

Network Threat Analysis and Mitigation

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.

This screenshot shows the Pestudio interface with the following details:

- File Path:** c:\users\brandoon\lmao\Desktop\cyb 528 final1.pcap
- File Type:** traffic.pcap
- Analysis Results:**
 - Properties:** sha256: 4569f5d98ca57d2e937b4ea6820d256a360fd608a439bfdb297df148ff06f94b4
 - CPU:** 64-bit
 - File Type:** dynamic-link-library
 - Subsystem:** Native
 - Entry Point:** 0x000029C0
 - Signature:** n/a
- Scan Results:** 4/59
- Details:** The properties panel lists various file metadata such as indicators, file size, entropy, and file type.

This screenshot shows the Pestudio interface with the following details:

- File Path:** c:\users\brandoon\lmao\Desktop\cyb 528 final1.pcap
- File Type:** traffic.pcap
- Analysis Results:**
 - Indicators:** 32
 - Score:** 4/59
 - Details:** The indicator section lists numerous suspicious findings, such as file checksums, API registry references, and URL patterns, along with their respective scores (1-4).
- Scan Results:** 4/59
- Details:** The indicators panel lists specific findings with their corresponding scores and details.

pestudio 9.09 - Malware Initial Assessment - www.winitor.com [c:\users\brandoon lmao\Desktop\cyb 528 final\1.pcap\traffic.pcap]

file settings about

engine (59/59)	score (4/59)	date (dd.mm.yyyy)	age (days)
Cyren	W64/Kryptik.DQZ.gen[Eldorado]	22.03.2021	51
Avast	Win64:MalwareX-gen [Trj]	23.03.2021	50
Microsoft	Program:Win32/Wacapew.Clml	22.03.2021	51
AVG	Win64:MalwareX-gen [Trj]	23.03.2021	50
Bkav	clean	22.03.2021	51
TotalDefense	clean	22.03.2021	51
ClamAV	clean	22.03.2021	51
CMC	clean	12.03.2021	61
CAT-QuickHeal	clean	22.03.2021	51
McAfee	clean	22.03.2021	51
Malwarebytes	clean	22.03.2021	51
VIPRE	clean	22.03.2021	51
SUPERAntiSpyware	clean	19.03.2021	54
Sangfor	clean	18.03.2021	55
K7AntiVirus	clean	22.03.2021	51
K7GW	clean	22.03.2021	51
Baidu	clean	18.03.2019	786
ESET-NOD32	clean	22.03.2021	51
TrendMicro-HouseCall	clean	22.03.2021	51
Cynet	clean	22.03.2021	51
Kaspersky	clean	22.03.2021	51
BitDefender	clean	22.03.2021	51
NANO-Antivirus	clean	23.03.2021	50
ViRobot	clean	22.03.2021	51
MicroWorld-eScan	clean	23.03.2021	50
Tencent	clean	23.03.2021	50
Ad-Aware	clean	22.03.2021	51
Emsisoft	clean	22.03.2021	51
Comodo	clean	22.03.2021	51
F-Secure	clean	22.03.2021	51

sha256: 4569f5d98ca57d2e937b4ea6820d256a36dfd608439bfd6297df148ff06f94b4

cpu: 64-bit file-type: dynamic-link-library subsystem: Native entry-point: 0x000029C0 signature: n/a

VirusTotal

virustotal.com/gui/file/4569f5d98ca57d2e937b4ea6820d256a36dfd608439bfd6297df148ff06f94b4/detection

4 security vendors flagged this file as malicious

4569f5d98ca57d2e937b4ea6820d256a36dfd608439bfd6297df148ff06f94b4

2021-03-19-iccid-ID-infection-traffic-carved.pcap

3.50 MB Size 2021-03-23 01:03:46 UTC 1 month ago CAP

Community Score: 4 / 59

DETECTION	DETAILS	COMMUNITY
Avast	① Win64:MalwareX-gen [Trj]	Avg ① Win64:MalwareX-gen [Trj]
Cyren	① W64/Kryptik.DQZ.gen[Eldorado]	Microsoft ① Program:Win32/Wacapew.Clml
Ad-Aware	Undetected	AegisLab Undetected
AhnLab-V3	Undetected	ALYac Undetected
Antiy-AVL	Undetected	Arcabit Undetected
Avira (no cloud)	Undetected	Baidu BitDefenderTheta Undetected

<https://www.virustotal.com/gui/file/4569f5d98ca57d2e937b4ea6820d256a36dfd608439bfd6297df148ff06f94b4/detection>

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 from 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.

The image displays two instances of the Wireshark application interface. Both instances show a list of network packets, a detailed packet list pane, a bytes/ascii dump pane, and a status bar at the bottom.

Top Wireshark Instance (General Capture):

- Packets:** 4161
- Displayed:** 4161 (100.0%)
- Profile:** Default
- Protocol:** TCP, HTTP, TLS, DNS
- Summary:** Shows a sequence of TCP connections between 10.3.19.101 and 188.127.237.152, with various ACK and SYN segments.
- Details:** Shows the raw hex and ASCII data for each packet.

Bottom Wireshark Instance (TLS Filtered Capture):

- Packets:** 4161
- Displayed:** 4161 (100.0%)
- Profile:** Default
- Protocol:** TLSv1.2
- Summary:** Shows a sequence of TLSv1.2 Application Data frames between 10.3.19.101 and 165.227.28.47.
- Details:** Shows the raw hex and ASCII data for each TLS frame.

