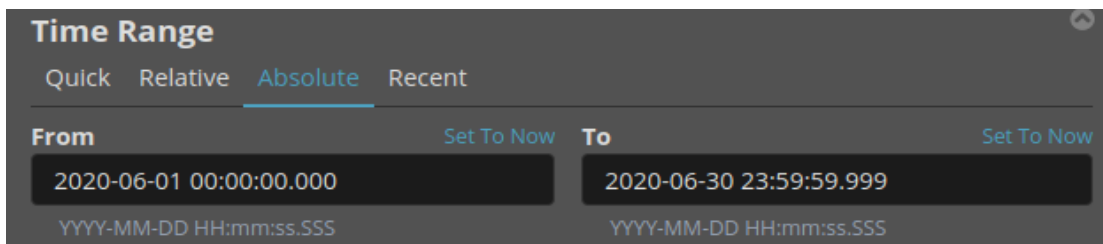


Bonus 1: Interpretare Dati HTTP e DNS per Isolare l'Attore della Minaccia

Passo 1

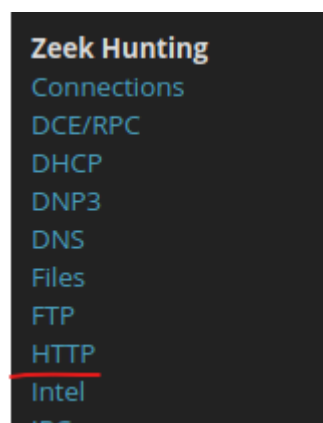
Cambiare l'intervallo di tempo. È stato determinato che l'exploit è avvenuto in un momento durante il mese di giugno 2020. Kibana mostra per impostazione predefinita i dati delle ultime 24 ore. Dovrai cambiare le impostazioni temporali per vedere i dati del mese di giugno 2020.



The screenshot shows the 'Time Range' configuration interface in Kibana. The 'Absolute' tab is selected. The 'From' field is set to '2020-06-01 00:00:00.000' and the 'To' field is set to '2020-06-30 23:59:59.999'. Both fields have a 'Set To Now' link next to them. The format 'YYYY-MM-DD HH:mm:ss.SSS' is indicated below each field.

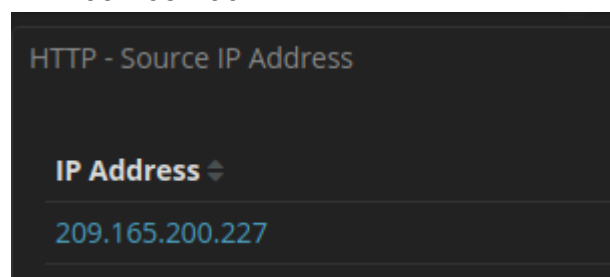
Passo 2

Filtrare per traffico HTTP. a. Poiché l'attore della minaccia ha avuto accesso a dati memorizzati su un server web, viene utilizzato il filtro HTTP per selezionare i log associati al traffico HTTP



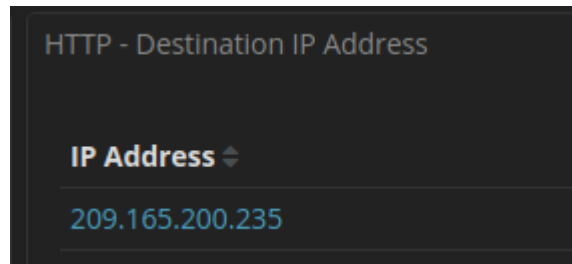
Qual è l'indirizzo IP sorgente?

