

Malware Traffic Analysis – Incident Report



The University Of

T A M P A[®]

By

Kranthi Kumar Manda

Executive Summary:

On March 21st 2022, at 20:58:11 UTC, A user named Patrick Zimmerman was the victim of a malware attack. By doing an analysis on the captured network traffic using tools like Wireshark & Brim (Zui), there are few evidences of network compromise. It was identified that the user infected with IcedID malware. IcedID is a generally banking trojan that is popular to steal sensitive information like financial data from infected systems. The malware was likely infected by the attacker through a malicious website oceriesfornot.top (this is the IP 188.166.154.118, user visited this site). The network trojan was detected from this website and downloaded a suspicious zip file.

The attacker started using Patrick's network right after the malware infection, On the victim's machine (10.0.19.14 & 00:60:52:b7:33:0f), the host (10.0.19.9) was using Patrick's network. By using smb_mapping, the attacker enumerated and gained access to the domain controller.

The attacker visited many malicious sites through gaining access to domain controller which include file sharing websites (filebin.net & situla.bitbit.net) and remaining sites mentioned in IOCs. I found a domain 'bupdater.com' in my analysis, this domain and IP address are also identified as malicious, and have been identified as a cobalt strike C2 server by the community (Virus Total). Then I was able to conclude that the attacker utilized the initial access granted by the IcedID infection to establish cobalt strike C2 (23.227.198.203:757 - bupdater.com) on the victim machine.

Details:

Client MAC address: PERIPHER_b7:33:0f (00:60:52:b7:33:0f)

Requested IP Address: 10.0.19.14

Host Name: DESKTOP-5QS3D5D

Client name: DESKTOP-5QS3D5D.burnincandle.com

Username: patrick.zimmerman (found through Kerberos)

Attacker: 188.166.154.118:80 - oceriesfornot.top (malware), Cobalt strike: 23.227.198.203:757 - bupdater.com

I started my analysis with Wireshark, and my goal was to identify the malware that infected Patrick's machine. So I went through statistics to find information like the IP address, DNS, Host name, and MAC address of the host. By doing this process, I figured out that '10.0.19.14' was the most common IP address in the captured packets. If this is the most common IP, then I can say this is most likely the target for attackers. By analyzing 'dhcp' packets, I got all the user details. And next, I analyzed 'Kerberos' for finding the owner of the system (PC user).

Next, I started filtering the 'http' traffic using Wireshark to get more details of the network traffic. I came across an http GET request from Patrick (user - 10.0.19.14) to 188.166.154.118 (http://oceriesfornot.top). This domain and its extension look weird to me, so I went to Google and did an advanced search about this 'oceriesfornot.top' domain and found that this is a malicious site related to Quantum Ransomware. Then I opened my Brim (Zui) to figure out what happened when the user visited this site. I quickly filtered the 'dns' traffic and analyzed this domain and found, 'oceriesfornot.top' was accessed by the user and downloaded a zip file, and got infected by a network trojan.

Continuing my search for more details about this trojan, I searched on VirusTotal about this domain and confirmed this is malicious malware. But both the 'MD5' (792ec837418da54679ac01a9b8c9f257) & 'sha1'(d5134cd34207addf6b483bdb39a24fbf847b1623) hash values found on Brim are not malware. Also, I checked for the TCP stream of this request and found an interesting cookie, and decoded it using 'Cyberchef' tools. I found the cookie is utilized for storing encoded information regarding the victim's host, which includes details such as the hostname, username, and Windows version. As a result, I had proof that the attacker was able to gather certain information regarding the victim's host.

I found more sites through 'dns' filter in both Brim & Wireshark. I saw our victim IP '10.0.19.14' is making unusual TLS requests with 'suncoastpinball.com' domain (160.153.32.99) on port 443, I saw some weird responses like 'Client Hello' & 'Server Hello'. This site is not self-signed but was issued by the Godaddy domain provider.

This DNS traffic disclosed the malicious operations of the attacker, I found another activity that within a fraction of seconds (like within 5-7 seconds) our victim tried to access 'antnosience.com' (157.245.142.66) 'filebin.net'(185.47.40.36) 'situla.bitbit.net'(87.238.33.8) 'bupdater.com'(23.227.198.203) sites. This is a nice pattern that I observed, all the sites mentioned are related to malicious malware (found through VirusTotal) some are related to 'Criminal IPs from different countries according to virus total. So basically the attacker used Patrick's network and accessed these malicious sites.

While going through the 'DNS' traffic I encountered another site 'bupdater.com' with the 23.227.198.203 . So I filtered the traffic with that Ip address 'ip.addr == 23.227.198.203' and found, It made a pattern that our victim host was sending multiple requests every minute on port 757. Again, I searched this site on VirusTotal and confirmed this as a 'Cobalt strike - Command and Control C2 server' by the community discussion about it.

Now, I can say that the attacker utilized the initial access he got through the IceID malware infection and used that access to start the cobalt strike attack on Patrick (our user).

To keep Patrick Zimmerman's system safe, it's a good idea to install anti-virus and implement firewall security. This will help scan all downloaded files for any dangerous viruses. We should use multiple layers of protection to stop attackers from harming any users on our network.

Appendices- Indicators of Compromise:

The Initial network traffic after the IcedID infection:

HTTP GET request - 188.166.154.118:80 - oceriesfornot.top (malware)

HTTPS traffic - 91.193.16.181:443 - seaskysafe.com and dilimoreast.com

HTTPS traffic - 157.245.142.66:443 - antnosience.com and otectagain.top

HTTPS traffic - 160.153.32.99:443 - suncoastpinball.com

The traffic to the file sharing websites:

HTTPS traffic - 185.47.40.36:443 - filebin.net

HTTPS traffic - 87.238.33.7:443 and 87.238.33.8:443 - situla.bitbit.net

The traffic to the cobalt strike command and control (C2):

HTTPS traffic - 23.227.198.203:757 - bupdater.com

* Detailed proofs with screenshots are in the next pages

This is first thing I did, Analyzing the protocol hierarchy. Statistics -> Hierarchy.

Wireshark - Protocol Hierarchy Statistics - Individual Assignment Spring 2023.pcap

