

# Investigating with Splunk Workshop

May 2023 | Version 2.2

**Based on BOTS 1.0 Dataset**

Randy Holloway, CISSP, MS / Staff Sales Engineer

**splunk**® turn data into doing™

# #whoami

Randy Holloway

[rholloway@splunk.com](mailto:rholloway@splunk.com)

Based in Houston, TX

23+ Years IT and Security Experience

14+ Years SIEM Experience

Came Over from ArcSight

Enjoys Michigan Football and Baseball



Why Investigating?

Scenario Review

Investigating an APT

Investigating Ransomware



# Investigate (Thanks, Google!)

in·ves·ti·gate

/in'vestə,gāt/ 

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"

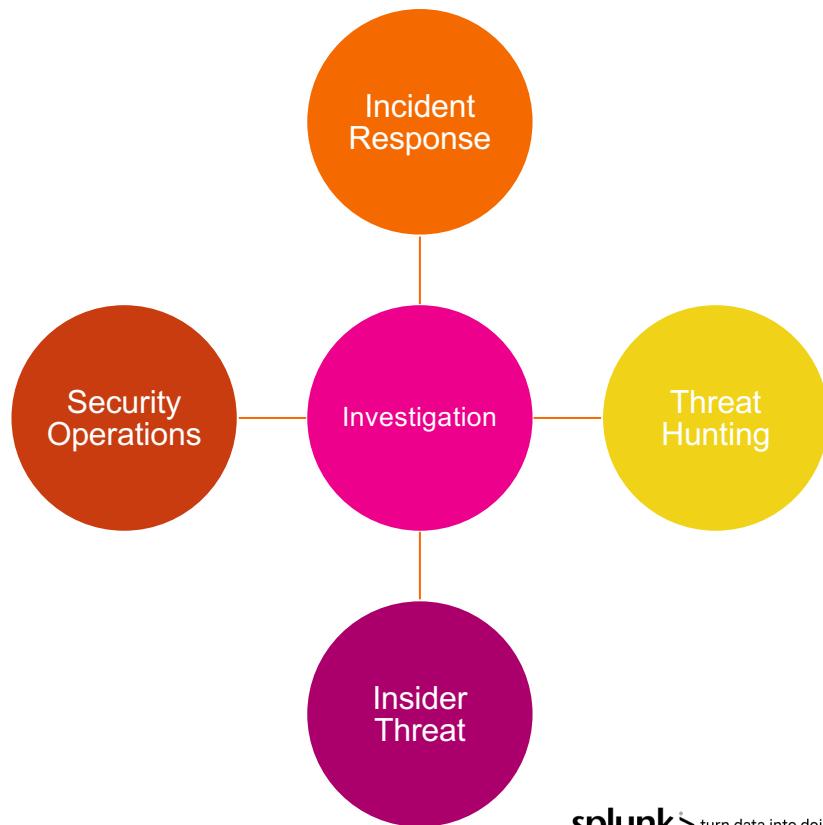


# Investigating Is A Core Competency

When something is detected, we want to figure out what happened

Who, what, where, when, why, how?

Investigating can be reactive or proactive



# Using Splunk for Security

Investigations



**YOUR  
SITE  
HAS BEEN  
DEFACED**

P01s0n1vy was HERE

Deal with it, Admin



# Luckily Everything Is Captured In Splunk

Microsoft Sysmon

Windows Events

Windows Registry

IIS

Splunk Stream (wire data)

Suricata

Fortigate (NGFW)

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

- Search Bar:** sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" EventCode=2 TargetFilename="C:\\Users\\bob.smith.WAYNECORPINC\\\"
- Results Summary:** 2,252 events (before 10/31/18 12:10:14.000 PM) No Event Sampling \*
- Event List:** The results list shows two events from August 24, 2016, at 5:17:17.000 PM. Both events are XML snippets representing Windows Sysmon logs. The first event is from host 'we8105desk' and the second is from host 'we8105desk'. Both events detail a process creation event for 'Image' (explorer.exe) with ProcessId 2044, triggered by User 'S-1-5-18' (bob.smith) on a computer named 'we8105desk'. The logs include various system metadata like ThreadId, Channel, and Correlation IDs.
- Interface Elements:** The interface includes standard Splunk search controls like 'Format Timeline', 'Zoom Out', 'Smart Mode', and a pagination bar showing page 1 of 8.

# 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

**splunk**<sup>®</sup> turn data into doing<sup>™</sup>

# Access Class Material

Items of Interest can be found by going to this Google Drive:

1. This link will have your Lab Guide, Splunk Instance Details and more:  
<https://tinyurl.com/splunkworkshops>
2. Follow the guidance of your instructor on accessing / noting which instance you will use for this workshop, along with getting access to the slides and lab guide.

# Starting Point

Please make sure you are logged in and seeing this window

Use the search & reporting app to hunt. ONLY use the Investigating app AFTER you find your results and you want to verify what you found is correct.

splunk>enterprise

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find Search icon

**Apps** ⚙️

-  Search & Reporting
-  Investigating with Splunk Workshop
- + Find More Apps

**Explore Splunk Enterprise**

 **Product Tours**  
New to Splunk? Take a tour to help you on your way.

 **Add Data**  
Add or forward data to Splunk Enterprise. Afterwards, you may [extract fields](#).

 **Explore Data**  
Explore data and define how Hunk parses that data.

 **Splunk Apps**  ⓘ  
Apps and add-ons extend the capabilities of Splunk Enterprise.

Close

# Quick Intro To The App

**App: Investigating with Splunk Workshop**

Overview ▾ Scenario #1 - APT ▾ Scenario #2 - Ransomware ▾ Supplemental Material ▾ Search Dashboards

Investigating with Splunk Workshop

**Introduction**

**Investigating with Splunk Workshop**

Welcome to the Investigating with Splunk Workshop based on the Boss of the SOC 2016 data set.

This workshop is designed to provide a hands-on walk through using Splunk as an investigative tool. The focus of this hands on will be an APT scenario and a ransomware scenario.

The hands-on exercise for this workshop is based on the BOTS data set that was developed in 2016 and used for the first iteration of Boss of the SOC. During this workshop, you assume the persona of Alice Bluebird, the analyst who has recently been hired to protect and defend Wayne Enterprises against various forms of cyberattack.

**YOUR SITE HAS BEEN DEFACED**

P01s0n1vy was HERE

Deal with it, Admin

Recycle Bin #DECRYPT MY FILES#

Your documents, photos, databases and other important files have been encrypted!

If you understand all importance of the situation then we propose to you to go directly to your personal page where you will receive the complete instructions and guarantees to restore your files.

There is a list of temporary addresses to go on your personal page below:

1. <http://cerberihyed5frqa.xmfir0.win/30EF-3C4E-A460-005E-93C9>  
2. <http://cerberihyed5frqa.gkfit9.win/30EF-3C4E-A460-005E-93C9>  
3. <http://cerberihyed5frqa.38iot.win/30EF-3C4E-A460-005E-93C9>  
4. <http://cerberihyed5frqa.dktis5.win/30EF-3C4E-A460-005E-93C9>  
5. <http://cerberihyed5frqa.cned9.win/30EF-3C4E-A460-005E-93C9>  
6. [http://cerberihyed5frqa.onion/30EF-3C4E-A460-005E-93C9 \(TOR\)](http://cerberihyed5frqa.onion/30EF-3C4E-A460-005E-93C9 (TOR))

9:49 PM 8/26/2016

We first suggest you check out the resources below to learn about the environment. Next, review how the dataset was constructed and what sourcetypes exist and why. Finally, work through the hands-on exercises for both APT and Ransomware to learn how an adversary would follow a Kill Chain to attack Wayne Enterprises.

# Screen Layout

## What Kinds of Events Do I Have?

Edit Export ...

### 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?

**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

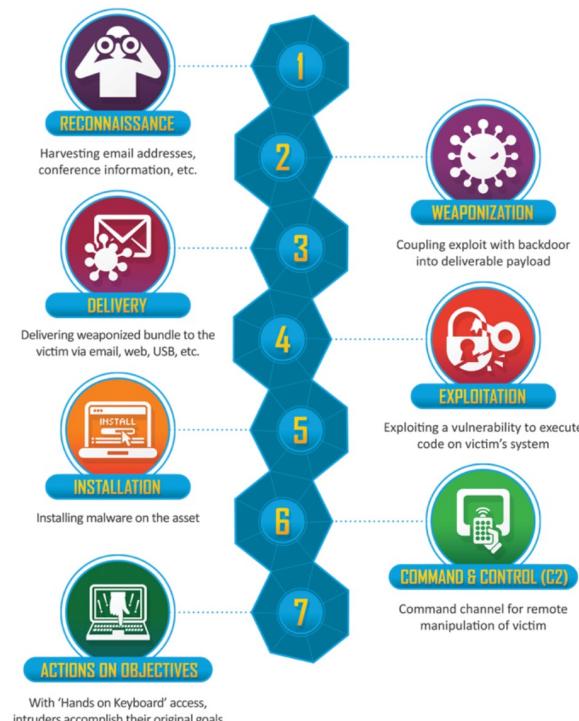
**splunk**<sup>®</sup> turn data into doing<sup>™</sup>

## 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.

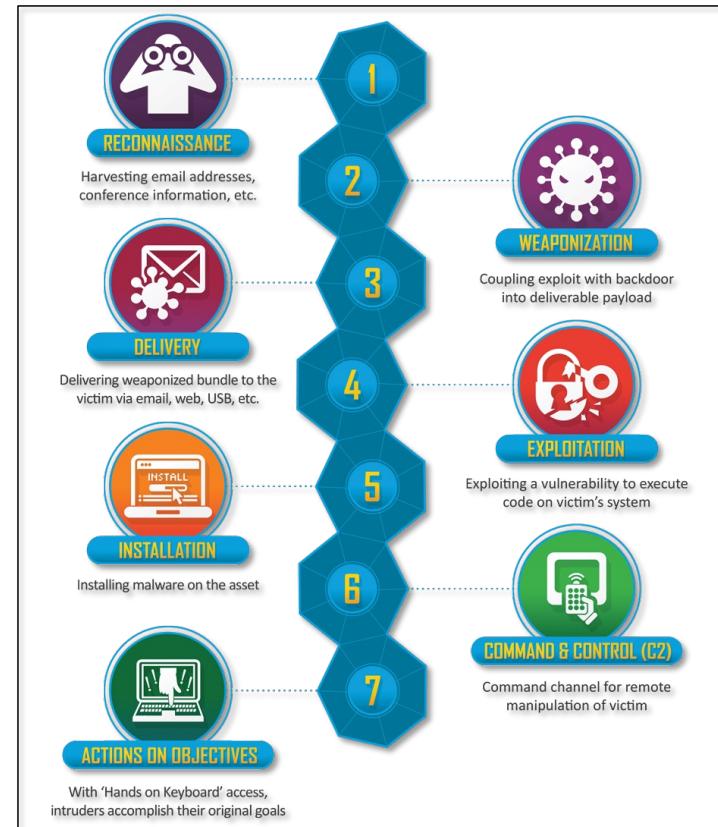


# Lockheed Martin Cyber Kill Chain

Method for characterizing 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

<http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf>



# 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 imreallynotbatman.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 sourcetypes Associated with Search Values

## Kill Chain Phase: Reconnaissance

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

- Search Bar:** index=botsv1 imreallynotbatman.com
- Results Summary:** 78,682 events (before 11/5/18 7:13:45.000 PM) No Event Sampling
- Event View:** Events (78,682) Patterns Statistics Visualization
- Timeline:** Format Timeline - Zoom Out + Zoom to Selection X Deselect 1 minute per column
- Selected Fields:** host 3 source 4 sourcetype 4
- Interesting Fields:** ack\_packets\_in 41 ack\_packets\_out 12 action 3 app 4 app\_proto 1 bytes\_100+ bytes\_in 100+ bytes\_out 100+ c\_ip 3 cached 2 capture\_hostname 1 client\_rtt 100+
- Sourcetype Report:** A modal window titled "sourcetype" is open, showing:
  - 4 Values, 100% of events
  - Reports: Top values, Top values by time, Rare values
  - Events with this field
  - Values table:

Values	Count	%
suricata	30,625	38.922%
stream:http	22,199	28.214%
fgt_utm	13,918	17.689%
iis	11,940	15.175%
  - Raw event example:

```
src_ip: 192.168.250.70
src_port: 80
timestamp: 2016-08-10T16:23:09.473182-0600
}
Show as raw text
```
  - Host information: host = suricata-ids.waynecorpinc.local | source = /var/log/suricata/eve.json | sourcetype = suricata

# Finding Source Addresses

## Kill Chain Phase: Reconnaissance

The screenshot shows a Splunk search results page for the index `botsv1` with the query `imreallynotbatman.com`. The search found 78,682 events between Aug 10, 2016, and Aug 11, 2016. A histogram at the top right shows event distribution over time. Below the search bar, there are tabs for Events (78,682), Patterns, Statistics, and Visualization. The Events tab is selected. On the left, under 'SELECTED FIELDS', the field `src` is highlighted. A modal window titled 'src' is open, showing '3 Values, 84.825% of events'. It has 'Selected' buttons for 'Yes' (highlighted) and 'No'. The 'Reports' section includes 'Top values', 'Top values by time', and 'Rare values'. Below this, a table lists 'Values' with their 'Count' and '%':

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%

At the bottom of the modal, there is raw JSON data:

```
src_port: 80
timestamp: 2016-08-10T16:23:09.473182-0600
}
Show as raw text
```

Below the modal, the main search results table shows the following fields for a selected event:

host	source	sourcetype
suricata-ids.waynecorpinc.local	/var/log/suricata/eve.json	data

A large pink arrow points from the bottom right of the modal down towards the bottom of the screen, pointing to the Splunk logo.

# Selecting a sourcetype and Searching for Source Address

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

- Search Bar:** The search bar contains the query `index=botsv1 imreallynotbatman.com sourcetype="stream:http"`, which is highlighted with a pink rectangle.
- Event Statistics:** 22,199 events (before 11/5/18 7:26:39.000 PM) with No Event Sampling.
- Event View:** The Events (22,199) tab is selected. A histogram shows event distribution over time. Below it, a table lists event values with counts and percentages:

Values	Count	%
40.80.148.42	20,964	94.437%
23.22.63.114	1,235	5.563%
- Field Details:** A modal window is open for the 'src' field, also highlighted with a pink rectangle. It shows:
  - Selected:** Yes (button is highlighted)
  - Reports:** Top values, Top values by time, Rare values
  - Events with this field:** A list of event details including:
    - client\_ip: 40.80.148.42
    - 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
    - date\_offset\_time: 0

A large pink arrow points from the bottom right towards the 'src' field details.

# Validation with suricata

The screenshot shows a Splunk search interface for Suricata logs. The search bar at the top contains the query: `index=botsv1 imreallynotbatman.com src=40.80.148.42 sourcetype=suricata`. The search results show 17,484 events from before November 5, 2018, at 7:31:58.000 PM. The interface includes tabs for Events (17,484), Patterns, Statistics, and Visualization. A timeline visualization shows event counts over time, with a note indicating "1 minute per column". Below the timeline is a table view of the first event. The event details are as follows:

Time	Event
8/10/16 10:21:19.243 PM	{ [-] 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 }

The table also includes a "Show as raw text" link. At the bottom of the search results, the host, source, sourcetype, and source IP are listed: host = suricata-ids.waynecorpinc.local | source = /var/log/suricata/eve.json | sourcetype = suricata | src = 40.80.148.42. A large red arrow points downwards towards the bottom right corner of the search results area.

