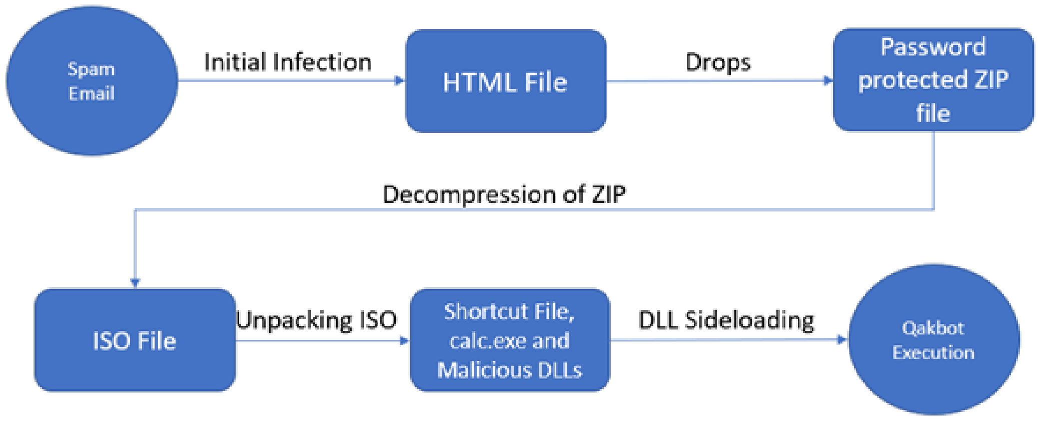
THREAT ACTORS LEVERAGES DLL-SIDELOADING TO SPREAD QAKBOT MALWARE

Pierluigi Paganini July 26, 2022



Qakbot malware operators are using the Windows Calculator to side-load the malicious payload on target systems.

Security expert ProxyLife and Cyble researchers recently uncovered a Qakbot campaign that was leveraging the Windows 7 Calculator app for DLL side-loading attacks. Dynamic-link library (DLL) side-loading is an attack method that takes advantage of how Microsoft Windows applications handle DLL files. In such attacks, malware places a spoofed malicious DLL file in a Windows' WinSxS directory so that the operating system loads it instead of the legitimate file

According to the researcher, the operators are using this technique since at least July 11.

Qakbot, also known as QBot, QuackBot and Pinkslipbot, is an info-stealing malware that has been active since 2008. The malware spreads via malspam campaigns, it inserts replies in active email threads.

Cyble experts, who started their investigation from the IoCs shared by ProxyLife, analyzed the attack chain employed in the latest Qakbot attacks.

RECENT ARTICLES

PTZOptics cameras zero-days actively exploited in the wild
HACKING / November 02, 2024

proxylife
@pr0xylife · Follow

#Qakbot - obama201 - html > .zip > .iso > .lnk > calc.exe > .dll > .dll

T1574 - DLL Search Order Hijacking

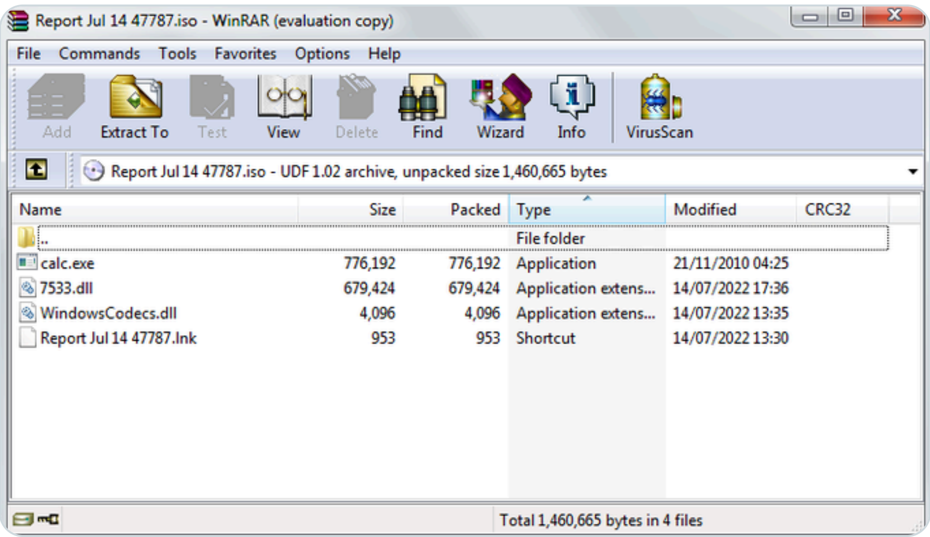
cmd.exe /q /c calc.exe

regsvr32 /s C:\Users\User\AppData\Local\Temp\WindowsCodecs.dll

regsvr32.exe 7533.dll

bazaar.abuse.ch/sample/cb83a65...

