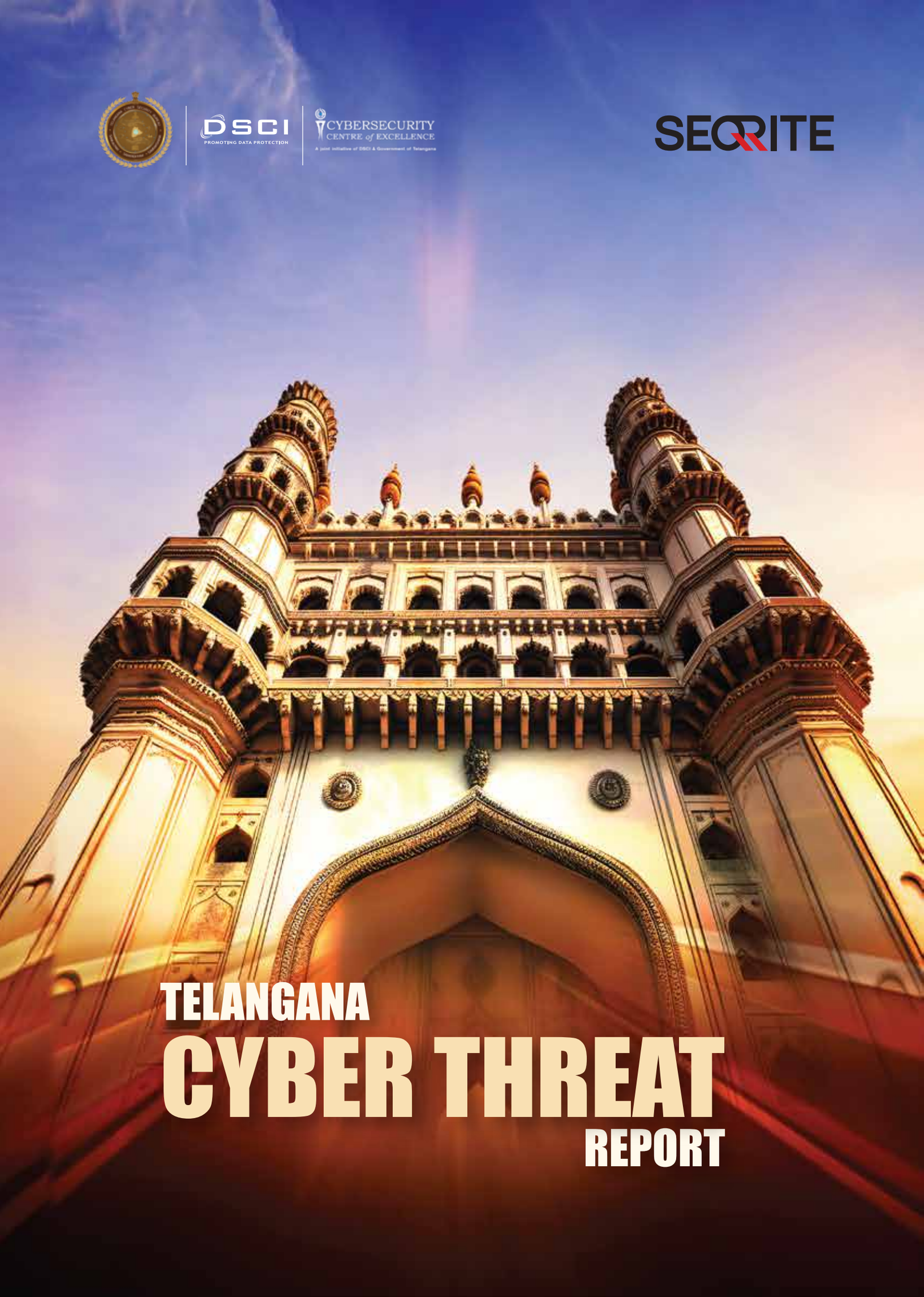


TELANGANA CYBER THREAT REPORT

Foreword – DSCI

VINAYAK GODSE
Chief Executive Officer,
Data Security Council of India

The Data Security Council of India (DSCI), in collaboration with Seqrite, is pleased to present the Telangana Cyber Threat Report 2025—an in-depth examination of the state's evolving cybersecurity landscape. This report underscores our dedication to reinforcing India's digital defenses and provides a strategic framework for confronting present and future threats.

In an era characterized by rapid digital transformation and shifting geopolitical dynamics, cyberattacks have become increasingly sophisticated. Threat actors now deploy AI-driven malware, orchestrate complex phishing campaigns, and exploit advanced persistent techniques to infiltrate vulnerable systems. Telangana's growing digital footprint and thriving innovation ecosystem make it a prime target—demanding not just vigilance, but a decisive, proactive stance on cybersecurity measures.

This report goes beyond superficial threat detection. It delves into the motivations, methods, and tactics of adversaries—providing stakeholders across government, critical infrastructure, enterprises, and law enforcement with data-driven insights. By examining localized trends and real-world case studies, the report equips security professionals with the knowledge and tools vital to counter rapidly evolving cyber risks effectively.

Further, the analysis underscores the pressing need for integrated defense strategies. Telangana's digital landscape, with its dynamic tech community and fast-growing economic sectors, benefits immensely from unified efforts that combine innovative technology and policy support. Strengthening inter-agency coordination, enhancing security protocols, and implementing resilient architectures remain at the forefront of these endeavors.

DSCI remains committed to fostering collaboration and driving excellence in the cybersecurity domain. By uniting resources, expertise, and best practices, we can ensure that Telangana's digital landscape becomes a model of resilience for India's broader digital ecosystem.

Foreword – Quick Heal

DR. SANJAY KATKAR
Joint Managing Director,
Quick Heal Technologies Limited

It is with great pride and a deep sense of responsibility that I present the Telangana Cyber Threat Report 2025. This report provides an in-depth analysis of the rapidly evolving cyber threat landscape in Telangana, leveraging the expertise of Seqrite Labs—India's largest malware analysis facility. With data gathered from nearly 85 lakh endpoints, we offer unparalleled insights into the cybersecurity challenges facing enterprises, government organizations, and individuals in the state. As one of India's leading technology hubs, Telangana has unfortunately become a prime target for cybercriminals. Our findings reveal that Telangana accounts for 2.3% of all malware detections in India, with over 6.25 million malware detections in 2024 alone. Additionally, 17,505 ransomware attacks were recorded in the state, averaging 47 attacks per day. The rising frequency of these threats highlights the growing sophistication of cybercriminals, further underscoring the need for advanced defense mechanisms in the region.

Telangana's rapidly expanding digital economy, coupled with an increase in cybercrime, calls for urgent action. The state's growing exposure to cyber risks is reflected in a significant number of reported cybercrimes, with over 123,000 cases recorded, including identity theft, business and investment fraud, and impersonation. These figures emphasize the widespread nature of fraud and the vulnerability of individuals and organizations alike. With cybercrime becoming increasingly prevalent, the need for comprehensive fraud prevention solutions is clearer than ever. In response to this growing threat, Quick Heal has launched AntiFraud.AI, India's first AI-powered fraud prevention solution, aimed at addressing the surge in financial fraud. This 'Made in India' solution is designed to protect users from the rising tide of digital fraud, offering real-time alerts, scam protection, and proactive fraud prevention to ensure a safer online experience for all.

As the cyber threat landscape continues to evolve, it is imperative that businesses, government organizations, and individuals take action to protect their digital ecosystems. At Seqrite, we are committed to driving innovation, strengthening defenses, and ensuring that organizations stay ahead of emerging threats. I encourage stakeholders across Telangana to utilize the insights in this report to bolster their cybersecurity measures and build a safer, more resilient digital environment for the state and beyond.

From the CEO’s Desk Quick Heal

VISHAL SALVI
Chief Executive Officer,
Quick Heal Technologies Limited

India’s digital landscape is evolving rapidly, with the digital economy projected to contribute 20% of GDP by 2026. However, this rapid growth has also positioned India, and specifically Telangana, as a prime target for cybercriminals. The increasing frequency and complexity of these attacks emphasize the need for a proactive, defense-first approach to cybersecurity.

The Telangana Cyber Threat Report 2025 offers a comprehensive analysis of the cybersecurity challenges facing the state, utilizing insights from Seqrite Labs, India’s largest malware analysis facility. Telangana, especially Hyderabad, has become a hotspot for cybercrime, with the state recording over 6.25 million malware detections and 17,505 ransomware attacks in 2024. These threats span a wide range of sectors, including BFSI, healthcare, and government, with cybercriminals continuously evolving their tactics. The report also highlights the growing role of geopolitical factors in cybercrime, further underscoring the importance of strengthening digital defenses.

At Seqrite, we are dedicated to advancing cybersecurity solutions that empower businesses, government organizations, and individuals to counter these growing threats. Our innovations, such as the Seqrite Malware Analysis Platform (SMAP) and Seqrite Threat Intel, provide enhanced threat visibility and intelligence-driven defense mechanisms, enabling organizations to stay ahead of sophisticated attacks. As the only Indian cybersecurity company to be part of the US Artificial Intelligence Safety Institute Consortium, we continue to contribute to the global AI security narrative while reinforcing India’s cybersecurity resilience.

I encourage organizations across Telangana to utilize the insights in this report to strengthen their cybersecurity strategies and protect themselves from emerging threats, including digital fraud. By investing in proactive security measures and leveraging cutting-edge technology, we can work together to create a safer, more resilient digital environment for Telangana, and India as a whole.

TABLE OF CONTENTS

69

Cyber Threat Predictions

75

Recommendations 2025 & Beyond

79

Telangana Cyber Bureau

EXECUTIVE SUMMARY

Key Highlights

Telangana Accounts for

2.3%

of all Malware detections in the **country in 2024**

Malware detection

62,52,023 malware detections recorded, averaging **17,128** malware attacks per day.

Ransomware detection

17,505 Ransomware detection i.e. average **47** attacks daily

Q1 saw highest detections at **16,82,842** in 2024

Hacktivism on rise

- Telangana Govt portal attacked
- Data leak attack on Deputy CM's site

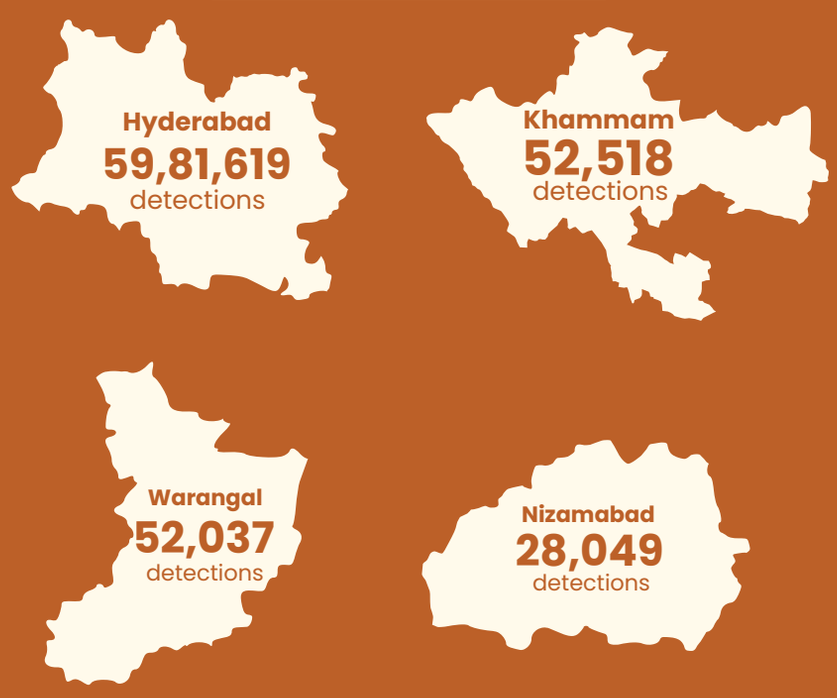
Top targeted industries detections

6.84 M
Professional Services

4.75 M
Education

5.85 M
Manufacturing

Top affected cities



Cyber Fraud Cases:

29,709	25,995	18,647
Identity Theft	**Business & Investment Fraud**	**Impersonation**

The cybersecurity landscape in Telangana has undergone a dramatic transformation throughout 2024, marked by an unprecedented surge in both the volume and sophistication of cyber threats. In the past year alone, Telangana recorded 6,252,023 malware detections and 17,505 ransomware incidents—averaging 47 ransomware attacks per day. These figures not only underscore the relentless nature of cyber threats but also indicate that Telangana accounts for almost 23% of all malware detections in India, highlighting the state's heightened vulnerability amid its rapid digital evolution.

The threat environment in Telangana is further complicated by the diverse range of attacks targeting critical sectors. Industries such as government, BFSI, healthcare, education, manufacturing, and IT/ITES have been particularly hit hard, with high-impact malware variants—ranging from advanced Trojans to disruptive worms—compromising sensitive systems and data. This report details that the attack patterns vary significantly across sectors; for instance, government infrastructures and public enterprises have seen a surge in targeted assaults, while the healthcare and educational institutions have been subjected to ransomware and data breach incidents that severely disrupt operational continuity. Notable recent cyberattacks, such as the breach on prestigious medical college and the ransomware on Asia's Largest Educational Conglomerates in Hyderabad, serve as stark reminders of the potential impact on critical services and the urgent need for enhanced defensive measures.

In addition to these malware and ransomware incidents, Telangana has witnessed a concerning rise in cybercrime, with 1,23,465 reported cases spanning identity theft, business and investment fraud, impersonation, UPI fraud, and other forms of digital fraud. These incidents, combined with the expanding attack surface due to increased cloud adoption and emerging technologies, underscore the critical need for comprehensive and adaptive cybersecurity strategies.

Furthermore, the evolving threat landscape is increasingly influenced by sophisticated tactics, including the use of generative AI for adaptive malware and highly targeted phishing campaigns. Hacktivist groups leveraging platforms such as Telegram have also amplified the risk by executing coordinated data leaks and defacement attacks on government portals and public institutions. These multi-faceted challenges call for a holistic approach to cybersecurity that goes beyond traditional defense mechanisms.

By presenting these critical insights, the Telangana Cyber Threat Report 2025 aims to guide stakeholders in developing robust, future-ready security strategies. As Telangana continues its digital transformation, it is imperative for both public and private sectors to invest in advanced cybersecurity solutions and cultivate a culture of proactive defense, ensuring a resilient and secure digital ecosystem for the future.

TELANGANA THREAT REPORT 2025

Telangana, particularly Hyderabad, is a hotbed for investment in 2024-2025.

Here are some key areas to watch:

Real Estate

- **Residential:** With a growing IT sector and influx of professionals, demand for housing is high. Areas like Kokapet, Narsingi, Tellapur, and Gachibowli are popular for their connectivity and amenities. Affordable housing projects in Uppal, LB Nagar, and Bachupally also offer opportunities.
- **Commercial:** IT parks and SEZs continue to attract major companies, driving demand for office spaces. Gachibowli, Hitech City, and Manikonda are prime locations.
- **Infrastructure Projects:** The expansion of the Regional Ring Road (RRR), Hyderabad Metro, and the development of Pharma City are boosting real estate in surrounding areas.

IT and IT-enabled Services

- Hyderabad is a major IT hub, attracting global giants like Apple, Amazon, and Microsoft. Investment in software devel opment, cloud computing, cybersecurity, and data analytics is expected to continue.
- The government is actively promoting the IT sector with initiatives like new IT parks and SEZs.

