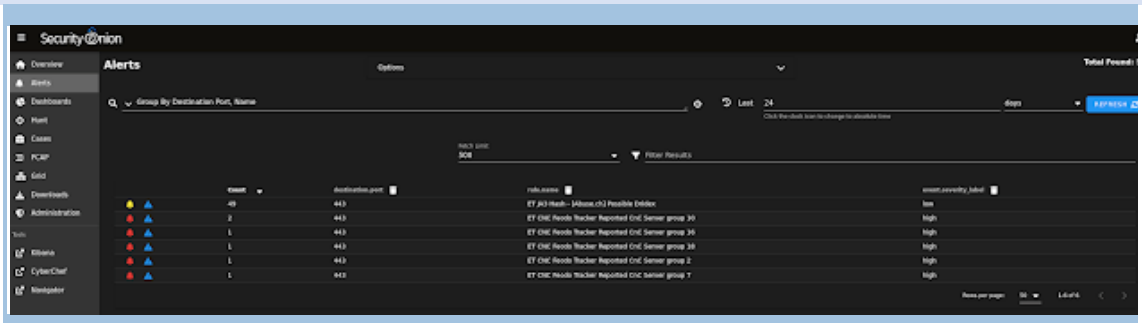
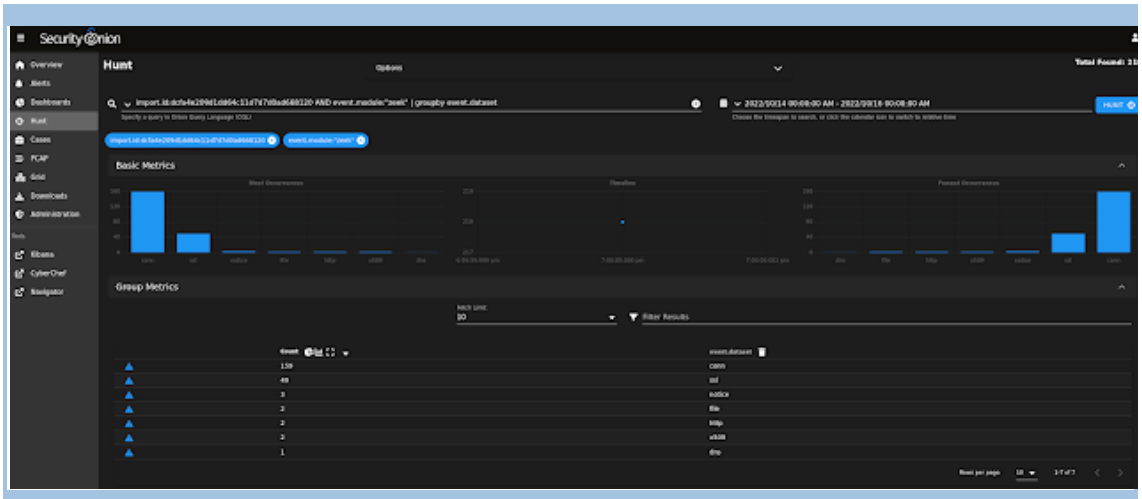
ANÁLISIS DE MALWARE: BB02 QAKBOT (QBOT) PCAP FROM 2022-10-14

Las siguientes capturas de pantalla muestran algunas de las interesantes alertas de Suricata, registros de Zeek y transcripciones de sesiones. Comenzamos con las alertas de Suricata y luego pasamos a los metadatos de Zeek. Por el camino, encontramos una descarga interesante a través de HTTP y utilizamos CyberChef para descifrarla y determinar la contraseña del archivo. Por último, examinamos todas las conexiones, incluidos el país de destino y el nombre de la organización.

