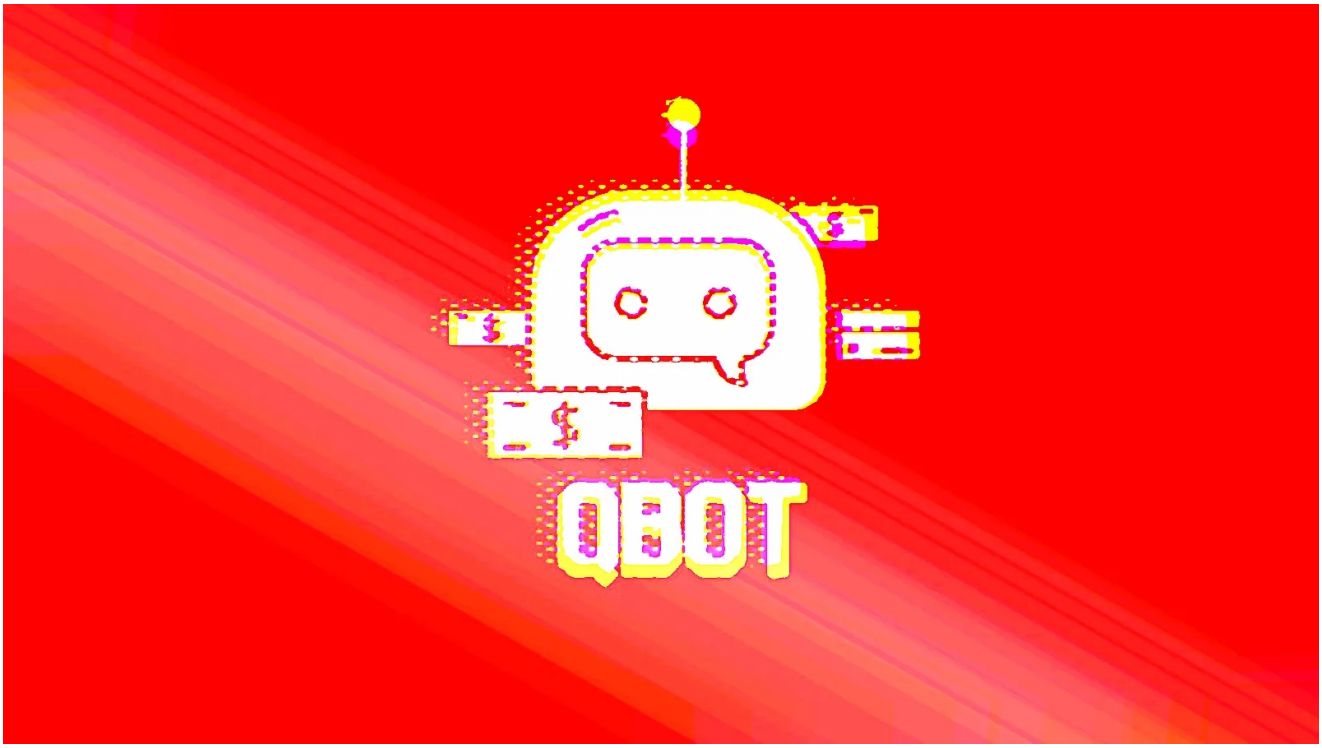
QBot phishing uses Windows Calculator DLL hijacking to infect devices

bleepingcomputer.com/news/security/qbot-phishing-uses-windows-calculator-sideloading-to-infect-devices/

Bill Toulas

By
Bill Toulas

- July 24, 2022
- 11:18 AM
- 0



The operators of the QBot malware have been using a DLL hijacking flaw in Windows Calculator to infect computers, which also helps evade detection by security software.

DLL hijacking is a common attack method that takes advantage of how Dynamic Link Libraries (DLLs) are handled in Windows. It consists of creating a malicious version of a legitimate DLL required by the program, and placing it early in the search order used to find a required DLL. This folder is commonly the same folder as the executable.

When the executable is launched, it will find the malicious version with the same name in the same folder, loading that instead and infecting the computer.

QBot, also known as Qakbot is a Windows malware strain that started as a banking trojan but evolved into a malware dropper, and is used by ransomware gangs in the early stages of the attack to drop Cobalt Strike beacons.

