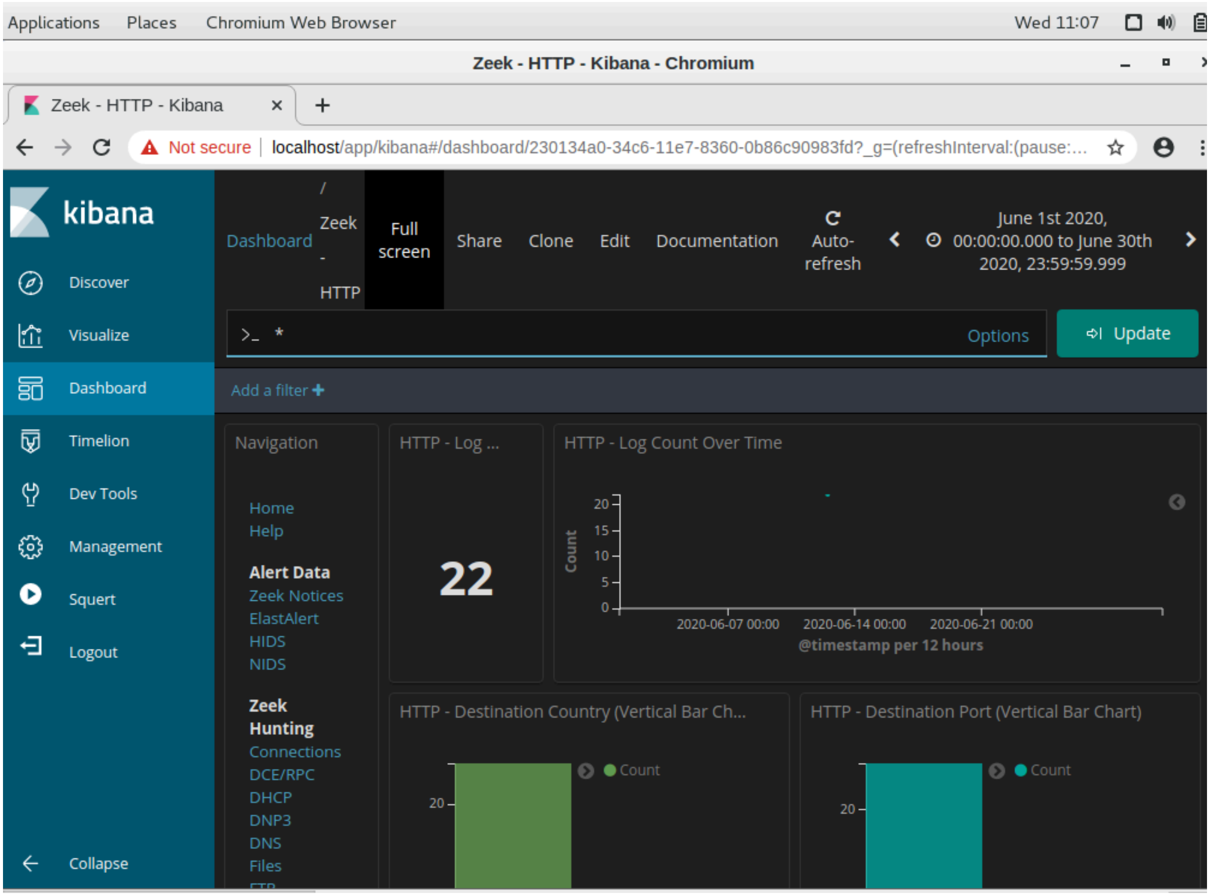
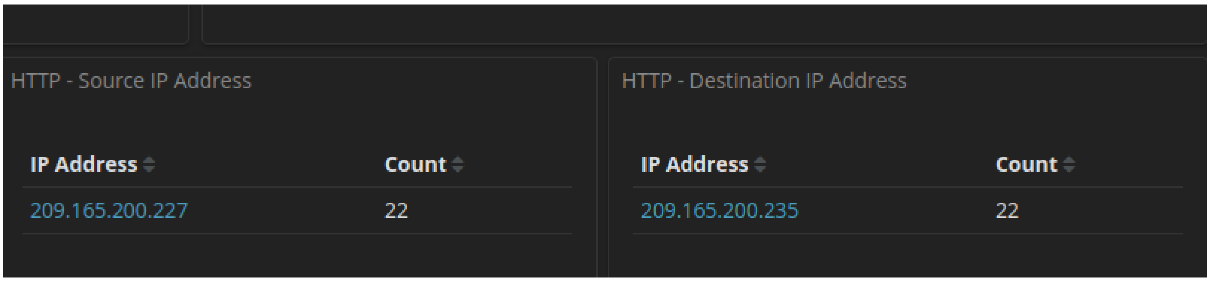
REPORT ATTIVITA': Interpretare Dati HTTP e DNS per Isolare l'Attore della Minaccia