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End B
Frame	100.0	16296	100.0	6591621	2318	0	0	0
Ethernet	100.0	16296	4.2	273818	96	0	0	0
Internet Protocol Version 4	94.5	15406	4.7	308204	108	0	0	0
User Datagram Protocol	5.7	928	0.1	7424	2	0	0	0
Simple Service Discovery Protocol	0.1	20	0.0	2704	0	20	2704	0
Network Time Protocol	0.2	34	0.1	4080	1	34	4080	1
NetBIOS Name Service	0.4	65	0.1	4198	1	65	4198	1
NetBIOS Datagram Service	0.4	67	0.2	12978	4	0	0	0
SMB (Server Message Block Protocol)	0.4	67	0.1	7484	2	0	0	0
SMB MailSlot Protocol	0.4	67	0.0	1675	0	0	0	0
Microsoft Windows Browser Protocol	0.4	67	0.0	1722	0	67	1722	0
Multicast Domain Name System	0.0	8	0.0	320	0	8	320	0
Link-local Multicast Name Resolution	0.1	9	0.0	371	0	9	371	0
Dynamic Host Configuration Protocol	0.0	4	0.0	1256	0	4	1256	0
Domain Name System	3.9	640	0.6	39696	13	640	39696	13
Data	0.1	13	0.2	10206	3	13	10206	3
Connectionless Lightweight Directory Access Protocol	0.4	68	0.2	14838	5	68	14838	5
Transmission Control Protocol	88.7	14455	89.3	5886160	2070	8711	3125249	1099
Transport Layer Security	21.3	3463	55.6	3661765	1287	3462	2825160	993
NetBIOS Session Service	7.4	1205	5.1	338534	119	6	228	0
SMB2 (Server Message Block Protocol version 2)	6.8	1116	5.0	330866	116	990	271271	95
SMB (Server Message Block Protocol)	0.5	83	0.2	11337	3	67	9889	3
SMB Pipe Protocol	0.1	16	0.0	232	0	0	0	0
Microsoft Windows Lanman Remote API Protocol	0.1	16	0.0	264	0	16	264	0
Lightweight Directory Access Protocol	2.0	328	8.1	535176	188	328	482185	169
Kerberos	0.3	44	0.8	54279	19	44	54279	19
Hypertext Transfer Protocol	0.2	35	0.2	10357	3	34	8760	3
PKIX CERT File Format	0.0	1	0.0	1306	0	1	1306	0
Distributed Computing Environment / Remote Procedure Call (DCE/RPC)	3.1	508	2.1	135544	47	146	61196	21
Server Service	0.0	2	0.0	940	0	1	164	0
Malformed Packet	0.0	1	0.0	0	0	1	0	0
SAMR (pidl)	0.6	102	0.1	6980	2	102	6980	2
Microsoft Network Logon	0.1	16	0.2	10052	3	16	10052	3
Local Security Authority	0.1	10	0.0	1232	0	10	1232	0
DRSUAPI	1.0	164	0.3	20864	7	164	20864	7

No display filter.

Help Copy Close

I filtered 'dhcp' traffic to gather the information of the user and found the Mac address, IP address, Host name.

The image shows a Wireshark network traffic analysis window titled "Individual Assignment Spring 2023.pcap". The filter is set to "dhcp". The packet list shows four DHCP packets:

No.	Time	Source	Destination	Protocol	Length	Info
3771	2022-03-21 21:28:30.838235	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0xe50fe596
3772	2022-03-21 21:28:30.843518	10.0.19.1	10.0.19.14	DHCP	344	DHCP Offer - Transaction ID 0xe50fe596
3773	2022-03-21 21:28:30.843938	0.0.0.0	255.255.255.255	DHCP	387	DHCP Request - Transaction ID 0xe50fe596
3774	2022-03-21 21:28:30.847846	10.0.19.1	10.0.19.14	DHCP	349	DHCP ACK - Transaction ID 0xe50fe596

The details pane for the selected DHCP Request packet (No. 3773) shows the following information:

- Client MAC address: PERIPHER_b7:33:0f (00:60:52:b7:33:0f)
- Client hardware address padding: 00000000000000000000
- Server host name not given
- Boot file name not given
- Magic cookie: DHCP
- Option: (53) DHCP Message Type (Request)
- Option: (61) Client identifier
 - Length: 7
 - Hardware type: Ethernet (0x01)
 - Client MAC address: PERIPHER_b7:33:0f (00:60:52:b7:33:0f)
- Option: (50) Requested IP Address (10.0.19.14)
 - Length: 4
 - Requested IP Address: 10.0.19.14
- Option: (54) DHCP Server Identifier (10.0.19.1)
 - Length: 4
 - DHCP Server Identifier: 10.0.19.1
- Option: (12) Host Name
 - Length: 15
 - Host Name: DESKTOP-5QS3D5D
- Option: (81) Client Fully Qualified Domain Name
 - Length: 35
 - Flags: 0x00
 - A-RR result: 0
 - PTR-RR result: 0
 - Client name: DESKTOP-5QS3D5D.burnincandle.com
- Option: (60) Vendor class identifier
- Option: (55) Parameter Request List
- Option: (255) End
 - Option End: 255

The packet bytes pane shows the raw data of the DHCP request packet, starting with the magic cookie 0xffffffff.

And to find out the username of the user, I filtered 'kerberos' traffic.

Kerberos:

The image shows a Wireshark capture of network traffic. The main pane displays a list of packets, with packet 4162 selected. The packet details pane shows the structure of the AS-REQ message, including the client name 'patrick.zimmerman' and realm 'BURNINCANDLE.COM'. The packet bytes pane shows the raw hex and ASCII data.

No.	Time	Source	Destination	Protocol	Length	Info
4150	2022-03-21 21:43:28.771958	10.0.19.14	10.0.19.9	KRBS	303	AS-REQ
4156	2022-03-21 21:43:28.772979	10.0.19.9	10.0.19.14	KRBS	267	KRB Error: KRBSKDC_ERR_PREAUTH_REQUIRED
4162	2022-03-21 21:43:28.773229	10.0.19.14	10.0.19.9	KRBS	303	AS-REQ
4164	2022-03-21 21:43:28.774133	10.0.19.9	10.0.19.14	KRBS	267	KRB Error: KRBSKDC_ERR_PREAUTH_REQUIRED
4171	2022-03-21 21:43:28.778106	10.0.19.14	10.0.19.9	KRBS	383	AS-REQ
4173	2022-03-21 21:43:28.779758	10.0.19.9	10.0.19.14	KRBS	436	AS-REP
4181	2022-03-21 21:43:28.782862	10.0.19.14	10.0.19.9	KRBS	383	AS-REQ
4183	2022-03-21 21:43:28.784427	10.0.19.9	10.0.19.14	KRBS	436	AS-REP
4192	2022-03-21 21:43:28.785269	10.0.19.14	10.0.19.9	KRBS	514	TGS-REQ
4195	2022-03-21 21:43:28.787474	10.0.19.9	10.0.19.14	KRBS	457	TGS-REP
4201	2022-03-21 21:43:28.787952	10.0.19.14	10.0.19.9	DCERPC	838	Bind: call_id: 2, Fragment: Single, 3 context items: DRSUAPI V4.0 (C
4203	2022-03-21 21:43:28.789116	10.0.19.9	10.0.19.14	DCERPC	338	Bind_ack: call_id: 2, Fragment: Single, max_xmit: 5840 max_recv: 58

Record Mark: 245 bytes

- as-req
 - pvno: 5
 - msg-type: krb-as-req (10)
 - padata: 1 item
 - req-body
 - padding: 0
 - kdc-options: 40010010
 - cname
 - name-type: kRB5-NT-PRINCIPAL (1)
 - cname-string: 1 item
 - CNameString: patrick.zimmerman
 - realm: BURNINCANDLE.COM
 - sname
 - till: Sep 12, 2037 22:48:05.000000000 EDT
 - rtime: Sep 12, 2037 22:48:05.000000000 EDT
 - nonce: 754335601
 - etype: 6 items
 - addresses: 1 item DESKTOP-5QS3D5D<20>

