“锐剑”——一站式反软件保护解决方案

主讲人：钱艺轩

目录

Add your valuable title

第一部分 项目简介

项目简介

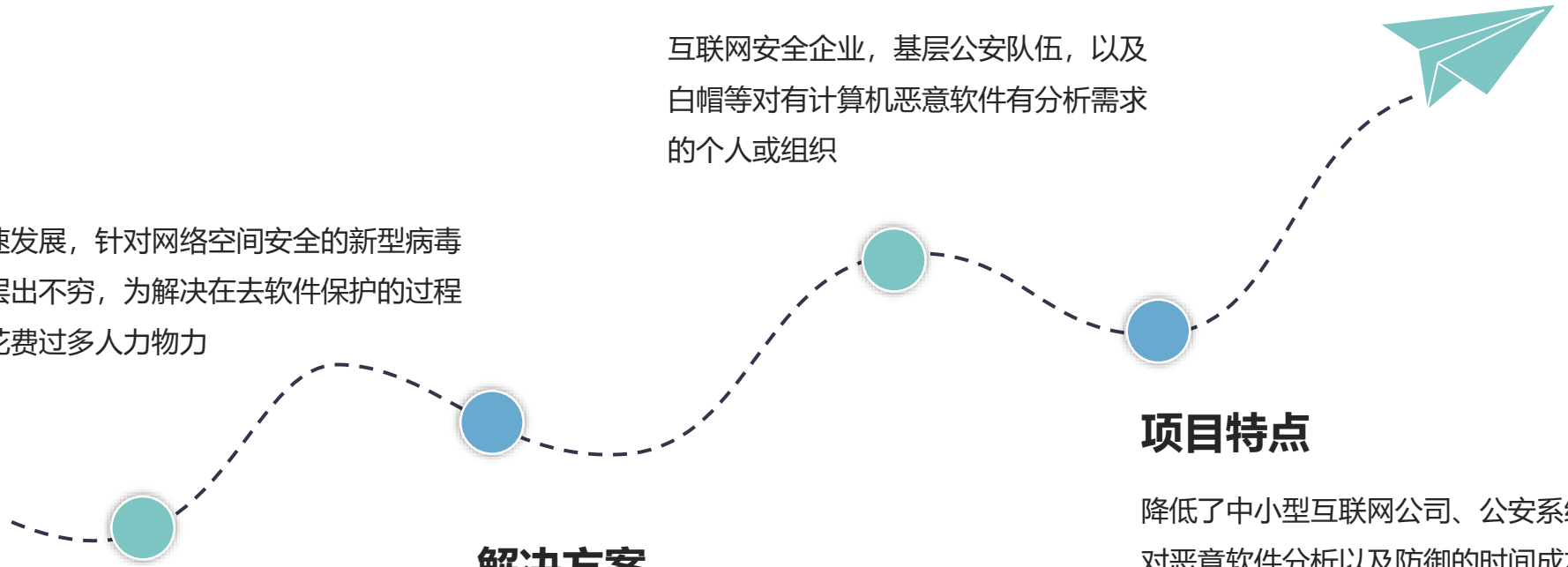
Add your valuable title

现有问题

互联网技术飞速发展，针对网络空间安全的新型病毒以及恶意软件层出不穷，为解决在去软件保护的过程中的分析需要花费过多人力物力

主要用户

互联网安全企业，基层公安队伍，以及白帽等对有计算机恶意软件有分析需求的个人或组织



解决方案

包括两大部分：恶意软件分析优化方案、恶意软件行为分析及应急响应方案。

项目特点

降低了中小型互联网公司、公安系统等对恶意软件分析以及防御的时间成本，尽可能损失，具有成本低、可靠性强、实用性高的特点。

项目简介

具体功能

二进制反反跟踪

恶意代码编写者防止恶意代码逻辑被调试观察，尽可能地延长恶意代码的分析时间的技术。

去控制流平坦化

通过一个主分发器来控制程序基本块的执行流程，从而模糊基本块之间的前后关系，增加程序分析的难度

去虚假控制流

通过加入包含不透明谓词的条件跳转和不可达的基本块来干扰IDA的控制流分析和F5反汇编。

软件脱壳

利用特殊的算法，对可执行文件里的资源进行压缩，阻止外部程序或软件对加壳程序本身的反汇编分析或者动态分析

社会价值

提供给运维人员有效的应急响应方案

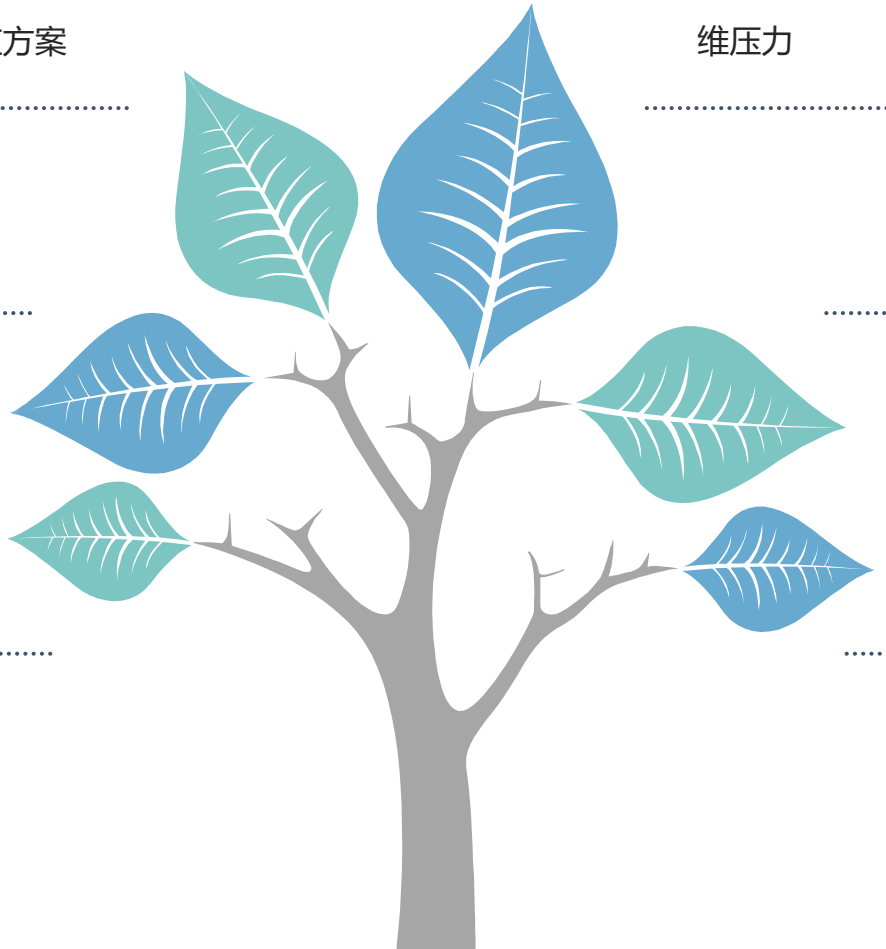
缓解中小型互联网企业的运维压力

减少分析恶意软件需要的工作量

提高互联网工资分析软件的效率，减少分析的经济成本

