

# **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](http://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**

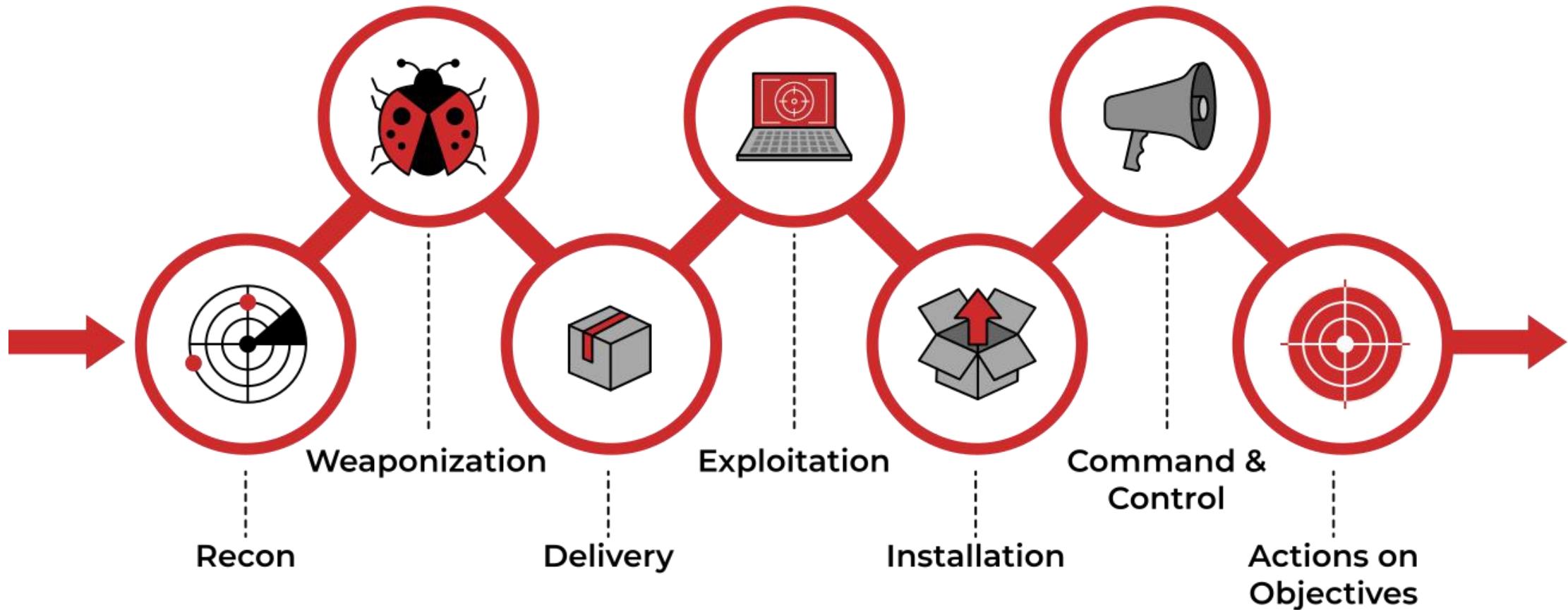
**Just Visit this link and start to perform Incident Response online With **Splunk**:**

