Interpretare dati HTTP e DNS per isolare un Threat Actor

Obiettivi

In questo laboratorio, si analizzano i log relativi all'exploit di vulnerabilità documentate su protocolli HTTP e DNS. L'obiettivo è isolare l'attore minaccioso esaminando attacchi di SQL Injection e tecniche di esfiltrazione di dati tramite DNS.

Background / Scenario

MySQL è un database ampiamente utilizzato nelle applicazioni web, ma è vulnerabile a tecniche di SQL Injection che consentono a un attore malintenzionato di eseguire istruzioni SQL dannose e ottenere accesso non autorizzato ai dati. Inoltre, il servizio DNS, progettato per tradurre i nomi di dominio in indirizzi IP, può essere sfruttato per esfiltrare dati in modo nascosto.

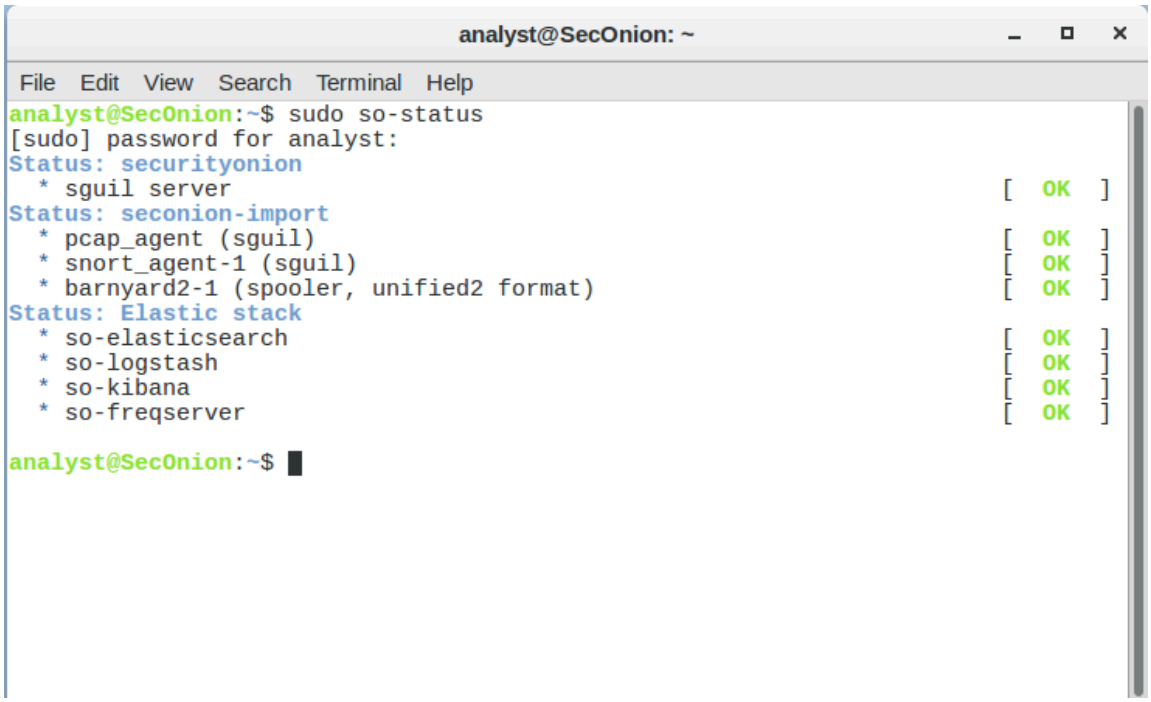
In questo laboratorio, si utilizza **Kibana** in esecuzione su una macchina virtuale **Security Onion** per indagare sugli exploit e identificare i dati esfiltrati tramite HTTP e DNS durante gli attacchi.

Procedura

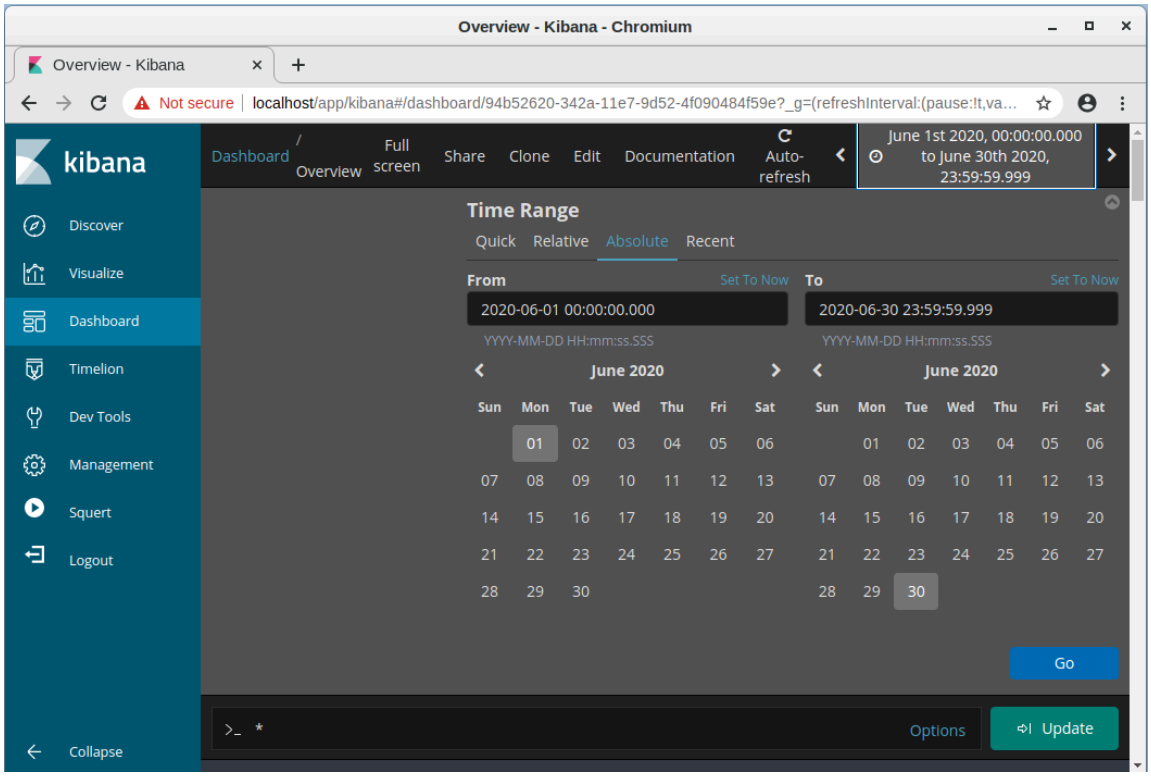
Parte 1: Identificazione di SQL Injection tramite HTTP

