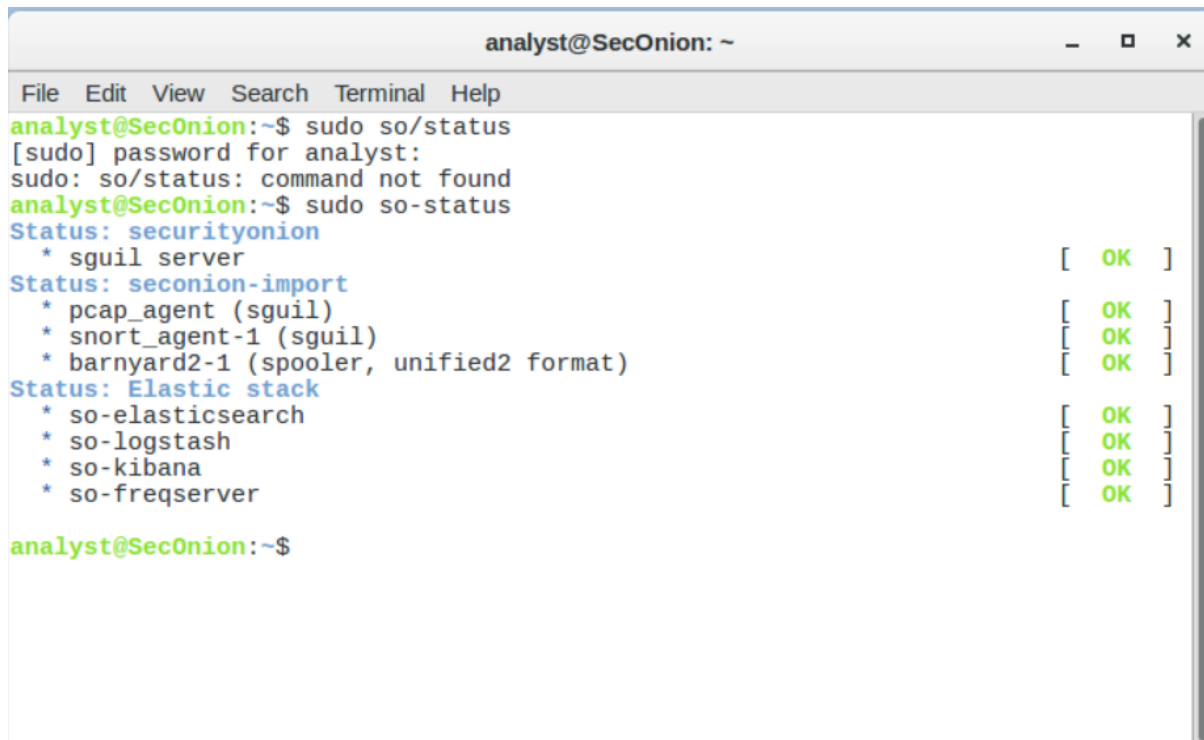


Lab – Interpret HTTP and DNS Data to Isolate Threat Actor

Indaghiamo su un attacco di iniezione SQL e tecniche di esfiltrazione DNS e utilizzeremo Security Onion.

