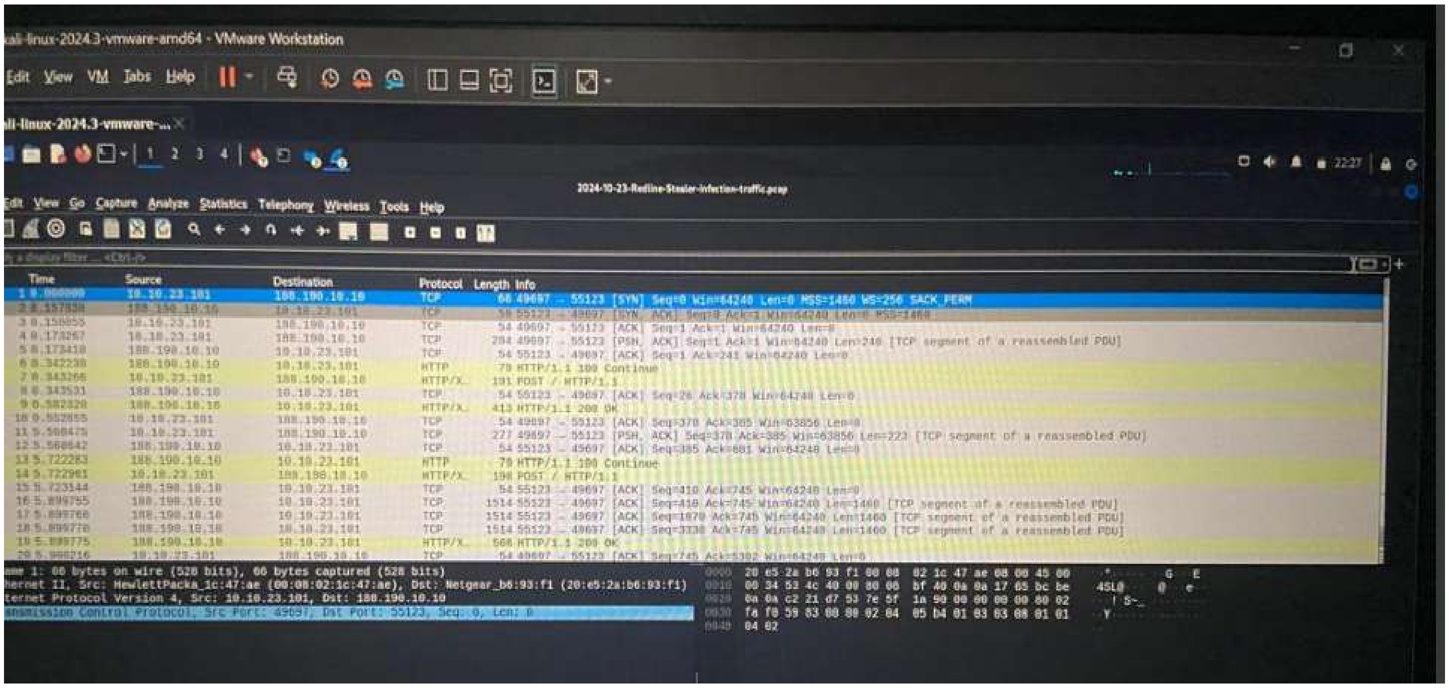
How I traced a malware attack across DNS, HTTP, and TLS traffic to uncover the C2 server and data exfiltration using Wireshark.

Short summary below

Before anyone noticed, an infected machine checked its public IP, established a connection with a remote server, and pushed sensitive data. But how exactly did it happen?

Here's how I uncovered the attack step by step.


kali-linux-2024.3-vmware-amd64 - VMware Workstation
Edit View VM Tabs Help
kali-linux-2024.3-vmware-...
2024-10-23-Redline-Stealer-infection-traffic.pcap
Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
y a display filter … <Ctrl-/>