Passaggio 1: Accesso e Configurazione di Kibana

- Dopo l’avvio della macchina Security Onion, sono stati verificati i servizi per assicurarsi del corretto funzionamento, utilizzando il comando `sudo so-status`.

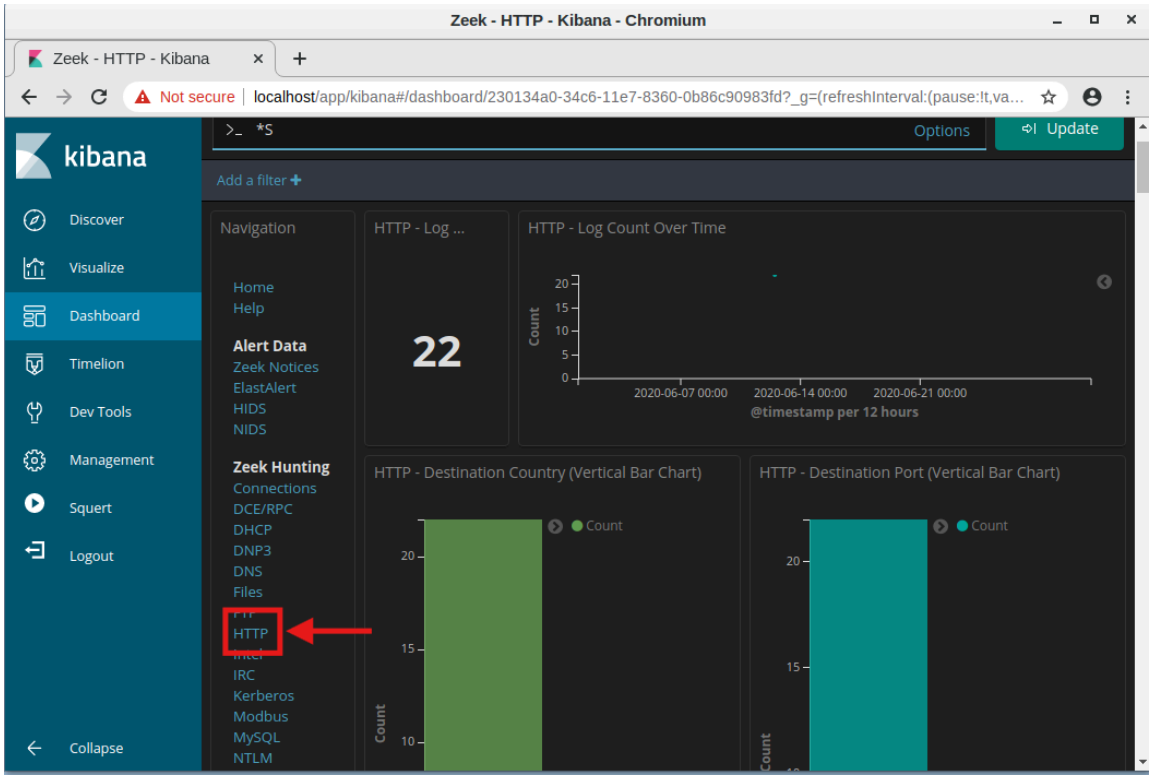


- Successivamente, è stato effettuato l'accesso a Kibana per l'analisi del traffico HTTP, impostando l’intervallo temporale per l'intero mese di giugno 2020, periodo durante il quale si è verificato l'attacco.

