2022 年度大赛结束了，是什么比赛，懂得都懂。

半个月搞完，心里还是很有些感触的。

攻击技术的本质还是不变，就是利用一切方法获取目标系统的权限，然后窃取数据，或者破坏。

钓鱼是老生常谈的问题，也是很有效的方法，但是真正的实战专家不多，一方面是实践机会少，再一方面，很多朋友对钓鱼认知不深，觉得就是简单的投递邮件，那是一种误认知，真正的实战环境，需要深入分析之后再做决策。

这里举一个案例，是笔者实践且成功的案例，属于定向钓鱼，就钓一个人。

首先信息搜集

在目标网站的底部找到了联系信息

同时观察邮箱前缀

发现是市场部的人

然后进一步搜集企业招标信息，并且自己在心里先演算剧本

首先大背景是比赛期间，那么目标的防御警惕心一定很高，这一点要想办法降下去

再一个要结合目标市场背景来投递钓鱼文案

简单确定了之后，然后开始设计行动方案

1、先电话沟通确立细节，确立行动方案

2、钓鱼邮件不要发的那么迫切，要在时间上延迟，延迟提供真实性，区分开其他钓鱼攻击者

3、上线一定要立即确定，即，先给目标打电话或者发微信，然后电话里说“我现在把相关资料发给您”这里利用了一个情绪延续，因为电话里，他是信任你的，但是这个信任是有时效性的，一定要在他沉浸在这个信任情绪的时候让他上线，不然后续就难说了。

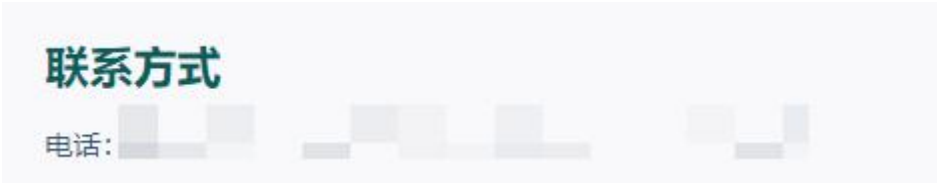
这个原理类似诈骗或者销售，骗子要在受害者没回过神来的时候，把钱骗了，或者销售在消费者没回过神来的时候，就把单做了，这种情绪发生的时候，可以理解为受害者体内分泌特定激素，这种激素会让他临时相信你，但是一旦过了这个窗口期，成功概率就小，就需要后续再找机会了，追女生或者追男生也是这个道理，万法通用。

所以才叫钓鱼，鱼儿咬钩的时候，把浮漂拉下去，这个时候提杆子，才能上鱼，提杆早了或者晚了，鱼都可能钓不上来。

基本的框架确立了，就开始实战，然后根据实战的每一步调整细节。

本案例的基本方法是假扮客户去和他们市场部门对接。

1、先打电话给他们市场部门（伏笔）



在官网找到了联系方式如图，直接打过去。

对方刚接电话的时候，我先说一串开场白

“您好，请问是 xxxx 公司吗，您这边能提供 xxxx 服务吗”

对方语气明显警惕

“请问你这边是？”

“我是做 xxxx（行业术语 专有名次）的”

对方语气一下子缓和下来（行业术语的效果，迅速区分开攻击者和真正的业内人士）

“噢噢噢 好的 那有什么事情吗 ”

接下来我再陈述事情，这里陈述的东西是我事先准备好的，已经打了底稿，并用notepad++写了重要步骤

这通电话的主要目的就是培养信任度，同时获取受害者的更多信息，然后便于写钓鱼文案。

最后我了解结束了，我这样说

“那 ok，贵公司的业务流程我了解了，现在我们供应商正好合作快到期了，我在负责采购新的供应商并且考察市场，这边我到时候把我们公司的详细资料发到你邮箱，然后请你提供一个报价单。”

对方

“好的好的，没有问题”

