### **BOTSv1 — Web site defacement**

**Scenario:** Today is Alice’s first day at the Wayne Enterprises’ Security Operations Center. Lucius sits Alice down and gives her first assignment: A memo from Gotham City Police Department (GCPD). Apparently GCPD has found evidence online (http://pastebin.com/Gw6dWjS9) that the website www.imreallynotbatman.com hosted on Wayne Enterprises’ IP address space has been compromised. The group has multiple objectives… but a key aspect of their modus operandi is to deface websites in order to embarrass their victim. Lucius has asked Alice to determine if www.imreallynotbatman.com. (the personal blog of Wayne Corporations CEO) was really compromised.

Note: These questions are not ordered as they appear in the actual website, I ordered them in the natural investigation order.

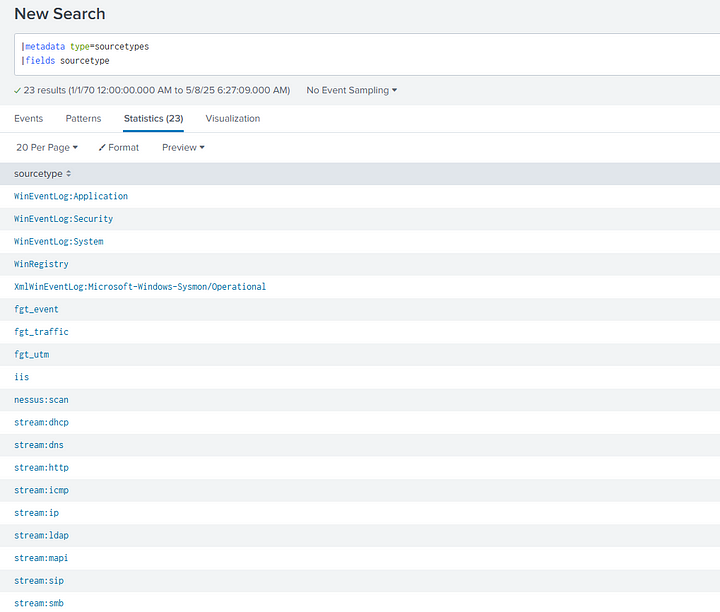
#### **Investigation**

**Note:** The questions are not in the order they were given in the challenge, they are ordered in a logical progression which I thought would depict the attackers actions in different stages.

Before starting the investigation let us look at the source types we are working with

|metadata type=sourcetypes

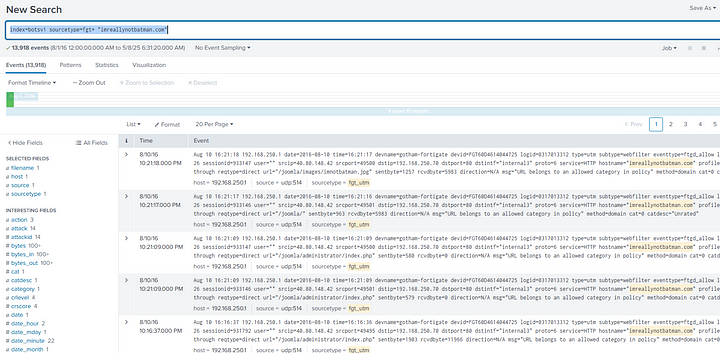
|fields sourcetype



1. **What is the likely IPv4 address of someone from the Po1s0n1vy group scanning imreallynotbatman.com for web application vulnerabilities?**

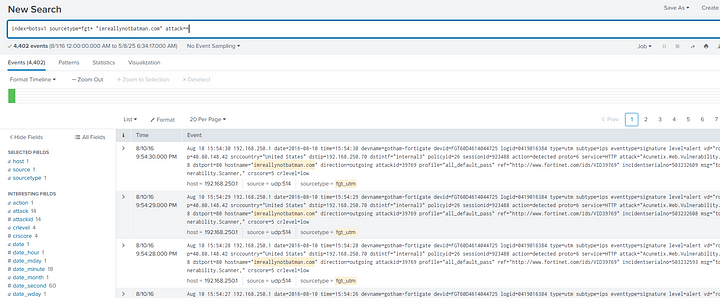
Let us look at the FortiGate logs specifically belonging to the website imreallynotbatman.com

index=botsv1 sourcetype=fgt\* "imreallynotbatman.com"



In the interesting fields section we can see a field called attack. This filed contains the signature of the attack detected. Let us filter out for the events that contain this field.

