

FLAG-1 IP sospechosa identificada



Para identificar la dirección IP sospechosa, accedí a la sección de **Conversaciones** en Wireshark, donde analicé el tráfico entre las diferentes direcciones IP activas en la red. Observando el volumen y comportamiento de los paquetes, detecté una IP que generaba ruido anómalo: 162.252.172.54

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	29771	5431 k	16010	1504 k	13761	3927 k	0.0000000	6880.0934	1749	4566
172.16.1.191	184.168.98.68	110	91 k	35	3142	75	88 k	0.009654	8.3678	3003	84 k
172.16.1.191	162.252.172.54	1130	1349 k	202	11 k	928	1398 k	41.558121	4.9051	18 k	2183 k
172.16.1.191	45.85.235.39	126	41 k	68	25 k	58	16 k	230.635856	8544.6235	24	15
172.16.1.191	132.146.79.222	123	27 k	68	8950	55	16 k	232.150737	8798.1666	8	16
172.16.1.191	172.16.1.255	13	3159	13	3159	0	0	385.730074	8642.9959	2	0
172.16.1.191	94.199.173.6	95	20 k	53	7082	42	13 k	783.004391	8542.3758	6	12
172.16.1.191	185.87.148.132	109	22 k	60	8689	49	14 k	998.372934	5736.2141	12	19
172.16.1.191	104.244.42.1	23	6872	12	1585	11	5287	1256.171265	109.9995	115	384
172.16.1.191	129.80.164.200	108	22 k	59	8640	49	14 k	1518.630725	5735.8632	12	19
172.16.1.191	129.153.135.83	114	22 k	63	8951	51	13 k	1767.925865	5731.4145	12	18
172.16.1.191	193.122.200.171	111	22 k	61	8748	50	14 k	2023.139920	5731.3266	12	19
172.16.1.191	144.172.126.136	107	21 k	59	8640	48	13 k	2280.097138	5729.6977	12	18
172.16.1.191	129.153.22.231	72	15 k	40	5290	32	10 k	2537.737639	5727.3353	7	14
172.16.1.191	129.213.54.49	73	15 k	41	5338	32	10 k	2792.928344	5727.2844	7	14
172.16.1.191	104.244.42.193	34	5460	18	3494	16	1966	4070.132264	2919.9748	9	5
172.16.1.191	23.163.6.37	6978	4022 k	3188	640 k	3790	3382 k	5811.959722	932.4236	5461	28 k
172.16.1.191	104.18.32.68	9	2665	5	442	4	2223	5813.540464	101.5020	34	175

Posteriormente, consulté esta IP en **VirusTotal**, donde fue clasificada como maliciosa.

162.252.172.54

4 / 94
Community Score

4/94 security vendors flagged this IP address as malicious

162.252.172.54 (162.252.172.0/22)
AS 9009 (M247 Europe SRL)

US Last Analysis Date
2 days ago

REanalyze Similar More

DETECTION DETAILS RELATIONS COMMUNITY

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

Crowdsourced context

HIGH 0 MEDIUM 1 LOW 0 INFO 0 SUCCESS 0

URLhaus IOCs for 2023-05-17 - according to source ArcSight Threat Intelligence - 2 years ago
↳ Malware payload delivery host

Security vendors' analysis

Vendor	Analysis
CRDF	Malicious
CyRadar	Malicious
ESET	Malware
Forcepoint ThreatSeeker	Malicious

Do you want to automate checks?

vemos que es maliciosa así encontrando la respuesta

Task 1

What is the IP address used for initial access?

162.252.172.54

✓

La flag: 162.252.172.54

FLAG-2 Hash SHA-256 del archivo malicioso

Task 2

What is the SHA256 hash of the malware?

SHA256 hash

Submit

Para identificar el hash 256 del malware me puse a observar las transferencia de dato de la ip atacante simplemente con el comando

