Splunk: Incident Handling Wayne Enterprises

Scenario.

Wayne Enterprises faced the cyber attack.

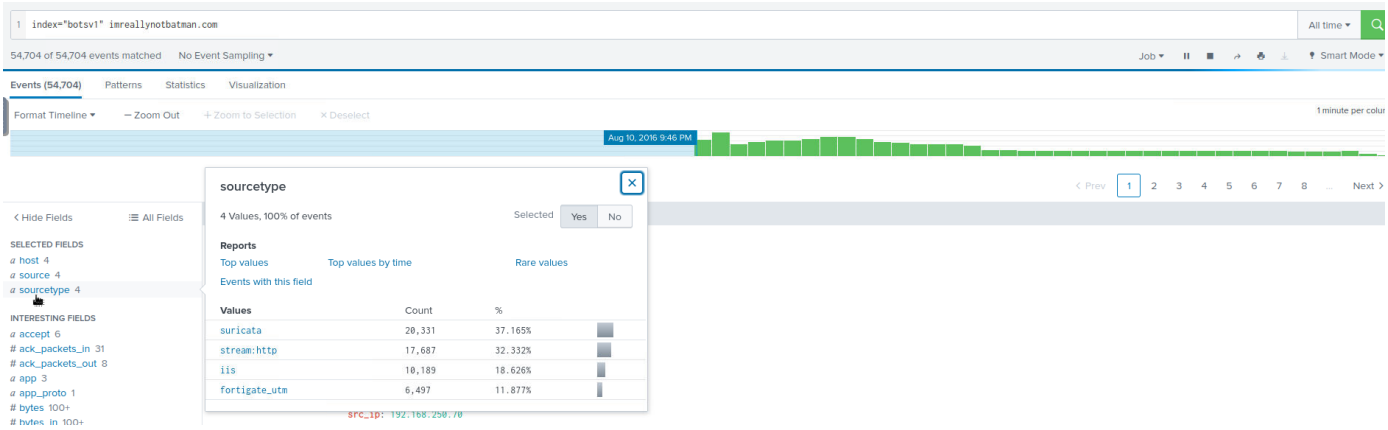
- The attacker broke into the network.
- The web server was compromised.
- The website was defaced.
    - imreallynotbatman.com
- The trademark of the attacker was recorded as YOUR SITE HAS BEEN DEFACED.
- Splunk was used as an SIEM solution for the investigation.
    - Suricata is investigated.
        - It is the Suricata IDS.
        - It shows the trigger alerts and causes the alert to get triggered.
        - It is the Log source Investigation.
    - Stream: HTTP is investigated.
        - Network flow related to http traffic.
    - Category is investigated.
        - It contains different category process actions on the Host of the Server.
    - Command Line is investigated.
        - It contains the executed command lines on the Host.
    - Domain name IP addresses are also investigated.
    - Statistic filter is used to display the output and narrow down the investigation.
- Cyber Kill Chain was used for this investigation.

Reconnaissance Phase.

During this phase, the information about the target is discovered and collected.

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

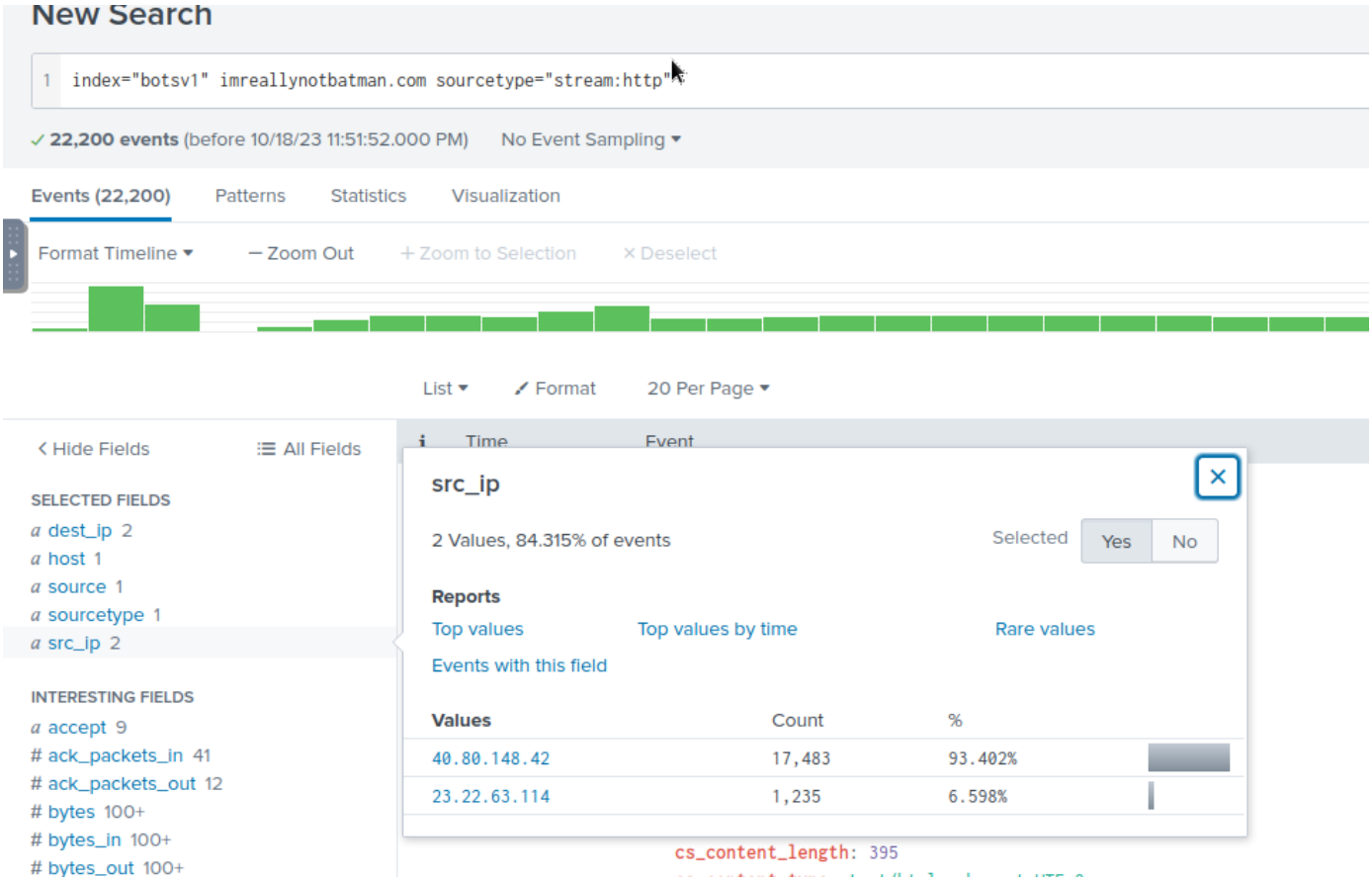
- We are going to search for any information about this DN.



According to the source type, there are 4 log sources contained in the source type.

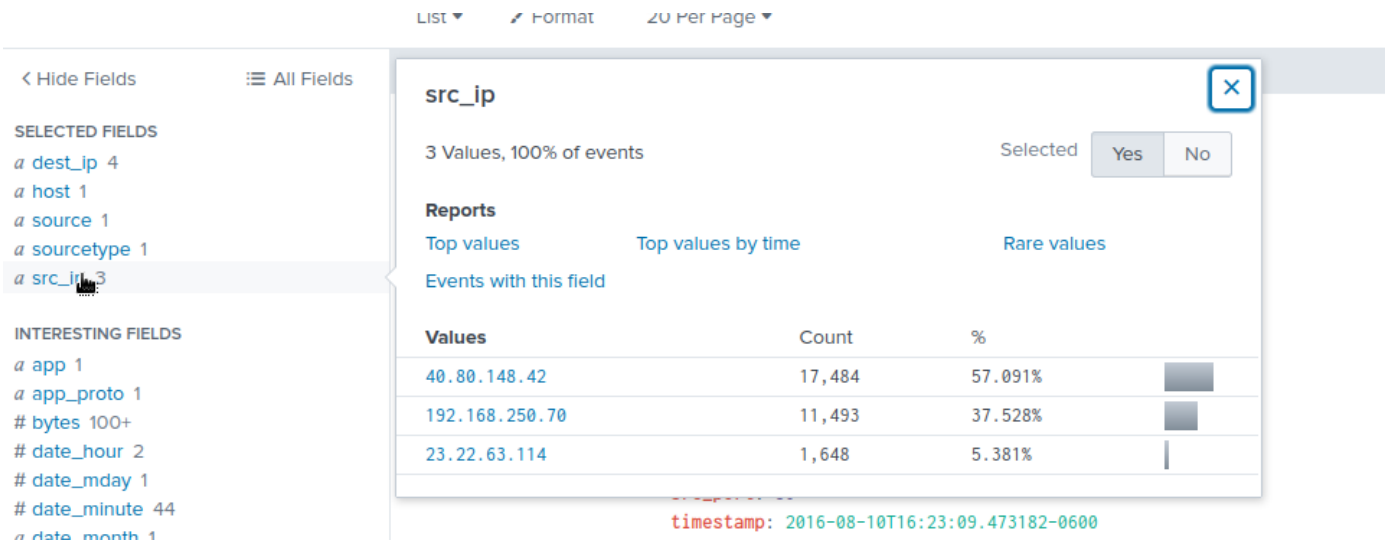
The stream. http is investigated to identify this DN's and another Server's communication.

- The source IP address contains the IP addresses that are used to communicate the internal webserver of the organisation.
- 40.80.148.42 has more than 93.402% of total events connecting the webserver.



The Suricata IDS is investigated next because it contains the most logs.

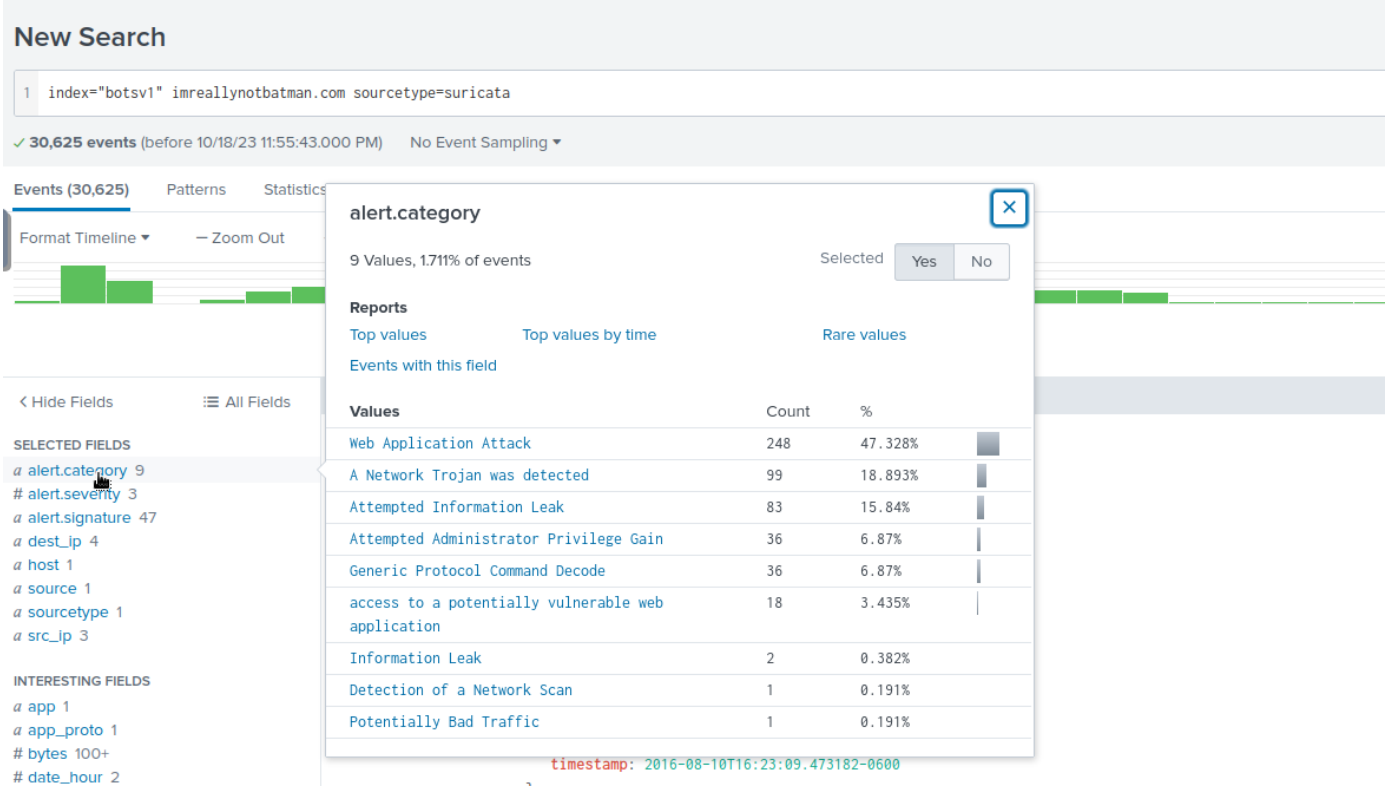
- The IP addresses are investigated, which are used to reconnaissance the information of this DN.