**<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](http://imreallynotbatman.com).

## 1. determine sourcetypes associated with [imreallynotbatman.com](http://imreallynotbatman.com)

**index=botsv1 imreallynotbatman.com**

New Search

index=botsv1 imreallynotbatman.com

✓ 78,683 events (before 3/22/19 10:27:55.000 PM) No Event Sampling ▾

Events (78,683) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect

List ▾ ✎ Format 20 Per Page ▾

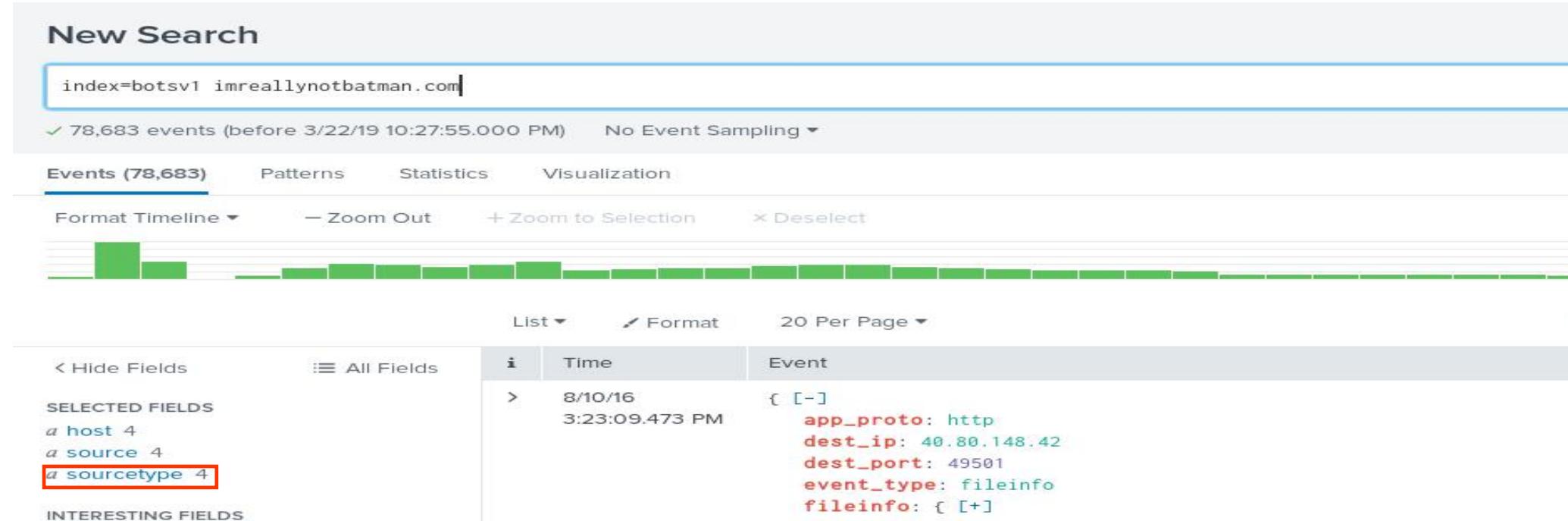
i	Time	Event
>	8/10/16 3:23:09.473 PM	{ [-] app_proto: http dest_ip: 40.80.148.42 dest_port: 49501 event_type: fileinfo fileinfo: { [+]

< Hide Fields All Fields

SELECTED FIELDS

a host 4  
a source 4  
a sourcetype 4

INTERESTING FIELDS



# 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**

The screenshot shows a Splunk Enterprise search interface. The search bar contains the query: `index=botsv1 imreallynotbatman.com sourcetype=stream:http`. The search results show 22,200 events from 8/10/16 at 3:22:27.614 PM. The timeline at the bottom indicates 1 minute per column. The event list table has columns for Time, Event, and a context menu icon. One event is selected, showing details: `{ [-] ack_packets_in: 0 ack_packets_out: 0 bytes: 834`. A modal window titled "SRC" is open, showing "2 Values, 100% of events" with "Selected Yes" and "No". The modal also includes tabs for "Reports", "Top values", "Top values by time", and "Rare values", and a section for "Events with this field". Two values are listed: `40.80.148.42` and `23.22.63.114`. The left sidebar lists "SELECTED FIELDS" including `a dest 2`, `a form_data 100+`, `a host 1`, `# http_content_length 100+`, `a http_method 6`, `a http_user_agent 52`, `a part_filename[] 2`, `a source 1`, `# sourcetype 1`, `a src 2`, `a uri 100+`, and `a url 100+`. The "INTERESTING FIELDS" sidebar includes `a accept 9`, `# ack_packets_in 41`, and `# ack_packets_out 12`.

