2021 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

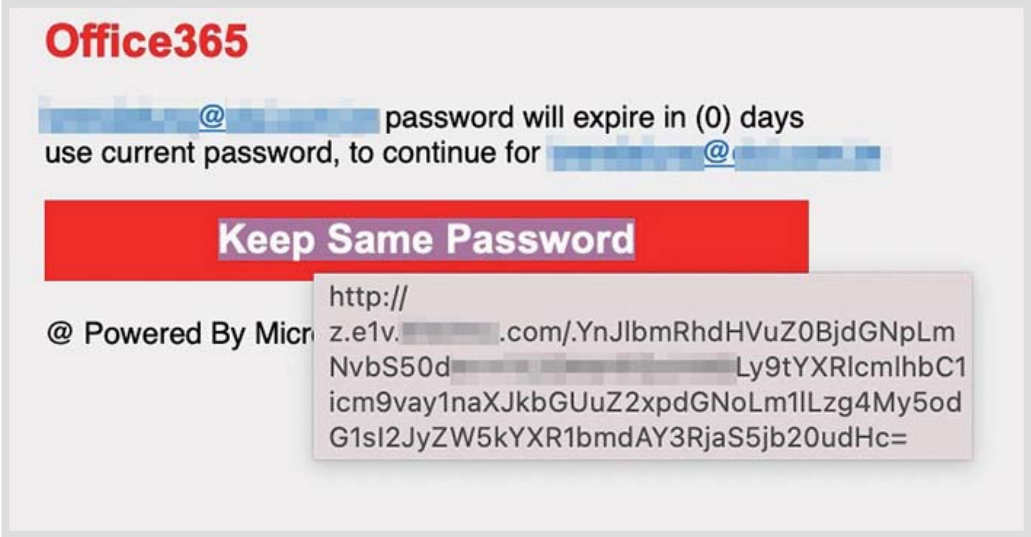
October 2021 released.

本季垃圾邮件总体数量并无明显波动，但钓鱼邮件仍然没有平息。利用 CVE-2018-0802 程序漏洞伪装成订单邮件的攻击，数量上相较上季略有趋缓，但仍需要特别留意；冒充企业的伪造邮件攻击，较上季增长约 1.5 倍，而针对个人诈骗邮件的数量较上季增长了 1.2 倍，个人与企业均须时刻提防中招。

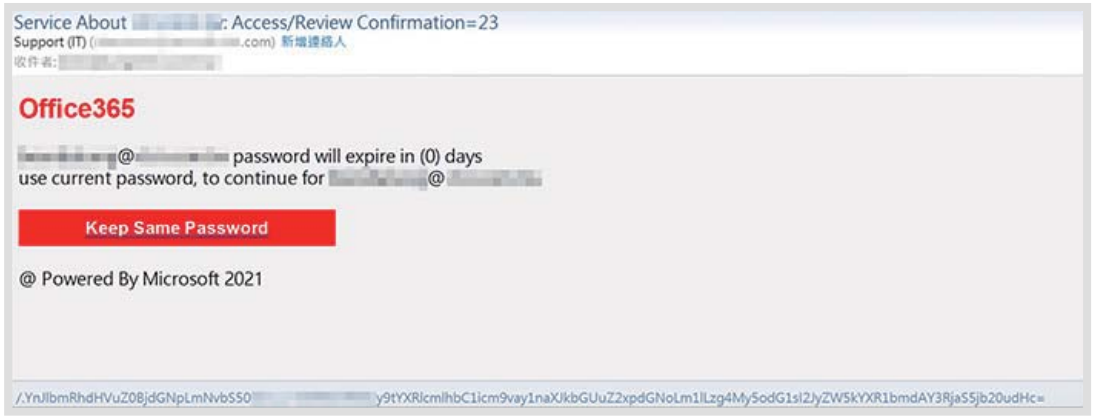
守内安信息科技 (上海) 与 ASRC 研究中心整理本季较为特殊的样本如下：

钓鱼邮件透过 HTML 标签挑选攻击目标

在第三季，我们发现特别的钓鱼邮件样本，这个样本在 Apple Mac 的默认邮件客户端开启时，会直接显示出可点击的链接；但若在其他的微软操作系统常见的邮件客户端，则不会显示出可点击的链接。

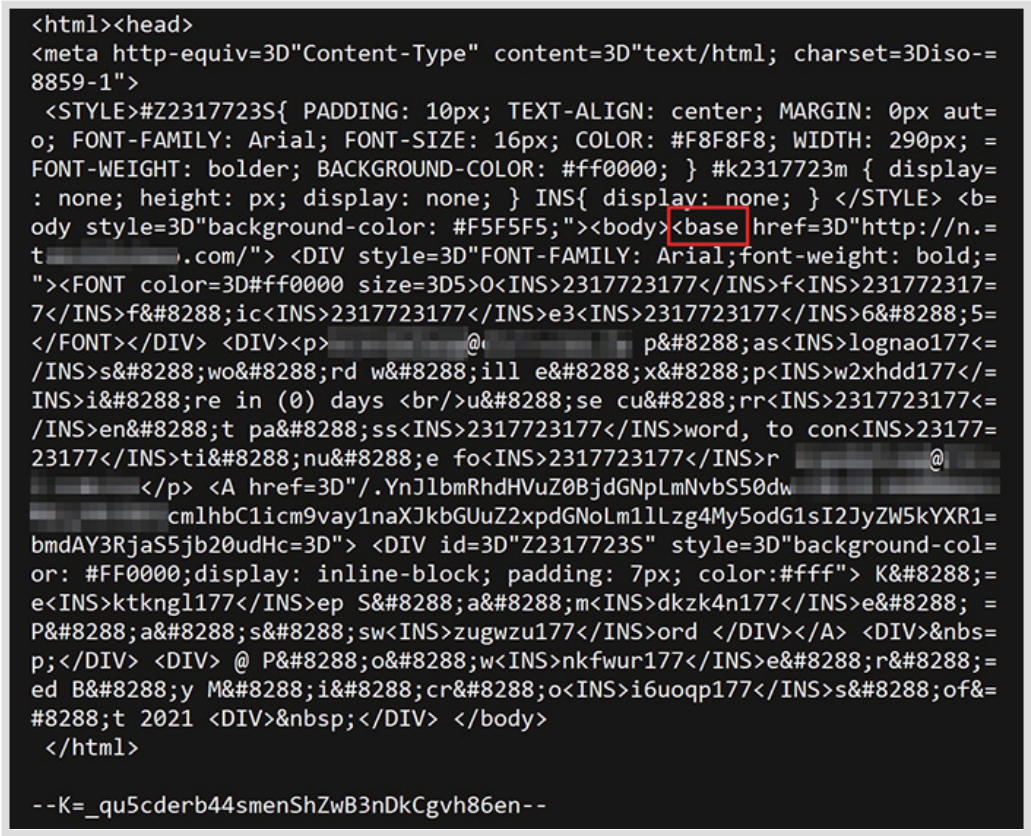


在 Apple Mac 的默认邮件客户端开启时，会直接显示出可点击的链接



在微软操作系统常见的邮件客户端则不会显示出可点击的链接

查看源代码，发现这封钓鱼邮件使用了 <base> HTML 标签。这个标签主要是用于设定整个页面中，所有链接类型属性的默认根网址。不过这个标签并非所有的客户端系统都支持，因此可借由使用这个标签来筛选攻击目标。



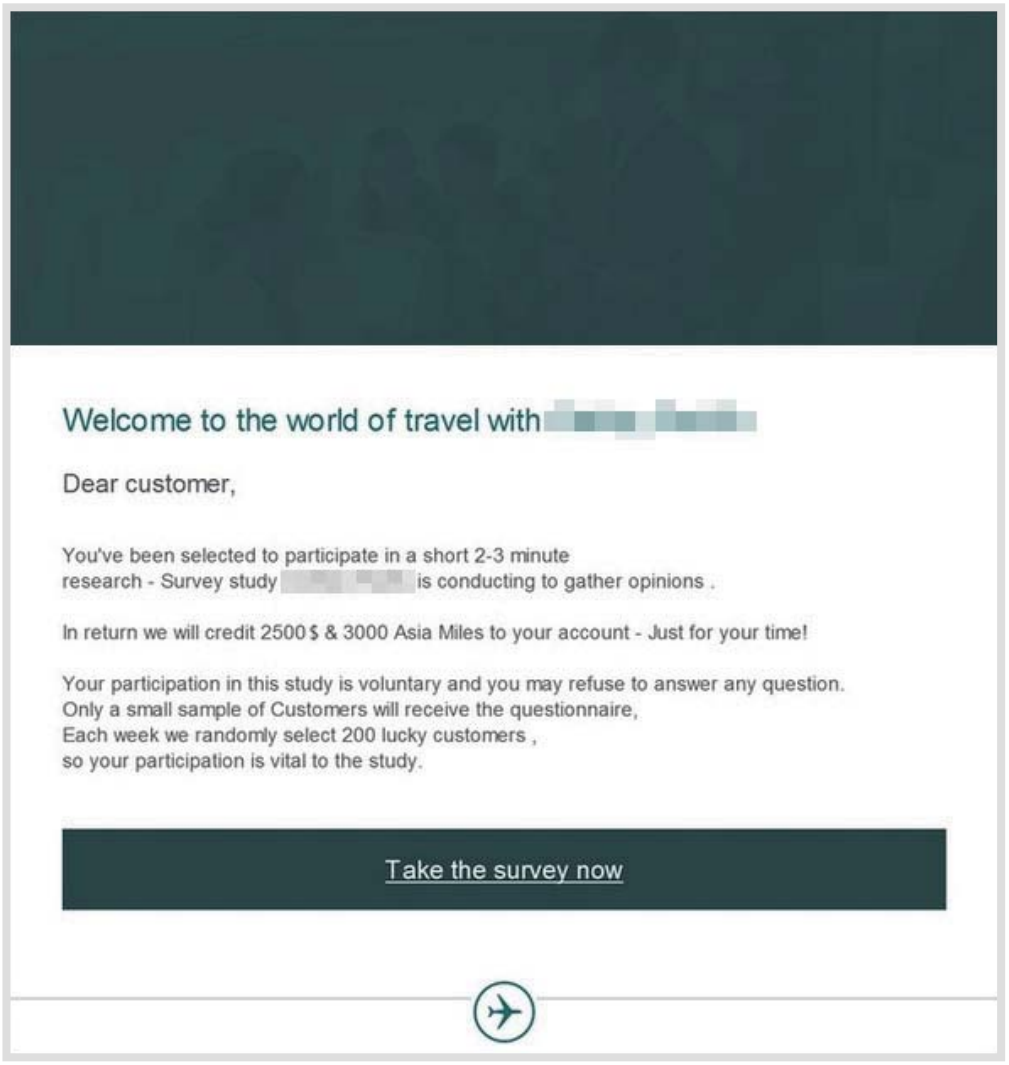
```
<html><head>
<meta http-equiv=3D"Content-Type" content=3D"text/html; charset=3Diso-=
8859-1">
 <STYLE>#Z2317723S{ PADDING: 10px; TEXT-ALIGN: center; MARGIN: 0px aut=
o; FONT-FAMILY: Arial; FONT-SIZE: 16px; COLOR: #F8F8F8; WIDTH: 290px; =
FONT-WEIGHT: bolder; BACKGROUND-COLOR: #ff0000; } #k2317723m { display=
: none; height: px; display: none; } INS{ display: none; } </STYLE> <b=
ody style=3D"background-color: #F5F5F5;"><body><base href=3D"http://n.=
t[redacted].com/"> <DIV style=3D"FONT-FAMILY: Arial;font-weight: bold;=
"><FONT color=3D#ff0000 size=3D5>O<INS>2317723177</INS>f<INS>231772317=
7</INS>f&#8288;ic<INS>2317723177</INS>e3<INS>2317723177</INS>6&#8288;5=
</FONT></DIV> <DIV><p>[redacted] p&#8288;as<INS>lognao177<=
/INS>s&#8288;wo&#8288;rd w&#8288;ill e&#8288;x&#8288;p<INS>w2xhdd177</=
INS>i&#8288;re in (0) days <br/>u&#8288;se cu&#8288;rr<INS>2317723177<=
/INS>en&#8288;t pa&#8288;ss<INS>2317723177</INS>word, to con<INS>23177=
23177</INS>ti&#8288;nu&#8288;e fo<INS>2317723177</INS>r [redacted]
[redacted]</p> <A href=3D"/.YnJlbmRhdHVuZ0BjdGNpLmNvbS50dw[redacted]
[redacted]cmlhbC1icm9vay1naXJkbGUuZ2xpdGNoLm1lLzg4My5odG1sI2JyZW5kYXR1=
bmdAY3RjaS5jb20udHc=3D"> <DIV id=3D"Z2317723S" style=3D"background-col=
or: #FF0000;display: inline-block; padding: 7px; color:#fff"> K&#8288;=
e<INS>ktkngl177</INS>ep S&#8288;a&#8288;m<INS>dkzk4n177</INS>e&#8288; =
P&#8288;a&#8288;s&#8288;sw<INS>zugwzu177</INS>ord </DIV></A> <DIV>&nbs=
p;</DIV> <DIV> @ P&#8288;o&#8288;w<INS>nkfwur177</INS>e&#8288;r&#8288;=
ed B&#8288;y M&#8288;i&#8288;cr&#8288;o<INS>i6uoqp177</INS>s&#8288;of&=
#8288;t 2021 <DIV> </DIV> </body>
 </html>

--K=_qu5cderb44smenShZwB3nDkCgvh86en--
```

这封钓鱼邮件使用了<base> HTML 标签

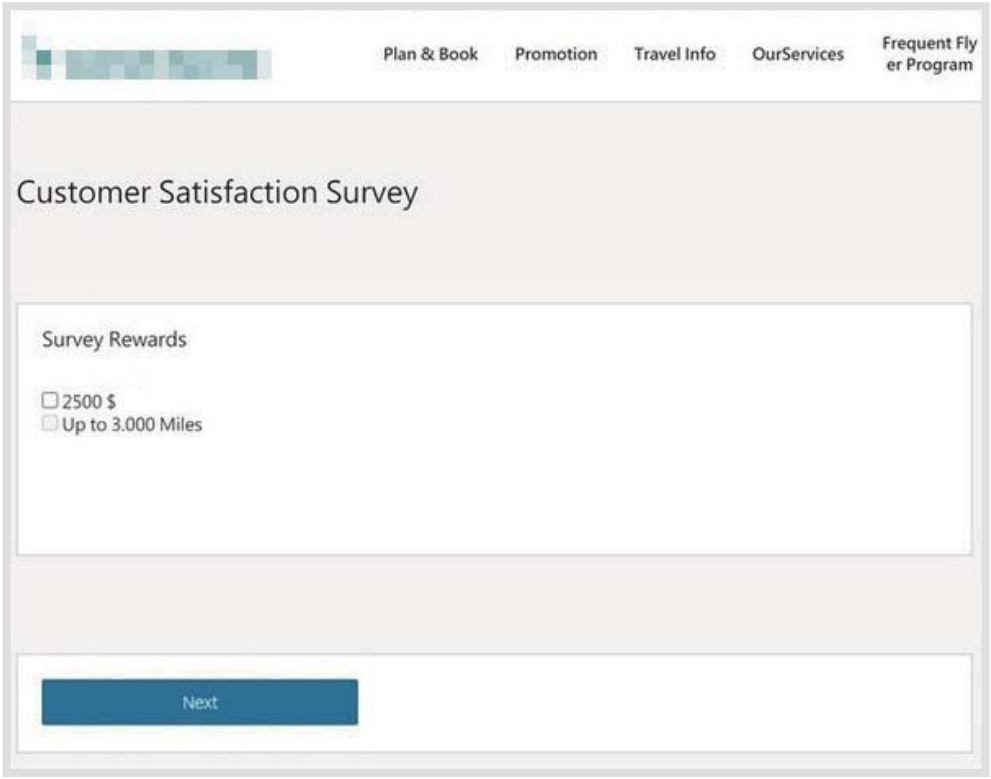
冒充航空公司的回馈问卷调查，目的在钓取个人信用卡信息

八月份有攻击者冒充某几家航空公司身份，以入选客户忠诚方案为名的问卷调查，肆意流窜出一波主题为「Congratulations ! You've been selected by xxxx Airline Loyalty Program」的邮件，目标是骗取收件人的信用卡信息。



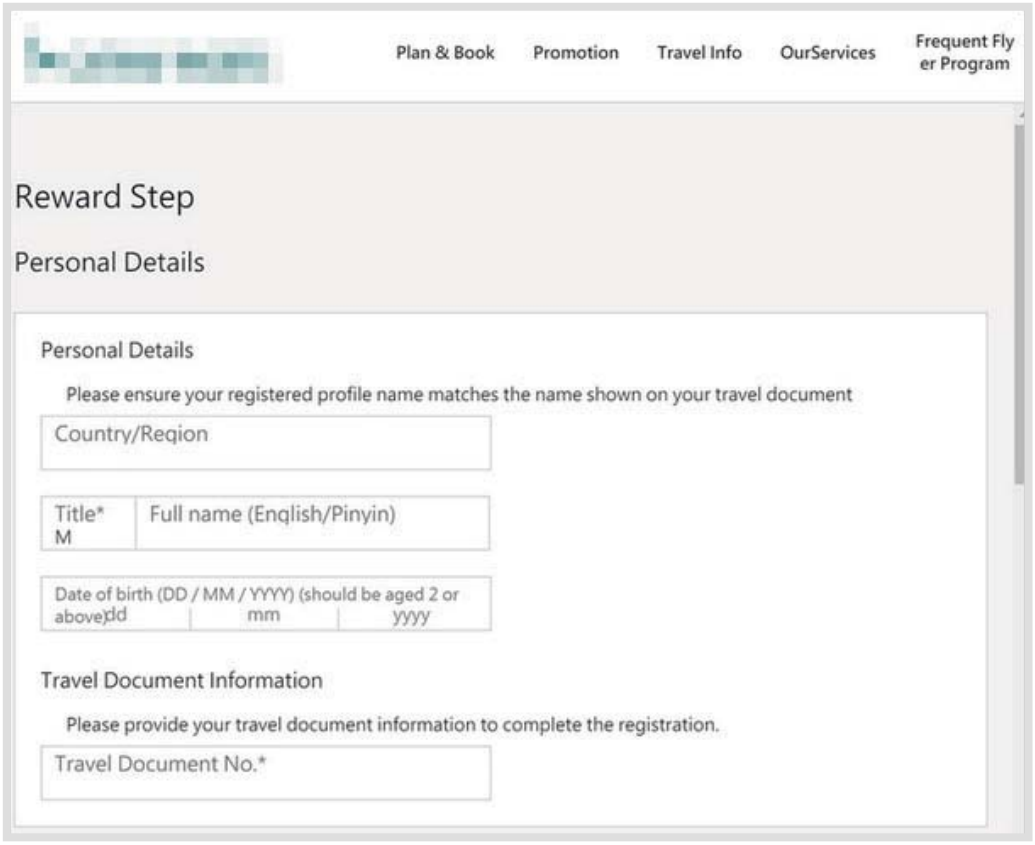
假冒某航空公司，以限时活动、花 2~3 分钟便可获得回馈的调查方案，引诱收件人填写问卷

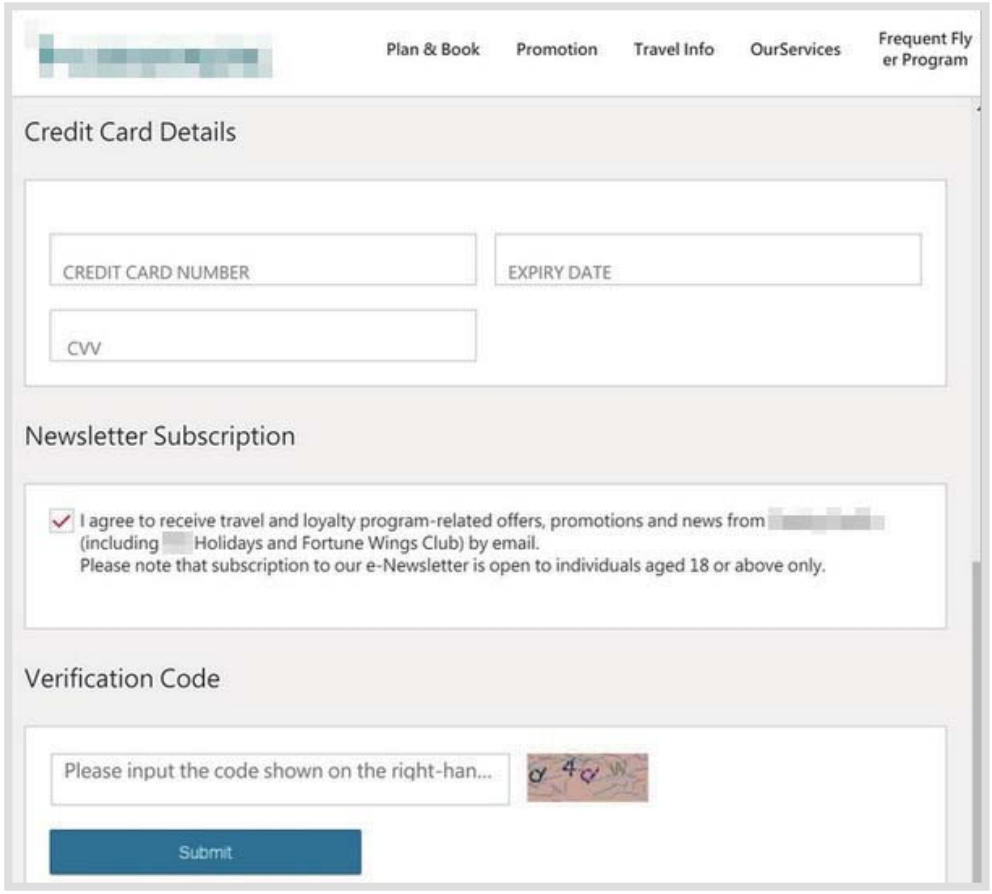
邮件中宣称只要花一点时间协助做完问卷调查，就能得到丰厚的账户奖励。为了取信收件人，邮件中所有的图片皆来自航空公司官方网站，只有问卷所在的网址暗藏于被篡改的网站。若收件人贸然点击链接前往此页，可能会被精心设计伪装好的问卷调查，松懈了戒心；在填完假问卷后，便会进一步要求个人的信息。



声称填完问卷可获得实质奖励

当被害人填写完个人信息后，接着会被要求输入信用卡信息，这一切都是为了取得「奖励」的必要步骤。





为取得奖励，必须填写个人资料与信用卡信息

被害人填写信用卡信息，并按下发送，则会收到要求填写手机短信验证码认证；若再配合输入短信验证码，则后续来的不是航空公司的奖励，而是一连串刷卡通知。此时，信用卡已经正式遭到盗刷！提醒大家在使用填写一些公共邮箱的问卷调查时，请注意自己最近是否有使用过相关产品，填写信息时注意信息合理性，特别是手机验证码等信息，加强此类钓鱼防范。

与自身业务有关的社交工程攻击

在企业加强倡导信息安全观念的当下，收到与自己业务无关或与自身习惯使用语言不同的邮件，多半会有所警觉，并且不会打开相关附件内容。但若出现与自身业务相关，内容也使用自身习惯用语撰写的恶意邮件，该如何提防呢？

