是谁在挑战Linux的安全性 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/244/2021_2022__E6_98_AF_E8_B0_81_E5_9C_A8_E6_c103_244547.htm 在操作系统中，如果用漏洞百出形容Windows，那么关于Linux我们最常听到的形容词恐怕就是“ 无懈可击 ”了。当人们越来越热衷于寻找微软的操作系统和软件的漏洞，使得Windows成为越来越多号称黑客的人攻击目标的时候，却往往忽略了世界上使用人数第二多的Linux操作系统。 其实1996年就出现了Linux平台下的第一个病毒Staog。据说这个病毒是由澳大利亚一个叫做VLAD的黑客组织用汇编语言写出的（这个组织在病毒光荣簿上留下了相当辉煌的印记，Windows 95下的第一个病毒程序Boza就是该组织的作品）。它只感染二进制文件，试图通过三种途径得到root权限，但是它仍然只能算是一个病毒的演示样本，它存在的意义只是向那些Linux爱好者们证明：Linux并不是无坚不摧的，它同样也存在着被病毒侵袭的危险，只是由于Linux操作系统设计上的完善使得这种危险系数比较低。 第二个出现在Linux操作系统上的病毒是Bliss病毒，它是一个实验品，只是在实验中不小心被释放的病毒，而且其本身就具有免疫能力，并不对系统具有太大的危险。 直到Ramen的出现，人们才对Linux操作系统无懈可击的安全性重新产生了怀疑。Ramen病毒可以自动传播，无需人工干预，和1988年大行其道的Morris蠕虫非常相似。它只感染Red Hat 6.2和7.0版使用匿名FTP服务的服务器，通过两个普通的漏洞RPC.statd和wu-FTP感染系统。和更多流行在Windows上的蠕虫病毒一样，它发作的迹象并不是感染文件，而是在扫

描时消耗网络带宽，让正常的资源请求无法到达服务。 实际上，利用安全漏洞攻击电脑的Ramen病毒也有助于Linux网管及时修复漏洞，因为它在攻击的时候也暴露了漏洞的存在。另外还有一种使用shell脚本语言编写的病毒，我们可以在网络上找到关于这种病毒的过多篇分析文章，不过大部分是在渲染它的严重性。Linux系统文件中有很多以.sh结尾的脚本文件，一个非常简单的shell病毒就可以感染到系统中所有的脚本文件。 最重要的是，它非常容易编写，一个数十行的shell病毒对于那些急于在网络上成名而又学术不精的“ 黑客 ”来说是很简单的事情。也就是说，容易被心存不轨的人利用才是shell病毒最厉害的地方。 很多文章中都提到，除去Linux先天的设计足够强壮，早期使用Linux操作系统的多为专业人士，在安全意识经验的传承上做的也非常出色，这让Linux有了良好的人文条件来保护自己。笔者认为，年轻，也是Linux免遭那些不负责任的黑客攻击的一个重要原因。不过随着Linux使用者开始变得“ 鱼龙混杂 ”以及业界不断给予它过高的评价，新的安全威胁也随之而来。 这个让Linux的安全性开始被更多的人关注的病毒叫做Linux.Lion，也就是我们在国内的Linux论坛上经常见到的“ 狮子 ”蠕虫病毒。如果说Linux下的第一个蠕虫病毒Ramen在还不足以在病毒史上绽放光芒，那么现在Lion病毒替它实现了这个“ 愿望 ”。 Lion病毒Ramen病毒一样不会感染Windows操作系统，但是它有一个特别危险的功能是可以把被感染的计算机的口令和配置文件用EMAIL发送给China.com的一个信箱。而它比Ramen病毒更难对付的地方正在于，黑客有了口令和配置文件，在对系统进行攻击的时候就无须使用安全漏洞，这使攻击更难防范。

跟在Windows平台肆虐的各种病毒相比，上述的几种病毒实在不能算是罪大恶极，它们所做的一切都只是在试图挑战Linux的安全神话，只是在向那些深信Linux绝对安全的用户发出警告：Linux并非安全无虞。 当然，存在于Linux操作系统的病毒远不止这些，Unux.Svat、BoxPoison等病毒同样给Linux用户带来过不同程度的伤害，而且随着Linux用户的大量增加，越来越多的Linux系统连接到了互联网上，这大大增加了该系统被侵害的可能。可以预见，会有更多的病毒出现在Linux上。保护Linux，还请尽早开始。 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