

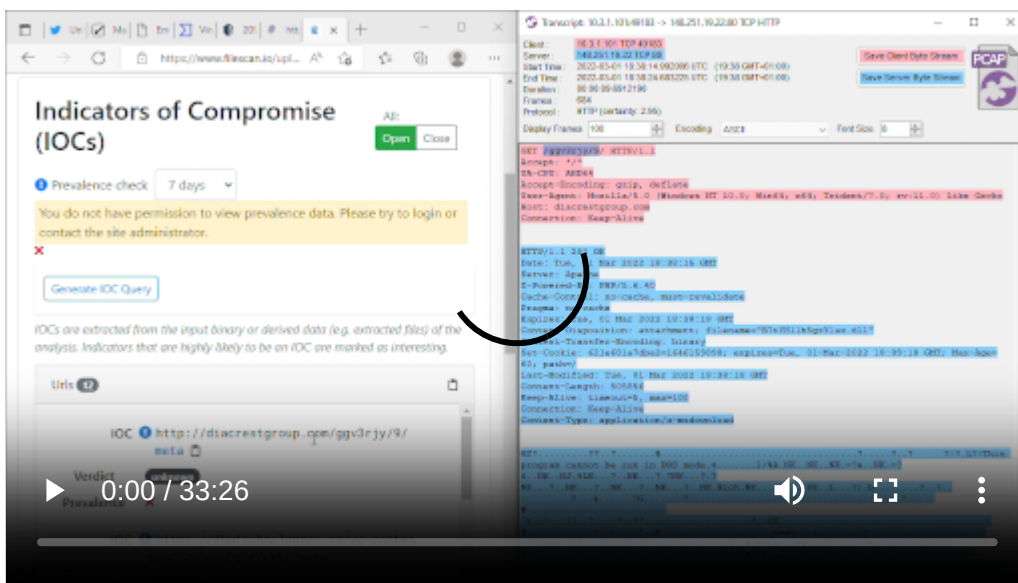
Emotet C2 and Spam Traffic Video

By Erik Hjelmvik

Published: 2022-05-09 · Archived: 2026-04-05 16:09:44 UTC

Monday, 09 May 2022 06:50:00 (UTC/GMT)

This video covers a life cycle of an Emotet infection, including initial infection, command-and-control traffic, and spambot activity sending emails with malicious spreadsheet attachments to infect new victims.



The video was recorded in a [Windows Sandbox](#) in order to avoid accidentally infecting my Windows PC with malware.

Initial Infection

Palo Alto's Unit 42 sent out a [tweet](#) with screenshots and IOCs from an Emotet infection in early March. A follow-up tweet by [Brad Duncan](#) linked to a PCAP file containing [network traffic from the infection](#) on Malware-Traffic-Analysis.net.

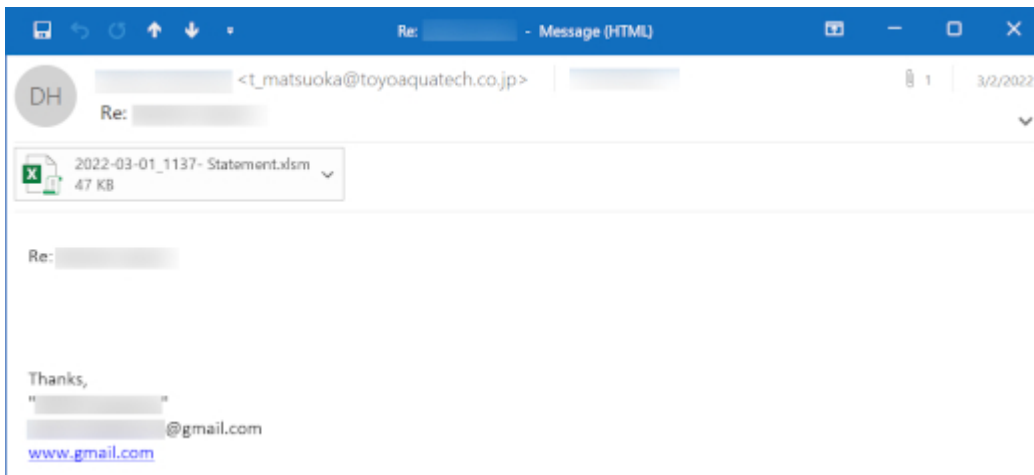


Image: Screenshot of original infection email [from Unit 42](#)

- Attachment MD5: 825e8ea8a9936eb9459344b941df741a

Emotet Download

The PCAP from Malware-Traffic-Analysis.net shows that the Excel spreadsheet attachment caused the download of a DLL file [classified as Emotet](#).

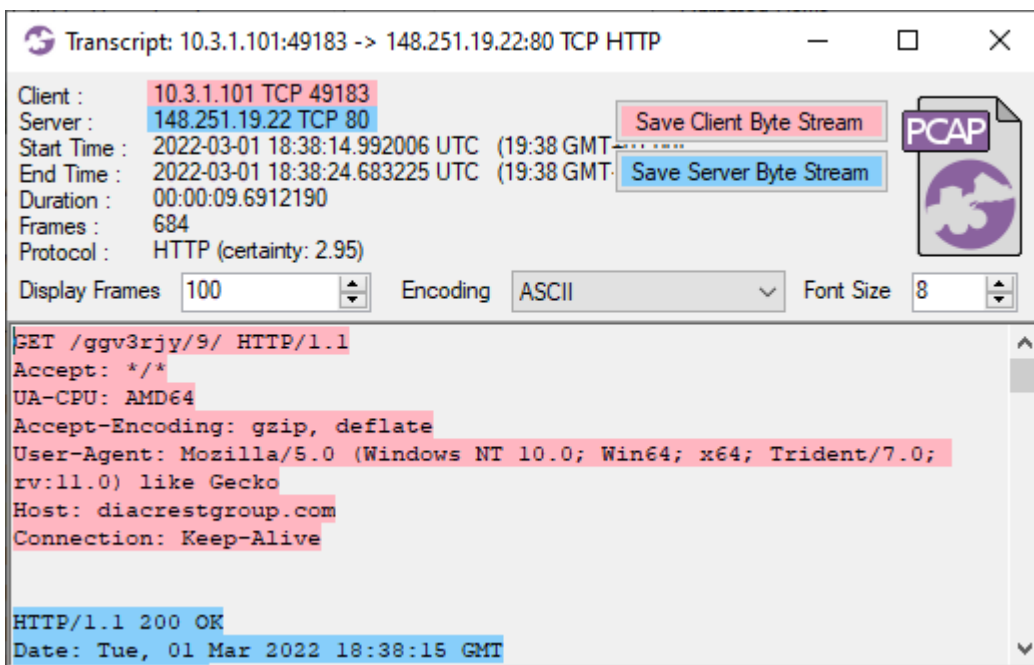


Image: [CapLoader](#) transcript of Emotet download

- DNS: diacrestgroup.com
- MD5: 99f59e6f3fa993ba594a3d7077cc884d

Emotet Command-and-Control

Just seconds after the Emotet DLL download completes the victim machine starts communicating with an IP address [classified as a botnet command-and-control server](#).

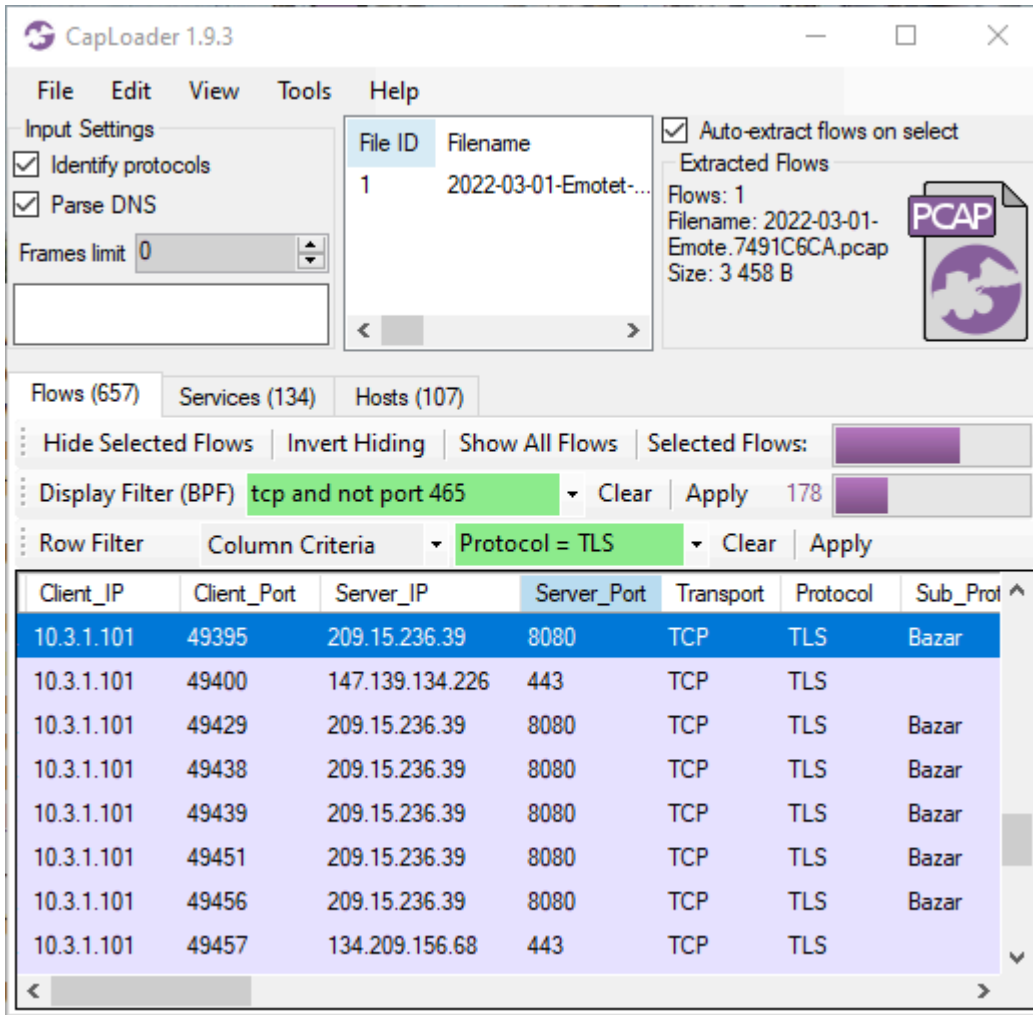


Image: Emotet C2 sessions in [CapLoader](#)

- C2 IP: 209.15.236.39
- C2 IP: 147.139.134.226
- C2 IP: 134.209.156.68
- JA3: 51c64c77e60f3980eea90869b68c58a8
- JA3S: ec74a5c51106f0419184d0dd08fb05bc
- JA3S: fd4bc6cea4877646ccd62f0792ec0b62

Emotet Spambot

The victim PC eventually started sending out spam emails. The spam bot used TLS encryption when possible, either through SMTPS (implicit TLS) or with help of STARTTLS (explicit TLS).

