2018广东省移动互联网应用安全态势报告

国家计算机网络应急技术处理协调中心广东分中心

2018年11月

提纲

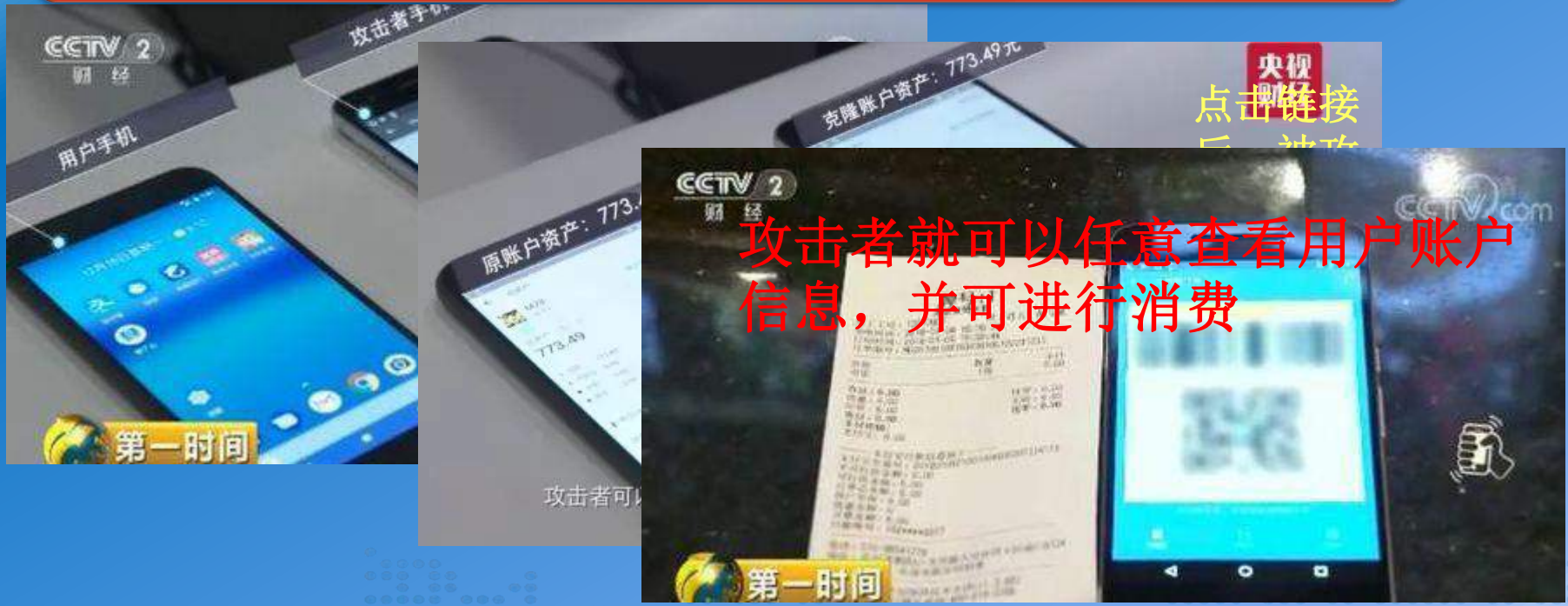
一 移动互联网应用安全形势

二 2018年移动互联网应用安全态势

三 AI时代移动互联网安全防护建议与展望

典型案例一

应用克隆攻击，可直接盗取用户账号、个人隐私、资金



典型案例一

应用克隆攻击，可直接盗取用户账号、个人隐私、资金

漏洞特征

漏洞影响范围

漏洞主要对使用了WebView控件，开启file域访问且未按安全策略开发的Android应用APP造成影响。由于大部分开发人员安全开发意识不足，所以该漏洞影响范围较大。

漏洞利用方式

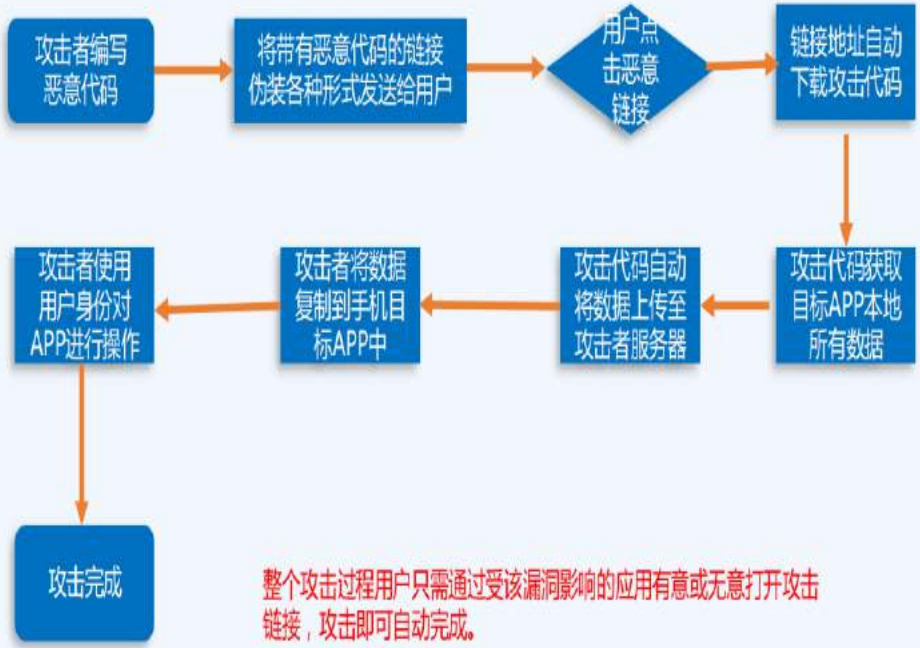
根据漏洞的特性，主要有三种利用方式：
1、通过聊天工具发送恶意链接让用户点击，即可利用该漏洞；
2、将恶意链接伪装成二维码让用户扫描，即可利用该漏洞；
3、通过在其他APP中植入恶意代码，用户打开程序即可利用；