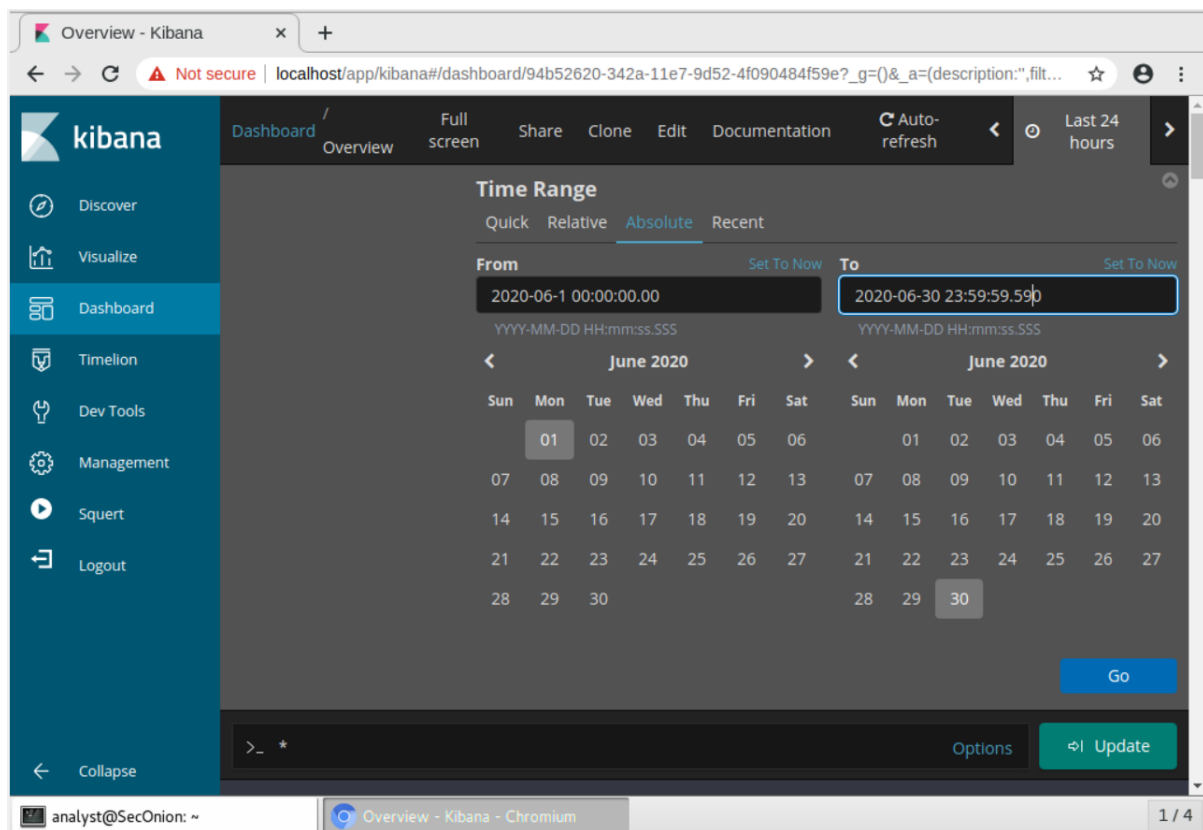
Per prima cosa avviamo la security Onion VM , con nome utente **Analyst** e password **cyberops**.

Apriamo il terminale inseriamo il comando **sudo so-status** per controllare lo status dei servizi.