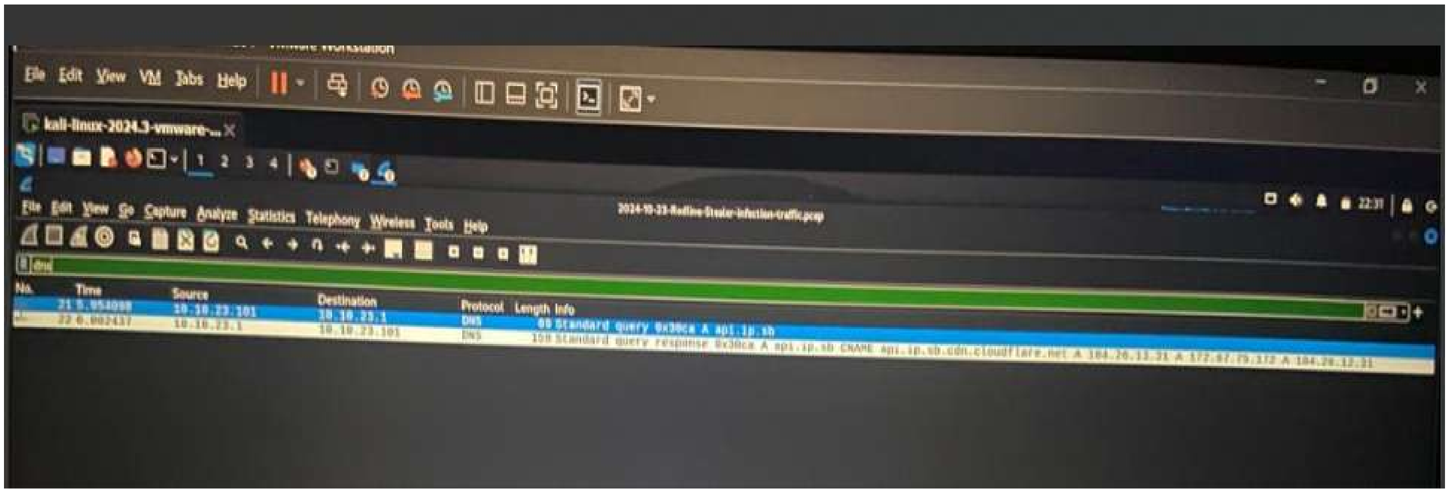
```
   Time       Source          Destination     Protocol Length Info
 1 0.000000   10.10.23.101    188.190.10.10   TCP        66 49697 → 55123 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
 2 0.157858   188.190.10.10   10.10.23.101    TCP        58 55123 → 49697 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
 3 0.158055   10.10.23.101    188.190.10.10   TCP        54 49697 → 55123 [ACK] Seq=1 Ack=1 Win=64240 Len=0
 4 0.173267   10.10.23.101    188.190.10.10   TCP       294 49697 → 55123 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=240 [TCP segment of a reassembled PDU]
 5 0.173418   188.190.10.10   10.10.23.101    TCP        54 55123 → 49697 [ACK] Seq=1 Ack=241 Win=64240 Len=0
 6 0.342238   188.190.10.10   10.10.23.101    HTTP       79 HTTP/1.1 100 Continue
 7 0.343266   10.10.23.101    188.190.10.10   HTTP/X…   191 POST / HTTP/1.1
 8 0.343531   188.190.10.10   10.10.23.101    TCP        54 55123 → 49697 [ACK] Seq=26 Ack=378 Win=64240 Len=0
 9 0.582328   188.190.10.10   10.10.23.101    HTTP/X…   413 HTTP/1.1 200 OK
10 0.552855   10.10.23.101    188.190.10.10   TCP        54 49697 → 55123 [ACK] Seq=378 Ack=385 Win=63856 Len=0
11 5.560475   10.10.23.101    188.190.10.10   TCP       277 49697 → 55123 [PSH, ACK] Seq=378 Ack=385 Win=63856 Len=223 [TCP segment of a reassembled PDU]
12 5.560642   188.190.10.10   10.10.23.101    TCP        54 55123 → 49697 [ACK] Seq=385 Ack=601 Win=64240 Len=0
13 5.722283   188.190.10.10   10.10.23.101    HTTP       79 HTTP/1.1 100 Continue
14 5.722961   10.10.23.101    188.190.10.10   HTTP/X…   198 POST / HTTP/1.1
15 5.723144   188.190.10.10   10.10.23.101    TCP        54 55123 → 49697 [ACK] Seq=410 Ack=745 Win=64240 Len=0
16 5.899755   188.190.10.10   10.10.23.101    TCP      1514 55123 → 49697 [ACK] Seq=410 Ack=745 Win=64240 Len=1460 [TCP segment of a reassembled PDU]
17 5.899766   188.190.10.10   10.10.23.101    TCP      1514 55123 → 49697 [ACK] Seq=1870 Ack=745 Win=64240 Len=1460 [TCP segment of a reassembled PDU]
18 5.899770   188.190.10.10   10.10.23.101    TCP      1514 55123 → 49697 [ACK] Seq=3330 Ack=745 Win=64240 Len=1460 [TCP segment of a reassembled PDU]
19 5.899775   188.190.10.10   10.10.23.101    HTTP/X…   566 HTTP/1.1 200 OK
20 5.900216   10.10.23.101    188.190.10.10   TCP        54 49697 → 55123 [ACK] Seq=745 Ack=5302 Win=64240 Len=0
```

```
ame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
hernet II, Src: HewlettPacka_1c:47:ae (00:08:02:1c:47:ae), Dst: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1)
ternet Protocol Version 4, Src: 10.10.23.101, Dst: 188.190.10.10
ansmission Control Protocol, Src Port: 49697, Dst Port: 55123, Seq: 0, Len: 0
```

```
0000  20 e5 2a b6 93 f1 00 08  02 1c 47 ae 08 00 45 00    *......G..E.
0010  00 34 53 4c 40 00 80 06  bf 40 0a 0a 17 65 bc be   .4SL@....@...e..
0020  0a 0a c2 21 d7 53 7e 5f  1a 90 00 00 00 00 80 02   ...!.S~_........
0030  fa f0 59 03 00 00 02 04  05 b4 01 03 03 08 01 01   ..Y.............
0040  04 02                                              ..
```

Step 1: Identifying suspicious DNS queries

- I started by filtering for DNS requests and found something unusual
- The infected machine (10.10.23.101) queried api.ip.sb
- The DNS resolver responded with multiple Ip addresses, including a cloudfare address
- Things started looking suspicious to me since api.ip.sb is a public IP lookup service used in malware attack to determine the external (public) ip address of the victim machine before communicating with its command and control infrastructure.

