Analyse de Malware

Mini-projet : Ecrire un Ransomware simple

1. Introduction

Un ransomware est un programme conçu pour empêcher un utilisateur ou une organisation d'accéder aux fichiers de son ordinateur. Il chiffre les fichiers et exige une rançon pour la clé de déchiffrement. Cela place les organisations et les particuliers dans une position où payer la rançon est le moyen le plus simple, le moins cher et le plus rapide de retrouver l'accès à leurs fichiers. Certains types de ransomware ont des fonctionnalités supplémentaires, comme le vol de données.

Les récentes attaques de ransomware ont eu un impact sur la capacité des hôpitaux à fournir des services essentiels et ont paralysé les services publics dans les villes. Les ransomwares n'ont pas besoin d'être complexes pour causer des dommages, ce qui les rend encore plus dangereux. Les mauvais acteurs n'ont pas non plus besoin de solides connaissances en programmation. Dans ce mini-projet, vous allez écrire un ransomware simple à l'aide du langage C ou C++ sous Linux.

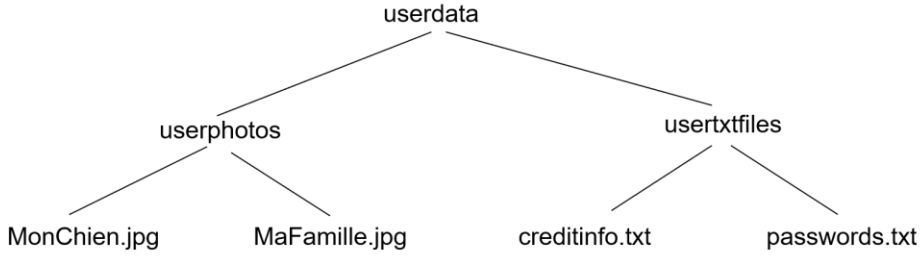
2. Principe des Ransomware

Le code du ransomware peut être divisé en trois parties : l'exploration du répertoire (**directory crawler**), le chiffrement (**encryption**) et le déchiffrement (**decryption**).

- La première fonction explore tous les répertoires accessibles dans le répertoire qui contient le logiciel malveillant. L'exploration recherche des fichiers et d'autres sous-répertoires et continue jusqu'à ce qu'elle atteigne le point le plus profond de l'arborescence du répertoire, puis enregistre les noms et les chemins des fichiers à utiliser pendant la phase de chiffrement.
- Une fois que le ransomware a acquis toutes ses cibles, il est prêt à commencer à chiffrer les fichiers des victimes. Lorsque le chiffrement commence, il utilise la liste établie par le crawler et commence à chiffrer tous les fichiers qu'il peut atteindre.
- Une fois le chiffrement terminé, il affiche à l'utilisateur un message lui indiquant que ses données ont été compromises et lui donne une série d'instructions à suivre s'il souhaite restaurer ses données ; par exemple, envoyer de la cryptomonnaie pour obtenir la clé de déchiffrement. Une fois que l'utilisateur a saisi la clé, toutes ses données peuvent être restaurées, ce qui lui permet d'accéder à nouveau aux données.

3. Implémentation

- Pour le chiffrement et le déchiffrement, vous pouvez utiliser la cryptographie asymétrique à l'aide de la librairie openssl (le fichier *rsa.c* est un exemple d'utilisation de la cryptographie asymétrique en utilisant RSA).
- Pour le parcours d'un répertoire sous Linux, vous pouvez vous inspirer de l'exemple *parcours.c*
- Pour infecter les programmes exécutables, vous **devez** développer une nouvelle librairie pour réimplémenter des fonctions d'une librairie (library wrapper). Ce qui vous permet d'intercepter les fonctions des librairies standards (exemple : *puts*, *printf*, *strcmp*, …).
- Pour récupérer ses données, l'utilisateur doit payer la rançon ou tenter de récupérer la clé de déchiffrement par force brute. Cette technique prendra beaucoup de temps et coûtera plus cher que le paiement de la rançon. Supposons donc que l'utilisateur ait payé la rançon et obtenu la clé de déchiffrement. Vous pouvez définir votre propre scénario de paiement et d'obtention de clé.
- Vous pouvez tester votre ransomware comme suit :
  - Créer un répertoire de victimes où le ransomware sera installé. Exemple :



  - Conserver des copies des fichiers au cas où quelque chose se passerait mal, afin de ne pas avoir à créer ou télécharger à nouveau les fichiers.

4. Livrable

- A la fin de ce travail, vous devez rédiger un rapport clair et complet et préparer une présentation Powerpoint pour une durée de 10 minutes suivie d'une démonstration pour une durée de 5 minutes.
- Il faut soumettre le rapport, la présentation ainsi que le logiciel développé et/ou le scénario implémenté au plus tard le **Lundi 11 Novembre 2024 avant minuit**.
- La présentation orale aura lieu le **Mercredi 13 Novembre 2024**.
- La note prend en considération :
  - La qualité et la quantité du travail effectué
  - Le contenu et la forme du rapport
  - La clarté de la présentation orale et de la démonstration