[CA] Trojan Bancking (Network Analysis)

Author

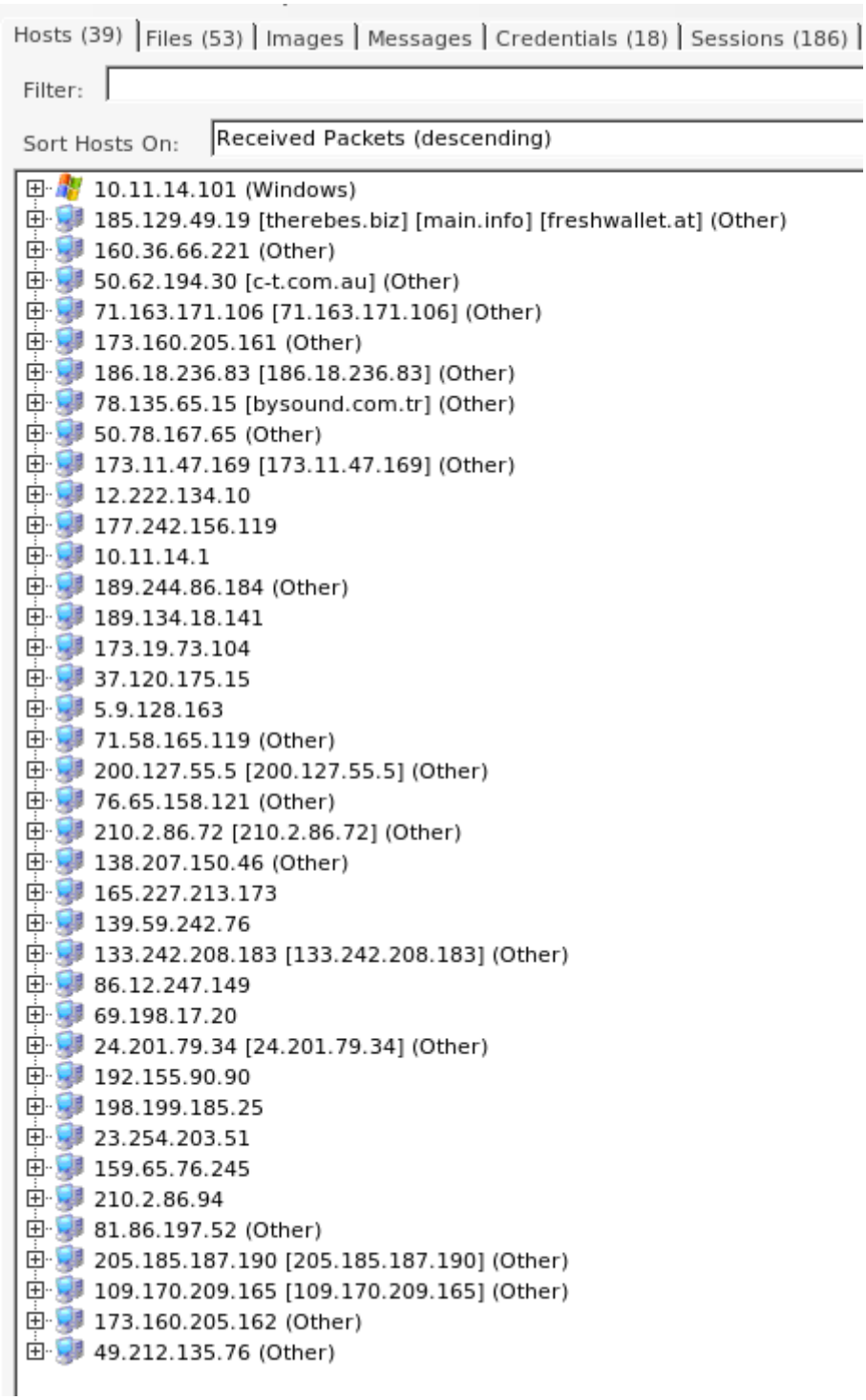
- **Name**: Steve Djumo Kouekam
- **Matricule**: ICT 2022 27 55
- **Email**: djumokouekam.steve@ictuniversity.edu.cm
- **Program**: Computer Science -- ICT University (Spring 2023)

Questions

Step 1: Seting up the tools for investigation

Ater donwloading `2018-11-14-Emotet-infection-with-IcedID-banking-Trojan.pcap` and `Network Miner for linux`, we lauch the tool and open the said `.pcap` file.

Step 2: Finding the Anomalies in the traffic



First and foremost, after ordering the **host by traffic amount**, it appear that the source PC had the most packets exchange with **10.11.14.101**, **185.129.49.19**, and **160.36.66.221** respectively. Since **10.11.14.101** account for twice the traffic of the second and third host combine, it is a good starting point to know what going on.

Hosts (39) | Files (53) | Images | Messages | Credentials (18) | Sessions (186) | DNS (2

Filter:

Sort Hosts On: Received Packets (descending)

- 10.11.14.101 (Windows)
  - IP: 10.11.14.101
  - MAC: 0008021C47AE
  - NIC Vendor: Hewlett Packard
  - MAC Age: 2001-10-24
  - Hostname:
  - OS: Windows
  - TTL: 128 (distance: 0)
  - Open TCP Ports:
  - Sent: 2461 packets (173,944 Bytes), 0.00 % cleartext (0 of 0 Bytes)
  - Received: 4056 packets (3,347,904 Bytes), 0.00 % cleartext (0 of 0 Bytes)
  - Incoming sessions: 0
  - Outgoing sessions: 97
  - Host Details
- 185.129.49.19 [therebes.biz] [main.info] [freshwallet.at] (Other)
  - IP: 185.129.49.19
  - MAC: 20E52AB693F1
  - NIC Vendor: NETGEAR
  - MAC Age: 2012-06-06
  - Hostname: therebes.biz, main.info, freshwallet.at
  - OS: Other
  - TTL: 128 (distance: 0)
  - Open TCP Ports: 443 (Ssl) 80 (Http)
  - Sent: 1626 packets (821,707 Bytes), 0.00 % cleartext (0 of 0 Bytes)
  - Received: 1010 packets (74,130 Bytes), 0.00 % cleartext (0 of 0 Bytes)
  - Incoming sessions: 48
  - Outgoing sessions: 0
  - Host Details
- 160.36.66.221 (Other)
  - IP: 160.36.66.221
  - MAC: 20E52AB693F1
  - NIC Vendor: NETGEAR
  - MAC Age: 2012-06-06
  - Hostname:
  - OS: Other
  - TTL: 128 (distance: 0)
  - Open TCP Ports: 990
  - Sent: 1272 packets (1,399,990 Bytes), 0.00 % cleartext (0 of 0 Bytes)
  - Received: 568 packets (35,399 Bytes), 0.00 % cleartext (0 of 0 Bytes)
  - Incoming sessions: 14
  - Outgoing sessions: 0
- 50.62.194.30 [c-t.com.au] (Other)
- 71.163.171.106 [71.163.171.106] (Other)
- 173.160.205.161 (Other)
- 186.18.236.83 [186.18.236.83] (Other)
- 78.135.65.15 [bysound.com.tr] (Other)
- 50.78.167.65 (Other)
- 173.11.47.169 [173.11.47.169] (Other)
- 12.222.134.10
- 177.242.156.119
- 10.11.14.1
- 189.244.86.184 (Other)
- 189.134.18.141
- 173.19.73.104

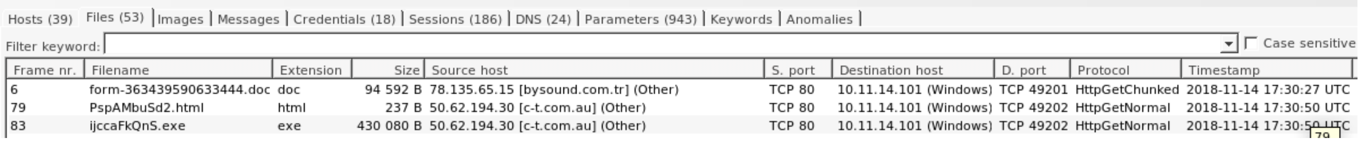
Furthermore, while investigating the exchange during the attack, the notice 2 uncommon file type: `.doc` and `.exe`. Normally, the traffic should be mostly made of `.htm` and `.cert` file. Thus, we investigate furhter the document and executable received

Hosts (39) | Files (53) | Images | Messages | Credentials (18) | Sessions (186) | DNS (24) | Parameters (943) | Keywords | Anomalies

Filter keyword:

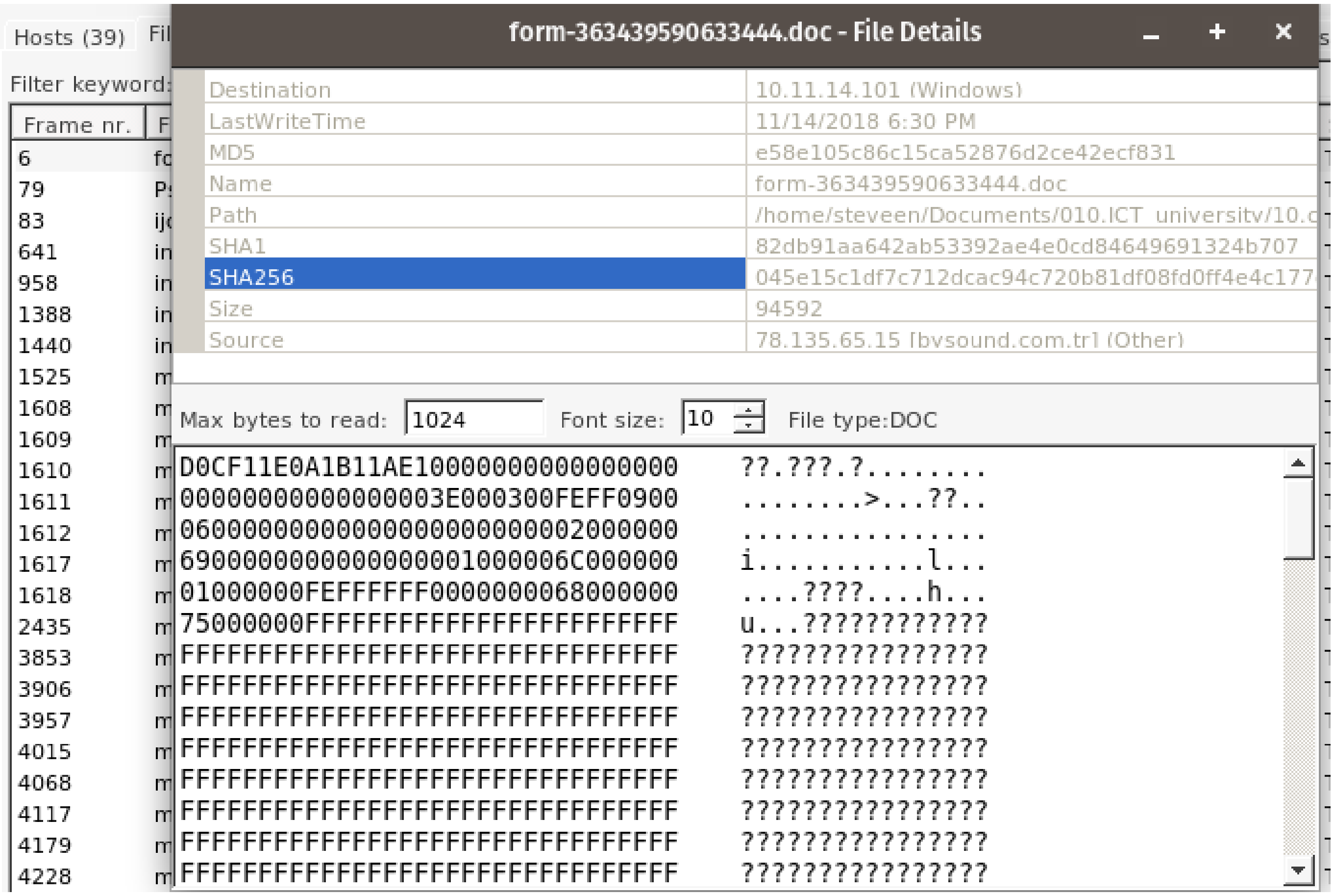
Frame nr.	Filename	Extension	Size	Source host	S. port	Destination host
6	form-363439590633444.doc	doc	94 592 B	78.135.65.15 [bysound.com.tr] (Other)	TCP 80	10.11.14.101 (Windows)
79	PspAMbuSd2.html	html	237 B	50.62.194.30 [c-t.com.au] (Other)	TCP 80	10.11.14.101 (Windows)
83	ijccaFkQnS.exe	exe	430 080 B	50.62.194.30 [c-t.com.au] (Other)	TCP 80	10.11.14.101 (Windows)
641	index.html	html	152 932 B	186.18.236.83 [186.18.236.83] (Other)	TCP 8080	10.11.14.101 (Windows)
958	index.html	html	296 228 B	71.163.171.106 [71.163.171.106] (Other)	TCP 80	10.11.14.101 (Windows)
1388	index.html 1608	html	548 B	24.201.79.34 [24.201.79.34] (Other)	TCP 8080	10.11.14.101 (Windows)
1440	index.html	html	552 B	133.242.208.183 [133.242.208.183] (Other)	TCP 8080	10.11.14.101 (Windows)
1525	main.info.cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshw...	TCP 443	10.11.14.101 (Windows)
1608	main.info[1].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshw...	TCP 443	10.11.14.101 (Windows)
1609	main.info[2].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshw...	TCP 443	10.11.14.101 (Windows)
1610	main.info[3].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshw...	TCP 443	10.11.14.101 (Windows)
1611	main.info[4].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshw...	TCP 443	10.11.14.101 (Windows)
1612	main.info[5].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshw...	TCP 443	10.11.14.101 (Windows)
1617	main.info[6].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshw...	TCP 443	10.11.14.101 (Windows)
1618	main.info[7].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshw...	TCP 443	10.11.14.101 (Windows)
2435	main.info[8].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshw...	TCP 443	10.11.14.101 (Windows)
3853	main.info[9].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshw...	TCP 443	10.11.14.101 (Windows)
3906	main.info[10].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshw...	TCP 443	10.11.14.101 (Windows)
3957	main.info[11].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshw...	TCP 443	10.11.14.101 (Windows)
4015	main.info[12].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshw...	TCP 443	10.11.14.101 (Windows)
4068	main.info[13].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshw...	TCP 443	10.11.14.101 (Windows)
4117	main.info[14].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshw...	TCP 443	10.11.14.101 (Windows)
4179	main.info[15].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshw...	TCP 443	10.11.14.101 (Windows)
4228	main.info[16].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshw...	TCP 443	10.11.14.101 (Windows)
4279	main.info[17].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshw...	TCP 443	10.11.14.101 (Windows)
4336	main.info[18].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshw...	TCP 443	10.11.14.101 (Windows)
4383	main.info[19].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshw...	TCP 443	10.11.14.101 (Windows)
4432	main.info[20].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshw...	TCP 443	10.11.14.101 (Windows)
4527	main.info[21].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshw...	TCP 443	10.11.14.101 (Windows)
4576	main.info[22].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshw...	TCP 443	10.11.14.101 (Windows)
4627	main.info[23].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshw...	TCP 443	10.11.14.101 (Windows)
4687	main.info[24].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshw...	TCP 443	10.11.14.101 (Windows)
4738	main.info[25].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshw...	TCP 443	10.11.14.101 (Windows)
4787	main.info[26].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshw...	TCP 443	10.11.14.101 (Windows)
4865	main.info[27].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshw...	TCP 443	10.11.14.101 (Windows)
4914	main.info[28].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshw...	TCP 443	10.11.14.101 (Windows)
4965	main.info[29].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshw...	TCP 443	10.11.14.101 (Windows)
5018	main.info[30].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshw...	TCP 443	10.11.14.101 (Windows)
5069	main.info[31].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshw...	TCP 443	10.11.14.101 (Windows)
5118	main.info[32].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshw...	TCP 443	10.11.14.101 (Windows)
5180	main.info[33].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshw...	TCP 443	10.11.14.101 (Windows)
5229	main.info[34].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshw...	TCP 443	10.11.14.101 (Windows)
5280	main.info[35].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshw...	TCP 443	10.11.14.101 (Windows)
5379	main.info[36].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshw...	TCP 443	10.11.14.101 (Windows)
5439	main.info[37].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshw...	TCP 443	10.11.14.101 (Windows)
5484	main.info[38].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshw...	TCP 443	10.11.14.101 (Windows)
5546	main.info[39].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshw...	TCP 443	10.11.14.101 (Windows)
5595	main.info[40].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshw...	TCP 443	10.11.14.101 (Windows)
5646	main.info[41].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshw...	TCP 443	10.11.14.101 (Windows)
5879	main.info[42].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshw...	TCP 443	10.11.14.101 (Windows)
5930	main.info[43].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshw...	TCP 443	10.11.14.101 (Windows)
5979	main.info[44].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshw...	TCP 443	10.11.14.101 (Windows)
6517	main.info[45].cer	cer	770 B	185.129.49.19 [therebes.biz] [main.info] [freshw...	TCP 443	10.11.14.101 (Windows)

Since the document file was download before (17:30:27) the executable (17:30:50) of the same, we investigate that angle first.



