Maximizing Threat Detections of Qakbot with Osquery

research.loginsoft.com/threat-research/blog-maximizing-threat-detections-of-qakbot-with-osquery/

April 12, 2023

April 12, 2023
By **Bhargav K**

Initially, Qakbot spreads using malicious email attachments, drive-by-download attacks, or other forms of social engineering. The recent variants of Qakbot employ OneNote, Windows Script File (WSF), and HTML smuggling to disseminate malware as part of a new campaign. These campaigns showcase the adaptability and sophistication of Qakbot and the constant evolution of malware as a menace to cybersecurity. This article will explore Qakbot's tactics, techniques, and procedures (TTPs) and detection of Qakbot behaviour by querying and monitoring the operating system using SQL-like syntax with the help of osquery.

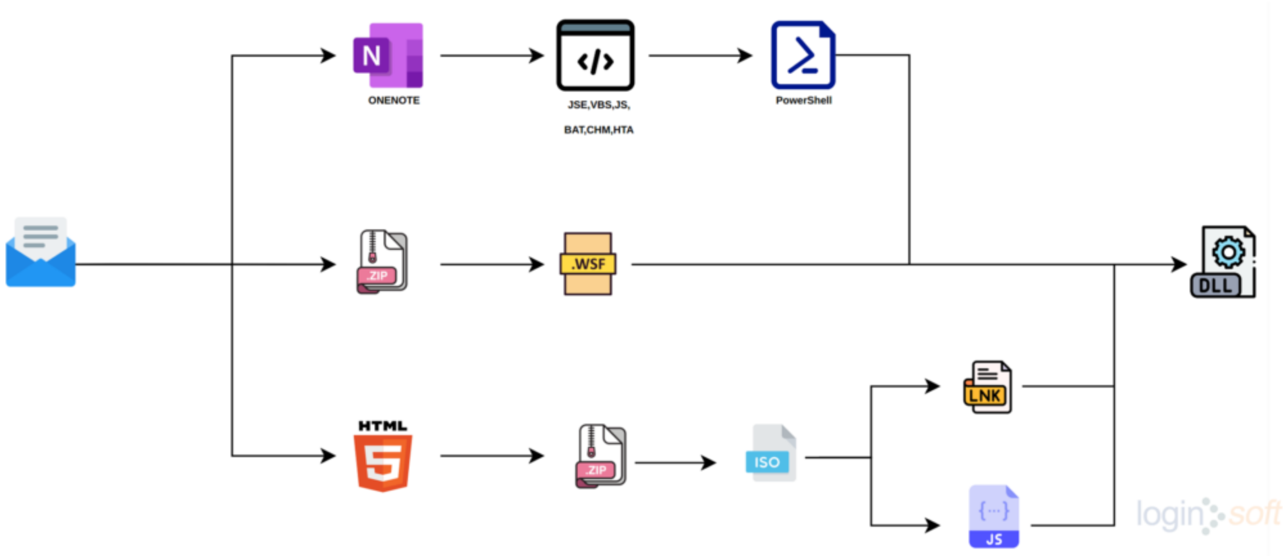


Fig: Qakbot Distribution Chain

Qakbot's Initial Infection

The chart below gives an overview of the campaigns carried out by threat actors over time to distribute Qakbot malware, and further we will delve into the details of these campaigns.

