|  |
| --- |
| [Nom de la société] |
| QakBot |
| Cyber Threat Intelligence | Malware Analysis |

|  |
| --- |
| Abdallah Chbaro (Student)  [Date] |

Table des matières

[About 2](#_Toc132043680)

[Overview of QakBot 3](#_Toc132043681)

[But what is HTML Smuggling? 3](#_Toc132043682)

[Attack Phases 4](#_Toc132043683)

[QakBot BB A.K.A TR/TA577 6](#_Toc132043684)

[WScript.exe 6](#_Toc132043685)

[QakBot Obama 7](#_Toc132043686)

[RegSVR32.exe 7](#_Toc132043687)

[IOCs 8](#_Toc132043688)

# About

Qakbot (AKA Qbot or Pinkslipbot) is a modular second-stage malware with backdoor capabilities, initially purposed as a credential stealer, and has been noted by CISA as one of the top malware strains of 2021. Classified as a banking trojan, worm, and remote access trojan (RAT), Qakbot steals sensitive data and attempts to self-propagate to other systems on the network. Qakbot also provides remote code execution (RCE) capabilities, allowing attackers to perform manual attacks to achieve secondary objectives such as scanning the compromised network or injecting ransomware.

Qakbot has been used by apex ransomware gangs such as REvil, ProLock, and Lockbit to distribute several big-game hunting ransomware strains. Qakbot's many modules also allow automated targeting of financial data, locally stored emails, system passwords or password hashes, website passwords, and cookies from web browser caches. They can also log keystrokes to steal any typed credentials.

# Overview of QakBot

1. HTML drops .ZIP via HTML Smuggling
2. ZIP contains ISO file
3. ISO contains .lnk file
4. Lnk file launches calc.exe
5. Calc.exe sideloads windowscodecs.dll
6. Windowscodes.dll executes the malicious payload DLL

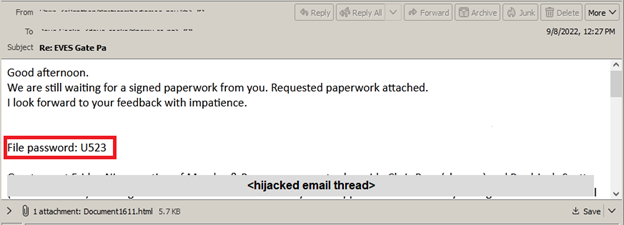
There are variations of QakBot malware, such as QakBot BB, QakBot Obama and others.

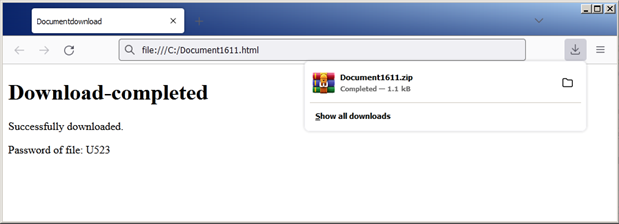
## But what is HTML Smuggling?

HTML smuggling employs HTML5 attributes that can work offline by storing a binary in an immutable blob of data within JavaScript code. The data blob, or the embedded payload, gets decoded into a file object when opened via a web browser. Threat actors take advantage of the versatility of HTML in combination with social engineering to lure the user into saving and opening the malicious payload.

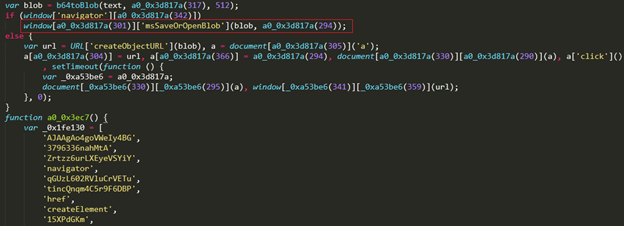
# Attack Phases

Qakbot, one of the notorious malware types actively distributed through spam, has been using HTML smuggling since June 2022. It shifted from macro documents to HTML as Microsoft pushed restrictions on using macros from the Internet.

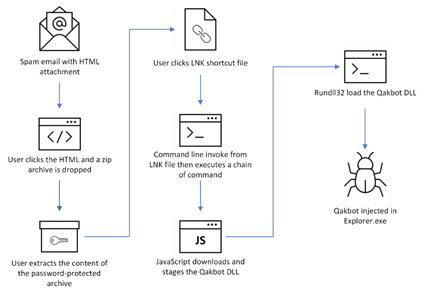




Looking at the HTML source code, the functions, and methods used to assemble the payload are obfuscated into arrays. This attempts to conceal suspicious commands and evade email gateway filters. This technique abuses the JavaScript function msSaveOrOpenBlob to dynamically generate and drop the malicious payload to disk.



The ZIP archive dropped contains one file, a Windows Shortcut (LNK). Once the user opens the ZIP archive and launches the LNK file, it invokes the Windows Command Processor which creates a download folder inside the %LOCAPPDATA% directory and downloads and executes a JavaScript using the built-in curl tool and WScript, respectively. The JavaScript file downloads the main payload, a Qakbot DLL. The payload is loaded using rundll32 and then injected into explorer.exe through process hollowing.



