中国移动
China Mobile

2018广东互联网大会
2018 GUANGDONG INTERNET CONFERENCE
同期举办：2018 全球未来科技大会(中国·广州站)

运营商特色的移动互联网恶意程序监测与处置

广东移动　李彬

Contents 目录

1 移动互联网安全现状
2 广东移动治理体系
3 监测与处置情况
4 效果与挑战

移动互联网安全现状-形势严峻

◆ 移动互联网恶意程序是指运行于包括智能手机在内的具有移动通信功能的移动终端之上，存在窃听用户通话、窃取用户信息、破坏用户数据、擅自使用付费业务、发送垃圾信息、推送广告或欺诈信息、影响移动终端运行、危害互联网网络安全等恶意行为的计算机程序。

◆ **移动互联网恶意程序危害大，近年形势严峻**

◆ **工信部**

✓《移动互联网恶意程序监测与处置机制》（工信部保[2011]545号）

✓ 工信部关于省级基础电信企业网络与信息安全工作考核要点

◆ **省委网信办**

✓ 2017年9月，广东省委网信办、省通信管理局联合主办，由国家互联网应急中心广东分中心、广东移动等多家单位共同参演广东网络安全应急演练，提高我省网络安全应急处置能力

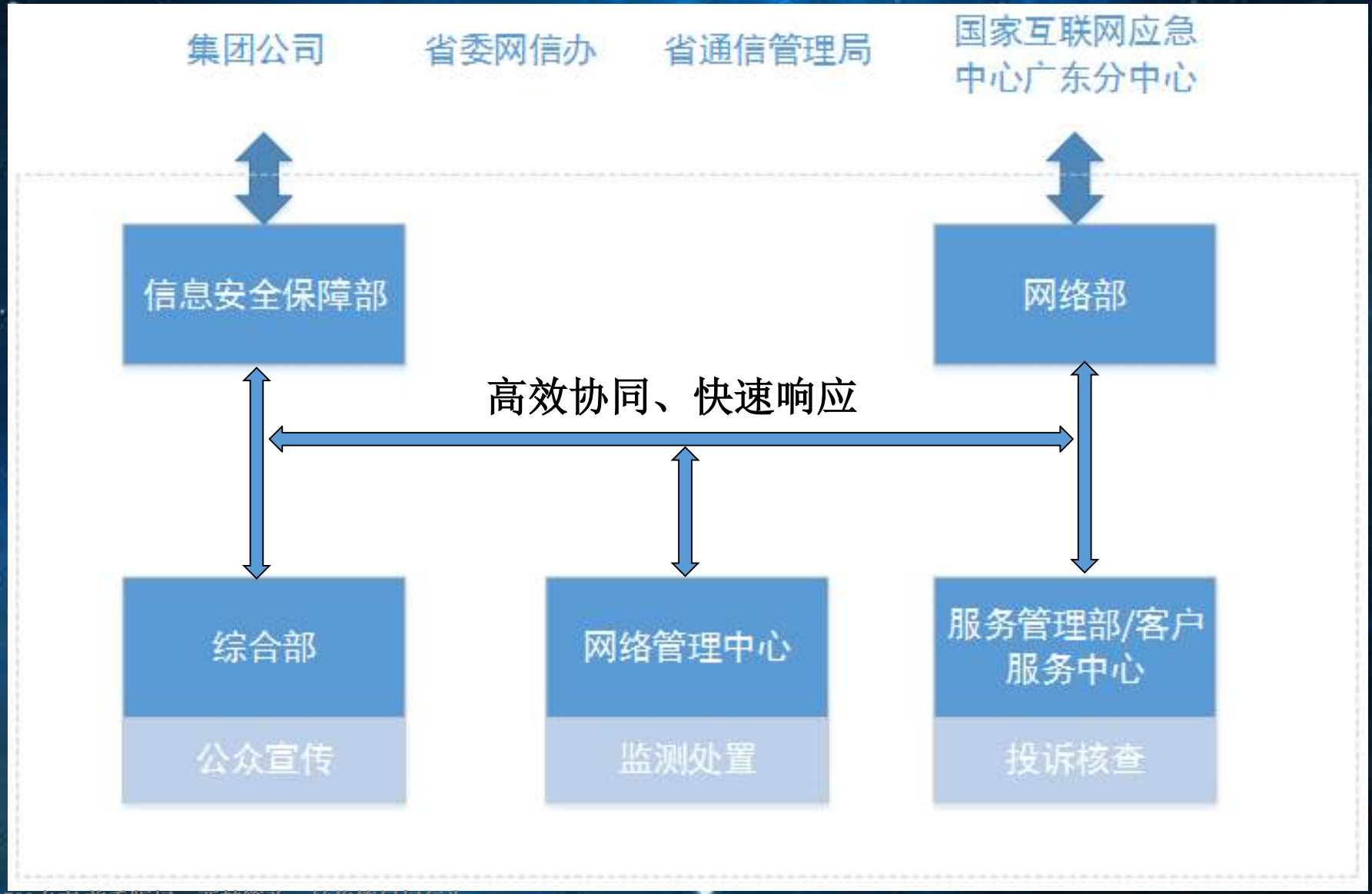
◆ **省通信管理局**

✓关于构建广东省移动互联网恶意程序应急处置工作体系的通知（粤通业函[2016]56号）

◆ **省互联网协会、国家互联网应急中心广东分中心、**

✓2016年共同发起成立广东省移动互联网应用安全发展联盟，共享应用威胁信息。

广东移动治理体系-组织架构和高效协同



广东移动治理体系-多维度侦测系统（MMDS）发展历程

2010

探索阶段，探究恶意程序侦测技术，搭建系统

●初步探索

2011

●技术研究

研究阶段，技术通过广东省通信管理局组织技术鉴定，结论为“国际领先”，申请一项发明专利

2012

构建‘云.管.端’手机恶意软件防治体系，提供手机安全先锋APP，获得公安部授予的"安全专用产品销售许可证"

