

## Cyber pirates at large, India readies moats

### Synopsis

The Indian Computer Emergency Response Team (CERT-In), Reserve Bank of India (RBI), Securities and Exchange Board of India (Sebi) and defence ministry have issued several advisories to energy utilities, telecom networks, banks and stock exchanges, telling them to strengthen protections against cyber espionage and hacktivist groups, said people with knowledge of the matter.



Cybersecurity threats against India’s critical infrastructure companies are mounting as several state actors in Europe, Russia, Israel, Iran and Southeast Asia are on the hunt for data they can steal, with the possible intent of crippling and blackmailing them for ransom.

The Indian Computer Emergency Response Team (CERT-In), Reserve Bank of India (RBI), Securities and Exchange Board of India (Sebi) and defence ministry have issued several advisories to energy utilities, telecom networks, banks and stock exchanges, telling them to strengthen protections against cyber espionage and hacktivist groups, said people with knowledge of the matter.

CERT-In is the country’s nodal cybersecurity agency. As the West Asia conflict intensifies, there is a looming threat of cyber warfare that could cripple critical global infrastructure.

“Companies are extremely concerned about the evolving threat landscape and vulnerabilities of the country’s critical infrastructure, particularly those run on legacy systems,” said Sundareshwar Krishnamurthy, partner, cybersecurity, PwC India. “Energy utilities, banks and aviation networks in the Middle East have already emerged as prime targets for state-backed actors, with several recent breaches. If tensions continue to escalate, cyber warfare could spill beyond conflict zones and trigger

wider economic disruptions.” In response, utilities have begun urgent stress tests to identify and plug vulnerabilities. Security firms are actively monitoring groups such as Handala and Seedworm. These typically state-backed entities are called advanced persistent threat (APT) groups. Seqrite, the enterprise security arm of Quick Heal Technologies, has uncovered Operation CamelClone, an active, multi-region cyber espionage campaign targeting government, defence, diplomatic and energy organisations in Algeria, Mongolia, Ukraine and Kuwait, according to a report the company shared with ET.

Attackers use phishing emails that are almost identical to communications from ministries and military departments. Once malware infects the system, it steals reports, policy drafts and even messaging data, such as Telegram sessions, according to the report. Security firms are also monitoring the Handala Hack Team, a pro-Palestinian hacktivist group widely assessed to be a state-sponsored entity operated by Iran's Ministry of Intelligence and Security.

Last week, Handala claimed responsibility for breaching the personal email of US Federal Bureau of Investigation (FBI) director Kash Patel and leaking his personal photos. Earlier in March, the group wiped out 50 terabytes of data belonging to Stryker Corp., the American medical device maker. It has also leaked the personal data of senior Israeli military and political figures, including Benny Gantz and Naftali Bennett, as a form of psychological warfare. The US government has designated Handala as a front for Iranian intelligence and currently offers a \$10 million reward for information leading to the identification of its members.

Iranian APT group Seedworm is also regarded as a persistent threat. The group is also known as MuddyWater. Similar attacks took place during Operation Sindoor when more than 650 cyber incidents were targeted at India's critical sectors in a coordinated offensive cyber campaign by state and non-state actors. “We have been observing several offensive cyber activities lately including Distributed Denial-of-Service (DDoS) attacks, malware, phishing etc.,” said Tarun Wig, cofounder and CEO of cybersecurity firm Innefu Labs. “But a unique threat here is GPS spoofing being carried out by the Iranian military of vessels passing through the Strait of Hormuz.” GPS spoofing can cripple the defences of aircraft and ships.