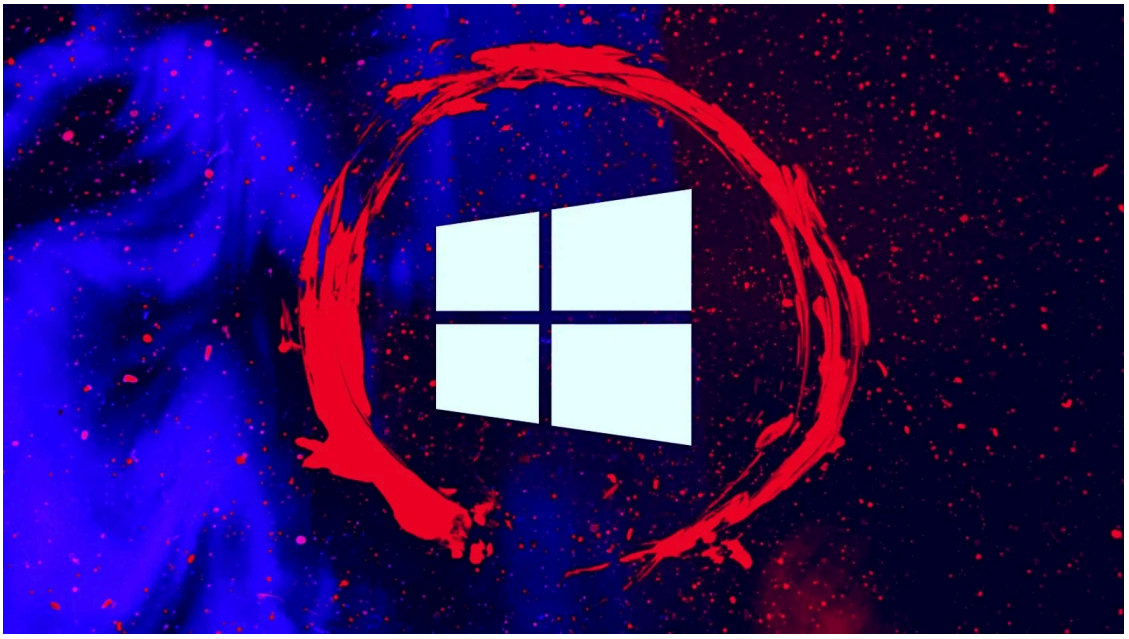
Windows MSDT zero-day now exploited by Chinese APT hackers

