

Recent Qakbot (Qbot) activity - SANS Internet Storm Center

By SANS Internet Storm Center

Archived: 2026-04-05 17:35:16 UTC

Introduction

Today's diary is a review of a [Qakbot](#) (Qbot) infection I generated on Tuesday 2020-12-08.

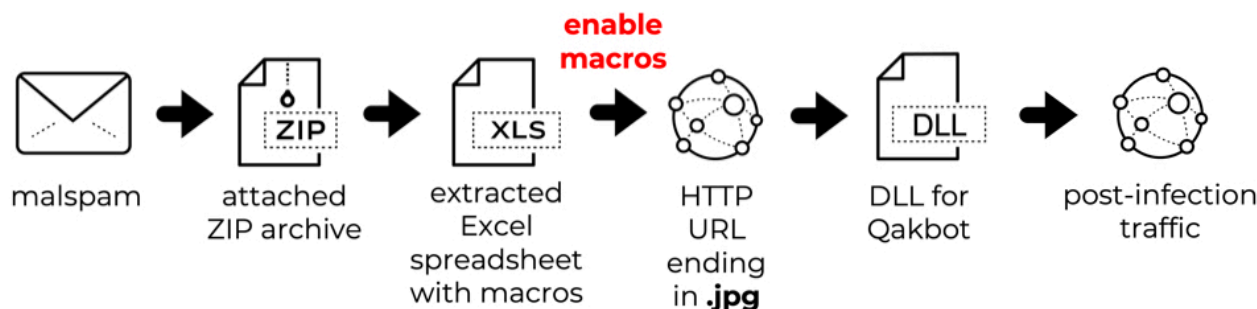
Qakbot generally includes follow-up malware like [Cobalt Strike](#) (such as [this example](#)), but my infection on Tuesday 2020-12-08 was a basic Qakbot infection that didn't run long enough for follow-up malware or other activity.

Of note, in late-November 2020, Qakbot underwent a version update. I've noticed this in my day-to-day research, but nothing comprehensive has been published yet. A few tweets about it:

- <https://twitter.com/lazyactivist192/status/1332363179729575938>
- https://twitter.com/alex_il/status/1333737189990158337
- <https://twitter.com/0verfl0w/status/1331598884431421441>

I'll review some of the changes I've noticed about the update in today's diary.

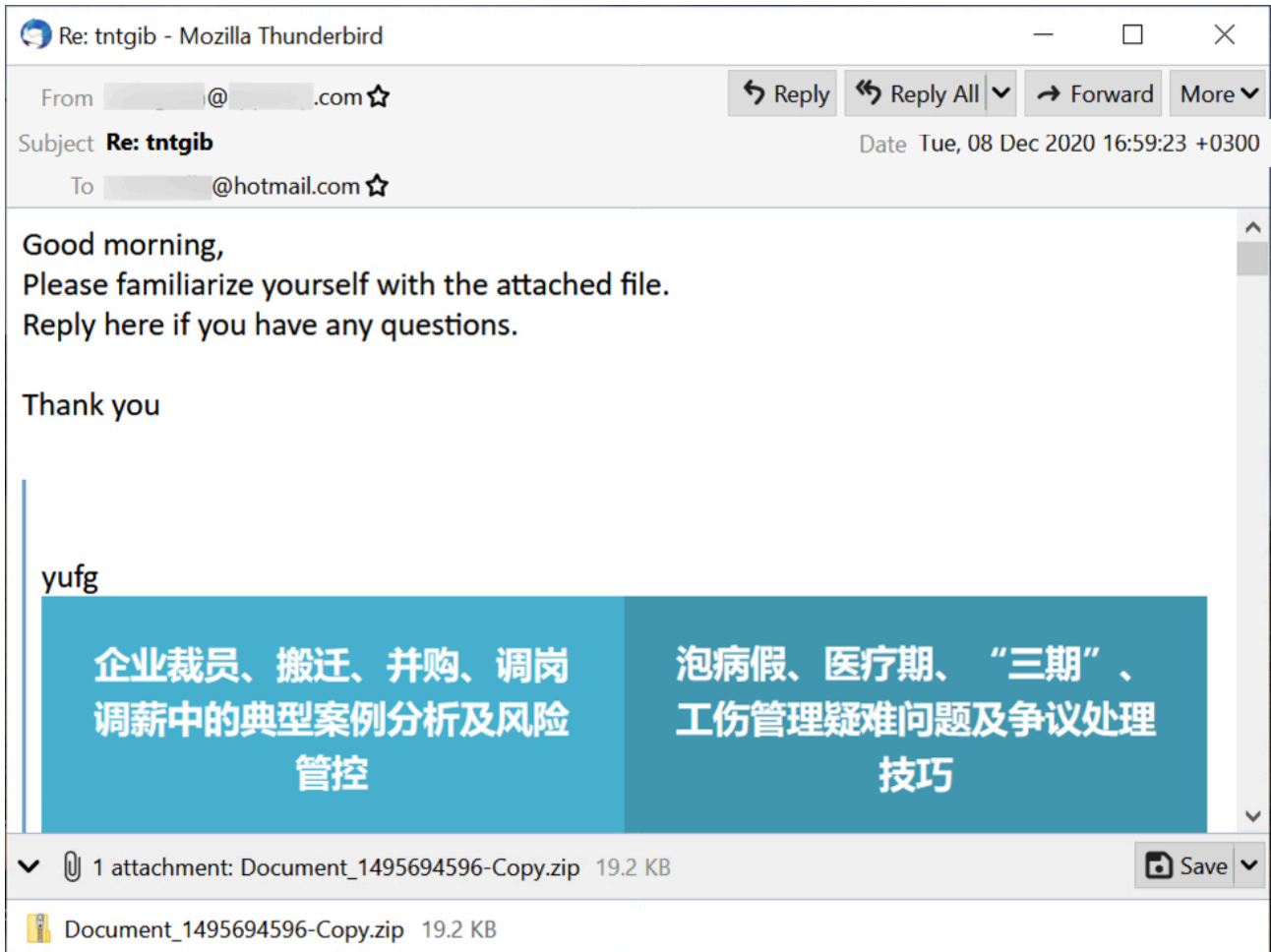
QAKBOT (QBOT) ACTIVITY - TUESDAY 2020-12-08