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.

No.	Time	Source	Destination	Protocol	Host	Info
4	2021-03-19 08:49:07.651637	10.3.19.101	188.127.237.152	HTTP	188.127.237.152	GET /44274.6591174769.dat HTTP/1.1
111	2021-03-19 08:49:08.676929	10.3.19.101	185.82.219.225	HTTP	185.82.219.225	GET /44274.6591174769.dat HTTP/1.1
484	2021-03-19 08:49:52.506409	10.3.19.101	178.128.243.14	HTTP	calldivorce.fun	GET / HTTP/1.1
1210	2021-03-19 08:49:55.736856	10.3.19.101	178.128.243.14	HTTP	calldivorce.fun	GET / HTTP/1.1

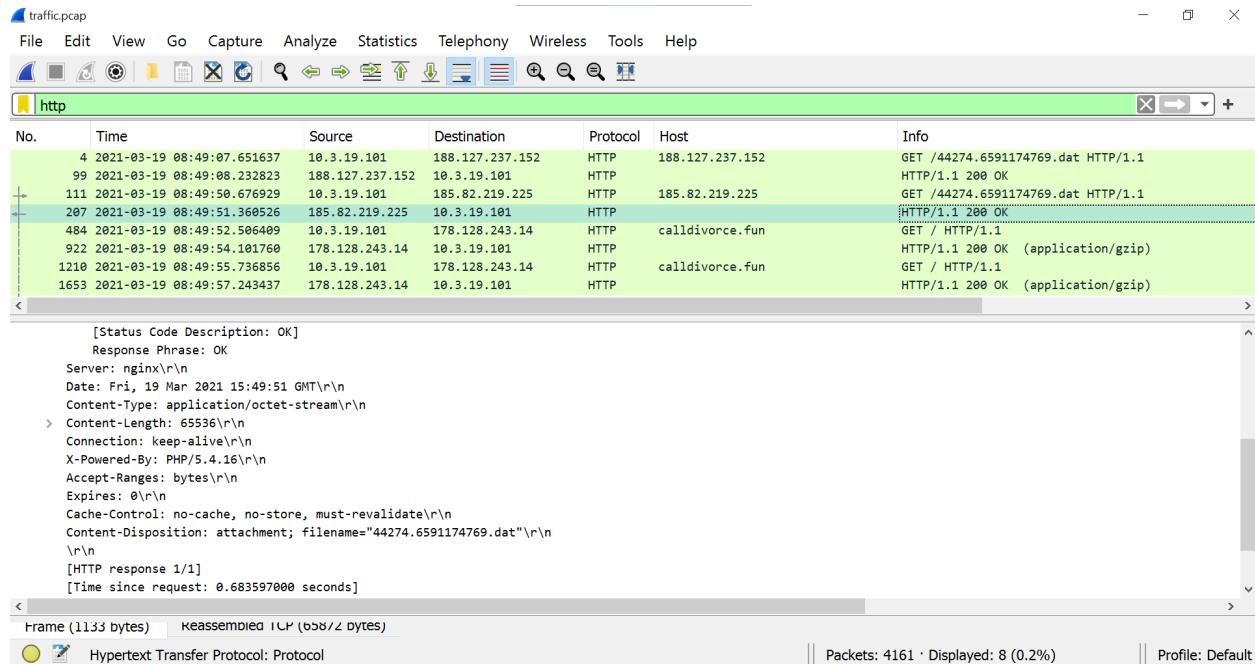
```

> Frame 484: 297 bytes on wire (2376 bits), 297 bytes captured (2376 bits)
> Ethernet II, Src: HewlettP_1c:47:ae (00:08:02:1c:47:ae), Dst: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1)
> Internet Protocol Version 4, Src: 10.3.19.101, Dst: 178.128.243.14
> Transmission Control Protocol, Src Port: 49232, Dst Port: 80, Seq: 1, Ack: 1, Len: 243
< Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    Connection: Keep-Alive\r\n
  > Cookie: __gads=20460581:670:40; __gat=6.1.7601.64; __ga=5.67194.576.8; __u=484F4D452D555345522D5043:686F6D652E75736572; __io=21_708424023_1356261834_1826261823; __gid=42E
    Host: calldivorce.fun\r\n
    \r\n
    [Full request URI: http://calldivorce.fun/]
    [HTTP request 1/1]
    [Response in frame: 922]
  
```

No.	Time	Source	Destination	Protocol	Host	Info
4	2021-03-19 08:49:07.651637	10.3.19.101	188.127.237.152	HTTP	188.127.237.152	GET /44274.6591174769.dat HTTP/1.1
99	2021-03-19 08:49:08.232823	188.127.237.152	10.3.19.101	HTTP		HTTP/1.1 200 OK
111	2021-03-19 08:49:08.676929	10.3.19.101	185.82.219.225	HTTP	185.82.219.225	GET /44274.6591174769.dat HTTP/1.1
207	2021-03-19 08:49:51.360526	185.82.219.225	10.3.19.101	HTTP		HTTP/1.1 200 OK
484	2021-03-19 08:49:52.506409	10.3.19.101	178.128.243.14	HTTP	calldivorce.fun	GET / HTTP/1.1
922	2021-03-19 08:49:54.101760	178.128.243.14	10.3.19.101	HTTP		HTTP/1.1 200 OK (application/gzip)
1210	2021-03-19 08:49:55.736856	10.3.19.101	178.128.243.14	HTTP	calldivorce.fun	GET / HTTP/1.1
1653	2021-03-19 08:49:57.243437	178.128.243.14	10.3.19.101	HTTP		HTTP/1.1 200 OK (application/gzip)

