

Maduro Arrest Used as a Lure to Deliver Backdoor

 darktrace.com/blog/maduro-arrest-used-as-a-lure-to-deliver-backdoor

Tara Gould

January 9, 2026

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

[Blog](#)

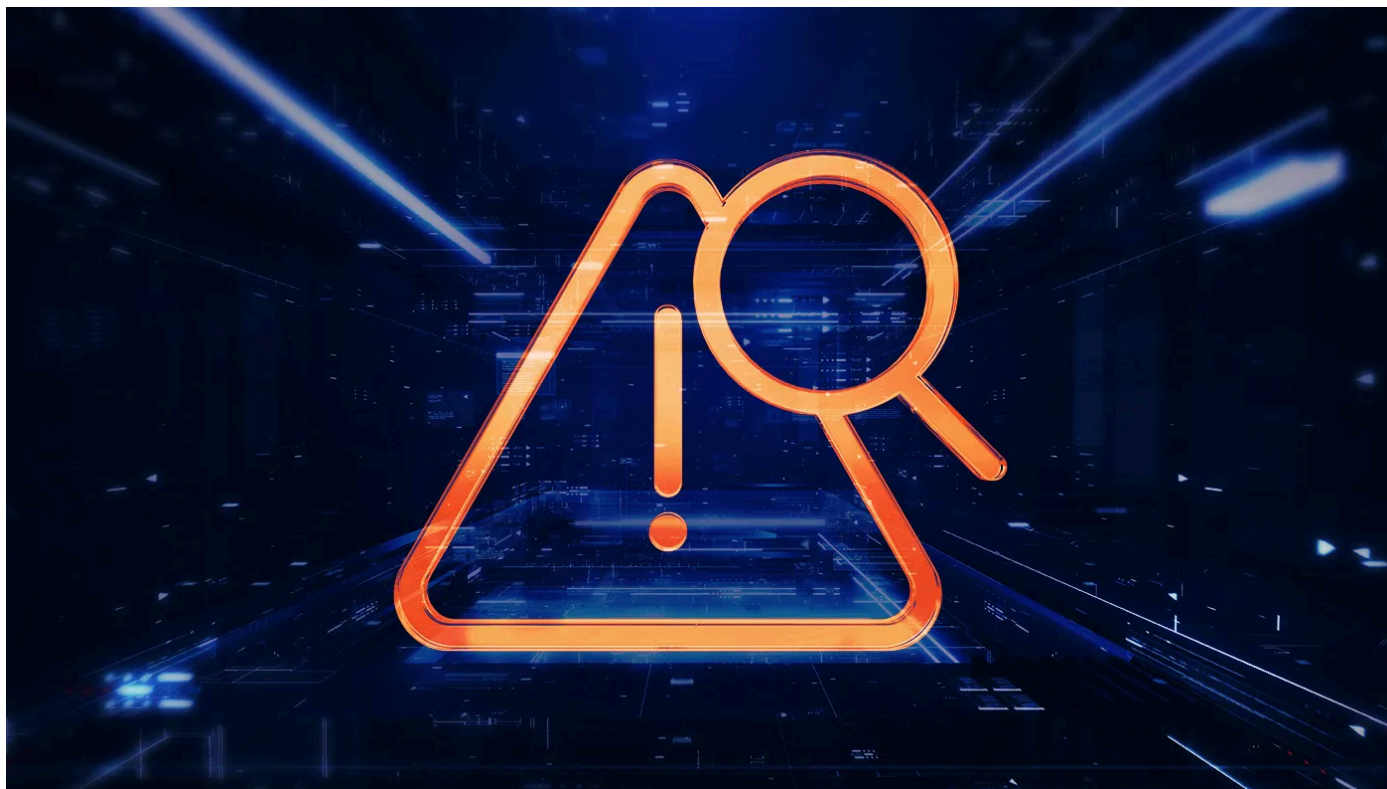
/

[Network](#)

/

January 9, 2026

Darktrace researchers observed threat actors exploiting reports of Venezuelan President Maduro's arrest to deliver backdoor malware. Attackers often use ongoing world events make their malicious content appear more credible, increasingly the likelihood of a successful attack.



Introduction

Threat actors frequently exploit ongoing world events to trick users into opening and executing malicious files. Darktrace security researchers recently identified a threat group using reports around the arrest of Venezuelan President Nicolás Maduro on January 3, 2025, as a lure to deliver backdoor malware.

Technical Analysis

While the exact initial access method is unknown, it is likely that a spear-phishing email was sent to victims, containing a zip archive titled *“US now deciding what’s next for Venezuela.zip”*. This file included an executable named *“Maduro to be taken to New York.exe”* and a dynamic-link library (DLL), *“kugou.dll”*.

The binary *“Maduro to be taken to New York.exe”* is a legitimate binary (albeit with an expired signature) related to KuGou, a Chinese streaming platform. Its function is to load the DLL *“kugou.dll”* via DLL search order. In this instance, the expected DLL has been replaced with a malicious one with the same name to load it.

```

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

```

Figure 1: DLL called with LoadLibraryW.

Once the DLL is executed, a directory is created C:\ProgramData\Technology360NB with the DLL copied into the directory along with the executable, renamed as “DataTechnology.exe”. A registry key is created for persistence in “HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Lite360” to run DataTechnology.exe --DATA on log on.

```

v15 = sub_10006730();
sub_100069E0(v15);
SHSetValueA(
    HKEY_CURRENT_USER,
    "Software\Microsoft\Windows\CurrentVersion\Run",
    "Lite360",
    1u,
    "C:\\ProgramData\\Technology360NB\\DataTechnology.exe --DATA",
    0x39u);

```

Figure 2. Registry key added for persistence.

