2016 年第三季度

中国互联网安全报告

360互联网安全中心

2016 年 11 月 9 日

摘　要

恶意程序

- 2016 年第三季度，360 互联网安全中心共截获 PC 端新增恶意程序样本 3707 万个，平均每天 40.3 万个，同比下降 64.4%；共为全国用户拦截恶意程序攻击 153.0 亿次，平均每天约 1.7 亿次，同比下降 44.7%。
- 2016 年第三季度，360 互联网安全中心共截获安卓平台新增恶意程序样本 349 万个，平均每天近 3.8 万个，同比下降 37.5%；累计监测到移动端用户感染恶意程序 5858 万人次，同比下降 24.1%，平均每天恶意程序感染量达到了 63.7 万人次。
- 2016 年第三季度，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（18.0%）、隐私窃取（3.8%）、流氓行为（2.8%）和远程控制（1.5%）。
- 2016 年第三季度，综合 PC 端和移动端的恶意程序拦截量，从省域分布来看，广东是占比最高的地方，占比为 13.1%，其次是江苏的 6.9%、山东的 6.6%、浙江的 6.5%和河南的 5.6%。
- 2016 年第三季度，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 4.8%，其次是上海的 3.4%、重庆的 2.8%、广州为 2.6%、深圳为 2.6%。

钓鱼网站

- 2016 年第三季度，360 互联网安全中心共截获各类新增钓鱼网站 56.6 万个，同比上升 37.8%；平均每天新增 6152 个，每小时涌现超过 256 个钓鱼网站。新增钓鱼网站中，境外彩票以 49.0%位居首位，虚假购物 5.9%、模仿登录 3.2%位列其后。
- 综合 PC 端和移动端的情况，共为全国用户拦截钓鱼攻击 53.7 亿次，同比下降 46.4%，平均每天拦截 5837.5 万次。其中 PC 端占总拦截量的 92.6%；移动端为 7.4%。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 6.2%、金融证券 4.0%。
- 从省域看，广东占比为 34.9%，福建 13.2%、广西 10.3%、湖南 7.0%、浙江 4.5%等，是钓鱼网站攻击次数排名前五的省份。拦截最多的城市为东莞 3.7 亿次，深圳 3.0 亿次、广州 2.6 亿次、南宁 2.1 亿次、泉州 1.8 亿次。
- 从新增钓鱼网站的服务器的地域分布来看，20.8%的钓鱼网站服务器位于国内，79.2%位于国外；其中国内的服务器位于香港的占比为 66.0%，其次是广东（15.7%）、北京（4.3%）、天津（2.1%）和河南（1.8%）。国外的服务器中，位于美国的最多，占比为 98.4%。
- 从钓鱼网站拦截量上看，21.2%的服务器来自国内，国外占 78.8%。在来自国内的攻击中，香港的占比为 22.2%，其次是江苏（18.0%）、浙江（15.9%）、福建（8.8%）、广东（7.6%）和北京（7.6%）。而在来自国外的攻击中，美国最多，占比为 55.4%，其次是加拿大（22.1%）、日本（4.4%）。

骚扰电话

- ✧ 2016 年第三季度，用户通过 360 手机卫士标记各类骚扰电话号码数量约 5533 万个，平均每天被用户标记的各类骚扰电话号码约 60 万个，同比下降 24.4%。
- ✧ 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 115.4 亿次，平均每天识别和拦截骚扰电话 1.3 亿次，同比大幅上升 57.2%。
- ✧ 从标记量来看，“响一声”占 51.1%；其次为诈骗电话（9.3%）、广告推销（8.9%）、房产中介（3.0%）、保险理财（2.5%）。
- ✧ 从骚扰电话识别和拦截量来看，广告推销以 15.9%位居首位，其次为诈骗电话 13.3%、响一声（5.3%）、房产中介（4.0%）、保险理财（1.6%）。
- ✧ 从地域看，广东省被拦截次数最多，占到了拦截次数总量的 20.8%，其次是北京 13.6%、上海 11.5%、江苏 7.7%、福建 6.3%。拦截最多的十个城市则分别是：北京、上海、广州、深圳、合肥、苏州、厦门、成都、郑州和杭州。

垃圾短信

- ✧ 2016 年第三季度，360 手机卫士共为全国用户拦截各类垃圾短信约 39.5 亿条，同比下降 43.2%；平均每天拦截垃圾短信 4290 万条。
- ✧ 从类型看，垃圾短信中广告推销最多，占比为 96.9%，其次是违法信息（2.0%）和诈骗短信（1.1%）。对诈骗短信作进一步分类，其中冒充电商、冒充银行类诈骗短信占比最高，分别为 47.5%和 25.1%，其次是冒充电信运营商 10.6%、冒充综艺节目 9.5%以及兼职诈骗 6.1%。
- ✧ 广东地区用户接到的垃圾短信数量最多，在全国各省市拦截量中占比为 15.8%；其次为山东（8.1%）、河南（7.3%）、北京（6.9%）、江苏（5.9%）。
- ✧ 从城市看，北京的垃圾短信拦截量依然最多，达 1.7 亿条，居于全国首位；其次是广州、郑州、上海、深圳、重庆、西安、南京、成都和石家庄。

网络诈骗

- ✧ 2016 年第三季度，猎网平台共接到来自全国各地的网络诈骗举报 4947 起，涉案总金额高达 4544.9 万元，人均损失 9187 元。其中，PC 用户举报 3694 例，人均损失 11259 元；手机用户举报 1253 例，人均损失约为 3534 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 1224 例，占比 24.7%；其次是网游交易 749 例（15.1%）、虚假购物 598 例（12.1%）、虚拟商品 486 例（9.8%）和金融理财 419 例（8.5%）。
- ✧ 从涉案总金额来看，金融理财类诈骗总金额最高，达 1730.7 万元，占比为 38.1%；其次是赌博博彩诈骗，涉案总金额 724.1 万元，占比 15.9%；虚假兼职诈骗排第三，涉案总金额为 535.5 万元，占比 11.8%。
- ✧ 从各省网络诈骗受害者用户举报情况来看，广东（564 起）、山东（321 起）、江苏（297

起）、辽宁（272 起）、四川（271 起），这 5 个地区用户的举报数量最多，约占了全国用户举报总量的 34.9%。从各城市的举报量来看，沈阳以 176 起位居榜首，其次为北京、上海、深圳、广州。

网站安全

- ✧ 2016 年第三季度，360 网站安全检测平台共扫描各类网站 111.1 万个，其中，存在安全漏洞的网站为 46.3 万个，占扫描网站总数的 41.6%。其中，存在高危安全漏洞的网站共有 4.4 万个，占扫描网站总数的 4.0%，同比 2015 年第三季度（14.2 万个）下降 69.0%。
- ✧ 2016 年第三季度，从有漏洞网站的省级区域分布来看，香港是占比最高的地区，占比为 18.4%，其次是北京（16.9%）、河南（9.5%）、浙江（9.2%）和上海（7.8%）。
- ✧ 2016 年第三季度，360 网站安全检测平台共对 391.3 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 2.5 万个，约占扫描网站总数的 0.6%。
- ✧ 2016 年第三季度，360 网站安全检测对 1.8 万次服务器进行了网站后门检测，扫描发现约 24.4%的网站服务器存在后门。
- ✧ 2016 年第三季度，360 网站安全检测的后门数量高达 1601.1 万个，平均每天检出后门数量 17.4 万个。

补天

- ✧ 2016 年第三季度，补天平台共收录 1226 名“白帽子”提交的有效漏洞 13749 个，平均每天收录有效漏洞 149 个。其中通用型漏洞 800 个，占比为 5.8%，事件型漏洞则占 94.2%。
- ✧ 2016 年第三季度补天平台新收录漏洞中，SQL 注入（47.8%）、信息泄露（11.2%）、弱口令（10.9%）是最多的漏洞类型。
- ✧ 从地域分布看，2016 年第三季度补天收录的漏洞中，北京地区网站占 22.5%，广东 8.7%、浙江 6.6%、上海 6.4%、山东 6.3%，上述 Top5 省区所占比例总和超过 50.5%。

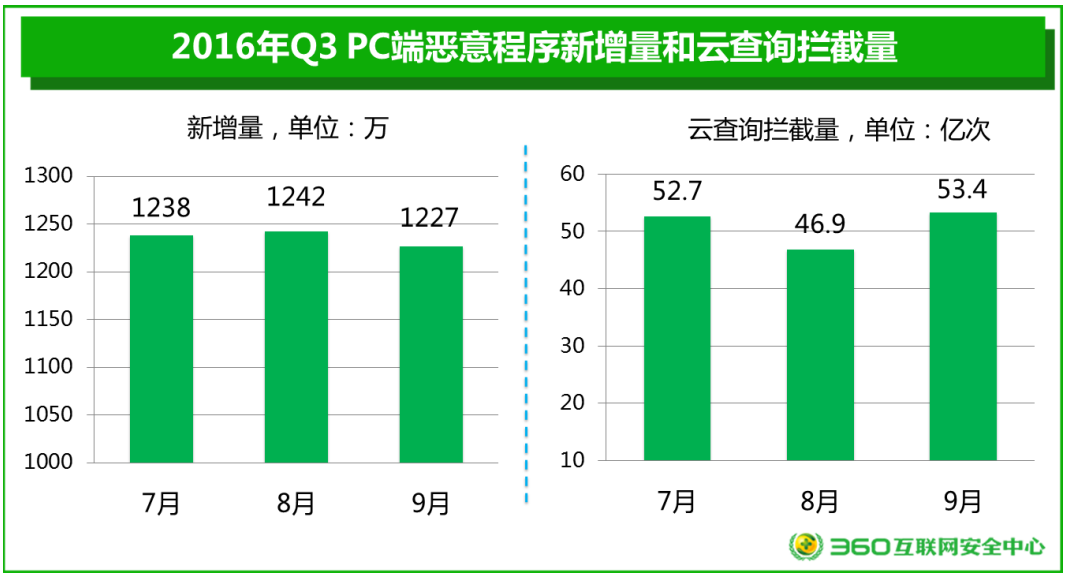
关键词：恶意程序、钓鱼网站、网络诈骗、网站安全、补天平台、白帽子

目　　录

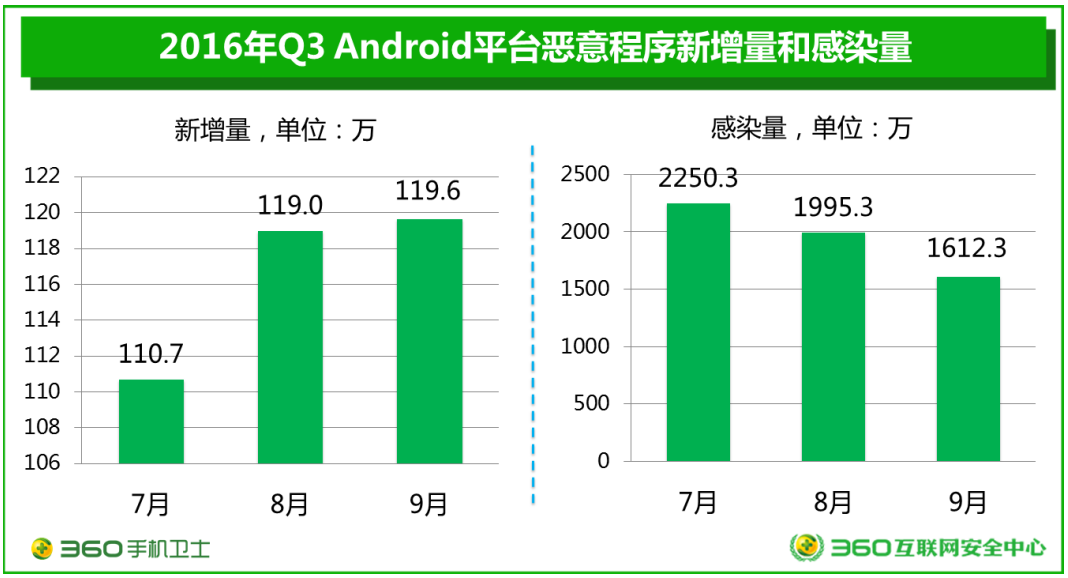
第一章 恶意程序

一、 新增量与拦截量

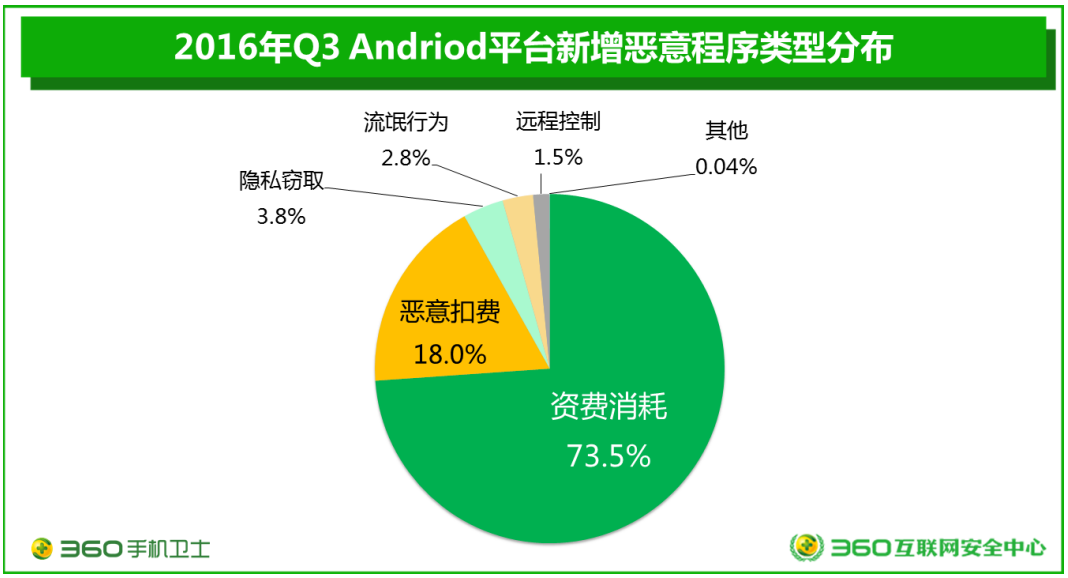
2016 年第三季度，360 互联网安全中心共截获 PC 端新增恶意程序样本 3707 万个，同比 2015 年第三季度（1.04 亿个）下降 64.4%，环比（5863 万）下降 36.8%，平均每天截获新增恶意程序样本 40.3 万个。从拦截量看，Q3 拦截恶意程序攻击 153.0 亿次，环比（167.1 亿次）下降 8.5%，同比（276.6 亿次）下降 44.7%，平均每天为用户拦截意程序攻击约 1.7 亿次。具体见下图。



