2022 守内安信息科技 & ASRC
电子邮件趋势安全回顾

ASRC

Spam Mail
Virus Mail
Malicious Mail

Feb 2023 released.

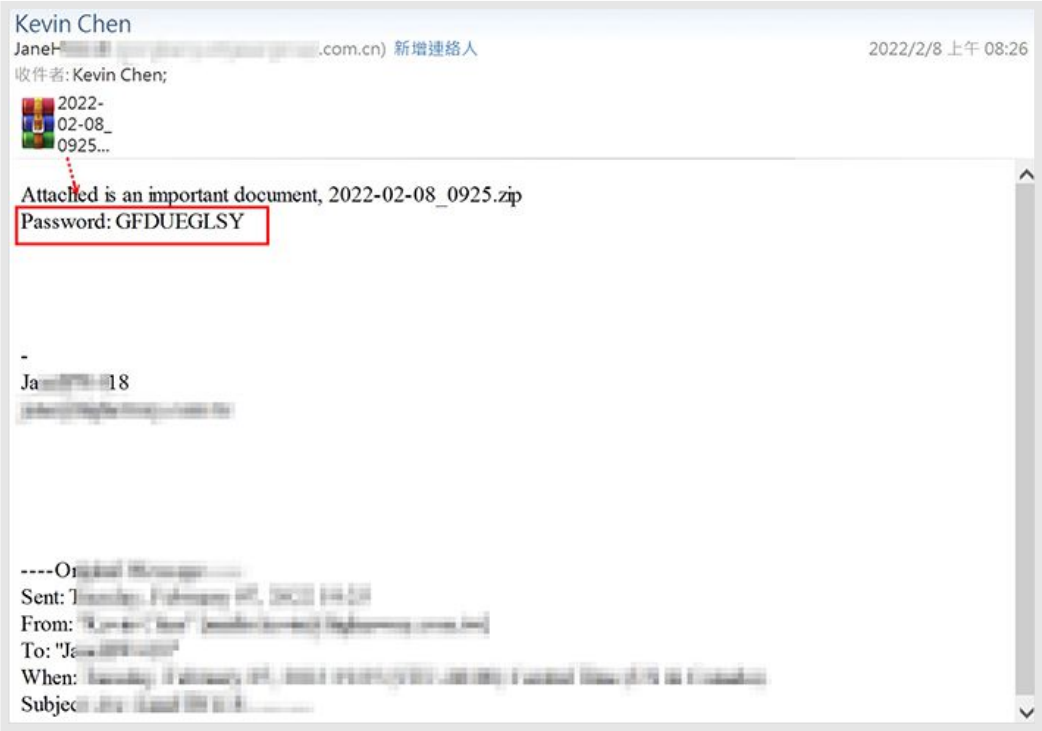
2022 年对许多人来说是艰难的一年，世界仍受疫情影响，全球通膨也让经济局势萎靡，加上地缘政治风险不断升高、战争爆发，更让信息安全的重要性被瞬间拉高。我们可通过回顾 2022 电子邮件的攻击形态，思考 2023 即将可能面对的攻击趋势与未知风险，并及早防范！

概要

根据守内安与 ASRC 研究中心的观测数据，相较 2021 年，2022 年的病毒邮件数量大约成长了 31%；419 scam 诈骗邮件成长了 76.37%；而恶意邮件中携带了 zip 及 rar 压缩文件的状况都增长了 50% 以上，其中很大一部分被密码加密保护，加密的恶意压缩文件很可能就此成为未来常见的趋势；而携带恶意文件增长最多的为恶意 pdf 文件，其次则分别为 Office 的 Word 格式文件与 Excel 文件。Office 文件漏洞利用以 CVE-2021-40444 增幅最多，更早的漏洞的利用情况也依然有所增长；CVE-2022-41049 也是在 2022 年 11 月揭露后就开始出现频繁被利用的迹象。文件型漏洞利用大致可看出：新的漏洞被揭露后会在短时间内遭到频繁尝试利用；但旧的文件漏洞利用攻击仍存在，显然，攻击者并不认为旧有漏洞会被全面修补。全年来看，攻击邮件数量最多的时间点则是集中在第二季。

恶意加密压缩附件

在 2022 年第一季度中大量流行的 Emotet 恶意邮件攻击，其所携带的恶意 Office 文件多为 xls、xlsx、xlsm、doc、docx、docm...等等。但值得注意的是，这些文件除了直接对外发送外，也会以 zip 加上密码的方式发送，目的就是为了躲避网络安全设备的侦查与拦截。此类攻击邮件最明显的特征是：解密的密码与加密文件的压缩同时存在同一封邮件中，此方式在日本已存在多年，与附件压缩加密的网络安全防护方式简称为 PPAP 最大的区别点是：PPAP 是由 4 个词所组成，Password、Password、An、Protocol。一般是指将电子邮件携带的附件，透过 ZIP 加密压缩。再将密码，通过另一封邮件发给对方解密。



