

Splunk 2

Platform: tryhackme

From: Asem Reda

Diploma: Cybersecurity 87


Challenge link: <https://tryhackme.com/room/splunk2gcd5>

The screenshot shows the 'Splunk 2' room interface on TryHackMe. At the top, it says 'Learn > Splunk 2' and 'Premium room'. Below this is a 'Boss of the SOC' logo and a description: 'Part of the Blue Primer series. This room is based on version 2 of the Boss of the SOC (BOTS) competition by Splunk.' It also shows a progress bar, a timer for 45 minutes, and a user count of 29,280. A row of buttons includes 'Share your achievement', 'Start AttackBox', 'Save Room', '674 Recommend', and 'Options'. A green bar indicates 'Room completed (100%)'. Below this is a list of tasks, all marked as completed with green checkmarks:

- Task 1: Deploy!
- Task 2: Dive into the data
- Task 3: 100 series questions
- Task 4: 200 series questions
- Task 5: 300 series questions
- Task 6: 400 series questions
- Task 7: Conclusion

Task 1: Deploy!

Task 1: Deploy!



Start Machine

BOTSV2 Dataset

The data included in this app was generated in August of 2017 by members of Splunk's Security Specialist team: Dave Herrald, Ryan Knapp, Steve Grant, Jim Agger, John Stinner, Ken Wertz, David Vane and James Brodsky. They stood up a few lab environments connected to the internet. Within the environment they had a few Windows endpoints instrumented with the Splunk Universal Forwarder and Splunk Shims. The forwarders were configured with best practices for Windows endpoint monitoring, including a full Microsoft Sysmon deployment and best practices for Windows Event logging. The environment included a Palo Alto Networks user generator Splunk to capture traffic and provide web proxy services, and tools to provide network based IDS.

Note: This information is from the **Advanced Hunting APTs with Splunk** app.

BOTSV2 Github: <https://github.com/splunk/botsv2>

It is recommended that you complete the Splunk 181 room before attempting this room.

Room Machine

Before moving forward, deploy the Splunk virtual machine.

From the AttackBox, open Firefox Web Browser and navigate to the Splunk instance (http://machine_01:8000).

You may need to refresh the page until Splunk loads. This can take up to five minutes to launch.

Task 2: Dive into the data

In this exercise, you assume the persona of Alice Bluebird, the analyst who successfully assisted Wayne Enterprises and was recommended to Grace Hoppy at Frothy (a beer company) to assist them with their recent issues.

What Kinds of Events Do We Have?

The SPL (Splunk Search Processing Language) command metadata can be used to search for the same kind of information that is found in the Data Summary, with the bonus of being able to search within a specific index, if desired. All time-values are returned in EPOCH time, so to make the output user readable, the eval command should be used to provide more human-friendly formatting.

In this example, we will search the botsv2 index and return a listing of all the source types that can be found as well as a count of events and the first time and last time seen.

Resources:

- <http://docs.splunk.com/Documentation/Splunk/latest/SearchReference/Metadata>
- <https://www.splunk.com/blog/2017/07/31/metadata-metalore.html>

Metadata command:

```
| metadata type=sourcetypes index=botsv2 | eval firstTime=strftime(firstTime,"%Y-%m-%d %H:%M:%S") | eval lastTime=strftime(lastTime,"%Y-%m-%d %H:%M:%S") | eval recentTime=strftime(recentTime,"%Y-%m-%d %H:%M:%S") | sort - totalCount
```

Note: This information is from the **Advanced Hunting APTs with Splunk** app.

Task 3: 100 series questions

Amber Turing was hoping for Frothy to be acquired by a potential competitor which fell through, but visited their website to find contact information for their executive team. What is the website domain that she visited?

✓ Correct Answer

Amber found the executive contact information and sent him an email. What image file displayed the executive's contact information? Answer example: /path/image.ext

✓ Correct Answer

What is the CEO's name? Provide the first and last name.

