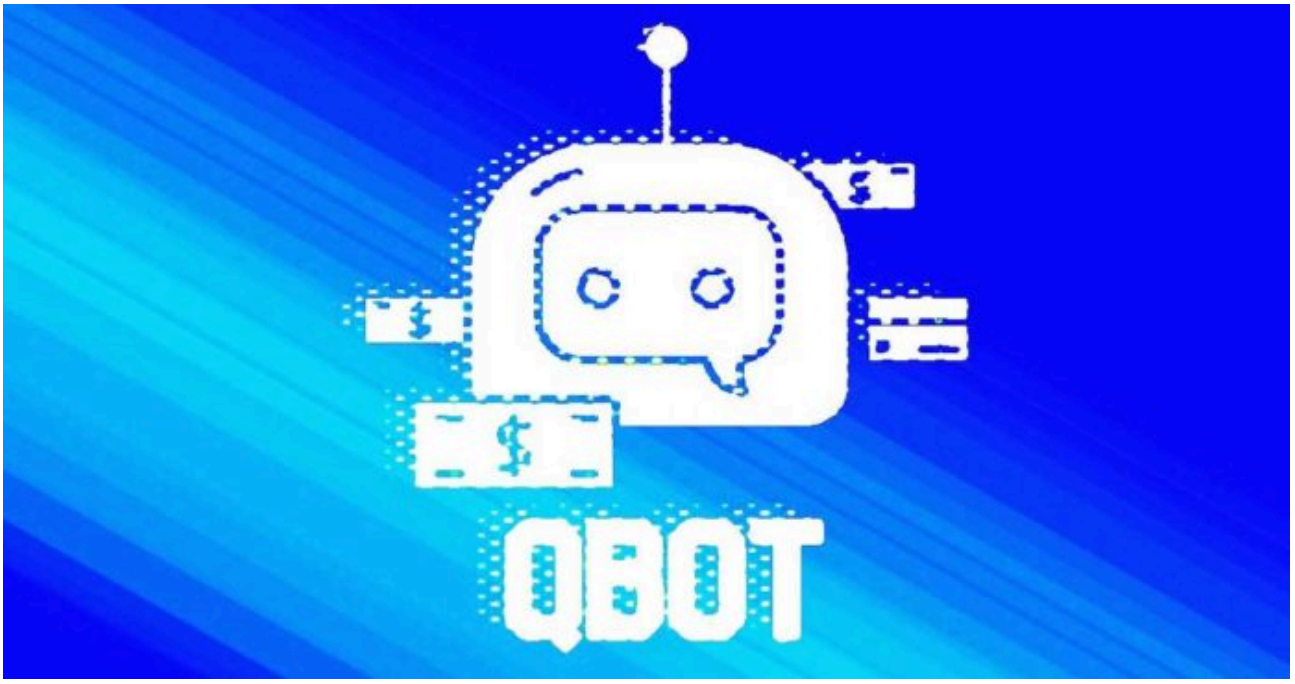
QBot Spreads via LNK Files – Detection & Response - Security Investigation

By Priyadharshini Balaji

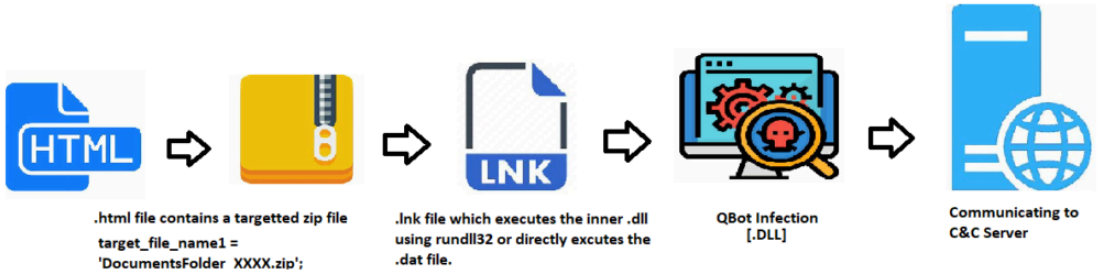
Published: 2022-07-05 · Archived: 2026-04-05 21:24:34 UTC



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:



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**

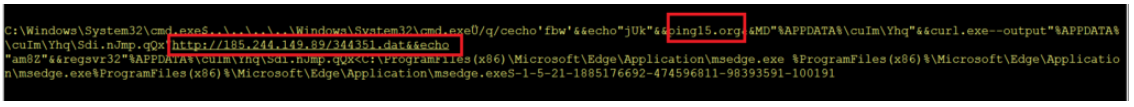
In the .lnk files, we can be able to see the target path if it’s in a shorter range. However, command-line arguments can be up to 4096, so malicious actors can that this advantage and pass on long arguments as they will not be visible in the properties section.

