谈谈“钓鱼”背后那点事儿

前言：钓鱼攻击多为钓鱼邮件攻击，种类可以分为钓鱼邮件攻击和钓鱼短信，前者用途广泛，而后者用于电信诈骗，本次详细讲钓鱼邮件。

何为钓鱼邮件？

钓鱼邮件攻击是社会工程学中一种常用技巧，在渗透测试中，多用于目标没有漏洞时，欺骗受害人进行一些欺骗操作，最终达到目的。
笔者所写这篇文章，主要介绍我所知的钓鱼邮件猥琐技巧以及应对策略，希望能使更多的人不被这些手段所迷惑和欺骗，也希望能给从事安全的人员一些思路。

来自10086的官方短信？

请看图

图中是10086所发的一个积分换现金的活动，很多人信以为真，包括我的父母，也收到过这类短信。
但我们认真看看 图中的域名 “l0086” 并不是“10086”。

这是一种欺骗，我们下文再讲。

很多人都是看是10086官方的短信，域名也不注意看，看着自己的积分就能换礼品或者现金，满生欢喜。

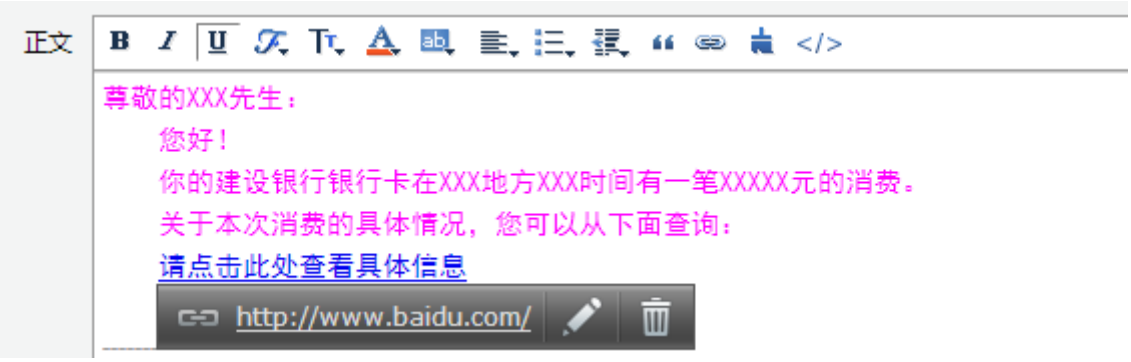
然而这是有猫腻的，这就是伪基站技术。

何为伪基站技术？

我的理解是，伪基站可以充当一个基站，当你链接到这个基站时，你的手机会断网一瞬间，很快便恢复，你的所有通讯，都不经过运营商，现在很多的改号技术也就是这样，号码18888888888这种，但伪基站很多都是放车上，到处游走，广播撒网。

那么我们就从上文所说的域名来聊聊钓鱼技术的前世今生。

原始的钓鱼邮件攻击：超链接替换（1）



这就是一个经典的钓鱼邮件，这里可以看到是伪造的建设银行的一封短信，我这里所用的超链接引向了“www.baidu.com”，这是最基础的一种方法，就是如图所示，插入超链接，期待用户来点击，这个链接可以是任何一个网站，建设银行或者是伪造的钓鱼页面。

这种欺骗方法很好理解，就好像HTML中的a标签一样，超链接显示内容和指向的URL可以不一样，就如同我上面。

攻击者可以设置为“点击此处转到淘宝网”，然而他却跳向了百度。

这种攻击在以前很容易成功，现在也不在少数，因为钓鱼者这种手段很容易迷惑受害者，受害者心理大多数都是这样的：

“怎么消费了？被盗刷了？我得看看详单”

然后因为手机邮件直接点这个超链接，又看不到网址，点进去一看，还真是个“建设银行”官网。

急急忙忙输入了自己的银行卡卡号和密码，却一直登陆不进去，这个时候，钓鱼者应该在后台守信了（业内称呼，收鱼，收信息的意思），然后被异地盗刷，建设发来大量短信提示消费，用流行说法就是：

“喔嚯，翻皮水了。”

不过还好，现在全民上网，安全意识很有提高，知道先看网址了，知道看邮箱发件人，不认识的邮箱发来的邮件一般不会去点击。

然后呢，又出现了更为猥琐的几种手段，来对用户进行欺骗攻击。

泛生之一：超链接替换（2）

还是超链接替换攻击内容，我们把“点击查看此处具体信息”替换成“http://www.ccb.com”这是建设官网，我把指向的URL引向钓鱼者的钓鱼建行官网，所以你直接点这个超链接进去还是进了钓鱼者的钓鱼网站，没想到吧。

