详细剖析Linux和Unix两系统病毒威胁（1） PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/144/2021_2022__E8_AF_A6_E7_BB_86_E5_89_96_E6_c103_144334.htm 不久以前，很多系统管理员还信誓旦旦的表示，Linux和其他基于UNIX的平台对于病毒和蠕虫事实上是无懈可击的。我不知道为什么他们对自己的威胁分析这么自信，特别是从第一个大型蠕虫在1988年被Robert Morris发明，在使用Sendmail程序的UNIX系统中被释放出来以后。我猜测每个人都变得热衷于批评微软的操作系统和软件，这已经成为越来越多病毒制造者的攻击目标，然而他们却遗忘了UNIX上的脆弱点。 Linux/UNIX威胁 随着Klez病毒在Linux平台上传染的通告，防毒软件厂商开始提醒我们微软的操作系统不再是唯一易受病毒攻击的操作系统了。即使Linux和其他一些主流UNIX平台的用户可能不是微软捆绑应用软件的大用户，不可能通过这些软件造成病毒的泛滥，Linux和UNIX仍然有它们自身并不引人注目的脆弱点。 除了Klez以外，其他Linux/UNIX平台的主要威胁有：Lion.worm、OSF.8759病毒、Slapper、Scalper、Linux.Svat和BoxPoison病毒，这些很少被提及。 我记得曾经在两年前参加了一个由欧洲最大的财政机构完成的安全审计项目，当时我听见一个知名的安全专家告诉审计师，UNIX是不易受病毒攻击的。审计师只是简单的说了一句"okay"，然后纪录下"UNIX系统对于病毒是安全的"。那个时代已经过去了，你现在可以预料到，安全审计师和99v安全团队已经开始强烈的需要UNIX平台上的病毒策略了。 一个叫Alexander Bartolich的奥地利学生甚至已经完成了如何一个编写Linux平台上ELF 病

毒的指南。Bartolich 没有要求做一个Linux病毒先锋，他表示，他只是更有效的说明了和反映了病毒、蠕虫和木马威胁Linux 更好的途径，那些很早就已经在别处被说明了。有了这样具启发性的、在网上发布的文档，基于UNIX的病毒数量只会增长的更快，特别是自Linux 在服务器领域的应用越来越广泛之后。系统管理员也许希望，在亲自读过那本指南以后，对Linux 病毒的理解发生飞跃，从而能够更好的掌握Linux 的脆弱点。 病毒的制造者是一些精通编写代码的黑客，他们远比那些胡乱涂改网站却对编写病毒知之甚少的黑客要危险。尽管一个被黑掉的网站可以很快的修好，病毒却加更隐蔽，会带来潜在的安全隐患。你也许不能相信，但是病毒会一直潜伏，直到它给系统带来不可挽回的损害。 