Analyse post-mortem

PPII2 - 2025

BELLEC – SORAGNA - FERNANDEZ DEL BUSTO JIMENEZ – ZANELLA

Sommaire

1. Contexte et description du projet

A. Contexte

Dans le cadre de notre première année de formation à TELECOM Nancy, il nous a été demandé ces dernières semaines de travailler sur un projet visant à réaliser un botnet en langage C.

Ce projet, à portée pédagogique et pluridisciplinaire, avait pour objectif de nous amener à mobiliser les compétences acquises au cours des différents modules du second semestre de cette année de formation, notamment ceux consacrés aux réseaux, au langage C et aux structures de données.

En raison de la spécificité de notre formation, spécialisée dans le domaine de la cybersécurité, l'équipe pédagogique de TELECOM Nancy a décidé pour cette année 2024-2025 de proposer aux élèves de FISEA un sujet correspondant davantage aux enjeux liés à la cybersécurité.

Ce document sert de rétrospective sur le travail qui a été mené ces dernières semaines et de rapport écrit concernant l'analyse post-mortem de ce projet.

B. Description du projet

Ce projet visait principalement à nous faire manipuler les sockets réseaux en langage C et à nous faire réfléchir sur l'architecture globale d'un réseau botnet. Les rendus devant comporter à minima un état de l'art sur le fonctionnement général des réseaux botnet ainsi qu'un projet en langage C permettant à un script « serveur de commande et de contrôle » d'envoyer des instructions à des scripts « esclaves » afin de forcer ces derniers à exécuter des commandes sur leur hôtes respectifs.

La phase de propagation et d'escalade de privilège étant en dehors du périmètre d'étude, nous avons considéré que les scripts esclaves étaient exécutés avec les droits administrateurs sur les machines victimes.

Si certains éléments (repris de manière exhaustive dans le cahier des charges décrit dans la charte du projet) étaient imposés, tels qu'une interface permettant au bot master de piloter les bots connectés au serveur C2, beaucoup de libertés nous ont été laissées quant à de potentielles améliorations.

Face à ces nombreuses possibilités, nous nous sommes, durant la phase de cadrage de ce projet, fixés des objectifs dont nous allons traiter dans la partie suivante.

2. Retours sur les objectifs initiaux

A. Objectifs initiaux

Compte tenu de la portée assez restreinte du cahier des charges minimal, nous avons décidé d'enrichir le projet en passant par l'ajout de fonctionnalités optionnelles.

Nous avons ainsi décidé durant la phase d'analyse, de cadrage et de préparation du projet de nous fixer des objectifs supplémentaires concernant le chiffrement des communications réseau entre les clients et le serveur de commande.

D'autres idées ont émergées, comme l'augmentation de la discrétion des communications réseau via des techniques découvertes durant la rédaction de notre état de l'art, mais nous avons décidé de nous fixer comme principal objectif de respecter dans un premier temps le cahier des charges minimal en réalisant un MVP (Minimum viable product) du projet avant de travailler à l'implémentation d'améliorations en lien avec les idées citées précédemment.

B. Résultats

Pour revenir sur ce qui a été effectivement réalisé, l'intégralité du cahier des charges minimal a été implémenté, ce qui nous a permis de valider notre objectif principal.

Les mécanismes d'augmentation de la discrétion ainsi que le chiffrement des communications réseau entre les clients et le serveur ont été abandonnés durant la phase de conception. En effet, nous avions sous estimé la complexité de certains de ces mécanismes et n'avions pas anticipé la lourdeur résultant de la manipulation des sockets réseau en langage C.

Une fonctionnalité majeure a néanmoins été ajoutée au projet, en grande partie portée par Milan, concernant l'interface d'administration du botnet. Le choix est en effet désormais proposé au botmaster entre un mode CLI ergonomique réalisé à l'aide de la librairie ncurses et une interface Web gérée grâce à la librairie mongoose.

Ainsi, si certains de nos objectifs secondaires n'ont pas été atteints, d'autres idées ont émergées en cours de route et ont été implémentées tandis que notre objectif principal a été atteint dans les temps.

3. Difficultés rencontrées

A. Organisationnelles

Tout projet comportant son lot de difficultés, nous en avons rencontré certaines durant ce projet, notamment du point de vue organisationnel et gestion de projet.

Tout d'abord, ce second semestre a été relativement intense en terme de charge de travail. Le rythme s'est accéléré au fil du temps et le nombre de cours est allé en augmentant au fur et à mesure des semaines tandis que nous entrions dans la phase de développement du projet. Grâce à notre organisation et à notre gestion de projet efficace nous avons cependant réussi à faire face à ces difficultés de gestion de nos emplois du temps. L'expérience engrangée durant le projet pluridisciplinaire du premier semestre a aussi été bénéfique dans ce contexte.

De plus, le projet a consisté en un travail de plusieurs semaines entre les membres de notre équipe. Cette collaboration a nécessité l'utilisation d'outils de travail collaboratif efficaces tels que YouTrack et Git.

B. Techniques

D'un point de vue technique, ce projet nous a permis d'apprendre et de développer nos compétences. Certains aspects du projet ont cependant nécessité un temps d'adaptation et d'apprentissage plus important que d'autres, à commencer par les sockets réseau.

Si certains membres de notre équipe avaient déjà manipulé les sockets à l'aide d'autres langages de programmation comme Python, l'utilisation des sockets réseau en langage C n'en reste pas moins relativement lourde. Les ressources disponibles sur internet nous ont été d'une grande aide, nous nous sommes par ailleurs principalement appuyés sur le cours portant sur les communications réseaux en langage C qui nous a été dispensé par M. Cholez.

L'ampleur du projet a été un défi intéressant à relever en raison de l'utilisation de l'outil CMake qui nous a été très utile dans l'optique de gérer notre compilation séparée. En raison du nombre important de fichiers sources et d'en tête, il nous a fallu faire preuve d'organisation et de méthode afin de garder une structure de projet relativement modulaire avec une bonne gestion des responsabilités dans le code.

4. Conclusion

Pour conclure, ce projet nous a permis de mobiliser nos compétences acquises au cours de ce second semestre à TELECOM Nancy. Travailler sur ce sujet nous a offert l'opportunité d'approfondir nos connaissances sur le fonctionnement des botnets en nous confrontant à des problématiques en lien avec les enjeux de cybersécurité actuels.

Si certains objectifs initiaux n'ont pas été atteints comme le chiffrement des communications réseau, l'intégralité du cahier des charges a été respecté et d'autres fonctionnalités optionnelles ont vues le jour, comme l'interface Web, permettant une grande personnalisation vis à vis des commandes envoyées aux bots et un confort amélioré pour le botmaster.

Pour finir, nous avons grandement apprécié travailler sur ce projet et nous espérons que le résultat sera à la hauteur des attentes de l'équipe pédagogique.

L'équipe MALT