2024-08-15

1. check alerts

23[.]205[.]110[.]48 - EX1

23[.]33[.]138[.]184 - EX2

10[.]8[.]15[.]4 - IN1 (DC)

10[.]8[.]15[.]133 - IN2

72[.]5[.]43[.]29 - EX3

• IN2 => EX1: request for txt, Microsoft connection test

• IN2 => EX2: TLSv1.0

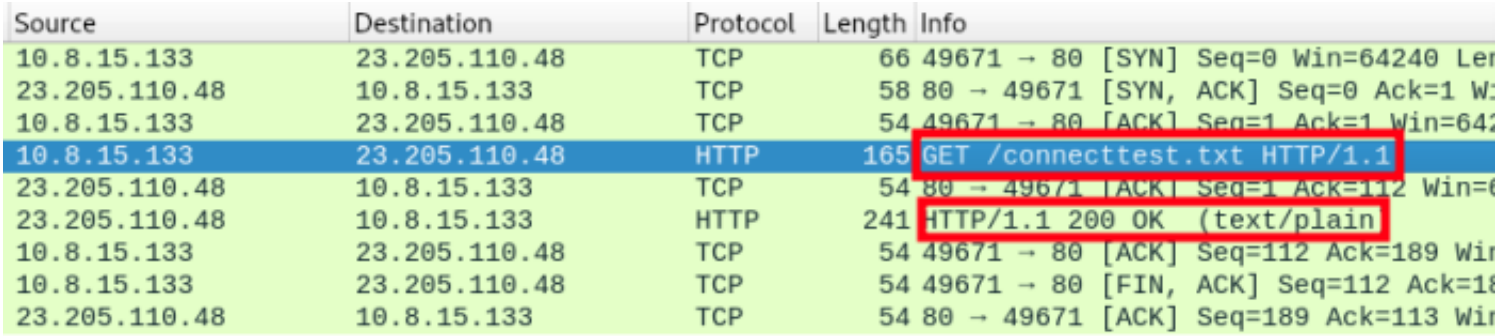
• IN2 => IN1: kerberos principal name overflow TCP

• EX3 => IN2: windows executable

• EX3 => IN2: suspicious dotted Quad host MZ response

• IN2 => EX3: suspicious POST to dotted Quad with Fake browser

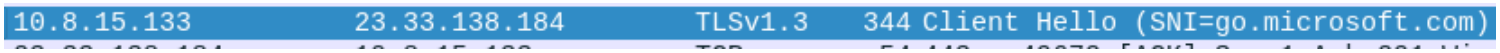
2. filter for EX1



Source	Destination	Protocol	Length	Info
10.8.15.133	23.205.110.48	TCP	66	49671 → 80 [SYN] Seq=0 Win=64240 Len
23.205.110.48	10.8.15.133	TCP	58	80 → 49671 [SYN, ACK] Seq=0 Ack=1 Wi
10.8.15.133	23.205.110.48	TCP	54	49671 → 80 [ACK] Seq=1 Ack=1 Win=642
10.8.15.133	23.205.110.48	HTTP	165	GET /connecttest.txt HTTP/1.1
23.205.110.48	10.8.15.133	TCP	54	80 → 49671 [ACK] Seq=1 Ack=112 Win=6
23.205.110.48	10.8.15.133	HTTP	241	HTTP/1.1 200 OK (text/plain
10.8.15.133	23.205.110.48	TCP	54	49671 → 80 [ACK] Seq=112 Ack=189 Wir
10.8.15.133	23.205.110.48	TCP	54	49671 → 80 [FIN, ACK] Seq=112 Ack=18
23.205.110.48	10.8.15.133	TCP	54	80 → 49671 [ACK] Seq=189 Ack=113 Wir