# More Fields...

*a tag* 3  
*a tag::eventtype* 3  
*# timeendpos* 1  
*a timestamp* 100+  
*# timestamppos* 1  
*a transport* 1  
*a url* 100+  
*a vendor* 1

**19 more fields**

**+ Extract New Fields**

Select Fields

sig

Field

	# of Values	Event Coverage	Type
alert.signature	46	2.71%	String
alert.signature_id	46	2.71%	Number
<b>signature</b>	46	2.71%	String

Reports

Top values Events with this field

ET WEB\_SERVER Script tag in URI, Possible Cross Site Scripting Attempt  
ET WEB\_SERVER Onmouseover= in URI - Likely Cross Site Scripting Attempt  
ET WEB\_SERVER Possible XXE SYSTEM ENTITY in POST BODY.  
SURICATA HTTP Host header invalid  
ET WEB\_SERVER Possible SQL Injection Attempt SELECT FROM  
ET WEB\_SERVER SQL Injection Select Sleep Time Delay  
ET WEB\_SERVER Possible CVE-2014-6271 Attempt  
ET WEB\_SERVER Possible CVE-2014-6271 Attempt in Headers  
ET WEB\_SERVER PHP tags in HTTP POST  
GPL WEB\_SERVER global.asa access

suricata\_signature\_id

# 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

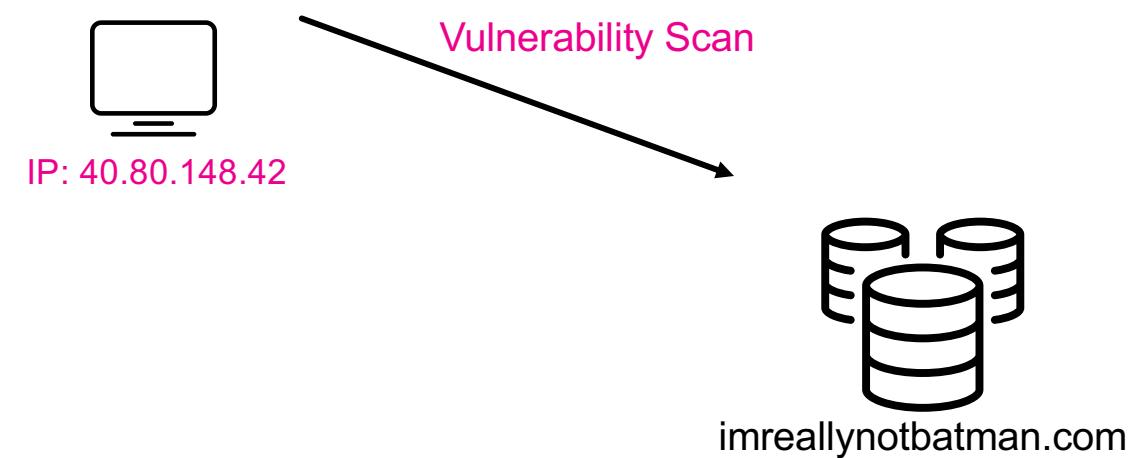


# Kill Chain

IP Scanning the Web Server: 40.80.148.42



# APT Picture



# Identifying The Web Vulnerability Scanner

Kill Chain Phase: Reconnaissance

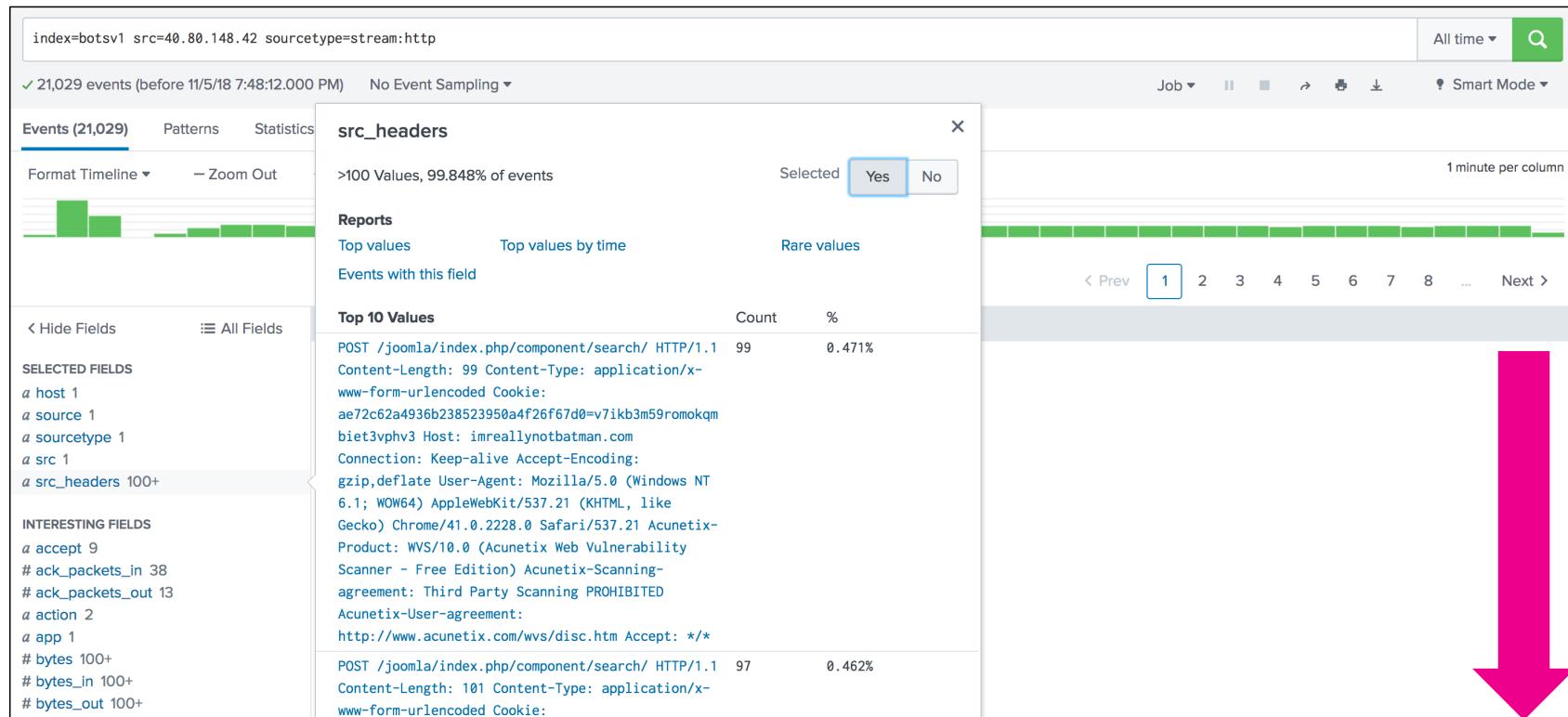
What company created the web vulnerability scanner used by Po1s0n1vy?

## 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 All time

✓ 21,029 events (before 11/5/18 7:53:25.000 PM) No Event Sampling ▾ Job ▾ II Smart Mode ▾

**Events (21,029)** Patterns Statistics Format Timeline ▾ — Zoom Out

51 Values, 99.762% of events 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 0GiavBMT)	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\``\`&nslookup 40z0JB6D\``\`	1	0.005%
" "	1	0.005%

1 minute per column

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

**SELECTED FIELDS**

- a host 1
- a http\_user\_agent 51
- a source 1
- a sourcetype 1
- a src 1
- a src\_headers 100+

**INTERESTING FIELDS**

- a accept 9
- # ack\_packets\_in 38
- # ack\_packets\_out 13
- a action 2
- a app 1
- # bytes 100+
- # bytes\_in 100+

# 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?

[acunetix.com - Web Vulnerability Scanner](https://www.acunetix.com/)  
Ad 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.

[Try Acunetix For Free Now](#)  
Test Acunetix Vulnerability Scanner With Our 14-Day Free Trial Today.

[Website security - keep in check with Acunetix](#)  
[https://www.acunetix.com/ ▾](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 ...



[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=uM6X42rXRoE ▾](https://www.youtube.com/watch?v=uM6X42rXRoE)  
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

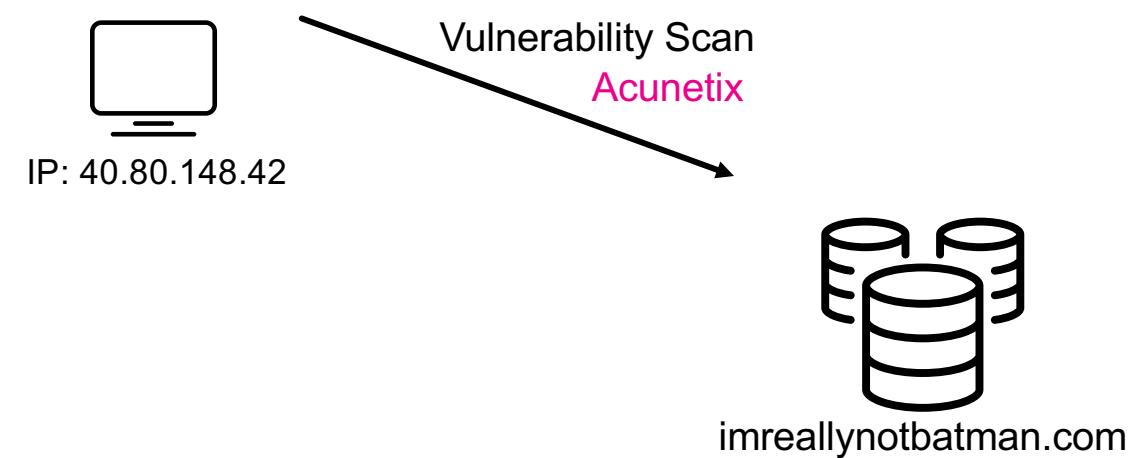
# Kill Chain

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
- URLs contain information that will lead you in the right direction

# Where to start?

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.navegabem.com/cms-website-design.html)  
<https://www.navegabem.com/cms-website-design.html>

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 All time

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

Events (21,029) Patterns Statistics Visualization

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



< Hide Fields All Fields

**SELECTED FIELDS**

- dest 2
- host 1
- http\_user\_agent 51
- source 1
- sourcetype 1
- src 1
- src\_headers 100+

**INTERESTING FIELDS**

- accept 9
- # ack\_packets\_in 38
- # ack\_packets\_out 13
- action 2
- app 1
- # bytes 100+
- 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

**dest**

2 Values, 100% of events Selected  Yes  No

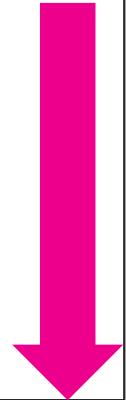
**Reports**

[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%

◀ Prev 1 2 3 4 5 6 7 8 ... Next ▶



# 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 ▾ Job ▾ || ⌂ ⌄ ⌅ ⌆ Smart Mode ▾

Events (22,671) Patterns Statistics Visualization Format Timeline ▾ – Zoom Out + Zoom to Selection × Deselect 1 day per column

**uri** Selected Yes No

>100 Values, 99.859% of events 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%

◀ Prev 1 2 3 4 5 6 7 8 ... Next ▶ , image/png, \*/\*

◀ 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
- a action 2
- a app 1
- # bytes 100+

# 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.navegabem.com/cms-website-design.html)  
<https://www.navegabem.com/cms-website-design.html>

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

What is WordPress content management system?

What is the Joomla?

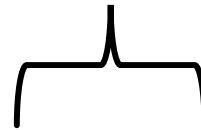
**Joomla** is an open source platform on which Web sites and applications can be created. It is a content management system (CMS) which connects your site to a MySQLi, MySQL, or PostgreSQL database in order to make content management and delivery easier on both the site manager and visitor.

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

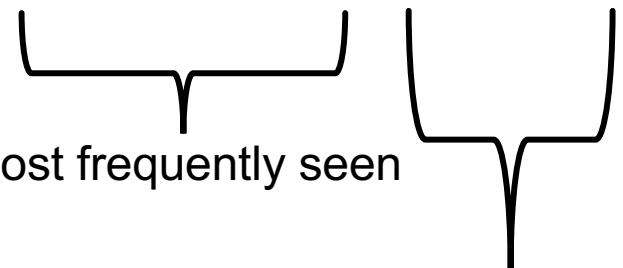
Search for: [What is the Joomla?](#)

# 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

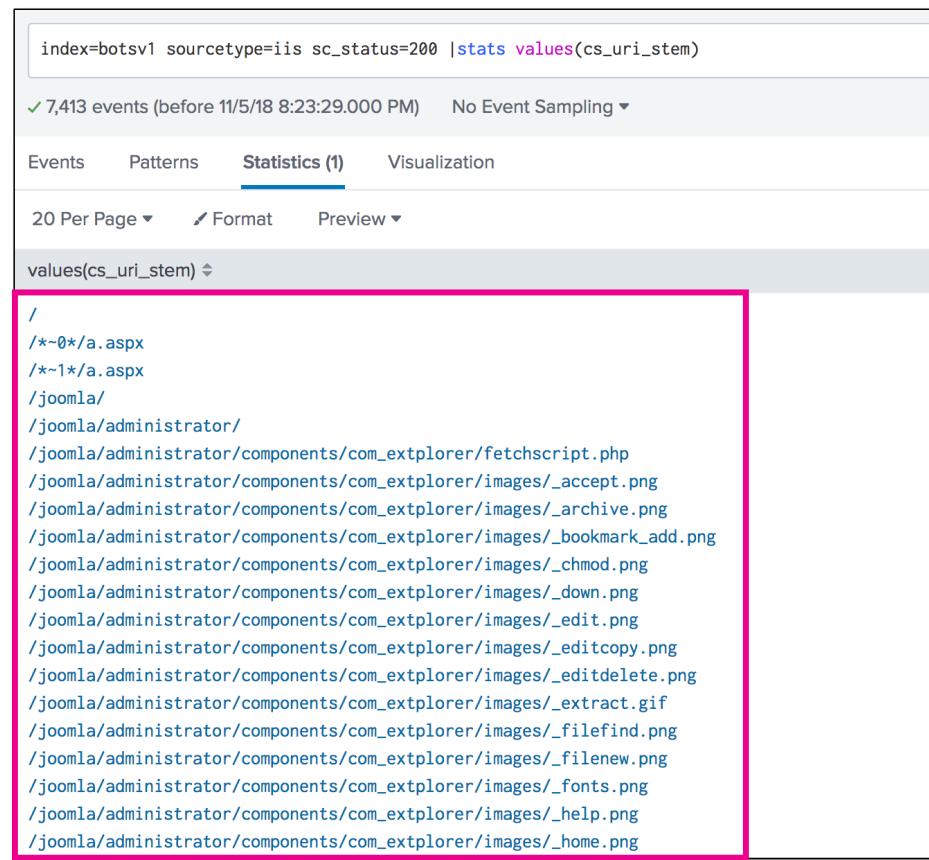
Sort descending by count so the greatest values come to the top

# 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 with the following details:

- Search bar: index=botsv1 sourcetype=iis sc\_status=200 |stats values(cs\_uri\_stem)
- Event count: 7,413 events (before 11/5/18 8:23:29.000 PM) No Event Sampling ▾
- Statistics tab selected (1 result)
- Events tab
- Patterns tab
- Visualization tab
- Formatting: 20 Per Page ▾, Format, Preview ▾
- Column header: values(cs\_uri\_stem) ▾
- List of URLs:
  - /
  - /\*~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

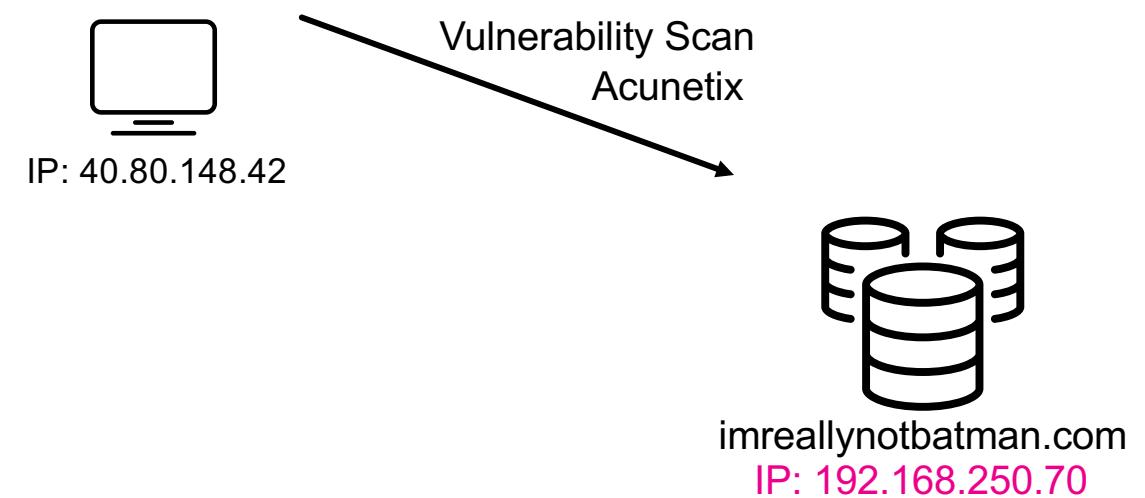
IP Scanning the Web Server: 40.80.148.42

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](http://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 a Splunk search interface with the following details:

- Search Bar:** index=botsv1 sourcetype=stream:http
- Results Summary:** 39,009 events (before 11/5/18 8:33:04.000 PM) No Event Sampling
- Event View:** Events (39,009) Patterns Statistics Visualization
- Time Range:** All time
- Panel Focus:** src
- Reports:** Top values, Top values by time, Rare values
- Selected Fields:** dest 100+, host 1, http\_user\_agent 100+, source 1, sourcetype 1, src 100+, src\_headers 100+, uri 100+
- Interesting Fields:** accept 100+, ack\_packets\_in 100+, ack\_packets\_out 14, action 2, app 1
- Top 10 Values:** (Table)

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%

A large red arrow points downwards from the top of the page towards the bottom right corner of the screenshot area.

# Refine Our Search with the Web Server Address

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

- Search Bar:** index=botsv1 sourcetype=stream:http dest=192.168.250.70
- Results Summary:** 22,671 events (before 11/5/18 8:41:35.000 PM) No Event Sampling
- Event View:** Events (22,671) Patterns Statistics Visualization
- Time Range:** All time
- Panel Options:** Job, Smart Mode
- Formatting:** Format Timeline, Zoom Out, Zoom to Selection, Deselect, 1 day per column
- List View:** List, Format, 20 Per Page, Page 1 of 8
- Selected Fields:** dest, host, http\_user\_agent, source, sourcetype, src, src\_headers, uri
- Interesting Fields:** accept, ack\_packets\_in, ack\_packets\_out
- Modal Window (src field):**
  - Reports:** Top values, Top values by time, Rare values
  - Events with this field:**
  - Values:**

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 a Splunk search interface with the following details:

- Search Bar:** index=botsv1 sourcetype=stream:http dest=192.168.250.70
- Event Count:** 22,671 events (before 11/5/18 8:41:35.000 PM) No Event Sampling
- Time Range:** All time
- Pivot Field:** http\_method
- Reports:** Top values, Top values by time, Rare values
- Selected:** Yes
- Values:** 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%)
- Page Navigation:** 1 day per column, Page 1 of 8

A large pink arrow points downwards from the pivot results area towards the bottom of the interface.

