

**INDIA**

**CYBER THREAT**

**REPORT**

**2025**

Copyright ©2024

All rights reserved.

This report has been jointly developed by Data Security Council of India (DSCI) and Seqrite. The information contained herein has been obtained or derived from sources believed by DSCI and Seqrite to be reliable. However, DSCI and Seqrite disclaims all warranties as to the accuracy, completeness, or adequacy of such information. We shall bear no liability for errors, omissions or inadequacies in the information contained herein, or for interpretations thereof.

The information contain herein should not be relied upon as a substitute for specific professional advice. Professional advice should always be sought before taking any action based on the information provided.

The material in this publication is copyrighted. You may not, distribute, modify, transmit, reuse, or use the contents of the report for public or commercial purposes, including the text, images, presentations, etc. without prior consent from either DSCI and/or Seqrite.

# Foreword – DSCI

---

Data Security Council of India (DSCI), in collaboration with Seqrite, presents the second edition of the **India Cyber Threat Report 2025**, marking a significant milestone in our continuous efforts to strengthen India's cybersecurity posture. This comprehensive analysis arrives at a crucial juncture when digital transformation intersects with evolving geopolitical dynamics, presenting both unprecedented challenges and opportunities for our nation's cybersecurity landscape.

The foundation of this report rests upon the analysis of **369.01 million** malware detections across **8.44 million** endpoints, complemented by insights from 200+ cybersecurity leaders. This extensive data collection and analysis have enabled us to present a granular, India-specific perspective on cyber threats, examining patterns and vulnerabilities at state, city, and industry segment levels.



**VINAYAK GODSE**

*Chief Executive Officer,  
Data Security Council of India*

Our findings corroborate key predictions from our last edition and identify new challenges, including AI-powered malware, a surge in ransomware for digital extortion, supply chain attacks, app scams, the enduring threat of hacktivism, and event-based assaults.

As cybercriminals develop increasingly complex and diverse malware, the need for behavior-based detection technologies becomes crucial. Our report highlights a significant rise in behavior-based detections this year, driven by constantly evolving malware variants that evade traditional signature-based systems. Additionally, while ransomware continues to have a higher hit rate than other malware categories, its frequency has decreased compared to last year, indicating improved cyber resilience. This year's report places special emphasis on the transformative impact of Generative AI in cybersecurity. While this technology presents enhanced capabilities for threat actors, it simultaneously offers unprecedented opportunities for advancing defensive strategies and automated security operations. Our PESTLE analysis framework provides additional context, illustrating how cyber threats reverberate across political, economic, social, technological, environmental, and legal dimensions.

Our collaboration with Seqrite has allowed us to develop detailed insights into malware classifications, network and host-based exploitations, and zero-day vulnerabilities specific to the Indian context. These insights, combined with comprehensive threat narratives, provide organizations with actionable intelligence for enhancing their security posture.

I invite you to use this report as your strategic compass for 2025 and beyond, transforming these insights into your defensive advantage as we collectively raise India's cybersecurity standards against evolving threats.

# Foreword – Quick Heal

It is with great pride and a deep sense of responsibility that I present to you the **India Cyber Threat Report 2025**. This year, we have drawn on valuable insights from India's largest malware analysis facility, Seqrite Labs, to provide a comprehensive and in-depth analysis of the evolving cyber threat landscape across the nation. Our findings are based on a vast pool of data, with telemetry gathered from nearly 85 lakh endpoints, offering an unparalleled view of the security challenges facing Indian enterprises.

The **India Cyber Threat Report 2025** dives deep into the emerging trends, sector-specific vulnerabilities, and the growing influence of geopolitical dynamics on cyberattacks. From government agencies to critical infrastructure, no industry or region in India is immune to the growing wave of cyber threats. This report offers actionable intelligence and strategic recommendations to help businesses and government organizations stay one step ahead of malicious actors.



**DR. SANJAY KATKAR**

*Joint Managing Director,  
Quick Heal Technologies Limited*

**2024 is a milestone year for us, marked by three key developments.** On the consumer side, we launched India's first fraud prevention solution, **Quick Heal AntiFraud.AI** to combat the rising menace of frauds. On the enterprise side, **Seqrite**, in collaboration with the **Data Security Council of India (DSCI)**, has conducted **a comprehensive market survey** to assess the state of enterprise cybersecurity adoption in India. This survey identifies key challenges, pain points, and gaps in the industry, highlighting the need for collective action and innovation to combat evolving cyber threats. The insights gathered will empower organizations to enhance their cybersecurity strategies and foster stronger industry-wide collaboration to address emerging risks.

In line with our commitment to innovate, simplify and secure, Seqrite has launched its **Seqrite Malware Analysis Platform (SMAP)**. SMAP represents a significant leap forward in how security professionals can analyze and respond to cyber threats. This advanced solution will offer static, dynamic & manual analysis, providing deep insights into suspicious files and URLs that may evade traditional detection methods allowing for faster and more informed decision-making, thereby averting Zero Day attacks. This year, we are excited to introduce **Seqrite Threat Intel** – a robust threat intelligence platform that provides real-time insights for proactive defense, operational efficiency, supports informed decision-making, and ensures regulatory compliance.

Our Seqrite Labs, a leader in malware analysis and threat intelligence, has been instrumental in identifying and neutralizing critical threats. Its relentless efforts have resulted in top scores from international certification bodies like AV-TEST and AVLab Poland, which are independent validations of robustness and prowess of our cyber security research and detection capabilities of our products. We are also proud to be the only cybersecurity focused Indian company to be a member of US Artificial Intelligence Safety Institute Consortium shaping the global AI narrative.

As we navigate the rapidly changing digital landscape, Seqrite remains steadfast in its goal to lead the industry with innovative solutions, rigorous research, and an unwavering commitment to securing the digital future of India. We are confident that, through our continued efforts, collaboration with industry leaders, and our relentless focus on innovation, we will help build a safer, more resilient digital ecosystem for businesses, governments, and citizens alike.

# From the CEO's Desk

## Quick Heal

India's economy remains robust, driven by strong government investments in infrastructure, local manufacturing, and consistent service industry performance. The digital economy is projected to contribute 20% of GDP by 2026, has also become a prime target for cyberattacks, accounting for 13.7% of global incidents.

At Seqrite, we are committed to simplifying cybersecurity for enterprises, government, and public sectors with innovative solutions. Following the success of last year's India-centric threat report, we proudly present the **India Cyber Threat Report 2025**. This collaborative effort with the Data Security Council of India (DSCI) draws on insights from Seqrite Labs, India's largest malware analysis lab, covering data from nearly 85 lakh endpoints. The report provides a comprehensive analysis of cyber threats and India-specific recommendations to help businesses strengthen their defenses.

This year's report highlights the widespread impact of cyberattacks, with no region or industry immune. We recorded over **369 million detections**, averaging **702 detections per minute**, highlighting the severe risk currently facing India's cyber landscape.

We've also observed an increase in sophisticated threats targeting sectors like **Healthcare, Hospitality and BFSI**, while government entities remain prime targets as well. Global geopolitical tensions, including the Russia-Ukraine and Israel-Iran conflicts, have further escalated cybersecurity risks, driving attacks from hacktivist groups. Additionally, cyber activity around key national events, such as Independence and Republic Days, reflects efforts to undermine India's standing on the global stage. **Attesting to this, over 1 million ransomware attacks were seen over the year.**

Our research also identifies **cross-border threat groups like ANON BLACK FLAG INDONESIAN and THE ANONYMOUS BANGLADESH, with ransomware families like RansomHub and LockBit 3.0 leading the charge.** Cyberattacks in Tier 2 and Tier 3 cities like **Surat, Jaipur and Ahmedabad** have surged due to their growing significance as key economic and business centers.

One of the most revealing insights from this report comes from our recent Cyber Security Maturity Survey. This survey, **which involved 204 participating organizations across India**, offers a comprehensive look into critical areas such as cyber resiliency, preparedness, and priorities. **The findings are truly eye-opening: nearly 73% of organizations are unaware if they have ever been attacked, and 57% lack cyber hygiene practices.** I strongly encourage you to review the survey's statistics and maturity scores and compare your organization's performance against industry benchmarks and market segment averages.

In our pursuit of making 'cyber safety a fundamental right for all' and creating a cybersecure world, our success is built on a foundation of cybersecurity excellence. To further strengthen defenses against growing threats, Seqrite is excited to announce the launch of our **Seqrite Malware Analysis Platform (SMAP)**. SMAP empowers security professionals with multiple layers of malware analysis powered by human intelligence offering deeper insights into the behavior of suspicious files and URLs once executed. This capability significantly enhances and complements traditional detection systems like EPP, XDR, and EDR, providing more robust protection against sophisticated and evasive threats. In addition to this, we are also launching **Seqrite Threat Intel**, a comprehensive threat intelligence platform that gives you real-time insights for proactive defense, enhanced decision making while remaining compliant with regulations.

Seqrite Labs continues to lead in cybersecurity innovation, with top scores from AV Test and other international certification bodies as the only Indian cybersecurity company in the **US Artificial Intelligence Safety Institute Consortium**, contributing to global AI narrative. While significant progress is being made in enterprise cybersecurity, we also recognize the escalating threat to consumers. To address this, we have launched **Quick Heal AntiFraud.AI, India's first fraud prevention solution.** Drawing on over 30 years of industry expertise, we leverage deep insights into consumer fraud and the evolving threat landscape. Just as we tackled the virus problem with our antivirus solutions in 1995, we now take on the growing risk of fraud—an issue that causes not only financial loss but also significant emotional distress.

As the cyber threat landscape evolves, we remain committed to developing cutting-edge solutions, investing in research, and collaborating with industry partners to secure India's digital future. We extend our thanks to DSCI, our partners, and the Seqrite Labs team for their continued dedication to safeguarding India's digital infrastructure and advancing a secure digital future for all.



**VISHAL SALVI**

Chief Executive Officer,  
Quick Heal Technologies Limited

09

Executive  
Summary

15

The State of  
Malware in  
India

41

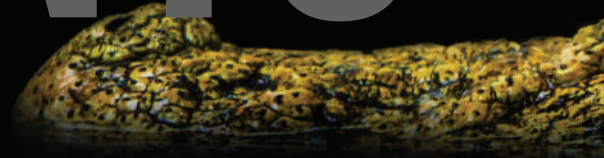
India  
Malware  
Landscape

53

Featured  
Stories  
2025

TABLE OF

CONTENTS



87

The  
Geopolitics of  
Cybersecurity

97

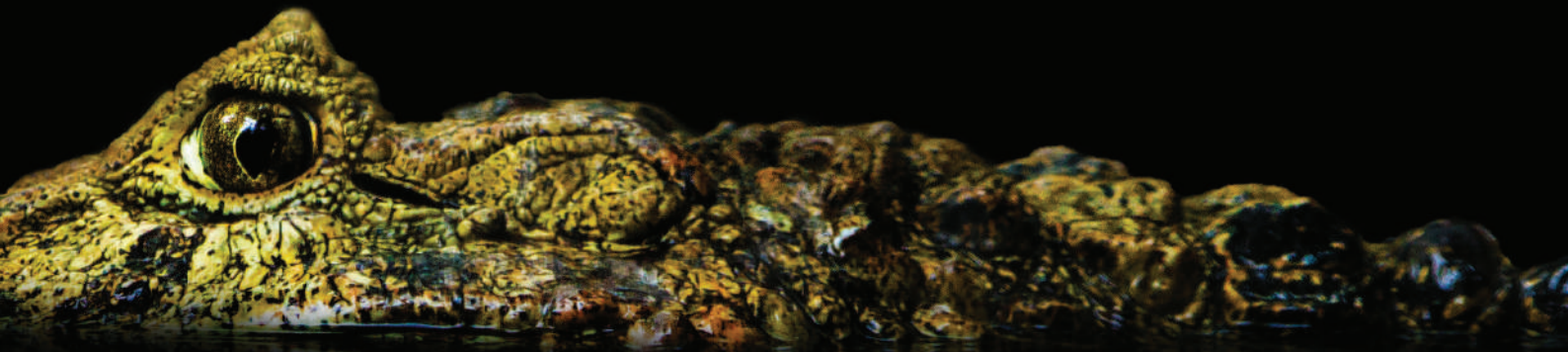
Industry  
Cybersecurity  
Preparedness  
Survey

111

Cyber  
Threat  
Predictions

119

Recommendations  
2025 & Beyond







# EXECUTIVE SUMMARY



# Key Highlights

Bigger spectrum of detections and endpoints

Over **369.01 million** detections recorded across **8.44 million** endpoints

Averaging **702 detections** per minute

Behavioral-based detection

**53.73 million** behavior-based detections, accounted for **14.56%** of total detections

Significant increase from **12.5%** in 2023

Primary attack vectors

**68%**

of attacks originated from Trojans and Infectors

Cloud detections contributed

**62%**

while 38% detections were on-premise

**~12** attacks per month on personal end user devices

Top most targeted industries

**21.82%** 

Healthcare

**19.57%** 

Hospitality

**17.38%** 

BFSI

Geographical Hotspots

Telangana

**15.03%** of detections

Tamil Nadu

**11.97%** of detections

Surat

**14.58%** of detections

Bengaluru

**11.93%** of detections

Jaipur

**11.72%** of detections

Malware and ransomware incidents

**1** Malware incident per **40,436** detections

**1** Ransomware incident per **595** detections

Approximately **1 million** Ransomware detections reported over the year

Based on Seqritre Labs' telemetry data from October 2023 to September 2024.

The cybersecurity landscape in India has witnessed an unprecedented evolution throughout 2024, marked by both escalating threats and significant advances in detection capabilities. This summary outlines the critical findings that shape India's current cybersecurity posture and its implications for the future.

First, the sheer scale of cyber threats is staggering. The detection of over 369.01 million security incidents across 8.44 million endpoints means that, on average, every minute sees 702 potential security threats. To put this in perspective, this is roughly equivalent to having eleven new cyber threats emerging every second somewhere in India. This volume of attacks demonstrate the relentless nature of modern cyber threats and the constant pressure on security systems.

A particularly noteworthy development is the significant shift in how malware is being detected. The increase in behavior-based detections from 12.5% to 14.5% represents an important evolution in both attack and defense strategies. This change tells us that attackers are creating more sophisticated malware that can evade traditional signature-based detection methods.

The geographical distribution of attacks reveals an interesting pattern about how cyber threats are spreading across India. While major tech hubs like Telangana (15.03% of detections) and Tamil Nadu (12%) remain primary targets, we're seeing increasing activity in Tier 2 cities. This suggests that cybercriminals are expanding their reach beyond traditional targets, possibly because smaller cities might have less robust cyber defenses.

The healthcare industry's position as the most attacked sector (21.82% of all attacks) is particularly concerning. This likely reflects the high value of medical data and the critical nature of healthcare systems, which might make organizations more likely to pay ransoms. The significant targeting of hospitality (19.57%) and banking sectors (17.38%) suggests that attackers are focusing on industries that handle large volumes of personal and financial data.

The rise in cloud-based detections is especially significant, with 62% of detections occurring in cloud environments. This reflects the broader digital transformation across Indian businesses, but it also highlights a critical security challenge. As more organizations move their operations to the cloud, they're creating new opportunities for attackers to exploit misconfigured or inadequately protected cloud resources.

In 2025, the cyber threat landscape will be dominated by AI-driven attacks, with cybercriminals leveraging generative AI to create more sophisticated and adaptive threats using AI-powered malware. Social media and generative AI will enable highly targeted scams and impersonations, making it harder to distinguish between real and artificial interactions. Ransomware will continue to evolve, targeting supply chains and critical infrastructure. The rise of cloud adoption is likely to expose misconfigured cloud environments and insecure APIs, resulting in attackers exploiting cloud vulnerabilities. Supply chain complexities in hardware will continue to pose challenges with tampered devices and IoT infrastructure. Fake apps, especially in the fintech and government sectors, will remain a significant concern. Additionally, the challenging geopolitical situation is likely to result in state actors targeting critical infrastructure and public utility services.

In addition to presenting a detailed overview of the current cyber threat landscape, this report delves into a PESTLE analysis, offering valuable insights into the macro impact of cyber threats across various dimensions. The Political aspect examines how cyber threats influence national security, government policies, and international relations. Economically, the report highlights the financial repercussions of cyber incidents, including costs related to data breaches, fraud, and business disruptions. The social dimension explores the effects on public trust, privacy concerns, and the societal implications of widespread cyber attacks. Legally, the analysis addresses the evolving regulatory landscape and the importance of compliance with cybersecurity laws and standards. Technologically, the report underscores the advancements in cyber defense mechanisms and the continuous innovation required to counteract sophisticated threats. Lastly, the environmental aspect considers the indirect impact of cyber threats on critical infrastructure and the potential consequences for environmental sustainability. This comprehensive PESTLE analysis aims to provide a holistic understanding of the far-reaching implications of cyber threats, guiding stakeholders in developing robust strategies to mitigate risks and enhance resilience.

The trends reported suggest that organizations need to take a more comprehensive approach to cybersecurity. This means not just investing in technical solutions, but also in training employees, developing incident response plans, and building relationships with security partners. The rise in politically motivated cyber attacks also indicates that organizations need to consider geopolitical factors in their security planning.

These findings paint a picture of a rapidly evolving threat landscape where traditional security approaches alone are no longer sufficient. Organizations need to adapt their security strategies to address both current and emerging threats while maintaining vigilance against traditional attack vectors. The report makes it clear that cybersecurity is no longer just an IT issue but a fundamental business risk that requires attention at all levels of an organization.





# THE STATE OF MALWARE IN INDIA



# Cybersecurity Outlook 2024

The analysis of India's malware detection, based on Seqritre Labs' telemetry data from October 2023 to September 2024, reveals critical insights into the current threat landscape. With **369.01 million** detections across **8.44 million** strong installation base, the data highlights both the scale of cyber threats and the gaps in protection. The majority of detections, **85.44%** relied on **signature-based methods**, underscoring the persistence of known threats. However, **14.56%** of detections came through **behavior-based detection**, emphasizing the growing need for adaptive security to identify emerging, unknown threats.

## Malware detection 2024

 **8.44 million endpoints** 

**369.01 million detections**

**85.44%**



**315.28 million**  
signature based detections

**14.56%**

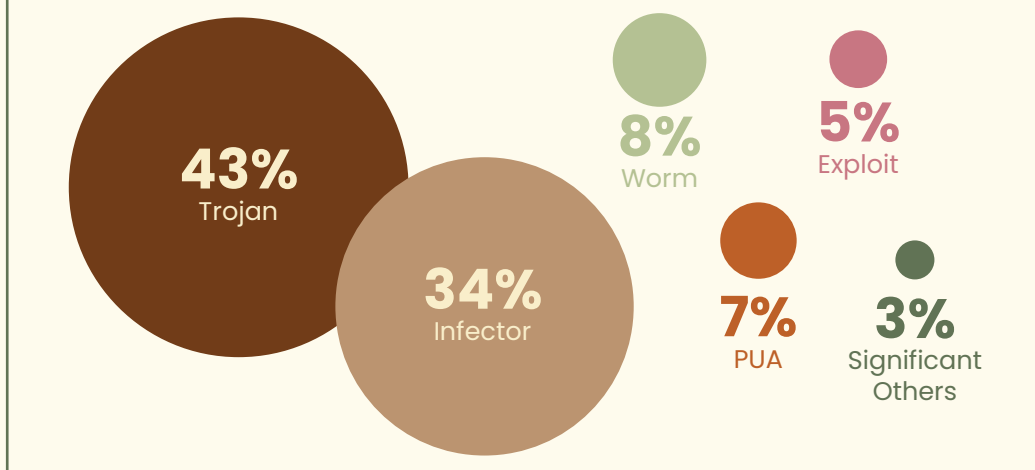
**53.73 million**  
behaviour based detections

 /  **43.72**  
detections per endpoint

 /  **6.37**  
behaviour based detections per endpoint

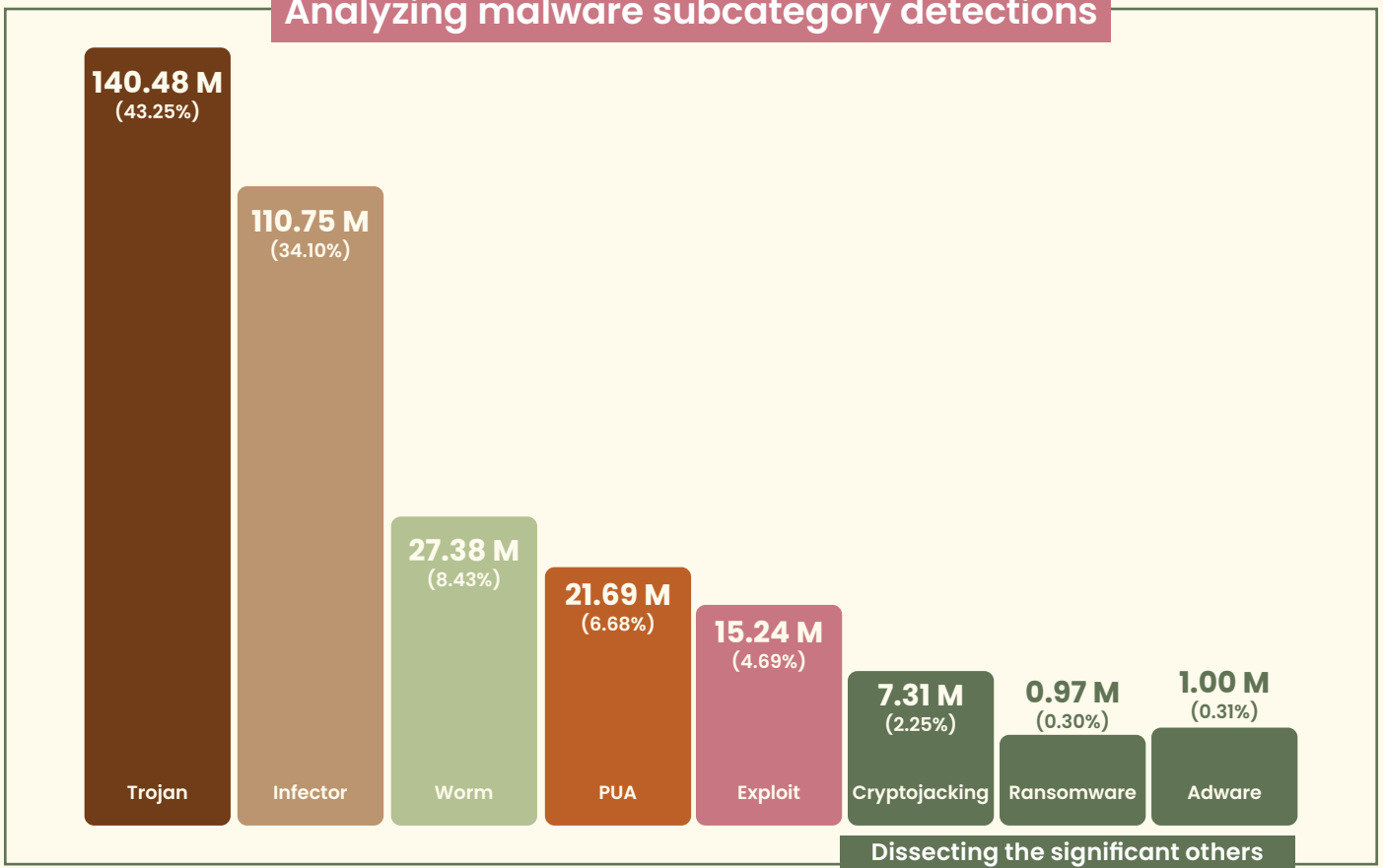
## Malware Threats in India:

### Analyzing malware subcategory detections





## Analyzing malware subcategory detections



In 2024, malware continues to be a significant challenge with various types of malicious software impacting millions of devices. A closer look at the malware subcategories and their detection rates provide valuable insights into the nature of cyber threats, highlighting the most prevalent forms of malware and the effectiveness of current detection methods.

### Trojan

140.48 million (43.25%)

These malicious programs often masquerade as legitimate software to trick users into executing them, giving attackers backdoor access to systems.

- ▲ Implement **behavioral analysis and heuristic-based detection** to identify malicious activity associated with Trojans. This can detect new or evolving Trojan variants that bypass traditional signature-based defenses.
- ▲ Deploy **email filtering** tools to block phishing emails (the most common Trojan delivery method) and **URL filtering** to block malicious links.

- ▲ Ensure that signature-based antivirus programs are up-to-date to catch known infectors, while also using heuristic or behavioral scanning for more advanced threats.

### Infector

110.75 million (34.10%)

**Infectors**, responsible for modifying or corrupting system files, often spread by attaching themselves to legitimate programs, making them particularly difficult to detect and remove.

## Worm

27.38 million (8.43%)

These self-replicating programs spread across networks, exploiting vulnerabilities to infect additional systems without user intervention.

- ▲ Prioritize patching vulnerabilities, network segmentation, and real-time traffic analysis to stop worms from spreading.

- ▲ Use **ad-blocking** software and **privacy-focused browsers** to prevent PUAs from displaying intrusive ads and collecting user data.

- ▲ Implement **system optimization tools** that can detect and remove unwanted programs that slow down the system.

## Potentially Unwanted Applications (PUA): 21.69 million (6.68%)

**PUAs**, often don't have malicious intent but can negatively impact system performance, display unwanted ads, or collect personal data without consent.

## Exploit

15.24 million (4.69%)

**Exploits**, which target vulnerabilities in software, often deliver other types of malware or provide unauthorized access to attackers.

- ▲ Use **sandboxing** techniques to isolate potentially vulnerable applications, preventing exploits from affecting the entire system.
- ▲ Invest in advanced exploit prevention tools that detect and block zero-day attacks by identifying unusual system behavior indicative of an exploit attempt.

- ▲ Deploy **endpoint detection and response (EDR)** solutions that specifically identify and mitigate cryptojacking activity by monitoring for unauthorized mining operations.

## Cryptojacking 7.31 million (2.25%)

**Cryptojacking** hijacks system resources to mine cryptocurrency. Although not as disruptive as ransomware, cryptojacking can significantly degrade system performance.

## Ransomware

0.97 million (0.30%)

**Ransomware** continues to be a high-impact threat, even though it accounts only **0.30%** of detections. This malware encrypts data and demands a ransom for decryption, causing significant financial and operational damage.

- ▲ Use **behavioral detection** tools to identify ransomware activity based on abnormal file access patterns, such as rapid encryption of file and ransomware attacks.
- ▲ Prioritize frequent backups, user training, and proactive detection to minimize the risk and impact of ransomware attacks.

- ▲ Use ad-blockers, secure browsing tools, and conduct routine clean-ups to prevent and mitigate adware infestations.

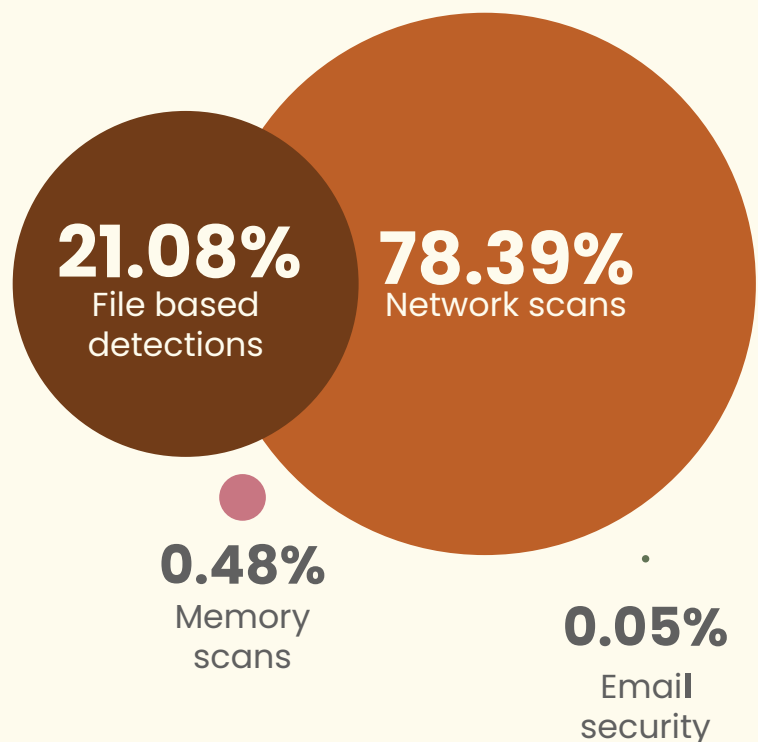
**Adware**  
1.00 million (0.31%)

**Adware** makes up **0.31%** of detections (**1.00 million**). While typically less harmful, adware disrupts user experience by flooding devices with unwanted ads, and in some cases, it can gather sensitive user data.

## Signature-Based Detection Landscape:

Traditional signature-based detections have served as the foundation of malware identification for decades. However, the distribution of detection methodologies have evolved to address modern attack vectors and sophisticated threats.




**The current landscape reveals a sophisticated multi-layered approach, where network-based detection dominates at 78.39%, followed by file-based detection at 21.08%, while memory and email scanning represent smaller but crucial components at 0.48% and 0.06% respectively.**



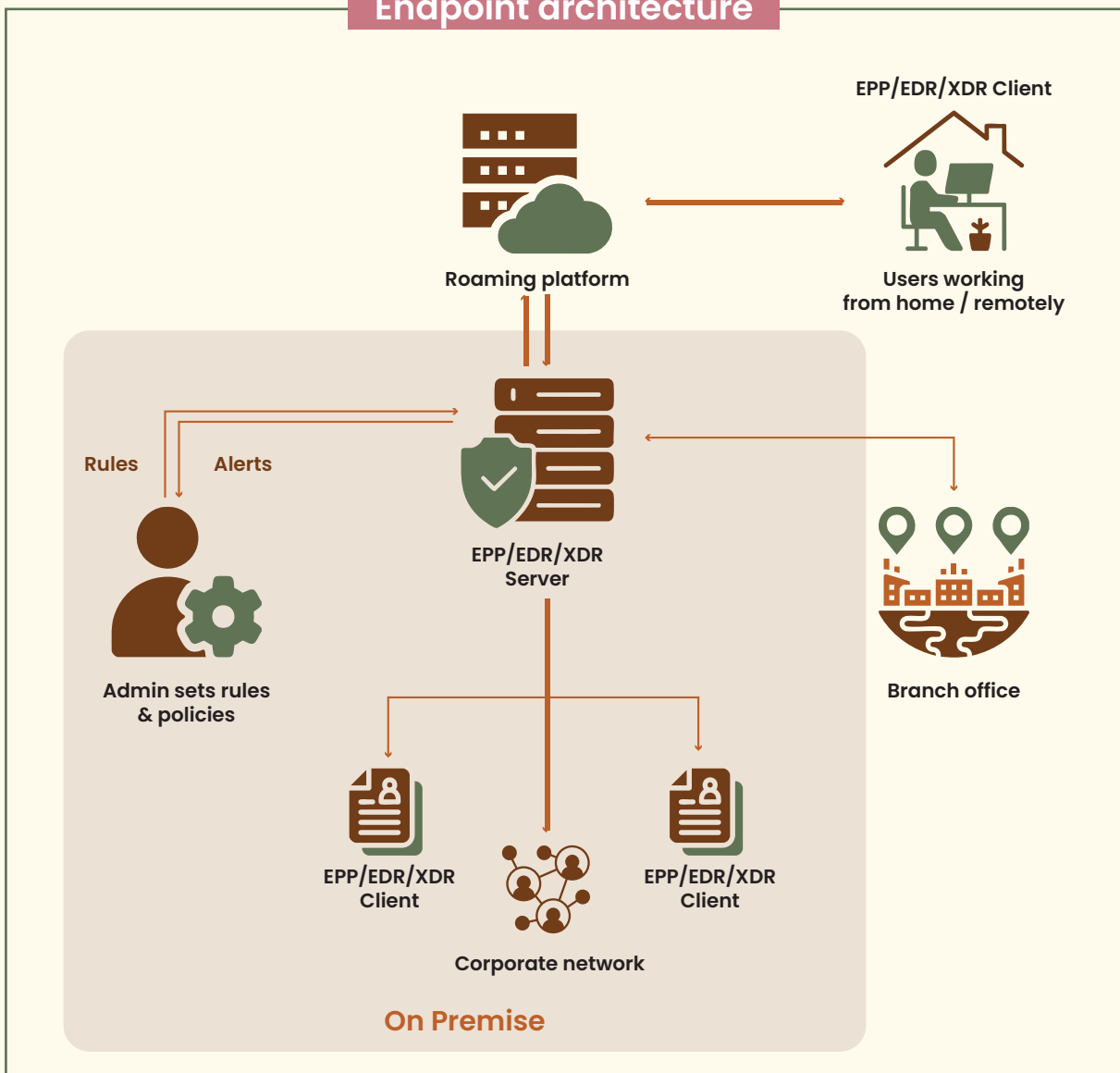
**The predominance of network-based detection (78.39%) is driven by:**

- ▲ Increased sophistication of network-based attacks
- ▲ Growth in cloud-based services
- ▲ Rise in remote workforce connectivity
- ▲ Advanced persistent threats (APTs)
- ▲ Complex malware distribution networks

## Primary detection distribution and strategic enhancement priorities

Detection Type	Percentage	Volume Impact	Primary Function	Short-term Focus	Mid-term Goals	Long-term Vision
Network Scans	78.39%	High 	Real-time threat detection	Enhanced monitoring	AI integration	Autonomous response
File-based	21.08%	Medium 	Static analysis & verification	Pattern optimization	Advanced analytics	Predictive detection
Memory Scans	0.48%	Low 	Runtime threat monitoring	Coverage expansion	Real-time analysis	Complete protection
Email Security	0.05%	Specialized	Targeted email protection	Filtering enhancement	Advanced detection	Predictive detection

## Endpoint architecture

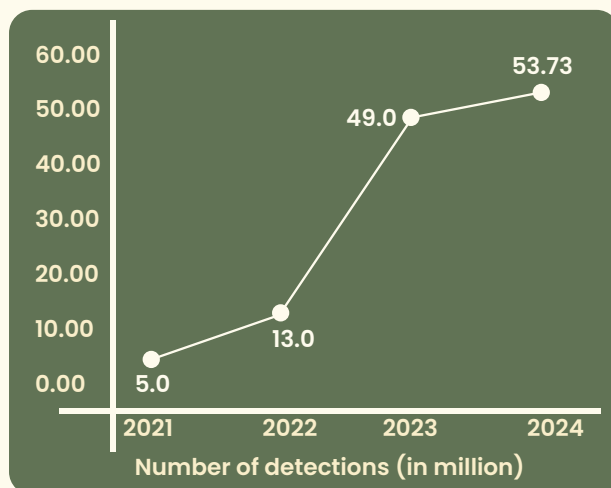


## Behavioral-Based Detection Landscape:

---

The dramatic increase in behavioral-based detections from 5 million in 2021 to 53.73 million in 2024 represents a paradigm shift in cybersecurity defense mechanisms. This 974.6% growth over three years signals not just an improvement in detection capabilities, but a fundamental transformation in how threats are identified and contained.

---



### Drivers behind the surge

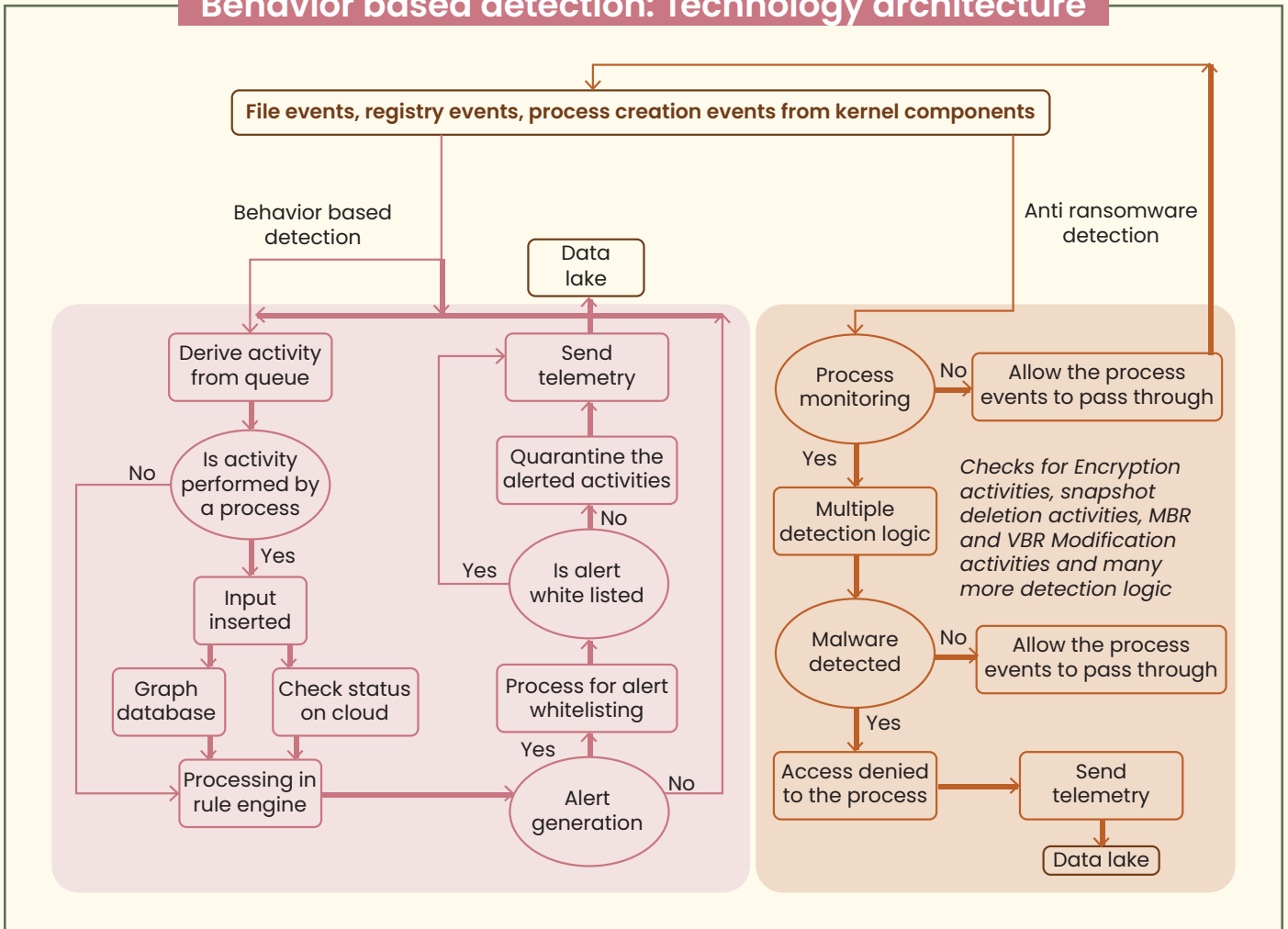
It can be attributed to several converging factors. First, the evolution of modern threats has rendered traditional signature-based detection increasingly insufficient. Sophisticated attackers now employ advanced techniques such as polymorphic malware, fileless attacks, and living-off-the-land tactics that easily evade conventional detection methods.