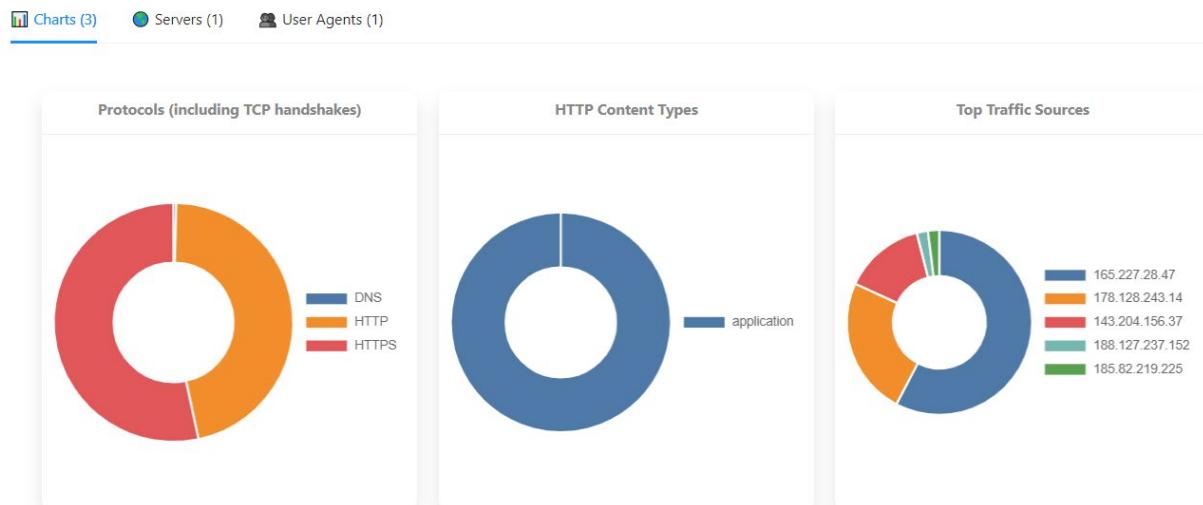
```

< [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
  [HTTP/1.1 200 OK\r\n]
  [Severity level: Chat]
  [Group: Sequence]
  Response Version: HTTP/1.1
  Status Code: 200
  [Status Code Description: OK]
  Response Phrase: OK
  Server: nginx\r\n
  Date: Fri, 19 Mar 2021 15:49:56 GMT\r\n
  Content-Type: application/gzip\r\n
  > Content-Length: 405224\r\n
  Connection: keep-alive\r\n
  \r\n
  [HTTP response 1/1]
  
```



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.



Charts (3) Servers (1) User Agents (1)

nginx

Charts (3) Servers (1) User Agents (1)

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)

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.

▼ 10.3.19.101:49230 ↲ 185.82.219.225:80 (GET)

▼ 10.3.19.101:49232 ↔ calldivorce.fun (178.128.243.14):80 (GET)

▼ 10.3.19.101:49235 ↔ calldivorce.fun (178.128.243.14):80 (GET)

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

← traffic.pcap Endpoint Stats

(Copy Link)

From	To	Bytes ▾
🇺🇸 agitopinaholop.uno (165.227.28.47)	10.3.19.101	2 Mb
🇨🇳 calldivorce.fun (178.128.243.14)	10.3.19.101	804 Kb
🇺🇸 dr49lng3n1n2s.cloudfront.net (143.204.156.37)	10.3.19.101	473 Kb
🇷🇺 188.127.237.152	10.3.19.101	66 Kb
🇷🇺 185.82.219.225	10.3.19.101	66 Kb
10.3.19.101	🇺🇸 agitopinaholop.uno (165.227.28.47)	33 Kb
10.3.19.101	🇨🇳 calldivorce.fun (178.128.243.14)	7 Kb
10.3.19.101	🇺🇸 dr49lng3n1n2s.cloudfront.net (143.204.156.37)	5 Kb
10.3.19.101	🇷🇺 188.127.237.152	2 Kb
10.3.19.101	🇷🇺 185.82.219.225	2 Kb

