

Badkid: ELF 文件病毒设计报告

柯嵩宇, 陈天垚, 万诚, 杨润哲

2014 级 ACM 班

January 3, 2017

这篇文档的目的, 在于还原我们小组对我们的 ELF 文件病毒 “badkid” 的设计过程, 以及我们在整个设计过程中的技术思考。但请原谅, 我们不会在此文中专门介绍 ELF 文件格式等网上随处可搜到的内容, 而是力图忠实地记录我们在实现设计目标中 “走过的弯路” 与 “乍现的灵光”, 希望以此给那些想要亲自动手写一个 ELF 文件病毒 (或是想要对抗此类病毒) 读者, 带来一些有益的启发。

Contents

1 项目简介	2
2 主要技术	2
2.1 初尝试: 一个静态病毒?	2
2.2 PIE: 位置无关可执行文件	2
2.3 使用一个 Wrapper	2
2.4 终极思路: 感染共享库	2
3 具体实现	2
3.1 源码解析	2
3.2 一些实验	2
4 小结	2

1 项目简介

此项目中，我们的目的是设计一个感染 ELF 文件的寄生病毒：当一个 ELF 文件受其感染时，会修改它的头入口点（entry point）；当用户运行一个被感染文件时，就会先执行病毒代码，感染同目录下的其他文件，从而达到复制与寄生的效果。

2 主要技术

- 2.1 初尝试：一个静态病毒？
- 2.2 PIE：位置无关可执行文件
- 2.3 使用一个 Wrapper
- 2.4 终极思路：感染共享库

3 具体实现

- 3.1 源码解析
- 3.2 一些实验

4 小结