

SECURITE



**KARNATAKA  
CYBER THREAT  
REPORT**

# Foreword – Quick Heal

---

I present to you the Karnataka Cyber Threat Report 2025 with great pride and a deep sense of responsibility.

This year, we have drawn on invaluable insights from Seqrite Labs, our state-of-the-art malware analysis facility in Bangalore, to provide a comprehensive and in-depth analysis of Karnataka's evolving cyber threat landscape. Our findings are based on extensive telemetry data gathered from numerous endpoints, giving us a unique view into the security challenges facing businesses and individuals in the state.

The Karnataka Cyber Threat Report 2025 delves into emerging trends, sector-specific vulnerabilities, and the growing threat posed by ransomware and other forms of malware. As a key hub for IT companies, startups, and digital enterprises, Karnataka faces a concentrated cyber risk, with a rising number of attacks targeting these sectors. The report has uncovered key findings that show Karnataka's cybersecurity landscape faced an unprecedented barrage of attacks, with 11.46 million malware detections—averaging around 31,388 incidents each day—and 1.78 million ransomware attacks, translating to nearly 4,887 ransomware events every day, especially in Bangalore, where attack volumes are considerably higher than in other cities.

This report also offers actionable intelligence and strategic recommendations designed to help organizations in the state stay one step ahead of malicious actors.

In line with our commitment to innovate, simplify, and secure, Seqrite has continuously advanced its solutions to help cybersecurity professionals stay ahead of emerging threats. Our Seqrite Malware Analysis Platform (SMAP) provides static, dynamic, and manual analysis, offering deep insights into suspicious files and URLs that may evade traditional detection methods. This enables faster, more informed decision-making and helps mitigate Zero-Day attacks before they cause harm.

Additionally, we are excited to introduce Seqrite Threat Intel – a robust threat intelligence platform that offers real-time insights for proactive defense and operational efficiency and supports informed decision-making, all while ensuring regulatory compliance.

As we continue to navigate the rapidly changing digital landscape, Seqrite remains committed to leading the industry with innovative solutions, rigorous research, and an unwavering dedication to securing Karnataka's digital future. Through continued innovation and collaboration, we will help build a safer, more resilient digital ecosystem for businesses and individuals in Karnataka.

2024 has been a milestone year for us, and with the growing cybersecurity challenges faced by Karnataka, our efforts in research, innovation, and actionable intelligence are more important than ever. We are dedicated to equipping businesses and organizations with the tools they need to protect themselves and contribute to a secure and thriving digital ecosystem.



**DR. SANJAY KATKAR**

*Joint Managing Director,  
Quick Heal Technologies Limited*

# From the CEO's Desk

## Quick Heal

---

It is with great pride and a deep sense of responsibility that I present to you the Karnataka Cyber Threat Report 2025. As India's economy continues to thrive, with significant government investments in infrastructure, manufacturing, and services, the digital economy has emerged as a central pillar of growth. Projected to contribute 20% of India's GDP by 2026, it 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 entities, and public sectors with innovative solutions. Along with the India Cyber

Threat Report 2025, we are pleased to present this year's Karnataka Cyber Threat Report 2025. This report, a collaborative effort with Seqrite Labs, India's largest malware analysis facility, provides a detailed analysis of the cybersecurity challenges facing Karnataka, drawing insights from data gathered across a vast array of endpoints.

While we recorded over 369 million detections, averaging 702 detections per minute across India, Karnataka accounted for 9.37% of all incidents reported in India. The state recorded 11.46 million malware detections, averaging approximately 31,388 detections per day and 1.78 million ransomware detections, equating to about 4,887 ransomware attacks daily.

Our findings underscore the growing risk that Karnataka faces in the face of an increasingly sophisticated cyber threat landscape. The state's booming tech sector, coupled with its prominence as a hub for businesses, makes it a key target for cybercriminals. As in the rest of India, Karnataka has experienced a sharp rise in ransomware and malware detections. The report highlights critical vulnerabilities in key industries, including IT, healthcare, and BFSI, all of which are being increasingly targeted by cybercriminals.

Seqrite's dedication to advancing cybersecurity is evident through the innovations we have introduced this year. We have launched the Seqrite Malware Analysis Platform (SMAP), which empowers security professionals with enhanced capabilities to detect and respond to complex threats. Furthermore, we have also introduced Seqrite Threat Intel, that provides real-time insights to help organizations strengthen their defenses and make informed decisions while remaining compliant with regulations.

As the cyber threat landscape evolves, Seqrite remains committed to investing in research, developing cutting-edge solutions, and collaborating with industry leaders to ensure a secure digital future for Karnataka, India, and the world. I would like to extend my heartfelt thanks to our partners, Seqrite Labs, and all those who continue to work tirelessly toward making cybersecurity a priority for businesses and individuals alike.

Through our continued efforts, we are determined to stay ahead of the threats of tomorrow, ensuring that Karnataka's digital ecosystem remains secure and resilient.



**VISHAL SALVI**

Chief Executive Officer,  
Quick Heal Technologies Limited

07

Executive  
Summary

11

Karnataka  
Threat Report  
2025

23

Featured  
Stories  
2025

44

The State of  
Malware in  
India

57

India  
Malware  
Landscape

69

Cyber Threat  
Predictions

TABLE OF  
CONTENTS



# 75

Recommendations  
2025 & Beyond

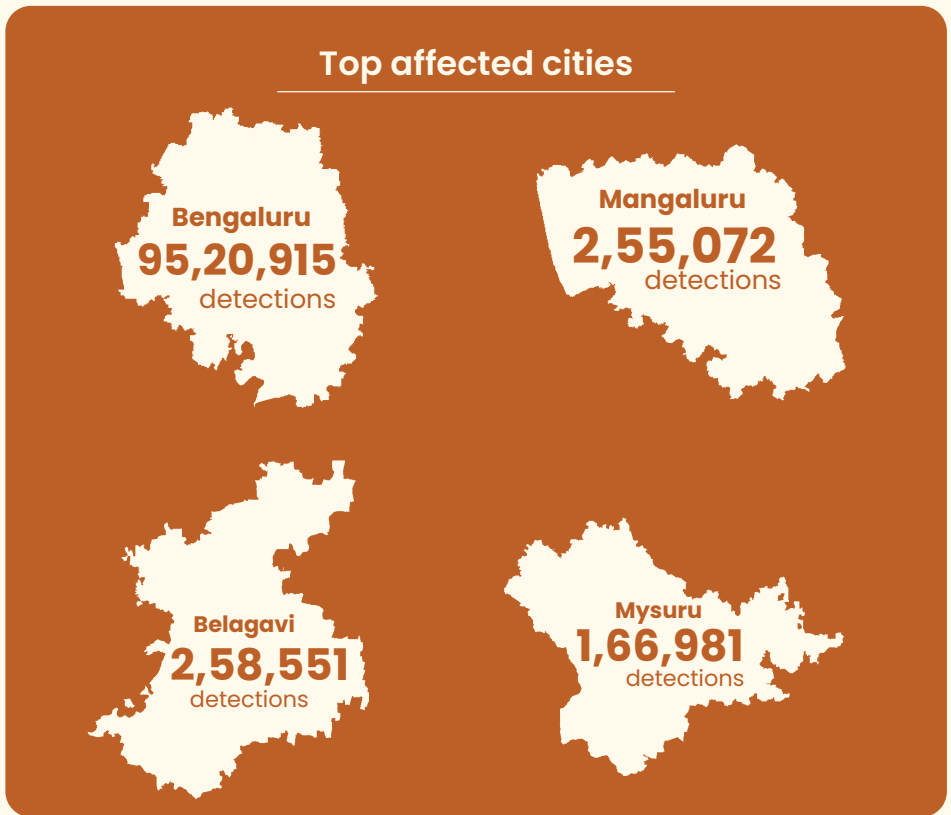
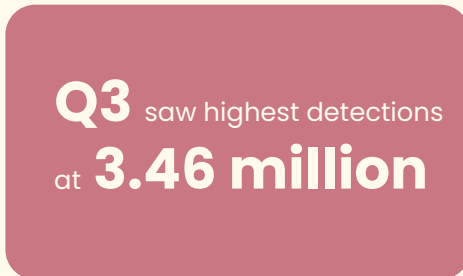
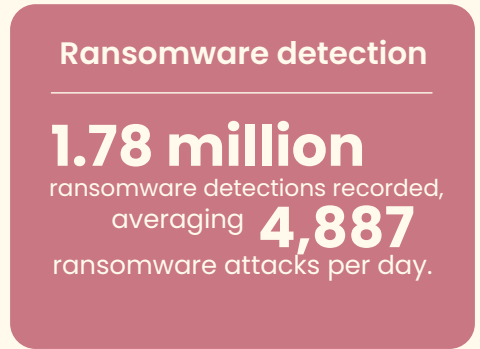
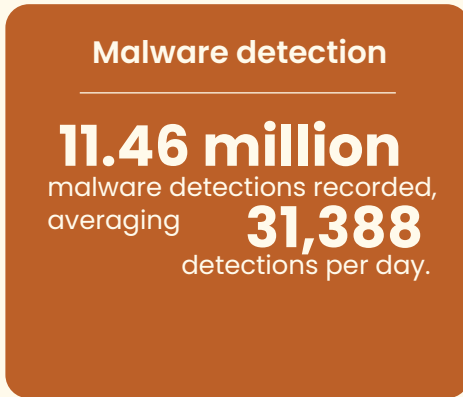




# EXECUTIVE SUMMARY



# Key Highlights





In 2024, Karnataka's cybersecurity landscape faced an unprecedented barrage of attacks, with 11.46 million malware detections—averaging around 31,388 incidents each day—and 1.78 million ransomware attacks, translating to nearly 4,887 ransomware events every day. Although these numbers represent 4.3% of the nation's total malware detections and 9% of its ransomware cases, they paint a clear picture of a region under significant digital siege, especially in Bangalore, where attack volumes are considerably higher than in other cities.

Throughout the year, cyber threats in Karnataka demonstrated distinct seasonal patterns, with a noticeable surge in Q3 followed by a mild dip in Q4. A closer look at industry-specific data reveals that sectors like Professional Services, Government, and Education have borne the brunt of these attacks. For instance, the Education sector recorded exceptionally high numbers for certain malware strains, while Government systems frequently faced aggressive attempts to exploit vulnerabilities. Meanwhile, key industries such as BFSI, Telecom, and Manufacturing also experienced targeted attacks, underscoring that cybercriminals are keenly focused on sectors that manage critical data and resources.

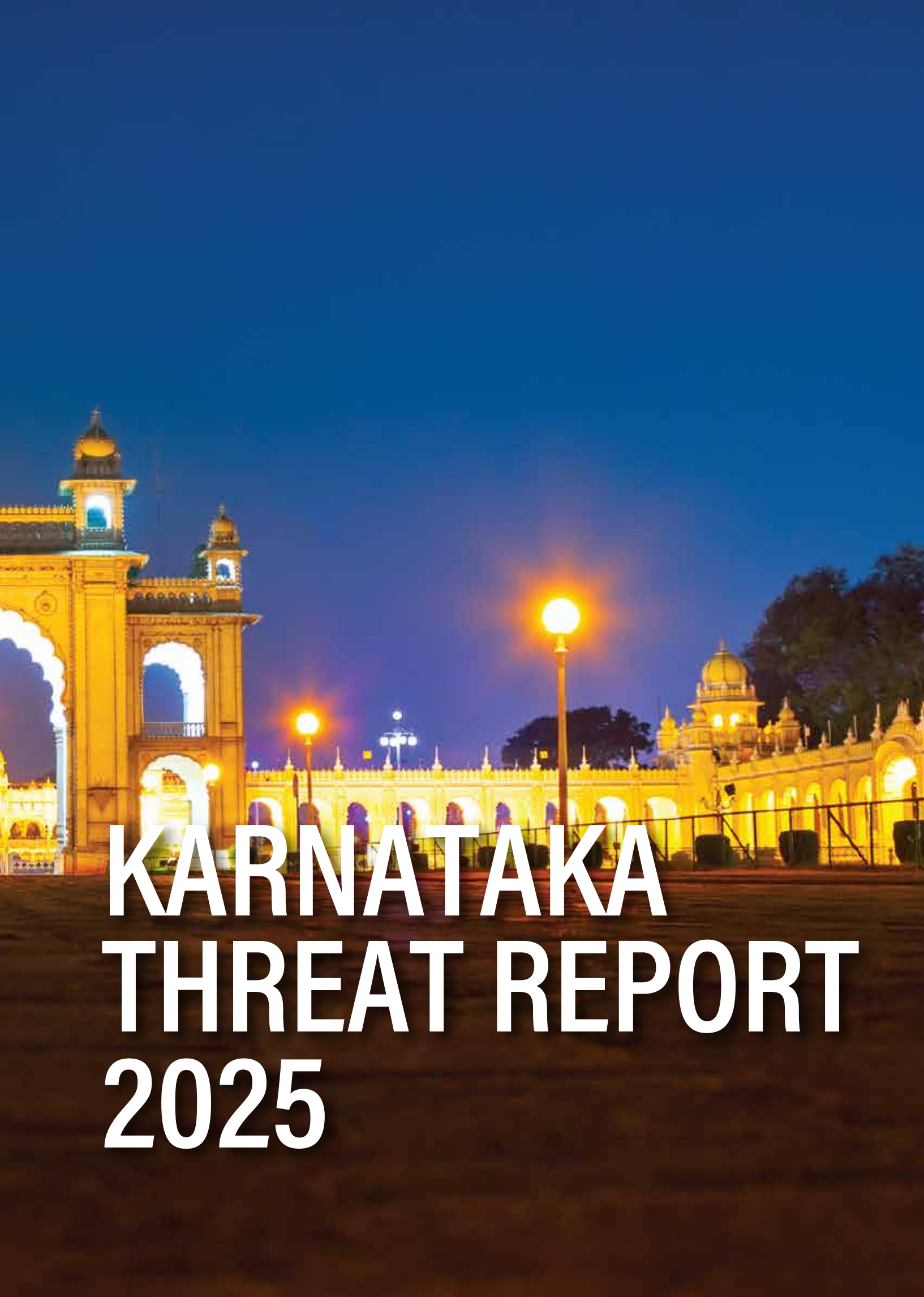
The report further delves into several high-profile case studies that illustrate the diverse tactics employed by threat actors. A notable breach at The telecom company's Karnataka operation exposed sensitive customer data through an exploited API vulnerability. Similarly, the cyberattack on the Indian Institute of Remote Sensing disrupted access to satellite research data, posing potential national security risks. The ransomware attack on India's leading multispecialty hospitals brought healthcare operations to a standstill, forcing a scramble to restore systems and secure patient data. In February 2025, the DDoS assault on a government portal severely disrupted property registrations, resulting in significant revenue losses and shaking public trust in government digital services.