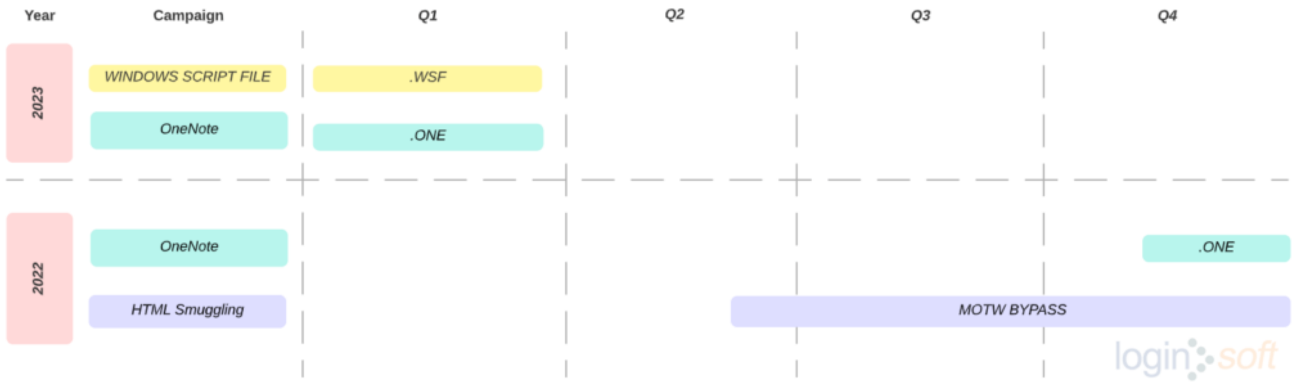


Fig: Qakbot’s Progression

Windows Script File (WSF) Campaign

The Qakbot threat actors are distributing an archive file containing .wsf files via spam mail as part of their campaign. When user attempts to open the .wsf file, the embedded JavaScript code will launch wscript which in turn downloads the Qakbot DLL.

The following query can be used to detect the launching of a WSF file.

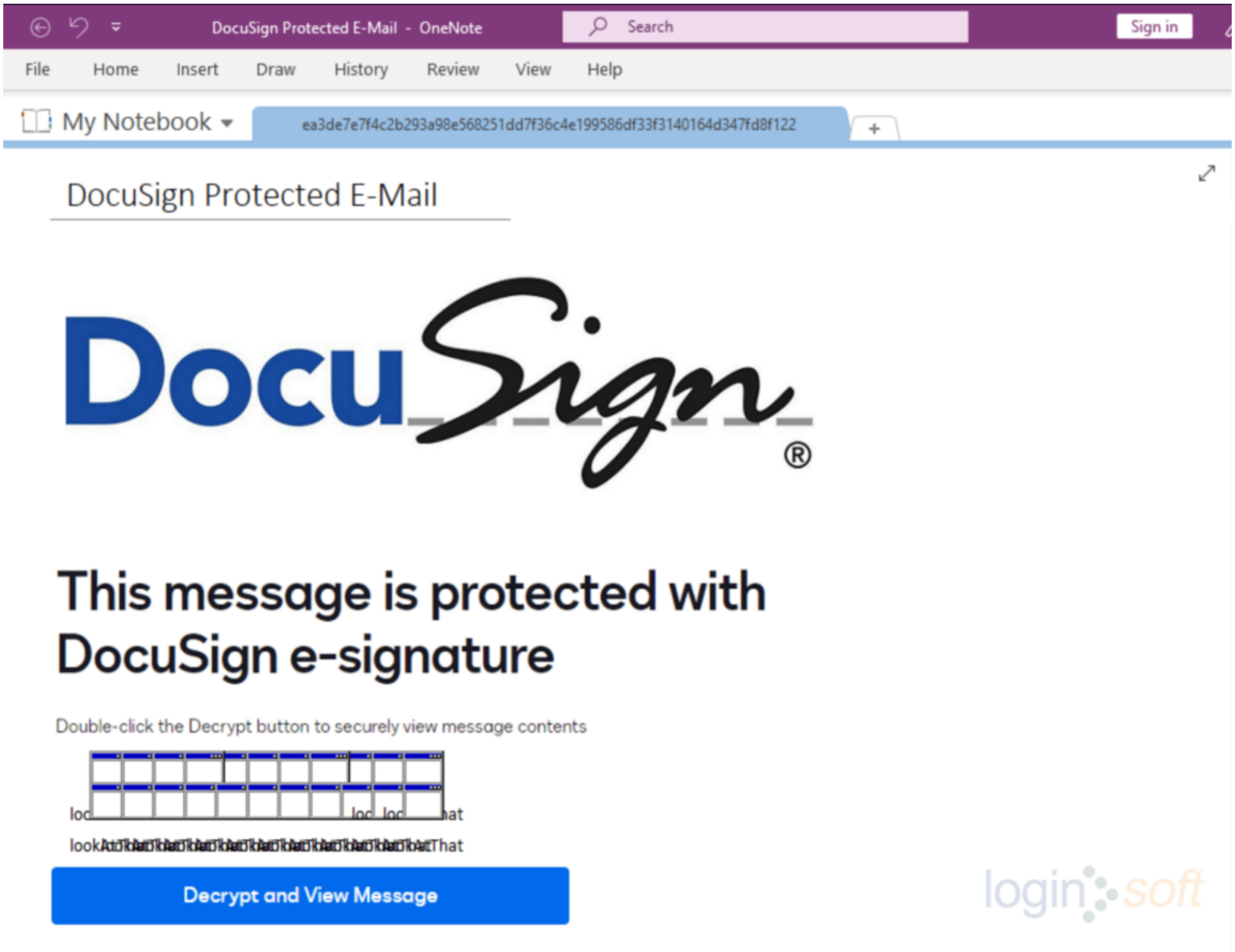
```
SELECT
   name,
   cmdline,
   path,
   pid,
   parent
FROM processes
WHERE cmdline LIKE '%.wsf%'
AND LOWER(name) IN ('wscript.exe','cscript.exe');
```

