LevelBlue - Open Threat Exchange

By Arek-BTC

Archived: 2026-04-06 15:34:06 UTC

Query Registry, Technique T1012 - Enterprise | MITRE ATT&CK®

CVE: 1 | **URL:** 6 | **Domain:** 2 | **Hostname:** 2

Adversaries can access the Windows Registry to gather information about the operating system, configuration, and installed software, as well as to make modifications to the system's registry, according to a report published in the Security Research Institute (CTI).

- 122 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

- 841 Subscribers

New SprySOCKS Linux malware used in cyber espionage attacks

CVE: 9 | **FileHash-MD5:** 1 | **FileHash-SHA1:** 1 | **FileHash-SHA256:** 1 | **Domain:** 1 | **Hostname:** 4

A Chinese espionage-focused hacker tracked as 'Earth Lusca' was observed targeting government agencies in multiple countries, using a new Linux backdoor dubbed 'SprySOCKS.' Trend Micro's analysis of the novel backdoor showed that it originates from the Trochilus open-source Windows malware, with many of its functions ported to work on Linux systems. However, the malware appears to be a mixture of multiple malware as the SprySOCKS' command and control server (C2) communication protocol is similar to RedLeaves, a Windows backdoor. In contrast, the implementation of the interactive shell appears to have been derived from Derusbi, a Linux malware.

- 431 Subscribers

New SprySOCKS Linux malware used in cyber espionage attacks

FileHash-MD5: 2 | **FileHash-SHA1:** 2 | **FileHash-SHA256:** 4 | **URL:** 1 | **Hostname:** 2

A round-up of interesting technology-related links shared over the past week, as well as the latest developments in the fight against cyber espionage, malware and other malware. Â£1.

- 47 Subscribers

- 841 Subscribers

- 52 Subscribers

- 181 Subscribers

Earth Lusca Employs New Linux Backdoor, Uses Cobalt Strike for Lateral Movement

CVE: 9 | **FileHash-SHA256:** 4 | **Hostname:** 2

Earth Lusca remained active during the first half of 2023, with its attacks focusing primarily on countries in Southeast Asia, Central Asia, and the Balkans (with a few scattered attacks on Latin American and African countries). The group’s main targets are government departments that are involved in foreign affairs, technology, and telecommunications.

- 374,261 Subscribers

- 44 Subscribers

APT-41

CIDR: 1 | **CVE:** 6 | **FileHash-MD5:** 52 | **FileHash-SHA1:** 35 | **FileHash-SHA256:** 23 | **Domain:** 25 | **Hostname:** 3

APT-41

- 40 Subscribers

- 37 Subscribers

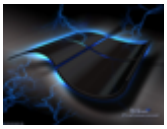
GhostEmperor: From ProxyLogon to kernel mode

FileHash-MD5: 10 | **FileHash-SHA1:** 6 | **FileHash-SHA256:** 6 | **Domain:** 7 | **Hostname:** 4

Demodex has been observed in a recent rise of attacks against Exchange servers. The malware could be used to hide and hide the source of the attack. The responsible cluster has been dubbed GhostEmperor.

- 374,261 Subscribers

- 505 Subscribers



[Identifican nuevo programa malicioso “Biopass RAT”]

nvestigadores descubrieron un nuevo programa dirigido a empresas chinas de juegos de azar en línea, en donde los usuarios son engañados para descargar un programa malicioso disfrazado de instalador legítimo para aplicaciones conocidas como Adobe Flash Player o Microsoft Silverlight, pero en realidad carga un código de Cobalt Strike o un programa previamente no documentado escrito en Python, llamado “Biopass RAT”. Biopass RAT, es un nuevo tipo de troyano de acceso remoto y posee características básicas que se encuentran en otros programas maliciosos, como la identificación del sistema de archivos, el acceso al escritorio remoto, la filtración de documentos y la ejecución de comandos. También tiene la capacidad de comprometer la información privada de sus víctimas mediante el robo de datos del navegador web y el cliente de mensajería instantánea.

- 266 Subscribers

[Hackers Spread BIOPASS Malware via Chinese Online Gambling Sites]

Cybersecurity researchers are warning about a new malware that's striking online gambling companies in China via a watering hole attack to deploy either Cobalt Strike beacons or a previously undocumented Python-based backdoor called BIOPASS RAT that takes advantage of Open Broadcaster Software (OBS) Studio's live-streaming app to capture the screen of its victims. The attack involves deceiving gaming website visitors into downloading a malware loader camouflaged as a legitimate installer for popular-but-deprecated apps such as Adobe Flash Player or Microsoft Silverlight, only for the loader to act as a conduit for fetching next-stage payloads. Specifically, the websites' online support chat pages are booby-trapped with malicious JavaScript code, which is used to deliver the malware to the victims.

- 431 Subscribers

- 14 Subscribers

- 505 Subscribers

Linux Derusbi, backdoor used by Chinese APT

A report from Fidelis Cybersecurity highlights the use of a 64-bit Linux variant of the Derusbi malware used in a series of high-profile cyber-attacks in the United States.

- 354 Subscribers

- 462 Subscribers

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