SANS ISC: InfoSec Handlers Diary Blog - SANS Internet Storm Center SANS Site Network Current Site SANS Internet Storm Center Other SANS Sites Help Graduate Degree Programs Security Training Security Certification Security Awareness Training Penetration Testing Industrial Control Systems Cyber Defense Foundations DFIR Software Security Government OnSite Training InfoSec Handlers Diary Blog

Qakbot infection with Cobalt Strike and VNC activity

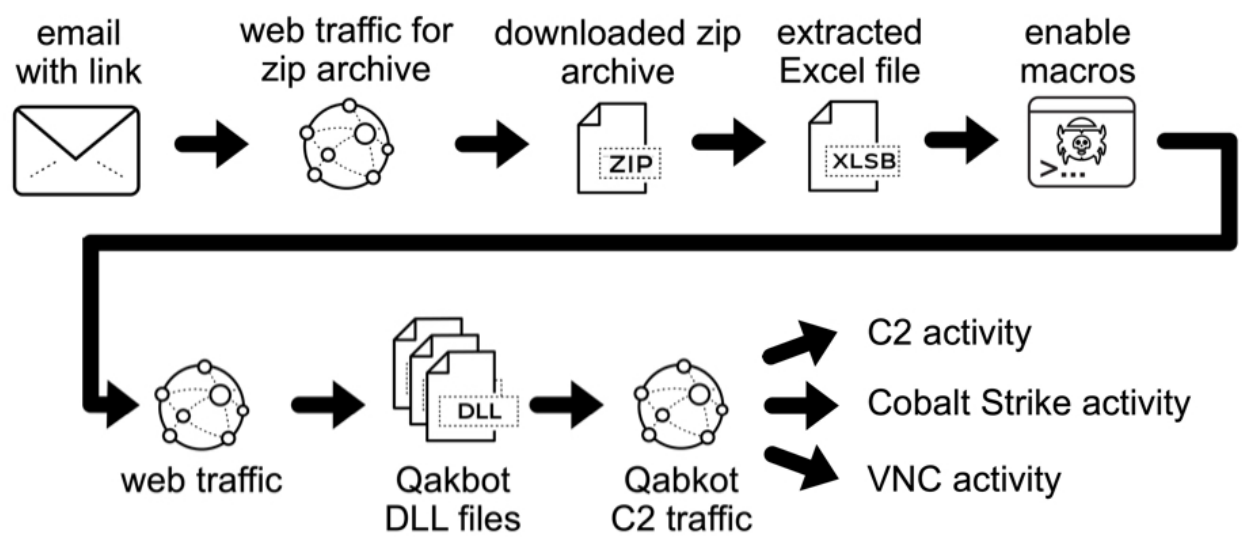
Published: 2022-03-16
Last Updated: 2022-03-16 05:27:22 UTC
by Brad Duncan (Version: 1)

Introduction

On Monday 2022-03-14, I infected a vulnerable Windows host with Qakbot (Qbot) malware. Approximately 17 hours later, the infected host generated traffic for Cobalt Strike and VNC (Virtual Network Computing) activity. Like Cobalt Strike, VNC provides remote access to an infected host.

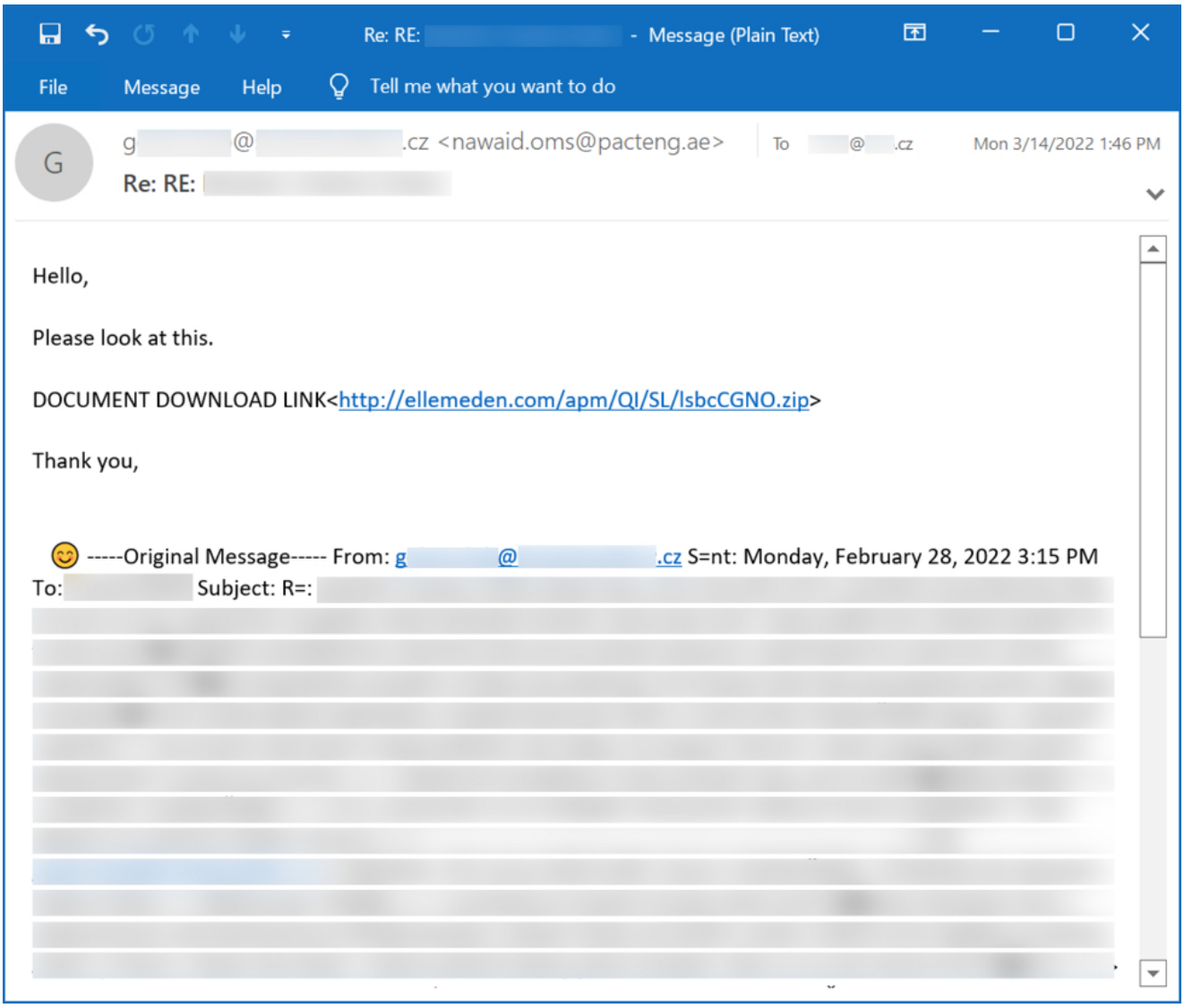
DLL files used for Qakbot infections have tags in the code that identify the malware sample's distribution channel. In this case, the distribution tag was obama166.

Today's diary provides a quick review of the infection activity.

