

Interpretare i dati HTTP e DNS per isolare l'attore malevolo

Dopo aver effettuato l'accesso a kibana con username **analyst** e password **cyberops** bisogna inserire un range orario dal 2020-06-01 al 2020-06-30.

The screenshot shows the Kibana interface with the 'Dashboard' sidebar on the left. The main content area displays the 'Time Range' configuration for a dashboard. The 'Absolute' tab is selected, showing the 'From' and 'To' date pickers. The 'From' date is set to '2020-06-01 00:00:00.000' and the 'To' date is set to '2020-06-30 23:59:59.999'. Below the date pickers, there are two calendar views for June 2020. The first calendar shows the date '01' selected, and the second calendar shows the date '30' selected. A 'Go' button is located at the bottom right of the time range configuration area.

kibana

Dashboard / Overview Full screen Share Clone Edit Documentation Auto-refresh

June 1st 2020, 00:00:00.000 to June 30th 2020, 23:59:59.999

Time Range

Quick Relative **Absolute** Recent

From Set To Now **To** Set To Now

2020-06-01 00:00:00.000 2020-06-30 23:59:59.999

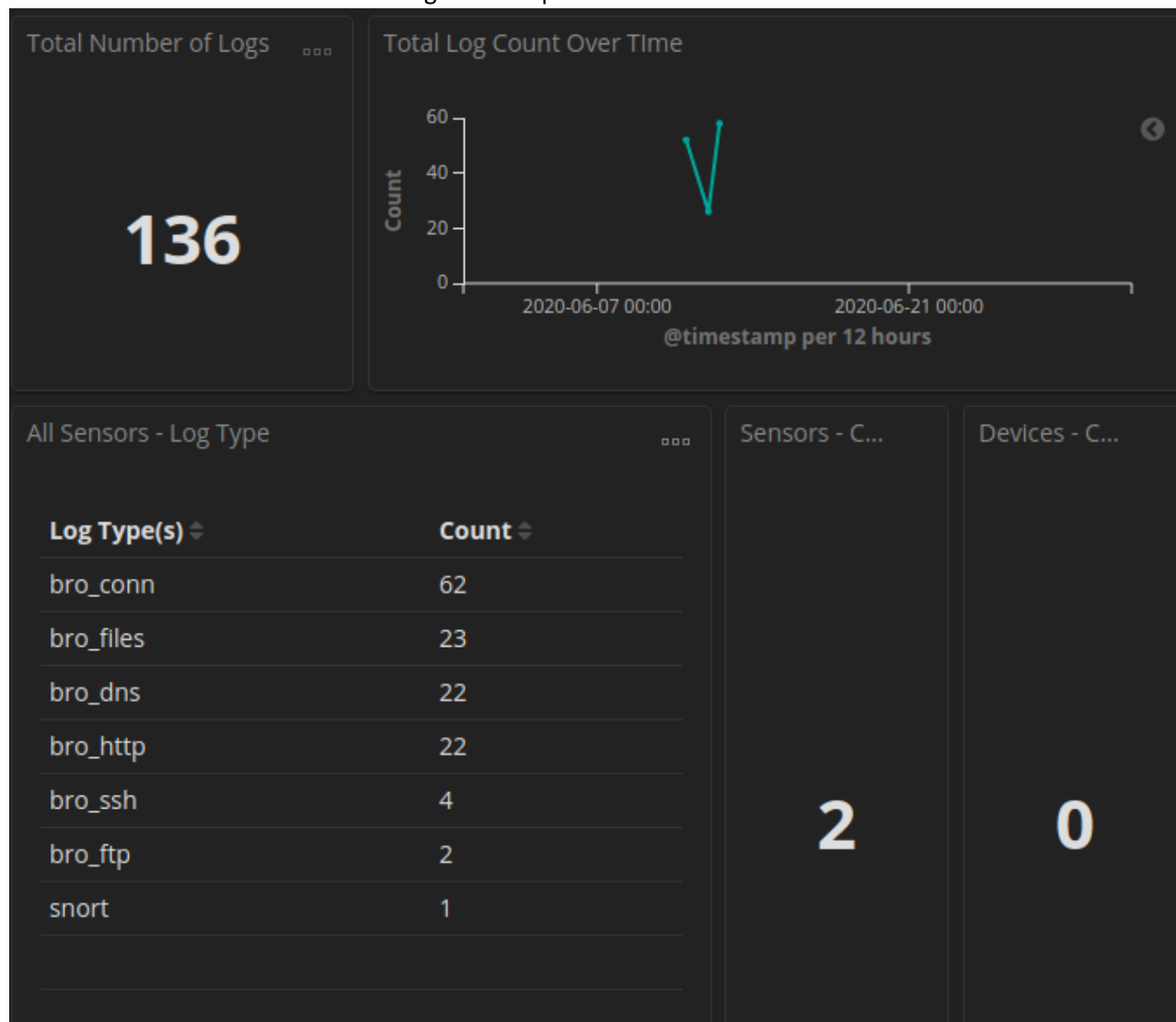
YYYY-MM-DD HH:mm:ss.SSS YYYY-MM-DD HH:mm:ss.SSS

< June 2020 > < June 2020 >

Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat
	01	02	03	04	05	06		01	02	03	04	05	06
07	08	09	10	11	12	13	07	08	09	10	11	12	13
14	15	16	17	18	19	20	14	15	16	17	18	19	20
21	22	23	24	25	26	27	21	22	23	24	25	26	27
28	29	30					28	29	30				

Go

Noteremo subito un numero di 136 log totali di quel mese



Utilizzando uno dei filtri già presenti andremo a filtrare per log di http

Applications

Places

Chromium Web Browser

Tue 08:57

Zeek - HTTP - Kibana - Chromium

Zeek - HTTP - Kibana

+

←

→

↻

⚠ Not secure

localhost/app/kibana#/dashboard/230134a0-34c6-11e7-8360-0b86c90983fd?_g=(refreshInterval:(pause:...

☆

👤

⋮

kibana

Discover

Visualize

Dashboard

Timelion

Dev Tools

Management

Squert

Logout

← Collapse

Dashboard

Zeek

Full screen

Share

Clone

Edit

Documentation

Auto-refresh

June 1st 2020, 00:00:00.000 to June 30th 2020, 23:59:59.999

HTTP

>_ *|

Options

↻ Update

Add a filter +

Navigation

Home

Help

Alert Data

Zeek Notices

ElastAlert

HIDS

NIDS

Zeek Hunting

Connections

DCE/RPC

DHCP

DNP3

DNS

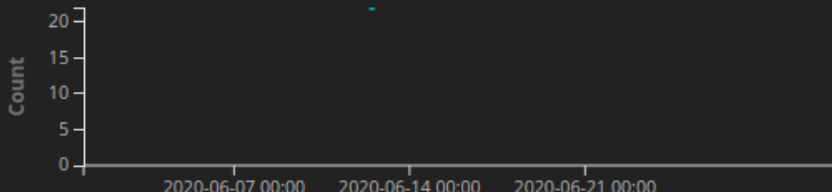
Files

FTP

HTTP - Log ...

22

HTTP - Log Count Over Time

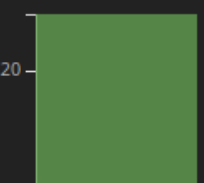


Count

2020-06-07 00:002020-06-14 00:002020-06-21 00:00

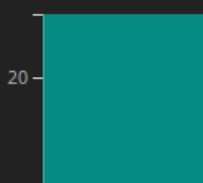
@timestamp per 12 hours

HTTP - Destination Country (Vertical Bar Ch...



Count

HTTP - Destination Port (Vertical Bar Chart)



Count

Zeek - HTTP - Kibana - Chromium

1 / 4

Scorrendo tra i risultati notiamo l'ip sorgente e di destinazione e la porta.

HTTP - Logs						...
Limited to 10 results. Refine your search. 1-10 of 22						< >
Time ▼	source_ip	destination_ip	destination_port	resp_fuids	uid	
▶ June 12th 2020, 21:30:09.445	209.165.200.227	209.165.200.235	80	FEvWs63HqvCqt h3LH1	CuKeR52 aPJRN7Pf qDd	2 E S
▶ June 12th 2020, 21:23:27.954	209.165.200.227	209.165.200.235	80	FCbbST2feBG6a AYvBh	CbSK6C1 mlm2iUV KkC1	2 6 D
▶ June 12th 2020, 21:23:27.881	209.165.200.227	209.165.200.235	80	FwkDT14TJaA2Yd NQ14	CbSK6C1 mlm2iUV KkC1	2 E S
▶ June 12th 2020, 21:23:17.789	209.165.200.227	209.165.200.235	80	FWOO3T1TT34U WLKr63	CbSK6C1 mlm2iUV KkC1	2 E S
▶ June 12th 2020, 21:23:17.768	209.165.200.227	209.165.200.235	80	F37eK1464vM8lh uCoj	CbSK6C1 mlm2iUV KkC1	Y E S
▶ June 12th 2020, 21:23:17.703	209.165.200.227	209.165.200.235	80	Fkpc6a3axDrC4G BqR5	CbSK6C1 mlm2iUV KkC1	Y 6 D
▶ June 12th 2020, 21:23:17.700	209.165.200.227	209.165.200.235	80	FxF0bx16vr1YO Wulch	C2S2w31 zFlvpV63 Lp	> 6

Espandendo i log noteremo varie informazioni tra cui anche l'event_type e message.

#	destination_port	🔍 📄 🗑️ *	80
t	event_type	🔍 📄 🗑️ *	bro_http
t	host	🔍 📄 🗑️ *	d68c9360b6ae
t	ips	🔍 📄 🗑️ *	209.165.200.235, 209.165.200.227
t	message	🔍 📄 🗑️ *	{"ts":"2020-06-12T21:30:09.445030Z","uid":"CuKeR52aPjRN7PfQDd","id_h":"209.165.200.227","id.orig_p":56194,"id.resp_h":"209.165.200.235","esp_p":80,"trans_depth":1,"method":"GET","host":"209.165.200.235","mutillidae/index.php?page=user-info.php&username='+union+select+ccber,ccv,expiration,null+from+credit_cards+-+&password=&user-info-it-button=View+Account+Details","referrer":"http://209.165.200.235dae/index.php?page=user-info.php","version":"1.1","user_agent":"Mozilla (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0","request_len":0,"response_body_len":23665,"status_code":200,"status_msg":"OK","s":["HTTP::URI_Sqli"],"resp_fuids":["FEvWs63HqvCqth3LH1"],"resp_mime_s":["text/html"]}
t	method	🔍 📄 🗑️ *	GET
t	path	🔍 📄 🗑️ *	/nsm/import/bro/bro-W5Ldfbf0/http.log
t	referrer	🔍 📄 🗑️ *	http://209.165.200.235/mutillidae/index.php?page=user-info.php
#	request_body_length	🔍 📄 🗑️ *	0
t	resp_fuids	🔍 📄 🗑️ *	FEvWs63HqvCqth3LH1
t	resp_mime_types	🔍 📄 🗑️ *	text/html
#	response_body_length	🔍 📄 🗑️ *	23,665
#	source_ip_city_name	🔍 📄 🗑️ *	Monterey

Da come si può verificare all'interno del campo message si può dedurre una SQLi per recuperare informazioni di carte di credito.

Successivamente è possibile entrare più nel dettaglio del log grazie al campo _id

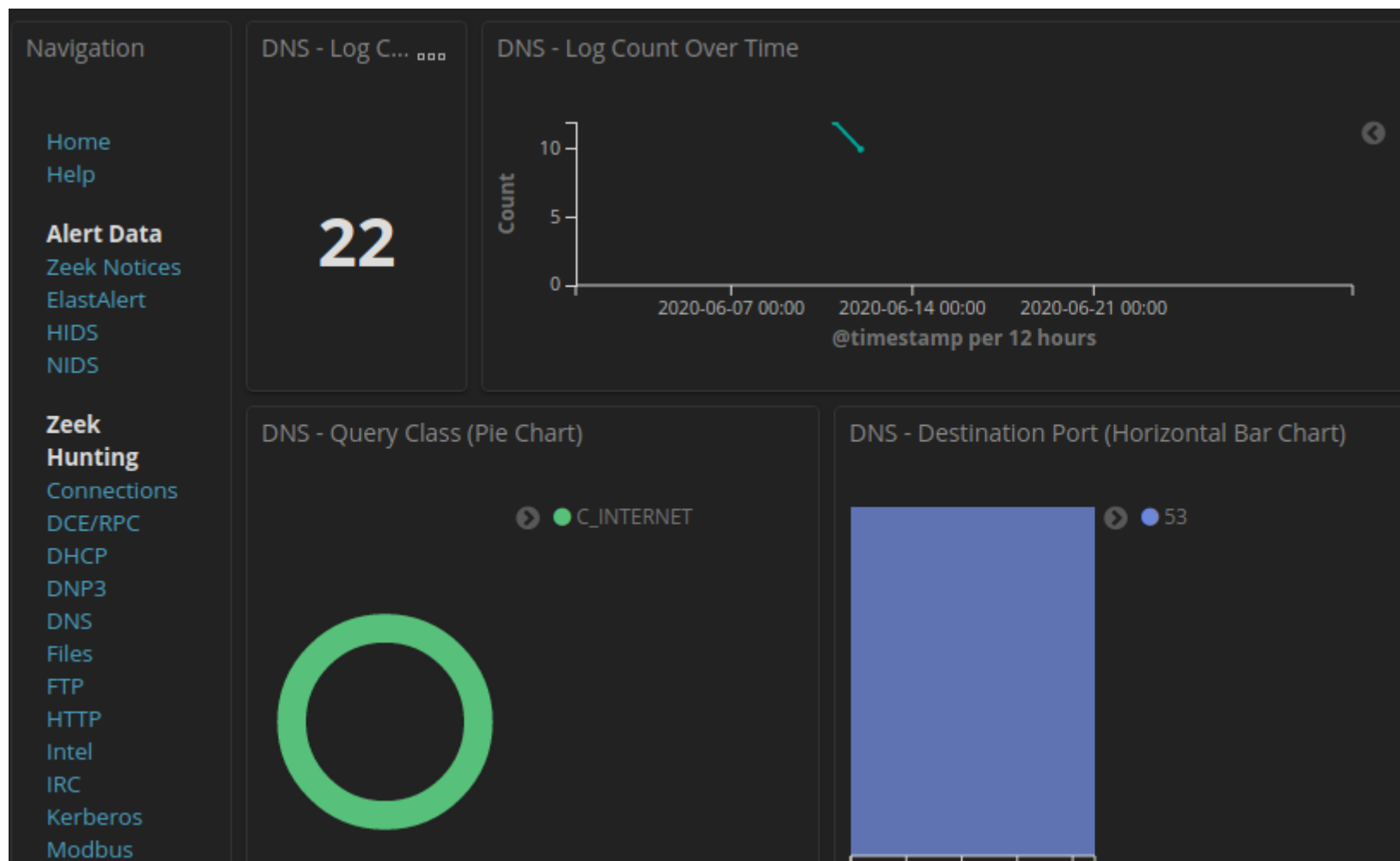
@timestamp	June 12th 2020, 21:30:09.445
@version	1
_id	ZzjrzXIBB6Cd-_0SD_iW
_index	seconion:logstash-import-2020.06.12

Il quale apre la seguente schermata che, filtrando per username, troviamo le informazioni estratte

```
DST: 17
DST: <b>Username=</b>7746536337776330<br>
DST:
DST: 17
DST: <b>Password=</b>722<br>
DST:
DST: 22
DST: <b>Signature=</b>2015-04-01<br><p>
DST:
DST: 24
DST: <b>Username=</b>8242325748474749<br>
DST:
DST: 17
DST: <b>Password=</b>461<br>
DST:
DST: 22
DST: <b>Signature=</b>2016-03-01<br><p>
DST:
DST: 24
DST: <b>Username=</b>7725653200487633<br>
DST:
DST: 17
DST: <b>Password=</b>230<br>
DST:
DST: 22
DST: <b>Signature=</b>2017-06-01<br><p>
DST:
DST: 24
```

PARTE 2

Un amministratore di rete ha notato sospette attività per quanto riguarda interrogazioni al DNS, quindi modificando il filtro su DNS possiamo iniziare ad analizzare i log.



Per effettuare una ricerca più dettagliata aggiungiamo un ulteriore filtro **example.com**

The screenshot shows the Kibana interface with a search query for **example.com**. The dashboard displays four visualizations:

- DNS - Log Count**: A large number **4** representing the total count of log entries.
- DNS - Log Count Over Time**: A line chart showing the count over time from 2020-06-07 00:00 to 2020-06-21 00:00. The y-axis is labeled 'Count' and ranges from 0 to 4. A single data point is visible at 2020-06-14 00:00 with a count of 4.
- DNS - Query Class (Pie Chart)**: A pie chart showing the distribution of query classes. A green segment represents **C_INTERNET**.
- DNS - Destination Port (Horizontal Bar Chart)**: A horizontal bar chart showing the distribution of destination ports. A blue bar represents port **53**.

The left sidebar contains navigation links: Discover, Visualize, Dashboard (selected), Timelion, Dev Tools, Management, Squert, and Logout. The top navigation bar includes links for Zeek, Full screen, Share, Clone, Edit, Documentation, Auto-refresh, and a date range selector set to June 1st 2020, 00:00:00.000 to June 30th 2020, 23:59:59.999. The bottom status bar shows the browser tab 'Zeek - DNS - Kibana - Chromium' and a page indicator '1 / 4'.

Dopo aver estratto premendo **EXPORT:RAW** in formato CSV le informazioni sospette

DNS - Queries

Query

434f4e464944454e5449414c20444f43554d454e540a444f.

484152450a5468697320646f63756d656e7420636f6e7461

666f726d6174696f6e2061626f757420746865206c617374.

697479206272656163682e0a.ns.example.com

Export:

Raw

Formatted

Eseguiamo un xxd per decodificare il CSV e rinominarlo in secret.txt e utilizziamo il cat per avere un output del file e noteremo questo risultato

```
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$ █
```