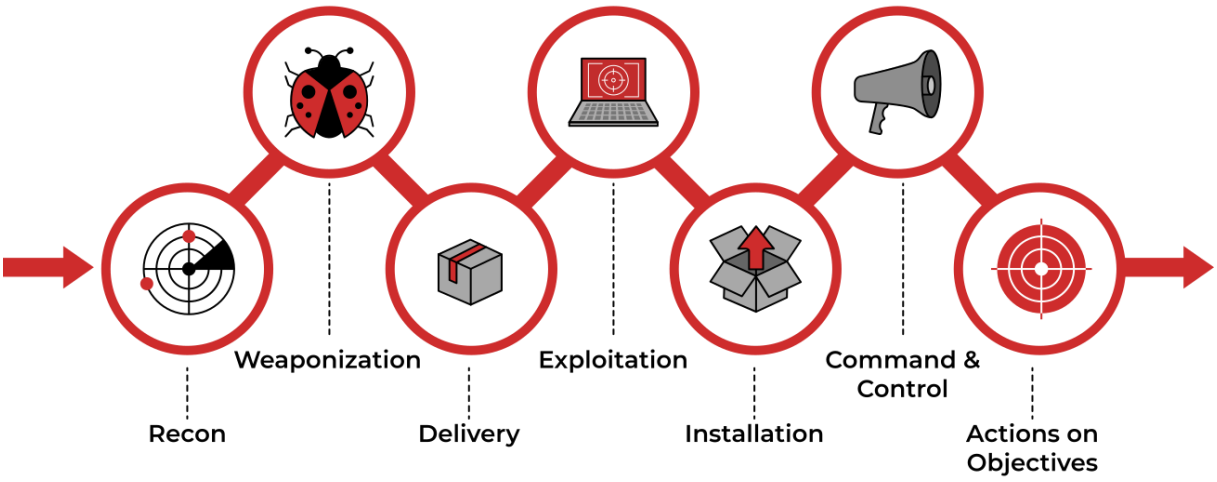
Investigating with Splunk

In this scenario we will act as security analyst with task to investigate recent incident in **Wayne Enterprises** where website **imreallynotbatman.com** was compromised. Website is now displaying attacker information.

Fortunately organization have Splunk already in place which we will use to find all attackers activities in network. We will also utilise OSINT to fill the gaps in our investigation.

We will follow Cyber kill chain model to map attackers activities in each phase.



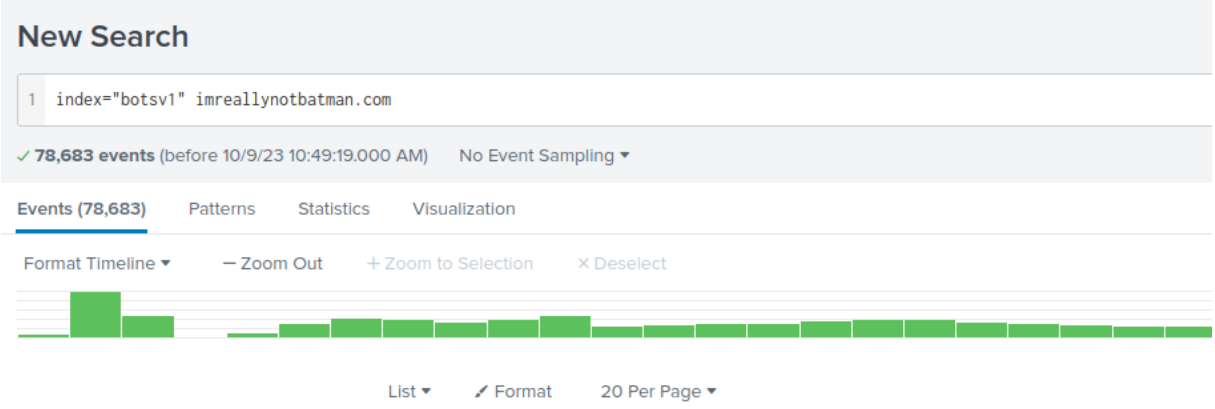
We are utilizing event logs present in **index=botsv1**

Reconnaissance Phase

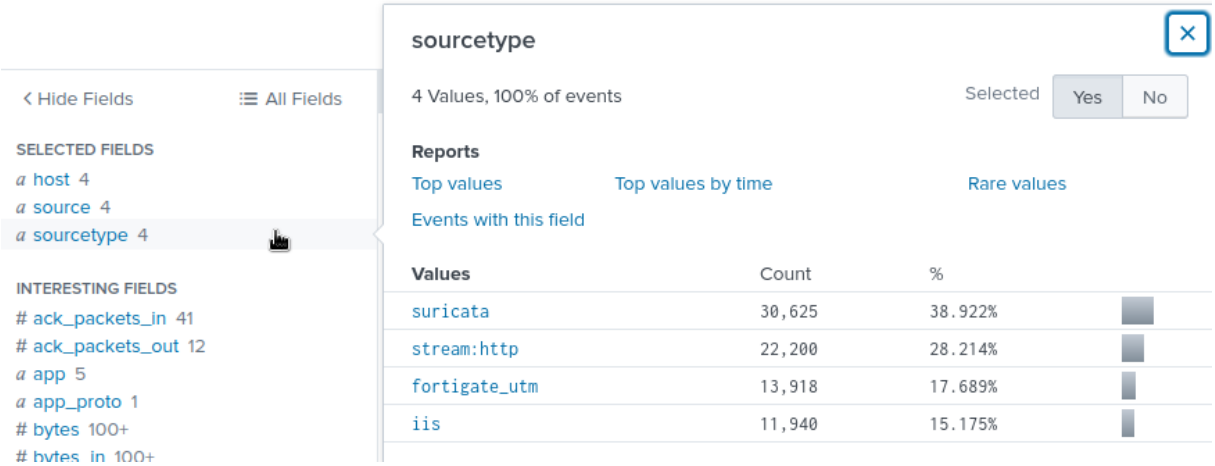
Reconnaissance Phase is attempt of an attacker to discover and collect any information about a target. Knowledge comes from systems, web applications, servers, employees and public data

We know that website **imreallynotbatman.com** was compromised. So from our side we should start checking all logs related to this webserver. Then we will investigate web traffic to determine who tried to connect with this webserver.

