Qakbot Malware: Exploring Its Diverse Distribution Methods

By cybleinc

Published: 2023-02-17 · Archived: 2026-04-05 22:58:20 UTC

Cyble revisits Qakbot malware and examines its recent distribution methods using various file formats.

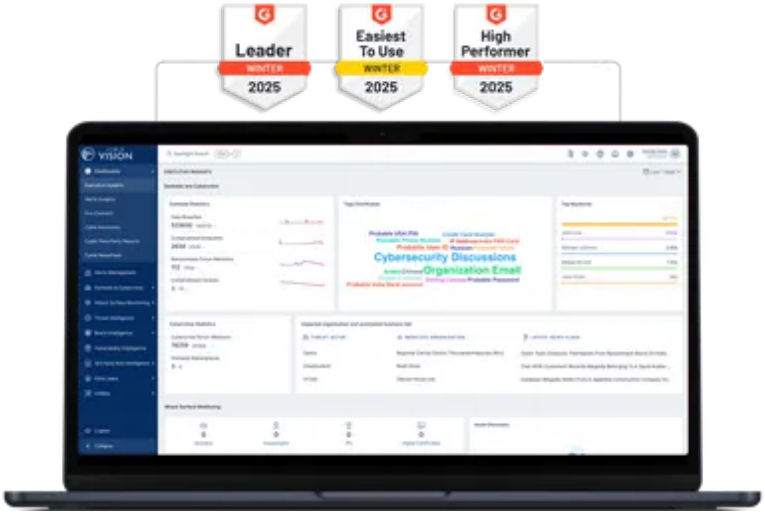
Threat Actor Uses Digital Certificate as a Cover to Hide Malicious Script

Threat Actors (TAs) are constantly devising new methods to infect users for various reasons, such as avoiding detection from anti-virus solutions, increasing the chances of successfully infecting their targets, and inventive ways to compromise their victims. Recently, many malware families have been observed utilizing OneNote attachments as part of their spam campaigns. OneNote is a robust digital notebook application developed by Microsoft, which enables users to collate and structure their notes, thoughts, and ideas in a single, convenient location.

Recently, multiple distribution methods have been detected for the widely known banking trojan Qakbot. These methods include using malspam with OneNote attachments, malspam with zip files containing WSF, and others. This analysis below has detailed the techniques employed by Qakbot to propagate its infection and reach a diverse audience.

See Cyble in Action

World's Best AI-Native Threat Intelligence



Distribution of Qakbot Via OneNote Using Batch & PowerShell

The initial phase of the infection begins with a spam email with a OneNote attachment. Once the recipient opens the attachment, an embedded BAT file is dropped and executed, leading to the launch of a PowerShell script. This script then proceeds to download a DLL for the Qakbot malware. Finally, the DLL is executed using rundll32.exe.

The delivery mechanism of Qakbot through OneNote using PowerShell is illustrated in the figure below.

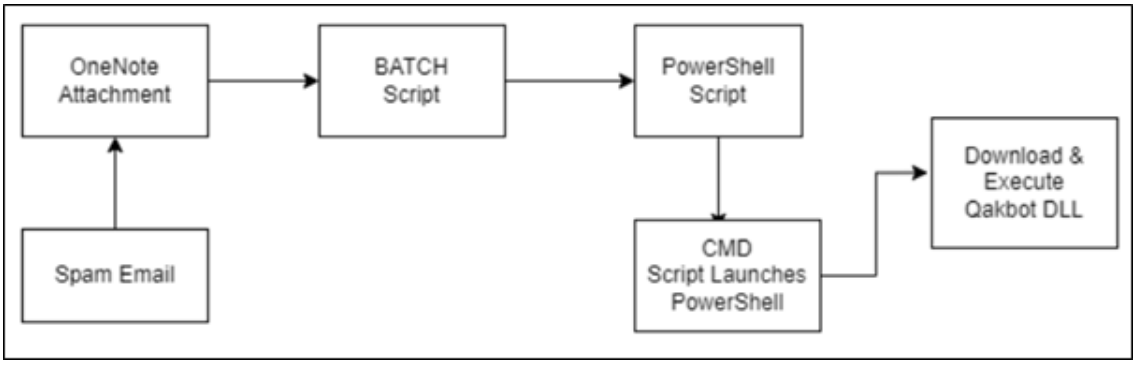


Figure 1 – Qakbot delivery using Batch & PowerShell

Qakbot malware is distributed to users through spam emails that contain a OneNote attachment. The email's subject line reads *"RE: DRCP Hire- Success Story.."* The attachment is named *"Contracts – Copy.one"*, as depicted in the image below.

