

**北京联通联网态势感知报告**

**{startDate}-{endDate}**

**北京联通**

目 录

[1 总体概况 1](#_Toc23124)

[1.1 基本情况 1](#_Toc26672)

[1.2 异常情况 2](#_Toc13791)

[2 物联网卡安全监测分析 4](#_Toc15737)

[2.1 业务合规监测 4](#_Toc4454)

[2.1.1 机卡分离 4](#_Toc24418)

[2.1.2 跨区域使用 5](#_Toc14935)

[2.1.3 流量超阈值使用 6](#_Toc13360)

[2.1.4 超白名单使用 7](#_Toc23080)

[2.1.5 人卡物用 8](#_Toc21157)

[2.2 异常使用监测 8](#_Toc31542)

[2.2.1 物卡人用（手机终端使用） 8](#_Toc6104)

[2.2.2 人联网行为（异常使用行为) 10](#_Toc22944)

[2.2.3 流量突增（异常流量使用） 12](#_Toc32054)

[2.2.4 超大流量卡 13](#_Toc2008)

[2.3 重点场景监测 14](#_Toc14131)

[2.3.1 漫游至诈骗高发地区 14](#_Toc27918)

[2.3.2 一机多卡 14](#_Toc10916)

[3 终端安全事件详细信息 16](#_Toc5023)

# 1 总体概况

## 1.1 基本情况

1. 本省境内总计发现物联网卡{IotCard.TotalNumber}张。
2. 本省境内活跃物联网卡{IotCard.ActiveNumber}张。
3. 本省境内总终端数{Imei.TotalNumber}个。
4. 本省境内活跃终端{Imei.ActiveNumber}个。
5. 本省境内活跃平台{Platform.ActiveNumber}个;
6. {#Caiot.IPType|percent}{name}通联流量{value}，占比{percent}；{/Caiot.IPType|percent}

## 1.2 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};
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{Abnormal.PeopleUsePhysicalCard}起人卡物用;
5. 发现{Abnormal.PhysicalUsePeopleCard}起物卡人用;
6. 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.IopDetail[0].domain}，最大流量{AbnormalDetail.IopDetail[0].value}MB;
7. 发现{Abnormal.TrafficJump}次物联网卡流量突增;
8. 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};
9. 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};
10. 发现{Abnormal.ImeiBeControl}个物联网卡终端被控事件，其中{#AbnormalDetail.ImeiBeControlDetail}{name}:{value}次;{/AbnormalDetail.ImeiBeControlDetail}
11. 发现{Abnormal.imeiAttack}次物联网卡主动攻击事件，其中{#AbnormalDetail.ImeiAttackDetail}{name}:{value}次;{/AbnormalDetail.ImeiAttackDetail}

# 2 物联网卡安全监测分析

## 2.1 业务合规监测

### 2.1.1 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：统计一定时间段内卡片限定和机卡绑定的物联网卡关联两个及以上用户终端型号IMEI的数据。**

表 1 机卡分离TOP10记录表（按终端数排名）

|  |  |  |
| --- | --- | --- |
| **物联网卡号** | **运营商** | **终端数** |
| {#Monitor.MachineCardSeparationOnOtherProvince}{msisdn} | {yys} | {value}{/Monitor.MachineCardSeparationOnOtherProvince} |

### 2.1.2 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：统计一定时间段内区域限定的物联网卡所属基站小区切换次数超过1次的数据。**

表1 跨区域使用TOP10记录表（按切换次数排序）

|  |  |  |
| --- | --- | --- |
| **物联网卡号** | **运营商** | **切换次数** |
| {#Monitor.CrossRegionalOnOtherProvince}{msisdn} | {yys} | {value}{/Monitor.CrossRegionalOnOtherProvince} |

### 2.1.3 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：对一定时间段内内使用流量超过1G的物联网卡的数据。**

表1 流量超阈值使用TOP10记录表

|  |  |  |
| --- | --- | --- |
| **物联网卡号** | **运营商** | **流量统计G** |
| {#Monitor.AboveThresholdOnProvince}{msisdn} | {yys} | {value}{/Monitor.AboveThresholdOnProvince} |

### 2.1.5 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：统计一定时间段内人网手机号关联物联网专用APN的数据。**

表1：人卡物用TOP10使用表（按关联专用APN次数排序）

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

## 2.2 异常使用监测

### 2.2.1 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：统计一定时间段内物联网卡号关联了手机终端IMEI的数据。**

表1 物卡人用TOP10使用表（按关联手机终端IMEI次数排序）

|  |  |  |
| --- | --- | --- |
| **运营商** | **物联网卡号** | **关联手机终端IMEI次数** |
| {#Monitor.PeopleUsePhysicalCardOnProvince}{yys} | {msisdn} | {value}{/Monitor.PeopleUsePhysicalCardOnProvince} |

### 2.2.2 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：统计一定时间段内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类网址或应用的数据。**

表 1 人联网行为统计总表

|  |  |  |  |
| --- | --- | --- | --- |
| **运营商** | **应用名称** | **流量MB** | **人联网行为物联网卡总数** |
| {#Monitor.IopBy}{yys} | {app\_name} | {value} | {msisdn\_value}{/Monitor.IopBy} |
|  | | {Monitor.IopBy|fieldSum:”value”} | {Monitor.IopBy|fieldSum:”msisdn\_value”} |

### 2.2.3 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:** **统计本月一定时间段内物联网卡使用流量大于上个月对应时间段内使用流量2倍的数据。**

表1 流量突增TOP10使用表（按突增百分比排序）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **物联网卡号** | **运营商** | **本月流量B** | **上月流量B** | **突增百分比（%）** |
| {#Monitor.TrafficJumpOnProvince}{msisdn} | {yys} | {value1} | {value2} | {value}{/Monitor.TrafficJumpOnProvince} |

### 2.2.4 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: 统计一定时间段内物联网卡使用流量存在大于50G的记录。**

表1 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** | **使用流量（G）** |
| {#Monitor.SuperTrafficOnProvince}{msisdn} | {yys} | {value}{/Monitor.SuperTrafficOnProvince} |

## 2.3 重点场景监测

### 2.3.2 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:统计一定时间段内1个终端IMEI号关联3个及以上物联网卡号的数据。**

表1：一机多卡关联终端数量TOP10记录表（按关联卡数排序）

|  |  |
| --- | --- |
| **终端号** | **关联的物联网卡数** |
| {#Monitor.OneMachineManyCard}{imei} | {value}{/Monitor.OneMachineManyCard} |

# 3 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:统计一定时间段内物联网终端疑似被控及对外主动发起攻击的的记录。**

表 1 安全事件统计总表

|  |  |  |
| --- | --- | --- |
| **终端号** | **事件类型** | **事件总数** |
| {#Monitor.SecurityEvent}{name} | {rule\_gzdl} | {value}{/Monitor.SecurityEvent} |

表2 疑似终端受控TOP10（物卡数量降序排列）

|  |  |
| --- | --- |
| **受控类型** | **受控次数** |
| {#Monitor.ImeiBeControl}{rule\_gzdl} | {value}{/Monitor.ImeiBeControl} |

表3 疑似主动攻击记录TOP10表（按受控次数排序）

|  |  |  |
| --- | --- | --- |
| **终端号** | **攻击类型** | **攻击次数** |
| {#Monitor.ImeiAttack}{imei} | {rule\_gzdl} | {value}{/Monitor.ImeiAttack} |