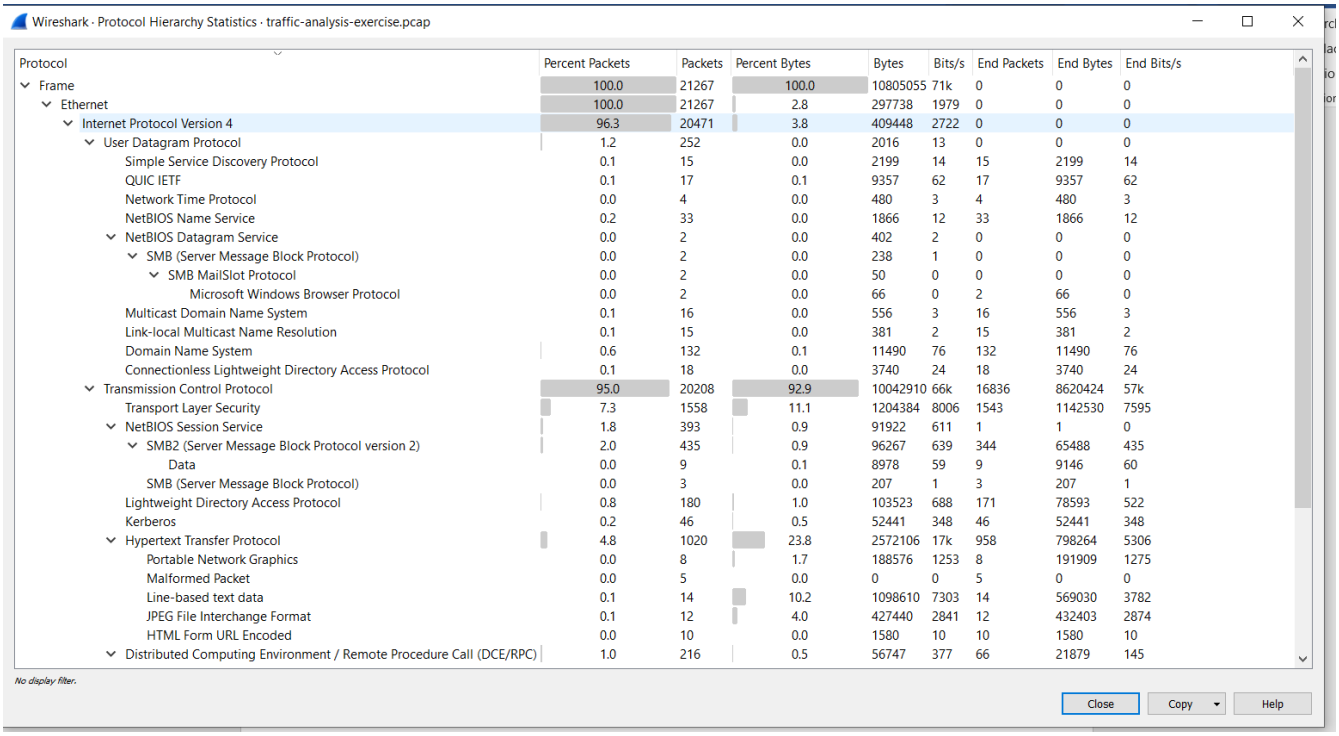
Sécurité SI

Wireshark

Auteur : Haraki Youness

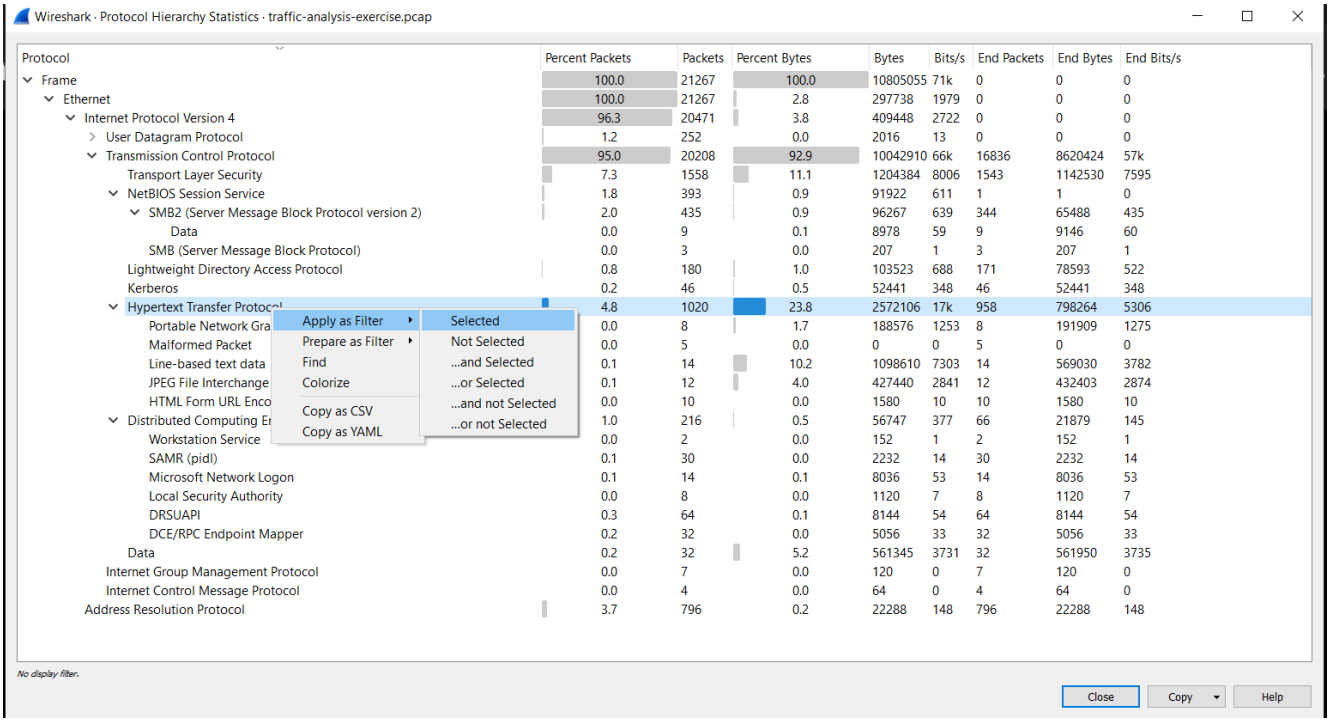
Looking at the hierarchy protocol we understand that all the traffic is IPV4; And mostly a TCP protocol.

We have high activity of hypertext transfer protocol; which indicates that this related to web traffic.