Frame nr.	Filename	Extension	Size	Source host	S. port	Destination host	D. port	Protocol	Timestamp
6	form-363439590633444.doc	doc	94 592 B	78.135.65.15 [bysound.com.tr] (Other)	TCP 80	10.11.14.101 (Windows)	TCP 49201	HttpGetChunked	2018-11-14 17:30:27 UTC
79	PspAMbuSd2.html	html	237 B	50.62.194.30 [c-t.com.au] (Other)	TCP 80	10.11.14.101 (Windows)	TCP 49202	HttpGetNormal	2018-11-14 17:30:50 UTC
83	ijccaFkQnS.exe	exe	430 080 B	50.62.194.30 [c-t.com.au] (Other)	TCP 80	10.11.14.101 (Windows)	TCP 49202	HttpGetNormal	2018-11-14 17:30:50 UTC

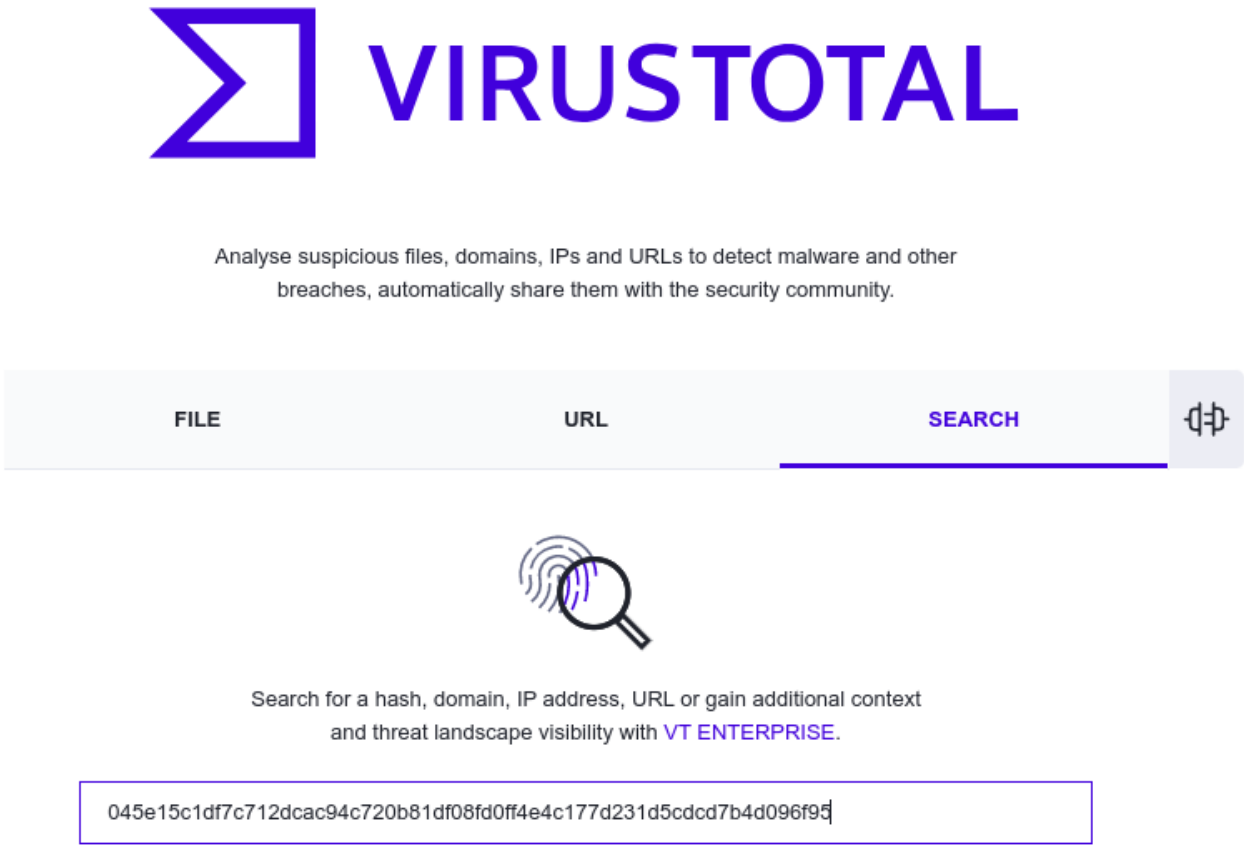
Looking at the document details, we can extract the **SHA256** signature to analyze on the **VirusTotal**.



Destination	10.11.14.101 (Windows)
LastWriteTime	11/14/2018 6:30 PM
MD5	e58e105c86c15ca52876d2ce42ecf831
Name	form-363439590633444.doc
Path	/home/steveen/Documents/010.ICT_university/10.c
SHA1	82db91aa642ab53392ae4e0cd84649691324b707
SHA256	045e15c1df7c712dcac94c720b81df08fd0ff4e4c177
Size	94592
Source	78.135.65.15 [bysound.com.tr] (Other)

Max bytes to read: 1024 Font size: 10 File type:DOC

```
D0CF11E0A1B11AE1000000000000000000    ??.???.?........
00000000000000003E000300FEFF0900    ........>...??..
06000000000000000000000002000000    ................
69000000000000000010000006C000000    i..........l...
01000000FEFFFFFF0000000068000000    ....????....h...
75000000FFFFFFFFFFFFFFFFFFFFFFFF    u...????????????
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF    ????????????????
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF    ????????????????
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF    ????????????????
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF    ????????????????
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF    ????????????????
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF    ????????????????
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF    ????????????????
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF    ????????????????
```



Upon analysis by **VirusTotal**, it become clear that the document `form-363439590633444.doc` is a trojan that execute `VBA` to possibly open the door to other more dangerous/malicious program (according to definition of trojan program).

45 / 63

Community Score

45 security vendors and 1 sandbox flagged this file as malicious

045e15c1df7c712dcac94c720b81df08fd0ff4e4c177d231d5cdcd7b4d096f95

form-363439590633444.doc

doc | run-file | runtime-modules | macros | attachment | direct-cpu-clock-access

92.38 KB
Size

2022-12-14 04:36:55 UTC
4 months ago

DOC

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY 10

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.w97m/pederr

Threat categories trojan | downloader

Family labels w97m | pederr | o97m

Security vendors' analysis

Do you want to automate checks?

Acronis (Static ML)	Suspicious	Ad-Aware	VB:Trojan.VBA.Agent.ABC
AhnLab-V3	VBA/Downloader	ALYac	Trojan.Downloader.VBA.gen
Antiy-AVL	Trojan/MSOffice.Pederr.gen	Arcabit	VB:Trojan.VBA.Agent.ABC
Avast	Script:SNH-gen [Drp]	AVG	Script:SNH-gen [Drp]
Avira (no cloud)	W97M/Agent.1231418	Baidu	VBA.Trojan-Downloader.Agent.dqd
BitDefender	VB:Trojan.VBA.Agent.ABC	ClamAV	Doc.Malware.Generic-6749861-0
Comodo	TrojWare.VBS.TrojanDownloader.Agent....	Cynet	Malicious (score: 99)
Cyren	W97M/Downldr.gen	DrWeb	W97M.DownLoader.3111
Elastic	Malicious (high Confidence)	Emsisoft	Trojan-Downloader.Macro.Generic.J (A)

The details section confirm even more our basic analysis.

