HAL
open science

Le projet CominLabs Kharon: aidons les malwares à s'exécuter

Jean-François Lalande, Valérie Viet Triem Tong

To cite this version:

Jean-François Lalande, Valérie Viet Triem Tong. Le projet CominLabs Kharon: aidons les malwares à s'exécuter. RESSI 2018 - Rendez-Vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information, May 2018, Nancy / La Bresse, France. pp.1. hal-01794223v2

HAL Id: hal-01794223

https://centralesupelec.hal.science/hal-01794223v2

Submitted on 17 May 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Le projet CominLabs Kharon: aidons les malwares à s'exécuter

Jean-François Lalande and Valérie Viet Triem Tong

CentraleSupélec, Inria, Université de Rennes 1, CNRS, F-35065 Rennes
jean-francois.lalande@centralesupelec.fr, valerie.viettriemtong@centralesupelec.fr

Abstract

Le projet Kharon est un projet du laboratoire d'excellence CominLabs, dont l'objectif est d'étudier les comportements des malwares pour téléphones mobiles. Le projet a débuté en 2015 et se termine en 2018. Il implique plusieurs partenaires académiques: Inria Rennes Bretagne Atlantique, CentraleSupélec et l'INSA Centre Val de Loire. Dans la présentation pour la conférence RESSI, nous proposons de présenter la problématique traitée et les résultats principaux obtenus durant ce projet.

Lors du projet Kharon, nous nous sommes intéressés à l'observation de l'exécution de malwares Android. Cette observation se déroule au niveau du système d'exploitation, à l'aide de l'IDS Blare[1]. La version Android de Blare permet de surveiller la propagation d'une marque depuis un objet ou un processus vers d'autres objets ou processus. En marquant le fichier APK du malware, on peut ainsi suivre les opérations qu'il réalise au sein d'un téléphone mobile.

Afin de pouvoir traiter automatiquement un grand nombre de malwares, nous avons développé la suite logicielle GroddDroid[2] qui permet d'orchestrer l'analyse c'est-à-dire l'analyse statique, le déploiement sur un téléphone surveillé par Blare, la stimulation de son interface graphique, la récolte des logs de l'expérience et la visualisation des résultats. Entre chaque expérience, GroddDroid réinitialise le téléphone, au cas ou celui-ci aurait été compromis par le malware testé. Tous les outils intégrés dans la suite logicielle sont le fruit de travaux de thèse (R. Andriatsimandefitra, M. Leslous) qui ont successivement amélioré la qualité des résultats obtenus lors de l'analyse d'un malware.

Le projet Kharon présente aussi les résultats obtenus sous la forme d'une plate-forme de démonstration déployée dans le LHS (Laboratoire de Haute Sécurité) d'Inria. Cette plate-forme[3] permet de présenter les expériences réalisées au travers d'un site web. À moyen terme, ce prototype pourrait devenir un service en ligne pour les utilisateurs finaux.

D'un point de vue des publications, nous avons présenté à plusieurs conférences les contributions suivantes: l'orchestrateur GroddDroid [1]; l'utilisation d'appels implicites par les malwares [3]; la caractérisation des applications bénignes [4]; la construction d'un dataset [2].

References

[1] A. Abraham, R. Andriatsimandefitra, A. Brunelat, J.-F. Lalande, and V. Viet Triem Tong. GroddDroid: a Gorilla for Triggering Malicious Behaviors. In *10th International Conference on Malicious and Unwanted Software*, pages 119–127, Fajardo, Puerto Rico, Oct. 2015. IEEE Computer Society. Best Paper Award.

[2] N. Kiss, J.-F. Lalande, M. Leslous, and V. Viet Triem Tong. Kharon dataset: Android malware under a microscope. In *The Learning from Authoritative Security Experiment Results (LASER) workshop*, pages 1–12, San Jose, United States, May 2016. USENIX Association.

[3] M. Leslous, V. Viet Triem Tong, J.-F. Lalande, and T. Genet. GPFinder: Tracking the Invisible in Android Malware. In *12th International Conference on Malicious and Unwanted Software*, Fajardo, Puerto Rico, Oct. 2017. IEEE Conputer Society.

[4] V. Viet Triem Tong, A. Trulla, M. Leslous, and J.-F. Lalande. Information flows at OS level unmask sophisticated Android malware. In *14th International Conference on Security and Cryptography*, volume 6, pages 578–585, Madrid, Spain, July 2017. SciTePress.

[1] http://www.blare-ids.org
[2] http://kharon.gforge.inria.fr/grodddroid.html
[3] http://kharon.irisa.fr