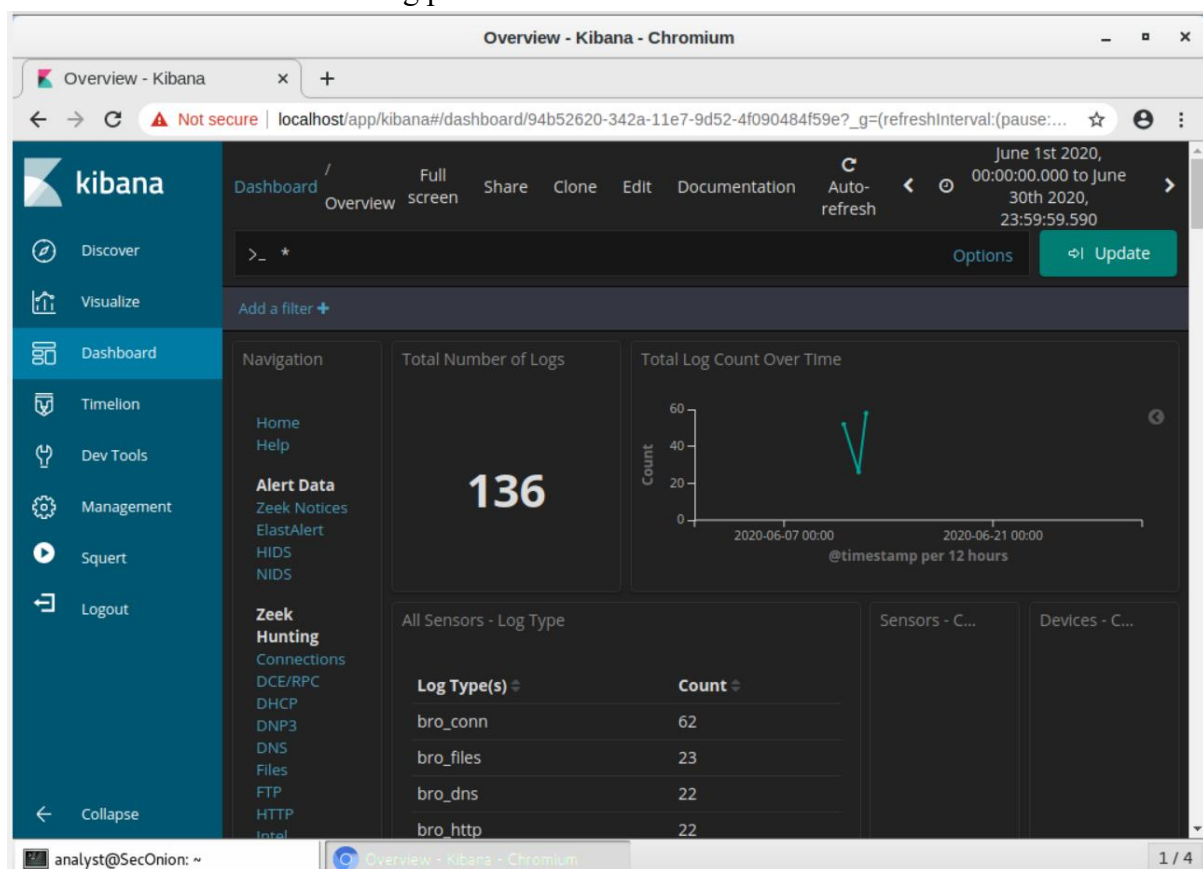


```
analyst@SecOnion: ~  
File Edit View Search Terminal Help  
analyst@SecOnion:~$ sudo so/status  
[sudo] password for analyst:  
sudo: so/status: command not found  
analyst@SecOnion:~$ sudo so-status  
Status: securityonion  
* sgul server [ OK ]  
Status: seconion-import  
* pcap_agent (sgul) [ OK ]  
* snort_agent-1 (sgul) [ OK ]  
* barnyard2-1 (spooler, unified2 format) [ OK ]  
Status: Elastic stack  
* so-elasticsearch [ OK ]  
* so-logstash [ OK ]  
* so-kibana [ OK ]  
* so-freqserver [ OK ]  
analyst@SecOnion:~$
```

Apriamo Kibana per il monitoraggio e l'analisi , con le stesse credenziali di accesso della VM e andiamo nel settaggio del time range e impostiamo la data inerente alla richiesta del compito (Giugno 2020).



Visualizziamo il numero dei log per l'intero mese



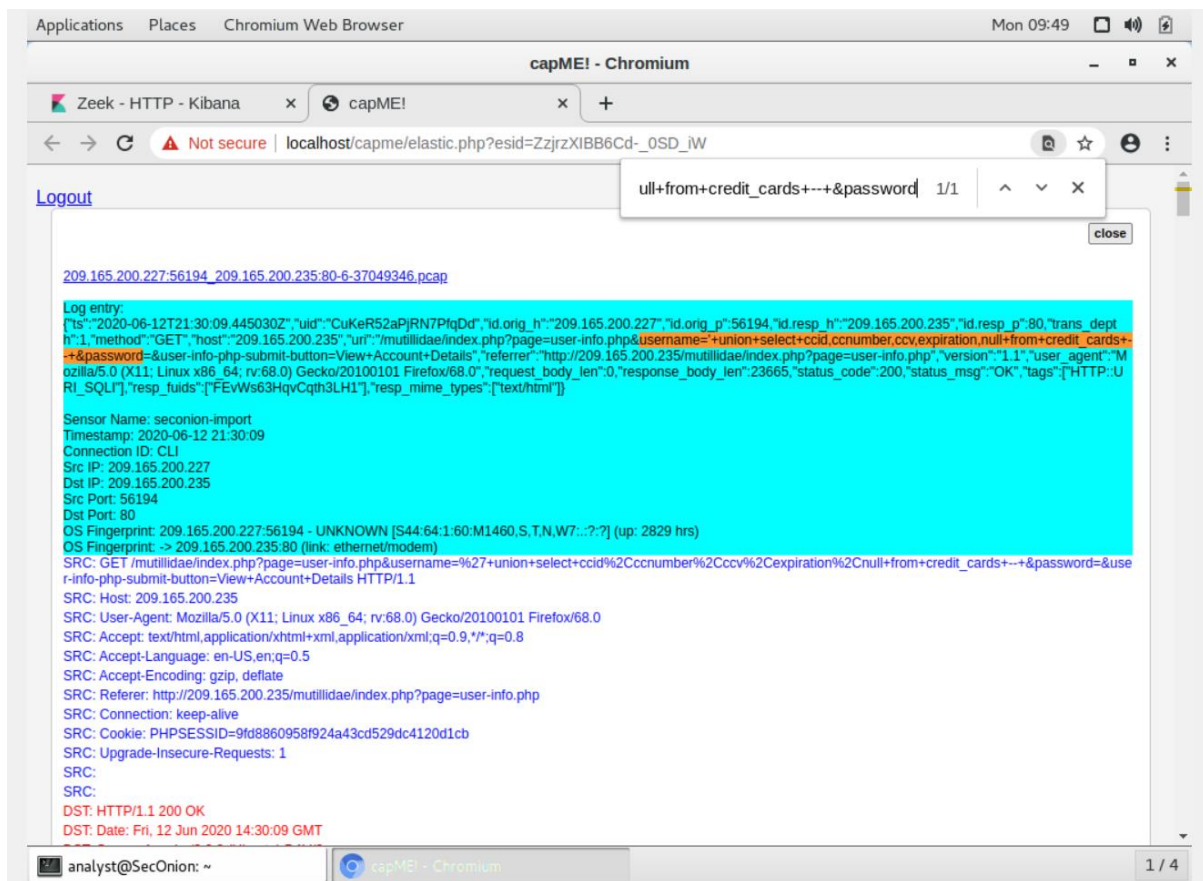
Filtriamo il traffico HTTP tramite l'intestazione di Zeek Hunting e vediamo che:

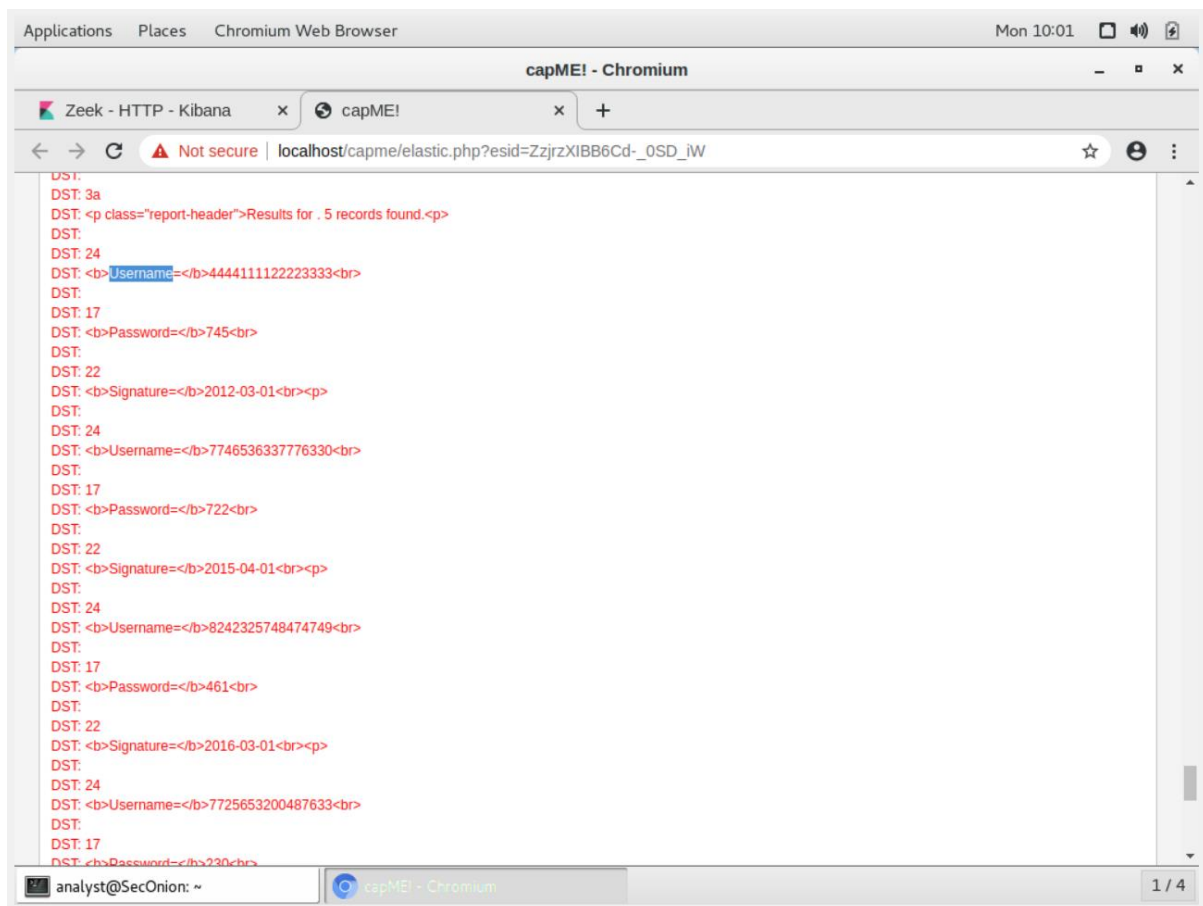
- L'indirizzo IP di origine è 209.165.200.227.
- L'indirizzo IP di destinazione è 209.165.200.235.
- La porta di destinazione è 80.
- La data e l'ora sono il 12 giugno 2020, 21:30:09.445.
- Il tipo di evento è bro_http.
- Il messaggio include nome utente, CCID, numero CC, CCV, scadenza e password.
- Si tratta di una richiesta di informazioni sulla carta di credito.

