Filière Tremplin Recherche

Titre du projet

Détection de *botnet* mobiles

Présentation générale du projet

Selon Kaspersky [1], un *botnet* désigne un groupe d'ordinateurs infectés et contrôlés par un pirate à distance. Les *botnets* sont généralement créés par un pirate informatique ou par un petit groupe de pirates qui utilise un malware afin d'infecter un grand nombre de machines. Les ordinateurs faisant partie du *botnet* sont souvent appelés « bots » ou « zombies » et il n'y a pas de taille requise pour pouvoir considérer un groupe d'ordinateurs comme un *botnet*. Les petits botnets peuvent désigner des centaines ou quelques milliers de machines, alors que les botnets les plus grands peuvent comprendre jusqu'à des millions d'ordinateurs.

La plupart des *botnets* sont spécifiques aux réseaux HTTP et peu d'études ont été spécialement effectuées pour détecter les *botnets* des réseaux mobiles (IoT, MANET, VANET, etc.). Beaucoup des techniques utilisées pour détecter les *botnets* sont basées sur des algorithmes de *Machine Learning* ou *Deep Learning* (*Random Forest*, KNN, SVM,…).

Objectifs du projet

Le but de ce projet consiste à :
- comprendre le fonctionnement des *botnets* mobiles ;
- analyser et comparer les techniques de détection et les algorithmes utilisés ;
- répertorier les *data sets* disponibles pour réalisation de simulations ;
- améliorer une méthode existante ou proposer une méthode originale pour la détection de *botnets*.

Bibliographie

[1] https://www.kaspersky.fr/blog/quest-ce-quun-botnet/888/

Informations pratiques :

Laboratoire : LIGM
Équipe : LRT (Logiciels, R2éseaux et Temps réel)
Partenaire international envisagé : *Netherlands Organisation for Applied Scientific Research (TNO)*
Tuteur : Éric Renault (eric.renault@esiee.fr)
Filière : CyberSécurité