

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC



Investigating with Splunk Workshop

Ethan Gardiner | Global Security Strategist
LTRAPP-2688

CISCO *Live!*

#CiscoLiveAPJC

Cisco Webex App

Questions?

Use Cisco Webex App to chat with the speaker after the session

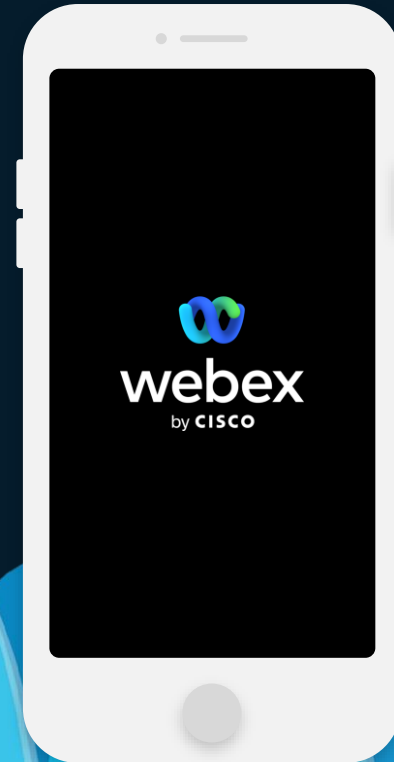
How

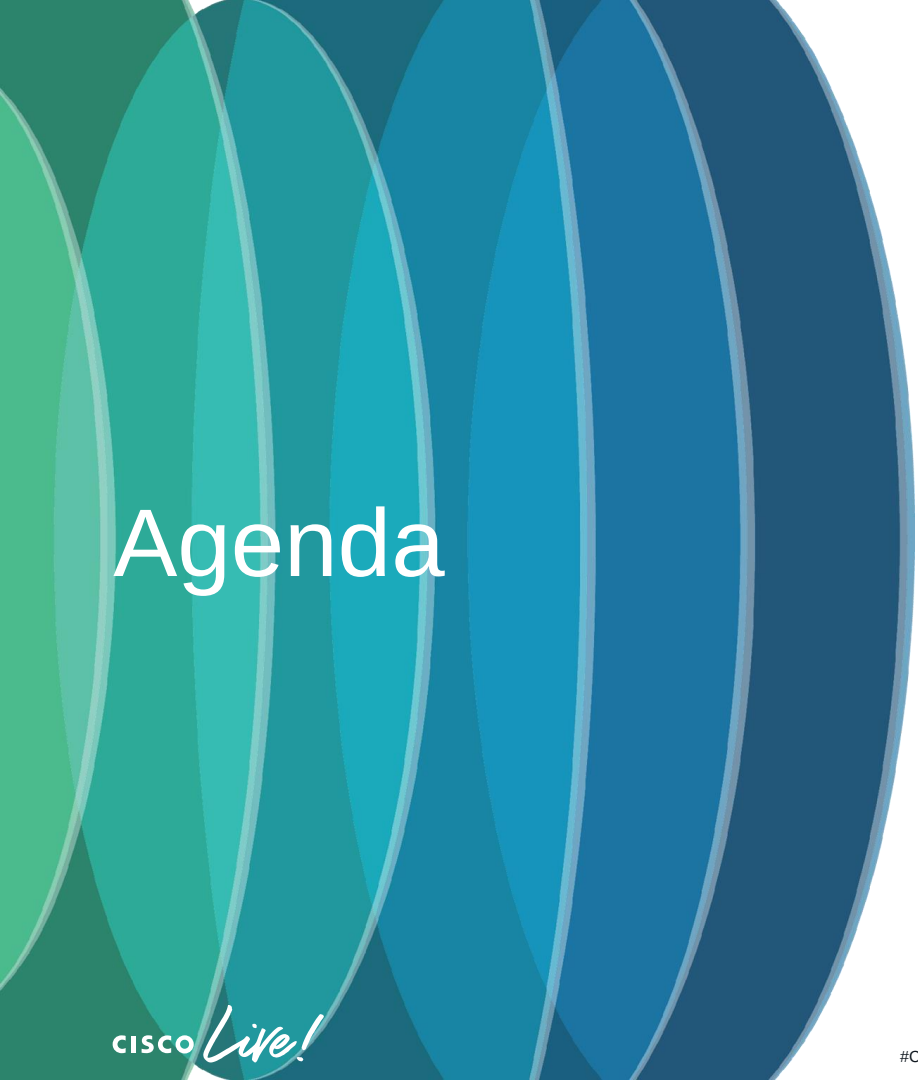
- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until November 15, 2024.



<https://ciscolive.ciscoevents.com/ciscolivebot/#LTRAPP-2688>





Agenda

- Introduction
- Why Investigating?
- Scenario Review
- Investigating an APT
- Investigating Ransomware
- Conclusion

#whoami



Ethan Gardiner
Global Security
Strategist
Splunk

Investigate (Thanks, Google!)

in·ves·ti·gate

/inˈvestəˌɡāt/ 

verb

verb: **investigate**; 3rd person present: **investigates**; past tense: **investigated**; past participle: **investigated**; gerund or present participle: **investigating**

carry out a systematic or formal inquiry to discover and examine the facts of (an incident, allegation, etc.) so as to establish the truth.

"police are investigating the alleged beating"

synonyms: inquire into, look into, go into, [probe](#), [explore](#), [scrutinize](#), conduct an investigation into, make inquiries about; [More](#)

- carry out research or study into (a subject, typically one in a scientific or academic field) so as to discover facts or information.

"future studies will investigate whether long-term use of the drugs could prevent cancer"

synonyms: inquire into, look into, go into, [probe](#), [explore](#), [scrutinize](#), conduct an investigation into, make inquiries about; [More](#)

- make inquiries as to the character, activities, or background of (someone).

"everyone with a possible interest in your brother's death must be thoroughly investigated"

synonyms: inquire into, look into, go into, [probe](#), [explore](#), [scrutinize](#), conduct an investigation into, make inquiries about; [More](#)

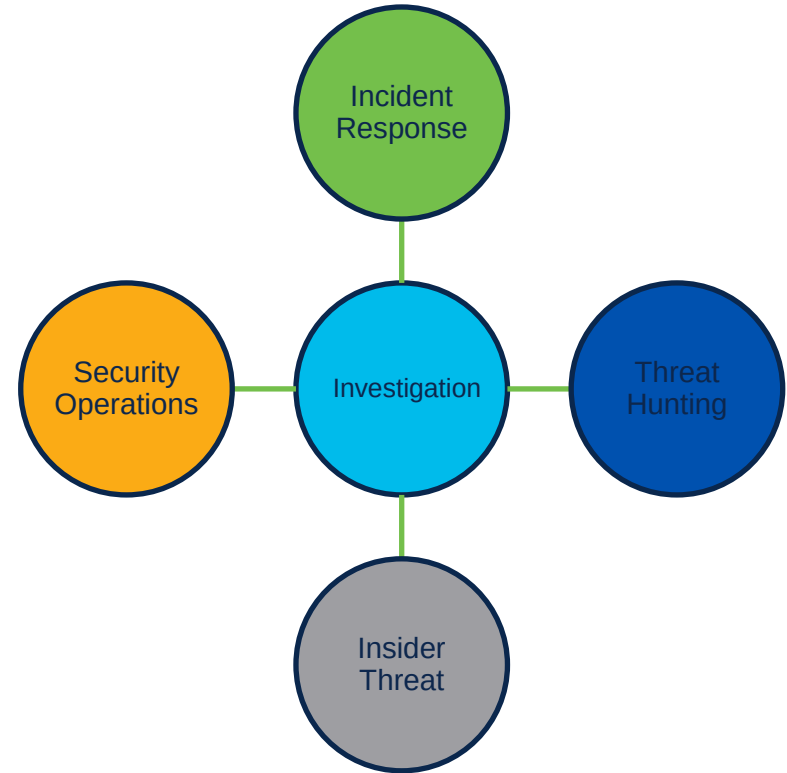
- make a check to find out something.

"when you didn't turn up, I thought I'd better come back to investigate"



Investigating is a core competency

- When something is detected, we want to figure out what happened
- Who, what, where, when, why, how?
- Investigating can be reactive or proactive



Luckily everything is captured in Splunk

- Microsoft Sysmon
- Windows Events
- Windows Registry
- IIS
- Splunk Stream (wire data)
- Suricata
- Fortigate (NGFW)

The screenshot displays the Splunk Enterprise Search & Reporting interface. The search bar contains the query: `sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" EventCode=2 TargetFilename="C:\\Users\\bob.smith.WAYNECORP\\..."`. Below the search bar, a visualization shows a timeline of events. The left sidebar lists fields under 'SELECTED FIELDS' and 'INTERESTING FIELDS'. The main panel shows a list of events with columns for Time and Event. The first event is dated 8/24/16 at 5:17:17.000 PM and contains XML data from a Sysmon event log.

Time	Event
8/24/16 5:17:17.000 PM	<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"><System-Provider Name="Microsoft-Windows-Sysmon" Guid="{5770385F-C22A-43E8-BF8C-06F5698FB09}" /><EventID><Version><Level><Level><Task><Task><Opcode><Opcode><Keywords><Keywords><TimeCreated SystemTime="2016-08-24T17:17:17.228734.608Z" /><EventRecordID>427556</EventRecordID><Correlation><Execution ProcessID="1376" ThreadID="1768" /><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>web0185desk.waynecorpinc.local</Computer><Security UserID="S-1-5-18" /></System><EventData><Data Name="UtcTime">2016-08-24 17:17:17.228</Data><Data Name="ProcessGuid">{0F2076F8-D61F-5780-0000-0018E0849500}</Data><Data Name="ProcessId">2404</Data><Data Name="Image">C:\\Program Files (x86)\\Internet Explorer\\iexplore.exe</Data><Data Name="TargetFilename">C:\\Users\\bob.smith.WAYNECORP\\AppData\\Roaming\\Microsoft\\Windows\\Recent\\CustomDestinations\\J74ZCQXW19IEBUTP2ZF.tmp</Data><Data Name="CreationUtcTime">2016-08-16 20:58:37.142</Data><Data Name="PreviousCreationUtcTime">2016-08-24 17:17:17.228</Data></EventData></Event>
8/24/16 5:17:17.000 PM	<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"><System-Provider Name="Microsoft-Windows-Sysmon" Guid="{5770385F-C22A-43E8-BF8C-06F5698FB09}" /><EventID><Version><Level><Level><Task><Task><Opcode><Opcode><Keywords><Keywords><TimeCreated SystemTime="2016-08-24T17:17:17.228734.608Z" /><EventRecordID>427556</EventRecordID><Correlation><Execution ProcessID="1376" ThreadID="1768" /><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>web0185desk.waynecorpinc.local</Computer><Security UserID="S-1-5-18" /></System><EventData><Data Name="UtcTime">2016-08-24 17:17:17.228</Data><Data Name="ProcessGuid">{0F2076F8-D61F-5780-0000-0018E0849500}</Data><Data Name="ProcessId">2404</Data><Data Name="Image">C:\\Program Files (x86)\\Internet Explorer\\iexplore.exe</Data><Data Name="TargetFilename">C:\\Users\\bob.smith.WAYNECORP\\AppData\\Roaming\\Microsoft\\Windows\\Recent\\CustomDestinations\\J74ZCQXW19IEBUTP2ZF.tmp</Data><Data Name="CreationUtcTime">2016-08-16 20:58:37.142</Data><Data Name="PreviousCreationUtcTime">2016-08-24 17:17:17.228</Data></EventData></Event>

Splunk commands used

metadata

stats – distinct count, count, values, average, AS

eval – lower, length, round

table

AND OR NOT

sort

reverse

head

transaction

rex

search

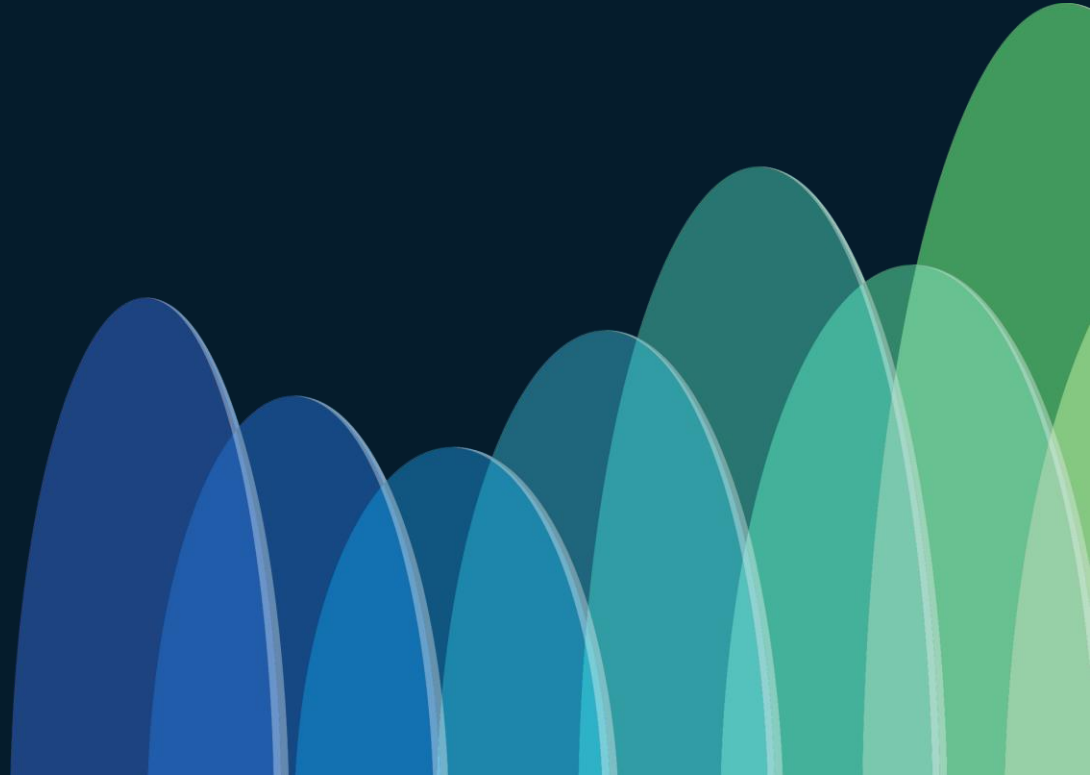
inputlookup

outputlookup

fields

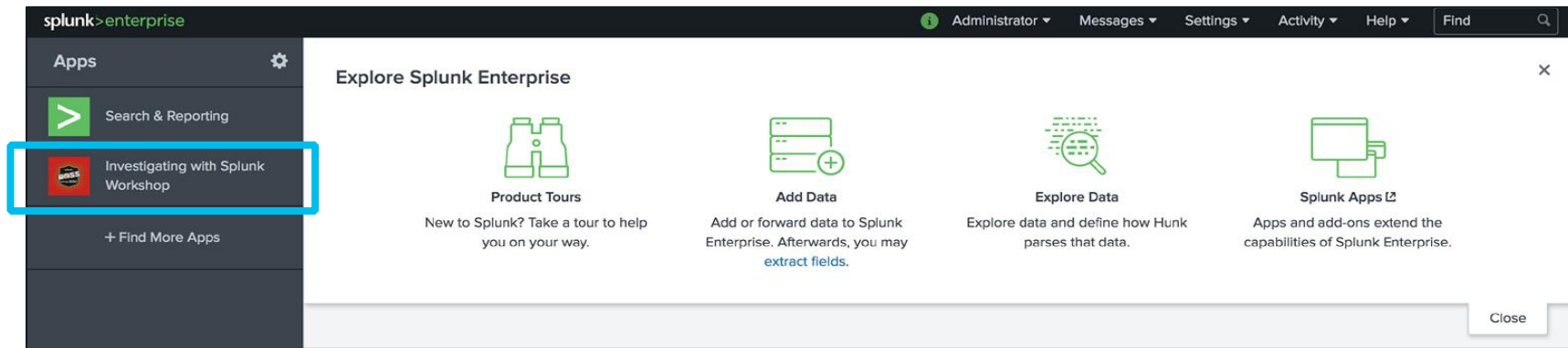
lookup

Let's Investigate



Starting point

Please make sure you are logged in and seeing this window



CISCO *Live!*

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Screen layout

What Kinds of Events Do I Have?

EditExport ...

Background

The SPL command **metadata** can be used to search for the same kind of information that is found in the Data Summary with the added bonus of being able to search within a specific index, if desired. All time values are returned in EPOCH time so to make the output user readable, the eval command should be used to provide more human-friendly formatting.

In this example, we will search the **botsv1** index and return a listing of all the sourcetypes that can be found as well a count of events and the first time and last time seen.

Resources

- metadata command - Splunk Docs

Sourcetypes

- We are looking for this list!

metadata Command

| metadata type=sourcetypes index=botsv1

Run Search in New Tab

We may not want to go to the main screen and open a pop-up or we might want to look for data inside specific indexes. To do that, **metadata** can be used to search with the added bonus of being able to search within a specific index. The one caveat to the **metadata** command is that all time values are returned in EPOCH time so to make them look nice for reporting, an eval command should be used to change the formatting to the layout you want. That said, it is a very effective command to use to explore a Splunk instance, and then additional Splunk commands can be fed from the output of the command as needed.

Listing of all data by sourcetype using the metadata command

firstTime ↕	lastTime ↕	recentTime ↕	sourcetype ↕	totalCount ↕	type ↕
1470009975	1472428471	1473366069	WinEventLog:Application	5173	sourcetypes
1470009600	1472428740	1473366071	WinEventLog:Security	14218920	sourcetypes
1470009654	1472428629	1473366070	WinEventLog:System	12226	sourcetypes
1472055742	1472063262	1472063262	WinRegistry	74720	sourcetypes
1470009602	1472428739	1473366114	XmlWinEventLog:Microsoft-Windows-Sysmon/Operational	830389	sourcetypes
1470009613	1472428700	1473366112	fgt_event	53422	sourcetypes

What kinds of events do I have?

What Kinds of Events Do I Have?

EditExport...

Background

The SPL command **metadata** can be used to search for the same kind of information that is found in the Data Summary with the added bonus of being able to search within a specific index, if desired. All time values are returned in EPOCH time so to make the output user readable, the eval command should be used to provide more human-friendly formatting.

In this example, we will search the **botsv1** index and return a listing of all the sourcetypes that can be found as well a count of events and the first time and last time seen.

Resources

- [metadata command - Splunk Docs](#)

Sourcetypes

- We are looking for this list!

metadata Command

| metadata type=sourcetypes index=botsv1

Run Search in New Tab

We may not want to go to the main screen and open a pop-up or we might want to look for data inside specific indexes. To do that, **metadata** can be used to search with the added bonus of being able to search within a specific index. The one caveat to the **metadata** command is that all time values are returned in EPOCH time so to make them look nice for reporting, an eval command should be used to change the formatting to the layout you want. That said, it is a very effective command to use to explore a Splunk instance, and then additional Splunk commands can be fed from the output of the command as needed.

Listing of all data by sourcetype using the metadata command

firstTime ↕	lastTime ↕	recentTime ↕	sourcetype ↕	totalCount ↕	type ↕
1470009975	1472428471	1473366069	WinEventLog:Application	5173	sourcetypes
1470009600	1472428740	1473366071	WinEventLog:Security	14218920	sourcetypes
1470009654	1472428629	1473366070	WinEventLog:System	12226	sourcetypes
1472055742	1472063262	1472063262	WinRegistry	74720	sourcetypes
1470009602	1472428739	1473366114	XmlWinEventLog:Microsoft-Windows-Sysmon/Operational	830389	sourcetypes
1470009613	1472428700	1473366112	fgt_event	53422	sourcetypes

APT Scenario



APT Prologue

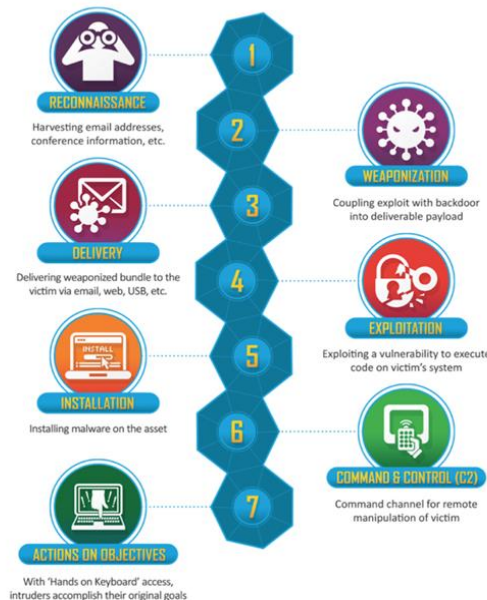
[Edit](#)[Export](#)[...](#)

Scenario #1 - APT

In this scenario, reports of the below graphic come in from your user community when they visit the Wayne Enterprises website, and some of the reports reference "P01s0n1vy." In case you are unaware, P01s0n1vy is an APT group that has targeted Wayne Enterprises. Your goal, as Alice, is to investigate the defacement, with an eye towards reconstructing the attack via the Lockheed Martin Kill Chain.

