计算机百科知识

计算机网络病毒

(十二)

本书编写组　编

山东科学技术出版社

图书在版编目(CIP)数据

计算机百科知识/本书编写组编．—济南：山东科学技术出版社，2003

ISBN 7-5331-1651-8
Ⅰ．计… Ⅱ．本… Ⅲ．计算机网络—基本知识—汇编
Ⅳ．TP39
中国版本图书馆 CIP 数据核字(2003)第 004271 号

山东科学技术出版社出版发行
(济南市玉函路 16 号 250001)
全国各地新华书店经销 莒县新华印刷厂印刷
开本：787×1092 1/32 印张：240 字数：4 000 千字
2003 年 7 月第 1 版 2003 年 7 月第 1 次印刷
印数：1～1 000 册
书号：ISBN 7-5331-1651-8/D·112
定价：698.00 元

目 录

NIMDA 蠕虫病毒已经侵入我国

计算机病毒防治产品检验中心暨国家计算机病毒应急处理中心2001年9月19日晨接到用户报告，发现一种新型计算机病毒，经分析确认，该病毒是昨日在美国发现的NImda蠕虫病毒，我们已经接到北京、深圳、厦门、安徽、成都、苏州等地的用户感染报告，该病毒已经侵入我国的计算机网络，并在迅速蔓延。

一、攻击的目标系统：

该病毒可以感染 Windows 95,98,ME,NT,或者2000 ，以及 Windows NT and2000 服务器。

二、传播方式：

1、通过邮件传播出，当用户邮件的正文为空，似乎没有附件，实际上邮件中嵌入了病毒的执行代码，当用户用 OUTLOOK、OUTLOOK EXPRESS（没有安装微软的补丁包的情况下）收邮件，在预览邮件时，病毒就已经执行了。

2、利用了 IIS 的漏洞，采用与“红色代码 II ”和“蓝色代码 ”类似的方式，通过网络传播。

3、通过局域网的共享传播到其他系统。

“尼姆达（NIMDA）”病毒解决方案

18 日又一新病毒“尼姆达（NImda）”在互联网上

通过 EMail 方式以惊人的速度传播，它能感染使用微软软件的服务器与 PC 机。这种新病毒通常采用三种方式，一是通过电子邮件传输，二是自动寻找局域网络内的共享目录进行传染，三是利用微软的 IIs 服务 UnIcode 漏洞和 MS-type spoofIng 漏洞。

(1)邮件方式：一旦用户登陆遭到感染的网站并且其互联网浏览器没有安装修补软件，那么整个计算机系统都有可能遭到病毒感染。到目前为止带有这种病毒的电子邮件大多没有主题，其附件一般都是“Readme.exe”(78k)形式。当用户收到邮件时，其正文为空，似乎没有附件，实际上邮件中嵌入了病毒的执行代码，当用户用 OUTLOOK、OUTLOOK EXPRESS 收邮件，在预览邮件时，病毒就已经不知不觉中执行了。病毒还在 Windows 的临时目录下生成一个 emL 格式的临时文件，大小为 79 字节，该文件已经用 BASE64 编码将病毒包含进去。并且在本机其他文件夹中快速复制，同时读取用户信件，取出 SMTP 地址、邮箱地址，利用这些地址将带有蠕虫病毒的信件对外发送。

(2)局域网内传播：通过局域网的共享，传播到其它 Windows98 系统下，病毒还会在 Windows 的 system 目录中生成 Load.exe 文件，同时修改 system.InI 中的 sheLL 从 sheLL=expLoreR.exe 改为

expLoreR.exe Load.exe -dontRunoLd，使病毒在下次系统启动时仍然被激活。另外，在 system 目录下，病毒还会生成一个副本：RIched20.dLL。而 RIched20.dLL 目录在 Windows 系统中就存在，而它就把它覆盖掉了，并将 C 盘根目录共享出来。还能通过“即时聊天”以及“FTP 程序”传播具有极高的传染性。特别注意此病毒一部分会在 Win2000 系统下传染.EXE 的文件，将病毒后门加在正常文件头部，当文件被执行时，先执行病毒程序，完成后病毒将正常程序吐出并执行此程序，由于被感染病毒文件病毒体在文件头部，容易造成杀毒软件误以为是同一木马程序并将其删除，往往造成严重后果。

(3)病毒采用类似“CodeBlue”蠕虫的攻击方式对外随机网络漏洞进行传染。利用微软的 UnIcode 漏洞和 MS-type spoofIng 漏洞。

此病毒迄今为止好象还没有发现这种新病毒具有删除计算机内文件或数据的能力，只是当这种病毒在进行自我复制时会导致计算机的运行变得缓慢。据称，这种病毒目前已在美国、欧洲以及拉丁美洲出现，而且很可能会以较快的速度向其他地区传播。这种新病毒也是利用运行于视窗 NT 或视窗 2000 上的微软互联网服务器软件存在的安全隐患展开攻击，这一点与

“红色代码”病毒相同。

北京北信源公司提醒广大企业和个人用户尽快到我公司网站下载微软补丁和升级杀毒软件。具体方法如下：

(1)到我公司网站：www.vRv.com.cn 或（www.LInhao.com.cn)下载你使用系统相应的补丁包到本地，然后双击执行即可。

(2)再下载我公司最新升级文件62g版网址同上。在运行北信源杀毒软件全盘杀毒，然后重新启机。

(3)我公司刚刚开发的kILLnImda程序，是NImda病毒的专用查杀程序。操作简单、易用。

具体手工清除方法：

1.结束系统进程列表中名称为“***.tmp.exe”和“Load.exe”的进程（其中***为任意文件名）；

2.进入系统的TEMP目录，寻找文件长度为57344的文件，删掉它们；

3.进入到系统的System目录，寻找名称为RIched20.DLL的文件；

4.删掉长度为57344字节的RIched20.DLL（长度大小在100K以上，为系统正常文件）；

5.再在System目录下寻找名称为Load.exe、长度为57344字节的文件，并删掉；

6.删除 C:\、D:\、E:\三个逻辑盘的根目录下的 AdmIn.DLL 文件；

7.打开 System.InI 文件，在[Load]中把“sheLL=expLoreR.exe Load.exe -dontRunoLd”，改为“sheLL=expLoreR.exe”；

8.系统为“WinNT、Win2000、WinXP”的用户，请打开“控制面板|用户和密码”，将 AdmInIstRator 组中的 guest 帐号删除；

9.将 C 盘完全共享“C$”去除；

10.搜索整个机器，查找文件名为 Readme.emL 的文件；

11.删除内容为“<html><head></head><body bgcoLor=3D$FFFFFF>
<IfRamesRc=3DcId:EA4DMG BP9pheIght=3DwIdth=3DO>
</IfRame></body></html>”或 Content-Type: audIo/x-wav；name=“Readme.exe”Content-Transfer-EncodIng:base64“。

针对 NImda 标本兼治的安全解决方案

一、NImda 黑客蠕虫病毒情况简介

肆虐全球的 CodeRed 红色代码蠕虫病毒的余波尚未平息，各网管还未来得及松一口气，又一种破坏力极强的新病毒已经开始象野火一样开始在互联网

上蔓延开来，这种名为 NImda ”尼姆达“的病毒于 18 日上午 9：08 被发现，半小时之内就传遍了世界，其传播范围和破坏程度将大大超过前一段时间极度肆虐的 ”红色代码“病毒。据冠群金辰反病毒监测网的报告，我国各地均有病毒的感染案例，由于此病毒能通过多种方法攻击 Win32 系统，一种方法不行它会尝试另外一种方法攻击，直至成功，其攻击对网络造成的通信阻塞是空前的。目前已有多家报告因受此病毒攻击，造成网络瘫痪，其危害性不言而喻。

那么，这种病毒是通过何种手段造成如此巨大的破坏呢？ 这个名为 NImda ”尼姆达“的蠕虫病毒与以往的蠕虫病毒有很大不同，它可通过三种方式传播：EMail 附件、HTTP、硬盘共享，并且能感染所有 32 位 Windows 操作系统：Windows 98/Me,NT,2000,XP。

这种新病毒也是利用运行于视窗 NT 或视窗 2000 上的微软互联网服务器软件存在的安全隐患展开攻击，这一点与 ”红色代码“病毒相同,但它同时也可以感染客户端。即用户在浏览染毒的网页时就可能会受到感染。此病毒还通过 OoutLook，OutLook Express 邮件客户端传播，会在用户访问带毒的邮件时在用户毫不知晓的情况下感染用户的系统，这一点又与前一段时间流行的邮件蠕虫病毒 HappytIme 很相似。此外，

它对系统共享也作了手脚，为每个盘符创建网络共享。在 Win9x/ME 系统上，该共享被设置为完全共享，无需密码。在 WinNT/2K 系统上，GUEST 用户被赋予管理员权限，并得到共享权限。在网络共享这一方面，又与 FunLove 病毒相似。

从上面的分析可以看到，此新病毒集各家之所长，从多方面利用了系统的漏洞，所以该种黑客蠕虫病毒的危害性非常大，并且来势汹汹，事实上这种黑客蠕虫病毒已经远远超越了反病毒的范畴，而且从最近病毒爆发的情况来看，这种病毒代表了未来病毒的发展趋势。通过单一的防病毒产品很难解决 NImda 及未来的各种类似病毒，治理 NImda 们需要一个完善的安全解决方案。

二、整体解决方案

当务之急是我们要先解决和防御 NImda 带来的破坏，另外我们需要比以往任何时候都要重视网络安全的问题，通过构建自身有效的安全防御系统来亡羊补牢、防患于未然。解决然眉之急--NImda 的清查方案 可按照如下步骤手动清毒：

1，从微软网站

http://www.Microsoft.com/technet/Security/Bulletin/ms00-078.asp 和

http://www.Microsoft.com/technet/Security/Bulletin/MS01-020.asp

下载相应补丁并执行，然后关闭本机的所有共享。

2，按 ctRL-aLt-deL，结束 ”xxx.tmp.exe“以及 ”Load.exe“的进程。

3，删除 temp 目录中的文件。

4，用干净的 RIched20.DLL（大约 100k）文件替换染毒的同名 RIched20.DLL 文件（57344 字节）。

5，删除系统目录下的 Load.exe 文件（57344 字节），Windows 根目录下的 mmc.exe 文件，在 C:\、D:\、E:\三个逻辑盘的根目录下如果有 AdmIn.DLL 文件，删除这些文件，查找文件名为 Readme.emL 的文件，删除它。

6， System.InI 文件[Load]中如果有一行 ”sheLL=expLoreR.exe Load.exe -dontRunoLd“，改为 ”sheLL=expLoreR.exe“

7 删除 HKLM \SOFTWARE \Microsoft \Windows \Current Version\Network\LanMan\ 和 HKLM\ Software\Microsoft\Windows\Current Version \ExpLoreR \MapMail\ 的键值。

8， 如果是 WinNT 或者 Win2000，打开 ”控制面

板|用户和密码“，将 AdmInIstRator 组中的 guest 帐号删除。KILL 的最新病毒特征码 28.06 已可查杀此病毒。

三、防患于未然--整体安全方案

1、从最近几次病毒的大规模爆发可看到，它们的肆虐主要是利用了系统的漏洞，如这次 NImda 就利用了 Microsoft Web FoLdeR TRansveRsaL 漏洞(W32/CodeBlue 病毒也使用了此漏洞)和 Microsoft IncorRect MIME Header 漏洞。它还利用了 W32/CodeRed.c 蠕虫创建的后门。如果服务器的安全性足够高，不存在可利用的安漏洞和隐患的话，NImda 和未来的 NImda 们则没有发作或传播的可能性。所以我们根治NImda和类似黑客蠕虫病毒的方法是提高服务器系统本身的安全性，我们建议使用冠群金辰公司的 eTRust PoLIcy CompLIance 定期扫描操作系统以及数据库系统的安全漏洞及错误配置，加强系统安全性，以做到事先预防，而不是事后的”亡羊补牢“。

2、在网络的关键网段中部署冠群金辰公司的 eTRust IntRusIon DetectIon（入侵监测），可提供主动的网络保护，自动探测网络流量中可能涉及潜在入侵、攻击和滥用的模式，并且在系统受到影响之前根据预定义策略采用适当的措施，实现对网络的安全

监控和保护。该软件在CodeRed病毒流行时就对发现、定位病毒源及采取相应措施方面立下了汗马功劳。

四、没有安装”天衡安防“防病毒系统的计算机用户：通过手工的方法来清除”NImda“病毒：

1、先断开网络连接；

2、查看 RIched20.DLL 的文件大小，系统的正常文件大小应该在 100K 以上，而 NImda 病毒的副本大小为 57344 字节，如果有长度为 57344 字节的 RIched20.DLL，用一个干净的 RICHED20.DLL 覆盖原来的文件；或是删除它之后，用安装盘中的文件恢复；

2、将系统 System 目录下名 10、为 Load.exe、长度为 57344 字节的文件删除；

3、System.InI 文件中如果有一行”sheLL=expLoreR.exe Load.exe-dontRunoLd“，将其改为”sheLL=expLoreR.exe“；

4、将 C:\、D:\、E:\三个逻辑盘的根目录下的 AdmIn.DLL 文件删除；

5、将下面文件夹 \documents and Settings\useRname\LocaL Settings\temp 和 \Windows\Temp 内的以.tmp 为扩展名 15、的文件全部删除。删除 HKLM \SOFTWARE \Microsoft \Windows\Current Version\Network\LanMan\和

HKLM\Software\Microsoft\Windows\Current Version\ExpLoreR \MapMail\的键值；

6、如果是 WinNT 或者 Win2000，打开 ”控制面板/用户和密码 “，将 AdmInIstRator 组中的 guest 帐号删除；如果是 Win9x 系列，则将硬盘共享改 为你要设置的状态；

7、搜索整个机器，查找文件名 为 Readme.emL 的文件，删除它；查找文件名为*.emL 的文件,长度为 79225 字节，如果文件内容中包含 <HTML><HEAD></HEAD><BODbgCoLor=3D#ffffff>

<IfRame sRc=3DcId:EA4DMGBP9p heIght=3D0 wIdth=3D0>
</IfRame></BODY></HTML> 以及 Content-Type: audIo/x-wavname= ”Readme.exe

Content-Transfer-EncodIng: base64 则删除该文件；

8、搜索整个机器， 查找所有的超文本语言类文件(如 html、htm、asp、shtml、shtm 等)，若发现其中包含以下字符串：

<html><scRIptLanguage=“JavaScRIpt ”>Window.open(“ Readme.emL ” ,nuLL, “ ReslzabLe =no, top=6000,Left=6000 ”)</scRIpt></html>则删除该段字符串；

9、重新启动计算机；

10、安装微软补丁程序：

http://www.Microsoft.com/technet/Security/Bulletin/MS01-020.asp

http://www.Microsoft.com/technet/Security/Bulletin/ms00-078.asp

注意：如果你已安装 ServicePack2 补丁，则不需再安装上述补丁。

11、重新连接网络。

启明星辰针对NImda病毒的解决方案--天衡安防用户　最近一段时期，人们总是被各种各样的计算机病毒所困扰，　“CodeRed ”　红色代码尚未平息，“CodeBlue ”烽烟再起，人们还没有从“代码 ”的困扰中挣脱出来，又一种破坏力极强的新病毒“NImda ”，却已经在网络上疯狂蔓延。

这种被命名为“NImda ”(“尼姆达 ”) 的病毒于 9 月 18 日被发现并迅速传遍了世界，如果得不到及时的控制，其传播范围和破坏程度将大大超过人们谈之色变的“红色代码 ”病毒。目前国内已经有大量用户感染了此种病毒。

启明星辰公司安全专家经过跟踪分析，发现“NImda ”病毒通过三种方式传播：电子邮件方式、

HTTP 方式、文件共享方式。并且能够感染所有 32 位的Windows操作系统。和“CodeRed ”雷同的是,“NImda ”也是利用运行于 WindowsNT/2000 上的微软互联网服务器软件存在的安全隐患展开攻击.并可以在用户浏览染毒的网页时候传播至客户端，或者通过电子邮件、文件共享方式传染给客户端。感染了病毒之后，网络通信受到阻塞，最终将造成网络瘫痪。

从“NImda ”病毒身上，我们可以看到“HappytIme ”、“CodeRed ”、“FunLove ”病毒的影子，可以说，“NImda ”病毒是综合了上述各病毒的技术特点发展而成的一个综合性病毒，并将在某种程度上代表着计算机病毒的一个未来发展方向。这也给我们网络安全厂商提出了一个新的课题。

启明星辰公司针对“NImda ”病毒的传播方式和技术特点，结合启明星辰公司的“天衢安防 ”防病毒系统，提出了一个完整的解决方案：

一、安装了“天衢安防 ”防病毒系统的用户：

1、首先将天衢安防病毒库更新到 9 月 19 号以后；

2、之后断开网络连接；

3、用天衢安防软件扫描整个硬盘；

4、将感染 NImda 的文件（MMC.EXE、LOAD.EXE、ADMIN.DLL、*.EML、*.NWS）删除；

如果在当前操作下，不能直接删除被感染的文件，你需退到 DOS 下或用干净的系统盘重新启动，然后再删除。

注意：SYSTEM 目录下的 RICHED20.DLL 不能直接删除，这个文件是OFFICE套件运行的必备库，WINDOWS的写字板等也要用到这个动态库，最好的办法就是用一个干净的 RICHED20.DLL 覆盖原来的文件。

也可以在用户清除后，可以从安装盘里面找到相应的文件拷贝回来。

Win98：在压缩包 Win98_35.CAB 中，解开找到 RIched20.dLL 拷贝到 system 目录。

Win98se：在压缩包 Win98_41.CAB 中。

Win2000：在 system32\dLLcache 目录有备份，将它拷贝到 system32 目录。

如果 NImda 感染了一些可执行文件，最好也是用干净的文件覆盖的方法来进行清除。

5、重新启动计算机，并用天蓠安防软件再扫描一次硬盘，以确保计算机中不 含有 NImda 病毒；

6 、 将 下 面 文 件 夹 \documents and Settings\useRname\LocaL Settings\temp 和 \Windows\Temp 内的以.tmp 为扩展名的文件全部删除。

7、System.Inl 文件中如果有一行“sheLL=expLoreR.exe Load.exe-dontRunoLd”，将其改为“sheLL=expLoreR.exe”；

8、删除HKLM\SOFTWARE\Microsoft\Windows\Current Version\Network\LanMan\和

HKLM\Software\Microsoft\Windows\Current Version\ExpLoreR\MapMail\的键值；

9、如果是 WinNT 或者 Win2000，打开“控制面板/用户和密码”，将 AdmInIstRator 组中的 guest 帐号删除；如果是 Win9x 系列，则将硬盘共享改为你要设置的状态；

10、安装微软补丁程序：

http://www.Microsoft.com/technet/Security/Bulletin/MS01-020.asp

（防止计算机通过 e-Mail 途径被感染）

http://www.Microsoft.com/technet/Security/Bulletin/ms00-078.asp

（弥补“Web Server FoLdeR TRaveRsaL”漏洞，防止系统感染上红色代码 II 蠕虫病毒，CodeRedII 病毒会在系统中留下“后门”，而 NImda 病毒会利用这个“后门”）

注意：如果你已安装 ServicePack2 补丁，则不需再安装上述补丁。

11、重新连接网络。

由于“NImda”病毒传播途径非常广泛，建议将“天衢安防”防病毒系统的实时防护功能随时开启。这样，用户将随时受到保护，并且能够随时自动得到“天衢安防”管理控制中心的最新升级服务。

关于一种新型病毒--“求职信病毒”的紧急报告

国家计算机病毒应急处理中心在2001年10月26日接到用户报告，通过电子邮件感染了未知病毒。经分析判定，该病毒为一种新型计算机病毒。目前已接到上海、北京、广东、福建等地用户的报告，遭受该病毒感染。经初步分析，由于病毒体代码包含以下内容，该英文信的内容与求职有关，所以我们将其命名为“求职信”病毒。

附件的名称也是随机的，如 NxRj.exe，URuo.exe，Vws.exe。如果用户使用微软的 OutLook 收发电子邮件，那么在预览含有该病毒的邮件时，病毒已经被执行。病毒一旦运行，将在 C:\\Windows\\System 下生成两个隐含文件 KRn132.exe 和 Wqk.exe，修改注册表，添加值：

HKEY_LOCAL_MACHINE\\Software\\Microsoft\\

Windows\\Current Version\\Run\\KRn132=C:\\WINDOWS\\SYSTEM\\KRn132.exe

HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Windows\\Current Version\\Run\\WQK=C:\\WINDOWS\\SYSTEM\\Wqk.exe

同时感染 PE 文件和.scR 文件。

一旦感染此病毒，系统将变得非常缓慢，并且该病毒还可以通过取 OutLook 地址簿中的邮件地址自动传播给其他用户。在系统日期为 13 日时，病毒会破坏文件造成系统瘫痪。

截止到目前，对该病毒尚没有完整的解决方案。建议用户将 Internet ExpLoreR 升级到 IE6.0 版本，即可对该病毒起到防范作用。当收到可疑邮件要求用户下载文件时，选择“取消”和“否”，而不要选择“打开”。

我们已将病毒样本转发给各防病毒软件生产厂商，并协调组织这些防病毒厂商进行对该病毒的分析研究工作。在这里，我们提醒广大计算机用户，在没有解决方案之前，慎重收发电子邮件，以避免该病毒的进一步传播。

同时请关注 CNCERT,国家计算机病毒应急处理中心及各防病毒软件生产厂家的网站，以便及时了解该病毒的发展动态，并及时更新手中的杀毒软件，预防该病毒。

细说 BadtRans.b 的技术特征(一)

BadtRans.b 病毒也是一种通过邮件传播的蠕虫病毒，同时它也是一种特洛伊木马程序，会对您的计算机安全造成威胁。此病毒具有如下特征：

1.伪装成回复的邮件。

2.会生成一个 DLL 文件

3.它会记录 Windows 所有的击键记录。

4.它会将这些记录（包括您键入的密码等信息）通过邮件发送到它自带的地址之一。

5.将受感染者的 IP 通过邮件发送给作者。

6.在特定时间停止运行。

7.使用 keRneL32 作为自己的别名。

8.将自己复制到 Windows 的 system 目录中（Win9x\Me 为 Windows\system，Winnt\2000 中为 Winnt\system32）。

当该病毒第一次执行时，它会将自己复制到 Windows\system 目录下面并改名为 keRneL32.exe，

在 Win9x\me 下还会将自己注册为服务进程。并且创建一个记录密码等信息的 DLL 文件 KdLL.dLL。

细说 BadtRans.b 的技术特征(二)

再经过 20 秒，如果设置了适当的控制位病毒会自动关闭。如果该计算机支持 RAS 加密的话，病毒会等待一个RAS加密的网络连接。当这种连接建立之后，有 33％的几率，该病毒会在个人文件夹和 IE 的缓冲的*.ht* 和 *.asp 文件中搜索 EMail 地址，找到之后它就会向这些地址发送邮件附件的名字为下列之一：

2001 年危害最大的 10 种电脑病毒

新华网蒙得维的亚１2 月 2 日专电（ 记者 胡积康）据此间媒体引用专门生产反病毒软件的 SoｐhoS 公司的材料说，该公司今年共发现１１１６０种电脑新病毒，其中１０种病毒危害性最大。SoｐhoS 公司的材料指出，最近发现的 NImdaYSIRcam 电脑病毒扩散的范围最广，其侵害的电脑数量约占全球受病毒影响的电脑总数的一半左右。但是，令人恐惧的“代码红色（CodIｇoroJo）”病毒没有列入本年度１０大电脑病毒行列。

该公司的管理人员克鲁莱说，NImda 蠕虫病毒是９月份在网上出现的，其炮制者尚未查明。“这种病毒破坏力很强，因为它可以利用许多技术侵入计算

机。今后电脑病毒很可能会模仿这种病毒”。至于SIRcam病毒,它通过邮件经常变换文件名称进入用户电脑，能偷窃计算机里储存的机密文件，然后把它散发给用户地址簿中所有的邮箱，使用户感到十分尴尬。

“将死者”病毒的完全介绍及手工清除方法

病毒类型：蠕虫病毒

病毒大小:39KB

病毒介绍：该病毒本身是一个压缩文件 ，如果打开压缩文件，就会变成136KB的文件。此病毒是用VIsuaL BasIc编写，且经过压缩软件UPX压缩，反解压工具处理，使之用原始的UPX不能解压。由于是VB编写的病毒，它运行时就需要一个 VB 的动态链接库msvbvm60.dLL，若用户的计算机里没这个文件，病毒就无法被激活，这些用户则会幸免于难。

传播方式:

(1).通过OutLook电子邮件地址簿向用户发送带有蠕虫病毒附件文件的邮件

(2).通过 IRC 聊天工具传送病毒文件

(3).通过 ICQ 聊天程序将病毒复制自身给其它ICQ用户

(4).通过 MIRC 方式,在系统中安装后门程序,病

毒制造者可远程控制

若存在上述程序，病毒将会自动关闭它们，同时查找硬盘上对应文件所在目录，并删除该目录下的所有文件。若无法删除，病毒会修改 WinInIt.InI 文件以便在系统重启时删除文件。

手工清除方法：

1、在纯 DOS 模式下,用类似 C:CD \WINNT\SYSTEM 的命令切换到 WINDOWS 的系统目录，键入 DEL GONE.SCR 删除 gone.scR 文件；

2、接着回到 WINDOWS，启动注册表编辑器，HKEY_LOCAL_MACHINE\Software\Microsoft\Windows \Current Version\Run\，删除其中名称中含有“gone.scR”的键值；

3、删除 mIRC 目录中的 REMOTE32.INI 文件；

4、删除 MIRC.INI 文件，用以前的备份文件中恢复该文件；

5、该病毒轻松清除。

笑哈哈（Shoho）病毒的手工清除法

据金山反病毒应急处理中心提供的数据显示：近日出现的笑哈哈病毒（Worm.Shoho.110592）是一种基于 Windows 的常驻内存型病毒，通过 EMail 方式传播,利用 IE 的漏洞自动执行,并向 Microsoft outLook

地址簿中的邮箱反复发送自身，造成邮箱堵塞，还会随机删除当前目录下的文件，造成系统启动困难。

该病毒利用已知的基于 Internet ExpLoreR 的漏洞，自动执行邮件附件，把自身复制到 Windows 目录下，文件名是 WinLOgOn.exe，每次启动 Windows 操作系统时，该病毒都将运行。感染病毒的计算机的 Windows目录下还将增添EMail.txt、EMailInfo.txt、dRwatson、dRwatsonfRame.htm 等文件。

该病毒利用微软 IE MIME 漏洞（Microsoft IE MIME Header Attachment ExecutIon VuLneRabILIty ）进行传播，金山公司提醒广大计算机用户，尽快下载并安装 IE 补丁程序，及时升级病毒码，谨防受到病毒的攻击。IE 用户请从微软网站下载补丁程序。

Update to IE5.01 SP2

Update to IE5.5 SP2

Update to IE6.0

以下是笑哈哈病毒的手动清除方法：

1。点击开始->运行，输入 RegedIt 命令，修改注册表文件。

2。双击如下条目：

HKEY_LOCAL_MACHINE>Software>Microsoft

>Windows>Current Version>Run

3。在右边的面板中寻找并删除如下项：WINLOGON.EXE = “%Windows%\WINLOGON.EXE”。

4。双击如下条目:

HKEY_CURRENT_USER>Software>Microsoft >Windows>Current Version>Run

5。在右边的面板中寻找并删除如下项：WINLOGON.EXE = “%Windows%\WINLOGON.EXE”。

6。双击如下条目:

HKEY_USER>.DefauLt>Software>Microsoft >Windows>Current Version>Run

7。在右边的面板中寻找并删除如下项：WINLOGON.EXE = “%Windows%\WINLOGON.EXE”。

每逢奇数月 13 日发作 “求职信”变种欲兴风作浪

1 月 22 日晚,“求职信”病毒的多个变种(KLez.e、KLez.f、KLez.g)正通过电子邮件大规模扩散。

“求职信”病毒于 2001 年的 11 月首次在国内出现，每逢奇数月 13 日发作。由于此病毒多以求职为邮件内容，所以很容易迷惑用户。本次截获的求职信变种，在原病毒的基础上增加了更多的工作线程，当病毒驻留系统后可能会强迫关闭用户正在进行的其

它正常操作，严重情况病毒会删除一些有用文件，从以上情况可以看出，此次出现的求职信变种病毒具有较大的破坏力。

求职信变种病毒主要以电子邮件的形式传播，其信件主题多为“HI,HeLLo，Re:，how are you”的英文短句，而病毒邮件附件的扩展名则以：txt、htm、html、wab、doc、xLs、jpg、cpp、cpas、mpg、mpeg、bak、mp3 为主，因此，当用户收到具有以上特征的英文信件时，需谨慎处理!

