安全小课堂第127期【威胁情报的不同玩法】

京东安全应急响应中心 1月21日

做威胁情报的目标是补充传统安全的遗漏面，对于甲乙方需要的都是及时的发现+足够的数据+全面仔细的分析，数据的全面性，开源向参考OSINT，闭源向就看各家资源与目标。白帽子则是爬虫与黑吃黑。

JSRC **安全小课堂第127期**，邀请到**智慧的西瓜**作为讲师就**威胁情报相关的的技术**为大家进行分享。同时感谢小伙伴们的精彩讨论

白帽子视角中的威胁情报？

京安小妹

智慧的西瓜：

白帽子眼中不同的是对溯源方向其实需求很少,多数的目标是发现目标问题且能产生价值的点。

比如：用户信息、员工账号和密码、公司特殊文件、业务敏感信息如代码等泄露事件，用户中心ID，手机号 ，售卖或者使用的工具、活动交流的渠道

且这类在甲方视野里是会有缺失的,原因也很多，一般是员工信息安全意识的普及与习惯问题导致,所以获取渠道多会以爬虫为主

比如github，网盘，印象笔记，论坛，QQ个人资料，邮箱，1pass

目标就是甲方企业的资产

还有一个方向则是黑吃黑

这类需要跟进黑产的动向玩法动态

比如羊毛信息，第三方安全问题，数据窃取售卖，但一般这部分甲方也会同时间得到，要看处理时间与深度

甲方视角中的威胁情报？

京安小妹

智慧的西瓜：

甲方讲体系

因为要对比得到付出比

且目标单一，问题一定要涉及自身

但由于甲方自身的风控系统或soc或日志系统类的存在已经算是威胁情报了

一般都是再由乙方补充一部分行业类数据，就可以发现很多存在的问题比如黑产IP类，除自身风控问题外，自己要做付出和得到的价值是不成比的

讲师

乙方视角中的威胁情报？

京安小妹

智慧的西瓜：

乙方最重要的是要全面、独有

比如，恶意ip，手机，信息

因为乙方的威胁情报定位是补充甲方和发现大规模事件预警

乙方是可以找一些警方顾问类头衔做一些深度玩法

乙方提供的东西最怕是不好利用的

比如一些时间标签有点久的IP库或者溯源里的结论只是真实与否这种情报溯源类服务一般都要点到问题全面的能力数据再加上脑洞

讲师

威胁情报溯源案例分析?

京安小妹

智慧的西瓜:

遇到过一个很有意思的过程
以国内某点发现的大匿名情况为背景
能拿到只有一个国内邮箱，和一个ID
发现前者是以未实名的虚拟号段注册的
后者id在国内各处也并未发现痕迹
分析已有在几处留言发现他的英文特别好
几乎没有中文语法类问题
中式英语这种
把id和邮箱做了组合类字典在国外做了查询分析
id是个英文短语
发现了疑似在国外的痕迹
但是个gmail的邮箱
后来在痕迹时间点上核对发现就是本人，然后就定位到了人
国外网上痕迹问题其实比国内还严重，只是习惯流程等不同

讲师

互动问答环节:

1.黑产动态如何追踪？或者你认为现在最有效的方法?

讲师:

先找到他们最常用的，再一步步的沟通加深，找到其它渠道
暗网监控、Q群，telegram，微信都算渠道

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，点击菜单栏进入“安全小课堂”即可浏览。

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