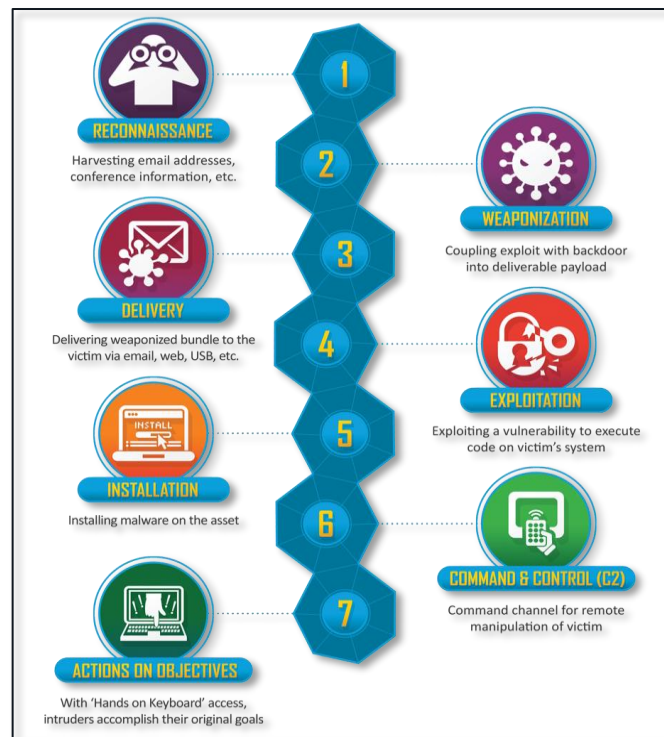
**YOUR
SITE
HAS BEEN
DEFACED**

P01s0n1vy was HERE
Deal with it, Admin



Lockheed Martin Cyber Kill Chain

- Method for characterising different parts of an attack for intelligence gathering, situational awareness and better understanding of a multi-stage threat
- Does not apply to all threats but is a good place to start for targeted attacks



Start investigating!

During an investigation, there are a number of questions that need to be answered.

- Some questions will build off of earlier questions
- Pro tip: have a notepad and pencil at the ready!

We created these questions to guide your investigation, there are more questions you can ask and more badness you can find!

- After each question, the instructor will set aside a few minutes to allow you to find the answer
- We will re-group to review the question and the process we took
- Reference the app if you get stuck or ask your instructors
- We will provide a couple of hints to get you started...

Finding the IP scanning your web server

Kill Chain Phase: Reconnaissance

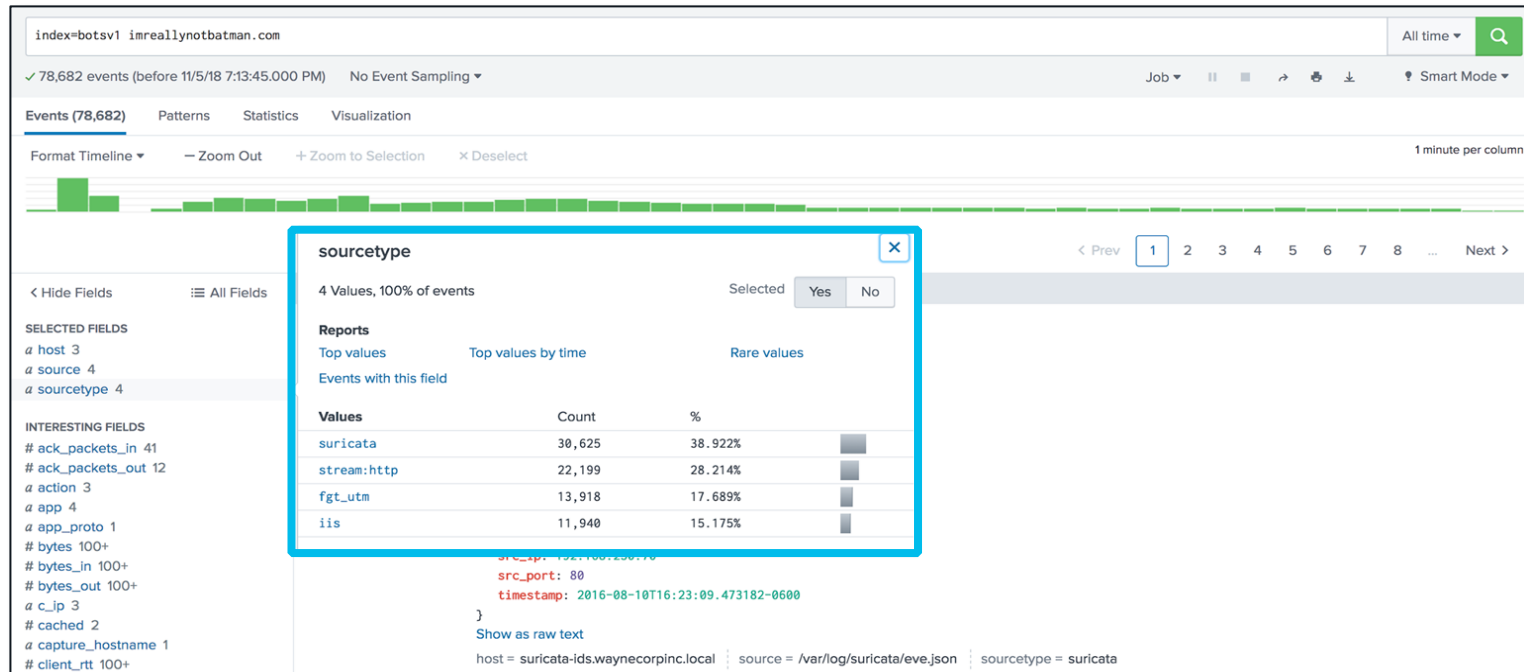
What is the likely IP address of someone from the Po1s0n1vy group scanning imrealllynotbatman.com for web application vulnerabilities?

Hints

- All searches used today will have an index of botsv1
 - index=botsv1
- The field src is the field you are looking for
- Focusing your search on specific sourcetypes will be helpful

Identify source types associated with search values

Kill Chain Phase: Reconnaissance



Finding source addresses

Kill Chain Phase: Reconnaissance

index=botsv1 imreallynotbatman.com during Wed, Aug 10, 2016

✓ 78,682 events (8/10/16 12:00:00.000 AM to 8/11/16 12:00:00.000 AM) No Event Sampling

Events (78,682) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 hour per column

< Hide Fields All Fields

SELECTED FIELDS

- a host 4
- a source 4
- a sourcetype 4
- a src 3

INTERESTING FIELDS

- # ack_packets_in 41
- # ack_packets_out 12
- a action 4
- a app 3
- a app_proto 1
- # bytes 100+
- # bytes_in 100+
- # bytes_out 100+
- a c_ip 3
- # cached 2
- a capture_hostname 1

SRC

3 Values, 84.825% of events Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
40.80.148.42	51,130	76.608%
192.168.250.70	11,493	17.22%
23.22.63.114	4,119	6.172%

src_port: 80
timestamp: 2016-08-10T16:23:09.473182-0600
}
Show as raw text
host = suricata-ids.waynecorpinc.local | source = /var/log/suricata/eve.json | sourcetype = suricata

Selecting a sourcetype and searching for source address

index=botsv1 imreallynotbatman.com sourcetype=stream:http

✓ 22,199 events (before 11/5/18 7:26:39.000 PM) No Event Sampling

Events (22,199) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 minute per column

List Format 20 Per Page

< Prev 1 2 3 4 5 6 7 8 ... Next >

< Hide Fields All Fields

SELECTED FIELDS

- a host 1
- a source 1
- a sourcetype 1
- a src 2

INTERESTING FIELDS

- a accept 9
- # ack_packets_in 41
- # ack_packets_out 12
- a action 2
- a app 1
- # bytes 100+
- # bytes_in 100+
- # bytes_out 100+
- a c_ip 2
- # cached 2

src

2 Values, 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	20,964	94.437%
23.22.63.114	1,235	5.563%

client_rtt_sum: 0
cs_content_length: 395
cs_content_type: text/html; charset=UTF-8
cs_date: Wed, 10 Aug 2016 22:22:27 GMT
cs_version: 1.1

Validation with suricata

index=botsv1 imreallynotbatman.com src=40.80.148.42 sourcetype=suricata All time Q

✓ 17,484 events (before 11/5/18 7:31:58.000 PM) No Event Sampling Job || ■ → ⌵ ⌴ Smart Mode

Events (17,484) Patterns Statistics Visualization

Format Timeline — Zoom Out + Zoom to Selection × Deselect 1 minute per column

List Format 20 Per Page < Prev 1 2 3 4 5 6 7 8 ... Next >

< Hide Fields All Fields	i Time	Event
SELECTED FIELDS a host 1 a source 1 a sourcetype 1 a src 1 INTERESTING FIELDS a app 1 a app_proto 1 # bytes 100+ # date_hour 2 # date_mday 1 # date_minute 43 a date_month 1 # date_second 60 a date_wday 1	> 8/10/16 10:21:19.243 PM	<pre>{ [-] dest_ip: 192.168.250.70 dest_port: 80 event_type: http flow_id: 2333561742 http: { [+] } in_iface: eth1 proto: TCP src_ip: 40.80.148.42 src_port: 49500 timestamp: 2016-08-10T16:21:19.243883-0600 tx_id: 1 }</pre> <p>Show as raw text</p> <p>host = suricata-ids.waynecorpinc.local source = /var/log/suricata/eve.json sourcetype = suricata src = 40.80.148.42</p>



More fields...

`a tag 3`
`a tag::eventtype 3`
`# timeendpos 1`
`a timestamp 100+`
`# timestartpos 1`
`a transport 1`
`a url 100+`
`a vendor 1`

19 more fields

+ Extract New Fields

Select Fields

Select All Within Filter

Deselect All

All fields ▾

sig

×

+ Extract New Fields

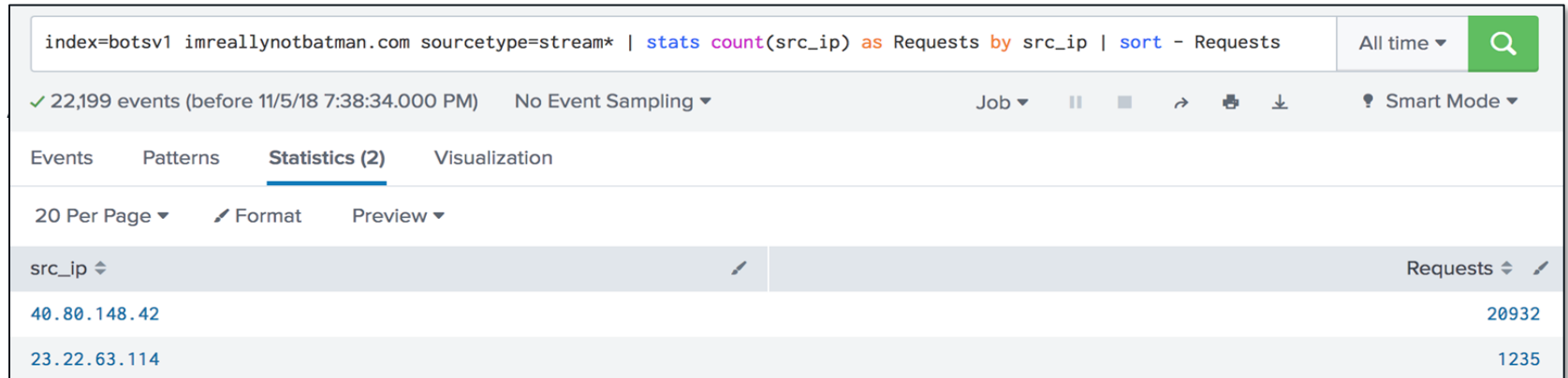
i	✓ ▾	Field ▾	# of Values ▾	Event Coverage ▾	Type ▾
>	☐	alert.signature	46	2.71%	String
>	☐	alert.signature_id	46	2.71%	Number
▾	☐	signature	46	2.71%	String
<div>Reports</div> <div>Top values</div> <div>Top values by time</div> <div>Rare values</div> <div>Events with this field</div>					
<div><div>ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt</div><div>103</div><div>21.776%</div><div></div></div> <div><div>ET WEB_SERVER Onmouseover= in URI - Likely Cross Site Scripting Attempt</div><div>48</div><div>10.148%</div><div></div></div> <div><div>ET WEB_SERVER Possible XXE SYSTEM ENTITY in POST BODY.</div><div>41</div><div>8.668%</div><div></div></div> <div><div>SURICATA HTTP Host header invalid</div><div>35</div><div>7.4%</div><div></div></div> <div><div>ET WEB_SERVER Possible SQL Injection Attempt SELECT FROM</div><div>33</div><div>6.977%</div><div></div></div> <div><div>ET WEB_SERVER SQL Injection Select Sleep Time Delay</div><div>32</div><div>6.765%</div><div></div></div> <div><div>ET WEB_SERVER Possible CVE-2014-6271 Attempt</div><div>18</div><div>3.805%</div><div></div></div> <div><div>ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers</div><div>18</div><div>3.805%</div><div></div></div> <div><div>ET WEB_SERVER PHP tags in HTTP POST</div><div>13</div><div>2.748%</div><div></div></div> <div><div>GPL WEB_SERVER global.asa access</div><div>12</div><div>2.537%</div><div></div></div>					
>	☐	suricata_signature_id	46	2.71%	String

Finding the IP scanning your web server

Kill Chain Phase: Reconnaissance

What is the likely IP address of someone from the Po1s0n1vy group scanning imreallynotbatman.com for web application vulnerabilities?

- 40.80.148.42



The screenshot shows the Cisco Live! interface with a search query: `index=botsv1 imreallynotbatman.com sourcetype=stream* | stats count(src_ip) as Requests by src_ip | sort - Requests`. The results show 22,199 events. The 'Statistics (2)' tab is active, displaying a table with two rows of data.

src_ip	Requests
40.80.148.42	20932
23.22.63.114	1235

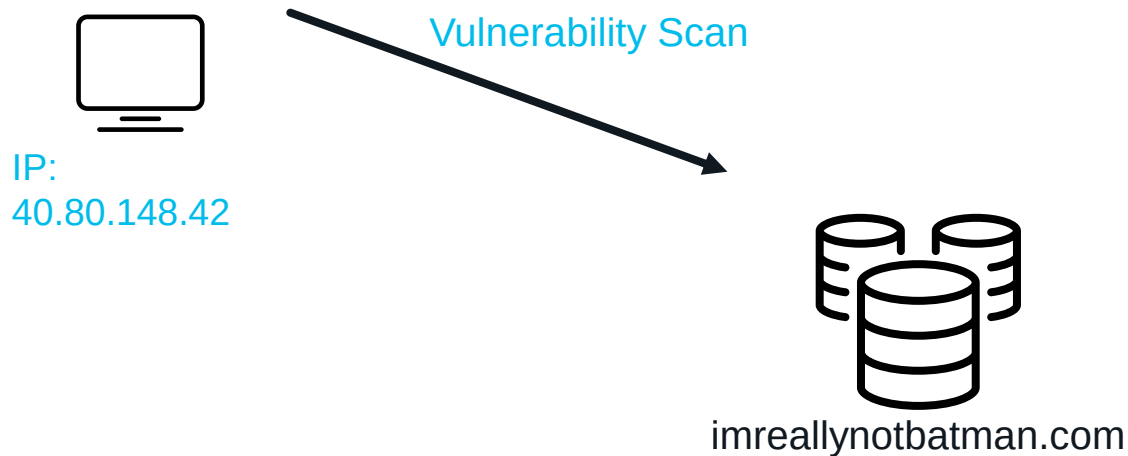
Kill Chain

IP Scanning the Web Server:

40.80.148.42



APT picture



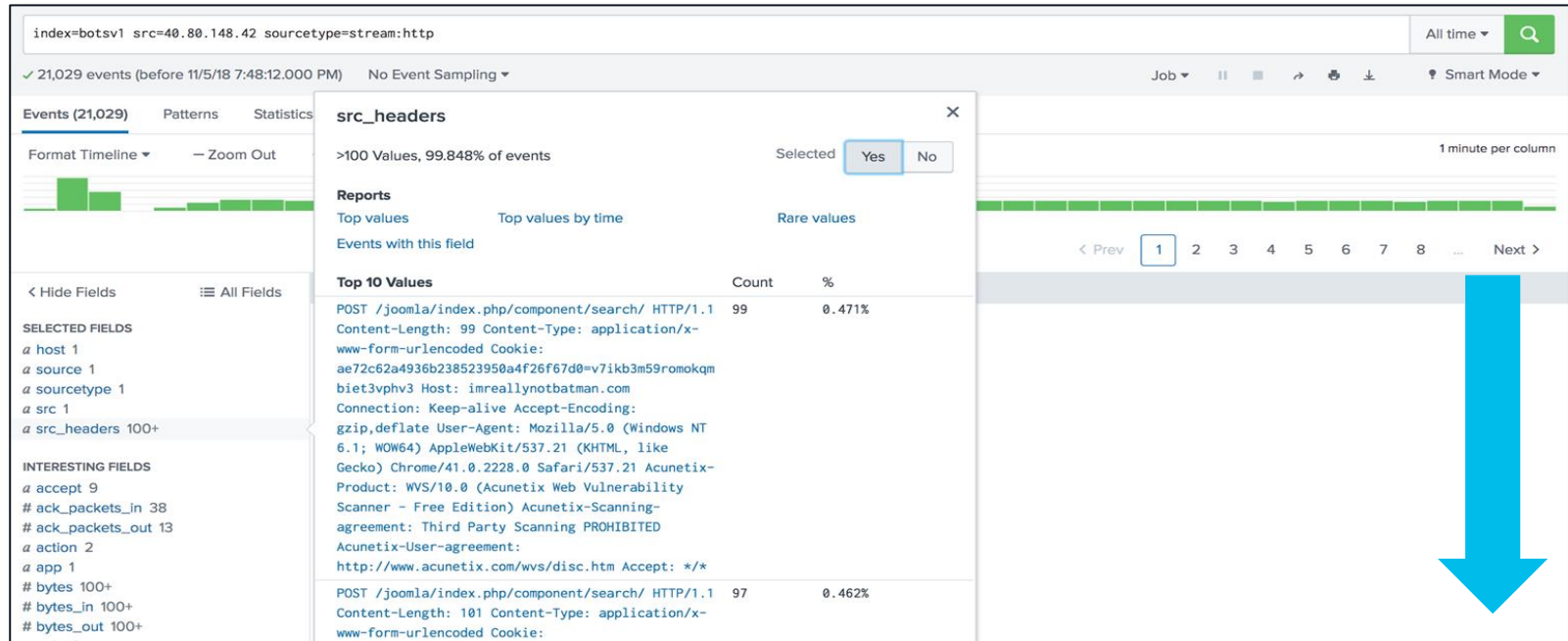
Identifying the web vulnerability scanner

Kill Chain Phase: Reconnaissance

- What company created the web vulnerability scanner used by Po1s0n1vy?
- Hints
 - Use the src found in the prior question as the source of the scans
 - The sourcetype stream:http provides a good deal of insight into communications between a web browser and server
 - User agent strings can provide value here
 - If you don't know what a term is, Google it!

