钓鱼邮件溯源之你写给我的信不是这么说的 - SecPulse.COM | 安全脉搏

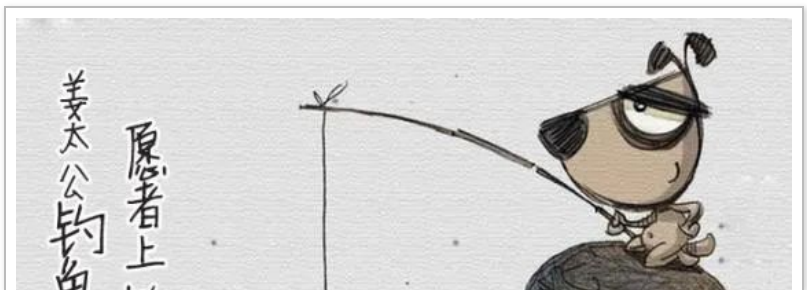
> 这是 酒仙桥六号部队 的第 115 篇文章。

这是 酒仙桥六号部队 的第 115 篇文章。

全文共计 1914 个字，预计阅读时长 6 分钟。

前言

姜太公钓鱼，愿者上钩，18 年网络钓鱼浪潮。钓鱼的手段是屡见不鲜，手段和方式也是层出不穷。据数据表明：Wandera 的《2020 年移动端威胁前景报告》表明每 20 秒就会有一个新的钓鱼网站上线。这意味着每分钟都会在互联网上弹出三个旨在针对用户的新的钓鱼网站。

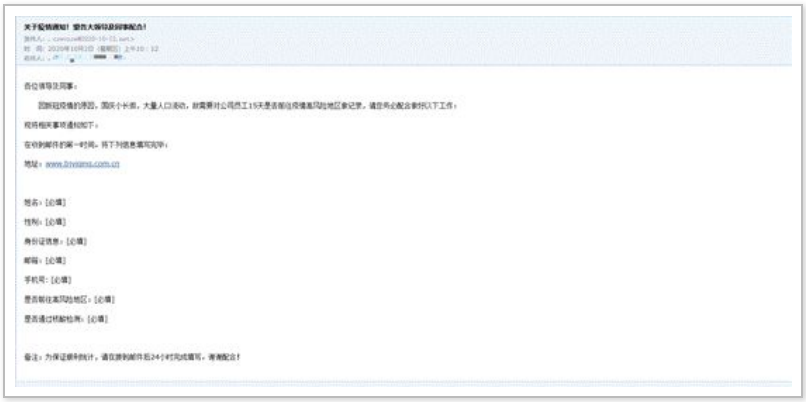


正文

2020 年 10 月中旬外出去某企业做一个项目，空闲的期间与员工聊天他说:"10 月 1 日放假回来收到了一封疑似钓鱼的邮件"。我看了看觉得挺有意思于是对这个邮件尝试进行一波溯源，没想到还有一些发现，下面是我溯源的一个过程跟大家来分享一下。

1
分析邮件内容

1.1、邮件截图



1.2、邮件内容

首先我们看来看一下邮件的整体内容，是以 10 月 1 日国庆小长假结束后关于疫情返京统计为主旨。如果不小心或者公司有相关统计要求的情况真的很容易就中招了。

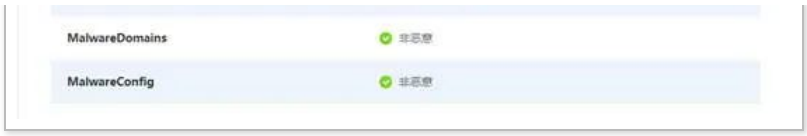
1.3、附带域名初步分析

接下来我们再看一下邮件里附带的域名 www.bjyiqing.com.cn 感觉很正规有没有，而且根据这个域名拼出来是不是很像“北京疫情”；在来看一下邮件的发件人，名字是 service，邮件地址 2020-10-12.net，这大概是个邮箱服务器发送的一个以日期命名的不存在的域名地址。