●构建防治体系

2013-2015

●扩大监测范围

全量覆盖2/3/4G移动客户

2016

恶意软件自动化研判、主动预警数据挖掘分析

● 能力提升，数据挖掘分析

2017

● 推出普惠式安全服务

为移动客户提供中毒提醒短信、恶意网址访问提醒闪信等免费安全服务

广东移动治理体系-多维度侦测系统（MMDS）架构

数据层

对接多套管道系统进行异常数据采集，包括异常上网、异常短信、异常投诉等

异常上网数据

异常短信数据

异常投诉数据

分析层

异常访问行为识别+手机病毒病毒包特征识别，分析疑似中毒事件和新病毒体

核心专利双引擎分析技术

行为扫描引擎

病毒体扫描引擎

应用层

实时研判病毒、监控最新中毒发作情况、挖掘病毒传播恶意链接，多维度展现

应用平台前端系统

广东移动治理体系-多维度侦测系统（MMDS）功能

①样本自动研判

反编译风险代码扫描、恶意标签属性分析，对疑似病毒样本进行静态、动态及标签联合研判分析，提高效率10倍以上。

②病毒监控分析

病毒当前发作情况、病毒传播轨迹、变种历史关联

③态势统计分析

恶意事件发作、传播的趋势统计分析及展现功能

⑥用户关怀提醒

向高中危中毒用户、访问恶意网址用户下发提醒信息，跟踪分析病毒清除率

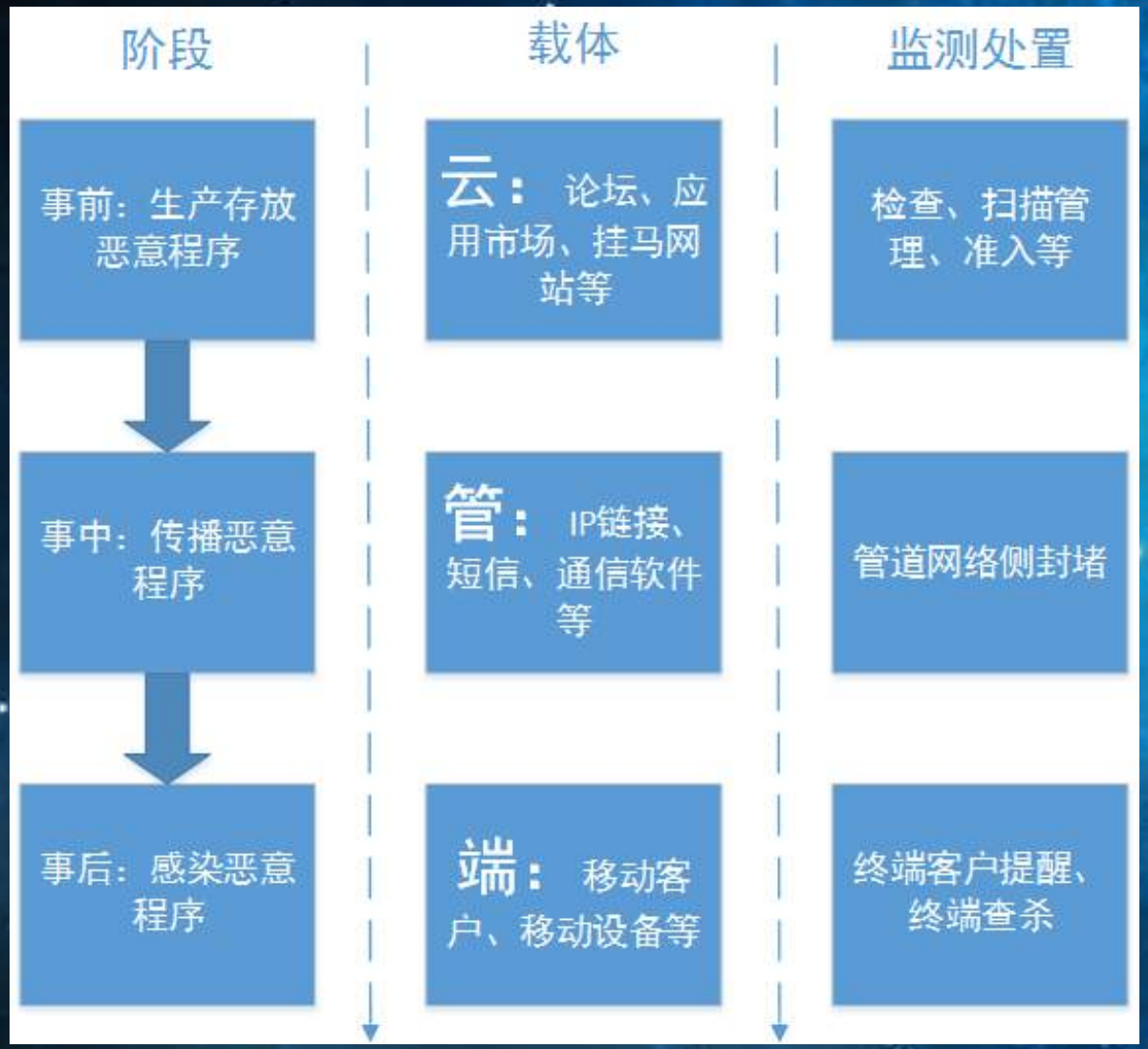
⑤封堵处置管理

短信封堵、域名/IP封堵管理

