威胁猎人产品总监彭巍：业务安全发展趋势及对安全研发的挑战

原创

csdn业界要闻 于 2017-12-01 15:45:06 发布 507 收藏
文章标签： 安全 彭巍 威胁猎人 看雪安全开发者峰会

11月18号，2017看雪安全开发者峰会在北京悠唐皇冠假日酒店举行。来自全国各地的开发人员、网络安全爱好者及相应领域顶尖专家，在2017看雪安全开发者峰会汇聚一堂，只为这场“安全与开发”的技术盛宴。

正如暗网之于互联网世界，现实生活中的黑灰产业远比你想象中得要复杂。在利益的驱动下，这些隐形产业逐步发展壮大并形成了各自的体系，如接码平台、撞库等，这些都给社会造成了严重的危害，特别是对企业的业务提出了极大挑战，如何对抗黑灰产业自然也就成了安全从业者迫切需要解决的问题。在《业务安全发展趋势及对安全研发的挑战》主题演讲中，威胁猎人产品总监彭巍为我们带来了有关企业业务安全的发展及相应对抗实践，重点揭露了无孔不入的地下暗黑世界，震惊之余也引发了我们对业务安全的思考。

威胁猎人产品总监彭巍

> 彭巍，威胁猎人产品总监。曾任职于猎豹移动，负责金山毒霸系统查杀引擎的研发，解决终端安全问题。2017年初加入威胁团队，专注业务安全相关黑灰产研究及对抗

以下为演讲速记：

彭巍：大家好。本次分享的主题是业务安全的发展趋势以及对抗思路，这里我先自我介绍一下，我之前在金山赌霸负责系统差还引擎开发，解决终端安全问题，今年年初加入了威胁猎人团队，这是一个专注业务安全相关黑灰产研究的团队。我的title，之前写的是产品总监，实际上我职务应该是产品总监加服务端研发负责人，希望大家接下来不要带种族歧视来鄙视我。

这是我分享的三个部分，第一，业务安全是什么。第二，业务安全昨天和今天。第三，针对对抗中的一些核心问题，提出对抗思路。

业务安全是什么

业务安全，顾名思义就是指企业业务上发生的安全问题。对比于中终端安全，网络安全，WEB安全，后者主要研究操作系统本身或者说网络、WEB系统的安全性，而业务安全是关注业务本身的问题，它的范围被大家所认知的，包括帐号安全、内容安全以及营销活动安全。下面是它的详细分支，包括黄牛刷单、羊毛党等属于业务安全的范畴。业务安全解决的问题，大部分的情况就是去识别访问业务的是机器还是人，这个人是业务用户还是正常用户？

业务安全昨天和今天

业务安全的昨天和今天。业务安全的历史，首先按照移动互联网的爆发分为两个大的阶段，PC互联网这边又可以分为两各小的部分：

第一个阶段，2007年之前，这个阶段可以总结为刚起步的黑产对抗腾讯阿里等企业。因为在这个阶段，2007年之前腾讯阿里等厂商因为各自业务逐渐开始涉及到庞大社交、游戏、线上交易等场景，于是黑产开始盯上这一块利益，厂商也开始逐步重视。这个阶段的特点其实是攻防节奏比较慢的，防守方也是简单风控规则。

第二个阶段，2008-2010年，这个阶段黑产开始形成成熟的产业链，分工明确，各点击穿，同时防护方也开始形成立体的风控手段，这个阶段业务安全开始作为企业安全的重要一环，被互联网所认知。目前为止攻守双方是你来我往。

第三阶段，随着互联网快速普及，互联网各个细分领域快速增长，这个黑黑键逐渐健壮，大厂商是小步快跑以及新互联网的崛起情况，这个时候攻守双方逐渐拉开了距离。在目前的阶段，两点明显的趋势：