漏洞危害程度

攻击者可以利用该漏洞远程复制特定APP存在本地的信息，包括登录凭证、密钥数据、照片、文档等敏感数据，利用这些数据就可以在攻击者自己的手机中完全拥有用户的权限，若APP没有对关键操作进行二次身份校验，则攻击者能够通过被攻击用户的身份进行APP内的所有操作。

漏洞修复难度

Google目前暂无针对该漏洞的修复补丁，所以需要APP的开发者通过修改WebView控件属性的方式来进行修复，由于漏洞影响较大建议强制最终用户更新APP版本。



典型案例二

旅行青蛙”游戏外挂藏风险

除了造成手机数据、资料丢失等，这类修改游戏金币(三叶草)的操作，对用户来说存在一定安全风险，“有时候可能会泄露用户的个人隐私，或是操作中，被安装一些木马软件，使设备在后续的使用中出现障碍”

典型案例三

恶意软件伪装“系统Wi-Fi服务”感染近五百万台安卓手机

这款名为“Rottensys”的恶意软件伪装成“系统Wi-Fi服务”，在供应环节上预装在数百万台全新的智能手机中，它们都是通过位于杭州的手机经销商发货的，受影响的品牌包括荣耀、华为、小米、OPPO、Vivo、三星和金力等。

黑客在过去10天内获得115,000美元

Date	Clicks	Impressions	Income (USD)
2018/03/12	50182	1207662	10,519.46
2018/03/11	52859	1352329	11,112.73
2018/03/10	53019	1315820	11,130.13
2018/03/09	52136	1293821	10,944.73
2018/03/08	56496	1306264	11,821.71
2018/03/07	57529	1326055	12,036.22
2018/03/06	56418	1321140	11,812.06
2018/03/05	55688	1342616	11,674.65
2018/03/04	58209	1395028	12,199.81
2018/03/03	56286	1390021	11,813.21
Total	548822	13250756	$115,064.7

典型案例四

会议App出现重大漏洞！英国多名高官信息遭泄露

近日，英国保守党的会议App出现漏洞，多位重要官员的个人信息遭到泄露，外界通过邮箱地址登陆后可看到与会人员的手机号码，并能够随意更改这些人的照片及其他信息，其中包括英国前外长鲍里斯·约翰逊、英国财政大臣菲利普·哈蒙德以及英国环境部长迈克尔·戈夫等

互联网移动化趋势明显

三大迁移

一、主体迁移（传统网民向移动网民转变），我国手机网民规模已达7.88亿，网民中使用手机上网人群占比提升至98.3%。

二、行为迁移（网络行为更多发生在移动端），移动互联网时代细分化的内容和多元化的渠道让用户行为分散在各个角落，包括社交平台、搜索、内容聚合平台以及各类工具型APP等。

三、信息迁移（信息内容更多在移动端传播），移动互联时代的到来不仅意味着互联网的移动化，同时也意味着信息与知识传播的移动化。

移动互联网应用安全-四大趋势

一、恶意代码

2017 年，CNCERT 通过自主捕获和厂商交换获得移动互联网恶意程序数量 253 万余个，同比增长 23.4%，仍保持高速增长趋势，通过对恶意程序的恶意行为统计发现，排名前三的分别为流氓行为类、恶意扣费类和资费消耗类，占比分别为 35.9%、34.3%和 10.4%。

二、安全漏洞

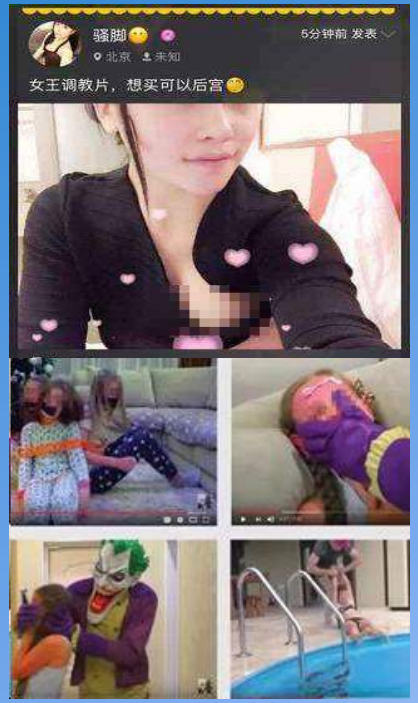
2017年移动应用安全漏洞数量规模累计超过2.8亿，相当于每一个移动应用含40个安全漏洞。移动应用在设计、开发、运行等过程中有意或无意产生的漏洞，很容易被病毒、木马、黑客等利用，导致用户信息、账号密码泄露，造成金钱财产损失。

