2016 年第二季度

中国互联网安全报告

360互联网安全中心

2016 年 8 月 30 日

摘　要

恶意程序

- 2016 年第二季度，360 互联网安全中心共截获 PC 端新增恶意程序样本 5863 万个，平均每天 64.4 万个，同比下降 26.7%；共为全国用户拦截恶意程序攻击 167.1 亿次，平均每天约 1.8 亿次，同比下降 26.3%。
- 2016 年第二季度，360 互联网安全中心共截获安卓平台新增恶意程序样本 426 万个，平均每天近 4.7 万个，同比下降 22.5%；累计监测到移动端用户感染恶意程序 6180 万人次，同比下降 6.0%，平均每天恶意程序感染量达到了 67.9 万人次。
- 2016 年第二季度，安卓平台新增恶意程序主要是资费消耗，占比高达 73.5%；其次为恶意扣费（18.8%）、隐私窃取（4.8%）、流氓行为（1.6%）和远程控制（1.2%）。
- 2016 年第二季度，综合 PC 端和移动端的恶意程序拦截量，从省域分布来看，北京是占比最高的地区，占比为 11.4%，其次是广东 10.1%、河北 6.0%、浙江 5.7%和江苏 5.6%。
- 2016 年第二季度，综合 PC 端和移动端的恶意程序拦截量，从城市分布来看，北京是占比最高的城市，占比为 11.4%，其次是上海 3.9%、成都 2.4%、天津 2.4%、重庆 2.3%、衡水 2.3%、深圳 2.2%、广州 2.1%、郑州 1.8%和西安 1.4%。

钓鱼网站

- 2016 年第二季度，360 互联网安全中心共拦截各类新增钓鱼网站 37.5 万个，同比下降 14.9%；平均每天新增 4121 个，每小时涌现超过 172 个钓鱼网站。新增钓鱼网站中，境外彩票的占比最大，达到了 42.6%，虚假购物 16.2%、假冒银行 8.7%。
- 综合 PC 端和移动端的情况，共为全国用户拦截钓鱼攻击 60.6 亿次，同比下降 32.3%，平均每天拦截 6659.3 万次。其中 PC 端占总拦截量的 92.2%；移动端为 7.8%，同比下降 44.7%。在钓鱼网站的拦截量类型方面，境外彩票占到了 56.3%，排名第一，其次是虚假购物 5.5%和金融证券 4.8%。
- 从省域看，广东地区占比为 32.5%，福建 12.1%、广西 9.6%、湖南 6.7%、北京 5.2%等地是钓鱼网站攻击次数排名前五的省份。拦截最多的城市为深圳 3.3 亿次，其次为广州 3.0 亿次、北京 3.0 亿次、南宁 2.2 亿次、东莞 2.2 亿次。
- 从钓鱼网站新增的服务器的地域分布来看，38.0%的钓鱼网站新增量所属服务器位于国内，62.0%位于国外。其中。国内的服务器位于香港的最多，占比为 61.8%，其次是广东（10.0%）、河南（5.1%）、江苏（3.9%）、上海（3.8%）和北京（3.5%）。国外的服务器中，位于美国的最多，占比为 93.0%。
- 从钓鱼网站拦截量上看，77.8%的钓鱼网站攻击来自国内，22.2%来自国外。在来自国内的攻击中，香港的占比为 19.8%，其次是浙江 18.1%、江苏 13.5%、福建 13.2%、广东 10.5%和北京 7.9%。而在来自国外的攻击中，美国的最多，占比为 58.7%，其次是加拿大 19.6%、日本 4.4%。相比而言，国外钓鱼网站的服务器地域分布集中度高。

骚扰电话

- ✧ 2016 年第二季度，用户通过 360 手机卫士标记各类骚扰电话号码数量约 6691 万个，平均每天被用户标记的各类骚扰电话号码约 74 万个，同比下降 19.3%。
- ✧ 从拦截量上看，360 手机卫士共为全国用户识别和拦截各类骚扰电话 91.2 亿次，平均每天识别和拦截骚扰电话 1.0 亿次，同比上升 13.9%。
- ✧ 从标记量来看，“响一声”电话以 53.1%的比例位居用户标记骚扰电话的首位；其次为诈骗电话 9.6%、广告推销 8.2%、房产中介 2.8%、保险理财 2.3%和招聘猎头 1.1%。
- ✧ 从骚扰电话识别和拦截量来看，诈骗电话以 13.5%位居首位，其次为广告推销 12.9%、响一声 7.6%、房产中介 4.3%、保险理财 1.4%和客服电话 0.7%。
- ✧ 从地域看，来自广东的骚扰电话被拦截次数最多，占到了拦截次数总量的 20.4%，其次是北京 12.2%、上海 11.6%、江苏 9.7%、福建 5.8%。拦截最多的十个城市则分别是：北京、上海、广州、深圳、苏州、合肥、成都、厦门、杭州和郑州。

垃圾短信

- ✧ 2016 年第二季度，360 手机卫士共为全国用户拦截各类垃圾短信约 45.5 亿条，同比下降 43.1%；平均每天拦截垃圾短信 5000 万条。
- ✧ 从类型看，垃圾短信中广告推销最多，占比为 79.6%，其次是违法信息 13.4%和诈骗短信 7.0%。对诈骗短信作进一步分类，其中冒充银行类诈骗短信占比最高，为 38.0%，其次是冒充电信运营商 28.4%、冒充会员推广 20.4%。
- ✧ 从地域看，广东地区用户接到的垃圾短信数量最多，占全国总量的 15.8%；其次为北京 7.8%、山东 7.8%、江苏 6.7%、河南 6.7%。
- ✧ 从城市看，北京用户接到的垃圾短信数量最多，排名前十的城市还有广州、上海、郑州、深圳、南京、西安、成都、重庆和天津。

网络诈骗

- ✧ 2016 年第二季度，猎网平台共接到来自全国各地的网络诈骗举报 5509 起，涉案总金额高达 4524.8 万元，人均损失 8213 元。其中，PC 端用户报案 3633 例，涉案总金额为 3673.9 万元，人均损失 10112 元；手机用户报案 1876 例，涉案总金额为 850.5 万元，人均损失约为 4534 元。
- ✧ 从类型看，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 1283 例，占比 23.4%；其次是虚假购物 862 例，占比 15.8%、网游交易 658 例，占比 12.0%、虚拟商品 654 例，占比 12.0%和金融理财 497 例，占比 9.1%。
- ✧ 综合涉案金额和人均损失来看，金融理财诈骗（497 人，30675 元）、赌博博彩（206 人，29366 元）、身份冒充（376 人，6146 元）和退款盗号（204 人，6397 元）属于高危诈骗类型，受害人多，人均损失大。

网站安全

- ✧ 2016 年第二季度，360 网站安全检测平台共扫描各类网站 321.8 万个，其中，存在安全漏洞的网站为 63.8 万个，占扫描网站总数的 23.5%。其中，存在高危安全漏洞的网站共有 9.3 万个，占扫描网站总数的 2.8%，同比下降 57.5%。
- ✧ 2016 年第二季度，从有漏洞网站的省级区域分布来看，广东是占比最高的地区，占比为 15.8%，其次是四川 15.2%、香港 12.2%、重庆 8.7%和福建 6.6%。前 5 名省区总和占全国的 58.5%。
- ✧ 2016 年第二季度，360 网站安全检测平台共对 252.0 万个网站进行了篡改检测，其中，被篡改（不包括被植入后门程序）的网站 1.7 万个，约占扫描网站总数的 0.7%。
- ✧ 2016 年第二季度，360 网站安全检测对 3.2 万台网站服务器进行了网站后门检测，扫描发现约 25.1%的服务器存在后门。
- ✧ 2016 年第二季度，360 网站安全检测的后门数量高达 1660.7 万个，平均每天检出后门数量 18.2 万个。

补天

- ✧ 2016 年第二季度，补天平台共收录 1618 名“白帽子”提交的有效漏洞 10909 个，平均每天收录有效漏洞 120 个。其中通用型漏洞 571 个，占比为 5.25%，事件型漏洞则占 94.8%。
- ✧ 2016 年第二季度补天平台新收录漏洞中，SQL 注入 38.7%、命令执行 18.0%、弱口令 10.9%是被报告数量最多的漏洞类型。
- ✧ 从地域分布看，2016 年第二季度补天收录的漏洞中，北京 28.0%、上海 7.6%、广东 7.4%、江苏 5.3%、浙江 4.9%等地的网站漏洞最多，总和超过总量的 53.2%。

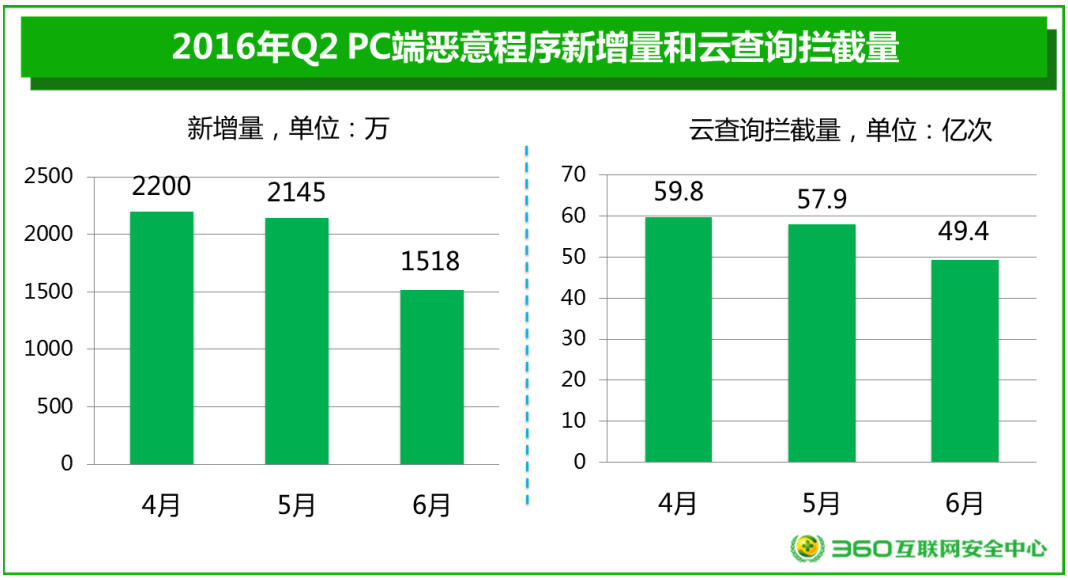
关键词：恶意程序、钓鱼网站、网络诈骗、网站安全、补天

目　　录

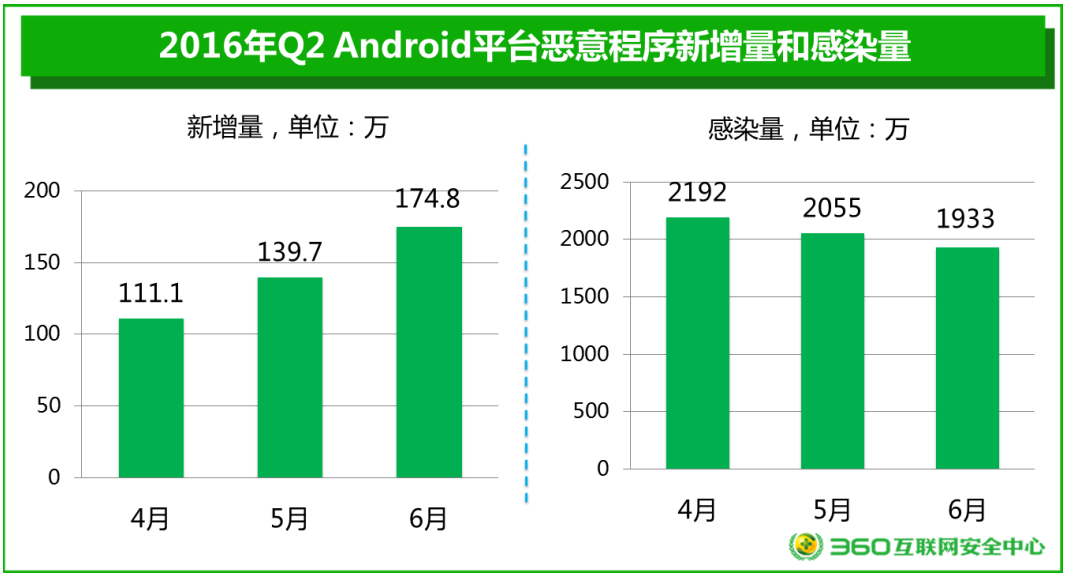
第一章 恶意程序

一、 新增量与拦截量

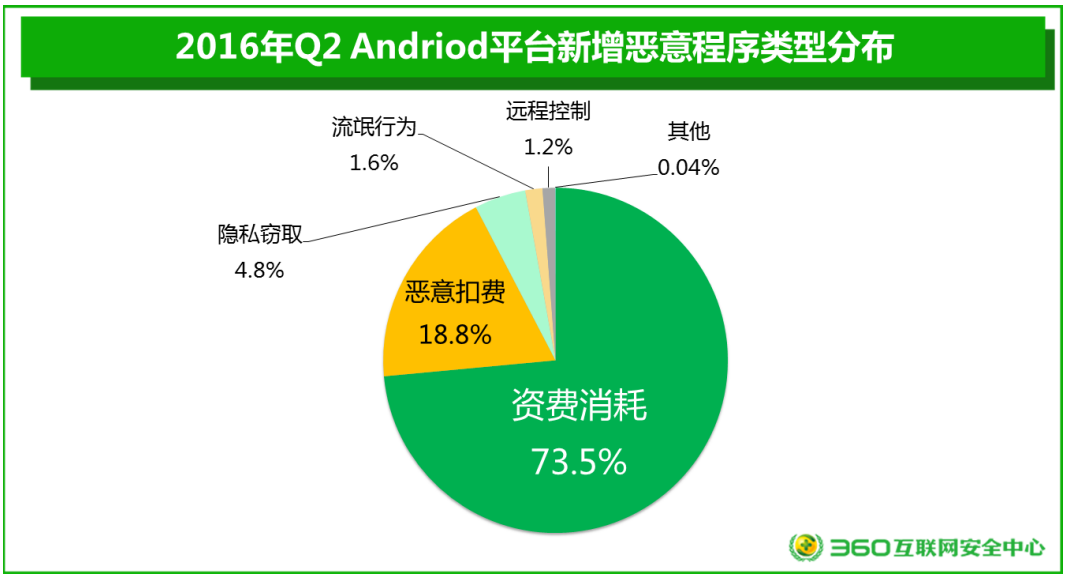
2016 年第二季度，360 互联网安全中心共截获 PC 端新增恶意程序样本 5863 万个，同比 2015 年第二季度（8002 万个）下降 26.7%，平均每天截获新增恶意程序样本 64.4 万个。360 安全产品共为全国用户拦截恶意程序攻击 167.1 亿次，同比 2015 年第二季度（226.7 亿次）下降 26.3%，平均每天为用户拦截恶意程序攻击约 1.8 亿次。下图给出了 2016 年二季度各月 PC 端恶意程序新增量和拦截量统计情况。



2016 年第二季度，360 互联网安全中心共截获安卓平台新增恶意程序样本 426 万个，同比 2015 年第二季度（550 万个）下降 22.5%，平均每天截获新增手机恶意程序样本近 4.7 万个。累计监测到移动端用户感染恶意程序 6180 万人次，同比 2015 年第二季度（6573 万次）下降 6.0%，平均每天恶意程序感染量达到了 67.9 万人次。

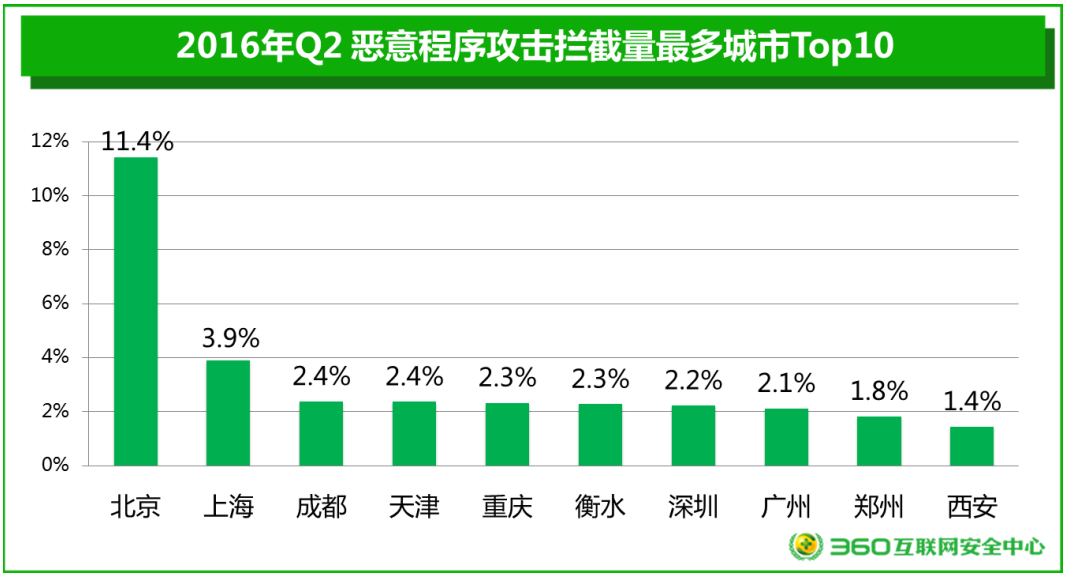


2016 年第二季度安卓平台新增恶意程序主要是资费消耗，占比高达 73.5%；其次为恶意扣费（18.8%）、隐私窃取（4.8%）、流氓行为（1.6%）和远程控制（1.2%）。

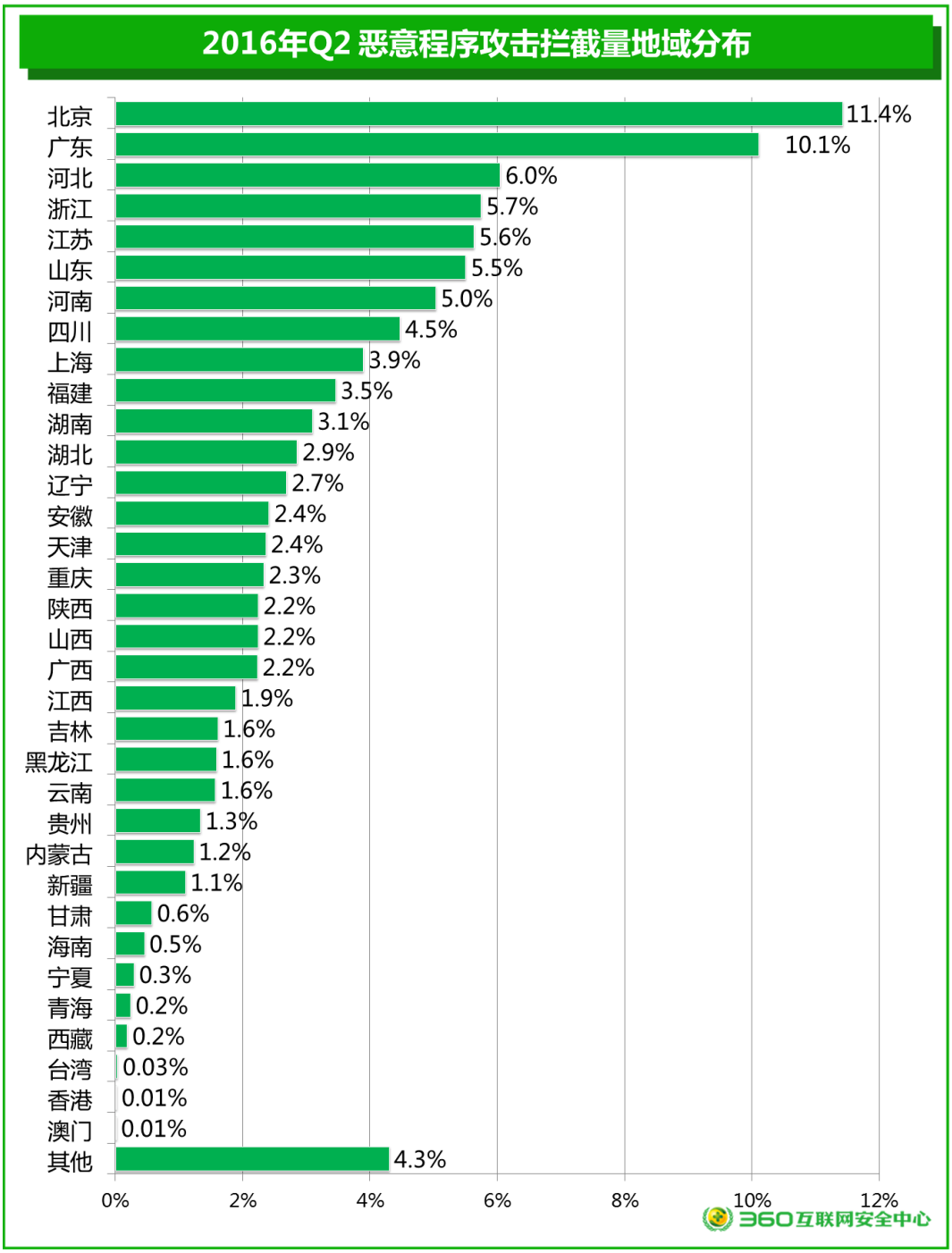


二、 地域分布

2016 年第二季度，从城市分布来看，综合 PC 端和移动端的恶意程序拦截量，北京是占比最高的城市，占比为 11.4%，其次是上海的 3.9%、成都的 2.4%、天津的 2.4%、 重庆的 2.3%、衡水为 2.3%、深圳为 2.2%、广州为 2.1%、郑州为 1.8%和西安为 1.4%。



2016 年第二季度，综合 PC 端和移动端的恶意程序拦截量，从地域分布来看，北京是占比最高的地方，占比为 11.4%，其次是广东的 10.1%、河北的 6.0%、浙江的 5.7%和江苏的 5.6%。



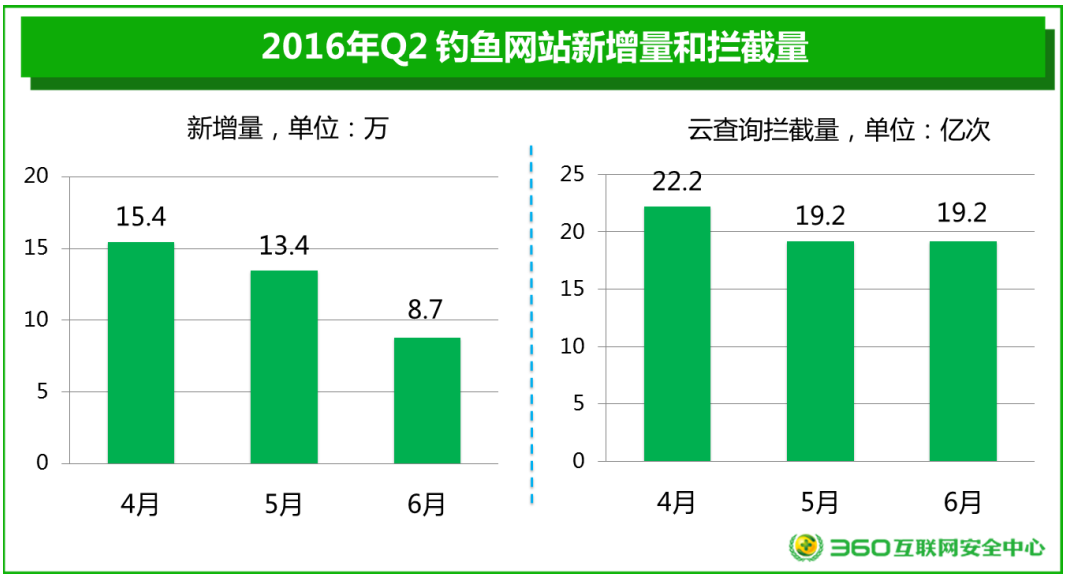
第二章 钓鱼网站

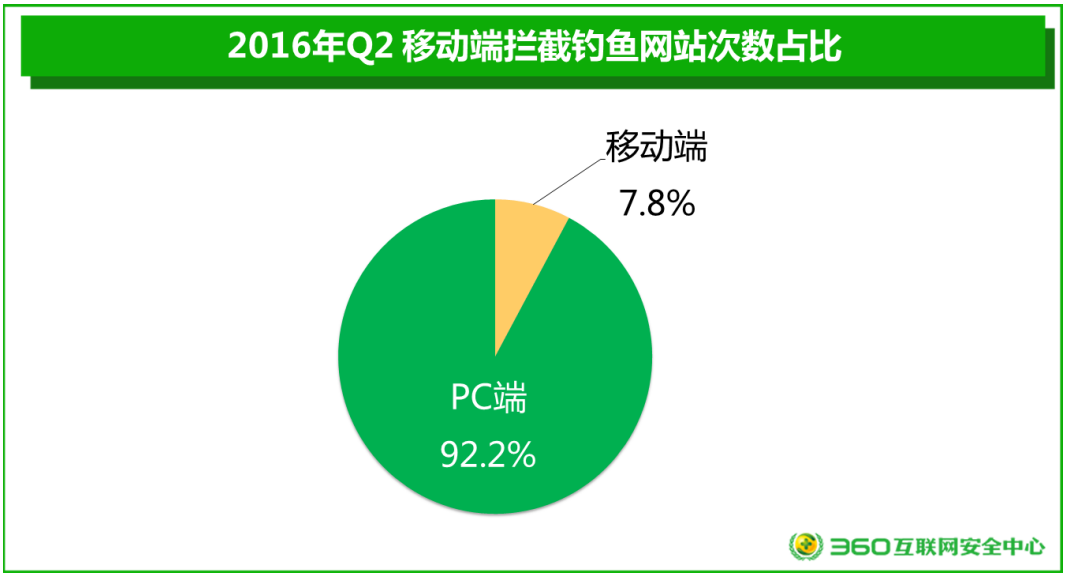
一、 新增量和拦截量

2016 年第二季度，360 互联网安全中心共截获各类新增钓鱼网站 37.5 万个，同比 2015 年第二季度（44.1 万个）下降 14.9%；平均每天新增 4121 个，每小时涌现超过 172 个钓鱼网站。

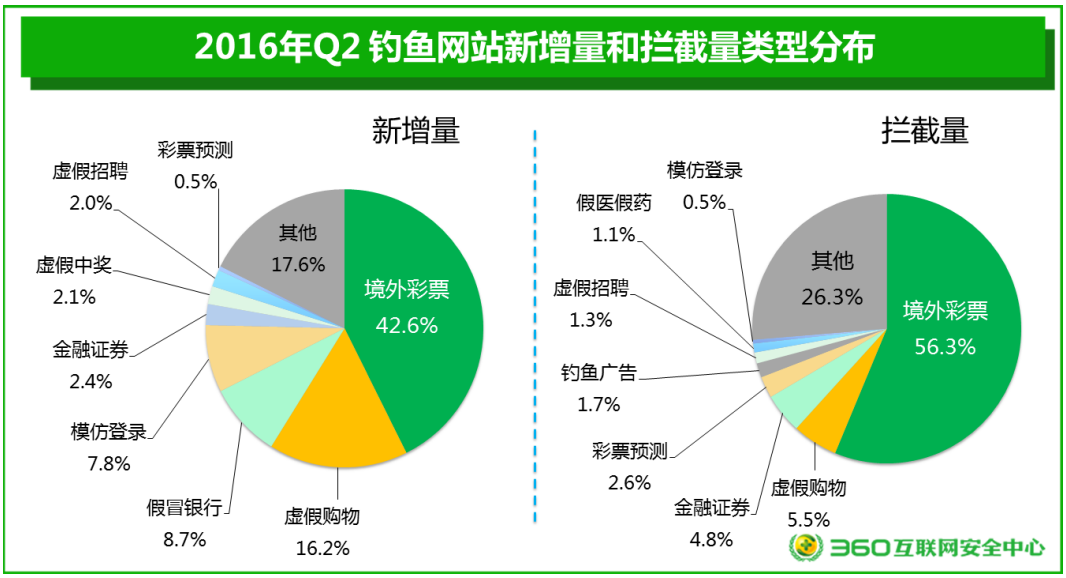
2016 年第二季度，360 的 PC 端和手机安全软件共为全国用户拦截钓鱼攻击 60.6 亿次，同比 2015 年第二季度（89.5 亿次）下降 32.3%，平均每天拦截 6659.3 万次。其中 PC 端拦截量为 55.9 亿次，占总拦截量的 92.2%；移动端为 4.7 亿次，占总拦截量的 7.8%，同比 2015 年第二季度（8.5 亿次）下降了 44.7%。

下图给出了综合 PC 端和移动端各月的钓鱼网站新增量和拦截量，及拦截量占比。

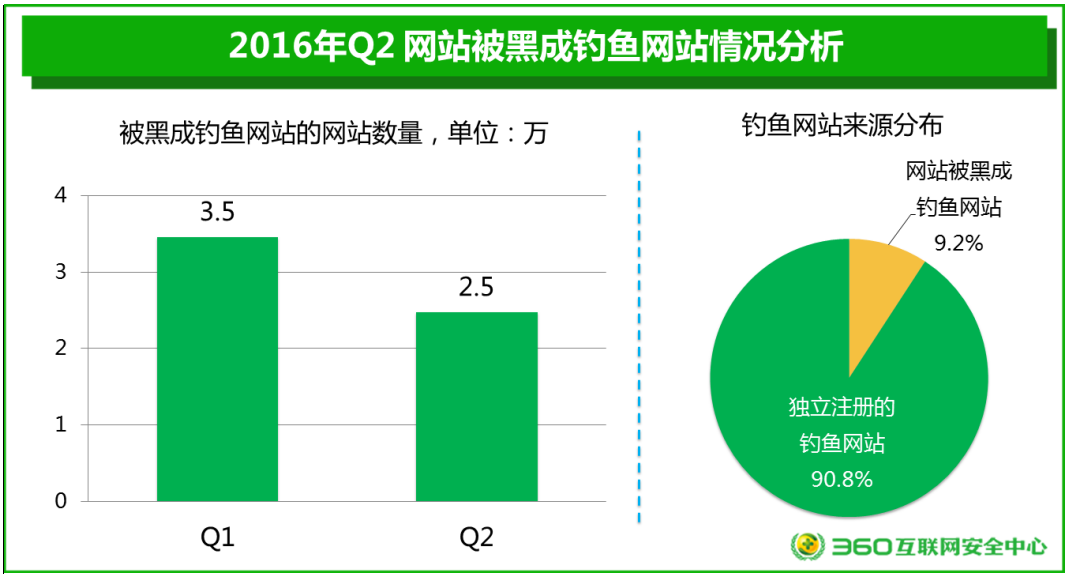




在新增钓鱼网站中，境外彩票以 16.03 万个位居首位，占比 42.6%，相比 2016 年第一季度的境外彩票（13.48 万个，占比 30.5%）上升 18.9%，虚假购物 16.2%、假冒银行 8.7%位列其后。钓鱼网站的拦截量方面，境外彩票占到了 56.3%，排名第一，其次是虚假购物 5.5%、金融证券 4.8%。

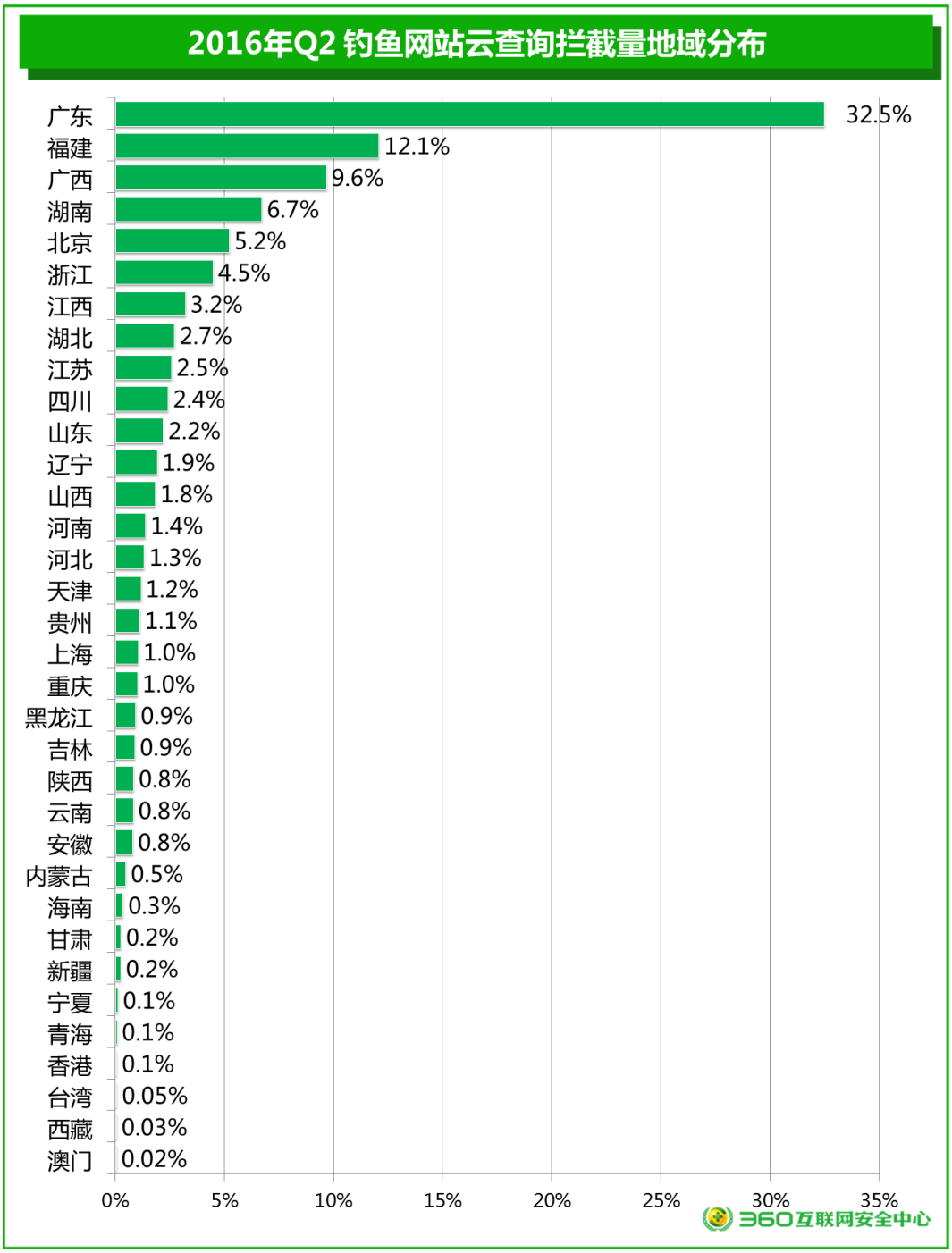


另据 360 互联网安全中心监测，2016 年以来，网站被黑并被篡改为钓鱼网站的情况日益严重。一季度就有至少 3.5 万个网站被黑成了钓鱼网站；而二季度以来，又有约 2.5 万个网站被黑成了钓鱼网站，占新增钓鱼网站总量的 9.2%。攻击者之所以会使用被黑网站作为钓鱼网站，主要目的就是为了躲避安全软件的监控与拦截。同时，网站被黑也表明网站存在着明显的没有修复的安全漏洞。

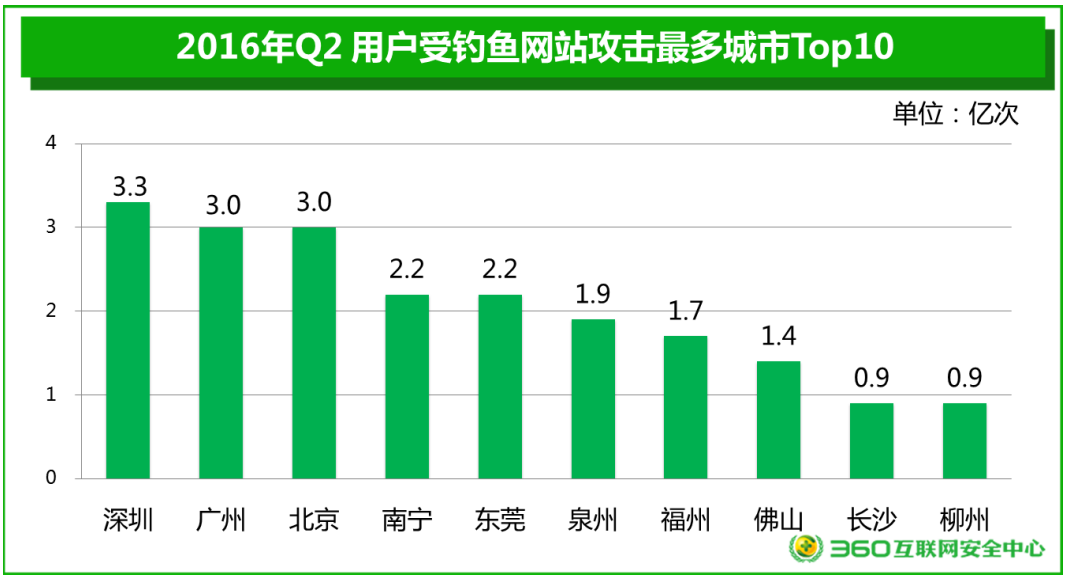


二、 拦截量地域分布

从用户遭遇钓鱼网站攻击的地域分布来看（综合 PC 端和移动端），广东占比为 32.5%，福建占比 12.1%、广西占比 9.6%、湖南占比 6.7%、北京占比 5.2%，这些是钓鱼网站攻击次数排名前五的省份。

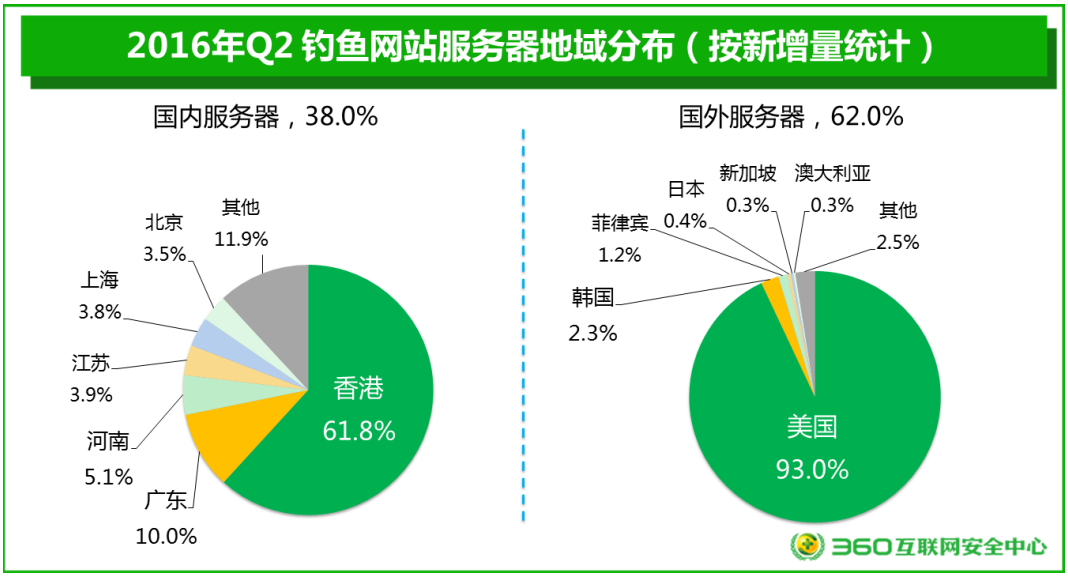


从各主要城市用户遭到钓鱼攻击的情况来看（综合 PC 端和移动端情况），排名前五的城市分别为深圳（3.3 亿次），广州（3.0 亿次）、北京（3.0 亿次）、南宁（2.2 亿次）、东莞（2.2 亿次）。

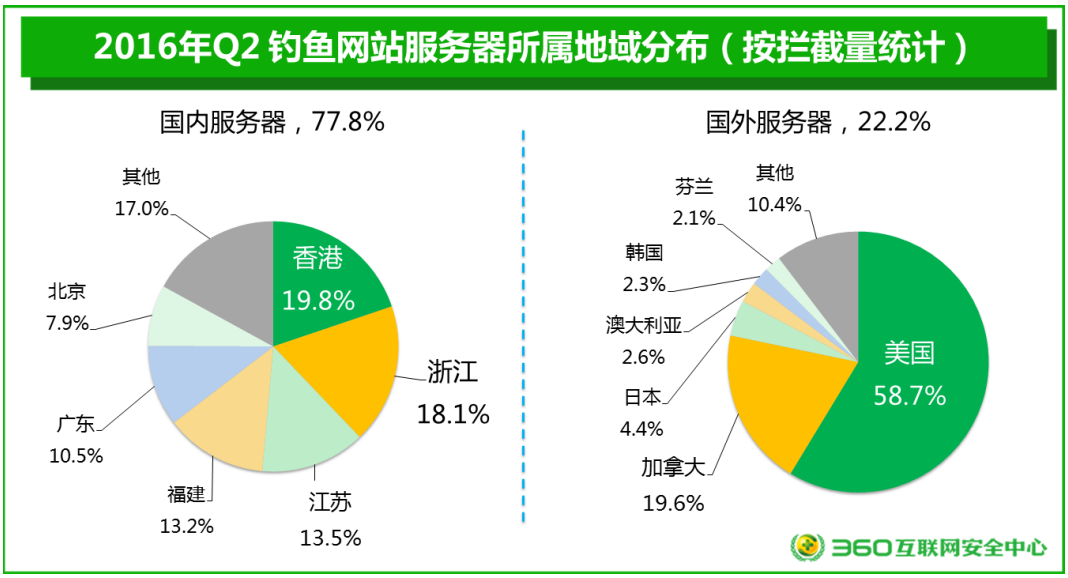


三、 服务器地域分布

从新增钓鱼网站的服务器的地域分布来看，38.0%的钓鱼网站服务器位于国内，62.0%位于国外。其中国内的服务器位于香港的占比为 61.8%，其次是广东（10.0%）、河南（5.1%）、江苏（3.9%）、上海（3.8%）和北京（3.5%）。国外的服务器中，位于美国的最多，占比为 93.0%。



从钓鱼网站拦截量上看，77.8%的钓鱼网站攻击来自国内，22.2%位于国外。在来自国内的攻击中，香港的占比为 19.8%，其次是浙江（18.1%）、江苏（13.5%）、福建（13.2%）、广东（10.5%）和北京（7.9%）。而在来自国外的攻击中，美国最多，占比为 58.7%，其次是加拿大（19.6%）、日本（4.4%）。总体而言，国外钓鱼网站的服务器地域分布集中度高。



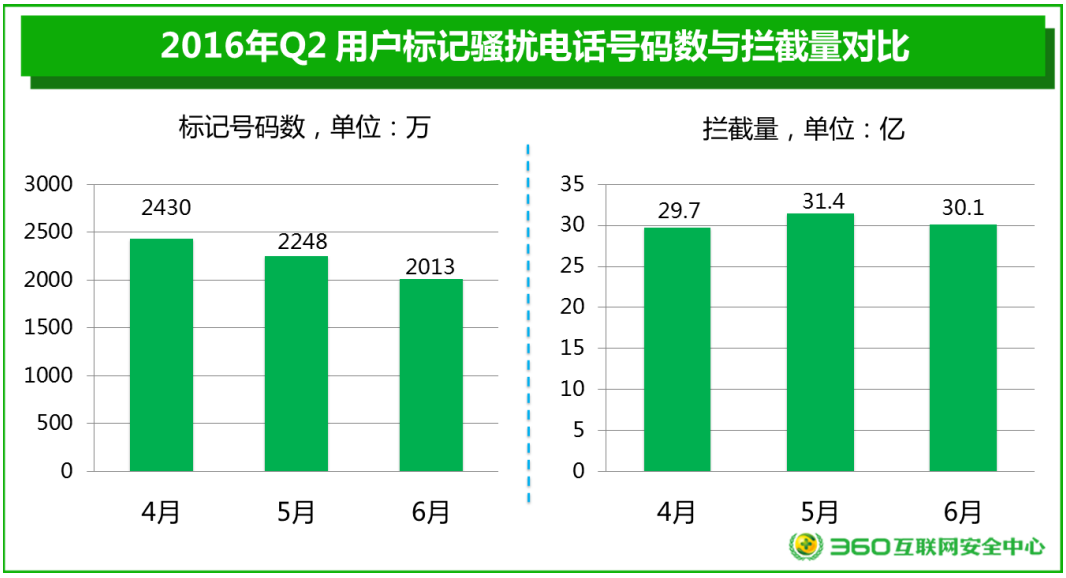
第三章 骚扰电话

一、 骚扰电话数量

2016 年第二季度，用户通过 360 手机卫士标记各类骚扰电话号码数量（包括 360 手机卫士自动检出的响一声电话）约 6691 万个，平均每天被用户标记的各类骚扰电话号码约 74 万个。从总量上看，相比 2015 年第二季度（8291 万）下降了 19.3%。

2016 年第二季度，从拦截量上看，360 手机卫士共为全国用户识别和拦截各类骚扰电话 91.2 亿次，平均每天识别和拦截骚扰电话 1.0 亿次；总量上较 2015 年第二季度的 80.1 亿次同比上升了 13.9%。

第二季度骚扰电话号码标记量与拦截量各月分布对比如下：

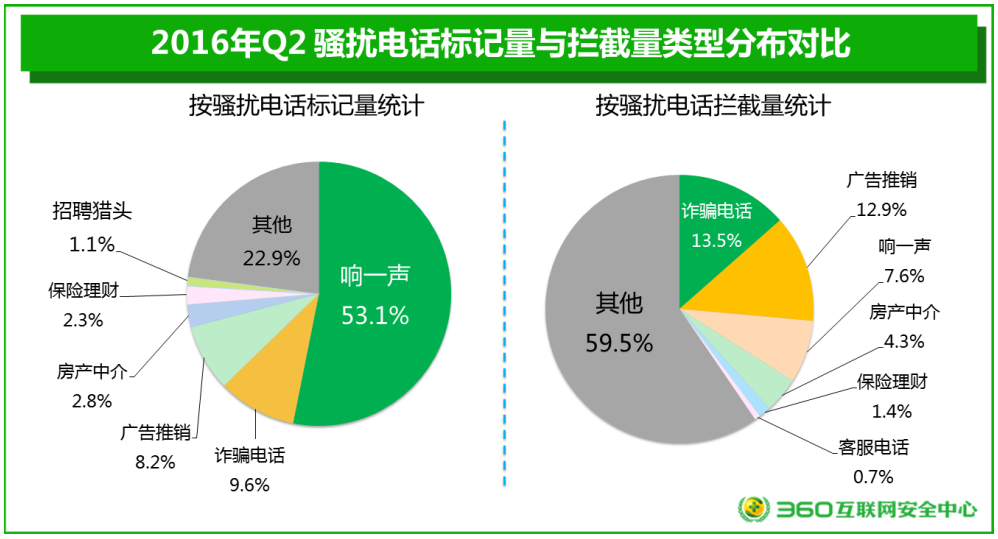


二、 类型分析

从标记量来看，“响一声”电话以 53.1%的比例位居用户标记骚扰电话的首位；其次为诈骗电话 9.6%、广告推销 8.2%、房产中介 2.8%、保险理财 2.3%、招聘猎头 1.1%以及其他骚扰 22.9%。

从骚扰电话的识别和拦截量来看，诈骗电话以 13.5%位居首位，其次为广告推销 12.9%、响一声 7.6%、房产中介 4.3%、保险理财 1.4%、客服电话 0.7%以及其他骚扰 59.5%。

下图给出了 2016 年第二季度骚扰电话标记量与拦截量类型分布：

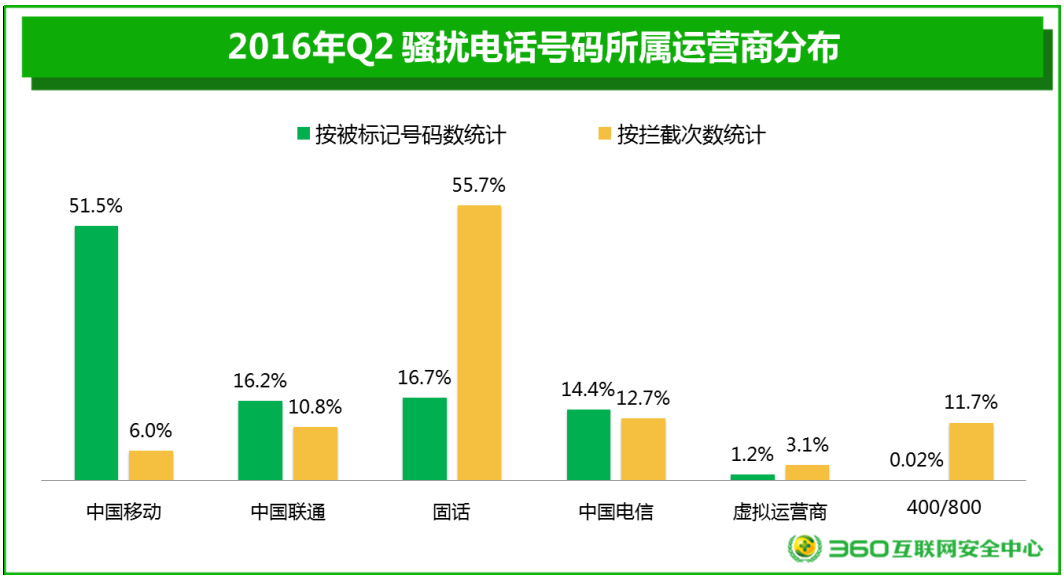


三、 骚扰号源归属运营商

从下图可以看出，2016 年第二季度，在用户标记的骚扰电话号码中，中国移动手机号最多，占比为 51.5%，这与中国移动的市场份额大致相当。而从拦截量上看，中国移动手机号占比仅为 6.0%，明显低于中国电信手机号的 12.7%和中国联通手机号的 10.8%。这说明，中国移动手机号的单个号码骚扰强度远远低于中国电信和中国联通，这可能与中国移动对高危号码的严格管理有关。

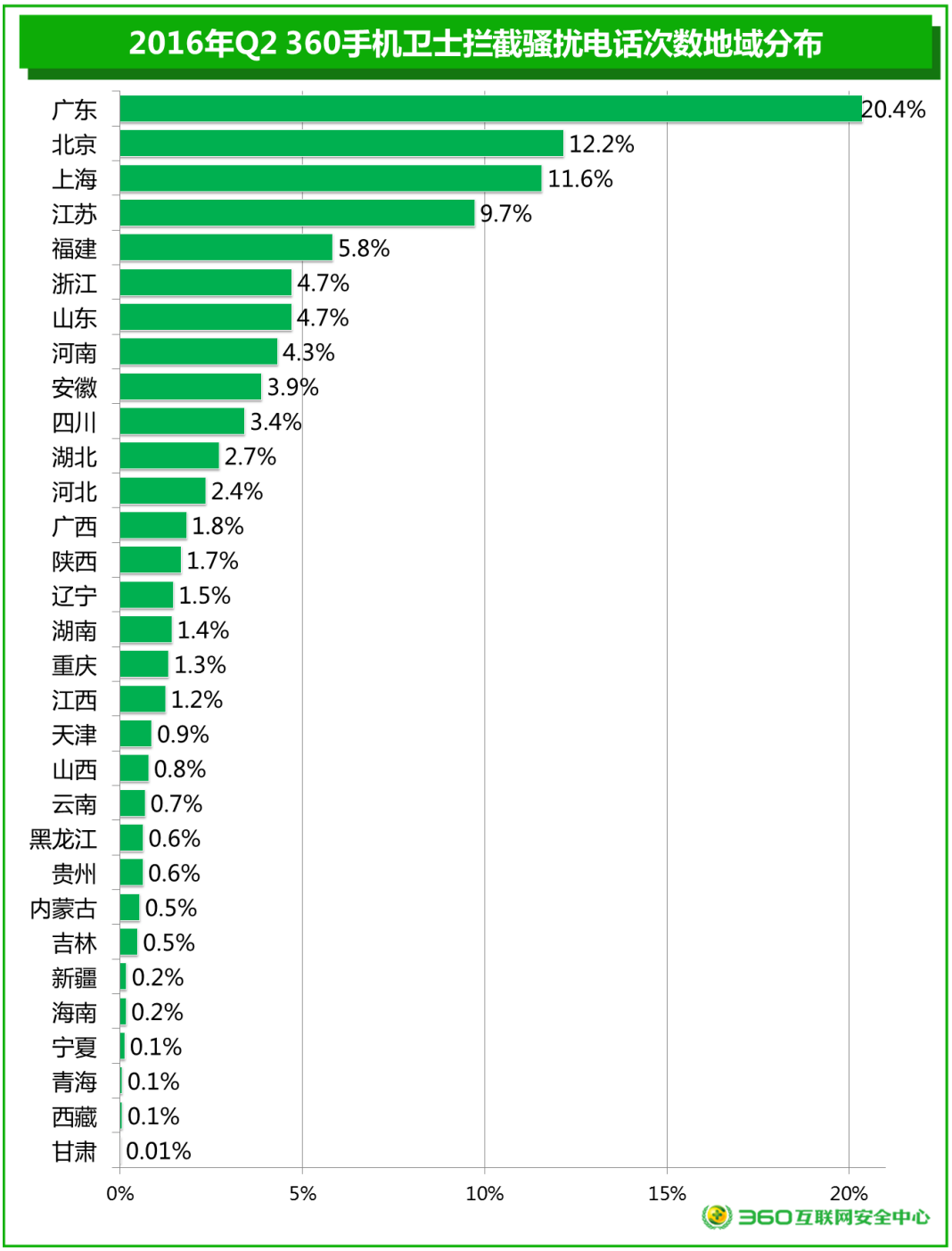
此外，单从拦截量上看，固定电话是最大的骚扰源，固定电话呼出的骚扰电话占骚扰电话总呼叫量的 55.7%。此外，400/800 号码呼出的骚扰电话也占到了 11.7%的比例。这表明，当前骚扰电话的治理工作重心应当从移动电话转移到固定电话和 400/800 电话。

下图给出了骚扰电话按号码归属运营商的比例分布：

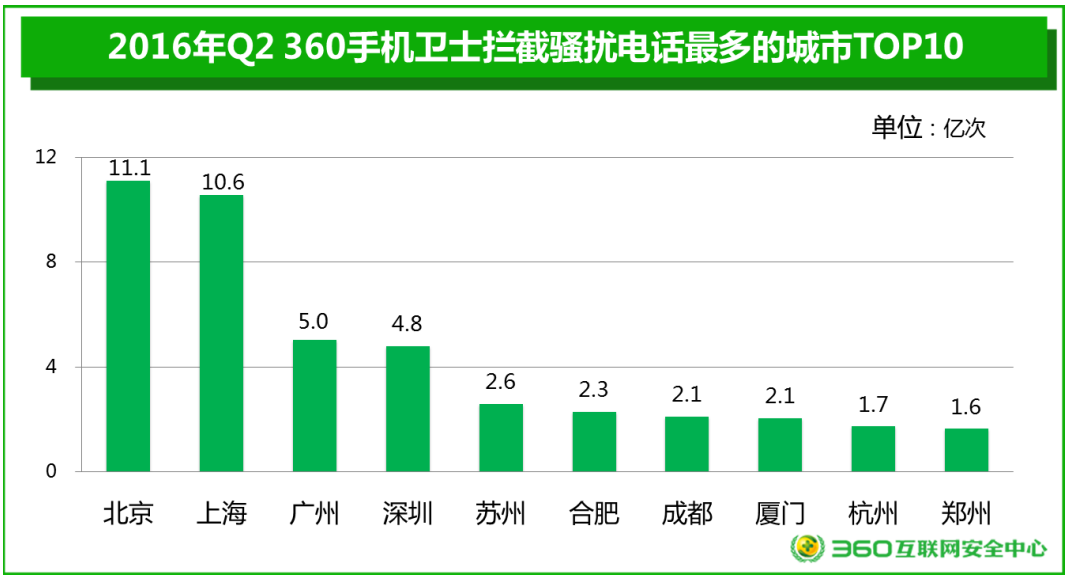


四、 地域分析

从骚扰电话的拦截量来看，广东省用户接到的骚扰电话最多，占到了骚扰电话总量的20.4%，其次是北京（12.2%）、上海（11.6%）、江苏（9.7%）、福建（5.8%）。



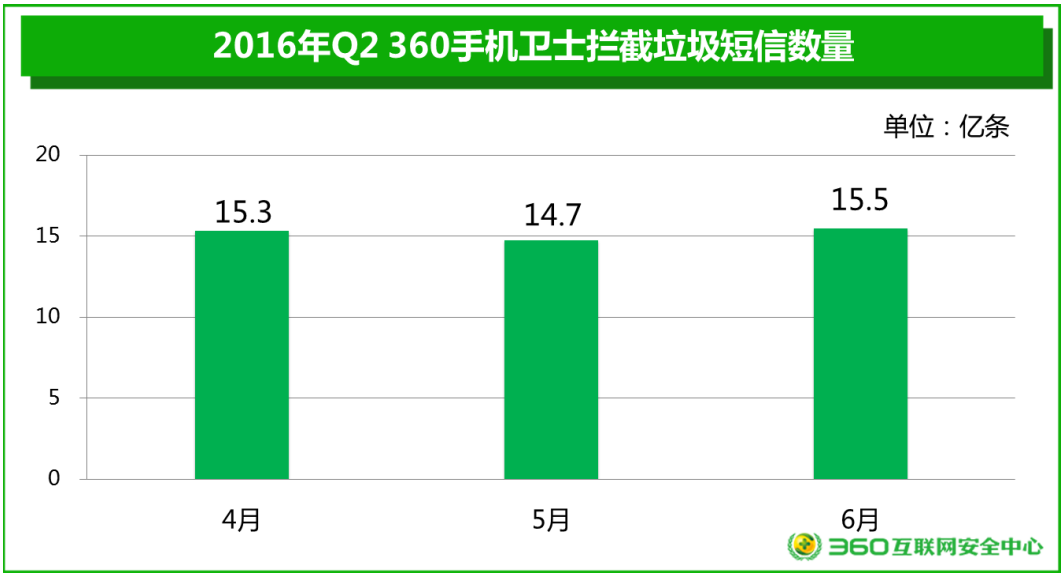
从城市情况来看，被骚扰电话骚扰最多的城市是北京，为 11.1 亿次，其次是上海（10.6 亿次）、广州（5.0 亿次），排名第四到第十位的城市分别是：深圳、苏州、合肥、成都、厦门、杭州和郑州。具体见下图：



第四章 垃圾短信

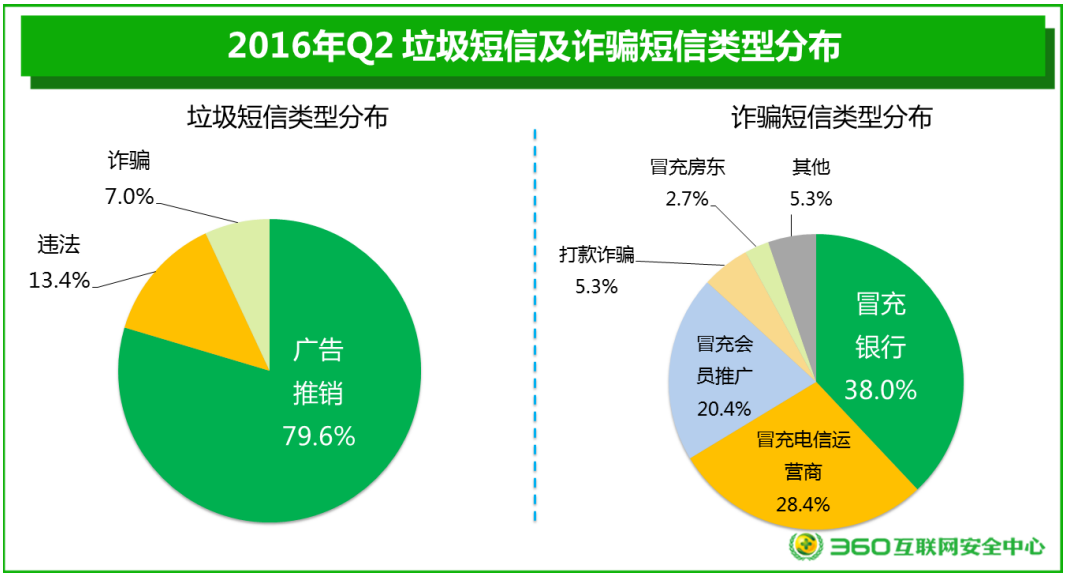
一、 垃圾短信数量

2016 年第二季度，360 手机卫士共为全国用户拦截各类垃圾短信约 45.5 亿条，同比 2015 年第二季度的 80.0 亿条同比大幅下降了 43.1%，平均每天拦截垃圾短信 5000 万条。



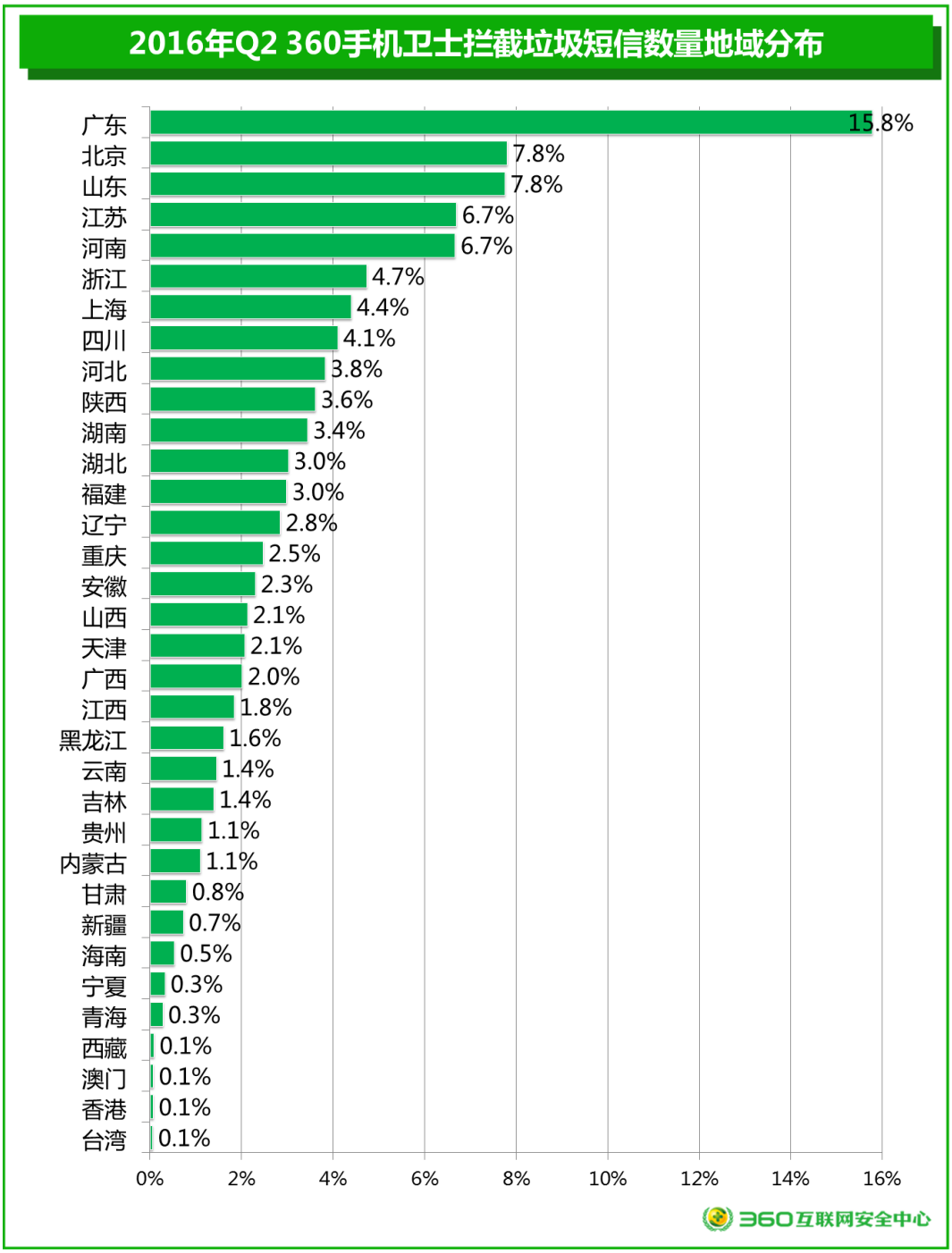
二、 类型分析

下图给出了 2016 年第二季度，所有垃圾短信与诈骗短信的类型分布。垃圾短信中广告推销最多，占比为 79.6%。其次是违法信息 13.4%和诈骗短信 7.0%。对诈骗短信作进一步分类分析显示，冒充银行类诈骗短信占比最高，为 38.0%，其次是冒充电信运营商 28.4%、冒充会员推广 20.4%、打款诈骗 5.3%和冒充房东 2.7%。

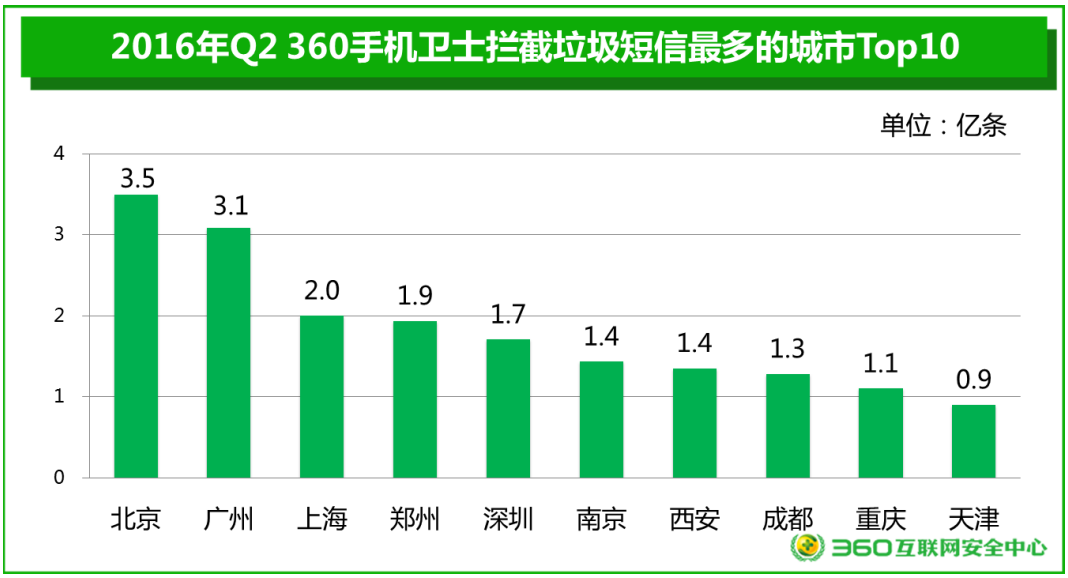


三、 地域分析

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 15.8%；其次为北京（7.8%）、山东（7.8%）、江苏（6.7%）、河南（6.7%）。下图给出了垃圾短信的地域分布：



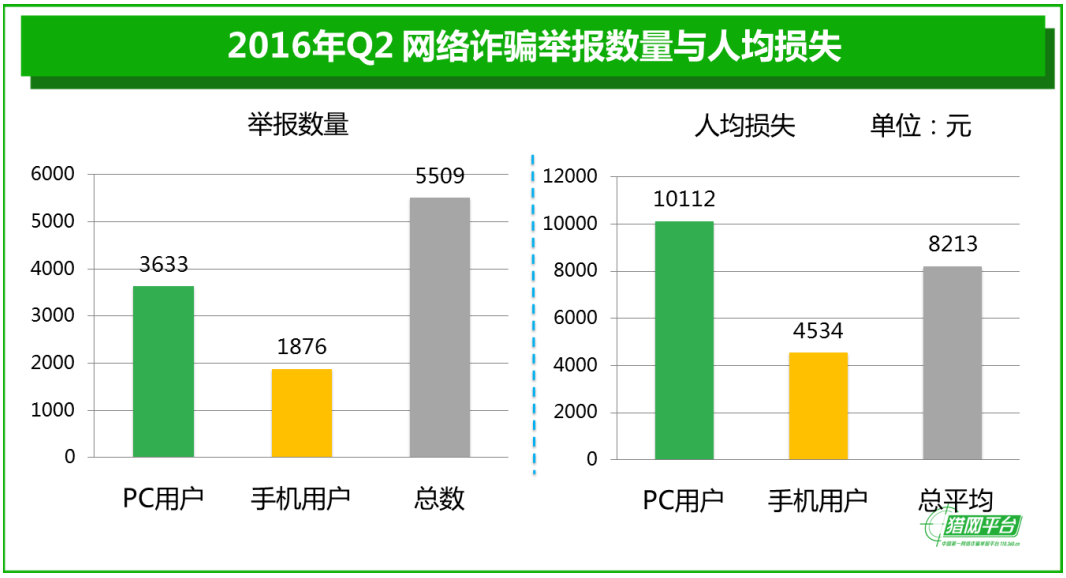
下图给出了 2016 年第二季度 360 手机卫士拦截垃圾短信数量最多的十大城市。其中，北京的垃圾短信拦截量最多，高达 3.5 亿条，居于全国首位；其次是广州（3.1 亿条）、上海（2.0 亿条）、郑州（1.9 亿条）、深圳（1.7 亿条）、南京（1.4 亿条）、西安（1.4 亿条）、成都（1.3 亿条）、重庆（1.1 亿条）和天津（0.9 亿条）。



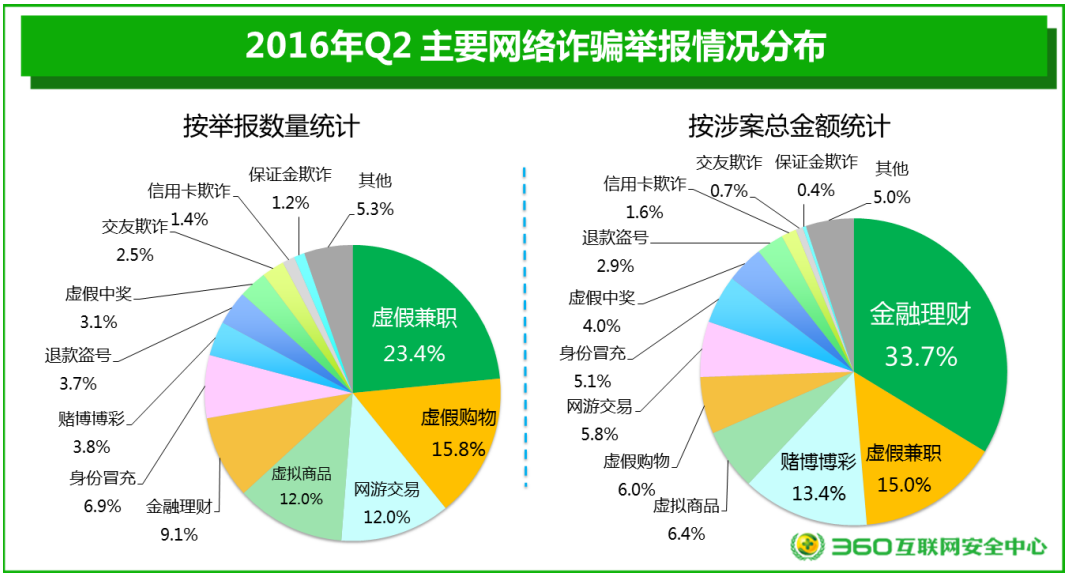
第五章 网络诈骗

一、用户举报情况

2016 年第二季度，猎网平台共接到来自全国各地的网络诈骗举报 5509 起，涉案总金额高达 4524.8 万元，人均损失 8213 元。其中，PC 用户报案 3633 例，涉案总金额为 3673.9 万元，人均损失 10112 元；手机用户报案 1876 例，涉案总金额为 850.5 万元，人均损失约为 4534 元。人均损失方面，PC 端用户人均损失相比 2016 年第一季度（4543 元）有显著的上升，可能和金融理财和赌博博彩的人均损失显著上升有关，移动端人均损失较 2016 年第一季度人均损失 7662 元有明显的下降。



二、类型分析

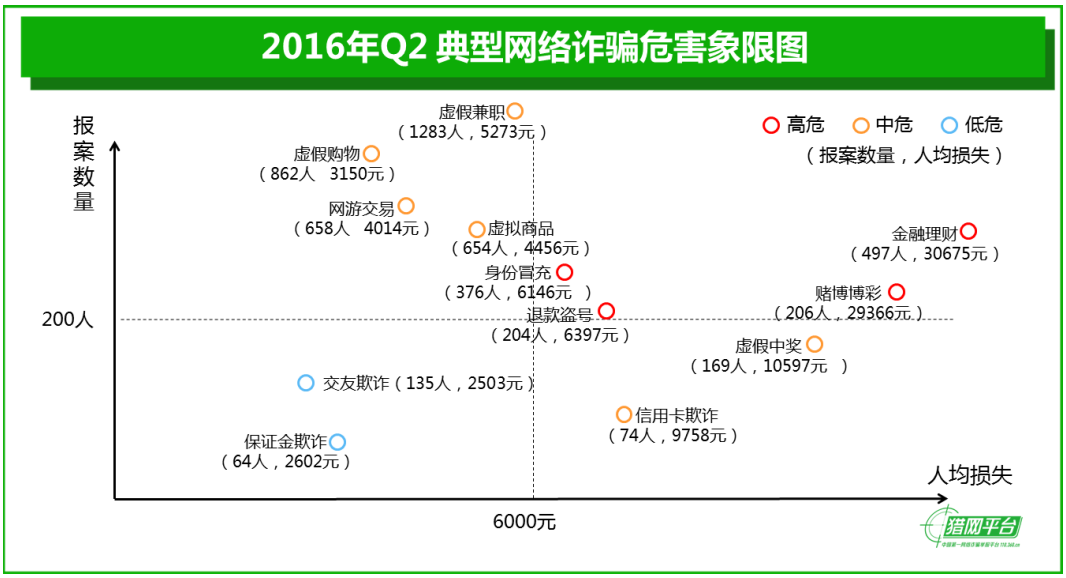


在所有举报的诈骗案情中，虚假兼职依然是举报数量最多的诈骗类型，共举报 1283 例，

占比 23.4%；其次是虚假购物 862 例（占比 15.8%）、网游交易 658 例（占比 12.0%）、虚拟商品 654 例（占比 12.0%）和金融理财 497 例（占比 9.1%）。

从涉案总金额来看，金融理财类诈骗总金额最高，达 1524.5 万元，占比为 33.7%；其次是虚假兼职诈骗，涉案总金额为 676.5 万元，占比为 15.0%；赌博博彩诈骗排第三，涉案总金额 604.9 万元，占比为 13.4%。下图给出了网络诈骗类型的举报量和涉案总金额分布。

下图给出了不同类型的网络诈骗人均损失和举报数量的象限图。从图中可见，金融理财诈骗（497 人，30675 元）、赌博博彩（206 人，29366 元）、身份冒充（376 人，6146 元）和退款盗号（204 人，6397 元）属于高危诈骗类型，受害人多，人均损失大。而虚假购物（862 人，3150 元）、网游交易（658 人，4014 元）、虚拟商品（645 人，4456 元）、虚假兼职（1283 人，5273 元）、虚假中奖（169 人，10597 元）和信用卡欺诈（74 人、9758 元）属于中危诈骗类型。

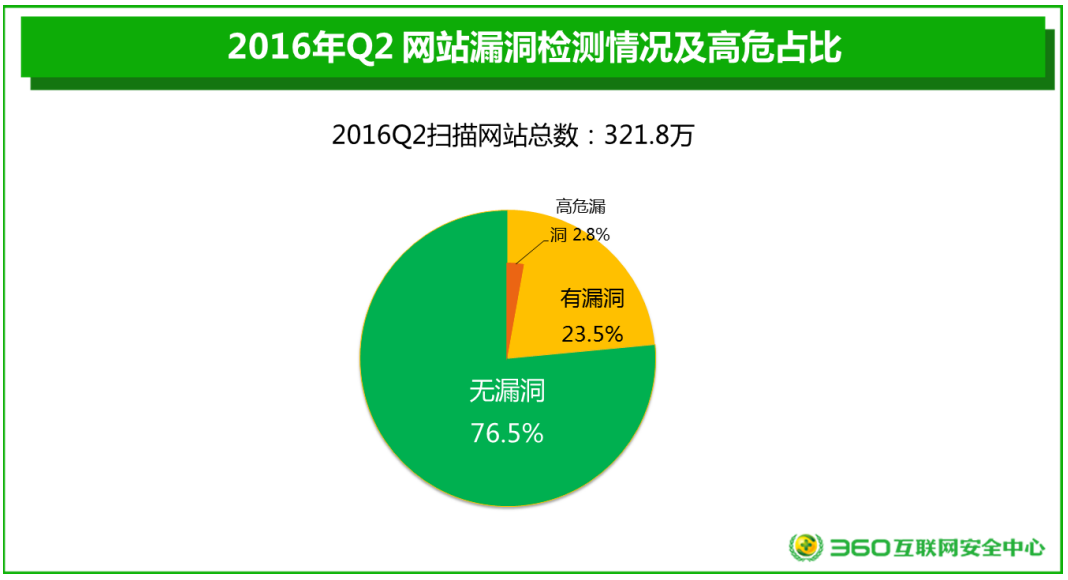


第六章 网站安全

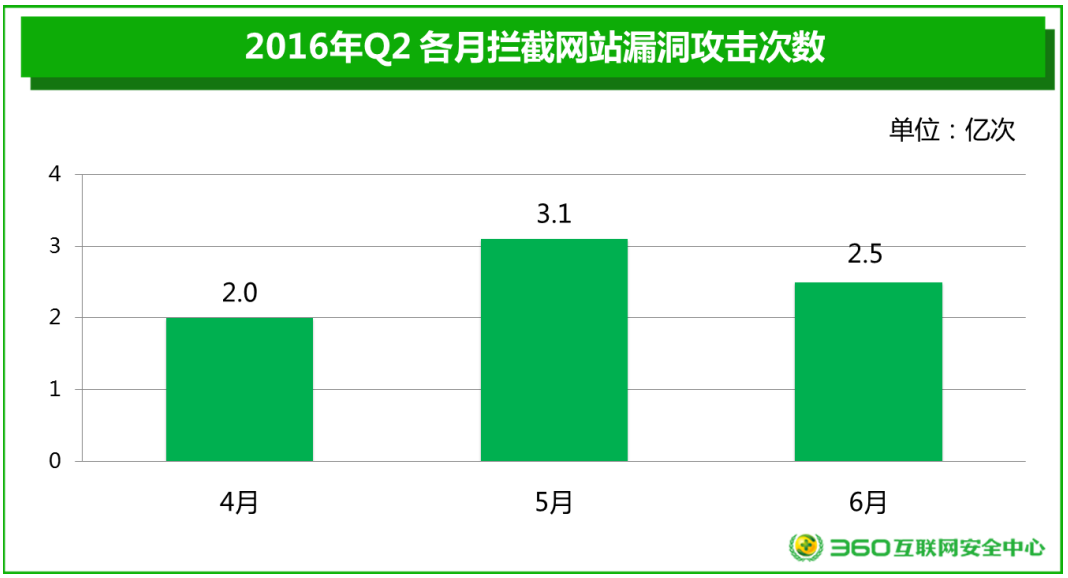
一、漏洞检测与攻击

2016 年第二季度，360 网站安全检测平台共扫描各类网站 321.8 万个，其中，存在安全漏洞的网站为 63.8 万个，占扫描网站总数的 23.5%。其中，存在高危安全漏洞的网站共有 9.3 万个，占扫描网站总数的 2.8%，同比 2015 年第二季度（21.9 万个）下降 57.5%。

下图给出了 2016 年第二季度存在安全漏洞网站比例情况。



2016 年第二季度，360 网站卫士共拦截各类网站漏洞攻击 7.7 亿次，其中 5 月的拦截量为 3.1 亿次，是第二季度拦截量最高的月份，4 月为 2.0 亿次、6 月为 2.5 亿次。

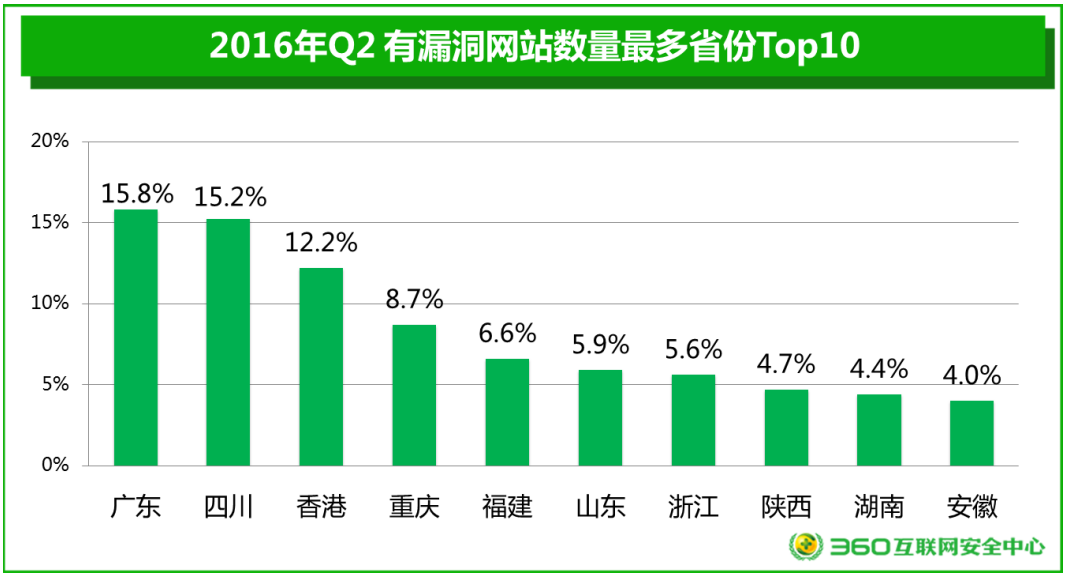


下表给出了扫出的数量排在前十位的漏洞类型。

排名	漏洞名称	危害程度	扫出次数（万）
1	页面异常导致本地路径泄漏	低危	75.0
2	跨站脚本攻击漏洞	中危	55.7
3	SQL 注入漏洞	高危	36.6
4	应用程序错误信息	低危	51.3
5	发现目录启用了自动目录列表功能	低危	19.8
6	IIS 短文件名泄露漏洞	低危	20.0
7	Mysql 可远程连接	低危	8.8
8	发现目录开启了可执行文件运行权限	低危	7.8
9	发现服务器启用了 TRACE Method	低危	7.0
10	Flash 配置不当漏洞	低危	4.2

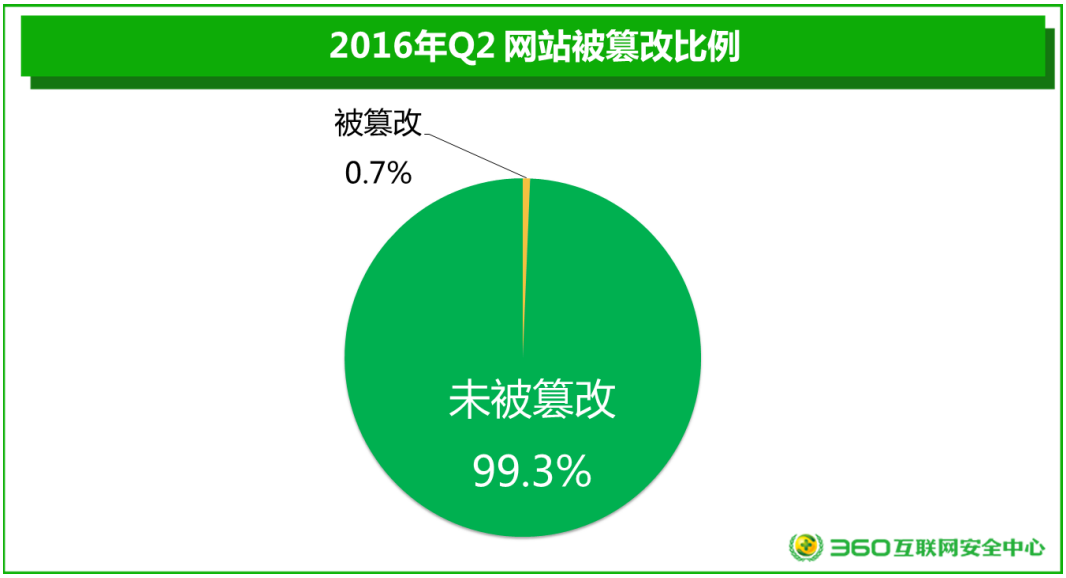
表 1　2016 年第二季度检出数量最多的漏洞类型

2016 年第二季度，从有漏洞网站的省级区域分布来看，广东是占比最高的地区，占比为 15.8%，其次是四川（15.2%）、香港（12.2%）、重庆（8.7%）和福建（6.6%）。前 5 名省区的总和占全国的 58.5%。

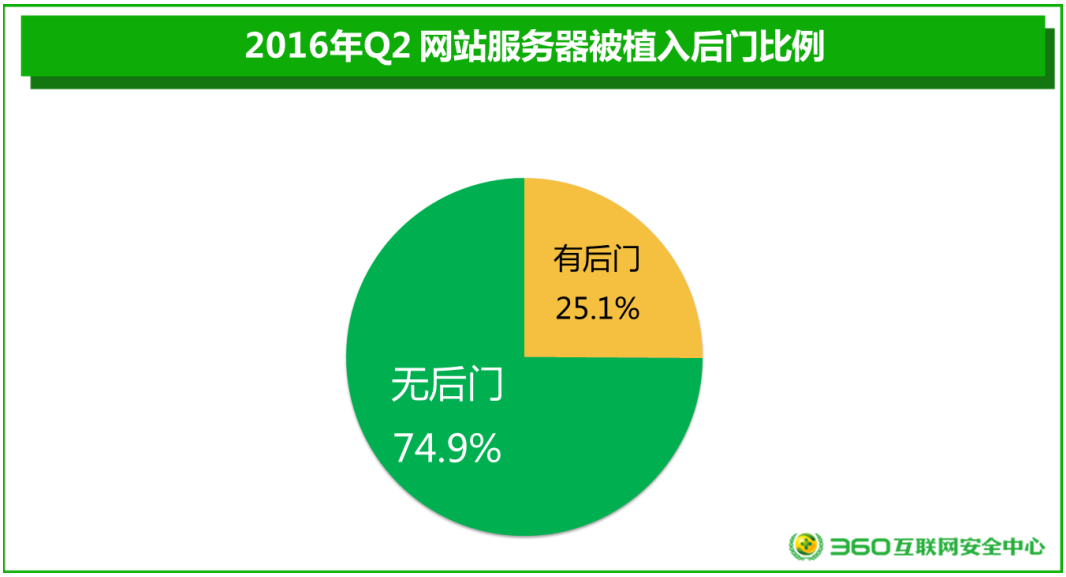


二、网页篡改与后门

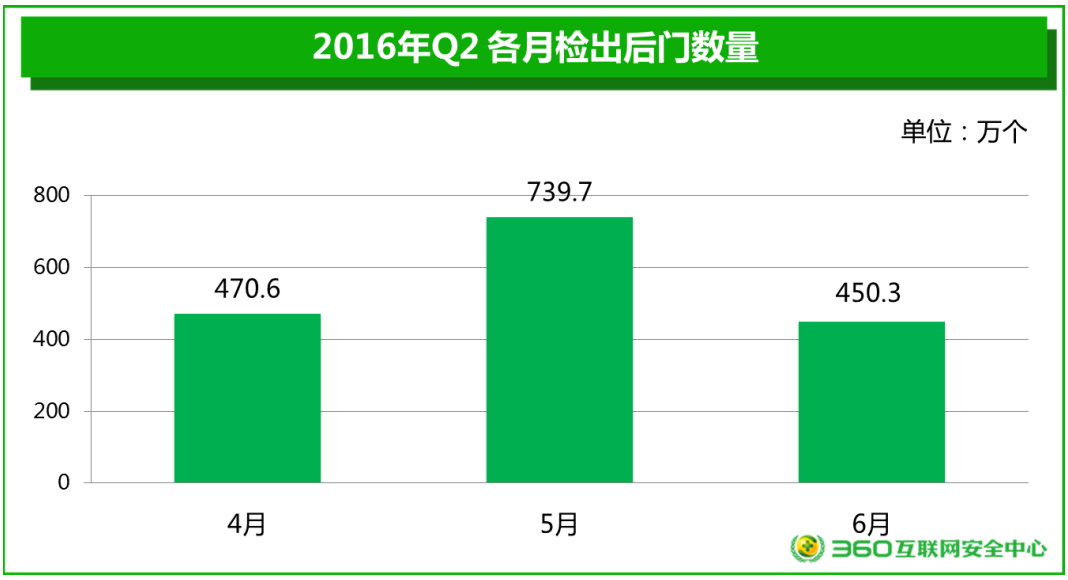
2016 年第二季度，360 网站安全检测平台共对 252.0 万个网站进行了篡改检测，其中，被篡改（不包括被植入后门程序）的网站 1.7 万个，约占扫描网站总数的 0.7%。同比，2015 年第二季度 4.4 万个，下降 61.6%



2016 年第二季度，360 网站安全检测对 3.2 万台网站服务器进行了网站后门检测，扫描发现约 25.1%的服务器存在后门。



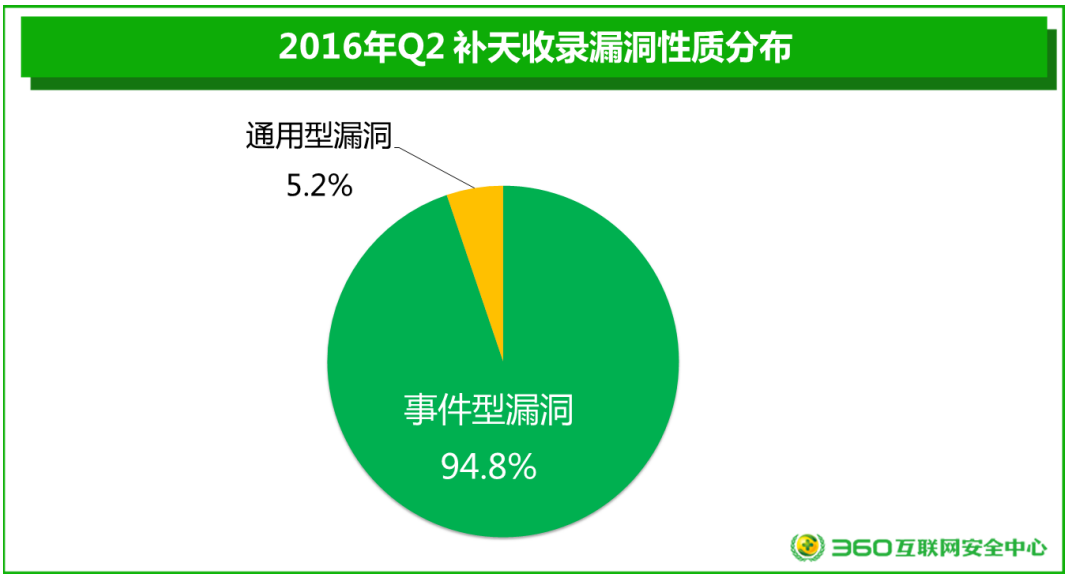
2016 年第二季度，360 网站安全检测的后门数量高达 1660.7 万个，平均每天检出后门数量 18.2 万个。各月检出后门数量见下图：4 月份检出后门 470.6 万个，5 月份检出后门 739.7 万个，6 月份检出后门 450.3 万个。



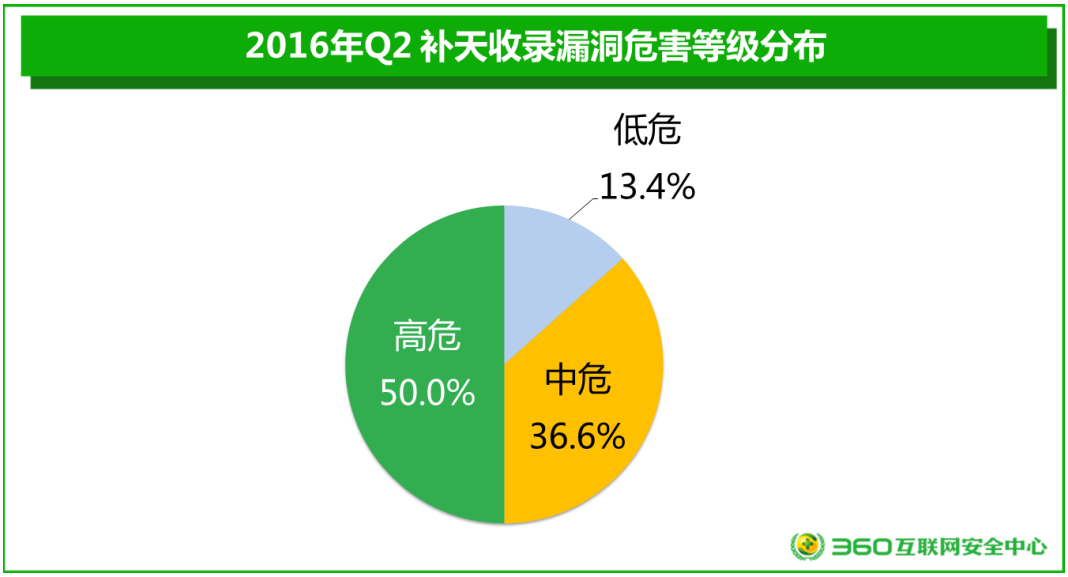
第七章 补天平台数据统计

一、 漏洞分析

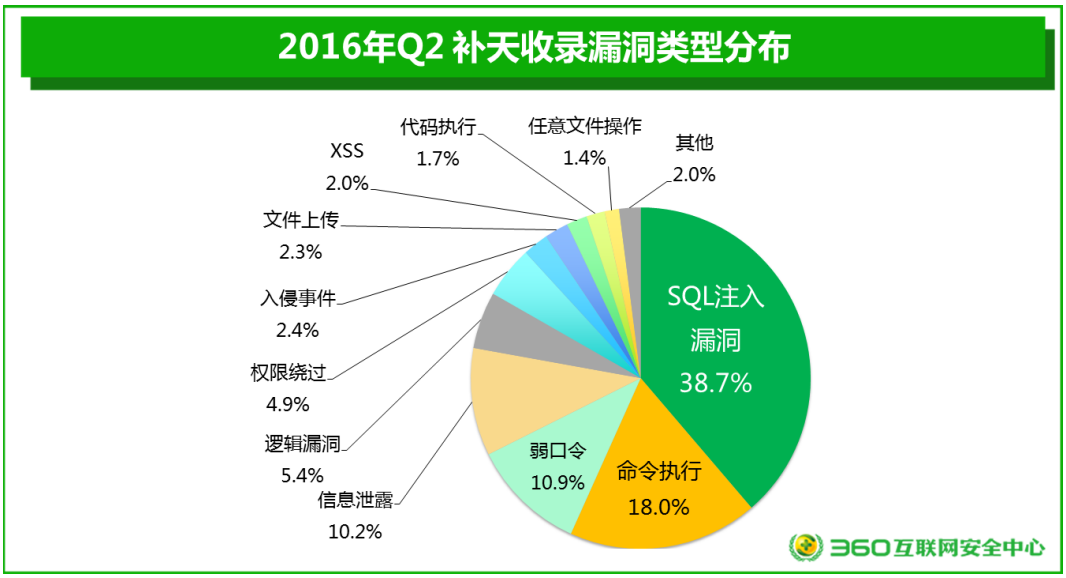
2016 年第二季度，补天平台共收录 1618 名“白帽子”提交的有效漏洞 10909 个，平均每天收录有效漏洞 120 个。其中通用型漏洞 571 个，占比为 5.25%，事件型漏洞则占 94.8%。下图给出了补天收录有效漏洞性质分布情况。



下图给出了补天平台新收录的 10909 个漏洞中，高危、中危和低危漏洞的比例分布。其中，高危漏洞的比例为 50.0%。



下图给出了补天平台新收录漏洞类型，其中 SQL 注入（38.7%）、命令执行（18.0%）、弱口令（10.9%）是最多的漏洞类型。



二、奖金发放

2016 年第二季度，补天平台共向 1618 名白帽子发布奖金 98.2 万元。

下表给出了 2016 年第二季度单笔奖金最高的三个漏洞的具体信息：

排名	0day 漏洞描述	白帽子网名	奖金金额
冠军	某保险平台系统高危漏洞，可致大量保单泄露	匿名	2000
冠军	某游戏平台内网漫游漏洞可致大量充值卡密码及游戏道具数据泄露	匿名	2000
季军	某电信运营商内网漫游漏洞可造成大量个人信息及通话记录息泄露	匿名	1500

表 2　2016 年第二季度补天平台发放奖金最高的三个漏洞

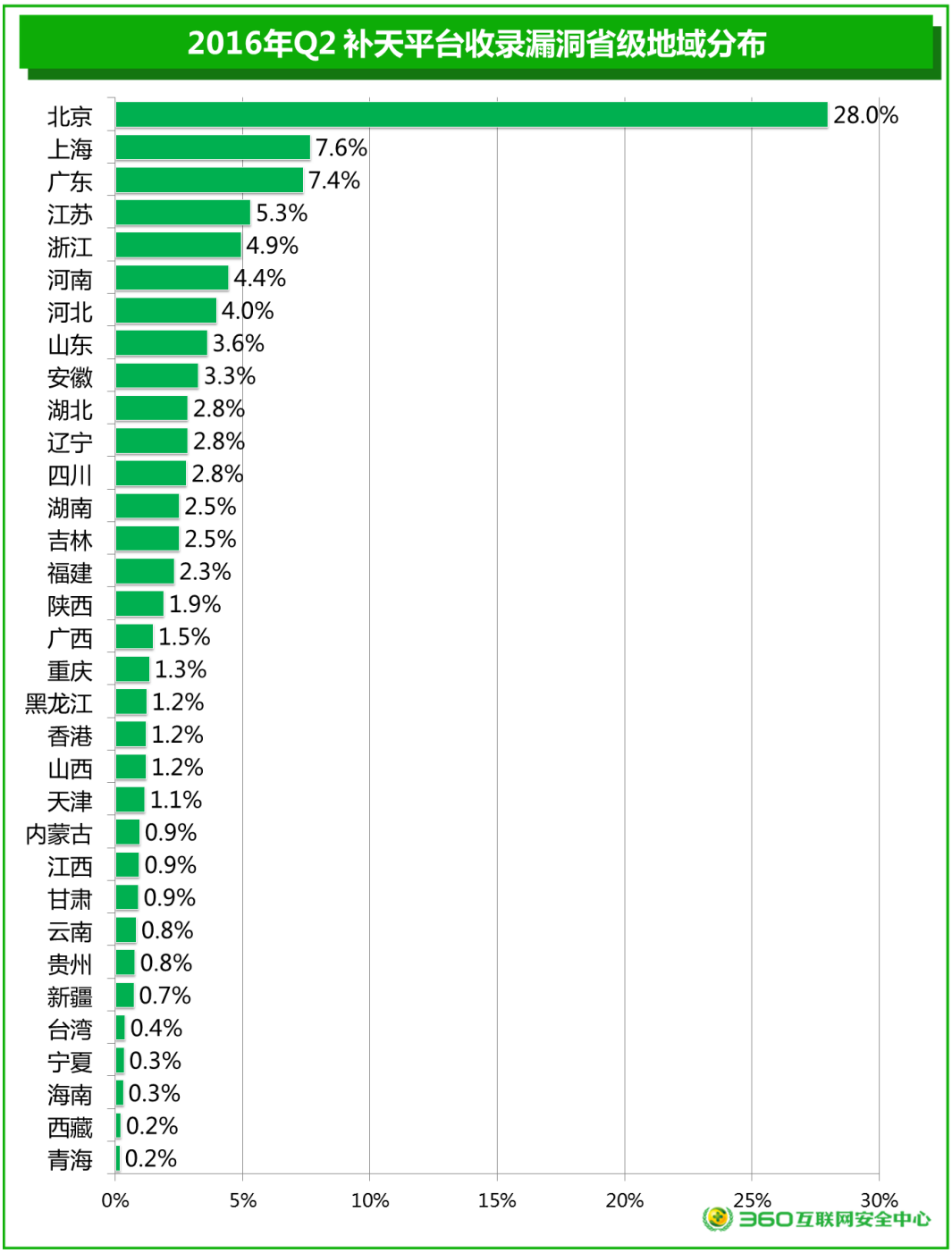
下表给出了 2016 年第二季度在补天平台获得奖金最多的三名白帽子的具体信息：

排名后	网名	报告 0day 漏洞个数	获奖金额
冠军	carry_your	302	144350
亚军	a0	164	54800
季军	system_gov	82	53600

表 3　2016 年第二季度补天平台获得奖金最多的三名白帽子

三、 网站漏洞地域分布

从地域分布看，2016 年第二季度补天平台收录漏洞的网站中，北京地区网站占 28.0%，上海地区网站 7.6%、广东地区网站 7.4%、江苏地区网站 5.3%、浙江地区网站 4.9%等地的网站漏洞最多，总和超过总量的 53.2%。



附录　2016 年第二季度热点网络安全事件

（一）　白帽报告世纪佳缘漏洞被抓事件

2015 年 12 月份，袁某在乌云提交发现的婚恋交友网站世纪佳缘的系统漏洞。在世纪佳缘确认漏洞，修复漏洞并按乌云平台惯例向漏洞提交者致谢后，事情突然发生转折。世纪佳缘在一个多月后以“网站数据被非法窃取”为由报警。2016 年 4 月份，袁某被司法机关逮捕。此后，袁某的父亲发出公开信为儿子鸣冤，让袁某的遭遇成为网络安全圈的热门事件。

（二）　孟加拉国中央银行曾遭多组黑客攻击

2016 年 4 月，黑客成功从孟加拉国央行在纽约联储的账户中转走 8100 多万美元。如果不是因为黑客拼错一个英文单词，该账户可能还会损失至少 8.5 亿美元。孟加拉国中央银行在美国纽约联储的账号失窃时，这家央行的服务器可能遭到多组黑客攻击。当时 3 组不同的黑客侵入孟加拉国央行的服务器。其中一组以偷钱为目的，另外两组似乎在搜集信息。

（三）　网络摄像头被曝近八成不合格-隐私泄露风险高

但是 2016 年 5 月初，360 攻防实验室发布了全国首份《国内智能家庭摄像头安全状况评估报告》。报告显示，国内市场上销售的近百个品牌的家庭智能摄像头，近八成产品存在泄露用户隐私风险。不法分子可以轻易控制摄像头，随时传输图像和语音信息，对安装摄像头的家庭或公司进行监控甚至做“网上直播”。

（四）　德国核电站检测出恶意程序被迫关闭

2016 年 4 月 24 日，德国 Gundremmingen 核电站的计算机系统，在常规安全检测中发现了恶意程序。此恶意程序是在核电站负责燃料装卸系统的 Block B IT 网络中发现的。

该恶意程序仅感染了计算机的 IT 系统，而没有涉及到与核燃料交互的 ICS/SCADA 设备。核电站表示，此设施的角色是装载和卸下核电站 Block B 的核燃料，随后将旧燃料转至存储池。

该 IT 系统并未连接至互联网，所以专家分析应该是有人通过 USB 驱动设备意外将恶意程序带进来的，可能是从家中，或者核电站内的计算机中。

（五）　全球银行业使用的恐怖嫌疑人数据库被泄露

2016 年 6 月初，一个包含约 220 万条恐怖分子与“高风险个人及实体”记录的数据库被泄露在互联网上。研究人员 Chris Vickery 在 Reddit 上称他成功获取到了一份 2014 版的 World-Check 的机密数据库，银行、政府及情报机构使用该数据库进行全球范围的风险扫描，数据库信息包括了恐怖分子嫌疑人。

（六）　BadTunnel：影响 Win95 到 Win10 的“超级漏洞”

2016 年 6 月，微软发布了一个高危漏洞的补丁，将其命名为“BadTunnel”，是目前 Windows 历史上影响最广泛的漏洞，从 Win95 到 Win10 都受影响。尤其对于微软已不支持的版本（如 Win XP），其用户将面临被秘密监控的危险。

该漏洞为原始设计问题。当用户打开一个 URL，或者打开任意一种 Office 文件、PDF 文件或者某些其他格式的文件，或者插上一个 U 盘——甚至不需要用户打开 U 盘里的任

何东西，攻击者都可以完成利用，其成功率极高。最终的结果是，攻击者可以劫持整个目标网络，获取权限提升。即使安全软件开启了主动防御机制，仍然无法检测到攻击。攻击者还可以利用该漏洞在目标系统中执行恶意代码。

（七） 揭秘 Patchwork APT 攻击

Patchwork APT 攻击是一个与东南亚和中国南海问题相关的 APT 攻击，该 APT 攻击目标是军事和政治机构，特别是那些与东南亚和南海问题相关的工作机构雇员，目标多是政府或与政府有间接联系的机构。Patchwork APT 自 2015 年 12 月被监测到之后，截止 2016 年 6 月底已经感染了大约 2500 台电脑。

经安全专家分析，该 APT 攻击所使用的全部工具代码都是通过复制-粘贴互联网公开代码组合而成，相对于其它 APT 特有的攻击工具而言，比较独特。其高度复杂的操作与其具有的低技术含量形成鲜明的矛盾对比，避免昂贵的开发工具而选择开源低廉的代码作为渗透工具，这也许是一种攻击趋势，也是一种避免被发现的手段。

（八） 台湾 ATM 机遭黑客攻击被窃取 7000 万

2016 年 7 月，台湾执法机构调查一起第一银行自动取款机被恶意攻击导致两百万美元失窃的案件。台湾当局确定的犯罪嫌疑人为两名戴口罩的俄罗斯人，他们被认定在周末攻击了几十个 ATM 取款机，根据当时的监控画面，黑客并没有使用 ATM skimmers(ATM 分离器)窃取银行卡数据，而是使用了恶意软件来控制 ATM 取款机达到吐钞目的。盗取钱款约 7000 万台币。当时正是台北被台风席卷之际，之后在周一他们便离开台北疑似逃往香港。