安全小课堂第七十九期【威胁情报】

原创：京东安全 京东安全应急响应中心 2017-11-28

在过去的几年中，术语“威胁情报”迅速出现在信息安全领域，许多安全厂商现在为消费者提供威胁情报服务。那么威胁情报到底是什么意思，它是一种什么概念或者机制呢？

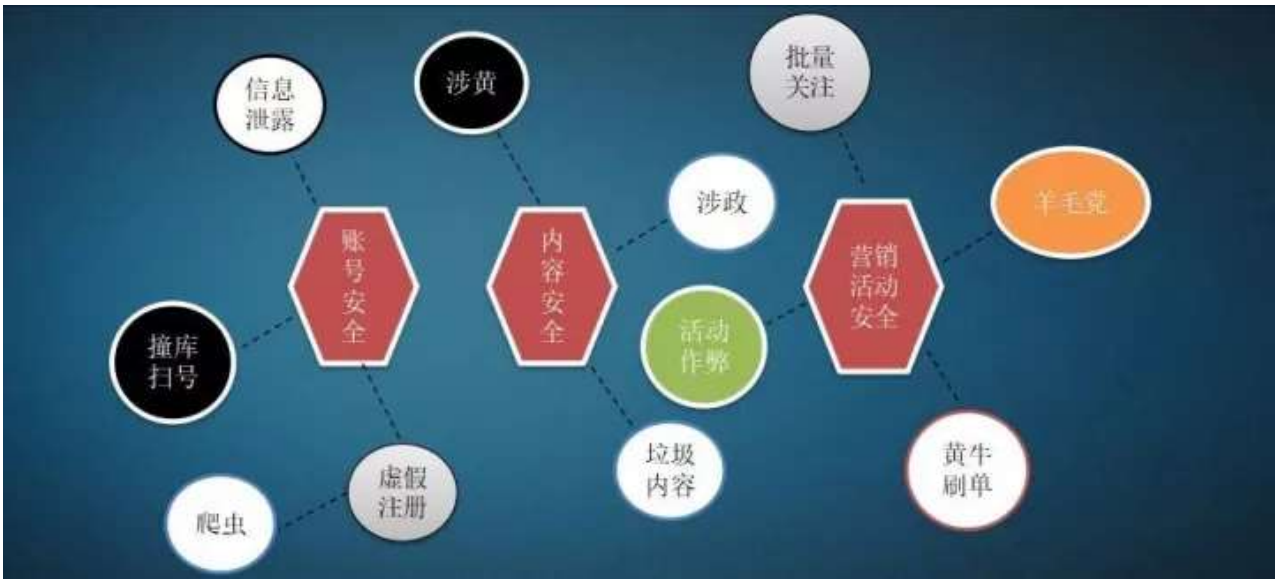
JSRC **安全小课堂第七十九期**，邀请**到彭巍**作为讲师就**威胁情报**为大家进行分享。同时感谢白帽子们的精彩讨论。

什么是威胁情报？

京安小妹

彭巍：

恩，可能要先解释下什么是业务安全。每个企业都有自己的业务，所谓业务安全，就是指在企业主要的业务上发生的安全问题。业务安全与终端安全、网络安全、web安全等对比来说的话，后者主要是研究操作系统本身、网络、web系统的安全性，而业务安全是关注业务本身的问题。业务安全范围内比较被大家所了解的场景包括账号安全、内容安全、营销活动安全三大块。所以业务安全的威胁情报，就是能发现业务正在被攻击的情报。这是一个业务安全锁涉及的范围图：



讲师

威胁情报有哪些种类？

京安小妹

彭巍：

业务安全威胁情报，可以分为两大类
1、开源情报：监控qq、论坛、接码平台、纳暗网内容获取到的情报，这部分情报经分析，可以直接还原出黑产针对某个业务的完整作案手段，起到告警作用和提前预防作用
2、闭源情报：监控暗网黑产攻击流量得到的情报，能直接监控到黑产攻击的接口详细信息、来源、路径等。

讲师

如何从威胁数据中提取出威胁情报?

