多方入手剿杀Linux操作系统病毒[1] 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_A4_9A_E6_96_B9_E5_85_A5_E6_c103_145240.htm 人们对 Windows 中的病毒已经习以为常，杀毒软件也基本针对这一领域，但却不了解 Linux系统是否会染毒，随着 Linux 的用户日益增多，Linux 的防毒问题日益凸显。 当心 Linux病毒 Linux 出现之初，其最初的设计似乎具有先天的病毒免疫能力，所以当时有许多人相信不会有针对 Linux 的病毒出现。但事实证明，Linux 并非乐土，不能例外。1996 年秋，澳大利亚一个叫 VLAD 的组织用汇编语言编写了据称是 Linux 系统下的第一个病毒 Staog，它专门感染二进制文件，并通过三种方式去尝试得到 root 权限。当然，设计 Staog 病毒只是为了演示和证明 Linux 有被病毒感染的潜在危险，它并没有对感染的系统进行任何损坏行动。 2001 年，一个名为 Ramen 的 Linux 蠕虫病毒出现了。Ramen 病毒可以自动传播，无需人工干预，虽然它没有对服务器进行任何破坏，但是它在传播时的扫描行为会消耗大量的网络带宽。Ramen 病毒是利用了 Linux 某些版本(Redhat6.2 和 7.0 )的 rpc.statd 和 wu-ftp 这两个安全漏洞进行传播的。 同年，另一个针对 Linux 的蠕虫病毒 Lion 则造成了实际的危害。当时 Lion 通过互联网迅速蔓延，并给部分用户的电脑系统造成了严重破坏。Lion 病毒能通过电子邮件把一些密码和配置文件发送到互联网上的某个邮箱中，攻击者在收集到这些文件后就可能通过第一次突破时的缺口再次进入整个系统，进行更进一步的破坏活动，比如获取机密信息、安装后门等。当 Linux 系统感染了这个病毒后，很有可能因为

不能判断入侵者如何改动了系统而选择重新格式化硬盘。而且，一台 Linux 主机在感染了 Lion 病毒后就会自动开始在互联网上搜寻别的受害者。事后的反馈表明， Lion 病毒给许多 Linux 用户造成了严重的损失。 其他 Linux 平台下病毒还有 OSF.8759、Slapper、Scalper、Unux.Svat 和 BoxPoison 等，当然，大多数普通的 Linux 用户几乎没有遇到过它们。这是因为直到目前，Linux 上的病毒还非常少，影响的范围也很小。但随着 Linux 用户的增加，越来越多的 Linux 系统连接到局域网和广域网上，自然增加了受攻击的可能。可以预见，未来会有越来越多的 Linux 病毒出现。因此，如何防范 Linux 病毒就成为每个 Linux 用户应该开始注意的事情了。 抓住弱点，个个击破 Linux 的用户也许听说甚至遇到过一些 Linux 病毒，这些 Linux 病毒的原理和发作症状各不相同，所以采取的防范方法也各不相同。为了更好地防范 Linux 病毒，我们先对已知的一些 Linux 病毒进行分类。 从目前出现的 Linux 病毒来看，可以归纳为以下几个类型： 1.感染 ELF 格式文件的病毒 这类病毒以 ELF 格式的文件为主要感染目标，通过汇编或者C语言可以写出能感染 ELF 文件的病毒。Lindose 病毒就是一种能感染 ELF 文件的病毒，当它发现一个 ELF 文件时，将检查被感染的机器类型。如果查找到匹配的类型，则查找该文件中是否有一部分大于 2784 字节(或十六进制 AEO )，如果有，病毒就会用自身代码覆盖它并添加宿主文件的相应部分的代码，同时将宿主文件的入口点指向病毒代码部分。 防范：由于 Linux 下有良好的权限控制机制，所以这类病毒要有足够的权限才能进行传播。在防范此类病毒时，我们要注意管理好自己 Linux 系统中的各种文件的权限，特别要注意的是在

做日常操作时不要使用 root 账号，最好不要以 root 身份运行来历不明的可执行文件，以免无意中触发了含病毒的文件从而传染到整个系统中。 2.脚本病毒 脚本病毒是指使用 shell 等脚本语言编写的病毒。此类病毒编写较为简单，不需要具有很高深的知识，很容易就实现对系统进行破坏，比如删除文件、破坏系统正常运行、甚至下载安装木马等。但它传播性不强，通常是在本机上造成破坏。 防范：防范此类病毒也是要注意不要随便运行来源不明的脚本，同时，要严格控制对 root 权限的使用。 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