**李德圆研究工作进展与规划**

目录

[一、2018年Q2已完成工作概述 1](#_Toc521403199)

[1.1 PE恶意文件静态检测技术研究成果 1](#_Toc521403200)

[1.2技术支持 2](#_Toc521403201)

[1.3 Q2季度KR与自我评定 2](#_Toc521403202)

[二、2018年Q3工作OKR 2](#_Toc521403203)

[2.1Windows恶意文件检测引擎 2](#_Toc521403204)

[目标O 2](#_Toc521403205)

[2.2深度神经网络 2](#_Toc521403206)

[目标O 2](#_Toc521403207)

[2.3 Key Results（可量化的关键成果） 3](#_Toc521403208)

# 一、2018年Q2已完成工作概述

蓝盾第三代FW的AI引擎，在实验环境下可以达到99%的识别率，体现出AI技术的巨大前景。我们从AI引擎的本地化及自主研发的角度，结合当前Windows恶意文件检测的新技术、大数据技术、以及安全对抗的新形势，致力于实现一个可用于公司安全产品检测引擎。

## 1.1 PE恶意文件静态检测技术研究成果

1）基于Spark大数据平台的PE文件检测系统特征算法优化与调试，**1个**

2）融入多学科知识优化PE深度恶意文件检测系统（**1个**），可视化功能（**1个**）与关键片段定位（**1个**），识别率可达**95.19%**，

3）加入对抗性学习与特征有效性与PE投稿论文（**1个**）：

4）收集与阅读国内外安全前沿技术论文，方向涉及：

收集论文：**35篇**，涉及病毒分析、AI安全与部署、异常流量分析、自然语言处理等

精读：Linux病毒分析（1篇）、AI模型一致性评估与自动更新时机选择（1篇）、人脸识别系统的后门攻击（1篇）、NLP中分类算法与摘要算法（若干）等

## 1.2技术支持

1）数据中心构建与维护

2）论文知识分享平台设计

## 1.3 Q2季度KR与自我评定

1. （中级）改善大数据PE恶意文件检测引擎，识别率可达95%，百万数据，**（评分：7），目前数据在进一步收集扩大和验证模型，过度到Q3季度**

2. 基于深度学习的恶意文件检测引擎

1）（初级）学习与生成经典的深度学习架构，如resnet等（**评分：10**）

2）（中级）结合深度学习与语义分析等相关研究，设计可用于恶意文件检测的深度学习架构**（评分：10**）

3）（高级）实现 基于深度学习 的 恶意文件检测引擎，识别率 >= 90%,(Test:50W)**（评分：6），目前数据有所欠缺，小数据集可达到95%的识别率，过度到Q3季度**

3. 前沿技术 文献阅读 & 知识分享

1）（中级）阅读并收集 至少10篇（其中，精读3篇）安全有关的 顶会论文，为公司提供 知识储备 和 前沿动态分析。**（评分：8）**

# 二、2018年Q3工作OKR

## 2.1Windows恶意文件检测引擎

### 目标O

* 自研PE恶意文件检测引擎，可部署于公司的云安全产品等

## 2.2深度神经网络

### 目标O

* 提升 PE 大数据 检测引擎 识别率
* 继续提升 基于深度学习 的 恶意文件检测引擎 识别率

## 2.3 Key Results（可量化的关键成果）

1. 在当前 **基于人工智能的PE检测引擎** 基础上，从 识别率 方面 改善 引擎：

* 1）提升现有的PE检测引擎性能，大数据基础下训练与识别（Training：>=200W , Test: >= 100W），识别率 需达到 >= **95%**

1. 基于 **深度学习** 的恶意文件检测引擎

* 1）提升 基于深度学习 的 恶意文件检测引擎，识别率 **>= 90%,(Test:50W)**
* 2）深度模型可解释性分析，关键 片段 定位与解析

1. 技术预研：流量异常检测，Side Project

* 1）除 主项目 基于人工智能的PE检测引擎外，预研 基于AI的 **异常流量** 检测模型，论文收集 至少10篇， 技术比较分析报告 1 份

1. 前沿技术 文献阅读 & 知识分享

* 1）阅读并收集 至少10篇（其中，精读3篇）安全有关的 顶会论文，为公司提供 知识储备 和 前沿动态分析