Additionally, the rise in zero-day exploits and advanced persistent threats (APTs) has necessitated a more dynamic approach to threat detection. The limitations of signature-based detection, primarily its reactive nature and inability to identify unknown threats, have pushed organizations toward behavioral analysis as a more effective security measure.

### Technological enablement and maturity

The significant growth in behavioral detections also reflects the maturation of underlying technologies. The integration of artificial intelligence and machine learning has dramatically enhanced the capability to analyze and identify suspicious patterns in real-time. Advanced processing capabilities and improved algorithms have made it possible to monitor and analyze vast amounts of behavioral data efficiently.

## Behavior based detection: Technology architecture

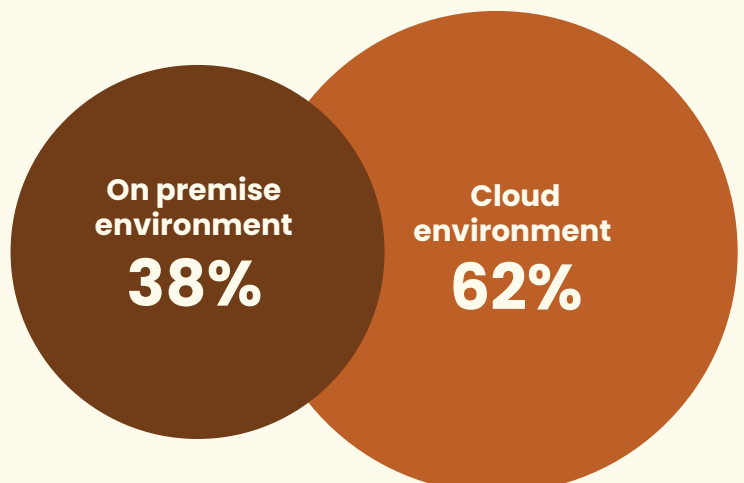



## Strategic considerations

For organizations, the rise in behavioral detections necessitates a strategic shift in security planning and implementation. This includes not only technological investments but also changes in security processes and team capabilities. The focus must extend beyond tool deployment to include enhanced analytical capabilities, improved incident response procedures, and better integration with existing security infrastructure.

## Detection Metrics across Infrastructure Types

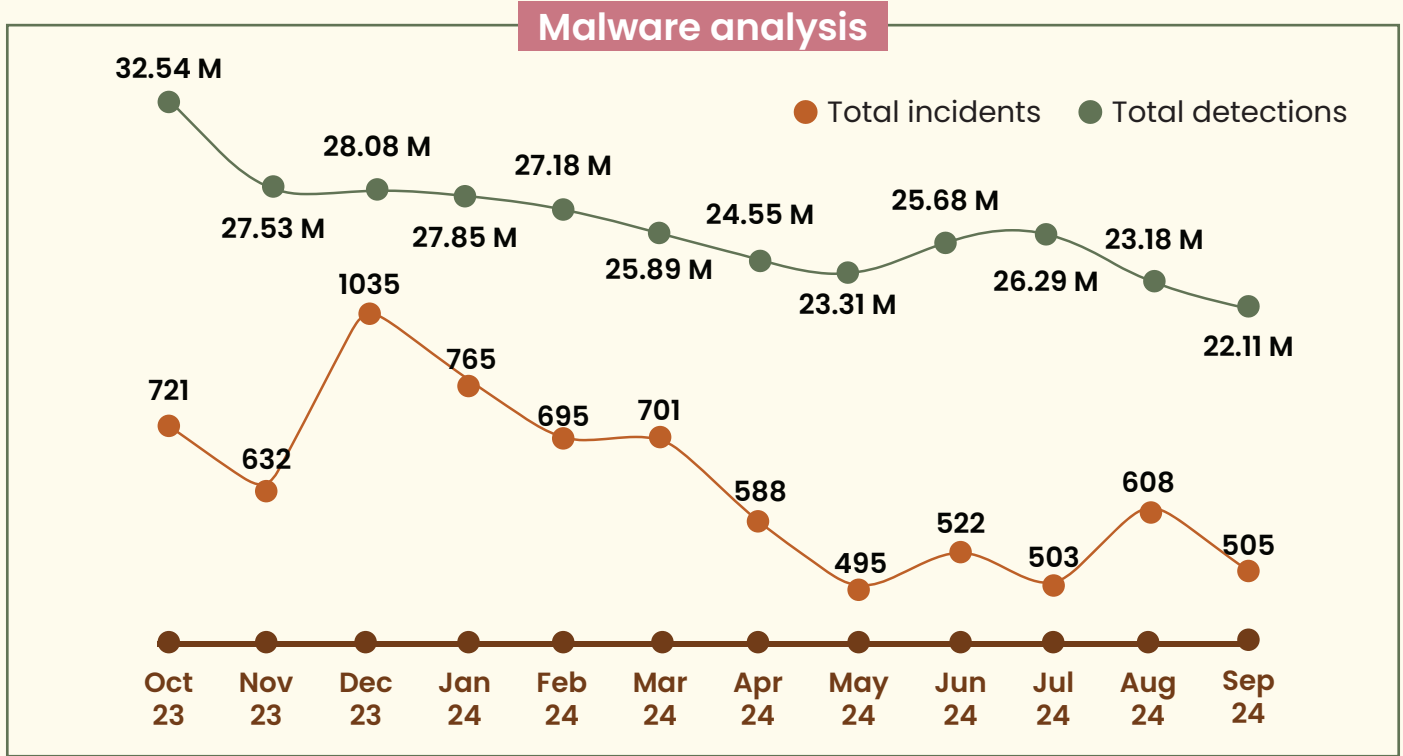
Cloud environment accounts for 62% of total detections (averaging 3.02 detections per endpoint) and on-premises environments contributing 38% (averaging 1.88 detections per endpoint).



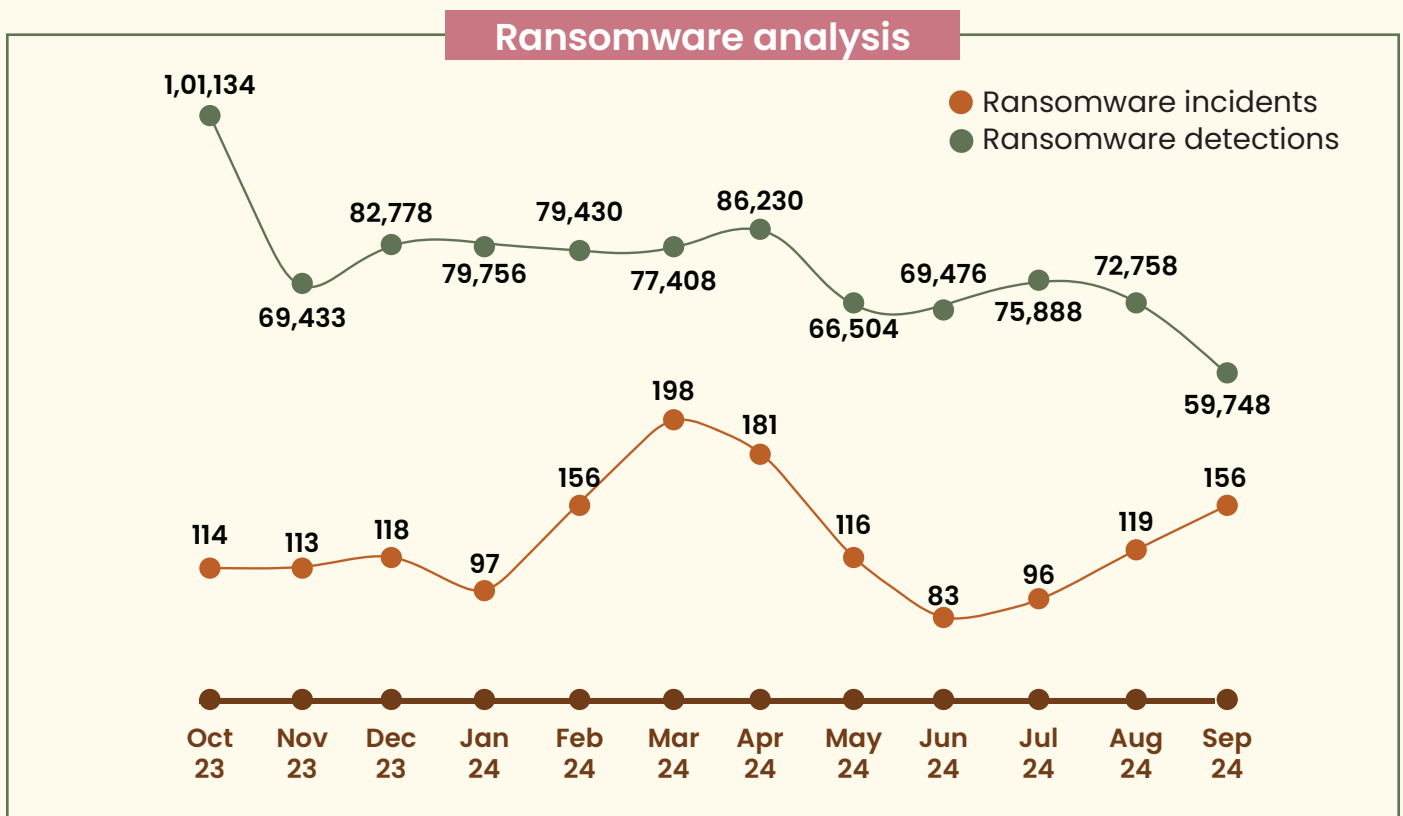
- 
- ▲ Cloud environment show a significantly higher detection rate, reflecting their growing prominence in enterprise operations. This trend can be attributed to:
    - 🌐 **Increased adoption of cloud services:** Organizations are rapidly migrating to the cloud, expanding their attack surface and consequently facing a higher volume of threats.
    - 🌐 **Advanced detection tools:** Cloud-native solutions often incorporate modern detection technologies, such as AI and machine learning, that provide better visibility and faster response times.
  - ▲ While on-premise environment account for a smaller share of detections, their lower average detection rate suggests possible gaps in visibility or security focus. On-premise environment may rely on older detection tools that are less equipped to handle modern threats.
    - 🌐 **Strategic Implications:** Organizations must recognize the growing dominance of cloud-based threats while ensuring balanced attention to both cloud and on-premises security. It is vital to implement advanced cloud workload protection platforms (CWPPs) for comprehensive threat coverage. It is important to perform regular security audits to identify gaps in endpoint detection and response (EDR) systems.

# Malware and Ransomware Analysis 2024

In 2024, malware analysis indicates 1 malware incident per 40,436 detections.

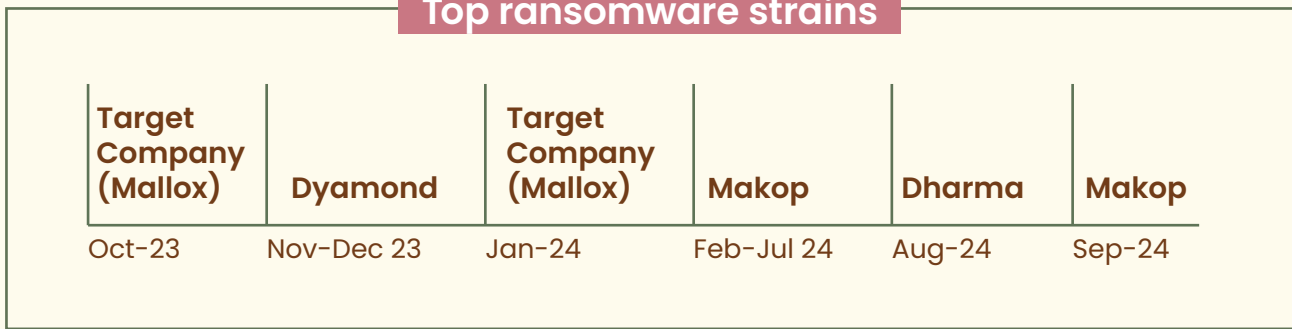


Ransomware analysis indicates 1 ransomware incident per 595 detections in 2024 showing strong detection and prevention capabilities.





## Top ransomware strains



## Malware of Prominence: Year 2024

This section provides an in-depth analysis of various malware threats encountered in 2024, detailing their number of detections, propagation methods, behavioral patterns, and potential impacts on affected systems. Understanding these characteristics is crucial for developing effective detection, prevention, and mitigation strategies to safeguard against evolving threats. **The total detections for the specified malware variants amount to 77.96 million, which constitutes 21.12% of the overall malware detections.**

### W32.Pioneer.CZ1

Number of Detections: 46.53 Million

Threat Level: Medium ■■

Category: File Infector

Propagation Vectors:

Removable media (e.g., USB drives), network-shared drives

#### Behavior:

- ▲ **File Injection:** Injects malicious code into executable files located on local storage and shared network drives, thereby compromising both individual systems and network resources.
- ▲ **DLL Dropping:** Decrypts embedded malicious dynamic link libraries (DLLs) from infected executables and deposits them onto the filesystem, enabling persistent and stealthy malicious activities.
- ▲ **Command and control (C2) Communication:** The deployed DLL conducts unauthorized operations, including system reconnaissance, data exfiltration, and communication with remote C&C servers to receive further instructions or updates.

# LNK.Cmd.Exploit

Number of Detections: 6.55 million

Threat Level: High 

Category: Trojan

Propagation Vectors: Email attachments, compromised/malicious websites

## Behavior:

- ▲ **File Injection:** Injects malicious code into executable files located on local storage and shared network drives, thereby compromising both individual systems and network resources.
- ▲ **DLL Dropping:** Decrypts embedded malicious dynamic link libraries (DLLs) from infected executables and deposits them onto the filesystem, enabling persistent and stealthy malicious activities.
- ▲ **Command and control (C2) Communication:** The deployed DLL conducts unauthorized operations, including system reconnaissance, data exfiltration, and communication with remote C&C servers to receive further instructions or updates.

# Trojan.Starter.YY4

Number of Detections: 4.44 Million

Threat Level: High 

Category: Trojan

Propagation Vectors: Email attachments, compromised/malicious websites

## Behavior:

- ▲ **Process Creation:** Initiates new processes to execute dropped malicious executables, ensuring persistent and continuous malicious activity within the infected system.
- ▲ **Registry Manipulation:** Alters critical system registry settings, potentially leading to system instability, crashes, or compromised security configurations.
- ▲ **Secondary Malware Deployment:** Downloads and installs additional malware components, such as keyloggers, to enhance data theft capabilities and expand the infection footprint.
- ▲ **System Performance Degradation:** Significantly slows down the system's boot and shutdown processes, disrupting normal operations and reducing user productivity.
- ▲ **Data Exfiltration:** Facilitates the theft of sensitive information, including credit card details and personal data, by providing unauthorized access to compromised systems.

## Nsis.Bitmin

Number of Detections: 1.38 Million

Threat Level: High 

Category: Cryptocurrency Miner

Propagation Vectors: Phishing emails, malicious hyperlinks, compromised websites

### Behavior:

- ▲ **Resource Exploitation:** Engages in excessive CPU and GPU usage to maximize cryptocurrency mining efficiency, leading to notable system performance degradation.
- ▲ **Thermal Stress Induction:** Causes CPU overheating by maintaining high utilization levels without corresponding legitimate application demands, potentially damaging hardware.
- ▲ **System Sluggishness:** Impairs the responsiveness and launch times of other applications due to monopolized system resources, adversely affecting overall device performance.

## Trojan.Shadowbrokers

Number of Detections: 0.19 Million

Threat Level: High 

Category: Trojan

Propagation Vectors: Malicious hyperlinks, compromised/malicious websites

### Behavior:

- ▲ **SMB Exploitation:** Targets and exploits vulnerabilities in the Server Message Block (SMB) protocol to facilitate unauthorized access and propagation across networks.
- ▲ **Self-Deletion Mechanism:** Deploys batch scripts designed to remove its own malicious files post-execution, evading detection and analysis.
- ▲ **PE File Deployment:** Drops Portable Executable (PE) files into the C:\Windows directory with names mimicking legitimate system processes (e.g., svchost.exe) to blend in and avoid suspicion, subsequently initiating these files to maintain persistence.
- ▲ **Network Reconnaissance:** Utilizes ping.exe to perform network mapping and status checks of other devices and networks, aiding in the identification of additional targets for compromise.

# W32.Mofksys.A4

Number of Detections: 2.00 million

Threat Level: High 

Category: Worm

Propagation Vectors: Removable media (e.g., USB drives), network-shared drives

## Behavior:

- ▲ **File Propagation:** Replicates itself by copying to critical system paths, including <System>\explorer.exe, <Windows>\svchost.exe, and <Windows>\spoolsv.exe, thereby embedding itself within essential system processes.
- ▲ **Persistence Mechanism:** Adds its executable paths to the RunOnce registry key, ensuring that the worm executes automatically upon system startup or reboot.
- ▲ **Surveillance Capabilities:** Implements keylogging and screen capture functionalities to monitor user inputs and screen activity, transmitting the harvested data to remote attackers for further exploitation.
- ▲ **System Compromise:** Facilitates unauthorized access and control over the infected system, enabling the execution of additional malicious activities as directed by remote adversaries.

## Key takeaways

### Prevalence of file infectors and trojans:

Multiple threats exhibit file infection and Trojan-like behaviors, emphasizing the need for robust file integrity monitoring and behavioral analysis.

### Advanced propagation techniques:

Exploitation of network protocols (e.g., SMB) and the use of legitimate system processes for malicious purposes demonstrate the sophistication of modern malware.

### Rise of cryptocurrency miners:

The presence of mining-specific malware like Nsis.Bitmin highlights the increasing trend of leveraging compromised systems for unauthorized financial gain.

### Resource exploitation And system degradation:

Many threats focus on maximizing system resource usage, leading to performance issues and potential hardware damage, which can indirectly impact organizational productivity and operational continuity.

# Top Network Based Exploits

## Detailed Malware Profiles

**0.17M\*** TCP/CrimsonRatIP.UN!AR.43879

**0.34M\*** DNS/MinerBot.CnC!PT.42350

**1.01M\*** HTTP/MoneroMiner.CnC!PT.3902

**1.37M\*** HTTP/RD-PlugX.APT!SP.38697

**9.59M\*** HTTP/Coinminer.CnC!SP.4843

\*Detection Count

This section provides an in-depth analysis of specific malware detection signatures identified in 2024. Each profile outlines the malware's characteristics, propagation methods, behaviors, and associated network-based exploits, offering valuable insights for cybersecurity professionals to enhance detection and mitigation strategies.

### HTTP/CoinMiner.CnC!SP.4843

#### Description:

HTTP/CoinMiner.CnC!SP.4843 is a sophisticated cryptocurrency miner malware variant that masquerades as a legitimate Flash updater. Once executed, it clandestinely engages in unauthorized cryptomining activities on infected devices without the user's knowledge.

#### Propagation methods:

- 🌐 **Fake software updates:** Disguised as a Flash Player update, enticing users to download and install the malicious software.
- 🌐 **Phishing campaigns:** Delivered through deceptive emails and malicious websites that lure users into downloading the malware.

#### Behavior:

- 🌐 **Cryptocurrency mining:** Utilizes system resources to mine cryptocurrencies, primarily targeting digital currencies like Bitcoin and Monero.
- 🌐 **Command and control (C2) communication:** Establishes connections with multiple CnC servers to receive instructions and report mining progress.
- 🌐 **Stealth operations:** Operates in the background to avoid detection, maintaining minimal impact on system performance to prolong its presence.

#### Impact:

- 🌐 **Resource exploitation:** Leads to significant CPU and GPU usage, causing system slowdowns and overheating.
- 🌐 **Financial loss:** Indirect financial impact through increased energy consumption and potential hardware damage.
- 🌐 **Security risks:** Opens additional vulnerabilities by establishing persistent CnC channels that could be exploited for further malicious activities.

## HTTP/MoneroMiner.CnC!PT.3902

### Description:

HTTP/MoneroMiner.CnC!PT.3902 targets the Monero (XMR) cryptocurrency, leveraging its privacy-centric blockchain to conduct mining operations while obscuring transaction activities. This malware variant blends malicious traffic with legitimate web traffic, complicating detection efforts.

### Propagation methods:

- 🌐 **Malicious downloads:** Embedded within compromised websites and drive-by downloads that trick users into installing the malware.
- 🌐 **Exploited vulnerabilities:** Takes advantage of unpatched software vulnerabilities to infiltrate systems without user interaction.

### Behavior:

- 🌐 **Monero mining:** Engages system resources to mine Monero, a cryptocurrency favored for its enhanced privacy features.
- 🌐 **Obfuscated communication:** Uses HTTP channels to communicate with CnC servers, making it difficult to distinguish between legitimate and malicious traffic.
- 🌐 **Persistence mechanisms:** Implements techniques such as registry modifications and scheduled tasks to maintain long-term presence on infected systems.

### Impact:

- 🌐 **Performance degradation:** Causes noticeable slowdowns and increased power consumption due to continuous mining activities.
- 🌐 **Hardware stress:** Prolonged high usage can lead to hardware wear and potential failure.
- 🌐 **Security concerns:** Maintains persistent CnC connections that can be exploited for additional malicious purposes.

## HTTP/RD-PlugX.APT!SP.38697 - (ShadowPad APT Backdoor)

### Description:

ShadowPad APT Backdoor is a multi-module malware developed in C and Assembly, designed to operate on both 32-bit and 64-bit Microsoft Windows systems. It is employed in targeted attacks on information systems to gain unauthorized data access and exfiltrate information to remote CnC servers.

### Propagation methods:

- 🌐 **Spear phishing:** Delivered through highly targeted phishing emails containing malicious attachments or links.
- 🌐 **Exploited vulnerabilities:** Utilizes zero-day exploits and known vulnerabilities to infiltrate secure environments.

### Behavior:

- 🌐 **Multi-Module architecture:** Comprises various hardcoded plug-ins that provide core functionalities such as data exfiltration, system reconnaissance, and lateral movement within networks.
- 🌐 **Data theft:** Collects sensitive information from compromised systems and transmits it to designated CnC servers.
- 🌐 **Stealth techniques:** Employs encryption and obfuscation to evade detection by traditional security solutions.

### Impact:

- 🌐 **Data breach:** Facilitates the unauthorized access and theft of confidential and proprietary information.
- 🌐 **Network compromise:** Enables attackers to move laterally within networks, compromising additional systems.
- 🌐 **Long-Term Presence:** Establishes persistent access points that can be exploited for extended periods, increasing the risk of sustained data loss.

## HTTP/RD-PlugX.APT!SP.38697 - (DOPLUGS)

### Description:

DOPLUGS is a customized variant of the PlugX malware, primarily serving as a downloader for more prevalent PlugX payloads. A notable variant of DOPLUGS includes an integrated “Kill Someone” module, functioning as a USB worm designed for malware propagation, document theft, and data harvesting.

### Propagation Methods:

- 🌐 **Malicious USB devices:** Spreads through infected USB drives, exploiting autorun features to install malware on connected systems.
- 🌐 **Malicious downloads:** Bundled with legitimate software downloads or delivered via compromised websites.

### Behavior:

- 🌐 **Payload delivery:** Downloads and installs additional PlugX payloads, enhancing the malware’s capabilities.
- 🌐 **USB worm functionality:** The “Kill Someone” module facilitates the spread of malware via USB devices, steals sensitive documents, and collects user data.
- 🌐 **Context menu integration:** Adds malicious entries to the system’s context menu, allowing for easier execution and persistence of the malware.

### Impact:

- 🌐 **Widespread infection:** Enables rapid propagation across networks and connected devices through USB drives.
- 🌐 **Data theft:** Steals valuable documents and personal information, posing significant privacy and security risks.
- 🌐 **System disruption:** Can lead to system instability and crashes due to the execution of malicious payloads and the alteration of system settings.

## DNS/MinerBot.CnC!PT.42350

### Description:

DNS/MinerBot.CnC!PT.42350 exploits vulnerabilities in internet-facing servers, particularly those with exposed RDP and SMB ports. By accessing systems via compromised DNS servers, it conducts cryptojacking activities, utilizing company resources for unauthorized cryptocurrency mining.

### Propagation methods:

- 🌐 **Exposed ports:** Targets systems with open RDP and SMB ports, exploiting them to gain unauthorized access.
- 🌐 **DNS server exploits:** Utilizes compromised DNS servers to infiltrate and distribute the malware across networks.

### Behavior:

- 🌐 **Cryptojacking:** Engages in unauthorized cryptocurrency mining, leveraging company resources to generate profits for attackers.
- 🌐 **Stealth operations:** Operates covertly to avoid detection, maintaining low system visibility while consuming significant resources.
- 🌐 **Resource exploitation:** Maximizes CPU and GPU usage for mining activities, leading to system performance degradation.

### Impact:

- 🌐 **Performance degradation:** Causes significant slowdowns and increased energy consumption, impacting overall system performance and operational efficiency.
- 🌐 **Hardware stress:** Prolonged high resource usage can lead to hardware overheating and potential failures.
- 🌐 **Security vulnerabilities:** Exploits open ports to gain unauthorized access, highlighting the importance of securing internet-facing servers.



## TCP/CrimsonRatIP.UN!AR.43879

### Description:

TCP/CrimsonRatIP.UN!AR.43879 is a Remote Access Trojan (RAT) utilized by the APT36 group, also known as Transparent Tribe, which primarily targets the education sector. This RAT facilitates unauthorized remote control over infected systems, enabling attackers to manipulate compromised devices for various malicious purposes.

### Propagation methods:

- 🌐 **Malicious office documents:** Distributed through deceptive Office documents embedded with malicious macros or OLE objects.
- 🌐 **Spear phishing:** Delivered via targeted phishing campaigns aimed at educational institutions and associated personnel.

### Behavior:

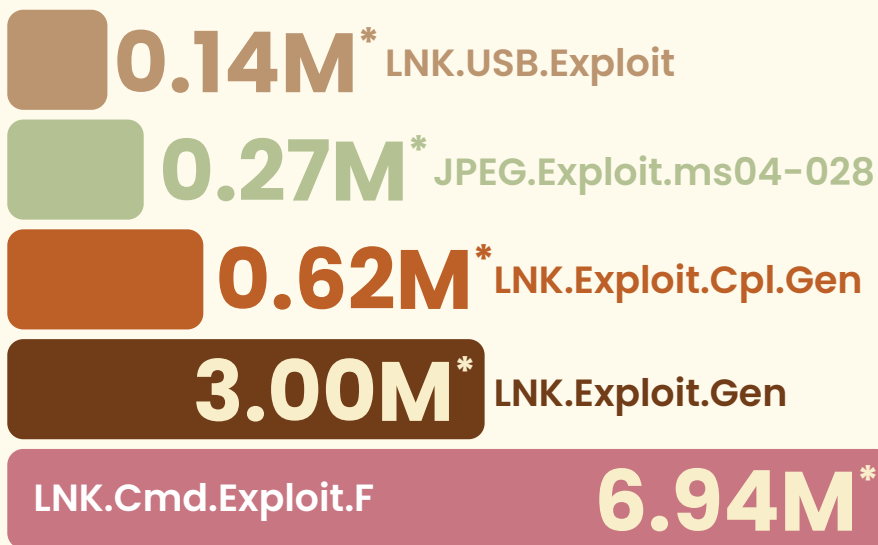
- 🌐 **Remote control:** Grants attackers full remote access to infected systems, allowing for data manipulation, theft, and system control.
- 🌐 **OLE embedding and macros:** Utilizes Object Linking and Embedding (OLE) techniques and Office macros to execute malicious payloads upon document interaction.
- 🌐 **Malware updates:** Regularly updates itself and its components to evade detection and enhance functionality.

### Impact:

- 🌐 **Data theft and manipulation:** Enables the exfiltration and alteration of sensitive data, posing significant risks to institutional integrity and privacy.
- 🌐 **System compromise:** Facilitates deep infiltration into networks, allowing for the compromise of multiple systems and the potential for broader network attacks.
- 🌐 **Operational disruption:** Can lead to significant operational disruptions within targeted educational institutions, affecting both administrative and academic functions.

# Top Host Based Exploits 2024

The table below provides a comprehensive overview of host-based exploits detected in 2024.



\*Detection Count

Host-based exploits have demonstrated significant prevalence and sophistication, with **LNK.Cmd.Exploit.F** leading the detections at **6.94 million**, followed by **LNK.Exploit.Gen** with **3 million** detections. These exploit variants leverage deceptive methods such as phishing campaigns and malicious downloads to infiltrate systems, exploiting vulnerabilities in link (.lnk) files and component libraries (.cpl). The widespread use of these exploits results in substantial resource exploitation, causing system slowdowns, overheating, and heightened security risks through persistent Command and control (CnC) channels. Additionally, specialized exploits like **JPEG.Exploit.ms04-028** and **LNK.USB.Exploit** highlight the diversification of attack vectors, targeting both software vulnerabilities and physical access points.

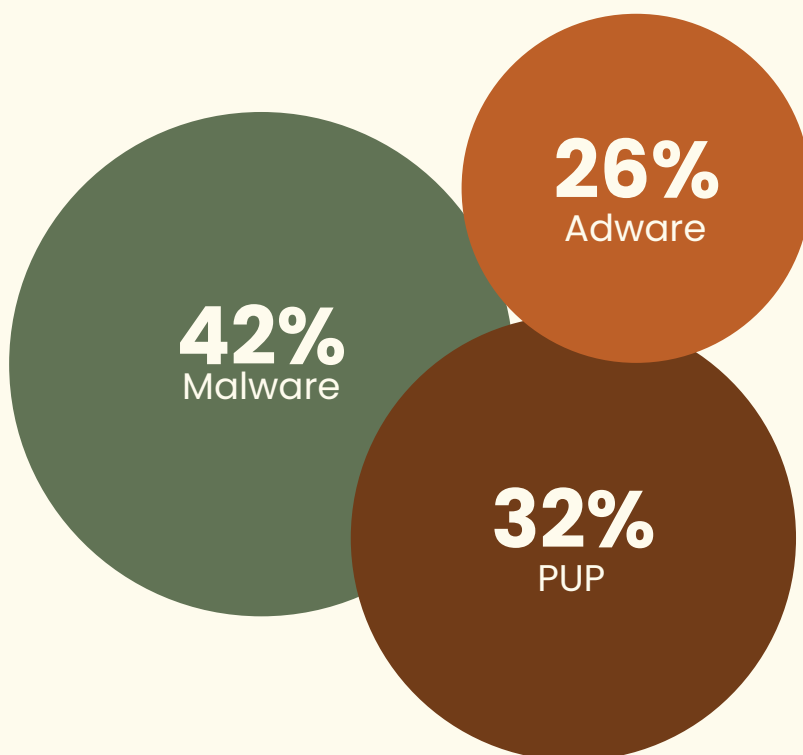
Malware Name	Family	Description	Propagation Methods	Behavior
LNK.Exploit.Gen	Pantera, Dorkbot, Jenxcus	A collection of Trojans and worms exploiting .lnk files to perform unauthorized activities such as data theft, system manipulation, and malware distribution without user knowledge.	<p><b>Phishing Emails:</b> Malicious attachments or links.</p> <p><b>Infected USB Drives:</b> Exploiting autorun features.</p> <p><b>Compromised Websites:</b> Drive-by downloads.</p>	<p><b>Remote Access:</b> Establishes connections for data exfiltration.</p> <p><b>System Reconnaissance:</b> Collects system information.</p> <p><b>Malware Deployment:</b> Drops additional malware.</p> <p><b>DoS Attacks:</b> Initiates denial-of-service operations.</p>

Malware Name	Family	Description	Propagation Methods	Behavior
LNK.Cmd.Exploit.F	Dinihou	A worm that spreads via removable drives and malicious downloads, autonomously replicating to infect multiple systems and facilitating further malware distribution.	<p><b>Removable Drives:</b> Copies itself to all connected USB devices.</p> <p><b>Malicious Websites:</b> Drive-by downloads.</p> <p><b>Email Attachments:</b> Spreads through infected files.</p>	<p><b>Autonomous Replication:</b> Spreads without user intervention.</p> <p><b>Network Propagation:</b> Uses network shares and email to infect additional systems.</p> <p><b>Persistence:</b> Ensures automatic execution on startup.</p>
LNK.Exploit.Cpl.Gen	CVE-2010-2568	Exploits a buffer overflow vulnerability in Microsoft GDI+ via malicious .lnk files, allowing remote code execution on vulnerable Windows systems.	<p><b>Malicious Shortcut Files:</b> Distributed via emails and compromised websites.</p> <p><b>Exploited Applications:</b> Targets software relying on GDI+ for image handling.</p>	<p><b>Buffer Overflow:</b> Triggers remote code execution by exploiting GDI+ vulnerability.</p> <p><b>Heap Management Manipulation:</b> Alters exception handling to execute arbitrary code.</p> <p><b>Stealth Execution:</b> Evades detection through obfuscation.</p>
LNK.USB.Exploit	winlnk, Bundpil, Linx	A set of Trojans and worms leveraging .lnk files on USB drives to launch malicious executables, steal data, and disrupt system operations.	<p><b>Infected USB Drives:</b> Uses autorun to execute malicious .lnk files.</p> <p><b>Bundled Downloads:</b> Packs malware with legitimate software.</p> <p><b>Compromised Websites:</b> Hosts malicious links.</p>	<p><b>Executable Launch:</b> Runs malicious programs via .lnk files.</p> <p><b>Data Theft:</b> Steals sensitive documents and personal information.</p> <p><b>System Disruption:</b> Alters or deletes data and interferes with system processes.</p>

Malware Name	Family	Description	Propagation Methods	Behavior
JPEG.Exploit.ms04-028	ms04, ms04-028	Exploits a buffer overflow in Microsoft GDI+ when processing specially crafted JPEG files, enabling remote code execution on vulnerable Windows XP systems.	<p><b>Malicious JPEG Files:</b> Distributed via emails and compromised websites.</p> <p><b>Drive-By Downloads:</b> Automatically downloads when visiting malicious sites.</p>	<p><b>Buffer Overflow:</b> Overruns buffer in GDI+ to execute arbitrary code.</p> <p><b>Heap Manipulation:</b> Alters exception handling to gain control.</p> <p><b>Stealth Execution:</b> Minimizes detection by blending with legitimate processes.</p>

## Android Threat Detections 2024

The analysis of Android-based security detections reveals a concerning distribution of threats across three main categories. **Malware** emerges as the predominant threat, accounting for **42%** of all detections, indicating a significant presence of malicious software targeting Android devices. **Potentially Unwanted Programs (PUPs)** follow as the second most common threat at **32%**, suggesting a substantial volume of questionable applications that may compromise device security or user privacy. **Adware** represents **26%** of detections, highlighting the persistent presence of aggressive advertising software that can degrade user experience and potentially serve as vectors for other threats.



# Top Zero Days 2024

---

Zero-day exploits are highly prized in the cybercrime underground due to their ability to bypass traditional security measures, enabling unauthorized access, data theft, system compromise, and the deployment of malicious payloads without detection.

This section outlines top zero days identified in 2024, detailing their nature, potential impacts, and associated CVE identifiers.

## **Ivanti Connect Secure Command Injection (CVE-2024-21887)**

A severe remote command execution vulnerability that allows attackers to execute unauthorized shell commands due to improper input validation. While authentication is typically required, an associated authentication flaw enables attackers to bypass this requirement, facilitating full system compromise.