这个时候第一步就完成了，

2、延迟发送邮件（信任递增）

之前电话里已经说了，需要发送邮件，但是这个邮件不能立即发出。

原因是人的信任是递增的，是需要时间的，这个是客观规律。

信任的递增，可以理解为个人大脑结构的改变。

更深入一点，可以理解为，信任一个人这个事情，作用在大脑，本质上，是大脑某些特定神经元被建立以及强化了，如果一直不断的正向强化，特定神经元就会稳固，从而演变成我们说的相信，因此时间上稍微拉长一点是很有好处的。

放长线钓大鱼，就是这个道理。

放在骗术中，也是这个道理，如果骗子想谋取更多长期利益，就会放弃一些短期的利益，拉长时间，增加成本，在可以收割短期利益的时候不断推迟，从而达到在将来谋取更多利益的目的，长达几个月的杀猪盘就是这个操作手法。

这里我是延迟了两天时间，先不发邮件，先打电话

“您好，我公司这边的资料已经整合完毕了”

对方

“你之前说发邮件，我没收到邮件啊”（可以听出来已经信任了，因为有需求）

我

“我和市场部门还有采购部门去对接了，刚把资料整合出来，不好意思啊，现在就发给您”

然后投递邮件，当天是周五，等了一会，发现并没有上线，然后一直过了两天，到周一也并没有上线，此时需要进一步变通行动方案。

3、微信+电话沟通（确保即时上线）

由于目标并没有上线，但是目标已经回复了邮件，如下：

同时下面打码的地方，有他自己的姓名和联系方式。

这里直接打过去，发现和之前不是一个人。

这里推测，之前负责沟通的是他领导，因为声音老一些。

这个人声音年轻一些，推测是具体负责做事的人。

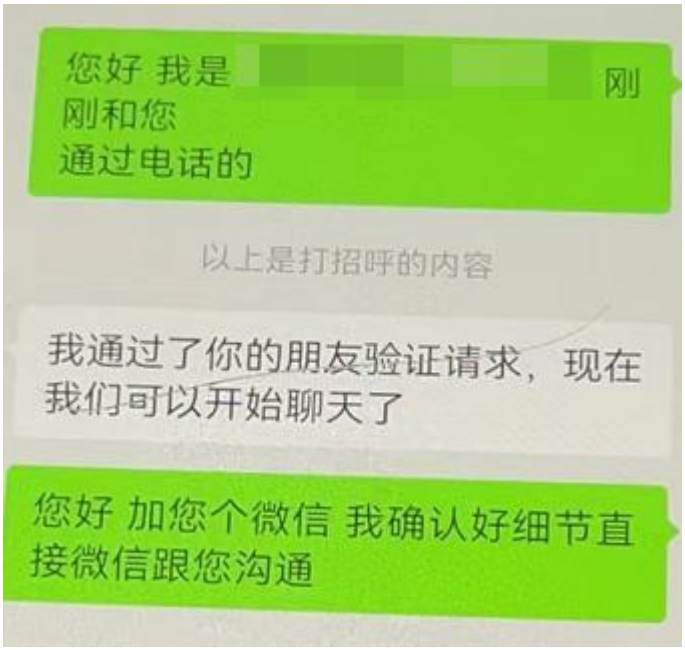
电话沟通完，对方说

“还需要你补充一些特定的细节，这样我们才方便定价，然后给你报价单”

我

“好的好的，那我回去跟业务部门再沟通一下，确定下细节，到时候同步给你”