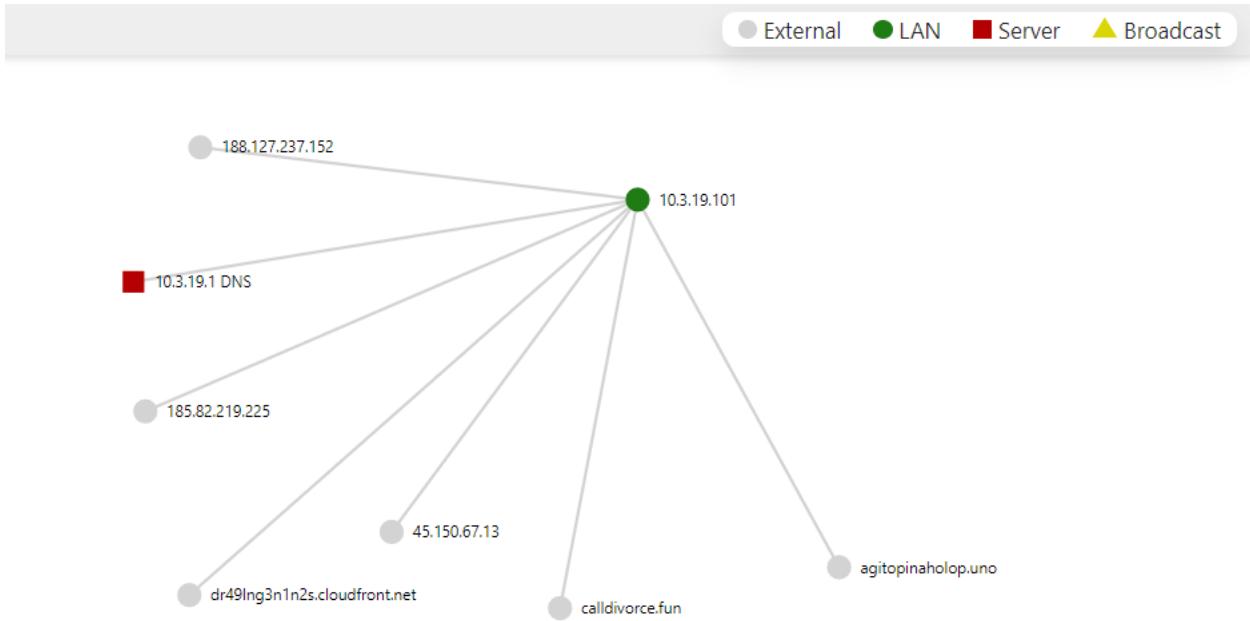
From	To	Bytes
10.3.19.1	10.3.19.101	665
10.3.19.101	10.3.19.1	427
10.3.19.101	45.150.67.13	184

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.

The screenshot shows the pestudio 9.09 interface. At the top, it says "pestudio 9.09 - Malware Initial Assessment - www.winitor.com [c:\users\brandoon\lmao\Desktop\cyb 528 final\2.artifacts\2021-03-19-binary-retreived-fromcalldivorce.fun.bin]". Below the menu bar, there's a toolbar with icons for file operations. The main area is a table with columns: "engine (58/58)", "score (0/58)", "date (dd.mm.yyyy)", and "age (days)". The table lists various antivirus engines with their results. At the bottom of the table, it says "sha256: C8CA58A0025A7AB633A35FE6E98943C9053CA49B18DE55F8B57C8EA7C88E8E00" and "signature: n/a".

engine (58/58)	score (0/58)	date (dd.mm.yyyy)	age (days)
Bkav	clean	23.04.2021	19
MicroWorld-eScan	clean	23.04.2021	19
FireEye	clean	23.04.2021	19
CAT-QuickHeal	clean	23.04.2021	19
McAfee	clean	23.04.2021	19
Malwarebytes	clean	23.04.2021	19
Zillya	clean	23.04.2021	19
Sangfor	clean	16.04.2021	26
K7AntiVirus	clean	23.04.2021	19
KTGW	clean	23.04.2021	19
Baidu	clean	18.03.2019	786
Cyren	clean	23.04.2021	19
Symantec	clean	23.04.2021	19
ESET-NOD32	clean	23.04.2021	19
TrendMicro-HouseCall	clean	23.04.2021	19
Avast	clean	23.04.2021	19
ClamAV	clean	23.04.2021	19
Kaspersky	clean	23.04.2021	19
BitDefender	clean	23.04.2021	19
NANO-Antivirus	clean	23.04.2021	19
ViRobot	clean	23.04.2021	19
SUPERAntiSpyware	clean	23.04.2021	19
Tencent	clean	24.04.2021	18
Ad-Aware	clean	23.04.2021	19
TACHYON	clean	24.04.2021	18
Sophos	clean	23.04.2021	19
Comodo	clean	23.04.2021	19
F-Secure	clean	31.03.2021	42
DrWeb	clean	23.04.2021	19
VIPRE	clean	23.04.2021	19

sha256: C8CA58A0025A7AB633A35FE6E98943C9053CA49B18DE55F8B57C8EA7C88E8E00 | signature: n/a

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Local
update_2046050.msi	0	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Allocated	unknown	/LogicalFileSet1/2021-03-19-binary-retreived-fromcalldivorce.fun.bin/update_2046050.msi

The screenshot shows the Autopsy interface with the "File Metadata" tab selected. It displays various file properties:

Name	/LogicalFileSet1/2021-03-19-binary-retreived-fromcalldivorce.fun.bin/update_2046050.msi
Type	Local
MIME Type	application/octet-stream
Size	0
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	d41d8cd98f00b204e9800998ecf8427e
SHA-256	e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855
Hash Lookup Results	UNKNOWN
Internal ID	3
Local Path	C:\CYB 528 Final\ModuleOutput\Embedded File Extractor\2021-03-19-binary-retreived-fromcalldivorce.fun.bin_2\0\0_update_2046050.msi

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

Hex		Text	Application	File Metadata	Context	Results	Annotations	Other Occurrences
Name		/LogicalFileSet1/2021-03-19-binary-retrieved-fromcaldivorce.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 LMa0\Desktop\CYB 528 Final\2.artifacts\2021-03-19-binary-retrieved-fromcaldivorce.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.artifacts\2021-03-19-scheduled-task-for-icedid.txt]

