腾讯电脑管家
GUANJIA.QQ.COM

iResearch
艾瑞咨询集团

个人网络安全年度报告

iResearch Personal Internet Security Report 2012年

北京 · 上海 · 广州 · 深圳 · 东京 · 硅谷 · 香港

www.iresearch.com.cn

报告摘要-1

- **我国网络信息立法迈出了重要的一步**

2012年12月28日，全国人大审议通过了《关于加强网络信息保护的决定》。这一举措为网络信息保护确定了立法原则，为后续细化网络法则奠定了基础。

网路安全立法仍任重道远：法规的细化、法律的落实与执行、网民的法律意识都将是通向安全法制网络必解决的问题。

- **网络安全事件频繁发生，社会高度关注信息安全**

从2011年年底的“CSDN事件”到年中的“小米MIUI被曝泄密事件”，网络安全事件沸沸扬扬，在暴露网络不安全问题的同时，也引起了网民网络安全意识。

- **安全软件综合化发展，“杀毒”为核心，“管理”为辅**

市面主流安全软件的功能除基础防护类外，也包含“系统优化”、“软件管理”和“电脑诊所”等功能，如2012年腾讯电脑管家推出的“2合1杀毒版”。

- **网络威胁凸显“趋利性”，渗透入移动互联网**

2012年“TOP10木马”、“TOP10漏洞”和恶意网站，以“盗号”、“获取信息”或“恶意推广”为主流；其中，95%欺诈恶意网站为购物欺诈。

手机端网络病毒从2012年1月的3369个涨到9月的30564个，病毒数增长迅速，预计未来将会持续增长。

报告摘要-2

- **经济发达省份和上网为网络威胁份子的主要目标**

  木马发生率和恶意网站发生率的TOP10省份集中在经济大省和上网大省，如广东和河北。

- **大部分网民担忧网络安全，“网络支付”和“个人信息”位居前茅**

  70.0%网民表示担心网络安全；其中，网民对网络支付的安全（67.0%）更为担忧，其次为个人信息（60.7%）。

- **网民对安全软件的依赖度高**

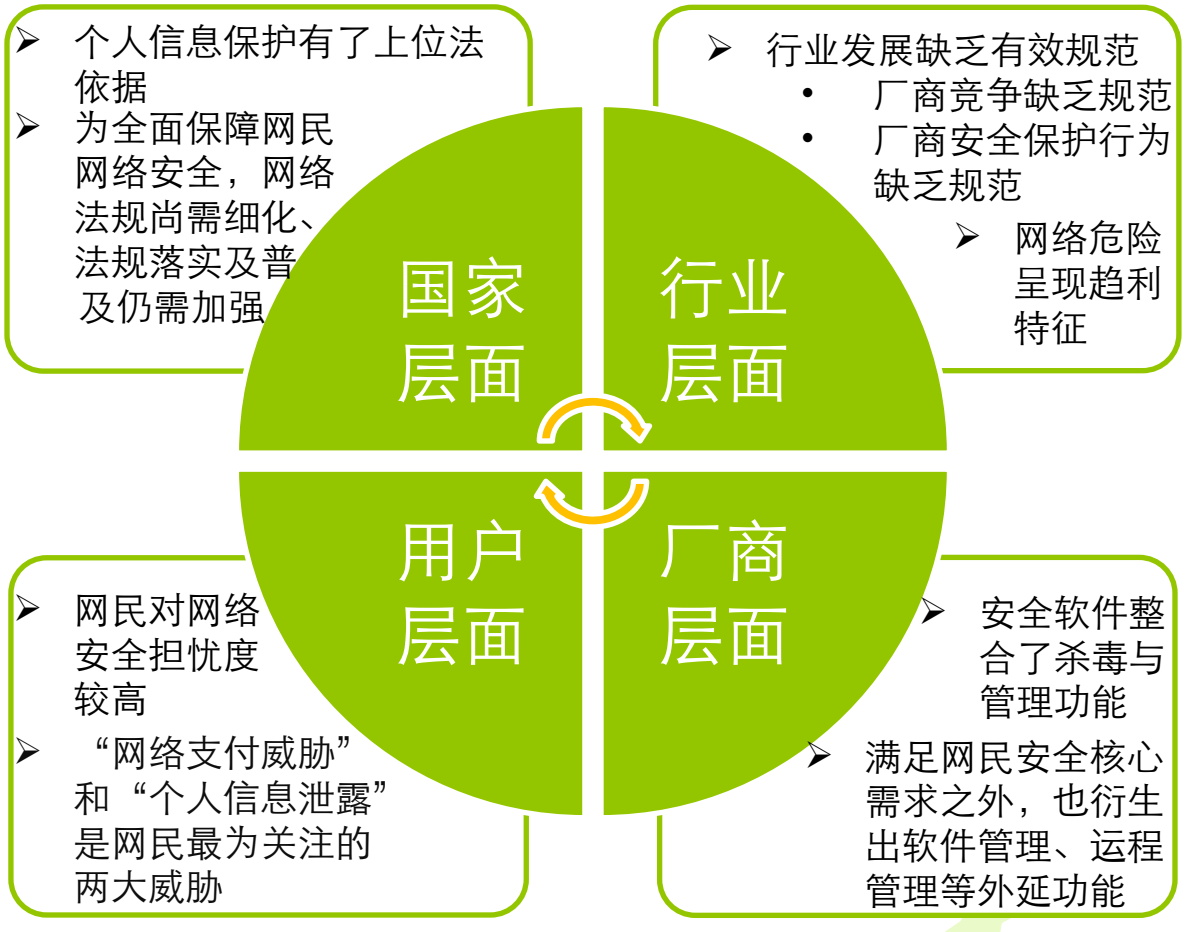
  安全软件成为网民保障网络安全的首选措施，80.3%网民将安全软件作为防范网络威胁方式。

- **“立法”成为网民期待改善网络安全的方式**

面对网络黑色产业化和网络厂商竞争与保护的不规范，网民期待通过网络立法来改善网络安全状况，79.9%网民期待完善相关政策法规。

目录

导读


国家层面
行业层面
用户层面
厂商层面
个人信息保护有了上位法依据
为全面保障网民网络安全，网络法规尚需细化、法规落实及普及仍需加强
行业发展缺乏有效规范
厂商竞争缺乏规范
厂商安全保护行为缺乏规范
网络危险呈现趋利特征
网民对网络安全担忧度较高
“网络支付威胁”和“个人信息泄露”是网民最为关注的两大威胁
安全软件整合了杀毒与管理功能
满足网民安全核心需求之外，也衍生出软件管理、运程管理等外延功能

我国首次专门为网络信息保护立法

——《关于加强网络信息保护的决定》颁布

2012年12月28日，全国人大审议通过了《关于加强网络信息保护的决定》，首次专门为网络信息保护立法，明确规定国家保护能够识别公民个人身份和涉及公民个人隐私的电子信息，为互联网用户的个人信息保护奠定了重要基石，互联网用户信息的保护将有法可依。

《关于加强网络信息保护的决定》出台背景

- **网民网络隐私遭侵害，网络信息保护法规薄弱**
  - ✓ 随着互联网技术在中国的广泛应用和迅猛发展，泄露和贩卖公民个人信息、网上诈骗、网络谣言等行为也“应运而生”，严重侵害了公民的隐私权，也对社会秩序造成严重干扰。
  - ✓ 在《关于加强网络信息保护的决定》出台前，我国有关网络信息保护的法律规范还比较薄弱，必要的管理措施缺乏上位法依据。

- **网民期待通过“网络立法”改善网络安全状况**
  - ✓ 根据艾瑞咨询调研，2012年网民首选“通过网络立法”改善我国网络安全现状，高达79.9%网民持此看法。

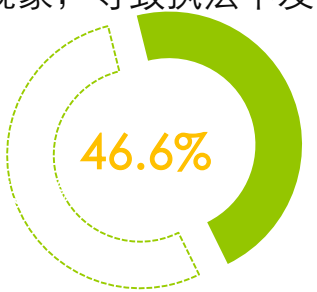
2012年网民安全立法期待率

Source：样本量N=3229。于2012年12月在艾瑞iClick和QQ平台联合回收。

但法规的细化、落实、普及仍需努力

《关于加强网络信息保护的决定》为互联网用户的个人信息保护奠定了重要基石，为后续相关行政法规提供了上位法依据。但要切实落实网络法制，我国尚需在立法、执法和普法上努力。

- **立法：**网络信息保护法规尚需细化明确，出台配套法规
  - ✓ 《关于加强网络信息保护的决定》的十二条内容都偏原则性，缺乏具体的监管部门、监管法律依据和处罚依据。对于复杂、具体的互联网行为，单纯的指导性法规是不足以完全保障参与方利益的，信息安全保护尚需要后续的立法和执法予以明确，比如制定个人信息保护法。
- **执法：**网络安全执法效能需留意
  - ✓ 由于《关于加强网络信息保护的决定》并没有对相关执法部门作出明确的规定，目前信息安全保护涉及到的监管部门较多，易出现多部门分散执法或执法不明确的现象，导致执法不及时等现象。
- **普法：**网络安全法规普及度有待提高
  - ✓ 现阶段，网民的法律意识不高，相比网民对网络立法的期望度，网民对我国现有的保护网络安全的相关法律法规了解较低，法律在网民中的普及尚待提高。



2012年网民网络安全法规了解率

Source：样本量N=3229。于2012年12月在艾瑞iClick和QQ平台联合回收。

行业发展缺乏有效规范

由于我国互联网安全体系化、全面化的法律法规尚未形成、网络安全立法相对滞后，网络安全发展秩序缺乏有效规范。

- **竞争缺乏规范**
  - ✓ 法律法规的不完善和滞后导致部分互联网企业凭借技术手段控制或打压竞争对手。这种游走在政策边缘的无秩序不正当竞争方式即便引起相关部门监管，但由于处罚细则不明或处罚力度较小，最终未能有效处置违规者，对领域内的竞争形成负面影响。
- **安全保护行为缺乏规范**
  - ✓ 针对“网络安全厂商对网民的安全保护范畴”、“厂商对网民电脑后台的扫描操作”等行为，国内尚无明确、针对性的法律规定。这导致不同厂商的保护行为不一致且不受约束，网民的个人信息和安全易受损坏。

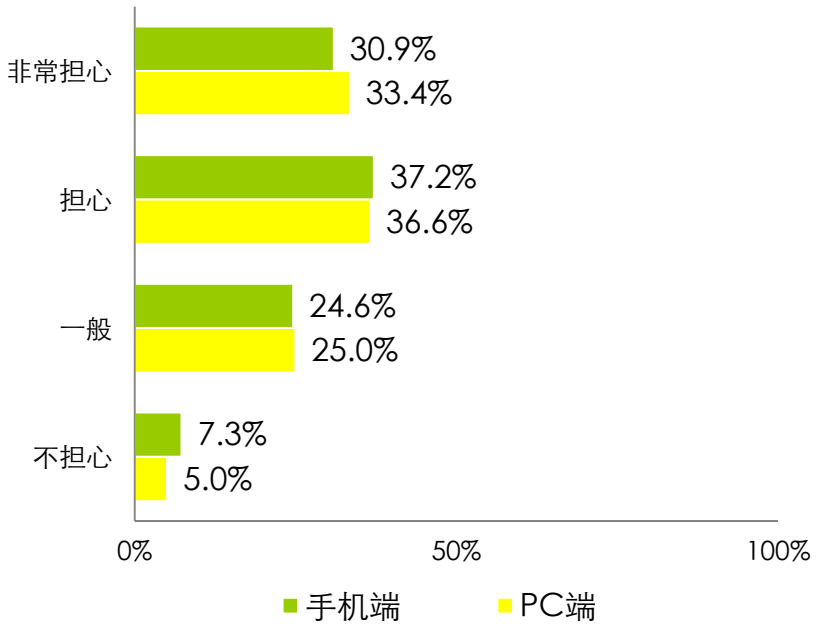
网络病毒趋利性强，安全厂商两手抓

- **网络安全呈现趋利性明显特征**
  - ✓ 在PC端上，50%的主流木马是以获取经济利益为导向，如盗号、广告恶意推广；电脑管家拦截的75%恶意URL属于虚假网络购物网站；
  - ✓ 在手机端上，“资源消耗”、“隐私获取”和“诈骗欺诈”类病毒占比超过70%。
- **木马仍是主要威胁，恶意网站威胁后劲强**
  - ✓ 2012年木马仍是国内网络安全的主要威胁，传播渠道为网民常规网络行为，每月有不计其数的新增木马；
  - ✓ 但恶意URL增长趋势不容忽视，腾讯电脑管家在2012年单就欺诈类URL拦截了44.8亿次，预估未来通过恶意网站和社会工程学相结合的威胁将会占主要地位。
- **手机端病毒增长迅速**
  - ✓ 2012年，手机端病毒呈现爆发式增长，表现最为突出的是Android平台的病毒增长。
- **安全厂商完善安全软件功能，整合“杀毒”与“管理”**
  - ✓ 主流安全厂商将安全软件的“杀毒功能”和“管理功能”整合，实现“2合1”便利全面的安全软件，如2012年10月腾讯电脑管家推出 “2合1杀毒版”；
  - ✓ 网民偏好功能齐全、操作便捷的多功能安全软件：82.5%用户偏好“一款软件集合了杀毒、安全和管理（软件管理、开机管理等）等多种功能”。

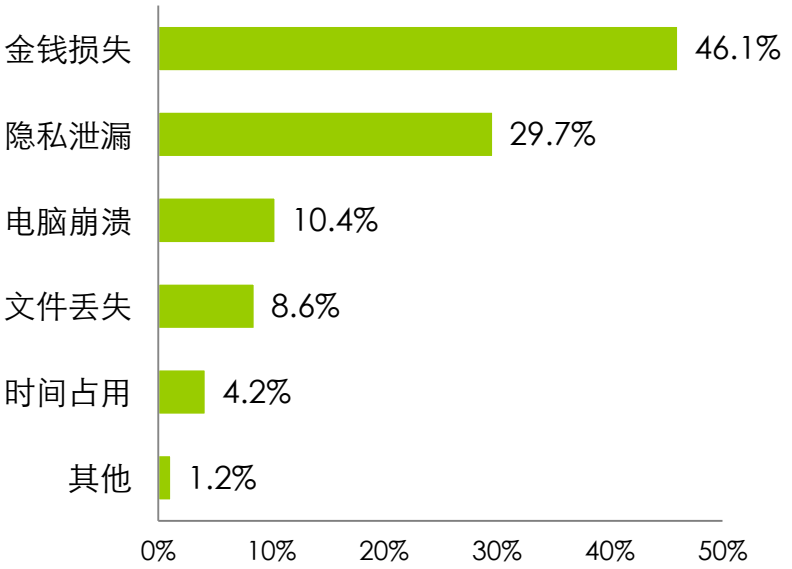
网民担忧网络安全，“隐私权”观念尚待提高

- 在2012年，网民对国内网络安全较担忧：70%左右的网民对国内PC端和手机端的网络安全表示担忧；
- 但对于网络安全对来的损失类型，网民最为关注的为直接显见的损失“金钱损失”，而“隐私泄露”担忧率为29.7%。

2012年网民对网络安全的担忧程度



2012年网民最担忧网络安全带来的损失类型



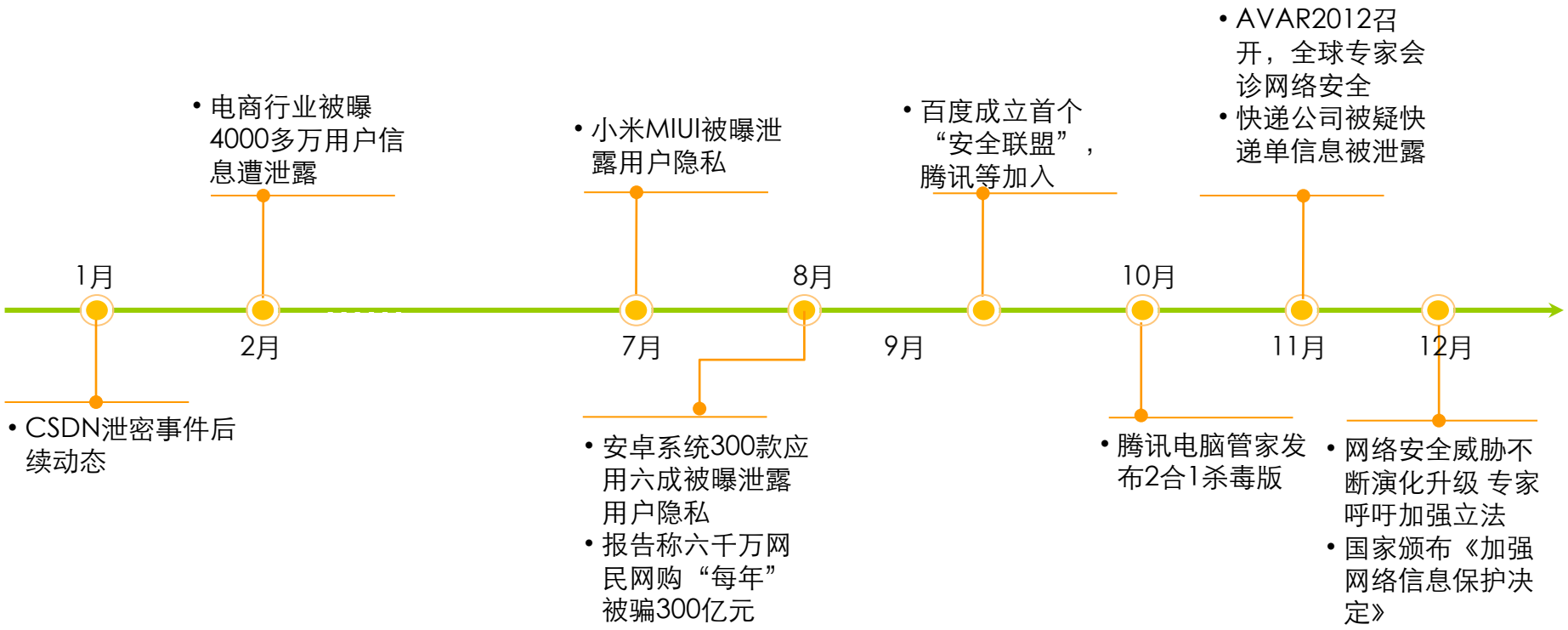
Source：样本量N=3229。于2012年12月在艾瑞iClick和QQ平台联合回收。

