Virologie & Malware - Projet Yharnam

Projet Yharnam

Projet à réaliser optionnellement en binôme. Le rendu contiendra un fichier AUTHORS.txt listant le ou les 2 membres du groupe. Soit il s'agit de poursuivre ce qui a été présenté en TP, soit de partir sur du trés complexe.

Dans le cas ou vous poursuivez les objectifs du TP, vous réaliserez:

- Injecteur PE: c'est à dire contaminant un fichier exécutable d'un répertoire.
- Modifie le point d'entrée du fichier cible de sorte à s'exécuter avant toute chose, puis à redonner la main aux instructions originelles.
- Le code injecté affiche une MessageBox afin de constater de l'infection puis réalise vos bonus.

Si vous êtes déjà à l'aise en maldev partir sur un multi-stage fileless injectant des process en exploitant les 2 aspects présentés en cours:

- Nouvelle technique pour se charger dans l'espace mémoire du process cible
- Nouvelle technique pour créer un thread dans le process cible sur cette zone mémoire
- Pas de process hollowing, thread injection, dll injection classique autorisé
- Demandez de valider l'idée en amont!

Dans le cas standard, il est recommandé de respecter la démarche des TPs:

- création d'une section à part pour stocker tout le code injectable dans l'injecteur originel.
- makefile pour le compilation.
- compilation conditionnel pour les tests.

Les fonctionnalités sont potentiellements étendues par les bonus suivants:

- Injection dynamique: à chaque exécution contamine tous les fichiers PE/64 bit du répertoire courant.
- Injection process en plus de l'injection de fichier: contamine un type de process connue s'il est actif dans la session (i.e: calc.exe).
- Packing / chiffrement: votre code n'est pas en clair dans le fichier PE injecté mais à subit des transformations.

Si vous faites du non-standard:

- Votre malware mets en place un mécanisme de persistance autre que celui présenté en cours (injection de PE), cela devra être complétement décrit dans votre fichier README.txt.

Le rendu sera rendu sous forme d'archive (7z chiffré avec mdp 'yharnam') contenant l'ensemble des fichiers requis pour la fabrication de votre projet. Celle-ci devra être téléversée sur l'espace google classroom dédié au projet.

Est demandé également un fichier README.txt expliquant les modalités de compilation.

Vous expliquerez aussi dans votre README.txt les comportements de votre malware:

- infection de process si bonus présent et quel process est ciblé
- packing/chiffrement
- etc...