nothing special, just connection test

3. filter for EX2

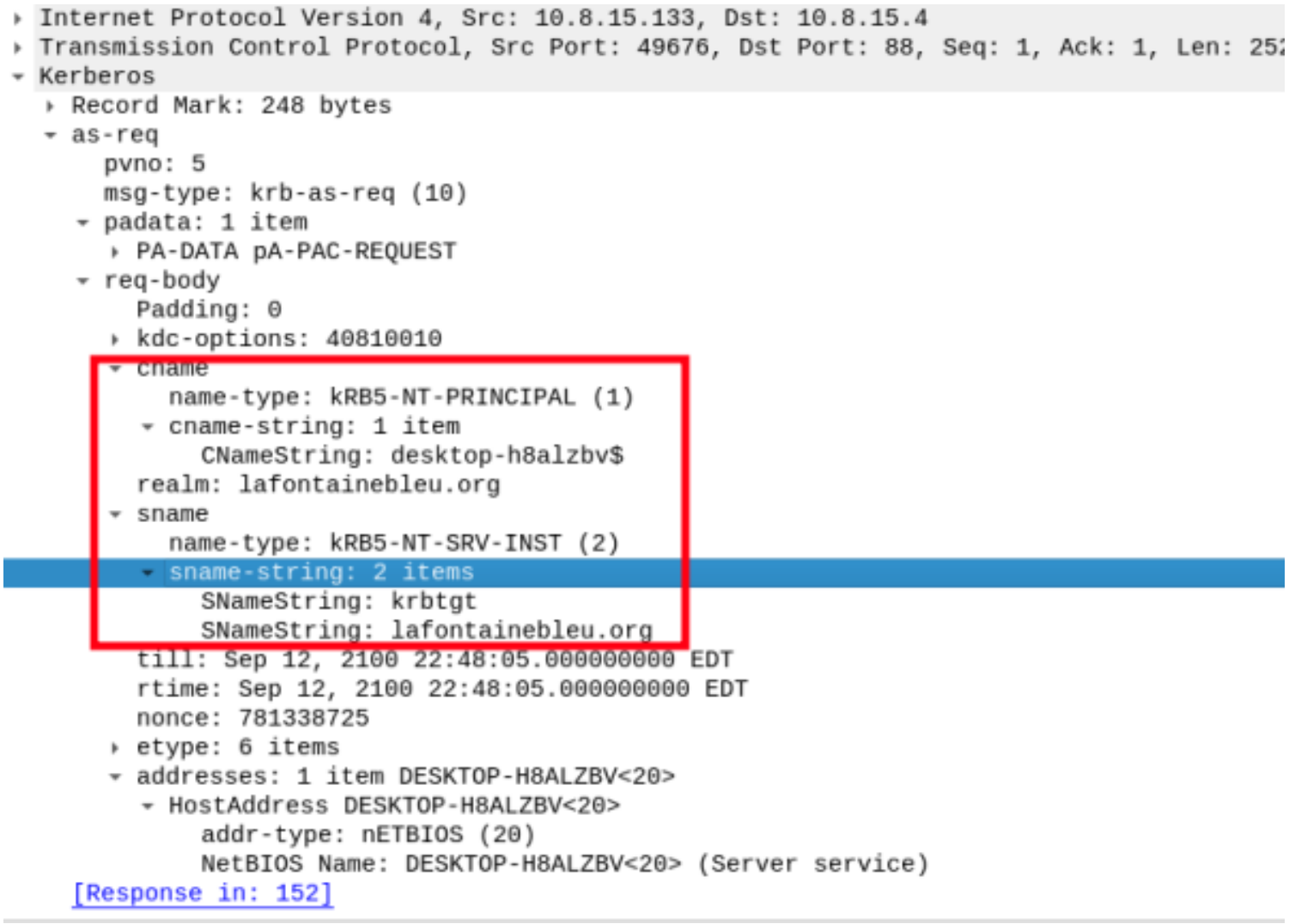


IP belongs to Microsoft

4. filter for IN2 => IN1
5. find packet that triggered alert:

```
Count:5 Event#3.637 2024-08-15 00:09 UTC
GPL RPC kerberos principal name overflow TCP
10[.]8[.]15[.]133 -> 10[.]8[.]15[.]4
IPVer=4 hlen=5 tos=0 dlen=292 ID=4991 flags=2 offset=0 ttl=128
chksum=46012
Protocol: 6 sport=49676 -> dport=88

Seq=3254969383 Ack=473947260 Off=5 Res=0 Flags=***AP*** Win=1026
urp=49696 chksum=0
```



• nothing seems suspicious

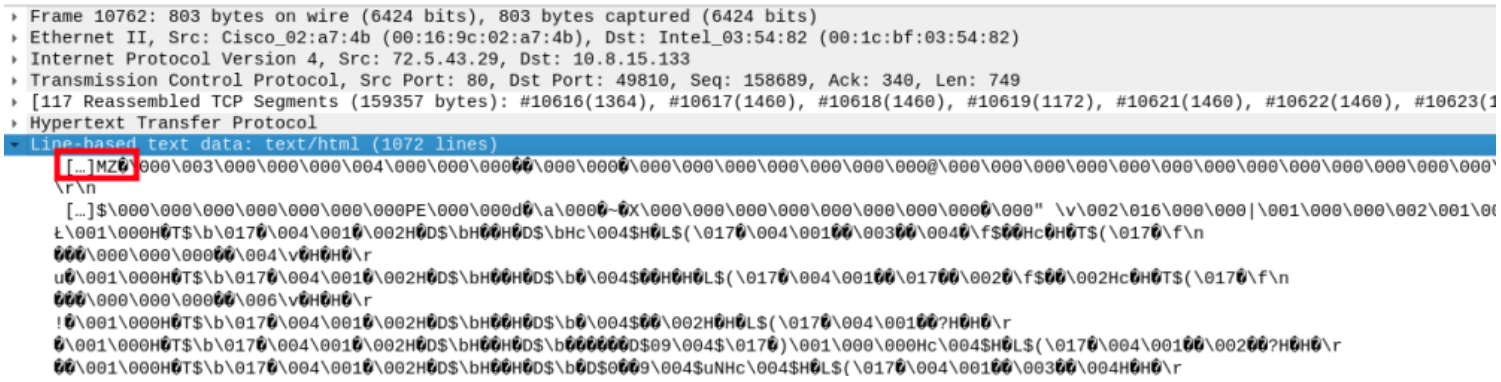
6. filter for IN2 => EX3

```
ip[.]addr == 10[.]8[.]15[.]133 and ip[.]addr == 72[.]5[.]43[.]29 and http[.]response[.]code != 400
```

No.	Time	Source	Destination	Protocol	Length	Info
10613	136.132929	72.5.43.29	10.8.15.133	HTTP	134	HTTP/1.1 200 OK
10762	136.898282	72.5.43.29	10.8.15.133	HTTP	803	HTTP/1.1 200 OK (text/html)
11030	197.053168	72.5.43.29	10.8.15.133	HTTP	207	HTTP/1.1 200 OK (text/html)