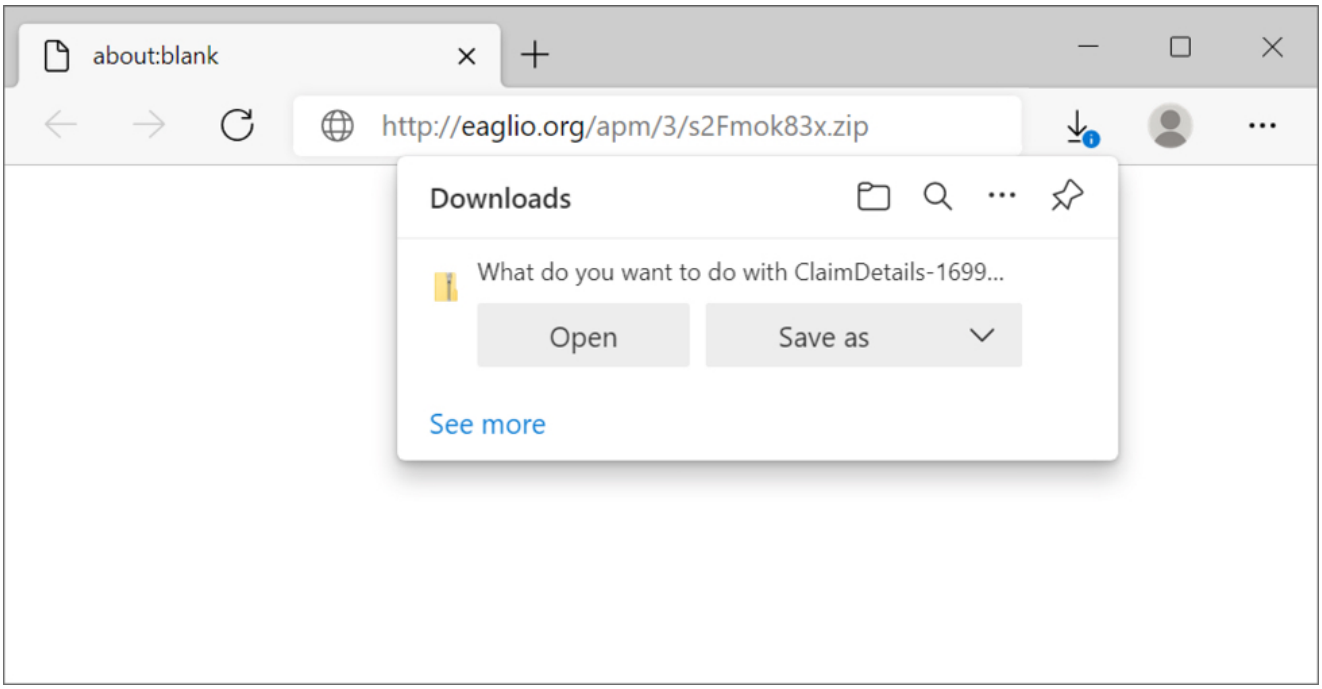


Shown above: Flow chart for Qakbot infection activity on Monday 2022-03-14.

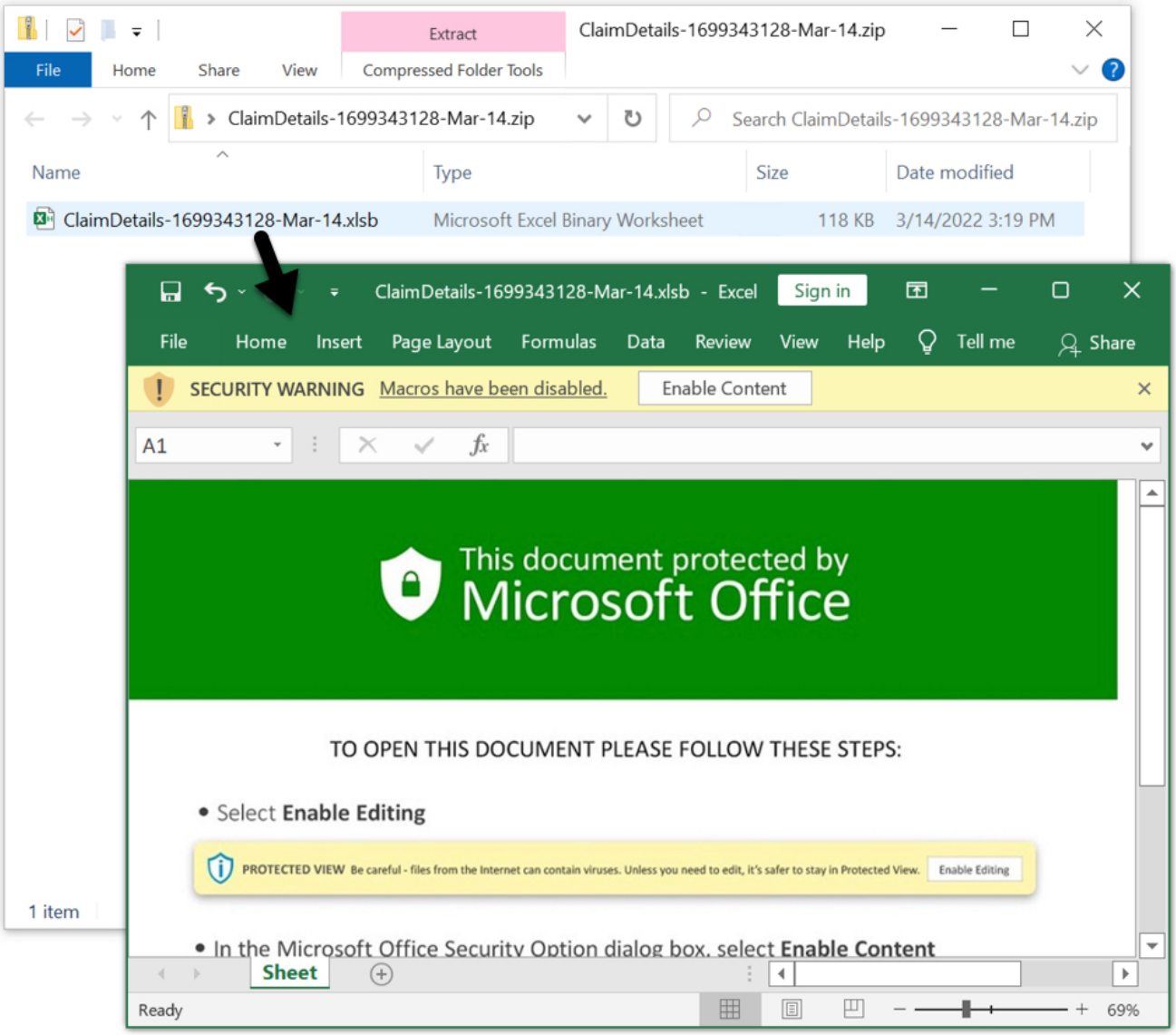
Images From the Infection



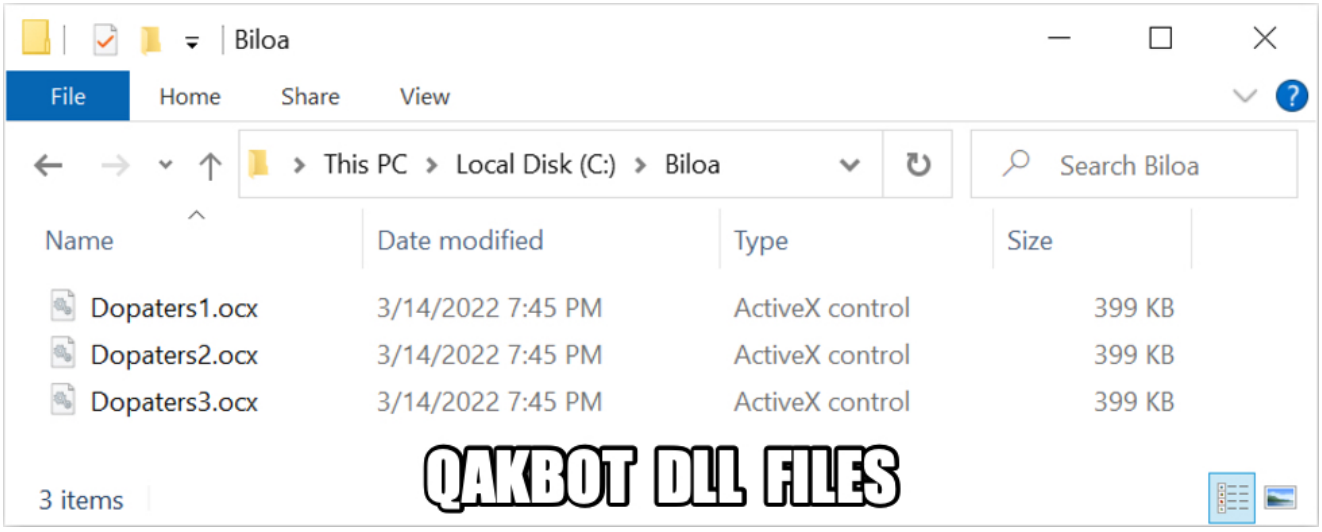
Shown above: Example of email for obama166 distribution Qakbot on Monday 2022-03-14.



