中移物联网安全态势感知平台

月报

2020年10月

目 录

[一、 网络信息安全态势综述 1](#_Toc54354844)

[1. 业务安全态势基本情况 1](#_Toc54354845)

[1.1 日志采集情况 1](#_Toc54354846)

[1.2 安全事件情况 2](#_Toc54354847)

[1.3 业务系统受害情况 3](#_Toc54354848)

[1.4 攻击事件成功率情况 3](#_Toc54354849)

[2. 内容安全态势基本情况 4](#_Toc54354850)

[3. 基础资产安全态势基本情况 4](#_Toc54354851)

[4. 物联网终端安全基本情况 4](#_Toc54354852)

[二、 网络信息安全事件详情 4](#_Toc54354853)

[1 业务安全事件详情 4](#_Toc54354854)

[1.1 Web攻击详情 5](#_Toc54354855)

[1.1.1. Web攻击受害业务系统分布 5](#_Toc54354856)

[1.1.2. Web攻击类型分布 6](#_Toc54354857)

[1.1.3. Web攻击最泛滥地区分析 6](#_Toc54354858)

[1.2 僵木蠕攻击详情 7](#_Toc54354859)

[1.2.1. 僵木蠕攻击受害业务系统分布 7](#_Toc54354863)

[1.2.2. 僵木蠕攻击类型分布 8](#_Toc54354864)

[1.2.3. 僵木蠕攻击最泛滥地区分析 9](#_Toc54354865)

[1.3 网络探测攻击详情 9](#_Toc54354866)

[1.3.1. 网络探测攻击受害业务系统分布 10](#_Toc54354868)

[1.3.2. 网络探测攻击类型分布 10](#_Toc54354869)

[1.3.3. 网络探测攻击最泛滥区域分析 11](#_Toc54354870)

[1.4 入侵攻击详情 12](#_Toc54354871)

[1.4.1. 入侵攻击受害业务系统分布 12](#_Toc54354873)

[1.4.2. 入侵攻击类型分布 13](#_Toc54354874)

[1.4.3. 入侵攻击最泛滥区域分析 13](#_Toc54354875)

[1.5 DDOS攻击详情 14](#_Toc54354876)

[1.5.1. DDOS攻击受害业务系统分布 14](#_Toc54354878)

[1.5.2. DDOS攻击类型分布 15](#_Toc54354879)

[1.5.3. DDOS攻击最泛滥区域分布 15](#_Toc54354880)

[1.6 数据安全事件详情 16](#_Toc54354881)

[1.6.1. 数据安全受害业务系统分布 17](#_Toc54354883)

[1.6.2. 数据安全攻击最泛滥地区分析 17](#_Toc54354884)

[1.7 篡改攻击详情 18](#_Toc54354885)

[1.7.1. 篡改攻击受害业务系统分布 18](#_Toc54354887)

[1.7.2. 篡改攻击最泛滥地区分布 19](#_Toc54354888)

[三、 改进建议 20](#_Toc54354889)

1. 网络信息安全态势综述

为全面反映本月中移物联网在业务安全、内容安全、基础资产安全、物联网终端安全方面的情况，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。

# 业务安全态势基本情况

## 日志采集情况

2020年XXX月，安全态势感知平台共采集到日志XXX条，包括流量安全分析设备侧日志XXX条，WAF侧日志XXX条，4A平台侧XXX条，IDS侧XXX条，DLP侧XXX条，爬虫XXX条。

**图1-1 采集日志数量图**

XXX月份日志数量呈现上升趋势，比X-1月份（XXX条）增加近XXX%，近半年日志采集数量趋势如下图所示：

**图1-2 采集日志数量趋势图**

## 安全事件情况

本月通过监测分析共发现安全事件XXX条，包括DDOS攻击、Web攻击、僵木蠕、入侵事件、数据安全事件、篡改事件、网络探测事件。

**图1-3 安全事件数量图**

XXX月份安全事件数量呈现下降趋势，比X-1月份（XXX条）减少近XXX%，近半年安全事件趋势如下图所示：

**图1-4 安全事件趋势图**

## 业务系统受害情况

2020年XXX月，各业务系统共被攻击XXX次，其中“Onenet平台”受害最为严重，本月被攻击XXX次，取代上个月“行车卫士系统”被攻击XXX次上升至第一位。

**图1-5 业务系统受害图**

## 攻击事件成功率情况

2020年XXX月，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**

# 内容安全态势基本情况

# 基础资产安全态势基本情况

# 物联网终端安全基本情况

1. 网络信息安全事件详情

# 业务安全事件详情

2020年XXX月，本月业务安全事件共XXX起，其中Web攻击事件最多，达到了XXX次，以下按攻击次数排名对各安全事件进行详细介绍

## Web攻击详情

2020年XXX月安全态势感知平台共监测到Web攻击事件XXX起，相比上个月（XXX次）增长了XXX%，近半年Web攻击事件数量趋势如下图所示：

**图2-1 Web攻击趋势图**

### Web攻击受害业务系统分布

从Web攻击倾向的业务系统来看，本月OneNET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Web攻击在各个业务系统的攻击分布如下图所示：

**图2-2 Web攻击业务系统分布**

### Web攻击类型分布

2020年XXX月，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**

### Web攻击最泛滥地区分析

2020年XX月，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**

## 僵木蠕攻击详情

2020年XXX月安全态势感知平台共监测到僵木蠕病毒XXX起，相比上个月（XXX次）增长了XXX%，近半年Web攻击事件数量趋势如下图所示：

**图2-5 近半年Web攻击趋势图**



### 僵木蠕攻击受害业务系统分布

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**

### 僵木蠕攻击类型分布

2020年XXX月，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**

### 僵木蠕攻击最泛滥地区分析

2020年XX月，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**

## 网络探测攻击详情

2020年XXX月安全态势感知平台共监测到网络探测攻击XXX起，相比上个月（XXX次）增长了XXX%，近半年网络探测攻击事件数量趋势如下图所示：

**图2-9 近半年网络探测攻击趋势图**



### 网络探测攻击受害业务系统分布

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**

### 网络探测攻击类型分布

2020年XXX月，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**

### 网络探测攻击最泛滥区域分析

2020年XX月，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**

## 入侵攻击详情

2020年XXX月安全态势感知平台共监测到入侵攻击XXX起，相比上个月（XXX次）增长了XXX%，近半年入侵攻击事件数量趋势如下图所示：

**图2-13 近半年入侵攻击趋势图**



### 入侵攻击受害业务系统分布

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**

### 入侵攻击类型分布

2020年XXX月，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**

### 入侵攻击最泛滥区域分析

2020年XXX月，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**

## DDOS攻击详情

2020年XXX月安全态势感知平台共监测到DDOS攻击XXX起，相比上个月（XXX次）增长了XXX%，近半年DDOS攻击事件数量趋势如下图所示：

**图2-17 近半年DDOS攻击趋势图**



### DDOS攻击受害业务系统分布

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**

### DDOS攻击类型分布

2020年XXX月，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**

### DDOS攻击最泛滥区域分布

2020年XXX月，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**

## 数据安全事件详情

2020年XXX月安全态势感知平台共监测到数据安全事件XXX起，相比上个月（XXX次）增长了XXX%，近半年数据安全事件数量趋势如下图所示：

**图2-17 近半年数据安全事件趋势图**



### 数据安全受害业务系统分布

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2-18 数据安全受害业务系统分布**

### 数据安全攻击最泛滥地区分析

2020年XXX月，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2-19 数据安全攻击区域TOP5**

## 篡改攻击详情

2020年XXX月安全态势感知平台共监测到数据篡改攻击事件XXX起，相比上个月（XXX次）增长了XXX%，近半年篡改攻击事件数量趋势如下图所示：

**图2-20 近半年篡改攻击趋势**



### 篡改攻击受害业务系统分布

从篡改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，具体篡改攻击在各个业务系统的攻击分布如下图所示：

**图2-21 篡改攻击受害业务系统分布**

### 篡改攻击最泛滥地区分布

2020年XXX月，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2-22 篡改攻击区域TOP5**

**内容安全**

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。