Looking at src_headers

Kill Chain Phase: Reconnaissance



Looking at src_headers

Top 10 Values	Count	%
POST /joomla/index.php/component/search/ HTTP/1.1 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: */*	99	0.471%
POST /joomla/index.php/component/search/ HTTP/1.1 Content-Length: 101 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: */*	97	0.462%

Looking at http_user_agent strings

index=botsv1 src=40.80.148.42 sourcetype=stream:http

21,029 events (before 11/5/18 7:53:25.000 PM) No Event Sampling

Job Smart Mode

Events (21,029) Patterns Statistics

Format Timeline Zoom Out

1 minute per column

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Top 10 Values

	Count	%
Mozilla/5.0 (Windows NT 6.1; WOW64)	20,850	99.385%
AppleWebKit/537.21 (KHTML, like Gecko)		
Chrome/41.0.2228.0 Safari/537.21		
Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko	80	0.381%
!(())&&! * *	1	0.005%
";print(md5(acunetix_wvs_security_test));\$a="	1	0.005%
\${nslookup 0GlaVBmt}	1	0.005%
\${10000071+9999854}	1	0.005%
\${@print(md5(acunetix_wvs_security_test))}	1	0.005%
\${@print(md5(acunetix_wvs_security_test))}\	1	0.005%
&nslookup 40z0JB6D&``"0&nslookup 40z0JB6D&``	1	0.005%
' "	1	0.005%

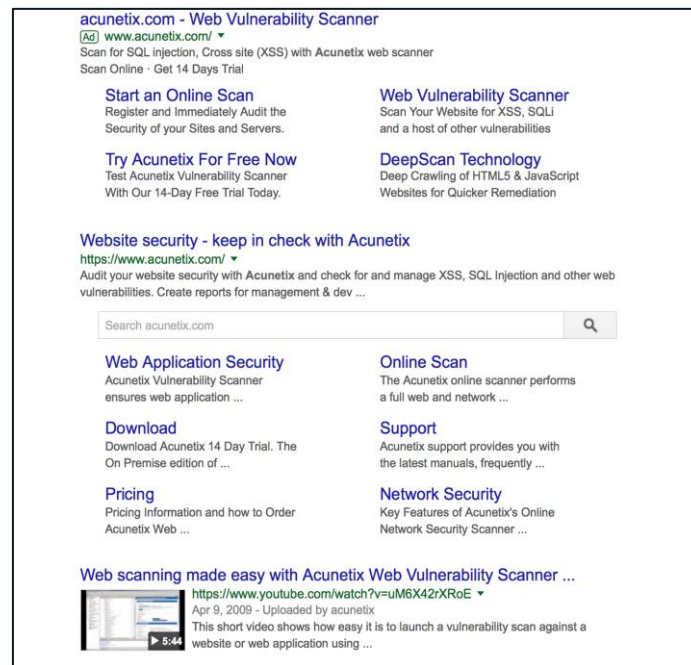
< Prev 1 2 3 4 5 6 7 8 ... Next >



Research on the internet

If you see something in the logs
you don't understand, Google it!

- What If You Don't Know What Acunetix Is?



The screenshot shows the Acunetix website with the following content:

- acunetix.com - Web Vulnerability Scanner**
www.acunetix.com/
Scan for SQL injection, Cross site (XSS) with Acunetix web scanner
Scan Online · Get 14 Days Trial
- Start an Online Scan**
Register and Immediately Audit the Security of your Sites and Servers.
- Web Vulnerability Scanner**
Scan Your Website for XSS, SQLi and a host of other vulnerabilities
- Try Acunetix For Free Now**
Test Acunetix Vulnerability Scanner With Our 14-Day Free Trial Today.
- DeepScan Technology**
Deep Crawling of HTML5 & JavaScript Websites for Quicker Remediation
- Website security - keep in check with Acunetix**
<https://www.acunetix.com/>
Audit your website security with Acunetix and check for and manage XSS, SQL Injection and other web vulnerabilities. Create reports for management & dev ...
- Search bar: Search acunetix.com
- Web Application Security**
Acunetix Vulnerability Scanner ensures web application ...
- Online Scan**
The Acunetix online scanner performs a full web and network ...
- Download**
Download Acunetix 14 Day Trial. The On Premise edition of ...
- Support**
Acunetix support provides you with the latest manuals, frequently ...
- Pricing**
Pricing Information and how to Order Acunetix Web ...
- Network Security**
Key Features of Acunetix's Online Network Security Scanner ...
- Web scanning made easy with Acunetix Web Vulnerability Scanner ...**
<https://www.youtube.com/watch?v=uM6X42rXR0E>
Apr 9, 2009 · Uploaded by acunetix
This short video shows how easy it is to launch a vulnerability scan against a website or web application using ...

Identifying the web vulnerability scanner

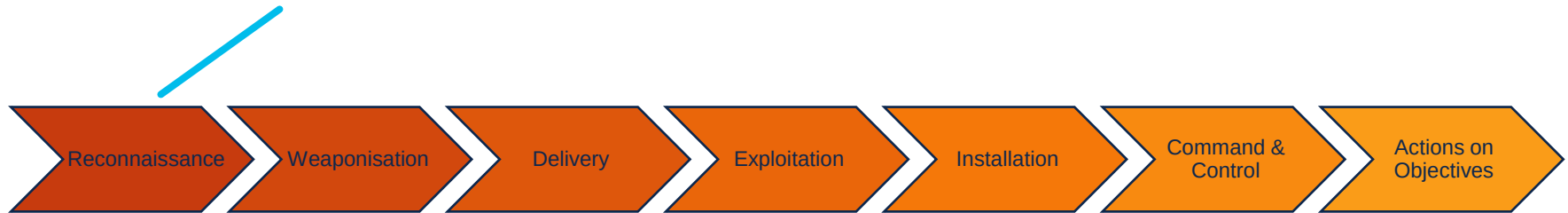
Kill Chain Phase: Reconnaissance

- What company created the web vulnerability scanner used by P01s0n1vy?
 - Acunetix

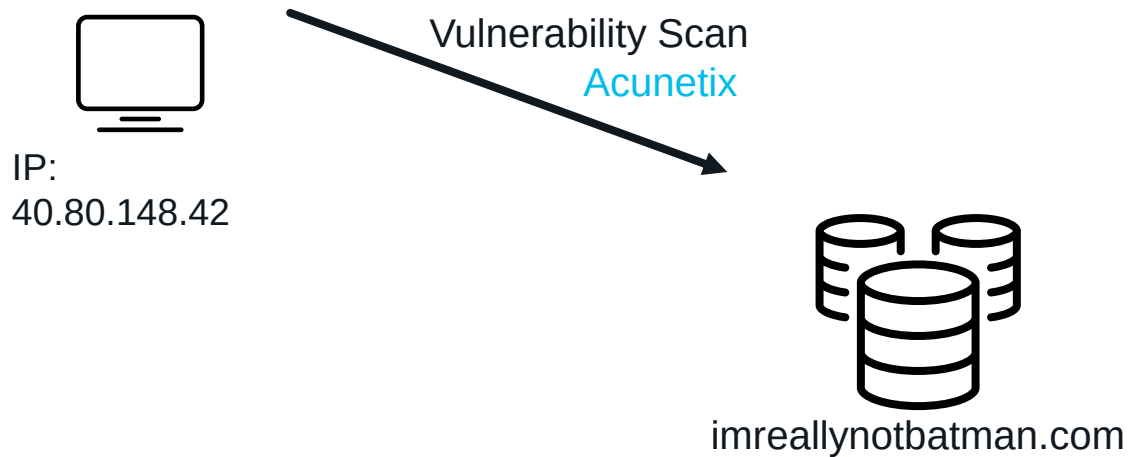
Kill Chain

IP Scanning the Web Server: 40.80.148.42

Web Vulnerability Scanner: [Acunetix](#)



APT picture



Determining which web server is the target

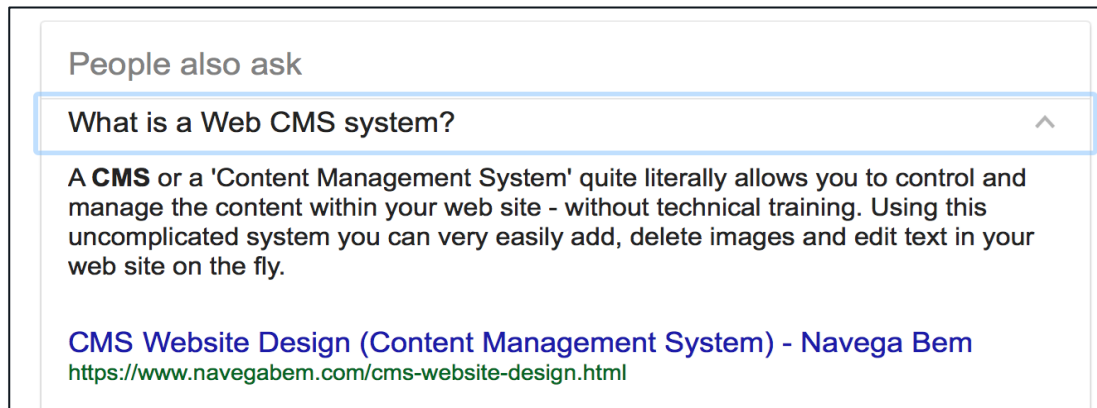
Kill Chain Phase: Reconnaissance

- What content management system is `imreallynotbatman.com` likely using?

- Hints

- If you aren't sure what a content management system is, Google it.
- Sourcetypes that are relevant to web communication are helpful
- URIs contain information that will lead you in the right direction

Where to start?



- Based on that in what kind of logs should I look?
- Do we have the IP of the system in question?
- Based on our previous findings, probably so...

Where to start?

index=botsv1 src=40.80.148.42 sourcetype=stream:http

21,029 events (before 11/5/18 8:07:25.000 PM) No Event Sampling

Events (21,029) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

1 minute per column

< Prev 1 2 3 4 5 6 7 8 ... Next >

dest

2 Values, 100% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
192.168.250.70	21,028	99.995%
192.168.250.40	1	0.005%

capture_hostname: demo-01

client_rtt: 0

client_rtt_packets: 0

client_rtt_sum: 0

cs_content_length: 395

cs_content_type: text/html; charset=UTF-8

cs_date: Wed, 10 Aug 2016 22:22:27 GMT

cs_version: 1.1

Digging into the URI

index=botsv1 dest=192.168.250.70 sourcetype=stream:http All time

✓ 22,671 events (before 11/5/18 8:13:56.000 PM) No Event Sampling

Events (22,671) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 day per column

uri

>100 Values, 99.859% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Top 10 Values	Count	%
/joomla/index.php/component/search/	14,218	62.803%
/joomla/administrator/index.php	1,252	5.53%
/joomla/index.php	798	3.525%
/	676	2.986%
/joomla/agent.php	194	0.857%
/windows/win.ini	33	0.146%
/joomla/media/jui/js/jquery-migrate.min.js	18	0.08%
/joomla/media/jui/js/jquery-noconflict.js	18	0.08%
/joomla/media/jui/js/bootstrap.min.js	17	0.075%
	14	0.062%

image/png, */*



Digging into the URI

External Research

- Much like the previous question, if you see values you have never seen before, Google is your friend

People also ask

What is a Web CMS system? ^

A **CMS** or a 'Content Management System' quite literally allows you to control and manage the content within your web site - without technical training. Using this uncomplicated system you can very easily add, delete images and edit text in your web site on the fly.

[CMS Website Design \(Content Management System\) - Navega Bem](https://www.navegabern.com/cms-website-design.html)
<https://www.navegabern.com/cms-website-design.html>

Search for: [What is a Web CMS system?](#)

What is WordPress content management system? v

What is the Joomla! ^

Joomla is an open source platform on which Web sites and applications can be created. It is a content management system (CMS) which connects your site to a MySQLi, MySQL, or PostgreSQL database in order to make content management and delivery easier on both the site manager and visitor.

[What is Joomla? - RocketTheme - Documentation](http://www.rockettheme.com/docs/joomla/platform)
www.rockettheme.com/docs/joomla/platform

Search for: [What is the Joomla?](#)

Looking for confirmation

Add The Response Code condition to ensure we have successful page loads

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

Generate a count by URI to see what values are most frequently seen

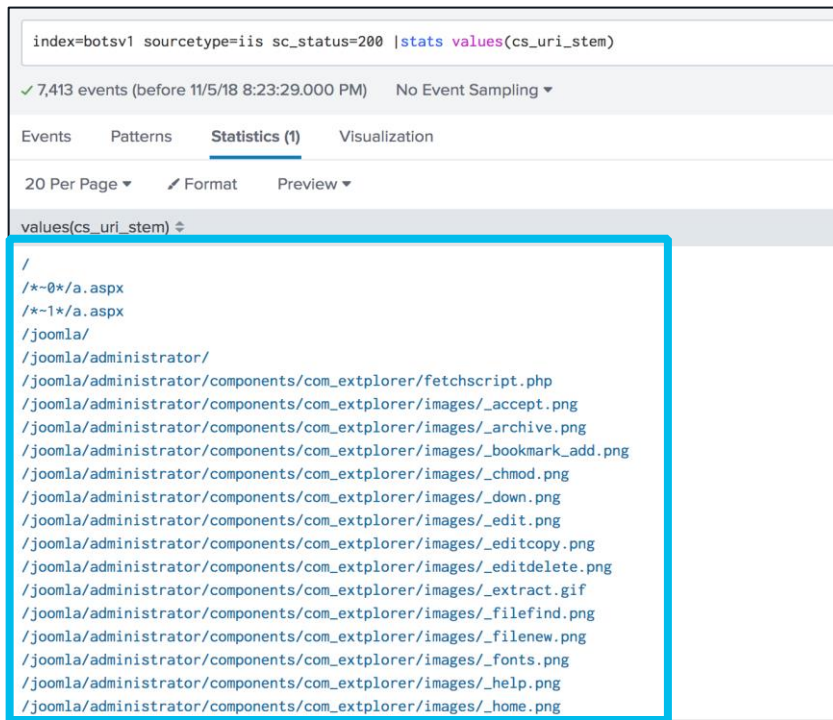
Sort descending by count so the greatest values come to the top

Our results? Lots of Joomla

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

uri ↕	count ↕
/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-migrate.min.js	17
/joomla/media/jui/js/jquery-noconflict.js	17
/joomla/media/jui/js/bootstrap.min.js	16
/joomla/media/system/js/html5fallback.js	13

Finding the answer with IIS



The screenshot shows a Splunk search interface. At the top, the search query is `index=botsv1 sourcetype=iis sc_status=200 |stats values(cs_uri_stem)`. Below the query, it indicates 7,413 events were found before 11/5/18 8:23:29.000 PM, with 'No Event Sampling' selected. The 'Statistics (1)' tab is active, showing a table with one column, `values(cs_uri_stem)`. A blue box highlights the list of URI stems returned by the search.

```
index=botsv1 sourcetype=iis sc_status=200 |stats values(cs_uri_stem)
```

✓ 7,413 events (before 11/5/18 8:23:29.000 PM) No Event Sampling ▾

Events Patterns **Statistics (1)** Visualization

20 Per Page ▾ ✎ Format Preview ▾

`values(cs_uri_stem)` ⇅

- /
- /~-0*/a.aspx
- /~-1*/a.aspx
- /joomla/
- /joomla/administrator/
- /joomla/administrator/components/com_explorer/fetchscript.php
- /joomla/administrator/components/com_explorer/images/_accept.png
- /joomla/administrator/components/com_explorer/images/_archive.png
- /joomla/administrator/components/com_explorer/images/_bookmark_add.png
- /joomla/administrator/components/com_explorer/images/_chmod.png
- /joomla/administrator/components/com_explorer/images/_down.png
- /joomla/administrator/components/com_explorer/images/_edit.png
- /joomla/administrator/components/com_explorer/images/_editcopy.png
- /joomla/administrator/components/com_explorer/images/_editdelete.png
- /joomla/administrator/components/com_explorer/images/_extract.gif
- /joomla/administrator/components/com_explorer/images/_filefind.png
- /joomla/administrator/components/com_explorer/images/_filenew.png
- /joomla/administrator/components/com_explorer/images/_fonts.png
- /joomla/administrator/components/com_explorer/images/_help.png
- /joomla/administrator/components/com_explorer/images/_home.png

Determining which web server is the target

Kill Chain Phase: Reconnaissance

- What content management system is `imreallynotbatman.com` likely using?
 - Joomla

Kill Chain

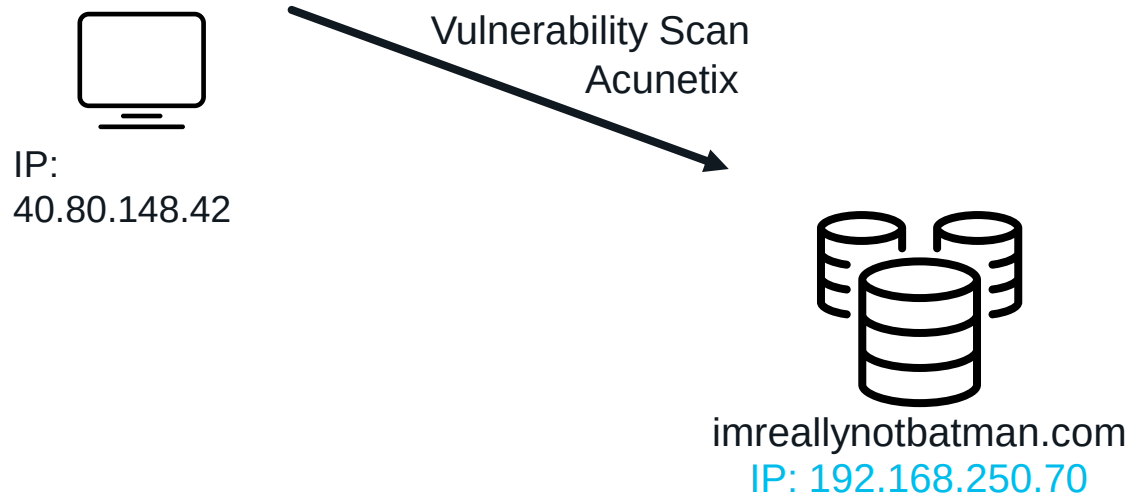
IP Scanning the Web Server: 40.80.148.42

Web Vulnerability Scanner: Acunetix

Which Web Server?: [192.168.250.70/Joomla](#)



APT picture



Identifying where a brute force attack originated

Kill Chain Phase: Exploitation

- What IP address is likely attempting a brute force password attack against `imreallynotbatman.com`?
- Hints
 - A sourcetype that can see web browser to server communication would be very helpful
 - Knowing the destination IP address of the web server being attacked would be good
 - The web method will be helpful to focus our search
 - The field `form_data` will have user names and passwords in it if you look closely

Looking in Wire Data - stream:http

The screenshot shows the Cisco Live! interface for analyzing wire data. The search bar at the top contains 'index=botsv' and 'sourcetype=stream:http'. The main view displays 39,009 events. A modal window titled 'src' is open, showing a table of the top 10 values for the 'src' field. The table has columns for the value, count, and percentage. A large blue arrow points downwards on the right side of the interface.