# Adding a HTTP Method to Narrow Our Results

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

- Search Bar:** index=botsv1 sourcetype=stream:http dest="192.168.250.70" http\_method=POST
- Results Summary:** 15,559 events (before 11/5/18 8:46:56.000 PM) No Event Sampling
- Event View:** Events (15,559) - The main view displays a timeline of green bars representing event times. A large pink arrow points down to the detailed event view below.
- Event Details:** The detailed view for the first event (8/10/16) shows the following:
  - Selected Fields:** dest 1, host 1, http\_method 1, http\_user\_agent 3, source 1, sourcetype 1, src 2, src\_headers 100+, uri 72
  - Interesting Fields:** accept 2, ack\_packets\_in 14
  - Event Data:** src: 40.80.148.42, Count: 15,148, %: 97.358%
  - Event Data:** src: 23.22.63.114, Count: 411, %: 2.642%

# Finding Passwords in HTTP Wire Data

```
index=botsv1 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 <a HREF="http://imreallynotbatman.com/joomla/administrator/index.php">here</a></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&e5ec827a3f67ce0fc546d81f7356acc =1
http_comment	HTTP/1.1 303 See other

# Finding Passwords in HTTP Wire Data

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

- Search Query:** index=botsv1 sourcetype=stream:http dest="192.168.250.70" http\_method=POST form\_data=\*username\*passwd\*  
|table form\_data
- Event Count:** 412 events (before 11/5/18 9:13:58.000 PM) No Event Sampling ▾
- Statistics:** Statistics (412)
- Formatting:** 20 Per Page ▾, Format, Preview ▾
- Column Headers:** form\_data
- Log Entries:** (The following log entries are highlighted with a pink box)
  - 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&a09349d0d6bdbf078ad72cf8e9348583=1
  - username=admin&task=login&return=aW5kZXgucGhw&option=com\_login&passwd=sammy&0d3bb0020f70044ffba32f7d0fa7fa88=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
- Text on the right:** > turn data into doing'

# Using stats for the Win!

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

- Search Bar:** index=botsv1 sourcetype=stream: http dest="192.168.250.70" http\_method=POST form\_data=\*username\*passwd\*  
| stats count by src
- Results Summary:** 412 events (before 11/5/18 9:18:42.000 PM) No Event Sampling
- Job Controls:** Job ▾, II, ⌂, ↗, +, ↓, Smart Mode ▾
- Navigation:** Events, Patterns, **Statistics (2)**, Visualization
- Table View:** 20 Per Page ▾, Format, Preview ▾
- Statistics Table:** A table showing the count of events by source IP address.

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 [imreallynotbatman.com](http://imreallynotbatman.com)?

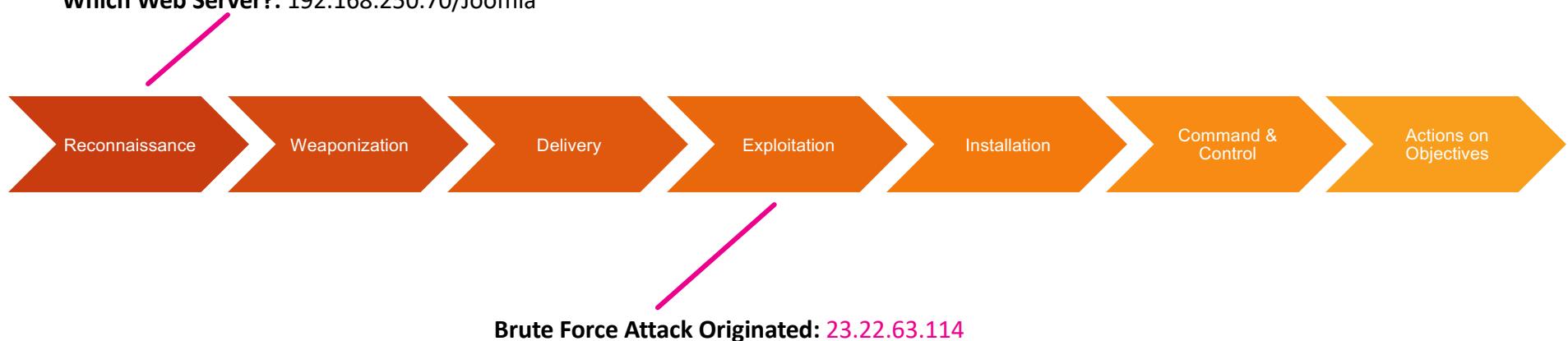
- 23.22.63.114

# Kill Chain

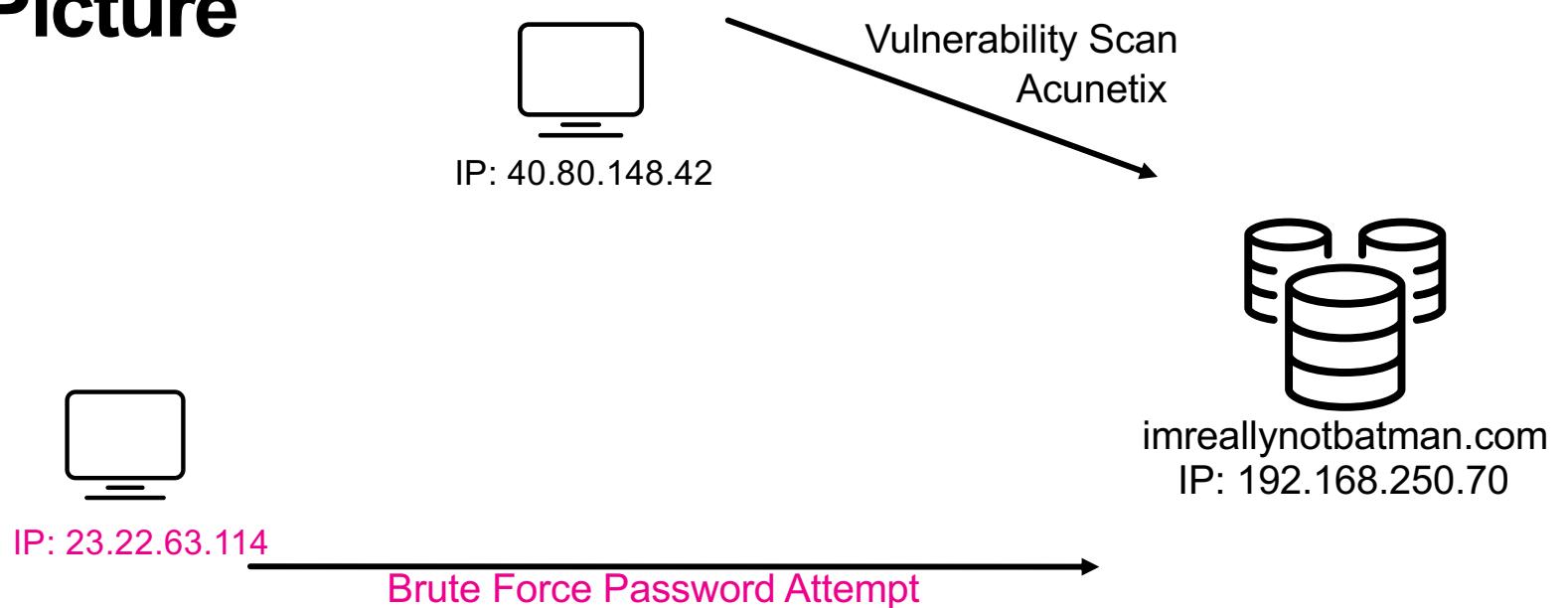
IP Scanning the Web Server: 40.80.148.42

Web Vulnerability Scanner: Acunetix

Which Web Server?: 192.168.250.70/Joomla

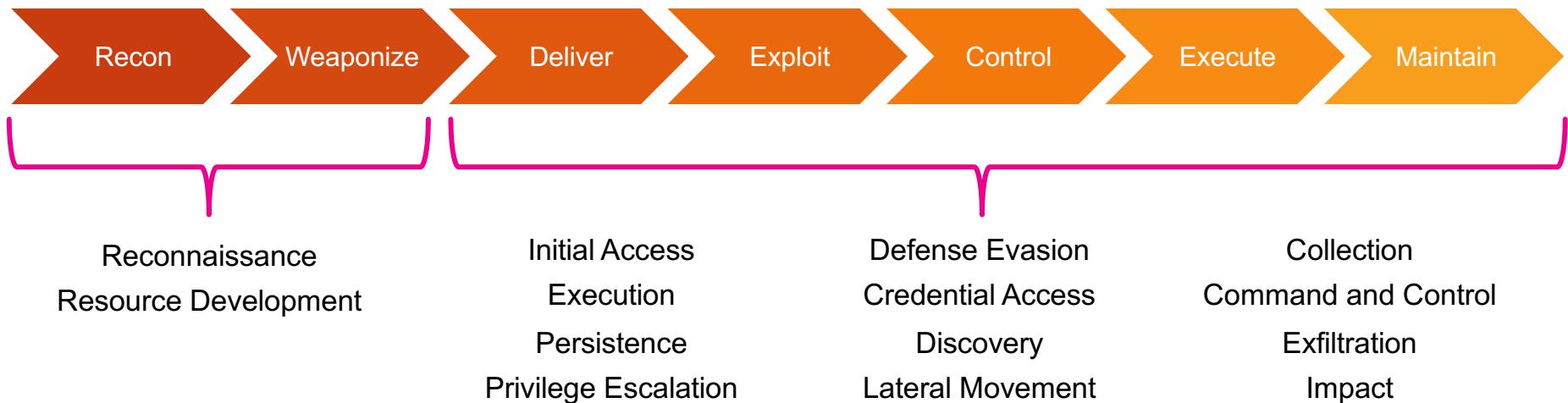


# APT Picture



# 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/>

splunk > turn data into doing®

# 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

✓ 412 events (before 11/5/18 9:54:40.000 PM) No Event Sampling ▾ Job ▾ All time ▾ Smart Mode ▾

Events Patterns Statistics (412) Visualization

20 Per Page ▾ Format Preview ▾ 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&d3bb0020f70044ffba32f7d0fa7fa88=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 ▾

All time ▾ 

Events Patterns Statistics (412) Visualization Job ▾  Smart Mode ▾

20 Per Page ▾  Preview ▾

### Password

\_time ▾ 

_time	form_data
2016-08-10 21:45:21.226	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=12345678&9d873c2becd118318849d13cf18b60ff=1
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

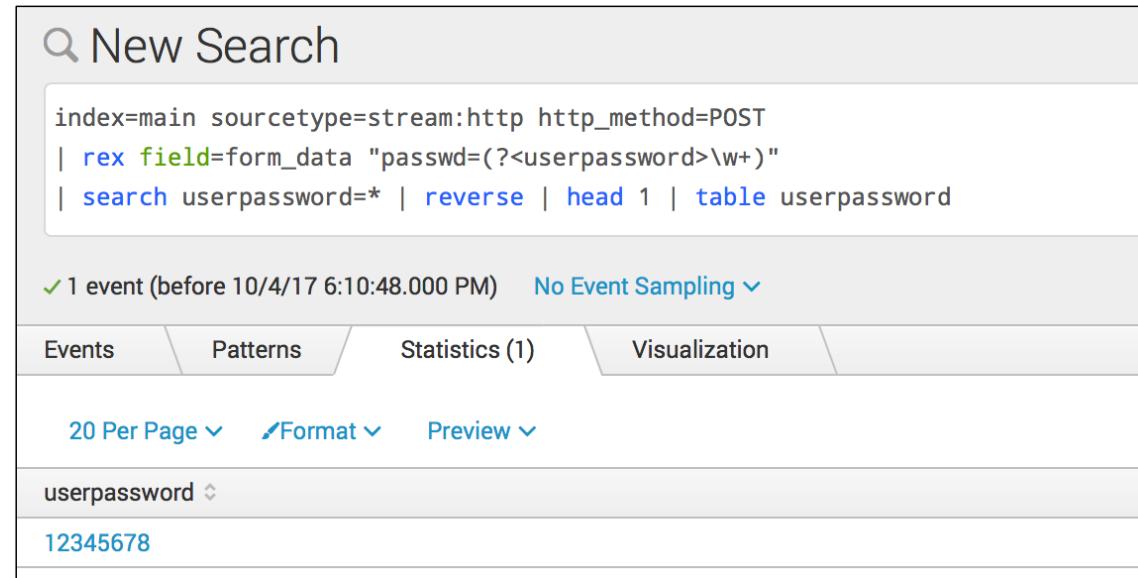
< Prev 1 2 3 4 5 6 7 8 ... Next >

# A More Elegant Way To View the Passwords

Kill Chain Phase: Exploitation

What was the first brute force password used?

- 12345678



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

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

Below the search bar, it says "✓ 1 event (before 10/4/17 6:10:48.000 PM) No Event Sampling".

The interface includes tabs for Events, Patterns, Statistics (1), and Visualization. Under Events, there are filters for "20 Per Page", "Format", and "Preview". The results table shows one row with the value "userpassword" followed by "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+)"
```

**splunk**® turn data into doing®

# What Else Do We Need?

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

```
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
```

The search results show 412 events found before 11/5/18 11:57:28.000 PM. The Statistics tab is selected, displaying the following table:

userpassword	count
batman	2
000000	1
1111	1
1111111	1
11111111	1

On the left, a list of bullet points provides context for the search:

- Focus our search on destination for greater precision
- Rex command will extract the passwords
- Add a stats command to count the number of times each password was used and sort by the count
- Second use of a password would likely indicate that it was the one the adversary wanted

# 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

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

```
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
```

The search results table displays the following data:

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 Splunk search interface with the following details:

- Search 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
```
- Results:** 1 event (before 11/6/18 12:09:05.000 AM)
- Event Details:**

_time	uri	userpassword
2016-08-10 21:48:05.858	/joomla/administrator/index.php	batman
- User Interface Elements:** Statistics (1) tab selected, Job, Smart Mode, and other search controls.

# Kill Chain

IP Scanning the Web Server: 40.80.148.42

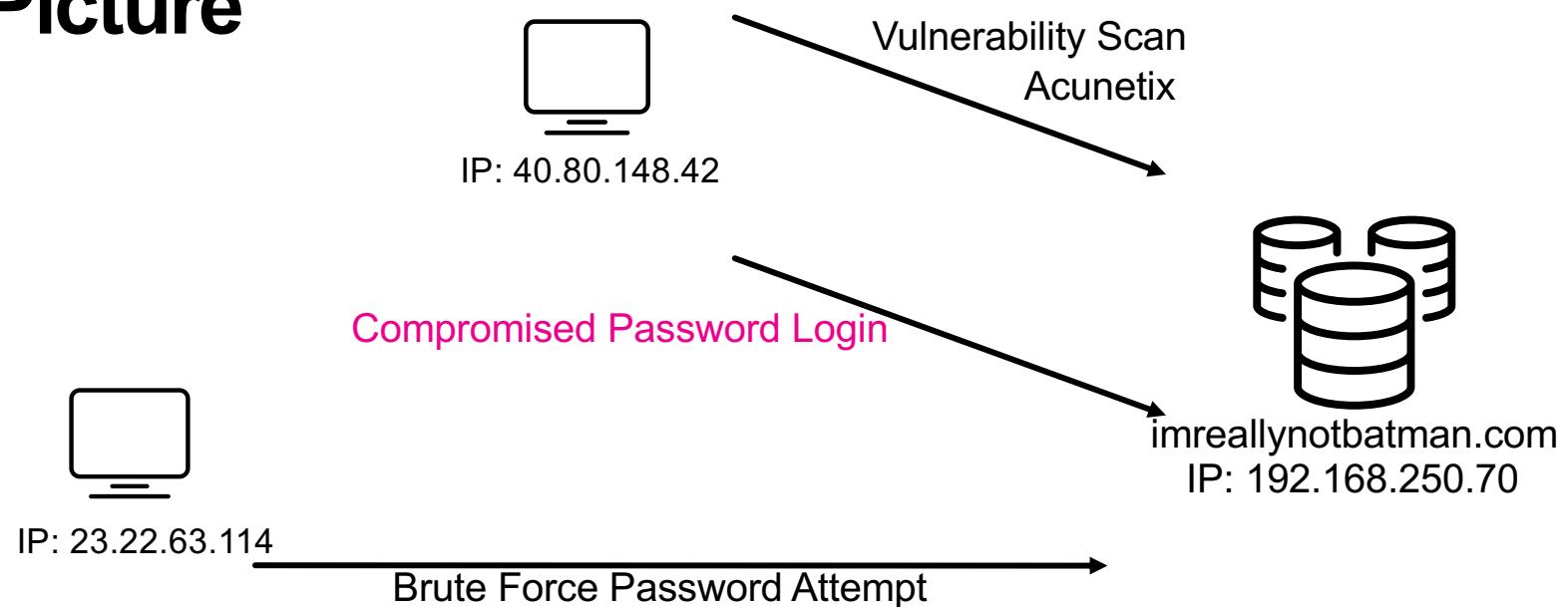
Web Vulnerability Scanner: Acunetix

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 command in the top-left is:

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

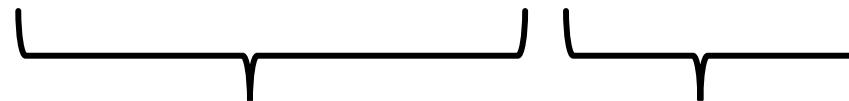
The search results table has three columns: \_time, userpassword, and src. It displays two rows of data:

_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

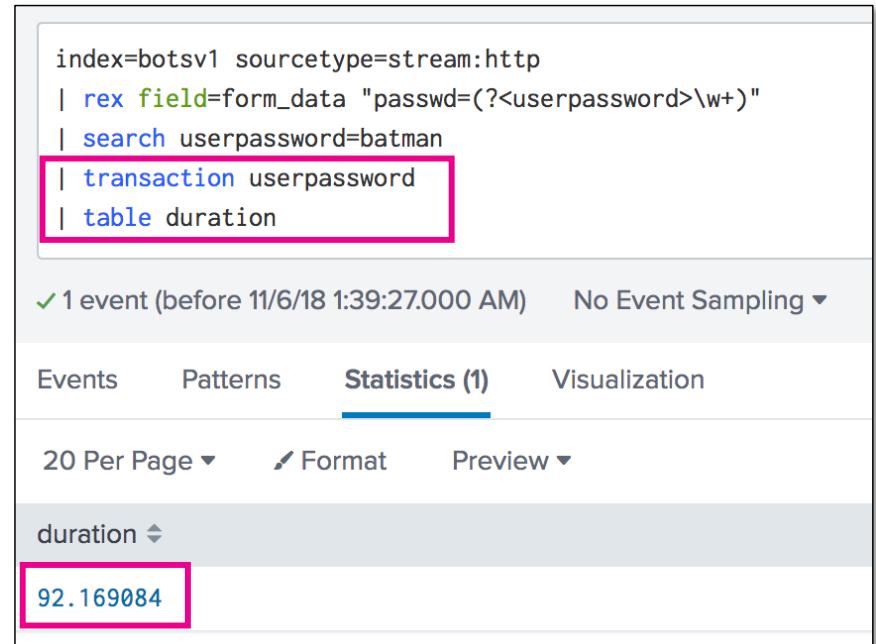
**splunk**> turn data into doing®

# 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. The search command is:

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

The search results show one event found before November 6, 2018, at 1:39:27.000 AM. The Statistics tab is selected, showing one event. The duration is listed as 92.169084. The interface includes buttons for Events, Patterns, Statistics (1), Visualization, Format, and 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

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

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

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

**Event View:** Events (18) Patterns Statistics Visualization

**Time Range:** All time ▾

**Format Timeline:** Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect 1 day per column

**Event List:** List ▾ Format 20 Per Page ▾

**Selected Fields:** part\_filename[]

**Reports:** Selected Yes No

**Events with this field:**

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

**Interesting Fields:** dest, host, http\_method, http\_user\_agent, part\_filename, source, sourcetype, src, src\_headers, uri

# Search for EXEs in Suricata

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

- Search Bar:** index=botsv1 sourcetype=suricata dest\_ip=192.168.250.70 .exe
- Results Summary:** 43 events (before 11/6/18 1:54:26.000 AM) No Event Sampling
- Event View:** Events (43) - The main pane shows a timeline with a green bar indicating event count over time.
- Selected Fields:** dest, fileinfo.filename, host, http\_method, http\_user\_agent, source, sourcetype, src
- Modal Window (fileinfo.filename):** A modal window is open, showing the following data:
  - Reports:** Top values, Top values by time, Rare values
  - Events with this field:** /vti\_bin/shtml.exe, 3791.exe
  - Values Table:**

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

# 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

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

4 events (before 11/6/18 5:50:19.000 PM) No Event Sampling ▾

Events (4) Patterns Statistics Visualization

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

**dest**

1 Value, 100% of events

**Reports**

Top values Top values by time Events with this field

**Values**

imreallynotbatman.com

**fileinfo.filename**

2 Values, 75% of events

**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%

The screenshot shows a Splunk search interface with a search bar containing the query: index=botsv1 sourcetype=suricata (dest="imreallynotbatman.com" OR dest="192.168.250.70") http.http\_method=POST .exe. Below the search bar, it says "4 events (before 11/6/18 5:50:19.000 PM)" and "No Event Sampling". The main pane displays two facets: "dest" and "fileinfo.filename". The "dest" facet shows one value, "imreallynotbatman.com", which is highlighted with a pink box. The "fileinfo.filename" facet shows two values: "/vti\_bin/shtml.exe" and "3791.exe", with counts of 2 and 1 respectively, and percentages of 66.667% and 33.333%. A "Selected" button with "Yes" and "No" options is shown next to the fileinfo.filename facet. On the left, a sidebar lists selected fields: dest 1, fileinfo.filename 2, host 1, http\_method 1, http\_user\_agent 2, source 1, sourcetype 1, and src 2. A tooltip for "imreallynotbatman.com" shows the full URL: http: { L+J }.

# Capturing the Source of the Executable

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

- Search Bar:** index=botsv1 sourcetype=suricata (dest=imreallynotbatman.com OR dest="192.168.250.70") http.http\_method=POST .exe "fileinfo.filename"="3791.exe"
- Event Count:** 1 event (before 11/6/18 5:55:35.000 PM) No Event Sampling
- Time Range:** All time
- Events View:** Shows a single event with a green bar indicating its duration. The event details are as follows:
  - Time: 8/10/16
  - Event: { [-] SRC}
  - Description: 1 Value, 100% of events
  - Selected: Yes
  - Reports: Top values, Top values by time, Rare values
  - Events with this field: 40.80.148.42
  - Values: 40.80.148.42, Count: 1, %: 100%
- Selected Fields:** dest 1, fileinfo.filename 1, host 1, http\_method 1, http\_user\_agent 1, source 1, sourcetype 1, src 1
- Interesting Fields:** app 1, app\_proto 1

# 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

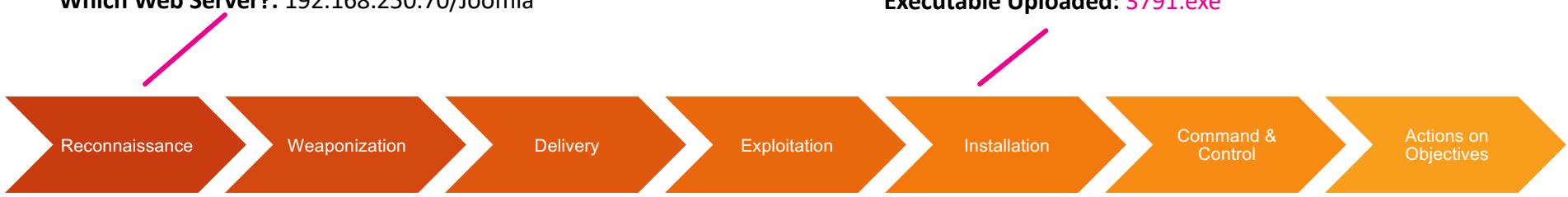
# Kill Chain

IP Scanning the Web Server: 40.80.148.42

Web Vulnerability Scanner: Acunetix

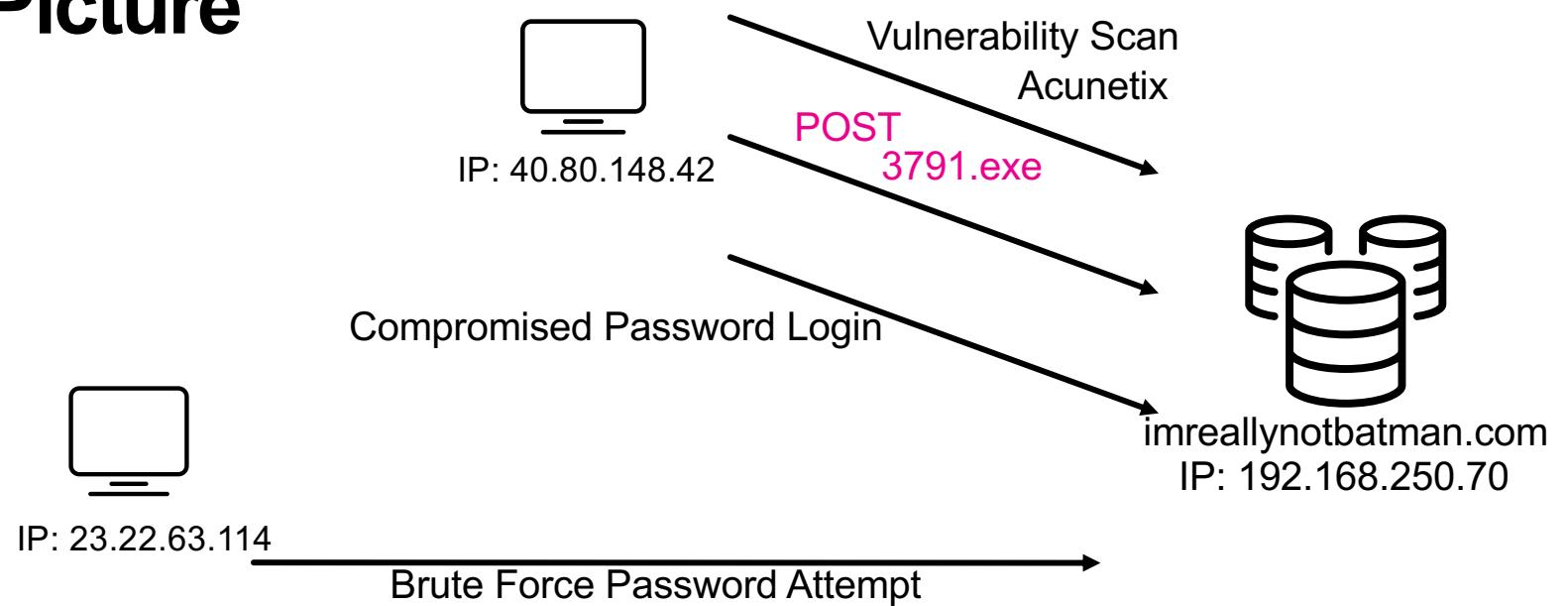
Which Web Server?: 192.168.250.70/Joomla

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?

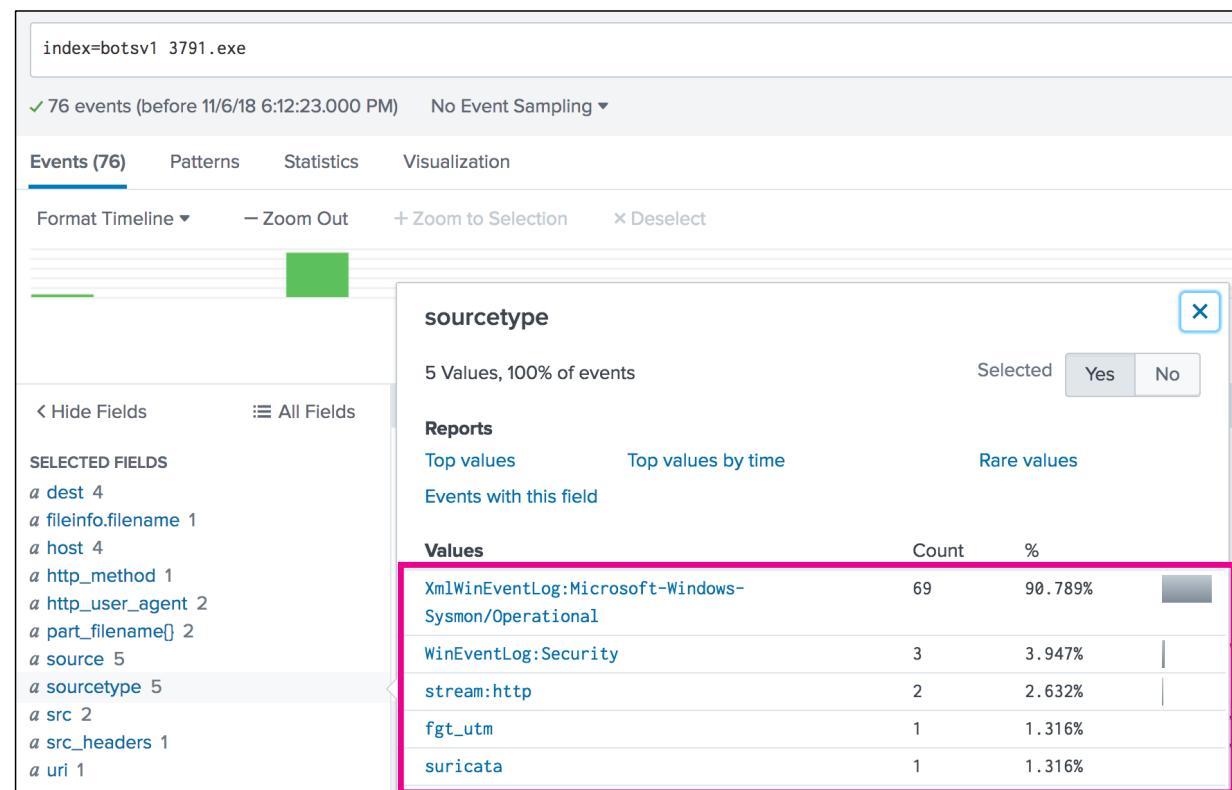
### Hints

- 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>



# 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>*
```

# What Can I Find With Sysmon?

## Part 1 of 2

index=botsv1\_3791.exe sourcetype=XmlWinEventLog:Microsoft-Windows-Sysmon/Operational

✓ 69 events (before 11/6/18 6:15:35.000 PM) No Event Sampling ▾

**Events (69)** Patterns Statistics Visualization

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

**EventDescription**

4 Values, 100% of events

**Reports**

Top values Top values by time Events with this field

Values	Count	%
Image Load	62	89.85%
Process Create	5	7.246%
Network Connect	1	1.449%
Process Terminate	1	1.449%

**Hashes**

55 Values, 97.101% of events

Selected Yes No

**Reports**

Top values Top values by time Rare values

Events with this field

**Top 10 Values**

	Count	%
SHA1=65DF73D77324D008C83C3E57B445DF0FD43A3A51,MD5=AAE3F5A29935E6ABC2C2754D12A9AF0,SHA256=E78C938D8453739CA2A370B9C275971EC46CAF6E479DE2B2D04E97CC47FA45D,IMPHASH=481F47BBB2C9C21E108D65F52B04C448	3	4.478%
SHA1=F5CFD4070EA7D2B40A29F21F9E29AF23341C59EC,MD5=59A1D4FACD7B333F76C4142CD42D3ABA,SHA256=E1A080E61FB1BAF0DA629D34BAEE6F0F9D0E0337BF6CED9F4B3AB9B1C23D91BA,IMPHASH=5B13496CE269DF7709AAB6B1BBF99CD3	3	4.478%
SHA1=1A7D45BC0AD6A7255159802137D20CB93F1B712C,MD5=522BF7088E69948A20DD5C89D359B2C4,SHA256=20949159376225C7D88B4CBBA1F0C06113E2DED7369B59329AF00D3295BC627B,IMPHASH=F0E5EF88099C621A94DB5D9BB363E847	2	2.985%
SHA1=52451D9630A6F45A3C092091B853879D57B92664,MD5=53D2FF6892E3D69D9CF5E1F1785872B0,SHA256=1459B0F53B9A6016E45B4B6CD2A8E8088B6BC484CDB942600864D5B38667BE2,IMPHASH=A77B19E8024D7D62FA77C62F95712442	2	2.985%

time ▾ **Smart Mode** ▾

1 minute per column

4 Next >

event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{577...}<Keywords>0<relation/><Task>1<Opcde>0</Opcde><Keywords>0<TimeCreated SystemTime='2016-08-10T22:08:13.902098100Z'/'><EventRecordID>443590</EventRecordID><CorrelationID>3791.exe</CorrelationID>

# What Can I Find With Sysmon?

## Part 2 of 2

**Select Fields**

Select All Within Filter		Deselect All	All fields ▾	Command <input type="text"/>	X	+ Extract New Fields
i	✓	Field		# of Values	Event Coverage	Type
>	<input checked="" type="checkbox"/>	CommandLine		4	7.25%	String
>	<input checked="" type="checkbox"/>	ParentCommandLine		3	7.25%	String

**CommandLine**

4 Values, 7.246% of events

Selected

**Reports**

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

[Events with this field](#)

**Values**

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

**ParentCommandLine**

3 Values, 7.246% of events

Selected

**Reports**

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

[Events with this field](#)

**Values**

3791.exe	Count	%
cmd.exe /c "3791.exe & 1"	2	40%
"C:\Program Files (x86)\PHP\v5.5\php-cgi.exe"	1	20%