1. 场景爆发带来的业务安全问题陡增。这是一张监控解码平台响马列表得出来的，可以看到2011-2017年，薅羊毛产业链主要目标O2O、互联网金融、电商等都是极速增长，并且每天都有新的项目出现。通过撞库供给线路图，每一年都有新增的出现。黑产的魔爪已经无处不在，这是快销行业常见的再来一瓶，也是我们通过解码平台发现有出现快销行业各种关键词，东鹏特饮、康师傅等，这个二维码不知道大家是否见过，现在快销行业为了提高再来一瓶的体验，直接会把二维码印在瓶身上扫码之后就可以挂住它的微信号或者公众号，再接下来可以进入它的公众号扫它的瓶盖领它的二维码，最终回流到垃圾站，被重复刷。产商本来花一千万想做五千万的的事情，结果被黑产薅走了三千万。
2. 黑产技术飞跃式的发展，黑产技术发展超乎想象，人多，耗的钱也多。另外获取IP资源的技术，IP作为互联网的紧缺资源，一直是厂商防守最重要的风控方案之一，如何获得IP资源也是黑灰产业获得主要解决的问题，可以总结为经历了三个阶段。通过逆命代理，批量获取个人ADSL拨号IP，虚拟化ADSL实现海量IP资源获取。最后一个阶段我们所说秒拨，目前黑产获取IP资源的成本已经大大降低，对于防守方的简单规则IP的品质这个策略就是一个颠覆。这是一个秒拨的截图，看起来像ADSL家用的一样，实际不是，这里会有一个启用换IP，还有某宝上的搜索关键词，大量类似服务都可以买到。接码平台，接码平台出现设备流转和卡的流转都极其不方便，且耗费成本。现在卡商和羊毛党通过接码平台实现了手机黑卡无缝流转，大量提高了黑产生产效率，同时也对防守方产生很大的压力，这是解码平台的截图，是接受验证码平台。

业务安全对抗的核心问题和对抗思路

业务安全对抗的时候核心问题和对抗思路。这是网上看到的图，这就是业务安全最核心的问题，就是有一群人比你聪明，他们比你有更多的资源。那你怎么办？言归正传。业务安全防守方目前核心问题是一个攻守双方严重信息不对称的问题，体现在三个方面从供给方来说供给的平面爆发，供给场景爆发带来平面快速增长，这对你防守方的安全管理系数难度大大增加，守方来说对黑产认知盲区增加，有一些触网的了大企业根本不知道这个面临业务安全问题是什么？传统安全管理失控，传统的安全团队都是期望与内部业务部门制定标准，但是随着业务的不断发展，安全团队其实是无法感知业务安全上接口风险，因为你甚至都不知道某一个业务新增的接口，这今天总结起来防守方都不知道自己被攻击了，都是事后被发现的。这是认知盲区的例子，是前段时间从某拼车APP血泪教育中的图，虽然不是导致他们倒在资本寒冬中的证明原因，但是证明大部分厂商对于业务安全是完全未知的，这是一个拼车APP，每天补贴掉100万，后来证明30%是被刷单者拿走了。

对抗思路，情报是各大安全领域的重大手段。业务安全的情报主要是搜集什么样的情报，两个类别来说明：

1. 开源情报。开源情报就是指监控QQ、论坛、QQ群、论坛、解码平台以及暗网获得的开源情报，这部分的情报经分析可以直接还原出企业某一个企业的作案手段直接起到告警或者预防的作用。这是我们的监控论坛的论坛截图，这是接码平台的截图，刚刚提到东鹏特饮的例子，就是我们通过关键词东鹏特饮这个入手还原出的作案手段。

谢谢大家！

> 注：本文根据大会主办方提供的速记整理而成，不代表CSDN观点。

2017看雪安全开发者峰会更多精彩内容：

- 2017看雪安全开发者峰会在京召开 共商网络安全保障之策
- 中国信息安全测评中心总工程师王军：用技术实现国家的网络强国梦
- 兴华永恒公司CSO仙果：Flash之殇—漏洞之王Flash Player的末路
- 中国婚博会PHP高级工程师、安全顾问汤青松：浅析Web安全编程
- 启明星辰ADLab西南团队负责人王东：智能化的安全——设备&应用&ICS
- 自由Android安全研究员陈愉鑫：移动App灰色产业案例分析与防范
- 腾讯反病毒实验室安全研究员杨经宇：开启IoT设备的上帝模式
- 绿盟科技应急响应中心安全研究员邓永凯：那些年，你怎么写总会出现的漏洞
- 腾讯游戏安全高级工程师胡和君：定制化对抗——游戏反外挂的安全实践
- 绿盟科技网络安全攻防实验室安全研究员廖新喜：Java JSON 反序列化之殇
- 阿里安全IoT安全研究团队Leader谢君：如何黑掉无人机