

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`.

Search | Splunk 8.2.4

10.10.135.101/en-US/app/search/search?earliest=0&latest=&q=search index%3Dbotsv1 imreallynotbatman.com&display_page.search.mode=verbose&dispatch.sample_ra...

TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef Revshell Generator Reverse Shell Cheat S... GitHub - swisskyrepo/...

index=botsv1 imreallynotbatman.com

78,683 events (before 11/16/22 12:17:31.000 AM) No Event Sampling

Events (78,683) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 minute per column

Hide Fields All Fields

SELECTED FIELDS

- # host 4
- # source 4
- # sourcetype 4

INTERESTING FIELDS

- # ack_packets_in 41
- # ack_packets_out 12
- # app 5
- # app_proto 1
- # bytes 100+
- # bytes_in 100+
- # bytes_out 100+
- # c_ip 3
- # cached 2
- # capture_hostname 1
- # client_rtt 100+
- # client_rtt_packets 27
- # client_rtt_sum 100+
- # connection_type 4
- # cookie 100+
- # cs_content_length 100+
- # cs_content_type 15
- # cs_version[] 1
- # data_center_time 100+
- # data_packets_in 8

sourcetype

4 Values, 100% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
suricata	30,625	38.922%
stream:http	22,200	28.214%
fortigate-utm	13,918	17.689%
iis	11,940	15.175%

src_ip: 192.168.250.70
src_port: 80
timestamp: 2016-08-10T16:23:09.473182-0600

Show as raw text

host = suricata-ids.waynecorpinc.local | source = /var/log/suricata/eve.json | sourcetype = suricata

> 8/10/16 10:22:27.614 PM { [-]
ack_packets_in: 0
ack_packets_out: 0
bytes: 834
bytes_in: 0
bytes_out: 834
c_ip: 40.80.148.42

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

Search | Splunk 8.2.4

10.10.135.101/en-US/app/search/search?earliest=0&latest=&q=search index%3Dbotsv1 imreallynotbatman.c

TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef Revshell Generator Reverse Shell Cheat S... GitHub - swisskyrepo/...

Hide Fields All Fields List Format 20 Per Page

a http_method 6
a http_referrer 98
a http_user_agent 52
a index 1
linecount 1
a location 100+
missing_packets_in 2
missing_packets_out 3
a network_interface 1
packets_in 25
packets_out 22
a punct 65
reply_time 100+
request 100+
request_ack_time 100+
request_time 100+
response_ack_time 100+
response_time 100+
a sc_date 100+
a server 2
server_rtt 100+
server_rtt_packets 8
server_rtt_sum 100+
a site 39
a splunk_server 1
a src_content 100+
a src_headers 100+
a src_ip 2
a src_mac 1
src_port 100+
status 11
time_taken 100+
timeendpos 1
a timestamp 100+
timestamppos 1
a transport 1
a uri 100+
a uri_path 100+

i Time Event

Date: Wed, 10 Aug 2016 22:22:27 GMT
Content-Length: 395

src_ip: 40.80.148.42
src_mac: 08:5B:0E:93:92:AF
src_port: 49491
status: 303
time_taken: 0
timestamp: 2016-08-10T22:22:27.614541Z
transport: tcp
uri:
uri_path:

Show as raw text

host = splunk-02 | source = stream:http | sourcetype = stream:http

> 8/10/16 10:22:27.612 PM { [-]
accept: /*/*

src_ip

2 Values, 84.315% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
40.80.148.42	17,483	93.402%
23.22.63.114	1,235	6.598%

cs_content_length: 78
cs_content_type: application/x-www-form-urlencoded
cs_version: [[+]
data_center_time: 1070125

c. Checking on the first IP

< Hide Fields

All Fields

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

List

Format

20 Per Page

i

Time

Event

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

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

1 index=botsv1 imreallynotbatman.com src=40.80.148.42 sourcetype=suricata All time

