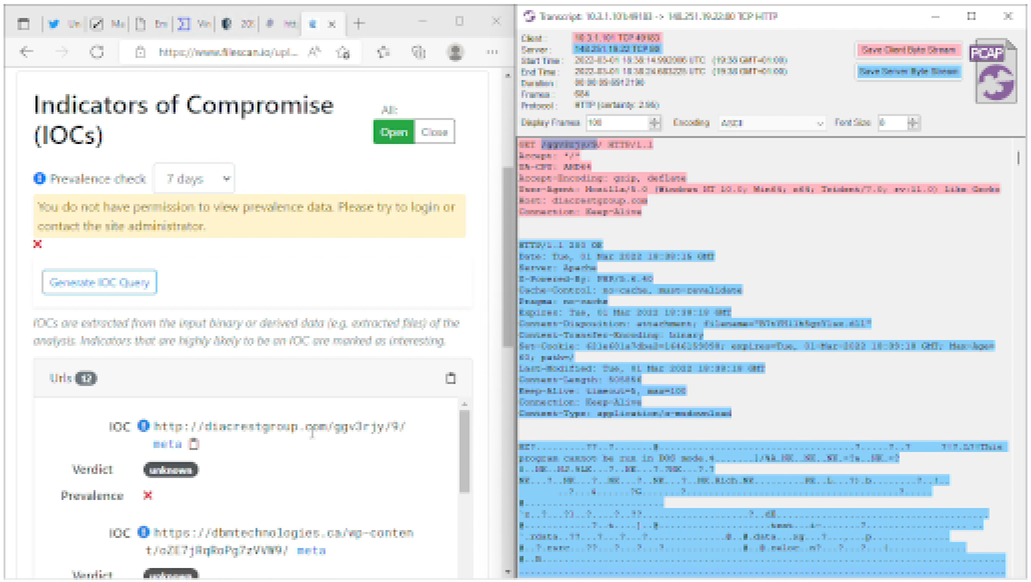
# Emotet C2 and Spam Traffic Video

netresec.com/

May 9, 2022



Indicators of Compromise (IOCs)

All: Open Close

Prevalence check 7 days

You do not have permission to view prevalence data. Please try to login or contact the site administrator.

Generate IOC Query

IOCs are extracted from the input binary or derived data (e.g. extracted files) of the analysis. Indicators that are highly likely to be an IOC are marked as interesting.

Urls 12

IOC http://diacrestgroup.com/ggv3rjy/9/ meta
Verdict unknown
Prevalence ✗

IOC https://dbmtechnologies.ca/wp-content/oZE7jRqRoPg7zVVW9/ meta
Verdict unknown

Transcript: 10.3.1.101:49183 -> 148.251.19.22:80 TCP HTTP

Client: 10.3.1.101 TCP 49183
Server: 148.251.19.22 TCP 80
Start Time: 2022-03-01 18:38:14.992066 UTC (19:38 GMT+01:00)
End Time: 2022-03-01 18:38:24.683225 UTC (19:38 GMT+01:00)
Duration: 00:00:09.6912190
Frames: 684
Protocol: HTTP (certainty: 2.66)
Display Frames 100 Encoding ASCII Font Size 8

```
GET /ggv3rjy/9/ HTTP/1.1
Accept: */*
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko
Host: diacrestgroup.com
Connection: Keep-Alive


HTTP/1.1 200 OK
Date: Tue, 01 Mar 2022 18:38:15 GMT
Server: Apache
X-Powered-By: PHP/5.6.40
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Expires: Tue, 01 Mar 2022 18:38:15 GMT
Content-Disposition: attachment; filename="[illegible].dll"
Content-Transfer-Encoding: binary
Set-Cookie: [illegible]; expires=Tue, 01-Mar-2022 18:39:15 GMT; Max-Age=60; path=/
Last-Modified: Tue, 01 Mar 2022 18:38:15 GMT
Content-Length: 505856
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/x-msdownload


MZ[illegible]This
program cannot be run in DOS mode.[illegible]
```

