信息安全动态

7

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

目 录 索 引

✧ 一、警钟篇

✧ 二、*案例篇*

✧ 三、管理篇

✧ 四、业界动态篇

✧ 五、技术篇

✧ 六、应用篇

✧ 七、争鸣篇

✧ 八、综合分析与对策研究

✧ 九、趋势篇

✧ 十、专家论坛

✧ 十一、爆光篇

✧ 十二、安全锦囊

篇

”

阱

增（相关报道 8 篇）

计算机世界 2001年4月9日

三种攻击威胁企业安全

今天，企业的生产经营活动越来越依赖于网络，在这种情况下，即使是很小的安全漏洞都可能带来破坏性的结果。由于贪欲、竞争或者纯粹的恶意，闯入者会把目标对准企业关键资产：信息、系统，并利用企业所依赖或所提供的服务进行破坏。因此，了解企业面临主要安全威胁并防患于未然是企业保持竞争力的基础条件之一。在所有的安全威胁中，以下三种是最为严重的。

攻击1：访问攻击

攻击方式 拒绝服务（DoS——Denial of Service）是一种比较简单而且正在日益流行的攻击。攻击者只要向被攻击的服务器发送信息洪流，就能使Web服务器、主机、路由器和其他网络设备淹没于洪流之中，使用户、客户和合作伙伴无法访问网络。

拒绝服务攻击的后果可能是破坏性的。2000年2月7日，一次经过改头换面的拒绝服务攻击使雅虎、eBay、CNN、亚马逊、Buy.com等多家大网络公司的网络反应速度减慢或严重瘫痪，导致了数千万美元的损失，而且公司的名誉也因此受到严重的损害。

有许多技术都可以帮助居心叵测的人实现拒绝服务攻击，这些方法大多非常简单，很容易实现，当然也有一些复杂的高级工具用于欺骗不明真相的系统，使这些系统变成一架实施攻击的机器，这就是分布式拒绝服务攻击（DDoS）。如果受到攻击的机器是一台Web服务器，那么拒绝服务就是一件很令人烦恼的事情。更糟糕的是，如果这台Web服务器是一家在线商店，那么系统一分钟不能正常运转，就会带来一分钟的经济损失，这种损失有时是巨大的。

除了来自外部的攻击，内部的拒绝服务攻击甚至破坏性更大，因为这有可能使企业的整个经营活动陷于停顿。您可能经历过暂时的网络或电子邮件服务中断，但如果有一次长时间的有意攻击，使所有员工的工作都陷于瘫痪，这将让企业付出沉重的代价。

如何面对 首先要确认攻击的来源，然后对来自这些站点的交易不予接受。这个过程需要花费时间，而且需要网络管理员具有广博的知识，了解网络信息包、路由信息以及其他一些有关Internet基础结构的深层次技术问题。但对大多数企业来说，最好的反击是有一个事先制定的紧急事件反应计划，该计划一般应该包括三个关键元素：

- **技术对策** 例如，在攻击出现时使用分组的IP地址，或者交换到可替换的应对安排上去。
- **事后的法律诉讼** 包括收集攻击者修改系统的证据，如果能够确认和抓获攻击者，应对其起诉。
- **公共关系反应** 包括直接通知客户、厂商、合伙人和投资人。

攻击2：偷窃专利信息

攻击方式 有两种形式的信息偷窃行为：智能资产偷窃（商业机密、销售预报、职员资料、会计资料等）和工业间谍（受雇于他人的高级专业间谍、外国政府间谍和目标是针对某一组织实施攻击的犯罪企业联合体）。攻击者可能拷贝或删除企业内部数据资源中的重要信息，或者把这些重要信息据为己有、出卖或者用来勒索钱财。

最令人头疼的是，并非所有的偷窃行为都是外部攻击的结果，某些不道德的员工也可能偷窃自己组织内部有可能出售给其下一个老板的重要信息，或者攫取那些能够帮助自己建立新公司的重要信息。程序员也可能在定制的软件中留下后门，让重要信息自动地传递出来。