Security researcher ProxyLife recently discovered that Qakbot, has been abusing the the Windows 7 Calculator app for DLL hijacking attacks since at least July 11. The method continues to be used in malspam campaigns.

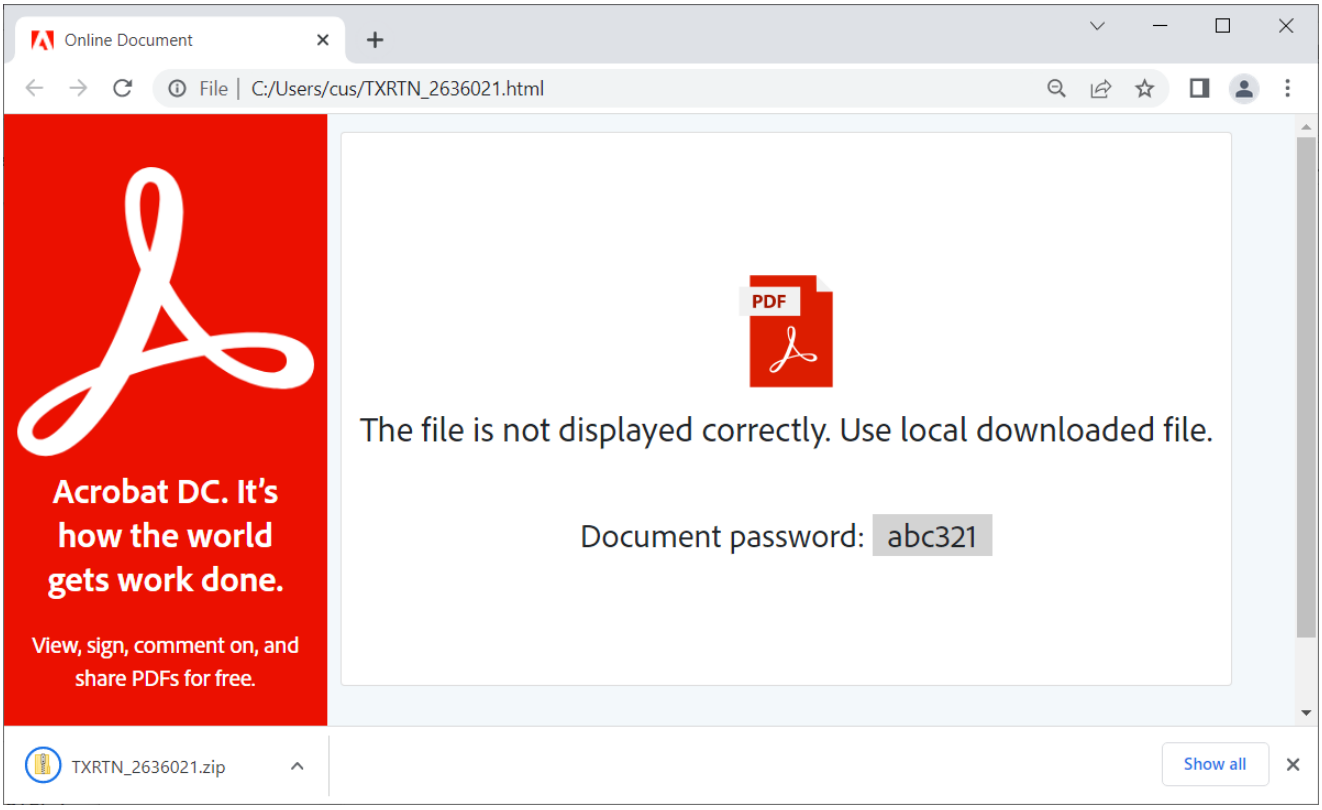
> #Qakbot - obama200 - html > .zip > .iso > .lnk > calc.exe > .dll > .dll
>
> T1574 - DLL Search Order Hijacking
>
> cmd.exe /q /c calc.exe
>
> regsvr32 /s C:\Users\User\AppData\Local\Temp\WindowsCodecs.dll
>
> regsvr32.exe 102755.dllhttps://t.co/2Vgg6cuRFh
>
> IOC'shttps://t.co/e7hkNW8eQu pic.twitter.com/sCH1xagkyR
>
> — proxylife (@pr0xylife) July 11, 2022

New QBot infection chain

To help defenders protect against this threat, ProxyLife and researchers at Cyble documented the latest QBot infection chain.

