中移物联网安全态势感知平台

{type}

{time}

1. 网络信息安全态势综述

为全面反映本月中移物联网在{modules}方面的情况，中移物联网安全态势感知平台根据本月监测分析数据，形成了如下分析报告。{#business.show}

# 业务安全态势基本情况{#business.steps.rzcj1.show || business.steps.rzcj2.show || business.steps.rzcj3.show}

## 日志采集情况{#business.steps.rzcj1.show}

{time}，安全态势感知平台共采集到日志{business.steps.rzcj1.data.total | numberFormat}条，包括{#business.steps.rzcj1.data.list}{name}侧日志{value | numberFormat}条{separator}{/business.steps.rzcj1.data.list}。

{% business.steps.rzcj1.data.list | chart:’bar’:’ ’}

**图1-1 采集日志数量图（条）**{/business.steps.rzcj1.show}{#business.steps.rzcj2.show}

{time}，日志数量呈现{business.steps.rzcj1.data.total>business.steps.rzcj2.data.total?’上升’:’下降’}趋势，比{previousTime}（{business.steps.rzcj2.data.total | numberFormat}条）{business.steps.rzcj1.data.total>business.steps.rzcj2.data.total?’增加’:’减少’}近{business.steps.rzcj1.data.total>business.steps.rzcj2.data.total?(business.steps.rzcj1.data.total-business.steps.rzcj2.data.total)/business.steps.rzcj2.data.total\*100:(business.steps.rzcj2.data.total-business.steps.rzcj1.data.total)/business.steps.rzcj2.data.total\*100 | numberFormat} %。{/business.steps.rzcj2.show}{#business.steps.rzcj3.show}近{type==’周报’?’5周’:(type==’月报’?’半年’:’’)}日志采集数量趋势如下图所示：

{% business.steps.rzcj3.data.timeTotal | chart:’line’:’’}

**图1-2 采集日志趋势图（条）**{/business.steps.rzcj3.show}{/}

## 安全事件情况{#business.steps.aqsj1.show}

{time}，通过监测分析共发现安全事件{business.steps.aqsj1.data.total | numberFormat}条，包括{#business.steps.aqsj1.data.list}{name}{value | numberFormat}条{separator}{/business.steps.aqsj1.data.list}。

{% business.steps.aqsj1.data.list | chart:’bar’:’ ’}

**图1-3 安全事件数量图（条）**{/business.steps.aqsj1.show}{#business.steps.aqsj2.show}

{time}安全事件数量呈现{business.steps.aqsj1.data.total>business.steps.aqsj2.data.total?’上升’:’下降’}趋势，比{previousTime}（{business.steps.aqsj2.data.total | numberFormat}条）{business.steps.aqsj1.data.total>business.steps.aqsj2.data.total?’增加’:’减少’}近{business.steps.aqsj1.data.total>business.steps.aqsj2.data.total?(business.steps.aqsj1.data.total-business.steps.aqsj2.data.total)/business.steps.aqsj2.data.total\*100:(business.steps.aqsj2.data.total-business.steps.aqsj1.data.total)/business.steps.aqsj2.data.total\*100 | numberFormat} %。{/business.steps.aqsj2.show}{#business.steps.aqsj3.show}近{type==’周报’?’5周’:(type==’月报’?’半年’:’’)}安全事件趋势如下图所示：

{% business.steps.aqsj3.data.timeTotal | chart:’line’:’ ’}

**图1-4 安全事件趋势图（条）**{/business.steps.aqsj3.show}{#business.steps.ywxtsh1.show && business.steps.ywxtsh2.show}

## 业务系统受害情况

{time}，各业务系统共被攻击{business.steps.ywxtsh1.data.total | numberFormat}次，其中“{business.steps.ywxtsh1.data.data[0][0].name}”受害最为严重，{type==’周报’?’本周’:(type==’月报’?’本月’:’’)}被攻击{business.steps.ywxtsh1.data.data[0][0].value | numberFormat}次{#business.steps.ywxtsh1.data.data[0][0].name!=business.steps.ywxtsh2.data.data[0][0].name}，取代{type==’周报’?’前一周’:(type==’月报’?’前一个月’:’’)}“{business.steps.ywxtsh2.data.data[0][0].name}”被攻击{business.steps.ywxtsh2.data.data[0][0].value | numberFormat}次上升至第一位{/}。

{% business.steps.ywxtsh1.data.data | chart:’verticalBar’:’ ’}

**图1-5 业务系统受害图TOP10（次）**{/}{#business.steps.gjsjcgl.show}

## 攻击事件成功率情况

{time}，攻击成功事件XXX起，攻击失败事件XXX起，整体攻击成功率比上个月下降XXX%，近半年攻击事件成功率趋势如下图：

**图1-6 攻击成功率趋势图**{/business.steps.gjsjcgl.show}{/business.show}{#content.show}

# 内容安全态势基本情况

{/content.show}{#asset.show}

# 基础资产安全态势基本情况

{/asset.show}{#terminal.show}

# 物联网终端安全基本情况

{/terminal.show}

1. 网络信息安全事件详情{#business.show}

# 业务安全事件详情{#business.steps.aqsj1.show}

{time}，业务安全事件共{business.steps.aqsj1.data.total | numberFormat}起，其中{business.steps.aqsj1.data.list[0].name}最多，达到了{business.steps.aqsj1.data.list[0].value | numberFormat}次，以下按攻击次数排名对各安全事件进行详细介绍{/business.steps.aqsj1.show}

## {business.steps.aqsj1.data.list[0].name}详情

{time}，安全态势感知平台共监测到{business.steps.aqsj1.data.list[0].name}{business.steps.aqsj1.data.list[0].value | numberFormat}起，相比{type==’周报’?’前一周’:(type==’月报’?’前一个月’:’’)}（{business.steps.aqsj2.data.list[0].value | numberFormat}次）{business.steps.aqsj1.data.list[0].value>business.steps.aqsj2.data.list[0].value?’增加’:’减少’}近{business.steps.aqsj1.data.list[0].value>business.steps.aqsj2.data.list[0].value?(business.steps.aqsj1.data.list[0].value-business.steps.aqsj2.data.list[0].value)/business.steps.aqsj2.data.list[0].value\*100:(business.steps.aqsj2.data.list[0].value-business.steps.aqsj1.data.list[0].value)/business.steps.aqsj2.data.list[0].value\*100 | numberFormat} %。近{type==’周报’?’5周’:(type==’月报’?’半年’:’’)}{business.steps.aqsj1.data.list[0].name}数量趋势如下图所示：

{% business.steps.aqsj3.data.timeSplitMap[business.steps.aqsj1.data.list[0].flag] ? business.steps.aqsj3.data.timeSplitMap[business.steps.aqsj1.data.list[0].flag] : business.steps.aqsj3.data.timeSplitMap | chart:’line’:’ ’}

**图2-1 近{type==’周报’?’5周’:(type==’月报’?’半年’:’’)}{business.steps.aqsj1.data.list[0].name}趋势图**

### {business.steps.aqsj1.data.list[0].name}受害业务系统分布

从{business.steps.aqsj1.data.list[0].name}倾向的业务系统来看，{type==’周报’?’本周’:(type==’月报’?’本月’:’’)}{business.steps[business.steps.aqsj1.data.list[0].flag+’1’].data.data[0][0].name}被攻击次数占攻击总量的XXX%，是被攻击的主要对象，具体{business.steps.aqsj1.data.list[0].name}在各个业务系统的攻击分布如下图所示：

{% business.steps[business.steps.aqsj1.data.list[0].flag+’1’].data.data[0] | chart:’pie10’:’ ’}

**图2-2 {business.steps.aqsj1.data.list[0].name}业务系统分布**{#business.steps.web2.show}

### {business.steps.aqsj1.data.list[0].name}类型分布

{time}，中移物联网安全态势感知平台监测到XXX次Web攻击事件，其中“XSS攻击特征[1]”攻击XXX次,占比XXX%； “TROJAN[PTsecurity]Botnet Nitol.B Checkin”攻击XXX次，占比XXX%；“Supervisord远程命令执行-CVE-2017-11610”攻击XXX次，占比XXX% ；“疑似XXE注入攻击尝试”攻击XXX次，占比XXX%；“Web弱口令登录尝试”攻击XXX次，占比XXX%。

