2017年北京市科学技术奖二等奖

恶意软件深度分析与检测关键技术及应用

苏璞睿、应凌云、严寒冰、钱秀槟、杨轶、
李琦、聂眉宁、王继刚、游浣权、闫佳

{purui, lingyun}@iscas.ac.cn

针对APT攻击、未知漏洞利用等高级攻击检测和复杂恶意代码分析的需要，基于硬件模拟技术、动态行为分析、控制流完整性分析等关键技术研制了金刚（KingKong）软件智能分析系统及系列安全产品，提供恶意代码检测、网络攻击防御、攻击实现机理分析等不同类型的安全服务。相关论文已经发表在USENIX Security、RAID、DSN、 ACSAC等国际会议上，系统已经在百度、中兴通讯、CNCERT、国测等单位实际应用。

主要技术特点

基于行为检测：不依赖于代码指纹和漏洞特征，可检测未知漏洞攻击；
适配多种平台：支持32位/64位的Windows、Linux及Android系统；
多种分析模式：提供全自动、半自动和人工分析接口，支持文件和流量输入；
行为全面监控：监控2000多个系统行为，可识别数百种恶意行为；
多重环境模拟：预置数十种分析环境，具备网络环境和人机交互模拟能力；
攻击过程识别：可识别堆喷射、ROP、代码注入、异常控制流转移等攻击过程。