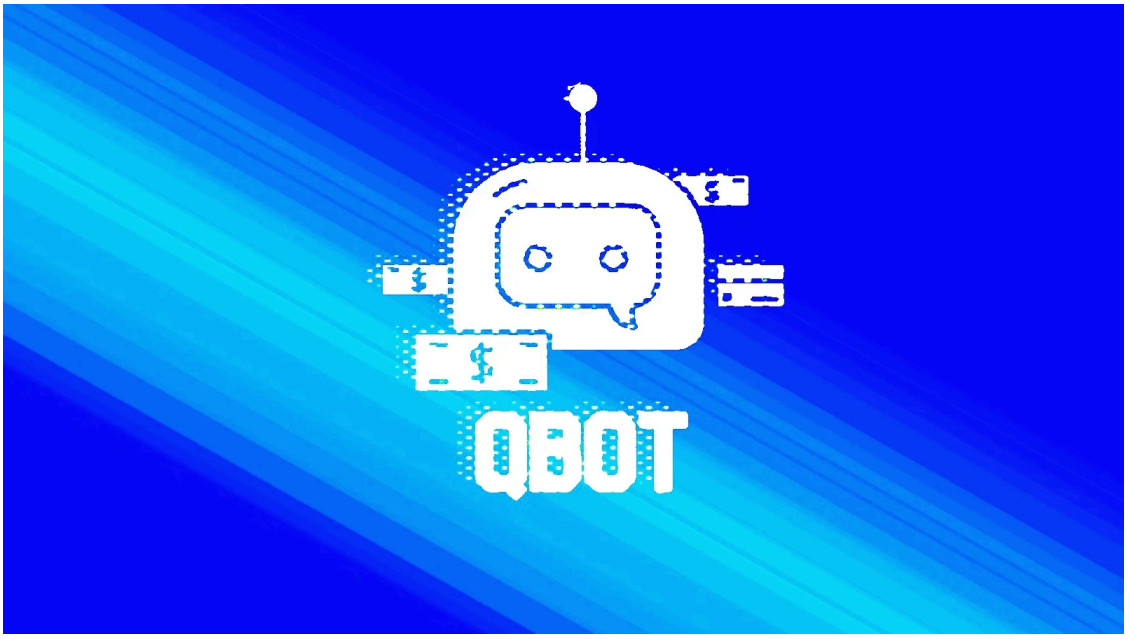
QBot malware abuses Windows WordPad EXE to infect devices

By Lawrence Abrams

Published: 2023-05-27 · Archived: 2026-04-05 14:07:03 UTC



The QBot malware operation has started to abuse a DLL hijacking flaw in the Windows 10 WordPad program to infect computers, using the legitimate program to evade detection by security software.

A DLL is a library file containing functions that can be used by more than one program at the same time. When an application is launched, it will attempt to load any required DLLs.

It does this by searching through specific Windows folders for the DLL and, when found, loads it. However, Windows applications will prioritize DLLs in the same folder as the executable, loading them before all others.


DIE LINKE.
0:00

DLL hijacking is when a threat actor creates a malicious DLL of the same name as a legitimate one, and places it in the early Windows search path, usually the same folder as the executable. When that executable is launched, it will load the malware DLL rather than the legitimate one and execute any malicious commands within it.

QBot abuses WordPad DLL hijacking flaw

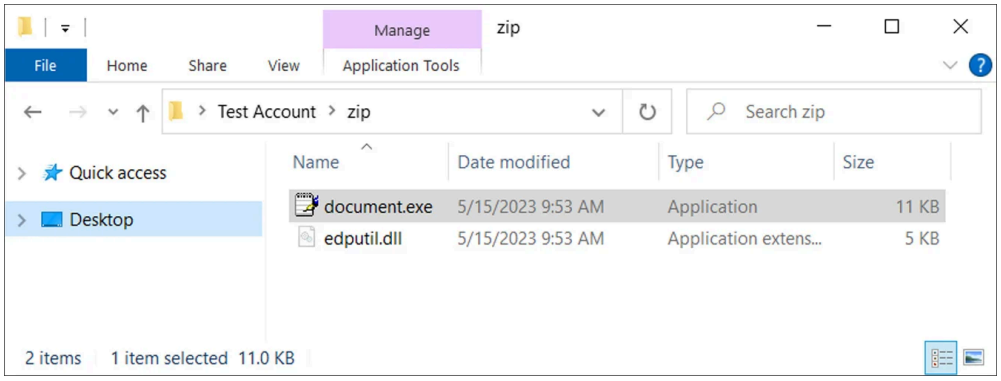
QBot, also known as Qakbot, is a Windows malware that initially started as a banking trojan but evolved into a malware dropper. Ransomware gangs, including Black Basta, Egregor, and Prolock, have partnered with the malware operation to gain initial access to corporate networks to conduct extortion attacks.

