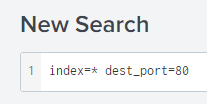
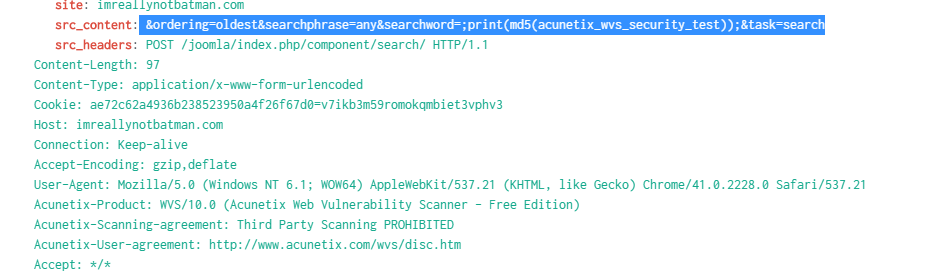
What is the likely IP address of someone from the Po1s0n1vy group scanning imreallynotbatman.com for web application vulnerabilities?

*Splunk Search =*

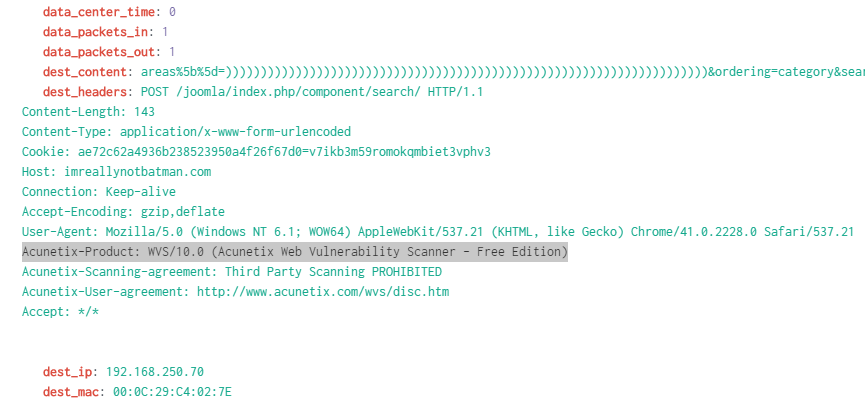


*Can see the ip under source IP:* ***40.80.148.42***

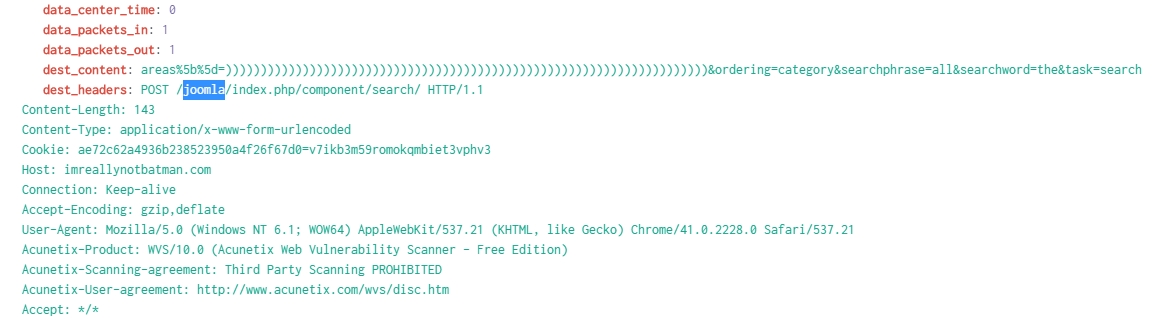
**Testing for vulns!**



What company created the web vulnerability scanner used by Po1s0n1vy?



What content management system is imreallynotbatman.com likely using?(Please do not include punctuation such as . , ! ? in your answer. We are looking for alpha characters only.)



What is the name of the file that defaced the imreallynotbatman.com website? Please submit only the name of the file with extension (For example "notepad.exe" or "favicon.ico")?