Nella sezione Log entry, che si trova all'inizio della trascrizione, si noti che la parte **username='+union+select+ccid,ccnumber,ccv,expiration,null+from+credit_cards+--+&password**

Cerca la parola chiave **username** nella trascrizione. Usa **Ctrl-F** per aprire una casella di ricerca.

Sembra che ci sia un elenco di nomi utente e password che fanno parte delle informazioni restituite in risposta alla richiesta HTTP GET. Ciò è insolito.





Alcuni tipi di username e password esfiltrati:

4444111122223333 745 2012-03-01
7746536337776330 722 2015-04-01
8242325748474749 461 2016-03-01
7725653200487633 230 2017-06-01

Filtriamo il traffico DNS e andiamo a vedere i principali tipi di query scorrendo ulteriormente la finestra puoi vedere un elenco delle principali query DNS per nome di dominio. Nota come alcune delle query abbiano sottodomini insolitamente lunghi associati a ns.example.com. Il dominio example.com dovrebbe essere esaminato ulteriormente

Applications Places Chromium Web Browser Mon 10:11

Zeek - DNS - Kibana - Chromium

Zeek - DNS - Kibana x +

Not secure | localhost/app/kibana#/dashboard/ebf5ec90-34bf-11e7-9b32-bb903919ead9?_g=(refreshInterval:(pause:!... to June 30th 2020, 23:59:59.590

kibana

Discover
Visualize
Dashboard
Timeline
Dev Tools
Management
Squert
Logout

Dashboard

DNS

>_ example.com Options Refresh

destination_port: "53" Add a filter + Actions

Navigation

- Home
- Help
- Alert Data**
 - Zeek Notices
 - ElastAlert
 - HIDS
 - NIDS
- Zeek Hunting**
 - Connections
 - DCE/RPC
 - DHCP
 - DNP3
 - DNS
 - Files
 - FTP
 - HTTP
 - Intel

DNS - Log Count

4

DNS - Log Count Over Time

Count

2020-06-07 00:00 2020-06-14 00:00 2020-06-21 00:00

@timestamp per 12 hours

DNS - Query Class (Pie Chart)

C_INTERNET

DNS - Destination Port (Horizontal Bar Chart)

53

analyst@SecOnion: ~ Zeek - DNS - Kibana - Chromium 1 / 4

Il client è 192.168.0.11 e il server è 209.165.200.235

Applications Places Chromium Web Browser Mon 10:11

Zeek - DNS - Kibana - Chromium

Zeek - DNS - Kibana x +

Not secure | localhost/app/kibana#/dashboard/ebf5ec90-34bf-11e7-9b32-bb903919ead9?_g=(refreshInterval:(pause:1... ☆ ⚙ ⋮

kibana

- Discover
- Visualize
- Dashboard
- Timelion
- Dev Tools
- Management
- Squert
- Logout

Collapse

DNS - Client

Client	Count
192.168.0.11	4

Export: Raw Formatted

DNS - Server

Server	Count
209.165.200.235	4

Export: Raw Formatted

DNS - Phishing Attempts Against ...

0 - 0

1 - 999999

Phishing

DNS - Phishing Attempts Against ...

0 - 0

1 - 999999

analyst@SecOnion: ~ Zeek - DNS - Kibana - Chromium 1 / 4

Applications Places Chromium Web Browser Mon 10:09

Zeek - DNS - Kibana - Chromium

Zeek - DNS - Kibana x +

Not secure | localhost/app/kibana#/dashboard/ebf5ec90-34bf-11e7-9b32-bb903919ead9?_g=(refreshInterval:(pause:1... ☆ ⚙ ⋮

kibana

- Discover
- Visualize
- Dashboard
- Timelion
- Dev Tools
- Management
- Squert
- Logout

Collapse

DNS - Queries

Query

17.201.165.209.in-addr.arpa

434f4e464944454e5449414c20444f43554d454e540a444f.

484152450a5468697320646f63756d656e7420636f6e7461

666f726d6174696f6e2061626f757420746865206c617374.

697479206272656163682e0a.ns.example.com

Export: Raw Formatted

DNS - Answers

No results found

analyst@SecOnion: ~ Zeek - DNS - Kibana - Chromium 1 / 4

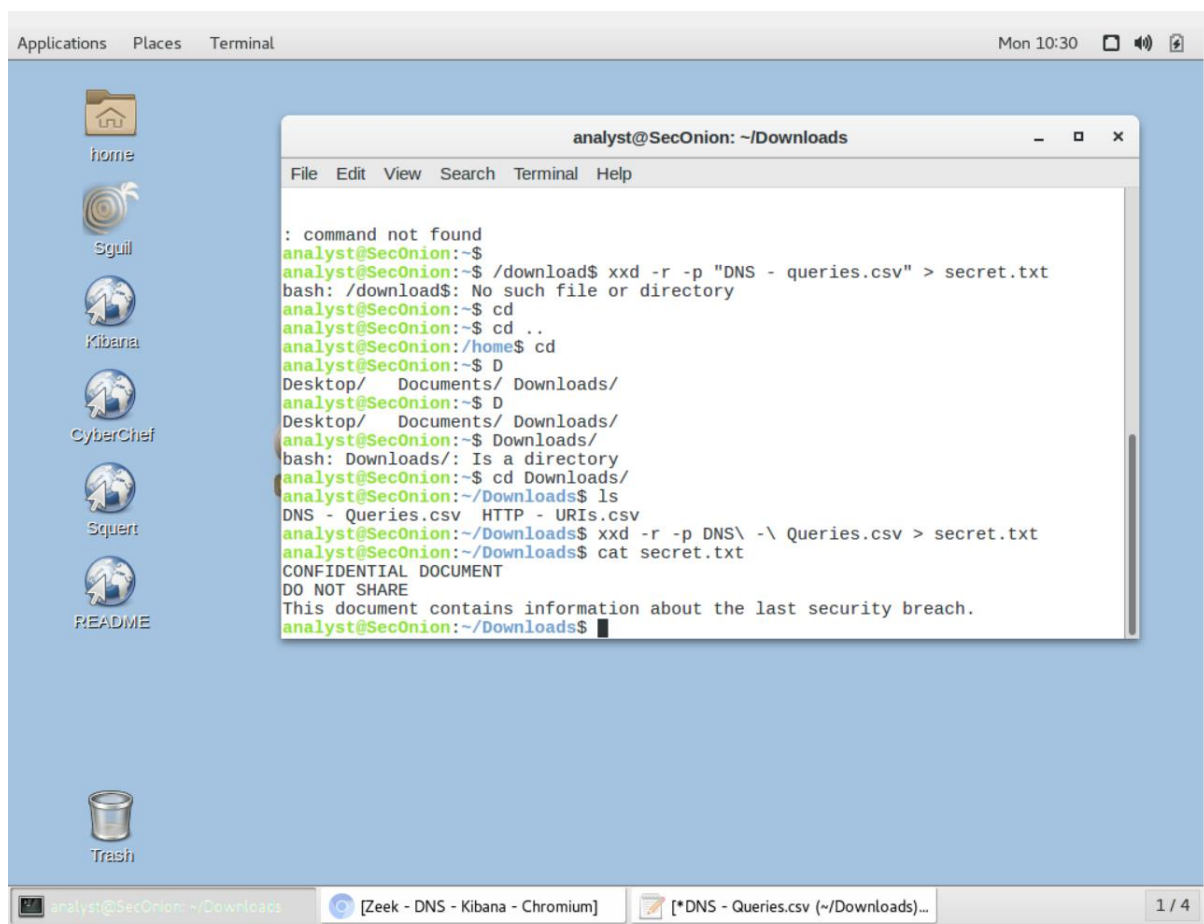
Le lunghe stringhe di numeri e lettere nei sottodomini sembrano testo codificato in esadecimale piuttosto che nomi di sottodomini legittimi. Fai clic sul collegamento esportando il download Raw per scaricare le query in un file esterno. Un file CSV viene scaricato nella cartella /home/analyst/Downloads.

