

多方入手剿杀Linux操作系统病毒[2] 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_145238.htm

3.蠕虫病毒

Linux 下的蠕虫病毒与 Windows 下的蠕虫病毒类似，可以独立运行，并将自身传播到另外的计算机上去。在 Linux 平台下的蠕虫病毒通常利用一些 Linux 系统和服务的漏洞来进行传播，比如，Ramen 病毒就是利用了 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。

防范：防范此类病毒要堵住蠕虫病毒发作的源头，从已经出现的几个 Linux 病毒爆发事件来看，它们都是利用了 Linux 已经公布的几个安全漏洞，如果用户及时采取了对应的安全措施就不会受到它们的影响。不过遗憾的是，许多 Linux 的管理员并没有紧密跟踪与自己系统和服务相关的最新信息，所以还是给病毒以可乘之机。所以，用户要做好本机的安全工作，特别要关心 Linux 的安全漏洞信息，一旦有新的 Linux 安全漏洞出现，就要及时采取安全措施。此外，还可以配合防火墙规则来限制蠕虫病毒的传播。

4.后门程序

后门程序也可以被看成广义的病毒，在 Linux 平台上也非常活跃。Linux 后门利用系统服务加载、共享库文件注射、rootkit 工具包，甚至可装载内核模块 (LKM) 等技术来实现，许多 Linux 平台下的后门技术与入侵技术相结合，非常隐蔽，难以清除。

防范：防范此类病毒可以借助一些软件来进行，有一些软件可以帮助用户找出系统中的各种后门程序，比如 chkrootkitR、rootkits 等可以发现蠕虫、后门等。

5.其他病毒

在 Linux 平台上除了面对针对 Linux 的病毒之外，还要注意到许多 Windows 病毒会

存在于 Linux 的文件系统中，当然，这类 Windows 病毒不会在 Linux 中发作，但它们可有机会被传递到 Windows 系统中。比如，Linux 的 Samba 服务器可以作为整个网络中的文件服务器，当有用户将含有 Windows 病毒的文件上传到 Samba 服务器后，Samba 服务器就成为一个病毒携带者，虽然它本身不会感染这种 Windows 病毒，但是其他访问过 Samba 服务的 Windows 系统就有可能从中感染病毒。防范：为了整体的安全，在 Linux 系统中也需要能查找和杀除 Windows 病毒。这就需要使用一些专门的反病毒软件。现在，已经有一些开放源码软件和商业软件可供用户选择了，而且其数量正在逐渐增加。多方入手，剿杀 Linux 病毒与 Windows 的病毒相比，从数量上看，Linux 的病毒几乎可以忽略不计，但是 Linux 病毒的制造者们并不会停止，他们多是一些精通编写代码的黑客，Linux 自身不可避免地存在的脆弱点很有可能会被他们利用编写出各式各样的新 Linux 病毒来。虽然，Linux 病毒还没有开始泛滥，但如果毫无防范意识的话，一旦某个 Linux 病毒暴发，就很可能造成严重的后果。所以 Linux 用户应该及早重视 Linux 病毒问题。最后，笔者对 Linux 平台下病毒的防范总结出以下几条建议，仅供参考：

- 做好系统加固工作.
- 留心安全公告，及时修正漏洞.
- 日常操作不要使用 root 权限进行.
- 不要随便安装来历不明的各种设备驱动程序.
- 不要在重要的服务器上运行一些来历不明的可执行程序或脚本.
- 尽量安装防毒软件，并定期升级病毒代码库.
- 对于连接到 Internet 的 Linux 服务器，要定期检测 Linux 病毒，检查蠕虫和木马是否存在.
- 对于提供文件服务的 Linux 服务器，最好部署一款可以同时查杀 Windows 和 Linux 病毒的

软件. ● 对于提供邮件服务的 Linux 服务器，最好配合使用一个 E-mail 病毒扫描器。总之，对于 Linux 平台下病毒的防范要采取多种手段，决不可因为现在 Linux 病毒很少就掉以轻心。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