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

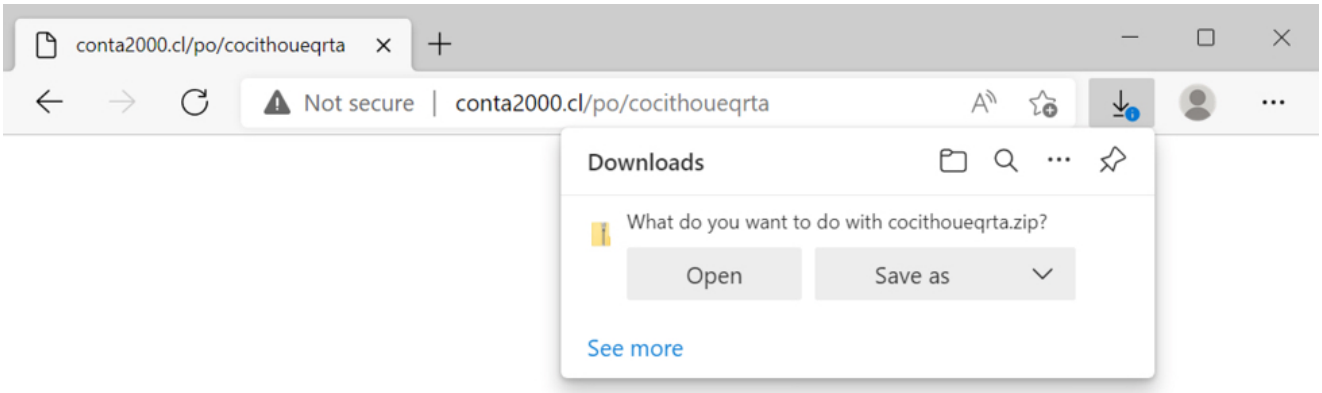
"aa" distribution Qakbot (Qbot) infection with DarkVNC traffic

Published: 2022-04-20
Last Updated: 2022-04-20 03:17:36 UTC
by Brad Duncan (Version: 1)
1 comment(s)

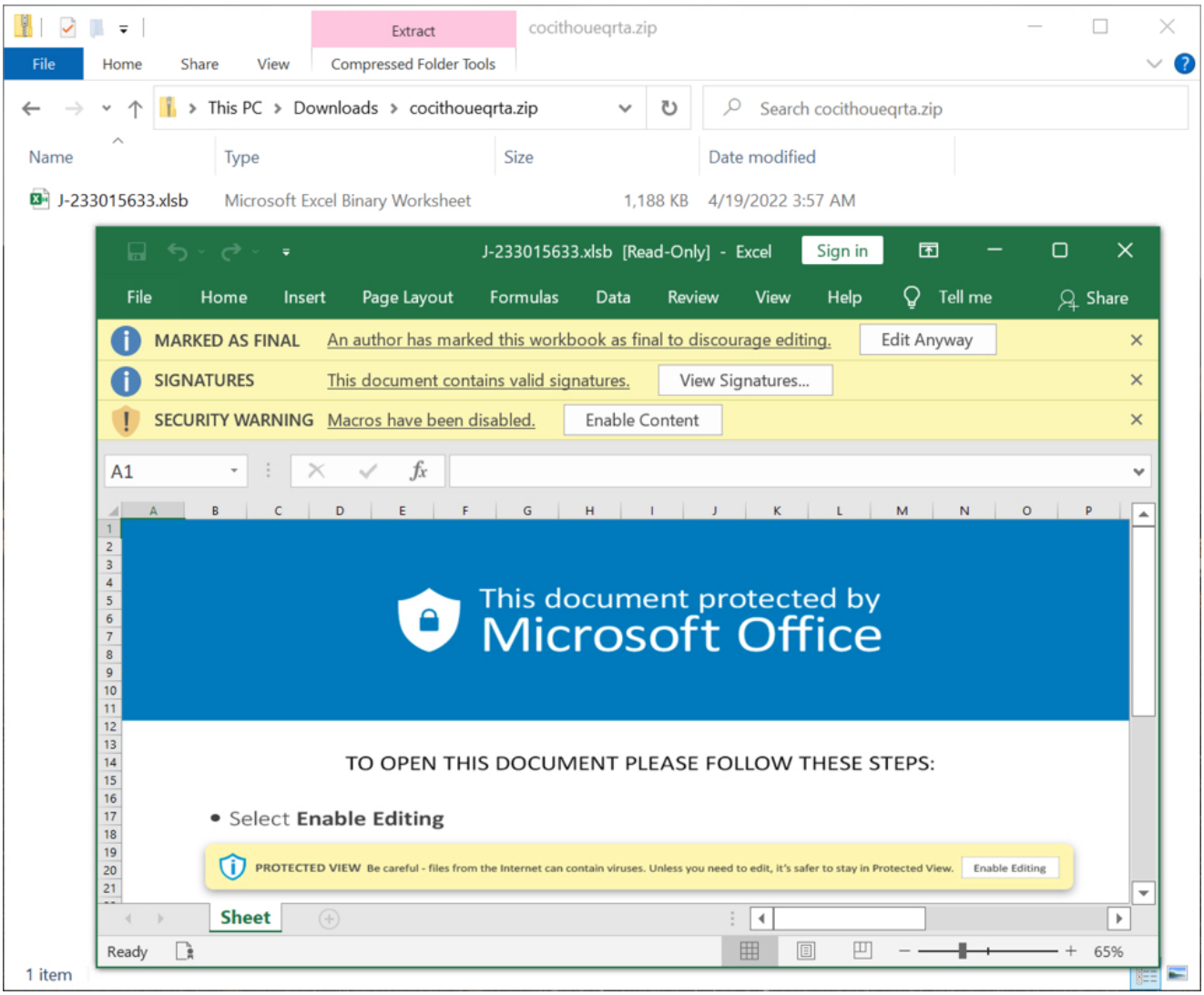
Chain of Events

Email --> link --> downloaded zip archive --> extracted Excel file --> enable macros --> HTTPS traffic for Qakbot DLL files --> Qakbot C2 activity --> DarkVNC traffic

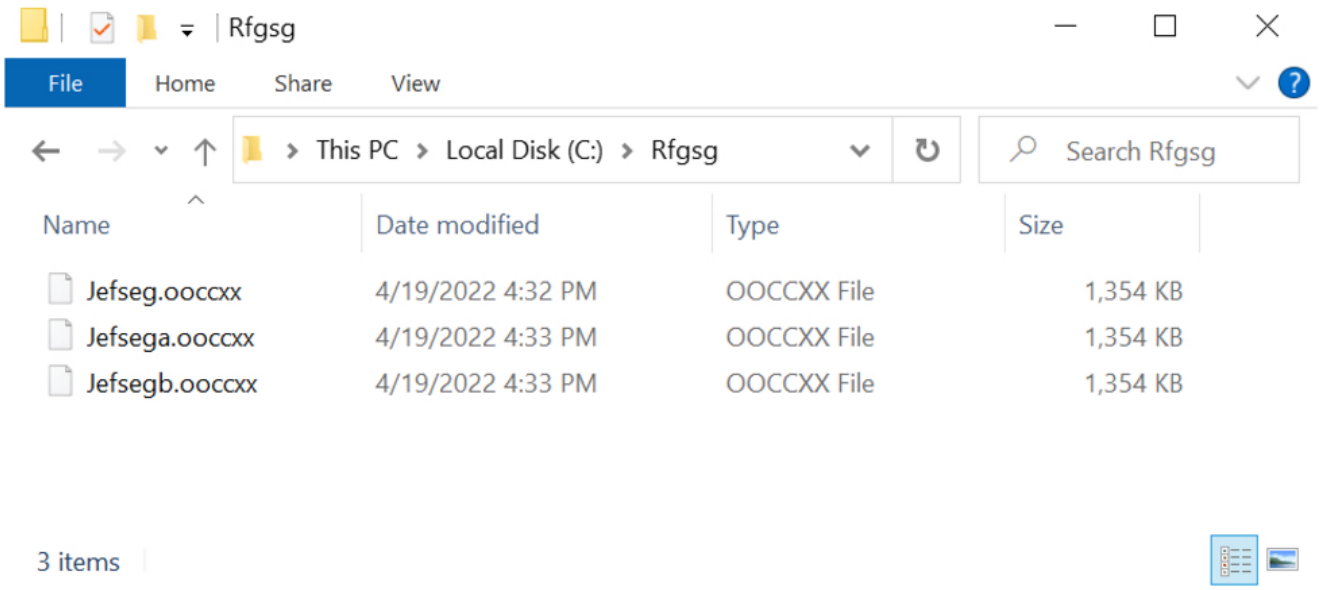
Images



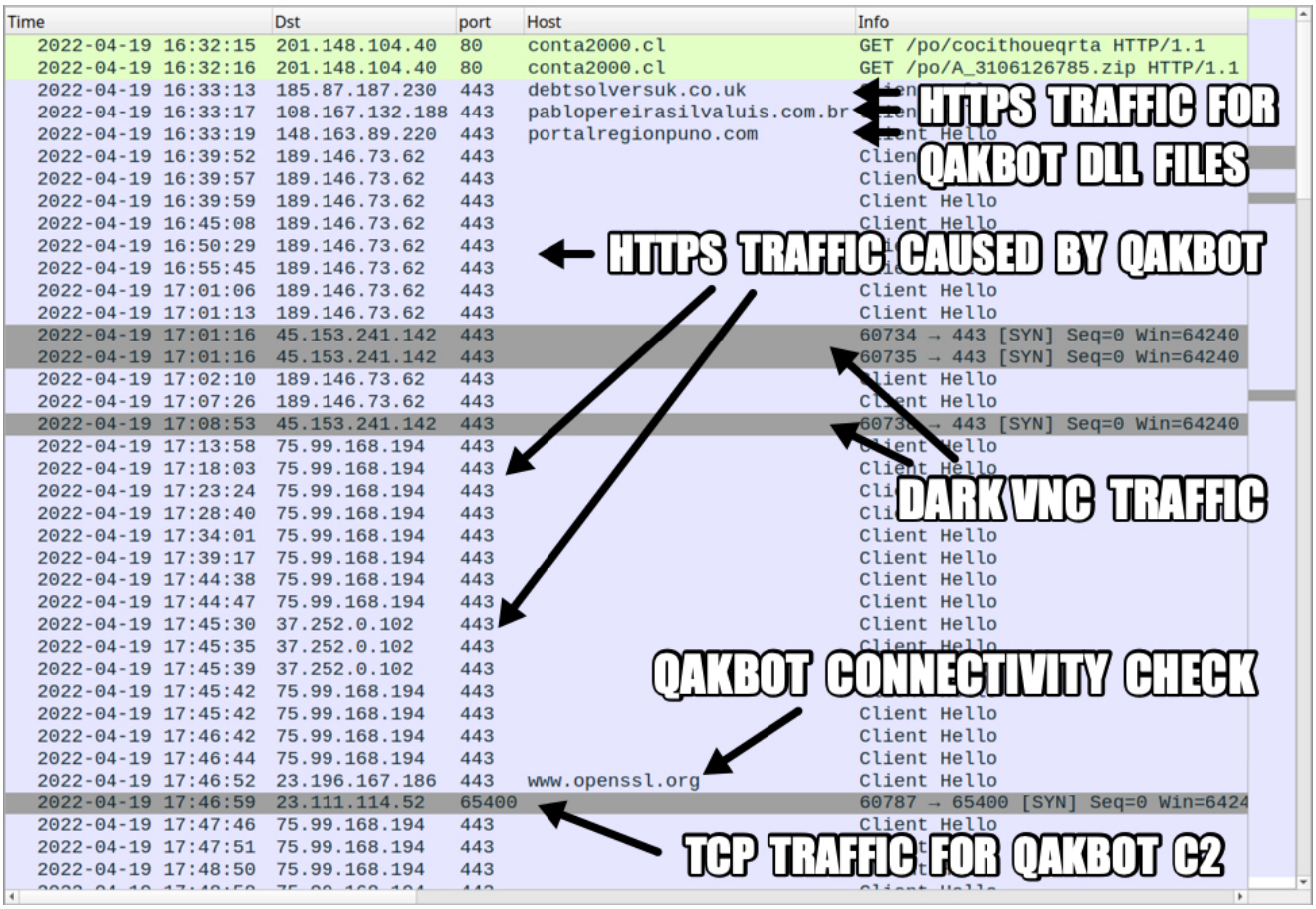
Shown above: Link from an email distributing Qakbot ("aa" distribution tag) in a web browser.



Shown above: Downloaded zip archive and extracted spreadsheet.

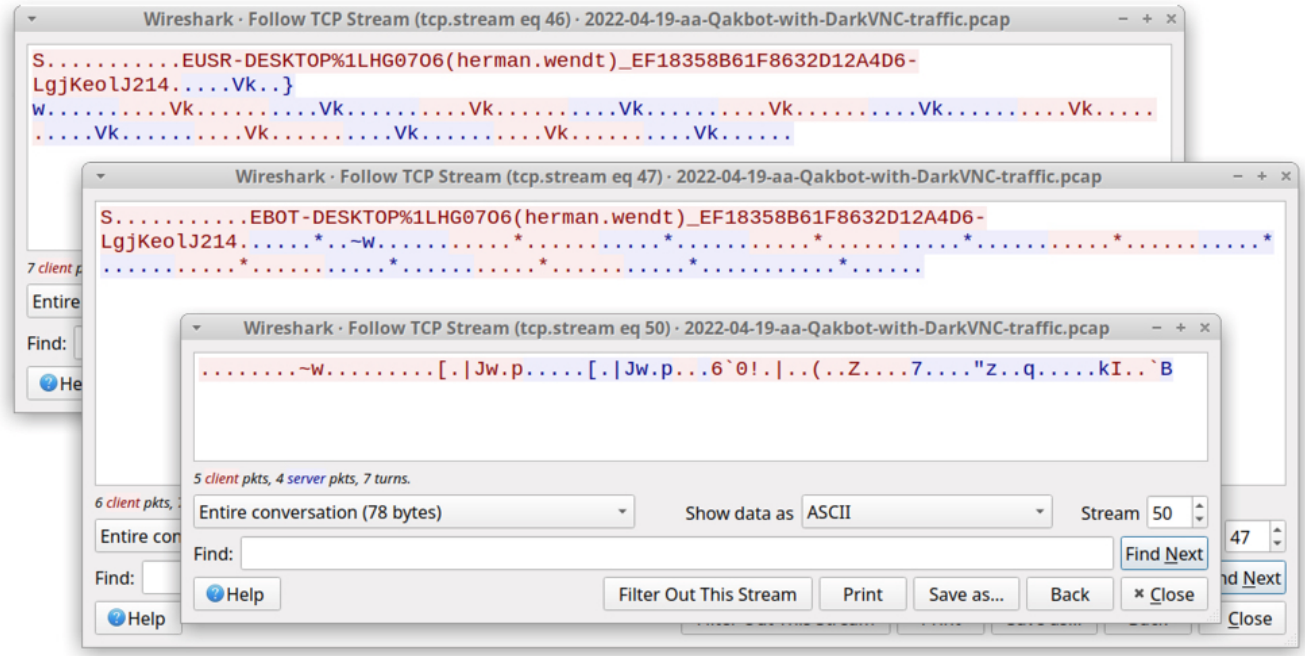


Shown above: Qakbot DLL files saved to an infected Windows host.

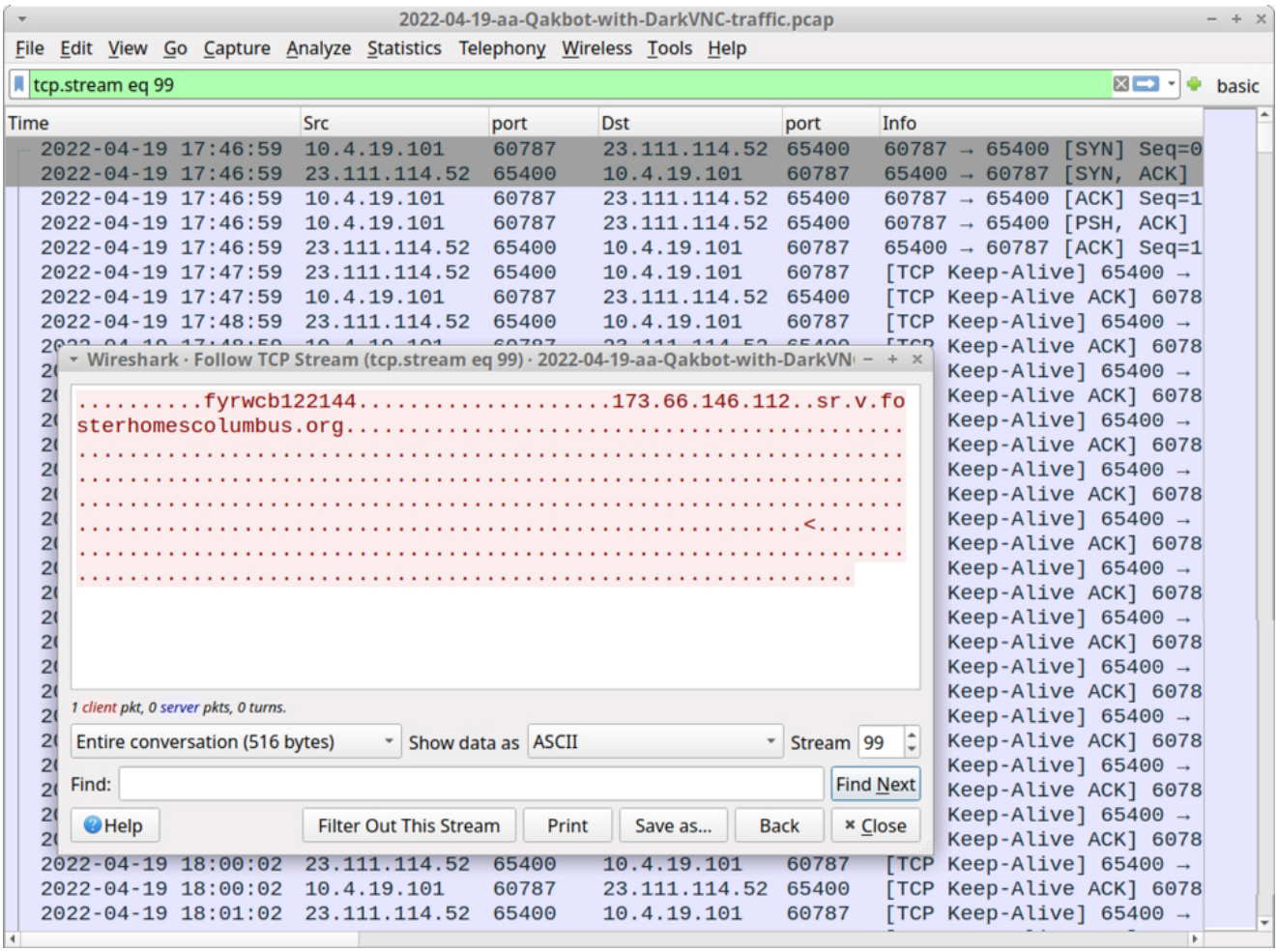


Time	Dst	port	Host	Info
2022-04-19 16:32:15	201.148.104.40	80	conta2000.cl	GET /po/cocithoueqrta HTTP/1.1
2022-04-19 16:32:16	201.148.104.40	80	conta2000.cl	GET /po/A_3106126785.zip HTTP/1.1
2022-04-19 16:33:13	185.87.187.230	443	debtsolversuk.co.uk	Client Hello
2022-04-19 16:33:17	108.167.132.188	443	pablopereirasilvaluis.com.br	Client Hello
2022-04-19 16:33:19	148.163.89.220	443	portalregionpuno.com	Client Hello
2022-04-19 16:39:52	189.146.73.62	443		Client Hello
2022-04-19 16:39:57	189.146.73.62	443		Client Hello
2022-04-19 16:39:59	189.146.73.62	443		Client Hello
2022-04-19 16:45:08	189.146.73.62	443		Client Hello
2022-04-19 16:50:29	189.146.73.62	443		Client Hello
2022-04-19 16:55:45	189.146.73.62	443		Client Hello
2022-04-19 17:01:06	189.146.73.62	443		Client Hello
2022-04-19 17:01:13	189.146.73.62	443		Client Hello
2022-04-19 17:01:16	45.153.241.142	443		60734 → 443 [SYN] Seq=0 Win=64240
2022-04-19 17:01:16	45.153.241.142	443		60735 → 443 [SYN] Seq=0 Win=64240
2022-04-19 17:02:10	189.146.73.62	443		Client Hello
2022-04-19 17:07:26	189.146.73.62	443		Client Hello
2022-04-19 17:08:53	45.153.241.142	443		60736 → 443 [SYN] Seq=0 Win=64240
2022-04-19 17:13:58	75.99.168.194	443		Client Hello
2022-04-19 17:18:03	75.99.168.194	443		Client Hello
2022-04-19 17:23:24	75.99.168.194	443		Client Hello
2022-04-19 17:28:40	75.99.168.194	443		Client Hello
2022-04-19 17:34:01	75.99.168.194	443		Client Hello
2022-04-19 17:39:17	75.99.168.194	443		Client Hello
2022-04-19 17:44:38	75.99.168.194	443		Client Hello
2022-04-19 17:44:47	75.99.168.194	443		Client Hello
2022-04-19 17:45:30	37.252.0.102	443		Client Hello
2022-04-19 17:45:35	37.252.0.102	443		Client Hello
2022-04-19 17:45:39	37.252.0.102	443		Client Hello
2022-04-19 17:45:42	75.99.168.194	443		Client Hello
2022-04-19 17:45:42	75.99.168.194	443		Client Hello
2022-04-19 17:46:42	75.99.168.194	443		Client Hello
2022-04-19 17:46:44	75.99.168.194	443		Client Hello
2022-04-19 17:46:52	23.196.167.186	443	www.openssl.org	Client Hello
2022-04-19 17:46:59	23.111.114.52	65400		60787 → 65400 [SYN] Seq=0 Win=6424
2022-04-19 17:47:46	75.99.168.194	443		Client Hello
2022-04-19 17:47:51	75.99.168.194	443		Client Hello
2022-04-19 17:48:50	75.99.168.194	443		Client Hello

Shown above: Traffic from the infection filtered in Wireshark.



Shown above: TCP streams for DarkVNC traffic on 45.153.241[.]142 over TCP port 443.



Shown above: Qakbot traffic on 23.111.114[.]52 over TCP port 65400.

Indicators of Compromise (IOCs)

Malware from an infected Windows host:

SHA256 hash: 685aa1d29540f5b63effec08fdf63f8bc7e995d1f15635cc1fd251bb7fb0dc73

- File size: 1,093,506 bytes
- File name: cocithoueqrta.zip
- File location: hxxps://conta2000[.]cl/po/cocithoueqrta
- File location: hxxps://conta2000[.]cl/po/A3105126785.zip
- File description: zip archive downloaded from link in email

SHA256 hash:
236b9d345a9b405c4850f880e1734712967d7cc34b176c270e78dd6f02f9839d

- File size: 1,215,731 bytes
- File name: J-233015633.xlsb
- File description: Excel file with macro for Qakbot

SHA256 hash: 74400f2acc98e59ddeba6d55da3ee0ea0c909eefdefeca4f1d3bf817a27b692b

- File size: 1,385,866 bytes
- File location: hxxps://debtsolversuk[.]co[.]uk/HLpeQJZi/NbVfNbhn.png
- File location: C:\Rfgsg\Jefseg.ooccxx
- File description: Initial Qakbot DLL
- Run method: regsvr32.exe *[filename]*

SHA256 hash: 29942eb47c0de0415b2507dff8822e3309dd4fcc2ac8d01434b37eb4f75efbe1

- File size: 1,385,893 bytes
- File location: hxxps://pablopereirasilvaluis[.]com[.]br/OHTvXEr9c/NbVfNbhn.png
- File location: C:\Rfgsg\Jefsega.ooccxx
- Run method: regsvr32.exe *[filename]*

SHA256 hash: 59fb3927427c68dee4c2f267f3ed4eea82dc07058061e06b3cd9b18d1a84b77f

- File size: 1,385,920 bytes
- File location: hxxps://portalregionpuno[.]com/088aFy0Xc8ap/NbVfNbhn.png
- File location: C:\Rfgsg\Jefsegb.ooccxx
- Run method: regsvr32.exe *[filename]*

Traffic for zip archive:

- hxxps://conta2000[.]cl/po/cocithoueqrta
- hxxps://conta2000[.]cl/po/A3105126785.zip

Traffic for Qakbot DLL files:

- hxxps://debtsolversuk[.]co[.]uk/HLpeQJZi/NbVfNbhn.png
- hxxps://pablopereirasilvaluis[.]com[.]br/OHTvXEr9c/NbVfNbhn.png
- hxxps://portalregionpuno[.]com/088aFy0Xc8ap/NbVfNbhn.png

Qakbot post-infection traffic:

- 189.146.73[.]62 port 443 - HTTPS traffic
- 75.99.168[.]194 port 443 - HTTPS traffic
- 37.252.0[.]102 port 443 - HTTPS traffic
- port 443 - www.openssl[.]org - HTTPS traffic (connectivity check, not inherently malicious)
- 23.111.114[.]52 port 65400 - TCP traffic

Dark VNC traffic:

45.153.241[.]142 port 443 - TCP traffic with encoded data.

Certificate issuer data for Qakbot HTTPS traffic:

Certificate issuer data for HTTPS traffic to 189.146.73[.]62:

- id-at-countryName=***AU***
- id-at-stateOrProvinceName=***DA***
- id-at-localityName=***Ieiaegim***
- id-at-organizationName=***Vuropti Mika Aguaugaf Inc.***
- id-at-commonName=***qchzpkuwhuh.org***

Certificate issuer data for HTTPS traffic to 75.99.168[.]194:

- id-at-countryName=***AU***
- id-at-stateOrProvinceName=***WD***
- id-at-localityName=***Ntp***
- id-at-organizationName=***Venyec Giteg Xgsw Inc.***
- id-at-commonName=***onuwbkiz.us***

Certificate issuer data for HTTPS traffic to 37.252.0[.]102:

- id-at-countryName=***US***
- id-at-stateOrProvinceName=***CA***
- id-at-localityName=***Los Angeles***
- id-at-organizationName=***vipsauna[.]com***
- id-at-commonName=***vipsauna[.]com***

Final words

A packet capture (pcap) of the infection traffic and the associated malware samples are available here. The pcap is from an Active Directory (AD) environment. The pcap been sanitized to disguise usernames, hostnames, domains, internal IP addresses, the public IP address used to connect from my test lab to the Internet, and any other information that could identify the environment.

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

Keywords: DarkVNC Excel macros Qakbot Qbot VNC zip
1 comment(s)

Top of page
×

Diary Archives