Our search query will be: **index="botsv1" imreallynotbatman.com**



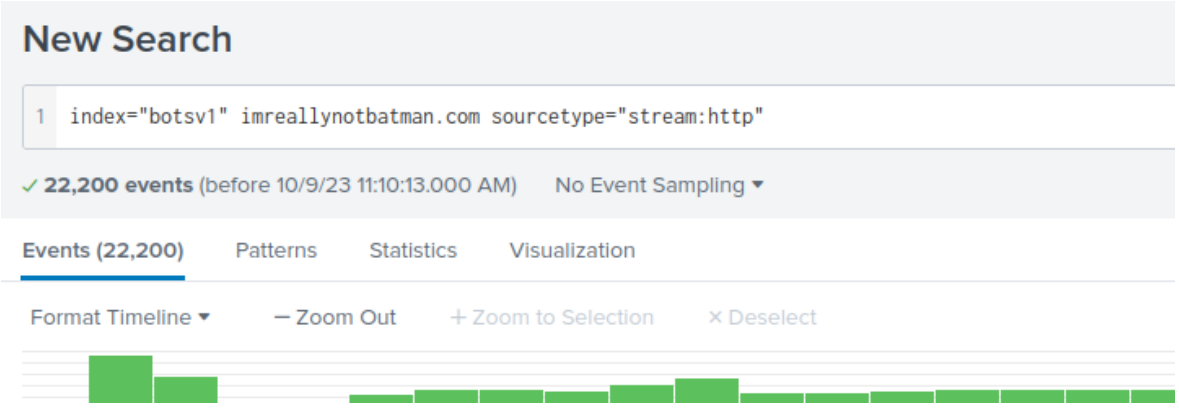
We will check all sources of logs. By clicking **sourcetype**



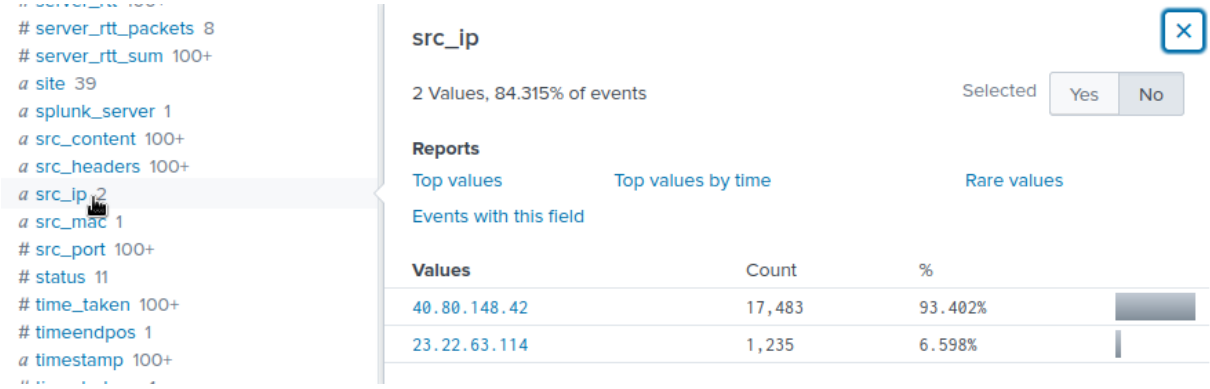
Log sources are:

- Suricata
- stream:http
- fortigate_utm
- iis

Our first task is to identify IP address attempting to perform recon activity on our web server. It is obvious to look at web traffic. Search Query: **index="botsv1" imreallynotbatman.com sourcetype="stream:http"**

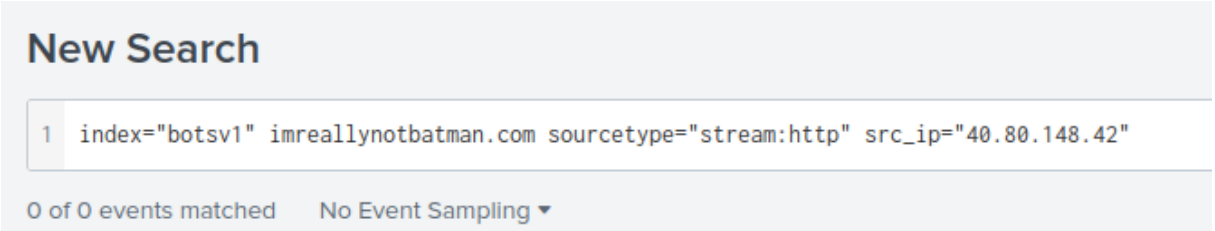


Let's see source ip addresses



We see only 40.80.148.42 and 23.22.63.114. First IP seems to contain far higher percentage of the logs compared to second one. Let's investigate further to be sure.

We will add query for ip 40.80.148.42 and then look at fields like User-Agent, Post request, URI etc.



Weird URI:

```
/"943671%40
/%21
/%21%21
/%21%21%21
/%21install
/%21test
/%23
/%24
/%24%7Bdirname%7D.jar
/%24%7Bdirname%7D.war
/%2B
/%3F
/%40
/%5C../%5C../%5C../%5C../%5C../%5C../%5C../%5C../%5C../etc/hosts
/%C0%AE/WEB-INF/web.xml
/%C0%AE/WEB-INF/web.xml%C0%80.jsp
```

Attempt in using vulnerability scanner:

```
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: */*
```

Sites:

a site 39	!(()&&!|*|*|	1	0.006%
a splunk_server 1	(select convert(int,CHAR(65)))	1	0.006%
a src_content 100+	(select(0)from(select(sleep(6)))v)/*'+ (select(0)from(select(sleep(6)))v)+'"+ (select(0)from(select(sleep(6)))v)+"*/	1	0.006%
a src_headers 100+	)	1	0.006%
a src_ip 1	-1 OR 2+618-618-1=0+0+0+1	1	0.006%
a src_mac 1	-1 OR 2+732-732-1=0+0+0+1 --	1	0.006%
# src_port 100+	-1 OR 3+618-618-1=0+0+0+1	1	0.006%
# status 11	-1 OR 3+732-732-1=0+0+0+1 --	1	0.006%
# time_taken 100+	-1" OR 2+866-866-1=0+0+0+1 --	1	0.006%
# timeendpos 1			
a timestamp 100+			
# timestartpos 1			
a transport 1			
a uri 100+			
a uri_path 100+			

We will validate scanning attempts with suricata logs to see if any rule is triggered.