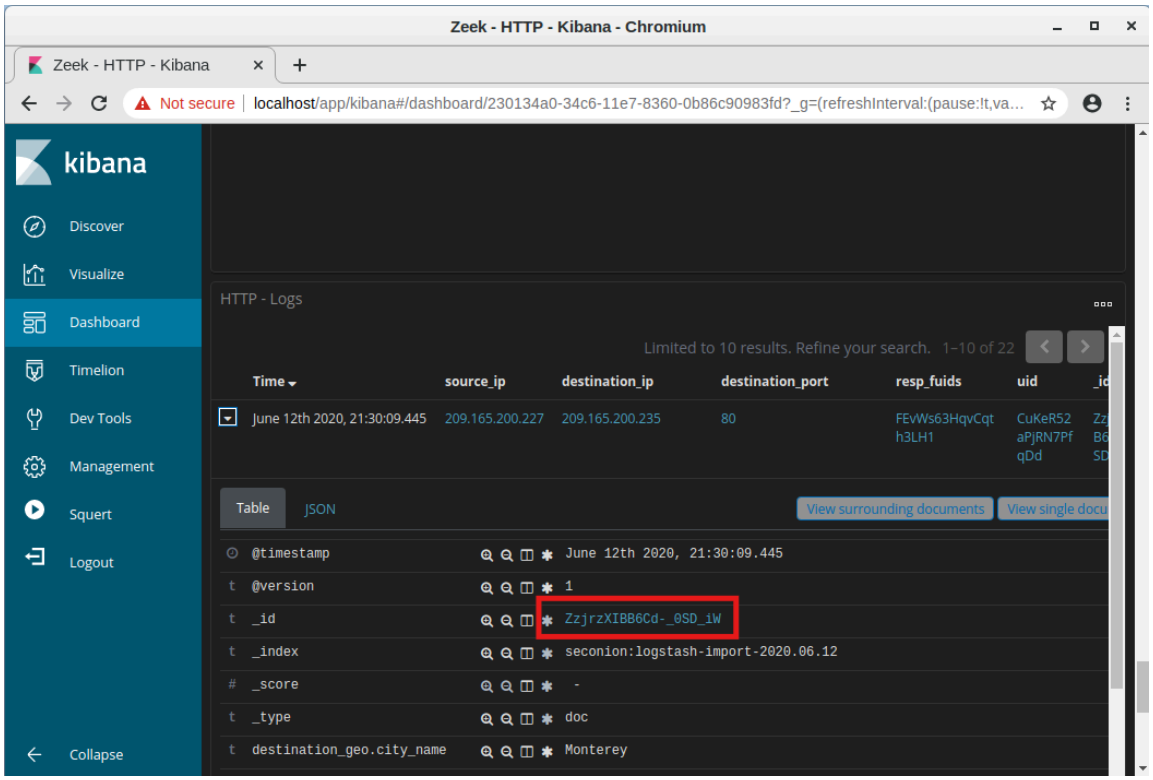


Passaggio 2: Applicazione del Filtro per il Traffico HTTP

- È stato applicato un filtro specifico per visualizzare solo il traffico HTTP. Questa selezione ha permesso di analizzare i log relativi alle richieste sospette, come gli indirizzi IP di origine e destinazione, e il numero di porta (80).

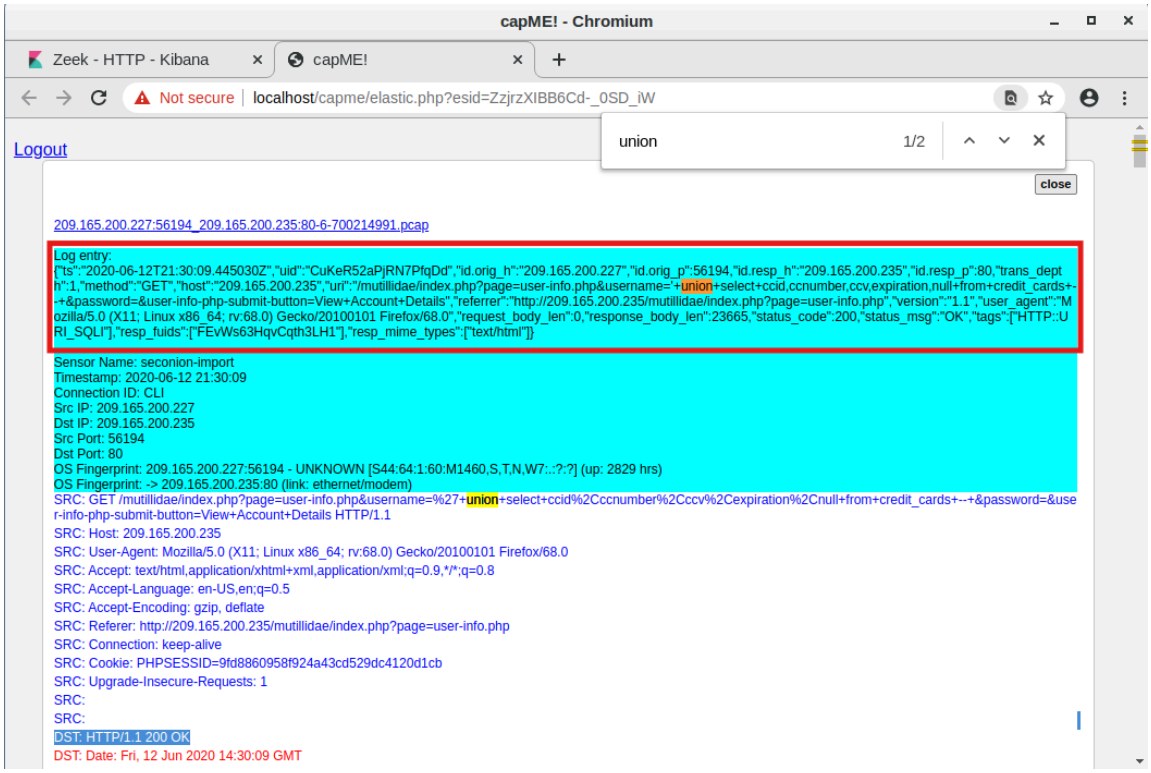


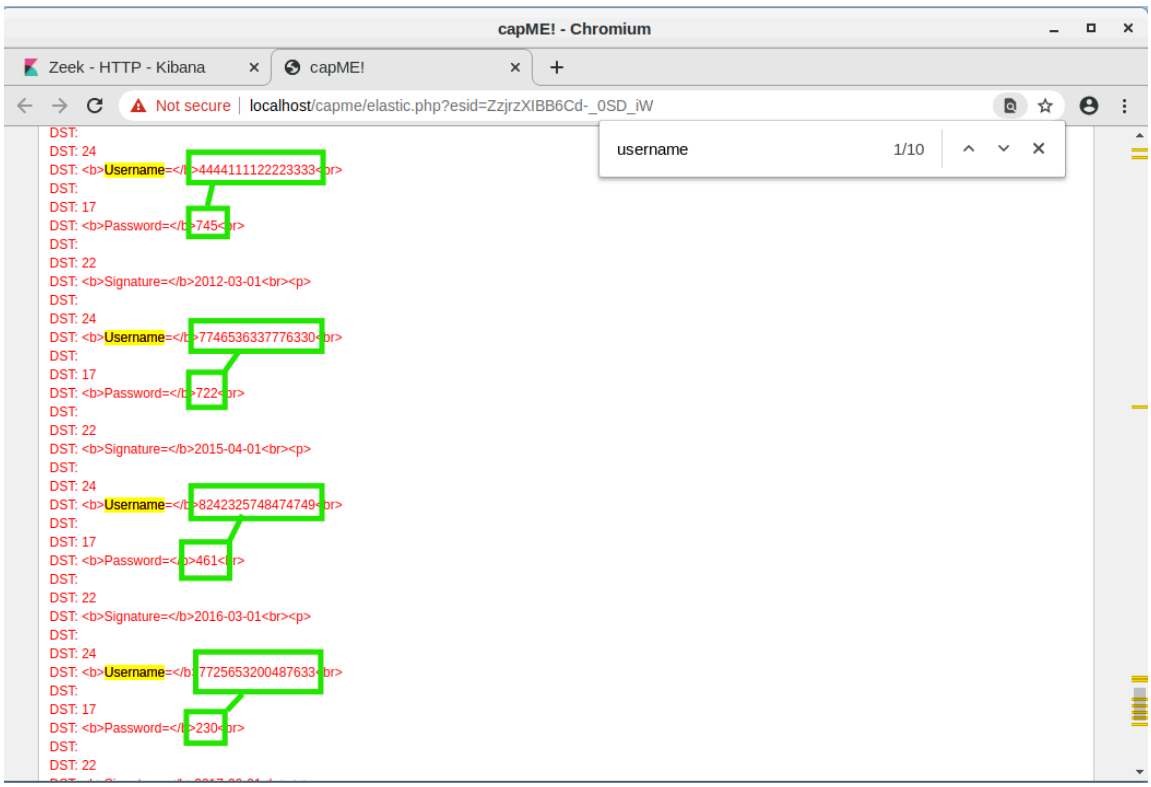
- Questi log hanno evidenziato attività anomale dirette al server web, suggerendo la possibilità di un attacco SQL Injection.