以 zip 加上密码的方式，躲避网络安全设备的侦查与拦截

PPAP 的使用有许多疑虑与弊病存在：加密文件与密码经常使用相同的通讯渠道分次传输、长久使用固定密码以及加密文件直接遭到拦截并被暴力破解的问题等，都说明了 PPAP 的使用并不安全。再加上 2022 年的加密恶意压缩附件数量大幅增长，已有多个大型企业集团直接废除 PPAP 的传输方式，并宣布接收外部邮件时，将会直接过滤掉带有密码的压缩文件。因此，未来带有加密附件的电子邮件在网络安全防护的角度下，很可能会由原有的保护敏感文件的角度，全面转变为需要受到重点检查，或被隔离的邮件。

以「安全」为名的攻击邮件

在 2022 年我们也经常看见教人防范钓鱼邮件的教学，内容却是带有连往钓鱼网站的钓鱼邮件链接。

货真价实的钓鱼邮件，内容却为防范钓鱼邮件的教学

假借安全通报，实则带有 CobaltStrike Beacon 后门程序的攻击邮件。虽然发送邮件的源头并非真的由技术安全中心而来，但在内容上，不论是格式或是用语都煞有其事，并附上了一个恶意附件，在邮件内容中还标注了解压缩的密码，并诱骗收件人要想知道完整的内容信息，需要解压附件后获取。

发布编号	NCCST-ANA-2022-1114	发布时间	Mon Nov 14 16:52:58 CST 2022
事件类型	预警	发现时间	Fri Nov 13 14:27:44 CST 2022
告警主题	社交工程攻击报告：请加强防范黑客假冒公务名义发送疫苗相关主题的恶意电子邮件		
内容说明	国家网络安全服务中心近期从恶意电子邮件检测服务中发现，黑客利用疫苗热点，假冒公务名义发送特定相关标题电子邮件，诱使用户开启恶意附件后植入恶意软件，已知相关攻击邮件特征如下: 1.假冒发件人:「lclect@sec[.]gov[2.恶意信件主题: (1)「疫苗情况通报」 (2)「疫苗情况通报」 (3)「疫苗事务变更公告.doc?[_空白_].exe」 3.恶意附件名称:「疫苗事件公告变更公告.doc.exe」 4.恶意中继站:「www[.]acceunt_mettgooggl[.]serveuser[.]com」		
影响平台	所有 Microsoft 环境系统		
影响等级	高		
建议措施	请参阅邮件所附附件，若需输入密码 压缩文件密码均为 nccst@2022		

攻击邮件冒充了某安全情报服务中心发布的漏洞信息

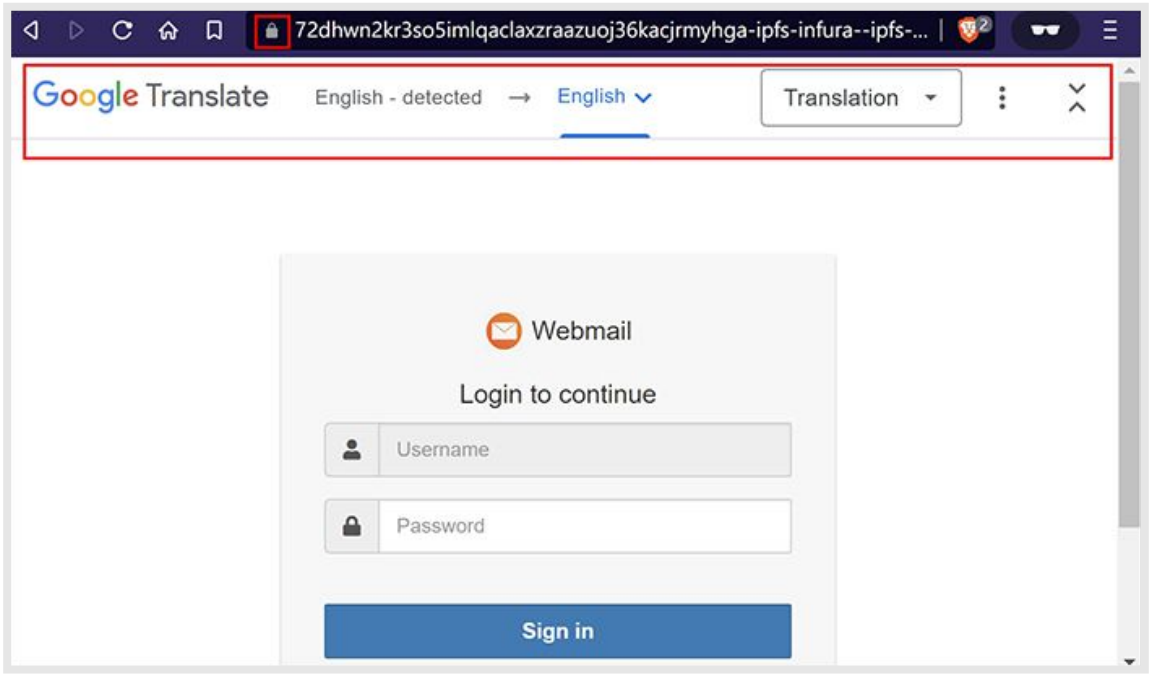
许多的攻击手法、通知常常通过邮件的渠道作发布，且配合近几年越来越多企业对于邮件安全性重视不断提高，通知员工提高相关防范。因此收件人可能会对「教学说明」、「安全通知」类的邮件放下戒心，误以为是公司组织的安全教育。这类型的社交工程手段在未来很可能会频繁出现。

钓鱼邮件大爆发的一年

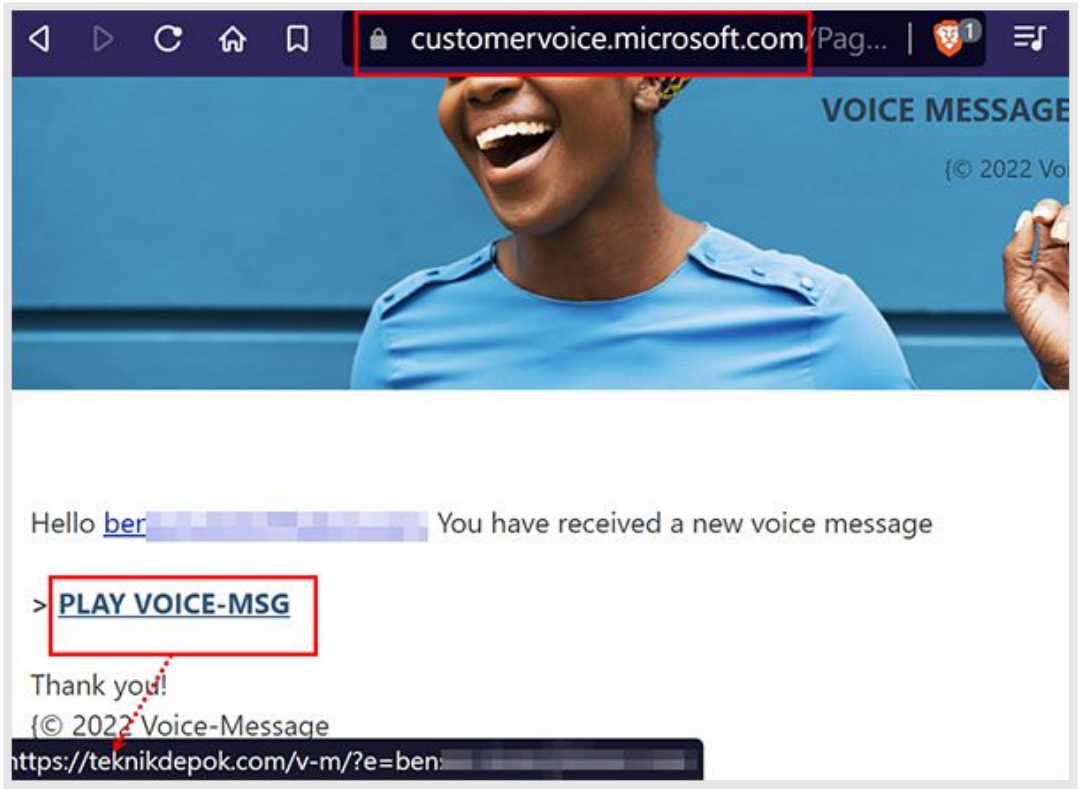
澳大利亚竞争与消费者委员会 (ACCC) 显示，2022 年 3 月，澳大利亚人因各种类型的诈骗共损失了 9500 万澳元。网络钓鱼攻击正变得越来越普遍，并且在未来几年没有任何趋缓的迹象。而根据 IBM 的 2021 年数据泄露成本报告，网络钓鱼是第二昂贵的攻击媒介，平均给组织造成 465 万美元的损失。网络钓鱼几乎是所有网络攻击最经典的攻击前奏，面对它所带来的损失，相信绝不是一个不采取任何行动就能被接受的风险。

网络钓鱼攻击事件的数量逐年增加，根据 ASRC 的统计，相较于 2021 年，2022 年的钓鱼邮件数量成长幅度高达 2 倍。在此所谓的网络钓鱼邮件意指：电子邮件中仅携带一个恶意超链接，且不存在除了图片以外的附件文件，将受害者带往特制的钓鱼网站，目的是骗取受害者的机敏数据，以作为后续其他攻击的利用。