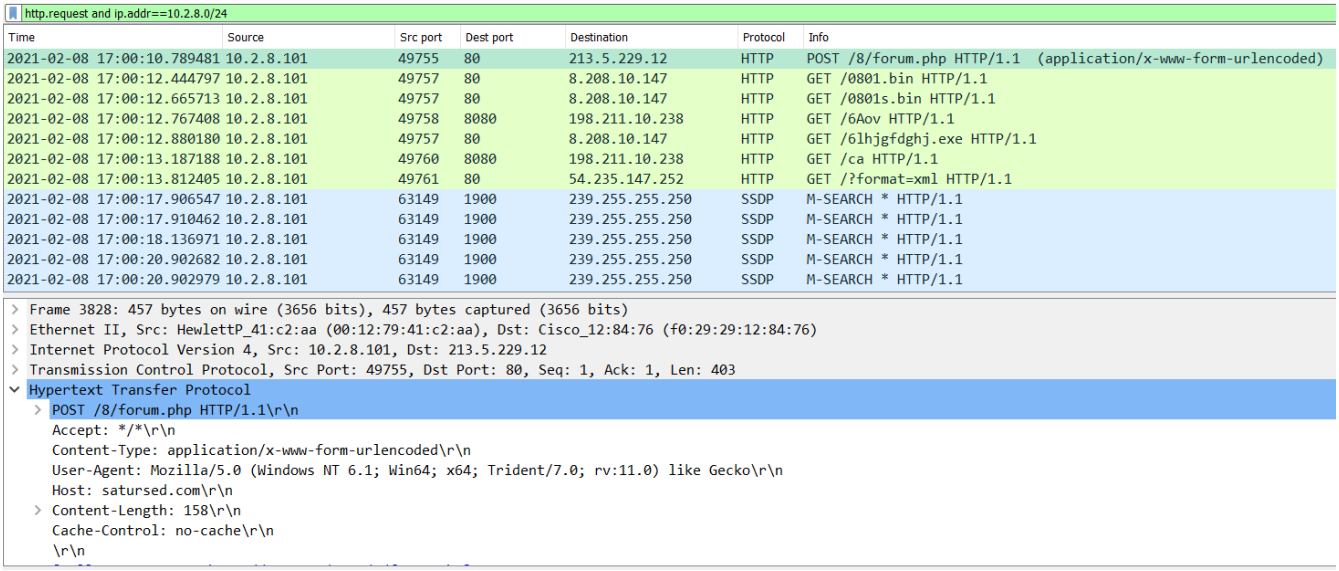
Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	21267	100.0	10805055	71k	0	0	0
Ethernet	100.0	21267	2.8	297738	1979	0	0	0
Internet Protocol Version 4	96.3	20471	3.8	409448	2722	0	0	0
User Datagram Protocol	1.2	252	0.0	2016	13	0	0	0
Simple Service Discovery Protocol	0.1	15	0.0	2199	14	15	2199	14
QUIC IETF	0.1	17	0.1	9357	62	17	9357	62
Network Time Protocol	0.0	4	0.0	480	3	4	480	3
NetBIOS Name Service	0.2	33	0.0	1866	12	33	1866	12
NetBIOS Datagram Service	0.0	2	0.0	402	2	0	0	0
SMB (Server Message Block Protocol)	0.0	2	0.0	238	1	0	0	0
SMB MailSlot Protocol	0.0	2	0.0	50	0	0	0	0
Microsoft Windows Browser Protocol	0.0	2	0.0	66	0	2	66	0
Multicast Domain Name System	0.1	16	0.0	556	3	16	556	3
Link-local Multicast Name Resolution	0.1	15	0.0	381	2	15	381	2
Domain Name System	0.6	132	0.1	11490	76	132	11490	76
Connectionless Lightweight Directory Access Protocol	0.1	18	0.0	3740	24	18	3740	24
Transmission Control Protocol	95.0	20208	92.9	10042910	66k	16836	8620424	57k
Transport Layer Security	7.3	1558	11.1	1204384	8006	1543	1142530	7595
NetBIOS Session Service	1.8	393	0.9	91922	611	1	1	0
SMB2 (Server Message Block Protocol version 2)	2.0	435	0.9	96267	639	344	65488	435
Data	0.0	9	0.1	8978	59	9	9146	60
SMB (Server Message Block Protocol)	0.0	3	0.0	207	1	3	207	1
Lightweight Directory Access Protocol	0.8	180	1.0	103523	688	171	78593	522
Kerberos	0.2	46	0.5	52441	348	46	52441	348
Hypertext Transfer Protocol	4.8	1020	23.8	2572106	17k	958	798264	5306
Portable Network Graphics	0.0	8	1.7	188576	1253	8	191909	1275
Malformed Packet	0.0	5	0.0	0	0	5	0	0
Line-based text data	0.1	14	10.2	1098610	7303	14	569030	3782
JPEG File Interchange Format	0.1	12	4.0	427440	2841	12	432403	2874
HTML Form URL Encoded	0.0	10	0.0	1580	10	10	1580	10
Distributed Computing Environment / Remote Procedure Call (DCE/RPC)	1.0	216	0.5	56747	377	66	21879	145

