Splunk 3 – Cryptomining Events

Within this task, the questions are mostly focused on an endpoint browser and cryptomining events.

The questions below are from the 200 series of the BOTSv3 dataset.

Again you're tasked to retrieve processor information, but this time it involves processor utilization.

Try some keywords related to processors and look at the available source types returned.

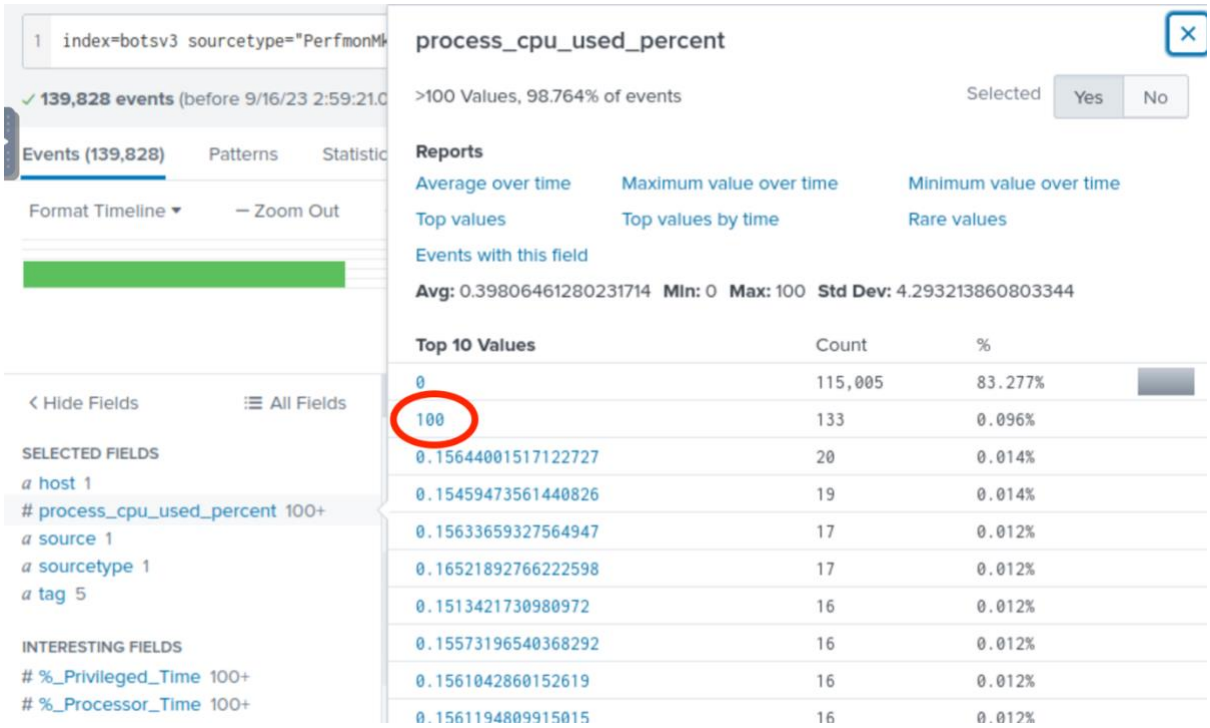
Start a new search query with the source type and look at the available fields.

Remember, you're looking for endpoints with 100% CPU utilization. Don't forget to reverse the order of the events.

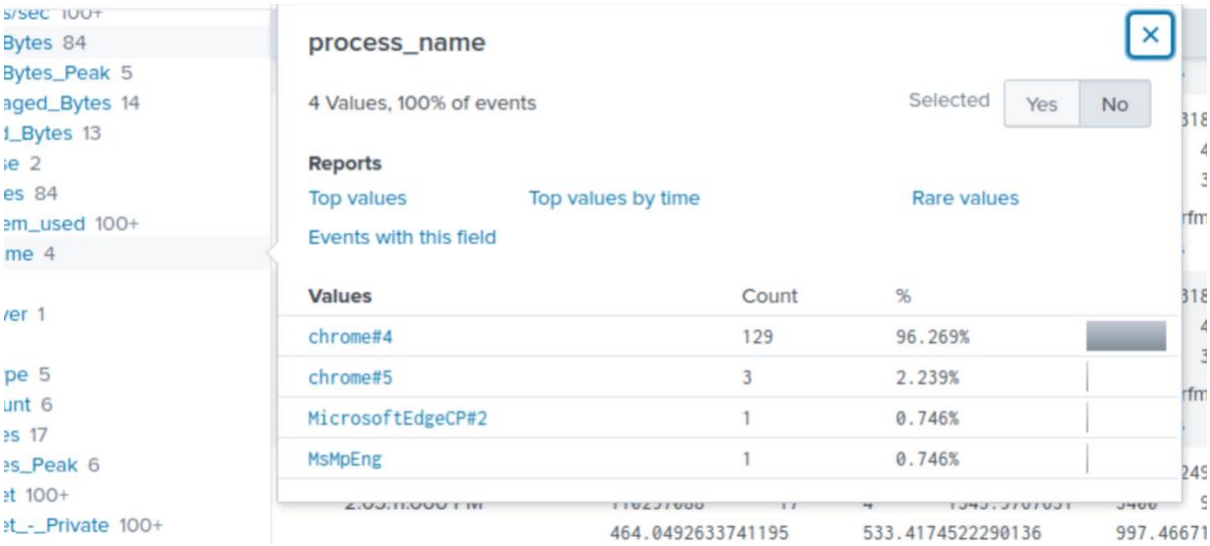
<u>Question: 1</u>
A Frothly endpoint exhibits signs of coin mining activity. What is the name of the second process to reach 100 percent CPU processor utilization time from this activity on this endpoint? Answer guidance: Include any special characters/punctuation.

Answer: chrome#5

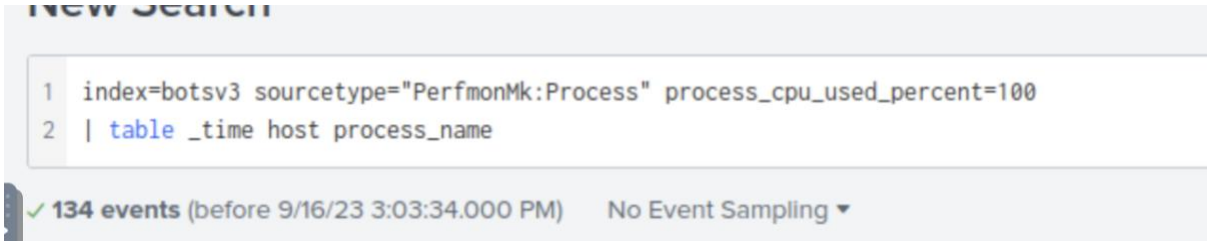
I initially used the query below with the sourcetype “PerfmonMK:process”. I then hunted the field names to find something related to CPU processors. The question stated that the process CPU had reached 100% and so from the field name below I was able to find the desired value as shown.

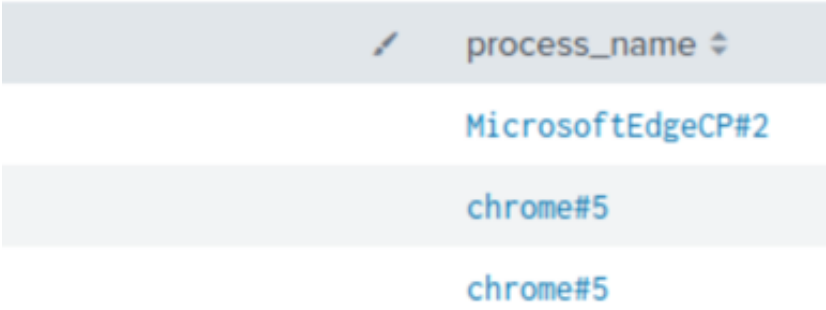


From there I could dive into the “process_name” field which provided 4 values.



The answer is 1 of the 4 values above, the question requested the second process to reach 100%. So I used the query below to create a table so that I could identify which was the second process_name. As you can see “chrome#5” was the answer.



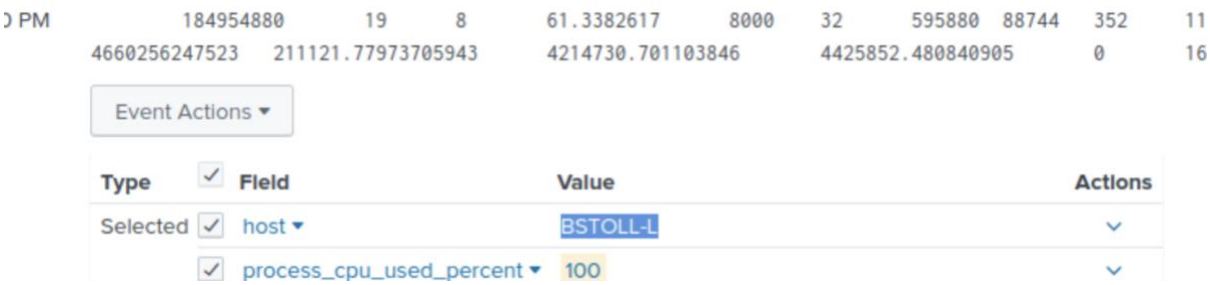


Question: 2

What is the short hostname of the only Frothly endpoint to actually mine Monero cryptocurrency? (Example: ahamilton instead of ahamilton.mycompany.com)

Answer: BSTOLL-L

The only hostname available was BSTOLL-L as seen in the image above that had high levels of CPU usage

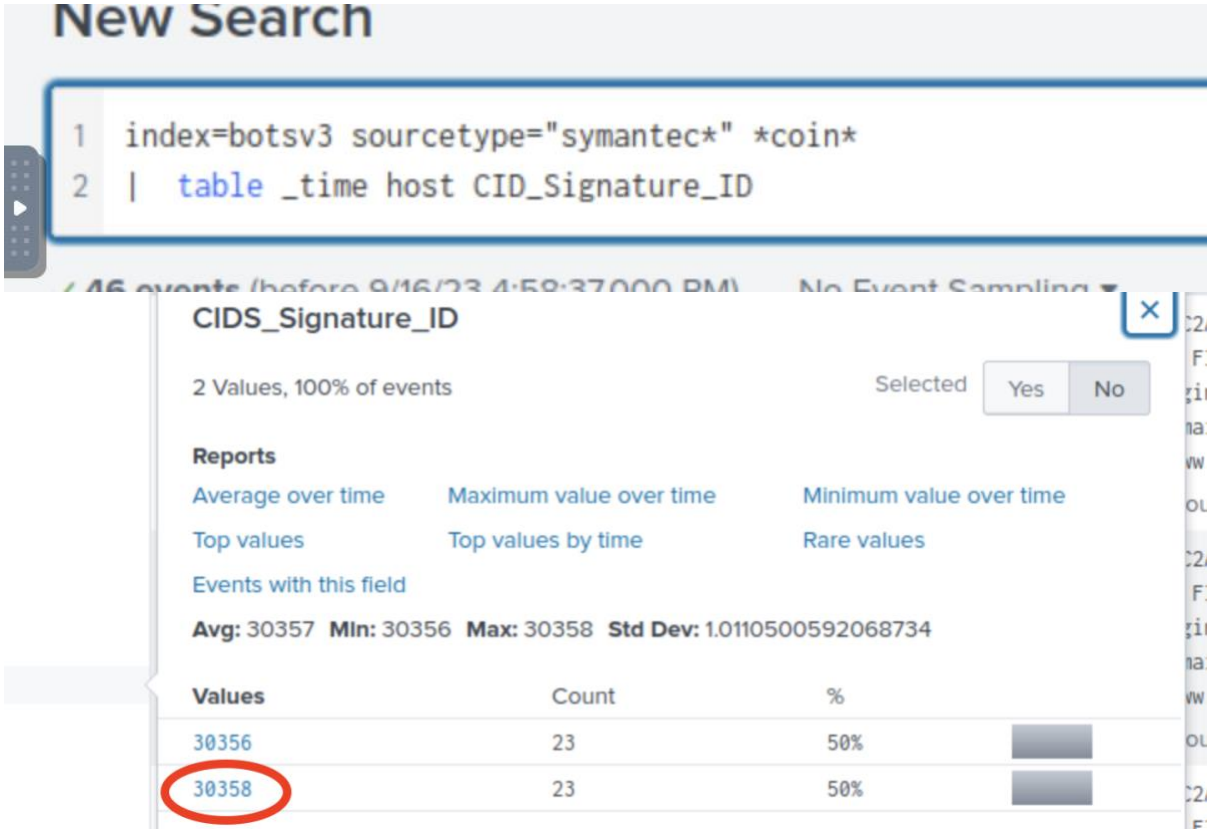


Question: 3

Using Splunk's event order functions, what is the first seen signature ID of the coin miner threat according to Frothly's Symantec Endpoint Protection (SEP) data?

Answer: 30358

I used “index=botsv3 sourcetype=”symantec*” *coin* before I was able hunt down the field name related to Signature IDs. The keyword “coin” helped within the query. I then used the query below and “table” function to show the correct value.



Question: 4
What is the name of the attack?

Answer: JSCoinminer Download 8

This was fairly straight forward, I used the Signature Id from the previous question in the query below

New Search

```
1 index="botsv3" 30358 CIDS_Signature_ID=30358
```

After analysing the first event under the "Web Attack" sub field we can clearly see the answer, JSCoinminer Download 8

```
[SID: 30358] Web Attack: JSCoinminer Download 8 attack bloc
cal: 192.168.3.130,Local: 000000000000,Remote: ,Remote: 54.
currences: 1,Application: C:/PROGRAM FILES (X86)/GOOGLE/CHR
```

Question: 5
According to Symantec's website, what is the severity of this specific coin miner threat?

Answer: Medium

Again I used the answer in the previous question to then search on Symantec's website and found the answer below

Web Attack: JSCoinminer Download 8

Severity:Medium

This attack could pose a moderate security threat. It does not require immediate action.

Question: 6

What is the short hostname of the only Frothly endpoint to show evidence of defeating the cryptocurrency threat? (Example: ahamilton instead of ahamilton.mycompany.com)

Answer: BTUN-L

Again the answer is in the same event as the previous question. It clearly states that “Traffic has been blocked for this application” and “JSCoinminer Download 8 attack blocked”. The short hostname is highlighted below .

2018-08-20 13:46:47,Major,BTUN-L,SHA-256: 268A0463D7CB907D45E1C2AB91703E71734116F08B2C090E34C2D506183F9BCA,MD-5: ,[SID: 30358] Web Attack: JSCoinminer Download 8 attack block
ed. Traffic has been blocked for this application: C:\PROGRAM FILES (X86)\GOOGLE\CHROME\APPLICATION\CHROME.EXE,Local: 192.168.3.130,Local: 000000000000,Remote: ,Remote: 54.6
7.127.227,Remote: 000000000000,Inbound,TCP,Intrusion ID: 0,Begin: 2018-08-18 21:00:27,End: 2018-08-18 21:00:27,Occurrences: 1,Application: C:/PROGRAM FILES (X86)/GOOGLE/CHROM
E/APPLICATION/CHROME.EXE,Location: Default,User: BillyTun,Domain: AzureAD,Local Port 63507,Remote Port 80,CIDS Signature ID: 30358,CIDS Signature string: Web Attack: JSCoinmi

2018-08-20 13:46:47,Major,BTUN-L,SHA-256: 268A0463D7CB90
ed. Traffic has been blocked for this application: C:\PR
7.127.227,Remote: 000000000000,Inbound,TCP,Intrusion ID:
E/APPLICATION/CHROME.EXE,Location: Default,User: BillyTu

End_Time	2018-08-18 21:00:23
Event_Description	[SID: 30356] Web Attack: JSCoinminer Download 6 attack blocked. T GLE\CHROME\APPLICATION\CHROME.EXE
Hack_Type	0
Host_Name	BTUN-L
Intrusion_URL	www.brewertalk.com/