Fiches techniques
Injection de code dans un PE Windows

Kaci Hammoudi

19 novembre 2021

1 Problématique

Dans le cadre du projet, le client souhaite pouvoir greffer l'utilitaire de protection de licence directement dans l'exécutable Windows de son choix. (Voir PE `https://fr.wikipedia.org/wiki/Portable_Executable`).

Pour se faire nous allons devoir utiliser des méthodes permettant de modifier un exécutable et d'injecter le code souhaité ; À savoir celui de la vérification d'une licence.

Ainsi à chaque lancement de l'exécutable, le greffé se verra exécuté en amont permettant de stopper le démarrage du programme dans le cas d'une licence non valide.

2 Méthode de réalisation

Afin de pouvoir injecter du code dans un PE, il faut en connaître sa structure. Nous aurons aussi besoin d'un outil afin de manipuler les PE Windows. Un outil qui nous a été conseillé est PEFile, un module python concu dans ce but.

Premièrement, il nous faudra créer un nouvel en-tête de section. Il faudra y définir :
- Le nom de la section,
- La taille de la section,
- Les pointeurs sur les différentes parties de la section,
- Un code caractérisant la section (Voir section 'Characteristics' `https://docs.microsoft.com/en-us/windows/win32/api/winnt/ns-winnt-image_section_header`).

Puis, modifier la structure FileHeader afin de définir :
- Le nouveau nombre de section,
- La nouvelle taille du PE,
- Le nouveau point d'entrée du PE (qui sera notre code injecté).

Finalement, écrire le shellcode souhaité, au bon endroit dans le PE, qui s'exécutera avant le programme originel.

La procédure plus détaillée est définie dans cet article conseillé par le client. À cette adresse : `https://axcheron.github.io/code-injection-with-python/`.

La manipulation du module python PEFile est présentée ici `https://axcheron.github.io/pe-format-manipulation-with-pefile/`.