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

```
1 index="botsv1" imreallynotbatman.com sourcetype="suricata" src_ip="40.80.148.42"
```

Then add new fields that are related to alerts.

16 more fields

Select Fields

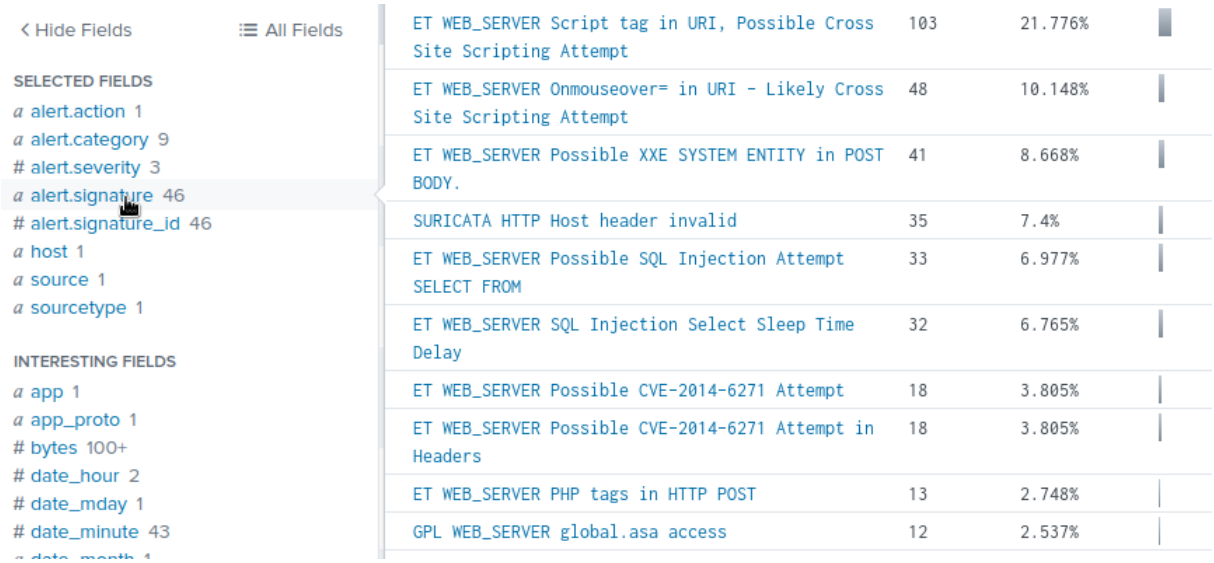
Select All Within Filter Deselect All Coverage: 1% or more alert

i	✓	Field
>	☑	alert.action
>	☑	alert.category
>	☑	alert.severity
>	☐	alert.gid
>	☐	alert.rev
>	☐	alert.signature
>	☐	alert.signature_id
>	☐	alert_gid
>	☐	alert_rev

Alert categories:

Values	Count	%
Web Application Attack	248	52.431%
A Network Trojan was detected	99	20.93%
Attempted Administrator Privilege Gain	36	7.611%
Generic Protocol Command Decode	36	7.611%
Attempted Information Leak	32	6.765%
access to a potentially vulnerable web application	18	3.805%
Information Leak	2	0.423%
Detection of a Network Scan	1	0.211%
Potentially Bad Traffic	1	0.211%

Alert signatures:



Exploitation Phase

Let's summarize our findings so far:

- Webserver ip is 192.168.250.70
- Ip 40.80.148.42 attempted to scan server
- Attacker used web scanner Acunetix

Exploitation phase is phase where attacker exploits vulnerability to gain access to the system/server.

Interesting for us field is **HTTP method** and **HTTP referrer.**

http_method

6 Values, 99.778% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
POST	14,238	72.062%
GET	5,512	27.898%
OPTIONS	5	0.025%
CONNECT	1	0.005%
PROPFIND	1	0.005%
TRACE	1	0.005%

As we see POST method dominates GET method which means user more frequently sent data do server.

http_referrer

98 Values, 53.651% of events

Reports

Top values Top values by time

Events with this field

Top 10 Values

http://imreallynotbatman.com:80/

http://imreallynotbatman.com/joomla/index.php/component/search

In http_referrer we see “joomla”. From Google we can easily discover it is Joomla CMS in the backend. Page /joomla/index.php is used for login access. We will need this information to investigate potential brute force attempts.

Let’s query index=botsv1 imreallynotbatman.com sourcetype=stream:http dest_ip="192.168.250.70" uri="/joomla/administrator/index.php"

```
index=botsv1 imreallynotbatman.com sourcetype=stream:http dest_ip="192.168.250.70"  uri="/joomla/administrator/index.php"
```

✓ **1,248 events** (before 10/9/23 12:12:01.000 PM) No Event Sampling

src_ip

2 Values, 100% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
23.22.63.114	1,235	98.958%
40.80.148.42	13	1.042%

This information is interesting because suggests us that ip 23.22.63.114 was frequently communicating with login page on joomla. This may indicate brute-force attempts.

