Compte Rendu de Réunion

26/02/2025 (Présentiel)

Participants de Réunion:

- Milan Soragna - Milan SORAGNA
- Teresa Fernandez Del Busto - Teresa FERNÁNDEZ DEL BUSTO
- Léo Zanella - Léo ZANELLA

Membres Présents en Distanciel:

- Alan Bellec - Alan BELLEC

— Début de réunion à 12:21 —

Thème de Réunion:

Le but de cette réunion est de discuter un peu de la vision projet générale de chaque participant, et d'évaluer les préférences personnelles quant à l'organisation, les techniques employées, et les fonctionnalités du botnet.
En l'absence d'un sujet de projet, cette réunion ne permet pas encore de prévoir un plan fonctionnel, ni d'évaluer les possibilités techniques du projet face aux contraintes ou cahier des charges du client.

Discussions entre participants:

Milan SORAGNA propose de créer un tableau à colonnes dans lequel se placent les idées de chaque participant "Within Scope (à intégrer)", "Upgrades (Améliorations)", et "Not in Scope (Ne sera pas intégré)".

Alan BELLEC suggère l'utilisation de CVE (Common Vulnerabilities and Exposures) afin de répandre le botnet et d'assurer sa propagation sur le plus de machines possibles. Une explication rapide de ce qu'est une CVE est faite au groupe. Un plan de recherche de CVE exploitable est faisable, quitte à simuler un environnement exploitable lors de la démo en preuve de concept.

Léo ZANELLA cite le "BYOB" (Build Your Own Botnet) comme une bonne source d'inspiration à prendre en compte, étant donné qu'il offre des outils assez avancés. Le code est cependant en Python, donc les connaissances techniques limitées en C de la part des membres du groupe sont à prendre en considération.

Milan SORAGNA part du BYOB pour ajouter différents éléments d'amélioration du projet (basé sur les concepts du BYOB), tel que le reverse TCP (Transmission Control Protocol), la protection face au reverse engineering, la persistance dans les machines, un site web de monitoring, … etc.

Le manque d'un sujet préparé revient sur la table, en son absence la préparation d'un plan fixe n'est pas vraiment possible, seulement une exploration des possibilités.

Milan SORAGNA demande au groupe leurs préférences sur le projet - avec en premier lieu la vision du travail (un projet dans lequel notre investissement sera très important, ou un projet fonctionnel et/ou dépassant les attentes mais sans plus), avec bien sûr l'un prenant un effort sur le temps bien plus considérable. Pour le moment, le groupe semble préparé à investir du temps et à dépasser les attentes *de loin*, mais fait remarquer que l'engagement temporel ne peut pas encore être évalué à l'avance, surtout sans connaître le cahier des charges du projet et n'ayant pas encore débuté tous les cours du module (en plus d'engagements personnels à prévoir).

La réunion repart sur une explication brève des concepts du botnet, la mise en pratique initiale du projet est jugée simple par Milan SORAGNA, avec surtout une partie importante dédiée aux améliorations ou fonctionnalités complémentaires. La notion de sockets est mentionnée, Alan BELLEC ajoutera aussi des protocoles supplémentaires comme SMB (Server Message Block) qui sont fréquemment employés dans les botnets.

Alan BELLEC demande quel mode de communication est préféré par le groupe, en proposant de garder un groupe sur l'application Discord, ou de créer un "Serveur Discord", lieu regroupant plusieurs salons de discussion centrés autour du projet. Ce dernier sera adopté par le groupe.

Léo ZANELLA et Alan BELLEC sont en accord sur le fait que l'utilisation de "l'IoT" (Internet of Things) est un moyen efficace pour déployer un botnet, car souvent peu protégés et trouvables en grande quantité avec (par exemple) une très haute bande passante et disponibilité dans le cadre d'un botnet de DDoS (Distributed Denial of Service).

La réunion prend fin en discutant des prochaines étapes à venir, un gros accent est mis sur l'analyse de l'existant, des méthodes et techniques employées par les botnets afin d'êtres prêts lorsque le sujet est finalisé à avoir une base de connaissances dans le domaine, et pouvoir (relativement) rapidement évaluer nos options.

— Fin de réunion à 12:52 —

Étapes suivantes:

- Milan SORAGNA :
    - Créer un serveur Discord pour centraliser les informations du projet.
    - Générer un compte-rendu de la présente réunion
    - Faire l'analyse de la persistance des botnets
        - Quels sont les mécanismes employés sur les différents systèmes d'exploitation?
        - Quelles sont les options en C pour s'en donner les moyens?
        - Ya-t-il des risques associés à ces méthodes (d'être découverts par exemple)?
- Alan BELLEC :
    - Faire une analyse sur les CVE et la propagation:
        - Existe-t-il des CVE sur lesquels nous pouvons agir?
        - Pour ces CVE, permettent-elles de propager le botnet?
        - Existe-t-il des exemples d'implémentation de ces CVE qui nous aideraient dans le développement?
- Léo ZANELLA :
    - Analyser les techniques réseau des botnets:
        - Quels sont les protocoles utilisés?
        - Existe-t-il une préférence sur certains protocoles (plus sécurisés, moins détectables, plus faciles à utiliser, …)?
        - Rechercher des moyens d'implémentation des protocoles identifiés comme pertinents en C.
- Teresa FERNÁNDEZ DEL BUSTO :
    - Analyse générale d'un botnet, et du principe de sockets:
        - Qu'est-ce qu'un botnet - à quoi sert-il et comment sont-ils utilisés?
        - Existe-t-il des botnets existants ayant une documentation (Zeus, Storm, Mirai, **EternalBlue**…) qui peut être utile?
        - Comment fonctionnent les sockets en C?