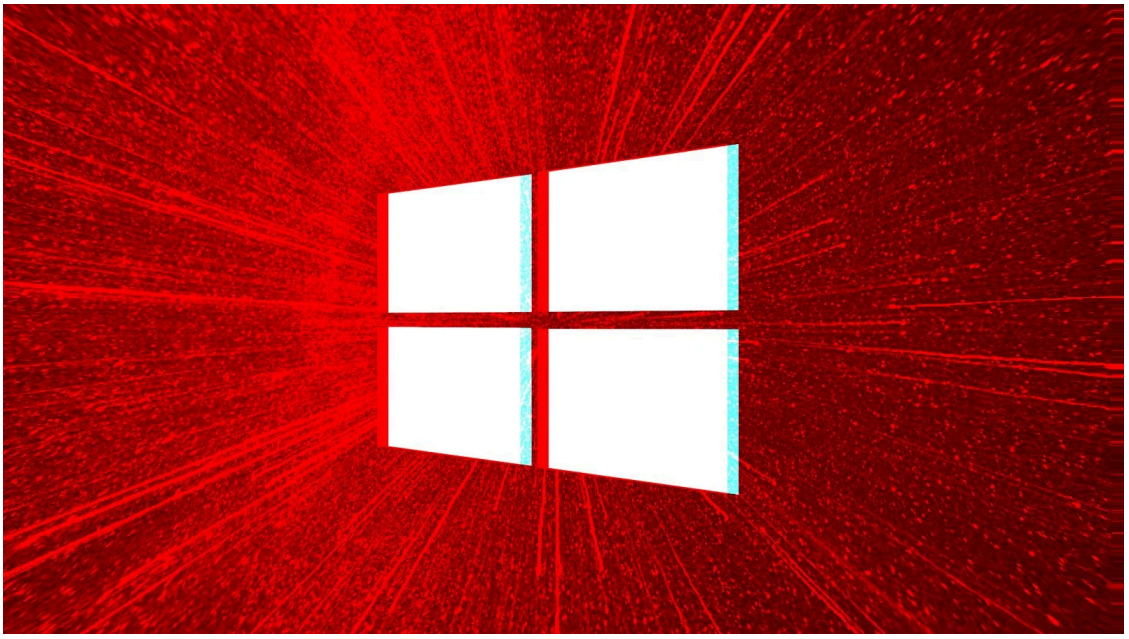
Hackers abuse Windows error reporting tool to deploy malware

By Bill Toulas

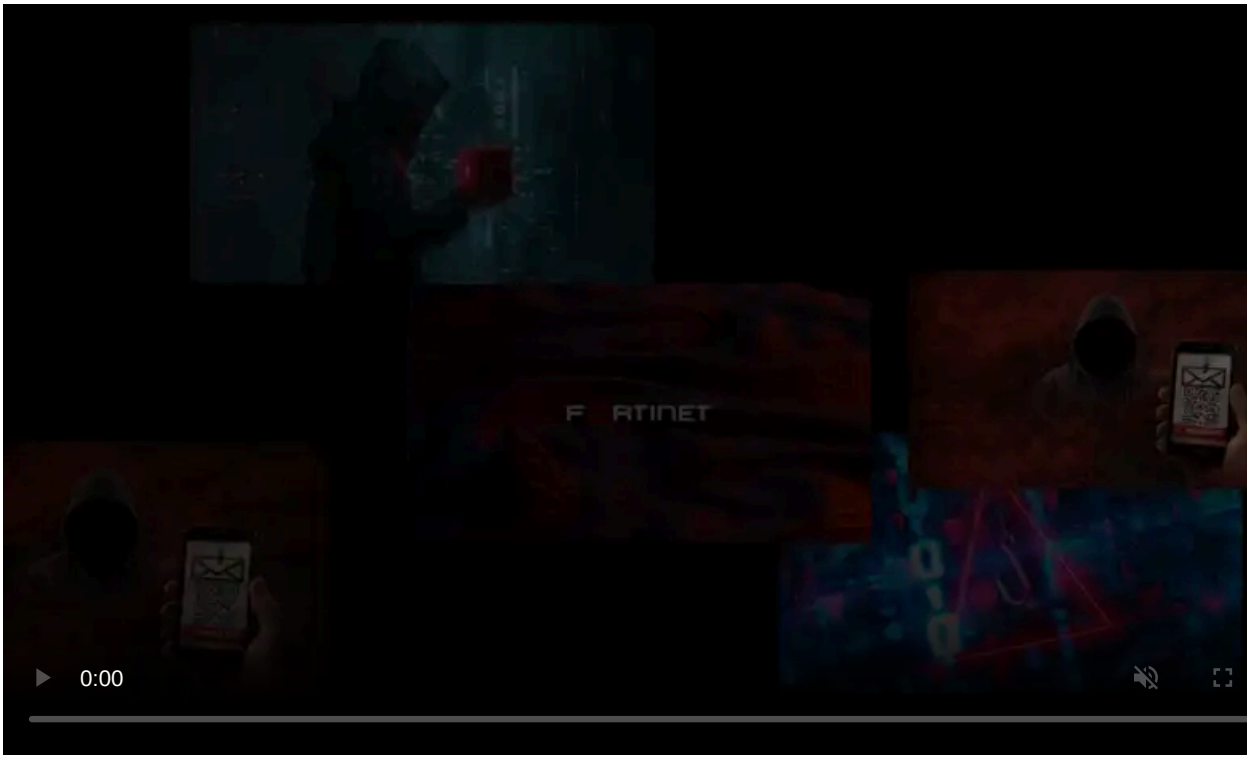
Published: 2023-01-04 · Archived: 2026-04-05 20:31:23 UTC