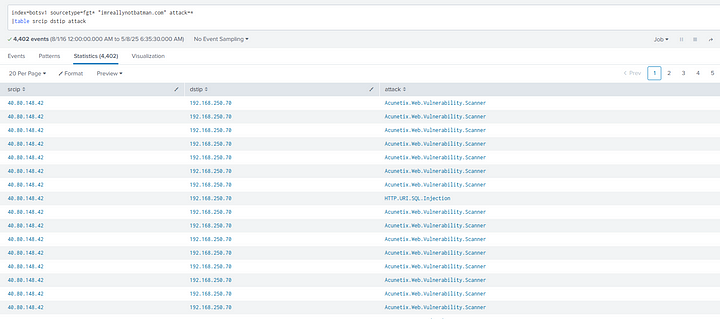
index=botsv1 sourcetype=fgt\* "imreallynotbatman.com" attack=\*



Now let us list the IP address and the attack field using the table command.

index=botsv1 sourcetype=fgt\* "imreallynotbatman.com" attack=\*

|table srcip dstip attack



We can find above the IP scanning the website.

**Answer:** 40.80.148.42

**2. What company created the web vulnerability scanner used by Po1s0n1vy? Type the company name.**

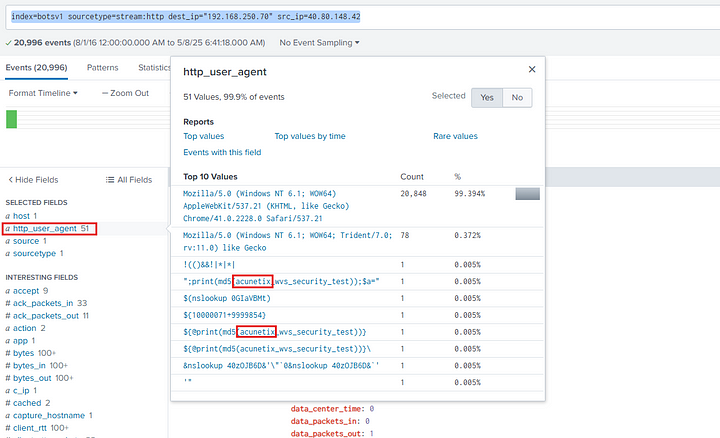
We can find this from the above image.

**Answer:** Acunetix

We can also find this from the http user agent.

index=botsv1 sourcetype=stream:http dest\_ip="192.168.250.70" src\_ip=40.80.148.42

Now we can see the http\_user\_agent field in the interesting fields section.

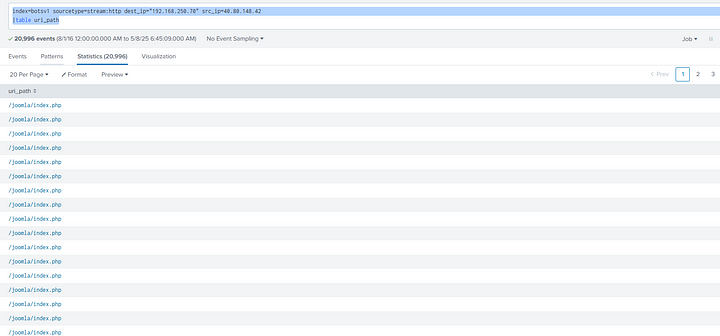


**3. What content management system is imreallynotbatman.com likely using?**

On the above search we can add a command to list out the URL's.

index=botsv1 sourcetype=stream:http dest\_ip="192.168.250.70" src\_ip=40.80.148.42

|table uri\_path



We can see in the URL’s which contain joomla which is a content management service.