Values	Count	%
<code>40.80.148.42</code>	20,964	94.432%
<code>23.22.63.114</code>	1,236	5.568%

# Reconnaissance:

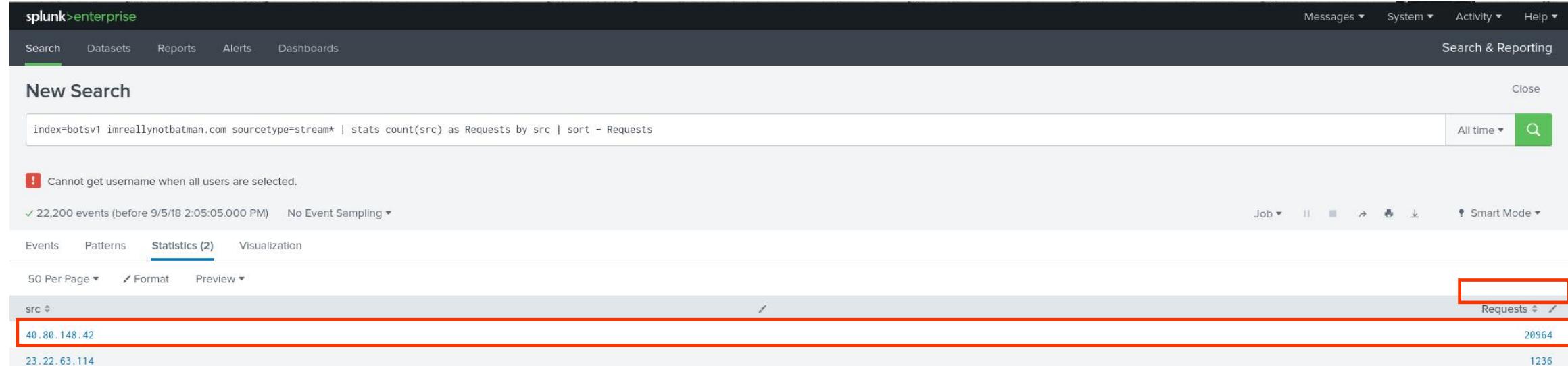
in **src** field i found 2 IP addresses:

**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**

The screenshot shows a Splunk search interface with the following details:

- Events (17,484)**: The total number of events found.
- signature**: The selected field for analysis.
- 46 Values, 2.705% of events**: The count and percentage of events containing the signature field.
- Reports**: Options to view **Top values**, **Top values by time**, and **Rare values**.
- Top 10 Values** table (highlighted with a red border):

Value	Count	%
ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt	103	21.776%
ET WEB_SERVER Onmouseover= in URI - Likely Cross Site Scripting Attempt	48	10.148%
ET WEB_SERVER Possible XXE SYSTEM ENTITY in POST BODY.	41	8.668%
SURICATA HTTP Host header invalid	35	7.4%
ET WEB_SERVER Possible SQL Injection Attempt SELECT FROM	33	6.977%
ET WEB_SERVER SQL Injection Select Sleep Time Delay	32	6.765%
ET WEB_SERVER Possible CVE-2014-6271 Attempt	18	3.805%
ET WEB_SERVER Possible CVE-2014-6271 Attempt in	18	3.805%
- SELECTED FIELDS**: A list of selected fields: **a host** 1, **a signature** 46 (highlighted with a red box), **a source** 1, **a sourcetype** 1.
- INTERESTING FIELDS**: A list of interesting fields: **a app** 1, **a app\_proto** 1, **# bytes** 100+, **# date\_hour** 2, **# date\_mday** 1, **# date\_minute** 43.

# 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.

The screenshot shows a Splunk search interface with a sidebar of available fields and a main panel for the 'src\_headers' field. The main panel includes sections for Reports, Top 10 Values, and a detailed view of the top value.

**Available Fields:**

- # missing\_packets\_out 3
- a network\_interface 1
- # packets 59
- # packets\_in 37
- # packets\_out 37
- a protocol 1
- a punct 65
- # reply\_time 100+
- a request 100+
- # request\_ack\_time 100+
- # request\_time 100+
- # response\_ack\_time 100+
- # response\_time 100+
- a sc\_cache\_control 3
- a sc\_date 100+
- a sc\_pragma 2
- a server 2
- # server\_rtt 100+
- # server\_rtt\_packets 9
- # server\_rtt\_sum 100+
- a site 93
- a splunk\_server 1
- a src 1
- a src\_content 100+
- a src\_headers 100+ (highlighted)**
- a src\_ip 1

**src\_headers Analysis:**

**Reports:** Shows Top values, Top values by time, and Rare values. The Events with this field section lists the top 10 values.