Top 10 Values	Count	%
40.80.148.42	21,029	53.908%
23.22.63.114	1,429	3.663%
192.168.2.50	818	2.097%
192.168.250.100	650	1.666%
169.229.3.91	210	0.538%
38.130.201.245	196	0.502%
45.33.5.165	180	0.461%
192.168.225.111	175	0.449%
192.168.229.203	71	0.182%
192.168.225.96	59	0.151%

Refine our search with the web server address

index=botsv1 sourcetype=stream:http dest=192.168.250.70

✓ 22,671 events (before 11/5/18 8:41:35.000 PM) No Event Sampling

Events (22,671) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 day per column

List Format 20 Per Page

< Prev 1 2 3 4 5 6 7 8 ... Next >

< Hide Fields All Fields

SELECTED FIELDS

- a dest 1
- a host 1
- a http_user_agent 100+
- a source 1
- a sourcetype 1
- a src 3
- a src_headers 100+
- a uri 100+

INTERESTING FIELDS

- a accept 100+
- # ack_packets_in 41
- # ack_packets_out 13

SRC

3 Values, 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	21,028	92.753%
23.22.63.114	1,429	6.303%
192.168.2.50	214	0.944%

Same search, different pivot

The screenshot shows the Cisco Live! interface with a search query: `index=botsv1 sourcetype=stream:http dest=192.168.250.70`. The search results show 22,671 events. A pivot table for the `http_method` field is displayed, showing the top values by time. The pivot table has columns for Values, Count, and %. The values are POST (15,559, 68.781%), GET (7,054, 31.183%), OPTIONS (5, 0.022%), CONNECT (1, 0.004%), PROPFIND (1, 0.004%), and TRACE (1, 0.004%). A large blue arrow points down from the pivot table to the bottom right corner of the interface.

index=botsv1 sourcetype=stream:http dest=192.168.250.70 All time

✓ 22,671 events (before 11/5/18 8:41:35.000 PM) No Event Sampling

Job || [] ↶ ↷ ⬇ ⬆ ⬇ ⬆ Smart Mode

Events (22,671) Patterns Statistics Visualization

Format Timeline ↕ Zoom Out + Zoom to Selection × Deselect 1 day per column

image/png, */*

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
POST	15,559	68.781%
GET	7,054	31.183%
OPTIONS	5	0.022%
CONNECT	1	0.004%
PROPFIND	1	0.004%
TRACE	1	0.004%

< Prev 1 2 3 4 5 6 7 8 ... Next >

Adding a HTTP method to narrow our results

index=botsv1 sourcetype=stream:http dest="192.168.250.70" **http_method=POST** All time 🔍

✓ 15,559 events (before 11/5/18 8:46:56.000 PM) No Event Sampling ▾ Job ▾ || ■ ➔ 📄 ⬇️ 🔔 Smart Mode ▾

Events (15,559) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect 1 minute per column

List ▾ ✎ Format 20 Per Page ▾ < Prev 1 2 3 4 5 6 7 8 ... Next >

< Hide Fields ≡ All Fields

SELECTED FIELDS

- a dest 1
- a host 1
- a http_method 1
- a http_user_agent 3
- a source 1
- a sourcetype 1
- a src 2
- a src_headers 100+
- a uri 72

INTERESTING FIELDS

- a accept 2
- # ack_packets_in 14

src 2 Values, 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	15,148	97.358%
23.22.63.114	411	2.642%



Finding passwords in HTTP Wire Data

index=botstv1 sourcetype=stream:http dest="192.168.250.70" http_method=POST form_data=*username*passwd*

☐ dest ▾	192.168.250.70
☐ dest_content ▾	<head><title>Document Moved</title></head> <body><h1>Object Moved</h1>This document may be found here</body>
☐ dest_headers ▾	HTTP/1.1 303 See other Content-Type: text/html; charset=UTF-8 Location: http://imreallynotbatman.com/joomla/administrator/index.php Server: Microsoft-IIS/8.5 X-Powered-By: PHP/5.5.38 Date: Wed, 10 Aug 2016 21:48:05 GMT Content-Length: 182
☐ dest_ip ▾	192.168.250.70
☐ dest_mac ▾	00:0C:29:C4:02:7E
☐ dest_port ▾	80
☐ duplicate_packets_in ▾	1
☐ duplicate_packets_out ▾	1
☐ duration ▾	1754955
☐ endtime ▾	2016-08-10T21:48:05.858372Z
☐ eventtype ▾	stream_network_traffic (communicate network) stream_web (web)
☐ form_data ▾	username=admin&passwd=batman&option=com_login&task=login&return=aW5kZXgucGhw&e5ec827a3f67ce0efc546d81f7356acc=1
☐ http_comment ▾	HTTP/1.1 303 See other

Finding passwords in HTTP Wire Data

index=batv1_source=stream:tcp dest="192.168.250.70" http_method=POST form_data=*username*passwd*

|table form_data

✓ 412 events (before 11/5/18 9:13:58.000 PM) No Event Sampling ▼

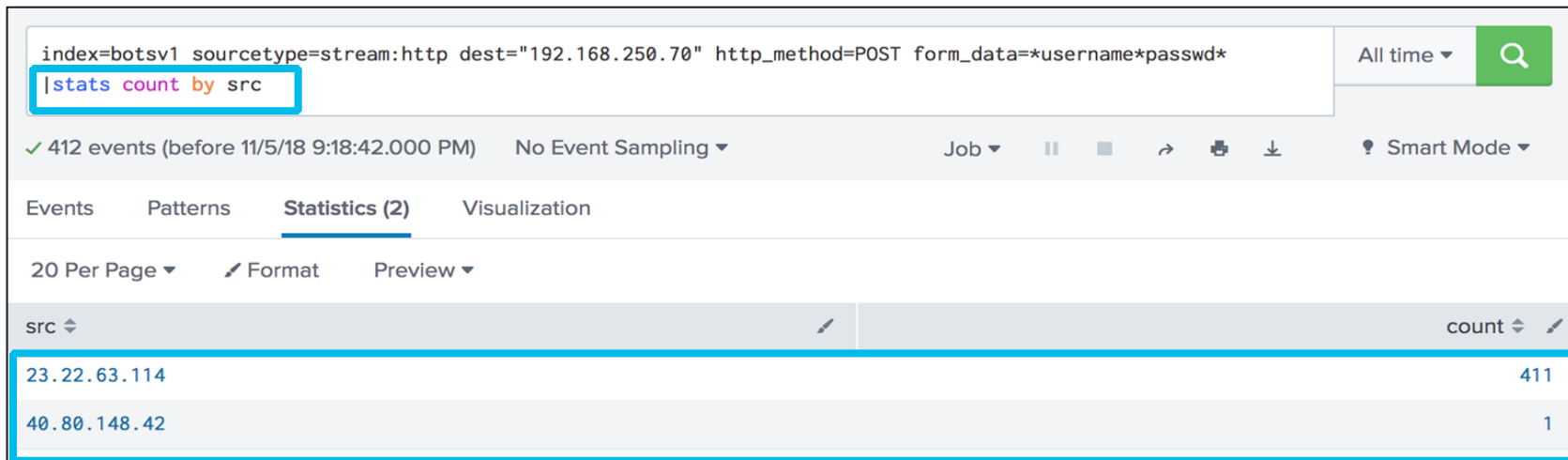
Events Patterns **Statistics (412)** Visualization

20 Per Page ▼ ✎ Format Preview ▼

form_data ⇅

username=admin&passwd=batman&option=com_login&task=login&return=aW5kZXgucGhw&e5ec827a3f67ce0efc546d81f7356acc=1
username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=rock&4a40c518220c1993f0e02dc4712c5794=1
username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=cool&a09349d0d6dbf078ad72cf8e9348583=1
username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=sammy&0d3bb020f70044ffa32f7d0fa7fa88=1
username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=august&9800c58b682f234e562dee5972a58b8d=1
username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=phantom&a083bf4d12c07976186d8a6efa6308cf=1
username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=williams&e3b1998d29669e83333a101735fd1c90=1
username=admin&ba11501d963f628dfb862d3a07bbe674=1&task=login&return=aW5kZXgucGhw&option=com_login&passwd=private
username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=baby&26a9247d113c378cdf06f31fa2154f2c=1
username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=dave&1b067a8762b4c8a9909ca68aae723e5a=1

Using stats for the win!



The screenshot shows the Splunk search interface. The search bar contains the query: `index=botsv1 sourcetype=stream:http dest="192.168.250.70" http_method=POST form_data=*username*passwd*`. Below the search bar, a blue box highlights the command `| stats count by src`. The search results show 412 events. The 'Statistics (2)' tab is selected, displaying a table with two rows of data. The first row shows the source IP `23.22.63.114` with a count of 411. The second row shows the source IP `40.80.148.42` with a count of 1. A blue box highlights the entire table.

src	count
23.22.63.114	411
40.80.148.42	1

Identifying where a brute force attack originated

Exploitation

- What IP address is likely attempting a brute force password attack against `imreallnotbatman.com`?
 - 23.22.63.114

Kill Chain

IP Scanning the Web Server: 40.80.148.42

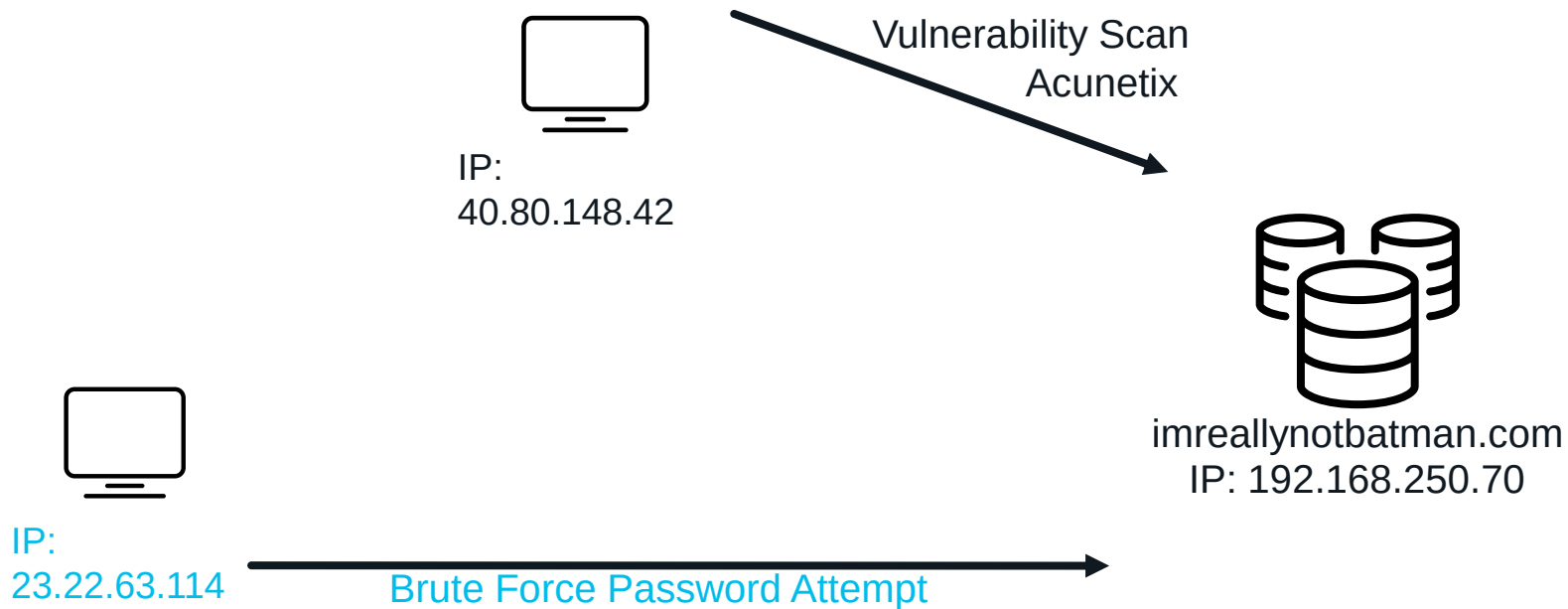
Web Vulnerability Scanner: Acunetix

Which Web Server?: 192.168.250.70/Joomla



Brute Force Attack Originated: 23.22.63.114

APT picture



MITRE ATT&CK

Adversarial tactics, techniques, and common knowledge



“The 14 tactic categories within ATT&CK for Enterprise were derived from the all stages (recon, weaponize, delivery exploit, control, maintain, and execute) of a seven-stage Cyber Attack Lifecycle (first articulated by Lockheed Martin as the Cyber Kill Chain®). This provides a deeper level of granularity in describing what can occur during an intrusion.”

<https://attack.mitre.org/>

Identifying the first password attempted in the attack

Kill Chain Phase: Exploitation

- What was the first brute force password used?

- Hints

- Sourcetype that logs interactions between web browser and server is important
- Form_data has usernames and passwords in it
- The _time field shows when the event occurred
- Build on the search from the previous question

Adding time

index=botsv1 sourcetype=stream:http form_data=*username*passwd* table _time form_data		All time	
✓ 412 events (before 11/5/18 9:54:40.000 PM) No Event Sampling		Job	Smart Mode
Events	Patterns	Statistics (412)	Visualization
20 Per Page	Format	Preview	< Prev 1 2 3 4 5 6 7 8 ... Next >
_time	form_data		
2016-08-10 21:48:05.858	username=admin&passwd=batman&option=com_login&task=login&return=aW5kZXgucGhw&e5ec827a3f67ce0efc546d81f7356acc=1		
2016-08-10 21:46:51.394	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=rock&4a40c518220c1993f0e02dc4712c5794=1		
2016-08-10 21:46:51.154	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=cool&a09349d0d6bdbf078ad72cf8e9348583=1		
2016-08-10 21:46:51.156	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=sammy&0d3bb0020f70044ffba32f7d0fa7fa88=1		
2016-08-10 21:46:50.873	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=august&9800c58b682f234e562dee5972a58b8d=1		
2016-08-10 21:46:50.634	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=phantom&a083bf4d12c07976186d8a6efa6308cf=1		
2016-08-10 21:46:50.627	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=williams&e3b1998d29669e83333a101735fd1c90=1		
2016-08-10 21:46:50.621	username=admin&ba11501d963f628dfb862d3a07bbe674=1&task=login&return=aW5kZXgucGhw&option=com_login&passwd=private		
2016-08-10 21:46:50.640	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=baby&26a9247d113c378cdf06f31fa2154f2c=1		
2016-08-10 21:46:50.637	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=dave&1b067a8762b4c8a9909ca68aae723e5a=1		

Reversing the order of output (Oldest First)

index=botsv1 sourcetype=stream:http form_data=*username*passwd*
| reverse
| table _time form_data

✓ 412 events (before 11/30/20 2:48:35.000 PM) No Event Sampling ▾

Events Patterns **Statistics (412)** Visualization

20 Per Page ▾ Format Preview ▾

Password

_time ↕	form_data ↕
2016-08-10 21:45:21.226	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=12345678&9d873c2becd118318849d13cf18b60ff=
2016-08-10 21:45:21.241	username=admin&863349a657c211fbfeb90ebe9427654c=1&task=login&return=aW5kZXgucGhw&option=com_login&passwd=letmein
2016-08-10 21:45:21.247	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=qwerty&af4df60674155567dee0566f87045251=1
2016-08-10 21:45:21.250	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=1234&aaf6297ae5c1e3df78a421bc55548d16=1
2016-08-10 21:45:21.260	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&76e93e8488d9a46878468d88954a0d54=1&passwd=123456
2016-08-10 21:45:21.263	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=football&d1181413b1a70460b8d425cec799cdca=1

A more elegant way to view the passwords

Kill Chain Phase: Exploitation

● What was the first brute force password used?

○ 12345678

New Search

```
index=main sourcetype=stream:http http_method=POST  
| rex field=form_data "passwd=(?<userpassword>\w+)"  
| search userpassword=* | reverse | head 1 | table userpassword
```

✓ 1 event (before 10/4/17 6:10:48.000 PM) [No Event Sampling](#) ✓

Events	Patterns	Statistics (1)	Visualization
20 Per Page Format Preview			
userpassword			
12345678			

Identifying the Password Used To Gain Access

Kill Chain Phase: Exploitation

- What was the correct password for admin access to the content management system running imreallynotbatman.com?

- Bonus Question: From what IP address was the password used?

- Hints

- Sourcetype should be one that provides communication between web browser and server
- The stats command will be helpful to identify the correct password
- The command to extract the password from the form_data is

```
| rex field=form_data "passwd=(?<userpassword>\w+)"
```

What else do we need?

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

412 events (before 11/5/18 11:57:28.000 PM) No Event Sampling Job || ■ → ☐ ↓ ! Smart Mode ▾

Events Patterns **Statistics (411)** Visualization

20 Per Page ▾ ✎ Format Preview ▾ < Prev 1 2 3 4 5 6 7 8 ... Next >

	userpassword ▾ ✎	count ▾ ✎
• Focus our search on destination for greater precision	batman	2
• Rex command will extract the passwords	000000	1
• Add a stats command to count the number of times each password was used and sort by the count	1111	1
• Second use of a password would likely indicate that it was the one the adversary wanted	111111	1
	11111111	1

Stats command provides a wider view

- From an investigation perspective, knowing the password was used twice is nice, but knowing where it was used is far more interesting

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

✓ 412 events (before 11/6/18 12:05:34.000 AM) No Event Sampling ▾ Job ▾ || ■ → 🖨️ ⬇️ ? Smart Mode ▾

Events Patterns **Statistics (411)** Visualization

20 Per Page ▾ / Format Preview ▾ < Prev 1 2 3 4 5 6 7 8 ... Next >

userpassword ▾ ✎	count ▾ ✎	values(src) ▾ ✎
batman	2	23.22.63.114 40.80.148.42
000000	1	23.22.63.114
1111	1	23.22.63.114
111111	1	23.22.63.114
11111111	1	23.22.63.114

Collecting additional attributes around the login events

Kill Chain Phase: Exploitation

● What was the correct password for admin access to the content management system running "imreallynotbatman.com"?

○ batman

● Bonus Question: From what IP address was the password used?

○ 40.80.148.42

The screenshot shows a network security tool interface with a search bar at the top containing the following query:

```
index=botsv1 sourcetype=stream:http form_data=*username*passwd* dest_ip=192.168.250.70 src=40.80.148.42
| rex field=form_data "passwd=(?<userpassword>\w+)"
| search userpassword=*
| table _time uri userpassword
```

Below the search bar, it indicates "1 event (before 11/6/18 12:09:05.000 AM)" and "No Event Sampling". The interface has tabs for "Events", "Patterns", "Statistics (1)", and "Visualization". The "Statistics (1)" tab is selected, showing a table with the following data:

_time	uri	userpassword
2016-08-10 21:48:05.858	/joomla/administrator/index.php	batman

Kill Chain

IP Scanning the Web Server: 40.80.148.42

Web Vulnerability Scanner: Acunetix

Which Web Server?: 192.168.250.70/Joomla



Brute Force Attack Originated:

23.22.63.114

Identifying the First Password Attempted in a Brute Force Attack

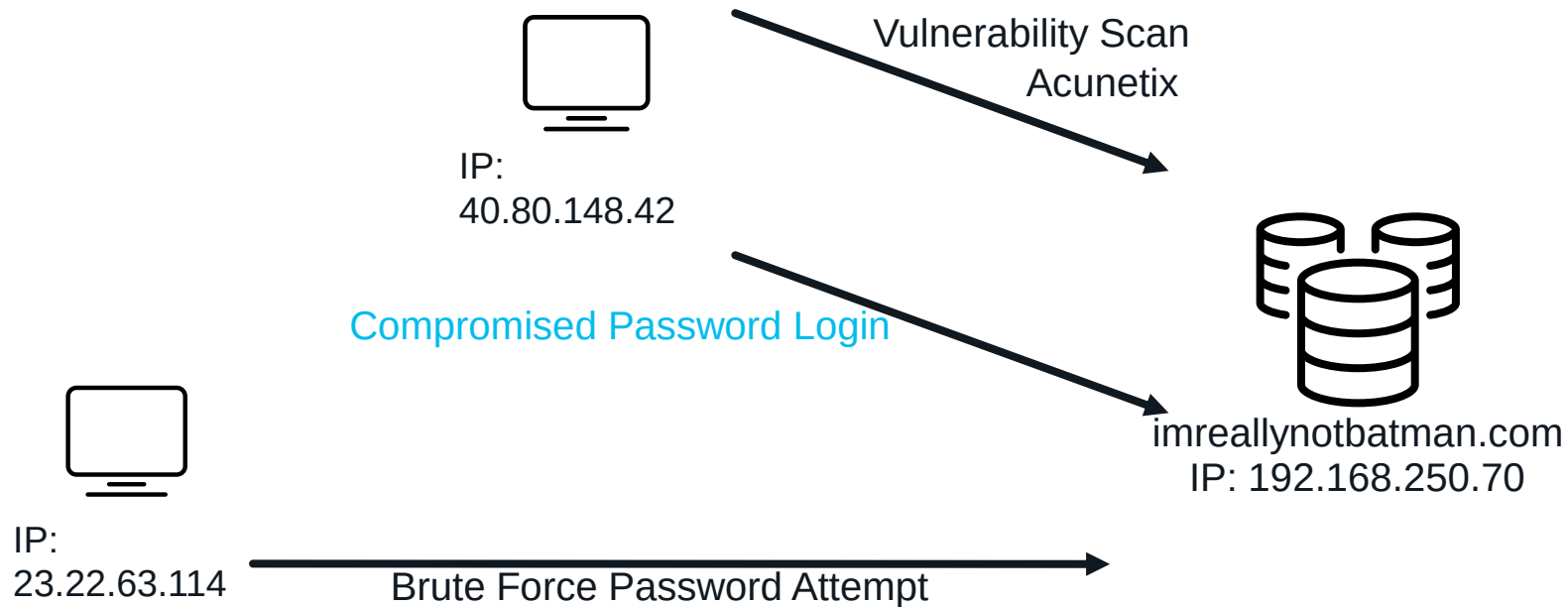
Extracting Passwords from

Events

Identifying the Password Used To Gain Access:

40.80.148.42

APT picture



Determining the elapsed time between events

Kill Chain Phase: Exploitation

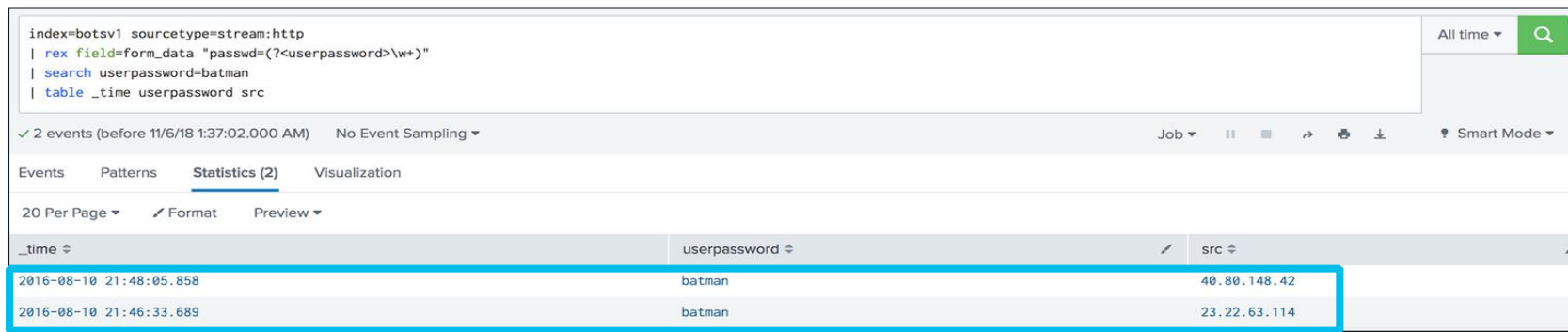
- How many seconds elapsed between the time the brute force password scan identified the correct password and the compromised login?