Life Sciences and Pharmaceuticals

- Telangana is a leader in the life sciences and pharmaceutical industry. The Pharma City project is expected to be a major growth driver, creating employment and investment opportunities.
- Research and development, manufacturing, and healthcare services are key areas for investment.

Biotechnology

- Telangana has a thriving biotechnology sector, with a focus on agriculture, healthcare, and industrial applications.
- Investment in research, development, and commercialization of biotech products is expected to grow.

Aerospace and Defense

- Telangana is emerging as a hub for aerospace and defense industries, with companies like Boeing and Lockheed Martin having a presence in the state.
- Investment in manufacturing, research, and development in this sector is expected to increase.

Renewable Energy

- The government is promoting renewable energy sources like solar and wind power.
- Investment in renewable energy projects and manufacturing of related equipment is expected to grow.

Infrastructure

- The government is investing heavily in infrastructure development, including roads, metro, and irrigation projects.
- This creates opportunities for construction companies, as well as businesses in related sectors.

Tourism

- Telangana has a rich cultural heritage and diverse tourist attractions.
- Investment in tourism infrastructure, including hotels, resorts, and transportation, is expected to increase.

E-commerce and Logistics

- The growth of e-commerce is driving demand for logistics and warehousing facilities.
- Investment in logistics parks, e-commerce platforms, and last-mile delivery solutions is expected to grow.

Food Processing

- Telangana has a strong agricultural base, providing opportunities for food processing industries.
- Investment in food processing, packaging, and cold storage facilities is expected to increase.

Factors Driving Investment:

- **Pro-business policies:** The Telangana government has implemented investor-friendly policies, such as TS-iPASS, which provides single-window clearances for projects.
- **Infrastructure development:** The state government is investing heavily in infrastructure, improving connectivity and creating a conducive environment for businesses.
- **Skilled workforce:** Telangana has a large pool of skilled professionals, particularly in the IT and pharmaceutical sectors.
- **Strategic location:** Telangana is strategically located, with good connectivity to major cities in India.

With increased investment in these sectors in Telangana, it's crucial to be aware of the potential threats.

Here's a breakdown of the associated cyber risks for each industry:

Real Estate

- **Data Breaches:** Real estate companies hold vast amounts of sensitive data (personal details, financial information, transaction records). A breach can lead to identity theft, fraud, and legal consequences.
- **Phishing and Social Engineering:** Attackers may impersonate clients, agents, or other parties to trick employees into revealing information or transferring funds.
- **Wire Transfer Fraud:** Hackers can intercept emails and modify wire transfer instructions, leading to significant financial losses.
- **Ransomware Attacks:** Cybercriminals encrypt company data and demand a ransom for its release, disrupting operations and potentially causing permanent data loss.
- **IoT Vulnerabilities:** Smart devices in properties (locks, cameras, thermostats) can be entry points for hackers if not properly secured.

IT and IT-enabled Services

- **Data Breaches:** IT companies handle massive amounts of data, making them prime targets for hackers seeking valuable information.
- **Software Vulnerabilities:** Flaws in software can be exploited by attackers to gain access to systems and data.
- **Cloud Security Risks:** Cloud computing introduces new security challenges, such as data breaches, unauthorized access, and denial-of-service attacks.
- **Insider Threats:** Malicious or negligent employees can compromise security by stealing data, installing malware, or granting unauthorized access.
- **Cyber Espionage:** Competitors or foreign governments may attempt to steal intellectual property or trade secrets.

Life Sciences and Pharmaceuticals

- **Data Breaches:** Pharmaceutical companies hold valuable research data, patient information, and intellectual property, making them attractive targets for hackers.
- **Supply Chain Attacks:** Cybercriminals may target suppliers or partners to gain access to sensitive data or disrupt operations.
- **Ransomware Attacks:** Disrupting research or manufacturing processes can be highly damaging, making pharmaceutical companies more likely to pay a ransom.
- **Counterfeit Drugs:** Cyberattacks can be used to facilitate the production and distribution of counterfeit drugs.

Biotechnology

- **Data Breaches:** Biotech companies hold sensitive research data, genetic information, and intellectual property.
- **Intellectual Property Theft:** Competitors or foreign entities may attempt to steal research findings or proprietary technologies.
- **Biohacking:** Cybercriminals could potentially manipulate biological data or systems for malicious purposes.

Aerospace and Defense

- **Cyber Espionage:** Foreign governments or competitors may target aerospace and defense companies to steal classified information or technology.
- **Sabotage:** Cyberattacks could be used to disrupt operations, damage equipment, or compromise critical systems.
- **Supply Chain Attacks:** Hackers may target suppliers or subcontractors to gain access to sensitive information or disrupt the supply chain.

Renewable Energy

- **SCADA System Attacks:** Supervisory control and data acquisition (SCADA) systems used to manage energy grids are vulnerable to cyberattacks, potentially causing widespread disruption.
- **Data Breaches:** Renewable energy companies collect data on energy consumption and grid operations, which could be targeted by hackers.

Infrastructure

- **SCADA System Attacks:** Similar to renewable energy, infrastructure systems (transportation, utilities) rely on SCADA systems that are vulnerable to cyberattacks.
- **Ransomware Attacks:** Disrupting critical infrastructure can have severe consequences, making organizations more likely to pay a ransom.

Tourism

- **Data Breaches:** Hotels, airlines, and travel agencies store sensitive customer data, making them potential targets for hackers.
- **Phishing and Social Engineering:** Tourists may be targeted by phishing scams or social engineering tactics to steal personal information or financial credentials.

E-commerce and Logistics

- **Data Breaches:** E-commerce platforms handle large volumes of customer data, including payment information, making them attractive targets for cybercriminals.
- **Phishing and Social Engineering:** Customers may be targeted by phishing scams to steal login credentials or payment information.
- **Supply Chain Attacks:** Hackers may target logistics companies to disrupt deliveries, steal goods, or gain access to sensitive data.

Food Processing

- **SCADA System Attacks:** Food processing facilities often use SCADA systems that can be vulnerable to cyberattacks, potentially disrupting production or causing contamination.
- **Supply Chain Attacks:** Hackers may target suppliers or distributors to disrupt the food supply chain or compromise product safety.

Malware Detections

62,52,023
Malware detected in Telangana in 2024

17,505
Ransomware detected for Telangana in last year.

Daily average
47 Ransomware attacks

Malware Detection Statistics 2024

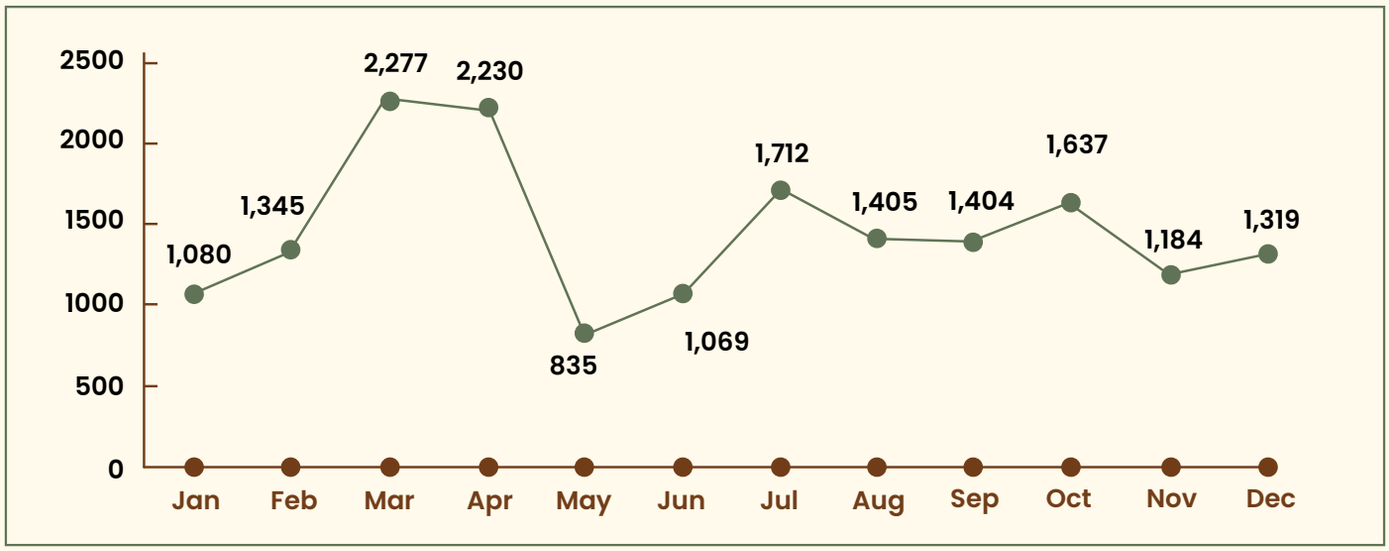
Detection	Detection Count	Per Day
Malware	62,52,023	17,128
Ransomware	17,505	47

Telangana Vs National Statistics

Detection Name	National Detections	Telangana Detections
Malware	26,66,74,935	62,52,023
Ransomware	1,98,58,035	17,505

Inference:
Telangana accounts for 2.3% of all malware detections in the country and 0.08% of ransomware detections. This indicates that while Telangana is not the most targeted state, it still faces significant cybersecurity threats, particularly in malware attacks.

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.

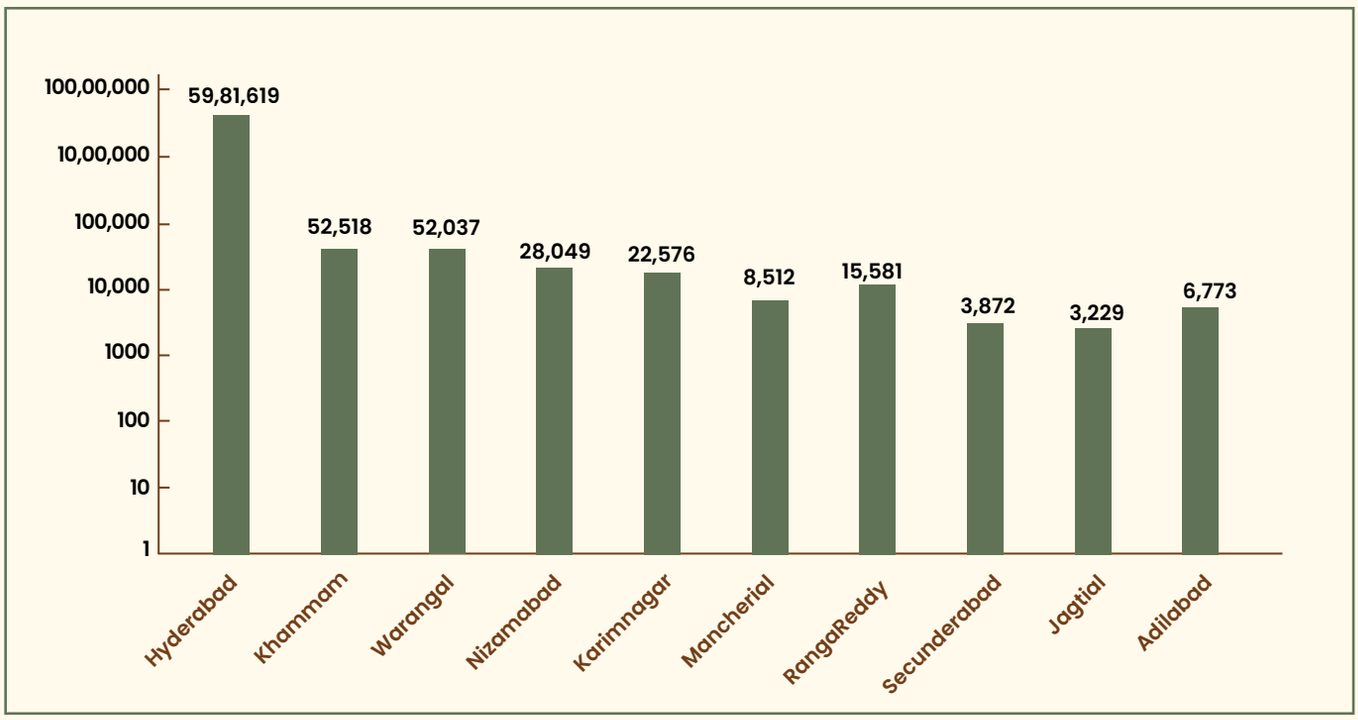
March-April 2024: A spike in ransomware attacks coincided with election-related misinformation campaigns, targeting government institutions and voter data.

July 2024: The highest number of attacks were recorded, driven by mass ransomware campaigns targeting IT and BFSI sectors.

September-October 2024: Festive season scams and targeting of students and job seekers led to a moderate increase in ransomware detections.

November-December 2024: A decline in attacks was observed as cybercriminals shifted focus to future planning, and organizations improved their security posture.

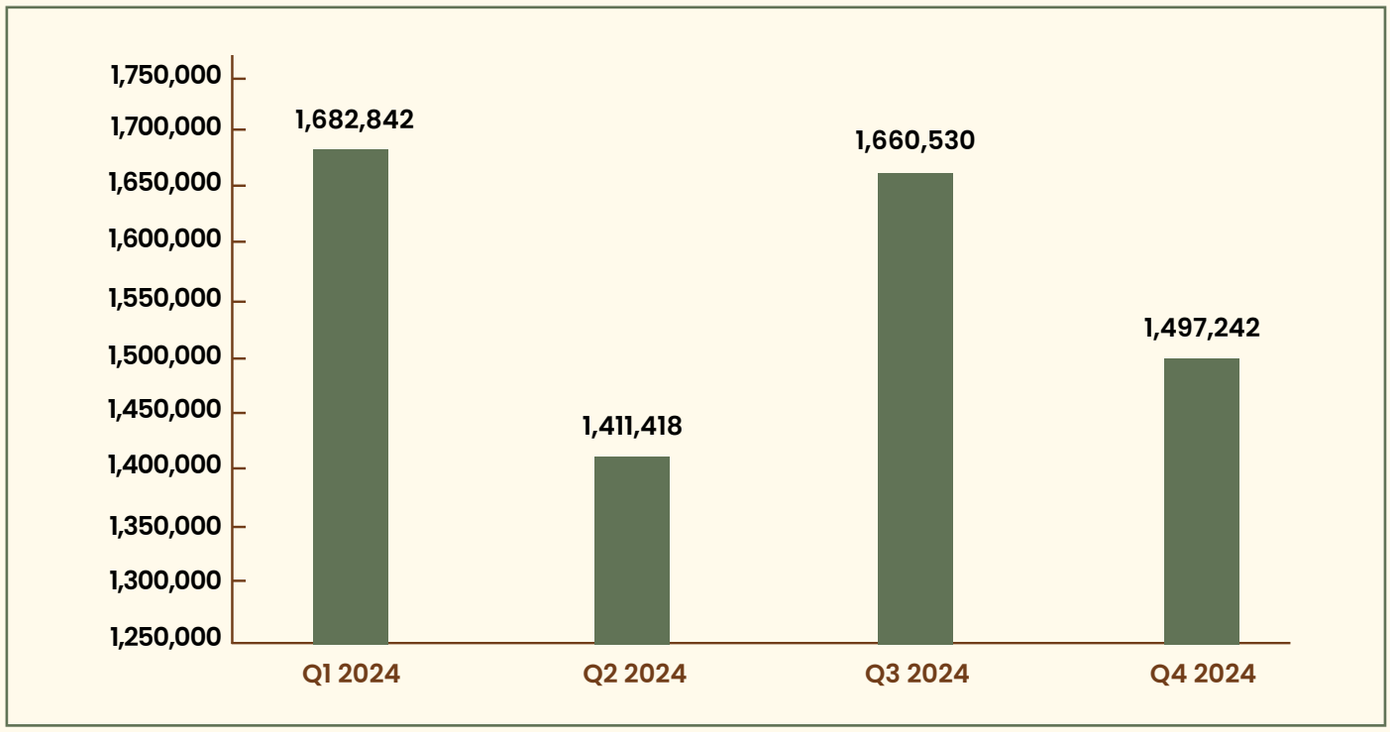
Top 10 Affected Cities



Telangana in top 10 most attacked states in India

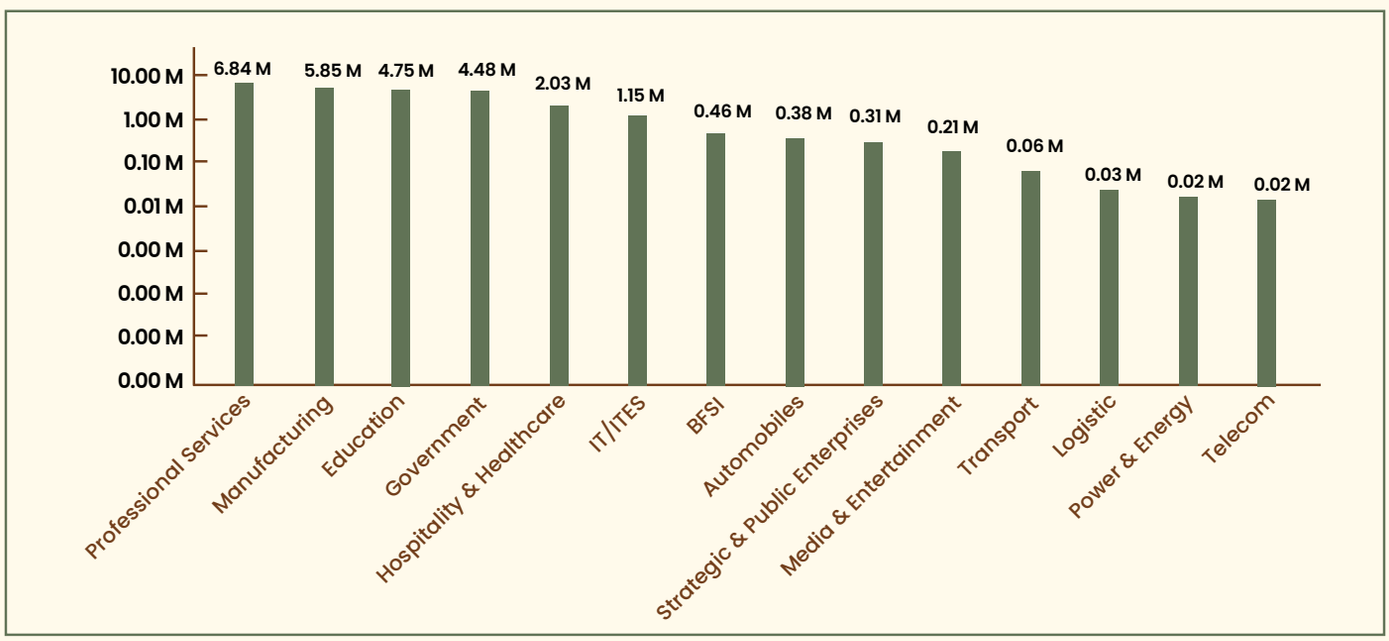
Telangana ranks amongst the top 10 most attacked states in India, with 6.25 million malware detections.

Quarter wise Detection Hits



The chart highlights a significant increase in detection hits in Q3 2024, reaching 2.1 million, followed by a slight decline in Q4. This trend suggests a surge in detections mid-year, driven by ransomware campaigns and phishing attacks targeting critical sectors.

Detection Statistics: Industry-wise



The chart illustrates industry-wise detection statistics, with Professional Services experiencing the highest detection hits followed by Manufacturing and Education.

Attack on Telangana's Top Industries

Power & Energy
- Detection Name: **LNK.RaspRobin.48713**
- Count of Top Malware: **15,355**

BFSI
- Detection Name: **Trojan.Convagent**
- Attacks: **27,837**

Telecom
- Detection Name: **Trojan.Mpcdotcash**
- Attacks: **8,641**

Transport
- Detection Name: **Worm.AutoIt.Nuqel.AT**
- Attacks: **5,118**

Government
- Detection Name: **Remoteadmin.Remoteexec**
- Count of Top Malware: **3,62,255**

Strategic & Public Enterprises
- Detection Name: **Trojan.Shadowbrokers**
- Attacks: **31,009**

Automobiles
- Detection Name: **Trojan.NSIS.Miner.SD**
- Attacks: **1,90,625**

Education
- Detection Name: **W32.Pioneer.CZ1**
- Attacks: **5,51,496**

Hospitality & Healthcare
- Detection Name: **Trojan.Shadowbrokers**
- Count of Top Malware: **1,28,254**

IT/ITES
- Detection Name: **PIF.StucksNet.A**
- Attacks: **1,15,552**

Manufacturing
- Detection Name: **Nsis.Bitmin**
- Attacks: **8,05,399**

Media & Entertainment
- Detection Name: **W32.Pioneer.CZ1**
- Attacks: **91,677**

Professional Services
- Detection Name: **Nsis.Bitmin**
- Attacks: **6,27,880**

Top Detections: Industry-wise

Manufacturing
Detection Name
Trojan.CoinMiner.S30910494
Attacks
2,481

Hospitality & Healthcare
Detection Name
Trojan.Shadowbrokers
Attacks
1,921

Professional Services
Detection Name
Trojan.InjectPyinc.PB6
Attacks
1,239

IT/ITES
Detection Name
Worm.Autoit.Sohanad.S
Attacks
434

Government
Detection Name
Trojan.Mauvaise.SL1
Attacks
147

General Cybersecurity Best Practices:

- **Strong Passwords and Multi-Factor Authentication:**
  Use strong, unique passwords and enable multi-factor authentication whenever possible.
- **Regular Software Updates:**
  Keep software and systems up to date with the latest security patches.
- **Firewall and Antivirus Software:**
  Use firewalls and antivirus software to protect against malware and other threats.
- **Employee Training:**
  Educate employees about cybersecurity risks and best practices.
- **Data Encryption:**
  Encrypt sensitive data both in transit and at rest.
- **Incident Response Plan:**
  Develop a plan to respond to cyberattacks and data breaches.

FEATURED STORIES 2025

Prominent Recent Cyber Attacks

Cyberattack on a prestigious medical college

Summary

The cyberattack on the medical colleges targeted both their Karnataka and Hyderabad campuses, compromising student records, financial transactions, and faculty payroll systems. The attackers gained initial access through phishing emails sent to faculty and administrative staff, tricking them into revealing credentials or executing malicious attachments. Using privilege escalation techniques, they moved laterally across the network, accessing sensitive databases.

The breach led to:

- Unauthorized access to personal and academic records of students and staff.
- Disruptions in administrative functions, including payroll and admissions.
- Potential legal and reputational consequences for the institution.

The attack was detected when anomalous data traffic and unauthorized access logs were identified. In response, the college isolated compromised systems, reset credentials, implemented MFA, and strengthened cybersecurity policies.

Stage 1: Initial Reconnaissance & Target Selection

- **Attackers first conducted reconnaissance** on the Medical Colleges, gathering intelligence about the institution's network infrastructure, administrative systems, and key personnel.
- **Possible reconnaissance methods:**
  1. Open-source intelligence (OSINT): Attackers scanned publicly available data on social media, the college's website, and forums to identify faculty members, IT staff, and system administrators.

2. Dark web research: If any previous breaches exposed staff email credentials, attackers might have leveraged them to access systems.
3. Automated scanning tools: Attackers may have used tools like Shodan or Nmap to scan for exposed servers, VPNs, or outdated software that could be exploited.

Stage 2: Initial Access – Phishing & Credential Theft

- **The attackers likely used a phishing campaign to gain an initial foothold.**
- **Emails were sent to faculty members, IT administrators, and financial department employees disguised as:**
  1. Official notices from university management or government education boards requesting login credentials.
  2. Fake security alerts prompting users to reset their passwords.
  3. Malicious attachments disguised as academic or finance-related documents.
- **When recipients opened the attachments or clicked on phishing links, malware (such as a keylogger or remote access trojan) was installed.**

Stage 3: Privilege Escalation & Lateral Movement

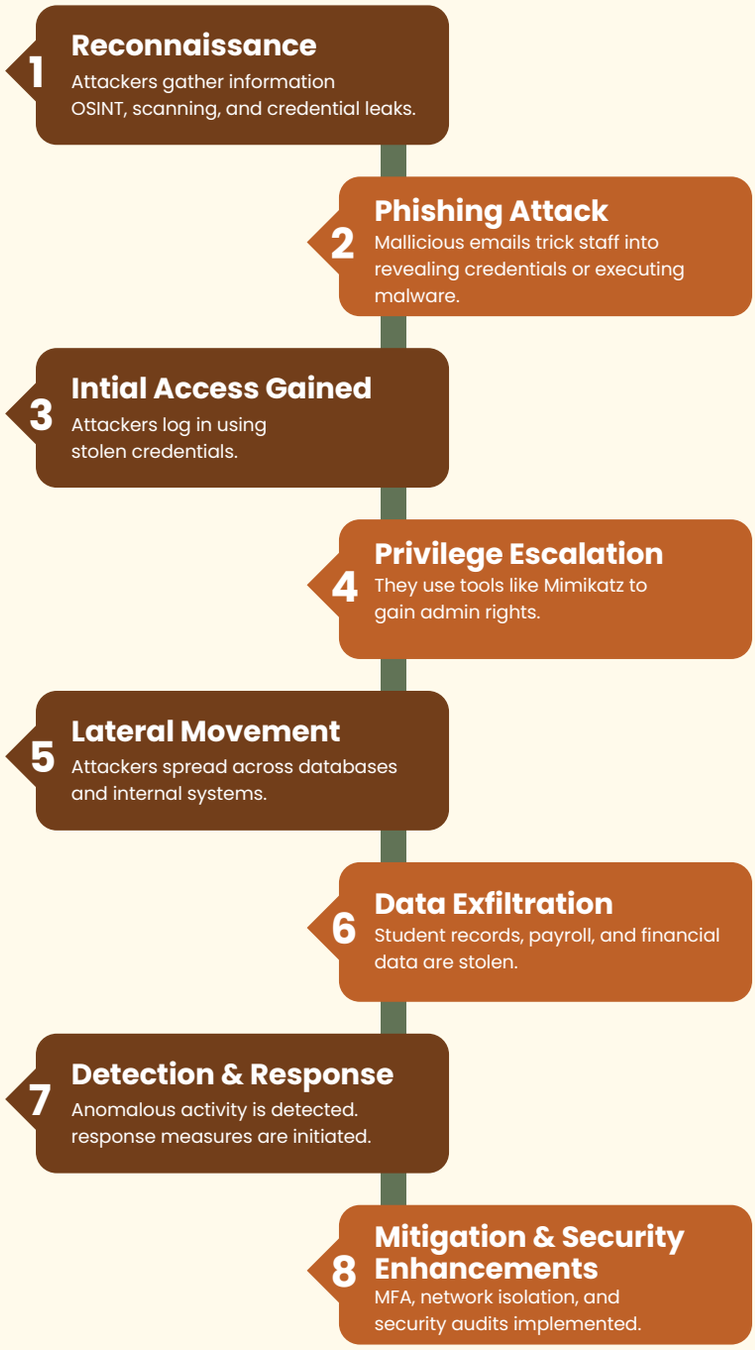
- **After gaining initial access, the attackers escalated privileges using credential harvesting techniques:**
  1. Extracting saved passwords from browsers using tools like Mimikatz.
  2. Exploiting default or weak passwords on internal applications.
  3. Using Pass-the-Hash attacks to move across systems without needing cleartext passwords
- **Once the attackers obtained administrative credentials, they moved laterally across the college's internal network, accessing:**
  1. Student and staff databases (containing personal information, academic records, and financial transactions).
  2. ERP (Enterprise Resource Planning) system used for student admissions and payroll.
  3. Email servers to spread the attack further.

Stage 4: Data Exfiltration & Impact

- **Sensitive information was exfiltrated, possibly to a remote server controlled by the attackers. The stolen data included:**
    1. Student personal details (names, phone numbers, email IDs, addresses).
    2. Financial transactions (tuition fees, scholarship details).
    3. Faculty payroll records (salary details, tax information).
- **The attack disrupted multiple administrative operations, leading to:**
    1. Delays in student admissions and examinations.
    2. Issues in payroll processing for faculty members.
    3. Potential reputational damage and loss of trust among students and staff.

Stage 5: Post Attack

- **The IT department noticed unusual access logs and detected large amounts of outgoing data traffic to unknown IP addresses.**
- **Immediate response measures taken:**
    1. Isolated compromised systems to prevent further data loss.
    2. Reset credentials and forced logouts of all administrative accounts.
    3. Notified affected students and staff to monitor for potential identity theft risks.
    4. Collaborated with cybersecurity agencies to analyze attack patterns and strengthen firewall protections.
- **Post-attack security enhancements:**
    1. Multi-Factor Authentication (MFA) implemented for all administrative access.
    2. Regular vulnerability assessments conducted.
    3. Cybersecurity awareness training provided to faculty and staff.



Conclusion

This attack underscores the importance of cybersecurity awareness in educational institutions, as attackers exploit weak security measures to access sensitive data. Phishing remains the primary attack vector, making employee training and email security solutions essential.

To prevent future incidents, institutions must:

- Implement strong access controls, including multi-factor authentication (MFA).
- Regularly audit security vulnerabilities in IT infrastructure.
- Strengthen endpoint detection and monitoring mechanisms to detect intrusions early.

Ransomware Attack on one of Asia's Largest Educational Conglomerates

Summary

The ransomware attack on one of Asia's largest educational conglomerates targeted its hospitals and educational services, disrupting patient care and administrative operations. The attackers likely gained access through phishing emails or RDP vulnerabilities, allowing them to install malware and deploy ransomware across critical systems.

The attack encrypted electronic medical records (EMR), billing systems, and student data, leaving hospital staff unable to access vital patient information. A ransom was demanded in cryptocurrency, but the conglomerates group refused to pay, opting instead to restore systems from secure backups.

The organization responded by isolating infected systems, deploying cybersecurity experts for forensic analysis, and implementing stronger security measures such as network segmentation, phishing awareness training, and continuous monitoring.

Stage 1: Initial Reconnaissance & Exploitation

- **Attackers targeted the conglomerates hospitals and educational services, aiming to disrupt critical operations by deploying ransomware.**
- **Possible reconnaissance tactics used by attackers:**
  1. Scanning hospital IT infrastructure for exposed Remote Desktop Protocol (RDP) ports.
  2. Searching employee email credentials from previous breaches.
  3. Identifying third-party vendors with weak security who might have access to hospital systems.

Stage 2: Gaining Initial Access – Phishing & Exploit Abuse

- **Attackers likely launched a spear-phishing attack targeting hospital administrative staff and IT teams.**
- **Phishing email tactics included:**
  1. Fake emails from healthcare regulatory bodies requiring urgent login verification.
  2. Malicious attachments disguised as patient reports or billing invoices.
- **If employees clicked the malicious link or downloaded the file, malware was installed.**

Stage 3: Deployment Of Ransomware

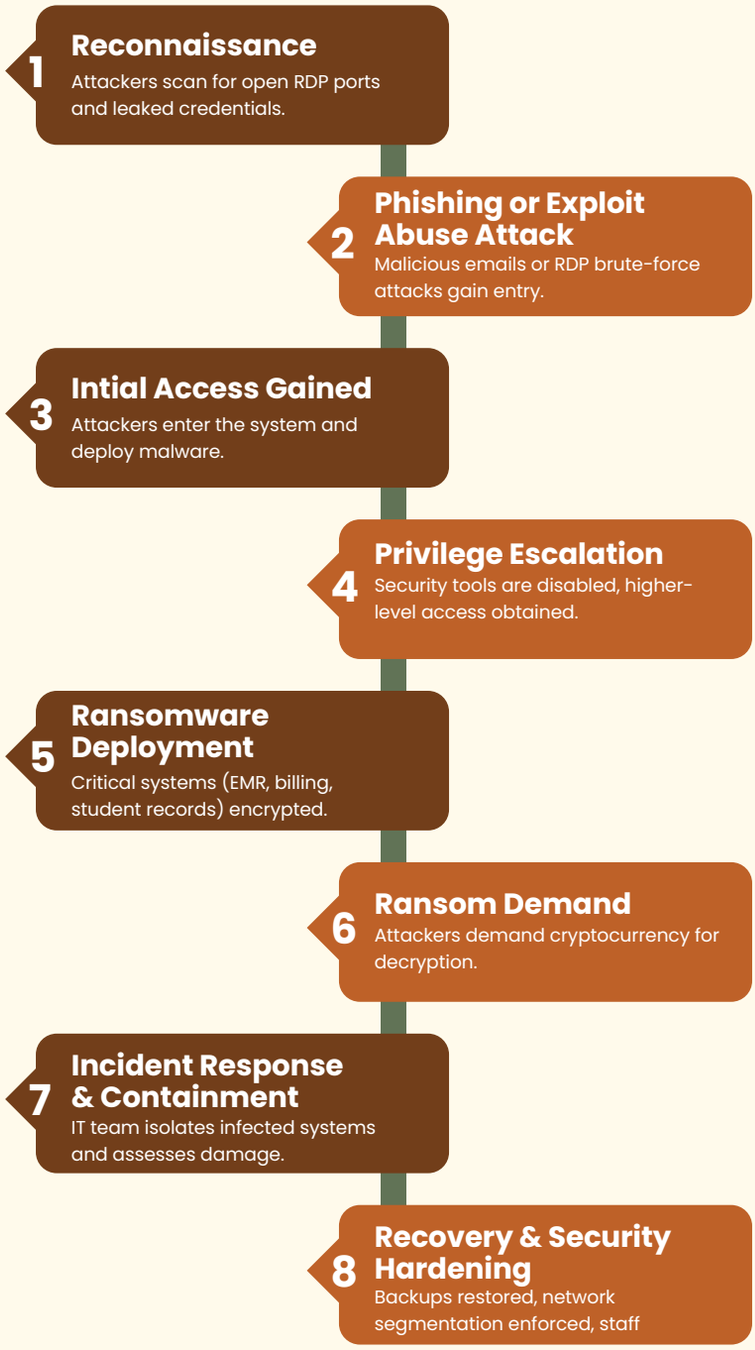
- **Once inside, attackers used Cobalt Strike or Mimikatz to escalate privileges and disable endpoint security tools.**
- **The ransomware payload was deployed across multiple servers, affecting:**
  1. Electronic Medical Records (EMR) systems, blocking access to patient histories and prescriptions.
  2. Hospital billing and finance systems, preventing processing of invoices and insurance claims.
  3. Educational service records, impacting administrative operations.

Stage 4: Encryption & Ransom Demand

- **The ransomware encrypted critical files using AES-256 encryption, making them inaccessible.**
- **A ransom note was displayed on infected systems, demanding cryptocurrency payment (Bitcoin or Monero) in exchange for the decryption key.**
- **Major disruptions faced:**
  1. Hospitals could not access patient records, affecting emergency and critical care services.
  2. Doctors and staff had to rely on handwritten notes, leading to delays in patient care.
  3. Educational services, including online classes and student databases, were temporarily inaccessible.

Stage 5: Incident Response & Recovery

- **The conglomerates IT team disconnected infected systems from the network to contain the spread.**
- **Recovery efforts included:**
  1. Restoring systems from secure backups instead of paying the ransom.
  2. Deploying advanced threat-hunting tools to remove residual malware.
  3. Implementing network segmentation to prevent future attacks.
- **Long Term Security Improvements:**
  1. Restricted remote access to hospital networks.
  2. Phishing awareness programs for staff.
  3. Continuous monitoring of IT infrastructure with real-time alert mechanisms.



Conclusion

This attack highlights the severe impact of ransomware on healthcare institutions, where system downtime can directly affect patient safety. Hospitals and educational institutions must:

- Secure remote access by closing unnecessary RDP ports and enforcing multi-factor authentication (MFA).
- Regularly back up critical data and store it securely offline to enable rapid recovery.
- Train staff on phishing threats and social engineering techniques to prevent initial access.

Key Takeaways

- Educational & healthcare institutions are prime cyberattack targets – Hackers exploit weak security measures in these sectors.
- Phishing remains the most effective attack vector – Employee awareness and email security solutions are crucial.
- Strong access controls and network segmentation are essential – Limiting access to critical systems prevents large-scale disruptions.
- Incident response plans must be in place – Rapid detection and containment reduce damage.
- Regular security assessments and audits are necessary – Identifying vulnerabilities before attackers do is key to cyber resilience.

Hacktivist Attack Report: Telegram-Based Operations

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

- On February 19, 2024, the Telegram Threat Actor (TA) group **"BLACK_CODE"** leaked the credentials of the Telangana Government Portal (data.telangana.gov.in). Login Credentials of Registered Users and other Sensitive Authentication details were exposed online, putting the organization at risk of further breaches and unauthorized access.

- On February 21, 2024, the Telegram Threat Actor (TA) group **"Nusantara"** leaked the credentials of the SC/ST Commission of Telangana Government Portal (https://scstcommission.telangana.gov.in/). Login Credentials of Registered Users and other Sensitive Authentication details were exposed online, putting the organization at risk of further breaches and unauthorized access.

- On March 02, 2024, the Telegram Threat Actor (TA) group **"Team insane Pakistan"** carried out a data leak on Deputy Chief Minister of Telangana - Mallu Bhatti Vikramarka's site. Sensitive internal documents, and other data /records were exposed to the public, rising serious concerns about data privacy and security.

- On March 06, 2024, the Telegram Threat Actor (TA) group **"Z-BL4CX-H4T"** leaked the credentials of the Telangana Government's Official Portal (https://www.telangana.gov.in/). Login Credentials of Registered Users and other Sensitive Authentication details were exposed online, putting the organization at risk of further breaches and unauthorized access.

- On March 16, 2024, the Telegram Threat Actor (TA) group **"GARUDA SECURITY"** executed a defacement attack on the Jawaharlal Nehru Architecture and Fine Arts University | Hyderabad (https://www.jnafau.ac.in/the-fucking-hacked-by-garuda-security/). The attacker altered the organization's website, replacing it with malicious content that tarnished the University's public image.

- On March 26, 2024, the Telegram Threat Actor (TA) group **"Bangladesh dark net hacker boys"** launched a DDoS attack on the University of Hyderabad | India's Institution of Eminence (https://uohyd.ac.in/). The cyberattack overwhelmed the University's servers, online platforms and including its learning management system and registration portals, causing widespread disruption to academic services and access for students and faculty.

From April 14 to July 11, 2024, the Telegram Threat Actor (TA) group **"Z-BL4CX-H4T"** leaked the data and credentials of the Telangana Government's different-different portals which are mentioned below:

- Nutrition and Health Tracking System: nhts.telangana.gov.in
- Telangana State eProcurement Portal: https://dpms.ghmc.telangana.gov.in/BPAMSClient/
- Medical Officer Telangana: mchkit.telangana.gov.in
- Data Portal of Telangana Government: data.telangana.gov.in
- CDM Telangana: cdm.telangana.nic.in
- Registration & Stamps Department, Telangana: https://registration.telangana.gov.in/EncumbranceSearch.htm
- Department of Labour: https://labour.telangana.gov.in/Entrepreneur.do
- Commissioner and Director of School Education, Telangana: https://schooledu.telangana.gov.in/ISMS/officialLogin.xls

Sensitive governmental documents, citizen data, and confidential communications were exposed to the public, leading to concerns over the security of public sector information and potential misuse of personal data.

On August 26, 2024, the Telegram Threat Actor (TA) group **"THE ANONYMOUS BANGLADESH"** leaked the credentials of the Agricultural Marketing Department, Telangana (https://eaggrimarket.telangana.gov.in/login/LoginPage.aspx). Login Credentials of Registered Users/Farmers and other Sensitive Authentication details were exposed online, putting the organization at risk of further breaches and unauthorized access.

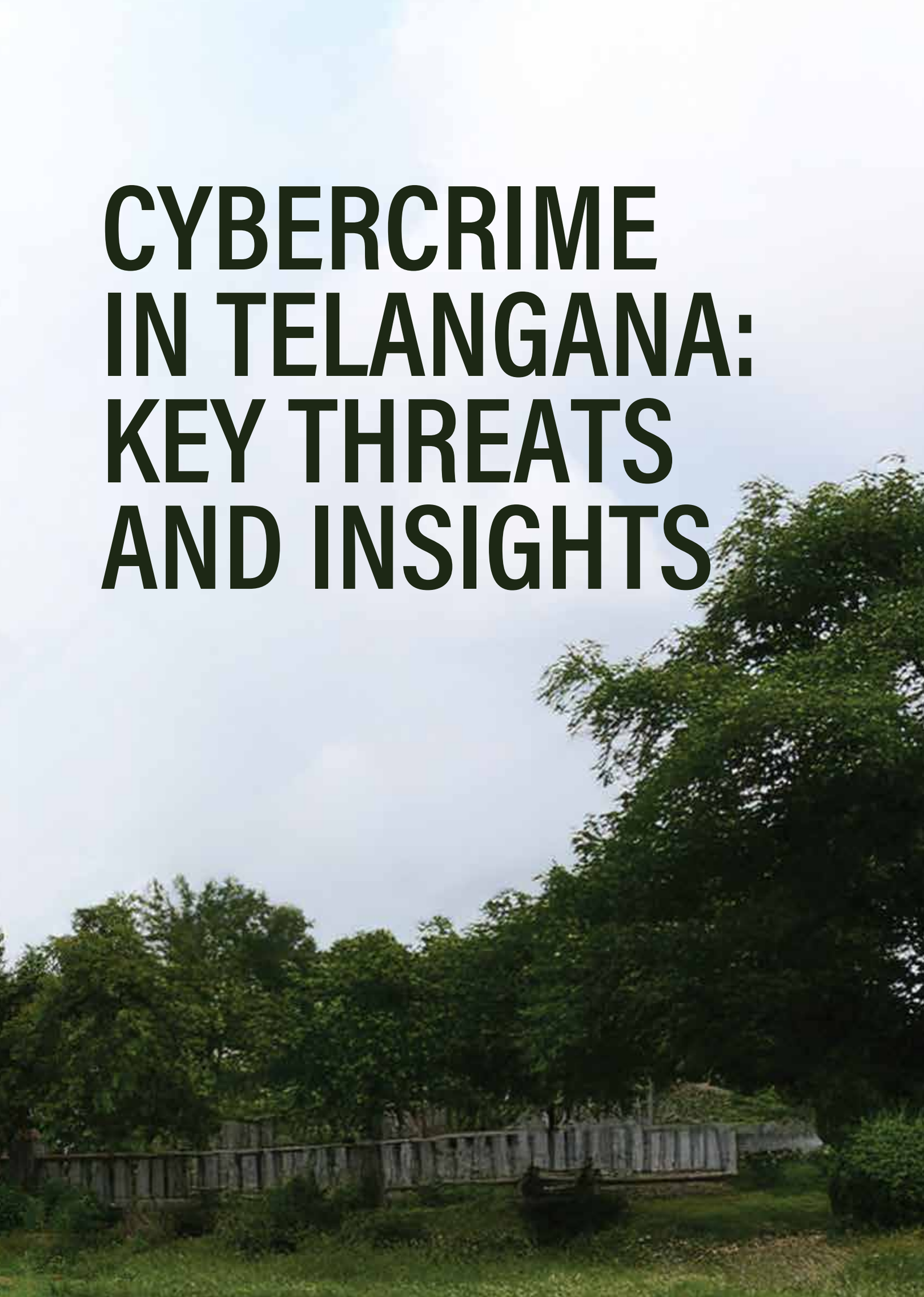
On September 19, 2024, the Telegram Threat Actor (TA) group **"BONDOWOSO BLACK HAT"** carried out a data leak on SSSS Of Hyderabad: Sri Sathya Sai Seva Organisations (https://ssssh.in). Confidential donor information, beneficiary data and internal operational documents were exposed, putting both the organization's reputation and the privacy of those it serves at significant risk.

On October 30, 2024, the Telegram Threat Actor (TA) group **"CyberDataPhantomsTeam"** executed a defacement attack on the SRK Industries, Hyderabad (http://neslweigh.in/about_us.php). The attacker altered the organization's website, replacing it with malicious content that tarnished the industries public image.

On November 12, 2024, the Telegram Threat Actor (TA) group **"Moroccan Cyber Forces"** carried out a data leak on TGBPASS Telangana Gov. (tgbpass.telangana.gov.in). Sensitive governmental documents, citizen data, and confidential communications were exposed to the public, leading to concerns over the security of public sector information and potential misuse of personal data.


RAMOJI
F·I·L·M C·I·T·Y

CYBERCRIME IN TELANGANA: KEY THREATS AND INSIGHTS



Some key insights and trends derived from the data:

1. Identity Theft Dominates Cyber Fraud

Identity Theft is the most reported cybercrime with **29,709** cases.

Key subcategories include:

Card Activation/PIN Generation/ Deactivation of Plans:
2,025 cases

Card Limit Enhancement:
2,501 cases

KYC Update:
5,369 cases

Unauthorized Transactions:
11,125 cases

Insight: The high number of cases indicates that fraudsters are heavily targeting personal and financial information, often through phishing, smishing, and vishing techniques. The use of fake bank calls, emails, and SMS to extract sensitive information like OTPs, card details, and KYC information is rampant.

2. Business & Investment Fraud is a Major Threat

Business & Investment Fraud is the second most reported category, with **25,995 cases**.

Key subcategories include:

Part-Time Job Scams:
18,690 cases

Stock Market Fraud
6,107 cases

Forex Scams
21 cases

Insight: The high number of cases indicates that fraudsters are heavily targeting personal and financial information, often through phishing, smishing, and vishing techniques. The use of fake bank calls, emails, and SMS to extract sensitive information like OTPs, card details, and KYC information is rampant.

3. Impersonation Scams are on the Rise

Impersonation accounts for **18,647 cases**

Key subcategories include:

Card Activation/PIN Generation/ Deactivation of Plans:
2,025 cases

Card Limit Enhancement:
2,501 cases

KYC Update:
5,369 cases

Unauthorized Transactions:
11,125 cases

Insight: Fraudsters are increasingly impersonating authority figures (police, customs, army officers) to instill fear and urgency in victims, leading them to transfer money or share sensitive information. The rise of "digital arrest" scams, where victims are threatened with legal action, is particularly concerning.