Form_data may contain credentials that attacker may have tried. We will add to our query: `| table _time uri src_ip dest_ip form_data`

New Search

```
index=botsv1 imreallynotbatman.com sourcetype=stream:http dest_ip="192.168.250.70" uri="/joomla/administrator/index.php" | table _time uri src_ip dest_ip form_data
```

✓ 1,248 events (before 10/9/23 12:17:31.000 PM) No Event Sampling

Events Patterns Statistics (1,248) Visualization

20 Per Page Format Preview Prev

_time	url	src_ip	dest_ip	form_data
2016-08-10 21:46:44.854	/joomla/administrator/index.php	23.22.63.114	192.168.250.70	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=scorpion&672dec7c835bcb02
2016-08-10 21:46:44.842	/joomla/administrator/index.php	23.22.63.114	192.168.250.70	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=2222&8771cb481c90942b16a7
2016-08-10 21:46:44.540	/joomla/administrator/index.php	23.22.63.114	192.168.250.70	
2016-08-10 21:46:44.646	/joomla/administrator/index.php	23.22.63.114	192.168.250.70	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=rebecca&ea1a1f61376ed4a9e

We zoom on form_data field:

```
username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=scorpion&672dec7c835bcb0208f89bb8d6a1167d=1
username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=2222&8771cb481c90942b16a708f2fd645c63=1

username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=rebecca&ea1a1f61376ed4a9e819ce28e7a27e0d=1

username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=boobs&2b3e8a52444384ace46940d8d438ef90=1

username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=star&8830ccd1f085f63e6ad42ba6cf8debc6=1
username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=birdie&ab62c6f01537aa011cf1767349edc467=1
```

We see multiple login attempts with username admin and changing password value. Time differences suggests us that attacker used automated tool to perform this brute force attempt.

Under http_user_agent filter we see only 2 values. We see that attacker used Python script to perform bruteforce attack.

Values	Count	%
Python-urllib/2.7	1,235	98.958%
Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko	13	1.042%

But why we see only 1 attempt from Mozilla? Let's check this.

40.80.148.42	192.168.250.70	option=com_extplorer&action=getdircontents&dir=&sendWhat=dirs&node=ext_root	Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
40.80.148.42	192.168.250.70	start=0&limit=150&dir=&option=com_extplorer&action=getdircontents&sendWhat=both	Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
40.80.148.42	192.168.250.70	username=admin&passwd=batman&option=com_login&task=login&return=aW5kZXgucGhw&e5ec827a3f67ce0efc546d81f7356acc=1	Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
23.22.63.114	192.168.250.70	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=scorpion&672dec7c835bcb0208f89bb8d6a1167d=1	Python-urllib/2.7
23.22.63.114	192.168.250.70	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=2222&8771cb481c90942b16a708f2fd645c63=1	Python-urllib/2.7
23.22.63.114	192.168.250.70		Python-urllib/2.7
23.22.63.114	192.168.250.70	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=rebecca&ea1a1f61376ed4a9e819ce28e7a27e0d=1	Python-urllib/2.7
23.22.63.114	192.168.250.70		Python-urllib/2.7

username=admin&passwd=batman&option=com_login&task=login&return=aW5kZXgucGhw&e5ec827a3f67ce0efc546d81f7356acc=1

Attacker logged from 40.80.148.42 using username = admin and passwd = batman. He probably guessed password using 23.22.63.114 ip address and then logged in using 40.80.148.42 and Mozilla browser.

Installation Phase

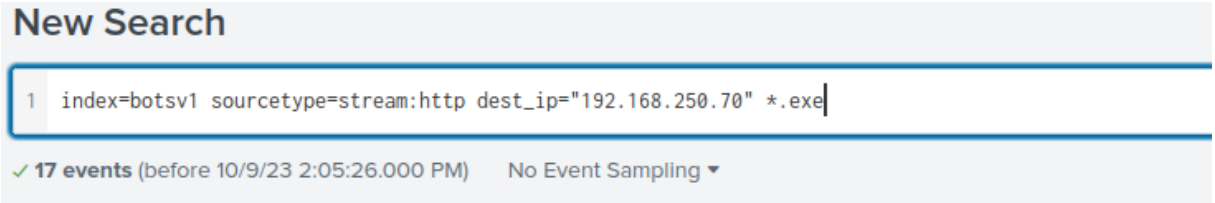
After attacker has successfully exploited security of a system. He will try to achieve persistence or to gain more control. This activity falls in installation phase category.

We found so far:

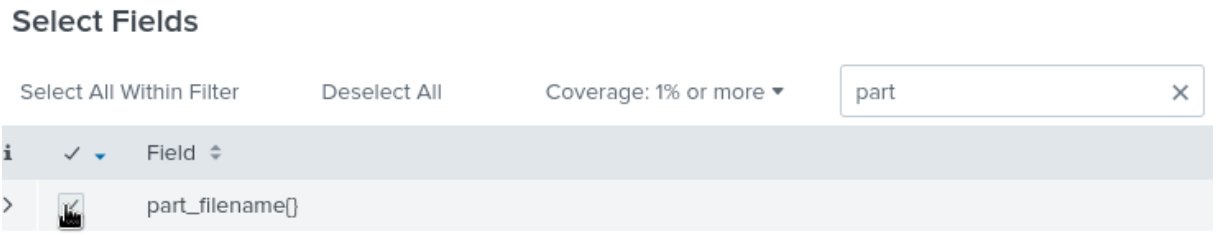
- Attacker performed bruteforce attack using Python script on joomla/index.php from ip address 20.23.63.144
- After successfully guessing password he logged in from ip 40.80.148.42

We now should expect some payload coming from address 40.80.148.42 and file execution.

Seach Query: index=botsv1 sourcetype=stream:http dest_ip="192.168.250.70" *.exe



Search for part_filename[] to find files with .exe extension



part_filename{}

2 Values, 5.882% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

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

Bingo, we found suspicious file 3791.exe. It was sent to our webserver via POST method. Let's check source IP to be sure that it was sent from suspicious address.

c_ip

1 Value, 100% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
40.80.148.42	1	100%

Now we only need to know if there was file execution event on webserver.