目录

2012年网络安全相关事件回顾

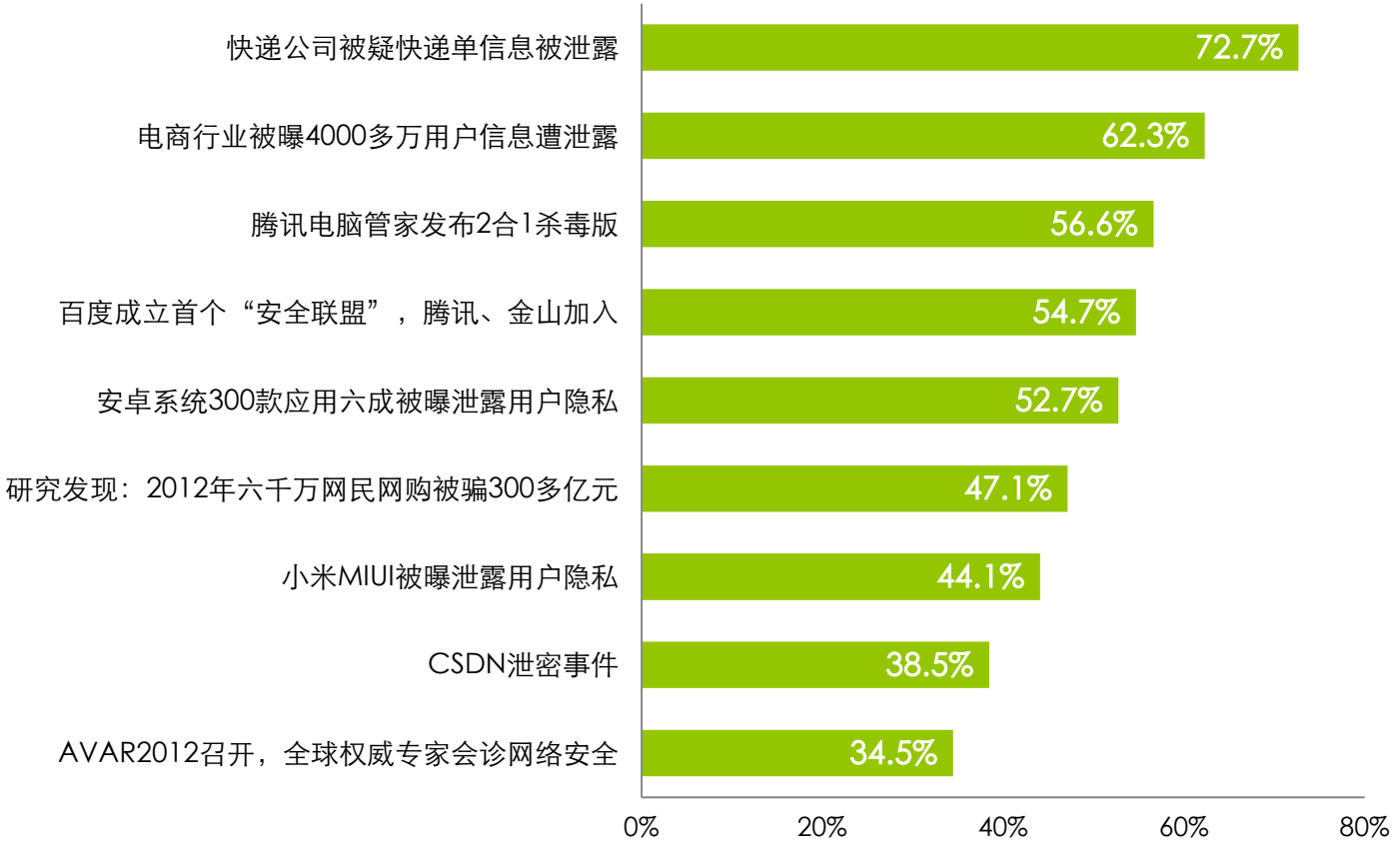
iResearch 艾瑞咨询集团

➢ 以下为2012年国内与网络安全相关的部分事件回顾。



2012年网络安全重点事件网民关注度

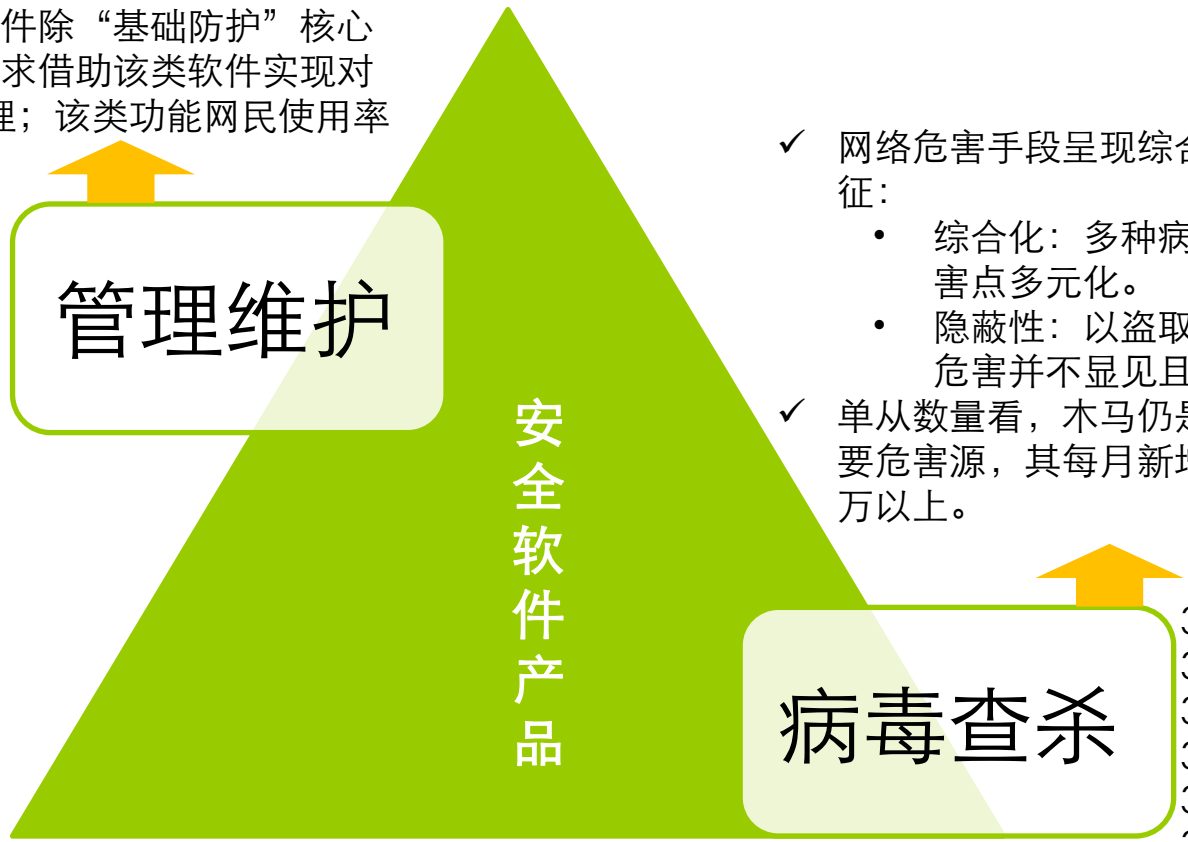
2012年网络安全重点事件网民关注度



Source：样本量N=3229。于2012年12月在艾瑞iClick和QQ平台联合回收。

目录

- 现阶段，安全软件兼具“杀毒”和“管理”双重功能：在当好网络安全守门员的核心职能之外，也满足了用户的“系统优化”、“软件管理”和“电脑诊所”等外延需求。



- ✓ 网民对安全软件除“基础防护”核心功能外，也需求借助该类软件实现对上网/电脑管理；该类功能网民使用率较高。

3.2.1系统优化
3.2.2软件管理
3.2.3电脑诊所

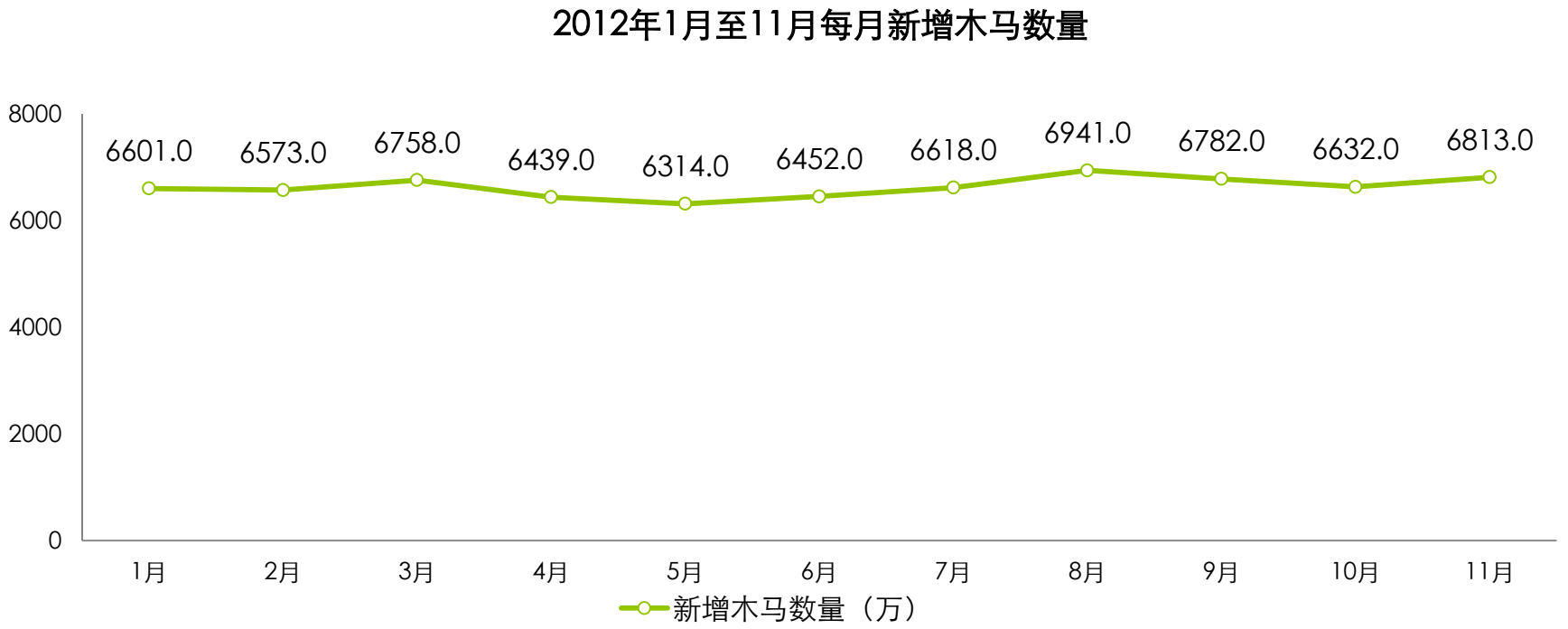
- ✓ 网络危害手段呈现综合化和隐蔽性特征：
  - 综合化：多种病毒形式夹杂、危害点多元化。
  - 隐蔽性：以盗取用户信息为主，危害并不显见且具有潜伏性。
- ✓ 单从数量看，木马仍是网络安全的主要危害源，其每月新增病毒数均在6千万以上。

3.1.1木马
3.1.2恶意网站
3.1.3漏洞
3.1.4恶意插件
3.1.5社会工程学
3.1.6移动端互联网

目录

2012年木马病毒每月新增6千多万

根据腾讯电脑管家监测分析：2012年全年木马新增数较为稳定，上半年略有下降，在5月份降至最低点，6月份开始反弹，下半年新增木马数量高于上半年。

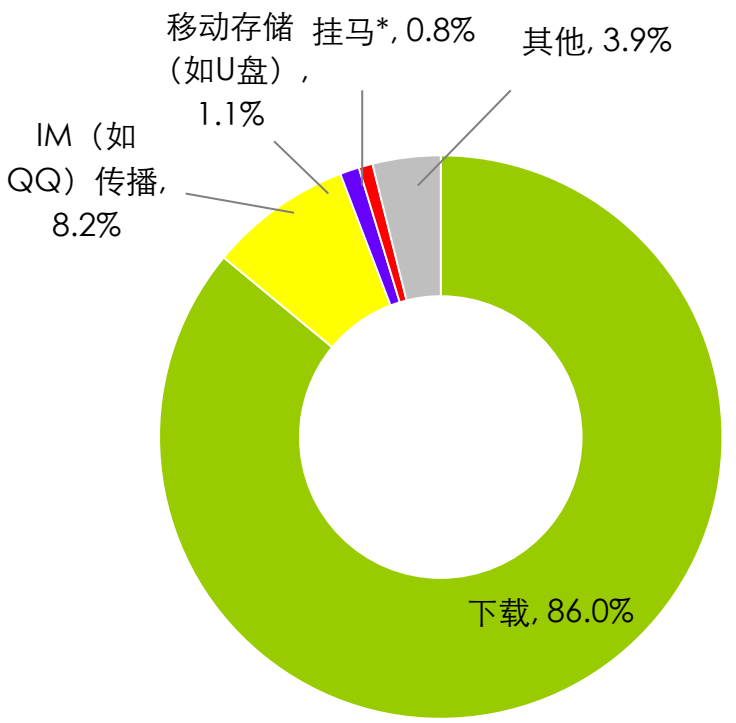


Source：腾讯电脑管家2012年1月-11月监测数据。

“下载”仍是电脑端木马传播最主要渠道

- 根据腾讯电脑管家监测分析：电脑端，木马传播渠道与往年相比没有出现新的方式，下载仍是木马主要推广方式；
- 下载渠道主要集中在各类游戏盗号木马捆绑外挂、色情类网站通过假QVOD捆绑木马这两种方式；
- IM（即时通讯软件，如QQ）传播略有增长，预计随着网游和网购市场的发展，这种点对点的传播方式将会继续增长；
- 随着安全软件对补丁的推送和Windows操作系统本身安全加强，移动存储（如U盘）和挂马*传播方式将会逐渐减少。