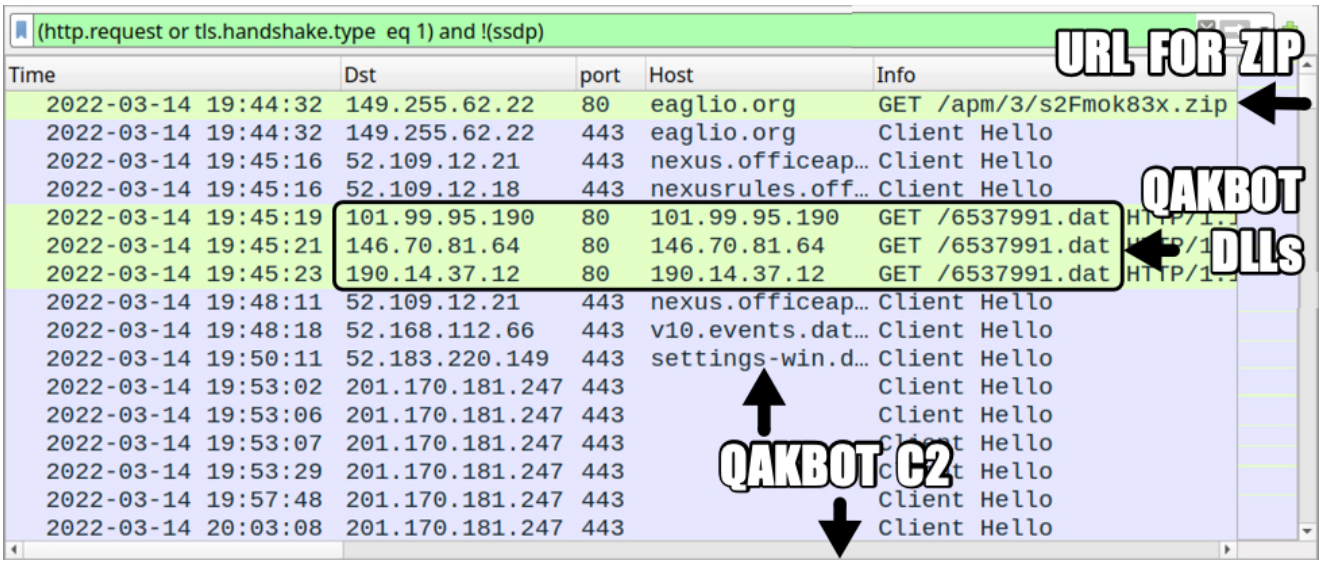
Shown above: Downloading a zip archive from link in an email.



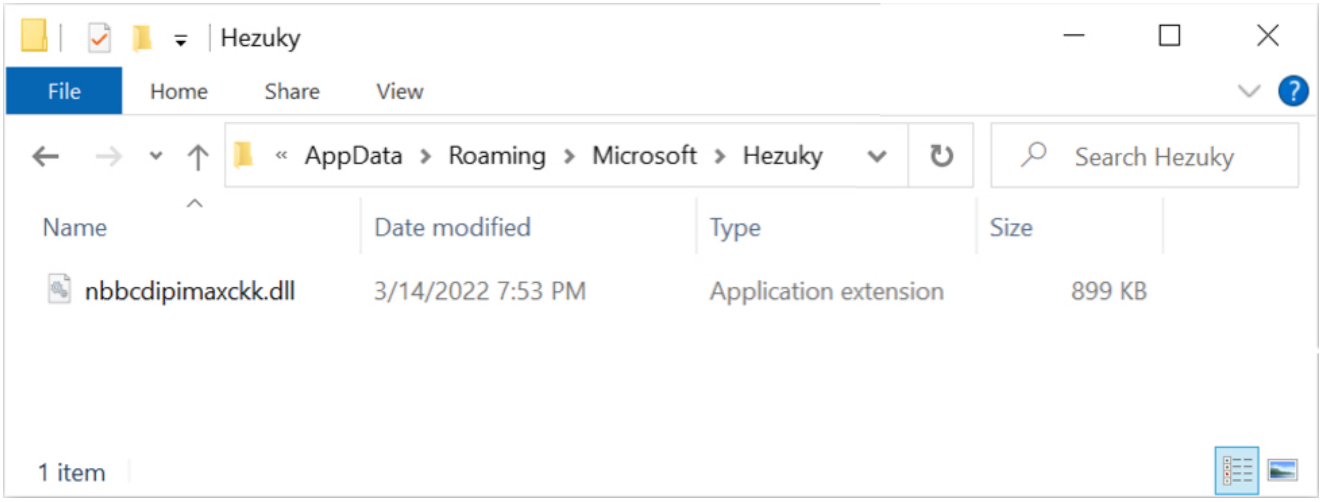
Shown above: Excel spreadsheet extracted from downloaded zip archive.



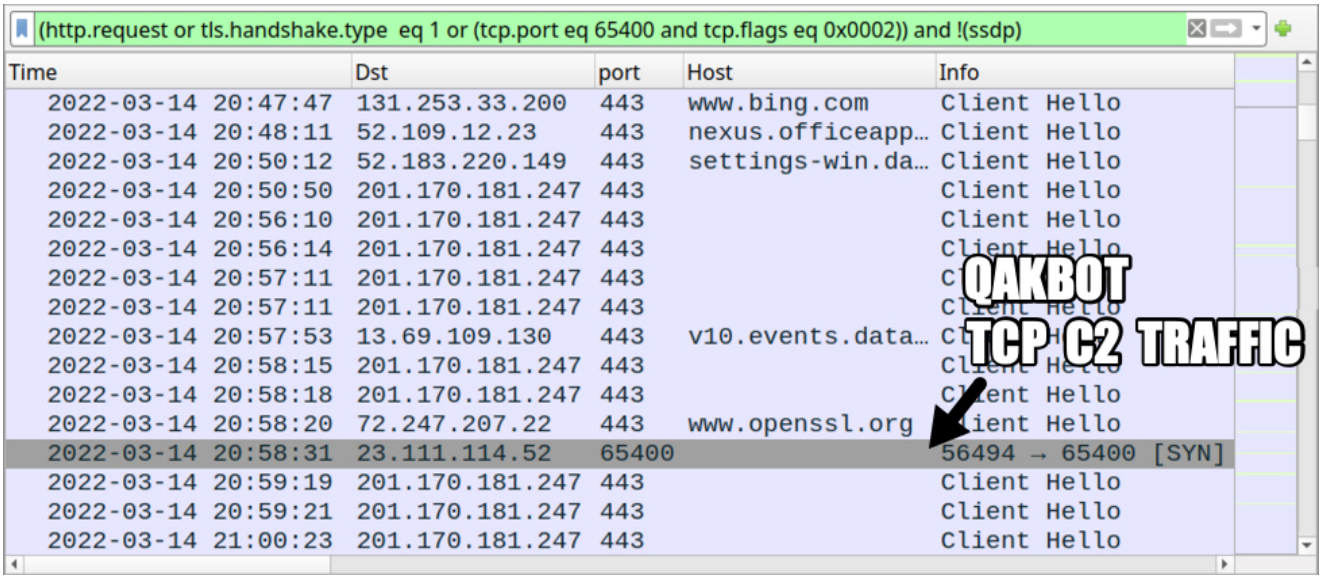
Shown above: DLL files downloaded for Qakbot infection.



