2010–2011
中国互联网安全研究报告

目录

第一章、2010 互联网安全威胁五大特征 3
一、 病毒木马呈现“互联网化”趋势，高度依赖联网传播 3
二、 80%的病毒传播渠道被病毒集团所操控，危害更深入 4
三、 网络购物人群成为入侵重点对象 5
四、 新型木马不断出现 破坏性超传统木马 10 倍 6
五、 病毒木马与钓鱼网站相互“勾结”越发突出 6
本章小结 6
第二章、2010 互联网安全威胁整体描述 7
一、 2010 年新增安全威胁描述 7
1、病毒木马新增数量以及类型 7
2、新增网络安全威胁：以“钓鱼网站”为首的互联网犯罪 7
二、 病毒感染的分布特征——互联网、经济双发达地区成重灾区 9
1、病毒感染的地区分布及感染数量 9
2、病毒传播的主渠道——传播渠道的互联网化 10
三、 病毒主要侵害的高危人群——互联网热门应用成主要目标 11
1、网购类人群—数量小成功率高，经济损失严重 11
2、下载类用户——覆盖面最广的受害用户群体 11
（1）网络视频爱好者 11
（2）盗版游戏爱好者、游戏外挂使用者 12
（3）热门软件爱好者 12
（4）电子书爱好者 13
3、偏好使用 U 盘交换文件的用户——数量在逐步减少 14
本章小结 14
第三章、2010 年网络安全威胁排行榜 14
一、2010 年十大典型的钓鱼网站 14
二、2010 年十大典型病毒 14
1、“极虎”病毒 14
2、“女人必看”类 qq 盗号木马 15
3、“杀破网”病毒 15
4、“鬼影”病毒 15
5、浏览器主页篡改病毒 15
6、牛皮癣病毒 15
7、数字大盗病毒 15
8、“伴随者”木马 16
9、“暴风 1 号”病毒 16
10、“震网”病毒 16
第四章、2011 年互联网安全趋势预测 16
一、 网购木马将集中爆发 16
二、 针对社交网络的攻击呈现上升趋势 17
三、 针对移动互联网的攻击加剧 17

第一章　2010 互联网安全威胁五大特征

一、病毒木马呈现“互联网化”趋势，高度依赖联网传播

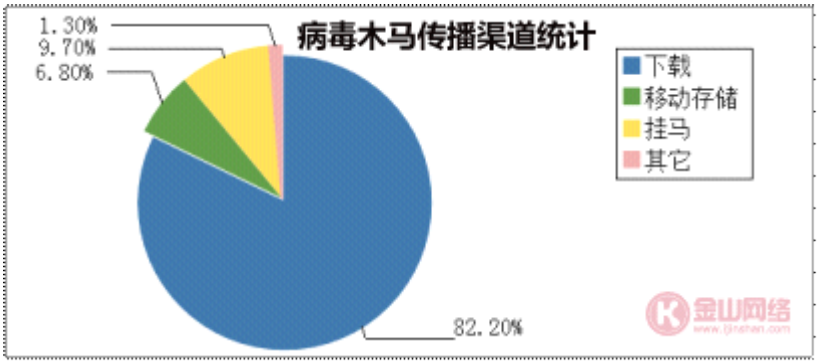
1.　计算机脱离互联网的机会越来越少

从网民的使用场景看，互联网宽带已经普及到中西部地区，网民数量超过4亿，3G 网络、Wi-Fi 城市的建设正如火如荼，计算机脱离互联网的机会越来越少。移动互联网、云存储、智能家电、车载3G 设备、物联网，互联网将要连接的不再是 PC，而是生产、物流、消费，未来的网络将无所不在。

据 CNNIC 最新发布的第27次中国互联网络发展状况统计报告显示，截至2010年12月底，我国网民规模达到4.57亿，宽带普及率接近100%。主流计算机用户几乎已经通过各种渠道连接上了互联网。

2.　93.2%的病毒木马依赖互联网手段进行传播

2010年数据显示，病毒木马的传播途径中，有93.2%直接依赖互联网完成，其中有82.2%是通过下载行为感染计算机。也就是说，脱离互联网环境，病毒木马即失去感染计算机的主要机会。



