Analyse des proxys résidentiels

Proposition de projet informatique – automne 2023
en collaboration avec l'Équipe d'enquêtes sur la cybercriminalité
Gendarmerie Royale du Canada

Marc Frappier, professeur, Département d'informatique, Faculté des sciences

Objectif

Analyser et évaluer les services de proxys résidentiels

Decsription

Un service proxy résidentiel permet aux clients de faire passer leur trafic par une autre adresse IP résidentielle, un peu comme le permet un VPN. Les adresses IP des VPN peuvent être détectées et éventuellement bloquées, mais les adresses IP résidentielles sont plus susceptibles de paraître légitimes. Cela les rend très attrayantes pour les acteurs malicieux.

Les adresses IP résidentielles elles-mêmes sont généralement acquises par des moyens illégitimes. Par exemple, des utilisateurs peu méfiants téléchargent un "VPN gratuit" qui peut fonctionner, mais qui ajoute en fait leur PC à un pool d'adresses IP offert par le service de proxy résidentiel. Des étudiants du Département d'informatique de l'UdeS travaillant sous ma supervision (Philippe-Antoine Plante et Guillaume Joly) ont réussi à faire tomber l'un de ces réseaux en 2022, 911.re, en dévoilant son mode d'infection via MaskVPN et DewVPN.[1] Ces travaux furent cités par Brian Krebs, un des cyber-journalistes les plus influents.[2] Ils furent aussi présentés dans une conférence Teams organisée par le CRTC 130 personnes à travers le monde, comprenant des représentants de divers corps policiers à travers le monde (Québec, Canada, USA, UK, EU, Australie).

Depuis, d'autres solutions sont apparues sur le marché, par exemple, SocksEscort[3]. Le projet consiste à effectuer une analyse d'un service proxy résidentiel particulier afin de déterminer son fonctionnement. En outre, il s'agit de rechercher des programmes qui infectent des machines pour les recruter dans ces réseaux.

[1] https://gric.recherche.usherbrooke.ca/rpaas/
[2] https://krebsonsecurity.com/2022/07/a-deep-dive-into-the-residential-proxy-service-911/
[3] https://krebsonsecurity.com/2023/07/who-and-what-is-behind-the-malware-proxy-service-socksescort/