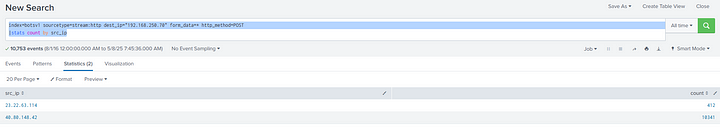
**Answer:** Joomla

**4. What IPv4 address is likely attempting a brute force password attack against imreallynotbatman.com?**

Let us look at the IP addresses that posted something to the website using the form\_data.

index=botsv1 sourcetype=stream:http dest\_ip="192.168.250.70" form\_data=\* http\_method=POST

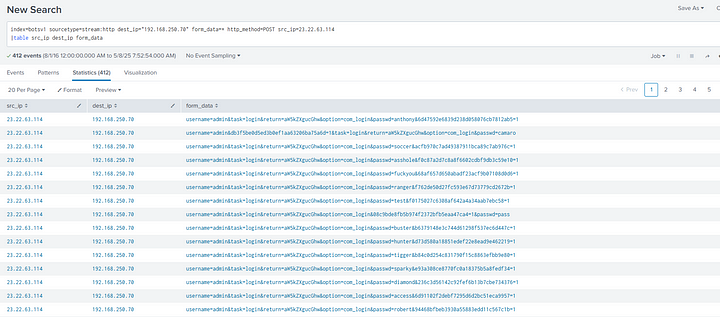
|stats count by src\_ip



We got two Ip addresses. Let us look at what the IP address 23.22.63.114 since it has lesser requests which will be easier to either rule out this IP or not.

index=botsv1 sourcetype=stream:http dest\_ip="192.168.250.70" form\_data=\* http\_method=POST src\_ip=23.22.63.114

|table src\_ip dest\_ip form\_data



As we can see, this IP tried a large number of passwords for the admin account.

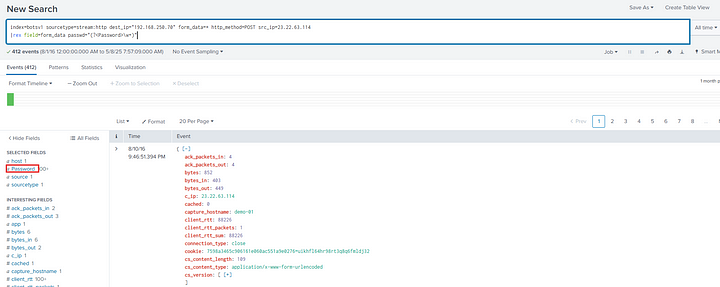
**Answer:** 23.22.63.114

**5. What was the first brute force password used?**

Let us first extract the passwords from the form data.

index=botsv1 sourcetype=stream:http dest\_ip="192.168.250.70" form\_data=\* http\_method=POST src\_ip=23.22.63.114

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

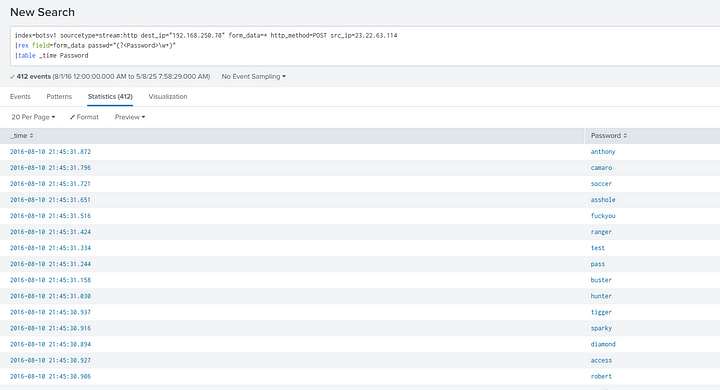


We can see a new filed named Password in the fields list. We can list these passwords in a table along with the time.

index=botsv1 sourcetype=stream:http dest\_ip="192.168.250.70" form\_data=\* http\_method=POST src\_ip=23.22.63.114

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

|table \_time Password



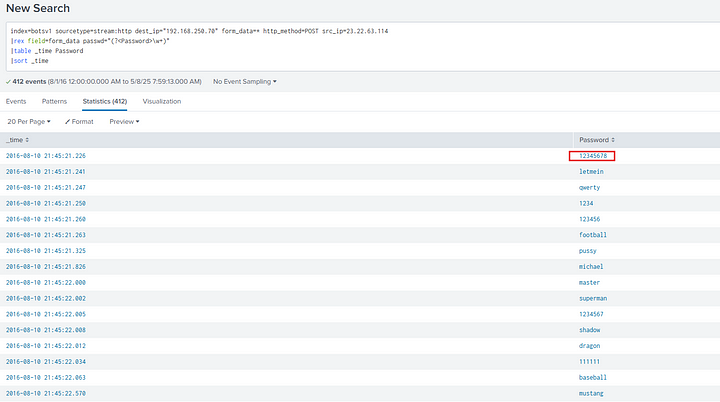
Now we can sort these results on time to find out the first password used.