**Top 10 Values:**

Value	Count	%
POST /joomla/index.php/component/search/ HTTP/1.1	99	0.471%
Content-Length: 99 Content-Type: application/x-www-form-urlencoded		
Cookie: ae72c62a4936b238523950a4f26f67d0=v7ikb3m59romokqm		
biet3vphv3 Host: imreallynotbatman.com		
Connection: Keep-alive Accept-Encoding: gzip, deflate		
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21 Acunetix-		
Product: WVS/10.0 (Acunetix Web Vulnerability Scanner - Free Edition) Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED		
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm		
Accept: */*		

The last three rows of the table are highlighted with a red box.

# 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
```

splunk>enterprise

Messages ▾ System ▾ Activity ▾ Help ▾

Search Datasets Reports Alerts Dashboards Search & Reporting

New Search Close

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

! Cannot get username when all users are selected.

✓ 7,365 events (before 9/5/18 2:58:41.000 PM) No Event Sampling ▾ Job ▾

Events Patterns Statistics (2,438) Visualization

50 Per Page ▾ 1 2 3 4 5 6 7 8 ... Next >

uri	count(uri)
/joomla/index.php/component/search/	2207
/joomla/administrator/index.php	840
/joomla/index.php	688
/	610
/joomla/agent.php	193
/windows/win.ini	33
/joomla/media/jui/js/jquery-noconflict.js	17
/joomla/media/jui/js/jquery-migrate.min.js	17
/joomla/media/jui/js/bootstrap.min.js	16

# 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
polson1vy.com	2018-07-09
www.polson1vy.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 registered 10 domains
Organization	Toxicodendron Inc	has registered 8 domains
Email	<b>lillian@po1s0n1vy.com</b>	has registered 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**
- **[+]**

## Malicious Domains (Phishing):

**wynecorpinc.com,**  
**wayncorpinc.com,**  
**wayneccorinc.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:	<b>aae3f5a29935e6abcc2c2754d12a9af0</b>
SHA1:	65df73d77324d008c83c3e57b445df0fd43a3a51
SHA256:	ec78c938d8453739ca2a370b9c275971ec46caf6e479de2b2d04e97cc47fa45d
SHA512:	N/A
SSDEEP:	N/A
IMPHASH:	N/A
Authentihash:	N/A
Related resources	<a href="#">VirusTotal</a> <a href="#">Hybrid-Analysis</a> <a href="#">VirusShare</a>

# Delivery:

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

Σ  ec78c938d8453739ca2a370b9c275971ec46caf6e479de2b2d04e97cc47fa45d

61 / 69

Community Score

! 61/69 security vendors and 1 sandbox flagged this file as malicious

Reanalyze Similar More

ec78c938d8453739ca2a370b9c275971ec46caf6e479de2b2d04e97cc47fa45d  
ab.exe

Size 72.07 KB Last Modification Date 9 days ago EXE

peexe overlay checks-user-input idle detect-debug-environment

DETECTION DETAILS RELATIONS BEHAVIOR TELEMETRY COMMUNITY 19

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label ! trojan.swrort/cryptz Threat categories trojan Family labels swrort cryptz marte

Security vendors' analysis ⓘ Do you want to automate checks?

Acronis (Static ML)	! Suspicious	AhnLab-V3	! Trojan/Win32.Shell.R1283
Alibaba	! Trojan:Win32/CobaltStrike.5c89	AliCloud	! Backdoor:Win/meterpreter.A
ALYac	! Trojan.CryptZ.Marte.1.Gen	Antiy-AVL	! GrayWare/Win32.Tampering.a
Arcabit	! Trojan.CryptZ.Marte.1.Gen	Avast	! Win32:SwPatch [Wrm]
AVG	! Win32:SwPatch [Wrm]	Avira (no cloud)	! TR/Patched.Gen2

# 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:	8fb3b09541b021e06eec455876526607114adb547eacb7556d578c08959154b80f01bac905383a5eb4c8a9091a3fb14dc13badc36a05ea7718bf4b1053f2fdb
SSDEEP:	12288:JCy+DdcUrYtO3Rc5F5H8q3/HSaRanZ0:Jj+COpO3Rc5F5H8q3/yaRaZ0
IMPHASH:	fae2c8486a11f609323cc15c0ee838cf
Authentihash:	N/A
Related resources	<a href="#">VirusTotal</a> <a href="#">Hybrid-Analysis</a> <a href="#">VirusShare</a>

# Delivery:

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

Σ  9709473ab351387aab9e816eff3910b9f28a7a70202e250ed46dba8f820f34a8

54 / 72

Community Score

① 54/72 security vendors and 1 sandbox flagged this file as malicious

9709473ab351387aab9e816eff3910b9f28a7a70202e250ed46dba8f820f34a8  
MirandaTateScreensaver.scr.exe

peexe long-sleeps direct-cpu-clock-access detect-debug-environment checks-user-input

Size 482.50 KB Last Modification Date 26 days ago EXE

DET ECTION DETAILS RELATIONS BEHAVIOR TELEMETRY COMMUNITY 22

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label ① trojan.redsip/sanwaicrypt Threat categories trojan Family labels redsip sanwaicrypt korplug

Security vendors' analysis	Do you want to automate checks?		
AhnLab-V3	① Malware/Gen.Generic.C1464467	Alibaba	① Backdoor:Win32/Zupdax.4fc05470
AliCloud	① Trojan.Win.UnkAgent	ALYac	① Gen:Variant.SanwaiCrypt.2
Antiy-AVL	① Trojan[Backdoor]/Win32.Redsip	Arcabit	① Trojan.SanwaiCrypt.2
Avast	① Win32:Malware-gen	AVG	① Win32:Malware-gen
Avira (no cloud)	① HEUR/AGEN.1318401	BitDefender	① Gen:Variant.SanwaiCrypt.2
BitDefenderTheta	① Gen>NN.Zexaf.36802.EuW@amuHyqei	Bkav Pro	① W32.AIDetectMalware
CrowdStrike Falcon	① Win/malicious_confidence_100% (W)	Cybereason	① Malicious.016917
Cylance	① Unsafe	DeepInstinct	① 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 trying to perform brute forcing on the web server's authentication.