## **Microsoft Windows Shortcut Handler (CVE-2024-21412)**

A critical security bypass vulnerability in Windows' shortcut file processing. It enables remote code execution through specially crafted shortcut (.lnk) files, circumventing established security controls when users interact with these malicious shortcuts.

## **Ivanti Connect Secure Server-Side Request Forgery (SSRF) (CVE-2024-21893)**

This Server-Side request forgery vulnerability in the SAML component allows attackers to initiate unauthorized requests through the application. Successful exploitation grants access to internal network resources and enables the forwarding of malicious requests, leading to broader network compromise.

## **Mozilla Firefox Animation Timeline Use-After-Free (CVE-2024-9680)**

A use-after-free vulnerability in Firefox's animation timeline component that permits remote code execution when users visit specially crafted websites. This vulnerability can lead to full system compromise, posing significant security risks to users.

# Critical Security Vulnerabilities: Impact Analysis

## A Comprehensive Assessment of High-Impact CVEs

The analysis in the section examines five significant vulnerabilities that have emerged, presenting substantial risks to enterprise and consumer systems worldwide. These vulnerabilities span browser engines, operating system components, and enterprise applications, demonstrating the diverse nature of current cyber threats.

### Browser Security: V8 Engine Vulnerability

#### CVE-2024-5274

##### Technical overview:

A high-severity zero-day vulnerability discovered in the V8 JavaScript and WebAssembly engine represents a significant security risk. This type of confusion vulnerability marks the eighth zero-day patched during 2024.

##### Impact assessment:

- ▲ Severity: High
- ▲ Attack Vector: JavaScript execution
- ▲ Exploitation Status: Zero-day
- ▲ Affected Systems: Chromium-based browsers

##### Technical implications:

- ▲ Arbitrary code execution
- ▲ Memory manipulation
- ▲ System level access
- ▲ Remote attack surface

### Operating System Infrastructure

#### CVE-2024-38063

##### Technical details:

- ▲ CVSS Score: 9.8
- ▲ Attack Vector: Network
- ▲ Protocol: IPv6
- ▲ Exploitation: Remote
- ▲ Status: Active threats

##### Attack requirements

- ▲ Crafted IPv6 packets
- ▲ Network access
- ▲ Vulnerable windows TCP/IP stack

##### Attack methodology:

The vulnerability enables remote code execution through specially crafted IPv6 packets, allowing attackers to compromise systems without authentication. The high CVSS score reflects the ease of exploitation and potential impact.

## System Component Vulnerability

### CVE-2024-43491

#### Technical details:

##### Affected systems

- ▲ Windows 10 version 1507
- ▲ Enterprise 2015 LTSB
- ▲ IoT Enterprise 2015 LTSB

#### Technical details:

##### Vulnerability characteristics

- ▲ RCE capability
- ▲ CVSS Score: 9.8
- ▲ Active exploitation
- ▲ Update stack impact

#### Root cause analysis:

The vulnerability stems from a code defect in the servicing stack, triggered by a March 2024 security update. This flaw affects the handling of optional components, reverting systems to vulnerable states.

## Enterprise Application Security

### CVE-2024-32113

#### Vulnerability profile:

- ▲ System: Apache OFBiz
- ▲ Type: Path traversal
- ▲ Impact: Command execution
- ▲ Status: Actively exploited
- ▲ Affected Versions: Pre-18.12.13

#### Technical impact:

- ▲ Directory traversal
- ▲ Arbitrary command Execution
- ▲ System compromise
- ▲ Data breach risk

#### Attack vector analysis:

The vulnerability exploits insufficient input validation, allowing attackers to bypass directory restrictions through traversal sequences. This can lead to unauthorized command execution and system compromise.

## Legacy Component Exploitation

### CVE-2024-38112

#### Technical assessment:

- ▲ Component: MSHTML
- ▲ Attack Type: Zero-day
- ▲ Exploitation: Active APT
- ▲ Vector: Spear-phishing
- ▲ Impact: Data theft

#### Attack chain:

- ▲ Phishing delivery
- ▲ PDF masquerading
- ▲ ZIP exploitation
- ▲ Malware deployment
- ▲ Data exfiltration





# INDIA MALWARE LANDSCAPE



# Top 10 States with Highest Malware Detections

The analysis reveals that **51.13%** of total national security detections are concentrated across ten states, indicating significant regional variations in cyber threat exposure and security incident patterns.

## High Detection Density States

### Telangana

- ▲ Highest detection rate: 55.90 detections/endpoint (**15.03%**)
- ▲ Likely influenced by Hyderabad's IT corridor
- ▲ Suggests sophisticated threat detection capabilities



### Tamil Nadu

- ▲ Second highest: 44.54 detections/endpoint (**11.97%**)
- ▲ Strong correlation with Chennai's tech hub status
- ▲ Indicates robust security monitoring infrastructure



### Delhi

- ▲ Third position: 43.86 detections/endpoint (**11.79%**)
- ▲ Capital region's high-value targets
- ▲ Dense business hub



## Regional Clustering Analysis Southern Technology Belt

**Combined contribution: 36.37%**

**States:** Telangana, Tamil Nadu, Karnataka

### Characteristics:

- ▲ High technology sector presence
- ▲ Advanced security infrastructure
- ▲ Greater digital service adoption

## Northern Business Corridor

**Aggregate share: 30.30%**

**States:** Delhi, Rajasthan, UP

### Drivers

- ▲ Diverse business landscape
- ▲ Varying urban-rural digital divide
- ▲ Mixed industry exposure

## Economic-Security Correlation Industrial States

**Gujarat: 38.44 detections/endpoint (10.34%)**

- ▲ Industrial exposure
- ▲ Manufacturing sector vulnerabilities

**Maharashtra: 23.65 detections/endpoint (6.36%)**

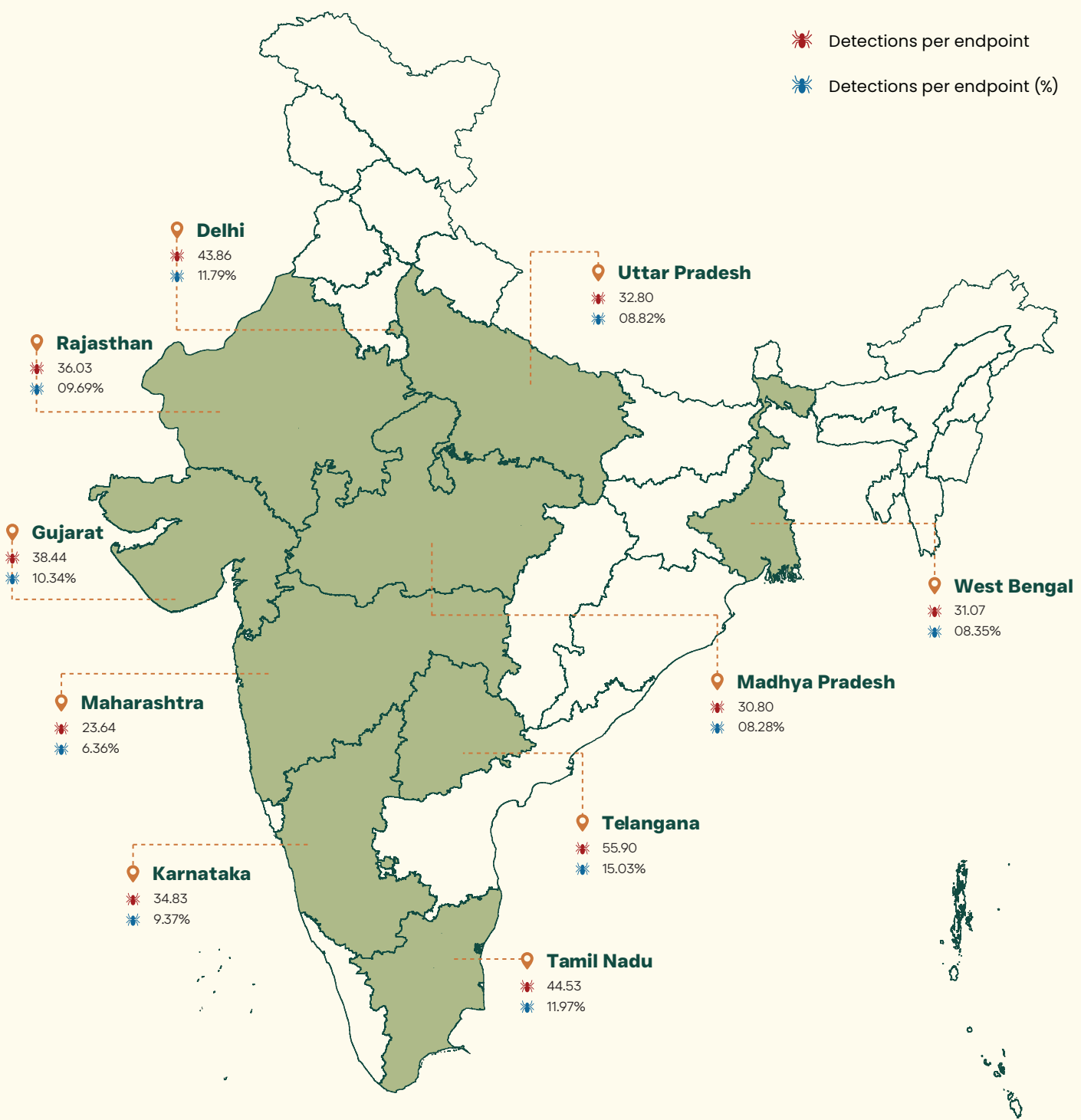
- ▲ Surprisingly low despite economic significance
- ▲ Potential underreporting or superior prevention

# Emerging Patterns

**Madhya Pradesh: 30.81 detections/endpoint**

**West Bengal: 31.07 detections/endpoint**

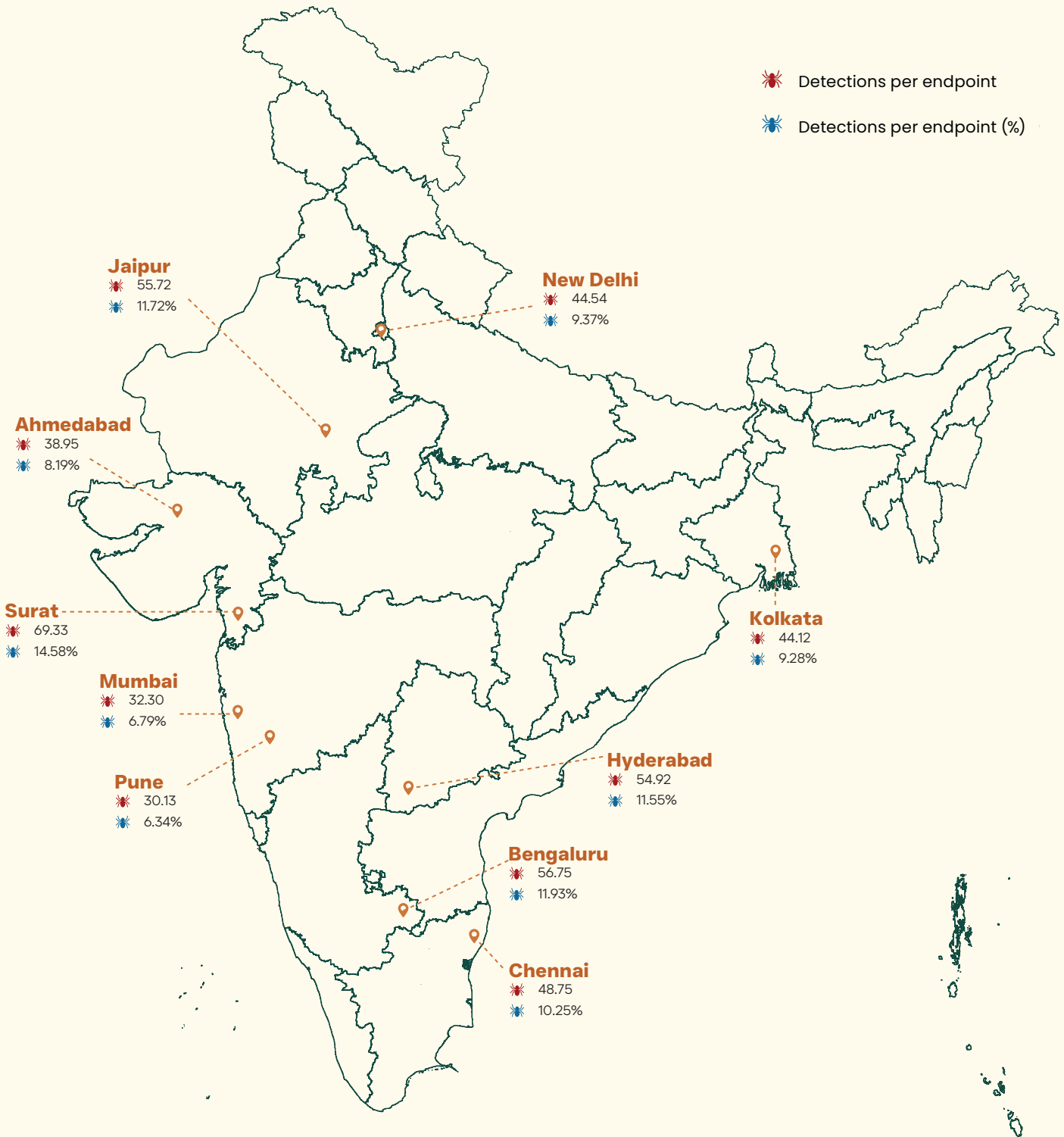
- ▲ Indicates growing digital adoption Infrastructure Impact
- ▲ Higher detections in states with better digital infrastructure
- ▲ Better internet penetration



Source: <https://www.surveeofindia.gov.in/pages/outline-maps-of-india>  
Disclaimer: The data has been rationalized and the insights provided are depicted as per Sqrite installation base.

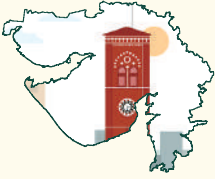
# Top 10 Cities with Highest Malware Detections

34.06% of detections originate from below mentioned cities.



Source: <https://www.surveymofindia.gov.in/pages/outline-maps-of-india>  
Disclaimer: The data has been rationalized and the insights provided are depicted as per Seqrite installation base.

## Surat: National Leader



Surat leads nationally with the highest detection rate of **69.34 detections per endpoint (14.58%)**. This position is unexpected given its industrial focus, suggesting either heightened security monitoring or increased exposure to cyber threats within the city.

## Technology Hubs

Technology-centric cities also exhibit significant detection rates:



**Bengaluru:**  
**56.75 detections per endpoint (11.93%)**



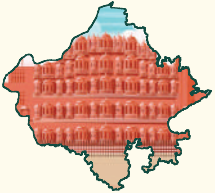
**Hyderabad:**  
**54.93 detections per endpoint (11.55%)**

Together, Bengaluru and Hyderabad account for **23.48%** of total detections, correlating with their substantial IT sector presence and the associated cyber threat landscape.

## Regional Business Centers

Detection rates in regional business centers are noteworthy:

Northern Cities:



**Jaipur:**  
**55.73 detections per endpoint (11.72%)**



**New Delhi:**  
**44.55 detections per endpoint (9.37%)**

Southern Metropolitan Areas:

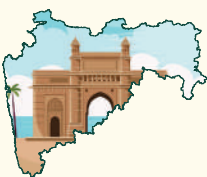


**Chennai:**  
**48.75 detections per endpoint (10.25%)**

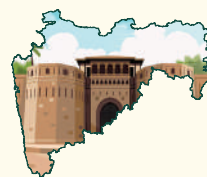
Chennai maintains a strong presence among top-tier metropolitan areas, reflecting its role as a key business center.

## Commercial Capitals

Commercial hubs like Mumbai and Pune demonstrate lower detection rates:



**Mumbai:**  
**32.30 detections per endpoint (6.79%)**

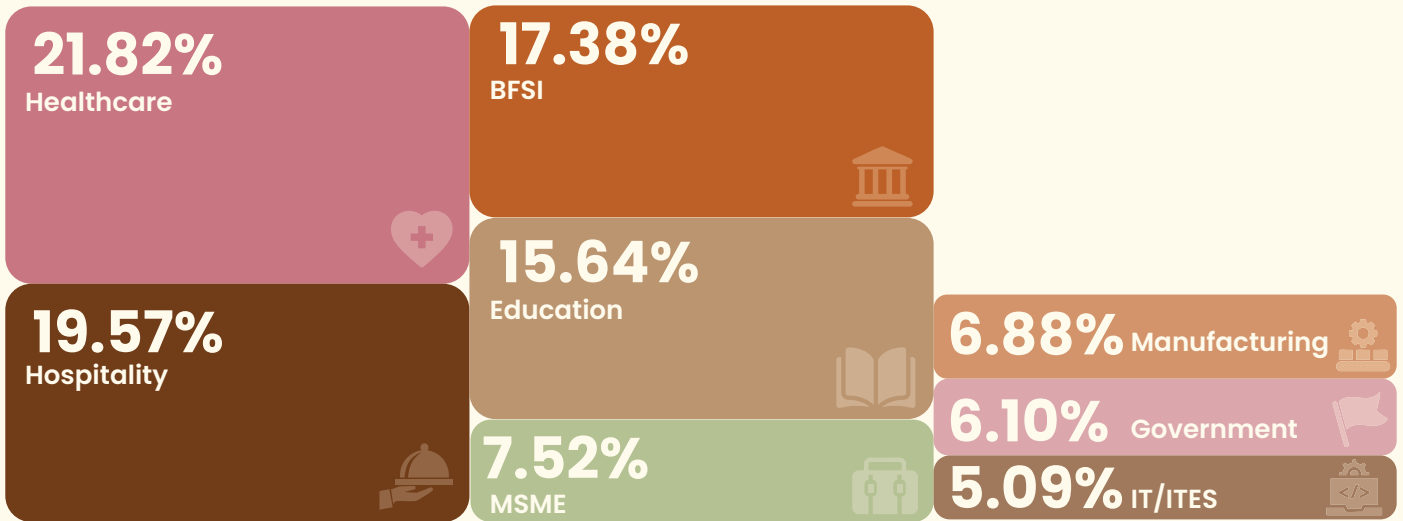


**Pune:**  
**30.14 detections per endpoint (6.34%)**

Despite their high business activity, Mumbai and Pune contribute **13.13%** of total detections, indicating lower detection densities compared to technology and industrial hubs.

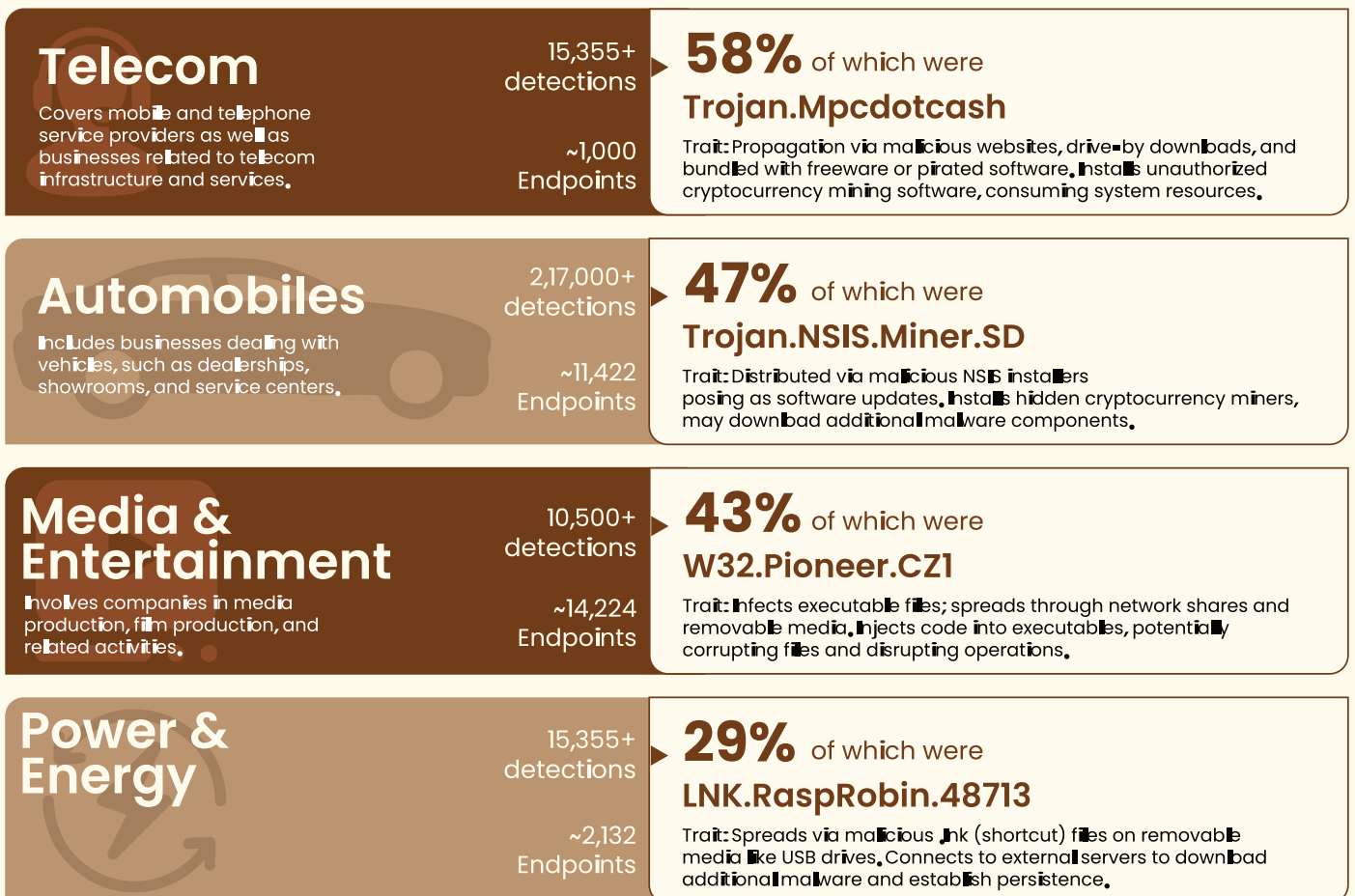
# Industry Insights


## Top industries with highest % of malware detections



For the purpose of visualization of the top affected industries, only those industries were considered where Seqrite's active installation base is more than 500.

## Industry view: Dominant malware %






**Logistics**  
Includes courier companies and logistics service providers.

11,000+ detections

~4,163 Endpoints

**27%** of which were **Trojan.Agent**

Trait: Propagates through various methods including phishing, malicious downloads, and exploiting software vulnerabilities. Performs activities like data theft, keylogging, and backdoor installation; behavior varies by variant.




**Healthcare**  
Covers all entities related to hospitals, clinics, pharmaceutical companies, and other medical-related businesses.

1,08,870+ detections

~24,287 Endpoints

**22%** of which were **Trojan.Shadowbrokers**

It propagates in healthcare systems by exploiting unpatched vulnerabilities (e.g., SMBv1) in legacy systems, medical devices, and networked infrastructure. It spreads via phishing, lateral movement, unsecured remote access, and compromised third-party vendors.




**Hospitality**  
This category includes hotels, lodges, restaurants, and other hospitality services.

82,130+ detections

~18,321 endpoints

**21%** of which were **Trojan.Shadowbrokers**

Trait: Trojan.Shadowbrokers exploits unsecured public Wi-Fi, vulnerable POS systems, and IoT devices, spreading via third-party integrations and phishing attacks targeting staff. Unlike healthcare, it focuses on payment data and guest-facing infrastructure vulnerabilities.




**Transport**  
Covers businesses specializing in the transportation of goods.

4,700+ detections

~1,471 Endpoints

**19%** of which were **Worm.AutoIt.Nuqel.AT**

Trait: Exploits instant messaging platforms; spreads through network shares and removable drives. Gathers user credentials, downloads additional malware, written in AutoIt scripting language to evade detection.




**Manufacturing**  
Encompasses businesses involved in any type of manufacturing activities.

3,32,000+ detections

~2,43,416 Endpoints

**14%** of which were **Nsis.Bitmin**

Trait: Propagates through compromised NSIS installers from fake or compromised websites. Installs unauthorized cryptocurrency miners, may use rootkits to avoid detection.



**Education**  
Comprises educational institutions such as schools, colleges, training centers, and coaching institutes.

8,53,000+ detections

~1,60,806 Endpoints

**12%** of which were **W32.Pioneer.CZI**

Trait: Infects executable files; spreads through network shares and removable media. Injects code into executables, potentially corrupting files and disrupting operations.

**ECP**  
Covers infrastructure development, engineering, construction, and similar industries.

12,600+ detections

~4,726 Endpoints

**10%** of which were **Trojan. Shadowbrokers**

Trait: Utilizes leaked exploits (e.g., EternalBlue) targeting unpatched Windows systems over networks. Installs backdoors, provides remote access, deploys ransomware or other malicious payloads.

**IT/ITES**  
Involves companies dealing with IT products, software development, and IT-enabled services.

77,005+ detections

~69,900 Endpoints

**10%** of which were **PIF.StucksNet.A**

Trait: Spreads via infected pif files on removable drives; exploits vulnerabilities in industrial control systems. Targets SCADA systems, alters processes and settings, can cause physical equipment damage.

**MSME**  
This category includes small-scale businesses, service providers, local shops, traders, chartered accountants (CAs), and other professional service providers.

5,02,000+ detections

~3,00,423 Endpoints

**9.23%** of which were **Nsis. Bitmin**

Trait: Propagates through compromised NSIS installers from fake or compromised websites. Installs unauthorized cryptocurrency miners may use rootkits to avoid detection.

**Government**  
Includes organizations under the government sector, such as public institutions, defense organizations, and allied institutes.

30,4000+ detections

~3,22,747 Endpoints

**8%** of which were **Remoteadmin. Remoteexec**

Trait: Misuses legitimate remote administration tools; attackers exploit weak credentials or system vulnerabilities. Executes remote commands, deploys malware, alters system configurations.

**BFSI**  
Covers small, medium, and large-scale banks, financial institutions, loan providers, and insurance companies.

27,837+ detections

~47,501 Endpoints

**6%** of which were **Trojan. Convagent**

Trait: Distributed through phishing emails with malicious attachments or links; may come bundled with untrusted software. Collects sensitive data, installs backdoors, and masquerades as legitimate applications.



# Key Malware Findings - 2024

## Prominent Hactivist Groups Targeting Indian Cyber Space

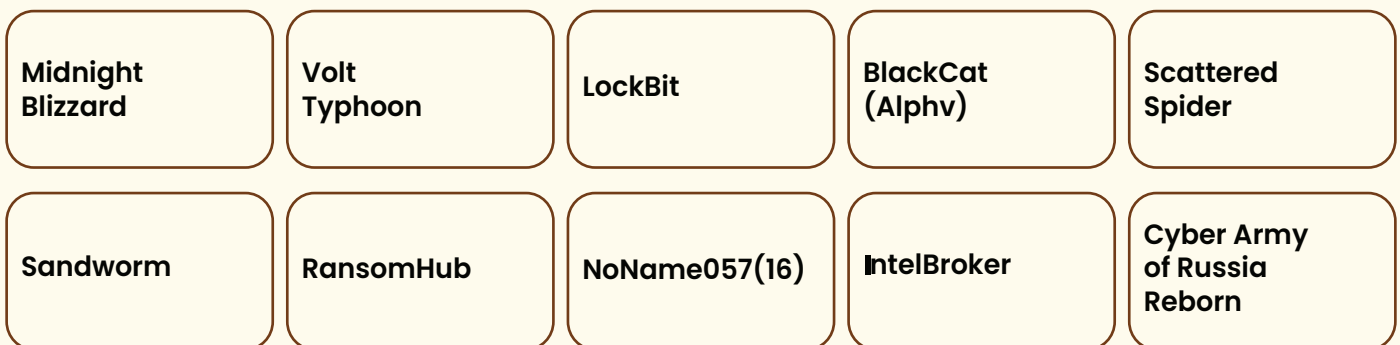
Total Reported Attacks: 5,842

Most Active Group: Anon Black Flag Indonesian



## Most Impactful Threat Actors

The cybersecurity landscape in 2024 saw significant disruptions from various threat actors. Here's a quick look at the most impactful ones:



These groups have been at the forefront of cyber-attacks, targeting industries, governments, and individuals worldwide with advanced tactics and tools.

# Top Vulnerable Driver Types Targeted by Attackers

Attackers increasingly exploit vulnerable device drivers to gain kernel-level access, bypass security mechanisms, and execute malicious code. The list below highlights the top drivers that have been targeted by attackers in 2024 due to their vulnerabilities or widespread usage:

<b>AFD.sys</b> (Ancillary Function Driver for WinSock)	<b>dbutil_2_3.sys</b> (Debian Driver)	<b>appid.sys</b>	<b>RTCore64.sys</b> (MSI Afterburner Driver)	<b>WinRing0.sys</b>
<b>nvlddmkm.sys</b> (NVIDIA Graphics Driver)	<b>gdrv.sys</b> (GIGABYTE Driver)	<b>SynTP.sys</b> (Synaptics Driver)	<b>RTCore64.sys</b> (MSI)	<b>atik64.sys</b> (ATI Radeon Driver)











# Most Abused LOLBins (Living-Off-the-Land Binaries)

LOLBins, or legitimate executables native to operating systems, are often abused by attackers to evade detection and persist within systems. The following binaries have been the most exploited in 2024:

<b>PowerShell</b>	<b>Rundll32</b>	<b>Mshta</b>	<b>Regsvr32</b>	<b>Msiexec</b>
<b>Certutil</b>	<b>Bitsadmin</b>	<b>Wmic</b>	<b>Notepad</b>	<b>SystemSettings AdminFlows</b>

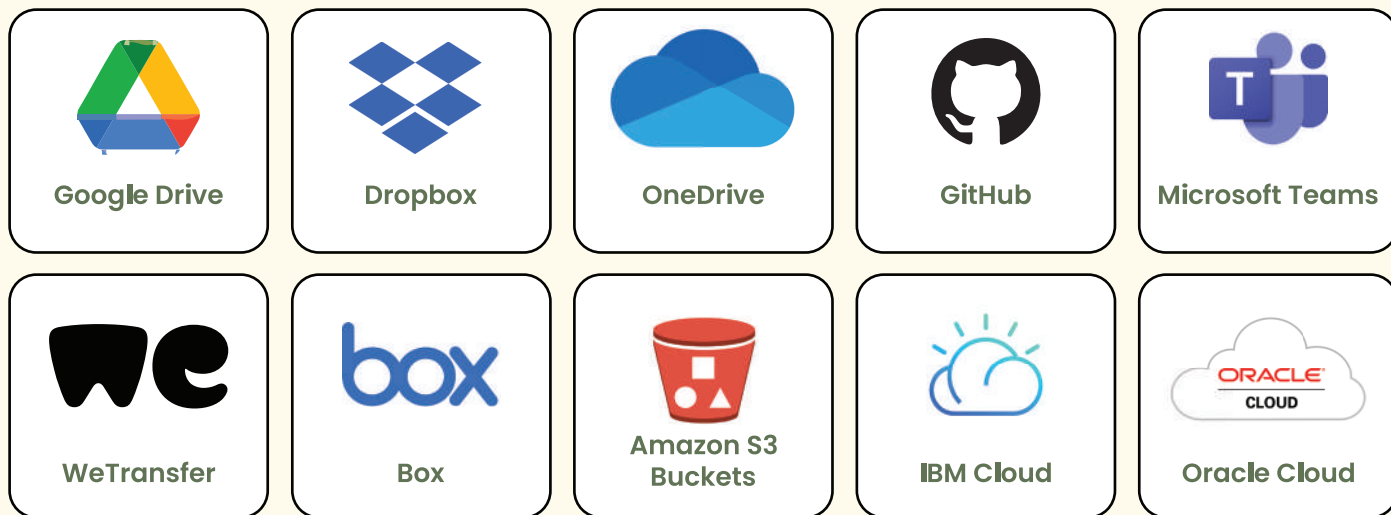
# Top Malicious File Types

Malicious actors utilize specific file types to deliver malware, exploit vulnerabilities, or launch phishing campaigns. The following file types have posed the highest risks in 2024:

 <b>Executable Files</b> (.exe, .bat, .scr)	 <b>Document Files</b> (.docx, .pdf, .xls)	 <b>Compressed Files</b> (.zip, .rar)	 <b>HTML Files</b> (.htm, .html)	 <b>JavaScript Files</b> (.js)
 <b>ISO and IMG Files</b>	 <b>Windows Shortcut Files</b> (.lnk)	 <b>Email Attachments</b> (.eml)	 <b>Script Files</b> (.ps1, .vbs)	 <b>Executable Jar Files</b> (.jar)

## Most Abused File Sharing Platforms

Cloud-based file-sharing platforms have become prime targets for cybercriminals due to their ubiquity and potential for hosting and distributing malicious files. Here are the platforms most abused in 2024:



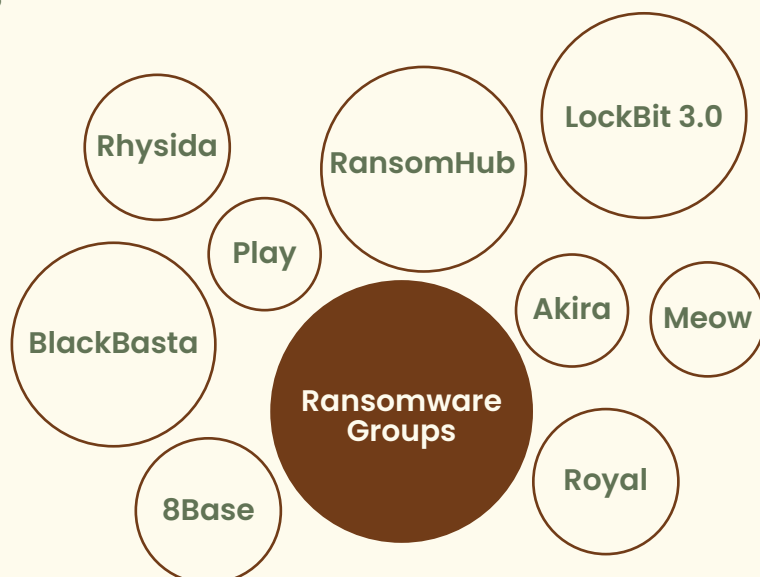
## Top MITRE Techniques Used

The MITRE ATT&CK framework categorizes tactics and techniques used by adversaries. In 2024, the following techniques emerged as the most utilized by attackers:

<b>T1055</b> Process injection	<b>T1059</b> Command and Scripting Interpreter	<b>T1562</b> Impair Defenses	<b>T1082</b> System Information Discovery	<b>T1486</b> Data Encrypted for Impact
<b>T1003</b> OS Credential Dumping	<b>T1071</b> Application Layer Protocol	<b>T1547</b> Boot or Logon Autostart Execution	<b>T1566</b> Phishing	<b>T1110</b> Brute Force

## Top Ransomware Groups

Ransomware remains one of the most devastating threats, and specific groups have dominated the landscape with sophisticated and large-scale attacks in 2024. Below is a list of the most prominent ransomware groups of the year:





# FEATURED STORIES 2025





Vespa mandarinia

# The Rise in APK Malware via WhatsApp

## Exploiting Trust and Urgency

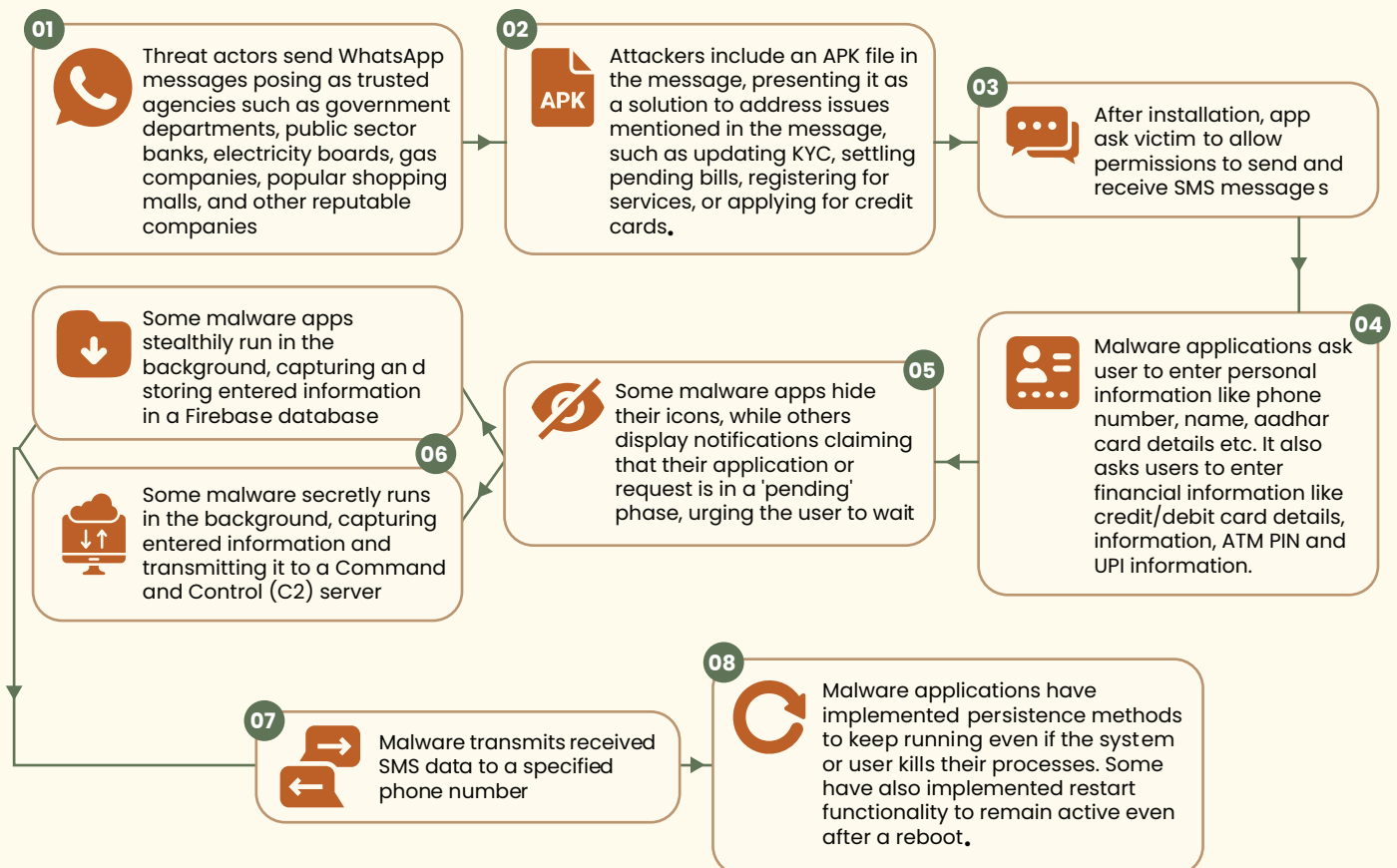
Criticality: High

Target: Android Users

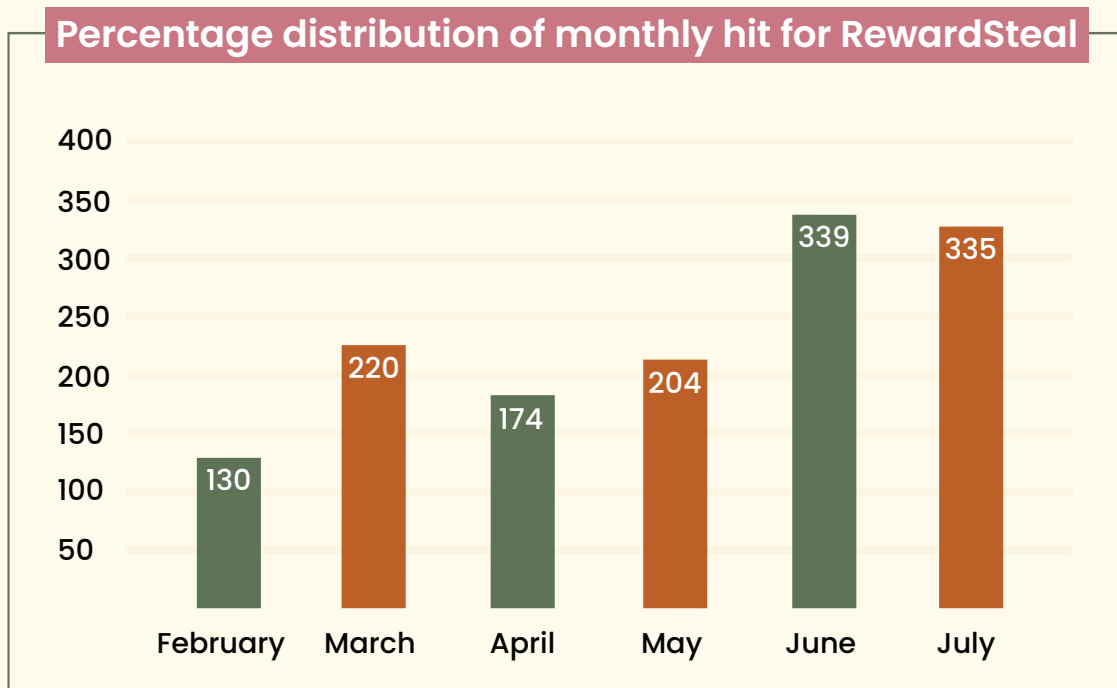
Country/State/Region: India

In the digital age, WhatsApp has become an indispensable communication tool for millions. However, its convenience and widespread use also make it a fertile ground for cybercriminals. One of the more insidious threats in this space is the distribution of APK malware via WhatsApp.