ip.addr == 162.252.172.54

capture.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 162.252.172.54

No.	Time	Source	Destination	Protocol	Length	Info
113	41.558121	172.16.1.191	162.252.172.54	TCP	66	51221 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
267	42.417642	162.252.172.54	172.16.1.191	TCP	86	80 → 51221 [PSH, ACK] Seq=152705 Ack=173 Win=64240 Len=32 [TCP segment of a reassembled PDU]
377	42.521537	162.252.172.54	172.16.1.191	TCP	86	80 → 51221 [PSH, ACK] Seq=276545 Ack=173 Win=64240 Len=32 [TCP segment of a reassembled PDU]
1232	42.521537	162.252.172.54	172.16.1.191	HTTP	153	GET / HTTP/1.1
395	42.521773	162.252.172.54	172.16.1.191	TCP	170	80 → 51221 [PSH, ACK] Seq=298477 Ack=173 Win=64240 Len=116 [TCP segment of a reassembled PDU]
459	42.559414	162.252.172.54	172.16.1.191	TCP	214	80 → 51221 [PSH, ACK] Seq=369895 Ack=173 Win=64240 Len=160 [TCP segment of a reassembled PDU]
116	41.895371	172.16.1.191	162.252.172.54	HTTP	226	667 / 667548/667551 HTTP/1.1
419	42.522212	162.252.172.54	172.16.1.191	TCP	110	100 → 51221 [PSH, ACK] Seq=327289 Ack=173 Win=64240 Len=356 [TCP segment of a reassembled PDU]
227	42.395479	162.252.172.54	172.16.1.191	TCP	590	80 → 51221 [PSH, ACK] Seq=109545 Ack=173 Win=64240 Len=536 [TCP segment of a reassembled PDU]
279	42.417828	162.252.172.54	172.16.1.191	TCP	590	80 → 51221 [PSH, ACK] Seq=167337 Ack=173 Win=64240 Len=536 [TCP segment of a reassembled PDU]
314	42.511489	162.252.172.54	172.16.1.191	TCP	842	80 → 51221 [PSH, ACK] Seq=201495 Ack=173 Win=64240 Len=788 [TCP segment of a reassembled PDU]
344	42.511978	162.252.172.54	172.16.1.191	TCP	842	80 → 51221 [PSH, ACK] Seq=238637 Ack=173 Win=64240 Len=788 [TCP segment of a reassembled PDU]
350	42.512069	162.252.172.54	172.16.1.191	TCP	1010	80 → 51221 [PSH, ACK] Seq=246725 Ack=173 Win=64240 Len=956 [TCP segment of a reassembled PDU]
402	42.521934	162.252.172.54	172.16.1.191	TCP	1010	80 → 51221 [PSH, ACK] Seq=305893 Ack=173 Win=64240 Len=956 [TCP segment of a reassembled PDU]

Frame 1238: 158 bytes on wire (1264 bits), 158 bytes captured (1264 bits) on interface 0
 Ethernet II, Src: Cisco7a:1d:39 (08:00:c7:a1:d3:39), Dst: HewlettP86:b7:a2 (00:0f:61:86:b7:a2)
 Internet Protocol Version 4, Src: 162.252.172.54, Dst: 172.16.1.191
 Transmission Control Protocol, Src Port: 80, Dst Port: 51221, Seq: 1288325, Ack: 173, Len: 104
 [926 Reassembled TCP Segments (1288428 bytes): #118(1376), #119(1376), #121(1376), #122(1376), #124(1376), #125(1460), #126(1292), #128(1376), #129(1460), #130(1292), #132(1460), #133(1292), #135(1460), #136(1460), #137(1460), #138(1124), #139(1460)]
 Hypertext Transfer Protocol
 Media Type

```

0000 00 0f 61 86 b7 a2 08 cc a7 7a 1d 39 08 00 45 00  - a-----z 9:E
0010 00 00 41 13 00 00 08 08 fc 52 a2 fc ac 36 ac 18  - A-----R-6-
0020 01 bf 00 50 c8 15 27 86 c8 58 0d de ae 44 50 18  - p.-.-X--dp-
0030 fa f9 43 08 00 00 00 00 00 00 00 00 00 00 00  - C-----
0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  - .....
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  - .....
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  - .....
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  - .....
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  - .....
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  - .....

```

Esta transferencia de imagen exitosa de parte de la ip atacante comprueba un claro indicador del delivery del malware por lo que extraje esta imagen con el fin de comprobar el hash

