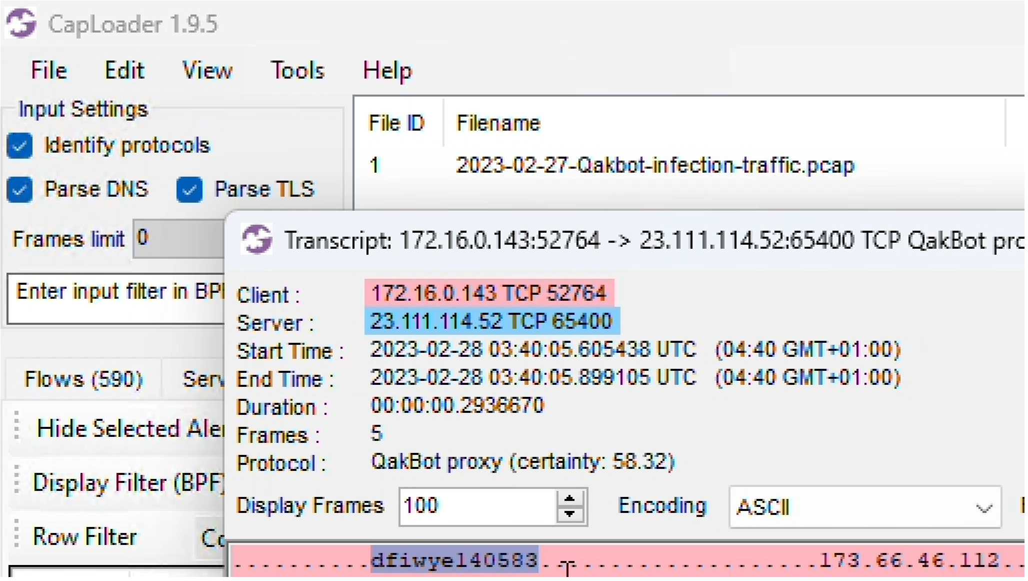
# QakBot C2 Traffic

netresec.com/

March 2, 2023



☑ Identify protocols

☑ Parse DNS ☑ Parse TLS

Frames limit 0

Enter input filter in BPF

| File ID | Filename |
|---|---|
| 1 | 2023-02-27-Qakbot-infection-traffic.pcap |

Transcript: 172.16.0.143:52764 -> 23.111.114.52:65400 TCP QakBot pro

Client : 172.16.0.143 TCP 52764
Server : 23.111.114.52 TCP 65400
Start Time : 2023-02-28 03:40:05.605438 UTC (04:40 GMT+01:00)
End Time : 2023-02-28 03:40:05.899105 UTC (04:40 GMT+01:00)
Duration : 00:00:00.2936670
Frames : 5
Protocol : QakBot proxy (certainty: 58.32)

Display Frames 100 Encoding ASCII

```
..........dfiwyel40583..................173.66.46.112..
```

Erik Hjelmvik

,

Thursday, 02 March 2023 12:43:00 (UTC/GMT)

In this video I analyze network traffic from a QakBot (QBot) infection in order to identify the Command-and-Control (C2) traffic. The analyzed PCAP file is from malware-traffic-analysis.net.

### IOC List

- C2 IP and port: 80.47.61.240:2222
- C2 IP and port: 185.80.53.210:443
- QakBot proxy IP and port: 23.111.114.52:65400
- JA3: 72a589da586844d7f0818ce684948eea
- JA3S: ec74a5c51106f0419184d0dd08fb05bc
- JA3S: fd4bc6cea4877646ccd62f0792ec0b62
- meieou.info X.509 cert hash: 9de2a1c39fbe1952221c4b78b8d21dc3afe53a3e
- meieou.info X.509 cert Subject OU: Hoahud Duhcuv Dampvafrog
- meieou.info X.509 cert Issuer O: Qdf Wah Uotvzke LLC.
- gifts.com X.509 cert hash: 0c7a37f55a0b0961c96412562dd0cf0b0b867d37
- HTML Body Hash: 22e5446e82b3e46da34b5ebce6de5751664fb867

- HTML Title: Welcome to CentOS

**Links**

For more analysis of QakBot network traffic, check out my Hunting for C2 Traffic video.

Posted by Erik Hjelmvik on Thursday, 02 March 2023 12:43:00 (UTC/GMT)

Tags: #QakBot #QBot #C2 #Video #malware-traffic-analysis.net #ThreatFox #ec74a5c51106f0419184d0dd08fb05bc #fd4bc6cea4877646ccd62f0792ec0b62 #CapLoader #NetworkMiner

## Recent Posts

» QakBot C2 Traffic

» TLS Redirection and Dynamic Decryption Bypass in PolarProxy

» How to Identify IcedID Network Traffic

» CapLoader 1.9.5 Alerts on Malicious Traffic

» Online Network Forensics Class

» IEC-104 File Transfer Extraction

» NetworkMiner 2.8 Released

» NetworkMiner in FLARE VM

## Blog Archive

» 2023 Blog Posts

» 2022 Blog Posts

» 2021 Blog Posts

» 2020 Blog Posts

» 2019 Blog Posts

» 2018 Blog Posts

» 2017 Blog Posts

» 2016 Blog Posts

» 2015 Blog Posts

» 2014 Blog Posts

» 2013 Blog Posts

» 2012 Blog Posts

» 2011 Blog Posts

List all blog posts

## News Feeds

» Google News

» FeedBurner

» RSS Feed

NETRESEC on Mastodon: @netresec@infosec.exchange

NETRESEC on Twitter: @netresec