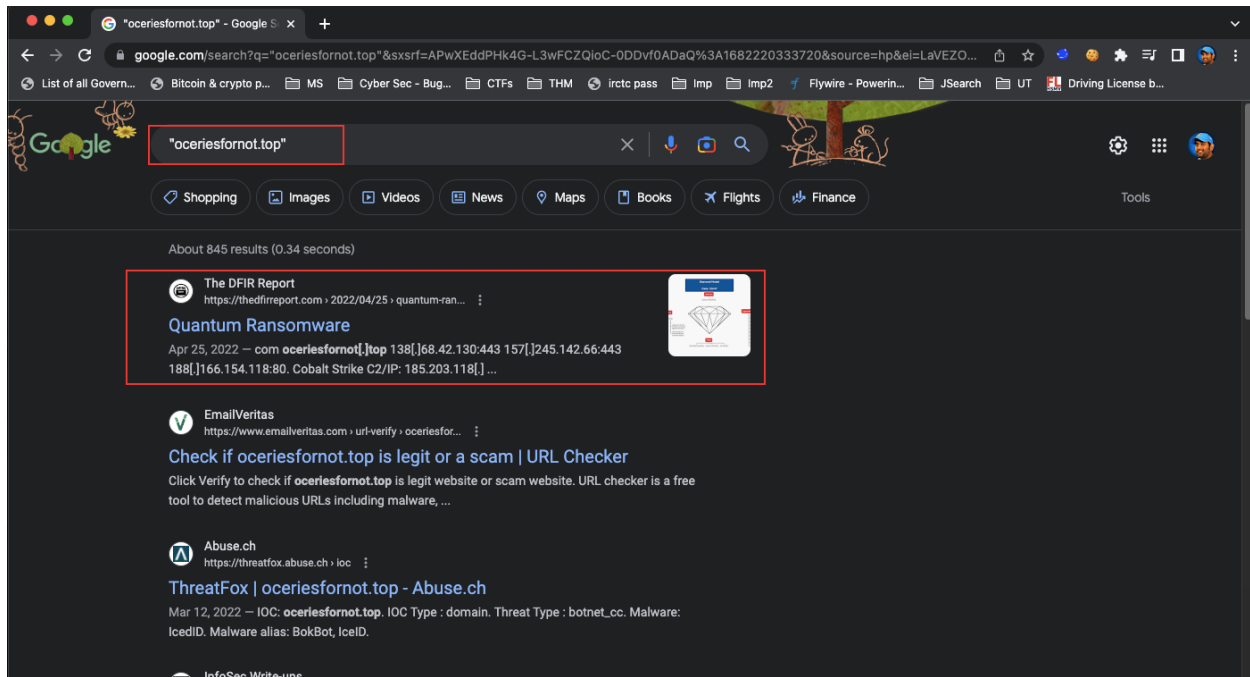
“ ip.addr==10.0.19.14 &&http.request.method==GET ”. This filter gave me all the http GET request method, I found three main sites and analyzed them.

The screenshot displays the Wireshark interface with the following components:

- Filter:** `ip.addr==10.0.19.14 &&http.request.method==GET`
- Packet List:** A table of captured packets, with the following columns: No., Time, Source, Destination, Protocol, Length, Host, and Info.

No.	Time	Source	Destination	Protocol	Length	Host	Info
4	2022-03-21 20:58:11.303409	10.0.19.14	188.166.154.118	HTTP	365	oceriesfornot.top	GET / HTTP/1.1
4074	2022-03-21 21:29:32.135617	10.0.19.14	68.142.107.129	HTTP	336	ctldl.windowsupdate.com	GET /msdownload/update/v3/static/trusted/en/pinr
5753	2022-03-21 21:54:44.353032	10.0.19.14	104.80.96.219	HTTP	169	r3.i.lencr.org	GET / HTTP/1.1
6059	2022-03-21 21:59:31.243136	10.0.19.14	104.80.96.219	HTTP	281	x1.c.lencr.org	GET / HTTP/1.1
6068	2022-03-21 21:59:31.580964	10.0.19.14	69.28.162.0	HTTP	336	ctldl.windowsupdate.com	GET /msdownload/update/v3/static/trusted/en/auth
8627	2022-03-21 22:29:35.281200	10.0.19.14	209.197.3.8	HTTP	336	ctldl.windowsupdate.com	GET /msdownload/update/v3/static/trusted/en/pinr
9268	2022-03-21 23:04:06.058127	10.0.19.14	104.80.96.219	HTTP	281	x1.c.lencr.org	GET / HTTP/1.1
9279	2022-03-21 23:04:06.356989	10.0.19.14	69.28.162.128	HTTP	336	ctldl.windowsupdate.com	GET /msdownload/update/v3/static/trusted/en/auth
9789	2022-03-21 23:21:56.047306	10.0.19.14	72.21.81.240	HTTP	341	ctldl.windowsupdate.com	GET /msdownload/update/v3/static/trusted/en/disa
10275	2022-03-21 23:44:34.371334	10.0.19.14	72.21.81.240	HTTP	336	ctldl.windowsupdate.com	GET /msdownload/update/v3/static/trusted/en/disa
11757	2022-03-22 00:29:34.887435	10.0.19.14	104.80.96.219	HTTP	281	x1.c.lencr.org	GET / HTTP/1.1
11767	2022-03-22 00:29:35.179327	10.0.19.14	209.197.3.8	HTTP	336	ctldl.windowsupdate.com	GET /msdownload/update/v3/static/trusted/en/auth
12502	2022-03-22 00:59:35.716220	10.0.19.14	209.197.3.8	HTTP	336	ctldl.windowsupdate.com	GET /msdownload/update/v3/static/trusted/en/pinr
12818	2022-03-22 01:04:42.964033	10.0.19.14	72.21.81.240	HTTP	341	ctldl.windowsupdate.com	GET /msdownload/update/v3/static/trusted/en/disa
14371	2022-03-22 02:04:06.526312	10.0.19.14	104.80.96.219	HTTP	281	x1.c.lencr.org	GET / HTTP/1.1
14380	2022-03-22 02:04:06.880749	10.0.19.14	68.142.107.1	HTTP	336	ctldl.windowsupdate.com	GET /msdownload/update/v3/static/trusted/en/auth
14383	2022-03-22 02:04:07.025310	10.0.19.14	68.142.107.1	HTTP	336	ctldl.windowsupdate.com	GET /msdownload/update/v3/static/trusted/en/pinr
14821	2022-03-22 02:19:47.324783	10.0.19.14	23.219.38.10	HTTP	341	ctldl.windowsupdate.com	GET /msdownload/update/v3/static/trusted/en/disa
- Packet Details:** Shows the structure of the selected packet (No. 4):
 - Frame 4: 365 bytes on wire (2920 bits), 365 bytes captured (2920 bits)
 - Ethernet II, Src: PERIPHER_b7:33:0f (00:60:52:b7:33:0f), Dst: Cisco_2f:13:5c (2c:54:2d:2f:13:5c)
 - Internet Protocol Version 4, Src: 10.0.19.14, Dst: 188.166.154.118
 - Transmission Control Protocol, Src Port: 62179, Dst Port: 80, Seq: 1, Ack: 1, Len: 311
 - Hypertext Transfer Protocol
 - GET / HTTP/1.1\r\n
 - Connection: Keep-Alive\r\n
 - [truncated]Cookie: __gads=3546287305:1:14094:123; _gat=10.0.19044.64; _ga=5.656979.4300.9; _u=44455348544F_\r\n
 - Host: oceriesfornot.top\r\n
 - \r\n
 - Full request URI: http://oceriesfornot.top/
- Packet Bytes:** Hexadecimal and ASCII representation of the packet data.