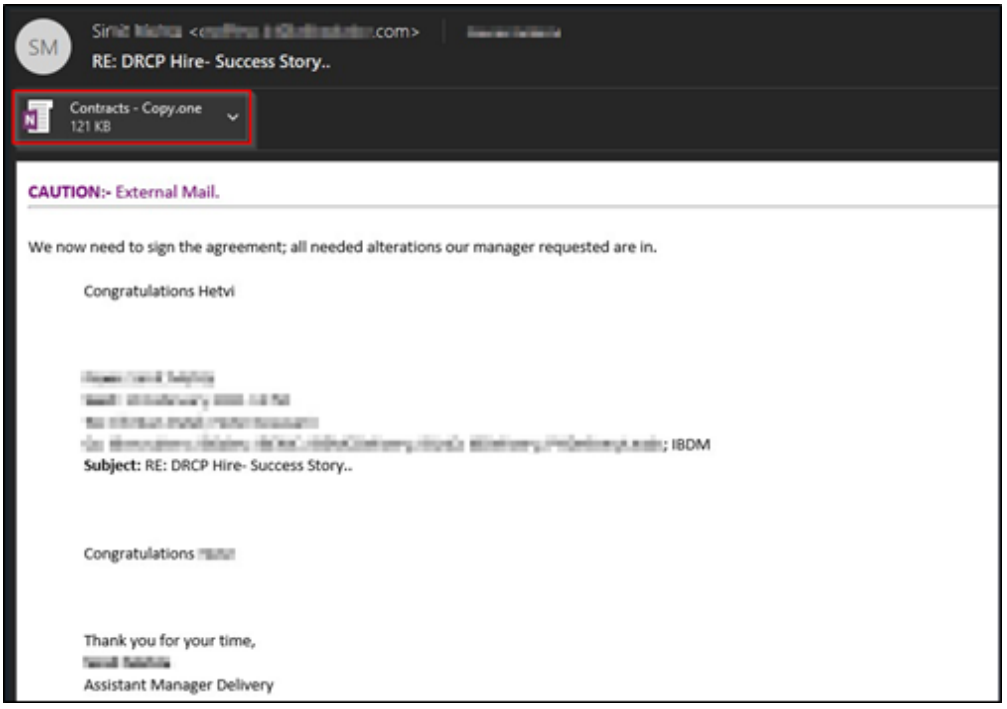
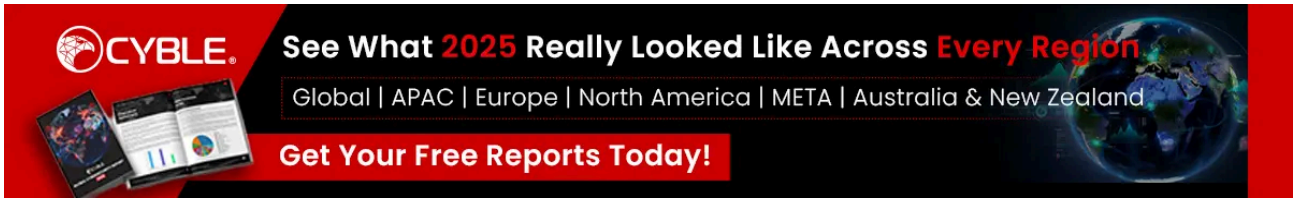


Figure 2 – Spam email with OneNote attachment

After the user opens the OneNote attachment, a page appears with a message that appears to contain a cloud-based attachment. This message is designed to deceive the user into double-clicking on it to view the attachment, which ultimately triggers the Qakbot infection process.