2012年1月至11月木马传播渠道



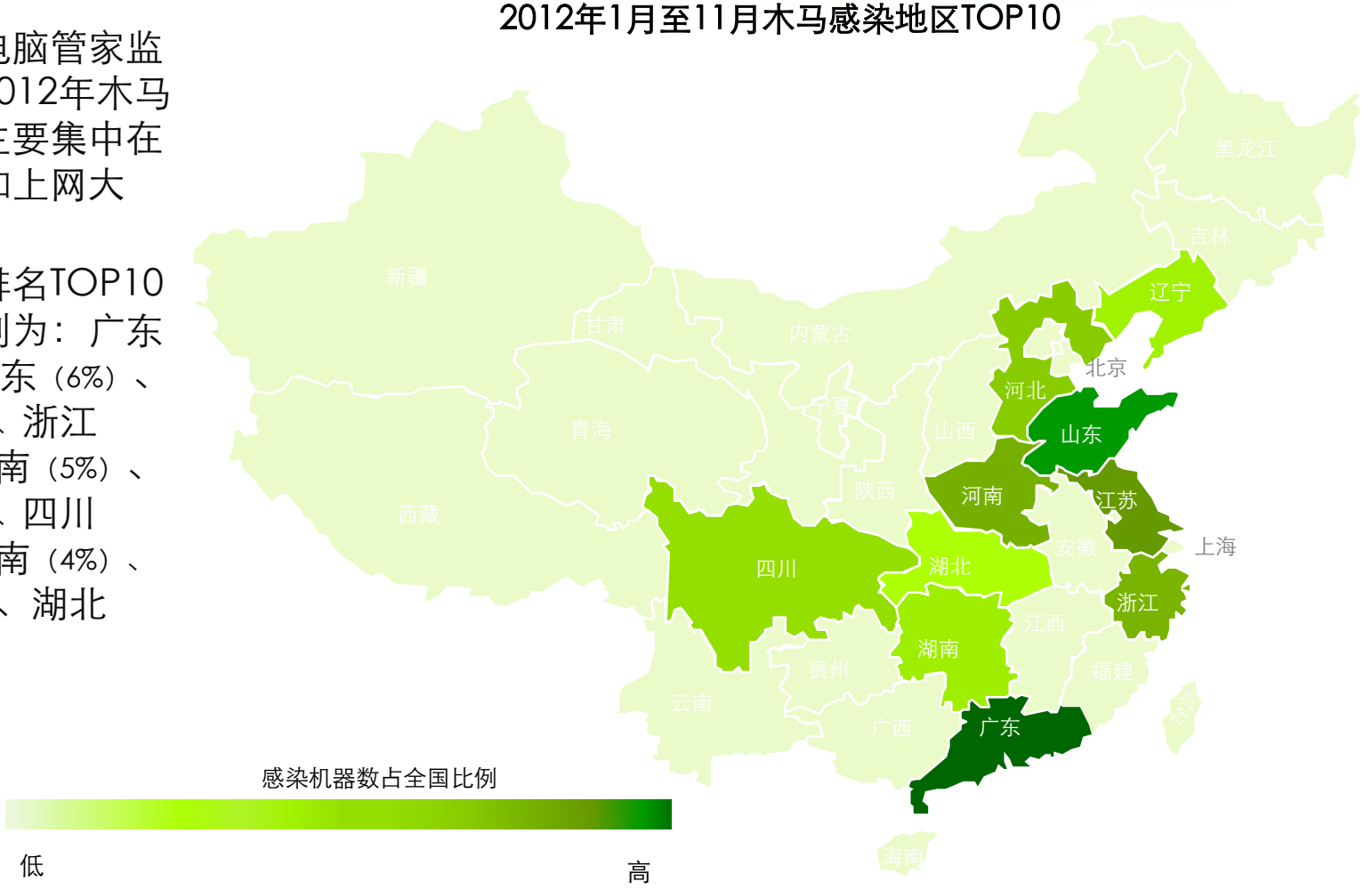
*注：“挂马”即黑客在网站页面中加入恶意转向代码，用户访问该页面时，就会自动访问被转向的地址或下载木马病毒。

Source：腾讯电脑管家2012年1月-11月监测数据。

经济大省和上网大省是木马感染重区

- 根据腾讯电脑管家监测分析：2012年木马感染地区主要集中在经济大省和上网大省；
- 感染地区排名TOP10的省份分别为：广东（11%）、山东（6%）、江苏（6%）、浙江（5%）、河南（5%）、河北（5%）、四川（4%）、湖南（4%）、辽宁（3%）、湖北（3%）。

2012年1月至11月木马感染地区TOP10



Source：腾讯电脑管家2012年1月-11月监测数据。

2012年网络木马类型TOP10

- 综合2012年网民感染量与该木马对电脑的危害程度，电脑管家评选出2012年TOP10木马类型；
- 同2011年相比，TOP10木马类型仍以“盗号类木马、病毒类木马、推广类木马和信息收集类木马”为主。大部分木马并不会对系统产生可见危害，而是以经济利益为目的，在不影响正常上网情况下，侵害网民利益。

2012年网络木马类型TOP10

病毒名称	病毒类型	病毒描述
Win32.Trojan-Downloader.Agent	病毒下载器	运行后从网络上下载并执行大量恶意程序
Win32.TenThief.QQPsw	QQ盗号木马	QQ盗号木马，盗取QQ用户帐号及密码信息
Win32.Risk.PatchLoader	修改系统文件病毒	劫持系统文件（一般是dll文件），实现木马或病毒入侵目的
Win32.Trojan.StartPage	修改浏览器主页病毒	修改IE主页，在收藏夹释放推广网址、广告网址，在桌面释放推广网址的快捷方式
Win32.Trojan.FakeIME	输入法文件劫持病毒	劫持系统输入法文件（一般是ime文件），通过这种方式注入到系统的所有进程
Win32.Trojan.Genome	病毒释放者	病毒释放程序，运行后会释放病毒程序并执行该病毒
Win32.Backdoor.Agent	用户隐私收集者病毒	收集用户电脑信息（如浏览器浏览记录、安装的软件等）通过网络发送到远程服务器
Win32.TenThief.DovqTroj	伪QVOD下载器木马	伪QVOD（播放器）下载器，下载木马到用户电脑
Win32.TenThief.DNFTrojan	某游戏盗号木马	某游戏盗号木马，盗取用户账号
Win32.Trojan.Bho	BHO木马	劫持浏览器，实现修改浏览器主页、收藏夹网站等目的

Source：腾讯电脑管家2012年监测数据。

2012年热点木马TOP10回顾-1

- 综合腾讯电脑管家监测数据，腾讯电脑管家评选出2012年十大热点木马：QQ大盗、新鬼影病毒、伪外挂木马、QQ刺客、伪QVOD下载器、LPK.DLL劫持者、网购木马、图标木马、恶意推广病毒、火焰病毒。

TOP1：QQ大盗

QQ大盗衍生出多个版本，危害方式越来越隐蔽，已能实现无痕获取用户账号密码的目的，严重影响了数量众多的QQ用户的帐号和财产安全。

TOP2：新鬼影病毒

又称“鬼影5”或“鬼影6”，该款病毒会修改用户的主引导记录，对抗目前国内的杀毒软件导致无法运行，并且会带动其账号继续下载其他盗号木马。

TOP3：伪外挂木马

通过和外挂捆绑在一起，伪装成正常外挂，引诱用户下载，盗取用户帐号和虚拟财产。由于和外挂捆绑，游戏玩家主动外挂率高，因此主要流传于游戏玩家中。

TOP4： QQ刺客

通过设置注册表使QQ进程启动加载，破坏QQ 密码输入框保护，构建假密码框，盗取QQ用户的密码和Q币。

Source：腾讯电脑管家2012年1月-11月监测数据。

2012年热点木马TOP10回顾-2

TOP5：伪QVOD下载器

伪QVOD是目前木马传播途径之一，排名TOP的木马基本都能在伪QVOD下载器的下载列表里面找到，包括QQ盗号木马，DNF盗号木马，新鬼影病毒。

TOP6： LPK.DLL劫持者

LPK.DLL劫持者就像牛皮癣一样在用户的系统中感染传播，很难根治。会先感染用户机器上可执行文件的目录和压缩包，用户通过传送文件/压缩包起到二次病毒传播。

TOP7：网购木马

随着电子商务的飞速发展，网购木马也随之激增，网购木马通过劫持浏览器等方式来诱骗用户转账。

TOP8：图标木马

木马的图标伪装成文件夹图标或者图片图标，诱导用户的点击然后运行起来控制用户的电脑。

TOP9：恶意推广病毒

恶意推广病毒通过修改浏览器首页，修改浏览器快捷方式，修改Windows系统文件等很多方式来恶意推广目标网站，达到提高目标网站流量的目的。

TOP10：火焰病毒

构造复杂，是一种全新的网络间谍装备。该病毒可以通过USB存储器以及网络复制和传播，并能接受来自世界各地多个服务器的指令，将用户信息和重要文件发送给远程操控病毒的服务器。

Source：腾讯电脑管家2012年1月-11月监测数据。

欺诈类网站占恶意网站主流

- 根据腾讯电脑管家监测分析：2012年欺诈类恶意网站仍是主流，全年腾讯管家共检测出钓鱼欺诈类网站125.6981万个，挂马类恶意网站17.2934万个；
- 病毒产业链的逐利特征和网购的发展促使欺诈类恶意网站呈现增长趋势；而与欺诈类恶意网站相反，随着安全软件越来越多关注各类系统漏洞，挂马成功几率在降低，时效也在缩短，挂马成本在提高，预计挂马类恶意网站将会持续减少。

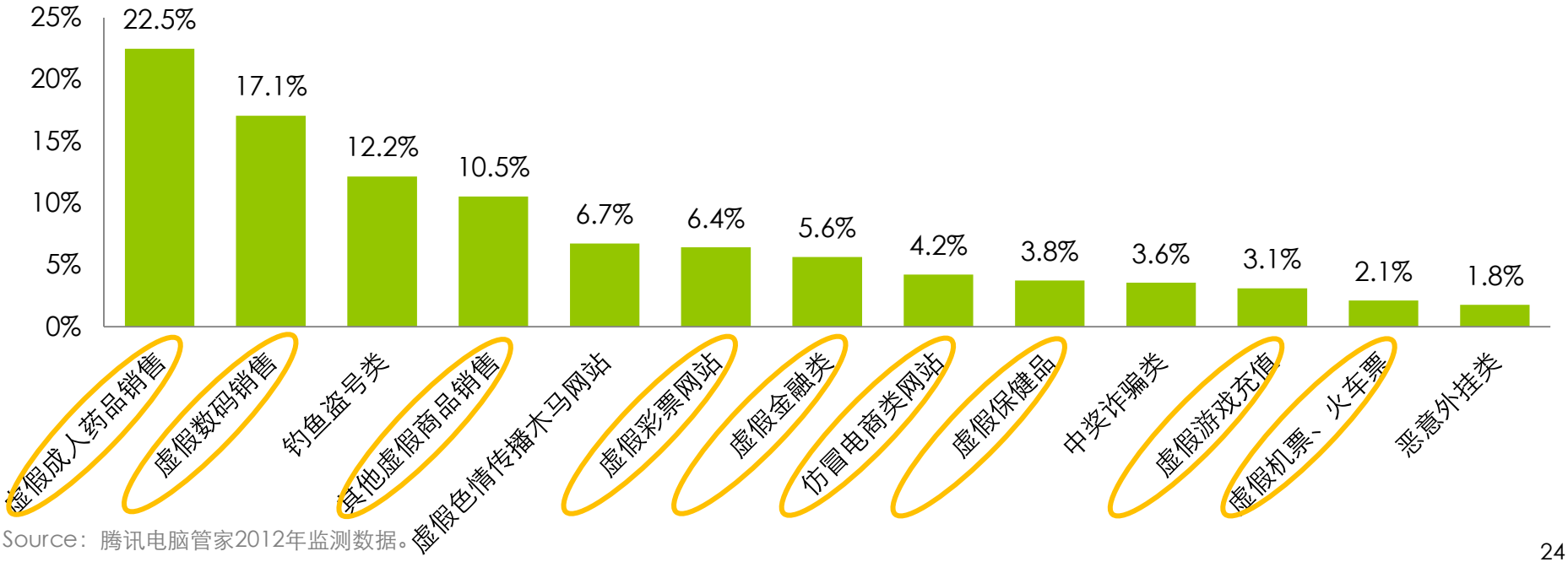
2012年电脑管家检测出的恶意网站数

Source：腾讯电脑管家2012年监测数据。

75%恶意网站为虚假购物网站

- 根据腾讯电脑管家监测分析：在电脑管家拦截的恶意URL上，网上虚假购物占据了所有拦截的75%，主要包括虚假成人药品、虚假保健品、虚假二手车交易网、虚假金融网站、虚假iPhone/小米销售、虚假游戏点卡交易站点，及各类电商仿冒网站；
- 预计随着电子商务发展，虚假购物网站占比将会继续增长，特别是一些虚假药品、保健品的网上销售。

2012年恶意网站内容分类

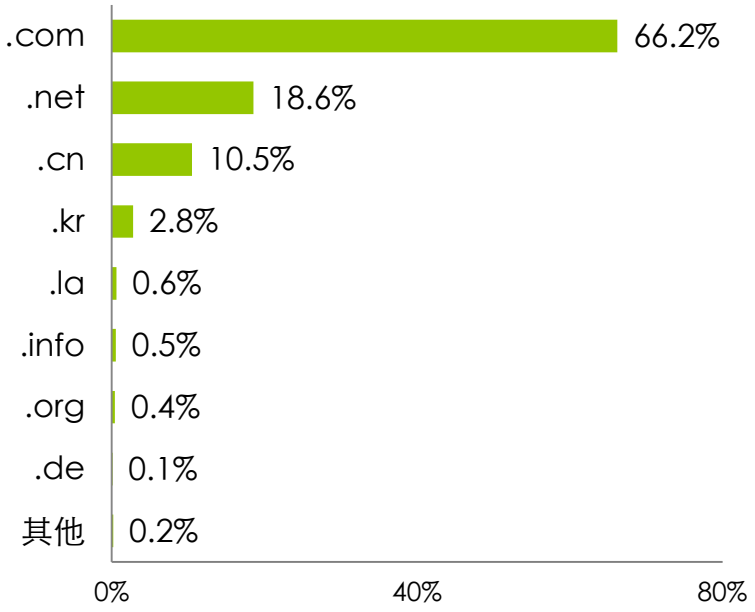


Source：腾讯电脑管家2012年监测数据。

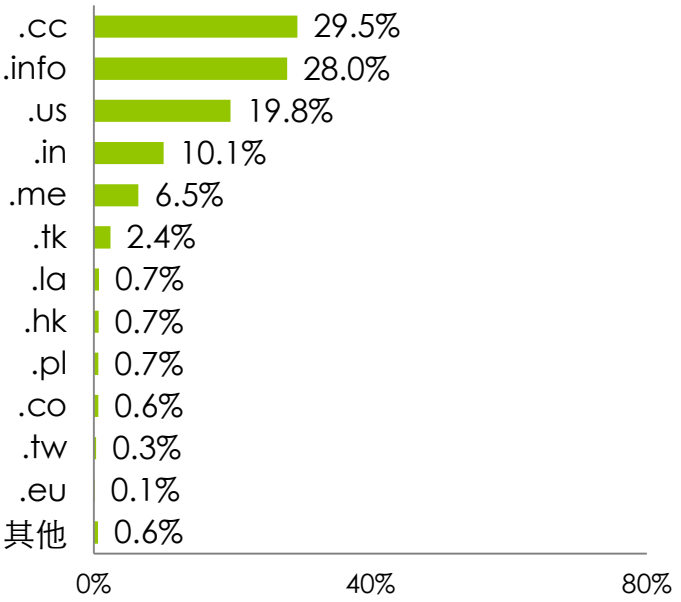
挂马网站以.com为主，欺诈网站偏好境外免费域名

- 根据腾讯电脑管家监测分析：挂马类恶意网站域名集中于国内常见域名，其中“.com”占绝大比例，以合法外衣隐藏其实质，以达到入侵目的。
- 欺诈类恶意网站境外域名主要集中在cc、info、us等免费域名，免费域名的快速获取使得钓鱼散播者可以方便变换URL来对抗查杀。

2012年挂马类恶意网站域名分布



2012年欺诈类恶意网站境外域名分布

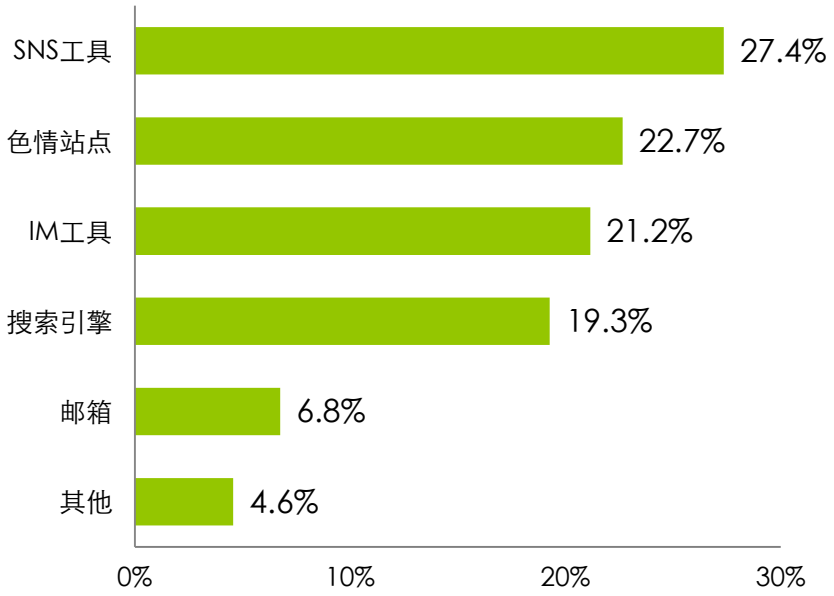


Source：腾讯电脑管家2012年监测数据。

色情网站成重要传播渠道、 日均500万电脑遭遇恶意网站

- 根据腾讯电脑管家监测分析，恶意网站主要通过SNS工具（如微博）、色情站点、IM工具（如QQ）等网民常用工具来传播。随着恶意虚假广告日益成为色情站长营收手段，色情站点逐渐成为各类恶意网站的主要传播渠道。
- 2012年管家用户中日均有500万台电脑遭遇恶意网站，全年约2亿台电脑遭遇过恶意网站的侵袭。