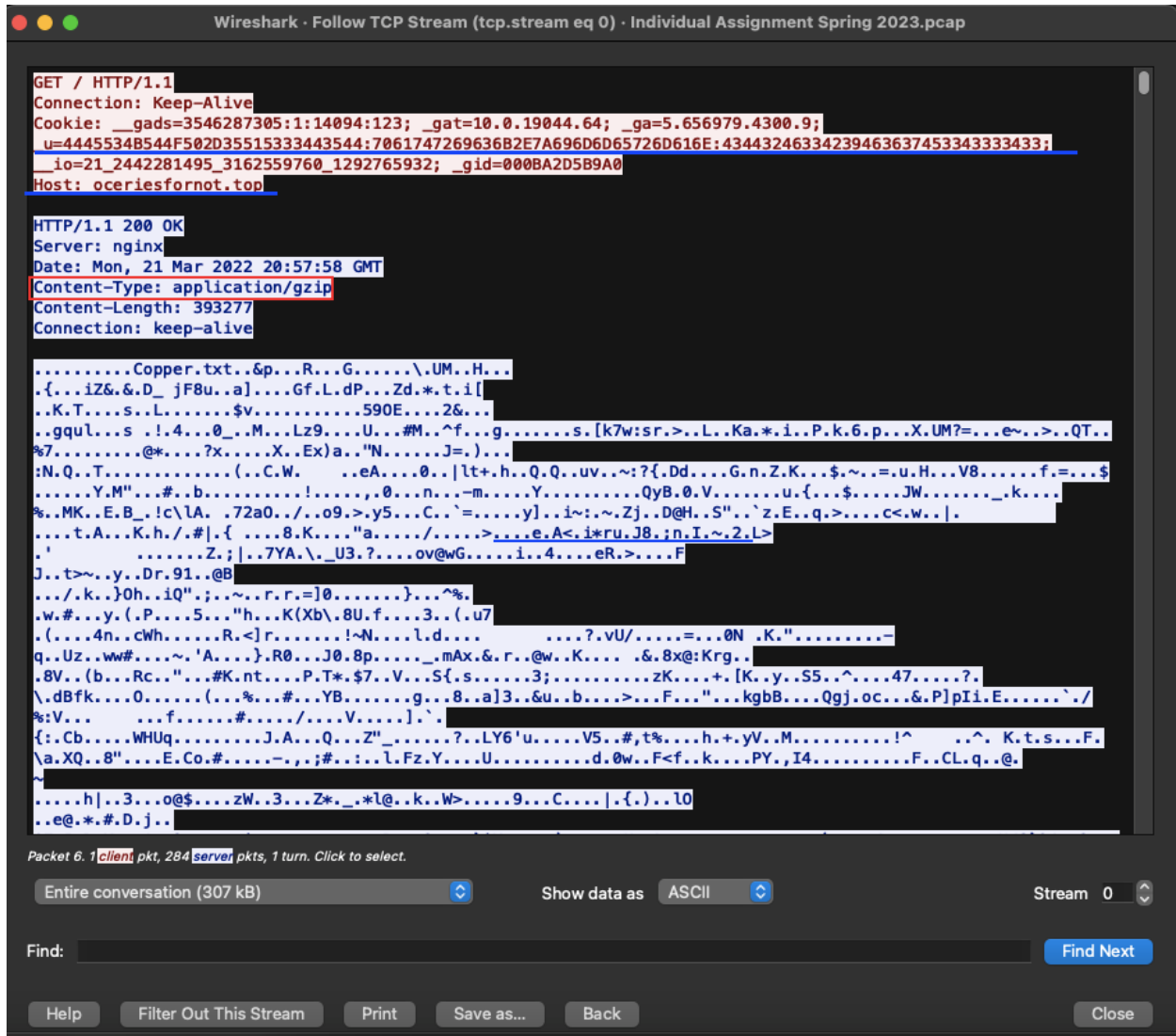
I looked up the two hosts, x1.c.lencr.org and ctldl.windowsupdate.com, and they appear to be genuinely owned by LetsEncrypt and Microsoft. However, oceriesfornot.top (188.166.154.118) appears to be linked to the Quantum Ransomware. See the google result below.



I find an unusual cookie after selecting the frame and following the TCP stream of “oceriesfornot.top” HTTP request:

(right click on frame -> Follow -> TCP Stream)

It will automatically download a zip file if we try to access the the site “oceriesfornot.top”



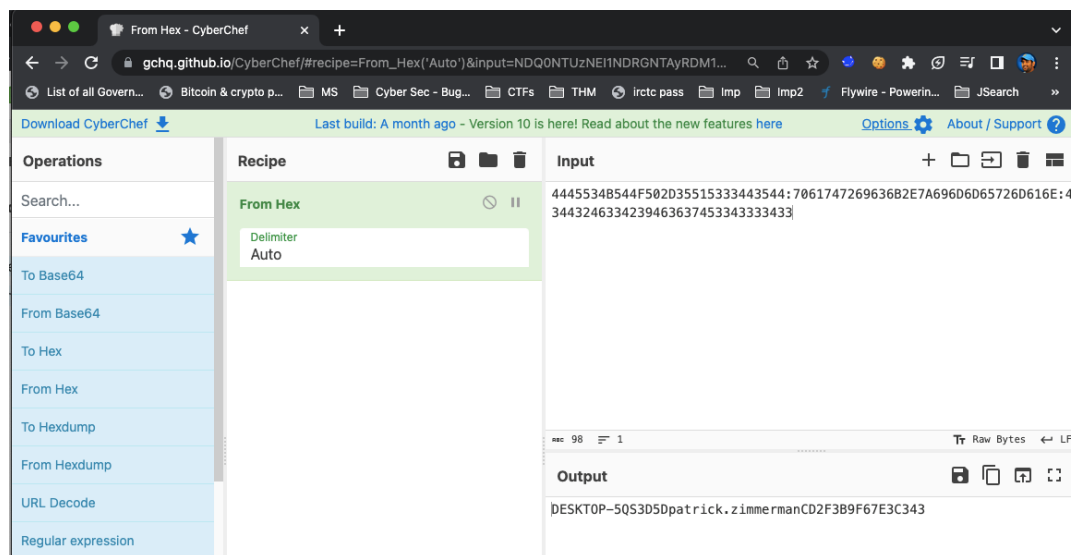
Upon discovering a gzip file, I did research on IcedID and gzip files. It became apparent to me that the extent of the infection went beyond what I initially assumed. The string "Copper.txt" acted as a simple facade. In reality, the data was encrypted IcedID configuration and not an actual file.