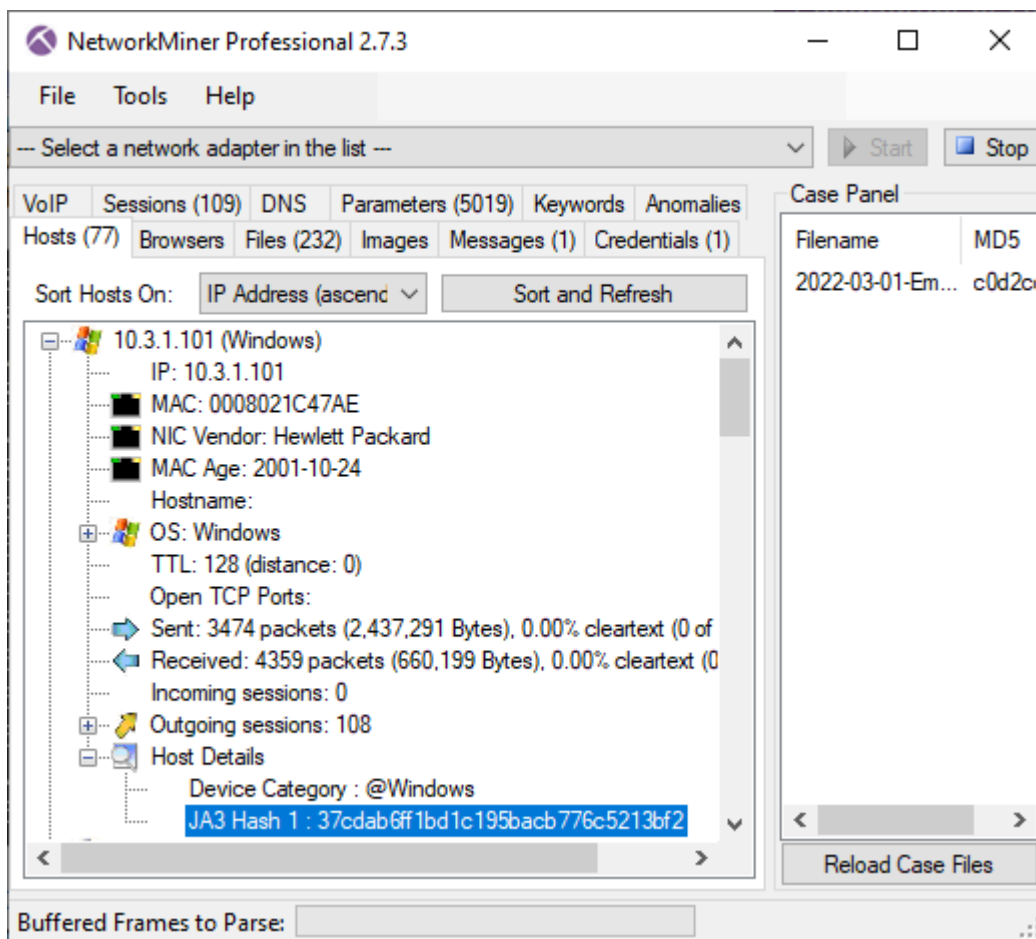


Image: Emotet spambot JA3 hash in [NetworkMiner Professional](#)

- SMTPS JA3: 37cdab6ff1bd1c195bacb776c5213bf2
- STARTTLS JA3: 37cdab6ff1bd1c195bacb776c5213bf2

Transmitted Spam

Below is a spam email sent from the victim PC without TLS encryption. The attached zip file contains a [malicious Excel spreadsheet](#), which is designed to infect new victims with Emotet.

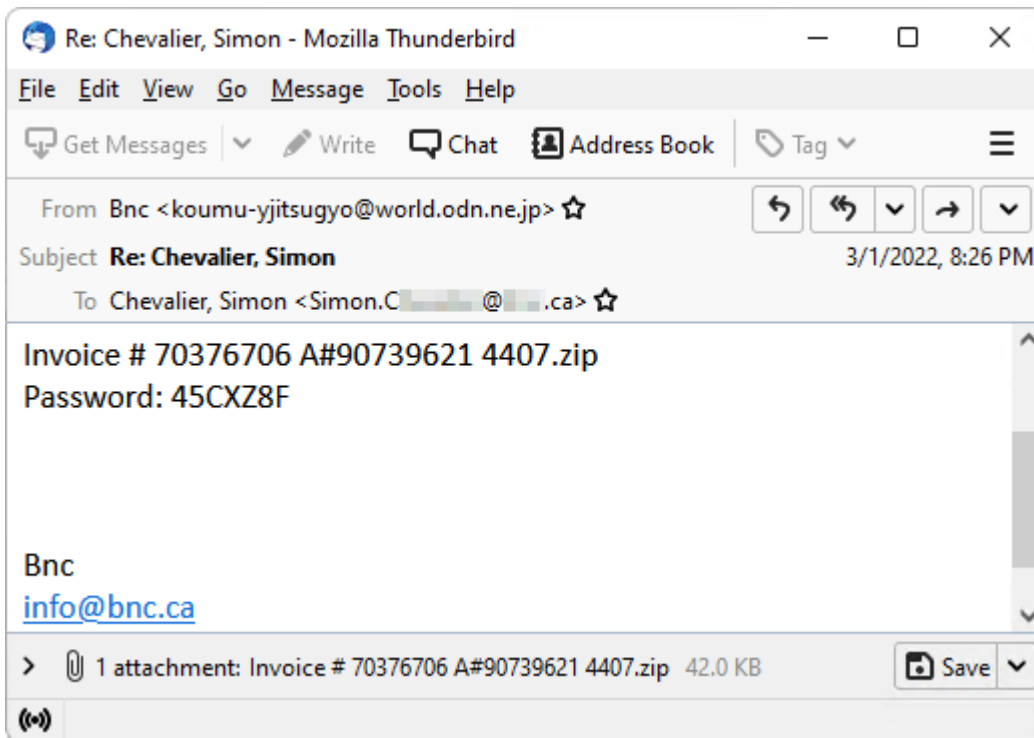


Image: Spam email extracted from Emotet PCAP with [NetworkMiner](#)

- .zip Attachment MD5: 5df1c719f5458035f6be2a071ea831db
- .xslm Attachment MD5: 79cb3df6c0b7ed6431db76f990c68b5b

Network Forensics Training

If you want to learn additional techniques for analyzing network traffic, then take a look at our upcoming [network forensic trainings](#).

Posted by Erik Hjelmvik on Monday, 09 May 2022 06:50:00 (UTC/GMT)

Tags: [#Emotet#C2#video#pcap#JA3#JA3S#51c64c77e60f3980eea90869b68c58a8](#)
[#ec74a5c51106f0419184d0dd08fb05bc#fd4bc6cea4877646ccd62f0792ec0b62#SMTP#SMTPS#Windows](#)
[Sandbox#videotutorial](#)

Short URL: <https://netresec.com/?b=225196a>