**2018 Q1季度 贡献**

**移动安全研究：**

* Android恶意软件检测模型 1个，检测率97%， 样本数5万。
* 投稿期刊论文 1篇（AI与android恶意软件检测）
* 输出论文阅读笔记24篇，方向涉及：恶意软件检测、apk加壳脱壳、机器学习、对抗分析等

**移动组：**

* Q1移动组 gdcert 3篇前沿报告，自评总分占比20%
* 2017年移动安全分析报告中，提供3组统计分析数据

**病毒分析：**

* 寻找恶意软件Globe Imposter样本 2 个
* 对 2个 PE木马进行文件分析,并且进行脱壳操作
* 输出态势感知组 2个病毒的分析报告

**未来研究方向：AI与Android恶意软件检测**

**目标O**

* 改善 apk 恶意软件的AI检测引擎，并增加引擎支持更多分类类型的功能

**时间范围**

* 2018 Q1-Q4

**可量化的关键成果KRs**

1. （基础）收集检测的 APK 数据至 20 万
2. （中级）增加 恶意软件家族 分类模型 1 个,识别率 到达 95%(FlowDroid-->Soot)
3. （中级）输出 实验报告 1 篇
4. （中级）增加 HSO 模型 1 个,识别率 到达 98%
5. （中级）增加 “深度特征” 2 个 提取（对 特征 按照深度 进行 排列,N-gram/敏感API调用依赖关系/上下文常量分析/API调用序列图/污点跟踪等,有必要的话,还需要研究动态分析相关技术,或者 静态/动态 脱壳技术），并 根据 4大国际 安全论文集，更新 现有 特征集，不再 仅停留于 浅层特征，最终 目的是 ：提高模型 的 健壮性
6. （高级 - 论文写作）新 完成 英文论文一篇 并 提交 到 信息安全 顶级会议中
7. （高级 - 研究方向初步确定）阅读并收集 至少 20份 顶会论文，形成自己独有的研究方向2个，由此产生技术壁垒