TELECOM Nancy

Projet "Malware et rétro-ingénierie"

Guillaume Bonfante

Le projet se fait en deux étapes, pour la première, vous écrirez un programme en tenant compte des spécifications présentées ci-dessous, et pour la seconde, vous serez amenés à déterminer le comportement du programme qui vous sera confié.

En cas de doute sur l'application des consignes, mieux vaut me demander.

Vous avez deux possibilités : soit vous écrivez un Malware, soit vous écrivez un Goodware. Commençons par décrire le Malware.

La spécification du malware est la suivante :

1. la chaine argv[1] est l'entrée, elle est supposée être une chaine de moins 8 caractères ASCII imprimables ;
2. si la donnée ne respecte pas la règle, le comportement du programme n'est pas spécifié. Si le programme n'a pas exactement un argument, le comportement n'est pas spécifié ;
3. pour une entrée au moins, le programme doit afficher sur la console "Vous avez gagné" ou toute autre phrase suffisamment explicite ;
4. par défaut, il affiche la chaîne elle-même.

La spécification du goodware est la suivante :

1. la chaine argv[1] est l'entrée, elle est supposée être une chaine de moins 8 caractères ASCII imprimables ;
2. si la donnée ne respecte pas la règle, le comportement du programme n'est pas spécifié. Si le programme n'a pas exactement un argument, le comportement n'est pas spécifié ;
3. il affiche la chaîne donnée en entrée.

Éléments supplémentaires :

1. Le programme doit fonctionner sur la machine virtuelle d'analyse, sans connexions réseau.
2. Il est autorisé de "casser" la machine virtuelle si l'utilisateur ne respecte pas la règle des entrées. Toutefois, il est interdit d'attaquer l'hôte.
3. Son processus de fabrication doit être explicite, il sera vérifié en fin de cours. Il est interdit d'utiliser un packer. Le programme est essentiellement écrit en C/ASM compilé avec VC. La chaine de compilation me sera confiée pour vérification.
4. Si le programme est débuggé/analysé, son comportement n'est pas spécifié.
5. Le temps de calcul doit être raisonnable $<$ 1minute.
6. En cas d'utilisation licite du programme, celui-ci ne doit pas modifier l'état général de la machine (pas de modification de registres, de fichiers, etc).
7. L'argument est donné en ligne de commande.

Critères d'évaluation : Sont considérés positivement, toute information d'analyse et d'identification de :

1. la clé,
2. des fonctions appelées,
3. de clés de chiffrement,
4. de code auto-modifiant,
5. de processus en cours,
6. de mesures anti-debug,
7. d'obfuscations syntaxiques.

A contrario, si une technique de votre code est identifiée, cela sera compté négativement.

Rendu : L'évaluation sera faite à l'oral. Vous présenterez l'analyse que vous avez faites du malware reçu. Prévoyez grosso modo un exposé d'1/4h. En outre, vous m'enverrez un dossier contenant :

- Votre code source, et la clé si c'est un Malware. Cela me permet de vérifier que vous n'avez pas triché.
- Votre présentation,
- Un document d'une ou deux page présentant les techniques d'attaque
- Un readme pour que je me repère dans votre dossier.