45 / 63

Community Score

45 security vendors and 1 sandbox flagged this file as malicious

045e15c1df7c712dcac94c720b81df08fd0ff4e4c177d231d5cdcd7b4d096f95

form-363439590633444.doc

doc | run-file | runtime-modules | macros | attachment | direct-cpu-clock-access

92.38 KB
Size

2022-12-14 04:36:55 UTC
4 months ago

DOC

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY 10

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Basic properties

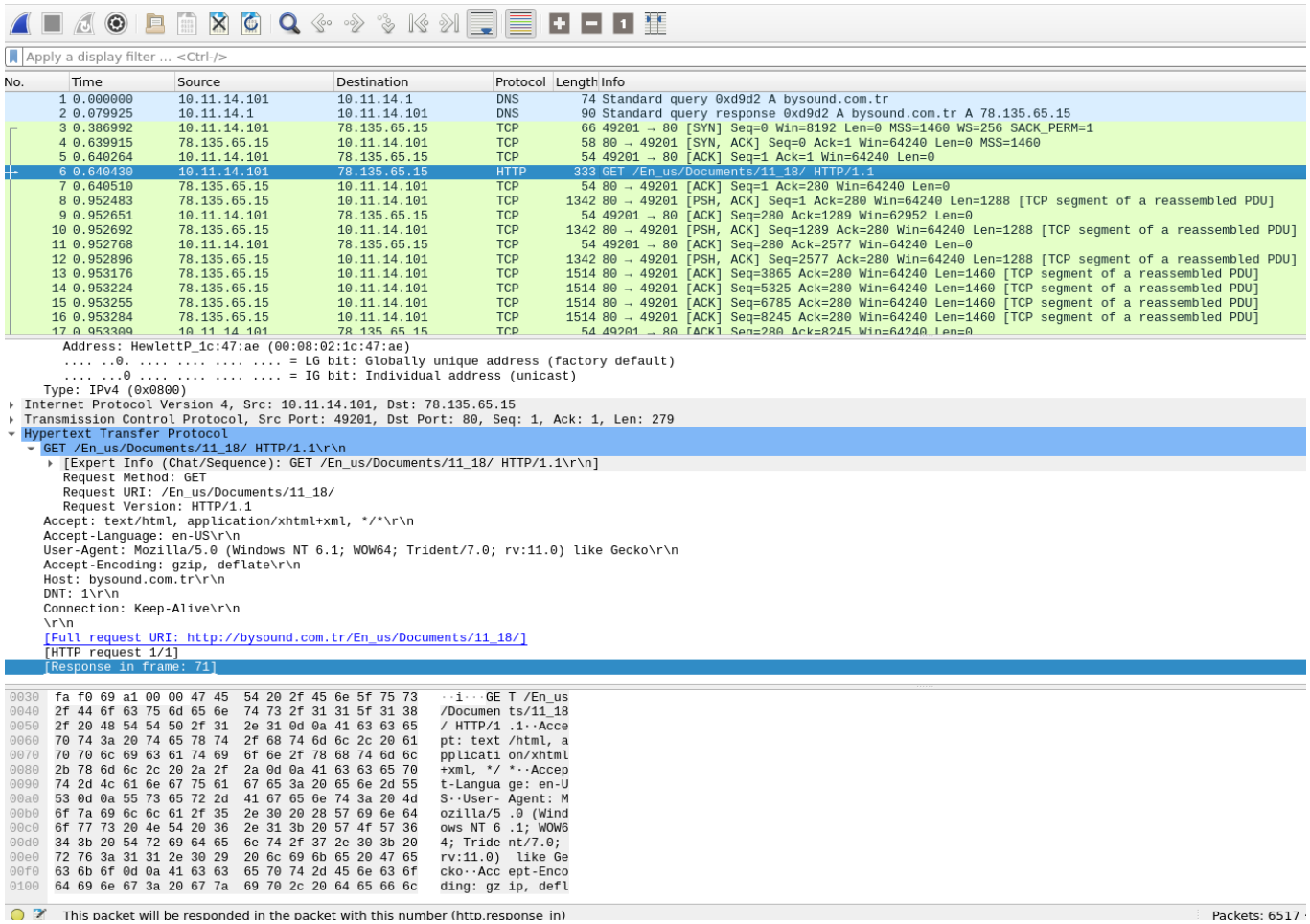
MD5	e58e105c86c15ca52876d2ce42ecf831
SHA-1	82db91aa642ab53392ae4e0cd84649691324b707
SHA-256	045e15c1df7c712dcac94c720b81df08fd0ff4e4c177d231d5cdcd7b4d096f95
Vhash	ac2f9682900bb154a0b4b2164427cd1a
SSDEEP	1536:YZuocn1kp59gxBK85fBt+a9XV6r2EBDxoRwBnRDhYxjhUx5xfxThoxtBqBYRM6UW:441k/W486FDxoRwBnRDhYxjhUx5xfxT6
TLSH	T125935B52B285ED5BFAA040305D87DBFA762DBC0E6D0A421F324C7FAEBF766208516741
File type	MS Word Document
Magic	CDF V2 Document, Little Endian, Os: Windows, Version 6.1, Code page: 1252, Author: Levi, Template: Normal.dotm, Revision Number: 1, Name of Creating Application: Microsoft Office Word, Create Time/Date: Tue Nov 13 12:45:00 2018, Last Saved Time/Date: Tue Nov 13 12:45:00 2018, Number of Pages: 1, Number of Words: 2, Number of Characters: 13, Security: 0
TrID	Microsoft Word document (52.6%) | Microsoft Word document (old ver.) (33.3%) | Generic OLE2 / Multistream Compound (14%)
File size	92.38 KB (94592 bytes)

History

Creation Time	2018-11-14 12:45:00 UTC
First Submission	2018-11-14 17:04:27 UTC
Last Submission	2022-12-13 18:47:16 UTC
Last Analysis	2022-12-14 04:36:55 UTC

Names

For details information on the how, the analysis with *Wireshark* of the initial **GET request** from **10.11.14.101** to server **78.135.65.15** is as follow.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.11.14.101	10.11.14.1	DNS	74	Standard query 0xd9d2 A bysound.com.tr
2	0.079925	10.11.14.1	10.11.14.101	DNS	90	Standard query response 0xd9d2 A bysound.com.tr A 78.135.65.15
3	0.386992	10.11.14.101	78.135.65.15	TCP	66	49201 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
4	0.639915	78.135.65.15	10.11.14.101	TCP	58	80 → 49201 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
5	0.640264	10.11.14.101	78.135.65.15	TCP	54	49201 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
6	0.640430	10.11.14.101	78.135.65.15	HTTP	333	GET /En_us/Documents/11_18/ HTTP/1.1
7	0.640510	78.135.65.15	10.11.14.101	TCP	54	80 → 49201 [ACK] Seq=1 Ack=280 Win=64240 Len=0
8	0.952483	78.135.65.15	10.11.14.101	TCP	1342	80 → 49201 [PSH, ACK] Seq=1 Ack=280 Win=64240 Len=1288 [TCP segment of a reassembled PDU]
9	0.952651	10.11.14.101	78.135.65.15	TCP	54	49201 → 80 [ACK] Seq=280 Ack=1289 Win=62952 Len=0
10	0.952692	78.135.65.15	10.11.14.101	TCP	1342	80 → 49201 [PSH, ACK] Seq=1289 Ack=280 Win=64240 Len=1288 [TCP segment of a reassembled PDU]
11	0.952768	10.11.14.101	78.135.65.15	TCP	54	49201 → 80 [ACK] Seq=280 Ack=2577 Win=64240 Len=0
12	0.952896	78.135.65.15	10.11.14.101	TCP	1342	80 → 49201 [PSH, ACK] Seq=2577 Ack=280 Win=64240 Len=1288 [TCP segment of a reassembled PDU]
13	0.953176	78.135.65.15	10.11.14.101	TCP	1514	80 → 49201 [ACK] Seq=3865 Ack=280 Win=64240 Len=1460 [TCP segment of a reassembled PDU]
14	0.953224	78.135.65.15	10.11.14.101	TCP	1514	80 → 49201 [ACK] Seq=5325 Ack=280 Win=64240 Len=1460 [TCP segment of a reassembled PDU]
15	0.953255	78.135.65.15	10.11.14.101	TCP	1514	80 → 49201 [ACK] Seq=6785 Ack=280 Win=64240 Len=1460 [TCP segment of a reassembled PDU]
16	0.953284	78.135.65.15	10.11.14.101	TCP	1514	80 → 49201 [ACK] Seq=8245 Ack=280 Win=64240 Len=1460 [TCP segment of a reassembled PDU]
17	0.953309	10.11.14.101	78.135.65.15	TCP	54	49201 → 80 [ACK] Seq=280 Ack=8245 Win=64240 Len=0

```
    Address: HewlettP_1c:47:ae (00:08:02:1c:47:ae)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: 10.11.14.101, Dst: 78.135.65.15
▸ Transmission Control Protocol, Src Port: 49201, Dst Port: 80, Seq: 1, Ack: 1, Len: 279
▾ Hypertext Transfer Protocol
  ▾ GET /En_us/Documents/11_18/ HTTP/1.1\r\n
    ▸ [Expert Info (Chat/Sequence): GET /En_us/Documents/11_18/ HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /En_us/Documents/11_18/
      Request Version: HTTP/1.1
  Accept: text/html, application/xhtml+xml, */*\r\n
  Accept-Language: en-US\r\n
  User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko\r\n
  Accept-Encoding: gzip, deflate\r\n
  Host: bysound.com.tr\r\n
  DNT: 1\r\n
  Connection: Keep-Alive\r\n
  \r\n
  [Full request URI: http://bysound.com.tr/En_us/Documents/11_18/]
  [HTTP request 1/1]
  [Response in frame: 71]

0030  fa f0 69 a1 00 00 47 45  54 20 2f 45 6e 5f 75 73   ··i···GE T /En_us
0040  2f 44 6f 63 75 6d 65 6e  74 73 2f 31 31 5f 31 38   /Documen ts/11_18
0050  2f 20 48 54 54 50 2f 31  2e 31 0d 0a 41 63 63 65   / HTTP/1 .1··Acce
0060  70 74 3a 20 74 65 78 74  2f 68 74 6d 6c 2c 20 61   pt: text /html, a
0070  70 70 6c 69 63 61 74 69  6f 6e 2f 78 68 74 6d 6c   pplicati on/xhtml
0080  2b 78 6d 6c 2c 20 2a 2f  2a 0d 0a 41 63 63 65 70   +xml, */ *··Accep
0090  74 2d 4c 61 6e 67 75 61  67 65 3a 20 65 6e 2d 55   t-Langua ge: en-U
00a0  53 0d 0a 55 73 65 72 2d  41 67 65 6e 74 3a 20 4d   S··User- Agent: M
00b0  6f 7a 69 6c 6c 61 2f 35  2e 30 20 28 57 69 6e 64   ozilla/5 .0 (Wind
00c0  6f 77 73 20 4e 54 20 36  2e 31 3b 20 57 4f 57 36   ows NT 6 .1; WOW6
00d0  34 3b 20 54 72 69 64 65  6e 74 2f 37 2e 30 3b 20   4; Tride nt/7.0;
00e0  72 76 3a 31 31 2e 30 29  20 6c 69 6b 65 20 47 65   rv:11.0)  like Ge
00f0  63 6b 6f 0d 0a 41 63 63  65 70 74 2d 45 6e 63 6f   cko··Acc ept-Enco
0100  64 69 6e 67 3a 20 67 7a  69 70 2c 20 64 65 66 6c   ding: gz ip, defl
```

This packet will be responded in the packet with this number (http.response_in) Packets: 6517

We see that the PC make a *GET Request* as such `GET /En_us/Documents/11_18/ HTTP/1.1\r\n` with a Mozilla browser engine. Below, Wireshark indicate that the **response is in frame 71**. Following the rabbit hole, we see that the server reply back with a **application/msword** file type named **Content-Disposition: attachment; filename="form-363439590633444.doc"\r\n**

