LevelBlue - Open Threat Exchange

By PetrP.73

Archived: 2026-04-05 18:47:03 UTC

MISSION2025 - APT41.

CVE: 6

APT41, also known as MISSION2025, is a Chinese state-sponsored advanced persistent threat group that has been active since at least 2012. The group is particularly focused on cyberespionage and financially motivated attacks, using sophisticated techniques to target a wide range of industries globally. Their operations are aligned with China's economic strategy, notably the "Made in China 2025" initiative, emphasizing intellectual property theft and corporate espionage.

- 161 Subscribers

Threat Research | FireEye Inc

Find out more about FireEye.com, the world's leading cyber security company, which provides security services to more than 1.5 million customers across the globe, and offers a wide range of products and services.

- 17 Subscribers

HDRoot Bootkit

FileHash-MD5: 27 | **URL:** 5

(Kaspersky) Some time ago while tracking Winnti group activity we came across a suspicious 64-bit sample. It was a standalone utility with the name HDD Rootkit for planting a bootkit on a computer. Once installed the bootkit infects the operating system with a backdoor at the early booting stage. The principles of this bootkit's work, named HDRoot, have been described in the first part of our article. During our investigation we found several backdoors that the HDRoot bootkit used for infecting operating systems. These backdoors are described in this part of the article.

- 373,972 Subscribers

Source: https://otx.alienvault.com/browse/pulses?q=tag:hdroot