

**江西省物联网态势感知报告**

**江西省通信管理局**

目 录

[1 2021年6月总体概况 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） 10](#_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 14](#_Toc78313457)

[3 终端安全事件详细信息 16](#_Toc78313458)

# 2021年6月总体概况

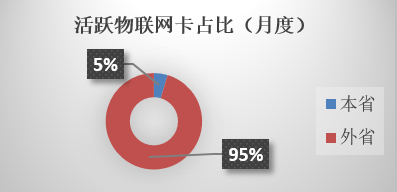
**一、基本情况：**

1. 三大运营商总计物联网发卡15140107张，其中江西电信累计发卡7324023张，江西移动累计发卡6713069张，江西联通累计发卡1103015张。



1. 三大运营商江西境内**1个月内**流量活跃物联网卡达**177万+**，**其中我省发卡8万+（占比4%），外省发卡169万+（占比96%）**；





1. 三大运营商江西省境内**1个月内**流量活跃终端达**8万+。**



**二、异常情况：**

1. 发现5552起机卡分离，其中单张物联网卡最多关联了27台终端，卡号为1440164934481，归属运营商为江西移动，使用区域为江西省南昌市南昌县艾溪湖南路;长胜村小学附近42米；



1. 发现40376起跨区域使用行为，其中江西赛格车圣科技有限公司和赣州市公共交通总公司为疑似车联网企业未上报限定措施，而萍乡市华顺房地产开发有限公司为高度疑似“跨区域使用”行为;
2. 发现 起超阈值使用;
3. 发现 起超白名单使用;
4. 发现 起人卡物用;
5. 发现197642起物卡人用;
6. 发现119904起人联网行为，其中使用流量最大的应用为pull-flv-f11.douyincdn.com（抖音）;
7. 发现 次流量突增（当前统计为6月份超5月份流量均值的2倍）;
8. 发现795张超大流量卡，其中使用流量最大超过210G，卡号为18069221430，归属运营商为浙江省宁波电信，使用区域为江西省赣州市章贡区文明大道赣南师范大学科技学院内。



1. 发现 个物联网号码漫游至诈骗高发区；
2. 发现432次一机多卡行为，其中单台设备最多关联了356张物联网卡;终端IMEI为0010680000000000，使用区域为江西省南昌市东湖区沿江北大道515号;江西省人民医院(爱国路院区)。



1. 发现109个被控终端（疑似被木马程序控制）;
2. 发现3080次物联网卡主动攻击事件，其中木马程序传播364次、僵尸网络攻击952次，蠕虫攻击2次，系统攻击（缓存区溢出、提权、代码执行、智能设备攻击等）1760次，病毒程序攻击2次。

# 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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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）** |
| 1440164934481 | 江西移动 | 27 |  | **□是 □否**  **□贴片 □嵌入（eSIM）□异形** |
| 14848621054 | 江西移动 | 17 |  | **□是 □否**  **□贴片 □嵌入（eSIM）□异形** |
| 1440516036180 | 江西移动 | 16 |  | **□是 □否**  **□贴片 □嵌入（eSIM）□异形** |
| 14848621098 | 江西移动 | 14 |  | **□是 □否**  **□贴片 □嵌入（eSIM）□异形** |
| 14848621094 | 江西移动 | 13 |  | **□是 □否**  **□贴片 □嵌入（eSIM）□异形** |
| 14803382522 | 江西移动 | 13 |  | **□是 □否**  **□贴片 □嵌入（eSIM）□异形** |
| 1064836076774 | 江西电信 | 12 |  | **□是 □否**  **□贴片 □嵌入（eSIM）□异形** |
| 14826825920 | 江西移动 | 11 |  | **□是 □否**  **□贴片 □嵌入（eSIM）□异形** |
| 1064749214748 | 江西电信 | 10 |  | **□是 □否**  **□贴片 □嵌入（eSIM）□异形** |
| 14826415310 | 江西移动 | 10 |  | **□是 □否**  **□贴片 □嵌入（eSIM）□异形** |

