企业防毒软件发展趋势分析*

胡 斌 昀
(中山大学软件研究所, 广东 广州 510275)

摘 要: 针对目前网络病毒的肆虐, 企业防病毒安全建设对杀毒软件厂商的要求不再仅仅停留在病毒库的及时升级, 更重要的是, 能够根据不同企业用户的特点, 为其灵活部署一整套有效的网络安全运行机制。通过作者深入企业防毒一线, 了解当前企业对杀毒软件关注的焦点, 对未来企业防毒软件功能之发展趋势作出分析。

关键词: 网络病毒; 杀毒引擎; 安全漏洞扫描; 威胁预警; 病毒邮件; 垃圾邮件
中图分类号: TP311.56 文献标识码: A 文章编号: 0529-6579 (2004) S1-0142-03

互联网的发展和迅速普及, 计算机病毒的肆虐和猖狂也紧随着 Internet 一浪高过一浪, 近年来越来越多的系统及应用安全漏洞被发现并被利用, 网络病毒已四处肆虐且难以阻挡。目前的安全解决方案, 都无法有效阻挡这些病毒。据统计, 仅仅在 2003 年 SQL Slammer、MSBlaster. A 和 Nachi 等网络病毒在全球所造成的损失, 即已爆增至 21.3 亿美元。而愈来愈多缺乏保护与安全管理的装置能够从各种进入点连上网络, 这种发展趋势更加深了网络病毒的危害。例如, 近期发生的蠕虫 Sasser、Agobot 病毒等, 以极快的速度攻击微软操作系统的弱点, Agobot 同时更将病毒原始码公布在 Internet 上, 其传播速度及潜在的危险性都已达到史上最高的境界。它具有黑客利用后门程序的特性, 可以在受保护的共享目录区, 植入病毒文件, 开启一个 IRC 服务, 让远程的黑客可以随意操控受感染的计算机。根据公安部公共信息网络安全监察局 2003 年中国计算机病毒疫情调查技术分析报告显示, 在 2003 年以来, 计算机通过光盘、磁盘等存储介质传播的比例明显下降, 而通过网络下载和网络浏览感染病毒的数量增幅最大。通过电子邮件传播的比例也有所上升。计算机病毒网络化的趋势愈加明显[1]。

同时, 随着电子商务的在企业中越来越广泛的应用, 网络安全问题的重视程度也已被企业提高到前所未有的高度。从最早的防毒卡到单机防毒软件、网络版防毒产品, 再到防毒墙, 这些杀毒产品的迅速升级无不展示着人类对反病毒的努力和决心。面对计算机病毒日益严重的威胁, 反病毒技术和产品也在不断地更新, 各路厂家逐鹿中原, 而未来的企业防毒之道将会是怎样? 代表杀毒软件的核心技术—杀毒引擎又将如何有效防御网络病毒, 是期望网络安全的人们最关心的问题。针对目前企业网络安全的现状, 企业对计算机网络病毒软件的要求及焦点已主要集中在以下 5 个方面:

1 部署企业网络安全策略

企业内部的安全管理员为了实现全公司的安全管理, 可能在每台个人计算机上安装了反病毒程序、个人防火墙或入侵检测系统等各种形式的安全措施, 但是由于人员所限, 很难对所安装的措施进行有效而持续的管理。个人安全管理是企业网络安全比较突出的薄弱环节。因此杀毒软件对个人安全管理的策略也是企业非常关注的焦点。公司内部的个人计算机安全, 不仅是只影响个人的计算机环境, 因为面对日益复杂而肆虐的安全威胁, 即使只有一两台计算机暴露出薄弱环节, 也有可能很容易地导致公司内部全部计算机网络出现瘫痪, 此外统一的安全对企业安全威胁迅速进行处理也是有非常重要的意义。因此, 能够建立整个公司的安全策略是今后企业杀毒软件的必备条件之一。

一些知名的杀毒软件厂商已经注意到这一点, 开发出的产品在软件的管理员界面中, 可以对注册的所有计算机的状态和安全环境等信息一目了然地加以掌握, 甚至可以作到杀毒软件的远程强制安装, 并且对于注册的计算机还提供了一个同时应用统一策略的、易于操作的界面。

目前也有些其他厂家提出针对企业网络内部分段保护的概念, 即在各网段之间部署防毒检测点, 可以实现对网络中的病毒爆发流行进行实时监控,

* 收稿日期: 2004-03-27
作者简介: 胡斌昀 (1973 年生), 男, 硕士研究生; E-mail: fresh_yun@hotmail.com

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

对没有安装防病毒客户端、没有安装系统安全补丁的计算机进行隔离或将其重定向到相应的软件安装服务器上；在一台或若干台计算机因为染毒而引起病毒爆发、大量病毒数据包在网络中传播时，防毒监测点可以及时地将网络流量异常的网段隔离，并自动调用清除恢复服务操作，直至网络状态恢复正常。