NOTE: Further analysis is required to determine whether the WSF file exhibits any malicious behavior.

OneNote Campaign

Following Microsoft’s decision to block macros, threat actors behind Qakbot resorted to email thread hijacking using a malicious OneNote document for wide-scale distribution by embedding scripts like JSE, CHM, HTA, MSF & BAT in the attachment.

The attacker entices the victim to click on a button labeled as “Decrypt and View Message” or “Double Click to View File” within an attachment. However, the concealed script executes and retrieves a malicious DLL file from a hardcoded URL. For more information refer to our blog on OneNote campaign.


DocuSign Protected E-Mail - OneNote
Search
Sign in
File
Home
Insert
Draw
History
Review
View
Help
My Notebook
ea3de7e7f4c2b293a98e568251dd7f36c4e199586df33f3140164d347fd8f122
+
DocuSign Protected E-Mail
DocuSign®
loginsoft

This message is protected with DocuSign e-signature

Double-click the Decrypt button to securely view message contents

Decrypt and View Message

Fig: Dragging button reveal embedded files

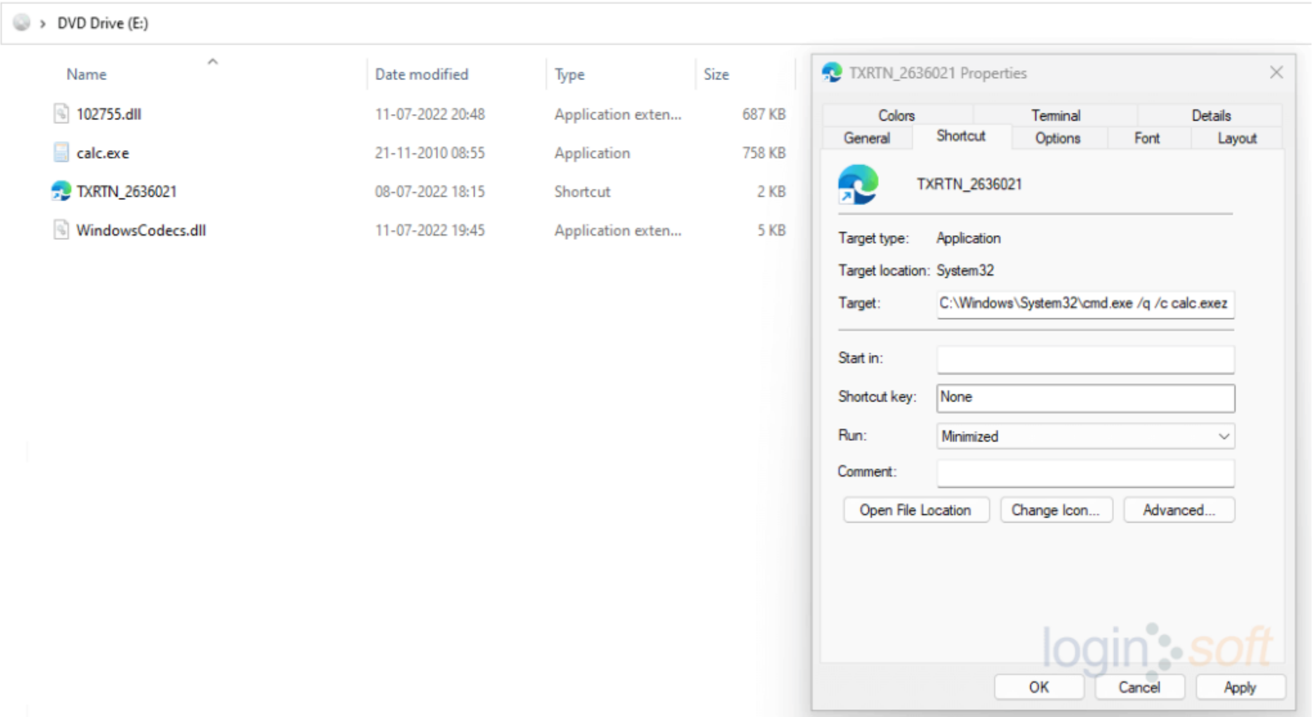
The following osquery detects the creation of suspicious child process on execution of the script in the OneNote attachment.

```
SELECT
    p1.name AS process_name,
    p1.pid AS process_pid,
    p1.cmdline AS process_cmdline,
    p2.name AS parent_process_name,
    p2.pid AS parent_process_pid,
    p2.cmdline AS parent_process_cmdline
FROM processes p1, processes p2
ON p1.parent = p2.pid
AND LOWER(parent_process_name) = 'onenote.exe'
AND
(
    process_cmdline LIKE '%\AppData\Local\Temp\OneNote\%'
    AND process_cmdline LIKE '%\Exported\%'
