第六代Android QDEX VMP加固引擎

嘉宾:孙日新

嘉宾职务:高级安全研究员

目录

CONTENT

01

加固技术的演化史

动态加载

依赖于Android系统提供DEX动态加载机制

不落地加载

使用Android虚拟机接口直接将内存中DEX数据进行加载

指令抽取

将用户DEX核心代码抽离加密保护，运行时进行还原

虚拟机

将用户DEX核心代码用VMP(虚拟机)去动态解释指令

OLLVM

采用自研PASS对指令进行平坦化等混淆处理，以及字符串加密和IR进行VMP处理，使指令更加隐蔽

02

现阶段安全防护强度

现阶段安全防护优势

- 颗粒维度方式进行VMP保护
- 安全密钥采用自研算法生成
- 操作码类型隔离，不同类型操作码不同算法
- 加固引擎核心，采用OLLVM VMP双重保护方案

现阶段安全防护不足

- 数据与系统存在关联性
- 使用标准DEX文件格式
- Dalvik字节码固定长度

03

第六代加固引擎

重构DEX文件

重新定义DEX文件，独立区别于系统之外。VMP解释引擎依赖自定义DEX文件进行动态执行

流式编码

对指令进行多种样式的自定义编码，用多种比特位数方式进行相应的编码转换。

独立指令操作码

QDEX VMP引擎自定义操作码，不依赖DEX与系统，完全脱离系统指令集，无法通过系统操作码表还原。

无缝兼容高级加固功能

使用QDEX VMP引擎，不会影响资源加密 、文件校验、环境检测等各种高级功能的使用。

04

未来的展望

持续对抗

三六零天御在持续对抗过程中不断优化与调整加固引擎，给用户提供安全、性能、兼容性等一体化的移动应用安全产品。

感谢聆听

三六零天御致力守护移动数字安全