信息安全动态

4

主编：四川大学信息安全研究所

吉林科学技术出版社

前　言

为全面、及时地反映国内计算机信息网络安全领域的发展动态，四川大学信息安全研究所选择了国内发行的中央和省市级的日报与经济类报刊以及 IT 业重要报刊(入选报纸的发行量至少 5 万份以上、杂志至少 2 万份以上)，将其中涉及计算机信息网络安全在技术、产品、市场、管理、案例等方面发展动态的报道加以精选并分类整合，逐月汇编为《信息安全动态》，自 2001 年 1 月起，由吉林科学技术出版社正式出版。

《信息安全动态》全年二十四辑，每月出书二辑。我们期望以此来快捷、全面地反映国内信息安全领域的发展动态和国内计算机信息网络安全市场的一些基本状况，能为应用、管理、决策人员提供有益的参考。

因无法与部分作者取得联系，故我们依照有关规定将其稿酬代为保管，同时敬请这部分作者见到本书后及时与我们联系，届时我们会将稿酬及利息汇出。

限于编者的经验，不足之处敬请批评指正。

四川大学信息安全研究所

《信息安全动态》编委会

信息安全动态第四辑目录索引

✧ 一、警钟篇

✧ 二、案例篇

✧ 三、管理篇

✧ 四、业界动态篇

✧ 七、争鸣篇

✧ 八、曝 光 篇

✧ 九、趋 势 篇

✧ 十、安全锦囊

✧ 十一、其 它

警钟篇

- “库尔尼科娃”碰不得
- 手机病毒大举入侵
- 黑客盯上各国政府和军方
- 专家警告——互联网运作中最重要的一套软件存在漏洞
- 互联网三大隐患：硬件损坏、病毒和黑客
- 数字签名技术“DSA”存在重大缺陷

……

電脑商情報

2001年2月20日

“网球美女”碰不得

——Anna病毒肆虐全球

新春佳节还未远去，正是春暖花开的季节，各种病毒已然苏醒，蠢蠢欲动，欲在网上大施拳脚。2月上旬北京地区的“反 love”病毒已使多家公司局域网瘫痪，接着两种新的“爱虫”病毒变种——“山姆”和“情人节小礼物”在2月10号出现，两种新病毒都与情人节有关，以电子邮件和 web 蠕虫的方式传播，目前还未肆虐，已引起了病毒专家的警惕。而从12日起，一个伪装成网球明星安娜·库尔尼科娃电子照片（见图）的病毒在北美和欧洲迅速传播开来。14日，“网球美女”已登陆到上海，对亚洲用户造成威胁。

AnnaKournikova 是一种与2000年年初被发现的“爱虫”蠕虫相类似的计算机病毒，以微软公司的“Outlook”为跳板，以电子邮件附件方式传播的。电子邮件的邮件名为“Here you have ;o)”，文本的正文为“Hi; Check This!”，附件名为“AnnaKournikova.jpg.vbs”，伪装成性感的俄国女子职业网球选手 Anna Kournikova 的图像。发明时，病毒在复制本身后向登记在 Outlook 地址簿中的所有地址发送带病毒软件，该病毒将大量发送电子邮件，由于传输量的增加有可能导致网络发生故障，短短几个小时之内，这种病毒迅速复制传播，使多个电子邮件服务器速度骤减，迫使一些公司不得不暂停电子邮件服务器以清理病毒。该病毒并不会给计算机系统造成永久性损坏，而只是类似以前的梅利莎病毒，造成邮件系统瘫痪，其传播速度堪与去年的“爱虫”媲美。

该病毒是由绰号为“OnTheFly”的荷兰人编写，他十分崇拜俄罗斯网球明星安娜·库尔尼科娃，所以将他所编写的病毒称为安娜－库尔尼科娃。他本人自称无意伤害任何人，只是想警告那些缺乏安全意识的人，此说法未免太牵强。据统计，自从2000年8月份首次发现 AnnaKournikova 以来，至少在财富500强企业（Fortune 500）企业中已有50多家公司受到感染。

（凌宁 编译）

齐鲁晚報

2001年2月14日

电脑病毒大闹情人节

“库尔尼科娃”当了杀手

本报2月13日消息 2月12日，随着情人节的临近，一种以网坛美少女库尔尼科娃的电子照片形式出现的计算机病毒肆意袭击了欧洲和北美的计算机服务器，给无数用户造成了麻烦。

据网络安全专家透露，这种最新的电脑病毒专门袭击电子邮件系统，其主要表现是造成电子邮件系统速度减缓，而许多企业在删除这一恶意程序的过程中导致整个电子邮件系统彻底关闭。在短短的几个小时之内，该病毒在欧美迅速扩散，其发作程度几乎和去年5月份给全球计算机用户带来灾难性后果的“我爱你”爱虫病毒一样厉害。

这一病毒制造者的聪明之处在于将对少男少女有着巨大吸引力的库尔尼科娃和坐在计算机前用户想入非非的幻想结合在一起，从而发挥了巨大的杀伤力。该病毒是以附件形式出现，附件的文件名是AnnaKournikovajpg.vbs，邮件正文上是英文“你好，请检查一下这个邮件”。

该病毒是一种蠕虫病毒，可以在用户电子邮件地址簿上自动扩散。这种病毒不会对计算机造成永久性的破坏。另外，到目前为止，该病毒只在使用微软操作系统的电脑上的OUTLOOK EXPRESS邮件系统上发作，而对于使用苹果电脑以及其他电子邮件系统的用户来说，最多只会通过手工方式感染该病毒。（子午）

互联网周刊

2001年2月19日

“库尔尼科娃”病毒来势凶猛

“库尔尼科娃”病毒的袭击，给互联网用户再次敲响警钟

本刊记者 刘莉莉

一种以网坛性感美女库尔尼科娃的图片为伪装的电脑病毒一夜之间袭击了欧洲和美国的电脑用户，这种病毒类似于去年的“爱虫”病毒。该病毒主题为：“Here you have,:o”，来势凶猛。此病毒在欧美的传播，使亚洲各大公司提前基本作好了准备，因此根据亚太地区各国发布的消息表明，整体来看，亚太地区遭受的损失不大。总部位于加州的Trend Micro公司的台湾发言人约翰·D·雷索说：“这个病毒给美国造成的损失比亚洲要大得多。因为亚洲这边开始工作的时候，所有大公司基本上都已经对他们的系统做了一次清理。”

该病毒是以电子邮件的方式传播的，邮件内容极其简短：“Hi:CheckThis!”。邮件附加文件为：AnnaKournikova.jpg.vbs。接到这个文件的人还以为能看到库尔尼科娃的照片，但是一旦打开这个附件就会大祸临头。因为该病毒可在Windows目录中自动复制，然后，他会将自身发送给Outlook中的通讯簿中的所有用户，但信息本身被删除，并且在已发送邮件里找不到刚才已发送出去的带病毒的附件。除此之外，病毒还在每年1月26日自动启动浏览器，到一个指定的网址访问。有专家称：“库尔尼科娃”病毒的传播速度比爱虫病毒慢但比梅利莎病毒快。

反病毒公司Symantec发言人称这种病毒来自荷兰，病毒的始作俑者化名“OnTheFly”，他使用了一种脚本工具，利用此工具，任何一个稍微有编程能力的人就可以编制出病毒。

2月13日，一个自称拜访过“OnTheFly”的人发布了一份声明，称病毒作者发布这个病毒的初衷是想告诫互联网用户注意网络安全。与此同时，Excite@Home网站找到了可以证明该网站在荷兰的一名用户与OnTheFly是同一个人的证据。

随后，OnTheFly在发给记者的电子邮件中称 自己年龄为二十岁，对电脑编程并不是很在行。“我编写这个病毒的目的并不是为了好玩，”OnTheFly于本周二在一家网站上发布消息说，“我从来没有想过要去伤害那些打开附件的人。如果他们的电脑因此而受到感染，这只能是他们自己的错。”OnTheFly发布的消息还证实了他的确使用了一种编写病毒的工具——Vbs Worm Generator，但他否认了该工具的作者对他提供过帮助。OnTheFly在信中还表示对编写了“库尔尼科娃”病毒感到非常后悔。

有些人表示相信这份声明的真实性。例如从事反病毒研究的F-Secure公司经理就不怀疑这份声明。但他说，要在网上找到真实的病毒编写者是非常困难的。而且，荷兰没有任何相关方面的法律，所以，要对他提起诉讼也会相当困难。

但无论是否能真正起诉这位编写病毒的OnTheFly，专家指出，在各反病毒公司对各种病毒作出相应解决方案的同时，用户要随时提高警惕，警惕以美女照片、各种动画Flash等附件传播的病毒。

E-mail:angela@ciweekly.com

金融早报
FINANCIAL MORNING POST
2001年2月23日

“安娜”病毒“异形”被发现

本报讯 据报道，“安娜·库尔尼科娃（Anna Kournikova）”病毒的一种新变种日前在德国出现。这种在德语圈内被称为“新价目”的变种病毒，采用了和“库尔尼科娃”病毒一样的结构和加密技术，但对有效荷载进行了修改。

德国的《Chip》杂志于周五披露了有关该变种病毒的消息。随后，F－Secure 公司的“雷达病毒和安全预警”服务，也针对此变种病毒向用户发出了高级别的警告。

将上述变种病毒称为“OnTheFly.B”的 F－Secure 表示，首次发现它的时间是在周五清晨，据信，病毒已经开始四处传播。“OnTheFly.B”改变了“安娜·库尔尼科娃”病毒的有效荷载，并发送一条简短的德语信息。这条德语信息和 T－Online 将在 3 月份实施的上网新资费政策有关。“OnTheFly.B”的附件名称为“Neue Tarife.txt.vbs”。

和“库尔尼科娃”病毒相同，“OnTheFly.B”病毒非常温和，主要任务是通过用户的微软的 Outlook 地址簿进行自我复制。不过，它会通过产生数量庞大的电子邮件信息，使企业的电子邮件服务器崩溃。

大家知道，病毒无国界，谁也不知道它什么时候传到中国。如果碰到名称为“Neue Tarife.txt.vbs”的附件，一定不要打开。细心防范总是没坏处的，亲爱的读者，您说呢？ （黑 客）

三秦都市报
2001年2月16日

专门感染掌上电脑的病毒出笼

本报综合消息 第一个专门感染掌上电脑的病毒近日被芬兰一家反病毒公司发现，这一病毒名为 Phage，它的文件很小。目前这一病毒还没有被广泛地传播，但一位反病毒专家指出，由于这一病毒的源代码已被公开，因此他预计这个具有破坏性的病毒目前已被许多人所掌握，不久其具有更大欺骗性或破坏性的变形病毒即将出笼。

中国高新技术产业导报
CHINA HIGH-TECH INDUSTRY HERALD
2001年2月9日

手机病毒大举入侵

今天的手机不仅仅作为通信工具，还可以通过接入互联网而获得大量的信息，也就是说手机接入互联网将是未来手机发展的必然趋势。

可以想象，由于必须要同 PC 机进行不断地信息交流，所以手机难免会染上与电脑病毒一样的破坏程序，同时手机上网也为病毒的传播提供了更有利的条件，使病毒造成危害的速度与程度都大大地超过了以往任何时候。

日前，出现了面向手机电话等便携式信息设备的“ EPOC”上运行的病毒。这次发现在 EPOC 上运行的病毒共有 6 种。第一种是“ EPOC- ALARM”，它总是持续发出警告声音，虽无大害，却也颇为烦人；第二种是“EPOC-BANDINFO.A”，它发作时会将用户信息变更为“ Som e foo l ow n th is”；第三种是“EPOC-FAKE.A”，它会在手机的屏幕上显示格式化内置硬盘时画面，无需惊慌，因为实际上手机并不会执行格式化操作的；第四种是“ EPOC- GHOST.A”，它会在画面上显示“ Eve ry on e h a te s you”的话；第五种是“ EPOC-ALIGHT.A”，它会使背景灯持续闪烁；第六种病毒是“ EPOC-ALONE.A”，它可以使键盘操作失败等等。

这 6 种病毒中前 5 种的危害并不很大，并且还很有些恶作剧的味道，但第六种叫做“ EPOC-ALONE.E”的病毒却是一种恶性病毒。当电脑接收有毒的程序时，会显示红外线通信接收文件时所显示的画面，并在此时将病毒悄悄地藏入内存之中。当病毒在内存中运行之后，会在电脑画面上显示“ W a rn in g- v iru s”的信息，此后手机便不接受任何键盘操作。当你发现以后，可以输入“ Leave m e a lon e”来解除病毒常驻。

目前，在越南已出现一种破坏移动电话的病毒。当对方拨电话到来时，本来(对于绝大多数显示来电者电话号码的数码技术移动电话)屏幕上显示的应该是来电者的电话号码，但却显示“ Un ava ilab le”字样或一些奇异的符号。

凡遇到上述场合情形，接电话者应不予回答且立即把电话关闭。倘若按键答复来电，移动电话就会染上该种病毒，同时机内所有资讯及设定均将被破坏(包括缴费使用电话卡的电话在内)，一旦发生此情况，可能要换上一台新的移动电话。

截至目前，在美国已有逾 300 万台移动电话染上该种病毒。

另外据报道，短消息接收也会传播手机病毒。据称，横行互联网的计算机病毒下一个入侵目标是手机和移动上网设备(PDA)，最终侵入上网电视和其他上网家电。这是去年亚洲反病毒大会(AVAR)上透露出的信息。会议重点讨论了计算机病毒的未来发展趋势和应对策略。与会者普遍关注手机病毒的发展进程和解决方案，目前，已出现通过短信息发布来传播病毒的手机概念病毒。所谓概念病毒是指已经实现潜伏、传播、感染和破坏等病毒特性的病毒雏形。一旦用户接收到带有病毒的短信息，阅读后便会出现手机键盘被锁死的现象，以后可能出现破坏手机内存储的信息，直至彻底破坏手机 IC 卡等恶性手机病毒。

目前应对手机病毒的主要技术措施有两种：其一是通过无线网站对手机进行杀毒；其二是通过手机的 IC 接入口或红外传输口进行杀毒。

针对电子设备病毒的新变化，防毒与杀毒公司都采取了相应的对策。早在去年 6 月，趋势科技为防范一种最近刚刚发现的可向手机乱发短消息的蠕虫病毒——VBS- TIMOFONICA，紧急推出了新版病毒码 725#，并提醒用户注意手动或自动下载新版。

该病毒是 6 月 6 日最早在西班牙发现的，目前已知的信息还不足以表明该病毒会在西班牙以外的地区传播和流行，但是鉴于 VBS 类病毒可以修改原码，容易出现变种的特点，不排除会出现类似新病毒的可能。严格说来，虽然其影响波及了手机，但并非通过手机传播，还是典型的电脑病毒。

不过，这足以引起防毒专家的注意，因为面对如此大量的手机用户，处理不好将会给世界带来巨大的损失。 (阿 彪)

中国计算机报
2001年2月15日

手机病毒来了

日前，专家们发现了面向手机等便携式信息设备在一种“EPOC”的程序上运行的病毒。这次发现的病毒共有6种，其中前5种的危害并不很大，但第6种病毒却是一种恶性病毒，它可以使手机不接受任何键盘操作。目前，在越南已出现一种破坏移动电话的病毒。在美国已有逾 300万台移动电话染上该种病毒。据报道，短消息接收也会传播手机病毒，计算机病毒下一个入侵目标是手机和PDA，最终侵入上网电视和其他上网家电。

三秦都市报

2001年2月12日

黑客盯上各国政府和军方

本报讯 根据监视黑客攻击的 Web 站点 Attrition.org 的消息，一群黑客最近袭击了美国、英国和澳大利亚政府网站。

Attrition.org 在其站点上说，这是迄今为止规模最大的有计划对各国政府服务器进行的破坏行为。一个名叫 Pentaguard 的国际黑客组织策划并实施了这次攻击。

在这次袭击中受害最深的 5 个官方网站是：美国内政部阿拉斯加办公室的网站、加利福尼亚州议会共和党党团的网站、英国伦敦市政府的疯牛病咨询网站、澳大利亚的立法院搜寻网站和澳大利亚海洋科学研究所的网站。

Pentaguard 还声称，"这将是人类历史上最大规模摧毁政府和军方网站行动的开始"。Attrition.org 说，从它所袭击的站点来看，无论从一个国家或者从一个政府部门的角度而言，都算不上是大规模的破坏。但是，由于 Pentaguard 是在处于 3 个不同时区内的 3 个不同的国家同时向这些网站发动攻击的，而且每次攻击之后最少 15 分钟才被发现，所以这次黑客攻击是不同寻常的。 (IDG 电讯)

