Badkid: ELF 文件病毒设计报告

柯嵩宇，陈天垚，万诚，杨闰哲

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

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，从而达到复制与传播的效果。寄主程序运行顺序的执行顺序如图 1所示。

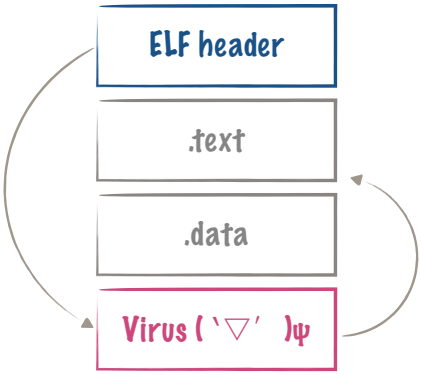

Figure 1: 受感染寄主程序的执行顺序

我们假定病毒工作于以下环境：

1. 指令集架构：x86_64
2. 操作系统：Linux
3. 被感染文件在 root 权限下运行

假定一个可获得的 root 权限，可以让我们专注于 ELF 文件的分析与重构、病毒的攻击行为与连接病毒本身，而不用操心其他问题。另外，我们选择用 C 语言写病毒代码，而不是 C++，因为 C++ 在编译的时候会包含全局的初始化，这会给改写 ELF 的过程增添不少麻烦。