**图2-3 Web攻击类型分布图**{/business.steps.web2.show}{#business.steps.web3.show}

### {business.steps.aqsj1.data.list[0].name}最泛滥地区分析

{time}，发起Web攻击攻次数最多的地域上前五个地区分别是上海、重庆、广东、浙江、江苏，分别占Web攻击总次数的23.58%、17.42%、14.8%、11.2%和9.6%。由此可知，64%的攻击者聚集在这五个地区发起攻击。较XX-1月比较，同样在这五个地区，发起攻击的次数分别是XXX次、XXX次、XXX次、XXX次和XXX次，同XX月环比分别是XXX%、XXX%、XXX%、XXX%和XXX%。

**图2-4 Web攻击区域TOP5**{/business.steps.web3.show}

## {business.steps.aqsj1.data.list[1].name}详情

{time}，安全态势感知平台共监测到{business.steps.aqsj1.data.list[1].name}{business.steps.aqsj1.data.list[1].value | numberFormat}起，相比{type==’周报’?’前一周’:(type==’月报’?’前一个月’:’’)}（{business.steps.aqsj2.data.list[1].value | numberFormat}次）{business.steps.aqsj1.data.list[1].value>business.steps.aqsj2.data.list[1].value?’增加’:’减少’}近{business.steps.aqsj1.data.list[1].value>business.steps.aqsj2.data.list[1].value?(business.steps.aqsj1.data.list[1].value-business.steps.aqsj2.data.list[1].value)/business.steps.aqsj2.data.list[1].value\*100:(business.steps.aqsj2.data.list[1].value-business.steps.aqsj1.data.list[1].value)/business.steps.aqsj2.data.list[1].value\*100 | numberFormat} %。近{type==’周报’?’5周’:(type==’月报’?’半年’:’’)}{business.steps.aqsj1.data.list[1].name}数量趋势如下图所示：

{% business.steps.aqsj3.data.timeSplitMap[business.steps.aqsj1.data.list[1].flag] ? business.steps.aqsj3.data.timeSplitMap[business.steps.aqsj1.data.list[1].flag] : business.steps.aqsj3.data.timeSplitMap | chart:’line’:’ ’}

**图2-5 近{type==’周报’?’5周’:(type==’月报’?’半年’:’’)}{business.steps.aqsj1.data.list[1].name}趋势图**{#business.steps.jmr1.show}



### {business.steps.aqsj1.data.list[1].name}受害业务系统分布

从僵木蠕攻击倾向的业务系统来看，本月行车卫士系统被攻击次数占攻击总量的XXX%，是被攻击的主要对象，具体僵木蠕攻击在各个业务系统的攻击分布如下图所示：

**图2-6 僵木蠕攻击业务系统分布**{/business.steps.jmr1.show}{#business.steps.jmr2.show}

### {business.steps.aqsj1.data.list[1].name}类型分布

{time}，中移物联网安全态势感知平台监测到XXX次僵木蠕攻击事件，其中“僵尸网络”攻击XXX次,占比XXX%； “病毒程序”攻击XXX次，占比XXX%；“蠕虫病毒”攻击XXX次，占比XXX% ；“恶意程序”攻击XXX次，占比XXX%；“勒索软件”攻击XXX次，占比XXX%。

**图2-7 僵木蠕攻击类型分布**{/business.steps.jmr2.show}{#business.steps.jmr3.show}

### {business.steps.aqsj1.data.list[1].name}最泛滥地区分析

{time}，发起僵木蠕攻击攻次数最多的地域上前五个地区分别是上海、重庆、广东、浙江、江苏，分别占僵木蠕攻击总次数的23.58%、17.42%、14.8%、11.2%和9.6%。由此可知，64%的攻击者聚集在这五个地区发起攻击。较XX-1月比较，同样在这五个地区，发起攻击的次数分别是XXX次、XXX次、XXX次、XXX次和XXX次，同XX月环比分别是XXX%、XXX%、XXX%、XXX%和XXX%。

**图2-8 僵木蠕攻击区域分布**{/business.steps.jmr3.show}

## {business.steps.aqsj1.data.list[2].name}详情

{time}，安全态势感知平台共监测到{business.steps.aqsj1.data.list[2].name}{business.steps.aqsj1.data.list[2].value | numberFormat}起，相比{type==’周报’?’前一周’:(type==’月报’?’前一个月’:’’)}（{business.steps.aqsj2.data.list[2].value | numberFormat}次）{business.steps.aqsj1.data.list[2].value>business.steps.aqsj2.data.list[2].value?’增加’:’减少’}近{business.steps.aqsj1.data.list[2].value>business.steps.aqsj2.data.list[2].value?(business.steps.aqsj1.data.list[2].value-business.steps.aqsj2.data.list[2].value)/business.steps.aqsj2.data.list[2].value\*100:(business.steps.aqsj2.data.list[2].value-business.steps.aqsj1.data.list[2].value)/business.steps.aqsj2.data.list[2].value\*100 | numberFormat} %。近{type==’周报’?’5周’:(type==’月报’?’半年’:’’)}{business.steps.aqsj1.data.list[2].name}数量趋势如下图所示：

{% business.steps.aqsj3.data.timeSplitMap[business.steps.aqsj1.data.list[2].flag] ? business.steps.aqsj3.data.timeSplitMap[business.steps.aqsj1.data.list[2].flag] : business.steps.aqsj3.data.timeSplitMap | chart:’line’:’ ’}

**图2-9 近{type==’周报’?’5周’:(type==’月报’?’半年’:’’)}{business.steps.aqsj1.data.list[2].name}趋势图**



### {business.steps.aqsj1.data.list[2].name}受害业务系统分布

从网络探测攻击倾向的业务系统来看，本月OneLink平台被攻击次数占攻击总量的XXX%，是被攻击的主要对象，具体网络探测攻击在各个业务系统的攻击分布如下图所示：

**图2-10 网络探测攻击业务系统分布**

### {business.steps.aqsj1.data.list[2].name}类型分布

{time}，中移物联网安全态势感知平台监测到XXX次网络探测攻击事件，其中“恶意扫描”攻击XXX次,占比XXX%； “服务扫描”攻击XXX次，占比XXX%；“端口扫描”攻击XXX次，占比XXX% ；“爬虫事件”攻击XXX次，占比XXX%；“漏洞扫描”攻击XXX次，占比XXX%。

**图2-11 网络探测攻击类型分布**

### {business.steps.aqsj1.data.list[2].name}最泛滥区域分析

{time}，发起网络探测攻击攻次数最多的地域上前五个地区分别是上海、重庆、广东、浙江、江苏，分别占网络探测攻击总次数的23.58%、17.42%、14.8%、11.2%和9.6%。由此可知，64%的攻击者聚集在这五个地区发起攻击。较XX-1月比较，同样在这五个地区，发起攻击的次数分别是XXX次、XXX次、XXX次、XXX次和XXX次，同XX月环比分别是XXX%、XXX%、XXX%、XXX%和XXX%。

**图2-12 网络探测攻击区域TOP5**

## {business.steps.aqsj1.data.list[3].name}详情

{time}，安全态势感知平台共监测到{business.steps.aqsj1.data.list[3].name}{business.steps.aqsj1.data.list[3].value | numberFormat}起，相比{type==’周报’?’前一周’:(type==’月报’?’前一个月’:’’)}（{business.steps.aqsj2.data.list[3].value | numberFormat}次）{business.steps.aqsj1.data.list[3].value>business.steps.aqsj2.data.list[3].value?’增加’:’减少’}近{business.steps.aqsj1.data.list[3].value>business.steps.aqsj2.data.list[3].value?(business.steps.aqsj1.data.list[3].value-business.steps.aqsj2.data.list[3].value)/business.steps.aqsj2.data.list[3].value\*100:(business.steps.aqsj2.data.list[3].value-business.steps.aqsj1.data.list[3].value)/business.steps.aqsj2.data.list[3].value\*100 | numberFormat} %。近{type==’周报’?’5周’:(type==’月报’?’半年’:’’)}{business.steps.aqsj1.data.list[3].name}数量趋势如下图所示：

{% business.steps.aqsj3.data.timeSplitMap[business.steps.aqsj1.data.list[3].flag] ? business.steps.aqsj3.data.timeSplitMap[business.steps.aqsj1.data.list[3].flag] : business.steps.aqsj3.data.timeSplitMap | chart:’line’:’ ’}

**图2-13 近{type==’周报’?’5周’:(type==’月报’?’半年’:’’)}{business.steps.aqsj1.data.list[3].name}趋势图**



### {business.steps.aqsj1.data.list[3].name}受害业务系统分布

从入侵探测攻击倾向的业务系统来看，本月OneLink平台被攻击次数占攻击总量的XXX%，是被攻击的主要对象，具体网络探测攻击在各个业务系统的攻击分布如下图所示：

**图2-14 入侵攻击业务系统分布图**

### {business.steps.aqsj1.data.list[3].name}类型分布

{time}，中移物联网安全态势感知平台监测到XXX次入侵攻击事件，其中“暴力猜测”攻击XXX次,占比XXX%； “获取权限”攻击XXX次，占比XXX%；“网络监听”攻击XXX次，占比XXX% ；“信息收集”攻击XXX次，占比XXX%；“系统攻击”攻击XXX次，占比XXX%。

**图2-15 入侵攻击类型分布**

### {business.steps.aqsj1.data.list[3].name}最泛滥区域分析

{time}，发起入侵攻击攻次数最多的地域上前五个地区分别是上海、重庆、广东、浙江、江苏，分别占网络探测攻击总次数的23.58%、17.42%、14.8%、11.2%和9.6%。由此可知，64%的攻击者聚集在这五个地区发起攻击。较XX-1月比较，同样在这五个地区，发起攻击的次数分别是XXX次、XXX次、XXX次、XXX次和XXX次，同XX月环比分别是XXX%、XXX%、XXX%、XXX%和XXX%。

**图2-16 网络探测攻击区域TOP5**

## {business.steps.aqsj1.data.list[4].name}详情

{time}，安全态势感知平台共监测到{business.steps.aqsj1.data.list[4].name}{business.steps.aqsj1.data.list[4].value | numberFormat}起，相比{type==’周报’?’前一周’:(type==’月报’?’前一个月’:’’)}（{business.steps.aqsj2.data.list[4].value | numberFormat}次）{business.steps.aqsj1.data.list[4].value>business.steps.aqsj2.data.list[4].value?’增加’:’减少’}近{business.steps.aqsj1.data.list[4].value>business.steps.aqsj2.data.list[4].value?(business.steps.aqsj1.data.list[4].value-business.steps.aqsj2.data.list[4].value)/business.steps.aqsj2.data.list[4].value\*100:(business.steps.aqsj2.data.list[4].value-business.steps.aqsj1.data.list[4].value)/business.steps.aqsj2.data.list[4].value\*100 | numberFormat} %。近{type==’周报’?’5周’:(type==’月报’?’半年’:’’)}{business.steps.aqsj1.data.list[4].name}数量趋势如下图所示：

{% business.steps.aqsj3.data.timeSplitMap[business.steps.aqsj1.data.list[4].flag] ? business.steps.aqsj3.data.timeSplitMap[business.steps.aqsj1.data.list[4].flag] : business.steps.aqsj3.data.timeSplitMap | chart:’line’:’ ’}