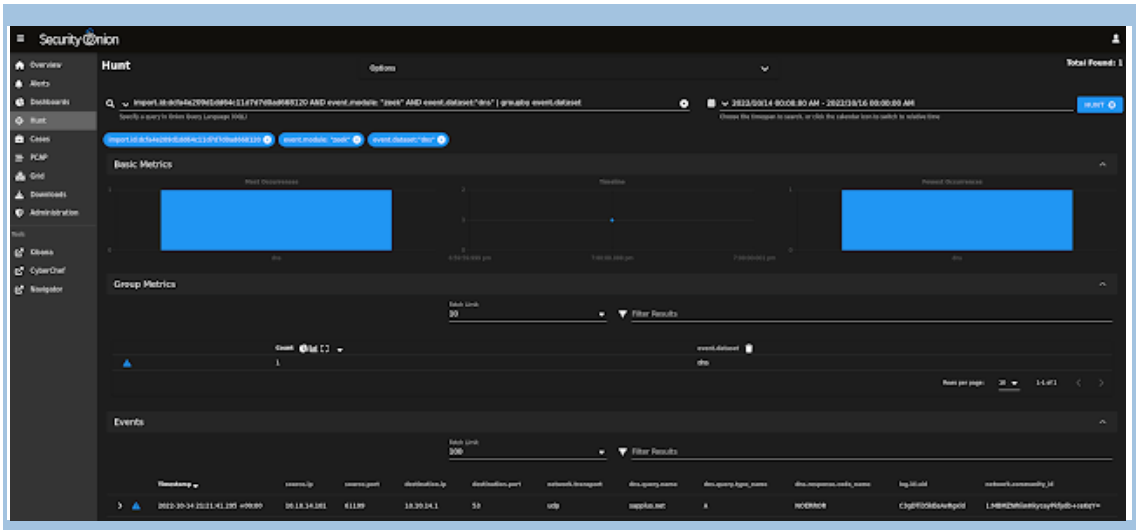
CAPTURAS DE PANTALLA



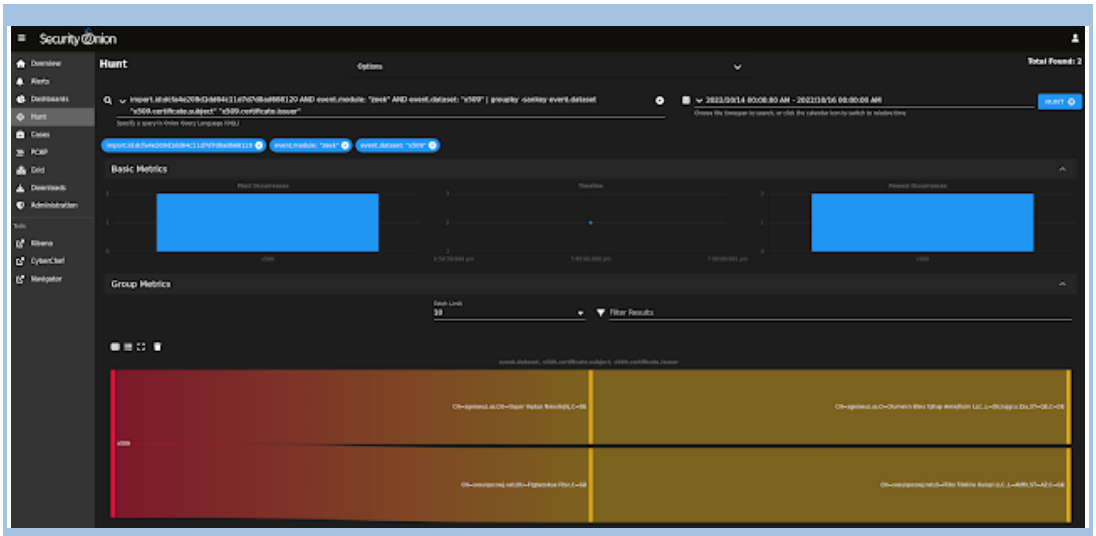
Alertas Suricata NIDS



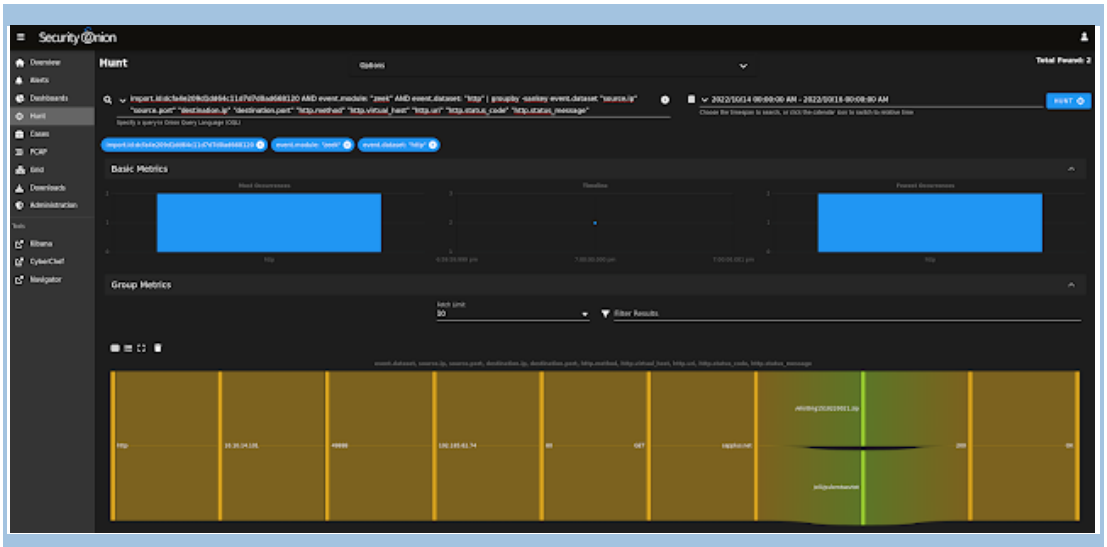
Metadatos de Zeek



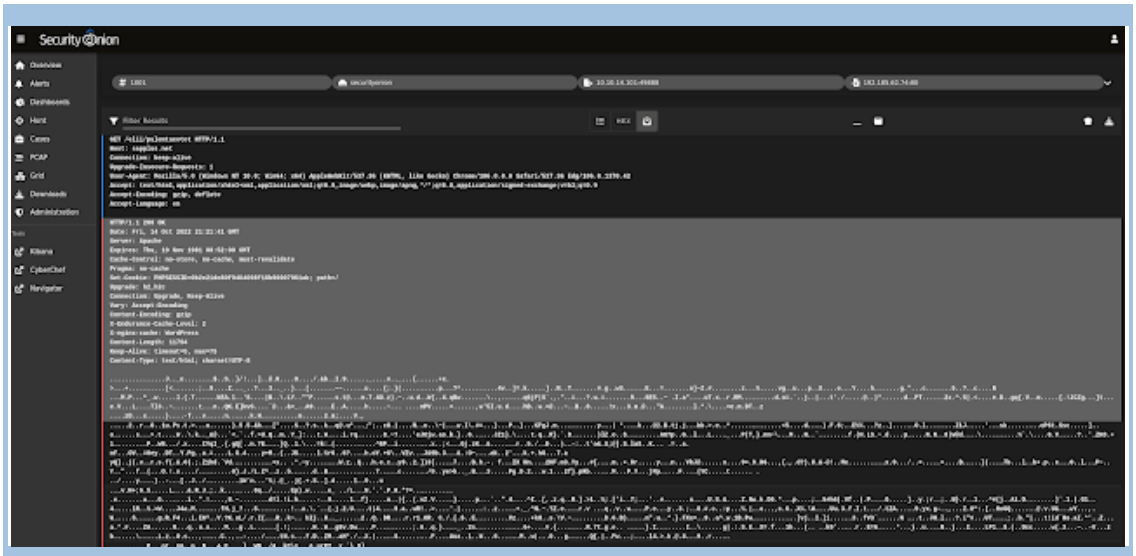