```
# date_year 1
# date_zone 1
a dest 1
a dest_content 1
a dest_headers 50
a dest_ip 1
a dest_mac 1
# dest_port 1
# duplicate_packets_in 1
# duplicate_packets_out 2
# duration 100+
a endtime 100+
a eventtype 2
a form_data 100+
a http_comment 1
# http_content_length 1
a http_content_type 1
a http_method 1
a http_user_agent 1
a index 1
# linecount 1
a location 1
# missing_packets_in 1
# missing_packets_out 2
a network_interface 1
# packets 3
# packets_in 2
```

form\_data

>100 Values, 100% of events

Selected  Yes  No

Reports

[Top values](#) [Top values by time](#) [Rare values](#)

[Events with this field](#)

Top 10 Values	Count	%
username=admin&0960d493674eb04861bd64da9b662118=1&task=login&return=aW5kZXgucGhw&option=com_login&passwd=arthur	1	0.243%
username=admin&115c3aa6072f4b02b4354909431510f6=1&task=login&return=aW5kZXgucGhw&option=com_login&passwd=blazer	1	0.243%
username=admin&12c709bcc2e14d5a015f054d18d36537=1&task=login&return=aW5kZXgucGhw&option=com_login&passwd=fire	1	0.243%
username=admin&2a2ddf97716c1d1e9da21cdaf82b231e=1&task=login&return=aW5kZXgucGhw&option=com_login&passwd=777777	1	0.243%

# Exploitation:

For more confirmation i will search with another query:

The screenshot shows a Splunk search interface titled "New Search". The search bar contains the query: "index=botsv1 sourcetype=stream:http dest=\"192.168.250.70\" http\_method=POST form\_data=\*username\*passwd\* | stats count by src". Below the search bar, a message says "Cannot get username when all users are selected." The search results show 413 events from before 9/6/18 10:15:25.000 AM with "No Event Sampling". The "Statistics (2)" tab is selected. The results table has columns "src" and "count". It shows two rows: "23.22.63.114" with a count of 412, and "40.80.148.42" with a count of 1.

src	count
23.22.63.114	412
40.80.148.42	1

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:

userpassword	count
batman	2
000000	1
1111	1
111111	1

I have found that password “**batman**” is used 2 times.

Now i will answer these simple questions 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
```

