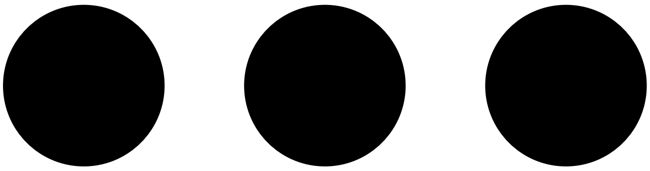
India Plagued by Series of Cyberattacks in Recent Years



Black_Kira/iStock/Getty Images Plus

India has been plagued with a series of small- and large-scale cyberattacks in recent years. For instance, although five million people globally have had their data stolen and sold on the bot market to date, 600,000 are from India, making it the morst-affected country.

These figures were based on a study by one of the world's largest VPN service providers, NordVPN of Lithuania's Nord Security.

NordVPN's study covered three major bot markets — the Genesis market, the Russian Market, and 2Easy — and discovered stolen logins such as those from Google, Microsoft, and Facebook accounts.

The stolen data entailed user logins, cookies, digital fingerprints, screenshots, and other information, with the average price for the digital identity of a person at 490 Indian rupees (around six dollars).

Hackers use bot markets to sell stolen data from victims' devices with bot malware.

Ever since the introduction of bot markets in 2018, NordVPN has been monitoring data.

Indian cybersecurity rules have become more stringent only earlier this year, with the Indian Computer Emergency Response Team mandating tech companies to report data breaches within six hours of noticing such incidents and to preserve IT and communications logs for six months.

"What makes bot markets different from other dark web markets is that they are able to get large amounts of data about one person in one place," said Marijus Briedis, chief technology officer at NordVPN.

"And after the bot is sold, they guarantee the buyer that the victim's information will be updated as long as their device is infected by the bot."

Researchers of NordVPN discovered 667 million cookies, 81,000 digital fingerprints, 538,000 auto-fill forms, numerous device screenshots, and webcam snaps in their investigation.

For some time already, India has been grappling with cybersecurity threats. In November 2022, multiple servers of the All India Institute of Medical Sciences (AIIMS), a federal government hospital that caters to ministers, politicians, and the general public, were infected, according to Reuters. The hospital where the country's top politicians typically go for treatment has caved in to a ransomware attack that has knocked out centralized records since November 23, the institution admitted in a statement.

Consequently, the institution had no choice but to operate a raft of key medical services and labs manually.

The hospital has instructed various departments to keep data individually until the restoration of systems, people familiar with the matter said, asking to remain anonymous as they were disclosing sensitive information. The downtime had a domino effect across a range of divisions, including clinics, making new patient registrations harder, the people said.

According to the hospital, "all hospital services, including outpatient, in-patient, laboratories, etc continue to run on manual mode" and "measures are being taken for cyber security." It provided no further information in the statement, except to characterize it as a cyber-security incident.

It was unclear what data the attackers may have targeted, or what their motives were. The hospital itself did not disclose what data — or whose — may have been undermined.

Police in the Indian capital Delhi, where the hospital is situated, denied any knowledge of ransom demands in response to local media reports.

However, the AIIMS incident is noteworthy given the target's significance and the duration it took to secure breached systems.

A week after the ransomware attack on AIIMS, the Indian Council of Medical Research experienced around 6,000 hacking attempts within 24 hours on November 30, based on a *Times of India* report.

These incidents are the more recent ones in a skyrocketing series of cyber-intrusions that have plagued India and other global institutions for some time. Hackers, ranging from state-sponsored agents to lone actors seeking to make quick money, take advantage of endemic lapses in cybersecurity.

Based on a study, India ranks third in terms of the highest number of internet users in the world after the United States and China. This figure has grown six-fold between 2012 and 2017, with a compound annual growth rate of 44 percent.

Notably, India was ranked among the top five countries to be plagued by cybercrime, based on a report by online security firm Symantec Corp. In the first three months of 2022 alone, India faced over 18 million cyberattacks and threats, at an average of nearly 200,000 threats every day, according to cybersecurity firm Norton.

A suspected ransomware attack in February 2022 briefly paralyzed the management information system at Jawaharlal Nehru Port Container Terminal (JNPCT), one of five marine facilities in India's top container gateway of JNPT (Nhava Sheva).

Ransomware is a type of malware that encrypts a victim's computers. The attackers then demand a ransom payment to unlock them. Payments involving ransomware have snowballed in recent years, according to U.S. government data. Besides encrypting files and demanding money, attackers also are stealing private troves of data and threatening to release it if victims fail to meet their demands.

What is more, voice call phishing, phishing on messaging apps, as well as malicious apps on the app store are seeing an increase.

Medical institutions especially are vulnerable targets because of the highly sensitive nature of the data they keep, as well as their vital societal functions.

Additionally, cybercriminals and threat actors can resort to supply-chain attacks for geopolitical and financial benefits. Such attacks have become more prevalent in the pharmaceutical, energy, and semiconductor sectors.

Cybersecurity and digital privacy firm Kaspersky (South Asia) General Manager Dipesh Kaura said, “Some countries, such as India, are still targets of advanced cybercrime. An elevated threat level is a consequence of its burgeoning economy and expected growth. Investing in infrastructure and capabilities to improve cyber intelligence by improving predictions is the only proper response. Providing our clients with such services is a crucial offering of Kaspersky. It is commendable that India has recently taken decisive steps toward enhanced cyber threat vigilance.”