提供完整的分析方案，尽快完成恶意软件的分析及总结

增加破案的效率，极大程度降低恶意软件的损害



社会价值

面向不同的用户

实践过程

Add your valuable title

技术实现

二进制反反跟踪技术、去控制流平坦化技术、去虚假控制流技术、软件脱壳技术

技术整合

我们将多种技术综合利用并优化，整合到一个软件中，提出有针对性的应急响应方案

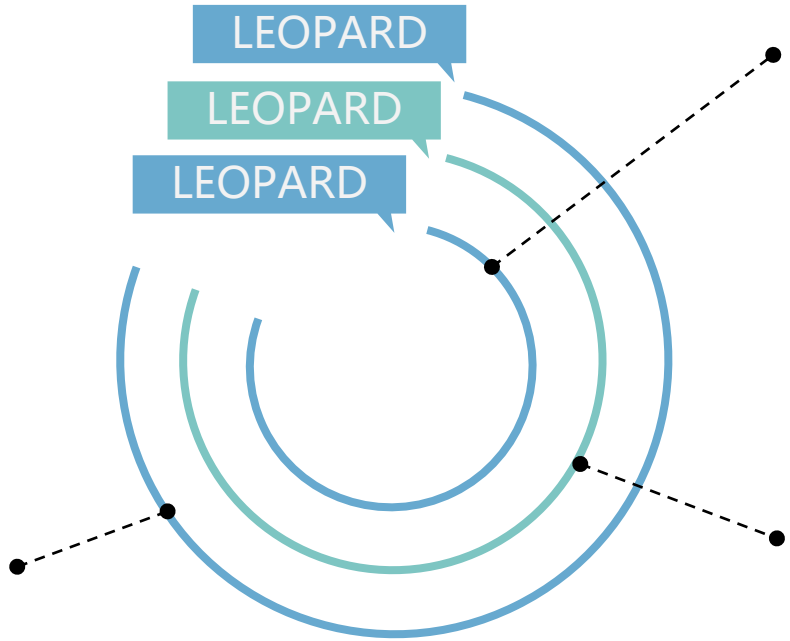
在初期针对多种不同种类的恶意软件的实验中，显著的减少了恶意软件分析的前期工作所花费的人力物力，大大提高了恶意软件分析的效率。

创新意义

- 改变传统的被动防御方式，主动防御的同时能够提供有效可行的应急解决方案。
- 病毒分析的前置条件与工作繁重，在遭受到病毒攻击时往往需要大量的人力以及物力。
- 现行互联网中暂且没有能够高效解决恶意代码以及病毒的外部保护的软件。

发展前景

Add your valuable title



提高基层民警进行电子取证的工作效率，减少工作压力

为中小型互联网企业，提供便捷的恶意软件分析程序

为较大型的互联网企业提供针对勒索病毒，后门程序等各种恶意软件的响应方案以及技术支持

团队协作

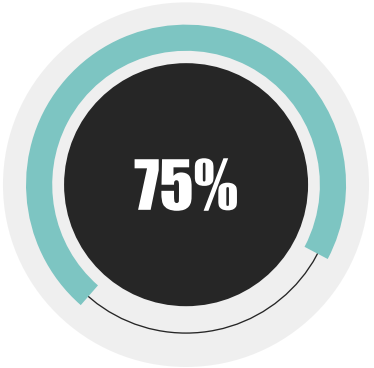
Add your valuable title

思路构想

本项目基于反反调试，全平台自动化脱壳机等项目，实现一个一站式反软件保护的解决方案

技术实现

由姚景宸，钱艺轩，钟宜均，颜瑞彬分别研究解决主要核心功能



平台整合

由姚景宸整合优化形成一个一站式反软件保护平台

非常感谢您的聆听