

# 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.

## Question: 1

A Frothy 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.

The screenshot shows a Splunk search interface. The search bar contains the query: `index=botsv3 sourcetype="PerfmonMK:process"`. The results show 139,828 events. A sidebar on the left lists selected fields: `host 1`, `process_cpu_used_percent 100+`, `source 1`, `sourcetype 1`, and `tag 5`. The main panel displays a summary for the field `process_cpu_used_percent`, indicating it has over 100 values and 98.764% of events. Below this, a table titled "Top 10 Values" lists the most frequent values. The value `100` is circled in red, indicating it is the second process to reach 100% CPU utilization.

Top 10 Values	Count	%
0	115,005	83.277%
100	133	0.096%
0.15644001517122727	20	0.014%
0.15459473561440826	19	0.014%
0.15633659327564947	17	0.012%
0.16521892766222598	17	0.012%
0.1513421730980972	16	0.012%
0.15573196540368292	16	0.012%
0.1561042860152619	16	0.012%
0.1561194809915015	16	0.012%

From there I could dive into the "process\_name" field which provided 4 values.

**process\_name**

4 Values, 100% of events

Selected

**Reports**

Top values      Top values by time      Rare values

Events with this field

Values	Count	%
chrome#4	129	96.269%
chrome#5	3	2.239%
MicrosoftEdgeCP#2	1	0.746%
MsMpEng	1	0.746%

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.

**NEW SEARCH**

```
1 index=botsv3 sourcetype="PerfmonMk:Process" process_cpu_used_percent=100
2 | table _time host process_name
```

✓ 134 events (before 9/16/23 3:03:34.000 PM)    No Event Sampling ▼

_time *	host *	process_name *
2018-08-20 09:36:26	BSTOLL-L	MicrosoftEdgeCP#2
2018-08-20 13:37:50	BSTOLL-L	chrome#5
2018-08-20 13:38:20	BSTOLL-L	chrome#5

**process\_name**

MicrosoftEdgeCP#2

chrome#5

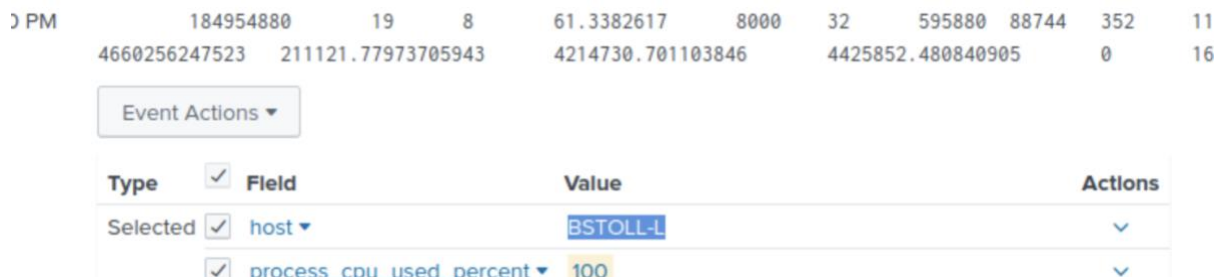
chrome#5

Question: 2

What is the short hostname of the only Frothy 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



The screenshot shows a table with columns: Type, Field, Value, and Actions. The 'Type' column has a 'Selected' checkbox. The 'Field' column has two entries: 'host' and 'process\_cpu\_used\_percent'. The 'Value' column shows 'BSTOLL-L' for the host and '100' for the process\_cpu\_used\_percent. The 'Actions' column has a dropdown arrow for each row.

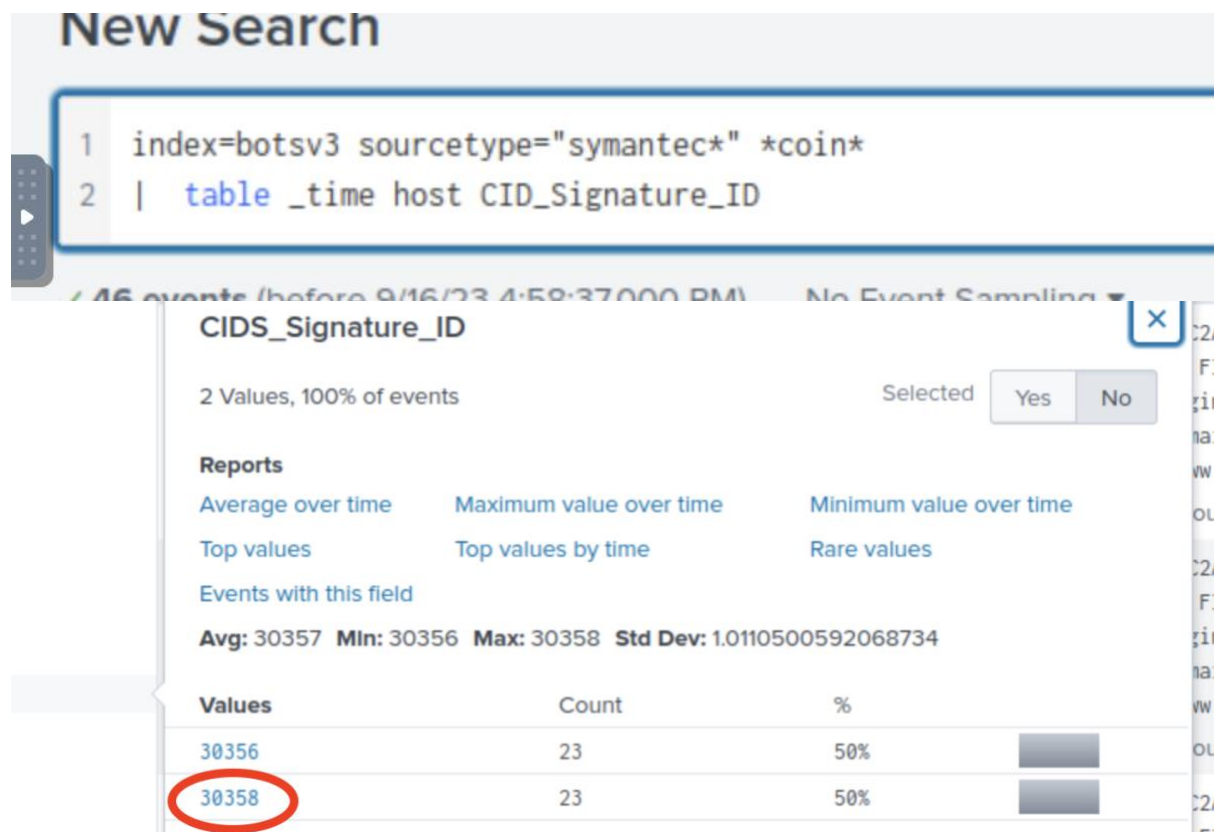
Type	Field	Value	Actions
Selected	host	BSTOLL-L	▼
	process_cpu_used_percent	100	▼