Passaggio 3: Esplorazione dei Log HTTP Dettagliati tramite capME!

- Utilizzando la funzionalità capME!, è stato possibile analizzare più in dettaglio le richieste HTTP, individuando elementi tipici di un tentativo di SQL Injection, come l'uso dei comandi `union` e `select` nella stringa di richiesta.
- Questo ha confermato che l'attore minaccioso stava cercando di bypassare l'autenticazione per accedere a dati sensibili presenti nel database, ottenendo informazioni come numeri di carte di credito e dati di autenticazione. In questo caso Username e Pass.

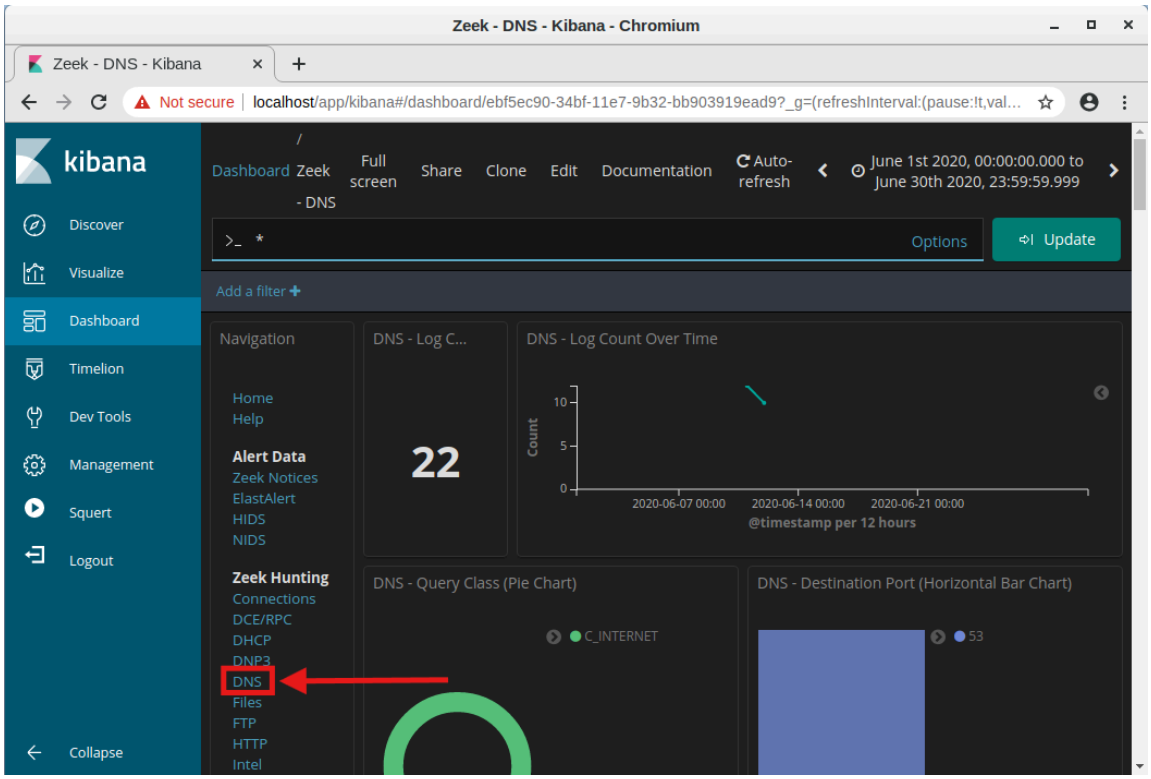


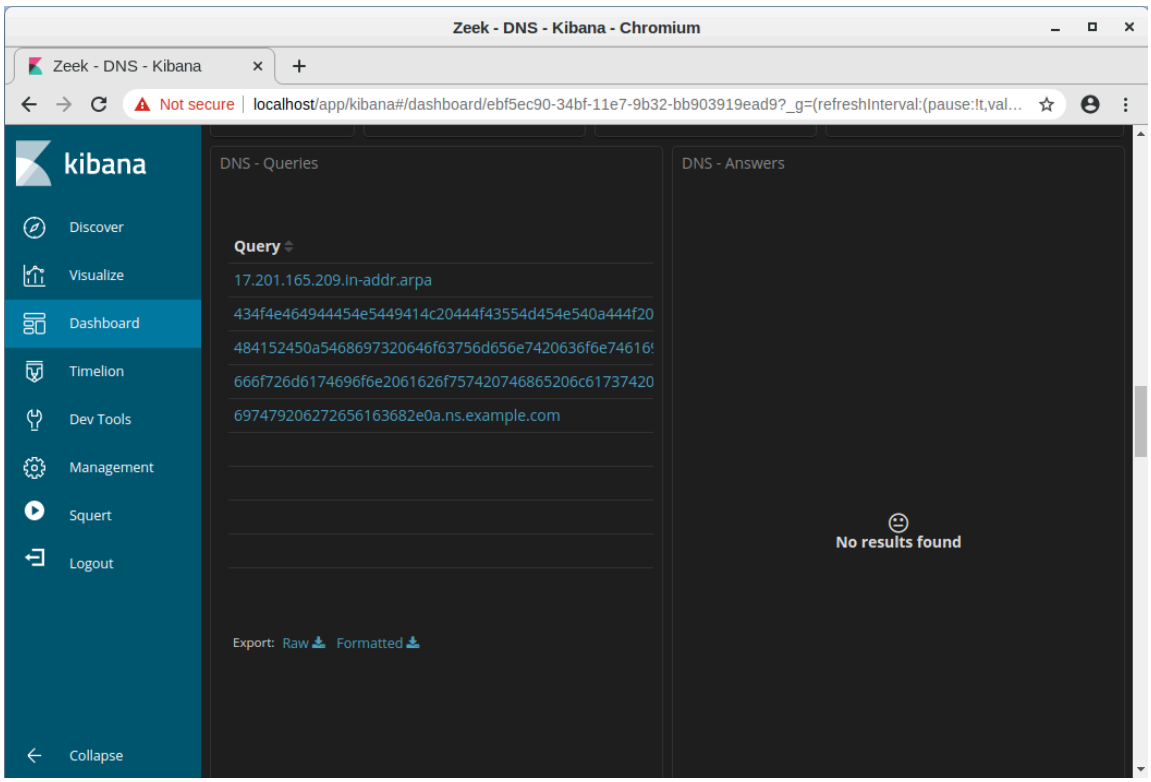


Parte 2: Esame dell'Esfiltrazione di Dati tramite DNS

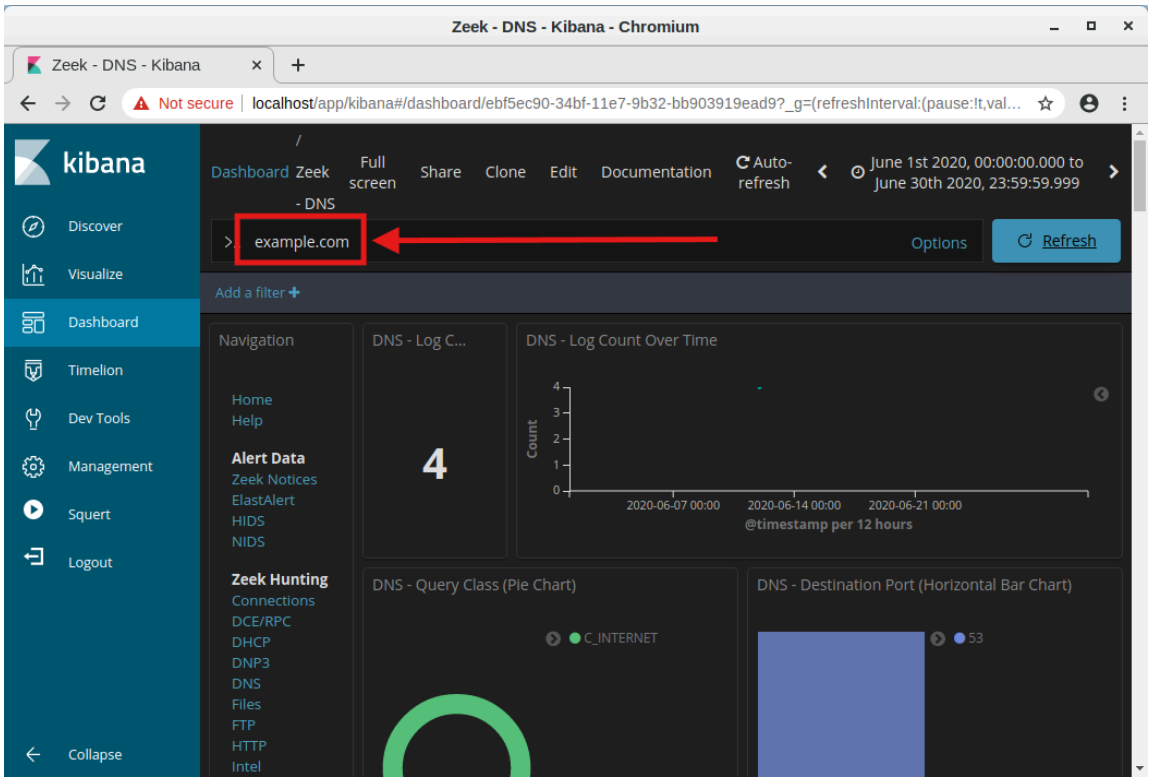
Passaggio 1: Analisi delle Query DNS Anomale