京安小妹

彭巍：

针对前面说的类型，分为两种手段
1、针对开源情报，开源情报一般只是提到一些关键路径，所以需要有运营人员专门跟进，然后挖掘出更深层的作案路径
2、针对闭源情报，就是根据数据包特征写提取规则，自动化提取情报了

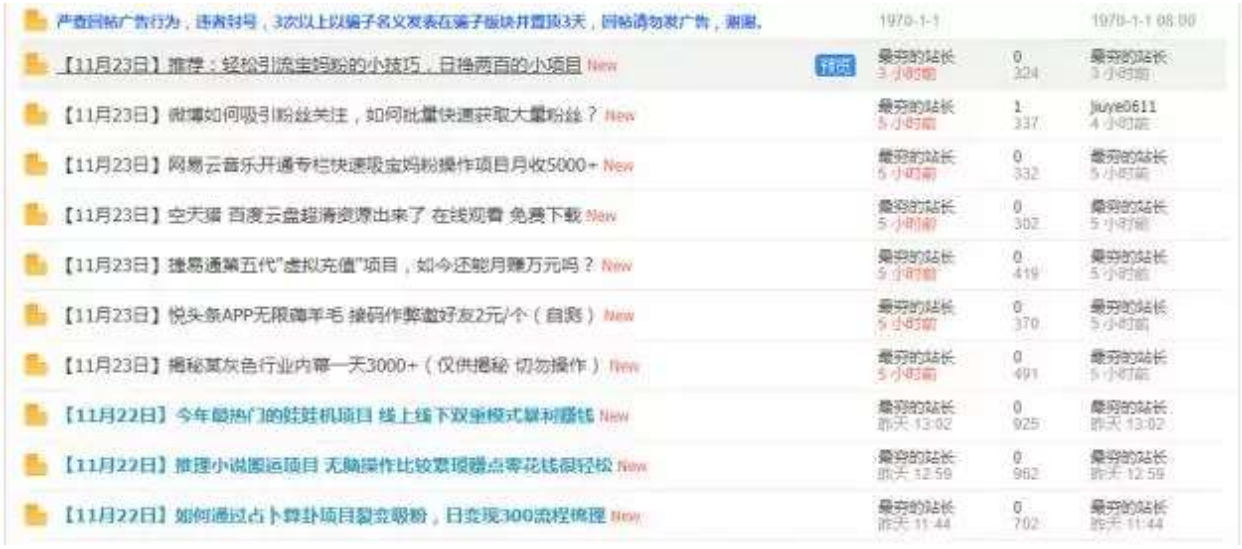
讲师

能否举一些实例，真实世界的威胁情报是什么样子的?

