SOC Analyst Project

Blue Team

SIEM Solution:

Splunk + Boss Of The SOC (BOTS) v1 dataset

By:

Munsif Abubker Hashim

Description:

- This Project Objective is performing analysis as Blue Team Member Using Splunk as SIEM Solution for Incident Response in your Company (Wayne Enterprises) which has been hit by APT group, And Your SOC Manager tasked you with responding to this incident by heavily utilizing Splunk and all the data that it ingested which consist of Windows event logs, Sysmon logs, Fortinet next-generation firewall logs, Suricata logs, etc.
- Company Website: imreallynotbatman.com

- This Project is based on Boss Of The SOC (BOTS) v1 dataset which is released by splunk for security analysts to help them practicing.

Practice Online:

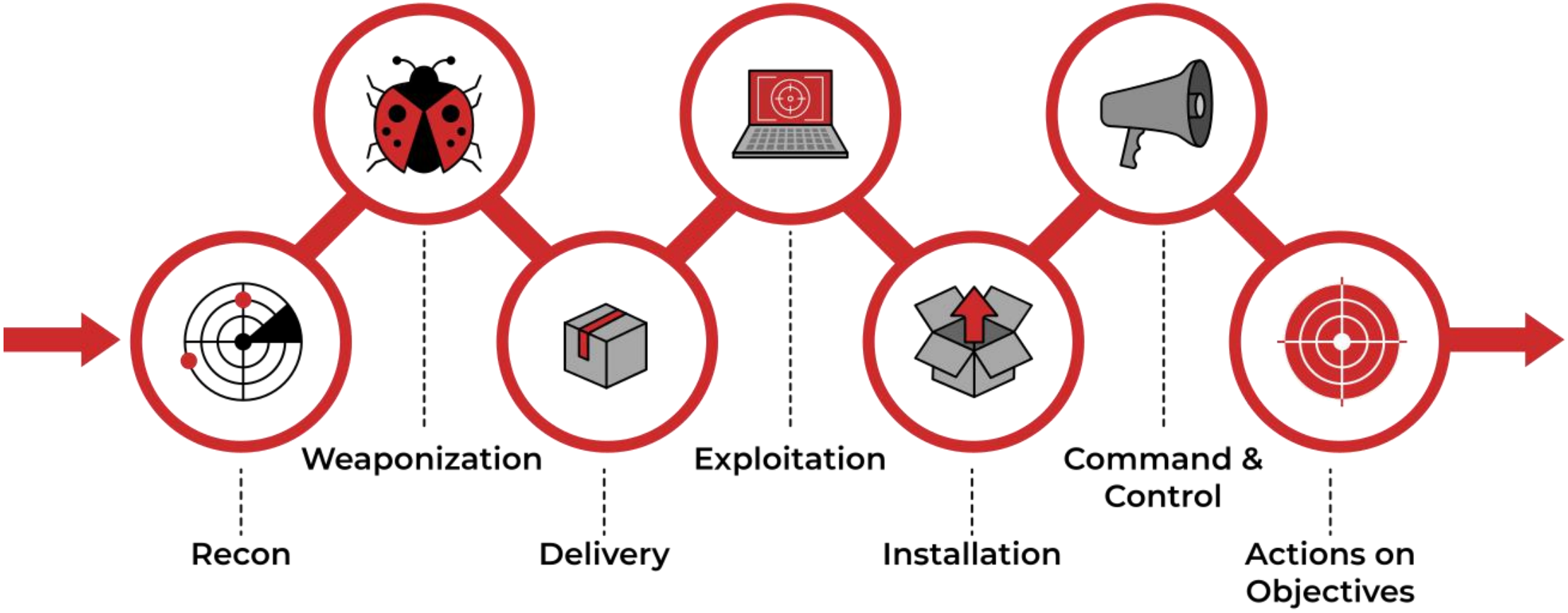
You don’t need to download Splunk & (Botsv1) Dataset

Just Visit this link and start to perform Incident Response online With Splunk:

https://splunk.samsclass.info

username : student1
password : student1

The cyber kill chain maps the stages of a cyberattack from the early **reconnaissance** stages to **data exfiltration**, help to understand and combat ransomware, security breaches, and advanced persistent attacks (**APTs**).



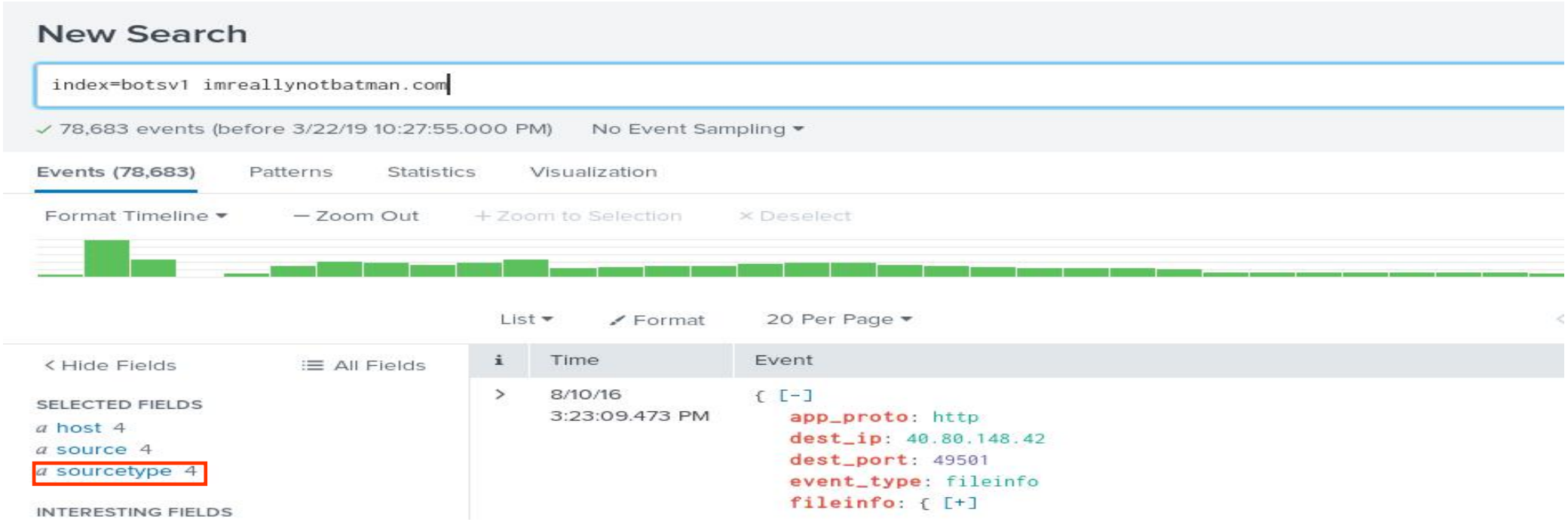
My Analysis will be performed based on Cyber Kill Chain Model.

Reconnaissance:

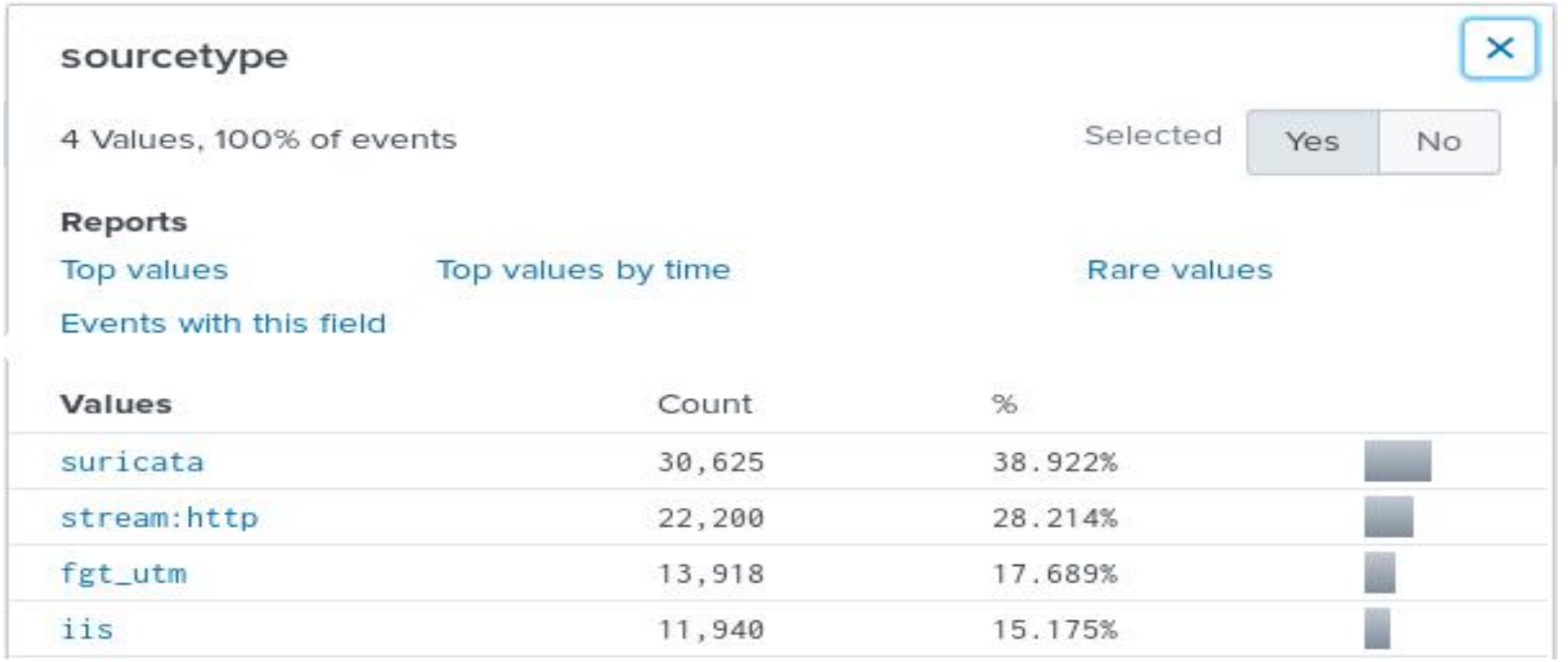
identify any reconnaissance activities performed by the APT group on organization's website: imreallynotbatman.com.

