

Phishing Campaign Uses Maduro Arrest Story to Deliver Backdoor Payloads

CSN cybersecuritynews.com/phishing-campaign-uses-maduro-arrest-deliver-malware

Dhivya

January 10, 2026



Cybercriminals are leveraging the recent arrest of Venezuelan President Nicolás Maduro to distribute sophisticated [backdoor malware](#).

The threat actors exploited news surrounding Maduro's arrest on January 3, 2025, demonstrating how geopolitical events continue to serve as effective lures for malicious campaigns.

The attack likely begins with a spear-phishing email containing a zip archive named "US now deciding what's next for Venezuela.zip".

Inside, victims find an executable file titled "Maduro to be taken to New York.exe" alongside a malicious dynamic-link library called "kugou.dll".

```

v4 = 0;
LibraryW = LoadLibraryW(L"kugou.dll");
v6 = LibraryW;
if ( LibraryW )
{
    DataImporterMain = GetProcAddress(LibraryW, "DataImporterMain");
    if ( DataImporterMain )

```

DLL called with LoadLibraryW

The executable is a legitimate KuGou binary, but has been weaponized via DLL hijacking to load the malicious library, according to [Darktrace security researchers](#).

Malware Behavior

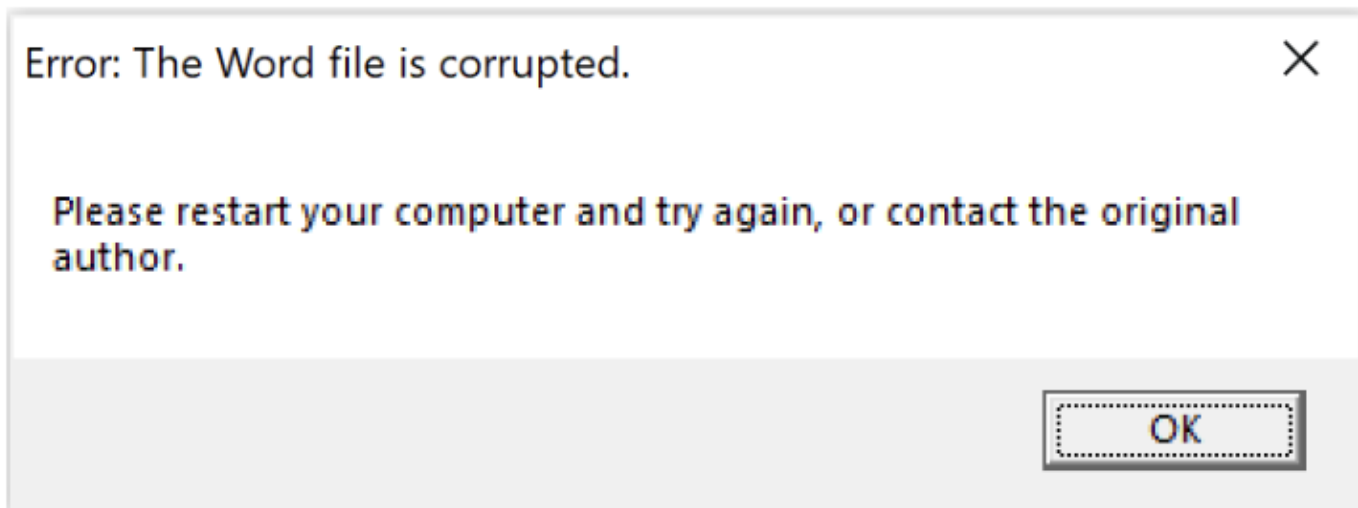
Once executed, the malware creates a directory at C:\ProgramData\Technology360NB and copies itself, renaming the files.

Disk (C:) > ProgramData > Technology360NB			Search Technology360NB
Name	Date modified	Type	
 DataTechnology.exe	1/3/2026 12:25 AM	Application	
 kugou.dll	1/3/2026 12:25 AM	Application extension	

Folder "Technology360NB" created

It establishes persistence by adding a registry key at "HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Lite360" that runs automatically at system startup.

The malware then displays a dialog box prompting users to restart their computer, which triggers the [malicious payload](#).



Message box prompting user to restart

After the system restarts, the malware initiates regular [encrypted](#) connections to a command-and-control server at 172.81.60[.]97 on port 443.

These periodic connections enable the malware to receive instructions and configurations from the attackers.

The campaign shares similarities with previous operations by Mustang Panda, a Chinese threat group known for exploiting current events such as the Ukraine war, Tibet-related conventions, and Taiwan-related topics.

However, researchers note that there is insufficient evidence to attribute this activity to any specific group definitively.

This incident highlights the ongoing threat of geopolitical-themed [phishing campaigns](#).

Organizations and individuals should exercise extreme caution when opening email attachments, especially those referencing breaking news or world events.

Indicators of Compromise (IoCs)

- 172.81.60[.]97
- 8f81ce8ca6cdb7d7eb10f4da5f470c6 – US now deciding what's next for Venezuela.zip
- 722bcd4b14aac3395f8a073050b9a578 – Maduro to be taken to New York.exe
- aea6f6edb0ab0f22568dcb503d731 – kugou.dll

Top 10

[Top 10 Best Practices for Cybersecurity Professionals to Secure Your Database](#)

[Top 20 Most Exploited Vulnerabilities: Microsoft Products Draw Hackers](#)

[10 Best DevOps Tools to Shift Your Security in 2026](#)

[Top 10 Best SaaS Security Tools – 2026](#)

[Top 10 Best Insider Risk Management Platforms – 2026](#)
