Kharon : Découvrir, comprendre et reconnaître des malware Android par suivi de flux d'information

Radoniaina Andriatsimandefitra Ratsisahanana, Thomas Genet, Laurent Guillo, Jean-François Lalande, David Pichardie, Valérie Viet Triem Tong

Projet Kharon du Labex CominLabs
Découvrir, comprendre et reconnaître des malware Android par suivi de flux d'information

Radoniaina Andriatsimanefitra [3], Thomas Genet[1], Laurent Guillo [3], Jean-Francois Lalande[4,3], David Pichardie[2], and Valérie Viet Triem Tong[5]

[1]*Université de Rennes 1, IRISA, Rennes, France*
[3]*INRIA Rennes - Bretagne Atlantique, France*
[4]*INSA Centre Val de Loire, Univ. Orléans, LIFO, Bourges, France*
[2]*Ens Rennes, IRISA, Rennes, France*
[3]*CentraleSupelec, Rennes, France*

L'avènement des téléphones et tablettes ces dernières années a favorisé le développement d'un nouveau modèle économique qui repose sur la livraison d'un téléphone nu sur lequel l'utilisateur peut installer des applications via des *magasins d'applications ou marchés*. Ces marchés sont aussi bien officiels car approuvés par les entreprises développant les systèmes d'exploitations de ces téléphones comme Google Play ou AppStore ou non officiels. Dans ce qui suit, nous nous consacrons aux téléphones et tablettes utilisant le système d'exploitation Android sur lesquelles un utilisateur peut installer des applications via Google Play. Sur ce marché, nous trouvons beaucoup d'applications (plus de un million d'applications) téléchargées par beaucoup d'utilisateurs. Une même application peut être téléchargée plus de 100 millions de fois. Les développeurs de ces applications sont d'origines très variées puisque pour la modique somme de 25 USD n'importe qui peut créer un compte développeur pour ce marché et distribuer sa propre application. Il est aussi possible d'installer des applications sans passer par Google Play. Android est ainsi devenu rapidement une cible de choix pour les développeurs malveillants et le nombre de malware n'a cessé d'augmenter pour atteindre 10 millions d'applications malveillantes en 2012-2013 selon Kaspersky [1].

Ces malware essaient principalement de soutirer de l'argent à un utilisateur. Par exemple, le malware Simplelocker [2] chiffre sur le téléphone les données de l'utilisateur comme ses photos, ses documents les rendant ainsi inutilisables et demande ensuite une rançon pour déchiffrer ces mêmes données. D'autres comme DroidKungFu1[3] installent des applications à l'insu de l'utilisateur. D'autres encore envoient des sms à des numéros sur-taxés à l'insu, là encore, de l'utilisateur. Ces malware sont souvent *repackagés* dans différentes applications pour atteindre

un plus grand nombres d'utilisateurs et se disséminer plus aisément dans l'offre disponible.

Pour débarrasser le marché de ces applications malveillantes, il existe deux grandes approches : l'analyse statique du bytecode des applications et l'analyse dynamique des exécutions de ces applications.

Le but du projet Kharon est de développer une plateforme d'analyse dynamique utilisant le suivi de flux d'information. Cette analyse dynamique surveillera le comportement d'un malware et étudiera comment ce malware se dissémine dans le système d'exploitation. Nous avons montré dans [4] que cette approche permet de créer des signatures comportementales de malware, c'est à dire des descriptions précises du comportement de ces malware. Cette approche se base sur l'hypothèse forte que le malware s'exécute effectivement durant l'analyse dynamique. Cette hypothèse n'est pas acceptable en pratique car les expériences que nous avons menées montrent que la plupart des malware ne s'exécutent pas automatiquement au lancement de l'application. Ces malware attendent des évènements particuliers comme l'envoi d'une commande par un serveur distant, une date précise, une série d'actions de l'utilisateurs. Dans le projet Kharon, nous proposons utiliser l'analyse statique pour découvrir quels sont ces évènements déclencheurs et développer une méthode de fuzzing utilisant ces données.

Ce projet regroupe des membres de l'équipe Celtique et Cidre de l'IRISA. L'équipe Celtique est spécialisée en analyse statique de bytecode java [5] et l'équipe Cidre a proposé les signatures comportementales utilisées dans ce projet. Les membres à temps plein de ce projet sont actuellement un ingénieur expert et un étudiant en master 2. Ce projet a débuté en janvier 2015.

Dans le cadre de la conférence RESSI, nous proposons de faire une présentation des objectifs de Kharon et de les illustrer au travers d'une démonstration.

Références

[1] "Kaspersky web site," http ://www.kaspersky.com/about/news/virus/2014/Mobile-malware-evolution-3-infection-attempts-per-user-in-2013.

[2] "Android community web site," http ://androidcommunity.com/simplelocker-a-holds-your-sd-card-hostage-using-encryption-20140606/.

[3] http://www.csc.ncsu.edu/faculty/jiang/DroidKungFu.html.

[4] R. Andriatsimandefitra and V. Viet Triem Tong, "Capturing android malware behaviour using system flow graph," in *NSS 2014-The 8th International Conference on Network and System Security*, 2014.

[5] L. Hubert, N. Barré, F. Besson, D. Demange, T. Jensen, V. Monfort, D. Pichardie, and T. Turpin, "Sawja : Static Analysis Workshop for Java," in *Proc. of the 1st International Conference on Formal Verification of Object-Oriented Software (FoVeOOS 2010)*, 2010.