- Hints

- Use the rex command that we used previously to extract the passwords
- Identify the password that was used multiple times
- Look at the transaction command

Tabling our logins with the same password

- Build on our earlier searches for the userpassword extraction
- We know from earlier research the password of interest is batman, isolate search on those events



The screenshot shows a Splunk search interface. The search bar contains the following query:

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

Below the search bar, the results are displayed in a table. The table has three columns: `_time`, `userpassword`, and `src`. Two rows are visible, both with the password `batman`. The first row has a timestamp of `2016-08-10 21:48:05.858` and a source IP of `40.80.148.42`. The second row has a timestamp of `2016-08-10 21:46:33.689` and a source IP of `23.22.63.114`. The table is highlighted with a blue border.

_time	userpassword	src
2016-08-10 21:48:05.858	batman	40.80.148.42
2016-08-10 21:46:33.689	batman	23.22.63.114

Transaction command

- Use transaction command to group these events together

```
index=main sourcetype=stream:http | rex field=form_data "passwd=(?<userpassword>\w+)"  
| search userpassword=batman | transaction userpassword | table duration
```



Group events together based on a common value or values. In this case group events as a transaction based on the same userpassword



Duration is a value created with transaction that calculates the difference between the first and last event

Determining the elapsed time between events

Kill Chain Phase: Exploitation

- How many seconds elapsed between the time the brute force password scan identified the correct password and the compromised login?

○ 92.169084

The screenshot shows a Splunk search interface. At the top, a search query is entered in the search bar: `index=botsv1 sourcetype=stream:http | rex field=form_data "passwd=(?<userpassword>\w+)" | search userpassword=batman | transaction userpassword | table duration`. The query is highlighted with a blue box. Below the search bar, the results are displayed. The first result is highlighted with a blue box and shows a duration of 92.169084. The interface includes tabs for Events, Patterns, Statistics (1), and Visualization. The Statistics (1) tab is selected. Below the tabs, there are options for 20 Per Page, Format, and Preview. The duration is displayed as 92.169084.

```
index=botsv1 sourcetype=stream:http
| rex field=form_data "passwd=(?<userpassword>\w+)"
| search userpassword=batman
| transaction userpassword
| table duration
```

✓ 1 event (before 11/6/18 1:39:27.000 AM) No Event Sampling ▼

Events Patterns **Statistics (1)** Visualization

20 Per Page ▼ ✎ Format Preview ▼

duration ⚡

92.169084

Identifying the executable uploaded

Kill Chain Phase: Installation

- What is the name of the executable uploaded by P01s0n1vy?
(For example, "notepad.exe" or "favicon.ico")
- Bonus Question: What is the source address of the executable?
- Hints
 - If we are looking for executables uploaded, what sourcetypes would have visibility into files in motion?
 - If a file is being uploaded what is likely to be the http_method?

Search for EXEs in stream:http

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

✓ 18 events (before 11/6/18 1:49:52.000 AM) No Event Sampling

Events (18) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 day per column

List Format 20 Per Page

< Hide Fields All Fields

SELECTED FIELDS

- a dest 1
- a host 1
- a http_method 2
- a http_user_agent 3
- a part_filename() 2
- a source 1
- a sourcetype 1
- a src 2
- a src_headers 17
- a uri 17

INTERESTING FIELDS

part_filename()

2 Values, 5.556% 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%

image/png, */*

Search for EXEs in Suricata

index=botsv1 sourcetype=suricata dest_ip=192.168.250.70 .exe

43 events (before 11/6/18 1:54:26.000 AM) No Event Sampling

Events (43) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

1 day per column

< Hide Fields All Fields

SELECTED FIELDS

- a dest 2
- a fileinfo.filename 2
- a host 1
- a http_method 2
- a http_user_agent 3
- a source 1
- a sourcetype 1
- a src 2

fileinfo.filename

2 Values, 4.651% of events

Selected Yes No

Reports

- Top values
- Top values by time
- Rare values

Events with this field

Values	Count	%
/_vti_bin/shtml.exe	1	50%
3791.exe	1	50%

1 2 3 Next >

Hostnames v IPs

Important Note About Fields

- Fields may not have the same values based on the logging structure
- dest v dest_ip could have different values
 - Try using OR and parenthesis to bracket the search (dest=1.1.1.1 OR dest_ip=1.1.1.1)

```
index=botsv1 sourcetype=suricata (dest="192.168.250.70" OR dest_ip="192.168.250.70") .exe
```

When destination and destination IP are different

The screenshot shows the Cisco Live! interface with a search query: `index=botsv1 sourcetype=suricata (dest=imreallynotbatman.com OR dest="192.168.250.70") http.http_method=POST .exe`. The query results show 4 events. The 'dest' field is highlighted, showing 1 value, 100% of events. The 'fileinfo.filename' field is also highlighted, showing 2 values, 75% of events. A detailed view of the 'fileinfo.filename' field is shown, displaying a table of values and counts.

fileinfo.filename

2 Values, 75% of events

Selected

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
/_vti_bin/shtml.exe	2	66.667%
3791.exe	1	33.333%

Capturing the source of the executable

The screenshot shows the Cisco Live! interface with a search query: `index=botsv1 sourcetype=suricata (dest=imreallynotbatman.com OR dest="192.168.250.70") http.http_method=POST .exe "fileinfo.filename"."3791.exe"`. The search results show 1 event. A modal window is open for the 'src' field, showing 1 value (100% of events) and a table of values.

src

1 Value, 100% of events

Selected

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
40.80.148.42	1	100%

A large blue arrow points downwards from the modal window.

Identifying the executable uploaded

Kill Chain Phase: Installation

● What is the name of the executable uploaded by P01s0n1vy? Please include file extension. (For example, "notepad.exe" or "favicon.ico")?

○ 3791.exe

● Bonus Question: What is the source of the executable?

○ 40.80.148.82

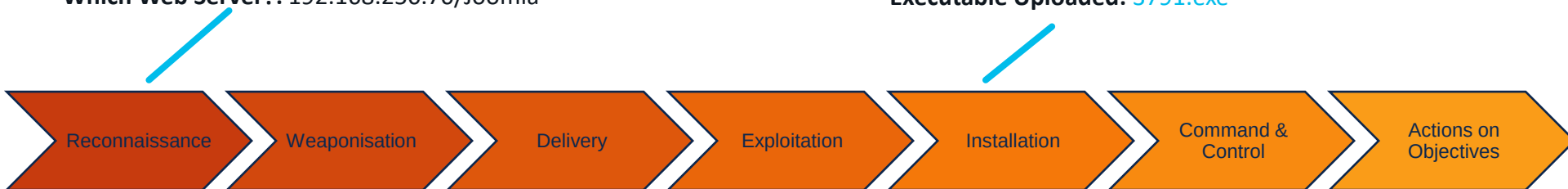
Kill Chain

IP Scanning the Web Server: 40.80.148.42

Web Vulnerability Scanner: Acunetix

Which Web Server?: 192.168.250.70/Joomla

Executable Uploaded: 3791.exe



Brute Force Attack Originated:

23.22.63.114

Identifying the First Password Attempted in a Brute Force Attack

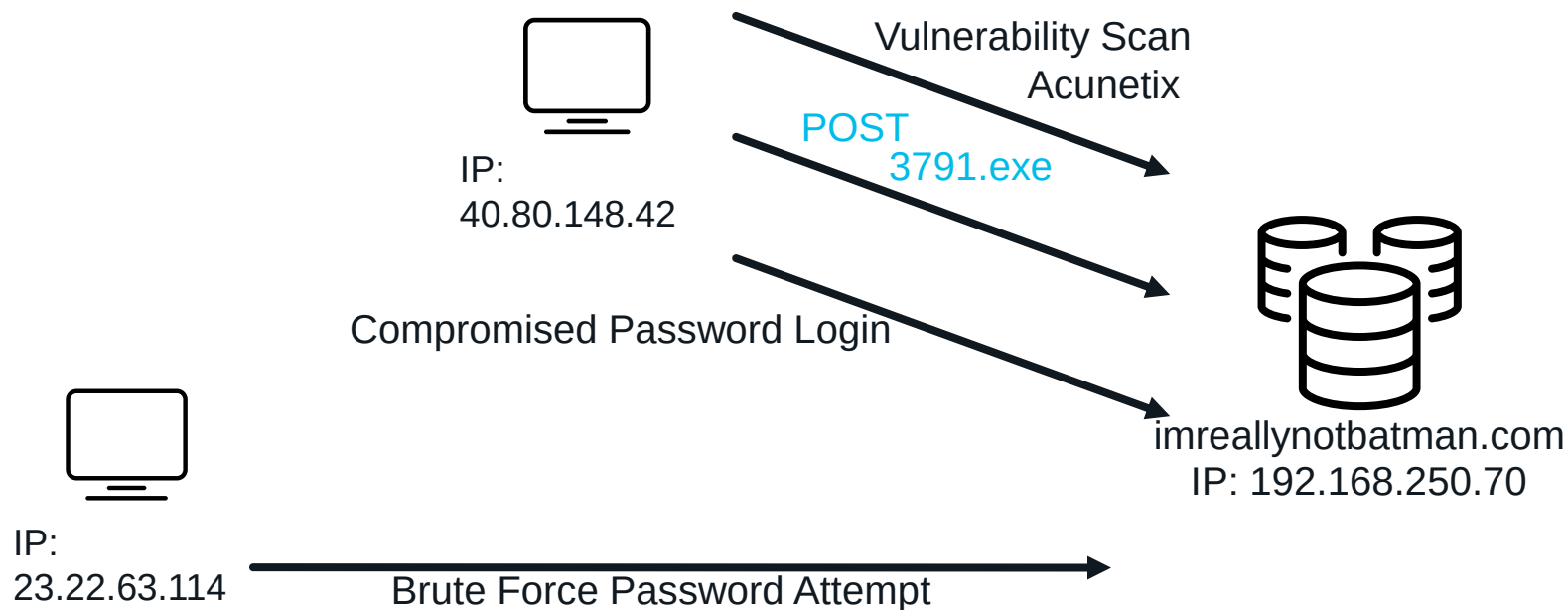
**Extracting Passwords from
Events**

Identifying the Password Used To Gain Access:

40.80.148.42

Determining The Elapsed Time Between Events

APT picture



Determining the Hash of the Uploaded File

Kill Chain Phase: Installation

- What is the MD5 hash of the executable uploaded?
- Hints
 - Which sourcetypes have the correct filename?
 - File hashes can be found in the log stream if you know which sourcetype to look in...
 - Process Execution events will capture the MD5 at process launch

What sourcetype should i start with?

● Overview of Sysmon Capabilities

- Records the hash of process image files using SHA1 (the default), MD5, SHA256 or IMPHASH.
- <https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon>

index=botsv1 3791.exe

✓ 76 events (before 11/6/18 6:12:23.000 PM) No Event Sampling ▼

Events (76) Patterns Statistics Visualization

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

< Hide Fields ≡ All Fields

SELECTED FIELDS

- a dest 4
- a fileinfo.filename 1
- a host 4
- a http_method 1
- a http_user_agent 2
- a part_filename[] 2
- a source 5
- a sourcetype 5
- a src 2
- a src_headers 1
- a uri 1

sourcetype

5 Values, 100% of events

Selected Yes No

Reports

- Top values
- Top values by time
- Rare values
- Events with this field

Values	Count	%
XmlWinEventLog:Microsoft-Windows-Sysmon/Operational	69	90.789%
WinEventLog:Security	3	3.947%
stream:http	2	2.632%
fgt_utm	1	1.316%
suricata	1	1.316%

sysmon Primer

- Windows System Service and Device Driver

- Resident across reboots

- Logs numerous Windows activities including

- Process Creation
- Network Connection
- Driver Loaded
- File Creation
- Registry Event
- And more...

- Configuration files in XML are used to determine which events are logged

- <https://github.com/SwiftOnSecurity/sysmon-config>

```
<Sysmon schemaversion="3.2">
  <!-- Capture all the hashes -->
  <HashAlgorithms>*</HashAlgorithms>
  <EventFiltering>
    <!-- Log all drivers except if the signature -->
    <!-- contains Microsoft or Windows -->
    <DriverLoad onmatch="exclude">
      <Signature condition="contains">microsoft</Signature>
      <Signature condition="contains">windows</Signature>
    </DriverLoad>
    <!-- Do not log process termination -->
    <ProcessTerminate onmatch="include"/>
    <!-- Log network connection if the destination port equals 443 -->
    <!-- or 80, and the process isn't InternetExplorer -->
    <NetworkConnect onmatch="include">
      <DestinationPort>443</DestinationPort>
      <DestinationPort>80</DestinationPort>
    </NetworkConnect>
    <NetworkConnect onmatch="exclude">
      <Image condition="end with">iexplore.exe</Image>
    </NetworkConnect>
  </EventFiltering>
</Sysmon>
```

What can I find with Sysmon?

Part 1 of 2

The screenshot displays the Sysmon event log interface. The main window shows a search for 'index=botsv1 3791.exe' with 69 events found. The 'EventDescription' pane is open, showing 4 values for 'Image Load'. The 'Hashes' pane is also open, showing 55 values for the selected event. The 'Top 10 Values' table is highlighted, showing the top 10 values for the selected event.

EventDescription

4 Values, 100% of events

Reports

Top values Top values by time Rare values

Events with this field

Values

Value	Count	%
Image Load	62	89.855%
Process Create	5	7.246%
Network Connect	1	1.449%
Process Terminate	1	1.449%

Hashes

55 Values, 97.101% of events

Reports

Top values Top values by time Rare values

Events with this field

Top 10 Values

Value	Count	%
SHA1=65DF73D77324D008C83C3E57B445DF0FD43A3A51, MD5=AAE3F5A29935E6ABCC2C2754D12A9AF0, SHA256=EC78C938D8453739CA2A370B9C275971EC46CAF6E479DE2B2D04E97CC47FA45D, IMPHASH=481F47BBB2C9C21E108D65F52B04C448	4	4.478%
SHA1=F5CFD4070EA7D2B40A29F21F9E29AF23341C59EC, MD5=59A1D4FACD7B33F76C4142CD42D3ABA, SHA256=E1A080E61FB1BAF0DA629D34BAE6E6F0F9D0E0337BF6CED9F4B3AB9B1C23D91BA, IMPHASH=5B13496CE269DF7709AAB6B1BBF99CD3	4	4.478%
SHA1=1A7D45BC0AD6A725159802137D20CB93F1B712C, MD5=522BF7088E69948A20DD5C89D35982C4, SHA256=20949159376225C7DB8B4CBBA1F0C06113E2DED7369B59329AF00D3295BC627B, IMPHASH=F0E5EF88099C621A94DB5D98B363E847	2	2.985%
SHA1=52451D9630A6F45A3C092091B853879D57B92664, MD5=53D2FF6892E3D69D9CF5E1F1785872B0, SHA256=1459B0F53B9A6016E45B4B6CD2A8E8088BB6BC484CDB942600864D5B38667BE2, IMPHASH=A77B19E8024D7D62FA77C62F95712442	2	2.985%

Drilling down on MD5 & CommandLine

The screenshot displays the Cisco Live! interface for analyzing event data. The main window shows a list of 5 events (before 11/7/18 2:47:22.000 AM) with a timeline visualization. The 'Events (5)' tab is selected, and the 'Format Timeline' dropdown is set to 'List'. The '20 Per Page' dropdown is also visible.

On the left, the 'SELECTED FIELDS' list includes: CommandLine 4, dest 1, EventDescription 1, Hashes 3, host 1, MD5 3, ParentCommandLine 3, source 1, and sourceType 1. The 'INTERESTING FIELDS' list includes: action 1 and app 3.

Two modal windows are open, both with a 'Selected' dropdown set to 'Yes'.

MD5 Modal:

- 3 Values, 100% of events
- Reports: Top values, Top values by time, Rare values
- Events with this field
- Values table:

Values	Count	%
59A1D4FACD7B333F76C4142CD42D3A8A	3	60%
626A9EC445D06FBC1502BF53A1E3356B	1	20%
AAE3F5A29935E6ABCC2C2754D12A9AF0	1	20%

CommandLine Modal:

- 4 Values, 100% of events
- Reports: Top values, Top values by time, Rare values
- Events with this field
- Values table:

Values	Count	%
C:\Windows\system32\cmd.exe	2	40%
3791.exe	1	20%
\\??C:\Windows\system32\conhost.exe 0xffffffff	1	20%
cmd.exe /c "3791.exe 2>&1"	1	20%

A large blue arrow points from the CommandLine modal towards the bottom right of the screen.

