Source : www.thehindu.com Date : 2019-11-07

SECURITY COMPROMISED

Relevant for: Security Related Matters | Topic: Basics of Cyber Security and related matters

Photo illustration: AP

On October 28, a user on VirusTotal identified a DTrack data dump linked with the Kudankulam Nuclear Power Plant — indicating that a system (or more) in the plant had been breached by malware. The Nuclear Power Corporation of India Ltd (NPCIL) confirmed the breach, doing a volte-face after an initial denial. Separately, WhatsApp sued the Israel-based NSO Group for the use of its 'Pegasus' spyware on thousands of WhatsApp users in the lead-up to the general elections.

These two incidents cast serious doubts on the Indian state's claims to being a legitimate power in cyberspace, both due to the vulnerability of its critical information infrastructure and blatant disregard for the fundamental rights of its citizens online. In essence, the government has signalled that it has no qualms about weakening the security of civilian digital platforms, even as it fails to secure its strategic infrastructure from sophisticated cyberattacks.

On September 4, an independent cybersecurity expert informed the National Security Council secretariat about a potential malware attack on the Kudankulam Plant. The malware used was identified as DTrack, a signature of the North Korean hacker group, Lazarus. The NPCIL claimed that the malware hit a non-critical "administrative computer" that was connected to the Internet, but not to the Nuclear Power Plant Control System. However, there is no clear indication what the said system contained, and whether valuable information stored in it could be harvested for more complex spear-phishing attacks against the NPCIL in the future.

As for Pegasus, it appears that over a two-week period in May 2019, an as-yet unknown number of Indian journalists, academics and activists were among those targeted by a government agency using Israeli spyware bought off the shelf. Following a lawsuit, the NSO Group, the Israeli company that created the spyware, released a statement claiming that it licenses its product "only to vetted and legitimate government agencies". There are but a handful of agencies that are authorised under the Information Technology Act, 2000 to intercept, monitor and decrypt data. Should the fingers point to the National Technical Research Organisation, the country's foremost TECHINT gathering agency?

There are three glaring issues highlighted by these cases. First, contrary to what the NPCIL may claim, air-gapped systems are not invulnerable. Stuxnet crossed an air gap, crippled Iran's nuclear centrifuges and even spread across the world to computers in India's critical infrastructure facilities. It is also not enough to suggest that some systems are less important or critical than others — a distributed and closed network is only as strong as its weakest link. Second, with the Indian military announcing that it will modernise its nuclear forces, which may include the incorporation of Artificial Intelligence and other cybercapabilities, the apparent absence of robust cybersecurity capability is a serious cause for concern. If it cannot secure even the outer layer of networks linking its nuclear plants, what hope does the government have of inducting advanced technologies into managing their security?

Third, the surveillance of Indian citizens through WhatsApp spyware in the lead-up to the general elections highlights once again the government's disregard for cybersecurity. It is in line with the government's ceaseless attempts at enforcing the "traceability" of end-to-end encrypted messages on WhatsApp. A backdoor, once opened, is available to any actor — good or bad. To use it without oversight belies reckless disregard for the integrity of electronic information.

Ironically, these instances point out to a weakening of India's cybersovereignty: the government comes across as incapable of protecting its most critical installations and, by rendering digital platforms susceptible to spyware, limiting its own agency to prosecute and investigate cybercrime These incidents also fly in the face of the country's claims to being a responsible power as a member of export control regimes such as the Wassenaar Arrangement. The possibility of such misuse of intrusion technologies is a frequent argument deployed by advanced economies to keep developing countries out of elite clubs.

If the Indian state plans to leverage offensive and defensive cybercapabilities, which are of course its right as a sovereign power, it needs to get serious about cybersecurity, both for its own narrow, political interests as well as those of its citizenry. There cannot be piecemeal, horses-for-courses approach: "security by obscurity" for India's nuclear power plants, and cutting-edge malware reserved for spying on citizens. The security of a billion hand-held devices are of equal strategic value to the country's nuclear assets. Only in this case, the government has been found wanting on the security of both.

Trisha Ray is a Junior Fellow at ORF's Cyber Initiative

END