



Credential theft surges as Indian IT firms see 265.52 mn detections: Report

With 265.52 million detections across over 8 million endpoints, credential theft and identity compromise has emerged as a primary entry point for large-scale cyberattacks against Indian IT firms, a report said on Monday.

The report from Seqrite said the enterprise security arm of Quick Heal Technologies Limited said the threat ecosystem is characterised by continuous, automated attack activity, as India's IT sector has become 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, the report noted.

Such a modus operandi enables attackers to move laterally, escalate privileges and carry out data exfiltration or ransomware campaigns.

Seqrite 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.

Trojans accounted for nearly 43 per cent of detections and often act as the primary payload for harvesting login information. Attackers combine phishing, malware and compromised applications to capture credentials that are then circulated on dark-web marketplaces, the firm said.

The report warned that 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.

Under the Digital Personal Data Protection Act, 2023, organisations are responsible for protecting personal and sensitive data. Credential compromise can therefore trigger breaches involving customer information, employee records, and intellectual property, triggering compliance failures and financial penalties.

The report urged an identity-first security framework, where organisations must implement zero-trust frameworks, enforce multi-factor authentication across all access points and monitor credential exposure beyond organisational boundaries.