

# 网络环境下恶意软件问题研究

陶书志

(华中师范大学信息管理系 湖北武汉 430079)

**摘要** 分析了治理恶意软件过程中存在的问题,并提出了建设性对策。

**关键词** 网络环境 恶意软件 流氓软件 对策

近年来,随着信息技术的飞速发展和普及应用,恶意软件(俗称“流氓软件”)肆意横行。据英国安全软件厂商 Sophos 的数据显示,2007年3月份全球恶意软件中有35.6%源自中国(含香港),而美国“贡献”32.3%,中国已经取代美国成为全球最大的恶意软件基地。恶意软件的泛滥严重威胁着网络社会的和谐健康发展和广大网民的合法权益,已日益引起人们的关注。因此,加强对恶意软件问题的研究,认真分析其存在的问题,并提出有效对策,对维护网络安全、推动我国互联网产业的持续、快速、健康发展以及保护广大网民的合法权益都具有重要现实意义。

## 1 恶意软件的概念

恶意软件是伴随着互联网的出现,且在2001年以后出现的新生事物。它不像计算机病毒那样,自身具有或使其它程序具有破坏系统功能、危害用户数据、不断自我复制的明显攻击性,但它通过强行入侵用户电脑、频繁弹出广告、无法卸载等恶意行为给用户带来实质危害。从技术上讲,恶意软件包括恶意广告软件、间谍软件、恶意共享软件等,它既不属于正规商业软件,也不属于真正的病毒;既有一定的实用价值,也会给用户带来种种干扰,处在合法商业软件和电脑病毒之间的灰色地带。中国互联网协会将“恶意软件”定义为在未明确提示用户或未经用户许可的情况下,在用户计算机或其他终端上安装运行,侵害用户合法权益的软件,但不包含我国法律法规规定的计算机病毒。

## 2 恶意软件的分类及危害

恶意软件在巨额经济利益的驱使下日益泛滥,所造成的灰色产业链相关市场规模已达到10亿元。据中国互联网协会统计数据显示,我国目前有130多种恶意软件通过互联网传播,2006年上半年新型恶意软件受害用户数量在历史上首次超过病毒,成为互联网第一大公害。新浪网、中国反流氓软件联盟以及互联网实验室最近的调研数据也一致显示,98%以上的网民都受到过恶意软件不同程度骚扰,受害面之广令人担忧。恶意软件从2001年在我国出

现以来,先后经历了“恶意网页代码”、“插件推广”、“软件捆绑”和“恶意软件病毒化”4个阶段。根据恶意软件的特征、危害及入侵对象,困扰和危害广大计算机用户的恶意软件主要分为以下几类:

### 2.1 广告软件(Adware)

指未经用户允许,下载并安装在用户电脑上,或与其他软件捆绑并通过弹出式广告等形式进行商业广告宣传的程序。此类软件除正常下载功能外,往往会强制安装并无法卸载,在后台收集用户信息牟利,危及用户隐私,并且频繁弹出广告,消耗系统资源,使其运行变慢等。例如,用户安装了某下载软件后会一直弹出带有广告内容的窗口,干扰用户正常使用电脑。还有一些软件安装后会在IE浏览器的工具栏添加与该软件功能不相干的网页链接图标,普通用户一般很难清除。

### 2.2 间谍软件(Spyware)

指一种能够在用户不知情的情况下,在其电脑上安装“后门程序”收集用户信息的软件。间谍软件在后台运行,通过“后门程序”收集用户隐私数据和重要信息,然后发送给互联网另一端操纵者——黑客、商业公司等。这些“后门程序”甚至能远程操纵用户电脑,组成庞大的“僵尸网络”,其危害远远超过传统病毒,成为目前互联网最大的安全威胁。例如,某些软件会获取用户的软硬件配置,并发送出去用于商业目的。

### 2.3 浏览器劫持(Browser Hijack)

指一种恶意程序,通过浏览器插件、BHO(浏览器辅助对象)、DLL(动态链接库)插件、WinsockLSP等形式对用户浏览器进行篡改,使用户浏览器配置不正常,被强行引导到商业网站。用户在浏览网站时会被强行安装此类插件,普通用户根本无法将其卸载,被劫持后,用户只要上网就会被强行引导到其指定网站,严重影响用户正常上网浏览。例如,用户在上网时,一些不良站点会频繁弹出安装窗口,迫使用户安装某浏览器插件,甚至根本不征求用户意见,利用系统漏洞在后台强制安装到用户电脑中。这种插件还采用不规范的软件编写技术(此技术通常被病

毒使用)来逃避用户卸载,往往会造成浏览器错误、系统异常重启等。常见的浏览器劫持症状有:访问正常网站时被转到恶意网页、当输入错误的网址时被转到劫持软件指定的网站、IE浏览器主页/搜索页等被修改为劫持软件指定的网站地址、不能打开IE浏览器选项卡等。

#### 2.4 行为记录软件(TrackWare)

指未经用户许可,窃取并分析用户隐私数据,记录用户使用电脑习惯、浏览网络习惯等个人行为的软件。这类软件危及用户隐私,可能被黑客利用进行网络诈骗。例如,一些软件在后台记录用户访问过的网站并加以分析,有的甚至会发送给专门的商业公司或机构,此类机构据此窥测用户爱好,然后根据用户爱好进行相应广告推广或商业活动。

#### 2.5 恶意共享软件(Malicious Shareware)

指某些共享软件为了获取利益,采用诱骗、试用陷阱等方式强迫用户注册,或在软件内采用不正当捆绑各类恶意插件,未经允许就将其安装到用户计算机上,并利用一些病毒常用的技术手段造成软件很难被卸载或采用一些非法手段强制用户购买的免费共享软件。这类软件通过使用试用陷阱强迫用户注册,否则可能会丢失个人资料等数据,软件集成的插件可能会造成用户浏览器被劫持、隐私被窃取等。例如,用户安装某款媒体播放软件时会自动安装其他与播放功能毫不相干的软件(如搜索插件、下载软件)而不给明确提示,并且用户卸载播放器软件时不会自动卸载这些附加安装的软件;还有一些软件,如某加密软件,试用期过后所有被加密的资料都会丢失,只有交费购买该软件才能找回丢失的数据。

### 3 治理恶意软件存在的问题

#### 3.1 立法滞后

恶意软件涉及到知识产权法、反不正当竞争法、民法、刑法等许多复杂的法律问题,立法难度较大。目前在国外许多国家都先后颁布了惩治恶意软件相关的法律法规。例如,2004年美国犹他州第一个通过针对恶意软件的法案《Spyware Control Act》,加州在2005年也生效一部,据全美洲立法委网站显示,到2006年10月份美国已有18个州通过相关的立法,至少还有18个州正在讨论或拟定相关法律,这一法律的出台对于净化美国互联网环境起到了积极的作用;欧盟从打击计算机犯罪和保护个人隐私角度研究打击恶意软件的对策;印度、俄罗斯等国也把恶意软件列入刑事犯罪的附加条目。然而,在我国恶意软件如此猖獗的主要原因就是目前尚未出台关于治理恶意软件的法律法规,缺乏具体判断标准和依据而一直游走在法律模糊地带,导致恶意软件泛滥又缺乏法律监管的尴尬局面,对恶意软件侵犯用户合法权益的现象也无法从法律上找到支持和计算恶

意软件对用户造成的损失,形成法律上的盲点。例如,虽然中国互联网协会制定了恶意软件的定义和界定标准,但缺乏法律权威性,在2006年中国关于反恶意软件的一系列官司中,法院并没有采纳这一标准,全部败诉,原因只有两条:证据缺乏和法律依据不足。