capture.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 162.252.172.54

No.	Time	Source	Destination	Protocol	Length	Info
113	41.558121	172.16.1.191	162.252.172.54	TCP	66	51221 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
267	42.417642	162.252.172.54	172.16.1.191	TCP	86	80 → 51221 [PSH, ACK] Seq=152705 Ack=173 Win=64240 Len=32 [TCP segment of a reassembled PDU]
377	42.521537	162.252.172.54	172.16.1.191	TCP	86	80 → 51221 [PSH, ACK] Seq=276545 Ack=173 Win=64240 Len=32 [TCP segment of a reassembled PDU]
1232	42.521537	162.252.172.54	172.16.1.191	HTTP	153	GET / HTTP/1.1
395	42.521773	162.252.172.54	172.16.1.191	TCP	170	80 → 51221 [PSH, ACK] Seq=298477 Ack=173 Win=64240 Len=116 [TCP segment of a reassembled PDU]
459	42.559414	162.252.172.54	172.16.1.191	TCP	214	80 → 51221 [PSH, ACK] Seq=369895 Ack=173 Win=64240 Len=160 [TCP segment of a reassembled PDU]
116	41.895371	172.16.1.191	162.252.172.54	HTTP	226	667 / 667548/667551 HTTP/1.1
419	42.522212	162.252.172.54	172.16.1.191	TCP	110	100 → 51221 [PSH, ACK] Seq=327289 Ack=173 Win=64240 Len=356 [TCP segment of a reassembled PDU]
227	42.395479	162.252.172.54	172.16.1.191	TCP	590	80 → 51221 [PSH, ACK] Seq=109545 Ack=173 Win=64240 Len=536 [TCP segment of a reassembled PDU]
279	42.417828	162.252.172.54	172.16.1.191	TCP	590	80 → 51221 [PSH, ACK] Seq=167337 Ack=173 Win=64240 Len=536 [TCP segment of a reassembled PDU]
314	42.511489	162.252.172.54	172.16.1.191	TCP	842	80 → 51221 [PSH, ACK] Seq=201495 Ack=173 Win=64240 Len=788 [TCP segment of a reassembled PDU]
344	42.511978	162.252.172.54	172.16.1.191	TCP	842	80 → 51221 [PSH, ACK] Seq=238637 Ack=173 Win=64240 Len=788 [TCP segment of a reassembled PDU]
350	42.512069	162.252.172.54	172.16.1.191	TCP	1010	80 → 51221 [PSH, ACK] Seq=246725 Ack=173 Win=64240 Len=956 [TCP segment of a reassembled PDU]
402	42.521934	162.252.172.54	172.16.1.191	TCP	1010	80 → 51221 [PSH, ACK] Seq=305893 Ack=173 Win=64240 Len=956 [TCP segment of a reassembled PDU]

Frame 1238: 158 bytes on wire (1264 bits), 158 bytes captured (1264 bits) on interface 0
 Ethernet II, Src: Cisco7a:1d:39 (08:00:c7:a1:d3:39), Dst: HewlettP86:b7:a2 (00:0f:61:86:b7:a2)
 Internet Protocol Version 4, Src: 162.252.172.54, Dst: 172.16.1.191
 Transmission Control Protocol, Src Port: 80, Dst Port: 51221, Seq: 1288325, Ack: 173, Len: 104
 [926 Reassembled TCP Segments (1288428 bytes): #118(1376), #119(1376), #121(1376), #122(1376), #124(1376), #125(1460), #126(1292), #128(1376), #129(1460), #130(1292), #132(1460), #133(1292), #135(1460), #136(1460), #137(1460), #138(1124), #139(1460)]
 Hypertext Transfer Protocol
 Media Type

Wireshark - Export - HTTP object list

Packet	Filename	Content Type	Size	Filename
1232	162.252.172.54	image/jpeg	1328 kb	667548.jpg
24044			230 bytes	
24056	crt.sectigo.com	application/pkix-cert	1559 bytes	SectigoRSADomainValidationSecureServerCA.c
24233			562 bytes	
24427			710 bytes	
24580			544 bytes	
24593			515 bytes	
24781			515 bytes	
24938			544 bytes	
24984			515 bytes	
24992			1460 bytes	
24995			457 bytes	
25007			711 bytes	
25322			1460 bytes	
25328			1340 bytes	
25329			1376 bytes	
25334			1389 bytes	
25344			1292 bytes	
25347			1375 bytes	
25350			1194 bytes	
25351			1460 bytes	
25357			1376 bytes	
25363			730 bytes	

Frame (158 bytes) Reassembled TCP (1288428 bytes)
 capture.pcap
 Packets: 39106 - Displayed: 1130 (2.9%)
 Profile: Default

