

How the dark web economy and malware hotspots are redrawing India's cyber map

India's digital growth story is now inseparable from its cyber risk story.

India is building one of the world's fastest-growing digital economies. But in the shadows of this expansion, a parallel economy is thriving one built on stolen credentials, spoofed domains, ransomware payloads, and dark web marketplaces. Every surge in digital adoption is mirrored by a surge in cyber exploitation. In today's India, growth and risk are advancing together.

According to the India Cyber Threat Report 2026 released by Seqrite, the country witnessed over 415 million signature-based malware detections in the past year. That number alone signals scale. But beneath it lies a deeper shift: India is no longer just battling random cyber incidents it is confronting a structured underground economy targeting brands and geographically concentrated digital war zones across states.

Two trends stand out:

1. The rise of the dark web economy targeting Indian enterprises, and
2. The emergence of specific malware hotspots across Indian states.

Together, they paint a picture of cybercrime that is industrialized, organized, and increasingly territorial.

The dark web economy targeting Indian brands

India's fastest-growing brands are now prime inventory on the dark web.

Seqrite's Digital Risk Protection Services (DRPS) monitors the surface web, deep web, and dark web to detect brand impersonation, domain spoofing, IP theft, exposed credentials, and infrastructure vulnerabilities. The fact that such monitoring is now essential reflects a stark reality: brand value has become a monetizable cyber asset.

Cybercriminals are not merely breaching systems they are exploiting brand trust.

What is being traded?

- Phishing domains mimicking Indian enterprises
- Stolen customer databases

- Leaked credentials
- Counterfeit digital assets
- Third-party vendor access points

With 600 million URLs classified and categorized, 2 billion known files tracked, and 100TB of data processed daily for ML training and analytics, the scale of surveillance required to track this shadow economy is staggering. It reveals how massive the underground marketplace has become.

The report notes that social engineering attacks like phishing, vishing, smishing are at the top the list of threats. These are precisely the tactics that thrive on brand impersonation. A cloned banking portal or a spoofed e-commerce notification doesn't need advanced malware. It needs trust.

And trust is what Indian brands have built at scale.

Malware hotspots: Why certain states are becoming digital war zones

Beyond the dark web marketplace, another worrying pattern emerges malware detections are not evenly distributed across India.

The report identifies the Top 10 states with the highest malware detections, underscoring how cyber risk is clustering geographically. While the report highlights the ranking, the broader implication is strategic: digital infrastructure density, enterprise concentration, startup ecosystems, and industrial corridors are creating high-value cyber territories.

Why are some states becoming hotspots?

1. Digital density

States with higher enterprise digitization and larger endpoint deployments naturally expand the attack surface. Secrite alone protects 8 million+ active endpoints globally, a reflection of how widespread device-level exposure has become.

2. SME vulnerability

Mid-sized enterprises in industrial belts often lack advanced threat detection and rapid patch orchestration. The report's recommendations explicitly call for accelerating patch management and reinforcing identity as the new perimeter suggesting that delayed updates remain a core weakness.

3. Supply chain exposure

Third-party vendor monitoring is now central to digital risk management. States with dense manufacturing or IT vendor ecosystems face amplified supply chain risk. A breach in a small subcontractor can cascade upward.

4. Social engineering at scale

With social engineering leading all threat types of urban centers with large consumer bases become fertile ground for phishing campaigns, banking fraud, and identity theft.

In effect, these states are not just economic hubs they are cyber battlegrounds.

415 million detections: Reactive security at scale

Crossing 415 million malware detections is more than a technical statistic. It signals that India's cybersecurity posture remains heavily detection-driven rather than prediction-driven.

The report emphasizes moving toward:

- Predictive intelligence
- Autonomous detection and response
- AI-layer hardening

- Cyber resilience frameworks

But the numbers suggest we are still firefighting.

Processing 1 million new malware samples, generating 500GB of new security telemetry, and categorizing 150,000 new classifications daily reflects a security ecosystem under constant siege. When volumes are this high, geography starts to matter. Attackers test campaigns in one region, refine them, and redeploy at scale.

That is how digital war zones form.

From prevention to resilience

The report makes a subtle but important shift: from prevention to resilience.

Ransomware Recovery as a Service (RRaaS) focuses on decrypting data without paying criminals, minimizing downtime, and preventing repeat targeting. This signals a recognition that breaches are inevitable the question is recovery speed.

But resilience does not neutralize the dark web economy.

As long as stolen data, spoofed domains, and brand impersonation remain profitable, Indian enterprises will remain targets.

The emerging reality

India is at an inflection point. On one side, it is a digital powerhouse with rapid enterprise expansion and deep consumer adoption. On the other, it is feeding a structured cybercrime marketplace that monetizes brand value, regional vulnerabilities, and human trust.

The dark web economy is organized. Malware hotspots are territorial. Social engineering is scalable. AI-driven attacks are emerging.

The question is no longer whether Indian brands are being targeted.

The real question is: Are India's most digitally advanced states prepared for the fact that they are now permanent cyber frontlines?