KLez.E 病毒每个月的第六天发威

美国当地时间 3 月 5 日，几家计算机安全公司发布警报称，一种危险的新互联网蠕虫病毒正在快速传播，而且会在本周三删除和覆盖被感染的计算机上的文件。F-SecuRe 公司反病毒研究经理 MIkko Hypponen 称，这种名字为 KLez.E 的病毒能够在每个月的第六天删除和覆盖 Word、ExceL、图像、视频、互联网以及其他文件。KLez 病毒是目前最常见的 10 种病毒之一，携带此病毒的电子邮件会显示不同的主题，它还能够删除反病毒软件。

Hypponen 表示，尽管能够感染运行任何电子邮件系统的计算机，但只能向微软的 OutLook 地址簿中的地址发送携带病毒的电子邮件。只要收件人阅读电子

邮件，即使不打开附件，附件就能够自动地执行。

这种病毒最早是在去年 11 月份被发现的，但早期的版本危害性较低，而且传播速度也不如 KLez.E。据 F-SecuRe 公司表示，这种变种病毒可能是东南亚人编写的，因为其中包含“我是亚洲人”、“我要养活我的父母”、“我需要一份月薪 5500 美元的工作”等语句。病毒的作者也许希望借病毒表明，他有极高的编程能力。

目前，大多数反病毒公司的产品都能查杀 KLez 及其变种病毒。

发现于日本的中度危险病毒 Fbound 新鲜出炉

病毒名称：W32/Fbound.c@MM

发现日期：2002-03-13

最早出现地区：日本

长度：12288 字节

病毒类型：邮件病毒

危害级别：中

别名：WORM_JAPANIZE.A (趋势命名)

病毒特征：

该病毒以邮件的形式进行传播，其附件名为 patch.exe。主题有可能是“Important”或用日语写成的。运行后，它会向 Windows 地址簿中的所有联

系人发送带毒邮件。此病毒不会以任何方式将自身安装在受染机器上。病毒体内含有文本“I-Worm.Japanlze”

中毒迹象：

染上该病毒后，它会立即将自身向外发送，没有任何明显的中毒迹象。

感染方式：

手动运行附件 EXE 文件后，病毒会向外发送带毒邮件。

新病毒 MyLIfe 冒充屏保 专毁硬盘数据

美国网络联盟(Network Associates)旗下反病毒紧急响应组 McAfee AVERT3 月 22 日发现了一种大规模邮件蠕虫病毒——“MyLIfe.b”(我的生活)。当天，有 2000 多台电脑被侦测出感染了这种病毒。

“MyLIfe.b”(我的生活)是一种采用 VIsuaL BasIc6 编写的大规模邮件蠕虫病毒，以主题为“bILL caRIcatuRe”的电子邮件形式进行传播，病毒就藏在名为“caRI.scR”的附件里，冒充屏保程序，以吸引用户点击。

一旦用户接收到主题为“bILL caRIcatuRe”的电子邮件并打开“caRI.scR”附件，病毒便自动复制到电脑的系统目录中。如果这部电脑在早上八点至九

点这段时间内重新开机的话，病毒将全部删除存储在C、D、E、F等硬盘上的所有文件，以及WindowsSystem目录下以SYS、VXD、OCX和NLS为扩展名的文件。

据了解，该病毒还会降低用户发送电子邮件和上网的速度，而且能自动把自身发送给Microsoft OutLook地址簿中的所有联系人，以此扩大传播范围。

对于这种最新型病毒，McAfee AVERT专家指出，MyLIfe.b源自何方目前还不得而知，但澳大利亚是目前受感染最为严重的地区。然而在病毒发作的第一天(即3月22日)中午之后，该蠕虫扩散的速度似乎开始减缓。

据受该病毒侵害的用户可登录McAfee AVERT相关网站vIL.nal.com/vIL/content/v_99414.htm，查找这种病毒的最新信息与对策。McAfee用户也可在AVERT网站上更新扫描引擎与DAT文件清除病毒，防止潜在的危害。

MyLIfe四变种惊现 尤以F传播速度快

反病毒公司近日宣称，具有破坏性的恶意蠕虫病毒MyLIfe上周末连续出现四个新变种，变种衍生速度之快实为罕见。不过，在四个新出现的变种当中，只有一个传播速度较快，目前正在互联网上广泛传播。

英国电子邮件服务提供商 MessageLabs 称，他们在周二上午已拦截了 140 封含有 MyLIfe.f 变种病毒的邮件，近一半是来自澳大利亚，其余大部分是出自英国，也有一小部分来自香港。

MyLIfe.f 是 MyLIfe.b（w32.myLIfe.b@mm,也叫 CaRIc.a）的一个变种。MyLIfe.b 是较早前出现的一个病毒，它以一幅克林顿挂着奶罩吹萨克斯管的讽刺动画而“闻名遐迩”。该病毒修补了前辈 MyLIfe.a (w32.myLIfe.a@mm)的一些 bug，并且除了向 Windows 地址簿中的所有收件人发送带毒邮件外，它还会在每逢 8：00 或 16：00 等 8 的倍数时刻受感染机器重启时执行一段可损坏文件的恶意程序。

MessageLabs 公司的高级反病毒技术专家亚历克斯.序普称，在复活节期间，他们发现 MyLIfe 的病毒作者共发布了 C、D、E 及 F 四个变种。今天上午，他们注意到 MyLIfe.f 是从澳大利亚开始往外传播的，不久到达英美等国。此变种从上周末就开始迅速传播，不过像变种 D 及 E 一样很容易防范。

然而，反病毒公司赛门铁克表示，MyLIfe.c 具有非常危险的有效载荷，能够根据系统时间来格式化硬盘并删除文件。而 MessageLabs 公司的序普则称，到周二上午他们已拦截到含有 MyLIfe.f 病毒的邮件，

目前仍在分析当中。

MyLife 的四个新变种共享最初的邮件发送引擎，能将自身发给 OutLook 地址簿中的所有收件人以及 MSNMessenger 联系人列表中的地址。

赛门铁克公司称， MyLife.c 的附件为 LIst.TXT.scR，当系统时间的分钟变化大于或等于 50 以及该蠕虫至少在系统上运行过一次时就会激活。若激活的话，它会试图格式化 D、E、F、G、H 及 I 盘，并删除 C 盘上的所有文件。

KLEZ 病毒变体来势汹汹 通过 EMAIL 传播害人不浅

据报道，星期二(4 月 16 日)在亚洲部分地区爆发的一种电脑病毒已经传播到了美国，扩散势头十分凶猛。这种病毒是臭名昭著的 KLez 蠕虫病毒的最新变体，据电脑安全专家指出，新发现的 KLez 蠕虫病毒变体“学名”有三种之多，即 KLez.g，KLez.h 和 KLez.k，其主要特点是通过电子邮件系统进行传播，感染电脑之后能主动关闭许多杀毒软件的运行，正是这一个特点使得它的传播速度明显快于其他病毒，其次它还能感染通过在局域网与电脑相连接的共享驱动器。

反病毒专家目前多数倾向于认为新发现的这种

变体危害不大，但是同时他们也表示正在密切关注疫情的发展，并将随时根据实际情况调整对它的评级。不过值得注意的是今年 1 月首次被发现的 KLez 蠕虫病毒一直高居最危险病毒排行榜前三名，2 月底出现的 KLez.e 变体不仅“毒性强”，而且是有史以来互联网上传播速度最快的病毒之一。

反病毒公司赛门铁克已经将最新发现的 KLez 变体(标识为 W32.KLez.H)从危害二级提升到了三级。赛门铁克的评级体系共分为五级，其中一级病毒的危害程度最轻。

据专家介绍，KLez 病毒借以传播的电子邮件主题有 120 种变化，如“Let\`s be friends(让我们交个朋友吧)”、“meetIng notIce(会议通知)”、“some questIons(几个问题)”、“honey(亲爱的)”等等。在许多情况下，它并不需要电脑用户的点击就能自动运行，这主要是利用了微软 OutLook 电子邮件程序所存在的一个缺陷。用户如果及时为 OutLook 软件打上了补丁，则可以防止发生这种情况。

反病毒专家建议电脑用户及时到有关网站上更新自己电脑中安装的杀毒软件以及电子邮件程序，加强自我保护。

求职信变种(wantjob.e/h)手工清除办法

一、在 WINDOWS 95/98/ME 系统下清除该病毒的方法：

1、立即断绝一切网络连接；

2、重新启动计算机并进入 WINDOWS 95/98/ME 系统下的安全模式下，使用注册表编辑工具 RegedIt 将蠕虫病毒增加的键值删除：HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CuRRent Version\Run 和 HKEY_LOCAL_MACHINE\System\CuRRentContRoLSet\Services 要删除的注册表项目是 Wink???.exe 的键值。

3、必须相应的将 WINDOWS 的 SYSTEM 目录下的该随机文件 Wink???.exe 删除,注意还必须将回收站清空。

4、删除了相应的病毒文件后，重新启动计算机。

5、连上网络。没安装 IE 补丁的用户，到 http://www.Microsoft.com/Windows/Ie/downLoad/cRItIcaL/Q290108/defauLt.asp 下载安装 IE 的补丁。

二、在 Windows2000/XP 系统下清除该病毒的方法:

清除方法基本和 Windows 95/98/ME 系统下的清除方法相同。

1、先以安全模式启动计算机，运行注册表编辑工具，同样删除该网络蠕虫增加的键值：HKEY_LOCAL_MACHINE\System\CuRRentContRoLSet\Services,要删除病毒增加的表项是:Wink 开头的随机的表项。当然你必须记住该项目的具体名称(虽然是随机的)。

2、然后在系统目录下将该文件删除。注意该文件是隐含的，您必须打开显示所有文件的选择项目才能查看该病毒文件。同样的注册表项还有 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\Run；

3、重新启动计算机。

4、连上网络。没安装 IE 补丁的用户，到 http://www.Microsoft.com/Windows/Ie/downLoad/cRItIcaL/Q290108/defauLt.asp 下载安装 IE 的补丁。

在我国已经发现国外流行的新蠕虫病毒 Win32/BugbeaR

国家计算机病毒应急处理中心通过对互联网的监测，于 2002 年 10 月 1 日发现一种新型的蠕虫病毒，

经分析证实该蠕虫病毒是国外正在流行的Win32/BugbeaR(妖怪)病毒。

该病毒是通过感染电子邮件传播的蠕虫病毒。用VC++写成，长度为50688字节（以UPX方式压缩），它的基本特征如下：

(1)复制自己到Windows系统目录并生成随机的文件名（如jmvy.exe），然后在注册表

HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Windows\\Current Version\\Run Once里添加键值，使自己可以在下次开机后自动运行。

(2)释放一个DLL文件到Windows系统目录并生成随机的文件名（如zqpgppu.dLL），用以监测键盘和鼠标输入。

(3)开启一个后门程序，打开36794端口监听被感染机器，可远程执行诸如发送接收文件，发送用户信息，执行指定文件，关闭程序等操作。

(4)该蠕虫会遍历局域网并搜索其中是否包含可写的系统启动目录，如果有就复制自己到该目录。

(5)在没有打补丁的机器上，该蠕虫会利用IFRame漏洞感染传播。

(6)搜索后缀名为*.ODS，*.MMF，*.NCH,*.MBX,*.EML,*.TBB,*.DBX的文件中的EMail地址，通

过系统默认的 SMTP 服务器发送带有该蠕虫的邮件，并随机选择用户机器中的文件做为邮件内容，随机生成附件名。

目前，该病毒在我国发现数量较少，国家计算机病毒应急处理中心提醒广大计算机用户，在十一长假后，要首先升级杀毒软件和操作系统，然后再处理电子邮件，防止该病毒发作、破坏。应急中心已经通知国内、外病毒防治产品生产厂家，截止到 10 月 2 日，熊猫软件公司和金山软件公司已经回复，并升级了各自的杀病毒软件。计算机用户发现该病毒后请向国家计算机病毒应急处理中心报告，以便做好各项病毒防治工作。

通过 MSN 传播的新病毒“GFLemIng”

病毒名称：Worm.GFLemIng.53248

病毒类型：蠕虫

感染长度：53248 字节

危害级别：低

传播速度：高

病毒特征：

1、该蠕虫通过现在较为流行的微软即时通讯工具 MSN MessageR 传播。

2、该病毒用 VB6.0 编写，大小约 53K。

3、一旦被运行，该蠕虫会首先查看用户是否安装了 MSN MessageR 并且已经登录。

链接执行了这个蠕虫的话，蠕虫就会继续通过 MSN MessageR 向其他联系人发送同样的信息，引起连锁反应，造成病毒的快速传播。

该病毒传播速度极快，建议您立刻升级金山毒霸进行查杀。

新时代下的网络病毒

传统的网络病毒定义是指利用网络进行传播的一类病毒的总称。而现在网络时代的网络病毒，已经不是如此单纯的一个概念了，它被溶进了更多的东西。可以这样说，如今的网络病毒是指以网络为平台，对计算机产生安全威胁的所有程序的总和。

由“骗子”升级为“间谍”——木马病毒（Trojan）

传统的木马病毒是指一些有正常程序外表的病毒程序，例如一些密码窃取病毒，它会伪装成系统登录框的模样，当用户在登录框中输入用户名与密码时，这个假的登录框木马便会将用户口令通过网络泄漏出去。

现在的木马病毒与传统的木马病毒相比已经有了很大的区别。如果说传统的木马病毒是个骗子的话，那么现在的木马病毒则更象一个间谍。现在的木

马病毒一般是指，利用系统漏洞进入用户的计算机系统，通过修改注册表自启动，运行时有意不让用户察觉，将用户计算机中的所有信息都暴露在网络中的病毒程序。如今木马病毒更多地是扮演“里通外国”的角色。大多数黑客程序的服务器端都是木马病毒。

不断自我完善——蠕虫病毒（Worm）

蠕虫病毒是指利用网络缺陷进行繁殖的病毒程序，象当年的“莫里斯”病毒就是典型的蠕虫病毒。它利用网络的缺陷在网络中大量繁殖，导致几千台服务器无法正常提供服务。

如今的蠕虫病毒除了利用网络缺陷外，更多地利用了一些新的技术，比如说：“求职信”病毒，是利用邮件系统这一大众化的平台，将自己传遍千家万户；“密码”病毒，是利用人们的好奇心理，诱使用户来主动运行病毒；“尼姆达”病毒，则是综合了系统病毒的方法，利用感染文件来加速自己的传播。

一枝“新秀”—黑客程序（Hack）

黑客程序产生的年代由来以久，但在过去，从没有人将它看做是病毒，理由是，黑客程序只是一个工具，它有界面又不会传染，不能算做病毒。

而随着网络的发展与人们日益增长的安全需求，我们必须重新来看待黑客程序。黑客程序一般都有攻

击性，它会利用漏洞在远程控制计算机，甚至直接破坏计算机；黑客程序通常会在用户的计算机中植入一个木马病毒，与木马病毒内外勾结，对计算机安全构成威胁。所以黑客程序也是一种网络病毒。象“冰河”病毒，“BO”病毒，它们功能强大到可以远端控制计算机做任何事情。

新型病毒——捆绑器病毒（Binder）

捆绑器病毒是一个很新的概念，人们编写这些程序的最初目的是希望通过一次点击可以同时运行多个程序，然而这一工具却成了病毒的新帮凶。比如说，用户可以将一个小游戏与病毒通过捆绑器程序捆绑，当用户运行游戏时，病毒也会同时悄悄地运行，给用户计算机造成危害。

由于捆绑器会将两个程序重新组合，产生一个自己的特殊格式，所以捆绑器程序的出现，使新变种病毒产生的速度大大增加了。为了对付新情况，各大杀毒厂商都将此类型程序定义成一种新病毒——捆绑器病毒，象瑞星 2003 版杀毒软件还针对此种病毒推出了新的杀毒引擎，可见此病毒已经得到了人们更多的观注。

新帮凶——网页病毒

网页病毒是利用网页来进行破坏的病毒，它存在

于网页之中，其实是利用一些 SCRIPT 语言编写的一些恶意代码。当用户登录某些含有网页病毒的网站时，网页病毒便被悄悄激活，这些病毒一旦激活，可以利用系统的一些资源进行破坏。轻则修改用户的注册表，使用户的首页、浏览器标题改变，重则可以关闭系统的很多功能，使用户无法正常使用计算机系统，严重者则可以将用户的系统进行格式化。而这种网页病毒容易编写和修改，使用户防不胜防，最好的方法是选用有网页监控功能的杀毒软件以防万一。

在新型网络环境下，滋生了许多新概念病毒，针对这种状况，反病毒厂商在研制其产品中也作了很大了改进，如瑞星公司在近期推出的“瑞星杀毒软件 2003 版”中的“文件级、邮件级、内存级、网页级一体化实时监控系统”，可以全面、有效地监控各种类型的电脑病毒。

新时代下的电脑病毒越来越“智能”，此时除了需要反病毒技术不断提高外，还需广大计算机用户提高防范病毒意识。只有厂商和用户的共同努力，才可以有效地遏制病毒的破坏。

金山公司截获最新病毒--蠕虫新娘 Worm.BRIde

病毒名称：Worm.BRIde.114688

病毒类型：蠕虫

感染长度：114688 字节

危害级别：中

传播速度：中

技术特征：

这是一个通过邮件传播的蠕虫，病毒本身是一个约 150K 的 PE 程序，用 VIsuaL BasIc 编写。病毒具有如下特征：

(1) 复制自身到系统目录下，命名为 REGEDIT.EXE；复制自身到 Windows 的桌面目录下，命名为 EXPLORER.EXE。

(2) 在注册表项 HKCUSoftwareMicrosoft WindowsCurrent VersionRun 下添加键值 RegedIt = %WinSystem%RegedIt.exe，使蠕虫随系统启动自动运行。

(3)该蠕虫会尝试关闭进程中的一些反病毒软件。

(4)该蠕虫会搜索所有 HTM 和 DBX 文件中的 EMAIL 地址，并将自己发送给搜索到的信箱地址。

(5)该蠕虫在传播过程中会创建一些临时文件，包括：Windows 桌面目录下，文件名为 HeLp.emL；Windows 临时目录下，文件名为 BRadeO.tmp，BRade1.tmp。

(6)该蠕虫会释放一个 FUNLOVE 病毒的变种到系统目录下，命名为 MSCONFIG.EXE 。

(7)当蠕虫内部的计数为特定值时，它会尝试打开以下网站：

http://www.HotMail.com

http://www.sex.com

(8)该蠕虫邮件具有以下特征：

.邮件主题为空。

.邮件的附件名为 README.EXE

.邮件内容会含有如下信息：

HeLLo,

PRoduct Name: < ..。 >

PRoduct Id: < ..。 >

PRoduct Key: < ..。 >

Process LIst: < ..。 >

Thank you。

其中括号中的内容为被感染机器上对应的系统信息。

(9)该蠕虫利用 IFRAME 漏洞传播，这样在没有打补丁的用户机器上，预览即会激活该蠕虫

“妖怪”病毒肆虐日本 恶名直逼“求职信”

日本信息处理振兴事业协会安全中心(IPA/ISEC)

于 11 月 7 日公布了日本 10 月份病毒发现情况。

发现病毒的报告数为 1510 件，其中实际受到损失的为 95 件。

求职信(KLez)病毒居第一位，为 702 件，排在第二位的是 10 月首次报告的“妖怪”(BugbeaR)病毒，为 323 件。为了防备可以通过 LAN 进行传播感染的“妖怪”病毒，该中心呼吁用户重新进行 Windows 的共享设置。

10 月份首次发现的“妖怪”和 OpaseRv 病毒利用 Windows 网络共享机制进行传播感染。具体来说就是，由已经感染病毒的设备向它能够访问的共享文件夹中复制病毒，实施感染。

为了防止这种病毒的进一步漫延，需要在每个客户端和文件服务器中安装防病毒软件的同时，还需将“解除不必要的共享设置”和“设置密码”这两种功能设置为有效。IPA/ISEC 使用窗口照片对设置方法进行了说明。

同一天，IPA/ISEC 还公布了计算机非法访问的情况。10 月份的总报告数为 49 件，其中遭受非法侵入的数量为 19 件，为 2002 年中最多的一个月份。

另外，关于 10 月份的病毒报告数，各防病毒软件开发商也公布了相关信息。与 IPA/ISEC 的信息相

同，报告数量最多的为求职信，其次是“妖怪”。

Roron(Worm.Roron)病毒分析报告

病毒类型：蠕虫病毒

发作时间：随机

传播方式：网络

感染对象：网络

病毒大小：118,784 字节

警惕程度：★★★★

一款恶意报复型蠕虫病毒 Roron（Worm.Roron），样本已于 11 月 7 日上午被瑞星公司全球病毒监测网率先拦截，并于当日进行紧急升级，用户只要升级瑞星便可完全清除此病毒。

据计，此病毒已在国外初露端倪，国内目前还未有被病毒攻击的迹象,此病毒目前已经发现有 6 个变种，并且已经全部被瑞星公司截获，瑞星公司正在紧张处理中，随后会在第一时间升级，使用户不再遭受病毒袭击。

此病毒由高级语言编写，本身没有加密、压缩。

此病毒有以下特性：

一、拷贝自身，完成感染

病毒运行后会首先将自身复制到多份到操作系统的目录和操作系统下的 SYSTEM 目录，名字一般是

随机的，但有两个病毒主程序的名字是固定的：一个是病毒的主程序体：RUNDLL16.EXE，存在于系统目录下，它主要用于病毒的正常运行；一个是病毒的配置文件：WINFILE.DLL，存在于系统的 SYSTEM 目录下，它主要用于病毒保存一些病毒生成的文件信息。

二、修改注册表，进行自启动

病毒会将病毒主程序体的路径加入注册表的自启动项，每次开机都引导病毒。病毒会在 HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Windows\\Current Version\\Run 项中添加键值 :LoadCuRRentPRofile，内容为：RundLL16.exe,powpRof.dLL,LoadCuRRentUseRPRofile。

三、首次运行，欺骗用户

如果病毒是被用户双击而且是首次运行，病毒会弹出一个 WINZIP 的错误框，告诉用户：“你的 WINZIP 自解压版本未被许可，或者许可信息丢失或不正确，请联系程序作者或登陆 www.WinZip.com 网站获得更多信息”,用户一般的反映是此文件已经损坏而将之删除，其实病毒已经运行。

四、修改 EXE 文件关联，运行任何程序等于运行病毒

病毒会将注册表中的与.EXE 文件类型的关联指向病毒体，这样，用户运行任何程序都等于运行了病毒，而且为了不引起用户的怀疑，病毒在运行后会将用户要执行的程序继续运行。

五、启动多线程，监控注册表与自身

病毒运行时会启动多个线程。其中一个线程负责监视注册表的操作，另一个线程负责监控自身的文件。如果病毒发现注册表中被病毒写入的两个键值被修改，或者病毒文件被用户尝试删除，病毒则会将自己休眠 5 秒，然后进行报复，将用户硬盘中的所有文件都进行删除，使用户资料丢失。

六、删除所病毒软件

病毒会对十几家知名杀毒软件进行攻击，如果病毒运行时发现有它认识的杀毒软件的主程序，则将之杀掉。

七、局域网与邮件传播

病毒在有网络连接的前提下，会在局域网中快速传播自身，并通过邮件系统，建立主题与内容随机的病毒邮件，在互联网中大量传播自身。

八、修改多处系统配置文件

病毒还会修改多处系统文件如：MSDOS.SYS,WIN.INI 等，而且在病毒体发现病毒有生

成脚本文件的代码，但在动态分析过程中未能再现此动作。

分析最近需要特别防护的三种病毒

1，Win32.OpaseRv.A

别 名 ： W32. OpaseRv. Worm,W32/ScRup. Worm,Worm.Win32.Opasoft.a

疯狂度：低

种类：Win32

破坏性：中

类型：蠕虫

普及度：高

特性

Win32.OpaseRv 是一种通过共享 Windows 驱动器传播的蠕虫，并且在 2002 年 10 月初开始大范围传播。

当运行的时候蠕虫会拷贝自己到 Windows 目录下。随后添加下面的值到注册表中以便每次 Windows 启动时这份拷贝都可以被运行：

HKLM\\Software\\Microsoft\\Windows\\Current Version\\Run\

ScrSvr=\“%Windows%\\ScrSvr.exe\”

蠕虫也创建下面的这个注册表健值：

HKLM\\Software\\Microsoft\\Windows\\Curre

nt Version\\Run\

ScrSvrOLd=\“ScrSvr.exe\”

这个值会设置文件使之达到蠕虫最初的运行状态。此注册表健值随后将被删除。

文件 ScRSIn.dat 和 ScRSout.dat 也将被创建在%Windows%目录下。

蠕虫通过 Windows NetworkIng(SMB)网络来拷贝自己，利用一个非常老的漏洞来阻止使用 Windows 95,98,98SE and ME machInes 的机器检验网络共享密码。简而言之，上述没有打补丁 的操作系统将会很愚蠢的接受一个单字符密码，而不管原来的共享密码实际上的长度。微软在 2002 年 10 月为这个漏斗出了一个补丁。问题的主要描述和补丁下载的地址以及安装说明可以访问下面的这个微软安全报告：

www.Microsoft.com>www.Microsoft.com

/technet/Security/Bulletin/ms00-072.asp

所有 Windows 95,98,98SE and ME 的使用者，当有文件或打印共享时，都应该安装这个补丁。可以不理会这个安全报告给出的安装建议，但你真的应该考虑这个重要的升级。利用代码，允许远程的密码发现相对应的共享级别的密码。OpaseRv 是第一个懂得利用这个弱点的蠕虫。

这个关于共享级别密码的漏洞只影响到 Windows non-NT 版本。

早期关于 OpaseRv 的报告指出，OpaseRv 通过不设密码的共享和只有简单密码的共享服务传 播。但这是错误的。OpaseRv 随机选择 IP 利用上面所提及的共享级别的密码漏洞特别是 C:盘的共 享密码来进行传播。如果蠕虫搜索到共享资源，它会尝试复制自己到共享资源的 \\WINDOWS\\ScrSvr.exe 下。

蠕虫会尝试访问 Web 站点下载 scRupd.exe 文件来升级自己。但是这个服务器已经被关闭了， 所以它不会给大家带来更多的恐惧了。病毒的检测/清除

KILL 安全胄甲 InocuLanIT v23.57.52 vet10.5/4136 版及 kILL 98/2000 v39.52 可检测/清除此病毒。(病毒生成的 ScrSvr.exe 文件由于系统正在使用中可能无法直接清除，此时需要推出系统进行清除工作)

2，Win32.FLemIng.A

别 名 : Backdoor /BRat, Win32/FLemIng.A.Worm,W32/FLemIng.Worm,W32.HLLW.Henpeck,W32/Rodok.A,WORM_RODOK.A

类别：Win32 类型：蠕虫最近修改：10/10/2002

疯狂度：低破坏性：中等普及度：高

特征：Win32.FLemIng 是一个利用 MSN(微软的 message 功能)信使，通过发送文字信息传播的 蠕虫。这个蠕虫本身需要从一个已经被封闭的网站下载，因此 Win32.FLemIng 已不再会有潜在的 危险。

蠕虫向 MSN 联系人发送以下的信息：Hey!! CouLd you

pLease check out This program for me? :) I made It myself

and want people to test It。Its a Readme With the program

that expLaIns what It does! home.no.net/

downLOad/BR2002.exe>home.no.net/downLOad/BR2002.exe <--

There you can downLoad It! gIve me advices on what to

upgRade pLease!!