The screenshot shows the Splunk Enterprise search interface. The search bar contains the command: `index=botsv1 sourcetype=stream:http | rexfield=form_data"passwd=(?<userpassword>\w+)" | search userpassword=batman | table _time uri userpassword src`. The results table displays two events. The first event, at `_time 2016-08-10 14:46:33.689`, has a `uri` of `/joomla/administrator/index.php`, a `userpassword` of `batman`, and a `src` IP of `23.22.63.114`. The second event, at `_time 2016-08-10 14:48:05.858`, also has a `uri` of `/joomla/administrator/index.php`, a `userpassword` of `batman`, and a `src` IP of `40.80.148.42`.

_time	uri	userpassword	src
2016-08-10 14:46:33.689	/joomla/administrator/index.php	batman	23.22.63.114
2016-08-10 14:48:05.858	/joomla/administrator/index.php	batman	40.80.148.42

**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
```

New Search

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

! Cannot get username when all users are selected.

✓ 18 events (before 9/6/18 12:12:37.000 PM) No Event Sampling ▾

Events (18) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect

List ▾ Format 20 Per Page ▾

Time Event

Selected Yes No

part\_filename()

2 Values, 5.556% of events

Reports Top values Top values by time Rare values

Events with this field

Values	Count	%
3791.exe	1	100%
agent.php	1	100%

SELECTED FIELDS  
a host 1  
a part\_filename{} 2  
a source 1  
a sourcetype 1

INTERESTING FIELDS  
a accept 3  
a accept\_language 2  
# ack\_packets\_in 3  
# ack\_packets\_out 4  
a action 2

# Installation:

i found file named “**3791.exe**”.

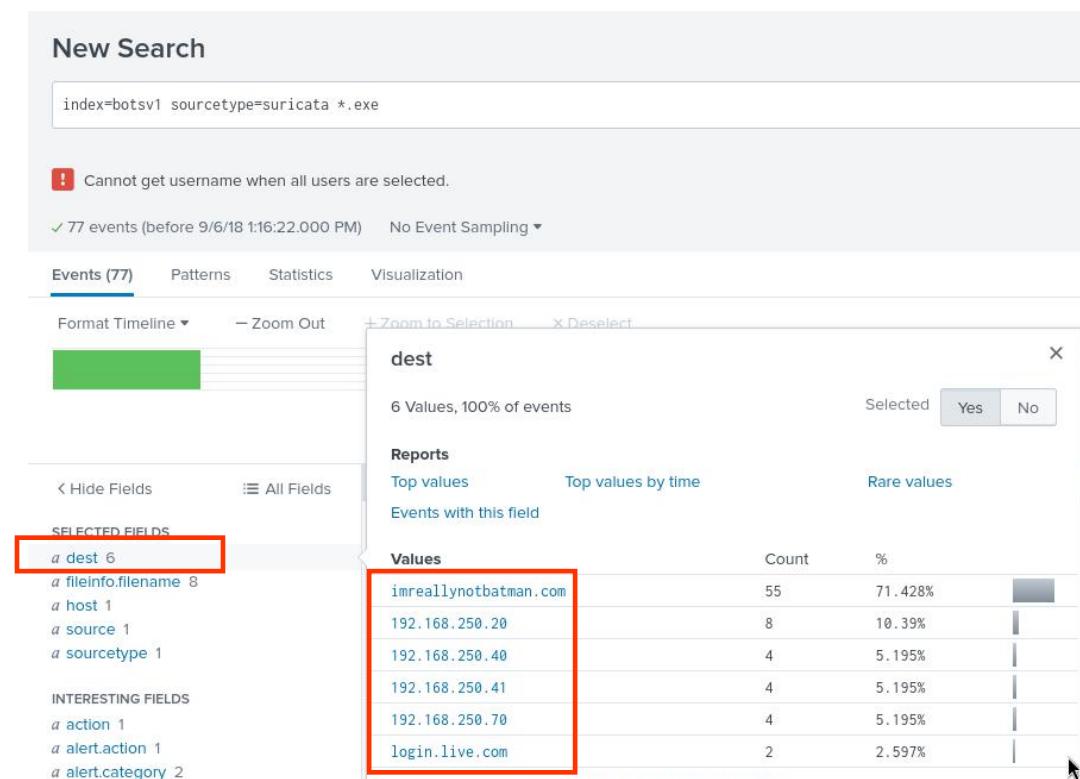
## 2. Search Suricata for any “**.exe**” files & Destination addresses.

**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
```

```
a index 1  
# linecount 1  
a product 1  
a proto 1  
a punct 1  
a splunk_server 1  
a src 1  
a src_ip 1  
# src_port 2  
# status 1  
a tag 1  
a tag:eventtype 1  
# timeendpos 1
```