④恶意链接源头追踪

通过大数据分析传播、主控地址的网络特征，追溯恶意软件发布源头

广东移动治理体系-多维度侦测系统（MMDS）特色



◆管道监测处置 效率高

- ✓ 监测效率高
  全网异常短信
  全网异常上网
  全网异常投诉
- ✓处置效率高
  一点处置、全网生效

◆终端提醒关怀 覆盖广

- ✓ 网络通道向终端侧下发提醒
  不需要依赖移动终端和APP
  普惠式
- ✓ 广东移动官媒发布预警

监测与处置情况-案例1 “XX神器”短信传播紧急事件

案例情况：
2014年8月2日凌晨2：30左右，广东监测发现“XX神器”，批量传播短信内容相似度极高，“某某某（通讯录姓名）看这个，http://cdn.yyupload.com/down/4279193/XXshenqi.apk ”一旦用户手机下载安装链接中的恶意软件，手机将自动向通讯录中的号码发送同样短信，进行发散式传播。

广东移动监测处置方案：

1、监测告警：异常短信和异常投诉告警，监测病毒发作情况；

2、预警通报：第一时间上报通信管理局和集团公司；

2、网络封堵：紧急封堵传播地址，当天阻断恶意地址访问超7万次。

3、短信拦截：紧急异常短信拦截，当天拦截异常传播短信90万条。

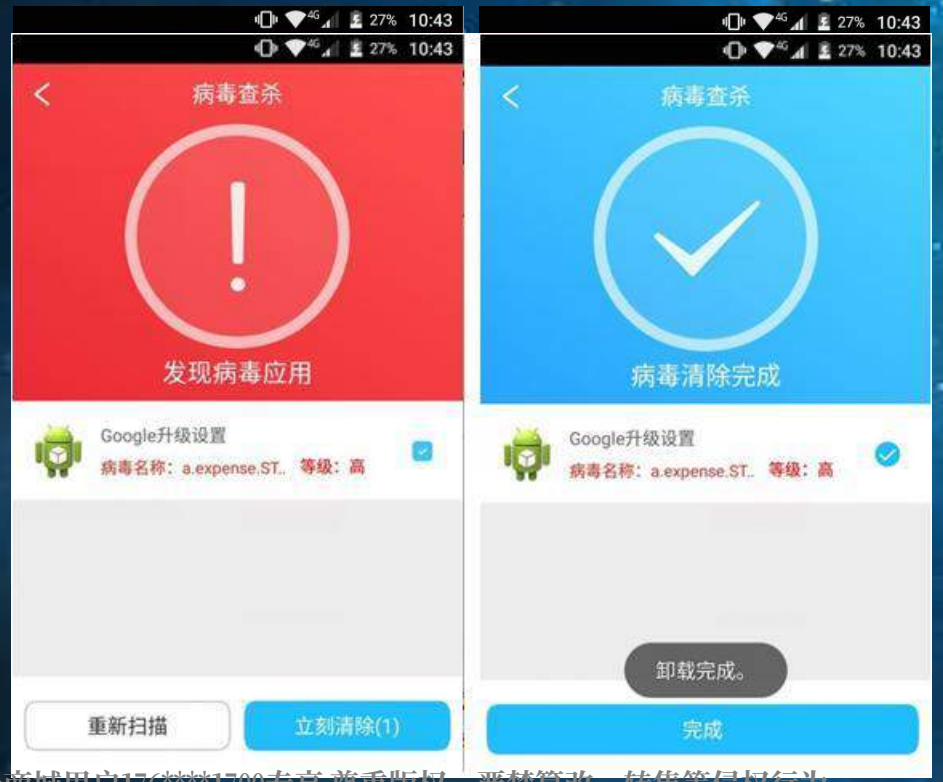
4、查杀提醒：当天更新手机安全先锋病毒库，具备查杀能力，向感染客户发送提醒短信；

