针对Word漏洞 安全警告升级 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/140/2021_2022__E9_92_88_E5_AF_B9Word_c100_140179.htm 来自反病毒研究者的一项警告声称在广泛被使用的微软WORD软件中，一个极其危险的“ 0-day ”漏洞已经被老练的中国和台湾黑客加以利用。 赛门铁克的Threat Analyst Team在确认了这个未打补丁的漏洞 逐步升级了他的安全威胁等级 这个漏洞以一个普通的微软WORD文件形式被加在文件中，然而文档被使用者打开时漏洞触发一个系统后门以rootkit面貌出现蒙骗杀毒软件的扫描。 SANS ISC（Internet Storm Center）在一份日志中声称收到了一个未透露名称组织的报告，该漏洞已经成为目标。邮件被写成国内邮件的样子，甚至还包含了签名。 不会被反病毒软件发现。一位ISC的调查人员Chris Carboni这样说。 当.doc附件被打开的时候，引发一个现在就存在于WORD中的位置漏洞，进而感染整个完全补丁的系统。这个漏洞的功能如同一个将恶意代码安装到系统上的Dropper程序，解压运行后一个木马程序立刻用一个空白副本（未被感染）覆盖原有WORD文档。ISC解释说，接下来WOED崩溃，提示用户出现问题正在尝试重新打开文件，如果用户同意，这个新的空白文件就会不时的打开。如果该特洛伊木马病毒在用户的计算机上“ 安营扎寨 ”，它会让黑客“ 执行任意的外部命令、下载其它特洛伊木马病毒、获得计算机屏幕截图、监视和记录用户的击键或密码。 联系域，IP地址和木马信息，ISC推断攻击邮件是由远东发起的，木马病毒代码会被Microsoft Word 2003执行，但Word 2000只会崩溃，并不会在系统中安装该木马。 安全厂

商McAfee公司也对此病毒提出了警告，并给此木马定名为BackDoor-CKB!cfaae1e6。 据称微软正在研究开发这个漏洞的补丁。 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