I spent some time researching more and came across sysopfb's blog where he did some research on "IcedID" malware that contains a similar cookie:

Link: <https://sysopfb.github.io/malware,icedid/2020/04/28/IcedIDs-updated-photoloader.html>

Cookie	Value
_gid	Based on physical address of NIC
_jo	Domain identifier from SID
_u	Username and Computername
_gat	Windows version info
_ga	Processor info via CPUID including hypervisor brand if available
_gads	First DWORD from decoded config data, flag from inspecting server certificate, a random DWORD or number passed as parameter with -id=, number of processes

He explains that the "_u" cookie value contains the victim's hexa-decimalized username and computer-name. Therefore, I utilized cyberchef to validate this, and indeed I got this outcome from the cookie value:



The screenshot shows the CyberChef web interface. The browser address bar shows the URL: [gchq.github.io/CyberChef/#recipe=From_Hex\('Auto'\)&input=NDQ0NTUzNEI1NDRGNTAyRDM1...](https://gchq.github.io/CyberChef/#recipe=From_Hex('Auto')&input=NDQ0NTUzNEI1NDRGNTAyRDM1...). The interface includes a sidebar with 'Operations' and 'Favourites' sections. The 'Favourites' section lists several operations: 'To Base64', 'From Base64', 'To Hex', 'From Hex', 'To Hexdump', 'From Hexdump', 'URL Decode', and 'Regular expression'. The main area shows a 'Recipe' section with 'From Hex' selected and 'Delimiter' set to 'Auto'. The 'Input' field contains a long hex string: `44455348544F502D35515333443544:706174726963682E7A696D6D65726D616E:43443246334239463637453343334333`. The 'Output' field shows the decoded result: `DESKTOP-5Q53D5Dpatrick.zimmermanCD2F3B9F67E3C343`.

The cookie is utilized for storing encoded information regarding the victim's host, which includes details such as the hostname, username, and Windows version. As a result, I had substantial proof that the attacker was able to gather certain information regarding the victim's host.

Using Zui software, I found and confirmed that '188.166.154.118' IP as malicious and a 'Network Trojan' was detected. Take a look at the below screenshot.

FROM Individual Assignment Spring 2023.pcap

```
1 event_type=="alert" src_ip==10.0.19.14 dest_ip==188.166.154.118
```

src_ip	dest_ip	proto	app_proto	alert	flow_id
10.0.19.14	188.166.154.	TCP	http	{ severity: 1, signature: ET MALWARE Win32/IcedID Request Cookie, category: A Network Trojan was detected, action: allowed, signature_id: 2032086, gid: 1, rev: 1, metadata: > {signature_severity: [Major], former_category: [MALWARE] ...+6 }	15761366122351
10.0.19.14	188.166.154.	TCP	http	> {severity: 2, signature: ET INFO HTTP Request to a *.top domain ...+6 }	15761366122351

Results: 2 Shapes: 1

FROM Individual Assignment Spring 2023.pcap

```
1 _path=="files" 188.166.154.118
```

_path	ts	tx_hosts	rx_hosts	conn_uids	source	mime_type
files	2022-03-21	> [188.166.154.118]	> [10.0.19.14]	> [CIm62hIL6bTeJJSLh]	HTTP	application/x-gzip

Downloading a zip file from 188.166.154.118 to the victims machine (10.0.19.14)

MD5: 792ec837418da54679ac01a9b8c9f257

Sha1: d5134cd34207addf6b483bdb39a24fbf847b1623

Details

Duration: 1 minute 24 seconds
Populated by uid & community_id

source	HTTP
depth	0
analyzers	[[...2]]
mime_type	application/x-gzip
filename	⊗
duration	24.206623s
local_orig	⊗
is_orig	false
seen_bytes	393,277
total_bytes	393,277
missing_bytes	0
overflow_bytes	0
timedout	false
parent_fuid	⊗
md5	792ec837418da54679ac01a9b8c9f257
sha1	d5134cd34207addf6b483bdb39a24fbf847b1623
sha256	⊗

MD5 CORRELATION

md5	count
792ec837418da54679ac01a9b8c9f257	1

filename	mime_type	count
⊗	application/x-gzip	1

tx_hosts	count	rx_hosts	count
[[...1]]	1	[[...1]]	1

Another confirmation on VirusTotal:

The screenshot shows the VirusTotal domain analysis page for `oceriesfornot.top`. The domain is highlighted in a red box. The page displays a community score of 17/87, 17 security vendors flagged as malicious, and a table of security vendor analyses. The table lists the following vendors and their detections:

Vendor	Detection	Vendor	Detection
alphaMountain.ai	Malicious	AlphaSOC	Malware
Antiy-AVL	Malicious	Avira	Malware
Bfore.Ai PreCrime	Malicious	BitDefender	Malware
CvRadard	Malicious	Dr.Web	Malicious

I came across the initial IOC and determined that the domain and IP address of “`oceriesfornot.top`” were identified as malicious through VirusTotal as well.

I noticed that the victim IP address established multiple unusual TLS connections with the suncoastpinball.com domain located at 160.153.32.99:443 (port 443), which provided me with another indicator of compromise (IOC). Despite not being self-signed, the domain's SSL certificate was issued by GoDaddy (SSL info found on Follow->TCP Stream). And people reported it as a virus site.

The screenshot shows a Wireshark capture of a network session. The main pane displays a list of packets, with frame 581 highlighted. This frame contains a 'Server Hello' message from the destination IP 160.153.32.99 to the source IP 10.0.19.14. The details pane below shows the structure of the captured data, including Ethernet II, Internet Protocol Version 4, and Transport Layer Security (TLSv1.2). The status bar at the bottom indicates that 163 out of 16296 packets are displayed.

The screenshot shows a domain reputation tool interface for the domain suncoastpinball.com. On the left, a circular gauge displays a score of 3 out of 87. A red warning icon and text state: "3 security vendors flagged this domain as malicious". Below the domain name, several tags are listed: "Business/Economy, Suspicious", "media sharing", and "restaurants and dining". At the bottom left, there is a "Community Score" section with a red 'X' icon and a green checkmark icon.

As I proceeded to examine Wireshark further, I decided to narrow my focus by filtering for DNS traffic. This particular type of traffic can disclose the domains and IP addresses employed by attackers to execute their malicious operations. After applying this filter, I observed that the victim's IP address made few DNS requests for domains, all within a brief interval of time (5 seconds difference like that).