1.4、邮件初步总结

总体来看该邮件格式内容很丰富、正规，而且刚好贴合了 10 月 1 日返京疫情统计的这个主题，这也难怪有许多企业会被钓鱼邮件攻击成功，确实是令人防不胜防。

2
域名威胁情报分析
下面我们正式的开展溯源工作首先对于邮件附带的域名 www.bjyiqing.com.cn 进行威胁情报分析，未发现异常。

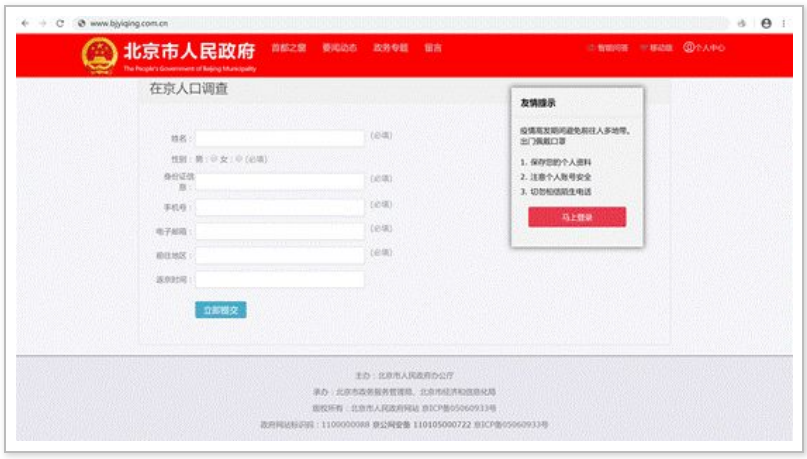


3

钓鱼网站解析

3.1、初访域名

扫描一下网站没有发现风险，我们在利用虚拟机访问邮箱附带的域名地址看看：www.bjyiqing.com.cn



3.2、页面内容与跳转

1、访问后，可以看到，该页面是一个以填写个人信息为主的，内容涉及到很严重的个人信息，包括 ***、手机号、邮箱等，尝试了随便填写一些内容进去，不需要验证就可以提交成功并且跳转到下面这个页面。

2、通过百度搜索网站内容证明为真实的网站，也就是说，该钓鱼邮件由一个 html 页面，填写完信息后重定向到真实的页面。

4

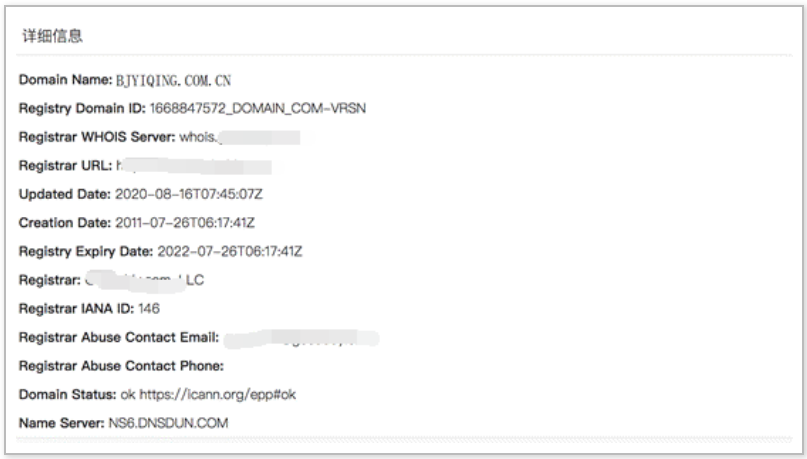
分析溯源

4.1、域名解析

分析了该钓鱼邮件收集信息的一个流程后，首先，先进行了查询该域名的解析记录：经查询后发现该域名解析的地址为香港。

4.2、网站信息查询

接下来，查询一下 whois 信息：信息查询出来后没有注册电话显示，还需要进一步查询。



4.3、邮箱反查

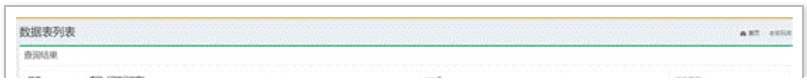
通过 whois 查询到的邮箱进行一波反查注册过该邮箱域名地址：发现该邮箱还注册了另一个站点。

