2015 年

中国互联网安全报告

360互联网安全中心

2016 年 2 月 29 日

摘　要

恶意程序：

- ✧ 2015 年全年，360 互联网安全中心共截获 PC 端新增恶意程序样本 3.56 亿个，和 2014 年相比增长 9.9%；360 安全卫士、360 杀毒共为全国用户拦截恶意程序攻击 855.4 亿次，相比 2014 年大幅增长 49.4%。
- ✧ 2015 年，从城市分布来看，拦截恶意程序攻击最多的城市为北京市（7.1%），其次为上海市（3.5%）、广州市（3.0%）、天津市（3.0%）、深圳市（3.0%）。
- ✧ 2015 年移动端累计监测到 Android 用户感染恶意程序 3.7 亿人次，较 2014 年增长了 15.0%，移动端恶意程序类型中资费消耗占比高达 73.6%；其次为恶意扣费（21.5%）和隐私窃取（4.1%），手机恶意程序趋利性极为明显。
- ✧ 2015 年，综合 PC 端和移动端遭到恶意程序攻击（云查询拦截）最多的地区为广东省（14.5%）、北京市（7.1%），其次为浙江省（6.7%）、河南省（5.8%）和江苏省（5.6%）。

钓鱼网站：

- ✧ 2015 年，360 互联网安全中心共拦截各类新增钓鱼网站 156.9 万个，相比 2014 年（262.1 万）下降了 40.1%；共为全国用户拦截各类钓鱼网站攻击 379.3 亿次，相比 2104 年（406 亿）下降了 6.6%。
- ✧ 在拦截的各类钓鱼网站攻击中，PC 端为 331.3 亿次，占 360 各类终端安全产品拦截钓鱼网站总量的 87.4%；手机端为 48.0 亿次，占 12.6%。手机端拦截的总攻击次数和在总拦截量中的占比，均创历史新高。
- ✧ 在新增钓鱼网站中，虚假购物的占比最大，达到了 44.7%，其次是金融理财 13.6%、虚假中奖 10.8%位列其后。而在钓鱼网站的拦截量方面，彩票钓鱼占到了 72.9%，排名第一，其次是虚假购物 10.8%、网站被黑 4.9%。
- ✧ 从拦截钓鱼网站次数（综合 PC 和移动端）的地域分布看，广东（28.9%）、北京（14.2%）、福建（9.7%）、广西（7.3%）、湖南（5.1%）等五省市拦截次数最多。
- ✧ 从钓鱼网站服务器的地域分布上看（按新增量统计），大约有 41.6%的钓鱼网站服务器分布在境内地区，58.4%在境外地区。从境内看，60.5%分布在香港，居于首位。从境外看，87.1%分布在美国。
- ✧ 从钓鱼网站服务器的地域分布上看（按拦截量统计），境内地区服务器占比大约在 25%，75%在境外地区。从境内看，20.4%分布在浙江，居于首位。从境外看，54.2%分布在美国。

骚扰电话：

- ✧ 2015 年，用户通过 360 手机卫士标记各类骚扰电话号码约 2.62 亿个（全年去重），比 2014 年增加了 2.3%；平均约 106.4 万个（当日去重）；识别和拦截各类骚扰电话 272.6 亿次，比 2014 年增加了 64.3%；平均每天识别和拦截 7468.5 万次。
- ✧ “响一声”电话以 37.0%的比例位居用户标记骚扰电话的首位；其次为广告推销（15.1%）、诈骗电话（9.5%）、房产中介（8.4%），保险理财（0.5%）。从骚扰电话识别和拦截情况

看，诈骗电话（21.0%）占比 21.0%位居首位，其次为广告推销（16.2%），“响一声”、房产中介和保险理财的占比分别为 11.4%、5.1%和 2.0%。

垃圾短信：

- 2015 年，360 手机卫士共为全国用户拦截各类垃圾短信约 318.3 亿条，较 2014 年（613 亿）下降了 48.1%。通过用户举报的垃圾短信内容分析来看，广告推销类短信最多，占比达 91.9%；其次是诈骗短信约占垃圾短信总量的 4.3%；违法短信占比为 3.8%。
- 在广告推销类垃圾短信中，电商网站推广类短信占到所有广告推销类垃圾短信的 23.5%，首次超于电信运营商和金融机构，成为垃圾短信发送的第一大户。之后为运营商推广（18.4%）、会员推广（10.5%）、实体商店推广（10.5%）、银行推广（9.5%）。
- 在诈骗短信中，92.9%的诈骗短信为身份冒充类短信，其次是打款诈骗，占 6.0%，其他各类诈骗短信占 1.1%。
- 在违法类垃圾短信中，代开发票垃圾短信占比最高，为 52.0%，之后依次为赌博类（33.5%）、办证刻章（4.9%）、复制电话卡（4.7%）、色情信息（2.9%）。
- 2015 年，根据 360 互联网安全中心的数据显示，广东地区用户接到的垃圾短信数量最多，占全国总量的 11.8%；其次为北京（7.2%）、江苏（6.2%）、河南（6.0%）、山东（5.6%）。

网络诈骗：

- 2015 年，猎网平台共收到网络诈骗举报 24886 例，举报总金额 1.27 亿余元，人均损失 5106 元。与 2014 年相比，举报数量只增长了 7.96%，但人均损失增却增长了将近 1.5 倍。其中，PC 用户举报 15913 例，人均损失 4840 元；手机用户举报 8973 例，人均损失约为 5577 元。
- 在所有举报的诈骗案情中，虚假兼职依然是举报数量最多的诈骗类型，共举报 8677 例，占比 34.9%；其次是网游交易 2059 例（占比 8.3%）、虚假中奖 1550 例（占比 6.2%）、退款欺诈 1380 例（占比 5.6%）和虚假购物 1253 例（占比 5.0%）。
- 而从涉案总金额来看，金融理财类诈骗最高，达 3768.6 万元，占比为 29.7%；其次是虚假兼职诈骗，涉案总金额为 2043.2 万元，占比为 16.1%；虚假中奖诈骗排第三，涉案总金额 1066.7 万元，占比为 8.40%。
- 在 PC 端被骗用户举报的所有案件中，虚假兼职以 41.6%排在首位，其次是网游交易 11.6%、退款欺诈 8.7%，这三种诈骗类型占 PC 端诈骗类举报总量的 61.9%。
- 在手机端被骗用户举报的所有案件中，虚假兼职以 23.0%排在首位，其次是虚假中奖 16.8%、账号被盗 10.7%，这三种诈骗类型占手机端诈骗类举报总量的 50.5%。
- 从诈骗信息传播的网络途径（不包括诈骗电话和诈骗短信的）看，社交工具是最主要途径，占 59.3%；其次是电子商务网站，占 26.2%；搜索引擎和分类信息网站分别占比 10.29%和 4.21%。在社交工具中，QQ 的占比最高，达 93.0%。
- 从用户举报情况来看，广东（3040 起）、山东（1992 起）、河南（1480 起）、江苏（1395 起）和四川（1354 起）这 5 个省级行政区的被骗用户最多。这 5 个地区用户的举报数量约占到了全国用户举报总量的 37.5%。

网站安全：

- 2015 年全年（截至 11 月 18 日），360 网站安全检测平台共扫描各类网站 231.2 万个，扫出存在漏洞的网站 101.5 万个，占比为 43.9%；其中存在高危漏洞的网站 30.8 万个，占扫描网站总数的 13.3%，
- 从检测出漏洞的危险等级看，高危占 21.7%，中危占 10.2%，低危占 68.1%。相比于 2014 年高中低危漏洞扫出数量较为平均，2015 年，高中危漏洞的扫出比例大幅下降。
- 从网站漏洞类型上看，跨站脚本攻击漏洞（21.9%）、异常页面导致服务器路径泄露（11.8%）和 SQL 注入漏洞（16.0%）这三类安全漏洞是占比最高的网站安全漏洞，三者之和接近网站所有漏洞检出总次数的一半。
- 2015 年截至 11 月 18 日，补天平台共收录漏洞 37943 个，涉及网站 26370 个；高危漏洞占比为 71.2%、中危漏洞占 9.3%，低危漏洞占 19.5%；事件型漏洞占比 86.3%，通用型漏洞占比 13.7%； SQL 注入漏洞最多，接近 50%，其次是弱口令和信息泄露，分别占 12.5%和 10.1%。
- 2015 年全年（截至 11 月 18 日），360 网站安全检测平台共扫描各类网站 231.2 万个，被篡改(不包括被植入后门程序)的网站 8.4 万个(全年去重)，比 2014 年下降了 52.5%，约占扫描网站总数的 3.6%，说明网站遭篡改情况明显好转。
- 2015 年全年（截至 11 月 18 日），360 网站安全检测共对 21854 台网站服务器进行了网站后门检测，扫描发现约 4097 台服务器存在后门，比 2014 年增加了 18.2%，占所有扫描网站服务器的 18.7%，占比较 2014 年减少了 22.5 个百分点。
- 2015 年全年（截至 11 月 18 日），360 网站卫士共拦截各类网站漏洞攻击 16.5 亿次，较 2014 年增长了约 135.7%。2015 年平均每天拦截漏洞攻击 512.2 万次。从漏洞攻击拦截量的类型分布看，SQL 攻击依然是最主要的攻击类型，占比达到 52.0%。
- 在补天平台收录的备案网站漏洞总量为 28050 个（共涉及 22084 个网站），其中高危漏洞为 18974 个。在备案网站中，企业网站的漏洞和高危漏洞的数量都是最多的，分别为 14981 个和 10092 个。
- 本报告对七个重点行业进行分析，共涵盖漏洞 5995 个（涉及网站 4280 个），高危漏洞 3944 个。统计显示，IT/互联网行业网站被报告的漏洞最多，达到 2330 个，高危漏洞 1463 个。
- 从个人信息泄露情况看，补天收录的“泄露信息的漏洞”（这与单纯技术上的“信息泄露漏洞”不是一个概念），共涉及网站 1282 个，可能泄露的个人信息量高达 55.3 亿条。

关键词：恶意程序、钓鱼网站、骚扰电话、垃圾短信、网络诈骗、网站安全

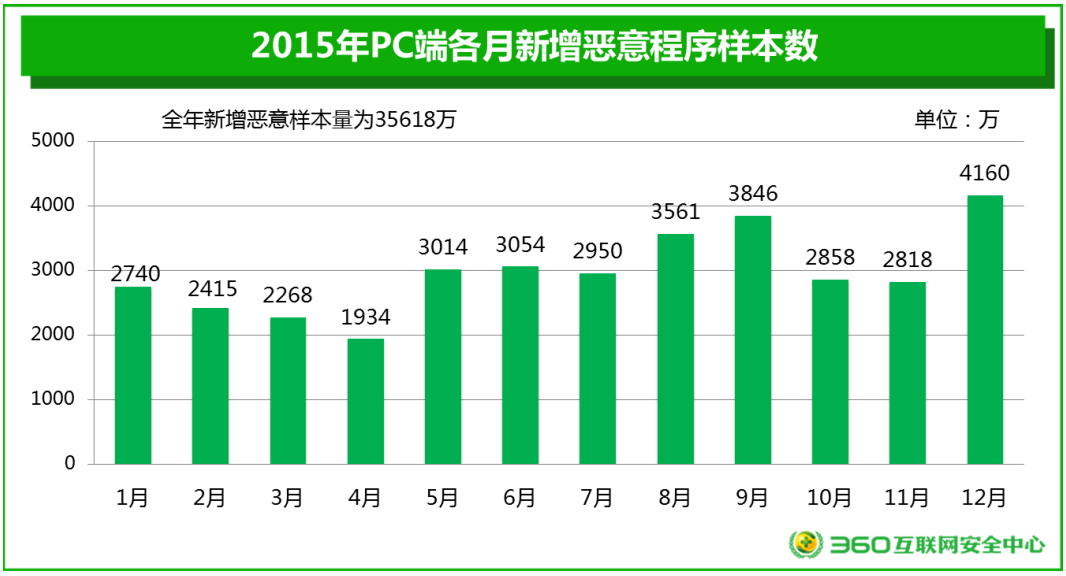
目　　录

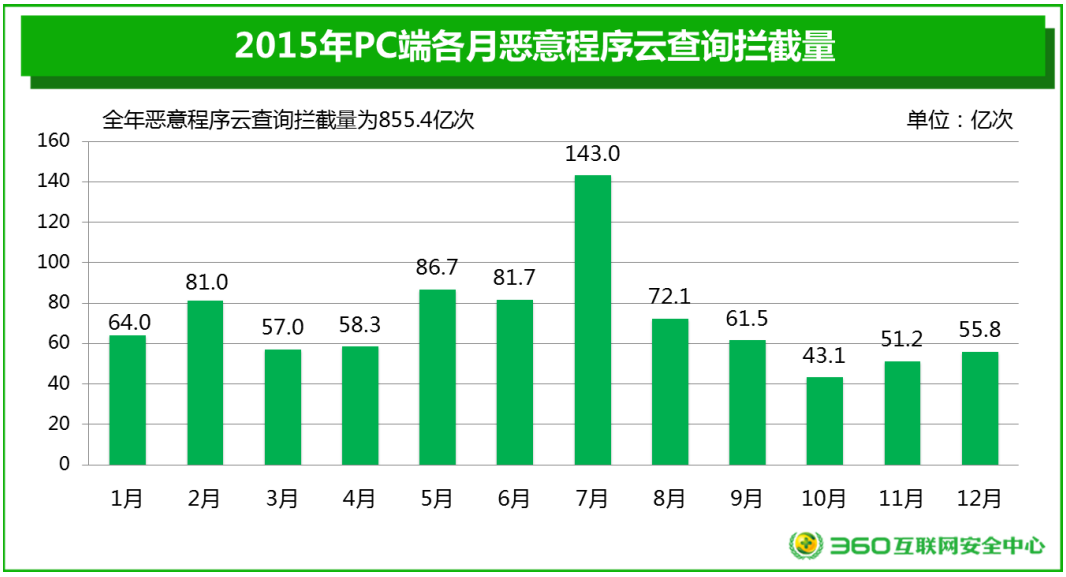
第一章 恶意程序

一、 恶意程序新增量与拦截量

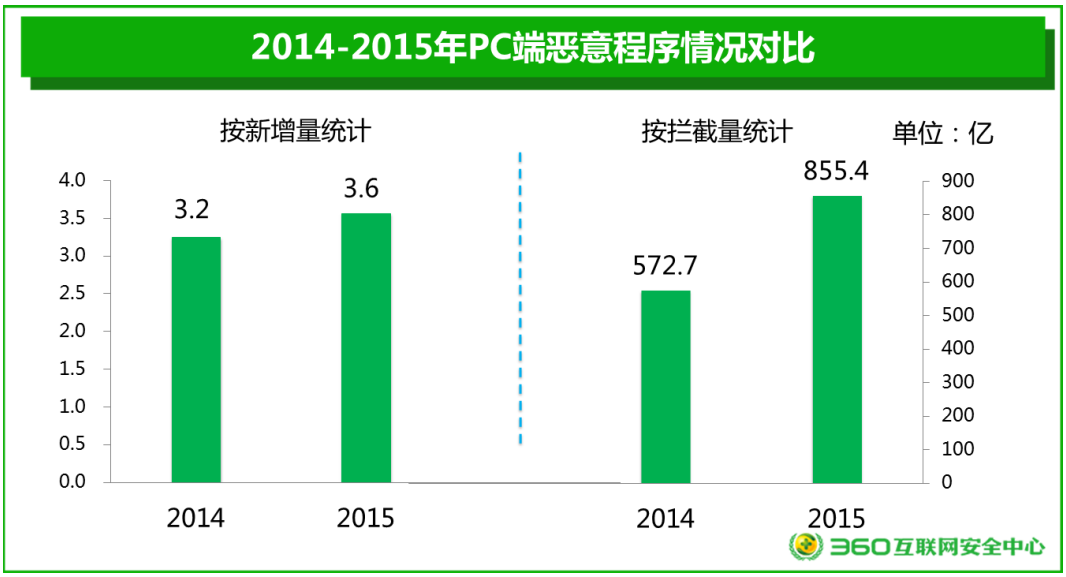
2015 年全年，360 互联网安全中心共截获 PC 端新增恶意程序样本 3.56 亿个，和 2014 年相比增长 9.9%；平均每天截获新增恶意程序样本 97.7 万个。360 安全卫士、360 杀毒共为全国用户拦截恶意程序攻击 855.4 亿次，相比 2014 年大幅增长 49.4%；平均每天为用户拦截恶意程序攻击约 2.3 亿次。

下面两图分别给出了 2015 年各月 PC 端恶意程序新增量和拦截量月度统计情况。

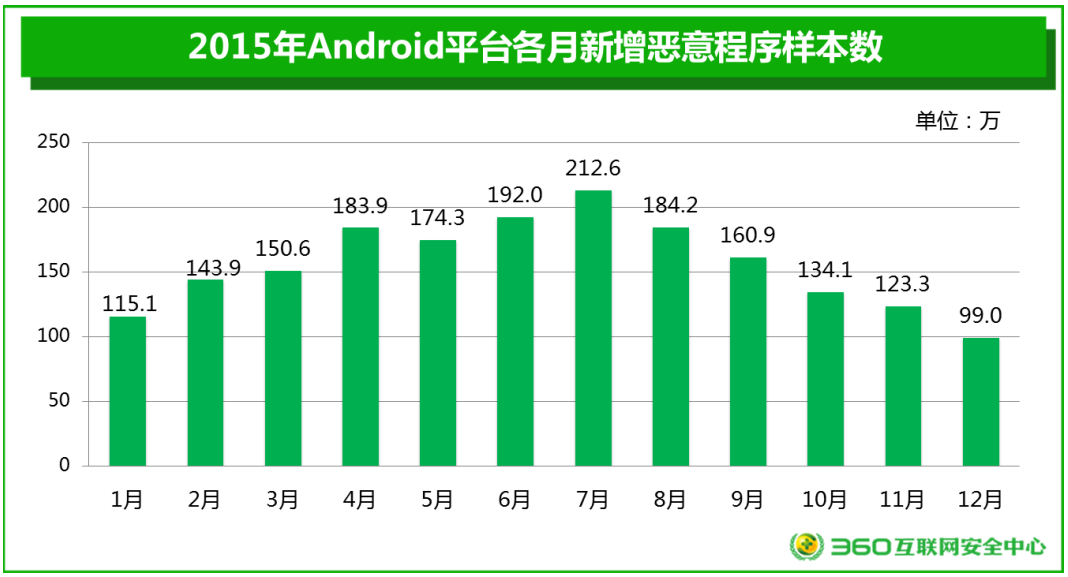




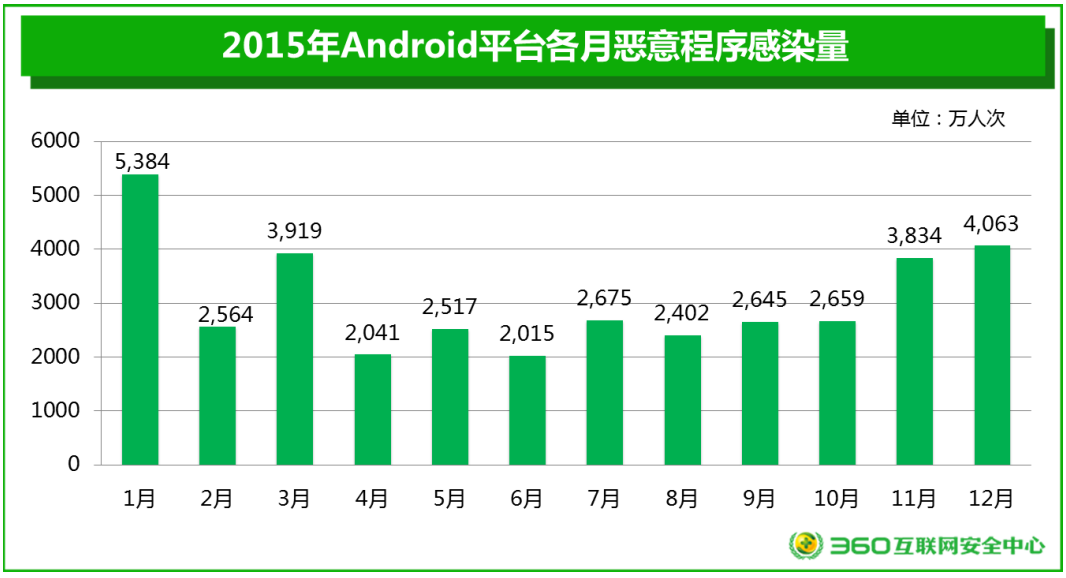
下图给出了最近两年，PC 端恶意程序新增量和云查询拦截量的对比情况。



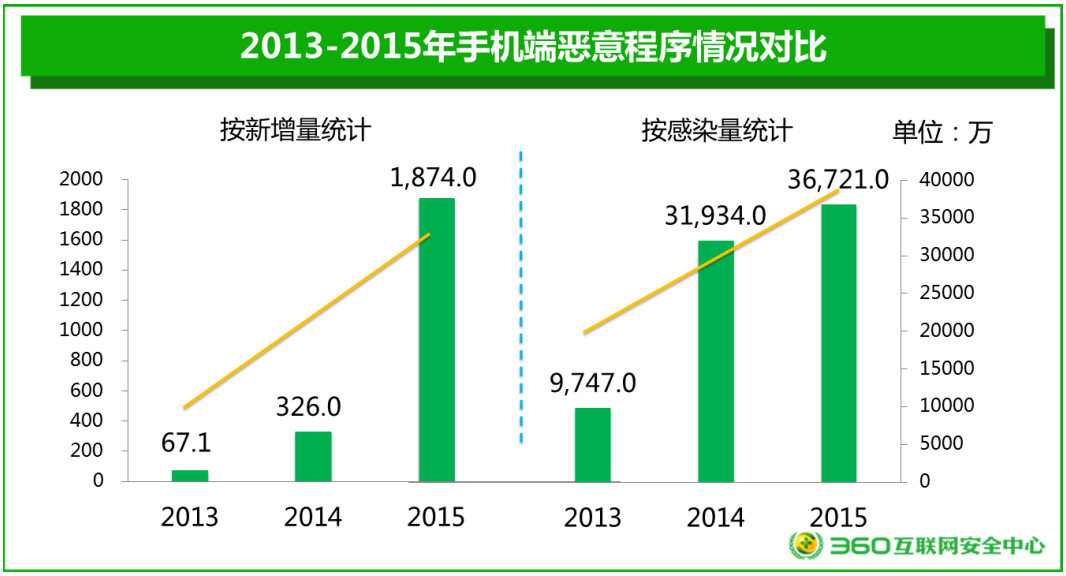
2015 年全年，360 互联网安全中心累计截获 Android 平台新增恶意程序样本 1874.0 万个，是 2014 年的 5.7 倍；平均每天截获新增恶意程序样本也高达 51342 个。下图是 2015 年各月 Android 平台新增恶意程序样本量的分布图。由图可见，新增恶意程序整体呈现中间高、两头低的态势，即上半年各月新增恶意程序量整体呈现上升，在 7 月达到最高峰。下半年从 8 月开始逐月下降，12 月份达到最低。



2015 全年，360 互联网安全中心累计监测到 Android 用户感染恶意程序 3.7 亿人次，较 2014 年增长了 15.0%；平均每天恶意程序感染量达到了 100.6 万人次。下图是 2015 年 Android 平台新增恶意程序感染量的按月分布图，分析可知，下半年恶意程序感染量和上半年相比，基本持平，但上半年波动较大，全年最高值和最低值分别出现在 1 月（5384 万）、6 月（2015 万）。下半年各月感染量略显平均，11 月和 12 月高于其他各月。



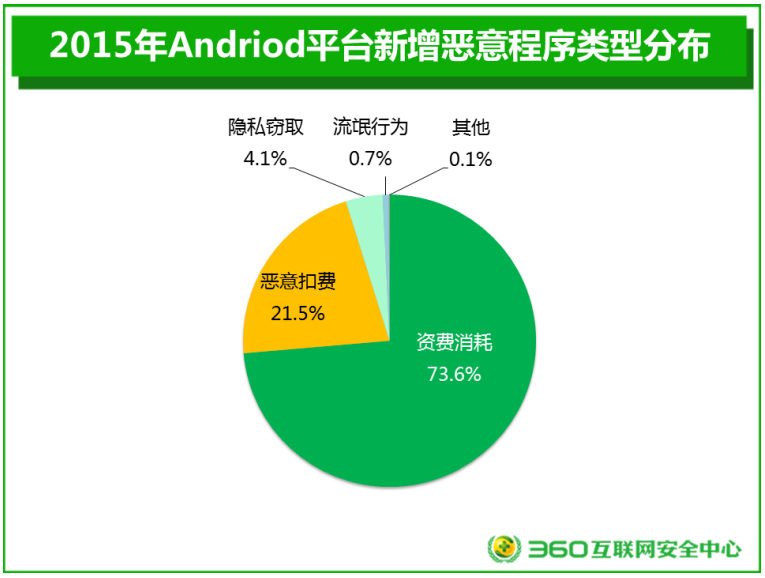
从 2013 年到 2015 年的情况看，2015 年手机端恶意程序样本新增量迅猛增长。从拦截量看，2014 年和 2015 年的拦截量相比 2013 年有大幅增长，近两年增长速度相对放缓。



2015 年，Android 平台新增恶意程序的样本量与感染量都一定幅度的提升，主要是因为 Android 系统、APP 的普及与发展，带动了 Android 手机等智能终端用户量的持续攀升，从而导致黑客的攻击目标也逐渐转向移动端。

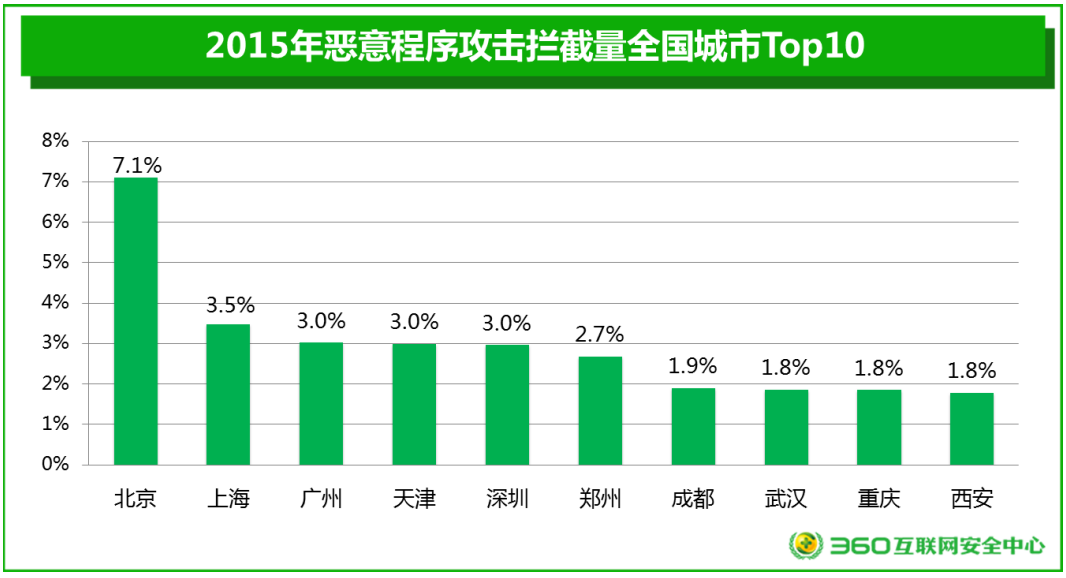
根据中国反网络病毒联盟的分类标准，360 互联网安全中心在 2015 全年监测的 Android 平台恶意程序的分类统计如下图。

从图中可见，2015 年 Android 平台新增恶意程序主要是资费消耗，占比高达 73.6%；其次为恶意扣费（21.5%）和隐私窃取（4.1%）。可以看到，已经有 90%以上的移动恶意程序是直接冲着用户“钱包”来的，关切到用户直接的经济损失。

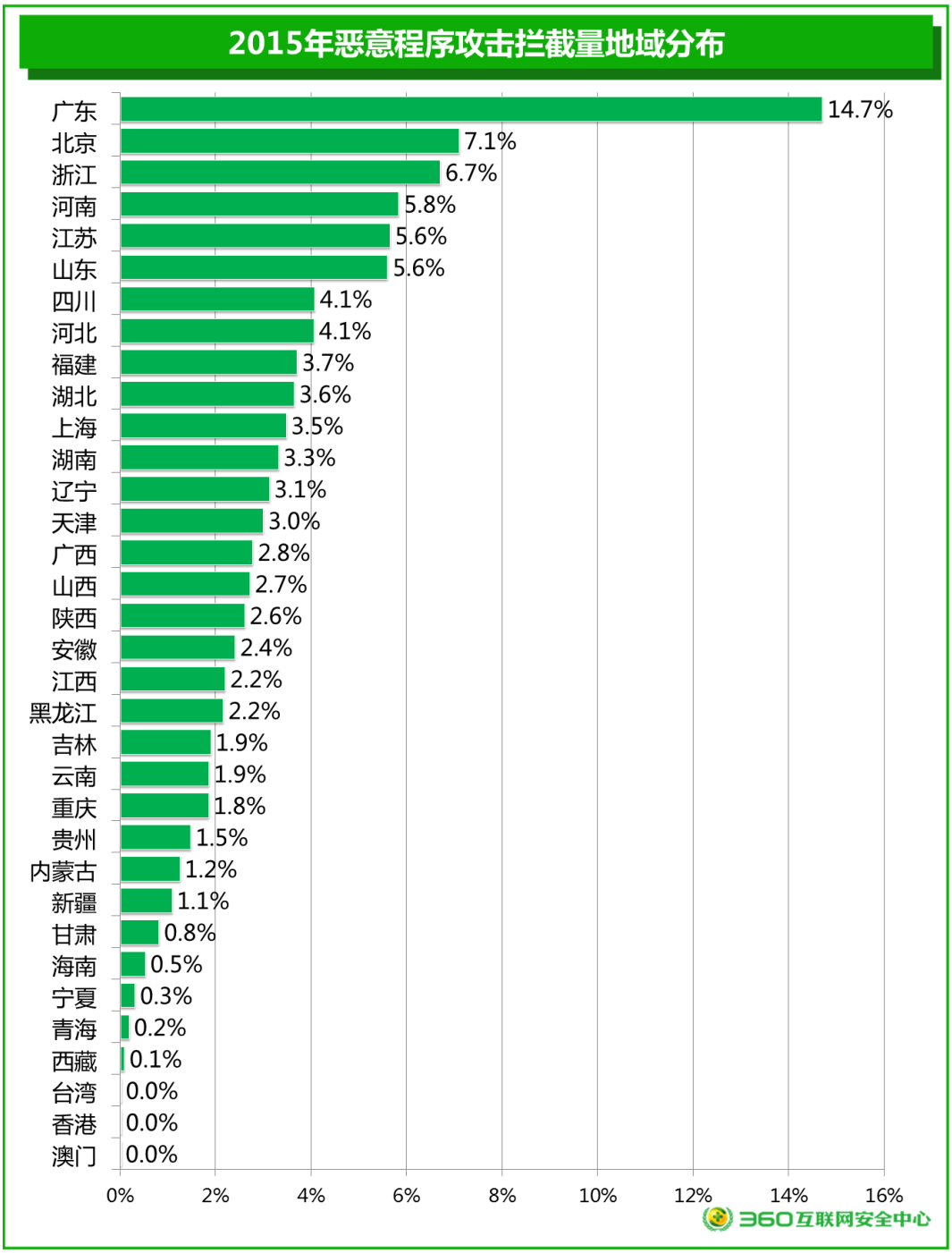


二、 恶意程序地域分布

2015 年，从城市分布来看，恶意程序攻击拦截次数（综合 PC 端和移动端情况）排名前十的城市，占全国拦截攻击总量的 29.6%。其中拦截最多的城市为北京市（7.1%），其次为上海市（3.5%）、广州市（3.0%）、天津市（3.0%）、深圳市（3.0%）。



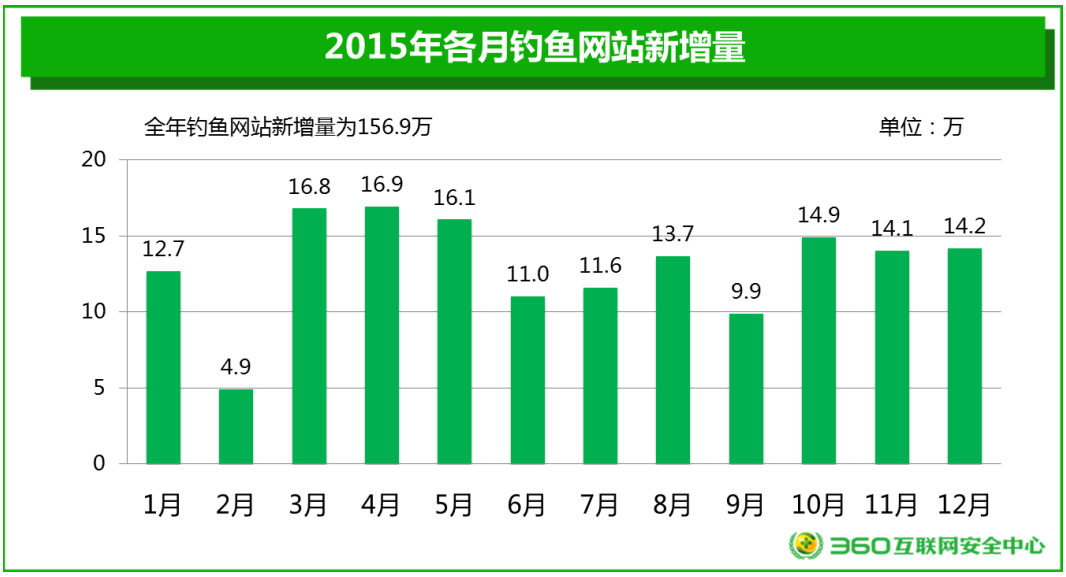
2015 年，从省级地域分布来看，遭到恶意程序攻击（云查询拦截量。综合 PC 端和移动端）最多的地区为广东省，占全国恶意程序攻击总量的 14.5%，其次为北京市（7.1%），浙江省（6.7%）、河南省（5.8%）和江苏省（5.6%）。



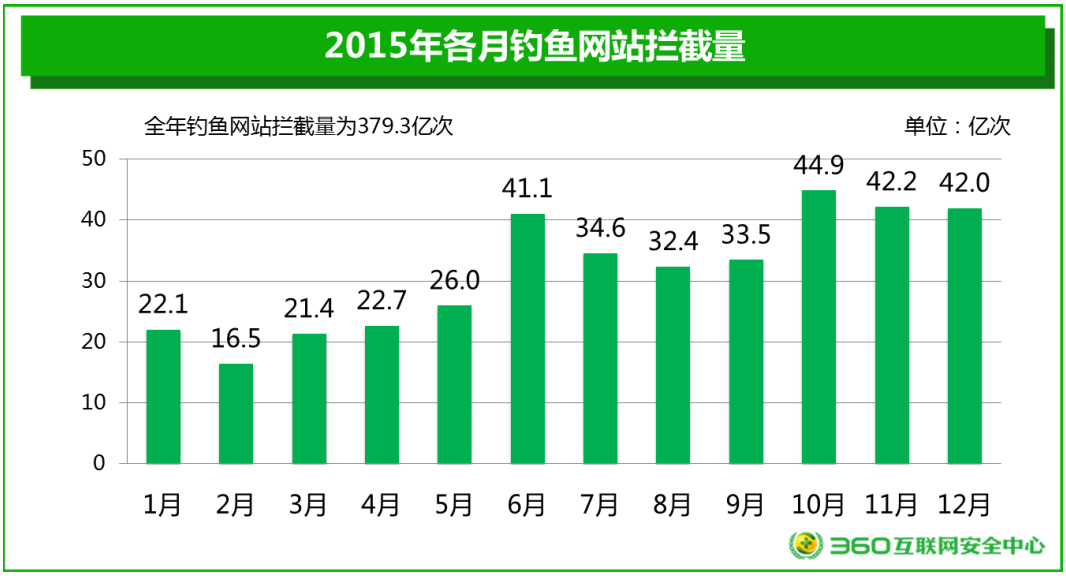
第二章 钓鱼网站

一、 钓鱼网站新增量与拦截量

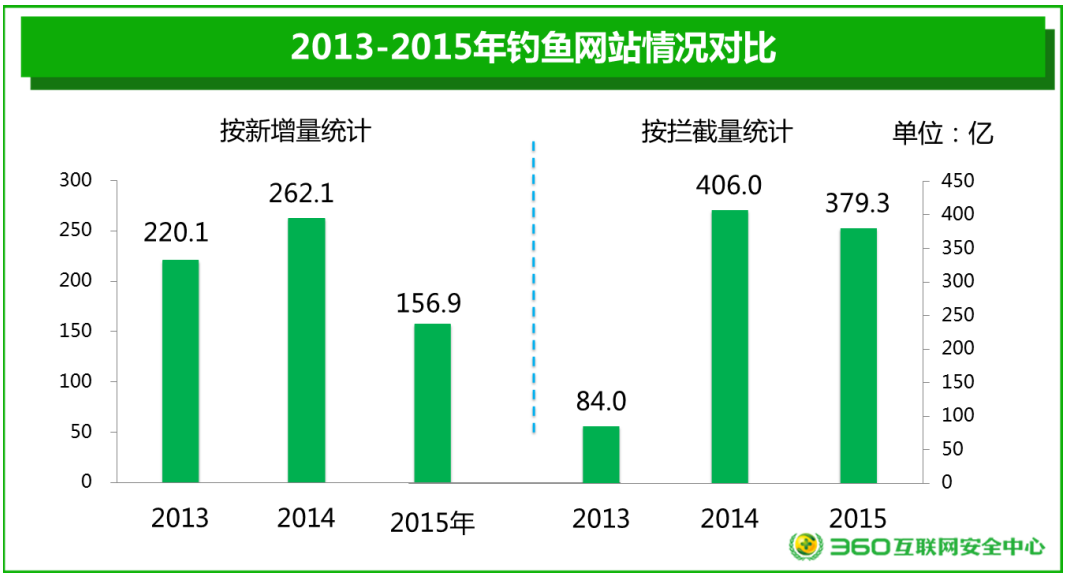
2015 年全年，360 互联网安全中心共截获各类新增钓鱼网站 156.9 万个，相比 2014 年下降了 40.1%；平均每天截获新增钓鱼网站 4299 个。从各月来看，3 月（16.8 万）、4 月（16.9 万）、5 月（16.1 万）的新增钓鱼网站最多，具体见下图：



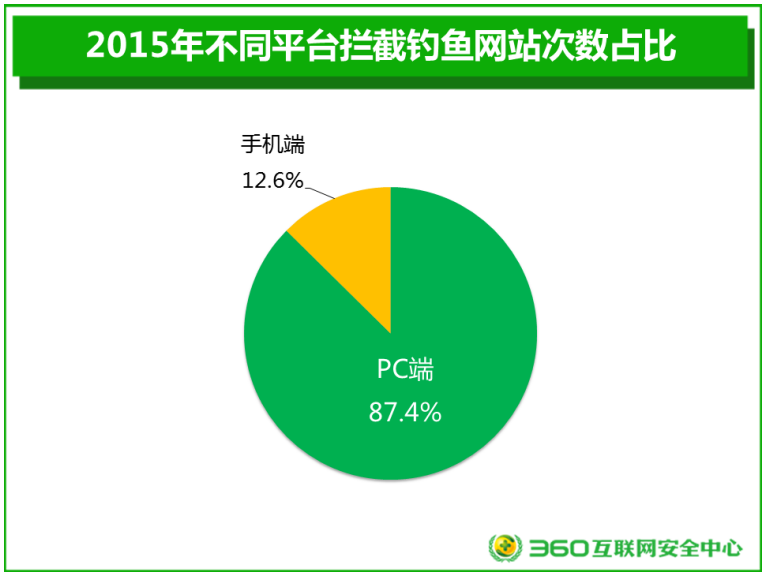
2015 年，360 互联网安全产品共为全国用户拦截各类钓鱼网站攻击 379.3 亿次，相比 2014 年（406 亿）下降了 6.6%；平均每天拦截钓鱼网站攻击 10392 万次。按月度分布如下图。从各月上看，钓鱼网站拦截量大致呈现逐步增长态势。



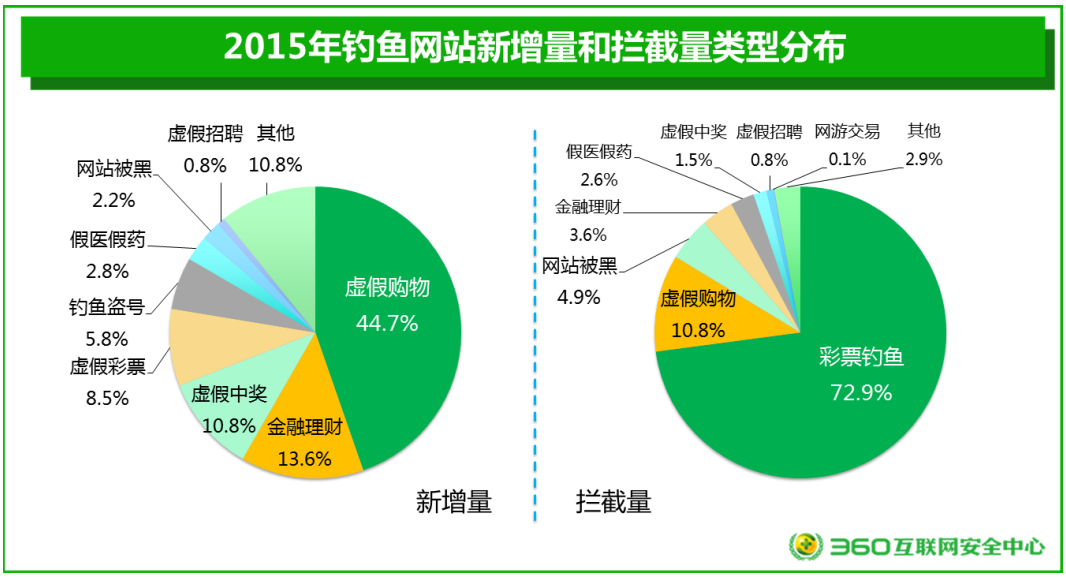
从 2013 年到 2015 年的情况看，2015 年 360 互联网安全产品截获的钓鱼网站新增量和 2013 年、2014 年有一定幅度下降。与此同时，在拦截量方面，相比 2013 年，2014 年和今年的拦截量增长了 3 至 4 倍，增长速度惊人。



2015 年，在拦截的各类钓鱼网站攻击中，PC 端为 331.3 亿次，占 360 各类终端安全产品拦截钓鱼网站总量的 87.4%；手机端为 48.0 亿次，占 12.6%。手机端拦截的总攻击次数和在总拦截量中的占比，均创历史新高。

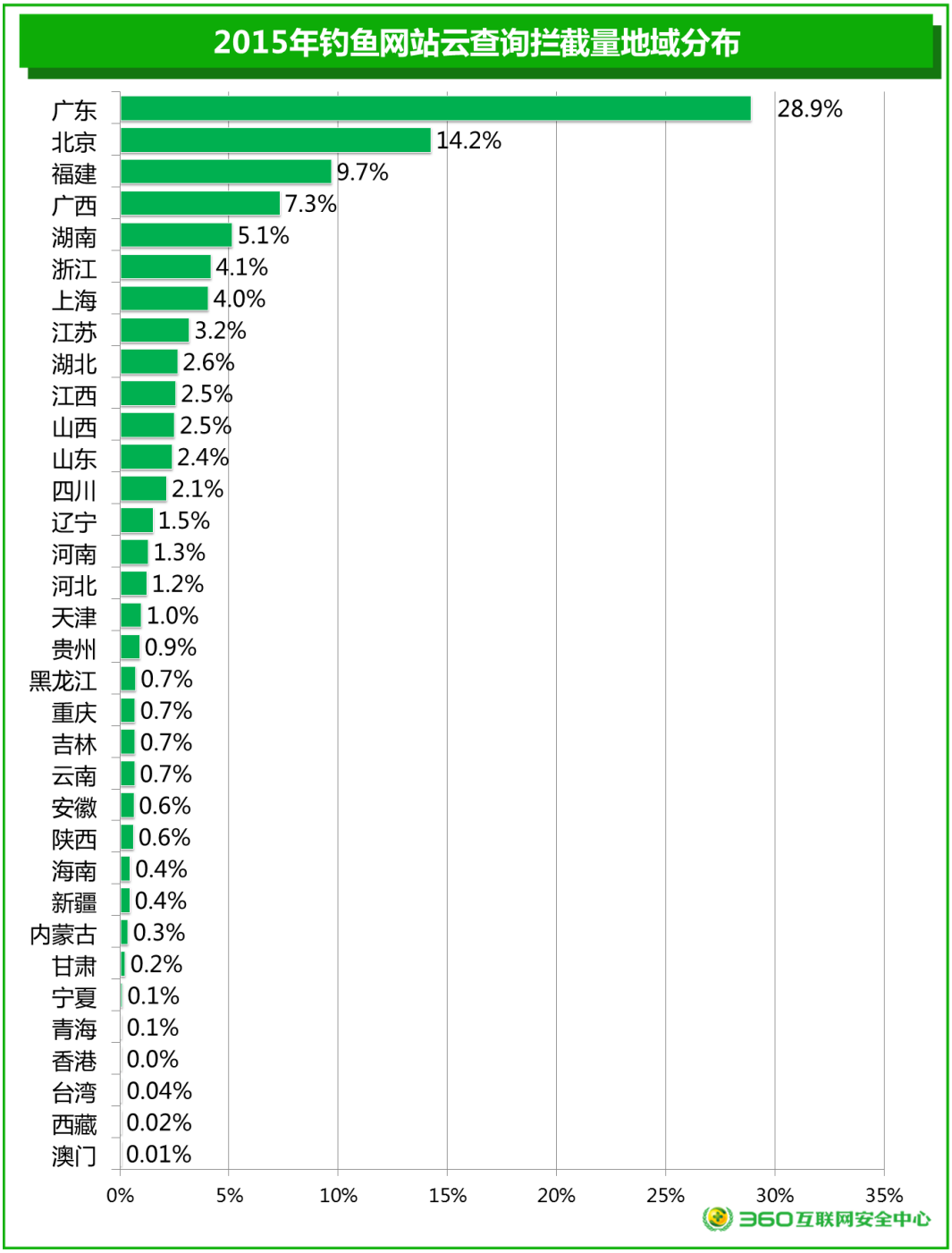


在新增钓鱼网站中，虚假购物的占比最大，达到了 44.7%，其次是金融理财 13.6%、虚假中奖 10.8%位列其后。而在钓鱼网站的拦截量方面，彩票钓鱼占到了 72.9%，排名第一，其次是虚假购物 10.8%、网站被黑 4.9%。



二、 钓鱼网站拦截量地域分布

综合 PC 和移动端拦截钓鱼网站的地域分布情况见下图，可以看出广东（28.9%）、北京（14.2%）、福建（9.7%）、广西（7.3%）、湖南（5.1%）等五省市拦截次数最高。

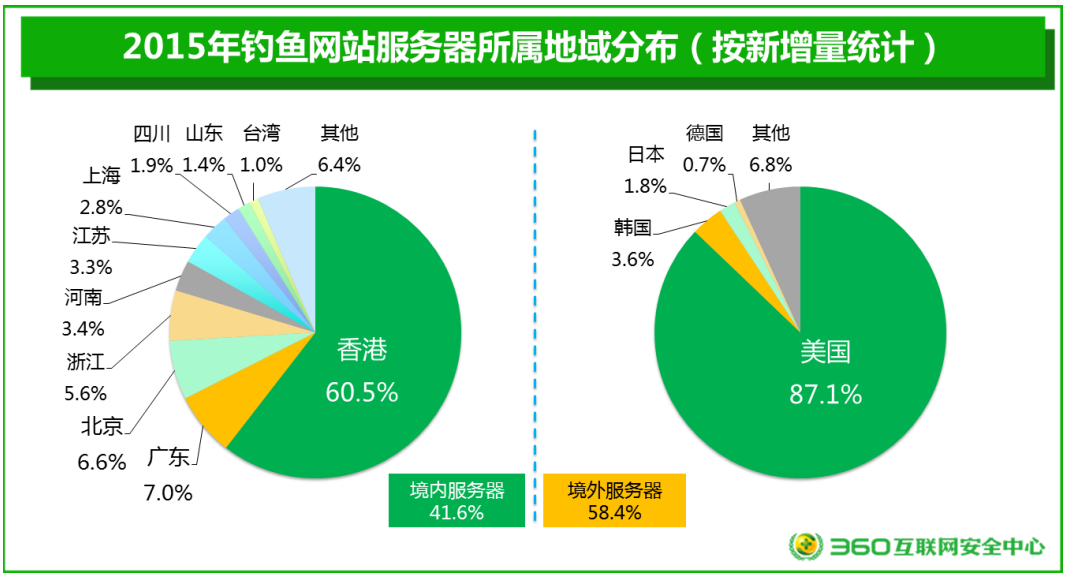


三、 钓鱼网站服务器地域分布

综合 PC 端和手机端钓鱼网站情况，新增钓鱼网站服务器的地域分布情况为：大约有 41.6%的钓鱼网站服务器分布在境内地区，58.4%在境外地区。

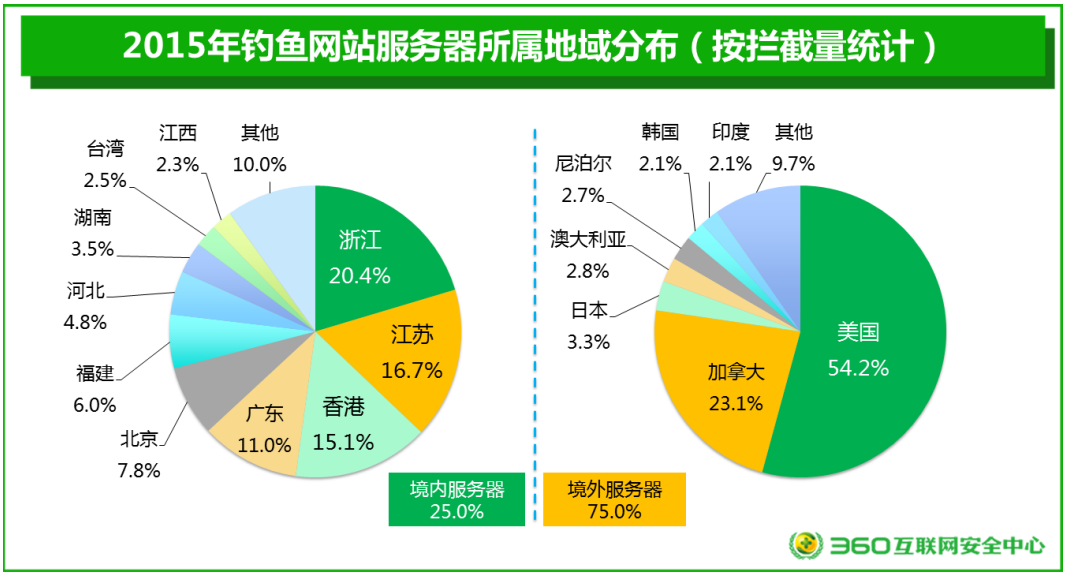
从境内新增钓鱼网站服务器地域分布上看，60.5%分布在香港，居于首位；其次分别为广东（7.0%）、北京（6.6%）、浙江（5.6%）、河南（3.4%）。

从境外新增钓鱼网站服务器地域分布上看，87.1%分布在美国，接近境外所有钓鱼网站服务器总量的九成，其次是韩国（3.6%）、日本（1.8%）。



从钓鱼网站拦截量来看，大约有 75%的服务器分布在境外地区，25%在境内地区。

从境内钓鱼网站服务器地域分布上看，20.4%分布在浙江，居于首位；其次分别为江苏（16.7%）、香港（15.1%）、广东（11.0%）、北京（7.8%）。从拦截钓鱼网站境外服务器地域分布上看，54.2%分布在美国，超过境外服务器总量的一半。其次是加拿大（23.1%）、日本（3.3%）、澳大利亚（2.8%）、尼泊尔（2.7%）等地区。



四、 钓鱼网站举例

钓鱼网站使用了包括模仿正规网站域名、篡改正规网站页面、特殊设计躲避安检、适配手机定向钓鱼等多种花样的钓鱼攻击技术来欺骗用户，并与安全厂商“斗法”，而且钓鱼网站所仿冒的对象也是应有尽有。下面根据不同类型的钓鱼网站举出若干例子：

1）模仿正规网站域名： 如模仿奇酷、小米、华为手机的钓鱼网站域名，如果光看域名前缀，很容易上当。

http://qiku.18cr2ni4wa.com.cn/

http://qiku.couchstore.com.cn/x7.htm

http://qiku.aeropower.com.cn/qiku_qcb.htm

http://www.360neigoubao.com/

http://xiaomi.beaucraft.com.cn/

http://m5.ebote.com.cn/xminote/note.asp?k=小米众筹

http://vmall.couchstore.com.cn/

2）篡改正规网站页面

某事业单位备案的网站被黑成了虚假游戏交易平台

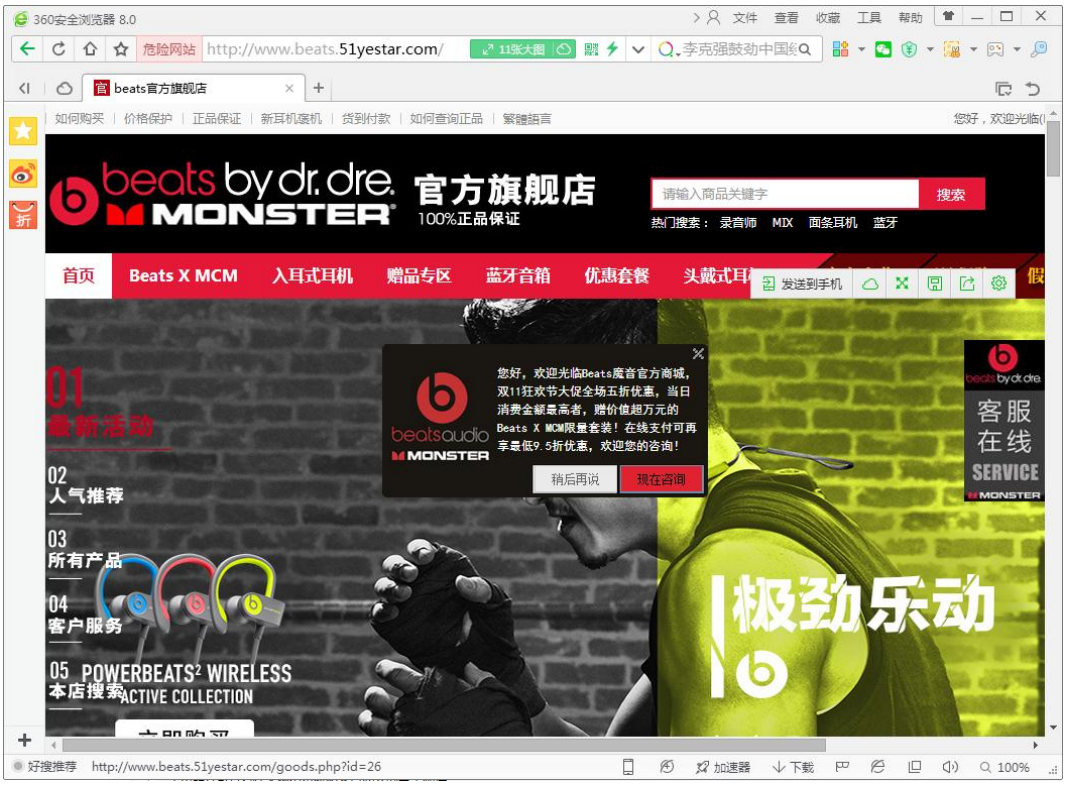
某报业网站被黑成了游戏交易平台

某云服务平台被骗子用来搭建钓鱼网站

3）冒充商业品牌官网的钓鱼网站

假冒纽百伦（NewBalance）官网

假冒摩声耳机官网的钓鱼网站



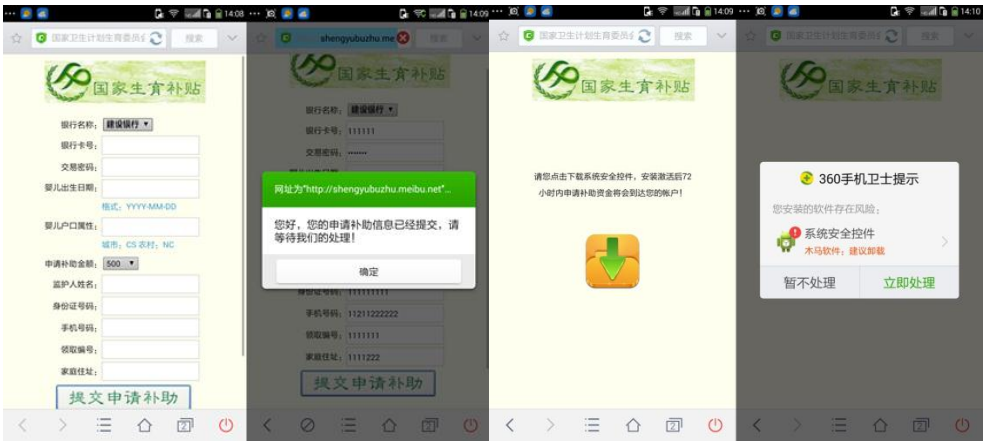
假冒淘宝店铺的钓鱼网站

同时假冒三大运营商的钓鱼网站

4）还有一些适配手机端的钓鱼网站，如冒充银行官网、冒充政府机构等，专门适配手机终端访问页面，迷惑性非常高。

冒充银行实名补录界面的钓鱼网站

某个冒充政府机构发放所谓生育补贴的钓鱼网站（含木马下载连接）

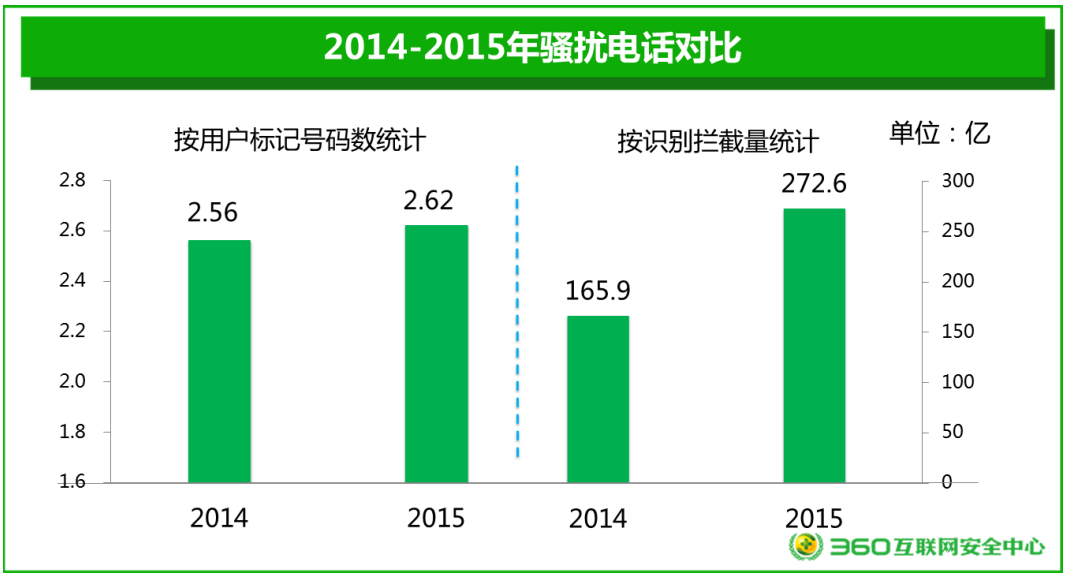


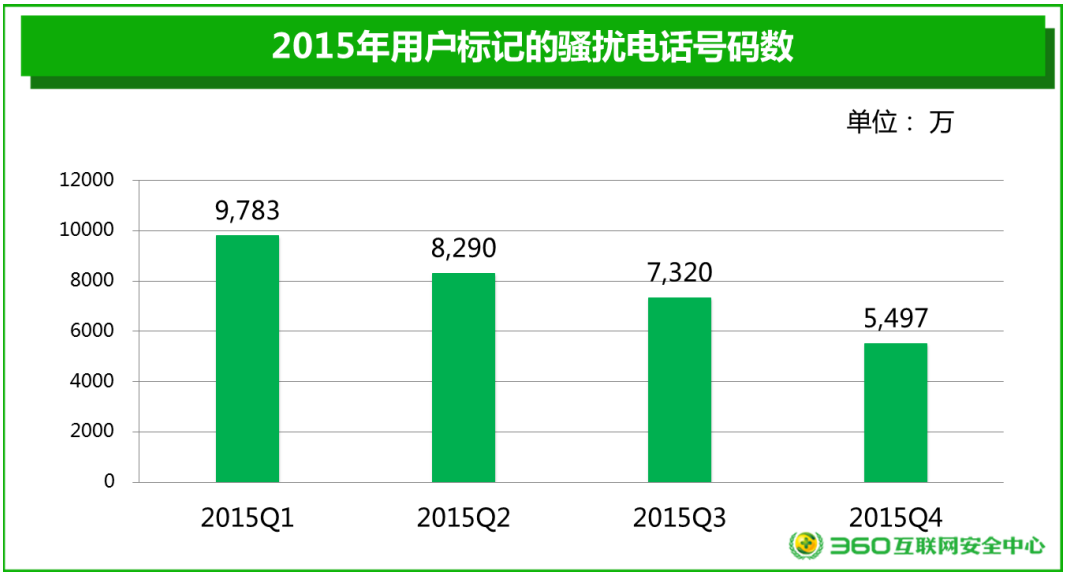
5）其他手机端典型钓鱼网站，如假冒正规手机厂商网站、假冒中国移动积分兑换的钓鱼网站等。

第三章 电信骚扰

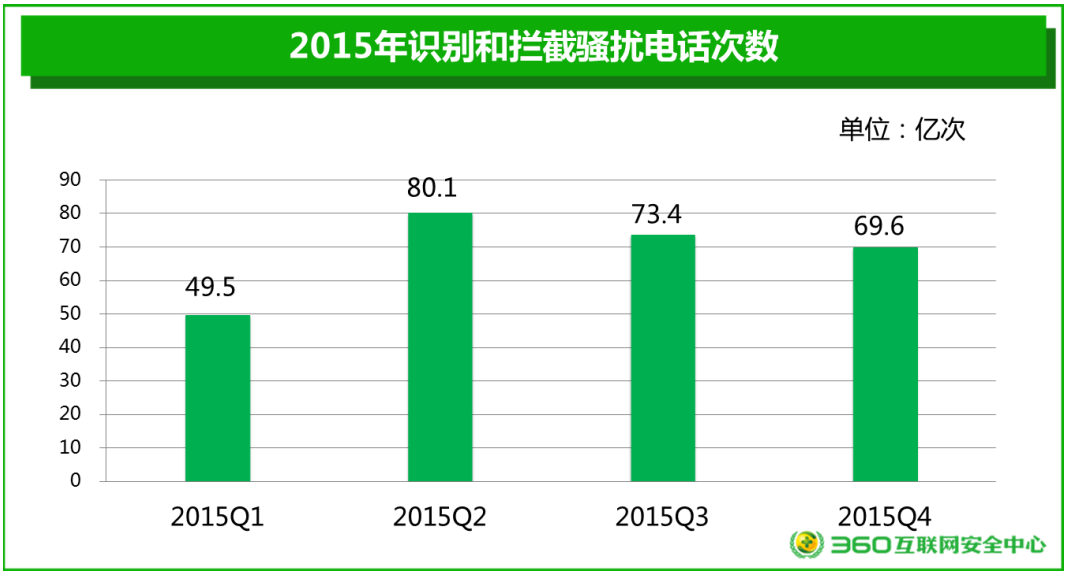
一、 骚扰电话号码标记量与拦截量

2015 年，用户通过 360 手机卫士标记各类骚扰电话号码（包括 360 手机卫士自动检出的响一声电话）约 2.62 亿个（全年去重），比 2014 年（2.56 亿）增加了 2.3%；平均每天被用户标记的各类骚扰电话号码约 106.4 万个（当日去重）；其中一季度用户标记的骚扰电话号码数量最多，达到 9783 万个（当季去重）。总体来看，骚扰电话的标记量呈现逐季度下降的趋势。这种情况在最近几年中还是首次出现。





2015 年，360 手机卫士共为全国用户识别和拦截各类骚扰电话 272.6 亿次，比 2014 年（165.9 亿）增加了 64.3%；平均每天识别和拦截骚扰电话 7468.5 万次。其中第二季度识别和拦截骚扰电话次数最多，高达 80.1 亿次。下图给出了 2015 年 360 手机卫士各季度识别和拦截骚扰电话的次数。

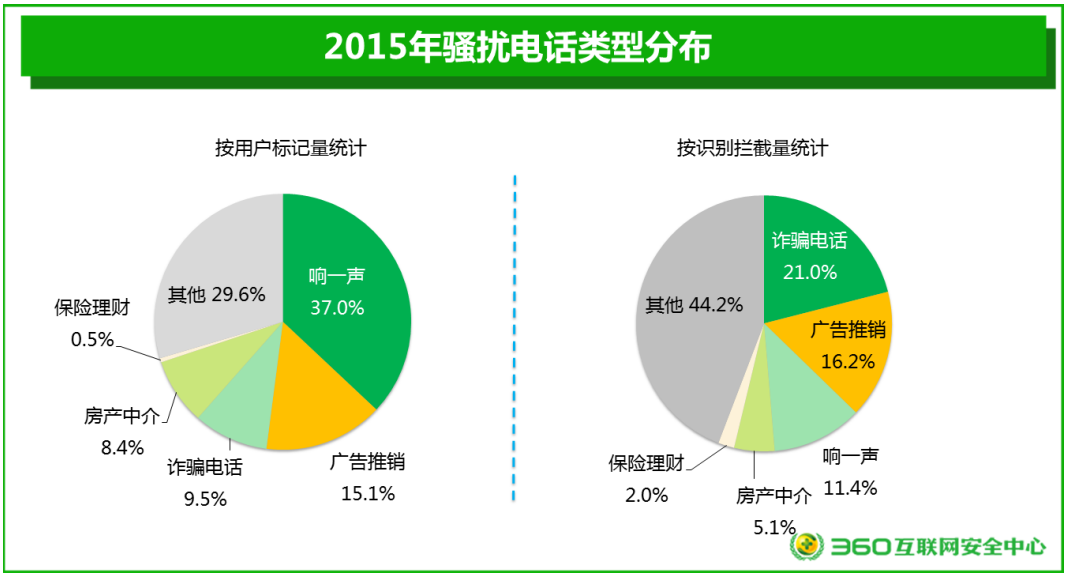


二、 骚扰电话类型分布

综合 360 互联网安全中心 2015 年全年的拦截监测与用户标记情况、用户调研分析，“响一声”电话以 37.0%的比例位居用户标记骚扰电话的首位；其次为广告推销（15.1%）、诈骗电话（9.5%）、房产中介（8.4%），保险理财（0.5%）。

从骚扰电话识别和拦截情况看，诈骗电话（21.0%）占比 21.0%位居首位，其次为广告推销（16.2%）、“响一声”、房产中介和保险理财的占比分别为 11.4%、5.1%和 2.0%。

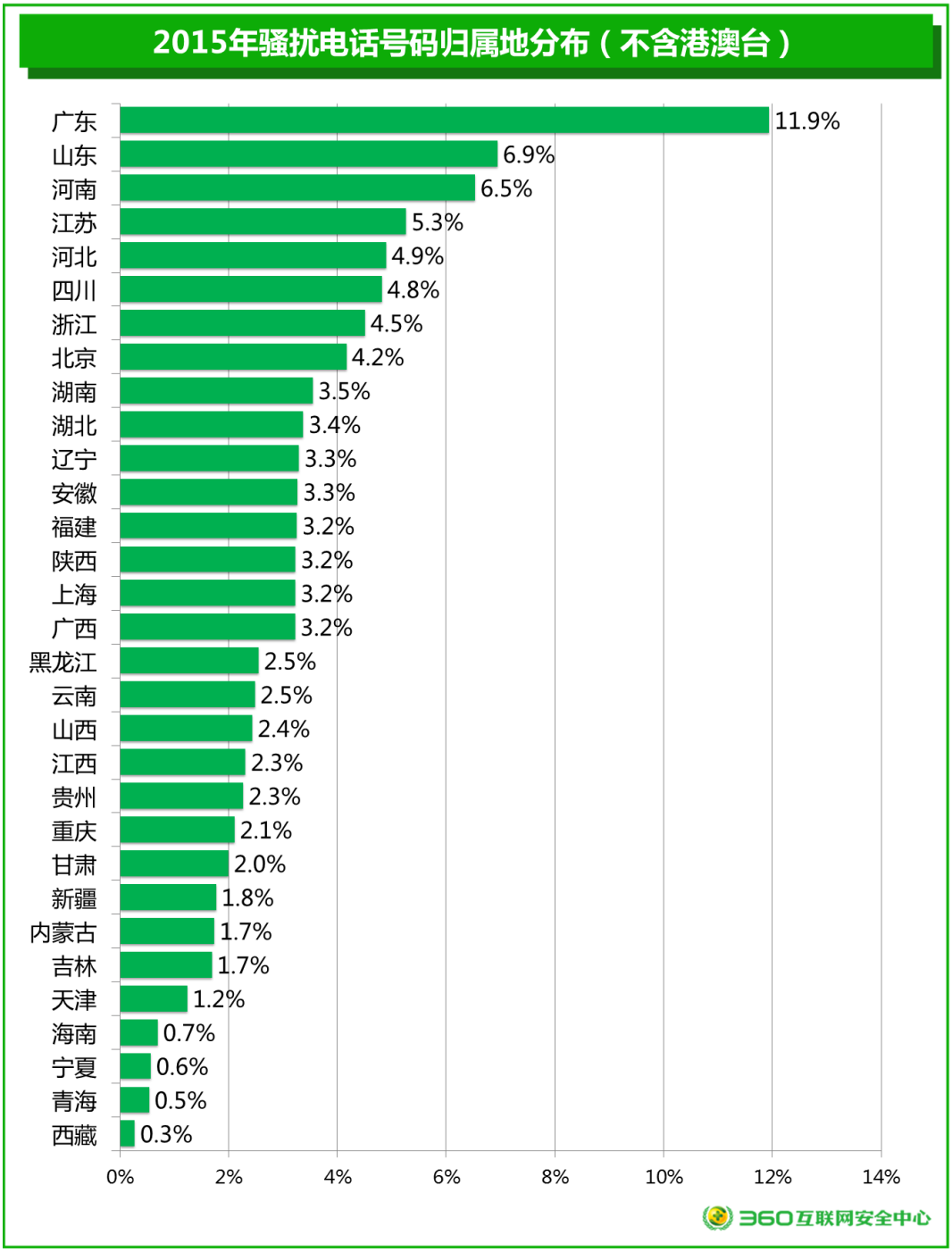
从季度趋势看，主要的骚扰电话类型拦截量呈现下降趋势。



三、 骚扰电话归属地分布

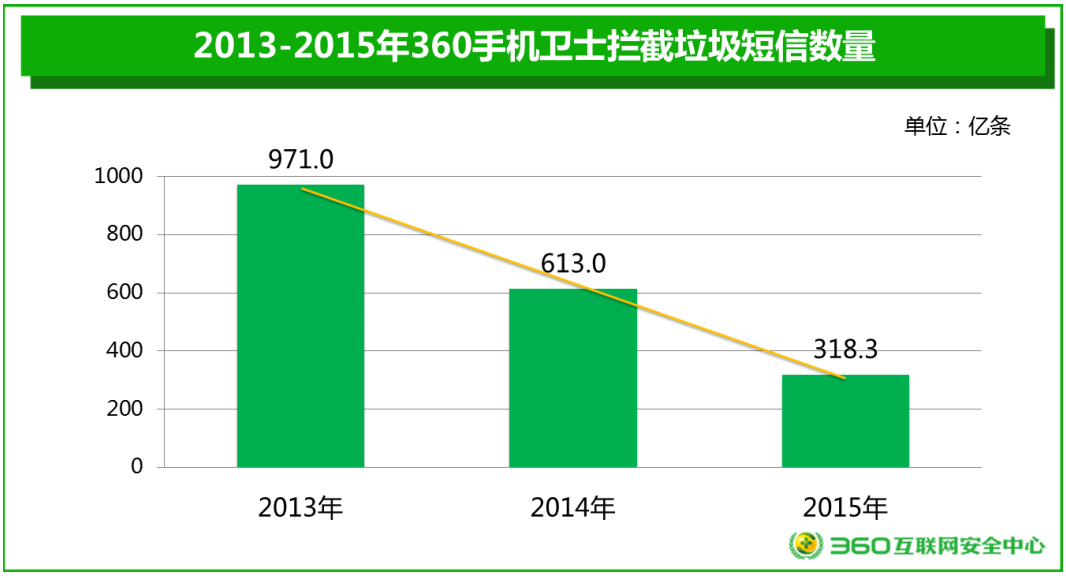
同 2014 年相比，广东、山东、河南依旧排在新增骚扰电话号码数的前三位，2015 全年数据显示，广东新增骚扰电话号码数最多，在全国各地的骚扰电话号码归属地中的占比高达 11.9%，全年始终在各省级行政区中排名第一；其次是山东与河南，用户新标记的骚扰电话

号码数占比分别为 6.9%、6.5%。

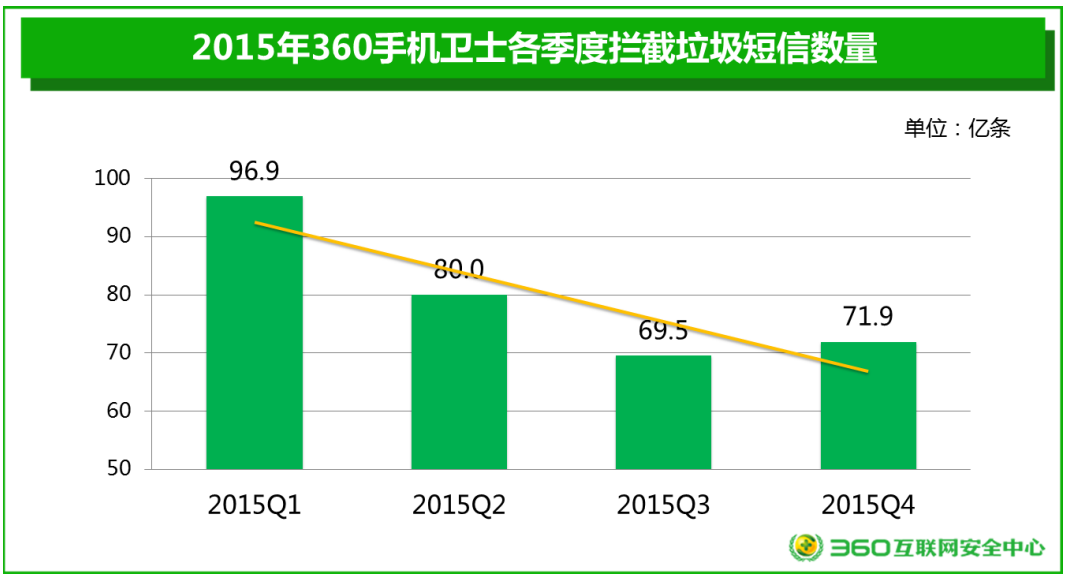


四、 垃圾短信拦截量

2015 年，360 手机卫士共为全国用户拦截各类垃圾短信约 318.3 亿条，较 2014 年（613 亿）下降了 48.1%，相比 2013 年更是下降了 67.3%。



2015 年各季度拦截的垃圾短信数量见下图，总体来看，各季度垃圾短信拦截量总体呈下降趋势，第三季度达到最低点，为 69.5 亿条。



垃圾短信拦截量的大幅下降反映出垃圾短信发送量同步下降。之所以垃圾短信的数量会连续三年年会出现持续下降，主要有以下几方面的原因：

1）手机安全厂商通过不断的技术进步，对垃圾短信的识别率和拦截率不断提高，使得垃圾短信绕过手机安全软件防护的机会越来越低，从而使发送垃圾短信的商业价值越来越低。

2）工信部等行业主管部门从 2013 年年末开始持续实施的垃圾短信严格治理政策成效日益明显。

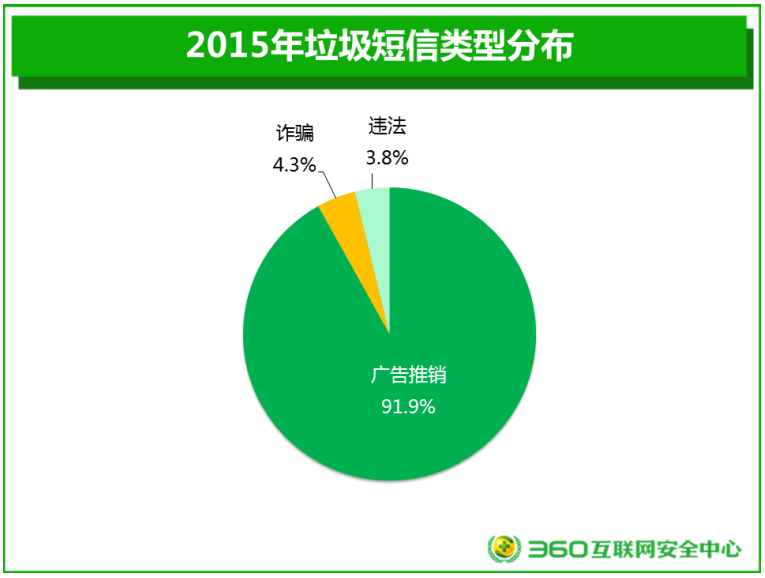
3）各大电信运营商越来越重视用户体验，对垃圾短信的过滤技术也得到了不断的提升。

五、 垃圾短信类型分析

通过用户举报的垃圾短信内容分析来看，广告推销类短信最多，占比达 91.9%；其次是

诈骗短信约占垃圾短信总量的 4.3%；违法短信占比为 3.8%。具体见下图。

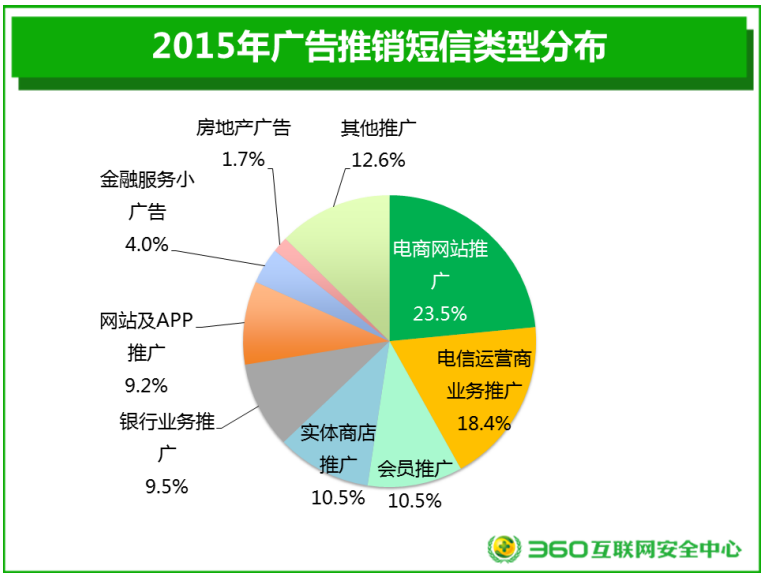
后面我们将对垃圾短信的各个分类进行深入分析，尤其是对诈骗类短信，及其包含的冒充类短信、打款类短信进一步分析其具体的冒充对象、打款对象等。



（一） 广告推销类短信分析

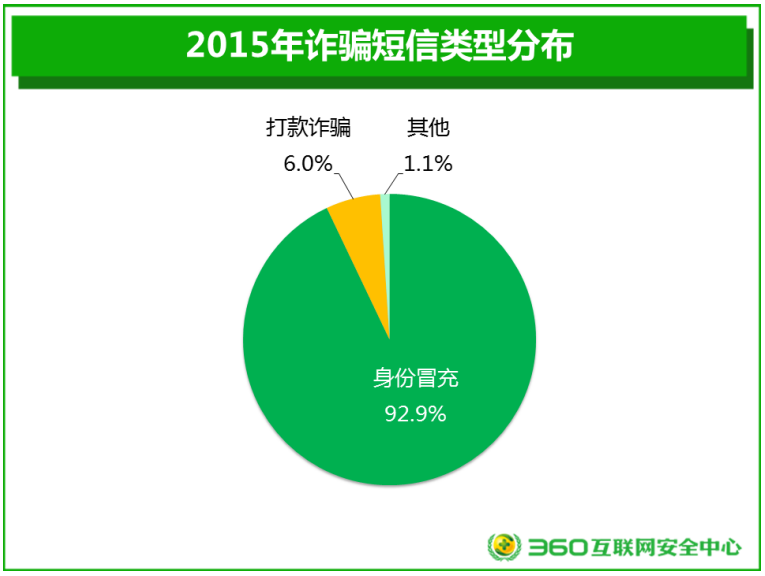
我们针对用户举报的各种广告推销类垃圾短信进行了抽样分析。其中，电商网站推广类短信占到所有广告推销类垃圾短信的 23.5%，首次超于电信运营商和金融机构，成为垃圾短信发送的第一大户。之后为运营商推广（18.4%）、会员推广（10.5%）、实体商店推广（10.5%）、银行推广（9.5%）。

关于广告推销类垃圾短信的类型分布，以及广告推销类垃圾短信的一些具体子类，如电商网站推广、电信运营商推广、银行推广类，以及金融服务小广告的进一步细分分类分析，可参见下面几图。其中，金融服务小广告（4.0%）包括保险广告、以及一些由个人或非大型金融机构发出的金融服务业务广告。



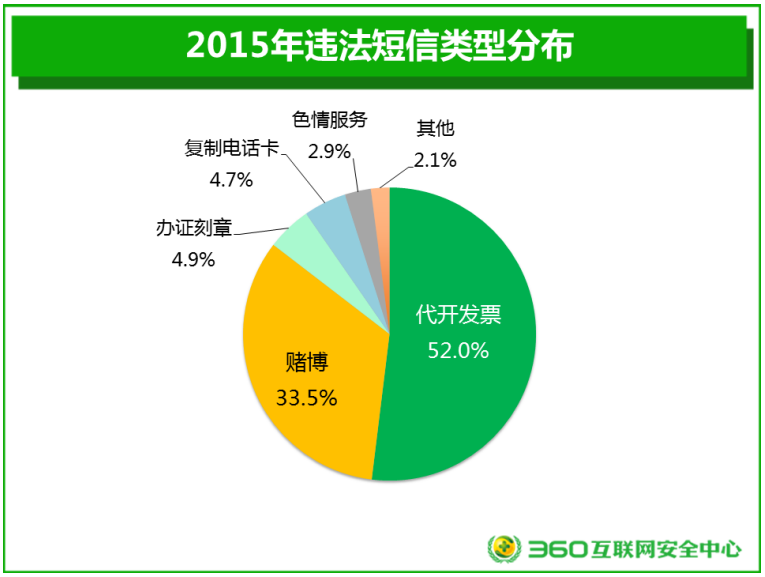
（二） 诈骗类短信分析

我们针对用户举报的各类诈骗短信也进行了抽样分析，其中，92.9%的诈骗短信为身份冒充类短信，其次是打款诈骗，占 6.0%，其他各类诈骗短信占 1.1%。



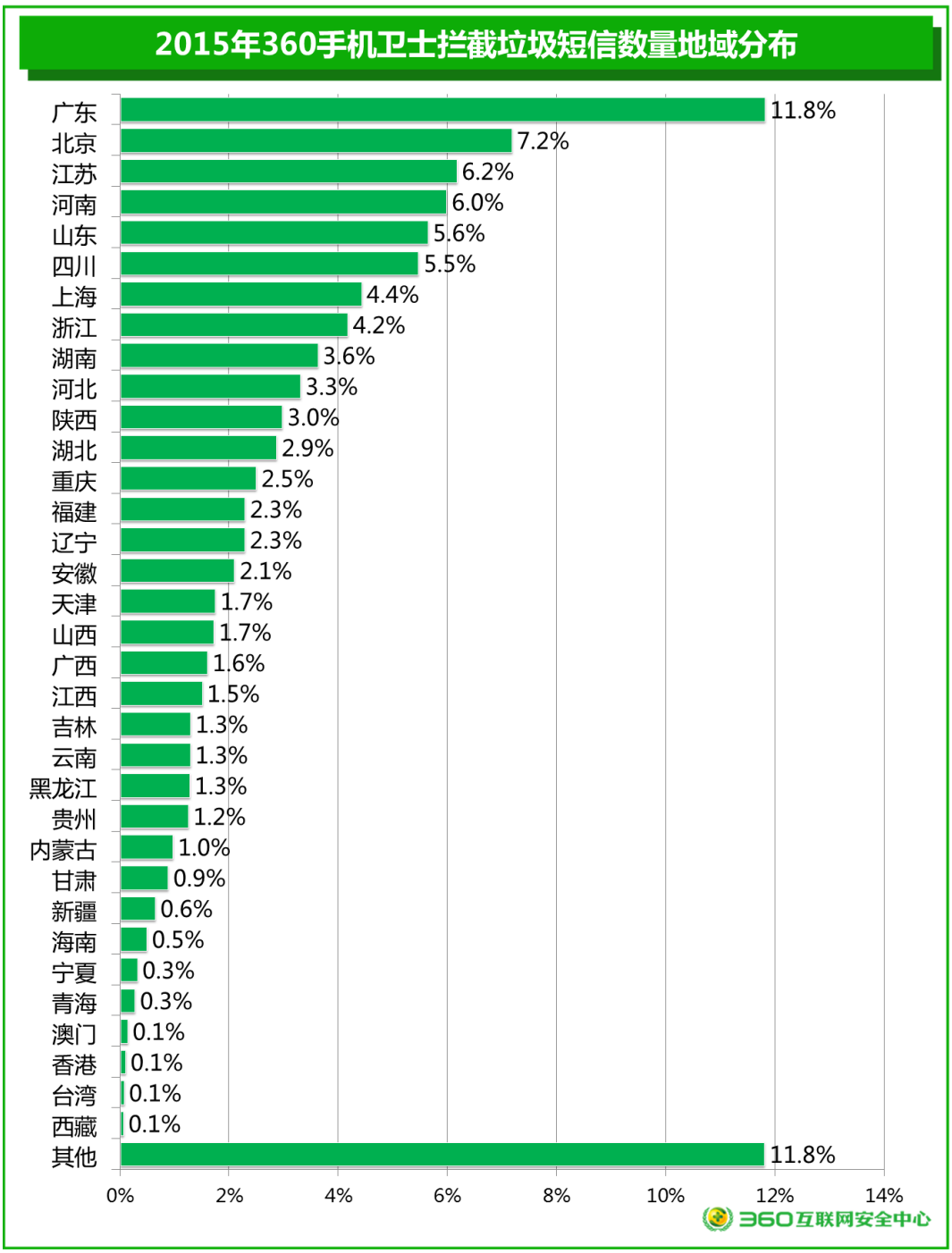
（三） 违法类短信分析

在违法类垃圾短信中，代开发票垃圾短信占比最高，为 52.0%，之后依次为赌博类（33.5%）、办证刻章（4.9%）、复制电话卡（4.7%）、色情信息（2.9%）。值得一提的是，色情信息在违法短信中的数量较往年有明显下降，这可能是由于更多的色情服务信息已经转移到了社交平台上。



六、 垃圾短信地域分布

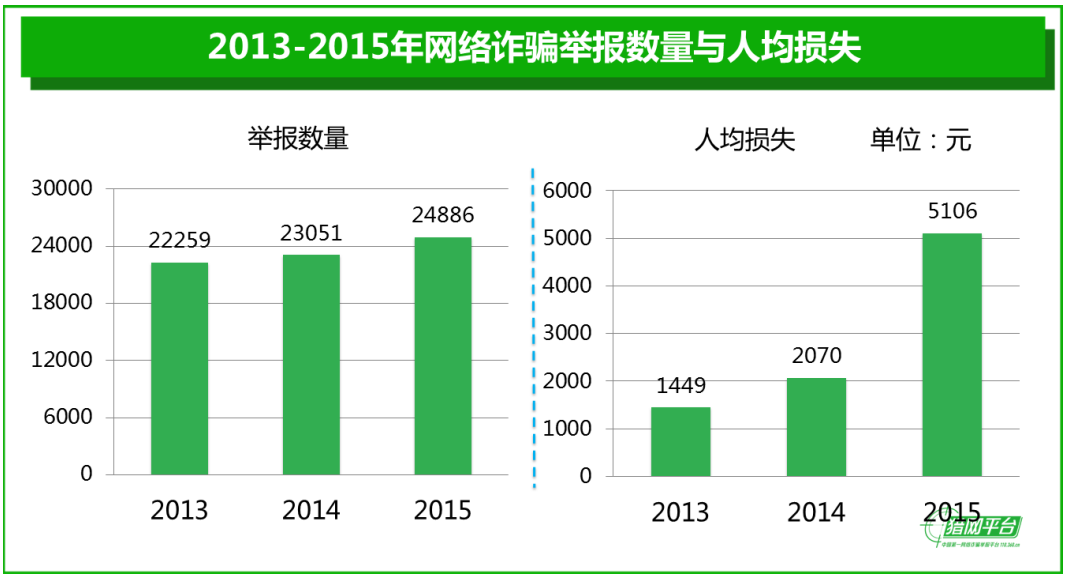
2015 年，根据 360 互联网安全中心的数据显示，广东地区用户接到的垃圾短信数量最多，占全国总量的 11.8%；其次为北京（7.2%）、江苏（6.2%）、河南（6.0%）、山东（5.6%）。下图给出了垃圾短信的地域分布：


2015年360手机卫士拦截垃圾短信数量地域分布
广东 11.8%
北京 7.2%
江苏 6.2%
河南 6.0%
山东 5.6%
四川 5.5%
上海 4.4%
浙江 4.2%
湖南 3.6%
河北 3.3%
陕西 3.0%
湖北 2.9%
重庆 2.5%
福建 2.3%
辽宁 2.3%
安徽 2.1%
天津 1.7%
山西 1.7%
广西 1.6%
江西 1.5%
吉林 1.3%
云南 1.3%
黑龙江 1.3%
贵州 1.2%
内蒙古 1.0%
甘肃 0.9%
新疆 0.6%
海南 0.5%
宁夏 0.3%
青海 0.3%
澳门 0.1%
香港 0.1%
台湾 0.1%
西藏 0.1%
其他 11.8%
0% 2% 4% 6% 8% 10% 12% 14%
360互联网安全中心

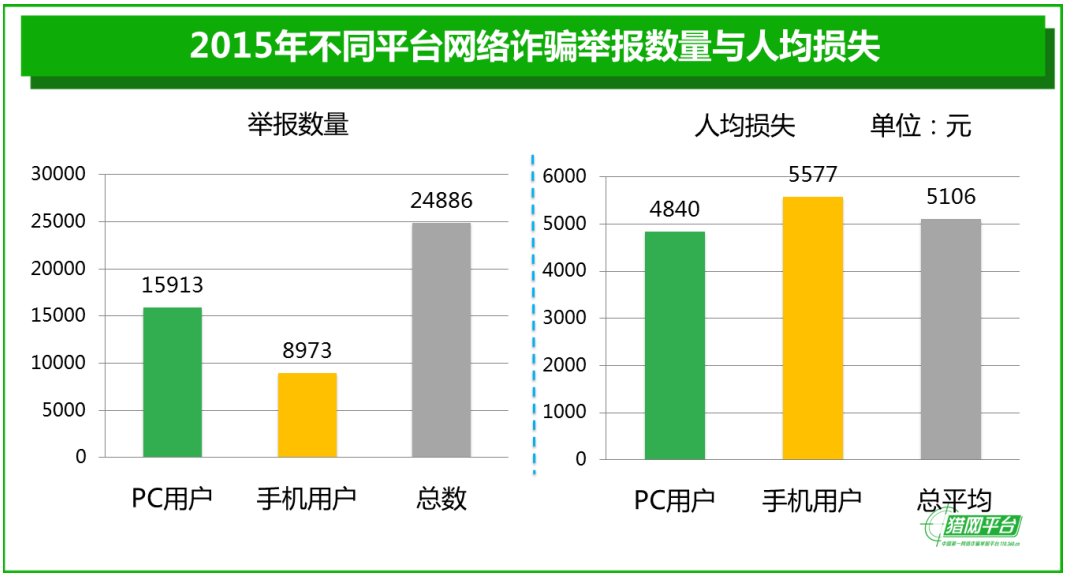
第四章 网络诈骗

一、 网络诈骗总体情况

2015 年，猎网平台共收到全国用户提交的网络诈骗举报 24886 例，举报总金额 1.27 亿余元，人均损失 5106 元。与 2014 年相比，虽然网络诈骗的举报数量只增长了 7.96%，但人均损失却增长了 146.67%，将近 1.5 倍。



其中，PC 用户举报 15913 例，涉案总金额为 7702.47 万元，人均损失 4840 元；手机用户举报 8973 例，涉案总金额为 5004.50 万元，人均损失约为 5577 元。虽然手机用户举报量大大低于 PC 用户举报量，但被骗金额均较高，平均损失比 PC 端高出 737 元。

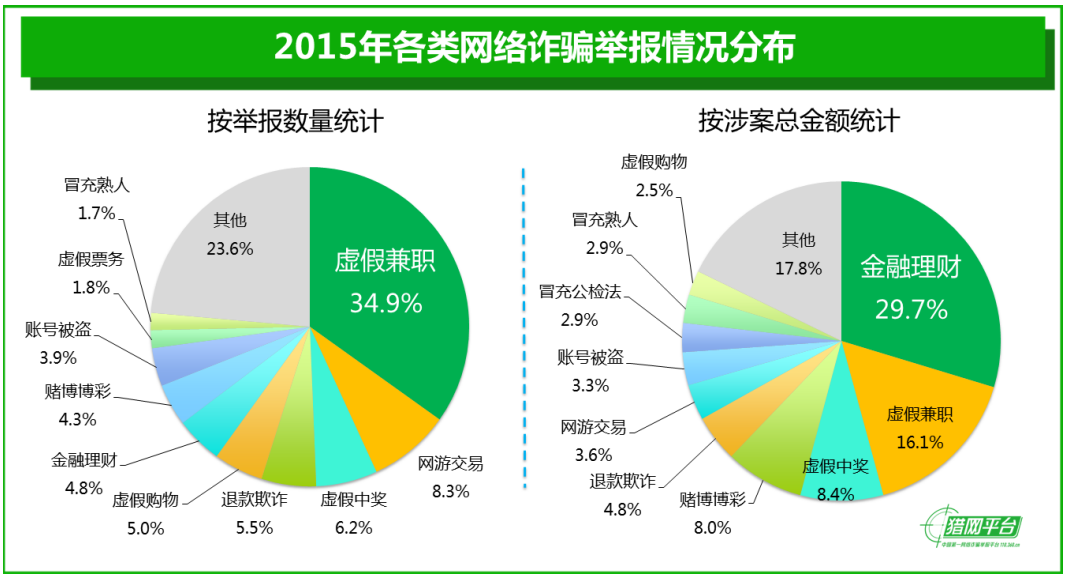


二、 网络诈骗类型分析

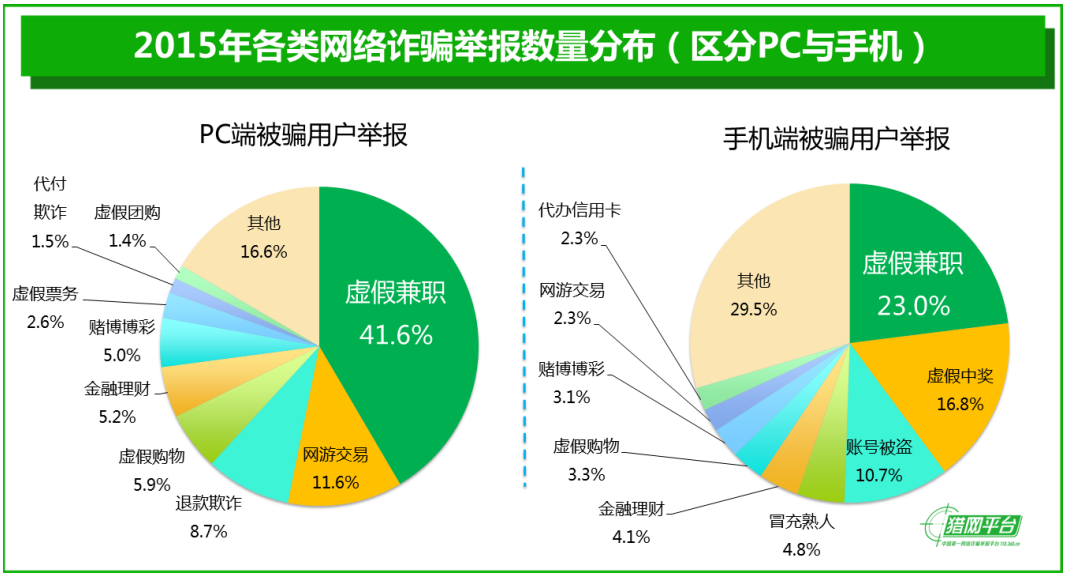
在所有举报的诈骗案情中，虚假兼职依然是举报数量最多的诈骗类型，共举报 8677 例，占比 34.9%；其次是网游交易 2059 例（占比 8.3%）、虚假中奖 1550 例（占比 6.2%）、退款欺诈 1380 例（占比 5.6%）和虚假购物 1253 例（占比 5.0%）。

而从涉案总金额来看，金融理财类诈骗最高，达 3768.6 万元，占比为 29.7%；其次是虚假兼职诈骗，涉案总金额为 2043.2 万元，占比为 16.1%；虚假中奖诈骗排第三，涉案总金额 1066.7 万元，占比为 8.40%。

下图给出了主要网络诈骗类型的举报量和涉案总金额分布情况。



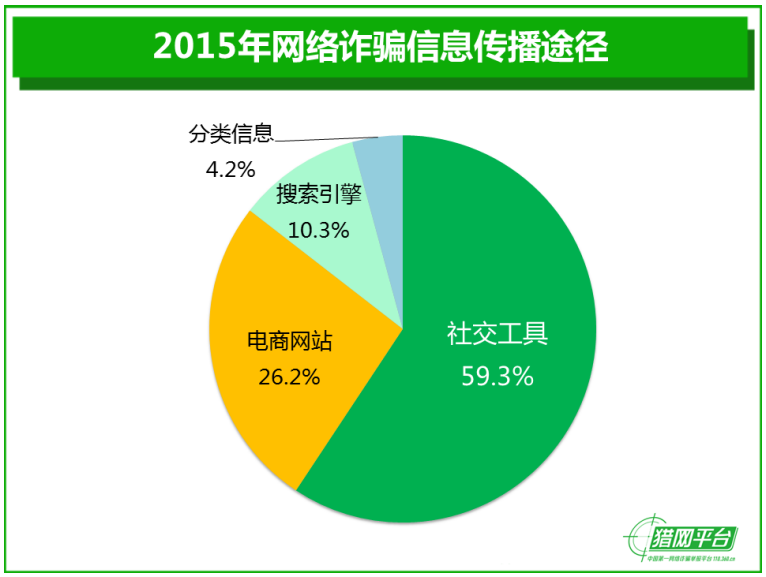
如果将 PC 端被骗用户和手机端被骗用户区分统计来看：在 PC 端被骗用户举报的所有案件中，虚假兼职以 41.6%排在首位，其次是网游交易 11.6%、退款欺诈 8.7%，这三种诈骗类型占 PC 端诈骗类举报总量的 61.9%。而在手机端被骗用户举报的所有案件中，虚假兼职以 23.0%排在首位，其次是虚假中奖 16.8%、账号被盗 10.7%，这三种诈骗类型占手机端诈骗类举报总量的 50.5%。



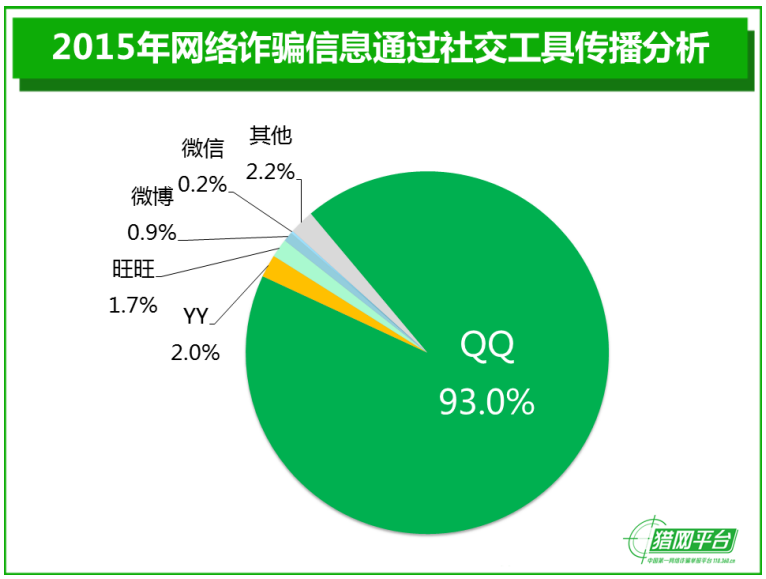
三、 网络诈骗传播途径

在所有 24886 名举报用户中，共有 5656 名用户能够准确的描述自己首次接触相关诈骗信息的网络途径（不包括诈骗电话和诈骗短信的）。我们对这些途径进行了详细的筛选和分析。统计结果显示，社交工具是网络诈骗信息传播的最主要途径，占 59.3%；其次是电子商务网站，占 26.2%；搜索引擎和分类信息网站分别占比 10.29%和 4.21%。

下图给出了 2015 年网络诈骗信息传播主要途径比例分布图。社交工具为诈骗信息的主要传播途径，占比将近 60%。



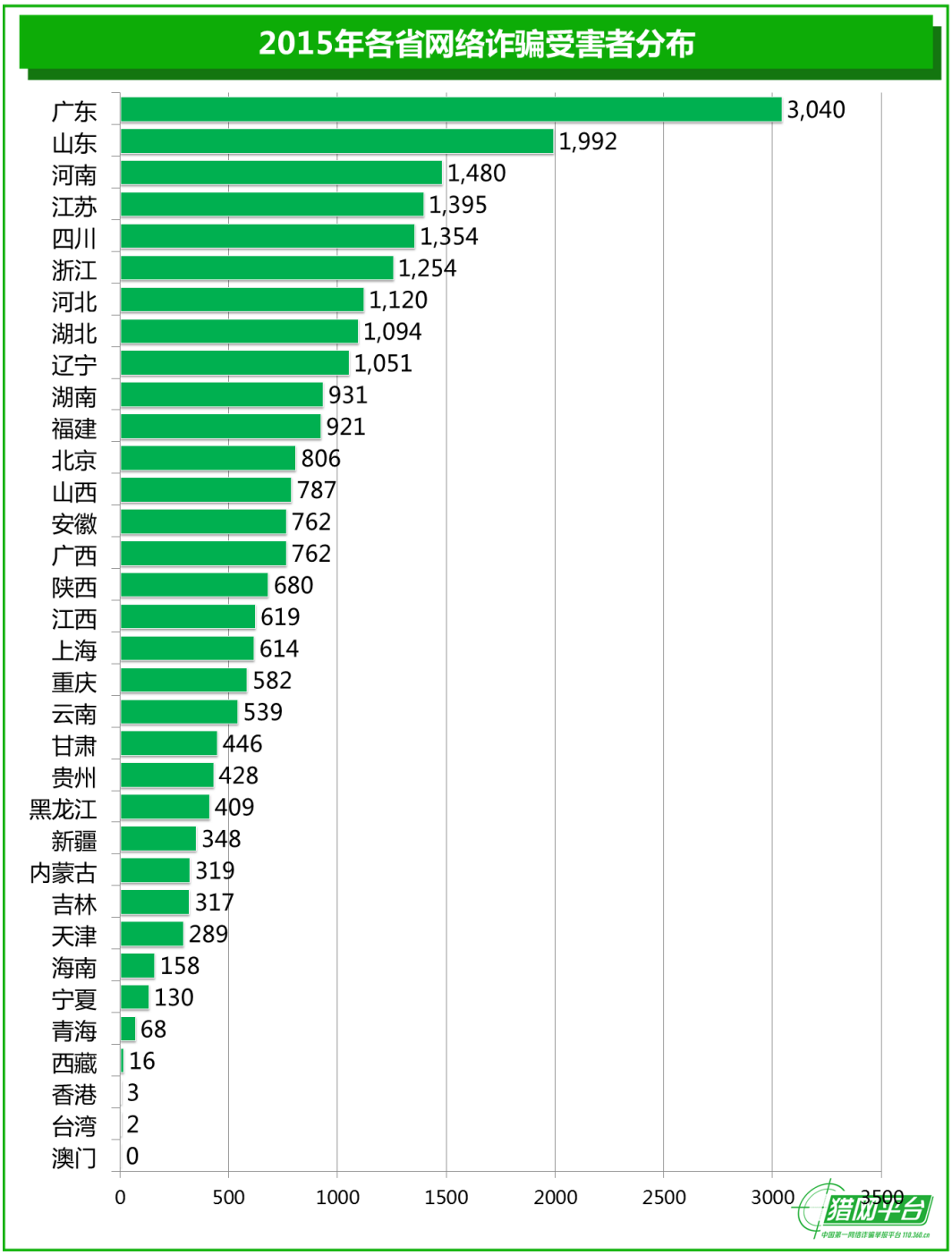
下图给出了 2015 年网络诈骗信息通过不同社交工具传播的比例分布情况。其中，QQ 的占比高达 93.0%。



四、 网络诈骗受害者地域分布

从用户举报情况来看，广东（3040 起）、山东（1992 起）、河南（1480 起）、江苏（1395 起）和四川（1354 起）这 5 个省级行政区的被骗用户最多。这 5 个地区用户的举报数量约

占到了全国用户举报总量的 37.5%。

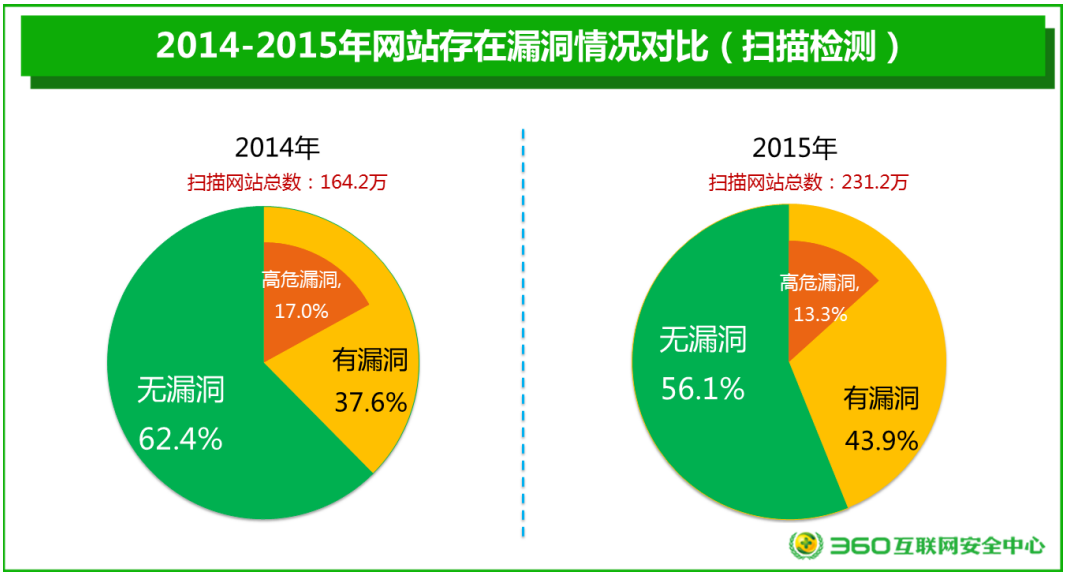


第五章 网站安全

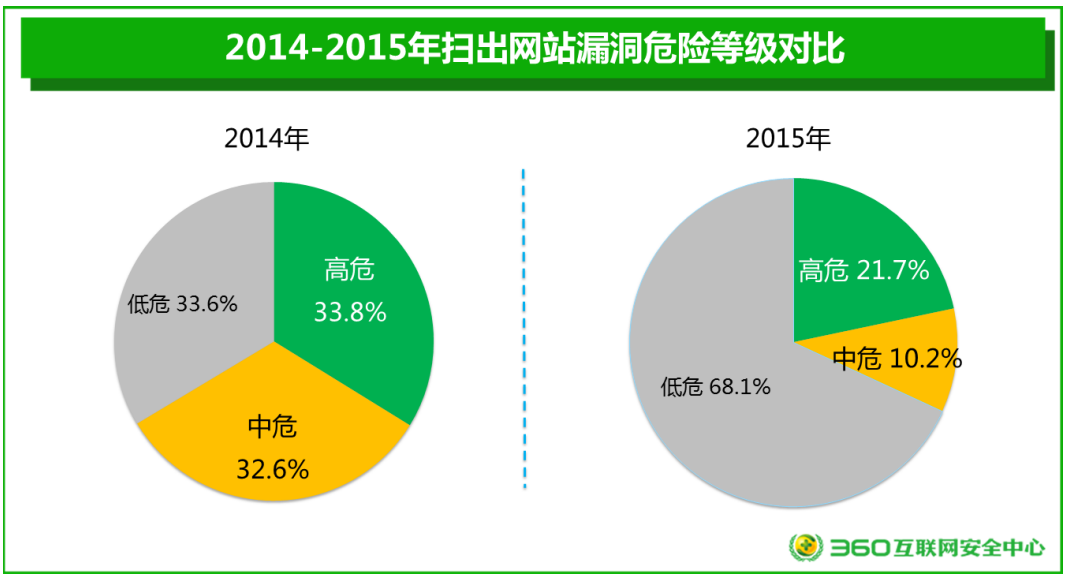
网站漏洞的整体形势可以有两个分析角度：一是网站安全检测的自动扫描结果统计，二是网站被报告漏洞情况的统计。本章将分别从这两个角度，分别以 360 网站安全检测的统计结果和补天平台收录的网站漏洞统计结果为依据，分析 2015 年中国网站的安全漏洞情况。

一、 漏洞扫描分析

2015 年全年（截至 11 月 18 日），360 网站安全检测平台共扫描各类网站 231.2 万个，较 2014 年的 164.2 万个增加了 40.8%。其中，扫出存在漏洞的网站 101.5 万个，占比为 43.9%，较 2014 年的 61.7 万个增长了 64.5%。其中，扫出存在高危漏洞的网站 30.8 万个，占扫描网站总数的 13.3%，较 2014 年的 27.9 万个增长了 10.4%。



从检测出漏洞的危险等级看，高危占 21.7%，中危占 10.2%，低危占 68.1%。和去年高中低三者占比大致相当不同，今年高、中危漏洞二者之和亦小于低危漏洞。

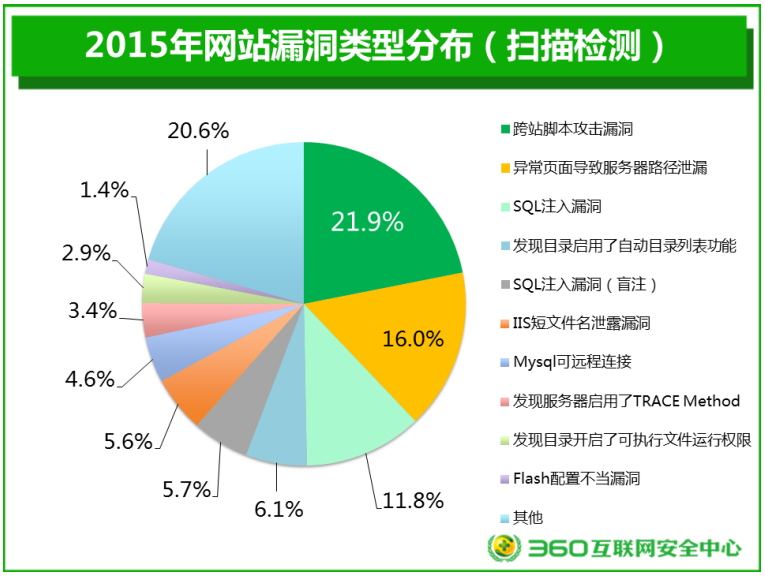


从网站漏洞类型上看，跨站脚本攻击（XSS）漏洞、异常页面导致服务器路径泄露、SQL 注入漏洞等是 2015 年最为频繁扫出的漏洞类型。下表给出了被扫出次数最多的十大类典型网站安全漏洞：

排名	漏洞名称	漏洞级别	扫出次数（万）
1	跨站脚本攻击漏洞	中危	270.7
2	异常页面导致服务器路径泄露	低危	197.9
3	SQL 注入漏洞	低危	145.9
4	发现目录启用了自动目录列表功能	低危	75.6
5	SQL 注入漏洞（盲注）	高危	70.2
6	IIS 短文件名泄露漏洞	低危	69.1
7	Mysql 可远程连接	低危	56.5
8	发现服务器启用了 TRACE Method	低危	42.4
9	发现目录开启了可执行文件运行权限	低危	36.1
10	Flash 配置不当漏洞	低危	17.8

表 1　2015 年扫出数量最多的 10 类网站漏洞

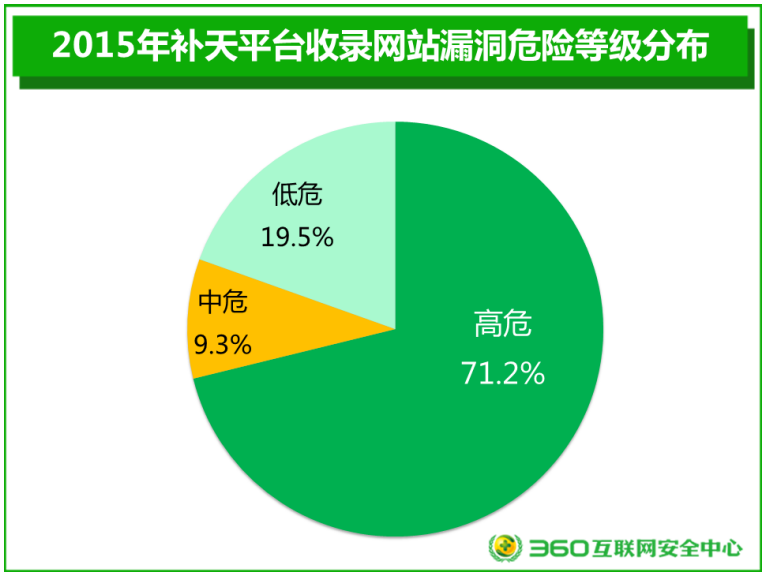
下图给出了各类网站安全漏洞被扫出次数的比例分布情况。从图中可以看出，跨站脚本攻击漏洞（21.9%）、异常页面导致服务器路径泄露（11.8%）和 SQL 注入漏洞（16.0%）这三类安全漏洞是占比最高的网站安全漏洞，三者之和接近网站所有漏洞检出总次数的一半。相比 2014 年，“异常页面导致服务器路径泄露”之漏洞是今年的“黑马”漏洞，超过 SQL 注入漏洞而跃居第二。



二、　漏洞收录情况分析

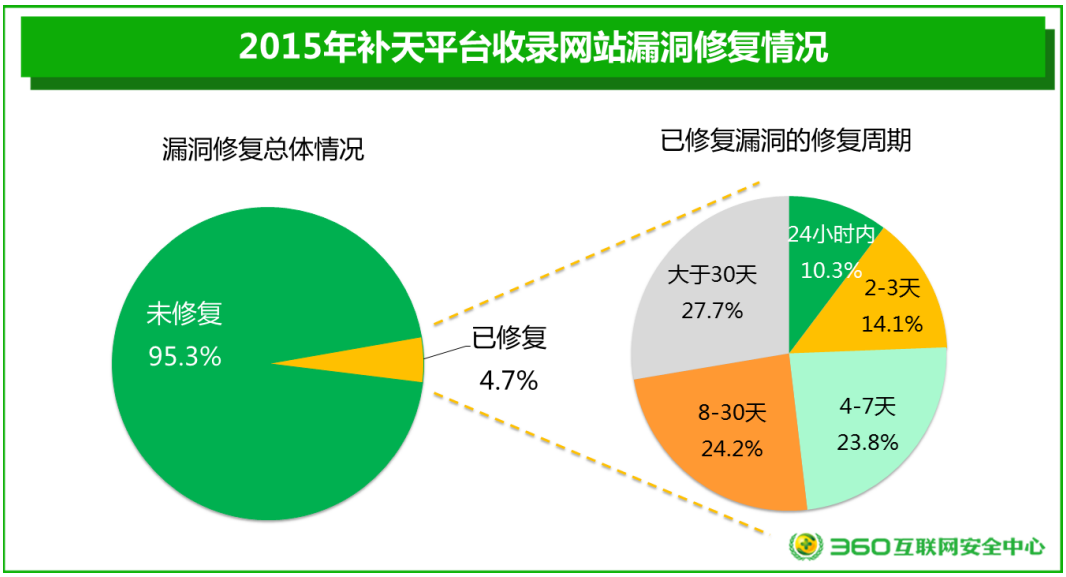
2015 年 1 月 1 日-11 月 18 日，补天平台共收录各类网站安全漏洞 37943 个，涉及网站 26370 个。

在补天平台 2015 年收录的网站漏洞中，高危漏洞占比为 71.2%、中危漏洞占 9.3%，低危漏洞占 19.5%。

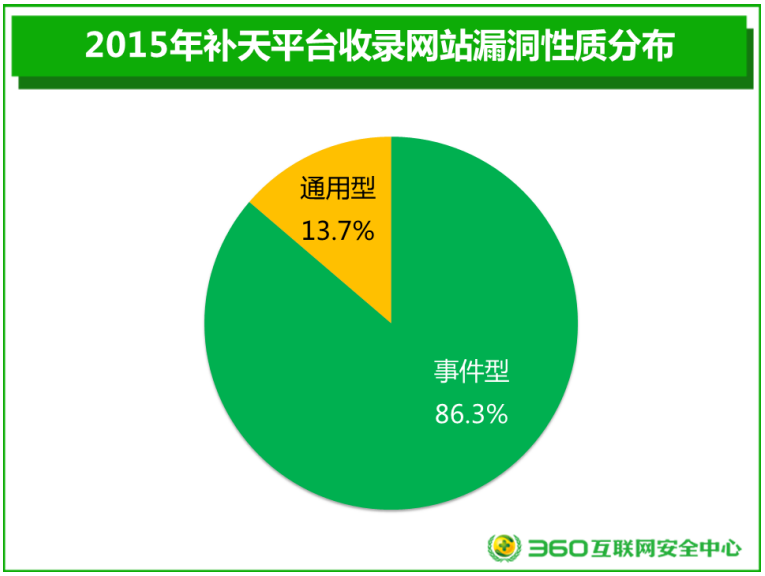


漏洞修复率过低，是目前网站安全面临的一个重大问题。2015 年的统计数据显示，网站在收到相关漏洞报告后，平均修复率仅为 4.7%。（网站修复漏洞后，需要在补天平台上进行标注，未进行标注的一律视为漏洞未修复。）也就是说，超过 95%的网站漏洞长期得不到修复，这就给黑客对网站发动攻击留下了非常充分的时间。

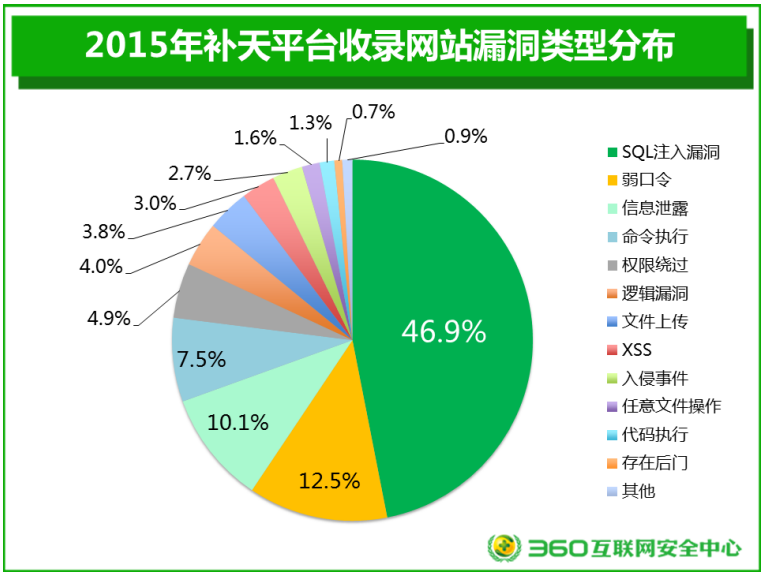
而在已修复的网站漏洞中，24 小时内修复的比例为 10.3%，2-3 天内修复的比例为 14.1%，4-7 天内修复的比例为 23.8%，8-30 天内修复的比例为 24.2%，而修复周期大于 30 天的，占比为 27.7%。总体而言，即便是在能够修复漏洞的网站中，仍有至少一半以上的网站，漏洞修复周期过长，修复很不及时（大于 7 天）。



网站漏洞的性质可以分为事件型漏洞和通用型漏洞。所谓事件型漏洞就是仅对该网站有危害，而对其他网站无影响的漏洞；通用型漏洞则是会对有相同技术架构、相近应用业务的网站皆有影响的漏洞。在 2015 年补天平台收录的网站安全漏洞中，事件型漏洞占比 86.3%，通用型漏洞占比 13.7%。

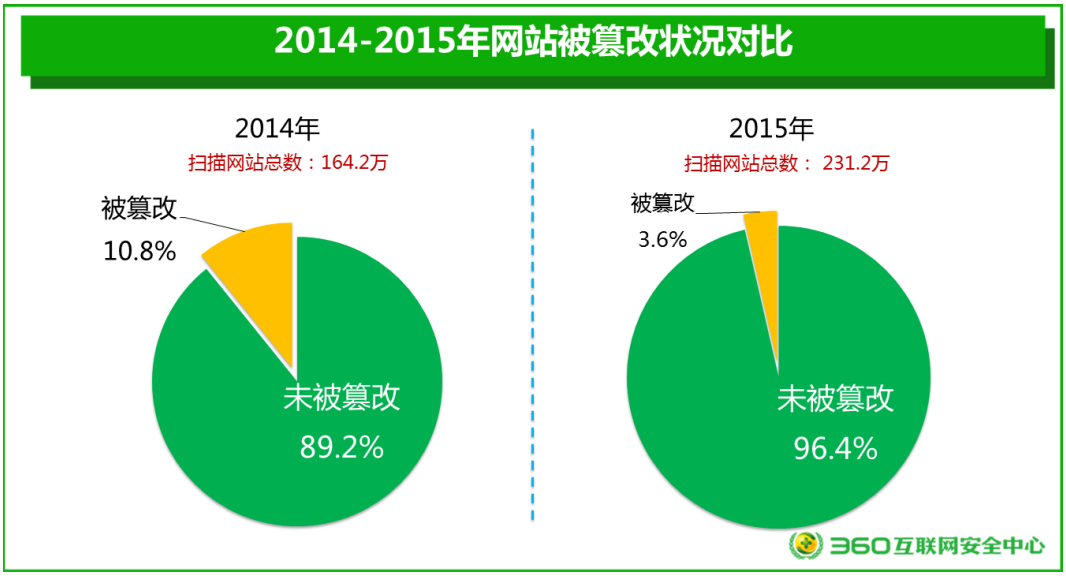


从补天平台收录漏洞的具体类型来看，SQL 注入漏洞最多，占比接近 50%，其次是弱口令和信息泄露，分别占 12.5%和 10.1%。漏洞类型分布请见下图：

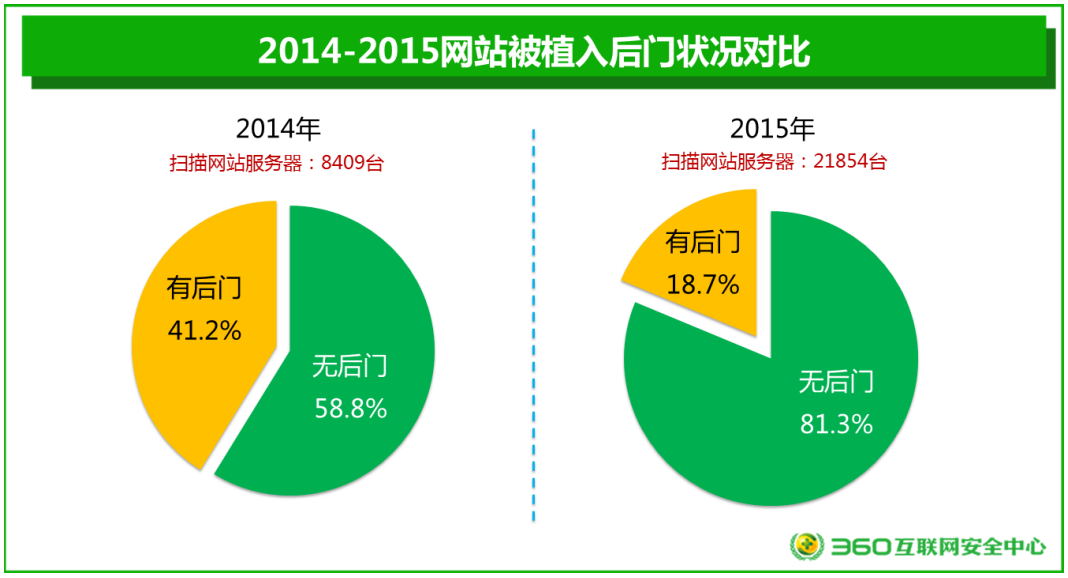


三、 网页篡改与后门

2015 年全年（截至 11 月 18 日），360 网站安全检测平台共扫描各类网站 231.2 万个，较 2014 年的 164.2 万个，增加了 40.9%。其中，被篡改（不包括被植入后门程序）的网站 8.4 万个（全年去重），比 2014 年的 17.7 万个下降了 52.5%，约占扫描网站总数的 3.6%，占比也较 2014 年的 10.8%下降了 7.2 个百分点。网站遭篡改情况明显好转。

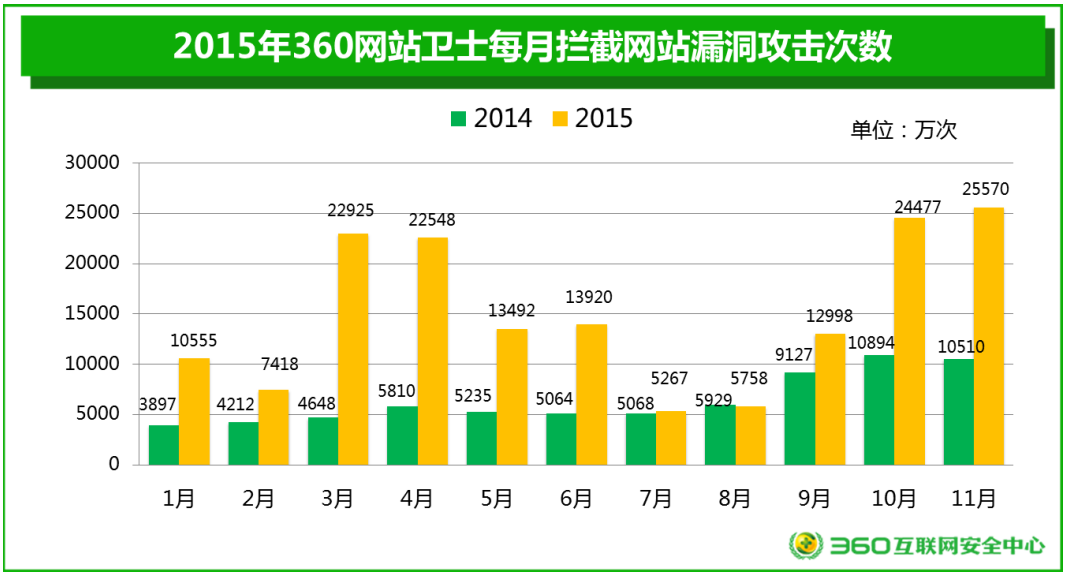


2015 年全年（截至 11 月 18 日），360 网站安全检测共对 21854 台网站服务器进行了网站后门检测，覆盖网站 322.3 万个（含子域名），扫描发现约 4097 台服务器存在后门，比 2014 年的 3465 台服务器增加了 18.2%，占所有扫描网站服务器的 18.7%，占比较 2014 年减少了 22.5 个百分点。

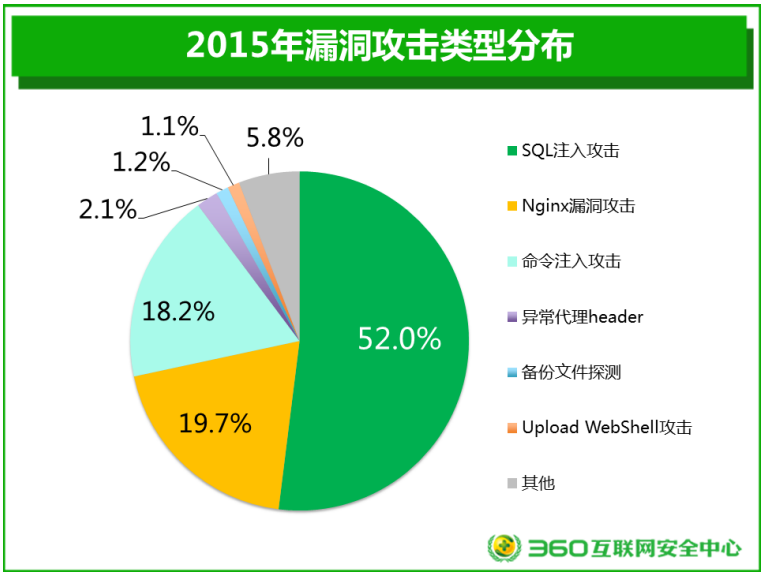


四、 漏洞攻击与类型

2015 年全年（截至 11 月 18 日），360 网站卫士共拦截各类网站漏洞攻击 16.5 亿次，较 2014 年 7.0 亿次，增长了约 135.7%。2015 年平均每天拦截漏洞攻击 512.2 万次。下图给出了每月漏洞攻击拦截量的具体统计。从图中可以看出，3 月、4 月和 10 月较 2014 年出现大幅增长。

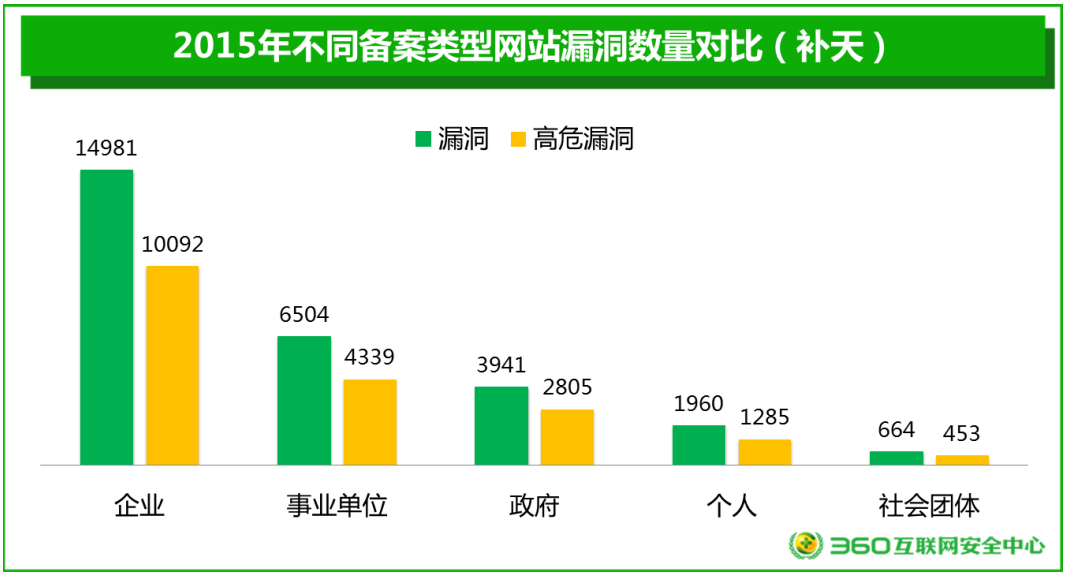


下图给出了漏洞攻击拦截量的类型分布情况。



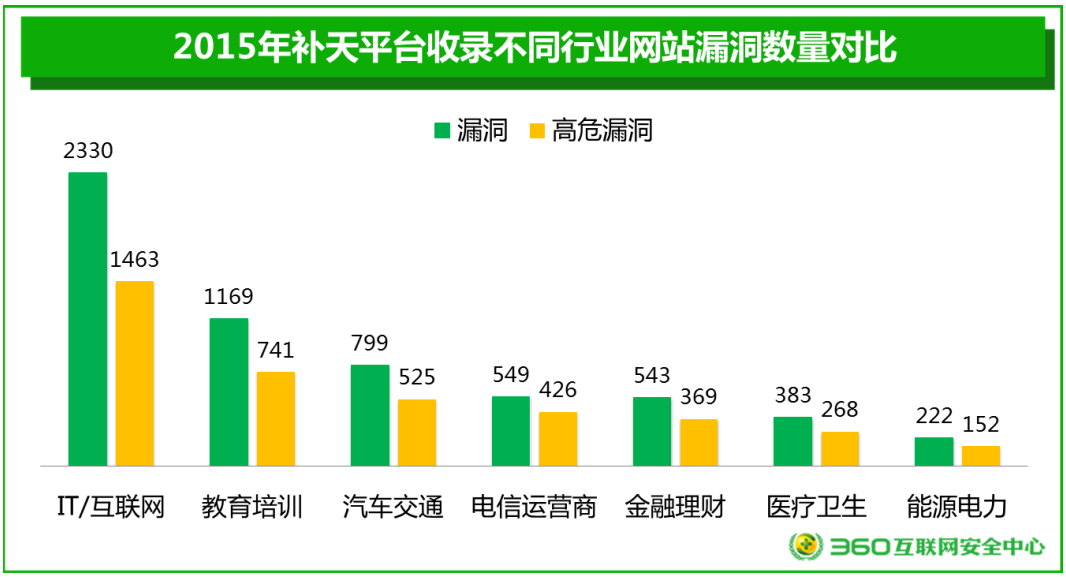
五、 网站安全行业分析

网站备案可以分为政府、事业单位、社会团体、企业、个人等五个类别。下图给出了补天平台收录的备案网站漏洞中，不同备案类型网站的漏洞数量和高危漏洞数量对比情况。其中，涉及备案网站的漏洞总量为 28050 个（共涉及 22084 个网站），其中高危漏洞为 18974 个。总体而言，补天平台收录的备案网站漏洞中，企业网站的漏洞和高危漏洞的数量都是最多的。企业网站报告的漏洞最多，达 14981 个，其中高危漏洞 10092 个，政府、事业单位、社会团体、个人等漏洞及高危漏洞数量具体见下图。从受影响网站角度看，上述漏洞涉及 11453 家企业网站、5179 家事业单位网站、3315 家政府网站、1583 家个人网站、554 家社会团体网站。



由于企业、个人备案的网站涵盖了众多商业行业领域，而且企业、个人类备案的网站漏洞数量最大，约为 1.69 万个，超过了 2015 年收录漏洞总量的 60%。本报告将所有企业/个人备案的网站分为教育培训、医疗卫生、金融理财、IT/互联网、汽车交通、能源电力、电信运管商等七个重点行业，共包含漏洞 5995 个（涉及网站 4280 个），高危漏洞 3944 个。

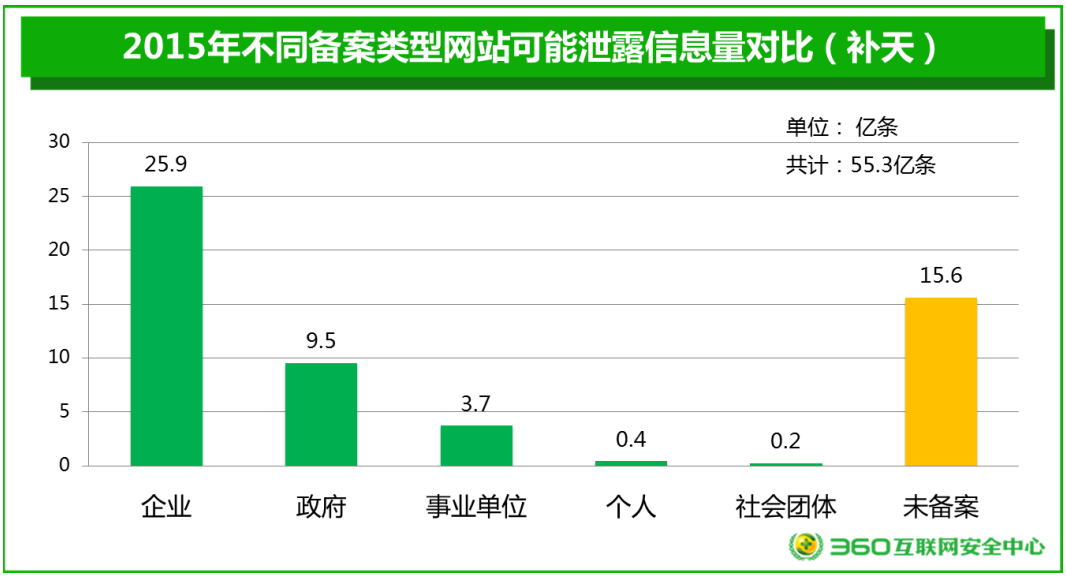
统计显示，IT/互联网行业网站被报告的漏洞最多，达到 2330 个，高危漏洞 1463 个；各行业漏洞及高危漏洞，具体见下图。从受影响网站角度看，上述漏洞涉及 IT/互联网行业网站 1535 个，涉及教育培训、医疗卫生、金融理财、汽车交通、能源电力、电信运管商类网站分别为 914 个、328 个、435 个、625 个、158 个、285 个。



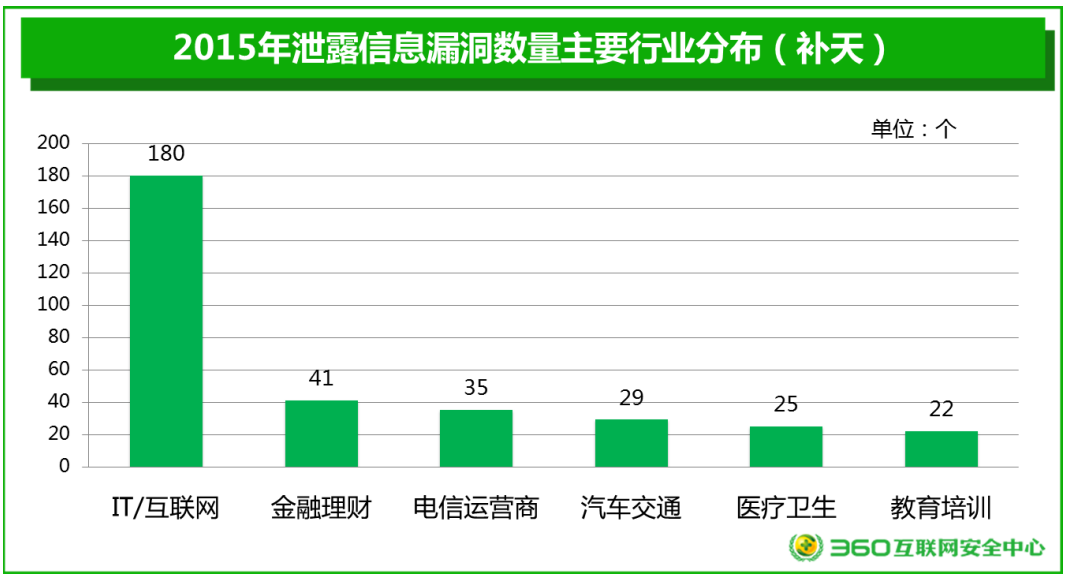
六、 个人信息泄露情况

统计显示，在 2015 年（截至 2015 年 11 月 18 日）补天平台收录的网站漏洞中，共有 1410 个漏洞可能造成网站上的个人信息泄露，本章统简称此类漏洞为“泄露信息漏洞”（这与单纯技术上的“信息泄露漏洞”不是一个概念），这些漏洞共涉及网站 1282 个，可能泄露的个人信息量（本章下文简称泄露信息量）高达 55.3 亿条。

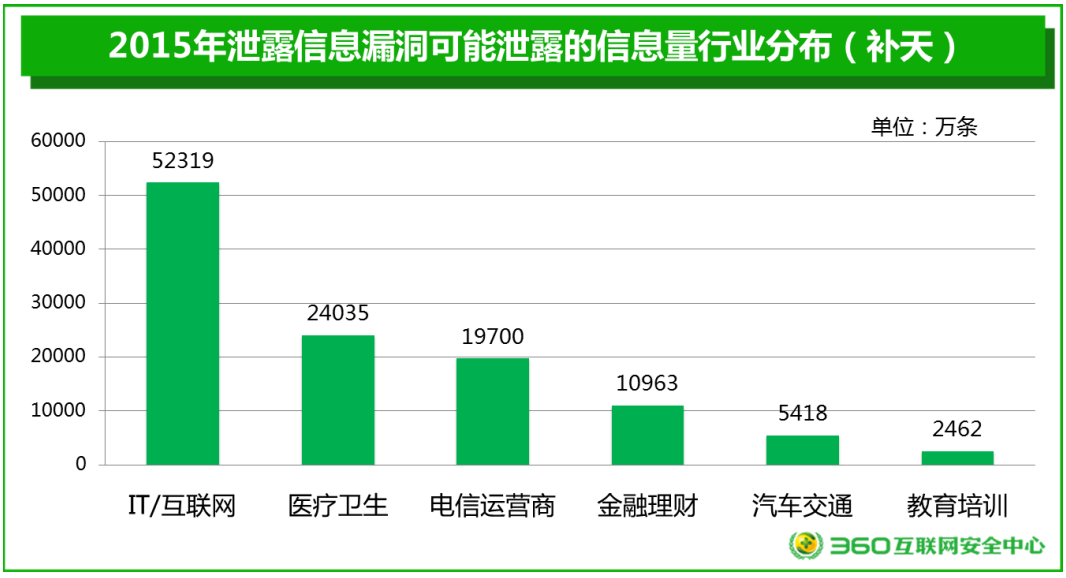
从可能泄露的个人信息量上来看：企业网站可能泄露的信息量为 25.9 亿条，政府、事业单位、个人和社会团体网站可能泄露的信息量分别为 9.5 亿、3.7 亿、0.4 亿和 0.2 亿条，占比分别为 65.2%、23.9%、9.3%、1.0%、0.5%。



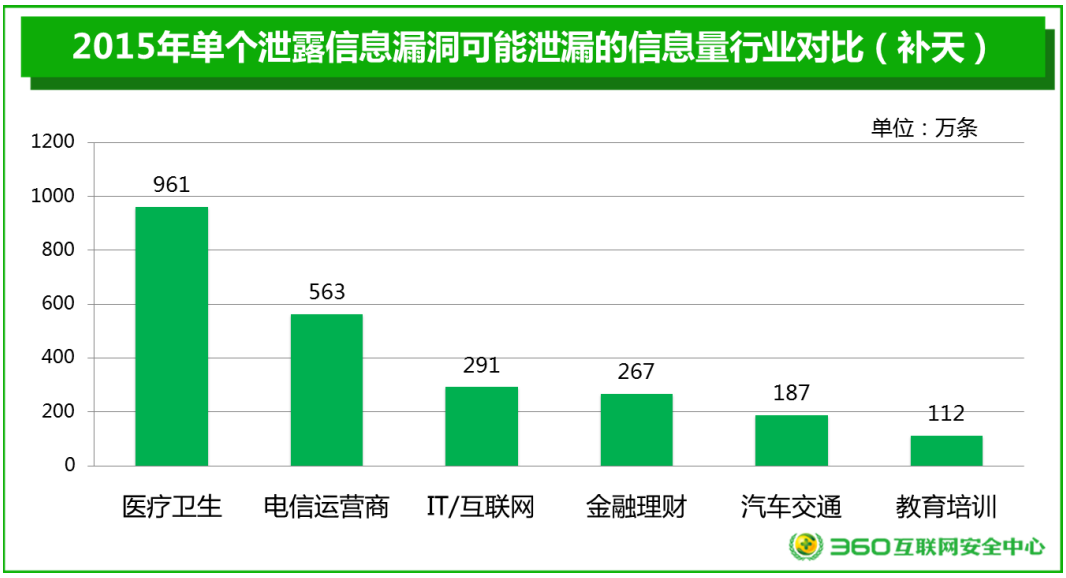
在所有存在泄露信息漏洞的企业和个人备案的网站中，我们选择了 332 个可以明确确认其所属行业的网站进行个人信息泄漏的行业分析。这 332 个网站主要分布在 IT/互联网、电信运营商、金融理财、汽车交通、教育培训和医疗卫生等六个重点领域。具体数量分布见下图。



这六个领域的网站存在的泄露信息漏洞共可导致约 11.5 亿条个人信息泄露，占到了企业/个人网站可能泄露信息总量（26.3 亿条）的 43.7%。其中：IT/互联网网站可能泄漏的个人信息最多，为 5.23 亿条；其次是医疗卫生网站 2.40 亿条；电信运营商 1.97 亿条；金融理财网站 1.10 亿条；汽车交通网站 5418 万条；教育培训 2462 万条。



而从平均单个漏洞泄露的信息量来看，医疗卫生行业排在首位，平均每个泄露信息漏洞可能导致 961 万条个人信息泄露，其次是电信运营商 563 万条/洞，接下来依次是 IT/互联网 291 万条/洞，金融理财 267 万条/洞，汽车交通 187 万条/洞、教育培训 112 万条/洞。



附录 1　2015 年国内外重大网络信息安全事件

（一） 斯诺登曝美英窃取全球数十亿手机 SIM 卡信息

英国《卫报》2 月 19 日报道，美国中央情报局前员工爱德华·斯诺登最新披露的资料显示，美英两国的情报机构入侵了世界最大的手机 SIM 卡制造商，从而可以不受限制地访问全球数十亿部手机。美国国家安全局(NSA)和英国政府通信总部(GCHQ)入侵了荷兰 SIN 卡制造商金雅拓公司(Gemalto)，窃取了加密秘钥，这样他们就能秘密地监控手机上的通话和数据信息，而不会被电信公司和外国政府所察觉。

（二） 中国数万手机感染“关机骇客”木马

2 月底，一款名为“关机骇客”(PowerOffHijack)的手机木马感染中国地区数万部安卓手机，“关机骇客”木马主要感染 Android5.0 以下操作系统的手机。进入手机后，木马会率先获得 root 权限，以便能够劫持手机关机过程。当手机用户点击应用时，图标就会隐藏，手机木马则潜伏在手机中。当中招手机用户按下电源键后，会出现一个假的对话框，如果机主选择关机，木马就会显示假的关机画面，屏幕关闭，但手机仍处于开机状态。为了使中招手机看起像是真的关机了，一些系统广播服务也会被劫持。

（三） 手机端“红包大战”现多种骗局

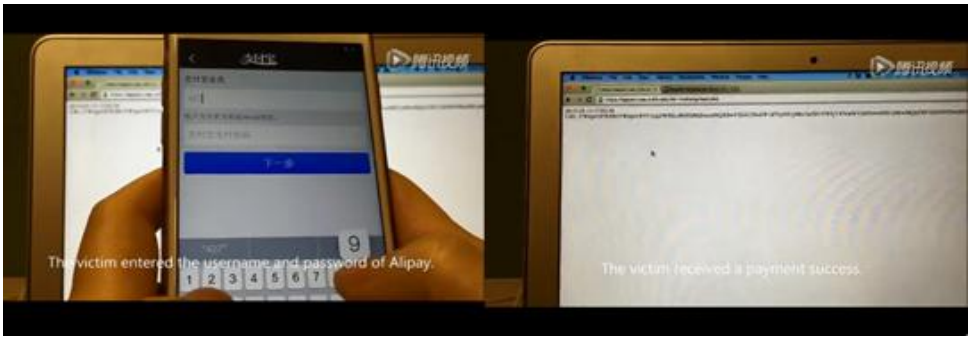
春节期间，新一轮红包大战爆发，同时，AA 红包骗局、合体抢红包、抢红包神器、“红包大盗”手机木马等多种骗局也不断翻新花样。骗子利用文字游戏对“AA 收款”功能进行了伪装。他们在收款留言处填写了“送钱“的字样后，广泛向群聊中发送，一旦手机用户点击输入密码则会被自动扣钱。商家推出的合体抢红包活动则可能造成手机用户隐私泄露，带来大量垃圾短信和骚扰电话。此外，抢红包神器、“红包大盗”木马则以窃取手机用户支付类信息为目的，盗刷手机用户银行卡。

（四） 谷歌修复中国安全研究员发现的安卓 5.1 漏洞

3 月 11 日，360 手机卫士安全研究员发现谷歌 Android 存在的 7 个漏洞，在经过谷歌官方确认后，特向 360 手机安全团队致谢。此次是 2015 年谷歌首次致谢中国安全公司发现漏洞，360 手机安全团队的龚广发现的 7 个漏洞已经被编入 CVE(Common Vulnerabilities & Exposures，相当于公共漏洞字典表)，其中两个则在最新推出的 Android 5.1 中被修复。

（五） URL Scheme 漏洞致手机支付账号密码可被劫持

3 月 26 日，网上一段未越狱 iPhone 支付账号密码被“偷”到电脑上的视频大热，看过视频的果粉惊呼“不越狱也不安全吗”？实际上，这是利用 URL Scheme 漏洞对支付账号和密码进行劫持实现的，URL Scheme 是苹果手机 App 间调用的一种方法。中国区 iOS 用户有 2/3 会通过非 Appstore 市场下载 App，给这类模仿 App 制造了很大的机会，而这种模仿正常 App 的 URL Scheme 的情况，目前只能通过 App 自身加上验证机制或苹果绑定 Bundle ID，因为 Bundle ID 在 App Store 上是唯一的。



（六） 购票软件“火车票达人”存在安全漏洞

1 月 7 日，白帽子向补天漏洞响应平台提交漏洞，发现购票软件“火车票达人”存在安全漏洞，使用该软件购买火车票的用户，大量用户名明文密码存在泄露风险。“移花互动”记录存储用户的明文密码，并且没有对数据库采取有效的安全防护措施，导致用户隐私信息处于危险境地。当天晚间，中国铁路客户服务中心发布消息，提醒用户“火车票达人”的这一风险。“火车票达人”官方微博也于数小时后发布致歉信，承认出现严重人为性失误，导致安全防护进程启动失效。

（七） 社保系统被曝漏洞，社保成为个人信息泄露“重灾区

4 月，补天平台曝出重庆、上海、山西、贵州、河南等省市卫生和社保系统出现大量高危漏洞，数千万用户的社保信息可能因此被泄露。相关数据显示，目前围绕社保系统、户籍查询系统、疾控中心、医院等大量曝出高危漏洞的省市已经超过 30 个，仅社保类信息安全漏洞统计就达到 5279.4 万条，涉及人员数量达数千万，其中包括个人身份证、社保参保信息、财务、薪酬、房屋等敏感信息。

（八） 携程网服务器遭攻击致宕机 12 小时

5 月 28 日，携程部分服务器遭到不明攻击，导致官方网站及 APP 一度无法正常使用，其网站和移动应用服务被中断，此次宕机近 12 个小时后才恢复正常。

（九） 安卓 WiFi 组件被曝存漏洞

4 月 24 日，安卓系统曝出重大漏洞，该漏洞主要影响安卓 WiFi 功能组件。只要安卓手机开启了 WLAN 直连功能的，那么攻击者就可以利用该漏洞，无需任何物理接触，也不用接入公共无线网络，就可以对这部安卓手机发起远距离恶意攻击和入侵，进而可以窃取用户手机中的隐私信息，甚至造成财产损失。而且用户即使没有默认开启 WLAN 直连功能，只要使用过一次后，也只有通过重启 WiFi 或设备才可以关闭该功能。

（十） 天眼实验室发布国内首个 APT 报告还原“海莲花”黑客攻击事件

5 月 29 日，360 旗下“天眼实验室”发布了国内首个 APT（高级持续性威胁）研究报告，报告披露了一个代号为“海莲花”的境外黑客组织自 2012 年 4 月以来，针对中国政府、海事机构、海域建设部门、科研院所和航运企业，展开了长达 3 年的 APT 攻击。该报告的发布引起业界的密切关注，国内多个安全厂商也相继展开了不同程度的研究。

截至 2015 年 11 月底，360 威胁情报中心监测到的针对中国境内科研教育、政府机构等组织机构发动 APT 攻击的境内外黑客组织累计 29 个，其中 15 个 APT 组织曾经被国外安全厂商披露过，另外 14 个为 360 独立发现并监测到的 APT 组织。

（十一） DDoS 僵尸发动攻击 涉及 109 国及数万台路由器

5 月网站安全公司 Incapsula 的一项调查显示，网络犯罪分子利用数万不安全的家庭路由器为实施 DDoS 攻击创建了大批僵尸网络，在 121 天内针对公司 60 个客户的恶意流量来自 109 个国家爱 1600 个互联网服务提供商的 40,269 个 IP 地址。

（十二） 一条会让 iPhone 崩溃并重启的简单文本信息

5 月，Apple 移动操作系统中被曝出一个新 bug，可导致任何 iPhone 的手机系统崩溃并重启。这个问题是由一条简单文本信息引起的。当 Messages 收到一条由特定字符组成的字符串时，iPhone 的 Message app 会持续崩溃。而如果接受信息时智能手机是锁定状态，则会导致 iPhone 在未接收到任何警告信息的情况下重启。

（十三） 6 亿部三星手机被曝存远程代码漏洞

6 月 17 日，NowSecure 公司的安全研究人员表示，约 6 亿部三星手机存在远程代码执行漏洞，且是一个软件设计漏洞。该漏洞可致三星智能手机被恶意软件感染，并被咖啡店、酒店等地的恶意 WiFi 热点远程控制，甚至被中间人劫持。研究发现，三星 GalaxyS6、S5、S4 以及 S4Mini 绑定的触摸屏键盘 APP 会使用未加密 HTTP 连接从网上下载文件进行自动更新。但整个过程中不会验证这些文件的真实性，因此不法分子就可以劫持下载，并向手机

发送恶意文件。

（十四） HackingTeam 被黑，“互联网军火”泄漏

7 月初，有“互联网军火库”之称的意大利监控软件厂商 Hacking Team 被黑客攻击，400GB 内部数据泄露。据了解，Hacking Team 掌握的大量漏洞和攻击工具也暴露在这 400GB 数据中。更可怕的是，泄漏的数据可以在互联网上公开下载和传播。业内人士担忧：一旦泄露数据广泛流传，将造成全世界黑客“人手一份核武器”的局面，很可能使世界安全形势迅速恶化。

（十五） 中国互联网安全大会

9 月 28 日~30 日，由中国互联网协会和 360 互联网安全中心共同主办的中国互联网安全大会（ISC 2015）在北京举行，包括美国前国家安全局局长、首任网络司令部司令在内的全球顶级安全智库、全球 19 所知名大学与国内 10 大研究机构的研究学者、全球 30 多家安全企业和安全团队的专家一起，在中国互联网安全领袖峰会、全球互联网安全精英峰会和 13 个分论坛上，围绕超过 110 个演讲议题进行头脑风暴，以世界级的眼光共同对网络安全做了深入有效的探讨。

（十六） 苹果手机 XCode 恶意代码感染事件

9 月中旬，由于从第三方渠道下载的 iOS 和 MAC OS 开发工具 XCode 被插入恶意代码，使编译出的 App 被注入第三方的恶意代码，向指定网站上传用户数据，导致大量染毒应用混入苹果官方应用商店，截止到 9 月 21 日，360NirvanTeam 共发现 1077 款 App 被植入恶意代码，其中不乏百度音乐、微信、滴滴、58 同城、12306 等热门应用。该事件打破了苹果系统的安全神话。

（十七） 国内首个威胁情报中心正式成立

9 月 29 日，360 宣布建成国内首个威胁情报中心，并正式商用，开放在线查询平台。截至 2015 年 7 月底，360 威胁情报中心监测到的针对中国境内政府部门、电信运营商、大型企业、科研院所等组织机构发动 APT 攻击的境内外黑客组织 13 个。最早可以追溯到 2007 年，而最近三个月（2015 年 5 月以后）内仍然处于活跃状态的 APT 组织至少有 7 个。

（十八） libstagefright 漏洞促成安卓每月发布补丁机制

2015 年 7 月，国外安全公司 Zimperium 爆出多处安卓系统漏洞, 瞬间占据各大媒体头条.。号称一条彩信即可控制手机的安卓 libstagefright 媒体库，影响范围从 Android 2.2 到 5.1 通杀，被业界称为安卓上的“心脏滴血”。

利用安卓 libstagefright 媒体库漏洞，黑客可以通过发送一段有特殊格式的视频到用户的手机——例如一个含视频的彩信——几乎就能获取用户手机的全部控制权。这一漏洞预计可能影响“95%” 的安卓手机用户安全。

libStagefright 默认会被 mediaserver 使用，也就是说，如果恶意的视频文件有机会被 mediaserver 处理到，该漏洞就有机会触发。例如，如果视频被存放在 sdcard，那么打开文件管理 APP，下拉列表到露出视频，就会触发缩略图解析，漏洞触发图库 APP，点击本地图片会出现缩略图，如果视频在 sdcard，或者 download 目录，这时候也会触发。

特别的，微信同样也会受到影响。通过微信发送的恶意视频，点击也会导致 media server 崩溃，并进而导致手机被控制。

安卓 libStagefright 系列漏洞事件，对谷歌安卓团队触动很大，直接促成了谷歌宣布执行安卓每月发布安全补丁的安全机制。

（十九） 百度相关 APP 几乎全线中招“虫洞（Wormhole）”漏洞

2015 年 10 月份，国内某知名第三方漏洞收集平台发布报告称，已经有白帽子发现了多款 Android 应用存在 WormHole 漏洞，黑客可以利用这个漏洞攻击任何存在漏洞的联网手机，执行恶意代码就可以直接操控用户手机。

而受此漏洞影响最大的知名互联网企业就是百度。据不完全统计，百度旗下的多款 APP 中招，包括：百度地图、百度浏览器、百度贴吧、百度翻译、百度视频、百度手机助手、百度云、百度音乐、百度新闻、百度图片、百度输入法等都受到了此漏洞的影响，堪称“全家桶”沦陷。

除了已经确认的百度系应用之外，使用了百度提供的软件开发工具包（SDK）的应用也有许多集体中招，比如途牛旅游、万达电影等等。另外，百度系的 91、hao123 等业务旗下的应用也都有上榜。

（二十） 首个国产手机厂商宣布每月更新安全补丁

2015 年 11 月，360 官方正式宣布，未来将每个月对其旗下品牌手机进行一次安全补丁更新，以确保给手机用户持续提供安全可靠的服务。这是继谷歌 Nexus 宣布进行月度安全更新之后，全球为数不多、国内首家宣布对手机实行每月更新安全补丁的手机厂商。

根据 360 官方统计数据显示，自 2015 年 9 月份发布以来， 360 互联网安全中心共发现其旗下手机系统安全漏洞 143 个（包括谷歌原生系统漏洞和自身的定制开发漏洞），其中高危漏洞共计 68 个，已经完成修复并且发布补丁至内测用户的安全漏洞 139 个。

目前，360 定期给手机打补丁的机制在国内仍属个例。但在未来 2-3 年内，可能会有越来越多的手机厂商加入这一行列，并将手机安全性作为其重要的卖点之一，并进而逐步形成给手机定期打补丁的新的行业规范。

附录 2　2015 年各省区市互联网安全状况态势图

根据 2015 年 360 互联网安全中心监测数据，我国各省、直辖市、自治区，以及香港、澳门、台湾地区的互联网安全状况态势，可以从恶意程序云查询拦截量、钓鱼网站拦截量、骚扰电话与垃圾短信拦截量和网络诈骗举报量等 5 个维度加以分析。根据本报告正文中的上述研究数据，通过对地区排名划分三个级别，画出各省区市互联网安全状况态势图，具体如下：

2015年全国各省（区、市）互联网安全状况态势分析

说明：2015年综合PC和手机端情况，360安全产品共检测恶意程序攻击拦截总量859.1亿人次，为全国用户拦截钓鱼网站353.3亿次、骚扰电话272.6亿次、垃圾短信318.3亿条；另外，猎网平台共接到全国手机诈骗举报24886例。下表给出各省（区、市）排名占比情况：

Top5　6-15　16-34

省区市（按首字拼音排序）	恶意程序	钓鱼网站	骚扰电话	垃圾短信	网络诈骗
安徽	2.4%	0.6%	3.3%	2.1%	3.1%
澳门	0.0%	0.01%	0.0%	0.1%	0.0%
北京	7.1%	14.2%	4.2%	7.2%	3.3%
重庆	1.8%	0.7%	2.1%	2.5%	2.4%
福建	3.7%	9.7%	3.2%	2.3%	3.7%
甘肃	0.8%	0.2%	2.0%	0.9%	1.8%
广东	14.7%	28.9%	11.9%	11.8%	12.3%
广西	2.8%	7.3%	3.2%	1.6%	3.1%
贵州	1.5%	0.9%	2.3%	1.2%	1.7%
海南	0.5%	0.4%	0.7%	0.5%	0.6%
河北	4.1%	1.2%	4.9%	3.3%	4.5%
河南	5.8%	1.3%	6.5%	6.0%	6.0%
黑龙江	2.2%	0.7%	2.5%	1.3%	1.7%
湖北	3.6%	2.6%	3.4%	2.9%	4.4%
湖南	3.3%	5.1%	3.5%	3.6%	3.8%
吉林	1.9%	0.7%	1.7%	1.3%	1.3%
江苏	5.6%	3.2%	5.3%	6.2%	5.6%
江西	2.2%	2.5%	2.3%	1.5%	2.5%
辽宁	3.1%	1.5%	3.3%	2.3%	4.3%
内蒙古	1.2%	0.3%	1.7%	1.0%	1.3%
宁夏	0.3%	0.1%	0.6%	0.3%	0.5%
青海	0.2%	0.1%	0.5%	0.3%	0.3%
山东	5.6%	2.4%	6.9%	5.6%	8.1%
山西	2.7%	2.5%	2.4%	1.7%	3.2%
陕西	2.6%	0.6%	3.2%	3.0%	2.8%
上海	3.5%	4.0%	3.2%	4.4%	2.5%
四川	4.1%	2.1%	4.8%	5.5%	5.5%
台湾	0.0%	0.04%	0.0%	0.1%	0.01%
天津	3.0%	1.0%	1.2%	1.7%	1.2%
西藏	0.1%	0.02%	0.3%	0.1%	0.1%
香港	0.0%	0.05%	0.0%	0.1%	0.01%
新疆	1.1%	0.4%	1.8%	0.6%	1.4%
云南	1.9%	0.7%	2.5%	1.3%	2.2%
浙江	6.7%	4.1%	4.5%	4.2%	5.1%

360互联网安全中心

附录 3　2015 年各省互联网安全情况介绍

（一） 安徽省

全年恶意程序云查询拦截总量为 20.6 亿人次，接到网络诈骗举报 762 例，拦截钓鱼网站 2.32 亿次，拦截的钓鱼网站服务器位于该省的次数为 929 万次，拦截垃圾短信量 6.66 亿条，骚扰电话 8.90 亿次。

（二） 澳门

全年恶意程序云查询拦截总量为 54 万人次，接到网络诈骗举报 0 例，拦截钓鱼网站 0.03 亿次，拦截的钓鱼网站服务器位于该省的次数为 2.6 万次，拦截垃圾短信量 0.42 亿条，骚扰电话 0 次。

（三） 北京市

全年恶意程序云查询拦截总量为 60.9 亿人次，接到网络诈骗举报 806 例，拦截钓鱼网站 53.90 亿次，拦截的钓鱼网站服务器位于该省的次数为 3.9 亿次，拦截垃圾短信量 22.83 亿条，骚扰电话 11.35 亿次。

（四） 重庆市

全年恶意程序云查询拦截总量为 15.9 亿人次，接到网络诈骗举报 582 例，拦截钓鱼网站 2.56 亿次，拦截的钓鱼网站服务器位于该省的次数为 335 万次，拦截垃圾短信量 7.92 亿条，骚扰电话 5.73 亿次。

（五） 福建省

全年恶意程序云查询拦截总量为 31.8 亿人次，接到网络诈骗举报 921 例，拦截钓鱼网站 36.65 亿次，拦截的钓鱼网站服务器位于该省的次数为 3.0 亿次，拦截垃圾短信量 7.26 亿条，骚扰电话 8.86 亿次。

（六） 甘肃省

全年恶意程序云查询拦截总量为 6.9 亿人次，接到网络诈骗举报 446 例，拦截钓鱼网站 0.85 亿次，拦截的钓鱼网站服务器位于该省的次数为 282 万次，拦截垃圾短信量 2.79 亿条，骚扰电话 5.43 亿次。

（七） 广东省

全年恶意程序云查询拦截总量为 126.2 亿人次，接到网络诈骗举报 3040 例，拦截钓鱼网站 109.58 亿次，拦截的钓鱼网站服务器位于该省的次数为 5.5 亿次，拦截垃圾短信量 37.59 亿条，骚扰电话 32.52 亿次。

（八） 广西

全年恶意程序云查询拦截总量为 23.8 亿人次，接到网络诈骗举报 762 例，拦截钓鱼网站 27.67 亿次，拦截的钓鱼网站服务器位于该省的次数为 1845 万次，拦截垃圾短信量 5.09 亿条，骚扰电话 8.77 亿次。

（九） 贵州省

全年恶意程序云查询拦截总量为 12.6 亿人次，接到网络诈骗举报 428 例，拦截钓鱼网站 3.31 亿次，拦截的钓鱼网站服务器位于该省的次数为 6371 万次，拦截垃圾短信量 3.96 亿条，骚扰电话 6.17 亿次。

（十） 海南省

全年恶意程序云查询拦截总量为 4.5 亿人次，接到网络诈骗举报 158 例，拦截钓鱼网站 1.69 亿次，拦截的钓鱼网站服务器位于该省的次数为 142 万次，拦截垃圾短信量 1.54 亿条，骚扰电话 1.89 亿次。

（十一） 河北省

全年恶意程序云查询拦截总量为 34.8 亿人次，接到网络诈骗举报 1120 例，拦截钓鱼网站 4.57 亿次，拦截的钓鱼网站服务器位于该省的次数为 2.4 亿次，拦截垃圾短信量 10.50 亿条，骚扰电话 13.35 亿次。

（十二） 河南省

全年恶意程序云查询拦截总量为 50.1 亿人次，接到网络诈骗举报 1480 例，拦截钓鱼网站 4.84 亿次，拦截的钓鱼网站服务器位于该省的次数为 3536 万次，拦截垃圾短信量 19.02 亿条，骚扰电话 17.78 亿次。

（十三） 黑龙江省

全年恶意程序云查询拦截总量为 18.5 亿人次，接到网络诈骗举报 409 例，拦截钓鱼网站 2.64 亿次，拦截的钓鱼网站服务器位于该省的次数为 230 万次，拦截垃圾短信量 4.04 亿条，骚扰电话 6.94 亿次。

（十四） 湖北省

全年恶意程序云查询拦截总量为 31.2 亿人次，接到网络诈骗举报 1094 例，拦截钓鱼网站 9.92 亿次，拦截的钓鱼网站服务器位于该省的次数为 1644 万次，拦截垃圾短信量 9.11 亿条，骚扰电话 9.18 亿次。

（十五） 湖南省

全年恶意程序云查询拦截总量为 28.4 亿人次，接到网络诈骗举报 931 例，拦截钓鱼网站 19.40 亿次，拦截的钓鱼网站服务器位于该省的次数为 1.7 亿次，拦截垃圾短信量 11.51 亿条，骚扰电话 9.66 亿次。

（十六） 吉林省

全年恶意程序云查询拦截总量为 16.2 亿人次，接到网络诈骗举报 317 例，拦截钓鱼网站 2.54 亿次，拦截的钓鱼网站服务器位于该省的次数为 1238 万次，拦截垃圾短信量 4.09 亿条，骚扰电话 4.60 亿次。

（十七） 江苏省

全年恶意程序云查询拦截总量为 48.4 亿人次，接到网络诈骗举报 1395 例，拦截钓鱼网站 11.95 亿次，拦截的钓鱼网站服务器位于该省的次数为 8.37 亿次，拦截垃圾短信量 19.61 亿条，骚扰电话 14.33 亿次。

（十八） 江西省

全年恶意程序云查询拦截总量为 18.8 亿人次，接到网络诈骗举报 619 例，拦截钓鱼网站 9.61 亿次，拦截的钓鱼网站服务器位于该省的次数为 1.2 亿次，拦截垃圾短信量 4.77 亿条，骚扰电话 6.28 亿次。

（十九） 辽宁省

全年恶意程序云查询拦截总量为 26.8 亿人次，接到网络诈骗举报 1051 例，拦截钓鱼网站 5.63 亿次，拦截的钓鱼网站服务器位于该省的次数为 8278 万次，拦截垃圾短信量 7.25 亿条，骚扰电话 8.97 亿次。

（二十） 内蒙古

全年恶意程序云查询拦截总量为 10.7 亿人次，接到网络诈骗举报 319 例，拦截钓鱼网站 1.32 亿次，拦截的钓鱼网站服务器位于该省的次数为 61 万次，拦截垃圾短信量 3.07 亿条，骚扰电话 4.73 亿次。

（二十一） 宁夏

全年恶意程序云查询拦截总量为 2.6 亿人次，接到网络诈骗举报 130 例，拦截钓鱼网站 0.33 亿次，拦截的钓鱼网站服务器位于该省的次数为 319 万次，拦截垃圾短信量 0.99 亿条，骚扰电话 1.54 亿次。

（二十二） 青海省

全年恶意程序云查询拦截总量为 1.5 亿人次，接到网络诈骗举报 68 例，拦截钓鱼网站 0.21 亿次，拦截的钓鱼网站服务器位于该省的次数为 2 万次，拦截垃圾短信量 0.85 亿条，骚扰电话 1.46 亿次。

（二十三） 山东省

全年恶意程序云查询拦截总量为 48.1 亿人次，接到网络诈骗举报 1992 例，拦截钓鱼网站 8.94 亿次，拦截的钓鱼网站服务器位于该省的次数为 8725 万次，拦截垃圾短信量 17.92 亿条，骚扰电话 18.91 亿次。

（二十四） 山西省

全年恶意程序云查询拦截总量为 23.3 亿人次，接到网络诈骗举报 787 例，拦截钓鱼网站 9.41 亿次，拦截的钓鱼网站服务器位于该省的次数为 1363 万次，拦截垃圾短信量 5.46 亿条，骚扰电话 6.62 亿次。

（二十五） 陕西省

全年恶意程序云查询拦截总量为 22.3 亿人次，接到网络诈骗举报 680 例，拦截钓鱼网站 2.25 亿次，拦截的钓鱼网站服务器位于该省的次数为 1024 万次，拦截垃圾短信量 9.44 亿条，骚扰电话 8.79 亿次。

（二十六） 上海市

全年恶意程序云查询拦截总量为 29.8 亿人次，接到网络诈骗举报 614 例，拦截钓鱼网站 15.28 亿次，拦截的钓鱼网站服务器位于该省的次数为 5031 万次，拦截垃圾短信量 14.06 亿条，骚扰电话 8.78 亿次。

（二十七） 四川省

全年恶意程序云查询拦截总量为 35.0 亿人次，接到网络诈骗举报 1354 例，拦截钓鱼网站 8.00 亿次，拦截的钓鱼网站服务器位于该省的次数为 2814 万次，拦截垃圾短信量 17.39 亿条，骚扰电话 13.13 亿次。

（二十八） 台湾省

全年恶意程序云查询拦截总量为 618 万人次，接到网络诈骗举报 2 例，拦截钓鱼网站 0.15 亿次，拦截的钓鱼网站服务器位于该省的次数为 1.2 亿次，拦截垃圾短信量 0.21 亿条，骚扰电话 0 次。

（二十九） 天津市

全年恶意程序云查询拦截总量为 25.7 亿人次，接到网络诈骗举报 289 例，拦截钓鱼网站 3.65 亿次，拦截的钓鱼网站服务器位于该省的次数为 4955 万次，拦截垃圾短信量 5.54 亿条，骚扰电话 3.37 亿次。

（三十） 西藏

全年恶意程序云查询拦截总量为 7317 万人次，接到网络诈骗举报 16 例，拦截钓鱼网站 0.09 亿次，拦截的钓鱼网站服务器位于该省的次数为 4 万次，拦截垃圾短信量 0.17 亿条，骚扰电话 0.74 亿次。

（三十一） 香港

全年恶意程序云查询拦截总量为 539 万人次，接到网络诈骗举报 3 例，拦截钓鱼网站 0.18 亿次，拦截的钓鱼网站服务器位于该省的次数为 7.5 亿次，拦截垃圾短信量 0.30 亿条，骚扰电话 0 次。

（三十二） 新疆

全年恶意程序云查询拦截总量为 9.3 亿人次，接到网络诈骗举报 348 例，拦截钓鱼网站 1.59 亿次，拦截的钓鱼网站服务器位于该省的次数为 40 万次，拦截垃圾短信量 2.04 亿条，骚扰电话 4.82 亿次。

（三十三） 云南省

全年恶意程序云查询拦截总量为 15.9 亿人次，接到网络诈骗举报 539 例，拦截钓鱼网站 2.49 亿次，拦截的钓鱼网站服务器位于该省的次数为 741 万次，拦截垃圾短信量 4.08 亿条，骚扰电话 6.75 亿次。

（三十四） 浙江省

全年恶意程序云查询拦截总量为 57.5 亿人次，接到网络诈骗举报 1254 例，拦截钓鱼网站 15.72 亿次，拦截的钓鱼网站服务器位于该省的次数为 10.20 亿次，拦截垃圾短信量 13.27 亿条，骚扰电话 12.29 亿次。