1. determine sourcetypes associated with imreallynotbatman.com

```
index=botsv1 imreallynotbatman.com
```



Reconnaissance:



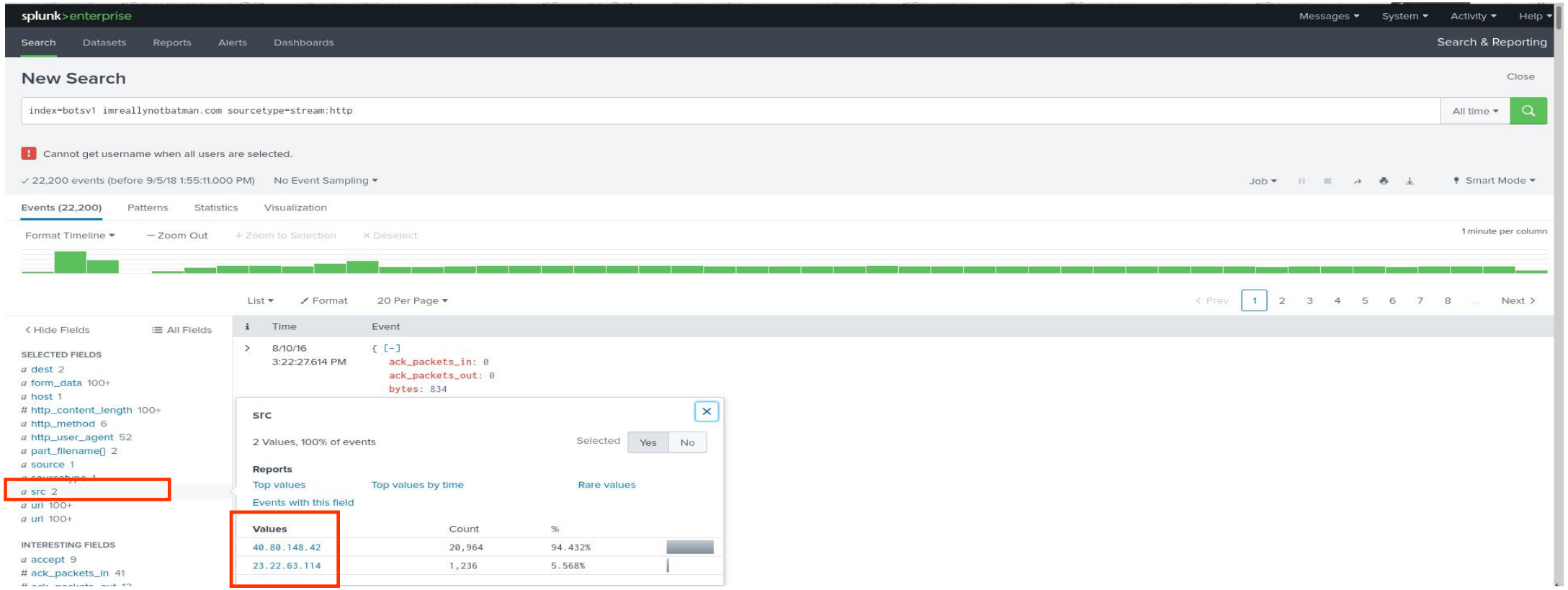
Sourcetypes related to imreallynotbatman.com are:

1. Suricata
2.HTTP Traffic
3.Fortigate Firewall
4.Windows IIS

Reconnaissance:

I will focus on stream:http sourcetype because it's HTTP traffic which related with imreallynotbatman.com

index=botsv1 imreallynotbatman.com sourcetype=stream:http



Reconnaissance:

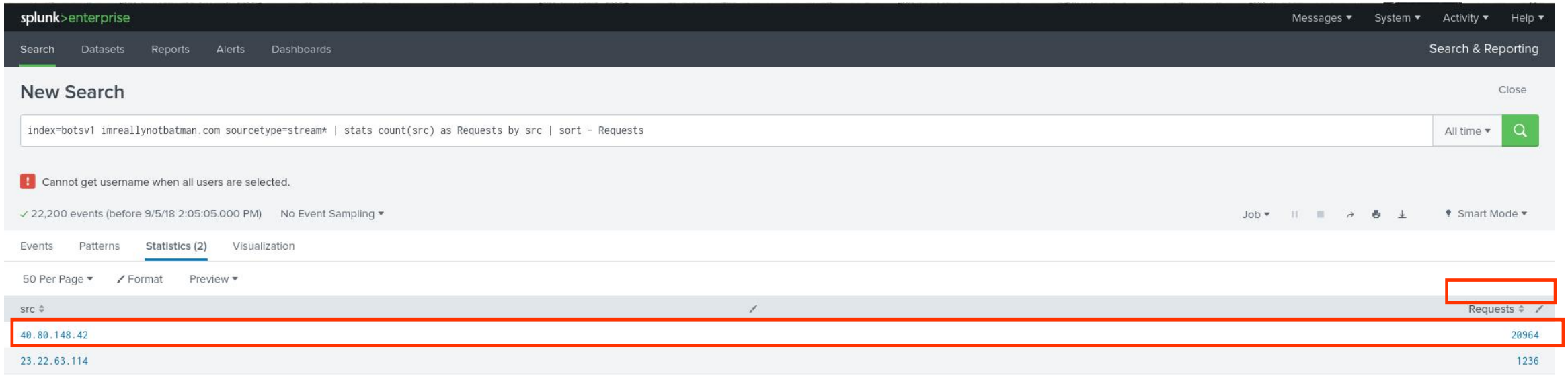
in src field i found 2 IP addresses:

40.80.148.42 ----> Most Traffic Request (95%)

23.22.63.114 (5%)

i will use another query to have better result on requests:

```
index=botsv1 imreallynotbatman.com sourcetype=stream* | stats count(src) as Requests by src | sort - Requests
```

