Présentation de DroidMal-Dec Tool

1. **Contexte Général (En version Originale)** The astonishingly widespread adoption of the Android operating system has been accompanied by the spread of malware across the Android ecosystem at an alarming rate. Detecting malicious software is thus a key issue and represents a huge challenge. At the same time, several studies have shown that experimental datasets used in the literature are too small and biased, resulting in misleading reported malware detection rates.

   We are promoting a methodology to generate realistic malware corner cases that are designed to challenge antivirus scanners. In particular we have demonstrated that we are able to massively generate malware variants to successfully evade state of the art scanners from both academia and industry. The purpose of this hackathon is to explores way to challenge scanners to improve their detection algorithms.

2. **Travail Proposé**
   - Un Modèle Machine Learning permettant de prédire à partir du fichier de permissions de l'application apk si ce dernier est maligne ou bénigne.
   - Un Tableau de Bords pour la visualisation du travail

3. **Méthodologie de Travail Proposé**
   - Un module python permettant d'extraire le fichier de permissions des applications contenus dans les répertoires **./MalwareAPK** pour les malignes et **./BenignAPK** pour les bénignes. Il suffit pour l'utilisateur sur son terminal de taper la commande suivante sur son terminal : ***python3 ExtractorAIO.py***
   - Un Modèle Machine Learning pour l'entrainement et la sauvegarde permanente et l'entraînement du module de prédiction
   - Un fichier utilisant **Streamlit** pour la visualisation du travail

4. **Limites**
   - Problèmes de dépassement de tampon lors du traitement de certains fichiers android
   - Pour le moment, il faudra passer par les informations du fichier csv, algorithme de réception directe du fichier apk en test/implémentation

5. **Perspectives**
   - **Scientifique** : Améliorer le module d'extraction de caractéristiques en trouvant des mécanismes simples de résolution du problème de dépassement de mémoire
   - **Professionnel** : Amélioration et Unification du Processus de travail côté utilisateur final

- Superviseurs du Travail :
  - **David BROMBERG**

- **Djob MVONDO**
- **Alain TCHANA**

— Candidat : **MEGNA MFOUAKIE Ibrahim : (+237) 697-816-276/ 679-117-027 hibrahimmfouakie@gmail.com**
— Date : **29/12/2023**
