Massive leak shows Chinese firm hacked foreign govts, activists: analysts

February 22 2024, by Oliver Hotham with Jing Xuan Teng in Shanghai

A trove of documents from I-Soon, a private contractor that competed for Chinese government contracts, shows that its hackers compromised more than a dozen governments, according to cybersecurity firms SentinelLabs and Malwarebytes.

A Chinese tech security firm was able to breach foreign governments,

infiltrate social media accounts and hack personal computers, a massive data leak analysed by experts this week revealed.

The trove of documents from I-Soon, a private company that competed for Chinese government contracts, shows that its hackers compromised more than a dozen governments, according to cybersecurity firms SentinelLabs and Malwarebytes.

I-Soon also breached "democracy organisations" in China's semi-autonomous city of Hong Kong, universities and the NATO military alliance, SentinelLabs researchers wrote in a blog post Wednesday.

The leaked data, the contents of which AFP was unable to immediately verify, was posted last week on the online software repository GitHub by an unknown individual.

"The leak provides some of the most concrete details seen publicly to date, revealing the maturing nature of China's cyber espionage ecosystem," SentinelLabs analysts said.

I-Soon was able to breach government offices in India, Thailand, Vietnam and South Korea, among others, Malwarebytes said in a separate post on Wednesday.

I-Soon's website was not available Thursday morning, though an internet archive snapshot of the site from Tuesday says it is based in Shanghai, with subsidiaries and offices in Beijing, Sichuan, Jiangsu and Zhejiang.

The firm did not reply to a request for comment.

Asked by AFP on Thursday about whether Beijing contracted hackers, China's foreign ministry said it was "not aware" of the case.

"As a principle, China firmly opposes all forms of cyberattacks and cracks down on them in accordance with law," spokesperson Mao Ning said.

Hacks for contracts

The leak contains hundreds of files showing chatlogs, presentations and lists of targets.

AFP found what appeared to be lists of Thai and UK government departments among the leaks, as well as screenshots of attempts to log into an individual's Facebook account.

Other screenshots showed arguments between an employee and a supervisor over salaries, as well as a document describing software aimed at accessing a target's Outlook emails.

"As demonstrated by the leaked documents, third-party contractors play a significant role in facilitating and executing many of China's offensive operations in the cyber domain," SentinelLabs analysts said.

In one screenshot of a chat app conversation, someone describes a client request for exclusive access to the "foreign secretary's office, foreign ministry's ASEAN office, prime minister's office national intelligence agency" and other government departments of an unnamed country.

Analysts who examined the files said the company also offered potential clients the ability to break into accounts of individuals on social media platform X—monitoring their activity, reading their private messages, and sending posts.

It also laid out how the firm's hackers could access and take over a person's computer remotely, allowing them to execute commands and

monitor what they type.

Other services included ways to breach Apple's iPhone and other smartphone operating systems, as well as custom hardware—including a powerbank that can extract data from a device and send it to the hackers.

Xinjiang ties

Analysts said the leak also showed I-Soon bidding for contracts in China's northwestern region of Xinjiang, where Beijing stands accused of detaining hundreds of thousands of mostly Muslim people as part of a campaign against alleged extremism. The United States has called it a genocide.

"The company listed other terrorism-related targets the company had hacked previously as evidence of their ability to perform these tasks, including targeting counterterrorism centers in Pakistan and Afghanistan," SentinelLabs analysts said.

The leaked data also revealed the fees that hackers could earn, they said, including $55,000 from breaking into a government ministry in Vietnam.

A cached version of the company's website showed the firm also runs an institute dedicated to "implementing the spirit" of President Xi Jinping's "important instructions" on developing cybersecurity education and expertise.

The FBI has said that China has the biggest hacking programme of any country.

Beijing has dismissed the claims as "groundless" and pointed to the United States's own history of cyber espionage.

Pieter Arntz, a researcher at Malwarebytes, said the leak will likely "rattle some cages at the infiltrated entities".

"As such, it could possibly cause a shift in international diplomacy and expose the holes in the national security of several countries."

Citation: Massive leak shows Chinese firm hacked foreign govts, activists: analysts (2024, February 22) retrieved 10 May 2024 from https://techxplore.com/news/2024-02-massive-leak-chinese-firm-hacked.html