

[Home \(https://www.bleepingcomputer.com/\)](https://www.bleepingcomputer.com/) > [News \(https://www.bleepingcomputer.com/news/\)](https://www.bleepingcomputer.com/news/)

> [Security \(https://www.bleepingcomputer.com/news/security/\)](https://www.bleepingcomputer.com/news/security/)

> **QBot phishing uses Windows Calculator sideloading to infect devices**

QBot phishing uses Windows Calculator sideloading to infect devices

By

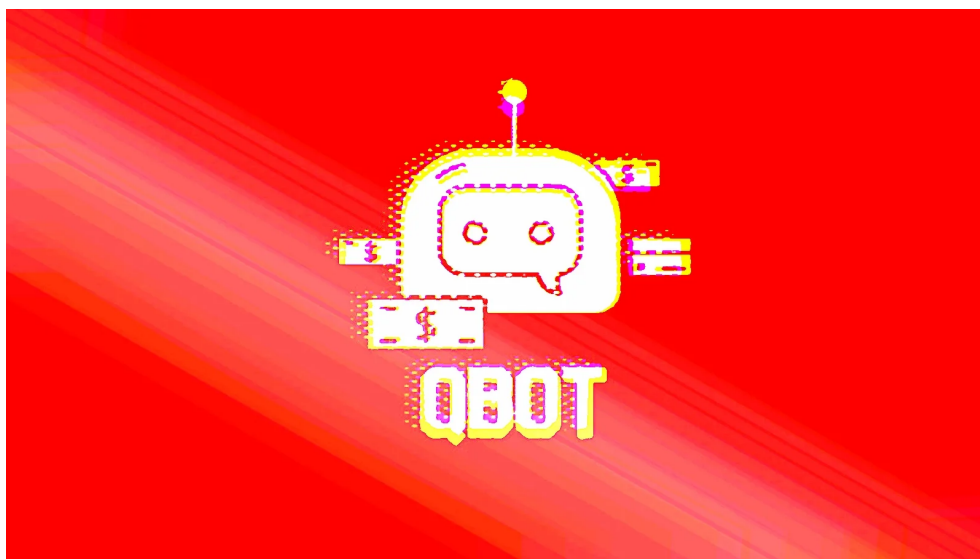
July 24, 2022

11:18 AM

0

Bill Toulas

(<https://www.bleepingcomputer.com/author/bill-toulas/>)



The operators of the QBot malware have been using the Windows Calculator to side-load the malicious payload on infected computers.

DLL side-loading is a common attack method that takes advantage of how Dynamic Link Libraries (DLLs) are handled in Windows. It consists of spoofing a legitimate DLL and placing it in a folder from where the



operating system loads it instead of the legitimate one.

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 (https://www.bleepingcomputer.com/news/security/qbot-now-pushes-black-basta-ransomware-in-bot-powered-attacks/) in the early stages of the attack to drop Cobalt Strike beacons.



Security researcher ProxyLife recently discovered (http://twitter.com/proxylife) that Qakbot, has been abusing the the Windows 7 Calculator app for DLL side-loading attacks since at least July 11. The method continues to be used in malspam campaigns.

proxylife

@pr0xylife · [Follow](#)



[#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

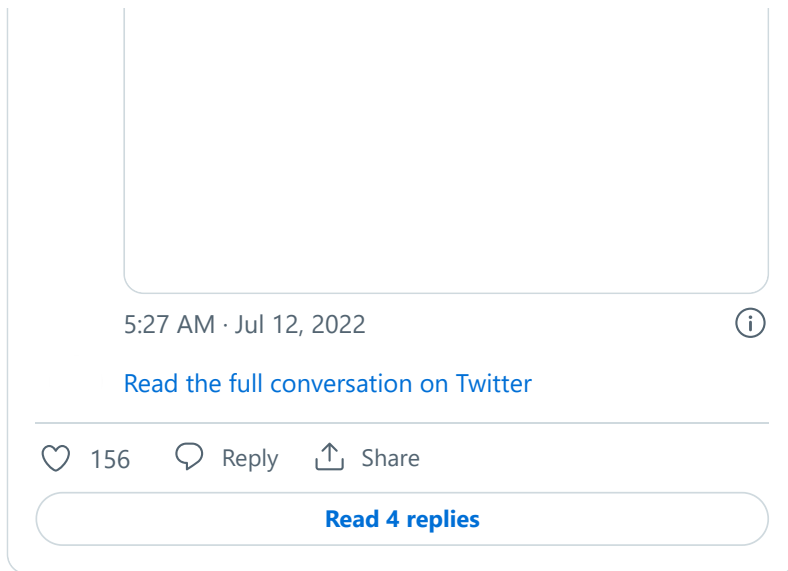
regsvr32.exe 102755.dll

bazaar.abuse.ch/sample/f5c1624...

IOC's

github.com/pr0xylife/Qakb...