Hackers are abusing the Windows Problem Reporting (WerFault.exe) error reporting tool for Windows to load malware into a compromised system's memory using a DLL sideloading technique.

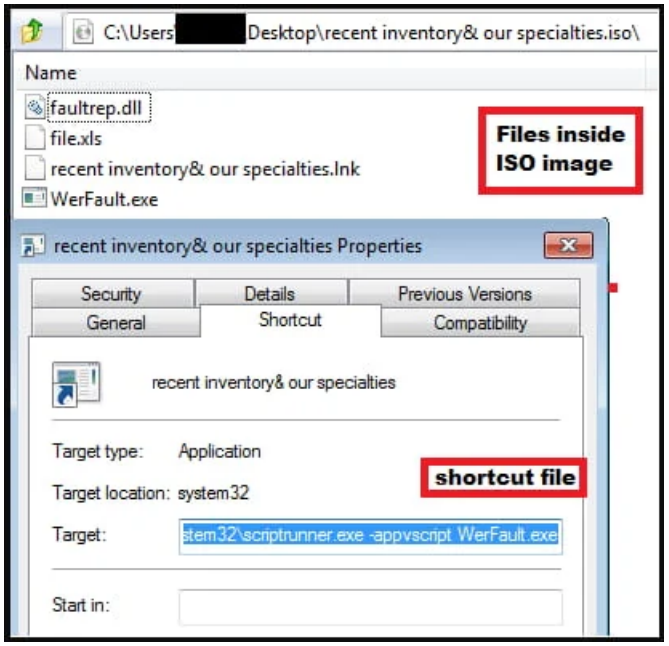
The use of this Windows executable is to stealthy infect devices without raising any alarms on the breached system by launching the malware through a legitimate Windows executable.

The new campaign was spotted by K7 Security Labs, which could not identify the hackers, but they are believed to be based in China.


F RTINET
0:00

Abusing WerFault.exe

The malware campaign starts with the arrival of an email with an ISO attachment. When double-clicked, the ISO will mount itself as a new drive letter containing a legitimate copy of the Windows WerFault.exe executable, a DLL file ('faultrep.dll'), an XLS file ('File.xls'), and a shortcut file ('inventory & our specialties.lnk').



Files contained in the ISO

Source: K7 Labs

The victim starts the infection chain by clicking on the shortcut file, which uses 'scriptrunner.exe' to execute WerFault.exe.

WerFault is the standard Windows error reporting tool used in Windows 10 and 11, allowing the system to track and report errors related to the operating system or applications.

Windows use the tool to report an error and receive potential solution recommendations.

Antivirus tools commonly trust WerFault as it's a legitimate Windows executable signed by Microsoft, so launching it on the system won't usually trigger alerts to warn the victim.

