, we have seen sophisticated fraud schemes, account takeovers, and ransomware campaigns aimed directly at disrupting financial stability. For us, **cybersecurity is no longer a back-office function, it is core to customer confidence and regulatory compliance.** The future of secure banking will belong to institutions that blend real-time fraud detection with proactive intelligence, where security, resilience, and trust go hand in hand."

RADHAKRISHNAN S.

CISO, Indian Overseas Bank, Chennai

"Cyber threats are no longer episodic—they are a continuous reality. Cybercriminals, empowered by AI and automation, now launch attacks in hours instead of months, making them faster, stealthier, and more persistent. **Traditional defenses alone won't suffice. Organisations must embrace adaptive security**—where detection, response, and resilience are embedded into core operations and recognize that employees are the first line of defense. Building a strong human firewall through awareness and training is as critical as deploying advanced technologies. This shift from static protection to dynamic resilience will define who thrives in the digital era."

DILEEP KUMAR MUKUNDAN

CISO, IFTAS

"Threat intelligence has evolved rapidly, moving beyond static threat lists to AI systems that can analyze data across sectors and predict attacks before they happen. This shift is especially critical for education, where schools, universities, and learning platforms hold sensitive student data, research records, and personal information. If India strengthens national-level intelligence sharing and combines it with adaptive, locally responsive defense across public systems, private enterprises, and educational institutions, **we can protect millions of learners and build one of the most secure digital ecosystems in the world, but only if we act now before threats outpace our defenses."**

GOUTHAM NANJUNDASWAMY

CTO, Ethnus

Acknowledgement

AUTHORS

Shayak Tarafdar, Sr. Manager - Engineering

Priyabrata Dash, Manager - Engineering

Jyoti Karlekar, Senior Content Writer

CONTRIBUTORS

Sangmesh S, Vice President & Head of Seqrite Labs

Jaswinder Singh, Director, Engineering

SURVEY DESIGNER AND SCORE CARD CREATOR

Bhupendra Shirsath, Lead, Performance Marketing

Bandu Sudnye, Manager, Web Development

EDITORS

Deepti Uppal, Director, Marketing Communications

Om Puran, Director - Marketing

DESIGN

Siddharth Sarathi, Design Manager

Kinkar De Sarkar, Senior Executive - Design

Seqrite is a leading enterprise cybersecurity solutions provider. With a focus on simplifying cybersecurity, Seqrite delivers comprehensive solutions and services through our patented, AI/ML-powered tech stack to protect businesses against the latest threats by securing devices, applications, networks, cloud, data, and identity. Seqrite is the Enterprise arm of the global cybersecurity brand, Quick Heal Technologies Limited, the only listed cybersecurity products and solutions company in India.

We are the first and only Indian company to have solidified India's position on the global map by collaborating with the Govt. of the USA on its NIST NCCoE's Data Classification project. We are differentiated by our easy-to-deploy, seamless-to-integrate comprehensive solutions providing the highest level of protection against emerging and sophisticated threats powered by state-of-the-art threat intelligence and playbooks backed by world-class service provided by best-in-class security experts at India's largest malware analysis lab – Seqrite Labs. We are the only Indian full-stack company aligned with CSMA architecture recommendations, offering award-winning Endpoint Protection, Enterprise Mobile Device Management, Data Privacy, Zero Trust Network Access, and many more. Seqrite Data Privacy Management solution enables organisations to stay fully compliant with the DPDP Act and global regulations. Seqrite also offers the Seqrite Malware Analysis Platform (SMAP) for deep, multi-layered malware analysis, along with Seqrite Threat Intel, a real-time cyber defense hub delivering enriched, actionable threat intelligence.

We have recently launched Digital Risk Protection Services for external threat monitoring and Ransomware Recovery as a Service for rapid, guided restoration after ransomware attacks. Seqrite has also unveiled SIA, an LLM-powered security co-pilot built on GoDeep.AI to help enterprises navigate growing cyber complexity with intelligent, conversational analysis.

Today, 30,000+ enterprises in more than 70 countries trust Seqrite with their cybersecurity needs. For more information, please visit: **https://www.seqrite.com**

SEQRITE