网页木马深度剖析以及手工清除3 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/474/2021_2022__E7_BD_91_E9_A1_B5_E6_9C_A8_E9_c67_474159.htm 当申明邮件的类型为audio/x-wav时，IE存在的一个漏洞会将附件认为是音频文件自动尝试打开，，结果导致邮件文件x.eml中的附件run.exe被执行。在win2000上，即使是用鼠标点击下载下来的x.eml，或是拷贝粘贴，都会导致x.eml中的附件被运行。整个程序的运行还是依靠x.eml这个文件来支持
。Content-Transfer-Encoding：base64Content-ID：从这我们可以看出，由于定义后字符格式为base64，那么一下的代码全部为加密过的代码，里面可以是任何执行的命令：
〈scriptlanguage=vbs〉 OnErrorResumeNext. 容错语句，避免程序崩溃 setaa=CreateObject（"Wscript.Shell"）。建立Wscript对象 Setfs=CreateObject（"scripting.FileSystemObject"）。建立文件系统对象 Setdir1=fs.GetSpecialFolder（0）。得到Windows路径 Setdir2=fs.GetSpecialFolder（1）。得到System路径 ……省略…… 下面代码该做什么各位都该清楚吧。这就是为什么很多人中毒后不能准确的清除全部的病毒体的原因，也是很多杀毒软件的一个通病。病毒监控只杀当时查到的，新建的却置之不理。 III。iframe漏洞的利用 ㈠ 多方便的办法，浏览者的COOKIES就这样轻松的被取走。 ㈡
〈iframesrc=run.emlwidth=0height=0〉〈/iframe〉 常见的木马运用格式，高度和宽度为0的一个框架网页，我想你根本看不到它。除非你的浏览器不支持框架！ ㈢ 又是一个框架引用的新方式，对type="text/x-scriptlet"的调整后，就可以实现和eml

格式文件同样的效果，更是防不胜防。 IV
。MicrosoftInternetExplorer浏览器弹出窗口Object类型验证漏洞漏洞的利用 精华代码
：-----codecutstartforrun.asp----------codecutendforrun.asp----- [作者注]我想，这个方法是现行的大部分木马网页中使用的频率最高的一个。效果绝对是最好的。不管是你IE5.0还是IE6.0还是 SP1补丁的。我们都敢大声的说：IE6.0 SP1也不是万能的。呵呵，是不是想改用mozilla了？ 总结： 几乎所有类型的网页病毒都有一个特性，就是再生，如何再生，让我们从注册表中的启动项开始分析：注册表中管理启动的主键键值分别为：
[HKEY_LOCAL_MACHINE/Software/Microsofthttp://windows.chinaitlab.com/CurrentVersion/RunServices]
[HKEY_LOCAL_MACHINE/Software/Microsofthttp://windows.chinaitlab.com/CurrentVersion/RunServicesOnce]
[HKEY_LOCAL_MACHINE/Software/Microsofthttp://windows.chinaitlab.com/CurrentVersion/Run]
[HKEY_LOCAL_MACHINE/Software/Microsofthttp://windows.chinaitlab.com/CurrentVersion/RunOnce]
[HKEY_CURRENT_USER/Software/Microsofthttp://windows.chinaitlab.com/CurrentVersion/Run]
[HKEY_CURRENT_USER/Software/Microsofthttp://windows.chinaitlab.com/CurrentVersion/RunOnce]
[HKEY_CURRENT_USER/Software/Microsofthttp://windows.chinaitlab.com/CurrentVersion/RunServices] 