Chinese hackers abuse VLC Media Player to launch malware loader

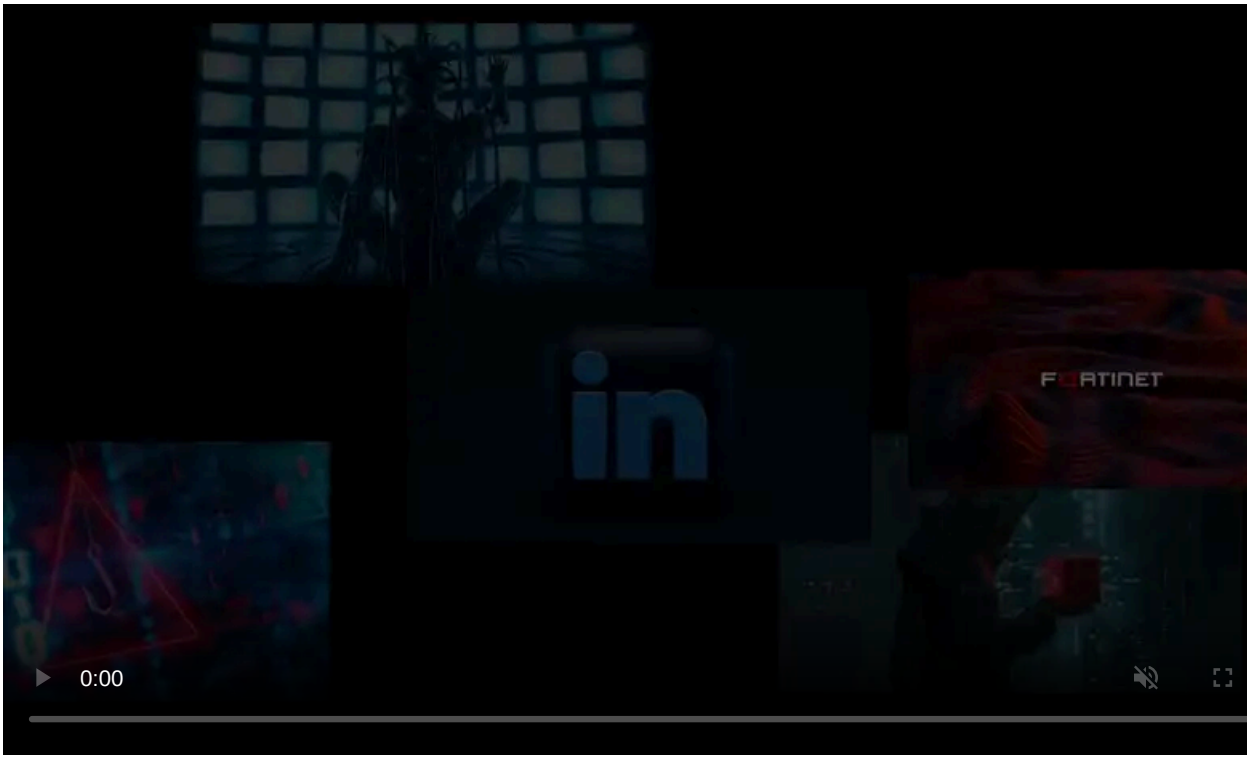
By Ionut Ilascu

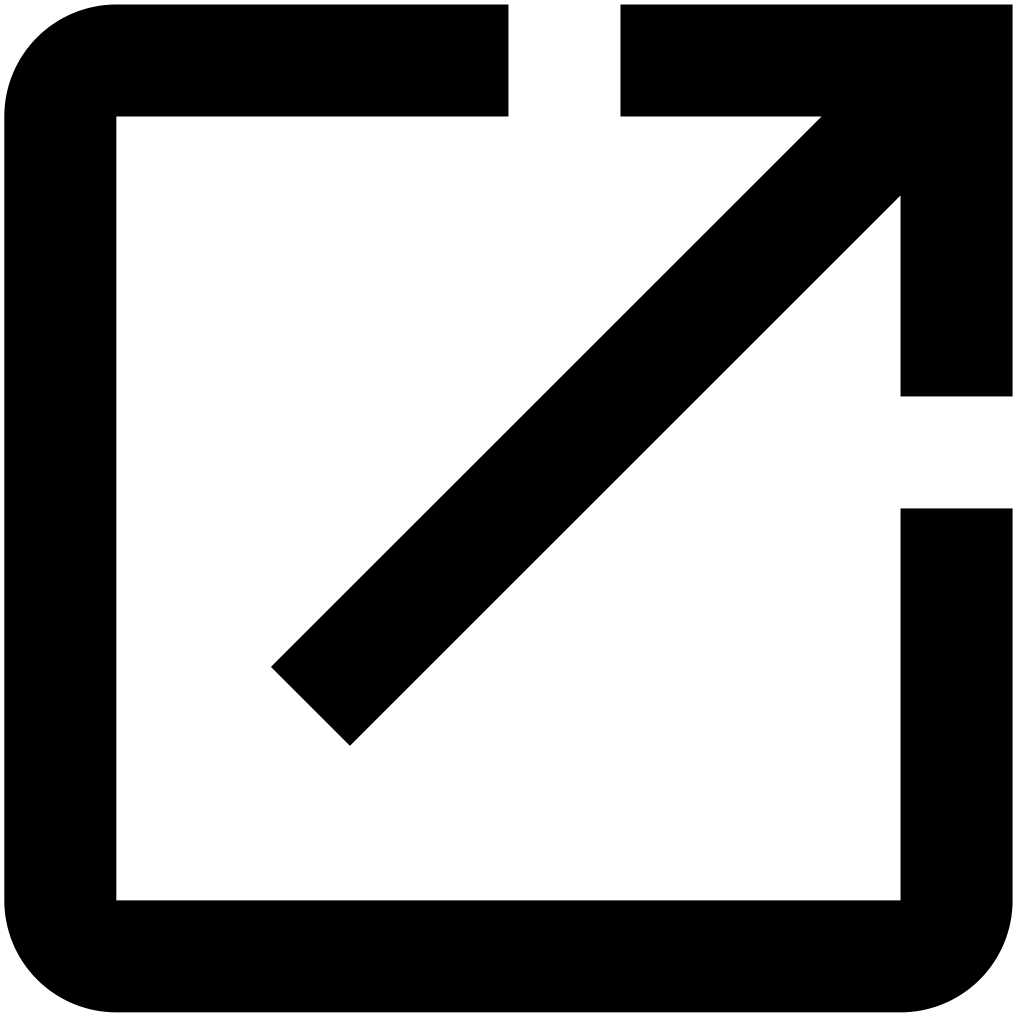
Published: 2022-04-05 · Archived: 2026-04-05 19:55:46 UTC

Security researchers have uncovered a long-running malicious campaign from hackers associated with the Chinese government who are using VLC Media Player to launch a custom malware loader.

The campaign appears to serve espionage purposes and has targeted various entities involved in government, legal, and religious activities, as well as non-governmental organizations (NGOs) on at least three continents.

This activity has been attributed to a threat actor tracked as Cicada (a.k.a. menuPass, Stone Panda, Potassium, APT10, Red Apollo) that has been active for more than 15 years, since at least 2006.


0:00



Using VLC to deploy custom malware loader

The start of Cicada's current campaign has been tracked to mid-2021 and was still active in February 2022. Researchers say that this activity may continue today.

There is evidence that some initial access to some of the breached networks was through a Microsoft Exchange server, indicating that the actor exploited a known vulnerability on unpatched machines.

Researchers at Symantec, a division of Broadcom, found that after gaining access to the target machine the attacker deployed a custom loader on compromised systems with the help of the popular VLC media player.

Brigid O Gorman of Symantec Threat Hunter Team told BleepingComputer that the attacker uses a clean version of VLC with a malicious DLL file in the same path as the media player's export functions.

The technique is known as DLL side-loading and it is widely used by threat actors to load malware into legitimate processes to hide the malicious activity.

Apart from the custom loader, which O Gorman said Symantec does not have a name but has been seen in previous attacks attributed to Cicada/APT10, the adversary also deployed a WinVNC server to gain remote control over victim systems.

The attacker also executed the Sodamaster backdoor on compromised networks, a tool believed to be used exclusively by the Cicada threat group since at least 2020.

Sodamaster runs in the system memory (fileless) and is equipped to evade detection by looking in the registry for clues of a sandbox environment or by delaying its execution.

The malware can also collect details about the system, search for running processes, and download and execute various payloads from the command and control server.

Several other utilities have been observed in this campaign include:

- RAR archiving tool - helps compress, encrypt, or archive files, likely for exfiltration
- System/Network discovery - a way for attackers to learn about the systems or services connected to an infected machine
- WMIExec - Microsoft command-line tool that can be used to execute commands on remote computers
- NBTScan - an open-source tool that has been observed being used by APT groups for reconnaissance in a compromised network

The attackers' dwell time on the networks of some of the discovered victims lasted for as long as nine months, the researchers note in a report today.

A wider focus

Many of the organizations targeted in this campaign appear to be government-related or NGOs (involved in educational or religious activities), as well as companies in the telecommunications, legal, and pharmaceutical sectors.

Symantec researchers highlight the wide geography of this Cicada campaign, which counts victims in the U.S., Canada, Hong Kong, Turkey, Israel, India, Montenegro, and Italy.

To note, only one victim is from Japan, a country that has been the focus of the Cicada group for many years.

Compared to the previous targeting from this group, which focused on Japanese-linked companies, the victims in this campaign indicate that the threat actor has broadened its interest.

While focused on Japanese-linked companies, Cicada has targeted in the past healthcare, defense, aerospace, finance, maritime, biotechnology, energy, and government sectors.

At least two members of the APT10 threat group have been charged in the U.S. for computer hacking activity to help the Chinese Ministry of State Security's (MSS) Tianjin State Security Bureau get intellectual property and confidential business information from managed service providers, U.S. government agencies, and over 45 technology companies.

Source: https://www.bleepingcomputer.com/news/security/chinese-hackers-abuse-vlc-media-player-to-launch-malware-loader/