Make sure to set no event sampling

C\_ip stands for client ip address, if victim server is a client means they download stuff

Search = sourcetype=stream:http c\_ip="192.168.250.70"



Dynamic DNS =

**prankglassinebracket.jumpingcrab.com**

Search Command =

*prankglassinebracket.jumpingcrab.com*

*| sort by dest\_ip*

*| stats count(dest\_ip) AS sum BY dest\_ip*

Ip address tied to dynamic DNS =

**23.22.63.114**

[l33tstyle.afraid.org](https://otx.alienvault.com/indicator/hostname/l33tstyle.afraid.org)

*From <*[*https://otx.alienvault.com/indicator/hostname/l33tstyle.afraid.org*](https://otx.alienvault.com/indicator/hostname/l33tstyle.afraid.org)*>*

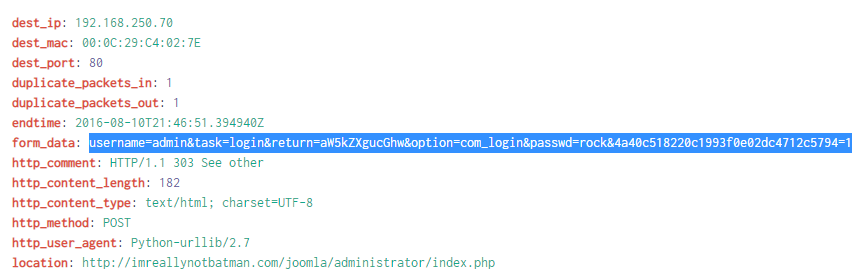
What IP address is likely attempting a brute force password attack against imreallynotbatman.com?

* Don’t know how to exclude from search the vulnerability scanner

Answer = **23.22.63.114**

Search Command =

*sourcetype=stream:http dest\_port=80 dest\_ip=192.168.250.70 http\_method=POST src!="40.80.148.42"*



What is the name of the executable uploaded by Po1s0n1vy?

Please include file extension. (For example, "notepad.exe" or "favicon.ico")

What was the first brute force password used?

Answer = **12345678**

Search =

*sourcetype=stream:http dest\_port=80 dest\_ip=192.168.250.70 http\_method=POST src!="40.80.148.42"*

*| sort Time*

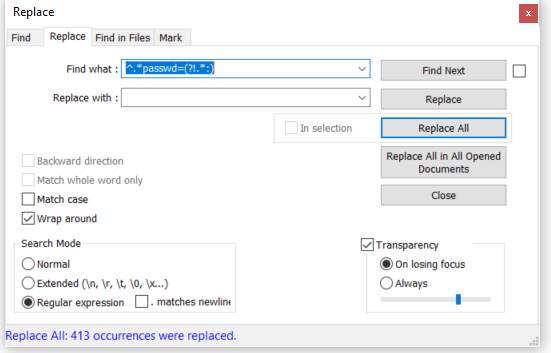
-> go to the last page



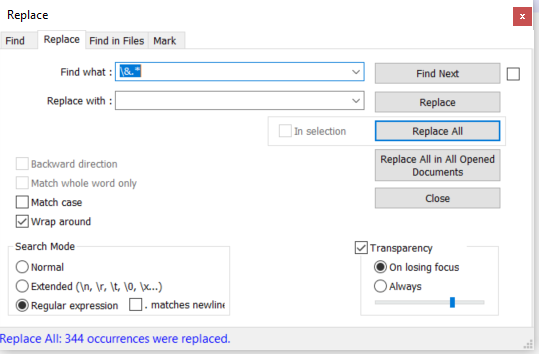
Look closely at the &, the things behind are not important.

Extracting passwords

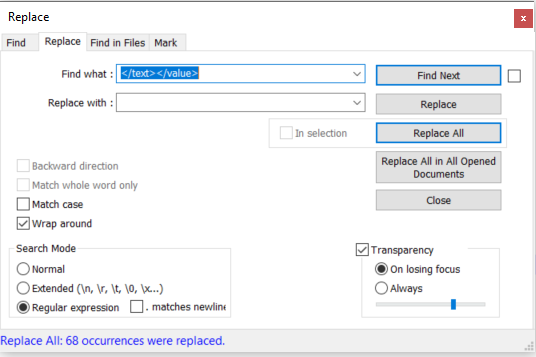
1. Export as xml all events
2. Paste into notepadd++
3. Do a ctrl F
4. Replace
5. Locate passwd and store only the string after
   1. Command = *^.\*passwd=(?!.\*:)*



1. Remove all the string after "&"
   1. Command = *\&.\**



1. Remove </test></value>



One of the passwords in the brute force attack is James Brodsky's favorite Coldplay song.

Hint: we are looking for a six character word on this one. Which is it?