We show all the http traffic

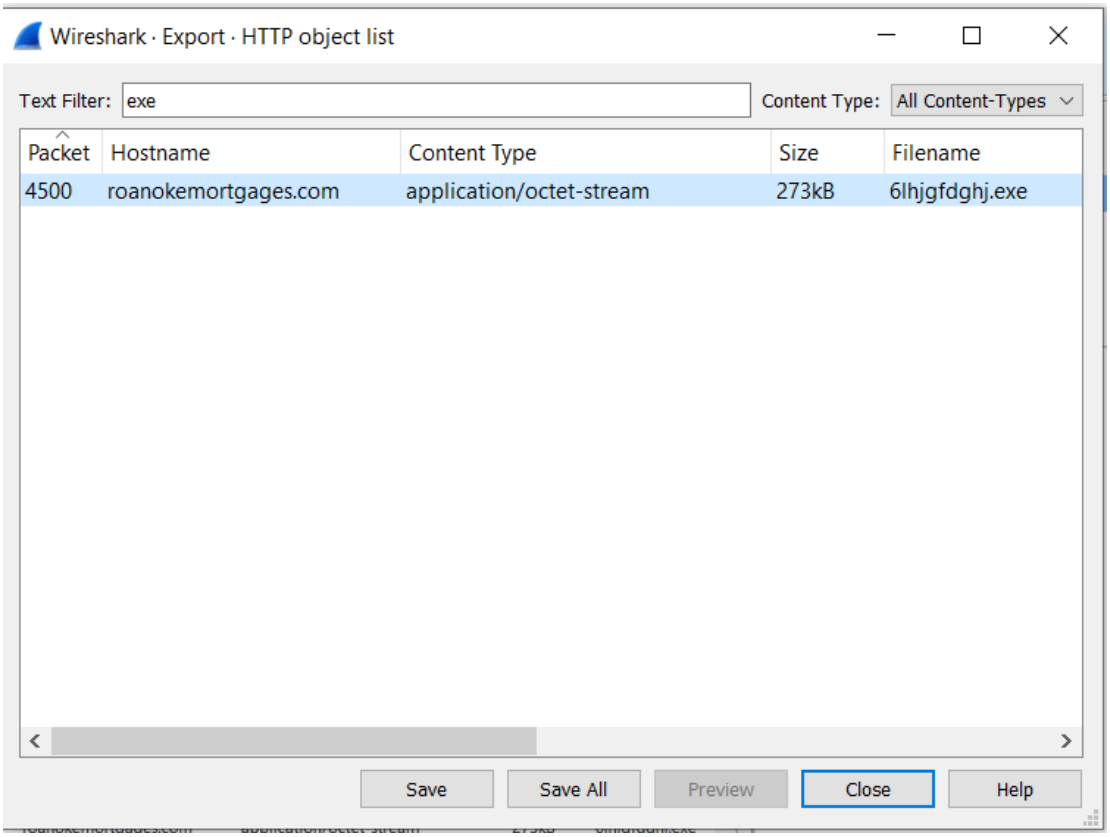


Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	21267	100.0	10805055	71k	0	0	0
Ethernet	100.0	21267	2.8	297738	1979	0	0	0
Internet Protocol Version 4	96.3	20471	3.8	409448	2722	0	0	0
User Datagram Protocol	1.2	252	0.0	2016	13	0	0	0
Transmission Control Protocol	95.0	20208	92.9	10042910	66k	16836	8620424	57k
Transport Layer Security	7.3	1558	11.1	1204384	8006	1543	1142530	7595
NetBIOS Session Service	1.8	393	0.9	91922	611	1	1	0
SMB2 (Server Message Block Protocol version 2)	2.0	435	0.9	96267	639	344	65488	435
Data	0.0	9	0.1	8978	59	9	9146	60
SMB (Server Message Block Protocol)	0.0	3	0.0	207	1	3	207	1
Lightweight Directory Access Protocol	0.8	180	1.0	103523	688	171	78593	522
Kerberos	0.2	46	0.5	52441	348	46	52441	348
Hypertext Transfer Protocol	4.8	1020	23.8	2572106	17k	958	798264	5306
Portable Network Gra	0.0	8	1.7	188576	1253	8	191909	1275
Malformed Packet	0.0	5	0.0	0	0	5	0	0
Line-based text data	0.1	14	10.2	1098610	7303	14	569030	3782
JPEG File Interchange	0.1	12	4.0	427440	2841	12	432403	2874
HTML Form URL Enco	0.0	10	0.0	1580	10	10	1580	10
Distributed Computing En	1.0	216	0.5	56747	377	66	21879	145
Workstation Service	0.0	2	0.0	152	1	2	152	1
SAMR (pidl)	0.1	30	0.0	2232	14	30	2232	14
Microsoft Network Logon	0.1	14	0.1	8036	53	14	8036	53
Local Security Authority	0.0	8	0.0	1120	7	8	1120	7
DRSUAPI	0.3	64	0.1	8144	54	64	8144	54
DCE/RPC Endpoint Mapper	0.2	32	0.0	5056	33	32	5056	33
Data	0.2	32	5.2	561345	3731	32	561950	3735
Internet Group Management Protocol	0.0	7	0.0	120	0	7	120	0
Internet Control Message Protocol	0.0	4	0.0	64	0	4	64	0
Address Resolution Protocol	3.7	796	0.2	22288	148	796	22288	148