# QakBot BB A.K.A TR/TA577

|  |  |  |  |
| --- | --- | --- | --- |
| Behavior | Tactic | Technique | Detection |
| Threat Actor sends an url or an .html file as attachment, that which invite the user to download a ZIP related to the campaign. The password to open the ZIP is contain in the initial email. | Initial Access [TA0001] | Spearphishing Attachment [T1566.001] | Gateway Mail:  file\_name: document[numbers].html OR infos[numbers].html |
| These .lnk files contains malicious commands to execute the download and the execution of Qakbot | Execution [TA0002] | Malicious file  [T1204.002] | EDR :  file\_name: \*.lnk AND file\_path contains \*cmd.exe /q/c\* |
| The .lnk file excute cmd.exe which will call curl.exe to download an .html web page and write it into a .js file on the victim’s system | Execution [TA0002]  Defense Evasion  [TA0005] | Command and Scripting Interpreter  [T1059] | EDR : parent\_process : « cmd.exe » AND (process : « ping.exe » OR process : « curl.exe ») |
| Qakbot uses wscript.exe to execute a script located in "AppData" using wscript.exe | Execution [TA0002] | Command and Scripting Interpreter  [T1059] | EDR :  process: “wscript.exe“ AND process\_cmdline:“\*\AppData\\*.js” |
| Scheduled task is used to do the privilege escalation. It contain a base64 encoded command used by powershell.exe | Execution [TA0002] | Scheduled Task  [T1053.005] | EDR :  process: “schtasks.exe“  AND process\_cmdline:“\*powershell.exe –encodedCommand\*” |
| Qakbot will excute the DLL with regsrv32.exe and has the ability to inject dll into memory. | Execution [TA0002]  Defense Evasion  [TA0005] | Process Injection [T1055] | EDR : parent\_process : « regsrv32.exe » AND (process : « explorer.exe » OR process « msra.exe » OR process : « OneDriveSetup.exe » OR process : « mobsync.exe » OR process :« iexplorer.exe ») |
| Communication C2 Qakbot BB Botnet | Command and Control [TA0011] | Application Layer Protocol: Web Protocols [T1071.001] | SIEM :  uri\_path : /t5 AND method : POST AND user-agent : Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0 |

## WScript.exe

Windows Script Host provides an environment in which users can execute scripts in various languages that use various object models to perform tasks.

# QakBot Obama

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Behavior | Tactic | Technique | | Detection |
| Threat Actor sends an .html file as attachment, that which invite the user to download a ZIP related to the campaign. The password to open the ZIP is contained in the initial email. | Initial Access [TA0001] | | Spearphishing Attachment [T1566.001] | Email :  Attachment name matches : Calculation#\S\*\.html  More restrictive regex : [A-Z]\w+\#\d+\(\w+\d+\)\.html  Ex: Calculation#8785(Sep16).html |
| lnk file contains malicious commands to execute the malicious Javascript | Execution [TA0002] | | Malicious file  [T1204.002] | EDR :  file\_name: \*.lnk AND  file\_path matches [a-z]+\/[a-z]+[A-Z][a-z]+\.js$  Ex: C:\more\seeSay.js |
| **The malicious Javascript will executes cmd.exe via wscript.exe**  You can find in the commandline a .bat extension and a specific argument linked to this bat file : «  r egs v » | Execution [TA0002]  Defense Evasion  [TA0005] | | Command and Scripting Interpreter  [T1059] | EDR : parent\_process : wscript.exe AND process : cmd.exe AND process\_commandline matches \.bat\"\sr\segs\sv\"$  Ex commandline : ""E:\more\myTheir.bat" r egs v" |
| The .bat file executes cmd.exe which will call regsvr32.exe to execute a dll file with a .db extension | Execution [TA0002]  Defense Evasion  [TA0005] | | Command and Scripting Interpreter  [T1059] | EDR : parent\_process : cmd.exe AND process : regsvr32.exe AND process\_commandline matches \.db$  Ex: commandline : regsvr32 more/veryAs.db |
| Qakbot will excute the DLL with regsrv32.exe and has the ability to inject dll into memory. | Execution [TA0002]  Defense Evasion  [TA0005] | | Process Injection [T1055]  Process Hollowing [T1055.012] | EDR : parent\_process : « regsrv32.exe » AND (process : « explorer.exe » OR process « msra.exe » OR process : « OneDriveSetup.exe » OR process : « mobsync.exe » OR process :« iexplorer.exe ») |
| Communication C2 Qakbot BB Botnet | Command and Control [TA0011] | | Application Layer Protocol: Web Protocols [T1071.001] | SIEM :  uri\_path : /t5 AND method : POST |
| Qakbot use abnormal port to reach its C2 | Command and Control [TA0011] | | Application Layer Protocol: Web Protocols [T1071.001] | SIEM :  An user that contact several direct IP on abnormal ports ("32101","2222","995","993") |

## RegSVR32.exe

Regsvr32 is a command-line utility to register and unregister OLE controls, such as DLLs and ActiveX controls in the Windows Registry. Regsvr32.exe is installed in the %systemroot%\System32 folder in Windows XP and later versions of Windows.

# IOCs

|  |  |
| --- | --- |
| File Name | Hash |
| Document1611.html | b79ff504eb6ec509b8b6b870dc2f0113825d859b |
| Document1611.zip | b5da32a803b31d769d4d330e9c923d8c2dc5da1f |
| File577.lnk | d92b31ddf25e30e7cc34239bf45c7ec913b713c4 |
| enhrP.s\_1L.QH0w.js | 0d17a7f60f7f5a6d5e00ed23635dd4998a5df307 |
| \_OIV.dll (Qakbot DLL) | 78542b48745136d9e77896ec77c7613c4386ad81 |
| jackboots. tmp (Qakbot DLL) | ed67cb8a6c44871ec6ffb6517d77b5e84f00b399 |
| PE40.vhd (VHD containing Qakbot) | 55781d120a91b71da2c51ed3657a73e819493f38 |
| Download URL for JS | hxxps://purepowerinc[.]net/nluGZ/082.html |
| Download URL for DLL (Qakbot) | hxxps://huhuwarcanoefestival[.]com/iSx1Ch/0509.html |