Performing Incident Response By Using Cyber Kill Chain Framework With Splunk and Creating Yara Rule

Table of Contents

Part One Cyber Kill Chain Framework With Splunk

1- Reconnaissance Phase

After examining HTTP Logs and IDS Logs I found the following:

- Scan Activity
- Web Application Attack
- Attempted Administrator Privilege Gain

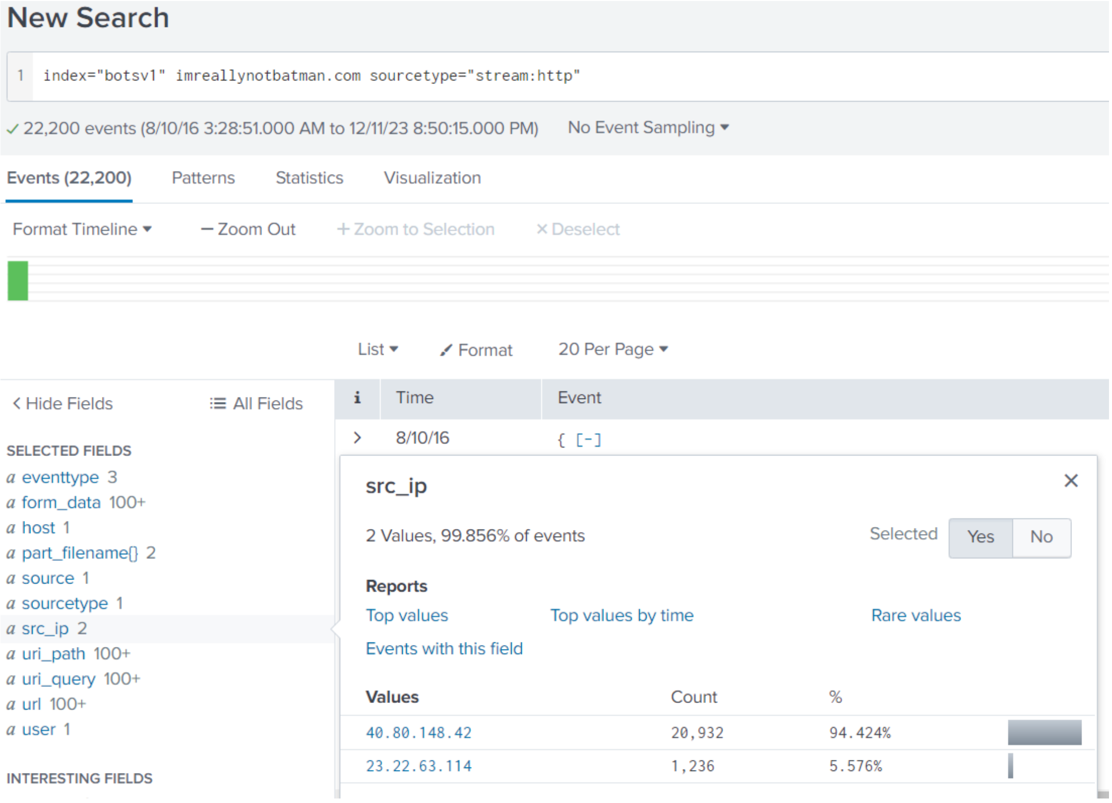
IP Address For Adversaries : 40.80.148.42

Scan Tool: Acunetix web application scan

Attacker Use The Vulnerability CVE-2014-6271 to Gain Access to web server

- The Evidence and Search Query

1.Scan Activity



```
index="botsv1" imreallynotbatman.com sourcetype="stream:http"
```

✓ 22,200 events (8/10/16 3:28:51.000 AM to 12/11/23 8:50:15.000 PM)

8/10/16 { [-]

SELECTED FIELDS

a eventtype	3
a form_data	100+
a host	1
a part_filename{}	2
a source	1
a sourcetype	1
a src_ip	2
a uri_path	100+
a uri_query	100+
a url	100+
a user	1