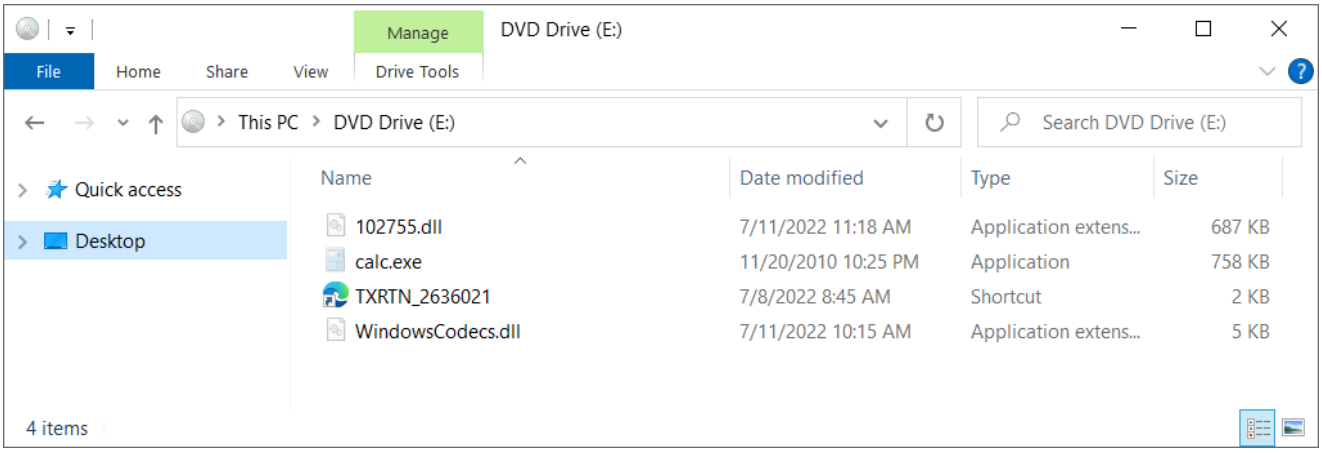
The emails used in the latest campaign carry an HTML file attachment that downloads a password-protected ZIP archive with an ISO file inside.

The password for opening the ZIP file is shown in the HTML file, and the reason for locking the archive is to evade antivirus detection.



