

瑞星 2016 年上半年中国信息安全报告

北京瑞星信息技术股份有限公司

2016 年 7 月

免责声明

本报告综合瑞星“云安全”系统、瑞星客户服务中心、瑞星反病毒实验室、瑞星互联网攻防实验室、瑞星威胁情报平台等部门的统计、研究数据和分析资料，仅针对中国 2016 年 1 至 6 月的网络安全现状与趋势进行统计、研究和分析。本报告提供给媒体、公众和相关政府及行业机构作为互联网信息安全状况的介绍和研究资料，请相关单位酌情使用。如若本报告阐述之状况、数据与其他机构研究结果有差异，请使用方自行辨别，瑞星公司不承担与此相关的一切法律责任。

目录

一、个人互联网安全	8
(一) 病毒和木马	8
1. 上半年病毒概述	8
2. 2016 年 1 至 6 月病毒 Top10	9
3. 2016 年 1 至 6 月广东省病毒 Top5	10
4. 2016 年 1 至 6 月北京市病毒 Top5	11
5. 2016 年 1 至 6 月山东省病毒 Top5	11
6. 2016 年 1 至 6 月江苏省病毒 Top5	12
7. 2016 年 1 至 6 月浙江省病毒 Top5	12
8. 2016 年 1 至 6 月 CVE 漏洞 Top10	13
专题：敲诈软件分析报告	13
(二) 恶意 URL	16
1. 2016 上半年全球恶意 URL 总体概述	16
2. 2016 上半年中国恶意 URL 总体概述	16
3. 2016 上半年中国钓鱼网站概述	17
4. 2016 上半年中国部分省市访问钓鱼网站类型概述	19
5. 钓鱼网站趋势分析	24
6. 2016 上半年中国挂马网站概述	26
二、移动互联网安全	27
(一) 手机安全	27
1. 手机病毒概述	27
2. 2016 年 1 至 6 月 Android 手机漏洞 Top5	28
3. 手机垃圾短信概述	28
4. 移动支付安全风险概述	29
(二) 2016 上半年移动安全事件	29
1. 手机扫描二维码存在安全隐患	29
2. 公共免费 WiFi 可瞬间盗取你的一切隐私	29
3. Android Qualcomm Wi-Fi driver 安全限制绕过漏洞	30
4. 病毒伪装“交行安全控件”盗取用户敏感信息	30

5. “短信拦截马”病毒来袭，谨慎点击带有链接的短信息	31
三、企业信息安全	31
（一）上半年全球重大网络安全事件	31
1.恶性敲诈软件国内大爆发	31
2.乌克兰电网遭黑客攻击之 Black Energy.....	32
3. 2.7 亿 Gmail、雅虎和 Hotmail 账号遭泄露.....	32
4.叙利亚政府网络被黑，泄露 43GB 数据	32
5.匿名者 DDoS 攻击希腊银行网站	32
6.德国贡德雷明根核电站发现病毒	33
7.全球 2.5 万网络摄像机被黑，用于构建僵尸网络	33
8.日本 16 州 ATM 机沦陷，14 亿日元不翼而飞	33
9.超 3200 万 Twitter 账户密码泄露	33
10.俄罗斯最大社交网站 VK.com 被黑，1.71 亿用户账号仅售 1 比特币.....	33
11.MySpace 出现史上最大规模数据泄露事件	34
12.卡塔尔国家银行被黑，1.4G 数据泄露（涉及王室、英国军情六处、法国和波兰等各国情报）	34
（二）政府、金融、互联网、教育类网站将遭受 Struts2 漏洞攻击.....	34
1.Struts2 漏洞概述	34
2.Struts2 漏洞引发的攻击	35
3.漏洞攻击分布监测	36
4. 漏洞攻击造成的危害	38
（三）大规模数据泄露使全球网民无秘	39
1.全球重大数据泄露事件	39
2.社交网站、色情网站成数据泄露“大头”	39
3.基于被泄露的用户量分析	40
4.商业和政治为数据泄露主要原因	41
5.Java、Flash 和 IE 最受攻击者青睐.....	42
6.数据泄露事件的影响	45
四、趋势展望	45
（一）敲诈软件依然是低成本高收益网络犯罪主流	45

（二）政治色彩严重的网络攻击已波及民生领域	46
（三）大规模数据泄露事件频发，云安全问题应得到高度重视	46
（四）第三世界金融系统成为黑客的提款机	46
专题：你可能不知道你正在被偷窥	47

报告摘要

- 2016 年 1 至 6 月，瑞星“云安全”系统共截获病毒样本总量 2,312 万个，病毒总体数量比 2015 年同期上涨 20.17%。报告期内，病毒感染次数 2.4 亿次，感染机器总量 823 万台，平均每台电脑感染 29.16 次病毒。
- 2016 年 1 至 6 月，瑞星“云安全”系统在全球范围内共截获恶意 URL 总量 6,807 万个，其中挂马网站 4,987 万个，钓鱼网站 1,820 万个。美国恶意 URL 总量为 3,466 万个，位列全球第一，其次是葡萄牙 415 万个，中国 408 万个，分别位列二、三位。
- 2016 年 1 至 6 月，北京市、广西壮族自治区访问钓鱼网站类型主要以赌博类为主，广东省访问钓鱼网站类型主要以论坛类为主，黑龙江省、新疆省、天津市访问钓鱼网站类型主要以情色类为主，江苏省、上海市访问钓鱼网站类型主要以情色类与下载站类为主，安徽省访问钓鱼网站类型则是主要以赌博类与情色类为主。
- 2016 年 1 至 6 月，瑞星“云安全”系统共截获手机病毒样本 198 万个，与 2015 年同期相比增长 155.15%，新增病毒以隐私窃取类为主。在报告期内，手机病毒类型中隐私窃取类占比 30%，位列第一位，其次是恶意传播类与恶意扣费类，分别占比 20%与 15%。
- 2016 上半年移动安全事件：手机扫描二维码存在安全隐患；公共免费 WiFi 可瞬间盗取你的一切隐私；Android Qualcomm Wi-Fi driver 安全限制绕过漏洞；病毒伪装“交行安全控件”盗取用户敏感信息；“短信拦截马”病毒来袭，谨慎点击带有链接的短信；
- 2016 上半年全球重大网络安全事件：恶性敲诈软件国内大爆发；乌克兰电网遭黑客攻击之 Black Energy；2.7 亿 Gmail、雅虎和 Hotmail 账号遭泄露；叙利亚政府网络被黑，泄露 43GB 数据；匿名者 DDoS 攻击希腊银行网站；德国贡德雷明核电站发现病毒；全球 2.5 万网络摄像机被黑，用于构建僵尸网络；日本 16 州 ATM 机沦陷，14 亿日元不翼而飞；超 3200 万 Twitter 账户密码泄露；俄罗斯最大社交网站 VK.com 被黑，1.71 亿用户账号仅售 1 比特币；MySpace 出现史上最大规模数据泄露事件；卡塔尔国家银行被黑，1.4G 数据泄露（涉及王室、英国军情六处、法国和波兰等各国情报）。
- 2016 年上半年，Struts2 相继暴露多个高危害漏洞，这些漏洞可远程代码执行，通过执行恶意代码对远程服务器实施攻击。由于 Struts 架构广泛应用于政府、大型互联网企业、金融机构等网站建设，并作为网站开发的底层框架使用，所以此次漏洞可能使大量政府、门户、电商、银行等网站遭受恶意攻击。电商、银行等网站很容易造成用户帐号密码丢失，由于门户、政府网站在用户心中可信度较高，很容易被不法分子利用，通过发布钓鱼欺诈链接诱使网民受骗。
- 2016 年上半年，大规模数据泄露使全球网民无秘，社交网站、色情网站成数据泄露“大头”，商业和政治为数据泄露主要原因。商业原因：竞争对手进行恶意竞争，毁坏对手的业界声誉等；政治原因：阻止选举、反对种族歧视等。Adobe、微软和甲骨文公司是数据泄露漏洞较多的企业，Java、Flash 和 IE 最受攻击者青睐。

- 趋势展望：敲诈软件依然是低成本高收益网络犯罪的主流；政治色彩严重的网络攻击已波及民生领域；大规模数据泄露事件频发，云安全问题应得到高度重视；第三世界金融系统成为黑客的提款机；
- 专题：你可能不知道你正在被偷窥。2016 年智能摄像头、智能手机引发的艳照门、偷窥门事件（三里屯、陆家嘴、宜家……）让互联网这个暗流涌动的大海彻底沸腾了。智能摄像头在给我们带来便利的同时，也存在着极大的安全隐患。无论是国际网站，还是国内网站都流出大量通过智能摄像头拍摄出的用户私密与不雅照片。

一、个人互联网安全

（一）病毒和木马

1.上半年病毒概述

（1）病毒疫情总体概述

2016 年 1 至 6 月，瑞星“云安全”系统共截获病毒样本总量 2,312 万个，病毒总体数量比 2015 年同期上涨 20.17%。报告期内，病毒感染次数 2.4 亿次，感染机器总量 823 万台，平均每台电脑感染 29.16 次病毒。

在报告期内，新增木马病毒占总体病毒的 52.78%，依然是第一大种类病毒。灰色软件病毒（垃圾软件、广告软件、黑客工具、恶意壳软件）为第二大种类病毒，占总体新增病毒样本的 22.95%，第三大种类病毒为蠕虫病毒，占总体比例的 9.83%。病毒释放器占总体数量的 9.03%，后门病毒占总体数量的 3.5%，漏洞攻击占总体数量的 1.75%，分别位列第四、第五和第六。

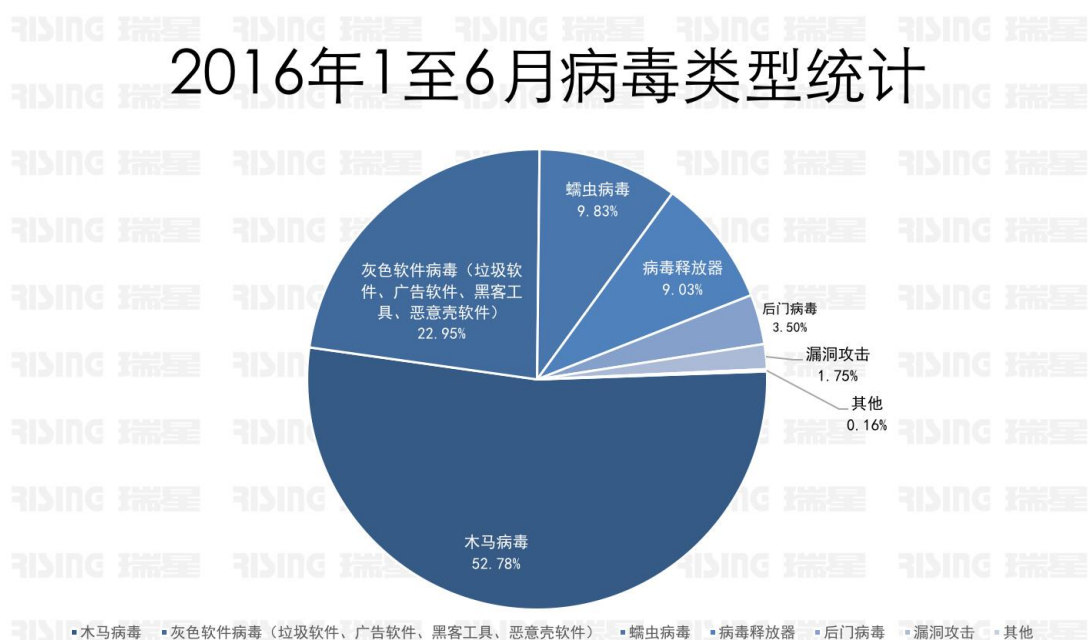


图 1：2016 年 1 至 6 月病毒类型统计

2015年上半与2016年上半年病毒对比

类别	年份	2015上半年	2016上半年
病毒样本数		1,924万个	2,312万个
病毒感染次数		2.1亿次	2.4亿次
病毒感染机器总量		933万台	823万台
平均每台电脑病毒感染次数		22.66次	29.16次

图 2：2015 年上半与 2016 年上半年病毒对比图

(2) 病毒感染地域分析

在报告期内，广东省病毒感染 2,910 万人次，依然位列全国第一，其次为北京市 2,493 万人次及山东省 1601 万人次。与 2015 年同期相比，北京成功排进前三，江苏则由第二名降到第四。

2016年1至6月病毒感染地域Top10

省份	数量
广东省	29098072
北京市	24927187
山东省	16010871
江苏省	13702517
浙江省	13688788
河南省	10749441
四川省	10660110
辽宁省	10513236
河北省	10105345
湖南省	8916334

图 3：2016 年 1 至 6 月病毒感染地域 Top10

2. 2016 年 1 至 6 月病毒 Top10

根据病毒感染人数、变种数量和代表性进行综合评估，瑞星评选出了 2016 年 1 至 6 月

病毒 Top10:

2016年1至6月病毒Top10

排名	病毒名称	感染次数	病毒描述
1	LNK:Worm.LnkBased	27920576	通常是由蠕虫释放的恶意快捷方式文件
2	PUA.Generic	16461772	不被需要的灰色软件，例如：软件下载/推广器、具备流量劫持功能的无用软件等
3	Virus.Ramnit	15064162	感染型病毒
4	Adware.SwiftBrowse	6990310	恶意广告软件，会劫持浏览器，大量消耗计算机资源
5	Ransom.Locky	6594192	勒索软件Locky家族，会加密200种以上的数据文件，支付赎金后才能解密
6	Adware.BrowseFox	5921637	恶意广告软件，会劫持浏览器，大量消耗计算机资源
7	Trojan.Crypto	4224640	采用了混淆、膨胀等技术对抗安全软件检测的恶意软件，例如：Zbot,Urausy等
8	VBS:Worm.Runner	4132160	蠕虫病毒，会通过移动存储设备传播
9	Backdoor.Overie	2875132	后门程序，感染后计算机会被黑客完全控制，成为“肉鸡”
10	LSP:Worm.Kenilfe	2433137	蠕虫病毒，基于AutoCAD软件传播，会尝试下载更多的恶意软件到计算机中

图 4：2016 年 1 至 6 月病毒 Top10

3. 2016 年 1 至 6 月广东省病毒 Top5

2016年1至6月广东省病毒Top5

排名	病毒名称	感染次数	病毒描述
1	NK:Worm.LnkBased	3574323	通常是由蠕虫释放的恶意快捷方式文件
2	PUA.Generic	1911682	不被需要的灰色软件，例如：软件下载/推广器、具备流量劫持功能的无用软件等
3	Virus.Ramnit	1291097	感染型病毒
4	Trojan.Crypto	742666	采用了混淆、膨胀等技术对抗安全软件检测的恶意软件
5	Ransom.Locky	496803	勒索软件Locky家族，会加密200种以上的数据文件，支付赎金后才能解密

图 5：2016 年 1 至 6 月广东省病毒 Top5

4. 2016 年 1 至 6 月北京市病毒 Top5

2016年1至6月北京市病毒Top5

排名	病毒名称	感染次数	病毒描述
1	LNK:Worm.LnkBased	2333214	通常是由蠕虫释放的恶意快捷方式文件
2	Virus.Ramnit	2189336	感染型病毒
3	PUA.Generic	1802133	不被需要的灰色软件，例如：软件下载/推广器、具备流量劫持功能的无用软件等
4	VBS:Worm.Runner	920129	蠕虫病毒，会通过移动存储设备传播
5	Ransom.Locky	529759	勒索软件Locky家族，会加密200种以上的数据文件，支付赎金后才能解密

图 6：2016 年 1 至 6 月北京市病毒 Top5

5. 2016 年 1 至 6 月山东省病毒 Top5

2016年1至6月山东省病毒Top5

排名	病毒名称	感染次数	病毒描述
1	LNK:Worm.LnkBased	1208114	通常是由蠕虫释放的恶意快捷方式文件
2	PUA.Generic	1138601	不被需要的灰色软件，例如：软件下载/推广器、具备流量劫持功能的无用软件等
3	Virus.Ramnit	595409	感染型病毒
4	Ransom.Locky	384818	勒索软件Locky家族，会加密200种以上的数据文件，支付赎金后才能解密
5	Trojan.Crypto	307249	采用了混淆、膨胀等技术对抗安全软件检测的恶意软件

图 7：2016 年 1 至 6 月山东省病毒 Top5

6. 2016 年 1 至 6 月江苏省病毒 Top5



图 8：2016 年 1 至 6 月江苏省病毒 Top5

7. 2016 年 1 至 6 月浙江省病毒 Top5



图 9：2016 年 1 至 6 月浙江省病毒 Top5

8. 2016 年 1 至 6 月 CVE 漏洞 Top10

2016年1至6月CVE漏洞Top10

排名	CVE漏洞编号	漏洞数量（个）
1	CVE-2010-2568	195264
2	CVE-2010-0188	123528
3	CVE-2012-0507	38376
4	CVE-2012-1723	28860
5	CVE-2013-0422	24384
6	CVE-2012-0158	20796
7	CVE-2011-1823	12624
8	CVE-2012-4681	10308
9	CVE-2013-2465	7968
10	CVE-2011-3544	5940

图 10：2016 年 1 至 6 月 CVE 漏洞 Top10

专题：敲诈软件分析报告

1. 什么是敲诈软件？

敲诈软件（也称密锁病毒）主要通过恶意钓鱼邮件进行传播，一旦用户运行邮件附件，病毒会将电脑中的各类文档进行加密，让用户无法打开，并出现弹窗，提示限时付款的勒索信息，如果用户未在指定时间缴纳黑客要求的金额，被锁文件将永远无法恢复。

敲诈病毒运作流程

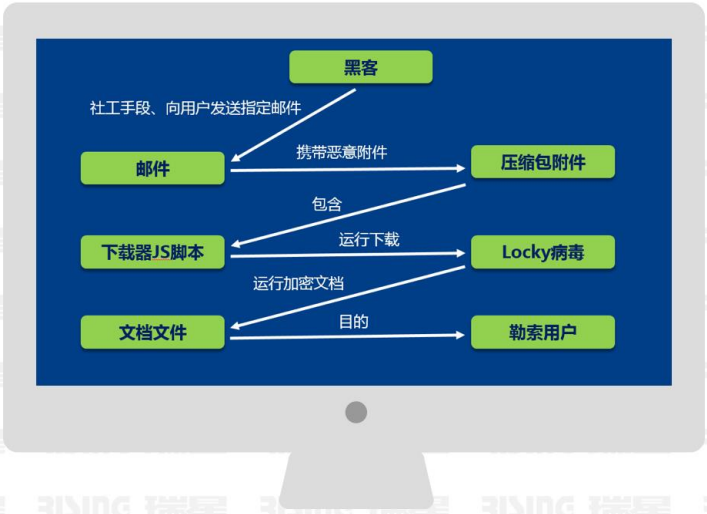


图 11：敲诈病毒运作流程

2. 敲诈软件技术分析

敲诈软件技术分析

投递能力	大量随机分发站点；大量的钓鱼邮件；小时级攻击全球。
免杀能力	高频量产免杀，利用时间差规避安全软件检测多分发站、多通讯代理、DGA规避网络安全设备的封锁。
加密能力	采用RSA2048+AES128加密，私钥在攻击者手中。加密本地磁盘、移动存储、网络共享，欲加密的资料型文件近两百种！
支付渠道	完全采用BTC支付，赎金接收账号及其分散，与CryptoWall 1等相比，同一BTC账户ID的使用频率更低。解密站点位于暗网，难以定位。

图 12：敲诈软件技术分析

3. 敲诈软件发展史

敲诈软件起源较早，最早于 1996 年。早年间以数据绑架为主，多用自定义加密算法，可技术还原。

2013 年，邮件传播，加密办公文件、照片、视频等几十种格式的文件，72 小时之内向其指定账户支付 300 美元，PayPal 等手段支付，FBI 都建议受害者支付“赎金”来解密文件。

2015 年 1 月，邮件传播，加密办公文件、照片、视频等百余种文件格式，在 96 小时内向其支付 8 比特币（当时约合人民币 1 万元左右）

2015 年 4 月，国内爆发，邮件传播，屏保格式病毒样本、加密办公文件、照片、视频等百余种文件格式，在 96 小时内向其支付比特币。

2016 年 1 月，邮件传播，通过合法数字签名绕开杀毒软件。

2016 年 3 月，利用 Office 宏进行攻击，加密硬盘上的所有文档并重置文件为 MP3，要求用户支付赎金（最少 500 美元）。

4. 敲诈软件感染数据

在报告期内，瑞星“云安全”系统共截获密锁病毒样本 13.45 万个，感染共计 659 万次，其中安徽省感染 49.56 万次，位列全国第一，其次为广东省 43.42 万次、浙江省 41.71 万次及北京市 41.14 万次。

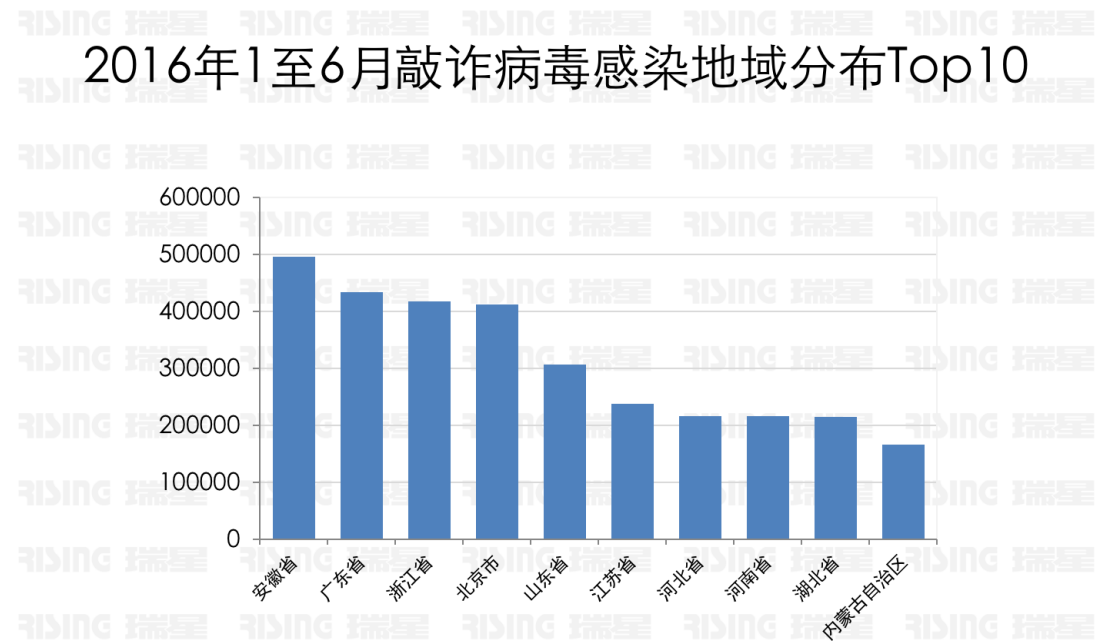


图 13：2016 年 1 至 6 月敲诈病毒感染地域分布 Top10

5. 瑞星给用户的建议

- 1)、定期备份系统与重要文件，并离线存储独立设备；
- 2)、使用专业的电子邮件与网络安全工具，可分析邮件附件、网页、文件是否包括恶意软件，带有沙箱功能；
- 3)、经常给操作系统、设备及第三方软件更新补丁；

- 4)、使用专业的反病毒软件、防护系统，并及时更新；
- 5)、设置网络安全隔离区，确保既是感染也不会轻易扩散；
- 6)、针对 BYOD 设置同样或更高级别的安全策略；
- 7)、加强员工（用户）安全意识培训，不要轻易下载文件、邮件附件或邮件中的不明链接。

（二）恶意 URL

1.2016 上半年全球恶意 URL 总体概述

2016 年 1 至 6 月，瑞星“云安全”系统在全球范围内共截获恶意 URL 总量 6,807 万个，其中挂马网站 4987 万个，钓鱼网站 1,820 万个。美国恶意 URL 总量为 3,466 万个，位列全球第一，其次是葡萄牙 415 万个，中国 408 万个，分别为二、三位。

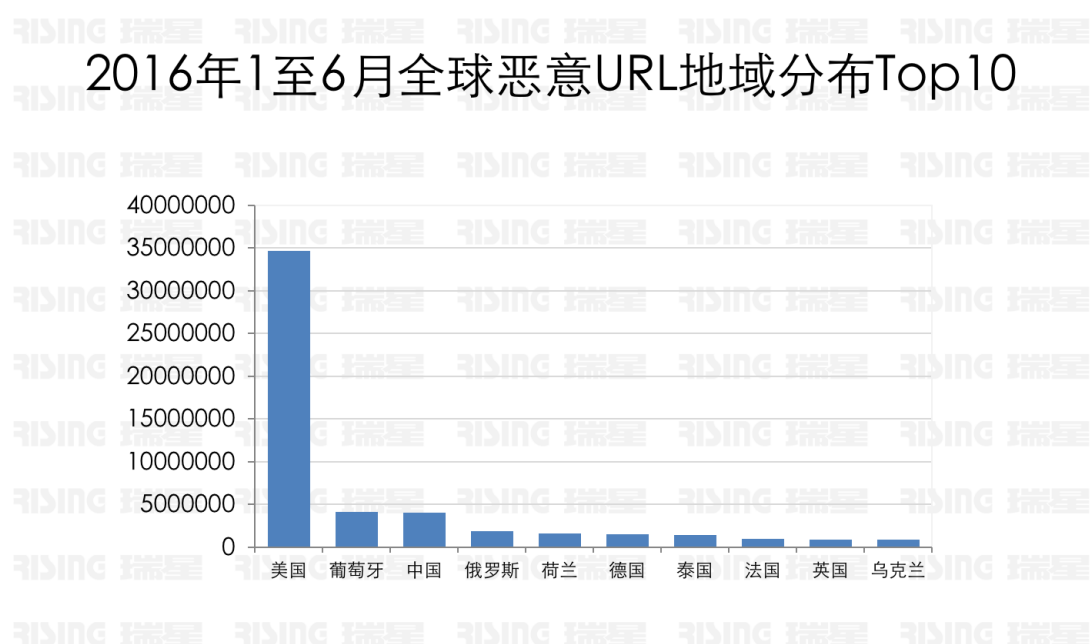


图 14：2016 年 1 至 6 月全球恶意 URL 地域分布 Top10

2.2016 上半年中国恶意 URL 总体概述

在报告期内，天津恶意 URL 总量为 73.31 万个，位列中国第一，其次是北京 71.27 万个，以及香港 50.16 万个，分别为二、三位。

注：上述恶意 URL 地址为恶意 URL 服务器的物理地址。

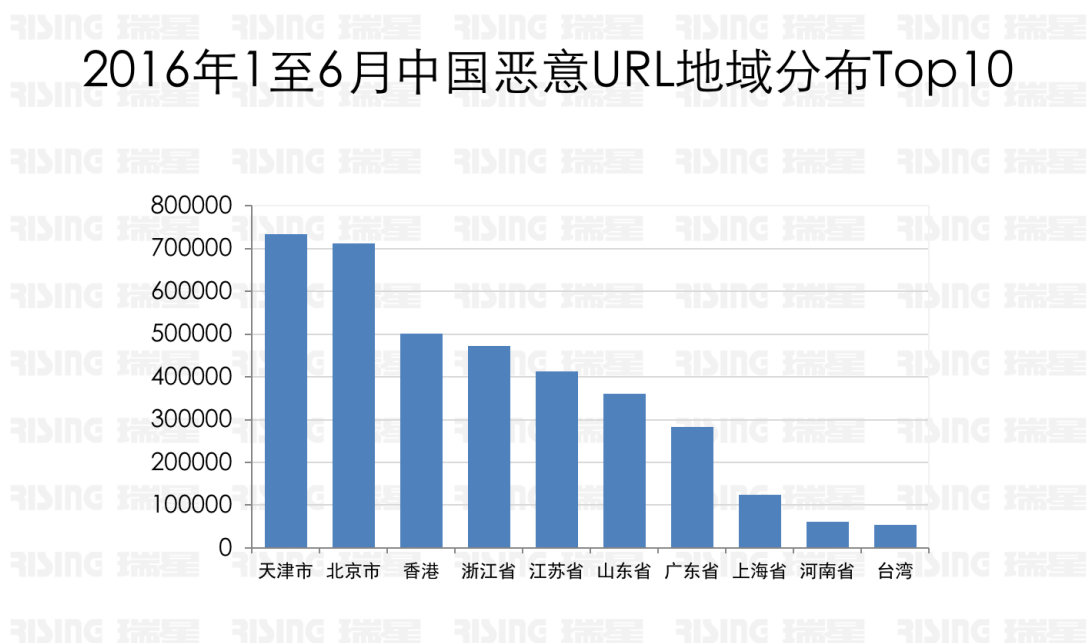


图 15：2016 年 1 至 6 月中国恶意 URL 地域分布 Top10

3.2016 上半年中国钓鱼网站概述

2016 年 1 至 6 月，瑞星“云安全”系统共拦截钓鱼网站攻击 2,223 万余次，攻击机器总量 216 万台，平均每台机器被攻击 10.29 次。

在报告期内，广东省受到钓鱼网站攻击 455 万次，位列第一位，其次是北京市受到钓鱼网站攻击 427 万次，第三名是山东省受到钓鱼网站攻击 139 万次。

2016年1至6月钓鱼网站攻击地域分布Top10

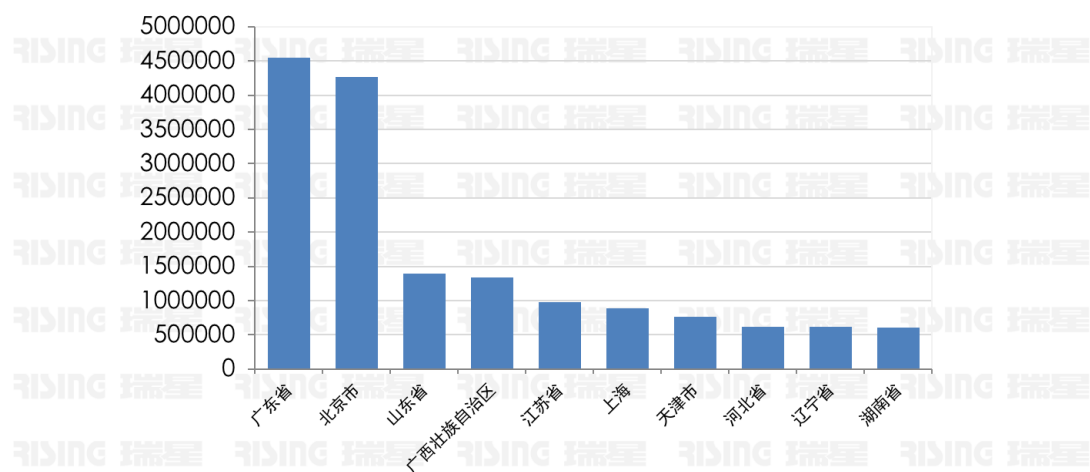


图 16：2016 年 1 至 6 月钓鱼网站攻击地域分布 Top10

2016年1至6月钓鱼网站类型

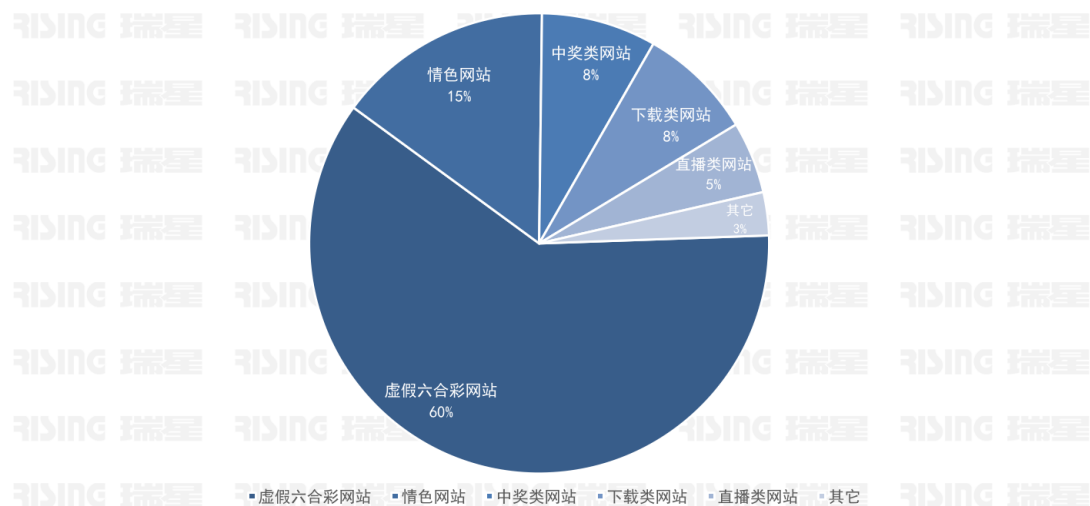


图 17：2016 年 1 至 6 月钓鱼网站类型

2016年1至6月重大钓鱼网站Top10

序号	网址	类型
1	http:// www. 442448. com/	六合彩诈骗
2	http://75ri. com	情色类
3	http://www. taolao. ygpyxy. com/	假冒淘宝中奖钓鱼
4	http://www. 163disk. com	下载类
5	http://www. xiunv333. com	在线直播秀
6	http://www. picobong. com/eshop/alibaba/	假冒Alibaba钓鱼
7	http://www. royalkingpackers. in/Update/login. php	假冒Paypal钓鱼
8	http://www. cursos-galilea. com/wp-includes/repack/	假冒Gmail邮箱钓鱼
9	http://10086xzcx. com/	假冒中国移动钓鱼
10	http://www. unlock-apple-iphone. com/	假冒Apple钓鱼

图 18： 2016 年 1 至 6 月重大钓鱼网站 Top10

4.2016 上半年中国部分省市访问钓鱼网站类型概述

在报告期内，北京市访问钓鱼网站类型主要以赌博类为主，占钓鱼网站总类型的 70%。

2016年1至6月北京市访问钓鱼网站类型

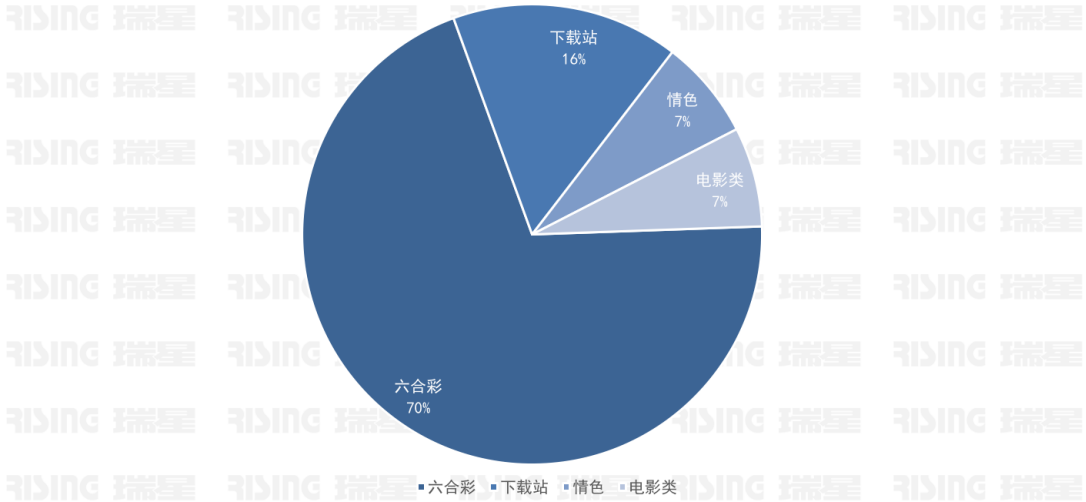


图 19： 2016 年 1 至 6 月北京市访问钓鱼网站类型

广东省访问钓鱼网站类型主要以论坛类为主，占钓鱼网站总类型的 59%。

2016年1至6月广东省访问钓鱼网站类型

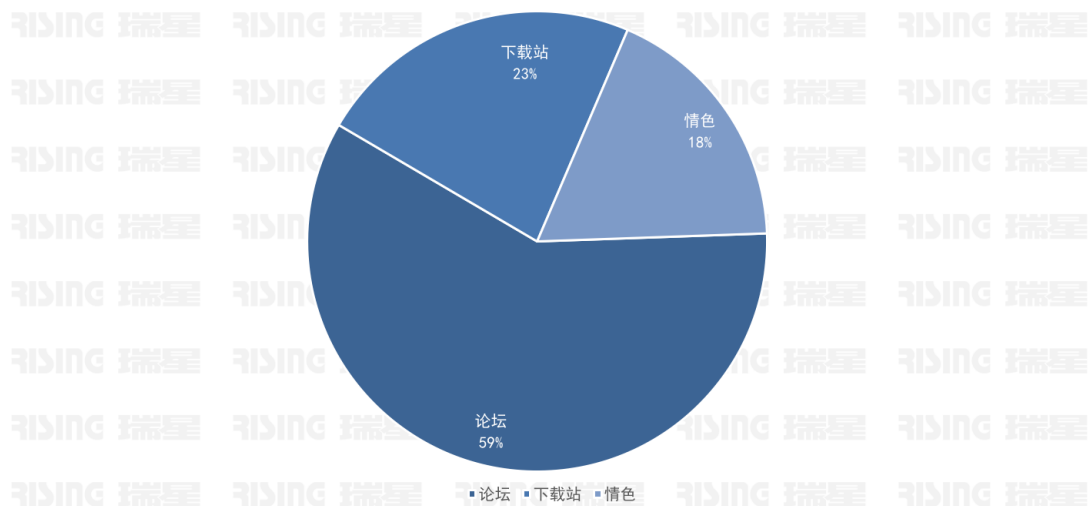


图 20：2016 年 1 至 6 月广东省访问钓鱼网站类型

广西壮族自治区访问钓鱼网站类型主要以赌博类为主，占钓鱼网站总类型的 56%。

2016年1至6月广西壮族自治区访问钓鱼网站类型

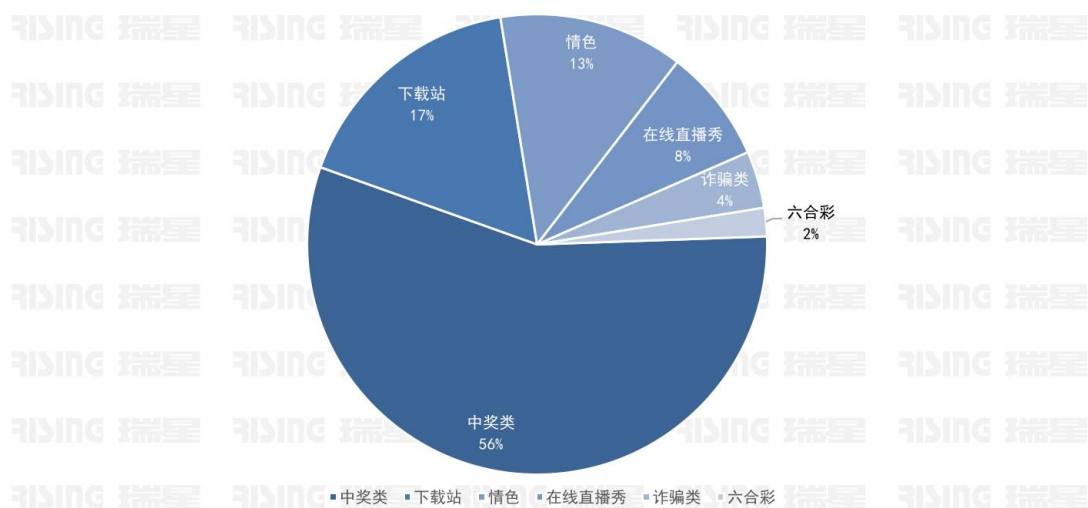


图 21：2016 年 1 至 6 月广西壮族自治区访问钓鱼网站类型

黑龙江省访问钓鱼网站类型主要以情色类为主，占钓鱼网站总类型的 94%。

2016年1至6月黑龙江省访问钓鱼网站类型

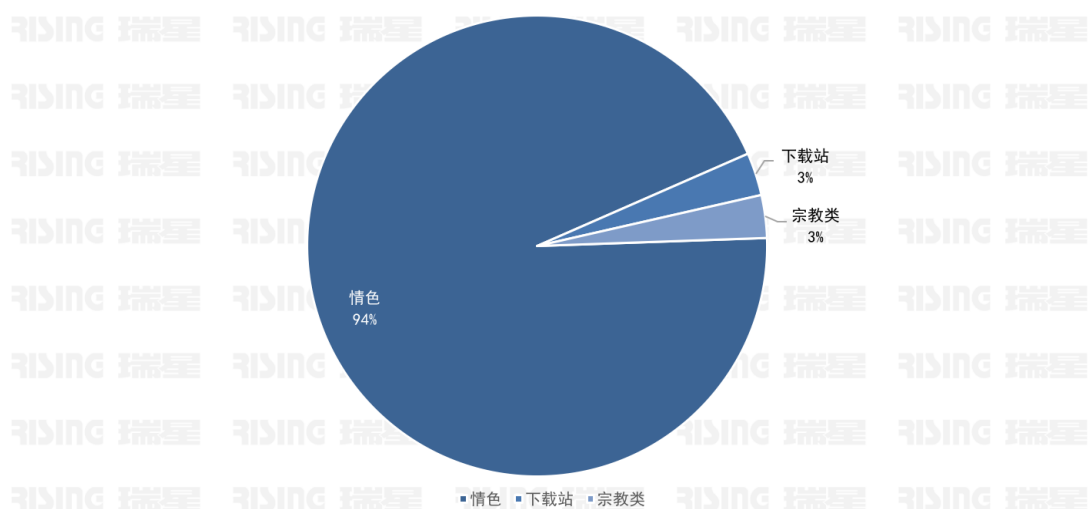


图 22：2016 年 1 至 6 月黑龙江省访问钓鱼网站类型

新疆省访问钓鱼网站类型主要以情色类为主，占钓鱼网站总类型的 96%。

2016年1至6月新疆省访问钓鱼网站类型

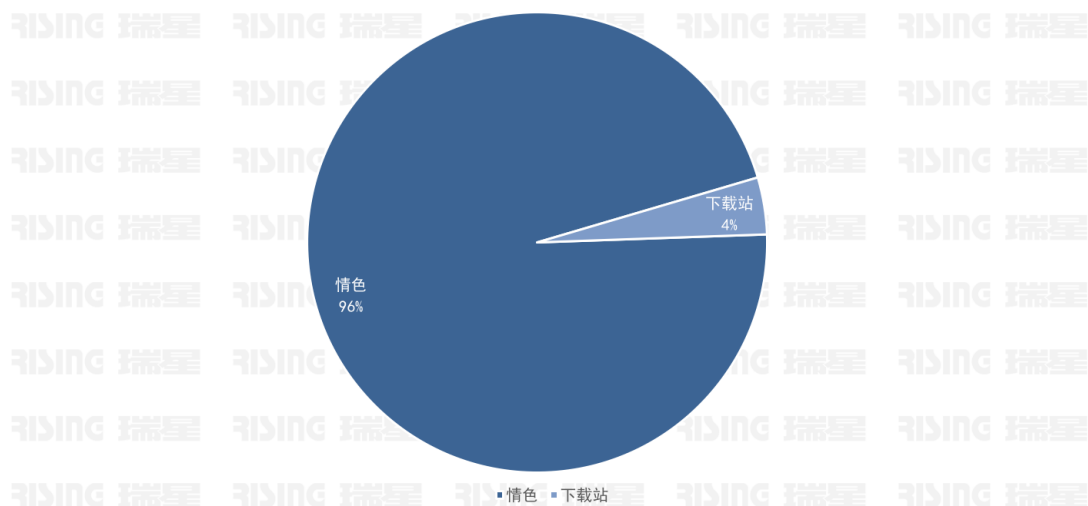


图 23：2016 年 1 至 6 月新疆省访问钓鱼网站类型

天津市访问钓鱼网站类型主要以情色类为主，占钓鱼网站总类型的 79%。

2016年1至6月天津市访问钓鱼网站类型

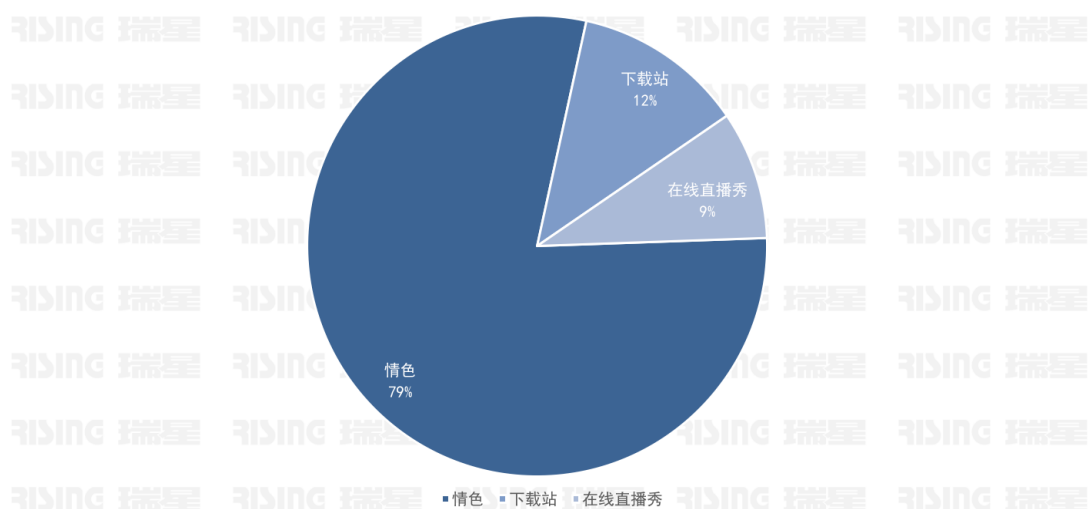


图 24：2016 年 1 至 6 月天津市访问钓鱼网站类型

上海市访问钓鱼网站类型主要以情色类与下载站类为主，分别占钓鱼网站总类型的 36%与 34%。

2016年1至6月上海市访问钓鱼网站类型

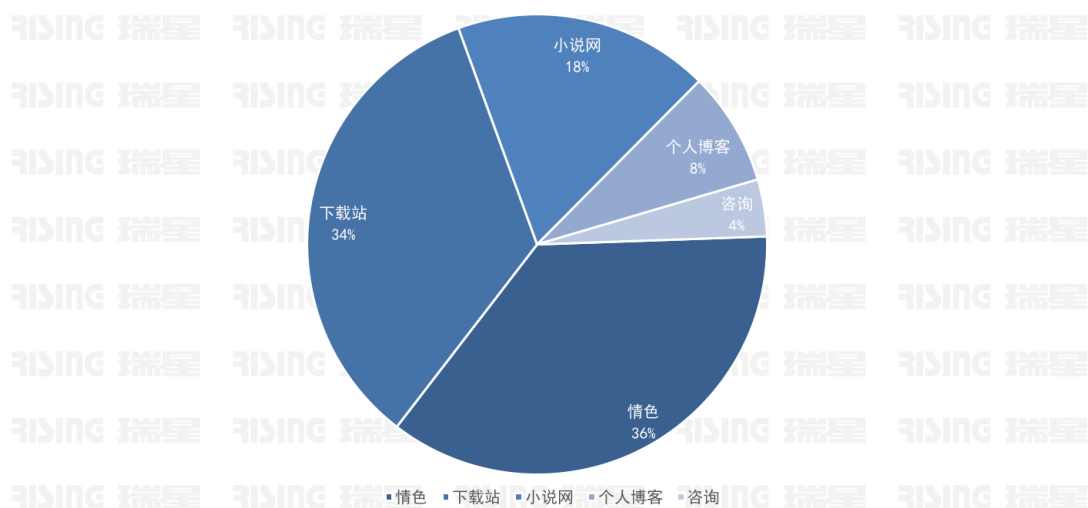


图 25：2016 年 1 至 6 月上海市访问钓鱼网站类型

江苏省访问钓鱼网站类型主要以下载站类与情色类为主，分别占钓鱼网站总类型的 41%与 32%。

2016年1至6月江苏省访问钓鱼网站类型

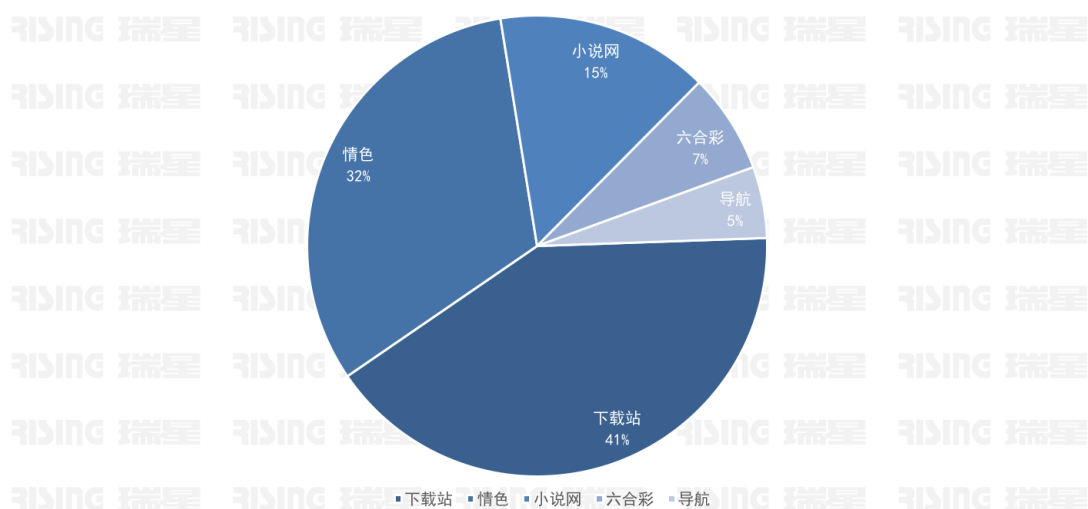


图 26：2016 年 1 至 6 月江苏省访问钓鱼网站类型

安徽省访问钓鱼网站类型主要以赌博类与情色类为主，分别占钓鱼网站总类型的 35% 与 19%。

2016年1至6月安徽省访问钓鱼网站类型

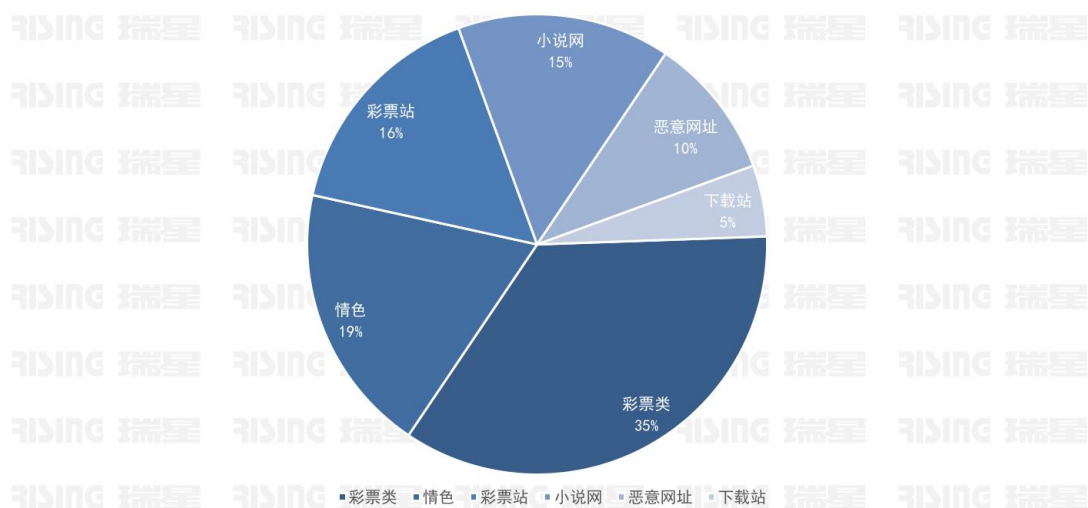


图 27：2016 年 1 至 6 月安徽省访问钓鱼网站类型

5.钓鱼网站趋势分析

2016 年金融、银行类钓鱼网站较往年有增加趋势，并且随着电子商务发展，支付类钓鱼网站也在增加。特别值得注意的是苹果 ID 钓鱼攻击，由于苹果手机加密性较高，攻击者可以使用苹果 ID 钓鱼方式进行篡改用户密码勒索用户。而钓鱼网站在 2016 年上半年数量有所增加，主要通过以下手段进行攻击。

- 利用垃圾短信“伪基站”推送恶意网址给用户，诱骗钓鱼。



图 28：“伪基站”推送恶意网址

- 利用移动 App 进行的钓鱼。随着手机移动终端的使用率逐渐上升，很多钓鱼攻击者利用终端缺少安全防护进行钓鱼攻击。

移动app进行的钓鱼



图 29：移动 App 进行的钓鱼

- 利用不同综艺节目、明星借钱或者中奖方式进行钓鱼诈骗。

利用综艺节目中奖方式进行钓鱼诈骗

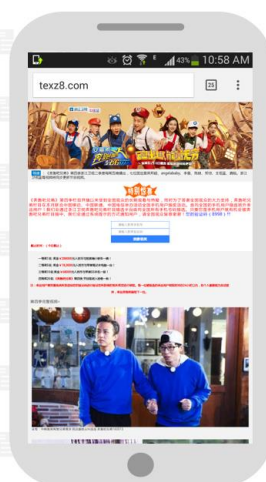


图 30：利用综艺节目中奖方式进行钓鱼诈骗

- 垃圾邮件配合 Web 漏洞形式进行盗取用户信息。

利用垃圾邮件盗取用户信息



图 31: 利用垃圾邮件盗取用户信息

6.2016 上半年中国挂马网站概述

2016 年 1 至 6 月, 瑞星“云安全”系统共拦截挂马网站攻击 971 万余次, 攻击机器总量 56 万台, 平均每台机器被攻击 17.34 次。

在报告期内, 辽宁省受到挂马攻击 337 万次, 位列第一位, 其次是北京市受到挂马攻击 236 万次, 第三名是上海市受到挂马攻击 126 万次。

2016年1至6月挂马攻击地域分布Top10

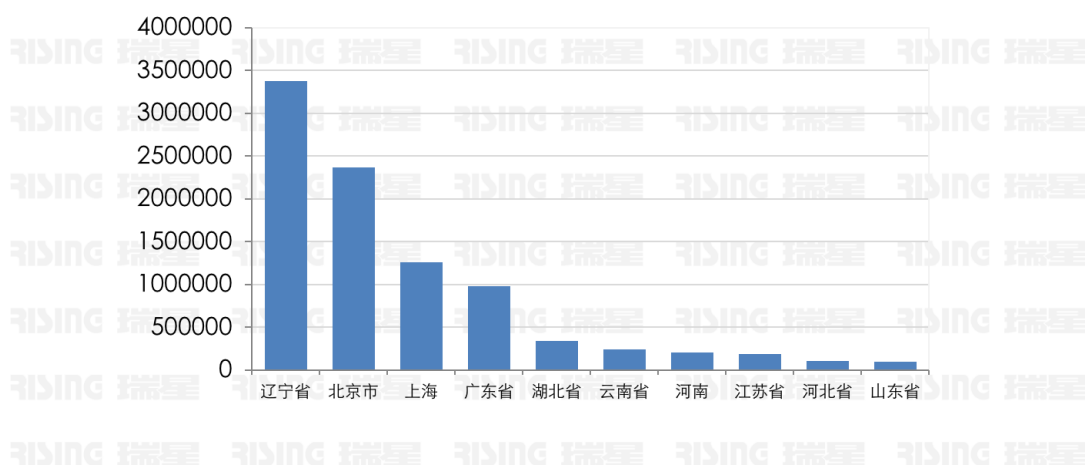


图 32：2016 年 1 至 6 月挂马攻击地域分布 Top10

由于 2016 年上半年漏洞爆发频率较低，相对挂马行为多数采用 2013-2015 年漏洞利用工具，随着杀毒软件的升级，瑞星安全软件已经可以对常见的漏洞利用工具进行有效的拦截。

二、移动互联网安全

（一）手机安全

1.手机病毒概述

2016 年 1 至 6 月，瑞星“云安全”系统共截获手机病毒样本 198 万个，与 2015 年同期相比增长 155.15%，新增病毒类型以隐私窃取类病毒为主。

在报告期内，手机病毒类型中隐私窃取类病毒占比 30%，位列第一位，其次是恶意传播类病毒与恶意扣费类，分别占比 20%与 15%。

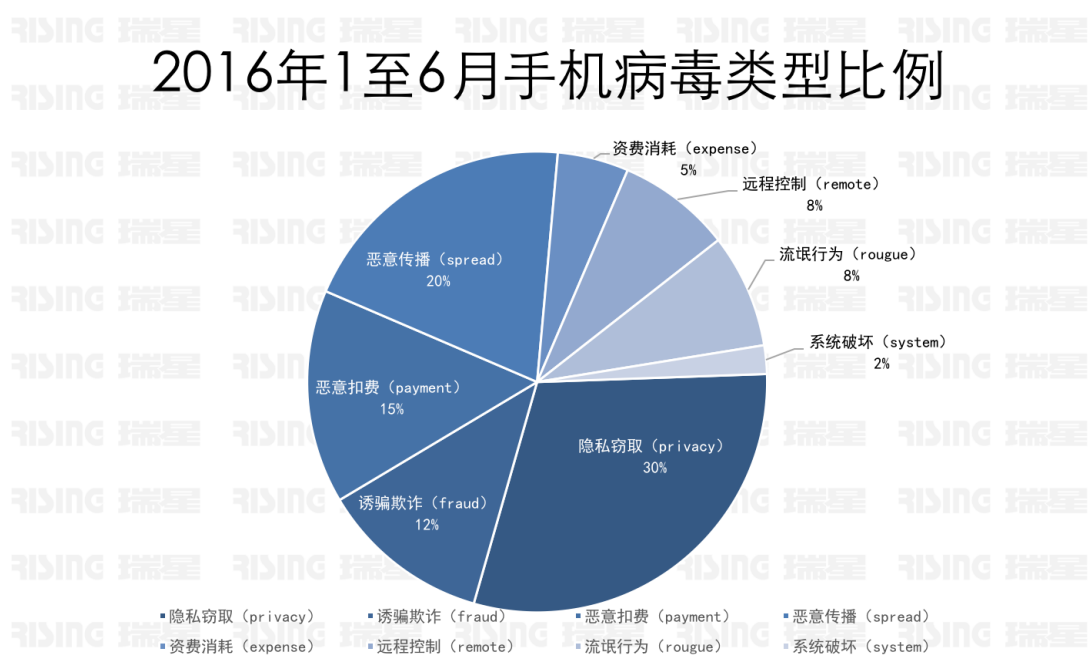


图 33：2016 年 1 至 6 月手机病毒类型比例

2016年1至6月手机病毒Top5

序号	病毒名称	感染数量	病毒行为
1	Trojan.Android.Zdtad!1.A21F	33264	具有弹出广告窗口、下载推广软件、让用户无法正常卸载、删除或退出软件进程行为
2	Trojan.Android.SmsPay.c	17316	具有通过自动拨打电话、发送短信、彩信、邮件、频繁连接网络行为
3	Trojan.Android.Spy.Agent!1.A405	2223	具有通过隐蔽执行、欺骗点击等手段订购各类收费业务或使用移动终端支付行为
4	Trojan.Android.Dowgin!1.A249	888	具有获取用户个人信息、通讯录信息、短信收件箱、手机号以及系统软硬件信息行为
5	Trojan.Android.FakeInstSms!1.A251	297	具有通过伪造、篡改、劫持短信、彩信、邮件、通讯录、通话记录、收藏夹、桌面等方式，诱导用户触发点击行为

图 34：2016 年 1 至 6 月手机病毒 TOP5

2. 2016 年 1 至 6 月 Android 手机漏洞 Top5

2016年1至6月Android手机漏洞Top5

序号	漏洞名称	漏洞编号	简介
1	Android/Linux内核 WiFi 模块栈缓冲区溢出漏洞	CVE-2016-0801	黑客可根据该漏洞私自窃取和篡改用户设备数据
2	Android拒绝服务漏洞	CVE-2016-2414	可使黑客对某台Android设备发动拒绝服务攻击
3	Android Compose Activity.java信息泄露漏洞	CVE-2016-2425	可使被攻击的设备崩溃，让黑客取得对设备的控制权
4	Android 5.0以下本地权限提升漏洞	CVE-2016-7911	黑客可通过构造的应用，远程攻击者可获取敏感信息
5	Android Trustzone权限提升漏洞	CVE-2016-6647	黑客可利用此漏洞进行远程攻击利用构造的应用获取提升的权限

图 35：2016 年 1 至 6 月 Android 手机漏洞 Top5

3.手机垃圾短信概述

2016 年 1 至 6 月，瑞星“云安全”系统共截获手机垃圾短信 45 亿条，短信类型主要以广告促销、运营商、金融服务、新闻播报为主，其中广告促销类占比最大高达 30%，运营商类占 25%，伪基站垃圾短信占比 19%，金融服务类占 16%，新闻播报类占 10%。

2016年1至6月手机垃圾短信类型比例

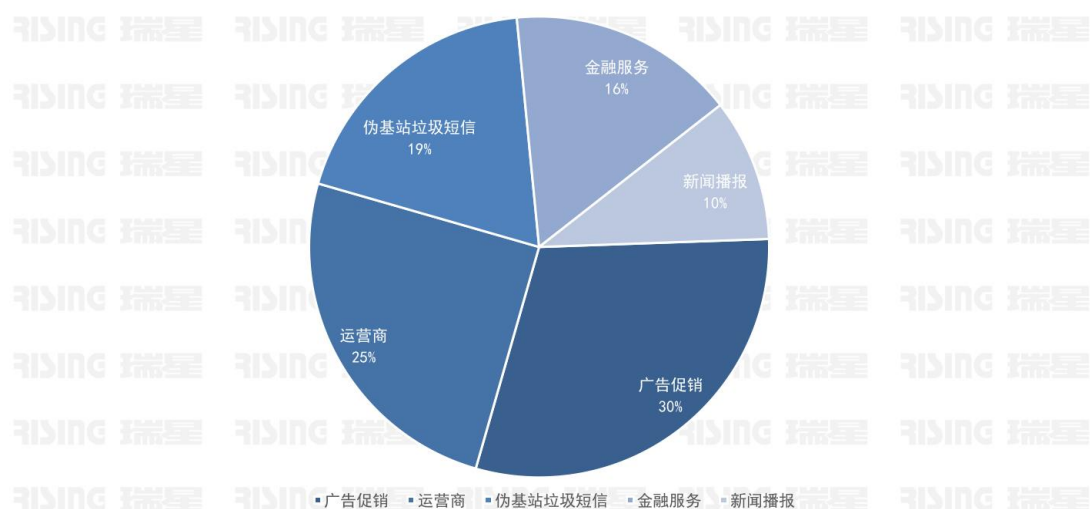


图 36：2016 年 1 至 6 月手机垃圾短信类型比例

4.移动支付安全风险概述

截止到 2016 年 6 月，中国手机网民总数达到 5.94 亿，使用手机支付的用户数已达到 2.76 亿。其中，28%的用户支付环境存在风险，移动支付安全的主要来自四大方面，恶意山寨应用、不明 WiFi 网络环境、支付应用自身漏洞、验证短信不安全，其中最主要风险是连接了不安全的 WiFi。

（二）2016 上半年移动安全事件

1.手机扫描二维码存在安全隐患

2016 年 3 月 15 日，央视 315 晚会曝光称不法分子利用二维码生成器把病毒植入到普通的二维码中，当用户使用手机扫描这些二维码时，病毒便会植入到用户手机中。这样，不法分子就就可以通过技术手段盗取用户信息，甚至拦截用户的通信信息，包括用户的身份证、验证码等，然后，不法分子便可以肆意更改用户的支付密码，从而盗取用户的钱财。

2.公共免费 WiFi 可瞬间盗取你的一切隐私

2016 年 3 月 15 日，央视 315 晚会主持人进行了这样一个实验：现场观众的手机都连上由主办方提供的免费无线网络，然后打开自己常用的一两个消费类软件，比如打车、订餐、购物的软件，浏览一下过去下的订单和消费记录。

令人惊讶一幕出现了，现场的大屏幕上各种地址、姓名、身份证号、银行卡号都显示了出来。用户消费的所有信息都可以看到，如果截取这些信息进行组合，一个人衣食住行的生活习惯甚至个人隐私，都可能被不法分子一点一点摸透。

该类攻击是通过在人流集中的公共场所设置无密码“黑网”实现的。攻击者往往采取假冒免费公共 WiFi 名称的方法引诱用户进入陷阱。一旦连接上“黑网”，用户发送的所有信息都将遭到监视。届时，不仅用户可能收到黑客推送的恶意信息，用户的隐私信息、网银账密还可能面临泄露。

3.Android Qualcomm Wi-Fi driver 安全限制绕过漏洞

2016 年 6 月 12 日，Android 系统被爆 Qualcomm Wi-Fi driver 存在安全漏洞。在 Nexus 7(2013)设备上，攻击者可利用此安全漏洞通过构造应用并直接授权应用程序最高权限来绕过目标数据访问的限制，可窃取用户手机中的 WiFi 模块驱动信息、序列号、WiFi 连接的账号和密码以及远程发送指令来控制设备等的操作。

4.病毒伪装“交行安全控件”盗取用户敏感信息

2016 年 6 月，一个伪装成“交行安全控件”的病毒潜伏在各大安卓电子市场中，诱导用户下载安装。该病毒运行后，会诱导用户激活系统设备管理器、隐藏自身启动图标、拦截用户短信并将短信内容发送到指定号码、还涉及登陆、支付等相关功能，给用户造成严重的隐私泄露等安全问题。



图 37：病毒伪装“交行安全控件”

5. “短信拦截马”病毒来袭，谨慎点击带有链接的短信息

2016 年 3 月，“短信拦截马”病毒卷土重来，在社会上爆发式扩散传播，中招用户和受骗用户也随之越来越多。此类木马最常见的手法是利用“你干过的事情别以为没有人知道”、“看你做的龌龊事”、“教育课程”、“移动兑换积分”等语句来诱导用户下载安装，在安装运行后病毒会在后台拦截和转发用户手机中的短信内容，以此来获取用户的个人隐私信息，如用户姓名、手机号、身份证号、银行卡账户、短信验证码、支付密码及各种登录账号和登录密码等信息。同时，攻击者还可利用盗取的用户信息达到盗刷银行账户、偷取用户财产的目的，直接威胁到用户的个人隐私和财产安全。

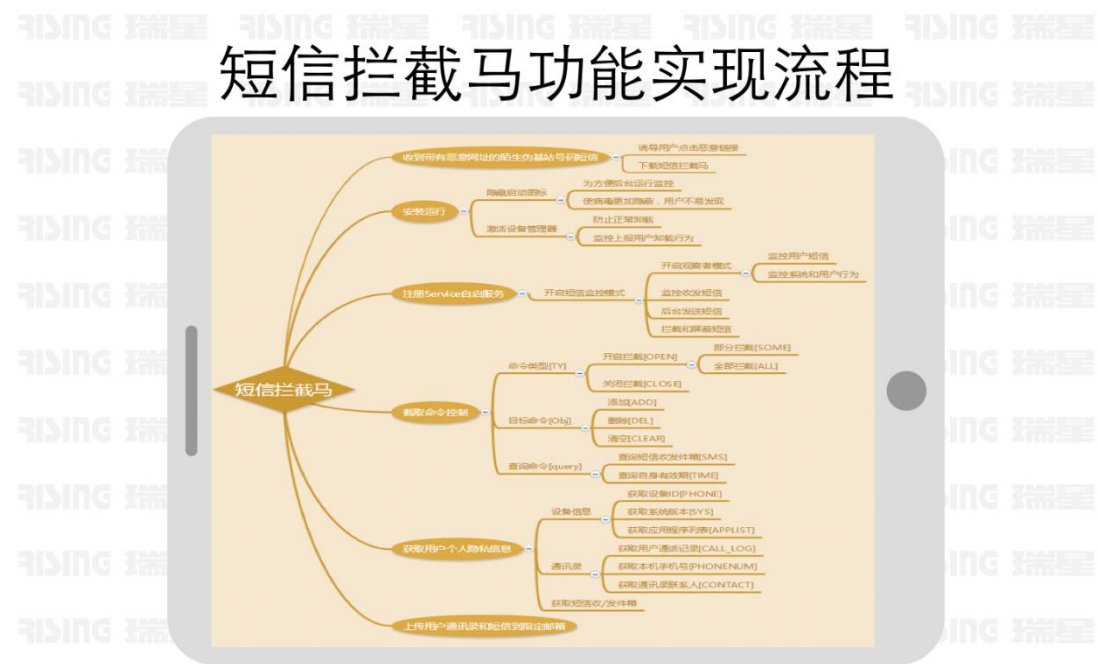


图 38：短信拦截马功能实现流程

三、企业信息安全

（一）上半年全球重大网络安全事件

1. 恶性敲诈软件国内大爆发

2016 年上半年，一类名为“密锁”的敲诈型恶性病毒开始在国内突然爆发，该类病毒通过电子邮件传播，一旦用户点击带毒附件，电脑中的各类文档、隐私文件都将被病毒“上锁”，如不按黑客要求付款，将永远无法恢复正常。据介绍，密锁病毒（敲诈软件）最早起源于 1996 年，2016 年开始大面积感染中国地区，并且技术支持活跃、更新频繁，给

广大用户带来严重的安全威胁。根据瑞星“云安全”系统数据显示，2016年1至6月，瑞星“云安全”系统共截获敲诈软件样本13.45万个，感染共计659万次，安徽、广东、浙江、北京、山东等地受此病毒威胁最大。

2.乌克兰电网遭黑客攻击之 Black Energy

2016年1月6日，据英国《金融时报》报道，乌克兰电网系统遭黑客攻击，数百户家庭供电被迫中断，这是有史以来首次导致停电的网络攻击。此次针对工控系统的攻击无疑具有里程碑意义，引起国内外媒体高度关注。导致此次攻击的核心是一个名为 Black Energy（黑暗力量）的恶意代码，Black Energy 最早可以追溯到2007年，由俄罗斯地下黑客组织开发并广泛使用在 BOTNET，主要用于建立僵尸网络，对定向目标实施 DDoS 攻击。Black Energy 有一套完整的生成器，可以生成感染受害主机的客户端程序和架构在 C&C（指挥和控制）服务器的命令生成脚本。攻击者利用这套黑客软件可以方便地建立僵尸网络，只需在 C&C 服务器下达简单指令，僵尸网络受害主机便统一执行其指令。

3. 2.7 亿 Gmail、雅虎和 Hotmail 账号遭泄露

2016年5月，俄罗斯用户的 Gmail、雅虎及微软电邮 Hotmail 等隐私信息惨遭泄露。在此次泄露的数据中，黑客盗取了 2.723 亿个帐号，以俄罗斯最受欢迎的电子邮件服务 Mail.ru 用户为主，还包括至少 3300 万 Hotmail，4000 万雅虎以及 2400 万 Gmail 地址。此外，还包括成千上万的中国和德国电子邮箱地址服务器的信息等。

4.叙利亚政府网络被黑，泄露 43GB 数据

2016年4月6日，叙利亚政府网络被黑客攻击，43GB 数据遭到泄露，Cyber Justice Team（网络空间正义小组）称对此事负责。起初曝光的是 10GB 敏感信息，但是解压数据之后发现有更多的数据浮现出来。解压文件之后发现总共有 55 个国家、私人域名（过半的域名是 .gov.sy 政府域名），27.4 万份文件。据基于风险的安全（RBS）分析，这些数据已经传播至 Pastebin 网站上，包含服务器密码、MySQL 主机权限和管理密码。

5.匿名者 DDoS 攻击希腊银行网站

2016年5月，Anonymous（匿名者）组织以反对银行金融腐败为由，对希腊银行网站进行一系列大规模的分布式拒绝服务攻击（DDoS）攻击，迫使希腊银行网站服务器离线时间超过 6 小时。Anonymous 组织的“Oplcarus 运动”于 2016 年 1 月启动，2016 年 3 月重新启动。参与此次运动的 Anonymous 组织坚信银行和金融巨头都参与了金融腐败，他们不得不采取新一轮的战斗，来对抗银行金融腐败。Anonymous（匿名者）组织还发布了一则 YouTube 视频，解释其攻击原因及接下来会遭受攻击的一系列银行列表。这份名单涉及巴西，孟加拉国，中国，美国，英国，巴基斯坦，伊朗等多个国家的银行和金融机构。

6.德国贡德雷明根核电站发现病毒

2016 年 4 月，根据德国 BR24 通讯社的报道，贡德雷明根核电站的一个系统中发现了病毒。根据专家作出的初步评估，这个病毒没有对核电站的关键部分造成影响，也不会构成重大威胁。审计表明，与 Stuxnet 不同，这款病毒不是为核电站设计的，而是一款普通的病毒。可能的感染渠道之一就是病毒通过某个员工所使用的 U 盘被带入贡德雷明根核电站。

7.全球 2.5 万网络摄像机被黑，用于构建僵尸网络

2016 年 6 月，据一份研究报告显示，黑客攻破了大量的网络摄像机，在网上发起 DDoS 攻击，有目的地对那些大型网站进行打击。被黑的网络摄像机 IP 地址分布在世界各地，不少于 105 个国家，总数量超过 2.5 万。由于安全标准和管控制度的缺失，目前脆弱的网络嵌入式设备，包括智能电视、冰箱、微波炉、机顶盒，摄像机以及联网打印机经常会被黑客盯上。此类智能设备被黑客入侵后，不但可以用于发动特定攻击，还可以直接盗取用户隐私信息，甚至偷拍隐私视频。

8.日本 16 州 ATM 机沦陷，14 亿日元不翼而飞

2016 年 5 月，据新闻报道，一伙罪犯团伙在日本的 16 个州，包括东京、大阪、福冈、神奈川、爱知、长崎、兵库、千叶和新泻等地同时在 1400 台便利店 ATM 机中取出现金。很多 ATM 被盗事件都涉及到一个出现很久的名为“ATM Skimming”的科技手段，犯罪份子通过磁条、或使用 ATM 恶意软件、或数据泄漏等方式获得信用卡或银行卡的详细信息，然后通过所谓的“carder”和钱螺窃取现金或进行网上购物。

9.超 3200 万 Twitter 账户密码泄露

2016 年 6 月，LinkedIn、MySpace、Tumblr 还有 VK.com 都相继曝出被俄罗斯黑客攻陷，大量用户数据在黑市倒卖。来自 Leaked Source 的消息，俄罗斯社交网站 VK.com 遭入侵，1.71 亿用户帐号信息泄露，泄露这些信息的黑客名为 Tessa88。而 Twitter 这次泄露的数据信息同样来自此人：超过 3200 万 Twitter 用户的登录信息正在暗网黑市出售，价格为 10 比特币（超过人民币 38000 元）。泄露的信息内容包括这超过 3200 万 Twitter 用户的用户名、邮箱地址，还有明文密码。黑客首先获得的其实是 LinkedIn 的泄露数据，并且破解了 SHA1 哈希过的密码，随后黑客再利用这些获取到的信息，成功进入了 Twitter 和 Pinterest。

10.俄罗斯最大社交网站 VK.com 被黑，1.71 亿用户账号仅售 1 比特币

2016 年 6 月，俄罗斯最大社交网站 VK.com 被黑客入侵，1.71 亿名用户账号信息泄露。此次被盗的 VK.com 网站数据库中，包括完整的用户名、电子邮件地址以及纯文本密码，很多账号还包括有位置和电话号码信息。该黑客组织在网络黑市上兜售了其中的部分账号数据

——涉及 1 亿个账户，容量约为 17GB。不过令人匪夷所思的是，他们在黑市上对这些数据的要价仅为 1 比特币，约合 580 美元。

11.MySpace 出现史上最大规模数据泄露事件

2016 年 5 月，有新闻曝光了 1.17 亿条 LinkedIn（领英）数据被泄露的消息，而最新的消息是社交网站 MySpace 也遭到了数据泄露，而泄露的数据比领英还要多。早在 2007 年底，MySpace 的 Alexa 全球排名已经稳定在第六名。曾有数据显示，每个 MySpace 的注册用户的平均浏览页面数高达 30 以上，用户粘性极强。而这次事件的主导者就是上次售卖超过 1.64 亿 LinkedIn 用户数据的同一个黑客，而现在该黑客宣称已经拿到了 3 亿 6000 万 MySpace 用户的电子邮件地址以及密码。

12.卡塔尔国家银行被黑，1.4G 数据泄露（涉及王室、英国军情六处、法国和波兰等各国情报）

2016 年 4 月，匿名黑客组织宣布攻破了卡塔尔国家银行系统，并在 Cryptome 网站上公开了从卡塔尔国家银行 (Qatar National Bank) 窃取容量超过 1.4GB 的数据转储文件。数据包含该银行客户资料、密码、PIN 码、支付卡数据、家庭住址、电子邮件和其他 PII（个人识别资料）数据等。此外，黑客还宣称窃取了卡塔尔王室 Al-Thani 以及卡塔尔 Al Jazeera 电视台记者的银行信息。访问过该泄露数据库的人都会被泄露数据中的一个标记为“间谍”的文件夹所吸引。浏览后发现，该文件里面包含了卡塔尔王室数据，卡塔尔国防部和各种情报机构信息，甚至涉及英国（军情六处），法国和波兰等国情报信息。

（二）政府、金融、互联网、教育类网站将遭受 Struts2 漏洞攻击

1.Struts2 漏洞概述

Struts2 应用于大型网站开发中，是网站开发中必不可少的开发组件，在 2013 年 6 月底发布的 Struts 2.3.15 版本被曝出存在重要的安全漏洞，主要问题如下：

1) 可远程执行服务器脚本代码，用户可以构造：

```
http://host/struts2-blank/example/X.action?action:%25{(new+java.lang.ProcessBuilder(new+java.lang.String[]{'command','goes','here'})).start()}链接, command goes here 可以换成是破坏脚本的路径和参数, 比如 fdisk -f 等, 造成破坏系统无法运行的目的。
```

2) 重定向漏洞

用户可以构造如知名网站淘宝的重定向连接，形如<http://www.taobao.com/item00001.html?redirect:http://www.hacker.com/getyourPassword>”，引导用户点击后进入钓鱼网站，在界面上让其进行登陆用以获取用户的密码。

3) 影响范围

对各大互联网企业均造成的一定的影响，如修复不及时被黑客利用将可能导致用户信息泄露。



图 39：受影响的互联网企业

2.Struts2 漏洞引发的攻击

从 2016 年 3 月起，Struts2 相继暴露多个高危害漏洞，这些漏洞都是可远程代码执行，通过执行恶意代码对远程服务器实施攻击。

在 4 月底，Apache Struts2 爆出新一轮的远程代码执行漏洞，该漏洞的出现导致了多行业领域单位网站遭受攻击。

根据国家安全漏洞库查询分析，近半年期间，Struts2 造成的严重漏洞就达 10 多个。高峰时期为 4 月份至 6 月份造成的高危漏洞。数据来源：（国家信息安全漏洞共享平台）

2016上半年高危害漏洞统计

漏洞标题	危害级别	点击数	评论	关注	时间↓
> Apache Struts2远程代码执行漏洞 (CVE-201...	中	518	0	0	2016-06-20
> Apache Struts2远程代码执行漏洞 (CVE-201...	中	467	0	0	2016-06-20
> Apache Struts2远程代码执行漏洞 (CVE-201...	中	481	0	0	2016-06-20
> Apache Struts2远程代码执行漏洞 (CVE-201...	中	478	0	0	2016-06-17
> Apache Struts2远程代码执行漏洞 (CVE-201...	中	502	0	0	2016-06-17
> Apache Struts2远程代码执行漏洞 (CVE-201...	高	966	0	0	2016-06-16
> Apache Struts 1跨站脚本漏洞	中	396	0	0	2016-06-13
> Apache Struts 1存在多个漏洞	中	391	0	0	2016-06-13
> Apache Struts2拒绝服务漏洞	中	823	0	0	2016-06-06
> Apache Struts2远程代码执行漏洞 (CVE-2016...	高	1169	0	0	2016-06-03
> Apache Struts XSSResult任意代码执行漏洞	高	1162	0	0	2016-04-29
> Apache Struts2远程代码执行漏洞 (CVE-201...	高	2364	0	0	2016-04-25
> Apache Struts Oracle JRE跨站脚本漏洞	中	809	0	0	2016-04-19
> Apache Struts IIORInterceptor跨站脚本漏洞...	中	1358	0	0	2016-03-17
> Apache Struts2远程代码执行漏洞	高	1806	0	0	2016-03-17
> Apache Struts安全绕过漏洞 (CVE-2016-012...	中	910	0	0	2016-02-24

图 40：2016 上半年高危害漏洞统计

3.漏洞攻击分布监测

根据 CNCERT 在互联网上的监测结果，在 2016 年 3 月 25 日到 6 月 2 日互联网上针对该漏洞的攻击和扫描尝试保持在高位状态。尽管后续评估认为本次 S2-032 漏洞较以往 S2-016 漏洞的检出率要低得多，但针对特定目标的搜寻（如：利用搜索引擎查找 action 页面）以及后续的攻击扫描仍然在黑客地下产业或网络安全从业者中持续进行。

S2-032攻击和扫描次数监测统计

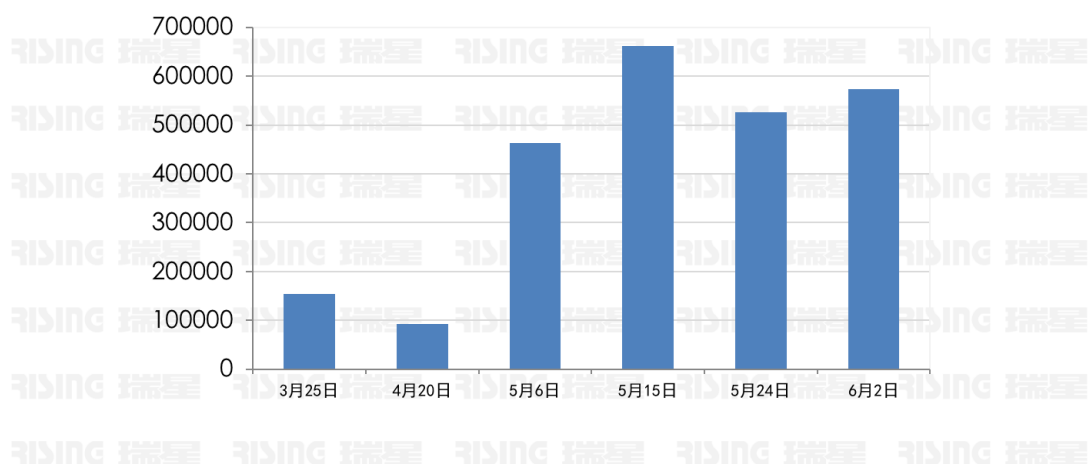


图 41：S2-032 攻击和扫描次数监测统计

根据互联网统计后的结果对 706 个采用 Apache Struts2 作为容器软件的网站进行测试，有 29 个网站存在 S2-032 漏洞，占比 4.1%，而存在 S2-016 及更低版本远程代码执行漏洞（如：S2-005）的网站有 196 个，占比 28%。为进一步评估 S2-032 漏洞在各行业领域单位网站的分布情况，如下表所示，境内共有 817 个网站存在 S2-032 漏洞，其中按行业领域划分，位于前三位（注：不计其他企业）的是政府部门（占比 28.3%）、互联网企业（25.3%）、教育机构（9.8%）。

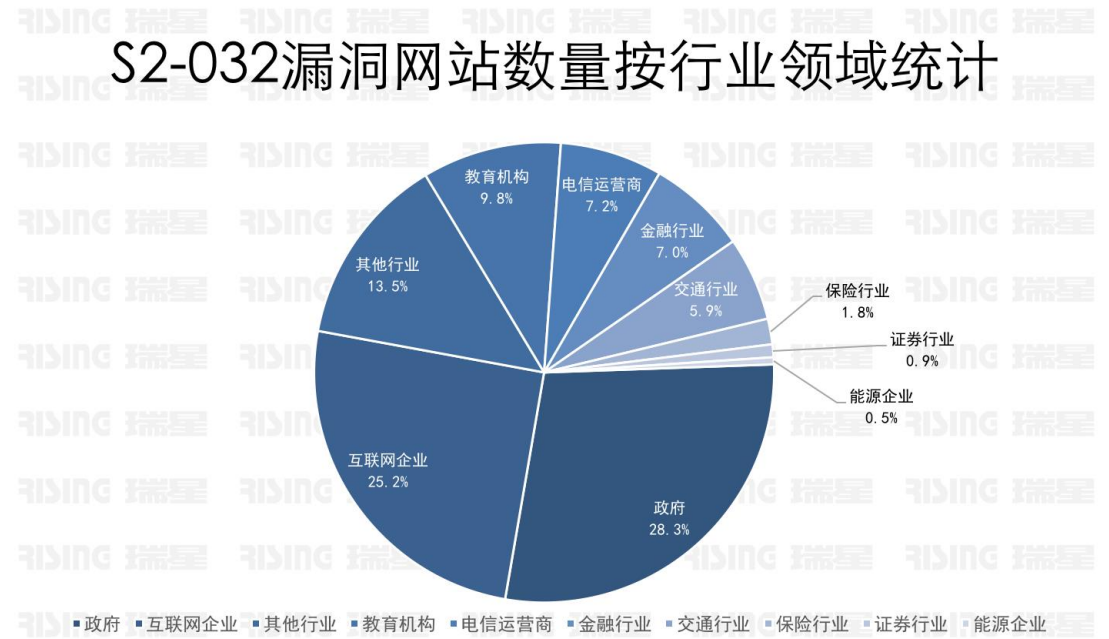


图 42：S2-032 漏洞网站数量按行业领域统计

根据发布的 Struts2 漏洞安全公告发现，从 2010 年 Struts2 就爆发高危漏洞，但在近年来高危漏洞频发，由于使用 Struts 框架的互联网企业较多，这些漏洞存在着潜伏期的危害，将可能导致互联网企业内部信息的泄露。

历年Struts2高危漏洞统计

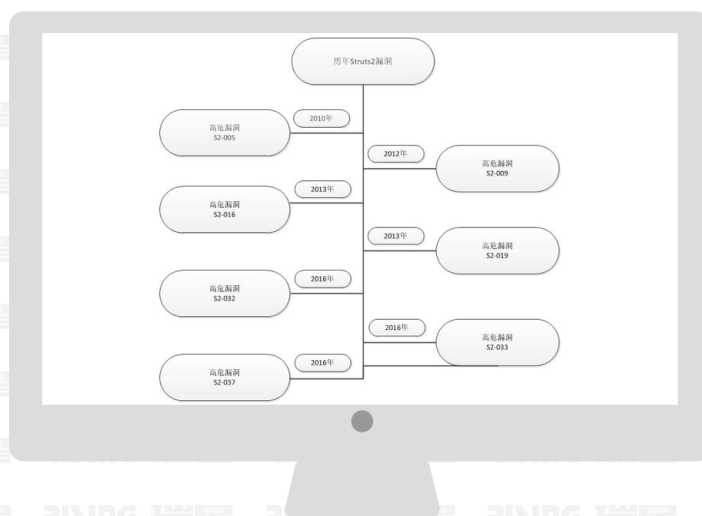


图 43：历年 Struts2 高危漏洞统计

4. 漏洞攻击造成的危害

由于 Struts 架构广泛应用于政府、大型互联网企业、金融机构等网站建设，并作为网站开发的底层框架使用，所以此次补丁绕过漏洞可能使大量政府、门户、电商、银行等网站遭受恶意攻击。电商、银行等网站，很容易导致用户帐号密码丢失，门户、政府网站由于在用户心中可信度较高，很容易被不法分子利用，通过发布钓鱼欺诈链接诱使网民受骗。

相比 Spring MVC 而言，在安全上 Spring MVC 比 Struts 相对安全。但很多企业还是选择使用 Struts2 框架，因为 Struts2 有自己独特的优点。Struts 在 M、V 和 C 上都有涉及，但它主要是提供一个好的控制器和一套定制的标签库上，Struts 有 MVC 所带来的一系列优点，如：结构层次分明，高可重用性，增加了程序的健壮性和可伸缩性，便于开发与设计分工，提供集中统一的权限控制、校验、国际化、日志等等。

（三）大规模数据泄露使全球网民无秘

1.全球重大数据泄露事件

全球数据泄露事件统计			
泄露事件	泄露日期	所属公司类型	泄露用户数量
MySpace信息泄露	2008年数据泄露 / 2016年数据流传	传媒公司	3.6亿
LinkedIn信息泄露	2016年	互联网求职平台	1.7亿
VK.com信息泄露	2012年数据泄露 / 2016年数据流传	社交网站	9400万
Nival信息泄露	2016年	文化娱乐公司	153万
Naughty America 信息泄露	2016年	成人娱乐提供商	140万
Uiggy信息泄露	2016年	社交应用程序	268万
土耳其公民信息泄露	2016年	政府机构	5000万
Nulled.io信息泄露	2016年	黑客论坛	60万
Patreon信息泄露	2015年	音乐众筹网站	233万
Ashley Madison信息泄露	2015年	成人社交网站	3000万
HackingTeam信息泄露	2015年	软件开发商	3万
R2Games信息泄露	2015年	海外游戏代理商	1318万
Vtech信息泄露	2015年	玩具公司	480万
Adult Friend Finder信息泄露	2015年	成人交友网站	400万
mSpy信息泄露	2015年	监控软件开发商	70万
Beautiful People信息泄露	2015年	社交网站	110万
iPmart信息泄露	2015年	在线商城网站	246万
000webhost信息泄露	2015年	免费空间提供商	1354万
Snapchat信息泄露	2014年	社交平台	460万
mail.ru信息泄露	2014年	邮件服务商	482万
Forbes信息泄露	2014年	商业杂志	105万
tumblr. 信息泄露	2013年	轻博客平台	6500万
Adobe Photoshop信息泄露	2013年	软件服务供应商	1.5亿

图 44：全球数据泄露事件统计

我们可以通过上面数据看出，数据泄露的公司类型大致集中在社交网站和互联网科技公司。而其中尤其以成人社交网站最为严重，接下来我们从几个方面入手来分析一下攻击者的动机。

2.社交网站、色情网站成数据泄露“大头”

公司平台类型数量统计		
平台类型	公司	数量
社交平台	LinkedIn、VK.com、Uiggy、Nulled.io、Ashley Madison、Adult Friend Finder、Beautiful People、Snapchat	8
传媒公司	MySpace、Nival、Forbes	3
互联网公司	HackingTeam、mSpy、Adobe Photoshop、000webhost、mail.ru、tumblr	6
其它	Naughty America、土耳其公民信息、Patreon、R2Games、Vtech、iPmart	6

图 45：公司平台类型数量统计

数据泄露的公司类型比例

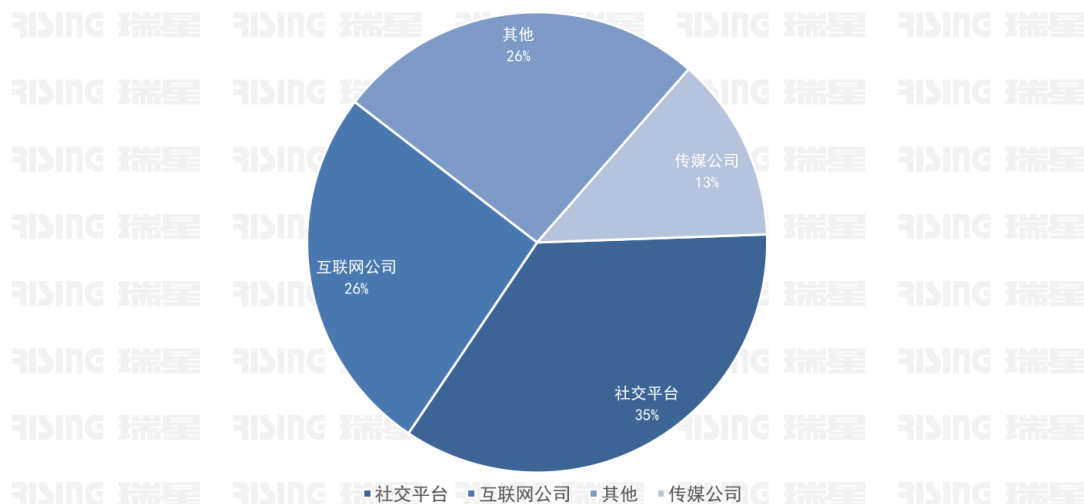


图 46：数据泄露的公司类型比例

社交网站和互联网科技公司的主要业务集中在线上，注册用户相对较多，人员信息较为完善，相对于传统行业，数据更容易获取。其次，类似于社交网站的平台用户群体数量庞大，即时性强，个人信息更新速度快，符合黑客需求。大多数黑色产业链所需数据要求保持“新鲜”，如果数据太过于陈旧，或者内容较少，就失去了一定的利用价值。其中，国外信息泄露事件的重灾区主要是成人社交网站，很大一部分原因是这种成人社交网站具有很强的隐私性，而黑客天生就对这些信息有很强的窥探欲与占有欲，同时，这类型的数据也满足地下黑色产业链的需求。被窃取的数据信息大部分都会流入到黑色产业链中，当其中的利用价值被榨取殆尽后，才会浮现到大众的视线里。以列表中的数据来讲，大多数是经过黑产售卖流通之后才被曝光的。

3.基于被泄露的用户量分析

从全球重大数据泄露事件的数据中可以看出，互联网科技公司和社交平台的用户量大都在百万级别，其中更是不乏上亿级别的存在。如此多的用户覆盖了各行各业，不仅交易价值极高，数据的分析价值也很高。通常用户数据泄露后的流向有如下几方面：

用户数据泄露后的流向

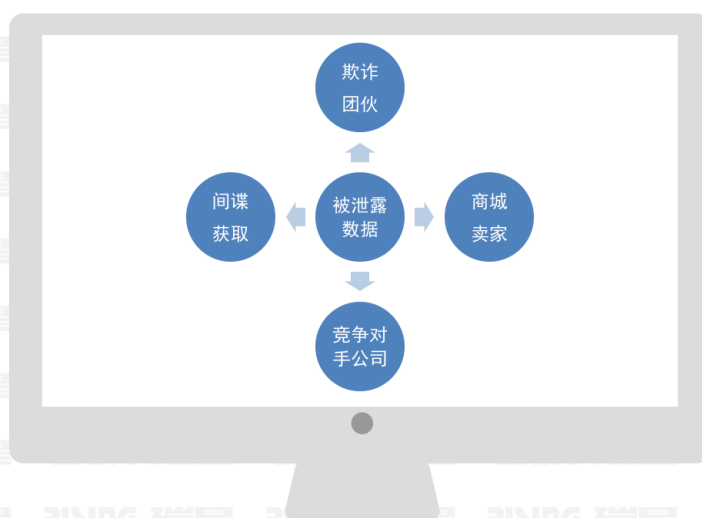


图 47：用户数据泄露后的流向图

通过这些被泄露数据的流通走向，我们可以看到一些利益集团的背影和不良意图。这些流向均是围绕个人信息衍生出的利益链条，这些利益或是携带社会以及利益团体的因素，或是携带攻击者自身的意图因素。

4.商业和政治为数据泄露主要原因

我们来分析一下基于个人因素的一些判断。部分攻击者会将窃取到的数据售卖给他人，从而获取相应的金钱报酬。而这其中又分为：黑产人员和普通的攻击者。黑产人员会根据雇主指定的目标去进行入侵，窃取指定的数据；普通的攻击者是将数据售卖给一些需要数据的下家。而将数据公布在网上的行为，大部分是为了进行炫耀，用以招揽一些崇拜者或者追随者。

从社会因素的角度来分析的话就要复杂的多，例如：商业原因、政治原因等。商业原因：竞争对手进行恶性竞争，毁坏对手公司的业界声誉等。政治原因：阻止选举、反对种族歧视等。最为出名的就是世界级黑客组织——匿名者组织，经常会发布一些带有政治性质的网络攻击宣传视频。

用户数据泄露背后的动机

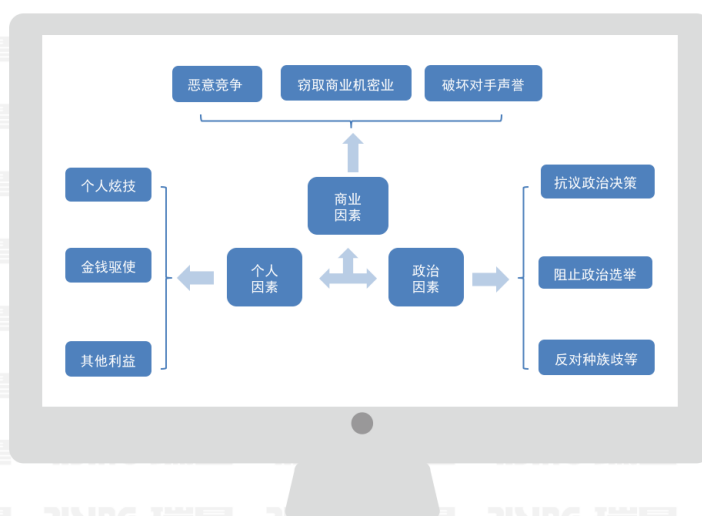


图 48：用户数据泄露背后的动机

5.Java、Flash 和 IE 最受攻击者青睐

CVE漏洞企业分布比例

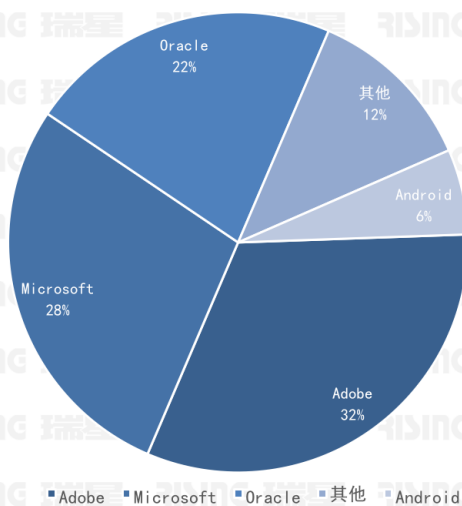


图 49：CVE 漏洞企业分布比例

从图中可以看出，Adobe、微软和甲骨文公司是数据泄露漏洞较多的企业，这里面的原因是大部分企业所使用的软件 90%均来自这三家公司，不仅涉及企业员工所使用的操作系统环境，而且涉及到网络办公所使用的第三方软件环境。

第三方软件CVE分布比例

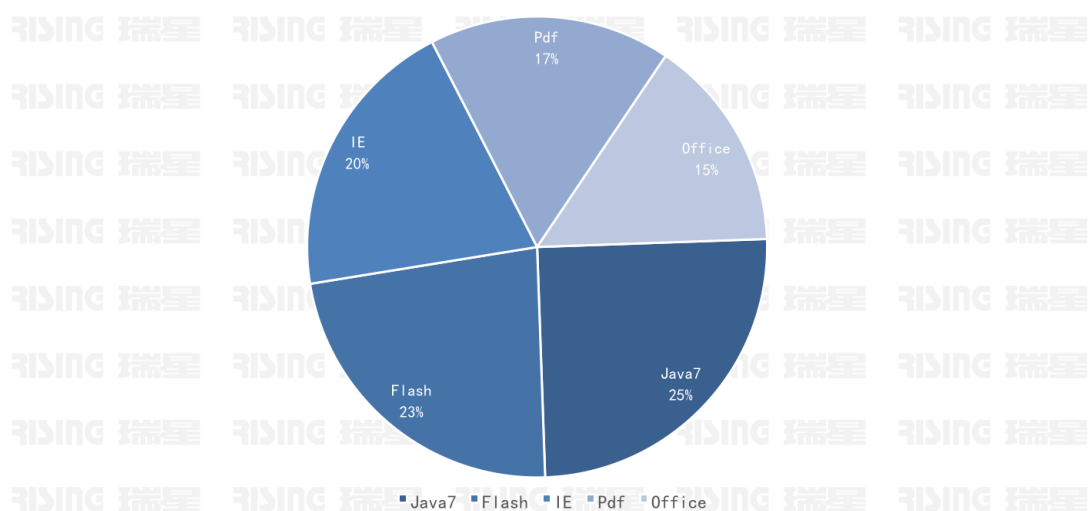


图 50：第三方软件 CVE 分布比例

从图中可以看出，针对企业的攻击主要针对浏览器溢出和文件溢出类型的 CVE，主要是因为针对企业的攻击多数采用邮件“鱼叉式攻击”和“水坑攻击”。

CVE公开时间分布比例

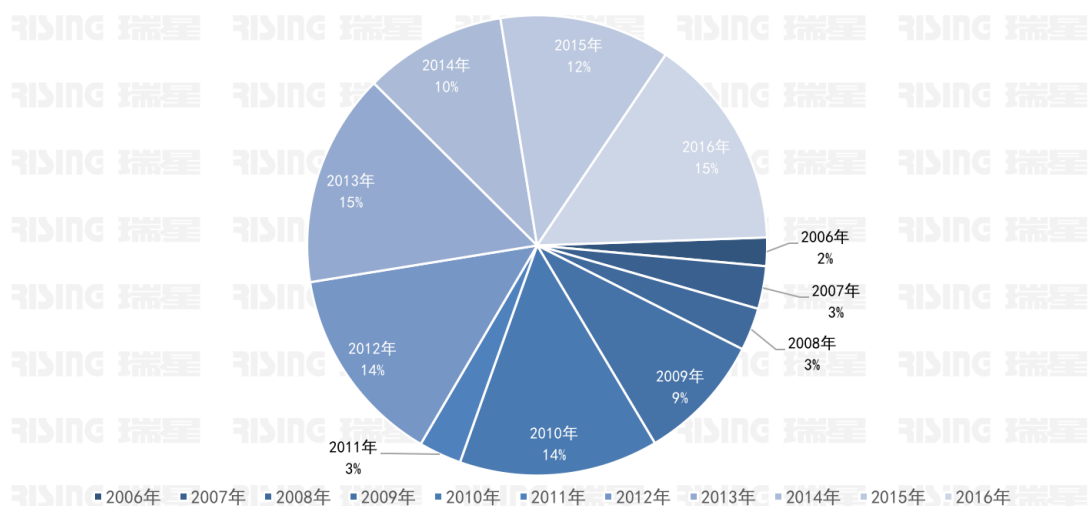


图 51：CVE 公开时间分布比例

从 CVE 公开时间 2006-2016 年近 10 年的 CVE 个数可以看出，新漏洞利用较少，或者说有组织的国际黑客手里有成熟稳定的 exploit，只有在遇到有价值的企业或目标才使用较新 CVE exploit。而相对时间较远的如 2012-2013 年所发布的 CVE 可以看出，老旧的 CVE 不仅网

上公开并且相对 exploit 利用较稳定容易实施攻击。

CVE Exploit攻击次数统计TOP10

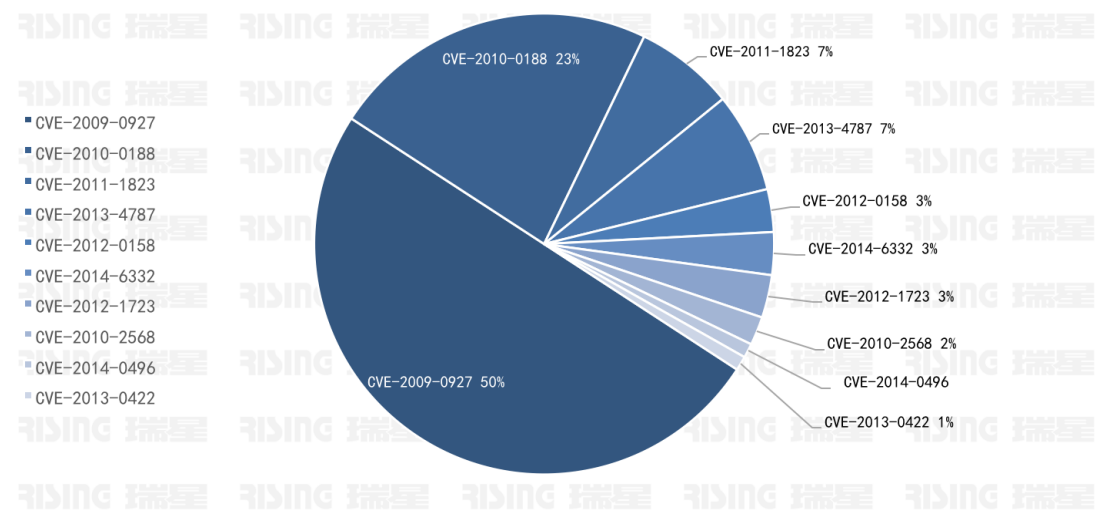


图 52： CVE Exploit 攻击次数统计 TOP10

CVE-2009-0927 为 Adobe 下产品漏洞，根据企业漏洞和攻击次数的统计分析可以看出，Adobe 公司虽然企业使用广泛，但企业所使用的 Adobe 软件并没有及时更新，所以旧的 CVE 会直接触发漏洞导致企业内部遭受恶意攻击。

2014-2016年CVE攻击次数比例

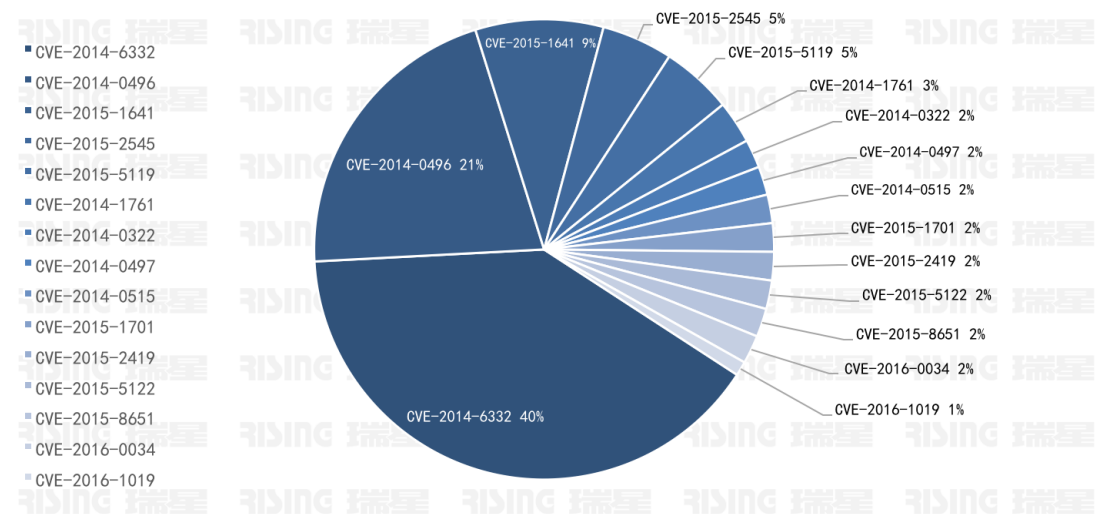


图 53： 2014-2016 年 CVE 攻击次数比例

根据瑞星云捕获到的 CVE-2015-8651 漏洞虽然攻击次数较少，但是该漏洞是某境外组织对国内企业进行 APT 所使用的重要漏洞。而 CVE-2016-1019 漏洞是 Adobe 漏洞，影响包括 XP/Win7/Win8.1/Win10，以及 Linux、Mac 和 Chrome OS 等操作系统。

6.数据泄露事件的影响

数据泄露事件的影响特点：范围广、涉及人员多，影响恶劣。其中受害最为严重的便是用户本身。用户的个人信息在被泄露之后，可能会被无数的欺诈电话、推销电话骚扰，而且所注册过的所有互联网账户都有可能存在被再次窃取的安全风险，整个人的生活成为透明状态被曝光到互联网中，最主要的我们财产也时刻存在着安全隐患。

其次便是受到攻击的互联网科技公司以及相关的社交网站。影响体现在如下几个方面：第一，客户流失，业务受影响；第二，公司信誉及影响下降；第三，针对上市公司，很可能由于用户信息的泄露造成股价的跌宕，并时刻面临着公关危机。

政治方面，同样受其影响。国外经常有为了阻止选举或者法案决策的通过发动的黑客攻击。或者是反对某种政治行为的黑客抗议行为，其中最具政治性的黑客组织便是匿名者。而受到攻击的政治活动，往往因为黑客攻击而人气下滑，导致选举或者决策失败。

总而言之，由于黑客攻击事件导致的用户数据泄露导致对用户个人，社会经济，政治等影响都是极大的。因此做好安全防御，提高安全意识的任务刻不容缓。而这需要我们共同去建设一个相对安全的互联网空间，降低因数据泄露对我们造成的困扰。

四、趋势展望

（一）敲诈软件依然是低成本高收益网络犯罪主流

敲诈软件在过去取得了巨大的“成功”，使得敲诈软件的种类、攻击范围、攻击目标越来越多，受害者数量也持续上升。同时，2016 上半年出现的新兴的敲诈软件中，充斥着大量使用了对称加密算法的变种，被它们加密的文件实际上是可以还原的。这类犯罪者，仅仅是想借 Locky/CryptXXX 等知名敲诈软件给人们带来“文件无法解密还原”的主观判定，以更低的成本和技术难度，达到成功勒索的目的。

同时，敲诈软件似乎已经盯上了企业，同个人数据相比，企业数据显得更加重要，勒索成功率会大幅上升。为了遏制敲诈软件带来的危害，产品提供商、安全提供商、政府都在做出相应的努力。例如：安卓系统将采用新的机制来遏制锁屏（Trojan.SLocker）类敲诈软件的攻击，政府和安全厂商有都在尝试追踪比特币交易来定位犯罪者。未来，敲诈软件也一定会因为法律的震慑作用而有所收敛。

（二）政治色彩严重的网络攻击已波及民生领域

2016 年上半年，乌克兰电网、叙利亚政府、希腊银行、德国核电站等遭到黑客攻击，可以看到，电力、能源、交通等与民生相关的行业已经成为政治化的网络攻击的首要目标。一旦攻击成功并实施破坏，民生便会受到影响，近而加深了民众对当前政府的不满情绪。这种攻击必定是政治目的的驱动，攻击伊朗核电站的 Stuxnet 仅仅是为了毁掉一个核电站，那乌克兰遭受到的网络攻击所承载的最终目的，便是推翻政府。由此可见，网络攻击已经成为一项重要的政治武器。

（三）大规模数据泄露事件频发，云安全问题应得到高度重视

无论是国家、还是企业、甚至是个人都正在遭受数据泄露的风险，数据泄露问题应该得到每一个人的高度重视。“云安全”是“云计算”技术的重要分支，已经在反病毒领域当中获得了广泛应用。云安全通过网状的大量客户端对网络中软件行为的异常监测，获取互联网中木马、恶意程序的最新信息，推送到服务端进行自动分析和处理，再把病毒和木马的解决方案分发到每一个客户端。

总之，云计算产业具有巨大的市场前景，云安全的发展给网络时代互联网的安全提供了更大的可能性，它将是未来市场发展的趋势，我们需要能发挥它的优势而规避其劣势，将虚拟化技术与云安全技术有机结合，实现完全意义上的云安全，只有安全得到保障，才能打破用户顾虑，使云计算得到更快、更深入的发展，让每个用户在享受云计算带来的便利时也成为识别安全威胁的贡献者。

（四）第三世界金融系统成为黑客的提款机

2016 年上半年，震惊全球的孟加拉央行盗窃事件被披露，被盗金额 8100 万美元，成为史上最大的银行盗窃案。5 月，越南先锋银行披露遭遇到与孟加拉央行一样的攻击，所幸被机制阻止。在这些攻击中，黑客不仅对目标银行的工作流程、员工工作习惯、内部管理制度漏洞了如指掌，也对 SWIFT 系统颇为熟悉，通过损坏打印机、替换 PDF 阅读软件、劫持 SWIFT 终端最终完成了这起神奇的盗窃案。由于基础设施、安全意识、职业操守等各方面的因素，第三世界国家的金融系统似乎已经成为黑客攻击的主要目标。虽然已经得手的黑客会金盆洗手，事件披露也一定程度上会遏制此类攻击，但绝对不能排除效仿者的跟进。

专题：你可能不知道你正在被偷窥

2016 年智能摄像头、智能手机引发的艳照门、偷窥门事件（三里屯、陆家嘴、宜家……）让互联网这个暗流涌动的大海彻底沸腾了。智能摄像头在给我们带来便利的同时，也存在着极大的安全隐患。

下图是某国际网站流出大量通过智能摄像头拍出的情侣生活照，其中记录了大量的用户隐私照片。

国际网站流出大量私密照片

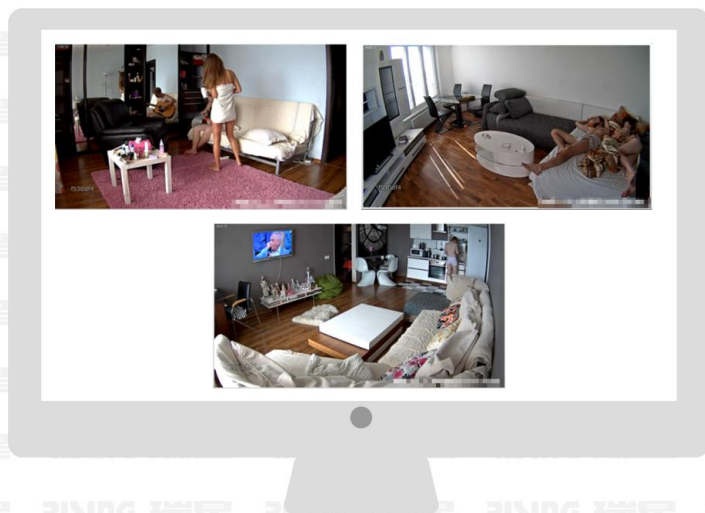


图 54：国际网站流出大量私密照片

国内某品牌摄像头也流出大量隐私照片：

国内某品牌摄像头流出大量私密照片

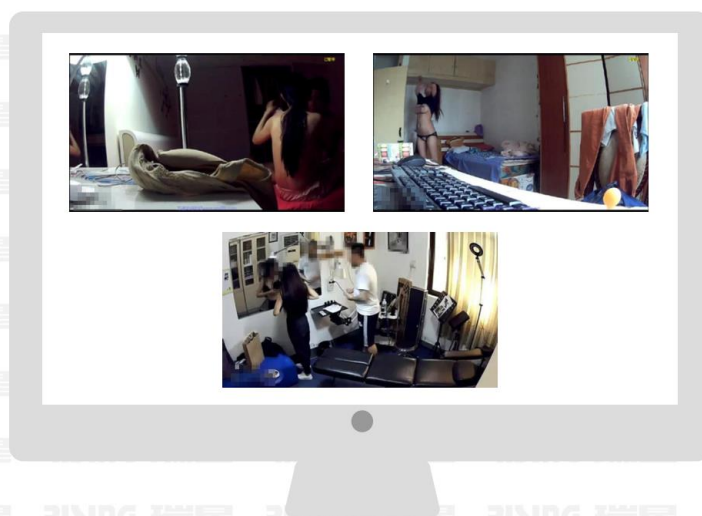


图 55：国内某品牌摄像头流出大量私密照片

从以上泄露的照片中可以看出，大部分照片都是在用户不知情的状况下泄露的。对于智能摄像头来说，使用最普遍的功能就是用来看家防盗、看护老人和孩子，可是在用它来保护我们的同时，却给我们带来了很大的安全隐患。

瑞星通过对国内某知名论坛进行数据分析发现类似于“偷拍”、“隐私”、“泄露”这类词语出现的频率很高，这说明一部分人更愿意关注这些方面，同时也说明隐私问题对于普通人来说的重要性。

国内某知名论坛关键词TOP10

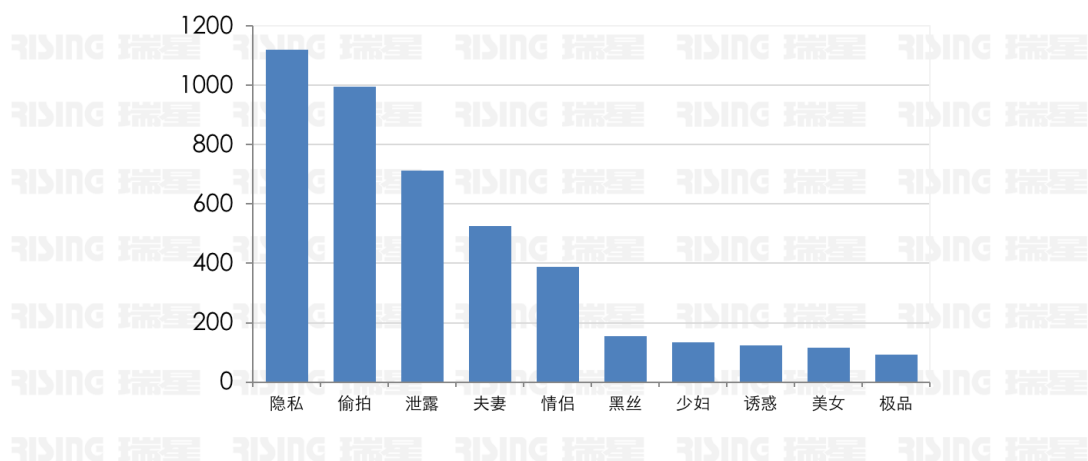


图 56：国内某知名论坛关键词 TOP10

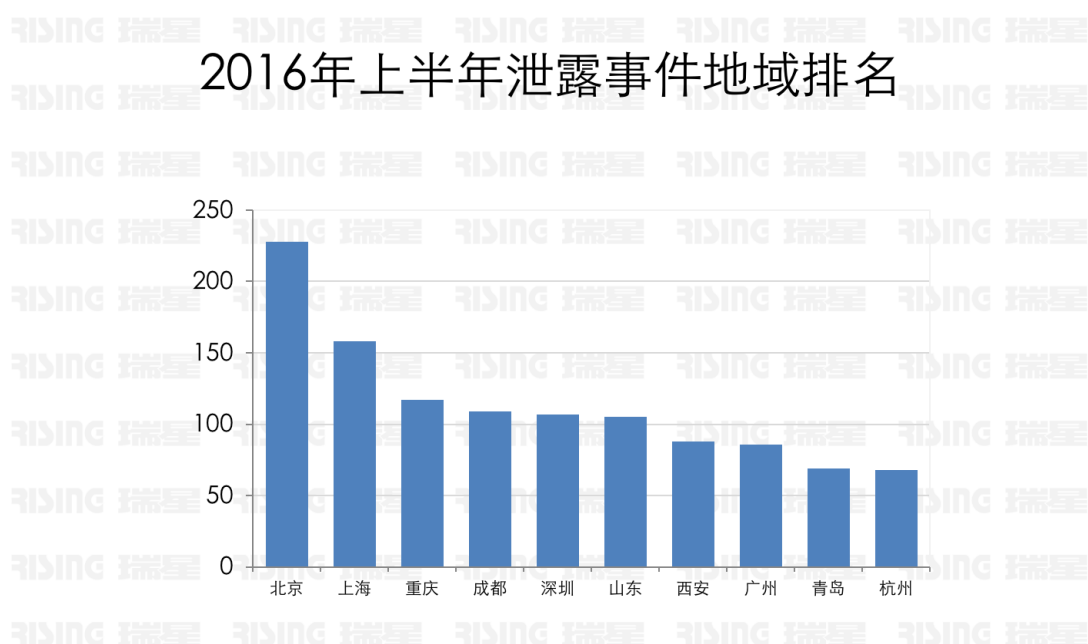


图 57：2016 年上半年部分地区出现次数

通过以上柱状图我们可以发现，在网上流传的偷拍、泄露视频中“北京”、“上海”、“重庆”等关键字出现频次最多。这说明在大城市中网民隐私存在的安全风险更高，这可能源于这些城市的智能化生活普及率高，很多家庭已经使用上了智能设备。从简单的智能手环、智能电视、智能摄像头，再到智能家居，我们的生活变得越来越智能化，可是越是智能化，存在的漏洞就越多。

接下来，我们分析一下黑客们的偷窥方式：

一、木马偷窥

早在 10 年前的“灰鸽子”时代，人们就对灰鸽子的摄像头的功能就情有独钟，再到“gh0st”时代作者优化了摄像头录像功能，高清录像功能让越来越多的黑客做起来利用浏览器挂马，各种第三方软件捆绑木马、下载者等情况。而归根到底就是为了窥视个人生活隐私。当下利用偷拍论坛数据再一次使用大数据进行论证的时候发现，2016 年人们对他人的“隐私”更加充满窥视的欲望。

二、智能设备

智能设备从 2010 年开始风起云涌，Android 手机变成一个高清自拍设备，存储着大量的个人隐私数据。基于 Android 的木马也逐步进入市场，而 Android 的木马功能最有价值的不是摄像头而是语音和文件传输。通过语音窃取周围声音，文件传输则窃取手机持有者自己拍摄的生活照，不仅图像清晰而内容更加真实。而手机只是智能设备的一种，还有一种则是智能摄像头。2016 年初，由于某厂商的智能摄像头默认是开启分享模式，导致大量用户装在

卧室，客厅等位置摄像头被公开直播引发了隐私泄露事件。

由于互联网智能设备发展迅速，而对于智能设备的安全没有得到足够重视，早在 2014-2015 年，大量的无线路由器由于配置不当或者存在后门等情况遭到了攻击。现在大量的安全研究人员发现智能摄像头由于使用互联网进行通信，也同样存在大量的安全漏洞导致摄像头被不法分子利用。

瑞星安全专家建议，首先在购买摄像头时，应对所选品牌进行一些调查，可以通过互联网查询与目标品牌相关的帖子或报道，“目的就是找到一个口碑不错，价格也合适的品牌”。

第二，在使用时，要注意设置一定强度的密码，及时关注摄像头软件的提醒。如果绑定的手机上发现了请求验证码的短信，就应该立刻修改密码。

第三，经常登录摄像头进行查看，如发现实际拍摄角度与安装时发生变化等情况，就需要考虑自己的账号安全了。同时，要关注所用品牌摄像头安全方面的消息，如果发现设备漏洞应停止使用，等待厂家更新，并保证所使用的摄像头软件是最新版本。