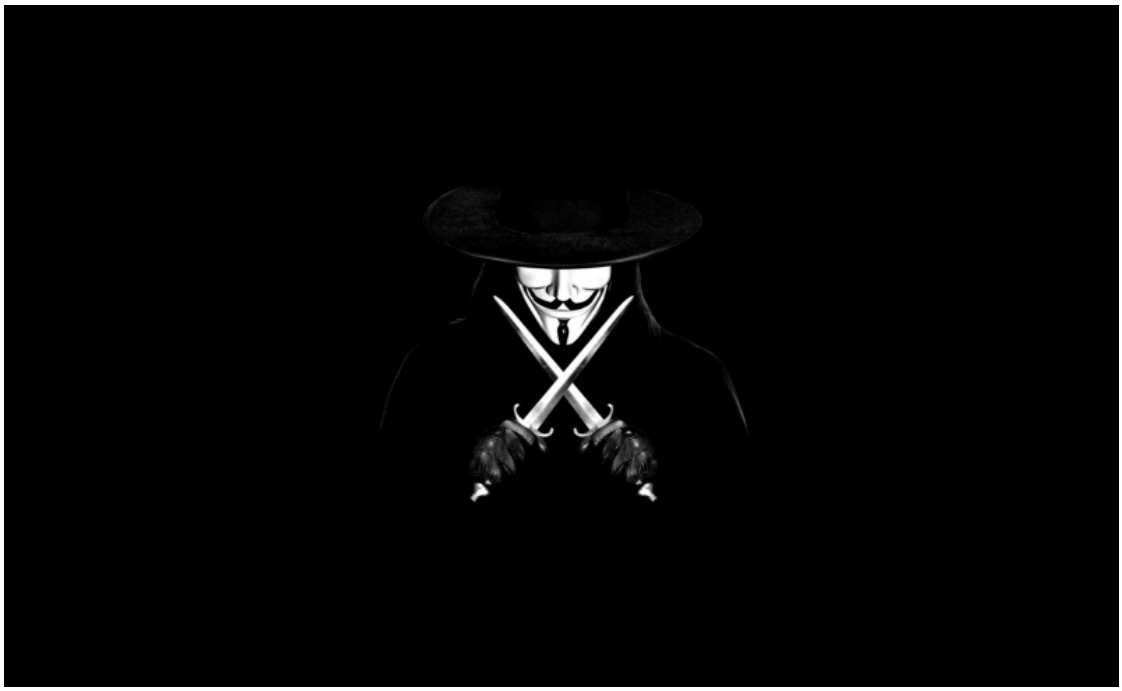
黑产无间道：黑产威胁情报工作实战

匿名用户 2015-09-17 ¥



与现在安全界流行的威胁情报不同，我们在威胁情报的工作更核心的是基于公司业务实际出发而开始的，整过程较为朴素，没有那么多高大上的工具整合，一切以为安全提供实际支撑为核心。

一、初创阶段

1.1 起因：

最初的起因是由于一起信息泄露案件，由于信息泄露产生了较大的金融欺诈损失，后来案件在公安机关的侦下查明。但我们发现整个作案过程，和我们在后台推测的情况有较大出入，所以我们的一些防控措施完全打了别处。在这件事的基础上我们认识到，知己知彼百战不殆，总是在家里分析日志，推测对方的攻击手法是够的，还要能够打出去，真正了解黑产运作环节，才能有针对性的进行精准打击。

最初在这个环节，我们并没有考虑成立一个团队来进行。仅是安排了两名同事来做，一个是偏技术的，主要作方向是找到黑产对漏洞的利用手法，由于我司业务规模大，一旦出现一个漏洞，迅速会被黑产利用，并做教材开培训班，这名技术人员就要打入到这种圈子里去学习技术。另一个是数据方向的，在黑市发现采购数据，并进行数据分析，查找泄露源。

1.2 进展:

工作迅速取得了成果，数据方向的同事在短期内，连续发现某物流公司、某银行的数据接口、某第三方软件出现大量的、带有明显集中特征的泄露。技术同事则发现了APP老版本存在的问题，渠道接口存在的漏洞。于这些情报是从黑产直接取得，所以效果非常好，可以迅速有针对性的修补漏洞，迅速止血，并能够根据攻路径找到受损客户进行加强保障。所以短期内解决了比较集中突出的问题。

但过程中我们也发现几处问题，一个是黑市欺诈多发，在黑市上贩卖技术也好、数据也好，相当多都是诈骗为，骗子们甚至几十块也骗，声称自己具有某种技术，并且伪装成果。这就需要有经验、熟悉业务的人去辨真假，即使这样，也存在被骗的可能性，而稳定有保障的黑市来源，又迅速被我们掐掉。被骗钱倒不是大问题，比起我们提供的保障来说，这只是小钱，但是浪费时间浪费人力，不是一般的浪费，每笔都要防骗，需大量的沟通。