然后我再顺便加上这个人的微信，用已经养好的真实号，进一步增加信任度。



同时翻看他的朋友圈，收集目标信息，发现他的头像是他女儿，并且朋友圈有和同事出

去爬山玩耍的合照，从面相看比较老实。

对目标进行心理画像：顾家，喜欢运动，有老婆孩子，不喜高风险。

基本可以看出他的心理没上什么 waf，通过之前那条线就可以钓进去。

于是再做一份文案，按他说的补充好，然后时间需要再等一天（增加真实度）。

大概第二天同一个时间点，差不多间隔 24 小时，下午三四点左右（人工作了一天有点劳累，警惕心下降），发邮件。

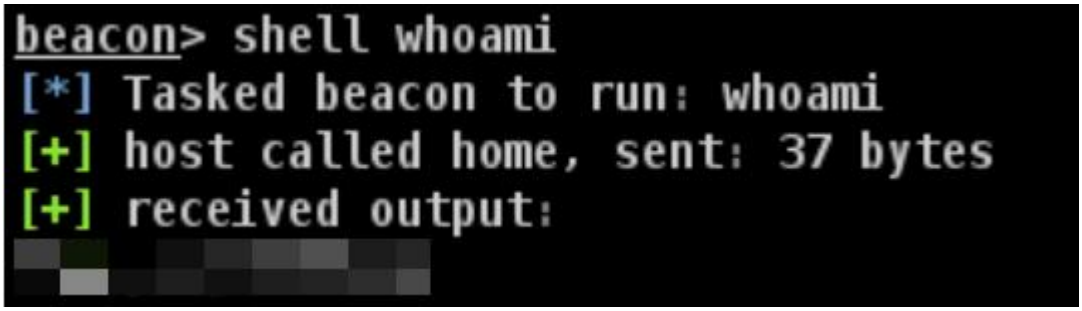
发完邮件之后，微信直接发消息

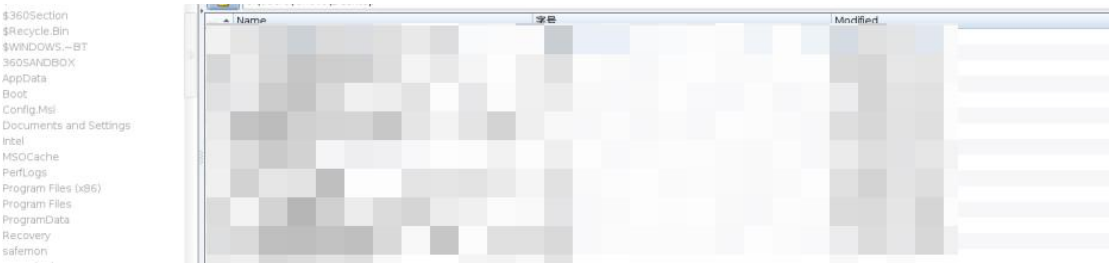
“您好，邮件已经发过来了，请查收”（即时确定）

过了几分钟，他回复

“好的，我看看”

然后过了一分钟，直接上线





接下来就是常规内网打法操作，这里只讲钓鱼，内网就不赘述了。

总结

我觉得钓鱼很好玩，因为钓鱼成功率高，而且和人博弈的感觉非常棒。

但是客观来讲，不是每个人都适合钓鱼，这玩意还是需要一定天赋打底的，不是靠单纯的死训练能出来，尤其是高阶的社工钓鱼，其实链条很长，错一步，就没了。

这里的天赋指的是对人的洞察力，有的人有，有的人没有，尤其是很多做技术的兄弟，平时大部分时间在写代码，沟通技能训练的少，加上天赋没往这块分布，所以这块是弱项。

当然，如果是普通，单纯只批量发邮件那种钓鱼，这很简单，大家都能来。

说这个的目的不是说我在彰显天赋或者什么，而是我觉得，每个人都要选择适合自己的攻击方式，因为不管是什么方式，最后有用，能打进去，那就行了。

有的人擅长挖洞，不擅长沟通，那就不要在钓鱼上多花精力，因为学起来很痛苦，漏洞挖好了，比赛期间那么多 oa，一打一个准，也很有效果。

有的人擅长钓鱼，不喜欢大段大段的看代码，那就钓鱼为主，然后配合再学习免杀和文案的制作，最后效果也相当好。

要在自己的长处上下功夫，最后凸出来，有杀伤力，能达到最终的效果即可。

永远不要用自己的短板去打别人的长处，会死得很惨。

避重就轻，用自己最优秀的地方去和别人竞争，其实会发现体验还是很棒的。