Another Case of a Pakistani APT Spying on Indian Military Personnel

By Catalin Cimpanu

Published: 2016-03-23 · Archived: 2026-04-05 23:37:41 UTC

Pakistani-linked threat actors have once again targeted Indian military personnel in a cyber-espionage campaign, for the third time this month alone.

The first time this happened was at the beginning of the month, when Proofpoint researchers blew the lid off a cyber-espionage campaign named **Operation Transparent Tribe**, which targeted the Indian embassies in Saudi Arabia and Kazakhstan.

The second incident came to light last week and involved the **SmeshApp** Android app, which was logging details about Indian army personnel and sending it to a server in Germany, bought by a person from Karachi, Pakistan. Google eventually removed the app.

Now, Trend Micro is reporting on a third campaign, which they've named Operation C-Major. According to the security firm, this campaign targeted Indian military officials via spear-phishing emails, distributing spyware to its victims via an Adobe Reader vulnerability.

Operation C-Major was the work of a novice

Security experts who analyzed this campaign say that the spyware was sending all stolen data to a C&C server in Pakistan. They could not confirm that this server or the person managing it was under the control of the Pakistani government or intelligence agency.

"This operation has the information theft capabilities that could be expected of the typical targeted attack - albeit not one that was particularly well-executed," Trend Micro reveals. "The attackers were unable to keep their server’s whereabouts completely hidden, leading to the discovery of information concerning the targets involved."

Trend Micro noticed that the threat actors behind this campaign had no experience in writing malware, mainly because they coded their malware in Visual Basic .NET and C#. Binaries written in these languages can be easily decompiled, and the researchers had full access to the malware's source code.

This code revealed the C&C server's IP address, where researchers discovered that the hackers left data storage directories open to public access.

The group targeted only military personnel

Researchers were able to sift through all the stolen data and easily identify what the group stole and from what targets. As initially suspected, researchers found only data related to Indian military targets.

Inside the C&C server's folders, Trend Micro found ID scans, passport scans, salary-related information, military personnel taxation details, personal photos, military training materials, and documents with data about the Indian army's strategies and tactical movements.

On the same server, researchers also discovered clues of another attack targeting Indian military officials via Android malware, with a possible connection to the SmeshApp campaign.

As the security firm concludes, it appears that even if the group lacked experience in running a cyber-espionage campaign, they compensated for their poor coding skills by using highly efficient social engineering tricks.

Some of the ID scans found on the C&C server

Source: https://news.softpedia.com/news/another-case-of-a-pakistani-apt-spying-on-indian-military-personnel-502093.shtml