Luego procedí hacer la comprobación de hash con el comando

Sha256sum 6ctf5jl

```
/bin/bash
/bin/bash 211x43

11:07:26 csi@csi ~/Desktop/temp_extract_dir
> sha256sum 6ctf5JL
9b8ffdc8ba2b2caa485cca56a82b2dcbd251f65fb30bc88f0ac3da6704e4d3c6 6ctf5JL

11:07:34 csi@csi ~/Desktop/temp_extract_dir
>
```

Procedi a llevar el hash a virus total a ver la reputación de este hash que presuntamente es del programa maligno

The screenshot shows the VirusTotal analysis page for the SHA256 hash `9b8ffdc8ba2b2caa485cca56a82b2dcbd251f65fb30bc88f0ac3da6704e4d3c6`. The page displays a community score of 59/72, indicating that 59 out of 72 security vendors have flagged the file as malicious. The file is identified as a DLL (Dynamic Link Library) and is 1.23 MB in size. The last analysis date was 8 days ago. The page also shows various threat categories and family labels, including `trojan.pikabot/mikey`, `trojan`, `pikabot`, `mikey`, and `qakbot`. The security vendors' analysis table lists several vendors that have flagged the file as malicious, including AhnLab-V3, AliCloud, Antiy-AVL, Arctic, Alibaba, ALYac, Arcabit, and Avast.

Security vendors' analysis	Do you want to automate checks?
AhnLab-V3	Trojan/Win.Qakbot.R579273
AliCloud	Trojan/Win/PikaBot.LH8PHU
Antiy-AVL	Trojan/Win32.Kryptik
Arctic	CSI Write Blocker
Alibaba	Trojan/Win32/Zenpak.42993aea
ALYac	Trojan.Agent.Pikabot
Arcabit	Trojan.Mikey.D23EB2
Avast	Win32:MalwareX-gen [Trj]

Asi encontrando la 2 flag:

9b8ffdc8ba2b2caa485cca56a82b2dcbd251f65fb30bc88f0ac3da6704e4d3c6

Task 2

What is the SHA256 hash of the malware?

`9b8ffdc8ba2b2caa485cca56a82b2dcbd251f65fb30bc88f0ac3da6704e4d3c6` ✓

La Flag-3 Identificación de la familia del malware

Task 3

What is the Family label of the malware?

p*****

Submit

Basándome en el análisis del hash proporcionado por Virus Total, pude identificar que el malware pertenece a la familia

9b8ffdc8ba2b2caa485cca56a82b2dcbd251f65fb30bc88f0ac3da6704e4d3c6

59 / 72
Community Score

59/72 security vendors flagged this file as malicious

Reanalyze Similar More

9b8ffdc8ba2b2caa485cca56a82b2dcbd251f65fb30bc88f0ac3da6704e4d3c6
6c7f5.jl

Size 1.23 MB Last Analysis Date 8 days ago

peddl detect-debug-environment checks-user-input overlay persistence spreader

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 12

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

Popular threat label trojan.pikabot/mikey Threat categories trojan pua Family labels pikabot mikey qakbot

Security vendors' analysis

AhnLab-V3	Trojan.Win.Qakbot.R579273	Alibaba	Trojan.Win32/Zenpak.42993aea
Alibaba	Trojan.Win/PikaBot.LH8PHU	ALYac	Trojan.Agent.Pikabot
Antiy-AVL	Trojan.Win32.Kryptik	Arcabit	Trojan.Mikey.D23EB2
Arctic Wolf	Unsafe	Avast	Win32:MalwareX-gen [Trj]

Do you want to automate checks?

La FLAG: pikabot

Task 3

What is the Family label of the malware?

Pikabot

Submit

La flag-4 Fecha de primera detección pública del malware

Task 4

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

YYYY-MM-DD HH:MM:SS

Submit

De igual manera nos vamos al apartado de detalles en virus total y encontramos la primera vez que se publicó el malware

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	2025-05-09 22:38:55 UTC
Last Analysis	2025-05-01 11:49:53 UTC