1.3 思考：

再一个是发现真正的问题不易，处理更不易。很多乙方做安全的，觉得这些问题都简单，上个WAF做个规则或者改一下代码就解决了。但实际到甲方，尤其是大型甲方的生产环境，需要沟通处理的环节很多。比如前发现的APP老版本存在漏洞可被利用，简单的办法是强制升级解决，版本不对就禁止使用。但实际上要考量这个低版本对于某些老旧机型是适用的，而新版本在一些老旧手机上运行不了，那就要拍板做决策，我们到要不要这批老客户，拍板的时候就要数据来说话，数据运营的同事来说，目前低版本用户量多大，活跃量多大。当你有几百万的低版本用户时候，安全的人说都不要，业务会立刻跳起来跟你拍桌子。这时候安全的就须要提供其他解决方案，而不是简单的一刀切，其他的解决方案就要考虑开发周期，短期内怎么处理，长期怎么处理—-所以，你看这一轮下来，还不算组织会议、邮件沟通、数据提取分析的时间。所以一个CASE处理来，就需要一个时间周期，而且解决方案也是一个比较复杂的过程，相关人员都要投入。

由于初期运行有一些快速重要的发现，所以我们决定这个领域要继续投入人力。

二、成长阶段

新增的人力投在几个方向，因为事件解决比较费时，所以重点投入，一个专职负责解决跟进漏洞，一个兼职跟进，按照两名人员的特长划分移动端和PC端。前端也增加了两名，一个在技术方向，一个在数据方向。所以这个小组变成了6个人，从中选了一位同事做组长。而对组长的考核是情报数量、质量、问题解决数量。由此情报工作进入了第二个发展阶段。

2.1 新问题：

随着人力的投入，情报的数量质量都有大幅提高–可见以前我们缺课太多，总是坐在办公桌后面看日志，会以为自己做的还不错，只有掌握黑产动态，才知道自己有多少问题。情报的来源也比较广泛，来自于各个黑产QQ群、论坛贴吧、网站，并且在线下也有比较稳定的中间人交易。解决方案的推动也开始走向规范化，而不是见洞补洞，开始向开发端延伸。

当然随之而来也产生了新问题，当前我们进行的都是收集情报，线上防御，存在情报传递失真的情况。所谓

报传递失真，要从产业链上下游来看，通常我们接触到的都是产业链最后一环，贩卖数据或出售技术的最后
益环节，但是往产业链上游溯源，还有拦截马、洗料加料等各个分工环节，所以如果只停留在终端环节，各
信息的来源实际上是模糊不清的，就造成情报信息需要多种解读才能处理成真正的情报，而风险对于我们来
每一秒都是损失，所以降低损失必须朝产业链上游挖掘。也在这个时候，正好发生了一件事情，从数据情报
我们发现一起案件，最后查明属于内外勾结，深入挖掘后，我们发现是黑产组织派人打入我们内部的，黑产
织了一些学历好、背景干净的人进入了我们的客服部门打探情报，收集数据，这个事情的发现使我们非常震
惊，看来情报工作已经进入了互相渗透、直接对抗的阶段。由此我们决定同样也要进行反渗透工作。

2.2 反渗透：

所谓反渗透，对于我们这样的正规机构来说，存在一个主要的操作难题，我们很难派一个自己的员工去从事
产工作，但不入虎穴焉得虎子。在咨询了法务、公安部门后，我们决定退一步，委托其他机构进行调查。其
机构里，最合适的就是记者了，记者职业发展这么多年，在如何寻找线索，如何让伪装沟通上还是有相当丰
的经验和方法的。通过我方人员配合记者深入调查，我们掌握了产业链相关生产、销售、沟通方法，为向上
产业链延伸提供了有力的支撑，同时也学到了记者们的工作方法，能够独立开展调查。

另外一个问题是，通过对产业链的溯源，我们聚焦了一批犯罪分子，这些人对业务了解程度高，具有相应的
发能力，能够批量生产攻击软件。很多案件的背后都有这些人的身影，如果把这批人抓住，将会明显降低当
风险。所以我们在情报部门，设立了协同警方的重案组，专门通过司法手段专项打击。重案组我们招了几名
安战线的同志，专门配合公安部门从事线下打击。几个大案的侦破，给我们带来了一手的新鲜材料，综合几
大案的情况，我们得到的结论是，第一：集团化地域化作案非常明显，已经不是趋势了，而是实实在在的存
在。第二，黑产有很多环节，实际上是个综合治理的过程，不是我们一家能够控制的。第三，线下打击是个
期持续的工作。第四，我们自己的情报来源还有很大的扩展空间。