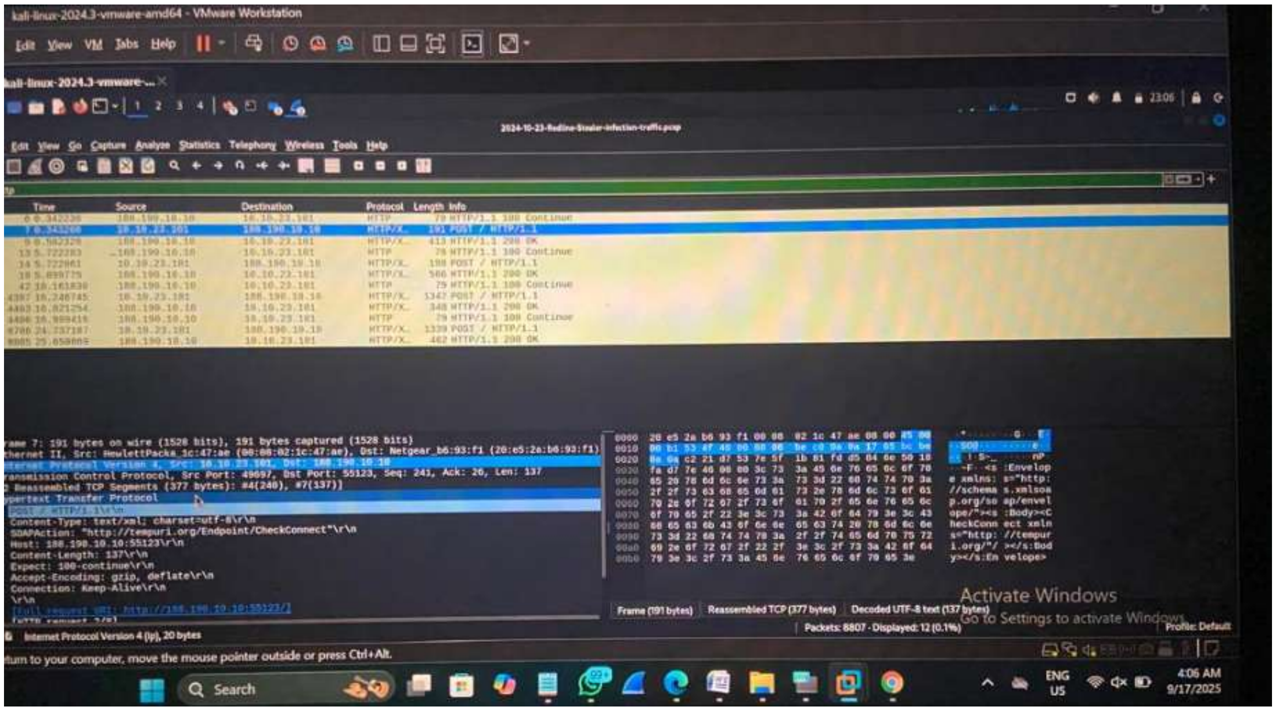


```
dns
No.  Time        Source         Destination    Protocol Length Info
  21 5.954098    10.10.23.101   10.10.23.1     DNS      69     Standard query 0x30ca A api.ip.sb
  22 6.002437    10.10.23.1     10.10.23.101   DNS      159    Standard query response 0x30ca A api.ip.sb CNAME api.ip.sb.cdn.cloudflare.net A 104.26.13.31 A 172.67.75.172 A 104.26.12.31
```

Step 2: Checking for HTTP Traffic

After filtering for HTTP traffic, things started to add up to me

- The infected machine sent multiple POST requests to 188.190.10.10
- The server responded with 200 OK confirming successful data transfer
- The use of HTTP/XML traffic showed structured exfiltration, and the rising payload sizes suggested data was stolen bit by bit.



```
     Time          Source          Destination     Protocol  Length Info
   6 0.342236      188.190.10.10   10.10.23.101    HTTP        79   HTTP/1.1 100 Continue
   7 0.342908      10.10.23.101    188.190.10.10   HTTP/X…    191   POST / HTTP/1.1
   9 0.582326      188.190.10.10   10.10.23.101    HTTP/X…    413   HTTP/1.1 200 OK
  13 5.722283      188.190.10.10   10.10.23.101    HTTP        79   HTTP/1.1 100 Continue
  14 5.722961      10.10.23.101    188.190.10.10   HTTP/X…    198   POST / HTTP/1.1
  18 5.899775      188.190.10.10   10.10.23.101    HTTP/X…    566   HTTP/1.1 200 OK
  42 10.161830     188.190.10.10   10.10.23.101    HTTP        79   HTTP/1.1 100 Continue
4387 10.246745     10.10.23.101    188.190.10.10   HTTP/X…   1347   POST / HTTP/1.1
4403 10.821254     188.190.10.10   10.10.23.101    HTTP/X…    348   HTTP/1.1 200 OK
4406 16.989419     188.190.10.10   10.10.23.101    HTTP        79   HTTP/1.1 100 Continue
8706 24.737187     10.10.23.101    188.190.10.10   HTTP/X…   1339   POST / HTTP/1.1
8805 25.658009     188.190.10.10   10.10.23.101    HTTP/X…    462   HTTP/1.1 200 OK
```

```
rame 7: 191 bytes on wire (1528 bits), 191 bytes captured (1528 bits)
thernet II, Src: HewlettPacka_1c:47:ae (00:08:02:1c:47:ae), Dst: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1)
nternet Protocol Version 4, Src: 10.10.23.101, Dst: 188.190.10.10
ransmission Control Protocol, Src Port: 49697, Dst Port: 55123, Seq: 241, Ack: 26, Len: 137
 Reassembled TCP Segments (377 bytes): #4(240), #7(137)]
ypertext Transfer Protocol
 POST / HTTP/1.1\r\n
 Content-Type: text/xml; charset=utf-8\r\n
 SOAPAction: "http://tempuri.org/Endpoint/CheckConnect"\r\n
 Host: 188.190.10.10:55123\r\n
 Content-Length: 137\r\n
 Expect: 100-continue\r\n
 Accept-Encoding: gzip, deflate\r\n
 Connection: Keep-Alive\r\n
 \r\n
 [Full request URI: http://188.190.10.10:55123/]
 [HTTP request 2/8]
```

```
0000  20 e5 2a b6 93 f1 00 08  02 1c 47 ae 08 00 45 00   ·*·······G···E·
0010  00 b1 53 4f 40 00 80 06  be c0 0a 0a 17 65 bc be   ··SO@········e··
0020  0a 0a c2 21 d7 53 7e 5f  1b 61 fd d5 84 6e 50 18   ···!·S~_·a···nP·
0030  fa d7 7e 46 00 00 3c 73  3a 45 6e 76 65 6c 6f 70   ··~F··<s :Envelop
0040  65 20 78 6d 6c 6e 73 3a  73 3d 22 68 74 74 70 3a   e xmlns: s="http:
0050  2f 2f 73 63 68 65 6d 61  73 2e 78 6d 6c 73 6f 61   //schema s.xmlsoa
0060  70 2e 6f 72 67 2f 73 6f  61 70 2f 65 6e 76 65 6c   p.org/so ap/envel
0070  6f 70 65 2f 22 3e 3c 73  3a 42 6f 64 79 3e 3c 43   ope/"><s :Body><C
0080  68 65 63 6b 43 6f 6e 6e  65 63 74 20 78 6d 6c 6e   heckConn ect xmln
0090  73 3d 22 68 74 74 70 3a  2f 2f 74 65 6d 70 75 72   s="http: //tempur
00a0  69 2e 6f 72 67 2f 22 2f  3e 3c 2f 73 3a 42 6f 64   i.org/"/ ></s:Bod
00b0  79 3e 3c 2f 73 3a 45 6e  76 65 6c 6f 70 65 3e      y></s:En velope>
```