    AND process_cmdline LIKE '%\NT\%'
)
AND
(
    process_name IN
    (
        'rundll32.exe', 'regsvr32.exe', 'bitsadmin.exe', 'certutil.exe',
'installutil.exe',
        'schtasks.exe', 'wmic.exe', 'WmiPrvSE.exe', 'cscript.exe', 'wscript.exe',
        'cmstp.exe', 'Microsoft.Workflow.Compiler.exe', 'regasm.exe', 'regsvcs.exe',
'mshta.exe',
        'msxsl.exe', 'ieexec.exe', 'cmd.exe', 'powershell.exe', 'hh.exe',
'javaw.exe', 'pcalua.exe',
        'curl.exe', 'scriptrunner.exe', 'certoc.exe', 'workfolders.exe',
'odbcconf.exe', 'msiexec.exe', 'msdt.exe'
    )
    OR
    (
        process_cmdline LIKE '%.bat%'
        OR process_cmdline LIKE '%.dat%'
        OR process_cmdline LIKE '%.exe%'
        OR process_cmdline LIKE '%.hta%'
        OR process_cmdline LIKE '%.vba%'
        OR process_cmdline LIKE '%.vbe%'
        OR process_cmdline LIKE '%.vbs%'
        OR process_cmdline LIKE '%.wsh%'
        OR process_cmdline LIKE '%.wsf%'
        OR process_cmdline LIKE '%.js%'
        OR process_cmdline LIKE '%.scr%'
        OR process_cmdline LIKE '%.pif%'
        OR process_cmdline LIKE '%.cmd%'
        OR process_cmdline LIKE '%.chm%'
        OR process_cmdline LIKE '%.ps%'
        OR process_cmdline LIKE '%.lnk%'
        OR process_cmdline LIKE '%.ps1%'
        OR process_cmdline LIKE '%.ps2%'
        OR process_cmdline LIKE '%.jse%'
    )
);
```

HTML Smuggling Campaign

Based on our observation, Qakbot malware is also being distributed via emails with HTML attachments containing malicious JavaScript code in HTML5 attributes. Upon opening the HTML file, the JavaScript code gets executed within the browser dropping an ISO image file.