• there are only 2 replies with payloads

7. analyze payload from frame 10762

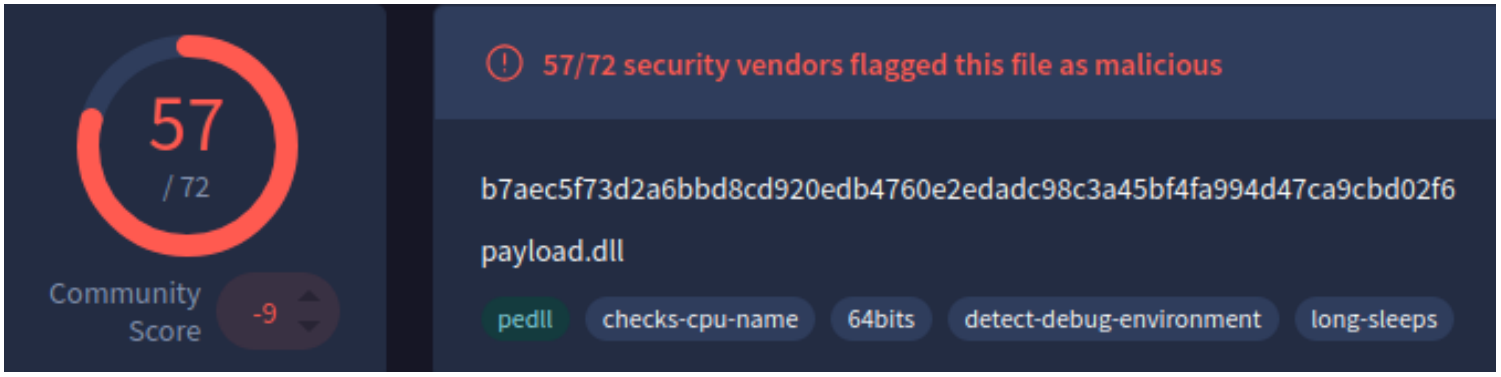


- seems to be Windows PE file

```
remnux@remnux:~/Downloads$ file 0f60a3e7baecf2748b1c8183ed37d1e4
0f60a3e7baecf2748b1c8183ed37d1e4: PE32+ executable (DLL) (GUI)
x86-64, for MS Windows
```

- look up hash

```
remnux@remnux:~/Downloads$ sha256sum
0f60a3e7baecf2748b1c8183ed37d1e4
b7aec5f73d2a6bbd8cd920edb4760e2edadc98c3a45bf4fa994d47ca9cbd02f6
0f60a3e7baecf2748b1c8183ed37d1e4
```



- view behavior

8. analyze payload from frame 11030

```
remnux@remnux:~/Downloads$ file 11030
11030: data
remnux@remnux:~/Downloads$ xxd 11030
00000000: afa5 39e1 ae05 69ab b756 35f4 66c1 a6e0  ..9...i..V5.f...
00000010: 7826 7332 9b6e b31b e5a1 a7e7 9ef5 3622  x&s2.n.......6"
remnux@remnux:~/Downloads$ xxd -p -c 256 11030
afa539e1ae0569abb75635f466c1a6e0782673329b6eb31be5a1a7e79ef53622
remnux@remnux:~/Downloads$ sha256sum 11030
```

dff7255b90139fbc8d3e76f31b480e65fc3eb7f49f70e7876cfb3f1cb56e5123
11030

• look up hash

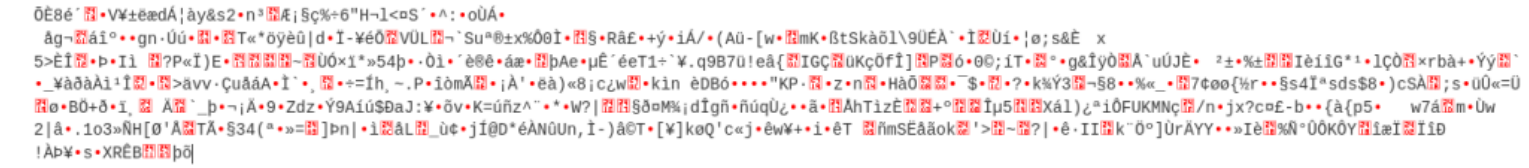
=> nothing

9. check for POSTs by IN2

ip[.]addr == 10[.]8[.]15[.]133 and ip[.]addr == 72[.]5[.]43[.]29 and http[.]request[.]method == POST

No.	Time	Source	Destination	Protocol	Length	Info
11032	197.064004	10.8.15.133	72.5.43.29	HTTP	649	POST / HTTP/1.1
11463	198.458033	10.8.15.133	72.5.43.29	HTTP	62	POST / HTTP/1.1
11496	199.060728	10.8.15.133	72.5.43.29	HTTP	786	POST / HTTP/1.1

10. analyze posted data



• doesn't seem to be encoded => maybe encrypted?