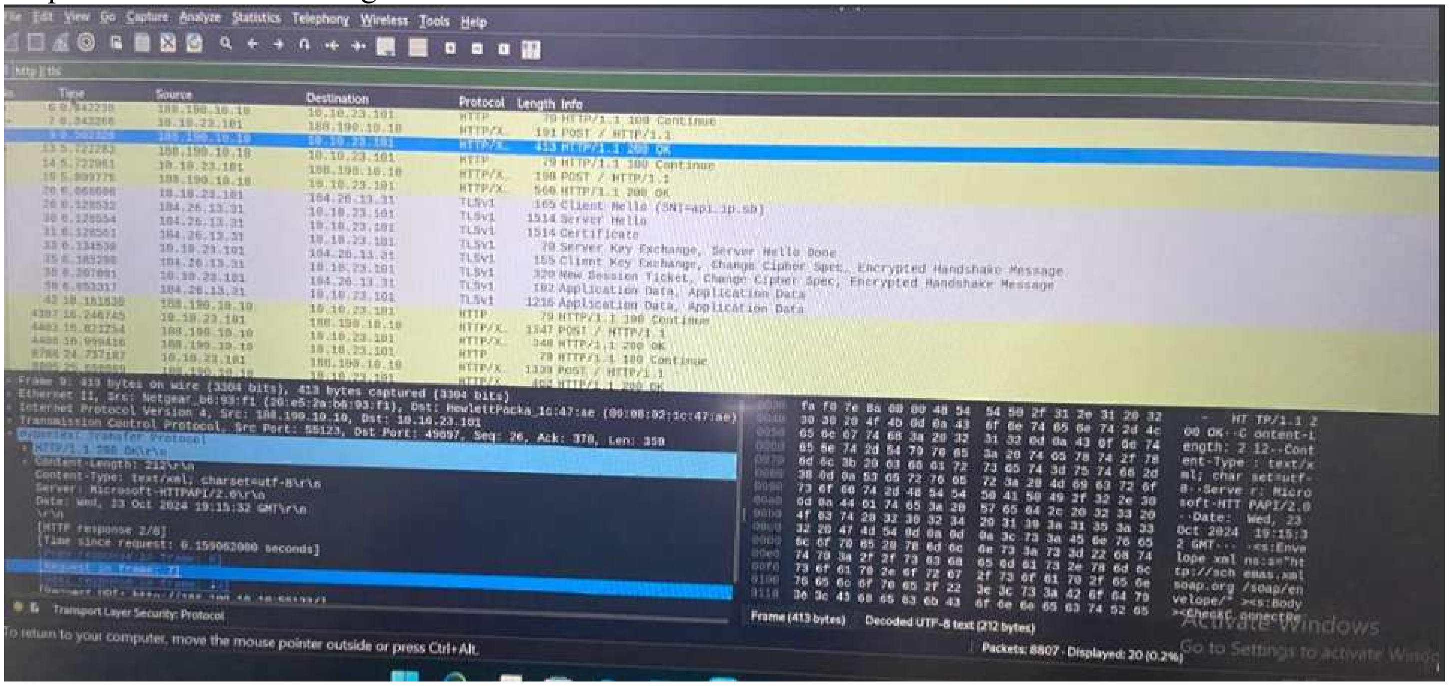
Frame (191 bytes) | Reassembled TCP (377 bytes) | Decoded UTF-8 text (137 bytes)

Packets: 8807 · Displayed: 12 (0.1%)

Step 3: Identifying the C2 communication

Upon checking the TLS traffic, I observed:

- A TLS handshake with a Cloudflare server hosting api.ip.sb.
- Continued requests to the same service, consistent with malware behavior of confirming a system's public IP before initiating data exfiltration.