Erik Hjelmvik

,

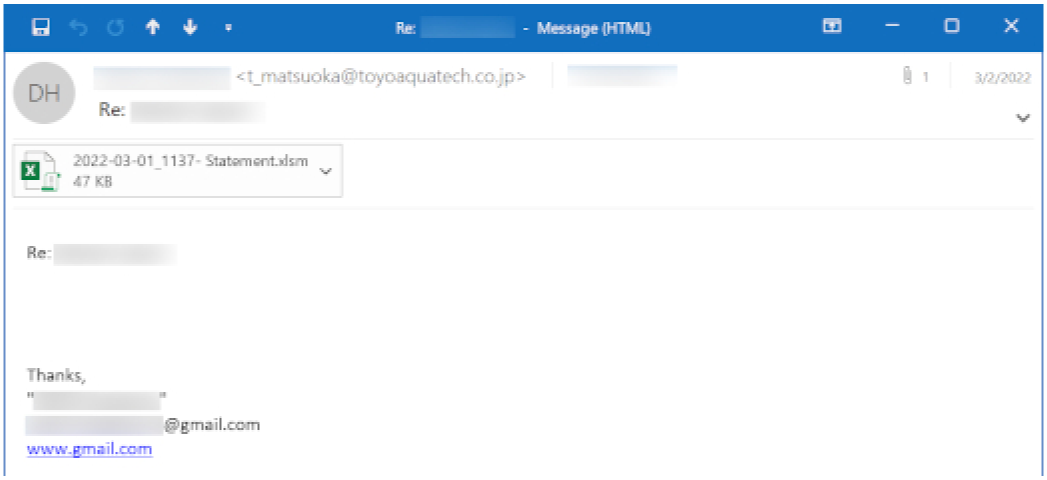
Monday, 09 May 2022 06:50:00 (UTC/GMT)

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.



DH [redacted] <t_matsuoka@toyoaquatech.co.jp> [redacted] 1 3/2/2022

Re: [redacted]

2022-03-01_1137- Statement.xlsm
47 KB

Re: [redacted]

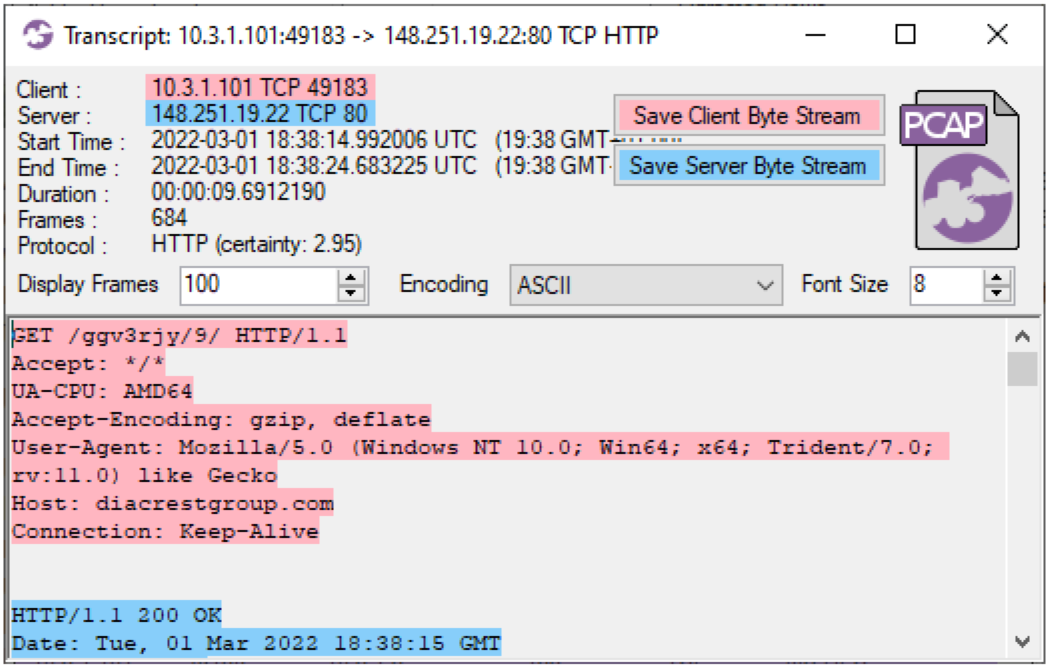
Thanks,
"[redacted]"
[redacted]@gmail.com
www.gmail.com

*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.