Búsqueda DNS



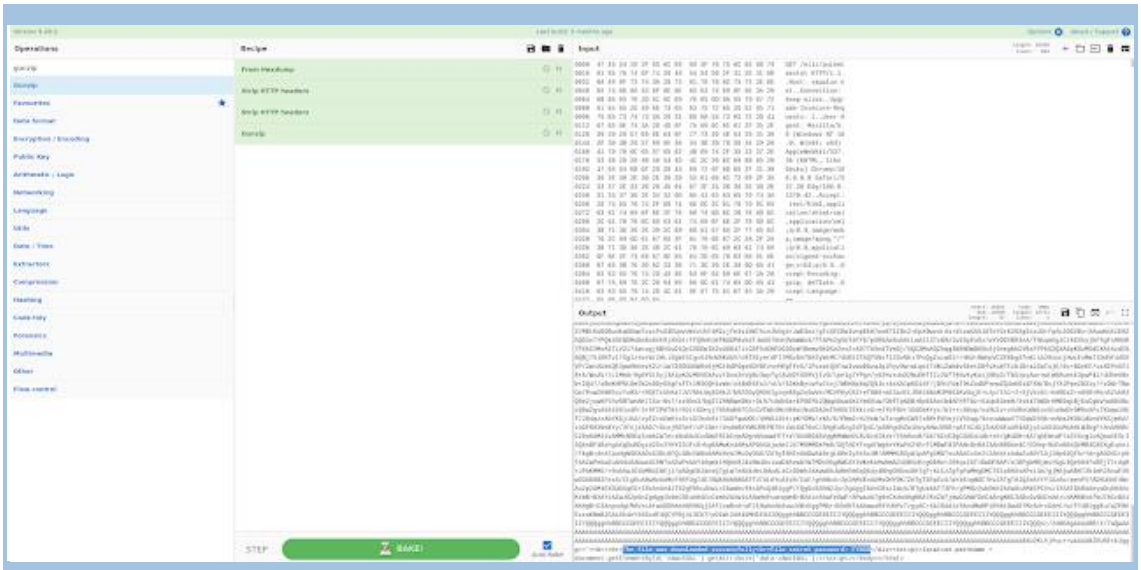
Certificados X509



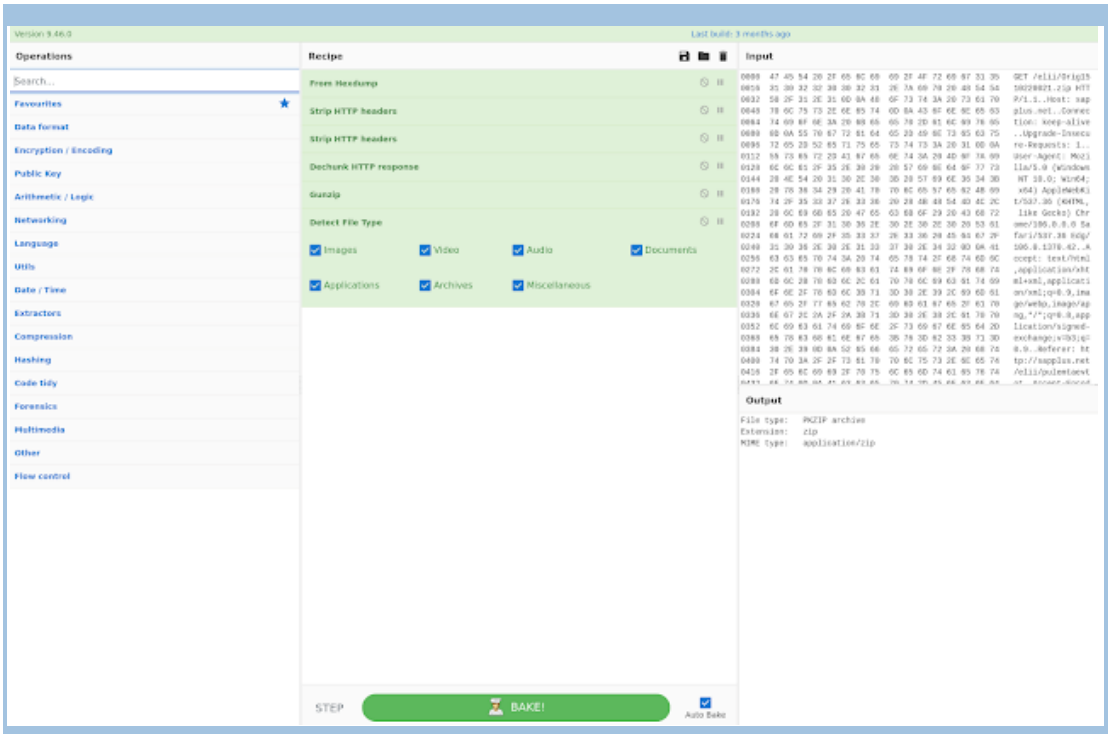
Transacciones HTTP



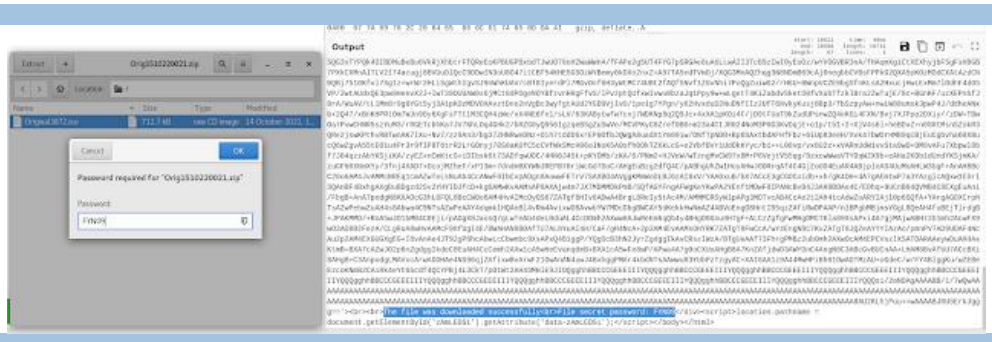
Transcripción ASCII de la transacción HTTP