✓ 17,484 events (before 11/17/22 4:04:59.000 PM) No Event Sampling Job

Events (17,484) Patterns Statistics Visualization

Format Timeline Zoom Out

1 minute per column

6 7 8 ... Next

Hide Fields All Fields

SELECTED FIELDS

- a alert.action 1
- a alert.category 9
- a alert.signature 46
- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS

- a app 1
- a app_proto 1
- # bytes 100+
- # date_hour 2
- # date_mday 1
- # date_minute 43
- a date_month 1
- # date_second 60

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%

host = suricata-ids.waynecorpinc.local source = /var/log/suricata/eve.json sourcetype = suricata

a file_state 2

a file_stored 1

file_tx_id 100+

a fileinfo.filename 68

fileinfo.size 100+

a fileinfo.state 2

a fileinfo.stored 1

fileinfo.tx_id 100+

a filename 68

flow_id 100+

a http.hostname 34

a http.http_content_type 15

a http.http_method 9

a http.http_refer 98

a http.http_user_agent 48

http.length 100+

a http.protocol 2

a http.redirect 100+

http.status 11

a http.url 100+

a http_content_type 15

a http_method 9

a http_protocol 2

a http_referrer 98

a http_user_agent 48

a ids_type 1

a in_iface 1

a index 1

linecount 1

a product 1

a proto 1

date_minute 43

a date_month 1

date_second 60

a date_wday 1

date_year 1

date_zone 1

a dest 34

a dest_ip 2

dest_port 2

a dvc 1

a event_type 3

a eventtype 2

file_size 100+

a file_state 2

a file_stored 1

file_tx_id 100+

http_user_agent

48 Values, 99.977% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Top 10 Values	Count	%
Mozilla/5.0 (Windows NT 6.1; WOW64)	17,329	99.136%
AppleWebKit/537.21 (KHTML, like Gecko)		
Chrome/41.0.2228.0 Safari/537.21		
Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko	103	0.589%
(select(0)from(select(sleep(9)))v)/*+	2	0.011%
(select(0)from(select(sleep(9)))v)/*+		
(select(0)from(select(sleep(9)))v)/*+		
Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) Version/6.0 Mobile/10A5376e Safari/8536.25	2	0.011%
!(())&&! *	1	0.006%
";print(md5(acunetix_wvs_security_test));\$a="	1	0.006%
\$(nslookup 0GiavBmt)	1	0.006%
\$(10000071+9999854)	1	0.006%
\$(@print(md5(acunetix_wvs_security_test)))	1	0.006%
\$(@print(md5(acunetix_wvs_security_test)))\	1	0.006%

dest_ip

2 Values, 100% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
192.168.250.70	17,483	99.994%
192.168.250.40	1	0.006%

tx_id: 1

Hide Fields

All Fields

SELECTED FIELDS

a alert.action 1
a alert.category 1
a alert.signature 2
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS

a action 1
alert.gid 1
alert.rev 2
alert.severity 1
alert.signature_id 2
alert_gid 1
alert_rev 2
bytes 2
a category 1
date_hour 1

Time

Event

8/10/16
9:37:00.830 PM

{ [-]
 alert: { [+]
 }
 dest_ip: 192.168.250.70
 dest_port: 80
 event_type: alert
 flow_id: 1577394704
 http: { [+]
 }
 in_iface: eth1
 proto: TCP
 src_ip: 40.80.148.42
 src_port: 49214
 timestamp: 2016-08-10T15:37:00.830090-0600
 }
Show as raw text
alert.action = allowed alert.category = Attempted Administrator Privilege Gain
alert.signature = ET WEB_SERVER Possible CVE-2014-6271 Attempt
host = suricata-ids.waynecorpinc.local source = /var/log/suricata/eve.json sourcetype = suricata

2. Exploitation Phase

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

New Search

Save As Create Table View Close

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

All time

22,200 events (before 11/17/22 4:28:16.000 PM) No Event Sampling

Job

Verbose Mode

Select visualization

Patterns

Statistics (2)