Sample Information:

Basic Properties

MD5	f5253fb1b38f3fff9b8661cc0c68b551
SHA-1	6792335374d8e1b2f3e722ab8237820d936c7ad9
SHA-256	7ba100e52afdf4408e2d12411df8a927b07a491e3ec7f58e08feb3524c98d5ea
Vhash	cf088e5075b0eeaecf21d8454aee5892
SSDEEP	24:8WOaCWJAneotSqcEaAAdcA+//BFRvXX6MLddNXuHY8482bK0/Am:8WOaSvaXeFRvXX9LdLXuHEbbKWA
TLSH	T10441FE103ED90726E7E25E72C67677199C37F546EA358F1D8581898C6C62B00AC29F3F
File type	Windows shortcut
Magic	MS Windows shortcut
TrID	Windows Shortcut (100%)
File size	2.18 KB (2233 bytes)

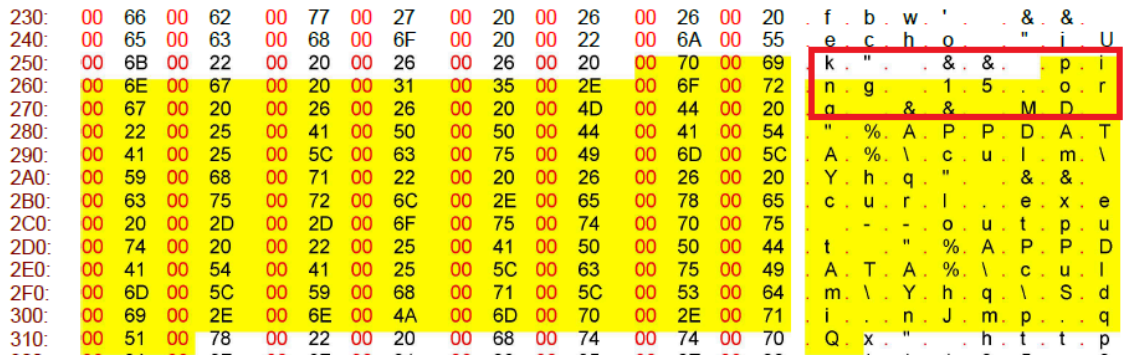
The main content of this QBot LNK:



How does QBot LNK work?

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

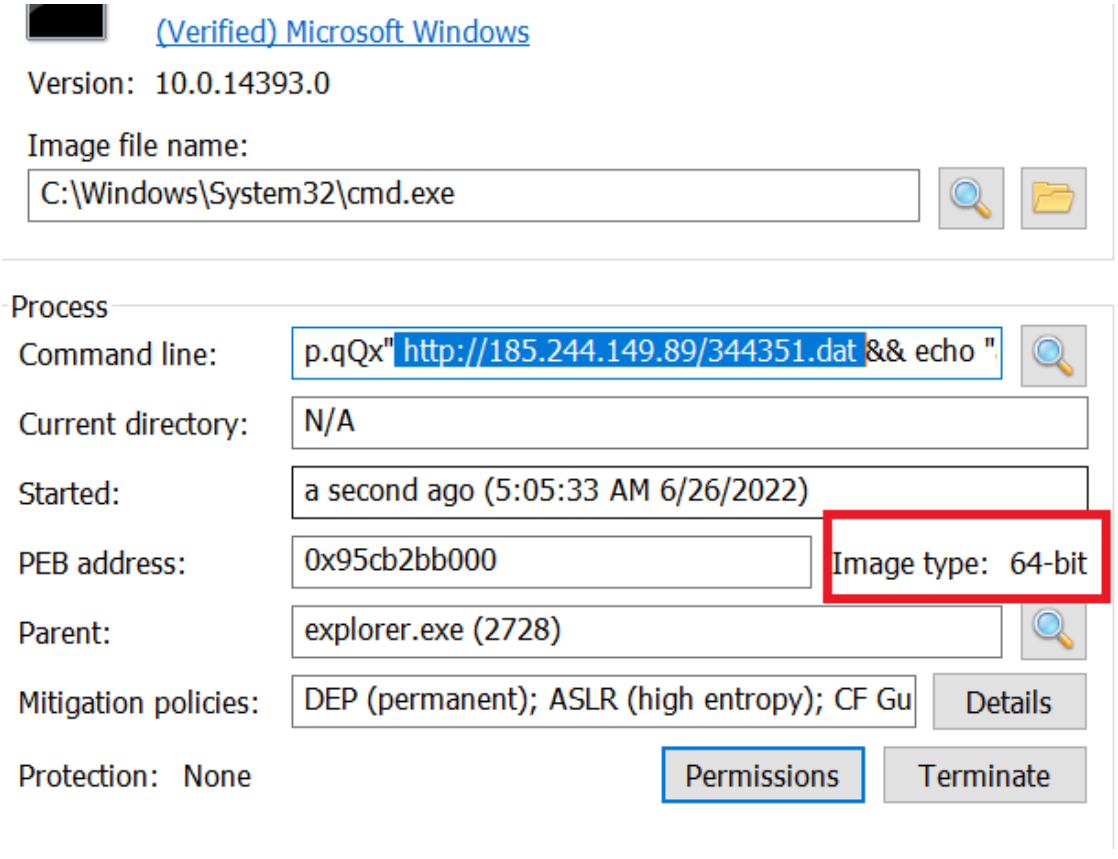
Ping [Packet Internet or Inter-Network Groper] utility uses the echo request, and echo reply messages within the Internet Control Message Protocol (ICMP), an integral part of any IP network. Here, the ping sends ICMP packets to the destination. Then it waits for the echo reply.