La flag: **2023-05-19 14:01:21**

Task 4

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

2023-05-19 14:01:21

✓

Flag-5 Puertos utilizados por el atacante

Task 5

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

Port1, Port2, Port3

Submit

Para encontrar los puertos del trafico aplique el filtro `tls || ssl`

Asi encontrando los puertos de transferencia de control utilizada por el host

No.	Time	Source	Destination	Protocol	Length	Info
31307	6389.460885	94.199.173.6	172.16.1.191	TLSv1.2	704	Certificate, Server Key Exchange, Server Hello Done
31306	6389.460672	94.199.173.6	172.16.1.191	TLSv1.2	1514	Server Hello
28476	6389.848278	132.148.79.222	172.16.1.191	TLSv1.2	85	Encrypted Alert
27676	6114.965580	132.148.79.222	172.16.1.191	TLSv1.2	388	Application Data
27662	6114.189137	132.148.79.222	172.16.1.191	TLSv1.2	296	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
27656	6114.616717	132.148.79.222	172.16.1.191	TLSv1.2	828	Certificate, Server Key Exchange, Server Hello Done
27654	6114.616543	132.148.79.222	172.16.1.191	TLSv1.2	1430	Server Hello
26168	5934.694370	45.85.235.39	172.16.1.191	TLSv1.2	85	Encrypted Alert
24760	5859.679544	45.85.235.39	172.16.1.191	TLSv1.2	388	Application Data
24750	5859.139296	45.85.235.39	172.16.1.191	TLSv1.2	296	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
24742	5858.948832	45.85.235.39	172.16.1.191	TLSv1.2	754	Certificate, Server Key Exchange, Server Hello Done
24741	5858.948817	45.85.235.39	172.16.1.191	TLSv1.2	1514	Server Hello
22788	5679.406127	129.213.54.49	172.16.1.191	TLSv1.2	85	Encrypted Alert
21883	5664.487615	129.213.54.49	172.16.1.191	TLSv1.2	388	Application Data

Transmission Control Protocol, Src Port: 2222, Dst Port: 32999, Seq: 1461, Ack: 324, Len: 748

TLSv1.2 Record Layer: Handshake Protocol: Certificate

Content Type: Handshake (22)

Version: TLS 1.2 (0x0303)

Encontrando 3 puerto en total son **2078, 2222, 32999**

Task 5

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

2078, 2222, 32999

✓

Flag-7 Campo inusual en el certificado TLS

Task 7

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

YYYY-MM-DD HH:MM:SS

Submit

Para encontrar esta seguí aplicando el filtro tls y entre al primer paquete que contiene información sobre certificado así encontrando la flag

capture.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tls

No.	Time	Source	Destination	Protocol	Length	Info
1249	231.379068	45.85.235.39	172.16.1.191	TLSv1.2	558	Certificate, Server Key Exchange, Server Hello Done
1252	231.399719	172.16.1.191	45.85.235.39	TLSv1.2	147	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
1254	231.577723	45.85.235.39	172.16.1.191	TLSv1.2	296	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
1256	231.580440	172.16.1.191	45.85.235.39	TLSv1.2	554	Application Data
1273	231.580602	172.16.1.191	45.85.235.39	TLSv1.2	1514	Application Data [TCP segment of a reassembled PDU]
1274	231.580605	172.16.1.191	45.85.235.39	TLSv1.2	515	Application Data
1288	232.137226	45.85.235.39	172.16.1.191	TLSv1.2	914	Application Data
1291	232.481471	172.16.1.191	132.148.79.222	TLSv1.2	285	Client Hello
1293	232.661069	132.148.79.222	172.16.1.191	TLSv1.2	1514	Server Hello
1294	232.661089	132.148.79.222	172.16.1.191	TLSv1.2	736	Certificate, Server Key Exchange, Server Hello Done
1296	232.662762	172.16.1.191	132.148.79.222	TLSv1.2	147	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
1298	232.736701	132.148.79.222	172.16.1.191	TLSv1.2	296	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
1300	232.737373	172.16.1.191	132.148.79.222	TLSv1.2	718	Application Data
1307	233.474872	132.148.79.222	172.16.1.191	TLSv1.2	254	Application Data

Certificate Length: 1508

Certificate: 3882686d588203c5a09302910202145651c79bfe6a17bc97bcb437c0f3ec25f7f6ec530. (id-at-commonName=votation.bzh,id-at-localityName=Pyopneumopericardium,id-at-organizationalUnitName=UndeLightful,id-at-organizationName=Unear..)

signedCertificate

version: v3 (3)

serialNumber: 0x5651c79bfe6a17bc97bcb437c0f3ec25f7f6ec5

signature (sha256WithRSAEncryption)

issuer: rdnSequence (9)

rdnSequence: 6 items (id-at-commonName=votation.bzh,id-at-localityName=Pyopneumopericardium,id-at-organizationalUnitName=UndeLightful,id-at-organizationName=Unear.. Inc.,id-at-stateOrProvinceName=KI,id-at-countryName=SX)

rdnSequence item: 1 item (id-at-stateOrProvinceName=KI)

rdnSequence item: 1 item (id-at-organizationName=Unear.. Inc.)