Exploring the Sysmon event

index=botsv1 3791.exe sourcetype=XmlWinEventLog:Microsoft-Windows-Sysmon/Operational EventCode=1 CommandLine="3791.exe"

8/10/16
9:56:18.000 PM

<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}' /><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2016-08-10T21:56:18.142461700Z' /><EventRecordID>428908</EventRecordID><Correlation><Execution ProcessID='1296' ThreadID='1416' /><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>we1149srv.waynecorpinc.local</Computer><Security UserID='S-1-5-18' /></System><EventData><Data Name='UtcTime'>2016-08-10 21:56:18.142</Data><Data Name='ProcessGuid'>{E500B0EA-A302-57AB-0000-00108D65C301}</Data><Data Name='ProcessId'>3880</Data><Data Name='Image'>C:\inetpub\wwwroot\joomla\3791.exe</Data><Data Name='CommandLine'>3791.exe </Data><Data Name='CurrentDirectory'>C:\inetpub\wwwroot\joomla</Data><Data Name='User'>NT AUTHORITY\IUSR</Data><Data Name='LogonGuid'>{E500B0EA-219E-57AA-0000-0020E3030000}</Data><Data Name='LogonId'>0x3e3</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>SHA1=65DF73D77324D008C83C3E57B445DF0FD43A3A51,MD5=AAE3F5A29935E6ABCC2C2754D12A9AF0,SHA256=EC78C938D8453739CA2A370B9C275971EC46CAF6E479DE2B2D04E97CC47FA45D,IMPHASH=481F47BBB2C9C21E108D65F52B04C448</Data><Data Name='ParentProcessGuid'>{E500B0EA-A302-57AB-0000-0010E63C301}</Data><Data Name='ParentProcessId'>2896</Data><Data Name='ParentImage'>C:\Windows\SysWOW64\cmd.exe</Data><Data Name='ParentCommandLine'>cmd.exe /c "3791.exe 2>&1"</Data></EventData></Event>

Event Actions ▾

Type	Field	Value	Actions
Selected	CommandLine ▾	3791.exe	▾
	EventDescription ▾	Process Create	▾
	Hashes ▾	SHA1=65DF73D77324D008C83C3E57B445DF0FD43A3A51,MD5=AAE3F5A29935E6ABCC2C2754D12A9AF0,SHA256=EC78C938D8453739CA2A370B9C275971EC46CAF6E479DE2B2D04E97CC47FA45D,IMPHASH=481F47BBB2C9C21E108D65F52B04C448	▾
	MD5 ▾	AAE3F5A29935E6ABCC2C2754D12A9AF0	▾
	ParentCommandLine ▾	cmd.exe /c "3791.exe 2>&1"	▾
	dest ▾	we1149srv.waynecorpinc.local	▾
	host ▾	we1149srv	▾
	source ▾	WinEventLog:Microsoft-Windows-Sysmon/Operational	▾
	sourcetype ▾	XmlWinEventLog:Microsoft-Windows-Sysmon/Operational	▾
Event	Computer ▾	we1149srv.waynecorpinc.local	▾
	CurrentDirectory ▾	C:\inetpub\wwwroot\joomla\	▾
	EventChannel ▾	Microsoft-Windows-Sysmon/Operational	▾
	EventCode ▾	1	▾

Putting it together

index=botsv1 3791.exe sourcetype=XmlWinEventLog:Microsoft-Windows-Sysmon/Operational EventCode=1 CommandLine="3791.exe" | stats values(MD5)

✓ 1 event (before 11/7/18 3:17:50.000 AM) No Event Sampling ▼

Events

Patterns

Statistics (1)

Visualization

20 Per Page ▼

✎ Format

Preview ▼

values(MD5) ⌵

AAE3F5A29935E6ABCC2C2754D12A9AF0

Determining the hash of the uploaded file

Kill Chain Phase: Installation

- What is the MD5 hash of the executable uploaded?
 - AAE3F5A29935E6ABCC2C2754D12A9AF0

Kill Chain

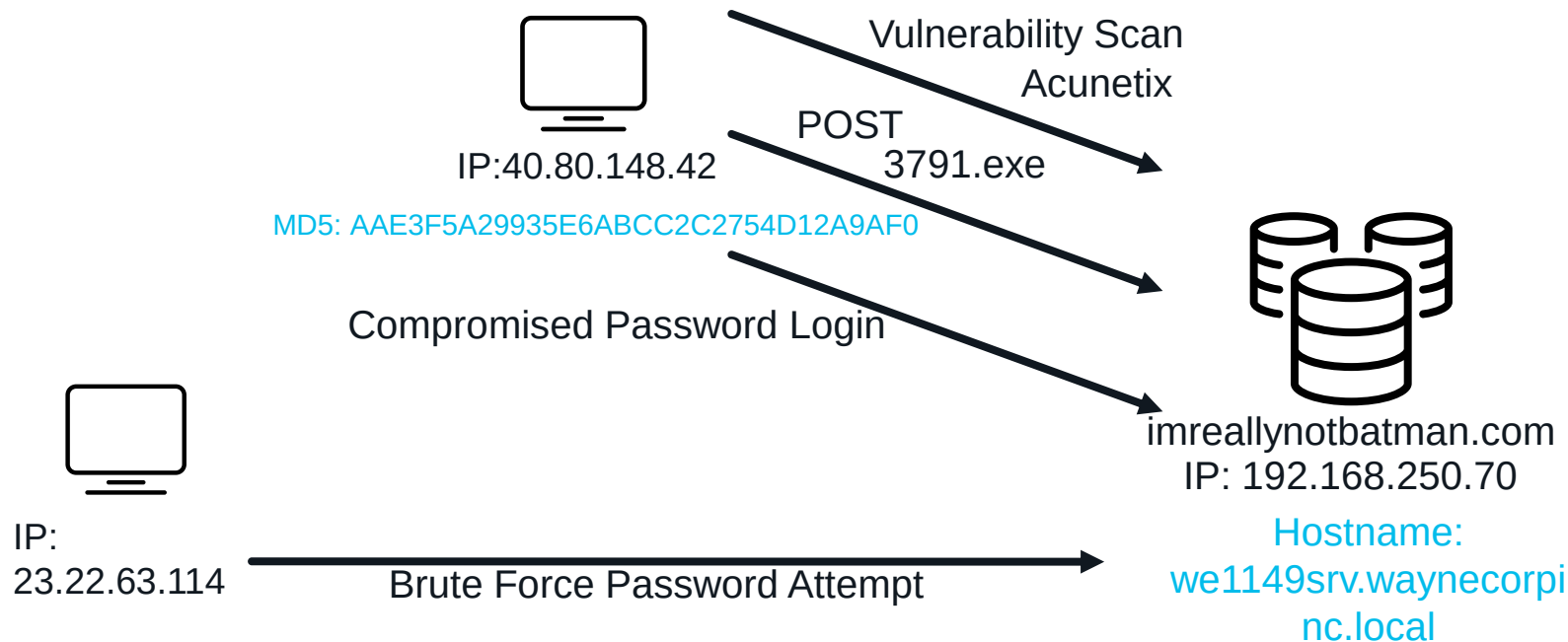
IP Scanning the Web Server: 40.80.148.42
Web Vulnerability Scanner: Acunetix
Which Web Server?: 192.168.250.70/Joomla

Executable Uploaded: 3791.exe
Hash of the Uploaded File:
[AAE3F5A29935E6ABCC2C2754D12A9AF0](#)



Brute Force Attack Originated:
23.22.63.114
Identifying the First Password Attempted in a Brute Force Attack
Extracting Passwords from Events
Identifying the Password Used To Gain Access:
40.80.148.42
Determining The Elapsed Time Between Events

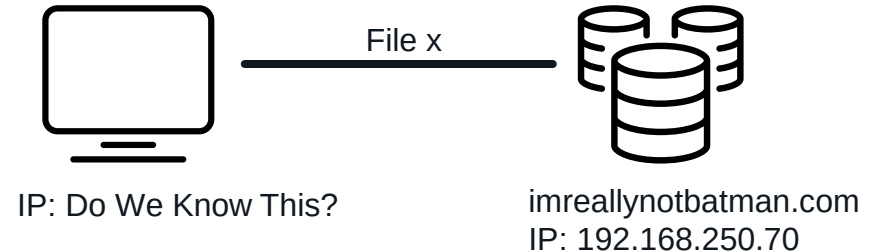
APT picture



Identifying the file that defaced our web server

Kill Chain Phase: Actions on Objective

- What is the name of the file that defaced the imreallynotbatman.com website?
- Hints
 - Data sources that show communication between the web browser and server will provide good visibility
 - Determining the IP address of the other system could be helpful
 - The flow of information (directionality) is the important key.
 - POST v GET
 - Previous information gathered in the investigation will be helpful here



Looking at directional flow of data - Part 1

Nothing coming from outside in

index=botsv dest=192.168.250.70 sourcetype=suricata

421 events (before 11/7/18 1:31:56.000 PM) No Event Sampling

Events (421) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 minute per column

List Format 20 Per Page

< Prev 1 2 3 4 5 6 7 8 ... Next >

< Hide Fields All Fields

SELECTED FIELDS

- a dest 1
- a fileinfo.filename 100+
- a host 1
- a http_method 2
- a http_user_agent 2
- a source 1
- a sourcetype 1
- a src 2

INTERESTING FIELDS

- a app 1
- a app_proto 1
- # bytes 4
- # date_hour 1
- # date_mday 1

Time Event

> 8/24/16 4:47:14.001 PM { [-] app_proto: http

SRC

2 Values, 100% of events Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
192.168.2.50	211	50.119%
192.168.250.70	210	49.881%

Looking at directional flow of data - Part 1

Looking from inside out

index=botsv src=192.168.250.70 sourcetype=suricata

✓ 12,601 events (before 11/7/18 1:34:23.000 PM) No Event Sampling

Events (12,601) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

1 day per column

< Prev 1 2 3 4 5 6 7 8 ... Next >

dest_ip

7 Values, 100% of events

Selected Yes No

Reports

Top values Top values by time Rare values

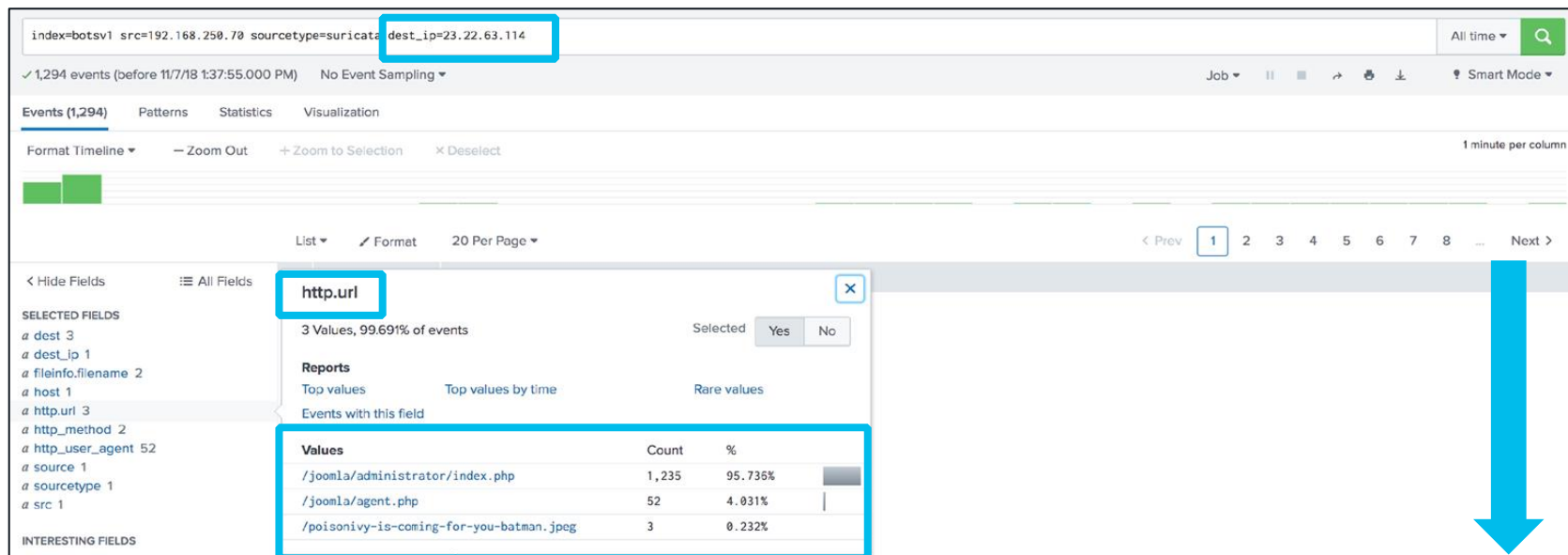
Events with this field

Values	Count	%
40.80.148.42	10,317	81.874%
23.22.63.114	1,294	10.269%
192.168.250.40	758	6.015%
192.168.2.50	214	1.698%
108.161.187.134	12	0.095%
192.168.250.255	3	0.024%
224.0.0.252	3	0.024%

SHOW AS RAW TEXT

dest_ip = 192.168.250.40 host = suricata-ids.waynecorpinc.local source = /var/log/suricata/eve.json sourcetype = suricata src = 192.168.250.70

Pivot into destination IP addresses to view URLs



The screenshot shows the Cisco Live! interface with a search bar at the top containing the query: `index=botsv1 src=192.168.250.70 sourcetype=suricata dest_ip=23.22.63.114`. Below the search bar, it indicates 1,294 events. The interface is divided into several tabs: Events (1,294), Patterns, Statistics, and Visualization. The Events tab is active, showing a timeline view. A large blue arrow points downwards from the timeline view towards the pivot table.

On the left side, there is a list of fields under "All Fields". The field `http.url` is selected and highlighted with a blue box. A pop-up window shows the details for `http.url`, including a "Reports" section with "Top values" and "Events with this field". The "Top values" section is expanded, showing a table of values.

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%

HTTP Get v Post Traffic Flow

HTTP GET will generally retrieve data



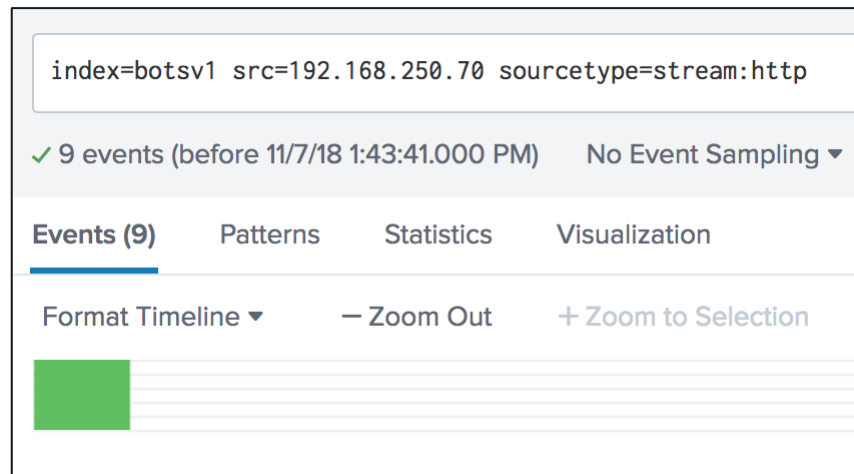
HTTP POST submits data to be processed



imrealllynotbatman.com

Do web servers start a conversation?

- How often should web servers start a conversation?



- If they are starting the conversation is that interesting and should be looked at?

Any similarities between Suricata and stream:http?

The screenshot shows the Cisco Live! Suricata interface. The search bar at the top contains the query: `index=botsv1 src=192.168.250.70 sourcetype=stream:http`. Below the search bar, it indicates 9 events were found. The main panel shows a list of events, with a modal window open for the 'uri' field. The modal window displays a report for the 'uri' field, showing 5 values and 88.889% of events. The report includes a table of values, counts, and percentages.

Values	Count	%
/core/list.xml	2	25%
/jed/list.xml	2	25%
/poisonivy-is-coming-for-you-batman.jpeg	2	25%
/core/extensions/com_joomlaupdate.xml	1	12.5%
/language/translationlist.3.xml	1	12.5%

The modal window also includes a 'Selected' button and a 'Rare values' link. The background shows a list of events with fields like 'uri', 'src', and 'sourcetype'.

What about firewall data?

index=botsv1 sourcetype=fgt_utm "192.168.250.70"

✓ 14,302 events (before 11/7/18 1:48:22.000 PM) No Event Sampling ▼

Events (14,302) Patterns Statistics Visualization

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

List ▼ Format 20 Per Page ▼

SELECTED FIELDS

- a dest 3
- a host 1
- a http_method 1
- a http_user_agent 2
- a source 1
- a sourcetype 1
- a src 3

INTERESTING FIELDS

- a action 3
- a attack 15
- # attackid 15
- # bytes 100+
- # bytes_in 100+

dest

3 Values, 100% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
192.168.250.70	14,293	99.937%
108.161.187.134	6	0.042%
23.22.63.114	3	0.021%

src

3 Values, 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	12,858	89.904%
23.22.63.114	1,435	10.034%
192.168.250.70	9	0.063%

eventname=gotham-fortigate devid=FGT60D4614044725 logid=0317013312 type=utm subtype=webfilter eventtype=f user="" srcip=23.22.63.114 srcport=47515 dstip=192.168.250.70 dstport=80 dstintf="internal3" proto=6 " action=passthrough retype=direct url="/joomla/agent.php" sentbyte=363 rcvdbyte=0 direction=N/A msg cat=0 catdesc="Unrated"

http_user_agent = unknown source = udp:514 sourcetype = fgt_utm src = 23.22.63.114

eventname=gotham-fortigate devid=FGT60D4614044725 logid=0317013312 type=utm subtype=webfilter eventtype=f user="" srcip=23.22.63.114 srcport=47515 dstip=192.168.250.70 dstport=80 dstintf="internal3" proto=6 " action=passthrough retype=direct url="/joomla/agent.php" sentbyte=418 rcvdbyte=0 direction=N/A msg cat=0 catdesc="Unrated"

Which search do I start with?

```
index=botsv1 sourcetype=fgt_utm "192.168.250.70" NOT dest="192.168.250.70" | stats count
```

✓ 9 events (before 11/7/18 1:50:52.000 PM) No Event Sampling ▼

```
index=botsv1 sourcetype=fgt_utm "192.168.250.70" NOT src="192.168.250.70" | stats count
```

✓ 14,293 events (before 11/7/18 1:50:55.000 PM) No Event Sampling ▼

Use web site categorisation to filter

The screenshot shows the Cisco Live! interface with a search query: `index=botsv1 sourcetype=fgt_utm *192.168.250.70 NOT dest="192.168.250.70"`. The search results show 9 events. A modal window titled "category" is open, displaying a table of values for the "category" field. The table has columns for "Values", "Count", and "%". The values are "Information Technology" (6, 66.667%) and "Malicious Websites" (3, 33.333%). A blue arrow points to the "Malicious Websites" row, indicating it is the selected filter.

index=botsv1 sourcetype=fgt_utm *192.168.250.70 NOT dest="192.168.250.70"

9 events (before 11/7/18 1:52:29.000 PM) No Event Sampling

Events (9) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

1 minute per column

category

2 Values, 100% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
Information Technology	6	66.667%
Malicious Websites	3	33.333%

10:13:46.000 PM gd_allow level=notice vd="root" policyid=10 sessionid=930693 user="" srcip=192.168.250.70 srcport=63139 srcintf="internal3" dstip=23.22.63.114 dstport=80 proto=6 service=HTTP hostname="prankglassinebracket.jumpingcrab.com:1337" profile="monitor-all" action="passthrough reqtype=direct url="/poisonivy-is-coming-for-atman.jpeg" sentbyte=106 rcvbyte=0 direction=N/A msg="URL belongs to an allowed category in policy" method=domain cat=26 catdesc="Malicious Websites" crscon=level=h

category = Malicious Websites dest = 23.22.63.114 host = 192.168.250.1 http_method = direct http_user_agent = unknown source = udp:514 sourcetype = fgt_utm src = 192.168.250.70

Firewall gives us confirmation

The screenshot shows the Cisco Firepower Management Center (FMC) interface. At the top, a search bar contains the query: `index=botsv1 sourcetype=fgt_utm "192.168.250.70" NOT dest="192.168.250.70" category="Malicious Websites"`. Below the search bar, it indicates 3 events were found. The main panel shows a timeline visualization with three green bars. A modal window is open, displaying the details for the `file_path` field. The modal shows a table with the following data:

Values	Count	%
/poisonivy-is-coming-for-you-batman.jpeg	3	100%

The modal also shows a list of events with details such as `devname=gotham-fortigate`, `devid=FGT6004614044725`, `logid=0317013312`, `type=utm`, `subtype=webfilter`, `eventtype=ft`, `srcip=192.168.250.70`, `srcport=51573`, `srcintf=internal3`, `dstip=23.22.63.114`, `dstport=1337`, `proto=6`, `profile=monitor-all`, `action=passthrough`, `reqtype=direct`, `url=/poisonivy-is-coming-for-you-batman.jpeg`, `method=domain`, `cat=26`, `catdesc=Malicious Websites`, `crscore=30`, `crlevel=h`.

