

**江西省物联网态势感知报告**

**江西省通信管理局**

目 录

[1 总体概况 1](#_Toc78313442)

[2 物联网卡安全监测分析 4](#_Toc78313443)

[2.1 业务合规监测 4](#_Toc78313444)

[2.1.1 机卡分离 4](#_Toc78313445)

[2.1.2 跨区域使用 5](#_Toc78313446)

[2.1.3 流量超阈值使用 6](#_Toc78313447)

[2.1.4 超白名单使用 7](#_Toc78313448)

[2.1.5 人卡物用 8](#_Toc78313449)

[2.2 异常使用监测 9](#_Toc78313450)

[2.2.1 物卡人用（手机终端使用） 9](#_Toc78313451)

[2.2.2 人联网行为（异常使用行为） 9](#_Toc78313452)

[2.2.3 流量突增（异常流量使用） 11](#_Toc78313453)

[2.2.4 超大流量卡 12](#_Toc78313454)

[2.3 重点场景监测 13](#_Toc78313455)

[2.3.1 漫游至诈骗高发地区 13](#_Toc78313456)

[2.3.2 一机多卡 13](#_Toc78313457)

[3 终端安全事件详细信息 16](#_Toc78313458)

# {reportDate}总体概况

**一、基本情况：**

1. 三大运营商总计物联网发卡{IotCard.OperatorNumber | arrayValueTotal}张，其中{#IotCard.OperatorNumber}{name}累计发卡{value}张；{/IotCard.OperatorNumber}

{% IotCard.OperatorNumber| chart:'pie':'累计开卡数据':450:250 }

1. 三大运营商江西境内**1个月内**流量活跃物联网卡达**{IotCard.ProvinceMonthNumber | arrayValueTotal}**，**其中我省发卡{(IotCard.ProvinceMonthNumber | rank:'本省').value}（占比{(IotCard.ProvinceMonthNumber | rank:'本省').percent}），外省发卡{(IotCard.ProvinceMonthNumber | rank:'外省').value}（占比{(IotCard.ProvinceMonthNumber | rank:'外省').percent}）**；

{% IotCard.OperatorMonthNumber | chart:'bar2':'活跃物联网卡统计（月度）':450:250}

{% IotCard.ProvinceMonthNumber | chart:'pie':'活跃物联网卡占比（月度）':450:250 }

1. 江西省境内总终端数达{Imei.TotalNumber}，其中手机终端数为{Imei.PhoneNumber}。
2. 江西省境内1个月内流量活跃终端达{Imei.MonthNumber}，其中手机终端数为{Imei.PhoneMonthNumber}。