✓ Correct Answer

What is the CEO's email address?

✓ Correct Answer

After the initial contact with the CEO, Amber contacted another employee at this competitor. What is that employee's email address?

✓ Correct Answer

What is the name of the file attachment that Amber sent to a contact at the competitor?

✓ Correct Answer

What is Amber's personal email address?

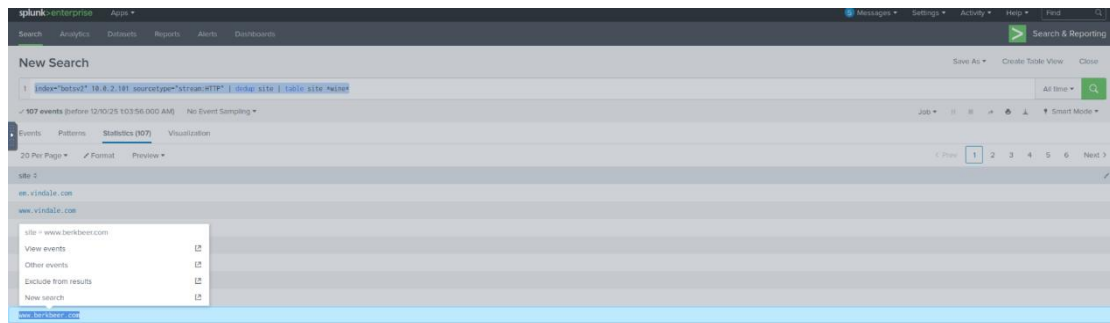
✓ Correct Answer 🔍

Solution method:

First, we need to get Amber's IP address. We'll do this by using the filter `index="botsv2" amber index="botsv2" sourcetype="pan:traffic"`, then going to the `src_ip` list. We'll find it there, and it's 10.0.2.101, When you scroll down to the sender_email field, you will find her email address, which is aturing@frothy.ly

First question:

We will use the filter `[index="botsv2" 10.0.2.101 sourcetype="stream:HTTP" | dedup site | table site *wine*]` to display the name of the site visited

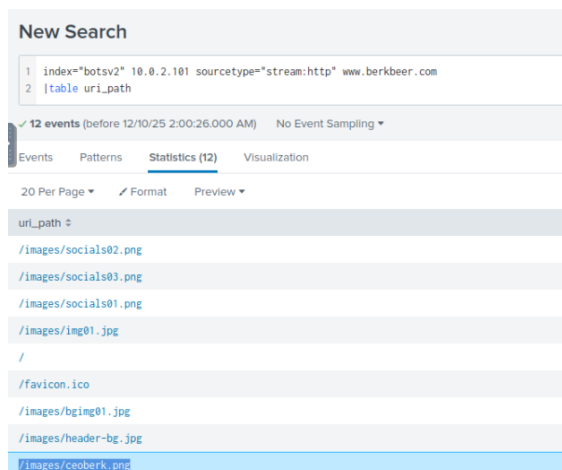


Second question:

We will use this filter to find the image file `[index="botsv2" 10.0.2.101 sourcetype="stream:http" www.berkbeer.com`

`|table uri_path]`

We will find it is `/images/ceoberk.png` because this is what belongs to ceo



Third question:

We will use this filter to find the CEO's email address: `index="botsv2" sourcetype="stream:smtp" berkbeer.com aturing@froth.ly`. We will scroll down to `sender_email` and find it is `mberk@berkbeer.com`. Therefore, the CEO's name is Martin Berk

Fourth question:

Using the same steps, we will find the CEO's email address , mberk@berkbeer.com

```
sender: mberk@berkbeer.com
sender_email: mberk@berkbeer.com
return: 250 2.0.0 OK: queued
```

Fifth question:

Using the same filter as the previous question, we will go down to receiver_email and find that the email address is hbernhard@berkbeer.com

```
]
receiver_email: [ [-]
  hbernhard@berkbeer.com
]
```

Sixth question:

Using the same filter as the previous question, we will go to attach_disposition and find that the filename is Saccharomyces_cerevisiae_patent.docx

The screenshot shows a network traffic analysis tool interface. The top section displays a search filter: `index="botsv2" sourcetype="stream:smtp" berkbeer.com aturing@froth.ly`. Below this, there are tabs for Events (4), Patterns, Statistics, and Visualization. The Events tab is active, showing a list of events. The selected event is expanded, showing details for an email attachment. The details include: `ack_packets_in: 0`, `ack_packets_out: 31`, `attach_content_decoded_md5_hash: [[+]`, `attach_content_md5_hash: [[+]`, `attach_disposition: [[+]`, and `attach_filename: [[-]`. The filename is `Saccharomyces_cerevisiae_patent.docx`.

Seventh question:

We will use the filter `index="botsv2" amber`, then scroll down to content_body, then take the base64 hash and go to a website to decode it, for example, <https://www.base64decode.org/>, then the email will appear

The screenshot shows a network traffic analysis tool interface. The top section displays a search filter: `index="botsv2" amber`. Below this, there are tabs for Events (4), Patterns, Statistics, and Visualization. The Events tab is active, showing a list of events. The selected event is expanded, showing details for an email attachment. The details include: `ack_packets_in: 0`, `ack_packets_out: 31`, `attach_content_decoded_md5_hash: [[+]`, `attach_content_md5_hash: [[+]`, `attach_disposition: [[+]`, and `attach_filename: [[-]`. The filename is `Saccharomyces_cerevisiae_patent.docx`.

The screenshot shows a website for base64 decoding. The input field contains a long base64 string. The output field shows the decoded email content. The email is from `hbernhard@berkbeer.com` to `aturing@froth.ly`. The subject is `Hiernz Bernhard Contact Information`. The body of the email says: "Hello Amber, Great talking with you today, here is my contact information. Do you have a personal email I can reach you at as well?"

Task 4: 200 series questions

What version of TOR Browser did Amber install to obfuscate her web browsing? Answer guidance: Numeric with one or more delimiter.

7.0.4 ✓ Correct Answer 5

What is the public IPv4 address of the server running www.brewertalk.com?

52.42.208.228 ✓ Correct Answer 5

Provide the IP address of the system used to run a web vulnerability scan against www.brewertalk.com.

45.77.65.211 ✓ Correct Answer 5

The IP address from Q42 is also being used by a likely different piece of software to attack a URI path. What is the URI path? Answer guidance: Include the leading forward slash in your answer. Do not include the query string or other parts of the URI. Answer example: /phpinfo.php

/phpinfo.php ✓ Correct Answer

What SQL function is being abused on the URI path from the previous question?

concatenate ✓ Correct Answer 5

What was the value of the cookie that Kevin's browser transmitted to the malicious URL, as part of an XSS attack? Answer guidance: All digits. Not the cookie name or symbols like an equal sign.

100000000 ✓ Correct Answer 5

What brewertalk.com username was maliciously created by a spear phishing attack?

kingfisher ✓ Correct Answer 5

First question:

We will use the filter `index="botsv2" amber tor`, then we will go to the app field in Interesting Fields. We will find the version number, which is 7.0.4

New Search

1 `index="botsv2" amber tor`

✓ 325 events (before 12/10/25 3:35:25.000 AM) No Event Sampling ▼

Events (325) Patterns Statistics Visualization

Format Timeline ▼ Zoom Out + Zoom to Selection X Deselect

< Hide Fields All Fields

SELECTED FIELDS

- host 1
- source 4
- sourcetype 4

INTERESTING FIELDS

app

4 Values, 43.692% of events Selected Yes No

Reports

- Top values
- Top values by time
- Rare values

Events with this field

Values	Count	%
C:\Users\amber.turing\Downloads\torbrowser-	124	87.324%
install-7.0.4-en-US.exe		

Second question:

We will use the filter `index="botsv2" sourcetype="stream:HTTP" "brewertalk.com"`

`|table dest_ip, site, uri_path` to find the IP address, and it will be the first one:
52.42.208.228

New Search

1 `index="botsv2" sourcetype="stream:HTTP" "brewertalk.com"`

2 `|table dest_ip, site, uri_path`

✓ 11,082 events (before 12/10/25 3:48:07.000 AM) No Event Sampling ▼

Events Patterns Statistics (11,082) Visualization

20 Per Page ▼ Format Preview ▼

dest_ip	site
52.42.208.228	www.brewertalk.com

Third question:

We will use the filter `index="botsv2" sourcetype="stream:HTTP" "brewertalk.com"`

Then we will go to Selected Fields and open `src_ip`. We will find that the IP address is `45.77.65.211`

The screenshot shows the 'New Search' interface in Splunk. The search bar contains the query: `index="botsv2" sourcetype="stream:HTTP" "brewertalk.com"`. Below the search bar, it indicates 11,082 events. The 'Selected Fields' list on the left includes `src_ip`. The 'src_ip' field is selected, and a pop-up window displays the 'Top values' for this field. The table shows the following data:

Values	Count	%
45.77.65.211	8,966	90.847%
52.40.10.231	317	3.184%
172.31.10.10	303	3.043%
71.39.18.125	133	1.336%
174.209.13.154	125	1.255%
10.0.2.109	90	0.904%
136.0.2.138	17	0.171%
136.0.0.125	6	0.06%

Fourth question:

We will use the filter `index="botsv2" sourcetype="stream:HTTP" 45.77.65.211`. Then we go to the Interesting Fields list and scroll down to `uri_path`. We will find that `/member.php`

The screenshot shows the 'Interesting Fields' list on the left, with `uri_path` selected. A pop-up window displays the 'Top 10 Values' for this field. The table shows the following data:

uri_path	Count	%
/member.php	662	7.383%
/search.php	164	1.829%
/	47	0.524%
/admin/	6	0.067%
/Debian-exin/	4	0.045%
/bakdd.html	4	0.045%
/apache/	4	0.045%
/archive/	4	0.045%
/backup/	4	0.045%
/cache/	4	0.045%

Fifth question:

We will use the filter `index="botsv2" sourcetype="stream:HTTP" 45.77.65.211 "uri_path="/member.php`

`|dedup form_data`

`|table form_data`

And we will find that the SQL function being abused on the URI path is **updatexml**

Task 5: 300 series questions

Answer the questions below

Mallory's critical PowerPoint presentation on her MacBook gets encrypted by ransomware on August 18. What is the name of this file after it was encrypted?

✓ Correct Answer

There is a Games of Thrones movie file that was encrypted as well. What season and episode is it?

✓ Correct Answer 6

Kevin Lagerfeld used a USB drive to move malware onto kutekitten, Mallory's personal MacBook. She ran the malware, which obfuscates itself during execution. Provide the vendor name of the USB drive Kevin likely used. Answer Guidance: Use time correlation to identify the USB drive.

✓ Correct Answer

What programming language is at least part of the malware from the question above written in?

✓ Correct Answer

When was this malware first seen in the wild? Answer Guidance: YYYY-MM-DD

✓ Correct Answer

The malware infecting kutekitten uses dynamic DNS destinations to communicate with two C&C servers shortly after installation. What is the fully-qualified domain name (FQDN) of the first (alphabetically) of these destinations?

✓ Correct Answer

From the question above, what is the fully-qualified domain name (FQDN) of the second (alphabetically) contacted C&C server?

✓ Correct Answer

First question:

Initially, we will use the filter index="botstv2" host="MACLORY-AIR13" (*.ppt OR *.pptx)

Then, the name of the critical presentation file will appear on the first line.

_Frothly_marketing_campaign_Q317.pptx.crypt

[illegible]

Second question:

First, we'll use the filter `index="botsv2" host="MACLORY-AIR13" *.crypt`. Then we'll see the season and episode, which will be S07E02

[illegible]

Third question:

First, we'll use the filter index="botsv2" kutekitten "\\users\\mkraeusen", then go to Selected Fields and choose sourcetype

then osquery_results

New Search

1 index="botsv2" kutekitten "\\users\\mkraeusen"

✓ 300 events (before 12/10/25 6:55:17.000 AM) No Event Sampling

Events (300) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

Hide Fields All Fields

SELECTED FIELDS

- calendarTime 22
- columns.path 17
- columns.pid 100+
- columns.target_path 1
- host 1
- source 1
- sourcetype 1

INTERESTING FIELDS

- action 2
- columns.key 2
- columns.value 2
- rtime hour 11

Time Event

8/29/17 11:10:15.000 AM action: added

sourcetype

1 Value, 100% of events

Reports

- Top values
- Top values by time
- Events with this field

Values

osquery_results

Then we go to columns.target_path and select the first option

columns.target_path

1 Value, 1,667% of events

Selected Yes No

Reports

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

Values

	Count	%
/Users/mkraeusen/Downloads	5	100%
Important_IR_Info_for_mkraeusen		

Then we go down to the last event, take the hash, and go to VirusTotal to verify it

b6f9b648b244c64db096522b4fd73fd1eakc4d3323fcbdeeb1ba08271

36/58 security vendors flagged this file as malicious

Reanalyze Similar More

lpsaud

Size 13.18 KB Last Analysis Date 3 months ago

Community Score -286

sets-process-name ssh detect-debug-environment malware check-hostname ssh-communication check-cpu-name exploit

First, we'll change the event time to the last minute. Then, we'll use the keyword "usb". Next, we'll take "model_id":"6387" and "vendor_id":"058f" and go to the DeviceHunt website to retrieve the USB name

index="botsv2" kutekitten usb

2 events (8/3/17 6:16:10.000 PM to 8/3/17 6:20:07.001 PM) No Event Sampling

Events (2) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

Hide Fields All Fields

SELECTED FIELDS

- calendarTime 1
- host 1
- source 1
- sourcetype 1

INTERESTING FIELDS

- action 2

Time Event

8/3/17 6:16:10.000 PM

8/3/17 6:15:10.000 PM

action: removed

calendarTime: Thu Aug 31 18:18:18 2017 UTC

columns: [{}]

Device Details

Type	Information
ID	6387

Vendor Details

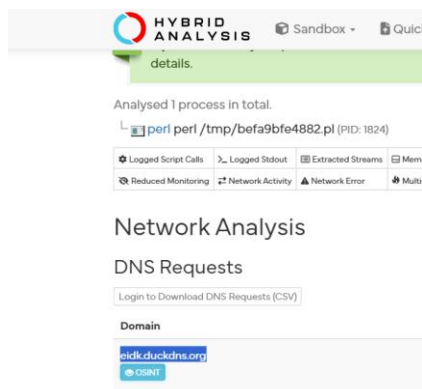
Alcor Micro Corp.

Go back to VirusTotal, then go to Details, and you will find the answer. perl



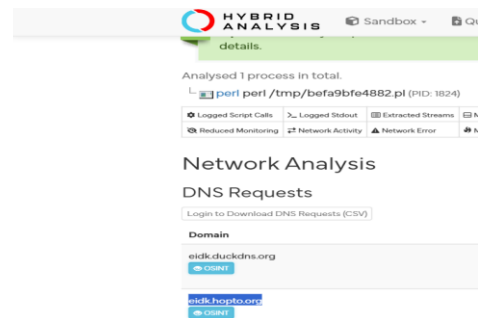
History ⓘ	
First Seen In The Wild	2017-01-17 19:09:06 UTC
First Submission	2017-01-31 16:54:15 UTC
Last Submission	2025-03-17 23:18:35 UTC
Last Analysis	2025-09-09 08:44:27 UTC

Go to the hybrid-analysis website. Then enter the hash and scroll down to Network Analysis. You will find the answer at eidk.duckdns.org



Seventh question:

In the same way as the previous question, you will find the answer below: eidk.hopto.org



Task 6: 400 series questions

A Federal law enforcement agency reports that Taedonggang often spear phishes its victims with zip files that have to be opened with a password. What is the name of the attachment sent to Frothy by a malicious Taedonggang actor?

invoice.zip ✓ Correct Answer

What is the password to open the zip file?

912345678 ✓ Correct Answer

The Taedonggang APT group encrypts most of their traffic with SSL. What is the "SSL Issuer" that they use for the majority of their traffic? Answer guidance: Copy the field exactly, including spaces.

C = US ✓ Correct Answer

What unusual file (for an American company) does winsys32.dll cause to be downloaded into the Frothy environment?

나는 데이비드를 사랑한다.hwp ✓ Correct Answer

What is the first and last name of the poor innocent sap who was implicated in the metadata of the file that executed PowerShell Empire on the first victim's workstation? Answer example: John Smith

Ryan Kovar ✓ Correct Answer

Within the document, what kind of points is mentioned if you found the text?

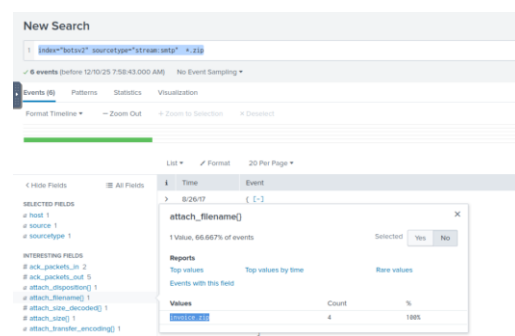
CyberEastEgg ✓ Correct Answer

To maintain persistence in the Frothy network, Taedonggang APT configured several Scheduled Tasks to beacon back to their C2 server. What single webpage is most contacted by these Scheduled Tasks? Answer example: index.php or images.html

process.php ✓ Correct Answer

Question 1:

We will use the filter `index="botsv2" sourcetype="stream:smtp" *.zip`. Then we will go to the Selected Fields list, then to `attach_filename{}`, and then we will find the attachment name `invoice.zip`



Question 2:

```
First, we'll use the filter index="botstv2" sourcetype="stream:smtp" *.zip  
""attach_filename{}="invoice.zip
```

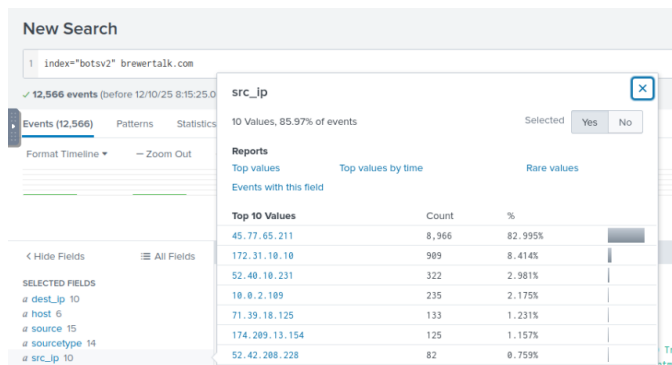
Then, we'll click on "Show as raw text" at the end of the first event, and then we'll search for the password, which will be 912345678



Question 3:

First, we need to find the attacker's IP address. Remember, there was an IP address scanning brewertalk.com. We'll use the filter `index="botsv2" brewertalk.com`

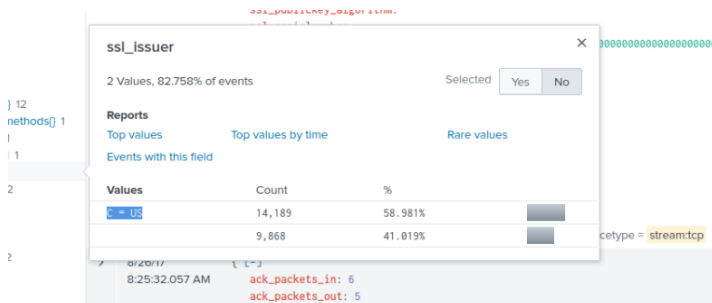
Then, we'll go to `src_ip`, and the IP address will be 45.77.65.211



Then we will use the filter `index="botsv2" sourcetype="stream:tcp" 45.77.65.211`

Then go down to ssl issuer

After that you will find the answer $C = US$



Question 4:

First, we'll use the filter `index="botsv2" sourcetype="stream:ftp"`

Then we'll go to method and then RETR to narrow down the search

After that, we'll go to filename and then find the unusual filename

filename

7 Values, 100% of events

Selected

Reports

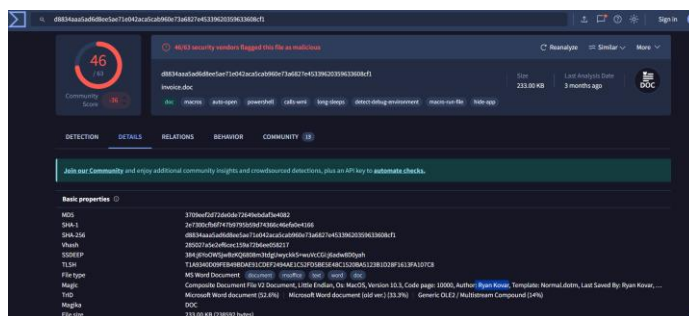
Top values Top values by time Rare values

Events with this field

Values	Count	%
dns.py	2	14.286%
nc.exe	2	14.286%
psexec.exe	2	14.286%
python-2.7.6.amd64.msi	2	14.286%
wget64.exe	2	14.286%
winsys64.dll	2	14.286%
나는.데이비드를.사랑한다.hwp	2	14.286%

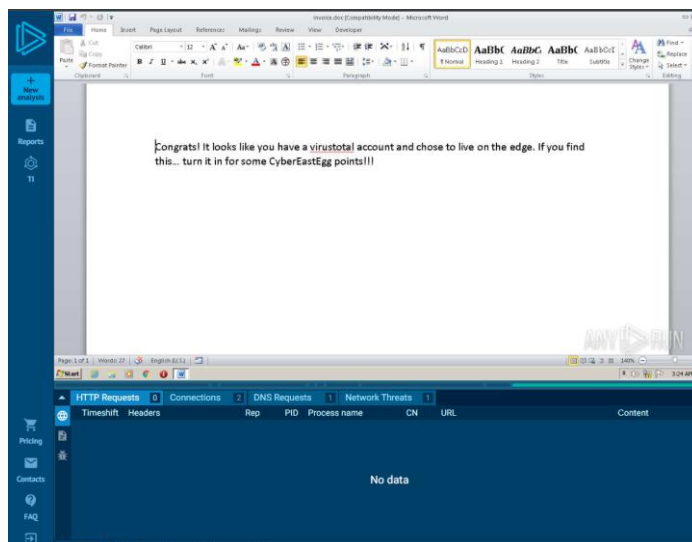
Question 5:

Using the hash of the malicious file, we will access the VirusTotal website and find the answer, which is Ryan Kovar



Question 6:

Go to app.any.run and you will find the answer CyberEastEgg



Question 7:

We will use the filter index="botsv2" HKLM\\Software\\Microsoft\\Network. Then we will go down to any event and look at the data. We will see that it is in base64 format. We will go to decompile it, and after that, the output will appear as process.php

Task 7: Conclusion

What is the Diamond Model? Read more about this [here](#).