11. find how IN2 got infected

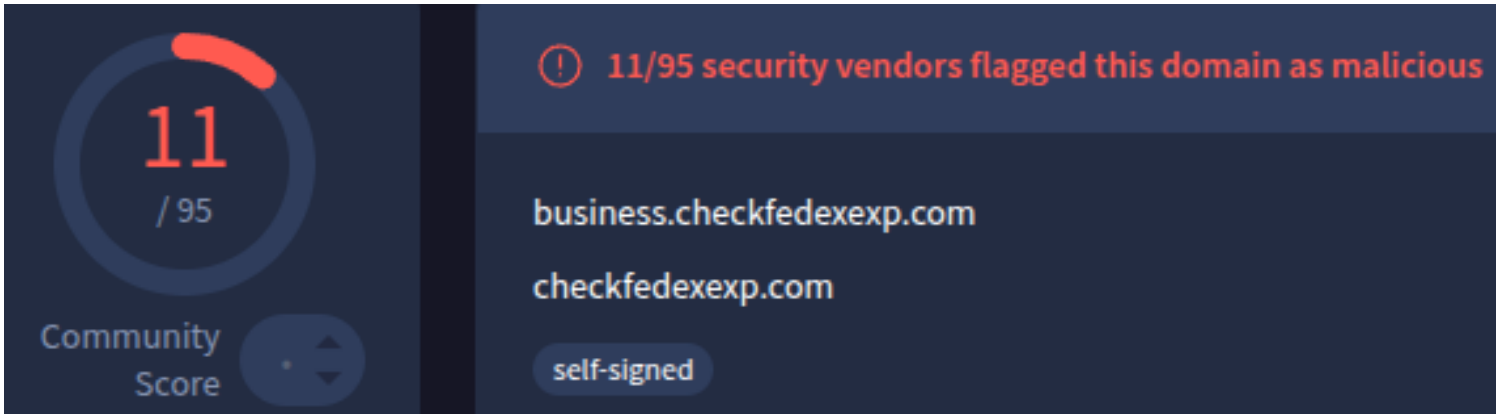
• check IN2 activity before contacting EX3

ip[.]src == 10[.]8[.]15[.]133 and frame[.]number <= 10598 and frame[.]number >= 9000 and dns

No.	Time	Source	Destination	Protocol	Length	Info
9026	100.165844	10.8.15.133	10.8.15.4	DNS	88	Standard query 0x762f A business.checkfedexexp.com
10193	101.909639	10.8.15.133	10.8.15.4	DNS	101	Standard query 0xe967 A msedge.b.tlu.dl.delivery.mp.microsoft.com
10235	109.974716	10.8.15.133	10.8.15.4	DNS	78	Standard query 0x9021 A edge.microsoft.com
10236	109.974862	10.8.15.133	10.8.15.4	DNS	78	Standard query 0xb0bc HTTPS edge.microsoft.com
10248	110.060608	10.8.15.133	10.8.15.4	ICMP	177	Destination unreachable (Port unreachable)
10281	122.680801	10.8.15.133	10.8.15.4	DNS	101	Standard query 0xadae A msedge.b.tlu.dl.delivery.mp.microsoft.com
10379	124.136436	10.8.15.133	10.8.15.4	DNS	85	Standard query 0x21e7 A login.microsoftonline.com
10406	125.016575	10.8.15.133	10.8.15.4	DNS	91	Standard query 0x037a A settings-win.data.microsoft.com

business[.]checkfedexexp[.]com

- investigate suspicious domain found



- find IP for suspicious domain

udp.stream eq 38

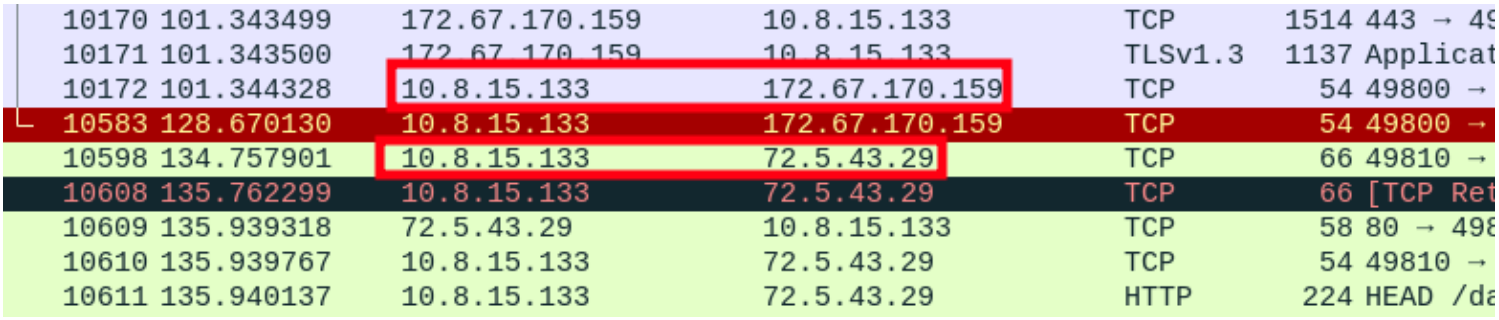
```
▾ Answers
  ▾ business.checkfedexexp.com: type A, class IN, addr 172.67.170.159
      Name: business.checkfedexexp.com
      Type: A (1) (Host Address)
      Class: IN (0x0001)
      Time to live: 300 (5 minutes)
      Data length: 4
      Address: 172.67.170.159
  ▾ business.checkfedexexp.com: type A, class IN, addr 104.21.55.70
      Name: business.checkfedexexp.com
      Type: A (1) (Host Address)
      Class: IN (0x0001)
      Time to live: 300 (5 minutes)
      Data length: 4
      Address: 104.21.55.70
```

172[.]67[.]170[.]159 - EX4

104[.]21[.]55[.]70 - EX5

- filter connection between IN2 and EX4

```
ip[.]addr ==10[.]8[.]15[.]133 and (ip[.]addr == 172[.]67[.]170[.]159 or ip[.]addr == 72[.]5[.]43[.]29)
```