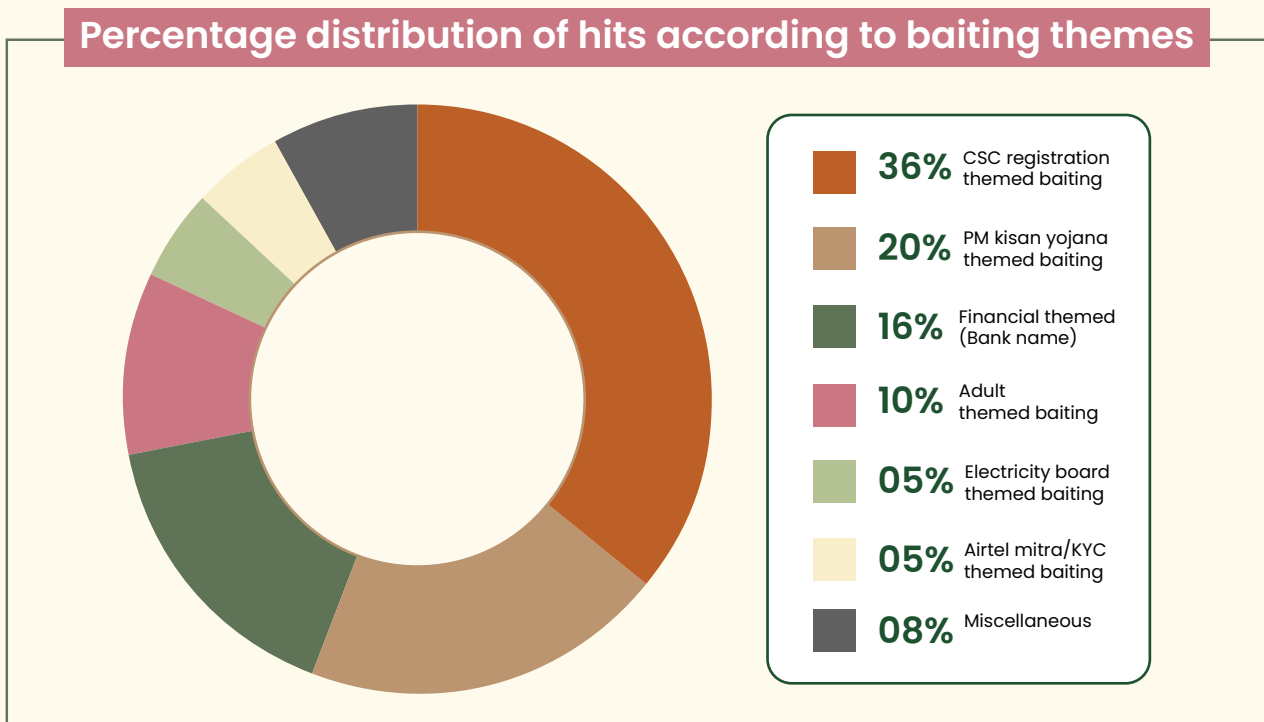
These malicious actors often exploit the trust users place in well-known organizations by posing as trusted agencies such as government departments, public sector banks, electricity boards, gas companies, popular shopping malls, and other reputable companies. By creating a false sense of urgency, they manipulate users into installing harmful APK files. **The malware family name RewardSteal is named for its strategy of enticing users with promises of rewards to trick them into downloading infected APK files.**



The spread of these malware applications has increased in the past few months. The graph below shows the number of hits received for RewardSteal from February to July, highlighting a significant rise in detections



Threat actors have distributed these malware applications under various names to deceive users. Malware applications have been categorized based on their names and the baiting themes employed by the malware authors under seven primary categories presented in the pie-chart below:



These malicious apps, delivered as APK files, are designed to steal Personally Identifiable Information (PII), and financial data, access SMS information, and even commit billing fraud without the user’s consent. Given WhatsApp’s deep integration into our daily communication, it has become an attractive target for these cyber threats.

# Malicious Android Malware Masked as Government Notifications



Cascabela thevetia

Criticality: High

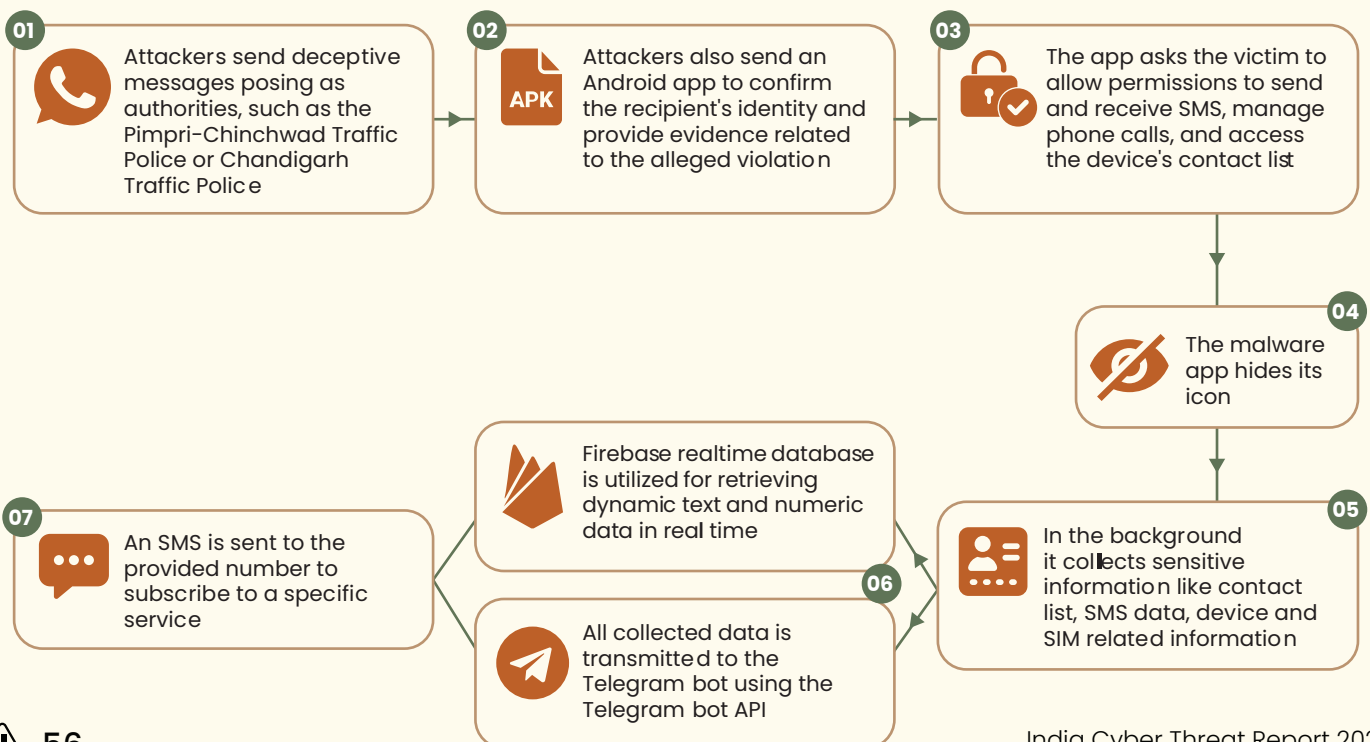
Target: Android Users

Country/State/Region: India

Cybercriminals have cleverly exploited the notification system of government’s traffic department to distribute malicious softwares. **Numerous instances of these deceptive messages, purportedly sent from authorities like the Pimpri-Chinchwad Traffic Police and Chandigarh Traffic Police, have been observed.**

These messages claim the recipient has been issued a traffic ticket for violating regulations. To lend authenticity, they include details such as the ticket number and vehicle registration information, along with the official logos of the Maharashtra Motor Vehicle Department and Chandigarh Administration as profile pictures. The messages often prompt recipients to download an application called “Vahan Parivahan,” to confirm their identity and review evidence of the violation.

However, unrecognized to recipients, the linked APK file contains malicious software designed to steal information from Android devices. This infostealer malware discreetly infiltrates devices, compromising sensitive data and engaging in billing fraud by sending messages to specific phone numbers.





# Pop-Up Ad Alert

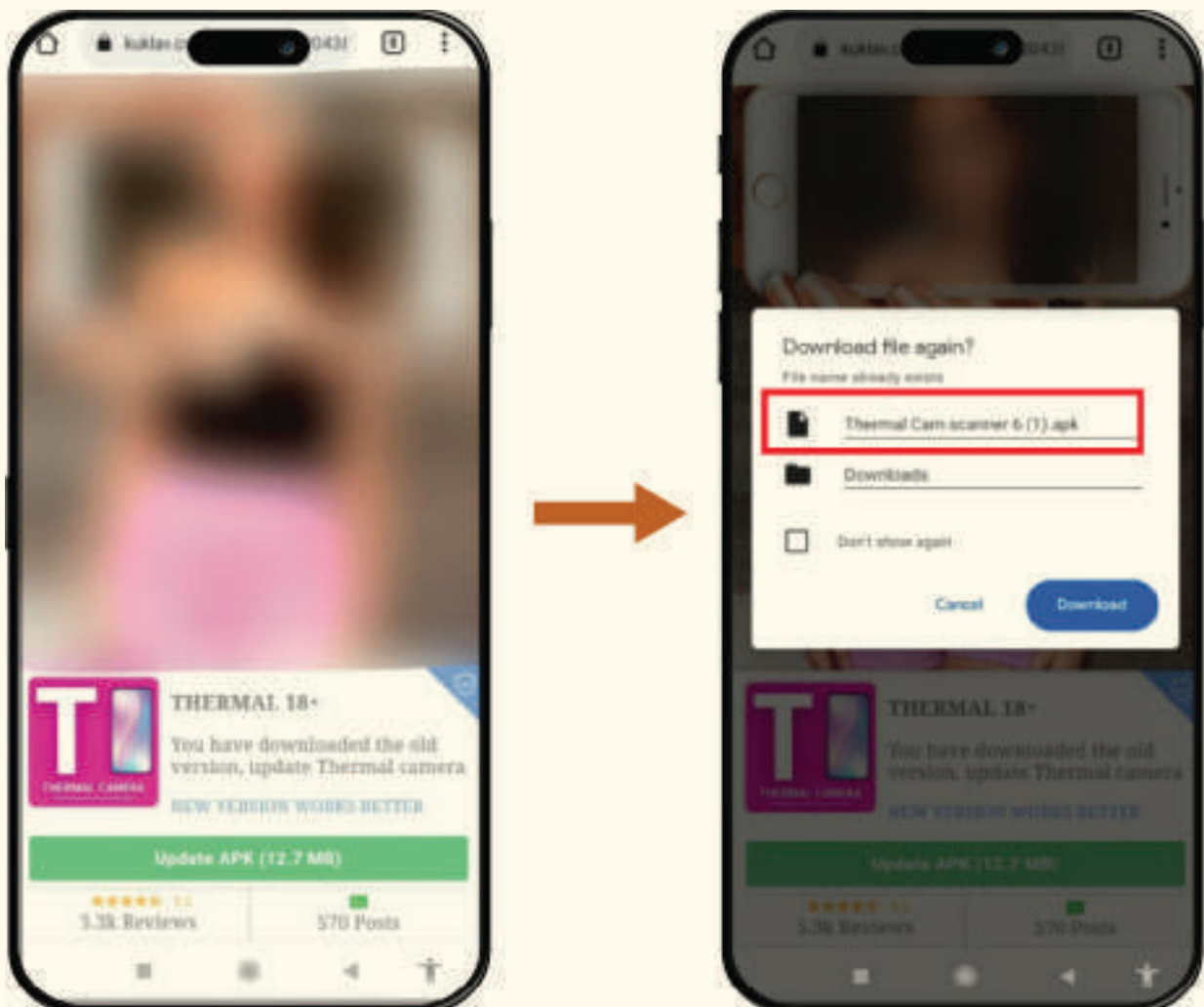
## Beware of Unrealistic Claims on Smartphones

Criticality: Medium ■■

Target: Android Users

Country/State/Region: India

A seemingly tempting pop-up ad, promising secrets or useful insights, can mask a serious threat. Many of these deceitful apps, posing as legitimate tools, can sneak into the device. Once installed, disguised under authentic-looking app icons, they can steal private SMS messages and other sensitive data. This stolen information is often misused to create fake social media accounts, compromising privacy and financial security. If the stolen SMS data includes sensitive financial information like bank verification codes or login credentials, the risk escalates, potentially leading to unauthorized access and identity theft.



**Cyber attackers exploit various techniques to infiltrate devices. One such tactic leverages an average user browsing habits, where an unintentional click on links or downloading of such apps that promise unrealistic benefits in areas like dating, gaming, or gambling.**


While these apps may seem harmless initially, installing them could severely compromise both privacy and financial safety. Sensitive data collected by these malicious apps can lead to devastating consequences, such as drained bank accounts and stolen identities.

Although not every case of downloading such apps leads to harm, it's always wise to exercise caution. The growing sophistication of cyber threats makes it critical for users to be aware and vigilant about the apps they interact with, ensuring they don't fall victim to these hidden traps.

# Anatsa Android Banking Trojan

## Evolving Threat Targeting Mobile Banking Users



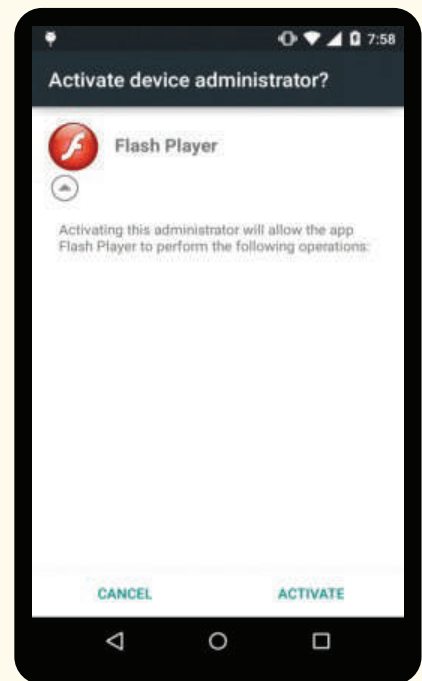
Criticality: High 

Target: Android Users

Country/State/Region: Europe, United States and other Countries

Anatsa, also known as TeaBot, is a highly sophisticated Android banking Trojan that has undergone significant evolution since its discovery in early 2021. Initially targeting banking apps across Europe, Anatsa used tactics such as screen streaming and keylogging to steal users' banking credentials. Disguising itself as seemingly benign apps like QR code scanners or PDF readers, it successfully infiltrated devices without detection.

As the Trojan evolved, its reach broadened, extending its targets beyond Europe to include financial institutions in the United States. Exploiting Android's accessibility services, Anatsa manipulated the user interface of infected devices, enabling attackers to directly steal sensitive information from banking applications.



**Requesting to grant device administrator rights**

In its later stages, Anatsa became even more dangerous by incorporating a Remote Access Trojan (RAT) module. This added capability allowed cybercriminals to remotely control infected devices, enabling complex attacks like monitoring user activity or performing fraudulent transactions without the victim's knowledge.


**By 2024, Anatsa continued to be distributed via the Google Play Store, hidden in apps that appear legitimate, such as PDF viewers and QR code scanners.**

The latest versions bypassed Android 13's restrictions on accessibility services and introduced advanced Device Takeover (DTO) capabilities, enhancing its ability to control compromised devices. This evolution underscores Anatsa's persistence and adaptability, making it a critical threat to mobile banking users worldwide.

## Rafel RAT

### How Advanced Malware Targets Vulnerable Android Devices

*Dionaea muscipula*

Criticality: High 

Target: Android Users

Country/State/Region: Europe, United States and other Countries

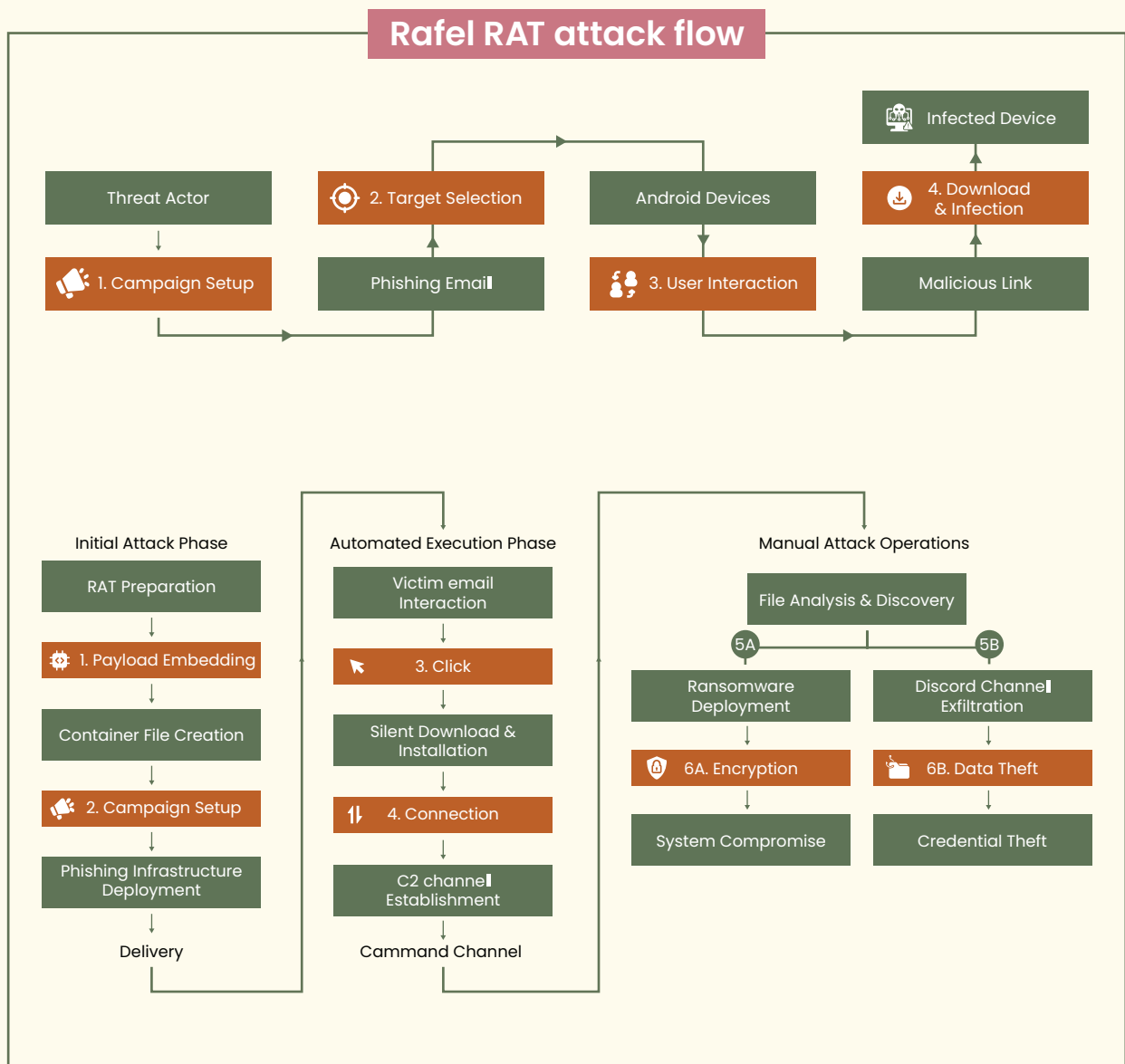
Rafel RAT is an advanced Android malware that serves multiple malicious purposes, including espionage, data theft, and ransomware attacks. It enables threat actors to remotely control infected devices, allowing them to steal sensitive information such as contacts, SMS messages, call logs, and even bypass two-factor authentication (2FA) protections. The malware's ability to persist on devices is particularly dangerous, as it exploits permissions and system optimizations to avoid detection and removal. This makes it a formidable threat, especially in campaigns where it has been deployed by espionage groups like APT-C-35, who have used Rafel RAT to infiltrate high-profile targets, including military sectors.

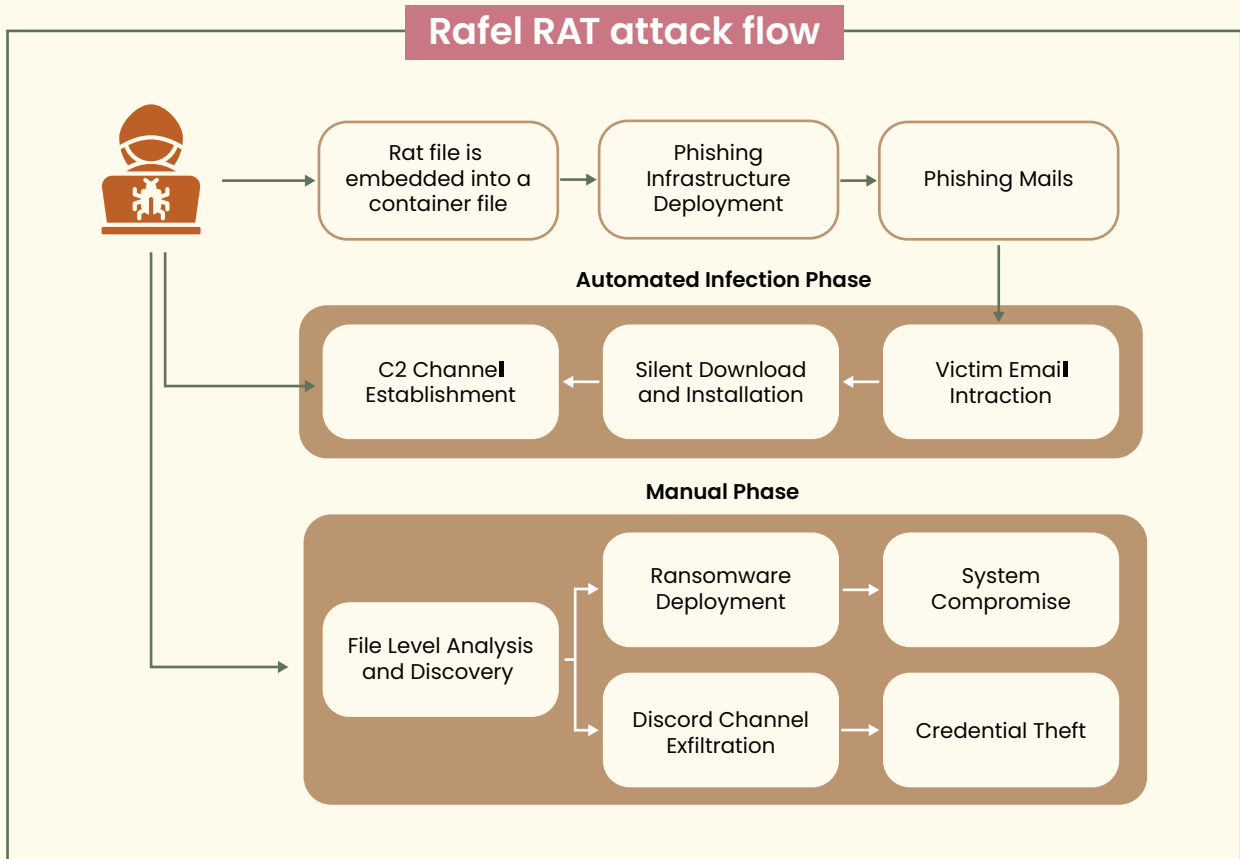
This malware is highly effective on devices running older Android versions, with many victims using outdated or unsupported operating systems. Devices from manufacturers like Samsung, Xiaomi, Vivo, and Huawei are especially vulnerable to Rafel RAT's attacks.

Beyond its use in espionage, Rafel RAT has been employed in ransomware operations, adding another layer of danger. In these scenarios, the malware locks devices and encrypts files, subsequently demanding ransom payments through methods like SMS notifications sent to the victim. Rafel RAT's communication with command-and-control (C2) servers are primarily HTTP-based, allowing attackers to easily manage infected devices through a web panel, where they can execute commands and control various aspects of the compromised systems.

What makes Rafel RAT particularly threatening is its adaptability across different types of attacks, from stealing sensitive information for espionage to executing ransomware campaigns.

The combination of remote control capabilities, its persistence on older Android devices, and its usage by both cybercriminals and espionage groups highlights the need for updated security measures, especially for users relying on outdated devices. Without such precautions, individuals and organizations remain highly susceptible to Rafel RAT's wide range of malicious activities.





*Amanita pantherina*

# Fake Apps Posing as Open AI's ChatGPT App

Criticality: High ■ ■ ■

Target: Android Users

Country/State/Region: Worldwide

The trend of fake apps is one offshoot of evolving technology and shows no signs of receding despite the steps taken by Google\* to purge 36 counterfeit Android security apps from the Google Play Store in 2018.

ChatGPT is one of the most rapidly expanding consumer internet apps in history. ChatGPT has become a game-changer in the AI landscape, enhancing content quality, providing virtual tutoring for education and training, and ensuring swift response times for users.

Android malware disguised as fake ChatGPT applications with harmful spyware capabilities. When clicking on the application icon to launch, users are redirected to the accessibility page where they are prompted to provide accessibility permission to the fake application. Upon providing accessibility permissions, the application hides its icon and runs in the background. This app collects location-related data and monitors incoming calls to the device.

Source - <https://blogs.quickheal.com/28-fake-apps-removed-google-play-store-post-quick-heal-security-lab-reports/>

### How a fake ChatGPT app appears in the app drawer



## Copybara Fraud Campaign



*Conium maculatum*

Criticality: High ■ ■ ■

Target: Android Users

Country/State/Region: UK, Spain and Italy

Copybara, identified by researchers in 2021, spreads through social engineering. In a recently found sample, threat actors adopted social engineering techniques such as smishing (SMS phishing) and vishing (voice phishing), alongside malware components, to perform unauthorized banking transfers.

**Copybara possesses all the necessary functionalities to execute On-Device Fraud (ODF) and initiate unauthorized money transfers directly from the victim's device.** Threat actors employed a phishing kit, which is a collection of malicious assets and scripts designed to replicate legitimate websites, often mimicking the login pages of banks, financial institutions, or other trusted platforms.

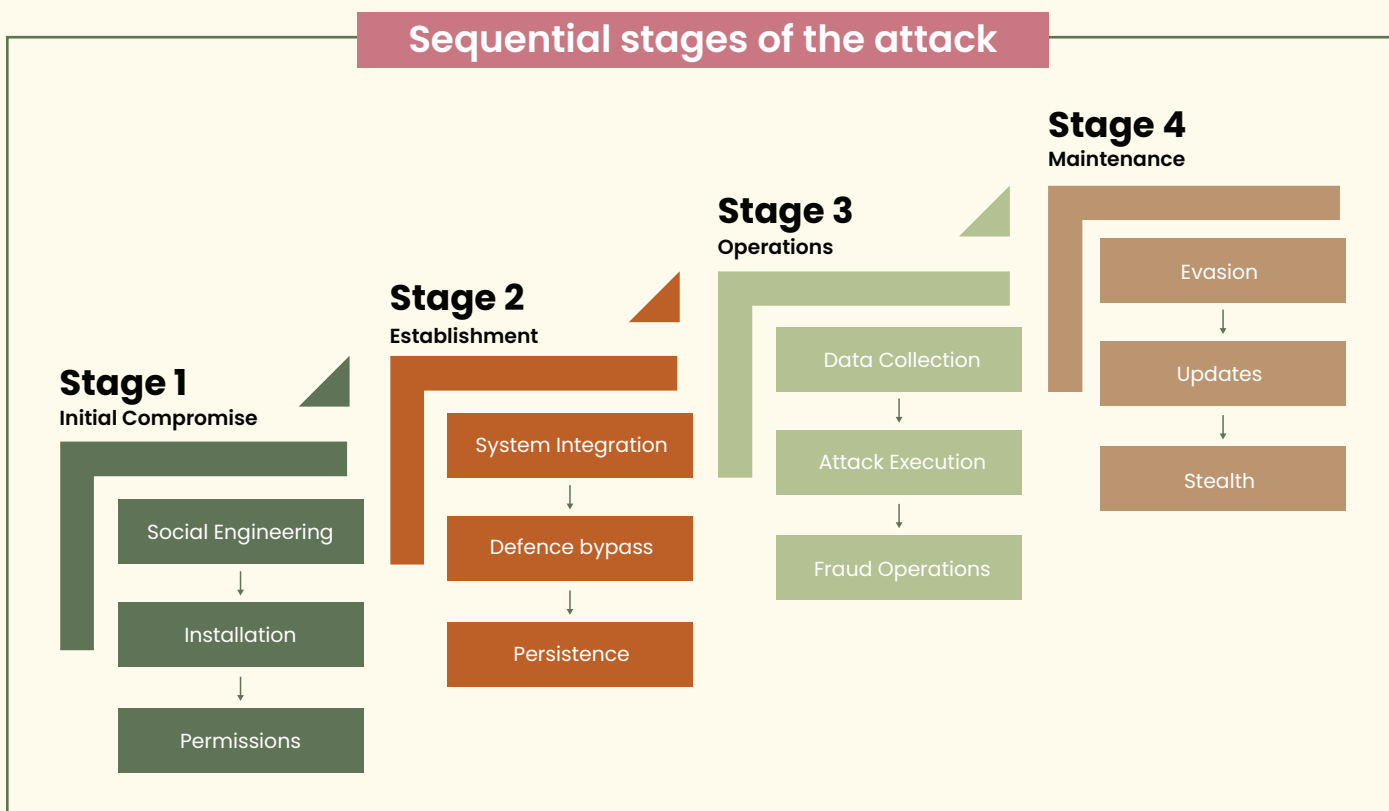
## Modern phishing kits utilize several anti-detection techniques, including:

- ▲ Geofencing checks
- ▲ Device fingerprinting
- ▲ Blacklisting specific ASN and network ranges
- ▲ Dynamic content generation
- ▲ Abuse of legitimate services, such as CDN & reverse proxies, to mask true location of web server

## The phishing kit used by threat actors typically operates through three main steps:

- ▲ **Step 1:** Ex-filtrate valid credentials along with the associated phone number.
- ▲ **Step 2:** Ex-filtrate a valid name and estimate the victim's bank account balance.
- ▲ **Step 3:** Display a fake message to victims after data ex-filtration.

All the collected data are typically sent to a dedicated Telegram group (if configured) and stored on the command and control (C2) panel.






*Pteropus giganteus*

# Mandrake Spyware Campaign

---

Criticality: High 

Target: Android Users

Country/State/Region: Canada, Germany, Italy, Mexico, Spain, Peru and the UK.

Mandrake, though identified in 2020, had been active in the wild since at least 2016, operating for years. Initially, it targeted users through traditional methods; however, the new variant of Mandrake represents a significant evolution in its design and functionality. The latest iterated version of Mandrake is engineered to bypass Google Play's robust security checks, making it more challenging for the platform to detect and remove it. To further obfuscate its malicious intent and hinder analysis efforts, the malware operators have cleverly shifted the core malicious functionality into native libraries. These libraries are heavily obfuscated using OLLVM, a technique that complicates reverse engineering and analysis by security professionals.

Communication with Command and control (C2) servers is another area where Mandrake demonstrates its advanced capabilities. It employs certificate pinning, a security measure that prevents man-in-the-middle attacks, thereby making it extremely difficult for researchers to intercept and analyze SSL traffic. This added layer of security allows the malware to maintain persistent communication with its operators while evading detection.