- The first IP address investigated is 40.80.148.82, which contains the highest number of events.
- Notes: 192.168.250.70 is not used as the IP address for reconnaissance information because it is a Private IP address, so it is used for internal orientation.
- The other two IP addresses are recognized as Public Addresses for communication over the Internet.
    - The attacker can use them to compromise the system.

Investigate Alerts from the Suricata in 40.80.148.82.

- Suricata is the IDS, which contains different alerts and logs them for more information.
- According to an alert category, the attacker tries different vectors to attack the web server.
- The attacker wants to compromise the Web Application Attack by uploading and installing the Network Trojan.
- The attacker wants to access the privilege's administrator account.
- The destination IP address is 192.168.250.70, the Web server IP address.
    - This IP uses port 80, the web server, for HTTP traffic.

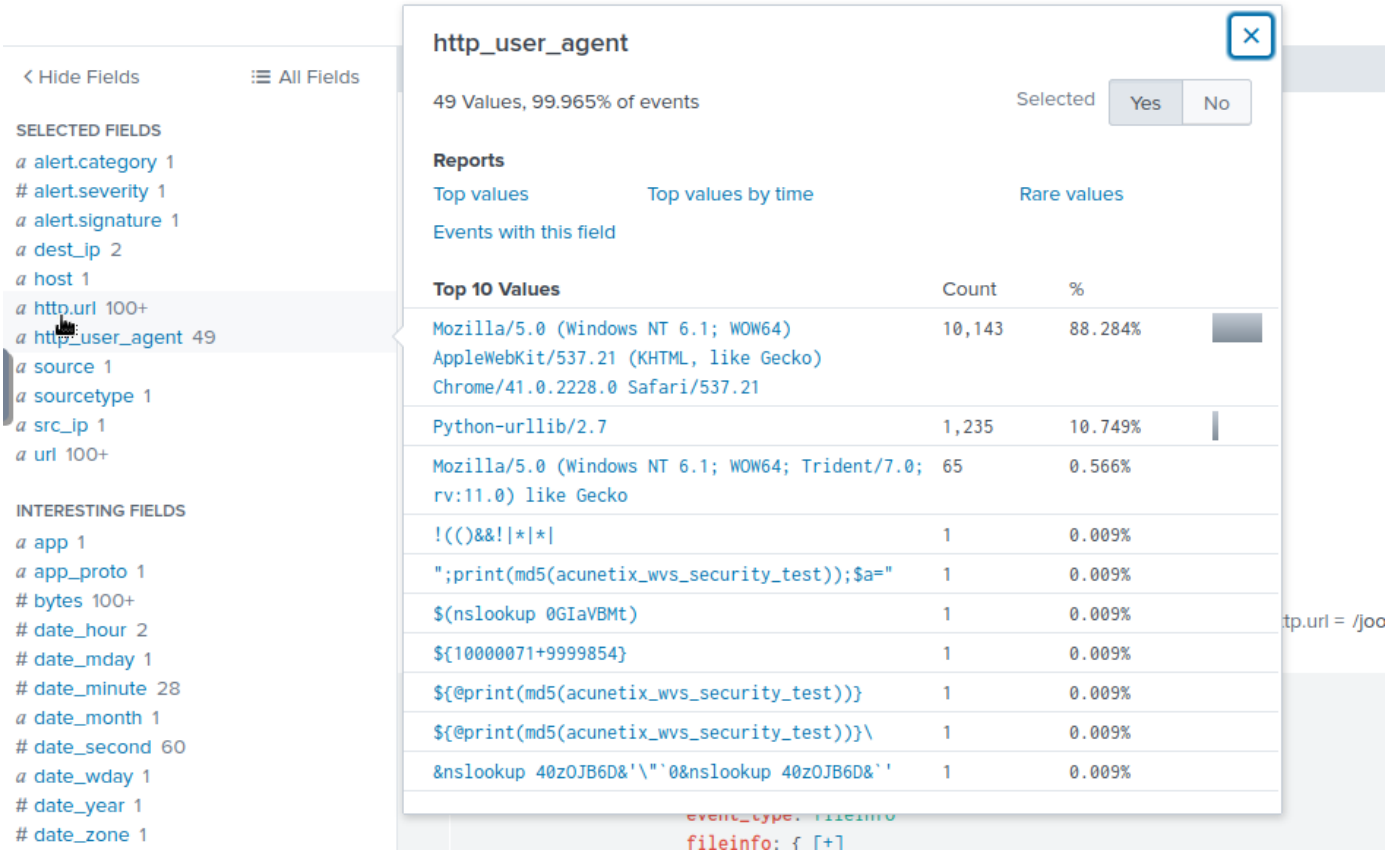


- An alert signature contains different signatures as predefined rules of the alert.
    - The CVE 2014-6271 is the NIST framework used as a resource for this signature.

Investigate the user agent of this IP 40.80.148.82.

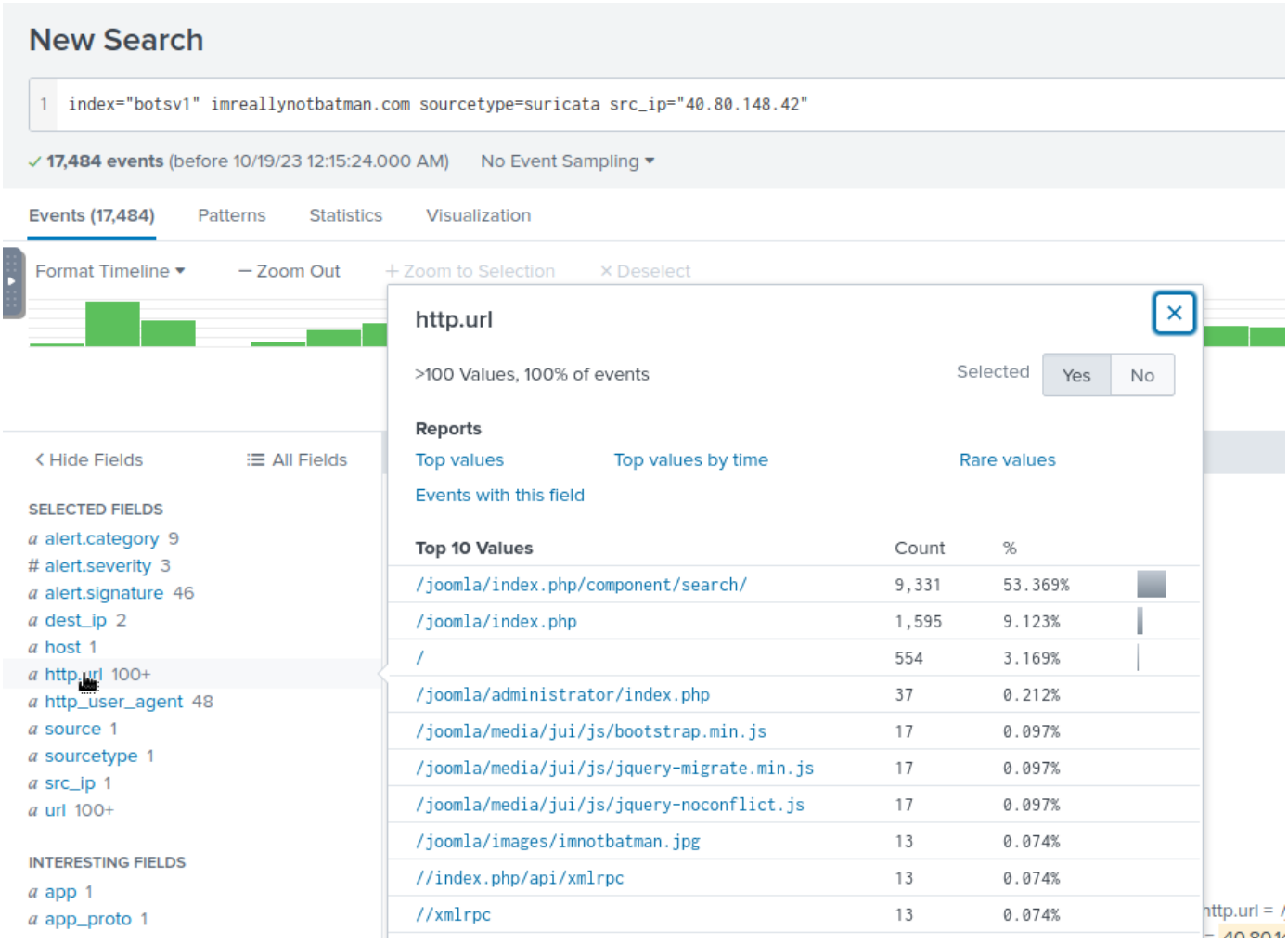
- User agent is the browser used to communicate between the User device and the webserver.
    - Note 1: The output of user agents of both the webserver and User must be the same because the browser can act as a third party for the communications.
    - Note 2: However, the web server can record different user agents when more than two users access the web server with different user agents. Or one user can access the webserver with two or more user agents.
        - For example, user 1 uses Chrome, and user 2 uses Mozilla to access the Webserver. The User agent of the webserver is recorded as Chrome and Mozilla.
        - User 1 uses Chrome and Acunetix to access the webserver. The User-agent on the web server is recorded as Chromes and Acunetix.

- Accunetix is the VS of the web application, which SOC can use for VS or hackers to find the V of the web application.



Investigate url of IP 40.80.148.82.

- The webserver and user would show the same output because the webserver uses only their URL for communication.
- joomla is recorded as Content Management System (CMS) software.
    - These web applications are used to manage content on a website. For example, blogs, news sites, e-commerce sites and more!



Exploitation Phase.

```
index=botsv1 imreallynotbatman.com sourcetype=stream* | stats count(src_ip) as Requests by src_ip | sort - Requests
```

- Counting the number of Requests Source IP to the webserver.