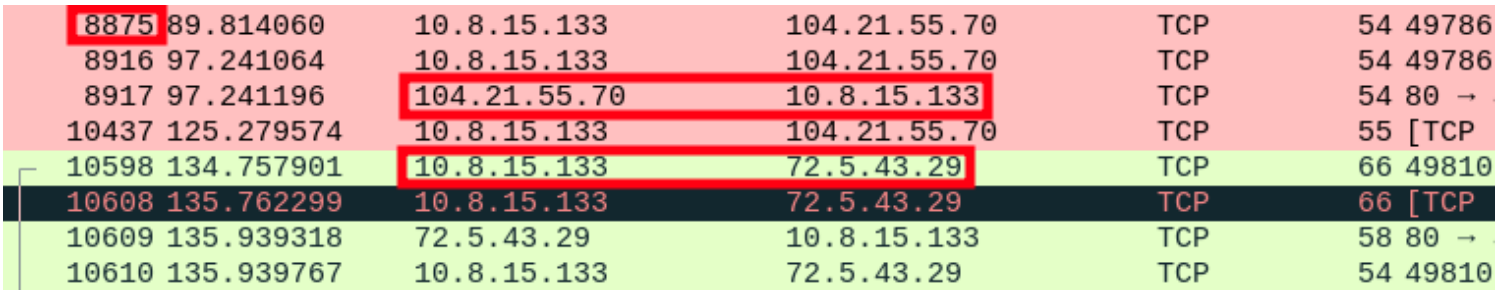


10170	101.343499	172.67.170.159	10.8.15.133	TCP	1514 443 → 49
10171	101.343500	172.67.170.159	10.8.15.133	TLSv1.3	1137 Applicat
10172	101.344328	10.8.15.133	172.67.170.159	TCP	54 49800 →
10583	128.670130	10.8.15.133	172.67.170.159	TCP	54 49800 →
10598	134.757901	10.8.15.133	72.5.43.29	TCP	66 49810 →
10608	135.762299	10.8.15.133	72.5.43.29	TCP	66 [TCP Ret
10609	135.939318	72.5.43.29	10.8.15.133	TCP	58 80 → 498
10610	135.939767	10.8.15.133	72.5.43.29	TCP	54 49810 →
10611	135.940137	10.8.15.133	72.5.43.29	HTTP	224 HEAD /da

IN2 contacts EX3 right after connection with EX4

• filter connection between IN2 and EX5

```
ip[.]addr ==10[.]8[.]15[.]133 and (ip[.]addr == 104[.]21[.]55[.]70 or ip[.]addr == 72[.]5[.]43[.]29)
```

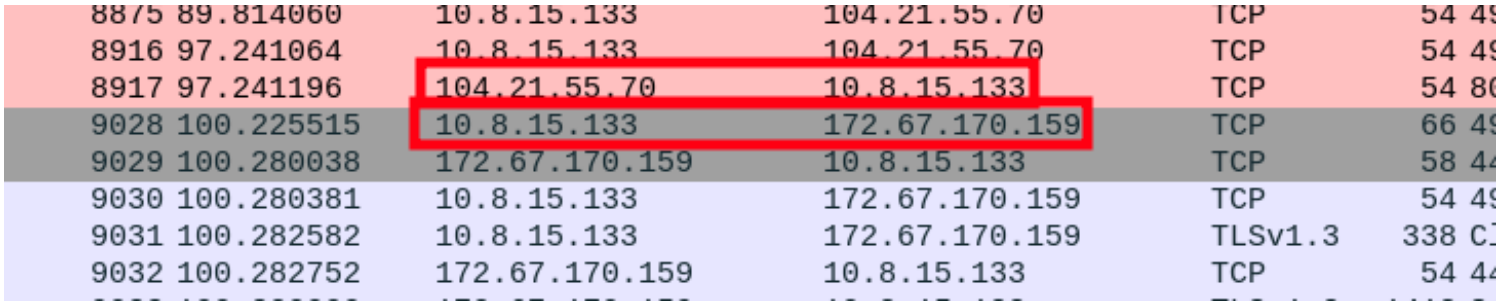


8875	89.814060	10.8.15.133	104.21.55.70	TCP	54 49786
8916	97.241064	10.8.15.133	104.21.55.70	TCP	54 49786
8917	97.241196	104.21.55.70	10.8.15.133	TCP	54 80 →
10437	125.279574	10.8.15.133	104.21.55.70	TCP	55 [TCP
10598	134.757901	10.8.15.133	72.5.43.29	TCP	66 49810
10608	135.762299	10.8.15.133	72.5.43.29	TCP	66 [TCP
10609	135.939318	72.5.43.29	10.8.15.133	TCP	58 80 →
10610	135.939767	10.8.15.133	72.5.43.29	TCP	54 49810

IN2 contacts EX5

• correlated EX4 and EX5

```
ip[.]addr ==10[.]8[.]15[.]133 and (ip[.]addr == 104[.]21[.]55[.]70 or ip[.]addr == 72[.]5[.]43[.]29 or ip[.]addr == 172[.]67[.]170[.]159)
```