Answer = **yellow**

*Search Command =*

*index=botsv1 sourcetype=stream:http form\_data=\*username\*passwd\**

*| rex field=form\_data "passwd=(?<userpassword>\w+)"*

*| eval lenpword=len(userpassword)*

*| search lenpword=6*

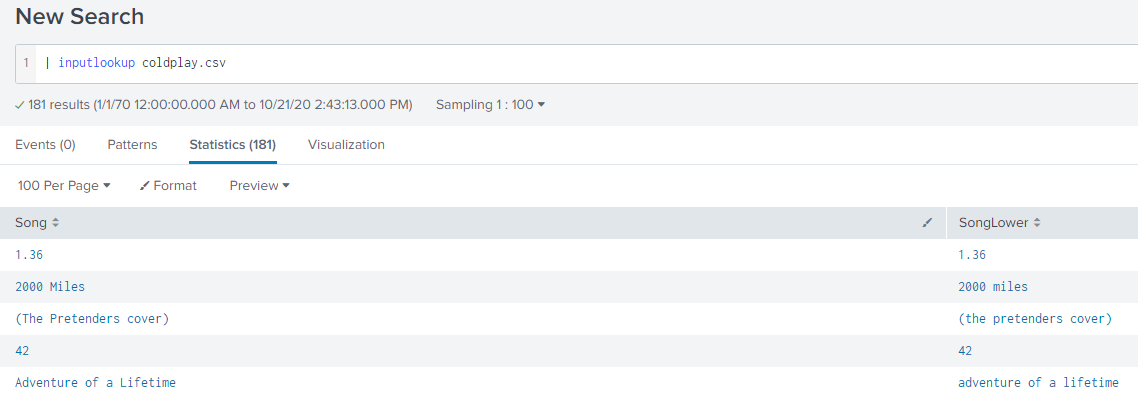
*| eval password=lower(userpassword)*

*| lookup coldplay.csv SongLower as password OUTPUTNEW SongLower*

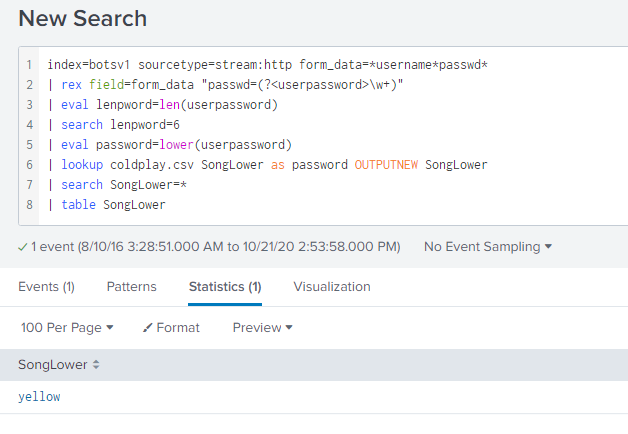
*| search SongLower=\**

*| table SongLower*

1. Using excel, import by url
   1. Go to Data Tab, go to From Web, enter URL = <https://en.wikipedia.org/wiki/List_of_songs_recorded_by_Coldplay>
2. Case sensitive comparison, convert song titles to lower
   1. In excel, Formula = Lower(value)
3. Open csv in notepad, save in encocding 8
4. Back to splunk, Settings > lookups > add lookup file
5. Check if csv has been imported



1. Enter the search command above
   1. Documentation to understand syntax: <https://docs.splunk.com/Documentation/Splunk/8.0.6/SearchReference/Lookup>