index=botsv1 sourcetype=stream:http dest\_ip="192.168.250.70" form\_data=\* http\_method=POST src\_ip=23.22.63.114

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

|table \_time Password

|sort \_time



**Answer:** 12345678

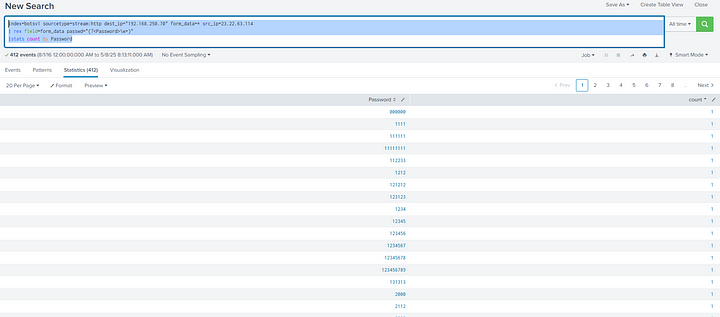
**6. What was the correct password for admin access to the content management system running “imreallynotbatman.com”?**

Once the attacker finds the right password, they will use to login, so we should look at any password that was used twice.

index=botsv1 sourcetype=stream:http dest\_ip="192.168.250.70" form\_data=\* src\_ip=23.22.63.114

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

|stats count by Password

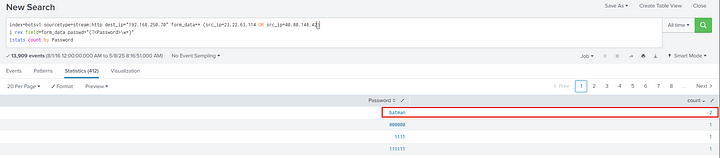


This did not give any results. So may be the attacker logged in with a different IP address to login, once they found out the right password, so we can check also with the IP address we found earlier.

index=botsv1 sourcetype=stream:http dest\_ip="192.168.250.70" form\_data=\* (src\_ip=23.22.63.114 OR src\_ip=40.80.148.42)

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

|stats count by Password



**Answer:** batman

**7. How many unique passwords were attempted in the brute force attempt?**

From the above investigation it is clear that the IP address 23.22.63.114 is the one which was used to conduct the bruteforce attack. So we can count the number of requests from this IP addresses to answer this question.

index=botsv1 sourcetype=stream:http dest\_ip="192.168.250.70" form\_data=\* src\_ip=23.22.63.114

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

|dedup Password

|stats count

**Answer:** 412

**8. What was the average password length used in the password brute forcing attempt?**

**Answer guidance:** Round to closest whole integer. For example “5” not “5.23213”

We can answer this by using the eval, len, stats and round functions in Splunk.

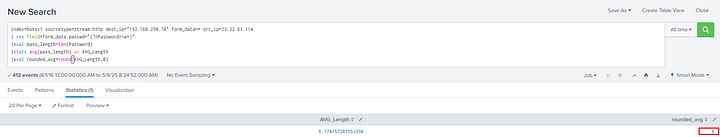
index=botsv1 sourcetype=stream:http dest\_ip="192.168.250.70" form\_data=\* src\_ip=23.22.63.114

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

|eval pass\_length=len(Password)

|stats avg(pass\_length) as AVG\_Length

|eval rounded\_avg=round(AVG\_Length,0)



**Answer:** 6

**9. One of the passwords in the brute force attack is James Brodsky’s favorite Coldplay song. We are looking for a six character word on this one. Which is it?**

This can be answered by using the lookup command in Splunk, but since there are not many results I just searched for the passwords which are 6 characters long.

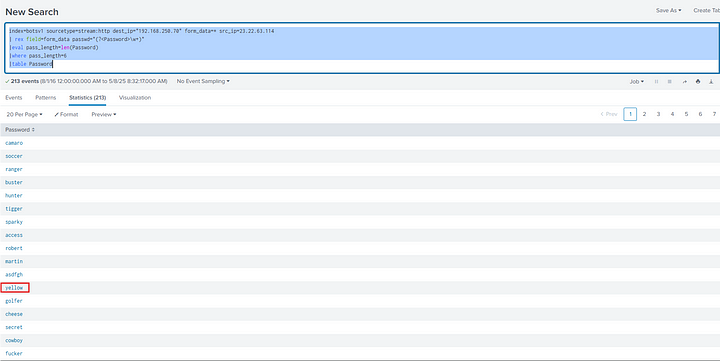
index=botsv1 sourcetype=stream:http dest\_ip="192.168.250.70" form\_data=\* src\_ip=23.22.63.114

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

|eval pass\_length=len(Password)

|where pass\_length=6

|table Password



And in the first page of the resuslts we can find the answer.