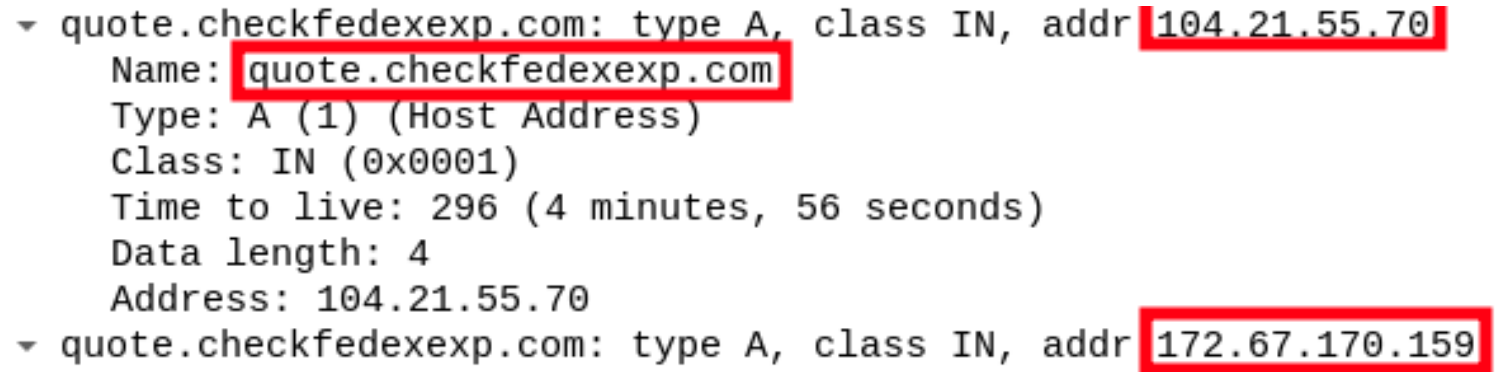


8875	89.814060	10.8.15.133	104.21.55.70	TCP	54 49
8916	97.241064	10.8.15.133	104.21.55.70	TCP	54 49
8917	97.241196	104.21.55.70	10.8.15.133	TCP	54 80
9028	100.225515	10.8.15.133	172.67.170.159	TCP	66 49
9029	100.280038	172.67.170.159	10.8.15.133	TCP	58 44
9030	100.280381	10.8.15.133	172.67.170.159	TCP	54 49
9031	100.282582	10.8.15.133	172.67.170.159	TLSv1.3	338 Cl
9032	100.282752	172.67.170.159	10.8.15.133	TCP	54 44

IN2 contacted EX5 then EX4 then EX3

• check how IN2 started contacting EX5

dns[.]a == 104[.]21[.]55[.]70

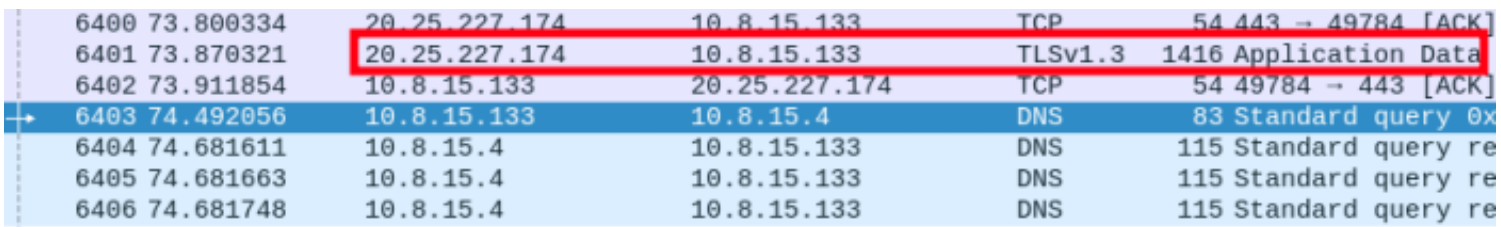


```
▾ quote.checkfedexexp.com: type A, class IN, addr 104.21.55.70
    Name: quote.checkfedexexp.com
    Type: A (1) (Host Address)
    Class: IN (0x0001)
    Time to live: 296 (4 minutes, 56 seconds)
    Data length: 4
    Address: 104.21.55.70
▾ quote.checkfedexexp.com: type A, class IN, addr 172.67.170.159
```

quote[.]checkfedexexp[.]com

• check activity right before

ip[.]addr == 10[.]8[.]15[.]133 and frame[.]number <= 6406 and frame[.]number >= 5000

