ET CISO.in
From The Economic Times

Seqrite warns of rising cryptojacking, targeted ransomware

Cybercriminals are shifting towards stealthy monetization tactics like cryptojacking and targeted ransomware, prioritizing silent infiltration and long-term exploitation over immediate disruption. These evolving threats, detailed in Seqrite's India Cyber Threat Report 2026, necessitate continuous visibility and adaptive defenses to counter covert access and data exfiltration.

As cyberattacks continue to evolve in sophistication and intent, Seqrite, a global provider of cybersecurity solutions, has identified a growing shift towards stealth-oriented monetisation tactics, particularly cryptojacking and low-volume, high-impact ransomware campaigns.

Unlike traditional ransomware attacks designed for immediate disruption and visibility, newer threat models are increasingly engineered for persistence, silent infiltration, and long-term monetisation. Attackers are now prioritising covert access to enterprise infrastructure, enabling them to exploit computing resources, exfiltrate sensitive data, or selectively deploy ransomware against high-value targets while remaining undetected for extended periods.

Insights from the India Cyber Threat Report 2026, developed by Seqrite Labs, indicate that cybercriminals are steadily moving towards attacks that maximise operational and financial impact without triggering immediate detection. The report recorded 265.52 million detections across more than 8 million endpoints, averaging 505 detections every minute, underscoring the scale and persistence of modern cyber threats.

One of the emerging concerns within this landscape is cryptojacking, where attackers secretly hijack enterprise systems to mine cryptocurrency using organisational computing power. These attacks often operate silently in the background, degrading system performance, increasing infrastructure costs, and creating hidden entry points for more severe compromises. Because cryptojacking prioritises persistence over disruption, organisations frequently remain unaware of infections for prolonged periods.

At the same time, ransomware operations are becoming more selective and intelligence-driven. Rather than pursuing mass-scale encryption campaigns, attackers are increasingly targeting critical systems, high-value data repositories, and operational choke points capable of causing disproportionate business disruption. These low-volume but high-impact attacks are often preceded by credential theft, lateral movement, and extensive reconnaissance, allowing threat actors to maximise leverage while minimising visibility.

The India Cyber Threat Report 2026 further highlights that Trojans and infectors together account for nearly 70 percent of all threats, reinforcing how attackers continue to rely on deceptive entry points such as phishing links, malicious downloads, compromised credentials, and user interactions to establish initial access. Once embedded within enterprise environments, these threats can remain dormant while enabling long-term exploitation.

The implications extend beyond operational disruption. Under the Digital Personal Data Protection (DPDP) Act, 2023, organisations are required to safeguard personal and sensitive data across their digital environments. Stealth-oriented attacks involving data exfiltration or prolonged unauthorised access can

expose organisations to regulatory penalties, compliance violations, and reputational damage, particularly where breaches remain undetected for extended periods.

Addressing these threats requires organisations to move beyond perimeter-centric defenses toward continuous visibility and intelligence-led security operations. Continuous endpoint monitoring, behavioural analytics, anomaly detection, zero-trust architectures, and proactive threat hunting are becoming essential in identifying attacks that deliberately avoid traditional detection mechanisms.

In this context, solutions such as Seqrite XDR enable organisations to correlate suspicious activity across endpoints, networks, and cloud environments to detect stealth-oriented attack behaviour in real time. Seqrite Data Privacy further supports DPDP compliance through automated data discovery, classification, and governance, while Seqrite Digital Risk Protection Service helps enterprises monitor external threat exposure and identify compromise indicators before escalation occurs.

At the user and endpoint level, Quick Heal Total Security and Quick Heal AntiFraud.AI provide an additional layer of defense by blocking malicious payloads, identifying suspicious behavioural patterns, and preventing fraud-led compromise initiated through phishing or deceptive digital interactions.

The rise of cryptojacking and selective ransomware reflects a broader transformation in cybercrime economics. Attackers are no longer solely pursuing visibility or immediate disruption. Increasingly, the objective is silent monetisation, persistent access, and strategic exploitation of trust, infrastructure, and data.

As the threat landscape evolves, organisations that prioritise continuous cyber resilience, visibility, and adaptive defense strategies will be better positioned to mitigate the next generation of stealth-driven attacks.