### 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14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

|  |  |  |  |
| --- | --- | --- | --- |
| **物联网卡号** | **运营商归属** | **购卡企业** | **区域限定措施** |
| 1064951356873 | 江西电信 | 江西赛格车圣科技有限公司 | **□是 □否**  **□绑定基站标识**  **□限制接入基站数量** |
| 1410369854699 | 江西电信 | 赣州市公共交通总公司 | **□是 □否**  **□绑定基站标识**  **□限制接入基站数量** |
| 1064972373599 | 江西电信 | 江西赛格车圣科技有限公司 | **□是 □否**  **□绑定基站标识**  **□限制接入基站数量** |
| 1410415154674 | 江西电信 | 赣州市公共交通总公司 | **□是 □否**  **□绑定基站标识**  **□限制接入基站数量** |
| 1064972372659 | 江西电信 | 江西赛格车圣科技有限公司 | **□是 □否**  **□绑定基站标识**  **□限制接入基站数量** |
| 1410300328000 | 江西电信 | 萍乡市华顺房地产开发有限公司 | **□是 □否**  **□绑定基站标识**  **□限制接入基站数量** |
| 1410417786770 | 江西电信 | 赣州市公共交通总公司 | **□是 □否**  **□绑定基站标识**  **□限制接入基站数量** |
| 1410417786290 | 江西电信 | 赣州市公共交通总公司 | **□是 □否**  **□绑定基站标识**  **□限制接入基站数量** |
| 1410417789400 | 江西电信 | 赣州市公共交通总公司 | **□是 □否**  **□绑定基站标识**  **□限制接入基站数量** |
| 1410369857195 | 江西电信 | 萍乡市华顺房地产开发有限公司 | **□是 □否**  **□绑定基站标识**  **□限制接入基站数量** |

### 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。**

表3：流量超阈值运营商排行记录表：

|  |  |  |
| --- | --- | --- |
| **排名** | **所属运营商** | **流量超阈值卡数** |
| 1 | 江西电信 | 314 |
| 2 | 江西移动 | 107 |
| 3 | 江西联通 | 15 |
| 总计 | 436 | |

### 超白名单使用

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：超白名单语音主被叫TOP10使用表：

|  |  |  |  |
| --- | --- | --- | --- |
| **物联网卡号** | **运营商** | **购卡企业** | **超白名单语音主被叫次数** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

表5：超白名单短信收发TOP10使用表：

|  |  |  |  |
| --- | --- | --- | --- |
| **物联网卡号** | **运营商** | **购卡企业** | **超白名单短信收发次数** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

表6：超名单IP和URL TOP1O使用表：

|  |  |  |  |
| --- | --- | --- | --- |
| **物联网卡号** | **运营商** | **购卡企业** | **超白名单IP和URL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：人网手机号访问物联网专用APN即判断为人卡物用。**

表7：人卡物用购卡企业TOP10使用表：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **购卡企业** | **所属运营商** | **人卡物用号码** |
| 1 |  |  |  |
| 2 |  |  |  |
| 3 |  |  |  |
| 4 |  |  |  |
| 5 |  |  |  |
| 6 |  |  |  |
| 7 |  |  |  |
| 8 |  |  |  |
| 9 |  |  |  |
| 10 |  |  |  |

## 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8：物卡人用购卡企业TOP10使用表：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **购卡企业** | **所属运营商** | **物卡人用号码** |
| 1 | 城市道路扬尘污染治理智慧化管理平台 | 江西电信 | 1064609321788 |
| 2 | 九江市交通运输局 | 江西电信 | 1410339176598 |
| 3 | 渣打银行（中国）有限公司 | 外省联通 | 14552292238 |
| 4 | 深圳市艾米通信有限公司 | 外省电信 | 1410335773548 |
| 5 | 九江市交通运输局 | 江西电信 | 1410339169775 |
| 6 | 九江市交通运输局 | 江西电信 | 1410339181079 |
| 7 | 九江市交通运输局 | 江西电信 | 1410339132310 |
| 8 | 九江市交通运输局 | 江西电信 | 1410339303389 |
| 9 | 九江市交通运输局 | 江西电信 | 1410339163506 |
| 10 | 九江市交通运输局 | 江西电信 | 1410322391507 |

### 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类网址的上月访问量统计。**

表9：人联网行为-社交类访问TOP5使用表：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **物联网卡号** | **运营商** | **购卡企业** | **社交类访问次数** | **主要社交应用名称** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

表10：人联网行为-视频类访问TOP5使用表：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **物联网卡号** | **运营商** | **购卡企业** | **视频类访问流量** | **主要视频应用名称** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

表11：人联网行为-购物类访问TOP5使用表：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **物联网卡号** | **运营商** | **购卡企业** | **购物类访问次数** | **主要购物应用名称** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

表12：人联网行为-游戏类访问TOP5使用表：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **物联网卡号** | **运营商** | **购卡企业** | **游戏类访问次数** | **主要游戏应用名称** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

### 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：短信用量突增缺数据源，实现逻辑由3个月调整为1个月。

表13：流量突增TOP10使用表：

|  |  |  |  |
| --- | --- | --- | --- |
| **物联网卡号** | **运营商** | **购卡企业** | **突增百分比** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

### 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。**

表14：当月使用流量超50G的TOP10使用表：

|  |  |  |  |
| --- | --- | --- | --- |
| **物联网卡号** | **运营商** | **购卡企业** | **当月使用流量（G）** |
| 1064986369531 | 电信 |  | 109 |
| 1410413275625 | 电信 |  | 108 |
| 1400052810748 | 电信 |  | 104 |
| 1064917763887 | 电信 |  | 97 |
| 1410341972924 | 电信 |  | 91 |
| 1410403799267 | 电信 |  | 90 |
| 1064939472512 | 电信 |  | 88 |
| 1064948911403 | 电信 |  | 88 |
| 1410814798847 | 电信 |  | 88 |
| 1410340029020 | 电信 |  | 85 |
| 总计 |  | | |

## 重点场景监测

### 漫游至诈骗高发地区

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15：诈骗高发区运营商TOP5排名表：

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

表16：漫游至诈骗高发区的物联网卡通联TOP5详表：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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14天内1个终端IMEI号关联3个及以上物联网卡号的记录。**

表17：一机多卡关联终端数量TOP10记录表：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **终端IMEI** | **运营商** | **购卡企业** | **关联物联网卡数** | **活动区域** |
| 0010680000000000 |  |  | 356 | LAC:26898 CI:141076695  位置信息：  江西省南昌市东湖区沿江北大道515号;江西省人民医院(爱国路院区)北118米 |
| 0044001520200000 |  |  | 345 | LAC:6432 CI: 250760079  位置信息：  江西省九江市湖口县S22(都九高速);湖畔山庄南697米 |
| 8674000203166101 |  |  | 322 | LAC:26927 CI:242097004  位置信息：  江西省九江市星子县;扈家咀东北589米 |
| 8686210217588800 |  |  | 111 | LAC:31144 CI:241485919  位置信息：  江西省鹰潭市贵溪市花之韵综合道;龙虎山内,植物迷宫附近26米 |
| 3566120447085104 |  |  | 78 | LAC:27083 CI:150824970  位置信息：  江西省上饶市鄱阳县;尧山东184米 |
| 3520990017614800 |  |  | 57 | LAC:30996 CI:26352611  位置信息：  江西省南昌市南昌县瑶湖西六路;南昌高新电子信息产业园东344米 |
| 3539190256801378 |  |  | 52 | LAC:30979 CI:129139792  位置信息：  江西省新余市渝水区沿江路;新余市城市管理局城北综合执法一大队附近31米 |
| 353857066016003 | 电信 |  | 28 | LAC:29313 CI:120037938  位置信息：  江西省赣州市定南县龙亭路51号;鑫辉洗车服务中心附近8米 |
| 353857066018017 | 电信 | 东莞市汇德思创通讯技术发展有限公司 | 17 | LAC:28232 CI:210915765  位置信息：  江西省南昌市青山湖区G6001(南昌绕城高速);市建筑材料厂北242米 |
| 3300730711000278 |  |  | 10 | LAC:26940 CI:240715884  位置信息：  江西省上饶市婺源县G56(杭瑞高速);婺源县天坛鸿达茶叶有限公司东195米 |

