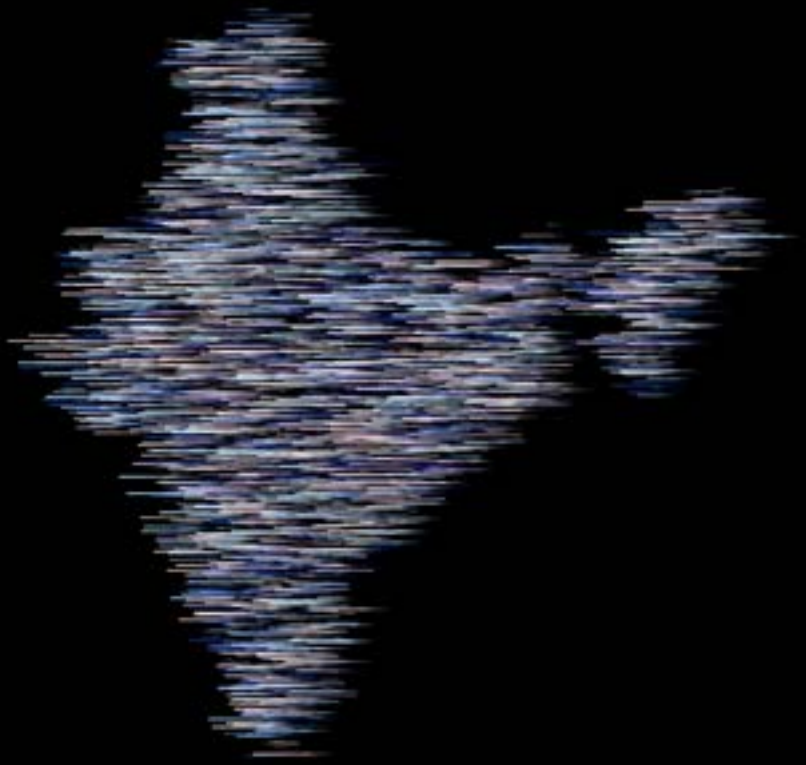
CYBLE®

REPORT

India Threat Landscape Report

July 2024 - September 2024

Introduction



In recent months, the cyber threat landscape in India has become increasingly sophisticated and widespread, affecting various sectors and industries. From ransomware attacks to hacktivism and general cybercrime, India has faced a barrage of attacks aimed at disrupting operations, exfiltrating sensitive data, and causing reputational and financial damage.

This report focuses on analyzing cyberattacks in the country between July 2024 and September 2024, highlighting key trends, statistics, and impacted sectors. By exploring the nature and motivations behind these attacks, organizations can better understand their vulnerabilities and implement robust defenses to mitigate risks.

Key Findings

Ransomware Attacks:

26 incidents, with LockBit, BianLian, BlackCat, and 8Base leading. A record $75 million ransom was paid to Dark Angels.

Hacktivism:

12 incidents targeting government websites and public sector portals, driven by political and social causes.

General Cybercrime:

103 incidents, including 70 data breaches, 20 phishing attacks, and 13 cases of malware, DoS, and unauthorized access.

Top Targeted Sectors:

- Manufacturing (29% of ransomware attacks)
- Healthcare, Technology, Financial Services, and Telecommunications were also heavily impacted.

Detailed Analysis of Attack Vectors

1. Ransomware Attacks

Ransomware continues to be a critical concern in India's cyber threat landscape. During the three-month period, 26 ransomware attacks were reported. The most active ransomware families were LockBit, BianLian, BlackCat, 8Base, and Mallox, accounting for the majority of the attacks.

Top Ransomware Families:

Ransomware Family	Percentage of Attacks
LockBit	23.33%
BianLian	16.67%
BlackCat	11.67%
8Base	10%
Mallox	5%

One of the most notable incidents involved the Dark Angels group, which successfully extorted $75 million, marking one of the largest ransom payments in India's history. This underscores the financial severity of ransomware attacks and the need for advanced threat detection and response strategies.

2. Hacktivism Incidents

Hacktivism incidents have also been on the rise, with 12 major cases reported during this period. Hacktivists primarily targeted government websites, public sector portals, and social media accounts to promote political statements, disrupt events, and advocate for social justice causes.

Common Hacktivism Targets:

- **Government Websites:** Hacktivists often deface or take down government sites to draw attention to their cause.
- **Public Sector Portals:** Attacks aimed at disrupting operations during key public events.
- **Social Media Accounts:** Prominent political figures and government officials have also been targeted.

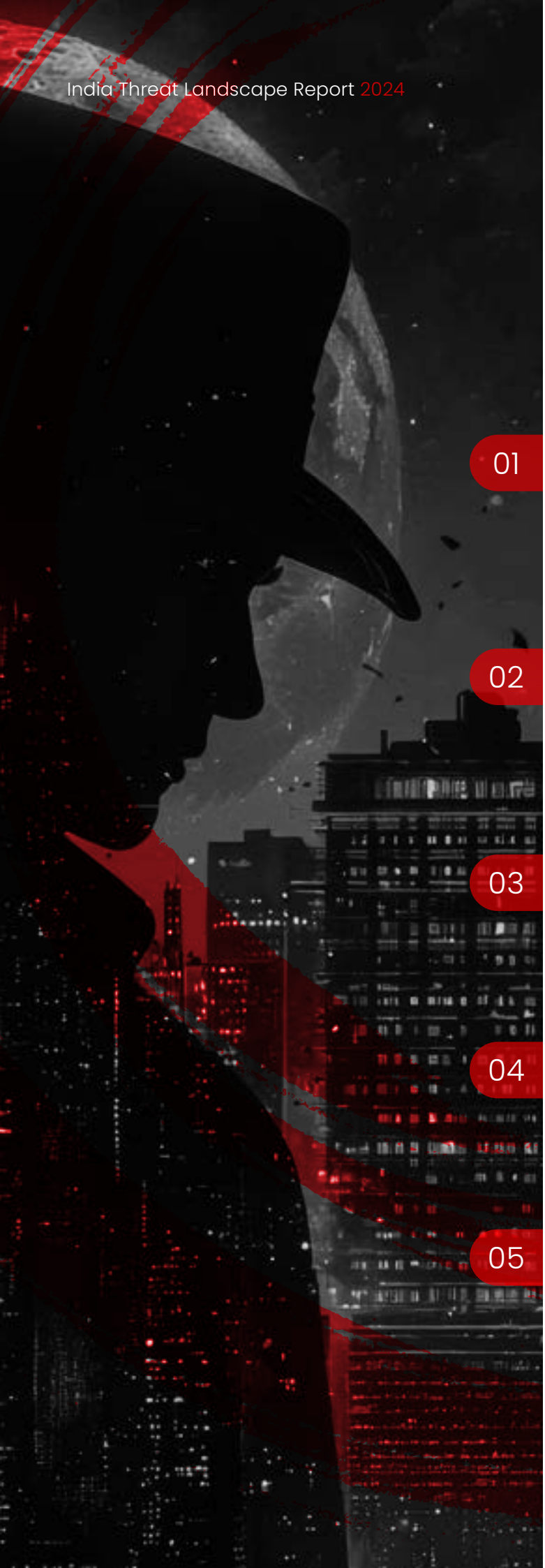
3. General Cybercrime

India witnessed 103 incidents of general cybercrime, including data breaches, phishing attacks, malware, denial-of-service (DoS) attacks, and unauthorized access.

Breakdown of General Cybercrime:

Type of Attack	Number of Incidents
Data Breaches	70
Phishing Attacks	20
Other Cybercrime (Malware, DoS, etc.)	13

- **Data Breaches:** Data breaches remain a significant challenge, with 70 breaches reported in the past three months. These breaches often result in the exposure of sensitive personal and corporate information, contributing to an increased risk of identity theft, fraud, and financial losses.
- **Phishing Attacks:** Phishing accounted for 20 incidents, typically targeting individuals and businesses via fraudulent emails designed to steal credentials or deploy malware.
- **Other Cybercrime Activities:** Other forms of cybercrime, such as malware, denial-of-service (DoS) attacks, and unauthorized access, were responsible for 13 reported incidents, affecting both private and public sectors.



Most Impacted Sectors

01

Manufacturing
(29% of Ransomware Attacks)

The manufacturing sector has been the hardest hit, making up nearly 29% of ransomware incidents. The sector's extensive digital transformation and adoption of AI technologies have made it a prime target for attackers.

02

Healthcare
(8.9% of Ransomware Attacks)

Healthcare is highly vulnerable due to its reliance on IoT and third-party service providers. Approximately 8.9% of ransomware attacks targeted healthcare, highlighting the need for improved security measures in this critical sector.

03

Technology
(6.67% of Ransomware Attacks)

The technology sector accounted for 6.67% of ransomware incidents. The sector's rapid digital innovation and high transaction volumes make it a lucrative target for cybercriminals.

04

Financial Services
(8.9% of Ransomware Attacks)

Financial services remain a key target due to the sensitive nature of the data they handle. The sector experienced 8.9% of ransomware incidents, in addition to data breaches and phishing attacks.

05

Telecommunications
(Key Target for Cybercrime and Hacktivism)

Telecommunications was targeted by hacktivists and cybercriminals, largely due to its role in infrastructure, making it a valuable target for those looking to disrupt communication networks and services.

Remediation Measures

To counteract the increasing cyber threats, organizations in India need to take proactive steps to secure their systems, data, and infrastructure. Key remediation measures include:

01

Comprehensive Threat Intelligence:

Invest in advanced threat intelligence platforms such as Cyble's Threat Intelligence solutions to detect and mitigate ransomware, phishing, and other cyber threats in real time.

02

Ransomware Defense:

Deploy robust endpoint protection, implement regular data backups, and establish a strong incident response plan to minimize the impact of ransomware attacks.

03

Employee Awareness and Training:

Conduct regular security awareness training sessions to educate employees about phishing, social engineering, and other cybercrime tactics.

04

Data Protection and Encryption:

Ensure that sensitive data is encrypted both at rest and in transit, and deploy strong access control measures to prevent unauthorized access.

05

Multi-factor Authentication (MFA):

Implement MFA across all critical systems and accounts to add an extra layer of security.

06

Vulnerability Management:

Conduct regular vulnerability assessments and patch management to reduce the risk of exploitation by attackers.

Why Choose Cyble?

Cyble provides cutting-edge cybersecurity solutions that offer comprehensive protection against modern threats, including ransomware, data breaches, and hacktivism. With AI-powered Threat Intelligence, Attack Surface Management, Dark Web Monitoring, and Takedown Services, Cyble empowers organizations to stay ahead of cyber threats and secure their digital landscape.

Cyble's Brand Protection and Digital Forensics services also ensure that businesses can quickly recover from incidents and safeguard their reputations. By partnering with Cyble, organizations can build resilient cyber defenses and minimize the impact of cyberattacks.

About Cyble

Cyble Inc. is a cybersecurity company specializing in dark web monitoring and threat intelligence services. Cyble leverages proprietary AI-based technology to help enterprises, federal bodies, and individuals stay ahead of cybercriminals. The company is known for its expertise in tracking cyber threats, data breaches, and other malicious activities.

See Cyble in Action

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