Client : 10.3.1.101 TCP 49183
Server : 148.251.19.22 TCP 80
Start Time : 2022-03-01 18:38:14.992006 UTC (19:38 GMT
End Time : 2022-03-01 18:38:24.683225 UTC (19:38 GMT
Duration : 00:00:09.6912190
Frames : 684
Protocol : HTTP (certainty: 2.95)
Display Frames 100 Encoding ASCII Font Size 8

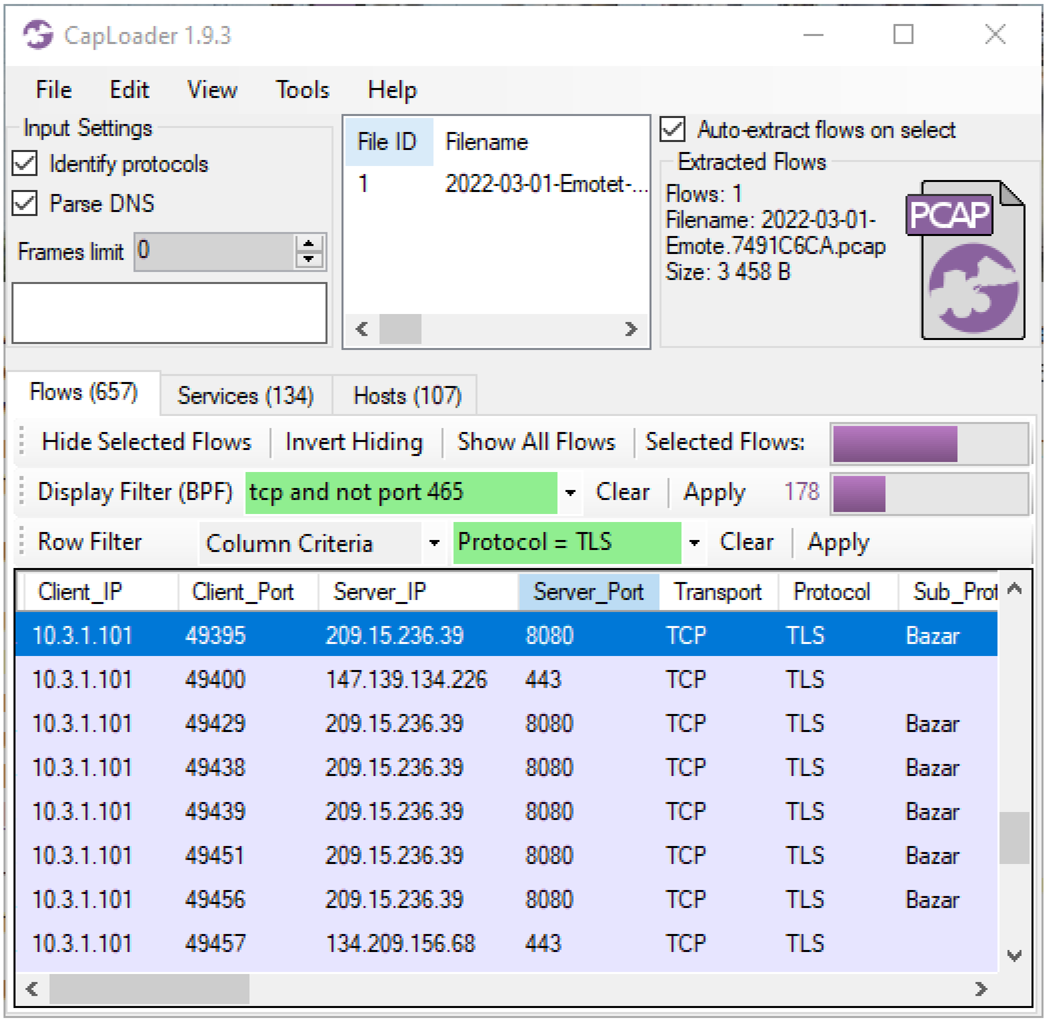
```
GET /ggv3rjy/9/ HTTP/1.1
Accept: */*
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0;
rv:11.0) like Gecko
Host: diacrestgroup.com
Connection: Keep-Alive


HTTP/1.1 200 OK
Date: Tue, 01 Mar 2022 18:38:15 GMT
```

*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.



