Cyber hackers launched 650 attacks on Indian infrastructure between May 7–10: Report

Synopsis The cyber assault by Pakistan-aligned actors began on April 17, weeks before India's counterterrorism strikes under Operation Sindoor. Quick Heal Technologies' Seqrite Labs, a malware analysis facility, identied 650 spear-phishing attacks, malware infections, website defacements, and data leaks carried out by 35 hacktivist groups.

Over 650 cyber incidents were targeted at India's critical sectors in a coordinated oensive cyber campaign, launched by Pakistan-aligned state and non-state actors during heightened military tensions earlier this month.

Quick Heal Technologies' Seqrite Labs, a malware analysis facility, identied spear-phishing attacks, malware infections, website defacements, and data leaks carried out by 35 hacktivist groups. Of these, seven groups are new entrants. These are — Death Slash Cyber Security, Rabbit Cyber Team, Red Wolf Cyber, Dark Cyber Gang, Moroccan Black Cyber Army, Ghosts of Gaza and Tengkorak Cyber Crew, the company said.

The cyber assault began on April 17, weeks before India's counterterrorism strikes between May 7-10. The attackers used malicious documents disguised as oicial advisories, named as "Final_List_of_OGWs.xlam" and "Preventive_Measures_Sindoor.ppam" to deploy malware.

At the heart of this digital siege was APT36, a Pakistan-linked advanced persistent threat (APT) group known for targeting Indian defense and government agencies, Seqrite said.

The attackers also spoofed legitimate Indian domains such as nationaldefensecollege[.]com and zohidsindia[.]com, using them to deliver payloads and communicate with command-and-control (C2) servers hosted at foreign locations. Infrastructure behind the operation was masked using VPS (virtual private servers) in Russia, Germany, Indonesia, and Singapore.

"This was not a standalone cyber espionage mission. It was a digitally coordinated war game," Seqrite Labs said in a report released Friday. "APT36's evolved tactics combined with simultaneous hacktivist disruptions show how cyber operations have merged with psychological warfare."

Hacktivist groups used hashtags like #OpIndia and #OperationSindoor, claiming responsibility for data leaks from municipal databases, defense contractors, telecom operators and hospital networks.

“Operation Sindoor is a stark reminder of how modern conicts transcend physical borders,” said Seqrite in its advisory. “The convergence of nation-state cyber units and ideologically driven hacktivists signals a new era of digital warfare—one designed to sow disruption, distrust, and disinformation.”