- X

file settings about

File: c:\users\brandoon lmao\desktop\cyb 528 final\2.artifacts\2021-03-19-scheduled-task-for-icedid.txt

Indicators (3)

- virustotal (2/58)
- abc 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.

pestudio 9.09 - Malware Initial Assessment - www.winitor.com [c:\users\brandoon\lmao\Desktop\cyb 528 final\2.artifacts\82025721897_03192021.xlsx]

file settings about

File indicators strings

virustotal (27/65)

abc strings (1449)

engine (65/65)	score (27/65)	date (dd.mm.yyyy)	age (days)
FireEye	Trojan.Vita.17	26.04.2021	16
CAT-QuickHeal	XLSDownloader.41785	25.04.2021	17
AegisLab	Trojan.MSOffice.SAgent.4lc	26.04.2021	16
Sangfor	Trojan.Generic-Script.Save.27b252f2	16.04.2021	26
BitDefender	Trojan.Vita.17	26.04.2021	16
Cyren	XLSM/Sneaky.P.gen!Camelot	26.04.2021	16
Symantec	Trojan.Gen.NPE	25.04.2021	17
ESET-NOD32	DOC/TrojanDownloader.Agent.CUL	26.04.2021	16
TrendMicro-HouseCall	TROJ_FRS.0NA104CM21	26.04.2021	16
Kaspersky	HEUR:Trojan.MSOffice.SAgent.gen	26.04.2021	16
Alibaba	TrojanDownloader:VBA/MalDoc.ali1000101	27.05.2019	716
ViRobot	XLS.Z.Agent.189684.A	26.04.2021	16
Tencent	Trojan.Win32.XmlMacroSheet.11003643	26.04.2021	16
Emsisoft	Trojan.Vita.17 (B)	26.04.2021	16
DrWeb	X97M.DownLoader.572	26.04.2021	16
McAfee-GW-Edition	X97M/Downloader.hk	25.04.2021	17
Sophos	Troy/DocDI-ACSP	25.04.2021	17
GData	Script.Trojan.Agent.AYH	26.04.2021	16
MAX	malware (ai score=87)	26.04.2021	16
Cynet	Malicious (score: 99)	12.04.2021	30
AhnLab-V3	Downloader/XML.XmlMacro.S1452	26.04.2021	16
ALYac	TrojanDownloader.XLS.gen	26.04.2021	16
Zoner	Probably Heur.W97ShellM	25.04.2021	17
Ikarus	Trojan-Downloader.Excel.Agent	25.04.2021	17
Fortinet	MSExcel/Agent.CTZltr	26.04.2021	16
AVG	SNIH:Script [Dropper]	26.04.2021	16
Bkav	clean	24.04.2021	18
MicroWorld-eScan	clean	26.04.2021	16
McAfee	clean	27.04.2021	15
Malwarebytes	clean	26.04.2021	16