2012年恶意网站传播渠道



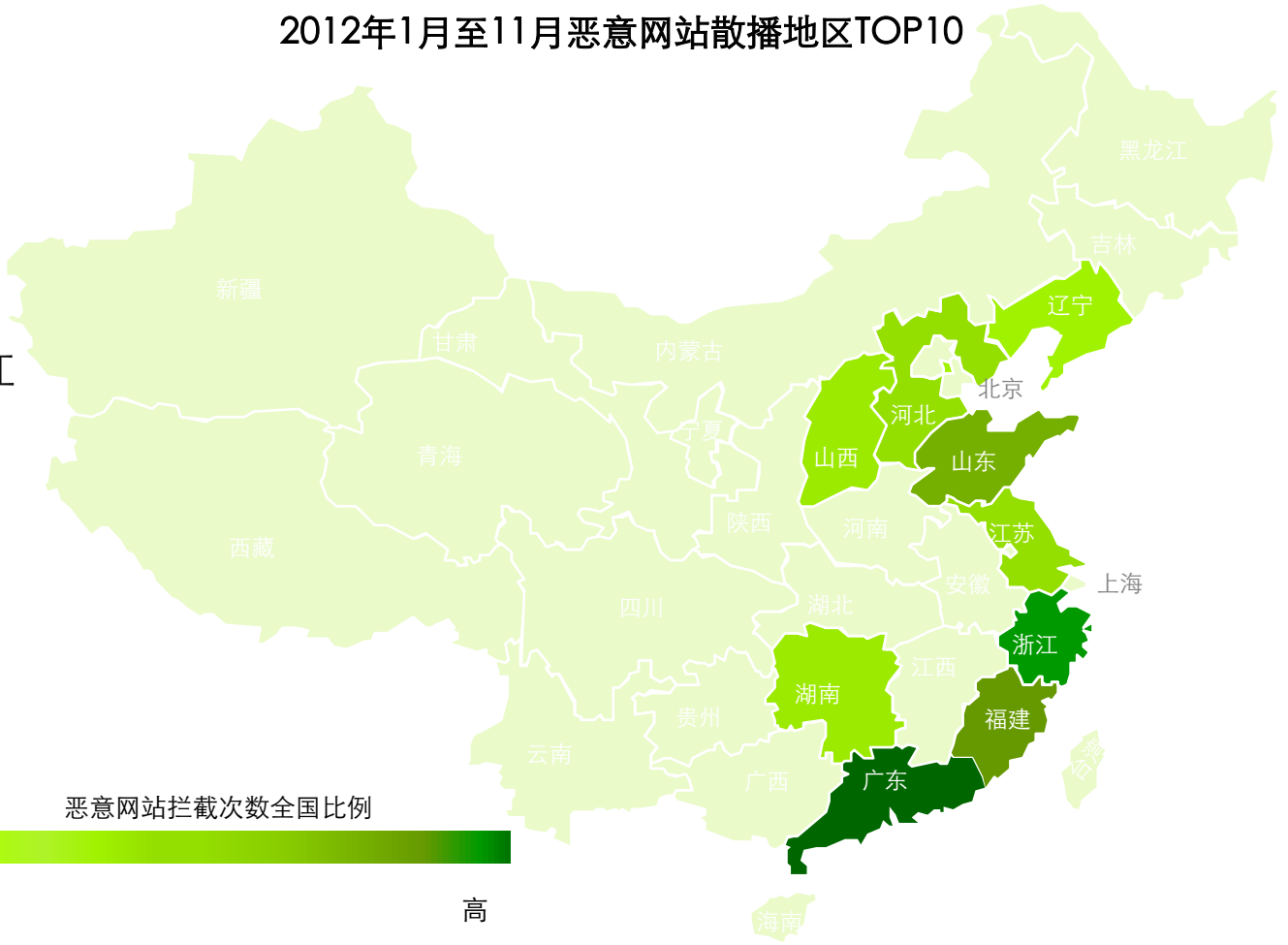
2012年电脑管家用户日均遭遇恶意网站电脑台数

Source：腾讯电脑管家2012年监测数据。

广东成为恶意网站散播率最高的省份

- 根据腾讯电脑管家监测分析：经济较发达的省份仍是恶意网站散播的主要对象；
- 感染地区排名TOP10的省份分别为：广东（20%）、浙江（8%）、福建（7%）、山东（6%）、江苏（6%）、北京（5%）、河北（5%）、山西（4%）、辽宁（4%）、湖南（4%）

2012年1月至11月恶意网站散播地区TOP10



Source：腾讯电脑管家2012年监测数据。

管家全年拦截欺诈网址44.8亿、挂马网址1.5亿

- 根据电脑管家监测分析，2012年电脑管家共拦截欺诈类URL共44.8亿，平均每日拦截恶意网址1200万人次。
- 2012年电脑管家共拦截挂马类URL共1.5亿，平均每日拦截挂马类网址41万人次。

拦截URL：44.8亿

欺诈类恶意网站

拦截URL：1.5亿

挂马类恶意网站

Source：腾讯电脑管家2012年监测数据。

2012年十大漏洞及其危险指数

- 综合腾讯电脑管家云安全中心监测数据，根据危险性，腾讯电脑管家评选出了2012年十大漏洞，分别如下：

2012年漏洞TOP10

漏洞名称	漏洞说明	危险指数	危害点	发布后24小时内修复量（万次）
“火焰病毒”漏洞	微软最紧急发布	★★★★★	易导致病毒木马局域网内爆发	2357.9952
“赤鬼”漏洞	影响面最大漏洞	★★★★★	资料、账号被盗	3506.7975
XML基础组件漏洞	影响人数最多	★★★★☆	账号被盗	3559.2200
远程桌面3389超级漏洞	黑市最贵漏洞	★★★★☆	电脑受操控	3176.3312
Java 沙盒漏洞	最具威胁的Java漏洞	★★★★	任意恶意程序被启动	2102.5583
IE8 内核漏洞	攻击方式流传最广	★★★★	资料、账号被盗	2747.5340
Flash 内存破坏漏洞	最具威胁的Adobe漏洞	★★★★	资料、账号被盗	2813.4384
Office 畸形文档漏洞	黑客最为青睐	★★★☆	易中木马病毒	2468.9384
Flash 嵌入式漏洞	最隐蔽的Adobe漏洞	★★★☆	恶意程序被启动	2254.8216
Windows Media 远程执行漏洞	2012年第一个严重级别漏洞	★★★	电脑系统被破坏	2027.8755

Source：腾讯电脑管家2012年监测数据。

十大漏洞危险说明-1

“火焰病毒”漏洞：微软最紧急发布

它与之前的“超级工厂”“Duqu”等病毒有着密切的关系，被称为目前最复杂的病毒。它通过非常罕见的蓝牙信号传递指令：启动被感染电脑的蓝牙设备,使它成为攻击周边蓝牙设备的“灯塔”。同时，该漏洞病毒会挟持Windows自动更新，利用漏洞的病毒木马可在短时间内感染所有局域网电脑，导致病毒木马大爆发。

“赤鬼”漏洞：影响面最大漏洞

允许黑客远程执行任意代码，危害程度极高。黑客可以通过该漏洞，创建一个虚假的恶意网站，当用户访问该网站时，黑客能够将木马植入用户电脑，窃取用户重要的资料和各种账号密码。

XML基础组件漏洞：影响人数最多

影响所有IE浏览器及多个版本的Office软件，致使大量Windows用户遭受威胁。通过利用漏洞制作恶意网页、文档等形式将木马病毒植入用户电脑，伺机进行盗号行为。

远程桌面3389超级漏洞：黑市最贵漏洞

利用该漏洞，黑客使用一系列数据包，即可完全控制用户电脑，成为任由黑客蹂躏的“肉鸡”（即被黑客远程控制）。国外某黑客组织，为了得到这个漏洞的详细利用方法，不惜动用5千美金悬赏金。且不说该漏洞在地下黑客市场上留存了多久，仅在微软公开该漏洞一天时间内，就有大面积的RDP服务扫描行为发生。黑客如此看重的漏洞，只能用“超级”二字形容。

Java 沙盒漏洞：最具威胁的Java漏洞

Oracle Java软件在实现上存在逻辑漏洞，黑客可利用此漏洞绕过沙盒防御系统，执行任意恶意指令。

Source：腾讯电脑管家2012年监测数据。

十大漏洞危险说明-2

IE8 内核漏洞： 攻击方式流传最广

该漏洞主要影响IE8内核浏览器。黑客通过制作恶意钓鱼网页、嵌入病毒广告等方式，将木马和后门（即绕过安全性控制而获取对程序或系统访问权的程序方法）等病毒程序植入到用户电脑中，窃取用户隐私和重要账号信息。该漏洞攻击方式已广为流传，大批黑客涌入该“漏洞市场”。

Flash 内存破坏漏洞： 最具威胁的Adobe漏洞

黑客通过构建特殊的Web网页，并诱骗用户点击恶意SWF文件，即可触发内存破坏逻辑，之后黑客便可轻易注入任意Web脚本，从而进行收集隐私、猎取帐号密码等非法行为，致使用户财产遭受损失。

Office 畸形文档漏洞：黑客最为青睐

黑客利用该漏洞可以轻易制作出颇具攻击性的恶意畸形Office文档，这些文档均木马病毒捆绑。用户打开文档后将会自动且连续释放大量木马病毒。由于Office软件非常普及，并且该类文件很容易在电子邮件中传播，因此该漏洞成为2012年黑客的“新宠”。

Flash 嵌入式漏洞：最隐蔽的Adobe漏洞

黑客利用Word文档嵌入恶意Flash文件，诱使用户点击运行后，即可触发该漏洞。该攻击方式较为隐蔽，且很多用户没有这方面的安全意识，危害性较高。

Windows Media 远程执行漏洞：2012年第一个严重级别漏洞

黑客可以利用该漏洞制作一些恶意的媒体文件，当用户使用Media播放器运行该文件时，将会执行黑客的恶意指令，破坏整个电脑系统。由于大部分的操作系统中均自带Media播放器，致使该漏洞颇具威胁。

Source：腾讯电脑管家2012年监测数据。

2012年恶意插件TOP10

➢ 综合腾讯电脑管家监测数据，根据中招用户数，评选出2012年恶意插件TOP10，具体如下：

2012年恶意插件TOP10

插件名	插件描述	中招用户数*（个）
系统目录恶意残留文件	木马或恶意软件查杀后的残骸文件，如果不清理很容易会被再次利用	34266
顺网广告组件	一款网吧管理软件的广告组件，强制在客户机器弹出广告较难清理	15108
PFbname广告程序	强制安装，无法彻底删除	8652
iShare	弹出广告、支持断点续传的下载工具、无法彻底删除	6034
酷站大全	强制安装，篡改用户首页，无法彻底删除	5051
cpush广告软件	强制安装、无法彻底删除、在使用计算机时会弹出广告网页	5002
地址搜索插件	一款在地址栏输入中文内容即可搜索出相关内容的插件	4052
恶意的篡改程序	强制安装，篡改IE首页和快捷方式	2521
健康上网专家插件	一款通过自动防范黄色有害信息、控制上网时长、控制聊天和游戏的免费防沉迷软件	1219
吐司传情专家工具栏	一款用于聊天工具发送表情、动漫等信息工具相关的浏览器工具栏	1165

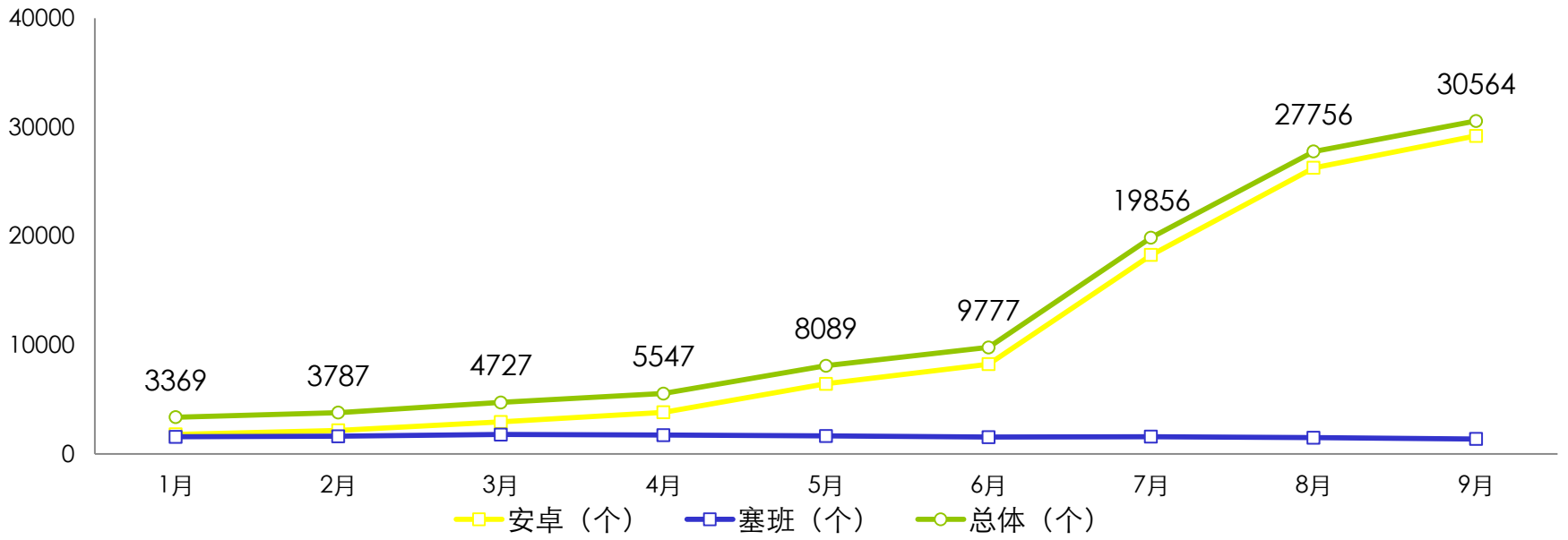
*此处中招用户数特指2012年4月-10月中每月20-26日监测去重数据。

Source：腾讯电脑管家2012年监测数据。

安卓平台病毒数增长迅速，塞班平台呈下降趋势（手机端）

- 根据腾讯移动安全实验室监测：2012年1月至9月，安卓系统平台的病毒量快速增长，而塞班系统平台则缓慢下降；
- 随着大批PC端黑客向手机端转移、塞班病毒制作者向安卓系统转移，艾瑞咨询预计在未来较长时间内，安卓系统病毒数将会持续增长。

2012年1月至9月手机端每月拦截病毒数

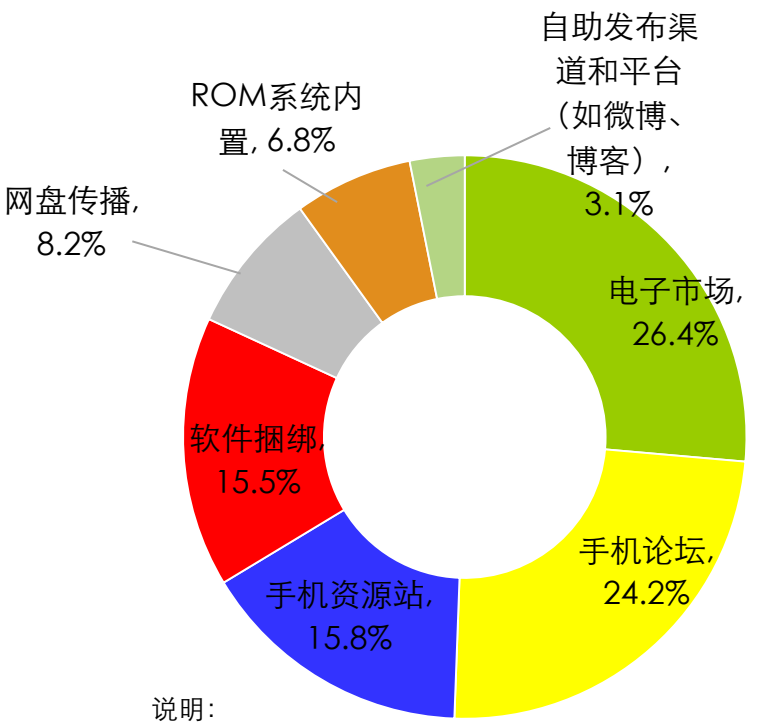


Source：腾讯移动安全试验室，2012年1月至9月监测数据。

手机病毒传播渠道多元化

- 根据腾讯移动安全实验室监测：手机端病毒传播渠道较分散，主要有：
  - ✓ 电子市场：病毒企图绕开电子市场的安全检测系统在审核上线之前被截获、又或者是通过一些没有接入安全检测的电子市场进行传播，占比为26.4%
  - ✓ 手机论坛：通过上传论坛附件或提供下载网络硬盘下载地址方式，占比为24.2%
  - ✓ 手机资源站：热门软件尤其是游戏软件经常包含病毒或者远程下载，占比为15.8%
- 随着电子市场监管理趋向严格化，电子市场的手机病毒检测专业性有所强化，电子市场的病毒传播将呈现下降趋势；
- 病毒来源的分散，加剧了病毒拦截的难度。