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
56	1.209761	10.11.14.101	78.135.65.15	TCP	54	49201 → 80 [ACK] Seq=280 Ack=36065 Win=51360 Len=0
57	1.209851	10.11.14.101	78.135.65.15	TCP	54	49201 → 80 [ACK] Seq=280 Ack=38641 Win=48784 Len=0
58	1.209943	10.11.14.101	78.135.65.15	TCP	54	[TCP Window Update] 49201 → 80 [ACK] Seq=280 Ack=38641 Win=64240 Len=0
59	1.457961	78.135.65.15	10.11.14.101	TCP	1342	80 → 49201 [PSH, ACK] Seq=38641 Ack=280 Win=64240 Len=1288 [TCP segment of a reassembled PDU]
60	1.458194	78.135.65.15	10.11.14.101	TCP	1342	80 → 49201 [PSH, ACK] Seq=39929 Ack=280 Win=64240 Len=1288 [TCP segment of a reassembled PDU]
61	1.458256	10.11.14.101	78.135.65.15	TCP	54	49201 → 80 [ACK] Seq=280 Ack=39929 Win=62952 Len=0
62	1.458319	10.11.14.101	78.135.65.15	TCP	54	49201 → 80 [ACK] Seq=280 Ack=41217 Win=64240 Len=0
63	1.458370	78.135.65.15	10.11.14.101	TCP	1342	80 → 49201 [PSH, ACK] Seq=41217 Ack=280 Win=64240 Len=1288 [TCP segment of a reassembled PDU]
64	1.458396	78.135.65.15	10.11.14.101	TCP	1342	80 → 49201 [PSH, ACK] Seq=42505 Ack=280 Win=64240 Len=1288 [TCP segment of a reassembled PDU]
65	1.458474	10.11.14.101	78.135.65.15	TCP	54	49201 → 80 [ACK] Seq=280 Ack=43793 Win=64240 Len=0
66	1.466424	78.135.65.15	10.11.14.101	TCP	1342	80 → 49201 [PSH, ACK] Seq=43793 Ack=280 Win=64240 Len=1288 [TCP segment of a reassembled PDU]
67	1.466685	78.135.65.15	10.11.14.101	TCP	1342	80 → 49201 [PSH, ACK] Seq=45081 Ack=280 Win=64240 Len=1288 [TCP segment of a reassembled PDU]
68	1.466689	10.11.14.101	78.135.65.15	TCP	54	49201 → 80 [ACK] Seq=280 Ack=45081 Win=62952 Len=0
69	1.466770	10.11.14.101	78.135.65.15	TCP	54	49201 → 80 [ACK] Seq=280 Ack=46369 Win=64240 Len=0
70	1.466890	78.135.65.15	10.11.14.101	TCP	1342	80 → 49201 [PSH, ACK] Seq=46369 Ack=280 Win=64240 Len=1288 [TCP segment of a reassembled PDU]
71	1.466969	78.135.65.15	10.11.14.101	HTTP	1313	HTTP/1.1 200 OK (application/msword)
72	1.467253	10.11.14.101	78.135.65.15	TCP	54	49201 → 80 [ACK] Seq=280 Ack=48916 Win=64240 Len=0

```
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Date: Wed, 14 Nov 2018 17:30:00 GMT\r\n
    Server: Apache\r\n
    Expires: Tue, 01 Jan 1970 00:00:00 GMT\r\n
    Cache-Control: no-store, no-cache, must-revalidate, max-age=0, post-check=0, pre-check=0\r\n
    Pragma: no-cache\r\n
    Content-Disposition: attachment; filename="form-363439590633444.doc"\r\n
    Content-Transfer-Encoding: binary\r\n
    Last-Modified: Wed, 14 Nov 2018 17:30:00 GMT\r\n
    Vary: Accept-Encoding,User-Agent\r\n
    Content-Encoding: gzip\r\n
    Keep-Alive: timeout=15, max=1000\r\n
    Connection: Keep-Alive\r\n
    Transfer-Encoding: chunked\r\n
    Content-Type: application/msword\r\n
    \r\n
    [HTTP response 1/1]
```

```
00d0  6e 6f 2d 63 61 63 68 65  0d 0a 43 6f 6e 74 65 6e   no-cache ··Conten
00e0  74 2d 44 69 73 70 6f 73  69 74 69 6f 6e 3a 20 61   t-Dispos ition: a
00f0  74 74 61 63 68 6d 65 6e  74 3b 20 66 69 6c 65 6e   ttachmen t; filen
0100  61 6d 65 3d 22 66 6f 72  6d 2d 33 36 33 34 33 39   ame="for m-363439
0110  35 39 30 36 33 33 34 34  34 2e 64 6f 63 22 0d 0a   59063344 4.doc"··
0120  43 6f 6e 74 65 6e 74 2d  54 72 61 6e 73 66 65 72   Content- Transfer
0130  2d 45 6e 63 6f 64 69 6e  67 3a 20 62 69 6e 61 72   -Encodin g: binar
0140  79 0d 0a 4c 61 73 74 2d  4d 6f 64 69 66 69 65 64   y··Last- Modified
0150  3a 20 57 65 64 2c 20 31  34 20 4e 6f 76 20 32 30   : Wed, 1 4 Nov 20
0160  31 38 20 31 37 3a 33 30  3a 30 30 20 47 4d 54 0d   18 17:30 :00 GMT·
0170  0a 56 61 72 79 3a 20 41  63 63 65 70 74 2d 45 6e   ·Vary: A ccept-En
0180  63 6f 64 69 6e 67 2c 55  73 65 72 2d 41 67 65 6e   coding,U ser-Agen
```

Frame (1313 bytes) | Reassembled TCP (48915 bytes) | De-chunked entity body (48321 bytes) | Uncompressed entity body (94592 bytes)

Response line (http.response.line), 70 bytes

Packets: 6517

DETECTION DETAILS **RELATIONS** BEHAVIOR COMMUNITY 10

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Contacted URLs (8)

Scanned	Detections	Status	URL
2022-07-16	7 / 87	-	http://50.78.167.65:7080/
2022-06-03	6 / 95	200	http://shajishalom.com/foh636qv
2020-04-07	3 / 77	404	http://shajishalom.com/FOH636qV
2022-10-31	11 / 90	404	http://c-t.com.au/PspAMbuSd2/
2023-03-22	8 / 86	200	http://866appliance.com/Y6TApcX8A
2022-03-19	8 / 93	404	http://c-t.com.au/pspambusd2
2020-01-17	2 / 72	200	http://planetefaune.com/yuaijLUGIN
2022-09-22	11 / 88	404	http://c-t.com.au/PspAMbuSd2

Contacted Domains (5)

Domain	Detections	Created	Registrar
866appliance.com	5 / 87	2017-10-13	Porkbun LLC
c-t.com.au	2 / 88	-	-
planetefaune.com	3 / 87	2022-12-07	-
pteacademicvoucher.in	7 / 87	-	-
shajishalom.com	7 / 87	2022-11-14	-

Contacted IP addresses (5)

IP	Detections	Autonomous System	Country
103.27.32.36	0 / 87	45638	AU
3.12.63.241	0 / 86	16509	US
50.78.167.65	6 / 87	7922	US
65.254.248.149	0 / 86	29873	US

After inspection of the relation tab (VirtusTotal), we notice that the document contacted a few host. Moreover, Wireshark support that conjecture. **10.11.14.101** made a *DNS* query to acquire the IP address of **c-t.com.au**, which was resolved to **50.62.194.30**. Then a few traffic down the line, **10.11.14.101** made 2 request to **50.62.194.30**. Precisely a *GET Request* as follow **GET /PspAMbuSd2 HTTP/1.1** and **GET /PspAMbuSd2/ HTTP/1.1** , since the first one redirect to the second one.