Shown above: Chain of events for the Qakbot infection we're reviewing today.

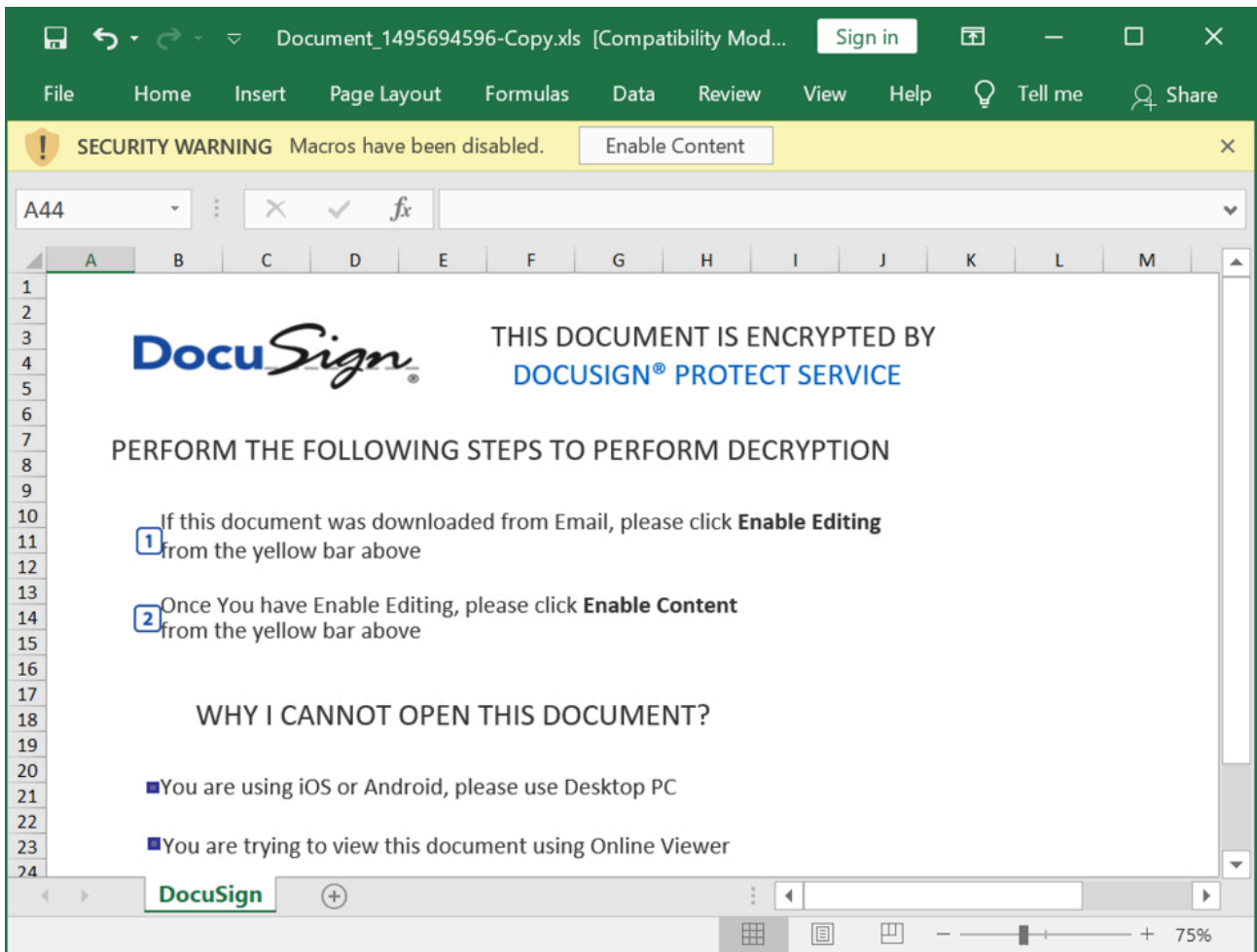
The malspam

Malspam examples I found from Tuesday 2020-12-08 were fake replies to legitimate email chains, although the example shown below might be a Qakbot-generated reply for an unsolicited spam message.



