Over 650 Cyberattacks Target India Amid ‘Operation Sindoor’ Strikes: Report

Seqrite Labs uncovers nation-state backed campaigns aimed at defence, healthcare, and telecom sectors during geopolitical escalation

As India carried out precision strikes against terror infrastructure in Pakistan-administered Kashmir under ‘Operation Sindoor’, a parallel cyber offensive targeted Indian institutions with over 650 incidents reported between 7 and 10 May, according to a threat intelligence report by Seqrite Labs, the cybersecurity arm of Quick Heal Technologies.

Seqrite identified the cyberattacks as part of a coordinated campaign launched by Pakistan-aligned threat actors who exploited heightened public concern after the 22 April Pahalgam terror attack. The attackers used spear-phishing emails with malicious attachments like Final_List_of_OGWs.xlam and Preventive_Measures_Sindoor.ppam, disguising them as official government advisories to lure unsuspecting users.

Forensic analysis traced the deployment of Ares RAT, a sophisticated variant of APT36’s Crimson RAT malware. These attacks established covert connections to command-and-control (C2) servers and spoofed Indian domains like nationaldefensecollege[.]com and zohidsindia[.]com to evade detection.

The campaign was not limited to any one sector. Seqrite’s telemetry recorded denial-of-service attacks on telecom giants like Jio and BSNL, credential theft attempts at leading healthcare institutions including AIIMS and Apollo, and defacements of state-run educational portals.

Hacktivist collectives such as #OpIndia and #OperationrSindoor amplified the attacks on social media and Telegram, claiming to leak sensitive data from municipal databases and defence contractors.

These operations were carried out using infrastructure hosted in countries like Russia, Germany, and Indonesia, helping attackers mask their true origins. Malicious file formats like .ppam and .lnk triggered PowerShell scripts that disabled antivirus tools, exfiltrated sensitive communication data, and even deployed ransomware into hospital systems.

“In today’s era of hybrid warfare, cyberattacks are a key weapon—used not only to disrupt critical systems but to destabilise economies and societies,” said Neehar Pathare, MD, CEO and CIO, 63SATS Cybertech. “It’s not just about safeguarding personal data anymore. Each compromised device can become an entry point for larger, coordinated attacks. Digital safety is now a patriotic duty—because securing your phone or laptop is part of securing the nation.”

The Seqrite report outlines how the traditional lines between state-sponsored espionage and hacktivist operations are blurring. The simultaneous use of evolved malware, spoofed communication channels, and psychological operations paints a picture of a digitally synchronised effort to destabilise India’s digital infrastructure during a period of military tension.

“The cyberattack has not been limited to government and military houses, but has now reached into our homes, devices, and everyday digital behaviours,” said Saloni Jain, Co-Founder, Plus91Labs. “Hackers are exploiting human emotions—urgency, fear, trust—by circulating malicious links and documents disguised as government alerts or job offers. Vigilance is non-negotiable now.”