Identifying the file that defaced our web server

Kill Chain Phase: Actions on Objective

- What is the name of the file that defaced the imreallynotbatman.com website?
 - poisonivy-is-coming-for-you-batman.jpeg

Kill Chain

IP Scanning the Web Server:

40.80.148.42

Which Web Server?:

192.168.250.70/Joomla

Web Vulnerability Scanner:

Acunetix

Executable Uploaded:

3791.exe

Hash of the Uploaded File:

AAE3F5A29935E6ABCC2C2754D12A9A
F0

File that Defaced Our Web

Server: [poisonivy-is-coming-for-you-batman.jpeg](#)

Reconnaissance

Weaponisation

Delivery

Exploitation

Installation

Command &
Control

Actions on
Objectives

Brute Force Attack Originated:

23.22.63.114

**Identifying the First Password Attempted
in a Brute Force Attack**

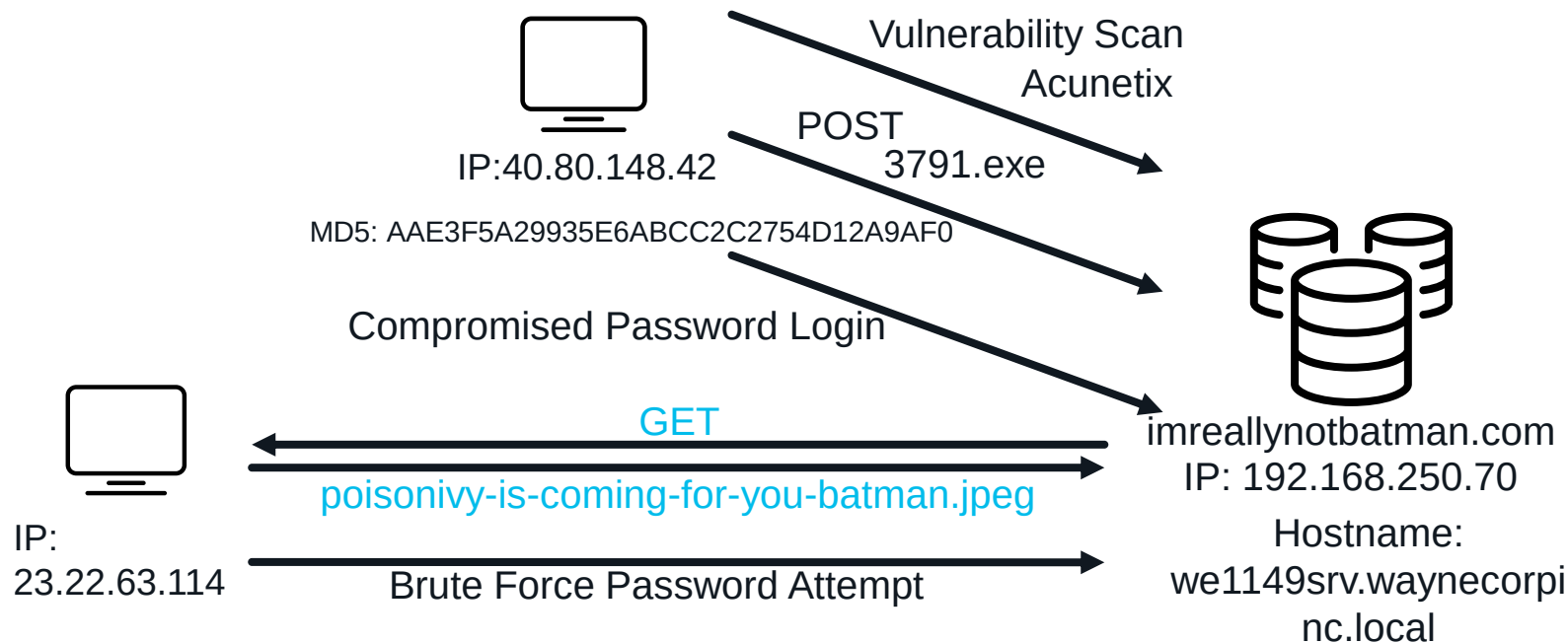
Extracting Passwords from Events

Identifying the Password Used To Gain Access:

40.80.148.42

Determining The Elapsed Time Between Events

APT picture



Identifying the FQDN of the system that defaced...

Kill Chain Phase: Command & Control

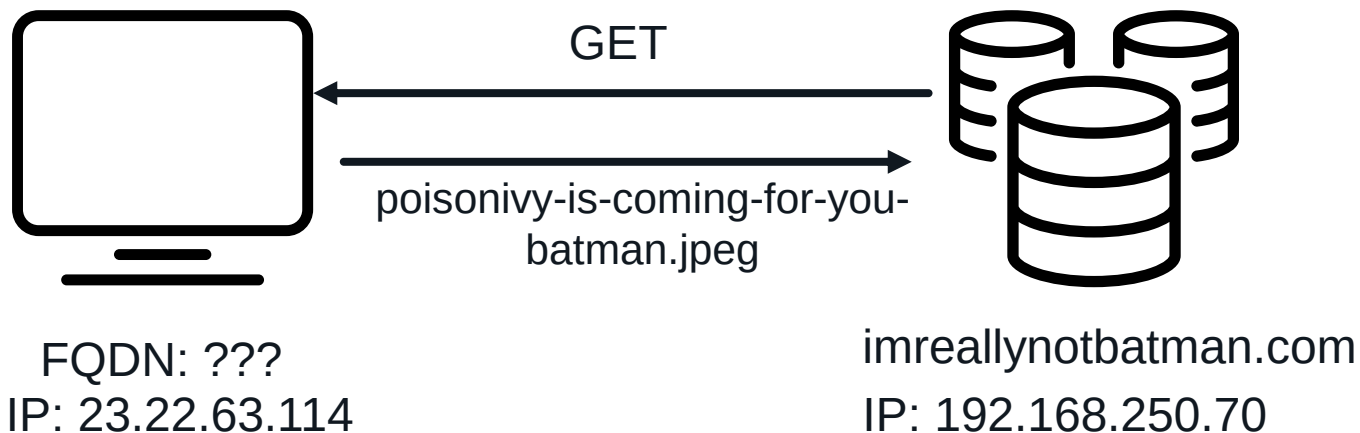
- This attack used dynamic DNS to resolve to the malicious IP. What fully qualified domain name (FQDN) is associated with this attack?

- Hint

- Information just recently uncovered will help answer this

HTTP Get traffic flow

- HTTP GET will generally retrieves data



Using Fortigate Firewall Events we just found

8/10/16 10:19:10.000 PM Aug 10 16:19:10 192.168.250.1 date=2016-08-10 time=16:19:10 devname=gotham-fortigate devid=FGT60D4614044725 logid=0317013312 type=utm subtype=webfilter eventtype=ftgd_allow level=notice vd="root" policyid=10 sessionid=932526 user="" srcip=192.168.250.70 srcport=51573 srcintf="internal3" dstip=23.22.63.114 dstport=1337 proto=6 service=HTTP hostname="prankglassinebracket.jumpingcrab.com:1337" profile="monitor-all" action=passthrough reftype=direct url="/poisonivy-is-coming-for-you-batman.jpeg" sentbyte=106 rcvbyte=0 direction=N/A msg="URL belongs to an allowed category in policy" method=domain cat=26 catdesc="Malicious Websites" crscore=30 crlevel=high

Event Actions ▾

Type	☒	Field	Value	Actions
Selected	☒	category ▾	Malicious Websites	▾
	☒	dest ▾	23.22.63.114	▾
	☒	file_path ▾	/poisonivy-is-coming-for-you-batman.jpeg	▾
	☒	host ▾	192.168.250.1	▾
	☒	http_method ▾	direct	▾
	☒	http_user_agent ▾	unknown	▾
	☒	source ▾	udp:514	▾
	☒	sourcetype ▾	fgt_utm	▾
	☒	src ▾	192.168.250.70	▾
	☒	url ▾	prankglassinebracket.jumpingcrab.com:1337/poisonivy-is-coming-for-you-batman.jpeg	▾
Event	☐	action ▾	allowed	▾



What data sets saw this file?

index=botsv1 dest=23.22.63.114 "poisonivy-is-coming-for-you-batman.jpeg" src=192.168.250.70 All time

✓ 6 events (before 11/7/18 2:03:41.000 PM) No Event Sampling

Events (6) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 minute per column

List Format 20 Per Page

< Hide Fields All Fields

SELECTED FIELDS

- a category 1
- a dest 1
- a dest_ip 1
- a file_path 1
- a host 2
- a http_method 2
- a http_user_agent 1
- a source 2
- a sourcetype 2
- a src 1
- a src_headers 1
- a url 1
- a url 2

INTERESTING FIELDS

- # ack_packets_in 2

Time Event

8/10/16 10:19:11.351 PM {"endtime":"2016-08-10T22:19:11.351975Z","timestamp":"2016-08-10T22:19:10.438743Z","ack_packets_in":387,"ack_packets_out":8,"bytes":554174,"bytes_in":106,"bytes_out":...

sourcetype

2 Values, 100% of events

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
fgt_utm	3	50%
stream:http	3	50%

src = 192.168.250.70

hostname=gotham-fortigate devid=FGT604614044725 logid=0317013312 type=utm subtype=webfilter eventtype=ftgd

poisonivy-is-coming-for-you-batman.jpeg host=192.168.250.1 http_method=direct http_user_agent=unknown

Using stream:http

index=botsv1 dest=23.22.63.114 "poisonivy-is-coming-for-you-batman.jpeg" src=192.168.250.70 sourcetype="stream:http"

3 events (before 11/7/18 2:05:14.000 PM) No Event Sampling

Events (3) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 minute per column

List Format 20 Per Page

< Hide Fields All Fields

SELECTED FIELDS

- a dest 1
- a dest_ip 1
- a host 1
- a http_method 1
- a source 1
- a sourcetype 1
- a src 1
- a src_headers 1
- a url 1
- a url 1

INTERESTING FIELDS

- # ack_packets_in 2
- # ack_packets_out 2
- a app 1

1 Value, 66.667% of events

Reports

- Top values
- Top values by time
- Rare values

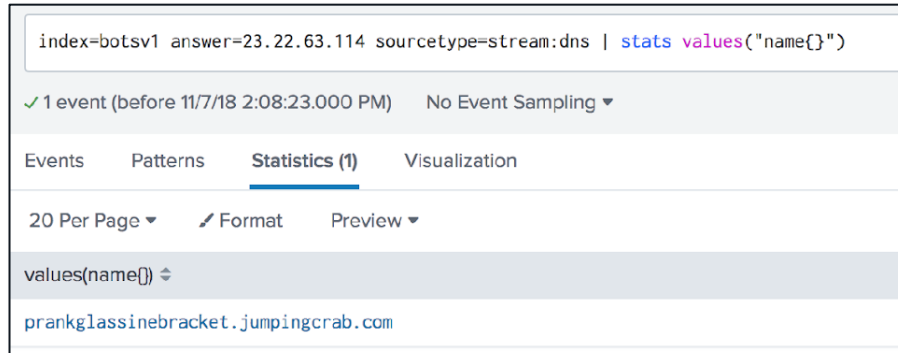
Events with this field

Values	Count	%
http://prankglassinebracket.jumpingcrab.com:1337:1337/poi	2	100%
sonivy-is-coming-for-you-batman.jpeg		

src=192.168.250.70

What if I don't have the file name?

- If we know there was DNS resolution to the malicious IP, how can we craft a search?
- DNS will be associated with the stream:dns sourcetype
- We identified a couple of IP addresses of interest even if we don't have the filename, we probably know that 23.22.63.114 is of concern



index=botsv1 answer=23.22.63.114 sourcetype=stream:dns | stats values("name{ }")

✓ 1 event (before 11/7/18 2:08:23.000 PM) No Event Sampling ▼

Events Patterns **Statistics (1)** Visualization

20 Per Page ▼ ✎ Format Preview ▼

values(name{ }) ⇅

prankglassinebracket.jumpingcrab.com

Identifying the FQDN of the system that defaced...

Kill Chain Phase: Command & Control

- This attack used dynamic DNS to resolve to the malicious IP. What fully qualified domain name (FQDN) is associated with this attack?

- `prankglassinebracket.jumpingcrab.com`

- More information on this topic

- <http://blogs.splunk.com/2015/08/04/detecting-dns-domains-in-splunk/>

Kill Chain

IP Scanning the Web Server:

40.80.148.42

Web Vulnerability Scanner:

Acunetix

Which Web Server?:

192.168.250.70/Joomla

Executable Uploaded:

3791.exe

Hash of the Uploaded File:

AAE3F5A29935E6ABCC2C2754D12A9A
F0

**File that Defaced Our Web
Server:** poisonivy-is-coming-
for-you-batman.jpeg



Brute Force Attack Originated:

23.22.63.114

**Identifying the First Password Attempted
in a Brute Force Attack**

Extracting Passwords from Events

Identifying the Password Used To Gain Access:

40.80.148.42

Determining The Elapsed Time Between Events

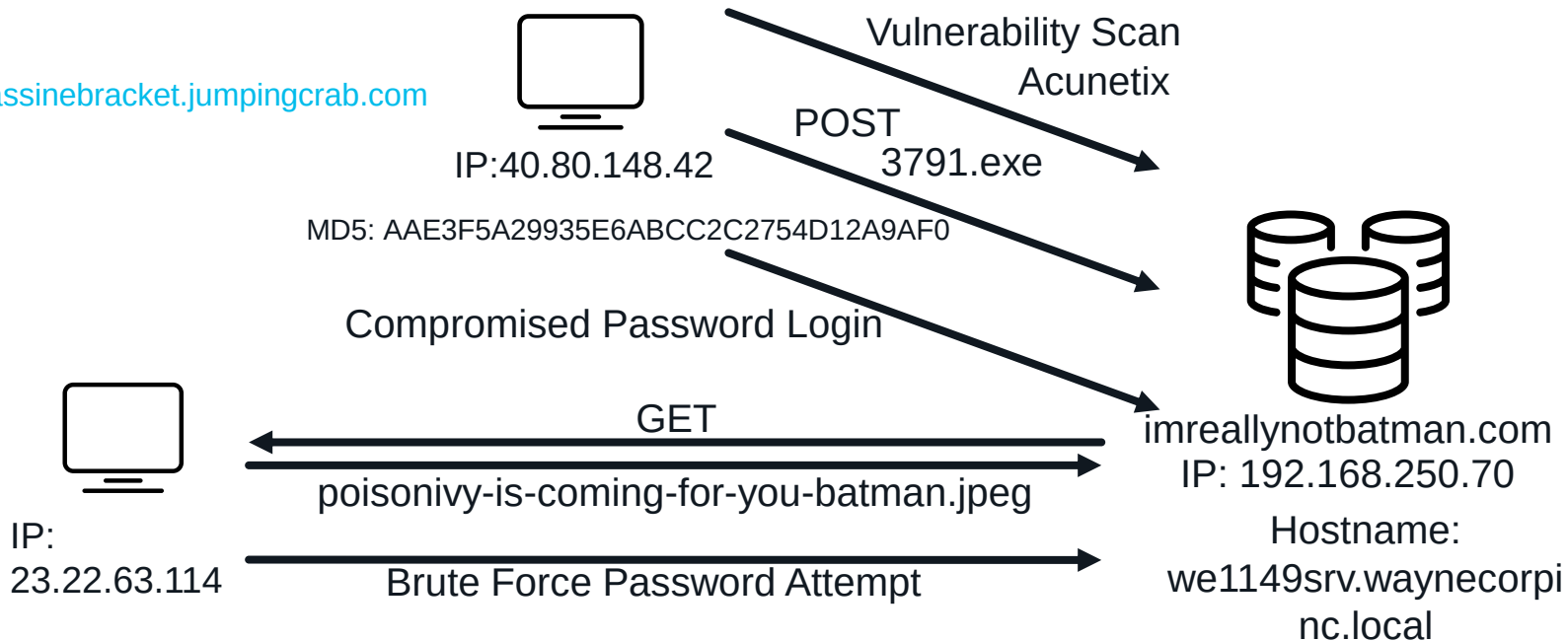
**Fully Qualified Domain Name of the System
that Defaced the Web Server:**

prankglassinebracket.jumpingcrab.com

APT picture

DNS:

prankglassinebracket.jumpingcrab.com

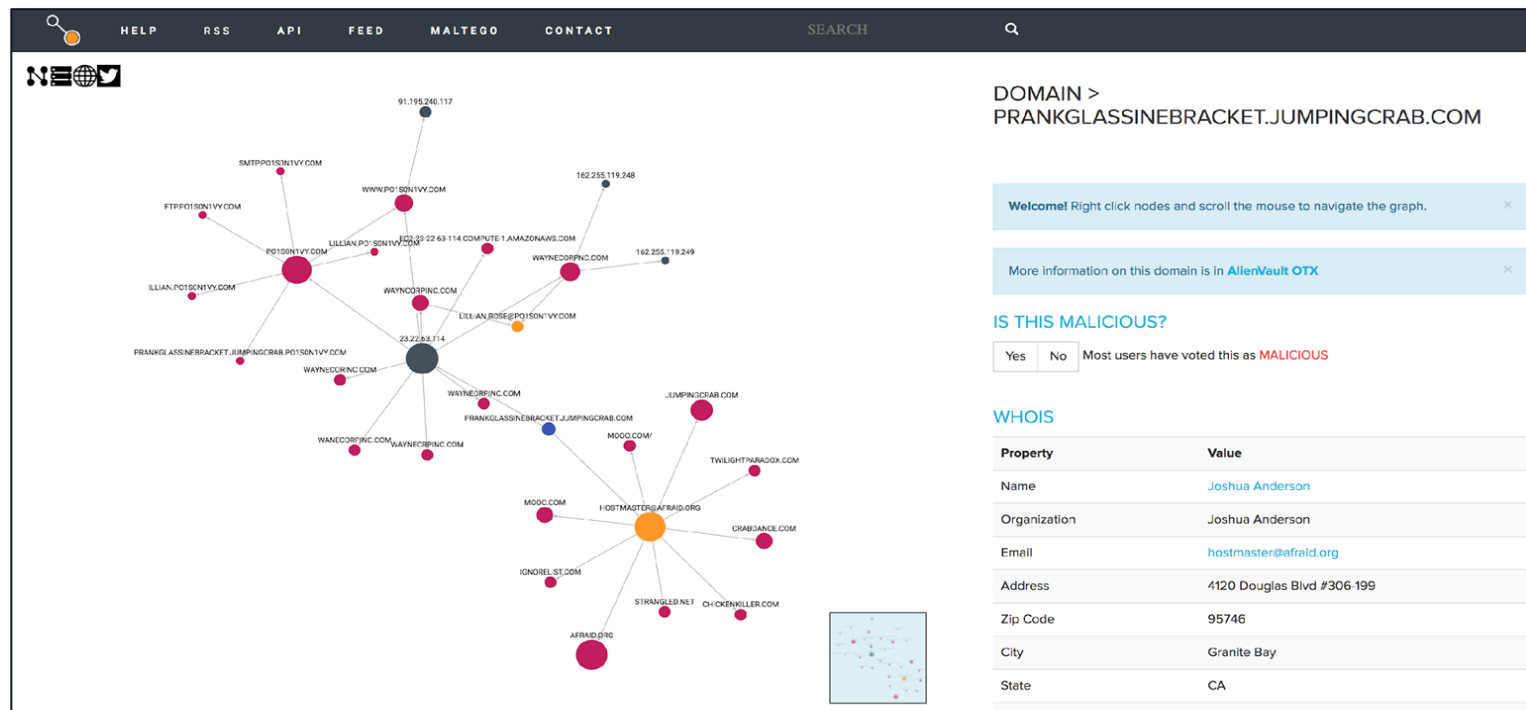


Using OSINT to identify attacker infrastructure

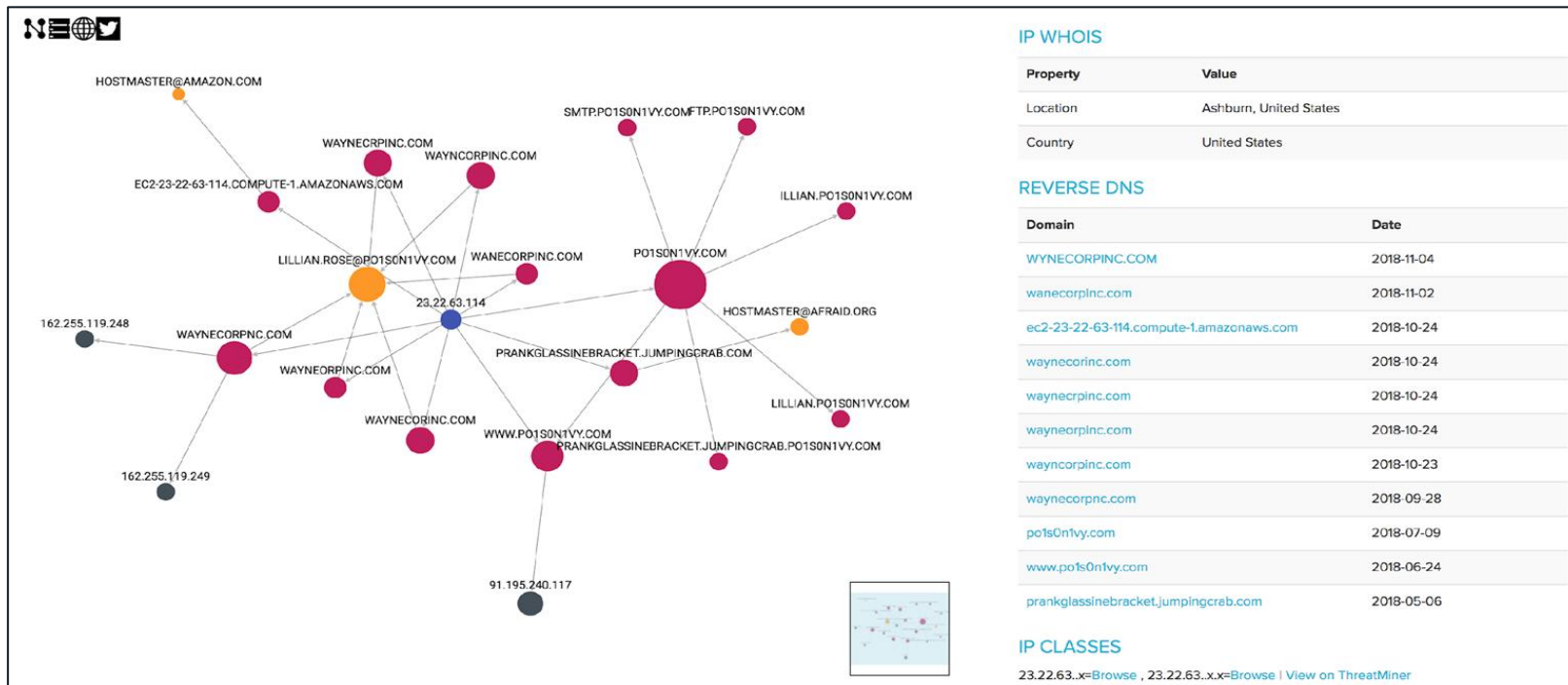
Kill Chain Phase: Weaponisation

- What IP address has P01s0n1vy tied to domains that are pre-staged to attack Wayne Enterprises?
- Bonus Question: What additional domains were tied to that IP address?
- Hints
 - Sites like VirusTotal and ThreatCrowd will help identify the domain to IP association

