LAB 2 : Analyse d'un Malware

1) Choisissez un Malware en ligne de votre choix. Voici quelques bases de données de malwares avec des exemples qu'on peut utiliser :

1. theZoo est une base de donné des malwares : https://github.com/ytisf/theZoo
2. Virus de tests (download for free) : https://www.ikarussecurity.com/en/private-customers/download-test-viruses-for-free/
3. https://www.reddit.com/r/Malware/comments/7fabu5/sites_to_download_malware/

Choix du malware à valider ensemble.

2) Réaliser une analyse statique et dynamique du malware :

1. Analyse statique basique : choisir au moins 2 des trois techniques vues dans le cours (choix des outils flexible) ;
2. Analyse dynamique : implémenter le malware dans un environnement isolé et analyser son comportement.

Modalités et Résultats attendus :

- Un rapport détaillant le choix du malware et les étapes d'analyse suivies (captures d'écran + analyse) à rendre (**1 rapport par groupe**).
- Le LAB sera travaillé pendant deux séances par un groupe de 2 à 5 personnes au maximum.
- Le LAB devra être déposé sur Moodle au plus tard le **2 février 2025**.