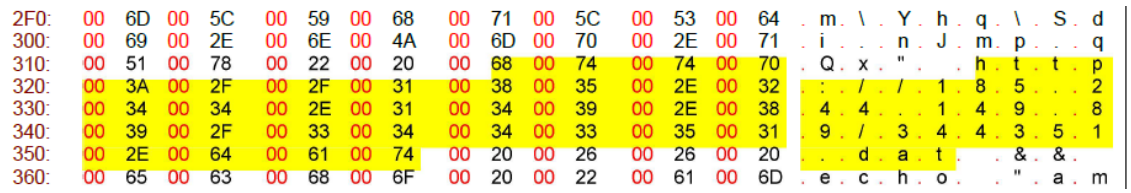


Also Read: [Latest Cyber Security News – Hacker News !]

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:





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
```

Splunk:

```
((ParentImage="*\\cmd.exe") AND CommandLine="*http://*" AND CommandLine="*ping15.org*" AND CommandLine="*..\\*"
```

Elastic Query:

```
(process.parent.executable:*\\cmd.exe AND process.command_line:*http\:\/\/* AND process.command_line:*ping15.or
```

Arcsight:

```
(sourceProcessName CONTAINS "*\\cmd.exe" AND ((deviceCustomString1 CONTAINS "*http://*" OR destinationServiceNa
```

CarbonBlack:

```
(parent_name:*\\cmd.exe AND process_cmdline:*http\:\/\/* AND process_cmdline:*ping15.org* AND process_cmdline:*
```

Crowdstike:

```
((ParentBaseFileName="*\\cmd.exe") AND (CommandLine="*http://*" OR CommandHistory="*http://*") AND (CommandLine
```

FireEye:

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

GrayLog:

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

Google Chronicle:

```
principal.process.file.full_path = /.*\\cmd\.exe$/ and target.process.command_line = /.*http:\/\/.*/ and target
```

Logpoint:

```
(ParentImage IN "*\\cmd.exe" CommandLine="*http://*" CommandLine="*ping15.org*" CommandLine="*..\\*" CommandLi
```

Microsoft Defender:

```
DeviceProcessEvents | where ((InitiatingProcessFolderPath endswith @"\cmd.exe") and ProcessCommandLine contains
```

Microsoft Sentinel:

```
SecurityEvent |  where EventID == 4688 | where ((ParentProcessName endswith @'\cmd.exe') and CommandLine conta
```

RSA Netwitness:

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

SumoLogic:

```
(_sourceCategory=*windows* AND (ParentImage = "*\cmd.exe") AND CommandLine="*http://*" AND CommandLine="*ping1
```

Aws Opensearch:

```
(process.parent.executable:*\\cmd.exe AND process.command_line:*http\:\/\/* AND process.command_line:*ping15.o
```

Source: https://www.socinvestigation.com/qbot-spreads-via-lnk-files-detection-response/