After user clicks on the shortcut file from the mounted drive, the LNK file initiates the execution of hidden Windows 7 calculator and side-loading of Qakbot DLL.



Name	Date modified	Type	Size
102755.dll	11-07-2022 20:48	Application exten...	687 KB
calc.exe	21-11-2010 08:55	Application	758 KB
TXRTN_2636021	08-07-2022 18:15	Shortcut	2 KB
WindowsCodecs.dll	11-07-2022 19:45	Application exten...	5 KB

TXRTN_2636021

Target type: Application
Target location: System32
Target: C:\Windows\System32\cmd.exe /q /c calc.exez
Start in:
Shortcut key: None
Run: Minimized
Comment:

Fig: Calc DLL Side-Loading

Using osquery, the calculator loading DLLs from unusual file paths can be detected.

```
SELECT
          datetime,
           source,
           provider_name,
           computer_name,
           eventid,
           json_extract(data,'$.EventData.Image') as process_name,
           json_extract(data,'$.EventData.ProcessId') as process_pid,
           json_extract(data,'$.EventData.ImageLoaded') as image_loaded
FROM windows_events
WHERE eventid = '7'
AND process_name LIKE '%calc.exe'
AND
(
      image_loaded NOT LIKE 'C:WindowsSystem32%'
      OR image_loaded NOT LIKE 'C:WindowsSysWOW64%'
);
```

Qakbot’s Behaviour in Later Stages

Once the Qakbot DLL was loaded into the targeted machine, the following behaviors were observed.

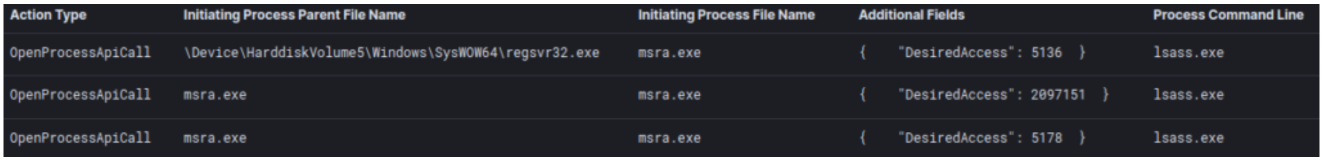
Qakbot establishes persistence by creating a scheduled task that registers the Qakbot DLL to execute with elevated privileges. This is achieved by creating a SYSTEM user account which is used to perform the task.

```
"schtasks.exe" /Create /RU "NT AUTHORITYSYSTEM" /tn {RandomTaskName} /tr
"regsvr32.exe -s "C:UsersREDACTED{QakbotDLL}"" /SC ONCE /Z /ST {Time} /ET
{Time}
```

The following query can be utilized to detect scheduled tasks that create a system user and registers a DLL.

```
SELECT
*
FROM scheduled_tasks
WHERE
(
action LIKE '%/create%'
AND action LIKE '%SYSTEM%'
AND action LIKE '%regsvr32%'
AND action LIKE '%-s%'
);
```

Qakbot then attempts to inject code into a preselected list of processes to evade detection and target LSASS through an injected process to gain credentials.