The figure below displays the OneNote page containing the fraudulent message.

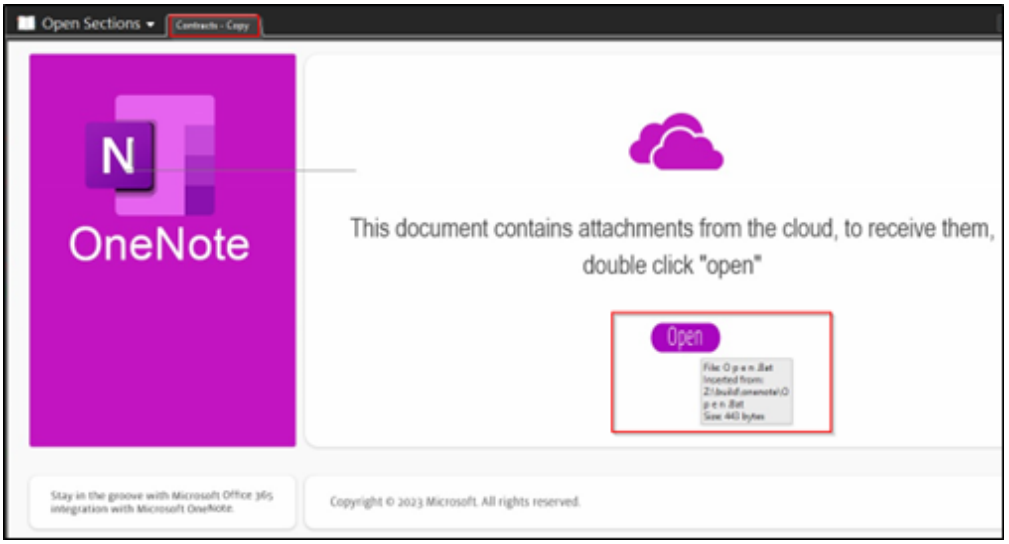


Figure 3 – OneNote file drops BAT file

When the “open” button is clicked on a OneNote page, it performs a covert action by dropping a BAT file named “O p e n .Bat” without user notification and then executing it. This batch script launches an obfuscated PowerShell content that, in turn, drops a CMD file named “i.cmd” in the *%temp%* location and runs it.

The below figure shows the obfuscated batch script and command file containing an URL to download a malware payload.

Figure 4 – CMD file & Obfuscated BAT file

Upon execution of the “i.cmd” file, it utilizes a PowerShell script to download a file in GIF format from the URL *hxxps[:]//casualscollection[.]com/l2iy4Dn/09[.]gif* by using the *Invoke-Webrequest* command.

The file is then saved as a JPG file in the *%programdata%* path. However, the downloaded file is not an actual GIF file but a DLL Qakbot executable file, which is subsequently run using “Rundll32.exe” with the “Wind” parameter.

The process tree diagram of Qakbot reveals that, following the execution of the DLL file, the malware injects malicious code into “wermger.exe”. This code injection enables Qakbot to carry out its malware activities, such as stealing sensitive information.

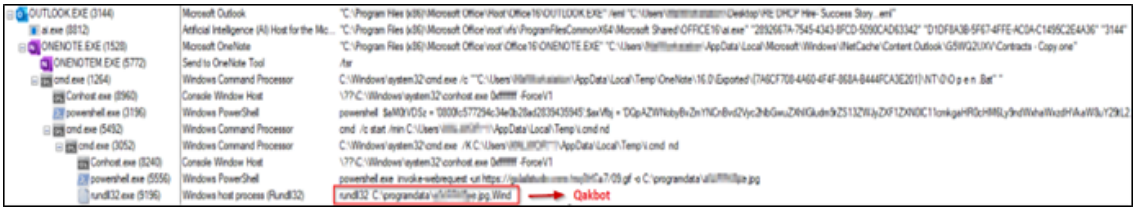


Figure 5 – Process tree of OneNote delivering Qakbot via BAT & PowerShell

Distribution of Qakbot Via Windows Script (.wsf) Files

The infection process starts with the distribution of a spam email containing an archive file. This archive file includes a script with a .wsf extension that is executed using the Windows system file WScript.exe.

The script then downloads a DLL file containing the Qakbot malware, which is subsequently run using rundll32.exe.

The figure below illustrates the delivery mechanism of Qakbot using WSF files.

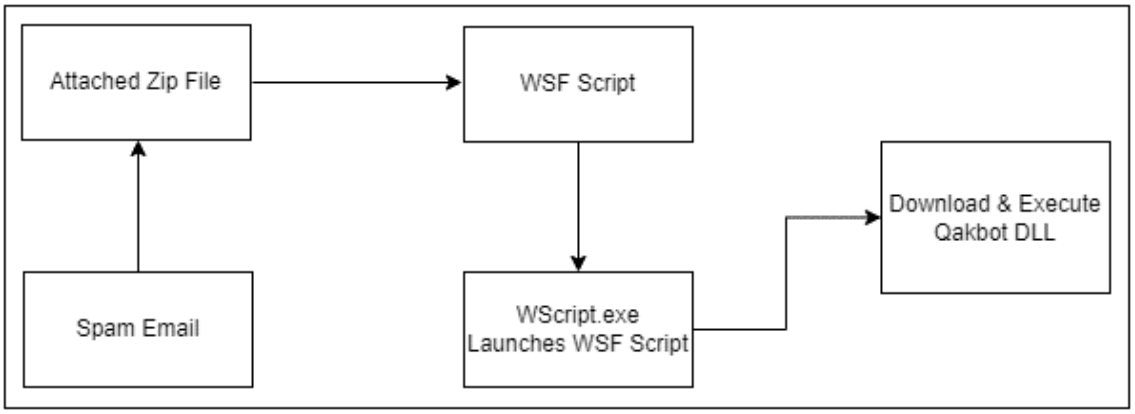


Figure 6 – Qakbot Delivery Mechanism using wsf file

One of the methods of disseminating the Qakbot malware involves sending spam emails that come with a compressed file attachment named “Shared Document From Cloud 913815.zip”, as shown below.

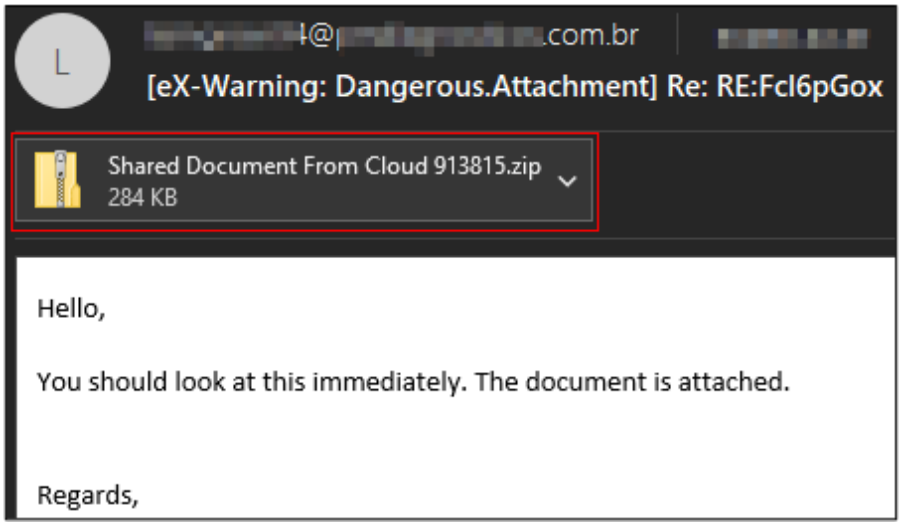


Figure 7 – Spam email with zip attachment

One of the three files that come with the email attachment is a .wsf file with the name “Adobe Cloud Certificate 913815.wsf”.

