Modélisation épidémique de malware sur smartphones

OSWEILER Ronny, FONTANA Alessandro, PEUCH Laurent, ZIRANI Jean-Luc

1 Introduction

Ce stand a comme sujet la propagation de malwares (logiciels malveillants) pour Smartphones (GSM « intelligents »).

Logiciels malveillant « Malware » : Un logiciel malveillant, en anglais « malware » a été développé dans le but de nuire à un système informatique. Depuis, ils représentent une grande menace de sécurité pour l'ordinateur qui doit être muni d'un d'antivirus, logiciel conçu pour les identifier, neutraliser et/ou éliminer.

Smartphones : Les Smartphones sont des téléphones mobiles « intelligents » disposant de nombreuses fonctions telles que la consultation de courrier électronique, navigation Web, messagerie instantanée etc. Avec des connexions comme le Wifi, 3G ou EDGE, les Smartphones ont un accès facile à internet et qui leur permet de télécharger toute sorte d'applications. De ce fait, ils deviennent de véritables ordinateurs de poche.

2 Types de malwares

Il existe 2 types principaux de malwares sur Smartphones. Il existe encore un type hybride, combinant les 2 autres.

Malware Bluetooth : La propagation d'un malware via Bluetooth dépend de la mobilité humaine et est à courte distance ($\pm$10m). La propagation prend la forme d'une vague, permettant d'infecter l'ensemble des possesseurs du même type de Smartphones. Par contre, cette lenteur de propagation, permet de déployer des contre-mesures pour limiter les dégâts.

Malware MMS : La propagation via MMS est aléatoire et nécessite un pourcentage minimal de Smartphones possédant le même OS sur le marché pour pouvoir se propager correctement (min. 9.5%). Elle s'effectue par copie et envoi à tout le carnet d'adresse du Smartphone, ce qui prend une durée d'environ 2 minutes. Il s'agit d'une propagation rapide ou le déploiement de contre-mesures est difficile. Néanmoins, la propagation via MMS ne touchera pas nécessairement la totalité des possesseurs du même type de Smartphones.

Malware hybride : La version hybride se base sur le taux minimal d'existence de l'OS sur le marché et applique la méthode de propagation correspondante. Si le pourcentage est au-dessus du taux minimal, la propagation infecte la plupart via MMS et infecte le reste du marché via Bluetooth. S'il est en-dessous du taux minimal, alors le MMS n'arrive pas à toucher suffisamment de Smartphones et la propagation s'effectue via Bluetooth.

3 Simulation

Pour simuler la propagation, on utilise les mêmes modèles de simulations qui sont utilisés dans le milieu de santé dans le cas d'une épidémie. Il existe 3 modèles principaux de simulation : SI, SIS et SIR. Ces modèles définissent les 3 types d'état qui sont S (susceptible), I (infecté) et R (guéri/« recovered »). Notre simulation est basée sur le modèle SIR. Dans le modèle SIR, suite à l'épidémie et le début de contre-mesure et de l'immunisation de la population principale, le virus survit en continuant à infecter de manière limitée des populations plus faibles jusqu'à la disparition de l'immunité. À ce moment-là, une épidémie peut à nouveau avoir lieu.

4 Implémentation

Notre simulation est écrite sous Linux en utilisant le langage Python. Elle simule la propagation d'un virus dans la ville de Bruxelles. Les visiteurs du stand pourront modifier les différents paramètres de la simulation, comme par exemple la part du marché d'un OS (iOS, Windows Mobile, Android), ou le nombre moyen de contacts dans le carnet d'adresses d'un Smartphone.