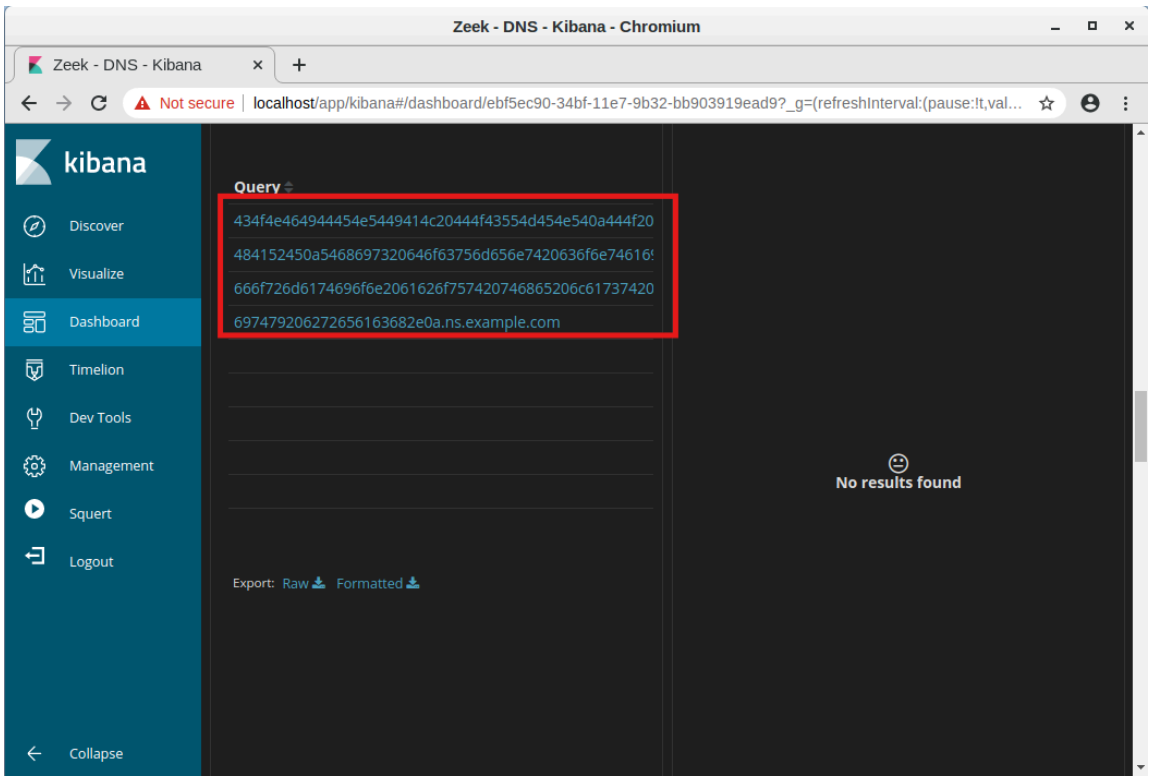
- Dopo l'analisi dell'attacco SQL Injection, l'attenzione si è spostata sul traffico DNS. Filtrando per DNS, sono state individuate query con subdomini insolitamente lunghi associati a `example.com`, suggerendo un possibile tentativo di esfiltrazione dati.





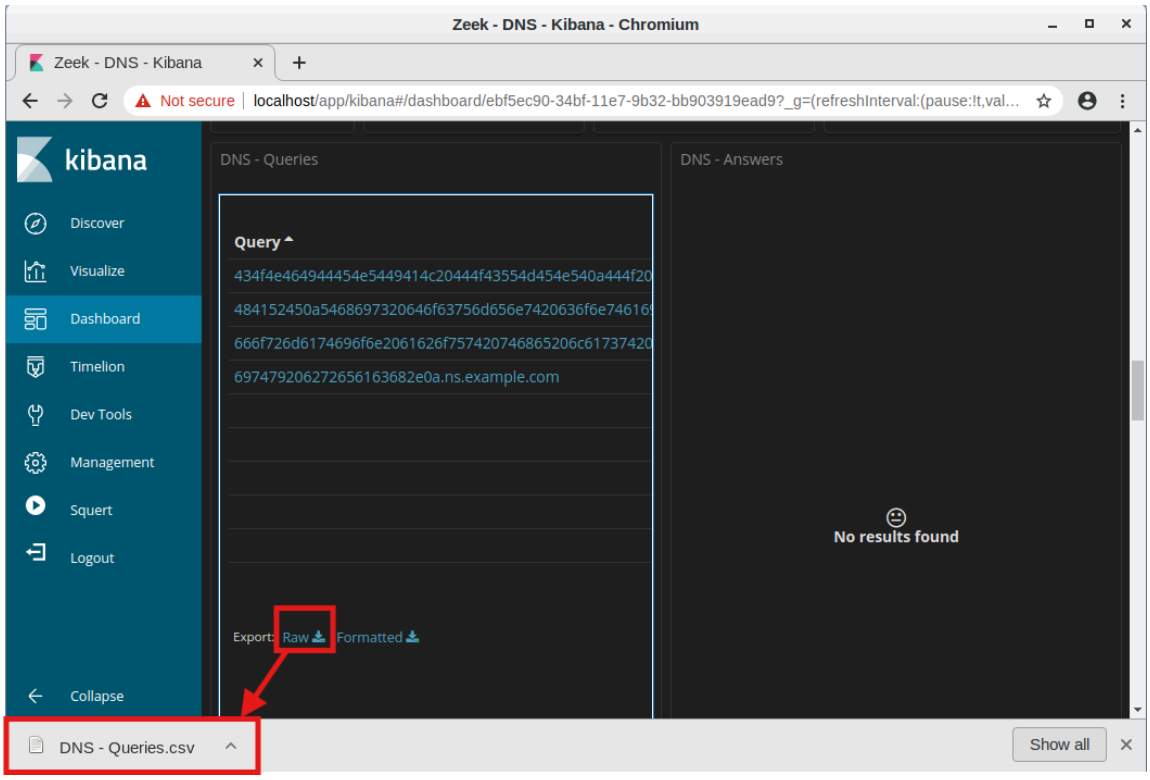
- Con il filtraggio delle query con il tag example.com abbiamo trovato le query in questione.Tali query contenevano stringhe esadecimali che indicavano una possibile codifica di dati sensibili all'interno dei subdomini DNS.