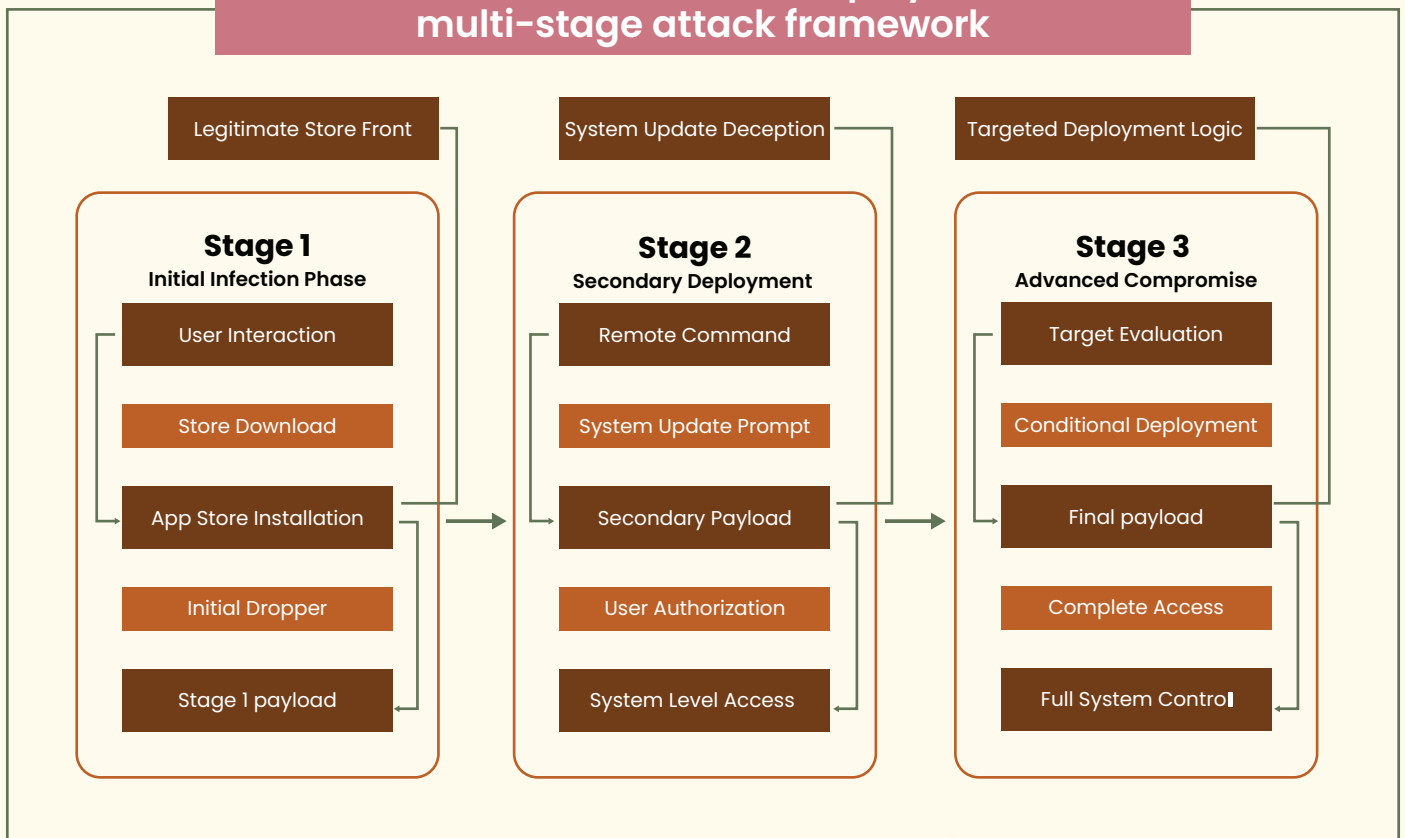
**Furthermore, Mandrake is equipped with a wide array of sandbox evasion and anti-analysis techniques, rendering it highly resistant to detection and dissection by security researchers.**

---

These strategies not only protect its operational integrity but also enable it to execute its malicious activities without drawing attention. As a result, Mandrake poses a significant threat to users, highlighting the ongoing challenges in combating sophisticated mobile malware in an increasingly complex cybersecurity landscape.



## Advanced android malware deployment chain multi-stage attack framework



# Operation RusticWe Targets Indian Government and Defense Entities



*Platycodon grandifloras*

Criticality: Medium ■

Target: Windows

Sector targeted: Government and Defense

Country/State/Region: India

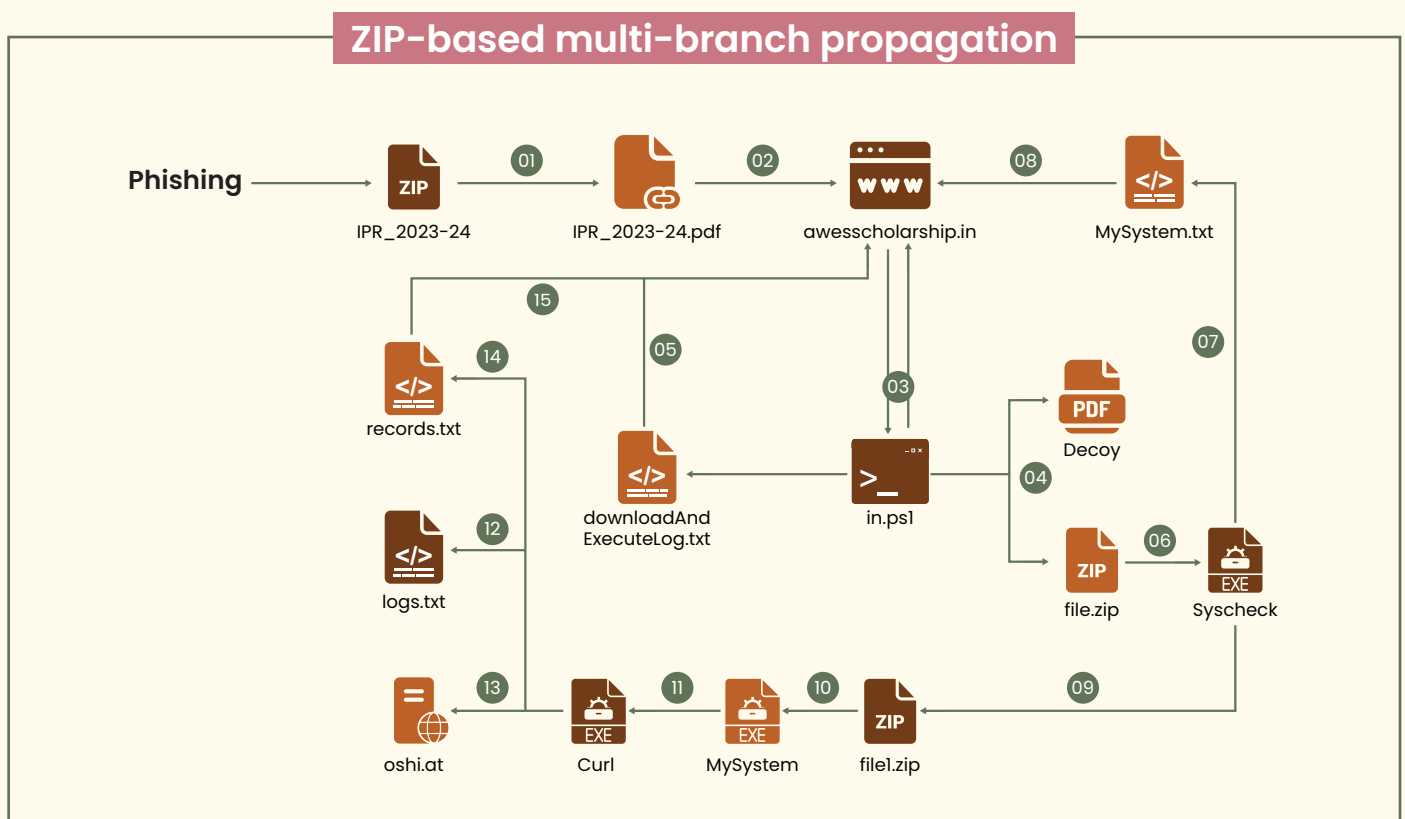
Since October 2023, a sophisticated phishing campaign has been targeting government personnel, with an escalation in December 2023 that expanded the focus to both government and private entities within the defense sector. The attackers have deployed new techniques, including Rust-based payloads and encrypted PowerShell commands, to exfiltrate sensitive documents. Rather than relying on traditional command-and-control (C2) servers, these documents are being transferred to a web-based service engine, making detection more difficult.

The campaign has shown significant flexibility, with threat actors utilizing fake domains to host malicious payloads and decoy files, further complicating efforts to detect the attack. **This operation, tracked as Operation RusticWeb, exhibits numerous similarities with the tactics, techniques, and procedures (TTPs) used by known advanced persistent threat (APT) groups.** These overlaps suggest possible links to groups previously identified for their targeted campaigns against similar sectors. Additionally, the campaign shows similarities to the Operation Armor Piercer report published by Cisco in 2021, and the use of fake forms to exploit specific targets was also observed by the team in earlier campaigns.

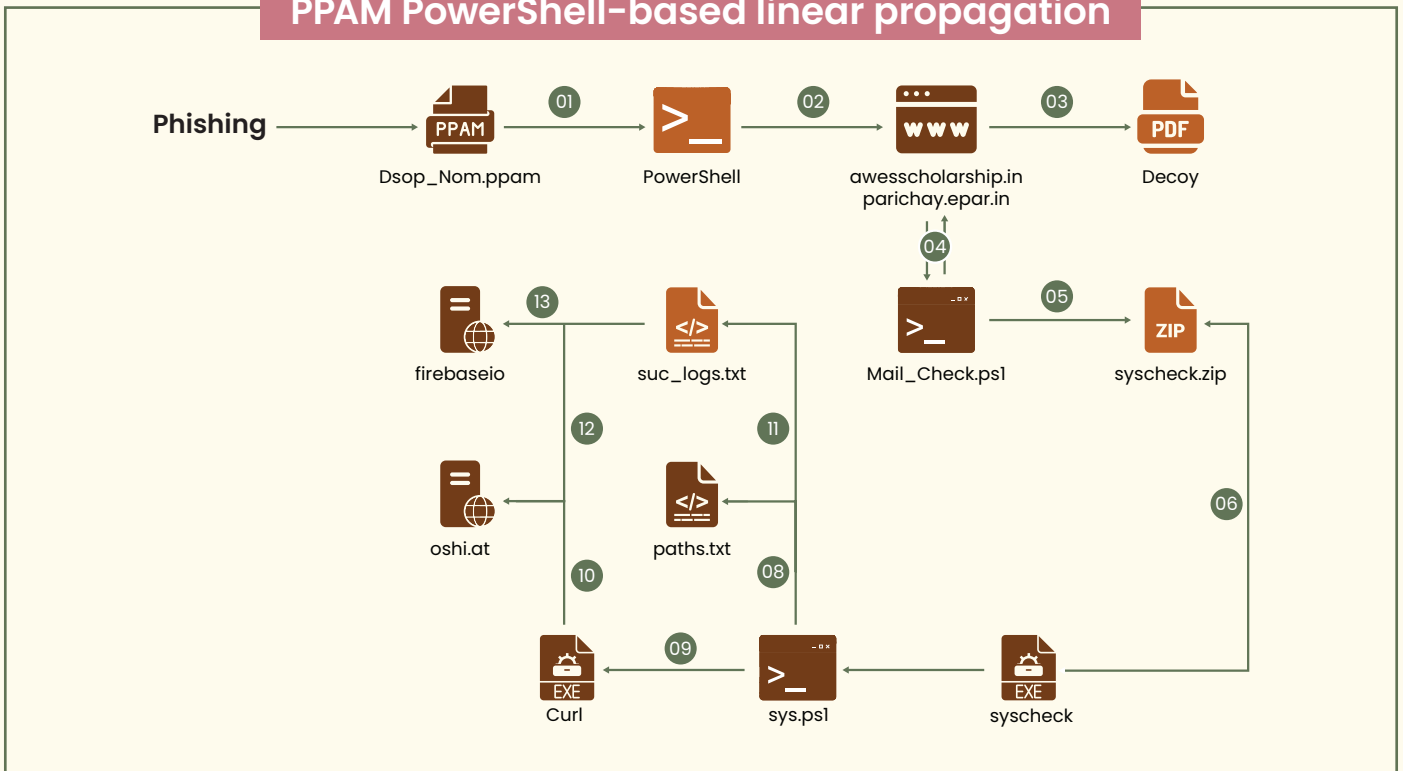
**A notable trend in this campaign is the shift from well-known compiled languages (such as C and C++) to more modern programming languages like Golang, Rust and Nim.**

This transition enables the attackers to create cross-platform malware while making it harder for security solutions to detect. Recently analyzed malware ecosystems built in Golang, such as the Windows-based Warp malware (which uses Telegram for C2) and a Linux-based stager payload associated with Ares RAT. At the same time, Ransomware-as-a-Service (RaaS) operators are migrating from Golang to Rust, which offers high-performance encryption, faster evasion, and greater memory safety.

The phishing campaign has been targeting various Indian government personnel since October 2023. New Rust-based payloads and encrypted PowerShell commands have been utilized to exfiltrate confidential documents to a web-based service engine, instead of a dedicated command-and-control (C2) server. With actively modifying its arsenal, it has also used fake domains to host malicious payloads and decoy files. Below are a few names of domains and sample baits used in this campaign.



## PPAM PowerShell-based linear propagation



# CVE-2024-3094 Unveiled

## “XZ Utils” Compromise Sparks Security Alarm

*Aconitum napellus*

Criticality: High

Target: Windows

Country/State/Region: Worldwide

A critical supply chain vulnerability (CVE-2024-3094) in XZ-Utils, rated with a CVSS score of 10, exploits a flaw in the XZ library (liblzma). This widely-used open-source compression tool, which is integrated into numerous Linux distributions, is compromised in this supply chain attack. The flaw impacts versions 5.6.0 and 5.6.1 of XZ-Utils, where malicious code is injected during the build process, compromising the integrity of the liblzma library. The attack introduces a backdoor, allowing Remote Code Execution (RCE) through SSH, specifically targeting systems using OpenSSH servers.

## How does it work?

The attack works by embedding malicious scripts in XZ-Utils' source code tarballs. During installation, the backdoor is invoked as part of the configuration step, leading to a modification of the Makefile and eventual compilation of liblzma with the malicious code. Once the library is linked with OpenSSH, the backdoor intercepts the `RSA_public_decrypt` function in the SSH authentication process, allowing attackers with specific private keys to inject arbitrary payloads before authentication completes. This results in the execution of malicious commands on the targeted machine.

The attack involves obfuscated and encrypted payloads hidden in test files such as `bad-3-corrupt_lzma2.xz` and `good-large_compressed.lzma`. Upon triggering, the payload is decrypted and executed within the SSH authentication process, compromising the victim's system. Major Linux distributions such as Fedora, Debian, Kali, OpenSUSE, and Arch Linux have been affected, with patches released to address this vulnerability. Updating to specific, earlier versions of XZ-Utils (like 5.4.6) or applying the latest security patches is critical to mitigate this vulnerability.

# Operation FlightNight Targets Indian Government and Energy



*Latrodectus hasselti*

Criticality: Medium ■■

Target: Windows

Sector targeted: Government and Energy

Country/State/Region: India

Since March 2024, an unidentified threat actor has been targeting Indian government entities and private energy companies with a modified version of the open-source information stealer, **HackBrowserData**. This malware exfiltrates sensitive data via Slack, which the attacker uses as a command-and-control (C2) channel. The attack begins with a phishing email containing a decoy message about an invitation letter from the Indian Air Force. Upon activation, the malware exfiltrates internal documents, private email communications, and cached browser data.

## Attack Chain

Codenamed “Operation FlightNight,” this cyber espionage campaign takes its name from the Slack channels employed by the attackers. The campaign has specifically targeted multiple Indian government entities, including those involved in electronic communications, IT governance, and national defense, as well as private energy companies. These organizations have been compromised, with approximately 8.81 GB of sensitive data exfiltrated. This includes financial documents, personal employee details, and information related to oil and gas drilling activities.

Given the critical nature of this data, which could enable further intrusions into the Indian government’s infrastructure, analysts have assessed the threat with medium confidence. Furthermore, similarities in the malware and metadata from the delivery mechanism suggest a connection to a previously reported attack on January 17, 2024. Based on these findings, analysts conclude with high confidence that the primary motive behind these activities is cyber espionage.

## Malware Delivery and Execution

The threat actor employed a decoy PDF document, disguised as an invitation from the Indian Air Force, which was delivered within an ISO file. The ISO file contained the malware in executable form. To trick the recipient into activating the malware, the ISO also included a shortcut file (LNK), which

appeared to be a harmless PDF due to its misleading icon. Once the victim mounted the ISO file and executed the LNK file, the malware was triggered. It then began exfiltrating documents and cached browser data to the attacker-controlled Slack channels.

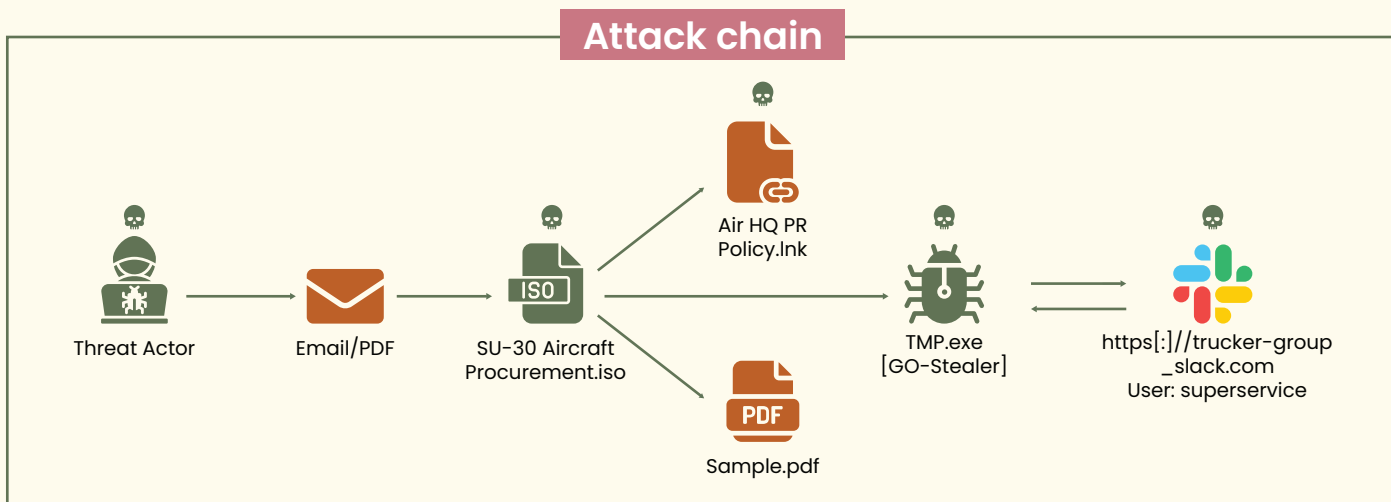
**The malware is a modified version of HackBrowserData, featuring additional capabilities for enhanced communication, data theft, and obfuscation.** It specifically targets file extensions commonly used for sensitive data, such as Microsoft Office documents and PDFs, to speed up data extraction. The malware communicates with Slack through API methods and stores static workspace and API keys, which can be used by analysts to monitor the Slack channels, revealing victim data such as timestamps and file paths for stolen information.

## Similar Campaigns and Behavioral Patterns

A similar campaign was observed earlier, in which the GoStealer malware was deployed using procurement-themed lures related to “SU-30 Aircraft Procurement.” In that case, a decoy file was shown to the victim while the stealer payload was used to exfiltrate sensitive information over Slack. The use of Slack channels, along with the similarity in techniques, suggests that both campaigns share common tactics, techniques, and procedures (TTPs) and may be attributed to the same threat actor or group

This ongoing campaign highlights the increasing sophistication of cyber espionage activities, with threat actors leveraging modern communication platforms like Slack for data exfiltration and operational stealth..

Given the targeted sectors and the nature of the stolen data, Operation FlightNight remains a significant concern for both national security and private sector organizations.



# Zero Day Campaign by DarkGate on a Microsoft SmartScreen Vulnerability

Criticality: High

Target: Windows

Sector targeted: Manufacturing, Financial, Transportation Science & Technology

Country/State/Region: United States, North America, Europe, Asia and Africa

A new wave of cyberattacks by the DarkGate malware operation has exploited a vulnerability in Windows Defender SmartScreen (CVE-2024-21412). This security bypass flaw in Microsoft Windows SmartScreen arises due to improper handling of maliciously crafted files, allowing remote attackers to evade security warnings. By exploiting this vulnerability, attackers can bypass SmartScreen's warning dialog, enabling them to deliver malicious files to users without detection. **Cybercrime groups such as Water Hydra, Lumma Stealer, and Meduza Stealer have already leveraged this flaw to launch attacks over the past year, demonstrating its active exploitation in the wild.**

Typically, attackers trick victims into clicking a crafted link that downloads a URL file leading to an LNK file. This LNK file downloads an HTA script, which then decodes and executes PowerShell code to retrieve decoy PDF files, final URLs, and a malicious shell code injector. The injector compromises legitimate processes by embedding the malware and sending stolen data back to a command-and-control (C2) server, giving attackers access to sensitive information.

Despite the availability of patches, DarkGate's resurgence, along with other malwares such as Pikabot, has filled the gap left by the disruption of previous malware campaigns. This poses a widespread risk as these malware strains are employed by various cybercriminals for large-scale malware dissemination. DarkGate, operating under a malware-as-a-service (MaaS) model, has become one of the most sophisticated and active strains in the cybercrime ecosystem. Its MaaS structure makes it accessible to different threat actors, many of whom are financially motivated. DarkGate has been used to target organizations across multiple regions, including North America, Europe, Asia, and Africa, highlighting its global reach.

Microsoft officially patched CVE-2024-21412 in its February 2024 security update. However, the persistence of DarkGate and the continued exploitation of this vulnerability by threat actors show the challenges of fully eradicating the risks associated with such flaws. Even with the patch in place, cybercriminals continue to adapt and find new ways to exploit similar vulnerabilities, emphasizing the need for vigilant security practices and timely system updates to mitigate future risks.



*Daboia russelii*

## Unmasking AsukaStealer

The USD \$80 Malware Threatening Digital Security

Criticality: Medium ■■

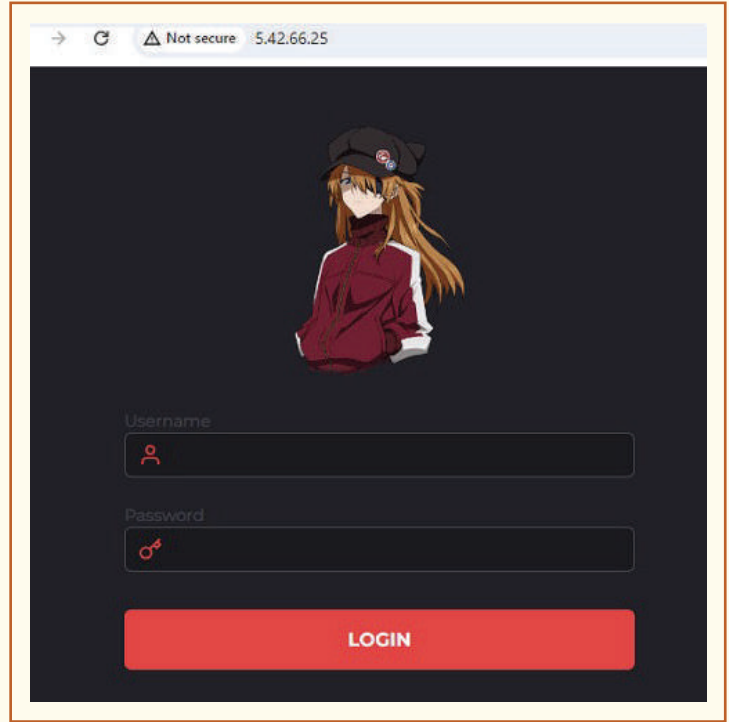
Target: Windows

Country/State/Region: Worldwide

AsukaStealer, marketed under the alias "Breakcore" on a Russian-language cybercrime forum, is a sophisticated piece of malware available for USD \$80 per month. Written in C++, it offers customizable configurations and a user-friendly web-based interface, making it highly accessible to cybercriminals looking for efficient tools to deploy and manage malware. Its primary focus is on popular web browsers such as Mozilla Firefox, Google Chrome, and Microsoft Edge, with the ability to extract sensitive data, including browser extensions, internet cookies, and saved login credentials. This creates a significant risk to user privacy and security by exploiting vulnerabilities in both Gecko and Chromium based browsers to maximize its reach across platforms.

In addition to targeting browsers, AsukaStealer also aims at a wide range of applications essential to both individuals and businesses. It actively seeks sensitive data from cryptocurrency wallets, FTP clients like FileZilla, and messaging platforms such as Discord and Telegram. Even gaming software like Steam is not exempt from its reach. This broad range of targets allows malware to collect a variety of personal and financial information, increasing the threat it poses to victims.

**Beyond data extraction, AsukaStealer enhances its capabilities by exfiltrating files from infected systems and capturing screenshots, giving cybercriminals comprehensive access to a victim's data and activities.**




These features make it a potent tool for harvesting sensitive information and conducting covert surveillance, contributing to its growing reputation as a significant cybersecurity threat worldwide.



*Amanita muscaria*

## Latrodectus Malware Replaces IcedID in Network Attacks

Criticality: High 

Target: Windows

Country/State/Region: WorldWide

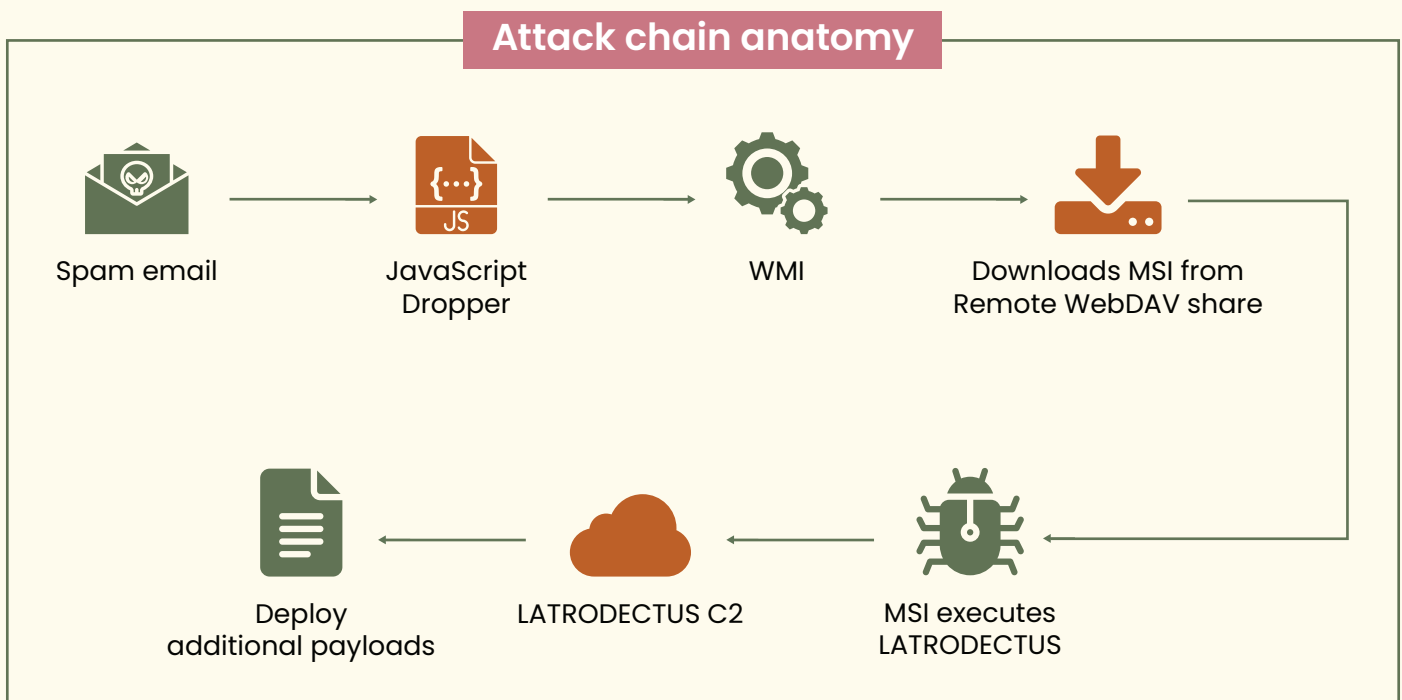
Cybersecurity researchers have reported a significant increase in email phishing campaigns delivering Latrodectus, a new malware loader believed to succeed IcedID. It has been actively sending malicious email campaigns since November 2023. These campaigns typically involve oversized JavaScript files exploiting Windows Management Instrumentation (WMI) to install remotely hosted MSI files. **Latrodectus has standard capabilities aimed at deploying additional malware, such as QakBot, DarkGate, and PikaBot, allowing attackers to perform post-exploitation activities.** Its focus on enumeration, execution, and self-delete techniques enhances its stealth, while its use of source code obfuscation and anti-analysis checks help evade detection in sandbox environments.



## Latrodectus establishes persistence on Windows hosts using scheduled tasks and communicates with a command-and-control (C2) server over HTTPS to collect system information, self-update, and execute payloads.

It introduces new commands to enumerate desktop files and retrieve process ancestry, suggesting ongoing development. Although it can download and execute IcedID from its C2 server, this behavior has not been observed in the wild. Researchers have documented its operational overlap with IcedID case initially identified in 2017, speculating that Latrodectus is an evolution of the IcedID loader, with both sharing infrastructure and distribution by initial access brokers TA577 and TA578 in phishing campaigns.

In addition to Latrodectus, phishing campaigns have been leveraging invoice-themed emails to deliver DarkGate malware, while phishing-as-a-service (PhaaS) platforms like Tycoon have been harvesting session cookies and bypassing multi-factor authentication (MFA). Latrodectus begins attacks by sending fake copyright infringement notices through online forms, dropping a JavaScript file via a Google Firebase URL that executes a DLL payload. Unlike its predecessor IcedID, Latrodectus performs sandbox evasion checks before execution, and researchers warn that multiple threat actors are likely to adopt the malware in future campaigns, continuing IcedID's legacy.





Catharanthus roseus

# New macOS Spyware LightSpy Unveiled

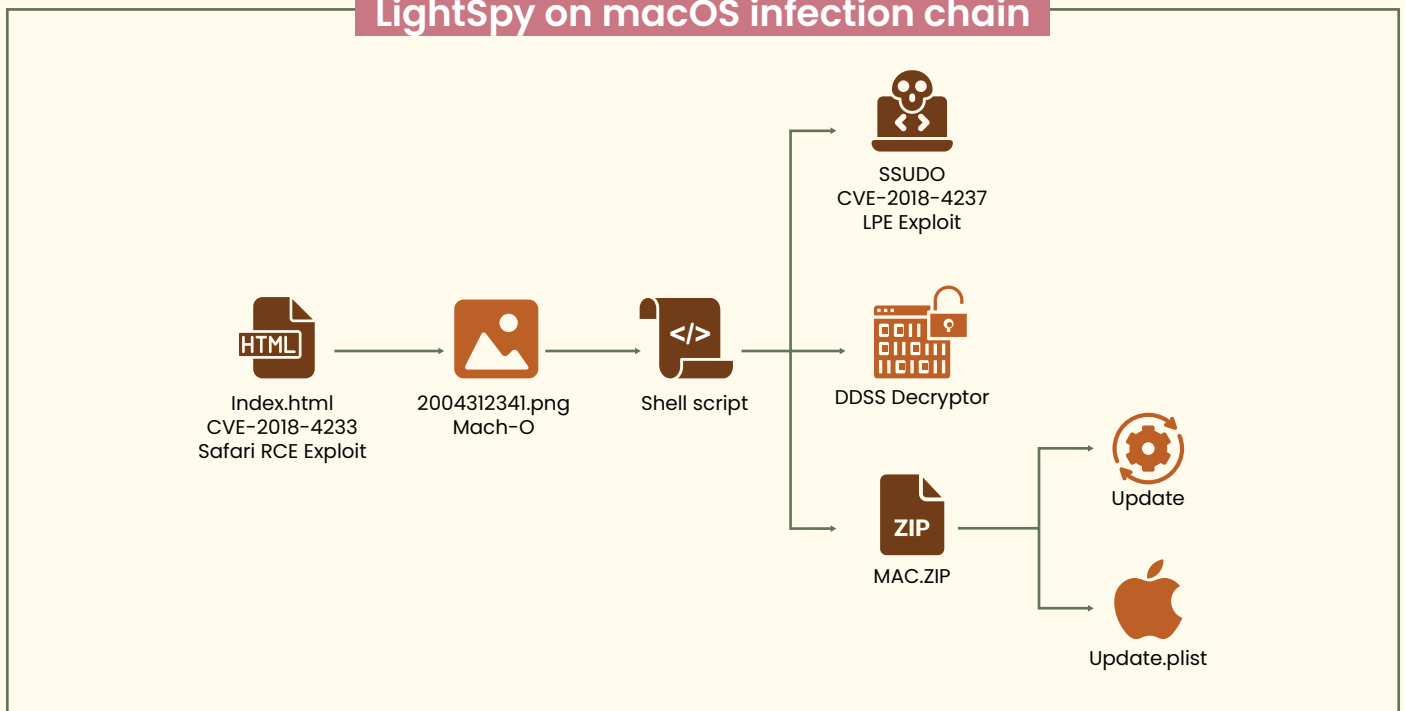
Criticality: Medium ■■

Target: Windows

Country/State/Region: South Asia

The LightSpy surveillance framework, previously known for targeting Android and iOS devices, has now been discovered on macOS. This tool is used to steal various types of data, including files, screenshots, location data, voice recordings, and payment information. The macOS version has been active since January 2024, primarily in testing environments. Researchers gained insights into its functionality by exploiting a misconfiguration in LightSpy's control panel.

## LightSpy on macOS infection chain



The macOS implant uses WebKit flaws to execute code within Safari on older macOS versions. It starts with a disguised binary file that decrypts and executes scripts to fetch further payloads. These payloads include a privilege escalation exploit and other utilities, eventually gaining root access and establishing persistence on the system. The core component, "macircloader," manages plugins and communicates with the command and control (C2) server, allowing extensive data exfiltration.

LightSpy's modular design includes various plugins for specific actions on compromised devices. While the macOS version uses ten plugins, the Android and iOS versions use more. Researchers also found evidence of implants for Windows, Linux, and routers, though their usage in attacks and operations remains unclear.



*Varanus komodoensis*

# Sophisticated Cyber-Espionage Campaign Targeting Indian Government Entities

Criticality: High 

Target: Windows

Sector targeted: Government agencies, Military, Maritime

Country/State/Region: India

A recent investigation has uncovered a sophisticated cyber-espionage campaign targeting multiple Indian government entities, including critical sectors such as the Air Force, maritime industries, including shipyards, docks, and ports. The campaign, attributed to a foreign APT group, has been observed using a variety of advanced techniques to infiltrate systems, maintain persistence, and exfiltrate sensitive data. Malicious payloads were hosted on compromised domains with open directories, often disguised as legitimate documents to deceive users into executing them.

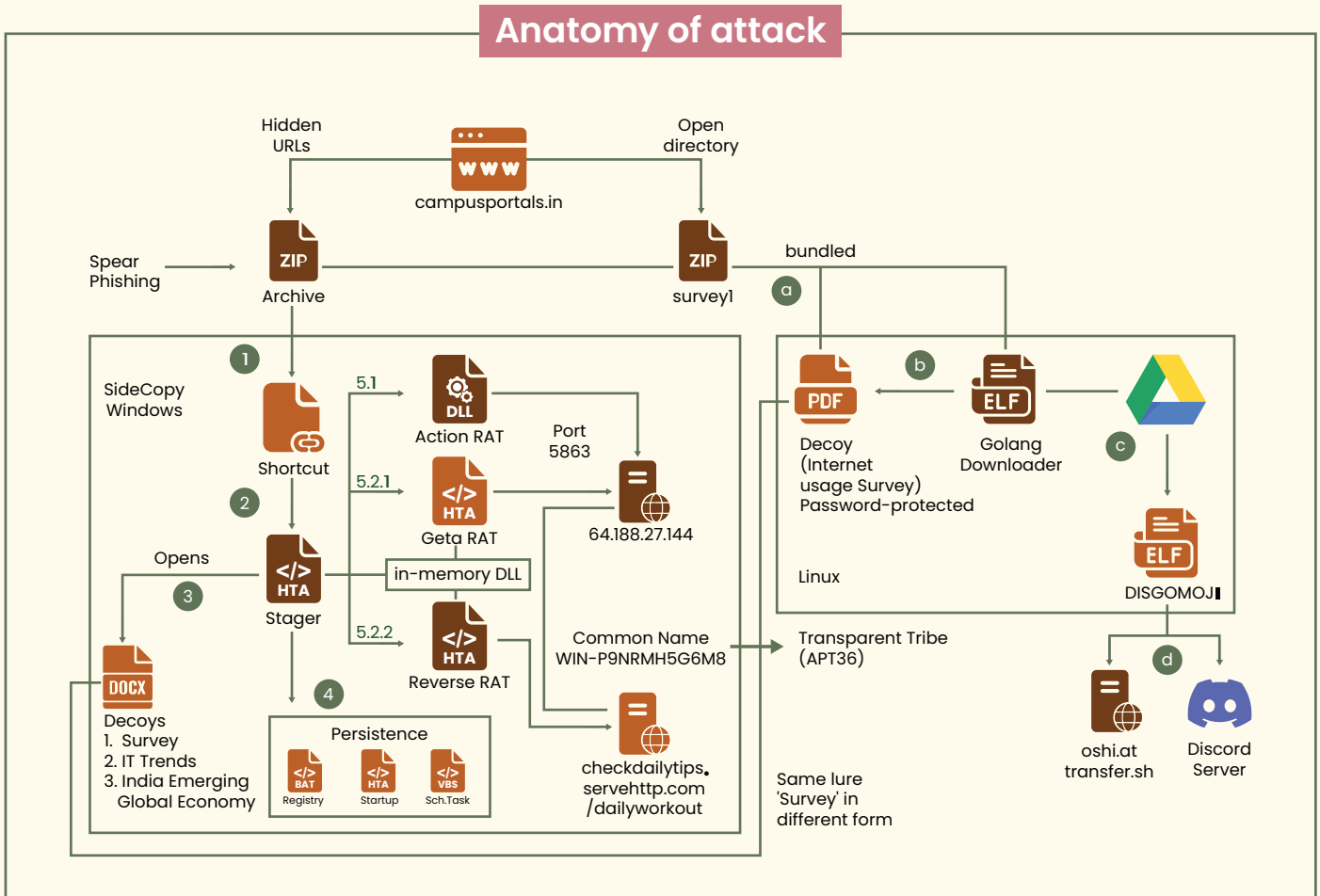
The attackers employed several sophisticated methods, including the use of Golang-based Linux payloads known as POSEIDON and DISGOMOJI. These payloads utilized Discord, a social platform, as a command-and-control (C2) platform, leveraging emojis for covert communication. Additionally, the threat actors used HTA (HTML Application) stagers, which fully evade detection by traditional security systems, and fileless remote access trojans (RATs) that run entirely in memory, making them difficult to detect and remove.

