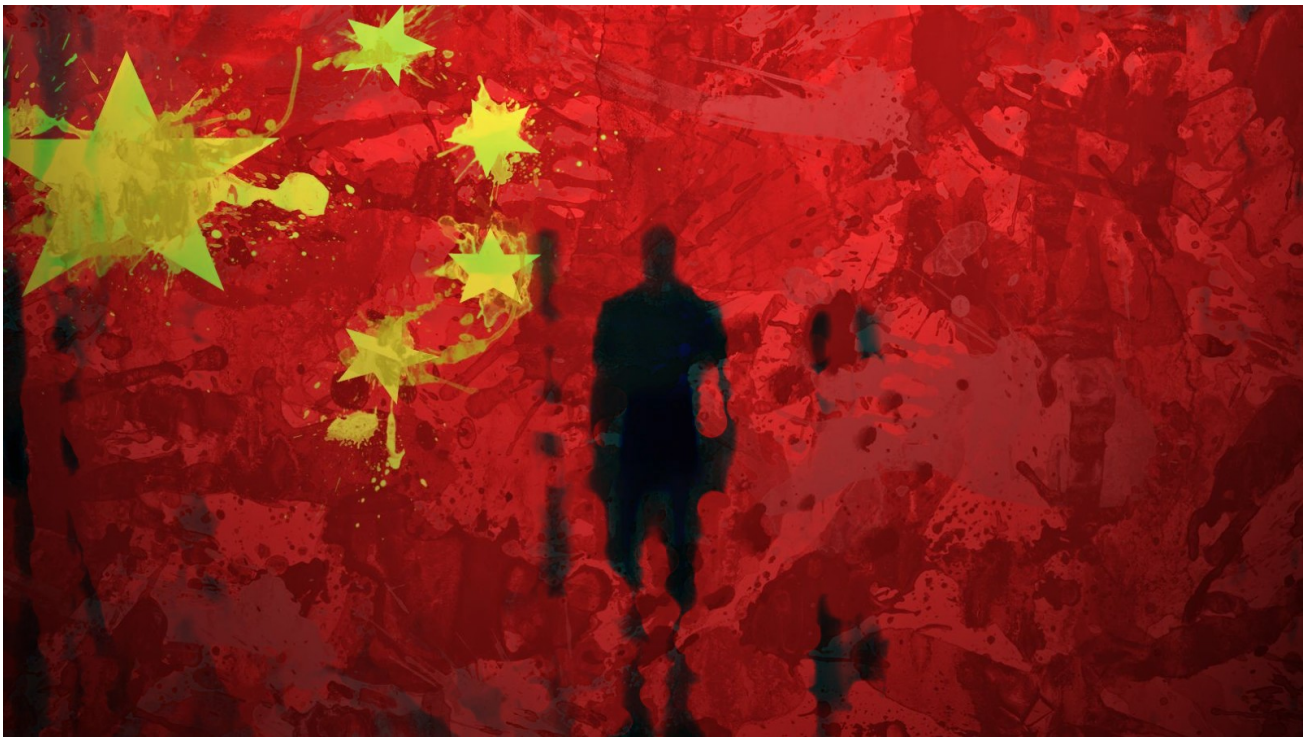
State hackers' new malware helped them stay undetected for 250 days

bleepingcomputer.com/news/security/state-hackers-new-malware-helped-them-stay-undetected-for-250-days/

Bill Toulas

By
Bill Toulas

- February 3, 2022
- 10:38 AM
- 1



A state-backed Chinese APT actor tracked as 'Antlion' has been using a new custom backdoor called 'xPack' against financial organizations and manufacturing companies.

The malware has been used in a campaign against targets in Taiwan that researchers believe spanned for more than 18 months, between 2020 and 2021, allowing the adversaries to run stealthy cyber-espionage operations.

According to a report from Symantec, a Broadcom company, shared with BleepingComputer, xPack enabled attackers to run WMI commands remotely, to leverage EternalBlue exploits, and mounted shares over SMB to deliver data to the command and control (C2) server.

In the network for 250 days

Details from one attack show that the threat actor spent 175 days on the compromised network. However, Symantec researchers analyzing two other attacks determined that the the adversary went undetected on the network for as long as 250 days.

Using custom malware unknown to threat analysts played a key role in achieving this level of stealthiness.

xPack is a .NET loader that fetches and executes AES-encrypted payloads, while it's also capable to execute system commands and stage data for exfiltration.

Symantec also spotted the following custom tools that accompanied xPack in this camapaign:

- **EHAGBPSL** – Custom C++ loader
- **JpgRun** – Custom C++ loader
- **CheckID** – Custom C++ loader based on a similar tool used by the BlackHole RAT
- **NetSessionEnum** – Custom SMB session enumeration tool
- **ENCODE MMC** – Custom bind/reverse file transfer tool
- Kerberos golden ticket tool based on the Mimikatz credentials stealer

Antlion also used various off-the-shelf and living-off-the-land (LoL) tools in combination with the above to achieve full operational capability without raising security flags.

Tools such as PowerShell, WMIC, ProcDump, LSASS, and PsExec were common in this campaign, leaving crumbs of evidence that easily blend with ordinary operating system functions.

Finally, the actors were also observed leveraging CVE-2019-1458 for privilege escalation and remote scheduling that helped execute the backdoor.

This vulnerability was recently included on CISA's list of actively exploited flaws, so it's still an attractive avenue for multiple adversaries.

"There is also evidence that the attackers likely automated the data collection process via batch scripts, while there is also evidence of instances where data was likely staged for further exfiltration, though it was not actually observed being exfiltrated from the network," explains Symantec

"In these instances, it appears the attackers were interested in collecting information from software pertaining to business contacts, investments, and smart card readers."

In the attacks dissected by Symantec's analysts, xPack was initially used to collect basic system information and running processes, and then for dumping credentials.

Afterwards, the actors returned periodically and launched xPack again to steal account credentials from several machines in the compromised organizations.

Antlion still active and dangerous

Antlion is believed to be involved in cyber-espionage activities since at least 2011, so this is an actor that has remained a threat to organizations for over a decade now.

Its interest in targeting Taiwanese firms has political extensions and is in line with the operational strategy of most Chinese state-sponsored groups.

As detailed in Symantec's report, the particular campaign focused on dumping credentials from the compromised systems and then using them to move laterally.

It's possible that Antlion shared these credentials with other Chinese hacker groups that had a different operational focus, as it is common for actors working for the same state to collaborate.

Related Articles:

Hackers target Russian govt with fake Windows updates pushing RATs

BPFDoor: Stealthy Linux malware bypasses firewalls for remote access

Chinese ‘Space Pirates’ are hacking Russian aerospace firms

Bitter cyberspies target South Asian govts with new malware

Hackers are now hiding malware in Windows Event Logs

- Antlion
- APT
- Backdoor
- China
- Hackers
- Taiwan

Bill Toulas

Bill Toulas is a technology writer and infosec news reporter with over a decade of experience working on various online publications. An open source advocate and Linux enthusiast, is currently finding pleasure in following hacks, malware campaigns, and data breach incidents, as well as by exploring the intricate ways through which tech is swiftly transforming our lives.

- Previous Article
- Next Article

Comments

Elko_NV - 3 months ago

-
-

Any good 0-day/DeepAI/Checkpoint wares out there? Choices thus far look like FalconSandbox, FortiSandbox, R80SM, ForcepointAMDetect, + running a 0-patch account. Not decided yet.

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: