# Compromised

Sherlock Scenario
Our SOC team detected suspicious activity in Network Traffic, the machine has been compromised and company information that should not have been there has now been stolen – it's up to you to figure out what has happened and what data has been taken.

Task 1:
What is the IP address used for initial access?

I checked the Conversations and filtered by the Packets and found an IP which is reported on OSINT sites.

Ethernet · 3 | IPv4 · 18 | IPv6 | TCP · 218 | UDP · 2188

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 172.16.1.191 | 172.16.1.16 | 29,771 | 5 MB | 16,010 | 2 MB | 13,761 | 4 MB | 0.000000 | 6880.0934 | 1749 bits/s | 4566 bits/s |
| 172.16.1.191 | 23.163.0.37 | 6,978 | 4 MB | 3,188 | 640 kB | 3,790 | 3 MB | 811.959972 | 937.4236 | 5461 bits/s | 28 kbps |
| 172.16.1.191 | 162.252.172.54 | 1,130 | 1 MB | 202 | 11 kB | 928 | 1 MB | 41.558121 | 4.9051 | 18 kbps | 2183 kbps |

Answer: 162.252.172.54

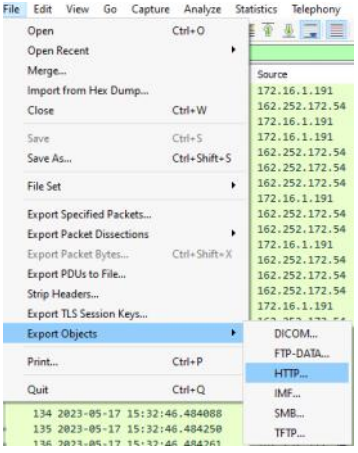
Task 2:
What is the SHA256 hash of the malware?

I filtered for ip.addr == 162.252.172.54 and found a suspicious GET request

ip.addr == 162.252.172.54

| No. | Time | Source | SRC Port | Destination | DST Port | Protocol | Length | Info |
|---|---|---|---|---|---|---|---|---|
| 113 | 2023-05-17 15:32:45.818015 | 172.16.1.191 | 51221 | 162.252.172.54 | 80 | TCP | 66 | 51221 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM |
| 114 | 2023-05-17 15:32:46.152656 | 162.252.172.54 | 80 | 172.16.1.191 | 51221 | TCP | 58 | 80 → 51221 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 |
| 115 | 2023-05-17 15:32:46.152858 | 172.16.1.191 | 51221 | 162.252.172.54 | 80 | TCP | 54 | 51221 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0 |
| 116 | 2023-05-17 15:32:46.155265 | 172.16.1.191 | 51221 | 162.252.172.54 | 80 | HTTP | 226 | GET /9GQ5A8/6ctf5JL HTTP/1.1 |

Then I downloaded the file from Export Objects - HTTP




Wireshark · Export · HTTP object list

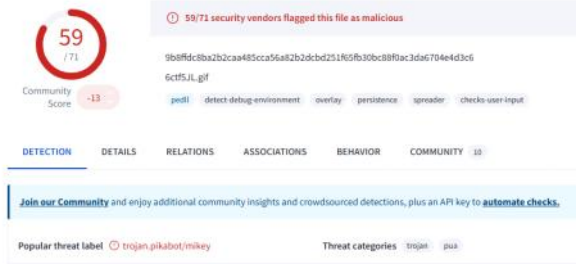
Text Filter:

| Packet | Hostname | Content Type | Size | Filename |
|---|---|---|---|---|
| 1238 | 162.252.172.54 | image/gif | 1288 kB | 6ctf5JL |

Answer: 9b8ffdc8ba2b2caa485cca56a82b2dcbd251f65fb30bc88f0ac3da6704e4d3c6

Task 3:
What is the Family label of the malware?

I checked the SHA256 on Virus Total and the threat label is "pikabot"




Answer: Pikabot

Task 4:
When was the malware first seen in the wild (UTC)?

The timestamp can be found from the Details tab in Virus Total

**History**

| | |
|---|---|
| Creation Time | 2023-05-17 09:38:43 UTC |
| First Seen In The Wild | 2023-05-19 14:01:21 UTC |
| First Submission | 2023-05-17 19:04:23 UTC |
| Last Submission | 2025-02-05 09:35:14 UTC |
| Last Analysis | 2025-02-03 22:43:25 UTC |

Answer: 2023-05-19 14:01:21

Task 5:
The malware used HTTPS traffic with a self-signed certificate. What are the ports, from smallest to largest?

I filtered for "tls.handshake.type == 2" and sort the source ports.
The first packets was from 443, I checked the TCP packets but it all look like a legitimate packets related to DigiCert.

After the 443 port there was several source IPs with same ports such as 2078, 2222, 32999.
I checked some of the source IPs on OSINT sites and some of them were reported as malicious.

tls.handshake.type == 2

| No. | Time | Source | SRC Port | Destination | DST Port | Protocol | Length | Info |
|---|---|---|---|---|---|---|---|---|
| 9496 | 2023-05-17 16:18:37.691808 | 129.213.54.49 | 2078 | 172.16.1.191 | 51291 | TLSv1.2 | 1430 | Server Hello |
| 9521 | 2023-05-17 16:22:53.166245 | 45.85.235.39 | 2078 | 172.16.1.191 | 51300 | TLSv1.2 | 1514 | Server Hello |
| 9659 | 2023-05-17 16:48:24.692515 | 129.153.135.83 | 2078 | 172.16.1.191 | 51336 | TLSv1.2 | 1430 | Server Hello |
| 9676 | 2023-05-17 16:48:25.471638 | 129.153.135.83 | 2078 | 172.16.1.191 | 51337 | TLSv1.2 | 163 | Server Hello, Change Cipher Spec, Encrypted Handshake Message |
| 9696 | 2023-05-17 16:48:26.445127 | 129.153.135.83 | 2078 | 172.16.1.191 | 51338 | TLSv1.2 | 163 | Server Hello, Change Cipher Spec, Encrypted Handshake Message |
| 13047 | 2023-05-17 16:52:41.814364 | 193.122.200.171 | 2078 | 172.16.1.191 | 51345 | TLSv1.2 | 1430 | Server Hello |
| 21783 | 2023-05-17 17:05:27.882466 | 129.213.54.49 | 2078 | 172.16.1.191 | 51369 | TLSv1.2 | 1430 | Server Hello |
| 24741 | 2023-05-17 17:09:43.208711 | 45.85.235.39 | 2078 | 172.16.1.191 | 51396 | TLSv1.2 | 1514 | Server Hello |
| 38917 | 2023-05-17 17:35:13.868735 | 129.153.135.83 | 2078 | 172.16.1.191 | 51748 | TLSv1.2 | 1430 | Server Hello |
| 38943 | 2023-05-17 17:39:28.973613 | 193.122.200.171 | 2078 | 172.16.1.191 | 51762 | TLSv1.2 | 1514 | Server Hello |
| 39015 | 2023-05-17 17:52:14.684657 | 129.213.54.49 | 2078 | 172.16.1.191 | 51767 | TLSv1.2 | 1430 | Server Hello |
| 39038 | 2023-05-17 17:56:29.988528 | 45.85.235.39 | 2078 | 172.16.1.191 | 51768 | TLSv1.2 | 1430 | Server Hello |
| 1293 | 2023-05-17 15:35:56.920963 | 132.148.79.222 | 2222 | 172.16.1.191 | 51227 | TLSv1.2 | 1514 | Server Hello |
| 1331 | 2023-05-17 15:40:11.973118 | 132.148.79.222 | 2222 | 172.16.1.191 | 51230 | TLSv1.2 | 163 | Server Hello, Change Cipher Spec, Encrypted Handshake Message |
| 1352 | 2023-05-17 15:44:27.958654 | 94.199.173.6 | 2222 | 172.16.1.191 | 51242 | TLSv1.2 | 1430 | Server Hello |
| 1611 | 2023-05-17 16:10:04.948494 | 144.172.126.136 | 2222 | 172.16.1.191 | 51275 | TLSv1.2 | 1514 | Server Hello |
| 1627 | 2023-05-17 16:10:06.007951 | 144.172.126.136 | 2222 | 172.16.1.191 | 51276 | TLSv1.2 | 163 | Server Hello, Change Cipher Spec, Encrypted Handshake Message |
| 1649 | 2023-05-17 16:10:07.087242 | 144.172.126.136 | 2222 | 172.16.1.191 | 51277 | TLSv1.2 | 163 | Server Hello, Change Cipher Spec, Encrypted Handshake Message |
| 9546 | 2023-05-17 16:27:08.521278 | 132.148.79.222 | 2222 | 172.16.1.191 | 51305 | TLSv1.2 | 1430 | Server Hello |
| 9571 | 2023-05-17 16:31:24.335926 | 94.199.173.6 | 2222 | 172.16.1.191 | 51319 | TLSv1.2 | 1430 | Server Hello |
| 15965 | 2023-05-17 16:56:57.189423 | 144.172.126.136 | 2222 | 172.16.1.191 | 51347 | TLSv1.2 | 1430 | Server Hello |
| 27654 | 2023-05-17 17:13:58.276437 | 132.148.79.222 | 2222 | 172.16.1.191 | 51415 | TLSv1.2 | 1430 | Server Hello |
| 31306 | 2023-05-17 17:18:13.728966 | 94.199.173.6 | 2222 | 172.16.1.191 | 51462 | TLSv1.2 | 1514 | Server Hello |
| 38967 | 2023-05-17 17:43:44.372072 | 144.172.126.136 | 2222 | 172.16.1.191 | 51765 | TLSv1.2 | 1430 | Server Hello |
| 39063 | 2023-05-17 18:00:44.813299 | 132.148.79.222 | 2222 | 172.16.1.191 | 51770 | TLSv1.2 | 1430 | Server Hello |
| 39087 | 2023-05-17 18:05:00.265465 | 94.199.173.6 | 2222 | 172.16.1.191 | 51772 | TLSv1.2 | 1430 | Server Hello |
| 1462 | 2023-05-17 15:57:15.359121 | 129.80.164.200 | 32999 | 172.16.1.191 | 51262 | TLSv1.2 | 1514 | Server Hello |
| 1478 | 2023-05-17 15:57:16.344685 | 129.80.164.200 | 32999 | 172.16.1.191 | 51263 | TLSv1.2 | 163 | Server Hello, Change Cipher Spec, Encrypted Handshake Message |
| 1497 | 2023-05-17 15:57:17.315625 | 129.80.164.200 | 32999 | 172.16.1.191 | 51264 | TLSv1.2 | 163 | Server Hello, Change Cipher Spec, Encrypted Handshake Message |
| 6583 | 2023-05-17 16:14:22.489372 | 129.153.22.231 | 32999 | 172.16.1.191 | 51280 | TLSv1.2 | 1430 | Server Hello |

Answer: 2078, 2222, 32999

Task 6:
What is the id-at-localityName of the self-signed certificate associated with the first malicious IP?

I searched for localityName as String and found the packet with the name

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 1249 | 2023-05-17 15:35:55.635902 | 45.85.235.39 | 2078 | 172.16.1.191 | 51226 | TLSv1.2 | 838 | Certificate, Server Key Exchange, Server Hello Done |
| 1253 | 2023-05-17 15:35:55.659668 | 45.85.235.39 | 2078 | 172.16.1.191 | 51226 | TCP | 54 | 2078 → 51226 [ACK] Seq=2161 Ack=241 Win=64240 Len=0 |

```
> Frame 1249: 838 bytes on wire (6704 bits), 838 bytes captured (6704 bits)
> Ethernet II, Src: Cisco_7a:1d:39 (08:cc:a7:7a:1d:39), Dst: HewlettP_86:bf:a2 (00:0f:61:86:bf:a2)
> Internet Protocol Version 4, Src: 45.85.235.39, Dst: 172.16.1.191
> Transmission Control Protocol, Src Port: 2078, Dst Port: 51226, Seq: 1377, Ack: 148, Len: 784
> [2 Reassembled TCP Segments (1520 bytes): #1248(1306), #1249(214)]
v Transport Layer Security
  v TLSv1.2 Record Layer: Handshake Protocol: Certificate
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 1515
    v Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 1511
        Certificates Length: 1508
      v Certificates (1508 bytes)
          Certificate Length: 1505
          Certificate: 308205dd308203c5a003020102021451651c79bfe60a17bc97bcb437c0f3ec25f7f6ec530… (id-at-commonName=votation.bzh,id-at-localityName=Pyopneumopericardium,id-at-organizationalUnitName=Undeligh
            v signedCertificate
                version: v3 (2)
                serialNumber: 0x5651c79bfe60a17bc97bcb437c0f3ec25f7f6ec5
              > signature (sha256WithRSAEncryption)
              v issuer: rdnSequence (0)
                > rdnSequence: 6 items (id-at-commonName=votation.bzh,id-at-localityName=Pyopneumopericardium,id-at-organizationalUnitName=Undelightful,id-at-organizationName=Uneared Inc.,id-at-stateOrPro
```

Answer: Pyopneumopericardium

Task 7:
What is the notBefore time(UTC) for this self-signed certificate?

I followed the TCP Stream from the packet in task 6, then I noticed something familiar ending with "Z" which is known format for UTC.
Then I gave It to the Chat to calculate it to UTC

Wireshark · Follow TCP Stream (tcp.stream eq 22) · capture.pcap

```
....>...:..dd.\.%.^.....9..6...`....{A.......$.,.+.0./.$.#.(.'.
.          .........=.<.5./.....
.................
.............................#.......i...l.N.$B.*@jzW.   ..X...I..2T.....=...N.(.b3..mg.'......[..
(C..yjv..?/..`N.r..Q.x.h........U.:R..]..*.;^.y..
..Yb..F..#:./Z...K
....m../b..r~7.M..?.._V..{3........^4..}................A...=.......7..M....3..F...z3...<3k......0.................#.....................0...0..........VQ...`.{.{.C|.>._.n.0
.          *.H..
.....0~1.0  ..U....SX1.0           ..U....KI1.0...U.
..Uneared Inc.1.0...U....Undelightful1.0...U....Pyopneumopericardium1.0...U....votation.bzh0..
230514083652Z.
240513083652Z0~1.0     ..U....SX1.0           ..U....KI1.0...U.
```

Answer: 2023-05-14 08:36:52

Task 8:
What was the domain used for tunneling?

I filtered for "DNS" and found a repeated queries to the domain "steasteel.net" with a TXT Records.
TXT (Text) records are a type of DNS (Domain Name System) record that allows domain owners to store arbitrary text data in the DNS system.
Attackers abuse TXT records for DNS tunneling, hiding malware communication inside these records.