**Shared domains, IP addresses, and decoy files suggest a coordinated effort among multiple threat groups. These groups employed similar attack methods and infrastructure to compromise Indian systems.**

The analysis of the campaign revealed significant overlaps in tactics, techniques, and infrastructure used by this group and others targeting Indian assets. The payloads deployed in these attacks were capable of stealing sensitive browser data, taking screenshots, executing remote commands, and performing other malicious actions.

On compromised Windows systems, attackers deployed multiple types of remote access trojans (RATs), including Reverse RAT, Action RAT, and Geta RAT. Notably, Geta RAT shares functionality with the widely recognized Async RAT. These RATs provided unauthorized access, allowing attackers to monitor victim activity and exfiltrate sensitive data.

Furthermore, investigators discovered evidence of stager evasion testing against anti-virus solutions at locations associated with the attackers.



# Operation Oxidový

## Sophisticated Malware Campaign Targets Czech Officials using NATO-Themed Decoys



*Gloriosa superba*

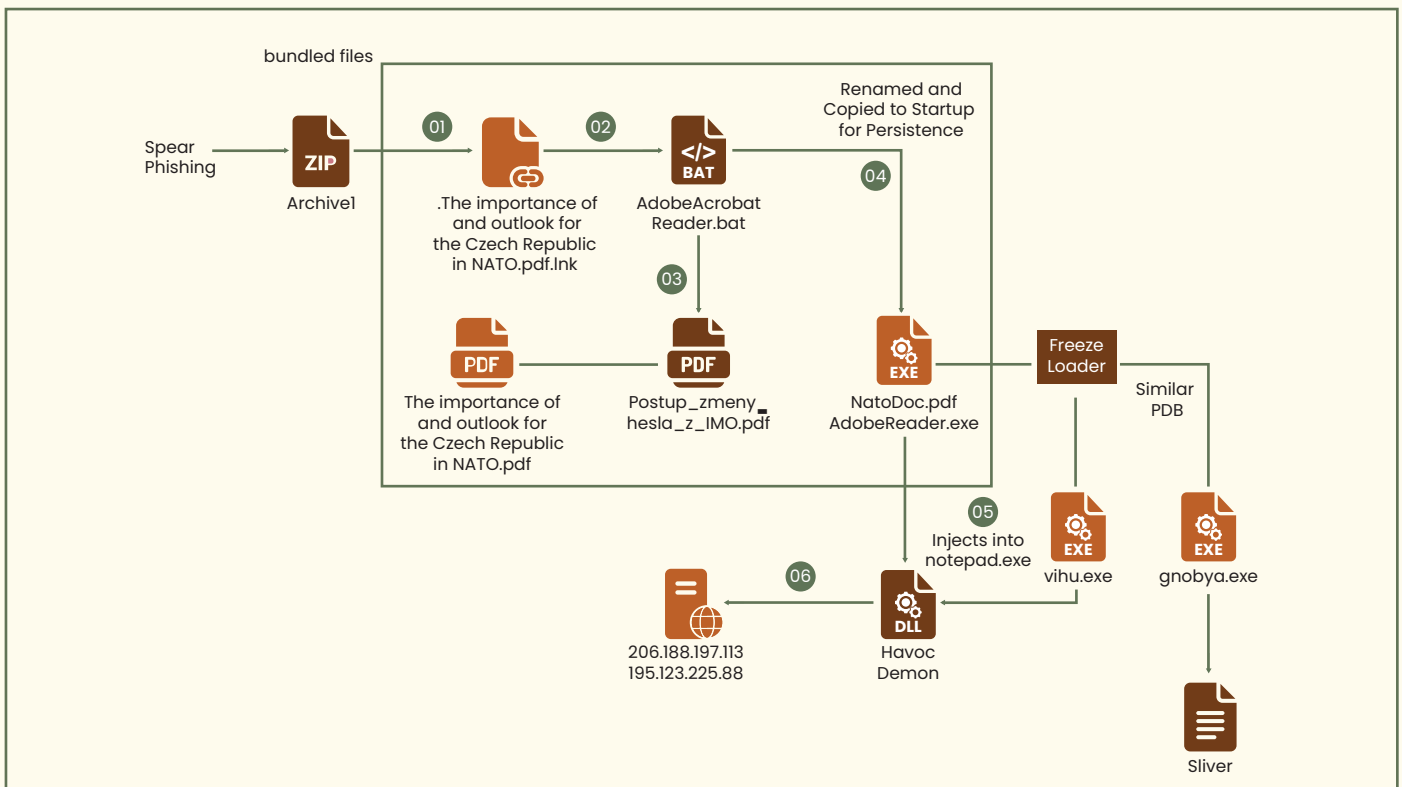
Criticality: Medium ■

Target: Windows

Sectors Targeted: Windows Users

Country/State/Region: Europe

Operation Oxidový is a highly sophisticated malware campaign which was uncovered in mid-2024, targeted Czech government and military officials. The attackers employed NATO-themed decoy documents to entice victims into downloading and executing malicious payloads. The decoys were cleverly crafted, appearing as official documents discussing Czech relations with NATO and internal password-change guidelines for the Ministry of Defense. Once the malicious documents were executed, they launched a batch script that delivered malware designed to infiltrate and persist on the victim's systems.



This campaign revolves around **Freeze**, a Rust-based malware loader originally created for legitimate red-team security operations. However, threat actors have since repurposed it for malicious use. Freeze employs sophisticated evasion techniques, such as ETW patching and DLL unhooking, to bypass security software. Once deployed, it delivers **Havoc**, a robust post-exploitation framework that allows attackers to retain control over compromised systems, exfiltrate sensitive data, and execute additional malicious commands remotely.

The operation has been attributed to a Russian linked threat group, likely driven by geopolitical motives related to the region. The sophistication of the malware tools and the specific targeting of Czech officials indicate a well organized campaign with substantial resources. Researchers analyzing the campaign have noted its extensive use of open-source offensive tools and advanced evasion tactics, making it a dangerous threat.



# Ghost Locker 2.0

## The Evolving Threat of Ransomware-as-a-Service Unveiled by GhostSec

*Atropa belladonna*

Criticality: High ■■

Target: Windows

Country/State/Region: Middle East, Africa & Asia

Ghost Locker ransomware is a sophisticated Ransomware-as-a-Service (RaaS) framework developed by the hacktivist group GhostSec, first introduced in October 2023. This advanced malware is designed to encrypt files on targeted systems, exfiltrate sensitive data and disable certain services or processes to evade detection by security measures.

### How does it work?

- ▲ By employing these tactics, Ghost Locker maximizes its chances of successfully extorting victims while minimizing the likelihood of early detection by cybersecurity defenses. Two distinct variants of Ghost Locker have been identified, one written in Python and the other in Go programming language, highlighting the ongoing development and adaptability of the framework to suit different threat actors and their operational preferences. After the encryption process is complete, the ransomware takes the additional step of deleting itself from the infected system, effectively covering its tracks and complicating recovery efforts for the victim.
- ▲ A key aspect of Ghost Locker's operation is its ability to communicate with a command and control (C2) server via a URL, enabling real-time interaction with the attacker. Upon successfully breaching a target, the ransomware informs the attacker of its progress and the successful execution of its malicious activities.

To secure the encrypted data, Ghost Locker generates a unique secret key using the Fernet symmetric encryption algorithm, which is then sent to the attacker in a JSON file. This key is crucial for the decryption of files, and it allows the attacker to retain control over the victim's data. In addition to encryption, the ransomware meticulously collects and exfiltrates victim data, sending this sensitive information directly to the attacker.

This capability not only facilitates further exploitation but also enables the attacker to make more informed ransom demands, potentially increasing the likelihood of financial gain from their malicious activities. The emergence of Ghost Locker underscores the evolving landscape of ransomware threats, where criminal groups are leveraging RaaS models to amplify their reach and effectiveness.

**By enabling less technically skilled criminals to access sophisticated ransomware tools, frameworks like Ghost Locker contribute to the rising tide of cyber extortion and data breaches, posing significant risks to individuals and organizations alike.**

```

v0 = gs_getenv("envpath")
v1 = gs_getenv("envpath")
v2 = gs_getenv("envpath")
v3 = gs_getenv("envpath")
v4 = gs_getenv("envpath")
v5 = gs_getenv("envpath")
v6 = gs_getenv("envpath")
v7 = gs_getenv("envpath")
v8 = gs_getenv("envpath")
v9 = gs_getenv("envpath")
v10 = gs_getenv("envpath")
v11 = gs_getenv("envpath")
v12 = gs_getenv("envpath")
v13 = gs_getenv("envpath")
v14 = gs_getenv("envpath")
v15 = gs_getenv("envpath")
v16 = gs_getenv("envpath")
v17 = gs_getenv("envpath")
v18 = gs_getenv("envpath")
v19 = gs_getenv("envpath")
v20 = gs_getenv("envpath")
v21 = gs_getenv("envpath")
v22 = gs_getenv("envpath")
v23 = gs_getenv("envpath")
v24 = gs_getenv("envpath")
v25 = gs_getenv("envpath")
v26 = gs_getenv("envpath")
v27 = gs_getenv("envpath")
v28 = gs_getenv("envpath")
v29 = gs_getenv("envpath")
v30 = gs_getenv("envpath")
v31 = gs_getenv("envpath")
v32 = gs_getenv("envpath")
v33 = gs_getenv("envpath")
v34 = gs_getenv("envpath")
v35 = gs_getenv("envpath")
v36 = gs_getenv("envpath")
v37 = gs_getenv("envpath")
v38 = gs_getenv("envpath")
v39 = gs_getenv("envpath")
v40 = gs_getenv("envpath")
v41 = gs_getenv("envpath")
v42 = gs_getenv("envpath")
v43 = gs_getenv("envpath")
v44 = gs_getenv("envpath")
v45 = gs_getenv("envpath")
v46 = gs_getenv("envpath")
v47 = gs_getenv("envpath")
v48 = gs_getenv("envpath")
v49 = gs_getenv("envpath")
v50 = gs_getenv("envpath")
v51 = gs_getenv("envpath")
v52 = gs_getenv("envpath")
v53 = gs_getenv("envpath")
v54 = gs_getenv("envpath")
v55 = gs_getenv("envpath")
v56 = gs_getenv("envpath")
v57 = gs_getenv("envpath")
v58 = gs_getenv("envpath")
v59 = gs_getenv("envpath")
v60 = gs_getenv("envpath")
v61 = gs_getenv("envpath")
v62 = gs_getenv("envpath")
v63 = gs_getenv("envpath")
v64 = gs_getenv("envpath")
v65 = gs_getenv("envpath")
v66 = gs_getenv("envpath")
v67 = gs_getenv("envpath")
v68 = gs_getenv("envpath")
v69 = gs_getenv("envpath")
v70 = gs_getenv("envpath")
v71 = gs_getenv("envpath")
v72 = gs_getenv("envpath")
v73 = gs_getenv("envpath")
v74 = gs_getenv("envpath")
v75 = gs_getenv("envpath")
v76 = gs_getenv("envpath")
v77 = gs_getenv("envpath")
v78 = gs_getenv("envpath")
v79 = gs_getenv("envpath")
v80 = gs_getenv("envpath")
v81 = gs_getenv("envpath")
v82 = gs_getenv("envpath")
v83 = gs_getenv("envpath")
v84 = gs_getenv("envpath")
v85 = gs_getenv("envpath")
v86 = gs_getenv("envpath")
v87 = gs_getenv("envpath")
v88 = gs_getenv("envpath")
v89 = gs_getenv("envpath")
v90 = gs_getenv("envpath")
v91 = gs_getenv("envpath")
v92 = gs_getenv("envpath")
v93 = gs_getenv("envpath")
v94 = gs_getenv("envpath")
v95 = gs_getenv("envpath")
v96 = gs_getenv("envpath")
v97 = gs_getenv("envpath")
v98 = gs_getenv("envpath")
v99 = gs_getenv("envpath")

```

**Creating Persistence**

```

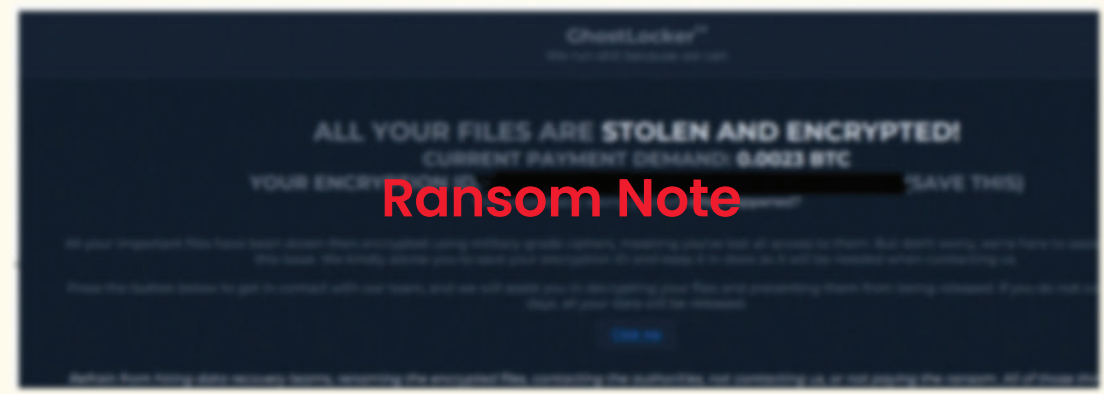
7
8 Drives = ghostlocker_file_getDrives();
9 v260 = v0;
10 v261 = v5;
11 v262 = (v0000 *)Drives;
12 v263 = ghostlocker_utils_kandstringbytesMaskImpBrc(32, v0, v5, v1, v2, v6);
13 v264 = v0;

```

**Obtainin Driver List**



**Creating ID**



**Ransom Note**

# ShadowCat Targets Indian Political Affairs



Criticality: Medium ■■

Target: Windows

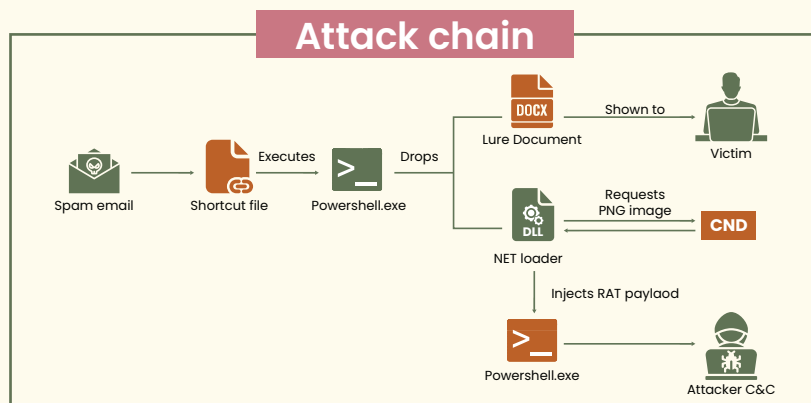
Country/State/Region: Worldwide

Operation ShadowCat is a sophisticated cyber-espionage campaign, likely carried out by a Russian speaking group, that targets individuals with a keen interest in Indian political affairs.

## How does it work?

- ▲ In this attack a malicious shortcut file (.LNK) is disguised as a legitimate document to lure victims. When executed, the LNK file triggers a series of commands through PowerShell, ultimately delivering a RAT written in the Go programming language. This RAT grants attackers control over compromised systems, enabling them to execute commands, manipulate files, and deploy ransomware. A key technique used in this attack is steganography, where a malicious Gzip-compressed payload is hidden within a PNG image hosted on a content delivery network (CDN). This payload is later injected into the system using asynchronous procedure call (APC) injection.

Operation ShadowCat is a sophisticated cyber-espionage campaign, likely carried out by a Russian speaking group, that targets individuals with a keen interest in Indian political affairs. The threat actors carefully avoid infecting systems in Russian-speaking countries, primarily targets government officials, journalists, researchers, and political analysts focused on Indian politics. The threat actors uses a command-and-control (C2) server and custom WebSocket communication to maintain control over the infected systems. Although CRIL cannot attribute the campaign to a specific threat actor or Advanced Persistent Threat (APT) group, the use of advanced techniques and the deliberate exclusion of Russian-speaking regions indicate that the group is likely financially motivated and may be associated with ransomware-as-a-service (RaaS) entities.





# Supply Chain Attack on Notezilla, RecentX and Copywhiz

Lantana camara

Criticality: Medium ■■

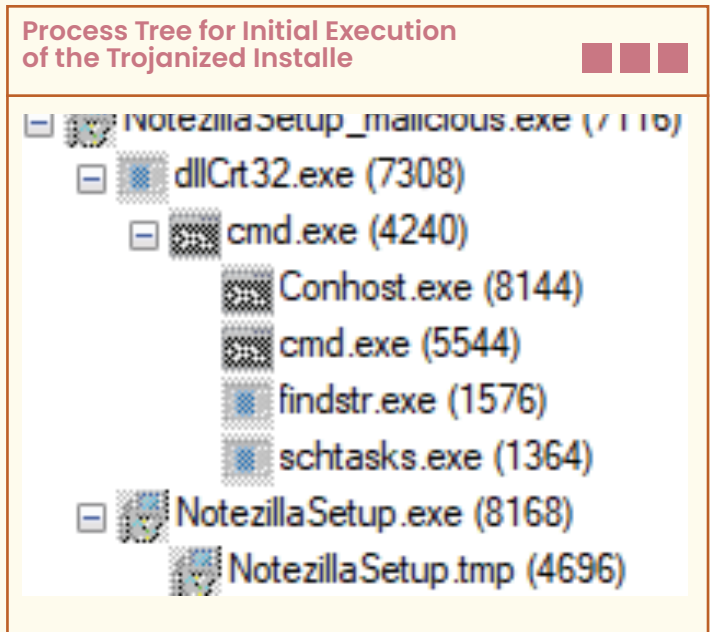
Target: Windows

Country/State/Region: Worldwide

Installers for Notezilla, RecentX, and Copywhiz, such popular software tools distributed by Indian based company Conceptworld Corporation has been in radar for doing malicious activities which upon investigation revealed several information. These installers had been trojanized to install malware that could steal browser credentials, cryptocurrency wallet data, and keystrokes, as well as download additional malicious payloads.

The malware was hidden within these legitimate softwares and persisted on infected systems via scheduled tasks, making it hard to detect. Conceptworld removed the infected installers and replacing them with legitimate versions.


The malware, observed in distribution since early June 2024, was designed to exfiltrate sensitive data by communicating with command-and-control (C2) servers. It targeted browsers like Google Chrome and Firefox and several cryptocurrency wallets. It is found that the malware used system tools like curl.exe to download more payloads and transfer stolen data to remote servers. It is always recommended users to verify software downloads for authenticity before installing.



# Ransomware Strikes Indian Banking Infrastructure



*Solenopsis invicta*

Criticality: High 

Target: Windows

Sector targeted: Technology, Government, Manufacturing

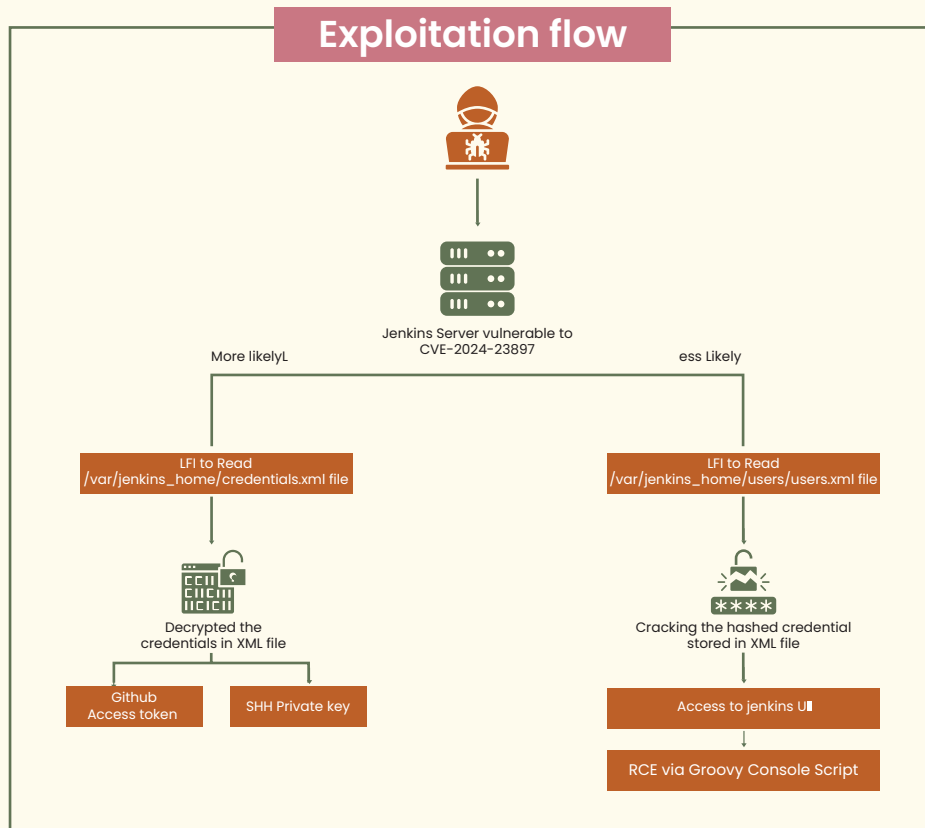
Country/State/Region: Asia, Europe, North and South America

The recent ransomware attack that disrupted India's banking ecosystem was traced back to a misconfigured Jenkins server at **Brontoo Technology Solutions, a key collaborator with C-EDGE**, a joint venture between Tata Consultancy Services (TCS) and the State Bank of India (SBI). The attack was facilitated by exploiting a Local File Inclusion (LFI) vulnerability, CVE-2024-23897, in the Jenkins instance used by Brontoo. This flaw allowed attackers to read sensitive internal files, including SSH keys, providing them unauthorized access to the server via an open SSH port (port 22).

**Misconfigured Jenkins servers are a common target for attackers due to their role in automating software development pipelines, making them an attractive entry point into larger networks.**


Once inside the compromised server, the attackers likely gained initial access through an Initial Access Broker (IAB), possibly linked to IntelBroker, a known threat actor in breach forums. Initial Access Brokers specialize in selling access to compromised systems to cybercriminal groups like RansomEXX, which use this access to deploy ransomware. **RansomEXX is a well-known ransomware group that has been active since 2018 (originally operating as Defray777) and targets large organizations through sophisticated attacks. By exploiting Brontoo's vulnerable Jenkins server**, the attackers were able to infiltrate the network and prepare for the ransomware deployment.

The RansomEXX v2.0 variant used advanced encryption methods, such as RSA-2048 and AES-256 which makes it nearly impossible without the decryption key. RansomEXX typically employs a dual strategy of encrypting critical files and backups while also exfiltrating sensitive data. The attack chain involved not only the exploitation of the LFI vulnerability but also sophisticated lateral movement techniques. After gaining initial access, the attackers deployed tools such as Cobalt Strike and Mimikatz to escalate privileges and move laterally across Brontoo's infrastructure.



*Nerium oleander*

# Operation Celestial Force Target Indian Entities

Criticality: High 

Target: Windows

Sector targeted: Government and Defense

Country/State/Region: India

Operation Celestial Force is a complex, multi-stage cyberattack campaign that has been active since at least 2018, targeting users primarily in the Indian subcontinent. The operation is conducted by a group of advanced persistent threat (APT) actors leveraging both Windows and Android-based malware. **This campaign utilizes a range of tactics, including spear phishing, social engineering, and malicious document attachments to compromise victim systems.** The malware used in this operation includes variants such as GravityRAT and HeavyLift, which are employed to establish remote access and exfiltrate sensitive information.

## Attack Progression and Malware Evolution

Initially, the campaign began with the use of a remote access trojan (RAT), delivered through malicious documents (maldocs) to compromise Windows systems. **By 2019, the threat actor expanded its toolkit, introducing Android based versions of GravityRAT, which allowed the group to target mobile devices.** The attackers also deployed HeavyLift, a malware loader designed to infect Windows systems via social engineering tactics, often disguised as legitimate software installers. HeavyLift is used to install additional payloads, further compromising infected systems.

The malware in this operation is managed through a command-and-control (C2) server called GravityAdmin, which controls both GravityRAT and HeavyLift infections. The C2 servers issue commands to infected systems, instructing them to execute specific tasks and exfiltrate data. **The operation includes various campaigns, each with unique identifiers such as SIERRA, QUEBEC, and FOXTROT. These labels correspond to distinct infection vectors, targeted operating systems, and specific malware functionalities within the campaign.**

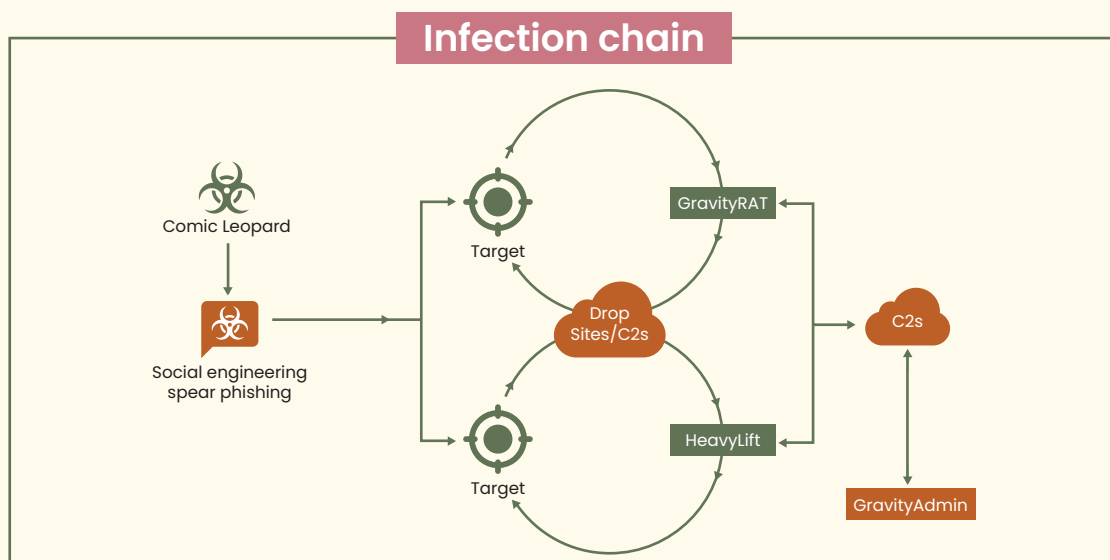
## Infection and Exfiltration Process

The infection process typically begins through spear phishing emails or targeted social media outreach, wherein victims are deceived into opening malicious attachments or links. Once the malware is installed, it connects to the C2 servers, where it receives instructions to perform malicious actions, including the exfiltration of sensitive data. **The attackers utilize Cloudflare services to obfuscate the location of their C2 infrastructure, adding another layer of complexity to the attack.**

To maintain persistence on compromised systems, the threat actors employ various techniques, including scheduled tasks on Windows and crontab on macOS. The use of electron-based malware loaders in GravityRAT suggests that the attackers are continually evolving their tools to evade detection and increase the effectiveness of their operations.

## Current Activity and Ongoing Threat

The Celestial Force campaign continues to evolve, with new variants of GravityRAT and HeavyLift regularly emerging. The campaign remains highly organized, with tailored C2 panels for different types of malware, enabling the attackers to adapt their tactics based on the specific target. This ongoing threat underscores the importance of robust cybersecurity measures, particularly in regions frequently targeted by advanced persistent threats.



# Ongoing Cyber Espionage Campaign Targeting Defense Personnel



*Couroupita guianensis*

Criticality: High

Target: Windows

Sector targeted: Government and Defense

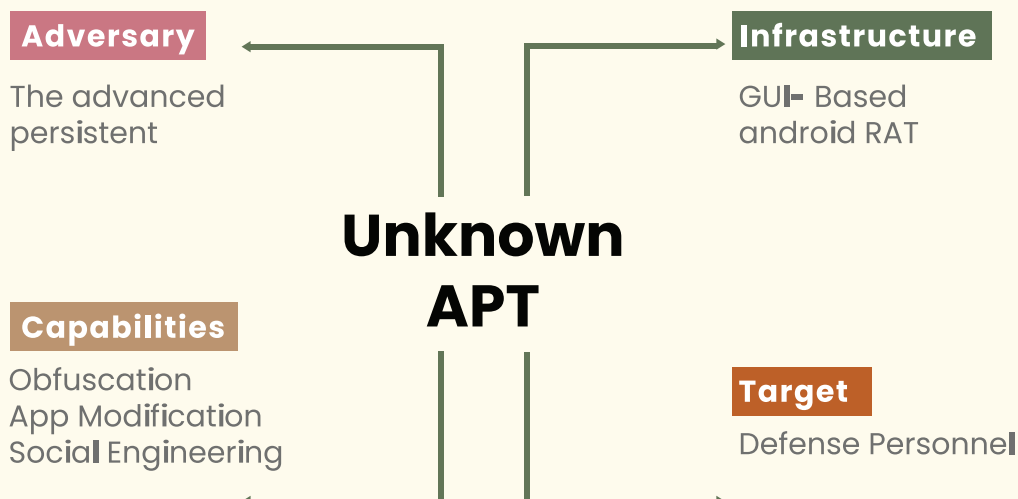
Country/State/Region: India

An advanced persistent threat (APT) group has been targeting Indian defense personnel for over a year using a modified Spynote remote access tool, known as Craxs Rat.

## How does it work?

- ▲ The campaign involves social engineering via WhatsApp, where the malware is disguised as defense-related applications like “MNS NH Contact.apk” and “Posted out off.apk.”
- ▲ Once installed, the malware requests minimal permissions but secretly accesses sensitive data, including SMS, contacts, and files. It includes a screen monitoring feature that activates only when accessibility settings are enabled, ensuring stealth. The app’s code is heavily obfuscated and is split into 600 parts to evade antivirus detection.

The threat actor uses Craxs Rat, a popular malware tool among cybercriminals, particularly in espionage operations. It’s designed for exfiltrating intelligence, specifically targeting defense and military personnel. The malware’s persistence and obfuscation tactics make it a serious, ongoing cyber espionage threat.





# THE GEOPOLITICS OF CYBERSECURITY

THREATS, STRATEGIES AND ALLIANCES



# The Geopolitics of Cybersecurity: Threats, Strategies and Alliances

## Near-Term Horizon (2025-2026)

### 01. Increased state-sponsored attacks

- AI enhanced APT
- Multi stage attack chain
- Supply chain infiltration

### 02. Advanced AI-powered threats

- Self evolving malware
- Adaptive evasion
- Context aware social engineering

### 03. Quantum computing challenges

- Cryptographic threats
- Blockchain risks

### 04. Supply chain compromises

- Software poisoning
- Hardware trojans
- Pipeline attacks

### 05. Critical infrastructure targeting

- Energy grid
- Financial networks
- Healthcare infrastructure

## Long-Term Projections (2026-2030)

### 01. Emergence of Quantum Warfare

- Quantum radar
- Communication
- Sensory technologies

### 02. Autonomy of AI in Cyber Operations

- Threat hunting
- Cognitive security operations
- Sentient defence systems

### 03. Targeting of Space Infrastructure

- Satellite communications
- GPS
- Space based sensors

### 04. Battles for Digital Sovereignty

- Data localization
- Currency digitalisation
- International sovereignty

The intersection of geopolitics and cybersecurity is more critical than ever, both in global and local contexts. Nations are leveraging cyber capabilities to advance their strategic objectives, while also facing the growing challenge of defending against sophisticated and coordinated cyberattacks.

India, one of the world's largest and fastest-growing digital economies, is finding itself at the intersection of regional geopolitical tensions and escalating cyber threats. The ongoing conflict between Israel and Iran, and the broader Middle Eastern instability, has led to a surge in cyberattacks targeting Indian infrastructure, driven largely by political motivations from both state actors and hacktivist groups.



# The Surge in Hacktivist Attacks: Israel–Palestine Fallout

---

India has become a significant target for hacktivist groups aligned with pro-Palestinian causes since the outbreak of the Israel– Hamas war in October 2023. The country’s diplomatic stance and growing relationship with Israel have made it a prime target for retaliatory cyberattacks. Pro-Palestinian hacktivist groups, such as Ghost of Palestine, Anonymous Arabic, and KromSec, have launched a steady barrage of cyberattacks against the Indian government entities, businesses, and critical infrastructure.

**These attacks have taken various forms, including:**

-  **Website defacements:** Hackers have defaced high-profile Indian websites, replacing them with political messages, often related to the Palestine cause. Some websites have been left with calls to action or explicit threats directed at the Indian government for its perceived support of Israel.
-  **DDoS attacks:** Distributed Denial of Service (DDoS) attacks have targeted critical services, disrupting operations of Indian financial institutions, government portals, and private corporations.
-  **Data leaks and breaches:** Hacktivist groups have leaked sensitive data from Indian entities, including personal information, financial records, and internal communications, with the intention of discrediting India’s political alliances and amplifying the narrative of the Israel– Palestine conflict.

**In 2023 alone, over 150 hacktivist groups have targeted Indian entities, with daily attack volumes surpassing 50 incidents.**

---

The sheer volume of these attacks has posed a significant challenge for India’s cybersecurity response frameworks, especially given the sophisticated methods employed by these groups.

## Indian Cyber Response and Retaliation

---

Ever since hacktivists began ramping up their attacks, India has experienced a rise in retaliatory cyber operations. Indian hacking groups, motivated by nationalistic sentiments or in defense of India’s position on the Israel– Palestine conflict, have launched their own cyberattacks against perceived pro-Palestinian targets. Indian hacktivist groups have defaced websites, leaked data from organizations supporting Palestine, and launched cyberattacks on countries viewed as sympathetic to the Palestinian cause.

The Indian Cyber Crime Coordination Centre (I4C), established by the Ministry of Home Affairs, has taken a proactive stance in responding to these threats. The Indian government has enhanced cybersecurity measures, launched public awareness campaigns, and ramped up collaborations with international cybersecurity organizations to strengthen defense capabilities. However, the speed and scale of hacktivist attacks have already tested India’s cyber defense infrastructure, highlighting the need for more robust and agile responses to politically motivated cyber incidents.

# Geopolitical Alliances and Cybersecurity Cooperation



---

India's position within the broader geopolitical context further complicates its cybersecurity challenges. As a key ally of Israel in the Middle East and a member of the Quad (with the US, Japan, and Australia), India faces mounting pressure from hostile state-sponsored actors and hackers.

India's cybersecurity alliances with countries like the US and Israel are becoming increasingly important as both countries share intelligence, and collaborate on cybersecurity research and development. Joint cybersecurity initiatives, such as threat intelligence sharing and coordinated defense measures, have proven critical in defending against sophisticated cyberattacks.