进阶技巧，相似URL进行欺骗

相似的URL进行欺骗，多用相近字符进行替换，比如：www.gitbook.cn

我们将他替换成 www.gitb00k.cn 上文的“I0086”也是如此。

把字母“o”替换成了阿拉伯数字”0”，粗心大意的小伙伴分不清，也就中招了。

进阶技巧，子域名欺骗

子域名，即二级域名，通常是别名解析，比如我有个域名是“taobao,com” 那么我们可以做一个二级域名 比如”abc.taobao.com“

利用子域名欺骗呢，比如我们的网站是“gitbook.cn”，攻击者可以这样，解析一个gitbook.cn的二级，比如 “gitbook.abc.cn”。

分析一下，abc是我的根域名，gitbook则是我们进行欺骗的域名，路人一看前面是对的上的，想也不想又进去受骗了。所幸现在大家都会看根域名，这种技巧也不算很实用。只要根域名没毛病，一般不用担心子域名，切莫只看前面，一定要认真看清楚。

高阶钓鱼技巧，连接符欺骗

连接符是个什么玩意？就是你键盘上第二排，第12号键，两个杠那个玩意，明白了吧。

“-“就是这个丑东西……

这个丑东西骗了不少人，比如（还是拿我们gitbook开刀）

“xiezuo-gitbook.cn”

我们假设gitbook的写作页面是”xiezuogitbook.cn”的话，这个域名就是个连接符欺骗。

如果你还是不能理解，我们拿QQ邮箱来讲。

QQ邮箱的域名是“https://mail.qq.com”

给他把连接符这个丑东西加进去后，就变成了这个模样…

“https://mail-qq.com”

这你还能分辨吗，简直猥琐的一批，这种用连接符来假装自己是个正经的子域名技巧，可以骗过大多数的人眼睛。

高阶技巧，伪造邮件欺骗

原本我是找了一个接口，做了一个伪造邮件地址，没想到刚刚测试已经死掉了，用Kali的swaks工具进行伪造一直返回“550 Mail content denied” 很遗憾。

```
    ``root@kali:~# swaks --from web@abc.org to admin@secus.org  -
heaeder "hello"
```

```
=== Trying mxdomain.qq.com:25...
=== Connected to mxdomain.qq.com.
<-  220 newmx.qq.com MX QQ Mail Server
 -> EHLO eaeder
<-  250-newmx.qq.com
<-  250-SIZE 73400320
<-  250-STARTTLS
<-  250 OK
 -> MAIL FROM:<web@abc.org>
<-  250 Ok
 -> RCPT TO:<admin@secus.org>
<-  250 Ok
 -> DATA
<-  354 End data with <CR><LF>.<CR><LF>
 -> Date: Sun, 09 Jul 2017 09:25:58 +0800
 -> To: admin@secus.org
 -> From: web@secus.com
 -> Subject: test Sun, 09 Jul 2017 09:25:58 +0800
 -> X-Mailer: swaks v20130209.0 jetmore.org/john/code/swaks/
 ->
 -> This is a test mailing
 ->
 -> .
<** 550 Mail content denied. http://service.mail.qq.com/cgi-
bin/help?subtype=1&&id=20022&&no=1000726
 -> QUIT
<-  221 Bye
=== Connection closed with remote host.
```


如果返回250.那么证明伪造成功。

以上是代码部分，很遗憾的是笔者伪造失败了，口头说明就是，能够伪造发信人的地址，但是为了防止邮件伪造，大型邮件提供商都做了SPF检查，目标邮件服务器返回550状态码，表明检查失败，极难绕过。

背后相关利益

伪基站这种大量撒网的技术，获取到的包括不限于姓名、发卡行、卡号、密码、身份证号码、手机号码、卡类。这些信息盗刷后还可以卖给黑产人员。

背后利益链关系庞大，但是你要相信，正义总会来临，无非了慢了一点。

结语

笔者曾见过钓鱼者的“聪明才智”，是在一个伪造QQ邮件主页的网站上，表面和QQ邮箱官网无二样，在你输入账号密码后，点击登录会提示你密码错误，请重新输入，当你点击确定后，页面会瞬间跳转真正的QQ邮箱主页，这时候你输入就进到了真正的页面，但你可能并不知道你第一次输入的时候就已经被钓鱼了。 **所以，擦亮眼睛，减少损失。**