电商和O2O行业诈骗那些事儿（上）——安全小课堂第八期

京东安全应急响应中心 2016-04-29

安全小课堂第八期

电商公司、O2O企业发展迅速，给你我生活增添不少便利，但刷单泛滥致大数据污染，信息安全隐患逼近电商平台。 例如，电商的诈骗电话、冒充客服、钓鱼网站、O2O的刷单现象等着实让人头疼。

为了更有效的、全方位的交流电商诈骗防护，本次我们特意邀请不同行业领域的专家来和大家分享电商和O2O行业诈骗那些事儿。鼓掌欢迎唯品会高级安全研究员森尼、大众点评业务安全负责人纪东、携程高级安全研究员小胖胖要减肥~

1

豌豆妹

电商和O2O行业的诈骗行为有哪几类呢？

哆啦A梦

主要分两块：1、不知晓用户详细信息。类似于快递费的诈骗，寄送一个无效电话卡等，骗取到付快递费；2、知晓用户详细信息。（1）针对订单取消、退货，如航空故障，问题商品等；（2）银行卡、信用卡类的欺诈，获取用户短信，盗用用户相关钱财。这类是当前影响较大的，如之前曝出拿到用户一个绑定手机验证码，可以将用户所有卡余额取完。

小丸子

在团购类网站，除了银行卡盗卡诈骗，目前比较典型的是以花呗套现为名的诈骗。在QQ群发布套现信息，在团购网站下一个订单，让受害人用花呗支付，支付完后不进行兑付。下的订单一般是容易变现的如电话卡，超市储值卡之类，或者是虚假商户团单。

小新

我们遇到比较多的还是基于订单和物流信息的诈骗，这些都可以通过黑市去购买，用来套取用户的银行卡信息，实施诈骗。当前各种新型诈骗手法凸显，也需要不断提高购物人的安全意识，包括购物后的短信提示，用户中心的下单提示等。

2

豌豆妹

诈骗的种类很多，针对恶意者来说，他们的目的和利益点分别是什么？

葫芦娃

最终获利的主要还是基于两点：1、获取用户更多信息实行另外的诈骗；2、直接通过该点进行获利。

小丸子

当前损失比较多的一般都是银行卡、信用卡类诈骗。诈骗多是为了获取一定的收入，不同诈骗团伙获利方式不一样。有的基于隐私数据、有的基于账户财产、有的基于信购能力等。

3

豌豆妹

如何有效防御行业内的相关诈骗行为呢？

小新

1、用户自身方面，进行相关诈骗信息的提示和预警；2、网站方面，从各个环节排查信息泄漏点，进行用户信息各层保护，包括物流、第三方系统等；3 、各个重要业务模块方面，包括卡类支付、余额、信贷，都需要严格进行风控和用户信息校验，进行相关风险防护。4、从业人员方面，安全人员需要不断了解新的攻击手法，同时也要深入到敌后，提前部署相关防御。

