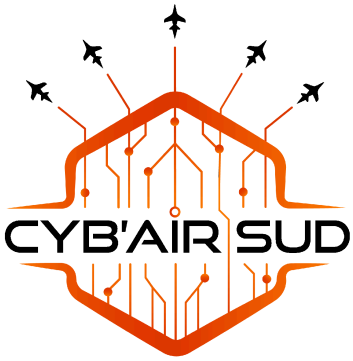


Obfuscation of Android Malware: Packing and Unpacking

CFP 2025 — English Version

Speaker: Alain M.

Short Description

This presentation focuses on several techniques specific to Android packers and on the methods used to recover the original code.

Detailed Summary

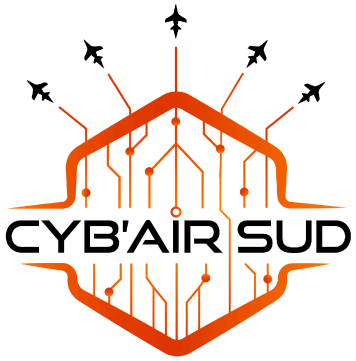
Obfuscation, whether legitimate or not, significantly complicates reverse-engineering work by making code far less readable and much more difficult to analyze. It encompasses numerous techniques—encryption, polymorphic or metamorphic approaches—all of which modify or alter the code. These increasingly sophisticated and effective techniques fuel the ongoing cat-and-mouse game between attackers and defenders.

During this presentation, we will illustrate several mechanisms observed in a recent malware sample, as well as the methodological approach used to analyze them.

Other Information

— Duration: 30 minutes

— Language: French



Obfuscation des malwares Android : Packing et Unpacking

CFP 2025 — Version Française

Intervenant : Alain M.

Description concise

Cette présentation se concentre sur quelques techniques propres aux packers sous Android et sur les méthodes permettant de retrouver le code d'origine.

Résumé détaillé

L'obfuscation, qu'elle soit légitime ou non, complexifie considérablement le travail de rétro-ingénierie en rendant le code beaucoup moins lisible et plus difficile à analyser. Elle englobe de nombreux procédés : chiffrement, techniques de polymorphisme ou de métamorphisme... autant de méthodes qui modifient ou altèrent le code. Ces techniques, de plus en plus élaborées et efficaces, alimentent l'éternel jeu du chat et de la souris entre attaquants et défenseurs.

Au cours de cette présentation, nous illustrerons plusieurs mécanismes observés sur un malware récent ainsi que la démarche méthodologique adoptée pour les analyser.

Autres informations

— Durée : 30 minutes

— Langue : Français