Visualization

Pie Chart

Format

Trellis

23.22.63.114

40.80.148.42

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

a sc_date 100+
a server 2
server_rtt 100+
server_rtt_packets 8
server_rtt_sum 100+
a site 93
a splunk_server 1
a src_content 100+
a src_headers 100+
a src_ip 3
a src_mac 1
src_port 100+
status 12
time_taken 100+
timeendpos 1
a timestamp 100+
timestartpos 1
a transport 1
a uri 100+

server_rtt: 0

src_ip

3 Values, 94.644% of events

Selected Yes No

Reports

Top values
Top values by time
Rare values

Events with this field

Values	Count	%
40.80.148.42	17,546	91.438%
23.22.63.114	1,429	7.447%
192.168.2.50	214	1.115%

Trident/4.0

image/png, */*

src_port: 46538

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

```

a dest_ip 1
a dest_mac 1
# dest_port 1
# duplicate_packets_in 12
# duplicate_packets_out 16
a endtime 100+
a form_data 100+
a http_comment 100+
# http_content_length 100+
a http_content_type 14
a http_method 6
a http_referrer 100+
a http_user_agent 100+
a index 1
# linecount 1
a location 100+
# missing_packets_in 2
# missing_packets_out 3
a network_interface 1
# packets_in 25
# packets_out 22

```

http_method			Selected <input type="button" value="Yes"/> <input type="button" value="No"/>	
6 Values, 99.738% of events				
Reports				
Top values	Top values by time	Rare values		
Events with this field				
Values	Count	%		
POST	14,238	70.408%		
GET	5,976	29.552%		
OPTIONS	5	0.025%		
CONNECT	1	0.005%		
PROPFIND	1	0.005%		
TRACE	1	0.005%		

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

2016-08-10 21:51:36.474	/joomla/administrator /index.php	40.80.148.42	192.168.250.70	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&a09349d0d6dbf078ad72cf8e9348583=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

1
index=botsv1 sourcetype=stream:http dest_ip="192.168.250.70" *.exe
All time

17 events (before 11/17/22 5:25:39.000 PM) No Event Sampling
Job
Verbose Mode

Events (17) Patterns Statistics Visualization

Format Timeline
Zoom Out Zoom to Selection Deselect
1 day per column

Hide Fields
All Fields

SELECTED FIELDS
a host 1
a part_filename() 2
a source 1
a sourcetype 1

INTERESTING FIELDS
a accept 3
ack_packets_in 2
ack_packets_out 3
bytes 9

part_filename()
2 Values, 5.882% of events
Selected Yes No

Reports
Top values Top values by time Rare values

Events with this field

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

canceled: 1
capture_hostname: damn-01

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

1 index=botsv1 "3791.exe" sourcetype="XmlWinEventLog" EventCode=1 All time

5 events (before 11/17/22 5:54:33.000 PM) No Event Sampling

Events (5) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 minute per column

Hide Fields All Fields

SELECTED FIELDS

- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS

- a Channel 1
- a CommandLine 4
- a Computer 1
- a CurrentDirectory 2
- a dvc 1
- a dvc_nt_host 1
- # event_Id 5
- # EventCode 1
- a EventData_Xml 5
- # EventID 1
- # EventRecordID 5
- a eventtime 2

Time Event

CommandLine

4 Values, 100% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

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>&1"	1	20%

<Data Name="ParentImage">C:\inetpub\wwwroot\joomla\3791.exe</Data><Data Name="ParentCommandL

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 caused defacement."

that

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

timestamp: 2016-08-24T10:47:14.000602-0600

src

2 Values, 100% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
192.168.2.50	211	50.119%
192.168.250.70	210	49.881%

proto: TCP

src_ip: 192.168.250.70

src_port: 80

timestamp: 2016-08-24T10:47:06.004155-0600

json sourcetype = suricata

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

1 index=botsv1 src=192.168.250.70 sourcetype=suricata

All time

✓ 12,601 events (before 11/17/22 8:39:35.000 PM) No Event Sampling

Job

Events (12,601) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 day per column

List Format 20 Per Page

1 2 3 4 5 6 7 8 ... Next

< Hide Fields All Fields

SELECTED FIELDS

- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS

- a app 2
- a app_proto 2
- # bytes 100+
- # date_hour 5
- # date_mday 2
- # date_minute 60
- a date_month 1
- # date_second 60
- a date_wday 1
- # date_year 1
- # date_zone 1
- a dest 91
- a dest_ip 7
- # dest_port 100+
- a dvc 1
- a event_type 5
- # file_size 100+
- a file_state 2

Time Event

8/24/16 6:27:32.734 PM { [-]

dest_ip: 192.168.250.40

dest_port: 8089

event_type: tls

dest_ip

7 Values, 100% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
40.80.148.42	10,317	81.874%
23.22.63.114	1,294	10.269%
192.168.250.40	758	6.015%
192.168.2.50	214	1.698%
108.161.187.134	12	0.095%
192.168.250.255	3	0.024%
224.0.0.252	3	0.024%

src_ip: 192.168.250.70

c. We'll pivot into the dest_ip to see what traffic is carried out.

Des_IP: 23.22.63.114

a src 1

a src_ip 1

src_port 5

status 3

timeendpos 1

a timestamp 100+

timestartpos 1

a transport 1

a url 3

a vendor 1

46 more fields

+ Extract New Fields

8/10/16 { [-]

url

3 Values, 99.691% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
/joomla/administrator/index.php	1,235	95.736%
/joomla/agent.php	52	4.031%
/poisonivy-is-coming-for-you-batman.jpeg	3	0.232%

Show as raw text

host = suricata-ids.waynecorpinc.local source = /var/log/suricata/eve.json sourcetype = suricata

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.

New Search Save As Create Table View Close

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

✓ 1 event (before 11/17/22 8:47:28.000 PM) No Event Sampling Job

Events (1) Patterns **Statistics (1)** Visualization

20 Per Page Format Preview

_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 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.

New Search Save As Create Table View Close

1 index=botsv1 sourcetype=fortigate_utm"poisonivy-is-coming-for-you-batman.jpeg" All time

✓ 3 events (before 11/17/22 9:08:05.000 PM) No Event Sampling Job

Events (3) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 minute per column

List Format 20 Per Page

Time	Event
8/10/16 10:19:10.000 PM	Aug 10 16:19:10 192.168.250.1 date=2016-08-10 time=16:19:10 devname=gotham-fortigate devid=FGT6004614044725 logid=0317013312 type=utm subtype=webfilter eventtype=ftgd_allow level=notice vd="root" policyid=10 sessionid=932526 user="" srcip=192.168.250.70 srcport=51573 srcintf="internal3" dstip=23.22.63.114 dstport=1337 proto=6 service=HTTP hostname="prankglassinebracket.jumpingcrab.com:1337" profile="monitor-all" action=passthrough reqtype=direct url="/poisonivy-is-coming-for-you-batman.jpeg" sentbyte=106 rcvbyte=0 direction=N/A msg="URL belongs to an allowed category in policy" method=domain cat=26 catdesc="Malicious Websites" crscore=30 crlevel=high host = 192.168.250.1 : source = udp:514 : sourcetype = fortigate_utm
8/10/16 10:13:46.000 PM	Aug 10 16:13:46 192.168.250.1 date=2016-08-10 time=16:13:46 devname=gotham-fortigate devid=FGT6004614044725 logid=0317013312 type=utm subtype=webfilter eventtype=ftgd_allow level=notice vd="root" policyid=10 sessionid=930693 user="" srcip=192.168.250.70 srcport=63139 srcintf="internal3" dstip=23.22.63.114 dstport=1337 proto=6 service=HTTP hostname="prankglassinebracket.jumpingcrab.com:1337" profile="monitor-all" action=passthrough reqtype=direct url="/poisonivy-is-coming-for-you-batman.jpeg" sentbyte=106 rcvbyte=0 direction=N/A msg="URL belongs to an allowed category in policy" method=domain cat=26 catdesc="Malicious Websites" crscore=30 crlevel=high host = 192.168.250.1 : source = udp:514 : sourcetype = fortigate_utm
8/10/16 10:06:21.000 PM	Aug 10 16:06:21 192.168.250.1 date=2016-08-10 time=16:06:21 devname=gotham-fortigate devid=FGT6004614044725 logid=0317013312 type=utm subtype=webfilter eventtype=ftgd_allow level=notice vd="root" policyid=10 sessionid=928318 user="" srcip=192.168.250.70 srcport=56504 srcintf="internal3" dstip=23.22.63.114 dstport=1337 proto=6 service=HTTP hostname="prankglassinebracket.jumpingcrab.com:1337" profile="monitor-all" action=passthrough reqtype=direct url="/poisonivy-is-coming-for-you-batman.jpeg" sentbyte=106 rcvbyte=0 direction=N/A msg="URL belongs to an allowed category in policy" method=domain cat=26 catdesc="Malicious Websites" crscore=30 crlevel=high host = 192.168.250.1 : source = udp:514 : sourcetype = fortigate_utm

Selected fields: a host 1, a source 1, a sourcetype 1

Interesting fields: a action 1, a app 1, # bytes 1, # bytes_in 1, # bytes_out 1, # cat 1, a catdesc 1, a category 1, a crlevel 1, # crscore 1, a date 1, # date_hour 1, # date_mday 1, # date_minute 3, # date_month 1, # date_second 3

Selected fields: a tag 1, a tag::eventtype 1, a time 3, # timeendpos 1, # timestartpos 1, a transport 1, a type 1, a url 1, a url_domain 1, a vd 1, a vendor 1, a vendor_action 1, a vendor_eventtype 1, a vendor_product 1, a vendor_url 1

url

1 Value, 100% of events Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
prankglassinebracket.jumpingcrab.com:1337/poisonivy-is-coming-for-you-batman.jpeg	3	100%

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)

```
canceled: 1
capture_hostname: demo-01
client_rtt: 1
client_rtt_packets: 1
client_rtt_sum: 1
cs_version: 1.0
data_center_time: 0
data_packets_in: 2
data_packets_out: 0
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
src_mac: 00:0C:29:C4:02:7E
src_port: 63139
time_taken: 61715
timestamp: 2016-08-10T22:13:46.853458Z
transport: tcp
uri: /poisonivy-is-coming-for-you-batman.jpeg
uri_path: /poisonivy-is-coming-for-you-batman.jpeg
}
Show as raw text
host = splunk-O2 | source = stream:http | sourcetype = stream:http
```

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`

pranklassinebracket.jumpingcrab.comGO

Click "Download" To Continue
Get Manuals with Web Search By Manual Maestro
WebSearchByManualMaestroDownload

ANALYSIS QUICK INFO REVERSE (NEW) RECORDS SEO WOT ALEXA THREATMINER SHARED GRAPH HISTORY WHOIS DNSBL GRAPH(oid)

ANALYSIS
This section shows a quick analysis of the given host name or ip number.
Results found
Jumpingcrab.com.

QUICK INFO
Quick summary of the host name
pranklassinebracket.jumpingcrab.com quick info

General	
FQDN	pranklassinebracket.jumpingcrab.com
Host Name	pranklassinebracket
Domain Name	jumpingcrab.com
Registry	com
TLD	com
Domain DNS	
Name servers	ns1.afraid.org ns2.afraid.org ns3.afraid.org ns4.afraid.org
Mail servers	mail.jumpingcrab.com
IP Numbers	69.197.18.183 70.39.97.227 169.47.130.85

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

23.22.63.114

Sage Rutty
A Century of Trust
Creating and Preserving Wealth for Generations

DirectionsWebsite

ANALYSIS QUICK INFO REVERSE (NEW) IPINFO.IO RECORDS THREATMINER SHARED GRAPH HISTORY WHOIS DNSBL GRAPH(oid)

ANALYSIS
This section shows a quick analysis of the given host name or ip number.
23.22.63.114 has one PTR.
PTR
The PTR is ec2-23-22-63-114.compute-1.amazonaws.com. The IP number is in Ashburn, United States. It is hosted by Amazon EC2 IAD prefix.
We investigated eight host names that point to 23.22.63.114. Example: ec2-23-22-63-114.compute-1.amazonaws.com, waynecorpinc.com, waynecorpnc.com and wanecorpinc.com.

QUICK INFO
Quick summary of the host name
23.22.63.114 quick info

DNS	
PTR	ec2-23-22-63-114.compute-1.amazonaws.com

REVERSE (NEW!)
Reverse DNS reports of the queried and related entities
Please login to see this section

d. Lets investigate the po1s0nivy.com

www.po1s0n1vy.com

0 / 96

No security vendors flagged this domain as malicious

www.po1s0n1vy.com
po1s0n1vy.com
dga

Registrar: GoDaddy.com, LLC
Creation Date: 2 years ago
Last Updated: 15 days ago

DETECTION DETAILS RELATIONS COMMUNITY 4

Passive DNS Replication (3)

Date resolved	Detections	Resolver	IP
2021-09-03	2 / 96	VirusTotal	34.102.136.180
2018-08-30	1 / 96	VirusTotal	91.195.240.117
2018-05-19	0 / 96	VirusTotal	23.22.63.114

Siblings (4)

ftp.po1s0n1vy.com	0 / 95	64.29.151.221
illian.po1s0n1vy.com	0 / 95	64.29.151.221
illian.po1s0n1vy.com	0 / 96	64.29.151.221
smtp.po1s0n1vy.com	0 / 95	91.195.240.117 64.29.151.235

Historical Whois Lookups (3)

Last Updated	Registrar	Registrant
+ 2022-11-14	GoDaddy.com, LLC	-
+ 2022-04-23	GoDaddy.com, LLC	-
+ 2021-09-03	GoDaddy.com, LLC	80315b2e6ac1a801 (US)

Graph Summary

e. Lets Use whois.domaintools.com to investigate the po1s0n1vy.com. We can see the name servers and IP addresses associated with the domain name.

IP

DomainTools PROFILE CONNECT MONITOR SUPPORT WHOIS

(P) 14806242505

Registrar Status	clientDeleteProhibited, clientRenewProhibited, clientTransferProhibited, clientUpdateProhibited
Dates	1,043 days old Created on 2020-01-09 Expires on 2023-01-09 Updated on 2022-01-10
Name Servers	NS37.DOMAINCONTROL.COM (has 59,928,212 domains) NS38.DOMAINCONTROL.COM (has 59,928,212 domains)
Tech Contact	Registration Private Domains By Proxy, LLC DomainsByProxy.com, Tempe, Arizona, 85284, us (p) 14806242599 (f) 14806242598
IP Address	34.102.136.180 - 29,089,734 other sites hosted on this server
IP Location	🇺🇸 - Missouri - Kansas City - Google
ASN	🇺🇸 AS396982 GOOGLE-PRIVATE-CLOUD, US (registered Aug 15, 2018)
Domain Status	Registered And Active Website
IP History	13 changes on 13 unique IP addresses over 6 years
Registrar History	2 registrars with 1 drop
Hosting History	12 changes on 8 unique name servers over 6 years
— Website	
Website Title	None given.
Whois Record (last updated on 2022-11-17)	

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

← → ↺ 🏠

🔒 https://www.threatminer.org/host.php?q=23.22.63.114 70% ☆

🔗 Kali Linux 🔗 Kali Linux 🌐 Kali Tools 📄 Kali Docs 🗉 Kali Forums 🛡️ Kali NetHunter 🔥 Exploit-DB 🗄️ Google Hacking DB 🛡️ OffSec

Copy Excel CSV PDF

Search:

MD5	Detections	Analysis Date
aae3f5a29935e6abcc2c2754d12a9af0	N/A	2019-05-30 16:36:52
39eecefa9a13293a93bb20036eaf1f5e	N/A	2019-02-12 17:13:29
c99131e0169171935c5ac32615ed6261	ALYac Trojan.GenericKD.3470547 AVG Agent5.APHV AVware Trojan.Win32.Generic!BT Ad-Aware Trojan.GenericKD.3470547 AegisLab Agent5.Aphv.Gen!c AhnLab-V3 Malware/Gen.Generic.N2081883700 Antiy-AVL Trojan[Backdoor]/Win32.Redsip Arcabit Trojan.Generic.D34F4D3 Avira TR/AD.Zupdax.qmyx BitDefender Trojan.GenericKD.3470547 DrWeb Trojan.MulDrop6.51432 ESET-NOD32 a variant of Win32/Korplug.HP Emsisoft Trojan.GenericKD.3470547 (B) F-Secure Trojan.GenericKD.3470547 Fortinet W32/Korplug.HP!tr GData Trojan.GenericKD.3470547 Ikarus Trojan.Win32.Korplug Jiangmin Backdoor.Redsip.f K7AntiVirus Trojan (004f0c211) K7GW Trojan (004f0c211)	2016-09-01 09:03:44

Sample: c99131e0169171935c5ac32615ed6261

Note: if you are new to ThreatMiner, check out the [how-to](#) page to find out **how** you can get the most out of this portal.

Search for domains, IPs, MD5[SHA1|SHA256, email address or APTnotes(aptnotes:), ssl(ssl:), user-agent(ua:), AV family(av:), filename (filename:), URI (uri:), registry (reg:), mutex (mute) 🔍

📄 Metadata

File name:	MirandaTateScreensaver.scr.exe
File type:	PE32 executable (console) Intel 80386, for MS Windows
File size:	494080 bytes
Analysis date:	2016-09-01 09:03:44
MD5:	c99131e0169171935c5ac32615ed6261
SHA1:	bc927ff06263351f43db8dec88e4b08485e07996
SHA256:	9709473ab351387aab9e816eff3910b9f28a7a70202e250ed46dba8f820f34a8
SHA512:	8fb3b09541b021e06ecec455876526607114adb547eacb7556d578c08959154b80f01bac905383a5eb4c8a9091a3fb14dc13badc36a05ea7718bf4b1053f2fdb
SSDEEP:	12288:JCy+DdcUrY4tO3Rc5F5H8q3/H5aRanZ0:jj+COpO3Rc5F5H8q3/yaRaZ0
IMPHASH:	fae2c8486a11f609323cc15c0ee838cf
Authentihash:	N/A
Related resources	<div>VirusTotal Hybrid-Analysis VirusShare</div>

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

9709473ab351387aab9e816eff3910b9f28a7a70202e250ed46dba8f820f34a8

50

71

Community Score

50 security vendors and no sandboxes flagged this file as malicious

9709473ab351387aab9e816eff3910b9f28a7a70202e250ed46dba8f820f34a8

482.50 KB

2022-11-11 00:16:07 UTC
6 days ago

detect-debug-environment direct-cpu-clock-access long-sleeps peexe spreader

DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 12

Security Vendors' Analysis

Ad-Aware	Gen:Variant.Doina.17144	AhnLab-V3	Malware/Gen.Generic.C1464467
Alibaba	Backdoor:Win32/Zupdax.4fc05470	ALYac	Gen:Variant.Doina.17144
Antiy-AVL	Trojan.Generic.ASMalwS.1B9D	Arcabit	Trojan.Doina.D42F8
Avast	Win32/Malware-gen	AVG	Win32/Malware-gen
Avira (no cloud)	TR/AD.Zupdax.qmyx	BitDefender	Gen:Variant.Doina.17144
BitDefenderTheta	Gen:NN.ZexaF.34784.EuW@amuHygei	Comodo	Malware@#orlqgcgfud1l
Cybereason	Malicious.016917	Cylance	Unsafe
Cynet	Malicious (score: 99)	DrWeb	Trojan.MulDrop6.51432
Elastic	Malicious (high Confidence)	Emsisoft	Gen:Variant.Doina.17144 (B)
eScan	Gen:Variant.Doina.17144	ESET-NOD32	A Variant Of Win32/Zupdax.E
Fortinet	W32/Korplug.HPltr	GData	Gen:Variant.Doina.17144
Google	Detected	Ikarus	Trojan.Win32.Korplug
Jiangmin	Backdoor.Redsip.f	K7AntiVirus	Trojan (004f0c211)
K7GW	Trojan (004f0c211)	Kaspersky	HEUR:Backdoor.Win32.Redsip.gen
Lionic	Trojan.Win32.Redsip.mlc	Malwarebytes	Malware.AI.3194230138
MAX	Malware (ai Score=100)	MaxSecure	Trojan.Malware.9833592.susgen
McAfee	Artemis/C99131E01691	McAfee-GW-Edition	BehavesLike.Win32.NetLoader.gh
Microsoft	Backdoor:Win32/Zupdax.Bldha	NANO-Antivirus	Trojan.Win32.Korplug.edojag

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



9709473ab351387aab9e816eff3910b9f28a7a70202e250ed46dba8f820f34a8



Community Score

50 security vendors and no sandboxes flagged this file as malicious

9709473ab351387aab9e816eff3910b9f28a7a70202e250ed46dba8f820f34a8

MirandaTateScreensaver.scr.exe

detect-debug-environment direct-cpu-clock-access long-sleeps peexe spreader

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 12

Contacted IP Addresses (14)

IP	Detections	Autonomous System	Country
13.107.4.50	0 / 96	8068	US
131.253.33.203	0 / 96	8068	US
192.168.0.12	1 / 96	-	-
192.168.0.141	0 / 96	-	-
20.62.24.77	0 / 96	8075	US
20.80.129.13	0 / 96	8075	US
20.99.132.105	0 / 96	8075	US
20.99.133.109	0 / 96	8075	US
20.99.184.37	0 / 96	8075	US
23.216.147.64	0 / 96	20940	US
23.216.147.76	0 / 96	20940	US
23.22.63.114	0 / 96	14618	US
23.223.54.145	0 / 95	20940	US
23.40.197.137	0 / 96	20940	US

Graph Summary

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

Incident Response

Risk Assessment

Network BehaviorContacts 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

Request Info

IP, Domain, Hash

MITRE ATT&CK™ Techniques Detection

Defense Evasion

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1027.002	Software Packing	<ul style="list-style-type: none"> Defense Evasion 	Adversaries may perform software packing or virtual machine software protection to conceal their code. Learn more			<ul style="list-style-type: none"> Matched Compiler/Packer signature

Credential Access

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1056.004	Credential API Hooking	<ul style="list-style-type: none"> Credential Access Collection 	Adversaries may hook into Windows application programming interface (API) functions to collect user credentials. Learn more		<ul style="list-style-type: none"> Installs hooks/patches the running process 	

Discovery

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1082	System Information Discovery	<ul style="list-style-type: none"> Discovery 	An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Learn more			<ul style="list-style-type: none"> Contains ability to read software policies

Download as CSV

Close

e. The file details

MirandaTateScreensaver.scr.exe

Filename

MirandaTateScreensaver.scr.exe

Size

483KiB (494080 bytes)

Type

peexe executable

Description

PE32 executable (console) Intel 80386, for MS Windows

Architecture

WINDOWS

SHA256

9709473ab351387aab9e816eff3910b9f28a7a70202e250ed46dba8f820f34a8

Compiler/Packer

VC8 -> Microsoft Corporation

PDB Timestamp

05/25/2016 07:39:35 (UTC)

PDB Pathway

Resources

Language

ENGLISH

Icon

Visualization

Input File (PortEx)

Classification (TrID)

- 41.0% (.EXE) Win32 Executable MS Visual C++ (generic)
- 36.3% (.EXE) Win64 Executable (generic)
- 8.6% (.DLL) Win32 Dynamic Link Library (generic)
- 5.9% (.EXE) Win32 Executable (generic)
- 2.6% (.EXE) OS/2 Executable (generic)

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.”