**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(65df73d77324d008c83c3e57b445df0fd43a3a51),**

**SHA256(ec78c938d8453739ca2a370b9c275971ec46caf6e479de2b2d04e97cc47fa45d)**

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

And Targeted Host is  
**we1149srv.waynecorpinc.local**

New Search

```
index=botsv1_3791.exe sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" EventCode=1 | table hashes dest
```

Cannot get username when all users are selected.

5 events (before 9/6/18 6:55:51.000 PM) No Event Sampling ▾

Events Patterns Statistics (5) Visualization

20 Per Page ▾ Format Preview ▾

hashes ▾ dest ▾

2C6B753628A3AA138AE52357F76AA4D5617D890E 626A9EC445D06FBC1502BF53A1E3356B 42A43BF18F7C0FA4DB997E8B7688711C9B36BD73D5F013FA5B418F0956A92266 766BBC554510CAA578DC083D295D781	we1149srv.waynecorpinc.local
65DF73D77324D008C83C3E57B445DF0FD43A3A51 AAE3F5A29935E6ABCC2C2754D12A9AF0 EC78C938D8453739CA2A370B9C275971EC46CAF6E479DE2B2D04E97CC47FA45D 481F47BBB2C9C21E108D65F52B04C448	we1149srv.waynecorpinc.local
F5CFD4070EA7D2B40A29F21F9E29AF23341C59EC 59A1D4FACD7B333F76C4142CD42D3ABA E1A080E61FB1BAF0DA629D34BAEE6F0F9D0E0337BF6CED9F4B3AB9B1C23D91BA 5B13496CE269DF7709AAB6B1BBF99CD3	we1149srv.waynecorpinc.local
F5CFD4070EA7D2B40A29F21F9E29AF23341C59EC 59A1D4FACD7B333F76C4142CD42D3ABA E1A080E61FB1BAF0DA629D34BAEE6F0F9D0E0337BF6CED9F4B3AB9B1C23D91BA 5B13496CE269DF7709AAB6B1BBF99CD3	we1149srv.waynecorpinc.local
F5CFD4070EA7D2B40A29F21F9E29AF23341C59EC 59A1D4FACD7B333F76C4142CD42D3ABA E1A080E61FB1BAF0DA629D34BAEE6F0F9D0E0337BF6CED9F4B3AB9B1C23D91BA 5B13496CE269DF7709AAB6B1BBF99CD3	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:

## New Search

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

! Cannot get username when all users are selected.

✓ 1 event (before 9/7/18 9:48:15.000 AM) No Event Sampling ▾

Events (1) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect

List ▾ ✓ Format 20 Per Page ▾

< Hide Fields

All Fields

X

### SELECTED FIELDS

a answer 1

a dest 1

a host 1

a name[] 1

a source 1

a sourcetype 1

a src 1

### INTERESTING FIELDS

a app 1

name[]

1 Value, 100% of events

Selected

Yes

No

### Reports

Top values

Top values by time

Rare values

Events with this field

### Values

Count

%

prankglassinebracket.jumpingcrab.com

2

200%

# 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](http://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](http://prankglassinebracket.jumpingcrab.com)**

**IP: [23.22.63.114](http://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>**

**Medium: <https://medium.com/@Munsif1>**



FOLLOW YOUR  
**DREAMS**