4. Advertisement Fraud is a Significant Issue

Advertisement Fraud has **17,669 cases**

Key subcategories include:

Fake Customer Care:
12,054 cases

OLX Frauds
1,574 cases

Undelivered Goods/Services
2,935 cases

Insight: Fraudsters are exploiting online marketplaces and social media platforms to advertise fake products or services. Victims are often lured into paying for goods that are never delivered or are of substandard quality. The high number of fake customer care scams indicates that fraudsters are also targeting individuals seeking help with banking or other services.

5. Loan Fraud is a Growing Concern

Loan Fraud has **12,589 cases**

Key subcategories include:

Loan Apps:
2,098 cases

Vishing/Smishing:
2,324 cases

Insight: Fraudsters are targeting individuals in need of quick loans, often through dubious loan apps that harvest personal data and use it for harassment or extortion. The rise in loan app frauds highlights the need for stricter regulation of such apps.

6. Gender-Related Frauds are Prevalent

Gender-Related Frauds account for **5,327 cases**

Key subcategories include:

Sextortion:
1,502 cases

Stalking:
3,287 cases

Insight: These frauds often involve emotional manipulation, blackmail, and threats, particularly targeting women. The high number of stalking cases suggests that social media platforms are being used to harass and exploit victims.

7. Job Fraud is a Persistent Problem

Job Fraud has **5,632 cases,** with victims being lured into paying fees for fake job opportunities or part-time work.

Insight: The job market, especially for part-time or remote work, is being exploited by fraudsters who promise lucrative opportunities but demand upfront payments or investments.

8. Emerging Threats: Crypto and Gaming Fraud

Crypto Currency Fraud:
67 cases

Gaming Fraud:
383 cases

Insight: While these numbers are relatively low compared to other categories, they represent emerging threats. Crypto frauds often involve fake investment platforms, while gaming frauds exploit in-game purchases and the psychology of gambling.

9. Low-Reported but Notable Frauds

Mobile Fancy Number Fraud:
18 cases

VISA Fraud:
251 cases

Matrimonial Fraud:
287 cases

Insight: These frauds, though less prevalent, target specific vulnerabilities. For example, matrimonial frauds exploit the emotional vulnerability of individuals seeking partners, while VISA frauds target those looking to migrate or travel abroad.

10. Not a Cyber Crime but Relevant

Not a Cyber Crime:
2,400 cases

Stolen Devices:
538 cases

Wrong Transactions:
477 cases

Insight: These cases, while not classified as cybercrimes, highlight the importance of securing personal devices and being cautious during financial transactions.

11. Unlawful Acts and Social Media Misuse

Unlawful Acts:
83 cases

Fake News:
34 cases

Inciteful Content:
12 cases

Insight: The spread of fake news and inciteful content on social media platforms is a growing concern, often leading to real-world consequences such as communal tensions or public panic.

Key Recommendations:

1. Awareness Campaigns: Public awareness campaigns should focus on the most prevalent frauds, such as identity theft, business & investment fraud, and impersonation scams.
2. Regulation of Loan Apps: Stricter regulations and monitoring of loan apps are needed to prevent data theft and harassment.
3. Social Media Vigilance: Platforms should enhance their monitoring systems to detect and remove fake profiles, fraudulent advertisements, and inciteful content.
4. Two-Factor Authentication (2FA): Encouraging the use of 2FA can help mitigate identity theft and unauthorized access to accounts.
5. Reporting Mechanisms: Improved reporting mechanisms for victims of cyber fraud can help authorities track and respond to these crimes more effectively.

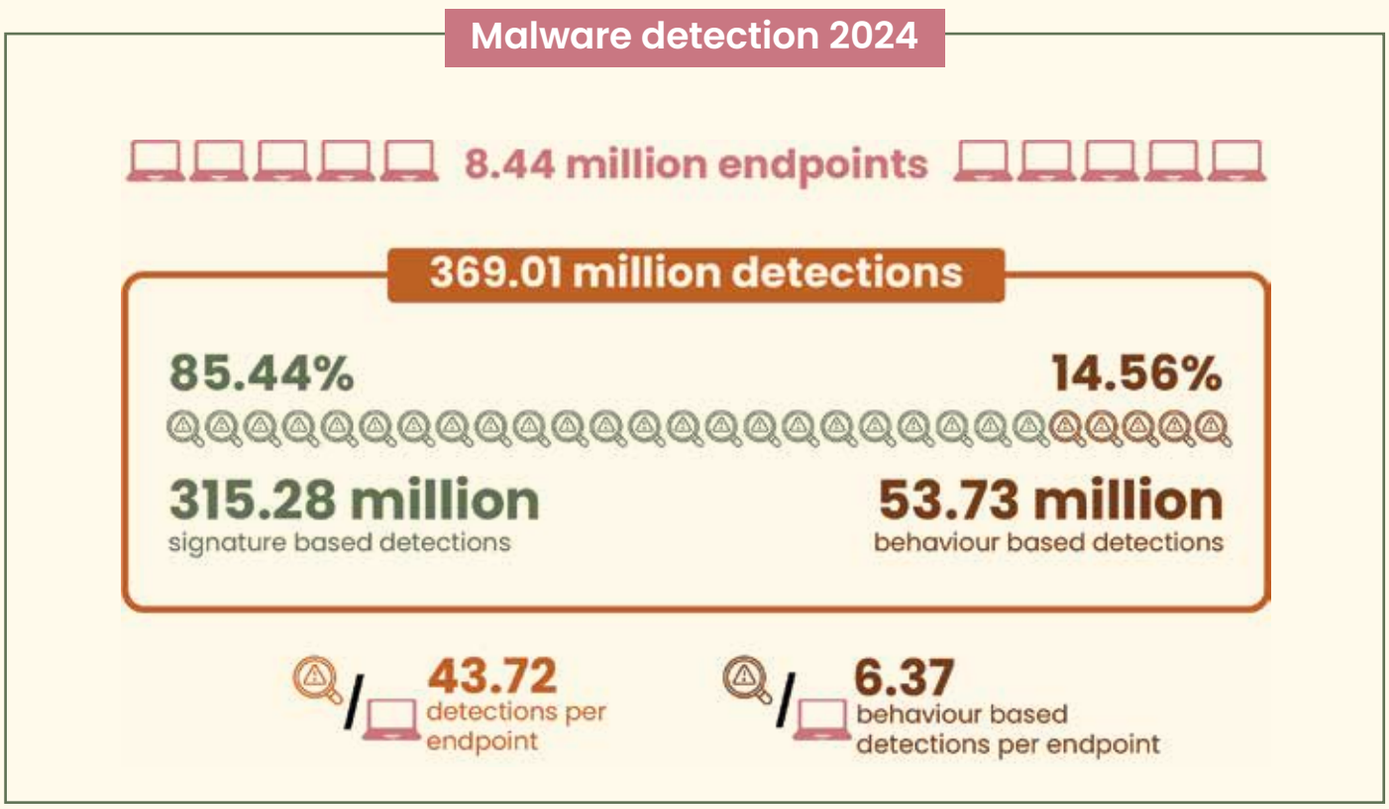
Conclusion:

The data reveals a diverse and evolving landscape of cyber fraud, with identity theft, business & investment fraud, and impersonation scams being the most prevalent. While traditional frauds like loan and job frauds remain significant, emerging threats such as crypto and gaming frauds are on the rise. Public awareness, regulatory measures, and technological solutions are essential to combat these cyber threats effectively.

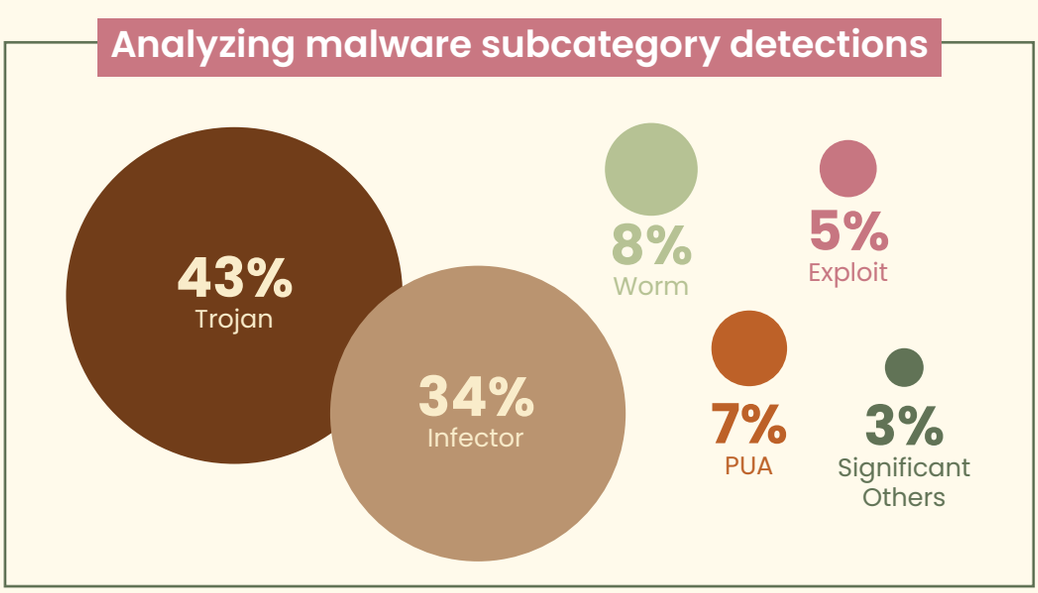
THE STATE OF MALWARE IN INDIA

Cybersecurity Outlook 2024

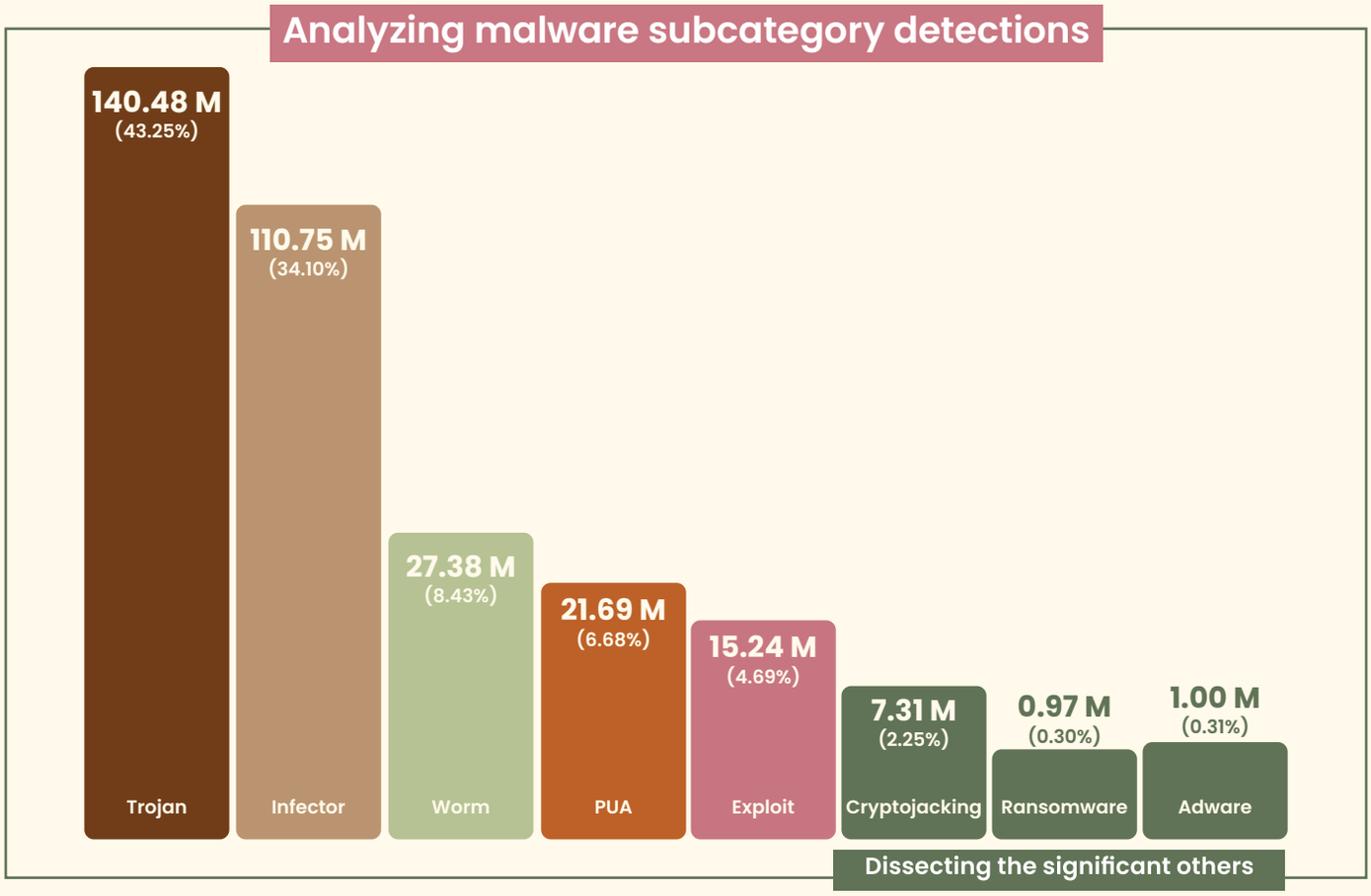
The analysis of India's malware detection, based on Seqritre Labs' telemetry data from October 2023 to September 2024, reveals critical insights into the current threat landscape. With **369.01 million** detections across **8.44 million** strong installation base, the data highlights both the scale of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



Malware Threats in India:



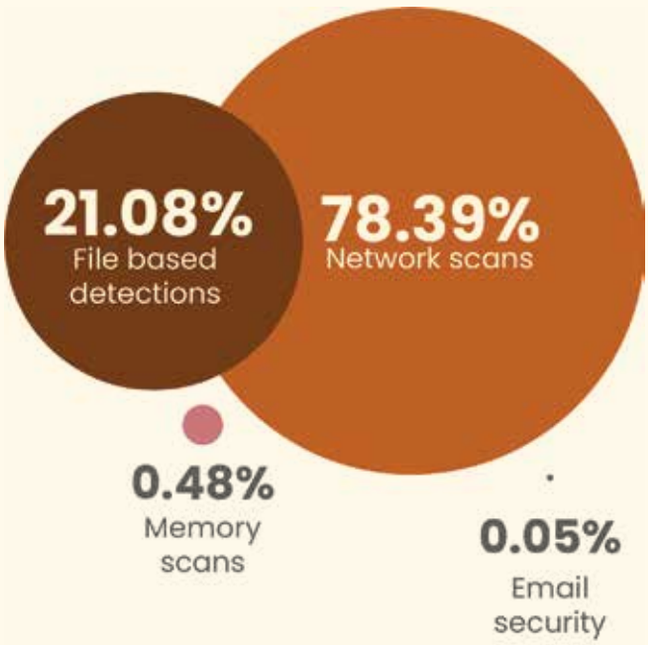
Analyzing malware subcategory detections



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.