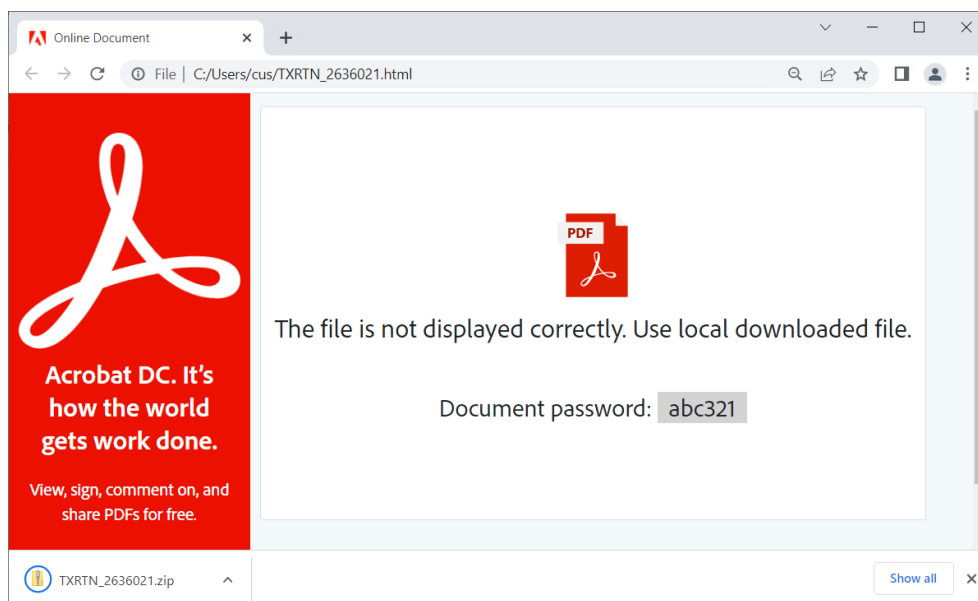


New QBot infection chain

To help defenders protect against this threat, ProxyLife and researchers at Cyble (<https://blog.cyble.com/2022/07/21/qakbot-resurfaces-with-new-playbook/>) documented (<http://blog.cyble.com/2022/07/21/qakbot-resurfaces-with-new-playbook/>) 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.

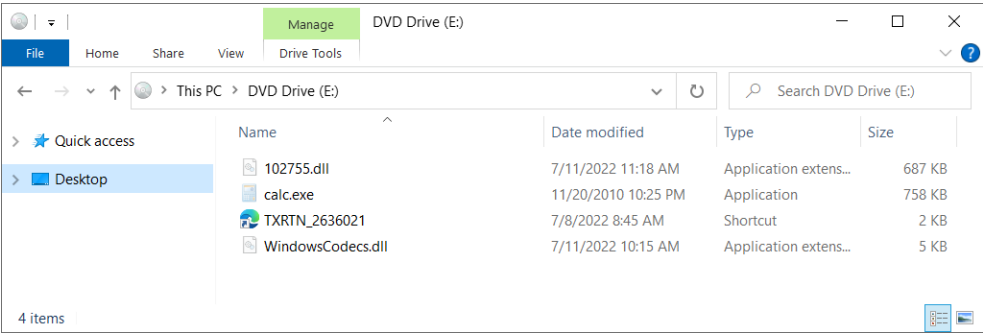
The password for opening the ZIP file is shown in the HTML file, and the reason for locking the archive is to evade antivirus detection.



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*.

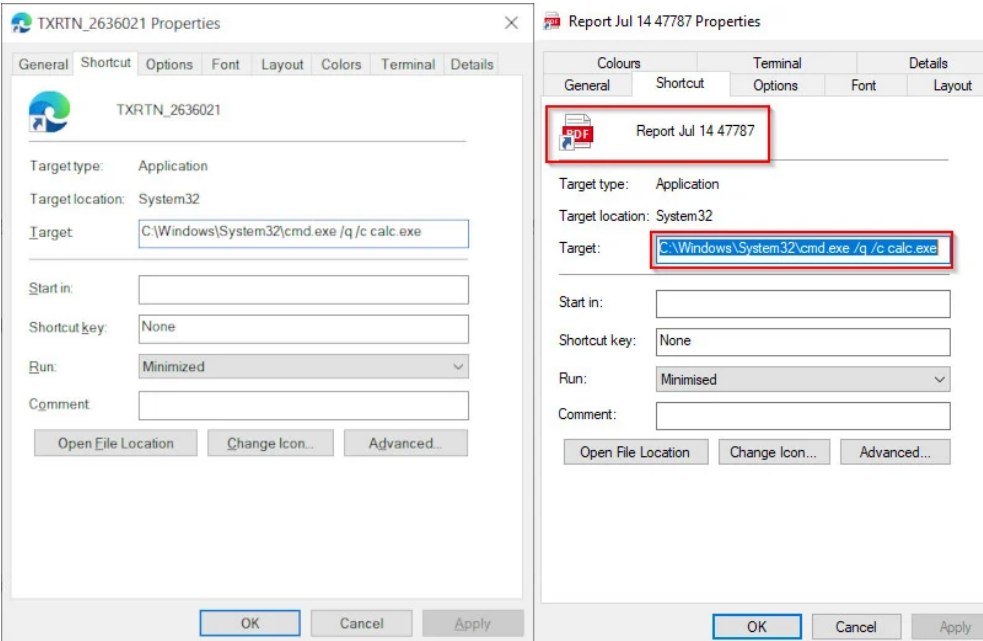




ZIP archive contents

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 sideloading 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 (<https://www.symantec.com/security-center/writeup/2009-050707-0639-99?tabid=3>), 2 (<https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32%2FQakbot>), 3 (<http://contagiodump.blogspot.com/2010/11/template.html>), 4 (<https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/80/qakbot-a-prevalent-infostealing-malware>)]. 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 (<https://www.bleepingcomputer.com/news/security/prolock-ransomware-teams-up-with-qakbot-trojan-for-network-access/>), and Eggregor (<https://www.bleepingcomputer.com/news/security/qbot-partners-with-egregor-ransomware-in-bot-fueled-attacks/>). More recently, the malware dropped Black Basta (<https://www.bleepingcomputer.com/news/security/qbot-now-pushes-black-basta-ransomware-in-bot-powered-attacks/>) ransomware.