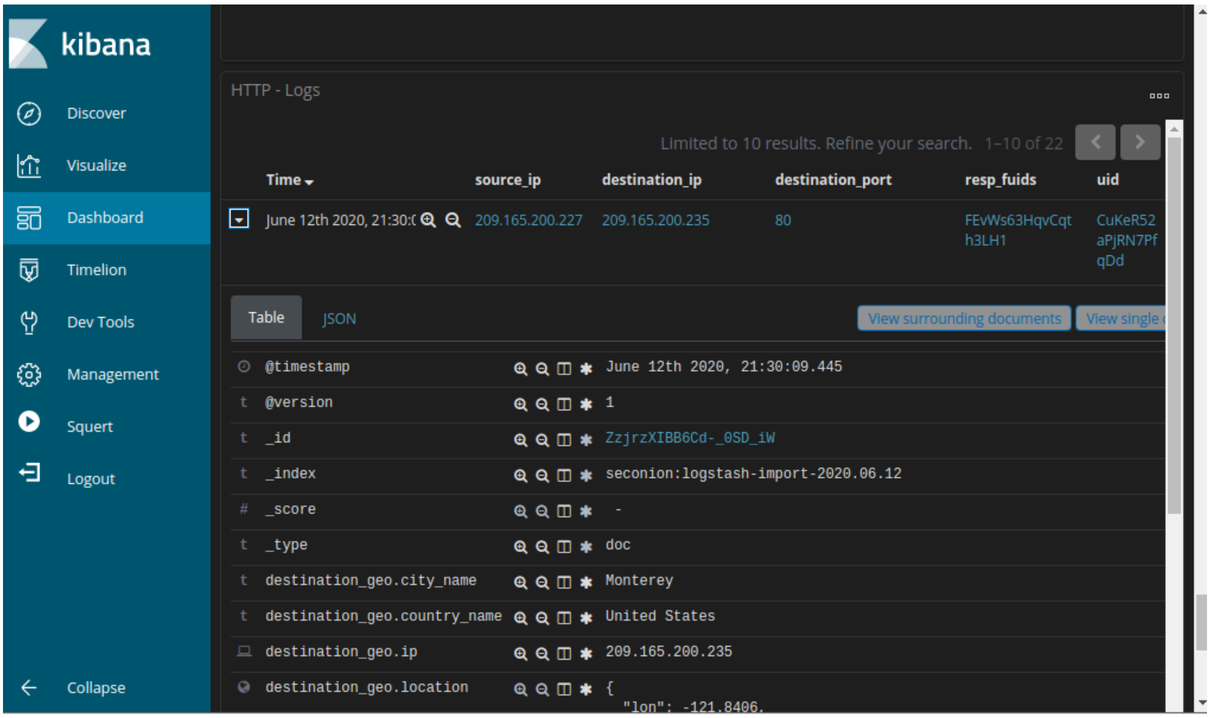
BW III

Investigare un Attacco di SQL Injection



Qual è l'indirizzo IP sorgente? 209.165.200.227
Qual è l'indirizzo IP destinazione? 209.165.200.235
Qual è il numero di porta destinazione? 80





Qual è il timestamp del primo risultato?

june 12th 2020 21:30:09. 445

Qual è il tipo di evento?

bro_http

Cosa è incluso nel campo message?

contiene un oggetto in formato JSON che riassume i metadati della transazione HTTP acquisiti dal sensore Zeek

Qual è il significato di queste informazioni?

- L'attaccante sta puntando alla pagina `user-info.php` dell'applicazione Mutillidae, un sistema test utilizzato per essere deliberatamente vulnerabile
- La presenza della stringa `union+select` indica che l'attaccante sta sfruttando una vulnerabilità di tipo **SQL Injection**. L'obiettivo è "unire" i risultati di una query legittima con i dati provenienti da un'altra tabella del database.
- Il comando specifica chiaramente il furto di informazioni sensibili: l'attaccante sta tentando di esfilatrare i numeri delle carte di credito (`ccnumber`), i codici di sicurezza (`ccv`) e le date di scadenza (`expiration`) dalla tabella chiamata `credit_cards`.

- I caratteri `--+` alla fine della stringa servono a "commentare" il resto della query SQL originale del server, impedendo che errori di sintassi possano bloccare l'esecuzione del comando malevolo.