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http || tls

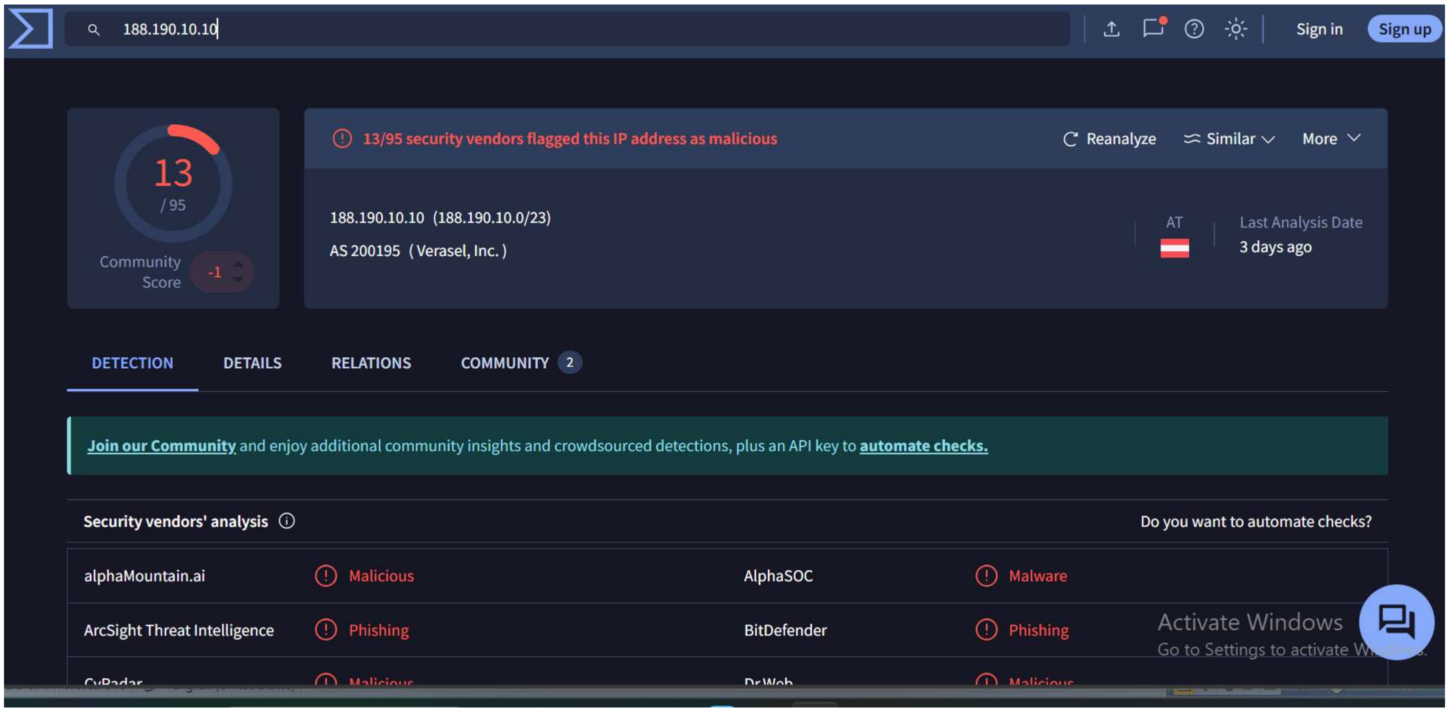
```
   Time          Source          Destination     Protocol  Length Info
      6 0.842238 188.190.10.10   10.10.23.101    HTTP        79 HTTP/1.1 100 Continue
      7 0.843266 10.10.23.101    188.190.10.10   HTTP/X…    191 POST / HTTP/1.1
      9 0.902329 188.190.10.10   10.10.23.101    HTTP/X…    413 HTTP/1.1 200 OK
     13 5.722283 188.190.10.10   10.10.23.101    HTTP        79 HTTP/1.1 100 Continue
     14 5.722961 10.10.23.101    188.190.10.10   HTTP/X…    198 POST / HTTP/1.1
     19 5.889775 188.190.10.10   10.10.23.101    HTTP/X…    566 HTTP/1.1 200 OK
     26 6.068686 10.10.23.101    104.26.13.31    TLSv1      165 Client Hello (SNI=api.ip.sb)
     28 6.128532 104.26.13.31    10.10.23.101    TLSv1     1514 Server Hello
     30 6.128554 104.26.13.31    10.10.23.101    TLSv1     1514 Certificate
     31 6.128561 104.26.13.31    10.10.23.101    TLSv1       70 Server Key Exchange, Server Hello Done
     33 6.134538 10.10.23.101    104.26.13.31    TLSv1      155 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
     35 6.185298 104.26.13.31    10.10.23.101    TLSv1      320 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
     36 6.207091 10.10.23.101    104.26.13.31    TLSv1      192 Application Data, Application Data
     38 6.453317 104.26.13.31    10.10.23.101    TLSv1     1216 Application Data, Application Data
     42 10.181838 188.190.10.10  10.10.23.101    HTTP        79 HTTP/1.1 100 Continue
   4387 16.248745 10.10.23.101   188.190.10.10   HTTP/X…   1347 POST / HTTP/1.1
   4403 16.821254 188.190.10.10  10.10.23.101    HTTP/X…    348 HTTP/1.1 200 OK
   4405 16.999416 188.190.10.10  10.10.23.101    HTTP        79 HTTP/1.1 100 Continue
   8786 24.737187 10.10.23.101   188.190.10.10   HTTP/X…   1339 POST / HTTP/1.1
   [illegible]    188.190.10.10  10.10.23.101    HTTP/X…    482 HTTP/1.1 200 OK

> Frame 9: 413 bytes on wire (3304 bits), 413 bytes captured (3304 bits)
> Ethernet II, Src: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1), Dst: HewlettPacka_1c:47:ae (00:08:02:1c:47:ae)
> Internet Protocol Version 4, Src: 188.190.10.10, Dst: 10.10.23.101
> Transmission Control Protocol, Src Port: 55123, Dst Port: 49697, Seq: 26, Ack: 378, Len: 359
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
  > Content-Length: 212\r\n
    Content-Type: text/xml; charset=utf-8\r\n
    Server: Microsoft-HTTPAPI/2.0\r\n
    Date: Wed, 23 Oct 2024 19:15:32 GMT\r\n
    \r\n
    [HTTP response 2/6]
    [Time since request: 0.159062000 seconds]
    [illegible]
    [Request in frame: 7]
    [illegible]
    [illegible]

0030  fa f0 7e 8a 00 00 48 54  54 50 2f 31 2e 31 20 32   ··~···HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 43  6f 6e 74 65 6e 74 2d 4c   00 OK··C ontent-L
0050  65 6e 67 74 68 3a 20 32  31 32 0d 0a 43 6f 6e 74   ength: 2 12··Cont
0060  65 6e 74 2d 54 79 70 65  3a 20 74 65 78 74 2f 78   ent-Type : text/x
0070  6d 6c 3b 20 63 68 61 72  73 65 74 3d 75 74 66 2d   ml; char set=utf-
0080  38 0d 0a 53 65 72 76 65  72 3a 20 4d 69 63 72 6f   8··Serve r: Micro
0090  73 6f 66 74 2d 48 54 54  50 41 50 49 2f 32 2e 30   soft-HTT PAPI/2.0
00a0  0d 0a 44 61 74 65 3a 20  57 65 64 2c 20 32 33 20   ··Date:  Wed, 23
00b0  4f 63 74 20 32 30 32 34  20 31 39 3a 31 35 3a 33   Oct 2024  19:15:3
00c0  32 20 47 4d 54 0d 0a 0d  0a 3c 73 3a 45 6e 76 65   2 GMT··· ·<s:Enve
00d0  6c 6f 70 65 20 78 6d 6c  6e 73 3a 73 3d 22 68 74   lope xml ns:s="ht
00e0  74 70 3a 2f 2f 73 63 68  65 6d 61 73 2e 78 6d 6c   tp://sch emas.xml
00f0  73 6f 61 70 2e 6f 72 67  2f 73 6f 61 70 2f 65 6e   soap.org /soap/en
0100  76 65 6c 6f 70 65 2f 22  3e 3c 73 3a 42 6f 64 79   velope/" ><s:Body
0110  3e 3c 43 68 65 63 6b 43  6f 6e 6e 65 63 74 52 65   ><CheckC onnectRe

Transport Layer Security: Protocol
Frame (413 bytes)   Decoded UTF-8 text (212 bytes)
Packets: 8807 · Displayed: 20 (0.2%)
```