**图2-17 近{type==’周报’?’5周’:(type==’月报’?’半年’:’’)}{business.steps.aqsj1.data.list[4].name}趋势图**



### {business.steps.aqsj1.data.list[4].name}受害业务系统分布

从DDOS攻击倾向的业务系统来看，本月OneLink平台被攻击次数占攻击总量的XXX%，是被攻击的主要对象，具体DDOS攻击在各个业务系统的攻击分布如下图所示：

**图2-18 DDOS攻击业务系统分布图**

### {business.steps.aqsj1.data.list[4].name}类型分布

{time}，中移物联网安全态势感知平台监测到XXX次DDOS攻击事件，其中“ACK\_FLOOD”攻击XXX次,占比XXX%； “Collaboration\_event”攻击XXX次，占比XXX% ；“HTTP\_FLOOD”攻击XXX次，占比XXX%；“Slow\_Dos”攻击XXX次，占比XXX%。

**图2-19 DDOS攻击类型分布**

### {business.steps.aqsj1.data.list[4].name}最泛滥区域分布

{time}，发起DDOS攻击攻次数最多的地域上前五个地区分别是上海、重庆、广东、浙江、江苏，分别占网络探测攻击总次数的23.58%、17.42%、14.8%、11.2%和9.6%。由此可知，64%的攻击者聚集在这五个地区发起攻击。较XX-1月比较，同样在这五个地区，发起攻击的次数分别是XXX次、XXX次、XXX次、XXX次和XXX次，同XXX月环比分别是XXX%、XXX%、XXX%、XXX%和XXX%。

**图2-20 DDOS攻击区域TOP5**

## {business.steps.aqsj1.data.list[5].name}详情

{time}，安全态势感知平台共监测到{business.steps.aqsj1.data.list[5].name}{business.steps.aqsj1.data.list[5].value | numberFormat}起，相比{type==’周报’?’前一周’:(type==’月报’?’前一个月’:’’)}（{business.steps.aqsj2.data.list[5].value | numberFormat}次）{business.steps.aqsj1.data.list[5].value>business.steps.aqsj2.data.list[5].value?’增加’:’减少’}近{business.steps.aqsj1.data.list[5].value>business.steps.aqsj2.data.list[5].value?(business.steps.aqsj1.data.list[5].value-business.steps.aqsj2.data.list[5].value)/business.steps.aqsj2.data.list[5].value\*100:(business.steps.aqsj2.data.list[5].value-business.steps.aqsj1.data.list[5].value)/business.steps.aqsj2.data.list[5].value\*100 | numberFormat} %。近{type==’周报’?’5周’:(type==’月报’?’半年’:’’)}{business.steps.aqsj1.data.list[5].name}数量趋势如下图所示：

{% business.steps.aqsj3.data.timeSplitMap[business.steps.aqsj1.data.list[5].flag] ? business.steps.aqsj3.data.timeSplitMap[business.steps.aqsj1.data.list[5].flag] : business.steps.aqsj3.data.timeSplitMap | chart:’line’:’ ’}

**图2-21 近{type==’周报’?’5周’:(type==’月报’?’半年’:’’)}{business.steps.aqsj1.data.list[5].name}趋势图**



### {business.steps.aqsj1.data.list[5].name}受害业务系统分布

从数据安全攻击倾向的业务系统来看，本月OneLink平台被攻击次数占攻击总量的XXX%，是被攻击的主要对象，具体网络探测攻击在各个业务系统的攻击分布如下图所示：

**图2-22 数据安全受害业务系统分布**

### {business.steps.aqsj1.data.list[5].name}最泛滥地区分析

{time}，发起数据安全攻击攻次数最多的地域上前五个地区分别是上海、重庆、广东、浙江、江苏，分别占网络探测攻击总次数的23.58%、17.42%、14.8%、11.2%和9.6%。由此可知，64%的攻击者聚集在这五个地区发起攻击。较XX-1月比较，同样在这五个地区，发起攻击的次数分别是XXX次、XXX次、XXX次、XXX次和XXX次，同XXX月环比分别是XXX%、XXX%、XXX%、XXX%和XXX%。

**图2-23 数据安全攻击区域TOP5**

{/business.show}

1. 改进建议

根据本月安全事件报告，可知XXX业务系统被攻击的次数增加了XXX次，其中Web攻击增加了XXX次，需要重点关注该业务系统的Web攻击防护能力。