2012年1月至9月手机端病毒传播渠道



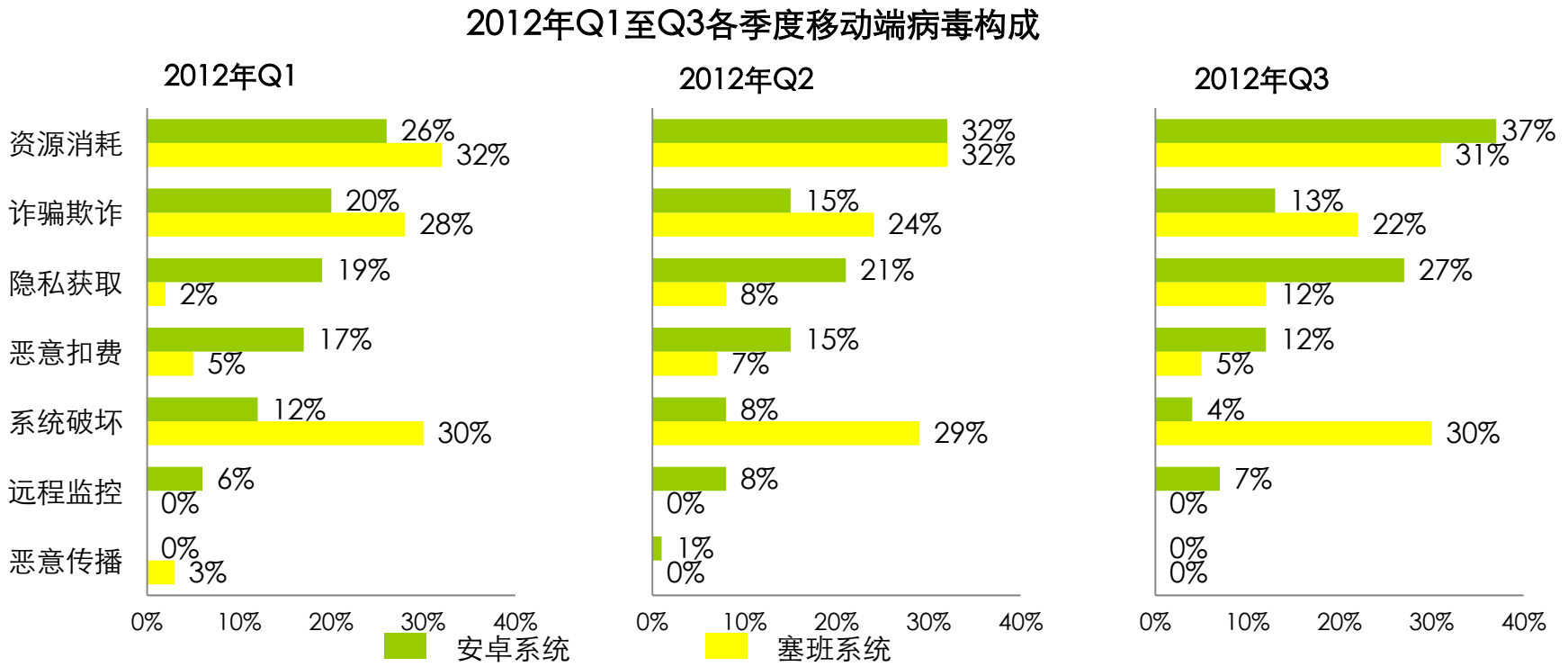
说明：

- 软件捆绑：通过录入或开设手机下载WEB/WAP资源站点，提供直接的软件下载地址；
- 网盘传播：通过网盘捆绑手机论坛提供下载链接；
- ROM系统内置：Rom制作者因利益驱动在ROM里预装病毒软件。

Source：腾讯移动安全试验室，2012年1月至9月监测数据。

资源消耗类病毒是手机端占比最大的病毒

- 根据腾讯移动安全实验室监测分析：安卓系统病毒以资源消耗类和隐私窃取类为主，而塞班系统则呈现“三分天下”特征，病毒集中在资源消耗、诈骗欺诈和系统破坏三大类。
- 从趋势上看，在两大手机平台上，隐私窃取类病毒皆呈上升趋势，手机病毒攻击行为从消耗流量资费转向更直接的窃取网银帐号盗取用户资金。



Source：腾讯移动安全试验室，2012年1月至9月监测数据。

手机端十大高危病毒

- 根据腾讯电脑管家云安全中心监测数据和病毒危险性，腾讯电脑管家评选出“2012年十大高危病毒”。

2012年手机端*高危病毒TOP10　　*此处手机端只指安卓系统上的病毒

病毒名	病毒描述	危险点
a.expense.apkquq	该病毒未经用户允许私自下载未知安装包，且不能正常退出，可能给用户带来一定的影响	操作干扰
a.expense.mdk	该病毒安装后，开机强制启动，从远端服务器自动下载恶意脚本代码，私自下载未知应用程序安装包，消耗用户流量，给用户造成资费消耗	资费消耗
a.remote.i22hk	该病毒安装后，自动上传IMEI、IMSI等信息,并获取云端指令控制用户手机，同时会修改浏览器书签以及联网下载未知程序。	手机受控
a.expense.cc	该病毒开机后私自下载软件并安装，可能会造成了一定的流量消耗，给用户的手机安全带来一定的威胁。	资费消耗
a.expense.forge.c	该病毒植入恶意推广广告，存在无提示私自下载推广软件的行为，给用户造成资费消耗。	资费消耗
a.payment.lemei	该病毒启动后会私自发送扣费短信，定制PS业务，可能会给用户的手机安全带来一定的威胁。	资费消耗
a.system.deviceadmin	该病毒伪装成系统关键程序，安装后会误导用户授予其系统高级权限，在后台定期发送扣费短信，而且无法通过正常流程卸载，影响系统的正常运行。	资费消耗
a.propagation.rootsmart	该病毒伪装成系统关键程序，启动后申请授予root权限，并在后台私自下载并静默安装其它恶意应用，同时会收集短信、通话记录等隐私信息。	隐私获取
a.expense.forge.b	该病毒植入恶意推广广告，存在无提示私自下载推广软件的行为，给用户造成资费消耗。	资费消耗
a.system.droiddream	该病毒安装后会获取手机root权限，并在后台静默安装内嵌子包，同时搜集手机上的信息，发送到指定服务器并在后台下载其他恶意安装包，给用户的隐私带来严重安全威胁。	隐私获取

Source：腾讯移动安全试验室，2012年数据。

网购、兼职和聊天工具占据社会工程学的主流

- 据不完全统计，2012年中国互联网的社会工程学攻击，对于用户造成的损失金额超过百亿。其中在网络购物、网上找工作、网上交友聊天等个典型场景中是社会工程学攻击的重灾区。
- 以下为现阶段主流的社会工程学欺骗手段：

网络购物类

- 销售虚假商品的网站，如假iPhone网站；
- 知名电商网站钓鱼：伪造知名电商网站，以此引诱用户付款。

网上兼职诈骗

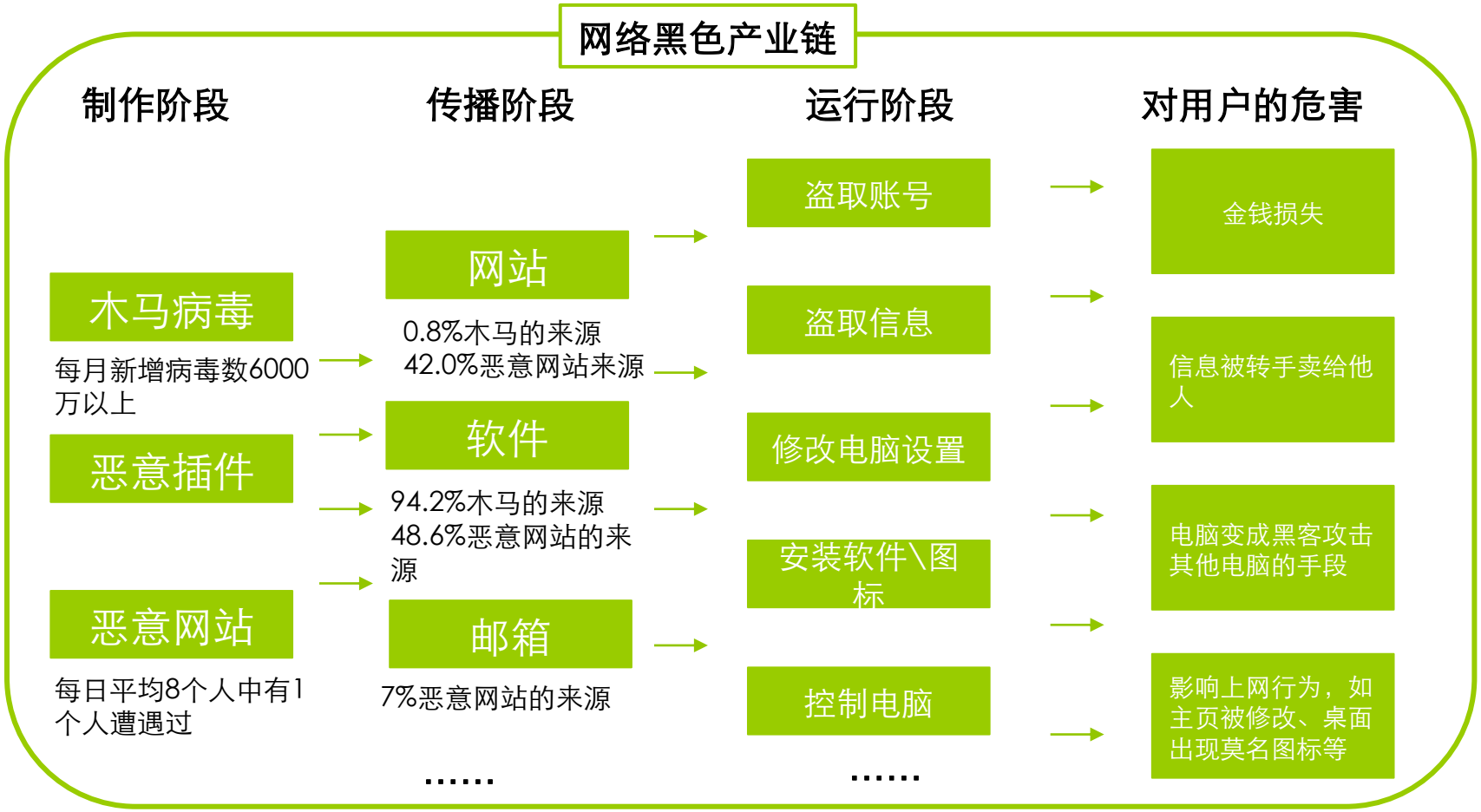
- 以网络兼职为名义，骗取用户钱财，如部分帮商家刷信用的兼职等。

网络聊天/社交

- 利用聊天工具直接诈骗，如MSN/QQ等；
- 通过盗取聊天工具的账号后，利用账号原有人际关系去诈骗。

网络安全黑色产业链

➢ 现阶段，网络黑色产业链以经济利益为主要导向，通过两种途径实现利益变现：盗取用户信息/账号变现为现金、借助网民恶意推广产品将流量变现为现金。



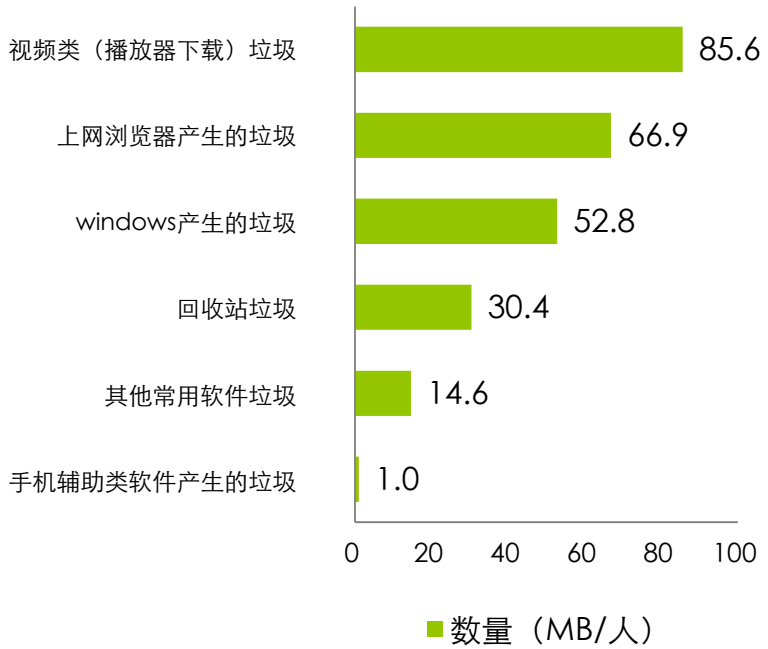
目录

电脑管家人均日产生251.3MB垃圾

- 根据腾讯电脑管家云安全中心监测：2012年，电脑管家用户每人日均产生251.3MB垃圾。其中，日均产生量最高的垃圾为视频类（人均日产生量为85.6MB）。

人均日产生251.3MB垃圾

2012年用户电脑每日产生的垃圾类型



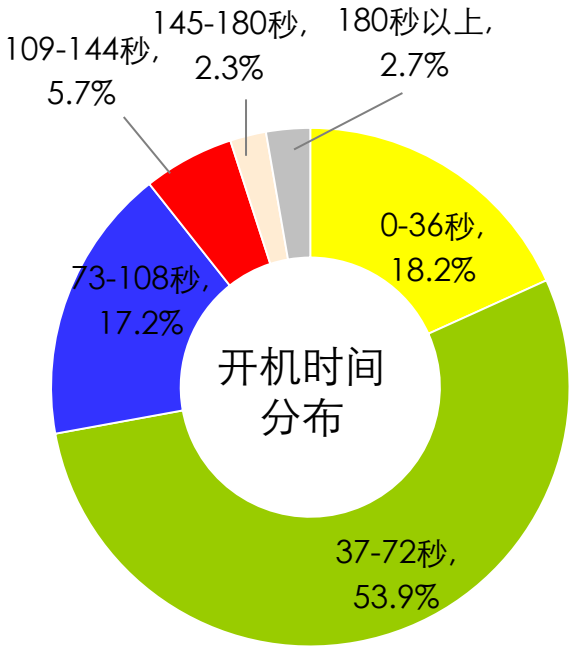
Source：腾讯电脑管家2012年监测数据。

人均电脑开机时间为68.5秒

- 根据电脑管家监测分析：2012年电脑开机时间平均为68.5秒；
- 其中，开机时间在36秒以内的电脑只占18.2%，超过80%电脑的开机速度较慢，建议养成定期加速、清理启动项的习惯。

电脑开机时间人均为68.5秒

2012年用户电脑开机时间分布



Source：腾讯电脑管家2012年监测数据。

安全软件的软件管理功能使用率高

- 根据腾讯电脑管家云安全中心监测：2012年电脑管家用户除使用该软件查杀病毒等防护功能外，也使用该软件管理电脑软件：下载软件、更新软件及卸载软件。
- 2012年全年，用户通过电脑管家下载软件20.2亿次，更新软件16.3亿次，卸载软件13.2亿次。

2012年用户使用电脑管家管理软件的情况

Source：腾讯电脑管家2012年监测数据。

电脑管家用户下载量最高的为视频播放类软件

- 根据腾讯电脑管家监测：2012年用户通过电脑管家下载软件情况：
  - ✓ 从软件类别来看，下载量最高的软件类别为“视频播放”、“联络沟通”和“音频播放”三类网络基础应用软件；
  - ✓ 从软件看，下载量最高的软件时QQ2012、QQ音乐和腾讯视频播放器等腾讯系产品。

2012年电脑管家软件类别下载量TOP10

排序	下载TOP10类别
1	视频播放
2	联络沟通
3	音频播放
4	浏览器
5	输入法
6	压缩刻录
7	网络下载
8	游戏休闲
9	安全防护
10	办公学习

2012年电脑管家软件下载量TOP10

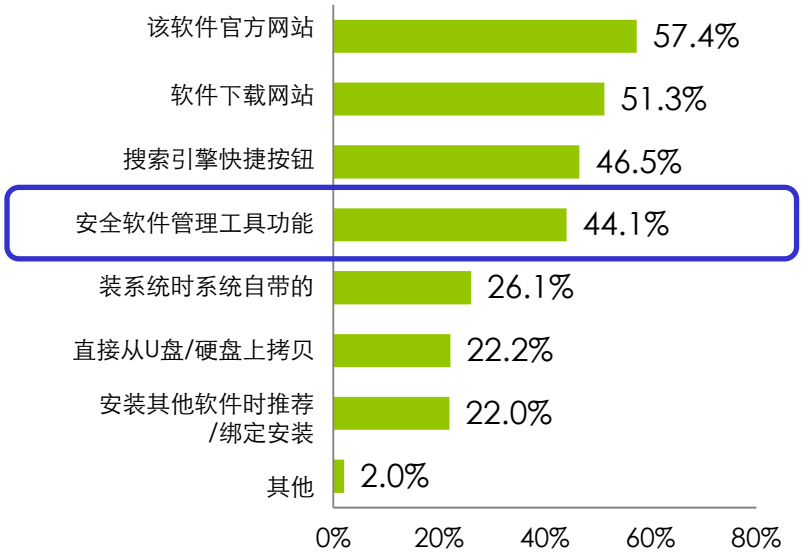
排序	下载TOP10软件
1	QQ2012
2	QQ音乐
3	腾讯视频播放器
4	QQ游戏2012
5	搜狗拼音
6	PPS影音
7	Adobe Flash Player
8	暴风影音
9	迅雷7
10	WINRAR