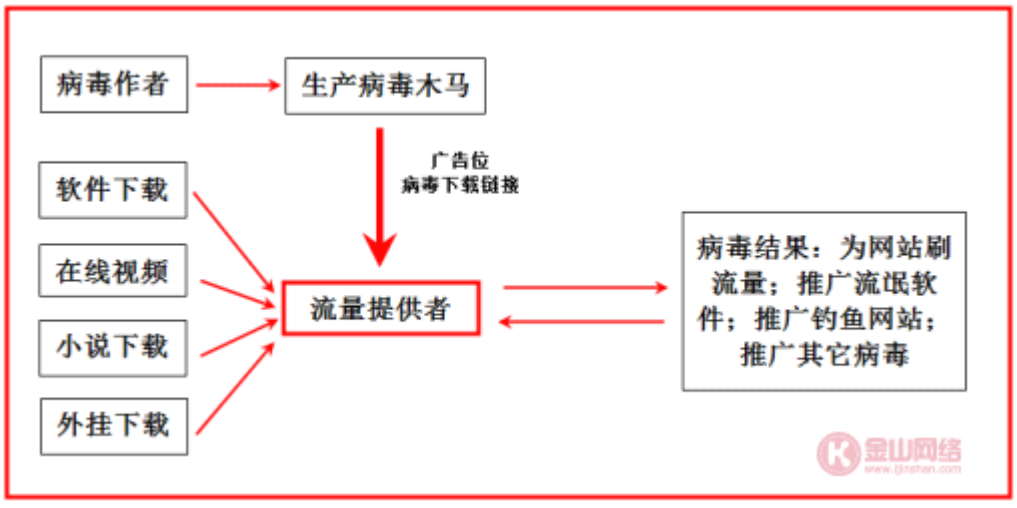
3.　网络畅通是病毒传播者获得非法利益的必要前提

病毒木马感染的最终目的是篡改浏览器、弹出广告、分发盗号木马、推广流氓软件来赚取推广分成；通过推广钓鱼欺诈网站来诱骗用户上当受骗；网购木马通过劫持篡改网购定单，强行将网民在线购物的款项转到自己的帐户。病毒程序要实现这些目的，必须要在网络畅通的情况下才可能做到，网络畅通是病毒传播者获得非法利益的必要前提。

病毒感染的目的	联网时	断网时
1.篡改浏览器首页，为某些商业网站刷流量	必须联网，才能令网民访问指定的首页	浏览器打不开
2.弹出钓鱼网站、广告网页	联网时，才能按服务端的指令弹出指定的网址。必须联网，钓鱼网站弹出才会有内容。	无法完成业绩
3.网购木马篡改交易单	必须联网，才能进行网上购物。只有购物之时，才可能发生交易劫持	无法断网购物
4.后台自动下载安装某些软件	必须联网才能完成指定程序的下载	无法断网下载。
5.盗窃网民个人信息、盗窃网游帐号	必须联网，才能将偷到的东西发到指定服务器。必须联网，才能登录网络游戏。不登录网游，木马不可能知道游戏帐号密码	断网，无法游戏，更不能盗号。

二、80%的病毒传播渠道被病毒集团所操控，危害更深入

金山网络云安全系统已经可以精确的统计出病毒传播的最初来源，分析出病毒木马通过网络下载传播的完整路径：



金山云安全系统在对病毒传播渠道长期跟踪中，根据病毒传播组织的技术特点对病毒下载链接进行自动监控。数据表明十大病毒集团控制了互联网上80%病毒下载通道。这些病毒集团传播病毒主要破坏行为包括：为某些商业网站（主要是中小网址导航站、不良网站、视频下载站）刷流量；推广一些商业软件（这些软件往往捆绑了各种插件，会篡改浏览器，弹出广告）；推广钓鱼网站，使中毒者上当受骗；推广其它病毒（主要是攻击网游盗号木马）。

据2010年4月中国互联网络信息中心 CNNIC 和国家互联网应急中心 CNCERT 联合发布的《2009年中国网民网络信息安全状况调查系列报告》显示，2009年，52%的网民曾遭遇网络安全事件，网民处理安全事件所支出的相关服务费用共计153亿元人民币。而这些病毒木马在给网民造成损失的同时，也在疯狂的获得非法利益，病毒产业的收益以百亿元计，这些总数不到50家的病毒集团获取的非法收益约占其中一半，领先的病毒集团一年可有数亿元的规模，令一般中小企业难望其项背。

1	6282	122	1.98%	[网站]http://...c14/Qvod.exe	危险
2	5580	523	10.34%	[网站]http://...l/QvodPlayer.exe	危险
3	5173	615	13.49%	[网站]http://...80/bofangqi/激情爽片成人电影.hta	危险
4	3896	1610	70.43%	[网站]http://...直接运行%20激情成人短片.hta	危险
5	2901	43	1.50%	[网站]http://...a03/QvodSetupPlus.exe	危险
6	2894	216	8.07%	[网站]http://...com.cn:55/yb/ybmd_myad_38967.exe	危险
7	2707	-22	-0.81%	[网站]http://...10/QvodSetup.exe	危险
8	2630	310	13.36%	[网站]http://...01/setup_0111.rar	危险
9	2508	173	7.41%	[网站]http://...m08/Qvod.exe	危险
10	2482	460	22.75%	[网站]http://...:8088/setup.rar	危险
11	2372	7	0.30%	[网站]http://...sa13/QvodSetup.exe	危险
12	2284	55	2.47%	[网站]http://...soft200.exe	危险
13	2270	139	6.52%	[网站]http://...Qvod_Player.exe	危险
14	2070	-5	-0.24%	[网站]http://...0/rz12/QvodSetupPlus.exe	危险
15	1917	-76	-3.81%	[网站]http://...php?bd=ccdu09987377497829388493384992	危险
16	1909	376	24.53%	[网站]http://...5see_a101.exe	危险

金山云安全系统已经建立了对十大病毒集团下载渠道的监控体系，能够第一时间发现新病毒木马，立即完成样本鉴定和 URL 识别，并通过云引擎分发给金山毒霸和金山卫士的用户，避免病毒木马入侵。与此同时，金山安全中心会优先完成此类病毒木马的破坏行为分析，发布完美查杀方案，帮助非金山产品的用户中毒后，能够使用金山毒霸或金山卫士完成病毒清除和系统修复。

三、网络购物人群成为入侵重点对象

从统计数据看，2009年新增病毒样本总量接近2000万个，2010年病毒样本总量下降了13%，约1798万个，这也是多年以来到病毒样本总量首次出现下滑迹象。其中的原因在于，2010年安全软件成功控制了网页挂马，致使病毒木马的传播锐减。