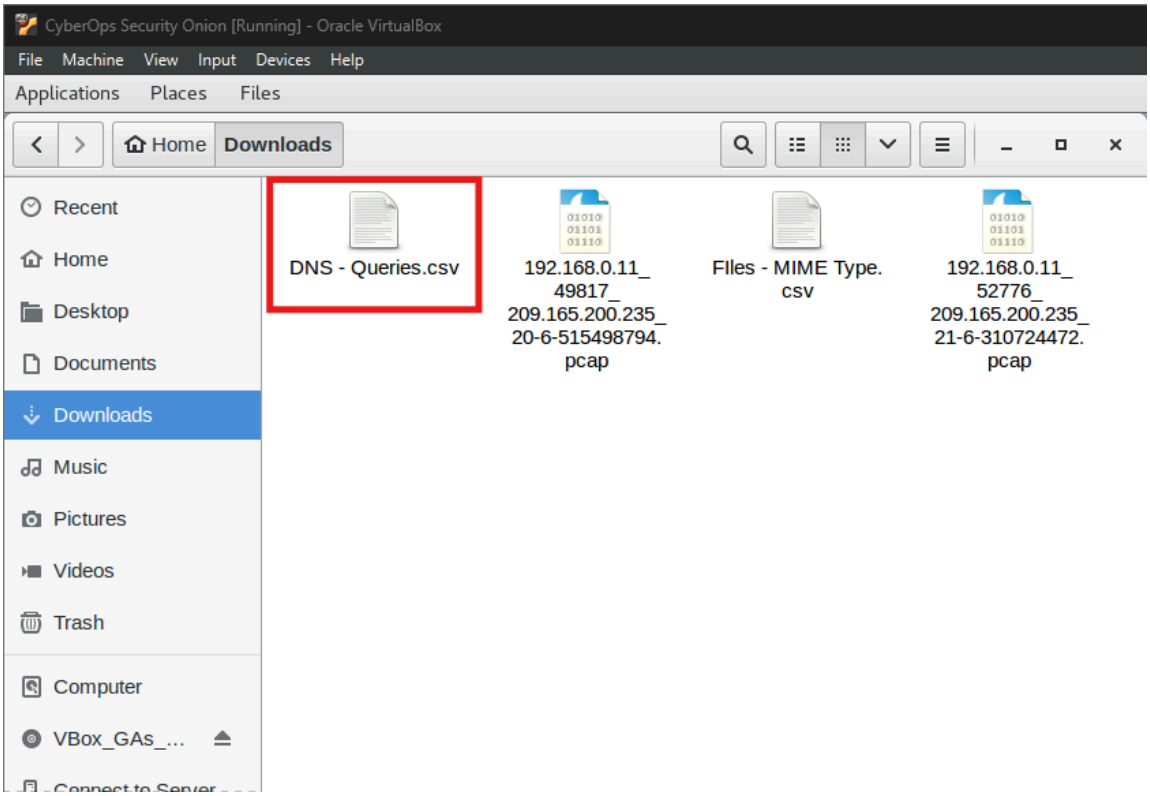




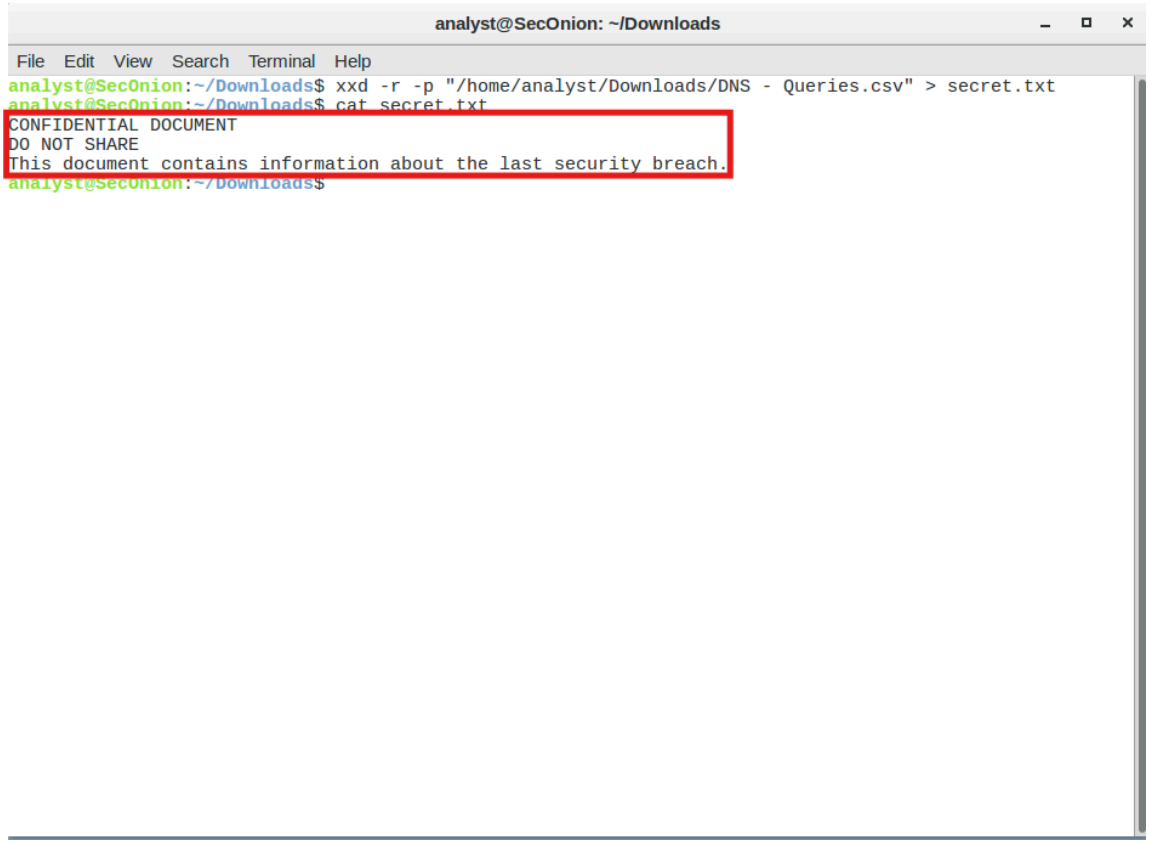
Passaggio 2: Esportazione e Decodifica delle Query DNS