拒绝服务

黑客攻击的手法之一是"拒绝服务"。

在一般的连接中，用户向服务器发送信息，请求服务器证明其身份。服务器向用户返回身份已获得证明的信息。用户获得身份已获证明的信息后，就可进入服务器了。

在拒绝服务(DOS)攻击中，黑客向服务器发送许多证明身份的请求信息，占满服务器的处理能力。所有这些请求信息所带的信息返回地址都是假的，这样当服务器要返回身份已获证明的信息时，无法找到用户。这时服务器就开始等待，有时等待时间超过 1 分钟，之后才会关掉这个连接。当服务器关掉这个连接以后，攻击者又发过来一批新的请求信息，上述过程又将重演一遍，从而使得服务器进入无限期的阻塞状态。

北京科技报

2001年2月9日

专家警告——互联网软件存在安全缺陷

安全专家警告说，互联网软件存在新的安全漏洞，它使得攻击者可以通过重新引导网络和电子邮件的路径来影响互联网的稳定性。

CERT 协调中心是政府资助的计算机应急反应组织，设在卡内基·梅隆大学。该中心说，安全漏洞源自 BIND 软件，它是引导互联网路径的重要电脑软件。漏洞是在 1 月早些时候发现的，软件制作人已经修复了漏洞。CERT 的工作人员为 BIND 用户提供咨询，以便让用户快速安装软件。BIND 名为域名服务器，其作用如同网络上的电话号码簿。电脑用户在上网时键入诸如 Yahoo 之类的域名，软件引导用户进入 Yahoo 的网站。安全专家说，如果没有矫正漏洞，它会使得网络入侵者改变引导目录。这样，电子邮件会发往错误的地址。网址也会导向错误的网址，比如，你键入 www. myfavorite－place. com，系统会引导你去一个色情网站，或者是一个看起来与你想看的网站差不多的错误网址。

Bind 在 90% 以上的美国国内域名服务器上被使用。安全专家指出，BIND 是入侵者的好目标，在几天或几周内，黑客就能找到突破的方法。 CERT 中心管理人说，这是影响互联网最严重的安全漏洞。但是目前还没有发现攻击者利用这个漏洞。虽然过去曾发现 BIND 的问题，但是潜在的威胁更严重，因为该程序安装在许多电脑上。世界上有上万台域名服务器，每个服务器伺服 1 万－2 万个用户，所以一次攻击只会影响一部分互联网用户。因特网还有 13 个主目录，也叫根服务器，它们告诉其它域名服务更新的信息。这些电脑位于美国、东京、斯德哥尔摩和伦敦，使用 BIND 软件。在极端的情况下，黑客可能改变根服务器的设置并重新引导所有的 . com 路径。如果没有 BIND，互联网用户就不得不记住数字字符来上网和收发电子邮件。

就在不久前，由于技术人员的错误和黑客对微软服务器的攻击，微软公司的网站关闭了四天。虽然没有证据表明这次攻击与 BIND 软件有什么联系，但是这也显示了域名服务器的重要性。

China Industrial Economy News
CIEN产经新闻
2001年2月6日

黑客开始利用互联网中枢漏洞

本报讯 美国互联网专家发现，互联网运作中最重要的一套软件存在某些缺陷，使电脑网络黑客有空子可钻。一旦黑客掌握了这些软件缺陷，就可以操纵网络服务器、偷取电子邮件，以及改变网页访客的寻访途径。

这套有缺陷的软件叫"伯克利互联网名域"(Bind)，它的第四版和第八版存在上述缺陷。组成互联网的电脑网络中估计有90%都使用Bind软件。

专家敦促使用那些Bind"危险版本"的网络服务器管理员尽快换用新版本。在向公众发出警告之前，互联网的13个全球网址主服务器已经全部更新升级。关于Bind软件缺陷的警告是由美国政府拨款的机构"电脑急救队"(CERT)发出的。

Bind在互联网上的角色类似电话号码查询系统。当一台电脑向它查询某个网站时，它就把该网站域名转换成数码网址，根据数码网址就能在互联网上打到那个网站。

一个网络通常有数百上千台电脑向一、两个运行Bind的服务器查询网址。美国PGP Covert实验室发现，Bind第四版和第八版存在上述严重漏洞，可能会被恶意的黑客利用，并控制服务器。一般情况下，当网络上的一台电脑接到它不理解的信息时，就会发出常规的"出错"提示，但Bind的漏洞可能导致它执行精心杜撰的假信息中隐藏的指令。黑客能够钻这个空子，由此操控网络服务器，把访客指引到他们控制的网站，或把电子邮件转投到别的地方。

Cert负责人赫南(Shawn Hernan)说，Bind可以说是互联网最重要的软件，这是历来发现的最严重的互联网安全漏洞。该组织一般都通过互联网发布新的网络安全方面的警告，但这次问题极其严重，Cert决定采用传统的新闻发布会方法发布警告，敦促网络服务器管理员尽快更新各自使用的Bind版本。

Cert的专家还强调说，由于电脑黑客密切注视有关网络安全问题通告，甚至比许多网络服务管理员更积极，所以大家必须尽快采取行动，否则可能很快就会遭到黑客袭击。

该组织估计，用不了多久，黑客就会蜂拥而至，来尝试钻Bind的空子。

Cert曾在1999年11月发布了一则有关Bind软件缺陷的通告，随后几个月中黑客尝试乘隙作祟的次数显著上升。

(周易)

投資導報
2001年2月12日

网络"臭虫"为黑客开方便之门

专家已发布除虫动员令，视其为对全球网络安全的最大威胁

令美国电脑专家冷汗连连的是，网络空间居然存有一只致命病毒，一旦黑客发现了这只危险的软件"臭虫"，他们就可肆无忌惮地"绑架"政府及企业网站，窃取敏感电子邮件，彻底搅乱网络访问。有鉴于此，专家已发布除虫动员令，视其为对全球网络安全的最大威胁。

据《华尔街日报》报道，致命的臭虫出现在控制网络访问最常用软件——BIND (Berkeley Internet Name Domain，伯克利互联网域名)上。BIND的软件功能犹如网络空间的门牌号码系统，装载BIND软件的域名服务器是实现网络访问功能的关键，正是它将方便易记的网络域名转换成网络服务器能辨认的数字式地址。因此，网络浏览器与域名服务器间的联系必须保持畅通，以确保浏览器获取正确域名信息。

但专家在现有版本的BIND软件中捉到的臭虫却偏偏可以搅乱网络空间的门牌系统，切断网络浏览器与域名服务器之间的正常联系。一旦黑客发现漏洞所在，他们就可改变或删除网络域名，人为扭曲网络访问线路或干脆使网站瘫痪。比方说，黑客可利用BIND臭虫将在线银行客户引向一个受自己控制的虚假网站，用以窃取访问者的密码与账户信息。

发现软件病毒的是受美国政府资助的协调中心，一般网民更熟悉该中心易名前使用的称呼——"电脑应急反应组"。协调中心的专家指出，BIND臭虫对"互联网的安全构成了巨大威胁"，正是在他们的敦促下，美国联邦政府已于上月底向其下属各联邦机构发出了系统病毒一级警报。"这是影响互联网的最严重问题之一，"在接受《华尔街日报》采访时，中心负责研究网络安全问题的团队领导人肖恩·赫尔南忧心忡忡地表示，"一旦病毒发作，网站将轻易被接管，电子邮件也很可能会改变路径，文档被送至你根本不想让它去的地方。"为此，赫尔南告诫网民们在网上冲浪时应多加小心，留神可能出现的诸如电子邮件邮路受阻等异常现象，因为这很可能意味着黑客偷袭行动的开始。

协调中心已紧急呼吁拥有网络域名服务器的大公司及网络服务提供商(ISP)立即升级其BIND软件系统，软件升级并不复杂，用时不会超过一个小时。协调中心同时建议消费者应向自己的ISP咨询，以确认公司方面已成功捉虫，以防在未来网上冲浪时遇到大麻烦。

尽管专家表示，可能有成百上千台域名服务器电脑需重装升级版BIND软件，但目前很难确认网络虫患的确切范围。"出现这种问题，一般消费者不会有什么好的应对办法，"美国马萨诸塞州坎布里奇电脑安全公司——"@stake"研究及开发经理魏尔德·庞德称，"我们的忠告是，上网时要多个心眼，不要轻易递交敏感的个人资料。"

《华尔街日报》称，时至新世纪伊始，控制全球