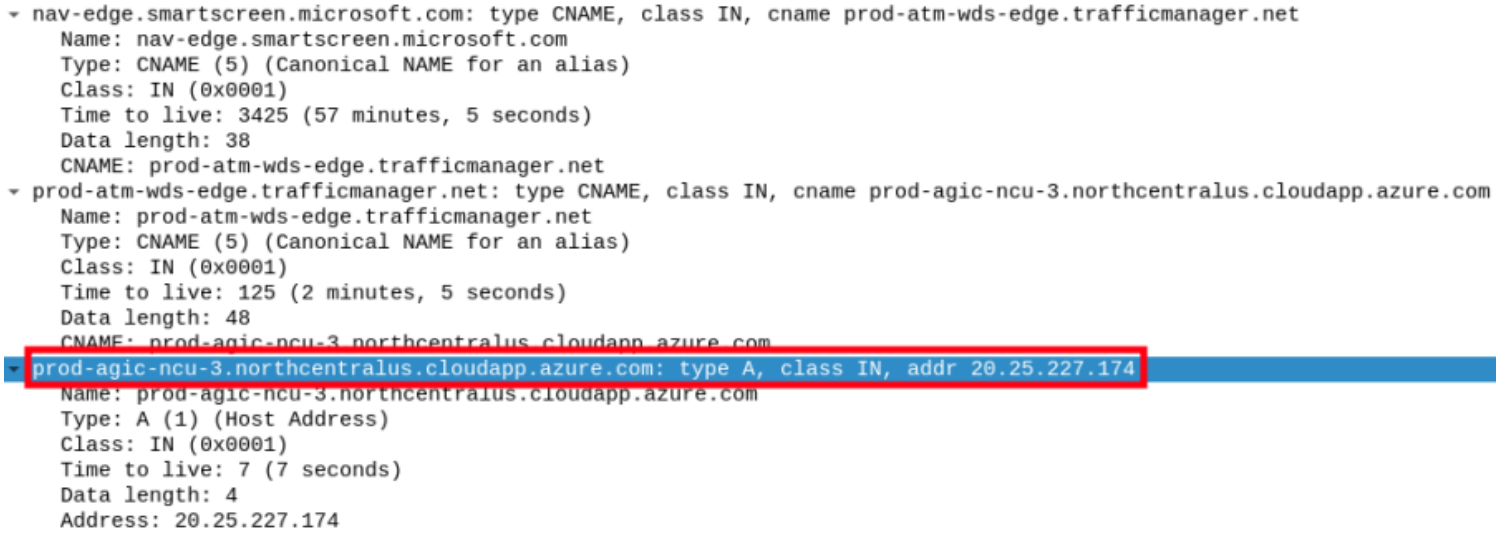


6400	73.800334	20.25.227.174	10.8.15.133	TCP	54 443 → 49784 [ACK]
6401	73.870321	20.25.227.174	10.8.15.133	TLSv1.3	1416 Application Data
6402	73.911854	10.8.15.133	20.25.227.174	TCP	54 49784 → 443 [ACK]
6403	74.492056	10.8.15.133	10.8.15.4	DNS	83 Standard query 0x
6404	74.681611	10.8.15.4	10.8.15.133	DNS	115 Standard query re
6405	74.681663	10.8.15.4	10.8.15.133	DNS	115 Standard query re
6406	74.681748	10.8.15.4	10.8.15.133	DNS	115 Standard query re

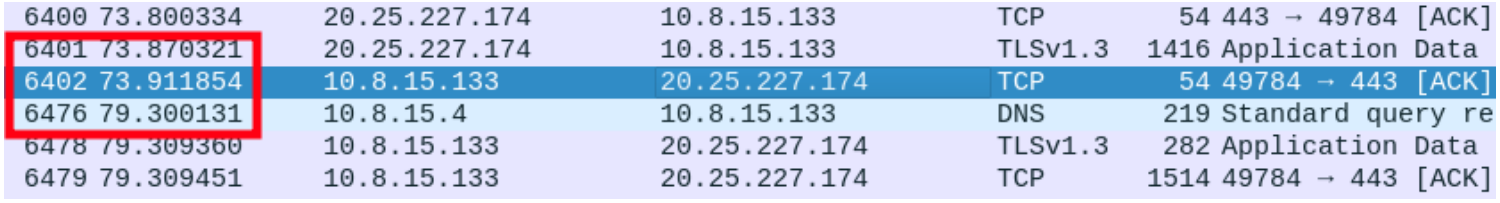
20[.]25[.]227[.]174 - EX6

• check DNS query for EX6

```
dns[.]a == 20[.]25[.]227[.]174 or (ip[.]addr == 10[.]8[.]15[.]133 and ip[.]addr == 20[.]25[.]227[.]174)
```



nav-edge[.]smartscreen[.]microsoft[.]com
prod-agic-ncu-3[.]northcentralus[.]cloudapp[.]azure[.]com
domain not malicious

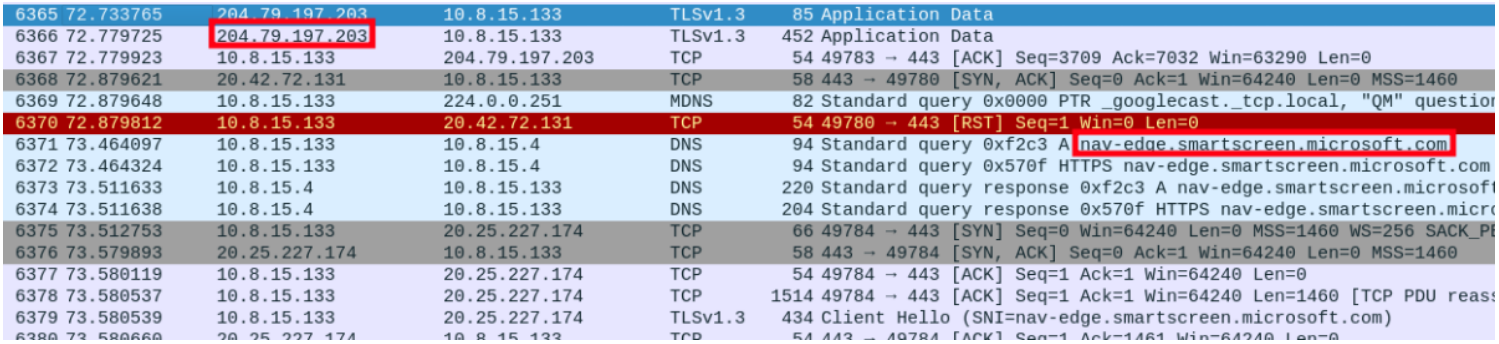


but stopping right before DNS query for quote[.]checkf-edexexp[.]com is suspicious

• investigate prod-agic-ncu-3[.]northcentralus[.]cloudapp[.]azure[.]com
=> nothing

• check what led to query for prod-agic-ncu-3[.]northcentralus[.]cloudapp[.]azure[.]com

```
ip[.]addr == 10[.]8[.]15[.]133 and frame[.]number <= 6500
```



