Chinese Hackers Target Taiwanese Financial Institutions with a new Stealthy Backdoor

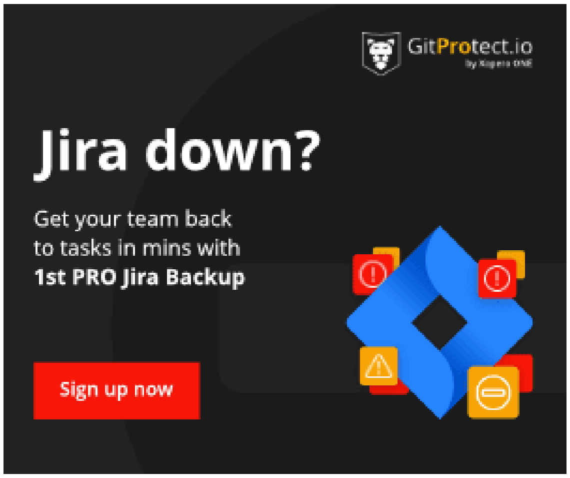
thehackernews.com/2022/02/chinese-hackers-target-taiwanese.html

February 6, 2022

A Chinese advanced persistent threat (APT) group has been targeting Taiwanese financial institutions as part of a "persistent campaign" that lasted for at least 18 months.

The intrusions, whose primary intent was espionage, resulted in the deployment of a backdoor called **xPack**, granting the adversary extensive control over compromised machines, Broadcom-owned Symantec said in a report published last week.

What's notable about this campaign is the amount of time the threat actor lurked on victim networks, affording the operators ample opportunity for detailed reconnaissance and exfiltrate potentially sensitive information pertaining to business contacts and investments without raising any red flags.



GitProtect.io
by Xopero ONE
Jira down?
Get your team back to tasks in mins with 1st PRO Jira Backup
Sign up now

In one of the unnamed financial organizations, the attackers spent close to 250 days between December 2020 and August 2021, while a manufacturing entity had its network under their watch for roughly 175 days.

Although the initial access vector used to the breach the targets remains unclear, it's suspected that Antlion leveraged a web application flaw to gain a foothold and drop the xPack custom backdoor, which is employed to execute system commands, drop subsequent malware and tools, and stage data for exfiltration.

Additionally, the threat actor used C++-based custom loaders as well as a combination of legitimate off-the-shelf tools such as AnyDesk and living-off-the-land (LotL) techniques to gain remote access, dump credentials, and execute arbitrary commands.

"Antlion is believed to have been involved in espionage activities since at least 2011, and this recent activity shows that it is still an actor to be aware of more than 10 years after it first appeared," the researchers said.

CyberSecurity

The findings add to a growing list of China-linked nation-state groups that have targeted Taiwan in recent months, what with malicious cyber activities mounted by threat actors tracked as Tropic Trooper and Earth Lusca striking government, healthcare, transportation, and educational institutions in the country.

SHARE □ □ □ □ ק
SHARE □