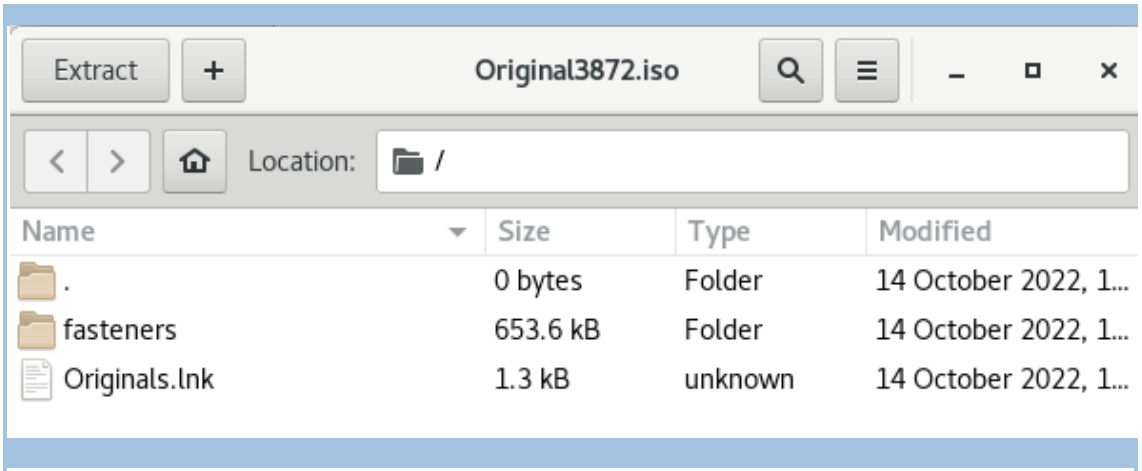
La primera transacción HTTP muestra la contraseña que utilizaremos para abrir el archivo descargado



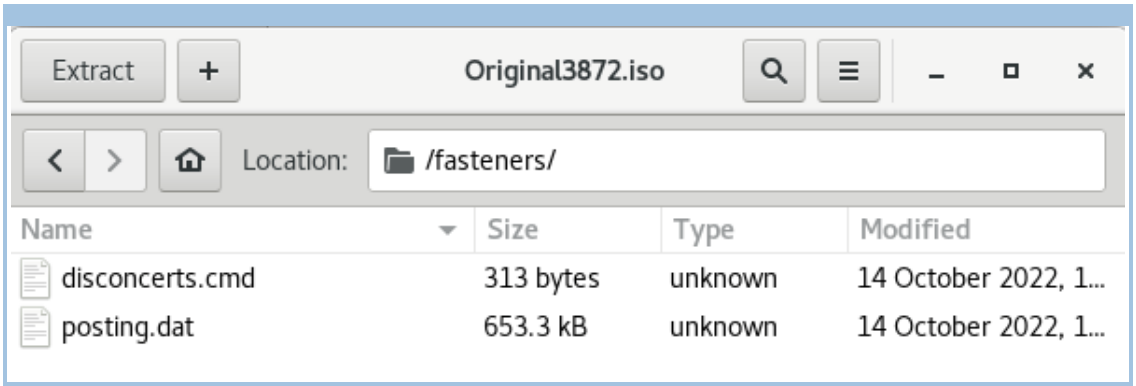
La segunda transacción HTTP es un archivo ZIP protegido por contraseña



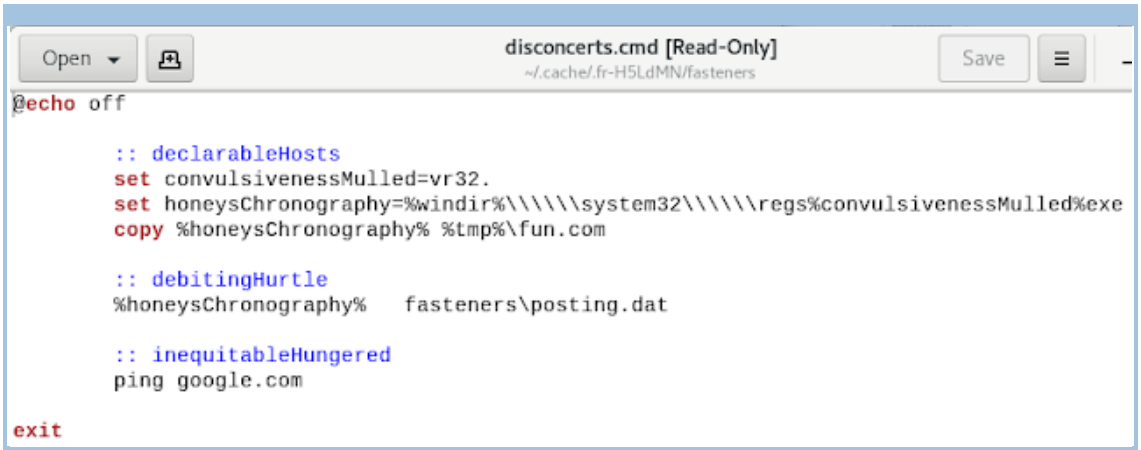
Abrir el archivo ZIP protegido con contraseña utilizando la contraseña descubierta anteriormente y extraer la imagen ISO incrustada.