迅速采取处置措施，全国范围病毒还在蔓延扩散时，广东移动及时切断病毒传播通道，遏制了“XX神器”在省内的进一步蔓延发作，将客户影响降到最低。

监测与处置情况-案例2—“彩信狂魔”群发垃圾彩信

案例情况：

2017年3月31日，广东移动自主监测发现一款“彩信狂魔”恶意软件。恶意软件伪装成‘Googel 升级’应用，终端感染后会自动发送彩信给其他客户，具有后台联网、窃取隐私、消耗资费等危害。



广东移动监测处置方案：

1、监测告警：异常投诉告警，研判病毒样本，监测病毒发作情况；短短十多天时间，仅广东移动至少3.7万个用户的手机遭遇此手机恶意软件，且呈增长趋势。

2、网络封堵：集团公司紧急封堵主控地址、传播地址，阻断恶意地址访问超200万次。

3、彩信拦截：集团公司拦截异常彩信，拦截近10万条。

4、终端提醒：向感染客户发送提醒短信4万条，协助客户清除病毒。

集团公司内，广东公司最先监测到该款病毒，随后外省陆续有监测报道。

监测与处置情况-案例3—伪“校园通”病毒事件

案例情况：

2017年寒假开学伊始，网络上针对学生家长的病毒抬头，“家长你好，你儿子的全科学习统计数据与体检结果，请你下班后点击*****查看[校园通]”。3月9日《羊城晚报》报道“警惕！校信通短信有你名字也别点”的新闻，温州某家长误点短信被骗7000元，累计有5万用户遭受这类“校信通”诈骗短信。

