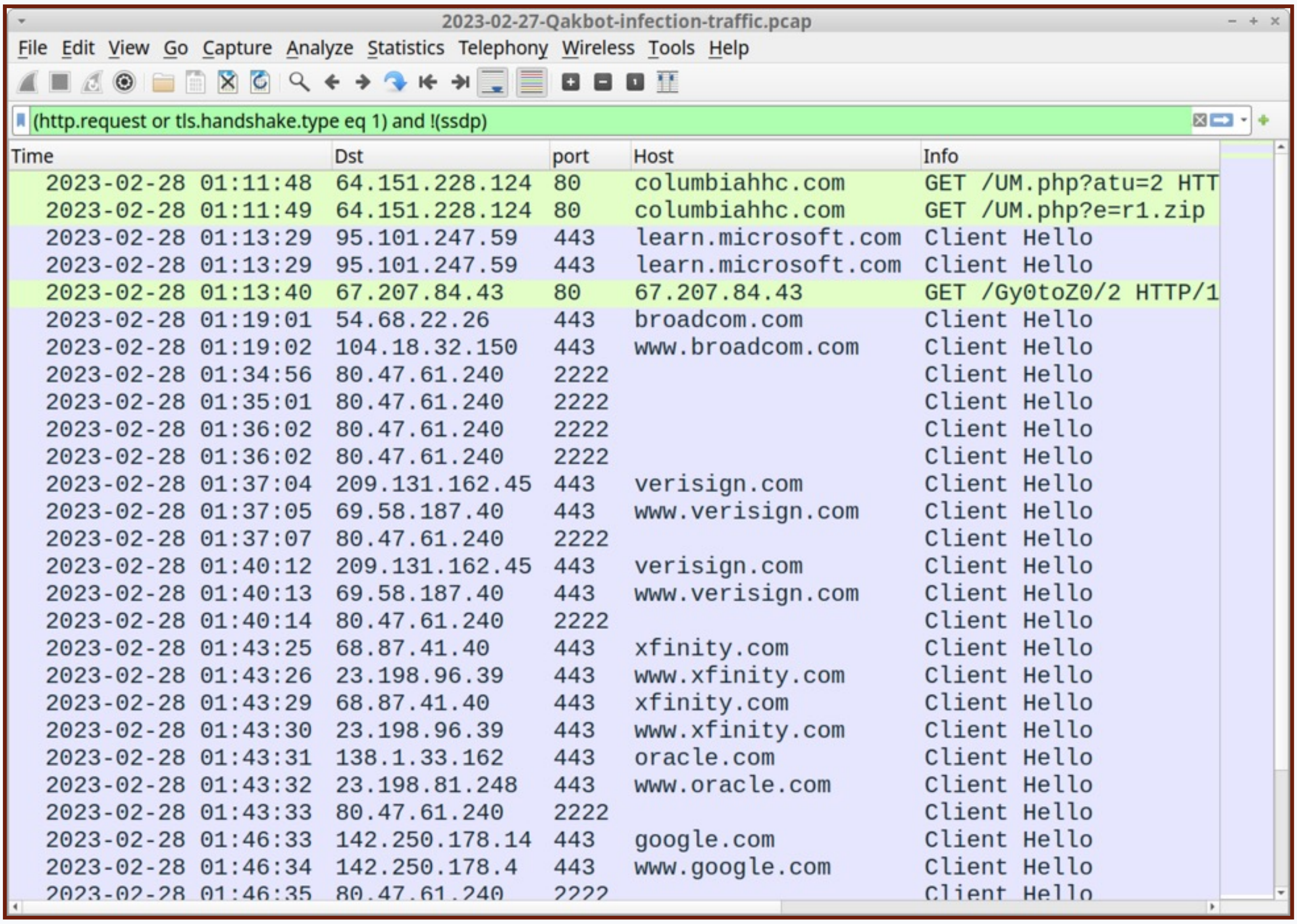
BB17 distribution Qakbot (Qbot) activity

Published: 2023-02-28
Last Updated: 2023-02-28 22:19:46 UTC
by Brad Duncan (Version: 1)

0 comment(s)

Introduction

Early morning Tuesday 2023-02-28, I generated an infection with a URL I found on VirusTotal after pivoting on a search for BB17-tagged distribution URLs for Qakbot (Qbot). Based on other public reports, I saw the expected Qakbot activity. Today's diary shares indicators from the infection.


2023-02-27-Qakbot-infection-traffic.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

```
Time                 Dst              port  Host                Info
2023-02-28 01:11:48  64.151.228.124   80    columbiahhc.com     GET /UM.php?atu=2 HTT
2023-02-28 01:11:49  64.151.228.124   80    columbiahhc.com     GET /UM.php?e=r1.zip
2023-02-28 01:13:29  95.101.247.59    443   learn.microsoft.com Client Hello
2023-02-28 01:13:29  95.101.247.59    443   learn.microsoft.com Client Hello
2023-02-28 01:13:40  67.207.84.43     80    67.207.84.43        GET /Gy0toZ0/2 HTTP/1
2023-02-28 01:19:01  54.68.22.26      443   broadcom.com        Client Hello
2023-02-28 01:19:02  104.18.32.150    443   www.broadcom.com    Client Hello
2023-02-28 01:34:56  80.47.61.240     2222                      Client Hello
2023-02-28 01:35:01  80.47.61.240     2222                      Client Hello
2023-02-28 01:36:02  80.47.61.240     2222                      Client Hello
2023-02-28 01:36:02  80.47.61.240     2222                      Client Hello
2023-02-28 01:37:04  209.131.162.45   443   verisign.com        Client Hello
2023-02-28 01:37:05  69.58.187.40     443   www.verisign.com    Client Hello
2023-02-28 01:37:07  80.47.61.240     2222                      Client Hello
2023-02-28 01:40:12  209.131.162.45   443   verisign.com        Client Hello
2023-02-28 01:40:13  69.58.187.40     443   www.verisign.com    Client Hello
2023-02-28 01:40:14  80.47.61.240     2222                      Client Hello
2023-02-28 01:43:25  68.87.41.40      443   xfinity.com         Client Hello
2023-02-28 01:43:26  23.198.96.39     443   www.xfinity.com     Client Hello
2023-02-28 01:43:29  68.87.41.40      443   xfinity.com         Client Hello
2023-02-28 01:43:30  23.198.96.39     443   www.xfinity.com     Client Hello
2023-02-28 01:43:31  138.1.33.162     443   oracle.com          Client Hello
2023-02-28 01:43:32  23.198.81.248    443   www.oracle.com      Client Hello
2023-02-28 01:43:33  80.47.61.240     2222                      Client Hello
2023-02-28 01:46:33  142.250.178.14   443   google.com          Client Hello
2023-02-28 01:46:34  142.250.178.4    443   www.google.com      Client Hello
2023-02-28 01:46:35  80.47.61.240     2222                      Client Hello
```

Shown above: Traffic from the infection filtered in Wireshark.

Indicators of Compromise (IOCs)

Files extracted from the pcap:

SHA256 hash: 5fb714dfc9206ab4d188bf3c0cb35c44fbf5246f863c1efd5fdaecaa0891bd7a

File size: 385,552 bytes
File name: ***clamouring.zip***
File location: hxxp://columbiahhc[.]com/UM.php?atu=2
File type: Zip archive data, at least v2.0 to extract, compression method=deflate
File description: password-protected zip archive containing malicious disk image
Password: ***764***

SHA256 hash: e62a7453020148080614f7bd81ae3c316b1655b60845606120a6d671c5aaac43

File size: 798,720 bytes
File name: ***clamouring.img***
File type: ISO 9660 CD-ROM filesystem data 'CD_ROM'
File description: Extracted from the above zip file, disk image with files for Qakbot infection

SHA256 hash: 442420af4fc55164f5390ec68847bba4ae81d74534727975f47b7dd9d6dbdbe7

File size: 606,304 bytes
File location: ***hxxp://67.207.84[.]43/Gy0toZ0/2***
File type: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
File description: Qakbot DLL returned from 67.207.84[.]43
Run method: ***rundll32.exe*** *[filename]* ***,N115***

Traffic from link for password-protected zip archive:

64.151.228[.]124 port ***80*** - ***columbiahhc[.]com*** - GET /UM.php?atu=2
64.151.228[.]124 port ***80*** - ***columbiahhc[.]com*** - GET /UM.php?e=r1.zip

Traffic to retrieve the initial Qakbot DLL:

67.207.84[.]43 port ***80*** - ***67.207.84[.]43*** - GET /Gy0toZ0/2

Qakbot C2:

80.47.61[.]240 port ***2222*** - HTTPS traffic
185.80.53[.]210 port ***443*** - HTTPS traffic
port 443 - ***www.openssl.org*** - HTTPS traffic <-- legitimate domain used for connectivity check by Qakbot
23.111.114[.]52 port ***65400*** - TCP traffic

Connectivity checks to legitimate domains generated by Qakbot C2 traffic. This traffic is not malicious, but was generated by the infection:

port 443 - ***broadcom.com***
port 443 - ***cisco.com***

port 443 - ***google.com***
port 443 - ***linkedin.com***
port 443 - ***irs.gov***
port 443 - ***microsoft.com***
port 443 - ***oracle.com***
port 443 - ***verisign.com***
port 443 - ***xfinity.com***
port 443 - ***yahoo.com***

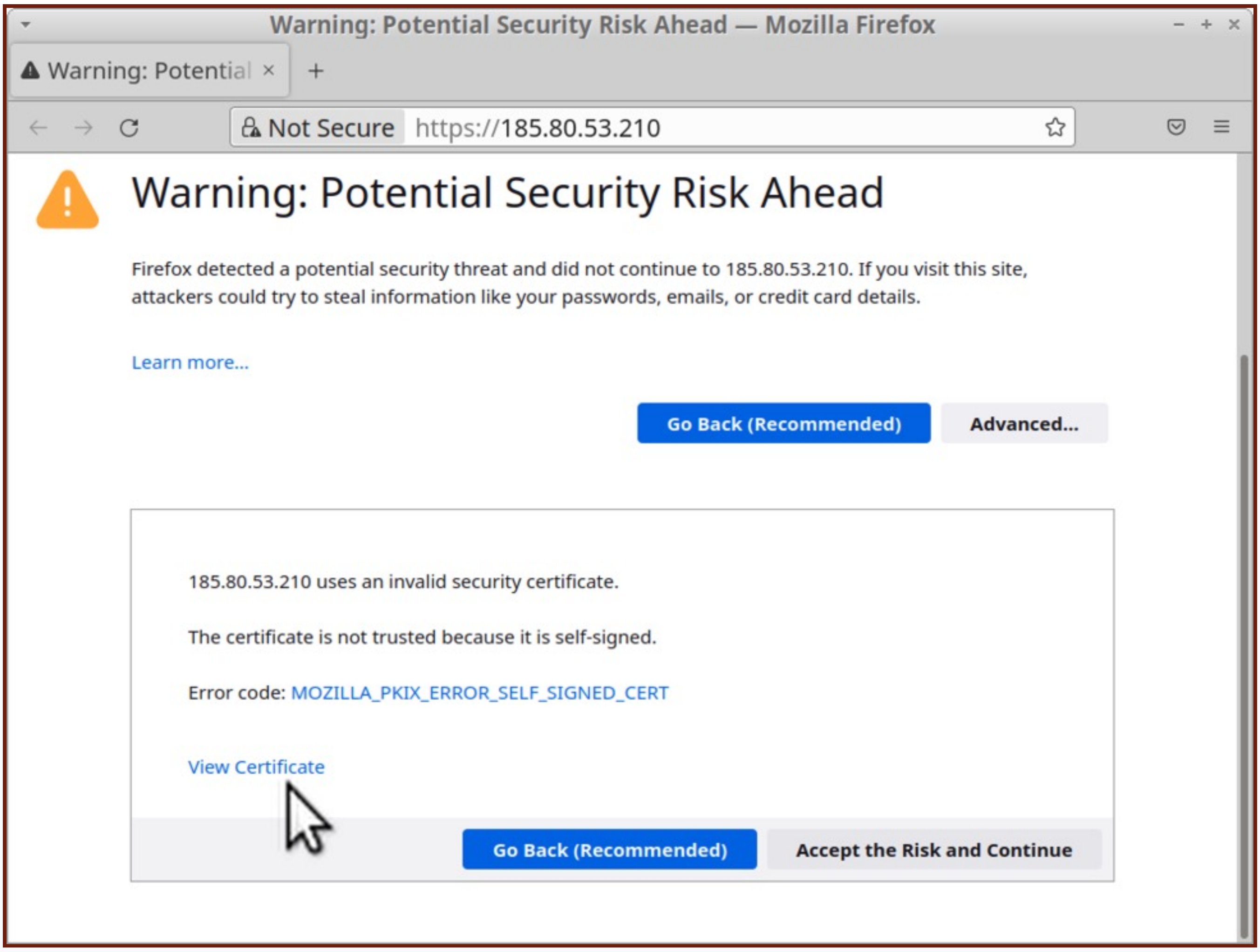
Self-signed certificate for Qakbot C2 at ***80.47.61[.]240***:

id-at-countryName=***PT***
id-at-stateOrProvinceName=***NO***
id-at-localityName=***Utjxyj***
id-at-organizationName=***Qdf Wah Uotvzke LLC.***
id-at-commonName=***meieou.info***

Self-signed certificate for Qakbot C2 at ***185.80.53[.]210***:

id-at-countryName=***US***
id-at-stateOrProvinceName=***NY***
id-at-localityName=***New York***
id-at-organizationName=***gifts.com***
id-at-commonName=***gifts.com***

Note: The above is a self-signed certificate used by the Qakbot C2 server and is not associated with the actual ***gifts.com*** website.



Warning: Potential Security Risk Ahead — Mozilla Firefox

Not Secure https://185.80.53.210

Warning: Potential Security Risk Ahead

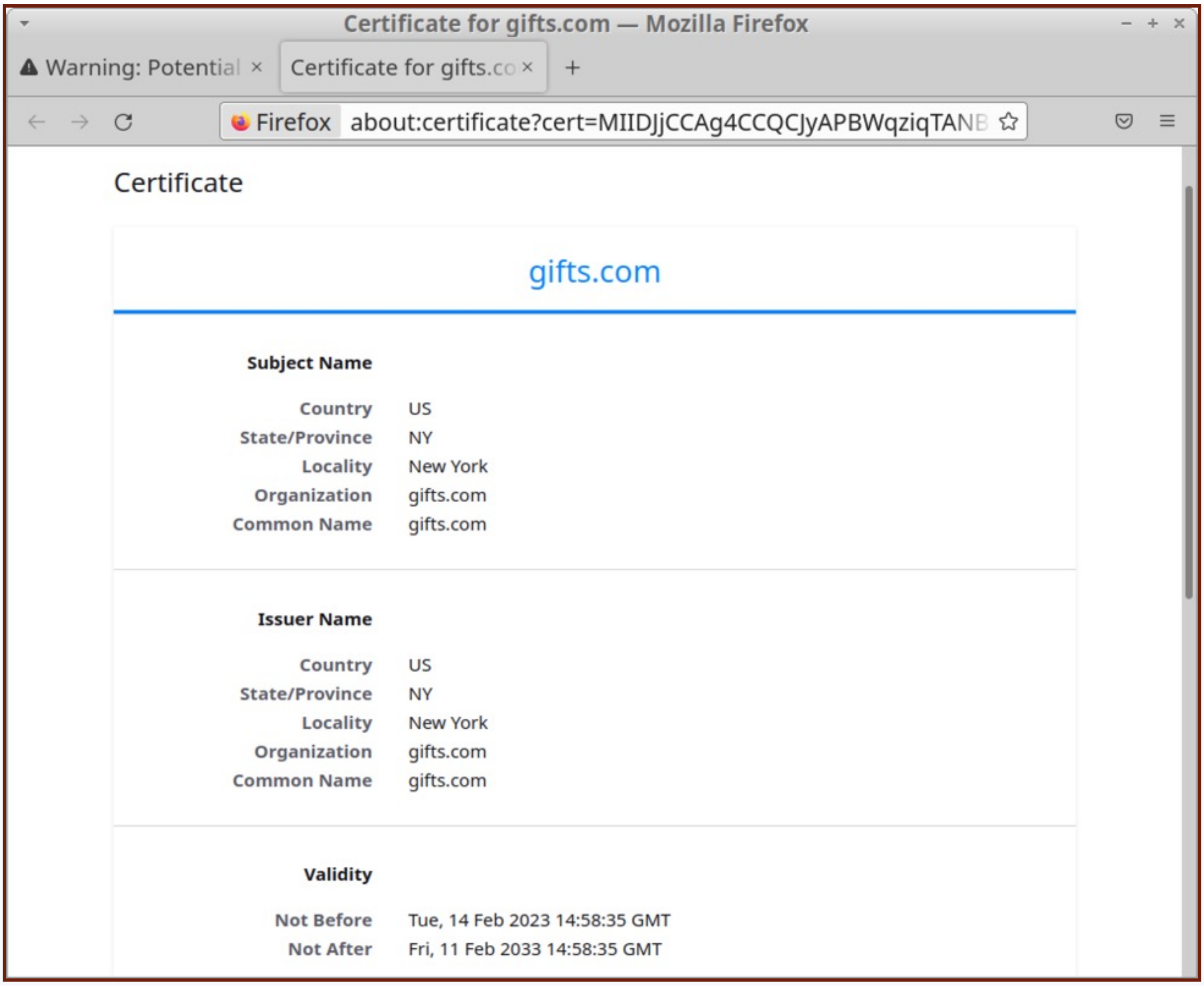
Firefox detected a potential security threat and did not continue to 185.80.53.210. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

185.80.53.210 uses an invalid security certificate.

The certificate is not trusted because it is self-signed.

Error code: MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT

Shown above: Qakbot C2 server at 185.80.53[.]210 shows security warning for self-signed certificate when viewed in a web browser.


Certificate for gifts.com — Mozilla Firefox
Warning: Potential
Certificate for gifts.co
Firefox
about:certificate?cert=MIIDJjCCAg4CCQCJyAPBWqziqTANB

Certificate

gifts.com

Subject Name

Country	US
State/Province	NY
Locality	New York
Organization	gifts.com
Common Name	gifts.com

Issuer Name

Country	US
State/Province	NY
Locality	New York
Organization	gifts.com
Common Name	gifts.com

Validity

Not Before	Tue, 14 Feb 2023 14:58:35 GMT
Not After	Fri, 11 Feb 2033 14:58:35 GMT

Shown abovve: Self-signed certificate data for Qakbot C2 server at 185.80.53[.]210.

Final Words

Pcap from today's dairy can be found here.

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