dns

| No. | Time | Source | SRC Port | Destination | DST Port | Protocol | Length | Info |
|---|---|---|---|---|---|---|---|---|
| 2 | 2023-05-17 15:32:04.260187 | 172.16.1.16 | 53 | 172.16.1.191 | 51176 | DNS | 92 | Standard query response 0x0aec A webmasterdev.com A 184.168.98.68 |
| 1433 | 2023-05-17 15:53:00.429463 | 172.16.1.16 | 53 | 172.16.1.191 | 63562 | DNS | 135 | Standard query response 0x30f0 A twitter.com A 104.244.42.1 A 104.244.42.65 A 104.244.42.193 A 104.244.42.129 |
| 1647 | 2023-05-17 16:10:07.078673 | 172.16.1.16 | 53 | 172.16.1.191 | 63893 | DNS | 351 | Standard query response 0x6394 TXT aaa.h.dns.steasteel.net TXT |
| 1656 | 2023-05-17 16:10:07.231749 | 172.16.1.16 | 53 | 172.16.1.191 | 52094 | DNS | 351 | Standard query response 0xb328 TXT baa.h.dns.steasteel.net TXT |
| 1659 | 2023-05-17 16:10:07.401972 | 172.16.1.16 | 53 | 172.16.1.191 | 52151 | DNS | 351 | Standard query response 0x28cf TXT caa.h.dns.steasteel.net TXT |
| 1662 | 2023-05-17 16:10:07.552499 | 172.16.1.16 | 53 | 172.16.1.191 | 49422 | DNS | 351 | Standard query response 0xf622 TXT daa.h.dns.steasteel.net TXT |
| 1665 | 2023-05-17 16:10:07.722425 | 172.16.1.16 | 53 | 172.16.1.191 | 51247 | DNS | 351 | Standard query response 0x8d0e TXT eaa.h.dns.steasteel.net TXT |
| 1668 | 2023-05-17 16:10:07.883772 | 172.16.1.16 | 53 | 172.16.1.191 | 53606 | DNS | 351 | Standard query response 0xc57e TXT faa.h.dns.steasteel.net TXT |
| 1673 | 2023-05-17 16:10:08.032401 | 172.16.1.16 | 53 | 172.16.1.191 | 51203 | DNS | 351 | Standard query response 0x149a TXT gaa.h.dns.steasteel.net TXT |
| 1676 | 2023-05-17 16:10:08.182033 | 172.16.1.16 | 53 | 172.16.1.191 | 63879 | DNS | 351 | Standard query response 0x8770 TXT haa.h.dns.steasteel.net TXT |
| 1679 | 2023-05-17 16:10:08.342492 | 172.16.1.16 | 53 | 172.16.1.191 | 60930 | DNS | 351 | Standard query response 0xcaaa TXT iaa.h.dns.steasteel.net TXT |
| 1682 | 2023-05-17 16:10:08.491904 | 172.16.1.16 | 53 | 172.16.1.191 | 52338 | DNS | 351 | Standard query response 0x49be TXT jaa.h.dns.steasteel.net TXT |
| 1685 | 2023-05-17 16:10:08.648652 | 172.16.1.16 | 53 | 172.16.1.191 | 57062 | DNS | 351 | Standard query response 0xf8be TXT kaa.h.dns.steasteel.net TXT |
| 1688 | 2023-05-17 16:10:08.804369 | 172.16.1.16 | 53 | 172.16.1.191 | 52735 | DNS | 351 | Standard query response 0xd836 TXT laa.h.dns.steasteel.net TXT |
| 1691 | 2023-05-17 16:10:08.969841 | 172.16.1.16 | 53 | 172.16.1.191 | 65249 | DNS | 351 | Standard query response 0x1c17 TXT maa.h.dns.steasteel.net TXT |
| 1694 | 2023-05-17 16:10:09.122749 | 172.16.1.16 | 53 | 172.16.1.191 | 49296 | DNS | 351 | Standard query response 0x7af5 TXT naa.h.dns.steasteel.net TXT |
| 1697 | 2023-05-17 16:10:09.281742 | 172.16.1.16 | 53 | 172.16.1.191 | 52476 | DNS | 351 | Standard query response 0xe7c3 TXT oaa.h.dns.steasteel.net TXT |
| 1700 | 2023-05-17 16:10:09.474627 | 172.16.1.16 | 53 | 172.16.1.191 | 51686 | DNS | 351 | Standard query response 0xffb1 TXT paa.h.dns.steasteel.net TXT |
| 1703 | 2023-05-17 16:10:09.622468 | 172.16.1.16 | 53 | 172.16.1.191 | 50802 | DNS | 351 | Standard query response 0xd406 TXT qaa.h.dns.steasteel.net TXT |
| 1706 | 2023-05-17 16:10:09.778613 | 172.16.1.16 | 53 | 172.16.1.191 | 60236 | DNS | 351 | Standard query response 0x98a5 TXT raa.h.dns.steasteel.net TXT |

Answer: steasteel.net