其 URL 实际指向蠕虫代码。代码一旦运行，蠕虫就会显示下列信息框：

如果点击“GeneRate”,就会产生一个随机数。如果点击“QuIt”,窗口会关闭但蠕虫仍继续 运行。同时它会寻找下列注册 值：HKEY_CURRENT_USER\\Software\\VaLve\\CounteRSt

RIke\\SettingsKeyHKEY_CURRENT_USER\\Software\\VaLve\\HaLf-LIfe\\Settings\\Key 如果找到，它会把这些 内容通过 MSN 信使送到蠕虫内部一个固定的地址储存起来。

它还会从相同网址下载另外两个程序。同样，这些文件可能已经不存在了，它们可作为 Win32.BRat.02.A IRC 后门程序的备份。home.no.net/downLOad/CSKeygen.exehttp://home.no.net/downLOad/Update.exe 这些文件会被蠕虫改存为下面的名 称：

C:\\hehe2397824.exeC:\\update35784.exe

Win32.BRat.02.A 是一个 IRC“bot”，它会连接到 IRC 的服务器上，并接受/执行一些能够威 胁系统安全的指令。它的主要作用是用来执行拒绝服务(DoS)袭击。

Win32.BRat 是可配置的，所以它的行为是多变的。被 Win32.FLemIng.A 下载的文件会有以下行为：* 自我复制到 %Windows% \\WINUPDAT.EXEUPDATE.UR.ADDRESS,(意味着产生对于缓冲 区文件名过长的错误)。*添加以下注册 值：HKLM\\SOFTWARE\\Microsoft\\Windows\\Current Version\\RunWinUpdat=\“%Windows% \\WinUpdat.

exeupdate.uR.addRess \"*连接到 IRC 服务器 IceBLaze.seRveIRc.com,6669 端口。

能够使系统变慢并阻塞网络的 bRIde 病毒

BRIde(Worm.bRIde)已于前几天由国外登陆我国，此病毒大有盖过“求职信”病毒的趋势，希望用户提高警惕。

病毒类型：黑客程序

发作时间：随机

传播方式：网络

感染对象：网络

警惕程度：★★★★

病毒介绍：

此病毒可以在 Windows2000、Windows XP 等操作系统环境下正常运行。运行时会自动连接 www.HotMail.com 网站，如果无法连接到此网站，则病毒会休眠几分钟，然后修改注册表将自己加入注册表自启动项，病毒会释放出四个病毒体和一个有漏洞的病毒邮件并通过邮件系统向外乱发邮件，病毒还会释放出 FUNLOVE 病毒感染局域网计算机，最后病毒还会杀掉已知的几十家反病毒软件，使这些反病毒软件失效。

病毒发现与清除：

此病毒会有如下特征，如果用户发现计算机中有这些特征，则很有可能中了此病毒。

一、病毒运行后会自动连接 www.HotMail.com 网站。

二、病毒会释放出 BRIde.exe，Msconflg.exe，RegedIt.exe 三个文件到系统目录；释放出：HeLp.emL,ExpLoreR.exe 文件到桌面。

三、病毒会在注册表的 HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\Current Version\\Run 项中加入病毒 RegedIt.exe 的路径。

四、病毒运行时会释放出一个 FUNLOVE 病毒并将之执行，而 FUNLOVE 病毒会在计算机中大量繁殖，造成系统变慢，网络阻塞。

五、病毒会寻找计算机中的邮件地址，然后按照地址向外大量发送标题为：<被感染的计算机机名>（例：如果用户的计算机名为：张冬， 则病毒邮件的标题为：张冬）的病毒邮件。

六、病毒还会杀掉几十家国外著名的反病毒软件。

用户如果在自己的计算机中发现以上全部或部

分现象，则很有可能中了 BRIde(Worm.bRIde)病毒，请用户立刻用手中的杀毒软件进行清除。

新木马病毒“TRojan.KILLonce”的技术特征

病毒名称：TRojan.KILLonce

病毒类型：Win32 木马

危害级别：高

传播速度：低

技术特征：

这是一个用 DeLphI 写的木马，并加 UPX 进行了加壳处理。木马运行后，会：

（1）将自己复制到系统目录下，并命名为 KILLOnce.exe。

（2）在注册表自启动项中添加键值，使得每次开机时都可自动运行。

（3）修改注册中的中的相关键值，关联 exe 文件及 txt 文件，这样当用户打开这两种类型的文件时都会使木马获得运行机会。

（4）锁定注册表的编功能，使得用户无法运行注册表编辑器对注册表进行恢复。

（5）遍历进程，并尝试关掉一些正在运行的反病毒软件。

(6)搜索 DOC 文件，并在搜到的目录下生成 RICHED20.DLL 文件；搜索 HTM 文件，在搜到的目录下生成 SHDOCVW.DLL 文件。使得病毒生成的文件可被 WORD 或 IE 等外部程序加载。

（7）木马还会删除 EML 文件。

（8）感染文件，方法是在被感染文件名后添加.sys,然后将自己命名为源文件的名字。

（9）该木马还会遍历局域网并进行传播。如果木马发现有完全共享的系统目录，它会将 Windows 目录下的 RunDLL32.exe 文件改名为 RunDLL.exe 文件，并用木马程序取代原文件。

请升级金山毒霸进行查杀。

病毒警报：威胁局域网用户的“kILLonce”

9 月 3 日，金山全球反病毒监测网曾截获了一个危害极高的恶意蠕虫“kILLonce”,此蠕虫会在 12 月 13 日这天删除 C 盘根目录下的所有文件。近日，金山公司截获了此病毒家族的另一成员 TRojan.KILLonce。

根据金山反病毒应急中心的技术人员分析，此新成员是一个特洛伊木马，运行后会将自己复制到系统目录下，并命名为 KILLOnce.exe。它会在被感染机器上含有.doc 及.htm 文件的目录下分别生成

RICHED20.DLL 及 SHDOCVW.DLL 文件。这样在用户打开 Word 文档或网页文件时,它所生成的 DLL 文件能够被 Word 或 IE 等外部程序加载，达到自动运行的目的。同时任何扩展名为“.EML”的文件会被删除。而且还会遍历内存中的进程，以关掉一些正在运行的反病毒软件。

另外，该木马还会遍历局域网，通过局域网中的共享目录进行广泛传播。如果发现局域网中有完全共享的系统目录，它会将 Windows 目录下的 RunDLL32.exe 文件改名为 RunDLL.exe 文件，并用木马程序取代原文件。

鉴于此木马高危害性，金山反病毒应急中心已紧急开发新的升级包，最新的升级包将可查杀“kILLonce”木马，敬请广大用户注意及时升级金山毒霸。金山反病毒应急中心将会继续关注此木马的发展趋势，根据用户反馈情况及时跟进，提供最快的解决方案。

警惕－爱吃掉硬盘资料 四角兽病毒来势汹汹

趋势科技昨天发布“WORM_WINEVAR.A”病毒中度警讯。这只名为四角兽的新病毒，利用电子邮件方式，迅速在全球各地扩散，尤以欧洲地区最为严重。

目前已有数千台电脑受感染，在韩国、美国也有

零星灾情传出。台湾地区因为发现得早，目前并无重大灾情传出。

趋势科技将此病毒列为中度风险病毒警讯，由于这个病毒感染行径类似日前掀起轩然大波的求职信系列病毒。趋势科技已对所有用户发布病毒警讯，并呼吁使用者即刻更新扫瞄引擎至 5.2 版以上，以侦测及清除此病毒。

趋势科技表示，此病毒攻击手法和先前 WORM_KLEZ 求职信系列病毒类似，不需执行邮件附加档案，只要预览此病毒邮件，就会受感染，而且一旦不小心中毒，病毒便会大量寄发邮件给通讯录中的邮址，造成伺服器的负荷。

此外，WORM_WINEVAR.A 病毒行为诡谲，专找浏览器的漏洞，并冒名大量发送电子邮件，还会卸载防毒软件以及监控程式。

电脑一旦中毒後，下次再开机时，硬盘中所有资料瞬间消失，桌面还会出现一个 expLoreR.pIf 的图示，更狡猾的是，病毒以电脑注册人的名义发放毒邮，电邮以一个叫 N`4xxxx 的组织为题，让收件人误以为是某组织来邮，一开电邮马上中镖。

电邮题的 xxxx 部分字眼会随机应变，成其他字母，以避开抗毒软件的拦截，因为太多相同题目的邮

件会引发抗毒软件的侦查。

专家提醒－“切尔诺贝利”病毒再次复活

西班牙杀毒软件公司熊猫软件发现了一种新的W95/CIH10XX系列病毒。这种病毒一般称作“CheRnobyL”(切尔诺贝利)，破坏力极大，可使计算机的输出输入系统甚至整个主板报废。熊猫公司截获了一份这种新的病毒，尽管这种病毒才刚刚开始传播。

这种病毒的变体每个月的第二天发作。原始的病毒是在1998年首次发现的，这种病毒在4月26日发作。4月26日是切尔诺贝利核电站灾难爆发的周年纪念日。

另一家杀毒软件公司在承认这种病毒的破坏性的同时敦促人们不要惊慌。网络联盟负责亚太地区的营销经理ALLan BeLL说，除非看到这种病毒的传播，才能说狼来了。

BeLL表示，这种新病毒虽然非常危险，但是这种病毒的危险因素必须考虑到它的传播情况。“CheRnobyL”病毒的这个新的变种并没有在没有控制的状态下出现，因此普通用户是不可能遇到的。

遇到“Chernobyl”病毒可不是一件愉快的事情。网络联盟介绍说，“Chernobyl”病毒包含非常危险的

病毒代码，其引发的日期根据变量而定。在发作那天，这种病毒将重写闪存输出输入系统。如果闪存输出输入系统是可重写的，计算机便再也不能启动，无法使用了。同时，这种病毒还将用垃圾数据覆盖硬盘。

这种病毒可影响运行微软 Windows 95、98 和 ME 操作系统。

改变用户桌面背景的W32.HLLW.DatRIx网络蠕虫病毒

病毒名称：W32.HLLW.DatRIx

发现日期：2002-12-02

病毒类型：蠕虫病毒

传播范围：低

危害级别：低

传播速度：低

病毒介绍：

W32.HLLW.DatRIx 病毒是又一个通过 KaZaA 文件共享进行传播的网络蠕虫病毒。此病毒是通过 Microsoft VIsuaL BasIc 语言编写的，感染长度为 20480 字节。此病毒感染安装有 Windows 95,Windows 98,Windows NT,Windows2000,Windows XP,Windows Me 操作系统的计算机，而不会感染安装有 Windows3.x,MacIntosh,OS/2,UnIx,Linux 操作系统

的计算机。

1.此病毒一旦被激活并开始运行，它将添加键值：

SharedDIR

到注册表编辑器：

HKEY_LOCAL_MACHINE\\SOFTWARE\\Kazaa\\CLoudLoad 中，并将本身复制到 Windows \\Kazaa\\CLoudLoad 文件夹中。

2.同时此病毒也添加键值：

DarkMatrix

到注册表编辑器：

HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Windows\\Current Version\\Run 中,使得机器启动时病毒就会自动运行。

3.此病毒还能够改变桌面背景为下面的图：

解决方案：

1.及时升级杀毒软件，之后认真在整个硬盘上查杀此病毒，彻底清除掉查到的 W32.HLLW.DatRIx 蠕虫病毒。

释放照片并删反病毒软件的新新娘病毒

前一段时间在网上疯狂传播的新娘（Worm.BRIde）病毒，如今又出新变种，于 12 月 6

日被瑞星公司率先截获！目前已造成小面积扩散，请网民关注此病毒的进一步动态。

病毒类型：蠕虫病毒

发作时间：随机

传播方式：网络/邮件

感染对象：网络

警惕程度：★★★★

病毒介绍：

此病毒可以在 Windows2000、Windows XP 等操作系统环境下正常运行。它伪装成一个虚假的发信人向外界网络发送大量的病毒邮件，并通过 htm 及 dbx 文件搜索用户所有的邮件地址，并向这些地址发送大量的病毒邮件，从而进行大面积传播。病毒运行时，会在桌面上生成一个Madam.exe文件及一个可以自动执行的病毒邮件 madam.emL。病毒运行还会弹出一幅照片，在用户欣赏这张照片时，病毒实际上已经将一些反病毒软件干掉。

病毒的发现与清除：

此病毒会有如下特征，如果用户发现计算机中有这些特征，则很有可能中了此病毒：

1、病毒会在桌面上生成一个 Madam.exe 文件及一个可以自动执行的病毒邮件 madam.emL

2、病毒运行时会弹出一幅照片

3、病毒会干掉几十家反病毒毒软件

用户如果在自己的计算机中发现以上全部或部分现象，则很有可能中了“新新娘（Worm.BRIde.b）”病毒，用户可以将病毒文件直接删除来消除病毒的影响，但如果想彻底地清除此病毒，最好还是用《瑞星杀毒软件 2003 版》的最新版本进行彻底清除。

为避免用户遭受损失，瑞星公司已于截获该病毒当天就进行了紧急升级，瑞星杀毒软件 15.12.01 及以上的版本可以自动截获并清除此病毒，望广大用户及时升级。目前瑞星用户只需及时升级手中的软件即可彻底拦截“新新娘（Worm.Bride.b）”病毒。

“杀手 13”如约而至 病毒昨日开始爆发

根据瑞星全球反病毒监测网和技术支持中心的最新报告，“杀手 13”病毒已于 12 月 12 日晚开始发威。

12 月 12 日晚上，瑞星技术支持中心接到了数百个咨询电话，其中部分求救用户已经遭受病毒侵害。此次“杀手 13”开始发作，江浙一带的病毒发作情况比较严重，仅南京一个地区就有十余起病毒发作案例，其中大部分是局域网用户。

瑞星工程师认为，导致“杀手 13”提前爆发的原

因是，上述用户的系统时间提前了一天，因此病毒在12号发作。经过了解，“中招”的个人用户是因为没有做好预防工作，而某些局域网单位则因为没有安装网络版杀毒软件，造成部分机器在升级时被遗漏，因此这些机器C盘下的文件被全部删除。

据了解，某些机关单位为了防止“杀手13”造成破坏，因此向员工宣布：除非有重要事务，否则禁止在13日开机。

今日是“杀手13”的发作日，瑞星提醒广大电脑用户提高防范意识，及时做好防毒准备。

以下是预防“杀手13”病毒的措施（针对个人用户）：

1、及时将杀毒软件升级到最新版本，然后进行全盘查杀。

2、没有使用瑞星杀毒软件的用户，请修改计算机的系统时间，最好将系统时间改为14号以后，而不是13号以前。

针对局域网用户，操作稍微复杂一些：

1、瑞星网络版杀毒软件的用户，请及时进行全网升级，并进行全网查杀。

2、没有使用网络版杀毒软件的用户，必须将所有机器断开，用最新升级的瑞星单机版杀毒软件逐一

查杀。

3、局域网用户也可以修改系统时间，操作同个人用户。

特别提示：

1、查看 C 盘根目录，如果发现有 AUTO EXEC.BAT 文件，请用户用文本编辑工具查看此文件内容，如果发现其中有“deLtRee /y c:*.*”的指令，请用户将该语句删除。如果用户对计算机不太了解，则可以直接将 AUTO EXEC.BAT 文件删除。

2、用户在查看 AUTO EXEC.BAT 文件内容的时候，请千万不要双击此文件（因为一些用户总是喜欢双击文件来查看文件内容），以免造成不必要的损失。另外，Windows 9X 系列系统的用户及 WINDOWS XP 的用户要特别注意。

3、请已经遭受病毒攻击的用户和瑞星公司联系，瑞星数据拯救工程师随时为您服务。

瑞星公司会密切关注该病毒的最新发作情况，并及时向媒体和公众发布最新病毒发作情况的报告。

新的“伊拉克石油”蠕虫病毒网上现身

计算机世界网消息 12 月 17 日，几家反病毒公司发布病毒警报信息指出，一种新的网络蠕虫病毒最近开始传播，可以感染运行微软 Windows NT/200/XP 操

作系统机器中的共享文件夹。据芬兰赫尔辛基的安全公司 F-SecuRe 介绍，这种病毒的名称为“W32/LIoten”，也称为“伊拉克石油”（IRaq_oIL）、“DatRIx”、“W32.LIoten”或“I-Worm.LIoten”。

与其他蠕虫通过大量电子邮件传播不同的是，这种 LIoten 蠕虫病毒扫描因特网上具有共享文件夹的易攻击的 Windows 机器。LIoten 病毒通过随机产生或试图连接因特网上的某一 IP 地址，寻找新的宿主机器，并监听使用 Windows 服务器信息块（SMB，Windows 环境下用于资源共享的协议文件）的机器中 445 端口上的响应。一旦这种病毒接到某一服务器的响应，就会通过一种所谓的“强力攻击”破坏所感染的机器。LIoten 病毒首先获得所感染机器的一个用户帐号列表，然后通过输入其本身列表中可能的密码（如“admIn”、“Root”、“1234”、“asdf”等）来试图登录每一个帐号。如果使用其中任意一个用户帐号登录成功，这种病毒就会在所感染机器中的 System32 目录下复制自己，即生成文件“IRaq_oIL.exe”，并在该机器上创建一个进程来运行这一可执行文件。

F-Secure 公司表示，除了复制其自身之外，目前还不清楚这种病毒会有其他什么影响，而且病毒名称与“伊拉克石油”有什么关系也尚不清楚。不过，如

果机器中安装了防火墙，则可能不会受这种病毒感染，而且即使是最基本的防火墙配置也可以阻止对445端口的访问。

包括赛门铁克、NAI、McAfee、F-SecuRe 以及Sophos等在内的大型反病毒软件制造商，都把LIoten病毒定为“低危险”级别，这表明该病毒还没有广泛传播，而且也很少有报道表明感染了有关 LIoten 病毒。

从预定网站下载文件的 TRojan. DownLoadeR. CILe 病毒

病毒名称：Trojan.DownLoader.CILe

发现日期：2002-12-12

病毒类型：木马病毒

传播范围：低

危害级别：低

传播速度：低

病毒介绍：

TRojan.DownLoadeR.CILe 木马病毒能够从预定的网站下载文件，并在下载成功后执行这些文件。此病毒的感染长度为 33280 字节。此病毒感染安装有Windows 95,Windows 98,Windows NT,Windows2000,Windows XP,Windows Me 操作系统的计算机，而不会

感染安装有 Windows3.x,Microsoft IIS,MacIntosh, OS/2,UNIX,Linux 操作系统的计算机。

1.如果此木马病毒被激活并开始运行，它将下列文件复制到%WindIR%文件夹中：

RegIstry.dLL

RegIstry.exe

Rt.dLL

其中：%WindIR%是变化的，此木马病毒会自动寻找的系统目录，并将自身复制到系统目录下，默认的是：C:\Windows 或 C:\Winnt。

2.此病毒添加键值：

RegIstry Services %WindIR%\RegIstry.exe

到注册表编辑器:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Run 中,使得机器启动时病毒就会自动运行。

3.如果用户使用的操作系统是 Windows NT3.51、Windows2000、Windows XP 或 Windows .NET Server，那么此病毒将会添加键值：

0 %WindIR%\RegIstry.exe

到注册表编辑器：

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Wind

ows\Current Version\PoLIcIes\ExpLoreR\Run 中。

4.最后，此木马病毒会从预定的网站上下载文件，如果下载成功，那么此病毒将执行它们。

解决方案：

1.及时升级杀毒软件，之后认真在整个硬盘上查杀此病毒，彻底清除掉查到的 TRojan.DownLoadeR.CILe 木马病毒。

2.到注册表编辑器：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Run 中将键值：

RegIstry Services %WindIR%\\RegIstry.exe 清除。

3.如果用户使用的是 Windows NT3.51、Windows2000、Windows XP 或 Windows .NET Server 操作系统，那么请到注册表编辑器：

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current Version\PoLIcIes\ExpLoreR\Run 中将键值：

0 %WindIR%\RegIstry.exe 清除。

2002 年十大热门病毒纵览

计算机世界网消息 2002 年十大病毒排行榜

1 求职信病毒（Worm.KLez）

2 新娘（Worm.bRIde）

3 怪物（Worm.BugbeaR-A）

4 汉城（Worm.WinevaR）

5 中国黑客（Worm.Runouce）

6 杀手 13（Worm.KILLOnce）

7 爱情森林（TRojan.sckIss）

8 IRC 克隆人（Backdoor.IRC.CLoneR.k）

9 百变金刚（Win32.Etap2）

10 新爱虫(MacRo.Word.MakeLove)

随着 2002 年即将结束，曾经在这一年中兴风作浪的各种病毒，也纷纷粉墨登场，开始为这一年中各自的表现作出一番总结。无疑，电脑和网络的普及让电脑病毒的发作市场日益增长。因此，要想在有限的篇幅中，对一年中产生重大影响的各种病毒进行全面的回顾，已经是一件越来越困难的事情。因此，在这里我们不妨依然按照病毒危害的程度和所采用的技术先进性，作为一个衡量标准，来为这些“毒宝宝”按以下类别、排个座次，也来一个“十大上榜评选”。

TOP.10

病毒名称：新爱虫(MacRo.Word.MakeLove)

危险指数：★★★★

发作时间：3，6，9，12 月 5 日

病毒类型：宏病毒

传播方式：文件

感染对象：Office 文件

病毒介绍：

该病毒的传播主要以 Word 文档为主，当用户打开被病毒感染的病毒文档时，病毒便躲入 NORMAL.DOT 模板文件中，当用户存新文档时，病毒便会悄悄将自己加入新建的文档中保存，当用户将染毒文档发给别人时，病毒就会继续进行传播。该病毒为周期性爆发，当计算机日期为“3、6、9、12”月份，并且日期为 5 号时，病毒从被感染的文件中激活，之后此病毒即开始对用户的系统进行“野蛮”的破坏：通过改写 C 盘下的重要系统文件 Auto Exec.bat（系统自启动文件），把一条恶性的删除 C 盘数据的命令写进去，当用户重新启动计算机时，就会发觉 C 盘下的所有文件已被删除，由此给用户造成的损失自然无法估量。同时，病毒发作后将试图删除 Windows 系统 system 目录中的文件，造成电脑启动障碍。

TOP.9

病毒名称：百变金刚（Win32.MetaPHOR.v1B）

发作日期：3、6、9、12 月的 17 号

危险指数：★★★★

病毒类型：系统病毒

感染对象：网络/文件

病毒介绍：

此病毒为 29A 病毒小组所作，感染文件时病毒会对自己先压缩，再放大，使它的长度与代码的变化毫无规律可言，使一般的反病毒软件失效。病毒发作后，系统会弹出对话框，其内容将由以下文字组成：\“MetaPHOR v1 by The MentaL DRILLeR/29A\”，别外，病毒在将代码覆盖到被感染文件上时，会造成大量被感染的.EXE 文件无法正常运行，使系统崩溃。

TOP.8

病毒名称：IRC 克隆人（Backdoor.IRC.CLoneR.k）

危险指数：★★★★

病毒类型：后门病毒

感染对象：网络/文件

病毒介绍：

IRC 克隆人（Backdoor.IRC.CLoneR.k）病毒运行时会放出 5 个核心病毒程序来感染系统，然后查找系统中的网络即时聊天工具 mIRC,然后病毒利用这个软件的强大功能，将这个软件改造成一个功能强大的网络病毒服务器，可以实现端口扫描、邮件炸弹、FLood 攻击、UDP 攻击、ICQ 页面炸弹、局域网文件传染、

局域网消息炸弹等多种攻击，给网络上其它的计算机造成损失。

TOP.7

病毒名称：爱情森林（TRojan.sckIss）

危险指数：★★★★

病毒类型：木马病毒

感染对象：网络/邮件

病毒介绍：

此病毒是已知的第一个利用 QQ 进行传播并破坏的恶性木马病毒。它利用本机 QQ，在用户不知道的情况下向用户的好友发送一句消息："http://sckIss.yeah.net 这个你去看看!很好看的"一旦登陆此网站，便会中毒。因为此网站的主页是一个恶意网页，它会自动下载"爱情森林"病毒并执行，从而对用户计算机造成破坏。

TOP.6

病毒名称：杀手 13（Worm.KILLOnce）

警惕程度：★★★★

病毒类型：蠕虫病毒

感染对象：网络/邮件

病毒介绍：

2002 年 11 月 14 日被瑞星公司率先截获的一智能

型新病毒：杀手 13（Worm.KILLOnce），日前在网络上疯狂传播，它具有极强的攻击局域网的能力，并且极难清除，需要计算机用户格外小心。此病毒可以在 Windows2000、Windows XP 等操作系统环境下正常运行。它运行时会将自身写入系统目录及回收站，并通过修改注册表进行自启动，同时在局域网进行疯狂传播，建立多个线程，干掉已知的反病毒软件，并用 NET 命令打开局域网上计算机的后门。12 月 13 日，病毒爆发时，还会给被感染的计算机带来毁灭性的攻击：删除 C 盘全部目录和所有文件！

TOP.5

病毒名称：中国黑客（Worm.Runouce）

危险指数：★★★★

病毒类型：蠕虫病毒

感染对象：网络/邮件

病毒介绍：

从这个病毒的命名上，就可看出这个病毒是一个充满“中国特色”的新型病毒。首先，这个病毒采用了时下最时髦的邮件病毒传播方式。其次，它更可以通过国内大量用户使用的实时聊天工具 QQ 来进行攻击和传播。最后，它更俱备两套不同的感染机制来适应 9X 与 NT 系列操作系统平台，这样它的感染力就会

比一般病毒大得多，而且它首次采用多线程互相守护的技术，使得多数杀毒软件无法彻底将它从内存中清除。至于利用局域网和 OutLook，更是不在话下。可以说，这个病毒在技术特性方面，几乎就是目前最新网络病毒的一个典型样板。

TOP.4

病毒名称：汉城（Worm.WinevaR）

危险指数：★★★★

病毒类型：蠕虫病毒

感染对象：网络/邮件

病毒介绍：

汉城（Worm.WinevaR）是一种智能型病毒，具有智能反跟踪技术，并携带 FUNLOVE 病毒。

此病毒可以在 Windows2000、Windows XP 等操作系统环境下正常运行。病毒除了会删除 NT 系统的服务（如：NTICE、tcpIp）外，更是会删除一些反病毒软件！病毒将自己复制到 system32 目录下，并改名为前三字母为 Win，扩展名为.pIf 的随机文件名。由于病毒本身做了反跟踪设计，当发现自己被跟踪时会弹出对话框：\“what a fooLIsh thIng you have done!\”，随即删除 system32 目录下的所有文件。病毒还会尝试从 http://www.symantec.com/上下载文

件，如果失败，病毒将放出 funLove 病毒并退出。病毒还利用邮件传播，并把自己复到到系统桌面上文件名为 expLoreR.pIf，同时删除各硬盘分区里的所有文件！

TOP.3

病毒名称：怪物（Worm.BugbeaR-A）

危险指数：★★★★

病毒类型：蠕虫病毒

感染对象：网络/邮件

病毒介绍：

杀掉反病毒软件、偷取用户机密信息并向外界发送、利用局域网和邮件传播、攻击打印机……一种恶性蠕虫病毒??“怪物”于 10 月 2 日在中国首次登陆时便被瑞星公司率先截获并查杀，在还没有造成大面积破坏时便已悄然落网。

此病毒可以在 Windows 9X、Windows NT、Windows2000、Windows XP 等操作系统环境下正常运行。运行时会释放出子病毒体监控电脑用户的键盘动作，并截获用户的登录名和密码，并修改注册表与启动目录来达到自动运行的目的。病毒会向外界病毒客户端发送被感染用户的机密信息，如用户名和密码等，并通过局域网与邮件系统向外传播。同时攻击打

印机，随机打印病毒二进制代码，浪费大量墨水，另外，病毒发作时还会自动搜索并杀掉它知道的反病毒软件！

TOP.2

病毒：新娘 BRIde(Worm.bRIde)

警惕程度：★★★★

病毒类型：蠕虫病毒

感染对象：网络/邮件

病毒特性：BRIde(Worm.bRIde)已于前几天由国外登陆我国，此病毒大有盖过“求职信”病毒的趋势，希望用户提高警惕。

此病毒可以在 Windows2000、Windows XP 等操作系统环境下正常运行。运行时会自动连接 www.HotMail.com 网站，如果无法连接到此网站，则病毒会休眠几分钟，然后修改注册表将自己加入注册表自启动项，病毒会释放出四个病毒体和一个有漏洞的病毒邮并通过邮件系统向外乱发邮件，病毒还会释放出 FUNLOVE 病毒感染局域网计算机，最后病毒还会杀掉已知的几十家反病毒软件，使这些反病毒软件失效。

TOP.1

病毒名称：求职信及其变种（Worm.KLez.）

危险指数：★★★★★

病毒类型：蠕虫病毒

感染对象：网络/邮件

病毒介绍：求职信及其变种病毒可谓是今年真正的“明星”病毒，病毒运行后，首先提升自身的运行级别，然后将自己复制到 Windows 系统目录下，同时会放出一个小的系统病毒体(Win32.Foroux.exe)，感染计算机中的所有可执行文件，另外病毒有很强的局域网传播特性，而且还会模拟用户来向外界发送大量可变标题的病毒邮件，病毒发作时会杀掉威胁它的程序和删除一些著名杀毒软件的数据文件，使反病毒程序失效。

求职信变种病毒主要以电子邮件的形式传播，其信件主题多为“HI,HeLLo，Re:，how are you”的英文短句，而病毒邮件附件的扩展名则以：txt、htm、html、wab、doc、xLs、jpg、cpp、mpg、mpeg、bak、mp3 为主。

结束语

可以说，这十大病毒的列出，并不能完全代表本年度所有新老病毒的“最佳”表现。之所以会选中这些病毒，只是因为它们在某些方面具有非常鲜明的代表性。而在此之外，例如垃圾桶 II(Worm.LentIn.e)、

密码（Worm.fRethem）、中国黑客Ⅱ（Worm.ChIneseHackeR-2）、QQ伪装专家（TRojan.QQcamoufLour）、Roron（Worm.Roron）等病毒也都在本年度的某一时段内，成为各大反病毒企业以及用户关注的焦点。因此，我们完全可以认同2002年度是病毒“繁荣发展之年”的说法。只不过，很明显的是，我们以及我们的电脑并不喜欢这一说法，以及其所代表的事实。事实其实很简单，那就是我们再也离不开杀毒软件，而我们真的非常希望能够有足够好用、管用的杀毒软件来保护我们的电脑和网络。但是，无论杀毒软件再怎么好用，我们总还是抱着一线期望--希望能有那么一天，病毒再也不“繁荣”。

病毒警告：垃圾桶III病毒出现

病毒名称：W32.HLLW.ZuLe

发现日期：2002-12-26

病毒类型：蠕虫病毒

传播范围：低

危害级别：低

传播速度：低

病毒介绍：

W32.HLLW.ZuLe蠕虫病毒是通过KaZaA共享文件夹进行传播感染的，并且也通过KaZaA共享文件来使

用户来下载和执行文件。同时此病毒也通过 IRC 通讯工具来进行传播。其也企图删除反病毒软件的文件。此病毒感染安装有 Windows 95,Windows 98,Windows NT,Windows2000,Windows XP,Windows Me 操作系统的计算机，而不会感染安装有 Windows3.x,MacIntosh,OS/2,UNIX,Linux 操作系统的计算机。

1.此病毒将企图删除反病毒软件的文件。

2.此病毒复制本身到 KaZaA 文件夹中。

3.此蠕虫病毒一旦被激活并开始运行，那么它将本身复制成如下的一个或多个文件中：

4.此病毒将创造子文件夹\CeRtIfIed，同时此病毒也将其本身复制到该子文件夹中。

清除“求职信”病毒

一、病毒简介

这是一个高危险性的恶性邮件病毒，因为病毒中带有特征字句“I want a good job,I must support my parents.（我必须找到一分工作来供养我的父母）”，因此被称之为“求职信”病毒。它与 NImda 病毒同样利用了 IfRame ExecCommand 漏洞，使没有打 IE 补丁的用户收到邮件后会自动运行，具有非常强的传播性。

“求职信”不仅具有尼姆达病毒自动发信、自动执行、感染局域网等破坏功能，而且在感染计算机后还不停的查询内存中的进程、检查是否有一些杀毒软件存在。如果存在则将该杀毒软件的进程终止。每隔0.1秒就循环检查进程一次，以至于这些杀毒软件无法运行。该病毒每过8小时就搜寻一切可写的网络资源（如局域网的完全共享目录），随机产生一个文件名，加密后把复制过去。因此感染性极强。

该病毒如果感染的是Windows NT/2000系统的计算机，即把自己注册为系统服务进程，一般方法很难杀灭。它还不停地向外发送邮件，把自己伪装成“Htm、Doc、Jpg、Bmp、XLs、Cpp、Html、Mpg、Mpeg”类型文件中的一种，文件名也是随机产生的，很具隐蔽性。

当计算机时间为每年单月13日时，该病毒将会自动搜索硬盘，用内存中的随机数据覆盖硬盘上的所有文件，因此会给用户数据带来无法估量的损失。

二、中毒特征

当你觉察系统资源变少，机器速度变慢，硬盘空间非正常减少，共享目录被非法写入文件时，很有可能中毒了。进一步的确认请依照以下方法进行：

1、在操作系统目录下检查是否包含WQK.exe和KRn132.exe两个文件，如果有则已感染病毒；

2、运行 RegedIt，展开 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\Run\，检查其中是否包含 WINDOWS\SYSTEM\KRN132.EXE 和 WINDOWS\SYSTEM\WQK.EXE，如有则已感染病毒。

教你如何对付“BadtRans”（坏透了）病毒

近来电脑用户请谨防一种叫 BadtRans 的病毒变种，这种病毒的英文全称为“W32.BadtRans.B@mm”，是 W32.BadtRans.13312@mm 病毒的变种。这种可以自行复制的蠕虫病毒同样具有很高的危害性，它利用了 OutLook 的漏洞，完全不需要邮件接收者打开邮件附件就自动可执行。

一、识别病毒

含有该病毒的邮件没有任何正文，但有一附件，附件名由下面这三部分名称组合而成：

1、FUN、HUMOR、DOCS、S3MSONG、Sorry_about_yesteRday、ME_NUDE、CARD、SETUP、SEARCHURL、YOU_ARE_FAT!、HAMSTER NEWS_DOC、New_NapsteR_SIte、README、IMAGES、PICS

2、.DOC、.MP3、.ZIP

3、pIf、scR

比如 HUMOR.DOC.SCR 就是一例。

二、清除病毒

1、查找操作系统目录下的 System 文件夹，找到 CP_25389.NLS 文件，将之删除；

2、打开注册表 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\Run Once，从中找到 Run Once，将其右边窗口出现的 keRneL32 键值删除；

3、下载专用杀毒工具，将所有查到的已感染了 BadtRans.B 的文件全部删除。

至此，你应该可以高枕无忧了。

可令防毒软件失效的新病毒

这种新的网络蠕虫病毒全称为 w32.gokeR.a@mm，它会尝试着给你 OutLook 通讯簿中每一个邮箱地址发信。同时 GokeR 还包含有 mIRC 脚本，这使得病毒可以从一个受感染的 IRC 用户感染给另一位用户。GokeR 甚至能通过 WEB 网页进行传播，当浏览一个受感染的网页时，用户会被要求下载一个名为 Web.exe 的文件，在用户受到感染之后，病毒会自动禁止防毒软件运行，

一、病毒特征

该病毒主要通过电子邮件传播，哪些如何才能识别包含病毒的邮件呢？幸好病毒邮件有特征可供识别。

邮件主题通常为下列一项：

If I weRe God and dIdn't beLive In mySelf wouLd It be bLasphemy I can't heLp This LongIng,comfort me.