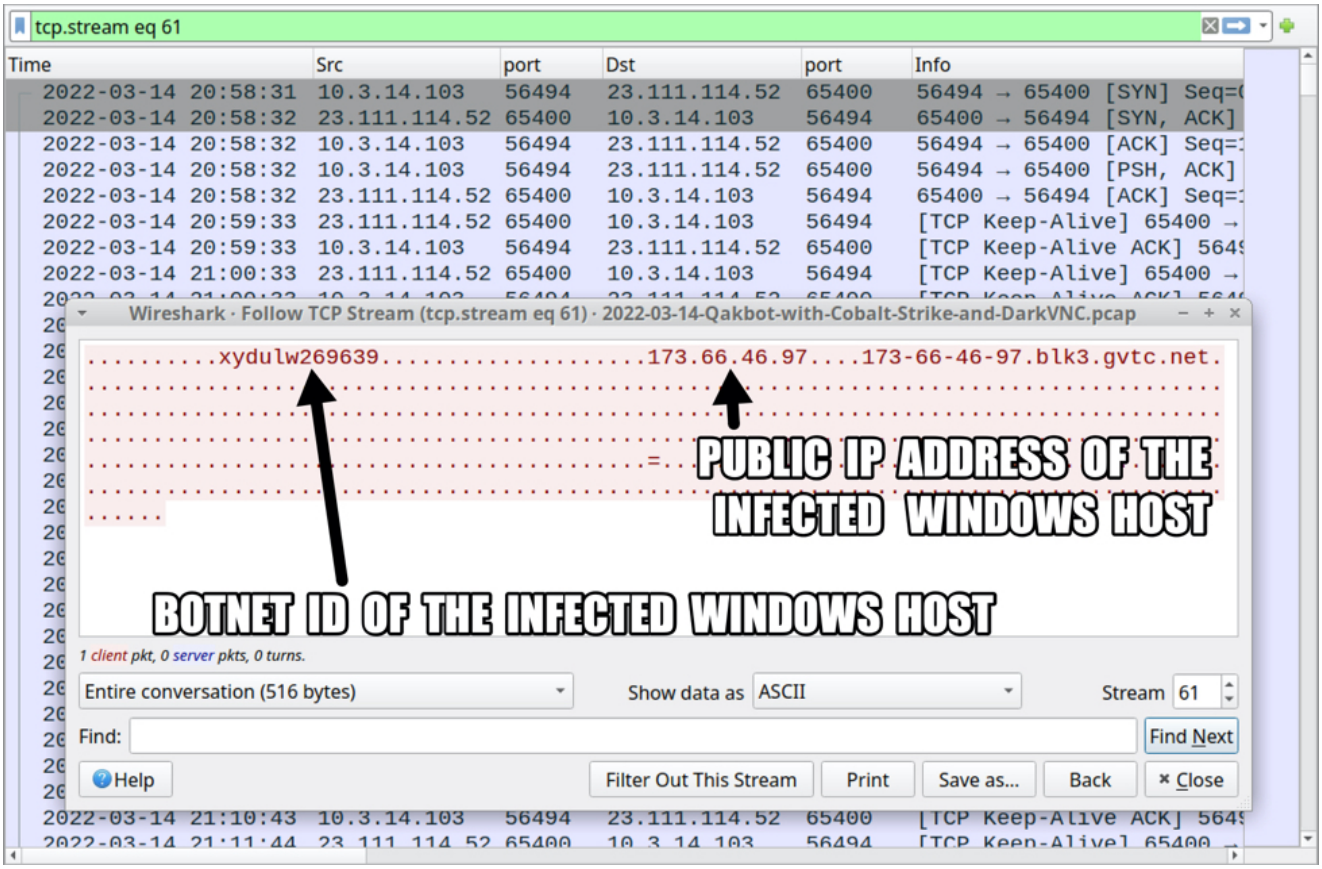
Shown above: Traffic from the infection filtered in Wireshark.



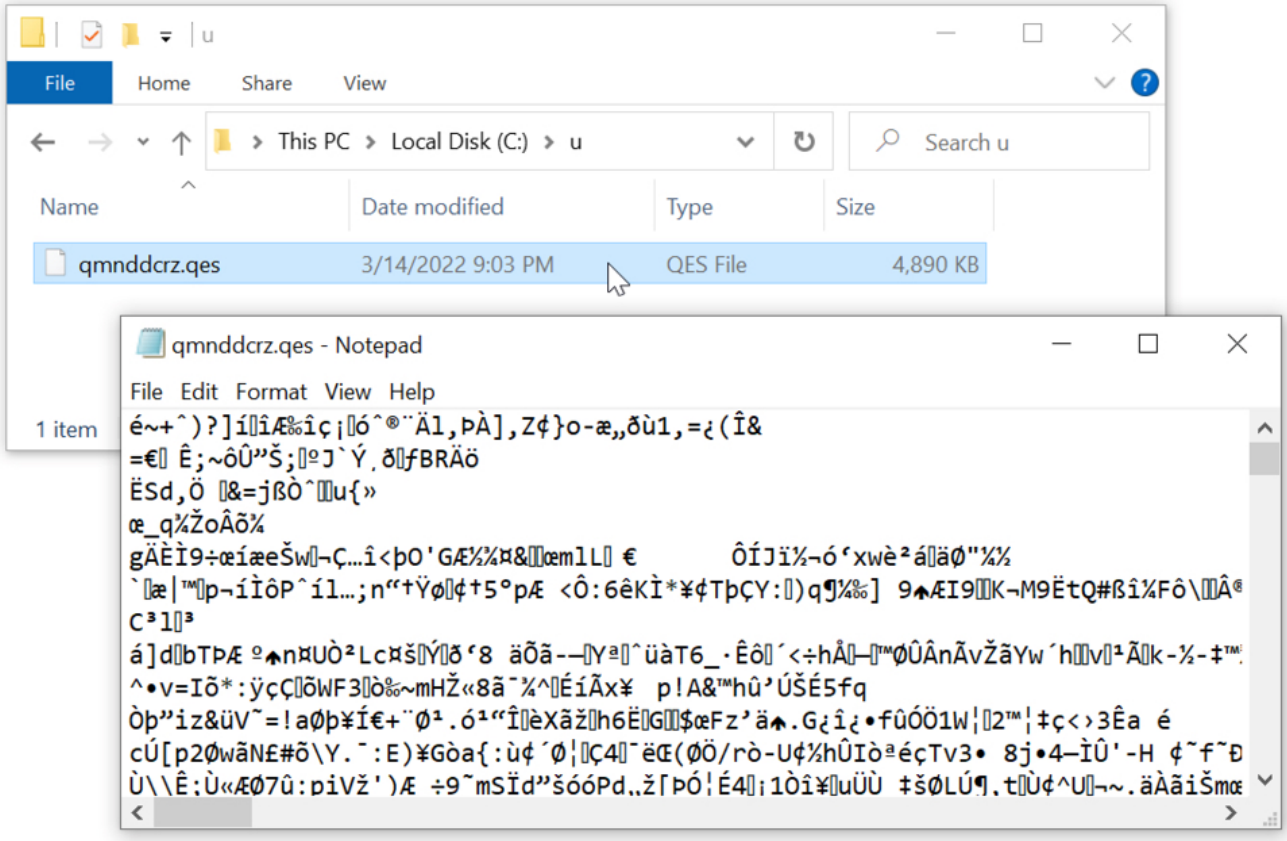
Shown above: New Qakbot DLL saved to the infected Windows host shortly after the initial infection.



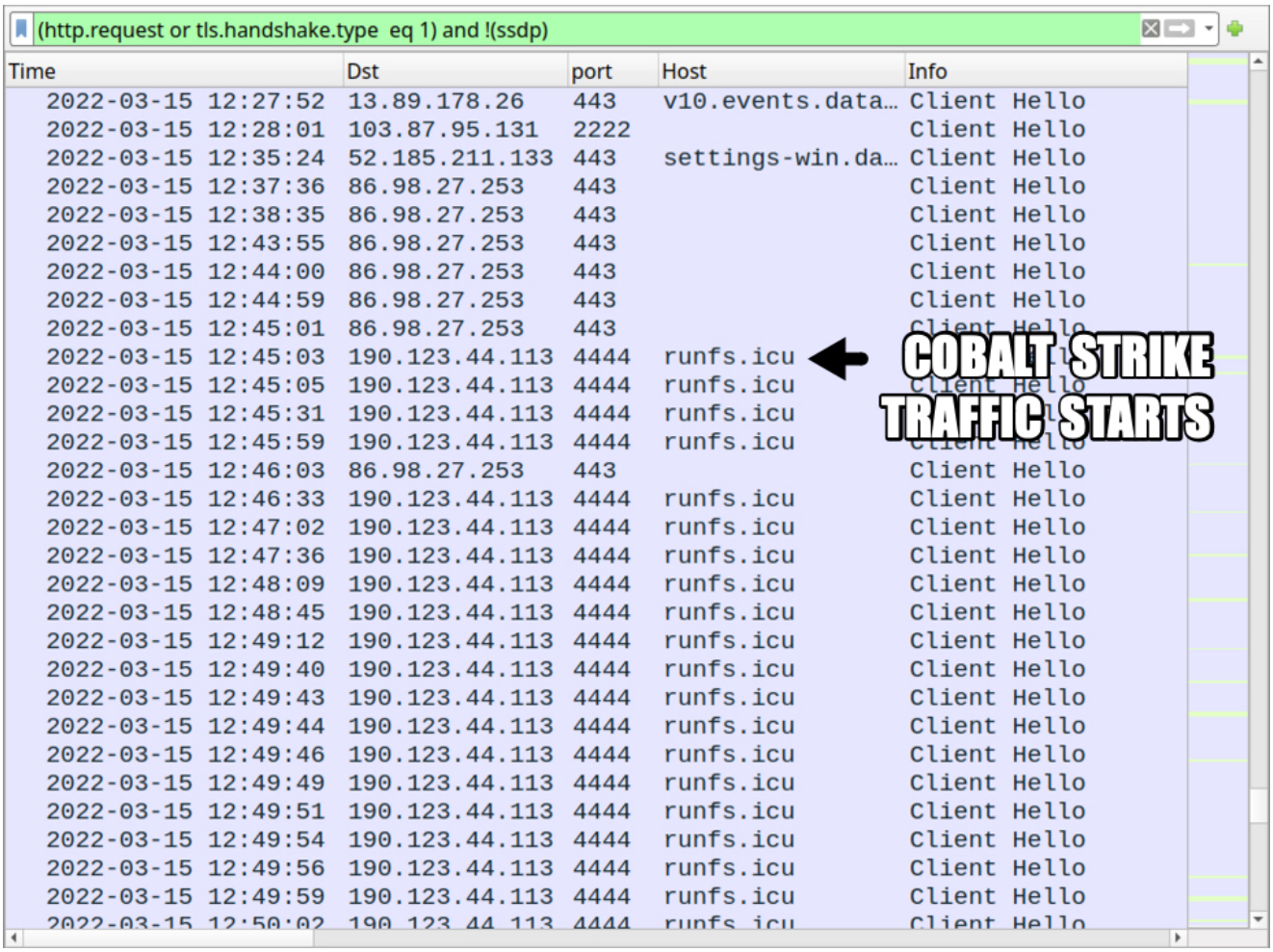
Shown above: More traffic from the Qakbot infection filtered in Wireshark.



Shown above: TCP traffic over port 65400 associated with this Qakbot infection.

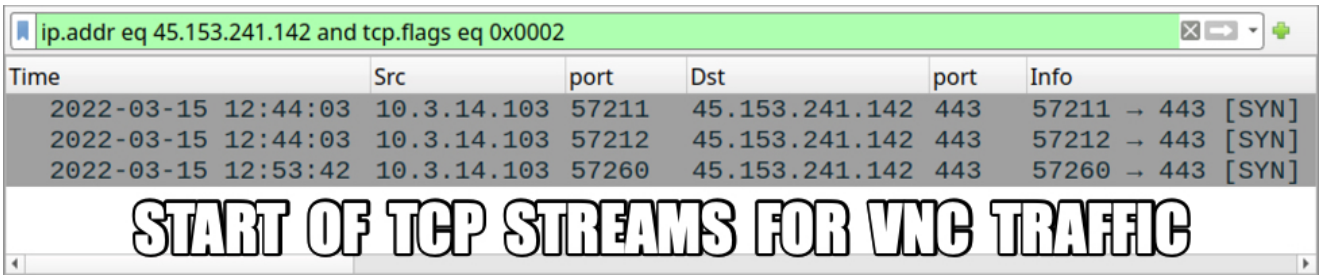


*Shown above: Data binary saved to disk at **C:\u** from the Qakbot infection.*



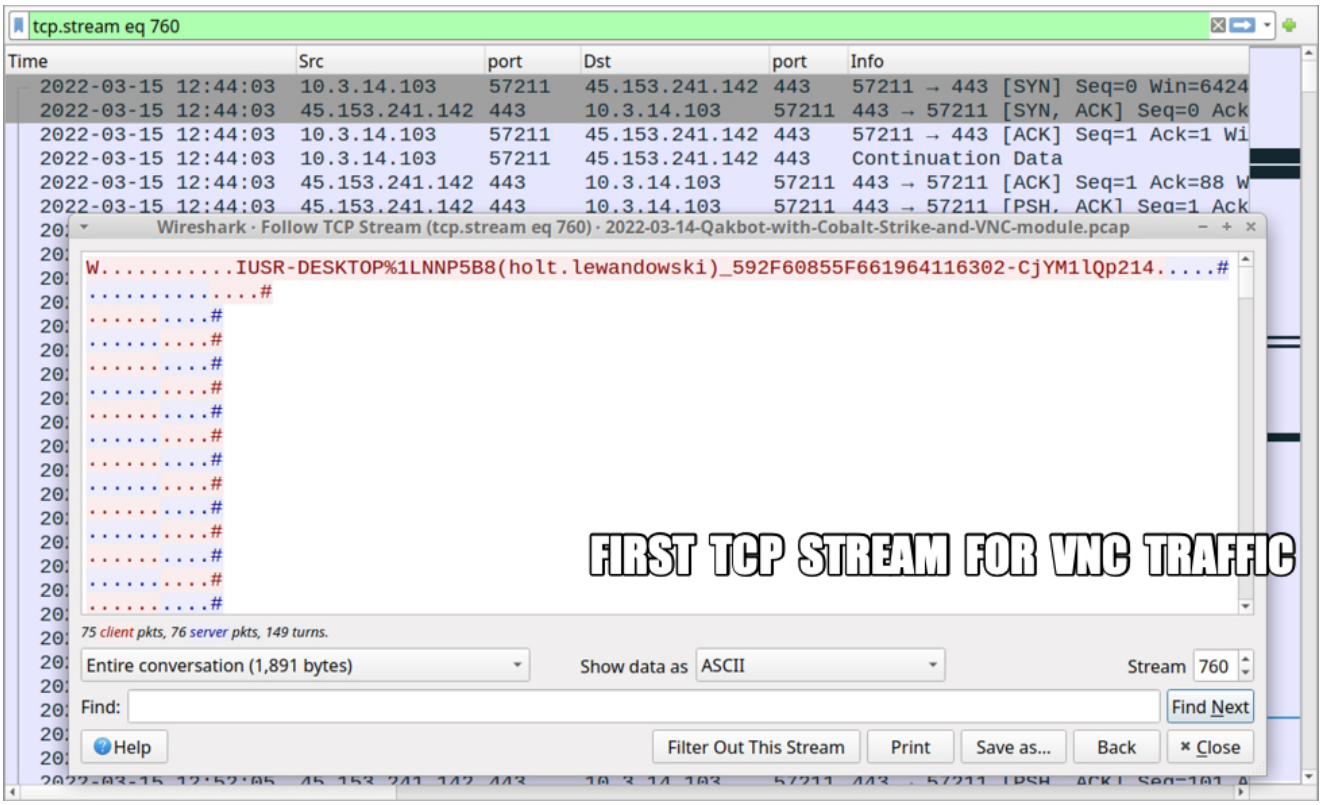
Time	Dst	port	Host	Info
2022-03-15 12:27:52	13.89.178.26	443	v10.events.data…	Client Hello
2022-03-15 12:28:01	103.87.95.131	2222		Client Hello
2022-03-15 12:35:24	52.185.211.133	443	settings-win.da…	Client Hello
2022-03-15 12:37:36	86.98.27.253	443		Client Hello
2022-03-15 12:38:35	86.98.27.253	443		Client Hello
2022-03-15 12:43:55	86.98.27.253	443		Client Hello
2022-03-15 12:44:00	86.98.27.253	443		Client Hello
2022-03-15 12:44:59	86.98.27.253	443		Client Hello
2022-03-15 12:45:01	86.98.27.253	443		Client Hello
2022-03-15 12:45:03	190.123.44.113	4444	runfs.icu	Client Hello
2022-03-15 12:45:05	190.123.44.113	4444	runfs.icu	Client Hello
2022-03-15 12:45:31	190.123.44.113	4444	runfs.icu	Client Hello
2022-03-15 12:45:59	190.123.44.113	4444	runfs.icu	Client Hello
2022-03-15 12:46:03	86.98.27.253	443		Client Hello
2022-03-15 12:46:33	190.123.44.113	4444	runfs.icu	Client Hello
2022-03-15 12:47:02	190.123.44.113	4444	runfs.icu	Client Hello
2022-03-15 12:47:36	190.123.44.113	4444	runfs.icu	Client Hello
2022-03-15 12:48:09	190.123.44.113	4444	runfs.icu	Client Hello
2022-03-15 12:48:45	190.123.44.113	4444	runfs.icu	Client Hello
2022-03-15 12:49:12	190.123.44.113	4444	runfs.icu	Client Hello
2022-03-15 12:49:40	190.123.44.113	4444	runfs.icu	Client Hello
2022-03-15 12:49:43	190.123.44.113	4444	runfs.icu	Client Hello
2022-03-15 12:49:44	190.123.44.113	4444	runfs.icu	Client Hello
2022-03-15 12:49:46	190.123.44.113	4444	runfs.icu	Client Hello
2022-03-15 12:49:49	190.123.44.113	4444	runfs.icu	Client Hello
2022-03-15 12:49:51	190.123.44.113	4444	runfs.icu	Client Hello
2022-03-15 12:49:54	190.123.44.113	4444	runfs.icu	Client Hello
2022-03-15 12:49:56	190.123.44.113	4444	runfs.icu	Client Hello
2022-03-15 12:49:59	190.123.44.113	4444	runfs.icu	Client Hello
2022-03-15 12:50:02	190.123.44.113	4444	runfs.icu	Client Hello

Shown above: Cobalt Strike activity started about 17 hours after the initial Qakbot infection.

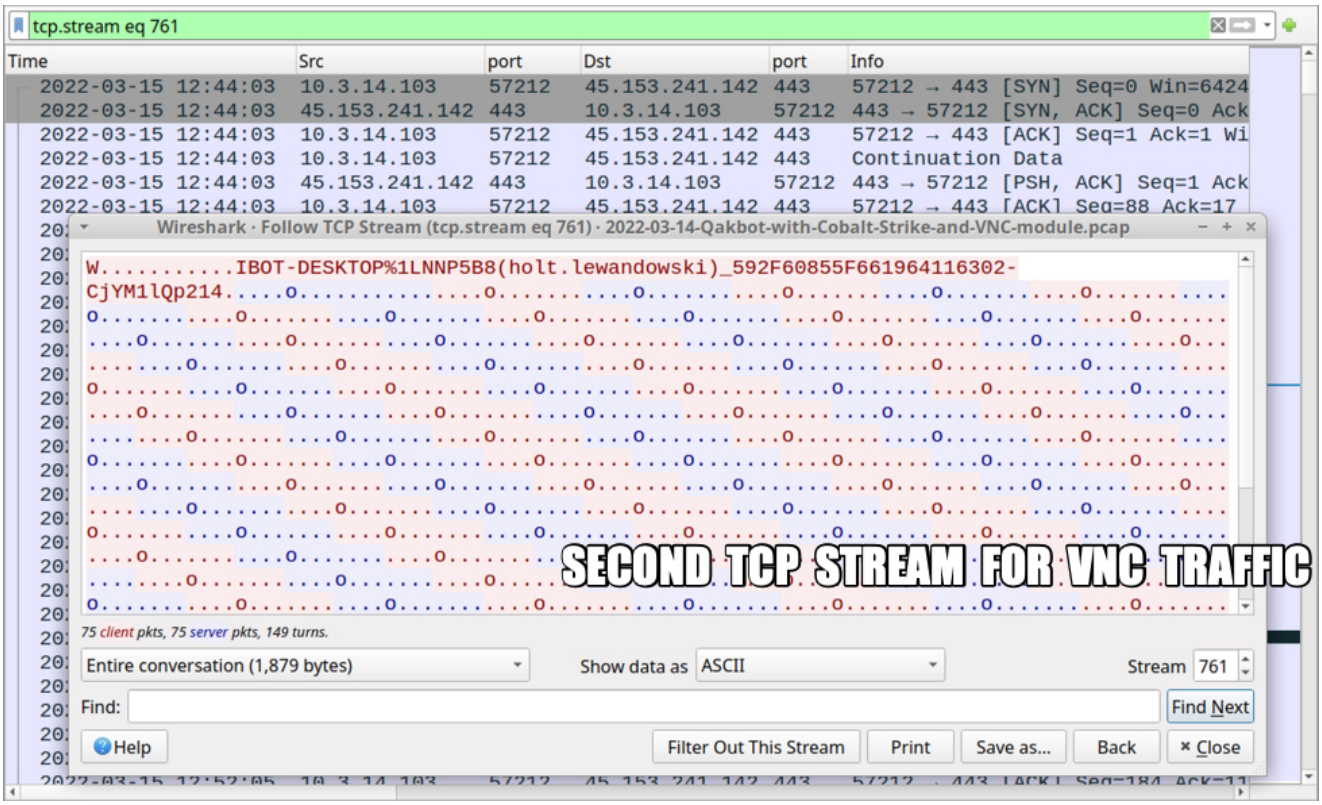


Time	Src	port	Dst	port	Info
2022-03-15 12:44:03	10.3.14.103	57211	45.153.241.142	443	57211 → 443 [SYN]
2022-03-15 12:44:03	10.3.14.103	57212	45.153.241.142	443	57212 → 443 [SYN]
2022-03-15 12:53:42	10.3.14.103	57260	45.153.241.142	443	57260 → 443 [SYN]

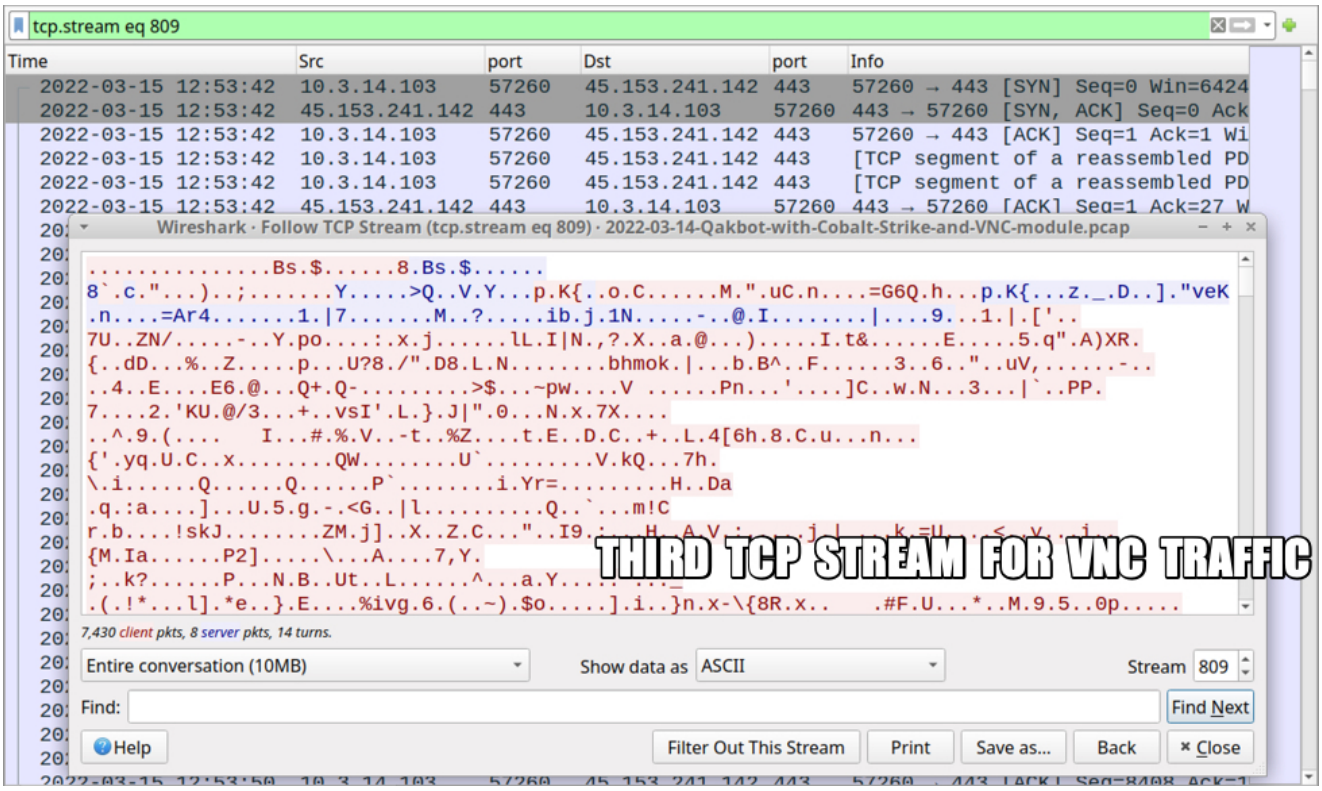
Shown above: TCP SYN segments for VNC traffic caused by this Qakbot infection.



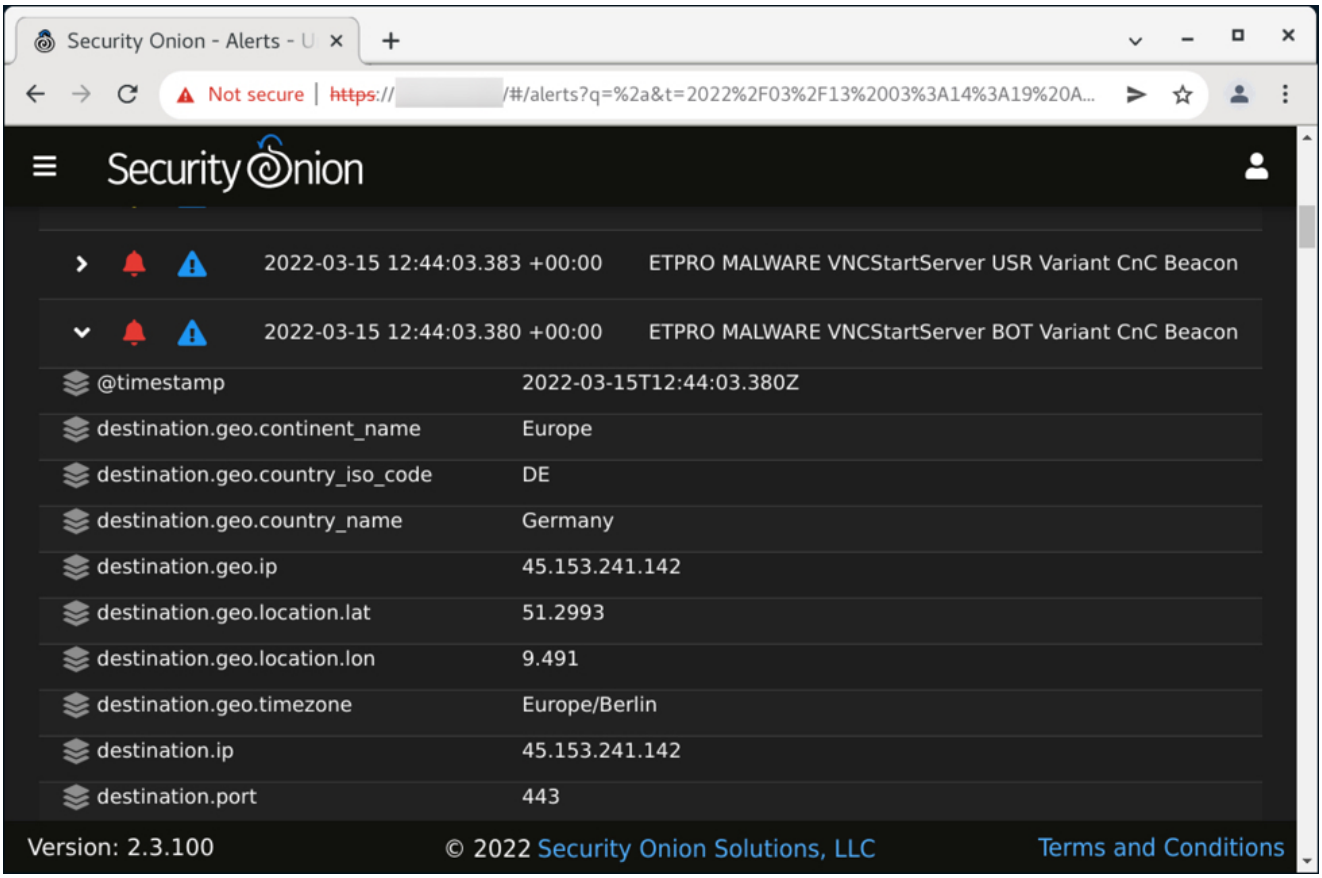
Shown above: First TCP stream for the VNC activity.