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.
Activate Windows
Go to Settings to activate Windows.

Key indicator of data exfiltration

- Multiple POST requests from the infected machine to 188.190.10.10 which is likely to be a C2 server.
- The consistent "100 continue" messages which suggests that the server was expecting more data.
- Gradually increasing payload which shows a strong sigh of data exfiltration in progress.

Additionally, a Virus Total check of the suspected C2 server showed that a couple of security vendors had flagged it as malicious, further validating the findings.



13 / 95

Community Score -1

13/95 security vendors flagged this IP address as malicious

188.190.10.10 (188.190.10.0/23)

AS 200195 (Verasel, Inc.)

AT

Last Analysis Date: 3 days ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

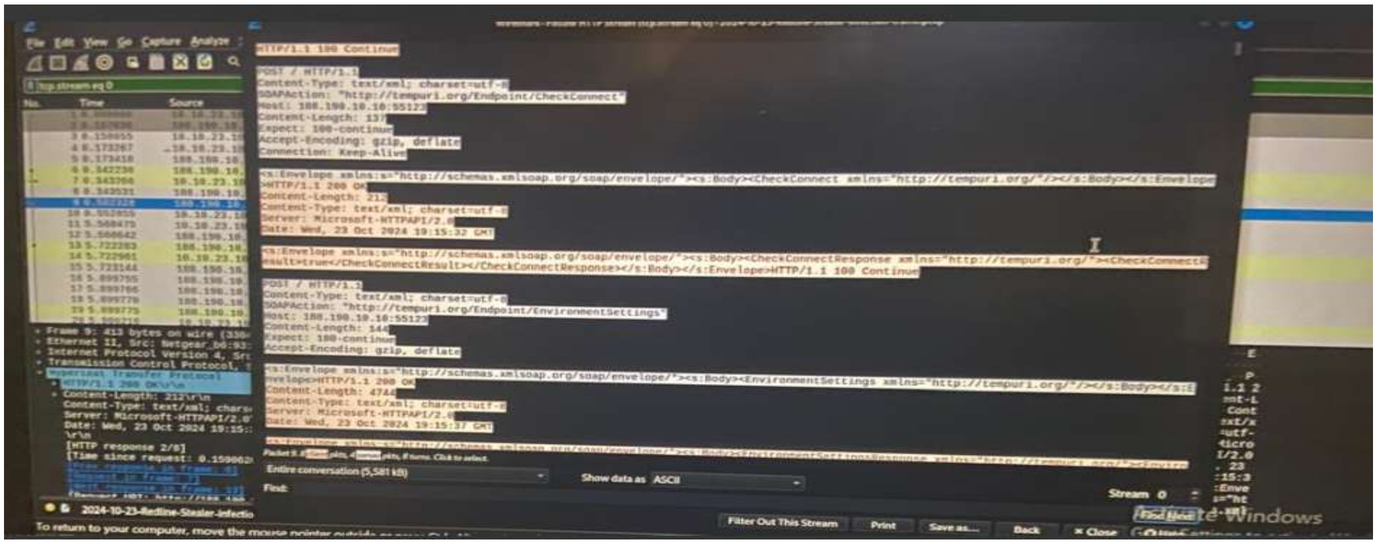
Security vendors' analysis

Do you want to automate checks?