No.	Time	Source	Destination	Protocol	Length	Info
4455	2022-03-21 21:43:30.343547	10.0.19.9	10.0.19.14	DNS	160	Standard query response 0xbf73 A teams-ring.msedge.net CNAME teams-ring...
4456	2022-03-21 21:43:30.343628	10.0.19.9	10.0.19.14	DNS	146	Standard query response 0x987f A fp-vp.azureedge.net CNAME fp-vp.ec.azur...
4463	2022-03-21 21:43:30.351545	10.0.19.9	10.0.19.14	DNS	220	Standard query response 0xf774 A www.bing.com CNAME a-0001.a-afdentry.ne...
4467	2022-03-21 21:43:30.410006	10.0.19.9	10.0.19.14	DNS	152	Standard query response 0x7ecb A spo-ring.msedge.net CNAME spo-ring.spo...
4726	2022-03-21 21:43:40.483805	10.0.19.9	10.0.19.14	DNS	205	Standard query response 0xc471 A checkappexec.microsoft.com CNAME wd-pr...
4768	2022-03-21 21:43:59.573949	10.0.19.9	10.0.19.14	DNS	220	Standard query response 0x1618 A www.bing.com CNAME a-0001.a-afdentry.ne...
4824	2022-03-21 21:44:29.513278	10.0.19.9	10.0.19.14	DNS	196	Standard query response 0x8d34 SRV _ldap._tcp.Default-First-Site-Name._...
4899	2022-03-21 21:44:29.930175	10.0.19.9	10.0.19.14	DNS	91	Standard query response 0x424b A antnosience.com A 157.245.142.66
4996	2022-03-21 21:49:31.287345	10.0.19.9	10.0.19.14	DNS	91	Standard query response 0xe7d3 A antnosience.com A 157.245.142.66
5060	2022-03-21 21:54:32.614809	10.0.19.9	10.0.19.14	DNS	91	Standard query response 0x8d73 A antnosience.com A 157.245.142.66
5075	2022-03-21 21:54:34.021764	10.0.19.9	10.0.19.14	DNS	87	Standard query response 0x40ea A filebin.net A 185.47.40.36
5100	2022-03-21 21:54:35.140469	10.0.19.9	10.0.19.14	DNS	109	Standard query response 0x59b5 A situla.bitbit.net A 87.238.33.8 A 87.2...
5736	2022-03-21 21:54:43.825443	10.0.19.9	10.0.19.14	DNS	88	Standard query response 0x2258 A bupdater.com A 23.227.198.203
5749	2022-03-21 21:54:44.275556	10.0.19.9	10.0.19.14	DNS	179	Standard query response 0xbf0c A r3.i.lencr.org CNAME crl.root-x1.letse...
5945	2022-03-21 21:58:30.335698	10.0.19.9	10.0.19.14	DNS	220	Standard query response 0x1938 A v10.events.data.microsoft.com CNAME gl...
5978	2022-03-21 21:58:31.999060	10.0.19.9	10.0.19.14	DNS	228	Standard query response 0x3b42 A settings-win.data.microsoft.com CNAME i...
6055	2022-03-21 21:59:31.120928	10.0.19.9	10.0.19.14	DNS	179	Standard query response 0xc669 A x1.c.lencr.org CNAME crl.root-x1.letse...
6064	2022-03-21 21:59:31.439881	10.0.19.9	10.0.19.14	DNS	196	Standard query response 0x8684 A ctldl.windowsupdate.com CNAME wu-bg-sh...
6073	2022-03-21 21:59:34.003979	10.0.19.9	10.0.19.14	DNS	91	Standard query response 0x90ed A antnosience.com A 157.245.142.66
6296	2022-03-21 22:04:35.400248	10.0.19.9	10.0.19.14	DNS	91	Standard query response 0xd3b2 A antnosience.com A 157.245.142.66
7931	2022-03-21 22:09:36.716133	10.0.19.9	10.0.19.14	DNS	91	Standard query response 0x4b5a A antnosience.com A 157.245.142.66
7957	2022-03-21 22:10:08.859056	10.0.19.9	10.0.19.14	DNS	205	Standard query response 0x3047 A checkappexec.microsoft.com CNAME wd-pr...
8002	2022-03-21 22:12:10.088913	10.0.19.9	10.0.19.14	DNS	196	Standard query response 0xab55 SRV _ldap._tcp.Default-First-Site-Name._...
8319	2022-03-21 22:14:38.134945	10.0.19.9	10.0.19.14	DNS	91	Standard query response 0x4c7e A antnosience.com A 157.245.142.66
8409	2022-03-21 22:19:39.367274	10.0.19.9	10.0.19.14	DNS	91	Standard query response 0x5f79 A antnosience.com A 157.245.142.66
8486	2022-03-21 22:24:40.625418	10.0.19.9	10.0.19.14	DNS	91	Standard query response 0x52a7 A antnosience.com A 157.245.142.66

The domains “filebin.net” and “situla.bitbit.net” are file sharing platforms (malicious). Connections to both domains were established, with each connection lasting for less than 10 seconds. At this point, it remains unclear whether this indicates that data was being exfiltrated, or if the malware was attempting to retrieve additional resources to be deployed on the victim's device.

All the these domains are malicious according to the Virus Total (people reported these websites as virus). I have all the screenshots in the next page.

Individual Assign... x Query Session x +

Save Run HISTORY DETAIL VERSIONS >>

FROM Individual Assignment Spring 2023.pcap v

1 `_path=="dns" id.orig_h==10.0.19.14 | count() by query, answers | sort -r count`

query <string>
answers <array>
count <uint64>

TABLE INSPECTOR

No Chart Data

query	answers	count ↓
antnosience.com	> [157.245.142.66]	65
wpad.mshome.net	null	41
wpad.burnincandle.com	null	41
dilimoreast.com	> [91.193.16.181]	26
otectagain.top	> [157.245.142.66]	23
seaskysafe.com	> [91.193.16.181]	22
burnincandle-dc.burnincandle.com	> [10.0.19.9]	11
_ldap_tcp.default-first-site-name._sites.dc_msc	> [burnincandle-dc.burnincandle.com	10
null	null	9
settings-win.data.microsoft.com	> [atm-settingsfe-prod-geo.trafficm	7
settings-win.data.microsoft.com	> [atm-settingsfe-prod-geo.trafficm	6
x1.c.lencr.org	> [crl.root-x1.letsencrypt.org.edgek	4
ctldl.windowsupdate.com	> [wu-bg-shim.trafficmanager.net, w	3
WPAD	null	3
www.bing.com	> [a-0001.a-afdentry.net.trafficman	3
desktop-5qs3d5d	null	3
BURNINCANDLE-DC	null	3

Results: 75 Shapes: 1

query	answers	count ↓
v10.events.data.microsoft.com	> [global.asimov.events.data.traffic	1
suncoastpinball.com	> [160.153.32.99]	1
config.edge.skype.com	> [config.edge.skype.com.trafficman	1
fp-vs-nocache.azureedge.net	> [fp-vs-nocache.ec.azureedge.net, i	1
spo-ring.msedge.net	> [spo-ring.spo-9999.spo-msedge.ne	1
hupdater.com	> [23.227.198.203]	1
teams-ring.msedge.net	> [teams-ring.teams-9999.teams-m	1
__MSBROWSE__	null	1
v10.events.data.microsoft.com	> [global.asimov.events.data.traffic	1
v10.events.data.microsoft.com	> [global.asimov.events.data.traffic	1
r3.i.lencr.org	> [crl.root-x1.letsencrypt.org.edgek	1
situla.bitbit.net	> [87.238.33.8, 87.238.33.7]	1
ctldl.windowsupdate.com	> [wu-bg-shim.trafficmanager.net, d	1
ctldl.windowsupdate.com	> [wu-bg-shim.trafficmanager.net, w	1



situla.bitbit.net



1 security vendor flagged this domain as malicious

situla.bitbit.net
bitbit.net



filebin.net



Did you intend to search

5 security vendors flagged this domain as malicious

filebin.net

known infection source media sharing personal network storage and ba

Community Score



seaskysafe.com



Did you intend to search

12 security vendors flagged this domain as malicious

seaskysafe.com

Malicious bot networks spyware and malware

Community Score



dilimoreast.com



Did you intend to search

15 security vendors flagged this domain as malicious

dilimoreast.com

bot networks spyware and malware unknown

Community Score



antnosience.com

Did you



Loading observable report...