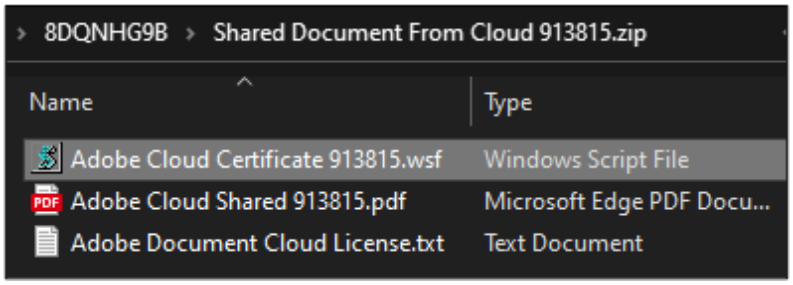


Figure 8 – Contents of Email Attachment

Interestingly, the Threat Actor (TA) has inserted a malicious JScript between digital certificates in the .wsf file, as shown below.

Figure 9 – Malicious JScript Inserted Between Digital Certificates

When the user attempts to open the “Adobe Cloud Certificate 913815.wsf” file, it will be launched through wscript.exe. The .wsf script has code to download a Qakbot DLL file from the URL: *hxxp://gkjdepok[.]org/crtfc/lwbYFO.dll* and saves it to the *C:\ProgramData* directory. Finally, the .wsf script launches the Qakbot DLL by utilizing “Rundll32.exe” with the “Wind” parameter.

The figure below shows the code of the .wsf script.

Figure 10 – Content of the .wsf file

Below, you can see the process tree of Qakbot's execution through the .wsf file.

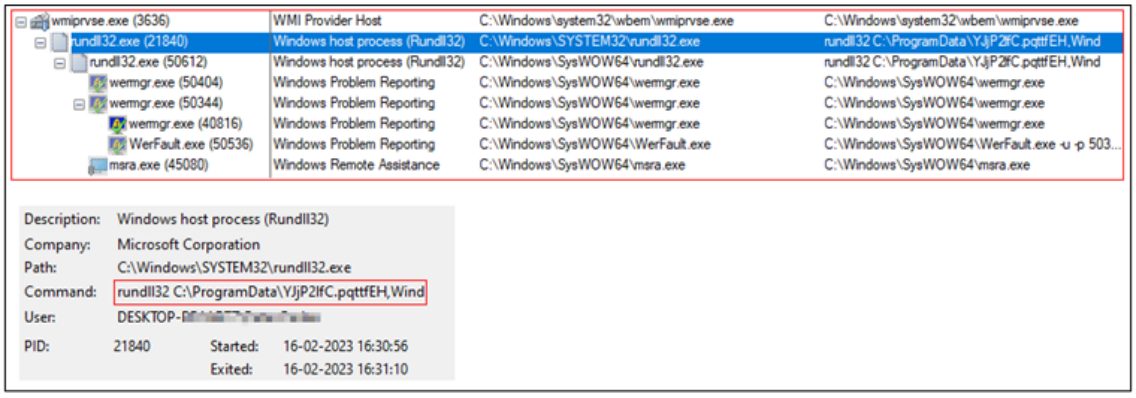


Figure 11 – Process Tree

Distribution of Qakbot Via OneNote Using Jscript (.jse) file

The first step of the infection process is initiated by a spam email that includes a OneNote attachment. Upon opening the attachment, an embedded JSE file is deployed and executed. This JSE file then drops and triggers the execution of a BAT file, which in turn launches a PowerShell script and will execute the QakBot payload.

The PowerShell script proceeds to download a DLL associated with the Qakbot malware, which is ultimately executed using the *rundll32.exe* command. The below figure shows the delivery mechanism of Qakbot using the .jse file.

