企鹅遭遇蠕虫Lupper变种盯上Linux 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__E4_BC_81_E9_B9_85_E9_81_AD_E9_c103_144414.htm 一个新的蠕虫病毒已经通过利用Web服务器的错误开始瞄准Linux系统。一些反病毒机构已经发布，所谓的Lupper-A病毒会在被感染的机器上留下后门，这样就可以方便入侵和在Web服务器中窃取电子邮件地址。 目前看来Lupper并没有迅速的扩散，但是，因为Linux系统比起Windows来说很少受到病毒的侵袭，所以这一事件引起了网络安全专家的关注。 按照加利福尼亚州Santa Clara的McAfee的说法，Lupper是通过Web 服务器中易受攻击的的PHP/CGI的脚本进行散布。“ 它是从Linux/Slapper 和 BSD/Scalper蠕虫衍生出来的，并继承了前两个特征。
“ McAfee在一次咨询会上提到。“ 蠕虫通过向80端口发送错误的HTTP要求，从而袭击Web服务器，如果服务器中正好有作为攻击对象的脚本，并且能够允许远程文件在PHP/CGI环境下的下载，一个含有蠕虫病毒的复制文件就会被下载下来，并且被执行。 McAfee说，Lupper的袭击会形成一个整个网络范围内的点对点的交流协议，网络就会被用来实施分布式的服务拒绝distributed denial of service (DDoS)攻击，或者是用来达到其他目的。因为现在的网络接受远程指令。同时，新病毒还能够盗取储存在Web服务器中的电子邮件地址。
Computer Associates的Islandia在一次咨询会上指出，Lupper还能够在7111端口出开出UDP的后门backdoor，从而允许远程的非法控制器进入到机器当中。 Symantec的Cupertino把这个蠕虫病毒起名为Linux.Plupii，并总结说，一旦病毒文件被执行

将会进行如下的操作: 通过UDP 端口 7222给远程的袭击者发送确认信息。 在UDP 端口 7222开出后门，允许远程非法袭击者进入计算机。 产生出还有一些列编码的URLs。 向URLs发送HTTP要求，并且试图通过PHP远程密码的弱点来探取XML-RPC或者AWStats以及Darryl Burgdorf Webhints从而进新传播。 试图下在并且实行自身的文件，通过名为[http://]62.101.193.244/[REMOVED]/lupii的网址并且把所下载的文件保存为名为/tmp/lupii的文件。 Symantec还在其病毒公告中进行了其他信息和易受蠕虫攻击弱点的描述。 在反病毒公司开始注意Lupper的行动之时，Danish vulnerability clearinghouse Secunia也宣布了其他基于Linux的错误警告:不安全使用FTP服务器vsprintf()函数用来回答FTP客户要求，产生了Linux-ftpd-ssl错误，按照Secunia的说法，一旦输出量超过2,048字节，这就会导致一个stack-based的缓冲器溢出。这个错误可以通过产生出一系列长文件名的子目录进行袭击，之后产生XPWD命令。而结果就是XPWD造成了超过2,048 的字节溢出。 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