# Drilling Down on MD5 & CommandLine

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

5 events (before 11/7/18 2:47:22.000 AM) No Event Sampling ▾

Events (5) Patterns Statistics Visualization

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

List ▾ Format 20 Per Page ▾

MD5

3 Values, 100% of events Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

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 &gt;&gt;1"	1	20%

CommandLine

4 Values, 100% of events Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

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 &gt;&gt;1"	1	20%

# 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	<pre>&lt;Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'&gt;&lt;System&gt;&lt;Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFBD9}' /&gt;&lt;EventID&gt;1&lt;/EventID&gt;&lt;Version&gt;5&lt;/Version&gt;&lt;Level&gt;4&lt;/Level&gt;&lt;Task&gt;1&lt;/Task&gt;&lt;Opcode&gt;0&lt;/Opcode&gt;&lt;Keywords&gt;0x8000000000000000&lt;/Keywords&gt;&lt;TimeCreated SystemTime='2016-08-10T21:56:18.142461700Z' /&gt;&lt;EventRecordID&gt;428908&lt;/EventRecordID&gt;&lt;Correlation/&gt;&lt;Execution ProcessID='1296' ThreadID='1416' /&gt;&lt;Channel&gt;Microsoft-Windows-Sysmon/Operational&lt;/Channel&gt;&lt;Computer&gt;we1149srv.waynecorpinc.local&lt;/Computer&gt;&lt;Security UserID='S-1-5-18' /&gt;&lt;System&gt;&lt;EventData&gt;&lt;Data Name='UtcTime'&gt;2016-08-10 21:56:18.142&lt;/Data&gt;&lt;Data Name='ProcessGuid'&gt;{E500B0EA-A302-57AB-0000-00108D65C301}&lt;/Data&gt;&lt;Data Name='ProcessId'&gt;3880&lt;/Data&gt;&lt;Data Name='Image'&gt;C:\inetpub\wwwroot\joomla\3791.exe&lt;/Data&gt;&lt;Data Name='CommandLine'&gt;3791.exe &lt;/Data&gt;&lt;Data Name='CurrentDirectory'&gt;C:\inetpub\wwwroot\joomla\&lt;/Data&gt;&lt;Data Name='User'&gt;NT AUTHORITY\IUSR&lt;/Data&gt;&lt;Data Name='LogonGuid'&gt;{E500B0EA-219E-57AA-0000-0020E303000}&lt;/Data&gt;&lt;Data Name='LogonId'&gt;0x3e3&lt;/Data&gt;&lt;Data Name='TerminalSessionId'&gt;0&lt;/Data&gt;&lt;Data Name='IntegrityLevel'&gt;High&lt;/Data&gt;&lt;Data Name='Hashes'&gt;SHA1=65DF73D77324D008C83C3E57B445DF0FD43A3A51,MD5=AAE3F5A29935E6ABCC2C2754D12A9AF0,SHA256=EC78C938D8453739CA2A37089C275971EC46CAF6E479DE2B2D04E97CC47FA45D,IMPHASH=481F47BBB2C9C21E108D65F52B04C448&lt;/Data&gt;&lt;Data Name='ParentProcessGuid'&gt;{E500B0EA-A302-57AB-0000-00102E63C301}&lt;/Data&gt;&lt;Data Name='ParentProcessId'&gt;2896&lt;/Data&gt;&lt;Data Name='ParentImage'&gt;C:\Windows\SysWOW64\cmd.exe&lt;/Data&gt;&lt;Data Name='ParentCommandLine'&gt;cmd.exe /c "3791.exe 2&amp;gt;&amp;1"&lt;/Data&gt;&lt;/EventData&gt;&lt;/Event&gt;</pre>																																																								
<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">Event Actions ▾</div> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Type</th> <th>Field</th> <th>Value</th> <th>Actions</th> </tr> </thead> <tbody> <tr> <td>Selected</td> <td>CommandLine</td> <td>3791.exe</td> <td>▼</td> </tr> <tr> <td></td> <td>EventDescription</td> <td>Process Create</td> <td>▼</td> </tr> <tr> <td></td> <td>Hashes</td> <td>SHA1=65DF73D77324D008C83C3E57B445DF0FD43A3A51,MD5=AAE3F5A29935E6ABCC2C2754D12A9AF0,SHA256=EC78C938D8453739CA2A37089C275971EC46CAF6E479DE2B2D04E97CC47FA45D,IMPHASH=481F47BBB2C9C21E108D65F52B04C448</td> <td>▼</td> </tr> <tr> <td></td> <td>MD5</td> <td>AAE3F5A29935E6ABCC2C2754D12A9AF0</td> <td>▼</td> </tr> <tr> <td></td> <td>ParentCommandLine</td> <td>cmd.exe /c "3791.exe 2&amp;gt;&amp;1"</td> <td>▼</td> </tr> <tr> <td></td> <td>dest</td> <td>we1149srv.waynecorpinc.local</td> <td>▼</td> </tr> <tr> <td></td> <td>host</td> <td>we1149srv</td> <td>▼</td> </tr> <tr> <td></td> <td>source</td> <td>WinEventLog:Microsoft-Windows-Sysmon/Operational</td> <td>▼</td> </tr> <tr> <td></td> <td>sourcetype</td> <td>XmlWinEventLog:Microsoft-Windows-Sysmon/Operational</td> <td>▼</td> </tr> <tr> <td>Event</td> <td>Computer</td> <td>we1149srv.waynecorpinc.local</td> <td>▼</td> </tr> <tr> <td></td> <td>CurrentDirectory</td> <td>C:\inetpub\wwwroot\joomla\</td> <td>▼</td> </tr> <tr> <td></td> <td>EventChannel</td> <td>Microsoft-Windows-Sysmon/Operational</td> <td>▼</td> </tr> <tr> <td></td> <td>EventCode</td> <td>1</td> <td>▼</td> </tr> </tbody> </table>		Type	Field	Value	Actions	Selected	CommandLine	3791.exe	▼		EventDescription	Process Create	▼		Hashes	SHA1=65DF73D77324D008C83C3E57B445DF0FD43A3A51,MD5=AAE3F5A29935E6ABCC2C2754D12A9AF0,SHA256=EC78C938D8453739CA2A37089C275971EC46CAF6E479DE2B2D04E97CC47FA45D,IMPHASH=481F47BBB2C9C21E108D65F52B04C448	▼		MD5	AAE3F5A29935E6ABCC2C2754D12A9AF0	▼		ParentCommandLine	cmd.exe /c "3791.exe 2&gt;&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	▼
Type	Field	Value	Actions																																																						
Selected	CommandLine	3791.exe	▼																																																						
	EventDescription	Process Create	▼																																																						
	Hashes	SHA1=65DF73D77324D008C83C3E57B445DF0FD43A3A51,MD5=AAE3F5A29935E6ABCC2C2754D12A9AF0,SHA256=EC78C938D8453739CA2A37089C275971EC46CAF6E479DE2B2D04E97CC47FA45D,IMPHASH=481F47BBB2C9C21E108D65F52B04C448	▼																																																						
	MD5	AAE3F5A29935E6ABCC2C2754D12A9AF0	▼																																																						
	ParentCommandLine	cmd.exe /c "3791.exe 2&gt;&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

The screenshot shows a Splunk search interface. At the top, there is a search bar containing the following command:

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

Below the search bar, a message indicates "1 event (before 11/7/18 3:17:50.000 AM)" and "No Event Sampling".

The interface includes several navigation tabs: "Events", "Patterns", "Statistics (1)", and "Visualization". The "Statistics (1)" tab is currently selected, indicated by a blue underline.

Below the tabs, there are dropdown menus for "20 Per Page", "Format", and "Preview".

The main results area displays the event details under the "values(MD5)" section, showing the value "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

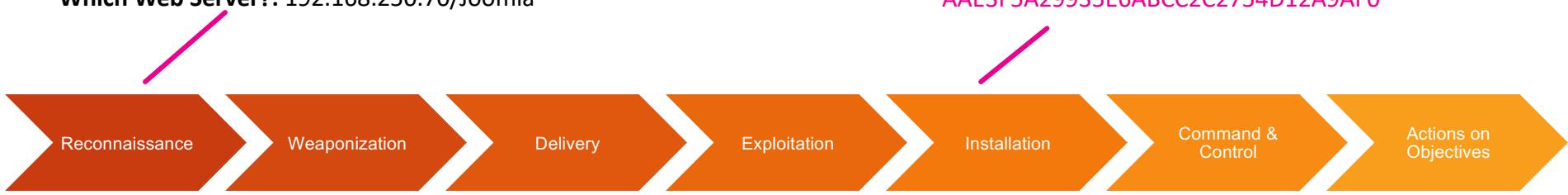
Web Vulnerability Scanner: Acunetix

Which Web Server?: 192.168.250.70/Joomla

Executable Uploaded: 3791.exe

Hash of the Uploaded File:

AAE3F5A29935E6ABCC2C2754D12A9AF0



Reconnaissance

Weaponization

Delivery

Exploitation

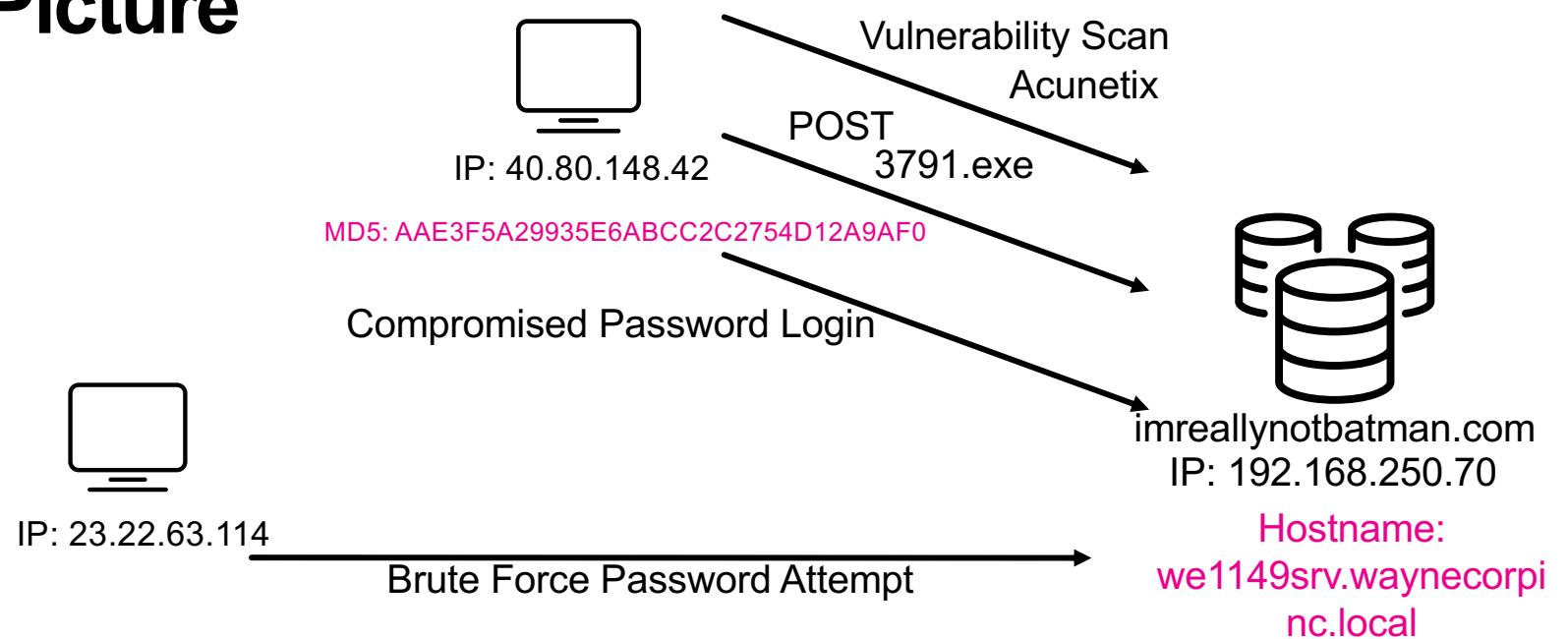
Installation

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 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



IP: Do We Know This?

imreallynotbatman.com  
IP: 192.168.250.70

# Looking at Directional Flow of Data - Part 1

Nothing Coming From Outside In

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

- Search Bar:** index=botsv dest=192.168.250.70 sourcetype=suricata
- Results Summary:** 421 events (before 11/7/18 1:31:56.000 PM) No Event Sampling
- Event List:** Events (421) - The main pane displays a timeline from 8/24/16 to 8/24/16, with a green bar indicating event selection. The list view shows 20 events per page, with page 1 selected.
- Selected Fields:** dest, fileinfo.filename, host, http\_method, http\_user\_agent, source, sourcetype, src.
- Interesting Fields:** app, app\_proto, bytes, date\_hour, date\_mday.
- Event Detail View:** A detailed view for the first event on 8/24/16 at 4:47:14.001 PM, showing app\_proto: http and src: 192.168.2.50.
- Value Distribution:** A table showing the distribution of src values:

Values	Count	%
192.168.2.50	211	50.119%
192.168.250.70	210	49.881%

A large pink arrow points downwards from the bottom right towards the value distribution table.

# Looking at Directional Flow of Data - Part 2

## Looking from Inside Out

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

- Search Bar:** index=botsv src=192.168.250.70 sourcetype=suricata
- Results Summary:** 12,601 events (before 11/7/18 1:34:23.000 PM) No Event Sampling
- Time Range:** All time
- Event Type:** Events (12,601)
- Visualizations:** Patterns, Statistics, Visualization
- Selected Field:** dest\_ip
- Reports:** Top values, Top values by time, Rare values
- Events with this field:** Values, Count, %
- Selected Fields:** dest, dest\_ip, fileinfo.filename, host, http\_method, http\_user\_agent, source, sourcetype, src
- Interesting Fields:** app, app\_proto, bytes
- Bottom Status Bar:** dest\_ip = 192.168.250.40 | host = suricata-ids.waynecorpinc.local | source = /var/log/suricata/eve.json | sourcetype = suricata | src = 192.168.250.70

A large red arrow points downwards from the top right towards the bottom status bar.

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%

# Pivot Into Destination IP Addresses to View URLs

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

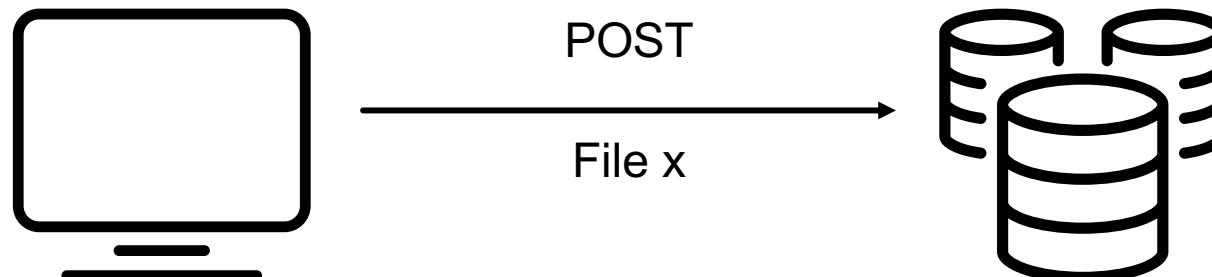
- Search Bar:** index=botsv1 src=192.168.250.70 sourcetype=suricata dest\_ip=23.22.63.114
- Event Count:** 1,294 events (before 11/7/18 1:37:55.000 PM) No Event Sampling
- Time Range:** All time
- Events (1,294) Tab:** Selected
- Format Timeline:** 1 minute per column
- Selected Fields:** http.url (highlighted with a pink box)
- Reports:** Top values, Top values by time, Rare values
- Events with this field:** /joomla/administrator/index.php, /joomla/agent.php, /poisonivy-is-coming-for-you-batman.jpeg
- Count and %:** 1,235 (95.736%), 52 (4.031%), 3 (0.232%)

# HTTP Get v Post Traffic Flow

HTTP GET will generally retrieve data



HTTP POST submits data to be processed

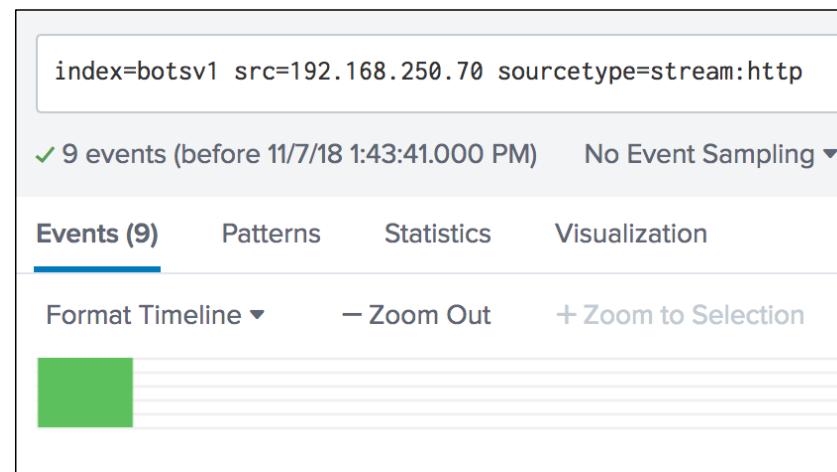


imreallynotbatman.com

splunk > turn data into doing®

# 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?

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

✓ 9 events (before 11/7/18 1:45:40.000 PM) No Event Sampling Job ▾ Smart Mode

Events (9) Patterns Statistics Visualization

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

List Format 20 Per Page

< Hide Fields

**SELECTED FIELDS**

a dest 2  
a dest\_ip 2  
a host 1  
a http\_method 1  
a source 1  
a sourcetype 1  
a src 1  
a src\_headers 5  
a uri 5

**INTERESTING FIELDS**

a accept 1  
# ack\_packets\_in 4  
# ack\_packets\_out 3  
a action 1

**uri**

5 Values, 88.889% of events Selected Yes No

**Reports**

Top values Top values by time Rare values

Events with this field

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%

urctype = stream:http | src = 192.168.250.70

splunk® turn data into doing™

# 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 ▾

◀ Hide Fields ▶ All Fields

**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+

Time Event

src

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%

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%

evname=gotham-fortigate devid=FGT60D4614044725 logid=0317013312 type=utm subtype=webfilter eventtype=f  
user="" srcip=23.22.63.114 srcport=47516 dstip=192.168.250.70 dstport=80 dstintf="internal3" proto=6  
l" action=passthrough reqtype=direct url="/joomla/agent.php" sentbyte=363 rcvbyte=0 direction=N/A msg  
cat=0 catdesc="Unrated"  
t | http\_user\_agent = unknown | source = udp:514 | sourcetype = fgt\_utm | src = 23.22.63.114  
evname=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  
l" action=passthrough reqtype=direct url="/joomla/agent.php" sentbyte=418 rcvbyte=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 Categorization to Filter

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

- Search Bar:** index=botsv1 sourcetype=fgt\_utm "192.168.250.70" NOT dest="192.168.250.70"
- Event Count:** ✓ 9 events (before 11/7/18 1:52:29.000 PM) No Event Sampling ▾
- Time Range:** All time ▾
- Visual Mode:** Smart Mode ▾
- Event Types:** Events (9), Patterns, Statistics, Visualization
- Format Timeline:** Format Timeline ▾, -Zoom Out, +Zoom to Selection, × Deselect, 1 minute per column
- Event List:** A list of 9 events is shown, with the first event highlighted in green. The event details include:
  - category: Malicious Websites
  - source: 192.168.250.70
  - http\_method: direct
  - http\_user\_agent: unknown
  - source: udp:514
  - sourcetype: fgt\_utm
- Category Distribution:** A modal window titled "category" shows the distribution of categories across the 9 events.