IOC's
github.com/pr0xylife/Qakb...



Report Jul 14 47787.iso - UDF 1.02 archive, unpacked size 1,460,665 bytes

Name	Size	Packed	Type	Modified	CRC32
..			File folder		
calc.exe	776,192	776,192	Application	21/11/2010 04:25	
7533.dll	679,424	679,424	Application extens...	14/07/2022 17:36	
WindowsCodecs.dll	4,096	4,096	Application extens...	14/07/2022 13:35	
Report Jul 14 47787.lnk	953	953	Shortcut	14/07/2022 13:30	

Total 1,460,665 bytes in 4 files

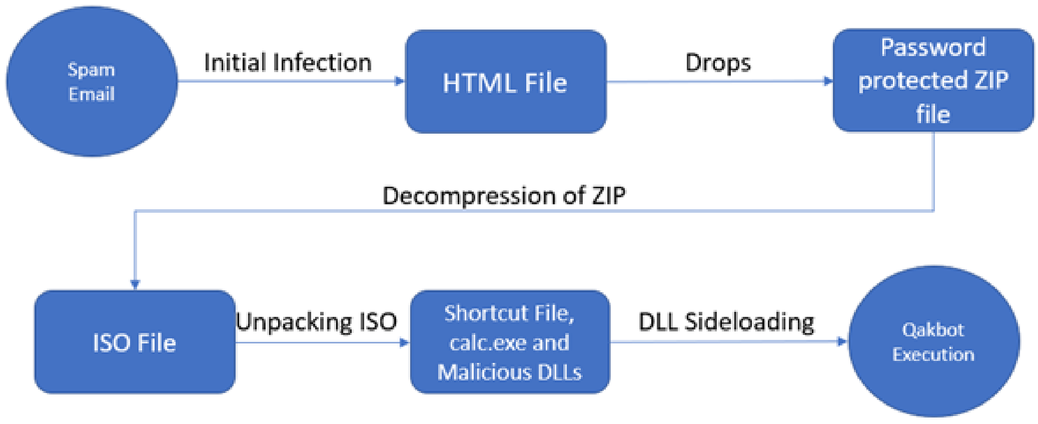
12:03 AM · Jul 15, 2022

154 Reply Copy link

Read 4 replies

In this campaign, the spam message contains an HTML file that has base64 encoded images and a password-protected ZIP file. The password-protected zip file contains an ISO file (i.e. Report Jul 14 47787.iso), and the password for opening it is reported in the HTML file. The use of password-protected zip file is a common technique adopted by threat actors to evade detection.

Once clicked the image file, it is mounted and shows a .lnk file masquerading as a PDF file. If the victim opens the .lnk file, the Qakbot infection process starts.



The ISO file contains four different files:

- WindowsCodecs.dll
- 7533.dll.

The .LNK file appears as a PDF containing information of interest for the victims. The shortcut points to the Calculator app in Windows. Upon executing the Windows 7 Calculator, it will automatically attempt to load the legitimate WindowsCodecs DLL file. The code will load any DLL with the same name if placed in the same folder as the Calc.exe executable resulting in the execution of a malicious DLL.

"In this case, the application is calc.exe, and the malicious file named WindowsCodecs.dll masquerades as a support file for calc.exe." reads the analysis published by Cyble. "Upon executing the calc.exe, it further loads WindowsCodec.dll and executes the final Qakbot payload using regsvr32.exe. The final payload injects its malicious code into explorer.exe and performs all the malicious activities."

The threat actors bundle the Windows 7 version of the DLL because the attack doesn't work against Windows 10 Calc.exe and later.

Cyber shared MITRE ATT&CK® Techniques and Indicators of Compromise (IoCs).

Follow me on Twitter: **@securityaffairs** and **Facebook**

[adrotate banner="9″]	[adrotate banner="12″]

Pierluigi Paganini

(SecurityAffairs – hacking, malware)

[adrotate banner="5″]

[adrotate banner="13″]

FACEBOOK LINKEDIN TWITTER

DLL-SideLoading | Hacking | hacking news | information security news | malware | QakBot | Security Affairs | Security News securityaffairs

To contact me write an email to:

Pierluigi Paganini :
pierluigi.paganini@securityaffairs.co

LEARN MORE

QUICK LINKS

Home
Cyber Crime
Cyber warfare
APT
Data Breach
Deep Web
Digital ID
Hacking
Hacktivism
Intelligence
Internet of Things
Laws and regulations
Malware
Mobile
Reports
Security
Social Networks
Terrorism
ICS-SCADA
POLICIES
Contact me