Shown above: An example of Qakbot malspam from Tuesday 2020-12-08.

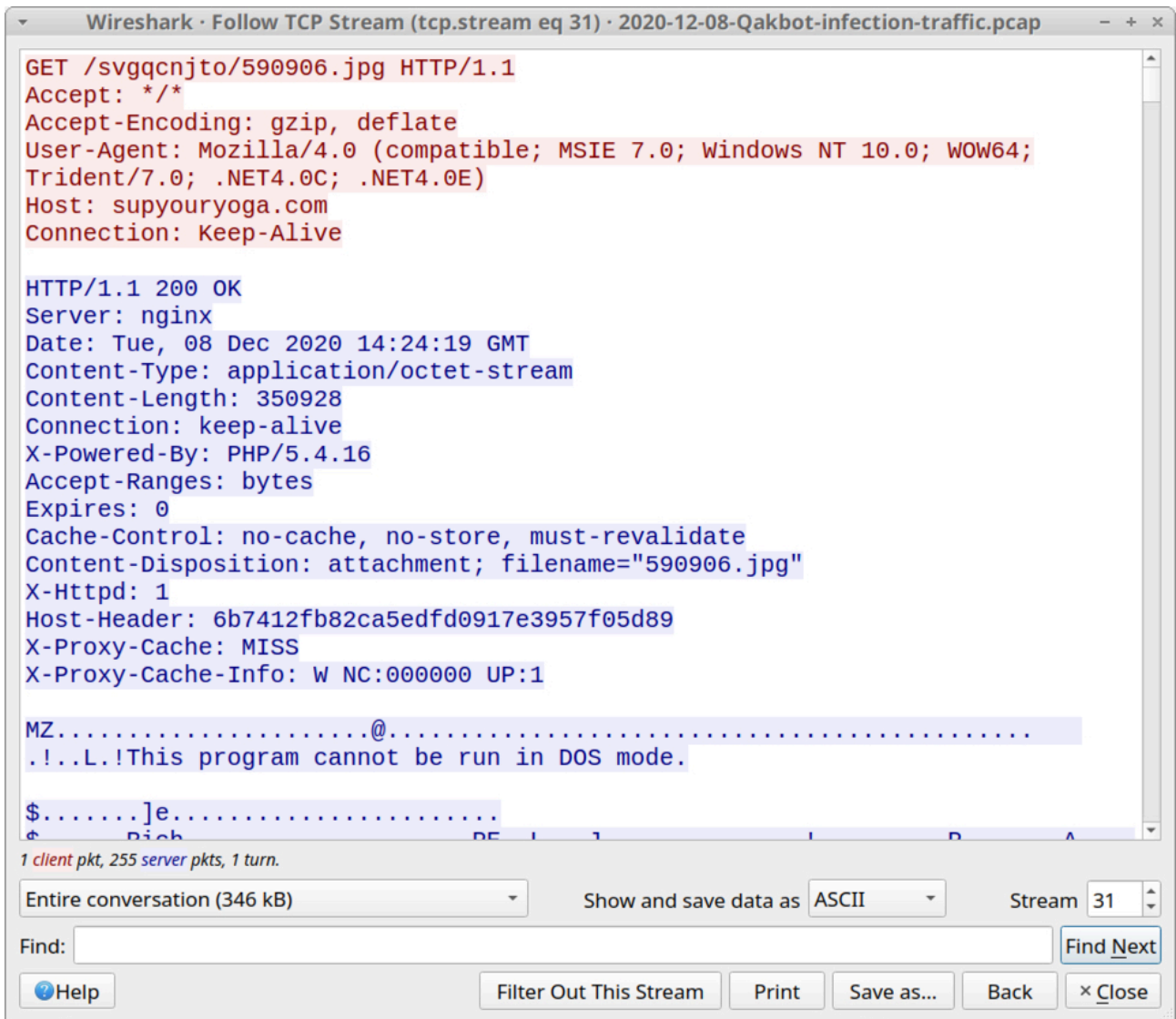
The attached ZIP archive has an Excel spreadsheet with macros designed to infect a vulnerable Windows host with Qakbot malware. Even with the version update, these spreadsheets distributing Qakbot have the same template we've seen for the past several months.



Shown above: Excel spreadsheet extracted from the ZIP attachment.

Infection activity

Typical for Qakbot, we see an HTTP GET request for a URL ending in **.jpg** that returned a Windows binary (in this case a DLL). This often is an HTTPS URL, where we would not see the Windows binary in a pcap. In recent months, I've seen as many HTTPS URLs for this as I have regular HTTP URLs.



Shown above: HTTP traffic that returned a Windows DLL file for Qakbot.

Filtering the traffic in Wireshark, we find typical Qakbot post-infection activity. But approximately 3 hours after the initial infection, I also saw web traffic to **wellsfargof.com**, which was unusual--especially since no browser had opened on the desktop of the infected Windows host.

(http.request or tls.handshake.type eq 1 or (tcp.port eq 65400 and tcp.flags eq 0x0002)) and !(ssdp) and !(frame.number < ...)

Time	Dst	port	Host	Info
2020-12-08 14:24:20	35.208.146.4	80	supyouryoga.com	GET /svgqcnjto/590906.jpg
2020-12-08 14:30:44	62.38.114.12	2222		Client Hello
2020-12-08 14:30:55	62.38.114.12	2222		Client Hello
2020-12-08 14:31:00	62.38.114.12	2222		Client Hello
2020-12-08 14:38:17	62.38.114.12	2222		Client Hello
2020-12-08 14:38:22	62.38.114.12	2222		Client Hello
2020-12-08 14:38:27	23.2.168.18	443	www.openssl.org	Client Hello
2020-12-08 14:38:31	54.36.108.120	65400		55100 → 65400 [SYN] Seq=
2020-12-08 14:39:21	62.38.114.12	2222		Client Hello
2020-12-08 16:26:10	62.38.114.12	2222		Client Hello
2020-12-08 16:31:27	62.38.114.12	2222		Client Hello
2020-12-08 16:37:15	197.45.110.165	995		Client Hello
2020-12-08 16:41:57	197.45.110.165	995		Client Hello
2020-12-08 16:47:14	197.45.110.165	995		Client Hello
2020-12-08 16:52:32	197.45.110.165	995		Client Hello
2020-12-08 16:57:49	197.45.110.165	995		Client Hello
2020-12-08 17:03:06	197.45.110.165	995		Client Hello
2020-12-08 17:08:23	197.45.110.165	995		Client Hello
2020-12-08 17:13:40	197.45.110.165	995		Client Hello
2020-12-08 17:18:53	197.45.110.165	995		Client Hello
2020-12-08 17:24:10	197.45.110.165	995		Client Hello
2020-12-08 17:25:40	159.45.66.143	80	wellsfargo.com	GET / HTTP/1.1

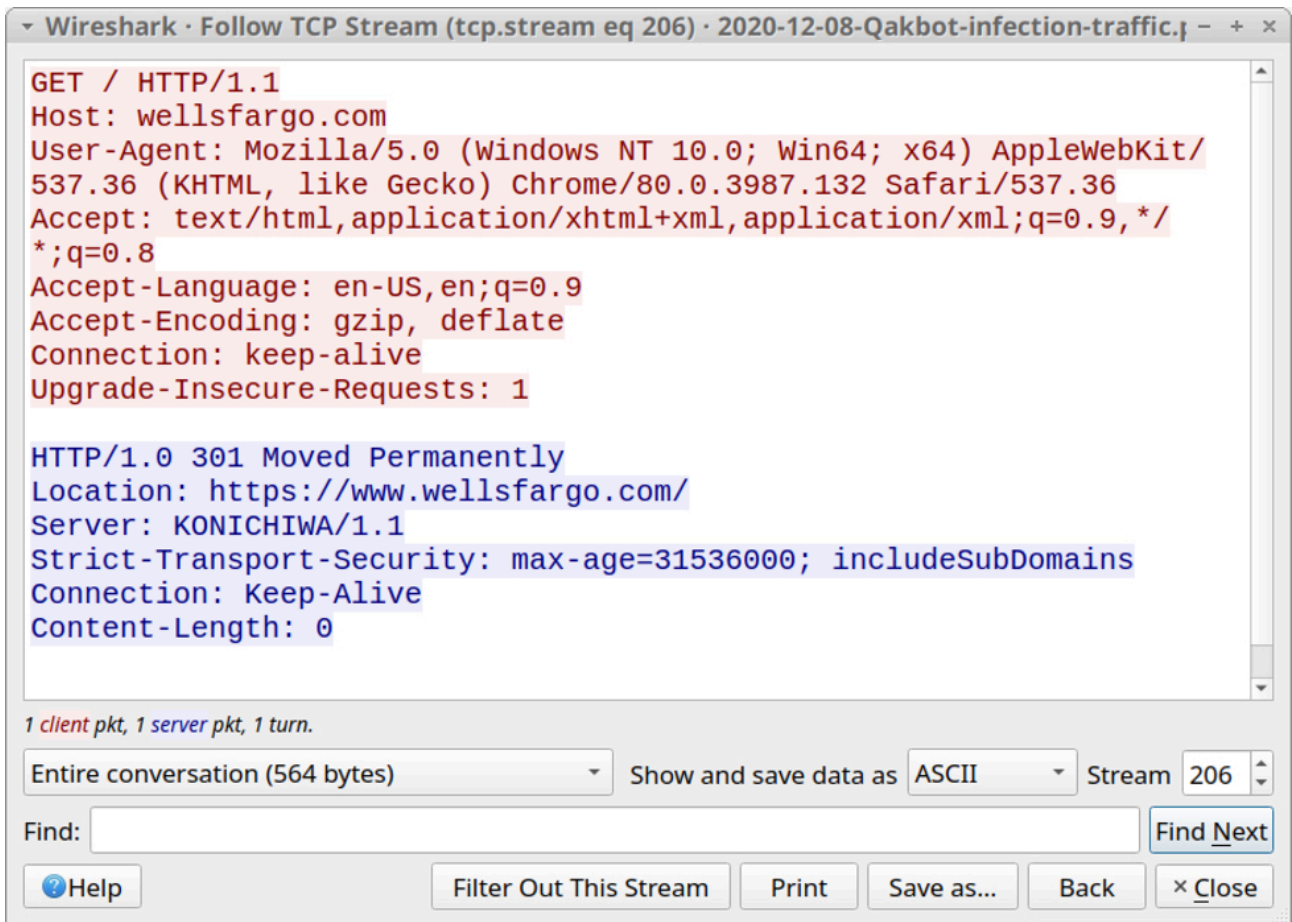
Shown above: Traffic from the infection filtered in Wireshark.

The user-agent string in HTTP traffic to **wellsfargo[.]com** indicated it may have been caused by Google Chrome. Keep in mind the user-agent string is often spoofed during malware infections. I also saw web traffic associated with the Firefox web browser. This traffic is likely related to one of the Qakbot modules; however, I could not find any modules saved to disk on my infected host.

(http.request or tls.handshake.type eq 1) and !(ssdp)

Time	Dst	port	Host	Info
2020-12-08 17:18:53	197.45.110.165	995		Client Hello
2020-12-08 17:24:10	197.45.110.165	995		Client Hello
2020-12-08 17:25:10	34.107.221.82	80	detectportal.firefox.com	GET /success.txt
2020-12-08 17:25:27	52.36.207.147	443	shavar.services.mozilla.com	Client Hello
2020-12-08 17:25:28	52.36.207.147	443	shavar.services.mozilla.com	Client Hello
2020-12-08 17:25:33	143.204.166.82	443	tracking-protection.cdn.mozilla...	Client Hello
2020-12-08 17:25:33	143.204.166.82	443	tracking-protection.cdn.mozilla...	Client Hello
2020-12-08 17:25:40	159.45.66.143	80	wellsfargo.com	GET / HTTP/1.1
2020-12-08 17:25:42	159.45.2.145	443	www.wellsfargo.com	Client Hello
2020-12-08 17:25:42	159.45.2.145	443	www.wellsfargo.com	Client Hello
2020-12-08 17:25:45	72.21.91.29	80	ocsp.digicert.com	Request
2020-12-08 17:25:46	72.21.91.29	80	ocsp.digicert.com	Request
2020-12-08 17:25:46	72.21.91.29	80	ocsp.digicert.com	Request
2020-12-08 17:25:46	72.21.91.29	80	ocsp.digicert.com	Request
2020-12-08 17:25:50	159.45.2.145	443	www.wellsfargo.com	Client Hello
2020-12-08 17:25:50	159.45.2.145	443	www.wellsfargo.com	Client Hello
2020-12-08 17:25:50	159.45.66.178	443	static.wellsfargo.com	Client Hello
2020-12-08 17:25:50	159.45.2.145	443	www.wellsfargo.com	Client Hello
2020-12-08 17:25:50	159.45.66.178	443	static.wellsfargo.com	Client Hello
2020-12-08 17:25:50	159.45.2.145	443	www.wellsfargo.com	Client Hello
2020-12-08 17:25:50	159.45.66.156	443	connect.secure.wellsfargo.com	Client Hello
2020-12-08 17:25:50	159.45.66.178	443	static.wellsfargo.com	Client Hello
2020-12-08 17:25:50	159.45.66.178	443	static.wellsfargo.com	Client Hello
2020-12-08 17:25:50	159.45.2.145	443	www.wellsfargo.com	Client Hello

Shown above: Filtering the traffic in Wireshark to show Firefox traffic, and other web traffic to wells Fargo[.]com from the infected host.



Shown above: Traffic to wells Fargo[.]com appears to be from Chrome, if the user-agent string is correct.

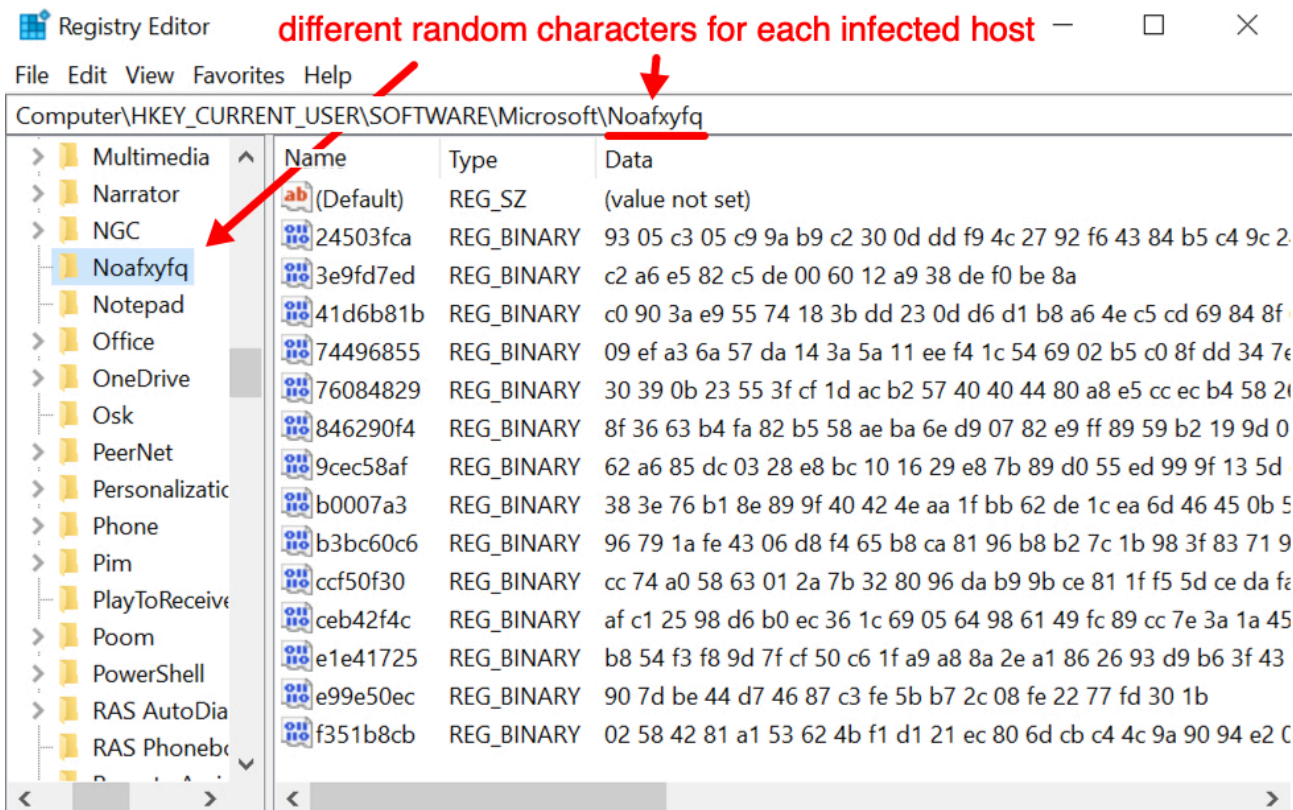
Qakbot malware version update

Sometime in late-November 2020, Qakbot malware was updated. I know of at least 3 related things that are noticeably different than before.

1) The Qakbot binary retrieved by Microsoft Office macros changed from an EXE to a DLL.

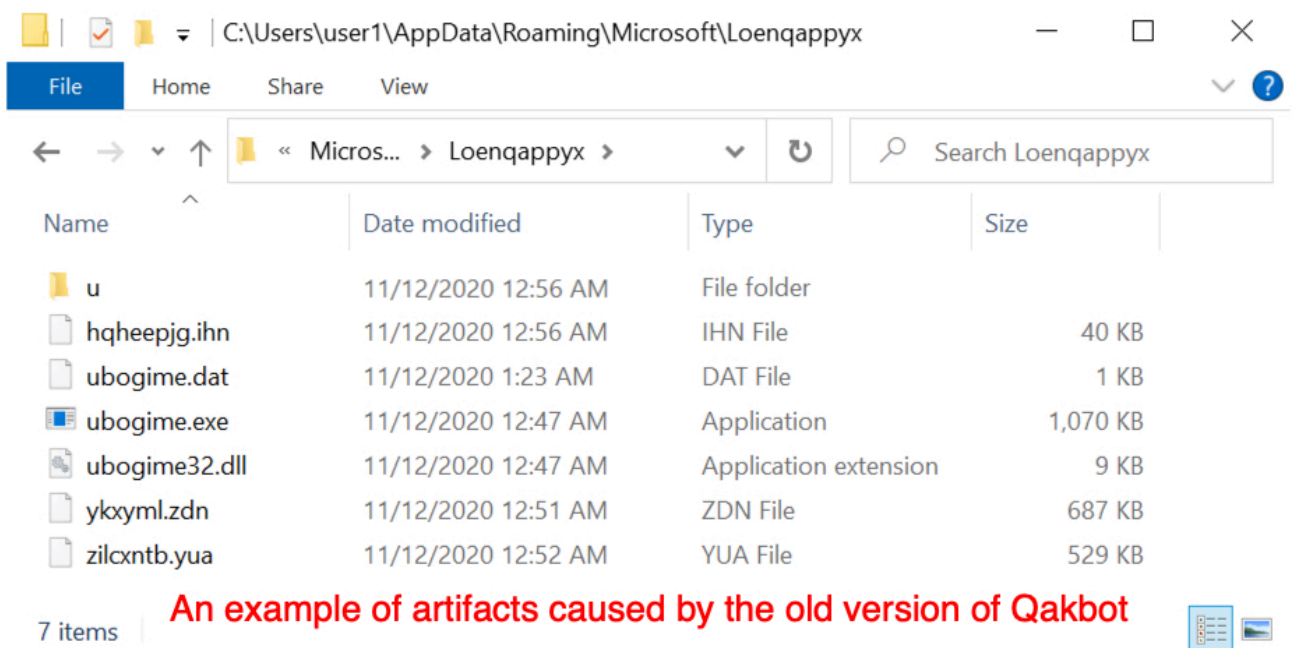
- Prior to the update, the initial Qakbot binary was an EXE made persistent through a Windows registry update at **HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run**.
- After the update, the initial Qakbot binary has been a DLL file, and there is no longer a Windows registry update at **HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run**.

2) Qakbot now creates other Windows registry updates. These updates are located at **HKCU\SOFTWARE\Microsoft** under a key that consists of a unique alphabetical string for each infected host. It consists of several entries containing encoded binary data as shown in the example below.



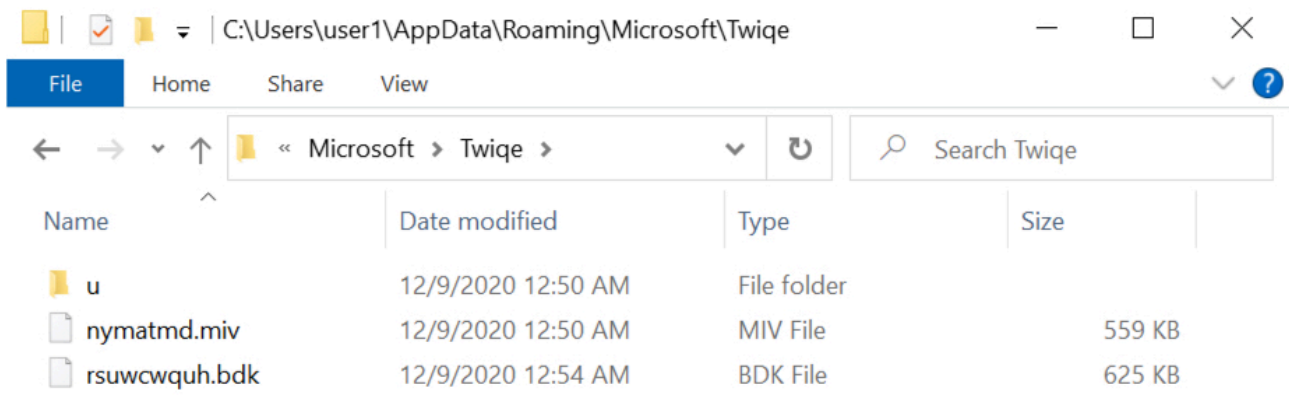
Shown above: An example of Windows registry update caused by the newest version of Qakbot.