Values	Count	%
Information Technology	6	66.667%
Malicious Websites	3	33.333%
- Selected Fields:** category, dest, host, http\_method, http\_user\_agent, source, sourcetype, src.
- Interesting Fields:** action, bytes, bytes\_in, bytes\_out.

# Firewall Gives Us Confirmation

index=botsv1 sourcetype=fgt\_utm "192.168.250.70" NOT dest="192.168.250.70" category="Malicious Websites"

All time

✓ 3 events (before 11/7/18 1:54:46.000 PM) No Event Sampling ▾ Job ▾ Smart Mode ▾

Events (3) Patterns Statistics Visualization

Format Timeline ▾ 1 minute per column

List 20 Per Page ▾

Hide Fields All Fields

**SELECTED FIELDS**

- category 1
- dest 1
- file\_path 1
- host 1
- http\_method 1
- http\_user\_agent 1
- source 1
- sourcetype 1
- src 1

**INTERESTING FIELDS**

- action 1
- bytes 1
- bytes\_in 1

**file\_path**

1 Value, 100% of events

Selected  Yes  No

**Reports**

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

**Events with this field**

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

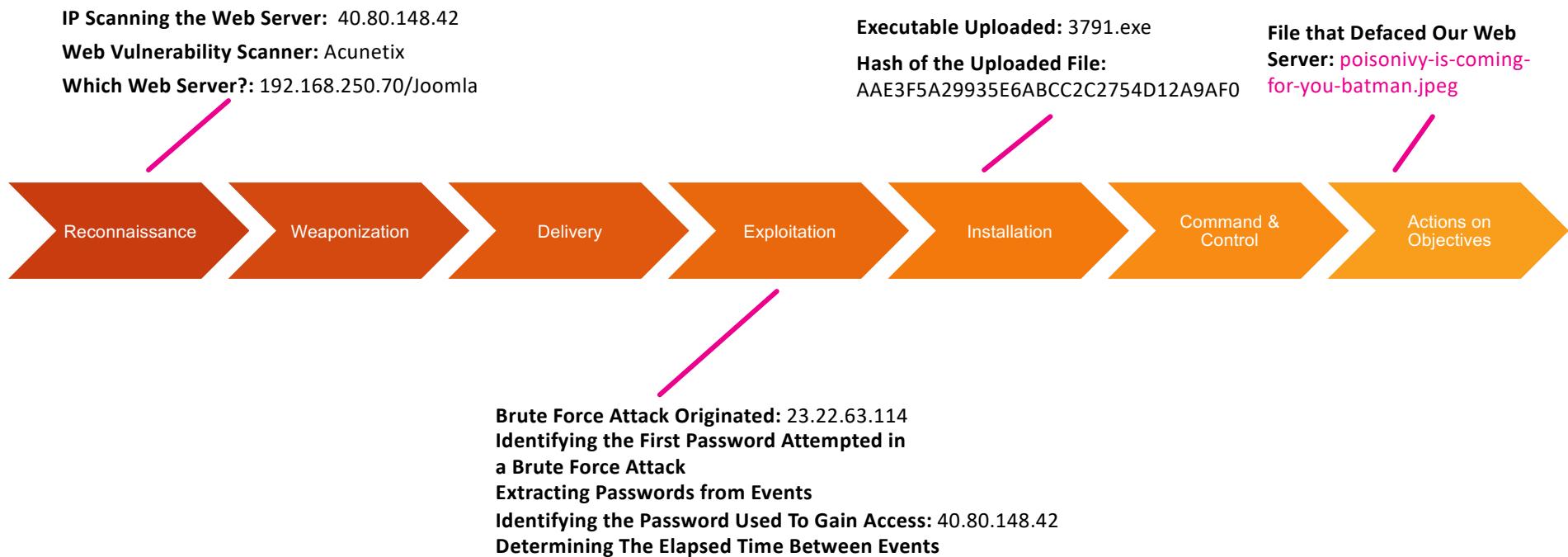
# Identifying the File that Defaced Our Web Server

## Kill Chain Phase: Actions on Objective

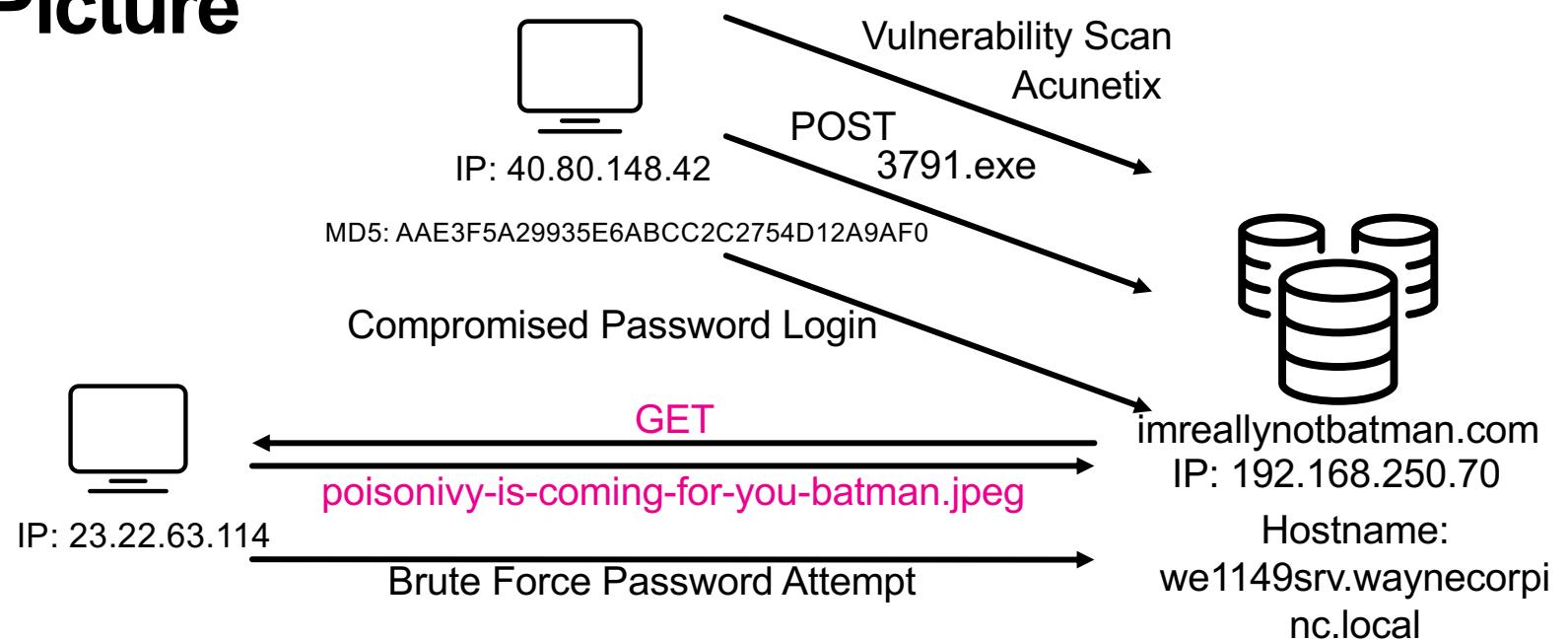
What is the name of the file that defaced the imreallynotbatman.com website?

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

# Kill Chain



# APT Picture



# Identifying the FQDN of the System that Defaced...

Kill Chain Phase: Command & Control

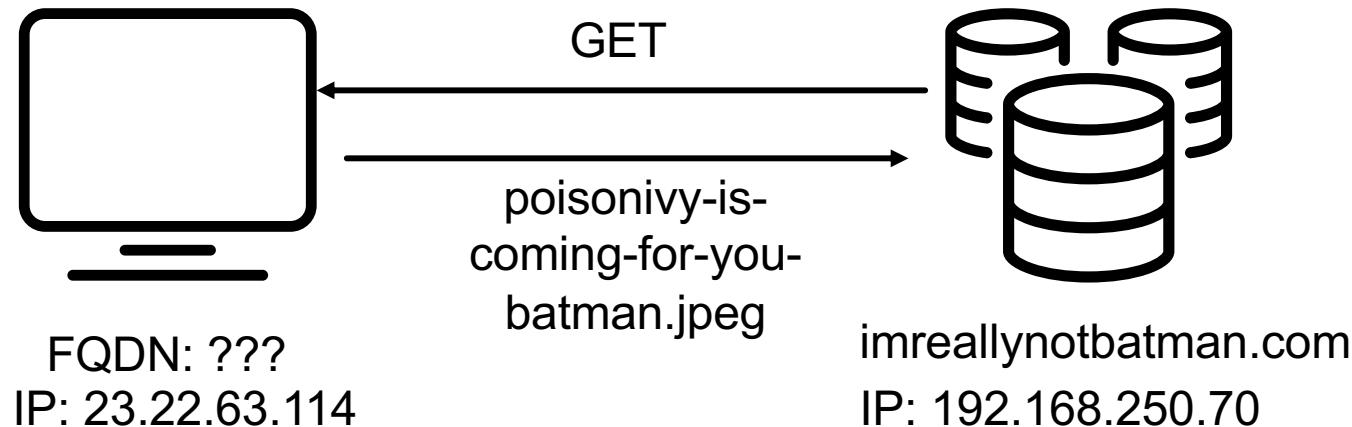
This attack used dynamic DNS to resolve to the malicious IP. What fully qualified domain name (FQDN) is associated with this attack?

## Hint

- Information just recently uncovered will help answer this

# HTTP Get Traffic Flow

HTTP GET will generally retrieves data

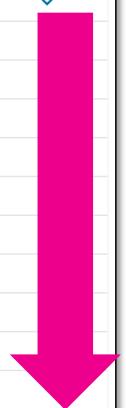


# Using Fortigate Firewall Events We Just Found

8/10/16 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=ft  
10:19:10.000 PM gd\_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 reqtype=direct url="/poisonivy-is-coming-for-you-batman.j  
peg" 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=h  
igh

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?

# 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"

All time 

✓ 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 ▾

Time	Event
8/10/16 10:19:11.351 PM	<pre>{   "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": 106,   "dest": "23.22.63.114",   "dest_ip": "23.22.63.114",   "host": "bot",   "http_method": "GET",   "source": "192.168.250.70",   "sourcetype": "stream:http",   "src": "192.168.250.70",   "uri": "/",   "url": "http://www.iec.ch/sonivy-is-coming-for-you-batman.jpeg" }</pre>

**url**

1 Value, 66.667% of events Selected Yes No

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	1	50%

sourcetype = stream:http | 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

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

- Search bar: index=botsv1 answer=23.22.63.114 sourcetype=stream:dns | stats values("name{}")
- Event count: ✓ 1 event (before 11/7/18 2:08:23.000 PM) No Event Sampling ▾
- Statistics tab selected (1 result)
- Formatting: 20 Per Page ▾, Format, Preview ▾
- Result table:

values(name[])
prankglassinebracket.jumpingcrab.com

# Identifying the FQDN of the System that Defaced...

Kill Chain Phase: Command & Control

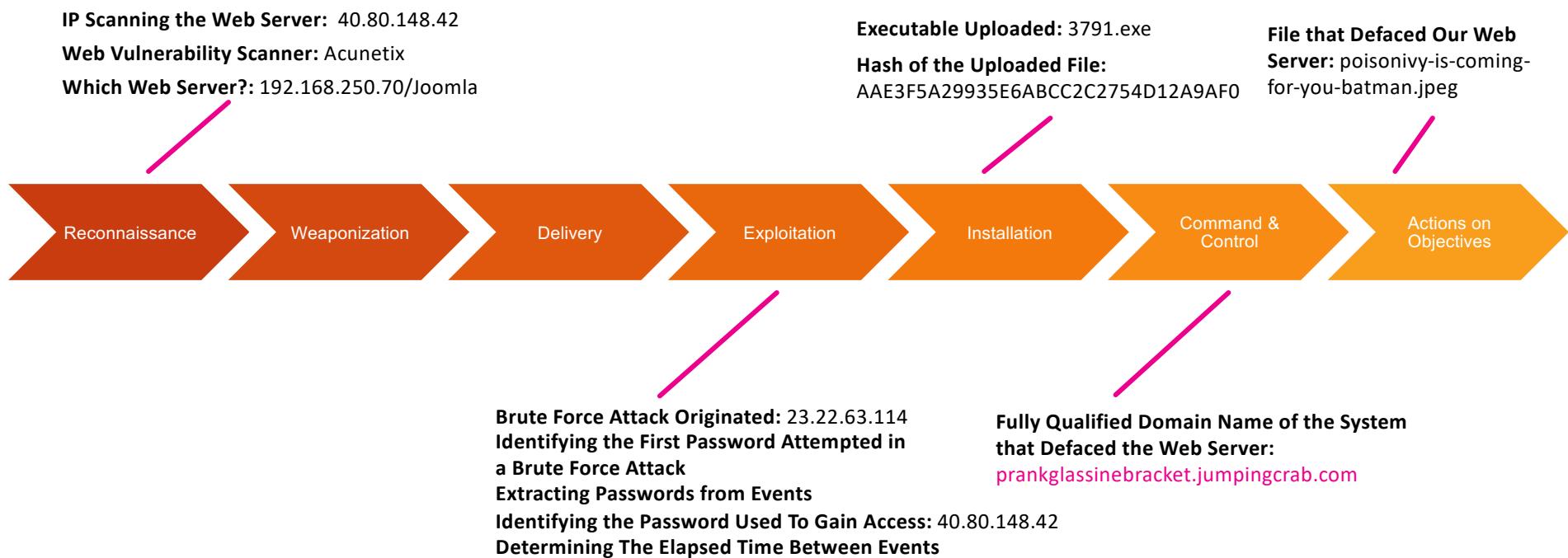
This attack used dynamic DNS to resolve to the malicious IP. What fully qualified domain name (FQDN) is associated with this attack?

- prankglassinebracket.jumpingcrab.com

More information on this topic

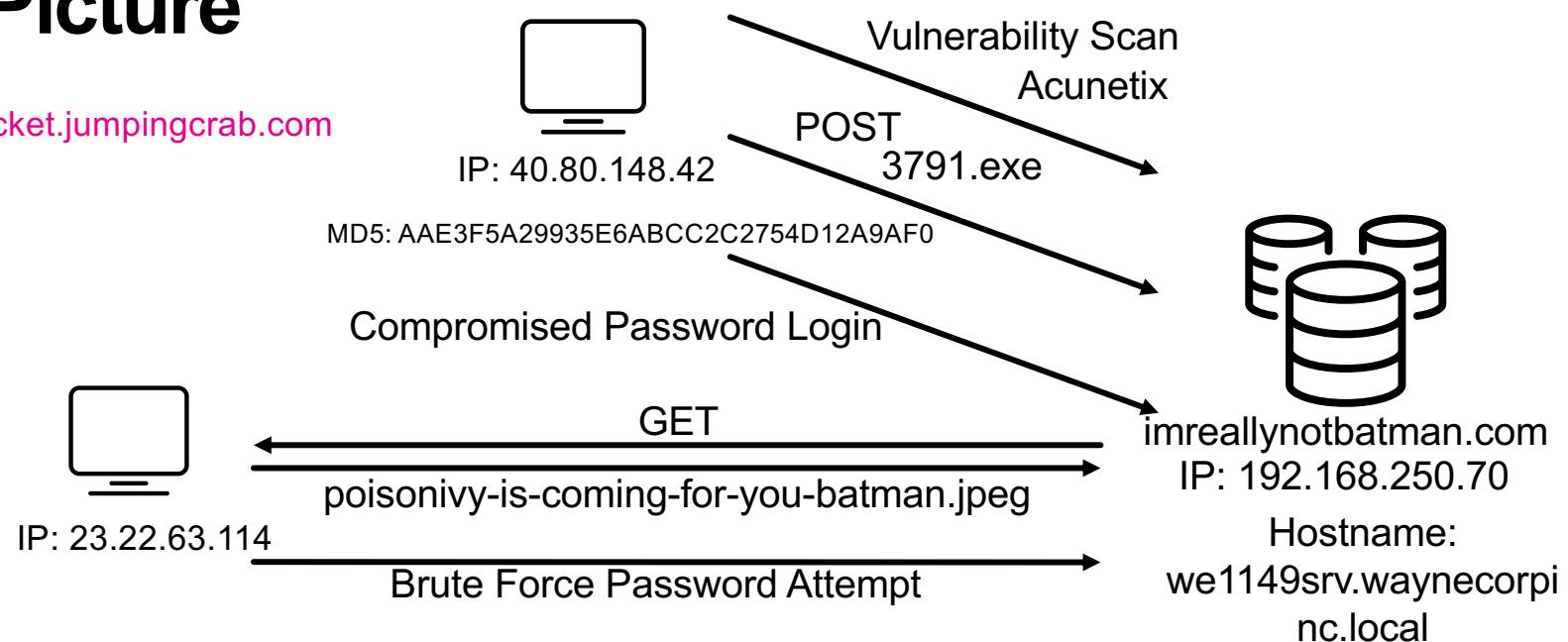
- <http://blogs.splunk.com/2015/08/04/detecting-dynamic-dns-domains-in-splunk/>

# Kill Chain



# APT Picture

DNS:  
prankglassinebracket.jumpingcrab.com



# Using OSINT to Identify Attacker Infrastructure

Kill Chain Phase: Weaponization

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?