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

numero carta di credito | CVV | data scadenza

Esempio 1:

- numero carta: `8242325748474749`
- CVV: `722`
- Scadenza: `2015-04-01`

Esempio 2:

- numero carta: `7725653200487633`
- CVV: `461`
- Scadenza: `2016-03-01`

Esempio 3:

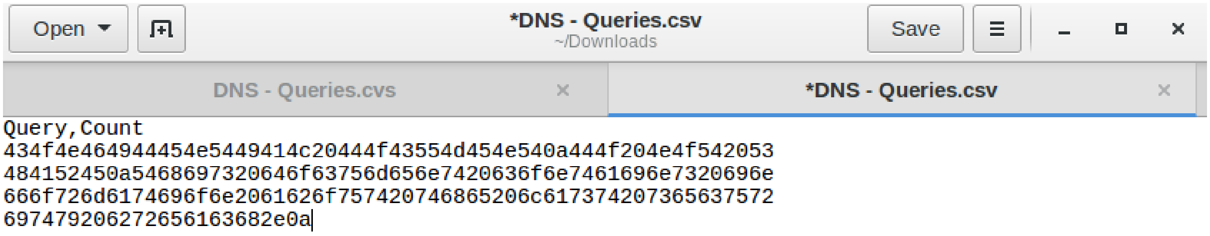
- numero carta: `1234567812345678`
- CVV: `230`
- Scadenza: `2017-06-01`

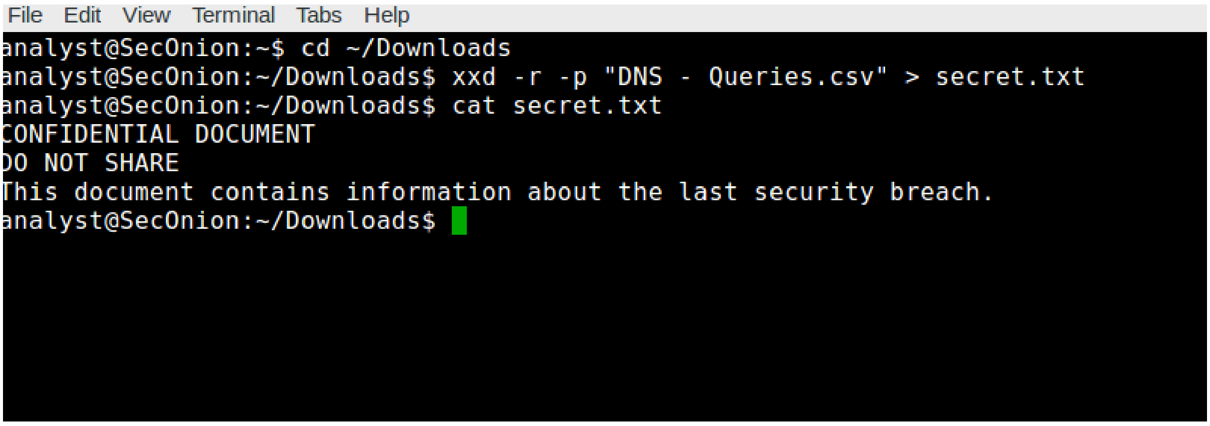
Questi dati confermano che l'attaccante è riuscito a risalire ai campi della tabella `credit_cards` (numero carta, CVV e scadenza) sui campi di output dell'applicazione `Username`, `Password` e `Signature`, completando con successo l'esfiltrazione.

Rivedere le voci relative al DNS

indirizzo IP del client: 192.168.0.11
indirizzo IP del server: 209.165.200.235

Determinazione dei dati esfiltrati





I sottodomini delle query DNS erano sottodomini?

No, non erano nomi di dominio legittimi. Si trattava di testo codificato in esadecimale (caratteri 0-9, a-f) che rappresentava il contenuto di un documento riservato.

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

Il risultato della decodifica mostra che le query DNS non erano affatto richieste di risoluzione nomi, ma un metodo di trasporto dati.

In modo più ampio significa:

che l'attaccante ha utilizzato il DNS Tunneling, una tecnica che sfrutta il protocollo DNS per creare un canale di comunicazione bidirezionale o per l'esfiltrazione unidirezionale di dati bypassando i controlli di rete.

che le stringhe esadecimali catturate nei sottodomini di `ns.example.com` contenevano un documento classificato come "CONFIDENTIAL", dimostrando che informazioni sensibili relative a una precedente violazione di sicurezza sono state sottratte con successo dall'azienda.

che questo metodo è stato scelto perché il traffico DNS è quasi sempre autorizzato a passare attraverso i firewall aziendali e spesso non viene ispezionato dai sistemi di monitoraggio standard, permettendo all'attaccante di operare "sotto il radar".

che l'esistenza di queste query implica che un dispositivo all'interno della rete è stato compromesso da uno script o da un malware programmato per leggere file locali, codificarli e inviarli all'esterno tramite richieste DNS fraudolente.

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

La query ha creato un software malevolo o uno script di esfiltrazione installato su un host compromesso all'interno della rete. Questo strumento ha frammentato il documento riservato e lo ha inserito nei sottodomini delle query DNS per inviarlo all'attaccante.

Il DNS è stato scelto perché è un protocollo quasi sempre consentito dai firewall per permettere la navigazione. Poiché il traffico DNS viene raramente ispezionato per il contenuto dei dati (payload), rappresenta un canale perfetto per rubare informazioni senza far scattare gli allarmi di sicurezza tradizionali.