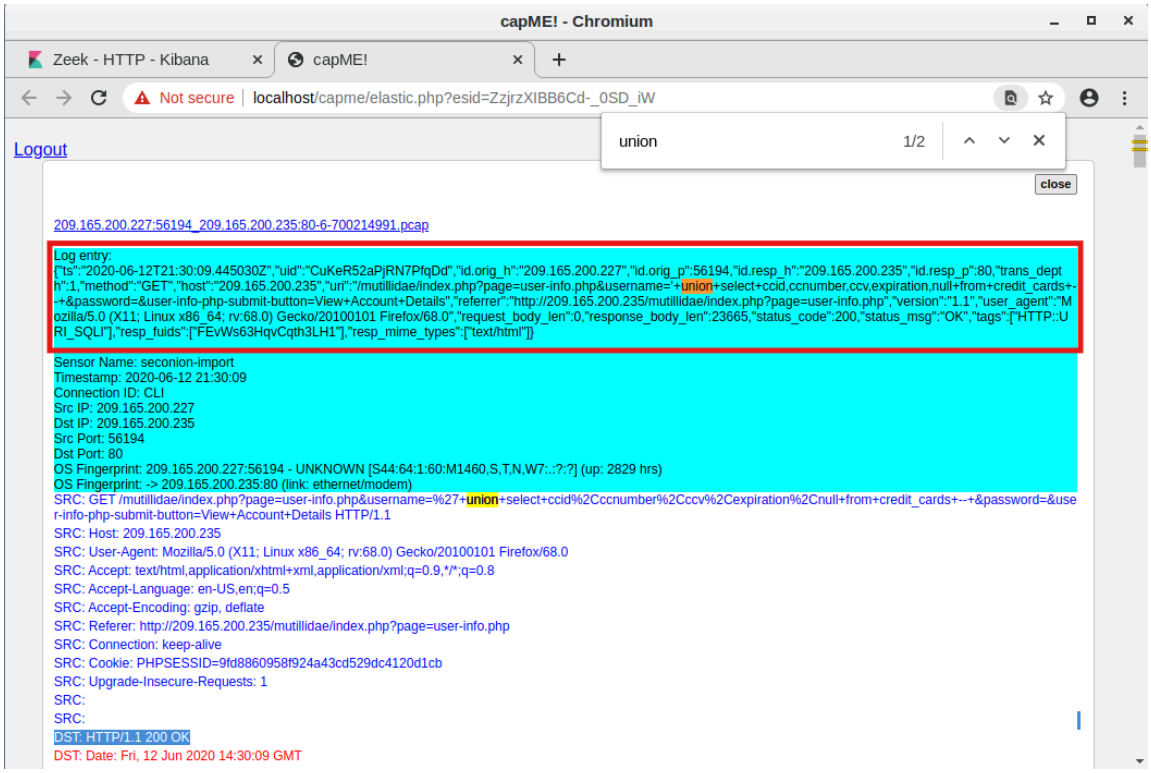
- Le query sospette sono state esportate in un file CSV, da cui sono state estratte le sequenze esadecimali.





- Attraverso il comando `xxd`, queste stringhe sono state decodificate in testo leggibile, rivelando contenuti riservati come messaggi con la dicitura “CONFIDENTIAL DOCUMENT,” implicando che le query DNS fossero usate per nascondere e inviare dati riservati all’esterno della rete.


analyst@SecOnion: ~/Downloads
File Edit View Search Terminal Help
analyst@SecOnion:~/Downloads$ xxd -r -p "/home/analyst/Downloads/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$


capME! - Chromium
Zeek - HTTP - Kibana
capME!
Not secure
localhost/capme/elastic.php?esid=ZzjrzXIBB6Cd-_0SD_iW
union
1/2
Logout
close
209.165.200.227:56194_209.165.200.235:80-6-700214991.pcap
Log entry:
{"ts":"2020-06-12T21:30:09.445030Z","uid":"CuKeR52aPjRN7PfqDd","id.orig_h":"209.165.200.227","id.orig_p":56194,"id.resp_h":"209.165.200.235","id.resp_p":80,"trans_depth":1,"method":"GET","host":"209.165.200.235","uri":"/mutillidae/index.php?page=user-info.php&username='+union+select+ccid,ccnumber,ccv,expiration,null+from+credit_cards+--+&password=&user-info-php-submit-button=View+Account+Details","referrer":"http://209.165.200.235/mutillidae/index.php?page=user-info.php","version":"1.1","user_agent":"Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0","request_body_len":0,"response_body_len":23665,"status_code":200,"status_msg":"OK","tags":["HTTP::URI_SQLI"],"resp_fuids":["FEvWs63HqvCqth3LH1"],"resp_mime_types":["text/html"]}
Sensor Name: seconion-import
Timestamp: 2020-06-12 21:30:09
Connection ID: CLI
Src IP: 209.165.200.227
Dst IP: 209.165.200.235
Src Port: 56194
Dst Port: 80
OS Fingerprint: 209.165.200.227:56194 - UNKNOWN [S44:64:1:60:M1460,S,T,N,W7:.:?:?] (up: 2829 hrs)
OS Fingerprint: -> 209.165.200.235:80 (link: ethernet/modem)
SRC: GET /mutillidae/index.php?page=user-info.php&username=%27+union+select+ccid%2Cccnumber%2Cccv%2Cexpiration%2Cnull+from+credit_cards+--+&password=&user-info-php-submit-button=View+Account+Details HTTP/1.1
SRC: Host: 209.165.200.235
SRC: User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
SRC: Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
SRC: Accept-Language: en-US,en;q=0.5
SRC: Accept-Encoding: gzip, deflate
SRC: Referer: http://209.165.200.235/mutillidae/index.php?page=user-info.php
SRC: Connection: keep-alive
SRC: Cookie: PHPSESSID=9fd8860958f924a43cd529dc4120d1cb
SRC: Upgrade-Insecure-Requests: 1
SRC:
SRC:
DST: HTTP/1.1 200 OK
DST: Date: Fri, 12 Jun 2020 14:30:09 GMT

Conclusioni

L’analisi conferma che l’attacco ha coinvolto una SQL Injection per l’accesso non autorizzato ai dati, e tecniche di esfiltrazione di informazioni tramite DNS per trasmettere dati riservati. Questi risultati sottolineano l’importanza di un monitoraggio continuo di traffico HTTP e DNS, e dell’utilizzo di strumenti avanzati per l’identificazione di anomalie e minacce nella rete aziendale.