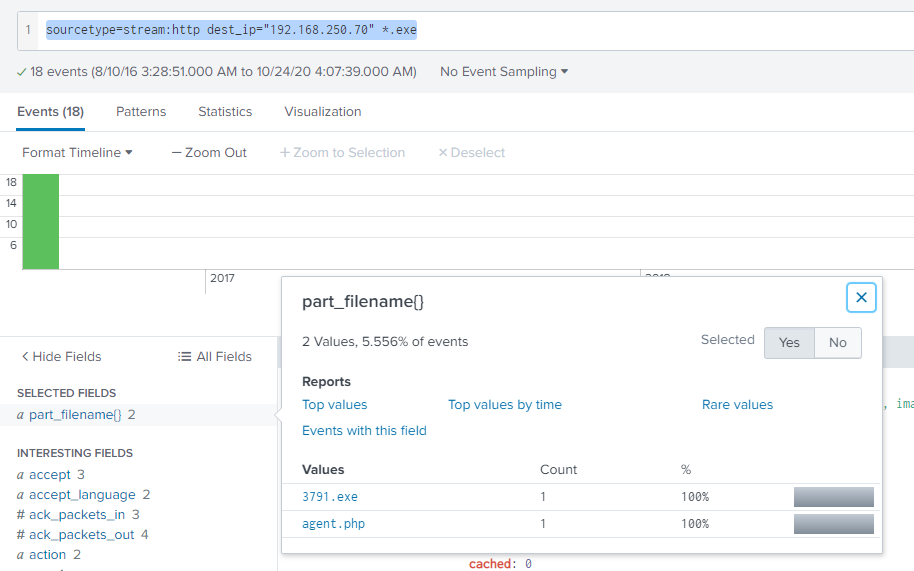


10        What is the name of the executable uploaded by Po1s0n1vy? Please include file extension. (For example, "notepad.exe" or "favicon.ico")

Answer = 3791.exe

Following this guide (<https://lantern.splunk.com/hc/en-us/articles/360049240973-Executable-uploaded-to-a-web-server->):

Command = sourcetype=stream:http dest\_ip="192.168.250.70" \*.exe



11        What is the MD5 hash of the executable uploaded?

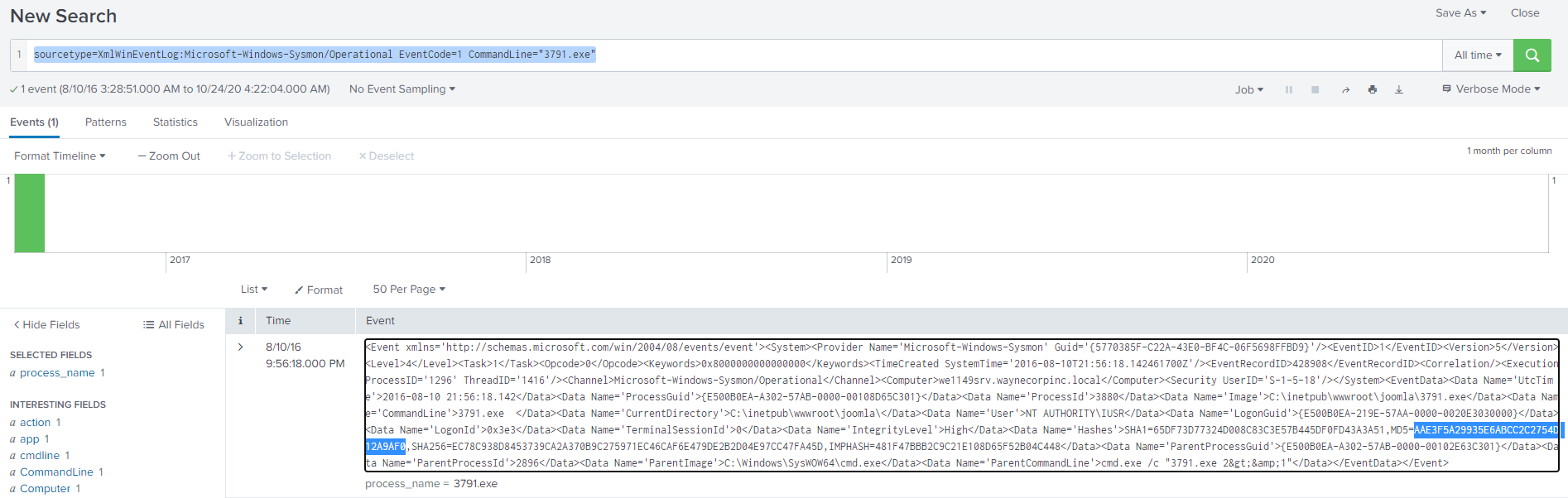
Answer = AAE3F5A29935E6ABCC2C2754D12A9AF0

