LevelBlue - Open Threat Exchange

By PetrP.73

Archived: 2026-04-05 18:55:23 UTC

Revisiting MoonBounce: Research Notes

FileHash-MD5: 1 | **FileHash-SHA1:** 1

The MoonBounce implant has been identified as a sophisticated UEFI firmware implant associated with the APT group APT41, also known as Winnti. This malware targets the Unified Extensible Firmware Interface (UEFI), enabling it to operate at a low level, essentially within the system's firmware. Once embedded, MoonBounce is capable of surviving operating system reinstallations and can remain undetected by conventional antivirus solutions. The primary characteristic of MoonBounce is its ability to manipulate the firmware of the device, allowing it to execute malicious payloads during the boot process, thus facilitating persistent access to the compromised system. This UEFI implant represents a significant threat due to its potential to compromise devices at the hardware level.

- 161 Subscribers

APT41 Cyber-Espionage Campaign Targets U.S. Policy Institutions

CVE: 6 | **FileHash-MD5:** 3 | **FileHash-SHA1:** 3 | **FileHash-SHA256:** 6

In April 2025, the advanced persistent threat group APT41, known for its ties to China, initiated a targeted cyber-espionage campaign aimed at a U.S.-based non-profit organization influential in shaping government policy and foreign relations. This operation is consistent with China's strategic interests in acquiring intelligence that allows for better anticipation of U.S. foreign policy moves and diplomatic actions. APT41's methods in this campaign exhibited notable technical sophistication and operational discipline. The group employed tools and techniques that mirror those used in previous campaigns, specifically referencing their affiliations with campaigns dubbed Kelp (Salt Typhoon) and Space Pirates. The nature of these tactics suggests a comprehensive approach in which APT41 utilizes overlapping strategies to maximize the efficacy of their espionage efforts.

- 161 Subscribers

- 212 Subscribers

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

- 103 Subscribers

- 47 Subscribers

RevivalStone：Winnti Group

FileHash-MD5: 3 | **FileHash-SHA1:** 3 | **FileHash-SHA256:** 7 | **YARA:** 4

Winnti Group, a group of security experts, has announced it will hold a conference on "new puzzle" for the next two years. Â£1.5bn..-

- 258 Subscribers

Kiteshield Packer is Being Abused by Linux Cyber Threat Actors

FileHash-MD5: 11 | **FileHash-SHA1:** 10 | **FileHash-SHA256:** 10 | **URL:** 1 | **YARA:** 1 | **Hostname:** 1

A team of researchers from XLab has uncovered a new method of hiding malware in ELF files on Linux, and discovered that it is being used by cybercrime groups to evade antivirus systems.

- 41 Subscribers

- 841 Subscribers

- 47 Subscribers

Threat Intel Report - W51-2024

FileHash-MD5: 13 | **FileHash-SHA1:** 13 | **FileHash-SHA256:** 16 | **URL:** 196 | **Domain:** 76 | **Hostname:** 79

This is a cyber-advisory document, presenting the compiled cyber threat intelligence sourced from various channels and tools. These are weekly base recommendations to all IT Administrators and CISOs to take corrective actions to upgrade their security infrastructure against newly identified threats and attacks in this week. Security is a continuous process, and it has to be reviewed and audited on a continuous manner through manual or automated tools. These details may be used as an additional layer to verify the current security posture of an organization against latest cyber trends.

- 105 Subscribers

- 841 Subscribers

- 505 Subscribers

Author Url

- 841 Subscribers

- 258 Subscribers

Test3-17 Dec

FileHash-MD5: 17 | **FileHash-SHA1:** 1 | **FileHash-SHA256:** 1 | **Hostname:** 2

- 258 Subscribers

Black and White Domination: Glutton Trojan Lurks in Mainstream PHP Frameworks

FileHash-MD5: 17 | **FileHash-SHA1:** 1 | **FileHash-SHA256:** 1 | **Hostname:** 2

The XLab threat detection system uncovered an advanced PHP trojan named Glutton, which has been active for over a year without detection. Glutton targets both legitimate businesses and cybercriminal operations, infiltrating popular PHP frameworks like ThinkPHP and Laravel. It employs modular components for information theft, backdoor installation, and code injection. The malware can deploy both ELF-based Winnti backdoors and PHP-based backdoors, demonstrating cross-platform capabilities. Notably, Glutton also targets black market operations by infecting their systems, potentially aiming to steal from cybercriminals themselves. The attack framework operates without leaving files on disk, making detection challenging.

- 373,974 Subscribers

staging test 2

FileHash-MD5: 17 | **FileHash-SHA1:** 1 | **FileHash-SHA256:** 1 | **Hostname:** 2

- 258 Subscribers

staging test -f1

FileHash-MD5: 17 | **FileHash-SHA1:** 1 | **FileHash-SHA256:** 1 | **Hostname:** 2

- 258 Subscribers

- 841 Subscribers

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