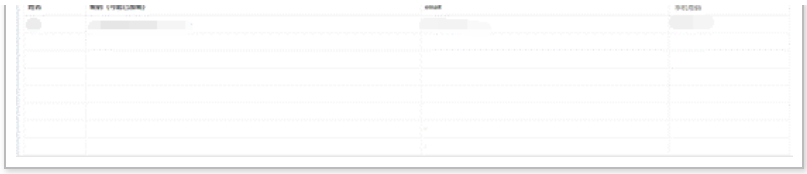
4.4、相关网站

对邮箱反查后的站点进行访问后得到。

4.5、逐步浮出水面

1、该网站为 ** 网站，有可能又是打着 ** 名义的钓鱼网站，发现里面有客服、qq 和联系电话等，继续尝试对该邮箱和 QQ 进行社工。

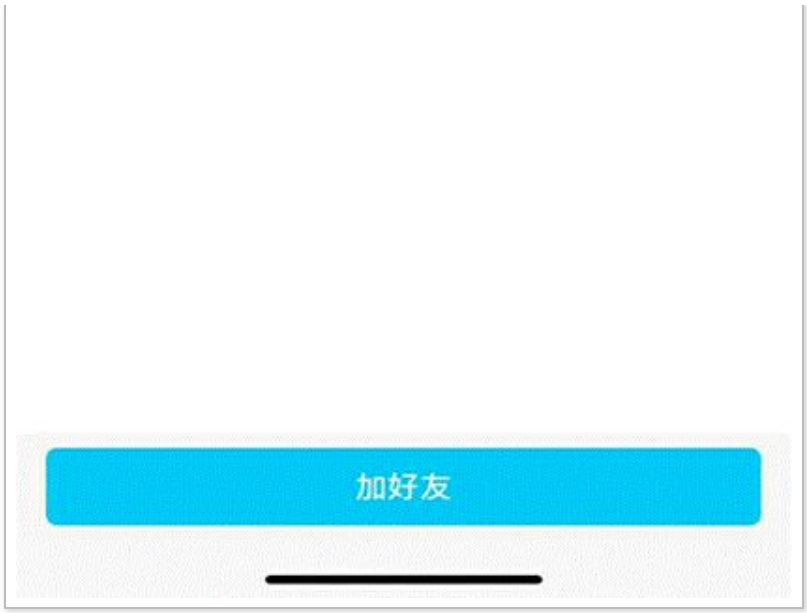




2、社工后发现一条信息，并且附带电话号码，看看发现了什么，查出来的手机号和网站上留的手机号竟然是相同的。尝试对该电话号码进行下一步利用，该电话用于微信、支付宝、脉脉 APP 上进行查找。

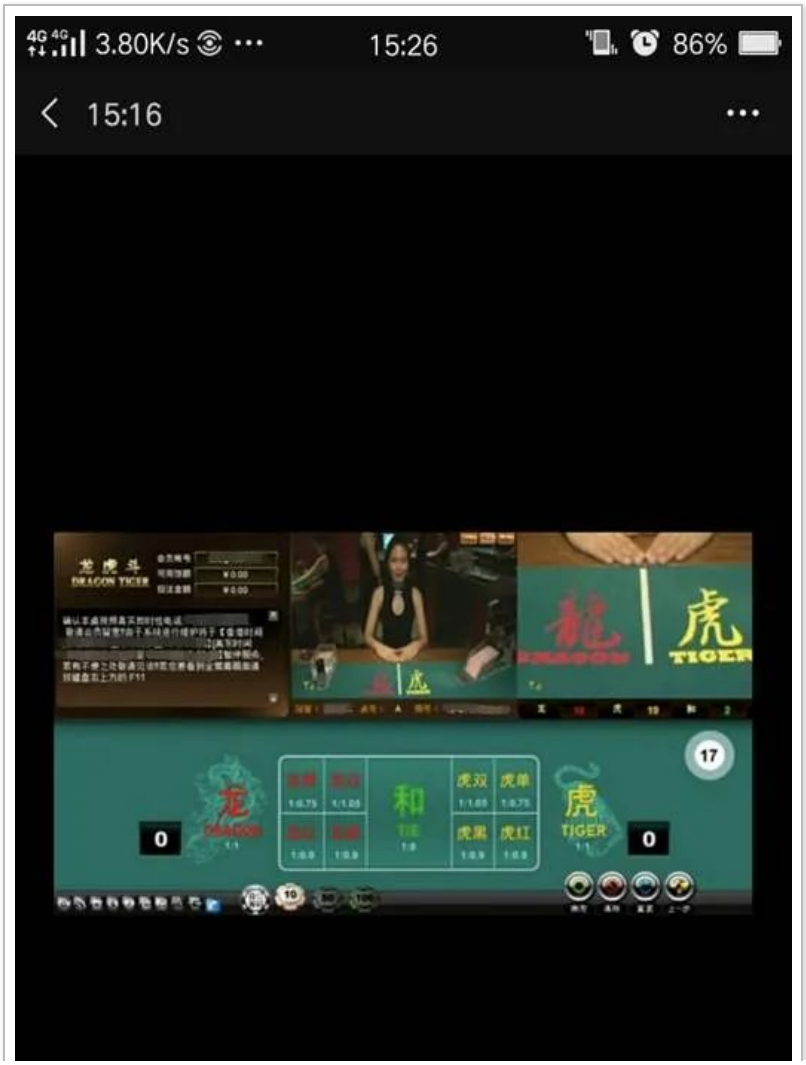
3、经查找后发现微信、支付宝均未查询到，说明该号码可能是虚假的，也可能是未注册。但是在查询 QQ 号的