L'indirizzo IP sorgente è 209.165.200.227



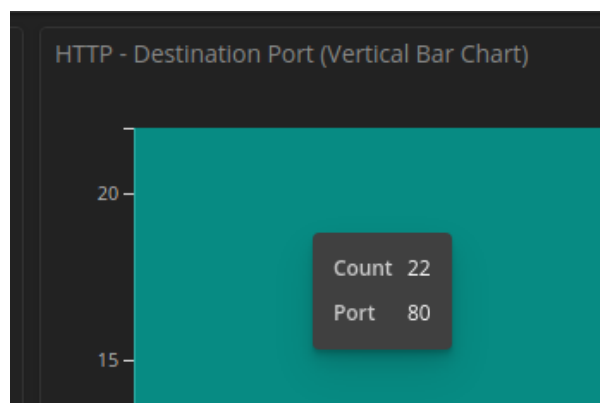
Qual è l'indirizzo IP destinazione?

L'indirizzo IP di destinazione è 209.165.200.235.



Qual è il numero di porta destinazione?

Il numero della porta di destinazione è la porta 80.

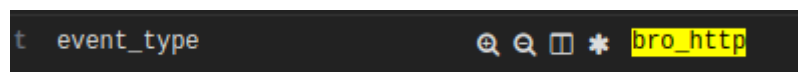


Qual è il timestamp del primo risultato?

Il timestamp del primo log è 12 giugno 2020, 21:30:09.445

Qual è il tipo di evento?

Il tipo di evento è bro_http, indica probabilmente che il log è stato processato da Zeek



Cosa è incluso nel campo message? Questi sono dettagli sulla richiesta HTTP GET fatta dal client al server. Concentrati specialmente sul campo uri nel testo del messaggio.

Nel campo message, più in particolare nel campo "uri" è presente una **sql injection**.

```
5.200.227", "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
```

Qual è il significato di queste informazioni?

È un attacco sql injection che mira al furto di molteplici dati, tra cui username, password e numeri di carte di credito.

Passo 3

Rivedere i risultati.

Cosa vedi più avanti nella trascrizione riguardo ai nomi utente? Fornisci alcuni esempi di nome utente, password e firma che sono stati esfiltrati.

Scorrendo tra i vari risultati ricercando la parola chiave username, si trovano dei valori numerici affiancati alla parola username.

4
b>Username=4444111122223333
 Username

7
b>Password=745
 Password

2
b>Signature=2012-03-01
<p> Firma

4
b>Username=7746536337776330

7
b>Password=722

2
b>Signature=2015-04-01
<p>

4
b>Username=8242325748474749

Parte 2 Analizzare l'Esfiltrazione DNS

Registra gli indirizzi IP del client e del server DNS.

Come indirizzo DNS Client abbiamo 192.168.0.11 e come DNS Server 209.165.200.235

DNS - Client		DNS - Server	
Client ▾	Count ▾	Server ▾	Count ▾
192.168.0.11	4	209.165.200.235	4

Passo 3 Determinare i dati esfiltrati.

I sottodomini delle query DNS erano sottodomini? Se no, qual è il testo?

Non sono sottodomini ma testo in esadecimale per offuscare il messaggio.

```
analyst@SecOnion:~/Downloads$ xxd -r -p "DNS - Queries.csv" > secret2.txt
analyst@SecOnion:~/Downloads$ cat secret2.txt
CONFIDENTIAL DOCUMENT
DO NOT SHARE
This document contains information about the last security breach.
```

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

Questo implica magari che si vogliano esfiltrare dei dati su un sito esterno, mandando i dati attraverso richieste DNS e ricostruisce i dati attraverso le richieste ricevute e usa le query crittate per non destare sospetti.

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

Queste query DNS possono essere state create dall'attaccante per inviare dati rubati dalla rete compromessa al proprio server di Command and Control (C2) su Internet, gli attori principali possono essere un trojan installato su un sistema compromesso oppure un utente malintenzionato che utilizza strumenti di DNS Tunneling per bypassare le misure di sicurezza.

Il DNS è un protocollo attraente per l'esfiltrazione dati perché è quasi sempre consentito e raramente ispezionato dai firewall e dai sistemi di sicurezza. La maggior parte delle organizzazioni configura i firewall per consentire il traffico DNS (porta UDP 53) sia in entrata che in uscita. Bloccare il DNS impedirebbe il normale funzionamento di Internet.