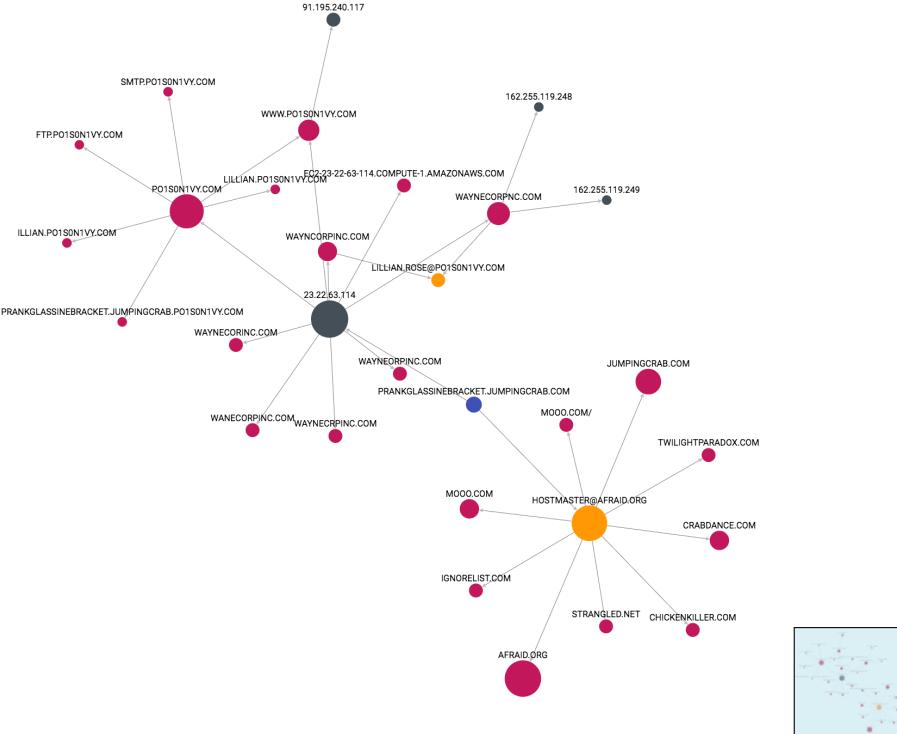
## Hints

- Sites like VirusTotal and ThreatCrowd will help identify the domain to IP association

# ThreatCrowd Domain Search

HELP RSS API FEED MALTEGO CONTACT SEARCH 

 [NEO4J](#)



DOMAIN >  
PRANKGLASSINEBRACKET.JUMPINGCRAB.COM

Welcome! Right click nodes and scroll the mouse to navigate the graph. 

More information on this domain is in [AlienVault OTX](#) 

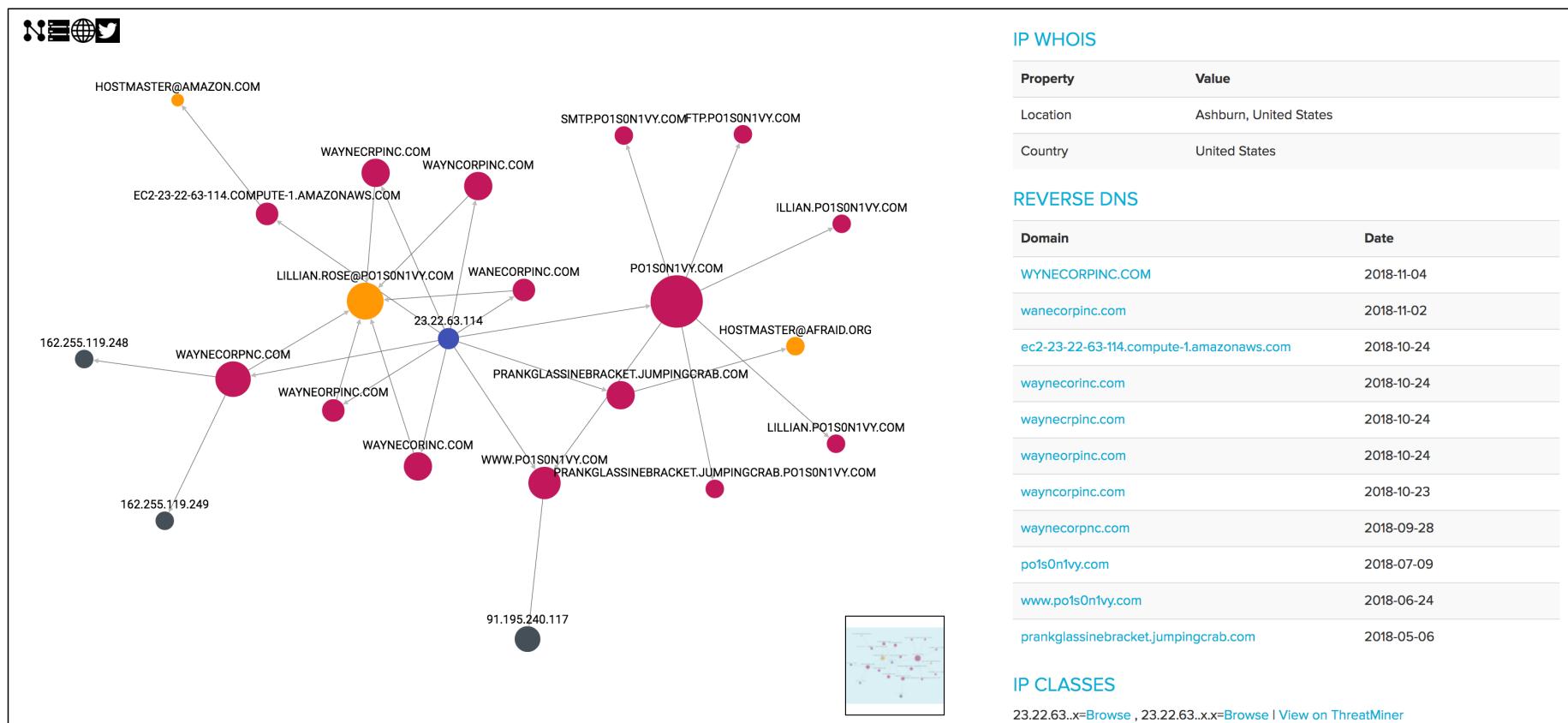
IS THIS MALICIOUS?

Yes	No	Most users have voted this as <b>MALICIOUS</b>
-----	----	--

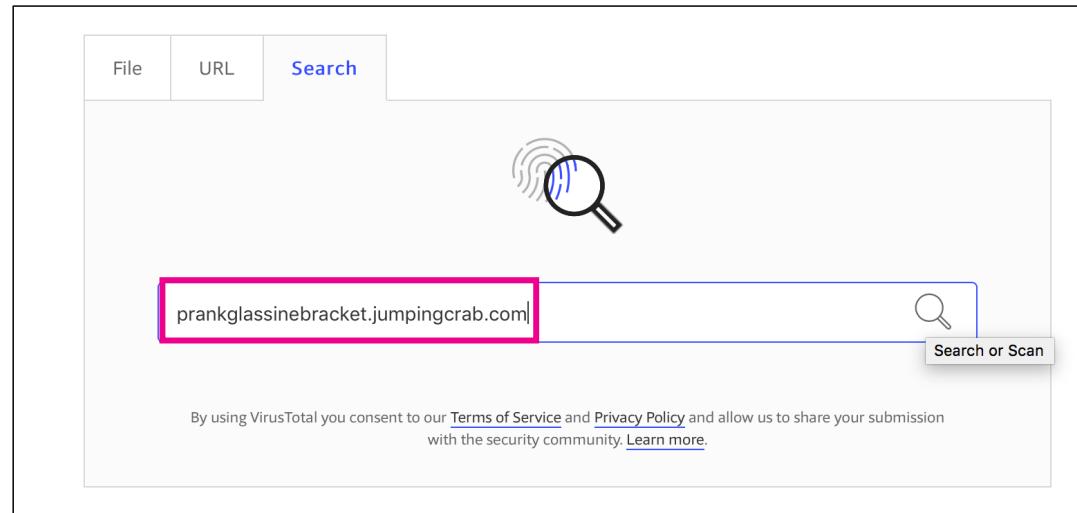
WHOIS

Property	Value
Name	<a href="#">Joshua Anderson</a>
Organization	Joshua Anderson
Email	<a href="mailto:hostmaster@afraid.org">hostmaster@afraid.org</a>
Address	4120 Douglas Blvd #306-199
Zip Code	95746
City	Granite Bay
State	CA

# ThreatCrowd – Pivot to IP



# Virus Total



The image shows the VirusTotal search interface. At the top, there are three input fields: "File", "URL", and "Search". The "Search" field is active and contains the URL "prankglassinebracket.jumpingcrab.com". Below the search bar is a large magnifying glass icon with a fingerprint pattern inside it. To the right of the search bar is a "Search or Scan" button with a magnifying glass icon. At the bottom of the interface, a small note states: "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

2016-09-14

IP address

23.22.63.114

# VirusTotal

23.22.63.114 IP address information

Country	US
Autonomous system	14618 (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	waneorpinc.com
2018-07-18	po1s0n1vy.com
2018-05-19	www.po1s0n1vy.com
2018-05-02	prankglassinebracket.jumpingcrab.com

into doing'

# Using OSINT to Identify Attacker Infrastructure

## Kill Chain Phase: Weaponization

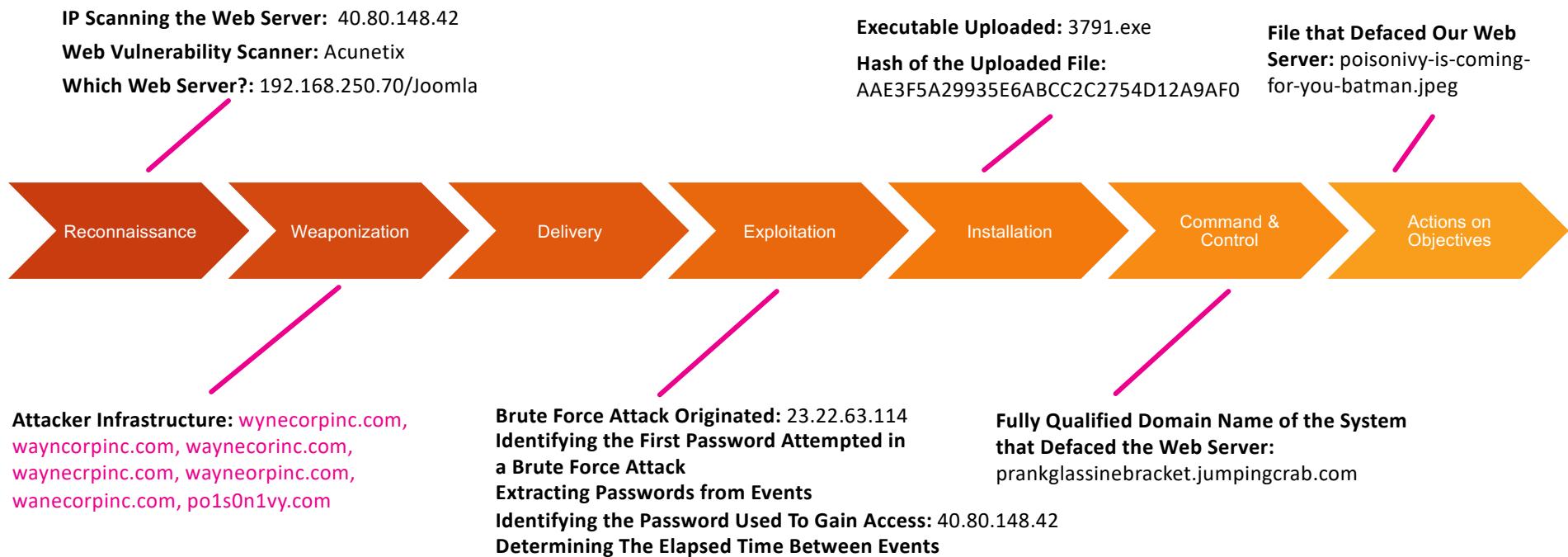
What IP address has P01s0n1vy tied to domains that are pre-staged to attack Wayne Enterprises?

- 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



# APT Picture

DNS:

prankglassinebracket.jumpingcrab.com

Other Domains:

wynecorpinc.com

wayncorpinc.com

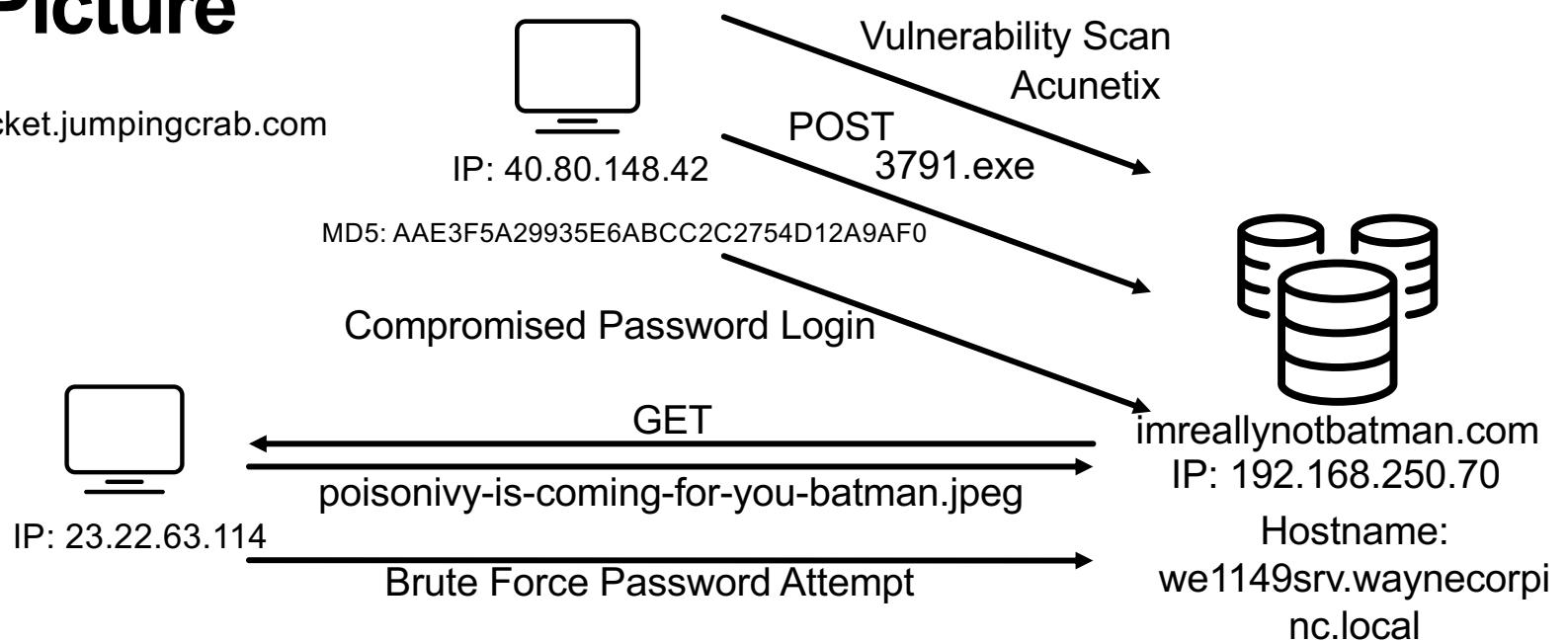
wayneccorinc.com

waynecrpinc.com,

wayneorpinc.com,

wanecorpinc.com

po1s0n1vy.com



# 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

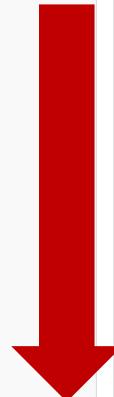


Threatminer can give me an MD5 of samples from 23.22.63.114 but not SHA256

Related samples

Copy Excel CSV PDF Search:

MD5	Detections	Analysis Date
c99131e0169171935c5ac32615ed6261	ALYac   Trojan.GenericKD.3470547	2016-09-01 09:03:44
	AVG   Agent5.APHV	
	AVware   Trojan.Win32.Generic!BT	
	Ad-Aware   Trojan.GenericKD.3470547	
	AegisLab   Agent5.Aphv.Gen!c	
	AhnLab-V3   Malware/Gen.Generic.N2081883700	
	Antiy-AVL   Trojan[Backdoor]/Win32.Redsip	
	Arcabit   Trojan.Generic.D34F4D3	
	Avira   TR/AD.Zupdax.qmyx	
	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.