3) The directory for Qakbot artifacts under **C:\Users\[username]\AppData\Roaming\Microsoft** now has fewer files. Before the version update, we saw a Windows EXE for Qakbot in this directory, and it was kept persistent in the Windows registry (see item 1 above). Now, the folder no longer has an EXE and some other files are missing. Compare the two images below.



An example of artifacts caused by the old version of Qakbot

Shown above: An example of artifact caused by the old version of Qakbot.



An example of artifacts caused by the new version of Qakbot

Shown above: Artifacts stores to the same type of directory after the late-November 2020 version update of Qakbot.

Qakbot's version update has resulted in other characteristics of the malware, and I'm certain someone will publish a more detailed write-up about it. These three changes are the one's I've noticed, but I focus mostly on dynamic analysis (not code analysis or reverse engineering).

Indicators of Compromise (IoC)

The following are IoCs from my Qakbot infection from Tuesday 2020-12-08.

ZIP archives from 4 malspam examples:

- [2ccc14f2bab2e9eb1d7228e225afda558fd4b52ed670303a912ace1984b35b06](#) Document_1204350147-Copy.zip
- [fa9935e6cda06866cb5aa062c16a73fdc85bd4146dca67202d22e225ddd3193b](#) Document_1356928040-Copy.zip
- [0a3a6163a5e8e372fa96fbef3feb793463f4e39bd2c4d6ea03afce045f90636](#) Document_1495694596-Copy.zip
- [66036cf566386c159e49191125497c77c13c75778492519000b9f61a4afdedad](#) Document_501487929-Copy.zip

Excel spreadsheets extracted from the above ZIP archives:

- [adad807fa22f398e0a40396ed65d0827f9f14baf7e1281b713dfb17e2683d743](#) Document_1204350147-Copy.xls
- [e14f6ab34e3506d6985816af85935932fb6faf8bad9d2c7dd96d6011d7c21a33](#) Document_1356928040-Copy.xls
- [4e2f37d4228e78faa1f34121ee934f58e1a9862ad6f183edf4c24e08cda20363](#) Document_1495694596-Copy.xls
- [94d759f43bcc647f7233e19ddc160a6b43458dcde6d2ea4274c8c06b2890def2](#) Document_501487929-Copy.xls

HTTP traffic after enabling that returned a Qakbot DLL file:

- 35.208.146[.]4 port 80 - **supyouryoga[.]com** - GET /svgqcnjto/590906.jpg

Qakbot post-infection traffic:

- 62.38.114[.]12 port 2222 - HTTPS traffic caused by Qakbot
- 197.45.110[.]165 port 995 - HTTPS traffic caused by Qakbot
- port 443 - **www.openssl[.]org** - connectivity check caused by Qakbot
- 54.36.108[.]120 port 65400 - TCP traffic caused by Qakbot

Unusual (to me) activity from Qakbot-infected host:

- port 80 - **wellsfargo[.]com** - GET /
- various IP addresses over TCP port 443 - Wells Fargo-related domains - traffic caused by viewing **wellsfargo[.]com**
- *Firefox-related HTTP and HTTPS web traffic*

Malware from an infected Windows host:

- SHA256 hash: [5060806228d3f2c1afd09566d0d2fa6b2e56f844cd044c4c4e6e7ade9fef3a22](#)
- File size: 350,928 bytes
- File retrieved from: hxxp://supyouryoga[.]com/svgqcnjto/590906.jpg
- File saved to victim as: C:\Users\[username]\AppData\Kipofe.mmaallaauu
- File description: DLL file for Qakbot retrieved by macro from Document_1495694596-Copy.xls
- Run method: Rundll32.exe [filename],DllRegisterServer

Final words

Qakbot been active for several years, and it continues to evolve. The latest version update has some significant changes, but infection traffic on vulnerable Windows hosts remains similar to what we've seen before with Qakbot.

A pcap of the infection traffic reviewed in this dairy and 4 examples of Qakbot malspam are available [here](#).

Brad Duncan

brad [at] malware-traffic-analysis.net

Source: <https://isc.sans.edu/diary/rss/26862>