Scenario (Learning Source: TryHackME)

A Big corporate organization **Wayne Enterprises** has recently faced a cyber-attack where the attackers broke into their network, found their way to their web server, and have successfully defaced their website http://www.imreallynotbatman.com. Their website is now showing the trademark of the attackers with the message **YOUR SITE HAS BEEN DEFACED** as shown below.

They have requested "**US**" to join them as a **Security Analyst** and help them investigate this cyber-attack and find the root cause and all the attackers' activities within their network.

The good thing is that they have Splunk already in place, so we have got all the event logs related to the attacker's activities captured. We need to explore the records and find how the attack got into their network and what actions they performed.

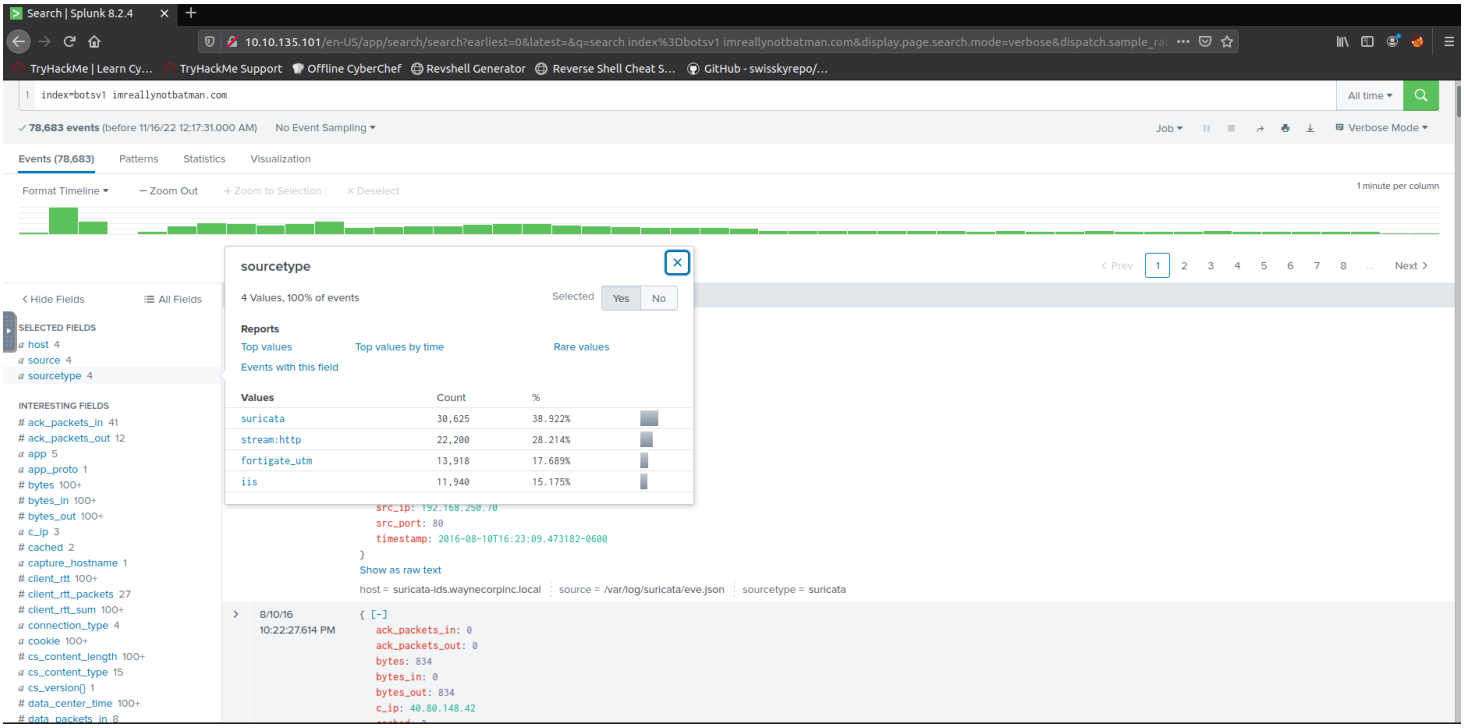
This Investigation comes under the Detection and Analysis phase.

+===+

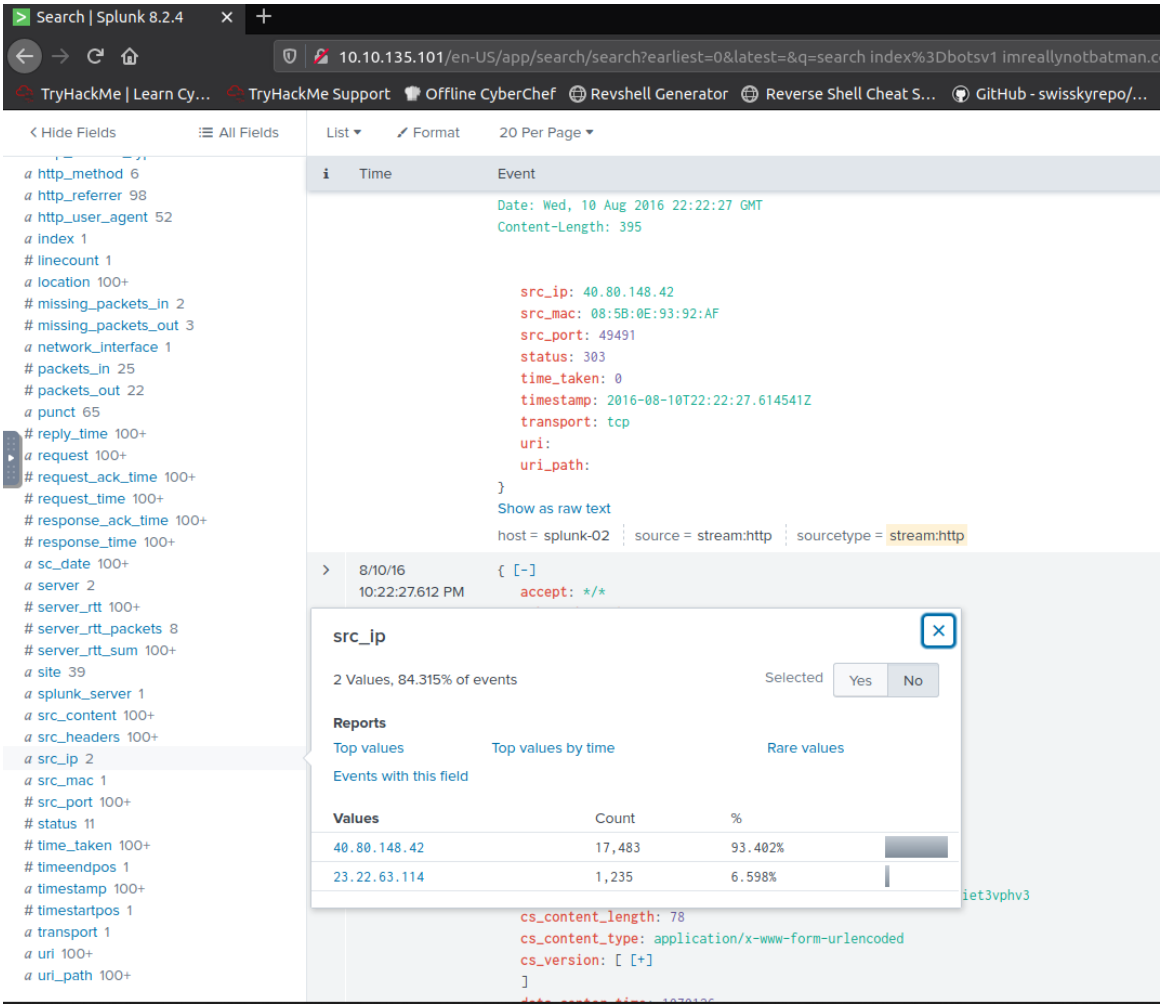
Cyber Kill Chain:

1. Reconnaissance Phase:

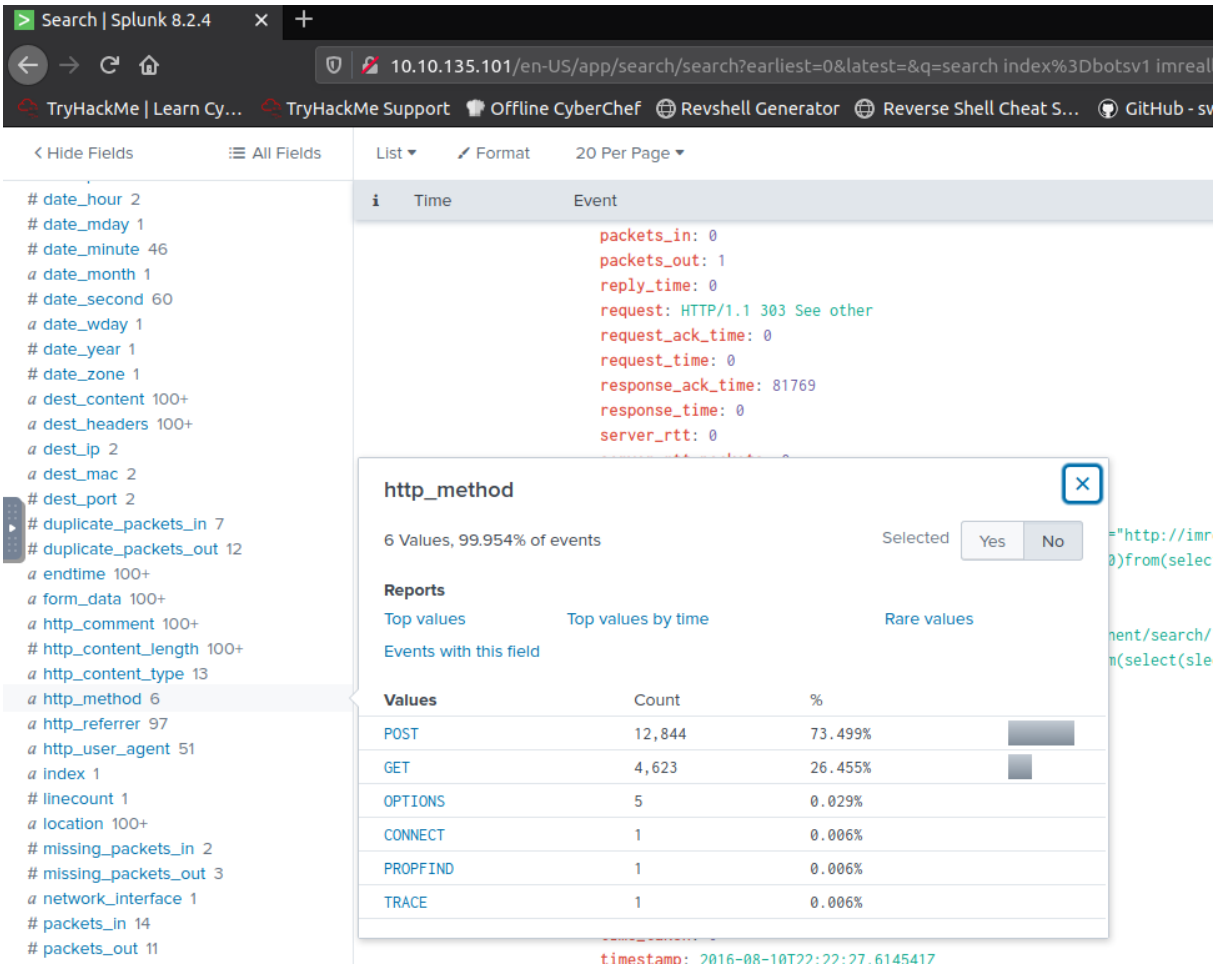
a. Start our analysis by examining any reconnaissance attempt against the webserver `mreallynotbatman.com`.