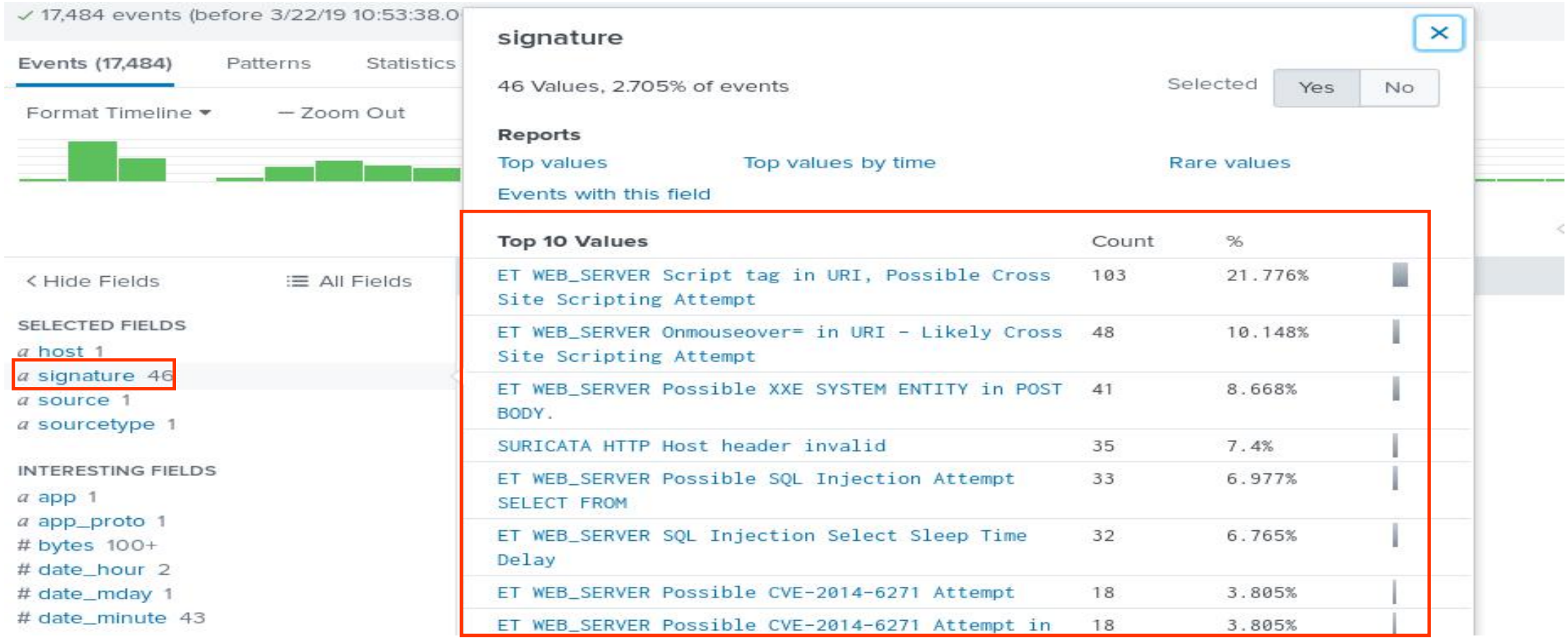


I Assumed that 40.80.148.42 is the IP that APT group used to perform reconnaissance/scanning activities , because of huge amount of traffic.

Reconnaissance:

I will use Suricata to validate that 40.80.148.42 is Malicious.(by using sourcetype=suricata)

index=botsv1 imreallynotbatman.com src=40.80.148.42 sourcetype=suricata



Reconnaissance:

from the Suricata signatures that were triggered, i found that 40.80.148.42 was actually Scanning imreallynotbatman.com for Web Vulns (XSS,XXE,SQLi,etc...).

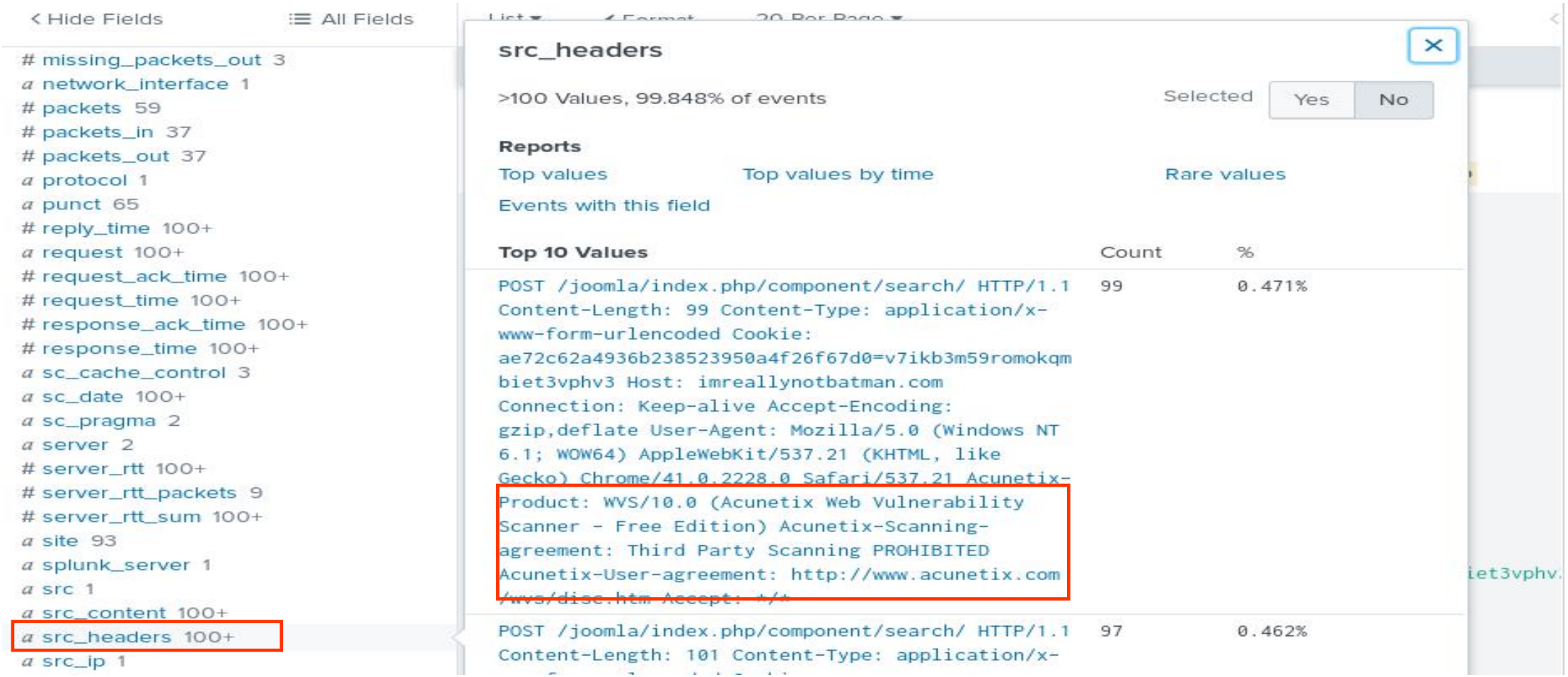
Now i will check for all HTTP traffic coming from 40.80.148.42 & know Destination IP.

```
index=botsv1 src=40.80.148.42 sourcetype=stream:http
```

Huge incoming traffic to 192.168.250.70, which mean it's Destination IP(Victom) for APT group

Reconnaissance:

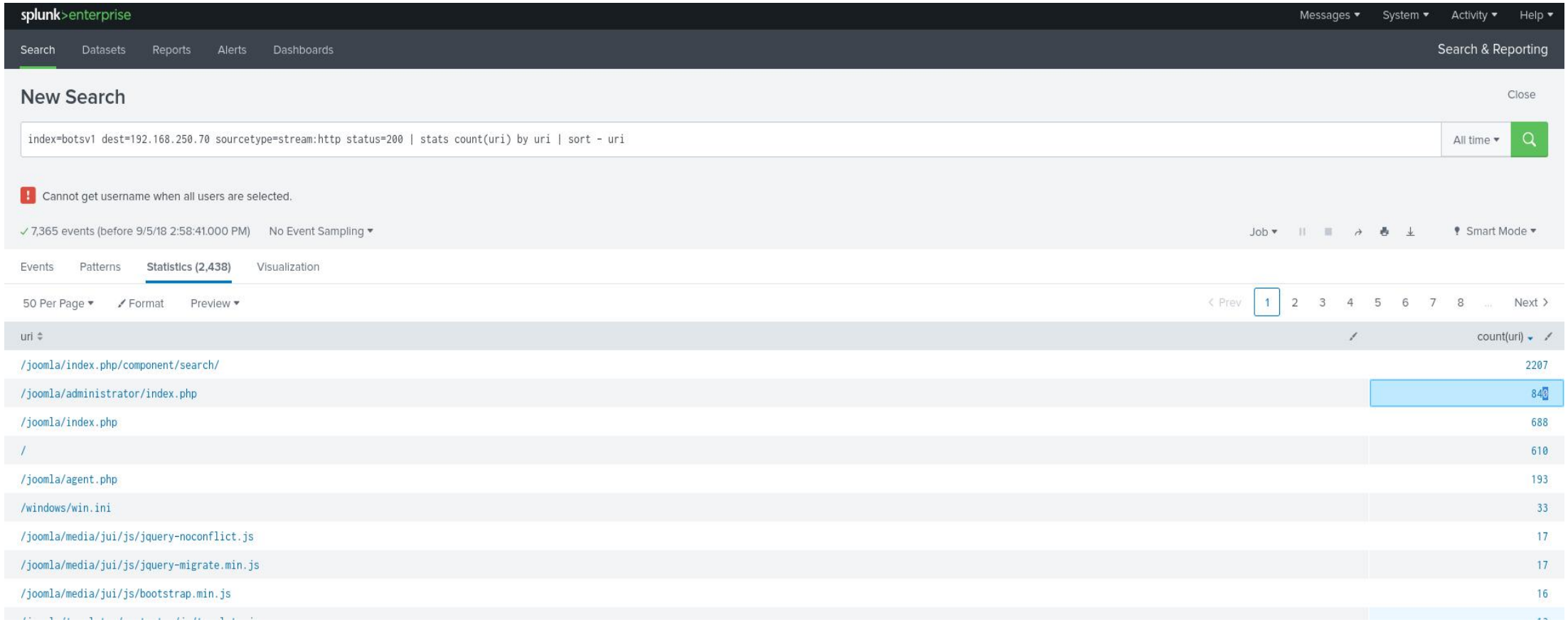
- **Also i checked HTTP Headers(src_headers) & User Agent Headers(http_user_agent) and discovered that the APT group use Acunetix vulnerability scanner.**



