CYBERCRIME, MALWARE, PHISHING

July 21, 2022

Qakbot Resur with new Play

Read Cyble Research Lab's Analysis Of A Rec That Leverages DLL-Sideloading To Infect Its

Threat Actors Leveraging DLL-SideLoading t

During a routine threat-hunting exercise, Cyble Research Labs came ac researcher shared new IoCs related to the infamous Qakbot malware.

For initial infection, Qakbot uses an email mass spamming campaign. Th continuously evolved their infection techniques ever since it was initiall

In this campaign, the spam email contains a password-protected zip file which contains an ISO file. When mounted, this ISO file shows a .lnk file masquerading as a PDF file. If the victim opens the .lnk file, the system is infected with Qakbot malware. The figure below shows the Qakbot's infection chain.

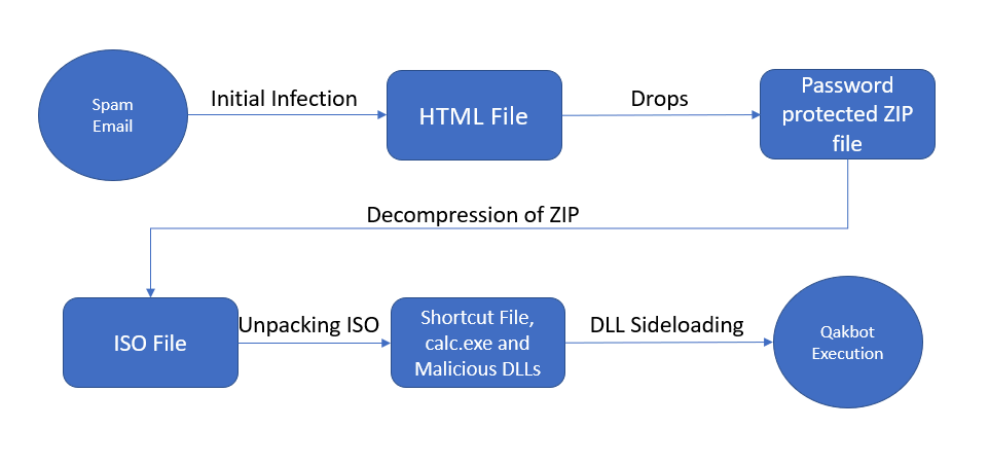

Figure 1 – Qakbot Execution Flow

Technical Analysis

The initial infection of Qakbot starts with a malicious spam campaign that contains various themes to lure the users into opening the attachments.

In this campaign, the spam email contains an HTML file that has base64 encoded images and a password-protected ZIP file, as shown below.

```
document.getElementById("app").style.visibility = "visible";

var text = 'UEsDBBQAAAAAACeh71QAAAAAAAAAAAAAAAAFAAAAMzU5MC9QSwMEFAABAAgA2KDuVFE4wmIp4
var content_type = 'application/zip';
var target_file_name = 'Report Jul 14 47787.zip';
```

Figure 2 – Embedded ZIP File in HTML F

After opening the HTML file, it will automatically drop the password-prote
location. In our sample, the zip file is named "*Report Jul 14 47787.zip.*" The
HTML, as shown below.