We apply filers



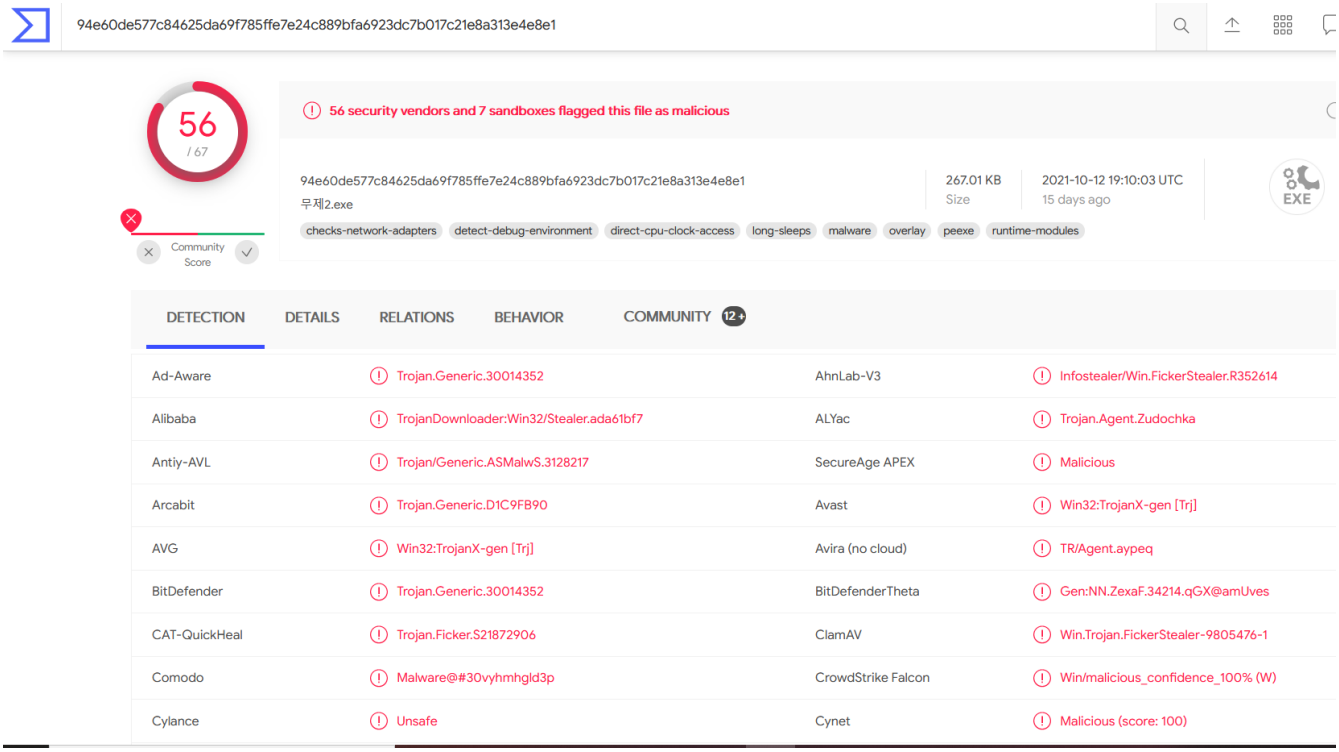
We save the suspicious files



We generate the hash code using **HashMyFile** ; in order to not divulge any sensitive information while testing the file for any malware (For ex: exporting files to VirusTotal)

HashCode: 77be0dd6570301acac3634801676b5d7

We test the HashCode with **VirusTotal**; which is an analyser for suspicious files and URLs to detect types of malwares, and automatically share them with the security community.