但与此同时，病毒集团开始谋求新的“互联网”转型，随着网络购物的发展，针对网络购物的安全威胁已经成为影响互联网安全的重要形式。在 2010 年，有近 28%的互联网用户遭遇过虚假钓鱼网站、诈骗交易、交易劫持、网银被盗等针对网络购物的安全攻击。

看起来技术含量不高的网络钓鱼，却让越来越多的网购人群深受其害。其中的原因，在于钓鱼网站的制作简单，投资少见效快。同时，传统安全软件对钓鱼网站的识别还不够及时、准确。

再加上网民的安全意识薄弱，疏忽大意普遍存在，而且一旦上当受骗之后，还存在电子取证难的问题，致使网络钓鱼的危害急剧飙升。2010年，病毒木马和钓鱼网站相互勾结、相互推广的情况也并不少见。

另据金山网络安全中心云网址鉴定系统统计数据显示，2010年1-10月，平均每天新增的与网络购物相关的钓鱼网站约为1500个。

四、新型木马不断出现　破坏性超传统木马 10 倍

以前，我们说到木马，大多是指那些盗号木马，盗号木马以窃取网游玩家的虚拟财产为目标。现在，随着互联网商业应用的不断拓展，病毒木马作者已经不屑于盗取虚拟财产。很多正常商业网站或商业软件的推广会提供丰厚的佣金，病毒木马传播者的目标就是强行修改用户系统配置，为这些商业网站带流量，或者使用流氓手段推广商业软件，再从商业公司赚取推广费。

2010年，中国互联网新增了两大类木马：绑架型木马、网购木马。在金山安全中心24小时监控的病毒传播渠道里，绝大部分样本属于绑架型木马。其特点是基本不改写系统启动加载项，而是会破坏一些广泛存在的系统组件，比如 DirectX 组件，输入法、声卡相关程序等等，当用户运行某个特定的程序时，病毒才会运行。

病毒的主要破坏是添加一些垃圾快捷方式，锁定用户浏览器，强迫用户浏览某些网站，中毒电脑无法简单修复这些破坏。金山网络为解决这些问题，专门对绑架型木马的破坏进行针对性的修复处理，用户可以使用金山急救箱或金山卫士快速修复来解决问题。

而网购木马更是病毒团伙互联网转型的一个杰作。该类木马技术含量高、一对一传播、破坏性强，用户在网络购物过程中一旦遭遇该类木马，被欺骗的可能性基本会在100%。

五、病毒木马与钓鱼网站相互“勾结”越发突出

同欺诈下载一样，钓鱼网站也是一种低技术含量的威胁，但网站采用的骗术却能屡屡得手。而数字大盗病毒实现了病毒技术和钓鱼网站近乎完美的结合，给网购用户构成严重威胁。大量病毒木马会在用户桌面弹出钓鱼网站的广告页面，用低价、中奖等诱饵，令网民上当受骗。

本章小结

2010年中国互联网网络安全威胁的最主要特征就是病毒集团的互联网转型，病毒木马的互联网特征越发明显，同时，病毒集团开始“分地盘”，十大病毒团伙控制近80%的病毒传播渠道。此外，伴随着互联网应用的日益深入，病毒集团的危害行为更加赤裸裸的以盗取经济利益为目的，病毒团伙与安全软件之间的技术对抗也更为激烈。

第二章　2010 互联网安全威胁整体描述

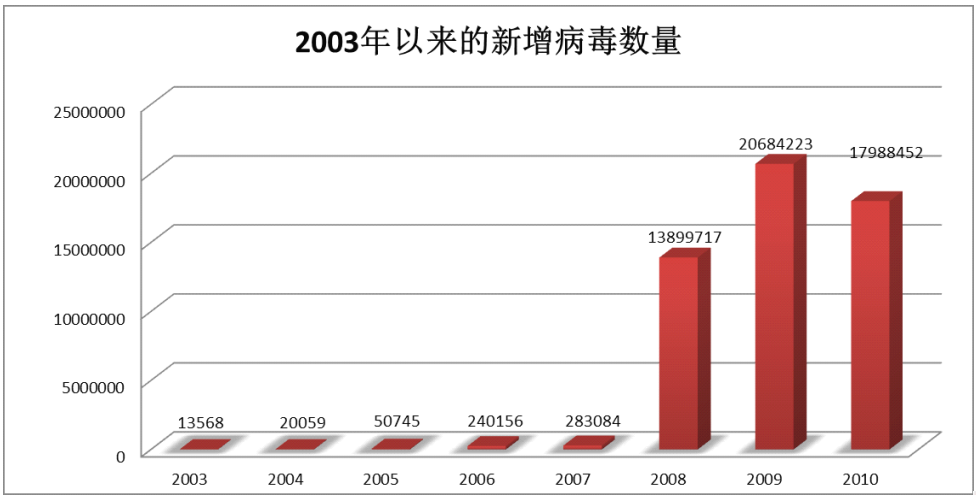
2010 年，中国互联网的病毒木马总体传播形势趋于平稳。病毒产业链日益成熟，国家有关法律法规持续完善，制造和传播计算机病毒的行为得到一定的遏制。与此同时，病毒集团开始谋求“互联网”转型，从新增病毒的种类、传播渠道以及危害等方面的情况来看，病毒木马的互联网化特征日益明显。