signature: n/a

```
[Content_Types].xml          xl/drawings/drawing2.xml
c{f}                          NLI.E
0d'                           |CDGz|X
kxHOM                         |xb@
X|4M                           5|F8
_rels.rels                     |B|5!
BkwvAH                         Xr=p
GJyU                           p$&k
USH9i                          xl/drawings/drawing3.xml
r:_y_dl                         p|zMD*
xl/workbook.xml                =CJZ
yKfl                           ~Y_Z
e%6U5,                         <|t
<ds                           9-u|l
Ru_dV                           v|5Z|Ck
:Nwd                          A|v@
xl/_rels/workbook.xml.rels    ?w|hX
;u|Bh                          Er+O(
ul*=U`                         dbP-
(D5i                           xl/worksheets/_rels/sheet1.xml.rels
?a5~x                         )NVC<
;sdl                           xl/macrosheets/_rels/sheet1.xml.rels
xl/worksheets/sheet1.xml      ,NzF
(d|525                         /|R
;j|U                           xl/macrosheets/_rels/sheet2.xml.rels
:shf                           >@lfwCw!3
.L6g                           |VaBq
4L0~                           ^We0
i<QP                          xl/drawings/_rels/drawing1.xml.rels
xl/macrosheets/sheet1.xml     AA/;
$poa<E                         t4,X
*x7a|+                         |KE4|(
s|Na                           {yMl
LLf7                           xl/drawings/_rels/drawing2.xml.rels
S6)T                           AA/;
(Zv-T                           t4,X
n|Xe                           |KE4|(
JOP-s5                         {yMl
t+s5                           xl/drawings/_rels/drawing3.xml.rels
JOP-s5                         AA/;
TS0sWd                         t4,X
2A@ä                           |KE4|(
TjER                           {yMl
JOP%                           xl/printerSettings/printerSettings1.bin
JOP%                           P_G1
K3{                           P_G
1^m_P                           xl/printerSettings/printerSettings2.bin
LYD1                           P_G1
WG8Y                           P_G
LE@1                           docProps/core.xml
LE@1                           %jvr
LE@1Pe                         _IQ
/a1>                           .X<|k
sheoajp                        /qBC
}IN1z<                         docProps/app.xml
$5a@                           flUn3
CnmS                           WFgd:II
%+'%                           Is#;}
5{="                           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.

pestudio 9.09 - Malware Initial Assessment - www.winitor.com [c:\users\brandoon\lmao\Desktop\cyb 528 final\2.artifacts\kiod.hod]

File settings about

sha256: D1634C8DD16B4B1480065039FAC62D6C1900692F0CCC9BF52C8DDC65599FBF3D | cpu: 64-bit | file-type: dynamic-link-library | subsystem: Native | entry-point: 0x000029C0 | signature: n/a

engine (69/69)	score (47/69)	date (dd.mm.yyyy)	age (days)
Elastic	malicious (high confidence)	20.04.2021	22
MicroWorld-eScan	Trojan.GenericKDZ.T3610	26.04.2021	16
FireEye	Trojan.GenericKDZ.T3610	26.04.2021	16
CAT-QuickHeal	Trojan.Generic.CS.19393063	25.04.2021	17
ALYac	Trojan.IcedID.gen	26.04.2021	16
Cylance	Unsafe	26.04.2021	16
Zillya	Trojan.Kryptik.Win64.10772	26.04.2021	16
AegisLab	Trojan.Win32.Generic.4lc	26.04.2021	16
Sangfor	Trojan.Script.Phonyz.A	16.04.2021	26
CrowdStrike	win/malicious_confidence_-100% (W)	03.02.2021	98
Alibaba	Trojan.Win64/Kryptik.2107a8c8	27.05.2019	716
K7GW	Trojan (005798f41)	26.04.2021	16
KTAntiVirus	Trojan (005798f41)	26.04.2021	16
Cyren	W64/Kryptik.DQ2.gen/Eldorado	26.04.2021	16
Symantec	Trojan.Gen.MBT	25.04.2021	17
ESET-NOD32	a variant of Win64/Kryptik.CJE	26.04.2021	16
APEx	Malicious	25.04.2021	17
Paloalto	generic.ml	26.04.2021	16
Kaspersky	HEUR:Trojan.Win64.Ligooc.gen	26.04.2021	16
BitDefender	Trojan.GenericKDZ.T3610	26.04.2021	16
NANO-Antivirus	Trojan.Win64.Bazar.itydf	26.04.2021	16
Avast	Win64:MalwareX-gen [Trj]	26.04.2021	16
Rising	Trojan.Win64/Kryptik!L.D436 (CLOUD)	26.04.2021	16
Ad-Aware	Trojan.GenericKDZ.T3610	26.04.2021	16
Sophos	Mal/Generic-R + Troy/Agent-BGRN	25.04.2021	17
DrWeb	Trojan.DownLoader37.55025	26.04.2021	16
VIPRE	Trojan.Win32.Generic!BT	26.04.2021	16
TrendMicro	TROJ_FRS.0NA103CM21	30.03.2021	43
McAfee-GW-Edition	BehavesLike.Win64.Drixd.km	25.04.2021	17
Emmisoft	Trojan.Crypt (A)	26.04.2021	16

pestudio 9.09 - Malware Initial Assessment - www.winitor.com [c:\users\brandoon\lmao\Desktop\cyb 528 final\2.artifacts\kiod.hod]

File settings about

sha256: D1634C8DD16B4B1480065039FAC62D6C1900692F0CCC9BF52C8DDC65599FBF3D | cpu: 64-bit | file-type: dynamic-link-library | subsystem: Native | entry-point: 0x000029C0 | signature: n/a

engine (69/69)	score (47/69)	date (dd.mm.yyyy)	age (days)
Jiangmin	Trojan.Ligooc.ao	25.04.2021	17
Webroot	W32.Trojan.Gen	26.04.2021	16
Avira	TR/AD.Bazar.yotke	26.04.2021	16
Gridinsoft	Trojan.Win64.Kryptik.oals1	26.04.2021	16
Microsoft	Trojan/Script/Phonyz.Alml	26.04.2021	16
GData	Trojan.GenericKDZ.T3610	26.04.2021	16
Cynet	Malicious (score: 99)	12.04.2021	30
AhnLab-V3	Trojan/Win.Generic.R373456	26.04.2021	16
McAfee	Drixd-FKLID7B3FE762D53	26.04.2021	16
MAX	malware (ai score=80)	26.04.2021	16
Malwarebytes	Trojan.IcedID	26.04.2021	16
TrendMicro-HouseCall	TROJ_FRS.0NA103CM21	26.04.2021	16
Yandex	Trojan.Kryptik.kobolyHQ10	23.04.2021	19
Ikarus	Trojan.Win64.Crypt	25.04.2021	17
MaxSecure	Trojan.Malware.115979971.susgen	23.04.2021	19
Fortinet	W64/GenKryptik.FDGAltr	26.04.2021	16
AVG	Win64:MalwareX-gen [Trj]	26.04.2021	16
Bkav	clean	24.04.2021	18
Arcabit	clean	26.04.2021	16
Baidu	clean	18.03.2019	786
ClamAV	clean	25.04.2021	17
SUPERAntiSpyware	clean	23.04.2021	19
TACHYON	clean	26.04.2021	16
Comodo	clean	26.04.2021	16
F-Secure	clean	31.03.2021	42
CMC	clean	27.03.2021	46
SentinelOne	clean	15.02.2021	86
eGambit	clean	26.04.2021	16
Kingsoft	clean	26.04.2021	16
ViRobot	clean	26.04.2021	16

```
This program cannot be run in DOS mode.  
Rich  
.text  
.rdata  
@.data  
.pdata  
@USVWATAUAVAWH  
} A+  
} A+  
} A+  

```

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.

✓ pestudio 9.09 - Malware Initial Assessment - www.winitor.com [c:\users\brandoon\lmao\Desktop\cyb 528 final\2.artifacts\license.dat]

file settings about

	engine (57/57)	score (5/57)	date (dd.mm.yyyy)	age (days)
dll indicators (4)	ALYac	Trojan.IcedID.gen	24.04.2021	18
virustotal (5/57)	TrendMicro-HouseCall	Trojan.Win64.ICEDID.THCOBBA.enc	24.04.2021	18
abc strings (4215)	TrendMicro	Trojan.Win64.ICEDID.THCOBBA.enc	30.03.2021	43
	McAfee-GW-Edition	Ransom-EncodeDAT	24.04.2021	18
	McAfee	Ransom-EncodeDAT	24.04.2021	18
	Bkav	clean	24.04.2021	18
	ClamAV	clean	24.04.2021	18
	CMC	clean	27.03.2021	46
	CAT-QuickHeal	clean	24.04.2021	18
	Malwarebytes	clean	24.04.2021	18
	Zillya	clean	23.04.2021	19
	Sangfor	clean	16.04.2021	26
	K7AntiVirus	clean	24.04.2021	18
	K7GW	clean	24.04.2021	18
	BitDefenderTheta	clean	14.04.2021	28
	Cyren	clean	24.04.2021	18
	Symantec	clean	24.04.2021	18
	ESET-NOD32	clean	24.04.2021	18
	Baidu	clean	18.03.2019	796
	Avast	clean	24.04.2021	18
	Cynet	clean	12.04.2021	30
	Kaspersky	clean	24.04.2021	18
	BitDefender	clean	24.04.2021	18
	NANO-Antivirus	clean	24.04.2021	18
	ViRobot	clean	24.04.2021	18
	AegisLab	clean	24.04.2021	18
	MicroWorld-eScan	clean	24.04.2021	18
	Tencent	clean	24.04.2021	18
	Ad-Aware	clean	24.04.2021	18
	Sophos	clean	24.04.2021	18