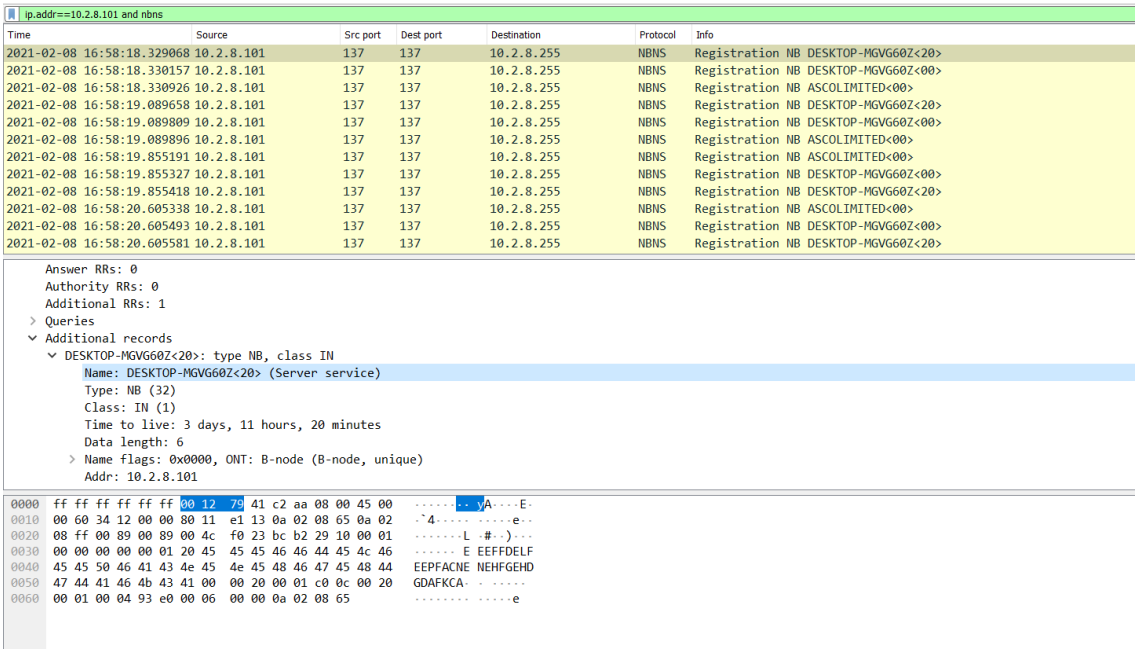
We can obviously see that the file is infected by a **Trojan**, and is categorized as unsafe.

Trojan

A Trojan horse, often known as a Trojan, is malicious malware or software that appears to be legal yet has the ability to take control of your computer. A Trojan is a computer program that is designed to hurt, disrupt, steal, or otherwise harm your data or network.