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

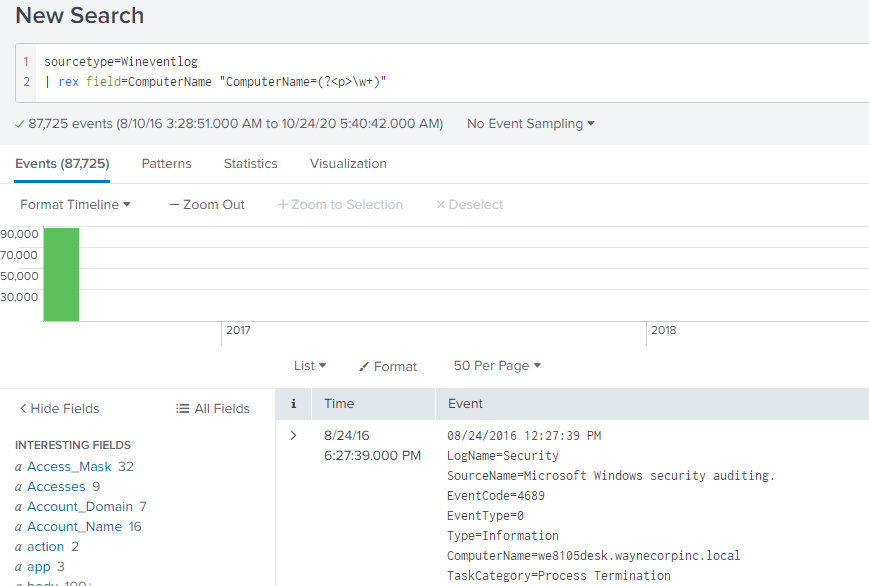
Reference: <https://lantern.splunk.com/hc/en-us/articles/360049240973-Executable-uploaded-to-a-web-server>-

Executing the exe is when the exe is on the command line.

The exe is executed with this cmd "cmd.exe /c "3791.exe 2&gt;&amp;1"

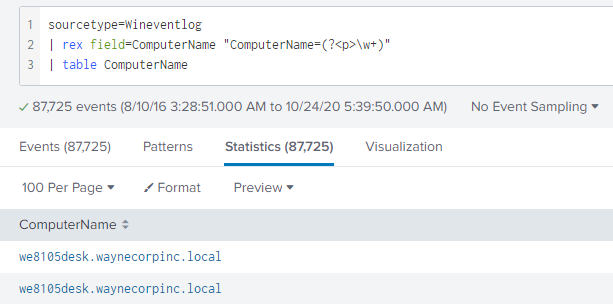


Understanding splunk regex

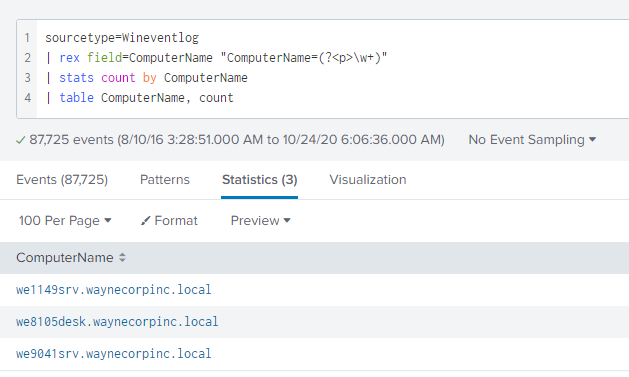


sourcetype=Wineventlog

| rex field=ComputerName "ComputerName=(?<p>\w+)"



Stats command is like group   
Stats count by ComputerName = group by computerName and do a count



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

Hint: if hdyra find correct password, will try it twice

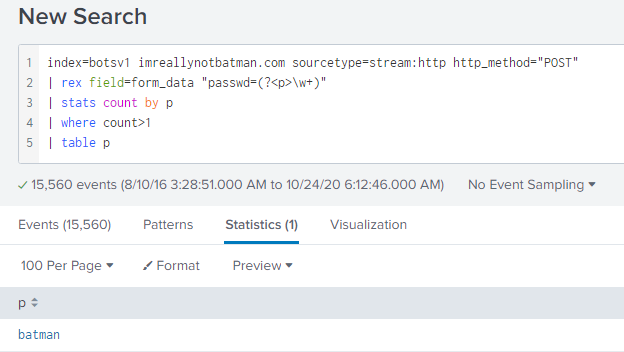
sourcetype=stream:http dest\_port=80 dest\_ip=192.168.250.70 http\_method=POST src!="40.80.148.42"

| rex field=form\_data "passwd=(?<p>\w+)"

| stats count by p

| where count>1

"P" refers to the things inside passwd!

