APT攻击检测关键技术研究与应用

苏璞睿、杨轶、闫佳、和亮、聂楚江

purui@iscas.ac.cn

获2018年通信学会科学技术一等奖

项目背景

高级持续性威胁(APT, Advanced Persistent Threat)攻击，是情报机构、黑客组织针对高价值目标实施的高隐蔽性、高破坏性攻击。高对抗性背景下的APT攻击检测、分析与追踪是网络安全领域亟需解决的重要技术难题。

主要创新点

中国科学院软件研究所软件智能分析协同创新团队从流量深度分析角度入手，突破了基于硬件模拟的流量深度分析，基于漏洞利用过程异常的网络攻击检测，基于细粒度数据流分析的网络攻击机理分析以及网络攻击溯源等关键技术，为APT攻击检测技术研究奠定了基础方法与技术，提升了网络攻击追踪溯源能力和应急处置能力。

成果鉴定

经中国通信学会组织的专家鉴定认为：项目“研究成果整体达到国内领先，国际先进水平，对类攻击代码的识别等技术达到国际领先水平。”

成果应用

项目研制系列产品已在电信、政务、金融、国家基础设施等行业和重要部门应用，发现了一系列的攻击威胁，同时，相关成果也在国家APEC会议、抗战胜利70周年纪念等重大活动保障中发挥重要作用，相关工作成绩多次获得国家领导人肯定与嘉奖，取得了显著的经济效益和社会效益。