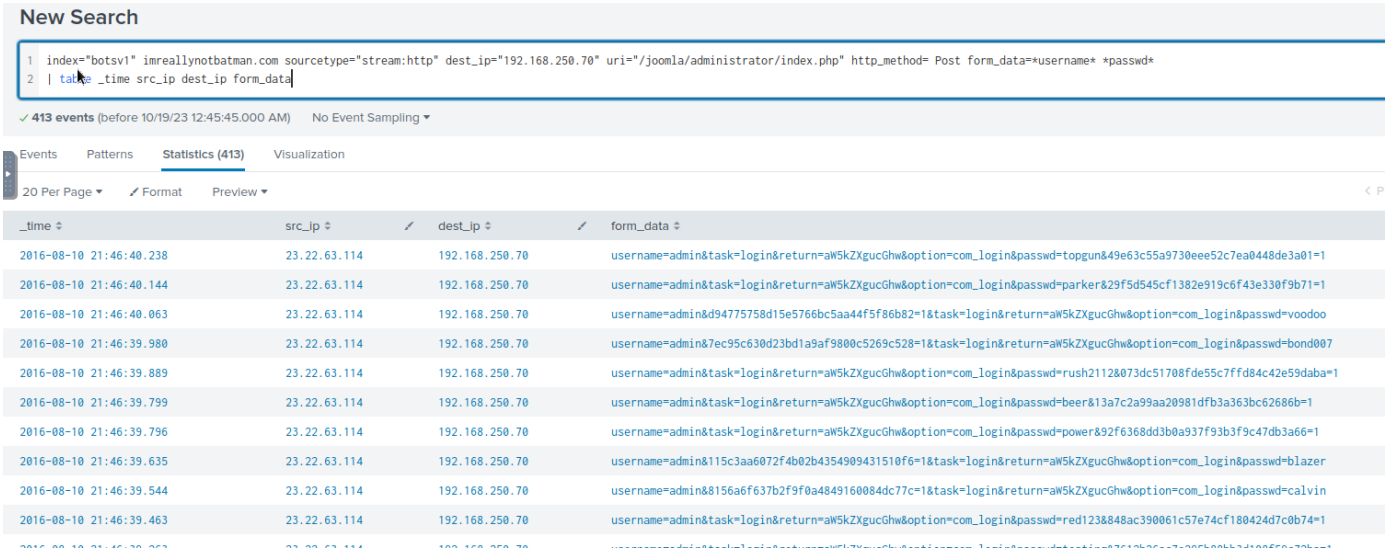
The web server with its IP address 192.168.250.70 is investigated.

According to the Scenario, the attacker have defaced the website, which means they must have a privileged account to perform this process. Two ways are used to gain privileged authneticaiton and authorization.

- The attacker creates the standard user account and tries their best to gain the privileged authorization via privilege escalation.
- The attacker brute forces the administrator account.

The URI contains the username and password of administrators within the form data.

According to the table, the attacker tries to brute-force passwords with username admin from source IP 23.22.63.114.

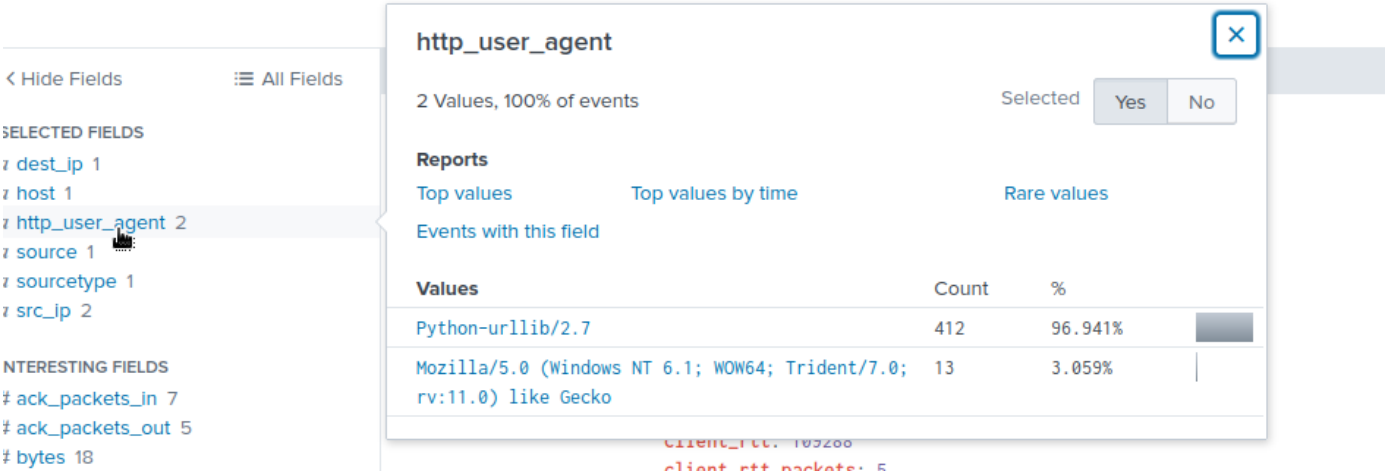


Investigate the HTTP traffic and POST request.

The attacker uses Python to brute force the password.

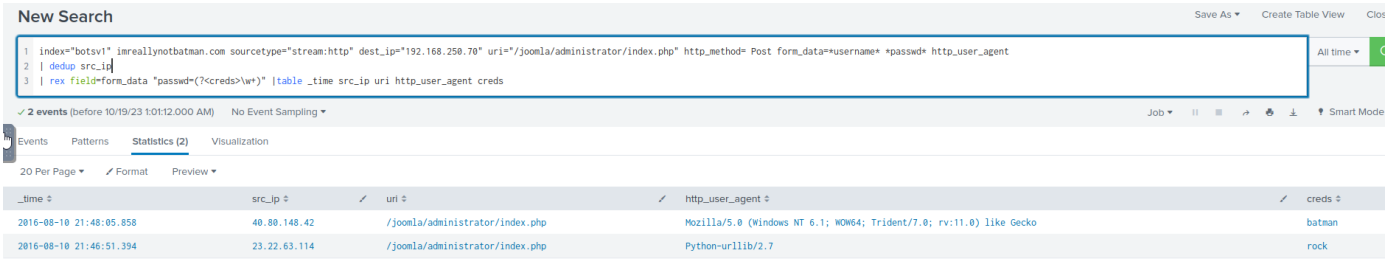
However, they also have one request from the Mozilla one.

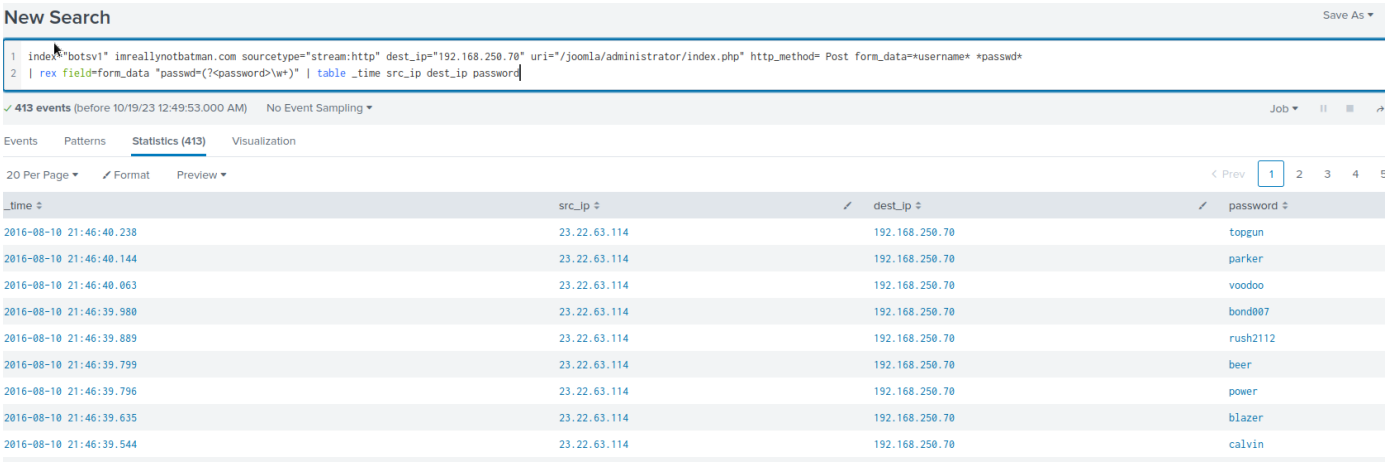
This means the attacker tries one password attack on this Mozilla agent from 40.80.148.12.



Investigate password with rex function.

- dedup can be used to narrow down the result.
- rex is the regular expression.
- `rex field=form_data "passwd=(?<creds>\w+)"`
    - This command means it extracts passwd values from the form_data field within the logs.





How do we know that the attacker has used the correct Password?

- The attacker tries their best to brute force the password.
- The FINAL password is known as the process's terminal because this is the correct password.

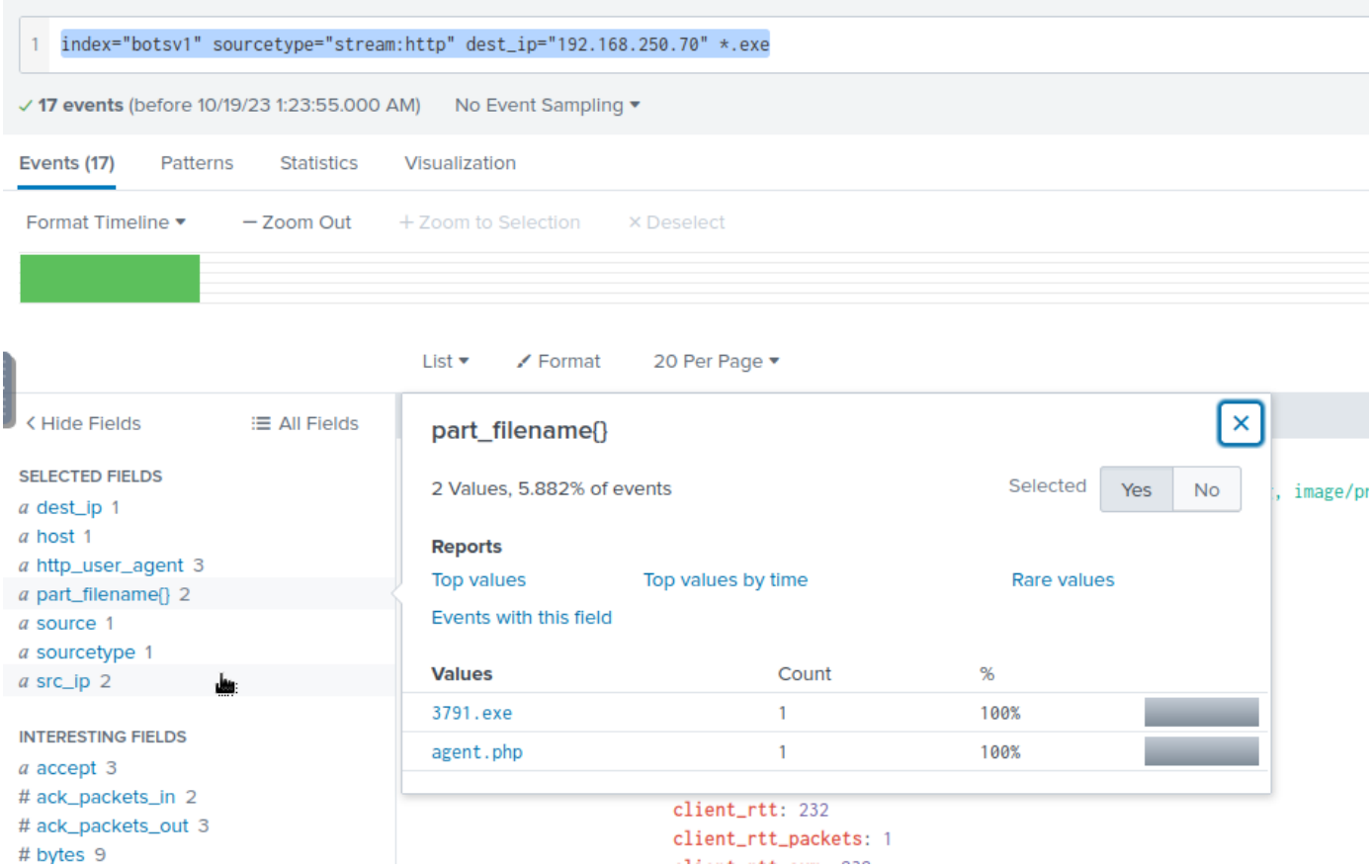
Installation Phase.

Investigate the HTTP traffic with execution files on server 192.168.250.70, not on the site DN.

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

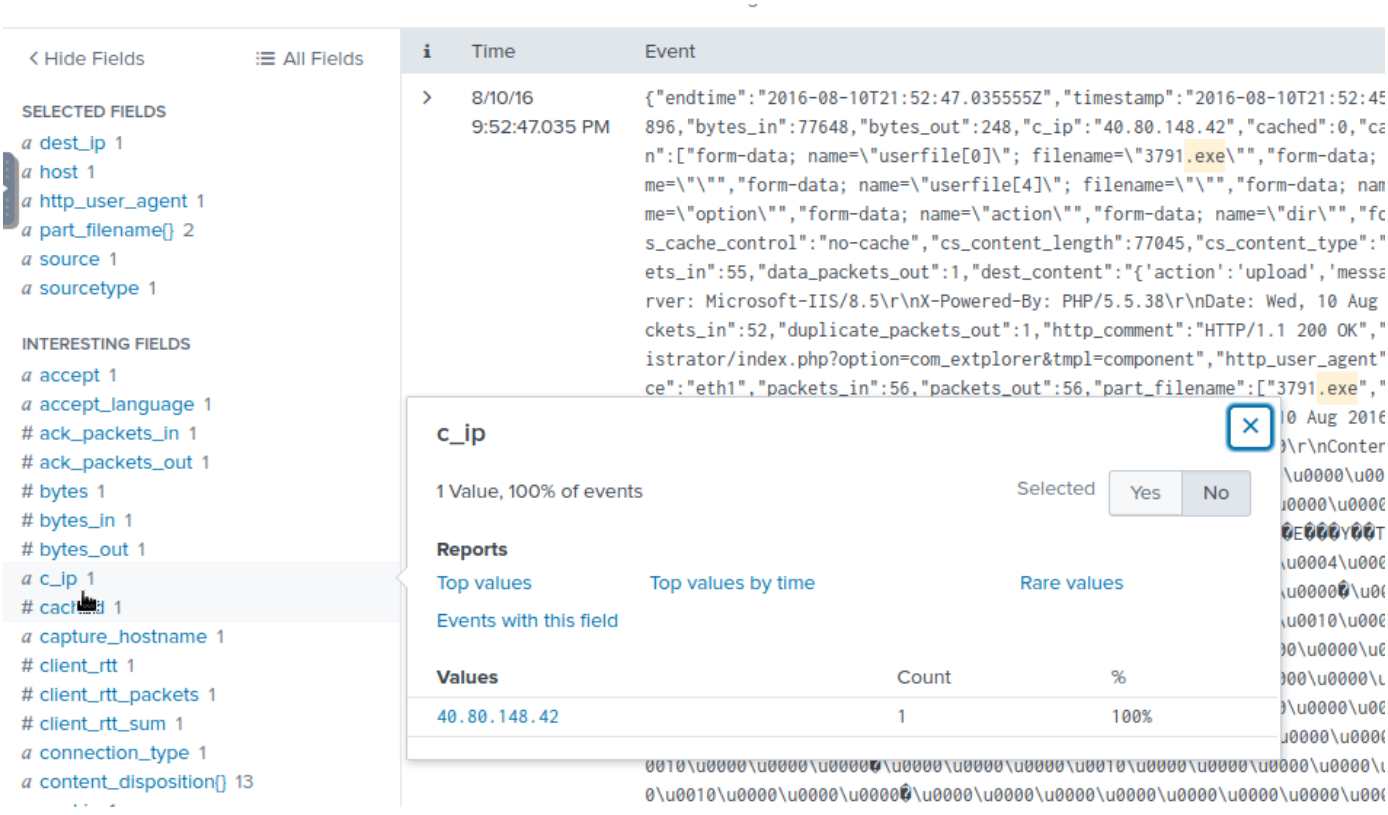
We understand that the attacker uses IP address as 40.80.148.82 which is known as the public IP address for the attack.

- This means the attack was processed remotely with the exe files as the backdoor.
- The .php format generates the HTML file, not the execution file.



c_ip is the command ip from the 40.80.148.82.

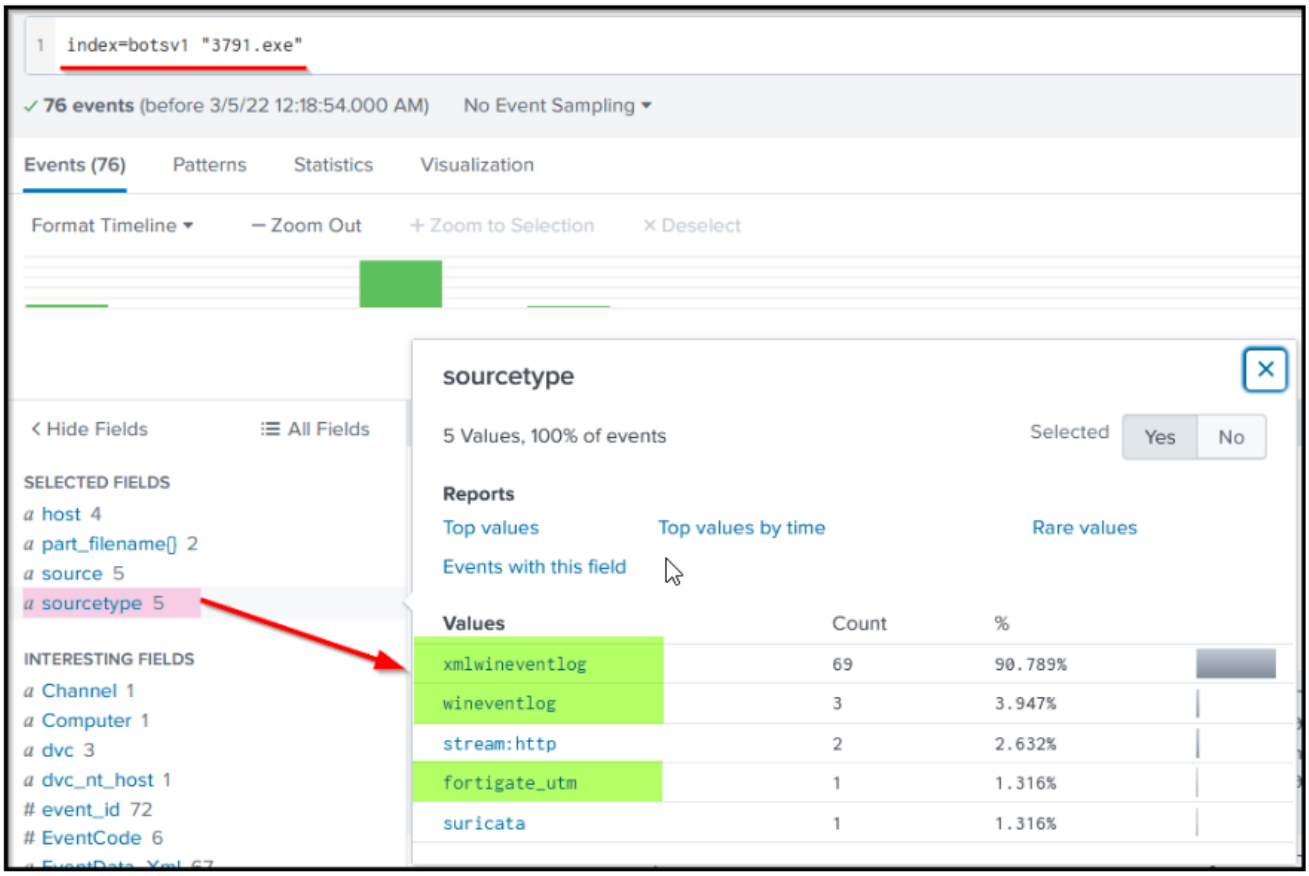
- The file is uploaded via this IP address.



Was this file executed on the server after being uploaded?

Three source logs are recorded to investigate this file.

- Hostcentric log is used for investigation of the execution of this file.
- xmlwineventlog is used for investigation.
    - EventID=1 is the event code for successful execution.



- For the evidence of execution, we can leverage sysmon and look at the EventCode=1 for program execution.

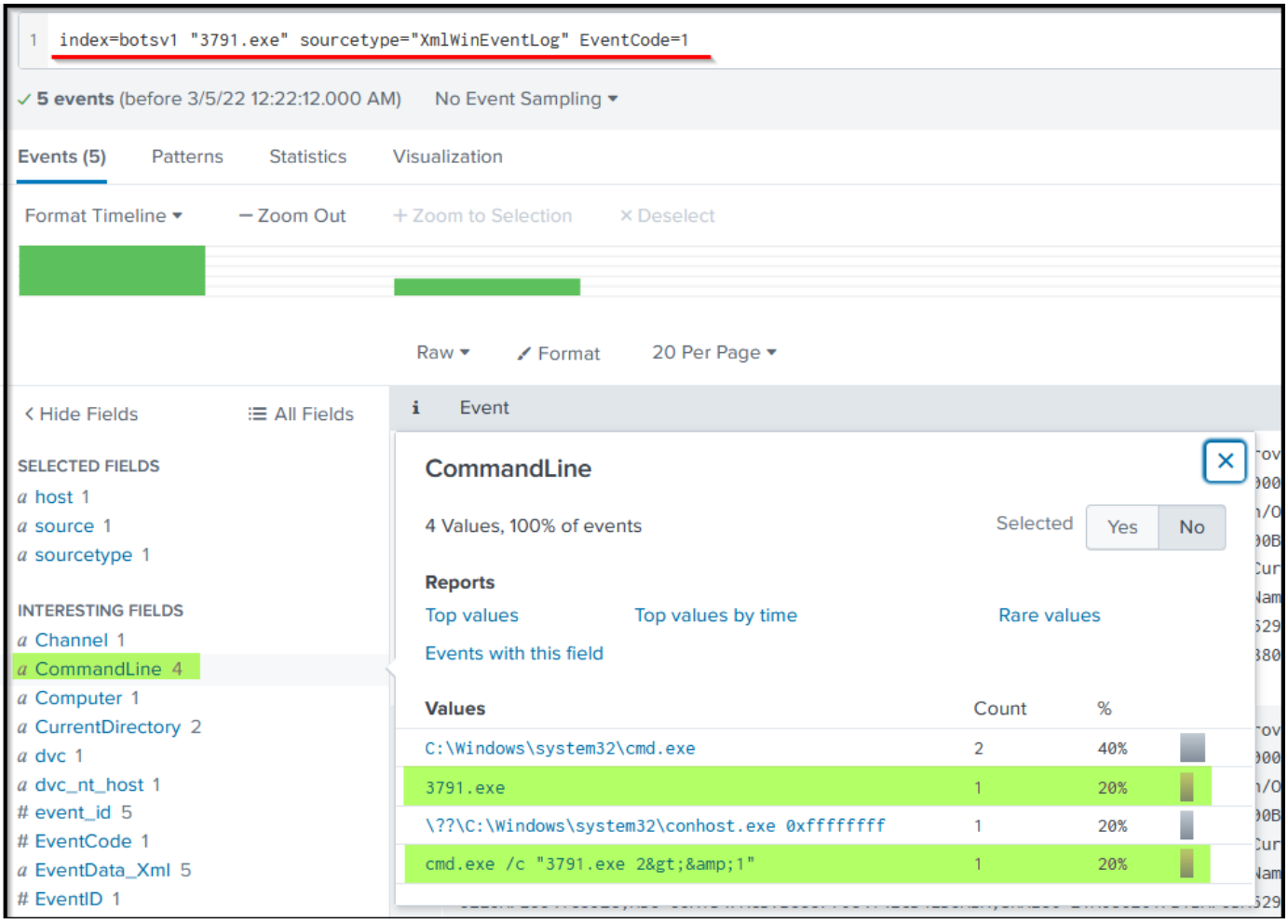
  Reference: https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

Event ID 1: Process creation

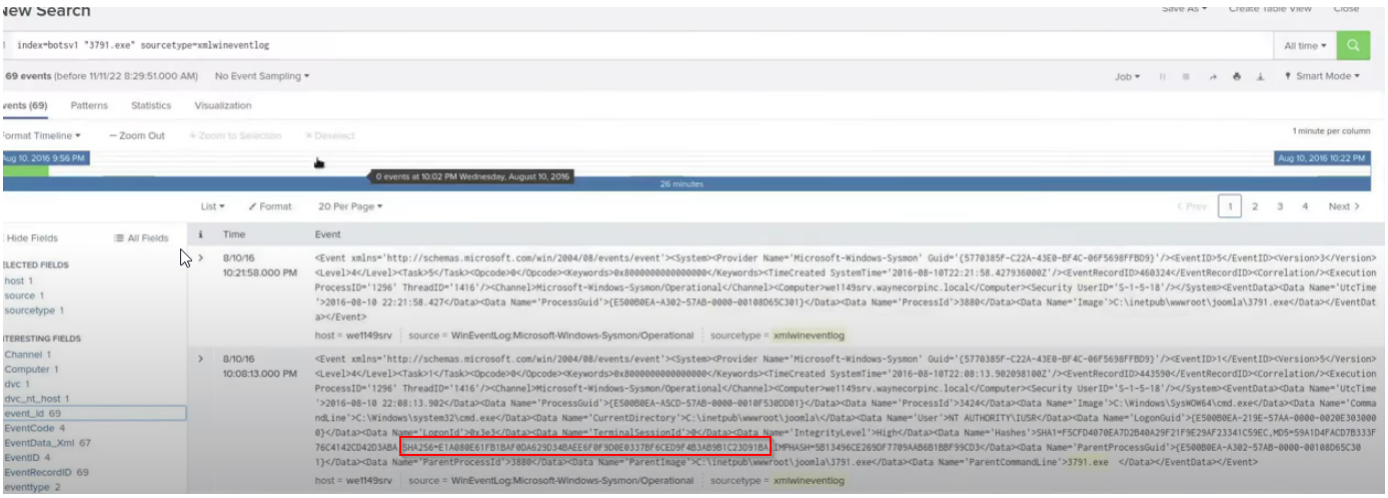
The process creation event provides extended information about a newly created process. The full command line provides context on the process execution. The ProcessGUID field is a unique value for this process across a domain to make event correlation easier. The hash is a full hash of the file with the algorithms in the HashType field.

Search Query: `index=botsv1 "3791.exe" sourcetype="XmlWinEventLog" EventCode=1`

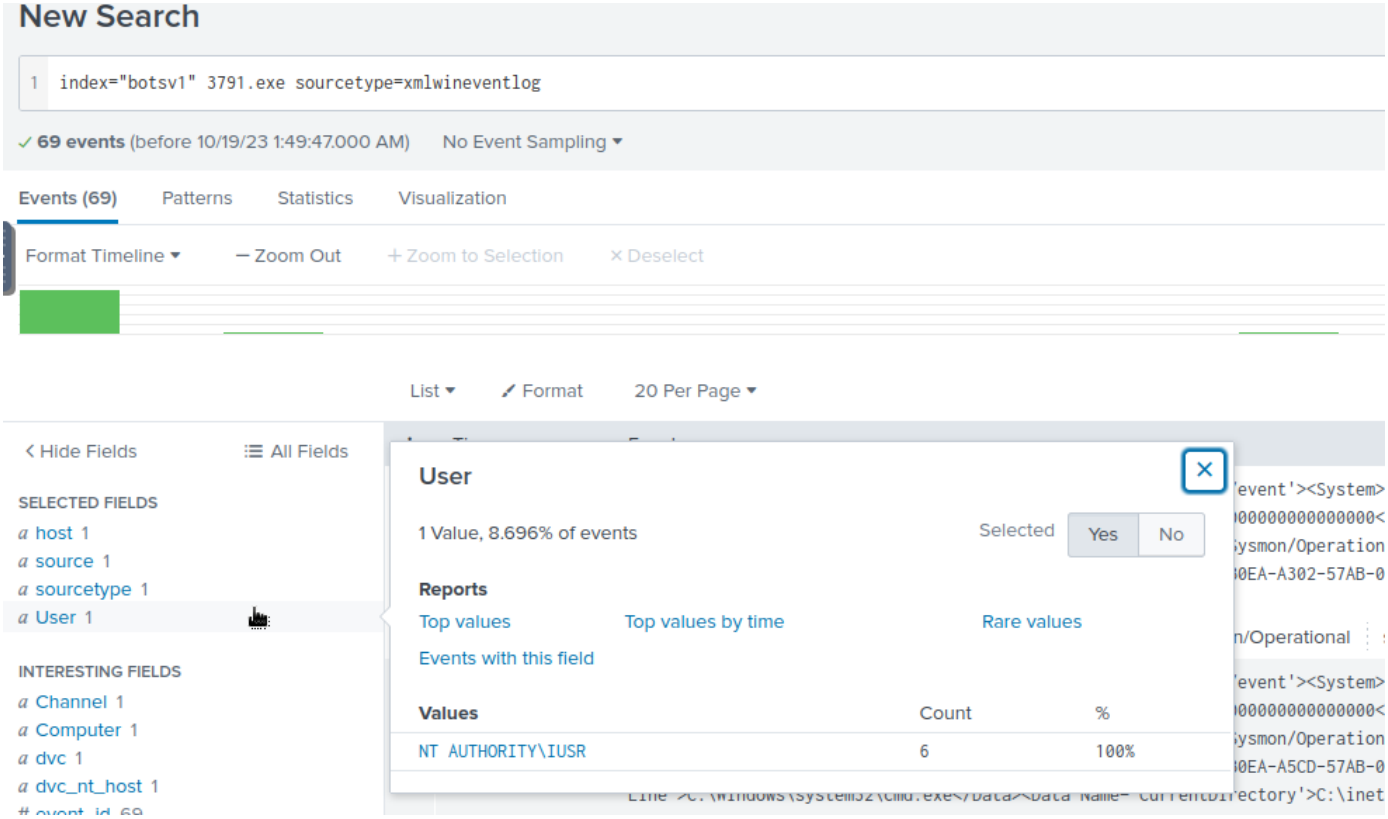
This shows that 3791.exe has been executed in the cmd.exe.



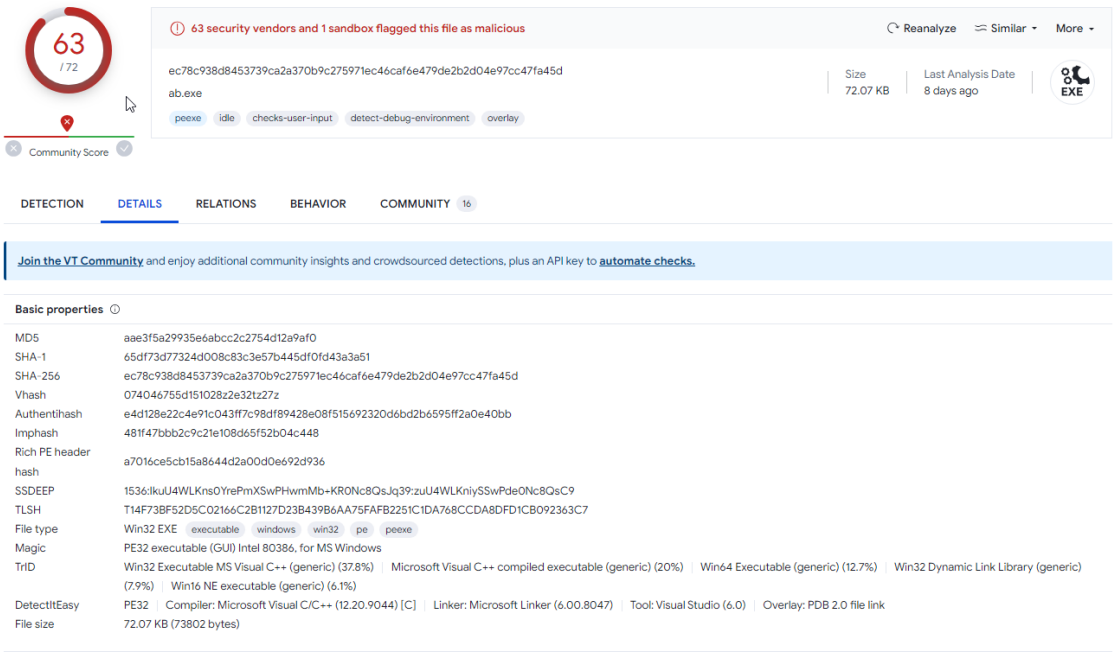
The SHA256 host is recorded within the Symson Logs.



Finding the user tab on the left to find the user for the execution.



Using the virustotal for the Investigation of the malware or malicious file.



Action on Objective.

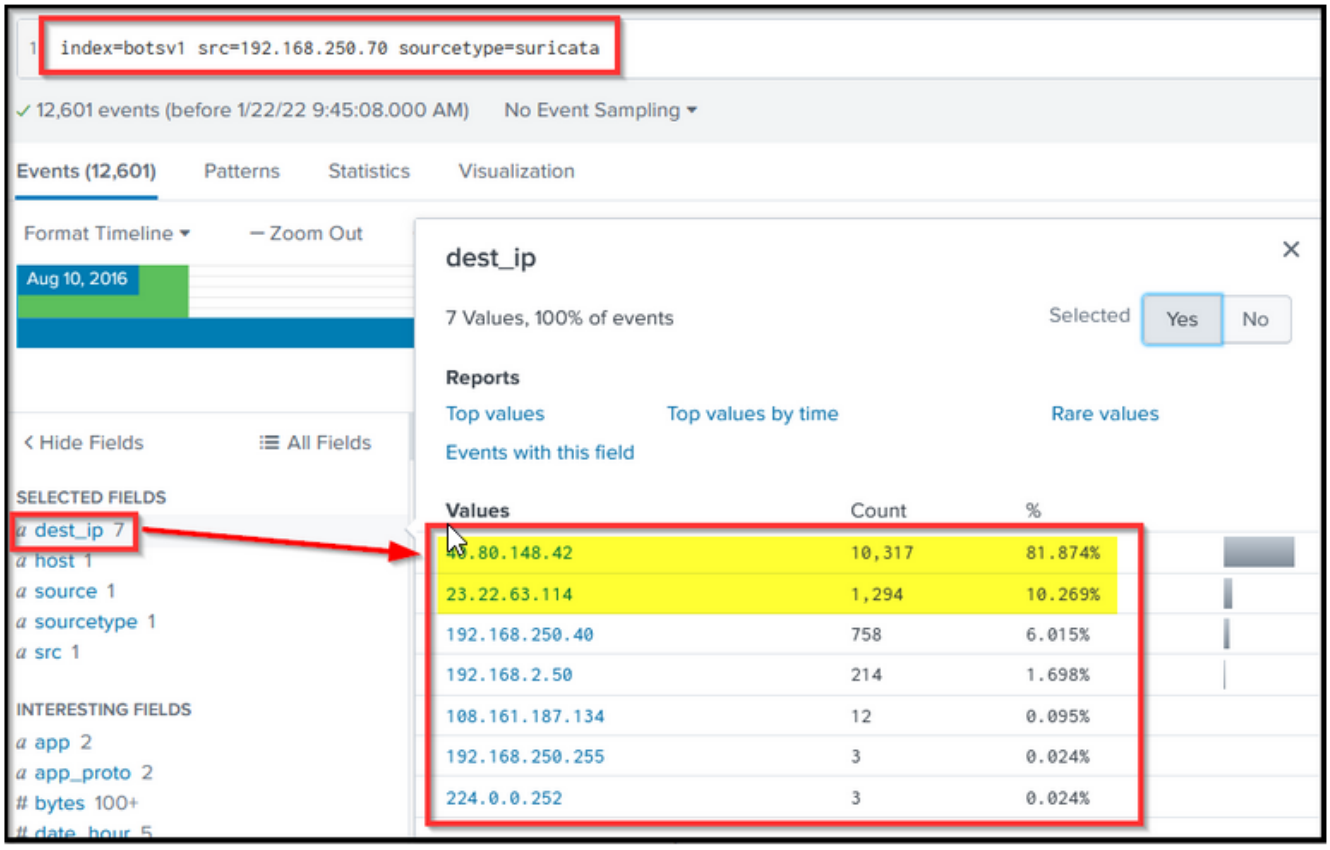
The main objective of the attacker was to deface the website.

We investigated what ended up on the website for the defacement.

Investigate the outbound traffic of the webserver.

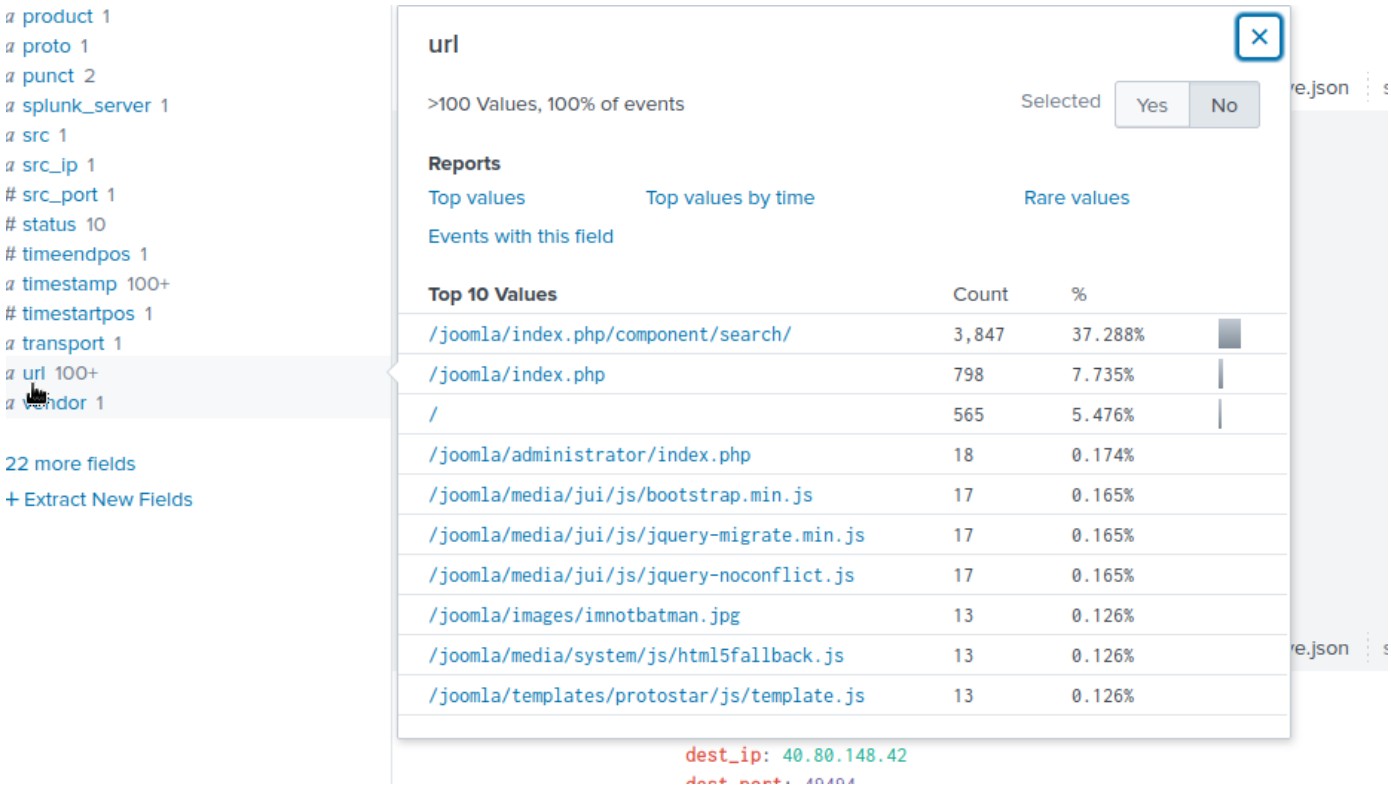
- The outbound traffic was connected to two primary IP addresses.

Search Query: `index=botsv1 src=192.168.250.70 sourcetype=suricata`



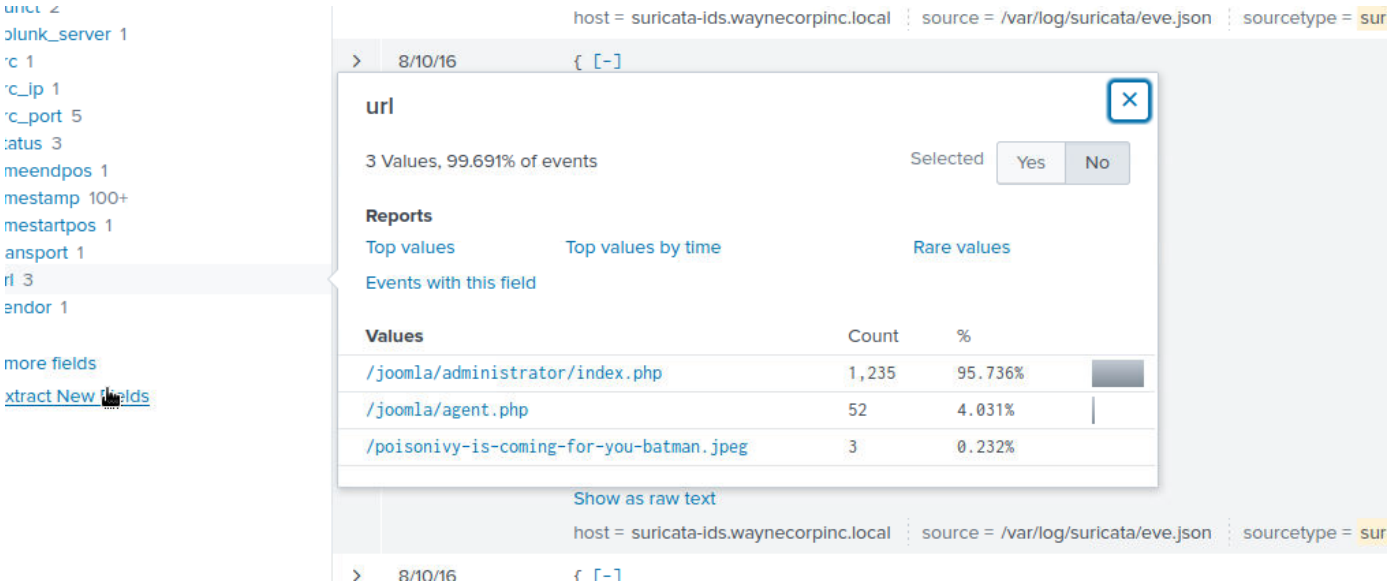
Investigation of URL agent.

The URL agent of the first IP address doesn't show any malicious information.



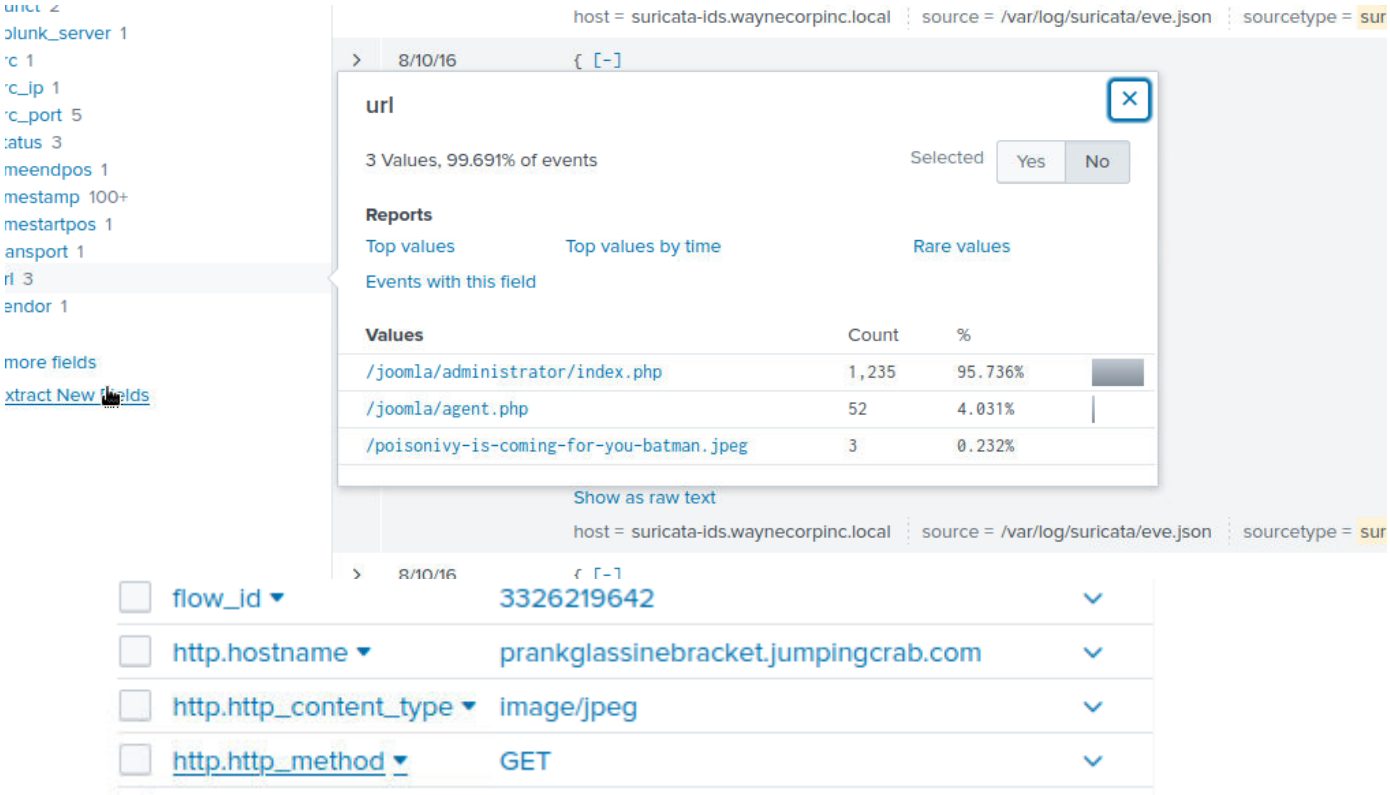
The URL agent of the second IP address shows the malicious information, which is the jpeg file.

- The png file can be uploaded and installed to deface the website.

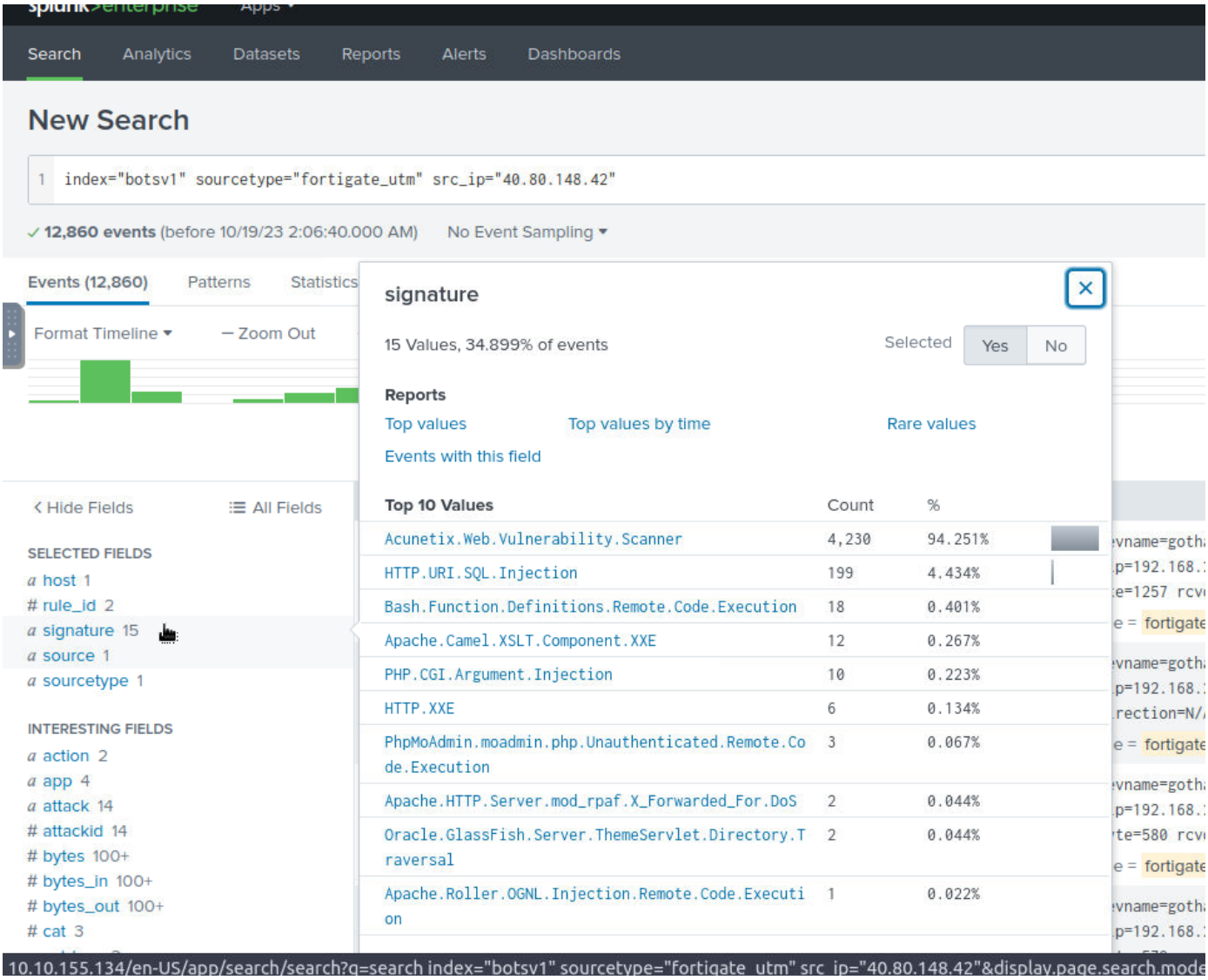


Investigate this .jpeg file.

- The http host name of this file is shown.
  - This means this file was downloaded from this attacker's host.



Investigate the rules from firewall Unified Threat Management.

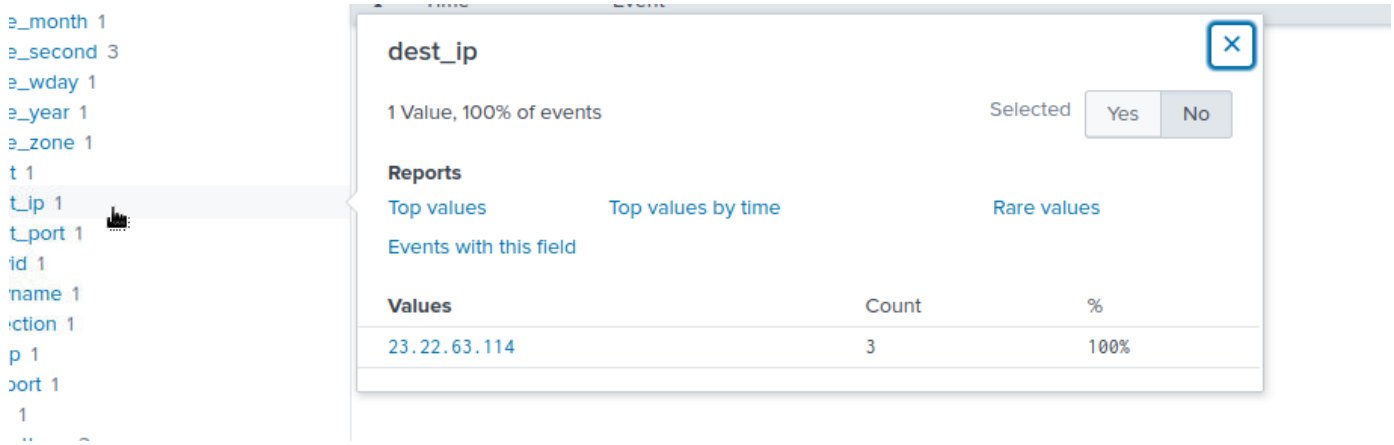


Command and Control

The attacker uses DNS to resolve the malicious IP address.

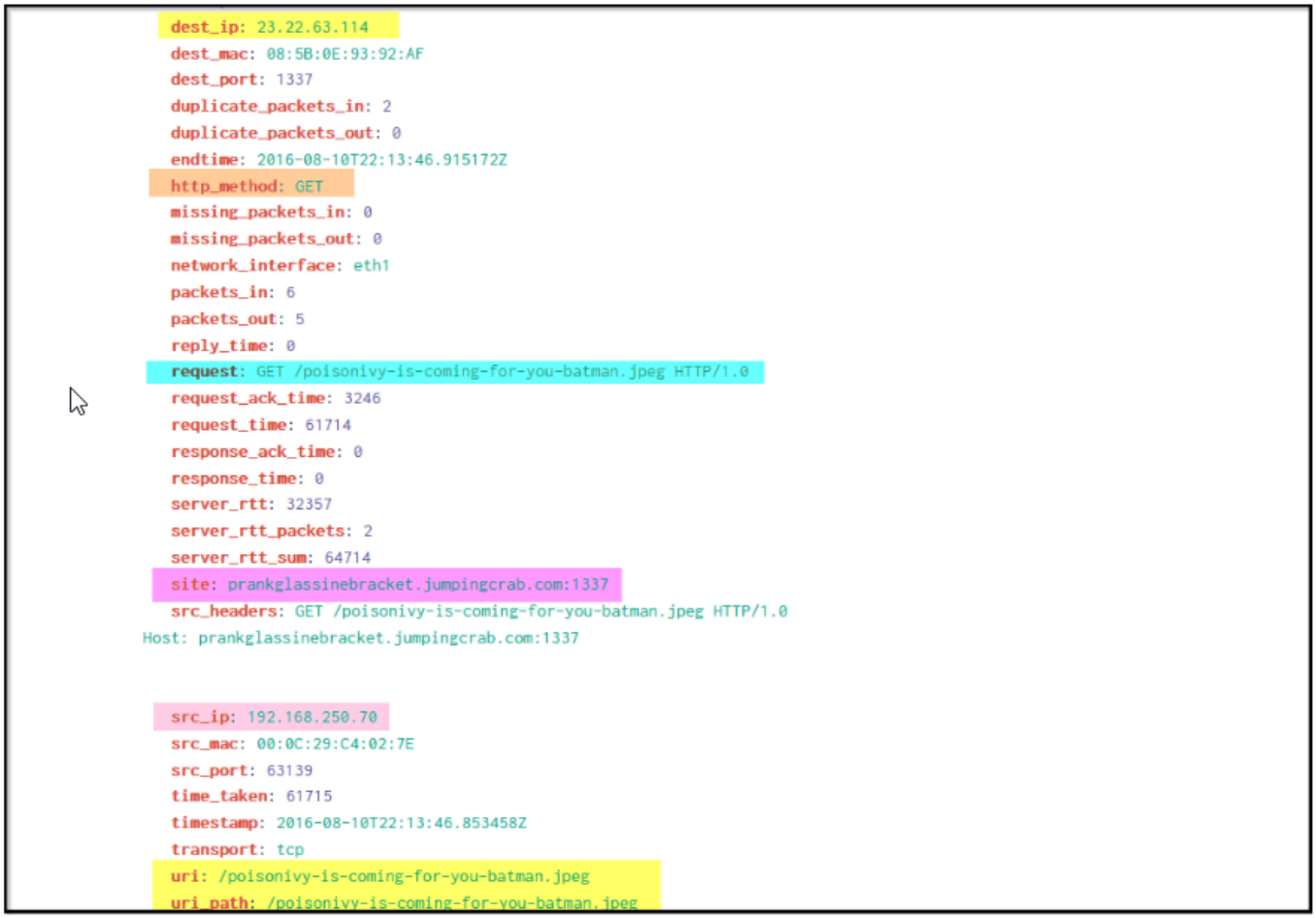
- Finding the DNS and IP address for this DN from the attacker.
- Finding the DN from the url.

The destination IP address for this DN is from 23.22.63.114.



Search Query:

```
index=botsv1 sourcetype=stream:http dest_ip=23.22.63.114 "poisonivy-is-coming-for-you-batman.jpeg"
src_ip=192.168.250.70
```



Weaponisation.

In the weaponisation phase, the adversaries would:

- Create Malware / Malicious documents to gain initial access / evade detection etc.
- Establish domains similar to the target domain to trick users.
- Create a Command and Control Server for the post-exploitation communication/activity etc.

We have found some domains / IP addresses associated with the attacker during the investigations. This task will mainly look into OSINT sites to see what more information we can get about the

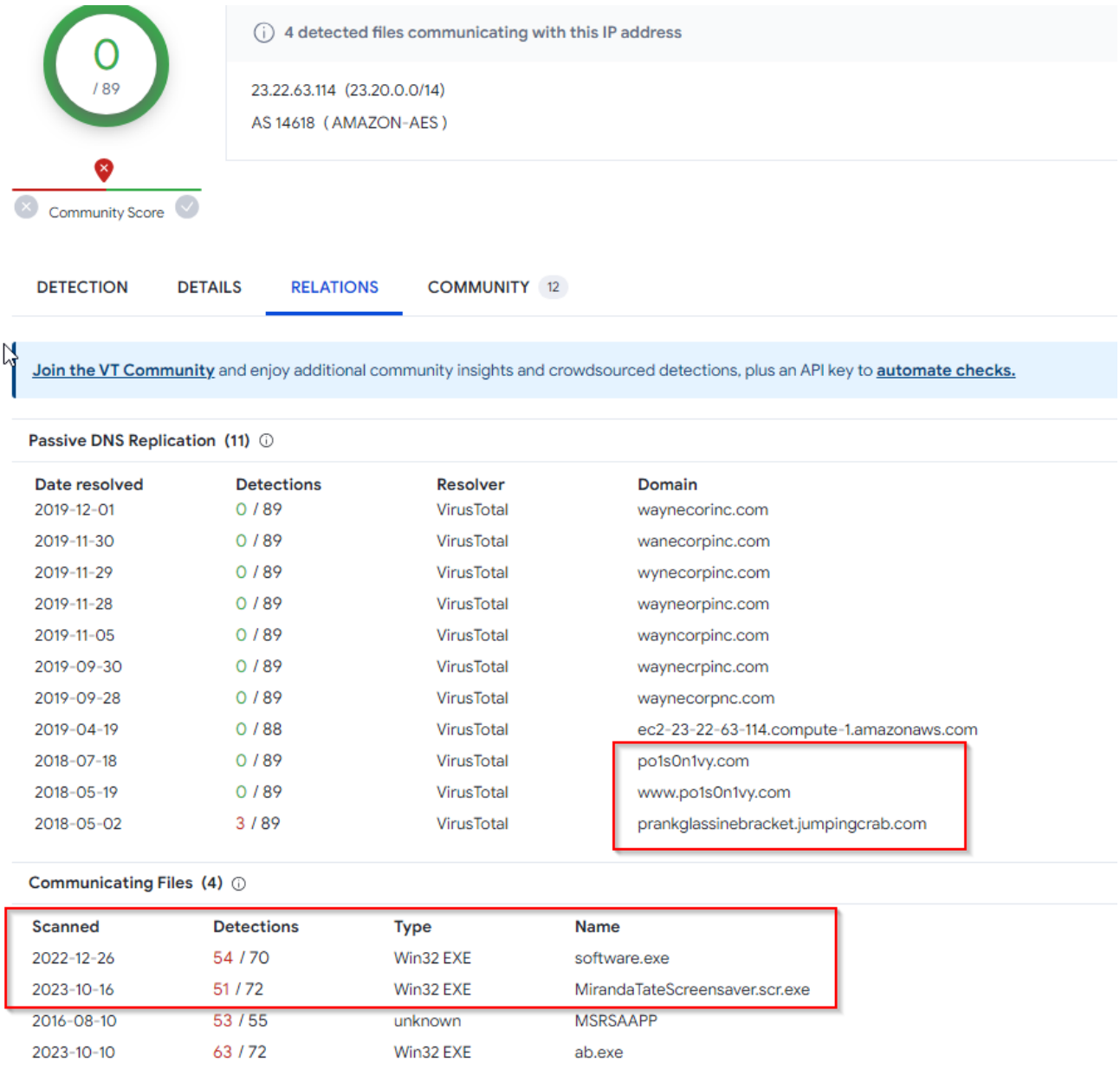
adversary.

According to the last step, the domain of the attacker is prankglassinebracket.jumpingcrab.com

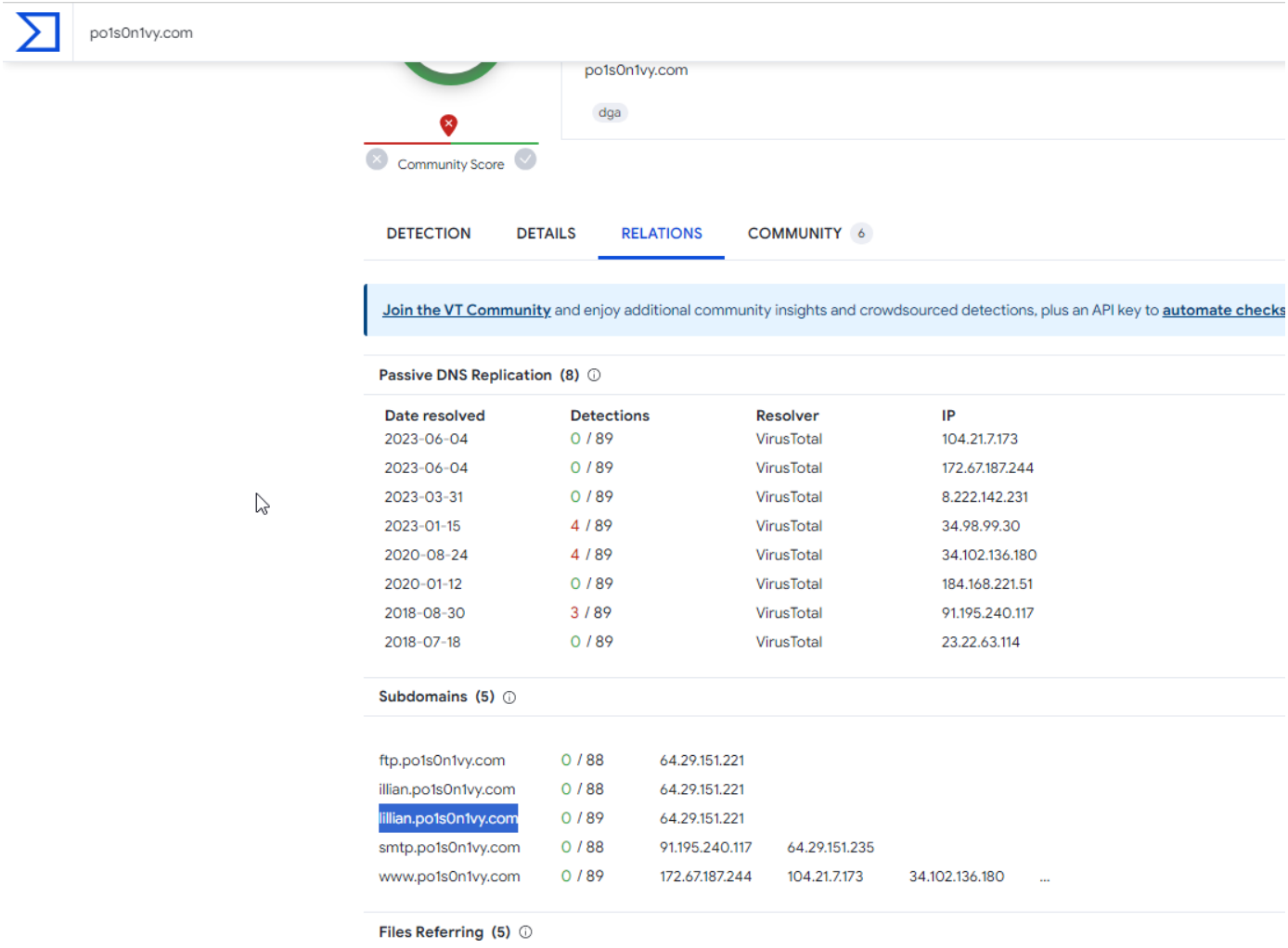
- The attacker uses IP address as 23.22.63.114

OSNIT tools.

- Robotex.
  - Provide information about IP address, domain names and subdomain names.
  - The input can be an IP address or any FDN.
  - https://www.robtex.com/dns-lookup/
- Virus total.
  - analyze suspicious files, domains, IP, etc.



According to the file's name, poisonivy is associated with this malicious file.



Ox alien.

- It is used to investigate the Name, Nameserver, city and country of the DN.
- https://otx.alienvault.com/indicator/hostname/lillian.po1s0n1vy.com

whois.domain.

- whois infomation is investigated.
- IP address and AS location can be found from this website.
- https://whois.domaintools.com/po1s0n1vy.com

Delivery Phase.

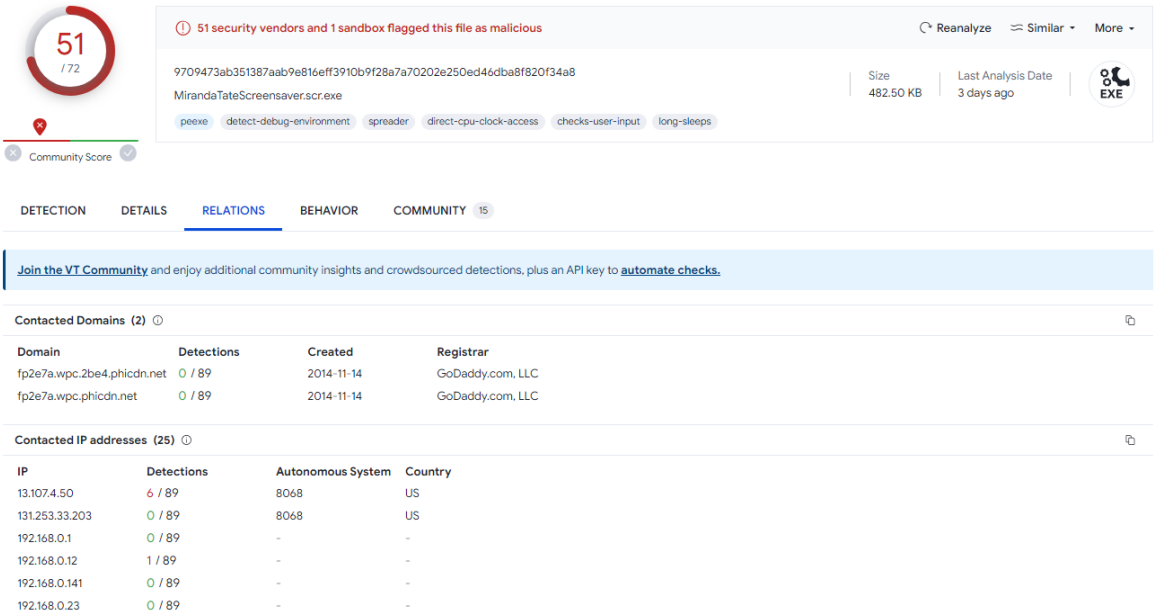
Using OSINT tools for searching the malwares which are associated with the attacker.

Threat Miner.

- Investigate the Sample malware from a specific IP address.
    - https://www.threatminer.org/host.php?q=23.22.63.114#gsc.tab=0&gsc.q=23.22.63.114&gsc.page=1
- Searching the MD5 of malware is associated with the attack.
- Click and choose the Hash=> Represent information of the Malware.
    - https://www.threatminer.org/sample.php?q=c99131e0169171935c5ac32615ed6261

Virus Total.

- Investigate the malware.
- Using the Hash 256 for searching the malware.



Hybrid analysis.

Hybrid Analysis is a beneficial site that shows the behaviour Analysis of any malware. Here you can look at all the activities performed by this Malware after execution. Some of the information that Hybrid-Analysis provides are:

-
    - Network Communication.
      - DNS Requests
      - Contacted Hosts with Country Mapping
      - Strings
      - MITRE ATT&CK Mapping
      - Malicious Indicators.
      - DLLs Imports / Exports
      - Mutex Information if created

    - File Metadata
    - Screenshots

- https://www.hybrid-analysis.com/sample/9709473ab351387aab9e816eff3910b9f28a7a70202e250ed46dba8f820f34a8?environmentId=100