INTERESTING FIELDS

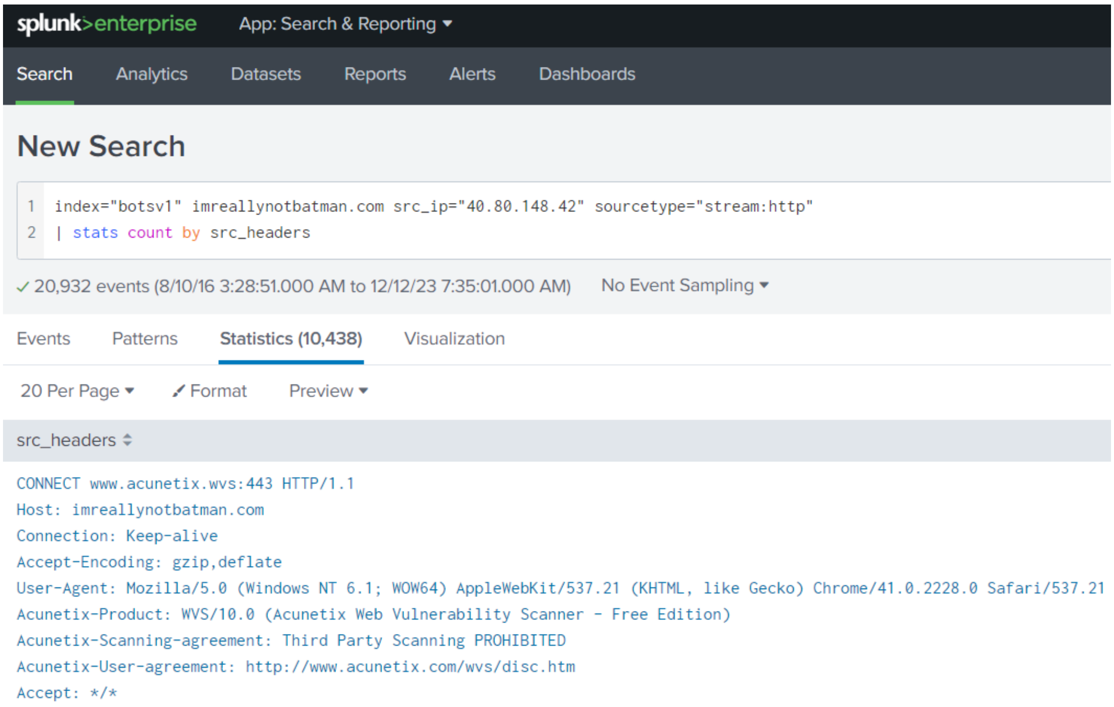
src_ip

2 Values, 99.856% of events

Selected [✓ Yes] No

Values	Count	%
40.80.148.42	20,932	94.424%
23.22.63.114	1,236	5.576%

2. The Name Tool used in enumeration



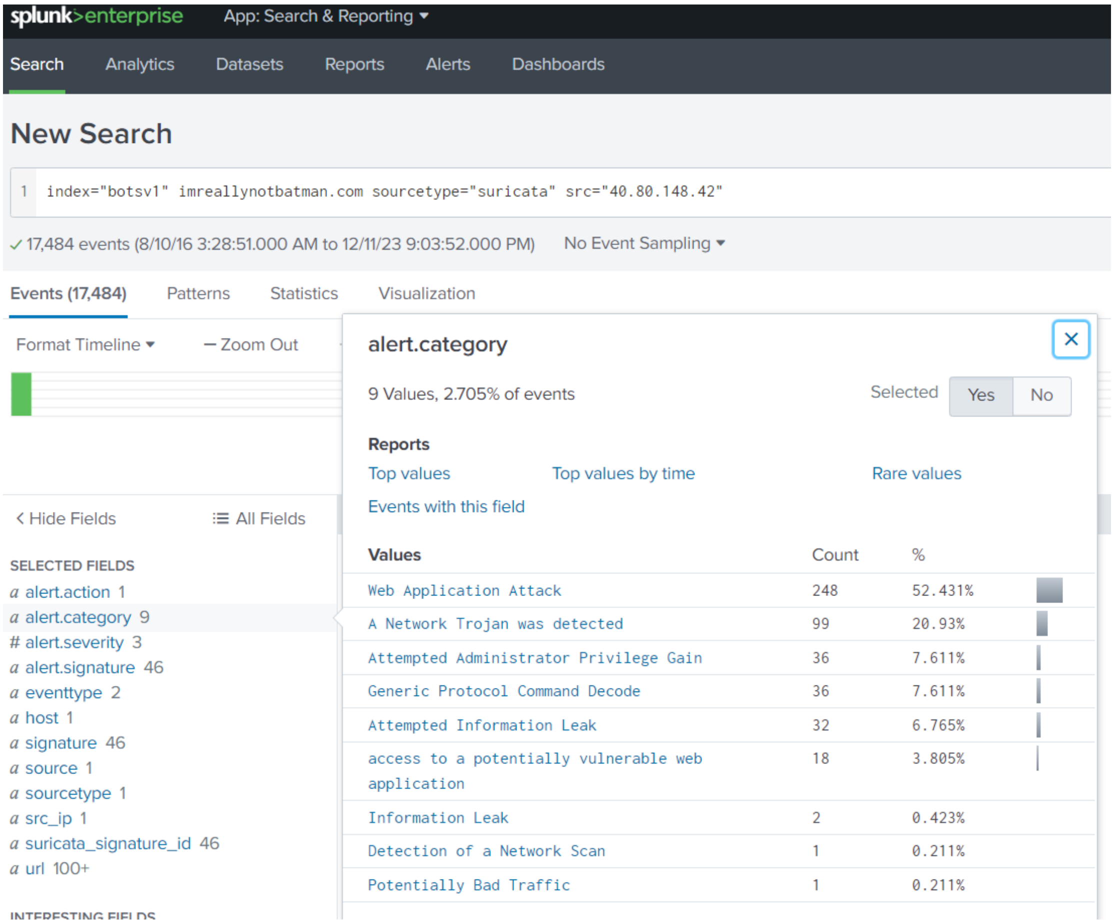
```
index="botsv1" imreallynotbatman.com src_ip="40.80.148.42" sourcetype="stream:http"
| stats count by src_headers
```

✓ 20,932 events (8/10/16 3:28:51.000 AM to 12/12/23 7:35:01.000 AM) No Event Sampling ▾

src_headers

```
CONNECT www.acunetix.wvs:443 HTTP/1.1
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: */*
```

3.Web Application Attack



```
index="botsv1" imreallynotbatman.com sourcetype="suricata" src="40.80.148.42"
```

✓ 17,484 events (8/10/16 3:28:51.000 AM to 12/11/23 9:03:52.000 PM) No Event Sampling ▾

SELECTED FIELDS
a alert.action 1
a alert.category 9
# alert.severity 3
a alert.signature 46
a eventtype 2
a host 1
a signature 46
a source 1
a sourcetype 1
a src_ip 1
a suricata_signature_id 46
a url 100+

INTERESTING FIELDS

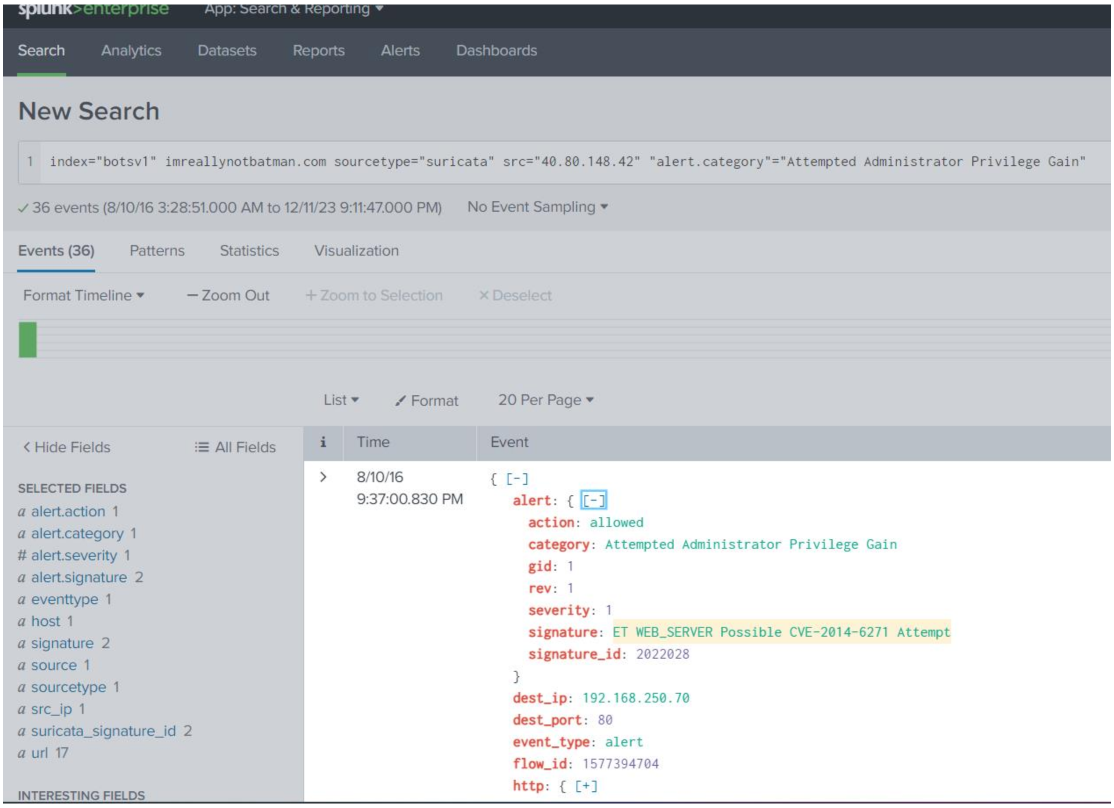
alert.category

9 Values, 2.705% of events Selected Yes No

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

Values	Count	%
Web Application Attack	248	52.431%
A Network Trojan was detected	99	20.93%
Attempted Administrator Privilege Gain	36	7.611%
Generic Protocol Command Decode	36	7.611%
Attempted Information Leak	32	6.765%
access to a potentially vulnerable web application	18	3.805%
Information Leak	2	0.423%
Detection of a Network Scan	1	0.211%
Potentially Bad Traffic	1	0.211%

3. Attempted Administrator Privilege Gain



New Search

```
index="botsv1" imreallynotbatman.com sourcetype="suricata" src="40.80.148.42" "alert.category"="Attempted Administrator Privilege Gain"
```

✓ 36 events (8/10/16 3:28:51.000 AM to 12/11/23 9:11:47.000 PM) No Event Sampling

Events (36)

SELECTED FIELDS

a alert.action	1
a alert.category	1
# alert.severity	1
a alert.signature	2
a eventtype	1
a host	1
a signature	2
a source	1
a sourcetype	1
a src_ip	1
a suricata_signature_id	2
a url	17

INTERESTING FIELDS

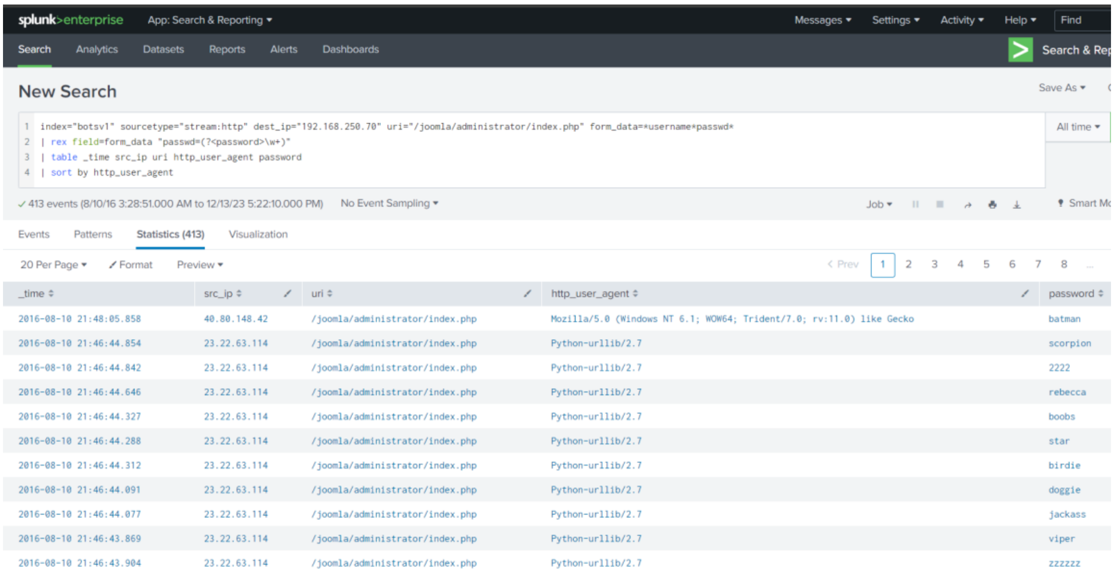
i	Time	Event
>	8/10/16 9:37:00.830 PM	

```
{ [-]
   alert: { [-]
     action: allowed
     category: Attempted Administrator Privilege Gain
     gid: 1
     rev: 1
     severity: 1
     signature: ET WEB_SERVER Possible CVE-2014-6271 Attempt
     signature_id: 2022028
   }
   dest_ip: 192.168.250.70
   dest_port: 80
   event_type: alert
   flow_id: 1577394704
   http: { [+]
```

2- Exploitation Phase

The Attacker Perform Brute Forse Attack for the Exploitation

- The Evidence and Search Query



```
index="botsv1" sourcetype="stream:http" dest_ip="192.168.250.70" uri="/joomla/administrator/index.php" form_data=*username*passwd*
| rex field=form_data "passwd=(?<password>\w+)"
| table _time src_ip uri http_user_agent password
| sort by http_user_agent
```

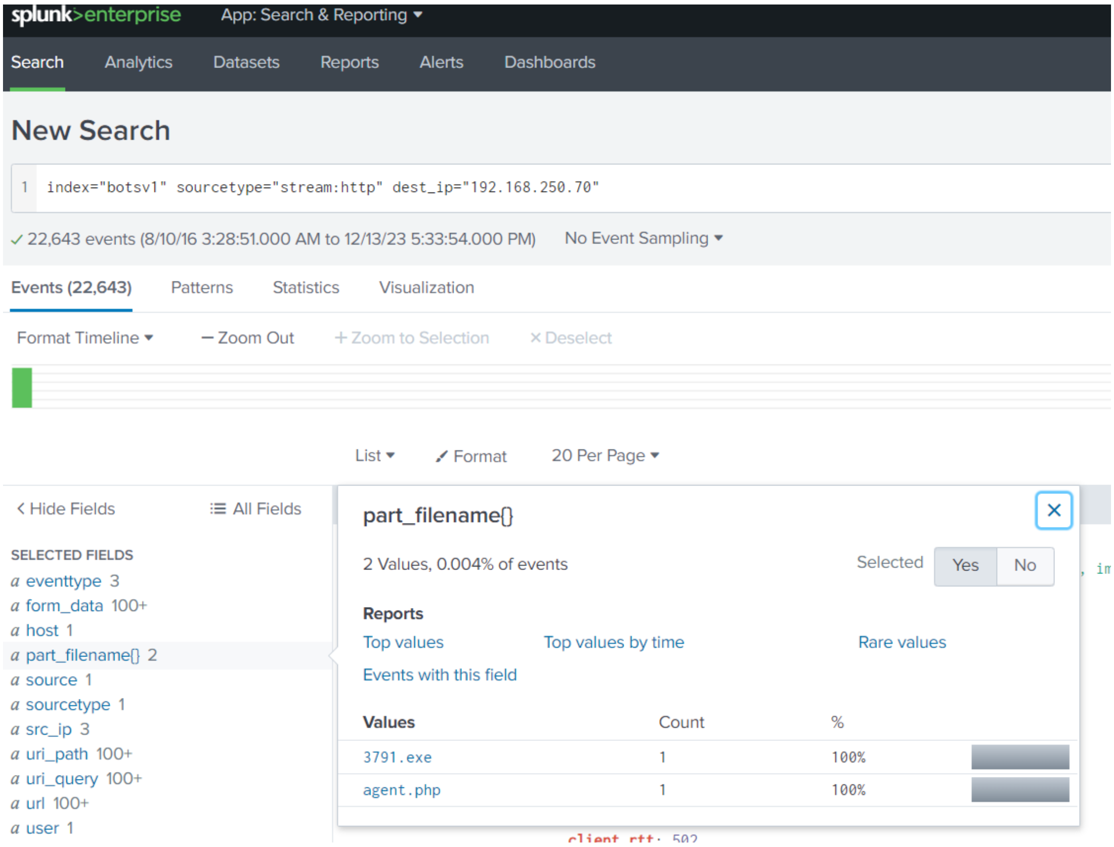
✓ 413 events (8/10/16 3:28:51.000 AM to 12/13/23 5:22:10.000 PM) No Event Sampling ▾

_time	src_ip	uri	http_user_agent	password
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 21:46:44.854	23.22.63.114	/joomla/administrator/index.php	Python-urllib/2.7	scorpion
2016-08-10 21:46:44.842	23.22.63.114	/joomla/administrator/index.php	Python-urllib/2.7	2222
2016-08-10 21:46:44.646	23.22.63.114	/joomla/administrator/index.php	Python-urllib/2.7	rebecca
2016-08-10 21:46:44.327	23.22.63.114	/joomla/administrator/index.php	Python-urllib/2.7	boobs
2016-08-10 21:46:44.288	23.22.63.114	/joomla/administrator/index.php	Python-urllib/2.7	star
2016-08-10 21:46:44.312	23.22.63.114	/joomla/administrator/index.php	Python-urllib/2.7	birdie
2016-08-10 21:46:44.091	23.22.63.114	/joomla/administrator/index.php	Python-urllib/2.7	doggie
2016-08-10 21:46:44.077	23.22.63.114	/joomla/administrator/index.php	Python-urllib/2.7	jackass
2016-08-10 21:46:43.869	23.22.63.114	/joomla/administrator/index.php	Python-urllib/2.7	viper
2016-08-10 21:46:43.904	23.22.63.114	/joomla/administrator/index.php	Python-urllib/2.7	zzzzzz

3- Installation Phase

The Attacker Install Executable file in the server.