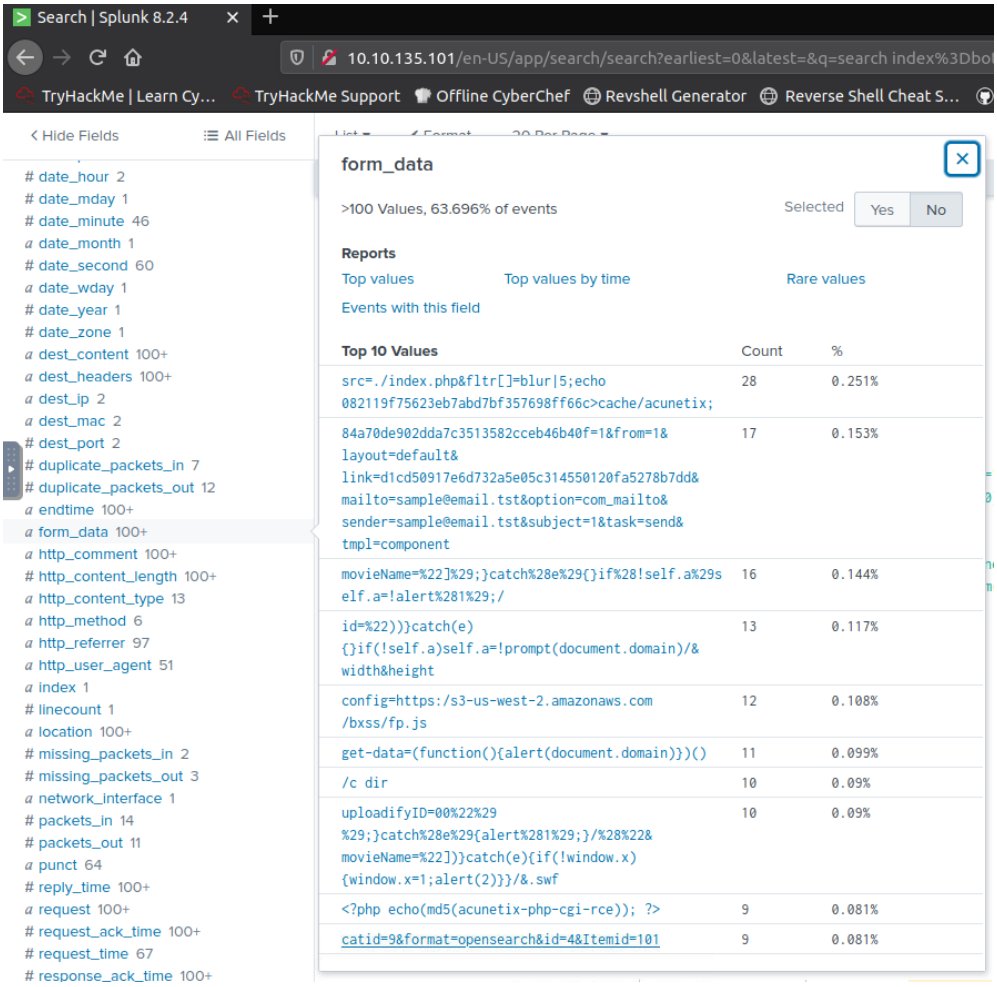


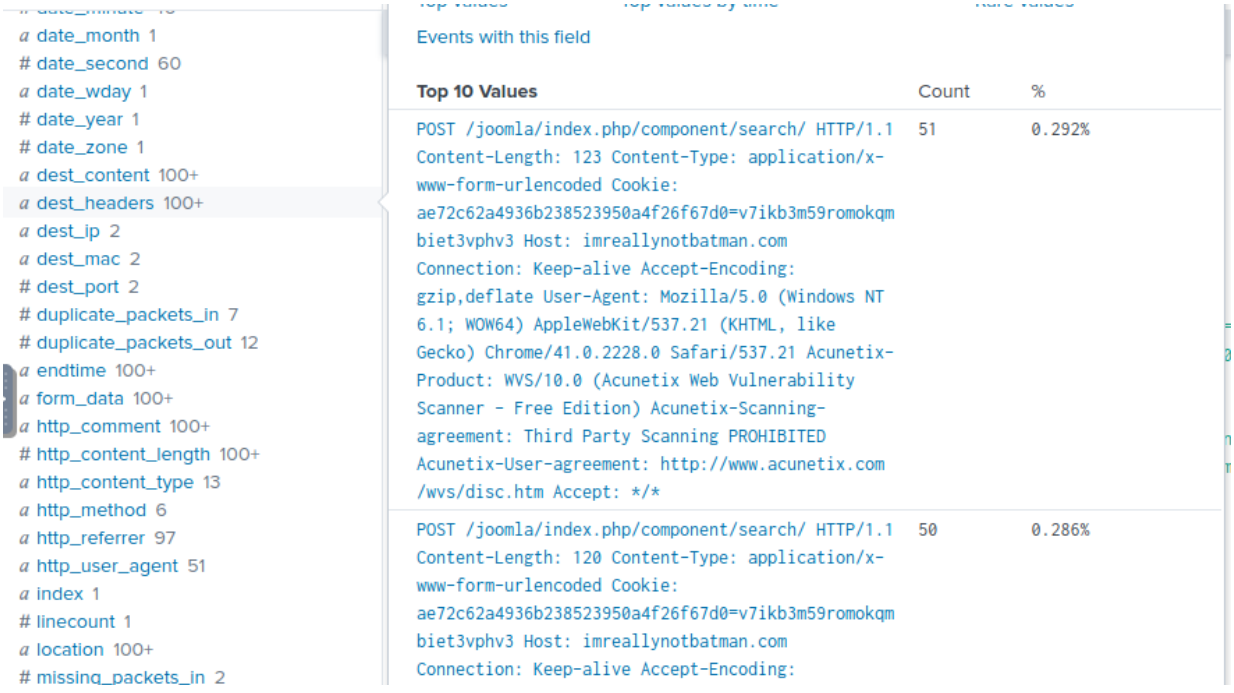
b. looking at the log source **stream:http,** and check the source_ip address



c. Checking on the first IP

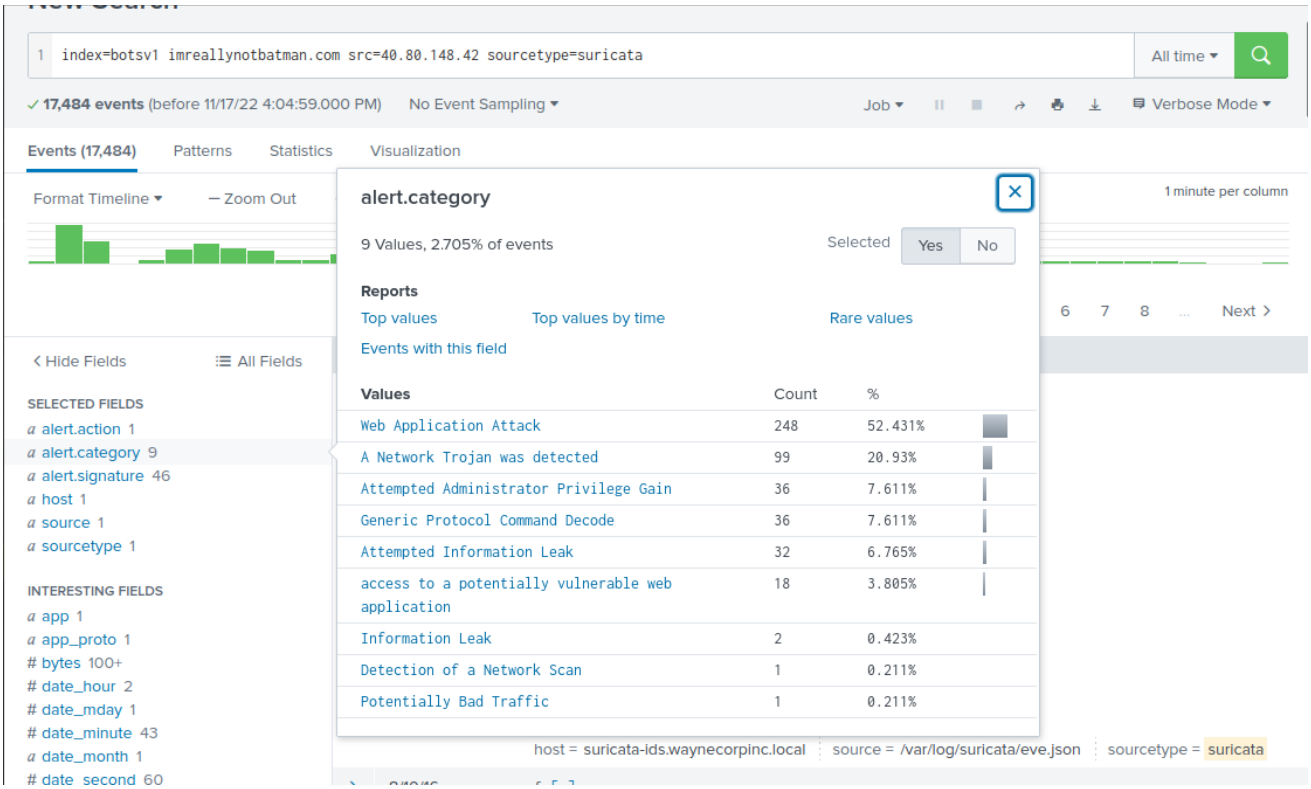

Search | Splunk 8.2.4
10.10.135.101/en-US/app/search/search?earliest=0&latest=&q=search index%3Dbotsv1 imreal
TryHackMe | Learn Cy...
TryHackMe Support
Offline CyberChef
Revshell Generator
Reverse Shell Cheat S...
GitHub - sv
Hide Fields
All Fields
List
Format
20 Per Page
Time
Event
date_hour 2
date_mday 1
date_minute 46
a date_month 1
date_second 60
a date_wday 1
date_year 1
date_zone 1
a dest_content 100+
a dest_headers 100+
a dest_ip 2
a dest_mac 2
dest_port 2
duplicate_packets_in 7
duplicate_packets_out 12
a endtime 100+
a form_data 100+
a http_comment 100+
http_content_length 100+
a http_content_type 13
a http_method 6
a http_referrer 97
a http_user_agent 51
a index 1
linecount 1
a location 100+
missing_packets_in 2
missing_packets_out 3
a network_interface 1
packets_in 14
packets_out 11
packets_in: 0
packets_out: 1
reply_time: 0
request: HTTP/1.1 303 See other
request_ack_time: 0
request_time: 0
response_ack_time: 81769
response_time: 0
server_rtt: 0
http_method
6 Values, 99.954% of events
Selected
Yes
No
Reports
Top values
Top values by time
Rare values
Events with this field
Values
Count
%
POST
12,844
73.499%
GET
4,623
26.455%
OPTIONS
5
0.029%
CONNECT
1
0.006%
PROPFIND
1
0.006%
TRACE
1
0.006%
timestamp: 2016-08-10T22:22:27.6145417

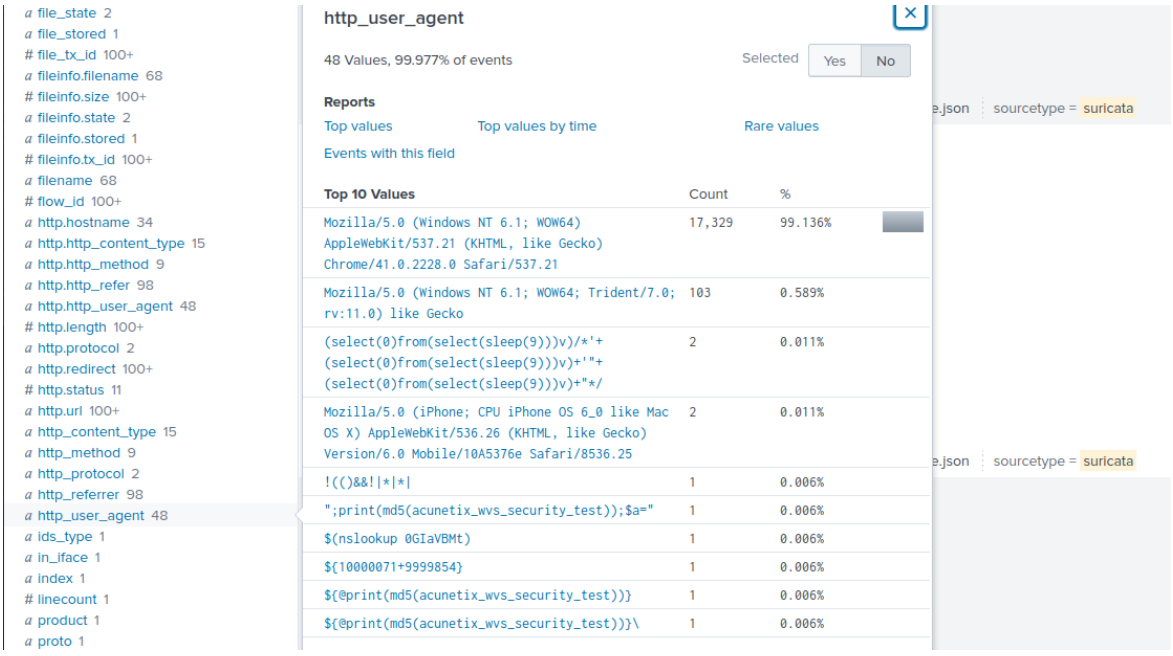


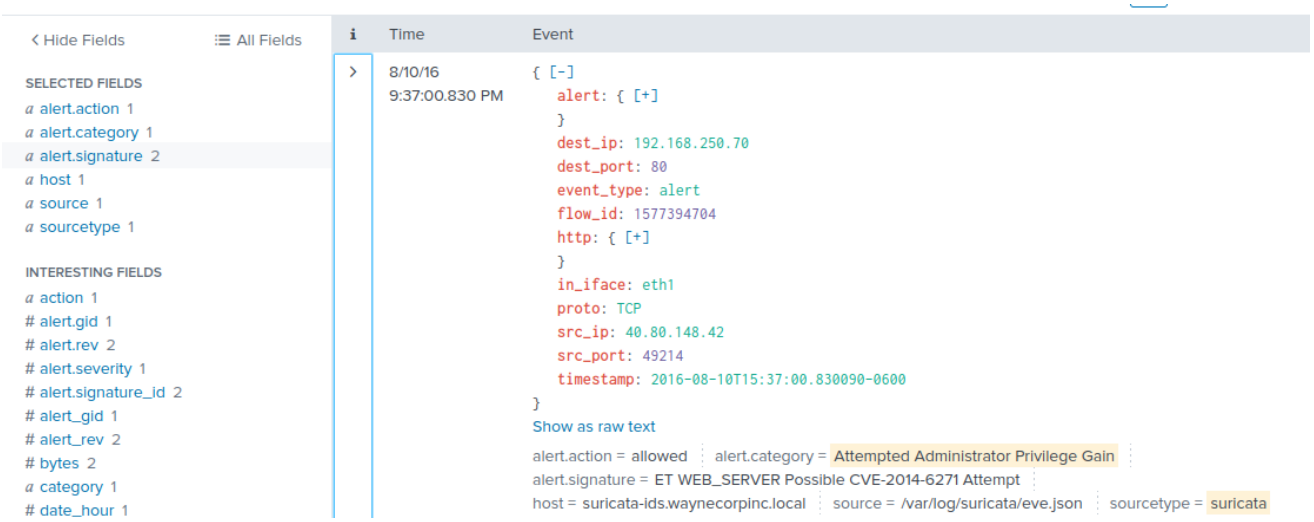


src_content: <head><title>Document Moved</title></head>
<body><h1>Object Moved</h1>This document may be found <a HREF="http://imreallynotbatman.com/joomla/index.php/component/search/?searchword=(select(0)from(select(sleep(3)))v)/*'%20(select(0)from(select(sleep(3)))v)%20'"%20(select(0)from(select(sleep(3)))v)%20"*/&ordering=newest&searchphrase=all&areas[0]=categories">here</body>
src_headers: HTTP/1.1 303 See other
Content-Type: text/html; charset=UTF-8
Location: http://imreallynotbatman.com/joomla/index.php/component/search/?searchword=(select(0)from(select(sleep(3)))v)/*'%20(select(0)from(select(sleep(3)))v)%20'"%20(select(0)from(select(sleep(3)))v)%20"*/&ordering=newest&searchphrase=all&areas[0]=categories
Server: Microsoft-IIS/8.5
X-Powered-By: PHP/5.5.38
Date: Wed, 10 Aug 2016 22:22:27 GMT
Content-Length: 395