#### 3.2 安全厂商的无奈

由于缺乏相关法律法规和国家执法部门许可,恶意软件界定模糊导致安全厂商处于一个尴尬地位,如果直接向恶意软件宣战,会引起法律诉讼。例如,2006年7月,奇虎与卡巴斯基联手推出奇虎“360安全卫士”免费软件,遭到雅虎中国诉讼,结果奇虎被法院判不正当竞争而败诉。因此,为了规避风险,安全厂商对自己进行角色定位,他们只负责找出用户电脑中恶意软件,而把卸载与否的权利留给用户,只要没有相关法律法规出台,他们处于一种观望态度。江民科技董事长王江民曾说:“如果有法可依,我们可以直接把符合条件的恶意软件加入病毒库,增强对恶意软件的查杀。”随着反流氓软件联盟等民间组织和瑞星、金山等安全厂商的一系列声势浩大的反恶意软件活动的展开,恶意软件的侵害行为有所收敛,取得了初步成效。但部分恶意软件仍然十分肆虐。从发展的态势看,要彻底根除恶意软件仍然还是一项长期而艰巨的任务。

#### 3.3 政府监管缺位

缺乏政府有效监管,是恶意软件肆意猖狂的一大原因。在与恶意软件斗争中,唱主角的不是政府管理部门,而是民间自发组织,来自政府层面的声音却处于“长期缺席”状态,政府监管实质上还处于真空地带。2006年,恶意软件数度被网民告上法庭,在民间力量的推动下,政府部门确立了恶意软件定义和认定标准,但没有上升到法律地位,缺少权威性,这无形中给恶意软件留下一定的生存空间,意味着整治恶意软件的过程将会更漫长。

### 4 有效治理恶意软件的建议

治理恶意软件应坚持“多管齐下、统筹兼顾、标本兼治”的方针,从立法、行政管理、行业自律、反恶意软件工具和网民教育等方面入手,形成治理恶意软件的长效机制,才能有效遏止恶意软件。

#### 4.1 加快立法步伐

法律是治理恶意软件、净化网络环境的重要保障。一些发达国家先后出台了专门针对恶意软件的法律,例如美国的《反间计算机间谍软件法案》(在美国国家一般把恶意软件称为“间谍软件”)。针对我国现状,要从根本上解决问题,必须积极借鉴国外立法经验,加快立法步伐。因此,国家立法机关要积极开展反恶意软件的立法研究,严格界定恶意软件的内涵及外延,明确恶意软件的判定标准,尽快出台具体

针对恶意软件的法律法规,为有效打击恶意软件提供法律依据。

#### 4.2 加强行政监管

由于法律的滞后性和被动性,所以仅依靠法律手段来抵制恶意软件是不行的,还必须充分发挥政府行政机关的作用。应对恶意软件,应积极借鉴国外治理经验,应加大惩罚力度,严格追究制作、传播恶意软件的相关法律责任,对制作、传播恶意软件的企业进行经济重罚。如2006年11月美国联邦贸易委员会(FTC)做出裁决,对原名180Solutions的Zango的广告软件公司罚款300万美元,原因是其引诱用户安装广告软件且无法卸载,而这正是网民通常所称的恶意软件。通过对制造恶意软件的企业进行高额经济处罚,从经济利益这个根本上治理恶意软件。同时,还必须加强对网络的有效监管。网络监管涉及到许多部门,因此,需要强化公安、工商和行政等部门之间的协调性,加强部门之间沟通协作,从而形成一个良好的治理模式,这是有效治理恶意软件问题的关键所在。

#### 4.3 建立行业自查自纠机制

在国家立法机关还没有出台应对恶意软件的法律法规情况下,一方面,发挥中国互联网协会作为一个非盈利性、全国性组织在治理恶意软件过程中的领导作用,在其制定的《恶意软件定义》、《抵制恶意软件自律公约》基础上,建立行业自查自纠机制,共同组织协会会员单位对照恶意软件的定义标准和自律公约,自觉开展自查自纠,培育网络道德,加强行业沟通协作,探讨有效抵制恶意软件模式,营造以自律促发展氛围,共同创建公平有序的市场竞争环境。另一方面,各软件和网络企业应规范软件开发行为,切实履行不制作、不传播恶意软件的承诺,向用户提供优质安全的产品,以实际行动抵制恶意软件,从而推进恶意软件治理进程。

#### 4.4 建立反恶意软件的社会监督举报机制

有效治理恶意软件,离不开全社会的监督。一方面,由中国互联网协会组织建立反恶意软件社会监督举报机制,动员全社会力量共同抵制恶意软件,设立专门的举报电话和邮箱,接受社会举报;同时,设立专门认证机构,对公众的举报进行认定。例如,互联网协会于2007年6月的公布“恶意软件定义”细则中公布了3家第三方恶意软件测评机构:信息产业部电信传输研究所、北京信息安全检测中心和北邮信息安全中心。对于被举报的恶意软件将督促其限期整改,逾期未予整改的,将向社会公布恶意软件的名称、制作者和传播者等并予以谴责。另一方面,充分发挥媒体的作用,深入开展反恶意软件的宣传

活动,及时报道恶意软件的发展动态,揭露恶意软件的卑劣行为,提高广大网民对恶意软件危害性的认识,激发更多机构和个人参与抵制和治理恶意软件,从而增强治理恶意软件的效果。

#### 4.5 研发恶意软件查杀工具

有效打击恶意软件对技术有较高的要求。以美国较著名的反间谍软件联盟(Anti-Spyware Coalition)和阻止不良软件联盟(Stop Badware Coalition)为例,通过与安全厂商、商业公司合作,从而获得强大的技术保障。就我国来说,安全厂商在清理恶意软件行动中发挥了不可或缺的作用。其中,国内最早进行反恶意软件行动的瑞星尤为典型,瑞星在瑞星卡卡助手中应用碎甲等多项反病毒核心技术,可以彻底查杀目前流行的400余种恶意软件。因此,有效治理恶意软件,要紧密依赖技术进步,同时加强安全厂商之间的沟通协作,有效解决技术标准制定、恶意软件判断等关键性问题,及时推出专业的恶意软件清理工具帮助用户有效清除恶意软件,从而为用户提供有效的技术保障。

#### 4.6 提高网民自我保护意识

目前,由于恶意软件还占有相当大的市场,因此在短时间内很难在我国互联网上彻底消失。当务之急是一方面要提高广大网民的觉悟,树立维权意识,在受到恶意软件侵犯时,勇于站起来拿起法律武器来捍卫自己的合法权益,及时运用反恶意软件工具来清除,遇到个人清除不掉的恶意软件,可以上报给反病毒厂商处理,从而对制造恶意软件的公司形成一种制约力量。另一方面,网民要改善自身的网上行为习惯,诸如不到来源不安全的网站下载软件,不开启来源不明的电子邮件以及经常更新密码,上网时应采用“杀毒软件+个人防火墙+安全助手”的立体防御体系,抵御恶意软件的侵害,增强自我保护能力,从而有效治理与遏止恶意软件问题。

#### 参考文献

- 1 高海燕. 中国取代美国成为恶意软件头号基地. <http://news.driverchina.com/Html/news/soft/094648306.html> (2007-6-10)
- 2 武俊生. 计算机的安全及防范措施. 电力学报, 2006(4)
- 3 郭翔鹤. 中国互联网协会正式公布恶意软件官方定义. <http://it.sohu.com/20061109/n246279922.shtml> (2007-6-10)
- 4 王一曦. 流氓软件:泛滥于法律空档. 中国社会导刊, 2006(21)
- 5 叶秀敏. 恶意软件有多恶. 沿海企业与科技, 2007(1)
- 6 王群. TCP/IP 管理及网络互联. 北京: 人民邮电出版社, 2004

(责任编辑:彭 奋 姜雪榕)