Reconnaissance:

Now i need to know what URLs has been requested by the APT group.

index=botsv1 dest=192.168.250.70 sourcetype=stream:http status=200 | stats count(uri) by uri | sort - uri



Reconnaissance:

- At this point i finished from Reconnaissance Stage with Good Informations:

  - Targeted IP = 192.168.250.70 -> imreallynotbatman.com
  - Attacker IP = 40.80.148.42
  - Web Vulnerability Scanners = Acunetix

Weaponization:

In Weaponization Stage analysis i will use external resources to find more info about

40.80.148.42

23.22.63.114

Resources I used:

- https://www.virustotal.com
- https://who.is
- http://www.robtex.com
- https://threatcrowd.org
- https://threatminer.com

I couldn't extract any usefull information about 40.80.148.42, But 23.22.63.114 is full of usefull information

1. Searching with https://threatcrowd.com for 23.22.63.114

Weaponization:

23.22.63.114 IP has a number of other domain names associated with it, which indicate that it's phishing domains since their name is similar to the organization (Wayne).

REVERSE DNS

Domain	Date
wayncorpinc.com	2019-03-22
waynecorinc.com	2019-03-22
waynecrpinc.com	2019-03-22
wayneorpinc.com	2019-03-22
wynecorpinc.com	2019-03-22
wanecorpinc.com	2019-03-21
23.22.63.114	2019-03-07
ec2-23-22-63-114.compute-1.amazonaws.com	2019-02-27
waynecorpnc.com	2019-01-25
po1s0n1vy.com	2018-07-09
www.po1s0n1vy.com	2018-06-24
prankglassinebracket.jumpingcrab.com	2018-05-06

Weaponization:

checking the whois information of wayncorpinc.com

IP : 23.22.63.114
IP-based Geolocation of Wayncorpinc.com : United States | Virginia
DNS Status : Online

Whois | DNS | Sites on same IP | Comments

Registrant

Name	Lillian Rose	has registred 10 domains
Organization	Toxicodendron Inc	has registred 8 domains
Email	lillian@po1s0n1vy.com	has registred 8 domains

found email address seems related with APT : lillian@po1s0nvy.com

Weaponization:

- At this point i finished from Weaponization Stage :

  - Targeted IP = 192.168.250.70 -> imreallynotbatman.com
  - Attacker IP = 40.80.148.42
  - Web Vulnerability Scanners = Acunetix

  - [+]

Malicios Domains (Phishing):

wynecorpinc.com,
wayncorpinc.com,
waynecorinc.com,
waynecrpinc.com,
wanecorpinc.com,
wayneorpinc.com,
www.po1s0n1vy.com,
po1s0nvy.com
prankglassinebracket.jumpingcrab.com

Emails:

lillian@po1s0n1vy.com

Delivery:

In Delivery Stage i used https://www.threatminer.org to know Malware informations related to IP 23.22.63.114 & I found 2 Malwares

[1] (aae3f5a29935e6abcc2c2754d12a9af0) ->

[2] (c99131e0169171935c5ac32615ed6261) -> (MirandaTateScreensaver.scr.exe)

aae3f5a29935e6abcc2c2754d12a9af0	N/A	2019-05-30 16:36:52
c99131e0169171935c5ac32615ed6261		2016-09-01 09:03:44

ALYac	Trojan.GenericKD.3470547
AVG	Agent5.APHV
AVware	Trojan.Win32.Generic!BT
Ad-Aware	Trojan.GenericKD.3470547
AegisLab	Agent5.Aphv.Gen!c
AhnLab-V3	Malware/Gen.Generic.N2081883700
Antiy-AVL	Trojan[Backdoor]/Win32.Redsip
Arcabit	Trojan.Generic.D34F4D3
Avira	TR/AD.Zupdax.qmyx

Delivery:

[1] ab.exe ---> ec78c938d8453739ca2a370b9c275971ec46caf6e479de2b2d04e97cc47fa45d

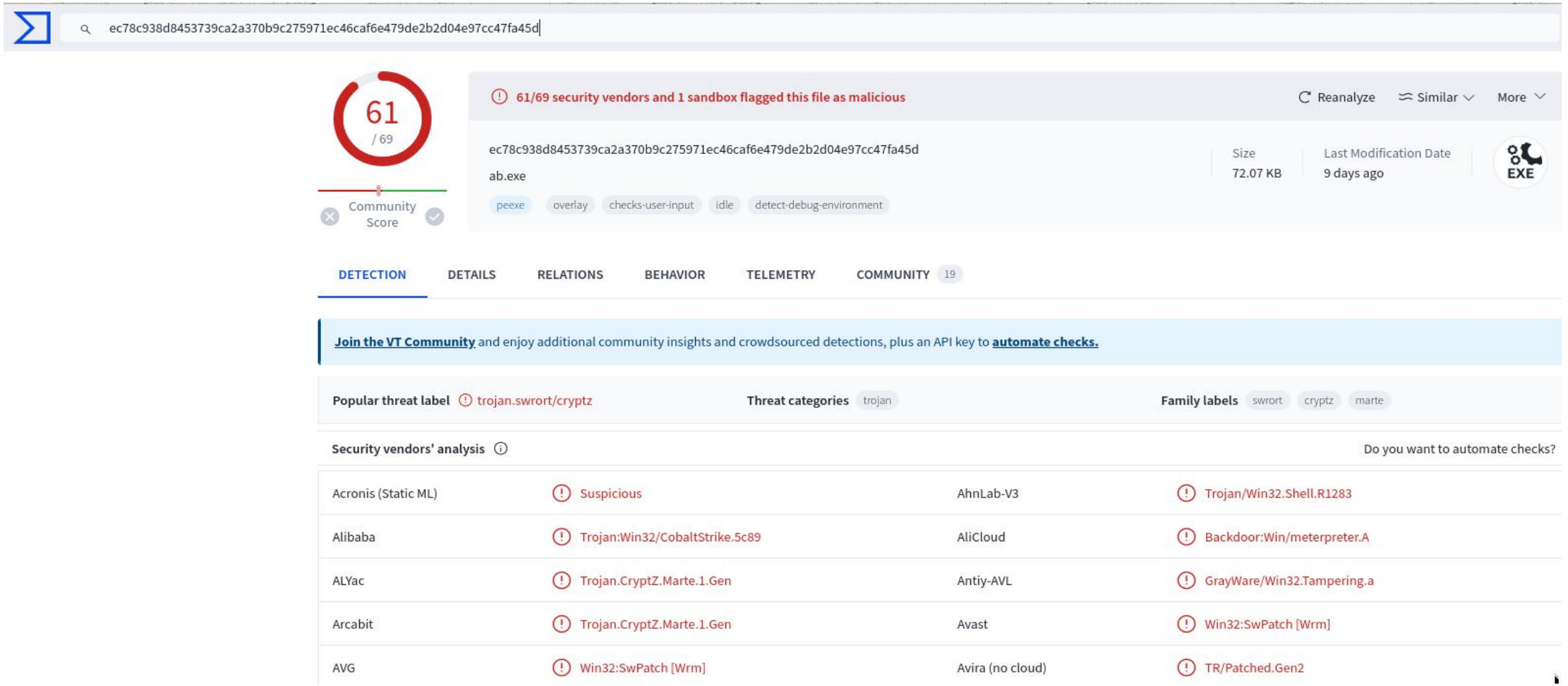
File: aae3f5a29935e6abcc2c2754d12a9af0

Metadata

File name:	ec78c938d8453739ca2a370b9c275971ec46caf6e479de2b2d04e97cc47fa45d
File type:	PE32 executable (GUI) Intel 80386, for MS Windows
File size:	73802
Analysis date:	2019-05-30 16:36:52
MD5:	aae3f5a29935e6abcc2c2754d12a9af0
SHA1:	65df73d77324d008c83c3e57b445df0fd43a3a51
SHA256:	ec78c938d8453739ca2a370b9c275971ec46caf6e479de2b2d04e97cc47fa45d
SHA512:	N/A
SSDEEP:	N/A
IMPHASH:	N/A
Authentihash:	N/A
Related resources	VirusTotal Hybrid-Analysis VirusShare

Delivery:

Checking First MD5 Hash with https://www.virustotal.com & Confirming that it's Malicious.



