关于Linux操作系统病毒的原型分析 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/145/2021_2022__E5_85_B3_E4_BA_8ELinu_c103_145302.htm 一、 介绍 写这篇文章的目的主要是对最近写的一个Linux病毒原型代码做一个总结，同时向对这方面有兴趣的朋友做一个简单的介绍。阅读这篇文章你需要一些知识，要对ELF有所了解、能够阅读一些嵌入了汇编的C代码、了解病毒的基本工作原理。 二、 ELF Infector (ELF文件感染器) 为了制作病毒文件，我们需要一个ELF文件感染器，用于制造第一个带毒文件。对于ELF文件感染技术，在Silvio Cesare的《UNIX ELF PARASITES AND VIRUS》一文中已经有了一个非常好的分析、描述，在这方面我还没有发现可以对其进行补充的地方，因此在这里我把Silvio Cesare对ELF Infection过程的总结贴出来，以供参考： The final algorithm is using this information is. * Increase p_shoff by PAGE_SIZE in the ELF header * Patch the insertion code (parasite) to jump to the entry point (original) * Locate the text segment program header * Modify the entry point of the ELF header to point to the new code (p_vaddr p_filesz) * Increase p_filesz by account for the new code (parasite) * Increase p_memsz to account for the new code (parasite) * For each phdr whos segment is after the insertion (text segment) * increase p_offset by PAGE_SIZE * For the last shdr in the text segment * increase sh_len by the parasite length * For each shdr whos section resides after the insertion * Increase sh_offset by PAGE_SIZE * Physically insert the new code (parasite) and pad to PAGE_SIZE, into the file - text segment p_offset p_filesz (original)

在Linux病毒原型中所使用的gei - ELF Infector即是根据这个原理写的。在附录中你可以看到这个感染工具的源代码: g-elf-infector.cg-elf-infector与病毒是独立开的，其只在制作第一个病毒文件时被使用。我简单介绍一下它的使用方法，g-elf-infector.c可以被用于任何希望--将二进制代码插入到指定文件的文本段，并在目标文件执行时首先被执行--的用途上。g-elf-infector.c的接口很简单，你只需要提供以下三个定义：* 存放你的二进制代码返回地址的地址，这里需要的是这个地址与代码起始地址的偏移，用于返回到目标程序的正常入口： #define PARACODE_RETADDR_ADDR_OFFSET 1232 * 要插入的二进制代码（由于用C编写，所以这里需要以一个函数的方式提供）： void parasite_code(void). * 二进制代码的结束（为了易用，这里用一个结尾函数来进行代码长度计算）： void parasite_code_end(void). parasite_code_end应该是parasite_code函数后的第一个函数定义，通常应该如下表示： void parasite_code(void) { ... ... } void parasite_code_end(void) {} 在这里存在一个问题，就是编译有可能在编译时将parasite_code_end放在parasite_code地址的前面，这样会导致计算代码长度时失败，为了避免这个问题，你可以这样做： void parasite_code(void) { ... ... } void parasite_code_end(void) {parasite_code().} 有了这三个定义，g-elf-infector就能正确编译，编译后即可用来ELF文件感染： face=Verdana> 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com