New Search

```
1 index=botsv1 "3791.exe"
```

✓ **76 events** (before 10/9/23 2:13:00.000 PM) No Event Sampling

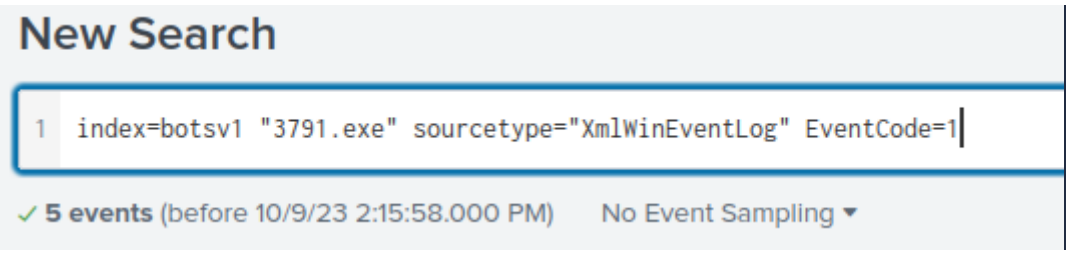
In sourcetype we see that we have 3 types of host-based logs to for disposal.

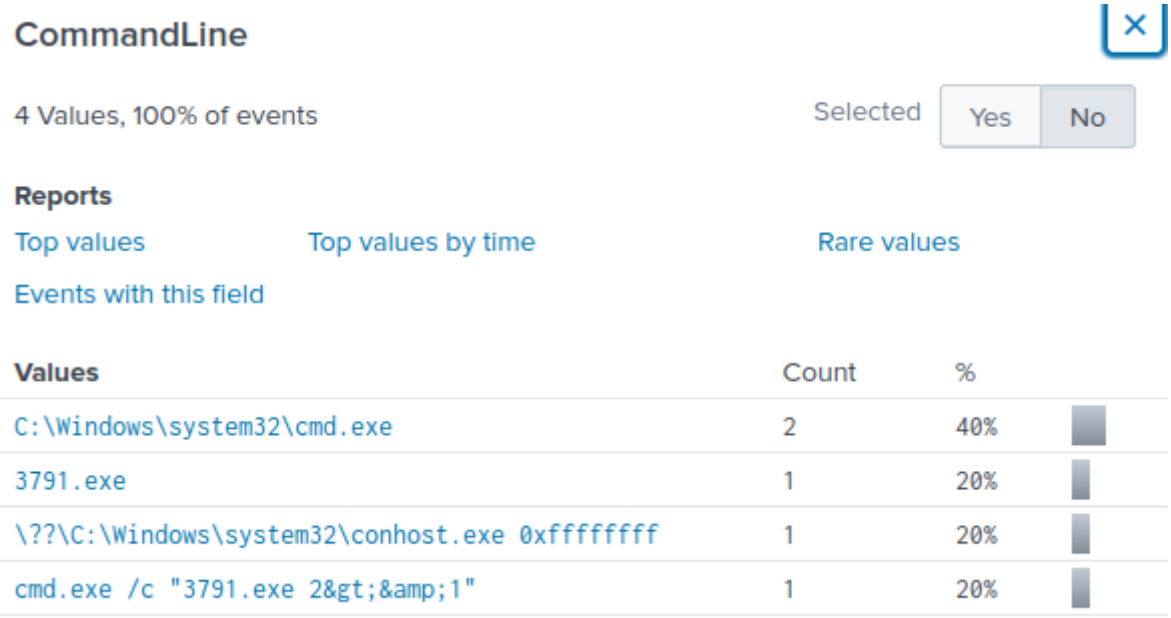
Values	Count
xmlwineventlog	69
wineventlog	3
stream:http	2
fortigate_utm	1

We will utilise Sysmon logs and its event id 1: Process Creation.

More about it: https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

Search Query: `index=botsv1 "3791.exe" sourcetype="XmlWinEventLog" EventCode=1`





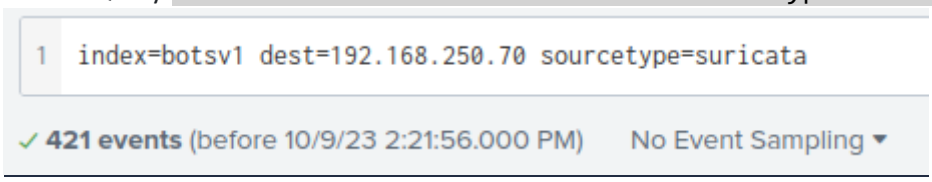
After clicking on 3791.exe we can extract it's hash value for further investigation with OSINT tools.

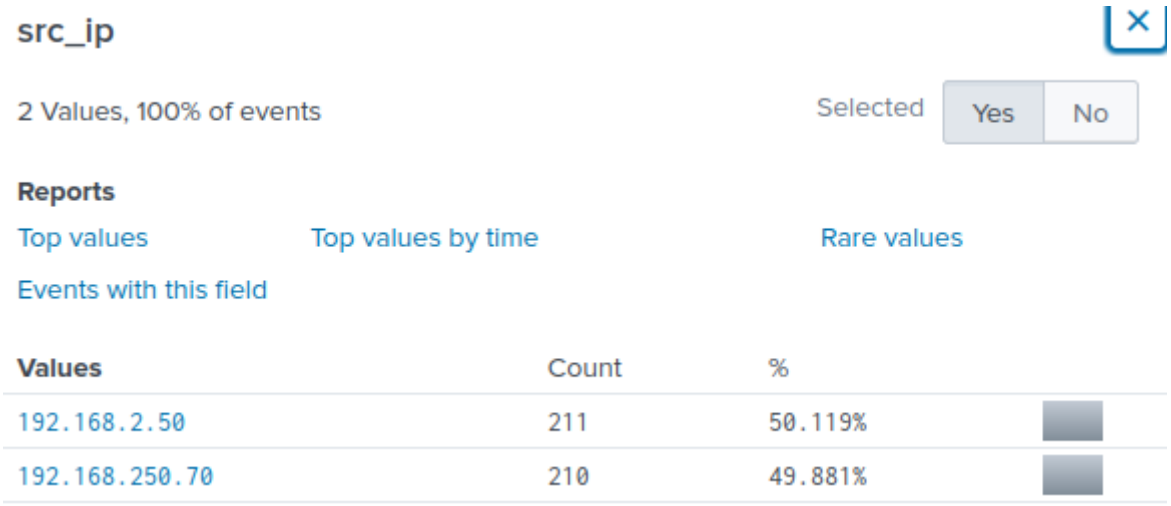
Action on Objectives

We know already how attacker gained access to website. Let's now investigate how website was modified.