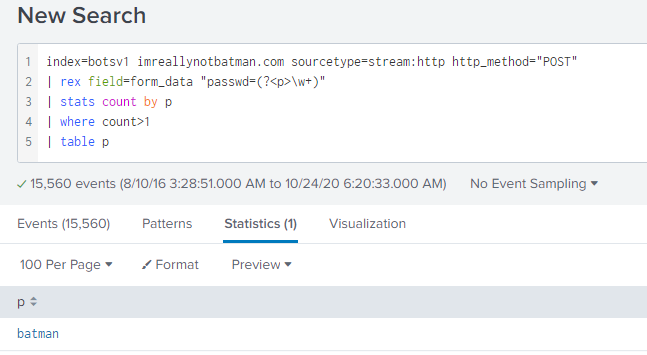


form\_data: username=admin&task=login&return=aW5kZXgucGhw&option=com\_login

&passwd=sammy&0d3bb0020f70044ffba32f7d0fa7fa88=1

Rex field=form\_data "passwd=(?<p>\w+)"

Means find in form\_data string until passwd=, the thing after is placed in <p>



18        What was the average password length used in the password brute forcing attempt? (Round to closest whole integer. For example "5" not "5.23213")

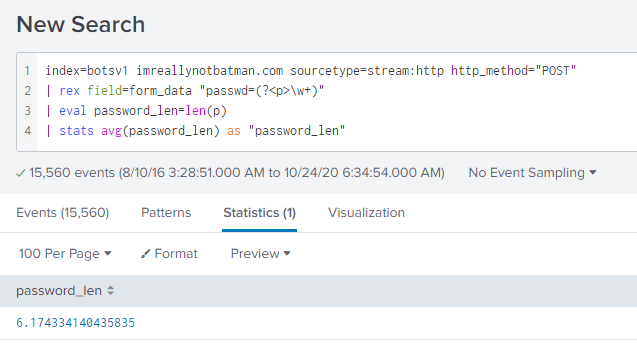
Command =

index=botsv1 imreallynotbatman.com sourcetype=stream:http http\_method="POST"

| rex field=form\_data "passwd=(?<p>\w+)"

| eval password\_len=len(p)

| stats avg(password\_len) as "password\_len"



19        How many seconds elapsed between the time the brute force password scan identified the correct password and the compromised login? Round to 2 decimal places.

Answer = 92.17

Command =

*index=botsv1 imreallynotbatman.com sourcetype=stream:http http\_method="POST" | rex field=form\_data "passwd=(?<p>\w+)" | search p=batman*

*| table \_time, p, src\_ip*

*| sort by \_time*



\_time is specific field that shows the time the log is captured. Not on the event

20        How many unique passwords were attempted in the brute force attempt?

Answer = 412

Since attacker IP = 23.22.63.114, need to specify src

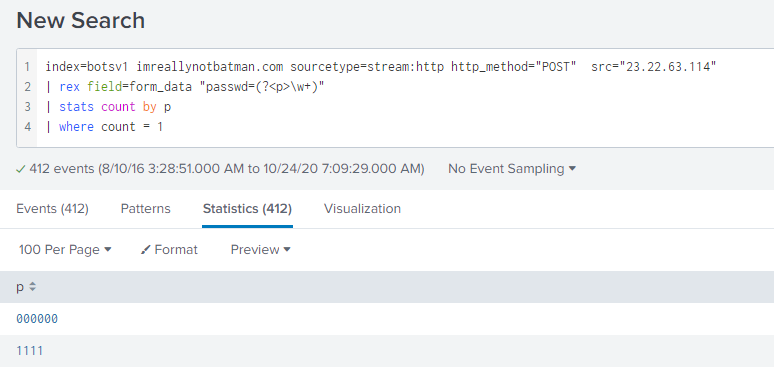
Command =

*index=botsv1 imreallynotbatman.com sourcetype=stream:http http\_method="POST" src="23.22.63.114"*