73	10.034582	10.11.14.101	78.135.65.15	TCP	54 49201 → 80 [RST, ACK] Seq=280 Ack=48916 Win=0 Len=0
74	23.631490	10.11.14.101	10.11.14.1	DNS	70 Standard query 0xd68d A c-t.com.au
75	23.710496	10.11.14.1	10.11.14.101	DNS	86 Standard query response 0xd68d A c-t.com.au A 50.62.194.30
76	23.717393	10.11.14.101	50.62.194.30	TCP	66 49202 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
77	23.802246	50.62.194.30	10.11.14.101	TCP	58 80 → 49202 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
78	23.802388	10.11.14.101	50.62.194.30	TCP	54 49202 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
79	23.802624	10.11.14.101	50.62.194.30	HTTP	361 GET /PspAMbuSd2 HTTP/1.1
80	23.802696	50.62.194.30	10.11.14.101	TCP	54 80 → 49202 [ACK] Seq=1 Ack=308 Win=64240 Len=0
81	23.905551	50.62.194.30	10.11.14.101	HTTP	609 HTTP/1.1 301 Moved Permanently (text/html)
82	23.905918	10.11.14.101	50.62.194.30	TCP	54 49202 → 80 [ACK] Seq=308 Ack=556 Win=63685 Len=0
83	23.908218	10.11.14.101	50.62.194.30	HTTP	362 GET /PspAMbuSd2/ HTTP/1.1
84	23.908326	50.62.194.30	10.11.14.101	TCP	54 80 → 49202 [ACK] Seq=556 Ack=616 Win=64240 Len=0

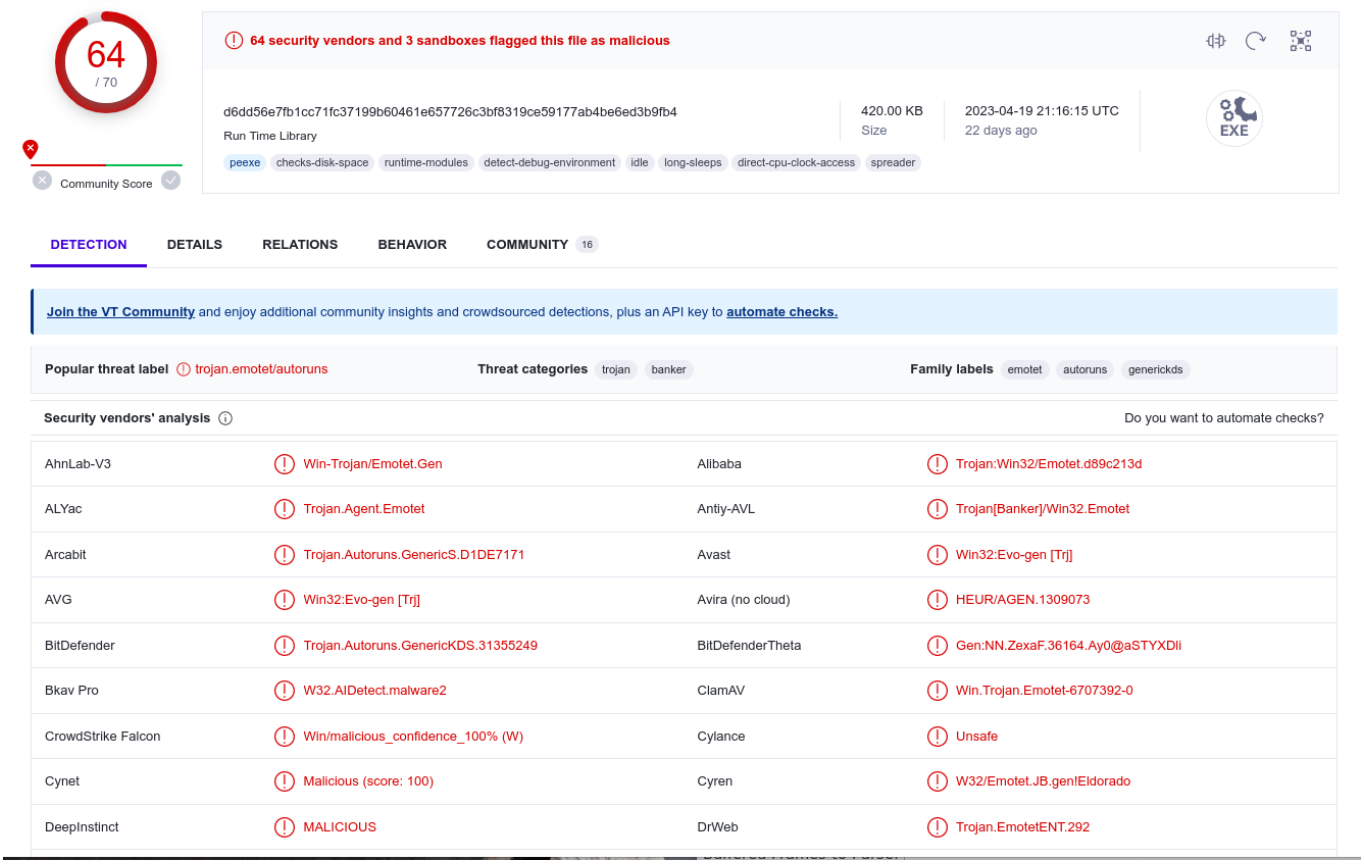
The second *Get Request* on the other hand, fetch something that will only appear at **frame 588**

```
82 23.905918    10.11.14.101    50.62.194.30    TCP     54 49202 → 80 [ACK] Seq=308 Ack=556 Win=63685 Len=0
83 23.908218    10.11.14.101    50.62.194.30    HTTP   362 GET /PspAMbuSd2/ HTTP/1.1
84 23.908326    50.62.194.30    10.11.14.101    TCP     54 80 → 49202 [ACK] Seq=556 Ack=616 Win=64240 Len=0
85 23.997263    50.62.194.30    10.11.14.101    TCP   1342 80 → 49202 [PSH, ACK] Seq=556 Ack=616 Win=64240 Len=1288 [TCP segment of
86 23.997427    10.11.14.101    50.62.194.30    TCP     54 49202 → 80 [ACK] Seq=616 Ack=1844 Win=64240 Len=0

    Type: IPv4 (0x0800)
  Internet Protocol Version 4, Src: 10.11.14.101, Dst: 50.62.194.30
  Transmission Control Protocol, Src Port: 49202, Dst Port: 80, Seq: 308, Ack: 556, Len: 308
  Hypertext Transfer Protocol
    GET /PspAMbuSd2/ HTTP/1.1\r\n
      [Expert Info (Chat/Sequence): GET /PspAMbuSd2/ HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /PspAMbuSd2/
      Request Version: HTTP/1.1
    Accept: */*\r\n
    Accept-Encoding: gzip, deflate\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.307
    Host: c-t.com.au\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://c-t.com.au/PspAMbuSd2/]
    [HTTP request 2/2]
    [Prev request in frame: 79]
    [Response in frame: 588]
```

The response of the previous *GET Request* give a file under the name of **Content-Disposition: attachment; filename="ijccaFkQnS.exe"\r\n**

```
587 24.704586    50.62.194.30    10.11.14.101    TCP     1342 80 → 49202 [PSH, ACK] Seq=429460 Ack=616 Win=64240 Len=
588 24.704652    50.62.194.30    10.11.14.101    HTTP     506 HTTP/1.1 200 OK
589 24.704659    10.11.14.101    50.62.194.30    TCP       54 49202 → 80 [ACK] Seq=616 Ack=430748 Win=53936 Len=0

    Pragma: no-cache\r\n
    Content-Disposition: attachment; filename="ijccaFkQnS.exe"\r\n
    Content-Transfer-Encoding: binary\r\n
    Last-Modified: Wed, 14 Nov 2018 17:17:56 GMT\r\n
    Content-Type: application/octet-stream\r\n
    X-Port: port_10802\r\n
    X-Cacheable: YES:Forced\r\n
  Content-Length: 430080\r\n
    Accept-Ranges: bytes\r\n
    Date: Wed, 14 Nov 2018 17:30:50 GMT\r\n
    Age: 774\r\n
    Vary: User-Agent\r\n
    X-Cache: cached\r\n
    X-Cache-Hit: HIT\r\n
    X-Backend: all_requests\r\n
    \r\n
    [HTTP response 2/2]
    [Time since request: 0.796434000 seconds]
```

As you can remember, we saw that filename previously in **NetworkMiner**. Going back in it, we extract his SHA_256 signature **(d6dd56e7fb1cc71fc37199b60461e657726c3bf8319ce59177ab4be6ed3b9fb4)** and anlysis it on *VirusTotal*. **64/70** score clearly indicate that it is a threat labeled **trojan.emotet/autoruns**.



64 / 70

Community Score

64 security vendors and 3 sandboxes flagged this file as malicious

d6dd56e7fb1cc71fc37199b60461e657726c3bf8319ce59177ab4be6ed3b9fb4

Run Time Library

peexe checks-disk-space runtime-modules detect-debug-environment idle long-sleeps direct-cpu-clock-access spreader

420.00 KB Size

2023-04-19 21:16:15 UTC 22 days ago

EXE

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 16

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.emotet/autoruns

Threat categories trojan banker

Family labels emotet autoruns generickds

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Win-Trojan/Emotet.Gen	Alibaba	Trojan:Win32/Emotet.d89c213d
ALYac	Trojan.Agent.Emotet	Antiy-AVL	Trojan[Banker]/Win32.Emotet
Arcabit	Trojan.Autoruns.GenericS.D1DE7171	Avast	Win32:Evo-gen [Trj]
AVG	Win32:Evo-gen [Trj]	Avira (no cloud)	HEUR/AGEN.1309073
BitDefender	Trojan.Autoruns.GenericKDS.31355249	BitDefenderTheta	Gen:NN.ZexaF.36164.Ay0@aSTYXDli
Bkav Pro	W32.AIDetect.malware2	ClamAV	Win.Trojan.Emotet-6707392-0
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cylance	Unsafe
Cynet	Malicious (score: 100)	Cyren	W32/Emotet.JB.gen!Eldorado
DeepInstinct	MALICIOUS	DrWeb	Trojan.EmotetENT.292

Furthermore, the relation tab indicate to us many address the program want to connect. Particularly, **50.78.167.65** appear to be the first address contacted before the others (according to Wireshark). Surely, that server was a **Command & Control Center** that delivered the others address to contact.

