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.

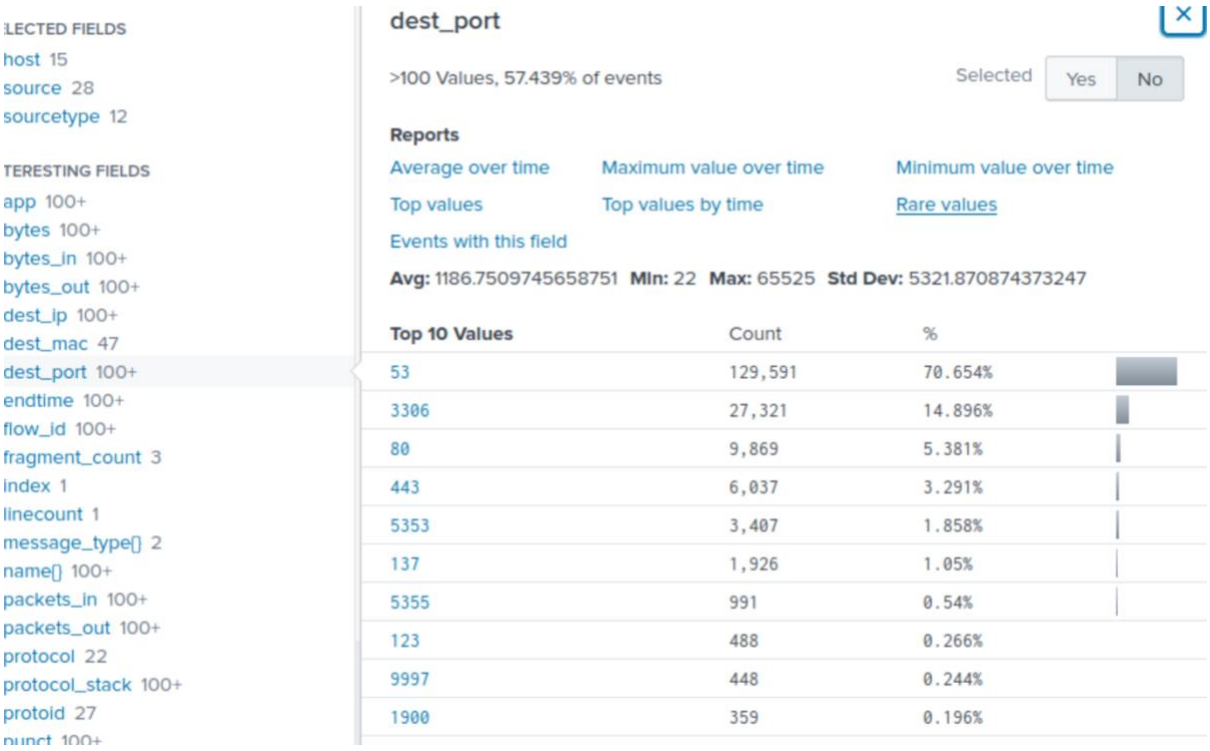
Question 1:
What port number did the adversary use to download their attack tools?

Answer: 3333

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

```
1  index=botsv3 sourcetype="stream:http"
```

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



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”.

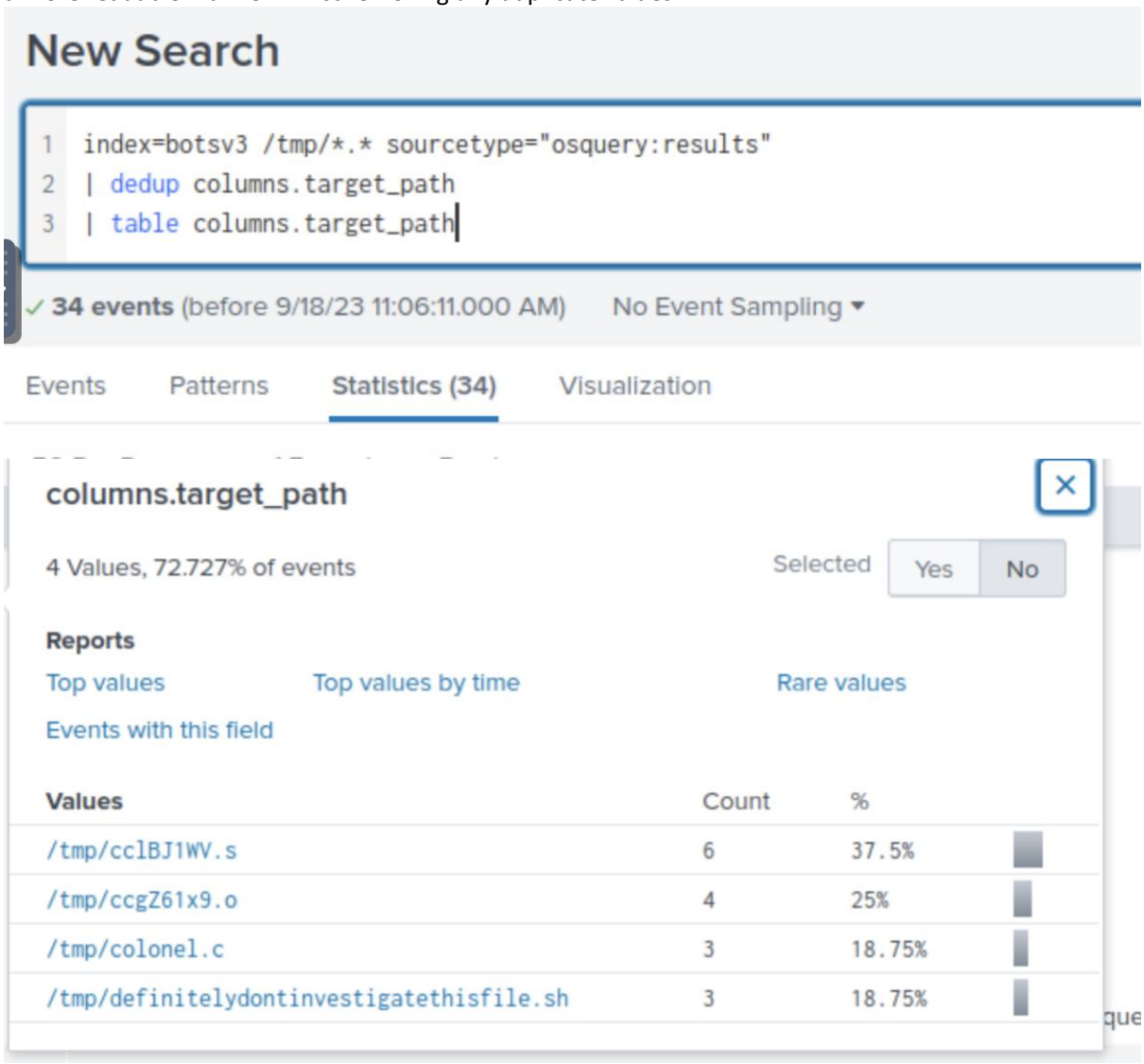
```
flow_id: e8947e90-2f4b-48eb-93e8-f0099d8f
http_comment: HTTP/1.1 200 OK
http_content_length: 5782482
http_content_type: image/png
http_method: GET
http_user_agent: Mozilla/5.0 (Windows NT
protocol_stack: ip:tcp:http
site: 45.77.53.176:3333
src_ip: 192.168.70.186
src_mac: 00:0C:29:55:51:1A
src_port: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

Question 3:

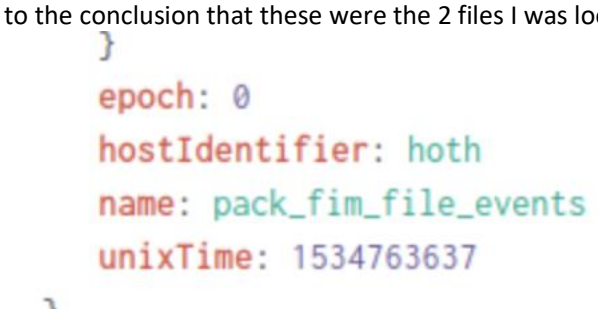
During the attack, two files are remotely streamed to the /tmp directory of the on-premises Linux server by the adversary. What are the names of these files? Answer guidance: Comma separated without spaces, in alphabetical order, include the file extension where applicable.

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.



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



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

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. ghoppy@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','tomsmit@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
intersted in discussing floral notes of peat and dirt in scottish ale',NULL,NULL,0),('d767c134-0327-6f28-5a14-5b4426f95e21','
```

Question 5:

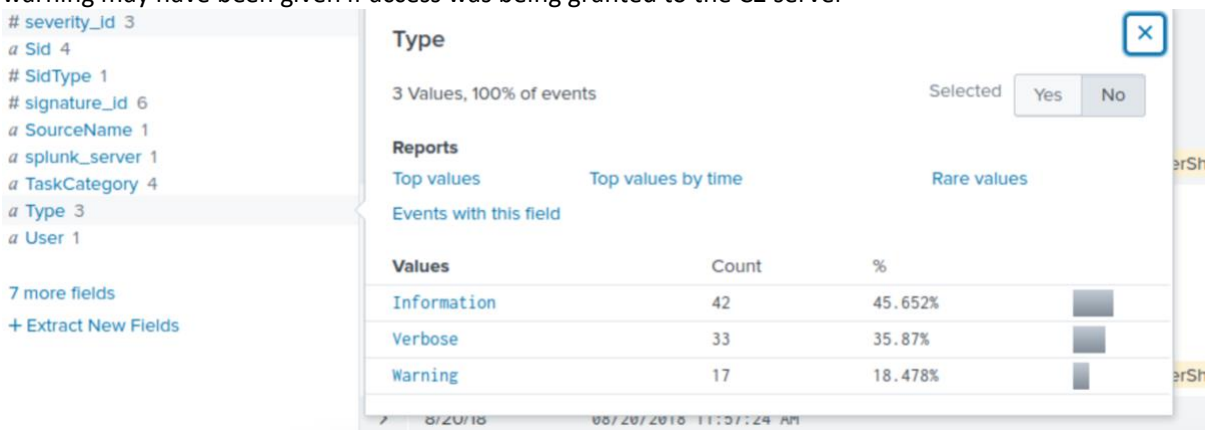
What is the path of the URL being accessed by the command and control server? Answer guidance: Provide the full path. (Example: The full path for the URL https://imgur.com/a/mAqgt4S/lasd3.jpg is /a/mAqgt4S/lasd3.jpg)

Answer: /admin/get.php

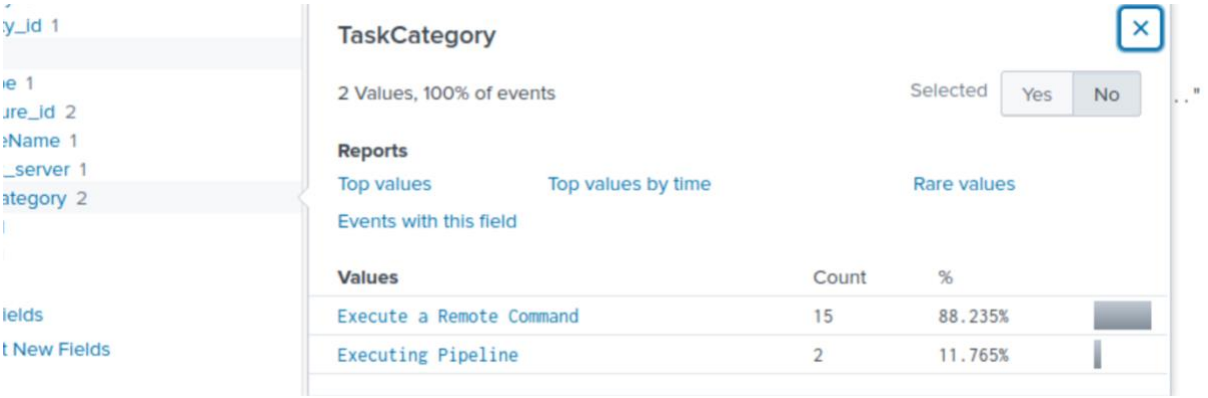
This one was challenging. The hint suggested looking at the source below and so I started there.

```
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



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



From there I investigated the events and found this suspicious encoded text. Now the reason I went deeper into this is that I previously had a task in another Splunk BOSS program very similar to this and the answer was hidden in the encoded text. So I selected the text and threw it into cyberchef to decode it using Base64

From there I scrolled down and found the URL which I highlighted below. Again if I hadn't had a task so similar to this prior I probably wouldn't of gone down this route. I looked into some other individuals and some of them went down a different path to successfully find the answer

Question 6:

At least two Frothly 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.