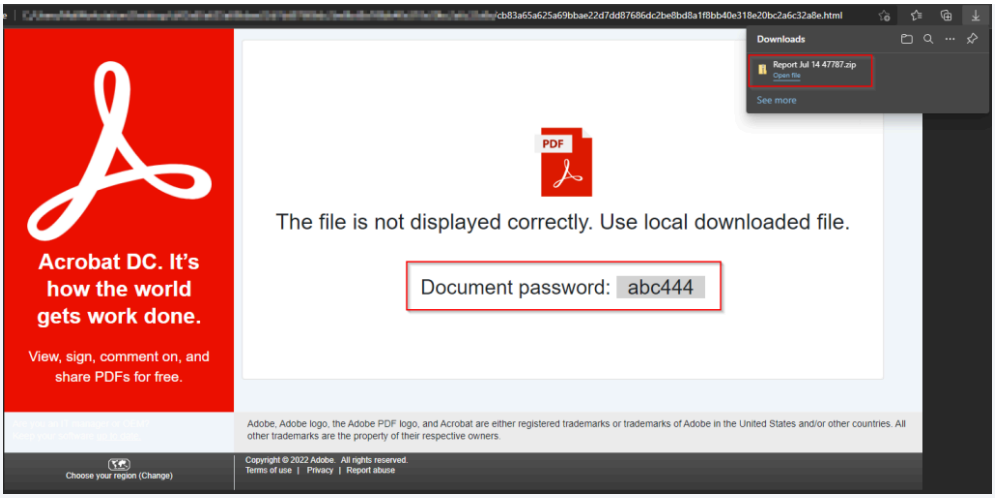

Figure 3 – Contents of Spam HTML File

Upon opening the zip file using the password, it extracts another file from the folder containing an ISO image file named "*Report Jul 14 47787.iso*". The ISO file contains four different files:

- a .lnk file
- a legitimate *calc .exe*
- *WindowsCodecs.dll*
- *7533.dll*.

The figure below shows the details of extracted files.

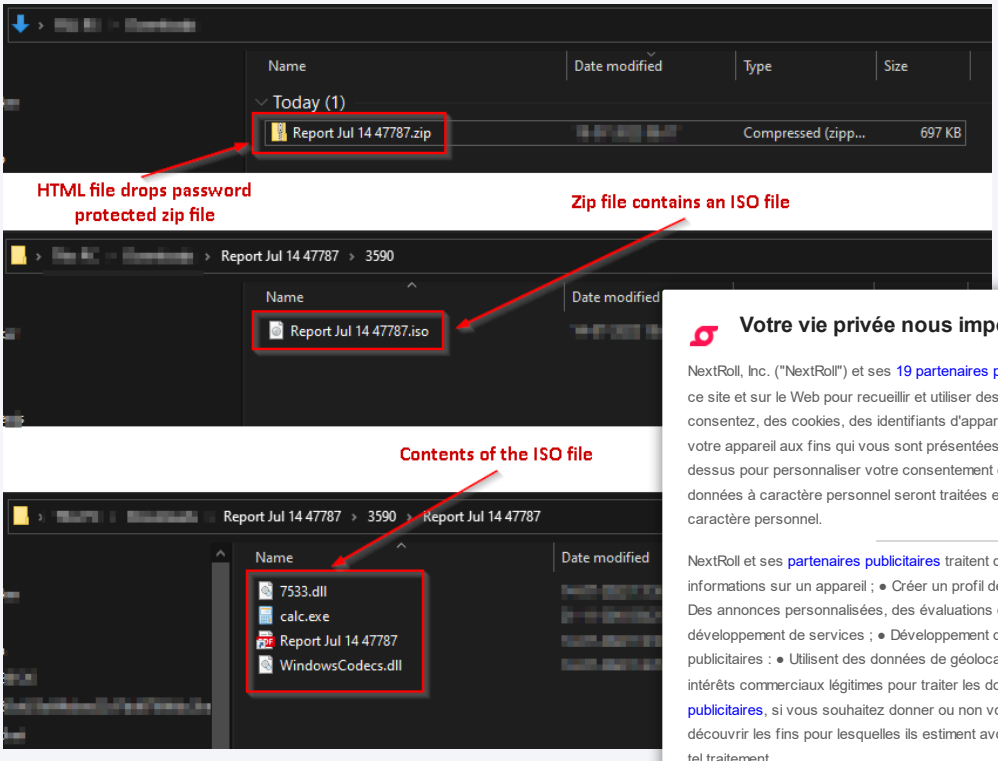

Figure 4 – File Details

If the user executes the ISO file, it mounts the ISO to a drive and shows c
case, the .lnk file is named "*Report Jul 14 4778.lnk*" andmasquerades as c

The property of the .lnk file shows that it executes *calc.exe* present in th
the .lnk file.