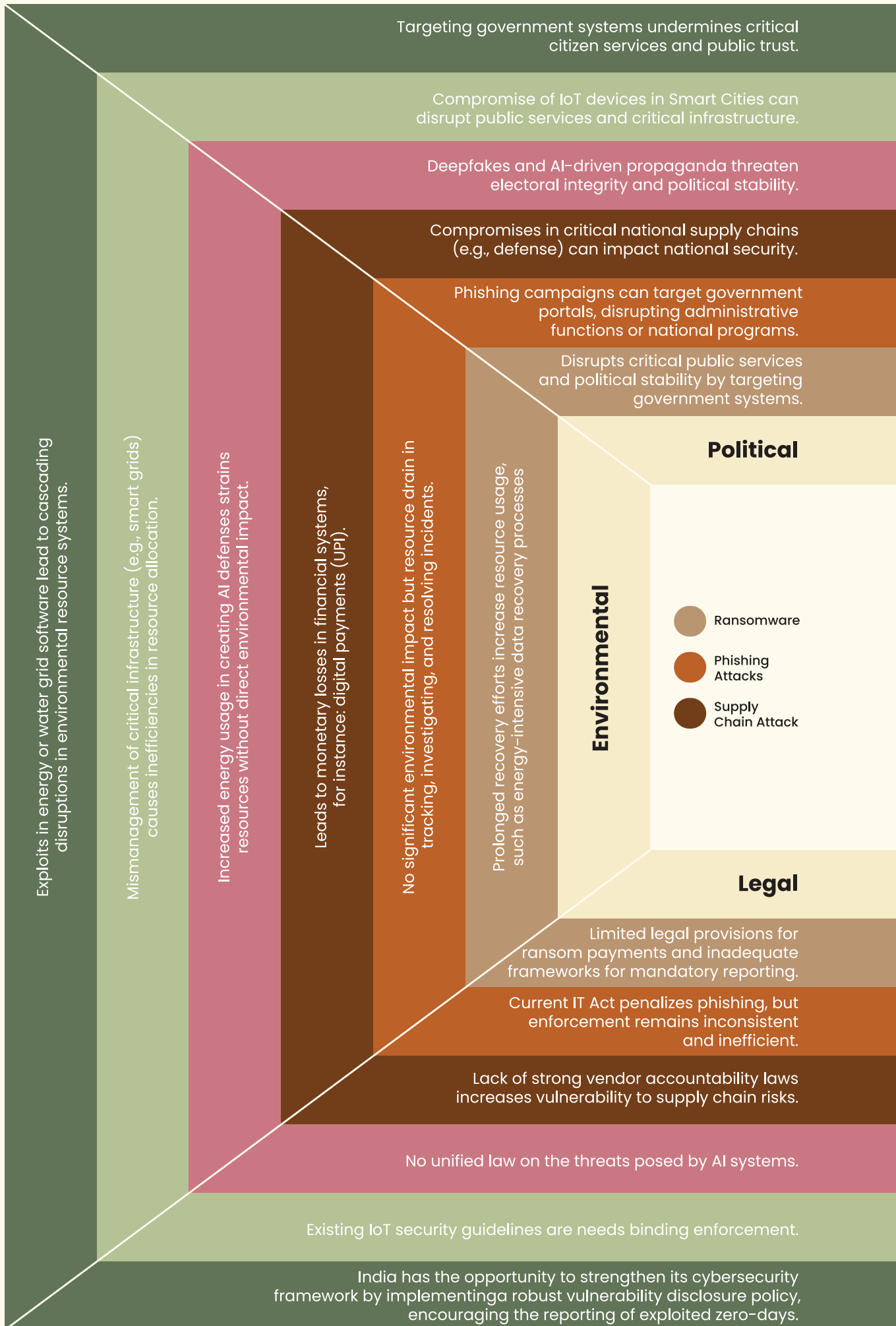
However, the evolving nature of cyber warfare means that India must continue to adapt its approach to cybersecurity, particularly in the face of regional instability. Proactively engaging with international partners to develop better cyber defense tools, fostering public-private partnerships, and increasing cybersecurity education and awareness will be the key in maintaining India's resilience against such politically motivated cyber threats.

## Key areas of focus for India's cybersecurity strategy in the coming years should include:

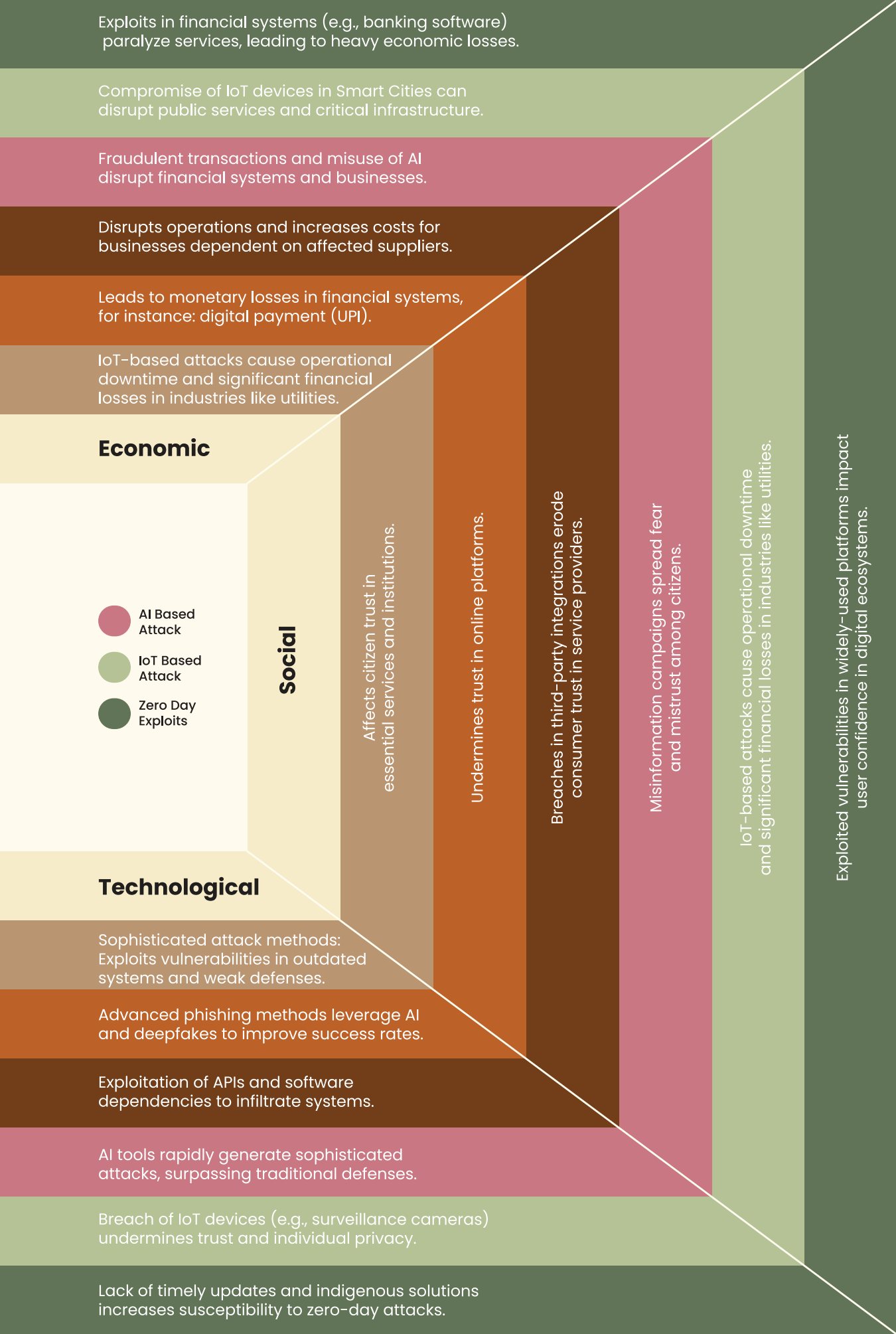
-  **Enhancing critical infrastructure protection:** Indian critical infrastructure, particularly in sectors like finance, energy, and healthcare, needs to be better shielded from cyberattacks. Implementing stronger cyber resilience measures, and ensuring continuity of services during an attack will be crucial.
-  **Developing a strong national cyber defense framework:** India has made significant strides in cybersecurity policy, but a more unified and coherent national strategy is needed to address the evolving threats from hacker groups and state-sponsored actors.
-  **Fostering international cooperation:** Expanding India's collaboration with global cybersecurity alliances, such as the Global Forum on Cyber Expertise (GFCE) and INTERPOL's Cybercrime Centre, will be an essential move to counter transnational cyber threats.



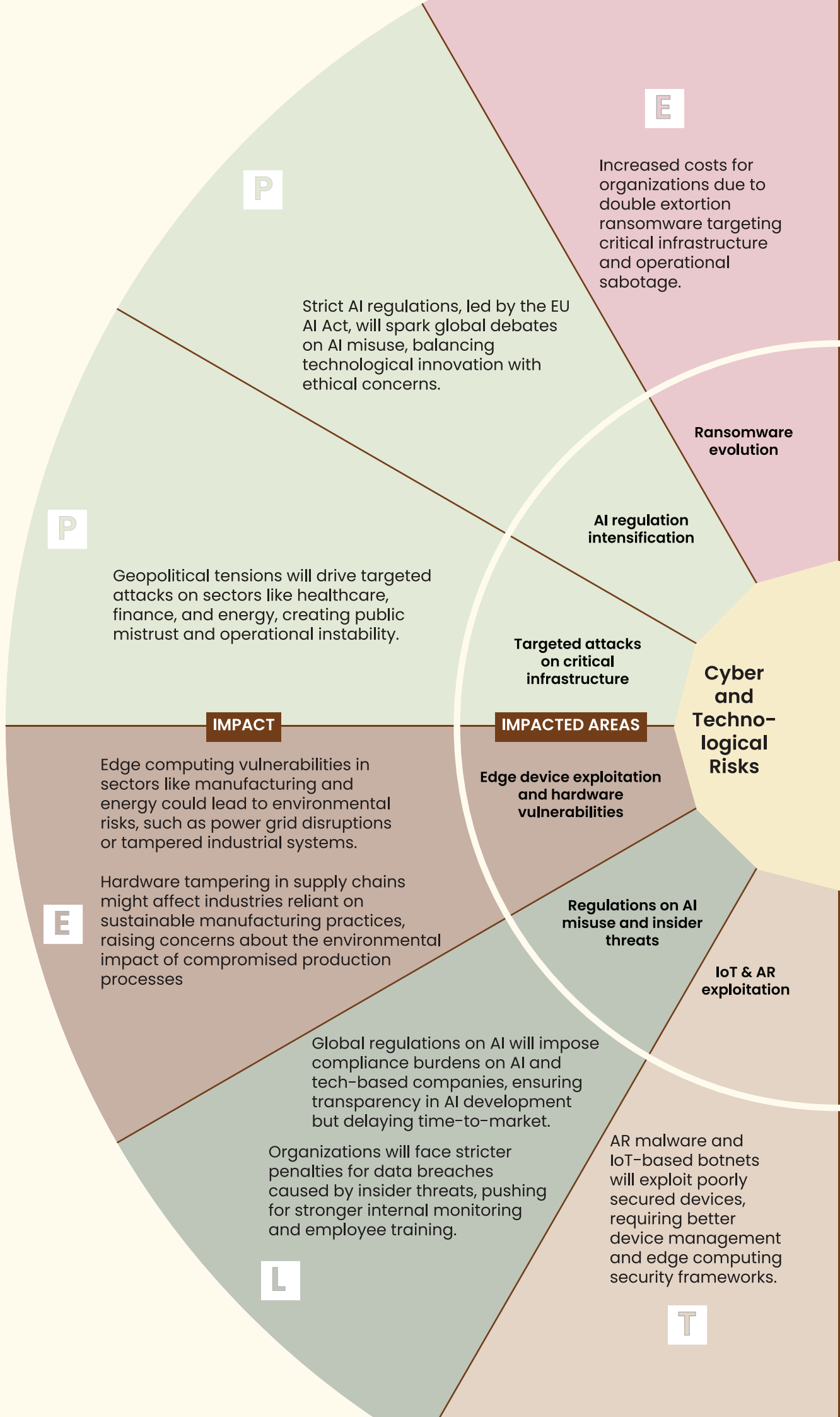
# PESTLE Analysis



# PESTLE Analysis

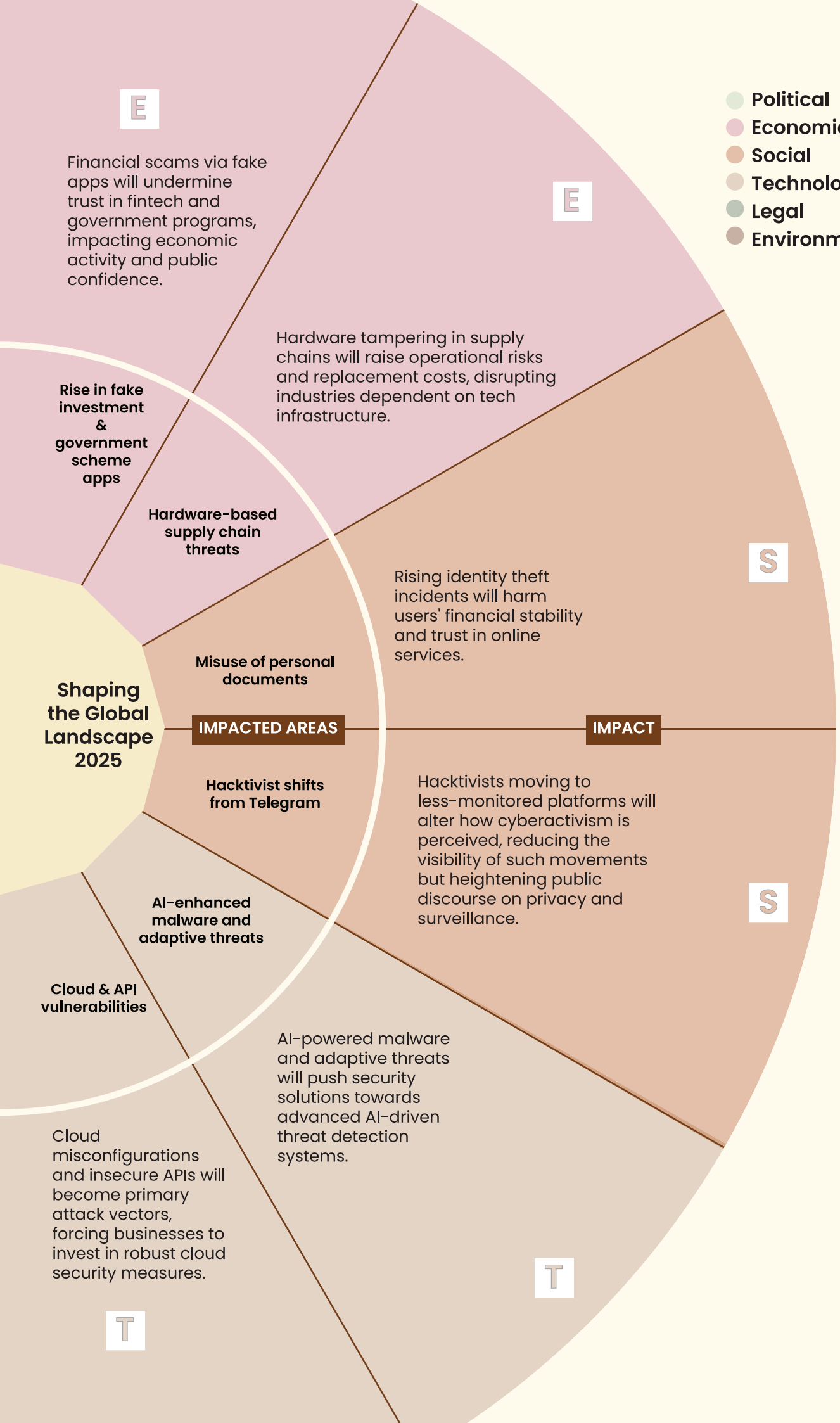


# Cyber and Technological Risks



# Risks Shaping the Global Landscape 2025

- Political
- Economic
- Social
- Technological
- Legal
- Environmental







# INDUSTRY CYBERSECURITY PREPAREDNESS SURVEY



# Industry Cybersecurity Preparedness

## Survey Methodology

### Research Objective

The primary objective of this study is to assess the cybersecurity maturity across various industries in India. Specifically, the research focuses on evaluating aspects such as cyber hygiene, investment in cybersecurity to foster awareness, data security, defenses against malware, and incident response capabilities. By doing so, the study aims to determine how well-prepared different industries are to tackle a range of cyber threats.

### Research Design

This study employs a quantitative research design, utilizing a structured survey to gather data from a diverse set of organizations. The quantitative approach allows for the systematic measurement and comparison of cybersecurity maturity across different sectors and organizational sizes.

### Sample Selection

A total of 204 organizations participated in the survey, representing 18 distinct industry sectors. The sample was stratified based on organizational size to ensure comprehensive coverage and to facilitate meaningful comparisons. Organizations were categorized into four distinct groups:

- ▲ **Enterprise:** Organizations with over 2,000 employees
- ▲ **Mid-Market:** Organizations with 500 to 2,000 employees
- ▲ **Small and Medium Businesses (SMB):** Organizations with 100 to 500 employees
- ▲ **Micro Enterprises:** Organizations with fewer than 100 employees

This stratification ensures that the study captures a wide spectrum of organizational structures and resources, which may influence cybersecurity maturity.

### Participant Profiles

Respondents within these organizations varied in their roles to provide a holistic view of cybersecurity practices and priorities. The survey targeted individuals in executive positions (CXOs) as well as those in mid-management roles. This range of respondent profiles ensures that the data reflects both strategic and operational perspectives on cybersecurity.

### Data Collection

The data for this study was gathered through a structured online survey distributed to a targeted group of organizations. The survey was designed to assess multiple facets of cybersecurity maturity. Key dimensions evaluated included:



## Data Analysis

The collected data was analyzed to achieve several key objectives:

- ▲ **Prioritization of Cybersecurity Investments for 2025:** Identifying the top areas where organizations plan to allocate resources to enhance their cybersecurity posture.
- ▲ **Maturity Scoring:** Developing maturity scores for each organizational size. These scores reflect the current state of cybersecurity practices and readiness to handle cyber threats.
- ▲ **Comparative Analysis:** Comparing maturity scores across different organization sizes to identify patterns, strengths, and areas needing improvement.

Statistical tools and software were employed to ensure the accuracy and reliability of the analysis. The maturity scores were mapped to provide a clear visualization of the cybersecurity landscape across organizational sizes.

## Reliability and Validity

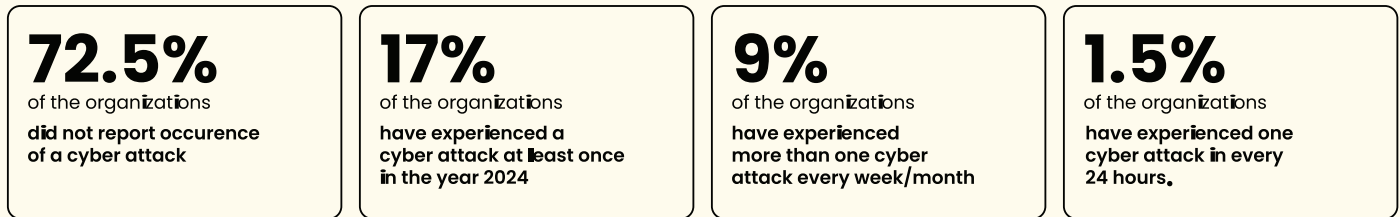
To ensure the reliability and validity of the findings, the survey was pre-tested with a small group of organizations to refine questions and eliminate ambiguities. Furthermore, data triangulation was conducted by complementing the primary research findings with insights gathered from secondary research.

## Limitations

While the study provides comprehensive insights into cybersecurity maturity, it is subject to certain limitations. The reliance on self-reported data may introduce biases, as respondents might overstate or understate their organization's cybersecurity capabilities.

# Survey Insights

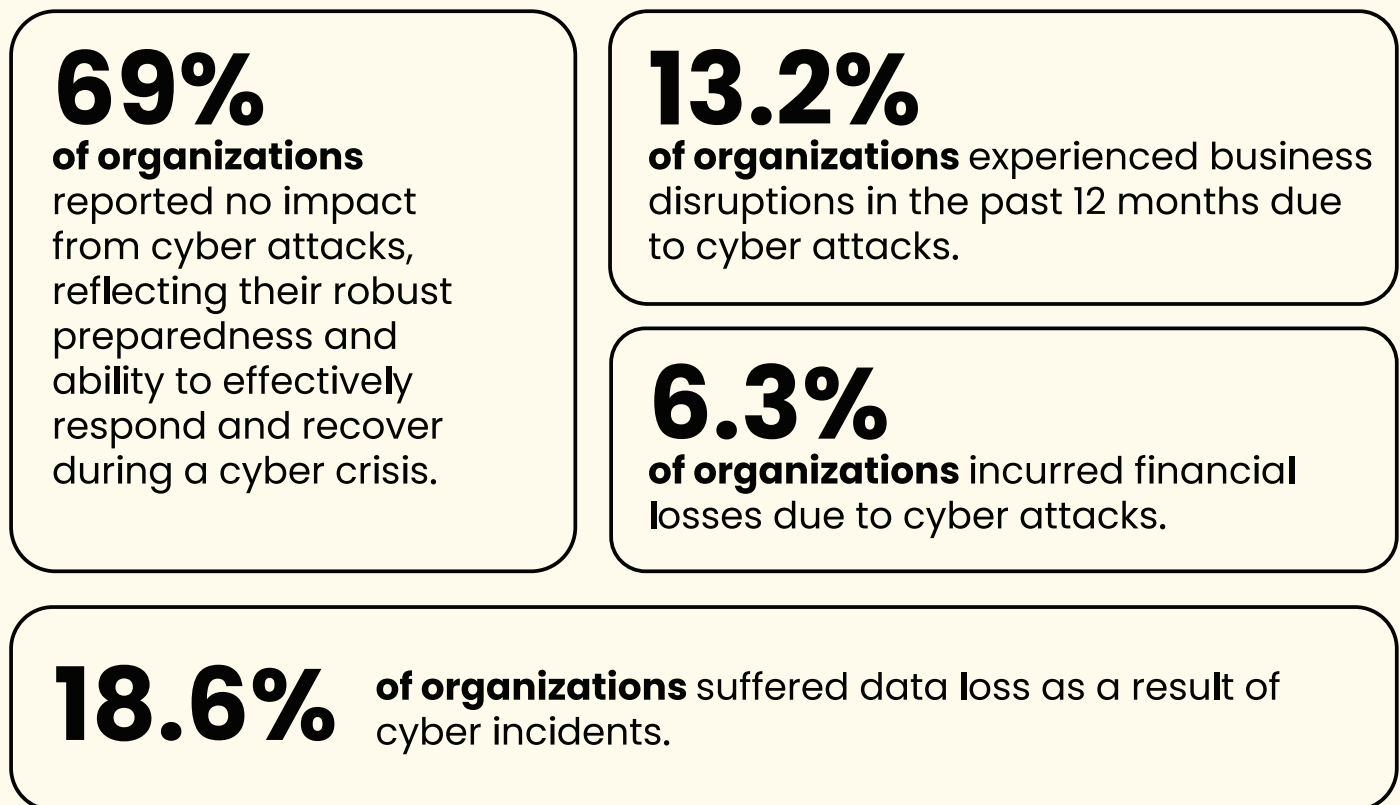
## Cyber attack target spectrum



## Types of threats observed

- ▲ Social Engineering attacks (Phishing, Vishing, Smishing, Shoulder Surfing, etc.) top the list, followed by malware attacks and ransomware.
- ▲ AI/ML based attacks are the new entrant in 2024.
- ▲ Software / 0-day vulnerabilities.

## Cyber resilience



## The top 5 challenges in adoption of cybersecurity workforce and expertise

- ▲ Lack of Cybersecurity Expertise and Knowledge
- ▲ Inadequate Staffing and Organizational Resources
- ▲ Budget Limitations Affecting Cybersecurity Initiatives
- ▲ Insufficient Board-Level Focus on Cybersecurity
- ▲ Executive Team's Limited Focus on Cybersecurity

### Threat Intelligence



Only **45%**  
of the participated organizations  
consume threat intelligence  
(either OSINT or commercial  
or both) for proactive  
cyber defence

### Attack Surface Monitoring



**39%**  
of the participated organizations  
monitor their attack surface  
continuously and take remedial  
actions on time

### Cyber Hygiene



**42.6%**  
organizations  
demonstrate maturity in  
defining and implementing  
effective cyber hygiene  
practices

### Securing Assets



**33.9%**  
organizations  
exhibit advanced maturity  
in safeguarding assets,  
including hardware, software,  
data, and related resources.

### Malware Protection



**63%**  
organizations  
demonstrate advanced  
maturity in defending  
against malware threats

### Data Security



**8.8%**  
of organizations  
are yet to implement  
data controls to  
protect data

**61.8%**  
of organizations  
have implemented  
systematic data  
classification to  
enhance security.

### Access Control



**46%**  
of the participated organizations  
have proper access control  
mechanisms for managing  
identity and ensuring only  
authorized personnel have  
access to the data

### Secure Configuration



**11.8%**  
of the organizations  
are yet to implement process  
and protocols to protect their assets  
via secure policies/configuration

### Software Updates & Patch Management



# 63.7%

of the organizations

have implemented patch management process to secure their systems from vulnerability exploitation

### Backup and Recovery



# 52.9%

of the organizations

have defined and implemented strategies backup strategy

### Incident Response



# 56.3%

of the organizations

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

### Process



# 19%

of the organizations

don't test their security processes

## Top Cybersecurity Investment Priorities for 2025

As cyber threats become increasingly sophisticated and pervasive, organizations must strategically allocate resources to strengthen their cybersecurity posture.

Based on the survey findings from industry experts, C-suite executives should prioritize the following cybersecurity investments in 2025.

### Core Security Foundation

# 1

#### THREAT DETECTION & RESPONSE

Focus

- ▶ AI/ML-powered real-time detection
- ▶ Automated threat hunting
- ▶ Behavioral analytics
- ▶ Incident response protocols

# 2

#### DATA PROTECTION

Focus

- ▶ Strong encryption
- ▶ Access controls
- ▶ Data loss prevention
- ▶ Information confidentiality

# 3

#### ENDPOINT SECURITY

Focus

- ▶ Next-gen antivirus
- ▶ Device monitoring
- ▶ IoT security
- ▶ Malware protection

# 4

#### CLOUD SECURITY

Focus

- ▶ Cloud posture management
- ▶ Trojan protection
- ▶ Security services integration
- ▶ Environment protection

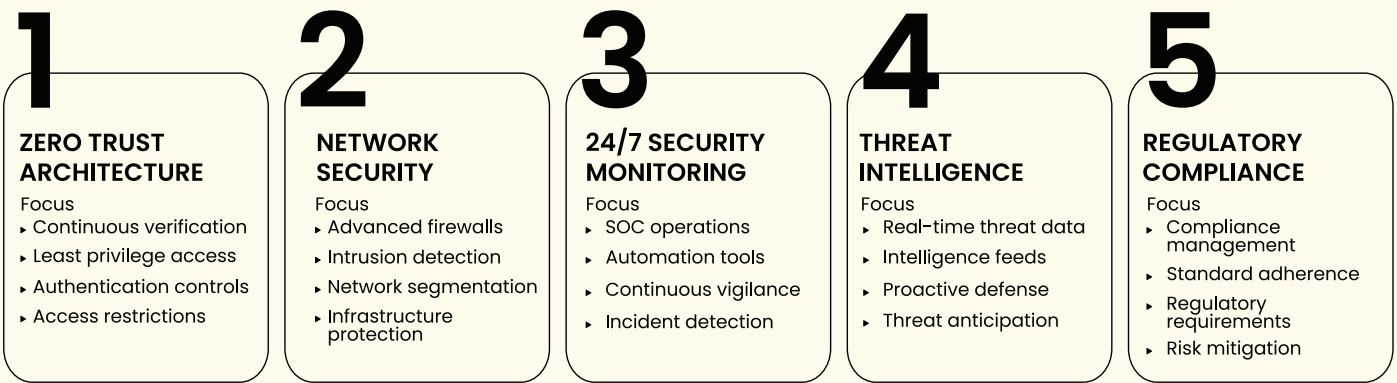
# 5

#### EMPLOYEE TRAINING

Focus

- ▶ Security awareness
- ▶ Phishing prevention
- ▶ Best practices
- ▶ Continuous education

## Advance Security Measures

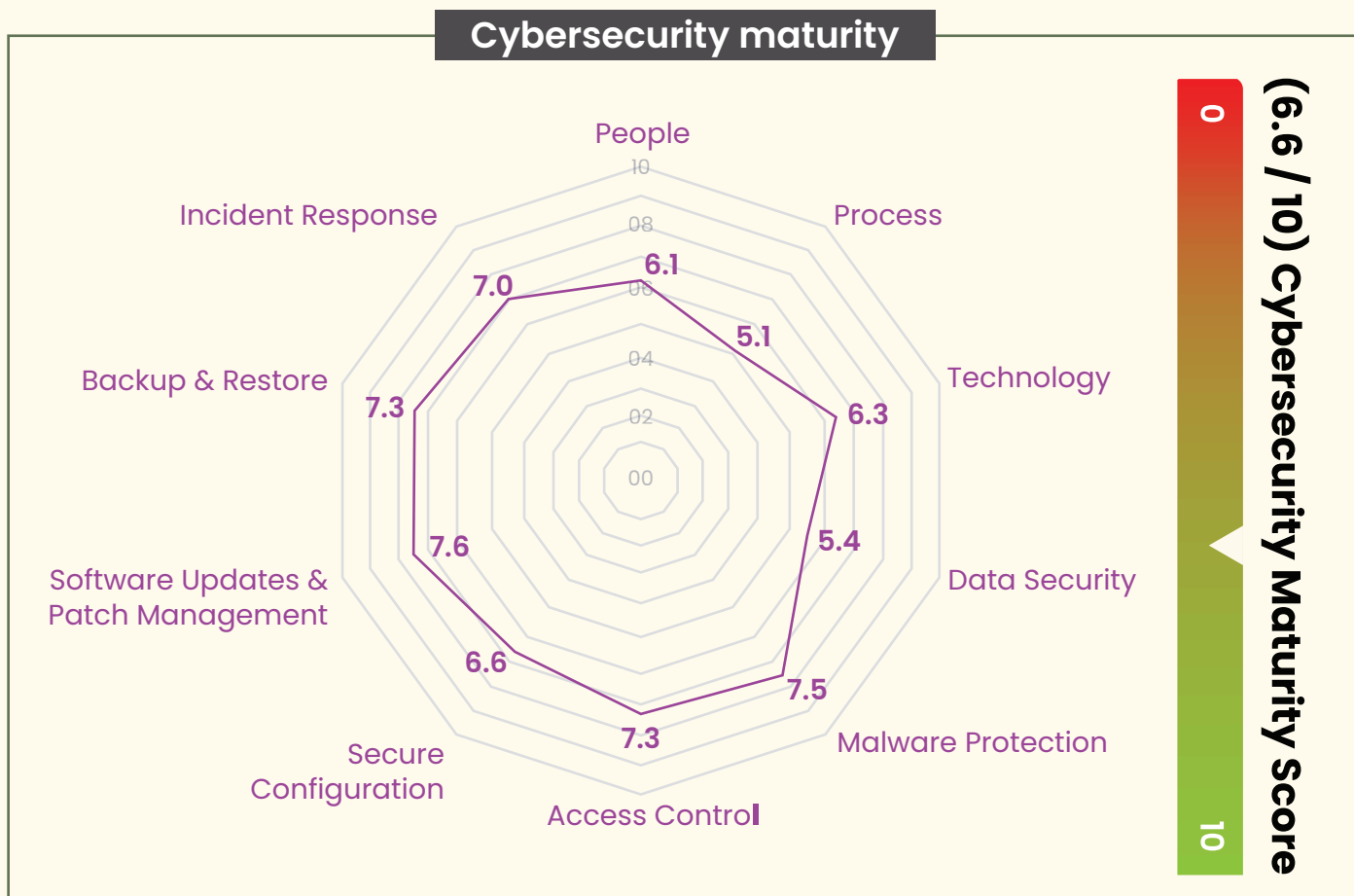


## Cybersecurity Maturity Radar Map

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 breaches.
- ▲ **Malware Protection:** Examines the ability to prevent, detect, and respond to malware threats.
- ▲ **Access Control:** Analyzes how well access to systems and information is restricted.
- ▲ **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 analyzed sample size, the maturity score stands at 6.6/10, indicating a moderate level of maturity with room for improvement.**



## Cybersecurity Maturity Radar Map – Market Segments

The cybersecurity maturity varies significantly across different organizational sizes and sectors, necessitating tailored approaches to address unique challenges. This section explores cybersecurity maturity and priorities across four key segments: Enterprise, Mid-Market, MSME, and SMB. Each segment reflects distinct security requirements, resource allocations, and strategic focuses.

### Interpreting the radar

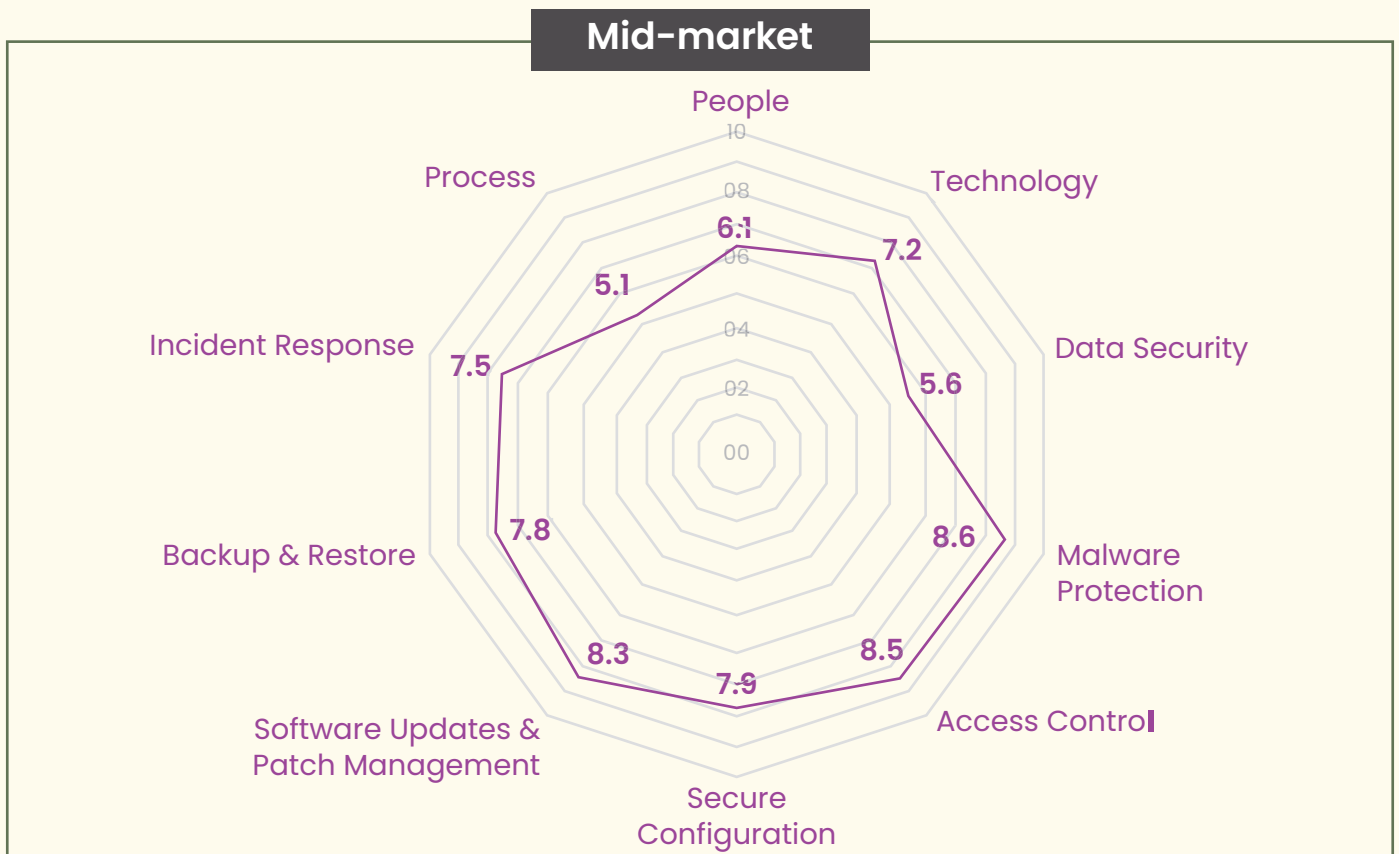
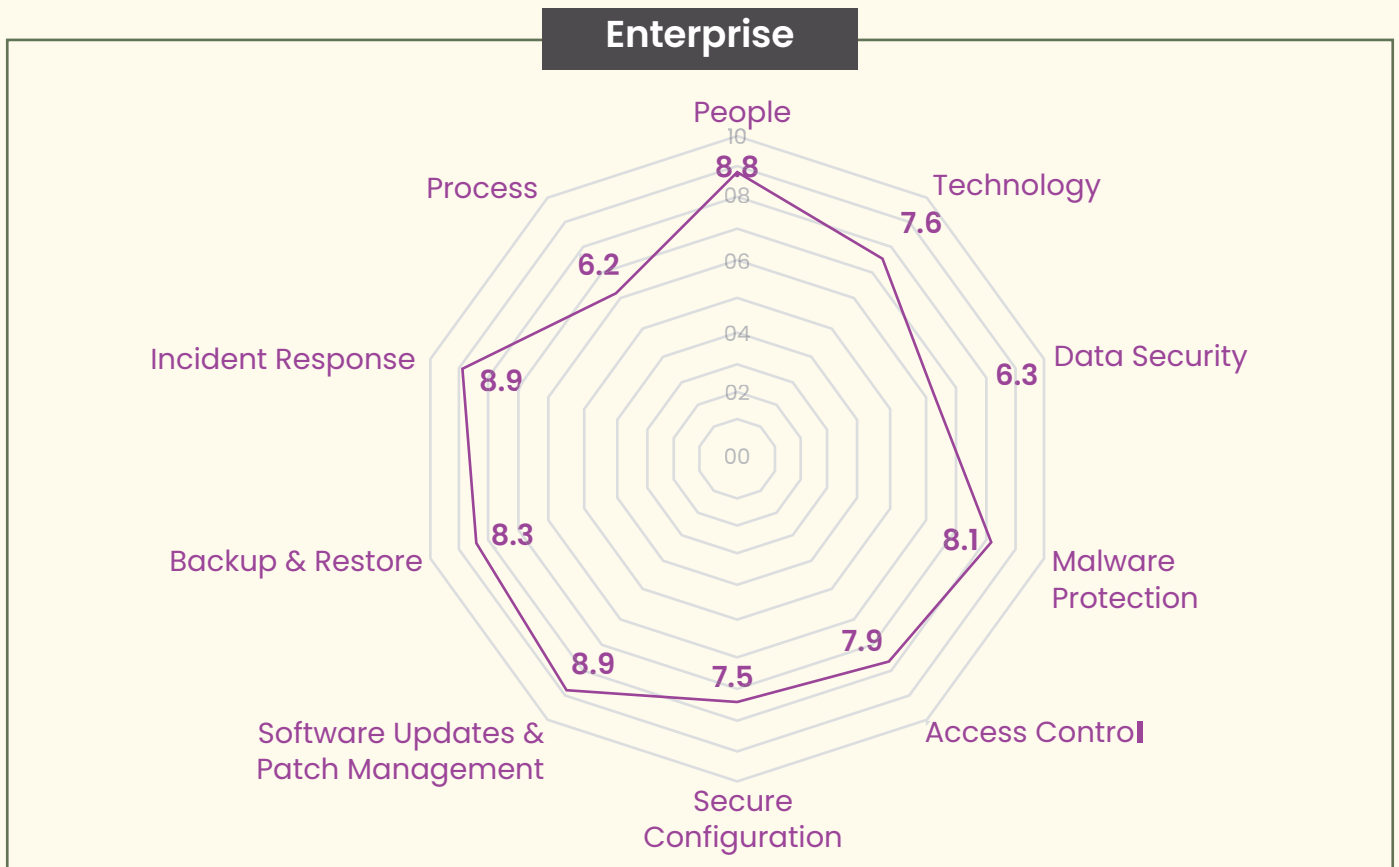
Each axis corresponds to a specific cybersecurity domain, such as People, Process, Technology, Data Security, Malware Protection, and others.