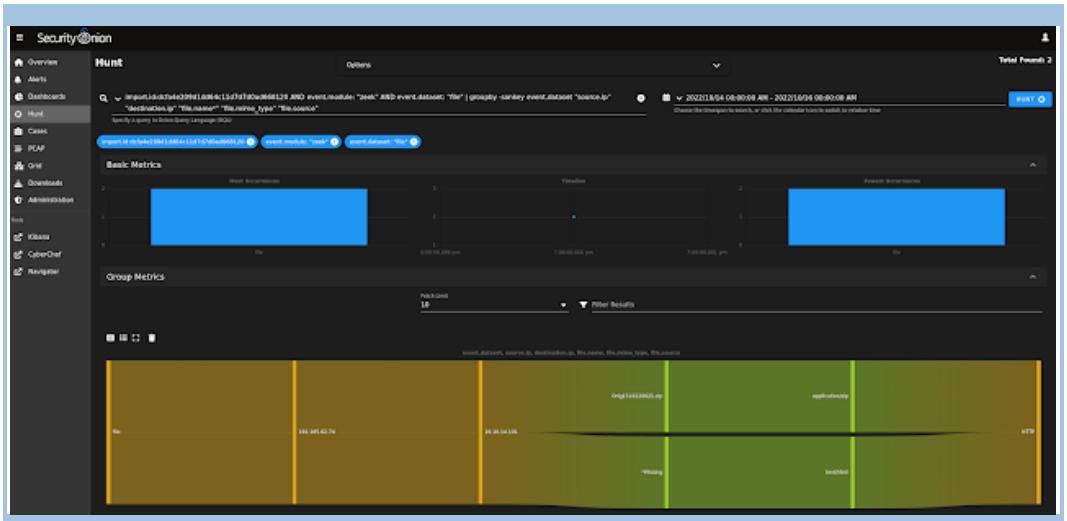
Abrir la imagen ISO



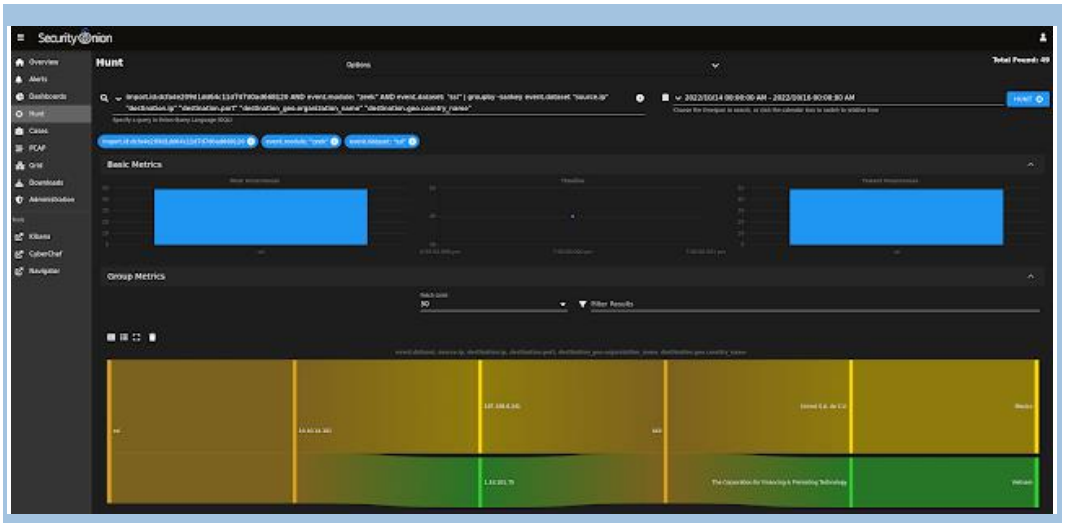
Archivos interesantes dentro de la imagen ISO



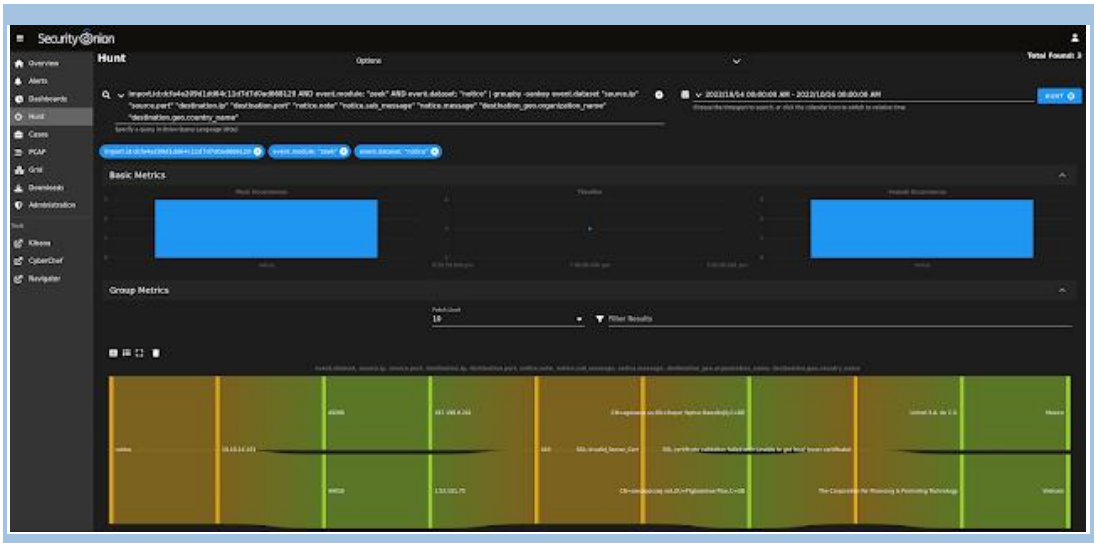
Script CMD desde imagen ISO



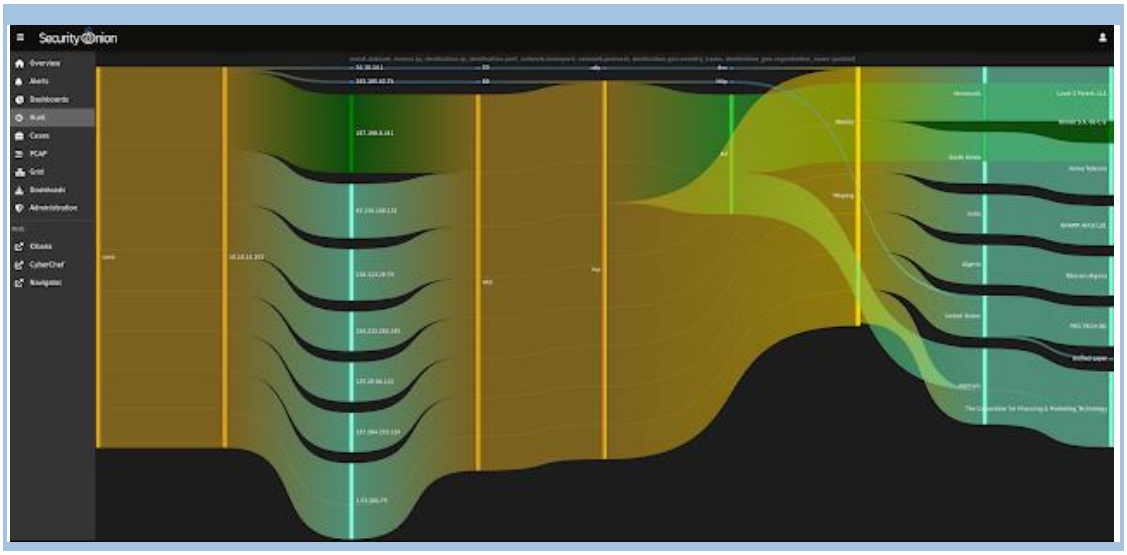
Registro de transferencias de archivos



Conexiones SSL



Zeek avisa de certificados SSL no válidos



Todas las conexiones, incluido el país de destino y el nombre de la organización

2022-10-14 (FRIDAY) BB02 QAKBOT (QBOT) INFECTION

CADENA DE INFECCIÓN:

- email --> link --> password-protected zip --> ISO --> Windows shortcut runs installer DLL --> Qakbot C2

ENLACE EN EL CORREO:

- hxxps://sapplus.net/elii/pulemtaevtot

ARCHIVOS DESDE EL ENLACE EN EL CORREO:

- SHA256 hash: 7dcc02a5947410627d94c50ed37a500335ccd9d7b30cd540e174457096a54a1e
- File size: 383,936 bytes
- File name: Orig1510220021.zip
- File location: https://sapplus.net/elii/Orig1510220021.zip
- File description: Password-protected zip archive downloaded through link in the email
- Password: FYN09
- SHA256 hash: f1b6767c8be1d9d0083dcc041469a5404e16ce96c60a62f76de7a88de873e0c5
- File size: 712,704 bytes
- File name: Original3872.iso
- File description: ISO image extracted from the above zip archive

CONTENIDO DE LA IMAGEN ISO:

- SHA256 hash: 200a604f819bcedd10258f4f58b30e1e36780a9e91c0686a1f08b4c144cc217d
- File size: 1,259 bytes
- File name: Originals.lnk
- File description: Windows shortcut (only visible file in the ISO image)
- SHA256 hash: 070272bda35f495343673b51cf871ae9e49b1aa0d3276aacc826b63768b8a860
- File size: 313 bytes
- File name: fasteners\disconcerts.cmd
- File description: .cmd batch script run by the above Windows shortcut
- SHA256 hash: bc672fe23b19898032b312ab849d781cfd450966e17f571b8e31a0328f2bafe8
- File size: 653,312 bytes
- File name: fasteners\posting.dat
- File description: Windows DLL file for Qakbot, distribution tag: bb02
- Run method: regsvr32.exe [filename]

TRAFIO DESDE UN HOST WINDOWS INFECTADO:

PÁGINA WEB PARA Y ENTREGA DE ARCHIVO ZIP PROTEGIDO CON CONTRASEÑA:

- 192.185.62.74 port 80 - sapplus.net - GET /elii/pulemtaevtot
- 192.185.62.74 port 80 - sapplus.net - GET /elii/Orig1510220021.zip
- Note: Link from the emails was https, but used http URL for this infection.

TRAFICO QAKBOT C2:

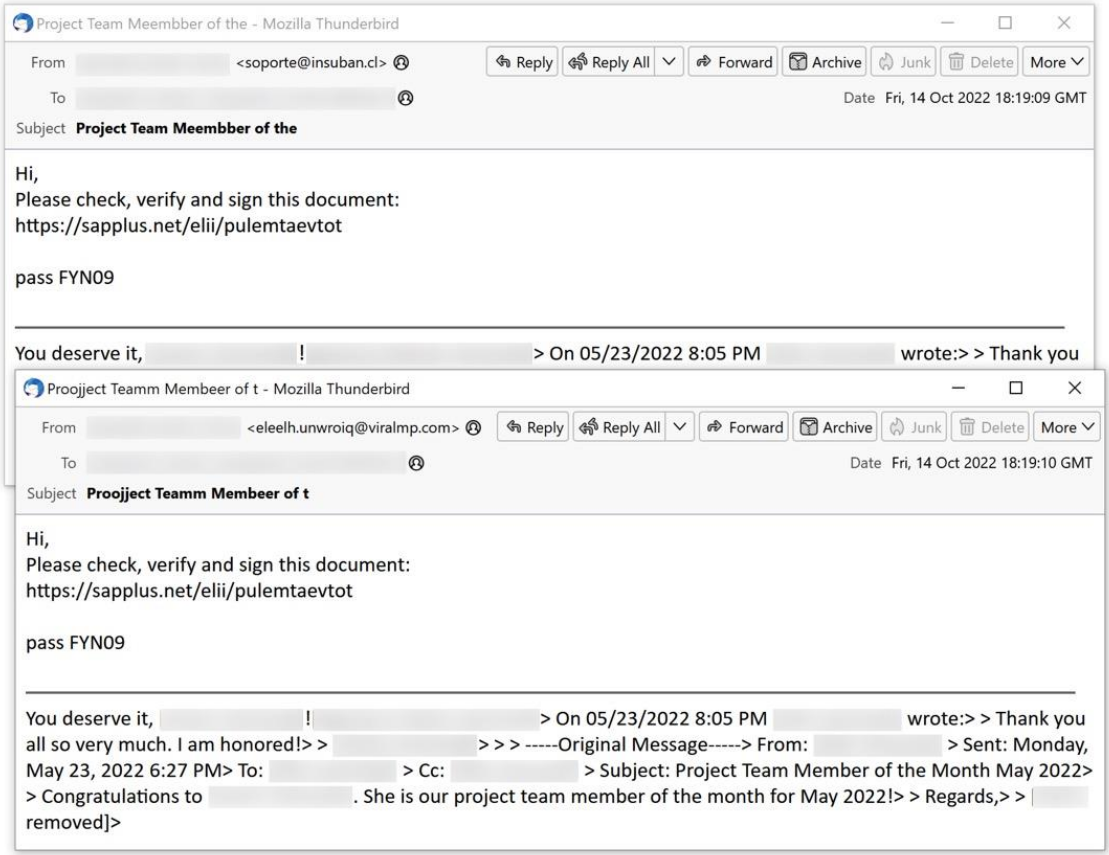
- 1.53.101.75 port 443 - HTTPS traffic (TLSv1.2)
- 125.20.84.122 port 443 - TCP connection attempts unsuccessful
- 220.123.29.76 port 443 - TCP connection attempts unsuccessful
- 197.204.233.216 port 443 - TCP connection attempts unsuccessful
- 45.230.169.132 port 443 - TCP connection attempts unsuccessful
- 104.233.202.195 port 443 - TCP connection attempts unsuccessful
- 187.198.8.241 port 443 - HTTPS traffic (TLSv1.2)

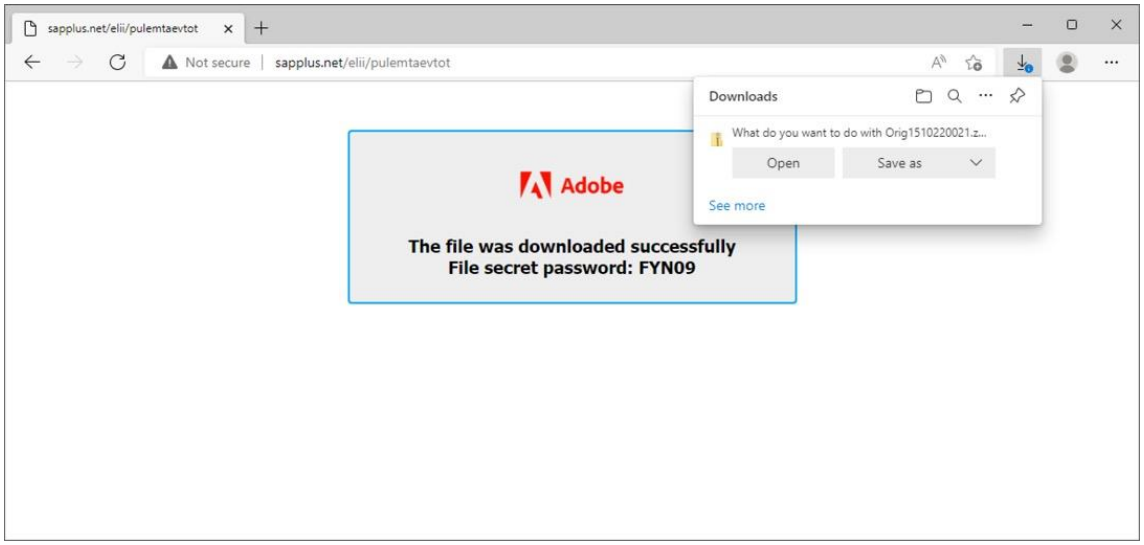
DATOS DEL EMISOR DEL CERTIFICADO PARA EL SERVIDOR QAKBOT C2 EN 1.53.101.75:

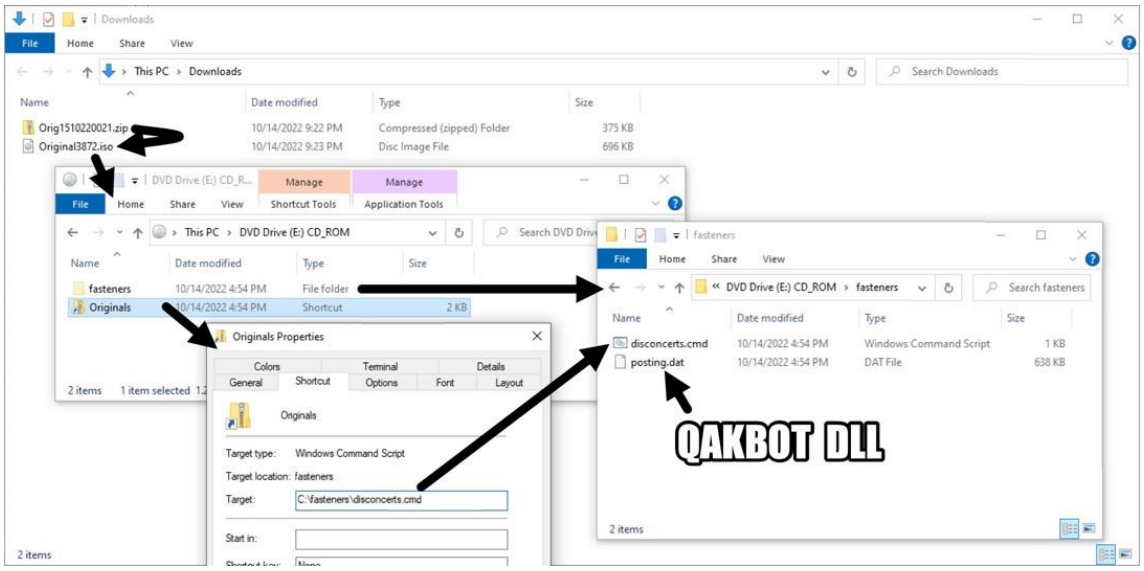
- id-at-countryName=GB
- id-at-stateOrProvinceName=AZ
- id-at-localityName=Akfth
- id-at-organizationName=Flibo Tdelirie Ouiopi LLC.
- id-at-commonName=sxeuiqecowj.net

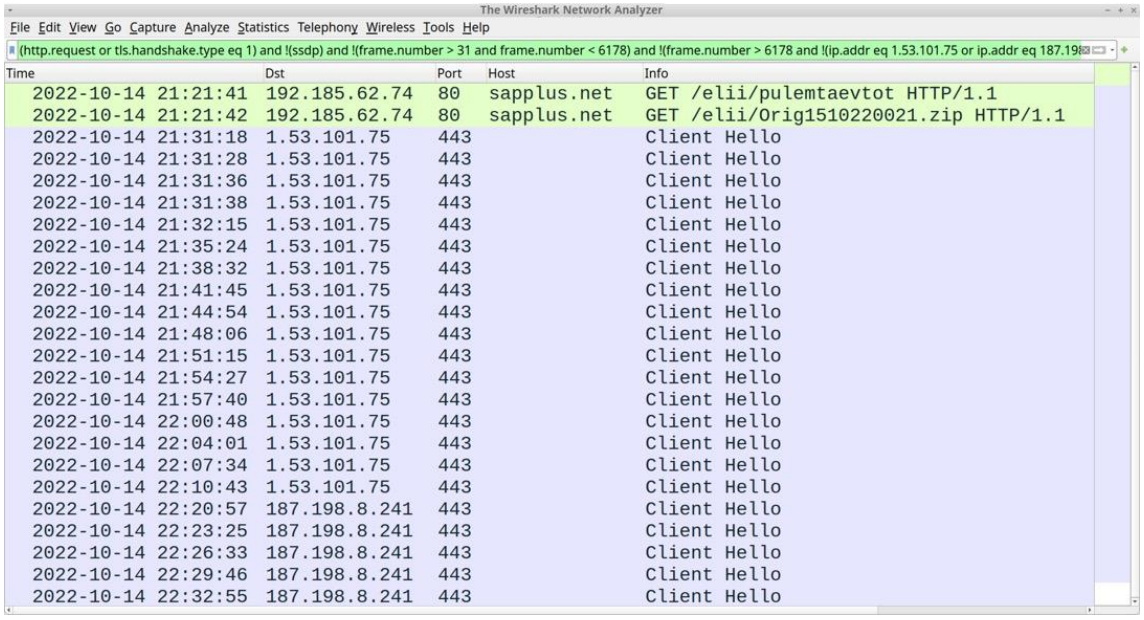
DATOS DEL EMISOR DEL CERTIFICADO PARA EL SERVIDOR QAKBOT C2 EN 187.198.8.241:

- id-at-countryName=DE
- id-at-stateOrProvinceName=QE
- id-at-localityName=Otcsvjgcu Zsu
- id-at-organizationName=Oiumeicn Bteu Yphap Aenejfcom LLC.
- id-at-commonName=sageiaeuz.us


Project Team Meembber of the - Mozilla Thunderbird
From <soporte@insuban.cl>
Reply
Reply All
Forward
Archive
Junk
Delete
More
To
Date Fri, 14 Oct 2022 18:19:09 GMT
Subject Project Team Meembber of the
Hi,
Please check, verify and sign this document:
https://sapplus.net/elii/pulemtaevtot
pass FYN09
You deserve it, ! > On 05/23/2022 8:05 PM wrote:> > Thank you
Proojject Teamm Membeer of t - Mozilla Thunderbird
From <eleelh.unwroiq@viralmp.com>
Reply
Reply All
Forward
Archive
Junk
Delete
More
To
Date Fri, 14 Oct 2022 18:19:10 GMT
Subject Proojject Teamm Membeer of t
Hi,
Please check, verify and sign this document:
https://sapplus.net/elii/pulemtaevtot
pass FYN09
You deserve it, ! > On 05/23/2022 8:05 PM wrote:> > Thank you all so very much. I am honored!> > > > > -----Original Message-----> From: > Sent: Monday, May 23, 2022 6:27 PM> To: > Cc: > Subject: Project Team Member of the Month May 2022> > Congratulations to . She is our project team member of the month for May 2022!> > Regards,> > removed]>


sapplus.net/elii/pulemtaevtot
Not secure | sapplus.net/elii/pulemtaevtot
Downloads
What do you want to do with Orig1510220021.z...
Open
Save as
See more
Adobe
The file was downloaded successfully
File secret password: FYN09


Downloads
File Home Share View
This PC › Downloads
Search Downloads
Name Date modified Type Size
Orig1510220021.zip 10/14/2022 9:22 PM Compressed (zipped) Folder 375 KB
Original3872.iso 10/14/2022 9:23 PM Disc Image File 696 KB
DVD Drive (E:) CD_R...
Manage Manage
File Home Share View Shortcut Tools Application Tools
This PC › DVD Drive (E:) CD_ROM
Search DVD Drive
Name Date modified Type Size
fasteners 10/14/2022 4:54 PM File folder
Originals 10/14/2022 4:54 PM Shortcut 2 KB
2 items 1 item selected
Originals Properties
Colors Terminal Details
General Shortcut Options Font Layout
Originals
Target type: Windows Command Script
Target location: fasteners
Target: C:\fasteners\disconcerts.cmd
Start in:
2 items
fasteners
File Home Share View
« DVD Drive (E:) CD_ROM › fasteners
Search fasteners
Name Date modified Type Size
disconcerts.cmd 10/14/2022 4:54 PM Windows Command Script 1 KB
posting.dat 10/14/2022 4:54 PM DAT File 638 KB
QAKBOT DLL
2 items


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
(http.request or tls.handshake.type eq 1) and !(ssdp) and !(frame.number > 31 and frame.number < 6178) and !(frame.number > 6178 and !(ip.addr eq 1.53.101.75 or ip.addr eq 187.19
Time Dst Port Host Info
2022-10-14 21:21:41 192.185.62.74 80 sapplus.net GET /elii/pulemtaevtot HTTP/1.1
2022-10-14 21:21:42 192.185.62.74 80 sapplus.net GET /elii/Orig1510220021.zip HTTP/1.1
2022-10-14 21:31:18 1.53.101.75 443 Client Hello
2022-10-14 21:31:28 1.53.101.75 443 Client Hello
2022-10-14 21:31:36 1.53.101.75 443 Client Hello
2022-10-14 21:31:38 1.53.101.75 443 Client Hello
2022-10-14 21:32:15 1.53.101.75 443 Client Hello
2022-10-14 21:35:24 1.53.101.75 443 Client Hello
2022-10-14 21:38:32 1.53.101.75 443 Client Hello
2022-10-14 21:41:45 1.53.101.75 443 Client Hello
2022-10-14 21:44:54 1.53.101.75 443 Client Hello
2022-10-14 21:48:06 1.53.101.75 443 Client Hello
2022-10-14 21:51:15 1.53.101.75 443 Client Hello
2022-10-14 21:54:27 1.53.101.75 443 Client Hello
2022-10-14 21:57:40 1.53.101.75 443 Client Hello
2022-10-14 22:00:48 1.53.101.75 443 Client Hello
2022-10-14 22:04:01 1.53.101.75 443 Client Hello
2022-10-14 22:07:34 1.53.101.75 443 Client Hello
2022-10-14 22:10:43 1.53.101.75 443 Client Hello
2022-10-14 22:20:57 187.198.8.241 443 Client Hello
2022-10-14 22:23:25 187.198.8.241 443 Client Hello
2022-10-14 22:26:33 187.198.8.241 443 Client Hello
2022-10-14 22:29:46 187.198.8.241 443 Client Hello
2022-10-14 22:32:55 187.198.8.241 443 Client Hello