To deceive you, a Trojan masquerade as a legitimate application or file. It tries to trick you into downloading and running malware on your device. Once installed, a Trojan can carry out the function for which it was created. A Trojan is also known as a Trojan horse virus or a Trojan virus, but this is a misnomer. Viruses have the ability to execute and replicate. A Trojan is unable to do so. Trojans must be executed by the user.

Finding Hostname



ip.addr==10.2.8.101 and nbns

Time	Source	Src port	Dest port	Destination	Protocol	Info
2021-02-08 16:58:18.329068	10.2.8.101	137	137	10.2.8.255	NBNS	Registration NB DESKTOP-MGVG60Z<20>
2021-02-08 16:58:18.330157	10.2.8.101	137	137	10.2.8.255	NBNS	Registration NB DESKTOP-MGVG60Z<00>
2021-02-08 16:58:18.330926	10.2.8.101	137	137	10.2.8.255	NBNS	Registration NB ASCOLIMITED<00>
2021-02-08 16:58:19.089658	10.2.8.101	137	137	10.2.8.255	NBNS	Registration NB DESKTOP-MGVG60Z<20>
2021-02-08 16:58:19.089809	10.2.8.101	137	137	10.2.8.255	NBNS	Registration NB DESKTOP-MGVG60Z<00>
2021-02-08 16:58:19.089896	10.2.8.101	137	137	10.2.8.255	NBNS	Registration NB ASCOLIMITED<00>
2021-02-08 16:58:19.855191	10.2.8.101	137	137	10.2.8.255	NBNS	Registration NB ASCOLIMITED<00>
2021-02-08 16:58:19.855327	10.2.8.101	137	137	10.2.8.255	NBNS	Registration NB DESKTOP-MGVG60Z<00>
2021-02-08 16:58:19.855418	10.2.8.101	137	137	10.2.8.255	NBNS	Registration NB DESKTOP-MGVG60Z<20>
2021-02-08 16:58:20.605338	10.2.8.101	137	137	10.2.8.255	NBNS	Registration NB ASCOLIMITED<00>
2021-02-08 16:58:20.605493	10.2.8.101	137	137	10.2.8.255	NBNS	Registration NB DESKTOP-MGVG60Z<00>
2021-02-08 16:58:20.605581	10.2.8.101	137	137	10.2.8.255	NBNS	Registration NB DESKTOP-MGVG60Z<20>

```
Answer RRs: 0
Authority RRs: 0
Additional RRs: 1
> Queries
v Additional records
  v DESKTOP-MGVG60Z<20>: type NB, class IN
      Name: DESKTOP-MGVG60Z<20> (Server service)
      Type: NB (32)
      Class: IN (1)
      Time to live: 3 days, 11 hours, 20 minutes
      Data length: 6
    > Name flags: 0x0000, ONT: B-node (B-node, unique)
      Addr: 10.2.8.101
```

```
0000  ff ff ff ff ff ff 00 12  79 41 c2 aa 08 00 45 00   ······ ·· yA····E·
0010  00 60 34 12 00 00 80 11  e1 13 0a 02 08 65 0a 02   ·`4····· ·····e··
0020  08 ff 00 89 00 89 00 4c  f0 23 bc b2 29 10 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 45 48 46 47 45 48 44   EEPFACNE NEHFGEHD
0050  47 44 41 46 4b 43 41 00  00 20 00 01 c0 0c 00 20   GDAFKCA· · ·····
0060  00 01 00 04 93 e0 00 06  00 00 0a 02 08 65         ·------- -----e
```

Summary

infected website

URL: roanokemortgages.com

IP Address: 8.208.10.147

Infection: Trojan malware on downloaded file ‘6lhjgfdghj.exe’

Infected machine

IP Address: 10.2.8.101

MAC address: 00:12:79:41:c2:aa

User Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko

Hostname: DESKTOP-MGVG60Z<20> (Server service)

Signature of infected file: 77be0dd6570301acac3634801676b5d7