rdnSequence item: 1 item (id-at-organizationalUnitName=UndeLightful)

rdnSequence item: 1 item (id-at-localityName=Pyopneumopericardium)

rdnSequence item: 1 item (id-at-commonName=votation.bzh)

validity

notBefore: 2023-05-14 08:36:52 UTC

notAfter: 2023-05-14 08:36:52 UTC

subject: rdnSequence (9)

subjectPublicKeyInfo

extensions: 3 items

algorithmIdentifier (sha256WithRSAEncryption)

padding: 0

encrypted: b17d152831681028ad4e95c6ebd236689de60b69e2809a6a7a9e36cb115fc82b28064e1f..

La flag: **Pyopneumopericardium**

Task 6

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

Pyopneumopericardium

✓

Flag-8 Hora UTC del certificado TLS

Task 7

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

YYYY-MM-DD HH:MM:SS

Submit

En el mismo paquete TLS que contenía el campo anterior, encontré también el timestamp UTC relacionado al certificado

RelativeDistinguishedName item (id-at-commonName=votation.bzh)

Id: 2.5.4.3 (id-at-commonName)

DirectoryString: uTF8String (4)

UTF8String: votation.bzh

validity

notBefore: 2023-05-14 08:36:52 (UTC)

notAfter: 2023-05-14 08:36:52 (UTC)

subject: rdnSequence (9)

subjectPublicKeyInfo

extensions: 3 items

algorithmIdentifier (sha256WithRSAEncryption)

padding: 0

encrypted: b17d152831681028ad4e95c6ebd236689de60b69e2809a6a7a9e36cb115fc82b28064e1f..

La flag: **2023-05-14 08:36:52**

Task 7

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

2023-05-14 08:36:52



FLAG-9 – Dominio identificado

Task 8

What was the domain used for tunneling?

domain name

Submit

Utilizando un filtro DNS en Wireshark, accedí a las peticiones realizadas desde el host comprometido. Esto reveló un dominio utilizado por el atacante

No.	Time	Source	Destination	Protocol	Length	Info
38857	6792.841253	172.16.1.16	172.16.1.191	DNS	177	Standard query response 0x8f6e TXT Inx.158b75a8b.26fa3eb6.dns.steasteel.net TXT
38858	6792.841734	172.16.1.191	172.16.1.16	DNS	106	Standard query 0xb3ab A hbpj.120.049e24b6.26fa3eb6.dns.steasteel.net
38859	6793.021555	172.16.1.16	172.16.1.191	DNS	158	Standard query response 0xb3ab A hbpj.120.049e24b6.26fa3eb6.dns.steasteel.net
38860	6793.021555	172.16.1.16	172.16.1.191	DNS	122	Standard query response 0xb3ab A hbpj.120.049e24b6.26fa3eb6.dns.steasteel.net
38861	6793.022275	172.16.1.191	172.16.1.16	DNS	160	Standard query 0xbc55 A hbpj.14b7a4fca84da0b04e5a65073c2724da8a43c0b1d0334b1da415a75.149e24b6.26fa3eb6.dns.steasteel.net
38862	6793.048183	172.16.1.191	172.16.1.16	DNS	160	Standard query 0xbc55 A hbpj.14b7a4fca84da0b04e5a65073c2724da8a43c0b1d0334b1da415a75.149e24b6.26fa3eb6.dns.steasteel.net
38863	6793.100005	172.16.1.16	172.16.1.191	DNS	176	Standard query response 0xbc55 A hbpj.14b7a4fca84da0b04e5a65073c2724da8a43c0b1d0334b1da415a75.149e24b6.26fa3eb6.dns.steasteel.net
38864	6793.100458	172.16.1.191	172.16.1.16	DNS	112	Standard query 0x903c A hbpj.115c17c22.249e24b6.26fa3eb6.dns.steasteel.net
38865	6793.219643	172.16.1.191	172.16.1.16	DNS	112	Standard query 0x903c A hbpj.115c17c22.249e24b6.26fa3eb6.dns.steasteel.net
38866	6793.339056	172.16.1.16	172.16.1.191	DNS	128	Standard query response 0x903c A hbpj.115c17c22.249e24b6.26fa3eb6.dns.steasteel.net
38868	6889.028125	172.16.1.191	172.16.1.16	DNS	71	Standard query 0x4688 A twitter.com
38869	6889.069792	172.16.1.191	172.16.1.16	DNS	71	Standard query 0x4688 A twitter.com
38870	6889.093373	172.16.1.16	172.16.1.191	DNS	87	Standard query response 0x4688 A twitter.com A 104.244.42.193