钓鱼邮件进化的方向主要是朝着钓鱼网址不要被侦测、不要被浏览器屏蔽的方向发展。在 2022 年我们可看到钓鱼网站利用了 Google 翻译、微软的在线问卷机制，遮蔽了真实的网址，使得邮件内恶意网址的侦测变得困难、同时受害者也不容易受到浏览器的网址安全功能保护。



Google 翻译本身支持了翻译整个网站的功能，也可被盗用于屏蔽钓鱼网站；识别的秘诀是：网页中存在 Google 的翻译列



钓鱼攻击盗用了微软的在线问卷调查机制

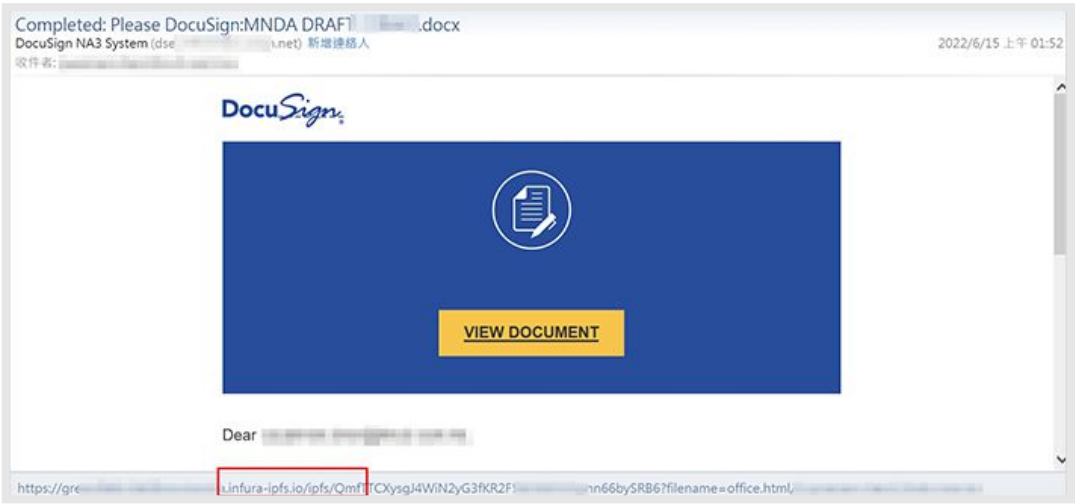
除了利用合法服务进行网址屏蔽外，部分的钓鱼邮件也利用QRcode来隐藏恶意网址，相较于其他区域，这样的攻击在中国更常见，但此类攻击占整体的钓鱼邮件数量其实不多，而且此类钓鱼邮件特别针对手机进行攻击。

钓鱼邮件利用 QRcode 隐藏恶意网址

二维码解码后的恶意网站只接受手机浏览器才会显示真正的钓鱼页面

钓鱼的目标主要针对银行卡的卡号

整个钓鱼攻击的过程，除了电子邮件外，钓鱼网站才是真正获取敏感信息的重要陷阱。钓鱼网站在过去几年的统计里，绝大多数存活天数都在一天以内，原因是这些钓鱼网站、页面所寄宿的虚拟专用服务器、免费网站窗口生成器、ISP 都会主动进行侦查或接受举报，而将这些钓鱼网站下架。因此，钓鱼网站也需要往更不易被下架的方向作演化！2022 年我们看见了钓鱼网站利用了星际文件系统（InterPlanetary File System，缩写为 IPFS）这个技术做为网站寄宿空间。星际文件系统是一个旨在实现文件的分布式储存、共享和持久化的网络传输协议。它是一种内容可寻址的对等超媒体分发协议。在 IPFS 网络中的节点构成一个分布式文件系统。传统的恶意文件寄存于单一网站，一旦服务器瘫痪或联机中断，这个恶意文件或是钓鱼页面就会瘫痪。但在 IPFS 上，文件可利用多个网络节点上传送，因此可确保内容长久存在，钓鱼网站也更难以被简单封锁或被网站管理员“下架”！



恶意页面或文件开始利用 IPFS 协议躲避封锁

总结

面对2023，企业应仔细考虑加密文件的流动是否存在绕过安全审核的风险。此外，千万别将所有的风险防范都寄望于“人体防火墙”，社交工程逐步精致复杂化，已经不是一般未经教育训练的人员可抵御的风险。再者，钓鱼的手段越来越多样化，难保敏感数据凭证不会因为一时的疏失而泄露，采取零信任的环境部署，针对每一个服务登入都要求验证、记录，并适当将操作权限开放在合理的最小化状态，将可有效减轻凭证遭到钓鱼攻击的风险！

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。