HTML attachment on QBot spam emails

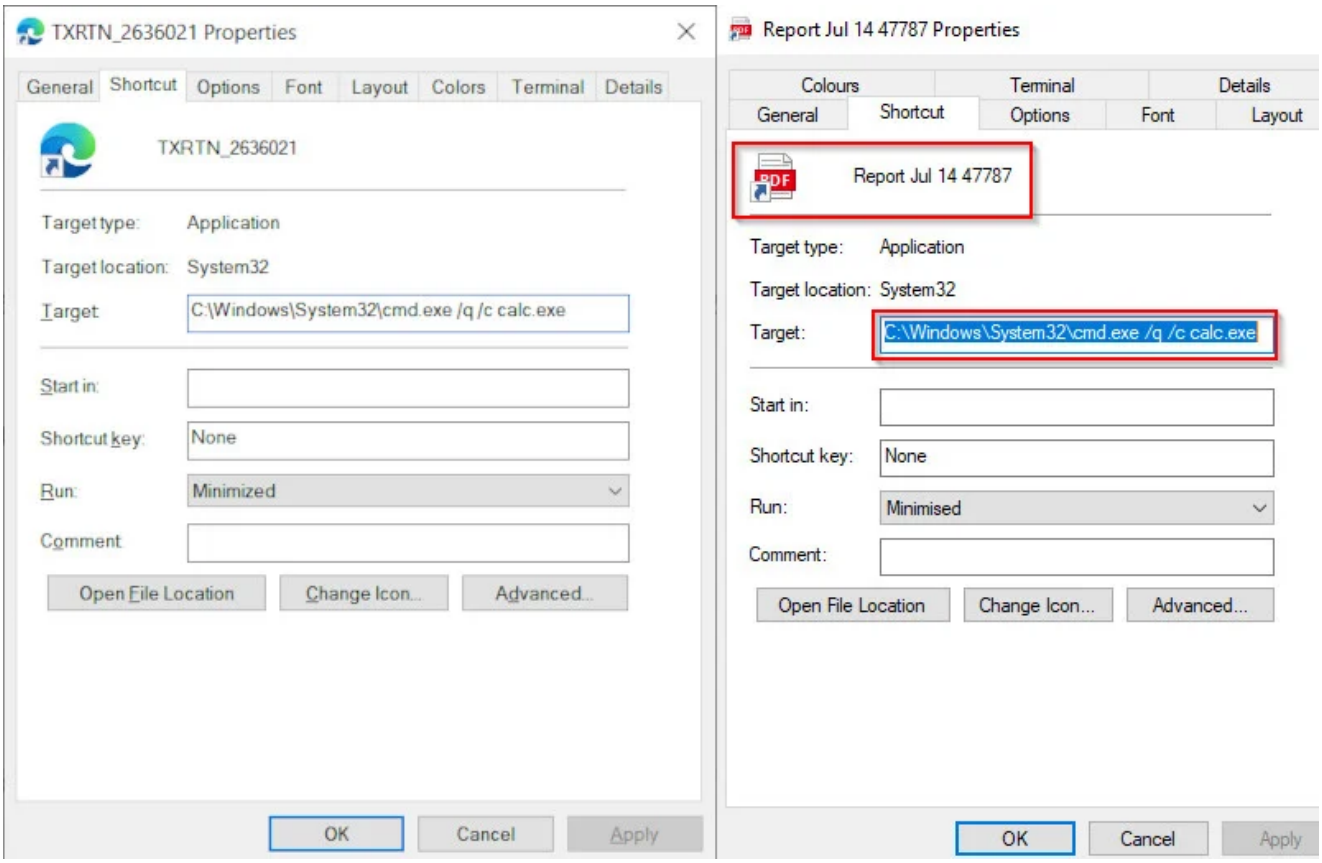
The ISO contains a .LNK file, a copy of *'calc.exe'* (Windows Calculator), and two DLL files, namely WindowsCodecs.dll and a payload named *7533.dll*.



ZIP archive contents

When the user mounts the ISO file, it only displays the .LNK file, which is masqueraded to look like a PDF holding important information or a file that opens with Microsoft Edge browser.

However, the shortcut points to the Calculator app in Windows, as seen in the properties dialog for the files.



Properties of the PDF file that triggers the infection

Clicking the shortcut triggers the infection by executing the Calc.exe through the Command Prompt.

When loaded, the Windows 7 Calculator automatically searches for and attempts to load the legitimate WindowsCodecs DLL file. However, it does not check for the DLL in certain hard coded paths, and will load any DLL with the same name if placed in the same folder as the Calc.exe executable.

The threat actors take advantage of this flaw by creating their own malicious WindowsCodecs.dll file that launches the other *[numbered].dll* file, which is the QBot malware.

By installing QBot through a trusted program like the Windows Calculator, some security software may not detect the malware when it is loaded, allowing the threat actors to evade detection.

It should be noted, that this DLL hijacking flaw no longer works in Windows 10 Calc.exe and later, which is why the threat actors bundle the Windows 7 version.

QBot has been around for more than a decade, with origins going as far back as 2009 [1, 2, 3, 4]. While campaigns delivering it are not frequent, it was observed being distributed by Emotet botnet in the past to drop ransomware payloads.

Among the ransomware families that QBot delivered are RansomExx, Maze, ProLock, and Egregor. More recently, the malware dropped Black Basta ransomware.

Related Articles:

Microsoft finds Raspberry Robin worm in hundreds of Windows networks

Malicious Windows 'LNK' attacks made easy with new Quantum builder

Malicious PyPi packages turn Discord into password-stealing malware

New Windows PowerToys OCR tool will let you copy text from images

Malware devs already bypassed Android 13's new security feature

Bill Toulas

Bill Toulas is a technology writer and infosec news reporter with over a decade of experience working on various online publications. An open source advocate and Linux enthusiast, is currently finding pleasure in following hacks, malware campaigns, and data breach incidents, as well as by exploring the intricate ways through which tech is swiftly transforming our lives.