Seqrite finds cyber attacks on Indian critical infra from cross-border threat actors

Updated - August 21, 2024 at 02:32 PM. | Hyderabad

These advanced persistent threats (APTs), allegedly orchestrated by multiple Pakistan-based threat actors, mark a significant escalation in cyber operations against India’s defense and infrastructure sectors

BY K V KURMANATH

Seqrite, the enterprise arm of Quick Heal Technologies Limited, has exposed a series of sophisticated cyber campaigns targeting critical Indian government entities.

These advanced persistent threats (APTs), allegedly orchestrated by multiple Pakistan-based threat actors, mark a significant escalation in cyber operations against India’s defense and infrastructure sectors.

The research, conducted by the APT team at Seqrite Labs, found a complex network of interconnected APT groups, including Transparent Tribe (APT36), SideCopy, and RusticWeb. These groups have been observed sharing infrastructure, tactics, and malware components, indicating an unprecedented level of coordination among these actors.

The campaigns specifically targeted the Indian Air Force, shipyards, and ports, demonstrating a clear focus on India's strategic assets.

Seqrite's research team conducted an in-depth technical analysis of the malware used in these campaigns. They found that the attackers were testing their stager evasion against anti-virus solutions at locations in Pakistan.

Concurrently, victim traffic from India, typically observed from C2 servers in Germany, was being routed through IPsec protocol from Pakistani IP addresses, as corroborated by Team Cymru.

"The APT groups demonstrated sophisticated social engineering tactics, leveraging themes such as salary increments, naval project reports, and government documents as lures. Many of these decoys were based on publicly available documents, showcasing the attackers' efforts to create convincing pretexts for their phishing campaigns," the Seqrite report said.

The convergence of tactics among these APT groups represents a significant evolution in the cyber threat landscape facing India. This level of coordination and sophistication demands a reassessment of cybersecurity strategies at the highest levels of government and critical infrastructure.

A key finding of the investigation was the discovery of open directories hosting malware linked to both Transparent Tribe and SideCopy.

Researchers found a single-domain hosting payload for both SideCopy and APT36, targeting Windows and Linux environments respectively. This overlap, along with shared command and control (C2) infrastructure, strongly suggests a convergence of operations among these previously distinct threat actors.

“The sophistication of these campaigns is evident in their use of advanced evasion techniques. SideCopy was observed employing updated HTML Application (HTA) files, similar to those used by the SideWinder APT group, to evade detection,” the report said.

“The group also introduced new payloads, including a tool called Cheex for document and image theft, a USB copier for exfiltrating files from attached drives, and deployments of the FileZilla application and SigThief scripts,” it said.

Seqrite’s analysis uncovered several novel malware variants. A new .NET-based payload named Geta RAT was identified, incorporating browser-stealing functionality from Async RAT. Another variant, Action RAT, was observed being side-loaded by charmap.exe, a deviation from previously used system binaries.