移动恶意程序监测系统产品彩页

1、产品介绍

1.1 产品简介

移动恶意程序监测系统主要实现2G/3G/4G/5G网络场景下的流量解析、协议识别、资产识别、样本还原、流量安全监测、封堵处置等功能，并且能够支持接收、执行工信部工业互联网网络安全公共服务平台（简称部平台），中国移动手机恶意软件监测系统（简称集团平台）下发的指定监测、处置指令，将对应的监测处置结果按规范上报反馈。

1.2 产品形态

软硬件一体机，通过交换机、路由器、分光器等镜像网络中的流量旁路部署在网络中。

1.3 核心功能

1）采集功能

- ✓ 支持HTTP、FTP、SMTP、POP3、IMAP等协议的识别、解析和还原；
- ✓ 支持MQTT、XMPP、COAP、ONVIF、RTSP、GB/T 32960、JT/T 808、JT/T905等物联网（车联网）协议的识别和解析；
- ✓ 支持对Android、IOS、Symbian、WindowsPhone、J2ME、HarmonyOS等移动平台文件样本的识别；
- ✓ 支持apk、ipa、jar、dex、hap、zip、elf和so等类型的文件还原；
- ✓ 支持流量以pcap的方式留存和上报。

2）自主监测功能

- ✓ 支持恶意受控事件、恶意传播事件、网络威胁事件和特定类型应用使用和传播事件监测。

3）处置功能

- ✓ 支持封堵和重定向动作，支持基于网元和位置信息的封堵。

4）协同联通功能

- ✓ 支持URL、域名、IMEI、Apn、目的IP、目的端口、传输层协议和应用层协议等维度的恶意资源监测指令；
- ✓ 支持Snort和MTX指令恶意报文监测指令；

✓ 支持目的IP、URL、域名、MD5和yara规则的恶意文件监测指令；
✓ 支持URL、IP、域名、MSISDN的处置指令。

1.4 产品优势

1）关联率高：有完整的从信令面流量采集、用户信息分发、用户面接收到用户面关联方案；有着高达 97%的关联率。

2）检出率高：持续积累了大量高质量本地规则，提升了网络威胁事件的检出；支持各类异常还原场景，保证了黑样本的检出率；部侧考核有 85%以上的检出。

3）封堵率高：支持多维度规则的封堵；部侧各类考核有近 100%封堵率。

4）考核流程化：在长期的恶意考核、反诈考核、安全中台考核中，已经形成一套完整的应对流程；监测和处置类能有将近 100%的命中率；自主安全类能有 85%的检出率，达到考核要求。

2、部署场景

1）控制面信令采集

大区制：大区中心通过转发网关将对应省份控制面数据回传至本省中心机房接收网关，经由汇聚分流设备送至控制面信令分发设备进行流量采集、解析。

省分自建：则直接在省中心机房通过汇聚分流设备输送控制面信令流量。

2）用户面流量采集

采用近源部署方式，在近 UPF 侧部署流量安全监测处置设备，从汇聚分流设备获取用户面流量。