Delivery:

. MirandaTateScreensaver.scr.exe

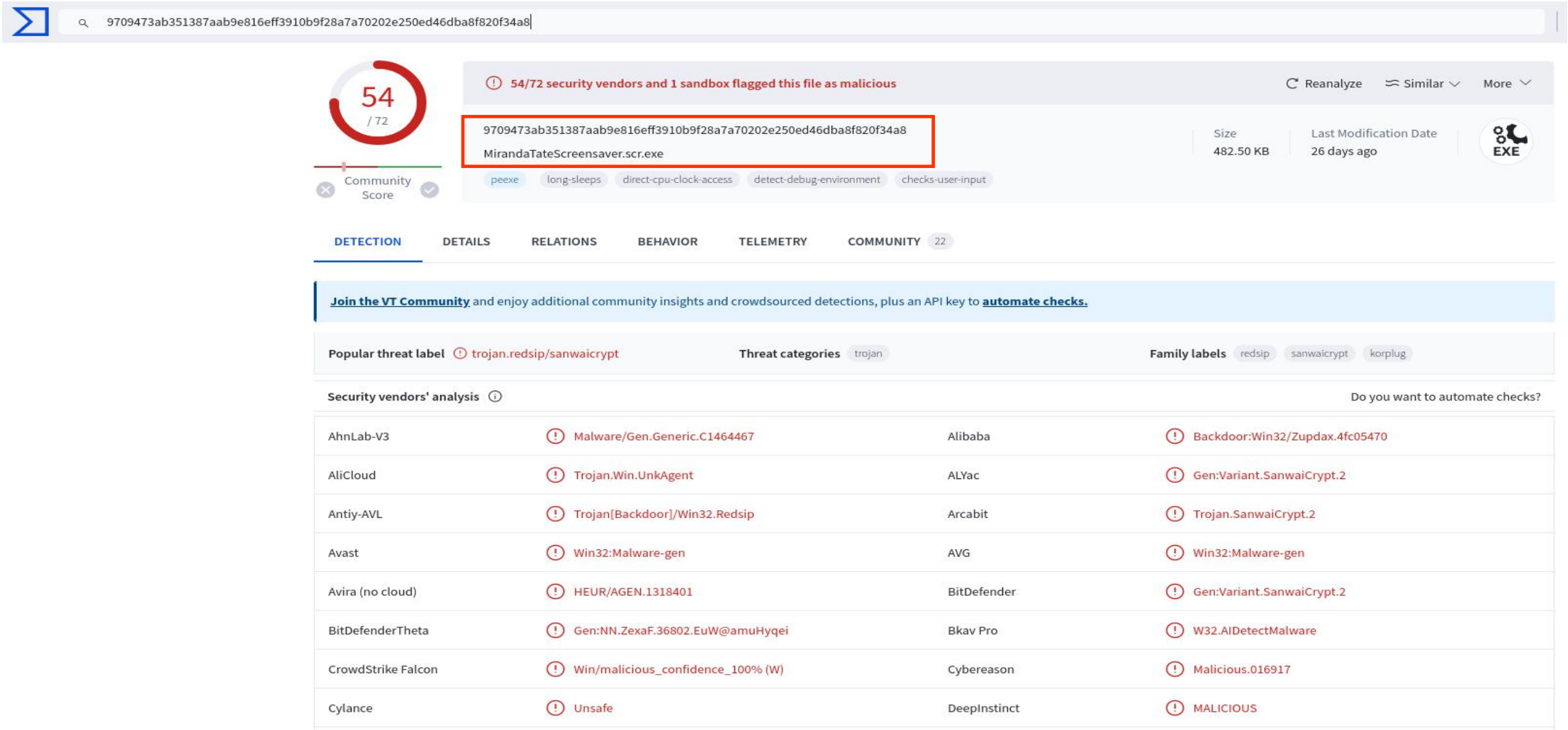
File: c99131e0169171935c5ac32615ed6261

Metadata

File name:	MirandaTateScreensaver.scr.exe
File type:	PE32 executable (console) Intel 80386, for MS Windows
File size:	494080 bytes
Analysis date:	2016-09-01 09:03:44
MD5:	c99131e0169171935c5ac32615ed6261
SHA1:	bc927ff06263351f43db8dec88e4b08485e07996
SHA256:	9709473ab351387aab9e816eff3910b9f28a7a70202e250ed46dba8f820f34a8
SHA512:	8fb3b09541b021e06eeec455876526607114adb547eacb7556d578c08959154b80f01bac905383a5eb4c8a9091a3fb14dc13badc36a05ea7718bf4b1053f2fdb
SSDEEP:	12288:JCy+DdcUrY4tO3Rc5F5H8q3/HSaRanZ0:Jj+COpO3Rc5F5H8q3/yaRaZ0
IMPHASH:	fae2c8486a11f609323cc15c0ee838cf
Authentihash:	N/A
Related resources	VirusTotal Hybrid-Analysis VirusShare

Delivery:

Checking Second MD5 Hash with https://www.virustotal.com & Confirming it's Malicious.



Delivery:

At this point i finished from Delivery Stage :

Malicious IP : 23.22.63.114

[1]

Filename: MirandaTateScreensaver.scr.exe
MD5: c99131e0169171935c5ac32615ed6261
SHA1: bc927ff06263351f43db8dec88e4b08485e07996
SHA256: 9709473ab351387aab9e816eff3910b9f28a7a70202e250ed46dba8f820f34a8

[2]

Filename: ec78c938d8453739ca2a370b9c275971ec46caf6e479de2b2d04e97cc47fa45d(ab.exe)
MD5: aae3f5a29935e6abcc2c2754d12a9af0
SHA1: 65df73d77324d008c83c3e57b445df0fd43a3a51
SHA256: ec78c938d8453739ca2a370b9c275971ec46caf6e479de2b2d04e97cc47fa45d

Exploitation:

In Exploitation Stage i will identify any exploitation activities performed on IP 192.168.250.70 By IPs [40.80.148.42][23.22.63.114].

I will check for POST Requests because attacks usually performed through POST requests.

(form_data field contains informations when dealing with POST requests)

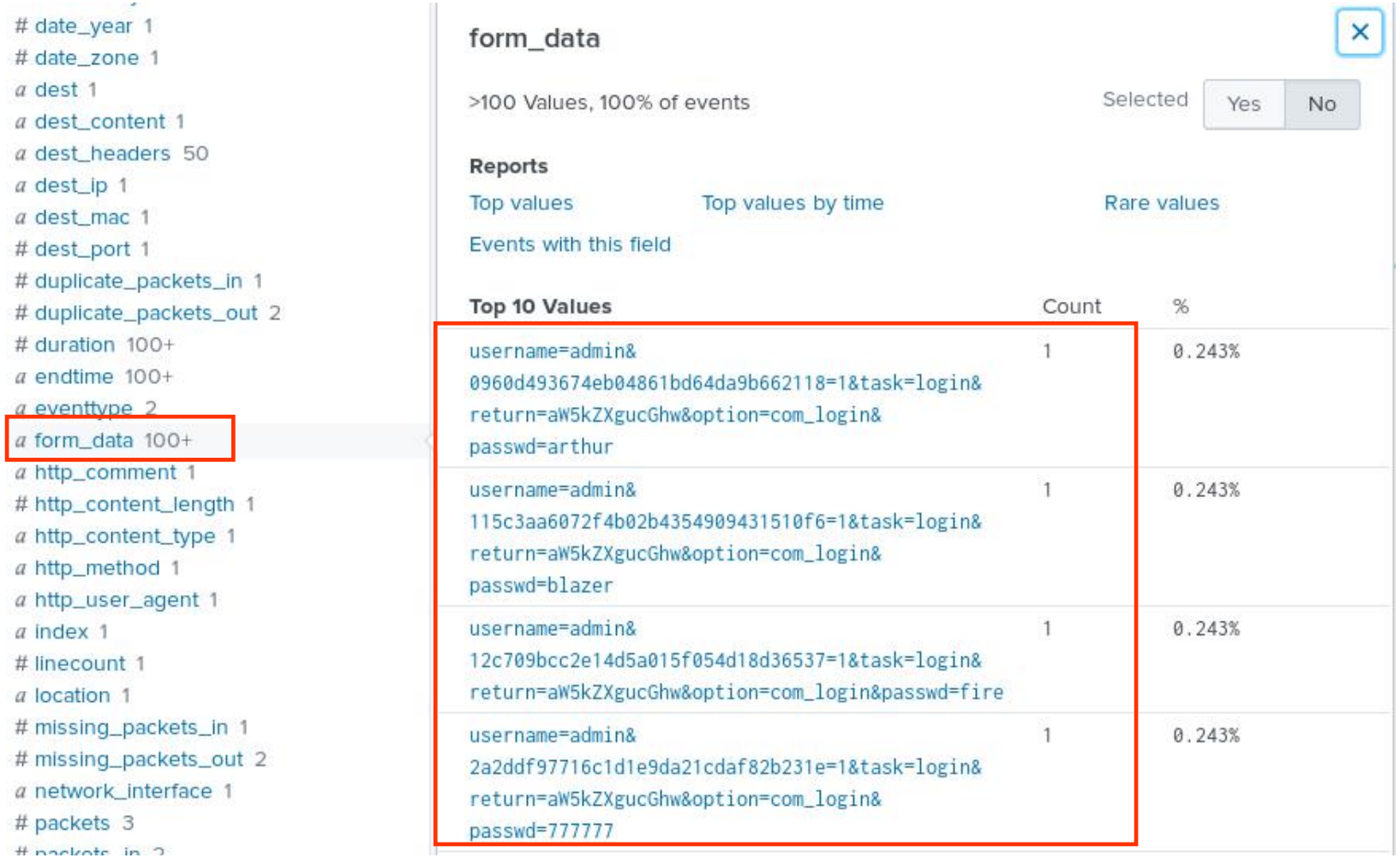
```
index=botsv1 sourcetype=stream:http dest="192.168.250.70" http_method=POST src="40.80.148.42"
```

```
index=botsv1 sourcetype=stream:http dest="192.168.250.70" http_method=POST src="23.22.63.114"
```

40.80.148.42 results bring no successfull exploitation activities.

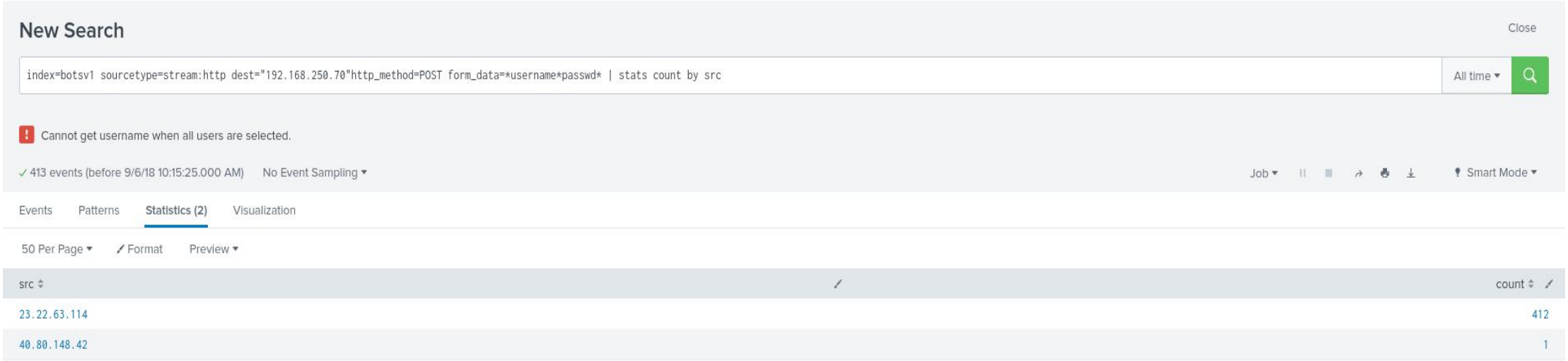
Exploitation:

23.22.63.114 is try to performing brute forcing on the web server's authentication.



Exploitation:

For more confirmation i will search with another query:

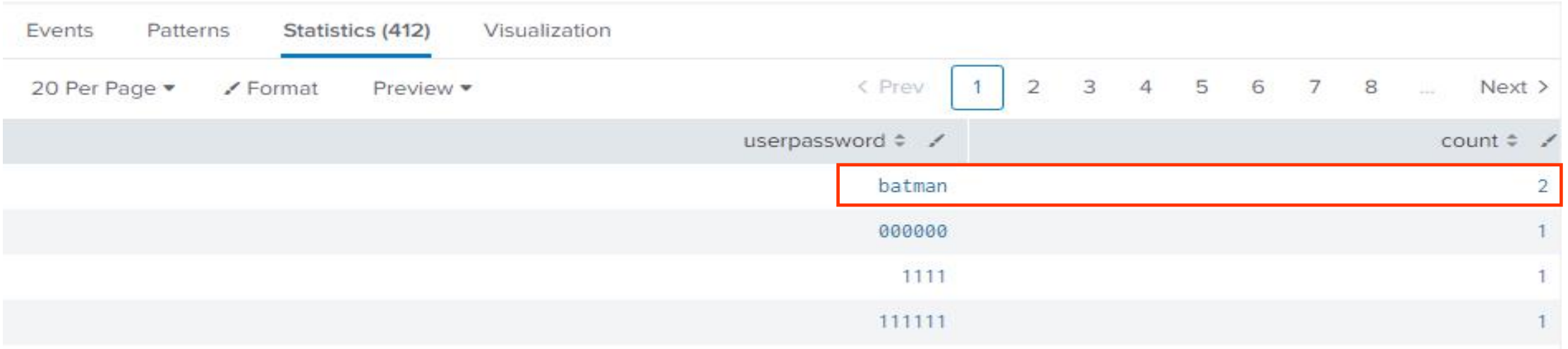


Now i will try to identify if the bruteforcing attack success, by checking Number of password used and if the password used more than one time.

if a Password used more than one time, it's good indication that the attack is success.

```
index=botsv1 sourcetype=stream:http form_data=*username*passwd*
dest_ip=192.168.250.70 | rex field=form_data "passwd=(?<userpassword>\w+)" | stats
count by userpassword | sort - count
```

Exploitation:



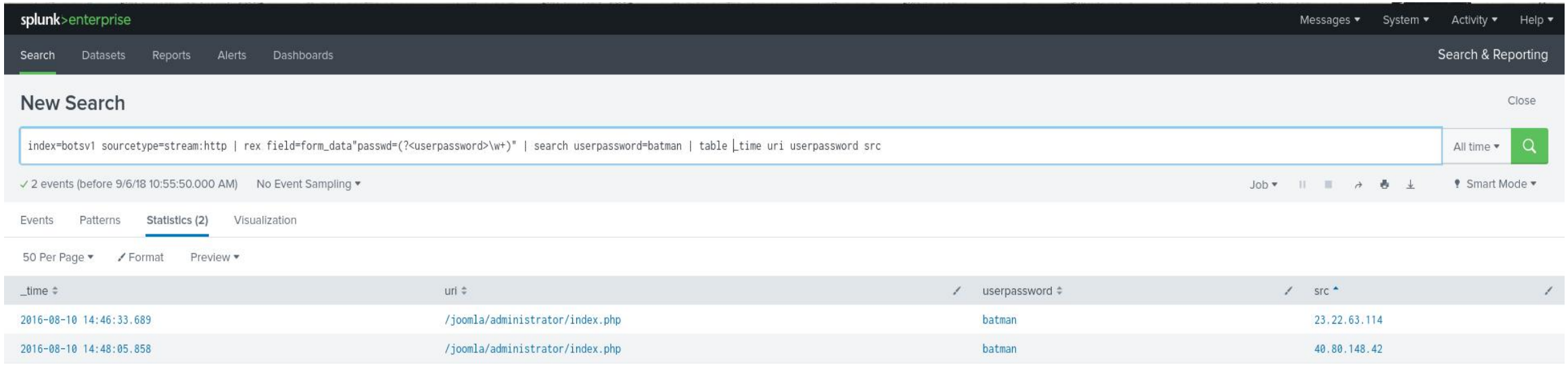
I have found that password"batman" is used 2 times.

Now i will answer these simple questiones about password "batman":
1. when the password is used?
2. what URI was targeted?
3. what IP address made the request?

All answers of these questions will be in one search Query.

Exploitation:

```
index=botsv1 sourcetype=stream:http | rexfield=form_data"passwd=(?<userpassword>\w+)"
search userpassword=batman | table _time uri userpassword src
```



From these Results i figured out that APT Group Success Finding correct password and Logged In Successfully with IP 40.80.148.42.

While Performing the Attack with IP 23.22.63.114.

Exploitation:

At this point i finished from Exploitation Stage :

Successfull Brute Force Attack.

IP Perform Brute Force : 23.22.63.114

IP Gain Access: 40.80.148.42

Tartget IP: 192.168.250.70

Password : batman

URI : /joomla/administrator/index.php

Time:

2016-08-10 14:46:33 ---> 23.22.63.114

2016-08-10 14:48:05 ---> 40.80.148.42

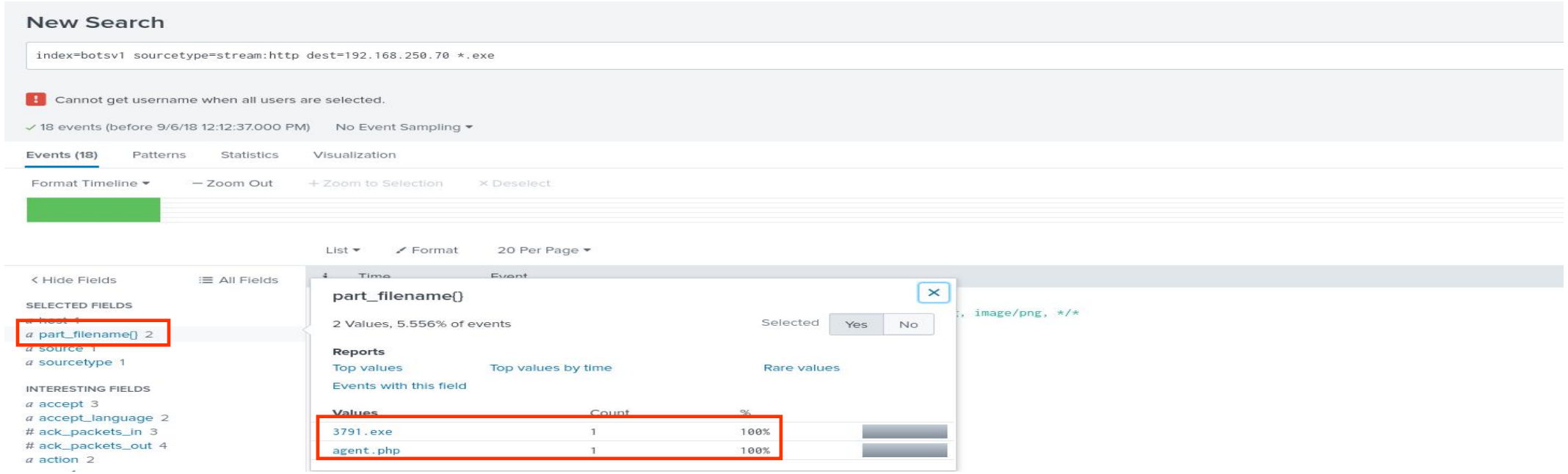
Installation:

In Installation Stage i will check for any malwares being uploaded after Exploitation.

i will search for any ".exe" programs with HTTP traffic & Suricata For IP 192.168.250.70

1. Search HTTP Traffic & check part_filename{} field which contains informations about files in HTTP traffic.

```
index=botsv1 sourcetype=stream:http dest="192.168.250.70" *.exe src=40.80.148.42
```



Installation:

i found file named “3791.exe” .

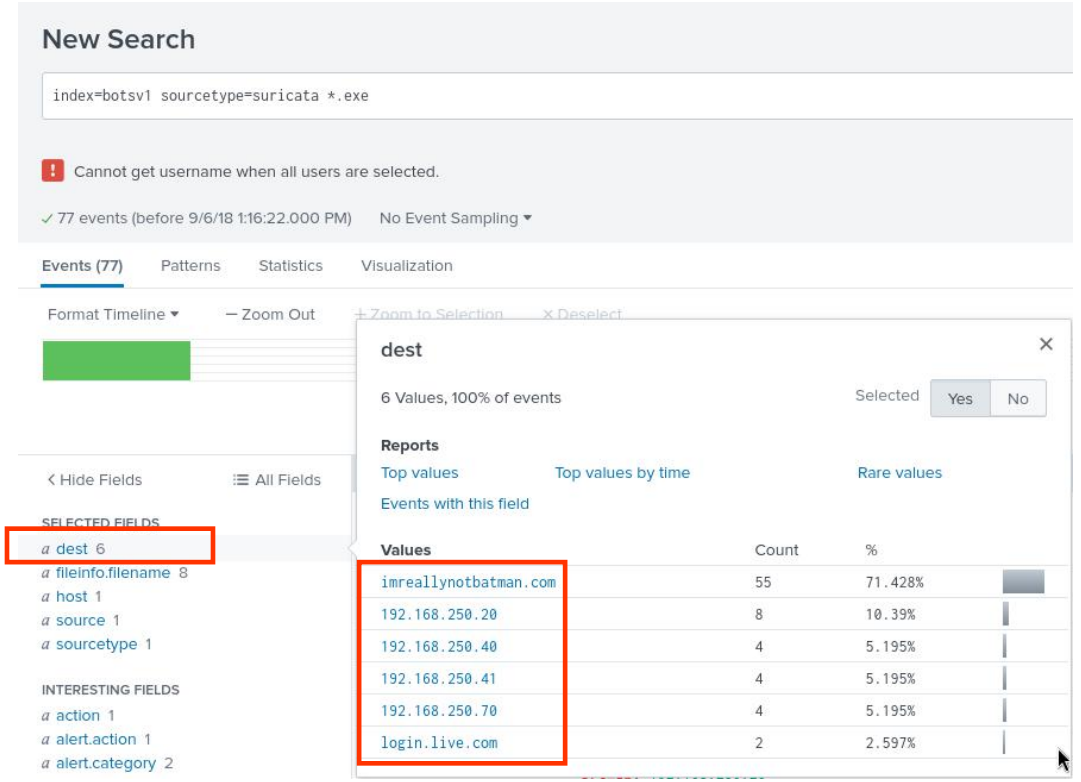
2. Search Suricata for any “.exe” files & Destination addresses.

```
index=botsv1 sourcetype=suricata *.exe
```

dest filed shows that there is multiple destinations and i’m interesting in two of them:

1. imreallynotbatman.com
2. 192.168.250.70

So I will search for these two address.



Installation:

3. Search with Suricata & check fileinfo.filename field which contains informations about files in Suricata.

```
index=botsv1 sourcetype=suricata (dest=imreallynotbatman.com OR dest="192.168.250.70")
http.http_method=POST .exe
```

I found the file "3791.exe" again and it's properly the Uploaded file.

Installation:

4. Check the Source from where the file was uploaded :

```
index=botsv1 sourcetype=suricata dest_ip="192.168.250.70" http.http_method=POST .exe
```

40.80.148.42 is the IP upload "3791.exe" file.

Now it's time to use Sysmon since it logs information such as MD5, SHA1, SHA256 hashes of files.

Installation:

Sysmon sourcetype is "XmlWinEventLog:Microsoft-Windows-Sysmon/Operational".

Important fields related to Sysmon Are:

1. ParentCommandLine
2. CommandLine
3. EventCode (Code 1 = Process Creation)
4. Hashes
5. Image

Search for "3791.exe" in Sysmon Logs :

```
index=botsv1 3791.exe sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational"
EventCode=1 | table hashes dest
```

I will search for Hashes related with "3791.exe" Online or check Hashes i obtained from Delivery Stage.

Installation:

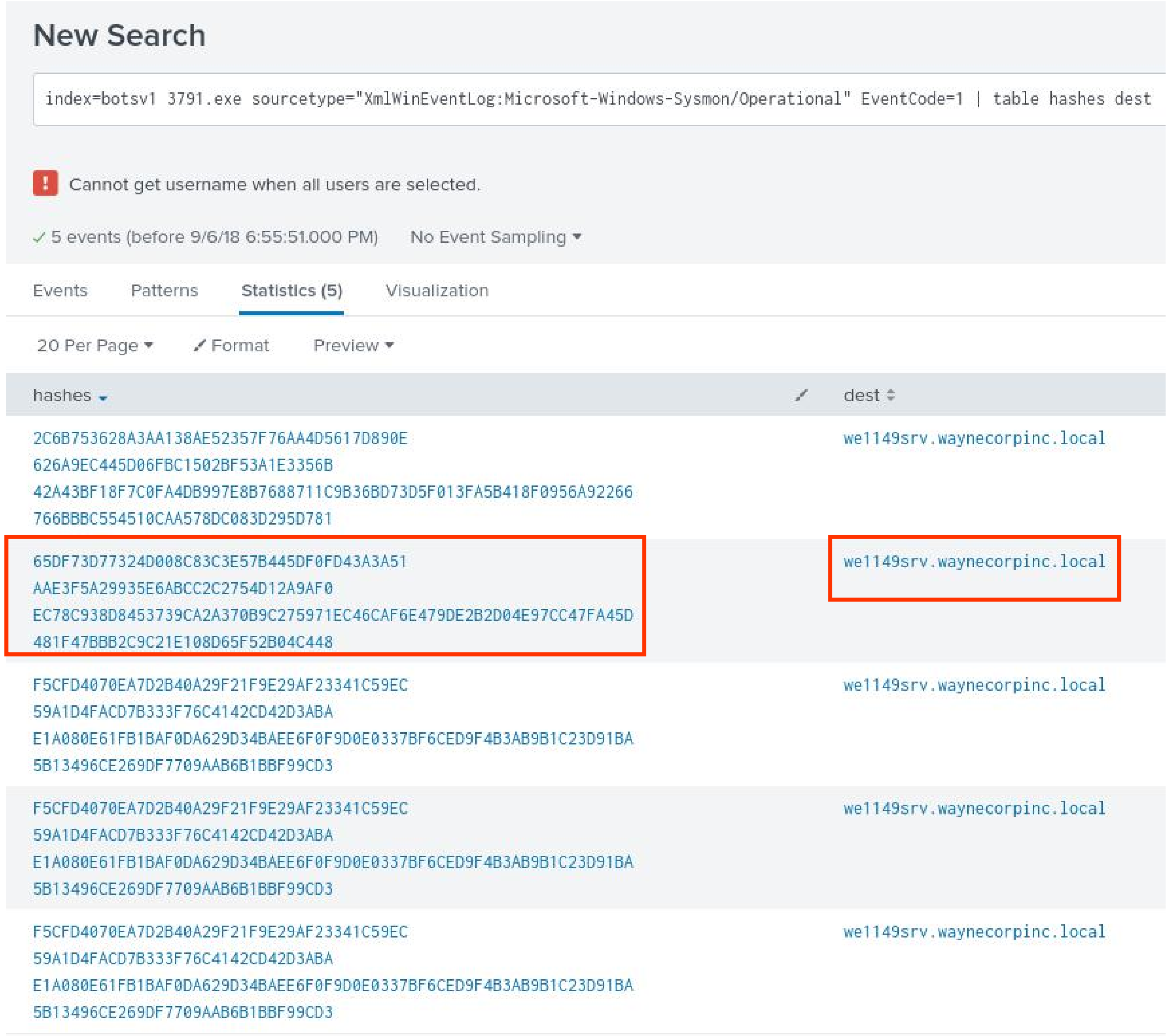
MD5 (aae3f5a29935e6abcc2c2754d12a9af0),

SHA1(65df73d77324d008c83c3e57b445df0f d43a3a51),

SHA256(ec78c938d8453739ca2a370b9c2759 71ec46caf6e479de2b2d04e97cc47fa45d)

All Hashes Above related to APT Group As I See earlier in Delivery Stage.

And Targeted Host is we1149srv.waynecorpinc.local



Installation:

At this point i finished from Installation Stage :

Successfull Installation Malware on we1149srv.waynecorpinc.local

Hostname: we1149srv.waynecorpinc.local

Program Name: 3791.exe

MD5: aae3f5a29935e6abcc2c2754d12a9af0

SHA1: 65df73d77324d008c83c3e57b445df0fd43a3a51

SHA256: ec78c938d8453739ca2a370b9c275971ec46caf6e479de2b2d04e97cc47fa45d

Command and Control:

In "Command & Control" Stage i will identify which (Server,Domain,IP) used for Command And Control by searching DNS traffic for IPs (40.80.148.42),(23.22.63.114).

DNS sourcetype is stream:dns

```
index=botsv1 sourcetype=stream:dns answer=40.80.148.42
```

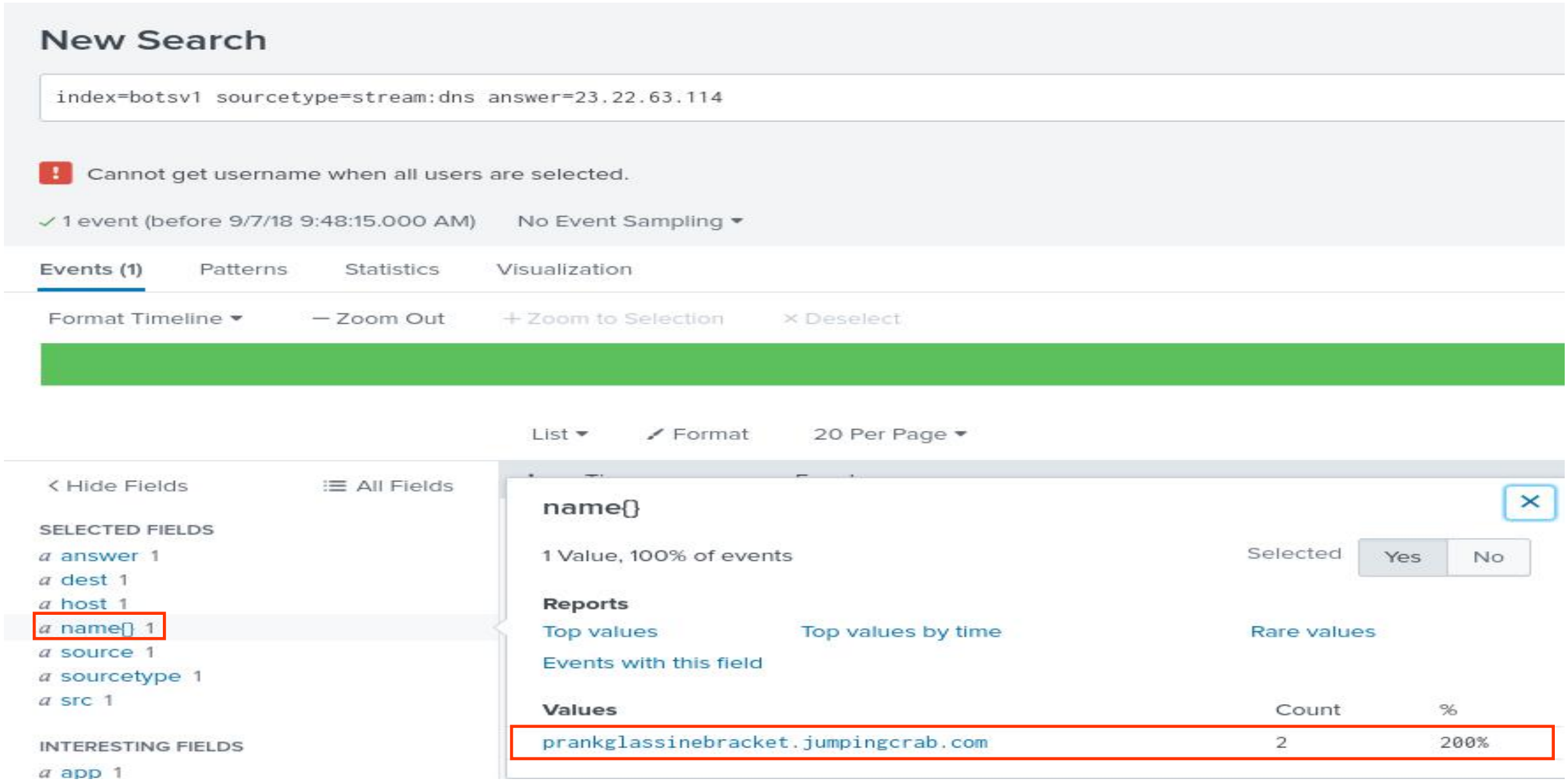
Search didn't bring any thing, i will look for other IP.

```
index=botsv1 sourcetype=stream:dns answer=23.22.63.114
```

Important Fileds in DNS:

1. name{}
2. answer

Command and Control:



Command and Control:

The Domain "prankglassinebracket.jumpingcrab.com" I found in the Weaponization phase was associated with an IP (23.22.63.114) with multiple other domains used by the attackers.

At this point i finished from Command & Control Stage :

Domain: prankglassinebracket.jumpingcrab.com
IP: 23.22.63.114

Command and Control:

The Domain "prankglassinebracket.jumpingcrab.com" I found in the Weaponization phase was associated with an IP (23.22.63.114) with multiple other domains used by the attackers.

At this point i finished from Command & Control Stage :

Domain: prankglassinebracket.jumpingcrab.com
IP: 23.22.63.114

Lesson Learned:

As My First Project as SOC Analyst I Learned:

1. Analyze Logs/Data From different Resources Using SIEM Solutions.
2. Dealing with Splunk (Searching & Reporting).
3. Using Open Source Intelligence (OSINT) to help identify more informations.
4. Analyze Incidents Based on Cyber Kill Chain Model.
5. Simulating the Process of Incident Responding in real life.
6. More Experience.

Social Media:

LinkedIn: https://www.linkedin.com/in/munsif1

Meduim: https://medium.com/@Munsif1


FOLLOW YOUR
DREAMS