☑ Identify protocols

☑ Parse DNS

Frames limit 0

| File ID | Filename |
|---|---|
| 1 | 2022-03-01-Emotet-... |

☑ Auto-extract flows on select

Flows: 1
Filename: 2022-03-01-Emote.7491C6CA.pcap
Size: 3 458 B

Display Filter (BPF) tcp and not port 465 — 178

Row Filter: Column Criteria — Protocol = TLS

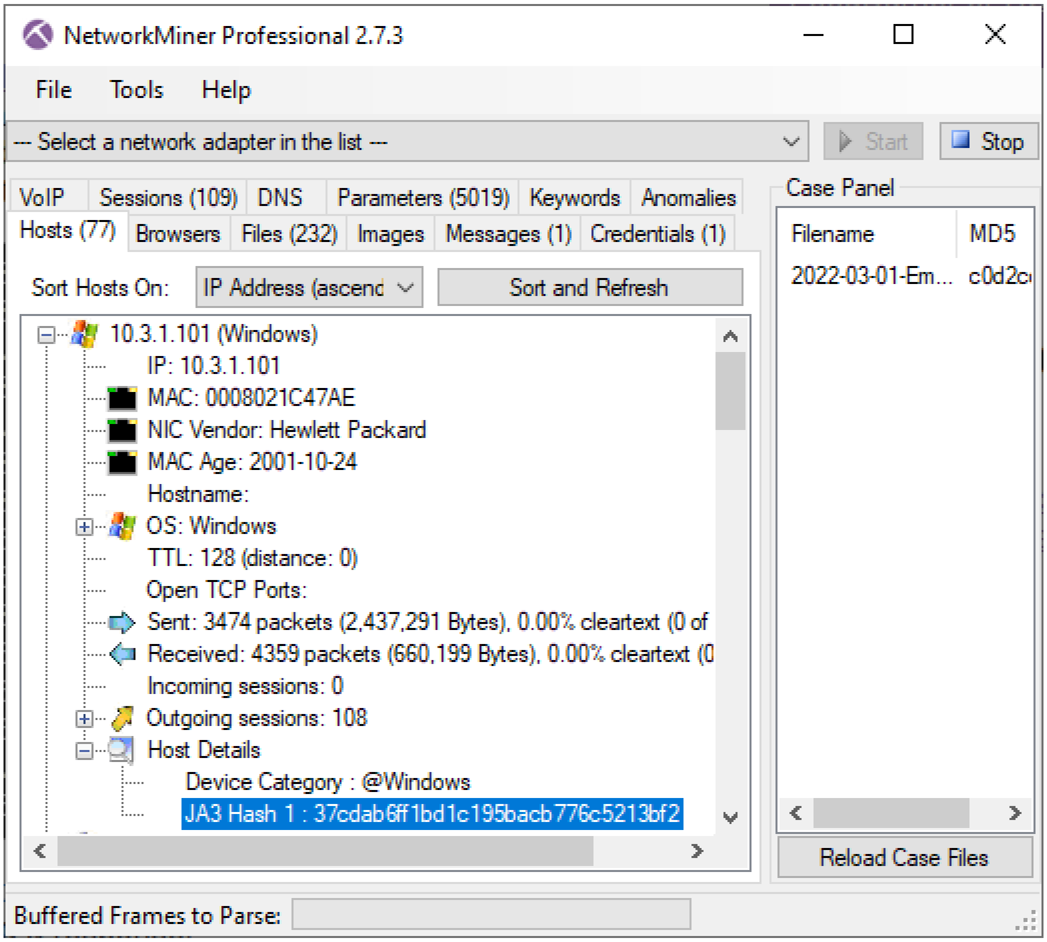
| Client_IP | Client_Port | Server_IP | Server_Port | Transport | Protocol | Sub_Prot |
|---|---|---|---|---|---|---|
| 10.3.1.101 | 49395 | 209.15.236.39 | 8080 | TCP | TLS | Bazar |
| 10.3.1.101 | 49400 | 147.139.134.226 | 443 | TCP | TLS | |
| 10.3.1.101 | 49429 | 209.15.236.39 | 8080 | TCP | TLS | Bazar |
| 10.3.1.101 | 49438 | 209.15.236.39 | 8080 | TCP | TLS | Bazar |
| 10.3.1.101 | 49439 | 209.15.236.39 | 8080 | TCP | TLS | Bazar |
| 10.3.1.101 | 49451 | 209.15.236.39 | 8080 | TCP | TLS | Bazar |
| 10.3.1.101 | 49456 | 209.15.236.39 | 8080 | TCP | TLS | Bazar |
| 10.3.1.101 | 49457 | 134.209.156.68 | 443 | TCP | TLS | |

*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).



Sort Hosts On: IP Address (ascend

```
10.3.1.101 (Windows)
    IP: 10.3.1.101
    MAC: 0008021C47AE
    NIC Vendor: Hewlett Packard
    MAC Age: 2001-10-24
    Hostname:
    OS: Windows
    TTL: 128 (distance: 0)
    Open TCP Ports:
    Sent: 3474 packets (2,437,291 Bytes), 0.00% cleartext (0 of
    Received: 4359 packets (660,199 Bytes), 0.00% cleartext (0
    Incoming sessions: 0
    Outgoing sessions: 108
    Host Details
        Device Category : @Windows
        JA3 Hash 1 : 37cdab6ff1bd1c195bacb776c5213bf2
```

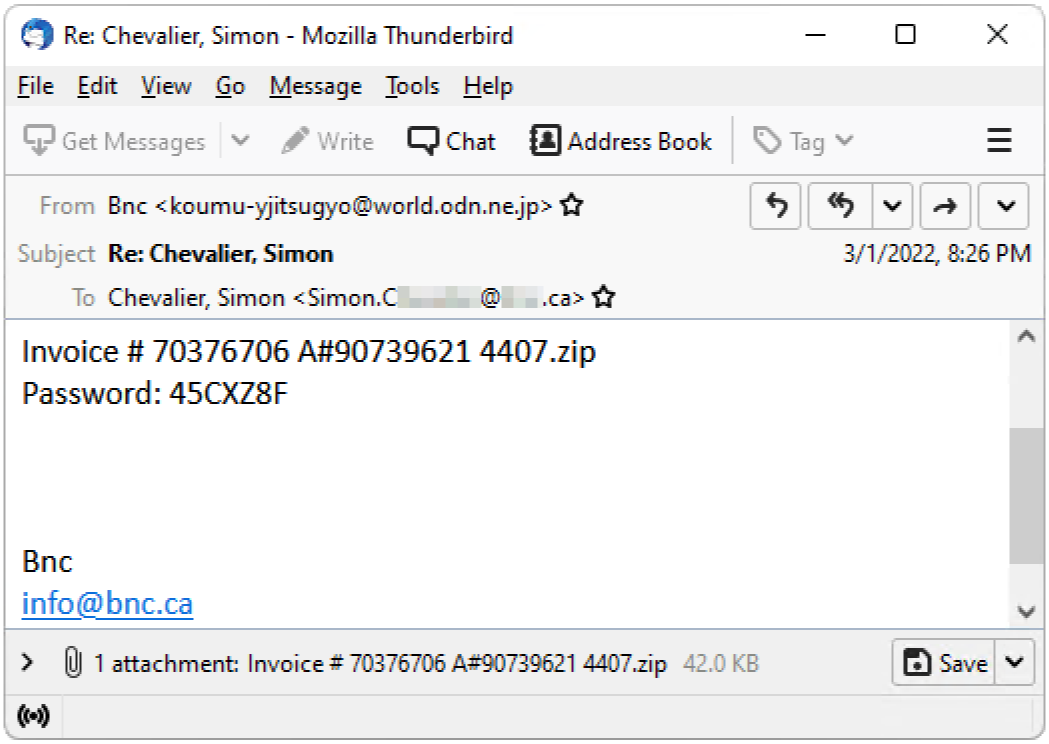
| Filename | MD5 |
|---|---|
| 2022-03-01-Em... | c0d2c |

*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.


Re: Chevalier, Simon - Mozilla Thunderbird
File Edit View Go Message Tools Help
Get Messages
Write
Chat
Address Book
Tag
Save

From Bnc <koumu-yjitsugyo@world.odn.ne.jp>

Subject **Re: Chevalier, Simon** 3/1/2022, 8:26 PM

To Chevalier, Simon <Simon.C[redacted]@[redacted].ca>

Invoice # 70376706 A#90739621 4407.zip
Password: 45CXZ8F

Bnc
info@bnc.ca

1 attachment: Invoice # 70376706 A#90739621 4407.zip 42.0 KB

*Image: Spam email extracted from Emotet PCAP with NetworkMiner*

- .zip Attachment MD5: 5df1c719f5458035f6be2a071ea831db
- .xlsm 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 #SMTP #SMTPS #Windows Sandbox

## Recent Posts

» Real-time PCAP-over-IP in Wireshark

» Emotet C2 and Spam Traffic Video

» Industroyer2 IEC-104 Analysis

» NetworkMiner 2.7.3 Released

» PolarProxy in Windows Sandbox

» PolarProxy 0.9 Released

## Blog Archive

» 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

## NETRESEC on Twitter

Follow @netresec on twitter:
» twitter.com/netresec