学术论文

网络病毒行为模式分析

山秀明，李 昊，焦 健，任 勇，仇 贲，曹轶群
（清华大学电子工程系 CESL 实验室，北京 100084）

[摘要] 计算机网络在为人类造福的同时，也为病毒的传播提供了便利。在网络环境下，病毒传播的范围扩大了，速度大大加快，网络已成为近年来病毒传播的主要途径。针对病毒在网络上传播的新特点，分析了网络环境下病毒传播的主要模式，包括 E-mail 传播、主动扫描传播、通过服务器传播等，介绍了业界的一些对策，并给出了一般用户有针对性的应对措施。

[关键词] 病毒；网络；传播；模式
[中图分类号] TP393 [文献标识码] A [文章编号] 1009－1742（2003）12－0055－05

1 引言

自 1988 年的莫里斯蠕虫出现，人们开始逐渐注意到病毒在网络上的传播。但直到 1999 年，出现了 Happy99 这样完全通过 Internet 传播的病毒，网络才真正开始成为病毒的主要传播途径[1]。最近两三年来，网络传播的病毒利用 Internet 全球互联的优势和计算机系统及网络系统安全性上的漏洞，成为计算机系统安全的主要威胁。

网络使病毒与传统病毒相比具有如下新特点：传播途径更多，传播速度更快，病毒种类、数量激增，感染力更强，具有突发性感染散播能力，隐蔽性更强，重复感染率高，危害持续时间长等。

图 1 是根据 CERT（美国计算机安全响应中心）网站[2]上公布的美国计算机安全响应中心收到的病毒求援信数量做出的年份统计图。图 1 显示，自 1999 年起，随着病毒的网络化发展，病毒的危害范围迅速增大。

Internet 使病毒很容易的在极短的时间内传遍全球。2001 年 8 月 4 日的 Code Red Ⅱ，2001 年 9 月 18 日的 Nimda，2003 年 1 月 25 日的 MS SQL Server Worm 都造成了全球网络的大规模瘫痪，与互联网相关的通信、商务和娱乐中断，“地球村”变成了一个个“信息孤岛”。

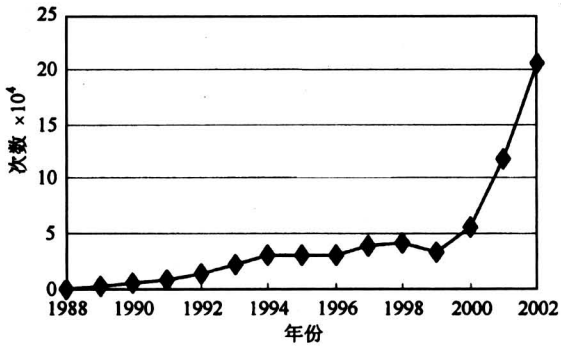

图 1 病毒数量抽样统计图

Fig.1 CERT/CC statistics 1988—2003: mail messages handled

因此，对网络病毒进行研究分析，对确保计算机系统安全和网络安全非常必要。对病毒通过网络传播的主要模式和应对措施进行分析和讨论。

[收稿日期] 2003－06－17；修回日期 2003－09－03
[基金项目] 国家自然科学基金资助项目（90204004）
[作者简介] 山秀明（1944－），男，黑龙江明水县人，清华大学教授，博士生导师

2 病毒在网络上传播的基本模式

2.1 通过 E-mail 传播

通过 E-mail 的传播是病毒在网络上传播的一个主要途径。很多网络病毒使用这种方式。网上传送的邮件中，染毒邮件的比例不断增大。在 2002 年病毒监控公司 Message Labs 统计的 20 亿封 E-mail 中，发现了 930 万个病毒，也就是说每 215 封 E-mail 中就有一个染毒邮件。而在 2001 年，这个数字是 1/398。染毒邮件在网上的泛滥，已经严重影响了正常的信息交换。

2.1.1 *病毒在 E-mail 中的存在方式有两种情况*

1) *感染 E-mail 正文* E-mail 正文可以是纯文本或 html 文本。能够被病毒感染的是 html 文本，病毒感染 html 文件的方法，一是在其中直接加入恶意的脚本语言代码，二是加入对恶意程序的引用。这里的恶意程序，可以是存在于附件中的，也可以是利用 URL 的远程调用。