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	

Figure 3: Folder “Technology360NB” created.

During execution, a dialog box appears with the caption “*Please restart your computer and try again, or contact the original author.*”

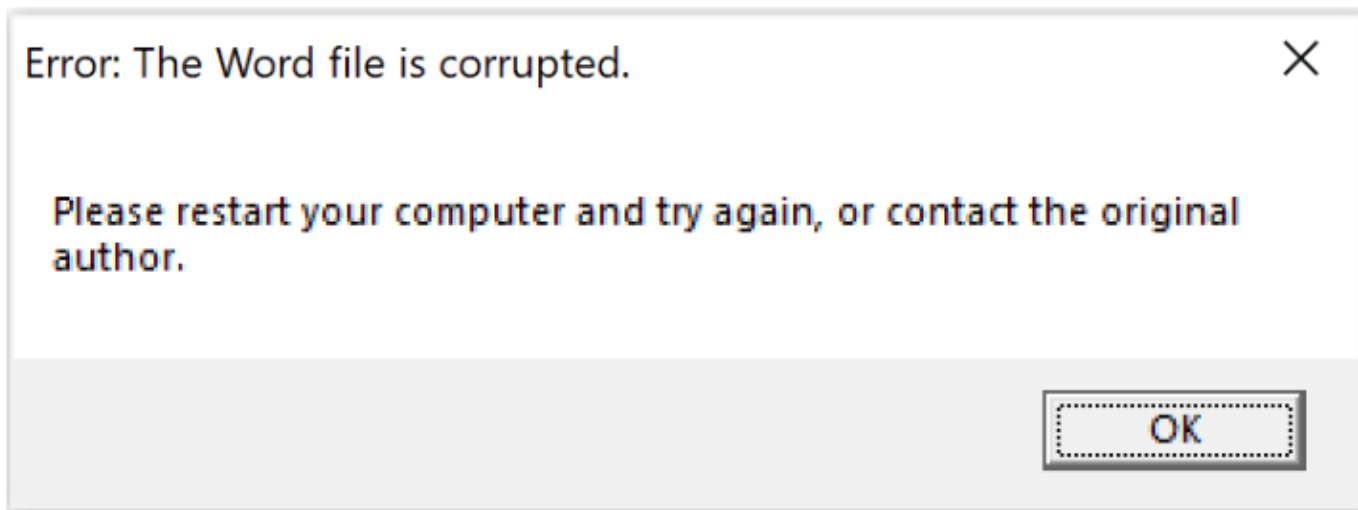


Figure 4. Message box prompting user to restart.

Prompting the user to restart triggers the malware to run from the registry key with the command - -DATA, and if the user doesn't, a forced restart is triggered. Once the system is reset, the malware begins periodic TLS connections to the command-and-control (C2) server 172.81.60[.]97 on port 443. While the encrypted traffic prevents direct inspection of commands or data, the regular beaconing and response traffic strongly imply that the malware has the ability to poll a remote server for instructions, configuration, or tasking.

Conclusion

Threat groups have long used geopolitical issues and other high-profile events to make malicious content appear more credible or urgent. Since the onset of the war in Ukraine, organizations have been repeatedly targeted with spear-phishing emails using subject lines related to the ongoing conflict, including references to prisoners of war [1]. Similarly, the Chinese threat group Mustang Panda frequently uses this tactic to deploy backdoors, using lures related to the Ukrainian war, conventions on Tibet [2], the South China Sea [3], and Taiwan [4].

The activity described in this blog shares similarities with previous Mustang Panda campaigns, including the use of a current-events archive, a directory created in ProgramData with a legitimate executable used to load a malicious DLL and run registry keys used for persistence. While there is an overlap of tactics, techniques and procedures (TTPs), there is insufficient information available to confidently attribute this activity to a specific threat group. Users should remain vigilant, especially when opening email attachments.

Edited by Ryan Traill (Analyst Content Lead)

Indicators of Compromise (IoCs)

172.81.60[.]97

8f81ce8ca6cd7d7eb10f4da5f470c6 - US now deciding what's next for Venezuela.zip

722bcd4b14aac3395f8a073050b9a578 - Maduro to be taken to New York.exe

aea6f6edbbbb0ab0f22568dcb503d731 - kugou.dll

References

[1] <https://cert.gov.ua/article/6280422>

[2] <https://www.ibm.com/think/x-force/hive0154-mustang-panda-shifts-focus-tibetan-community-deploy-pubload-backdoor>

[3] <https://www.ibm.com/think/x-force/hive0154-targeting-us-philippines-pakistan-taiwan>

[4] <https://www.ibm.com/think/x-force/hive0154-targeting-us-philippines-pakistan-taiwan>

Inside the SOC

Darktrace cyber analysts are world-class experts in threat intelligence, threat hunting and incident response, and provide 24/7 SOC support to thousands of Darktrace customers around the globe. *Inside the SOC* is exclusively authored by these experts, providing analysis of cyber incidents and threat trends, based on real-world experience in the field.

Share this post

Latest blogs



[React2Shell Reflections: Cloud Insights, Finance Sector Impacts, and How Threat Actors Moved So Quickly](#)

[Cloud](#)

[:](#)

[January 14, 2026](#)

[Nathaniel Jones](#)

[VP, Security & AI Strategy, Field CISO](#)



Runtime Is Where Cloud Security Really Counts: The Importance of Detection, Forensics and Real-Time Architecture Awareness

Cloud

•

January 13, 2026

Adam Stevens

Senior Director of Product, Cloud | Darktrace