Using lookup

index=botsv1 sourcetype=stream:http dest\_ip="192.168.250.70" form\_data=\* src\_ip=23.22.63.114

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

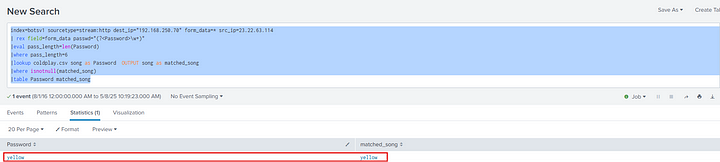
|eval pass\_length=len(Password)

|where pass\_length=6

|lookup coldplay.csv song as Password OUTPUT song as matched\_song

|where isnotnull(matched\_song)

|table Password matched\_song



**Answer:** Yellow

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

**Answer guidance:** Round to 2 decimal places.

Since we know that the password is batman, we can use the transaction command to find the answer.

index=botsv1 sourcetype=stream:http dest\_ip="192.168.250.70"

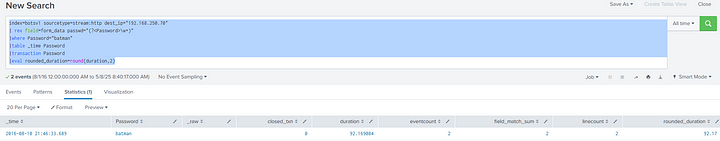
| rex field=form\_data passwd="(?<Password>\w+)"

|where Password="batman"

|table \_time Password

|transaction Password

|eval rounded\_duration=round(duration,2)



**Answer:** 92.17

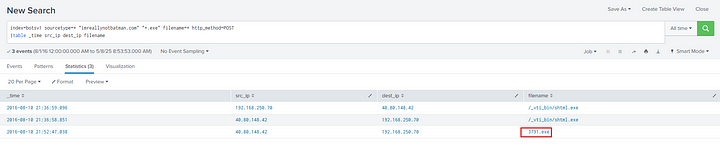
**11. What is the name of the executable uploaded by Po1s0n1vy?**

**Answer guidance: Please include file extension. (For example, “notepad.exe” or “favicon.ico”)**

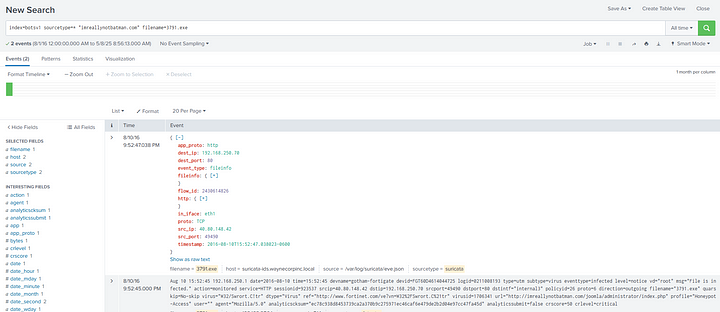
Lets look for any exe files that were uploaded from the above identified IP addresses.

index=botsv1 sourcetype=\* "imreallynotbatman.com" "\*.exe" filename=\* http\_method=POST

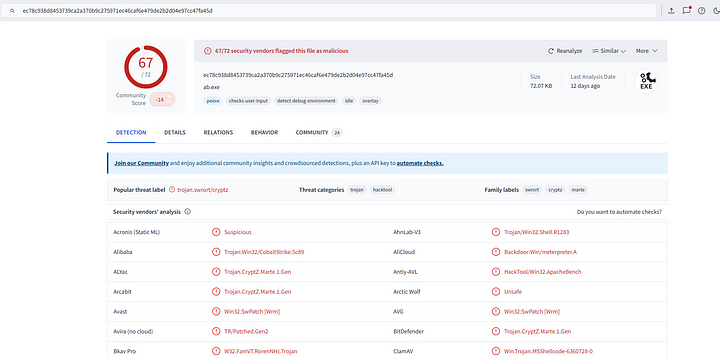
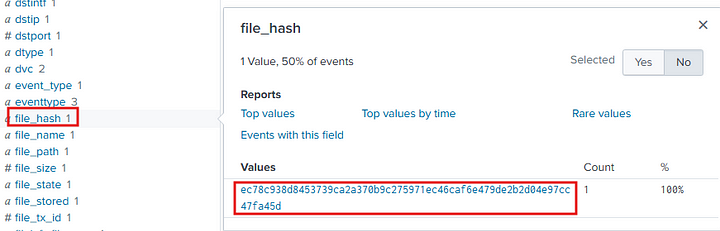
|table \_time src\_ip dest\_ip filename



Let us examine this 3791.exe file closely to find out if this is the actual malware executable we are looking for.



We got two events. In the interesting fields section we can see the file\_hash. Let us take this and upload it to VirusTotal.

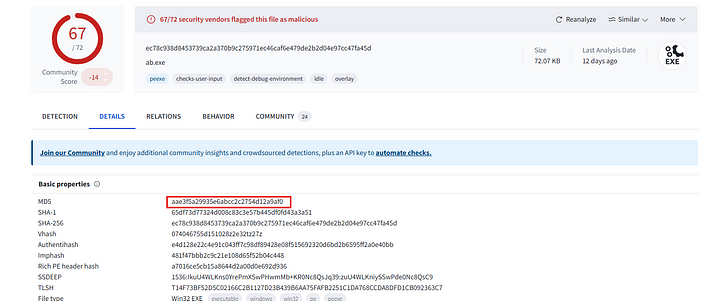


As we can see this is indeed a malicious file and this is the answer we are looking for.

**Answer:** 3791.exe

**12. What is the MD5 hash of the executable uploaded?**

In the VirusTotal details tab, we can find the MD5 hash of this file.

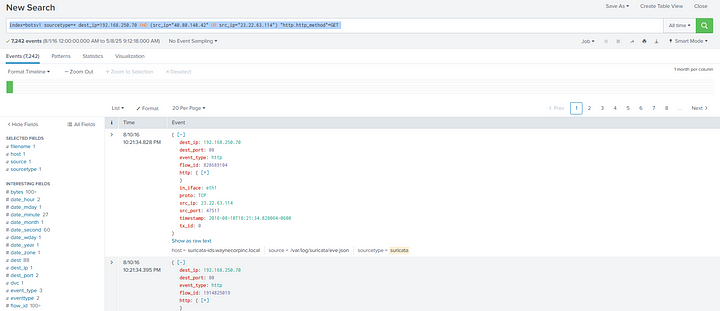


**Answer:** aae3f5a29935e6abcc2c2754d12a9af0

**13. What is the name of the file that defaced the imreallynotbatman.com website? Please submit only the name of the file with extension?**

Since we already looked at the POST requests, let us look at the GET requests to see if anything is suspicious. Also since the question metions the defacement of the website, the attacker probably uploaded an image to the website.

index=botsv1 sourcetype=\* dest\_ip=192.168.250.70 AND (src\_ip="40.80.148.42" OR src\_ip="23.22.63.114") "http.http\_method"=GET



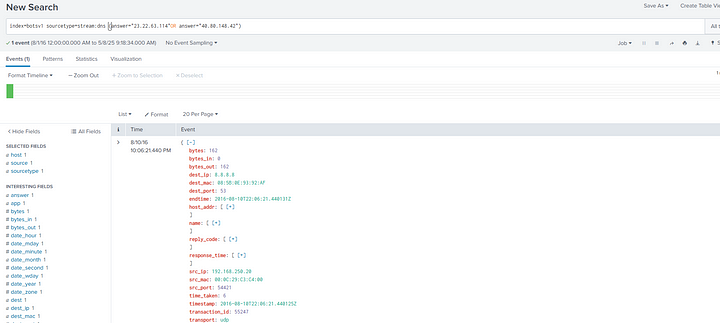
There are over 7000 events. Let us see for any files uploaded. There seems to be only one file that is poisonivy-is-coming-for-you-batman.jpeg. This should be our answer.

**Answer:** poisonivy-is-coming-for-you-batman.jpeg

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

We can check the DNS stream to find the answer to this question.

index=botsv1 sourcetype=stream:dns (answer="23.22.63.114"OR answer="40.80.148.42")



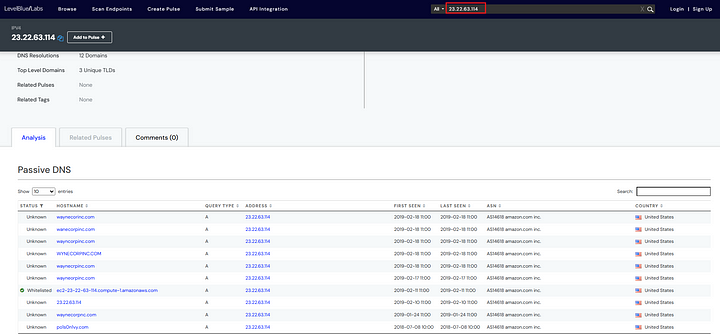
We got only one event, If we look at the name field in the interesting fields section, we can find the answer.



Answer: prankglassinebracket[.]jumpingcrab[.]com

**15. What IPv4 address has Po1s0n1vy tied to domains that are pre-staged to attack Wayne Enterprises?**

We have Identified two malicious IP addresses so far, so let us use open threat intelligence platforms to answer this question.

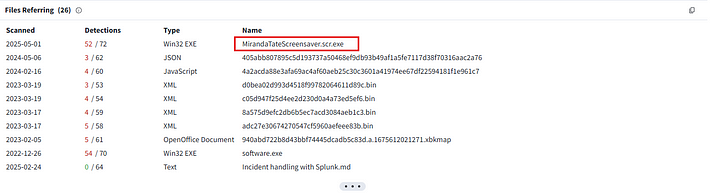


When we post the 23.22.63.114 IP address, we can see different typo squatted URL’s that are related to waynecorp.

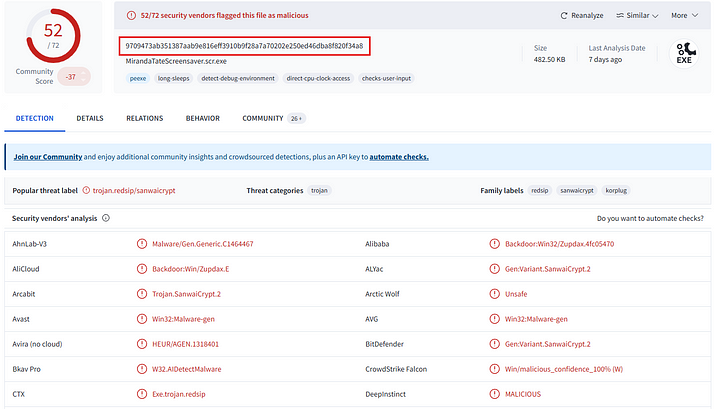
**Answer:** 23.22.63.114

**16. 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 Po1s0n1vys initial attack infrastructure. Using research techniques, provide the SHA256 hash of this malware.**

The hint states to look for the associated files for the above identified IP addresses. So Let us put the above IP address into VirusTotal and see for any associated files.



Click on the file to open the related VirusTotal page.



**Answer:** 9709473ab351387aab9e816eff3910b9f28a7a70202e250ed46dba8f820f34a8

**17. What special hex code is associated with the customized malware discussed in question 111?**

Since this will require static analysis, I checked the VirusTotal community section which had the answer

53 74 65 76 65 20 42 72 61 6e 74 27 73 20 42 65 61 72 64 20 69 73 20 61 20 70 6f 77 65 72 66 75 6c 20 74 68 69 6e 67 2e 20 46 69 6e 64 20 74 68 69 73 20 6d 65 73 73 61 67 65 20 61 6e 64 20 61 73 6b 20 68 69 6d 20 74 6f 20 62 75 79 20 79 6f 75 20 61 20 62 65 65 72 21 21 21

Which translates to

“Steve Brant’s Beard is a powerful thing. Find this message and ask him to buy you a beer!!!”

**Answer:** 53 74 65 76 65 20 42 72 61 6e 74 27 73 20 42 65 61 72 64 20 69 73 20 61 20 70 6f 77 65 72 66 75 6c 20 74 68 69 6e 67 2e 20 46 69 6e 64 20 74 68 69 73 20 6d 65 73 73 61 67 65 20 61 6e 64 20 61 73 6b 20 68 69 6d 20 74 6f 20 62 75 79 20 79 6f 75 20 61 20 62 65 65 72 21 21 21