2) *存在于 E-mail 附件中* 将病毒体本身或染毒程序作为附件发送。

2.1.2 *病毒通过 E-mail 传播过程有 3 个步骤*

1) *在本地找到目标地址* 病毒在整个硬盘或某些文件夹如 Internet 临时文件夹中搜索 htm，html 及 wab，dbx 文件，提取其中的 E-mail 地址。或者通过 MAPI 从邮件的客户端如 Outlook 中提取邮件地址。

2) *通过各种方式将自己作为 E-mail 的附件发出* 值得注意的是，有些病毒如 VBS. KJ 病毒不会主动发送电子邮件。而是修改系统中 Microsoft Outlook Express，Microsoft Outlook 2000/XP 的设置，采用 html 格式的信纸来撰写邮件，病毒感染全部信纸。当发送邮件时病毒自动感染邮件正文，这种方法隐蔽性更强。

3) *获取系统控制权* 通过 E-mail 到达接受端后，病毒一般通过以下方法获取系统控制权：

a. 社交工程[3] 社交工程即指利用欺骗手段使用户执行染毒文件，病毒会用多变的吸引人的标题和内容来诱骗人们。例如 Klez，拥有数量庞大的 mail 主题和主体，据说高达 120 种组合，而且很多具有极大的欺骗性，比如其中有的竟然冒充是 Klez 自己的免疫工具。

W32. Langex，W32. HLLW. Lovgate. C 邮件蠕虫使用 MAPI 来复制自身。它会恢复受感染系统上的所有邮件，所以其邮件主题变化不定。

W32. Frethem. J 的邮件主题为“Your password!”（您的密码），内文是“ATTENTION! /You can access very important information by this password/DO NOT SAVE/password to disk use your mind/now press cancel.”（注意：您可用该密码访问一些重要信息，不要保存到硬盘上，直接记住就可，请按“取消”）……

b. 利用系统漏洞 如上文分析，HTML 格式的 E-mail 正文可以感染病毒。其中一种染毒的 HTML 包含有恶意的脚本语言病毒代码，如果你使用的浏览器是 IE 5.0，而且其安全设定等级设在 medium 或是 low 时，病毒就会直接启动，其间，IE 不会给用户任何提示。

在某些系统如较早版本的 Outlook 中，附件能够自动执行，从而获得控制权，感染整个系统。这里病毒常常利用微软 IE 异常处理 MIME 头漏洞[4]，这一漏洞使 IE 在解释一些 html 邮件的时候，由于未能正确处理一些代码而导致附件自动下载，而且更为严重的是下载结束后自动打开附件。这一漏洞的问题还在于，即使 IE 在解释带毒邮件的时候开始提示用户，其提示信息也可被病毒修改为如 .txt 下载之类无害信息。

c. 以上两种方法的综合使用 另一些系统漏洞并不会使病毒直接运行，但可能会被病毒利用，作为自己的伪装。

如病毒常利用双扩展名来骗取用户点击附件。Windows 系统默认“隐藏已知文件类型的扩展名”，病毒使用双扩展名时，后面真正的扩展名被 Windows 隐藏，用户看到的是前面病毒伪造出的扩展名，这个扩展名通常是无害的，如 .txt，.jpg 等，当用户放心的点击了一个文本文件或图片后，病毒就获得了系统的控制权。

特别是含有下列双扩展名的文件，即使在关闭了“隐藏已知文件类型的扩展名”选项之后，仍将显示为 .txt 文件。具有很强的欺骗性。

.txt.shs (碎片对象)

.txt. {3050F4D8-98B5-11CF-BB82-00AA00BDCE0B}

其实是 html 文件。

2.2 通过主动扫描传播

这类病毒一般是远程扫描 Intranet 或 Internet 中远程主机的漏洞，通过这些漏洞将自己注入远程计算机并取得控制权。

病毒试图利用网络中的各种漏洞：有些病毒在局域网中进行口令字扫描，如果目标机器上存在弱口令账号（如 Administrator 账号口令为空），蠕虫便会利用该账号将自身远程注入到目标系统，直接获得系统控制权。另外一些病毒是搜索网络中的可写文件夹，并将病毒体复制到其中，或感染已有文件。

它们获得系统控制权的方法跟通过 E-mail 传播的病毒类似，但也有一些自己的特点，常见的有以下几种：

2.2.1 *社交工程即欺骗手段*　与通过 E-mail 的传播相比，这里的差别在于，安全上的漏洞使病毒可能访问及写入局域网内机器上的很多目录。这样病毒可以在目标机器上广泛传播，使其被执行概率增大。

2.2.2 *利用系统漏洞*　病毒常利用一些系统缺陷和漏洞，如：Windows Explorer 有一个默认打开的选项——“按 web 页方式察看”，打开此选项后，Explorer 在打开每一个目录时，会自动执行其下的 folder.htt。某些版本的 Windows Explorer 为了实现预览，还会自动执行其中的 .eml 文件。

Nimda 会搜索本地网络的共享文件夹，无论是文件服务器还是终端客户机，一旦找到，便会将一个名为 RICHED20.DLL 的隐藏文件加入到每一个包含 DOC 和 EML 文件的目录中。当别的用户打开这些目录下的 DOC 或 EML 文档时，Word、写字板、Outlook 等应用程序将执行 RICHED20.DLL 文件，从而使机器被感染。

与 E-mail 传播不同的一点是，利用系统漏洞，病毒常常可以在远程获得联网主机的控制权。也就是说，它们首先控制目标机，而后再将自己全部复制过去，进行下一步操作。

如最近流行的冲击波病毒（Blaster），利用了微软 DCOM 服务中 RPC 接口缓冲区溢出可能允许执行代码的漏洞[5]，控制目标机。然后在目标机上执行 TFTP 指令，从已染毒机上下载病毒。

2.2.3 *直接改写目标机的系统文件或系统文件夹*　这是病毒通过局域网传播时的一种独特方法。有些局域网上机器，其系统文件夹是远程可写的。这也许是由于管理员安全意识上问题，也可能有其他原因，如 Nimda 病毒会将所有盘根目录完全共享。

有些病毒通过在局域网中寻找可写的 win.ini 或注册表文件并修改，以便在下次重新启动后蠕虫被自动运行。

病毒还可以直接拷贝本身到局域网内可写的启动目录中，如 Win9x：Windows \ All Users \ Start Menu \ Programs \ StartUp；winNT/2k：Documents and Settings \ All Users \ Start Menu \ Programs \ Startup \ 。如 Lentin.g 蠕虫可以在局域网中传播。其中的一个流在网络中扫描，寻找所有的带有如下名称的开放的目录资源：WINXP WINME WIN WINNT WIN95 WIN98 WINDOWS。蠕虫在这些目录中寻找文件 win.ini，如果文件找到，那么用 MSTASKMON.EXE 把自己复制到这个目录中，并改变 win.ini，以便在下次重新启动后蠕虫被自动运行。

2.3 通过服务器传播

利用一些常见的，如 IIS 漏洞，IFrame 漏洞，利用缓冲区溢出等手段，病毒可以获得远程服务器主机的控制权。之后，病毒可以随意传染至服务器。而后通过服务器，传染至所有访问该服务器的客户机。如 Nimda 会通过扫描 Internet 来试图寻找 WWW 服务器，一旦找到服务器，该病毒便会利用已知的安全漏洞来感染该服务器，若感染成功，就会任意修改该站点的 Web 页，当在 Web 上冲浪的用户浏览该站点时，不知不觉中便会被自动感染。还有些病毒可以在局域网内搜索 FTP 并向其中上传带毒文件。再利用社交工程欺骗用户下载运行。

3 用户应采取的网络病毒预防措施

通过以上分析可以看到，病毒通过网络的传播有一些基本的模式和方法，如通过 E-mail 传播，通过主动扫描传播，通过服务器传播等。在了解到网络上病毒的主要传播方式后，除使用防病毒软件外，还可以采取各种有针对性的措施来应对，从而在一定程度上减小网络病毒的危害。

3.1 提高用户安全防范意识和防范能力

从上文分析可以看到，病毒获得执行，并最终取得系统控制权的重要手段是社交工程。从这个角度来讲，用户提高安全防范意识，增强对程序的判别能力，可以很大程度上阻止病毒的扩散。

另外，只有用户安全防范意识得到切实提高，下面的其他方法才能够真正得到实施。

3.2 及时修补系统漏洞

系统漏洞中，操作系统及其一些附件的漏洞是

最普遍存在的，而且又有很大的危害。以 Windows 操作系统为例，针对 Windows 系统和其附件的漏洞，2001 年 Microsoft 共发布 60 个安全公告，2002 年达到了 72 个[6]。同时，Microsoft 为一些安全漏洞提供了补丁程序。

作为 Windows 用户，应有的保护措施是，定期使用 Windows Update 为操作系统升级，或打开自动升级功能，及时修补安全漏洞。

3.3 正确进行系统安全设置

提高系统密码的安全性。重要的密码如 Administrator 密码不能太简单而易于猜出，更不能是空密码。比较安全的做法是：使用字母、数字和特殊字符的组合，并保证密码长度在 810 位以上。

将 IE 的安全等级至少设置为“中”：在用户一无所知的情况下，很多系统的安全级别被病毒、木马程序或黑客由默认的“中”更改为“低”，IE 的安全系数已经被大大降低了，将 IE 的安全级别设为“中”，可以降低运行恶意代 码的危险性。如果对自己的安全需求有更高的要求，还可以进行自定义设置，更好地保证安全性。

将文件夹设置为在局域网上共享时，尽量不要赋予写权限。确实需要时，也应设置密码。

作为服务器的计算机遭受病毒侵害的危险更大，为了减少受攻击的可能，无用的服务不开，很少用到的服务应该少开，如在这次冲击波病毒的流行中，没有开放 DCOM 服务的主机就可以幸免。

4 反病毒业界应对网络病毒的策略

网络病毒会在很短的时间内造成大范围的感染，如果仅仅使用传统的防病毒软件，靠管理员到在每台计算机上扫描和杀毒，不仅会浪费人力物力资源，而且由于网络中计算机的交叉感染，常常达不到好的防范效果。

所以，针对网络病毒，必须有新的防护措施。目前，反病毒业界主要致力于防护联入 Internet 的企业网。使用包括防火墙、VPN、入侵检测、防病毒、安全审计、加密等多项技术，利用集中控制的方式进行管理升级。并向集成化解决方案的方向发展。

4.1 电子邮件防护

为了截断网络病毒的主要传播途径——E-mail 传播，很多实际应用系统都设计了一些方案，如下图是对一个子网安全解决方案的描述（台湾趋势科技）。在防火墙后，专设了 ScanMail 系统，检查进出的电子邮件。

但在 E-mail 病毒的网络监控中，有些防毒软件只注意了防止附件中的病毒，而忽略了病毒在邮件中的其他存在形式，包括 HTML 邮件正文中的脚本和嵌入的 OLE 对象。

4.2 网络病毒防护的自动化

今天的网络防毒系统越来越庞大。首先，网络规模的迅速扩大，使一个局域网络防毒系统所要保护的的主机数目越来越多。其次，为了防范来自各个方面的威胁，每个防毒系统中所含的防护模块数量也在迅速增加。

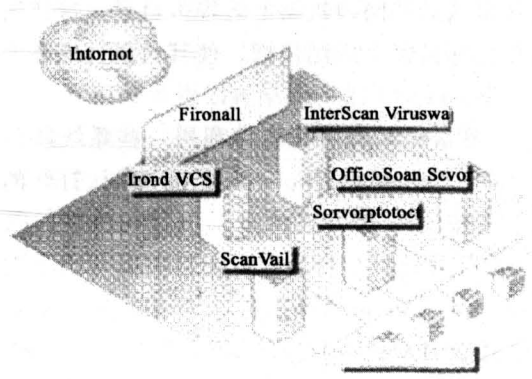

图 2 一个子网安全解决方案的描述

Fig.2 A solution of subnet security

在一个拥有几千台乃至更多主机的系统中，如果依靠传统的办法，要逐台机器安装，配置防毒软件的每个部分，这样的工作量，从人力和物力上看都是极大的浪费。为解决这一问题，目前的主要方法是在中心控制下的分布式防毒。