{% Imei.OperatorMonthNumber | chart:'bar2':'活跃物联网终端统计（月度）':450:250}

1. 江西省境内平台数达{Platform.TotalNumber}。
2. 江西省境内1个月内流量活跃平台达{Platform.MonthNumber}。

**二、异常情况：**

1. 发现{Abnormal.MachineCardSeparation}起机卡分离，其中单张物联网卡最多关联了{AbnormalDetail.MachineCardSeparationDetail[0].value}台终端，卡号为{AbnormalDetail.MachineCardSeparationDetail[0].msisdn}，归属运营商为{AbnormalDetail.MachineCardSeparationDetail[0].yys}，使用的LAC为{AbnormalDetail.MachineCardSeparationDetail[0].LAC}，使用的CI为{AbnormalDetail.MachineCardSeparationDetail[0].CI}，使用地理位置是\_\_\_\_；
2. 发现{Abnormal.CrossRegional}起物联网卡跨区域使用行为;
3. 发现{Abnormal.AboveThreshold}起物联网卡超阈值使用行为;
4. 发现0起超白名单使用，其中物联网卡行为0起;
5. 发现{Abnormal.PeopleUsePhysicalCard}起人卡物用;
6. 发现{Abnormal.PhysicalUsePeopleCard}起物卡人用;
7. 发现{Abnormal.Iop}起物联网卡人联网行为，其中使用流量最大的应用为{AbnormalDetail.MaxTrafficIopDetail[0].domain}，最大流量{AbnormalDetail.MaxTrafficIopDetail[0].value}MB。
8. 发现{Abnormal.TrafficJump}次物联网卡流量突增;
9. 发现{Abnormal.SuperTraffic}张物联网卡超大流量卡，其中使用流量最大超过{AbnormalDetail.SuperTrafficDetail[0].value}G，卡号为{AbnormalDetail.SuperTrafficDetail[0].msisdn}，归属运营商为{AbnormalDetail.SuperTrafficDetail[0].yys}，使用的LAC为{AbnormalDetail.SuperTrafficDetail[0].LAC}，使用的CI为{AbnormalDetail.SuperTrafficDetail[0].CI}，使用地理位置为\_\_\_\_。
10. 发现{0}个物联网号码漫游至诈骗高发区；
11. 发现{Abnormal.OneMachineManyCard}次物联网卡一机多卡行为，其中单台设备最多关联了{AbnormalDetail.OneMachineManyCardDetail[0].value}张物联网卡;终端IMEI为{AbnormalDetail.OneMachineManyCardDetail[0].imei}，使用的LAC为{AbnormalDetail.OneMachineManyCardDetail[0].LAC}，使用的CI为{AbnormalDetail.OneMachineManyCardDetail[0].CI}，使用地理位置为\_\_\_\_。
12. 发现{Abnormal.ImeiBeControl}个物联网卡终端被控事件，其中{#AbnormalDetail.ImeiBeControlDetail}{name}:{value}次;{/AbnormalDetail.ImeiBeControlDetail};
13. 发现{Abnormal.imeiAttack}次物联网卡主动攻击事件，其中{#AbnormalDetail.ImeiAttackDetail}{name}:{value}次;{/AbnormalDetail.ImeiAttackDetail}

# 物联网卡安全监测分析

## 业务合规监测

### 机卡分离

工信部文件要求：当要求“卡片限定”和“机卡绑定”的物联网卡与终端的绑定关系发生变化或用在非IMEI池中的终端上时，电信企业应能及时发现，并输出相关的机卡分离记录。

**当前实现逻辑：统计1个月内1个物联网卡号关联的用户IMSI对应两个及以上用户终端型号IMEI的个数。**

**备注：“卡片限定”和“机卡绑定”的物联网卡，限定情况收集中，目前暂定发现问题后由运营商针对性上报业务数据。**

表1：机卡分离TOP10记录表（按终端数排名）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **物联网卡号** | **运营商归属** | **终端数** | **购卡企业** | **卡片限定措施（运营商提供）** |
| {#Monitor.MachineCardSeparation}  {msisdn} | {yys} | {value} | {company\_name} | **□是 □否**  **□贴片 □嵌入（eSIM）□异形**  {/Monitor.MachineCardSeparation} |

### 跨区域使用

工信部文件要求：分析物联网话单数据中所在地小区标识，当要求“区域限定”的物联网卡超出该使用区域，电信企业应输出相关的跨区域使用记录。

**当前实现逻辑：取一个月天内物联网卡所属基站小区切换次数超过2次的数据。**

**备注：“区域限定”的物联网卡，限定情况收集中，目前暂定发现问题后由运营商针对性上报业务数据。**

表2：跨区域使用TOP10记录表（按切换次数排序）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **物联网卡号** | **运营商归属** | **购卡企业** | **切换次数** | **区域限定措施** |
| {#Monitor.CrossRegional}  {msisdn} | {yys} | {company\_name} | {value} | **□是 □否**  **□绑定基站标识**  **□限制接入基站数量**  {/Monitor.CrossRegional} |

### 流量超阈值使用

工信部文件要求：当物联网卡超出每月短信、流量实际使用量超出开户时选择的阈值的行为。电信企业应对物联网卡超阈值使用的行为进行监测，且在发现物联网卡超阈值使用后，应输出相关的超阈值使用记录