Let's start by looking at suricata logs related to webserver ip address

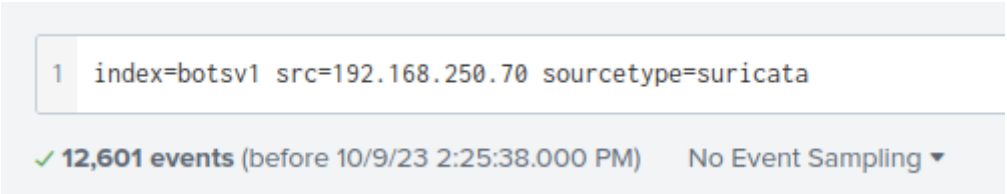
Search Query: `index=botsv1 dest=192.168.250.70 sourcetype=suricata`





Logs show no external communication with server. But let's see communication from the server

Search Query: index=botsv1 src.192.168.250.70 sourcetype=suricata

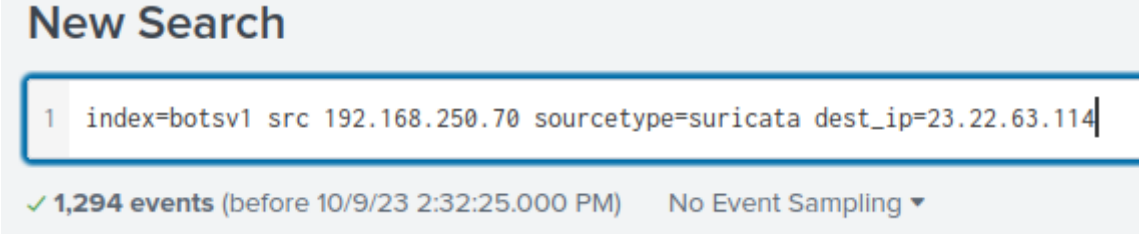


Usually server do not originate the traffic. The client would be the source and the server destination. Here we see external IP to which our server initiates outbound traffic. Let's check one by one.

Search Query: index=botsv1 src 192.168.250.70 sourcetype=suricata dest_ip=40.80.148.42

On this ip nothing particularly interesting…

Search Query: index=botsv1 src 192.168.250.70 sourcetype=suricata dest_ip=23.22.63.114



url

3 Values, 99.691% of events

Selected Yes No

Reports

Top values | Top values by time | Rare values

Events with this field

Values	Count	%
/joomla/administrator/index.php	1,235	95.736%
/joomla/agent.php	52	4.031%
/poisonivy-is-coming-for-you-batman.jpeg	3	0.232%

But here we have poisonivy-is-coming-for-you-batman.jpeg.

Type	Field	Value	Actions
Selected	dest_ip	23.22.63.114	
	host	suricata-ids.waynecorpinc.local	
	source	/var/log/suricata/eve.json	
	sourcetype	suricata	
	src_ip	192.168.250.70	
Event	bytes	553879	
	dest	prankglassinebracket.jumpingcrab.com	

It's coming from attacker's website.

Command and Control Phase

Attacker uploaded file to the server before defacing it. Doing so he resolved malicious IP using DNS. We want to discover this malicious ip address and we know that file was called "posionivy-is-coming-for-you-batman.jpeg"

We will grab fortigate_utm first to review firewall logs.

Search Query: index=botsv1 sourcetype=fortigate_utm"poisonivy-is-coming-for-you-batman.jpeg"

New Search

```
index=botsv1 sourcetype=fortigate_utm"poisonivy-is-coming-for-you-batman.jpeg"
```

✓ **3 events** (before 10/9/23 2:51:32.000 PM) No Event Sampling

Events (3) Patterns Statistics Visualization

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

url

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:1337/poisonivy-is-coming-for-you-batman.jpeg	3	100%

We will look also to stream:http log source

Search Query: index=botsv1 sourcetype=stream:http dest_ip=23.22.63.114 "poisonivy-is-coming-for-you-batman.jpeg" src_ip=192.168.250.70


```
dest_ip: 23.22.63.114
dest_mac: 08:5B:0E:93:92:AF
dest_port: 1337
duplicate_packets_in: 2
duplicate_packets_out: 0
endtime: 2016-08-10T22:13:46.915172Z
http_method: GET
missing_packets_in: 0
missing_packets_out: 0
network_interface: eth1
packets_in: 6
packets_out: 5
reply_time: 0
request: GET /poisonivy-is-coming-for-you-batman.jpeg HTTP/1.0
request_ack_time: 3246
request_time: 61714
response_ack_time: 0
response_time: 0
server_rtt: 32357
server_rtt_packets: 2
server_rtt_sum: 64714
site: prankglassinebracket.jumpingcrab.com:1337
src_headers: GET /poisonivy-is-coming-for-you-batman.jpeg HTTP/1.0
Host: prankglassinebracket.jumpingcrab.com:1337

src_ip: 192.168.250.70
src_mac: 00:0C:29:C4:02:7E
src_port: 63139
time_taken: 61715
timestamp: 2016-08-10T22:13:46.853458Z
transport: tcp
uri: /poisonivy-is-coming-for-you-batman.jpeg
uri_path: /poisonivy-is-coming-for-you-batman.jpeg
```

Weaponization Phase

In this phase adversaries would:

- Create Malware/ Malicious document to gain initial access etc.
- Establish domains similar to the target domain to trick users
- Create C2 server for the post-exploitation activity

We found domain prankglassinebracket.jumpingcrab.com, and few IP addresses associated with this attack. We will search online Threat Intel sites for additional information.