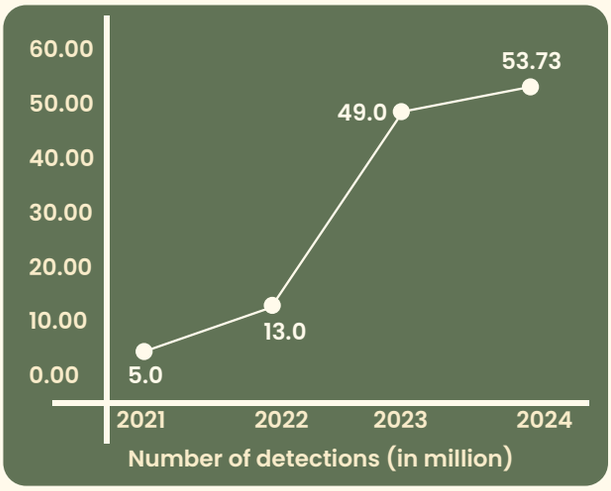


The predominance of network-based detection (78.39%) is driven by:

- 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

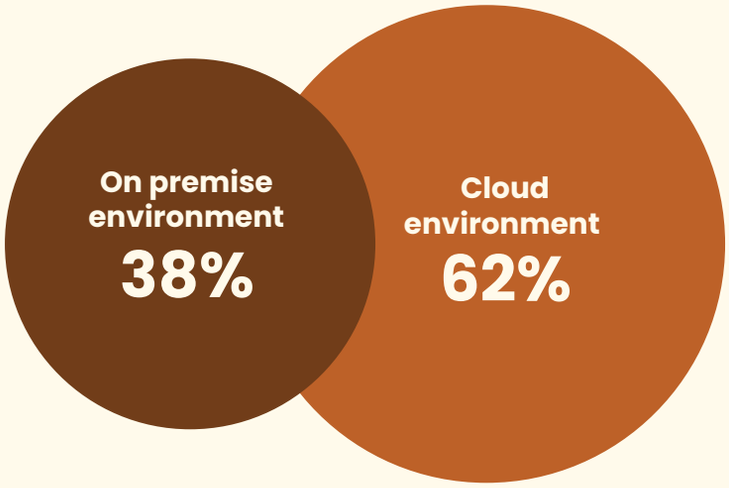
The significant growth in behavioral detections also reflects the maturation of underlying technologies. The integration of artificial intelligence and machine learning has dramatically enhanced the capability to analyze and identify suspicious patterns in real-time. Advanced processing capabilities 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

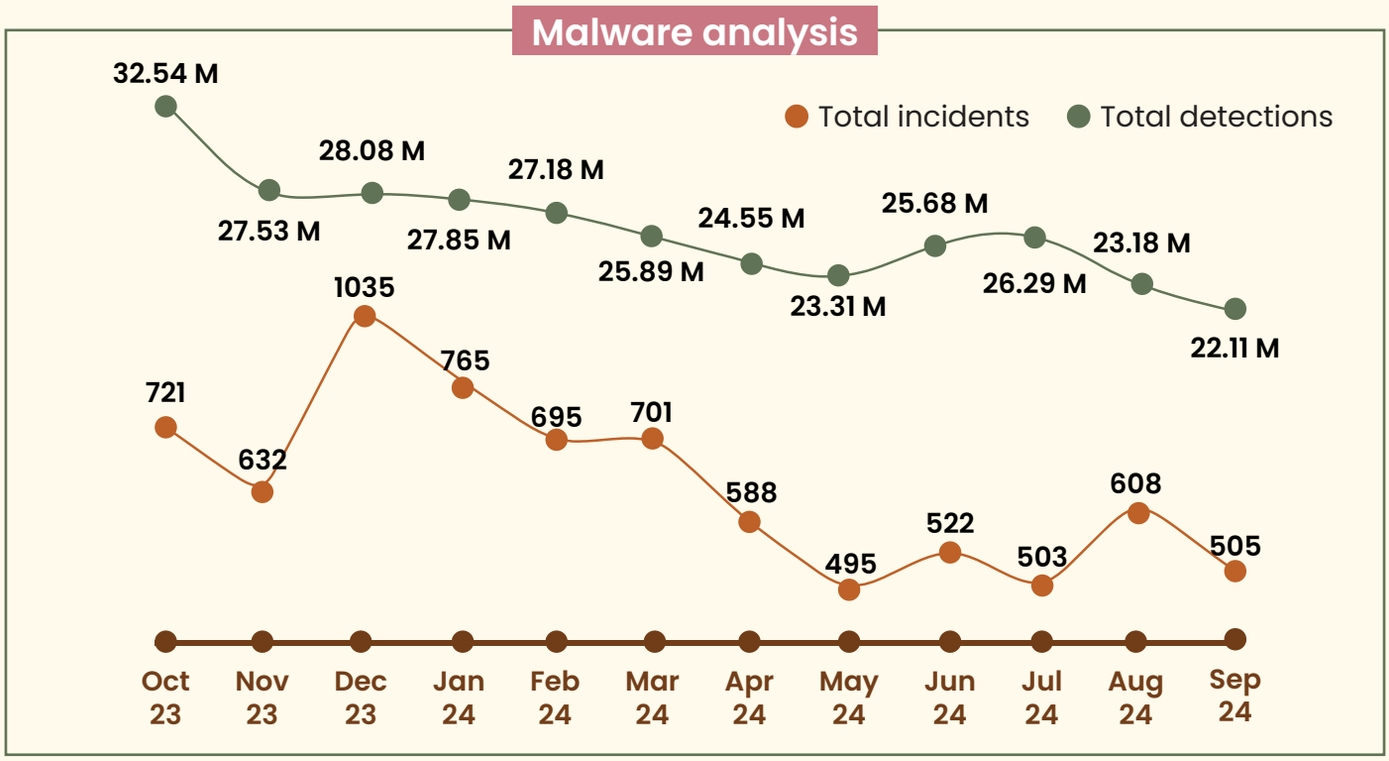
Cloud environment accounts for 62% of total detections (averaging 3.02 detections per endpoint) and on-premises environments contributing 38% (averaging 1.88 detections per endpoint).



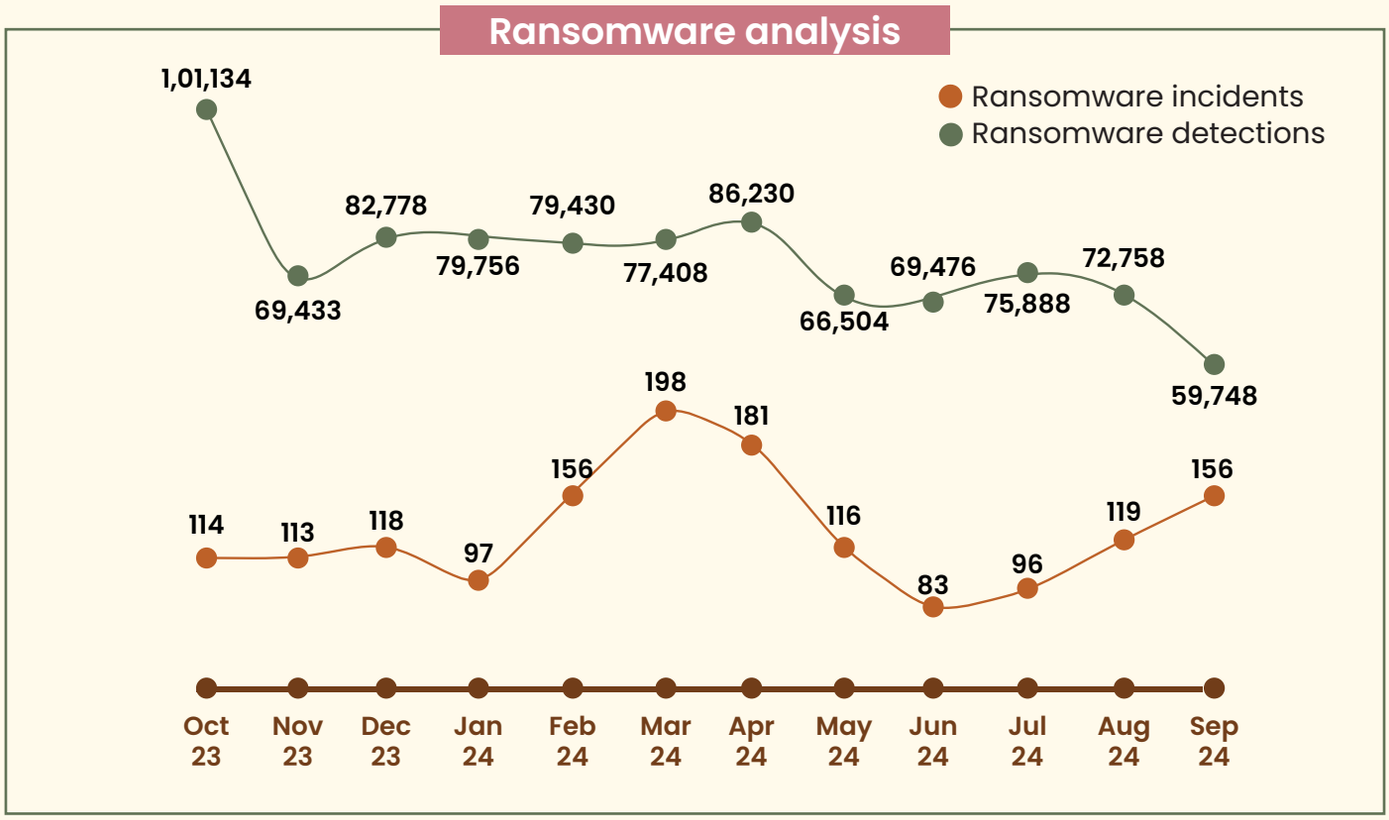
- Cloud environment show a significantly higher detection rate, reflecting their growing prominence in enterprise operations. This trend can be attributed to:
  - **Increased adoption of cloud services:** Organizations are rapidly migrating to the cloud, expanding their attack surface and consequently 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)	Dyamond	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.

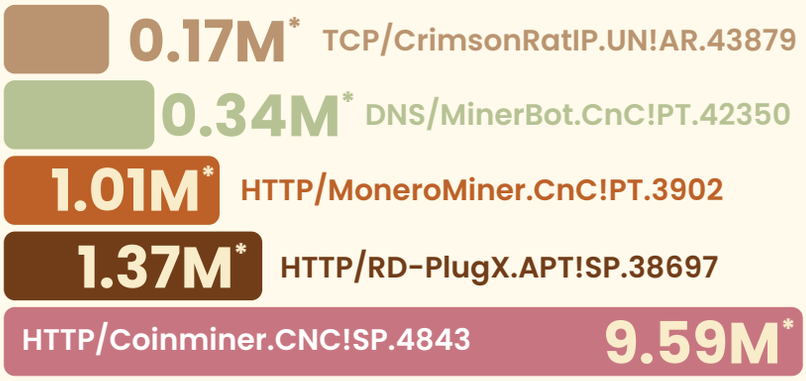
Rise of cryptocurrency miners:

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

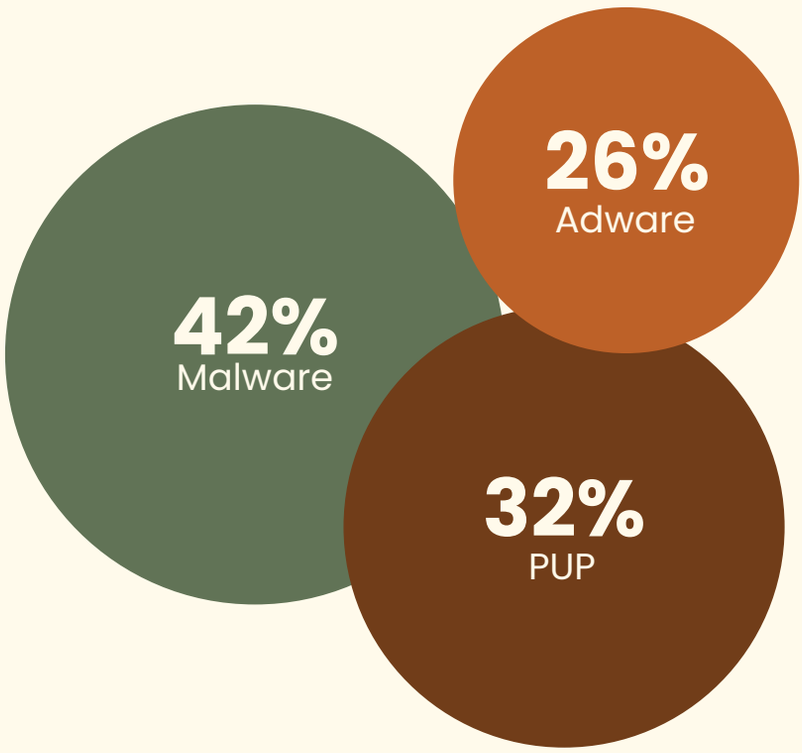


*Detection Count

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

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 high 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)

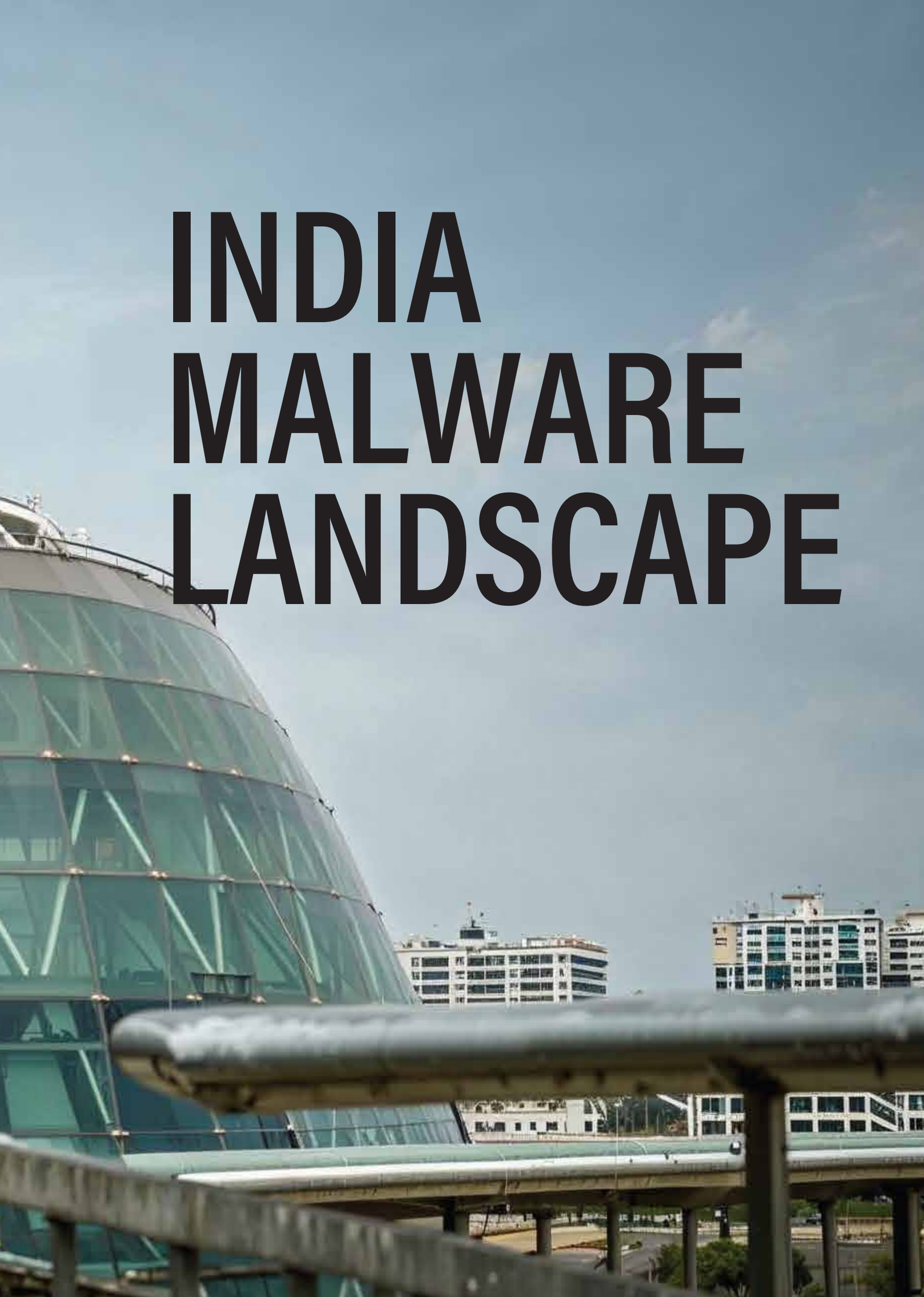
A critical security bypass vulnerability in Windows' shortcut file processing. It enables remote code execution through specially crafted shortcut (.lnk) files, circumventing established security controls when users interact with these malicious shortcuts.