6365	72.733765	204.79.197.203	10.8.15.133	TLSv1.3	85 Application Data
6366	72.779725	204.79.197.203	10.8.15.133	TLSv1.3	452 Application Data
6367	72.779923	10.8.15.133	204.79.197.203	TCP	54 49783 → 443 [ACK] Seq=3709 Ack=7032 Win=63290 Len=0
6368	72.879621	20.42.72.131	10.8.15.133	TCP	58 443 → 49780 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
6369	72.879648	10.8.15.133	224.0.0.251	MDNS	82 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
6370	72.879812	10.8.15.133	20.42.72.131	TCP	54 49780 → 443 [RST] Seq=1 Win=0 Len=0
6371	73.464097	10.8.15.133	10.8.15.4	DNS	94 Standard query 0xf2c3 A nav-edge.smartscreen.microsoft.com
6372	73.464324	10.8.15.133	10.8.15.4	DNS	94 Standard query 0x570f HTTPS nav-edge.smartscreen.microsoft.com
6373	73.511633	10.8.15.4	10.8.15.133	DNS	220 Standard query response 0xf2c3 A nav-edge.smartscreen.microsoft
6374	73.511638	10.8.15.4	10.8.15.133	DNS	204 Standard query response 0x570f HTTPS nav-edge.smartscreen.micro
6375	73.512753	10.8.15.133	20.25.227.174	TCP	66 49784 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PE
6376	73.579893	20.25.227.174	10.8.15.133	TCP	58 443 → 49784 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
6377	73.580119	10.8.15.133	20.25.227.174	TCP	54 49784 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
6378	73.580537	10.8.15.133	20.25.227.174	TCP	1514 49784 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=1460 [TCP PDU reass
6379	73.580539	10.8.15.133	20.25.227.174	TLSv1.3	434 Client Hello (SNI=nav-edge.smartscreen.microsoft.com)
6380	73.580660	20.25.227.174	10.8.15.133	TCP	54 443 → 49784 [ACK] Seq=1 Ack=1461 Win=64240 Len=0

204[.]79[.]197[.]203 - EX7

IN2 stops contacting EX7 right before DNS query for nav-edge[.]smartscreen[.]microsoft[.]com

• find query for EX7

```
dns[.]a == 204[.]79[.]197[.]203
```

```
▾ windows.msn.com: type CNAME, class IN, cname www-msn-com.a-0003.a-msedge.net
    Name: windows.msn.com
    Type: CNAME (5) (Canonical NAME for an alias)
    Class: IN (0x0001)
    Time to live: 497 (8 minutes, 17 seconds)
    Data length: 33
    CNAME: www-msn-com.a-0003.a-msedge.net
▾ www-msn-com.a-0003.a-msedge.net: type CNAME, class IN, cname a-0003.a-msedge.net
    Name: www-msn-com.a-0003.a-msedge.net
    Type: CNAME (5) (Canonical NAME for an alias)
    Class: IN (0x0001)
    Time to live: 120 (2 minutes)
    Data length: 2
    CNAME: a-0003.a-msedge.net
▾ a-0003.a-msedge.net: type A, class IN, addr 204.79.197.203
    Name: a-0003.a-msedge.net
    Type: A (1) (Host Address)
    Class: IN (0x0001)
    Time to live: 120 (2 minutes)
    Data length: 4
    Address: 204.79.197.203
```

windows[.]msn[.]com
non-malicious domain

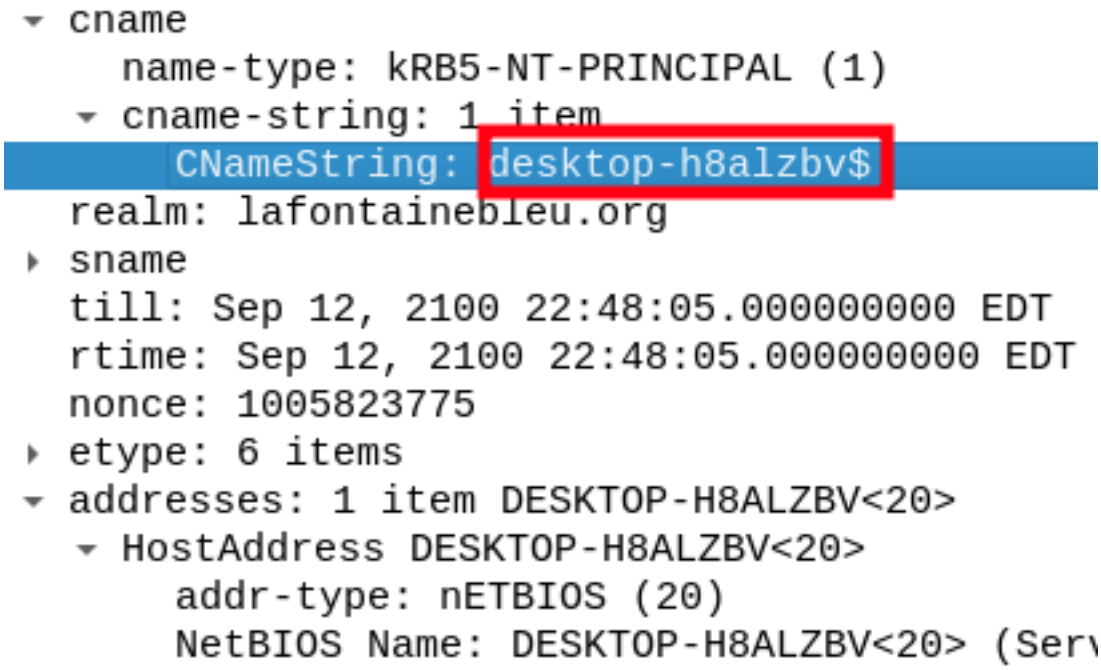
• find first instance of quote[.]checkfedexexp[.]com

dns[.]qry[.]name == quote[.]checkfedexexp[.]com

• check context
can't find any suspicious domains

12. find victim information

ip[.]addr == 10[.]8[.]15[.]133 and kerberos[.]CNameString



machine is authenticating, not user..