The ATeam VS KnIghtRIdeR …who wouLd Win ?

Just one kIss,will make It betteR。just one kIss,and we will be aLRIght.

The aIR will hoLd you If you try,tRust my Wings of desire.GLory,GLorIfIed.....

And I mIss you most of all,my daRLIng …

You just take a gIant step,one step higher.

It's daRk In heRe,you can feeL It all aRound。The underground.

I will aLways be With you sometImes bLack sometImes white …

…When autumn Leaves Start to fall

..and there's no need to be scared,you Re aLways on my mInd。

邮件正文至少包含下列一项：

Hey

They say Love Is bLInd …weLL,the attachment pRobabLy pRoves It.

PRetty good eItheR way though,Isn't It ?

Happy BIRthday

Yeah ok,so It's not yours It's mIne :)

stILL cause for a ceLebRatIon though,check out the detaILs I attached

You shouLd LIke This,It couLd have been made for you

speak to you LateR

This made me Laugh

Got some more stuff to tell you LateR but I can't stop RIght now

so I'LL EMail you LateR or gIve you a RIng If thats ok ?!

Speak to you LateR

附件名由字符串随机组合而成，后缀名有.plf,.scR,.exe,.com,or .bat.等等。

中度危险病毒 Fbound 新鲜出炉

病毒名称：W32/Fbound.c@MM

发现日期：20020313

最早出现地区：日本

长度：12288 字节

病毒类型：邮件病毒

危害级别：中

别名：WORM_JAPANIZE.A (趋势命名)

病毒特征：

该病毒以邮件的形式进行传播，其附件名为patch.exe。主题有可能是“Important”或用日语写成的。运行后，它会向Windows地址簿中的所有联系人发送带毒邮件。此病毒不会以任何方式将自身安装在受染机器上。病毒体内含有文本“IWorm.JapanIze”。

中毒迹象：

染上该病毒后，它会立即将自身向外发送，没有任何明显的中毒迹象。

感染方式：

手动运行附件EXE文件后，病毒会向外发送带毒邮件。

认清“尼姆达”病毒及其变种

今年出现的“尼姆达”(NImda) 给全球用户带来了无可弥补的损失，这种恶意蠕虫病毒来势凶猛，传播速度快，危害性大，作恶多端。自它出现以来，已发现有五种变种。现在就对这五种变种作一些简介，以便大家更好地掌握这种病毒的特性。

一、NImda.a

使用 Windows95，98，ME，NT 和 2000 操作系统的用户，均有可能在接收 EMail 的同时受到该病毒的感染。用户在浏览受感染的 WEB 服务器时，浏览器的安全级别设置在中级以下时，会感染上病毒；用户也有可能被开放网络中的另一客户端感染。

该病毒以电子邮件为传播媒介，携带该病毒的邮件的包含两部分：第一部分定义成 MIME 的“text/html”格式，但实际上没有任何文本，所以邮件内容是空的；第二部分定义成 MIME 的“audIo/xwav”格式，但实际上附带了一个 base64 编码的可执行二进制文件，名称为“Readme.exe”。通过 MAPI 从邮件的客户端及本地的 HTML 文件中搜索邮件地址，然后将病毒发送给这些地址。在某些系统“Readme.exe”附件能够自动执行，从而感染整个系统。

该病毒可以通过文件感染，它能在本地机器上寻找系统中的 EXE 文件，并将病毒代码置入原文件体内，从而达到对文件的感染。此外，它还会通过扫描 Internet，来试图寻找有漏没的 WEB 服务器，若感染成功，浏览该网站的用户便有可能惨遭其害。在局域网内，它还会搜索本地网络的共享文件，一旦发现机会便写入文件，从而使机器被感染。

二、NImda.b

在 NImada.a 的基础上作了轻微的改变，利用 PCShRInk 进行了压缩。附件名从 README.EXE（README.EML）改成了 PUTA!!.SCR（PUTA!!.EML）。

三、NImda.c

在 NImada.a 的基础上作了改变，通过 UPX 进行了压缩。

四、NImda.d

与 NImada.a 相似，利用 PECompact 进行了压缩。唯一明显不同的是源文件中出现的“版权”文本变为“大屠杀”病毒（HoLoCaust VIRus.!）； 作者为西班牙的 Stephan FeRnandez（V.5.2 by Stephan FeRnandez.SpaIn）.

五、NImda.e

该变种是金山公司反病毒应急处理中心于 10 月 30 日凌晨发现。根据金山公司对此变种的技术分析得知，其危害性与最初版的尼姆达有过之而无不及，而且将会是近期在互联网上迅速传播的大热恶意蠕虫。它与 NImda.a 的不同之处在于：

1、附件名字从 Readme.exe 改为 SampLe.exe

2、感染 IIS 系统时生成的文件从 AdmIn.dLL 改为 Httpodbc.dLL

3、在 NT/2000 及相关系统，病毒拷贝自己到 Windows 的 system 目录下，不再叫 mmc.exe，而用 CsRss.exe 的名字。

圣诞新年防“毒”心

圣诞节就快到了，新年的脚步声近了，您收到好友寄来的电子贺卡了吗？在节日的氛围中接收电子贺卡时千万不要马虎大意，因为你极有可能收到包藏电脑病毒的电子贺卡，如果你打开了，一些新的圣诞节、新年病毒则乘此机会粉墨登场。

一种名叫 Reezak 的病毒出现，该病毒以一幅圣诞动画示人，能够删除计算机的重要系统文件，从而导致计算机瘫痪。被感染的系统需要重装操作系统，然后经手工从备份文件中才能恢复那些被删的重要系统文件。

此病毒借以传播的邮件主题为：“HI.”（或“新年快乐”），附件是可执行文件 ChRIstmas.exe，它感染使用微软 Microsoft OutLook 或 OutLook Express 的电脑，并同时向外传播。该病毒有一系列化名，分别是 W32/MaLdaL.c@MM 、 W32/KeyLuc@MM 、 或 W32/ZackeR@MM。

另一种病毒被称为 JS_ExceptIon.GEN，其邮件主题为“HI!”，其内容是“HI，我发现了一个极酷的网

站 http://ceLebxx.，它真的很酷！”

这两种新病毒 19 日刚刚在互联网上亮相，尽管破坏力与此前出现的一些病毒不能相提并论，但它们刚刚开始传播，最终会影响到多少用户现在还是个未知数，但考虑到圣诞节日益临近，上网发送贺卡的用户与日剧增，所以计算机用户一定要谨防受到这两种病毒的攻击。

网友们圣诞期间收到“来路不明”的电子邮件，而且它带有附件文件的话，必须小心处理，千万不要随意开启附件。正确的方法是利用病毒扫描功能，或从杀毒软件公司网站下载最新病毒扫描程序，侦测邮件是否带毒。

谨防情书病毒的再度发作

收到情书，是每个人都高兴的事。可是，现在就怕你收到藏有病毒情书，便会乐极生悲。目前这种情书病毒共出现 19 个变种，引诱无数台机器中招。包含破坏（.VBS）、（VBE）、（.js）、.jse）、(.css)、.wsh、.sct、.hta、.jpg、.jpeg、.MP2、.MP3 等类型文档，以至于系统被破坏。这样的情书，你还敢接吗？

VBS/LoveLetteR（别名 I LOVE YOU，我爱你，爱虫，情书）病毒是一个用 VBS 编写的蠕虫病毒，该病

毒通过电子邮件及 IRC (Internet ReLay Chat)传播。爱虫病毒的触角甚至伸到了电子邮件以外的领域。该病毒侵袭的还有年轻人热衷的互联网实时聊天室(IRC)。另外，用户桌面上的一些软件也可能受到袭击，例如包含数字音乐的 MP3 或数码相片等。该病毒可能将逐渐覆盖这些文件，而用户可能要在数周之后才会发现。

一、病毒邮件特征

1、主题栏信息选自下列文本：

ILOVEYOU

SusItIkIm shI vakaRa kavos uodukuI...。

fwd: Joke

Mothers Day ORdeR ConfIRmatIon

Dangerous VIRus Warning

VIRus ALERT!!!

Important ! Read carefuLLy !!

2、附件信息将选自下列文件：

LOVELETTERFORYOU.TXT.vbs

VERY FUNNY.VBS。

MOTHERSDAY.vbs

VIRUS_WARNING.JPG.VBS

PROTECT.VBS

IMPORTANT.TXT.vbs

走进“万花谷”

你进入了网址为“http://www.on888.xxx.xxx.com”之类的网站，也许是因为它有一个非常好听的名称：万花谷，然而当你离开这个网站时，会突然弹出无数个浏览器窗口，这时即使你关闭所有的浏览器窗口，WINDOWS 仍然会出错，而且按任何按键都会失去反应，如果用“CtRL+ALt+DeL”结束任务，马上就会出现蓝屏死机的现象。重新启动计算机，会出现一个奇怪的提示：“欢迎你来万花谷，你中了‘万花病毒’请与 QQ：4040465 联系”，按下“确定”按钮，可以进入 WINDOWS，但桌面上所有的图标都消失了，而且你会发现 C 盘不能使用了，“开始”菜单上的“运行”、“注销”和“关机”项也都不见了，注册表也被禁用了。打开 IE 浏览器你会发现窗口的标题变成了“欢迎来到万花谷！你中了‘万花病毒’请与 OICQ:4040465 联系！”，打开收藏夹，你会发现多了一个名为“万花谷”的快捷方式，网址是“http://96xx.xxx.com”，打开该网址后，如果你的浏览器版本在 IE4.0 以上，显示的是一个有 4 种光效滤镜效果的网页，随着鼠标的移动，会造成光线照在网页图片不同地方的效果。

一、病毒特征

“万花谷”实际上是一个含有 Java ScRIpt 脚本代码的网页文件，但因为其脚本代码具有恶意破坏能力，而且许多个人网站竞相模仿该网站，给上网用户造成了极大的影响，因此也被反病毒厂商作为一种病毒对待。

“万花谷”病毒和其它普通脚本病毒有所不同的是，它具有极强的隐蔽性，它巧妙地利用了 encode 把自己的脚本隐藏，使得人们用“查看源文件”的方法来查看含有“万花谷”病毒的网页文件源代码时，只能看到一大段的乱字符。它没有传播能力，但却能修改或添加注册表的键值，给用户带来诸多的麻烦。

“万花谷”病毒是通过 ActIveX 对注册表进行修改的，为了达到破坏的目的，它要修改或添加注册表的以下键值。

设置

HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\PoLIcIes\ExpLoreR 主键下的“Norun”键值数据为“00000001”，以取消开始菜单上的“运行”项。

设置

HKEY_CURRENT_USER\Software\Microsoft\Wind

ows\Current Version\PoLIcIes\ExpLoreR\主键下的“NoCLose”键值数据为“00000001”，以取消开始菜单上的“关闭”项。

设置HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\PoLIcIes\ExpLoreR\主键下的“NoLogOff”键值数据为“00000001”，以取消开始菜单上的“注销”项。

设置HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\PoLIcIes\ExpLoreR\主键下的“NoDRIves”键值数据为“00000004”，以取消对 C 盘的访问权限。

清除 Shoho 病毒

又一种新病毒出现了！此病毒名叫Worm.Shoho.110592，又名 WeLyah，在某些操作系统中，只要受感染邮件被预览或打开，系统即会中毒。它会像 SIRcam 病毒一样利用自身的 SMTP 引擎向地址簿中的所有收件人发送邮件。并且该病毒还会删除一些 Windows 文件，以致在系统重启时导致常规性保护错误。

一、病毒特征

如果近期收到一封电子邮件，附件不是令人生疑的 EXE 文件，却是文本文件（.txt），请注意了，说不定这就是一封病毒邮件。

Shoho 蠕虫病毒以邮件的形式进行传播，其主题为："WeLcome to Yahoo! Mail."

邮件正文为：

This messages a chaRacteR set that Is not supported by the Internet Service.

To vIew the orIgInaL message content,open the attached message.

If the text doesn't dIspLay corRectLy,save the attachment to disk ,and then open It using a vIeweR that can dIspLay the orIgInaL chaRacteR set.

附件为 Readme.txt，其实这只是用于迷惑人的幌子，此文件是一个进行了伪装的含有恶意代码的 EXE 可执行文件。该附件一旦被打开，Shoho 蠕虫就会在 Windows 目录下生成 WinLOgOn.exe，并修改注册表，以致在每次启动 Windows 时病毒都会自动运行。

二、病毒危害

该蠕虫病毒利用的是 ms01020 IfRame 漏洞，一旦预览或打开邮件，其附件程序

README.TXT_____.pif 就会自动运行。当附件被自动执行后，电脑用户只要开启电脑后，病毒就会自动发作，并寄送大量邮件，对企业用户来说，大量的邮件将会造成服务器瘫痪。

清除 W32.HLLW.GOP@mm 病毒

W32.HLLW.GOP@mm 是新近发现的一种群发邮件的蠕虫病毒，它可以通过邮件与网络平台进行传播。其危害表现在它可向打印机不断发打印请求，打印乱码，由此造成严重的资源浪费。

一、病毒介绍

当该病毒被执行后，会将自身拷贝至 C:\Windows\System\KeRneLsys32.exe，同时在注册表 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\RunIMEKeRneL32 中增加一条键值：C:\Windows\System\KeRneLsys32.exe。

接下来病毒会“例行公事”地群发邮件，发出的大部分邮件会包含有中文字符，附件通常以.bmp、.Rtf、.doc、.txt、.gIf、jpeg 等“图片格式”，其实真正的后缀为.exe 或.Lnk。比如，一个名为“BIRthday pIc.bmp。exe”或“BIRthday pIc.bmp.Lnk”的附件，会打着“BIRthday pIc.bmp”

蛊惑他人。

病毒可以在.htm与.html文件以及邮箱中自动搜索邮件地址，发现目标后会利用自身的 SMTP 引擎群发邮件，而接收方收到邮件，一旦阅读则病毒会自动执行。

注意:之所以病毒可以自动执行，缘于利用了微软 OutLook 的系统漏洞，关于该漏洞的详细介绍与补丁下载，请参阅下面的网址。

http://www.Microsoft.com/Windows/Ie/downLoads/cRItIcaL/q290108/defauLt.asp

该病毒还具有网络传播的特性，它可以搜索网络上的映射磁盘，通过修改 Win.Inl 文件，可以感染网络中另一台计算机。

能够删除防毒软件的病毒 MaLdaL.D

W32.MaLdaL.D@mm（简称为“MaLdaL.D”，也称作“ZaCkeR”）是一个危害性极大的病毒，它用 VB 语言写成，大小只有 27KB 且用 Aspack 进行过压缩处理。病毒使用 Microsoft OutLook 向其通讯簿中的名单传播。

这种能够破坏杀毒软件的新型蠕虫病毒于去年 12 月 29 日首次在国外出现，1 月 2 日开始在互联网上缓慢传播。这种病毒该病毒可能会影响未升级的防

病毒软件，使杀毒软件不能运行或者删除某些文件。

一、病毒特征

这款病毒针对某些杀毒软件，先破坏杀毒软件，然后删除硬盘中的文件。因此该病毒的危害性主要体现在以下两个方面：

1、该病毒会试图删除一些杀毒软件。这也是该病毒的可恶之处，它能令防毒（或防火墙）软件失效或删除防毒软件，包括的产品有：AntIVIRaL TooLkIt PRo，FPROT95，PCCILLIn，FmacRo，McAfeeVIRusScan，Norton AntIVIRus，Zone Labs 等等。全是国外的产品，看来对国内的杀毒软件产品尚不起作用。

2、病毒会删除带有以下扩展名的文件：INI,.PHP,.EXE,.COM,.MPEG,.DAT,.ZIP,.TXT,.EXE,.XLS,.DOC,.JPG，由于可能删除重要的系统文件，因而会导致系统的不稳定性。

“MaLdaL.D”病毒通过电子邮件附件的形式进行传播，首次被用户执行时，它将自身安装至\Windows\System\Win.exe，同时在注册表HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\Run 中增加一行：

%System%\Win.exe

这样在下次启动计算机时，病毒便会自动运行

Win.exe。然而，在大部分情况下，只要您运行了此病毒，一般都是无法启动计算机的。

当附件再一次被执行时，病毒会通过邮件传播出去，主题为“ZaCkeR”，附件名为“ZaCkeR.exe”(这也是为什么该病毒也被称作“ZaCkeR”病毒的原因)，

其主题为“ZaCkeR”，邮件正文则是从某些固定字句中随机选择。

二、清除病毒

请用正版杀毒软件，下载最新病毒特征库后再查杀。

警惕伪装成安全补丁的 GIggeR 病毒

天下没有免费的午餐，如果你没有订阅相关的邮件列表，然而却突然收到一封主题为“OutLook Express 安全补丁”的邮件，可要注意了！因为至今尚未听说微软主动给用户发送安全补丁。您收到的只是 GIggeR 病毒伪装成的补丁！

这个名叫 js.gIggeR.a@mm 的新病毒是用 JavascRIpt 写成的，大小为 17K 左右，它会在被感染系统上利用 Windows ScRIptIng Host 自动执行。此病毒会通过 OutLook 地址簿中的联系人及 mIRC 聊天工具进行自我传播，而且还能借助本地网络感染其他计算机。一旦深中此毒，不仅会堵塞邮件服务器，更

为严重的是，它会在您重启机器试图格式化你的硬盘！

病毒毒特征：

病毒邮件主题为“OutLook Express Update”或为收件人的邮件地址，正文是“MSNSofware Co.”或者“Microsoft OutLook 98.”，附件为mmsn_offLIne.htm。

一旦用户不慎执行了附件，该病毒就会在电脑的根目录下创建两个文件：

BLa.hta

B.htm

同时还会在以下目录创建不同的文件：

C:\Windows\SampLes\Wsh\ChaRts.js

C: \Windows\SampLes\Wsh\ChaRts.vbs

C: \Windows\HeLp\Mmsn_offLIne.htm

改注册表也是此类病毒的一贯技俩：

HKEY_CURRENT_USER\Software\Microsoft\Windows ScRIptIng Host\Settings\TImeout

HKEY_CURRENT_USER\Software\TheGRave\badUsers\v2.0

同时添加 NAV DefALeRt 到以下注册表键中：

HKEY_LOCAL_MACHINE\Software\Microsoft\Win

dows\Current Version\Run

更为恶毒的是，病毒最后会在批处理文件 AutoExec.bat 中添加“ECHO y|format c:”命令，懂 DOS 命令的用户都知道，这是一条不显示命令行本身的格式化命令，也就是说，当用户重新启动计算机时，该病毒可以不动声色地执行格式化命令，令用户损失惨重！

病毒通过 mIRC 传播是通过它创建的 scRIpt.InI 文件来执行的，当被感染机器与网络相连时，它还会创建病毒副本，伺机传染。

二、病毒查杀

第一，关掉 Windows ScRIptIng Host，防患于未然；

第二，不要执行附件；第三，用正版杀毒软件扫描。

专攻 WORD 的宏病毒现形

一种专门征对 WORD 设计的宏病毒 W97M/PacoL.a 出现了。该病毒最早发现于菲律宾，可以感染 Word 97 及 Word2000 文档，是一个文件感染型病毒，无须通过感染标准模板而直接感染别的文档。

一、病毒特征

W97M/PacoL.a 可将 Word 的安全级别设置为

“低”，并创建以下文件：

c:\Windows\Startm~1\programs\Start Up \Winword.bat

**Windows 启动并执行了下面两个文件后，该批处理文档自动执行。

c:\Windows\Winword.Reg **包含了修改注册表安全级别设置的代码

c:\Windows\Normal.doc **此为受病毒感染的 Word 模板文档

接下来病毒会在硬盘与网络驱动器中搜索 Word 文档（.doc）并覆盖之，其后会搜索所有的.txt、.wRI、.pdf 文件并覆盖，同时删除原文件，并将这些文件的后缀名改为.doc。

当病毒成功感染文件时，Office 助手会出现如下图所示的画面：

因此，不难得出结论，打开一个受感染的文件会导致整个儿硬盘（或网络）中的相关文档受感染。病毒通过隐藏自身的文档与网络传播。

二、中毒迹象

打开电脑，查找这三个文件，若存在，则表明中毒：

“ c:\Windows\Start m~1\programs\Start

Up\Winword.bat”

“c:\Windows\Winword.Reg”

“c:\Windows\Normal.doc”

另一迹象是 Windows 启动完毕，Word AppLIcatIon 自动打开，且有上图所示的画面弹出来。

三、防杀方法

1、请用正版杀毒软件清除。

2、在 MS Office 中禁用宏。

3、下载升级包 Office2000 updates 与安全补丁。

新病毒 W32/FagLed@MM 解析

W32/FagLed@MM 病毒最早于本月 21 日发现，这是一个蠕虫病毒，通过电子邮件传播，也可以通过 mIRC 与 Microsoft Messenger 等程序传播。

一、病毒特征

病毒主要通过电子邮件传播，邮件主题与正文变化多端，附件通常为 LED.EXE（也可发生变化）。下面是一些常见的组合：

主题：check out my ePhoto ALbum

正文：

主题：LOL!

正文：

主题：Why sex feeLs so good?

正文：；）

主题：This Is how you RemInd me,WHAT I REALLY AM,I'm NOT LIKE YOU,SO SORRY!

正文：

主题：uRgent!! you sent me a vIRus!

正文：HI,I just ReceIved a EMail fRom you contaInIng the hIghLy destRuctIve one of the foLLoWing Is RandomLy seLected [W32/ToagDIpust,W32/LLehmorfTaog.C,W32/LOAeSuI.A,W32/StRIng.!eRehemIttaeRgagnIvahmI,W32/BadTRans,W32/LED,W32/MatRIx,W32/AOL,W32/CockRoach,W32/Dunno.k] vIRus。It Looks LIke your Computer Is Infected With This dangeRIous vIRus,so I attached a cLeaneR to This EMail to cLean your Computer fRom the vIRus..。

or

主题：uRgent!! you sent me a vIRus!

正文：HI,I just ReceIved a EMail fRom you contaInIng the W32/ResudaB vIRus。

It Looks LIke your Computer Is Infected With This dangeRIous vIRus,so I attached a cLeaneR to This EMail to cLean your Computer fRo

m the vIRus..。

主题：haha

正文：

新病毒“我的晚会”完全档案

病毒名称：W32/MypaRty.a@MM

发现日期：20020127

最早出现国家：俄罗斯

长度：29,696 字节

病毒类型：邮件蠕虫病毒

危险级别：中

别名：IWorm.MypaRty (AVP),MyPaRty (FSecuRe),W32.MypaRty@mm (NAV),W32/MyPaRtyA (Sophos),W32/MypaRty@MM ,W32/MypaRty@MM (熊猫),Win32.MyPaRty (CA),Win32.MyPaRty.A (AVX),WORM_MYPARTY.A (趋势科技)

一、病毒简介

该邮件病毒会在WindowsNT/2K/XP系统上生成一个后门程序 BackDoorAAF。蠕虫本身不带有具破坏性的有效载荷。它的邮件信息如下：

主题：new photos fRom my paRty!

内文：HeLLo!

My paRty..。It was absoLuteLy amazIng!

I have attached my web page With new photos!

If you can pLease make coLor pRInts of my photos。Thanks!

附件：www.mypaRty.yahoo.com（29696 字节的 PE 文件）

从附件的文件名来看，它会诱使有些用户认为点击此超链接将会链接至雅虎网站。

某些邮件客户端，特别是那些在文件名下面加下划线的客户端，会使得附件更像一个 URL 地址。其实，病毒的附件是一个后缀为.COM 的可执行文件，并不是 URL，只要一运行就会感染机器。

“我的晚会”病毒技术特征

时至年尾，病毒再起作乱。近日，金山反病毒应急中心又成功捕获一例通过电子邮件传播的蠕虫病毒“我的晚会”（My PaRty），金山毒霸命名为 Worm.MyPaRty.29696。此病毒最早于 1 月 27 日出现在俄罗斯，第二日便在亚洲地区突现，目前已开始向欧洲蔓延。

据金山反病毒应急中心对这一病毒的分析得知，这是一个通过 Internet EMail 进行传播的蠕虫病毒。蠕虫病毒体文件长度 29696 字节，解压缩之后为 92050 字节，是用 Microsoft VIsuaL C++编写的。

该蠕虫所发送的邮件如下所示：

主题：new photos fRom my paRty!

正文： HeLLo!

My paRty...。It was absoLuteLy amazIng!

I have attached my web page With new photos!

If you can pLease make coLor pRInts of my photos。Thanks!

附件：www.mypaRty.yahoo.com（注意：这是文件名，并非 URL）

所幸的是，这个蠕虫并没有象最近流行的几个蠕虫一样利用 IfRam 漏洞，这份附件必须要接到邮件的人主动打开它才会生效。

MyPaRty 蠕虫运行后，将把自身种植在系统内并开启一份传播程序。依据系统的不同，该病毒所拷贝文件的路径也不同，在 Win9X 以及 WinMe 下，该蠕虫将在 C:\根目录下生成一份 RegctRL.exe 的文件，而在 WinNT 系列操作系统上（包括 2K/XP），这份名为 RegctRL.exe 的文件是拷贝到 C:\ReCycled 目录下的。

同时病毒将会复制自身到 C:\RECYCLER\F%d%d%d 或者 C:\RECYCLED\F%d%d%d

其中%d 会被病毒以随机数字代替，比如病毒有可

能在选定的目录下生成类似这样的文件名：F10027293491986、F251951496223584、F315483318454、F63752183529323等等。

一、病毒疫情周报表

计算机病毒疫情监测周报

1、“网络天空”变种(Worm_Netsky.D)

该病毒通过邮件传播，使用UPX压缩。运行后，在%Windows％目录下生成自身的拷贝，名称为WinLogon.exe。（其中，%Windows% 是 Windows 的默认文件夹，通常是 C:\Windows 或 C:\WINNT），病毒使用Word的图标，并在共享文件夹中生成自身拷贝。病毒创建注册表项，使得自身能够在系统启动时自动运行。病毒邮件的发信人、主题、内容和附件都是不固定的，

2、“爱之门”病毒(Worm_Lovgate.C)

该病毒兼有蠕虫和黑客的功能，并能够通过局域网进行传播，局域网中一旦一台计算机被感染，病毒就会扩散到整个局域网，从而导致网内所有计算机均处于被控的危险状态，系统安全和信息安全收到极大的威胁。值得注意的是，由于病毒可以通过对Microsoft OutLook和OutLook Express中收到的邮件进行回复的形式向外发送病毒邮件，与以往的病毒

邮件相比，更具欺骗性和迷惑性。

3、“高波”病毒变种（Worm_AgoBot）

该病毒是常驻内存的蠕虫病毒，利用 RPC DCOM 缓冲区溢出漏洞、IIS5/WEBDAV 缓冲区溢出漏洞和 RPC Locator 漏洞进行传播，还可通过弱密码攻击远程系统进行主动传播以及利用 mIRC 软件进行远程控制和传播。病毒运行后，在%System%文件夹下生成自身的拷贝 nvchIp4.exe。添加注册表项，使得自身能够在系统启动时自动运行。

4、“贝革热”病毒变种（Worm_BbeagLe.J）

病毒通过电子邮件进行传播，病毒运行后，在%System%文件夹下生成自身的拷贝，名称为 IRun4.exe。病毒还在%system%文件夹下生成 IRun4.exeopen，该文件是一个加过密的.zIp 文件包，其内容为病毒代码，密码是随机生成的。病毒添加注册表项，使得自身能够在系统启动时自动运行。

二、本周病毒动态分析

通过对以上监测结果分析，本周“网络天空”病 Worm_Netsky.D

排名还是第一位，还保持很高的发作率。再次提醒计算机用户做好防病毒的措施。

“爱之门”病毒 (Worm_Lovgate.C)及其变种这

周的排位依旧第二位，该病毒还是比较顽固，发作率一直都很高，还有不少计算机用户受到该病毒的感染，估计该病毒及其变种在其后的时间里还会继续对计算机用户造成危害，因此提醒广大计算机用户注及时升级杀毒软件，做好防毒的措施，以免受到侵害！

“高波”（Worm_AgoBot）病毒及其变种这周第三位，请计算机用户关注该病毒的发展变化，做好必要的防毒措施！

“贝革热”病毒的变种 Worm_BbeagLe.J 这周排名第四位，该病毒的一个新变种 Worm_BbeagLe.AF 这周时间里没有大规模的爆发，得到有效的控制，但还是提醒用户密切注意该病毒变种的发展趋势，做好防毒措施！

从这周病毒的发作情况来看，一些老病毒仍对计算机用户造成危害，这些老病毒依旧交替给计算机用户带来很大的危害，再次提醒计算机用户要对自己的系统做好防范措施，及时打安全漏洞补丁，升级杀毒软件。

三、建议可采用以下病毒防范措施

1、对于感染“网络天空”的新变种 Worm_Netsky.D 病毒的计算机用户提醒用户及时升级杀毒软件，或可以登陆网站：

http://www.antIvIRusChina.org.cn/content/Worm_Netsky.D.htm 查阅

2、对于感染 Worm_Lovgate.c 病毒及其变种的计算机用户可以用杀毒软件进行查杀或是手工清除该病毒，其具体清除的方法可以登陆：http://www.antIvIRusChina.org.cn/content/Worm_Lovgate.C.htm 查阅

3、对于感染“高波”病毒新变种 Worm_AgoBot 的计算机用户提醒用及时打补丁或登陆到网站：http://www.antIvIRusChina.org.cn/content/Worm_AgoBot.htm 查阅。

4、对于感染“贝革热”病毒变种（Worm_BbeagLe.J）的计算机用户提醒用户及时升级杀毒软件，或可以登陆网站：http//www.antIvIRusChina.org.cn/content//Worm_BbeagLe.J.htm 或 http//www.antIvIRusChina.org.cn/content//Worm_BbeagLe.AF.htm 查阅

5、不要轻易打开来历不明的邮件，尤其是邮件的附件。

6、闭不必要的服务和端口。

7、将浏览器的安全级别设为中级以上。

8、不要随便登录不明网站。

9、Office 软件的安全级别设定为中级以上。

10、使用光盘、软盘进行数据交换前，先对其进行病毒检查。

11、将系统配置改为从硬盘引导，不要用软盘引导系统，防止感染引导型病毒。

12、做好系统和重要数据的备份，以便能够在遭受病毒侵害后及时恢复。

13、发现网络和系统异常，及时与国家计算机病毒应急处理中心或防病毒厂家联系。

万花谷“中的”陷阱“

据悉，最近监测到国内有心怀不轨的人到处在互连网上散发一个美丽诱人的网址”万花谷“，这实际是一个恶意”陷阱“，有人经不住诱惑，只用鼠标轻轻点一下，计算机就立即就瘫痪了，这是有人利用 Java 最新技术进行破坏的又一个恶意网址。北京江民公司提醒广大上网用户注意严加防范，遇到有 On888.xxx 之类的网址请不要点击，并开启 KVW3000 的病毒实时监视防火墙进行防杀。

附该病毒的技术特征和修复方法：

JS/On888 是一个新的含有有害代码的 ActIveX 网页文件，它通过在一个网络地址来对计算机用户造

成破坏,其破坏特性如下：

（1）用户不能正常使用 WINDOWS 的 DOS 功能程序；

（2）用户不能正常退出 WINDOWS，

（3）开始菜单上的”关闭系统“、”运行“等栏目被屏蔽，防止用户重新以 DOS 方式启动，关闭 DOS 命令、关闭 REGEDIT 命令等。

（4）将 IE 的浏览器的首页和收藏夹中都加入了含有该有害网页代码的网络地址。

具体的表现形式是：

a 网络地址是：www.on888.xxx.xxx.com；

b 在 IE 的”收藏夹“中自动加上”万花谷“的快捷方式,网络地址是：”http://96xx.xxx.com“；

进入该网页的话，如果你的浏览器的版本在 IE4.0 以上，那么该网页显示的是一个有光效滤镜的网页，随着鼠标的移动，会造成光线照在网页图片不同地方的效果，光效一共有 4 种。

将 IE 的首页通过系统注册表项

HKEY_LOCAL_CURRENT_USER\\Software\\Microsoft\\Internet ExpLoreR\\Main \\Start Page”，设置成为“on888.xxx.xxx.com/”；

为了达到该网页文件的破坏性，该 ActIveX 对系

统的注册表做了如下的修改：

首先在开始菜单上禁止了“运行”项目，使用户不能通过通常的注册表编辑器来修改该有害网页对系统注册表的修改：

以下的注册表项表现在没有“运行”菜单：

“HKCU\\Software\\Microsoft\\Windows\\Current Version\\PoLIcIes\\ExpLoreR\\Norun”;

以下的注册表项表现在没有“关闭系统”项目：

“HKCU\\Software\\Microsoft\\Windows\\Current Version\\PoLIcIes\\ExpLoreR\\NoCLose”;

以下的注册表项表现在没有“注销”项目；

“HKCU\\Software\\Microsoft\\Windows\\Current Version\\PoLIcIes\\ExpLoreR\\NoLogOff”;

以下的注册表项表现在没有所有的逻辑驱动器：

“HKCU\\Software\\Microsoft\\Windows\\Current Version\\PoLIcIes\\ExpLoreR\\NoDRIves”;

以下的注册表项表现在禁止注册表的编辑工具REGEDIT：

“HKCU\\Software\\Microsoft\\Windows\\Current Version\\PoLIcIes\\System\\DIsabLeRegIstryTooLs

以下的注册表项表现在没有桌面：

”

HKCU\\Software\\Microsoft\\Windows\\Current Version\\PoLIcIes\\ExpLoreR\\NoDesktop“；

以下的注册表项表现在禁止运行所有的DOS应用程序；

”

HKCU\\Software\\Microsoft\\Windows\\Current Version\\PoLIcIes\\WinOLdApp\\DIsabLed“；

以下的注册表项表现在系统不能启动到”实模式（传统的 DOS 模式）“下；

”

HKCU\\Software\\Microsoft\\Windows\\Current Version\\PoLIcIes\\WinOLdApp\\NoreaLMode“；

以下的注册表项表现在WINDOWS系统登录时显示一个登录窗口（在 MICROSOFT 网络用户登录之前）：

”

HKLM\\Software\\Microsoft\\Windows\\Current Version\\WinLogon\\LegaLNotIceCaptIon“,（窗口的标题是）”欢迎来到万花谷!你中了※万花奇毒※.请与 OICQ:4040465 联系!“)；

”

HKLM\\Software\\Microsoft\\Windows\\Current Version\\WinLogon\\LegaLNotIceText,（窗口中的文字是）\“欢迎来到万花谷!你中了※万花奇毒※.请与 OICQ:4040465 联系!”)；

以下的注册表项表现在所有 IE 的窗口都会加上以下的 WINDOWS 标题窗口：

“ HKLM\\Software\\Microsoft\\Internet ExpLoreR\\Main \\Window TItLe”,“欢迎来到万花谷!请与 OICQ:4040465 联系!”)；

“ HKCU\\Software\\Microsoft\\Internet ExpLoreR\\Main \\Window TItLe”,“欢迎来到万花谷!请与 OICQ:4040465 联系!”)；

最后的表现是在用户的计算机的 IE 浏览器上打开无数的窗口，使得 IE 根本无法使用。同时用户正常的一些功能：桌面、开始中的运行、DOS 方式、REGEDIT 等都无法使用。

请所有的 KV3000 的用户抓紧升级到 KVW3000 最新的防杀病毒库，来预防该类恶意网页的侵害。用户可以使用 KVD3000 和 KV3000.exe 来清除计算机上的所有有害的网页文件。

受害用户的修复方法：系统的注册表的恢复，建议用户使用 F8 启动到 MSDOS 方式下，使用

SCANREG/RESTORE 命令来恢复原来正常的注册表。

警惕“Leave”病毒!

FBI 下属的国家基础设施保护中心（NIPC）和几家反病毒企业在上周六发出警告称，一种被称为“W32Leave.Worm”的新病毒，会自行在网上寻找感染了“SubSeven”特洛伊木马程序的电脑，可以被用来下载和储存其他带有恶意的文件，包括那些被用来发起分布式拒绝服务攻击的文件。

SubSeven 是一种极具侵略性的远程管理程序，包括一个客户和服务器应用程序。一旦被安装到受害者的电脑上之后，服务器应用程序会收集该电脑的连接信息。一个使用 SubSeven 客户应用程序的攻击者，在连接到后门端口之后，可以浏览受害者电脑上的文件，获取他们的击键信息，浏览他们的虚拟桌面，打开和关闭程序，甚至远程关闭被感染的电脑。

“W32Leave.Worm”攻击运行 Windows 9x、2000 和 Windows ME 的电脑，不过，对每一种版本操作系统的影响都不相同。例如，在 Windows ME 上，这种新病毒将在系统运行一个程序清单中的任何一种程序时自行启动，这个程序清单中包括微软 OutLook、Wordpad 和 NapsteR 等最常用的程序。

这种新病毒看起来可以使用一个加密的链接清

单，从一些网站上下载组件，并包括可以接收来自 IRC 指令的代码。一旦运行之后，这种新病毒将对互联网进行扫描，寻找感染了 SubSeven 的电脑，并自动把自己安装在这些电脑上。据赛门铁克公司发出的一份病毒警告称，这种新病毒只能影响那些已经感染了 SubSeven 的电脑，似乎无法通过电子邮件四处传播。

赛门铁克还表示，这种新病毒瞄准的显然是那些没有运行反病毒软件的电脑，因为几乎所有的反病毒软件都可以侦测到 SubSeven 和它的许多种变形。

苹果迷小心！ SImpsons 辛普森病毒入侵 Mac OS

近日发现一只名为“Mac_SImpsons.A 辛普森”的计算机新病毒，主要针对 Mac 操作系统进行攻击。该病毒由 AppLescRIpt 所撰写，主要通过 Mac OS 的 OutLook Express 或 Entourage 电子邮件系统来传播，信件主题为：SecRet SImpsons epIsodes!(未公开的辛普森家庭影集!)，并夹带名为“SImpsons EpIsodes”(辛普森家庭影集)的文件。Mac 使用者一旦执行该附加文件，病毒会寻找电子邮件系统的通讯簿，自动发送大量垃圾邮件。SImpsons 辛普森病毒还会启动 IE 浏览器，连结至著名卡通「辛普森家庭」的官方网站：http://www.snpp.com/epIsodes.html。

趋势科技技术支持部经理康宏旭表示：「由于“辛

普森病毒”具有大量传播垃圾邮件的特性，除了会感染 Mac OS，还会针对 PC 使用者发送夹带病毒的信件。虽然不致于造成PC中毒，但网络频宽将会因此拥塞。」趋势科技呼吁苹果迷，不要开启主题为：SecRet SImpsons epIsodes 的电子邮件。趋势科技产品用户请立即更新病毒码，以侦测、清除此病毒。

如何判断 Mac_SImpsons.A 辛普森病毒

信件主题：SecRet SImpsons epIsodes!(未公开的辛普森家庭影集)

信件内容：

HundReds of SImpsons epIsodes weRe just secRetLy pRoduced and sent out on the Internet,If This message gets to you,the epIsodes are encLosed on the attachment program,whIch will onLy Run on a MacIntosh。You must have system 9.0 or 9.1 to watch the hILaRIous epIsodes,In hIgh quaLIty。Just downLoad and open It。

FRom,<寄件者>

附件名称：“SImpsons EpIsodes”(辛普森家庭影集)

新蠕虫病毒太厉害

美国 Norman Data Defense Systems 于美国当地

时间 6 月 28 日发出警告说，目前已发现电子邮件蠕虫(EMail Worm)和网络爬行者(network cRawLeR)成对出现的“W32/LInong.A@mm”和“VBS/LoveLetteR.CQ@mm”病毒。其危险度为“高”。

蠕虫“W32/LInong.A@mm”和“VBS/LoveLetteR.CQ@mm”会侵入用户系统并写入怀有恶意的恶作剧代码。还能够向 OutLook 和共享硬盘扩散，从而最终在 WWW 上漫延。该病毒主要感染小企业、SOHO 和个人用户的个人电脑。一旦被感染，MS Exchange Server 就有崩溃的危险。

上述蠕虫发来的电子邮件的主题、正文及附件的名称各种各样，目前已经确认的有如下之例：

One of This Mail,TRue Story ...。myLInong.exe

Info FROm CFusIon,You can update your CFusIon Online For FRee,CFusIon.exe

Patch Your CFusIon,Are You Ready FIx Your CFusIon,PLease Update PatchFusIon.exe

StILL RemembeR You,She Is MY sexy LInong,MyLInong.exe

LIght Up The NIght,LIght up The NIght PARTY...,LIght up the nIght.exe

Man ChoIce,Are You Man or women。This Is The

sponsor fRom our sIte The man choIce StaRMILd.exe

KIss Me100 way to kIss your GIRLFRIend or your boyfRIend KIss.exe

Sexy ModeL DId you eveR see the sexy gIRLs LIke heR Sexy.exe

Popeye CaRtoon The New Popeye New CaRtoon NetWork Popexe.exe

OLive & Popeye OLive And Popeye CaRtoon OLive.exe

MyGIRLFRIend Dogs NIce dog..。BuLLBuLL.exe

My GIRL FRIend\` Dogs Good Dog and SmaRt dogs MoLy.exe

Sweet LoveLy My Icq FRIend Sweet and LoveLy LoveLy.exe

Password HeRe The LIst of Nude Password WebsIte。ALL of them StILL ActIve,and few of them are death password 868879.exe

Need HeLp Do you need heLp ? to get money oveR the Internet。You can Read the heLp HeLp.exe

BILL BILL.。BILLGate

MIkRopos The New MIkRopos Software FRom MIkRopos Network MIkRopos

其执行文件“PCPoweR.exe”和“MyLInong.exe”能够自我复制，并将 VBS 文件“myLInong.vbs”写入 Windows 系统文件夹。这些文件由如下注册表键值指定： HKEY_LOCAL_MACHINESoftwareWindowsCurrent VersionRun

而且该病毒还会把上述文件中的某一个复制到 Windows 系统目录中，并向 OutLook 的地址簿中保存的所有地址发送复制的蠕虫程序。之后，将以“LInong I Love U So Muc LInong For eveR My LoveX”的名称制作 501 个目录。其中 X 为从 0 到 500 的 501 个数字。

上述蠕虫可将 VB ScRIpt“VBS/LoveLetteR.CQ”Windows 保存到 Windows 系统目录下，然后再复制到如下 4 个文件中。

myLInong.jpg.shs

KeRn32LIn.vbs

VbRun32DLL.vbs

myLInong.jpg.vbs

接着将设定如下注册表键值：

HKEY_LOCAL_MACHINESoftwareMicrosoft WindowsCurrent VersionRun

KeRn32LLIn KeRn32LIn.vbs

HKEY_LOCAL_MACHINESoftwareMicrosoft WindowsCurrent VersionRunServices

VbRun32DLL vbRun32DLL.vbs

HKCUSoftwareMicrosoftInternet ExpLoreRMain Start Page

http://www.thewebpost.com/Lovepoems/1198/dpt112098ILy.shtml

最后通过电子邮件把原蠕虫执行文件发送给OutLook地址簿中的所有地址。

更为恶劣的是，这些蠕虫还会自动生成IP地址并进行连接。如果硬盘是共享的话，就可能会把蠕虫自身“LInong.vbs”复制到其他个人电脑的根目录、Windows文件夹和启动文件夹中。然后，每隔一天这些蠕虫就会显示一遍这样的信息：“I Love You LInong，You are the Love of my Love...”。

Norman公司已经在该公司的网站（http://www.norman.com/vIRus_Info/w32_LInong.shtml）上提供详细信息以及驱虫文件等。

“目前小企业中防火墙的设置等措施还不尽完善，硬盘共享等情形下的安全和风险管理也多有疏忽之处，因此极易受到蠕虫入侵”（Norman公司首席执行官HenRy Dugan）。

小心七月六日电脑病毒快乐时光报到

日前肆虐台湾的电脑病毒‘快乐时光(vbs.haptIme@mm)’，将在七月六日再度发作，电脑族务必在此之前做好扫毒工作，或是避免用 MS OutLook 收信软件看‘伊妹儿’；若是信件中有以‘HELP’为发信主旨的邮件，不要打开、立即杀除该信件，则可逃过中毒一劫。

VBS 病毒通常藉由发信主旨为‘HELP’的电子邮件传播，并夹带‘.UNTITLED.HTM’的档案，或是直接将病毒码夹带于邮件之中发出。收件人若是没有防毒软件、或是扫毒过期，只要一开启夹带 VBS 病毒的邮件，病毒就会感染电脑。

据了解，中毒的电脑除了将会向通讯录中记载的邮件帐号，自动发出含毒的信件外，还会破坏电脑中的 .EXE、.DLL 等执行档，进而瘫痪应用程序。

为了防范 VBS 于六日来攻，最好的方式是在电脑中安装防毒软件。一般可以到以下网站下载免费的防毒软件试用版及最新病毒码。

Sophos:六月份前 10 大病毒

英国反病毒公司 Sophos 公布了 6 月份十大病毒，按照发作频率排名如下：

1.W32/ MagistrA22.2%（Magistr）马吉斯病毒

2.W32/BadTRansA10.9%（BadTRans）BadTRans 邮件病毒

3.VBS/VBSWGX 9.6%（Homepage）主页病毒

4.W32/ApoLogyB7.4%（ApoLogy vaRIant）一种复合病毒

5.W32/HybRIsB6.3%（HybRIs vaRIant）白雪公主病毒

6.TRoj/KeyLogC4.6%（KeyLog vaRIant）一种木马程序

7.W32/FLcss2.8%（FunLove）FunLove 病毒

8.W32/NavIdadB2.6%（NavIdad vaRIant）圣诞节病毒

9.VBS/KakWorm2.2%（KakWorm）一种网络病毒

10.VBS/VBSWGZ2.2%（MawaneLLa）一种政治性病毒

日本今年上半年病毒报告数增长 3 倍

日本信息处理振兴业务协会(IPA)安全中心(www.Ipa.go.jp/Security/)于 7 月 5 日公布了 2001

年上半年(1月到6月)和2001年6月份的病毒报告情况。该报告显示，日本上半年收到的报告数总共为9569件，为去年同期的大约3倍。按照不同病毒分析以后发现，“HybRIs”占总数的3分之1，而“MTX”大约占总数的4分之1。另外，7成以上的病毒是通过电子邮件的附件感染的。

2001年6月份收到的报告数总共为1335件，其中实际受到感染和损失的有153件。从上一个月开始这一数字略为减少。但是实际上这一数字只不过是冰山露出水面的一小部分。所以，最好不要误以为情况已经开始好转。收到报告较多的病毒依次为“HybRIs”(376件)、“Magistr”(253件)以及“MTX”(203件)。“HybRIs”和“MTX”仍然在盛行。

同时IPA还提请人们注意，VaccIn软件(反病毒软件)只是用来检测病毒的软件而不是用来修复被感染的文件。即使具有修复功能，也未必能够将文件完全修复到原来的状态，在被感染以后再安装没有实际意义。

另外，该机构还公开了最近该中心经常收到的咨询的“5个问题”。将以下内容收集到FAQ中。

(1)如果在发件人和主题名等空白的电子邮件中附有附件则为“HybRIs”病毒

(2)如果由于感染“MTX”导致文件受到破坏，那么不能用消除病毒软件进行修复

(3)要想检查是否被病毒感染需要使用消除病毒软件

(4)如果 Windows 的“最大化”按钮等乱码，原因不在于病毒而在于字体文件出了问题

(5)即使使用消除病毒软件，如果病毒库文件陈旧的话也未必能够检测得到病毒

funLove 病毒解决方案

长期以来，funLove 病毒在我国感染率居高不下，关于被FunLove病毒感染和寻求解决方案的电话和邮件不断，尤其是 NT 服务器感染该病毒后的清除一直存在问题。为了解决当前用户存在的问题，国家计算机病毒应急处理中心针对这一状况，向各应急单位征集关于该病毒的解决方案，要求各应急单位针对自己的产品提供在当前主流系统下清除 funLove病毒的具体方法（包括手工方法、使用各自产品的清除方法），希望能为用户在解决该病毒的过程中予以参考和帮助。

对于感染 FunLove 病毒的用户，国家计算机病毒应急处理中心建议，在查杀病毒时注意以下几点：

1、网络用户在清除该病毒时，首先要将网络断

开，

2、然后用软盘引导系统，用单机版杀毒软件对每一台工作站分别进行病毒的清除工作。

3、对于单机用户直接从第二步开始。

4、若服务器端染毒 funLove 病毒的，且使用 NTFS 格式，用 DOS 系统盘启动后，找不到硬盘，则需将染毒的硬盘拆下，放到另外一个干净的 Windows NT/2000 系统下作为从盘，然后用无毒的主盘引导机器后，使用主盘中安装的杀毒软件再对从盘进行病毒检测、清除工作。

5、确认各个系统全部清除病毒后，在服务器和个工作站安装防病毒软件，同时启动实时监控系统，恢复正常工作。

Symantec 发布防范星期五(13 日)病毒警讯

防病毒专业厂商 Symantec 公司日前向用户和网络管理人员发出警讯，告诫他们在星期五(7 月 13 日)之前务必使其防病毒保护技术达到最新水准，因为病毒作者特别喜欢这类“黑色星期五”。

这家防病毒公司的新西兰经理 RIchaRd BatcheLaR 说：“我们不能肯定今年 7 月 13 日(星期五)会有病毒发作，然而，我们正鼓励管理人员和计算机用户知道这些可能威胁，并做好防范准备。”

BatcheLaR 称，有许多已知病毒会在为星期五的 13 号发作，同时还有许多病毒可在任何月份的 13 号启动。他指出，对付已被识别病毒的最佳防御措施是使病毒防护技术保持最新水平。

ITAA 发现针对 IIS 的“Code Red”蠕虫

美国 IT 业界团体 InformatIon TechnoLogy Association of AmeRIca (ITAA)与安全产品开发商于美国当地时间 7 月 20 日发布了有关蠕虫“Code Red”的警告。目前受这种蠕虫破坏的面积正在迅速扩大。

Code Red 是利用美国微软的“Internet InformatIon Server(IIS)”的缓冲器溢出这一安全漏洞进行感染的蠕虫。这一安全漏洞早在上个月就已经被发现，该蠕虫可以感染那些

没有使用补丁程序的个人电脑。

攻击者除了控制被感染的服务器对 WWW 站点进行改写外，还会发动 DoS(拒绝服务)攻击以及格式化硬盘等非法行为。

CodeRed 的主要特征如下：

改写英语 WWW 站点，显示“WeLcome to www.Worm.com! Hacked by ChInese!”等信息。

每月 20 日—28 日将对白宫的 WWW 站点的 IP 地址发动 DoS 攻击。

每月 20 日以前尽可能对更多的服务器发动随机攻击。

同时，微软公司已在 WWW 站点上公开了 IIS 的最新补丁程序。

另外，面向企业的安全服务提供商美国 Security 也于当日宣布发现了 Code Red 的变种。这种变种蠕虫虽然随机感染服务器，但并不改变 WWW 站点的内容。

其它各安全产品公司也纷纷发布了解决 Code Red 的解决办法，比如：

美国 Network Associates 的子公司 McAfee 在自己的站点(www.mcafeeasap.com)上提供了可以确认安全漏洞的在线扫描工具“CybeRCop WormScan”。

美国 Symantec 提供的各种产品和安全服务“Symantec Web Security”能够检测出 Code Red 恶意使用的安全漏洞，此外还正通过 www.symantec.com/avcenteR 免费发放检测工具“FIxCodeR”。

小心 Worm.SIRcam 病毒

Worm.SIRcam.137216 病毒是一个蠕虫病毒，如果不小心运行，它会拷贝自己的有效代码到 Windows 的 system 目录，名为 Scam32.exe，并修改注册表 HKLM Software Microsoft Windows CuRRent Version Run

Services DRIveR32 指向该文件。以便下次启动时启动。同时，它还会拷贝自己到 ReCycled 目录，并修改注册表的 exe 文件关联(HKLM SOFT WARE CLasses exe file sheLL open command)指向改文件。

病毒发送附件时会选择一个正常文件做伪装，将自身代码放在前面，正常文件附加在后面。在发送出去。当收信人打开附件，病毒文件会将自身文件和正常文件分开放到 ReCycled 目录，运行自身并打开正常文件。极具隐蔽性。病毒还会通过网络共享将自己拷贝到共享了 Windows 目录的其它机器中(Windows 目录)文件名为 RundLL32.exe，原来的 RundLL32.exe 改名 Run32.exe。

该病毒最大的特点就是传播非常迅速，感染后 20 分钟搞定，然后从你的 outLook 里使劲发垃圾邮件给邮件列表中的地址。请大家小心防范。

OICQ 用户当心：专门盗取 QQ 密码的病毒爆发

一个专门盗取ＱＱ密码的病毒“TRoJan. OIcｑSｐY５”近日爆发。

据瑞星反病毒专家介绍，“TRoJan. OIcｑSｐY５”属于木马类病毒，主要感染 WIN９５／９８／2０００操作系统。其感染过程是：首先将自身复制到 Windows 目录下，然后修改注册表中的启动键值，使自身得到

运行，并驻留内存，监控本地电脑，从而盗取用户的OICQ密码，并将造成电脑的运行速度大大降低。

可以想象，这样的危害对“Q友”们无疑将是一枚重磅炸弹。QQ密码一旦被盗，诸多网上好友从此将杳无音信。在此，瑞星公司提醒广大网民，尽快升级您手中的杀毒软件，将“TRoJan．OIcqSpY5”病毒拒之门外。对于暂时无法升级或未安装杀毒软件的用户，也可通过删除该病毒文件进行防范。

由于“TRoJan．OIcqSpY5”病毒的发作时间不固定，请一定注意及时安装杀毒软件并开启实时监控。

当心“Red Code”红色代码

最近一段时期，“红色代码”病毒的变种“红色代码II”正肆虐全球。从8月1日起，该病毒的疫情开始蔓延到我国境内。这种集病毒、蠕虫、木马、黑客程序于一身的恶意代码，能够大面积地感染安装有微软视窗2000和NT的操作系统，取得系统的控制权，进而泄露系统中的文件并对网络中其他系统进行感染和攻击，导致网络通信和网络信息服务的拥塞甚至瘫痪。目前，该病毒已经给我国部分网络及其节点造成严重的破坏，并正在继续蔓延。

鉴于该病毒不仅使一些单个的计算机系统受到

损失，而且还威胁到网络通信和服务的正常运营，为遏制病毒疫情的扩散，救助遭受破坏的网络系统，形成各方面群策群力、协查联防的严密的安全保障体系，国家因特网应急小组协调办公室于 2001 年 8 月 10 日上午组织召开了“网络病毒紧急救助措施研讨会”。信息产业部电信管理局副局长韩夏、国家计算机网络与信息安全管理中心副主任方滨兴到会并作了重要指示。来自国家计算机网络应急协调中心、国家计算机病毒应急处理中心、国家计算机网络入侵防范中心和各大互联网运营单位、各主要防病毒厂商和我国首批网络安全服务企业试点单位的代表 50 余人参加了会议。

信息产业部电信管理局的韩夏副局长在讲话中指出，互联网在高速发展的同时，也暴露出缺乏安全保证和服务质量保证的弱点。虽有这样的缺陷，但是还是要发展。面对各种安全威胁，要积极想办法解决安全问题。国际上的做法是建立一些紧急救助的组织，我国也正在积极地开展这方面的工作。作为信息产业部，对整个电信网络的运营、质量监督和市场监管，具有管理的职责。这次病毒的问题涉及面很广，危害很大，不同以往。我们提出如下的要求：一、各大互联网运营单位对整个网络的安全负有很大的责

任。出了问题，一定要及时补救，一定要有保护用户利益的意识和及时采取必要的救助措施；二、根据国家信息化工作领导小组赋予信息产业部的职能，要对包括网络安全服务在内的网络服务类企业实行经营许可证制度。质量不高的、没有资质的服务商来做安全，会造成很多问题；三、我国公安部门负有打击犯罪的职能，遇到触犯刑律的案件，在开展救助工作的同时，要及时向公安部门报案。

国家计算机网络与信息安全管理中心方滨兴副主任在讲话中指出，我们这次会议的目的，是了解疫情，探讨紧急救助措施，建立相应的救助机制。虽然源头是病毒，但是表现出来的则是对网络产生直接的威胁。所以要把互联网的运营单位和刚刚选定的网络安全安服务试点单位一块请来，拿出办法来进行救助。不能让这样一种现象就这么继续下去。

会上，国家计算机病毒应急处理中心报告了红色代码 II 病毒的主要特点、危害、处理办法和截至 2001 年 8 月 9 号下午 5 点的病毒感染统计结果。此次病毒疫情涉及十几个省市，感染病毒的网络主要集中在信息行业、网站、教育科研机构和政府部门。各大互联网运营单位介绍了各自管辖的网络中感染病毒的状况。一些反病毒厂商介绍了最新的病毒查杀措施。国

家计算机网络应急处理协调中心提出了针对红色代码 II 病毒疫情建立群策群力、协查联防的严密的安全保障体系的建议，与会代表对建议进行了热烈的讨论。最后，达成如下共识：

（1） 尽快建立一个高效率的、负责任的、反应及时的信息通报机制，各应急处理机构、互联网运营机构、反病毒厂商、网络安全服务机构要就病毒攻击源、补救措施、病毒查杀措施等及时通报最新的进展，共享信息；

（2） 在此基础上形成一种群策群力、协查联防的工作机制，最大限度地遏制“红色代码 II ”病毒疫情的传播，并为今后网络病毒、网络攻击的联合防范作好组织上、技术上的准备；

（3） 国家计算机网络应急处理协调中心（CNCERT）负责协调信息通报和协查联防的具体工作。CNCERT 网站将会随时发布最新的动态和有关的链接，受理救助请求，网址是：http://www.ceRt.org.cn。

冠群金辰关于 codeRedII 的报告

代号红色 B（CodeRed B）,代号红色蠕虫的新变种,目前已经发现一种能够破坏 WINDOWS2000 服务器安全体系的新的代号红色（CodeRed）蠕虫变种.关于

原始代号红色（CodeRed）蠕虫的介绍,请访问网址 :http://sc.kILL.com.cn 同原版代号红色（CodeRed）蠕虫不同,新的蠕虫变种在 WINDOWS 系统中更改系统设置,修改 WINDOWS 文件并放置特洛伊木马程序,最终导致受感染系统后门大开,丧失安全策略.以下是关于代号红色（CodeRed）新变种的一些初步分析:

CodeRed B 仅在运行微软 IIS 的 WINDOWS2000 的系统中传播。入侵系统后,蠕虫将 CMD.EXE 拷贝到 C:盘及 D:盘以下目录中：\Inetpub\scRIpts\program files\common files\system\msadc 之后,蠕虫将开始扫描网络,寻找其它可被攻击的系统,这一过程在英文 WINDOWS2000 系统中将持续 24 小时,而在运行中文 WINDOWS2000 的系统中将持续 48 小时.接着,蠕虫程序在 C:盘和 D:盘的根目录下生成一个大小为 8,192 字节的 EXPLORER.EXE 木马程序,然后重启系统,执行木马程序.这个木马程序首先运行 WINDOWS 的 EXPLORER 程序,然后通过修改以下注册表键值使 WINDOWS 系统丧失对系统文件的保护能力 :HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\WinLogon\SFCDIsabLe=0xFFFFFF9D 这一设置的缺省值为 0。

之后,木马程序通过修改注册表以下键值创建两个虚拟 IIS 目录 C 和 D,分别映射到系统的 C:盘和 D:盘 .HKLM\SYSTEM\CuRRentContRoLSet\Services\W3SVC\PaRameteRs\VIRtuaL Roots 这些虚拟目录被赋予读写及可执行权限,这样木马程序通过 IIS 向所有黑客提供了对被感染服务器 C:盘和 D:盘的完全控制能力.在这之后,木马程序完成了它的感染周期,并会每各 10 分钟重复进行以上提到的注册表项修改.KILL26.50 版本增加了对木马程序的检测和实时监测,然而,如果您的系统在 KILL 升级之前已经被 CodeRed.B 蠕虫入侵,您将很难确定是否有黑客借助该蠕虫对系统进行了修改.清除:

1,红色代码一型 运行相应补丁程序（从微软公司网站获得） 重启机器

2，红色代码二型运行相应补丁程序（从微软公司网站获得）

删除 c:\expLoreR.exe 和 d:\expLoreR.exe(这两个为隐藏，只读文件）（改 KLM\SOFTWARE\Microsoft\WindowsNT\Current Version\WinLogon\SFCDIsabLe 键值为 0，把 HKLM\SYSTEM\CuRRentContRoLSet\Services\W3SVC\PaRameteRs\VIRtuaL Roots 对于 c:和 d:的完全控制

键值删除 \Inetpub\scRIpts 和 \program files\common files\system\msadc 如有 cmd.exe 删掉）其中括号内的东西不是每台机器都有重启计算机

警惕“罗密欧与朱丽叶”（BLebLa）病毒的新动向

国家计算机病毒应急处理中心提醒用户注意罗密欧与朱丽叶病毒，该病毒在 2000 年 12 月在波兰发现。但近日在我国发现该病毒活动较为频繁，有多个用户已经遭受此病毒的感染。

“罗密欧与朱丽叶”病毒是一个网络蠕虫，通过电子邮件进行传播。邮件包含一个超文本格式的文档和两个附件，附件的名称分别为 xRomeo.exe 和 xjuLIet.chm。当收到带毒信件时，如果使用 OutLook，当光标选中带毒信件时，他将被激活，此特点类似于“欢乐时光”病毒。它的 HTML 部分被执行，这部分包含一个能自动运行的脚本，由它来启动一个名为 xjuLIet.chm 的文件。最后由 CHM 运行真正的病毒实体 xRomeo.exe。并将以上两个文件作为附件，向被感染用户邮件地址簿的地址发送邮件。

病毒运行的时候，它将自身复制到 C:\Windows\sysRnj.exe，并在注册表中创建以下内容：

HKEY_CLASSES_ROOT\Rnjfile
\DefauLtIcon= %1
\sheLL\open\command = sysRnj.exe “%1” %

当“Rnjfile”被指定，上面提到的键值将运行这个蠕虫副本，接着修改下列键值：

HKEY_CLASSES_ROOT
\.exe = Rnjfile
\.jpg = Rnjfile
\.jpeg = Rnjfile
\.jpe = Rnjfile
\.bmp = Rnjfile
\.gIf = Rnjfile
\.avI = Rnjfile
\.mpg = Rnjfile
\.mpeg = Rnjfile
\.wmf = Rnjfile
\.wma = Rnjfile
\.wmv = Rnjfile
\.mp3 = Rnjfile
\.mp2 = Rnjfile
\.vqf = Rnjfile
\.doc = Rnjfile

\.xLs = Rnjfile
\.zIp = Rnjfile
\.RaR = Rnjfile
\.Lha = Rnjfile
\.aRj = Rnjfile
\.Reg = Rnjfile

上面列出的任何一个文件被打开都将使该蠕虫副本启动。

该蠕虫将自身发送到新闻组 aLt.comp.vIRus ，消息内容如下：

FRom: “Romeo&JuLIet”
Subject:[Romeo&JuLIet] R.I.P。

蠕虫病毒执行时，将读取用户邮件地址簿中的地址，并向这些地址发送邮件，邮件包含超文本格式的文档和两个附件。使用空的、随机产生的主题或是下面列出的任意一个主题：

Romeo&JuLIet
where Is my juLIet
where Is my Romeo
hI
Last wIsh
LoL :)

,,...`
!!!
newborn
meRRy chRIstmas!
suRpRIse !
CautIon: NEW VIRUS !
scandaL !
Re:

目前，国内、外防病毒产品都已经可以检测、清除该病毒。同时，我们建议用户可将 WSH 卸载，这样做会影响系统的部分功能，不过对一般用户没有影响。这样，可以防止“欢乐时光”、“爱虫”以及“主页”(Homepage)等 VBS 脚本语言病毒。有关 WSH 的卸载方法可参见：WSH 在 Windows 平台上的安装与卸载。

“欢乐时光”病毒的最新发展动态和处理方法

国家计算机病毒应急处理中心从 4 月 30 日至 5 月 8 日，已收到来自全国各地计算机用户的 300 多封电子邮件和 400 多个咨询、求救电话，我们都作了回复和处理。同时，中央电视台和多家报纸都发布了国家计算机病毒应急处理中心的病毒预警通知。在 5 月 8 日，我们收到一百多例遭受破坏的报告，低于我们的预期数量，对“欢乐时光”病毒的应急处理工作取

得阶段性成果。

但是，由于“欢乐时光”病毒的传染特点，它可以染.htm、.vbs、.asp、.html

后缀的文件。目前，我们已经发现个别网站遭受该病毒的感染。那么，访问这些网站的用户都会感染此病毒。我们已经通知了相关网站做好紧急处置工作。

目前江民公司、瑞星公司、金山公司、创源公司、熊猫公司、新趋公司、冠群金辰公司都有了解决方案，用户可下载他们的升级程序，及时查杀该病毒。同时，国家计算机病毒应急处理中心提醒广大计算机用户，可以将 Windows ScRIptIng Host 卸载，这样，可以阻止 VBS 脚本程序执行，从而，保证即使收到带毒邮件，也可以防止“欢乐时光”病毒传染、破坏。卸载方法如下：

Windows 98：控制面板－〉添加／删除程序－〉附件－〉Windows ScRIptIng Host,将 WSH 卸载，然后，再收发邮件。

从目前情况来看，遭受该病毒感染的网站数量有增长的趋势，这个渠道会导致病毒大量传播。所以，国家计算机病毒应急处理中心提醒各网站和网站维护人员，务必加强对“欢乐时光”病毒的预防工作，

保证自身的网站免遭病毒的感染，遏制病毒进一步扩散、传播。同时，广大计算机用户如果已遭受该病毒传染、破坏，首先及时升级杀毒软件，使用软盘引导系统，使用单机版杀毒软件将系统中残留的病毒彻底清除，然后重新安装系统和防病毒软件，并将病毒防治产品的实时监控功能打开，防止再次感染此病毒。国家计算机病毒应急处理中心正在密切监测“欢乐时光”病毒的发展动态，防止出现该病毒的变种，如果用户发现新的变种，请立即将病毒样本报送给国家计算机病毒应急处理中心。

5 月 8 日小心恶性病毒“欢乐时光”发作

国家计算机病毒应急处理中心 4 月 29 日接到北京用户的报告，发现一种通过电子邮件传播的新病毒，我们将其命名为“欢乐时光”(HappytIme)病毒。

“欢乐时光”属于 VBS/HTM 蠕虫类病毒，通过邮件传播，但不是作为邮件的附件，而是作为邮件内容。如果用户使用 OutLook，收到带毒邮件，当用户用鼠标指向带病毒的邮件时，不必打开信件，欢乐时光病毒将被激活，并生成如下文件：

c:heLp.htm

c:WindowsheLp.vbs

c:WindowsheLp.hta

c:WindowsNTITLED.HTM

然后传染硬盘中的.HTM、.VBS、.HTA、.ASP、.HTML后缀的文件。并修改注册表中部分键值：

1、在 HKEY_CURRENT_USERSOFTWARE 下新建 HELP 项，然后新建 COUNT 键值用于记录病毒感染的次数；新建 WALLPAPER 键值用于记录修改后的墙纸文件；

2、修改 HKEY_CURRENT_USERIDENTITIESXXXXXXXXSOFTWAREMICROSOFTOUTLOOKEXPRESS .OMAIL其中XXXXXXXX为缺省用户 ID值)下键值MESSAGE SEND HTML为1；COMPOSE USESTATIONERY 为 1；STATIONERY NAME 为 %WINDOWS%UNTITLED.HTM。

当用户安装了 VB，该病毒将会自动给地址薄中的邮件地址发信，邮件标题为“HELP”。但是，该病毒不能正确取到邮件地址，没有发件人，因而不能发送。如果收件箱中的有未读邮件，则病毒会自动回复这些信件。如果未安装 VB，则该病毒不会自动通过邮件传播。只有当染毒的用户在发送邮件时，该病毒会自动插入到邮件体中。当用户收到上述邮件后，如果使用 OUTLOOK，当光标条移到带毒邮件时，OUTLOOK 的预览功能将使病毒自动执行。

当染毒的计算机内的时间是日+月=13，该病毒将

逐步删除硬盘中的 EXE,DLL 文件，最后，导致系统瘫痪。

国家计算机病毒应急处理中心提醒广大计算机用户，可以将 WINDOWS SCRIPTING HOST 卸载，这样，可以阻止 VBS 脚本程序执行，从而，保证即使收到带毒邮件，也可以防止“欢乐时光”病毒传染、破坏。卸载方法如下：

WINDOWS 98:控制面板〉添加／删除程序〉附件〉WINDOWS SCRIPTING HOST,将 WSH 卸载，然后，再使用 OUTLOOK 接受邮件。

节后 5 月 8 日将是该病毒第一次发作的日子，国家计算机病毒应急处理中心提醒广大计算机用户，“欢乐时光”病毒不同于以往通过邮件附件传播的计算机病毒，具有极强的传播能力，必须严加防范。

注意 IWorm.Magistr 病毒的发展动态

国家计算机病毒应急处理中心通过监测 2001 年 3 月发现一种可通过互联网电子邮件进行传播，又可在本地机或局域网中快速感染 PE 格式的 IWorm.Magistr 恶性病毒。在 4 月 13 日接到北京江民公司报告在国内已发现该病毒的活动。

该病毒可通过互联网上电子邮件或在局域网内进行传播。可通过 OutLook、Netscape Messenger 等

其他电子邮件软件和新闻组在内的软件读取其中地址簿中的地址发送带毒电子邮件进行传播。

要注意的是，电子邮件的标题和正文都不是固定的，而是病毒在当前机上随机查找.DOC 和.TXT 文件中的一段文字作为邮件的标题和正文或不带正文。其附件也是不固定的，病毒随机在当前机上找一个.EXE 或.SCR 文件和一些.DOC 或.TXT 文件作为附件发出去，这很可能将重要的文件发给别人。

该病毒采用了多变形引擎和两组加密模块，病毒感染文件的中部和尾部，将中部的原文件部分代码加密后潜藏在病毒体内，病毒长为 2400030000 字节。病毒使用了非常复杂的感染机制，感染.EXE、.DLL、.OCX、.SCR、.CPL 等文件，病毒每传染一个目标，就变化一次，具有无穷次变化，其目的是使反病毒软件难以发现和清除。带毒文件和邮件被执行后，病毒驻留内存，伺机传染文件和网上传播。

病毒还修改注册表中 HKLM\Software\Microsoft\Windows\Current Version\Run（键值和键值名视被修改的文件名而定）。

病毒还修改 Win.Inl 中“Run=”一项（启动程序名视被修改的文件名而定）。

病毒对以上的修改，使 WINDOWS 每次启动的时候都会激活病毒，并感染其它文件。

如果机器联着局域网，病毒就会搜索局域网上的共享驱动器，如果是开放和授权可改写的驱动器，病毒便查找 WINDOWS/NT,WIN9X 目录，并感染这些目录中的文件，同时会像在本地机上修改注册表和 Win.Inl 中的“Run=”。

如果在 WIN9X 环境下，病毒乱写 BIOS 和清除硬盘上的数据，并显示以下信息：

Another haughty bLoodsuckeR.....。

YOU THINK YOU ARE GOD ,

BUT YOU ARE ONLY A CHUNK OF SHIT

该病毒有和 CIH、KRIZ4250 等病毒的破坏作用相类似，是危害性非常大的一种病毒。

该病毒的清除时须注意以下问题：

1）删除注册表中的键值：

HKLM\Software\Microsoft\Windows\Current Version\Run（键值和键值名视被修改的文件名而定）。

2）删除 Win.Inl 中“Run=”项后的文件名，（启动程序名视被修改的文件名而定）。

3）重新启动您的计算机；将 OUTLOOK EXPRESS

电子邮件中的相应的含有该病毒的邮件删除：

4）个别被病毒改坏的文件，请用别的机器相应的无毒文件将带毒文件覆盖掉。

请国内用户密切注意该病毒的活动，如发现或遭受该病毒的侵入，可与国家计算机病毒应急处理中心联系。

当心 W32.BadtRans.13312@mm 病毒

国家计算机病毒应急处理中心通过监测，在近期发现了病毒 W32.BadtRans.13312@mm，并于今日收到亚洲反病毒研究者协会（AVAR）关于该病毒的疫情通告，该病毒先期主要是在欧洲传播，现在韩国也已发现用户遭受该病毒的感染

根据目前掌握的情况，该病毒一旦执行，常驻内存的蠕虫就会显示一个对话框,内容如下，

File data corrupt:

bad disk access or bad data tRansmIssIon。

它还将拷贝自身存放在 Windows 目录下，名为 INETD.EXE，并修改注册表信息以便在系统再次启动时装载自身。

病毒一旦运行，该程序会将被感染者的 IP 地址发送给病毒的作者，病毒作者获得此信息后，就可以通过 Internet 连接到被感染的系统，并窃取被害者

的个人信息，如用户名和密码、信用卡和银行的账号及密码。

再次启动 Windows 后，蠕虫尝试回复 Microsoft OutLook 文件夹中的未读邮件，并将其自身作为附件，

邮件包含以下内容：

Take a Look to the attachment。

附件的名称可能是下列名称之一：

CaRd.pIf

docs.scR

fun.pIf

hamsteR.ZIP.scR

Humor.TXT.pIf

Images.pIf

New_NapsteR_SIte.DOC.scR

news_doc.scR

Me_nude.AVI.pIf

PIcs.ZIP.scR

README.TXT.pIf

s3msong.MP3.pIf

seaRchURL.scR

SETUP.pIf

Sorry_about_yesteRday.DOC.pIf

YOU_are_FAT!.TXT.pIf

希望广大用户提高警惕。如发现上述内容的不明电子邮件，请勿打开，可将该邮件转发给应急中心。

当心 4 月 13 日 计算机病毒

本月 13 日碰巧是星期五，已经有许多计算机病毒来势汹汹，预计在当天将有四、五种病毒发作。而且，防毒公司发现还出现许多新种病毒，一共大约有二三十种计算机病毒，提醒您要小心。

13 日当天如果打开计算机，发现系统变慢了，而且还出现许多奇奇怪怪的窗口，一会和您玩心算游戏，一会开启了二、三十个文件，那么您的计算机可能中了专挑在 13 日发作的病毒。

现在的计算机病毒中，不但有取名十三号星期五的病毒，每年 4 月 26 日才发作的 cIh 病毒也来势汹汹，一不小心中毒，计算机硬盘就全部被格式化，不过这些破坏力都比不上专门教人制作病毒的可怕 vbs 病毒。

13 日星期五病毒再加上 26 日发作的 CIH 病毒，算一算这个月一共有二、三十种病毒，提醒您如果确定要在 13 日或是 26 日开机，不妨先将电脑系统日期稍作调整，提前几日，最保险还是赶快更新病毒码，

免得一不小心计算机就中毒了。

第一个跨 Windows 和 Linux 平台的病毒 Winux 出现

美国反病毒软件开发商 CentRaL Command 公司当地时间 3 月 27 日(北京时间 3 月 28 日)发布消息称，该公司发现了一种既能感染 Windows 操作系统，也能感染 Linux 操作系统的新型病毒 W32.Winux。这是世界上首例具有双重感染能力的病毒。CentRaL Command 公司称，这种病毒的破坏力相对有限，到目前为止，该公司尚未发现被这种病毒破坏的计算机。

CentRaL Command 公司声称，W32.Winux 病毒是用汇编语言编写的，主要感染可执行程序，它在微软公司的 Windows 95，98，Me，NT 以及 2000 操作系统中都有传播的能力，不仅如此，它还能够感染使用各种版本 Linux 操作系统的计算机。当用户不经意之中双击感染了病毒的应用程序或者电子邮件附件时，W32.Winux 病毒就会被激活，该病毒会自动寻找 100K 以上的应用程序并将之感染，从而使病毒迅速扩散。CentRaL Command 公司称，他们是在一封来自捷克的匿名电子邮件中首次发现这个病毒的，它可能是一个名叫“本尼”的人编写的。本尼自称隶属于一个名为“29A”的病毒开发集团。

CentRaL Command 公司总裁兼首席执行官肯思皮尔(KeIth PeeR)表示，“在发现 W32.Winux 病毒之前，我们从未想到过存在这样的病毒。客观地说，这的确是病毒编写方面的一大进步。但对于计算机用户来说这显然不是什么好消息。W32.Winux 病毒的出现意味着 Windows 操作系统和 Linux 操作系统对病毒的相互封闭已被打破，以后反病毒的工作将会更加艰巨。”

瑞星公司 3 月 30 日已向国家计算机病毒应急处理中心报送了病毒样本，我们正在密切注视该病毒发展情况。用户如发现该病毒可与应急中心联系。

爱虫刚走，Kak 又来

此病毒同样是通过电子邮件的附件进行传播的。只要当用户打开或预览含有这一病毒的文件时，计算机系统就会遭到 Kak 病毒的袭击。Kak 病毒是在电脑运行 Internet ExpLoreR5.0 或 Microsoft Office2000 时，借助于 ActIveX 控制器中的 scRIptLet.typeLIb 程序，把其作为安全的突破口，而对电脑系统发起攻击的。

专家确定这种病毒起源于法国。由于 Kak 病毒不是被人恶意制造的，所以目前 Kak 病毒在某种程度上还未散播开来。然而一旦大面积蔓延，将造成比“爱虫”更大的破坏力。

电脑用户如果在电子邮件或浏览器的对话框中看到“你想运行 ActIveX 和插件程序吗？ ”的问题时，一定不要运行。

白雪公主(HybRIs)病毒

这是一只可以通过 EMAIL 接收的网络蠕虫，它只运行在 WIN32 系统下。蠕虫的代码中包含插件，这些插件是执行蠕虫所依靠的，并且可以从一个 Internet 网站上下载，很可能该站点就是病毒作者的站点。该蠕虫的主要版本采用了半多态加密技术。这种下载加密组件的方式与第一次使用该方法的 W95/BabyLonIa 病毒相似。蠕虫包含下列加密的文本串：HYBRIS(c) Vecna 。蠕虫的主要感染目标是 WSOCK32.DLL 动态链接库。在感染链接库的同时，它还将自身写入文件最后部分的结尾（附着了“connect ”,“Recv ”,“send ”功能）；修改动态链接库的入口地址并对原入口地址进行加密。如果蠕虫启动时不能感染 WSOCK32.DLL（一旦该文件正被使用或被进行写锁定），该蠕虫将创建 WSOCK32.DLL 的副本（该文件的文件名由 8 个随机字母组成）感染它并将“Rename ”指令写入 WININIT.INI 文件中。那么 WSOCK32.DLL 将在系统下次启动时被替换。

蠕虫同样在 Windows system 目录下以随机文件

名创建其自身的副本，并在注册表中添加下列注册键：

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\Run Once

{DefauLt} = %WinSystem%\WormName

或

HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\Run Once

{DefauLt} = %WinSystem%\WormName

其中“WormName”是随机文件名,例如:

CCMBOIFM.EXE

LPHBNGAE.EXE

LFPCMOIF.EXE

当蠕虫处于激活状态时,它将截获 Windows 用于建立网络连接的函数，包括 Internet 连接。蠕虫截获发送和接收的数据并扫描其 EMail 地址，一旦地址被检查到，蠕虫将等待一段时间然后将一个染毒的消息（扩展名为.EXE 或 .SCR）发送给这些地址。当 HybRIs 被启动后,它将从站点服务器上下载一个名为 INDEX.TXT 的文本文件，其中包含了蠕虫下载的其他有用的文件列表。

11 月 13 日那个站点依旧运作并且包含下列升级

组件文件：

HTTP.DAT； NEWS.DAT； ENCR.DAT； PRON.DAT； SPIRALE.DAT； SUB7.DAT； DOSEXE.DAT； AVINET.DAT；

11 月 20 日包含病毒的站点被卸载。但病毒继续从新闻组 aLt.comp.vIRus 上下载插件。

11 月 21 日一个新的插件发布，它将使 W32/HybRIs 以一种不可修复的方式感染 PE 文件。

这个网络蠕虫向一个叫 aLt.comp.vIRus 的新闻组发送病毒升级的细节。这个消息是一个通讯信息，能够使主机上运行的蠕虫自动升级。

第二节 计算机犯罪

计算机犯罪的概念

计算机犯罪（ComputercRIme)一词从被人们提出来到现在已经有许多年了，并且得以广泛使用，频繁见诸于报端。但是计算机犯罪究竟是什么？理论界至今仍然众说纷纭、各有其理，计算机犯罪的内涵仍然模糊不清。虽然在我国新修订的刑法第 285 条、286 条、287 条当中对计算机犯罪作了法律上的规定，但是仍然没有解决计算机犯罪定义的问题。

计算机犯罪作为一类特殊的犯罪，具有其它犯罪所不具有的特点，因此必须对之进行研究，而研究的首要问题就是要解决其概念问题。只有在明确了其内

涵之后，我们才能进行深入的研究。目前理论界对计算机犯罪的定义虽然有诸多讨论，但在论述过程中往往忽视了一个最基本的问题，到底什么是计算机？在大家看来，计算机似乎是一个很普通的概念，不需要进行特殊的说明。然而事实上对计算机的定义可以有很多种，因此在讨论计算机犯罪之前我们有必要首先解决计算机概念的问题。

从计算机科学的角度我们可以看到，所谓计算机，就是能够按照人们预先编制的程序对信息进行处理的机器，这也就是指计算机硬件。因此，主板、CPU、内存三者组成的主机就是基本的计算机，主机加上外部设备也是计算机，甚至连单独的 CPU 也应该被视为计算机，因为它们都符合计算机的定义。那么在法律上计算机的概念究竟应该是什么呢？

单纯的计算机硬件在法律上具有的主要是财物的性质，因此以硬件意义上的计算机为对象的犯罪行为大多可以归入普通的财产犯罪中去，没有必要单独研究之。现代社会中所说的计算机，事实上指的是“计算机系统（Computersystem）”。所谓计算机系统是指由计算机硬件与软件紧密结合在一起而构成的系统，这样的系统能够实现一定的自动信息处理功能，为普通使用者提供一定的服务。在这样的系统中，软件的

价值和重要性与硬件相同，甚至远远超过硬件。这种系统同普通机械装置有了本质上的区别，它具有一定的智能性，这些特征是普通的财物所不具有的。

虽然计算机硬件中也有一些软件成份，例如人们往往在 ROM 中固化的引导程序等等，但这些程序都是为了实现硬件的基本功能而设计的，可以说是硬件的附属，没有它们硬件就不能相互配合甚至不能发挥作用，因此我们也将它们看作计算机硬件的组成部分。一台主机与相应的外部设备以及在它们上面运行的软件就构成了一个基本的计算机系统；多个单机系统以一定的方式联结就构成了一个大的系统，我们一般将其称为局域网，局域网中还包含了网络控制软件等等系统软件；若干局域网联结在一起就构成了更大的网络系统，例如现在最大的国际网络 Internet 上面联结得有无数的局域网和个人计算机。所有这些我们都称之为计算机系统。正如计算机工业界的名言“网络就是计算机”所蕴含的意义那样，所有的计算机系统我们都在法律上称为计算机，关键的一点在于计算机系统必须是硬件和软件紧密有机的结合，二者缺一不可。

由此，我们在法律上对计算机作如下定义：计算机是由计算机硬件和计算机软件按照一定方式联系

和结合而构成的，具有按照指令处理或者是自动处理信息的装置系统。计算机包括单机系统和网络系统。

针对和利用计算机系统进行的犯罪具有许多传统犯罪所不具备的特征，如隐秘性强、破坏性大、技术含量高等等，传统的犯罪理论对之缺乏完善的描述与研究，因此必须单独对其进行研究。有关计算机的犯罪一般是采用窃取、篡改、破坏、销毁计算机系统内部的程序、数据和信息从而实现犯罪目的，因此这类犯罪事实上是信息犯罪。

据以上讨论，笔者认为，所谓计算机犯罪是指针对和利用计算机系统，通过非法操作或者以其他手段对计算机系统的完整性或正常运行造成危害后果的行为。计算机犯罪的犯罪对象是计算机系统内部的数据，所谓数据包括计算机程序、文本资料、运算数据、图形表格等等在计算机内部的信息（以下我们均在这种意义上使用“数据”一词）。这种犯罪在主观上不一定表现为谋取利益，客观上的表现是非法使用计算机系统。

所谓非法操作，是指一切没有按照操作规程或是超越授权范围而对计算机系统进行的操作。非法操作是对计算机系统造成损害的直接原因，可以说没有非法操作就没有计算机犯罪。我们还需要将法律上规定

的非法操作同计算机科学上的非法操作区分开来，计算机学中将一切错误的指令均视为非法操作，对这种操作计算机一般会给出错误信息，提醒使用者操作错误，这种意义上的非法操作含义非常广，只要是计算机系统不接受的操作都是非法操作。而我们在法律上所说的非法操作主要是指未经授权的操作，例如使用者可以通过某些手段使计算机系统错误地认为其操作是合法的并且接受和运行这些指令，再如使用者可以利用计算机系统设计上的某些缺陷来超越权限地接触一些数据或者修改它们，这样的操作都是计算机认为合法但在事实上是超越了使用权限的。这种操作在法律上的特征就是越权使用。在法律上我们不把哪些仅仅由于拼写错误而不被计算机所接受的指令认为是非法操作。

计算机犯罪中包括针对系统的犯罪和针对系统处理的数据的犯罪两种，前者前者是对计算机硬件和系统软件组成的系统进行破坏的行为，后者是对计算机系统处理和储存的信息进行破坏。由以上定义我们可以看到计算机犯罪在法律上具有以下特点：

1.计算机犯罪具有社会危害性。同所有的犯罪一样，正是因为计算机犯罪的行为具有社会危害性，我们才在刑法中规定其为犯罪，并且对其采取刑事制

裁，没有社会危害性的行为绝对不是犯罪。虽然计算机犯罪人在主观上不一定是为了谋取利益，但是所有的计算机犯罪在客观上都会造成社会或者社会的损失。例如非法侵入计算机系统，虽然在表面上看犯罪者不一定获得什么利益，被侵入的计算机系统也不一定会发生什么变化，似乎这种行为没有什么危害，但是在事实上对计算机系统成功的侵入势必使得整个计算机系统的安全系统要重新构置，耗费的人力物力甚大，同时计算机系统所有者对资料的安全性在心理和物质上的损失也不小。

2.计算机犯罪具有非法性。这种非法性体现在：首先计算机犯罪是法律所不允许行为，这种行为的后果是法律所禁止的，计算机犯罪的后果直接触犯法律；其次计算机犯罪必然是犯罪者超越了由法律或是权利人所授予的权利范围，也就是说计算机犯罪的本身表现为越权操作。

3.计算机犯罪具有广泛性。这种犯罪是一类特殊的犯罪形态，其中包含有许多具体的罪名，有学者曾经说过，“除了强奸罪，计算机可以犯一切罪”。当然犯罪的只能是人而不是计算机，但是由此可见计算机犯罪的复杂性，事实上，除了有关人身的一些犯罪，一般的犯罪都可以通过计算机犯罪来完成。

4.计算机犯罪具有明确性。虽然计算机犯罪的范围很广，但是其内涵十分明确，即它一定是对计算机系统内部的数据进行未经许可的处理并且造成社会危害后果的行为。并非一切有关普通意义上的犯罪都是计算机犯罪，例如盗窃或者毁损一台没有任何软件和资料的计算机的行为，在性质上和普通的盗窃或者毁损财物犯罪并无二致，这种行为不属于计算机犯罪。

在1997年3月15日全国人民代表大会通过的《中华人民共和国刑法》的第285条、286条、287条中对计算机犯罪进行了如下规定。“第二百八十五条违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。”“第二百八十六条违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行，后果严重的，处五年以下有期徒刑或者拘役；后果特别严重的，处五年以上有期徒刑。违反国家规定，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作，后果严重的，依照前款的规定处罚。故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的，依照第一款的规定处罚。”

“第二百八十七条利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密或者其他犯罪的，依照本法有关规定定罪处罚。”从《刑法》的规定我们可以看到，我国刑法对计算机犯罪采取了概括列举的方式。从这三款的条文来看，刑法主要是将那些以计算机系统作为犯罪对象的行为划入了计算机犯罪中，而以计算机为工具的犯罪则按其他犯罪进行处罚。刑法的规定和我们对计算机犯罪的定义基本是一致的，刑法也强调是针对计算机信息系统的犯罪才是计算机犯罪，至于涉及其他罪名的计算机犯罪则按刑法理论中的一罪和数罪的理论来规定。总的来说，计算机犯罪就是信息犯罪，是针对计算机系统内部信息而进行的犯罪。把握这一点，我们就能准确地研究计算机犯罪。

计算机犯罪成本分析

计算机犯罪是指行为人以计算机作为工具或以计算机资产作为攻击对象实施的严重危害社会的行为。所以计算机犯罪包括利用计算机实施的犯罪行为和把计算机资产作为攻击对象的犯罪行为。近年来计算机犯罪已成为一个严重的社会问题，因此如何预防和降低计算机犯罪迫在眉睫。本文用经济学中有关成本理论知识来探讨计算机犯罪的有关问题，提出

一些对策。

一、计算机犯罪成本和收益概念的届定

计算机犯罪成本是指行为人因利用计算机或以计算机资产作为攻击对象而实施的严重危害社会的行为所承受的精神性、物质性代价，是一种成本支出。计算机成本由直接成本（包括心理成本和经济成本）和间接成本（包含法律成本和竞争成本）组成。

心理成本是行为人实施犯罪行为受社会道德谴责和可能受法律惩罚的恐惧所导致的心理压力，经济成本是实施犯罪行为造成的经济损失。

间接成本也称制约成本，是指在外界因素作用下行为人对其犯罪行为需要付出的代价。如犯罪行为被发现后由于各种惩罚所造成的人身自由、名誉及权力、经济上的现实损失以及为达到犯罪的目的而与其它罪犯之间竞争的投入。法律成本是指计算机犯罪行为可能被司法机关或其它具有同等功能的机关抓获概率的产物，具有惩罚性和不确定性，如果犯罪行为没有被发现，则该成本为零；反之，则有一个法定惩罚成本。竞争约束力构成竞争成本（本文对此不予讨论）。

一般认为，侦破率的高低和法定惩罚力度的强弱对间接成本产生重大影响。计算机犯罪收益是指行为

人通过实施犯罪行为后谋取的利益，也可以说是计算机犯罪成本投入之后的产出除去成本之后，行为人所得到的利益。当然，这种收益绝非仅指经济上的利益，还包括对财物占有欲望的满足，感官上的愉悦和精神享受也是犯罪预期收益的重要内容。当行为人经过分析发现有利可图时，便会决策实施犯罪行为，且其实施的坚决程度也取决于收益的大小，预期收益越大，态度越坚决。反之，预期收益很小甚至没有，行为人就会觉得投入成本不值得而放弃行为。

需要说明的是上述“成本”与“收益”都具有不确定性。尽管如此，从理论上分析，可以得出这样的结论：计算机犯罪成本越高，计算机犯罪的预期收益就越小，继而计算机犯罪现象也就减少。

二、计算机犯罪成本现状分析

（一）直接成本不高。

1.心理成本不高。

因需要破译密码和进网程序，计算机犯罪筹划阶段一般较长，但一旦进入系统执行一项犯罪指令则只需用秒或微秒来计算。所以计算机犯罪作案时间的短促性使罪犯在作案时自我谴责和“现场”心理恐惧感大大降低。

目前许多国家将计算机犯罪的主观要件定为直

接故意和间接故意，即行为人在明知其行为是非法或会破坏计算机信息系统的情况下，故意实施侵入或破坏系统的行为和行为人对计算机系统的性能不了解，但仍然进行违规操作，导致计算机信息系统被破坏。

但该要件与计算机罪犯的伦理（尤其是“黑客伦理”）相去甚远。如美国康奈尔（CorneLL）大学的研究生莫里斯（RobbeRt T。MorRIs，JR.）通过美国最大的计算机网络系统，把自己设计的病毒程序输入五角大楼远景规划网络，结果导致美国军事基地和国家航天航空局的 6000 多台电脑全部瘫痪，给美国造成直接经济损失近一亿美元。这就是轰动中外的“Internet 网络事件”。之后，几乎所有的报道认为 MorRIs 编写蠕虫程序并非出于故意，而且 MorRIs 被推上被告席后也不认为或不知道自己行为是犯罪。大多数黑客认为对计算机网络的访问是无限制的，完全的，只要动机纯洁，就有权闯入任何网络。所以他们即使在非法入侵计算机系统、破坏计算机安全后仍坚持认为是为了更好地完善系统，非但无罪，反而有功。可见持“黑客网络伦理”的行为者将犯罪的心理成本几乎置于零。

2．经济成本很少。

计算机犯罪与传统手段的犯罪相比所冒的风险

小而获益大，作案者只要轻轻按几下键盘，就可以使被害对象遭受巨大损失，而使罪犯获得巨大利益或对计算机系统入侵的刺激和挑战给他的心里带来极大的满足。他们中有的在网络上制作、传播破坏性程序；有的涂改计算机结算单，删除计算机数据库中储户姓名、金额、伪造存户底卡、冒领存款；有的对计算机数据库结算尾数进行修改，将余出的息数加在自己和亲属的账户内提出；有的窃取大公司的商业秘密或渗入军方的绝密计算机网络系统等等。更为值得重视的是，网络的负面影响令人担忧的还在于其对“关键性基础设施”的威胁，一旦出现问题，不仅是经济损失，而且会给地区或国家安全带来巨大的、毁灭性的影响。而要达到这些目的只是举手之劳。经济成本少而又少。

（二）间接成本低下。计算机犯罪行为如不被发现，其制约成本就等于零。究其原因主要有：

1．发现概率太低。正是由于计算机犯罪的作案不受时间、地点的限制，犯罪行为实施终了后对机器硬件的信息载体可以不造成任何损坏，甚至不留下任何痕迹，所以犯罪行为不易被发现、识别和侦破，犯罪成功率极高。据统计，在号称“网络王国”的美国，计算机犯罪的破案率还不到 10%，其中定罪的则不到

3%。就新闻报道方面，计算机犯罪只有 11%被报道，其中仅 1%的罪犯被侦察过，而高达 85%以上的犯罪根本就没有发现。发现概率低是由计算机犯罪的特性所决定的。

（1）计算机犯罪的隐蔽性。首先计算机犯罪案件侦破难。计算机犯罪的实施主要通过程序和数据等各种无形信息的操作来进行，而且可以从任何一个计算机网络终端实施计算机犯罪行为，难以觉察。

其次搜集证据难。“计算机空间没有指纹”，因为犯罪的本身经常是虚拟的，有时候会留下纪录，但更多时间无迹可寻，它只是发生在电脑的空间，唯一的证据便是那转瞬即逝的电子脉冲。更何况，现场的计算机系统内所存储的有关证据方面的数据很容易被破坏。如盲目移动、开、关计算机系统设备而导致计算机内存储存的数据丢失或系统程序被破坏；作案者自行在计算机系统中设置的“陷阱”，防止其它人操作电脑访问自己的系统，一旦发生异常情况，系统将自行销毁数据或已运行的文件；作案者自行在自己的计算机系统设备的某些部位安装自动引燃、引爆装置或电源短路装置，若有意外，便可瞬间引发等等。

再次受害者不愿报案。许多计算机犯罪往往涉及公民的隐私、企业的秘密乃至商业的信誉，特别是法

律难以弥补计算机犯罪造成的损失，加上执法机关破案率低，使许多受害者愿意自行处理，极少公开报案。因此，司法机关没有发现没有统计的犯罪数字即犯罪黑数也极为巨大和惊人。

（2）计算机犯罪的技术性。如今使用一台最普通的计算机，从世界任何一个角落，就有可能破坏别国战船或卫星，修改他人银行账号，享受各种免费服务等等。

罪犯分子往往只需一台计算机、一条电话线、一个调制解调器就能为所欲为，而现有的科技手段却往往难以破解有些计算机犯罪分子的伎俩。计算机安全技术受制于人类社会科学技术发展的整体水平，而我们目前所采用的各项措施，只能是相对的、临时性的“补救”，还无法从根本上来解决。万无一失的安全系统是永远无法研制出来的，即便是研制出来的完全可靠的安全系统，它大概会干扰网络的信息共享自由－而这是对大多数网络用户来说是不可接受的。

2．安全意识和监督力度不够。计算机网络中存在的安全漏洞使计算机犯罪活动猖獗的原因之一。世界上许多网络用户认为计算机使用方便比安全更加重要。结果他们的许多人把计算机操作系统软件上的安全措施置于零。面对计算机罪犯的疯狂入侵，许多

人希望能加强安全措施，而做到计算机的绝对安全几乎是不可能的。即使安全的措施推广，许多人也会以阻碍信息自由而拒绝使用。以我国为例。据调查，在我国电脑应用单位 80%未设立相应的安全管理组织，58%无严格的调存管理制度，59%无应急措施，48%无事故发生后的系统恢复方案，可见安全意识是何等的弱。同时，公众对计算机犯罪也是十分的大度和宽容。因为计算机犯罪没有直接的人员伤害，损失的大都是政府和公司的财产，而且会有人认为这不是犯罪，而是安全系统的工作没做好。而且计算机罪犯基本上都是些计算机技术和知识方面的天才，惩治不能太过分了。应该说这些都或多或少地助长了计算机罪犯的嚣张气焰。

3．法律成本太低。

JamesA。SchweltzeR 在他的《计算机犯罪和商业信息》中指出："计算机犯罪本身就是法律不力造成的恶果"。法律成本的低下首先表现为各国立法参差不齐，罪犯能熟练地规避法律。比如对网络上色情文化的传播的处罚。1996 年 2 月 8 日美国颁布《通信行为准则法案》（CommunIcatIon Decency Act），该法案规定："企图干扰、诋毁、威胁或刁难别人的淫秽、淫荡、猥亵、肮脏或下流的网络通信"为犯罪，任何

人故意向 18 岁以下的未成年人散布网络色情资料即处以 10 万美元的罚款及 2 年有期徒刑。

但该法案一出台，美国联邦法院就以“政府想以此对传统印刷品或广播严厉控制的方式来规范网络内容而违背了美国宪法第一修正案有关言论自由的规定”为理由，于 1997 年 6 月裁决该法案无效。1998 年10月，美国国会通过了《儿童网络保护法案》(ChILd Online PRotectIon Act)，但该法案已被言论自由基金会联合 17 名原告起诉，称它的出台是政府再次企图限制网络言论自由，目前正由费城地方法院审理中。各国立法也是“百家争鸣”。某行为在一个国家属触犯刑法之列，而在另一个国家却与法无缘，最多只是对罪犯进行舆论上的谴责的现象很多。

比如在澳大利亚的刑法典上尚不存在“盗窃数据”的罪名，澳大利亚的新南威尔斯州连计算机滥用的法案也没有。由于各国立法的不一致性导致了计算机罪犯利用各国不同的法律规定来逃避法律的制裁。

其次从现有的法律和相关的案例来看，法定惩罚成本不高，对计算机罪犯的惩罚有些法不责众。集中体现为财产刑很低，生命刑、自由刑偏轻，资格刑几乎没有。如美国《康涅狄克州计算机犯罪法（草案，1983）》规定：“破坏程度、财产或服务损失超 1 万美

元者，属计算机犯罪一级罪。破坏程度、财产或服务损失超 5 千美元者，属计算机犯罪二级罪。破坏程度、财产或服务损失超 1 万美元者，或粗心地参与了使他人受到严重伤害的危险行为者，属计算机犯罪三级罪。破坏程度、财产或服务损失超 5 百美元者，属计算机犯罪四级罪”等等。而我国刑法有关于计算机犯罪的一些规定，重点突出了计算机信息系统的保护，但没有体现出对计算机资产的巨大价值的认识，所以有些计算机犯罪无法给与相应的惩治。从目前我国制定《中国计算机信息系统安全保护条例》、《中国公用计算机互联网国际联网管理办法》、《计算机信息网络国际联网出入口信道管理办法》、《计算机信息网络国际联网安全保护管理办法》等条例来看，对计算机犯罪的惩治很轻。如《中华人民共和国计算机信息系统安全保护条例》23 条规定：“故意输入计算机病毒以及其它有害数据危害计算机信息系统安全的，或者未经允许出售计算机信息系统安全专用产品的，由公安机关处以警告或者对个人处以 5000 元以下的罚款、对单位处以 15000 元以下的罚款；有违法所得的，除予以没收外，可以处以违法所得 1 至 3 倍的罚款”。相关的案例也很多：制造“Internet 网络事件”的 RobbeRt T。MorRIs，JR.给美国造成直接经济损失近

一亿美元。而 1990 年 1 月 22 日联邦法院判他处 5 年监禁和 25 万美元的罚款。《洛杉矶每日新闻》称“可以在 10 分钟内颠覆全世界”的头号黑客米特尼克在 1989 年被判处 1 年的有期徒刑；臭名昭著的黑客组织“诈骗高手小组”的创建者之一、计算机黑客约翰·李承认：虽然坐牢“一点都不好玩”，但他肯定不能抵制再干一次的诱惑。法律成本的低廉使许多罪犯在巨大且轻松易得的利润面前铤而走险。

三、一些对策

1．依法严厉打击的计算机犯罪行为。对违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的犯罪行为和故意破坏计算机信息系统的犯罪和利用计算机实施的金融诈骗、盗窃、贪污、挪用公款等方面的犯罪严厉打击。面对形形色色的计算机犯罪，我国应进一步规范信息安全、信息保护等方面的法律、法规。全面制定信息安全法、计算机安全法、数据保护法、信息犯罪法、网上知识产权法以及保护网民的个人隐私等立法。对于造成国家和社会重大损失的罪犯要从严、从快、从重、从速处罚。真正形成“法网恢恢，疏而不漏”的良好运行机制。

2．加强对网民集体主义教育。

在网络社会中应多倡导集体主义价值观。首先加强对内部人员集体观的培养。计算机犯罪属于智能型犯罪，实施这种犯罪的人，必须具有一定计算机专业知识，或从事计算机系统的操作、管理、维护工作的人员及其它人员，计算机罪犯中许多罪犯是内部人员，所以对职员的集体主义教育十分重要。其次用集体观代替个人主义。网络源于西方，西方文化中的个人主义价值观赋予网络开放的自由的特性，个人至上、绝对自由是网络运行机制的集中体现。而恰恰是网络世界的绝对自由导致了计算机犯罪愈演愈烈之势，尤其是非法入侵计算机信息系统罪。因此必须在网络世界中形成一种新的文化理念，即中华文化倡导的集体主义理念，为了保障公众和国家的信息利益与安全，有限制地牺牲一些个人信息自由。

3．加快全球统一立法进程。对开放的、全球的计算机犯罪的惩治要求我们尽快形成全球的、统一的法律体系。笔者认为在构建全球性法律体系时应具有以下几个特征：

（1）开放性。即应当全面体现和把握计算机网络的基本特点和法律问题，对于目前尚无法确定的问题应尽可能在宏观上加以规范；

（2）权利和义务的对等性。在计算机网络中表

现为每一个网络用户享有权力的同时必须承担社会赋予的责任，如有义务为网络提供有价值的信息或通过网络帮助他人或遵守各种网络的规范，维护网络的道德等；

（3）可操作性。制定网络法规都要视立法环境、条件成熟程度来确定轻重缓急，加强科学性论证。从维护网络资源及其被合理使用，维护信息正常流通，维护网络用户正当权益出发，制订出便于当事人的起诉，便于司法机关办案的科学的法律体系。

（4）自由性原则。网络时代突出的表现在于资源的共享性和信息的自由性。网民有根据自己的意愿选择自己的生活方式，享有表达自己意见和观点的自由，任何组织和个人都不能擅自干预和非法压制。

（5）国家利益和国际合作相结合。即网络立法应充分考虑国家、民族和国际化、全球化利益相结合。一方面，网络立法要从自身的实际出发，结合自身的国情制定出切实可行的法律法规，坚决维护国家主权和民族文化传统，绝不可盲目照搬照抄他国法律；另一方面，网络的开放型和全球性打破了地域和民族界限，全世界由此连成了“地球村”和“网络共同体”。计算机犯罪的跨国性要求各国立法注意与国际接轨和联合，若得不到罪犯所在地或犯罪行为地或结果发

生地国家的同情和支持，惩治罪犯只能是一句空话。对于网络管理和计算机犯罪的惩治，目前较为流行的办法是“有赖于政府更多的介入：建立一个某种意义上的世界政府。全世界的国家和这些国家的人民首先就一些基本原则达成一致，然后世界政府着手制定一系列法律并敦促公民执行这些法律。通过这样的办法，世界政府可以对所有这些问题进行公平而有效的处理。

”由于美国仍然控制着全球一半以上的 Internet 通讯流量，支持者一半以上的 Internet 服务器，并且一半以上的 Internet 用户是美国公民，所以埃瑟·戴森提出网络管理上的另一个选择途径——遵守美国的法律，如遵守美国白宫提出的“全球电子商业框架”（FRamework for GLobaL ELectRonIc CommeRce）。对此埃瑟·戴森指出：“未来的挑战在于怎样把分权的做法同美国的法律和文化区分开来。分权的做法是要避免任何国家，甚至美国，控制 Internet。”而“世界政府将通过各国政府和私人机构之间的一系列多边协议建立起来，而不是一个中央权威的保留地。”

总之，网络立法是一件十分慎重的事情。严格遵循网络立法的各种特性和原则，建立合理、有效的网

络法规，对网络合理有序地发展极为重要。

计算机犯罪初探

随着社会、经济及计算机应用技术的高速发展，计算机的应用已普及到现代社会的各行各业，以计算机为技术支持的信息产业已成为现代社会的三大支柱产业之一，然而，正如汽车的发明在拓展人类生活空间的同时也带来诸如废气、噪音、交通事故等社会问题一样，计算机技术在给人类社会带来巨大进步的同时，也使一些新型违法犯罪活动和新的社会问题随之产生，并日趋严重。

在我国，随着军事、安全、经济、银行、电力、气象和民航等全国性信息系统的逐步建成，整个社会对计算机信息系统的依赖性越来越大，计算机犯罪对社会造成的危害也日趋严重。自 1986 年发现第一起计算机犯罪以来，几年来计算机犯罪趋势正逐年迅速递增，在我国已发现的计算机犯罪案件中，损失金额小的数千元，大的已超过千万元。如我区桂林市某储蓄所一起计算机犯罪案件涉及金额即高达二千一百五十万元。

计算机犯罪损失如此巨大，是多方面原因造成的，其主要原因有以下几个方面：

一 随着全社会对计算机应用技术的普及和社会

信息化，计算机信息系统逐步成为整个国家政府机构运转的命脉和社会活动的支柱，强烈地吸引着犯罪分子和敌对势力的注意力。

二 由于计算机信息系统本身存在的脆弱性，极易被犯罪分子攻击。计算机系统的脆弱性是由其逻辑结构的简单性，硬件体系的易损性和软件程序的易变性等几个方面决定的。

三 计算机安全技术远远落后于计算机应用技术的发展水平，自 1946 年人类研制出第一台数字式计算机以来，计算机应用技术日新月异；而对计算机安全技术的研究，是在七十年代中后期，由于出现了较严重的计算机犯罪和其它安全问题，才有少数国家的部分专家开始进行对计算机犯罪和安全技术的研究。

四 计算机同时具备阻止与促进犯罪的双重因素。由于计算机系统具备高技术特性，行为人必须洞察、熟悉计算机系统的特点，才能加以滥用，加以破坏，才能从事计算机犯罪。所以计算机系统本身无疑是一种阻止犯罪的因素。但是，对于熟悉计算机技术特别是洞悉本部门计算机系统各种功能的人来说，他会感到如果他做些手脚，别人不会发现，不干白不干。

所以就计算机本身的脆弱性来说无疑是一种促进犯罪的因素。在其它犯罪领域中很少有这种兼具

正、反两个因素的现象。

目前，在计算机领域发生的犯罪，大多数是针对金融、电子商业系统和 Internet(国际互连网络)。由于大多数银行业务都实现了电子化,用电脑处理的往来业务数额大大超过了支票和现金量，其业务往来大都是通过内部电脑网络完成的，所以了解内情、可自由使用电脑而又心怀不轨职员将对企业构成严重威胁。而随着信息化社会的到来，将来几乎所有的商业活动都将实现电子网络化，它的一个重要内容就是要在公众网络上实现“电脑现金”，所谓“电脑现金”就是把现金变为数字信号，在电脑网络上使用数字信号代替资金的传送。然而，由于无现金社会的逐步形成及进入电脑网络费用急剧下降，导致能够进入电脑网络的人大幅增加，在电脑网络里进行犯罪的机会也逐步增加。

作为许多专门业务技术支持的公众网络，国际互连网创造了一个特殊的、虚拟的空间，它消除了国境线的限制，也打破了社会和空间界限，它将从根本上改变了工作岗位、家庭、地区以及社会的面貌。在这个虚拟的空间，人与人的关系转变成了一种数字信号的联系。从这个意义而言，在国际互连网上的诈骗、攻击变得异乎容易。而许多具有反政府 反社会、反

文化传统意识的人，在掌握了娴熟的计算机技术之后，很自然地会把攻击目标对准国际互联网。而以计算机技术为支持的其它各种犯罪，如非法操纵、计算机间谍、传播黄色、淫秽、反动信息等等。莫不随着计算机技术的发展而日益猖獗。

面对来自电脑世界的挑战，我们仅仅依靠教育防范是远远不够的，对于一切犯罪行为来说，道德的约束犹如院子外的篱笆，大风刮来，吹倒篱笆，不良行为便会长驱直入；只有法律的威慑才会象悬在人们头上的利剑，对企图以身试法的人来说，利剑随时都有可能落下。

因此，针对电脑领域目前的严峻形势，于 97 年 10 月 1 日正式实施的新刑法，增添了有关惩治计算机犯罪的条款，明确了计算机犯罪的范畴和处罚的措施，为有效地打击计算机犯罪行为提供了法律依据。

第十篇　　预防计算机犯罪篇

关于涉及计算机及网络的法律法规

根据法律出版社 1999 年 1 月出版的《计算机及网络法律法规》一书统计，1991 年至 1999 年 1 月间，我国颁布有关的法律法规 23 个，涉及计算机软件保护及著作权登记、计算机信息系统安全保护、计算机信息网络国际联网管理，计算机工程、电信设备进网

管理、中国互联网络域名注册管理、中国公众多媒体通信管理、计算机信息系统保密、软件产品管理、金融机构计算机信息系统安全等诸多方面。

其中和公民个人有较直接关系的法律法规有：

L 计算机软件保护条例（199 年 6 月 4 日国务院发布）。

2 中华人民共和国计算机信息系统安全保护条例（199 年 2 月 8 日国务院发布）。

3 中华人民共和国计算机信息网络国际联网管理暂行规定（1996 年 2 月 1 日国务院发布，根据 1997 年 5 月 20 日《国务院关于修改《中华人民共和国计算机信息网络国际联网管理暂行规定》的决定》修正）。

4 中国公用计算机互联网国际联网管理规定（1996 年 4 月 9 日邮电部发布）。

5 计算机信息网络国际联网安全保护管理办法（1997 年 12 月 16 日公安部发布）。

6 中华人民共和国计算机信息网络国际联网管理暂行规定实施办法（1998 年 2 月 13 日国务院信息化工作领导小组发布）。

7 计算机信息系统保密管理暂行规定（1998 年 2 月 26 日国家保密局发布）。

据初步统计，分散在上述法律法规中的涉及公民个人的禁止性规定及法律责任规定有 16 条 22 款。在中国法律管辖的范围内，所有利用计算机信息系统及互联网从事活动的组织和个人，都不得进行相关的违法犯罪活动，否则，必将受到法律制裁。

关于计算机方面大学生必须遵守的法律规定

1 遵守《中华人民共和国计算机信息系统安全保护条例》，禁止侵犯计算机软件著作权（有关法规条文见附录）。

2 任何组织或者个人、不得利用计算机信息系统从事危害国家利益、集体利益和公民合法利益的活动，不得危害计算机信息系统的安全。

3 计算机信息网络直接进行国际联网，必须使用邮电部国家公用电信网提供的国际出人口信道。

任何单位和个人不得自行建立或者使用其他信道进行国际联网。

4 从事国际联网业务的单位和个人，应当遵守国家有关法律、行政法规，严格执行安全保密制度，不得利用国际联网从事危害国家安全、泄露国家秘密等违法犯罪活动，不得制作、查阅、复制和传播妨碍社会治安的信息和淫秽色情等信息。

5 任何组织或个人，不得利用计算机国际联网从事危害国家安全、泄露国家秘密等犯罪活动；不得利用计算机国际联网查阅、复制、制造和传播危害国家安全、妨碍社会治安和淫秽色情的信息。发现上述违法犯罪行为和有害信息，应及时向有关主管机关报告。

6 任何组织或个人，不得利用计算机国际联网从事危害他人信息系统和网络安全，侵犯他人合法权益的活动。

7 国际联网用户应当服从接入单位的管理，遵守用户守则；不得擅自进入未经许可的计算机系统，篡改他人信息；不得在网络上散发恶意信息，冒用他人名义发出信息，侵犯他人隐私；不得制造、传播计算机病毒及从事其他侵犯网络和他人合法权益的活动。