Action Type	Initiating Process Parent File Name	Initiating Process File Name	Additional Fields	Process Command Line
OpenProcessApiCall	\Device\HarddiskVolume5\Windows\SysWOW64\regsvr32.exe	msra.exe	{ "DesiredAccess": 5136 }	lsass.exe
OpenProcessApiCall	msra.exe	msra.exe	{ "DesiredAccess": 2097151 }	lsass.exe
OpenProcessApiCall	msra.exe	msra.exe	{ "DesiredAccess": 5178 }	lsass.exe

Fig: Qakbot Injected msra.exe accessing lsass.exe
Image source: DFIR

The Qakbot-injected processes accessing lsass.exe for credentials can be detected using the query below.

```
SELECT
  p1.name as process_name,
  p1.pid as process_pid,
  p1.cmdline as process_cmdline,
  p2.name as parent_process_name,
  p2.pid as parent_process_pid,
  p2.cmdline as parent_process_cmdline
FROM processes p1, processes p2
ON p2.pid = p1.parent
AND LOWER(parent_process_name) IN
('wermgr.exe','onedrivesetup.exe','msra.exe','dxdiag.exe','xwizard.exe','atbroker.exe
','mobsync.exe','certenrollctrl.exe','explorer.exe')
AND LOWER(process_name) = 'lsass.exe';
```

Qakbot conducts a system discovery process to gather information about the systeminfo, ipconfig, nslookup and arp on the targeted machine, allowing the adversary to carry out lateral movement activities.

Below query can be used to detect Qakbot injected process executing system discovery commands.

```
SELECT name,
 pid,
 path,
 cmdline,
 parent
FROM processes
WHERE LOWER(name) IN
('wermgr.exe','onedrivesetup.exe','msra.exe','dxdiag.exe','xwizard.exe','atbroker.exe
','mobsync.exe','certenrollctrl.exe','explorer.exe')
AND
(
    cmdline LIKE '%whoami%'
    OR cmdline LIKE '%arp%'
    OR cmdline LIKE '%ipconfig%'
    OR cmdline LIKE '%net view%'
    OR cmdline LIKE '%nslookup%'
    OR cmdline LIKE '%nltest%'
    OR cmdline LIKE '%net share%'
    OR cmdline LIKE '%netstat%'
    OR cmdline LIKE '%net localgroup%'
    OR cmdline LIKE '%qwinsta%'
);
```

Note: All the queries were tested on the Osquery version 5.6.0 & above.

Qakbot employs multiple threads to carry out its activities. One such thread involves gathering information about the compromised device and exfiltrating data to its Command and Control (C2) server.

These queries can be tested in a controlled, sandbox environment on below samples

Threat Synopsis

MITRE ATT&CK Techniques

Tactic	Technique ID	Technique Name
Initial Access	T1566.001	Phishing: Spearphishing Attachment
Execution	T1204.001 T1204.002	User Execution: Malicious Link User Execution: Malicious File
Defense Evasion	T1055.012 T1218.010 T1218.011	Process Injection: Process Hollowing System Binary Proxy Execution: Regsvr32 System Binary Proxy Execution: RunDll32

Discovery	T1033 T1047 T1049 T1082 T1518.001	System Owner/User Discovery Windows Management Instrumentation System Network Connections Discovery System Information Discovery Security Software Discovery
Persistence	T1053	Scheduled Tasks
Credential Access	T1555	Credentials from Password Stores
Command and Control	T1071 T1105	Application Layer Protocol Ingress Tool Transfer
Exfiltration	T1041	Exfiltration Over C2 Channel

Conclusion

Qakbot’s adaptability and constant evolution make it a significant threat to financial institutions and businesses alike. Additionally, the malware’s multifaceted nature allows it to serve as an initial infection vector for ransomware and further increasing its potential impact on organizations.

References

- https://thedfirreport.com/2022/02/07/qbot-likes-to-move-it-move-it/
- https://www.attackiq.com/2023/01/25/emulating-qakbot/
- https://www.trellix.com/en-us/about/newsroom/stories/research/demystifying-qbot-malware.html
- https://www.fortinet.com/blog/threat-research/new-variant-of-qakbot-spread-by-phishing-emails

Author: Bhargav K
Senior Threat Researcher, Loginsoft