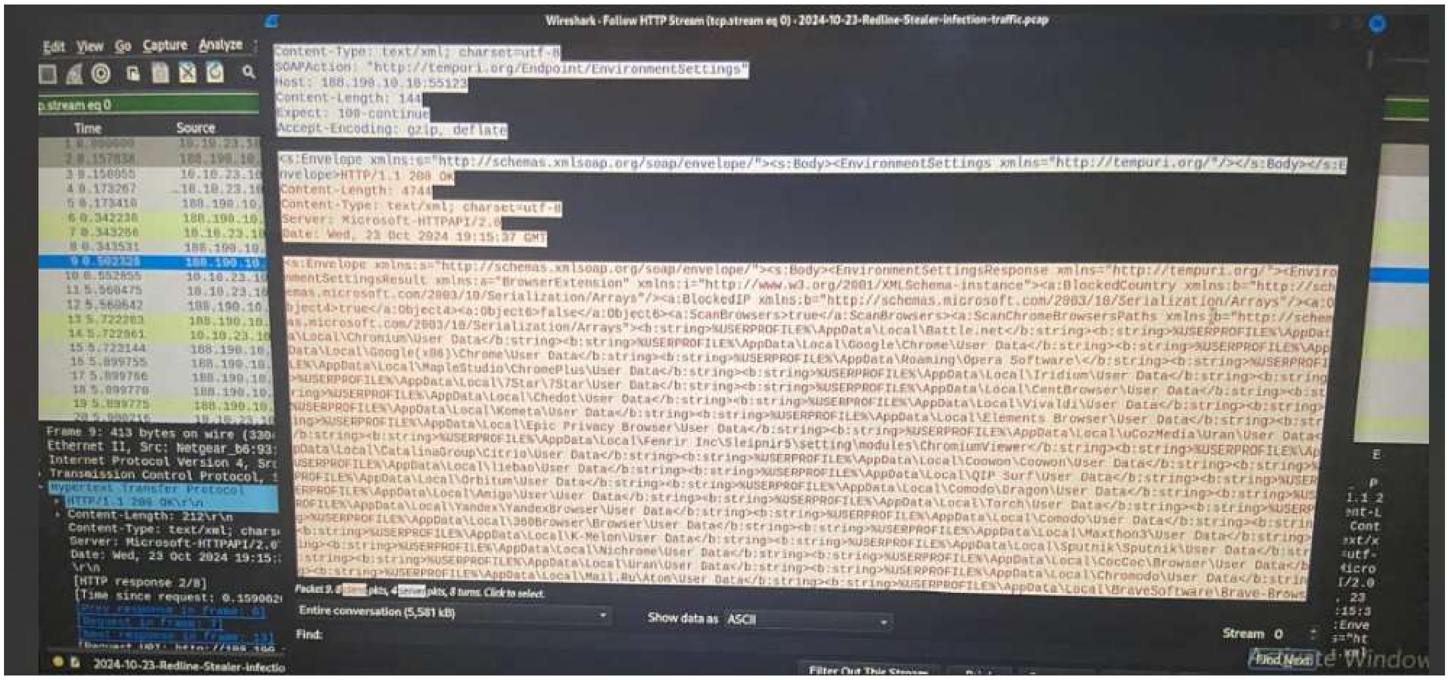
alphaMountain.ai	Malicious	AlphaSOC	Malware
ArcSight Threat Intelligence	Phishing	BitDefender	Phishing
CyRadar	Malicious	Dr.Web	Malicious

Step 4: Following the HTTP stream

To confirm my suspicions, I followed the HTTP stream of the POST requests
Data was actively being exfiltrated.



```
HTTP/1.1 100 Continue

POST / HTTP/1.1
Content-Type: text/xml; charset=utf-8
SOAPAction: "http://tempuri.org/Endpoint/CheckConnect"
Host: 188.190.10.10:55123
Content-Length: 137
Expect: 100-continue
Accept-Encoding: gzip, deflate
Connection: Keep-Alive

<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"><s:Body><CheckConnect xmlns="http://tempuri.org/"/></s:Body></s:Envelope
>HTTP/1.1 200 OK
Content-Length: 212
Content-Type: text/xml; charset=utf-8
Server: Microsoft-HTTPAPI/2.0
Date: Wed, 23 Oct 2024 19:15:32 GMT

<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"><s:Body><CheckConnectResponse xmlns="http://tempuri.org/"><CheckConnectR
esult>true</CheckConnectResult></CheckConnectResponse></s:Body></s:Envelope>HTTP/1.1 100 Continue

POST / HTTP/1.1
Content-Type: text/xml; charset=utf-8
SOAPAction: "http://tempuri.org/Endpoint/EnvironmentSettings"
Host: 188.190.10.10:55123
Content-Length: 144
Expect: 100-continue
Accept-Encoding: gzip, deflate

<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"><s:Body><EnvironmentSettings xmlns="http://tempuri.org/"/></s:Body></s:E
nvelope>HTTP/1.1 200 OK
Content-Length: 4744
Content-Type: text/xml; charset=utf-8
Server: Microsoft-HTTPAPI/2.0
Date: Wed, 23 Oct 2024 19:15:37 GMT
```



```
Content-Type: text/xml; charset=utf-8
SOAPAction: "http://tempuri.org/Endpoint/EnvironmentSettings"
Host: 188.190.10.10:55123
Content-Length: 144
Expect: 100-continue
Accept-Encoding: gzip, deflate

<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"><s:Body><EnvironmentSettings xmlns="http://tempuri.org/"/></s:Body></s:E
nvelope>HTTP/1.1 200 OK
Content-Length: 4744
Content-Type: text/xml; charset=utf-8
Server: Microsoft-HTTPAPI/2.0
Date: Wed, 23 Oct 2024 19:15:37 GMT

<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"><s:Body><EnvironmentSettingsResponse xmlns="http://tempuri.org/"><Enviro
nmentSettingsResult xmlns:a="BrowserExtension" xmlns:i="http://www.w3.org/2001/XMLSchema-instance"><a:BlockedCountry xmlns:b="http://sch
emas.microsoft.com/2003/10/Serialization/Arrays"/><a:BlockedIP xmlns:b="http://schemas.microsoft.com/2003/10/Serialization/Arrays"/><a:O
bject4>true</a:Object4><a:Object6>false</a:Object6><a:ScanBrowsers>true</a:ScanBrowsers><a:ScanChromeBrowsersPaths xmlns:b="http://schem
as.microsoft.com/2003/10/Serialization/Arrays"><b:string>%USERPROFILE%\AppData\Local\Battle.net</b:string><b:string>%USERPROFILE%\AppDat
a\Local\Chromium\User Data</b:string><b:string>%USERPROFILE%\AppData\Local\Google\Chrome\User Data</b:string><b:string>%USERPROFILE%\App
Data\Local\Google(x86)\Chrome\User Data</b:string><b:string>%USERPROFILE%\AppData\Roaming\Opera Software\</b:string><b:string>%USERPROFI
LE%\AppData\Local\MapleStudio\ChromePlus\User Data</b:string><b:string>%USERPROFILE%\AppData\Local\Iridium\User Data</b:string><b:string
>%USERPROFILE%\AppData\Local\7Star\7Star\User Data</b:string><b:string>%USERPROFILE%\AppData\Local\CentBrowser\User Data</b:string><b:st
ring>%USERPROFILE%\AppData\Local\Chedot\User Data</b:string><b:string>%USERPROFILE%\AppData\Local\Vivaldi\User Data</b:string><b:string>
%USERPROFILE%\AppData\Local\Kometa\User Data</b:string><b:string>%USERPROFILE%\AppData\Local\Elements Browser\User Data</b:string><b:str
ing>%USERPROFILE%\AppData\Local\Epic Privacy Browser\User Data</b:string><b:string>%USERPROFILE%\AppData\Local\uCozMedia\Uran\User Data<
/b:string><b:string>%USERPROFILE%\AppData\Local\Fenrir Inc\Sleipnir5\setting\modules\ChromiumViewer</b:string><b:string>%USERPROFILE%\Ap
pData\Local\CatalinaGroup\Citrio\User Data</b:string><b:string>%USERPROFILE%\AppData\Local\Coowon\Coowon\User Data</b:string><b:string>%
USERPROFILE%\AppData\Local\liebao\User Data</b:string><b:string>%USERPROFILE%\AppData\Local\QIP Surf\User Data</b:string><b:string>%USER
PROFILE%\AppData\Local\Orbitum\User Data</b:string><b:string>%USERPROFILE%\AppData\Local\Comodo\Dragon\User Data</b:string><b:string>%US
ERPROFILE%\AppData\Local\Amigo\User\User Data</b:string><b:string>%USERPROFILE%\AppData\Local\Torch\User Data</b:string><b:string>%USERP
ROFILE%\AppData\Local\Yandex\YandexBrowser\User Data</b:string><b:string>%USERPROFILE%\AppData\Local\Comodo\User Data</b:string><b:strin
g>%USERPROFILE%\AppData\Local\360Browser\Browser\User Data</b:string><b:string>%USERPROFILE%\AppData\Local\Maxthon3\User Data</b:string>
<b:string>%USERPROFILE%\AppData\Local\K-Melon\User Data</b:string><b:string>%USERPROFILE%\AppData\Local\Sputnik\Sputnik\User Data</b:str
ing><b:string>%USERPROFILE%\AppData\Local\Nichrome\User Data</b:string><b:string>%USERPROFILE%\AppData\Local\CocCoc\Browser\User Data</b
:string><b:string>%USERPROFILE%\AppData\Local\Uran\User Data</b:string><b:string>%USERPROFILE%\AppData\Local\Chromodo\User Data</b:strin
g><b:string>%USERPROFILE%\AppData\Local\Mail.Ru\Atom\User Data</b:string><b:string>%USERPROFILE%\AppData\Local\BraveSoftware\Brave-Brows
```

