Report: Chinese state-sponsored hacking group highly active

March 30 2023, by David Rising

The flags of the U.S. and Chinese are displayed together on top of a trishaw in Beijing on Sept. 16, 2018. American cybersecurity firm says a Chinese hacking group that is likely state-sponsored and has been linked previously to attacks on U.S. state government computers is still “highly active” and is focusing on a broad range of targets that may be of strategic interest to China’s government and security services.Credit: AP Photo/Andy Wong, File

A Chinese hacking group that is likely state-sponsored and has been linked previously to attacks on U.S. state government computers is still "highly active" and is focusing on a broad range of targets that may be of strategic interest to China's government and security services, a private American cybersecurity firm said in a new report Thursday.

The hacking group, which the report calls RedGolf, shares such close overlap with groups tracked by other security companies under the names APT41 and BARIUM that it is thought they are either the same or very closely affiliated, said Jon Condra, director of strategic and persistent threats for Insikt Group, the threat research division of Massachusetts-based cybersecurity company Recorded Future.

Following up on previous reports of APT41 and BARIUM activities and monitoring the targets that were attacked, Insikt Group said it had identified a cluster of domains and infrastructure "highly likely used across multiple campaigns by RedGolf" over the past two years.

"We believe this activity is likely being conducted for intelligence purposes rather than financial gain due to the overlaps with previously reported cyberespionage campaigns," Condra said in an emailed response to questions from The Associated Press.

China's Foreign Ministry denied the accusations, saying, "This company has produced false information on so-called 'Chinese hacker attacks' more than once in the past. Their relevant actions are groundless accusations, far fetched, and lack professionalism."

Chinese authorities have consistently denied any form of state-sponsored hacking, instead saying China itself is a major target of cyberattacks.

APT41 was implicated in a 2020 U.S. Justice Department indictment that accused Chinese hackers of targeting more than 100 companies and

institutions in the U.S. and abroad, including social media and video game companies, universities and telecommunications providers.

In its analysis, Insikt Group said it found evidence that RedGolf "remains highly active" in a wide range of countries and industries, "targeting aviation, automotive, education, government, media, information technology and religious organizations."

Insikt Group did not identify specific victims of RedGolf, but said it was able to track scanning and exploitation attempts targeting different sectors with a version of the KEYPLUG backdoor malware also used by APT41.

Insikt said it had identified several other malicious tools used by RedGolf in addition to KEYPLUG, "all of which are commonly used by many Chinese state-sponsored threat groups."

In 2022, the cybersecurity firm Mandiant reported that APT41 was responsible for breaches of the networks of at least six U.S. state governments, also using KEYPLUG.

In that case, APT41 exploited a previously unknown vulnerability in an off-the-shelf commercial web application used by 18 states for animal health management, according to Mandiant, which is now owned by Google. It did not identify which states' systems were compromised.

Mandiant called APT41 "a prolific cyber threat group that carries out Chinese state-sponsored espionage activity in addition to financially motivated activity potentially outside of state control."

Cyber intelligence companies use different tracking methodologies and often name the threats they identify differently, but Condra said APT41, BARIUM and RedGolf "likely refer to the same set of threat actor or

group(s)" due to similarities in their online infrastructure, tactics, techniques and procedures.

"RedGolf is a particularly prolific Chinese state-sponsored threat actor group that has likely been active for many years against a wide range of industries globally," he said.

"The group has shown the ability to rapidly weaponize newly reported vulnerabilities and has a history of developing and using a large range of custom malware families."

Insikt Group concluded that the use of KEYPLUG malware through certain types of command and control servers by RedGolf and similar groups is "highly likely to continue" and recommended that clients ensure they are blocked as soon as they are detected.

Citation: Report: Chinese state-sponsored hacking group highly active (2023, March 30) retrieved 25 April 2024 from https://techxplore.com/news/2023-03-chinese-state-sponsored-hacking-group-highly.html