*| rex field=form\_data "passwd=(?<p>\w+)"*

*| stats count by p*

*| where count = 1*



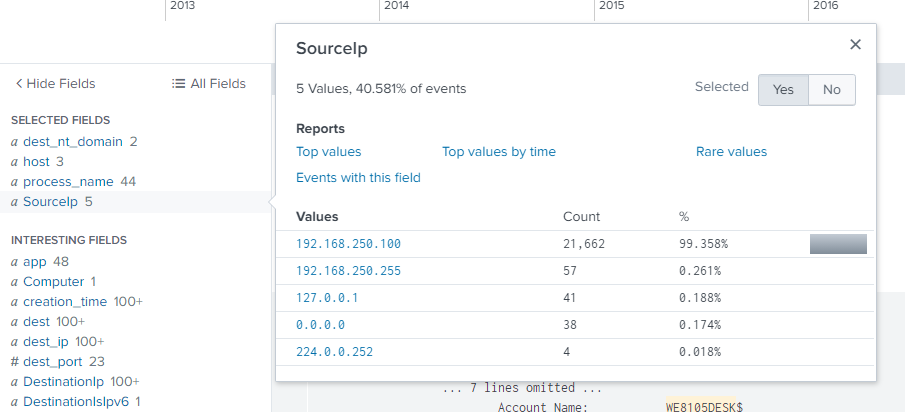
Answer derived from looking at statistics count

21        What was the most likely IP address of we8105desk on 24AUG2016?

Answer = 192.168.250.100

Command = we8105desk

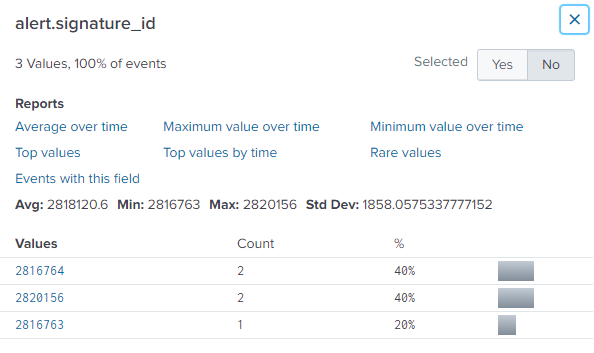
-> go to all fields and add sourceip



22        Amongst the Suricata signatures that detected the Cerber malware, which one alerted the fewest number of times? Submit ONLY the signature ID value as the answer. (No punctuation, just 7 integers.)

Answer = 2816763

Command = Cerber sourcetype=suricata



23        What fully qualified domain name (FQDN) does the Cerber ransomware attempt to

direct the user to at the end of its encryption phase?

Answer = **cerberhhyed5frqa.xmfir0.win**

Search =

*index=botsv1 src\_ip="192.168.250.100" sourcetype=stream:dns*

*| spath "query{}"*

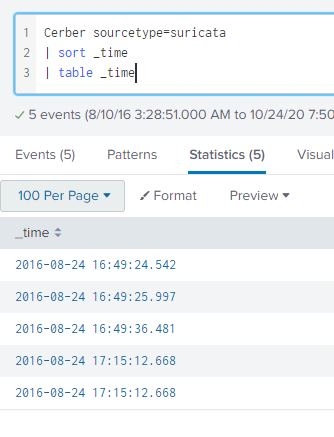
*| search "query{}"!="\_ldap.\_tcp.pdc.\_msdcs.waynecorpinc.local" "query{}"!="\_ldap.\_tcp.dc.\_msdcs.waynecorpinc.local" record\_type=A*

*| table query{},\_time*

*| sort \_time*

Go to the time after 08/24, 1649pm

* Examine the five Suricata alerts about Cerber. View them as "raw text" in time order. Alerts came about 16.49



24        What was the first suspicious domain visited by we8105desk on 24AUG2016?

Answer = **solidaritedeproximite.org**

Command =

*index=botsv1 src\_ip="192.168.250.100" sourcetype=stream:http*

*| table query{},\_time*

*| sort \_time*

Go to Time and select the time before 16:49

At time:

8/24/16

4:48:13.285 PM



25        During the initial Cerber infection a VB script is run. The entire script from this execution,

pre-pended by the name of the launching .exe, can be found in a field in Splunk.

What is the length in characters of the value of this field?