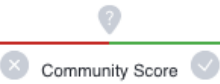
antnosience.com

bot networks media sharing spyware and malware



otectagain.top

Did you intend to search



⚠ 11 security vendors flagged this domain as malicious

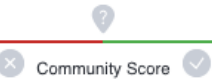
otectagain.top

bot networks media sharing spyware and malware



suncoastpinball.com

Did you intend to search acc



⚠ 3 security vendors flagged this domain as malicious

suncoastpinball.com

Business/Economy, Suspicious media sharing restaurants and dining

I noticed a pattern after configuring 23.227.198.203 (bupdater.com) as my destination address. Specifically, the host appeared to communicate with 'bupdater.com' every minute on port 757.

The image shows a Wireshark capture of network traffic. The main pane displays a list of packets with columns for No., Time, Source, Source Port, Destination, Destination Port, Protocol, Length, and Info. A filter is applied: 'ip.dst==23.227.198.203'. The packets show a regular pattern of connections to the destination IP 23.227.198.203 on port 757. The source IP is consistently 10.0.19.14. The packets are primarily TCP connections, with some showing FIN, ACK, RST, and SYN flags. The time intervals between packets are approximately one minute.

No.	Time	Source	Source Port	Destination	Destination Port	Protocol	Length	Info
6223	2022-03-21 22:02:20.673519	10.0.19.14	62275	23.227.198.203	757	TCP	60	62275 → 757 [FIN, ACK] Seq=2387 Ack=3718 Win=261632 Len=0
6224	2022-03-21 22:02:20.673519	10.0.19.14	62275	23.227.198.203	757	TCP	60	62275 → 757 [RST, ACK] Seq=2388 Ack=3718 Win=0 Len=0
6226	2022-03-21 22:02:20.793054	10.0.19.14	62275	23.227.198.203	757	TCP	60	62275 → 757 [RST] Seq=2388 Win=0 Len=0
6201	2022-03-21 22:02:20.191990	10.0.19.14	62275	23.227.198.203	757	TCP	66	62275 → 757 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=2
6237	2022-03-21 22:03:06.947800	10.0.19.14	62276	23.227.198.203	757	TCP	60	62276 → 757 [ACK] Seq=1 Ack=1 Win=262144 Len=0
6238	2022-03-21 22:03:06.948538	10.0.19.14	62276	23.227.198.203	757	TCP	1415	62276 → 757 [ACK] Seq=1 Ack=1 Win=262144 Len=1361 [TCP
6245	2022-03-21 22:03:07.073285	10.0.19.14	62276	23.227.198.203	757	TCP	60	62276 → 757 [ACK] Seq=1769 Ack=1456 Win=262144 Len=0
6247	2022-03-21 22:03:07.194209	10.0.19.14	62276	23.227.198.203	757	TCP	60	62276 → 757 [ACK] Seq=1769 Ack=1727 Win=261632 Len=0
6244	2022-03-21 22:03:07.073285	10.0.19.14	62276	23.227.198.203	757	TCP	60	62276 → 757 [ACK] Seq=1769 Ack=95 Win=261888 Len=0
6254	2022-03-21 22:03:07.334689	10.0.19.14	62276	23.227.198.203	757	TCP	60	62276 → 757 [ACK] Seq=2387 Ack=1890 Win=261632 Len=0
6256	2022-03-21 22:03:07.334773	10.0.19.14	62276	23.227.198.203	757	TCP	60	62276 → 757 [ACK] Seq=2387 Ack=3718 Win=262144 Len=0
6257	2022-03-21 22:03:07.334850	10.0.19.14	62276	23.227.198.203	757	TCP	60	62276 → 757 [FIN, ACK] Seq=2387 Ack=3718 Win=262144 Len=0
6258	2022-03-21 22:03:07.334895	10.0.19.14	62276	23.227.198.203	757	TCP	60	62276 → 757 [RST, ACK] Seq=2388 Ack=3718 Win=0 Len=0
6260	2022-03-21 22:03:07.453698	10.0.19.14	62276	23.227.198.203	757	TCP	60	62276 → 757 [RST] Seq=2388 Win=0 Len=0
6235	2022-03-21 22:03:06.835954	10.0.19.14	62276	23.227.198.203	757	TCP	66	62276 → 757 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=2
6267	2022-03-21 22:03:57.725872	10.0.19.14	62277	23.227.198.203	757	TCP	60	62277 → 757 [ACK] Seq=1 Ack=1 Win=262144 Len=0
6268	2022-03-21 22:03:57.726544	10.0.19.14	62277	23.227.198.203	757	TCP	1415	62277 → 757 [ACK] Seq=1 Ack=1 Win=262144 Len=1361 [TCP
6275	2022-03-21 22:03:57.861771	10.0.19.14	62277	23.227.198.203	757	TCP	60	62277 → 757 [ACK] Seq=1769 Ack=1456 Win=262144 Len=0
6277	2022-03-21 22:03:57.976726	10.0.19.14	62277	23.227.198.203	757	TCP	60	62277 → 757 [ACK] Seq=1769 Ack=1727 Win=261632 Len=0
6273	2022-03-21 22:03:57.854449	10.0.19.14	62277	23.227.198.203	757	TCP	60	62277 → 757 [ACK] Seq=1769 Ack=95 Win=261888 Len=0
6283	2022-03-21 22:03:58.099967	10.0.19.14	62277	23.227.198.203	757	TCP	60	62277 → 757 [ACK] Seq=2387 Ack=1890 Win=261632 Len=0
6286	2022-03-21 22:03:58.102191	10.0.19.14	62277	23.227.198.203	757	TCP	60	62277 → 757 [ACK] Seq=2387 Ack=3718 Win=262144 Len=0
6287	2022-03-21 22:03:58.102362	10.0.19.14	62277	23.227.198.203	757	TCP	60	62277 → 757 [FIN, ACK] Seq=2387 Ack=3718 Win=262144 Len=0
6288	2022-03-21 22:03:58.102362	10.0.19.14	62277	23.227.198.203	757	TCP	60	62277 → 757 [RST, ACK] Seq=2388 Ack=3718 Win=0 Len=0
6290	2022-03-21 22:03:58.222208	10.0.19.14	62277	23.227.198.203	757	TCP	60	62277 → 757 [RST] Seq=2388 Win=0 Len=0
6265	2022-03-21 22:03:57.612200	10.0.19.14	62277	23.227.198.203	757	TCP	66	62277 → 757 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=2
6320	2022-03-21 22:04:52.864724	10.0.19.14	62279	23.227.198.203	757	TCP	60	62279 → 757 [ACK] Seq=1 Ack=1 Win=262144 Len=0
6321	2022-03-21 22:04:52.865402	10.0.19.14	62279	23.227.198.203	757	TCP	1415	62279 → 757 [ACK] Seq=1 Ack=1 Win=262144 Len=1361 [TCP
6327	2022-03-21 22:04:53.011453	10.0.19.14	62279	23.227.198.203	757	TCP	60	62279 → 757 [ACK] Seq=1769 Ack=1456 Win=262144 Len=0
6329	2022-03-21 22:04:53.133282	10.0.19.14	62279	23.227.198.203	757	TCP	60	62279 → 757 [ACK] Seq=1769 Ack=1727 Win=261632 Len=0
6325	2022-03-21 22:04:53.007366	10.0.19.14	62279	23.227.198.203	757	TCP	60	62279 → 757 [ACK] Seq=1769 Ack=95 Win=261888 Len=0
6335	2022-03-21 22:04:53.264108	10.0.19.14	62279	23.227.198.203	757	TCP	60	62279 → 757 [ACK] Seq=2387 Ack=1890 Win=261632 Len=0