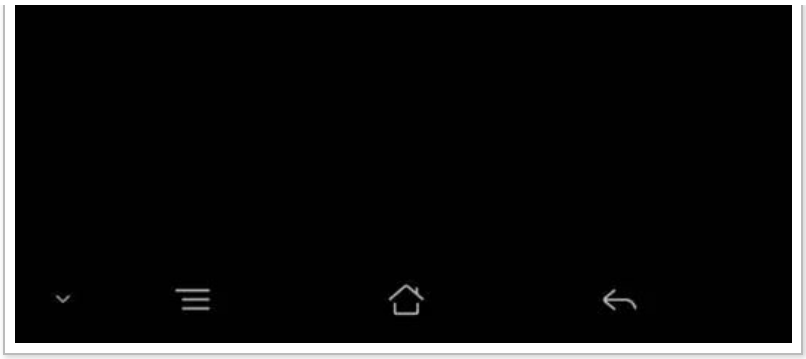
时候有了进展，发现该电话绑定了一个 QQ 号。



4、利用该 QQ 号码进行微信查询：发现此 QQ 还绑定了一个微信，并且查询到了有用信息：手机号码和朋友圈。

5、点击查看朋友圈，发现朋友圈存在 ** 网站广告。



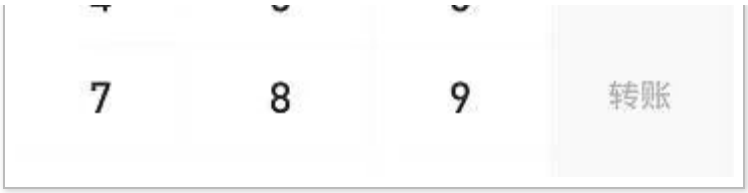



7.11K/s
15:26
86%
15:16
官网直营 玩家首选
ABOUT US
菲凰娱乐
PAYMENT
CONTACT US
联系方式

6、可以初步确定该微信号主人也在涉及 ** 网站。

后续通过微信上显示的手机号码再通过支付宝搜索后发现：


中国移动
下午 3:51
43%
转账
转账记录
峰(*峰)
点此验证
转账金额
¥
谢谢
生活费
房租
代买
还款
添加备注（50字以内）
1
2
3
4
5
6



7、该支付名称为 * 峰与社工库查询出来的 ** 网站邮箱注册人一致。

4.6、真相只有一个

从种种信息来看，最终查询所有查询出来的线索都指向同一个人，基本可以判断就是该人所为，到此我们的溯源就结束了。

总结

从一封邮件，一个域名，逐步探索出许多条信息，根据种种线索的指向，到最后汇集到了同一个人完成了闭环。有一个清晰的思路和细心的心都会查询出一个结果。最后给大家送上一句柯南名言：

犯罪手法是人想出来的，只要人绞尽脑汁，还是会想出答案的。——工藤新一

结尾

钓鱼事件屡见不鲜，经过种种案例所示，大家可以看出来钓鱼网站往往会伪装在我们生活中，利用相关的内容来诱使我们上当，轻则我们个人信息泄露，重则公司系统遭到入侵，形成不必要的损失；最后在这里提醒一下大家今后接收到不明邮件时，我们需要注意一下以下几点：

一、收到陌生邮不要轻易点开邮件及内容中出现的链接。

二、如若接收到不知名邮件，请先确认邮件的真实性。

三、在公共场上遇到免费网络Ｗｉ－Ｆｉ及热点建议不要轻易去使用。

四、仔细比对发件人名称是否出现相近后缀导致造成不必要失误。

本文作者： 酒仙桥六号部队