

Indian IT Firms Face Highest Credential Theft Attempts on Dark Web, Reveals Seqrite



As India's IT sector continues to power global digital infrastructure, it is also becoming a high-value target for credential theft and identity compromise. Stolen login credentials, increasingly traded and weaponised on the dark web, are emerging as one of the most effective entry points for large-scale cyberattacks.

Amidst this, [Seqrite](#), the enterprise security arm of [Quick Heal Technologies Limited](#), a global provider of cybersecurity solutions, has identified a growing concentration of credential theft attempts targeting Indian IT firms, driven by their access to global

systems, intellectual property, and interconnected enterprise networks.

Credential theft is no longer a standalone attack. It is the starting point of a broader intrusion chain. Attackers harvest login data through phishing campaigns, malware infections, and compromised applications, and then deploy these credentials across multiple systems to gain persistent access, escalate privileges, and execute data exfiltration or ransomware attacks.

Insights from the *India Cyber Threat Report 2026*, developed by Seqrite Labs, highlight the scale of this risk. With **265.52 million detections recorded across more than 8 million endpoints**, the threat ecosystem is characterised by continuous, automated attack activity.

The report further indicates that **Trojans, accounting for nearly 43 percent of detections**, often act as the primary payload for credential theft, enabling attackers to capture login information and deploy secondary exploits. Once compromised, these credentials are frequently circulated on dark web marketplaces, making them accessible to multiple threat actors.

India's IT firms are particularly exposed due to their extensive use of cloud platforms, remote access systems, and third-party integrations. A single compromised credential can provide access to multiple environments, significantly amplifying the potential impact.

Beyond operational risk, credential theft also carries significant regulatory implications. Under the Digital Personal Data Protection (DPDP) Act, 2023, organisations are responsible for protecting personal and sensitive data from unauthorised access. Credential compromise can lead to data breaches involving customer information, employee records, and intellectual property, triggering compliance failures and financial penalties.

Mitigating this risk requires a shift toward identity-first security. Organisations must implement zero-trust frameworks, enforce multi-factor authentication across all access points, and continuously monitor credential exposure across external environments, including the dark web. In this context, solutions such as **Seqrite Digital Risk Protection Service** enable organisations to detect exposed credentials and monitor threat activity beyond organisational boundaries. **Seqrite Data Privacy** further strengthens compliance posture by ensuring visibility and control over sensitive data across systems.

At the endpoint and user level, **Quick Heal Total Security** and **Quick Heal AntiFraud.AI** provide additional safeguards by preventing malware infections and detecting suspicious behaviour linked to credential misuse. The rise in credential theft attempts underscores a fundamental shift in cyber strategy. Attacks are no longer focused on breaking systems. They are focused on acquiring access. As the threat landscape evolves, identity will remain the most targeted and the most critical layer of defense.