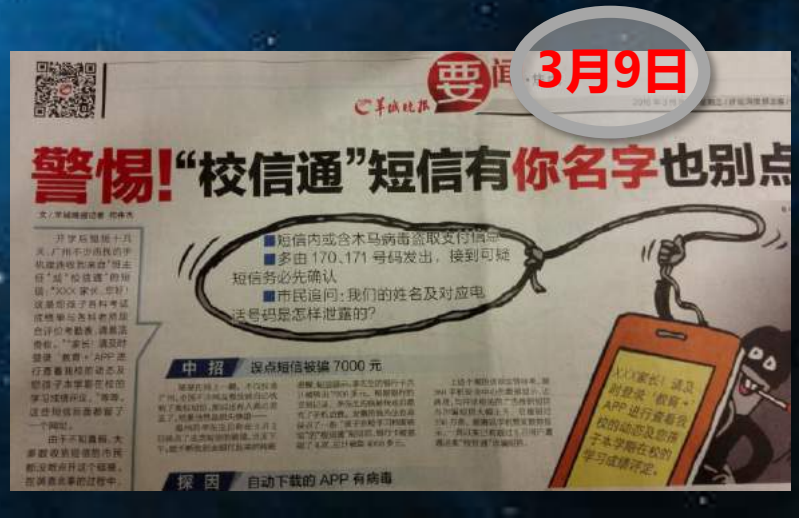
广东移动监测处置方案：

1、**监测告警：**异常短信和异常上网告警，监测病毒发作情况；

2、**网络封堵：**紧急封堵传播地址，阻断恶意地址访问超35万次。

3、**短信拦截：**紧急异常短信拦截，拦截异常传播短信52万条。

4、**终端提醒：**通过官方公众号发布预警，先于外省和媒体报道，保护广东移动客户的权益。



监测与处置情况-案例4 手机端流氓勒索病毒传播事件

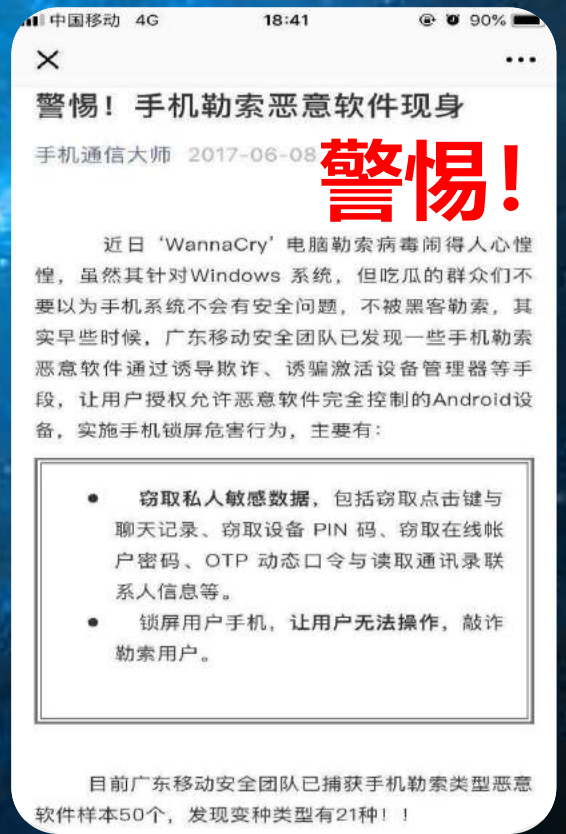
案例情况：

2017年5月份，全球范围内爆发的PC版的勒索病毒“永恒之蓝”，影响了全球一百多个国家。随之而来手机端也出现各类流氓勒索恶意程序，它伪装成各类外挂、神器、辅助等工具，锁屏用户手机进行勒索，成为用户关注的安全焦点。广东移动及时跟踪监控，发现型发现该类病毒变种超过21种。

广东移动监测处置方案：

1、网络封堵：紧急封堵已发现传播病毒地址，阻断传播地址访问超过5万次。

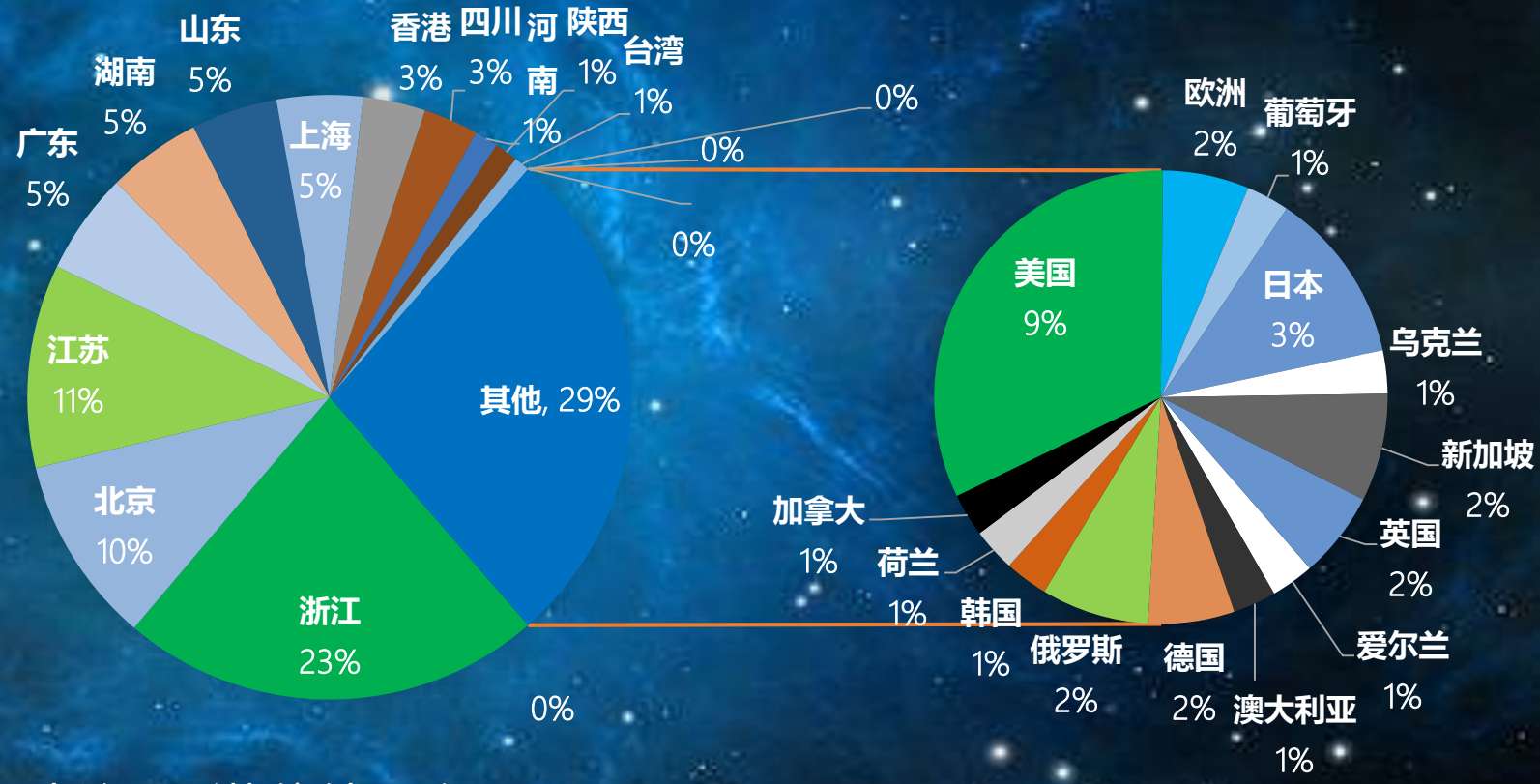
2、终端提醒：通过官方公众号发布勒索病毒预警播报，保护广东移动客户的权益。



监测与处置情况-主控地址特征分析

01 特征分析

从封堵的主控来看，中国占比70%左右，其中浙江、江苏和北京排行前三，分别是23%、11%和10%；海外主控占比27%，其中美国占9%。



Tags

恶意程序的主控地址大部分在国内，国内治理形势依然严峻

数据来源：广东移动MMDS系统

监测与处置情况-中高危恶意程序感染事件统计

02 感染事件数量

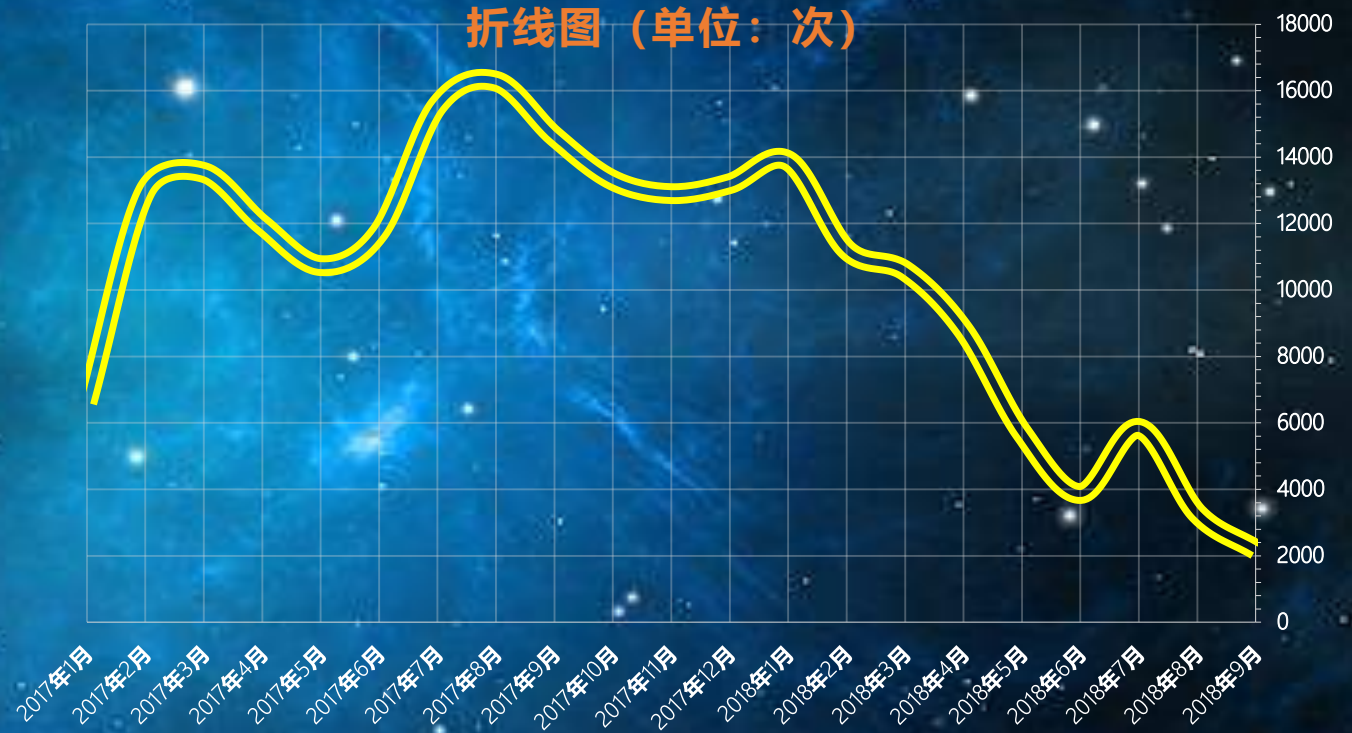
（1）2017年1月-2018年9月广东移动中高危恶意程序感染事件总量2180万次，数量体仍较大，整体形势依然严峻；

（2）2017年10月份推出中高危感染客户短信提醒服务后，中高危感染事件整体成下降趋势，提醒效果明显。

Tags

（整体形势依然严峻，中毒短信提醒效果明显）

2017-2018年每月中高危恶意程序感染事件数量折线图（单位：次）



数据来源：广东移动MMDS系统

监测与处置情况-恶意程序危害类型分类

03 危害类型

（1）2017年广东移动现网发现新恶意程序样本危害类型分布，主要是资费消耗占比高达71%。恶意扣费类型恶意样本占比18%；

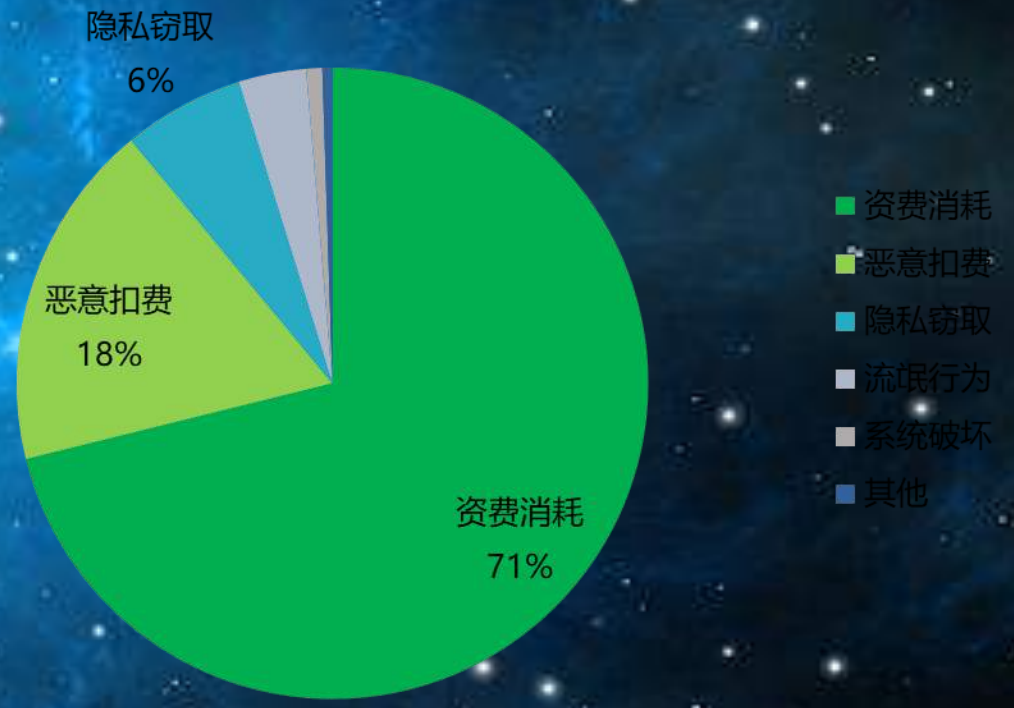
（2）目前资费消耗类主要表现是在未授权情况下，私自频繁连接网络下载安装推广软件，频繁出现弹窗，跳出广告，消耗用户手机的流量，其中伪装色情类应用占主流。

（3）恶意扣费类主要表现为用户不知情隐蔽执行，或者通过界面诱导、欺骗用户点击等手段，订购各类收费业务或使用终端支付，导致用户经济损失的，多伪装成色情应用或者热门游戏APP；

Tags

资费消耗类型传播占主流，同时要提防恶意扣费类危害

恶意程序危害类型分布



数据来源：广东移动MMDS系统

监测与处置情况-感染客户地域分布统计

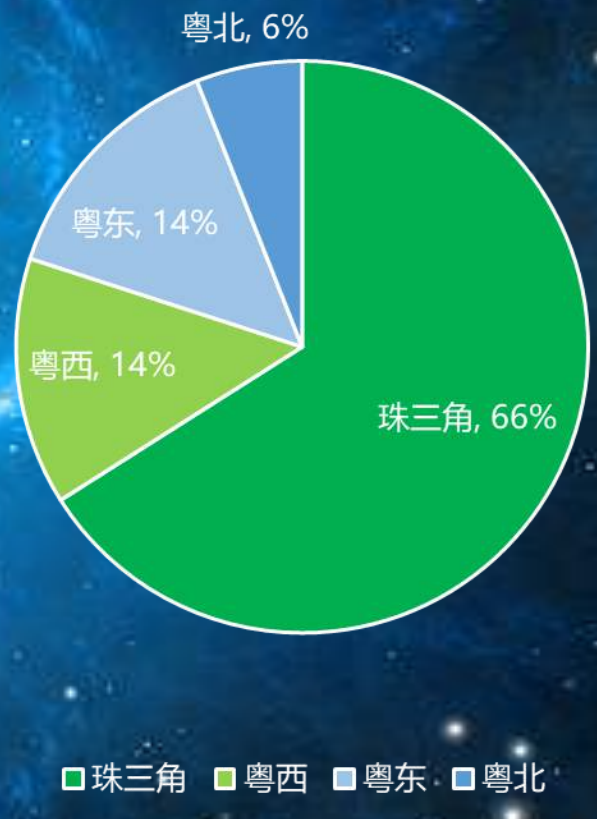
04 地域

从省内不同地区的人群维度分析，珠三角洲地区、粤东地区和粤西地区受恶意软件感染的用户总量排名前三，所占比例分别为66%，14%，14%。

Tags

越是经济发达地区，用户移动应用使用越频繁，恶意程序感染客户数量越多

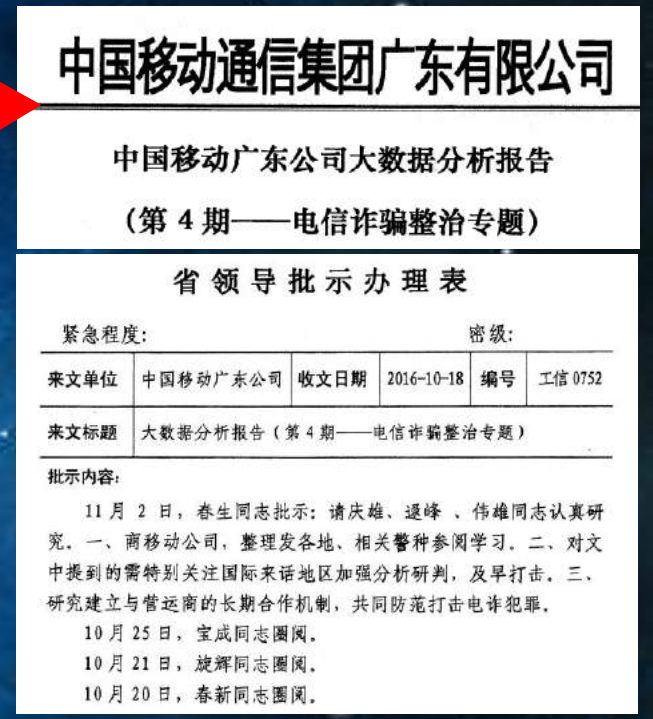
广东感染用户地域分布



数据来源：广东移动MMDS系统

效果与挑战-整体处置效果

□ 大数据分析：2016年为省政府提供大数据分析报告，得到省领导批示。



中国移动通信集团广东有限公司

中国移动广东公司大数据分析报告

（第 4 期——电信诈骗整治专题）

省 领 导 批 示 办 理 表

紧急程度：　　密级：

来文单位	中国移动广东公司	收文日期	2016-10-18	编号	工信 0752
来文标题	大数据分析报告（第 4 期——电信诈骗整治专题）				

批示内容：

11 月 2 日，春生同志批示：请庆雄、逯峰 、伟雄同志认真研究。一、商移动公司，整理发各地、相关警种参阅学习。二、对文中提到的需特别关注国际来话地区加强分析研判，及早打击。三、研究建立与营运商的长期合作机制，共同防范打击电诈犯罪。

10 月 25 日，宝成同志圈阅。

10 月 21 日，旋辉同志圈阅。

10 月 20 日，春新同志圈阅。

□ 封堵拦截：2017年至今封堵异常地址超过1万条，拦截病毒异常传播短信约60万条

- 月均阻断病毒主控访问量450万次、阻断恶意样本传播地址访问量87万次。

□ 关怀提醒：2017年至今发送提醒信息340万条，累计减少中高危感染用户166万。

- 感染客户短信提醒后94%以上客户及时进行病毒清理，**总共减少中高危感染用户166万**
- 为全省63万访问恶意网址的用户提供提醒服务超过95万次

效果与挑战-未来挑战威胁

抗检查能力加强：
移动恶意程序生产趋于工具自动化，抗检查能力越来越强。如色情软件和勒索软件等

恶意程序与电信诈骗结合
隐私窃取恶意程序与电信诈骗手段结合，降低用户感知度，实现电信诈骗

移动客户端智能化
随着移动端承载的个人信息越来越丰富，未来针对移动网络的攻击也会愈发多

1 2 3 4 5

利用虚拟引擎等新技术躲避监控：
创建一个虚拟环境，可以在虚拟空间内任意的安装、启动和卸载APP，与外部隔离，被恶意程序滥用，躲避监控

新兴移动设备带来新的风险
如利用物联网设备，嵌入恶意后门后形成僵尸网络发起DDOS攻击

携手共进，打造智能、融合、安全的移动互联网空间

THANKS

2018/11/4