1	webview远程执行漏洞
2	界面劫持漏洞
3	权限漏洞
4	篡改和二次打包漏洞
5	SharedPref读写安全漏洞
6	WebView组件忽略SSL证书验证错误漏洞
7	固定端口监听风险漏洞
8	数据弱加密漏洞
9	动态注册广播暴露风险
10	业务逻辑漏洞

移动互联网应用安全-四大趋势

三、应用仿冒

2017年，仿冒应用规模从2.3万+增长到2.8万+，累计下载量竟然已高达3000万次。仿冒应用通过名称、图标等维度的伪造，或者使用重打包等手段，不仅可以通过仿冒界面诱骗用户信息，还可以劫持短信，突破短信验证的防护；后台定制服务，恶意扣费；推广垃圾应用；甚至后台远程控制手机等设备。



四、内容违规

影音娱乐、社交通讯等类型的APP成为涉黄、涉赌、涉恐、涉暴等违规内容传播的温床。违规内容大肆在部分APP中传播，如果任由不良信息的散布，将污染网民视听，引起不良导向。

提纲

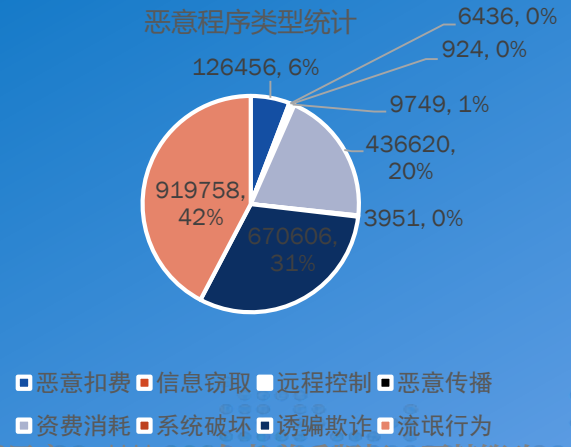
一 移动互联网应用安全形势

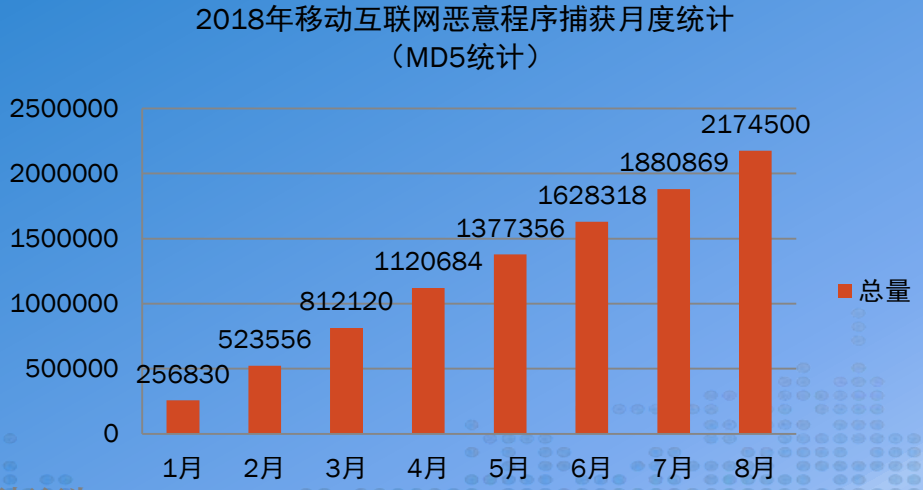
二 2018年移动互联网应用安全态势

三 AI时代移动互联网安全防护建议与展望

2018全国移动互联网安全态势综述

截止2018年8月底，发现移动互联网恶意程序（按恶意程序名称统计）716个，其中新捕获发现样本2174500个（MD5值不同）。按照工信部《移动互联网恶意程序描述格式》的八类分类标准，发现的移动互联网恶意程序分类统计数据为：恶意扣费126456个；信息窃取6436个；远程控制924个；恶意传播9749个；资费消耗436620个；系统破坏3951个；诱骗欺诈670606个；流氓行为919758个。其中诱骗欺诈占比30.8%，流氓行为占比42.3%。可以看出目前移动互联网恶意程序主要以诱骗欺诈和流氓行为为主。



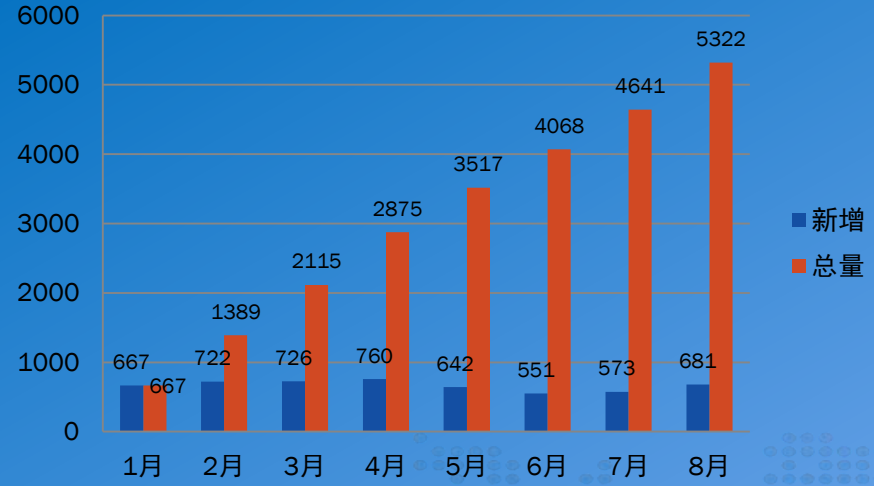


2018全国移动互联网安全态势综述

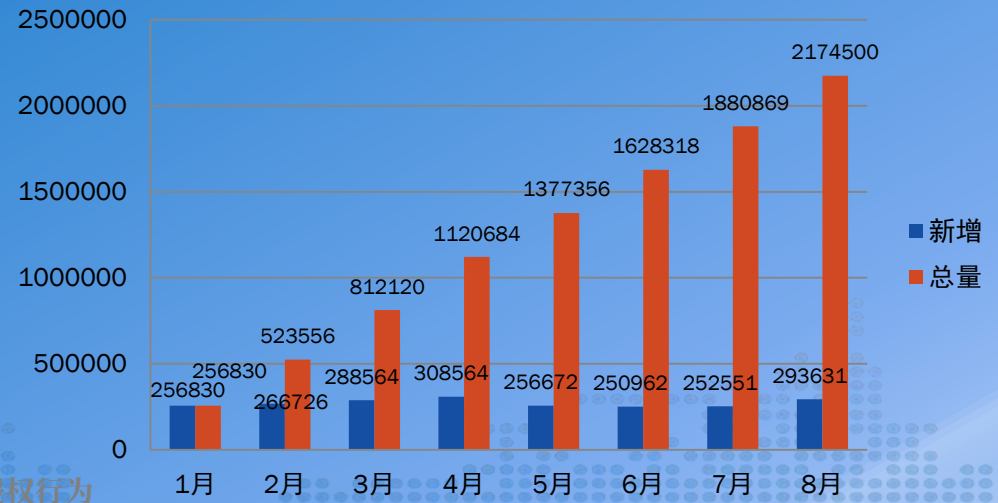
2018年各月捕获移动互联网恶意程序数量（按恶意程序名称统计）如图所示，其中6月达到上半年最低值（551个），4月达到上半年最高值（760个）

2018年各月捕获移动互联网恶意程序样本数量（MD5值不同）如图所示，其中6月达到上半年最低值（250962个），4月达到上半年最高值（308564个）

2018年移动互联网恶意程序捕获月度统计
（病毒名称统计）

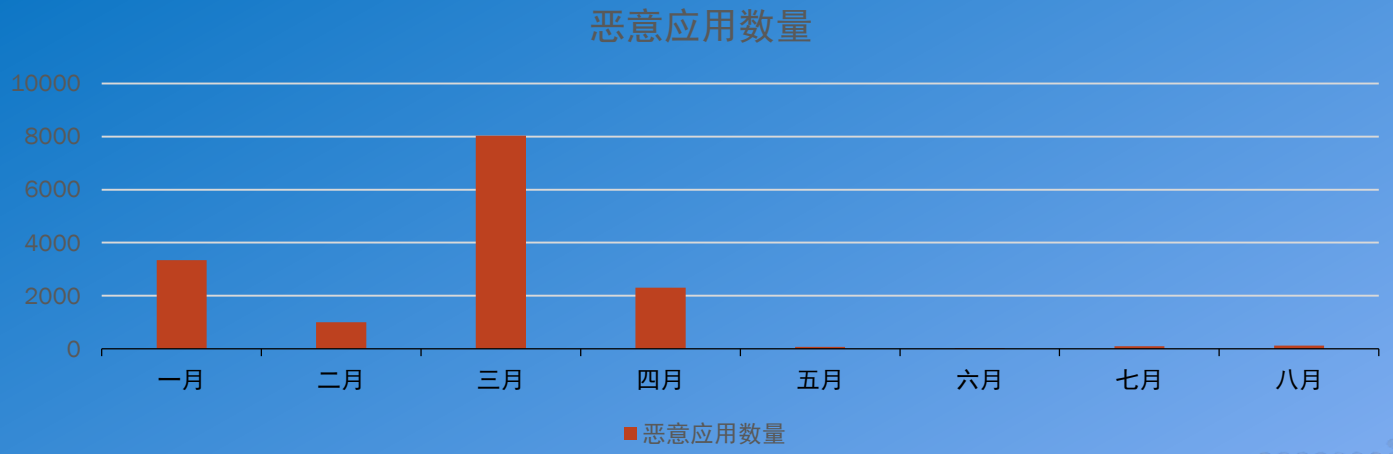


2018年移动互联网恶意程序捕获月度统计
（MD5统计）



广东省月度恶意应用统计

国家互联网应急中心广东分中心移动互联网应用安全管理平台数据显示，截止2018年8月移动互联网应用安全管理平台对广东32家移动应用商店进行监测共发现恶意应用14999个。其中，3月发现的恶意应用数量最多，达8027个。在3月之后恶意应用的滋生得到了有效的控制，呈现出明显下降趋势。



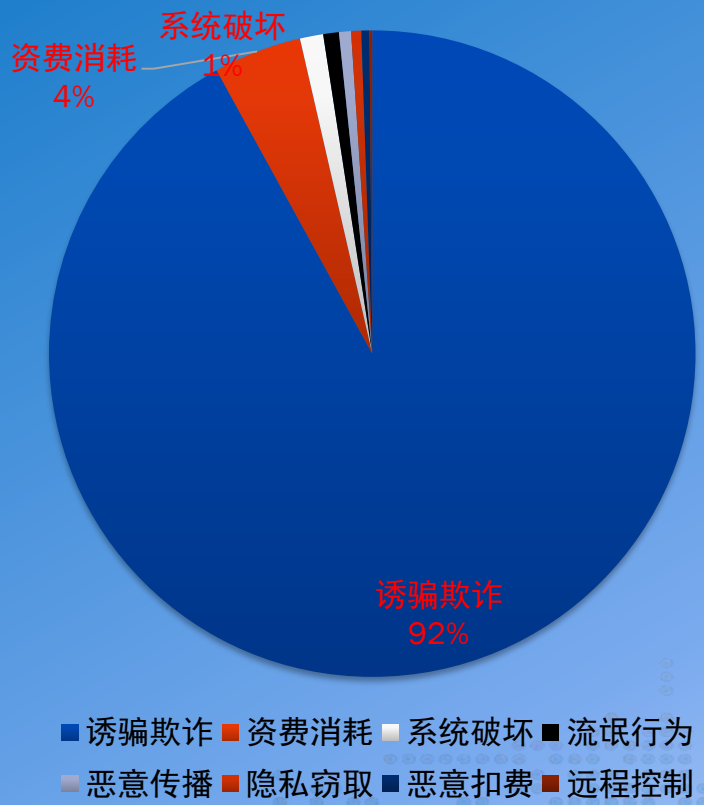
2018广东恶意应用类型统计

2018年发现的恶意应用中，诱骗欺诈类13965个、资费消耗类669个、系统破坏类176个、流氓行为类119个、恶意传播类91个、隐私窃取类77个、恶意扣费类61个、远程控制类21个。

诱骗欺诈类恶意应用位居榜首，占比92%，此类应用通过伪造、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，诱骗用户，而达到不正当目的的，具有诱骗欺诈属性

资费消耗类恶意应用排名第二，占比4%，此类应用在用户不知情或未授权的情况下，通过自动拨打电话、发送短信、彩信、邮件、频繁连接网络等方式，导致用户资费损失

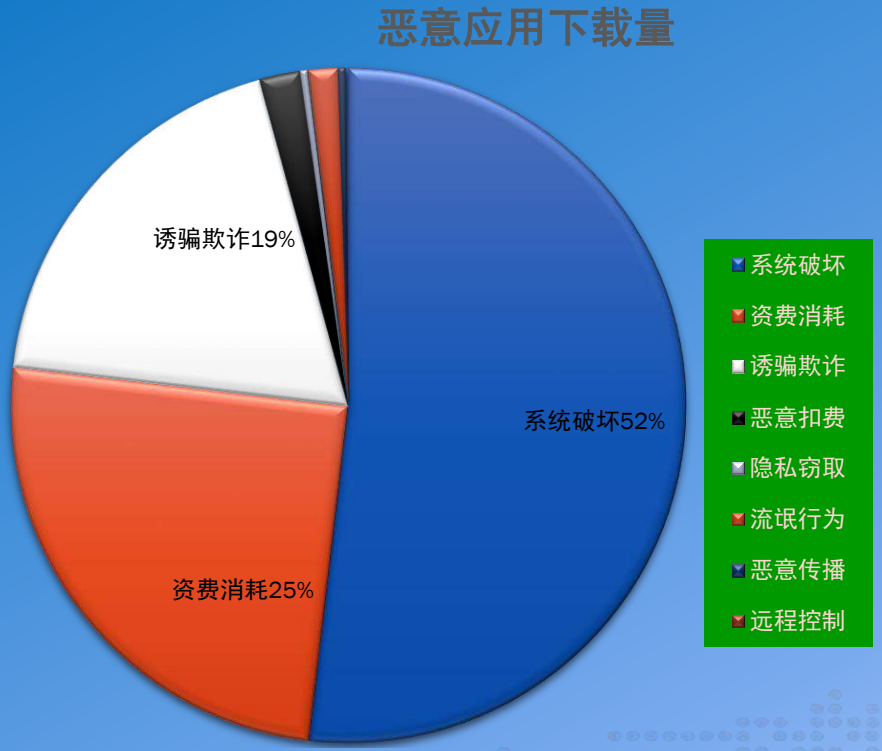
系统破坏类恶意应用排位第三，占比1%，此类应用在用户下载的软件安装包中植入恶意代码，破坏手机系统，造成用户手机耗电增加、操作卡顿等问题。



恶意应用下载统计

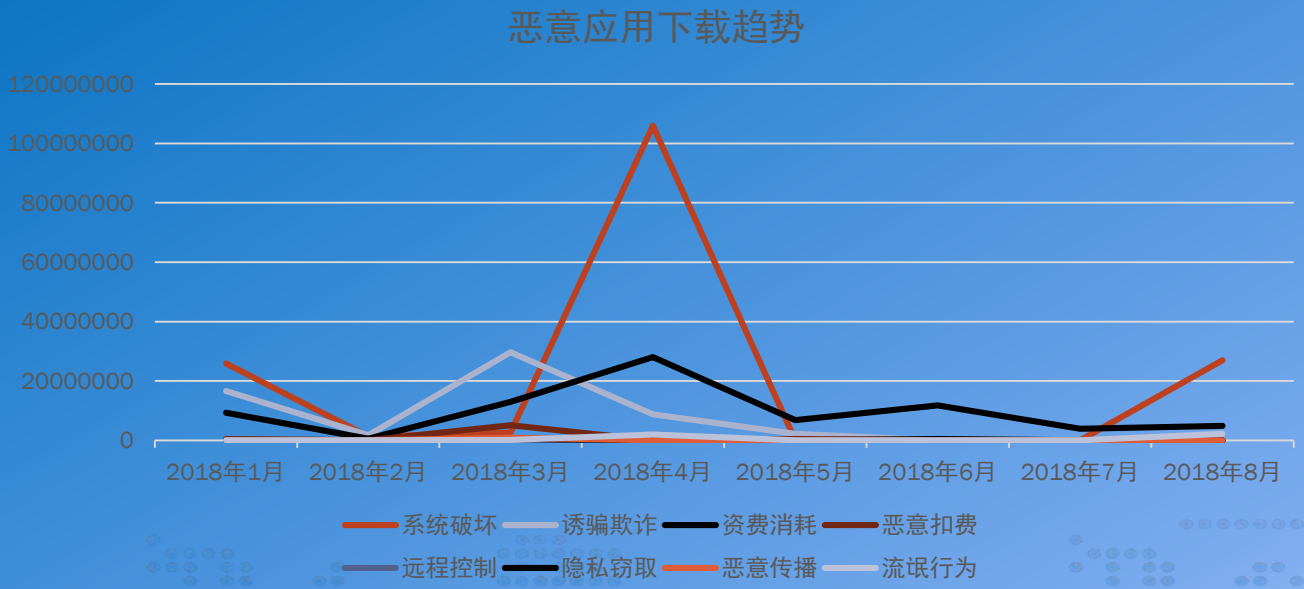
截止到2018年8月底，发现的恶意应用下载总量达3亿余次，其中下载量最大的是系统破坏类1.6亿余次，其次是资费消耗类780万次、诱骗欺诈类近6000万次。

相比恶意应用分类中资费消耗泛滥成灾，系统破坏类下载量数巨大说明了用户在使用过程中，存在着一定的自我保护意识，面对容易分辨的恶意应用有较高的警惕性，但是面对隐藏较深的恶意破坏类型时缺乏认知，也从侧面验证了**专业监管的必要性和重要性**。



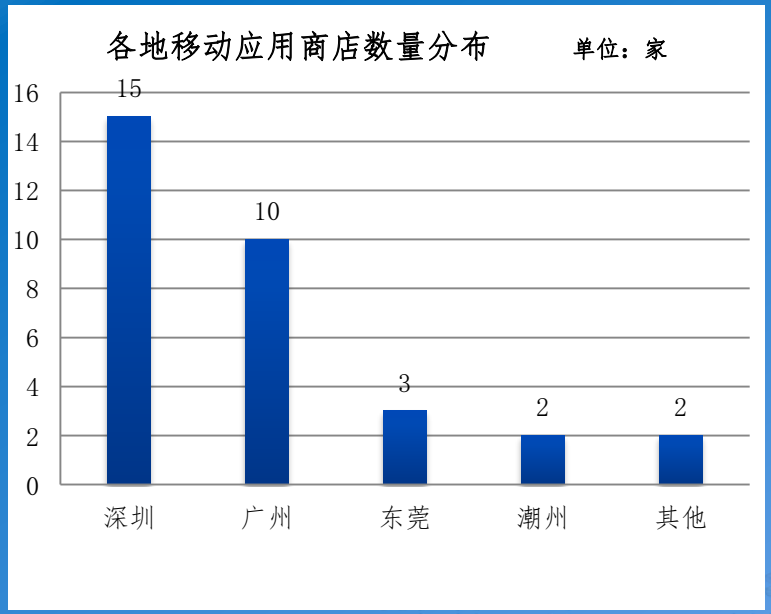
恶意应用下载趋势

2018年以来，恶意应用下载量总体呈现下降趋势，其中4月系统破坏类下载数反常激增，据中心分析为小作坊应用发布导致，数据不具特别参考意义。下载量的普遍下降说明了用户对应用安全越来越重视，自我保护意识越来越强。



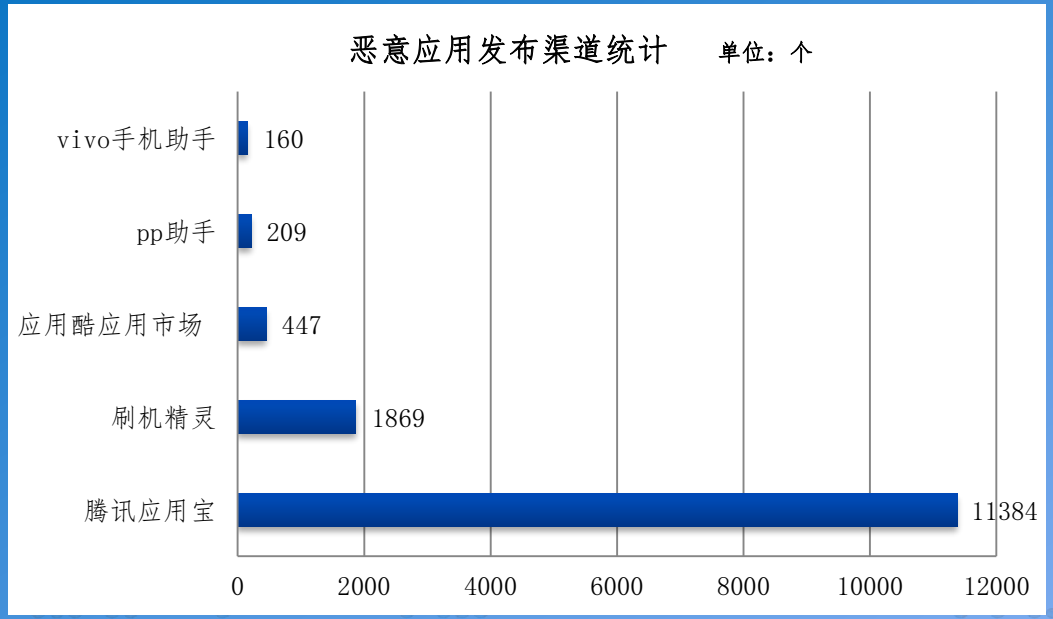
恶意应用地域统计

2018年国家互联网应急中心广东分中心监测的32家移动应用商店主要分布在深圳、广州、东莞等3个城市。发现的恶意应用主要分布在深圳、东莞、广州地区，对应的恶意应用数量分别为13436个、227个、186个。



恶意应用渠道统计

2018年度发布恶意应用最多的应用商店是腾讯应用宝，其中三月恶意发布爆发式增长，多为个体开发者发布的小空壳应用，大小都在5M以内，无法正常运行；恶意发布量其次的是刷机精灵。



提纲

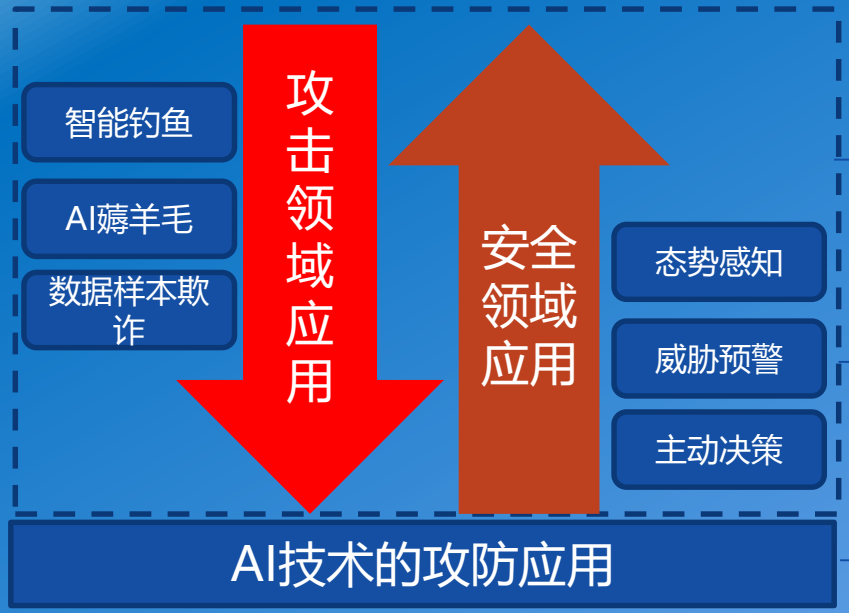
一 移动互联网应用安全形势

二 2018年移动互联网应用安全态势

三 AI时代移动互联网安全防护建议与展望

AI时代移动互联网安全防护建议

AI时代对于移动互联网是一个充满挑战的时代



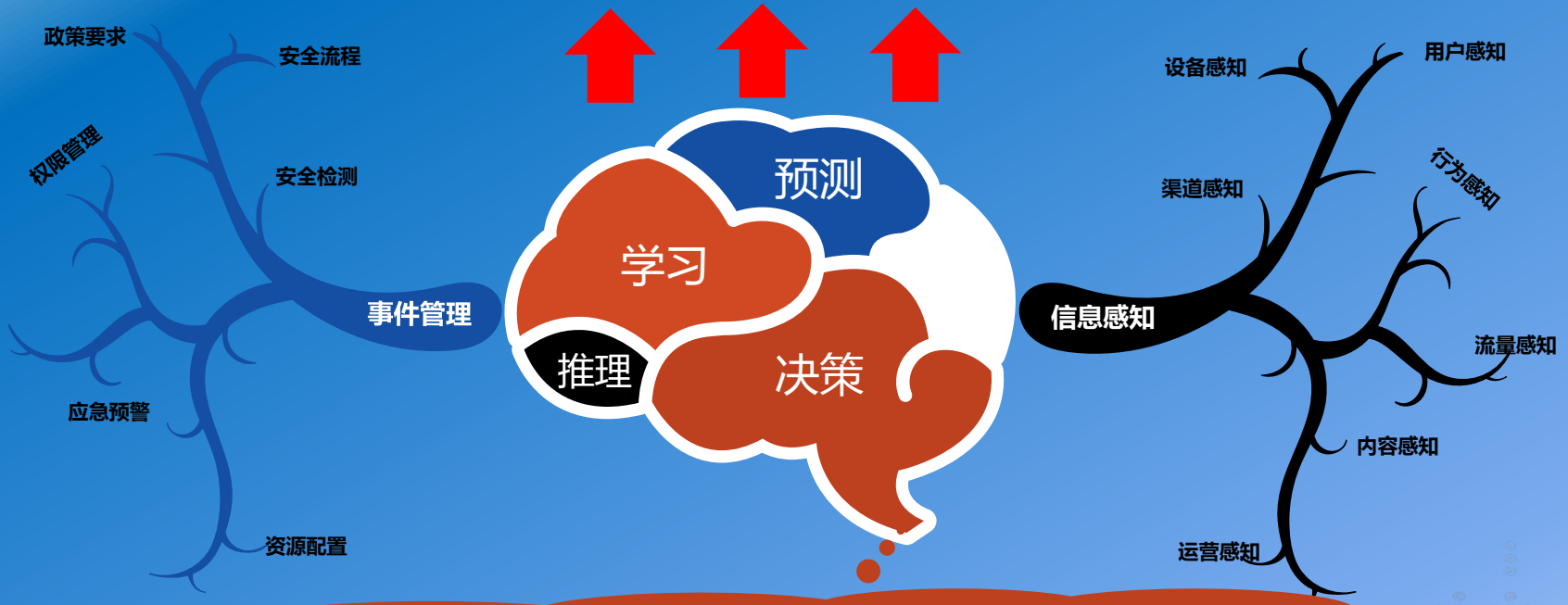
1. 设备、应用、新技术等个体防护能力，再高也无法应对新时代的挑战
2. 构建安全大数据生态体系，形成安全产业链以对抗“黑色产业链”成为大势所趋
3. 智能数据构建安全防护的过程就是新时代安全的防护建设过程

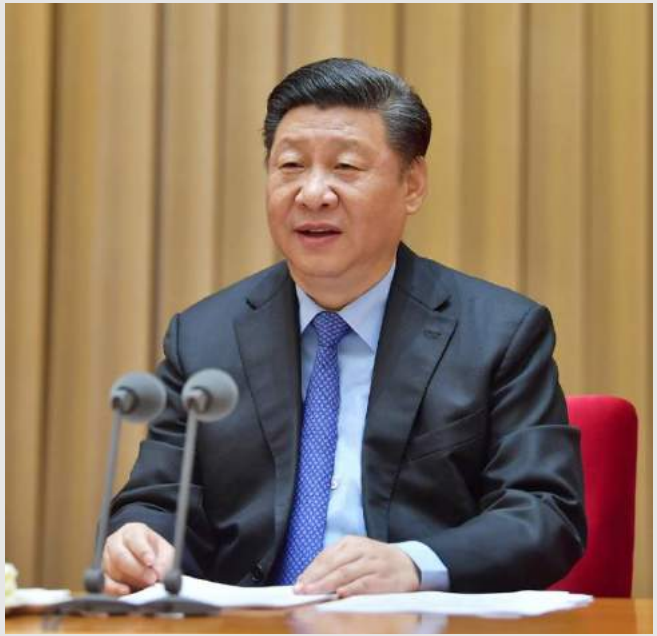
AI时代移动互联网安全展望

一物一安全

一人一安全

一事一安全





习近平在全国网络安全和信息化工作会议上强调

敏锐抓住信息化发展历史机遇

自主创新推进网络强国建设

谢 谢！

国家计算机网络应急技术处理协调中心
广东分中心