8、任何单位和个人发现计算机信息系统泄密后，应及时采取补救措施，并按有关规定及时向上级报告。

《计算机信息网络国际联网安全保护办法》

第四条、第五条、第六条、第七条的规定

第四条　任何单位和个人不得利用国际联网危害国家安全、泄露国家秘密，不得侵犯国家的、社会的、集体的利益和公民的合法权益，不得从事违法犯

罪活动。

第五条　任何单位和个人不得利用国际联网制作、复制、查阅和传播下列信息：

（一）煽动抗拒、破坏宪法和法律、行政法规实施的；

（二）煽动颠覆国家政权，推翻社会主义制度的；

（三）煽动分裂国家、破坏国家统一的；

（四）煽动民族仇恨、民族歧视，破坏民族团结的；

（五）捏造或者歪曲事实，散布谣言，扰乱社会秩序的；

（六）宣扬封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖，教唆犯罪的；

（七）公然侮辱他人或者捏造事实诽谤他人的；

（八）损害国家机关信誉的；

（九）其他违反宪法和法律、行政法规的。

第六条　任何单位和个人不得从事下列危害计算机信息网络安全的活动：

（一）未经允许，进入计算机信息网络或者使用计算机信息网络资源的。

（二）未经允许，对计算机信息网络功能进行删除、修改或者增加的；

（三）未经允许，对计算机信息网络中存储、处理或者传输的数据和应用程序进行删除、修改或者增加的；

（四）故意制作、传播计算机病毒等破坏性程序的；

（五）其他危害计算机信息网络安全的。

第七条　用户的通信自由和通信秘密受法律保护。任何单位和个人不得违反法律规定，利用国际联网侵犯用户的通信自由和通信秘密。

关于计算机病毒

1 病毒是生物学领域的术语，是指能够自我繁衍并传染的使人或动物致病的一种微生物。人们借用它来形容计算机信息系统中能够自我复制并破坏计算机信息系统的恶性软件。

关于计算机病毒的定义；众说纷坛，莫衷一是。

《中华人民共和国计算机信息系统安全保护条例》第二十八条规定：“计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。”这是一个具有法律效力的定义。

2 计算机病毒实质上是一段可执行程序，它具有广泛传染性、潜伏性、破坏性、可触发性、针对性和

衍生性、传染速度快等特点。早期的计算机病毒多是良性的，偏重于表现自我而不进行破坏；后来的恶性计算机病毒则大肆破坏计算机软件，甚至破坏硬件，最终导致计算机信息系统和网络系统瘫痪，给人们造成各种损失。计算机病毒可被预先编制在程序里，也可通过软件、网络或者无线发射的方式传播。

在我国，故意制作、传播计算机病毒等破坏性程序是违法犯罪行为，要受法律制裁。

怎样保护你的计算机安全

1 注意防止盗窃计算机案件，在高校经常会发生此类案件。小偷趁学生疏忽、节假日外出、夜晚睡觉不关房门或外出不锁门等机会，偷盗台式电脑、笔记本电脑或掌上电脑，或者偷拆走电脑的 CPU、硬盘、内存条等部件，给学生造成学习困难和经济损失。

2 注意防止火灾、水害、雷电、静电、灰尘、强磁场、摔砸撞击等自然或人为因素对计算机的危害，要注意保证计算机运行环境和辅助保障系统的可靠性、安全性。

报纸上曾报道过（新电脑也有大麻烦）的新闻。一户人家花了一万多元买了一台名牌电脑，没用 20 天主权就坏了。维修人员认为是静电引起的，人身静电“烧毁”主板，电脑公司不承担保修义务。这静电

不得不防。

3 防止计算机病毒侵害电脑，要使用正版软件，不要使用盗版软件或来路不明的软件；从网络上下载免费软件要慎重，注意电子邮件的安全可靠性；不要自己制作或试验病毒。重创世界计算机界的CIH病毒，据说是一个台湾大学生制作的，它给全世界带来了电子灾难。

4 如果你把计算机接人互联网，经常进行网上冲浪，就必须小心“黑客”的袭击，后面的“防黑十招”请你注意。

5 有了计算机，就要同时选用正版杀毒软件，应选用可靠的、具有实时（在线）杀毒能力的软件。

6 养成文件备份的好习惯。首先是系统软件的备份，重要的软件要多备份并进行写保护，有了系统软件备份就能迅速恢复被病毒破坏或误操作破坏的系统。其次是重要数据备份，不要以为硬盘是永不消失的保险数据库、某高校一位研究生把毕业论文存储在笔记本电脑里，没有打印和备份，后来该笔记本电脑丢失，令他十分痛苦，几个月的心血白费了。另外，病毒也会破坏你的硬盘或数据。

7 给电脑买个保险。据《中国经济时报》报道，中国人民保险公司开始在全国范围内推广计算机保

险。

此险种，包括计算机硬件损失保险、数据复制费用保险和增加费用险（设备租赁费用险）等，主要承保火灾、爆炸、水管爆裂、雷击、台风、盗抢等导致的硬件损失，数据复制费用和临时租赁费用。对于风险较难以控制的病毒、“黑客”侵害和计算机 2000 年问题，则列人责任免除条款。

8 要树立计算机安全观念，心理上要设防。网络虽好；可是安全问题丛生，网络陷讲密布，“黑客”伺机做案，病毒层出不穷，秩序不是很好，你要特别小心。不要以为我是高手我怕谁，须知天外有天，网上杀手多如牛毛，弄不好你就被人“杀了”。

9 保护电脑安全的其他措施：

（1）最好选购与你周围的人的电脑有明显区别特征的产品，或者在不被人轻易发觉的地方留有显著的辨认标志；

（2）当你和机器分别较久之时，如寒暑假等，最好把机器内部较贵重的芯片取下另保存它处；

（3）上网的电脑千万注意防止密码泄露他人，并经常更改密码；

（4）在有条件的院校，可寄放到专门的保管场所。

防止“黑客”攻击的十种办法

1 要使用正版防病毒软件并且定期将其升级更新，这样可以防止“黑客”程序侵入你的电脑系统。

2 如果你使用数字用户专线或是电缆调制解调器连接因特网，就要安装防火墙软件，监视数据流动。要尽量选用最先进的防火墙软件。

3 别按常规思维设置网络密码，要使用由数字、字母和汉字混排而成，令“黑客”难以破译的口令密码。另外，要经常性地变换自己的口令密码。

4 对不同的网站和程序，要使用不同的口令密码，不要图省事使用统一密码，以防止被“黑客”破译后产生“多米诺骨牌”效应。

5 对来路不明的电子邮件或亲友电子邮件的附件或邮件列表要保持警惕，不要一收到就马上打开。要首先用杀病毒软件查杀，确定无病毒和“黑客”程序后再打开。

6 要尽量使用最新版本的互联网浏览器软件、电子邮件软件和其他相关软件。

7 下载软件要去声誉好的专业网姑，既安全又能保证较快速度，不要去资质不清楚的网站。

8 不要轻易给别人的网站留下你的电子身份资料，不要允许电子商务企业随意储存你的信用卡资

料。

9 只向有安全保证的网站发送个人信用卡资料，注意寻找浏览器底部显示的挂锁图标或钥匙形图标。

10 要注意确认你要去的网站地址，注意输入的字母和标点符号的绝对正确，防止误入网上歧途，落入网络陷阱。

本世纪最大的一起计算机病毒犯罪案

近十几年来，伴随着计算机突飞猛进的发展，计算机病毒也在不断泛滥，它们侵入研究所、银行、电话交换中心、政府机关甚至航天发射中心，产生了巨大的危害。据不完全统计，每年在世界范围内由于计算机病毒所造成的经济损失高达数百亿美元。由于计算机病毒本身所具有的隐蔽性、突发性、感染性和破坏性，许多年来一直都是令各国警察和计算机专家头痛的事情。

1988 年 11 月 2 日，是一个令大部分美国计算机科技人员永远难忘的日子。

美国东部标准时间下午 5 点刚过，位于纽约州的康奈尔大学计算机系统突然变得比以前慢了许多。

正在使用计算机系统进行计算的科研人员立刻就此事向计算机系统管理中心发出咨询，因为康奈尔大学当时采用的是当时美国乃至全世界都是最先进

的计算机系统，在一般情况下，即使系统连接的终端机同时起用，也不会给计算机造成太大的负担。其实管理中心的管理工作值班员已经发现了这个从来没有发生过的现象，并已经开始着手进行检测。

发现“蠕虫”

几分钟后，计算机系统专用检测软件就找出了系统速度严重下降的原因：系统内多了一段能够快速自我复制、并且占用系统资源空间堵塞系统通讯通道的一段小程序（这段小程序后来被计算机科学家们称作“蠕虫”）。值班员发现这段程序后，立刻对该程序进行分析，分析的结果十分令人沮丧，由于这段程序设计的精巧使其具有快速传播和自我复制的能力，很可能已经传播到了与康奈尔大学相联接的其它计算机网络。值班员立刻把这个十万火急的情况向系统管理中心报告，并且向联邦调查局报案。

果然，时间不到晚上 9 点，康奈尔大学获悉位于加利福尼亚的斯坦福大学和著名的智囊机构兰德的计算机系统出现了蠕虫。

紧接着，晚上 10 点，加利福尼亚大学伯克利分校的计算机系统发现蠕虫，并受到其严重危害。

晚上 11 点，麻省理工学院人工智能实验室找到蠕虫。

11 点半，戴维斯和圣地亚哥的加利福尼亚大学、加利福尼亚州的劳伦斯·里福莫尔实验室、位于加利福尼亚州的美国国家航空航天局计算机网络系统被蠕虫传染，陆军弹道研究实验室发现蠕虫。

危害还在延续。

次日凌晨 1 点，15 台 ARpanet 网络（我们今天见到的英特网的前身）的主机报告发现蠕虫。

2 点，哈佛大学检测出蠕虫。

3 点半，蠕虫入侵麻省理工学院计算机中心。

4 点，由于蠕虫堵塞信息通道，造成蠕虫的传播速度变慢，但也大约有 1000 台主机被蠕虫击中。

5 点一刻，宾夕法尼亚州的匹兹堡大学报告发现蠕虫。

3 日晨，当人们走到自己的计算机面前，发现的是令他们目瞪口呆的事实，他们的计算机已经基本无法运转了。

大约在 2 日晚 11 点，也就是发现第一个蠕虫之后 6 个小时，联邦调查局已经意识到这将是一场最为严重的计算机犯罪案，调查局有关人员立即赶赴岗位，一个由联邦调查局最干练的警探和纽约州最能干的计算机系统分析专家组成的特别侦破小组已经成立，并开始了一项最为特别的侦破工作。

一张全美计算机系统网络图已经展开在警探和计算机专家面前。

发现蠕虫的消息不断传来，并且发现蠕虫的地点呈辐射状不断地扩展开来。特别侦破小组认定，蠕虫的发源点就在这个辐射网的中心：康奈尔大学。

立刻康奈尔大学计算机系统在 11 月 2 日中午 12 时到下午5时之间上机的所有用户名单传到了侦破小组。在康奈尔大学计算机科学系的配合下。疑点逐渐集中到了该系研究生罗伯特·莫里斯身上。

11 月 3 日晨，睡眼惺松的莫里斯从床上被叫起来。

莫里斯承认了他研制并放出“蠕虫”的全部过程

蠕虫案件立刻轰动了全世界！全球的新闻媒介由此刮起了报导计算机病毒的旋风。

令人吃惊的是，莫里斯的父亲竟是纽约州计算机系统安全协会的主席！

聪明过人的莫里斯在他 20 岁那年就考入康奈尔大学计算机科学系，并且对计算机安全产生了浓厚的兴趣，在这方面还颇有些研究，当然，他的成果是十分显赫的，不过只是没有产生正面的效应。

莫里斯研制的计算机蠕虫是一小段程序，它采用截取口令字，并在系统中试图做非法动作的方式直接

攻击计算机。蠕虫与一般的计算机病毒不同，它不采用将自身拷贝附加到其他程序中的方式来复制自己。蠕虫一般由许多代码模块构成，欲将其隐藏在操作系统的文件中不大可能，因为它比较大。

蠕虫在进入计算机网络后，利用空闲的处理器测定网络中的计算机跨度。蠕虫程序由许多段构成，在其主段的控制下，蠕虫的某个段运行在单独的计算机上。蠕虫典型的传播方式是采用网络链或电子邮件方式由一台计算机传播到另一台计算机。这不同于病毒对文件的操作系统的感染。计算机系统把需要运算的数据都存放在内存区内，蠕虫可以用重写某个特定内存区的方法来得到对正在运行的内存区数据进行破坏的目的，在蠕虫运行中也可以破坏程序，蠕虫通常造成的后果是系统崩溃。蠕虫的作乱通常是借助于系统的缺陷，为了说明莫里斯编写的蠕虫工作原理，先介绍一下莫里斯蠕虫所攻击的 ARpanet 网络的情况。

莫里斯蠕虫攻击的ARpanet网络是为了使计算机专家能够共事电子信息、程序和数据而设计的。因为该网络是一个通用的科学研究工具，所以通过简单的口令字例可进行读取。ARpanet 网络依据容易理解的操作指令运行，并能用命令使之与其他网络拼接。

1983 年 ARpanet 网络分裂为两个网络。一个是

MILnet 网络，它用于密级较高的军事通讯，但不涉及极密的军事信息。

在莫里斯蠕虫事件中，该网络发言人承认，附加到 ARpanet 网络和 MILnet 网络的非保密部分的几台主机被蠕虫击中。第二个网络是环绕主网联结着数百个民用网络的大网。在莫里斯蠕虫事件中，有报告报导，在该网络中有 300 多台计算机被击中，涉及到网络中的大学、医院和研究中心的计算机，其中包括海军研究实验室、宇航局的 Ame 研究中心、SRI 等著名机构。

剖析莫里斯蠕虫程序的计算机专家声称：莫里斯蠕虫程序编程技巧非凡。它利用了 ARpanet 网的三个安全规则。

在莫里斯蠕虫事件中，有数台计算机幸免于难，因为其系统管理人员重写了有关规则的安全程序。

莫里斯蠕虫具有其特殊的工作原则，它窃取口令字，而后伪装成一个合法用户拷贝自身发送到远处的另一计算机中。结果导致蠕虫不受控制地疯狂拷贝，致使英特网计算机通讯网络的 10％约 6000 多台计算机被传染并遭破坏。

莫里斯的程序诡诈而且复杂。此程序长达 6 万字节，它可以对 UNIX 操作系统中经过复杂加密处理的

口令字进行译码，利用口令字将自己伪装成合法用户。康奈尔大学的负责人说，他们在莫里斯的计算机文件中发现了一张口令字表，它和从网络中的蠕虫中找到的口令字表相像。

根据专家们分析，蠕虫是利用了信息发送程序SendMail（也称电子邮件）蒙骗计算机的安全机构混入计算机的，而后蠕虫隐藏在内存中，接着它产生一个程序，被该程序命令攻击的计算机能够产生特殊的加过密的口令字文件，利用口令字蠕虫可以混入其他计算机。

使用美国伯克利大学编写的 UNIX 操作系统的计算机系统最容易遭受攻击。

蠕虫利用 UNIX 的 E－Mail 程序（也即 SendMail）接触计算机，蠕虫被认为是一个合法的E－Mail信息，计算机打开其 E－Mail 通道，允许蠕虫进入计算机。事实上，蠕虫是由可执行代码构成的程序（被作为了SheLL外壳程序），就像一个合法的用户调试一个UNIX程序那样。

蠕虫程序的初始部分作为一个合法的 UNIX 外壳程序运行的同时，蠕虫程序的第二部分通过 E－Mail 系统进入计算机。这一部分也是由可执行代码构成的信息序列，它向蠕虫的外壳直接发出命令。第一组命

令让计算机去读取与该机通讯的计算机登录表，并将蠕虫的初始部分送到网络中的其他计算机。第二组命令是由一批通用口令字构成的表，其中的内容用 DES 算法加密处理过，利用附加的命令将计算机中的口令字表（也是经 DES 算法加过密的）与蠕虫的口令字表做比较。

每个加密的蠕虫的口令字与计算机的各个合法用户口令字相比较时，蠕虫记住严格相符合的那些口令字。在计算机的 3000 多个口令字中，蠕虫可得到 20 个。这些口令字之一可以读写系统用户的数据。在 UNIX 操作系统环境中，系统用户具有读写被保护的数据表和文件的特权，可以读写网络中的其他计算机，具有通过计算机系统读、写、删除文件的能力。此时，蠕虫通过窃取到的系统用户的特权，可以传播蠕虫自身到网络中的其它计算机，它已经可以对数据和程序文件做更严重的破坏动作。但是，莫里斯蠕虫没有做，唯一感受到的损害是计算机合法程序的处理速度显著变慢。由此可见，莫里斯设计蠕虫时，似乎没有使之具有毁灭性的意图。

上述是第一种莫里斯蠕虫的工作过程。有人还发现了另一种蠕虫，估计也是莫里斯编写的。这种蠕虫也是通过 UNIX 的电子邮件系统进入计算机，但是采

用了不同的攻击方式。在多数 UNIX 电子邮件系统中，有一个“手指”实用程序，它对本地用户和网络中的远程用户同样有用。它可以给出在特定计算机现场的用户的有关信息。蠕虫通过计算机的“手指”通道询问与 UNIX 计算机相关联用户的信息，为回答这一询问，计算机加载“手指”程序，该程序调用存储器阵列去加载所要求的“手指”数据表，但是蠕虫改变了这个存储器阵列，使此调用指向蠕虫自己并开始 UNIX 外壳的运行。其他信息类似于前述的第一种蠕虫。例如命令外壳程序去读取主机数据和口令字表，并开始上述加密口令字的比较处理等。

莫里斯的蠕虫揭露了系统的弱点。这些弱点是由于人为疏忽造成的。设计网络的电子信件程序的编程人员，保留了一个秘密的“天窗”，他可以很容易地读写其工作关注的目标。当编程人员完成任务以后，他忘记关闭这个“天窗”。他设置这个“天窗”是为了读那些管理人员不允许读写的程序。莫里斯发现了这个秘密的“天窗”。系统中还存在着其他的秘密入口，这些入口已被其他的攻击者所揭露。莫里斯蠕虫还揭露了另一漏洞。英特网中的“手指”程序允许用户在远处的计算机上了解近处在其他网络机器上工作的用户情况。莫里斯利用了这一程序漏洞，窥探他

冲破计算机安全机制的方法。“手指”程序的缺陷众所周知，如果一个很长的信息发送给“手指”的话，可以使用户读取计算机的中央控制程序。

根据莫里斯朋友的介绍，第一个被蠕虫击中的目标是麻省理工学院的一台计算机。当时，莫里斯本人在纽约的康奈尔大学他的计算机上使用了远程控制。远程控制是英特网络最有用的特征之一。蠕虫程序具有一种机制，它可以隐藏蠕虫的入侵源点。蠕虫程序自身的全部拷贝作为信息被周期性地发送出，并且在加利福尼亚大学的伯克利分校的计算机上发现了这些信息，这意味着蠕虫已经击中该计算机。

当莫里斯准备检查他的程序的进展时，他发现网络已经过载。他自己也遇到了麻烦，不能读取监控器，也不能中止他的程序。他马上请求在哈佛大学的朋友在英特网上发出报警和指示如何阻止蠕虫。莫里斯的朋友用技术术语发出了一则简短信息。但是，这些信息出现在模糊的电子公告牌上，因为网络严重过载，到处如此，只有很少的计算机用户收到这一信息。

被蠕虫击中的哈佛大学一位专家报告说，当蠕虫击中他们学院时，它成了热门话题，引起了恐慌。人们纷纷议论，蠕虫是如何工作的？怎样才能杀死它们？蠕虫是1988年11月3日早晨入侵我们的系统的。

我们的系统管理员和工作人员早晨做的第一件事情是按照惯例读取电子邮件信息。他们发现了有关蠕虫的报警信息。其中一些奇怪文件的存在表示系统中有一个或多个蠕虫，以及如何制服蠕虫。

系统管理员迅速查出了一个正在运行的 UNIX 外壳程序，它与终端不相联系，系统管理员发出了杀毒命令，杀死了第一只蠕虫。

大约一小时后，系统管理员在终端上看到了第二个蠕虫出现的新信息和报警。此时，英特网络已处于一片慌乱之中，建议系统管理员们关闭电子邮件或者将机器同网络脱开。幸而，系统管理员继续监视我们的 UNIX 系统并没有脱网。不久，他们收到了由伯度大学系统员编写的蠕虫治疗程序。这个程序使蠕虫去调用和写入一个空文件，从而消除掉蠕虫的部分代码，以阻止蠕虫通过系统继续传播。蠕虫使学院计算机运行迟缓，为了检测和消除蠕虫花费了系统管理员的一个工作日（大约 120 美元）。

蠕虫的大范围蔓延，促使加利福尼亚大学伯克利分校的 UNIX 操作系统研究室重新分析他们的系统，改写了系统中的错误，关闭了 UNIX 系统 debug 状态，改写了“手指”，使它做阵列边界检查，这使非法入侵者再也不能利用蠕虫程序将自己的代码重写内存

的内容。

全国首例黑客操纵股价案一审判决

被告人赵哲被判处有期徒刑 3 年

全国首例非法操纵证券价格案，在上海市静安区人民法院进行了一审判决。被告人赵哲被一审判处有期徒刑三年。法院的判决书指出，被告人赵哲为了使自己和朋友获利，在今年 4 月 16 日，通过某证券营业部的电脑非法侵入该证券公司的内部计算机信息系统，对待发送的委托数据进行修改，造成当天下午开市后，“兴业房产”、“莲花味精”两种股票的价格被拉至涨停板价位，造成这家证券营业部遭受损失 295 万余元，被告人的行为已经构成操纵证券交易价格罪。法院根据刑法 182 条等条款，判处被告人有期徒刑三年，处罚金一万元并赔偿某证券公司损失 249 万元，同时追缴赵哲违法所得 7277 元。据悉，作案人赵哲，现年 28 岁，在上海市某河北证券营业部工作。今年 4 月 16 日窜至上海新闸路某证券公司营业部，利用该营业部电脑安全防范上的漏洞，修改该营业部部分股票交易数据，致使下午股市开盘不久，兴业房产和莲花味精两只股票瞬间便被拉到涨停板价位，成交量也急剧放大。仅仅维持了片刻，这两只股

票的价格又迅速回落，从而引起股价在短时间内剧烈震荡。上海证券交易所发现这一情况后，查出是海南某证券公司出现大笔买盘所致。经查询，发现电脑系统遭“黑客”侵入。今天一审判决后，赵哲说：“法院的判决是公正的”。此案给疏于防范的证券营业部敲响了警钟。

网上犯罪者戒！

最近，从武汉市公安局计算机管理监察处获悉，他们于 1998 年 2 月组建的计算机国际互联网安全监察专业队伍从 1999 年 11 月正式获得刑事办案权以来，已查获网上刑事案件 14 起，查处网上色情活动达 30 多起，真正发挥了“网上侦察兵”的战斗作用。

网上犯罪在逼近

随着高科技的发展，电脑逐渐进入千家万户，人们利用电脑获取信息、增长知识，特别是电脑上网之后，互联网更是发挥着不可估量的作用。然而，一些人却利用互联网从事各种违法犯罪活动，如敲诈、传递色情信息、从事破坏和反动宣传活动等。

1999 年 11 月 3 日，一名武汉网民在互联网上敲诈一香港巨富，索要 3 亿港元。

2000 年 3 月 9 日，武汉大学校园网“珞珈山水”的网络中的电子公告栏（BBS）被一黑客恶意“灌水”，

部分版面瘫痪。

2000 年 3 月 18 日，武汉警方发现有人在网上粘贴诽谤攻击他人的文章。

2000 年 2 月始，警方发现部分网上服务商在网上散布大量色情呼号、色情电话及黄色电子邮件。一些个人网站专走“美女路线”，收罗色情照片入网，毒害青少年，致使一些人走上犯罪道路。这些色情内容大多来自国外，包括照片、文字描述及影片剪辑，此外，还有色情小说。一名少年因模仿网上色情画面犯罪而被抓，其父母对公安机关说：“我们给孩子上网，是想让他了解更多的知识，然而他每天看的都是色情画面。”

网上警察在行动

随着国际互联网的开通，武汉警方深感网上犯罪危害极大，不可轻视，它对国家的政治、经济安全可能造成不可估量的损失，对下一代的身心健康也是一种严重的威胁。武汉警方深感责任重大，专门成立了计算机国际互联网安全监察队伍，并对网上犯罪活动予以重拳打击。

1999 年 11 月，公安部发出通报，香港某公司在国际互联网上收到一封发自武汉的电子邮件，发件人公开向一巨富索要 3 亿港元，并威胁如不给将遭受更

大损失。武汉警方迅速成立了专案组，他们先从电信部门入手，获取发信人的 IP 地址，然后查找其网络公司，走访网吧密集的地区。功夫不负有心人，侦查人员终于查到有人利用武昌区八一路“同志网吧”注册的邮箱，再通过位于同一条路上的“天际网络”网吧发送出了敲诈邮件。由于这两个网吧都坐落在大专院校周边，每天上网人数众多，而网吧管理者又没按公安机关的要求逐人登记，要想找到发信人犹如大海捞针。

侦查人员在两个网吧附近对经常出入网吧的人员进行了详细调查，终于获得了一条有价值的线索，一个 20 来岁的男青年在网吧里曾对别人说过，现在是网上时代，可以通过网络敲诈外地富翁。据调查，那青年个子不高，每隔几天就会来此上网。侦查人员不分昼夜守候在两个网吧周围。11 月 13 日，当这名青年走进“天际网络”时，被当场抓获。这位武汉某大学 4 年级学生感叹地说：“我怎么也想不到，公安人员能有破获网上敲诈案的本事。”

2000 年 1 月，警方在调查一公司老板被杀案中得知，此案与该老板的网友有关。“网上侦察兵”再次出动，在网上对被害人结交的上百个网友展开调查，终于找到了这位躲在电脑屏幕后的凶手，并千里追踪

将其抓获。这名犯罪嫌疑人说：“我原以为以网上交友的方式谋取钱财，公安人员就是有天大的本事也破不了案，谁知一个月就找到了我！”

2000 年 3 月，3 名网民听说制作色情信息是网上赚钱的好手段，就建立了自己的个人网站，利用色情内容发财。他们将色情照片传给网络服务商，从中获利，这 3 人很快就被“网上侦察兵”全部抓获。

2000 年 3 月 18 日，武汉市公安局接到举报，有人在网上粘贴诽谤攻击他人的文章。“网上侦查兵”认真走访查询，终于在 3 月 29 日凌晨将犯罪嫌疑人刘某抓获，并据他提供线索逮捕了其他 2 名同案犯。他们发出了同样的感慨：“我们万万没想到，将道听途说的东西上网粘贴，也能被捉到。网上犯罪是做不得啊！”

网络是高科技发展的产物，是人类智慧的结晶，应该用来为人类的健康发展服务。有人以为网络如浩翰大海，做了任何事都能轻易躲藏起来，殊不知网络也是一片天空，随时都在监测者的注视之中。天网恢恢，疏而不漏，触犯法律者都将受到法律的惩罚。

扬州宣判盗窃银行巨款的“黑客”死刑

扬州市中级人民法院近日对利用计算机盗窃银行巨款案的郝景文、郝景龙两兄弟作出二审判决，

以盗窃罪判处郝景文死刑，剥夺政治权利终身，并处以没收财产５万元人民币，其兄郝景龙因检举郝景文其他重大盗窃属实，被法院认定为重大立功，被判处无期徒刑，剥夺政治权利终身，并处没收财产人民币3万元人民币。

郝氏兄弟于１９９８年９月22日，利用自制的装置侵入扬州工商银行电脑系统，将７2万元转入其以假名开设的银行活期存折，并在工商银行扬州分行下设的储蓄所取款26万元，当两人在扬州某储蓄所要求支取人民币４万元时，因该所工作人员向其查验身份证件，两犯害怕罪行败露，遂逃回镇江市。

案发后，郝景龙分得赃款１2万多元，郝景文分得赃款１3万多元，侦察机关追回23万多元，及赃款购买的物品。1９９８年１2月22日，扬州市中级人民法院以盗窃罪判处两兄弟死刑。

两犯不服，向江苏省高级法院提出上诉，在二审期间郝景龙检举其弟郝景文的６起盗窃余罪，省高级法院依照有关程序撤消扬州中院的一审判决，发回扬州中院重审。之后扬州中院另行组成合议庭审理此案，法院经审理，认定了郝景文伙同他人盗窃丹徒县某银行“福特”面包车一辆、镇江市某商场人民币１万多元、镇江市某典当行人民币５０００元及寻呼机

7只的犯罪事实。扬州中院认为郝景龙检举被告郝景文其他重大盗窃事实，经查证属实，属重大立功，故依据法律，对其从轻处理。

北京首例利用计算机犯罪案件告破

我国新刑法实施以来，京城首例利用计算机进行犯罪的案件近日被北京市公安局朝阳分局破获，犯罪嫌疑人张文明已被抓获归案。

据介绍，1998 年 12 月 31 日，北京无忧电脑软件开发公司向北京市公安局朝阳分局报案称：该公司在1998年底开发的一级A类计算机等级考试DOC学习软件中发现病毒。接报案后，朝阳公安分局立即成立了由专业技术人员参与的专案组，迅速展开全面调查。

经有关方面初步测试，已发现的病毒为“逻辑炸弹”病毒，它将于 1999 年 3 月 27 日和以后的每月 27 日爆发。届时，只要运行该学习软件，此病毒将导致硬盘文件被删除，并破坏分区，从而给用户造成不可估量的损失。

为及时侦破这一高科技犯罪案件，公安机关多次走访有关人员，收集了大量的证据材料，并找到了制作计算机病毒的代码和有害程序的原文打印件，初步确认该公司开发部原主管张文明有重大嫌疑。

今年 1 月 10 日， 公安机关依法传唤了张文明。

在证据面前，张文明终于供认了因与公司领导发生矛盾，为了报复，就利用工作之便将一个外国病毒修改逻辑后植入公司开发的这个学习软件中的事实。目前，无忧公司已售出的带有病毒的学习软件大部分已被收回。