**当前实现逻辑：对1个月内使用流量超过1G的物联网卡进行取值并输出数据统计。**

表3：流量超阈值运营商排行记录统计表：

|  |  |
| --- | --- |
| **所属运营商** | **流量超阈值卡数** |
| {#Monitor.AboveThreshold}{name} | {value}{/Monitor.AboveThreshold} |
| {Monitor.AboveThreshold | arrayValueTotal} | |

### 超白名单使用---无法实现

工信部文件要求：当物联网卡的语音主被叫号码超出开户时设定的语音白名单号码、短信收发号码超出开户时设定的短信白名单号码，访问的IP或URL超出定向访问白名单的通信行为。电信企业应对物联网卡超白单使用的情况进行监测，且在发现物联网卡超白名单使用后，应输出相关的超白名单使用记录。

**当前实现逻辑：比对物联网卡开户白名单数据，统计异常使用记录。**

**备注：暂无物联网卡白名单开户数据及语音、短信数据源。**

表4：超名单IP和URL TOP1O使用表（按访问次数排序）：

|  |  |  |  |
| --- | --- | --- | --- |
| **物联网卡号** | **运营商** | **购卡企业** | **超白名单IP和URL访问次数** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

### 人卡物用

省管局要求：当人网手机号段使用物联网终端或物联网专用网络，应输出相关的人网卡号使用记录。

**当前实现逻辑：人网手机号关联物联网专用APN即判断为人卡物用。**

表5：人卡物用TOP10使用表（按关联专用APN次数排序）：

|  |  |  |
| --- | --- | --- |
| **所属运营商** | **人卡物用号码** | **关联专用APN次数** |
| {#Monitor.PhysicalUsePeopleCard}{yys} | {msisdn} | {value}{/Monitor.PhysicalUsePeopleCard} |

## 异常使用监测

### 物卡人用（手机终端使用）

工信部文件要求：当物联网卡有放置在手机终端上使用的行为时，电信企业应基于各企业内部的手机终端IMEI库，对物联网卡所使用的终端IMEI值进行监测，应输出相关的手机终端使用记录。

**当前实现逻辑：物联网卡号关联了手机终端IMEI。**

表6：物卡人用TOP10使用表（按关联手机终端IMEI次数排序）：

|  |  |  |  |
| --- | --- | --- | --- |
| **购卡企业** | **所属运营商** | **物卡人用号码** | **关联手机终端IMEI次数** |
| {#Monitor.PeopleUsePhysicalCard}{company\_name} | {yys} | {msisdn} | {value}{/Monitor.PeopleUsePhysicalCard} |

### 人联网行为（异常使用行为)

工信部文件要求：当物联网卡实际访问的URL为社交、视频、购物、游戏等异常网址时，应输出相关的异常使用记录。

**当前实现逻辑：物联网卡访问了社交类（微信、QQ、微博等）、视频类（抖音、快手、优酷、爱奇艺、腾讯视频等）、购物类（淘宝、京东、唯品会等）、游戏类（QQ游戏等）等4类网址或应用的上月访问次数和流量统计。**

**备注：7月新增规则逻辑，下月输出数据。**

表7：人联网行为-访问量TOP100使用表（按访问次数排序）：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **物联网卡号** | **运营商** | **购卡企业** | **访问次数** | **访问流量** | **域名** |
| {#Monitor.Iop}{msisdn} | {yysn} | {company\_name} | {value} | {traffic} | {domain}{/Monitor.Iop} |

表8：人联网行为-社交类访问TOP5使用表（按访问次数排序）：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **物联网卡号** | **运营商** | **购卡企业** | **社交类访问次数** | **网址或应用名称** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

表9：人联网行为-视频类访问TOP5使用表（按访问流量排序）：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **物联网卡号** | **运营商** | **购卡企业** | **视频类访问流量** | **网址或应用名称** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

表10：人联网行为-购物类访问TOP5使用表（按访问次数排序）：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **物联网卡号** | **运营商** | **购卡企业** | **购物类访问次数** | **网址或应用名称** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

表11：人联网行为-游戏类访问TOP5使用表（按访问次数排序）：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **物联网卡号** | **运营商** | **购卡企业** | **游戏类访问次数** | **网址或应用名称** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

### 流量突增（异常流量使用）

工信部文件要求：当物联网卡当月流量使用量存在大于前三个月均流量使用量2倍以上的行为时，电信企业应对物联网卡异常流量使用的行为进行监测，且在发现物联网卡流量使用异常后，应输出相关的异常流量使用记录。

**当前实现逻辑:** **统计物联网卡当月流量使用量存在大于前一个月均流量使用量2倍的记录。**

**备注：由于数据累积时间未到，实现逻辑由3个月调整为1个月，下月可输出数据，另短信缺数据源。**

表12：流量突增TOP10使用表（按突增百分比排序）：

|  |  |  |  |
| --- | --- | --- | --- |
| **物联网卡号** | **运营商** | **购卡企业** | **突增百分比（%）** |
| {#Monitor.TrafficJump}{msisdn} | {yys} | {company\_name} | {value}{/Monitor.TrafficJump} |

### 超大流量卡

省管局要求：当物联网卡当月流量使用量存在大于50G的行为时，电信企业应对物联网卡异常流量使用的行为进行监测，应输出相关的异常流量使用记录。

**当前实现逻辑: 统计物联网卡当月流量使用量存在大于50G的记录。**

**备注：该功能为7月上线新增功能，下表取值为7月前14天数据。**

表13：当月使用流量超50G的TOP10使用表（按使用流量排序）：

|  |  |  |  |
| --- | --- | --- | --- |
| **物联网卡号** | **运营商** | **购卡企业** | **当月使用流量（G）** |
| {#Monitor.SuperTraffic}{msisdn} | {yys} | {company\_name} | {value}{/Monitor.SuperTraffic} |

## 重点场景监测

### 漫游至诈骗高发地区---无法实现

工信部文件要求：当物联网卡漫游至诈骗高发区使用时，应输出相关的漫游至诈骗高发区使用记录。

**当前实现逻辑:** **取漫游至诈骗高发区的通联记录。**

**备注：本省无诈骗高发区，漫游至外省需对接反诈平台数据源。**

表14：诈骗高发区运营商TOP5排名表（按漫游次数排序）：

|  |  |  |
| --- | --- | --- |
| **诈骗高发区** | **物联网卡漫游次数** | **所属运营商** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

表15：漫游至诈骗高发区的物联网卡通联详表（按运营商排序）：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **物联网卡号** | **所属运营商** | **通联卡号** | **通联IP** | **通联URL** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

### 一机多卡

省管局要求：当同一个物联网终端设备同时插入了多张物联网卡使用时，应输出相关的一机多卡使用记录，并找出疑似多卡宝、猫池、GOIP的使用地点。

**当前实现逻辑:取1个月内1个终端IMEI号 关联3个及以上物联网卡号和人网号码的记录。**

表16：一机多卡关联终端数量TOP10记录表（按关联卡数排序）：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **终端IMEI** | **运营商** | **购卡企业** | **卡号** | **LAC** | **CI** |
| {#Monitor.OneMachineManyCard}{imei} | {yys} | {company\_name} | {msisdn} | {LAC} | {CI}{/Monitor.OneMachineManyCard} |

# 终端安全事件详细信息

省管局要求：发现物联网终端疑似被控及对外主动发起攻击的行为，应输出相应的记录。

**当前实现逻辑:取1个月内物联网终端疑似被控及对外主动发起攻击的的记录。**

表17：疑似终端受控记录表（按受控次数排序）：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **终端IMEI** | **物联网卡号** | **受控类型** | **受控次数** | **运营商** | **购卡企业** |
| {#Monitor.ImeiBeControl}{imei} | {msisdn} | {rule\_gzdl} | {value} | {yys} | {company\_name}{/Monitor.ImeiBeControl} |

表18：疑似主动攻击记录表（按受控次数排序）：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **终端IMEI** | **物联网卡号** | **攻击类型** | **攻击次数** | **运营商** | **购卡企业** |
| {#Monitor.imeiAttack}{imei} | {msisdn} | {rule\_gzdl} | {value} | {yys} | {company\_name}{/Monitor.imeiAttack} |