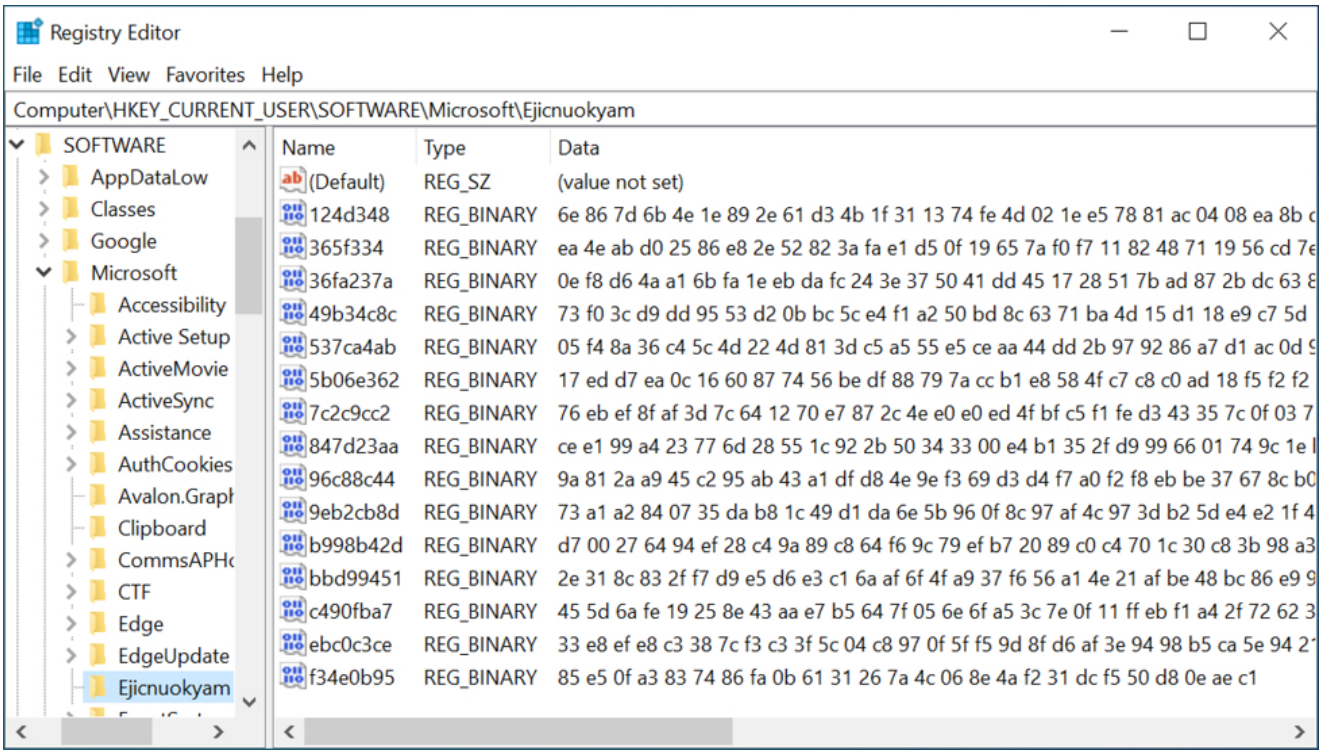
Shown above: Second TCP stream for the VNC activity.



Shown above: Third TCP stream for the VNC activity (10 MB of data).



Shown above: ETPRO alerts in Security Onion for the VNC traffic from this infection.



Shown above: Registry update made by the Qakbot infection.

Indicators of Compromise (IOCs)

Link from email for zip download:

hxxp://eaglio[.]org/apm/3/s2Fmok83x.zip

Traffic generated by Excel macro for Qakbot DLL files:

- hxxp://101.99.95[.]190/6537991.dat
- hxxp://146.70.81[.]64/6537991.dat
- hxxp://190.14.37[.]12/6537991.dat

Qakbot C2 traffic:

- 201.170.181[.]247 port 443 - HTTPS traffic
- port 443 - www.openssl[.]org - HTTPS traffic (connectivity check)
- 23.111.114[.]52 port 65400 - TCP traffic
- 76.169.147[.]192 port 32103 - HTTPS traffic
- 103.87.95[.]131 port 2222 - HTTPS traffic
- 86.98.27[.]253 port 443 - HTTPS traffic
- various IP addresses over various ports - attempted TCP connections

Cobalt Strike traffic:

190.123.44[.]113 port 4444 - runfs[.]icu - HTTPS traffic

VNC module traffic:

> 45.153.241[.]142 port 443 - encoded/encrypted traffic and beacon channels

Rule hits on VNC module traffic:

- ETPRO MALWARE VNCStartServer USR Variant CnC Beacon
- ETPRO MALWARE VNCStartServer BOT Variant CnC Beacon

Malware retrieved from the infected Windows client:

SHA256 hash: ba80720c42704e8e1a73e60906f6f289ba763365c8f6b16ccf47aac8a687b83e

- File size: 92,828 bytes
- File location: hxxp://eaglio[.]org/apm/3/s2Fmok83x.zip
- File name: ClaimDetails-1699343128-Mar-14.zip

SHA256 hash: 5a6157eefc8d0b1089a5bfdee351379b27baff4c40b432fd22e0cbe1f6102fab

- File size: 120,410 bytes
- File name: ClaimDetails-1699343128-Mar-14.xlsb

SHA256 hash:
47fe3cbab19b43579e3312d90f7a8c7021c84e228e7c8ef97d39a1a7a261ea01

- File size: 408,576 bytes
- File location: hxxp://101.99.95[.]190/6537991.dat
- File location: C:\Biloa\Dopaters1.ocx
- File type: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
- Run method: regsvr32.exe *[filename]*

SHA256 hash:
8751f8aedc65a10826071515b4b7896a8800152b8e3bcbbe9e8a64970deb9b49

- File size: 408,576 bytes
- File location: hxxp://146.70.81[.]64/6537991.dat
- File location: C:\Biloa\Dopaters2.ocx
- File type: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
- Run method: regsvr32.exe *[filename]*

SHA256 hash: 7312353bab71ecefec6888bb804afd71f67178ded4ce41960924d3d6f7400320

- File size: 408,576 bytes
- File location: hxxp://190.14.37[.]12/6537991.dat
- File location: C:\Biloa\Dopaters3.ocx
- File type: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows

- Run method: regsvr32.exe *[filename]*

SHA256 hash: 7264fc1e81ff854b769f8e19ced247fb95210a58ddd5edce4a6275ddc38e5298

- File size: 920,064 bytes
- File location: C:\Users\ *[username]*\AppData\Roaming\Microsoft\Hezuky\bbcdipimaxckk.dll
- File type: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
- Run method: regsvr32.exe *[filename]*

Note: No binaries for Cobalt Strike or the VNC activity were found on the infected Windows host.

Final words

This infection shows some changes in Qakbot.

Earlier this year, Qakbot samples created a scheduled task that pointed to an additional registry update with base64 code used to re-create the Qakbot binary after a reboot. I no longer see that with recent Qakbot samples.

Also, this infection didn't stay persistent after logging out or doing a reboot. Normally, Qakbot keeps the active DLL in memory. If a victim logs our or reboots, Qakbot saves the in-memory DLL to disk and creates a registry update at ***HKCU\Software\Microsoft\Windows\CurrentVersion\Run***. After rebooting and/or logging back in, this registry update loads the DLL, then Qakbot deletes the registry update and erases the DLL that had been saved to disk.

In this case, a Qakbot DLL was already saved to disk long before I tried logging out/rebooting. Furthermore, the infection did not persist after I logged out.

There's also a data binary stored at a `C:\u\` directory created by Qakbot. From a forensic point of view, things are noticeably different with recent Qakbot infections. Not drastically different, but the changes are noticeable.

A pcap of the infection traffic along with malware (Excel file and DLL) from an infected host can be found here.

Brad Duncan
brad [at] malware-traffic-analysis.net

Keywords: VNC Qbot Qakbot malspam CobaltStrike Cobalt Strike

Top of page

×

Diary Archives