Packet details for Frame 6146:

- Frame 6146: 461 bytes on wire (3688 bits), 461 bytes captured (3688 bits)
- Ethernet II, Src: PERIPHER_b7:33:0f (08:60:52:b7:33:0f), Dst: Cisco_2f:13:5c (2c:54:2d:2f:13:5c)
- Internet Protocol Version 4, Src: 10.0.19.14, Dst: 23.227.198.203
- Transmission Control Protocol, Src Port: 62273, Dst Port: 757, Seq: 1362, Ack: 1, Len: 407

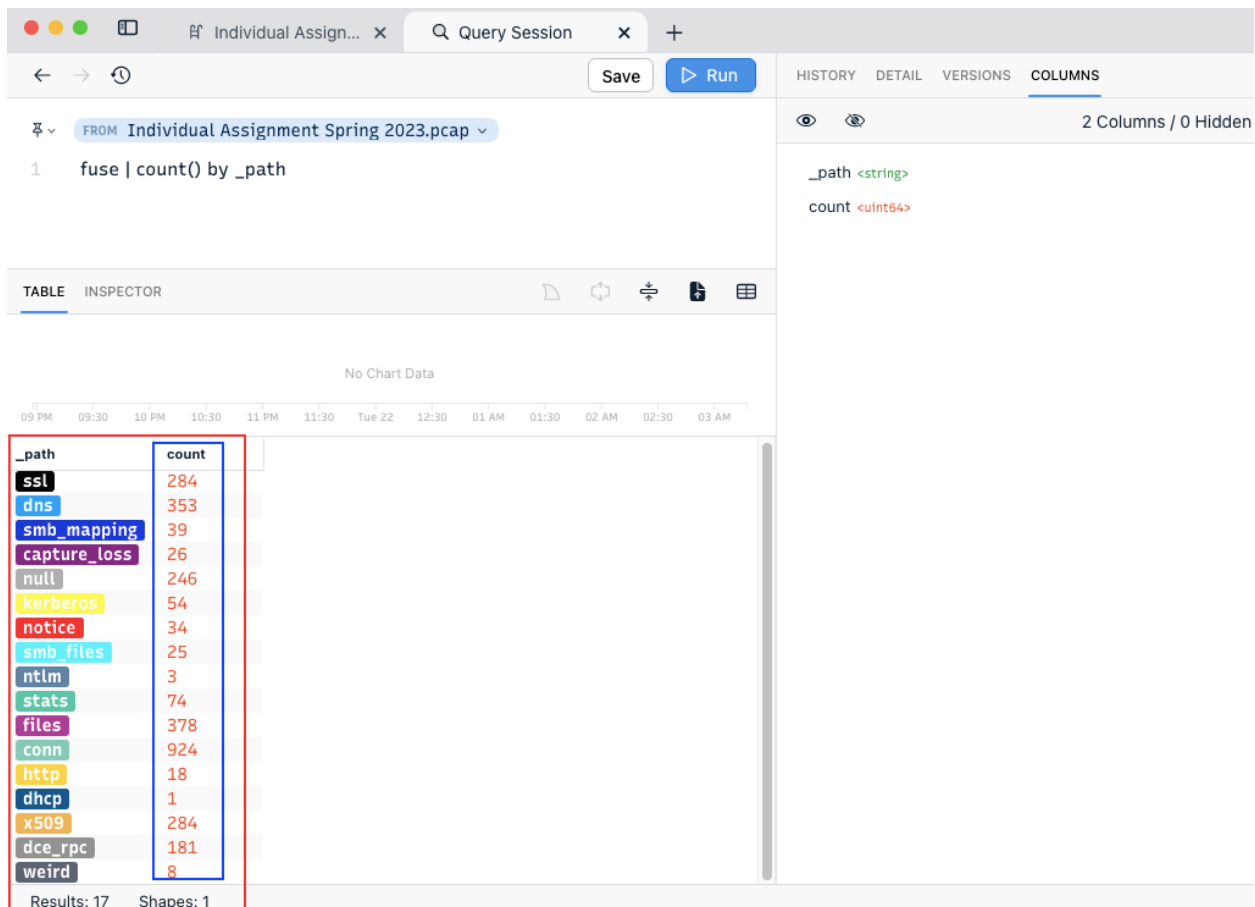
Packet bytes: 0000 2c 54 2d 2f 13 5c 00 60 52 b7 33 0f 00 00 45 06 00 10 01 bf 2b c2 40 00 00 06 d1 ba 0a 00 13 0e 17 e5

After performing a search on VirusTotal (23.227.198.203), I discovered that multiple individuals had previously reported it as a Cobalt Strike Command-and-Control (C2) server.

The screenshot shows a web browser window with the address bar containing `virustotal.com/gui/ip-address/23.227.198.203/community`. The search bar contains `23.227.198.203`. The main content area displays two community reports:

- Sekoia.io** (10 months ago):
Hey! 🙌
This server was seen as a #CobaltStrikeC2 server on 2022-05-10 by SEKOIA.IO trackers.
Do not hesitate to get more C2s by searching #CobaltStrikeC2 on VT. 🚀
For more information, visit: <https://www.sekoia.io/en/homepage/>
- drb_ra** (11 months ago):
Cobalt Strike Server Found
C2: HTTPS @ 23[.]227[.]198[.]203:1443
C2 Server: downloads[.]lastupdatebd[.]com,/sq
POST URI: /panel
Country: United States
ASN: HVC-AS
Host Header: downloads[.]lastupdatebd[.]com
#c2 #cobaltstrike

So I confirmed this as Cobalt Strike Command-and-Control (C2) server.



Above screenshot is for overall activity from Brim (Zui)

Finally, The user was affected by the IcedID malware from the 'oceriesfornot.top' domain and attacker gained access to domain controller, so attacker visited malicious sites or links and utilized the access to do Cobalt strike on the victim (bupdater.com).