Robtex:

https://www.robtex.com/

Robtex is a threat intel site that provides IP addresses, domain names.

General	
FQDN	prankglassinebracket.jumpingcrab.com
Host Name	prankglassinebracket
Domain Name	jumpingcrab.com
Registry	com
TLD	com
Domain DNS	
Name servers	ns1.**afraid**.org ns2.**afraid**.org ns3.**afraid**.org ns4.**afraid**.org
Mail servers	mail.**jumpingcrab**.com
IP Numbers	69.197.18.183 70.39.97.227 169.47.130.85

SHARED

This section shows related hostnames and ipnumbers

Siblings

Siblings are domains or hostnames on the same level

adjazd.**jumpingcrab**.com
easythere.**jumpingcrab**.com
lev.**jumpingcrab**.com
miegum.**jumpingcrab**.com
nonesuch.**jumpingcrab**.com
piranhabrothers.**jumpingcrab**.com
sendmgs.**jumpingcrab**.com
sslsd.**jumpingcrab**.com
www.**jumpingcrab**.com
zim.**jumpingcrab**.com

Next we will search IP address 23.22.63.114.

SHARED

This section shows related hostna

Using as IP numbe

wanecorpinc.com
wayncorpinc.com
waynecorinc.com
waynecorpnc.com
waynecrpinc.com
wayneorpinc.com
wynecorpinc.com

This ip address is in relation with wayneorpinc.com, we will go on with investigation to Virustotal

VirusTotal:

https://www.virustotal.com/

Virustotal is OSINT site to analyze suspicious files, domains and IP etc.

We searched for ip 23.22.63.114

2023-08-07	61 / 71	Win32 EXE	ab.exe

We can see it is related to ab.exe

ec78c938d8453739ca2a370b9c275971ec46caf6e479de2b2d04e97cc47fa45d

61 / 71

61 security vendors and 1 sandbox flagged this file as malicious

ec78c938d8453739ca2a370b9c275971ec46caf6e479de2b2d04e97cc47fa45d

ab.exe

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

Using hash value from Splunk we can find that 3791.exe is ab.exe, which is widely recognized as malware.

Passive DNS Replication (11)

Date resolved	Detections	Resolver	Domain
2019-12-01	0 / 89	VirusTotal	waynecorinc.com
2019-11-30	0 / 89	VirusTotal	wanecorpinc.com
2019-11-29	0 / 89	VirusTotal	wynecorpinc.com
2019-11-28	0 / 89	VirusTotal	wayneorpinc.com
2019-11-05	0 / 89	VirusTotal	wayncorpinc.com
2019-09-30	0 / 89	VirusTotal	waynecrpinc.com
2019-09-28	0 / 89	VirusTotal	waynecorpnc.com
2019-04-19	0 / 88	VirusTotal	ec2-23-22-63-114.compute-1.amazonaws.com
2018-07-18	0 / 89	VirusTotal	po1s0n1vy.com
2018-05-19	0 / 89	VirusTotal	www.po1s0n1vy.com

Communicating Files (4)

Scanned	Detections	Type	Name
2022-12-26	54 / 70	Win32 EXE	software.exe
2023-10-03	52 / 72	Win32 EXE	MirandaTateScreensaver.scr.exe
2016-08-10	53 / 55	unknown	MSRSAAPP
2023-08-07	61 / 71	Win32 EXE	ab.exe

We see suspicious domain po1s0n1vy.com. Thanks to google we discover that this domain is in relation with APT Group PoisonIvy

Squarespace

https://static1.squarespace.com › static › Cyber+... PDF

Summary of APT Group- PoisonIvy

Report of the Cyber Kill Chain for **APT Group PoisonIvy** (P01s0n1vy). Threat actor is APT Group known as PoisonIvy. PoisonIvy has defaced Wayne Enterprises ...

5 stron

Delivery Phase

Attackers create malware and infect devices to gain initial access or evade defences and find ways to deliver it.

Our task is to use information we have about the adversary to find any malware linked with adversary

Threat Miner

https://www.threatminer.org/host.php?q=23.22.63.114#gsc.tab=0&gsc.q=23.22.63.114&gsc.page=1

We will start by looking 23.22.63.114 in threatminer

Malware Samples

Malware samples associated with 23.22.63.114.

Copy | Excel | CSV | PDF

MD5	Detections	
39eecefa9a13293a93bb20036eaf1f5e	N/A	
aae3f5a29935e6abcc2c2754d12a9af0	N/A	
c99131e0169171935c5ac32615ed6261	ALYac	Trojan.GenericKD.3470547
	AVG	Agent5.APHV
	AVware	Trojan.Win32.GenericIBT
	Ad-Aware	Trojan.GenericKD.3470547
	AegisLab	Agent5.Aphv.Genlc
	AhnLab-V3	Malware/Gen.Generic.N2081883700
	Antiy-AVL	Trojan[Backdoor]/Win32.Redsip
	Arcabit	Trojan.Generic.D34F4D3
	Avira	TR/AD.Zupdax.qmyx
	BitDefender	Trojan.GenericKD.3470547

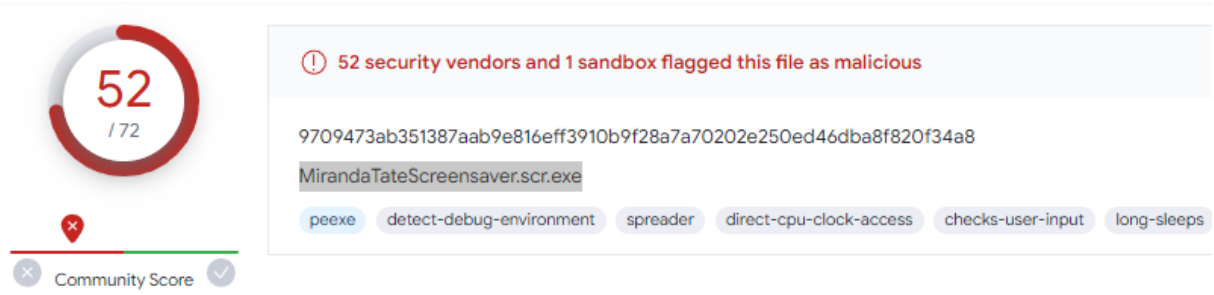
We found three files associated with this IP from which third one is confirmed to be malicious. We will click on this hash value to dig deeper.