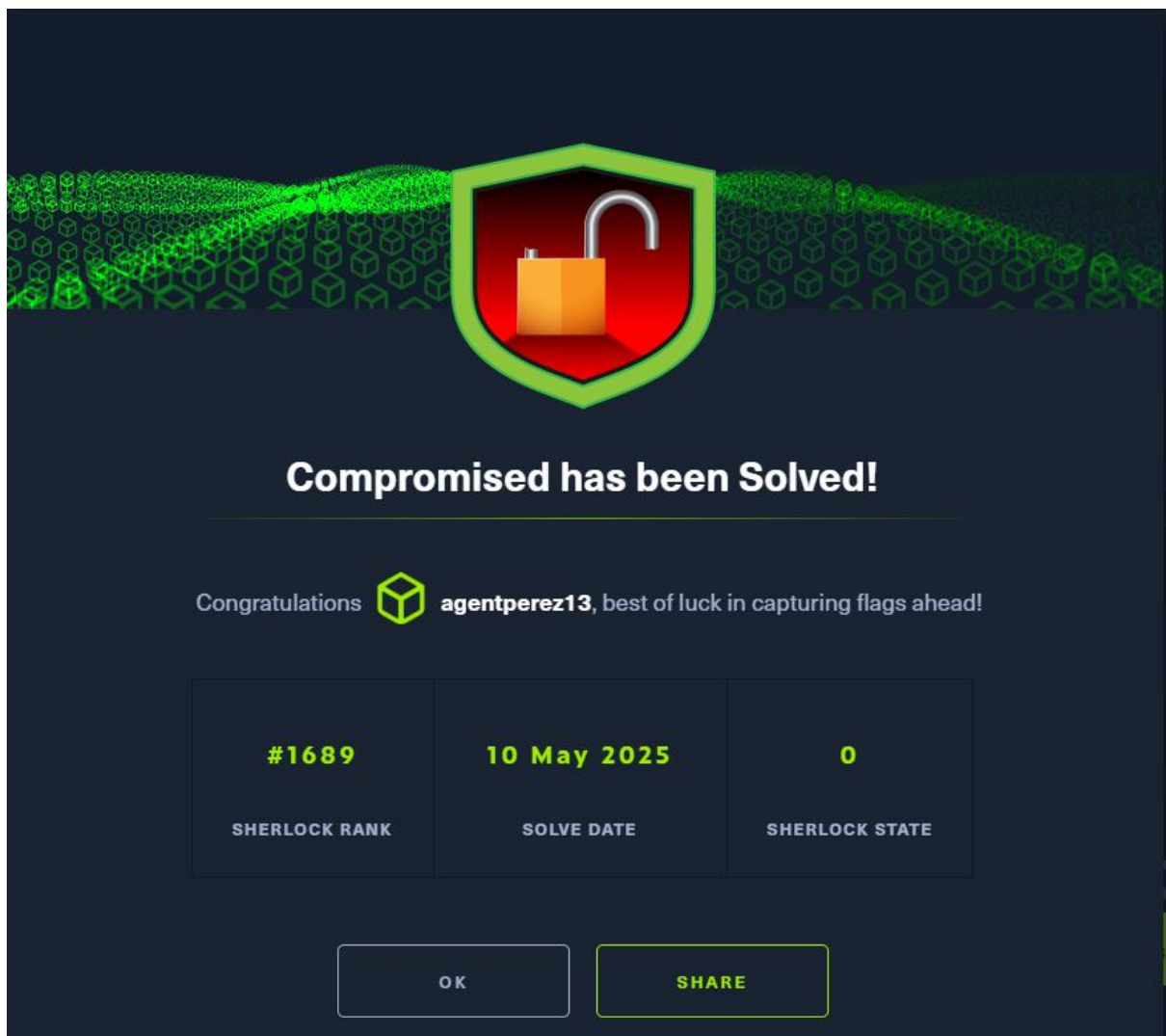
La flag: steasteel.net

Task 8

What was the domain used for tunneling?

steasteel.net





By Manuel Perez

NK Maloweer