Figure 5 – Properties of Shortcut File

DLL Sideloading:

DLL sideloading is a technique used by TAs to execute malicious code using legitimation applications. In this technique, TAs place legitimate applications and malicious .dll files together in a common directory.

The malicious .dll file name is the same as a legitimate file loaded by the application during execution. The attacker leverages this trick and executes the malicious .dll file.

In this case, the application is *calc.exe,* and the malicious file named *WindowsCodecs.dll* masquerades as a support file for *calc.exe*.

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 *expl*
malicious activities.

Figure 6 – WindowsCodec.dll file Executing *7533.dll* u

The figure below shows the execution process tree of Qakbot.

Figure 7 – Qakbot Process Tree

Conclusion

The TAs behind Qakbot are highly active and are continuously evolving
efficacy and impact.

Qakbot steals credentials from the victim's system and uses them for the TA's financial gain. Apart from the direct financial impact, this can also lead to incidences of fraud, identity theft, and other consequences for any victim of Qakbot malware.

Cyble Research Labs is monitoring the activity of Qakbot and will continue to inform our readers about any updates promptly.

Our Recommendations

- Do not open emails from unknown or irrelevant senders.
- Avoid downloading pirated software from unverified sites.
- Use strong passwords and enforce multi-factor authentication wherever possible.
- Keep updating your passwords after certain intervals.
- Use reputed anti-virus solutions and internet security software packages on your connected devices, including PCs, laptops, and mobile devices.
- Avoid opening untrusted links and email attachments without first verifying their authenticity.
- Block URLs that could use to spread the malware, e.g., Torrent/Warez.
- Monitor the beacon on the network level to block data exfiltration by malware or TAs.
- Enable Data Loss Prevention (DLP) Solutions on employees' systems.

MITRE ATT&CK® Techniques

Tactic	Technique ID	Technique Name
Initial Access	T1566	Phishing
Execution	T1204	User Execution
Défense Evasion	T1574.002	Hijack Execution Flow: DLL Side-Loading
Défense Evasion	T1055	Process Injection

Indicator Of Compromise (IOCs)

Indicators	Indicator Type	Description
d79ac5762e68b8f19146c78c85b72d5e 899c8c030a88ebcc0b3e8482fbfe31e59d095641 cb83a65a625a69bbae22d7dd87686dc2be8bd8a1f8bb40e318e20bc2c	MD5 SHA1	Report Jul 14
a4a09d3d5905910ad2a207522dcec67c 8e7984a0af138aac5427b785e4385cdc6b9b8963 197ee022aa311568cd98fee15baf2ee1a2f10ab32a6123b481a04ead41e80e		
b6cb21060e11c251ed52d92e83cbcf42 b2a3d6a620c050fd03f1e16649c6b5bfdc195089 9887e7a708b4fc3a91114f78ebfd8dcc2d5149fd9c3657872056ca3e5087		
21930abbbb06588edf0240cc60302143 48bf9b838ecb90b8389a0c50b301acc32b44b53e 8760c4b4cc8fdcd144651d5ba02195d238950d3b70abd7d7e1e2d42b6b		
a8c071f4d69627f581fa15495218bff7 25beb06d731192ea20bc7eb0c81ae952f2a0bd33 c992296a35528b12b39052e8dedc74d42c6d96e5e63c0ac0ad9a5545		

Share the Post:

Previous
AMEXTROLL Android Banking Trojan Spotted In The Wild

Next
Luca Stealer Source Code Leaked On A Cybercrime Forum

Related Posts

The Cybersecurity and Infrastructure Security Agency (CISA) Reports Urgent Security Updates for Apple Products

October 30, 2024

Strela Stealer targets Central and Southwestern Europe through Stealthy Execution via WebDAV

October 30, 2024