Question: 3

Using Splunk's event order functions, what is the first seen signature ID of the coin miner threat according to Frothy'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.



The screenshot shows the Splunk Search interface. The search bar contains the query: `1 index=botsv3 sourcetype="symantec*" *coin*` and `2 | table _time host CID_Signature_ID`. Below the search bar, the results are displayed as a field summary for **CIDS\_Signature\_ID**. The summary shows 2 values, 100% of events. The reports section includes: Average over time, Maximum value over time, Minimum value over time, Top values, Top values by time, and Rare values. The statistics section shows: Avg: 30357, Min: 30356, Max: 30358, Std Dev: 1.0110500592068734. The values table shows two values: 30356 (Count: 23, %: 50%) and 30358 (Count: 23, %: 50%). The value 30358 is circled in red.

**New Search**

1 index=botsv3 sourcetype="symantec\*" \*coin\*  
2 | table \_time host CID\_Signature\_ID

46 events (before 9/16/23 4:58:37 PM) No Event Sampling

**CIDS\_Signature\_ID**

2 Values, 100% of events Selected Yes No

**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: 30357 Min: 30356 Max: 30358 Std Dev: 1.0110500592068734

Values	Count	%
30356	23	50%
30358	23	50%

Question: 4

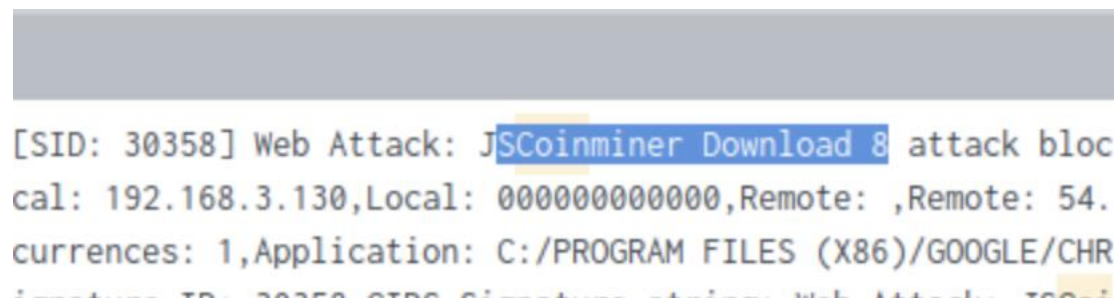
What is the name of the attack?

Answer: JSCoinminer Download 8

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



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



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 Frothy 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, S, A-256: 268A0463D7CB907D45E1C2AB91703E71734116F08B2C090E34C2D506183F9BCA, MD-5: , [SID: 30358] Web Attack: JSCoinminer Download 8 attack blocked. Traffic has been blocked for this application: C:\PROGRAM FILES (X86)\GOOGLE\CHROME\APPLICATION\CHROME.EXE, Local: 192.168.3.130, Local: 000000000000, Remote: 54.67.127.227, 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\CHROME\APPLICATION\CHROME.EXE, Location: Default, User: BillyTun, Domain: AzureAD, Local Port 63507, Remote Port 80, CIDS Signature ID: 30358, CIDS Signature string: Web Attack: JSCoinminer Download 8 attack blocked.

2018-08-20 13:46:47, Major, BTUN-L, S, A-256: 268A0463D7CB907D45E1C2AB91703E71734116F08B2C090E34C2D506183F9BCA, MD-5: , [SID: 30356] Web Attack: JSCoinminer Download 6 attack blocked. Traffic has been blocked for this application: C:\PROGRAM FILES (X86)\GOOGLE\CHROME\APPLICATION\CHROME.EXE, Local: 192.168.3.130, Local: 000000000000, Remote: 54.67.127.227, 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\CHROME\APPLICATION\CHROME.EXE, Location: Default, User: BillyTun, Domain: AzureAD, Local Port 63507, Remote Port 80, CIDS Signature ID: 30356, CIDS Signature string: Web Attack: JSCoinminer Download 6 attack blocked.

<input type="checkbox"/> End_Time ▼	2018-08-18 21:00:23
<input type="checkbox"/> Event_Description ▼	[SID: 30356] Web Attack: JSCoinminer Download 6 attack blocked. Traffic has been blocked for this application: C:\PROGRAM FILES (X86)\GOOGLE\CHROME\APPLICATION\CHROME.EXE
<input type="checkbox"/> Hack_Type ▼	0
<input type="checkbox"/> Host_Name ▼	BTUN-L
<input type="checkbox"/> Intrusion_URL ▼	www.brewertalk.com/