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

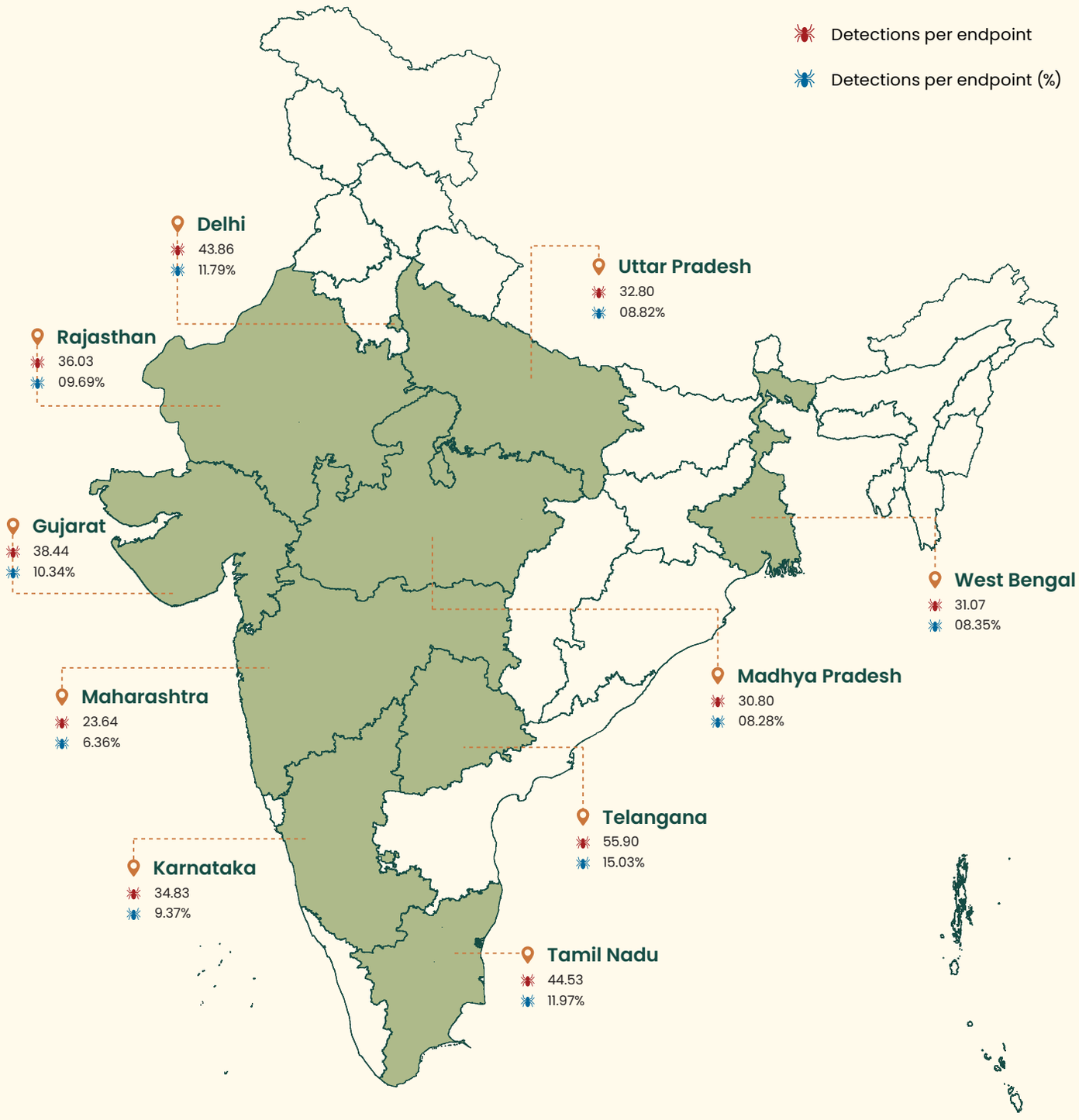
Maharashtra: **23.65 detections/endpoint (6.36%)**

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

Emerging Patterns

Madhya Pradesh: **30.81 detections/endpoint** **West Bengal:** **31.07 detections/endpoint**

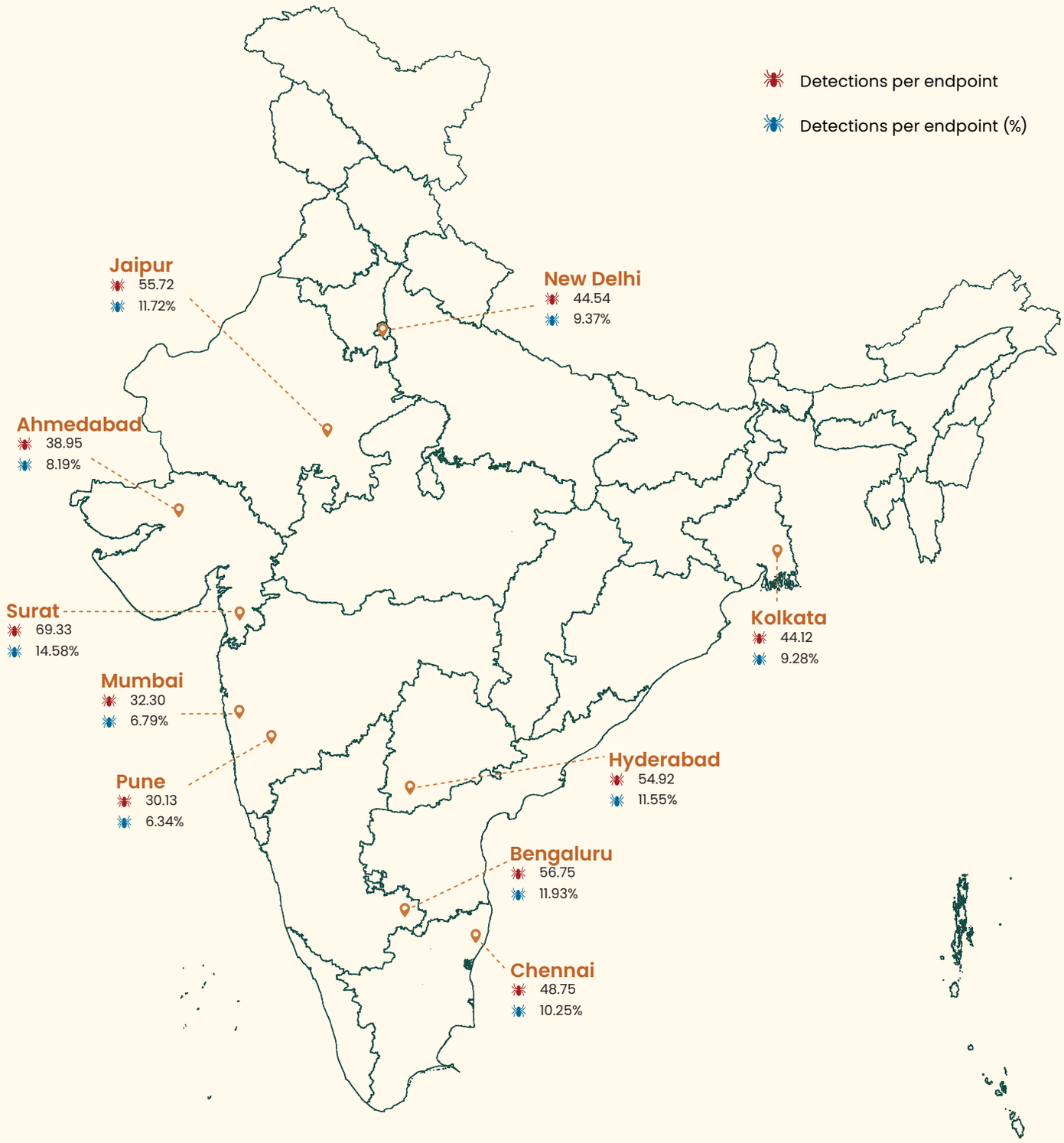
- Indicates growing digital adoption Infrastructure Impact
- Higher detections in states with better digital infrastructure
- Better internet penetration



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:

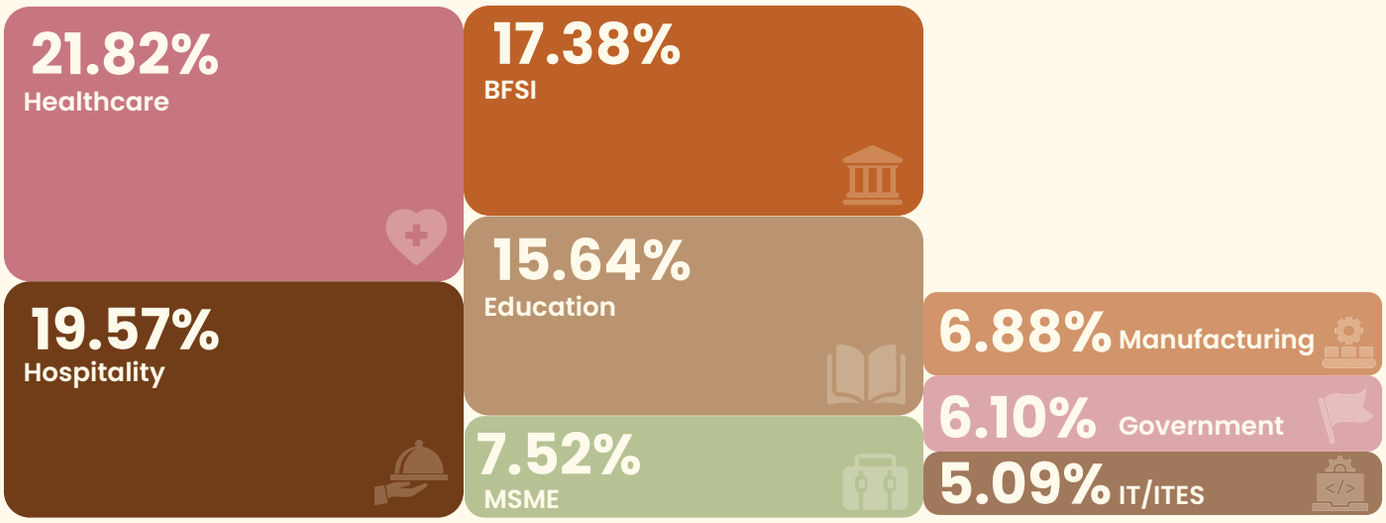
Mumbai:
32.30 detections per endpoint (6.79%)

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 %

Telecom

Covers mobile and telephone service providers as well as businesses related to telecom infrastructure and services.

15,355+ detections

~1,000 Endpoints

58% of which were

Trojan.Mpcdotcash

Trait: Propagation via malicious websites, drive-by downloads, and bundled with freeware or pirated software. Installs unauthorized cryptocurrency mining software, consuming system resources.

Automobiles

Includes businesses dealing with vehicles, such as dealerships, showrooms, and service centers.

2,17,000+ detections

~11,422 Endpoints

47% of which were

Trojan.NSIS.Miner.SD

Trait: Distributed via malicious NSIS installers posing as software updates. Installs hidden cryptocurrency miners, may download additional malware components.

Media & Entertainment

Involves companies in media production, film production, and related activities.

10,500+ detections

~14,224 Endpoints

43% of which were

W32.Pioneer.CZ1

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

Power & Energy

Comprises companies involved in power generation, electricity distribution, petroleum, and other fuel industries.

15,355+ detections

~2,132 Endpoints

29% of which were

LNK.RaspRobin.48713

Trait: Spreads via malicious .lnk (shortcut) files on removable media like USB drives. Connects to external servers to download additional malware and establish persistence.

Logistics

Includes courier companies and logistics service providers.

11,000+ detections

~4,163 Endpoints

27% of which were

Trojan.Agent

Trait: Propagates through various metheds including phishing, malicious dawnloads, 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. Uniike 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.CZ1

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

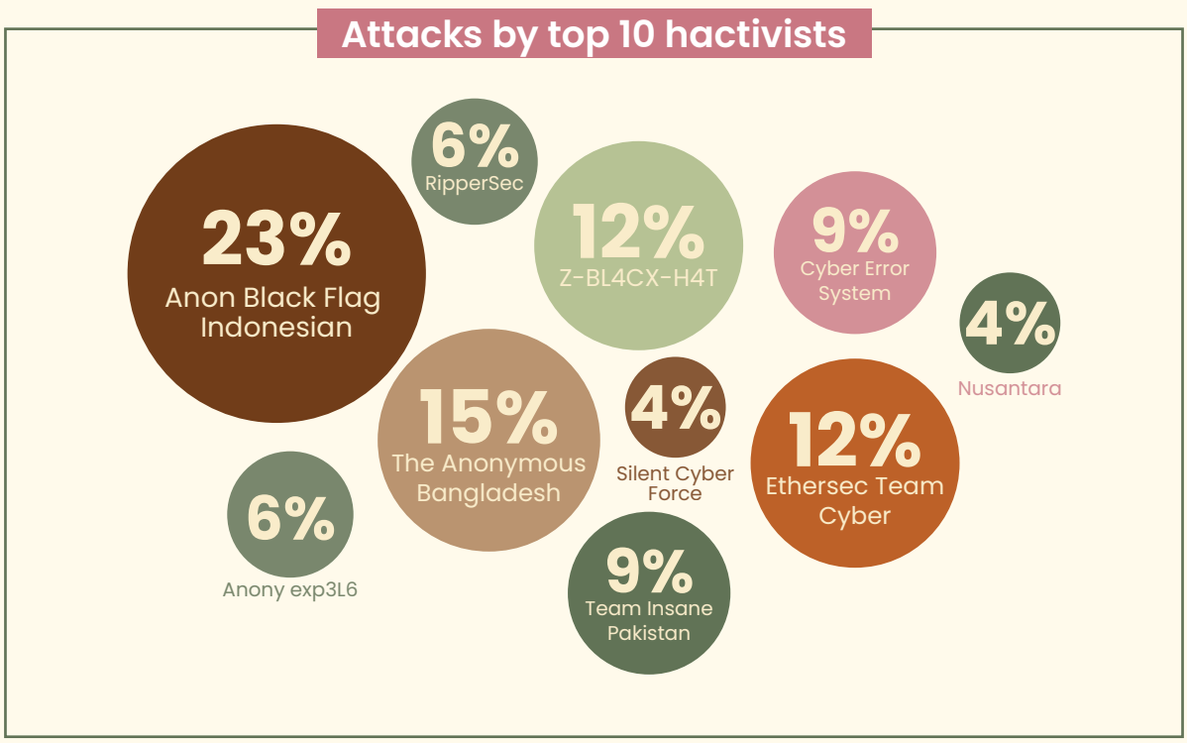
Trojan. Convagent

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 Hacktivist 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:

Midnight Blizzard	Volt Typhoon	LockBit	BlackCat (Alphv)	Scattered Spider
Sandworm	RansomHub	NoName057(16)	IntelBroker	Cyber Army of Russia Reborn

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:

AFD.sys (Ancillary Function Driver for WinSock)	**dbutil_2_3.sys** (Dell Driver)	**appid.sys**	**RTCore64.sys** (MSI Afterburner Driver)	**WinRing0.sys**
nvlddmkm.sys (NVIDIA Graphics Driver)	**gdrv.sys** (GIGABYTE Driver)	**SynTP.sys** (Synaptics Driver)	**RTCore64.sys** (MSI)	**atillk64.sys** (ATI Radeon Driver)

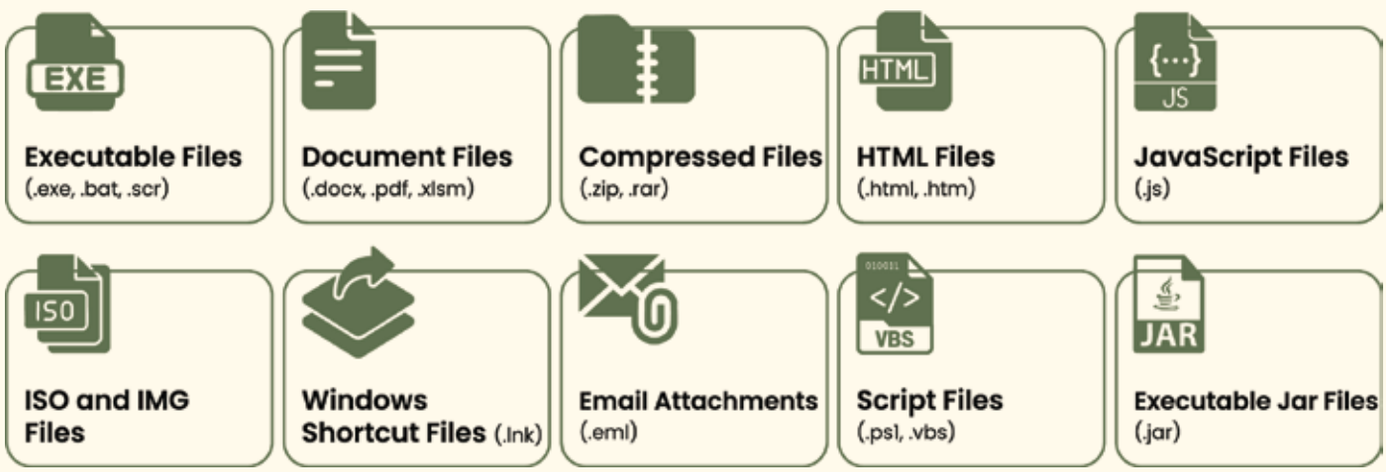
Most Abused LOLBins (Living-Off-the-Land Binaries)

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:

PowerShell	**Rundll32**	**Mshta**	**Regsvr32**	**Msiexec**
Certutil	**Bitsadmin**	**Wmic**	**Notepad**	**SystemSettings AdminFlows**

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:



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:

- Google Drive
- Dropbox
- OneDrive
- GitHub
- Microsoft Teams
- WeTransfer
- Box
- Amazon S3 Buckets
- IBM Cloud
- Oracle Cloud

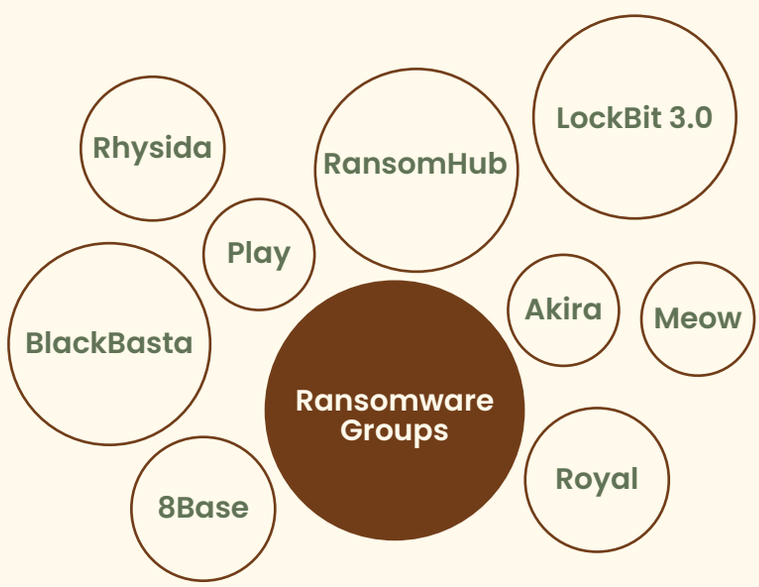
Top MITRE Techniques Used

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

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

Hacktivist Shifts: Migration to Secure Platforms

In response to stricter data-sharing policies and increased surveillance, hacktivist 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

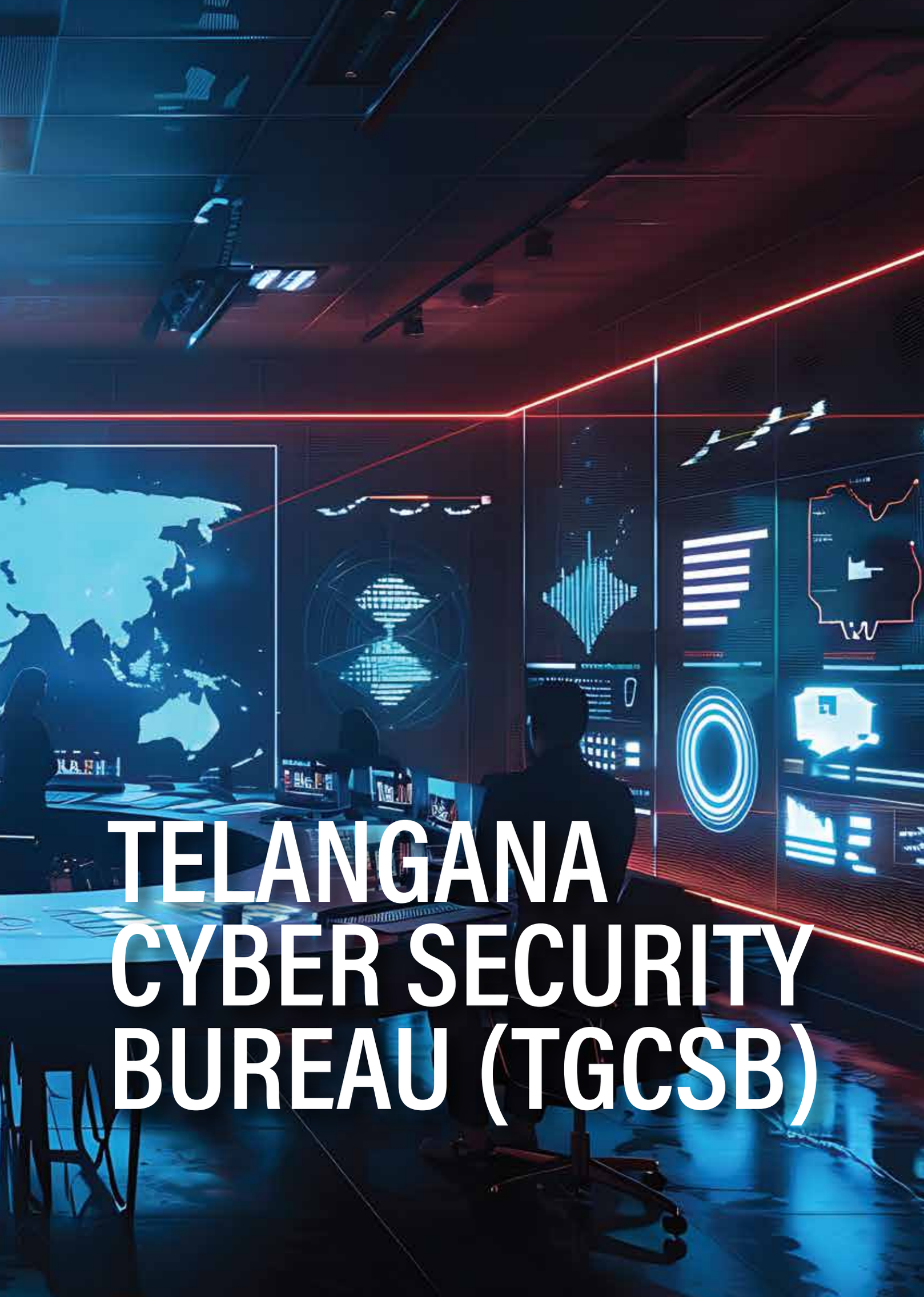
The increasing frequency and sophistication of cyberattacks hint that prevention alone is no longer sufficient. CISOs must ensure that their organizations are resilient enough to recover quickly from cyber incidents. This requires a holistic approach to cybersecurity and business continuity planning.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



TELANGANA CYBER SECURITY BUREAU (TGCSB)

Telangana Cyber Security Bureau (TGCSB): Strengthening Cybersecurity in the Digital Age

The Telangana Cyber Security Bureau (TGCSB) is a specialized agency dedicated to ensuring a secure and resilient digital environment across the state. As cyber threats continue to evolve, TGCSB plays a crucial role in preventing cybercrimes, protecting critical digital infrastructure, and creating awareness. Functioning under the Telangana Police, the bureau leverages advanced tools and technology, intelligence-driven operations, and strategic collaborations to tackle today's cybersecurity challenges.

A Holistic Approach to Cybersecurity

With cyberattacks becoming more sophisticated, TGCSB follows a comprehensive strategy that combines monitoring, prevention, response, and capacity building. It works closely with various stakeholders, including law enforcement agencies, technology firms, and cybersecurity professionals, to stay ahead of digital threats. By integrating artificial intelligence (AI), big data analytics, and digital forensics, TGCSB enhances its ability to detect and mitigate cyber risks effectively.

One of its core objectives is to protect government and private sector organizations from cyber threats. Whether it is financial fraud, ransomware attacks, or misinformation campaigns, TGCSB actively monitors and neutralizes online threats. The bureau also educates the public on safe online practices through workshops, awareness campaigns, and digital literacy programs.

Cyber Fusion Center Monitoring Unit

At the core of TGCSB's operations is the Cyber Fusion Center Monitoring Unit, a state-of-the-art facility designed for real-time cyber threat monitoring and response. This unit acts as a centralized hub where multiple data sources are analyzed to detect suspicious activities and cyberattacks.

Key functions of the Cyber Fusion Center Monitoring Unit include:

- **Threat Intelligence Gathering:** The unit continuously monitors global cyber trends, malware outbreaks, and emerging hacking techniques to anticipate potential risks.
- **Incident Response:** When cyber threats are detected, the team quickly assesses the impact and coordinates response efforts to minimize damage.
- **Digital Forensics:** Using advanced tools, forensic experts analyze cybercrimes, recover lost data, and trace digital footprints to identify perpetrators.
- **Inter-Agency Collaboration:** The unit works with national and international cybersecurity organizations, ensuring swift action against cybercriminal networks.

By integrating artificial intelligence and predictive analytics, the Cyber Fusion Center enhances proactive defense mechanisms, making it a critical asset in Telangana's fight against cybercrime.

Social Media Unit

In today's digital age, social media plays a powerful role in shaping public perception, communication, and even crime trends. The Social Media Unit of the Telangana Cyber Security Bureau is responsible for monitoring online platforms to detect and counteract digital threats, including cyber harassment, financial fraud, fake news, and extremist propaganda.

The unit performs several important functions, such as:

- Detecting and Addressing Misinformation: False information can spread rapidly on social media, leading to confusion, panic, or even law-and-order issues. The unit identifies and flags such content for appropriate action.
- Cybercrime Prevention: From cyber bullying to online financial scams, the Social Media Unit tracks and investigates cases, ensuring swift intervention.
- Public Awareness Campaigns: The bureau actively engages with the public by spreading cybersecurity awareness through social media, and educating users on best practices to stay safe online.
- Law Enforcement Assistance: The unit supports police investigations by providing real-time insights into cybercriminal activities occurring on digital platforms.

With the rise of cybercrimes linked to social media, this unit serves as a crucial first line of defense in tackling digital threats and ensuring online safety for citizens.

Telangana Cyber Security Bureau: Leading the Fight Against Evolving Cyber Threats with Innovation and Collaboration

As technology continues to advance, cyber threats will also become more complex. The Telangana Cyber Security Bureau remains committed to strengthening its cybersecurity framework through continuous innovation, enhanced infrastructure, and deeper collaborations with global cybersecurity organizations.

By staying ahead of cyber threats and adapting to new challenges, the Telangana Cyber Security Bureau is setting a benchmark in digital security, cyber law enforcement, and public awareness initiatives. Through its proactive approach, it continues to ensure a safe and resilient cyberspace for businesses, government institutions, and citizens alike.

Acknowledgement

Authors
Lalit Mohan, Chief Product Officer, Quick Heal
Sangamesh S, Vice President & Head of Seqrite Labs, Quick Heal
Jaswinder Singh, Director - Engineering, Seqrite Labs, Quick Heal

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

Editor
Jyoti Karlekar
Bineesh Mathew

Designer
Manoj Joshi
Mukund Shrigadi

Scan Here for
India Cyber Threat Report 2025 and Telangana Cyber Threat Report 2025

About Telangana Cyber Security Bureau (TGCSB)

The Telangana Cyber Security Bureau (TGCSB) is the state's dedicated agency for tackling cyber threats and enhancing cybersecurity resilience. It works to prevent, detect, and investigate cybercrimes while ensuring a secure digital ecosystem. TGCSB collaborates with law enforcement, government bodies, and industry stakeholders to strengthen cyber defense, promote awareness, and implement advanced cybersecurity measures across Telangana.

About DSCI

The Cybersecurity Centre of Excellence (CCoE) is a global cybersecurity hub based in Hyderabad, Telangana. Established in collaboration with the Data Security Council of India and the Government of Telangana, CCoE is dedicated to creating a secure and trusted cyberspace while fostering best practices in cybersecurity and privacy.

To date, CCoE has trained over 2,000 Law Enforcement Agency (LEA) professionals and over 15,000 students and professionals with essential cybersecurity skills. Beyond training, CCoE has supported over 60 startups in their growth and engaged in 10+ international collaborations. Additionally, CCoE has published nearly 20 reports and white papers to advance global cybersecurity standards and best practices.

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-ofthe- 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.

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 | W: www.seqrite.com

/Seqrite /seqrite
/@seqrite385 /company/seqrite

DSCI PROMOTING DATA PROTECTION | CYBERSECURITY CENTRE of EXCELLENCE
A joint initiative of DSCI & Government of Telangana