一、2010 年新增安全威胁描述

1、病毒木马新增数量以及类型

2010年，新增电脑病毒木马1798万余种，仅从病毒数量增长情况来看，病毒疫情趋于平稳增长态势，感染数量没有出现类似2009年的飙升。

伴随着互联网的发展，病毒不再单纯的以破坏用户系统，炫耀技术为目的，而更多的是以来互联网赚取钱财。木马作为病毒集团“互联网转型”的主要工具，是黑客实现经济利益的最直接手段。伴随着电子商务的发展，在经济利益最集中的互联网应用领域，如网络购物，木马的危害会越来越大，因此木马仍然在2010年病毒总数中占据绝对优势。从病毒种类的构成比例也可以看出，木马以85.4%的比例依然占据主流，而传统病毒仅占4.3%、蠕虫2.6%、后门程序7.7%。

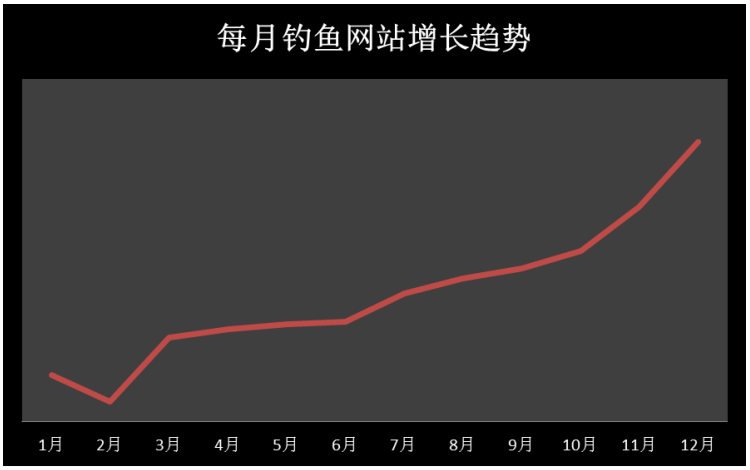


2、新增网络安全威胁：以“钓鱼网站”为首的互联网犯罪

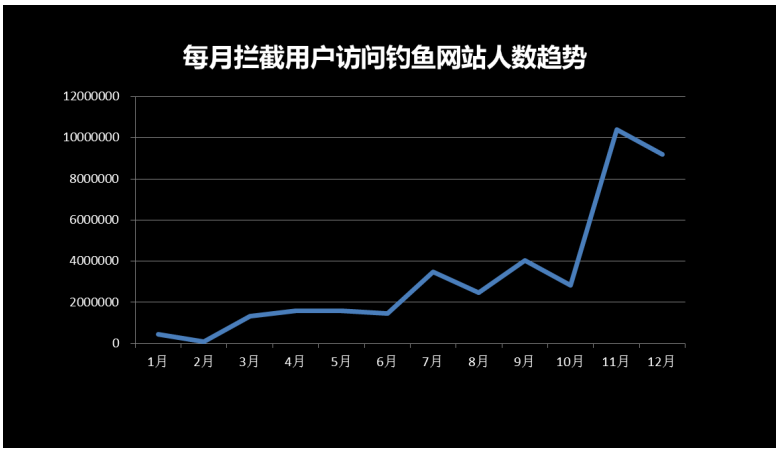
2010 年，除了传统的病毒木马之外，安全威胁的互联网化特征也越发明显。最突出的就是钓鱼网站。

钓鱼网站是病毒集团“互联网化”转型最明显的特征。钓鱼网站也是目前为止黑客所采取的最直接的获取经济利益的手段。而网络购物又是互联网上钱财最集中汇聚的地方，因此网购经济也在一定程度上催生了钓鱼网站的泛滥。