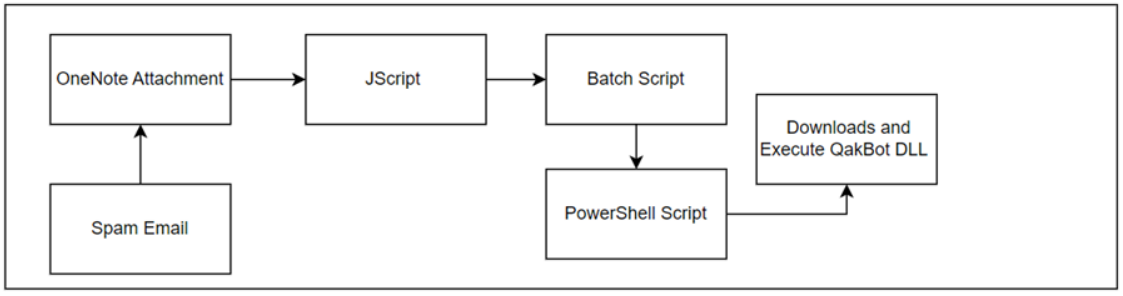


Figure 12 – QakBot Delivery Mechanism Using JScript and Batch Script

Once the user opens the malicious OneNote file, a page is displayed, which contains a deceptive message that appears to contain a cloud-based attachment.

The message is intended to mislead the user into double-clicking it to view the attachment, which initiates the Qakbot infection process.

The image below depicts the OneNote page that contains the false message.

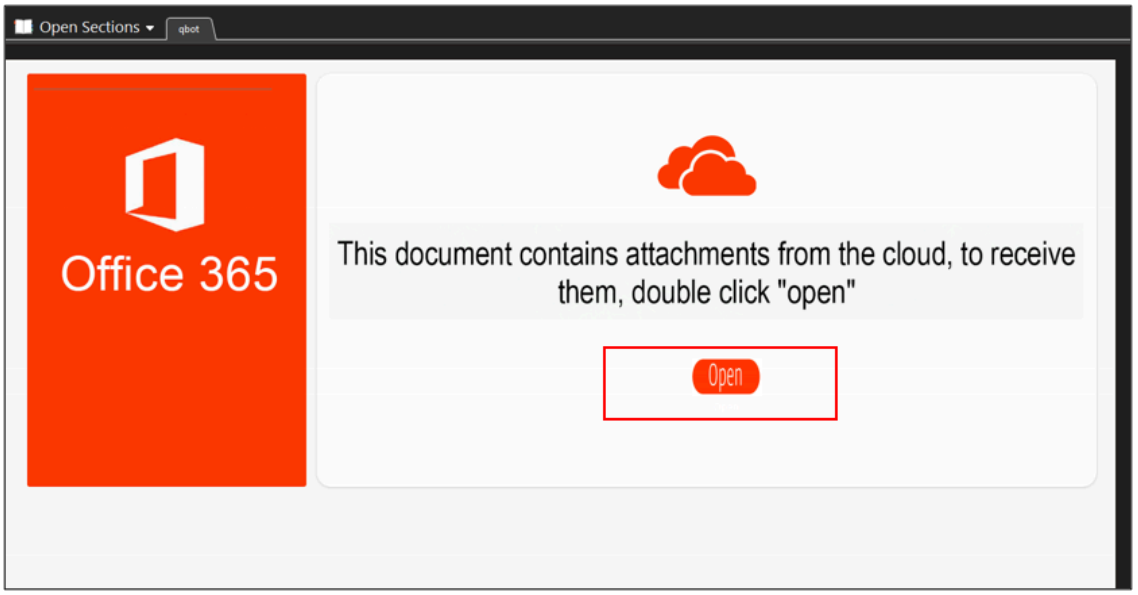


Figure 13 – Malicious OneNote Attachment

After a user clicks on the “Open” button, the OneNote file drops a file named “Open.jse” in the temp folder. It is an encoded script file, which will further drop and execute the .bat file named “default.bat”.

The figure below shows the encoded/decoded .jse file.

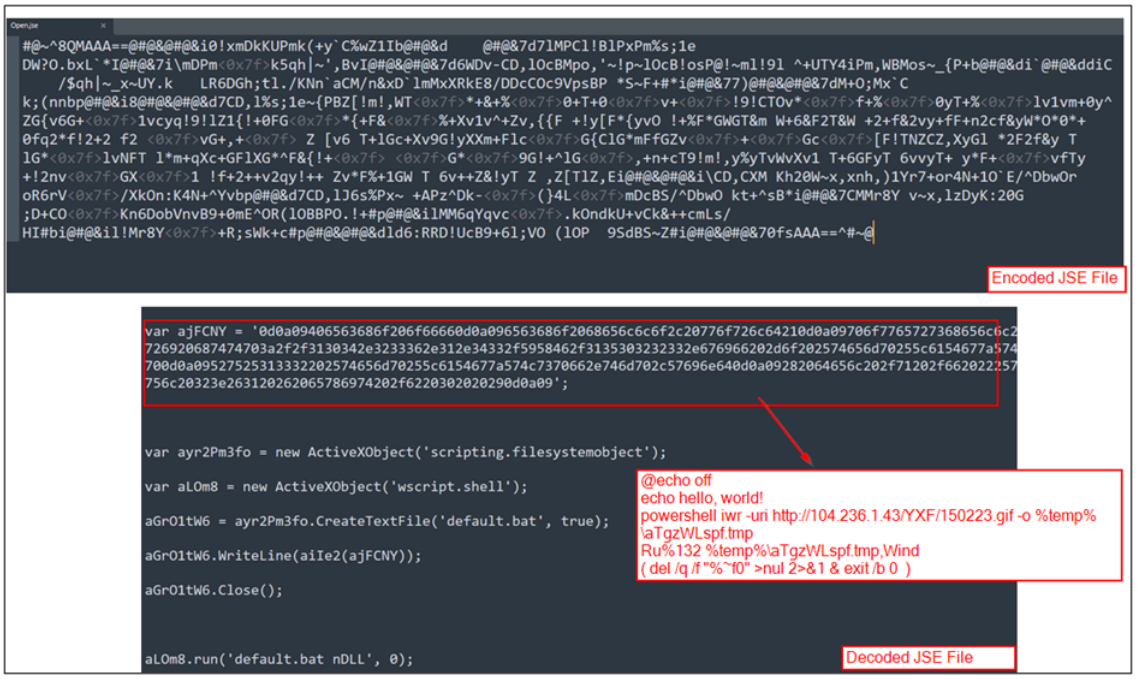


Figure 14 – Encoded/Decoded JScript File

Upon execution of the “default.bat” file, it utilizes a PowerShell script to download a file named “150223.gif” from the URL *http[:]//104.236[.]1.43/YXF/* using the PowerShell command and saves it to the temporary folder of the user’s system with a random name, “aTgzWLspf.tmp”.

The file downloaded from the provided URL is not a genuine GIF file but rather an executable file of the Qakbot malware in DLL format, which is then executed using the “Rundll32.exe” command with the “Wind” parameter.

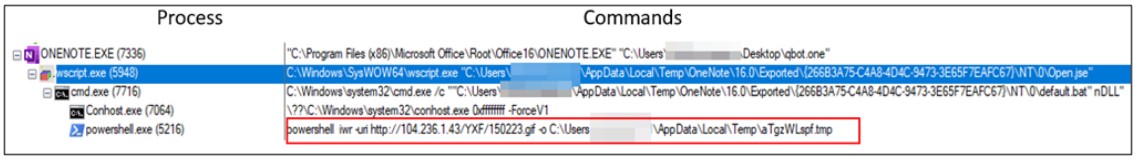


Figure 15 – Process Tree

Distribution of Qakbot Via OneNote Using html Application (hta) file

In this method, the Qakbot infection begins with a spam email that contains a OneNote attachment. Once the user opens the attachment, an embedded HTA file is dropped, which then executes through mstha.exe. This leads to the download of a Qakbot DLL file that is subsequently executed via rundll32.exe.

Our earlier blog here contains a thorough analysis of Qakbot malware’s infection chain.

Final Payload

QakBot, also known as QBot or QuakBot, is a type of banking Trojan that mainly targets Windows systems. It was first discovered in 2007 and has since undergone numerous updates and changes to its code in order to evade detection by security software. It can steal sensitive information, exfiltrate confidential data, and propagate to other machines on the network to install other malicious software.

Its modular design makes it customizable to carry out specific tasks such as keylogging, credential theft, network reconnaissance, botnet functionality, and ransomware deployment. Its operators continuously update its code to evade detection and carry out successful attacks.

Conclusion

Qakbot malware represents a clear example of the constantly evolving threat landscape, underlining the importance of remaining vigilant in the cybersecurity domain.

Its complex structure, extensive impact, and widespread prevalence reinforce the need for proactive and robust security measures. The TAs responsible for Qakbot remain highly active. They consistently adapt their methods to avoid detection and maximize their gains, using innovative attack vectors such as OneNote attachments to display their sophistication and ingenuity.

Cyble Research and Intelligence Labs continues to monitor the activity of Qakbot and other malware and will provide timely updates to our readers.

Our Recommendations

We have listed some essential cybersecurity best practices that create the first line of control against attackers. We recommend that our readers follow the best practices given below:

- Do not open emails from unknown or unverified 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	Spearphishing Attachment	
Execution	T1204 T1059 T1218 T1059	User Execution Command and Scripting Interpreter Rundll32 PowerShell	
Defense Evasion	T1140 T1564	Deobfuscate/Decode Files or Information Hidden Window	

	T1055	Process Injection	
Credential Access	T1555 T1056	Credentials from Password Stores Keylogging	
Discovery	T1087 T1518 T1057 T1007	Account Discovery Software Discovery Process Discovery System Service Discovery	
Collection	T1113 T1115	Screen Capture Clipboard Data	
Command and Control	T1071 T1105	Application Layer Protocol Ingress Tool Transfer	

Indicators Of Compromise (IoCs)

Indicators	**Indicator Type**	**Description**
e0481af37fbb369ced2bff17468218b4676995b609fac1f96f604d93c55cfb5a	Sha256	Spam Email
82ea16ea858ac6b9580f604695ebeaf1f004ae882a7d0e48688c28d466662f10	Sha256	OneNote Attachment
518518b0929911353cd7ab95d873e1fb290d8a494122cfb88e7f8bcf015576c8	Sha256	O p e n .Bat
5ade2a474118032ab353c7e835a0ca90669e690c997c8b374f94f408a9510b4e	Sha256	i.cmd
7dd17b8cb0639732fe6929a5d7e1431fedae58acd401a7810afc0be8f9c42ad0	Sha256	a8qZzTS.jpg (DLL file)
hxxps[:]//casualscollection[.]com/l2iy4Dn/09[.]gif	URL	URL used to download Qakbot DLL
d80f18f5fc088c87905ee19c3f7b1dfd22920584913cc7b5925d64ad375e838f	Sha256	Spam Email
9981bf6ad64c2f48de970948b4dc6ca5e3e5f9ca8b86c2db921e032cd4a4c6cb	Sha256	wsf Zip Attachment
d13f70c241681df78ffa91ef105bfee069e78e7daa125cb7c47a50d34b234f12	Sha256	wsf file
4949b9d77f80cdb79f498b2def775dea9371dd08e2d66b4f513da35337af38c9	Sha256	lwbYFO.dll (DLL file)
hxxp://gkjdepok[.]org/crtfc/lwbYFO.dll	URL	URL used to download

		Qakbot DLL
eca50ee3c2ed694bf8b42a4e0eb14555c70c0d6186cc2dc863af8265c25ba4f1	Sha256	OneNote Attachment
b0339e18da6bfea0c60e388e631de79a83e2bc20880d6b9624d4784465a330b7	Sha256	Open .jse
b435653b9e1860cf38d78911eb7341c4b9c8e09af765b28a490ed269413eb2b1	Sha256	default.bat
hxxp[:]//104.236.1[.]43/YXF/150223[.]gif	URL	URL used to download Qakbot DLL

Source: https://blog.cyble.com/2023/02/17/the-many-faces-of-qakbot-malware-a-look-at-its-diverse-distribution-methods/