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key t

Contacted URLs (33)

Scanned	Detections	Status	URL
2023-04-22	13 / 89	200	http://133.242.208.183:8080/
2022-07-16	6 / 87	200	http://173.19.73.104:443/
2022-07-16	7 / 87	-	http://50.78.167.65:7080/
2022-07-16	5 / 87	-	http://138.207.150.46:443/
2023-04-20	12 / 89	407	http://192.155.90.90:7080/
2023-04-15	11 / 89	200	http://198.199.185.25:443/
2021-12-29	2 / 93	200	http://71.163.171.106/
2022-07-16	5 / 87	-	http://173.160.205.161:990/
2022-07-16	4 / 87	-	http://24.201.79.34:8080/
2023-04-21	13 / 89	400	http://159.65.76.245:443/

Contacted IP addresses (15)

IP	Detections	Autonomous System	Country
12.222.134.10	5 / 87	7018	US
173.11.47.169	6 / 87	7922	US
177.242.156.119	4 / 87	13999	MX
186.18.236.83	5 / 87	27747	AR
189.244.86.184	9 / 87	8151	MX
20.80.129.13	0 / 87	8075	US
20.99.132.105	1 / 87	8075	US
200.127.55.5	0 / 86	7303	AR
205.185.187.190	1 / 87	7029	US
23.216.147.64	3 / 87	20940	US

3193a93f3f1b65a7d8bf9d73d8f459a7b51f8afa8d6d5f6ec6518ebf

As we can see below, after the initial contact with the server, many connection to various IP address are made.

593	45.314618	10.11.14.101	50.78.167.65	TCP	66	49209 → 7080 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
594	48.322608	10.11.14.101	50.78.167.65	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 49209 → 7080 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
595	54.331366	10.11.14.101	50.78.167.65	TCP	62	[TCP Retransmission] [TCP Port numbers reused] 49209 → 7080 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
596	66.332051	10.11.14.101	50.78.167.65	TCP	66	49210 → 7080 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
597	66.347680	50.78.167.65	10.11.14.101	TCP	54	7080 → 49209 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
598	69.452523	50.78.167.65	10.11.14.101	TCP	58	7080 → 49210 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
599	69.452716	10.11.14.101	50.78.167.65	TCP	54	49210 → 7080 [ACK] Seq=1 Ack=1 Win=64240 Len=0
600	69.452910	10.11.14.101	50.78.167.65	HTTP	765	GET / HTTP/1.1
601	69.452996	50.78.167.65	10.11.14.101	TCP	54	7080 → 49210 [ACK] Seq=1 Ack=712 Win=64240 Len=0
602	99.503306	10.11.14.101	50.78.167.65	TCP	54	49210 → 7080 [RST, ACK] Seq=712 Ack=1 Win=0 Len=0
603	99.534645	10.11.14.101	177.242.156.119	TCP	66	49211 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
604	102.534207	10.11.14.101	177.242.156.119	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 49211 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
605	108.549806	10.11.14.101	177.242.156.119	TCP	62	[TCP Retransmission] [TCP Port numbers reused] 49211 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
606	120.550159	10.11.14.101	177.242.156.119	TCP	66	49212 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
607	120.581046	177.242.156.119	10.11.14.101	TCP	54	80 → 49211 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
608	123.565524	10.11.14.101	177.242.156.119	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 49212 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
609	129.582646	10.11.14.101	177.242.156.119	TCP	62	[TCP Retransmission] [TCP Port numbers reused] 49212 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
610	141.596645	177.242.156.119	10.11.14.101	TCP	54	80 → 49212 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
611	141.612665	10.11.14.101	189.244.86.184	TCP	66	49213 → 990 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
612	142.211121	189.244.86.184	10.11.14.101	TCP	58	990 → 49213 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
613	142.211278	10.11.14.101	189.244.86.184	TCP	54	49213 → 990 [ACK] Seq=1 Ack=1 Win=64240 Len=0
614	142.211510	10.11.14.101	189.244.86.184	HTTP	811	GET / HTTP/1.1
615	142.211581	189.244.86.184	10.11.14.101	TCP	54	990 → 49213 [ACK] Seq=1 Ack=758 Win=64240 Len=0
616	151.626764	189.244.86.184	10.11.14.101	HTTP	342	HTTP/1.1 200 OK (text/html)
617	151.629217	10.11.14.101	189.244.86.184	TCP	54	49213 → 990 [ACK] Seq=758 Ack=289 Win=63952 Len=0
618	202.554736	10.11.14.101	189.244.86.184	HTTP	787	GET / HTTP/1.1
619	202.554972	189.244.86.184	10.11.14.101	TCP	54	990 → 49213 [ACK] Seq=289 Ack=1491 Win=64240 Len=0
620	232.596292	10.11.14.101	189.244.86.184	TCP	54	49213 → 990 [RST, ACK] Seq=1491 Ack=289 Win=0 Len=0
621	232.605561	10.11.14.101	12.222.134.10	TCP	66	49214 → 7080 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
622	235.627470	10.11.14.101	12.222.134.10	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 49214 → 7080 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
623	241.627486	10.11.14.101	12.222.134.10	TCP	62	[TCP Retransmission] [TCP Port numbers reused] 49214 → 7080 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
624	253.611865	12.222.134.10	10.11.14.101	TCP	54	7080 → 49214 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
625	253.612746	10.11.14.101	12.222.134.10	TCP	66	49215 → 7080 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
626	256.627528	10.11.14.101	12.222.134.10	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 49215 → 7080 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
627	262.627524	10.11.14.101	12.222.134.10	TCP	62	[TCP Retransmission] [TCP Port numbers reused] 49215 → 7080 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
628	274.643141	12.222.134.10	10.11.14.101	TCP	54	7080 → 49215 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
629	274.675436	10.11.14.101	173.11.47.169	TCP	66	49216 → 8080 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
630	283.835048	173.11.47.169	10.11.14.101	TCP	58	8080 → 49216 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
631	283.835386	10.11.14.101	173.11.47.169	TCP	54	49216 → 8080 [ACK] Seq=1 Ack=1 Win=64240 Len=0
632	283.835883	10.11.14.101	173.11.47.169	HTTP	767	GET / HTTP/1.1
633	283.836050	173.11.47.169	10.11.14.101	TCP	54	8080 → 49216 [ACK] Seq=1 Ack=714 Win=64240 Len=0
634	305.172626	173.11.47.169	10.11.14.101	TCP	54	8080 → 49216 [FIN, PSH, ACK] Seq=1 Ack=714 Win=64240 Len=0
635	305.172886	10.11.14.101	173.11.47.169	TCP	54	49216 → 8080 [ACK] Seq=714 Ack=2 Win=64240 Len=0
636	305.173118	10.11.14.101	173.11.47.169	TCP	54	49216 → 8080 [FIN, ACK] Seq=714 Ack=2 Win=64240 Len=0
637	305.173244	173.11.47.169	10.11.14.101	TCP	54	8080 → 49216 [ACK] Seq=2 Ack=715 Win=64239 Len=0
638	305.206345	10.11.14.101	186.18.236.83	TCP	66	49217 → 8080 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
639	305.455892	186.18.236.83	10.11.14.101	TCP	58	8080 → 49217 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460

Returning to *NetworkMiner*, a investigation of the **Credential Tab**, indicate that data are sent using **cookies**.

Hosts (39) | Files (53) | Images | Messages | Credentials (18) | Sessions (186) | DNS (24) | Parameters (943) | Keywords | Anomalies |