Wireshark · Follow HTTP Stream (tcp.stream eq 0) · 2024-10-23-Redline-Stealer-infection-traffic.pcap
Entire conversation (5,581 kB)
Show data as ASCII
Find:
Stream 0
Find Next

CONCLUSION:

The compromised host (10.10.23.101) transmitted stolen data to 188.190.10.10, then the malware leveraged XML over HTTP, a common approach for covert exfiltration. It appeared to query its public IP prior to data theft possibly to evade sandbox detection.

Note: Careful traffic analysis is essential as malware always leaves artifacts, and with proper methods, these can be detected.

What’s your preferred way to spot malicious traffic? Let’s discuss below!

Incident Response Report: Malware Infection Leading to Data Exfiltration

Incident Summary: A malware infection resulted in unauthorized data exfiltration via HTTP POST requests to an external server. Network traffic analysis revealed suspicious DNS, HTTP, and TLS activity, leading to the discovery of potential C2 communication and structured data exfiltration.

This report follows the four key steps of the incident response process: Identification, Containment, Eradication, and Recovery.

Identification

The incident was first detected through suspicious network activity originating from an internal host (10.10.23.101). A detailed packet-level investigation in Wireshark revealed clear signs of malware behavior and data exfiltration.

Evidence of Compromise

- **DNS Analysis**
  - The host queried for api.ip.sb
  - The local resolver (10.10.23.1) returned multiple IPs, including Cloudflare infrastructure.
  - This domain, often used to check a system's public IP, is frequently abused by malware to determine if it is running in a sandbox before establishing C2 communication.
- **HTTP Analysis**
  - Shortly after the DNS query, the host initiated multiple HTTP **POST** requests to 188.190.10.10
  - The server acknowledged with 200 OK, confirming successful data uploads.
  - Payload sizes gradually increased, pointing to staged exfiltration.
- **TLS Analysis**
  - A TLS handshake occurred with Cloudflare services hosting api.ip.sb
  - Multiple encrypted requests reinforced that the system was validating its public IP prior to data theft.
- **C2 Indicators**
  - Repeated XML-based POST requests to the external server were observed.
  - Intermittent 100 Continue messages suggested the server was expecting larger uploads.
  - Progressive payload growth confirmed ongoing exfiltration attempts.

Containment

After confirming the malicious behavior, immediate steps were taken to contain the threat and stop further data leakage.

Short-Term Actions

- Blocked all outbound traffic to 188.190.10.10 at the perimeter firewall.
- Disconnected the compromised host (10.10.23.101) from the corporate network.
- Suspicious processes were identified and terminated on the infected system.

Long-Term Actions

- Monitored network logs for any repeated connections to malicious domains/IPs.
- Placed the affected host in isolation for forensic examination.
- Implemented DNS filtering rules to block unauthorized requests to api.ip.sb.

Eradication & Recovery

With the threat contained, the focus shifted to eliminating the malware and restoring system integrity.

Eradication Steps

- Performed in-depth forensic analysis on the infected endpoint.
- Located and removed persistence mechanisms, such as registry entries and scheduled tasks.
- Executed comprehensive malware scans to ensure no secondary infections remained.

Recovery Measures

- Reimaged or restored the host from a verified clean backup.
- Strengthened network segmentation to restrict unauthorized external communications.
- Enhanced EDR policies to flag anomalous HTTP POST behavior and unusual TLS connections.

Lessons Learned: Monitoring DNS and HTTP traffic is crucial, as even small anomalies can reveal larger exfiltration attempts. Strengthening segmentation, DNS filtering, and EDR helps prevent future incidents.