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

## Metadata

File name:	MirandaTateScreensaver.scr.exe
File type:	PE32 executable (console) Intel 80386, for MS Windows
File size:	494080 bytes
Analysis date:	2016-09-01 09:03:44
MD5:	c99131e0169171935c5ac32615ed6261
SHA1:	bc927ff06263351f43db8dec88e4b08485e07996
SHA256:	9709473ab351387aab9e816eff3910b9f28a7a70202e250ed46dba8f820f34a8
SHA512:	8fb3b09541b021e06eeec455876526607114adb547eacb7556d578c08959154b80f01bac905383a5eb4c8a9091a3fb14dc13badc36a05ea7718bf4b1053f2fd
SSDEEP:	12288:JCy+DdcUrY4tO3Rc5F5H8q3/HSaRanZ0:Jj+COpO3Rc5F5H8q3/yaRaZ0
IMPHASH:	fae2c8486a11f609323cc15c0ee838cf
Authentihash:	N/A
Related resources	<a href="#">VirusTotal</a> <a href="#">Hybrid-Analysis</a> <a href="#">ThreatExpert</a> <a href="#">Malwr</a> <a href="#">VirusShare</a>

# VirusTotal - File Hash

## virustotal

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 )

 1 0

[Analysis](#) [File detail](#) [Additional information](#) [Comments 1](#) [Votes](#) [Behavioural information](#)

Antivirus	Result	Update
Ad-Aware	Trojan.Generic.17934902	20170816
AegisLab	Agent5.Aphv.Genic	20170816

splunk > turn data into doing®

# 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?

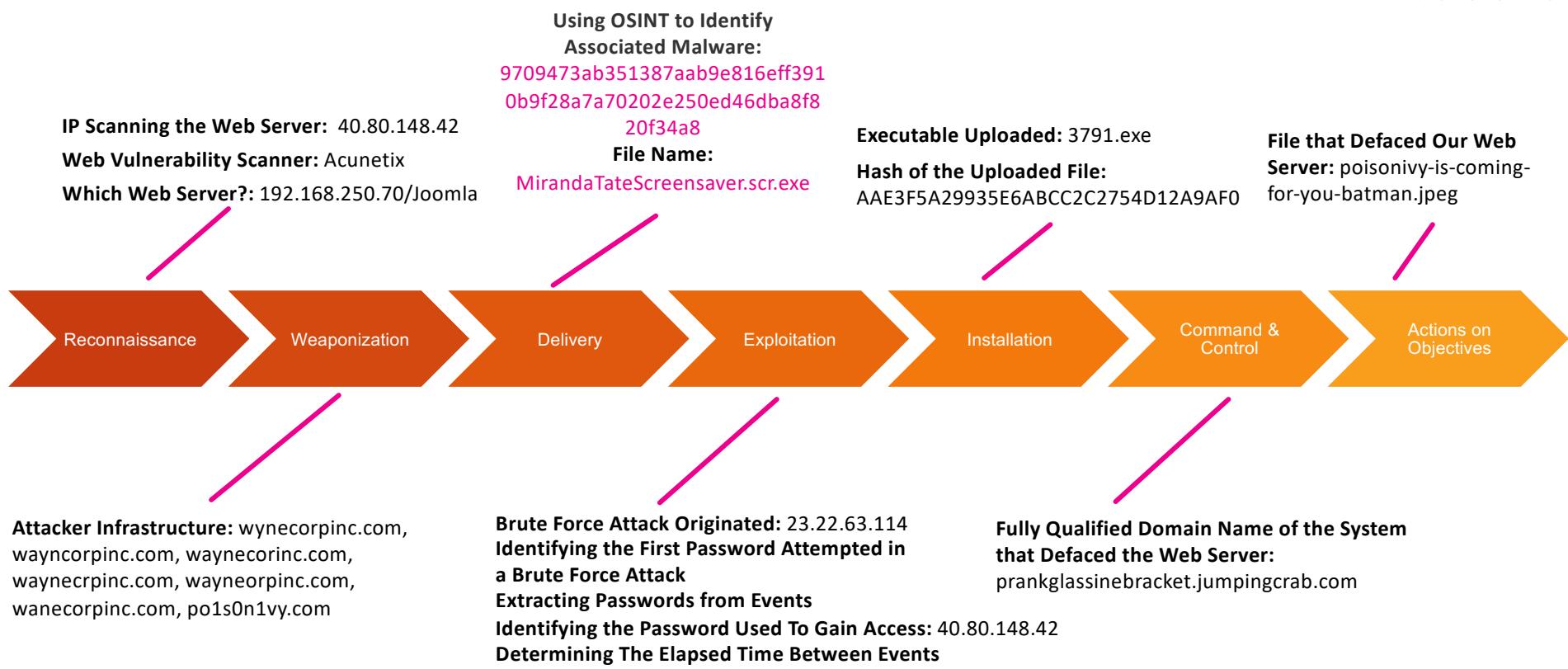
- MirandaTateScreensaver.scr.exe

Other sites of interest:

- [www.hybrid-analysis.com](http://www.hybrid-analysis.com)
- [virusshare.com](http://virusshare.com)

The screenshot shows the 'File Details' page for the file 'MirandaTateScreensaver.scr.exe'. The file is identified as a PE32 executable (console) for MS Windows, 32 Bit, with a SHA256 hash of 9709473ab351387aab9e816eff3910b9f28a7a70202e250ed46dba8f820f34a8. The classification section shows the following results:

- 67.4% (EXE) Win32 Executable MS Visual C++ (generic)
- 14.2% (DLL) Win32 Dynamic Link Library (generic)
- 9.7% (EXE) Win32 Executable (generic)
- 4.3% (EXE) Generic Win/DOS Executable
- 4.3% (EXE) DOS Executable Generic



# APT Picture

DNS:

prankglassinebracket.jumpingcrab.com

Other Domains:

wynecorpinc.com

wayncorpinc.com

wayneccorinc.com

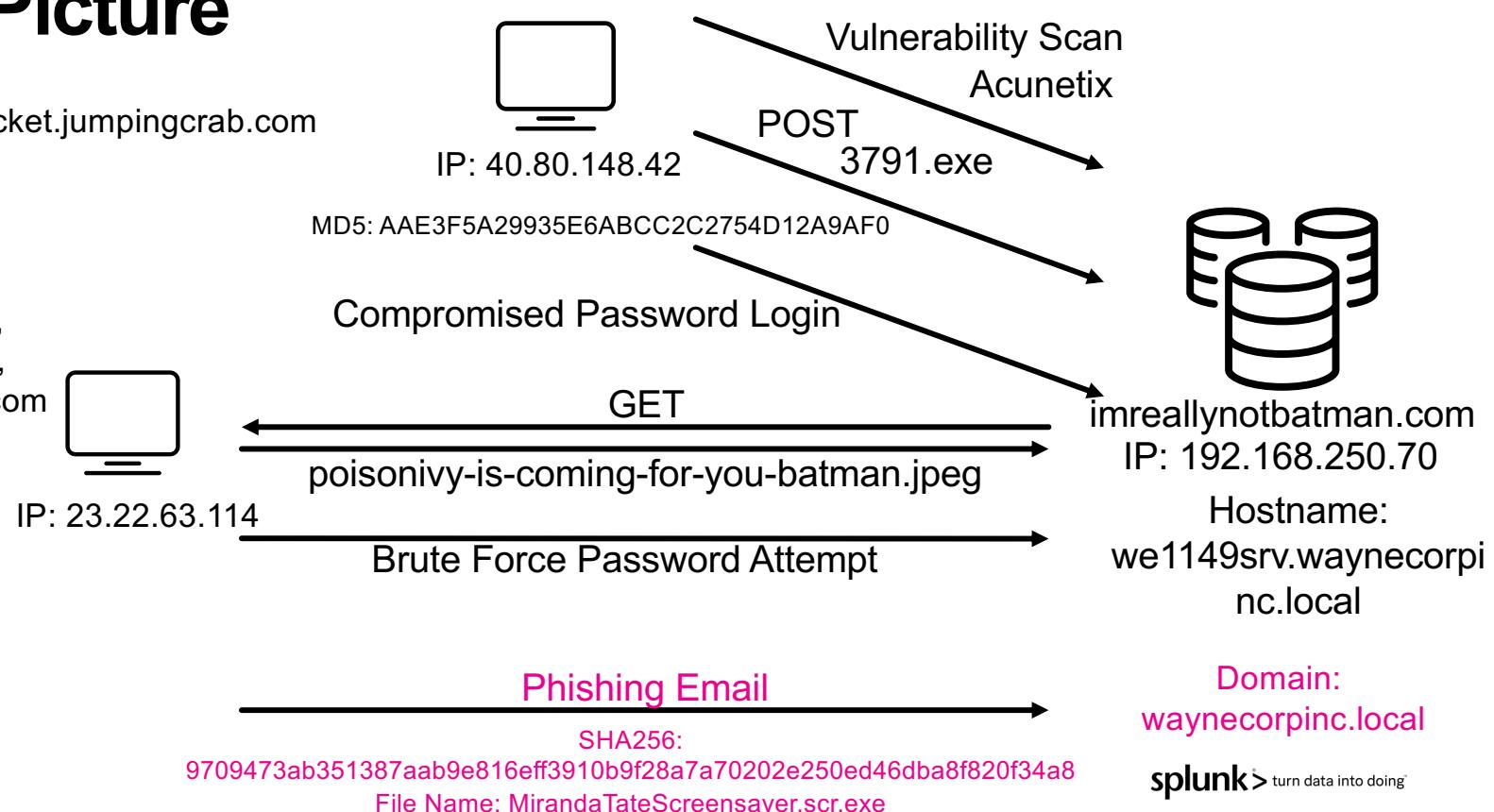
waynecrpinc.com,

wayneorpinc.com,

www.po1s0n1vy.com

wanecorpinc.com

po1s0n1vy.com



# APT Summary

Scanned for vulnerabilities

Found site is running Joomla

Performed a brute force password scan, logged into Joomla, installed file upload modules

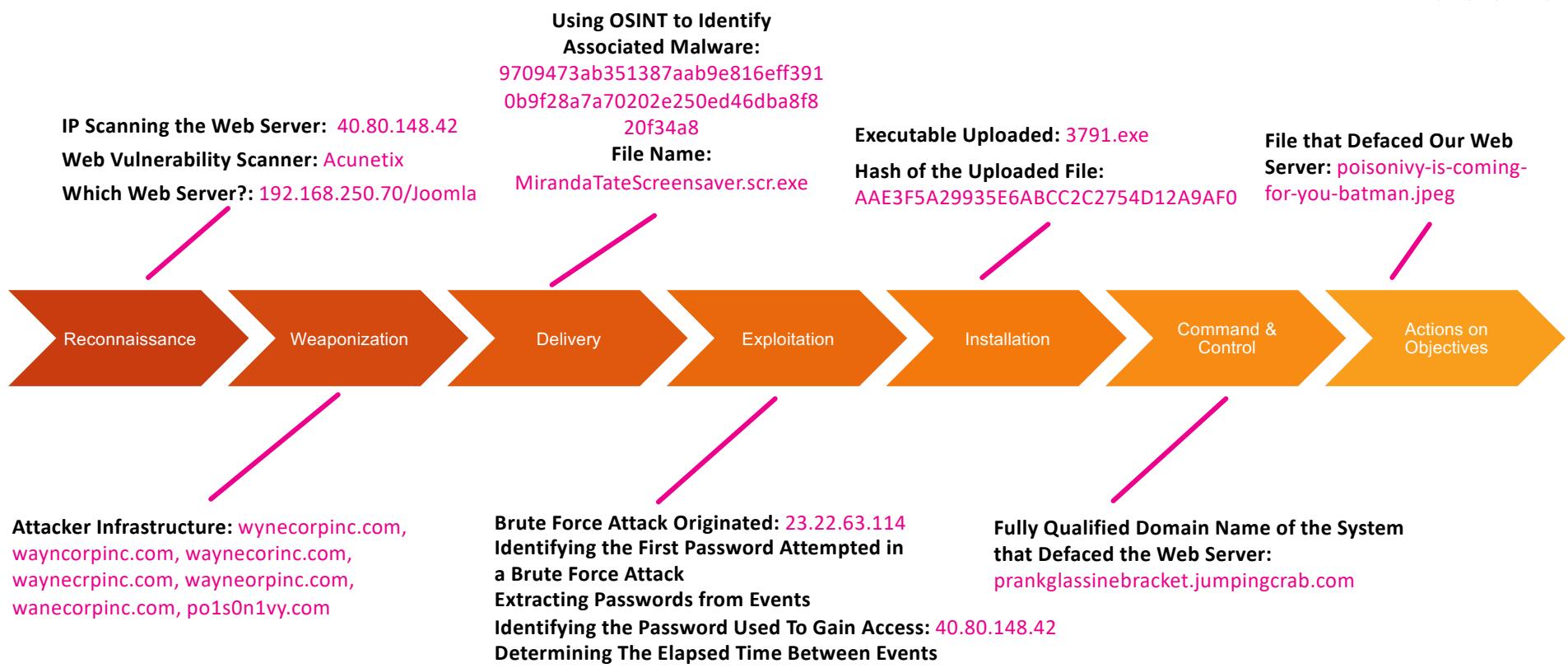
Uploaded webshell

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



# Overall APT Picture

DNS:

prankglassinebracket.jumpingcrab.com

Other Domains:

wynecorpinc.com

wayncorpinc.com

wayneccorinc.com

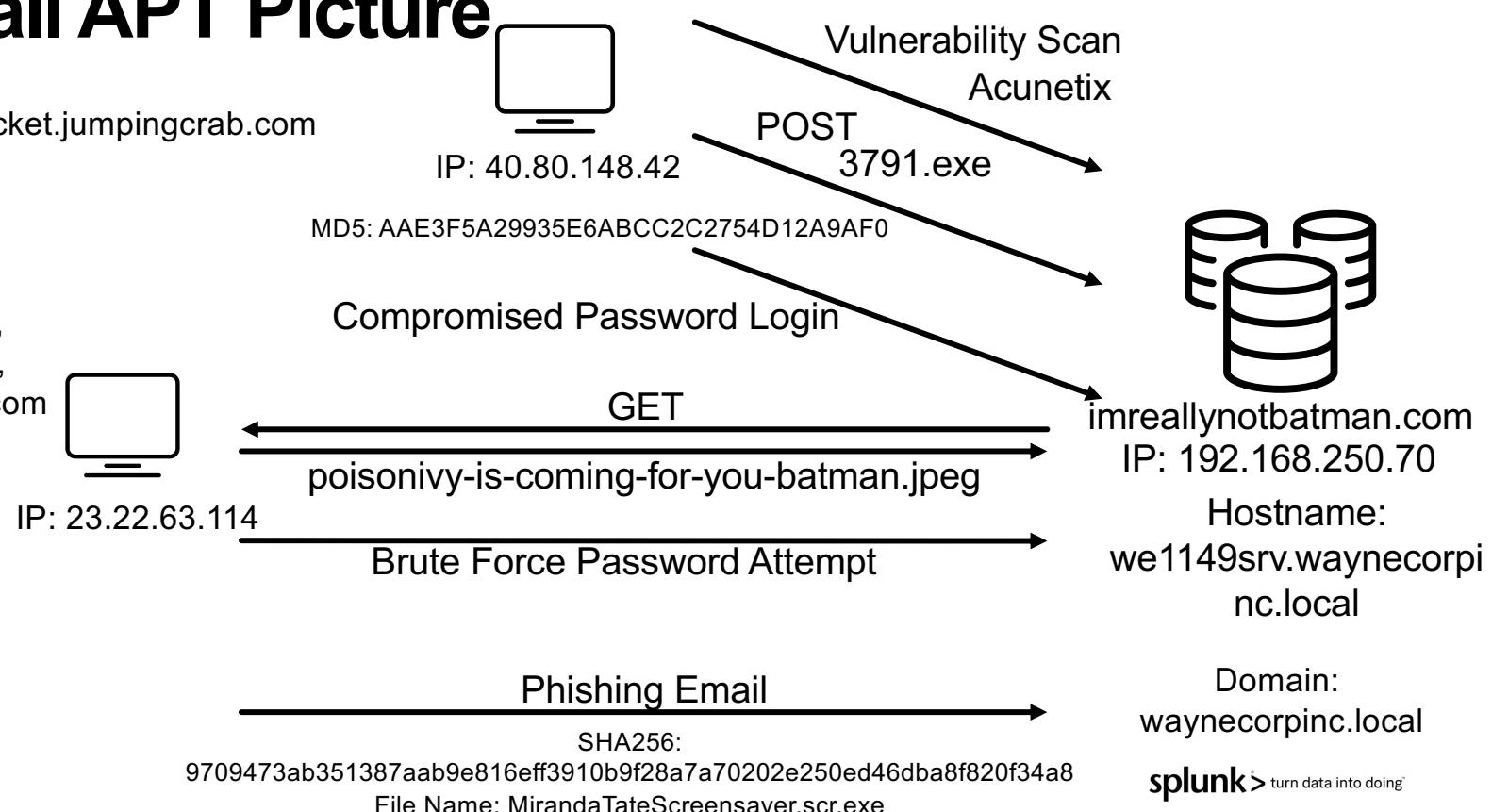
waynecrpinc.com,

wayneorpinc.com,

www.po1s0n1vy.com

wanecorpinc.com

po1s0n1vy.com



Domain:  
wayneccorinc.local

splunk > turn data into doing®

# Thank you!

**splunk**<sup>®</sup> turn data into doing<sup>™</sup>