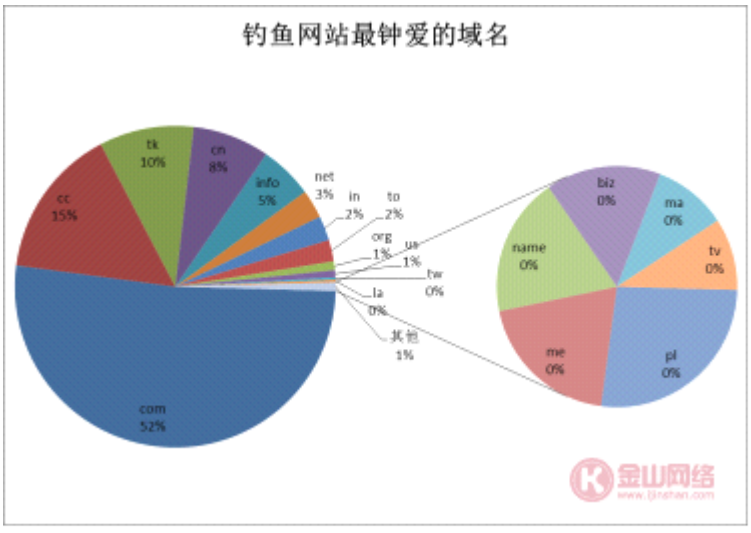
统计数据显示，2010年，新增钓鱼网站数量明显一路走高。

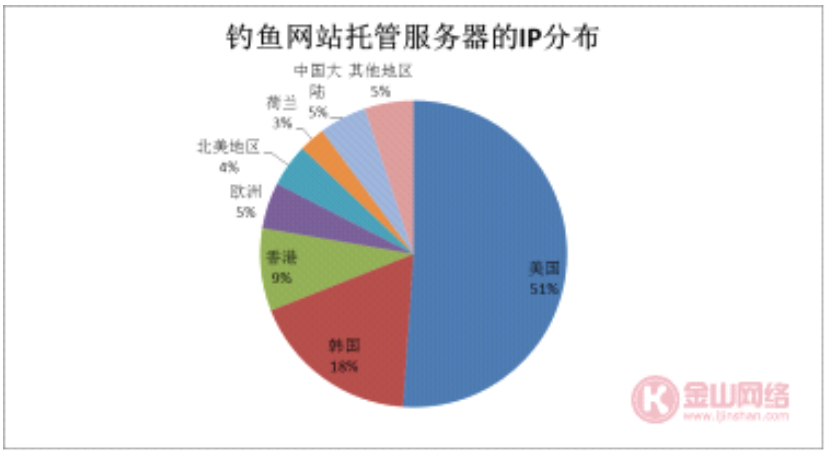


金山系列安全软件拦截网民访问钓鱼网站的次数也呈快速上升态势，在11月份达到峰值，总拦截量超过1000万次。

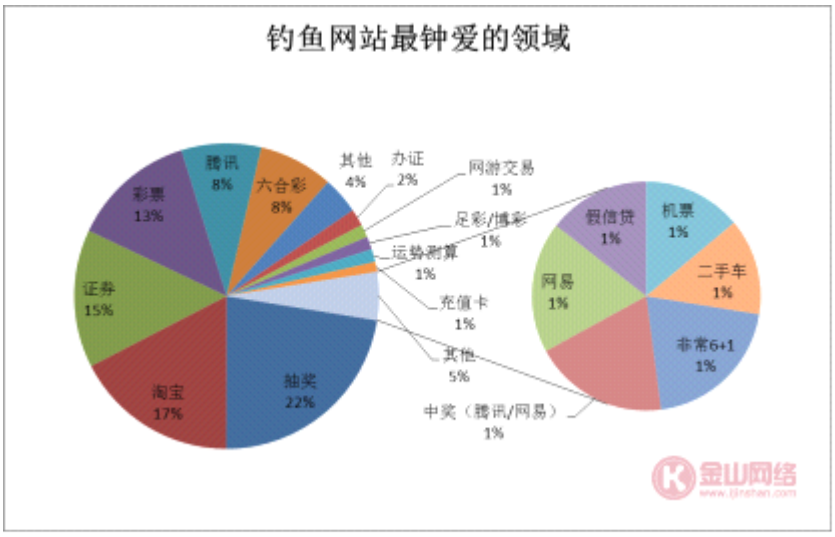


同时，多数钓鱼网站申请国际域名，服务器主要托管在海外，增加了有关部门依法打击的难度。





钓鱼网站最钟爱六大类欺诈内容，包括：各种抽奖（22%），购物类网站，如假淘宝（17%）、假彩票分析（13%）、非法的六和彩网站（8%），假腾讯网站（8%），假证券网站（15%）。而伴随着电子商务的发展，互联网上直接经济活动的增多，购物类钓鱼网站依然会不断增加。



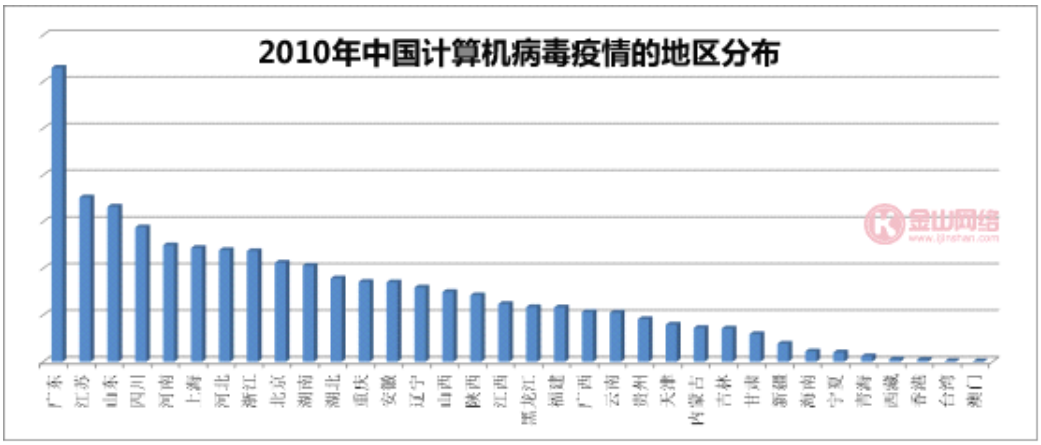
二、病毒感染的分布特征——互联网、经济双发达地区成重灾区

根据金山网络安全中心有关数据显示，在我国经济与互联网双发达地区依然是病毒木马侵害的重灾区。统计数据显示，广东、江苏等地区的病毒感染情况依然居高不下，同时，与2009年相比，上海、四川等地区的病毒感染情况有所上升。

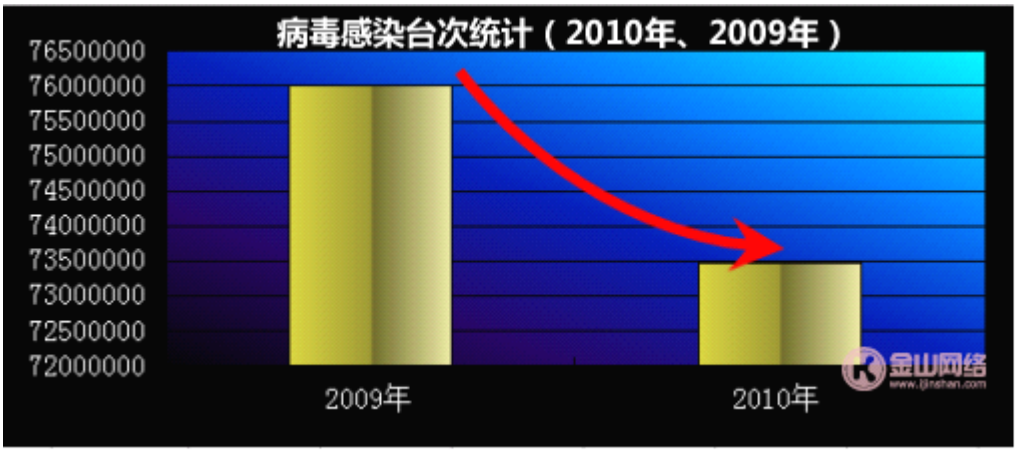
1、病毒感染的地区分布及感染数量

分31个省统计感染情况表明，广东、江苏、山东、四川、河南、上海、河北、浙江、北京、湖南这10个省份处于病毒感染数的第一梯队，占据感染总数的63%。这一数字可大致估计该地区计算机网络应用的普及程度。

2010 年中国计算机病毒疫情的地区分布示意图

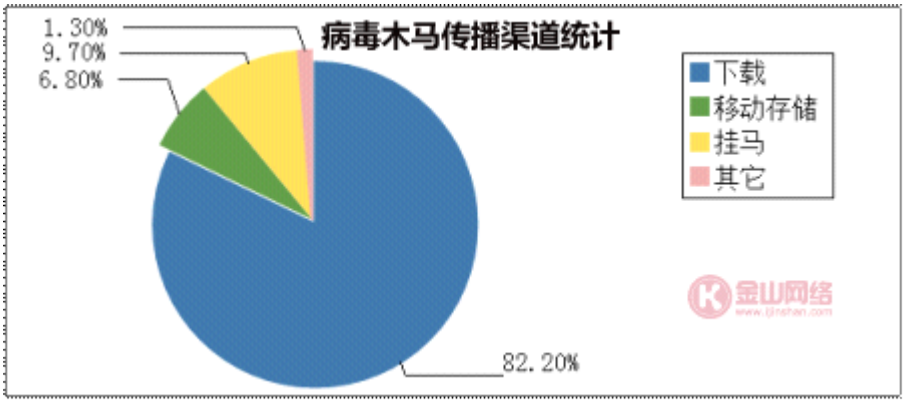


金山网络安全中心统计发现，2010年共发生计算机病毒感染事件约7300万台次，金山毒霸各产品及合作通道拦截病毒的报警达到82亿次。2009年，感染计算机病毒的电脑数量为7600万台次，从感染台次上看，2010年比2009年的情况略有减少。这对所有网民来说，是个好消息。



2、病毒传播的主渠道——传播渠道的互联网化

统计数据表明，93.2%的病毒传播渠道直接与互联网有关。通过 U 盘等移动存储介质传播的占6.8%。而这些 U 盘病毒也是先通过网络感染计算机，再感染中毒计算机上使用过的 U 盘，实现局部反复传播。病毒入侵后的主要破坏，如网游盗号、弹广告、篡改浏览器、下载流氓软件必须依赖于互联网的畅通。



据金山毒霸、金山卫士下载保护的拦截数据显示：在网民使用迅雷、QQ 旋风和浏览器直接下载的行为中，有10%的下载目标指向包含病毒木马的危险下载。这意味着，每十次点击下载的操作，可能会有一次将病毒木马下载到自己的电脑中。

三、病毒主要侵害的高危人群——互联网热门应用成主要目标

根据金山毒霸拦截网络威胁数据统计显示，诸如网购用户、网游爱好者、视频达人等人群是病毒团伙的主要目标，尤其是直接关乎经济利益的网络购物等上网行为更是成为了黑客的首要目标。

1、网购类人群—数量小成功率高，经济损失严重

因网购木马的特殊攻击方式，导致网购受害用户呈现总体数量小，但成功率高，经济损失严重的现象。根据目前截获的网购木马分析显示，病毒木马传播者为求自身安全，并没有使用可以让病毒短时间大面积传播的渠道，而是大多利用 QQ 或淘宝旺旺一对一的行骗，这种行骗方式成功率非常高，若本地安全软件没能及时拦截，受害者多半会遭受经济损失。另外，网购达人是钓鱼网站最主要的受害者。骗子往往先骗倒淘宝店主，再用店主的 ID 登录淘宝店，继续欺骗更多买家。

2010年出现的绑架型木马则是专门针对网购人群设计的，绑架型木马会通过篡改浏览器，锁定主页等方式，将用户的主页引导到其指定的网址导航站，通过修改用户桌面图标或收藏夹的网址，使用户防不胜防的掉入欺诈钓鱼的陷阱。

2、下载类用户——覆盖面最广的受害用户群体

（1）网络视频爱好者

这些网民喜欢看在线视频，有热门大片上映一定要先睹为快。与此同时，一部分专门分享盗版电影、热门影视剧、进口大片的网站成为毒源。

这些在线视频网站，会利用热门视频或不良视频分享为诱饵，吸引这部分网民上勾。在这些网站下载视频，无一例外，会被推荐安装一些专用播放器，这些专用播放器中，捆绑病毒的概率接近100%。

