TCA软件动态分析系统

苏璞睿　应凌云
{purui, lingyun}@iscas.ac.cn

面向APT攻击、0 Day漏洞利用、网络间谍等高级攻击活动的检测和分析需求，基于硬件模拟技术、软件动态行为分析方法、控制流完整性分析方法等关键技术研制的软件分析系统，可用于软件行为实现机理分析、恶意代码检测、软件安全性评估、网络安全教学等工作。

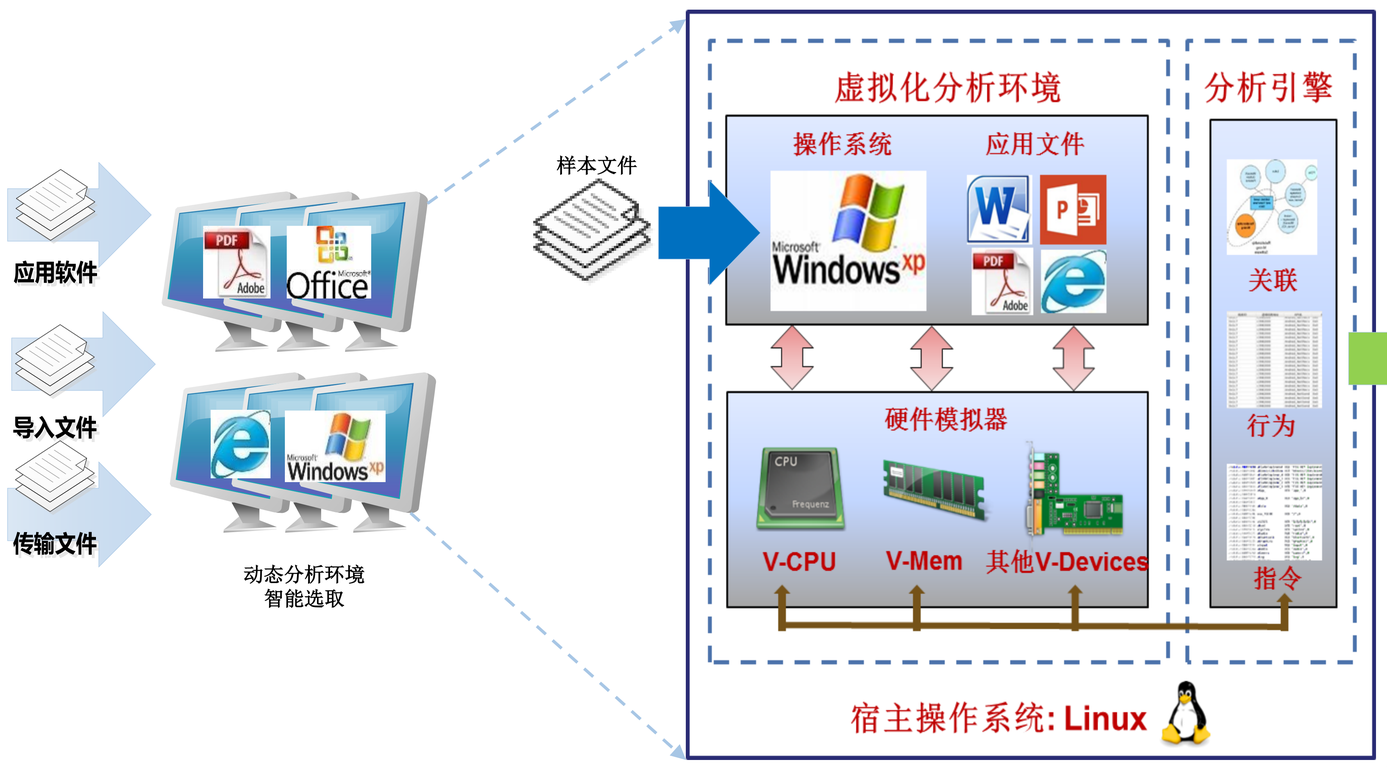
功能特点

- 基于行为模式检测，不依赖于静态特征匹配，可检测未知漏洞利用和攻击；
- 适配多种体系架构，支持Windows、Linux、Android等系统环境；
- 支持多种系统平台，支持32位、64位操作系统的虚拟系统环境；
- 支持多种文件格式，支持exe、dll等代码，office、pdf等文档，图片、网页等文件；
- 具备多种分析模式，提供全自动、半自动和人工分析三种接口。