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:	9709473ab351387aab9e816eff3910b9f28a7a70202e250ed46dba8f82
SHA512:	8fb3b09541b021e06eeec455876526607114adb547eacb7556d578c08
SSDEEP:	12288:JCy+DdcUrY4tO3Rc5F5H8q3/HSaRanZ0:Jj+COpO3Rc5F5H8c
IMPHASH:	fae2c8486a11f609323cc15c0ee838cf
Authentihash:	N/A
Related resources	VirusTotal | Hybrid-Analysis | VirusShare

Let’s search for this hash in virustotal



In relations tab

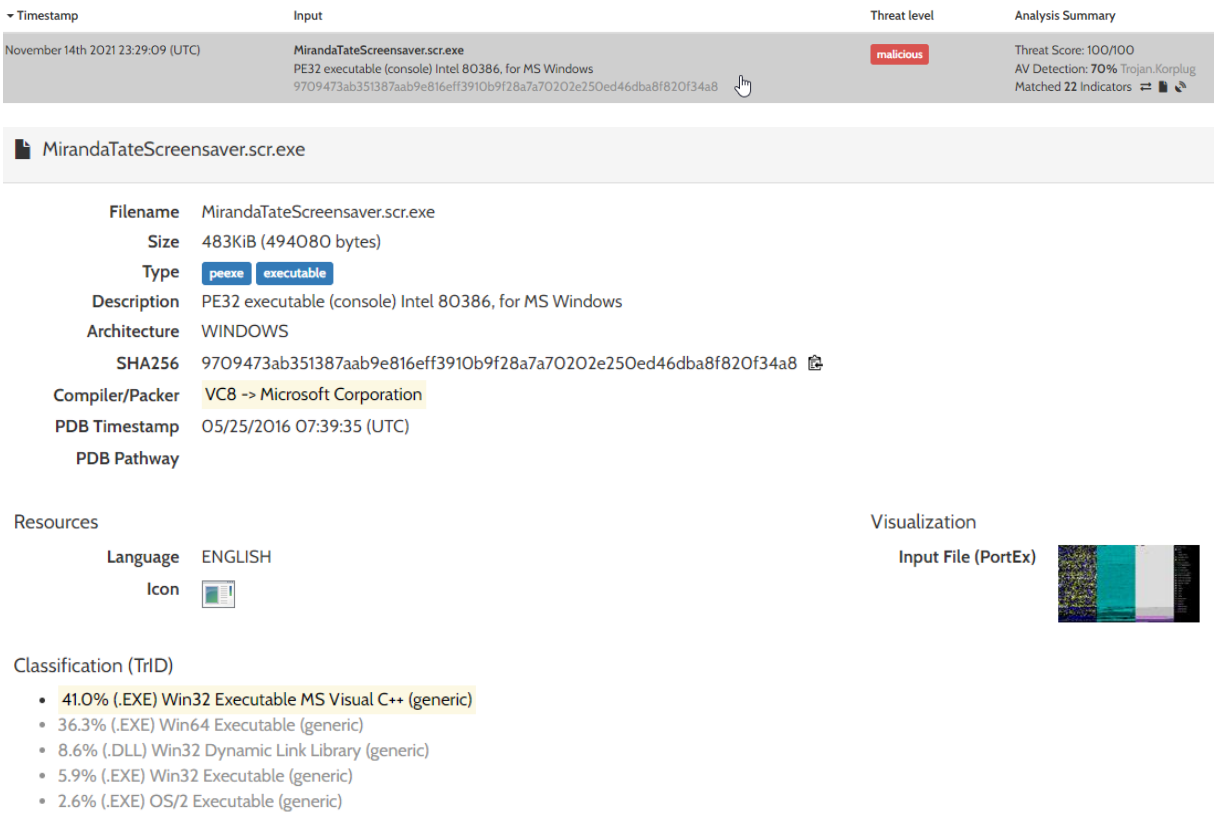
23.216.147.64	1 / 89	20940	US
23.216.147.76	1 / 89	20940	US
23.22.63.114	0 / 89	14618	US
23.223.54.145	0 / 88	20940	US
23.35.98.25	0 / 89	20940	US

It is related to our suspicious ip address.

Hybrid-Analysis site.

https://www.hybrid-analysis.com/

We will finish our investigation on **Hybrid-Analysis site.**



Summary

Recon Phase:

- IP address 40.80.148.42 was attempting vulnerability scan on our webserver.
- Attacker was using Acunetix web scanner.

Exploitation Phase:

- Brute force attack originated from 23.22.63.114.
- After successfully guessing password, adversary gained access through ip address 40.80.148.42.
- Adversary performed multiple brute force attempts with unique password where one was successful.

Installation Phase:

- Malicious file 3791.exe was uploaded to the webserver
- We found hash values of the file

Action on Objective:

- After compromising the web server, the attacker modified the website.
- We found that they used file called “poisonivy-is-coming-for-you-batman.jpeg”.

Weaponization Phase:

Attacker infrastructure:

- Domain: prankglassinebracket.jumpingcrab.com
- IP address: 23.22.63.114
- Multiple domains that masquerade original domain.

Deliver Phase:

Using various Threat Intel sites we found malware associated with malicious IP address

- Malware name: MirandaTateScreensaver.scr.exe
- MD5 value of malware was: c99131e0169171935c5ac32615ed6261

Thank you for reading this guide in the assignment conducted on the THM platform. I hope that the information here has been useful in some way. If you want to try it yourself, check it out here!

https://tryhackme.com/room/splunk201