- ▲ **Scores range from 0 to 10:** The scale on each axis runs from the center (0) to the outer edge (10), with higher values indicating greater maturity in that domain.
- ▲ **Purple line denotes current maturity:** The purple line represents the maturity level achieved by enterprises in each domain. The closer the line is to the outer edge, the stronger the performance in that area.
- ▲ **Comparative analysis:** Variations in the purple line across domains highlight strengths and weaknesses. For instance:
  - Peaks in the radar indicate areas of strong performance
  - Dips suggest areas needing improvement

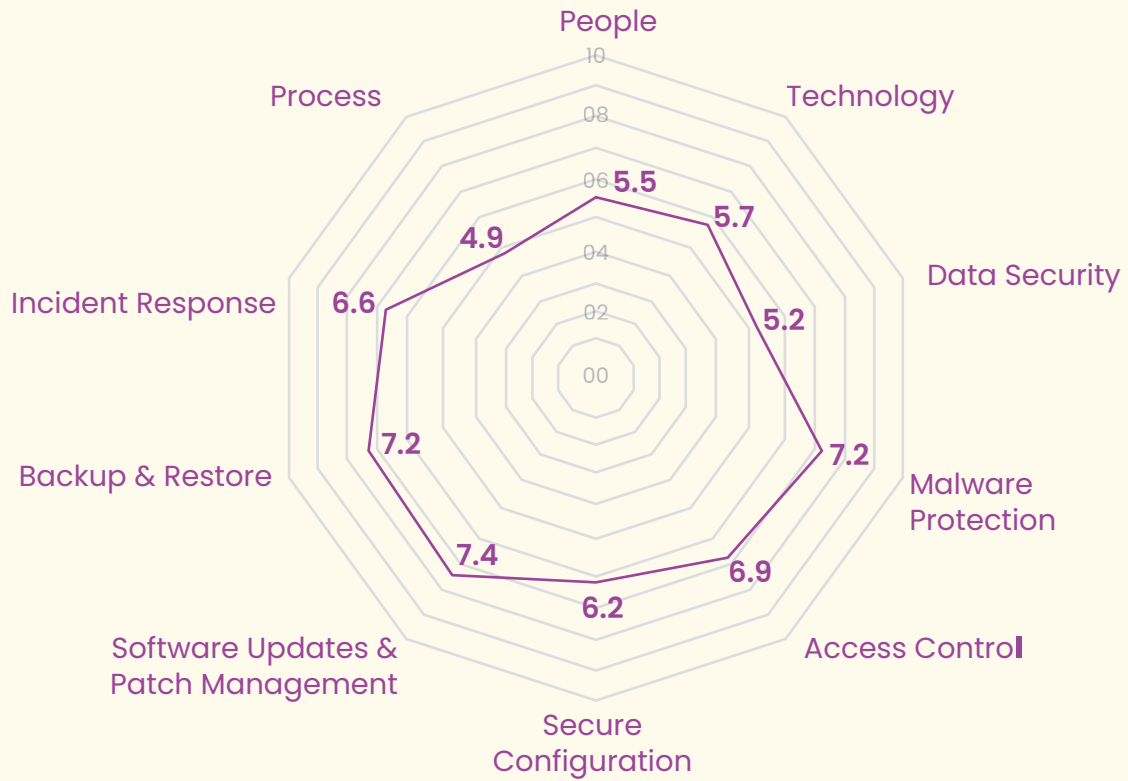


The overall shape of the purple line provides a quick snapshot of the cybersecurity profile for enterprises, showing balanced areas and gaps that require attention.

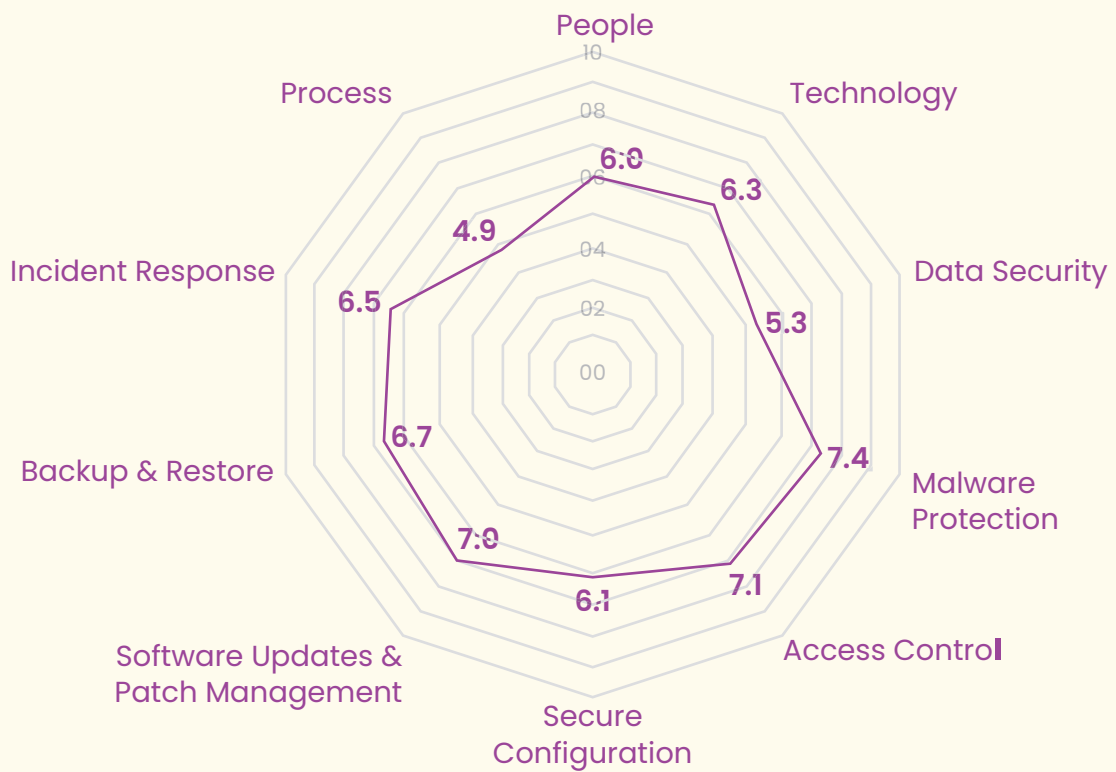
By examining this radar map, enterprises can prioritize their cybersecurity investments to address weaknesses and sustain strengths for a well-rounded security posture.



## Micro



## SMB



# Evaluation Parameters

---

In the context of this survey and analysis, the following cybersecurity components are evaluated based on specific key parameters. Each section outlines the essential aspects that contribute to a robust cybersecurity posture within an organization.

**Cyber Hygiene** is evaluated based on key parameters, including the establishment of employees as the first line of defense, investment in a strong cybersecurity culture through training and awareness programs, and the implementation of robust security processes, practices, and guidelines to govern daily operations effectively.

**Securing Assets** is evaluated based on key parameters, including the identification and protection of all hardware and software assets, maintaining an accurate Configuration Management Database (CMDB), ensuring diligent data handling and secure disposal of assets, eliminating End of Life (EOL)/End of Support (EOS) systems from the network, and implementing mechanisms to safeguard assets from unauthorized access and threats.

**Data Security** is evaluated based on key parameters, including the identification and protection of sensitive and business-critical data, implementation of processes such as password protection and data encryption, and measures to prevent the unauthorized leakage of confidential or sensitive information, ensuring the confidentiality, integrity, and availability of organizational data.

**Malware Protection** is evaluated based on key parameters, including the deployment of antivirus (AV) solutions to safeguard systems and devices, regular execution of virus and malware scans, configuration and management of firewalls to control network traffic, automatic scanning of accessed files from various sources, and ensuring that employees utilize only authorized software from trusted sources to minimize malware risks.

**Access Control** is evaluated based on key parameters, including the establishment of measures to restrict access to data and services, defined workflows for provisioning and revoking access, adherence to best practices for credential management and password policies, approval processes for access rights, role-based access limitations, requirements for third parties to sign non-disclosure agreements (NDAs), restricted use of administrator accounts, and comprehensive management of all user, administrator, third-party, and service accounts inventories.

**Secure Configuration** is evaluated based on key parameters, including the avoidance or upgrading of default, weak, or insecure configurations, disabling or removing unused features, services, or applications, disabling vulnerable features such as auto-connect to open networks and auto-run of non-essential programs, enforcing security configurations based on industry standards and recommendations (e.g., CIS benchmarks), and adherence to industry best practices to minimize security risks and vulnerabilities across all hardware and software assets.

## **Software Updates & Patch Management**

is evaluated based on key parameters, including the prioritization of patch deployment regardless of severity, comprehensive focus on deploying all relevant updates (not just critical and important ones), and the establishment of a defined and structured process for managing software updates and patches to mitigate vulnerabilities, enhance system performance, and protect against emerging threats effectively.

## **Data Backup and Recovery**

is evaluated based on key parameters, including the implementation of reliable backup processes for essential data, protection of backups from unauthorized access, storage of backups offline and separately from the primary operating environment, and regular identification and backing up of business-critical systems and essential business information, including data stored in cloud environments. This ensures data availability and integrity in the event of data loss, corruption, or cyber incidents, facilitating swift recovery and continuity of operations.

## **Incident Response**

is evaluated based on key parameters, including the establishment of an incident response management system, defined processes for managing cybersecurity incidents, employee awareness of incident reporting protocols, and the presence of actionable plans to detect, respond to, and recover from security breaches or cyberattacks. The goal is to minimize incident impacts and restore normal operations swiftly.

## **Security Process Management**

is evaluated based on key parameters, including the regular testing and updating of security processes to assess their effectiveness, periodic revisitation and evaluation of cybersecurity procedures after their initial development or deployment, and continuous assessment of the effectiveness of cybersecurity processes to identify weaknesses and implement improvements. This ensures the organization maintains a resilient and adaptive security posture that can respond to evolving threats and changing organizational needs.





# CYBER THREAT PREDICTIONS



# Validating 2024 Predictions

Cybersecurity experts and organizations continue to grapple with emerging threats that were predicted in the last edition of the India Cyber Threat Report 2023. With an accuracy rate of **75%**, the predictions have proven to be a reliable indicator of evolving cybersecurity risks. In the last edition, **8 critical threats and 4 new threat** categories were identified which have been now validated in the current year. These threats are reshaping how organizations approach risk management, requiring rapid adaptation to protect sensitive data, infrastructure, and operations from growing cyber risks.

The threats identified span across various sectors, from **AI-powered cyberattacks and election-related threats to infrastructure exploitation and deepfake frauds.**

## AI-Powered Threats

---

**Severity:** CRITICAL

**Prediction Validation:** The emergence of polymorphic malware like BlackMamba has underscored the potential threats posed by AI-powered cyber-attacks.

**Key Developments:**

- BlackMamba keylogger utilizing AI for evasion.
- Integration with OpenAI for payload generation.
- Android OS infiltration capabilities.
- Automated attack process advancement.

**Industries Impacted:** BFSI, Healthcare, IT/ITeS, Government.

## Infrastructure Exploitation

---

**Severity:** HIGH

**Prediction Validation:** Recent security breaches have underscored the considerable risk posed by 'living off the land' binaries.

**Key Developments:**

- PowerShell exploitation.
- CertUtil abuse.
- Kernel privilege escalation.
- DarkGate malware emergence.

**Industries Impacted:** BFSI, Healthcare, IT/ITeS, Government.



## Election Related Threats

---

**Severity:** CRITICAL

**Prediction Validation:** With the Indian elections scheduled for May 2024, there is an anticipated increase in cyber threats.

**Key Developments:**

- Election-themed phishing campaigns.
- Targeted malvertising.
- Campaign-related social engineering.
- Influence operations.

**Industries Impacted:** Government, Media, IT/ITeS, Telecommunications.

## MFA Fatigue Attacks

---

**Severity:** HIGH

**Prediction Validation:** MFA fatigue attacks have emerged as a significant threat in cybersecurity landscape.

**Key Developments:**

- Increased MFA bombing incidents.
- Push notification exploitation.
- Social engineering integration.
- Ransomware deployment tactics.

**Industries Impacted:** BFSI, Public and Strategic Enterprises, Cloud Services, Critical Infrastruc-

## Deepfake Exploitation

---

**Severity:** CRITICAL

**Prediction Validation:** AI-generated voice and video scams emerge as significant threats.

**Key Developments:**

- Advanced voice imitation.
- Video manipulation techniques.
- Social engineering integration.
- Targeted executive fraud.

**Industry Impacted:** BFSI, IT/ITeS, Social Media, Public Sector.

# Cyberstorm 2025

## Predicting the Next Wave of Threats

### AI & Advanced Threats

- AI-Powered Adaptive Malware
- Deepfake-Enabled Attacks
- Enhanced Social Engineering
- Data Poisoning Attacks

### Infrastructure Threats

- Critical Infrastructure Attacks
- Cloud & API Vulnerabilities
- Supply Chain Compromises
- IoT & Edge Device Exploitation

### Financial & Identity Threats

- Fake Government Apps
- Investment Platform Fraud
- Cryptojacking Attacks
- Identity Theft Campaigns

### Ransomware Evolution

- Double-Extortion Tactics
- Physical Infrastructure Targeting
- OT/IoT System Exploitation
- Supply Chain Ransomware

### Mobile & Device Threats

- Advanced Mobile Malware
- Cloud-Controlled Android Threats
- Biometric Data Exploitation
- AR System Attacks

### Emerging Tech Vulnerabilities

- Zero-Day Exploits
- Quantum Computing Threats
- Advanced AI System Attacks
- AR/VR Platform Vulnerabilities

**As India continues its rapid digital transformation, cybersecurity threats are evolving in complexity and scope. Drawing insights from emerging trends, we present the following malware threat predictions for India in 2025**

### **Ransomware Evolution: Complex Extortion and Physical Sabotage**

Ransomware attacks will advance beyond simple encryption, incorporating double-extortion tactics that involve data theft and threats to release sensitive information. Additionally, ransomware may target critical infrastructure sectors like energy, healthcare, and transportation, leveraging vulnerabilities in operational technology (OT) and Industrial IoT (IIoT) to cause physical disruptions and sabotage.

### **Cloud & API Vulnerabilities: Expanding Attack Surfaces**

The widespread adoption of cloud services will lead to an increase in vulnerabilities, particularly through misconfigured cloud environments and insecure APIs. Cybercriminals will exploit these weaknesses to access sensitive data and disrupt services, especially targeting industries such as finance, IoT, and SaaS where API security is often insufficient.

### **Supply Chain Attacks: Amplified Cybersecurity Risks**

India's integration into global supply chains will make it a prime target for supply chain attacks. Cybercriminals will exploit trusted vendors and open-source vulnerabilities to inject malicious code, similar to the SolarWinds incident. The reliance on third-party services will heighten the risk, necessitating enhanced supply chain security measures.

### **IoT & Edge Device Exploitation: The Next Botnet Frontier**

The proliferation of IoT devices will provide new opportunities for cybercriminals to create large-scale botnets. Poorly secured IoT and edge devices will be exploited to launch Distributed Denial-of-Service (DDoS) attacks, disrupting critical services in sectors like manufacturing and healthcare that rely on edge computing.

### **AI-Driven Attacks: Enhanced Social Engineering & Data Poisoning**

Artificial Intelligence (AI) will be used to develop highly sophisticated phishing campaigns utilizing deepfake technology and personalized attack vectors, making them harder to detect. AI-driven malware will adapt in real-time to evade traditional security measures, while data poisoning attacks will compromise the integrity of critical AI systems in sectors such as healthcare and autonomous transportation.

### **Hactivist Shifts: Migration to Secure Platforms**

In response to stricter data-sharing policies and increased surveillance, hactivist groups in India may move from mainstream social media platforms to more secure, private channels. This shift will require enhanced monitoring and security measures on these platforms to prevent and mitigate cyberactivism-related threats.

### **Targeted Attacks on Critical Infrastructure: Increasing Sophistication**

Critical infrastructure sectors in India, including healthcare, finance, and energy, will remain prime targets for cybercriminals. These attacks will aim to disrupt services, steal sensitive data, and exploit geopolitical tensions, emphasizing the need for robust security frameworks and continuous monitoring to protect essential services.

### **Convergence of AI-Driven TTPs and Supply Chain Attack Vectors**

The combination of AI capabilities with supply chain vulnerabilities will give rise to a new breed of cyber threats. Attackers will use AI-driven tactics to orchestrate complex attacks while exploiting compromised development resources and hardware manufacturing processes, enabling the insertion of malicious code through corrupted libraries and embedded hardware.

### **AR Malware: Emerging Threats in Augmented Reality**

As Augmented Reality (AR) technology becomes more prevalent, malware targeting AR systems will emerge as a significant security challenge. Cybercriminals may develop fake AR applications to steal user credentials, manipulate AR content, and expose sensitive data, necessitating robust security measures to protect AR-integrated systems.

### **AI-Powered Adaptive Malware: Real-Time Evasion Tactics**

AI-powered malware will continuously evolve by adapting its attack strategies based on user behavior and system vulnerabilities. This dynamic nature will make detection and prevention more challenging for traditional security systems, requiring advanced, adaptive security solutions to counter real-time threats.

### **Cloud-Controlled Malware on Android: Evading Detection**

Malware leveraging cloud infrastructure will increasingly target Android devices. By offloading processing tasks to the cloud, these threats can bypass traditional detection mechanisms, making it difficult for security teams to identify and neutralize them. Enhanced cloud security and mobile threat detection solutions will be essential to combat this evolving menace.

### **Emerging Financial Application Threats: Government and Investment Platform Exploitation**

The convergence of fake government service applications and fraudulent investment platforms will create hybrid threats in 2025. Cybercriminals will deploy sophisticated apps that impersonate government benefits systems and investment platforms, using social engineering, influencer marketing, and advanced malware to execute large-scale financial fraud and identity theft, targeting both public welfare recipients and retail investors.

### **Deepfake-Enabled Malware: Enhanced Deception Techniques**

Deepfake technology will be utilized to create highly convincing malicious content, including fake video or audio messages from trusted sources. This will facilitate more effective social engineering attacks, making it easier for cybercriminals to deceive users into executing malware or revealing sensitive information.

### **Zero-Day Exploits in Emerging Technologies**

As new technologies such as quantum computing and advanced AI systems are adopted, zero-day vulnerabilities specific to these technologies will be exploited by cybercriminals. These exploits will target the underlying software and hardware, leading to significant breaches and data compromises before patches can be developed and deployed.

### **Mobile Malware Sophistication: Beyond Traditional Threats**

Mobile devices will continue to be a major target, with malware becoming more sophisticated in evading detection and exploiting mobile-specific vulnerabilities. Advanced mobile malware will integrate seamlessly with legitimate applications, making it harder for users and security solutions to identify malicious activities.

### **Cryptojacking and Resource Exploitation Attacks**

The rise of cryptocurrency mining will lead to an increase in cryptojacking attacks, where malware hijacks computing resources to mine cryptocurrencies without the user's knowledge. This will result in degraded system performance, increased energy consumption, and potential hardware damage.

### **Biometric Data Exploitation: Targeting Authentication Systems**

As biometric authentication becomes more widespread, cybercriminals will target biometric data stores and authentication systems. Malware designed to steal or manipulate biometric data will pose significant risks to personal and organizational security, undermining trust in biometric authentication methods.

### **Insider Threats Enhanced by Malware**

Malware will increasingly be used to facilitate insider threats, allowing malicious insiders to exfiltrate data, disrupt systems, or manipulate information without detection. This will be exacerbated by the use of advanced malware that can hide its presence and activities within legitimate network traffic.


### **AI-Driven Offensive Capabilities: Enhanced Attack Automation**

Cybercriminals will increasingly leverage AI to automate and enhance their attack strategies. This includes the use of machine learning algorithms to identify vulnerabilities, optimize phishing campaigns, and develop more sophisticated malware that can adapt to and evade security measures in real-time. The automation of these offensive capabilities will enable attackers to launch more frequent and effective assaults with reduced effort and resources.

### **Cyber Warfare & Geopolitical Tensions**

The geopolitical cyber threat landscape in 2025 will be shaped by escalating state-sponsored activities, regional conflict spillovers, and critical infrastructure targeting. Organizations face increased risks from trade-based cyber attacks, digital sovereignty disputes, and sophisticated information warfare campaigns. Advanced persistent threats, quantum computing exploitation, and AI-driven attacks will become prominent tools in cyber warfare.





# RECOMMENDATIONS 2025 & BEYOND

# Future Directions and Strategic Recommendations: 2025 and Beyond

The evolving threat landscape of 2025 demands a fundamental shift in how CISOs approach cybersecurity. Traditional security models are becoming obsolete against quantum-enabled threats, AI-powered attacks, and state-sponsored operations. This section provides strategic direction for security leaders.

## Embrace Artificial Intelligence (AI) and Machine Learning (ML) for Threat Detection and Response

AI and ML will continue to play an essential role in threat detection and incident response. The increasing complexity of cyber threats—such as zero-day exploits, polymorphic malware, and advanced persistent threats (APTs)—requires the automation and speed that AI-driven systems provide. CISOs should, therefore, prioritize the following:

- ▲ **Adopt AI-enhanced security operations:** Implement AI-powered Security Information and Event Management (SIEM) systems, which can analyze massive datasets in real time to identify anomalous patterns and potential threats faster than traditional methods.
- ▲ **Leverage ML for predictive threat intelligence:** Use machine learning models to predict emerging attack vectors and behaviors, providing actionable insights that enable early defense and mitigation.
- ▲ **Automate incident response:** Integrate AI with automated incident response tools to quickly contain breaches, limit damage, and reduce the time to recovery.

## Adopt a Zero Trust Security Framework

Zero Trust has emerged as a critical paradigm when traditional perimeter-based security models are becoming ineffective in a world of remote work and cloud adoption. In a Zero Trust model, trust is never assumed, and every access request is authenticated and authorized based on least privilege principles. Hence focus should be rendered on the following:

- ▲ **Continuous authentication:** Implement multi-factor authentication (MFA) and identity verification technologies that validate users' identities and device security at all points of access.
- ▲ **Micro-Segmentation:** Break down internal networks into smaller, isolated segments to prevent lateral movement by attackers even if one part of the network is compromised.
- ▲ **Data-centric security:** Protect sensitive data with encryption and access controls, to ensure that unauthorized users cannot access critical systems or data even if they breach the network perimeter.



## Prepare for Cloud-Native Security Challenges

CISOs must also account for the security challenges specific to cloud-native architectures as organizations increasingly migrate to cloud environments. The cloud might offer flexibility and scalability, but it also introduces new risks, such as misconfigured cloud settings, insecure APIs, and inadequate cloud provider security measures. Suggested recommendations for CISOs would be:

- ▲ **Secure cloud configurations:** Implement automated tools that continuously monitor cloud environments for misconfigurations and vulnerabilities, ensuring compliance with security best practices and regulatory requirements.
- ▲ **Cloud security posture management (CSPM):** Adopt CSPM solutions to assess and manage risks across cloud infrastructure, applications, and services.
- ▲ **Multi-Cloud and hybrid cloud security:** Ensure a cohesive security strategy across multiple cloud providers and on-premises environments, focusing on secure interconnectivity, identity management, and encryption.

## Focus on Cyber Resilience, Not Just Prevention

The increasing frequency and sophistication of cyberattacks hint that prevention alone is no longer sufficient. CISOs must ensure that their organizations are resilient enough to recover quickly from cyber incidents. This requires a holistic approach to cybersecurity and business continuity planning. Key actions include:

- ▲ **Incident response and recovery planning:** Regularly update and test incident response (IR) and business continuity plans (BCPs). Ensure that teams are well-drilled in responding to ransomware, data breaches, and other high-impact incidents.
- ▲ **Implement backup and restore procedures:** Maintain offsite, encrypted backups and regularly test data recovery capabilities to minimize downtime during an attack.
- ▲ **Post-Breach analysis and continuous improvement:** After an incident, conduct thorough post-mortem analysis to identify vulnerabilities and improve defensive measures for the future.

## Invest in Threat Intelligence and Collaboration

CISOs should prioritize threat intelligence-sharing and collaboration with industry peers, government agencies, and law enforcement to stay ahead of emerging threats. By joining threat intelligence forums, CISOs can gain valuable insights into emerging threats and best practices for defense.

- ▲ **Leverage threat intelligence platforms (TIPs):** Integrate TIPs into the security infrastructure to automatically gather, correlate, and act on external threat intelligence in real-time.
- ▲ **Collaborate with industry peers:** Establish relationships with other CISOs within the same industry to share insights and best practices related to emerging threats.
- ▲ **Engage with law enforcement:** Build strong relationships with local and international law enforcement to ensure rapid response in the event of significant incidents like ransomware attacks or data breaches.

# Expert Quotes



The complete threat perception has shifted dramatically, with an increasing variety of sophisticated attacks targeting even secured systems. Malware continues to evolve, forcing organizations to enhance their security posture to address these emerging threats effectively.

**Asit Kumar**  
CISO, Digi Yatra Foundation



Over the past 18-24 months, cyber threats in our industry have evolved significantly. While ransomware, phishing, and social engineering remain the primary threats, they have become much more sophisticated thanks to the use of Artificial Intelligence. AI-driven attacks are now more targeted and harder to detect, rendering traditional training ineffective. To address these challenges, it is vital to implement AI-based threat mitigation tools for real-time detection and alerts. It is also crucial to revamp our training programs to better equip our staff and stakeholders against these advanced threats. This proactive approach ensures we maintain a robust security posture in an increasingly complex threat landscape.

**Patrick Jasper**  
General Manager, NABARD



Cyber attack patterns against the BFSI sector have evolved significantly in recent years. We are now witnessing advanced persistent threats (APTs) targeting core banking systems, supply chain attacks designed to exponentially increase the impact of breaches, ransomware-as-a-service models, the utilization of AI-based tools, and hybrid DDoS attacks, among others. Cyber threat vectors have become extremely diverse and are constantly evolving. In the recent past, we have seen a notable increase in phishing, malware, cloud vulnerabilities, mobility-related threats, and supply chain compromises. To effectively address these changing attack patterns, our organization is continuously realigning our security strategies and defenses to the evolving cyber threat landscape.

**Makesh Chandramohan**  
Group CISO, Aditya Birla Capital Ltd



Over the past couple of years, our organization, as part of the critical information infrastructure, has experienced a significant rise in sophisticated cyber-attacks. We've seen an increase in email spear-phishing, attacks on official social media handles and websites, impersonation of senior leadership on WhatsApp, and malicious SMS links targeting our employees. Additionally, web shell exploits, advanced network scanning, more frequent and complex DDoS attacks, and ransomware delivered through compromised downloads and weaponized email attachments have become prevalent. To address these evolving threats it is important to prioritize continuous employee education, strengthen 24x7 Security Operations Center, implement robust security controls for internet-facing servers, deploy advanced DDoS mitigation solutions, and enhance our defenses against phishing and malicious emails with anti-spam gateways and sandboxing technologies. This comprehensive strategy ensures we stay ahead of cybercriminals and maintain the security of our critical infrastructure.

**Susheel Kumar**  
Chief General Manager (Business Information System), GAIL (INDIA) LIMITED



In today's evolving threat landscape, organizations must adopt strategic measures to strengthen cyber resilience. A comprehensive cybersecurity framework should include Attack Surface Management, Breach Attack Simulation, and Brand Monitoring to enhance both internal operations and vendor security. Beyond traditional Vulnerability Assessment and Penetration Testing, multi-layered defenses like ASM enable continuous vulnerability mitigation. Breach Attack Simulation allows us to test security controls against real-world scenarios, ensuring robust defenses. Effective Brand Monitoring safeguards our reputation by proactively detecting and addressing threats and frauds. Together, ASM, BAS, and Brand Monitoring create a dynamic defense strategy that maintains organizational integrity and builds customer trust in our digital world.

**Madhur Joshi**

Chief Information Security Officer, HDB Financial Services Limited



In the past year, cyber threats have become significantly more sophisticated and targeted. We've observed key trends such as regulatory changes, the evolution of ransomware, zero-day exploits, supply chain attacks, vulnerabilities from remote work, and AI-powered attacks. To address these challenges, it is important to implement enhanced threat intelligence, adopt a Zero Trust Architecture, and conduct regular training and drills.

**Rajesh K Singhal**

CISO, HDFC Securities Ltd



Ransomware in banking has evolved to double and triple extortion and RaaS, heightening financial and reputational risks. We mitigate these threats with patch management, network segmentation, endpoint detection, backups, and staff training. To enhance resilience, we've onboarded Breach & Attack Simulation, upgraded to a Next-Gen SOC with SOAR and UEBA, conducted comprehensive security assessments, and are exploring AI. Additionally, we are leveraging Quantum Computing and Generative AI to strengthen our security posture.

**Ramesh Babu**

CISO, Canara Bank



In the manufacturing sector, cyber threats are rapidly evolving, targeting operational technology and industrial control systems through IoT vulnerabilities and Industry 4.0 technologies. Supply chain attacks are on the rise, necessitating robust cybersecurity measures to protect critical infrastructure. To strengthen our resilience, we implement multi-layered security strategies guided by frameworks like NIST, adopt zero-trust architecture, conduct regular assessments, and provide comprehensive employee training. Emerging trends such as AI and enhanced supply chain security are reshaping our priorities, ensuring we maintain a strong cybersecurity posture.

**Dr. Yusuf Hashmi**

Group CISO, Jubilant Bhartia Group



Cyber threats have become increasingly sophisticated, including targeted ransomware, Malware-as-a-Service, state-sponsored APTs, AI-powered polymorphic malware, mobile malware, supply chain attacks, and social engineering tactics. Additionally, generative AI introduces complex intent vector threats like automated disinformation and autonomous malicious code generation. To combat these, our organization leverages AI-driven anomaly detection, real-time threat intelligence, and a Zero Trust Architecture. Leveraging advanced endpoint detection solutions and conducting regular threat-hunting and red-team drills becomes non-negotiable. A comprehensive approach, encompassing People, Policies, and Processes, ensures robust protection.

**Wg Cdr S Sudhakaran (Retd)**

MD & CEO, QuGates Technologies Pvt Ltd



The view on "Never Trust and Always Verify" with Zero Trust solutions continue to gain traction as VPN solutions for remote connectivity became highly vulnerable. Secondly, while AI governance will become reality after Data Privacy rules, the adoption of AI agent with right guardrails will become a necessity to handle skills shortage. With many security tools and related skills shortage, a single pane view or platform based solutions are becoming a new normal so that "Job To be Done" for various security personas is rightfully visible.

**Dr. Lalit Mohan Sanagavarapu**  
Chief Product Officer, Quick Heal



According to the World Economic Forum's 2024 report, Cybersecurity has emerged as the 4th most pressing global risk. The report also highlights that Infectious Diseases and Chronic Health Conditions rank 23rd and 27th respectively. Cyber risks threaten the very systems that enable life-saving breakthroughs. The Pharma Industry bears the critical responsibility of protecting humanity from the devastating impact of infectious and chronic diseases alongside safeguarding themselves against the escalating risk related to cyber-attacks.

Addressing the Cyber risk demands faster response to threats and vulnerabilities. There is need for continuously fortifying our defences to ensure both short-term agility and long-term resiliency.

**Vivek Gupta**  
Vice President, Chief Information Security Office



The cyber threat landscape continues to evolve rapidly, posing significant risks to individuals, organizations, and critical infrastructure. This report provides a comprehensive overview of the current threat landscape, highlighting key trends, emerging threats, and strategic recommendations to mitigate potential risks. The insights on this report provides an overview of the threats we have observed in India and different sectors within the country. The rise in malware infections and the time taken to resolve calls for a wakeup call. Other threats like Ransomware poses serious risks to the organization and has been one of the top threats that the organization should be worried. While the commodity malware and threats are significant, targeted and advanced threats, with evasion techniques and AI capabilities makes it complex for the defensive controls to detect and quarantine. The cyber threat landscape is constantly evolving, and organizations must remain vigilant to protect themselves from emerging threats. Therefore, it is very important for the enterprises to strengthen their detection capabilities, incident response and focus on cyber resiliency. By adopting a proactive approach to cybersecurity, organizations can mitigate risks and safeguard their critical assets.

**Sangamesh S**  
VP and Head of Seqrite Labs and MDR



At Seqrite Labs, we have witnessed innovative mechanisms employed by threat actors to infiltrate their targets and our technologies and protection layers have evolved to stay a step ahead of the nefarious designs of these threats. This is critically important in light of the potent risks posed by exploitation of weaknesses in system applications, utilities and processes. In addition to mitigating the risks posed by evolving malwares and the interesting mechanisms they employ. One of the prominent highlights of the year was the impact due to geo-political conflicts across the seas, the offshoots of which were evident in dark web and in actuation of the attacks on Indian cyber assets. Seqrite Labs has been at forefront to proactively identify the malicious entities and neutralize them in their tracks.

**Jaswinder Singh**  
Director Engineering, Seqrite Labs



# Acknowledgement

## Authors

Neha Mishra, Associate Consultant, Strategy and Insights, DSCI  
Jaswinder Singh, Director, Engineering, Seqrite Labs

## Contributors

Prasad Deore, Senior Director, DSCI  
Sangamesh S, Vice President & Head of Seqrite Labs

## Editors

Amit K. Ghosh, Sr. Manager, Communications, DSCI  
Charu Sharma, Manager, Marketing & Communications, DSCI

## Design by

Buffalo Soldiers Digital



## About DSCI

Data Security Council of India (DSCI) is a not-for-profit, industry body on data protection in India, setup by nasscom®, committed towards making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cyber security and privacy. DSCI works together with the Government and their agencies, law enforcement agencies, industry sectors including IT-BPM, BFSI, CII, Telecom, industry associations, data protection authorities and think tanks for public advocacy, thought leadership, capacity building and outreach initiatives.

For more information, visit: [www.dsci.in](http://www.dsci.in)

## About Seqrite

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 Mobility Management, Zero Trust Network Access, and many more. Seqrite Data Privacy management solution enables organizations to stay fully compliant with the DPDP Act and global regulations. Today, 30,000+ enterprises in more than 70+ countries trust Seqrite with their cybersecurity needs.

For more information, please visit: <https://www.seqrite.com/>

### DATA SECURITY COUNCIL OF INDIA

Nasscom Campus, 4th Floor, Plot No. 7-10,  
Sector 126, Noida, Uttar Pradesh - 201303

For any queries, contact: E: [info@dsci.in](mailto:info@dsci.in) | W: [www.dsci.in](http://www.dsci.in)

X /DSCI.Connect    f dsci.connect    @ dsci.connect  
v dscivideo    data-security-council-of-india



### QUICK HEAL TECHNOLOGIES LIMITED

Solitaire Business Hub, Office No. 7010 C & D, 7th Floor,  
Viman Nagar, Pune - 411014

For any queries, contact: E: [info@seqrite.com](mailto:info@seqrite.com) | W: [www.seqrite.com](http://www.seqrite.com)

X /Seqrite    f /seqrite  
v /@seqrite385    /company/seqrite