Windows Error Reporting Tool Abused to Load Malware

By Ian Reynolds

Published: 2023-01-08 · Archived: 2026-04-06 02:06:17 UTC

A legitimate Windows executable is being abused by malicious actors to stealthily infect devices with malware without raising any alarms. The Windows Error Reporting tool *WerFault.exe* can be exploited to load malware onto a system using a DLL sideloading technique in an attack K7 Security Labs have published an analysis for last week. This legitimate Windows 10 and 11 tool is normally used to report errors related to applications or the operating system itself, and can also receive solution recommendations for the problem experienced.

The attack studied in this analysis resulted in the execution of Pupy RAT malware, an open-source remote admin tool believed to have originated in 2013. Pupy RAT is credited for the Iranian-backed attack on a European energy sector mail server in late 2019, along with other attacks of Iranian origin by groups known as APT33 and APT35. Written mostly in Python, this cross-platform remote access trojan is available on GitHub for free, making it easily available for widespread use by any threat actors and therefore a high security risk businesses and individuals need to be aware of.

An attack begins by the threat actors sending the victim an email with an ISO image called *recent inventory & our specialities.iso* as an attachment. This ISO image contains a shortcut file with the same name, *recent inventory & our specialities.lnk*, which when run is the start of the infection chain. The ISO image also contains 3 other files used in the attack: a legitimate copy of Windows tool *WerFault.exe*, a DLL file called *faultrep.dll*, and an XLS file called *File.xls*. The XLS file analysed was in Chinese, leading to the assumption that the victim in the K7 Labs analysis was Chinese and the XLS sheet is translated by the targeted device. When the ISO image is clicked, it mounts itself as a new drive letter containing the 4 files. When the shortcut file *recent inventory & our specialities.lnk* is then opened it uses *scriptrunner.exe*, a living off the land binary via command line interpreter, to run *WerFault.exe* from this location.

Because the default Windows DLL used by *WerFault.exe* is called *Faultrep.dll*, the attacker can manipulate the outcome so that when *WerFault.exe* starts executing, the version of *faultrep.dll* from the ISO is loaded instead. This is performed through a DLL sideloading technique where the legitimate path is hijacked, and a malicious file is executed instead. To mimic the function of the legitimate DLL, the malicious *faultrep.dll* has a dummy export function called *WerpInitiateCrashReporting*, and has two custom API resolving arguments, a DLL hash and a Function hash. Despite the majority of this attack being written in python code, the malicious DLL is compiled in C. The DLL resolves these APIs through *kernel32.dll* and *advapi32.dll* using the same resolving function as shellcode-based downloader malware GuLoader.

After the APIs are resolved, the function *CreateThread* is used to create two threads, the first of which opens the final file from the ISO image, the Excel sheet *file.xls*. The second thread resolves *SystemFunction032* through *advapi32.dll*, which can go unnoticed as the XLS file has opened in front as a decoy event. *SystemFunction032* is the Pupy RAT, *dll_pupyx64.dll*, which is first loaded into the memory and then executed from the memory in the background while the *WerFault.exe* is being executed in the foreground. Pupy RAT can then remotely execute any

portable executable file in memory through a *ReflectiveLoader* function. The RAT attempts a C2 connection to download additional files and proceed with the attack, however during the time of analysis by K7 Security Labs this connection was down, and the RAT was unable to connect to the C2 server.

Because *WerFault.exe* is a legitimate Windows reporting tool, it's launch does not trigger the response from antivirus software that might otherwise warn the user that the device has been infected with malware. If the C2 servers are functional, this malware attack could result in threat actors having full access to the victim's device, including the ability to execute arbitrary commands, data exfiltration, install additional malware or ransomware files, and possibly even spread laterally through the network. K7 Security Labs included a table of the Indicators of Compromise (IoCs) for this attack, including the filenames and hash values, that can be used to determine whether a system has fallen victim to this attack.

Despite the ability of Pupy RAT to disguise itself behind legitimate executables to trick some antivirus software, there are precautions that can be taken to protect your device from this form of attack. Behavioural patterns of known malware are tracked by some endpoint detection systems, which can identify malicious execution patterns in the early stages and prevent the attack from continuing to the point of full infection. Most importantly, this attack involves user interaction to initiate the download and launch of the malicious executable files. Falling victim to this attack can be prevented by not opening the initial email attachment of an ISO image and by not running the shortcut file included in the ISO. Email attachments from unknown sources should always be treated with high suspicion, and educating colleagues to do the same will help protect your entire network from attack.