2016 年第三季度，360 互联网安全中心共截获安卓平台新增恶意程序样本 349 万个，比 2015 年第三季度（558 万个）减少了 209 万个，平均每天截获新增手机恶意程序样本近 3.8 万个。累计监测到移动端用户感染恶意程序 5858 万人次，同比 2015 年第二季度（7722 万次）下降 1864 万人次，平均每天恶意程序感染量达到了 63.7 万人次。

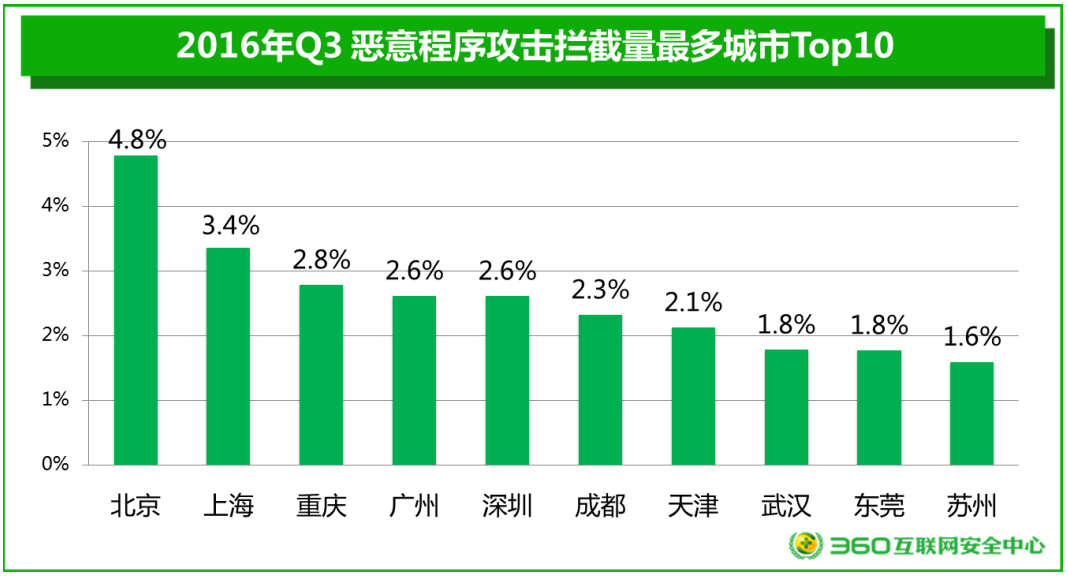


2016 年第三季度安卓平台新增恶意程序主要是资费消耗，占比高达 73.5%；其次为恶意扣费（18.0%）、隐私窃取（3.8%）、流氓行为（2.8%）和远程控制（1.5%）。

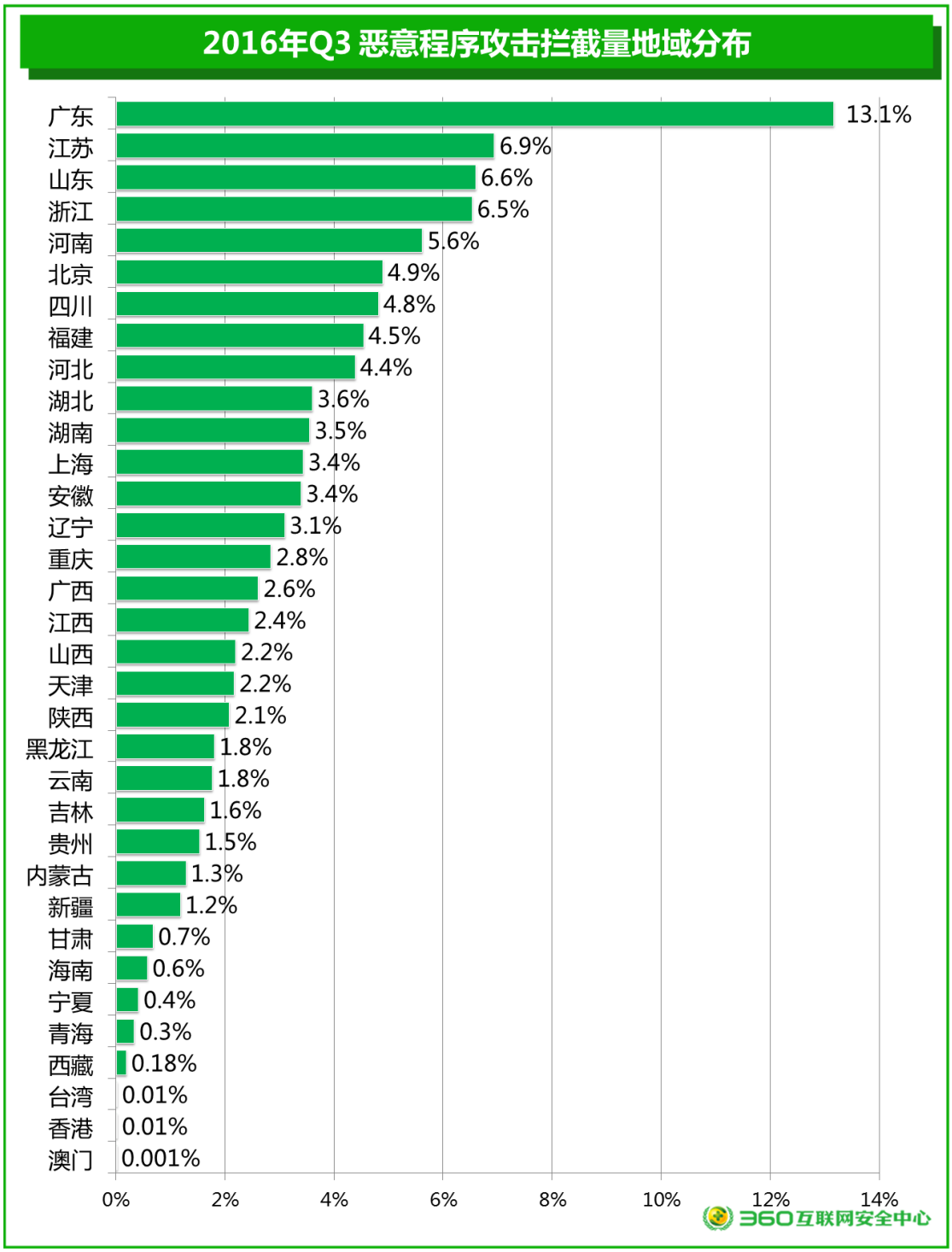


二、地域分布

2016 年第三季度，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 4.8%，其次是上海的 3.4%、重庆的 2.8%、广州为 2.6%、深圳为 2.6%、成都的 2.3%、天津的 2.1%、武汉为 1.8%、东莞为 1.8%和苏州为 1.6%。



2016 年第三季度，综合 PC 端和移动端的恶意程序拦截量，从地域分布来看，广东是占比最高的地方，占比为 13.1%，其次是江苏的 6.9%、山东的 6.6%、浙江的 6.5%和河南的 5.6%。



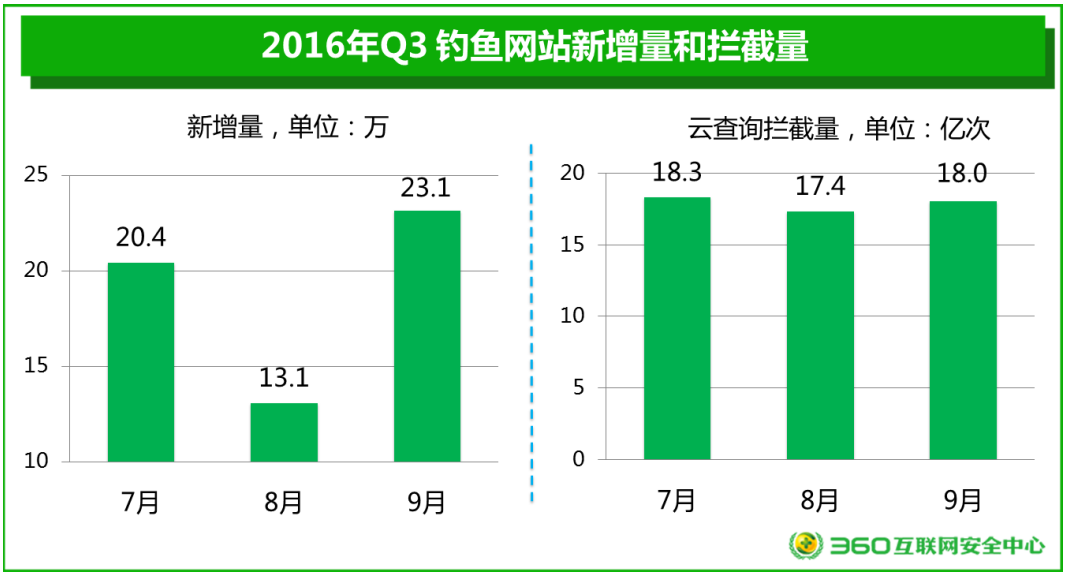
第二章 钓鱼网站

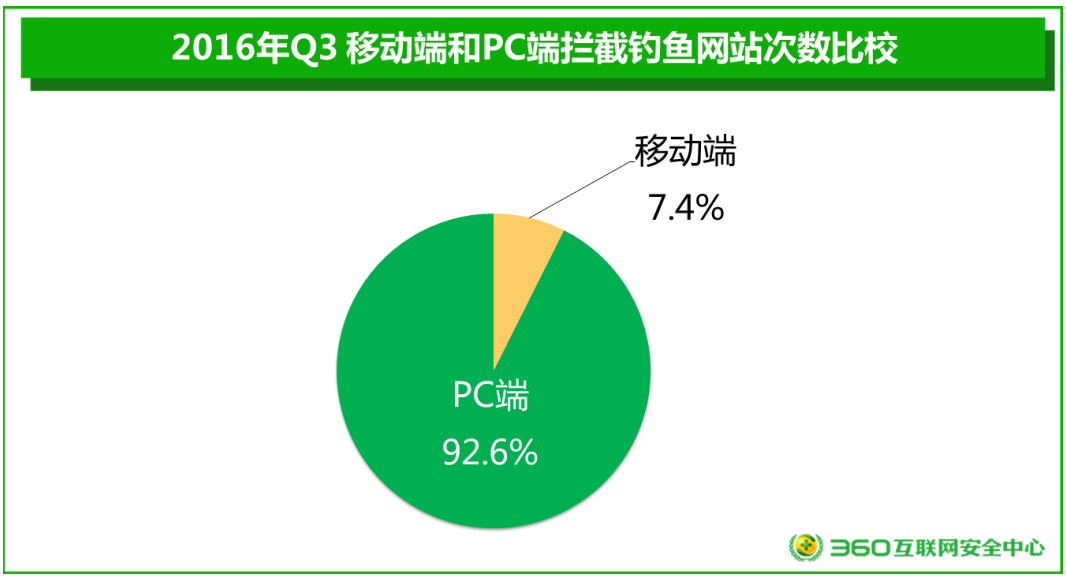
一、 新增量和拦截量

2016 年第三季度，360 互联网安全中心共截获各类新增钓鱼网站 56.6 万个，同比 2015 年第三季度（35.2 万个）上升 37.8%；平均每天新增 6152 个，每小时涌现超过 256 个钓鱼网站。

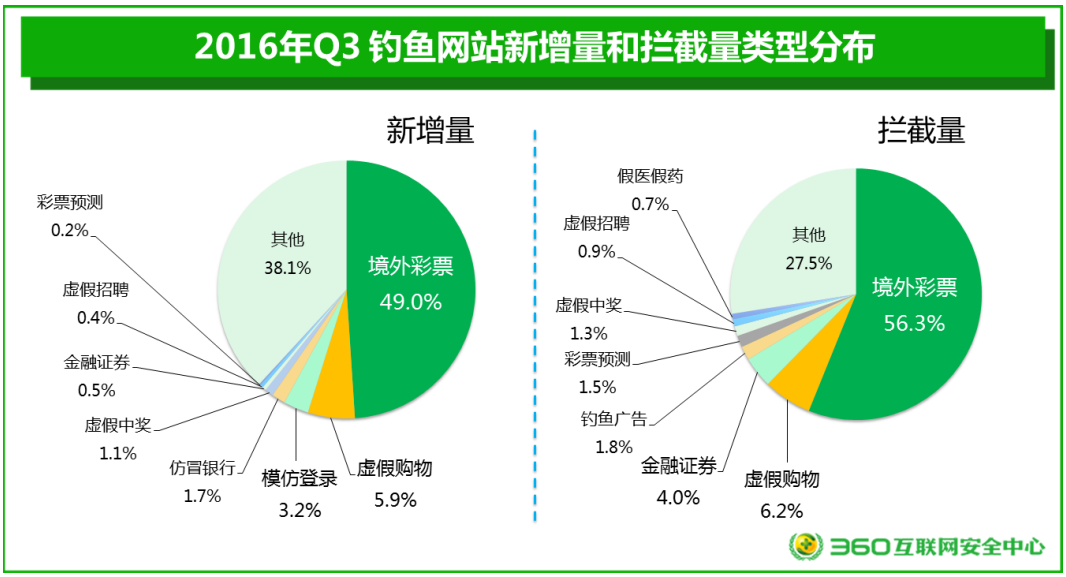
2016 年第三季度，360 的 PC 端和手机安全软件共为全国用户拦截钓鱼攻击 53.7 亿次，同比 2015 年第三季度（100.2 亿次）下降 46.4%，平均每天拦截 5837.5 万次。其中 PC 端拦截量为 49.8 亿次，占总拦截量的 92.6%；移动端为 3.9 亿次，占总拦截量的 7.4%。

下图给出了整体的钓鱼网站新增量和拦截量，及移动和 PC 拦截量份额对比。

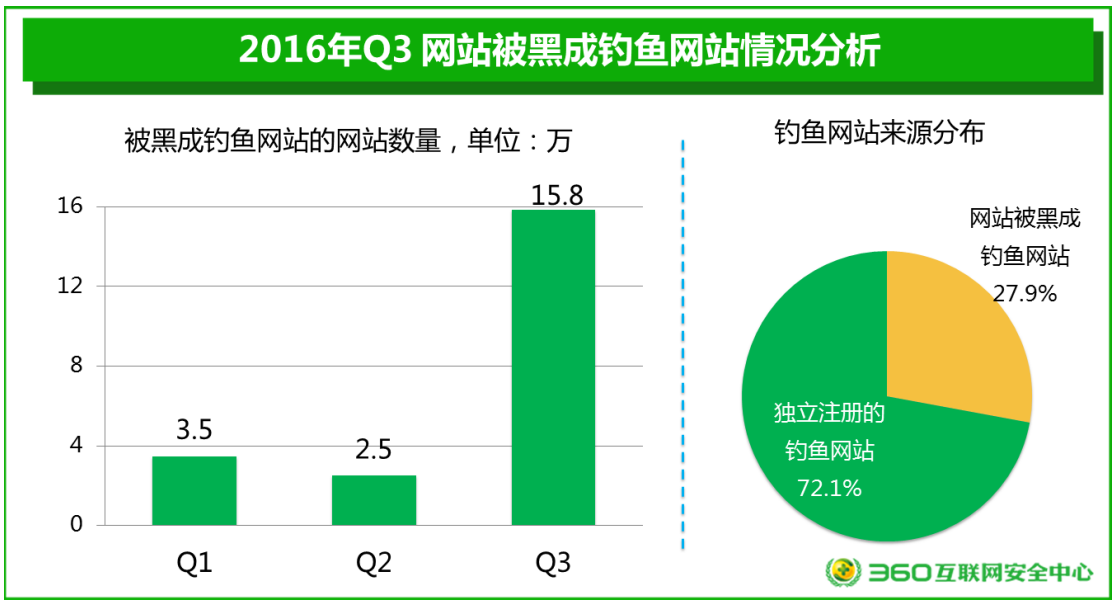




在新增钓鱼网站中，境外彩票以 49.0%位居首位，虚假购物 5.9%、模仿登录 3.2%位列其后。钓鱼网站的拦截量方面，境外彩票占到了 56.3%，排名第一，其次是虚假购物 6.2%、金融证券 4.0%。

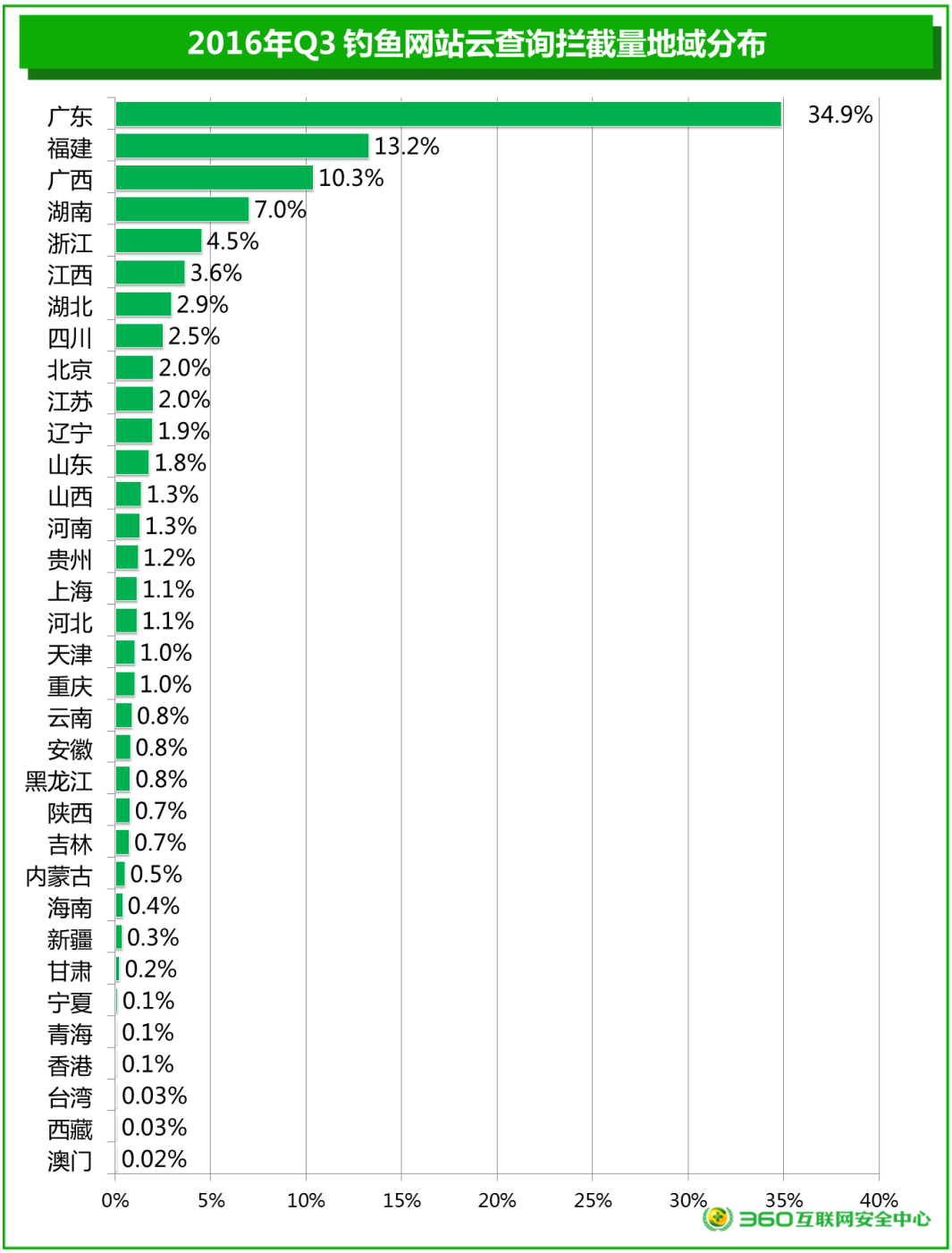


另据 360 互联网安全中心监测，2016 年以来，网站被黑并被篡改为钓鱼网站的情况日益严重。相比一季度 3.5 万、二季度 2.5 万个网站被黑成了钓鱼网站，三季度数量达到 15.8 万，占新增钓鱼网站总量的 27.9%，比二季度增加了 8.7 个百分点。攻击者之所以会使用被黑网站作为钓鱼网站，主要目的就是为了躲避安全软件的监控与拦截。同时，网站被黑也表明网站存在着明显的没有修复的安全漏洞。

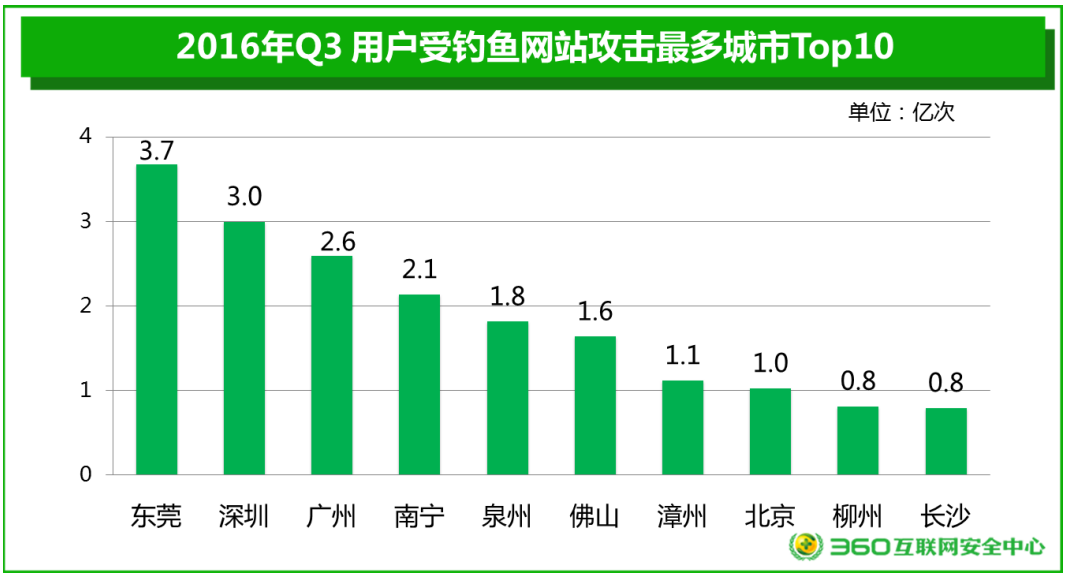


二、 拦截量地域分布

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 34.9%，福建占比 13.2%、广西占比 10.3%、湖南占比 7.0%、浙江占比 4.5%，钓鱼网站攻击次数排名前十的省份还有江西、湖北、四川、北京和江苏。

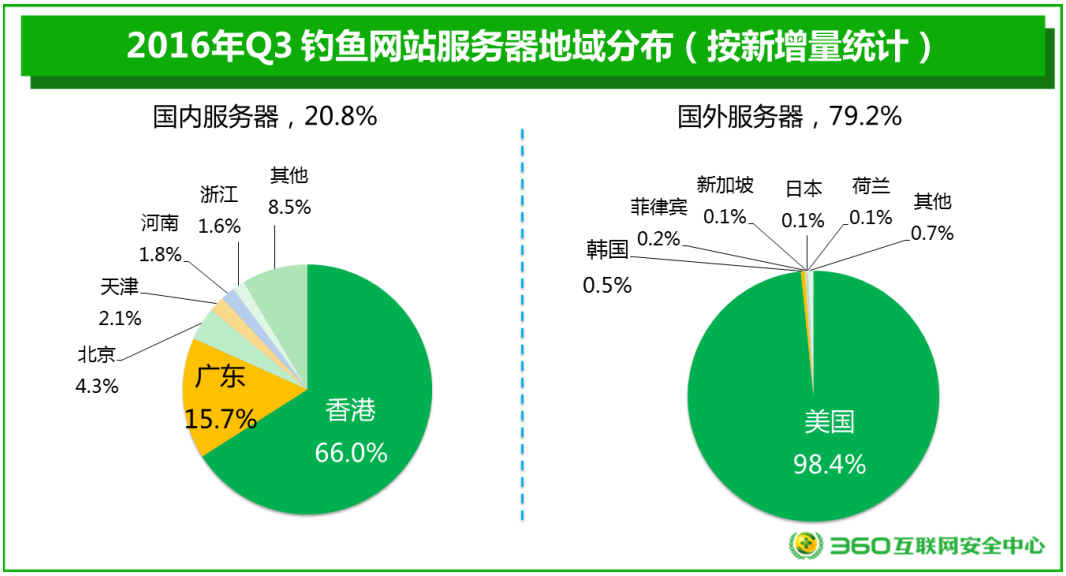


从各主要城市用户遭到钓鱼攻击的情况来看（综合 PC 端和移动端情况），排名前五的城市分别为东莞（3.7 亿次），深圳（3.0 亿次）、广州（2.6 亿次）、南宁（2.1 亿次）、泉州（1.8 亿次）。

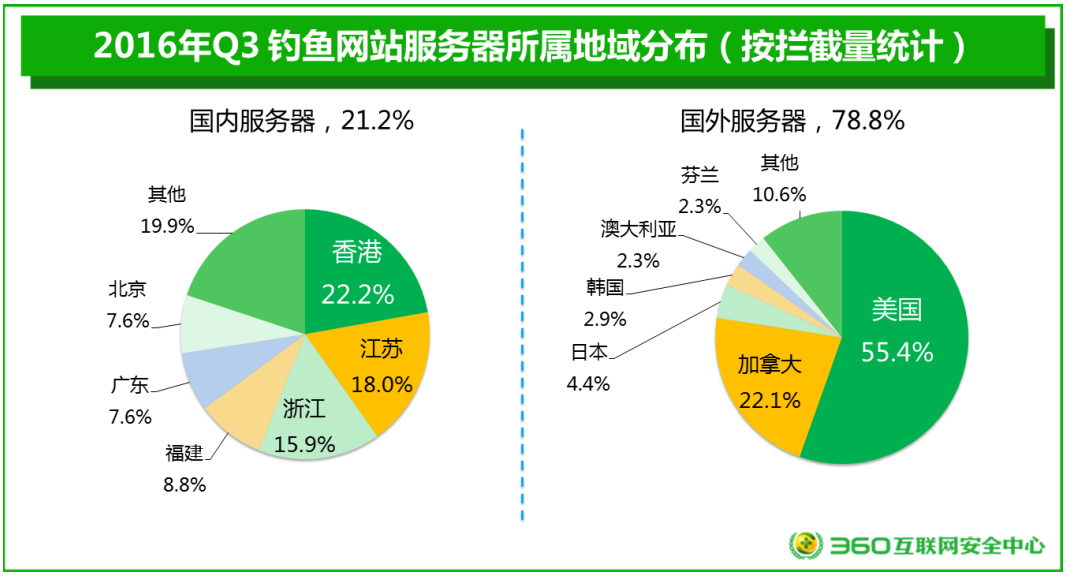


三、 服务器地域分布

从新增钓鱼网站的服务器的地域分布来看，20.8%的钓鱼网站服务器位于国内，79.2%位于国外。国外占比相较二季度增加 17.2 个百分点。其中国内的服务器位于香港的占比为 66.0%，其次是广东（15.7%）、北京（4.3%）、天津（2.1%）和河南（1.8%）。国外的服务器中，位于美国的最多，占比为 98.4%。



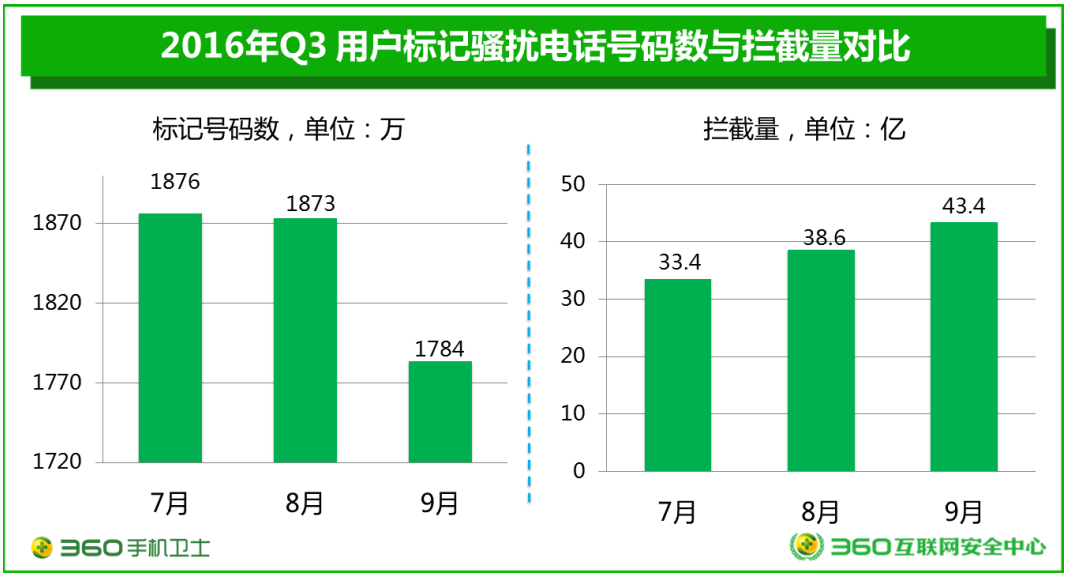
从钓鱼网站拦截量上看，21.2%的钓鱼网站攻击所属服务器来自国内，相较二季度下降56.6 个百分点，位于国外的服务器占 78.8%。在来自国内的攻击中，香港的占比为 22.2%，其次是江苏（18.0%）、浙江（15.9%）、福建（8.8%）、广东（7.6%）和北京（7.6%）。而在来自国外的攻击中，美国最多，占比为 55.4%，其次是加拿大（22.1%）、日本（4.4%）。总体而言，国外钓鱼网站的服务器地域分布集中度高。



第三章 骚扰电话

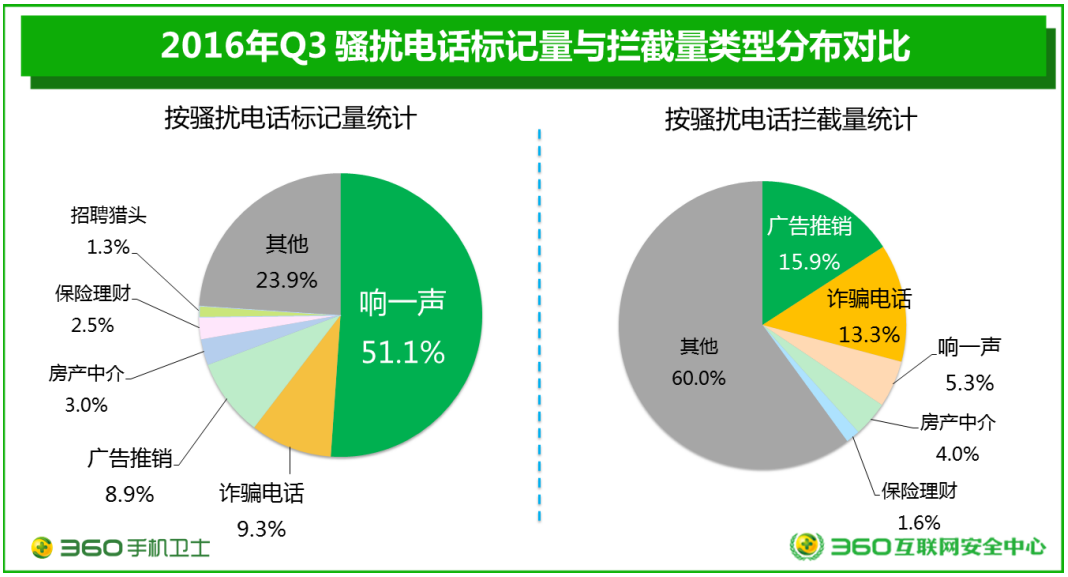
一、 骚扰电话数量

2016 年第三季度，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 5533 万个，平均每天约 60 万个。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 115.4 亿次，平均每天识别和拦截 1.3 亿次；总量较 2015 年第三季度 73.4 亿次大幅上升 57.2%。



二、 类型分析

从标记量来看，“响一声”占 51.1%；其次为诈骗电话（9.3%）、广告推销（8.9%）、房产中介（3.0%）、保险理财（2.5%）。从拦截量看，广告推销以 15.9%位居首位，其次为诈骗电话 13.3%、响一声（5.3%）、房产中介（4.0%）、保险理财（1.6%）以及其他骚扰（60.0%）。

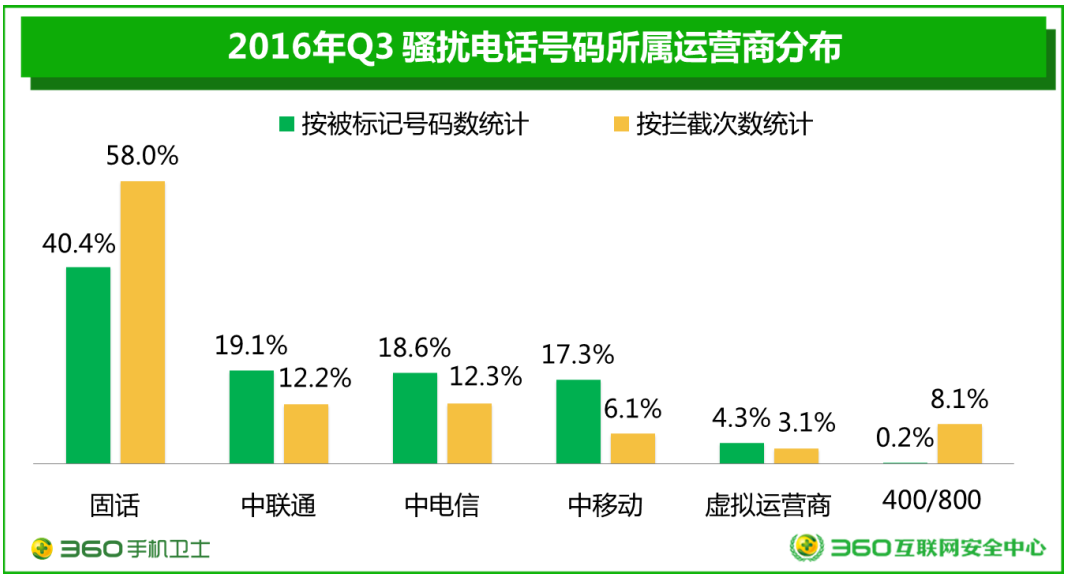


三、 骚扰号源归属运营商

从下图可以看出 2016 年第三季度，骚扰电话号码里面固定号码最多，占比 40.4%，同时被拦截次数最多的也是固话，比例超过一半，达到 58.0%。

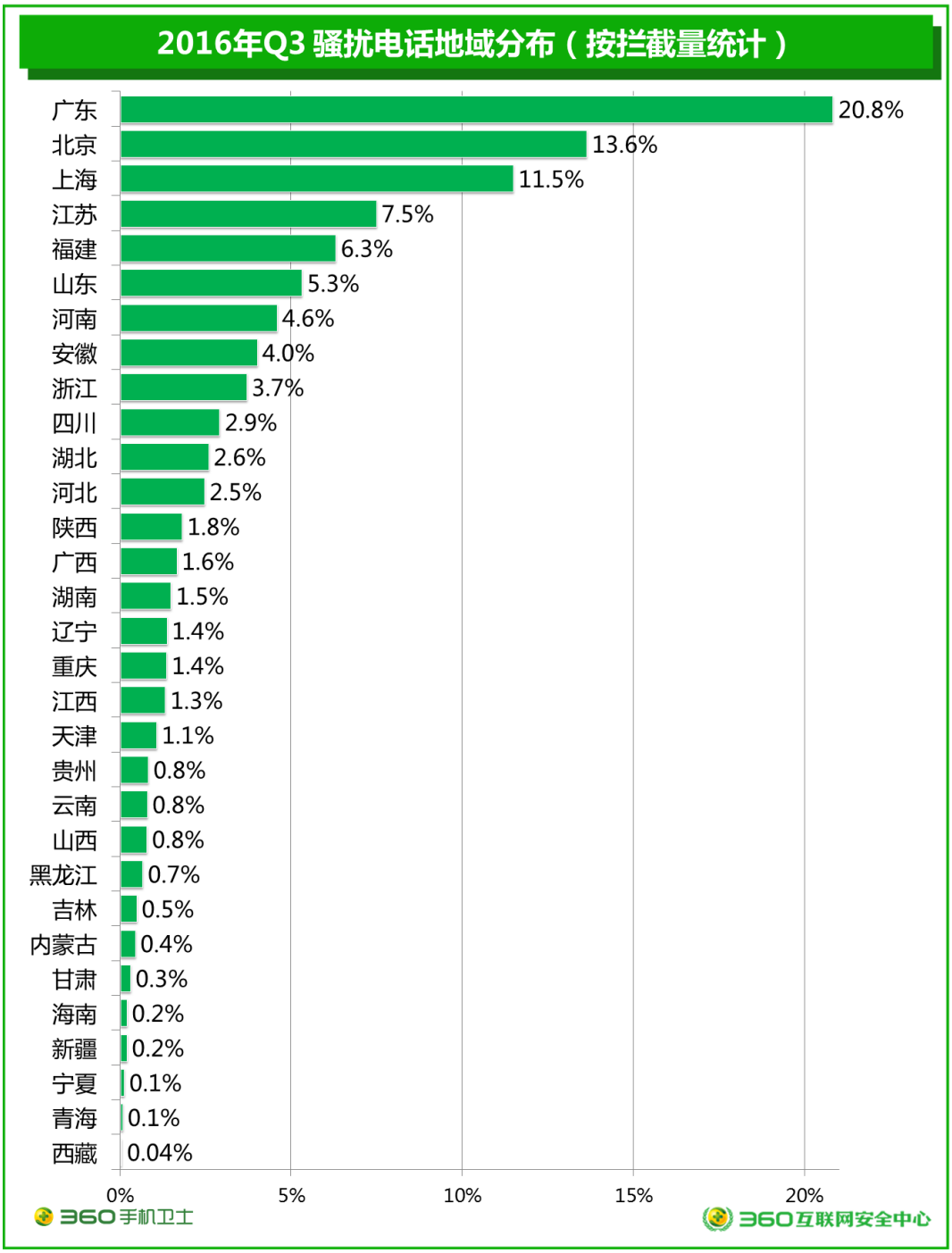
从虚拟运营商类型看，骚扰电话号码中号码比重达到 4.3%，比二季度高出 3.1 个百分点；拦截次数占比也达到 3.1%。

下图描述了按骚扰电话按号码统计和拦截量统计的归属运营商比例分布：



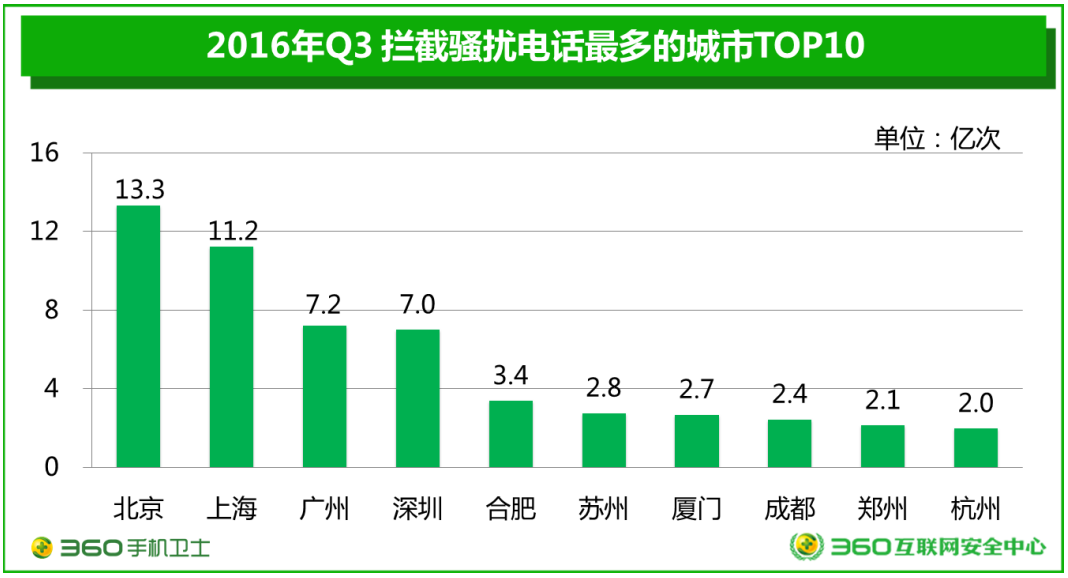
四、 地域分析

从 2016 年三季度骚扰电话的拦截量来看，广东省被拦截次数最多，占到了拦截次数总量的 20.8%，其次是北京 13.6%、上海 11.5%、江苏 7.7%、福建 6.3%。和 2016 年二季度的数据相比，前五名的省份位次丝毫未变。



从拦截骚扰电话次数看，最多的十个城市则分别是：北京（13.3 亿次）、上海（11.2 亿

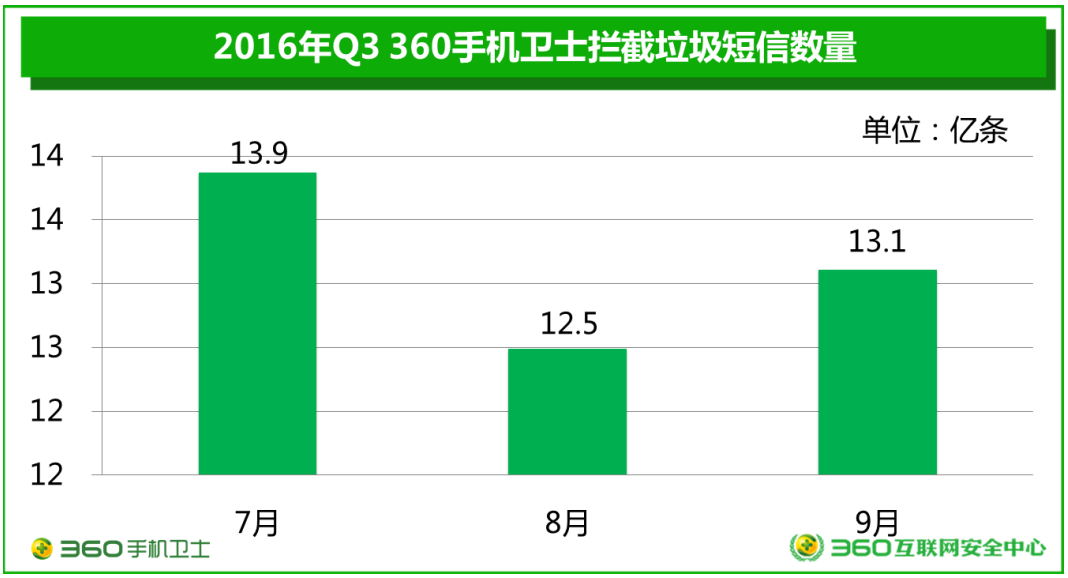
次）、广州（7.2 亿次）、深圳（7.0 亿次）、合肥、苏州、厦门、成都、郑州和杭州。前四名的城市被拦截的次数均达到或超过 7 亿人次。具体见下图：



第四章 垃圾短信

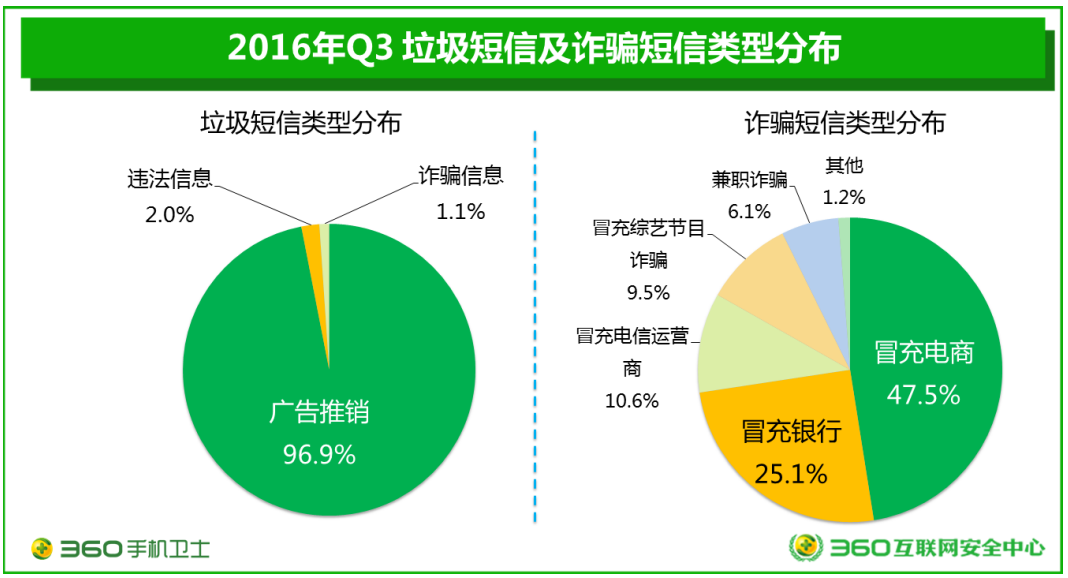
一、 垃圾短信数量

2016 年第三季度，360 手机卫士共为全国用户拦截各类垃圾短信约 39.5 亿条，较 2015 年第三季度的 69.5 亿条同比大幅下降了 43.2%，较 2016 年第二季度的 45.5 亿条环比下降了 13.2%；平均每天拦截垃圾短信 4290 万条。



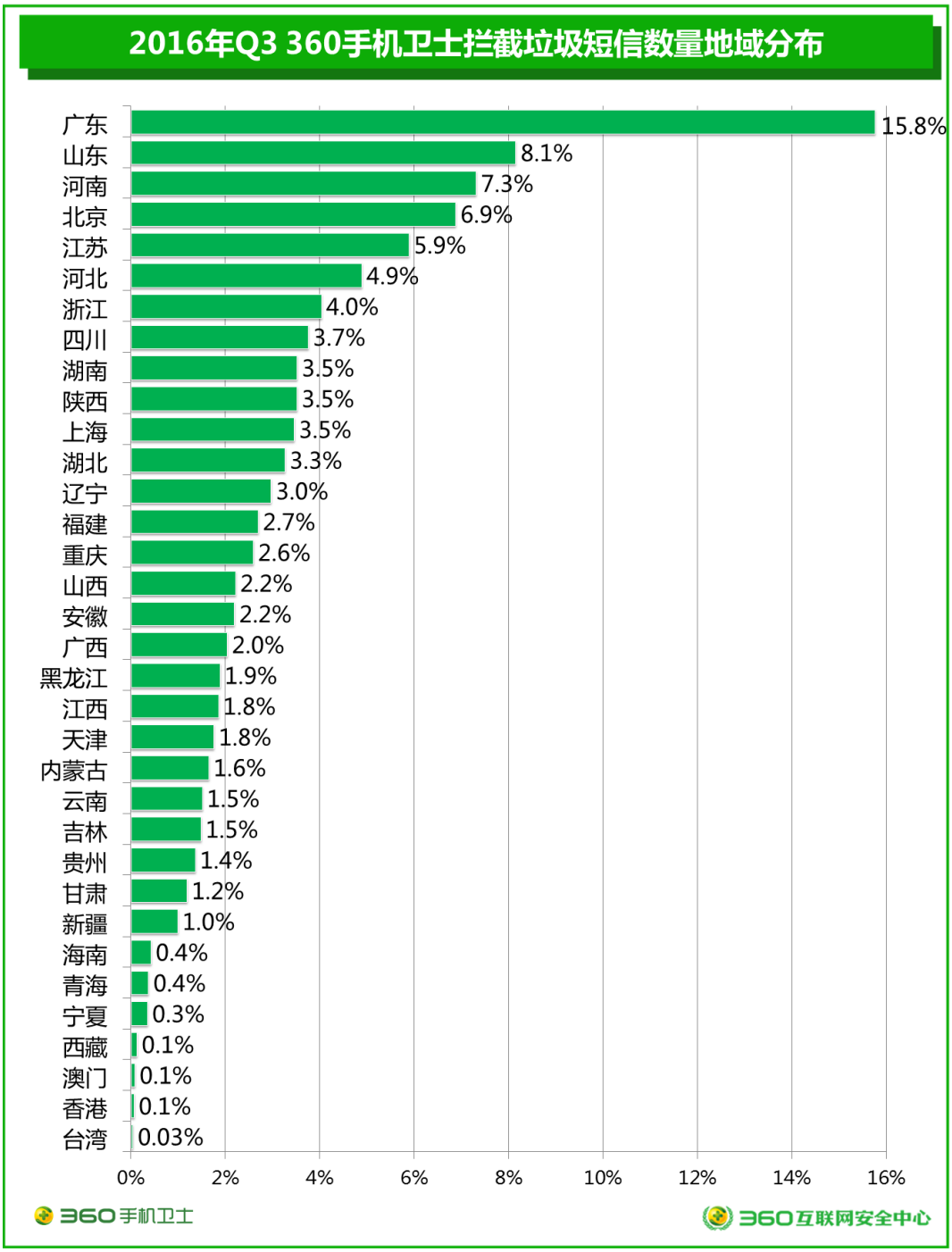
二、 类型分析

从类型分布看，垃圾短信中广告推销最多，占比为 96.9%，相比 2016 年第二季度的广告推销（79.6%）有所回升。其次是违法信息（2.0%）和诈骗短信（1.1%）。对诈骗短信作进一步分类，其中冒充电商、冒充银行类诈骗短信占比最高，分别为 47.5%和 25.1%，其次是冒充电信运营商 10.6%、冒充综艺节目 9.5%以及兼职诈骗 6.1%。

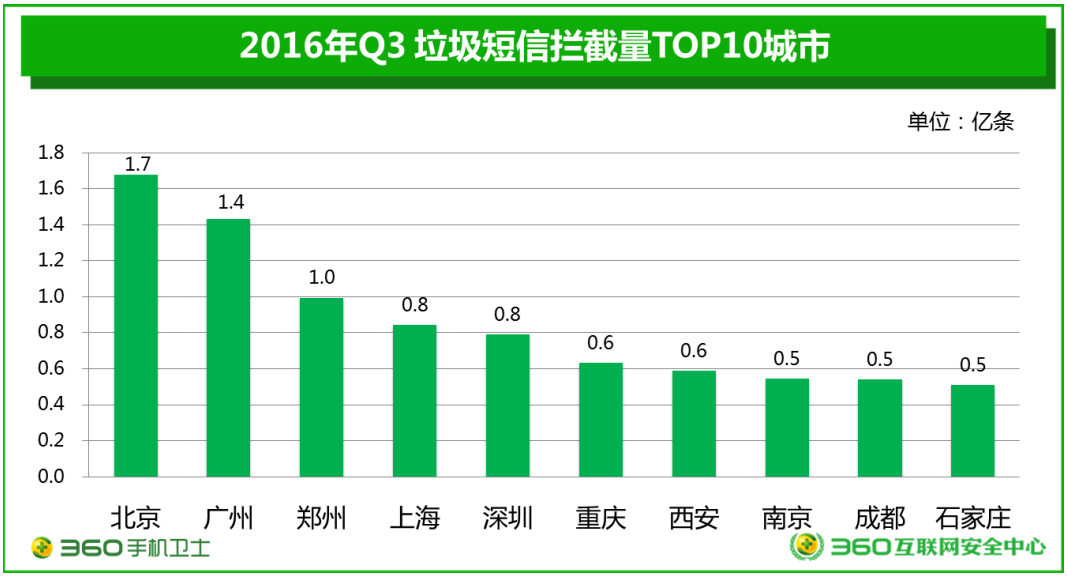


三、 地域分析

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，在全国各省市拦截量中占比为 15.8%；其次为山东（8.1%）、河南（7.3%）、北京（6.9%）、江苏（5.9%）。上述五省区在二季度也是垃圾短信 Top5，仅是座次有所调整。下图给出了三季度垃圾短信的地域分布：



下图给出了 2016 年第三季度 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依然最多，达 1.7 亿条，居于全国首位；其次是广州（1.4 亿条）、郑州（1.0 亿条）、上海（0.8 亿条）、深圳（0.8 亿条）、重庆（0.6 亿条）、西安（0.6 亿条）、南京（0.5 亿条）、成都（0.5 亿条）和石家庄（0.5 亿条）。

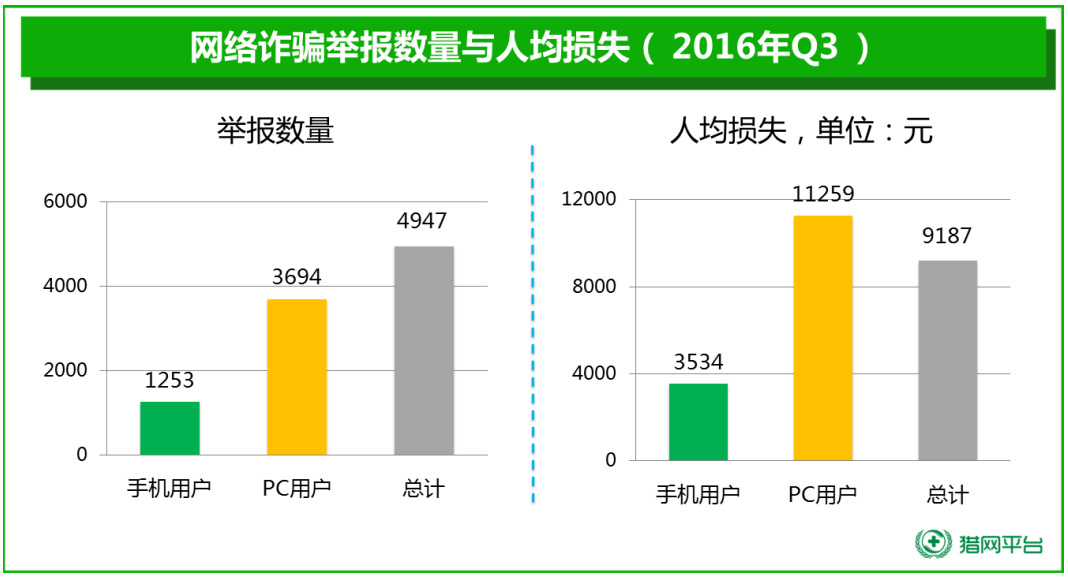


第五章 网络诈骗

一、 举报量与损失金额

2016 年第三季度，猎网平台共接到来自全国各地的网络诈骗举报 4947 起，涉案总金额高达 4544.9 万元，人均损失 9187 元。其中，PC 端用户举报 3694 例，人均损失 11259 元；手机端用户举报 1253 例，人均损失约为 3534 元。

人均损失方面，总体人均损失较 2016 年第二季度（8213 元）有上升趋势，PC 端用户人均损失相比 2016 年第二季度（10112 元）有上升趋势，手机端人均损失较 2016 年第二季度（4534 元）有下降趋势。



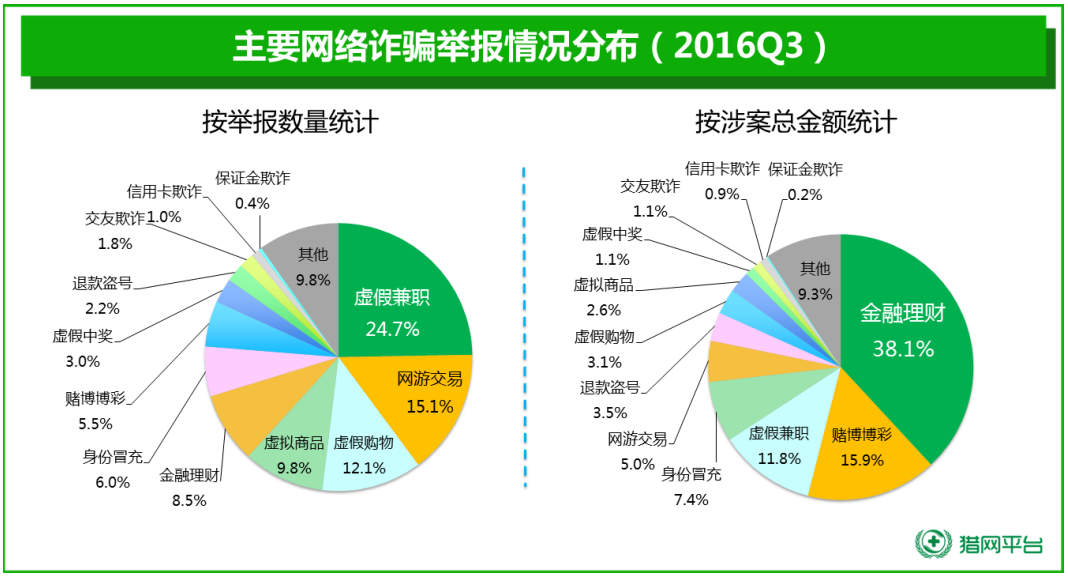
二、 类型分析

2016 年第三季度，从所有举报的诈骗案情来看，猎网平台共收到全国用户有效申请的网络诈骗举报 4947 例，虚假兼职诈骗依然是举报数量最多的类型，共举报 1224 例，占比 24.7%；其次是网游交易 749 例（15.1%）、虚假购物 598 例（12.1%）、虚拟商品 486 例（9.8%）和金融理财 419 例（8.5%）。

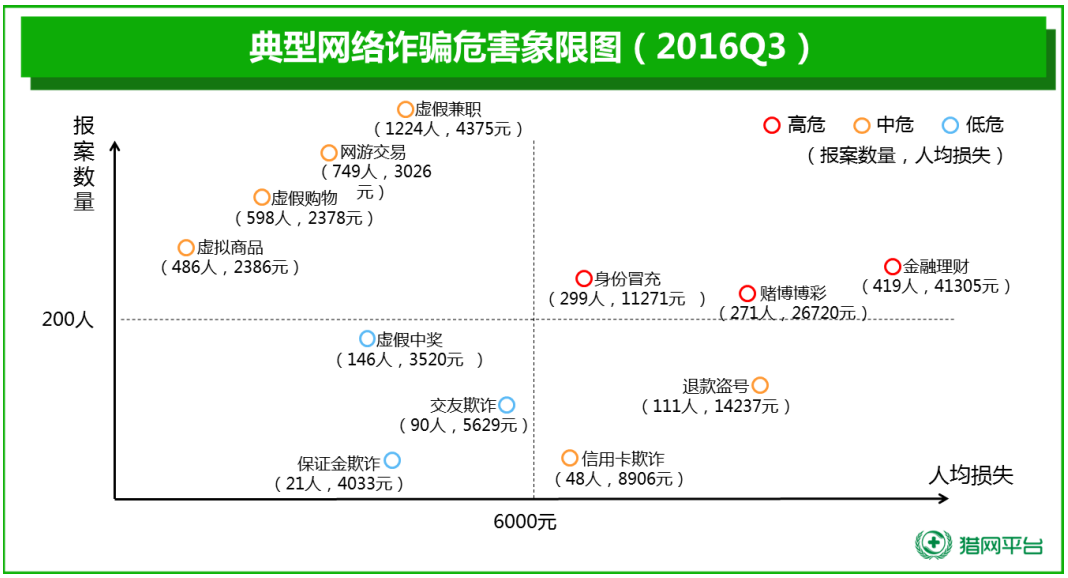
从涉案总金额来看，金融理财类诈骗总金额最高，达 1730.7 万元，占比 38.1%；其次是赌博博彩诈骗，涉案总金额 724.1 万元，占比 15.9%；虚假兼职诈骗排第三，涉案总金额为 535.5 万元，占比 11.8%。

从人均损失来看，金融理财类诈骗人均损失最高，达到了 41305 元；其次是赌博博彩诈骗为 26720 元，退款盗号诈骗为 14273 元。

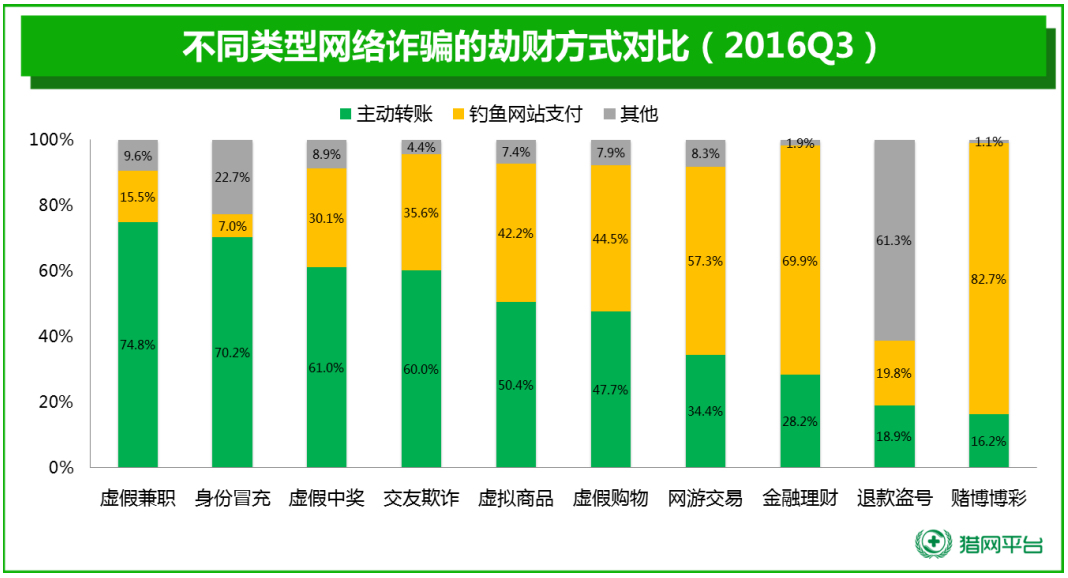
下图给出了主要网络诈骗类型的举报量和涉案总金额分布情况:



下图给出了不同类型的网络诈骗在人均损失和举报数量的象限图。从图中可见，金融理财诈骗（419 人，41305 元）、赌博博彩（271 人，26720 元）和身份冒充（299 人，11271 元）属于高危诈骗类型，受害人数多，人均损失金额大。而虚假兼职（1224 人，4375 元）、网游交易（749 人，3026 元）、虚假购物（598 人，2378 元）、虚拟商品（486 人，2386 元）、信用卡欺诈（48 人、8906 元）和退款盗号（111 人，14237 元）属于中危诈骗类型。



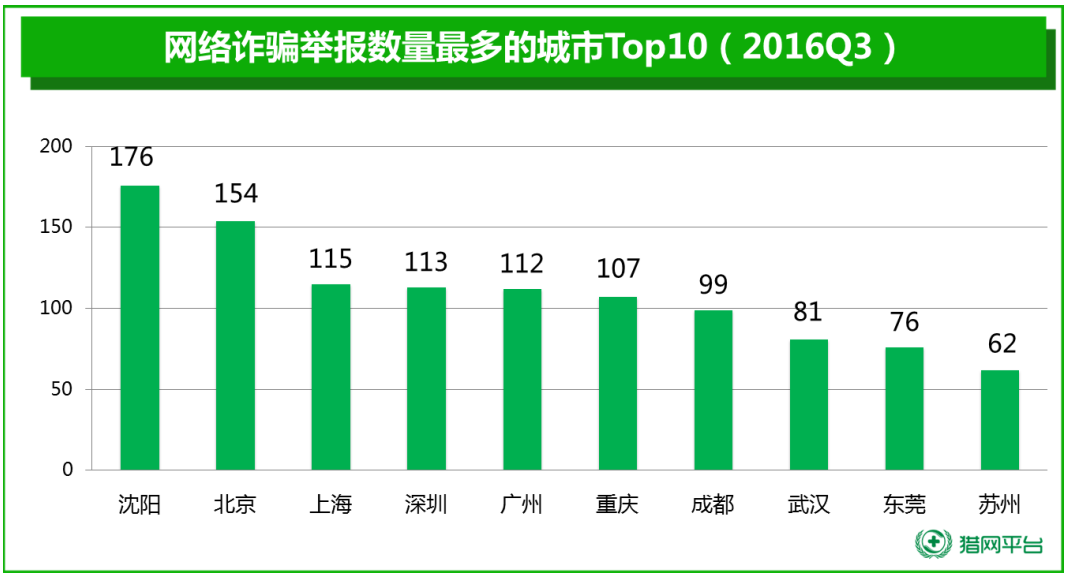
不同类型网络诈骗的劫财方式也有很大的不同，下图给出了部分主要网络诈骗类型的劫财方式对比，从中可以看出，虚假兼职、身份冒充类网络诈骗形式，七成以上的受害者都是深受骗子的蒙骗和蛊惑主动将钱转至骗子的指定账户中；而如赌博博彩和金融理财类诈骗，绝大多数受害者都是因为登录了钓鱼网站并进行支付而被骗的。



三、受害者地域分析

从用户举报情况来看，广东（564 起）、山东（321 起）、江苏（297 起）、辽宁（272 起）、四川（271 起），这 5 个地区用户的举报数量最多，约占了全国用户举报总量的 34.9%。

从各城市的举报量来看，沈阳以 176 起位居榜首，其次为北京、上海、深圳、广州四个一线城市，其举报量也较多。

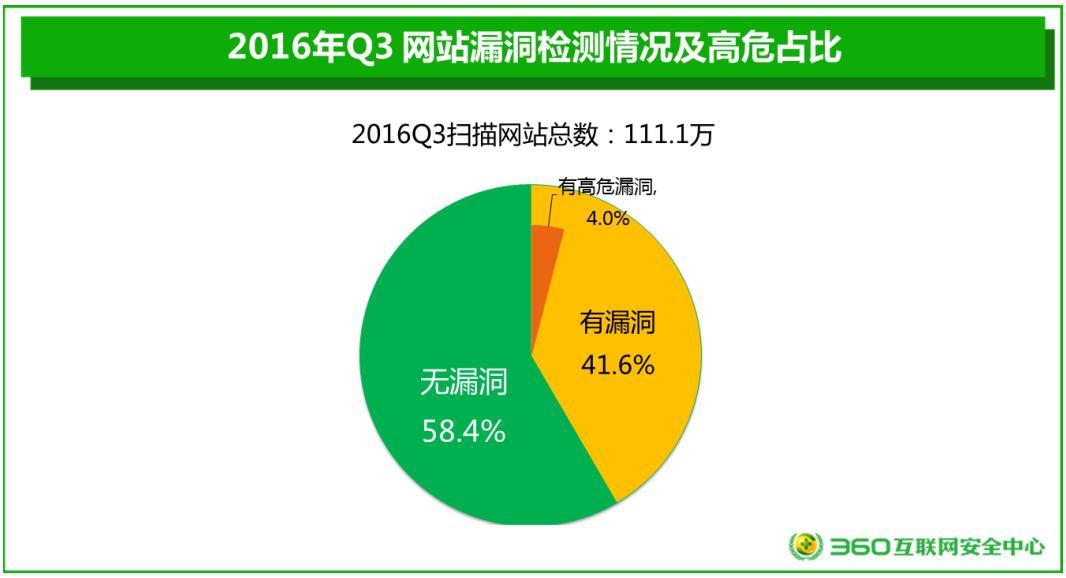


第六章 网站安全

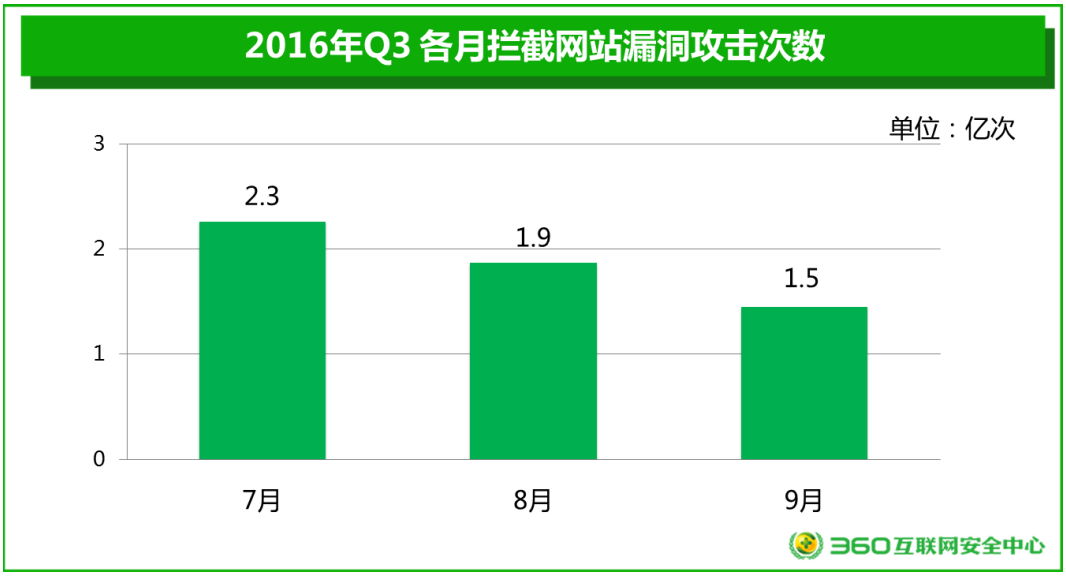
一、漏洞检测与攻击

2016 年第三季度，360 网站安全检测平台共扫描各类网站 111.1 万个，其中，存在安全漏洞的网站为 46.3 万个，占扫描网站总数的 41.6%。其中，存在高危安全漏洞的网站共有 4.4 万个，占扫描网站总数的 4.0%，同比 2015 年第三季度（14.2 万个）下降 69.0%。

下图给出了 2016 年第三季度存在安全漏洞网站比例情况。



2016 年第三季度，360 网站卫士共拦截各类网站漏洞攻击 5.6 亿次，其中 7 月的拦截量为 2.3 亿次，是第三季度拦截量最高的月份，8 月为 1.9 亿次、9 月为 1.5 亿次。



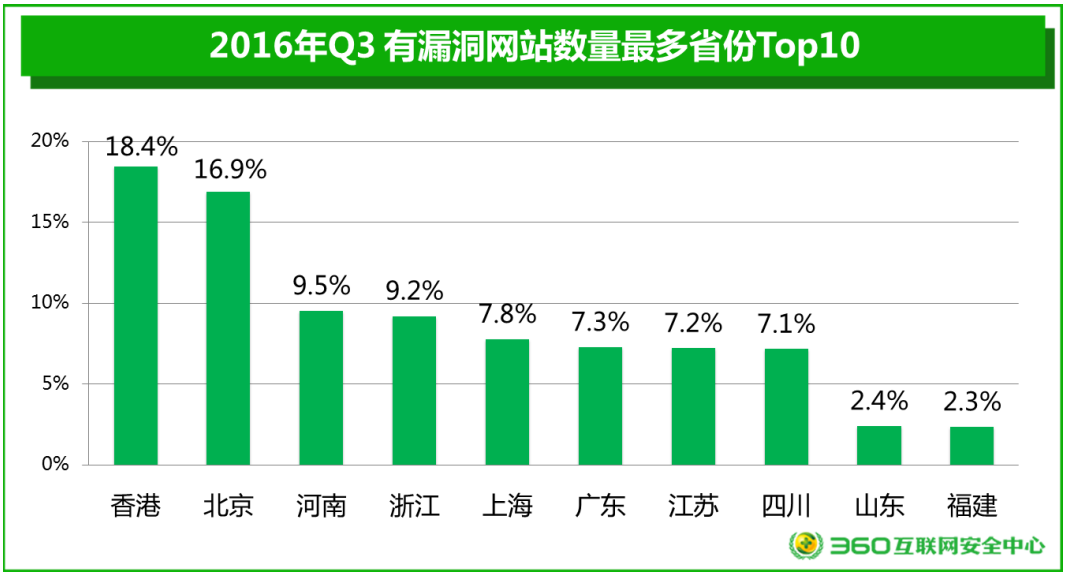
下表给出了扫出的数量排在前十位的漏洞类型。

排名	漏洞名称	危害程度	扫出次数（万）
1	应用程序错误信息	低危	108.4
2	跨站脚本攻击漏洞	高危	42.3
3	异常页面导致服务器路径泄漏	低危	34.6
4	发现敏感名称的目录漏洞	中危	25.4
5	WEB 服务器启用了 OPTIONS 方法	中危	22.0
6	发现 robots.txt 文件	中危	21.2
7	SQL 注入漏洞	高危	17.3
8	IIS 版本号可以被识别	中危	15.0
9	发现目录启用了自动目录列表功能	低危	8.2
10	Mysql 可远程连接	中危	3.7

表 1　2016 年第三季度检出数量最多的漏洞类型

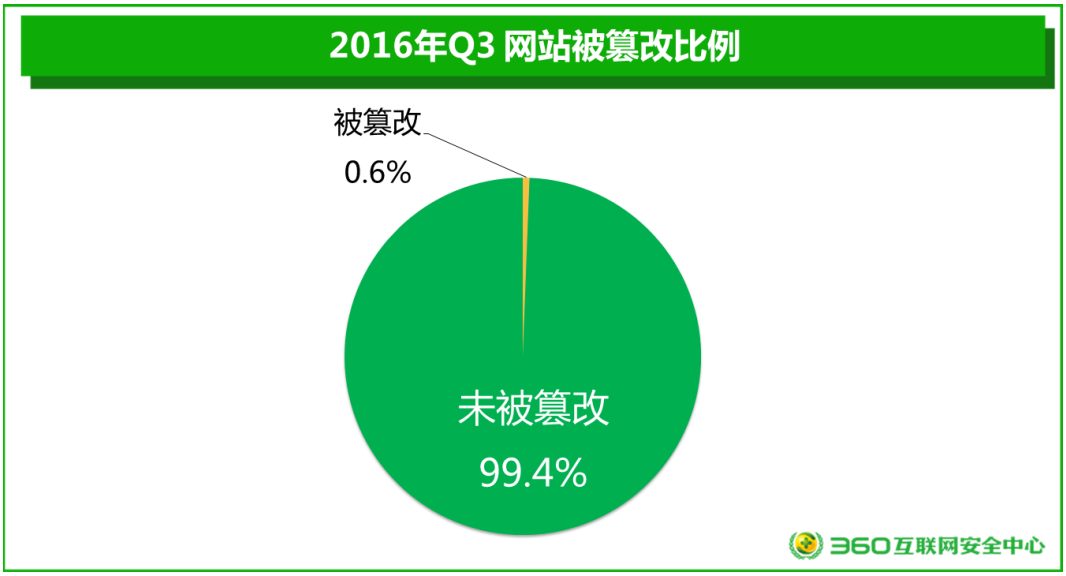
2016 年第三季度，从有漏洞网站的省级区域分布来看，香港是占比最高的地区，占比为 18.4%，其次是北京（16.9%）、河南（9.5%）、浙江（9.2%）和上海（7.8%）。

前 5 名省区的总和占全国的 61.8%，相比第二季度（58.5%）增长 3.3 个百分点，说明全国各地网站漏洞隐患问题相对集中。

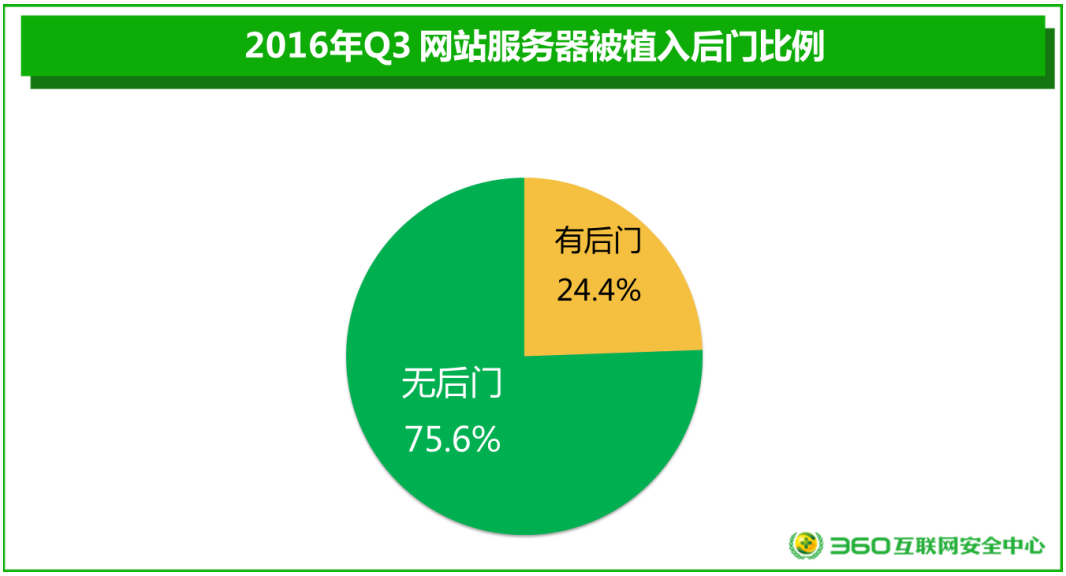


二、网页篡改与后门

2016 年第三季度，360 网站安全检测平台共对 391.3 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 2.5 万个，约占扫描网站总数的 0.6%。同比，2015 年第三季度 3.7 万个，下降 32.4%



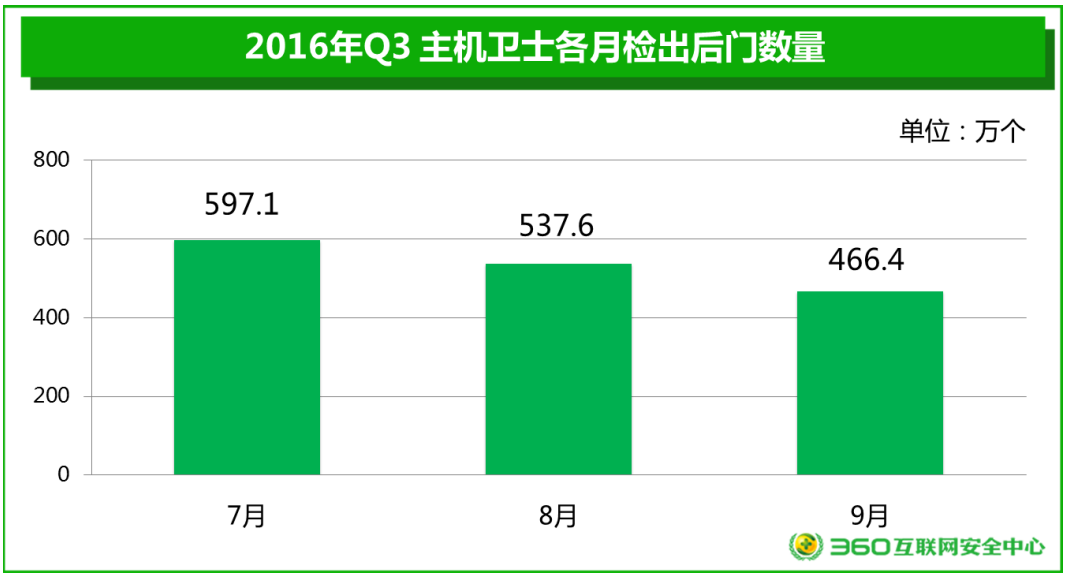
2016 年第三季度，360 网站安全检测对 1.8 万台网站 web 服务器进行了网站后门检测，覆盖网站数量为 289.2 万（含二级域名）；扫描发现约 24.4%的 web 服务器存在后门。



2016 年第三季度，360 网站安全检测的后门数量高达 1601.1 万个，平均每天检出后门数量 17.4 万个。

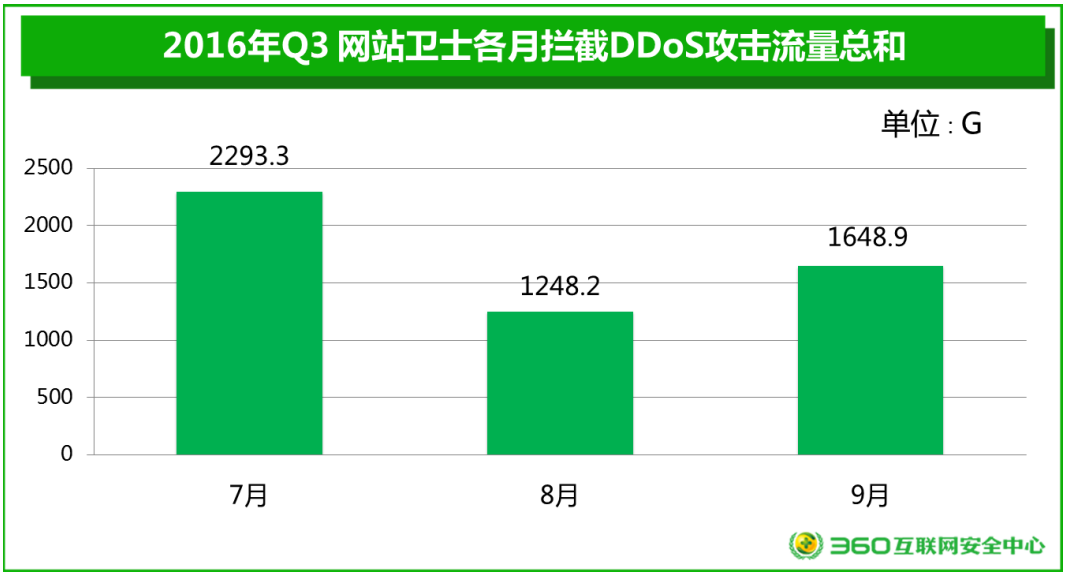
2016 年 Q3 各月检出后门数量见下图：7 月份检出后门 597.1 万个，8 月份检出后门 537.6

万个，9 月份检出后门 466.4 万个。

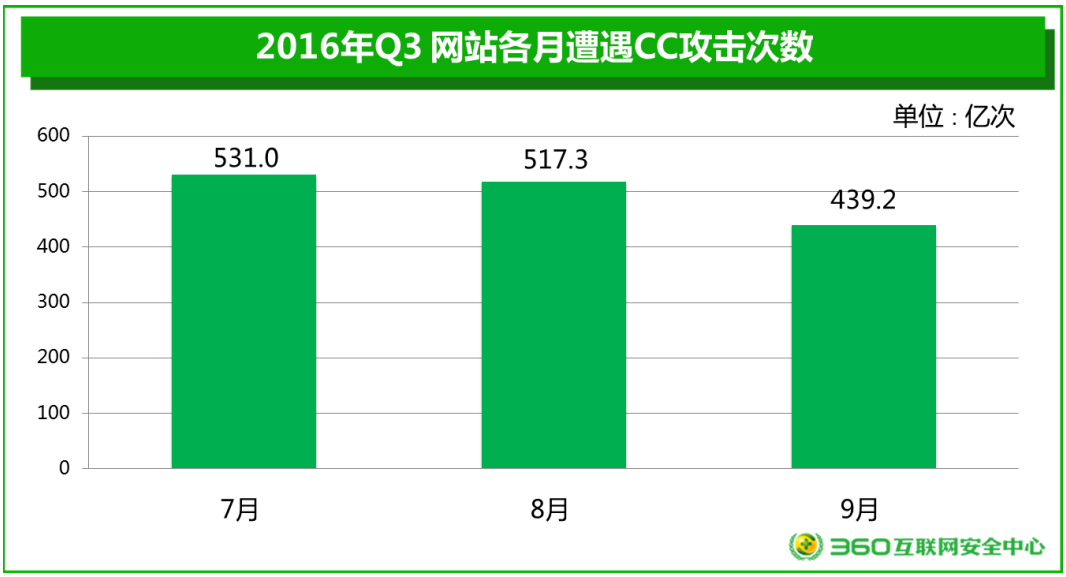


三、 流量攻击

2016 年第三季度，360 网站卫士共拦截的 DDoS 攻击流量如下图。其中 7 月拦截的 DDoS 攻击最高达 2293.3G，8 月的拦截量大幅下降。但 9 月的攻击流量又回升到 1648.9G。



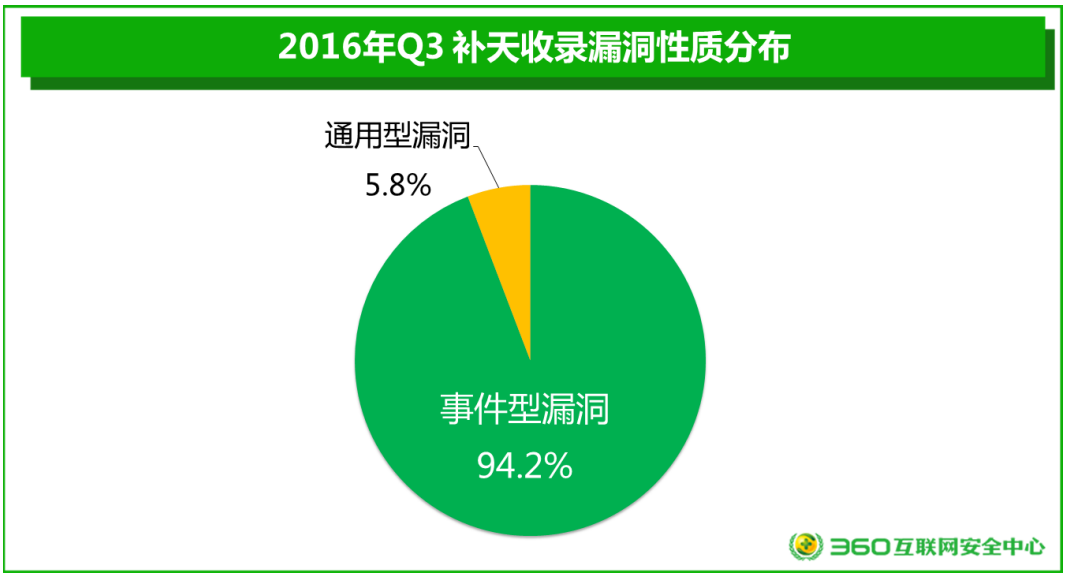
2016 年第三季度，360 网站卫士共拦截 CC 攻击共计 1487.5 亿次，平均每个月拦截 495.8 亿次。其中 7 月份拦截的攻击量最大，达 531.0 亿次；8 月和 9 月的攻击拦击次数略有下降，分别为 517.3 亿次和 439.2 亿次。



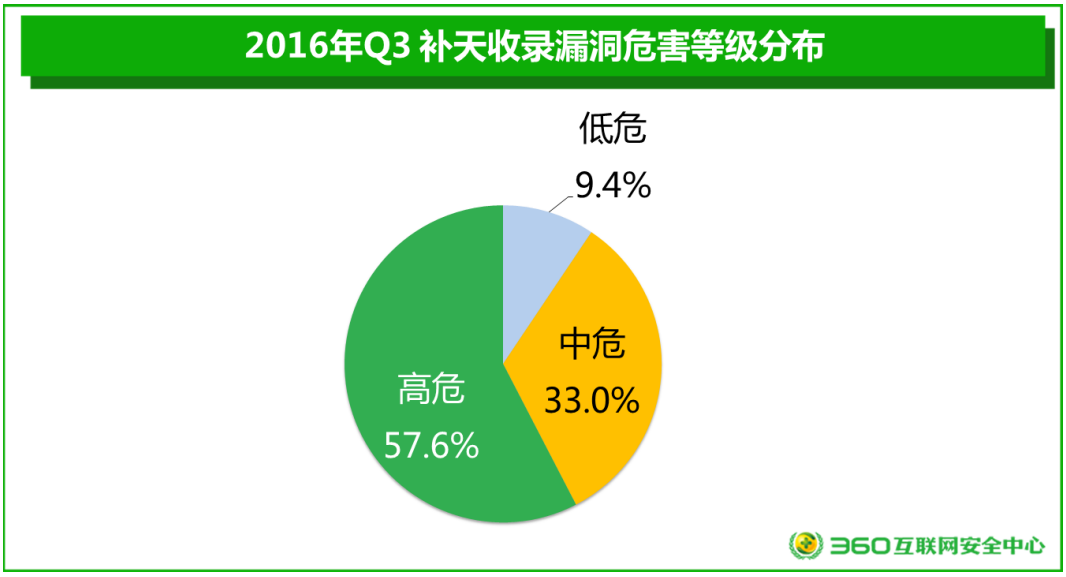
第七章 补天平台数据统计

一、 漏洞分析

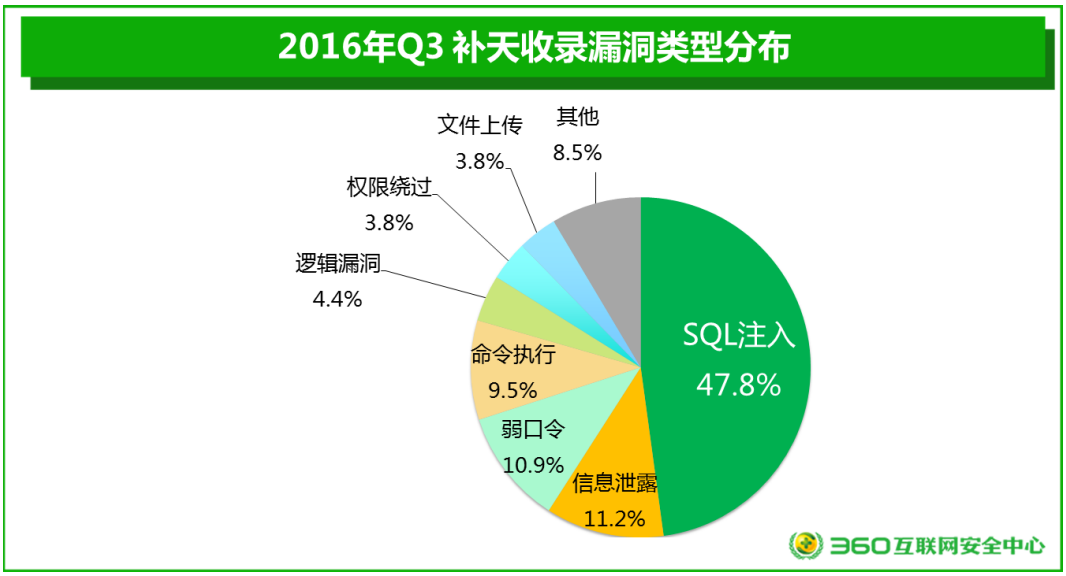
2016 年第三季度，补天平台共收录 1226 名“白帽子”提交的有效漏洞 13749 个，平均每天收录有效漏洞 149 个。其中通用型漏洞 800 个，占比为 5.8%，事件型漏洞则占 94.2%。下图给出了补天收录有效漏洞性质分布情况。



下图给出了补天平台新收录的 13749 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 57.6%。



下图给出了补天平台新收录漏洞类型，其中 SQL 注入（47.8%）、信息泄露（11.2%）、弱口令（10.9%）是最多的漏洞类型。



二、奖金发放

2016 年第三季度，补天平台共向 1226 名白帽子发布奖金 80.6 万元。

下表给出了 2016 年第三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	live800 全球在线客服任意文件操作	匿名	2000
亚军	某通用无线集成控制器无需登录可实现 GetShell	匿名	1500
亚军	某通用无线集成控制器无需登录可实现命令执行	匿名	1500

表 2　2016 年第三季度补天平台发放奖金最高的三个漏洞

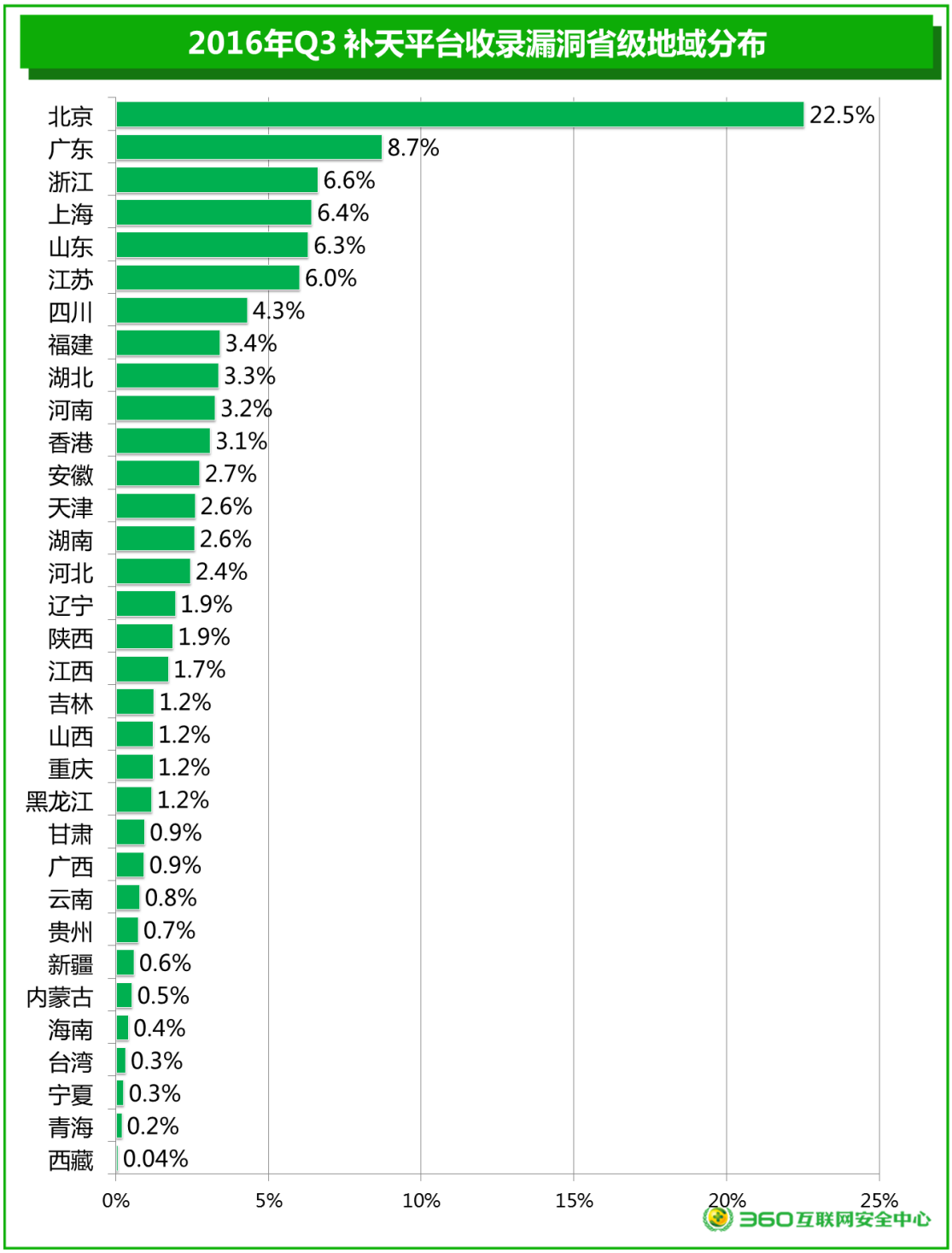
下表给出了 2016 年第三季度在补天平台获得奖金最多的三名白帽子的具体信息：

排名后	网名	报告 0day 漏洞个数	获奖金额
冠军	carry_your	187	107500
亚军	system_gov	63	45500
季军	华不再扬	25	43200

表 3　2016 年第三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 年第三季度补天平台收录漏洞的网站中，北京地区网站占 22.5%，广东地区网站 8.7%、浙江地区网站 6.6%、上海地区网站 6.4%、山东地区网站 6.3%等地的网站漏洞最多，总和超过总量的 50.5%。



附录　2016 年第三季度热点网络安全事件

一、　中华人民共和国网络安全法（草案二次审议稿）公布

7 月 5 日，作为网络空间基础性法律的《中华人民共和国网络安全法（草案二次审议稿）》正式向社会公布。草案二审稿进一步强化国家的责任和公民、组织的义务，加强关键信息基础设施保护，协同推进网络安全与发展，切实维护国家网络主权、安全和发展利益。相比 2015 年的一审稿，草案改动较大，社会各界依然高度关注。据最新消息，《中华人民共和国网络安全法》2016 年 11 月 7 号已由全国人大常委会审议通过。

二、　台湾多台 ATM 机现安全漏洞被盗取 7000 万元新台币

7 月份据台湾媒体报道，第一金控旗下第一银行 32 台 ATM 提款机出现安全漏洞，遭人植入恶意程序，被盗取金额超过 7000 万元新台币。

三、　白帽社区“乌云”关闭 公告称网站服务升级

7 月 19 日晚间 23 点，微博“互联网的那件事”曝出乌云官方网站显示无法访问。乌云发公告称，原因是官方正在进行升级。乌云运营团队在官网声明中称，乌云及相关服务将进行升级，将在最短的时间内回归……不管是从前，现在，还是未来，我们都将坚持这么做下去。乌云还在公告中强调：一直以来，乌云致力于让安全性作为用户选择产品的重要考量之一，促进企业更重视安全，让更多人重视安全关注安全，从而营造出更好的安全生态。

四、　第四届中国互联网安全大会（ISC2016）召开

8 月 16-17 日，第四届中国互联网安全大会（ISC 2016）在北京成功召开。作为亚太地区规模最大、最为权威的安全领域的年度盛会，这次会议云集了全球顶级的智库、专家、业界领袖和安全机构共同参与。

360 公司总裁齐向东在大会中指出，在网络威胁越来越大的今天，从政府到企业都表现出了强烈的联动和协同的意愿，单一的政府部门和企业如果不能进行数据的共享和情报的共享，几乎无法更好地解决现在的网络安全问题，而协同联动才是安全行业未来的风向标。

五、　8.19 山东临沂徐玉玉案件震惊全国，网络电信诈骗人人喊打

8 月份网络诈骗的案件接连不断，18 岁临沂女孩“被骗致死”引起举国上下公愤。在徐玉玉案之后，又爆出若干起某校大学生遭电信诈骗后猝死、某师范学生接航班取消短信被骗致 6100 元学费被转走的案件。8 月 27 日山东临沂徐玉玉电信诈骗案的头号犯罪嫌疑人陈文

辉落网。在公安部 A 级通缉令下，8 月 28 日徐玉玉案件宣布告破。

六、 微信曝远程任意代码执行漏洞，可被远程控制

8 月份，360 手机卫士阿尔法团队（AlphaTeam）独家发现微信远程任意代码执行漏洞，将其命名为 BadKernel。据阿尔法团队介绍，通过此漏洞攻击者可获取微信的完全控制权，危及用户朋友圈、好友信息、聊天记录甚至是微信钱包，可使上亿微信用户受到影响，危害巨大。目前，阿尔法团队的相关研究人员已经将此漏洞报告给腾讯应急响应中心并提供了修复建议。

七、 20 万山东高考生信息遭泄露，所有数据一起打包售 6000 元

2016 年 8 月根据山东卫视记者调查，在网上搜索与“考生数据”有关的 qq 群，发现基本上全国各地都有贩卖考生数据的 qq 群，每个群里多则 800 多人，少则十几人。这些群主们大胆的在群里介绍里写着出售信息的分类，有的直接标价：“交易一元一条、验证一元一条，10 元一批。”

记者随意加了几个贩卖学生数据的 qq 号，一个 qq 号的简介里写着“2016 年最新考生名单”的卖家说，他手上有 20 多万山东高考考生的信息，全是今年最新的。信息里包含了学校、姓名、电话、家庭住址、家长电话，而这些数据能够保证 90%都是有效信息。当记者询问购买价格时，对方表示，所有山东的数据一起打包买最合算，只要 6000 元，如果分开买就会贵一点。

八、 北京六年共 1.6 亿多条个人信息遭泄露

2016 年 9 月北京晚报记者分析了北京各法院的相关判例 67 个，数据显示，北京近 6 年，有 1.6 亿多条公民个人信息被泄露。掌握这些信息资源的快递、网购、物业、教育等机构，甚至包括个别公安内部人员，是信息泄露的源头，而保健品、保险、理财、房地产中介等行业以及职业倒卖人员是这些信息的主要购买者。相关专业律师认为，目前刑法关于侵害公民个人信息类犯罪，规定不完善，司法解释缺位，在定罪方面，起点过于模糊，量刑方面相对过轻，个人信息保护方面立法亟待加强。

九、 360 率先推出“反勒索服务”、“敲诈先赔”等业务

2016 年 8 月 15 日，360 安全卫士发布 11.0 beta 版。该版本的安全卫士首次推出了 360 反勒索服务。用户在主界面上点击“反勒索服务”按钮，就可以按照提示申请开通 360 反勒索服务。用户在完全开通此项服务后，如果在没有看到 360 安全卫士的任何风险提示的情况下感染敲诈者木马，360 公司将替受害者支付最高 3 个比特币的赎金。

继 360 安全卫士之后，2016 年 9 月，360 企业安全集团于业内率先推出了‘敲诈先赔’服务。” 360 公司总裁齐向东表示，对于所有安装了 360 安全卫士的互联网用户，如果开启“360 文档保护功能”和“360 反勒索服务”，仍然感染了敲诈者木马，360 可以代替用户向黑客缴纳最高 3 个比特币的赎金。对于安装了 360 天擎的企业用户，如果用户在开启了敲诈先赔功能后仍然感染了敲诈者病毒，360 企业安全集团负责赔付赎金，提供每个企业最高一百万元的先赔保障。