从以上结论，我们开展了后续工作。也就进入了第三个阶段。

三、优化阶段

所谓集团化地域化作案，实际上需要去做关联分析，举例子来说，我们与黑产某人做交易，向对方付款买了
笔数据。而黑产交易的这个人，则会向上游购买数据，上游又会向上游购买，层层批发下来。我们根据资金
系抓这一条链，同时扩展到二度、三度关系圈，再结合通话记录、IP、设备、帐户等多个维度关联，基本上
以得到这个圈子的情况。但这种工作，显然不是人工能够完成的，二度关系还好，到三度关系的时候，人就
溃了。再加上其他维度，是人不可计算的一个量，所以这块，我们开发出了一个关系链分析系统，可以根据
则，自动抓出这个圈子。抓到的圈子，可以移交重案组打击，可以进入黑名单处理。

综合治理工作，比如加料环节，黑产会用一套账号体系去多个网站撞库，撞库的结果是拿到一个人的详细数
据，这些数据可以支撑找回密码、补卡攻击、钓鱼木马等。而这些技术支撑工作，都有专门的组织在做，对
个人的数据集合，可以多次出售，可以和其他犯罪分子做交换。这里的问题是，作为一个单独机构，我们无
控制其他网站的信息泄露，而业务上也不允许我们对用户身份增加更多的验证环节。所以不存在一劳永逸彻
解决的办法，但是可以与其他受害机构联合起来做联防联控，因此我们发起了黑名单交换合作联盟，在当前

产已经形成合作组织的情况下，我们如果还各自为战，将被黑产远远的甩在后面。但遗憾的是，参与合作的构各自都有自己的小算盘，联盟运作并不理想，但即使不理想也要坚持开展，因为这是方向。

线下打击持续开展，实际上，一个案件从发现线索到最后立案抓捕等环节，有一个漫长的过程，需要非常多卷宗和取证。而且新型手法层出不穷，需要我们持续的在这里投入力量保障。

在情报来源上，我们也在从黑市收集情报的基础上，开始从合作机构收集情报。比如针对钓鱼网站的情报收

据来源的种类越来越多，就追

这样就形成了正规情报系统的

擎得出判断结果，从而形成了

动就立案阻断系统，而通过线下打击、关联分析、联防合作，继续丰富数据源和规则，形成了一个闭环的

态。关注黑客与极客

入扩大战果，一步一步的发

的过程，但也正是这种摸索

从甲方机构的角度来说，也是

某购物网站安全测试
2015-09-14
高级
3楼 回

亮了

某集团业务安全测试
2015-09-07
高级

互联网漏洞
2014-12-29
互联网
亮了

去漏洞盒子看看
4楼 回

了， 即使真是派驻， 也要分种类， 并且大部分情报人员的身份都会通报给派驻国， 主要是公明处勤（明哨，使馆武官，文书，外交官 秘书）暗哨（各行各业的各种人）外围（多在行业内混） 其中明哨是会被通报给派驻国的，他们之间多多少少都会存在联系，所以 实现代情报战有相当多的一部分都是盯梢， 更多的其实是策反和利用， 这篇文章可以概括

我们利用自己的大数据平台+人员分析+向公安部门给钱帮我们查案（招聘转业和辞职公安打通关系）最后抓到几个小黑客

这不是情报战， 这是典型的公权私用， 而且查案只是相互利用工作的一点吧？ 呵呵。。。。

亮了

登录

選擇檔案 未選擇任何檔案

昵称
请输入昵称

必须 您当前尚未登录。登陆？注册

邮箱
请输入邮箱地址

必须（保密）

表情 插图

提交评论(Ctrl+Enter) 取消 有人回复时邮件通知我

关键字查找

[职业人生]一位信息安全从业者的工作…

黑产无间道：黑产威胁情报工作实战

FreeBuf年终策划：2014年互联网安全…

安全建设需求：生态级公司vs平台级…

用实际危害说话：评定产品安全性的…

特别推荐

不容错过

【金融、游戏专场火热进行中：高额奖金，最后5天】漏洞马拉松：第一届互联网漏洞“奥运会”

漏洞盒子 2015-05-26

剑走偏锋：细数Shell那些事

xia0k 2014-11-10

[专题]叙利亚电子军专访：如果美国打我们，我们会开始攻击他们

maxcoco 2013-09-18

一周海外安全事件回顾（12.23－12.28）

blackscreen 2013-12-30

Copyright © 2013 WWW.FREEBUF.COM All Rights Reserved 沪ICP备13033796号

本站架设于 阿里云+ 由云盾提供安全保