Security researcher and Cryptolaemus member ProxyLife told BleepingComputer that a new QBot phishing campaign began abusing a DLL hijacking vulnerability in the Windows 10 WordPad executable, write.exe.

While BleepingComputer has not seen the original phishing emails, ProxyLife told us they contain a link to download a file.

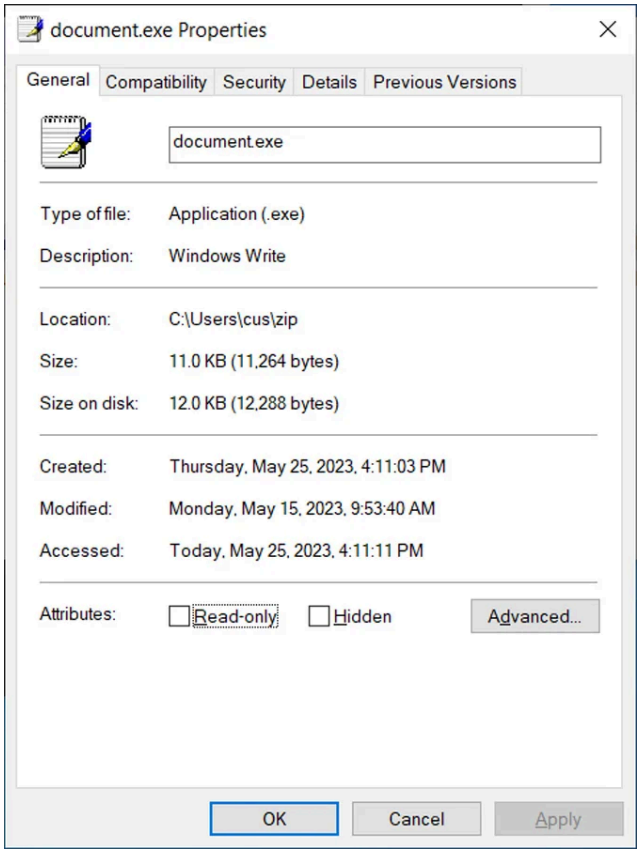
When a person clicks on the link it will download a random named ZIP archive from a remote host will be downloaded.

This ZIP file contains two files: *document.exe* (the Windows 10 WordPad executable) and a DLL file named *edputil.dll* (used for the DLL hijack).



Contents of the downloaded ZIP file
Source: BleepingComputer

As you can see from the properties of the document.exe file, it is simply a renamed copy of the legitimate Write.exe executable used to launch the Windows 10 WordPad document editor.



Renamed Windows 10 WordPad executable

Source: BleepingComputer

When document.exe is launched, it automatically attempts to load a legitimate DLL file called edputil.dll, which is normally located in the C:\Windows\System32 folder.

However, when the executable attempts to load edputil.dll, it does not check for it in a specific folder and will load any DLL of the same name found in the same folder as the document.exe executable.

This allows the threat actors to perform DLL hijacking by creating a malicious version of the edputil.dll DLL and storing it in the same folder as document.exe so it is loaded instead.

Once the DLL is loaded, ProxyLife told BleepingComputer that the malware uses C:\Windows\system32\curl.exe to download a DLL camouflaged as a PNG file from a remote host.

This PNG file (actually a DLL) is then executed using rundll32.exe with the following command:

```
rundll32 c:\users\public\default.png,print
```

QBot will now quietly run in the background, stealing emails for use in further phishing attacks and eventually downloading other payloads, such as Cobalt Strike (a post-exploitation toolkit threat actors use to gain initial access to the infected device).

This device will then be used as a foothold to spread laterally throughout the network, commonly leading to corporate data theft and ransomware attacks.

By installing QBot through a trusted program like the Windows 10 WordPad (write.exe), the threat actors hope security software will not flag the malware as malicious.

However, using curl.exe means that this infection method will only work on Windows 10 and later, as earlier operating system versions do not include the Curl program.

For the most part, this should not be an issue, as older versions of Windows have been phased out after reaching the end of support.

At this time, the QBot operation has moved on to other infection methods in recent weeks, but it is not uncommon for them to switch to previous tactics in later campaigns.

Source: https://www.bleepingcomputer.com/news/security/qbot-malware-abuses-windows-wordpad-exe-to-infect-devices/