如何面对 安装在线的防盗警报器，在失窃事件发生时起到制止作用。简单地说，在线防盗警报器是一种对防火墙起补充作用的入侵检测系统，它实时监控网络的运行过程，捕获和分析信息包的标题和内容。对那些能够承受开发代价和执行安全策略的组织，或者是必须遵守政府的安全规定的大型机构来说，做好内部的安全工作是最佳的选择。当然，要想运用好这些方法，就必须使用安全评估技术以保证防火墙、加密引擎和其他安全基础设施能够正确地配备和正确地运行。

入侵检测和反应系统提供了基础层面的防卫。这些应用系统可以对攻击或各种误操作行为做出实时反应，包括报警、记录或者终止攻击人的网络连接。一些著名的安全产品厂商一直在提供保证信息安全的硬件、软件和专业服务。其中最著名的有Check Point、RSA Security、VeriSign、Symantec、Network Associates、Trend Micro、Internet Security Systems等。其中，Internet Security Systems的经营有一些独特之处，它专门研究管理安全服务、安全评估、入侵检测和决策支持系统。

外购信息安全服务是另一种可选方案，其优点是客户只购买最急需的信息安全服务。随着市场的增长，服务需求会随之升级，客户只要支付更多的费用，就能享受更高级的服务。公共安全服务包括防火墙、入侵检测与反应、远程安全评估、虚拟专用网络和反病毒解决方案。

攻击3：破坏硬件、软件和数据

攻击方式 这类攻击的目的是破坏硬件、应用程序或数据资源。目前已经有一些软件能显示出攻击的来源，确定攻击是由可信任的内部职员、承包人还是由严重危害信息安全基础设施的入侵者发动的。攻击人为了永久地改变或删除这些软件，必须进行物理型访问。

组织内部的滥用职权也会带来严重的威胁。在电影“超人”中，主人公Richard Pryor通过编写会计系统程序，让系统将所有账目的零头划归到自己的账上，从而获取了大笔非法收入。虽然这是一部有趣的科幻电影中表现的出轨行为，但这种滥用职权的行为在现实生活中同样存在。事实上，许多公司都发现，有些Y2K咨询人员都在其程序代码中留下了后门，这些后门可能给未来的攻击者带来便利。

此外，企业常用的数据库也为不怀好意的攻击提供了机会。大多数企业级数据库（例如Microsoft SQL Server、Oracle、Sybase Adaptive Server等）都有一些存储程序。这些程序大多是用宏编程语言制作的，它们自动地为数据库应用程序安排任务，而且可以模仿一些基本的操作系统功能。许多组织对其主机上的操作系统给予了充分的保护，但对数据库应用程序却很少提供保护，最终的结果是数据库软件可能被用来发动对数据或网络其他部分的攻击。

如何面对 因为硬件攻击需要对网络资源进行物理访问，对这类系统的安全保护相对来说比较简单：注意屏幕，看看是谁访问了重要的服务器和网络基础设施（例如网络集线器、交换机和路由器）；保证您确实把那些包含了有价值信息的可移动设备和备份介质（CD-ROM、磁带、压缩盘、操作维护卡式带盒等）存放在安全的地方，这些设备和介质只有经过授权的职员才能拿到。将拷贝副本存放其他地方也是一个极好的做法，你甚至可以考虑不在工作站上装备可移动的存储设备。

笔记本电脑的大量使用给企业数据安全带来了新的挑战。数据存储设备是可移动的，因此也就成为主要的偷窃对象。解决的方法是要求笔记本电脑在规定的时间必须与主服务器连接，以确认持有人的合法性。此外，每台笔记本电脑还应该使用商业级操作系统，必须有用户标识（ID）和口令才能使用。移动锁和可锁定的存放场所有助于临时保护放在桌面上、台面上及其他非移动支撑物上笔记本电脑的安全。加密也有助于保证存储在被偷窃的机器内的敏感数据。事实上，偷窃来的机器对任何没有经过彻底的安全审查而又想读出这些数据的人是没有用处的。定期复审服务器的用户登录主日志和使用方式也可以显示出不正常的行为，确定哪台设备被盗用了。

适当地审查职员和承包人，限制未经授权人员的访问权，是保护软件代码和基本商业数据的最佳办法。由于不同机构或机构内部不同部门所采用的软件常常是不相同的，因此标准的信息安全核查是必须要做的事情。

（李明琪 编译）

微电脑世界

“移动”病毒来了！

2001年3月25日

王凌云

以为移动设备就不会受到病毒的骚扰吗？您错了！随着移动设备使用的日益普及，病毒制造者也将他们的目标瞄准了蜂窝电话和PDA等手持设备。一场魔高道更高的持久战将在移动领域打响。

越来越强的计算能力和越来越好的通信连接一定是好事吗？未必如此。如果销售商们盲目追求这两点的话，可能会导致病毒的再一次泛滥。原因有两方面：第一、摩尔定律告诉我们，蜂窝电话、数字手表等将很快具备运行所有软件的能力；第二、人们正在试图通过蓝牙或其他联网技术将所有设备相连，而这将不可避免地为那些能够自我复制的病毒程序提供一种新的扩散途径。如果一个设备受到病毒感染，病毒将以光速传播给与该设备相连的所有其他设备。

即将出现的“移动”病毒的首个受害者肯定是所谓的移动设备——蜂窝电话和PDA。前者就不需要介绍了，后者包括从极小的Palm V到Microsoft的Jupiter级机器，其大小类似膝上电脑，但能提供更长的电池寿命。为防毒起见，膝上电脑并不将自身归为移动设备，因为它们的易攻击性与台式PC和Mac机相似，也需要与之相同的保护。现在的PDA都相当复杂，它们被设计成具有GUI、办公套件、手写识别等特性，处理器的速度至少也与Intel 80386相当，此外它们还能够装载和运行各种各样的程序，而这也恰恰构成了病毒存在的一大威胁。

移动设备天生就比较脆弱

结合了PDA操作系统和无线通信终端的智能电话，被反病毒界认为是最易受攻击的移动设备。病毒制造者已经放弃了基于Palm OS和Windows CE的设备，因为他们不得不依靠热同步和红外线来传播。而有了移动电话，他们就有了新的选择，病毒可通过Internet传播，甚至还可以通过直接拨打其他智能电话来传播。

Symantec反病毒研究中心的专家指出，移动设备天生就比PC易受病毒攻击，因为它们基于不安全的处理器。Pentium能够提供存储器级的保护，但移动电话中的芯片却不能。存储器级的保护意味着每个应用或过程在存储器中都拥有它自己的空间，不能被其他应用或过程访问。自80286以来的所有Intel兼容的处理器都包含了这一特性。

然而，移动电话在存储器级保护方面的缺陷主要还是个理论问题。存储器级保护必须在操作系统中实现，这在Windows 95/98/Me的桌面版中都还没有实现，因为它们的核心还是基于DOS，而DOS是为更老的处理器写的。虽然现在还没有哪种操作系统能够完全发挥芯片的安全特性，但Unix和Windows NT/2000确实能够提供某些程度的保护。

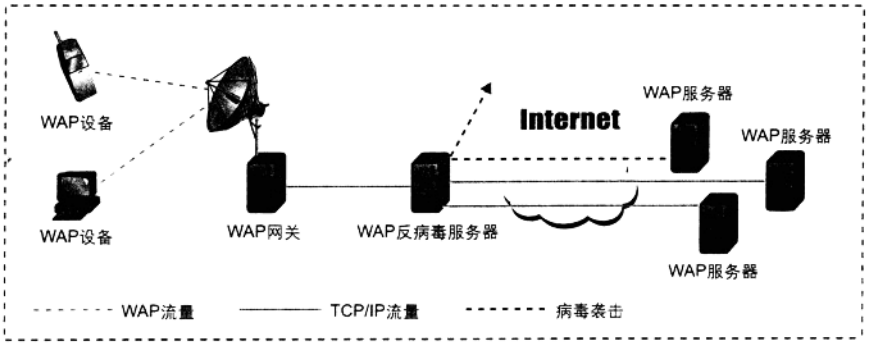
使得存储器级保护意义不大的另一个因素是脚本语言和宏病毒的增多，这些病毒在更高的级别运行，根本不需要直接访问存储器。最近发生的病毒恐慌大多与.vbs文件有关，它是利用Microsoft的Visual Basic脚本语言VBS写的，能够运行在Windows 98以来的所有Windows版本上。宏病毒也非常猖獗，它利用了Word、Excel等应用程序中实现自动运行任务的一些特性，比传统的病毒程序更加好写，并且能够轻易地跨越各种操作系统之间的屏障。虽然目前Windows CE中包含的Pocket Word和Pocket Excel还不支持宏，但最终它们也会的，因为只有能以常用的Office软件格式读写文件，才能使PDA更受欢迎。而与之相伴的是，很可能病毒也就来了。

脚本语言是“移动”病毒的温床

电话和PDA也正在开发其自身的脚本语言，这对病毒制造者很有利。1999年夏天Sun公司发布了Java的嵌入版J2ME，这是一个专门用于移动设备的常用语言版本。和其同类软件一样，J2ME使编程者能够写出运行于任何平台的Java小程序，而不论它是基于何种操作系统和处理器。

Java小程序在虚拟机内部运行，这使得它们无法访问本地的文件、通信链

接或病毒可能进入的系统的任一部分。不幸的是，这也同样使得Java小程序不能完成许多有用的任务，因此Java允许小程序请求访问虚拟机外部，而用户也不得不允许这样的请求。如果用户足够警惕的话，Java应该是安全的。然而问题的关键在于，大多数的用户都不够警惕。正如几乎所有的E-mail病毒都需要用户打开一个附件，但这点"难度"并未能阻止病毒的传播。2000年致命的"爱虫"泛滥就是一个很好的例证。而两年以前，人们甚至非常高兴地运行送到他们面前的.exe文件，结果却感染了无害却烦人的Happy99。



附图 WAP的防病毒解决方案位于网关前面，防止病毒及其他恶意代码到达移动设备。

比Java造成更大威胁的是Wscript，它是嵌入WAP中的脚本语言，几乎存在于所有的新型蜂窝电话（包括非智能电话）和新版的Palm OS和Symbian操作系统中。现在世界上蜂窝电话的数量已经多于PC，分析家预计在未来4年内它们将取代PC成为主要的Internet接入方式。因此WAP很快比Windows还要流行，而它也将成为病毒的一个极具吸引力的目标。Wscript的安全性不如Java。WAP赋予脚本直接访问电话的特权，以便能够实现在线目录帮助等功能。这就意味着病毒能够通过一个用户的电话簿，呼叫其他每个用户，以发送其自身的副本。日本NTT DoCoMo的用户已经遭遇过类似的情形，起因只是一个基于PC的病毒。在那次事故中，无论用户何时将电话连到同步信息，计算机都会取得控制并向警方发送一个愚弄性的紧急呼叫。

所有的反病毒公司都声称对于有害的Wscript小程序的最好防护就是在移动网络和Internet之间的接口——WAP网关安置防毒软件（见附图）。WAP网关的一个功能是将Wscript小程序编译成可执行的代码，这样就使得病毒无从传播。因为如果病毒在一个没有运行防病毒软件的网关被编译，它就有可能直接在各个电话间传播。到目前为止，还没有哪个厂商开发出电话自身的防病毒程序，尽管有些制造商希望最终能将防病毒程序内置在硬件中。

"无线"病毒中的赝品和真品

2000年6月，媒体报告了一种叫做Timofonica的病毒袭击了蜂窝电话，告诉人们病毒已将目标瞄准蜂窝电话。尽管从某种程度上来说这是实情，但实际上该病毒并不是真正在蜂窝电话上运行。Timofonica只是一种普通的.vbs病毒，感染的是运行Windows 98/2000的PC机。该病毒运行后，整个屏幕会显示一段控诉某厂商从事非法商业行为的文本，然后将同样的讯息通过短信息业务发送给所有的蜂窝电话用户。

Symantec公司认为目前病毒对电话并不能构成威胁，原因是电话目前的处理能力还不能完成病毒运行所需的复杂计算。WAP将文件的大小限定在1KB以内，这只够写一小段文本的长度。但在未来的几年以内，就会出现能够支持病毒的电话。不过与此同时，反病毒厂商也已经生产出了据说是能够保护移动设备免受未来病毒威胁的产品（见附表）。目前的防病毒软件都是运行在PC而非PDA上，从理论上说，防病毒软件要装入移动设备也需要通过一个PC主机。当这两个机器相连时，防病毒软件就会扫描移动设备并将可疑"物品"全部清走。基于PC的病毒扫描程序不会占用移动设备本身就很稀缺的存储空间和系统资源，但同时也不能提供完全的保护。现在人们经常将PDA彼此相连或连到Modem，因为无线互联已使得不通过PC装载软件更为容易。这也促使有些厂商大力开发运行在PDA自身的软件，但目前还不能带给用户更多的选择。

PDA自身的防病毒软件开发始于1998年，但并没有一个好的开头。当时Iris软件公司发布了一个保护Windows CE的软件包，随后就没有了这方面的任何消息。然而我们知道，防病毒软件是需要时常升级和更新的，以跟上病毒的不断演变，过时的保护软件只能给用户一种安全的假象。

如今就连病毒也不怎么理会Windows CE了，或许是因为它的应用实在太少。但对应用多得多的EPOC则另当别论，尽管到目前为止大多威胁都还表现为无害的玩笑方式。最令人担忧的是一种叫做Fake的病毒，它表现为一个生动的对话框和"格式化磁盘"的信息，但如果用户能记起PDA实际上并不需要磁盘，它就不能带来任何恐慌了。所有这些玩笑程序都能被现有的基于PC的扫描程序识破，而厂商F-Secure还发布了一款专门用于EPOC的程序。随着越来越多包含WAP和蓝牙的移动电话中嵌入了操作系统，相信其他反病毒厂商在这方面也会有所动作。

附表 防病毒程序

	Palm OS	Windows SE	Symbian EPOC	WAP
F-Secure (http://www.f-secure.com)	本地和在PC上	——	本地	在网关上
Sophos (http://www.sophos.com)	在PC上	——	——	在网关上
McAfee (http://macfee.com)	本地和在PC上	在PC上	在PC上	——
Symantec (http://www.sarc.com)	本地和在PC上	——	——	——
Trend Micro (http://www.trend.com)	——	——	——	在网关上
Panda Software (http://www.pandasoftware.com)	在PC上	在PC上	在PC上	——

注：许多厂商宣称其软件能够检测是否有病毒侵入PDA，但这些软件大多运行在PC上而非PDA上。同样，WAP电话也是通过位于网关的软件得到保护的。

那么Palm OS是否安全呢？目前有3家厂商生产用于Palm OS的防病毒软件，似乎这一平台是最可靠的，但是用户还是得小心。因为目前针对Palm设备的3种防病毒程序都是免费提供下载的，开发厂商没有得到相应的经济效益，其提供的技术支持也就非常有限。正是关于Palm的一切都应免费的观点导致了第一次真正的恶意程序的爆发，它就是Liberty Crack。其实Liberty Crack并不是一个真正的病毒，因为它不能传播。它实际上是一个特洛伊木马程序，假扮成其他程序诱使用户下载。而第一个袭击Palm设备的货真价实的病毒是2000年9月的Phage，它的影响与Liberty Crack很相似，但它毕竟是病毒，可以通过红外线端口传播。

Symantec的反病毒研究中心一直在追踪各种计算机病毒，并对每一种病毒的影响划定一个从1－5的严格等级。最严重的级别是5，声名狼籍的“梅莉莎”病毒和其他一些能够摧毁整个网络的恶意代码都被赋予这一级别。在这个评定标准下，所有为移动设备写的病毒都被赋予级别1，因为它们为数极少并且大多都是无害的。但是“移动”病毒的这种“好心肠”并不会持续太久，也许在不远的将来，您就会被它吓得目瞪口呆。■