同时，在这些网站上，还会提供与视频浏览相匹配的大量广告链接，广告链接直接指向病毒下载地址。

（2）盗版游戏爱好者、游戏外挂使用者

游戏玩家的数量仍然庞大，盗号木马的传播主要依赖网页挂马这个通道，当网页挂马基本无效之后，盗号集团将传播渠道转移到那些伪装成游戏外挂的软件下载站或网盘中。病毒传播者会利用游戏相关论坛、贴吧以及游戏内的聊天频道，传播外挂、插件有关的消息，吸引玩家下载。部分外挂插件下载站的经营者也非常狡猾，这些站点在多数时间提供正常软件下载，但会在某个特定的时间将下载链接替换成病毒下载。

（3）热门软件爱好者

这部分网民对系统有较多的理解，能够主动寻找和尝试新软件，特别是一些破解、盗版的商业软件。但提供这些软件的下载站往往暗藏陷阱，提供非法软件下载的网站上，广告收入几乎是网站唯一的收入来源，这些网站的广告成为重要的病毒发布通道。小型软件下载站的广告位，几乎被病毒传播者所占据，一不留神点击到广告链接，下载的就是病毒。

（4）电子书爱好者

一些提供电子书下载的网站有稳定的流量和访客，某些热门下载可能被人为植入木马进行传播。

3、偏好使用 U 盘交换文件的用户——数量在逐步减少

统计数据表明，在学校机房、文印室、机关单位这些场景，U 盘病毒的危害高于一般网

民。著名的 conficker 病毒、超级工厂病毒，U 盘、移动硬盘均为其重要传播媒介。但伴随着安全软件 U 盘保护等安全功能的推出，U 盘用户感染病毒的几率也在不断下降。

本章小结：

2010年病毒集团正在进行着互联网化的转型，病毒木马的互联网化特征也更加明显，感染手段、传播途径，甚至攻击目标都依赖互联网进行，在断网情况下，病毒木马将无法完成入侵用户计算机实施流量劫持或者偷窃用户账号密码等目标。病毒木马的互联网化，将给安全软件提出更高的要求，如何在互联网时代提升安全综合能力，在充分保证用户上网自由的前提下，保障用户的安全。

第三章　2010 年网络安全威胁排行榜

一、 2010年十大典型的钓鱼网站

序号	钓鱼网站种类	占总钓鱼网站比例	相关钓鱼网站数量	访问人数统计
1	抽奖	22%	80 万个	1400 万次
2	购物	17%	68 万个	1000 万次
3	证券	15%	60 万个	900 万次
4	彩票	13%	52 万个	870 万次
5	假冒 QQ 中奖	8%	32 万个	762 万次
6	六合彩	8%	32 万个	650 万次
7	假药	1%	约 4 万个	400 万次
8	网游交易	1%	约 4 万个	320 万次
9	假信贷	1%	约 4 万个	240 万次
10	机票	1%	约 4 万个	186 万次

注：数据来源于金山云安全监测平台

二、 2010 年十大典型病毒

1、“极虎”病毒

集合各种病毒、木马、木马下载器、蠕虫特征于一体的病毒程序。该病毒会破坏杀毒软件，感染正常程序文件，伪造系统资源文件 usp10.dll 和 lpk.dll，并联网下载大量其他木马病毒。该病毒在2010年春节期间开始流行，日感染10万台 PC。

2、“女人必看”类 qq 盗号木马

该类病毒主要通过 qq 群共享和 qq 好友之间传播，文件名为“传统男人对老婆的5大不讲

理”或“女人必看”之类的压缩文件。该病毒假冒 DAEMONTools 数字签名，不注意查看签名属性会被骗。查看详细信息，会发现签名无效。病毒作者登录已盗取的 qq 账号，伪装 qq 账号所有者，发送该盗号木马给其 qq 好友或者共享到已加入的 qq 群，欺骗其它不明真相的 qq 用户主动运行盗号木马，如此扩散开来，打造出一条独特的传播产业链。

3、“杀破网”病毒

对抗杀软云查杀病毒。该病毒会释放并加载 NDIS 驱动，通过该驱动判断网络数据包通讯地址，屏蔽目标地址属于安全软件厂商，中毒电脑会无法登录杀毒软件的网站。该病毒主要通过色情网站的专用播放器传播。

4、“鬼影”病毒

一种罕见的利用硬盘主引导记录(MBR)启动的病毒，颠覆了“中毒后重装系统可解决”的定律。用户系统感染该病毒后，在常规的系统启动项、进程模块中无法找到病毒真正源头。在未恢复成正常 MBR 前，即使能成功删除其释放、下载的所有木马，系统重启后病毒也会死灰复燃。一般用户重装系统时并不会恢复 MBR，因此简单的重装系统也不能处理好鬼影病毒，鬼影病毒改写 MBR 的方法在2010年被大量病毒模仿。

5、浏览器主页篡改病毒

本类是指本年度已发现的所有篡改浏览器主页病毒集合，其中涉及的浏览器包括 ie，搜狗，360，傲游，firefox，chrome，腾讯 tt 等。病毒利用的手法通常为伪造假 IE 图标，新建恶意 url 协议，修改浏览器配置文件，伪装正常 BHO、IE 插件加载。病毒锁定的主页往往是各类导航站点，这些站点通过锁定用户主页来刷取商业网站的流量分成而获利。这也成为恶意软件最常采用的赢利模式。

6、牛皮癣病毒

牛皮癣病毒是桌面，开始菜单，快速启动等目录下所有删不掉图标和文件的总称。牛皮癣病毒与篡改浏览器主页病毒往往同时出现，其目的也类似。病毒会在桌面，开始菜单，快速启动栏等路径下新建一个系统图标或者删不掉的文件，双击该图标或文件时就会跳转到病毒指定的站点。由于删除这些图标或文件通常需要操作注册表或者修改文件权限等，因此用户一般很难手动直接删掉，这类牛皮癣也就成为最让用户恶心的病毒。

7、数字大盗病毒

数字大盗病毒的目标直指网购用户的淘宝，支付宝账号。病毒作者伪装为淘宝或其它平台卖家，发送名字类似"实物图"，"细节图"的文件给买家，一旦买家信以为真点击这些文件运行，数字大盗病毒会立即运行。数字大盗病毒会不停判断用户是否处在支付过程中，再通过篡改正常的支付页面，将中毒网民的资产直接转到病毒指定的帐户。该病毒堪称2010年危害最严重的病毒，预计该病毒的抢钱方法会在2011年被更多病毒效仿。

8、“伴随者”木马

该类木马主要通过感染或者替换系统文件如 d3d8thk.dll 的方式潜伏在系统中，病毒选取的这些 dll 都是网络游戏，聊天软件需要用到的系统文件。当用户打开网游或者聊天软件时，病毒即被激活，开始监视用户输入信息，截取当前屏幕并发送到指定收信地址，从而窃取到所需信息。这类木马的启动方式在2010年相当普遍，因安全软件普遍对改写注册表关键位置报警，导致病毒作者变换新方法获得运行机会。

9、“暴风 1 号”病毒

该病毒是一个由 VBS 脚本编写，采用加密和自变形手段，主要通过 U 盘传播的恶意蠕虫病毒。该病毒在2009年即大量爆发，在2010年内出现新变种。新变种在继承了原"暴风1号"U 盘传播方式，ntfs 文件流启动等特点后，病毒的主要目的集中在篡改浏览器主页上。该病毒会修改桌面正常的快捷方式， 当用户双击这些修改过的快捷方式时，病毒即获得启动机会，这给手动清除该病毒带来很大的麻烦。

10、“震网”病毒

又名 Stuxnet 病毒、超级工厂病毒。该病毒主要针对特定工业设施系统内的计算机，在我国个人用户的电脑上并未出现如上述9大病毒类的爆发现象，但由于该病毒近乎完美的技术手法，极其隐蔽传播方式和罕见的针对工业系统，虽未将普通用户的电脑做为攻击目标，我们仍然决定把它列入年度十大病毒之一。"震网"病毒利用 windows 操作系统内全新的0day 漏洞传播，并完美的伪造了某知名公司的数字签名来伪装自身关键文件。当"震网"病毒感染到安装有特定工业系统的计算机后，会再利用该工业系统自身的漏洞，篡改系统数据，展开破坏性攻击。据称，因超级工厂病毒攻击，伊朗核计划受重创。超级工厂病毒攻击，被视为网络战的成功范例。

第四章　2011 年互联网安全趋势预测

一、网购木马将集中爆发

伴随着病毒集团“互联网转型”的加速，互联网最集中的经济交易平台，同时，网购市场自身也在高速增长，这个领域必然成为黑客显而易见的攻击目标。

2010年，针对网购的钓鱼网站给网民造成重大损失，电商平台和安全厂商的合作会帮助用户减少损失。预计2011年，这方面的攻击数量还会持续增长。安全软件针对骗术的鉴定和拦截仍然需要不断改进，目前的拦截成功率仍然不够理想。网络骗术花样不断翻新，当一种骗术成功率不高时，骗子们就会尝试新招数。

金山网络安全实验室观察到，通过劫持篡改交易数据的网购木马出现多个不同破坏行为的变种，这意味更多病毒作者正开发出新的网购木马，须警惕针对在线购物的攻击欺骗方式会出现新变化。

二、针对社交网络的攻击呈现上升趋势

新浪微博、腾讯微博、人人网、QQ 社区等等，这些社交网络包含了众多隐私信息，普遍支持分享短链接，短链接很可能被利用来传播恶意信息。社交网络又具有传播非常快速的特点，若某个社交网络被黑客发现有漏洞可以利用，将会在极短的时间内影响庞大的用户群。

三、针对移动互联网的攻击加剧

手机平台由于其封闭型以及操作系统的分散性，给病毒木马传播制造了一定的门槛，但伴随着移动应用的爆发和 Andorid 平台的开放，风险在逐步增大。

据中科院调研报告显示：当前 68.6%的手机用户正面临移动安全威胁，存在恶意扣费行为的“扣费”类手机病毒已累积感染手机 250 万部以上，成为影响用户手机安全的主要威胁。

在中国，用户为应用商店付费的意愿较低，一些手机病毒经常伪装成有正常功能的盗版软件诱骗用户下载，并通过彩信、短信中内嵌链接进行扩散，给广大用户的个人隐私及财产安全带来极大隐患。

此外，由于 Andorid 平台的逐渐普及，以及其本身开放的特性，相较于 iOS、Windows Phone、Symbian 等系统，基于 Android 平台病毒的泛滥可能性较大。Andorid 平台的第一个真正意义的病毒，就诞生在中国。

联系方式：金山安全实验室　　电话：010-62927779