# 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18：疑似终端受控记录表：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **终端IMEI** | **物联网卡号** | **受控类型** | **受控次数** | **运营商** | **购卡企业** |
| 864317036706805 | 140005951155966 | 木马程序 | 66 |  |  |
| 864317036706722 | 1400059511370 | 木马程序 | 13 |  |  |
| 869160043946021 | 19172886850 | 木马程序 | 4 |  |  |
| 869763046955319 | 18970307518 | 木马程序 | 3 |  |  |
| 358801092943462 | 19170214200 | 木马程序 | 3 |  |  |
| 863836048516036 | 18170142266 | 木马程序 | 2 |  |  |
| 860281044621386 | 18970881594 | 木马程序 | 1 |  |  |
| 862282045138089 | 19147012509 | 木马程序 | 1 |  |  |
| 862581045274160 | 17379523856 | 木马程序 | 1 |  |  |
| 864034048749067 | 18068447412 | 木马程序 | 1 |  |  |
| 861390043085136 | 1410301221152 | 木马程序 | 1 |  |  |

备注:本月受控终端共计109个。

表19：系统攻击TOP5记录表：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **终端IMEI** | **物联网卡号** | **运营商** | **购卡企业** | **对外攻击次数** |
| 860384044104211 | 15579057065 | 江西联通 |  | 86 |
| 357257090044442 | 19100232824 | 江西电信 |  | 29 |
| 864574041266155 | 19979510809 | 江西电信 |  | 25 |
| 863489048733126 | 18689733971 | 外省联通 |  | 22 |
| 860566043553147 | 13027246703 | 江西联通 |  | 19 |

表20：僵尸网络TOP5记录表：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **终端IMEI** | **物联网卡号** | **运营商** | **购卡企业** | **对外攻击次数** |
| 356589102165307 | 18979986114 | 江西联通 |  | 28 |
| 860128049188087 | 17379190160 | 江西电信 |  | 18 |
| 864687047512628 | 19179761106 | 江西电信 |  | 16 |
| 862169040890501 | 19979929144 | 江西电信 |  | 13 |
| 866882045797192 | 17338172198 | 江西联通 |  | 8 |

表21：病毒程序TOP5记录表：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **终端IMEI** | **物联网卡号** | **运营商** | **购卡企业** | **对外攻击次数** |
| 869987053173934 | 18174017808 | 江西电信 |  | 2 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

表22：木马程序TOP5记录表：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **终端IMEI** | **物联网卡号** | **运营商** | **购卡企业** | **对外攻击次数** |
| 861695046271115 | 15588230604 | 外省联通 |  | 163 |
| 868916042313732 | 1410814837878 | 外省联通 |  | 64 |
| 868296020177106 | 18010135910 | 外省电信 |  | 43 |
| 864759031489665 | 13366696406 | 外省电信 |  | 20 |
| 868204040274960 | 18501689581 | 外省联通 |  | 18 |

表23：蠕虫程序TOP5记录表：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **终端IMEI** | **物联网卡号** | **运营商** | **购卡企业** | **对外攻击次数** |
| 861038034075174 | 18579160698 | 联通 |  | 1 |
| 868217041734428 | 17398763894 | 联通 |  | 1 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |