Cyberattacks against governments jumped 95% in last half of 2022, CloudSek says

By by Apurva Venkat Special Correspondent

Published: 2023-01-04 · Archived: 2026-04-05 12:47:51 UTC

India, the US, Indonesia, and China accounted for 40% of the total reported cyberattacks in the government sector.

The number of attacks targeting the government sector increased by 95% worldwide in the second half of 2022 compared to the same period in 2021, according to a new report by AI-based cybersecurity company CloudSek.

The increase in attacks can be attributed to rapid digitization and the shift to remote work during the pandemic, which broadened the attack surface of government entities and paved the way for an increase in cyberwarfare waged by nation-state actors, according to the report.

Government agencies collect and store huge amounts of data, which include information about individual citizens that can be sold on the dark web. There is also a risk that national security and military data can be used by terrorist organizations.

Increase in hacktivism and ransomware

In 2022 there was an increase in so-called hacktivist activity — hacking for political purposes — which accounted for about 9% of the recorded incidents reported in the government sector. Ransomware groups accounted for 6% of the total incidents reported. LockBit was the most prominent ransomware operator, the report noted.

The number of government-sponsored attacks has also multiplied. This increase is due to the advent of offerings such as initial-access brokers and ransomware-as-a-service.

“These statistics are suggestive of the fact that cyberattacks in this particular industry are no longer limited to financial gains; rather, they are now used as a means to express support or opposition for certain political, religious, or even economic events and policies,” the report said.

“Threat actors have started developing and advertising services of dedicated criminal infrastructure which can be bought by governments or individuals and used for various nefarious purposes,” the report added.

Meanwhile, the average total cost of a breach in the public sector increased from $1.93 million to $2.07 million — a 7.25% increase between March 2021 and March 2022 — according to IBM.

KelvinSecurity, AgainstTheWest are most prominent threat actors

KelvinSecurity and AgainstTheWest were the two most prominent threat actors last year, according to Cloudsek. The two groups were the most prominent in 2021 as well.

KelvinSecurity, operating under the handle Kristina, uses targeted fuzzing and exploits common vulnerabilities to target victims. The group shares their tools for free and targets victims with common underlying technologies or infrastructure. The group publicly shares information such as new exploits, targets, and databases on cybercrime forums and Telegram. They also have a data-leak website where other threat actors can share databases, the CloudSek report notes.

AgainstTheWest started operations in October 2021 and identifies itself as APT49 or BlueHornet. It is focused on exfiltrating region-specific data and selling it on the dark web. The group has launched campaigns such as Operation Renminbi, Operation Ruble, and Operation EUSec, which targeted various countries. They also collaborate with different threat actors.

“A confidential source in contact with the group ascertained that the group was exploiting SonarQube zero-day and Swagger UI vulnerabilities,” the CloudSek report noted. SonarQube is an open-source tool by SonarSource that automates code inspections; Swagger is a set of tools for API developers from SmartBear Software.

India, US, and China are most affected

India, the US, Indonesia, and China continued to be the most targeted countries in the past two years, accounting for 40% of the total reported incidents in the government sector.

The attacks on the Chinese government were mainly attributed to APT groups. AgainstTheWest’s campaign Operation Renminbi was responsible for almost 96% of attacks against China, the report noted. The operation began as retaliation for China’s activities against Taiwan and the Uyghur community. Allegations that China was responsible for the outbreak of the pandemic also contributed to the increase in attacks.

The Indian government was the most frequently targeted in 2022 due to the hacktivist group Dragon Force Malaysia’s #OpIndia and #OpsPatuk campaigns. Several hacktivist groups joined and supported these campaigns, which led to further attacks. Government agencies in India have become popular targets of extensive phishing campaigns, the report noted.

After Russia attacked Ukraine, several state-sponsored actors and activists showed their support for Ukraine by attacking Russia. Attacks against Russia increased by over 600% during the year, as the Russian government became the fifth most targeted public sector in 2022.

To prevent future attacks government agencies need to shift to a zero-trust model, wherein it is assumed that the user identities or the network itself may already be compromised, proactively verifying the authenticity of user activity, CloudSek noted.