- The Evidence and search query



```
index="botsv1" sourcetype="stream:http" dest_ip="192.168.250.70"
```

✓ 22,643 events (8/10/16 3:28:51.000 AM to 12/13/23 5:33:54.000 PM)

SELECTED FIELDS

a eventtype	3
a form_data	100+
a host	1
a part_filename{}	2
a source	1
a sourcetype	1
a src_ip	3
a uri_path	100+
a uri_query	100+
a url	100+
a user	1

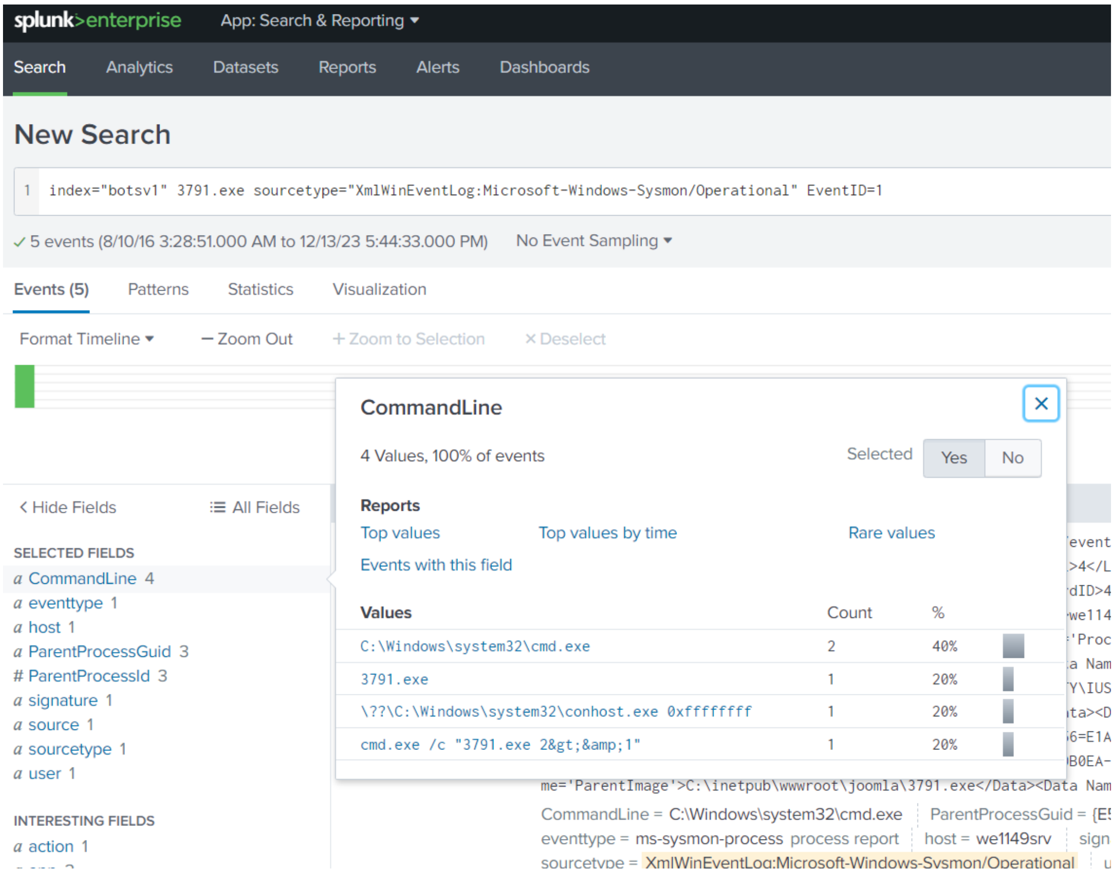
part_filename{}

2 Values, 0.004% of events

Selected [✓ Yes] No

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

client_rtt: 502



New Search

```
index="botsv1" 3791.exe sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" EventID=1
```

✓ 5 events (8/10/16 3:28:51.000 AM to 12/13/23 5:44:33.000 PM) No Event Sampling ▾

SELECTED FIELDS
- *a* CommandLine 4
- *a* eventtype 1
- *a* host 1
- *a* ParentProcessGuid 3
- # ParentProcessId 3
- *a* signature 1
- *a* source 1
- *a* sourcetype 1
- *a* user 1

INTERESTING FIELDS
- *a* action 1

CommandLine

4 Values, 100% of events

Selected [✓ Yes] No

Reports

Values	Count	%
C:\Windows\system32\cmd.exe	2	40%
3791.exe	1	20%
\??\C:\Windows\system32\conhost.exe 0xffffffff	1	20%
cmd.exe /c "3791.exe 2&gt;&amp;1"	1	20%