4.2.1 网络防毒系统自动升级，同步扫描 局域网内同步的升级和扫描病毒是早期网络防毒系统的重要特性之一，至今分布式同步扫描仍是防止网络病毒的交叉感染的重要手段。

4.2.2 网络防毒系统的中心控制 在网络防毒系统中设置网络防毒中心控制服务器，使管理员在中心服务器上就能远程管理网内主机的防毒配置。一个实际的中心控制服务器要提供自动节点发现、安装、实时配置及锁定、按需管理任务、事件日记、报警及自动响应等等一系列复杂的功能，从而减少人工参与，保证整个系统的稳定性。

4.2.3 建立网络防毒系统快速反应机制 网络病毒前所未有的传播速度，使一个新病毒在产生之后

数小时内就能传遍全球。所以，必须有新的机制来及时地发现并处理新病毒的威胁。网络防毒中心控制机制为此提供了便利。

某个商业系统的新病毒快速反应系统工作方式如下[7]：

1）*检测和免疫*　凌晨 2:00，用防病毒启发式技术检测可疑病毒活动。在客户机上安全地隔离可疑文件并通过系统管理中心控制台向中心免疫服务器发送文件副本。

2）*病毒提交*　凌晨 2:10，被隔离的文件准备好提交。IT 管理员可以选择在通过 Internet (HTTPS) 自动把被感染文件提交给网络安全公司之前剥离其中的内容。利用中心免疫控制台，管理员可以实时跟踪提交的状态。

3）*病毒解决方案和部署*　凌晨 3:00，网络安全公司技术人员分析该病毒并创建和测试解决方案。通过 Internet (HTTPS) 自动、安全地把新病毒定义发回客户的中心隔离区服务器。

4）凌晨 3:10　IT 管理员可以先测试该解决方案，也可以直接部署到被感染系统或全企业。

5）凌晨 3:15　现在，该病毒解决方案可通过该公司安全响应中心提供给其全球客户。

6）整个过程约在凌晨 3:20 结束。

5　结语

在网络环境下，病毒传播的速度大大加快了，范围几乎遍布整个网络，网络成为近年来病毒传播的主要途径。病毒通过网络的传播有几种基本模式和方法，如通过 E-mail 传播，通过主动扫描传播，通过服务器传播等。研究这些模式，可以掌握病毒通过网络传播的行为，从而采取针对性的措施，大大减小受病毒感染的可能。

参考文献

[1] Schneier B. Secrets and lies: digital security in a networked world [M]. New York: John Wiley Press, 2000. 90～124

[2] CERT. CERT/CC statistics 1988—2003 [EB/OL]. http://www.cert.org/stats/cert-stats.html, 2003－07－15

[3] Brenton C. Active defense: a comprehensive guide to network security [M]. San Francisco: Sybex Press, 2001. 100～146

[4] Microsoft. Microsoft security bulletin (MS01-020): incorrect MIME header can cause IE to execute E-mail attachment [EB/OL]. http://www.microsoft.com/technet/security/bulletin/MS01-020.asp, 2003－06－23

[5] Microsoft. Microsoft security bulletin (MS03-026): buffer overrun in RPC interface could allow code execution (823980) [EB/OL]. http://www.microsoft.com/technet/security/bulletin/MS03-026.asp, 2003－08－25

[6] Microsoft. Security bulletins [EB/OL]. http://www.microsoft.com/security/security-bulletins/, 2003－08－20

[7] Symantec. Symantec antivirus TM corporate edition [EB/OL]. http://www.symantec.com/region/cn/enterprise/article/nav-corpo-edition-7.6.html, 2003

The Mode of Net-virus Actions

Shan Xiuming, Li Ying, Jiao Jian, Ren Yong, Qiu Ben, Cao Yiqun

(*Department of Electronics Engineering of Tsinghua University, Beijing*　100084, *China*)

[**Abstract**] The computer network is not only of benefit to the people, but also helpful for the spreading of viruses. The net-viruses spread more widely and rapidly than the traditional viruses, and network has become the major way of the virus spreading. This article analyzes the mode of the net-virus spreading, including E-mail spreading, positive scanning spreading and through-server spreading. Then some defense strategies in the anti-virus field are introduced, and some countermeasures of the net computer users are discussed.

[**Key words**] virus; network; spread; mode