2007年 IT 通讯总盘点系列报道杀毒软件篇

回顾 2007 年的电脑病毒及查杀领域，从春节前后的熊猫烧香，到电脑被放灰鸽子；从 ANI 漏洞到 MSN 的相片也会传毒；从天才儿童小浩到 U 盘全面封杀；电脑病毒迅速地繁殖。与此同时，瑞星、趋势科技、赛门铁克、江民、金山、等诸多国内外的杀毒软件厂商也纷纷拿出“看家”本领，来维护整个业界的安宁。而特别值得我们深思的是，我们真的能用今天的子弹打中明天的敌人？

2007年新增电脑病毒36.3万种！

专家指出：病毒靠“防”不靠“杀”

07年新病毒 36.3 万余种 “U 盘寄生虫”为“毒王”

日前，记者从某权威反病毒中心提供的数据获悉，截止到 2007 年 12 月 31 日，共有 36.3 万余种新病毒被截获，较去年全年增长 601%。根据全球病毒监测网(国内部分)、病毒预警中心、客户服务中心等多个部门联合监测统计，截止到 2007 年 12 月份，病毒累计感染计算机 34414793 台，其中 78% 以上的病毒为木马、后门病毒。监测数据还显示，利用微软系统自动播放功能传播的 Autorun （U 盘寄生虫）病毒感染率居高不下，全年高居病毒排行榜榜首，“U 盘寄生虫”也因此成为 2007 年年度“毒王”；从 2007 年下半年开始，ARP 病毒开始发威，众多企业局域网感染了 ARP 病毒，ARP 病毒由于其发作的时候会向全网群发伪造的 ARP 数据包，一台机器中毒，就可能导致整个局域网瘫痪，严重影响了企业网络的正常运行，ARP 病毒也因此被多家权威机构评测为 2007 年十大病毒之亚军。

“网游大盗” 病毒变种最多

除了 “U 盘寄生虫”“ARP 病毒”成为 07 年的头等和二等“通缉犯”外，“网游大盗” 病毒明显地成为了整个 2007 年繁殖种类最多的病毒之一。“网游大盗”变种 hwd、“网游大盗”变种 i-fy、“网游大盗” 变种 kwr、“网游大盗” 变种 gdt 等诸多变种病毒的存在，已严重地影响了整个互联网的安全性。

据了解，“网游盗号”病毒自 2006 年就一直位居十大病毒之列，进入 2007 年更是不断变种，频频发作，今年六七月份更是进入病毒发作高峰，众多网络游戏玩家反映游戏账号、密码被盗。国内最著名的安全软件瑞星科技副总裁毛一丁先生分析表示，之所以有这么多“网游大盗”变种病毒的存在，主要是这些病毒的制造者们想通过此途径获得一些经济方面的价值，而这也正是当前及未来病毒出现的重要特征。

时间差的存在 让“主动防御”呼之欲出

在病毒数量日增、种类繁多、传染迅速的同时，若干病毒感染者对病毒更是谈之色变、深恶痛绝。小到数据丢失、重做系统，大到网络整体瘫痪、产生重大经济损失等等。“各种电脑病毒的存在已严重地影响了整个互联网的安全。”

对此现状，各大安全厂商也纷纷使出看家本领，针对各种病毒拿出了自己不同的解决方案，可很多用户发现恶意程序的快速传播相比反病毒数据库的更新升级总是落后一拍。因为相对于新病毒，传统病毒特征码技术必然需要先截获病毒再升级病毒库的过程，虽然现在反病毒厂商的反应机制足够快，但从截获用户升级到最新病毒库必然存在一个时间差，这还不包括许多因为互联互通的问题导致无法及时升级的因素。基于这一因素，电脑用户更需要一种能防范于未然的方法，一种能够在未升级病毒库的情况下，就可以有效防范和处理病毒的技术和产品，而“主动防御”就明显地成为了诸多电脑使用者及各大安全厂商关心的重点。

“主动防御” 病毒靠“防”不靠“杀”

何谓“主动防御”？业内人士表示，主动防御不仅仅是一种技术、一种功能，它需要达到一系列的标准，才能被称为“主动防御”。也正因为主动防御技术的这个特点，现在涉足主动防御领域的各家厂商对 “主动防御”产品都有自己不同的看法。瑞星科技副总裁毛一丁先生表示，可自动识别、明确报出未知病毒并自动清除才是真正的“主动防御”产品。似是而非、含糊不清的监控报警系统，肯定不是用户需要的“主动防御”产品。趋势科技的安全专家建议，通过智能安全防护，实时准确地检测已知和未知威胁并识别网络威胁的来源，让所有的网络威胁清晰地完全暴露出来，以便于有的放矢地解决问题就是“主动防御”。赛门铁克方面表示，主动防御在封锁可疑威胁之余，会更重视使用者体验，例如在遇到可疑威胁时能自行判断、不去询问使用者，且只封锁有危害的程序代码，而非整个网页，让威胁被阻挡之余，使用者仍能获得所需信息。“尽管不同的安全厂商对主动防御的认识不一，但能以更加主动而积极的姿态来迎接病毒“漫天飞” 的世界，是整个 2007 年杀毒软件最大的进步。” 多位业内人士进一步分析，安全隐患的加重和人们风险意识的提升使得主动防御的需求飞速增长，基于快速反应技术的反病毒保护要求也会越来越高。

■相关新闻

主动防御的未来趋势

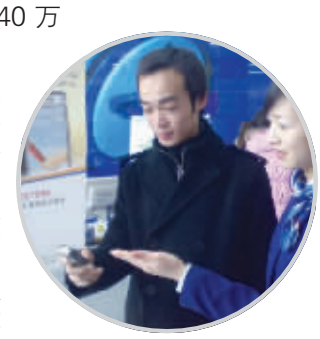
主动防御已成为当前杀毒软件行业最受关注的话题，那主动防御有怎样的未来趋势？

业内人士表示，在未来几年主动防御市场会出现更多比以往防御更积极的技术，但随着不安全的事件比例增加，和各种应用的成熟与规范化，真正实现主动防御不在于识别不安全的信息如何发展，而在于如何准确地识别安全的信息，除了安全地信息之外的其他信息都是不可信的、不安全的。只有这样才是真正意义上的主动防御。但相当长的时间内，主动防御的思路和被动防御的思路是相互补充、长期共存的。

快报记者 徐勇

宿迁奥运火炬“手机舵手”进社区

全省参与数量突破 340 万



已进入 2008 奥运年，随着北京奥运会的一步步临近，日前，奥运火炬彩信传递如火如荼。宿迁移动近日展开了 “奥运火炬手机舵手”进社区的活动，社区的居民们抢发彩信，争当“火炬手机舵手”。以市民这样的热情参与，昨天全省的参与数量已经突破 340 万。

据了解，为了让更多的市民了解奥运，为奥运做贡献，宿迁移动公司组织了客户经理、优秀营业员走进社区，近距离宣传“奥运火炬彩信传递”活动，让广大市民了解奥运知识，亲身体验奥运火炬 “手机舵手”的激情。

在沭阳，工作人员到各大社区聚积地宣传奥运知识，在社区广场的显眼位置放置大型宣传牌，客户经理与优秀营业员还手把手帮助市民转发 “奥运火炬彩信”。社区居民路过时，纷纷驻足观看，拿出手机发送 2008 到 1065799 获取奥运火炬传递种子，并发送给自己的亲朋好友。

居民张先生说：“奥运会是我们国家的大事情，我今天传了 20 多条出去，我感觉我们有义务为奥运做贡献。当‘奥运火炬彩信传递手机舵手’，我非常自豪！”

除了进社区，宿迁移动还开展了主题为 “喜迎 08 奥运，共传公益彩信”的系列大型户外宣传活动。活动分为三个环节，奥运知识有奖参与、公益彩信抢发和奥运彩信比比看，现场气氛热烈，市民纷纷参与。在泗洪西大街沟通 100 店的活动中，围观的群众超过了 400 人，一个小时的时间就传递了 700 多条奥运火炬彩信。

从昨天的江苏移动彩信平台显示看。截止到昨天上午 9 点，全省参与数量突破 340 万，参与用户超过 152 万人，这个数字还在不断增长中。

[参与方式]

用户参与传递奥运火炬彩信可以发送短信“2008”到“106587999”去主动申请种子彩信后转发，也可以直接将亲友发到自己手机上的奥运火炬彩信直接转发。只要发送的对象成功接收到了彩信，系统就会回复一条参与序号给发出者。序号数量达到 50 万后，主办方将在公证处的公证下进行抽奖。收发彩信方面的问题移动用户可以咨询 10086。

快报记者 赵丹丹

瑞星反病毒反木马一周播报

本周病毒：

“VB 破坏者变种 N (Harm.Win32.VB.n)”

警惕程度：★★★

这是一个破坏性程序。病毒运行后会在系统目录下建立文件名为：SDGames.exe 的病毒文件。病毒查找电脑中的所有脚本文件和可执行文件，并在这些文件中添加病毒代码，使其运行后即可打开指定的网页。病毒修改系统，使注册表和任务管理器以及系统防火墙等失效，同时修改系统时间，试图关闭多种杀毒软件，给用户带来很大的安全威胁。病毒具有映像劫持功能，可以在用户打开多种应用程序的同时使病毒程序运行。病毒将自身复制到 U 盘，并以此传播。

[专家建议]

1、养成良好的上网习惯，不去点击不明网页和可疑邮件；2、打开 Windows 自动更新，及时安装最新系统补丁，避免病毒通过系统漏洞入侵电脑；3、安装瑞星杀毒软件 2008 版，及时升级，并定时进行全盘查杀病毒；4、开启瑞星杀毒软件 2008 的“账号保险柜”，其主动防御技术可自动屏蔽木马、病毒常用的多种恶意行为，有效防止账号密码被盗窃；5、使用瑞星卡卡助手 2008 的 U 盘防护功能，阻止病毒通过 U 盘传播。