```

Page: 1 of 21 Page
B2ch
q,Nv
4XI@UT
o2DY
i4YY
fa%2NzI
E@CzU
Zdesc
wd~y
p'mN
mOy;
#f3
0w8b[
Mj:k;V
f4_6j
9/*)
!-r{N
VO3U
{NLH
c)A<
K!6v
<ne*
Bagi
YYB4}9
{[v2
Swzk
n!9Y
F$0R
8L(a
)Y>-C
KuwiX
JA3FO
}}|c
ynsw`'
b){[2
a-e!@
|+.
ZiyI
|(S6hb

```

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.

pestudio 9.09 - Malware Initial Assessment - www.winitor.com [c:\users\brandoon\lmao\Desktop\cyb 528 final\2.artifacts\oxiwko.dll]

file settings about

engine (69/69)	score (43/69)	date (dd.mm.yyyy)	age (days)
Elastic	malicious (high confidence)	20.04.2021	22
MicroWorld-eScan	Trojan.GenericKD.45944042	26.04.2021	16
FireEye	Trojan.GenericKD.45944042	26.04.2021	16
CAT-QuickHeal	Trojan.Cig	25.04.2021	17
ALYac	Trojan.IcedID.gen	26.04.2021	16
Cylance	Unsafe	26.04.2021	16
Zillya	Trojan.Kryptik.Win64.10927	26.04.2021	16
Sangfor	Trojan.Win64.Ligoc.gen	16.04.2021	26
CrowdStrike	win/malicious_confidence_100% (W)	03.02.2021	98
Alibaba	Trojan:Win64/Kryptik.71f74e46	27.05.2019	716
K7GW	Trojan (00579691)	26.04.2021	16
K7AntiVirus	Trojan (00579691)	26.04.2021	16
Cyren	W64/Ligoc.A.gen:Eldorado	26.04.2021	16
Symantec	Trojan.Gen.MBT	25.04.2021	17
ESET-NOD32	a variant of Win64/Kryptik.CIG	26.04.2021	16
APEX	Malicious	25.04.2021	17
Avast	Win64:MalwareX-gen [T]	26.04.2021	16
Kaspersky	HEUR:Trojan.Win64.Ligoc.gen	26.04.2021	16
BitDefender	Trojan.GenericKD.45944042	26.04.2021	16
NANO-Antivirus	Trojan.Win64.Loader.itygcd	26.04.2021	16
AegisLab	Trojan.Win64.Ligoc.4!	26.04.2021	16
Ad-Aware	Trojan.GenericKD.45944042	26.04.2021	16
Sophos	Mal/Genetic-S	25.04.2021	17
DrWeb	Trojan.Loader.728	26.04.2021	16
VIPRE	Trojan.Win32.GenericIBT	26.04.2021	16
TrendMicro	TROJ_FRS_VSNTCM21	30.03.2021	43
McAfee-GW-Edition	Artemis!Trojan	25.04.2021	17
Emsisoft	Trojan.GenericKD.45944042 (B)	26.04.2021	16
GData	Trojan.GenericKD.45944042	26.04.2021	16
Webroot	W32.Trojan.GenKD	26.04.2021	16

sha256: 48B72914126B6B4A3E5AEFA9BC8D5EAC1187543EB0FA42C98A70A2F2AD07A60A cpu: 64-bit file-type: dynamic-link-library subsystem: Native entry-point: 0x00003738 signature: n/a

File Details				
File Path		Engine	Score	Date
c:\users\brandoon\lmao\Desktop\cyb 528 final\2	virusTotal (43/69)	engine (69/69)	score (43/69)	date (dd.mm.yyyy)
		Avira	TR/AD.Bazar.amdgw	26.04.2021
		ZoneAlarm	HEUR:Trojan.Win64.Ligoo.gen	26.04.2021
		Cynet	Malicious (score: 99)	12.04.2021
		AhnLab-V3	Trojan.Win.Bokbot.R414720	26.04.2021
		McAfee	Artemis!19D5172B1ABE	26.04.2021
		MAX	malware (ai score=85)	26.04.2021
		VBA32	Trojan.Win64.Ligoo	23.04.2021
		Malwarebytes	Trojan.IcedID	26.04.2021
		TrendMicro-HouseCall	TrojanSpy.Win64.ICIEDID.SMYABDET	26.04.2021
		Rising	Trojan.Kryptik8.8 (CLOUD)	26.04.2021
		Ikarus	Trojan.Win64.Crypt	25.04.2021
		AVG	Win64:MalwareX-gen [Tr]	26.04.2021
		Bkav	clean	24.04.2021
		Qihoo-360	clean	26.04.2021
		SUPERAntiSpyware	clean	23.04.2021
		Baidu	clean	18.03.2019
		ClamAV	clean	25.04.2021
		Paloalto	clean	26.04.2021
		Tencent	clean	26.04.2021
		TACHYON	clean	26.04.2021
		Comodo	clean	26.04.2021
		F-Secure	clean	31.03.2021
		CMC	clean	27.03.2021
		SentinelOne	clean	15.02.2021
		Jiangmin	clean	25.04.2021
		Anti-AVL	clean	26.04.2021
		Kingssoft	clean	26.04.2021
		Gridinsoft	clean	26.04.2021
		ArcaBit	clean	26.04.2021
		ViRobot	clean	26.04.2021

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: ddc45c82a484a420888aabef66588cbb1658cb2a7a5cc833b0438fa06ca84a991
- File size: 189,684 bytes
- File name: 82025721897_03192021.xlsx
- 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: c9ca58a0025a7ab633a35fe6e98943c9053ca49b10de55f8b57c8ea7c88e8eb0
- File size: 405,224 bytes
- File location: http://calldivorce.fun/
- File description: Binary with gzip compressed data retrieved from calldivorce.fun
- File note: Used by installer DLL to create the initial IcedID DLL file and license.dat

- SHA256 hash: b8502cc6fd41a558012e7cc0a7f4e0ed5746bf106b8bf5b6a27ef9cba18a9e3
- 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: 45b6349ee9d53278f350b59d4a2a28890bbe9f9de6565453db4c085bb5075065
- 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:

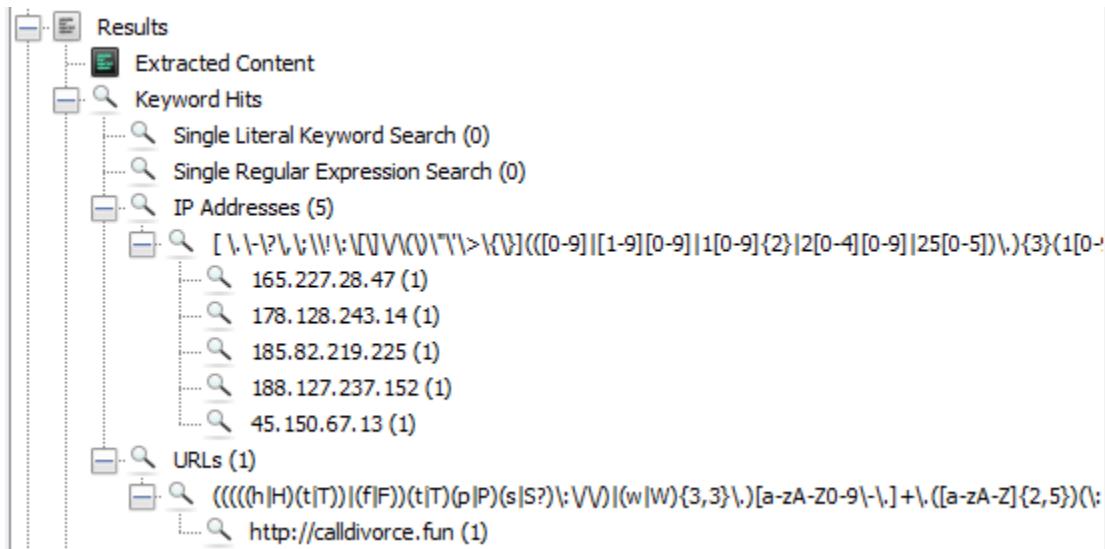
- port 443 - aws.amazon.com - HTTPS traffic  
- 178.128.243.14 port 80 - calldivorce.fun - GET /

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

No security vendors flagged this file as malicious

13289ea587fa9be9477eef5279932a225ebcbade085570d0fc930823d435b1fd
file.txt

Community Score: 0 / 57

2.87 KB | 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.