2023 守内安信息科技 & ASRC
第三季度邮件安全观察

ASRC

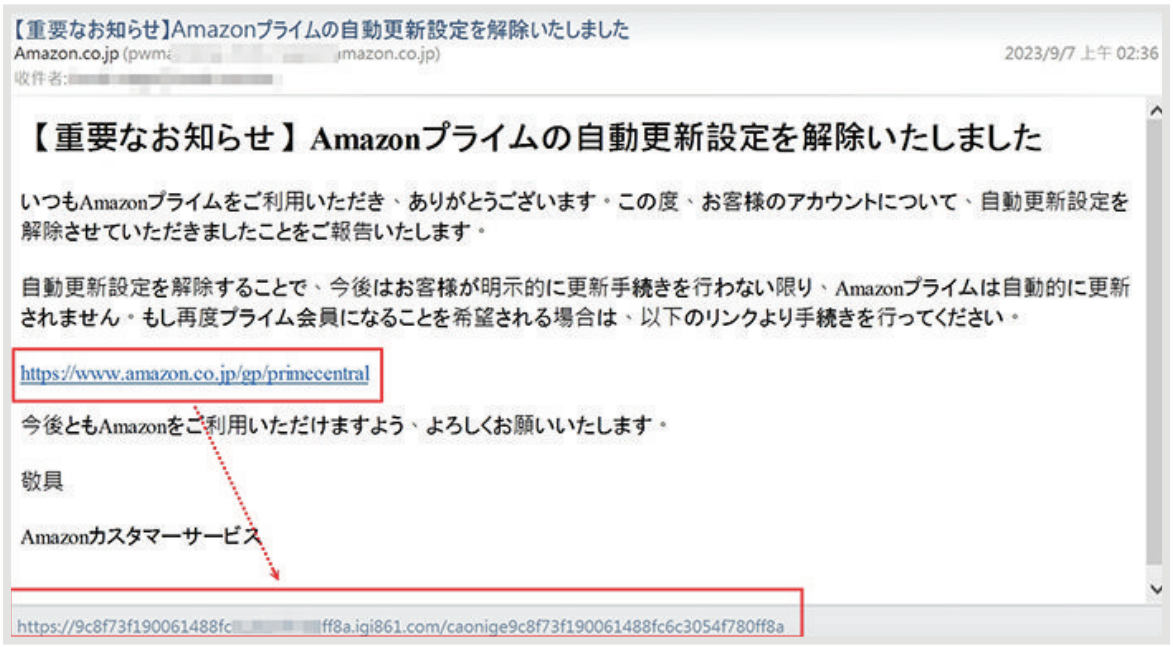
Spam Mail
Virus Mail
Malicious Mail

Oct 2023 released.

在第三季，我们发现邮件内带有恶意链接的情况较上一季增加了60%；垃圾邮件的大小与419scam的数量，与上一季相比都减少了30%左右，钓鱼邮件是本季最主要的攻击。以下是本季度在东亚发现的几个特殊的样本：

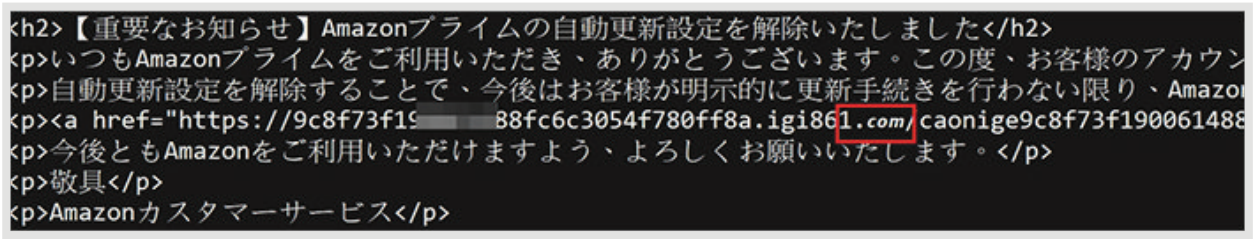
通过字符变换躲避侦测的钓鱼邮件

在第三季，我们观察到一个特殊的钓鱼邮件。这个钓鱼邮件冒充了Amazon通知信，并且出现了一般钓鱼邮件常见的特征：显示的链接与真实前往的链接不一致。



一般钓鱼邮件常见的特征：显示的链接与真实前往的链接不一致

值得一提的是，若是直接检查这封钓鱼邮件的原始文件，会发现有些字符显示的样子有种违和感。



检视这封钓鱼邮件的原始档，会发现 .com 的显示似乎与其他英文字符不太一致

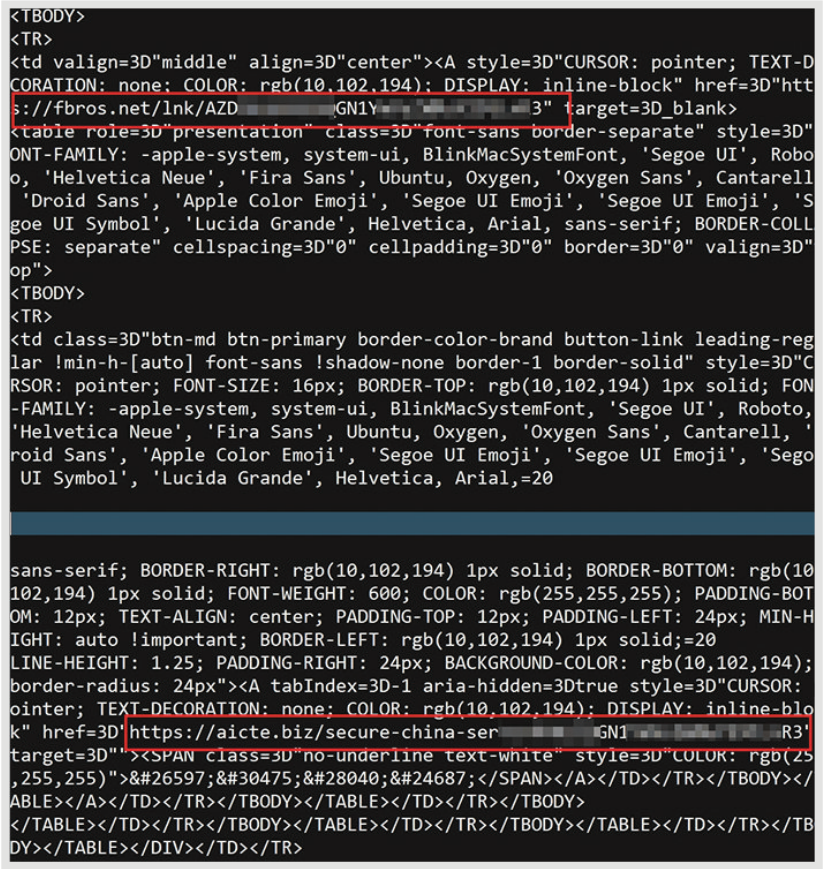
这是因为攻击使用 Unicode 字符替换域名中的部分字符。攻击者也能对邮件内恶意链接中的域名做其他改变，例如：将小写字母切换为大写字母，或加入不可见字符...等，借此绕过数据库的比对判断，而这样的手法对于浏览器、邮件系统，都还是能够解析为可被收件者点击的恶意域名网址。

一个按钮两个钓鱼链接

我们也发现了一个奇怪的案例：一封伪冒 Linkedin 的钓鱼邮件，在同一个按钮中，潜藏了两个钓鱼链接。通过在按钮上操作鼠标移动，可以看见两个超链接的切换。

这两个超链接连往的是不同的服务器，似乎都是被入侵的网站，而在其网站支系的某个目录，藏有转址程序代码，会将上钩的受害人连往另一个被入侵的钓鱼网址，例如：
hxxps://cendas.com.ar/wp-content/china/chinaserver-LINKEDIN/#(受害人以 base64 编码的 E-mail Address)，同时在一个按钮设置两个钓鱼链接，可能是为了逃过封锁，提高钓鱼的成功机率。

通常见的伪冒钓鱼邮件



检视原始档后，可看见连往两个不同的钓鱼网站

复合钓鱼手段

通过假冒宝岛某电商的诈骗邮件，复合多重技巧。先以社交工程的手段告知该电商无法验证用户的信用卡，可能造成用户无法付款，接着明确显示电商的超链接，但实际联机到遭入侵的钓鱼网页，这是钓鱼邮件常见手段。

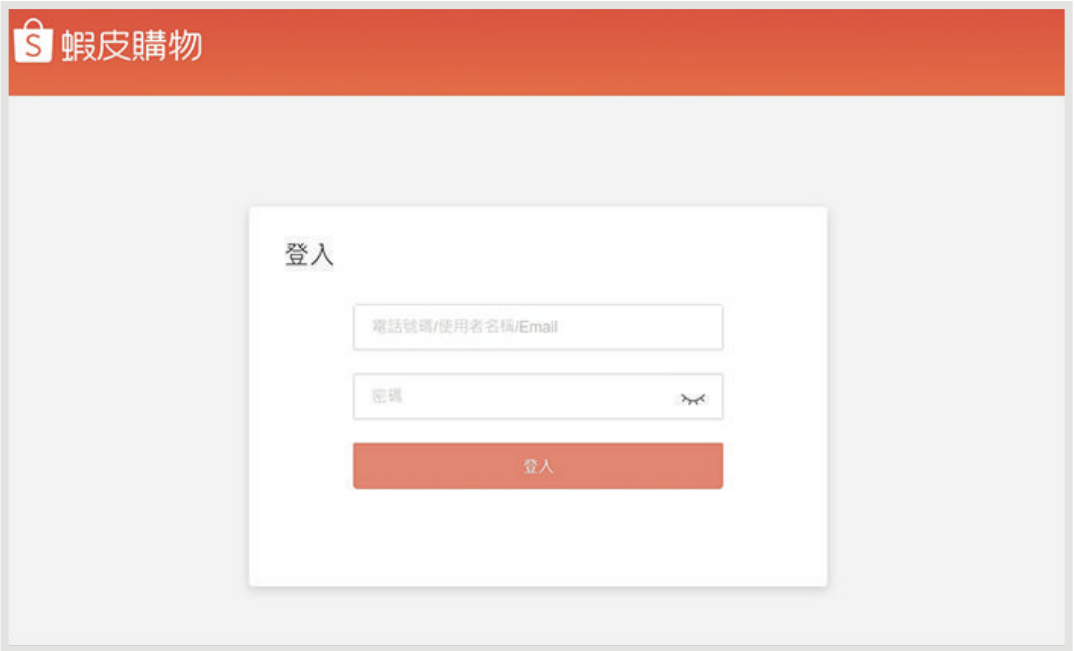
伪冒电商的诈骗邮件

分析原始文件，我们发现攻击者在邮件中藏入一张长宽为1的图片，图片来源为 [[TRACKINGPIXEL]]，可能是攻击者忘了将钓鱼样板定义的变量替换成追踪链接。但若此处被置入一个有效的追踪链接，当用户开启这封邮件时，若没有封锁图片，则会通知统计的主机记录这封信的所有点击人信息，包括时间、IP、MUA 版本，并且让攻击者知道攻击对象的防护状态...等相关资料。

```
</td>
</tr>
</tbody>
</table>
<div><img style=3D"position: absolute; visibility: hidden;" src=3D"about:bl=
ank" width=3D"0" height=3D"0" border=3D"0" /></div>
<img src=3D"%5B%5BTRACKINGPIXEL%5D%5D" width=3D"1" height=3D"1" border=3D"0=
" /></td>
</tr>
</tbody>
```

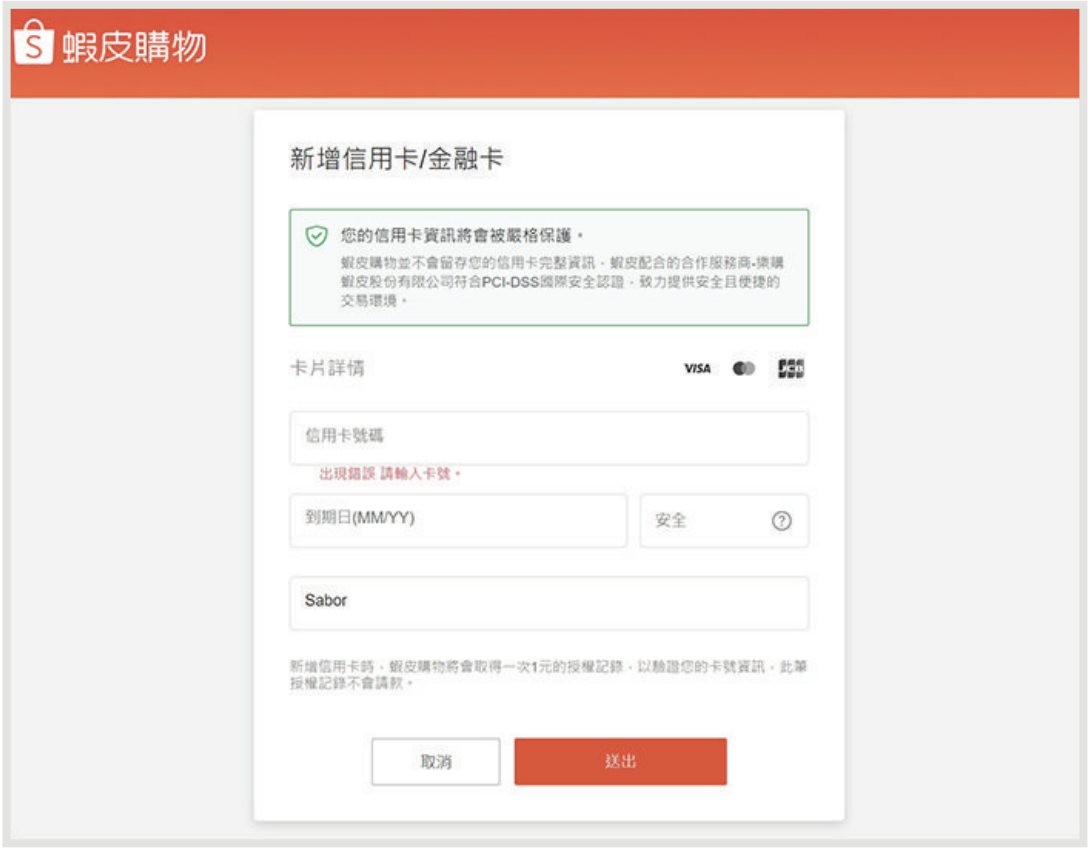
攻击者忘了将钓鱼样板定义的变量替换成追踪链接

当受害人不慎连往钓鱼网页时，第一步将被骗取的是使用于电商的账号密码。在这个阶段，不论输入的账号密码为何，都会被攻击者纪录。随后，成功跳转至下一个页面；遭到盗取的账号密码则可能用于后续其他的攻击。



第一步将被骗取的是使用于电商的账号密码

第二步是骗取信用卡的相关资料。在这个阶段，受害人为了购物便利，可能会受骗新增信用卡。巧妙的是，在此页面不论输入任何信用卡数据，在发送后都会被攻击者纪录，接着显示「出现错误 请输入卡号」的提示，并且清空信用卡数据的相关字段，受害人可能在情急之下，换另一张卡输入，有可能因此被连续窃取多张信用卡数据。这个遭到入侵的钓鱼网站，直至截稿前仍在运行。



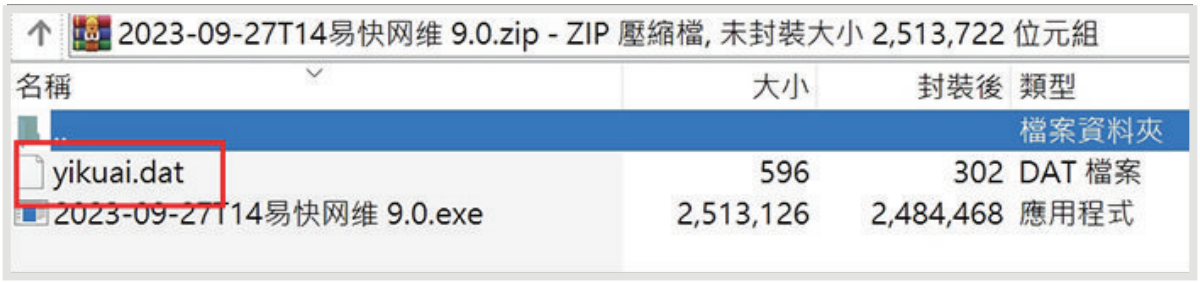
受害人可能在情急之下，换另一张卡输入，有可能因此连续被窃取多张信用卡的数据

留意远程遥控、维护软件的滥用情况

这一季中也发现有攻击者试图以社交工程的方式，在邮件中未提及远程及需维护动作信息，巧妙的将远程控制软件放置于外部公共链接，躲避邮件安全系统扫描的检测，使用户不经意间执行安装导致被远程控制用于恶意用途。

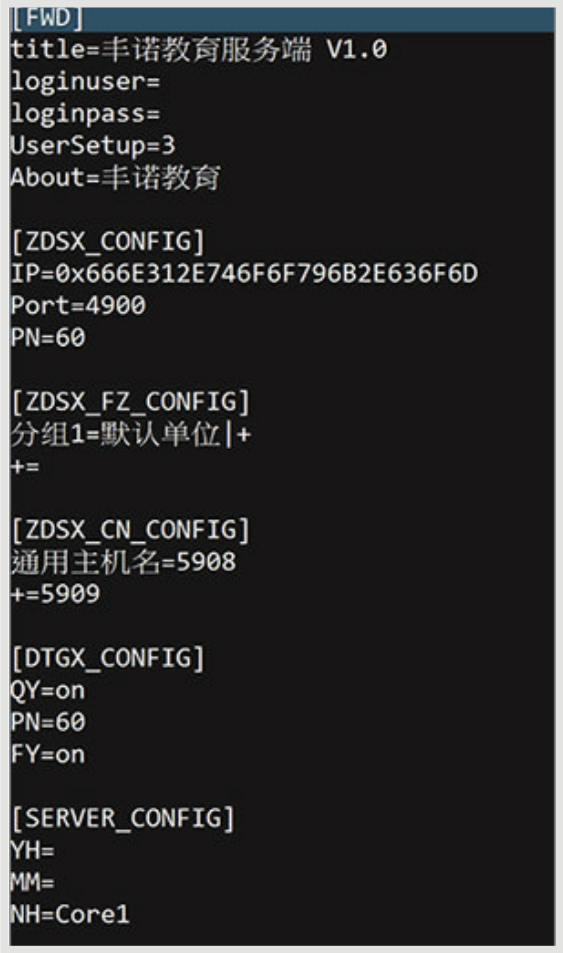
将远程控制软件放置于外部链接，躲避邮件扫描的检测

当受害人下载了远程控制软件压缩文件后，攻击者将远程控制软件的配置文件设定为隐藏文件；因此在 Windows 的预设情况下，解压缩出来的文件看起来只有一个远程控制软件。



远程控制软件的配置文件被攻击者设定为隐藏档

查看配置文件的内容就能发现这个配置文件并不单纯，除了改变安装软件显示的标题外，也将连接的 IP、通讯端口都设定好了，在安装完成后，也能在受害人无法察觉的情况下，远程监控、操作受害人的计算机。而这个远程控制软件本来的远程维修用途，未必会被所有的防病毒软件视为有害。



查看設定檔的內容就會發現這個設定檔並不單純

结语

在这一季，虽然有漏洞被揭露，但似乎尚未遭到大规模的利用，整体仍以钓鱼邮件为主要攻击手段。钓鱼邮件顾名思义，目标就是要钓取后续可以再利用的信息；钓鱼邮件除了不停的进化出各种规避侦测的技术以外，我们也注意到钓鱼邮件的攻击者更加专注于遭到钓鱼的目标，诸如：点击率、是否上钩、钓取数据的有效性、更多可以一并得到的目标信息。这些遭到钓取的敏感信息都可以再组合、拼凑并且重复被使用，或结合诈骗、伪造身分等攻击。

关于 ASRC 垃圾讯息研究中心

ASRC 垃圾讯息研究中心 (Asia Spam-message Research Center)，长期与守内安合作，致力于全球垃圾邮件、恶意邮件、网络攻击事件等相关研究事宜，并运用相关数据统计、调查、趋势分析、学术研究、跨业交流、研讨活动等方式，促成产官学界共同致力于净化因特网之电子邮件使用环境。