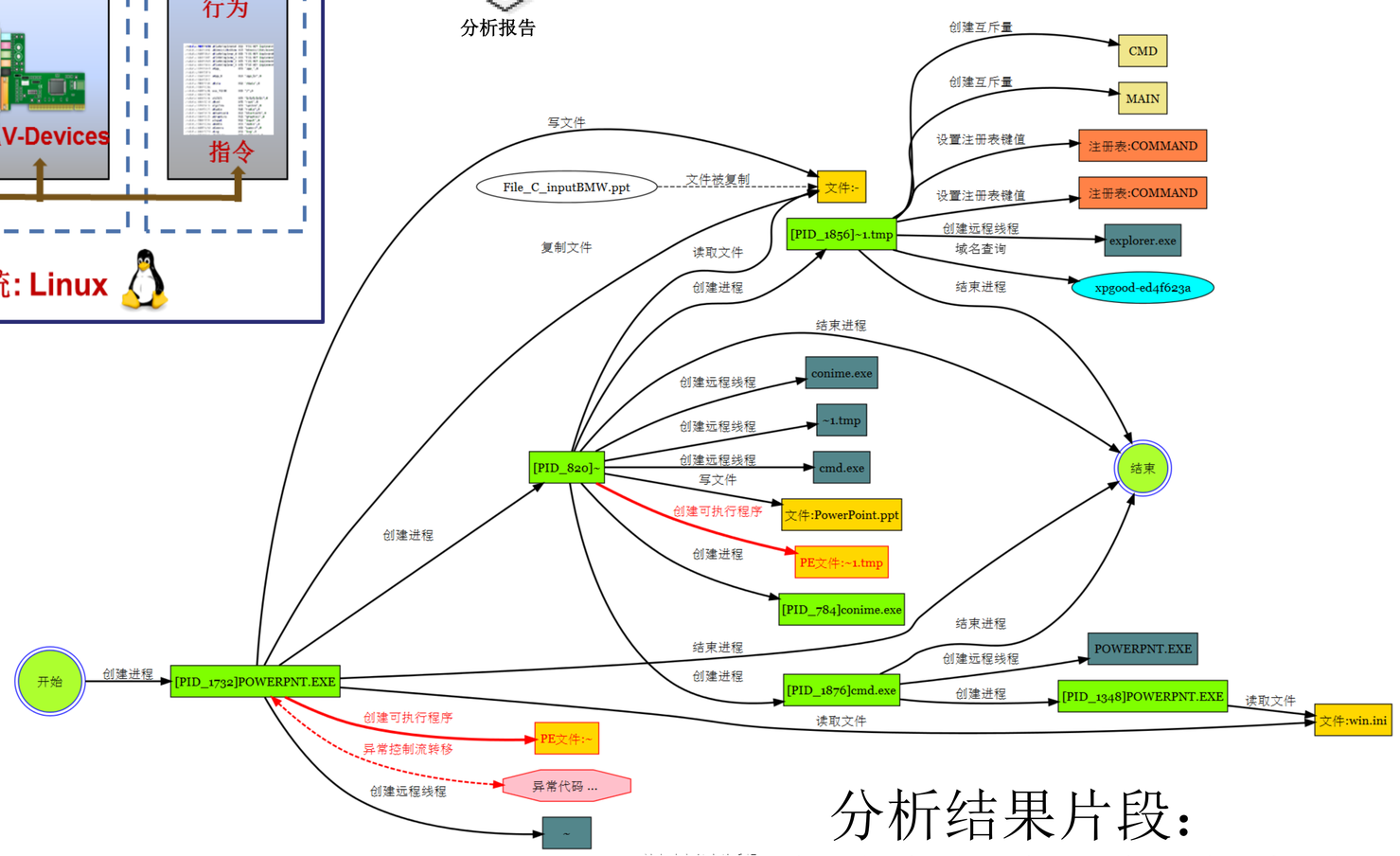
技术指标

- 行为监控能力：监控2000多个系统行为，可识别数百种恶意行为；
- 环境仿真能力：预置数十种典型分析环境，并可按需定制和扩展；
- 网络模拟能力：可模拟DNS、HTTP、SMTP、POP3、FTP等典型网络服务；
- 攻击识别能力：可识别堆喷射、ROP、代码注入、异常控制流转移等攻击过程；
- 分析对抗能力：可模拟用户自动完成UI操作，可识别并跳过耗时的延时代码。

该系统相关研究论文已经发表在RAID、ACSAC、SECURECOMM等国际会议上，系统已经在百度、中兴通讯、CNCERT、中国信息安全测评中心等单位实际部署应用，日均分析超过50万个样本文件。



样本分析流程示意图



分析结果片段：
样本动态行为逻辑关系图