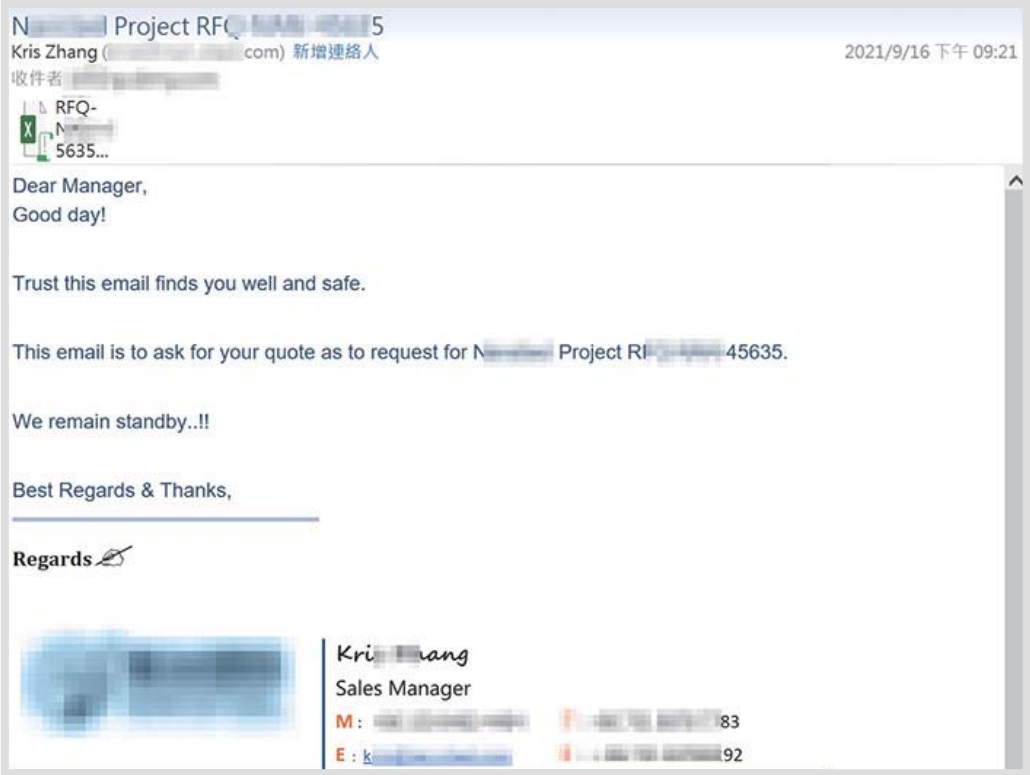
在第三季度出现许多假借业务咨询、保费、客服等问题，却夹带攻击文档的恶意邮件。这些恶意文档，都以压缩文件的方式夹带一个可执行文件，并且将图示或扩展名，试图伪造为 PDF 文件档。

假借业务询问，却夹带攻击档案的恶意邮件

虽然这些假借业务咨询、保费、客服等问题邮件在内的社交工程手法类似，但邮件中所附带的恶意软件并没有明确的关联性，部分恶意软件也会以压缩文件加密的方式躲避扫描；运行时攻击目的也有所不同，目前只发现攻击 Windows 的样本。防范这类邮件，建议不要隐藏扩展名、不要运行解压缩后文件名不明的 .exe 档案。

邮件压缩包炸弹，瘫痪过滤系统

Microsoft Office 自 2007 版本之后，提供了新的文件包装格式，使用 XML 体系结构和 ZIP 压缩将文档、公式、VBA 等内容储存到行和列的组织，常见格式附文件名为 .docx、xlsx、pptx、xlsm…等。我们发现这个 ZIP 的包装结构，与早期的压缩文件炸弹手法进行结合，用以干扰电子邮件的内容扫描机制。



电子邮件中一个 .xlsm 的附件文档，大小约为 2mb，之中掺入了压缩文件炸弹的手法

将这个 .xlsm 解压缩后，产生三个 OLE 对象的 .bin 文档，其中较小的两个档案，是由 VBScript 写成的恶意软件主体内容下载器，执行结束后会自我清除；oleObject3.bin 则是通过 CVE-2017-11882 的代码漏洞去执行前述的 VBScript。而 oleObject3 解压缩后的大小约为 2GB，由于这个文档大小过大，会对某些扫描机制产生干扰，也可能造成扫描时缓存空间瞬间用罄，导致非预期的问题。

oleObject3.bin 压缩文件炸弹膨胀后的大小约为 2GB

结语

攻击者如何发送恶意邮件到目标对象的信箱?主要有两种方式,一种是以字典文件针对一个域名持续尝试;另一种,则是根据暴露于网络上的数据,以及遭到外泄的数据库。以字典文件尝试发送的方式,多半具有较低的针对性,容易侦测出尝试的行为并加以阻断;较为危险及常被忽视的会是后者。根据暴露于网络上的数据,以及遭到外泄的数据库名单所发送的攻击信件,多半还伴随有该邮件地址拥有者的其它相关资料,如:个人信息、兴趣、其他联系信息等等,能够用于更有针对性且为受害目标量身打造的攻击。

因此,在使用电子邮件地址申请任何服务时,最好能依照功能分类,或区分使用私人邮箱注册和公司邮箱注册,用以区别收件来源的重要性,必要时也可以关闭不用的私人邮箱,避免信息关联,将自己彻底从攻击者的名单中移除。

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。