China's APT41 Manages Library of Breached Certificates

By Phil Muncaster

Published: 2021-11-18 · Archived: 2026-04-05 23:21:22 UTC

A freelance Chinese APT group is actively managing a library of compromised code-signing digital certificates to support cyber-espionage attacks targeting supply chain vendors, according to Venafi.

The security vendor's latest research report details the work of APT41, an unusual group in that it has previously been observed carrying out attacks for both traditional state-sponsored cyber-espionage and personal financial gain.

Venafi claimed that using the certificates and keys that authenticate pieces of code are a key part of its tactics.

APT41 is reportedly managing a library of these certs and keys – some purchased from underground marketplaces, some obtained from other Chinese attack groups and some stolen by APT41 itself.

This shared resource allows members of the group to select the appropriate certificate for their needs, "dramatically" improving success rates, according to Venafi.

These attacks, conducted in support of China's long-term economic, military and political goals – are often directed at the digital supply chain, allowing easy compromise of downstream customers.

"Code-signing machine identities allow malicious code to appear authentic and evade security controls. The success of attacks using this model over the past decade has created a blueprint for sophisticated attacks that have been highly successful because they are very difficult to detect," explained Venafi threat intelligence specialist Yana Blachman.

"Since targeting the Windows software utility CCleaner in 2018 and Asus LiveUpdate in 2019, APT41's methods continue to improve. Every software provider should be aware of this threat and take steps to protect their software development environments."

Once the targeted downstream organization is compromised via secondary malware, APT41 then moves laterally across networks, using stolen credentials and reconnaissance tools to steal IP and customer data, the report claimed.

APT41 was responsible for one of the most widespread Chinese cyber campaigns of recent years when it exploited Citrix and Zoho endpoints at scores of global organizations across multiple verticals.