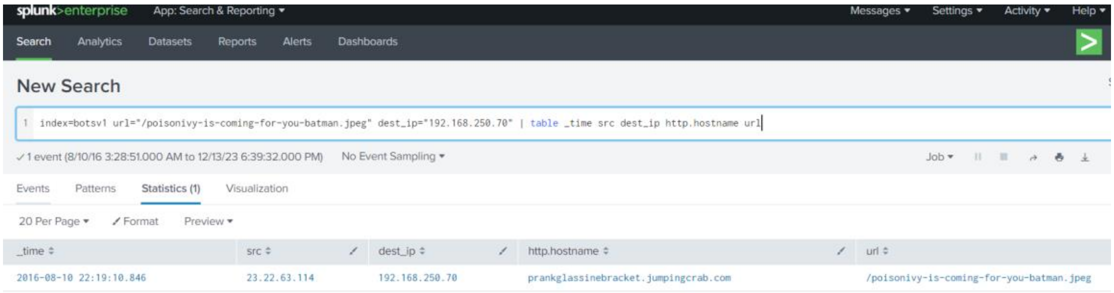
```
'event
>4</L
dID>4
we114
'Proc
a Nam
Y\IUS
ta><D
6=E1A
B0EA-
me='ParentImage'>C:\inetpub\wwwroot\joomla\3791.exe</Data><Data Nam
```

CommandLine = C:\Windows\system32\cmd.exe | ParentProcessGuid = {E5
eventtype = ms-sysmon-process process report | host = we1149srv | sign
sourcetype = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | u

4- Action on Objective

The attacker Defaced the Web Site

- The Evidence and search query



New Search

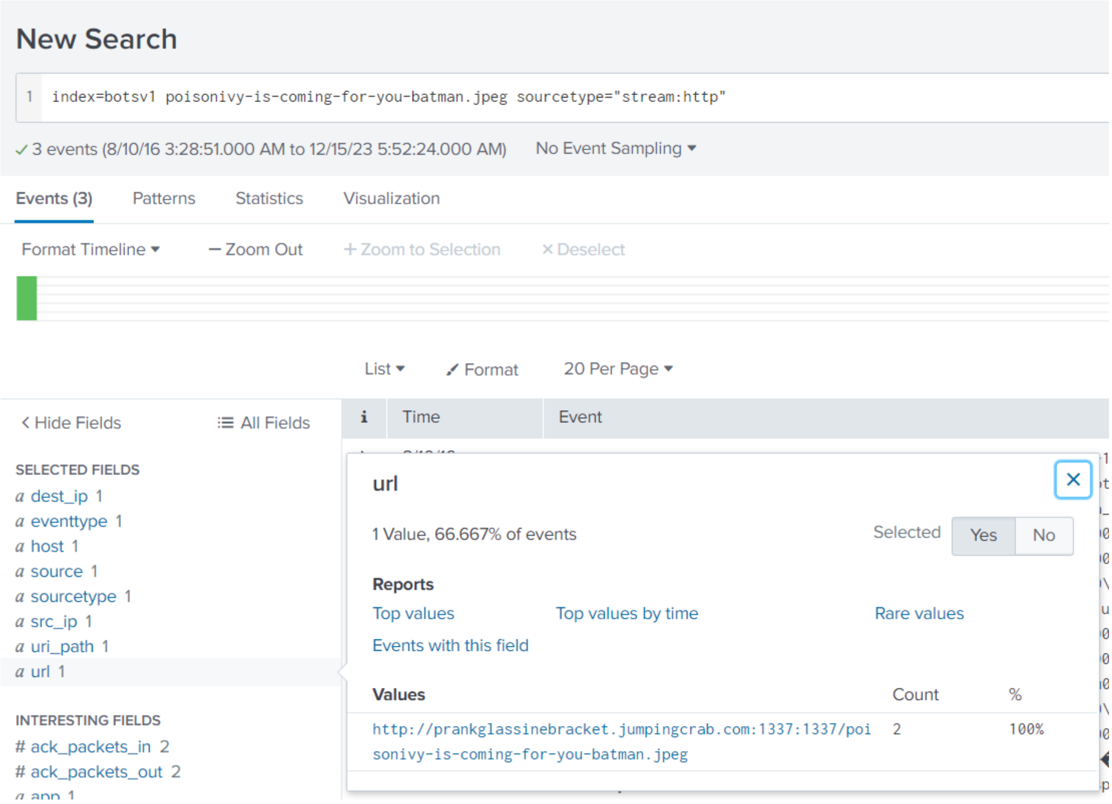
```
index=botsv1 url="/poisonivy-is-coming-for-you-batman.jpeg" dest_ip="192.168.250.70" | table _time src dest_ip http.hostname url
```

✓1 event (8/10/16 3:28:51.000 AM to 12/13/23 6:39:32.000 PM) No Event Sampling ▾

_time	src	dest_ip	http.hostname	url
2016-08-10 22:19:10.846	23.22.63.114	192.168.250.70	prankglassinebracket.jumpingcrab.com	/poisonivy-is-coming-for-you-batman.jpeg

5- Command And Control

identified the suspicious domain as a Command and Control C2 Server in the Previous Phase associated with the image.



New Search

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

✓3 events (8/10/16 3:28:51.000 AM to 12/15/23 5:52:24.000 AM) No Event Sampling ▾

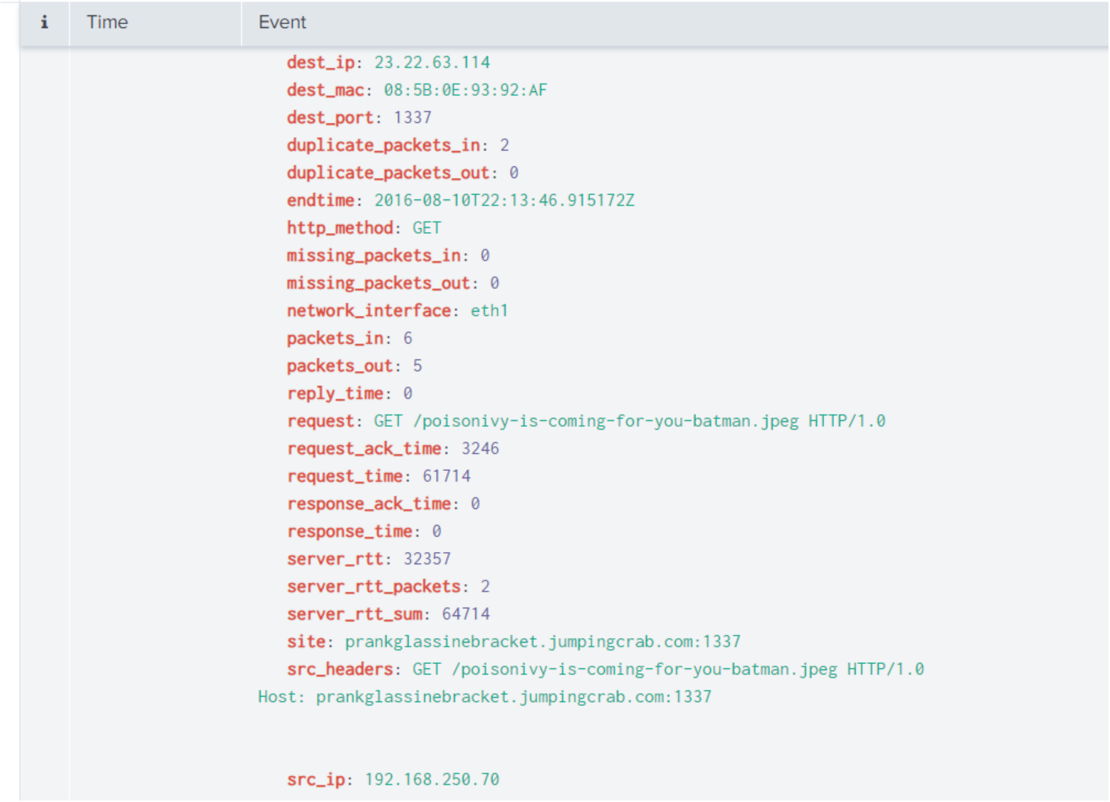
SELECTED FIELDS
a dest_ip 1
a eventtype 1
a host 1
a source 1
a sourcetype 1
a src_ip 1
a uri_path 1
a url 1

INTERESTING FIELDS
# ack_packets_in 2
# ack_packets_out 2
a app 1

url

1 Value, 66.667% of events

Values	Count	%
http://prankglassinebracket.jumpingcrab.com:1337:1337/poisonivy-is-coming-for-you-batman.jpeg	2	100%



```
   dest_ip: 23.22.63.114
   dest_mac: 08:5B:0E:93:92:AF
   dest_port: 1337
   duplicate_packets_in: 2
   duplicate_packets_out: 0
   endtime: 2016-08-10T22:13:46.915172Z
   http_method: GET
   missing_packets_in: 0
   missing_packets_out: 0
   network_interface: eth1
   packets_in: 6
   packets_out: 5
   reply_time: 0
   request: GET /poisonivy-is-coming-for-you-batman.jpeg HTTP/1.0
   request_ack_time: 3246
   request_time: 61714
   response_ack_time: 0
   response_time: 0
   server_rtt: 32357
   server_rtt_packets: 2
   server_rtt_sum: 64714
   site: prankglassinebracket.jumpingcrab.com:1337
   src_headers: GET /poisonivy-is-coming-for-you-batman.jpeg HTTP/1.0
Host: prankglassinebracket.jumpingcrab.com:1337


   src_ip: 192.168.250.70
```

6- Weaponization Phase And 7- Delivery Phase

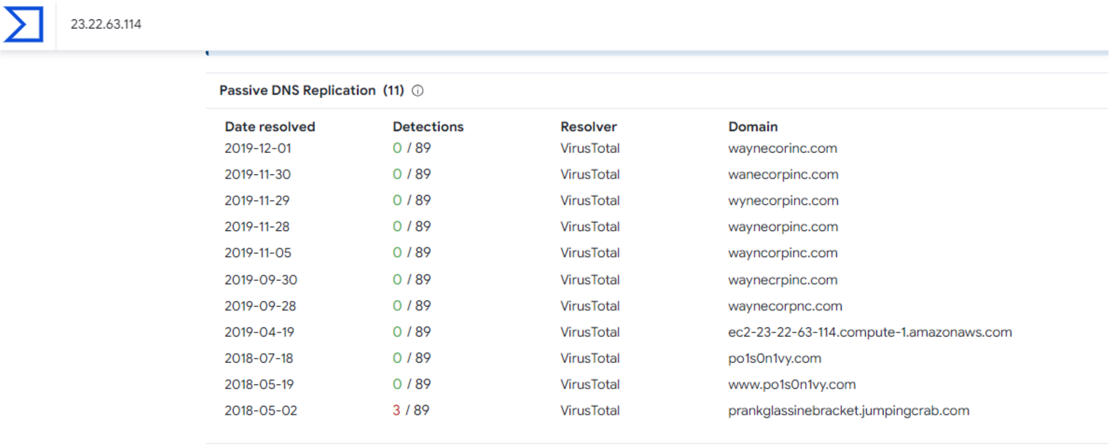
Using OSINT www.virustotal.com to search for IP Address Associated with the attacker 23.22.63.114

The Malicious Domain name associate with the IP: www.po1s0n1vy.com

The Malicious file name:

ab.exe

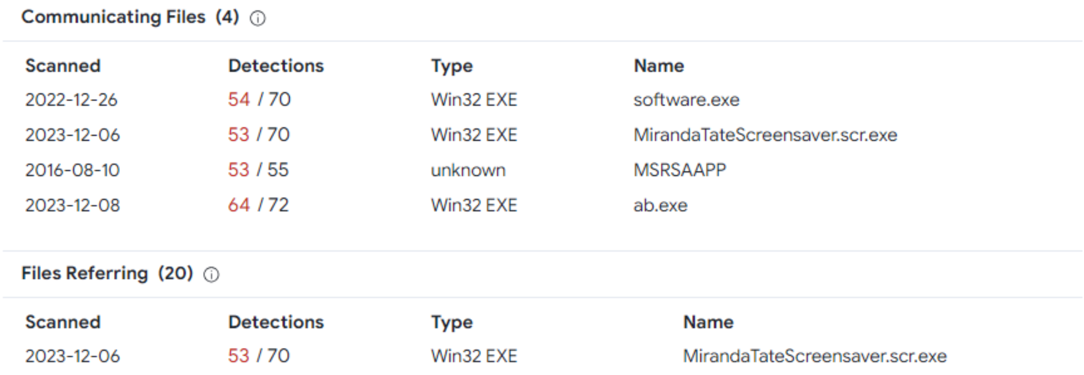
Miranda.Tate.Screenserver.scr.exe



23.22.63.114

Passive DNS Replication (11)

Date resolved	Detections	Resolver	Domain
2019-12-01	0 / 89	VirusTotal	waynecorinc.com
2019-11-30	0 / 89	VirusTotal	wanecorpinc.com
2019-11-29	0 / 89	VirusTotal	wynecorpinc.com
2019-11-28	0 / 89	VirusTotal	wayneorpinc.com
2019-11-05	0 / 89	VirusTotal	wayncorpinc.com
2019-09-30	0 / 89	VirusTotal	waynecrpinc.com
2019-09-28	0 / 89	VirusTotal	waynecorpnc.com
2019-04-19	0 / 89	VirusTotal	ec2-23-22-63-114.compute-1.amazonaws.com
2018-07-18	0 / 89	VirusTotal	po1s0n1vy.com
2018-05-19	0 / 89	VirusTotal	www.po1s0n1vy.com
2018-05-02	3 / 89	VirusTotal	prankglassinebracket.jumpingcrab.com



Communicating Files (4)

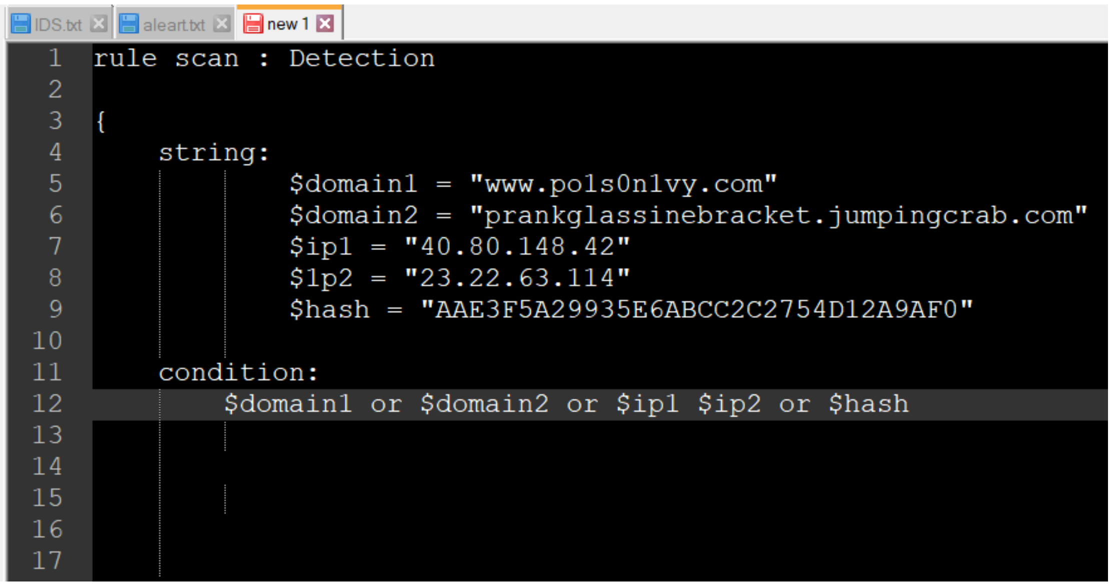
Scanned	Detections	Type	Name
2022-12-26	54 / 70	Win32 EXE	software.exe
2023-12-06	53 / 70	Win32 EXE	MirandaTateScreensaver.scr.exe
2016-08-10	53 / 55	unknown	MSRSAAPP
2023-12-08	64 / 72	Win32 EXE	ab.exe

Files Referring (20)

Scanned	Detections	Type	Name
2023-12-06	53 / 70	Win32 EXE	MirandaTateScreensaver.scr.exe

Part Tow Creating Yara Rule

Collecting the artifact IP Addresses and domains and Hash File Associated with the attacker and creating Yara Rule



```
rule scan : Detection

{
    string:
            $domain1 = "www.po1s0n1vy.com"
            $domain2 = "prankglassinebracket.jumpingcrab.com"
            $ip1 = "40.80.148.42"
            $1p2 = "23.22.63.114"
            $hash = "AAE3F5A29935E6ABCC2C2754D12A9AF0"

    condition:
        $domain1 or $domain2 or $ip1 $ip2 or $hash
```