责任编辑：於丹 yu_dan@ccw.com.cn
责任美编：王战辉 wang_zhanhui@ccw.com.cn

计算机世界 工商时报 2001年4月3日

黑客比病毒更危险

当你上网时，是否意识到有人在不知道的暗处在监视你的动作，更可怕的是网友在OICQ上一边和你亲密地聊天，一边在偷看你电脑硬盘里的资料，任何人想做黑客都很容易，他们不需要多么高超的技术，只要会使用一些从网上下载的黑客软件就够了，宽带将带来更大隐患

□康梁／文

恶意攻击无时不在

前不久，北京赛门铁克信息技术有限公司举行了一个“一千个伤心的理由”——互联网不安全因素问卷调查。经过统计，在调查问卷中所列出的众多令人头疼的互联网不安全因素中，最令网友担心的是：1、从网上下载的文件可能带有病毒；2、我收到带病毒的电子邮件；3、网上购物时，我担心我提供给网站的个人信息会被非法利用；4、上网时，我的电脑资源会不会暴露；5、网上聊天时IP地址被盗用；6、访问某些网站时，某些程序自动下载到我的电脑；7、带有病毒的电子邮件会自动发送到地址簿上的所有地址；8、如何才能避开有害的cookies；9、访问陌生网站是否安全；10、我希望网上文件下载更快。

从上面的调查来看，电脑病毒依然是人们关注的头等大事，但是信息安全也越来越引起人们的注意。看来，安全问题并不简简单单的是防病毒的问题，丢失数据和丢失个人资料、隐私就像丢东西和丢人一样，丢掉哪一个损失更大是不言自明的。

根据一份国际统计资料显示，平均有大约30%的个人电脑遭受过恶意攻击，这个比例在网络发达的国家还要高，在中国的比例要低一些，但随着上网人数和上网计算机的增加，这个数字正在呈上升的趋势。

在你上网浏览的时候，在你下载软件、资料的时候，或者在你使用ICQ、OICQ与人联络的时候，攻击随时都会发生，令你防不胜防。这些恶意攻击导致的结果是，你的上网账号被窃取，银行账号被盗用，密码被修改，硬盘里的私人资料和数据被窃取，隐私被曝光，甚至整个系统全线崩溃。

宽带带来更大隐患

从来也没有人说过宽带的缺点，但宽带给个人隐私带来的威胁却是巨大的。如果用户上网时未在计算机上安装正确的安全措施，实际上任何黑客或“解密高手”都可以在用户不知情时非法进入你的计算机。宽带网络使黑客攻击更容易，因为尽管连接会加快，但永久域名地址使连接永远保持，永远有一条通路到达你的计算机。黑客可以扫描你的IP地址，尝试尽可能的密码直到进入你的系统。更多恶意的黑客通过这些宽带网络通路，使用移动代码，可以偷窃或捣毁你的文件。除了宽带，无线技术、芯片技术、虚拟技术、基因技术等都给网络安全带来了新的挑战。人人都在盼望宽带时代早点到来，可是宽带带给人如此大的安全隐患是很多人没有想到的。在未来，如何在享受宽带带给人的便利的同时也能很好地保护自己免受攻击，专家给出了建议。在一次“中国网络安全论坛”上，专家们透露出两点趋势性信息：一是网络安全无国界，国内的网站越来越可能受到来自国外的最先进攻击技术的攻击；二是光靠防火墙、安全扫描和入侵检测软件等根本无法保证网络的安全，只有把技术、设备和专业人员综合起来，构件全方位的网络安全服务，才是解决问题的途径。

最危险的是个人的警惕性差

在网络安全领域，人们常说的一个例子就是木桶理论，亦即一个木桶如果有一块木板是短的，那么即使其他的木板再长，水也会从短木板处流出来。有人说那块短木板是服务，其时更确切地说，那块短木板是人的安全意识，也即是人的警惕性。

人们对于病毒的防范和警惕往往要