d. Validate the scanning attempts and look into the Suricata logs

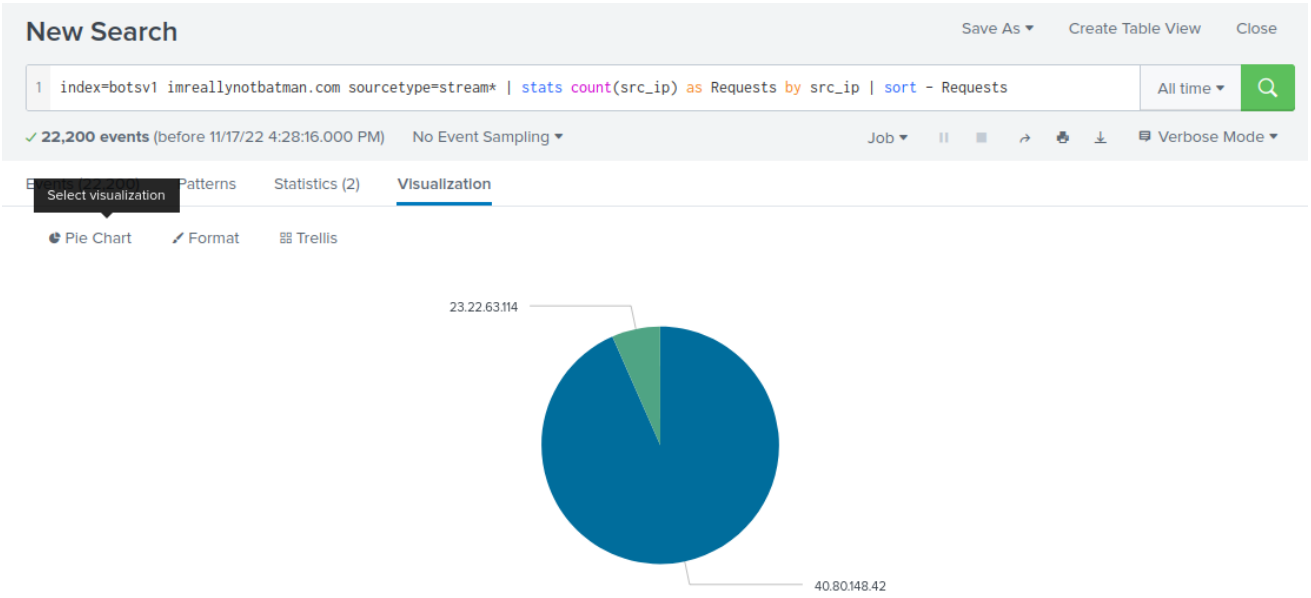






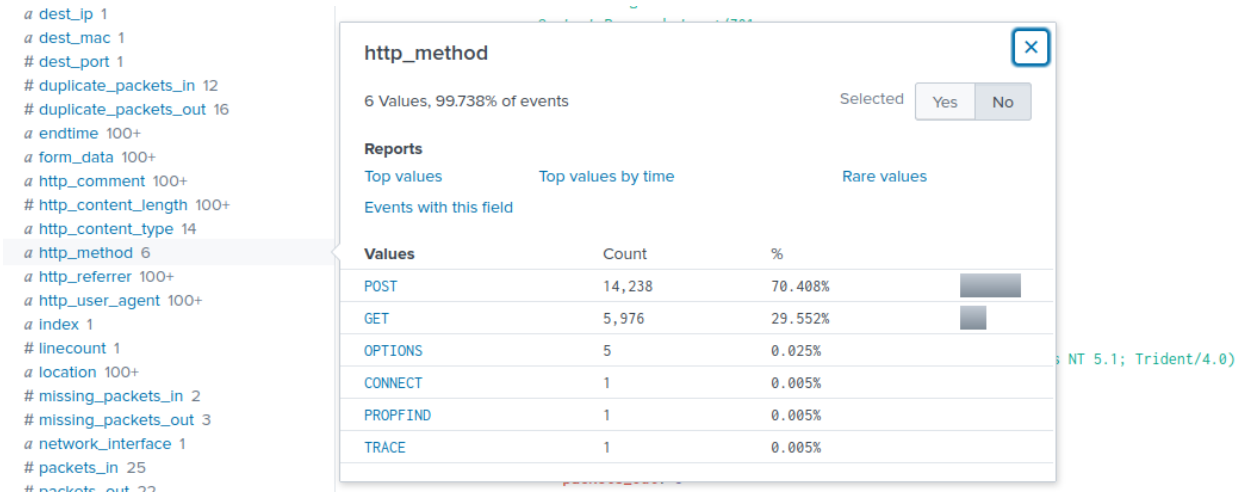
2. Exploitation Phase

a. see the number of counts by each source IP against the webserver.



b. show requests sent to our web server, which has the IP 192.168.250.70

c. We see most of the http traffic coming through the POST request



d. From reconnaissance part, we were able to determine that Joomla is used as the webservers as content management service and multiple attempts was done to login to the page or brute force by looking the form_data field in Splunk.

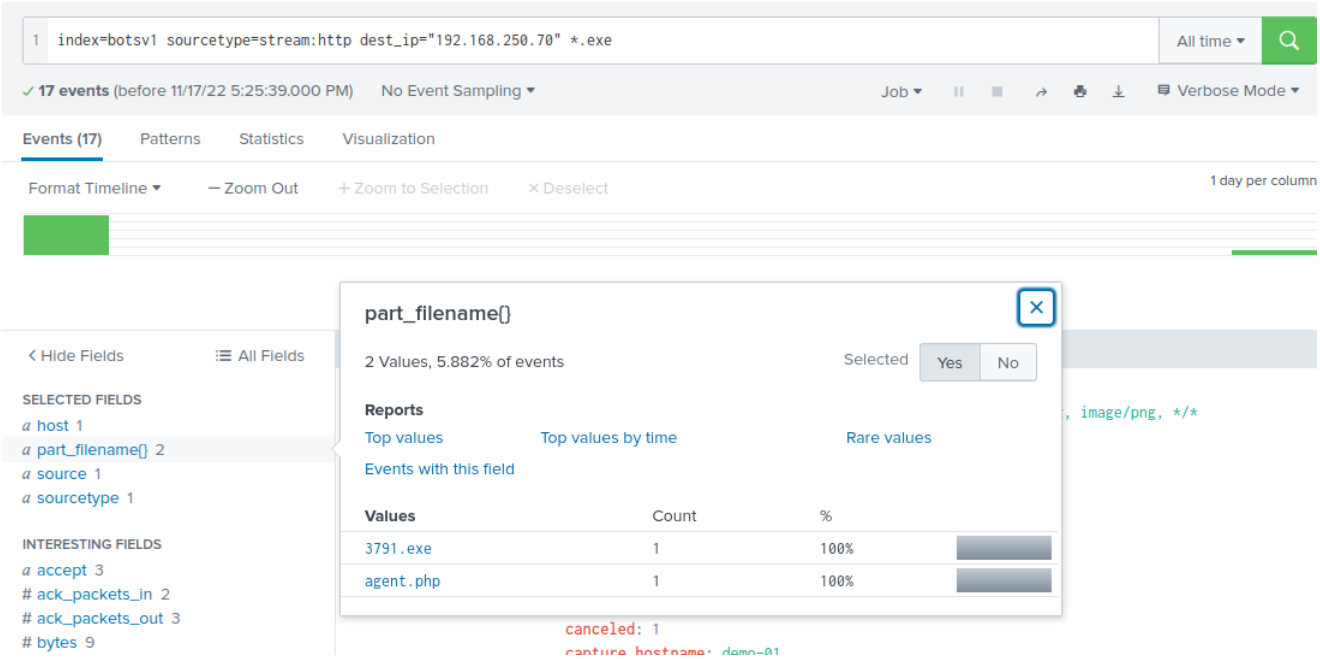
21:51:36.474	/index.php			sendWhat=both
2016-08-10 21:51:36.472	/joomla/administrator /index.php	40.80.148.42	192.168.250.70	action=chdir_event&dir=&option=com_extplorer
2016-08-10 21:48:05.858	/joomla/administrator /index.php	40.80.148.42	192.168.250.70	username=admin&passwd=batman&option=com_login&task=login& return=aW5kZXgucGhw&e5ec827a3f67ce0efc546d81f7356acc=1
2016-08-10 21:46:51.394	/joomla/administrator /index.php	23.22.63.114	192.168.250.70	username=admin&task=login&return=aW5kZXgucGhw&option=com_login& passwd=rock&4a40c518220c1993f0e02dc4712c5794=1
2016-08-10 21:46:51.156	/joomla/administrator /index.php	23.22.63.114	192.168.250.70	username=admin&task=login&return=aW5kZXgucGhw&option=com_login& passwd=sammy&0d3bb0020f70044ffba32f7d0fa7fa88=1
2016-08-10 21:46:51.154	/joomla/administrator /index.php	23.22.63.114	192.168.250.70	username=admin&task=login&return=aW5kZXgucGhw&option=com_login& passwd=cool&a09349d0d6bdbf078ad72cf8e9348583=1
2016-08-10 21:46:50.873	/joomla/administrator /index.php	23.22.63.114	192.168.250.70	username=admin&task=login&return=aW5kZXgucGhw&option=com_login& passwd=august&9800c58b682f234e562dee5972a58b8d=1
2016-08-10 21:46:50.640	/joomla/administrator /index.php	23.22.63.114	192.168.250.70	username=admin&task=login&return=aW5kZXgucGhw&option=com_login& passwd=baby&26a9247d113c378cdf06f31fa2154f2c=1
2016-08-10 21:46:50.637	/joomla/administrator /index.php	23.22.63.114	192.168.250.70	username=admin&task=login&return=aW5kZXgucGhw&option=com_login& passwd=dave&1b067a8762b4c8a9909ca68aae723e5a=1
2016-08-10 21:46:50.634	/joomla/administrator /index.php	23.22.63.114	192.168.250.70	username=admin&task=login&return=aW5kZXgucGhw&option=com_login& passwd=phantom&a083bf4d12c07976186d8a6efa6308cf=1

e. Using regex to extract the password and the source IP and user agent

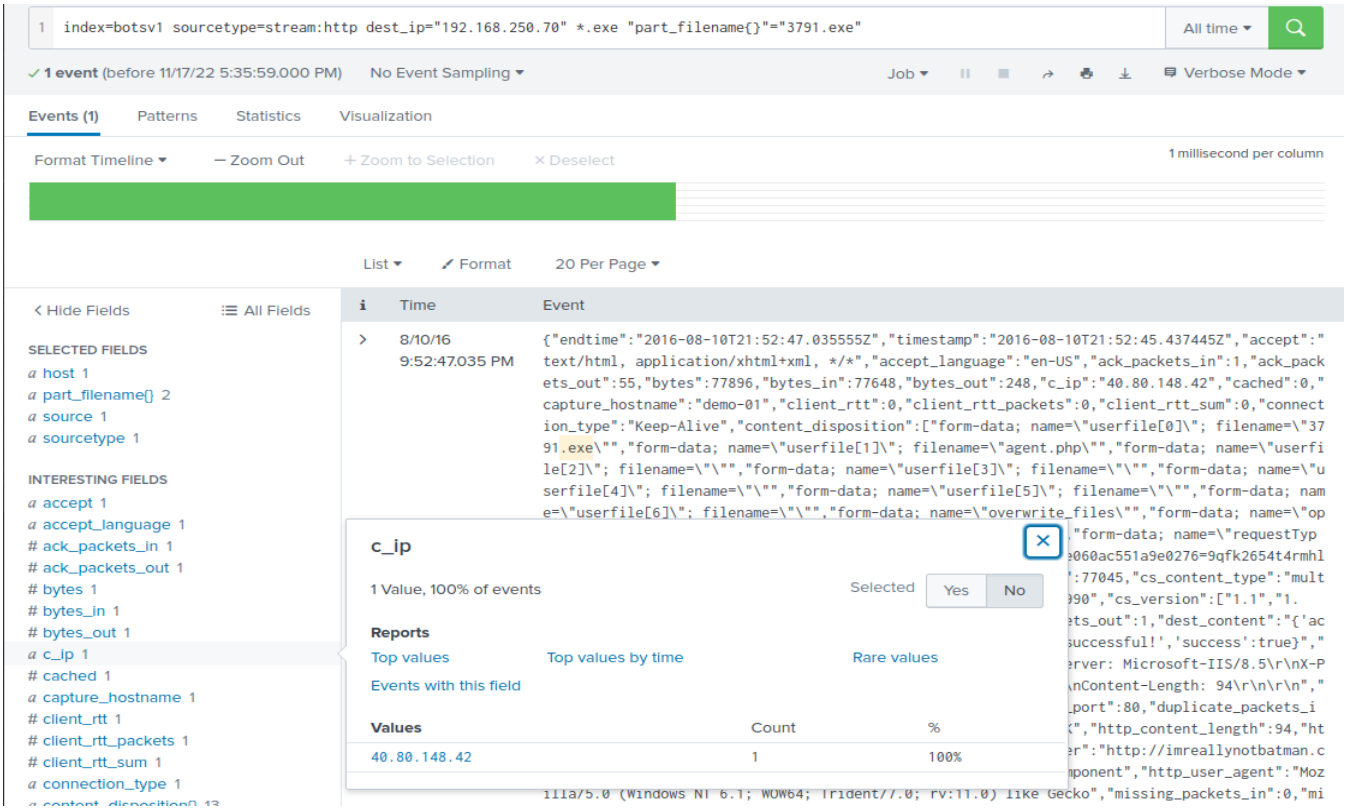
_time	src_ip	uri	http_user_agent	creds
2016-08-10 21:48:05.858	40.80.148.42	/joomla/administrator /index.php	Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko	batman
2016-08-10 21:46:51.394	23.22.63.114	/joomla/administrator /index.php	Python-urllib/2.7	rock
2016-08-10 21:46:51.156	23.22.63.114	/joomla/administrator /index.php	Python-urllib/2.7	sammy
2016-08-10 21:46:51.154	23.22.63.114	/joomla/administrator /index.php	Python-urllib/2.7	cool
2016-08-10 21:46:50.873	23.22.63.114	/joomla/administrator /index.php	Python-urllib/2.7	august
2016-08-10 21:46:50.640	23.22.63.114	/joomla/administrator /index.php	Python-urllib/2.7	baby
2016-08-10 21:46:50.637	23.22.63.114	/joomla/administrator /index.php	Python-urllib/2.7	dave
2016-08-10 21:46:50.634	23.22.63.114	/joomla/administrator /index.php	Python-urllib/2.7	phantom
2016-08-10 21:46:50.632	23.22.63.114	/joomla/administrator /index.php	Python-urllib/2.7	donald
2016-08-10 21:46:50.629	23.22.63.114	/joomla/administrator /index.php	Python-urllib/2.7	lifehack
2016-08-10 21:46:50.627	23.22.63.114	/joomla/administrator /index.php	Python-urllib/2.7	williams
2016-08-10 21:46:50.624	23.22.63.114	/joomla/administrator /index.php	Python-urllib/2.7	godzilla
2016-08-10 21:46:50.621	23.22.63.114	/joomla/administrator /index.php	Python-urllib/2.7	private

3. Installation Phase: we will investigate any payload / malicious program uploaded to the server from any attacker's IPs and installed them into the compromised server.

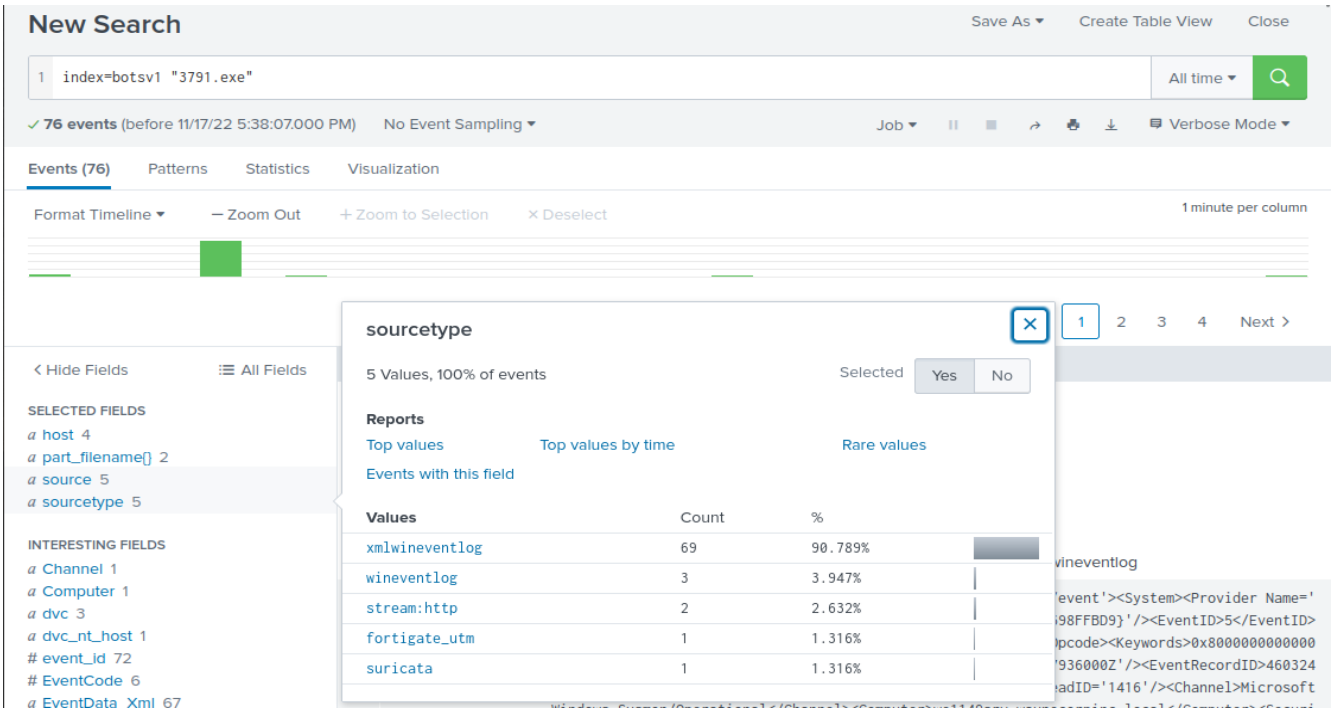
a. Looking for any .exe or executable files



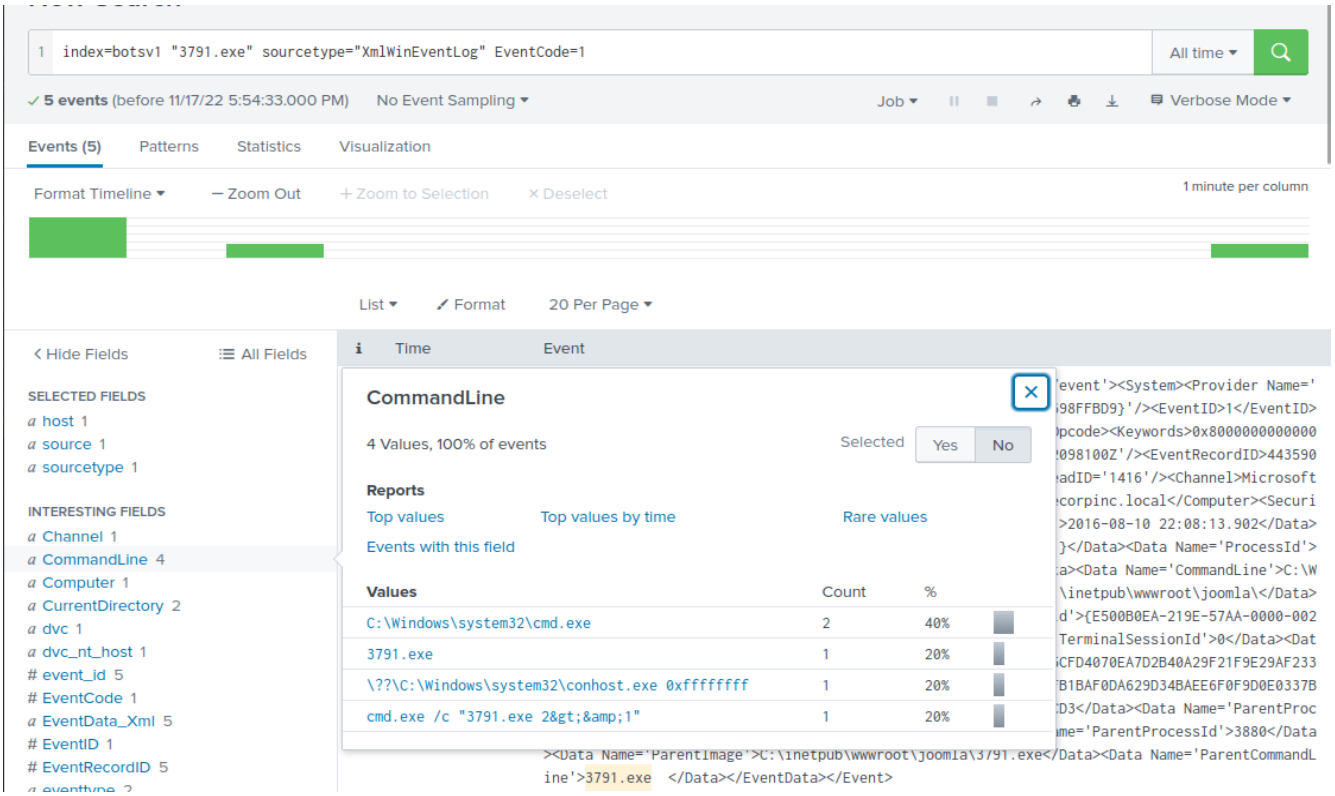
b. Clicking on the .exe file we can see the c_ip or the clients ip



c. Was this file executed in the webserver? To investigate more, we show the logs from host-centric log sources. Which includes Sysmon, WinEventLog, Fortigate_utm

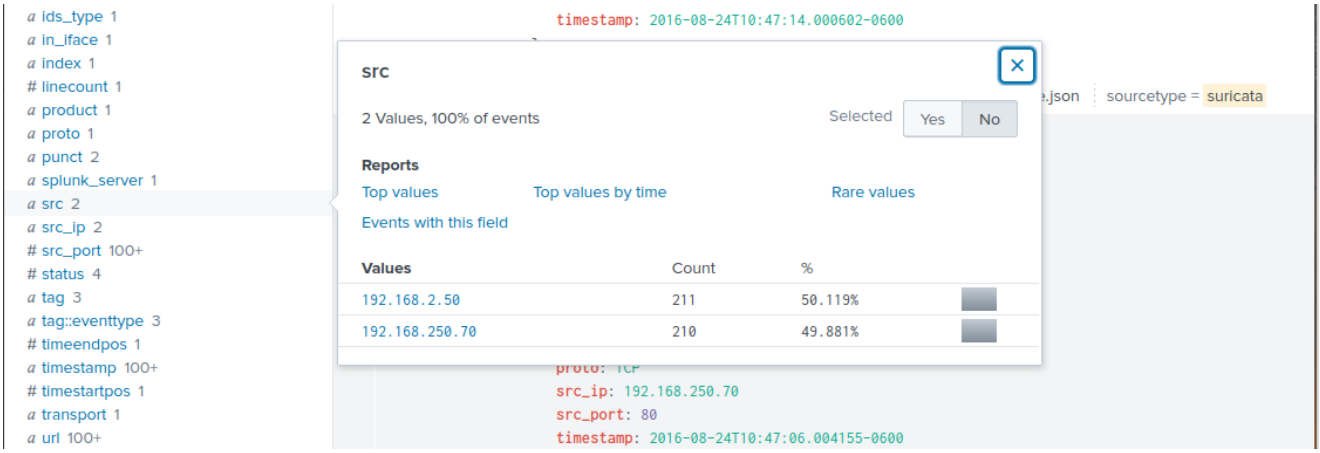


d. we can leverage sysmon and look at the EventCode=1 for program execution. By looking as sysmon logs we can say that it used cmd to execute this executable in the server.

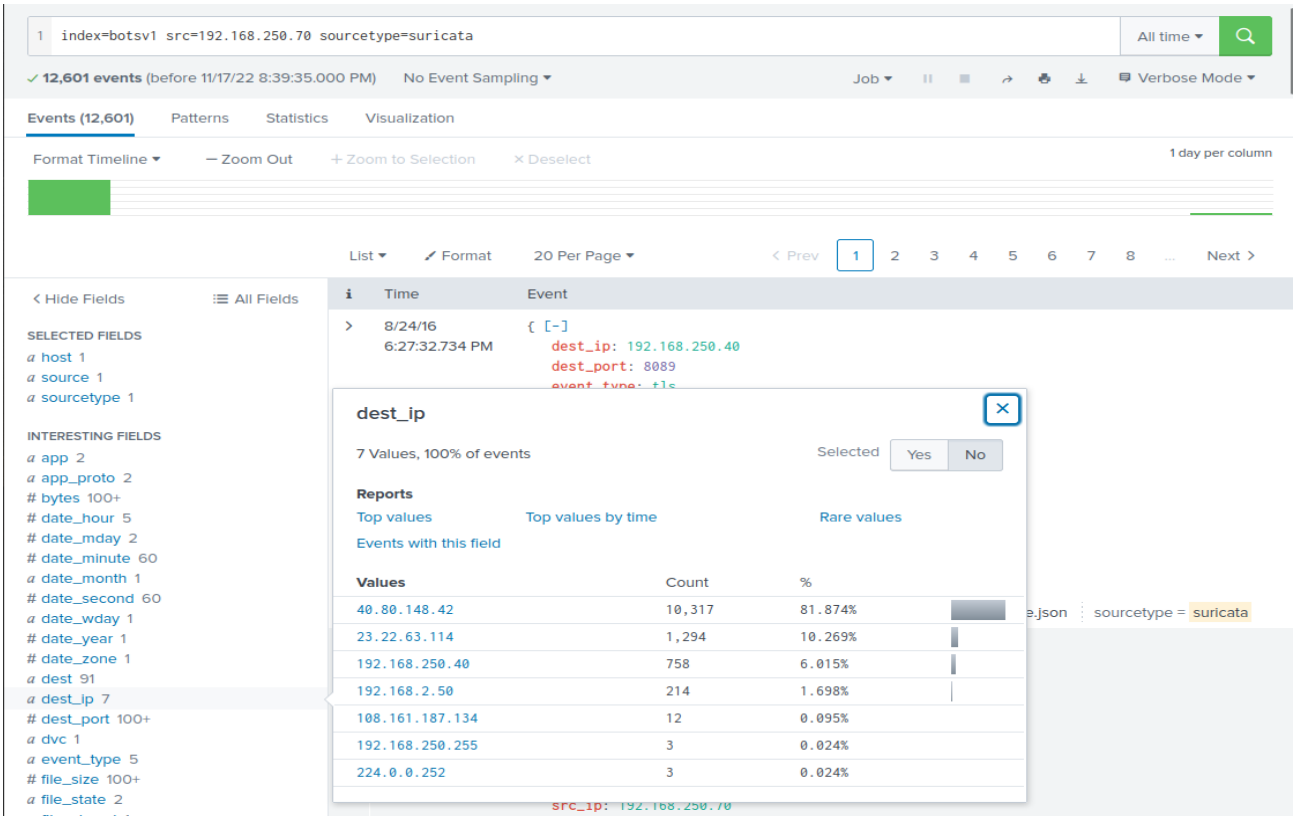


4. **Action on Objectives:** "As the website was defaced due to a successful attack by the adversary, it would be helpful to understand better what ended up on the website that caused defacement."

a. start our investigation by examining the Suricata log source and the IP addresses communicating with the webserver 192.168.250.70. However, there is no external IP that communicates with the server.

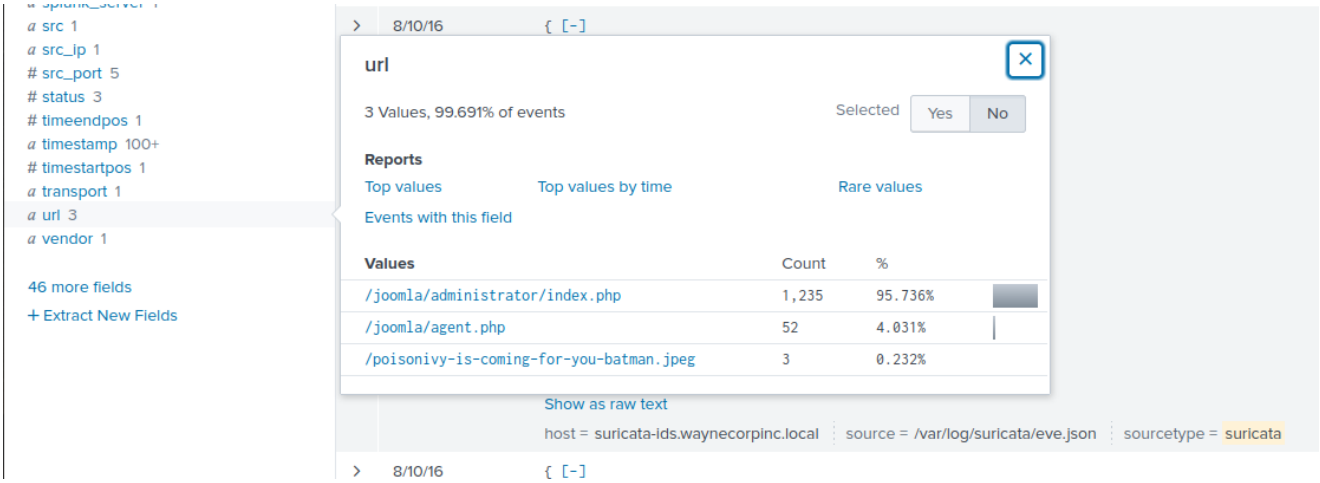


b. So, Let's see if any communicates originates from the server.

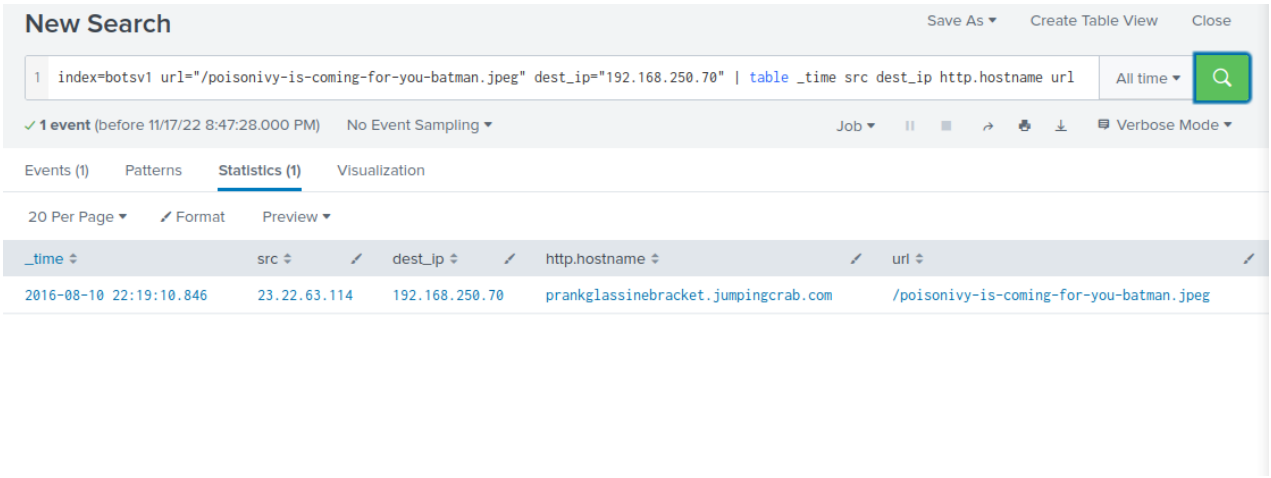


c. We'll pivote into the des_ip to see what traffice is carried out.

Des_IP: 23.22.63.114

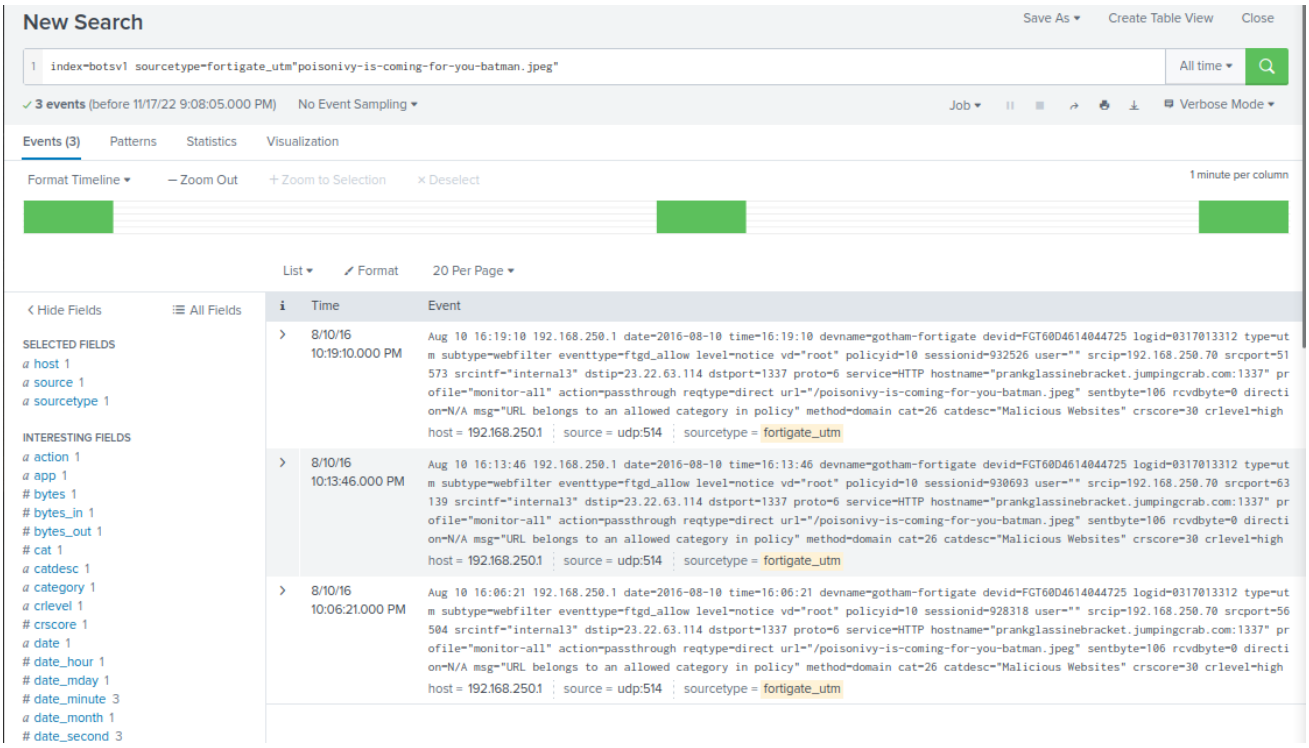


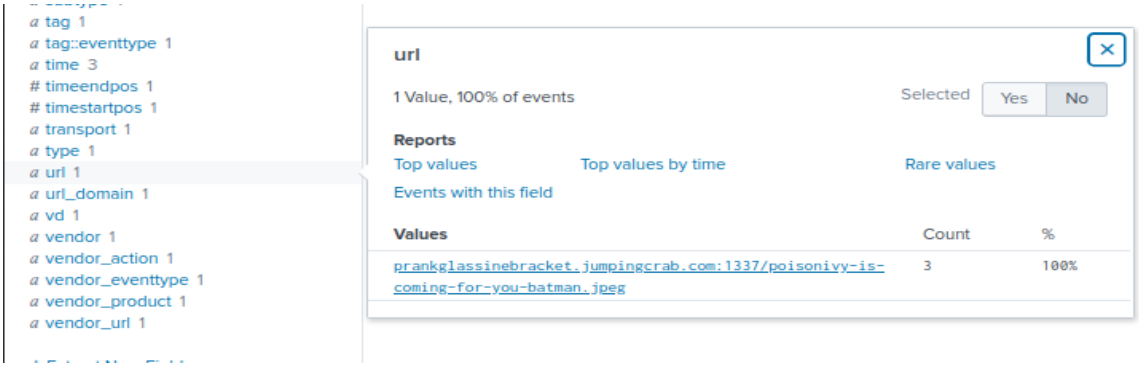
d. There is a jpeg file and let's see where it came from. It's clearly shows that it was most likely was downloaded from an attacker's host that defaced the site.



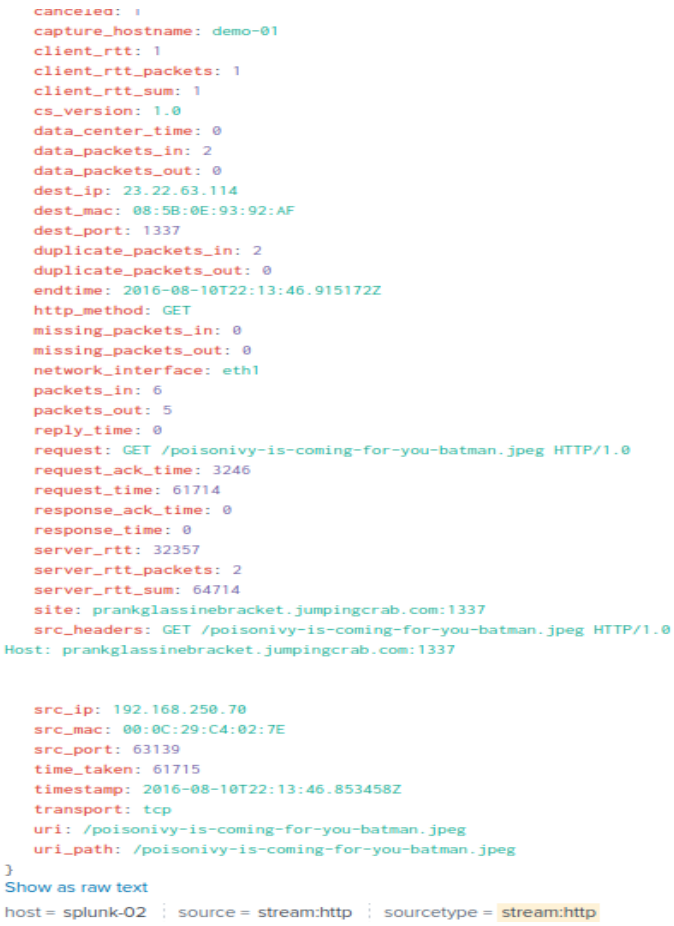
5. Command and control phase: "The attacker uploaded the file to the server before defacing it. While doing so, the attacker used a Dynamic DNS to resolve a malicious IP. Our objective would be to find the IP that the attacker decided the DNS."

a. We'll look at the Fortinet firewall or fortigate_utm firewall, and looking at the url field we see the FQDN of the attacker's host.



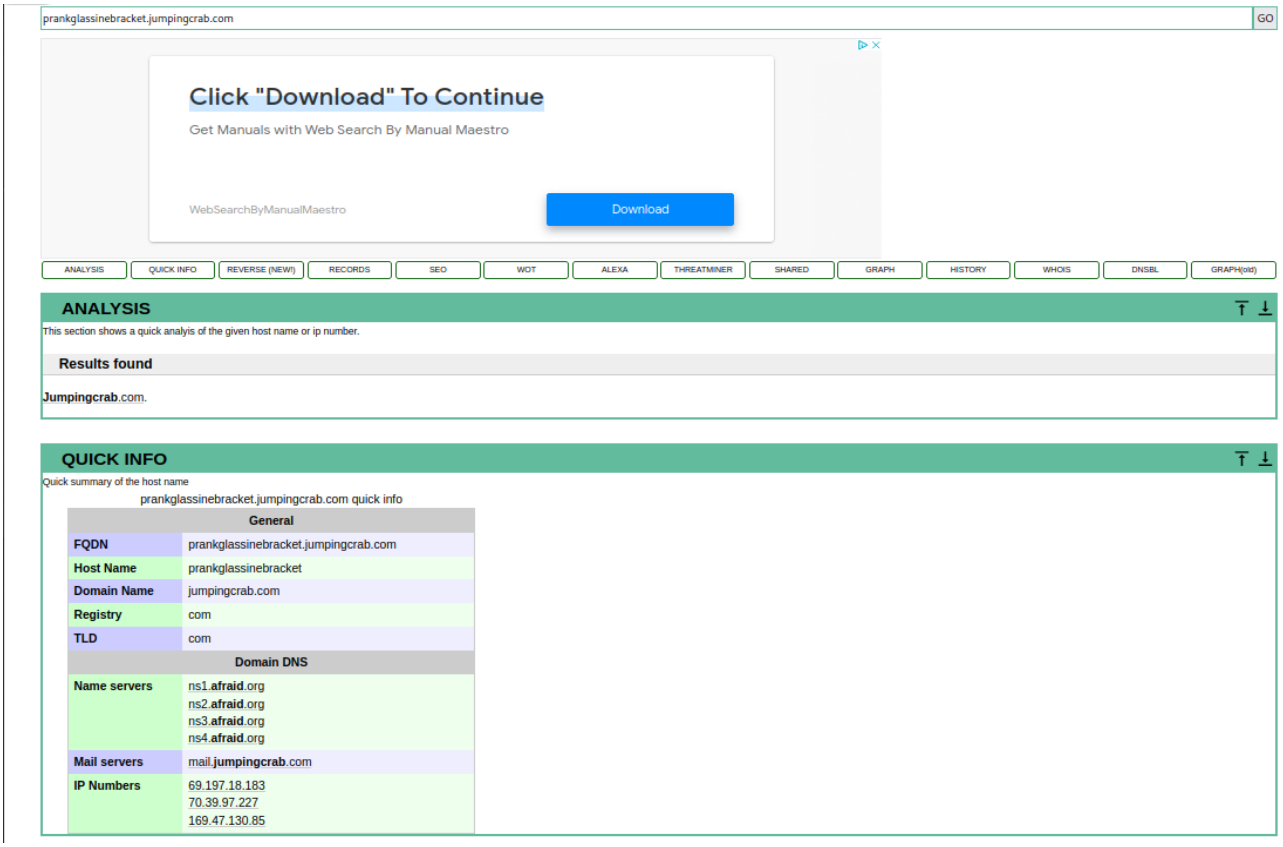


b. Let us verify by looking at another source. By looking at stream:http we see suspicious domain as C2 server (also can look at stream:dns)

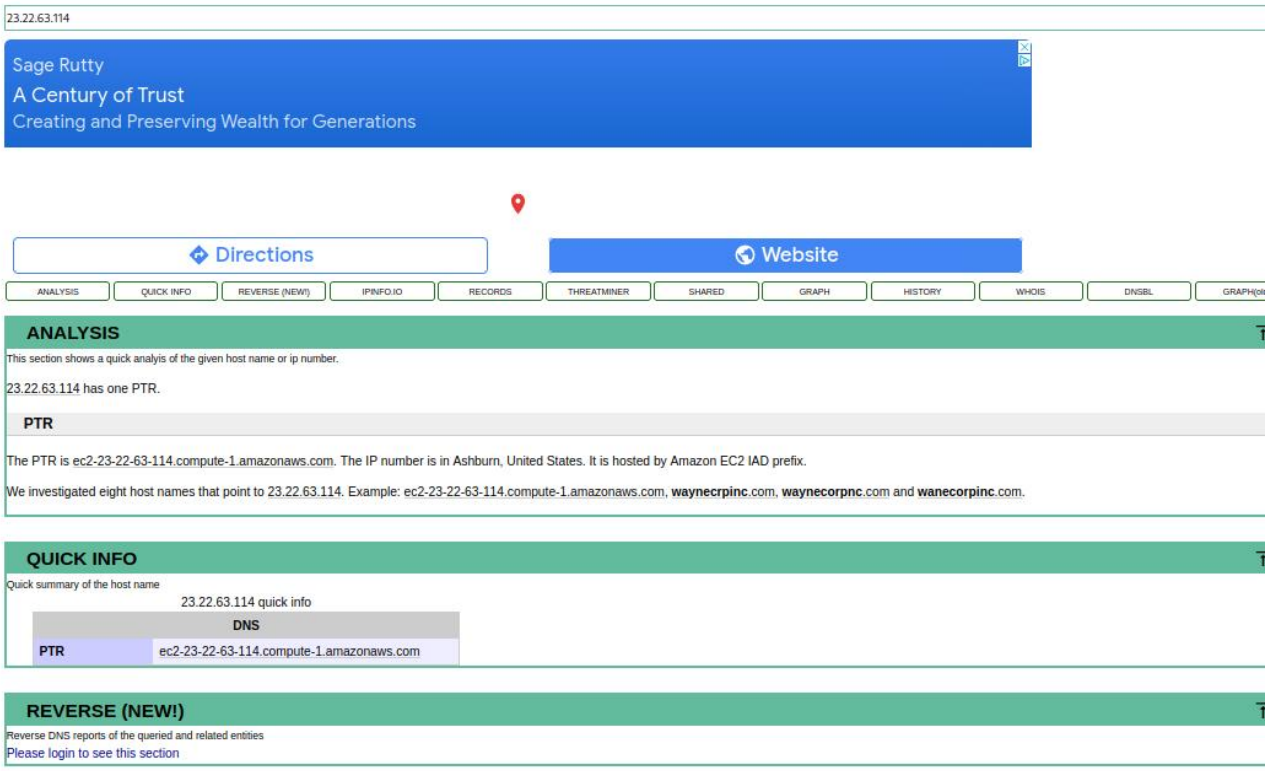


6. **Weaponization Phase:** So far, we have found a domain prankglassinebracket.jumpingcrab.com associated with this attack. Our first task would be to find the IP address tied to the domains that may potentially be pre-staged to attack Wayne Enterprise. In the following exercise, we will be searching the online Threat Intel sites for any information like IP addresses/domains / Email addresses associated with this domain which could help us know more about this adversary.

a. Using Robtex we will find the IP address associated with the domain name prankglassinebracket.jumpingcrab.com



b. Next, we will search for the IP 23.22.63.114 on this website.



RECORDS

Hierarchical analysis of the entity

23.22.63.114

whois	Amazon.com, Inc. (AMAZO-4)
route	23.22.0.0/15
bgp	AS14618
asname	Amazon-AES-IAD Amazon-AES-IAD
descr	Amazon EC2 IAD prefix
location	Ashburn, United States
ptr	ec2-23-22-63-114.compute-1.amazonaws.com
a	23.22.63.114

THREATMINER

Threat information such as virus etc

Source: Threatminer

SHARED

This section shows related hostnames and ipnumbers

Using as IP number

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

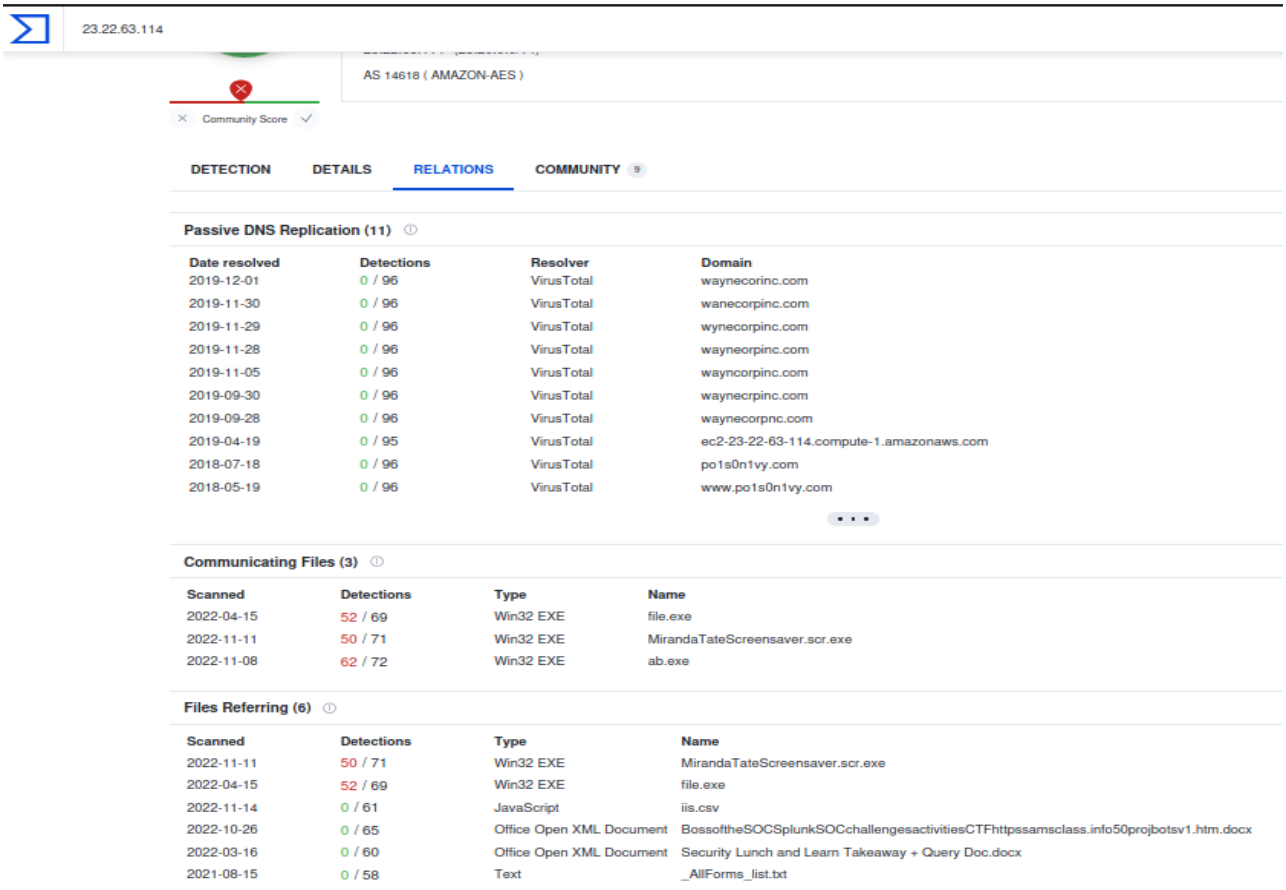
8 results shown.

IP numbers used in conjunction

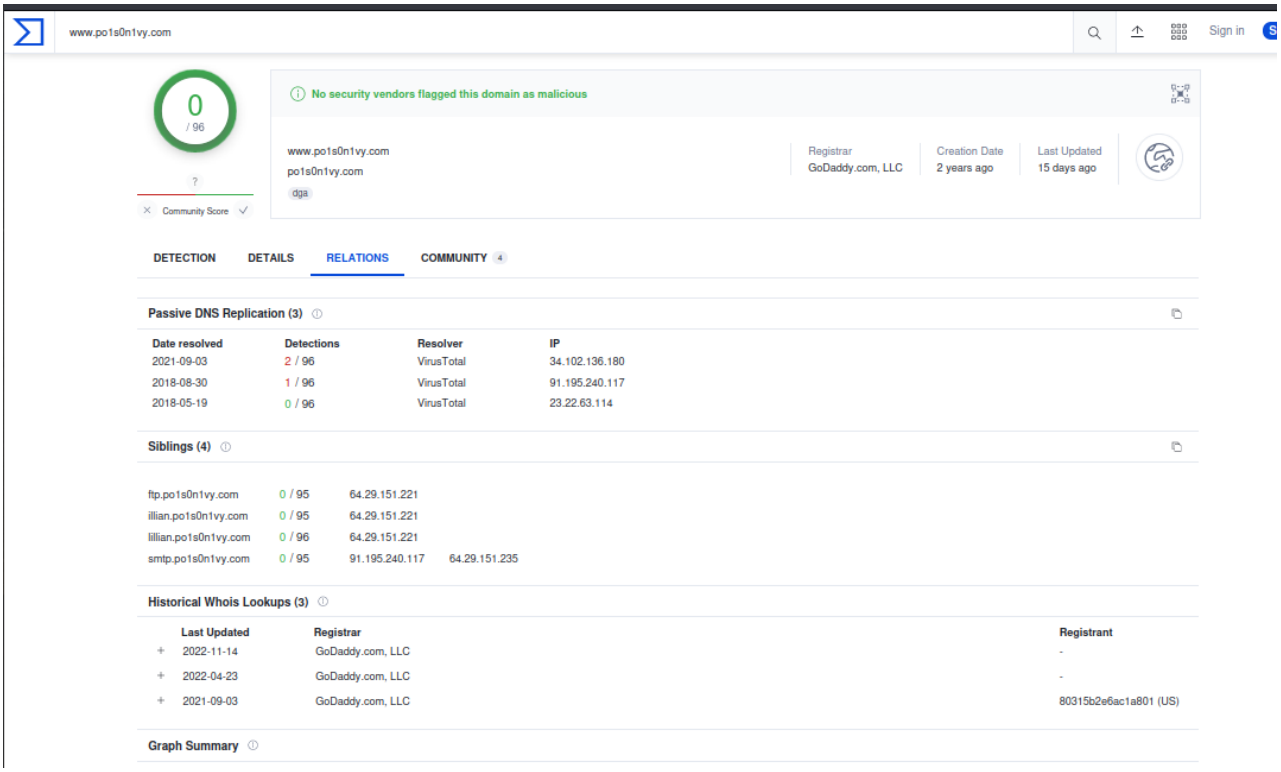
162.255.119.248

1 results shown.

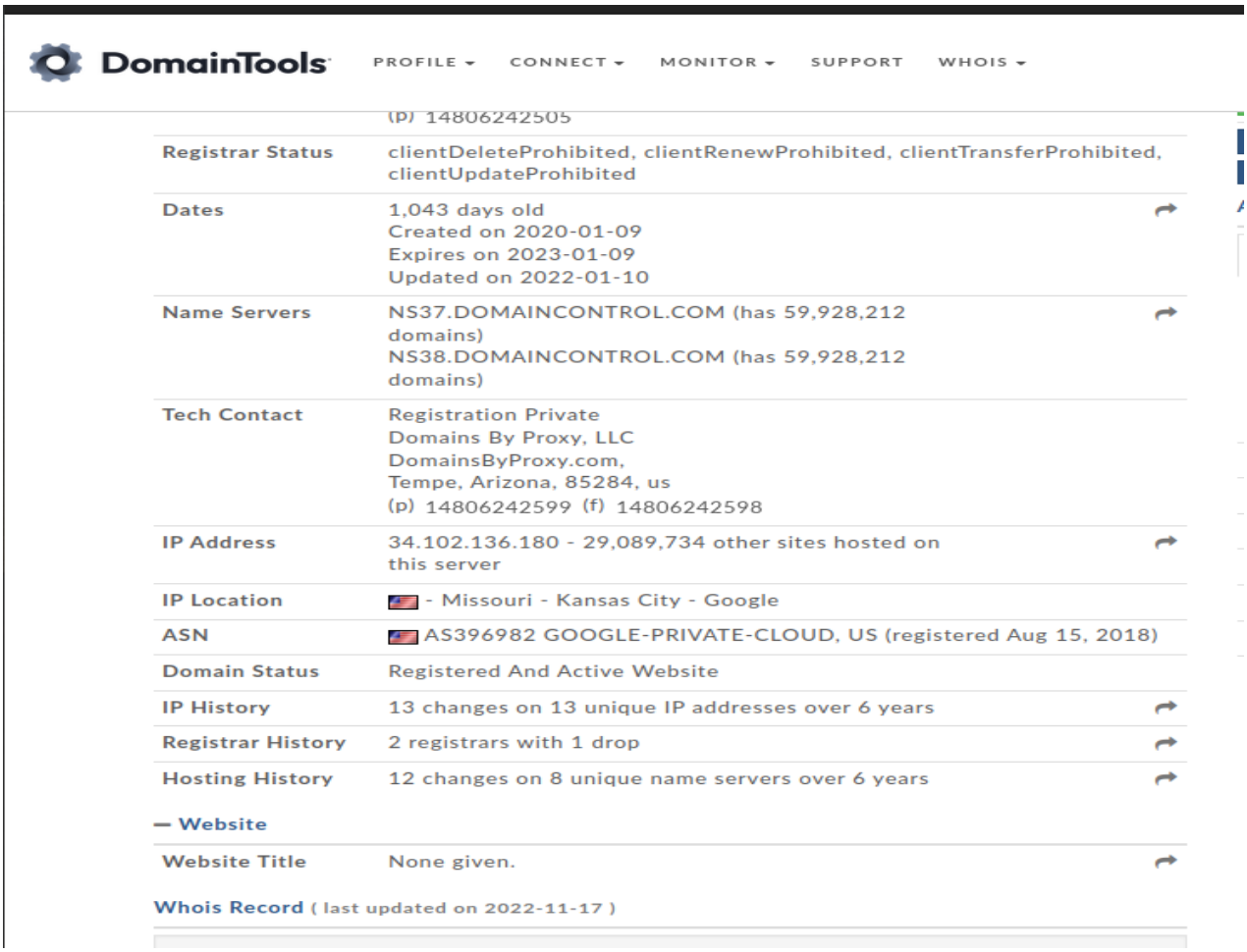
c. Using Virustotal lets investigate IP more.



d. Lets investigate the po1s0nivy.com

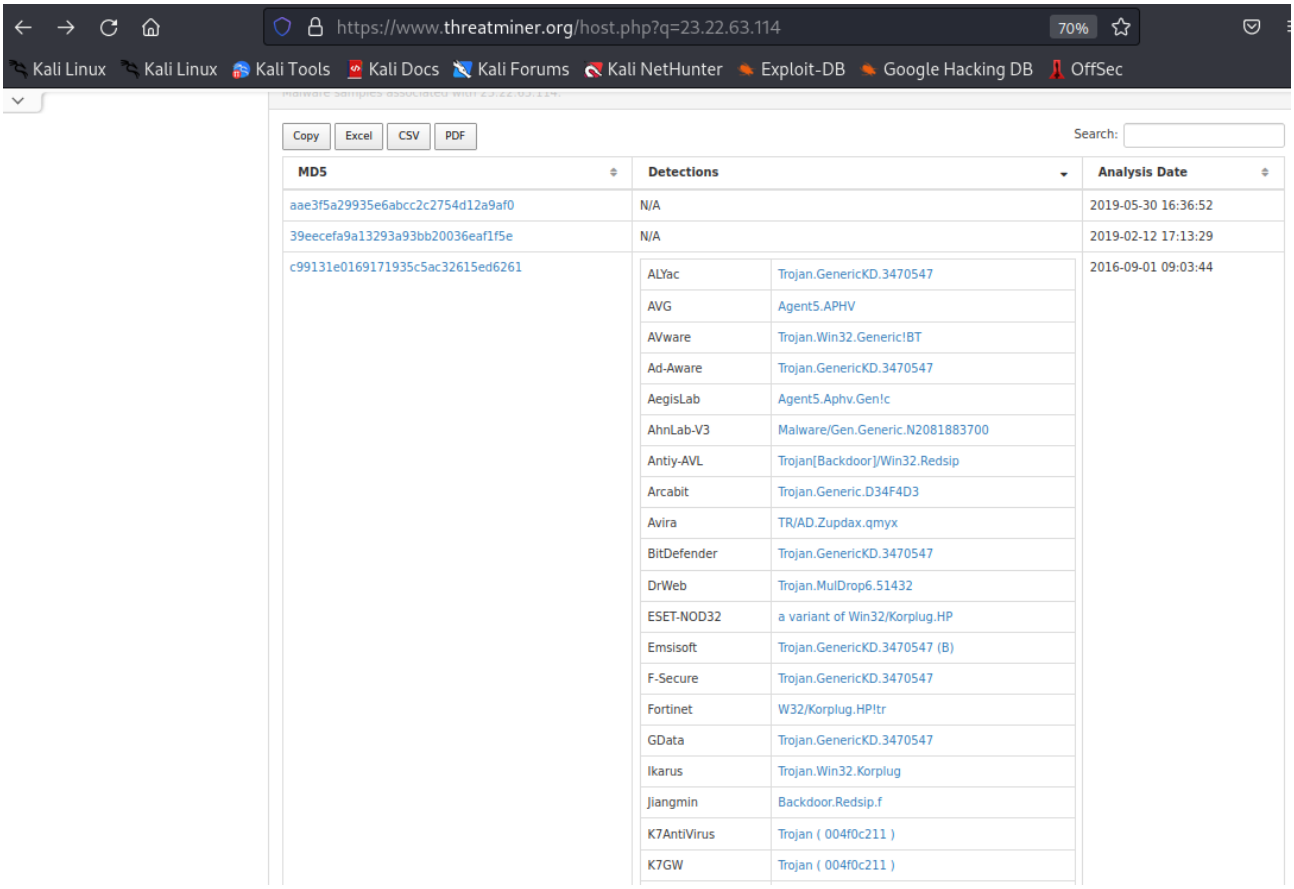


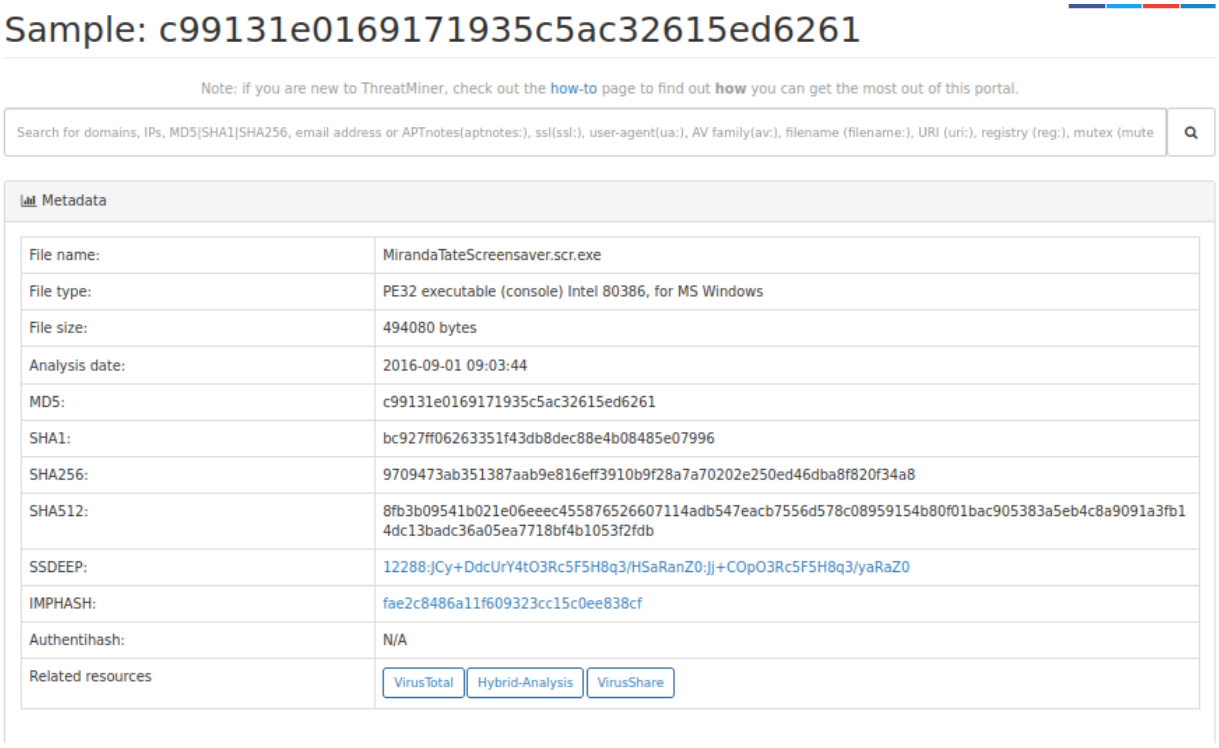
e. Lets Use whois.domaintools.com to investigate the po1s0nivy.com. We can see the name servers and IP addresses associated with the domain name.



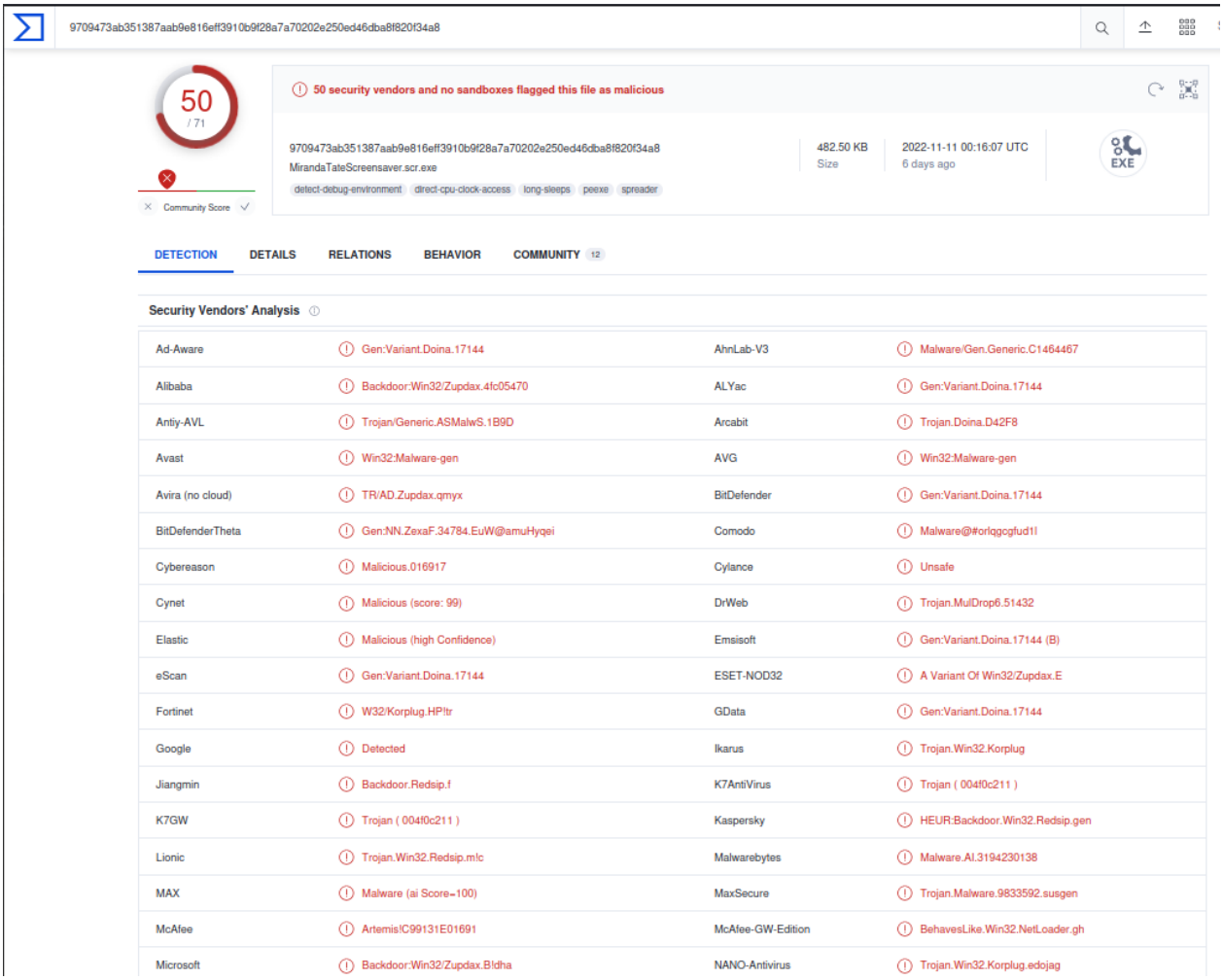
7. **Deliverable Phase: "**Threat Intel report suggested that this adversary group Poison Ivy appears to have a secondary attack vector in case the initial compromise fails. Our objective would be to understand more about the attacker and their methodology and correlate the information found in the logs with various threat Intel sources."

a. Lets use ThreatMiner to investigate the IP 23.22.63.114. Found the third file to be malicious

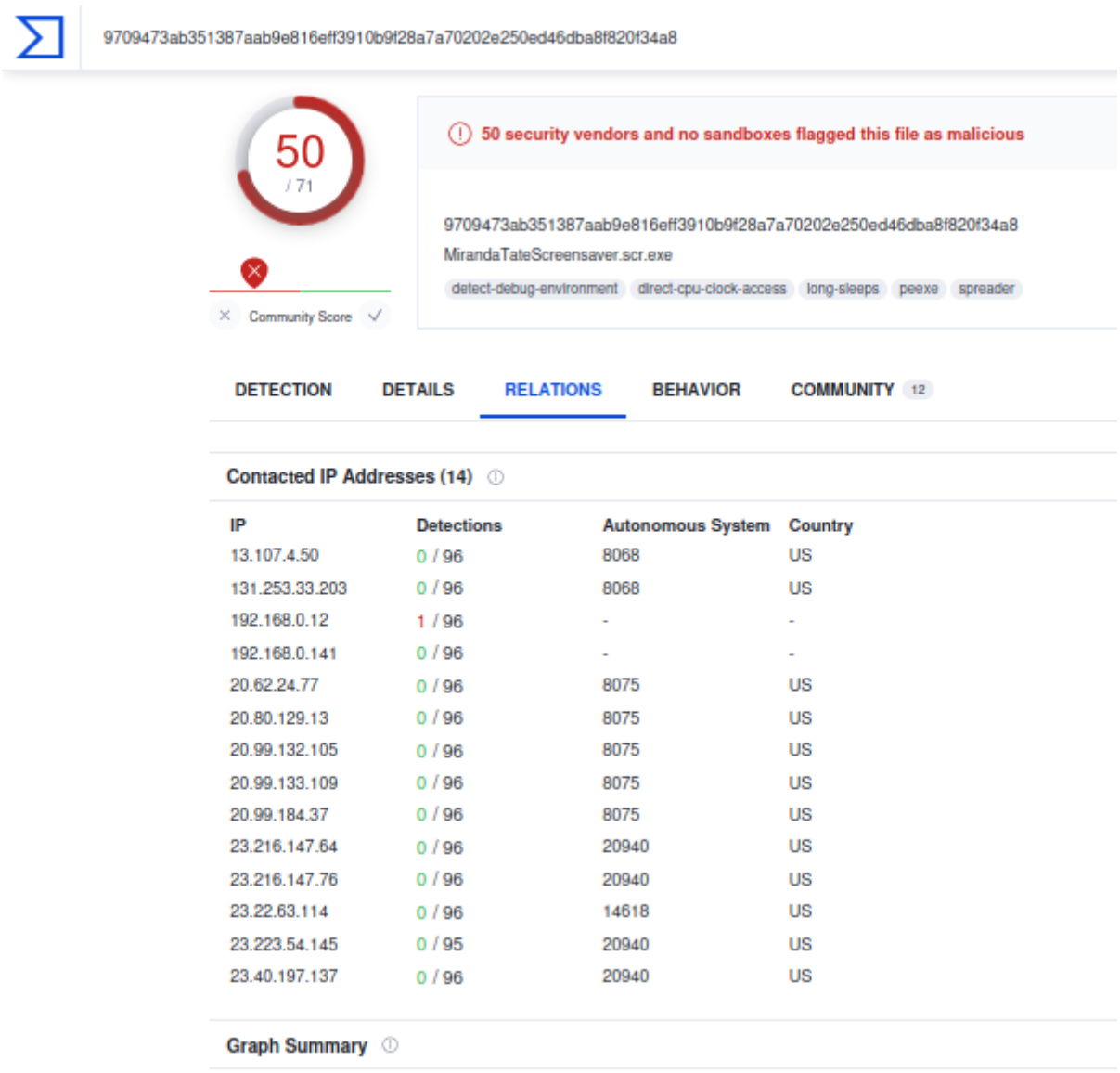




b. Lets use the SHA256 hash of the file to investigate it in VirusToal, and see that it's called MirandaTateScreensaver.scr.exe



c. We can also see the IP address as one of the IPs for to grab this file from



d. Using Hybrid analysis we can further analyze the malware.

MirandaTateScreensaver.scr.exe

malicious

This report is generated from a file or URL submitted to this webservice on November 14th 2021 23:29:13 (UTC)
Guest System: Windows 7 32 bit, Professional, 6.1 (build 7601), Service Pack 1
Report generated by Falcon Sandbox v8.49.7 © Hybrid Analysis

Threat Score: 100/100
AV Detection: 71%
Labeled as: Doina.Generic

Overview | Sample unavailable | Downloads | External Reports | Re-analyze | Link | Twitter | E-Mail
Hash Not Seen Before | No similar samples | Request Report Deletion

Incident Response

Risk Assessment

Network Behavior Contacts 1 host. View all details

MITRE ATT&CK™ Techniques Detection

This report has 7 indicators that were mapped to 7 attack techniques and 6 tactics. View all details

e. The IP address that it contacts is 23.22.63.114.

IP Address	Port/Protocol	Associated Process	Details
23.22.63.114 OSINT	80 UDP	mirandatatescreensaver.scr.exe PID: 3232	United States

Contacted Countries

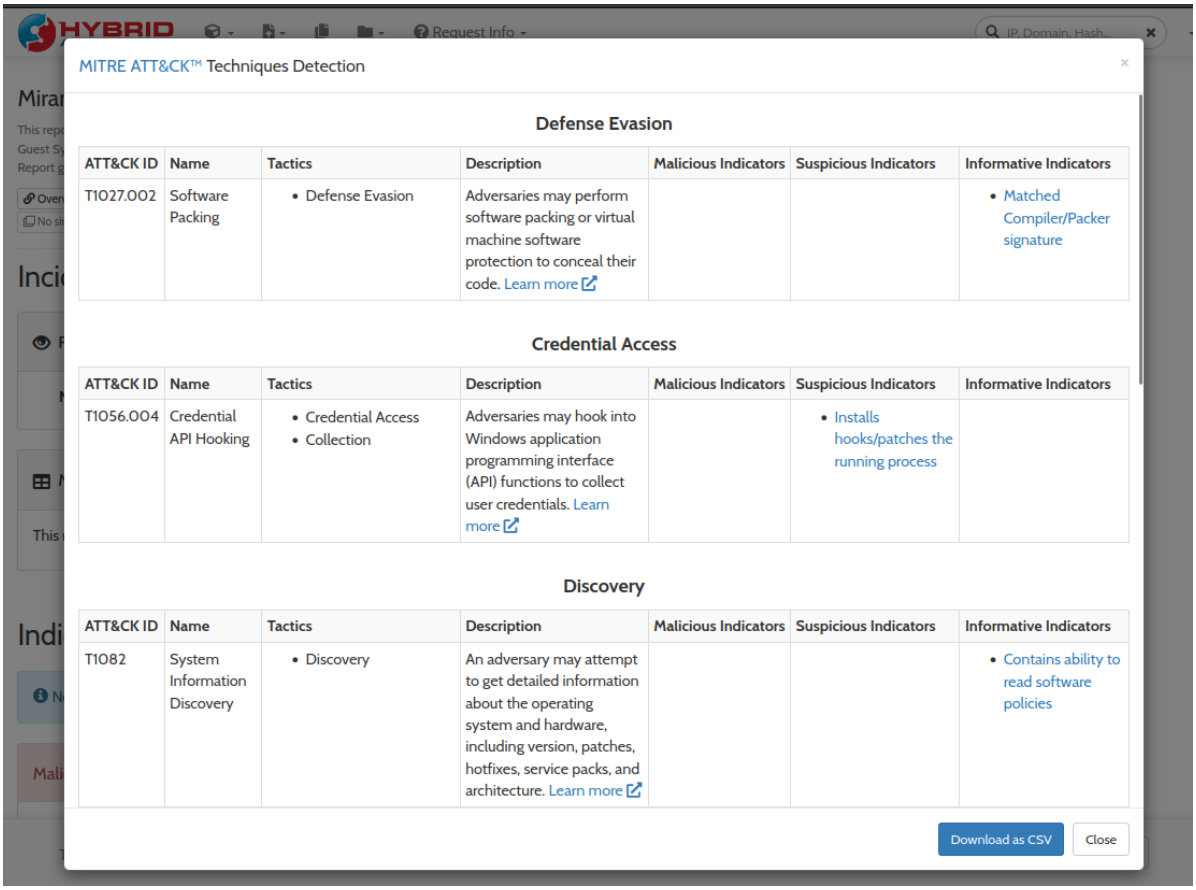
HTTP Traffic

No relevant HTTP requests were made.

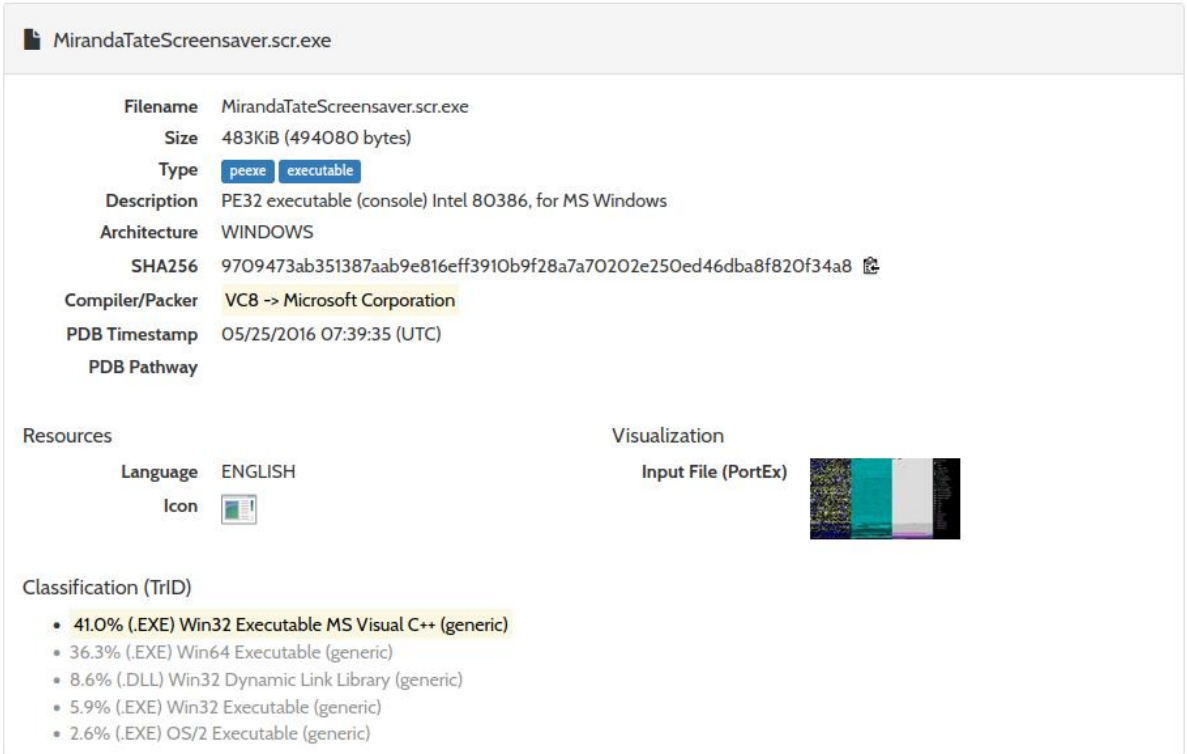
Memory Forensics

String	Context	Stream UID
23.22.63.114	Domain/IP reference	8695-703-004055A0
127.0.0.1	Domain/IP reference	8695-851-00405BE0

f. The technique used according to the MITRE ATT&CK Framework



e. The file details



IN CONCLUSION: “we have investigated a cyber-attack where the attacker had defaced a website 'imreallynotbatman.com' of the Wayne Enterprise. We mapped the attacker's activities into the 7 phases of the Cyber Kill Chain.”