New Chinese hacking tool found, spurring U.S. warning to allies

reuters.com/technology/new-chinese-hacking-tool-found-spurring-us-warning-allies-2022-02-28/

By Christopher Bing

A man holds a laptop computer as cyber code is projected on him in this illustration picture taken on May 13, 2017. REUTERS/Kacper Pempel/Illustration/

Feb 28 (Reuters) - Security researchers with U.S. cybersecurity firm Symantec said they have discovered a “highly sophisticated” Chinese hacking tool that has been able to escape public attention for more than a decade.

The discovery was shared with the U.S. government in recent months, who have shared the information with foreign partners, said a U.S. official. Symantec, a division of chipmaker Broadcom (AVGO.O), published its research about the tool, which it calls Daxin, on Monday.

“It’s something we haven’t seen before,” said Clayton Romans, associate director with the U.S. Cybersecurity Infrastructure Security Agency (CISA). “This is the exact type of information we’re hoping to receive.”

CISA highlighted Symantec’s membership in a joint public-private cybersecurity information sharing partnership, known as the JCDC, alongside the new research paper.

The JCDC, or Joint Cyber Defense Collaborative, is a collective of government defense agencies, including the FBI and National Security Agency, and 22 U.S. technology companies that share intelligence about active cyberattacks with one another.

The Chinese embassy in Washington did not respond to a request for comment. Chinese officials have previously said China is also a victim of hacking and opposes all forms of cyber attacks.

"The capabilities of this malware are remarkable and would be extremely difficult to detect without this public research," said Neil Jenkins, chief analytics officer at the Cyber Threat Alliance, a non-profit group that brings together cybersecurity experts to share data.

Symantec's attribution to China is based on instances where components of Daxin were combined with other known, Chinese-linked computer hacker infrastructure or cyberattacks, said Vikram Thakur, a technical director with Symantec.

Symantec researchers said the discovery of Daxin was noteworthy because of the scale of the intrusions and the advanced nature of the tool.

"The most recent known attacks involving Daxin occurred in November 2021," the research report reads. "Daxin's capabilities suggest the attackers invested significant effort into developing communication techniques that can blend in unseen with normal network traffic."

Daxin's victims included high-level, non-Western government agencies in Asia and Africa, including Ministries of Justice, Thakur added.

"Daxin can be controlled from anywhere in the world once a computer is actually infected," said Thakur. "That's what raises the bar from malware that we see coming out of groups operating from China."

Romans said he did not know of affected organizations in the United States, but there were infections all around the globe, which the U.S. government was helping to notify.

"Clearly the actors have been successful in not only conducting campaigns but being able to keep their creation under wraps for well over a decade," said Thakur.

(This story refiles to add missing word 'not' in paragraph 13)

Reporting by Christopher Bing; Editing by Nick Zieminski and Mark Porter