Adding another layer of complexity, hacktivist groups operating on Telegram have launched a series of disruptive attacks against various public and private sector targets—from educational institutions and hospitals to government websites—further highlighting vulnerabilities across the state's digital infrastructure. Prominent threat actors, including groups linked to Lazarus, APT41, and FIN11, are actively targeting critical assets, reinforcing the urgent need for robust, layered security measures.

Government efforts to bolster cybersecurity in Karnataka are making strides through targeted policies and investments, yet the continuous rise in attacks underscores that much more must be done. It is essential for organizations and public bodies to embrace proactive measures, such as regular security audits, enhanced threat intelligence, and comprehensive employee training programs, to build a resilient digital future.

This report not only outlines the significant challenges Karnataka faces but also serves as a call to action for all stakeholders to come together, strengthen their defenses, and foster a culture of cybersecurity awareness. By addressing these vulnerabilities head-on, Karnataka can hope to safeguard its digital transformation and secure its position as a leading technology hub in India.





# KARNATAKA THREAT REPORT 2025

# Karnataka is attracting significant investment across a diverse range of sectors. Here are some key areas where investments are flowing:

## Technology

Karnataka, particularly Bengaluru, remains a major hub for IT, software development, and startups. Investments continue to pour into these areas, driving innovation and growth.



## Manufacturing

The state is witnessing increased investment in manufacturing, especially in sectors like aerospace, defense, automobiles, and electronics.



## Renewable Energy

With a focus on sustainability, Karnataka is attracting substantial investments in renewable energy projects, including solar and wind power.



## Infrastructure

Development of infrastructure, including roads, railways, and airports, is a priority, leading to significant investments in these areas.



## Biotechnology and Pharmaceuticals

Karnataka is a leading state in biotechnology and pharmaceuticals, and these sectors continue to attract investments.



## Tourism

With its rich cultural heritage and natural beauty, Karnataka's tourism sector is also receiving attention from investors.



Overall, Karnataka is a preferred investment destination due to its favorable business environment, skilled workforce, and supportive government policies. The state government is also actively promoting investment through initiatives like the Global Investors Meet and single-window clearance systems.

# Karnataka, being a hub for technology and innovation, faces a wide range of cyber risks and threats.

Here are some of the key concerns:

 <b>Data Breaches</b> <p>With numerous IT companies and government institutions handling sensitive data, data breaches are a significant threat. These breaches can lead to the loss of personal information, financial details, and intellectual property.</p>	 <b>Ransomware Attacks</b> <p>Ransomware attacks, where hackers encrypt critical data and demand a ransom for its release, are on the rise. These attacks can cripple businesses and government services.</p>	 <b>Phishing and Social Engineering</b> <p>Phishing attacks, where individuals are tricked into revealing sensitive information through emails or fake websites, are common. Social engineering tactics are also used to manipulate people into divulging confidential data.</p>
 <b>Distributed Denial of Service (DDoS) Attacks</b> <p>DDoS attacks, where websites or online services are flooded with traffic, disrupting their availability, are a concern. These attacks can target businesses, government portals, and critical infrastructure.</p>	 <b>Malware Attacks</b> <p>Malware, including viruses, worms, and spyware, can infiltrate systems and cause damage or steal data. Mobile malware is also a growing threat, especially in a state with high mobile penetration.</p>	 <b>Cyber Espionage</b> <p>With a strong presence of defense and aerospace industries, Karnataka is vulnerable to cyber espionage attempts aimed at stealing sensitive information.</p>
 <b>Internet of Things (IoT) Vulnerabilities</b> <p>The increasing use of IoT devices creates new vulnerabilities that hackers can exploit to gain access to networks and data.</p>	 <b>Lack of Awareness</b> <p>A lack of awareness about cybersecurity best practices among individuals and organizations can make them more susceptible to attacks.</p>	 <b>Insider Threats</b> <p>Threats from within organizations, whether intentional or accidental, can also lead to data breaches and other security incidents.</p>
 <b>Emerging Technologies</b> <p>New technologies like Artificial Intelligence (AI) and Machine Learning (ML) can also be used by cybercriminals for malicious purposes, creating new challenges for cybersecurity.</p>		

# Malware Detection Statistics 2024

Karnataka recorded **11.46 million** malware detections in 2024, averaging **31,388** detections per day

- ▶ This suggests a significant cybersecurity threat in the region, likely driven by factors such as increased internet penetration, growing digital infrastructure, and targeted cyber campaigns on the state.

Detection Name	Detection Count	Per Day
Malware	11.46 M	31388
Ransomware	1.78 M	4887

**1.78 million** ransomware detections were recorded in Karnataka, averaging **4,887** ransomware attacks per day.

- ▶ Ransomware attacks involve cybercriminals encrypting user data and demanding ransom payments, which indicates targeting of businesses, institutions, and individuals.
- ▶ The high number suggests an active ransomware ecosystem exploiting vulnerabilities.

## Karnataka VS National Detection

Karnataka accounted for **4.3%** of total malware detections in India  
**11.46M** out of **266.67M**

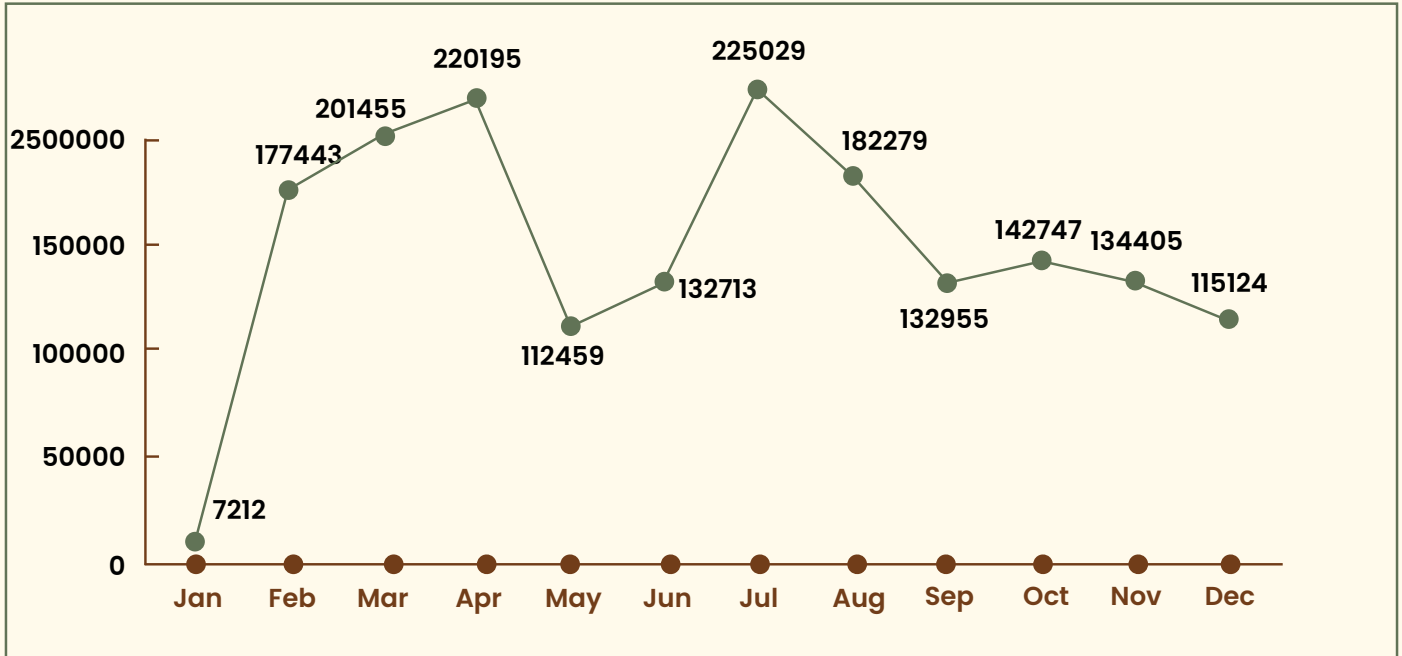
For ransomware, Karnataka contributed **9%** of the national detections  
**1.78M** out of **19.85M**

- ▶ This higher percentage for ransomware implies that Karnataka is a significant target for such attacks, possibly due to its strong presence of IT companies, startups, and digital enterprises, making it a lucrative target for cybercriminals.

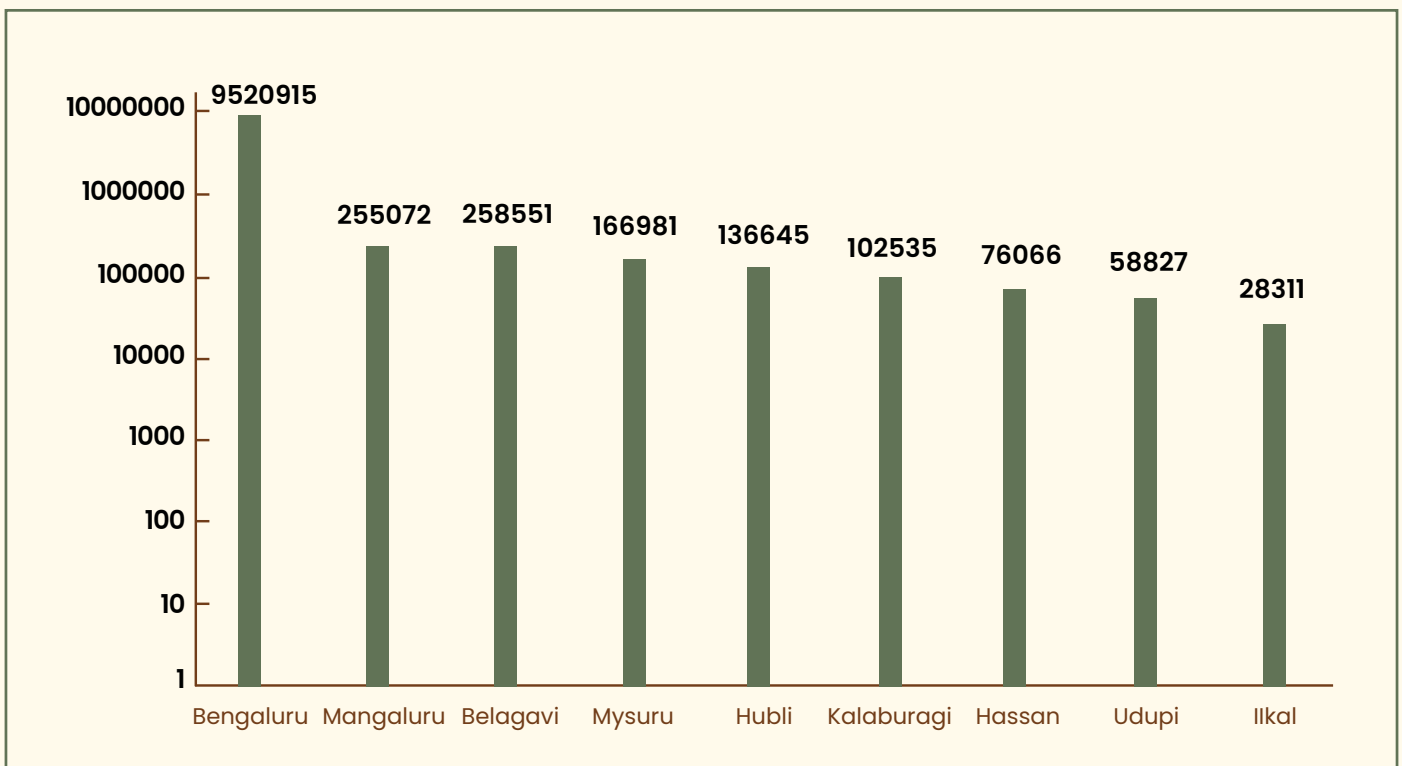
Detection Name	National Detection Count	Karnataka Detections
Malware	266674935	11456799
Ransomware	19858035	1784016

# Ransomware Month-Over-Month Trend

The month-over-month ransomware trend highlights the evolving tactics of ransomware operators, showing how they adapt their campaigns based on elections, financial cycles, seasonal trends, and major cybersecurity responses.



# Top 10 Affected Cities



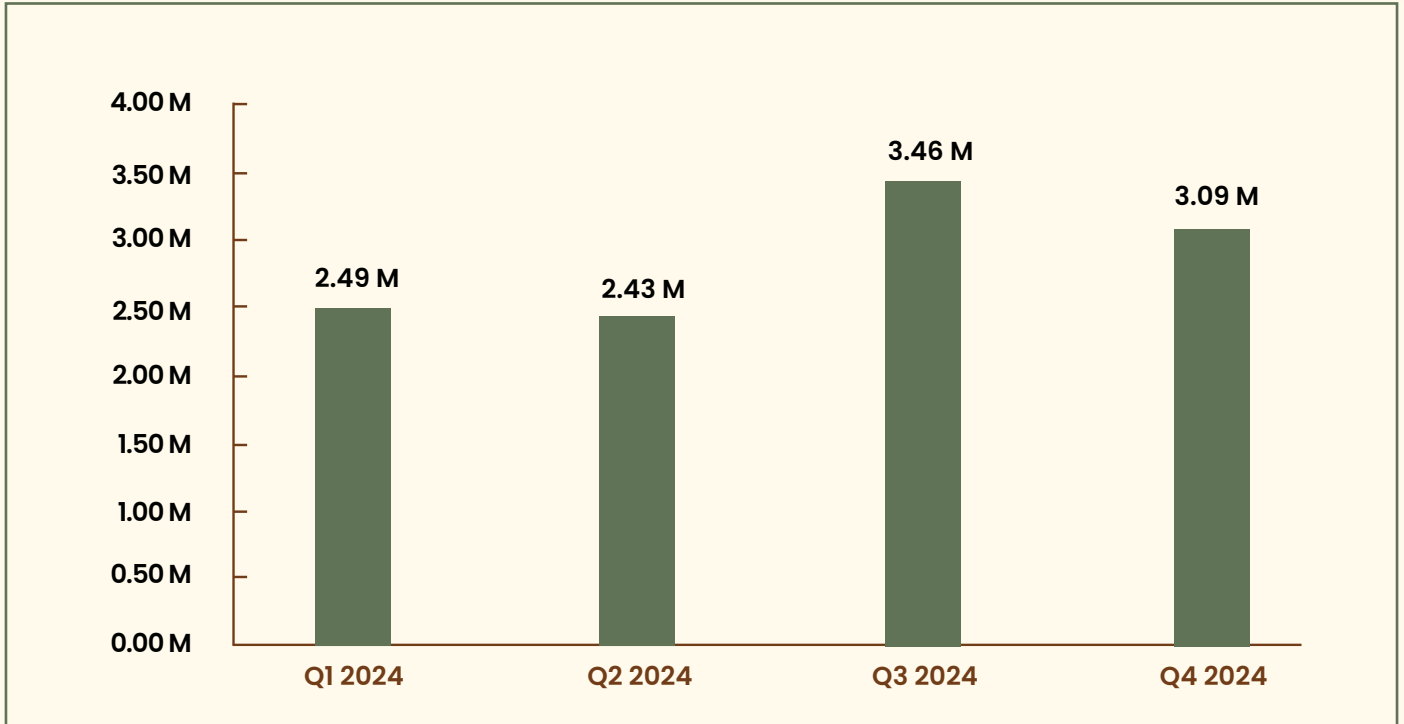
Bangalore leads in malware detection, with the number of hits being more than four times higher than the average of other cities

# Karnataka in top 10 most attacked states in India



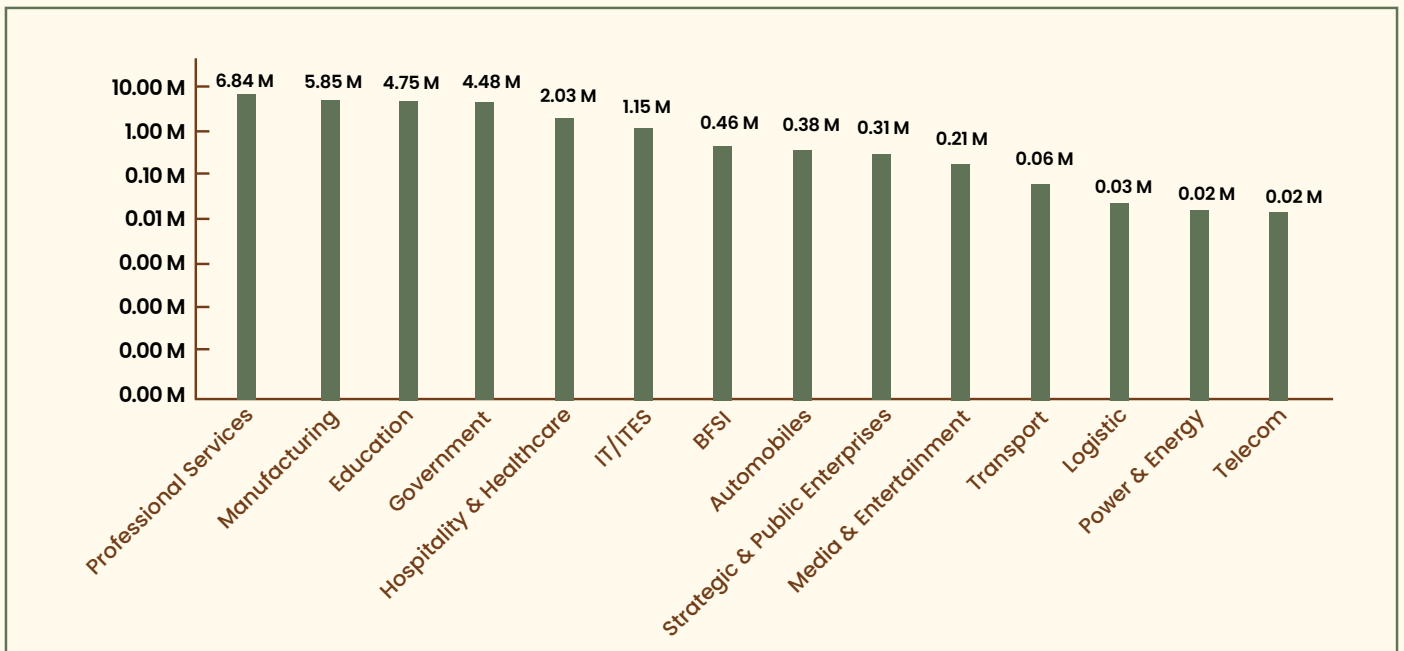


## Quarter wise Detection Hits



The chart highlights a significant increase in detection hits in Q3 2024, reaching 3.46 million, followed by a slight decline in Q4. This trend suggests a surge in detections mid-year.

## Detection Statistics Industry-wise








The chart illustrates industry-wise detection statistics, with Professional Services experiencing the highest detection hits at 6.84 million, followed by Government and Education. In contrast, industries like Telecom and Power & Energy recorded the lowest detections, indicating attackers are much inclined towards attacking Government agencies and Professional services.

# Attack on Karnataka's Top Industries



This section provides an in-depth analysis of sector-wise segregation of attacks encountered in 2024. Understanding these characteristics is crucial for developing effective detection, prevention, and mitigation strategies to safeguard against evolving threats. The total detections for the specific sectors amount to 3 million, which constitutes 20.8% of the overall malware detections of Karnataka.

# Top Detections: Industry-wise

 <b>Education</b>	Detection Name <b>W32.Pioneer.CZ1</b> Attacks <b>18,966</b>	 <b>Government</b>	Detection Name <b>Remotedadmin.Remoteexec</b> Attacks <b>11,244</b>
 <b>Hospitality &amp; Healthcare</b>	Detection Name <b>PIF.StucksNet.A</b> Attacks <b>9,118</b>	 <b>Professional Services</b>	Detection Name <b>O97M.Agent.34591</b> Attacks <b>3,097</b>
 <b>BFSI</b>	Detection Name <b>LNK.Cmd.Exploit.F</b> Attacks <b>1,567</b>	 <b>IT/ITES</b>	Detection Name <b>W32.Perite.A</b> Attacks <b>719</b>
 <b>Manufacturing</b>	Detection Name <b>Riskware.Dupatcher.A4</b> Attacks <b>596</b>		

The table highlights the top detections across industries, with Education experiencing the highest detection count, followed by Government.

## Key Takeaways

- 1. Election Season Drives Ransomware Spikes (March–April 2024)**
  - a. Cybercriminals leveraged election-related misinformation and phishing campaigns, targeting voter data, political organizations, and government institutions.
  - b. Increased cyber activity around financial transactions and media coverage made organizations more vulnerable.
- 2. Financial Year-End & BFSI Sector Attacks (March–July 2024)**
  - a. Attackers targeted businesses, banks, and financial services handling sensitive transactions.
  - b. July saw the highest attacks due to mass ransomware campaigns targeting IT and BFSI sectors, possibly using exploit kits and leaked credentials.
- 3. Festive Season Scams & Student Targeting (Sep–Oct 2024)**
  - a. Ransomware gangs shifted focus to students and job seekers, using fake admissions and hiring portals.
  - b. Diwali-season phishing scams were common, though organizations had improved security, leading to a drop in successful attacks.
- 4. Holiday Season Decline (Nov–Dec 2024)**
  - a. Cybercriminals shifted focus to future planning rather than immediate attacks.
  - b. Security awareness programs launched post-July spike helped reduce detections.

# The Karnataka government and various organizations are taking steps to address these cyber risks and threats. These include:

---

◆ **Developing cybersecurity policies and frameworks:**

The government has formulated a dedicated cyber security policy to strengthen the state's IT infrastructure and combat cybercrime.

---

◆ **Establishing Security Operation Centers (SOCs):**

SOCs are being set up to monitor and respond to cyber threats in real-time.

---

◆ **Promoting awareness and training:**

Initiatives are being taken to educate individuals and organizations about cybersecurity best practices.

---

◆ **Encouraging collaboration:**

Collaboration between government, industry, and academia is being fostered to share information and expertise on cybersecurity.

---

◆ **Investing in cybersecurity infrastructure:**

Investments are being made to enhance the state's cybersecurity infrastructure and capabilities.







A scenic view of a tea plantation on a hillside. The foreground shows a dirt road winding through rows of green tea bushes. In the background, there are several trees and a hazy sky. The text "FEATURED STORIES 2025" is overlaid in large white letters.

# FEATURED STORIES 2025

# Prominent Recent Cyber Attacks

## Leading Telecom Provider Data Breach (Karnataka)



### Summary

In late 2024, a significant data breach targeted India's leading telecom provider Karnataka operation, compromising sensitive customer information, including phone numbers, email addresses, and KYC (Know Your Customer) documents. The attackers infiltrated their internal systems through an exposed API vulnerability, allowing unauthorized access to customer databases.

#### The breach resulted in:

- Exposure of personally identifiable information (PII) of thousands of subscribers.
- Potential SIM swapping risks due to leaked identity documents.
- Loss of customer trust and regulatory scrutiny from Indian telecom authorities.

The breach was identified when unusual data access patterns were detected in the telecom service provider's internal logs. In response, the telecom company revoked API access, notified affected customers, and worked with cybersecurity firms to analyse the attack.



Figure Showing Attack Flow



## Stage 1: Initial Reconnaissance & Target Selection

Before launching the attack, cybercriminals conducted reconnaissance to identify vulnerabilities in the telecom company's infrastructure. Possible reconnaissance methods included:

- **Open-Source Intelligence (OSINT):** Attackers scanned telecom company's official website, customer support portals, and public documentation for API endpoints and configuration details. Social media and dark web forums were monitored to identify leaked employee credentials from previous breaches.
- **Automated Scanning & Exploitation:** Using tools like Shodan, attackers searched for exposed APIs or misconfigured cloud storage buckets. Nmap and other scanning tools were used to probe the network for outdated services or improperly secured endpoints.
- **Third-Party Vendor Risk:** Attackers identified external vendors providing services to telecom company, looking for weaker security measures that could serve as entry points.

## Stage 2: Initial Access – Exploiting API Vulnerabilities

The attackers gained access to the telecom company's customer database through an unsecured API endpoint, allowing them to retrieve user data without authentication.

### Possible methods used:

- **API Misconfiguration:** Public-facing APIs that lacked proper authentication were exploited to pull customer records.
- **Broken Access Control:** The attackers leveraged insecure direct object references (IDOR), altering API parameters to access other users' data.
- **Leaked API Keys:** If API keys were exposed in source code repositories or other online platforms, they could be misused to retrieve sensitive information.

### Once inside, the attackers accessed large volumes of customer data, including:

- Mobile numbers
- Email addresses
- KYC documents (Aadhaar, PAN, etc.)
- SIM activation details

## Stage 3: Data Exfiltration & Impact

After breaching the API, the attackers extracted large datasets and stored them in offshore servers.

### Exfiltrated Data:

- Customer personal information, increasing risks of phishing and identity theft. KYC documents, which could facilitate SIM swapping attacks and financial fraud.
- Internal logs, revealing system architecture details for future exploitation.

### Consequences of the Breach:

- **Regulatory Action:** The Telecom Regulatory Authority of India (TRAI) and the Indian Computer Emergency Response Team (CERT-In) initiated investigations.
- **Customer Trust Issues:** The telecom company customers were alarmed by the exposure of sensitive data, leading to public outcry.
- **Dark Web Listings:** The stolen data was reportedly found for sale on underground forums, increasing risks of fraud.

## Stage 4: Detection & Response

The telecom company's security teams detected the breach after identifying abnormal API traffic and excessive data queries from unauthorized IP addresses.

### Immediate Response Measures Taken:

- Customer personal information, increasing risks of phishing and identity theft. KYC documents, which could facilitate SIM swapping attacks and financial fraud.
- Internal logs, revealing system architecture details for future exploitation.

### Consequences of the Breach:

- **Revoked API access:** The vulnerable endpoint was disabled to prevent further data leakage.
- **Reset authentication tokens:** API keys were rotated, and stricter authentication policies were enforced.
- **Informed affected customers:** The telecom company issued security advisories warning users about potential phishing threats.
- **Strengthened monitoring:** Implemented real-time threat detection to flag abnormal data access patterns.

## Stage 5: Long-Term Security Enhancements

In the aftermath, the telecom company implemented several security measures to prevent similar breaches:

### Enhanced API Security:

- OAuth2.0 authentication was enforced for all API endpoints.
- Rate-limiting was introduced to detect and block bulk data extraction attempts.

### Regular Security Audits:

- Penetration testing was conducted to identify vulnerabilities in existing APIs.
- Bug bounty programs were expanded to engage ethical hackers in finding security gaps.

### Stronger Customer Security Policies:

- Multi-factor authentication (MFA) was encouraged for all customer accounts.
- SIM swap verification enhancements were implemented to prevent unauthorized number porting.

## Conclusion

The telecom company Karnataka data breach highlights the growing threat posed by API vulnerabilities. Attackers increasingly exploit misconfigured endpoints to access sensitive data, making API security a critical focus area for telecom providers. This breach underscores the need for telecom companies to enhance customer data protection measures.

# Cyberattack on the Research Institute – Early 2024

## Summary

In early 2024, the research institute, a premier research institution under ISRO, suffered a sophisticated cyberattack. The breach targeted satellite research data, remote sensing databases, and administrative systems, potentially impacting India's geospatial intelligence efforts.

The attackers gained initial access through spear-phishing emails sent to research faculty and IT administrators. Using privilege escalation techniques, they navigated critical networks, accessing sensitive remote sensing data, satellite control documentation, and research projects.

### The breach resulted in:

- Exfiltration of confidential satellite and geospatial data.
- Disruptions in ongoing remote sensing research projects.
- Potential national security risks due to exposure of sensitive information.

The attack was detected when anomalous outbound traffic was identified. The institute isolated affected systems, collaborated with ISRO's cybersecurity team, and enhanced security measures to prevent future intrusions.



Figure Showing Attack Flow

## Stage 1: Initial Reconnaissance & Target Selection

Before launching the attack, cybercriminals conducted extensive reconnaissance on the research institute to identify vulnerabilities and key personnel.

### Possible Reconnaissance Techniques Used:

- **Open-Source Intelligence (OSINT):** Attackers studied publicly available research papers, institutional websites, and employee LinkedIn profiles to map key researchers, IT personnel, and administrators.
- **Dark Web Research:** If past breaches exposed the research institute staff credentials, attackers might have exploited them for access.
- **Scanning Network Infrastructure:** Tools like Shodan or Nmap may have been used to detect exposed servers, VPN vulnerabilities, or unpatched remote access systems.

## Stage 2: Gaining Initial Access, Spear-Phishing & Credential Theft

The attackers sent sophisticated spear-phishing emails to research scientists, IT administrators, and faculty members, impersonating trusted entities such as:

- Official emails from ISRO headquarters requesting urgent login verification.
- Fake research collaboration invitations containing malicious attachments.
- Security alert emails prompting password resets, redirecting users to phishing sites.

### Initial Access Was Gained By:

- **Malware Payloads:** If victims downloaded and opened infected attachments, malware (such as keyloggers or remote access trojans) was deployed.
- **Credential Harvesting:** Users who entered login credentials on fake websites unknowingly handed them over to attackers.

## Stage 3: Privilege Escalation & Lateral Movement

Once inside the network, attackers sought higher privileges to access sensitive data.

### Privilege Escalation Techniques Used:

- Stealing saved credentials from browsers using tools like Mimikatz.
- Exploiting weak/default passwords on internal applications and databases.
- Pass-the-Hash attacks to gain unauthorized access to critical systems.
- Lateral Movement Across Networks

### Using stolen credentials, attackers moved laterally within the research institute network, accessing:

- Remote Sensing Databases (containing high-resolution satellite imagery and classified geospatial data).
- Satellite Research Projects (sensitive information related to upcoming ISRO satellite missions).
- Email Servers (potentially compromising sensitive communication among researchers).

## Stage 4: Data Exfiltration & Impact

The attackers systematically extracted and transferred sensitive files to remote servers. The stolen data likely included:

- Geospatial data sets & satellite imagery crucial for national security.
- Confidential research reports on remote sensing applications.
- Internal documents related to ISRO's satellite control operations.

### **Impact of the Cyberattack:**

- Loss of critical research data, affecting ongoing scientific projects.
- Potential compromise of national security, as sensitive geospatial intelligence might be used for strategic analysis by adversaries.
- Disruptions in satellite data processing, delaying research in agriculture, defense, and disaster management.

## Stage 5: Detection, Incident Response & Mitigation

The research institute security teams detected anomalous outbound traffic flowing to unrecognized foreign IP addresses. Further forensic analysis revealed unauthorized logins from multiple locations, triggering an internal investigation.

### **Immediate Response Actions Taken:**

- Isolated infected systems to contain further data loss.
- Reset credentials and enforced multi-factor authentication (MFA) on all accounts.
- Engaged ISRO's cybersecurity division to conduct a detailed forensic investigation.

### **Long-Term Mitigation Strategies Implemented:**

- Strengthened Endpoint Security: Advanced threat detection systems were deployed across the research institute's network.
- Phishing Awareness Training: Faculty and researchers received training on identifying and reporting phishing attempts.
- Enhanced Network Monitoring: Real-time traffic analysis tools were implemented to detect unusual data transfers.

## Conclusion

This cyberattack highlights the growing threat to research institutions, especially those handling sensitive national security data. Attackers exploited human vulnerabilities via phishing, underscoring the need for continuous cybersecurity vigilance.

# Multi-Specialty Hospital Chain Ransomware Attack (Karnataka) – Mid 2024



## Summary

In mid-2024, one of the largest healthcare providers in Karnataka suffered a ransomware attack that disrupted its operations across multiple branches. The attackers deployed a sophisticated ransomware variant that encrypted critical healthcare data, including patient medical records, administrative documents, and hospital management systems. The breach severely impacted hospital operations, leading to delays in patient care and extensive recovery efforts.

The attack originated from a phishing email that compromised hospital staff credentials, enabling attackers to gain access to the internal network. The encrypted files were held hostage, and the attackers demanded a large ransom for the decryption keys.

### The breach resulted in:

- Data encryption of medical records, patient histories, and internal communications.
- Disruption of hospital services, including delayed surgeries and patient admissions.
- Potential exposure of personal health information (PHI), leading to privacy concerns.
- Financial losses due to ransom payment and operational downtime.

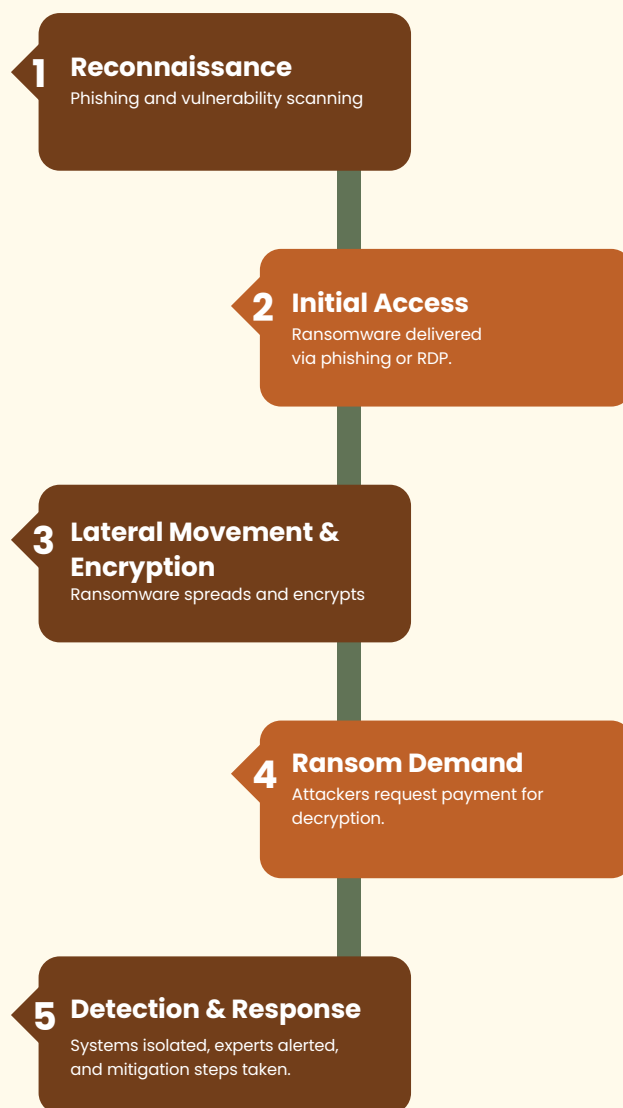


Figure Showing Attack Flow

## Stage 1: Initial Reconnaissance & Target Selection

Before launching the ransomware attack, the cybercriminals conducted reconnaissance to identify vulnerabilities within the hospital's network infrastructure. Potential reconnaissance methods used:

### Reconnaissance Techniques:

- **Open-Source Intelligence (OSINT):** Attackers likely explored publicly available hospital websites, patient portals, and related systems to identify potential vulnerabilities such as outdated software or exposed services.
- **Employee Social Media & Phishing Targets:** Attackers may have used employee information from public social media profiles or past breach data to craft targeted phishing emails.
- **Vulnerability Scanning:** Attackers scanned for unpatched network services, weak authentication practices, and public-facing administrative interfaces using automated tools like Shodan or Nmap.

## Stage 2: Initial Access – Phishing Attack

The attackers gained initial access to the hospital's internal network through a spear-phishing email that targeted hospital staff and administrators. The email appeared legitimate, often mimicking communications from internal hospital management or external vendors.

### Phishing Techniques:

- **Malicious Attachments:** The phishing email contained a malware-laden attachment that, when opened, executed a payload on the victim's system, establishing an initial foothold within the network.
- **Credential Harvesting:** Users who interacted with fake login portals provided their credentials, allowing attackers to access hospital systems with legitimate privileges.
- **Exploiting Weak Authentication:** Weak password practices across hospital systems may have been leveraged to escalate the attack.

Once the malware was deployed, the attackers had access to the hospital's internal systems and began to escalate privileges to gain more control.

## Stage 3: Lateral Movement & Ransomware Deployment

After gaining access to the network, the attackers used privilege escalation techniques to move laterally and deploy the ransomware across critical hospital systems. The following steps were likely involved:

### Privilege Escalation Techniques:

- **Credential Dumping:** Tools like Mimikatz or built-in system utilities were used to extract additional administrator credentials.



- **Exploiting Unpatched Services:** Attackers used known exploits for unpatched services to escalate privileges within the hospital's network.
- **Pass-the-Hash Attacks:** Using hashed passwords obtained from the network, attackers accessed key systems with elevated privileges.

#### **Ransomware Deployment:**

- **Mass Encryption:** The ransomware encrypted crucial files, including medical records, scheduling data, patient history files, and internal email communication.
- **File System Lockdown:** The ransomware also encrypted backup files, ensuring that hospital operations could not be restored without decryption.

### **Stage 4: Data Exfiltration & Impact:**

While the primary objective was to encrypt data and demand ransom, the attackers also likely exfiltrated sensitive healthcare information. This data could be used for further attacks, such as identity theft or extortion.

#### **Data Exfiltration:**

- **Patient Health Records:** Potential exposure of patient personal health information (PHI), including medical histories, diagnoses, and treatment details.
- **Internal Emails & Administrative Data:** Stolen administrative data, including billing information and operational protocols, could have been sold or used for further attacks.
- **Sensitive Medical Research:** If any medical research data was stored on compromised systems, it could have been exfiltrated for strategic purposes.

#### **Consequences of the Breach:**

- **Healthcare Disruption:** The hospital had to revert to manual systems for patient management, leading to delays in treatment and surgeries.
- **Ransom Demand:** The attackers demanded a large ransom, and while the hospital did not publicly disclose the payment, reports suggested that the ransom was substantial.
- **Regulatory Scrutiny:** The breach prompted investigations by healthcare regulatory bodies, including the National Health Authority of India, over the exposure of patient data.

### **Stage 5: Detection & Response:**

The hospitals detected the ransomware attack when staff began experiencing issues accessing essential systems. The security teams initiated the response protocol, isolating affected systems and initiating an internal investigation.

#### **Immediate Response Actions:**

- **System Isolation:** The affected systems were disconnected from the network to prevent further encryption of files.

- **Ransomware Analysis:** Cybersecurity teams worked with external cybersecurity firms to analyze the ransomware variant, identify its entry point, and develop a decryption strategy.
- **Backup Restoration:** The hospital attempted to restore critical systems from backups that had not been affected by the encryption process.
- **Law Enforcement Involvement:** The breach was reported to local authorities, including the Cyber Crime Cell in Karnataka, to investigate potential criminal activities.

#### **Longer-Term Mitigation Actions:**

- **Enhanced Endpoint Protection:** Endpoint detection and response (EDR) tools were deployed across all hospital systems to detect and block ransomware activity.
- **Phishing Awareness Training:** Hospital staff underwent intensive training on identifying phishing emails and suspicious attachments.
- **Network Segmentation:** The hospital network was segmented to limit lateral movement of attackers in case of future breaches.
- **Backup System Hardening:** Backup systems were hardened to ensure they were inaccessible to future ransomware attacks, with regular checks for integrity and redundancy.

## **Conclusion**

The hospital's ransomware attack demonstrates the growing threat faced by healthcare organizations, which hold sensitive and high-value data. This attack underscores the importance of a comprehensive security strategy that includes robust email filtering, employee training, and system backups.

# Cyberattack on a Government portal– February 2025



## Summary

In February 2025, one of the government portal suffered a Distributed Denial of Service (DDoS) attack, causing major service disruptions and financial losses. The attack affected 256 sub-registrar offices across the state, delaying property registrations, legal transactions, and revenue collection.

This attack marks another instance of cyber threats targeting government digital services, highlighting vulnerabilities in public sector IT infrastructure and the growing sophistication of threat actors.

## Stage 1: Reconnaissance

Attackers identified the government portal as a high-impact target due to its role in real estate and revenue collection.

### Reconnaissance tactics included:

- Traffic analysis to pinpoint peak operational hours.
- Network scanning to detect weaknesses in the infrastructure.
- Open-source intelligence (OSINT) to gather information on portal security.

The attackers likely mapped out the server endpoints and backend connections before executing the attack.

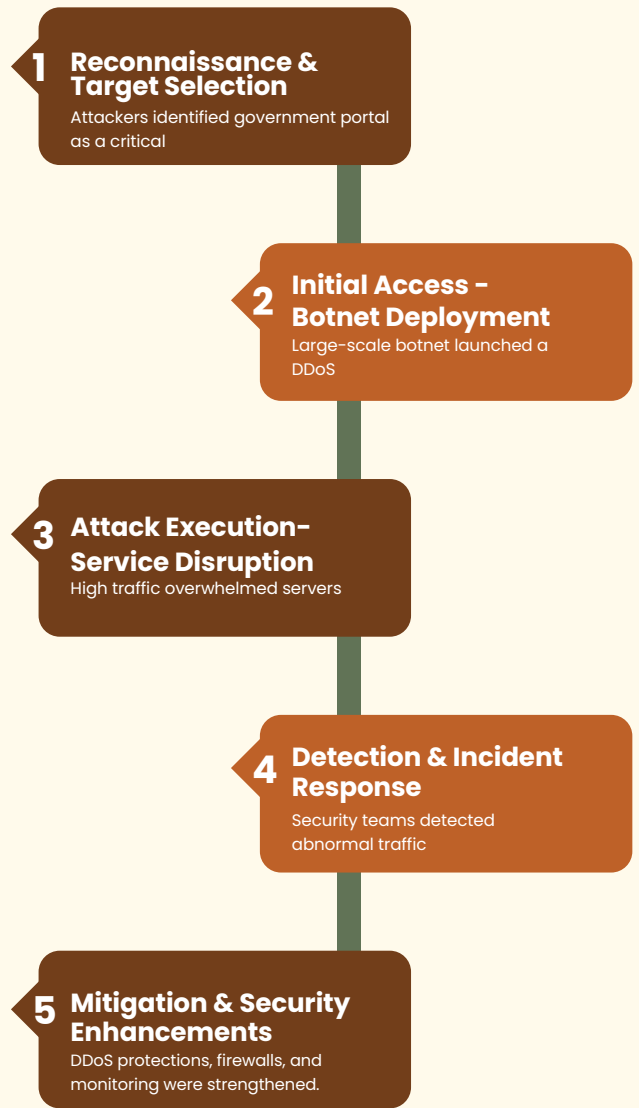


Figure Showing Attack Flow

## Stage 2: Initial Access

The attackers initiated the DDoS attack by flooding the system with massive amounts of malicious traffic.

Karnataka's cybersecurity team traced the source of the attack to an external IP address outside the state.

### **Possible attack techniques included:**

- Botnet-driven volumetric flooding to exhaust bandwidth.
- Application-layer DDoS targeting login and document submission pages.
- IP spoofing to mask the actual origin of attack requests.

## Stage 3: Execution & Impact

The attack crippled property registration services for multiple days, severely affecting both citizens and businesses.

Users faced system slowdowns and transaction failures, preventing essential property documentation and legal approvals.

### **Karnataka's revenue dropped sharply due to the service outage:**

- February 1, 2025: 556 registrations processed (₹15.18 crore revenue).
- Normal daily average (December 2024): 7,721 registrations (₹62.93 crore revenue).
- The revenue loss amounted to ₹47.75 crore in a single day.

### **Broader consequences:**

- Delays in property transactions impacted buyers, sellers, and real estate developers.
- Legal bottlenecks arose as property registration is mandatory for ownership transfers.
- Trust in government digital services was shaken, leading to concerns over future cyber resilience.

## Stage 4: Detection & Response

Government officials detected the attack when the portal slowed down significantly, causing user complaints.

### **Incident response teams, including Karnataka's e-Governance department and CERT-In, began mitigation efforts:**

- Traffic filtering was deployed to block malicious IPs.
- Load balancing measures were applied to handle the increased traffic.
- Continuous system monitoring was implemented to detect further anomalies.

The state coordinated with cybersecurity experts to analyze attack patterns and prevent further disruptions.

## Stage 5: Recovery & Mitigation

By February 5, 2025, services were restored with 7,225 registrations processed, signaling normal system operations.

**Karnataka's e-Governance department implemented enhanced security measures, including:**

- Stronger DDoS mitigation solutions via cloud-based traffic filtering.
- Real-time network monitoring to detect unusual traffic spikes earlier.
- Server scalability enhancements to absorb future attack attempts.
- Security audits and stress testing to ensure resilience against similar attacks.

Public communication efforts were made to assure citizens and businesses of improved security.

## Conclusion

The cyberattack on a government portal underscores the evolving threats faced by critical government digital services. As seen in the telecom company data breach, the research institute attack, and now the government portal DDoS incident, cybercriminals are increasingly targeting sectors vital to national infrastructure, disrupting essential operations and causing significant financial losses.

This incident highlights the urgent need for robust cybersecurity measures in public sector IT systems. DDoS attacks, phishing, and privilege escalation remain common tactics, emphasizing the necessity of real-time monitoring, proactive threat intelligence, and scalable security solutions. The rapid response by Karnataka's e-Governance department helped mitigate prolonged service disruptions, but the attack serves as a reminder that reactive security is not enough; governments must anticipate threats and implement preventive safeguards.

Moving forward, collaboration between government agencies, cybersecurity experts, and regulatory bodies is crucial to fortifying India's digital infrastructure. By adopting zero-trust architectures, advanced DDoS protection, and continuous security audits, organizations can better defend against cyber threats and ensure public trust in digital governance remains intact.

# Key Takeaways from the Telecom Company(2024), Research Institute(2024), Multispeciality Hospital (2024), and Governement Portal Cyberattacks:

## Critical Infrastructure as a Prime Target

- Telecom, healthcare, research, and government services were targeted, showing that cybercriminals focus on high-impact sectors.
- Attacks on these sectors disrupt essential services and pose national security risks.

## Phishing, Exploits & DDoS Remain Key Entry Points

- India's leading telecom service provider, research Institute, and one of the biggest multispeciality hospital in India were all infiltrated through phishing emails and exploitation of vulnerabilities (unpatched APIs, weak RDP access).
- Employees remain the weakest link in all cases, highlighting the need for continuous cybersecurity awareness training.
- The government portal was a botnet-driven DDoS attack crippled public services.
- Different attack vectors highlight the need for layered security approaches

## Privilege Escalation and Lateral Movement Are Common Tactics

- Attackers escalated privileges using stolen credentials, misconfigured access controls, and weak authentication mechanisms.
- They moved laterally across networks to access sensitive data, often avoiding detection in telecom company, the research institute, and hospitals.
- Exploiting misconfigured access controls and weak credentials allowed deeper infiltration.
- Highlights the necessity of zero-trust security frameworks.

## Data Exfiltration, Ransomware & Service Disruptions Have Long-Term Impacts

- **Leading Telecom Company:** Exposed customer data affected millions, raising concerns over identity theft and triggering regulatory scrutiny.
- **Research Institute:** Loss of critical satellite and geospatial data posed a national security risk and disrupted scientific progress.
- **Multispeciality Hospital:** Ransomware encrypted patient data and disrupted the hospital's operations, with potential long-term impacts on healthcare delivery.
- **Government Portal:** No data breach, but the DDoS attack disrupted thousands of transactions, affecting governance and public services.

## Incident Response & Post-Attack Measures Are Crucial

- All organizations isolated compromised systems, reset credentials, and enhanced security measures.
- Real-time threat detection, multi-factor authentication (MFA), and implementing zero-trust architecture were emphasized as critical response strategies.
- The Telecom company & the multispeciality hospital chain implemented stricter API & access controls.
- The government portal improved DDoS mitigation strategies to prevent future attacks.

## Final Thoughts





- Proactive cybersecurity measures such as regular patching, continuous monitoring, and security audits are essential to prevent large-scale breaches.
- Human error remains a significant factor, making security awareness training non-negotiable.
- Robust backup systems and incident response plans are crucial to minimizing operational disruption and data loss.

# Hacktivist Attack Report: Telegram-Based Operations

Threat actors have been launching daily cyberattacks across India, with a rising focus on Karnataka. Operation through Telegram, these groups target various sectors, causing significant disruptions and data breaches. The victims, ranging from Government to Private organizations.

- On January 25, 2024, the Telegram Threat Actor (TA) group “**HELANG MERAH GROUP**” leaked the credentials of the St John's Medical College Hospital, Bengaluru, Karnataka, South India (<https://www.stjohns.in/>). Login Credentials of students and other Sensitive Authentication details were exposed online, putting the organization at risk of further breaches and unauthorized access.
- On February 03, 2024, the Telegram Threat Actor (TA) group “**NIXON CYBER TEAM**” launched a DDoS attack on the Indian Medical Association Karnataka State Branch-IMA-KSB (<https://www.imakarnataka.in/>). The cyberattack overwhelmed the Organization's servers, online platforms and including its management system and registration portals, causing widespread disruption to organization's services and access for members.
- On February 21, 2024, the Telegram Threat Actor (TA) group “**ANON TEN BD**” launched a DDoS attack on the Karnataka Tourism (<https://karnatakaturism.org/>). The cyberattack overwhelmed the servers, online booking platforms and including its management system and registration portals, causing widespread disruption to transportation services and access for registered users.
- On March 24, 2024, the Telegram Threat Actor (TA) group “**Z-BL4CX-H4T**” launched a DDoS attack on the Common Entrance Test Unit Portal of Karnataka Government (<https://cetonline.karnataka.gov.in/kea/>). The cyberattack overwhelmed the servers, online platforms and including its management system and registration portals, causing widespread disruption to entrance test portal's services and access for candidates.
- On March 23, 2024, the Telegram Threat Actor (TA) group “**Team insane Pakistan**” successfully hacked the Suvarna Karnataka Housing Co-operative Society Limited(R) (<https://suvarnakarnatakahousing.com/>). The attack led to unauthorized access to the society's website, exposing sensitive data, housing projects, and internal communications. The hacker defaced the website, replacing its content with malicious messages and potentially compromising personal information that tarnished the Co-operative society's public image.
- On March 23, 2024, the Telegram Threat Actor (TA) group “**Team insane Pakistan**” successfully hacked the National Association for the Blind (NAB-K) (<https://nabkarnataka.org/>). The attack led to unauthorized access to the association's website, exposing sensitive data, doner's information and internal communications. The hacker defaced the website, replacing its content with malicious messages and potentially compromising personal information that tarnished the association's public image.



-  On April 25, 2024, the Telegram Threat Actor (TA) group “GARUDA SECURITY” executed a defacement attack on the Tejas International Residential School (TIRS), Karnataka (<https://anonblackflag.tirs.edu.in/>, <https://fuckindia.tirs.edu.in>). The attacker altered the school’s website, replacing it with malicious message, compromising the site’s integrity. This defacement not only disrupted access to the website but also raised significant concerns about the site’s integrity.
  
-  On May 01, 2024, the Telegram Threat Actor (TA) group “AnonymousSusukan” launched a DDoS attack on the Karnataka Government’s E-parichay Portal (<https://epar.karnataka.gov.in>). The attack overwhelmed the Government’s online infrastructure, flooding its servers with massive traffic and rendering the website inaccessible for an extended period. This disruption caused server interference with public services, preventing citizens from accessing critical government info., online services.
  
-  On Jul 24, 2024, the Telegram Threat Actor (TA) group “NetSycho” launched a DDoS attack on the Bank of Karnataka (<https://karnatakabank.com/>). The attack overwhelmed the Bank’s online infrastructure, flooding its servers with massive traffic and rendering the website inaccessible for an extended period. This disruption caused server interference with public services, preventing citizens from accessing banking services. This may lead to a temporary loss of trust among customers.
  
-  On September 11, 2024, the Telegram Threat Actor (TA) group “DEFACER INDONESIA” executed a defacement attack on Karnataka’s media Associations (<https://themakkarnataka.in>). The attacker altered the website, replacing it with malicious message, compromising the site’s integrity. This defacement not only disrupted access to the website but also raised significant concerns about the site’s integrity.

# Prominent Threat Actors and Targeted Assets

## Key Threat Actors in Karnataka

- Lazarus Group (North Korea) - Targeted IT firms, fintech, and cryptocurrency exchanges.
- APT41 (China) - Focused on government and telecom networks.
- FIN11 (Russia) - Engaged in ransomware campaigns against BFSI and healthcare.
- BlackCat/ALPHV - Active in targeting manufacturing and education sectors.
- TA505 - Conducted phishing and ransomware attacks against professional services and retail.

## Top Targeted Assets

- Financial Institutions: Banking networks and payment gateways.
- IT & Software Companies: Targeted through supply-chain compromises.
- Government Portals: Election-related infrastructure and citizen databases.
- Healthcare & Hospitals: Patient records, medical devices, and hospital networks.
- Educational Institutes: University systems, student portals, and research.

# Government Investment in Cybersecurity – Karnataka vs. India

## Karnataka's Cybersecurity Initiatives

### Cyber Security Policy 2024:

- Focused on awareness, skill development, and tech adoption to counter cyber threats.
- ₹100 crore allocated to train 40,000 cybersecurity professionals.

### Sector-Specific Focus:

- Government & BFSI: Addressing remote admin exploit malware & banking trojans.
- Education & Manufacturing: Tackling pioneer malware & cryptojacking threats.

## India (National-Level Investments)

### **National Cyber Security Policy (NCSP):**

- Strengthening critical infrastructure defenses across BFSI, telecom, healthcare, and government sectors.
- Focus on public-private collaborations and threat intelligence sharing.
- CERT-In mandates for vulnerability disclosures & proactive threat mitigation.

# Top 3 Cyber Crime Types in Karnataka

## Karnataka's Cybersecurity Initiatives

### **Ransomware Attacks:**

- Attackers use advanced encryption techniques to lock critical data and demand ransom payments.
- Major targets include IT firms, Hospitals, and BFSI sectors.
- Double extortion tactics—where data is also leaked—are increasingly common.

### **Phishing and Social Engineering:**

- Cybercriminals deploy sophisticated phishing emails and fake websites to steal login credentials.
- Banking customers, government employees, and university students are frequently targeted.
- Deepfake scams and AI-powered phishing attacks are emerging threats.

### **Banking Trojans and Financial Fraud:**

- Malware designed to steal banking credentials and execute fraudulent transactions.
- Notable malware families include Dridex, Emotet, and QakBot.
- Attacks spike during tax filing periods and major financial events.

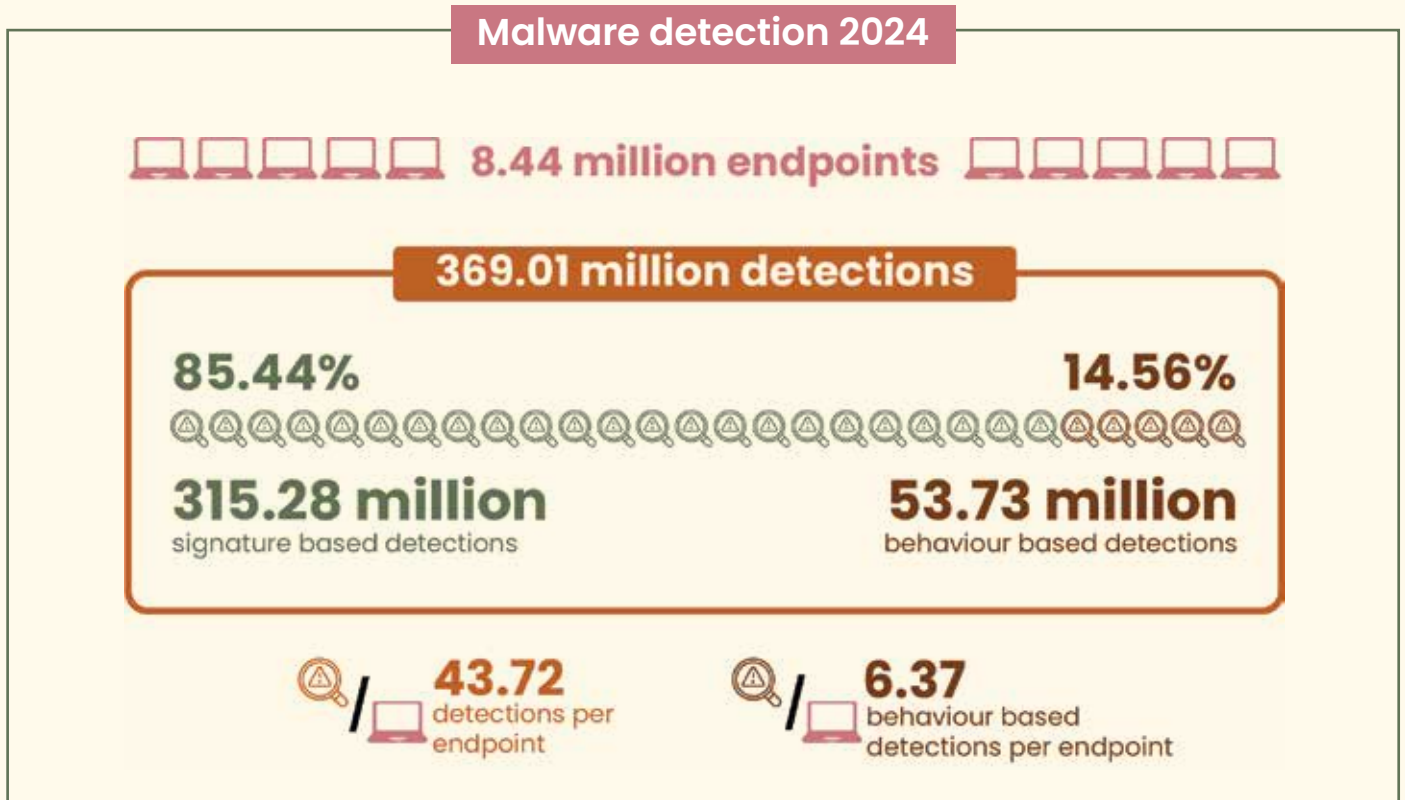
# THE STATE OF MALWARE IN INDIA



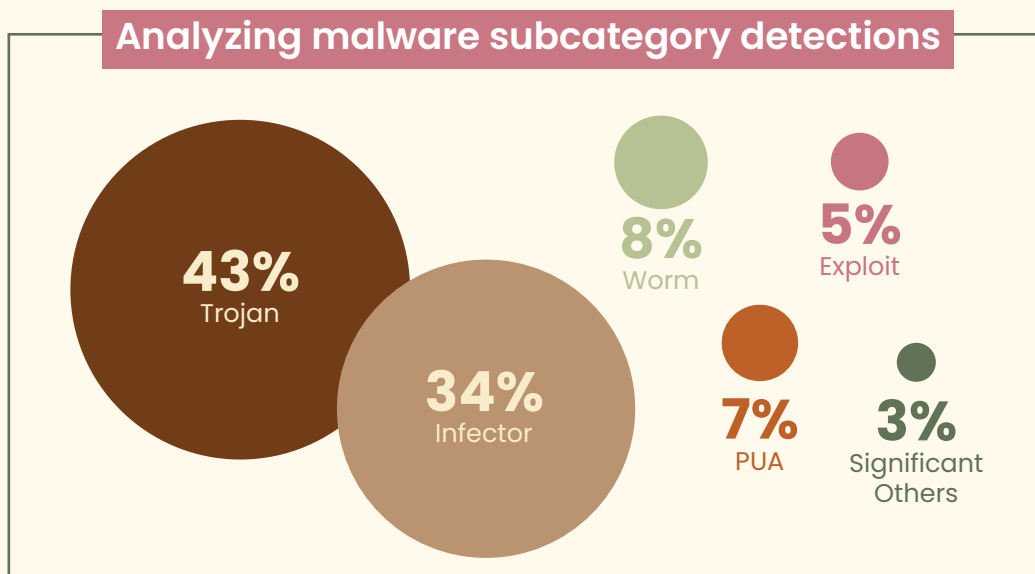


# Cybersecurity Outlook 2024

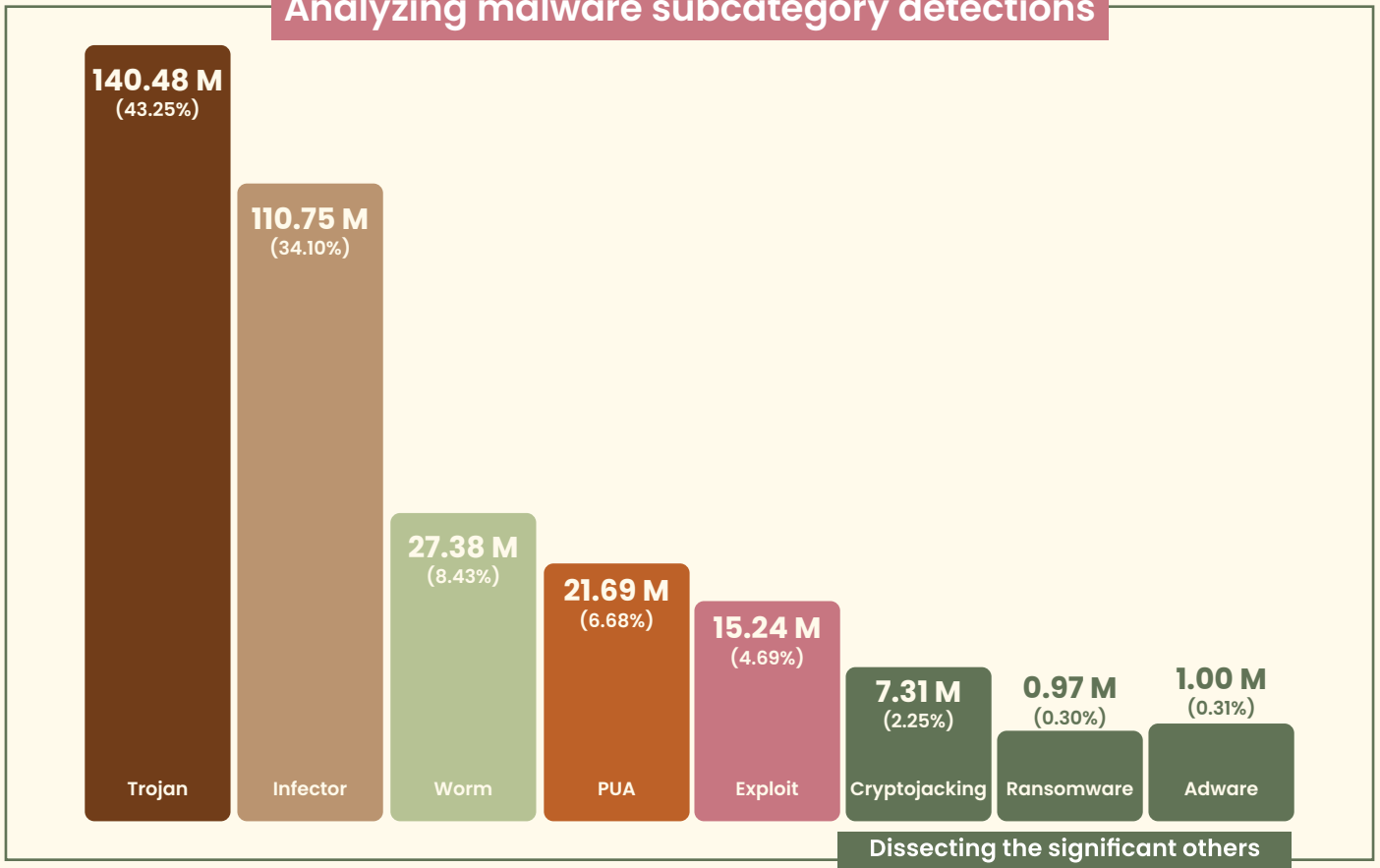
The analysis of India’s malware detection, based on Seqrite Labs’ telemetry data from October 2023 to September 2024, reveals critical insights into the current threat landscape. With **369.01 million** detections across **8.44 million** strong installation base, the data highlights both the scale of 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 Threats in India:



## Analyzing malware subcategory detections



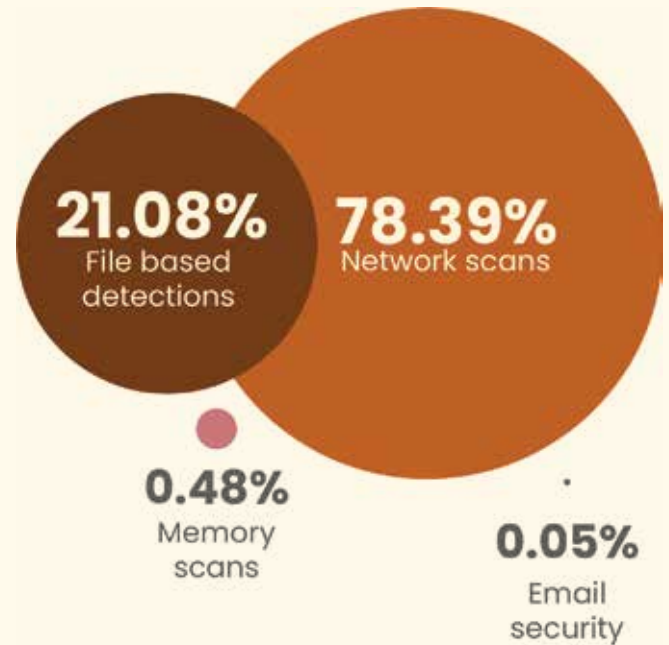
## Signature-Based Detection Landscape:

---

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

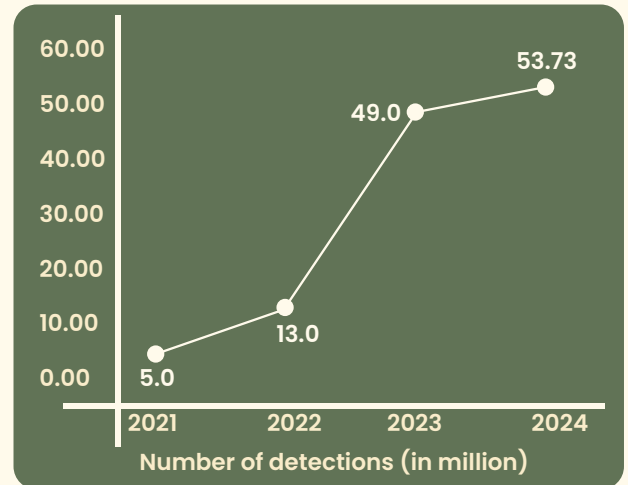


# Behavioral-Based Detection Landscape:

---

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

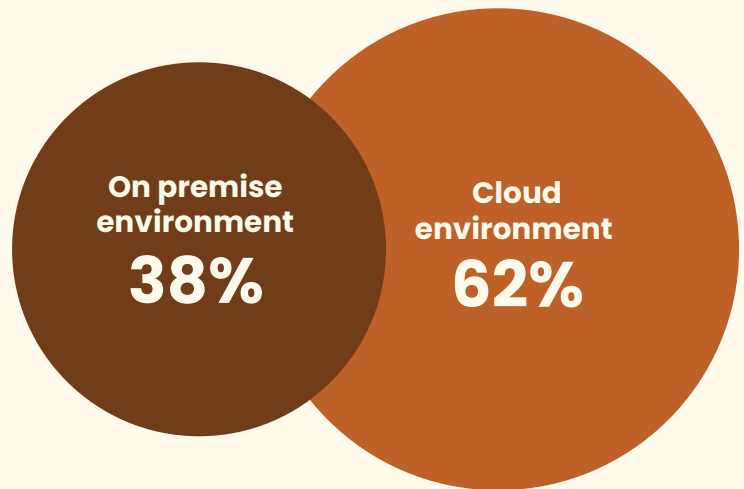
The significant growth in behavioral detections also reflects the maturation of underlying technologies. The integration of artificial intelligence and machine learning has dramatically enhanced the capability to analyze and identify suspicious patterns in real-time. Advanced processing capabilities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

## 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

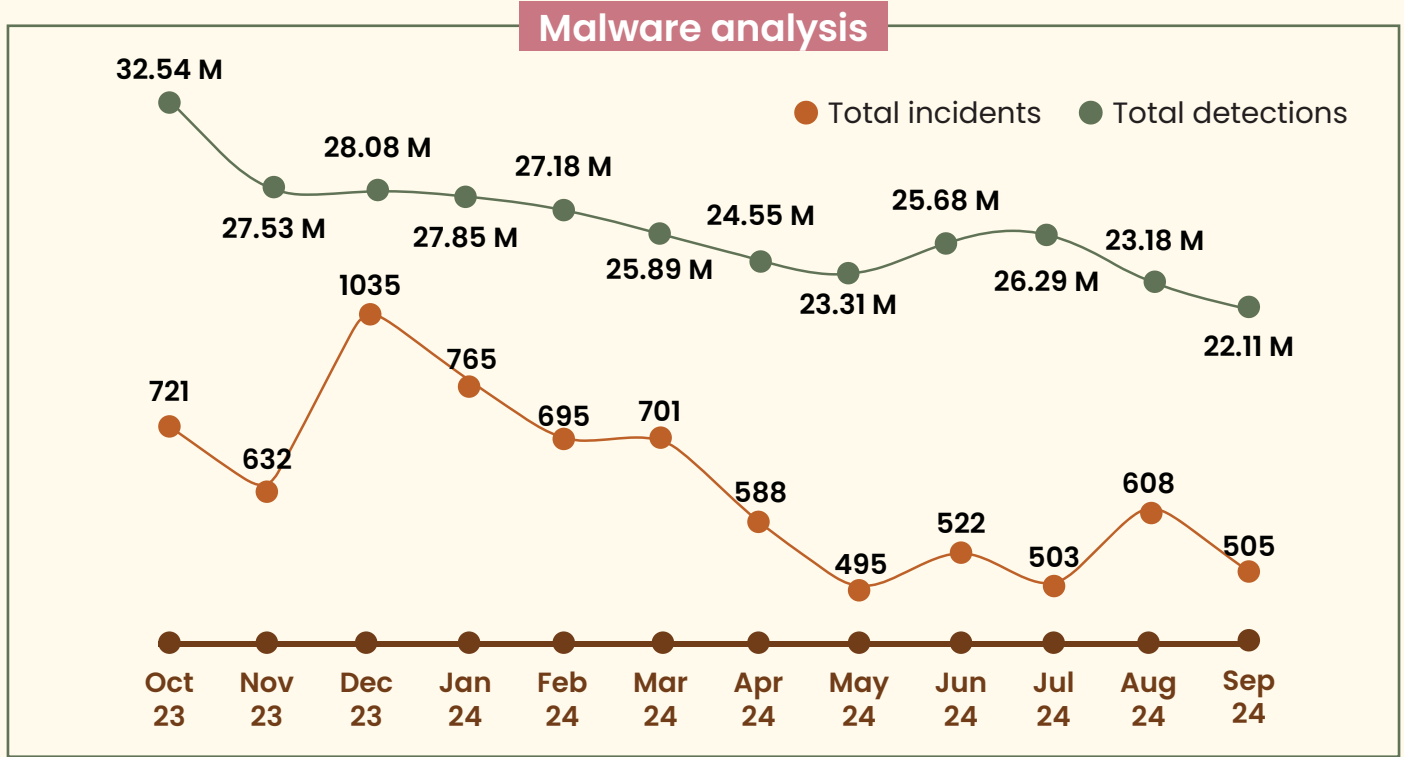
Cloud environment accounts for 62% of total detections (averaging 3.02 detections per endpoint) and on-premises environments contributing 38% (averaging 1.88 detections per endpoint).



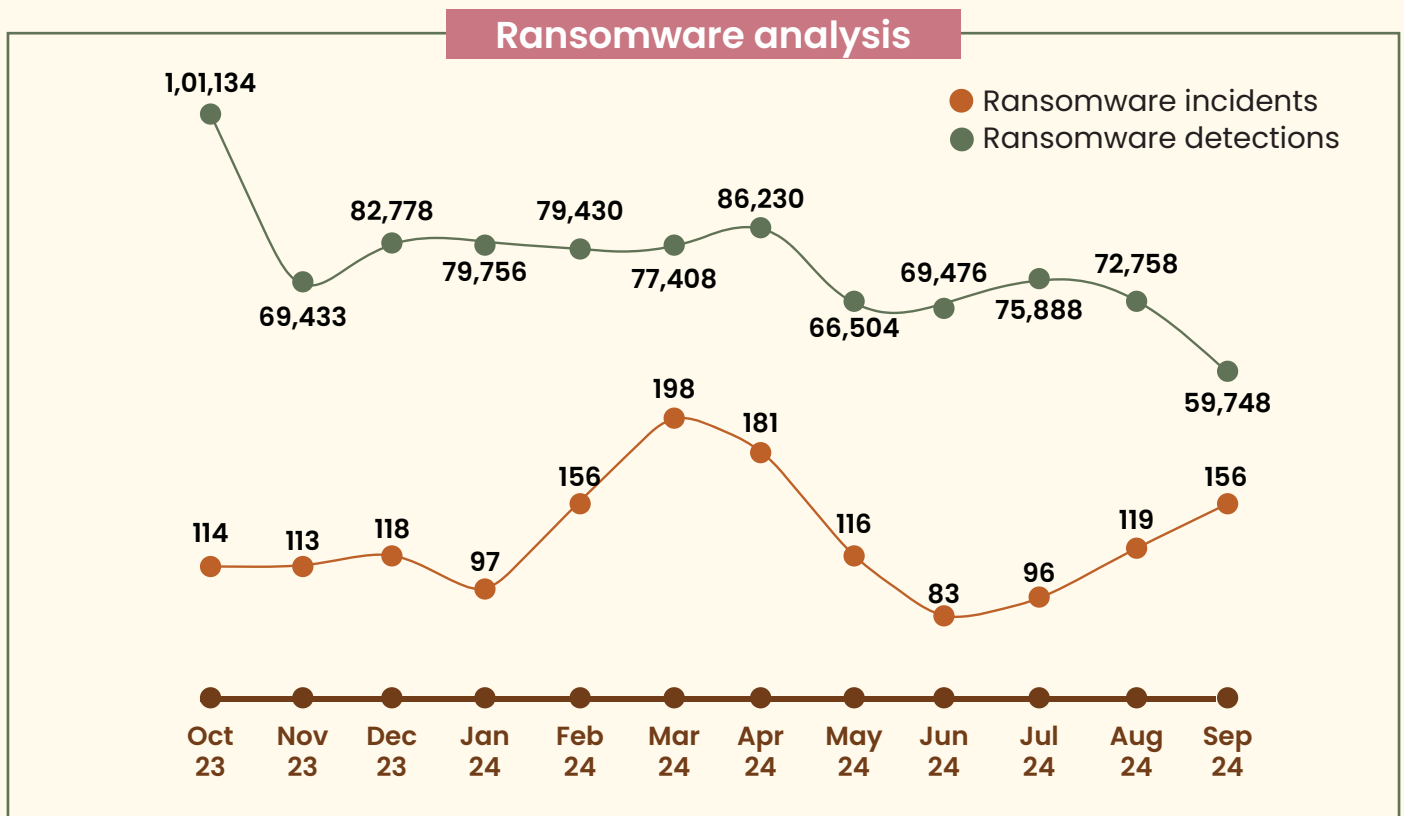
- ▲ Cloud environment show a significantly higher detection rate, reflecting their growing prominence in enterprise operations. This trend can be attributed to:
  - 🌐 **Increased adoption of cloud services:** Organizations are rapidly migrating to the cloud, expanding their attack surface and consequently 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					
Target Company (Mallox)	Dyiamond	Target Company (Mallox)	Makop	Dharma	Makop
Oct-23	Nov-Dec 23	Jan-24	Feb-Jul 24	Aug-24	Sep-24

### 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.

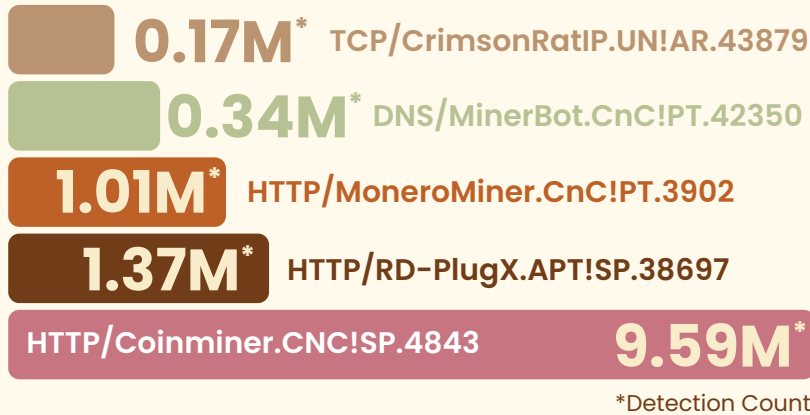
#### Rise of cryptocurrency miners:

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.

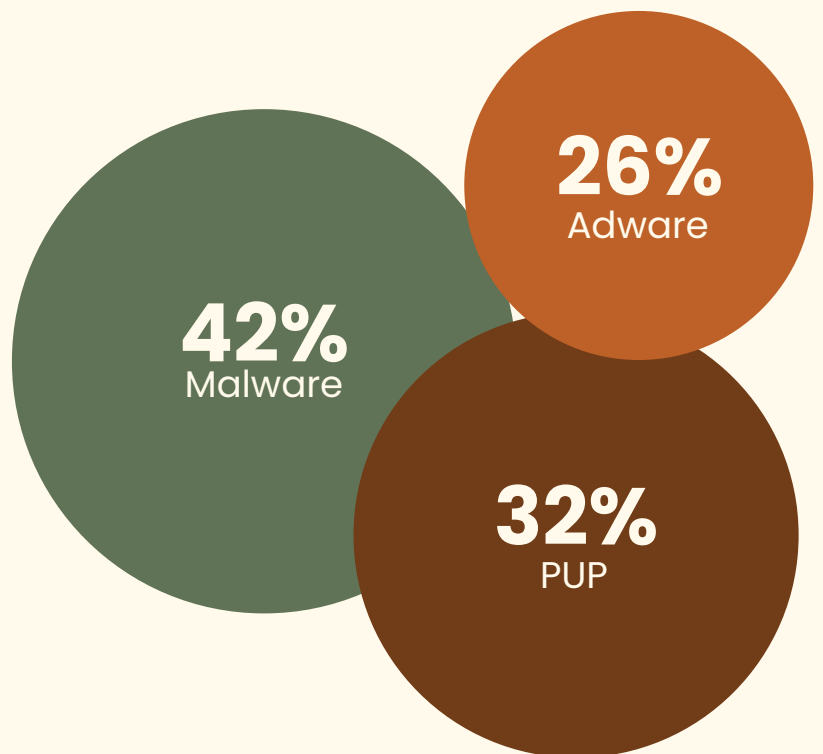
## Top Network Based Exploits Detailed Malware Profiles



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.

## 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.









# 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%)**

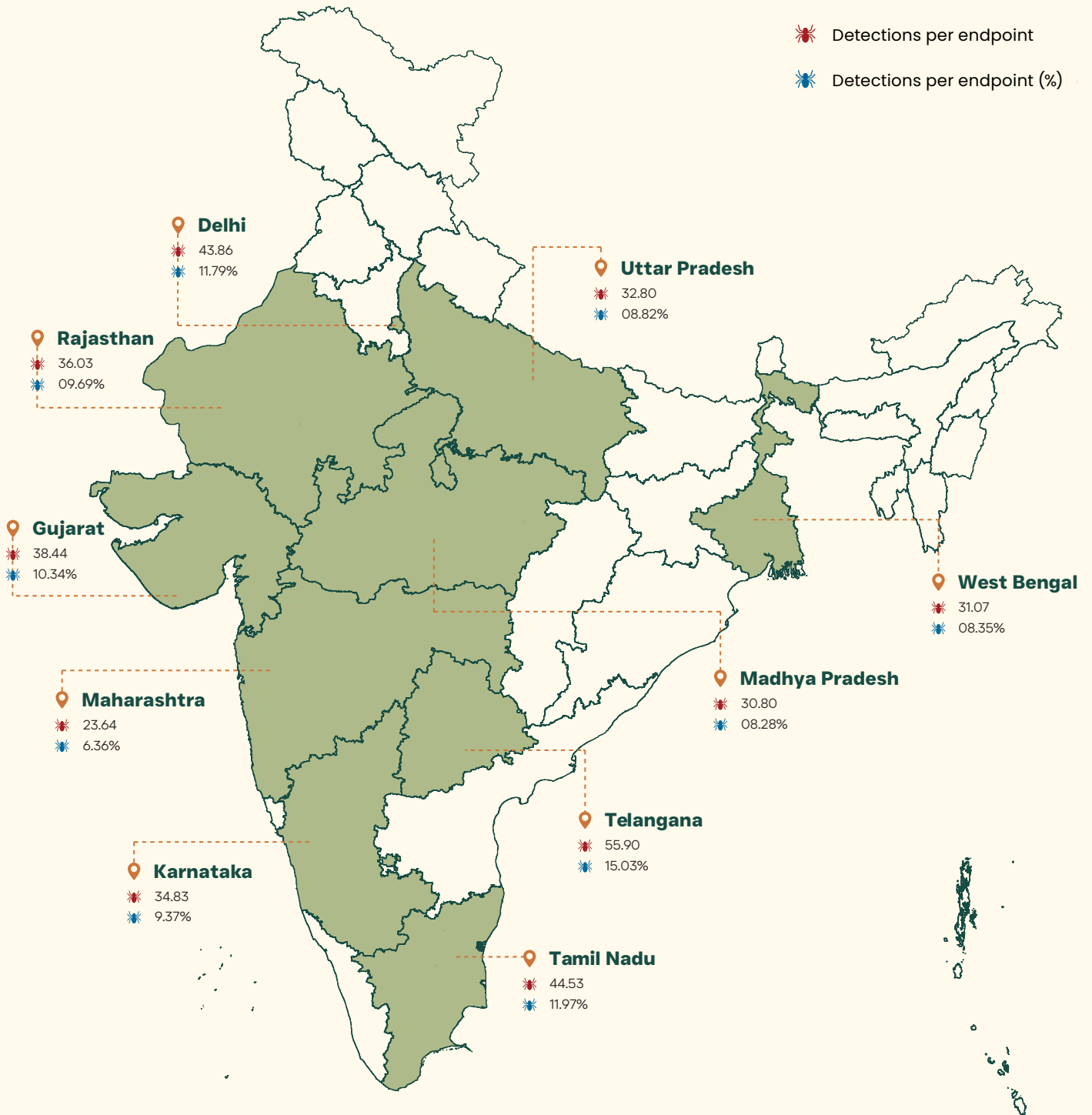
- ▲ Surprisingly low despite economic significance
- ▲ Potential underreporting or superior prevention

## Emerging Patterns

**Madhya Pradesh: 30.81 detections/endpoint**

**West Bengal: 31.07 detections/endpoint**

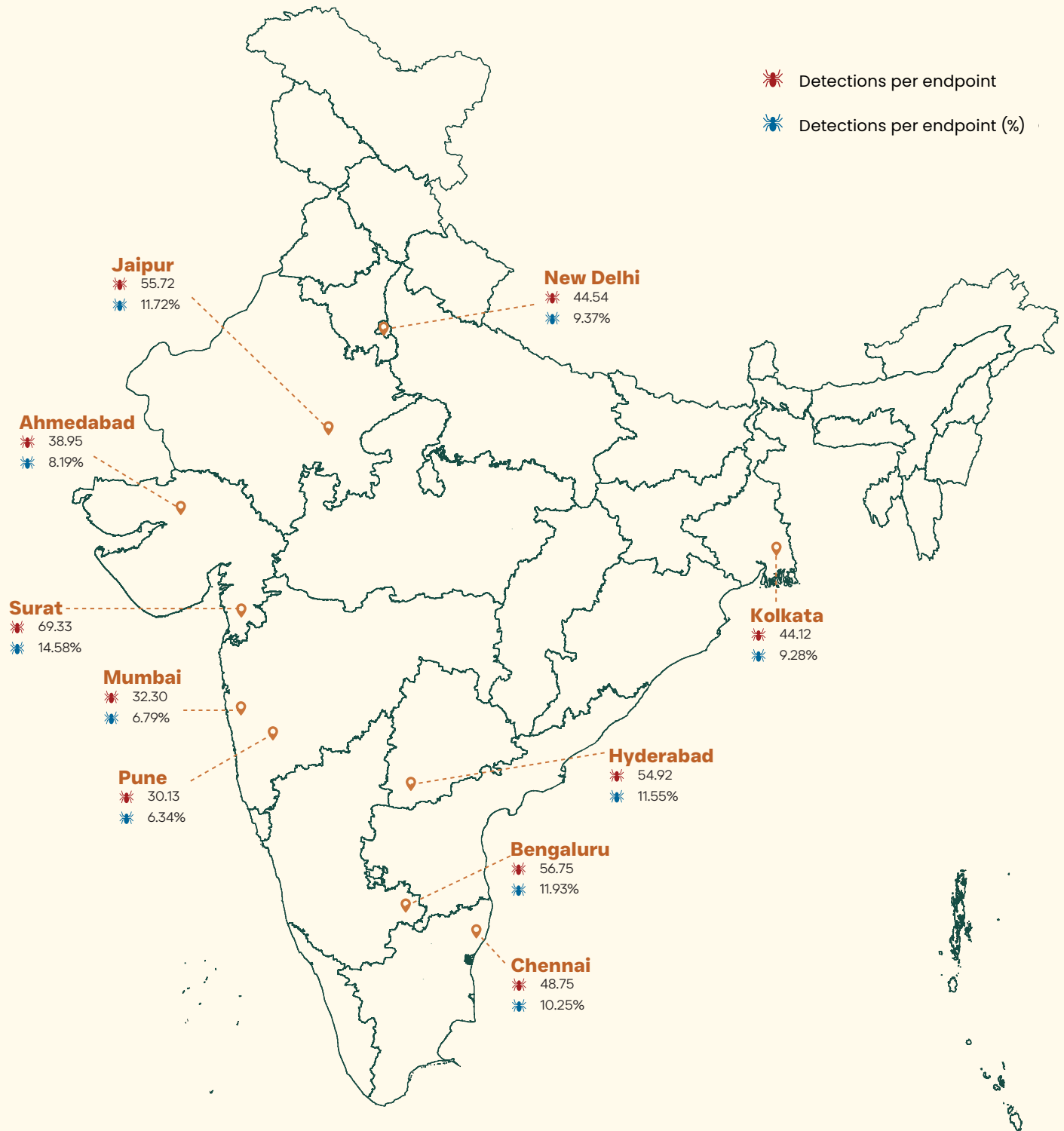
- ▲ Indicates growing digital adoption Infrastructure Impact
- ▲ Higher detections in states with better digital infrastructure
- ▲ Better internet penetration



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

# Top 10 Cities with Highest Malware Detections

34.06% of detections originate from below mentioned cities.



Source: <https://www.surveyofindia.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%)**



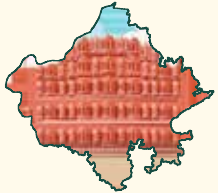
**Hyderabad:**  
**54.93 detections per endpoint (11.55%)**

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%)**

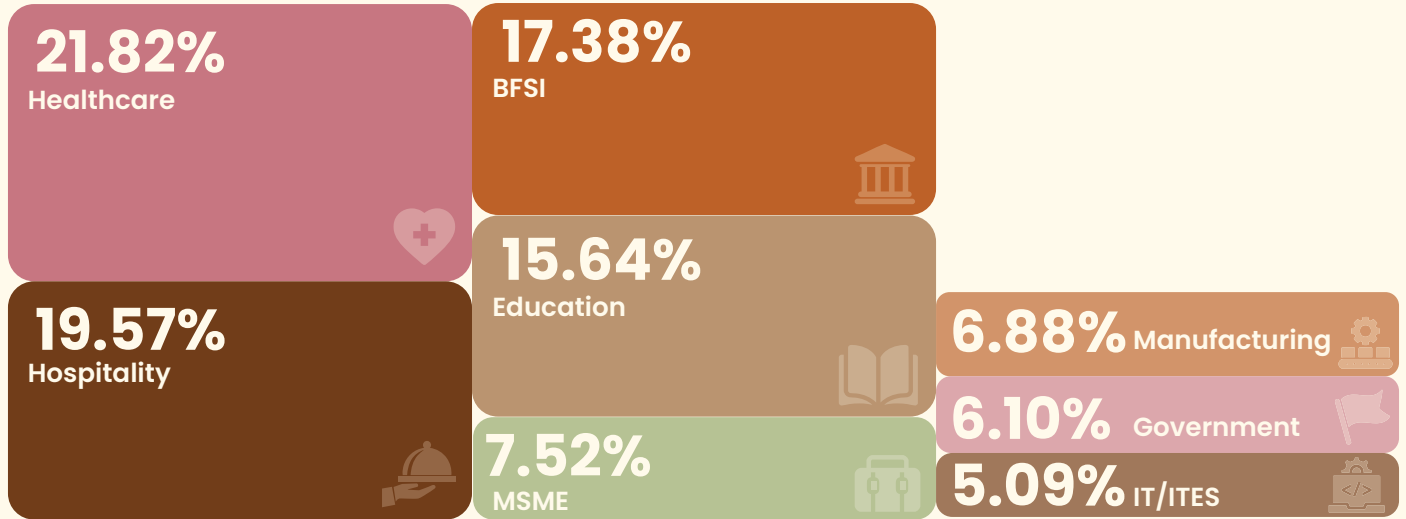


**Pune:**  
**30.14 detections per endpoint (6.34%)**

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

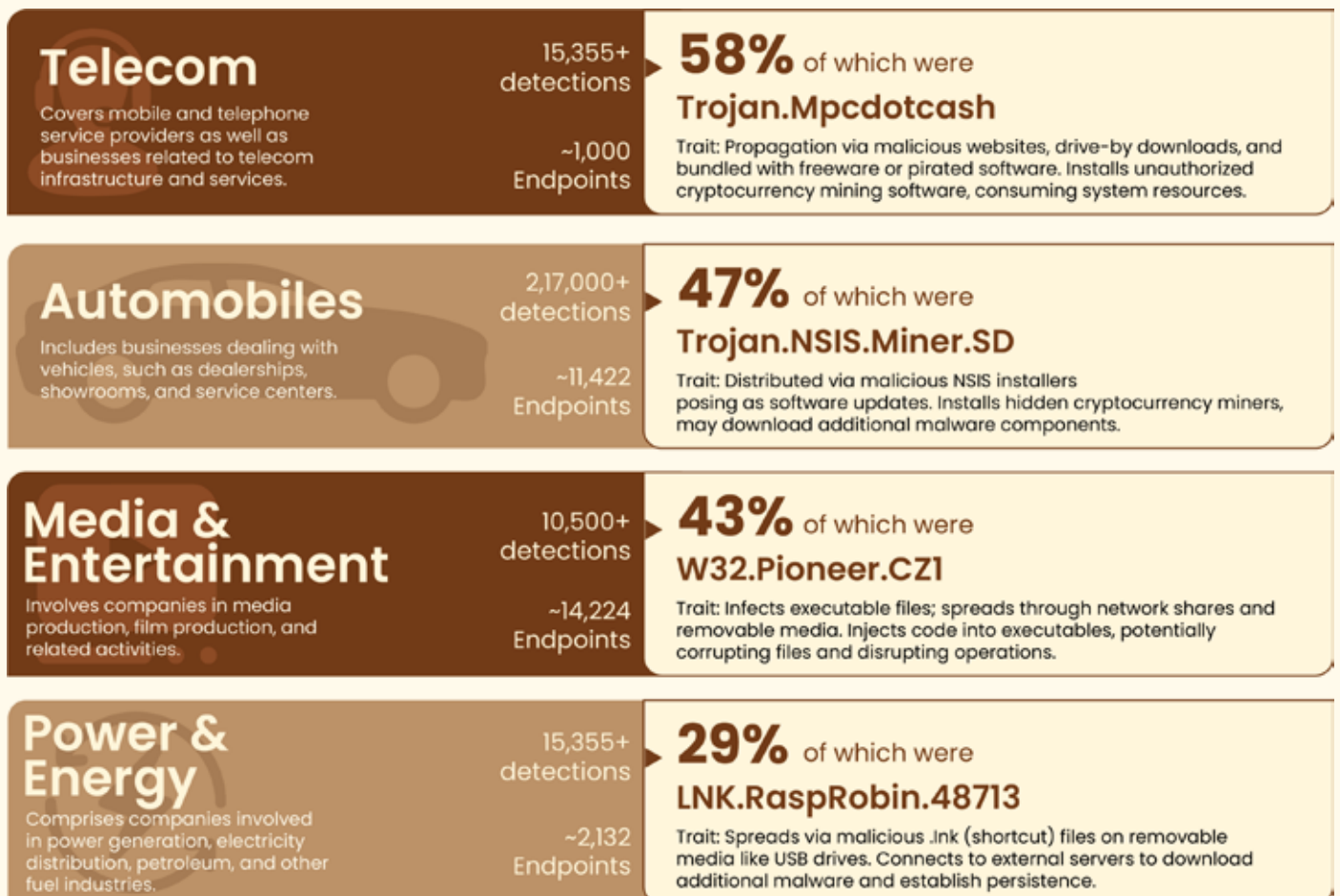
# Industry Insights

## 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.Autolt. Nuqel.AT**

Trait: Exploits instant messaging platforms; spreads through network shares and removable drives. Gathers user credentials, downloads additional malware, written in Autolt 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.

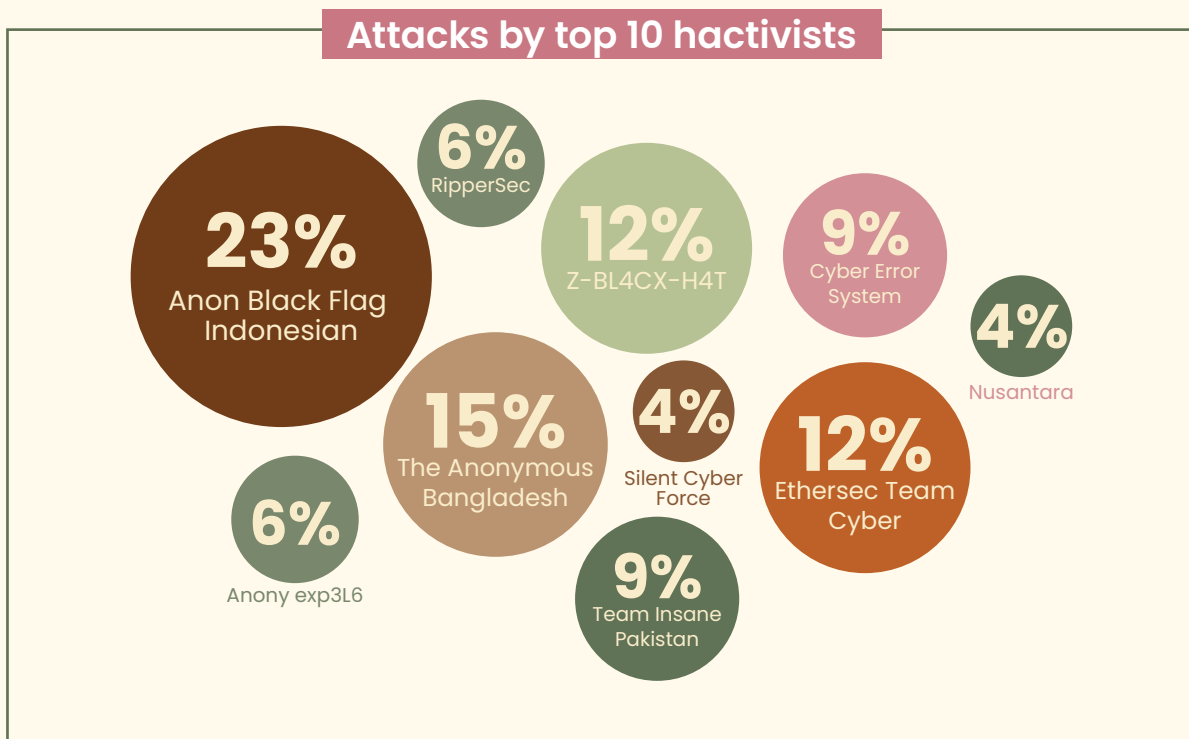


# Key Malware Findings – 2024

## Prominent Hactivist Groups Targeting Indian Cyber Space

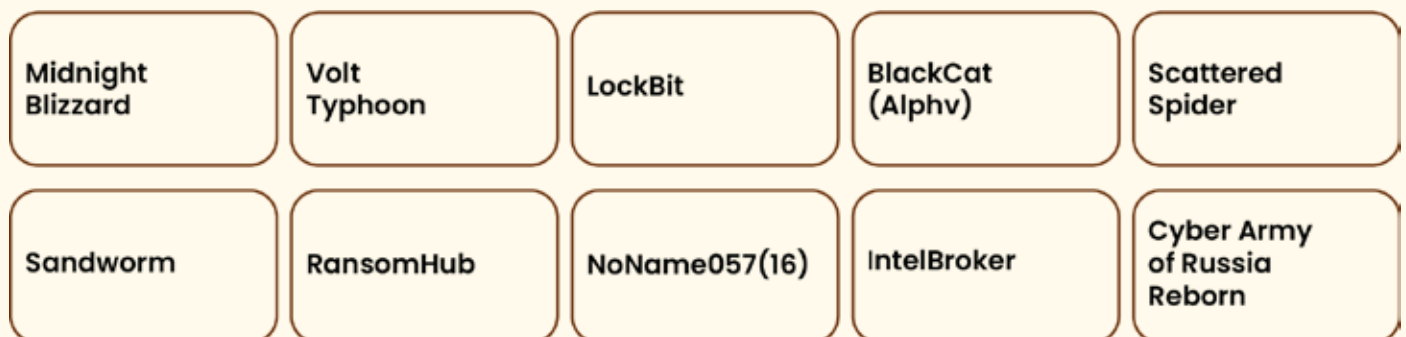
Total Reported Attacks: 5,842

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> (Dell Driver)	<b>appid.sys</b>	<b>RTCore64.sys</b> (MSI Afterburner Driver)	<b>WinRing0.sys</b>
<b>nvlldmkm.sys</b> (NVIDIA Graphics Driver)	<b>gdrv.sys</b> (GIGABYTE Driver)	<b>SynTP.sys</b> (Synaptics Driver)	<b>RTCore64.sys</b> (MSI)	<b>atilk64.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>

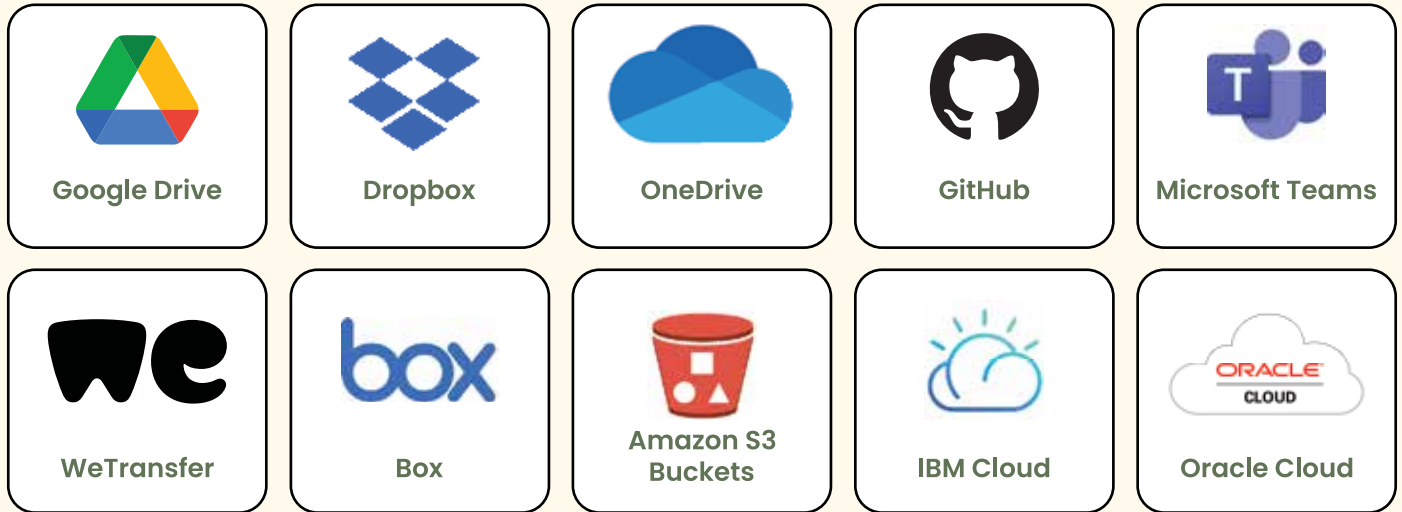
## Top Malicious File Types

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, .xlsm)	 <b>Compressed Files</b> (.zip, .rar)	 <b>HTML Files</b> (.html, .htm)	 <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:



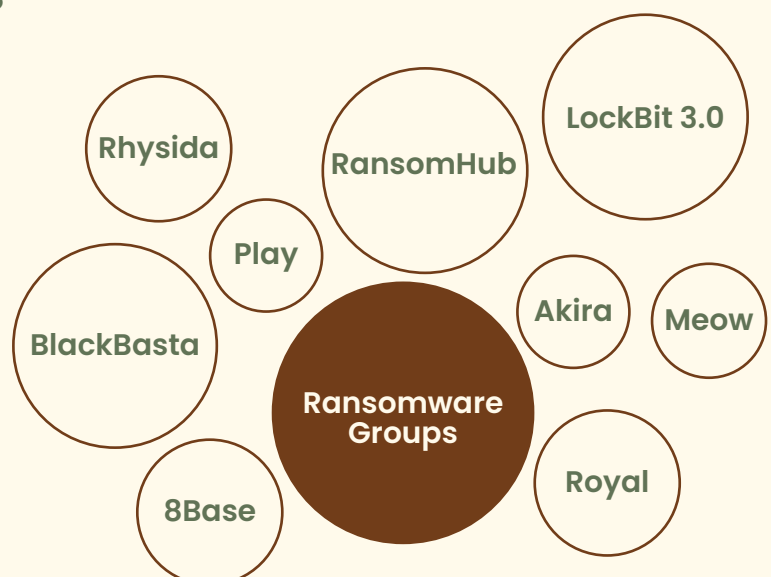
## Top MITRE Techniques Used

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:








# CYBER THREAT PREDICTIONS

# 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.

# Acknowledgement

## Authors

Sangamesh S, Vice President & Head of Seqrite Labs  
Jaswinder Singh, Director - Engineering, Seqrite Labs

## Contributors

DSCI - Data Security Council of India  
Sudhanshu Tripathi, CMO, Quick Heal

## Editors

Jyoti Karlekar

## Designer

Manoj Joshi  
Mukund Shrigadi



Scan Here For  
India Cyber Threat  
Report 2025



Copyright ©2025. All rights reserved. Quick Heal Technologies Limited.

This report has been developed by Quick Heal Technologies Limited ("Seqrite"). The information contained herein has been obtained or derived from sources believed by Seqrite to be reliable. However, Seqrite disclaims all warranties as to the accuracy, completeness, or adequacy of such information. This report is made available on "as-is" basis and we shall bear no liability for errors, omissions, or inadequacies in the information contained herein, or interpretations or reliance thereof.

The information contained 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 and protected by intellectual property legislations. You must 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 written consent from authorized representative of Seqrite.

## 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 fullstack 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/>



### 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

ytv /@seqrite385

in /company/seqrite