QakBot C2 Traffic

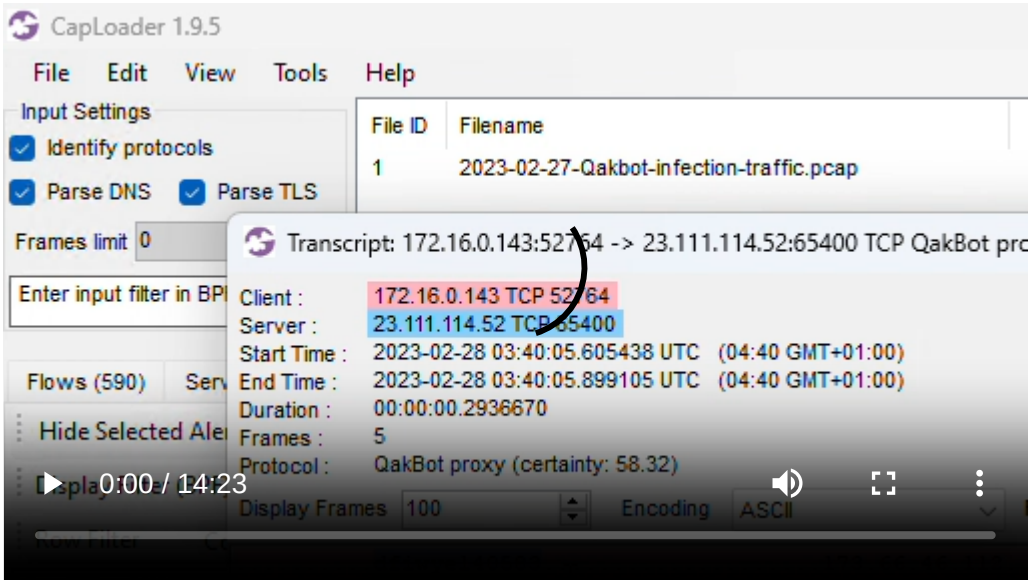
By Erik Hjelmvik

Published: 2023-03-02 · Archived: 2026-04-05 18:52:39 UTC

,

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

- QakBot PCAP download (malware-traffic-analysis.net)
- 80.47.61.240 (VirusTotal)
- 80.47.61.240:2222 (ThreatFox)
- 80.47.61.240 (Feodo Tracker)
- 80.47.61.240 (Censys)
- 185.80.53.210 (Censys)

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

Short URL: https://netresec.com/?b=233eaa1
