DroidMage 恶意代码检测平台

张东红 (导师：张震宇)

zhangdh@ios.ac.cn

DroidMage 是一个Android恶意代码检测平台。它以市面主流应用市场应用为基础样本库，基于恶意代码图像技术，训练深度学习模型对未知样本进行检测。

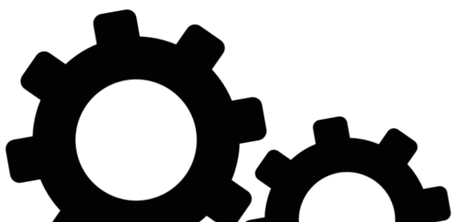
How does it work?

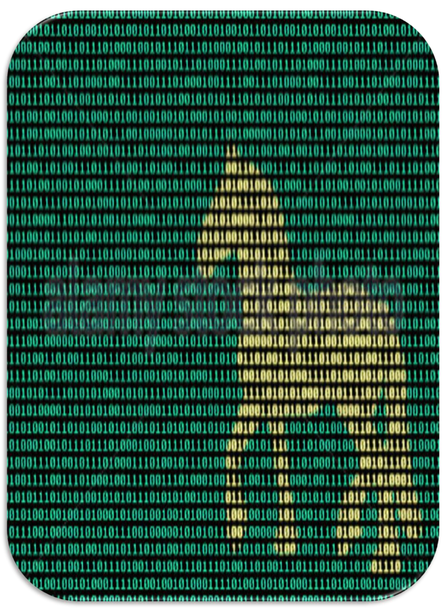
Input Raw Data

HUAWEI

Google Play

Model Training





Malware Images

It is malicious!

Model Trained

Input Data

What are the advantages?

- 基于恶意代码图像技术处理样本
- 自动化处理样本并进行恶意代码检测
- 使用卷积神经网络深度学习模型进行检测

What can it be used for?

- 识别新型Android恶意代码
- 识别 Android恶意代码家族
- 分析现有应用市场安全现状
- Android应用安全性评分

References

[1] 张东红,张震宇. 一种恶意代码自动化检测平台及方法[P]. CN108920954A,2018-11-30.

[2] 张东红.基于文本分类技术的恶意代码检测工具[J].电子产品世界,2018,25(09):75-76+74.

[3] Donghong Zhang, Zhenyu Zhang, Bo Jiang, and T.H. Tse, "The Impact of Lightweight Disassembler on Malware Detection: An Empirical Study", in Proceedings of The 42nd IEEE International Conference on Computers, Software and Applications, Tokyo, Japan.