2 提高杀毒引擎效率

在普通网络上的杀毒引擎与在大流量环境下的杀毒引擎完全不同，这也是为什么高端杀毒厂商与新进入者在市场定位上几乎没有矛盾的原因。首先，大流量环境下的杀毒引擎都是需要经过专门设计的，必须在保证杀毒效率的同时还要保证数据的高速传输，可为运行在网络上的多个引擎自动提供负载均衡能力，使网络流量均衡地分配，减少了单个引擎的压力，可以负担任何扫描量；其次，引擎的跨平台处理能力非常重要，因为大型企业由于历史原因具备各类数据平台，如 Unix、Solaris、Linux、Windows 等，引擎应该是与平台无关的；第三，必须具备统一管理能力；第四，大型企业一般具有网络存储设备，如果引擎不理想，将使病毒带入存储系统，这将是非常危险的。

3 网络安全威胁的早期发现与预警，变被动防守为主动预防

正如人体健康重在预防，计算机网络安全也应该以预防和早期预警为首。在公司内部网络受到威胁的时候，管理员可以通过软件提供的管理界面，只需单击鼠标，一系列应急病毒处理命令就可以及时下达到公司内部所有的计算机。另外通过管理人员界面，可以实现对中央服务器和个人用户代理程序的主要行为及状态信息进行实时监控。尤其是在病毒警报窗口中实时地对病毒发生状况进行报告，以此为根据，管理员可以及时采取安全应对措施。

当杀毒管理软件在判定蠕虫病毒正在通过网络传播或出现黑客威胁时，管理员可以依据预警信息，立即通过对附带的个人防火墙功能的控制，阻止共享文件夹的使用，或在更为严重的状况下切断个人计算机的网络连结，以迅速应对网络安全的威胁。此外，杀毒软件应该可以自动实现网络远程杀毒与系统修复，尽快恢复受感染文件，降低企业感染病毒后的损失。

目前一些知名厂商的杀毒软件都已内嵌漏洞扫描工具，可以针对 Windows 系统存在的“系统漏洞”和“安全设置缺陷”进行检查，并提供相应的补丁下载和安全设置缺陷自动修补的工具。但此方面的功能还不尽完善，扫描的对象主要是针对本地主机。未来的企业杀毒软件还应支持网络扫描，以及对数据库漏洞的扫描。管理员可以根据这种主动式网络漏洞扫描的报告，即时修补企业安全隐患，大幅减少漏洞数量，不给黑客和病毒留有可乘之机。

4 强化控制垃圾邮件和带病毒邮件的查杀功能

针对 2003－2007 年间的防病毒、防垃圾邮件以及内容过滤等市场的发展趋势，美国 Radicati 集团日前发表的一项调查报告预测，到 2007 年病毒造成的经济损失将超过 750 亿美元。欧洲防毒厂商 Sophos 在去年侦测到近千种新病毒、病虫及特洛伊病毒，其中有九成以上是用电子邮件作为主要的扩散方式，再利用中毒计算机中的通讯簿数据将病毒传播出去。以最近在网络上肆虐的 Sobig-Worm 为例，Mail2000 电子信箱每天都会扫到大约 30 万封的 Sobig-Worm 病毒信件，由此可见病毒邮件问题的泛滥程度。

电子邮件已经成为计算机病毒传播的主要媒介，其比例已占到所有计算机病毒传播媒介的 56％。由于电子邮件可以附带任何类型的文件，因此，所有类型的计算机病毒都可以通过它来迅速传播，与此同时，大量泛滥的垃圾邮件也会和病毒邮件一样，会给用户带来麻烦和一定的经济损失。所以加强控制垃圾邮件和带病毒邮件的查杀功能，是切断网络病毒传播的必要和最有效的手段，也是用户对杀毒软件实力的主要评测点。

针对以上企业网络安全中存在的问题，以及人们需求和认识的不断提高，目前的杀毒市场已上演一场全新的变革。各杀毒软件厂商也纷纷展开了激烈的竞争，不断推出功能更新更强的版本，防毒不仅只在终端机上演绎，在工作站、服务器、邮件服务器及网关处都能看到。日趋激烈的市场竞争，需要厂商及时洞察市场发展的趋势，不断的提升产品性能。

参考文献：

[1] 刘宏伟. 防毒墙之“矩阵革命”[N]. 中国计算机报，2004－02－16

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

The Trend Analysis of Enterprises Anti-virus Software

HU bin yun
(Software Research Instiute, Sun Yet-sen University, Guangzhou 510275, China)

Abstract: Facing to threats by network virus danger at present, only update anti virus engine is not enough to help all enterprises users. It's more important how to set up a whole effective Website System Security Professionals according to different characters of enterprises. The author works in front line and well-known what enterprises needed and the focus of anti virus software people concerned. He dedicates to analyze further trends of development of enterprises anti—voris spftware.

Key words: network virus; antivirus engine; security scan; early-warning; virus email; spam email

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net