**\*\*\*研究工作进展与规划**

目录

[一、工作概述 1](#_Toc513732644)

[1.1 PE恶意文件静态检测 1](#_Toc513732645)

[1.2技术支持 1](#_Toc513732646)

[二、2018年OKR 2](#_Toc513732647)

[2.1 Windows恶意文件检测引擎 2](#_Toc513732648)

[目标 O 2](#_Toc513732649)

[关键成果KR 2](#_Toc513732650)

[2.2深度神经网络 2](#_Toc513732651)

[目标O 2](#_Toc513732652)

[关键成果KR 2](#_Toc513732653)

# 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

1）基于Spark大数据平台的PE文件检测系统设计，在百万测试数据，识别率接近95%

2）基于深度学习的PE文件检测系统，在小数据集中，识别率接近90%

3）投稿期刊论文一篇

4）收集与阅读国内外安全前沿技术论文，方向涉及：

沙箱逃逸，AI与恶意文件检测，深度学习等

## 1.2技术支持

1）沙箱技术原理解析、技术交流、技术支持

2）病毒文件收集与行为分析

3）AI化产品咨询等

# 二、2018年Q3工作OKR

## 2.1 Windows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

### 关键成果KR

* 完成1篇恶意文件检测方面的论文；
* 实现性能可对标TP的AI引擎，可部署于公司云安全等产品；

## 2.2深度神经网络

### 目标O

* 将深度学习与公司安全产品结合，提出可行的解决方案

### 关键成果KR

* 完成至少1篇基于深度学习的恶意文件检测相关的论文或专利；
* 完成至少2项基于深度学习的恶意文件检测相关的技术方案设计与实现；