☑ Show Cookies ☑ Show NTLM challenge-response ☐ Mask Passwords

Client	Server	Protocol	Username	Password	Valid login	Login timestamp
10.11.14.101 (Windows)	173.11.47.169 [173.11.47.169]	HTTP Cookie	34606=BpEzQBGF5YlNzrLOuwD9H4baQLCWgsC...	N/A	Unknown	2018-11-14 17:35:10 UTC
10.11.14.101 (Windows)	186.18.236.83 [186.18.236.83]	HTTP Cookie	65135=GaEALOJY/7DRwduLNUhx84NVim44QHE...	N/A	Unknown	2018-11-14 17:35:32 UTC
10.11.14.101 (Windows)	173.11.47.169 [173.11.47.169]	HTTP Cookie	49430=kBYNNtBLgBTmxGaHHxcNpdCmn+1fPZj...	N/A	Unknown	2018-11-14 17:39:38 UTC
10.11.14.101 (Windows)	186.18.236.83 [186.18.236.83]	HTTP Cookie	14034=GoGfAuXoIqOvVDBBO6o8/n4ASWGsiNJ5...	N/A	Unknown	2018-11-14 17:40:29 UTC
10.11.14.101 (Windows)	200.127.55.5 [200.127.55.5]	HTTP Cookie	65515=FbuPCofjx1HSpEFlpqCZZkjM0NyyVyO8...	N/A	Unknown	2018-11-14 17:41:00 UTC
10.11.14.101 (Windows)	210.2.86.72 [210.2.86.72]	HTTP Cookie	50088=e7sp79Kq5TdBnt9D5eY23uf9Qyp7IjUckD...	N/A	Unknown	2018-11-14 17:42:55 UTC
10.11.14.101 (Windows)	71.163.171.106 [71.163.171.106]	HTTP Cookie	62913=QNd+zpG1HHBqvBIlbdPpaoGTSo1Cqnn...	N/A	Unknown	2018-11-14 17:45:19 UTC
10.11.14.101 (Windows)	71.163.171.106 [71.163.171.106]	HTTP Cookie	17783=FsyDBpTGtLqi8VqhDR4TZu0Yp+plo/YQzT...	N/A	Unknown	2018-11-14 17:45:39 UTC
10.11.14.101 (Windows)	109.170.209.165 [109.170.209.165]	HTTP Cookie	22714=G4FrsIA4CeaTUI60MD77TyFv+Gocfg/Hju...	N/A	Unknown	2018-11-14 17:46:51 UTC
10.11.14.101 (Windows)	205.185.187.190 [205.185.187.190]	HTTP Cookie	52495=WXQ/wrJDCM5kc5BOqzFLLHmOd3Y5780...	N/A	Unknown	2018-11-14 17:47:23 UTC
10.11.14.101 (Windows)	24.201.79.34 [24.201.79.34]	HTTP Cookie	1530=HZgHPtDQiZen+EvduVVsbIl9pd5uZxtmxa...	N/A	Unknown	2018-11-14 17:47:34 UTC
10.11.14.101 (Windows)	133.242.208.183 [133.242.208.183]	HTTP Cookie	16242=NgjGq49OG7ePJc6EHQGWiFB/eLx0VASJd...	N/A	Unknown	2018-11-14 17:48:55 UTC
10.11.14.101 (Windows)	173.11.47.169 [173.11.47.169]	HTTP Cookie	8742=UbfU45wArb6xe8PGQOvHW0h3RoPiu+ov...	N/A	Unknown	2018-11-14 17:53:39 UTC
10.11.14.101 (Windows)	186.18.236.83 [186.18.236.83]	HTTP Cookie	60082=GkkPXTsSSc+q3sQ4Ii15VutXa4bPG0B5T...	N/A	Unknown	2018-11-14 17:54:01 UTC
10.11.14.101 (Windows)	200.127.55.5 [200.127.55.5]	HTTP Cookie	[illegible] xAifFBnv2RVn0N6AUGpD...	N/A	Unknown	2018-11-14 17:54:30 UTC
10.11.14.101 (Windows)	210.2.86.72 [210.2.86.72]	HTTP Cookie	[illegible] P/VsV7C+v/SSvEjUdKYfag...	N/A	Unknown	2018-11-14 17:56:24 UTC
10.11.14.101 (Windows)	173.11.47.169 [173.11.47.169]	HTTP Cookie	5283=F5ijsdh1zc2QSjiAZ30k5ol4sGu7VUgGbWl/...	N/A	Unknown	2018-11-14 21:01:22 UTC
10.11.14.101 (Windows)	186.18.236.83 [186.18.236.83]	HTTP Cookie	42427=nwcSn1dG1AEPiAGuV/Ay2WQy7gSqg6...	N/A	Unknown	2018-11-14 21:01:35 UTC

10.11.14.101 (Windows)

Analysis Overview

Request Report Deletion

Submission name:	2018-11-14-Emotet-infection-with-IcedID-banking-Trojan.pcap
Size:	3.5MiB
Type:	unknown
Mime:	application/vnd.tcpdump.pcap
SHA256:	910c11b89d5aabf3ce13037516d15d97a5f29963bc54412f054ff74fe8dcc6b0
Last Anti-Virus Scan:	05/12/2023 10:49:14 (UTC)
Last Sandbox Report:	03/12/2021 23:02:12 (UTC)

suspicious

AV Detection: 2%

Labeled as: Trojan.Emotet

#tag

Link Twitter E-Mail

Analysis Overview
Anti-Virus Scanner Results
Community (2)

Back to top

Anti-Virus Results

Up-to-date

MetaDefender

3%

Multi Scan Analysis

Last Update: 05/12/2023 10:49:14 (UTC)

View Details:

Visit Vendor:

VirusTotal

CLEAN

Multi Scan Analysis

Last Update: 05/12/2023 10:49:14 (UTC)

View Details:

Visit Vendor:

Latest News

Behind the Curtain: Falcon OverWatch Hunting Leads Explained
Falcon OverWatch Team - April 27, 2023

How Falcon OverWatch Investigates Malicious Self-Extracting Archives, Decoy Files and Their Hidden Payloads
Jai Minton - Falcon OverWatch Team - March 31, 2023

QakBot eCrime Campaign Leverages Microsoft OneNote Attachments
Robert Dean - Anthony Witten - March 17, 2023

CrowdStrike's Free TensorFlow-to-Rust Conversion Tool Enables Data Scientists to Run Machine Learning Models as Pure Safe Code
Lukasz Woznicki - March 2, 2023

CrowdStrike Uncovers I2Pminer MacOS Mineware Variant
Mitch Datka - Ron Bolger - February 23, 2023

See More!

File Collections

Name	Files number	Verdict

Continuing the investigation, since **Hybrid Analysis** didn't land us worth while results, we were lucky on **Packet Total instead**. It appear our host made many crypted conversation with **185.129.49.19**. Furthermore, after the **Suspicious Activity** tab, we notice that the **SSL Certification to 185.129.49.19 failed !** Now the picture is clear, the certificated provided is not registered in list of trusted certificate. Thus, we can assume that host the master attack who is sending instruction the target to gain an authorized access to the network.

Malicious Activity | Suspicious Activity | Connections | DNS | HTTP | SSL Certificates | PKI (X.509) | Transferred Files | Extracted Executable Files | Dynamic Protocol Detection | Strange Activity | Community Tags | Similar Packet Captures

Search in results

Timestamp	Connection ID	Sender IP	Sender Port	Target IP	Target Port	Version	Cipher	Curve	Server Name	Resumed?	Next Protocol	Established?	Certificate Chain File IDs
2018-11-14 17:50:55 Z	CqjFr14NZSknJg8U6c	10.11.14.101	49274	185.129.49.19	443	TLSv10	TLS_RSA_WITH_AES_128_CBC_SHA	null	therebes.biz	F	null	T	FFTPS14FPQ70EVL...
2018-11-14 17:50:58 Z	Cj04k44WFoG4WXDaf8	10.11.14.101	49277	185.129.49.19	443	TLSv10	TLS_RSA_WITH_AES_128_CBC_SHA	null	therebes.biz	F	null	T	F9LW6CMDJN6H99A...
2018-11-14 17:50:58 Z	C3QS0s4LYWLCwUvlKd	10.11.14.101	49280	185.129.49.19	443	TLSv10	TLS_RSA_WITH_AES_128_CBC_SHA	null	therebes.biz	F	null	T	FQ6GHH3YA8JBEYZ...
2018-11-14 17:50:58 Z	CdFC6WJO5FxSYQMmj	10.11.14.101	49279	185.129.49.19	443	TLSv10	TLS_RSA_WITH_AES_128_CBC_SHA	null	therebes.biz	F	null	T	FDVET0ATQJ0YCBZ...
2018-11-14 17:50:58 Z	CoZc36ZI0ohhrgbZS2	10.11.14.101	49278	185.129.49.19	443	TLSv10	TLS_RSA_WITH_AES_128_CBC_SHA	null	therebes.biz	F	null	T	FWYNFM37DU0PI6Y...
2018-11-14 17:50:58 Z	CoLZdV23RxgUkTeGzh	10.11.14.101	49276	185.129.49.19	443	TLSv10	TLS_RSA_WITH_AES_128_CBC_SHA	null	therebes.biz	F	null	T	FNJJJI30MVSZMJT...
2018-11-14 17:50:58 Z	COEZWg3kHBAb8bXB41	10.11.14.101	49281	185.129.49.19	443	TLSv10	TLS_RSA_WITH_AES_128_CBC_SHA	null	therebes.biz	F	null	T	FRI95O4VJM4P95H...
2018-11-14 17:50:58 Z	CxtV7yQyavsn6TCC6	10.11.14.101	49282	185.129.49.19	443	TLSv10	TLS_RSA_WITH_AES_128_CBC_SHA	null	therebes.biz	F	null	T	FAWVVE1LKZR5BTZ...
2018-11-14 17:55:58 Z	CDUwWhCGOOLNI6bhf	10.11.14.101	49298	185.129.49.19	443	TLSv10	TLS_RSA_WITH_AES_128_CBC_SHA	null	therebes.biz	F	null	T	FDGGZX6H6K3NO2Z...
2018-11-14 18:00:59 Z	Czhqyvdw7kKYgD3E6	10.11.14.101	49311	185.129.49.19	443	TLSv10	TLS_RSA_WITH_AES_128_CBC_SHA	null	therebes.biz	F	null	T	FU5NIG2JJJNZZSZ...

Showing entries 1 to 10 (46 total)

Show 10 entries

CSV Print

2018-11-14 17:50:58 Z	CqjFr14NZSknJg8U6c	SSL::Invalid_Server_Cert	SSL certificate validation failed with (self signed certificate)	CN=main.info	10.11.14.101	49274	185.129.49.19	443	10.11.14.101	443	185.129.49.19	null