ThreatCrowd domain search



ThreatCrowd – Pivot to IP



Virus Total

File

URL

Search



prankglassinebracket.jumpingcrab.com



Search or Scan

By using VirusTotal you consent to our [Terms of Service](#) and [Privacy Policy](#) and allow us to share your submission with the security community. [Learn more.](#)

Passive DNS Replication ⓘ

Date resolved

IP address

2016-09-14

23.22.63.114

VirusTotal

23.22.63.114 IP address information

CountryUS

Autonomous system14618 (Amazon.com, Inc.)

Passive DNS Replication ⓘ

Date resolved	Domain
2018-11-04	wynecorpinc.com
2018-11-04	wayneorpinc.com
2018-11-04	ec2-23-22-63-114.compute-1.amazonaws.com
2018-11-04	waynecrpinc.com
2018-11-04	waynecorpnc.com
2018-11-04	waynecorinc.com
2018-11-04	wayncorpinc.com
2018-11-04	wanecorpinc.com
2018-07-18	po1s0n1vy.com
2018-05-19	www.po1s0n1vy.com
2018-05-02	prankglassinebracket.jumpingcrab.com

Using OSINT to identify attacker infrastructure

Kill Chain Phase: Weaponisation

● What IP address has P01s0n1vy tied to domains that are pre-staged to attack Wayne Enterprises?

○ 23.22.63.114

● Bonus Question: What additional domains were tied to that IP address?

○ wynecorpinc.com

○ wayneorpinc.com

○ waynecrpinc.com

○ waynecorpnc.com

○ waynecorinc.com

○ wayncorpinc.com

○ wanecorpinc.com

○ po1s0n1vy.com

Kill Chain

IP Scanning the Web Server:

40.80.148.42

Web Vulnerability Scanner:

Acunetix

Which Web Server?:

192.168.250.70/Joomla

Executable Uploaded:

3791.exe

Hash of the Uploaded File:

AAE3F5A29935E6ABCC2C2754D12A9A
F0

File that Defaced Our Web

Server: poisonivy-is-coming-
for-you-batman.jpeg



Reconnaissance

Weaponisation

Delivery

Exploitation

Installation

Command &
Control

Actions on
Objectives

Attacker Infrastructure: wynecorpinc.com,
wayncorpinc.com, waynecorinc.com,
waynecrpinc.com, wayneorpinc.com,
wanecorpinc.com, po1s0n1vy.com

Brute Force Attack Originated:

23.22.63.114

Identifying the First Password Attempted in a Brute Force Attack

Extracting Passwords from Events

Identifying the Password Used To Gain Access:

40.80.148.42

Determining The Elapsed Time Between Events

Fully Qualified Domain Name of the System that Defaced the Web Server:

prankglassinebracket.jumpingcrab.com

APT picture

DNS:
prankglassinebracket.jumpingcrab.com

Other Domains:
wynecorpinc.com
wayncorpinc.com
waynecorinc.com
waynecrpinc.com,
wayneorpinc.com,
wanecorpinc.com
po1s0n1vy.com



MD5: AAE3F5A29935E6ABCC2C2754D12A9AF0

Compromised Password Login

GET

poisonivy-is-coming-for-you-batman.jpeg

Brute Force Password Attempt

Vulnerability Scan
Acunetix

POST
3791.exe



imreallynotbatman.com
IP: 192.168.250.70
Hostname:
we1149srv.waynecorpi
nc.local

Using OSINT to identify associated malware

Kill Chain Phase: Delivery

- GCPD reported that common TTPs (Tactics, Techniques, Procedures) for the P01s0n1vy APT group if initial compromise fails is to send a spear phishing email with custom malware attached to their intended target. This malware is usually connected to P01s0n1vy's initial attack infrastructure. Using research techniques, provide the SHA256 hash of this malware.
- Bonus Question: What is the name of the file that matches the hash?
- Hints
 - The initial compromise was successful, so the email was never sent. Splunk will not contain the answer.
 - You have a number of indicators already collected, use these!
 - ThreatMiner, VirusTotal and Hybrid-Analysis are all good OSINT sites to look for malware

Back to OSINT

- What do we know about the attack infrastructure from our earlier investigation?
 - IPs of Attack Infrastructure
 - List of Domains
- Anything else?

TheatMiner

Host: 23.22.63.114

Note: if you are new to ThreatMiner, check out the [how-to](#) page to find out **how** you can get the most out of this portal.

Search for domains, IPs, MD5|SHA1|SHA256, email address or ssl(ssl:), user-agent(ua:), AV family(av:), filename (filename:), URI (uri:), regi



- Threatminer can give me an MD5 of samples from 23.22.63.114 but not SHA256

Related samples

Copy

Excel

CSV

PDF

Search:

MD5	Detections	Analysis Date																						
c99131e0169171935c5ac32615ed6261	<table><tr><td>ALYac</td><td>Trojan.GenericKD.3470547</td></tr><tr><td>AVG</td><td>Agent5.APHV</td></tr><tr><td>AVware</td><td>Trojan.Win32.GenericIBT</td></tr><tr><td>Ad-Aware</td><td>Trojan.GenericKD.3470547</td></tr><tr><td>AegisLab</td><td>Agent5.Aphv.Genlc</td></tr><tr><td>AhnLab-V3</td><td>Malware/Gen.Generic.N2081883700</td></tr><tr><td>Antiy-AVL</td><td>Trojan[Backdoor]/Win32.Redsip</td></tr><tr><td>Arcabit</td><td>Trojan.Generic.D34F4D3</td></tr><tr><td>Avira</td><td>TR/AD.Zupdax.qmyx</td></tr><tr><td>BitDefender</td><td>Trojan.GenericKD.3470547</td></tr><tr><td>DrWeb</td><td>Trojan.MulDrop6.51432</td></tr></table>	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	DrWeb	Trojan.MulDrop6.51432	2016-09-01 09:03:44
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																							
DrWeb	Trojan.MulDrop6.51432																							

ThreatMiner - File Metadata

Sample: c99131e0169171935c5ac32615ed6261

Note: if you are new to ThreatMiner, check out the [how-to](#) page to find out how you can get the most out of this portal.

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:	bc927ff06263351f43dbdec88e4b08485e07996
SHA256:	9709473ab351387aab9e816eff3910b9f28a7a70202e250ed46dba8f820f34a8
SHA512:	8fb3b09541b021e06eeec455876526607114adb547eacb7556d578c08959154b80f01bac905383a5eb4c8a9091a3fb14dc13badc36a05ea7718b4b1053f2fdb
SSDEEP:	12288:JCy+DdcUrY4tO3Rc5F5H8q3/HSaRanZ0:Jj+COpO3Rc5F5H8q3/yaRaZ0
IMPHASH:	fae2c8486a11f609323cc15c0ee838cf
Authentihash:	N/A
Related resources	<div><div>VirusTotal</div><div>Hybrid-Analysis</div><div>ThreatExpert</div><div>Malwr</div><div>VirusShare</div></div>

VirusTotal - File Hash

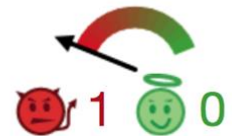


SHA256: 9709473ab351387aab9e816eff3910b9f28a7a70202e250ed46dba8f820f34a8

File name: MirandaTateScreensaver.scr.exe

Detection ratio: 39 / 64

Analysis date: 2017-08-16 17:42:13 UTC (1 month, 2 weeks ago)



Analysis

File detail

Additional information

Comments 1

Votes

Behavioural information

Antivirus	Result	Update
Ad-Aware	Trojan.Generic.17934902	20170816
AegisLab	Agent5.Aphv.Gen!c	20170816

Using OSINT to identify associated malware

Kill Chain Phase: Delivery

●GCPD reported that common TTPs (Tactics, Techniques, Procedures) for the Po1s0n1vy APT group, if initial compromise fails, is to send a spear phishing email with custom malware attached to their intended target. This malware is usually connected to Po1s0n1vy's initial attack infrastructure. Using research techniques, provide the SHA256 hash of this malware.

○9709473ab351387aab9e816eff3910b9f28a7a70202e250ed46dba8f820f34a8

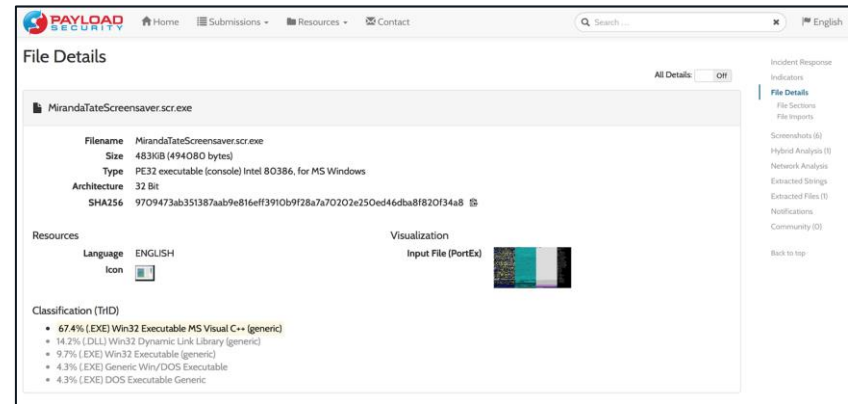
●Bonus Question: What is the name of the file that was matches the hash?

○MirandaTateScreensaver.scr.exe

●Other sites of interest:

○www.hybrid-analysis.com

○virusshare.com



IP Scanning the Web Server:

40.80.148.42

Web Vulnerability Scanner:

Acunetix

Which Web Server?:

192.168.250.70/Joomla

**Using OSINT to Identify
Associated Malware:**

9709473ab351387aab9e816eff3

910b9f28a7a70202e250ed46dba

8f820f34a8

File Name:

MirandaTateScreensaver.scr.exe

Executable Uploaded:

3791.exe

Hash of the Uploaded File:

AAE3F5A29935E6ABCC2C2754D12A9A

F0

**File that Defaced Our Web
Server:** poisonivy-is-coming-
for-you-batman.jpeg



Attacker Infrastructure: wynecorpinc.com,
wayncorpinc.com, waynecorinc.com,
waynecrpinc.com, wayneorpinc.com,
wanecorpinc.com, po1s0n1vy.com

Brute Force Attack Originated:

23.22.63.114

**Identifying the First Password Attempted
in a Brute Force Attack**

Extracting Passwords from Events

Identifying the Password Used To Gain Access:

40.80.148.42

Determining The Elapsed Time Between Events

**Fully Qualified Domain Name of the System
that Defaced the Web Server:**
prankglassinebracket.jumpingcrab.com

APT picture

DNS:

prankglassinebracket.jumpingcrab.com

Other Domains:

wynecorpinc.com

wayncorpinc.com

waynecorinc.com

waynecrpinc.com,

wayneorpinc.com,

www.po1s0n1vy.com

wanecorpinc.com

po1s0n1vy.com

IP:
23.22.63.114



IP:40.80.148.42

MD5: AAE3F5A29935E6ABCC2C2754D12A9AF0

Compromised Password Login

GET

poisonivy-is-coming-for-you-batman.jpeg

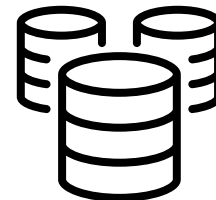
Brute Force Password Attempt

Phishing Email

SHA256: 9709473ab351387aab9e816eff3910b9f28a7a70202e250ed46dba8f820f34a8
File Name: MirandaTateScreensaver.scr.exe

Vulnerability Scan
Acunetix

POST
3791.exe



imreallynotbatman.com
IP: 192.168.250.70

Hostname:
we1149srv.waynecorpin
c.local

Domain:
waynecorpinc.local

APT summary

- Scanned for vulnerabilities
- Found site is running Joomla
- Performed a brute force password scan, logged into Joomla, installed file upload modules
- Uploaded webshell
- Used webshell to upload reverse TCP shell
- Connected via metasploit
- Tried to move around but couldn't get out of locked down Windows 2012R2
- Defaced website with downloaded defacement image

IP Scanning the Web Server:

40.80.148.42

Web Vulnerability Scanner:

Acunetix

Which Web Server?:

192.168.250.70/Joomla

**Using OSINT to Identify
Associated Malware:**

9709473ab351387aab9e816eff3

910b9f28a7a70202e250ed46dba

8f820f34a8

File Name:

MirandaTateScreensaver.scr.exe

Executable Uploaded:

3791.exe

Hash of the Uploaded File:

AAE3F5A29935E6ABCC2C2754D12A9A

F0

**File that Defaced Our Web
Server: [poisonivy-is-coming-
for-you-batman.jpeg](#)**



Attacker Infrastructure: [wyneorpinc.com](#),
[wayncorpinc.com](#), [waynecorinc.com](#),
[waynecrpinc.com](#), [wayneorpinc.com](#),
[wanecorpinc.com](#), [po1s0n1vy.com](#)

Brute Force Attack Originated:

23.22.63.114

**Identifying the First Password Attempted
in a Brute Force Attack**

Extracting Passwords from Events

Identifying the Password Used To Gain Access:

40.80.148.42

Determining The Elapsed Time Between Events

**Fully Qualified Domain Name of the System
that Defaced the Web Server:**
[prankglassinebracket.jumpingcrab.com](#)

Overall APT picture

DNS:
prankglassinebracket.jumpingcrab.co
m

Other Domains:
wynecorpinc.com
wayncorpinc.com
waynecorinc.com
waynecrpinc.com,
wayneorpinc.com,
www.po1s0n1vy.com
wanecorpinc.com
po1s0n1vy.com

IP:
23.22.63.114



IP:40.80.148.42

MD5: AAE3F5A29935E6ABCC2C2754D12A9AF0

Vulnerability Scan
Acunetix

POST
3791.exe

Compromised Password Login

GET

poisonivy-is-coming-for-you-batman.jpeg

Brute Force Password Attempt

Phishing Email

SHA256: 9709473ab351387aab9e816eff3910b9f28a7a70202e250ed46dba8f820f34a8
File Name: MirandaTateScreensaver.scr.exe



imreallynotbatman.com
IP: 192.168.250.70

Hostname:
we1149srv.waynecorpi
nc.local

Domain:
waynecorpinc.loca
l

In summary

Use the data you have

- If you see gaps in coverage, consider expanding them
- Stream (wire data) and sysmon are good for detecting things AV or other security technologies may miss

Find web sites of value and save them for when you need them

Learn the Splunk commands

At search, if you don't see the data you are looking for, find those additional fields

Use time picker to narrow the field of search

- Performance improvements and fewer results to examine

Pivot down on interesting fields and keep pivoting as needed

Next steps

If you would like to work with this data set or practice the exercises from this workshop further, now you can!

- <https://www.splunk.com/blog/2018/05/10/boss-of-the-soc-scoring-server-questions-and-answers-and-dataset-open-sourced-and-ready-for-download.html>
- http://explore.splunk.com/BOTS_1_0_datasets

Looking for a Sandbox with the Data Sets?

- <https://www.splunk.com/blog/2018/05/03/introducing-the-security-datasets-project.html>
- <http://live.splunk.com/splunk-security-dataset-project>

If you load BOTS v1 data, the Boss of the SOC Investigation Workshop for Splunk app can be installed to practice some of the techniques used today

- This app is already embedded in the dataset project
- <https://splunkbase.splunk.com/app/3985/>

BOSS Platform

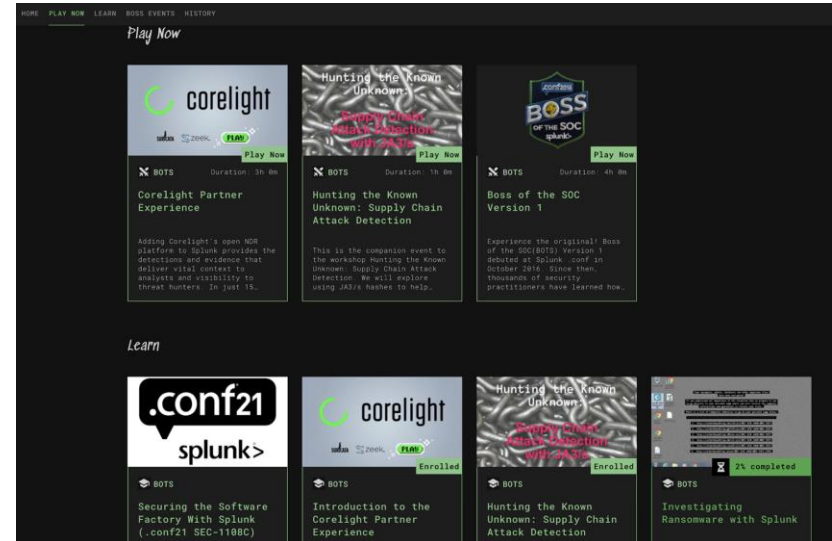
<https://bots.splunk.com>

24x7 Access

Login with Splunk.com account (just like Splunkbase)

Used for all BOTS competition events

More content to be added



Splunk for security workshops



Legend

 Splunk Enterprise / Cloud  Enterprise Security  SOAR  UBA

Keynote Deep Dives

Wednesday
10:30am – 11:30am



Experiences Amplified:
How AI Can Fuel
Better Employee
and Customer
Experiences

Level 1
Room 106



Smart, Secure,
Seamless:
Transforming
Experiences with
Next-Generation
Networking

Level 2
Room 204



Harness a Bold
New Era:
Transform Data
Centre and
Service Provider
Connectivity

Level 2
Room 203



Securing User to
Application and
Everything in
Between

Level 2
Melbourne Room 2



Unlocking
Digital Resilience
through Unified
Observability

The HUB
Centre Stage

Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.



Complete your surveys in the **Cisco Live mobile app**.



Continue your education

- Visit the Cisco Stand for related demos
- Book your one-on-one Meet the Expert meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand



Thank you

CISCO *Live!*

#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC