NATIONAL CSIRT-CY

Microsoft Windows GUI 0-Day Vulnerability **14/2/2025**

Executive Summary

A newly discovered vulnerability in Microsoft Windows, identified by ClearSky Cyber Security, is reportedly being actively exploited by the Chinese state-sponsored Advanced Persistent Threat (APT) group Mustang Panda.

Analysis

The flaw involves how Windows handles files extracted from compressed "RAR" archives. When extracted into a folder, these files appear invisible in the Windows Explorer GUI, misleading users into believing the folder is empty.

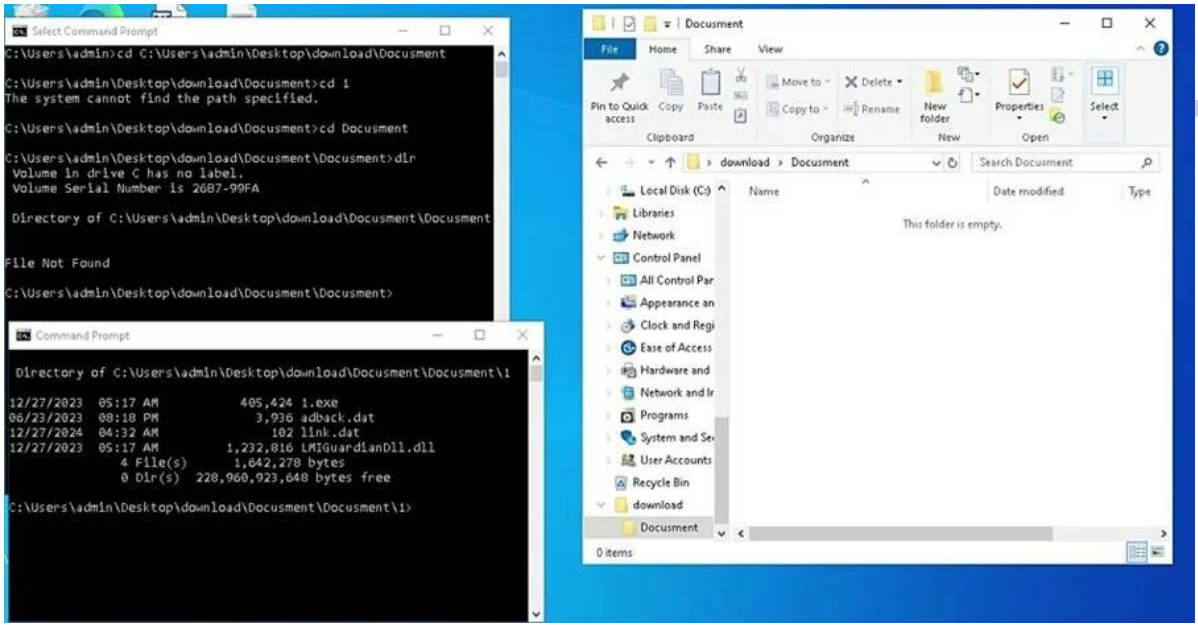
However, the files can still be accessed and executed via command-line tools if their exact path is known.

For instance:

Using the dir command reveals these hidden files, and executing attrib -s -h on system-protected files results in the creation of an unknown file type associated with an "Unknown" ActiveX component.

This exploitation method allows threat actors to conceal malicious files within seemingly benign archives, bypassing detection and enabling stealthy execution of harmful payloads.

Screenshot



Please distribute this information among your subsidiaries and partners, and also share with us any pertinent information and findings you may have (e.g IOCs, TTPs etc)

The Digital Security Authority extends its appreciation for the continued collaboration.

Disclaimer

Organizations are advised to consult with relevant cybersecurity professionals and follow best practices for their specific environments.