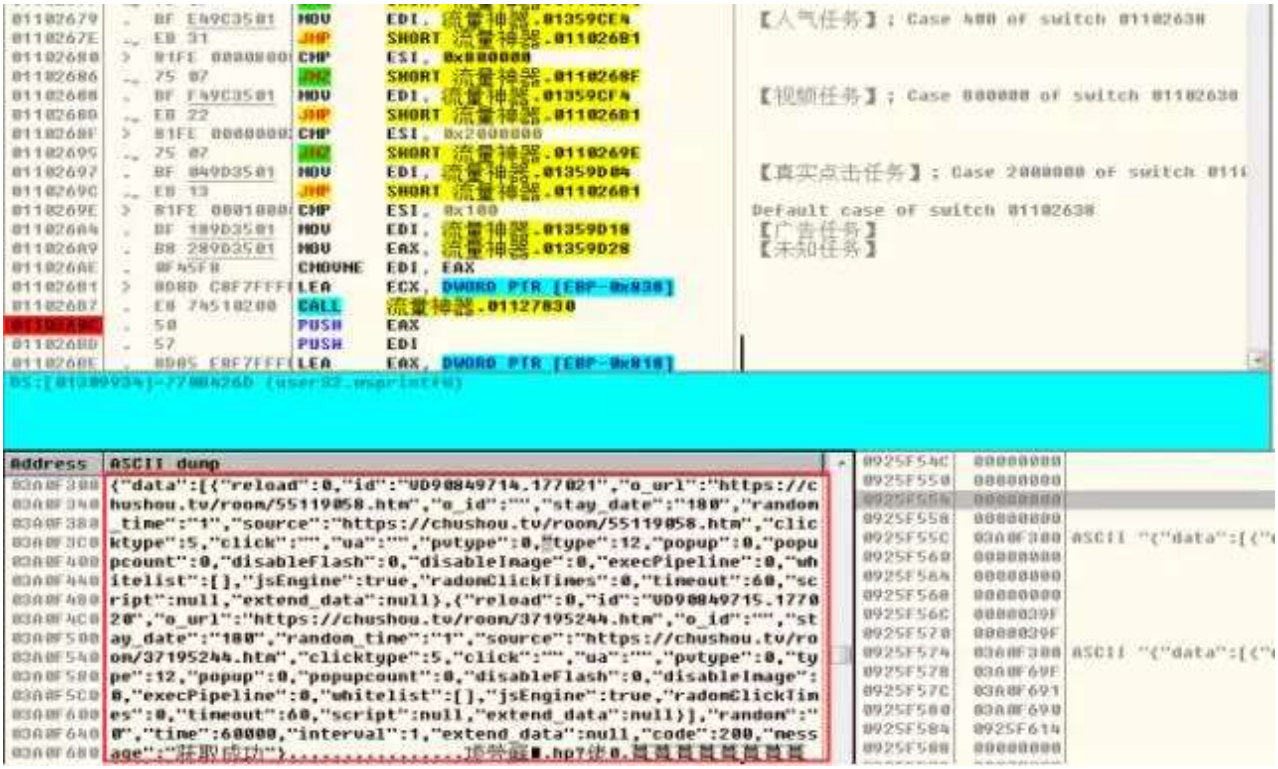
京安小妹

彭巍：

http://www.huaxiawz2.com/
这是一个薅羊毛项目平台，爬取这里的信息就是刚说的开源情报的一部分



然后运营通过项目列表，还原出作案手段，最后如果有工具的话再通过od分析工具，提取出下发任务的数据包，就可以实时抓取到开源情报并通知给被攻击方



上面是一个刷爱奇艺播放量工具的情报数据包，就可以实时监控当前是在刷哪个视频。

讲师

企业拿到威胁情报后有哪些应对措施呢?

京安小妹

彭巍:

没有情报之前，企业往往是事后才能发现业务被攻击了。情报实际上就是起到了一个实时报警功能，可以立马根据情报调整接口的访问策略，例如限制访问的ip频次，直接拉黑攻击的来源ip、地域、设备id等

讲师

有哪些好的威胁情报分析平台推荐?

京安小妹

彭巍：

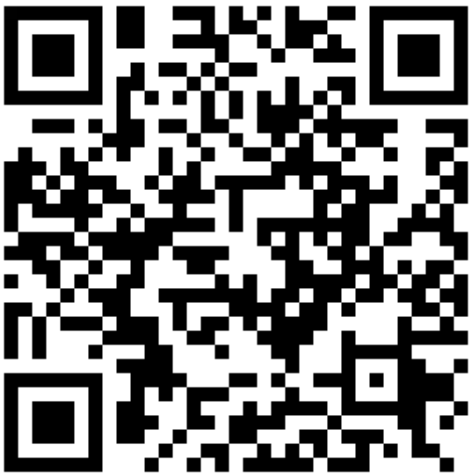
针对业务安全的威胁情报分析平台目前还没有公开开放的= =

讲师

本期JSRC 安全小课堂到此结束。更多内容请期待下期安全小课堂如果还有你希望出现在安全小课堂内容暂时未出现，也欢迎留言告诉我们。

安全小课堂的往期内容开通了自助查询，回复“安全小课堂”或者点击阅读原文进行查看。

最后，广告时间，京东安全招人，安全开发、运营、风控、安全研究等多个职位虚位以待，招聘内容具体信息请扫描二维码了解。



简历请发送：cv-security@jd.com

微信公众号：jsrc_team

新浪官方微博：京东安全应急响应中心