Source：腾讯电脑管家2012年监测数据。

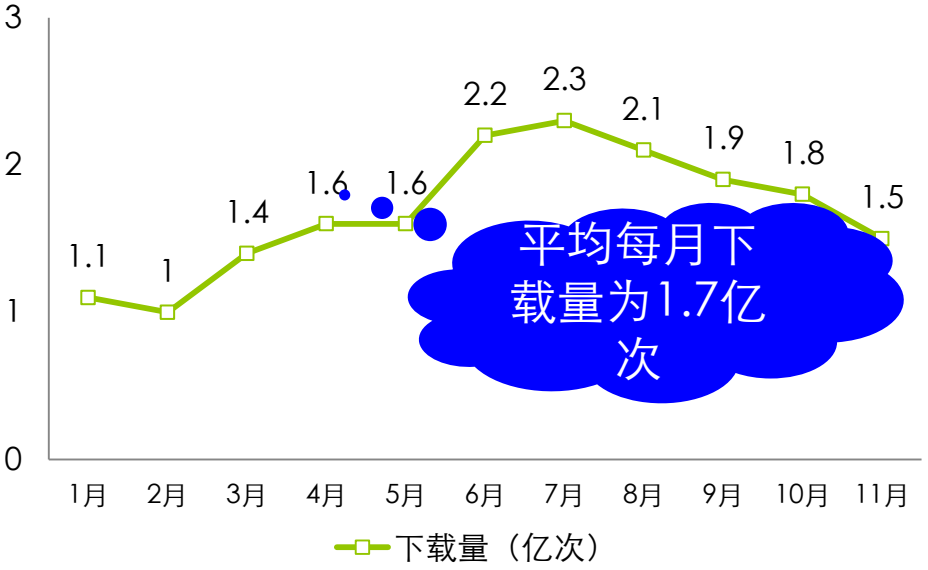
“软件管理”功能成为下载软件的主要途径

- 根据艾瑞咨询调研：“安全软件的软件管理功能”已成为网民下载软件的主要途径之一，44.1%网民通过该途径下载软件；
- 根据腾讯电脑管家监测，2012年用户通过软件管理功能下载软件的数量平均每月下载1.7亿次，整体呈现上涨趋势。

2012年网民软件下载途径



2012年电脑管家软件管理工具的软件下载量

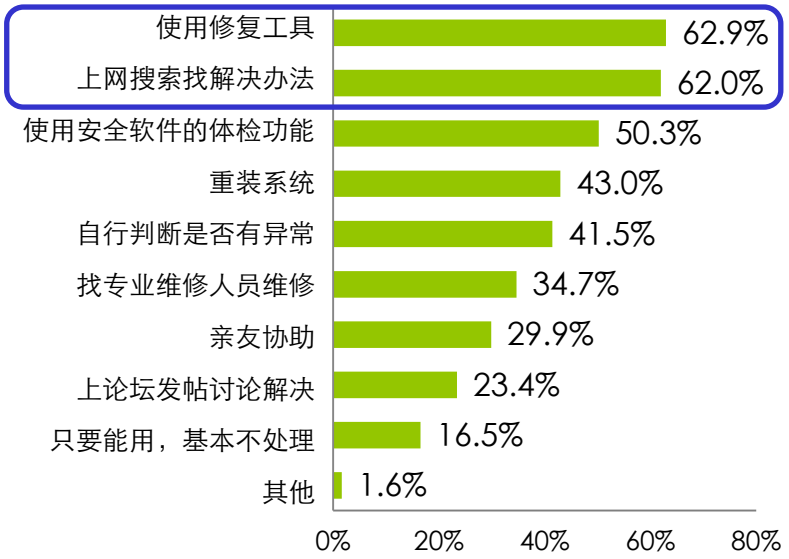


Source：软件下载量来源于腾讯电脑管家2012年监测数据；软件下载途径来源于2012年12月在艾瑞iClick和QQ平台联合回收，样本量N=3229。

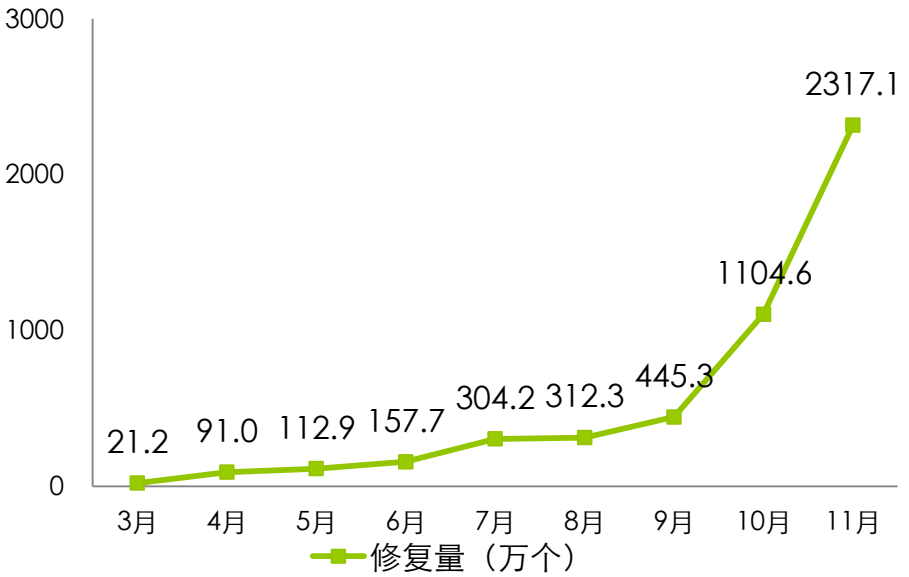
“电脑诊所”有助于用户修复电脑问题

- 根据艾瑞咨询调研：随着网络发展，“自助”已成为网民解决电脑问题的最主要方式，62.9%网民会使用修复工具，62.0%网民则通过上网搜索寻找解决方法；
- 根据腾讯电脑管家监测，自2012年3月开始，用户通过“电脑诊所”修复电脑的次数翻倍增长。

2012年网民处理电脑问题的方式



2012年电脑管家用户通过该软件修复的电脑量



Source：电脑修复量来源于腾讯电脑管家2012年监测数据；电脑修复方式来源于2012年12月在艾瑞iClick和QQ平台联合回收，样本量N=3229。

网络使用异常是用户常遇的电脑/网络问题

- 腾讯电脑管家根据用户使用电脑诊所修复的情况，评选出2012年用户经常遇到的十大电脑或网络问题。十大常见问题中，前三个问题都是涉及到网络使用过程中出现异常。

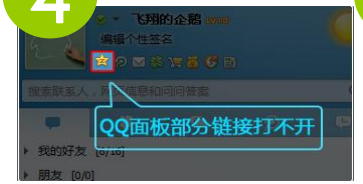
2012年电脑管家用户遇到的电脑/网络问题TOP10

1. 
农场等网页游戏玩不了

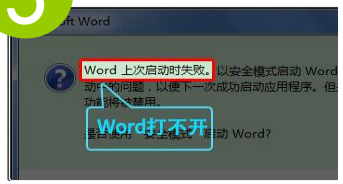
2. 

QQ空间打不开

3. 
浏览器打开主页异常

4. 

QQ面板的邮箱、空间打不开

5. 

Word等Office文档打不开

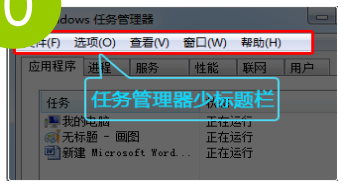
6. 
网站二级页面打不开

7. 
网络视频看不了

8. 

桌面图标删除不了

9. 
桌面图标有蓝色阴影

10. 

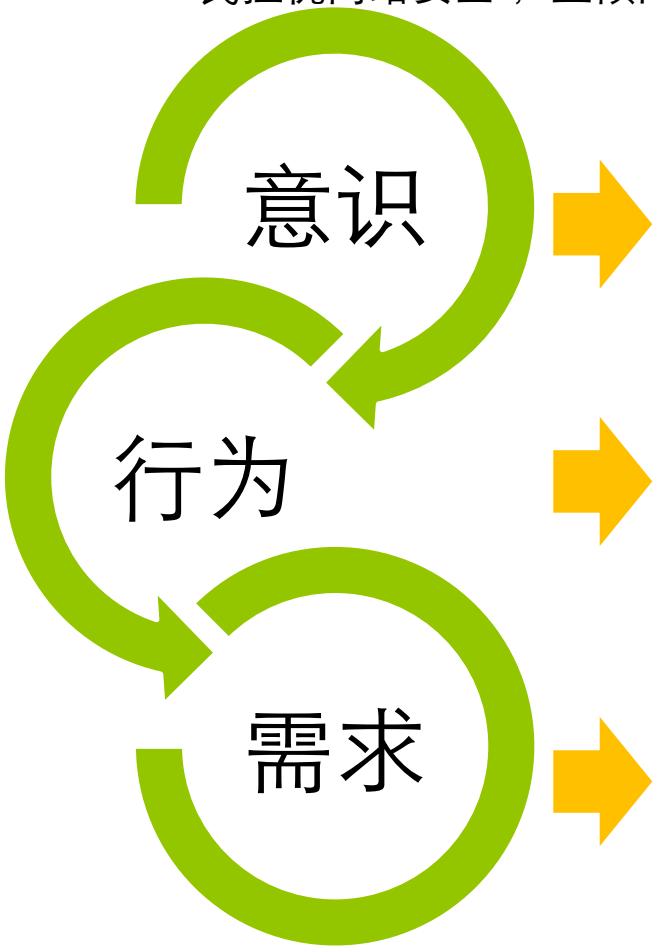
任务管理器菜单栏消失

Source：腾讯电脑管家2012年监测数据。

目录

导读

- 本章节通过对网民安全意识、安全行为和安全保障需求三层面调研分析得出，现阶段，网民担忧网络安全 ，且倾向依赖外在力量来保障自身安全。



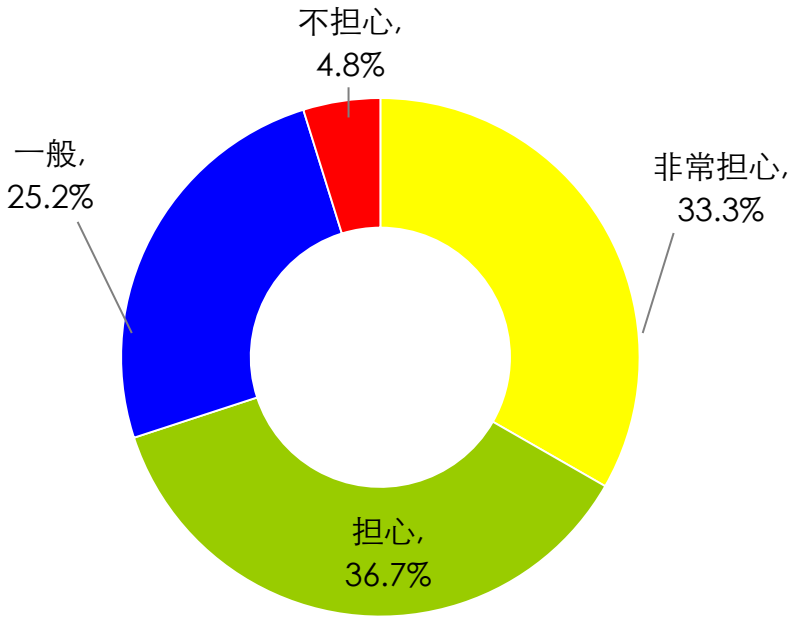
- ✓ 网民网络安全忧患意识高，最担忧威胁带来的“金钱损失”和“隐私泄露”。
- ✓ 网民网络安全防范倾向于依赖外在力量，如安装安全软件，但对于自身行为的留意及控制意识有待提高，如在上网时主动留意各类威胁。
- ✓ 对网络安全越担忧的网民采取网络安全保障措施越全面。
- ✓ 网民期待通过建立网络安全法制及加强安全技术改善网络安全状况。

目录

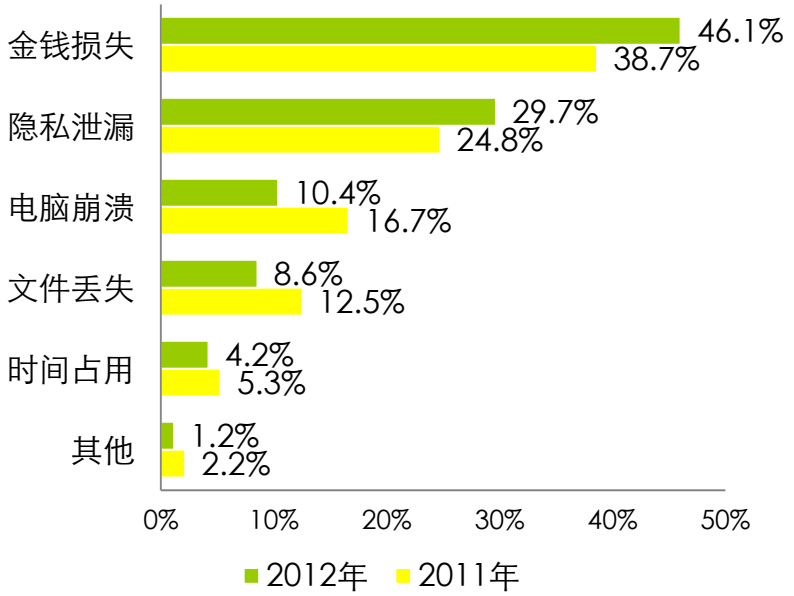
网民网络安全忧患意识高，担忧金钱及隐私损失

- 根据艾瑞咨询调研显示，2012年大部分网民对网络安全持不乐观态度：70.0%网民对网络安全表示担心，其中33.3%持非常担心态度；
- 相比2011年，网民对网络危险的担心首先为“金钱损失”：“金钱损失”相对2011年上涨7.4%；其次为“隐私泄露”。

2012年网民对网络安全的担忧情况



2012年网民担忧网络安全带来的损失类型



Source：样本量N=3229。于2012年12月在艾瑞iClick和QQ平台联合回收。

网民安全担忧意识众生相

➢ 根据对网络安全的担忧程度划分，安全担忧度不同的网民具有不同的属性特征：非常担忧的人群呈现年纪大、学历高、收入高三大特征，相对而言，不担忧人群则呈现低年龄、偏男性用户两大特征。

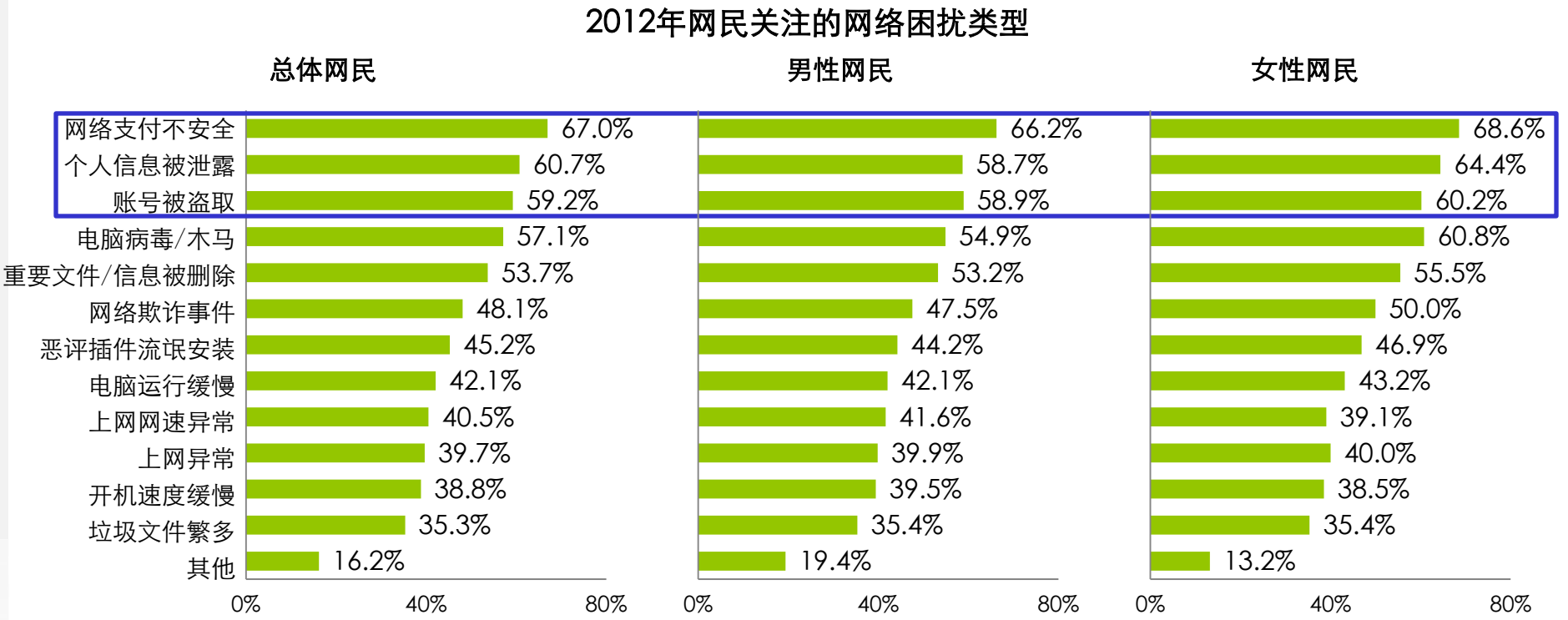
对网络安全的担忧程度

不担忧	担忧	非常担忧
		
占比：5.7%	占比：69.7%	占比：24.6%
• 年龄偏小：平均年龄=25.9岁	• 年龄中等：平均年龄=27.4岁	• 年龄偏大：平均年龄=30.5岁
• 男性为主，75.7%为男性	• 男女比例较为均衡	• 男女比例较为均衡
• 学生为主，且大部分为低年级学生，整体收入最低	• 普通员工或高年级学生为主，收入中等	• 高学历、高收入人群为主，以企业中高层管理人员占比最高
• 网络行为：较单一	• 网络行为：丰富度中等	• 网络行为：非常丰富
• 网络安全担忧度：几乎不担忧	• 网络安全担忧度：略有担忧	• 网络安全担忧度：非常担忧
• 网络防范措施意识：弱	• 网络防范措施意识：中等	• 网络防范意识：高