By Sergiu Gatlan

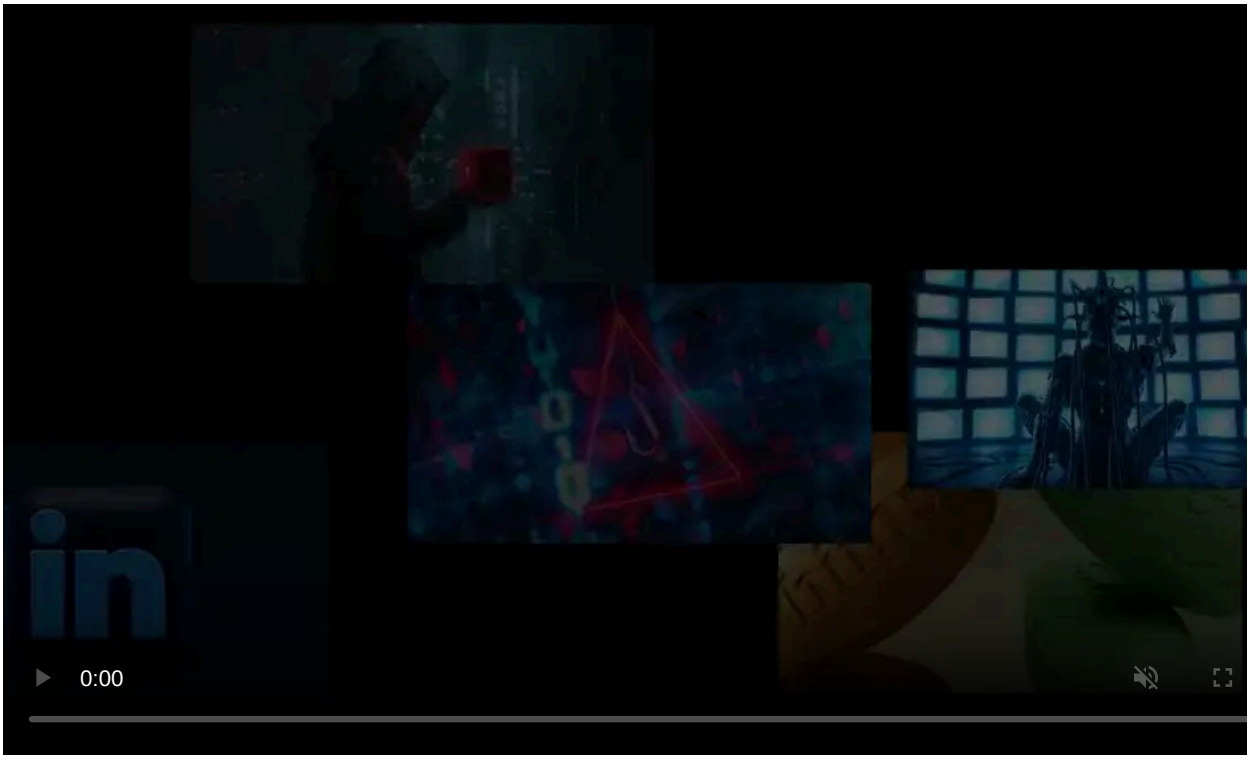
Published: 2022-05-31 · Archived: 2026-04-05 18:00:43 UTC

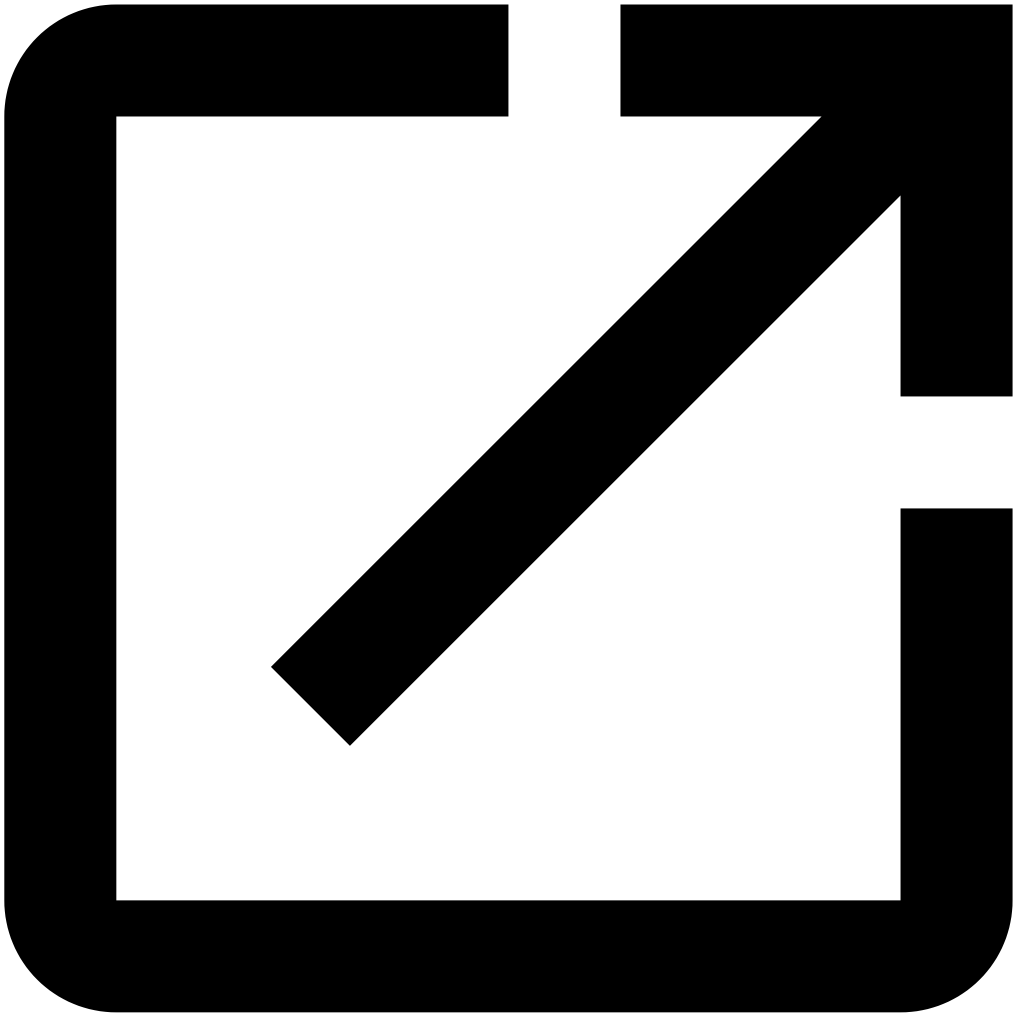


Chinese-linked threat actors are now actively exploiting a Microsoft Office zero-day vulnerability (known as 'Follina') to execute malicious code remotely on Windows systems.

Described by Microsoft as a remote code execution flaw in the Microsoft Windows Support Diagnostic Tool (MSDT) and tracked as CVE-2022-30190, it impacts all Windows client and server platforms still receiving security updates (Windows 7 or later and Windows Server 2008 or later).

Shadow Chaser Group's crazyman, the researcher who first reported the zero-day in April, said Microsoft initially tagged the flaw as not a "security-related issue," however, it later closed the vulnerability submission report with a remote code execution impact.

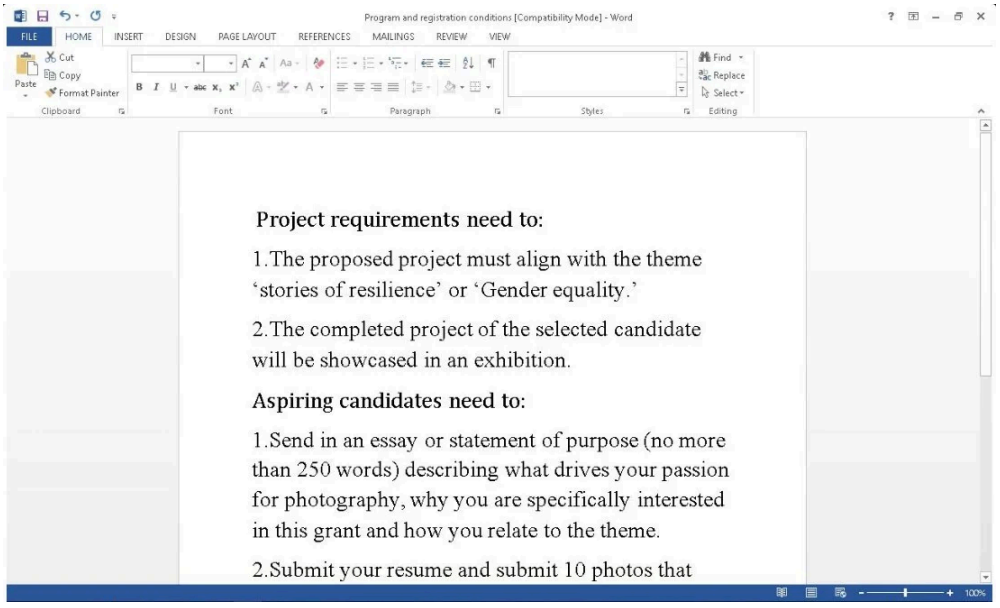

0:00



Actively exploited in the wild

The TA413 APT group, a hacking outfit linked to Chinese state interests, has adopted this vulnerability in attacks against their favorite target, the international Tibetan community.

As observed on May 30 by Proofpoint security researchers, they're now using CVE-2022-30190 exploits to execute malicious code via the MSDT protocol when targets open or preview Word documents delivered in ZIP archives.



TA413 malicious Word document (Proofpoint)

"TA413 CN APT spotted ITW exploiting the Follina 0Day using URLs to deliver Zip Archives which contain Word Documents that use the technique," enterprise security firm Proofpoint revealed today.

"Campaigns impersonate the 'Women Empowerments Desk' of the Central Tibetan Administration and use the domain tibet-gov.web[.]app."

Security researcher MalwareHunterTeam also spotted DOCX documents with Chinese filenames being used to install malicious payloads detected as password-stealing trojans via http://coolrat[.]xyz.

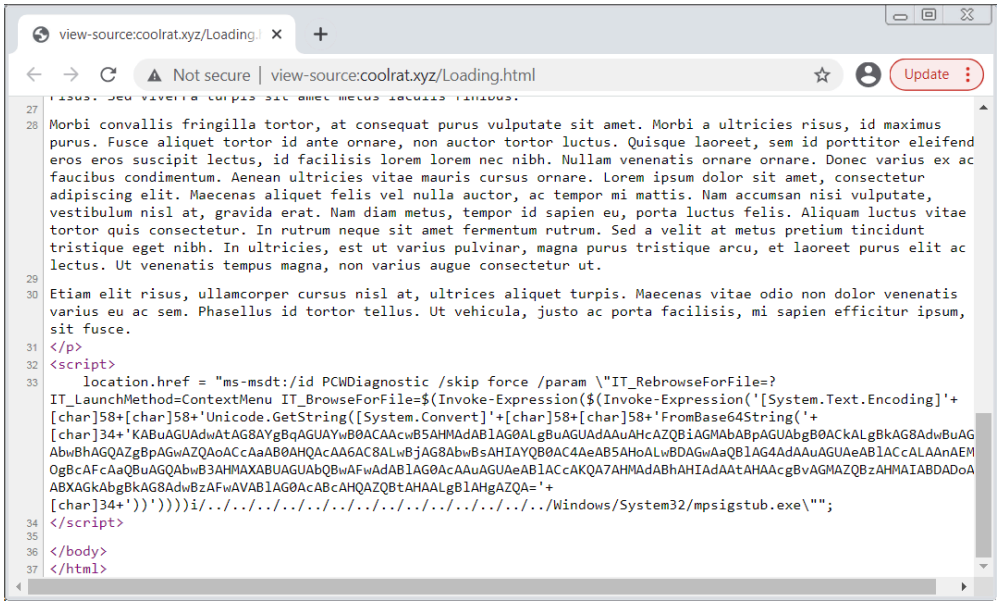


Image: BleepingComputer

Mitigation available

"An attacker who successfully exploits this vulnerability can run arbitrary code with the privileges of the calling application," as Microsoft explained in new guidance issued today to provide admins with mitigation measures.

"The attacker can then install programs, view, change, or delete data, or create new accounts in the context allowed by the user's rights."

You can block attacks exploiting CVE-2022-30190 by disabling the MSDT URL protocol malicious actors abuse to launch troubleshooters and execute code on vulnerable systems.

You are also advised to disable the Preview pane in Windows Explorer since this is another attack vector exploitable when targets preview the malicious documents.

Today, CISA also urged admins and users to disable the MSDT protocol on their Windows devices after Microsoft reported active exploitation of this vulnerability in the wild.

The first CVE-2022-30190 attacks were spotted over a month ago using sextortion threats and invitations to Sputnik Radio interviews as lures.

Source: https://www.bleepingcomputer.com/news/security/windows-msdt-zero-day-now-exploited-by-chinese-apt-hackers/