Answer = 4490

Command =

*\*.vbs \*.exe*

*| eval length=len(CommandLine)*

*| table CommandLine, length*

26        What is the name of the USB key inserted by Bob Smith?

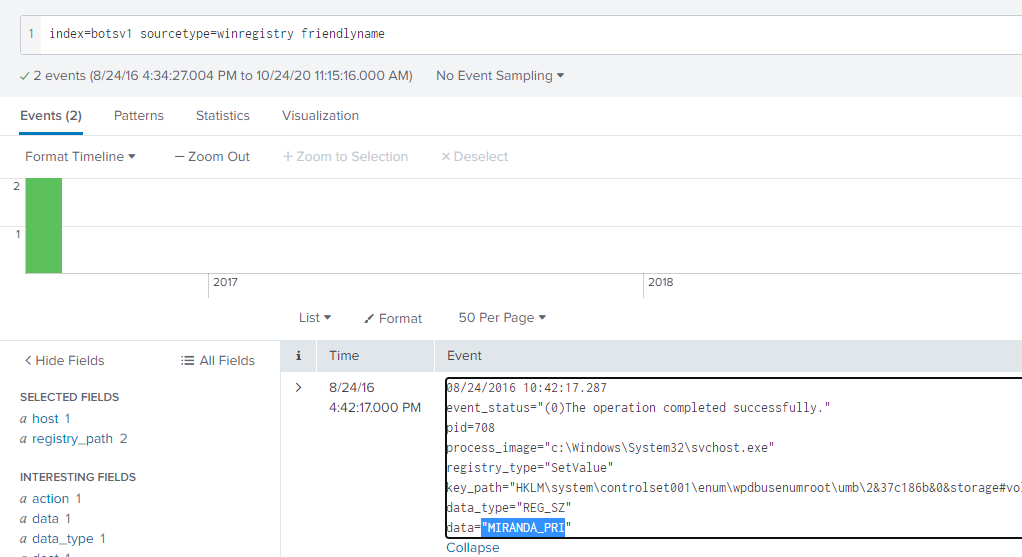
Answer = MIRANDA\_PRI

Command =

*sourcetype=winregistry friendlyname*

<https://lantern.splunk.com/hc/en-us/articles/360048497294-Removable-devices-connected-to-a-machine>

The value in the registry\_value\_data field is the name of the USB device. After you have identified the device, you might want to look at the host or src\_ip fields in the search result to identify the machine the device was plugged into. You might also want to identify any files that were downloaded from the removable device.



27        Bob Smith's workstation (we8105desk) was connected to a file server during the

ransomware outbreak. What is the IP address of the file server?

Plugged in at 4.42:17

Answer = **192.168.250.20**

Command =

*host="we8105desk" fileshare*

*| sort \_time*

28        How many distinct PDFs did the ransomware encrypt on the remote file server?

Answer = 257

Command =

*index=botsv1 \*.pdf sourcetype="wineventlog" dest="we9041srv.waynecorpinc.local"*

*| stats count by Relative\_Target\_Name*

*| sort count*

Learning point is to look for distinct destinations, those with abnormal counts usually suspicious,

Not too sure why its on we9041srv instead of the we8105desk tho…

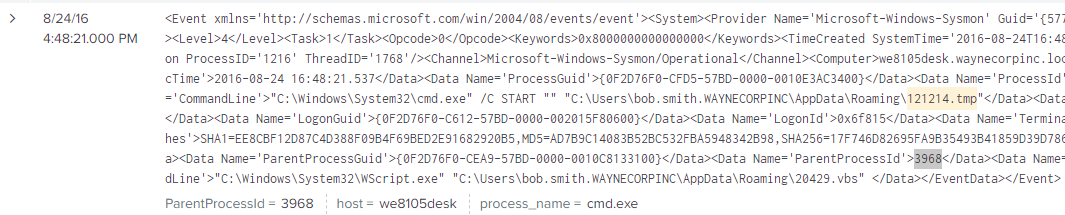
29        The VBscript found in question 25 launches 121214.tmp. What is the ParentProcessId of this initial launch?

Answer = 3968

Command =

121214.tmp EventDescription="Process Create"

| sort -time



30        The Cerber ransomware encrypts files located in Bob Smith's Windows profile. How many .txt files does it encrypt?

Answer = 406

Command =

*host=we8105desk \*.txt TargetFilename="C:\\Users\\bob.smith.WAYNECORPINC\\\*.txt"*

*| stats count by TargetFilename*

*| table TargetFilename, count*

Learning point filtering text files and files that start with bob.smith… etc

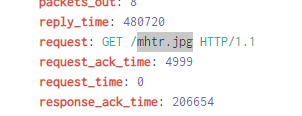
TargetFilename also is an interesting field to take note

31        The malware downloads a file that contains the Cerber ransomware cryptor code. What is the name of that file?

Answer = mhtr.jpg

Command =

solidaritedeproximite.org



32        Now that you know the name of the ransomware's encryptor file, what obfuscation technique does it likely use?

Answer =

Steganography