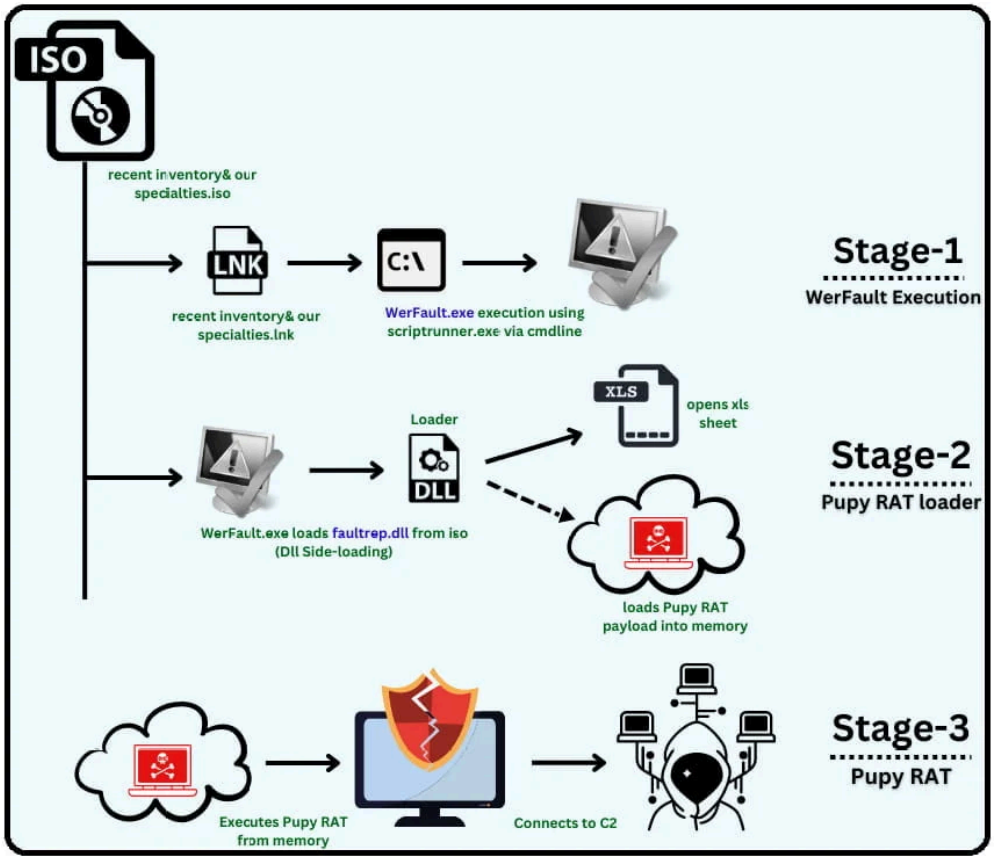
When WerFault.exe is launched, it will use a known DLL sideloading flaw to load the malicious 'faultrep.dll' DLL contained in the ISO.

Normally, the 'faultrep.dll' file is a legitimate DLL by Microsoft in the C:\Windows\System folder required for WerFault to run correctly. However, the malicious DLL version in the ISO contains additional code to launch the malware.

The technique of creating malicious DLLs under the same name as a legitimate one so that it is loaded instead is called DLL sideloading.

DLL sideloading requires a malicious version of a DLL to be located in the same directory as the executable that invokes it. When the executable is launched, Windows will prioritize it over its native DLL as long as it has the same name.

When the DLL is loaded in this attack, it will create two threads, one that loads Pupy Remote Access Trojan's DLL ('dll_pupyx64.dll') into memory and one that opens the included XLS spreadsheet to serve as a decoy.



Complete infection chain
Source: K7 Labs

Pupy RAT is an open-source and publicly available malware written in Python that supports reflective DLL loading to evade detection, and additional modules are downloaded later.

The malware allows threat actors to gain full access to the infected devices, enabling them to execute commands, steal data, install further malware, or spread laterally through a network.

As an open-source tool, it has been used by several state-backed espionage actors like the Iranian APT33 and APT35 groups, as those tools make attribution and persistent operation harder to track.

QBot malware distributors were seen adopting a similar attack chain last summer, abusing the Windows Calculator to evade detection by security software.

Source: https://www.bleepingcomputer.com/news/security/hackers-abuse-windows-error-reporting-tool-to-deploy-malware/