Source：样本量N=3229。于2012年12月在艾瑞iClick和QQ平台联合回收。

财产安全和信息保密是网民最关注的网络安全

- 根据艾瑞咨询调研显示，网民对涉及财产安全和信息隐私的安全困扰最为关注，其关注的TOP3安全困扰类型为“网络支付不安全”、“个人信息被泄漏”和“账号被盗取”；
- 相对男性用户，女性网民对各类网络困扰的关注都更高，反映出女性网民对网络威胁警惕性更高。

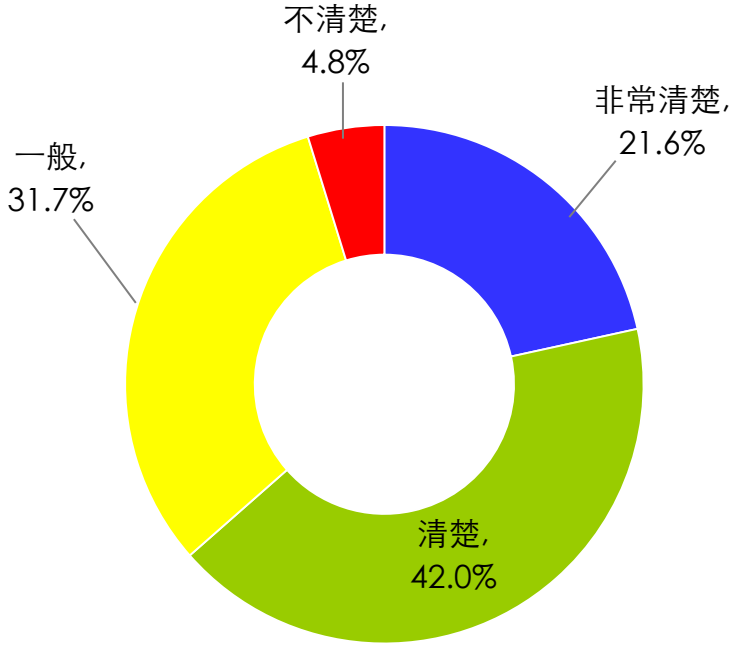


Source：样本量N=3229。于2012年12月在艾瑞iClick和QQ平台联合回收。

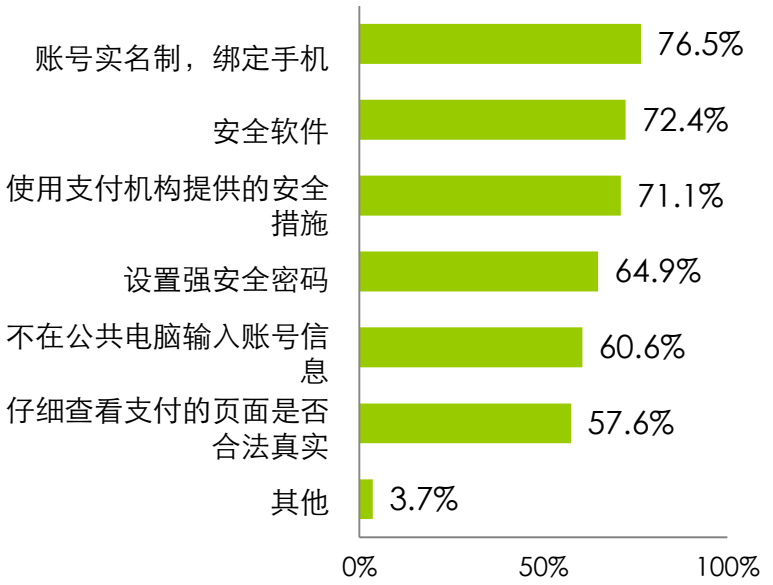
网民网络支付安全保障意识强

- 根据艾瑞咨询调研显示，随着电商发展和网银技术普及，网民网络支付保障意识高，63.6%用户表示知晓网络支付保障措施；
- 网民倾向通过硬件手段保障支付安全，如账号绑定手机、安装安全软件和使用支付机构提高的安全措施；但是在自我可控的操作行为上，尚待提高安全防范意识。

2012年网民对网络支付保障的知晓度



2012年网民网络支付采取的安全保障措施

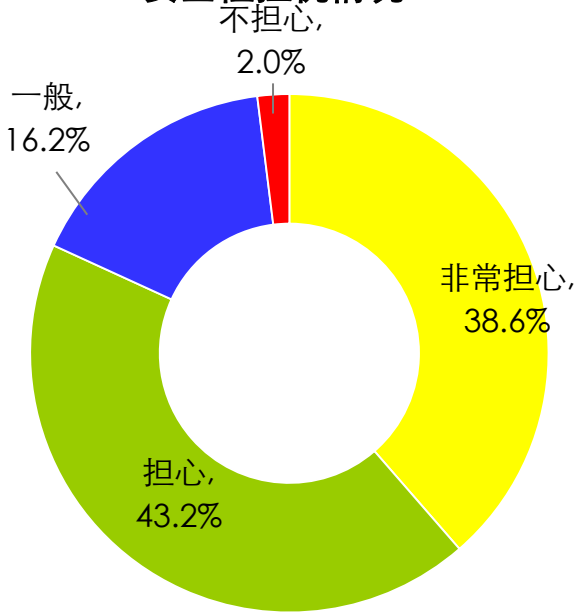


Source：样本量N=3229。于2012年12月在艾瑞iClick和QQ平台联合回收。

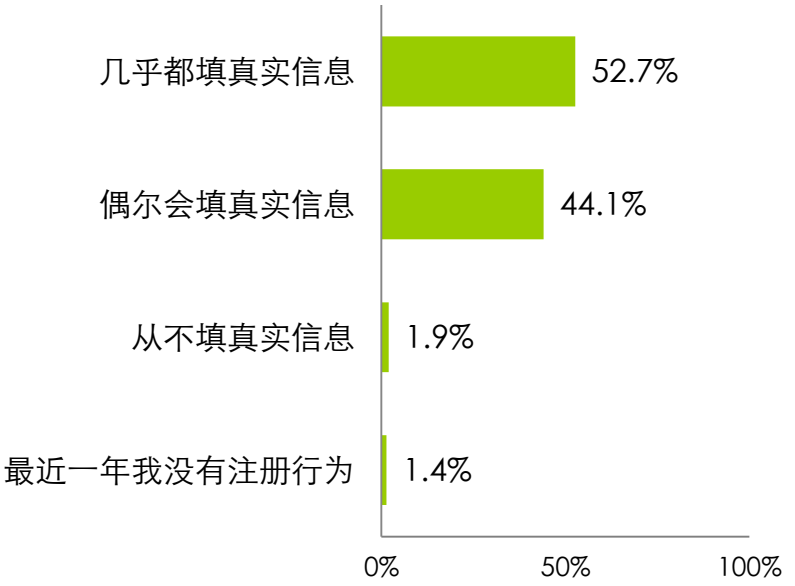
个人信息的担忧意识强，超五成网民常填写真实信息

- 根据艾瑞咨询调研显示，随着曝出多件隐私泄露事件后，网民对个人信息的隐私性持非常高的担忧度：81.8%网民表示对个人信息的隐私表示担心，高于网民对整体网络安全的担心程度；
- 在注册填写时，大部分网民选择填写自己真实个人信息，从不填写真实信息的只有1.9%。

2012年网民对“在网上填写真实信息”的安全性担忧情况



2012年网民注册填写真实个人信息的频率

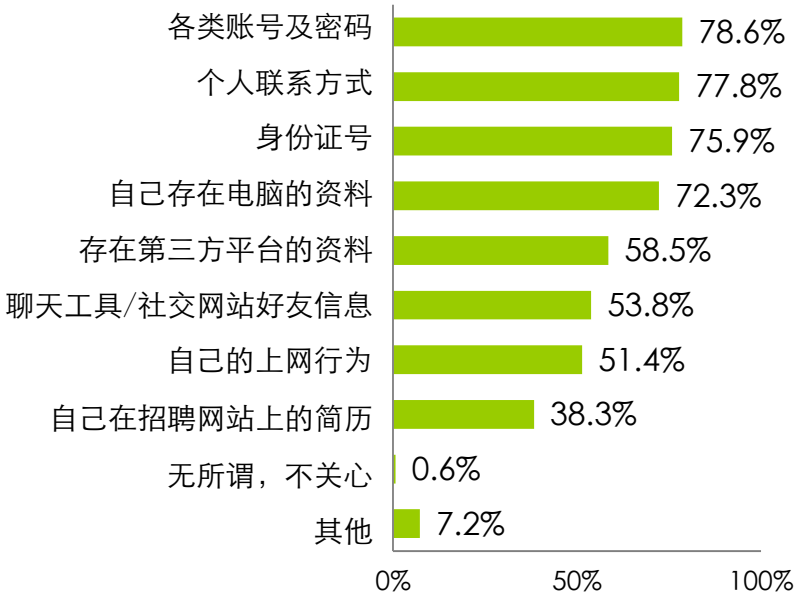


Source：样本量N=3229。于2012年12月在艾瑞iClick和QQ平台联合回收。

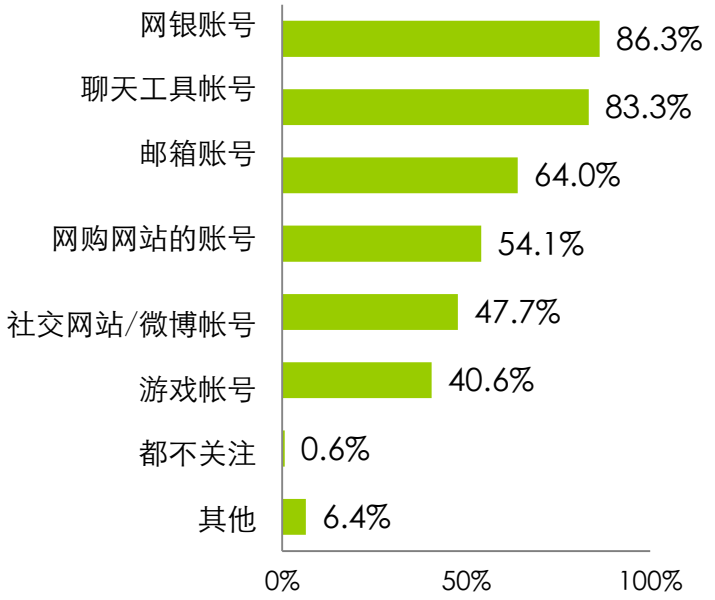
相对而言，账号和密码是网民最担忧的个人信息

- 根据艾瑞咨询调研显示，网民对与个人利益有直接挂钩的个人信息更为关注，如各类账号/密码、个人联系方式及身份证号；
- 其中，“网银账号”和“聊天工具账号”的安全性最受网民关注，关注度超过80%。

2012年网民对各类私人信息泄露的抗拒度



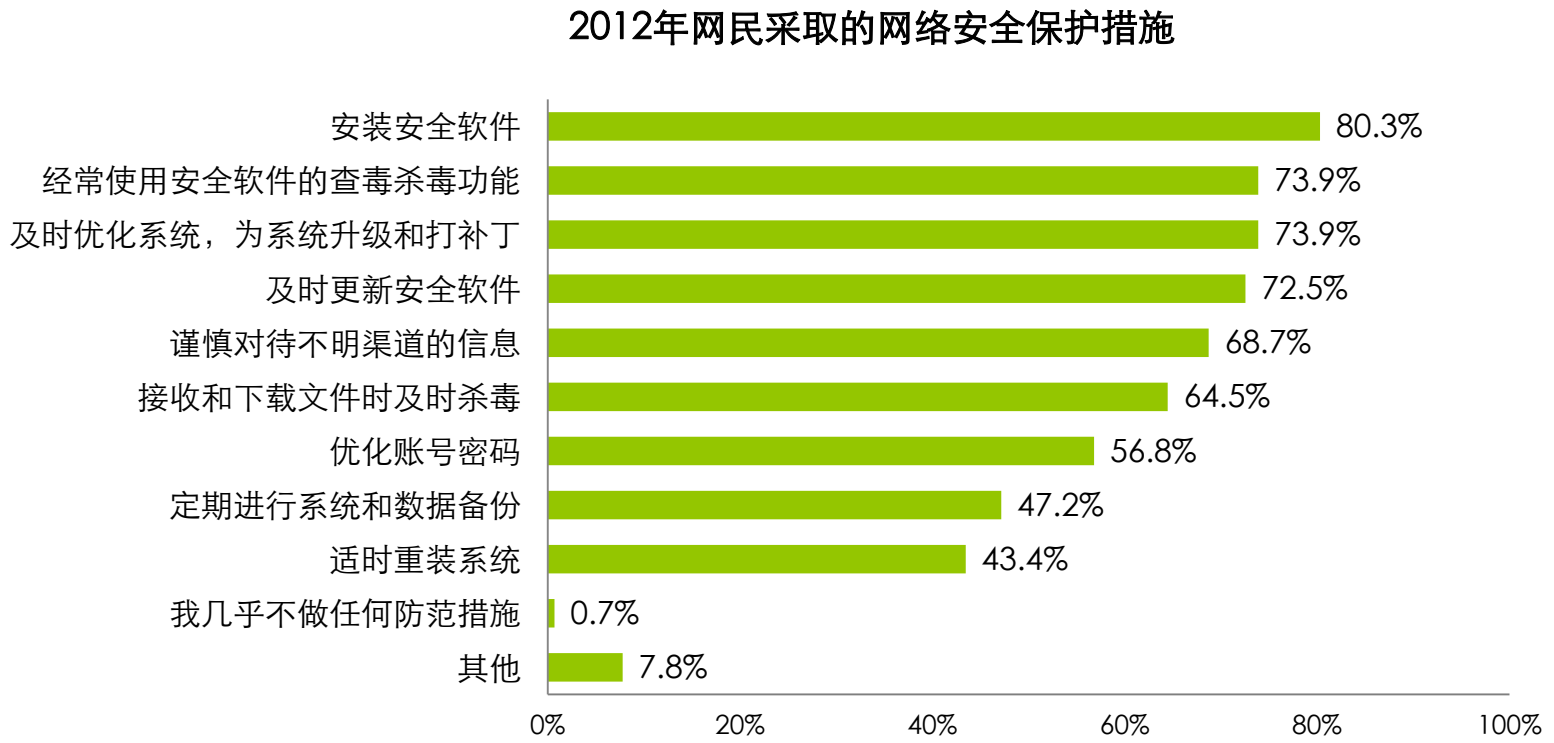
2012年网民对各类账号安全的关注度



Source：样本量N=3229。于2012年12月在艾瑞iClick和QQ平台联合回收。

安全软件是网民首选的网络安全保护措施

- 根据艾瑞咨询调研显示，网民保障自身网络安全更多依赖于安全软件，如安装安全软件、经常使用安全软件相关功能。

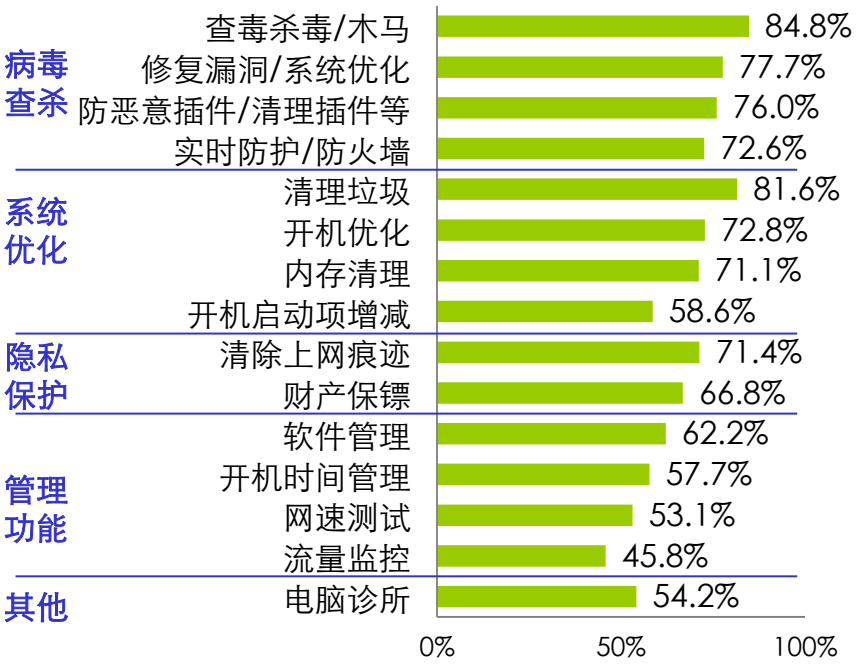


Source：样本量N=3229。于2012年12月在艾瑞iClick和QQ平台联合回收。

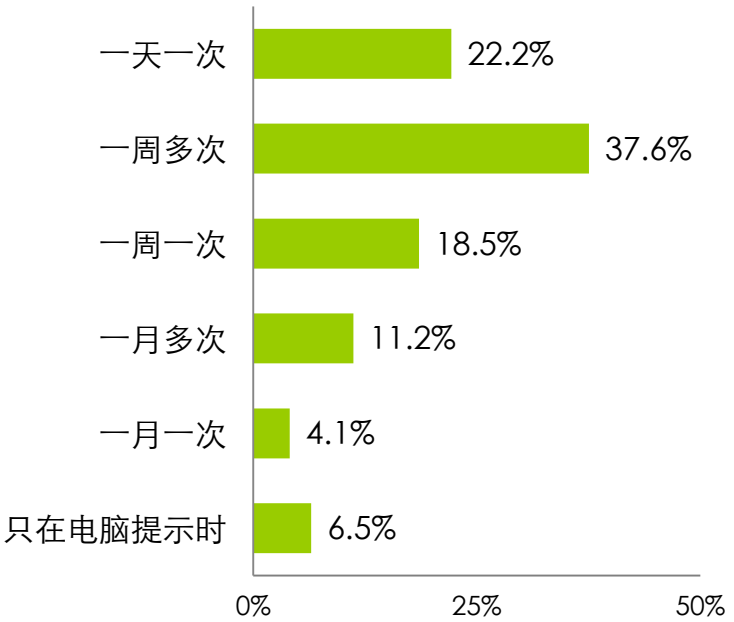
安全杀毒功能是用户使用率最高的功能

- 根据艾瑞咨询调研显示，网民对安全软件的使用以“安全杀毒”为核心，向“系统优化”、“隐私保护”等功能衍生；
- 网民主动查杀病毒频次高，78.2%用户表示每周至少主动查杀一次病毒。

2012年用户经常使用的安全软件功能



2012年用户查杀电脑病毒的频次



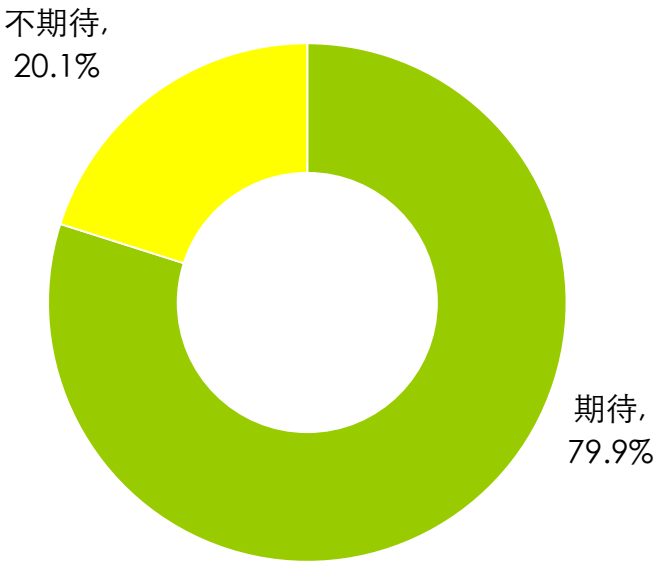
Source：样本量N=3229。于2012年12月在艾瑞iClick和QQ平台联合回收。

目录

近八成网民期待“网络安全立法”

- 根据艾瑞咨询调研显示，网民期待通过“完善政策法规” 来改善国内网络安全现状，79.9%网民持此态度。2012年年末颁布的《关于加强网络信息保护的决定》正是顺应主流民意。

2012年网民对通过“网络立法”改善网络安全的期待度

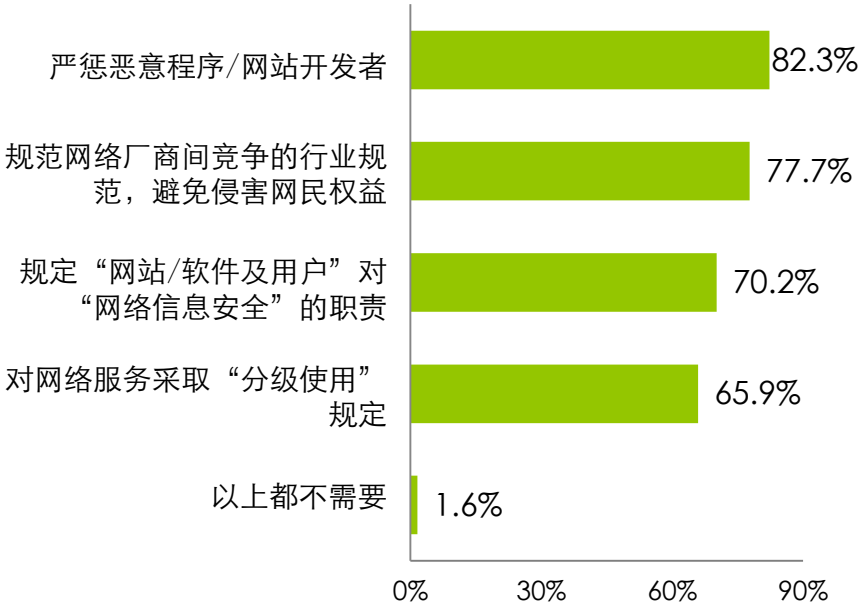


Source：样本量N=3229。于2012年12月在艾瑞iClick和QQ平台联合回收。

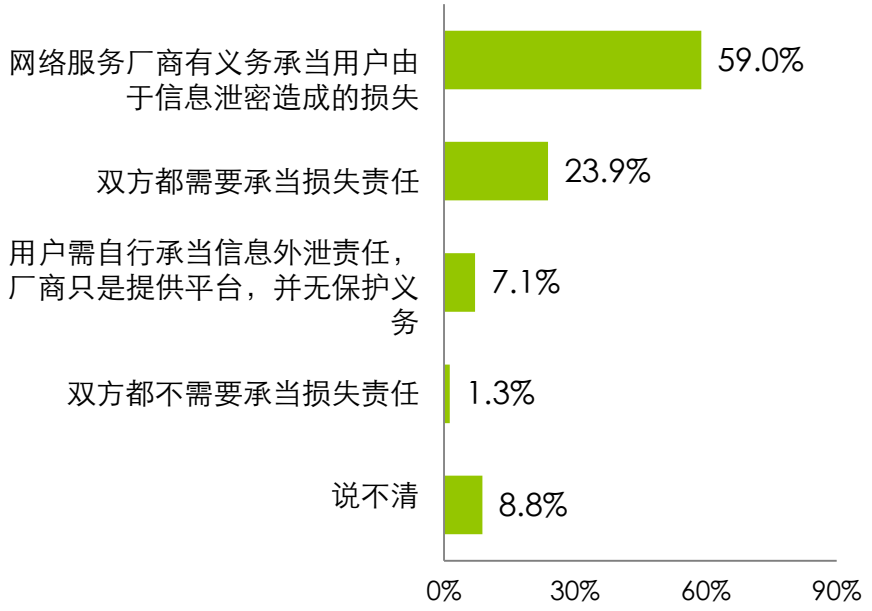
网民期待权责清晰、分级对待的法规出台

- 根据艾瑞咨询对网民调研数据分析：在立法层面上，网民期待通过对源头和行业发展层面规范立法解决网络威胁，82.3%网民期待能加大对“恶意程序/网站开发者”的惩罚力度；
- 70.2%网民期待立法明确“网络服务商和用户”对网络威胁的权责，大多数网民认为信息泄露的责任承担者应是网络服务厂商。

2012年网民期待出台的安全法规



2012年网民对于用户信息泄露的权责态度

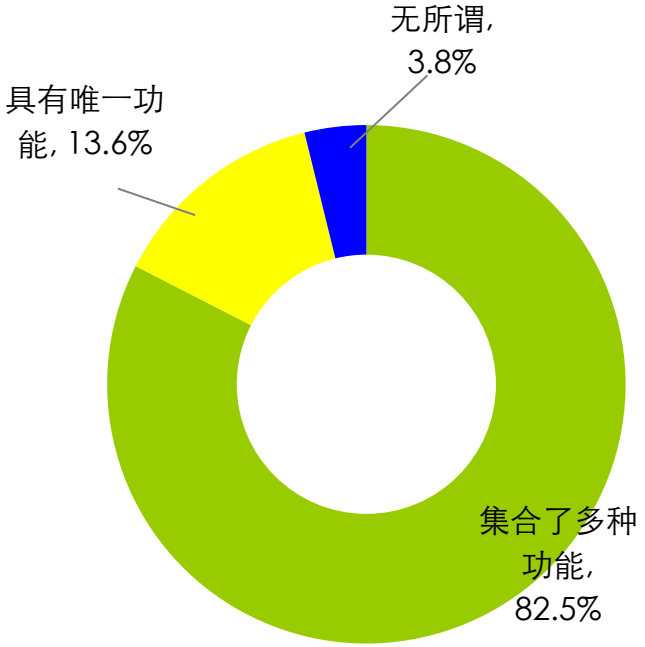


Source：样本量N=3229。于2012年12月在艾瑞iClick和QQ平台联合回收。

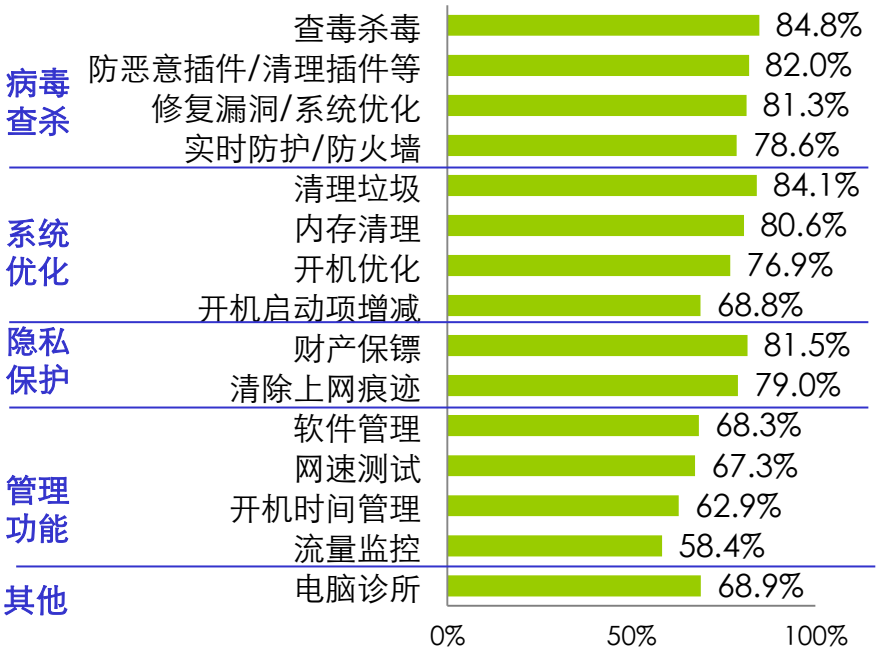
综合型安全软件更受网民欢迎

- 根据艾瑞咨询调研显示，网民偏好综合型的安全软件，82.5%网民表示更喜欢融合了“杀毒”和“管理”功能的安全软件；
- 细分软件功能看，基础防护类功能仍是网民需求度最高的功能，其次为系统优化类功能。

2012年网民对安全软件功能模式的偏好



2012年网民对安全软件的功能需求



Source：样本量N=3229。于2012年12月在艾瑞iClick和QQ平台联合回收。

附录一：研究方法

报告数据的收集和分析主要采用iUserSurvey在线问卷调查方法，结合腾讯电脑管家监测的后台数据、腾讯移动安全实验室提供的数据而获得。iUserSurvey是艾瑞公司专为网络媒体用户调研而开发的市场调研平台。

（一）艾瑞网络调研（网络用户）说明

✓ 调研方法

依据统计学理论和国际惯例，本次调查主要采用了计算机网上联机调查方法进行，问卷放置在iResearch的调研网站上，于2013年12月-2013年1月期间通过在iUserSurvey社区投放焦点图广告，由用户主动参与填写问卷的方式来获取信息。本次调研参与答卷人数达33862人，经处理排除无效问卷，并根据网民的性别和年龄进行配比加权，最终分析样本数为3229份。

✓ 关于网民男女性别年龄配额

根据CNNIC于2012年1月公布的网民性别分布和年龄分布进行配比加权。

（二）腾讯QQ电脑管家和腾讯移动安全实验室数据监测（行业研究）说明

行业研究部分的数据来源于腾讯电脑管家和腾讯移动安全实验室监测数据，其中，腾讯电脑管家监测时间为2012年1月1日-2012年12月31日，腾讯移动安全实验室监测时间为2012年1月1日-2012年9月30日。

附录二：概念定义

- **个人网络安全：**

个人网络安全是指使用个人计算机的网络用户保护所使用的计算机网络系统硬件、软件和数据，不因偶然和恶意的原因而遭到破坏、更改和泄漏，系统连续正常运行。

- **木马：**

木马是指通过入侵计算机、能够伺机盗取帐号密码的恶意程序，它是计算机病毒中的一种特定类型。木马通常会自动运行，在用户登录帐号的过程中记录用户输入的帐号和密码，并自动将窃取到的信息发送到黑客预先指定的信箱中。这将直接导致用户帐号被盗用，账户中的虚拟财产被转移。

- **恶意网站：**

恶意网站是指以获取经济利益为主要目的，故意在计算机系统上执行恶意任务的、以合法网站为载体的病毒、蠕虫或木马，或伪造合法网站的非法网站。

- **漏洞：**

漏洞是在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，从而可以使攻击者能够在未授权的情况下访问或破坏系统。

- **恶意插件：**

指表面上看有一定使用价值但同时具备一些电脑病毒和黑客程序特征的软件，表现为强行侵入上网用户的电脑，强行弹出广告，强迫用户接受某些操作，或在用户不知情的前提下，强行安装IE插件，不带卸载程序或无法彻底卸载，甚至劫持用户浏览器转到某些指定网站等。

- **社会工程学：**

社会工程学是指通过利用受害者心理弱点、本能反应、好奇心、信任、贪婪等心理陷阱，进行欺骗和伤害，取得自身利益的手法。

法律声明

公司服务介绍：

艾瑞咨询集团：http://www.iresearch.com.cn

公司产品介绍：

艾瑞客户解决方案：http://www.iresearch.com.cn/solution

艾瑞连续数据研究产品：http://www.iresearch.com.cn/product

艾瑞专项研究咨询服务：http://www.iresearch.com.cn/consulting

艾瑞研究观点报告：http://www.iresearch.com.cn/report

艾瑞学院培训业务：http://www.iresearch.com.cn/institute

艾瑞媒体会议服务：http://www.iresearch.com.cn/meeting

公司资讯网站：

艾瑞网：http://www.iresearch.cn

艾瑞广告先锋：http://www.iresearchad.com

艾瑞网络媒体精品推荐：http://www.iwebchoice.com

报告购买/咨询：

艾瑞市场咨询有限公司 北京

地址：北京市朝阳区金桐西路10号远洋光华国际AB座A501室，100020

电话：010-51283899-209

艾瑞市场咨询有限公司 上海

地址：上海市徐汇区漕溪北路333号中金大厦B幢701室，200030

电话：021-51082699-业务部

艾瑞市场咨询有限公司 广州

地址：广州市天河区159号中泰北塔707室，510620

电话：020 -38010229

报告总顾问：

杨伟庆iResearch总裁

Email: henry@iresearch.com.cn。

选择艾瑞，

选择可以信任的合作伙伴！

iResearch 艾瑞咨询集团 | 10 艾瑞十年 2002-2012