Aprendo il file usando un editor di testo, come gedit. Modifichiamo il file eliminando il testo che circonda la parte esadecimale dei sottodomini, lasciando solo i caratteri esadecimali. Salva il file di testo modificato con il nome del file originale.

```
434f4e464944454e5449414c20444f43554d454e540a444f204e4f542053
484152450a5468697320646f63756d656e7420636f6e7461696e7320696e
666f726d6174696f6e2061626f757420746865206c617374207365637572
697479206272656163682e0a
```

c. In un terminale, usa il **xxd** comando per decodificare il testo nel file CSV e salvarlo in un file denominato secret.txt. Usa **cat** per inviare il contenuto di secret.txt alla console.

analista@SecOnion:~/Download\$ xxd -r -p "DNS - Queries.csv" > secret.txt
analista@SecOnion:~/ \$ cat secret.txt



The screenshot shows a Linux desktop with a blue background. On the left, there is a sidebar with icons for 'home', 'Sguil', 'Kibana', 'CyberChef', 'Squert', 'README', and 'Trash'. A terminal window titled 'analyst@SecOnion: ~/Downloads' is open in the center. The terminal output shows the following commands and results:

```
analyst@SecOnion:~/Downloads$ xxd -r -p "DNS - queries.csv" > secret.txt
bash: /download$: No such file or directory
analyst@SecOnion:~/Downloads$ cd
analyst@SecOnion:~/Downloads$ cd ..
analyst@SecOnion:~/Downloads$ cd
analyst@SecOnion:~/Downloads$ D
Desktop/ Documents/ Downloads/
analyst@SecOnion:~/Downloads$ D
Desktop/ Documents/ Downloads/
analyst@SecOnion:~/Downloads$ Downloads/
bash: Downloads/: Is a directory
analyst@SecOnion:~/Downloads$ cd Downloads/
analyst@SecOnion:~/Downloads$ ls
DNS - Queries.csv HTTP - URIs.csv
analyst@SecOnion:~/Downloads$ xxd -r -p DNS\ -\ Queries.csv > secret.txt
analyst@SecOnion:~/Downloads$ cat secret.txt
CONFIDENTIAL DOCUMENT
DO NOT SHARE
This document contains information about the last security breach.
analyst@SecOnion:~/Downloads$
```

The desktop taskbar at the bottom shows the terminal window, a browser window titled '[Zeek - DNS - Kibana - Chromium]', and a file manager window titled '[* DNS - Queries.csv (~/.Downloads)...]'. The system clock in the top right corner indicates 'Mon 10:30'.

Cosa implica questo risultato su queste particolari richieste DNS? Qual è il significato più ampio?

I risultati indicano che le richieste DNS erano richieste separate e coordinate contenenti contenuti nascosti. Il significato più ampio del risultato è che le query DNS potrebbero essere utilizzate per nascondere l'invio di file e aggirare la sicurezza della rete.

Cosa potrebbe aver creato queste query DNS codificate e perché il DNS è stato scelto come mezzo per esfiltrare i dati?

È possibile che il malware stia creando queste richieste scorrendo i documenti sull'host e codificandone il contenuto in esadecimale, quindi creando query DNS che utilizzano le stringhe esadecimali come sottodomini DNS. Le richieste DNS vengono molto comunemente inviate da una rete a Internet, quindi le richieste DNS potrebbero non essere monitorate.