哆啦A梦

赞，补充一点。从B端，要加强对商户、商品的审核和管控。杜绝虚假商户、限制易变现商品的信用支付等。

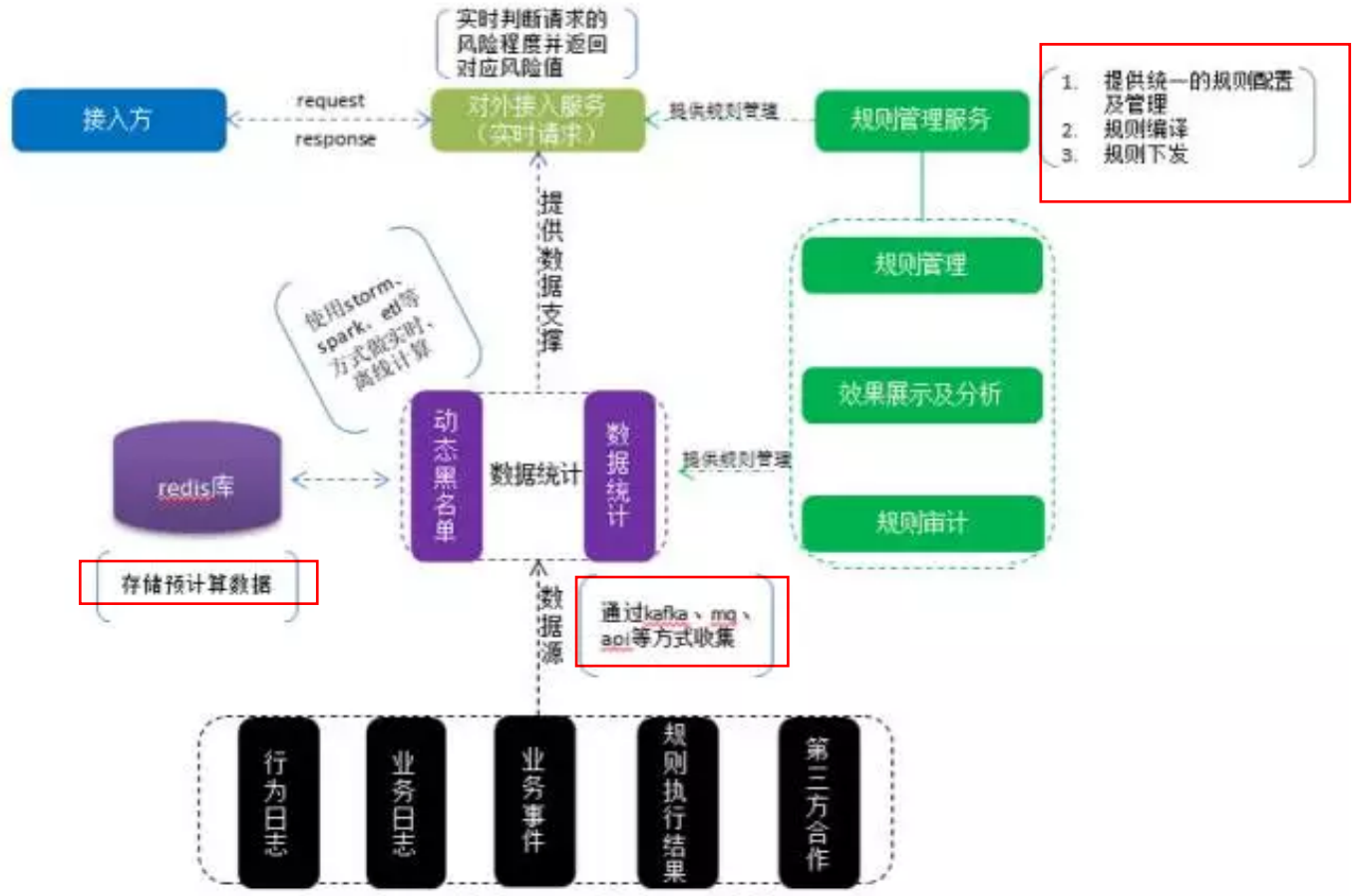
4

豌豆妹

甲方的小伙伴能给介绍下电商和O2O行业方面风控平台的搭建么？

小丸子

以下系统架构图可以参考。



小新

风控系统主要分几方面：1、规则引擎；2、底层数据；3、api接口服务。同时业务人

员需要对数据进行分析，提炼相关规则进行设定，同时底层数据这块可以进行聚类拟合等模型算法。当前输出大多平台都是以api服务模式，当然也有进行直接流量层的防护。风控是一个复杂的系统工程，会用到各类大数据技术，高并发，还有模型算法等，来支撑恶意行为的防护。

葫芦娃 

我们的风控平台由规则服务，处罚中心，数据中心组成。规则服务主要用于定制风控的规则，处罚中心处理触发的规则事件，这里分为人工和自动处理。数据平台是挖掘用户数据，构建模型，优化规则的平台。当然，风控识别离不开和业界其他团队合作。

豌豆妹

不觉明厉！！！聊了那么久，大家想必都累了吧，休息~休息~一会儿~我们下期再见，接着聊“电商和O2O行业诈骗那些事儿”。




安全小课堂往期回顾：

1、论安全响应中心的初衷；
2、安全应急响应中心之威胁情报探索；
3、论安全漏洞响应机制扩展；
4、企业级未授权访问漏洞防御实践；
5、浅谈企业SQL注入漏洞的危害与防御；
6、信息泄露之配置不当；
7、XSS之攻击与防御。

JSRC http://security.jd.com/

长按识别左侧二维码，关注我们