2023 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

April 2023 released.

2023 年第一季度，网络世界似乎也受到全球复苏的影响，攻击者蠢蠢欲动：今年第一季整体垃圾邮件及病毒邮件的数量，相较去年第四季成长将近一倍；由打信机或殭尸网络进行的邮件试探发送的频率较去年第四季度提升 450%！

以下为守内安与 ASRC 研究中心在本季观察到的特殊邮件攻击案例：

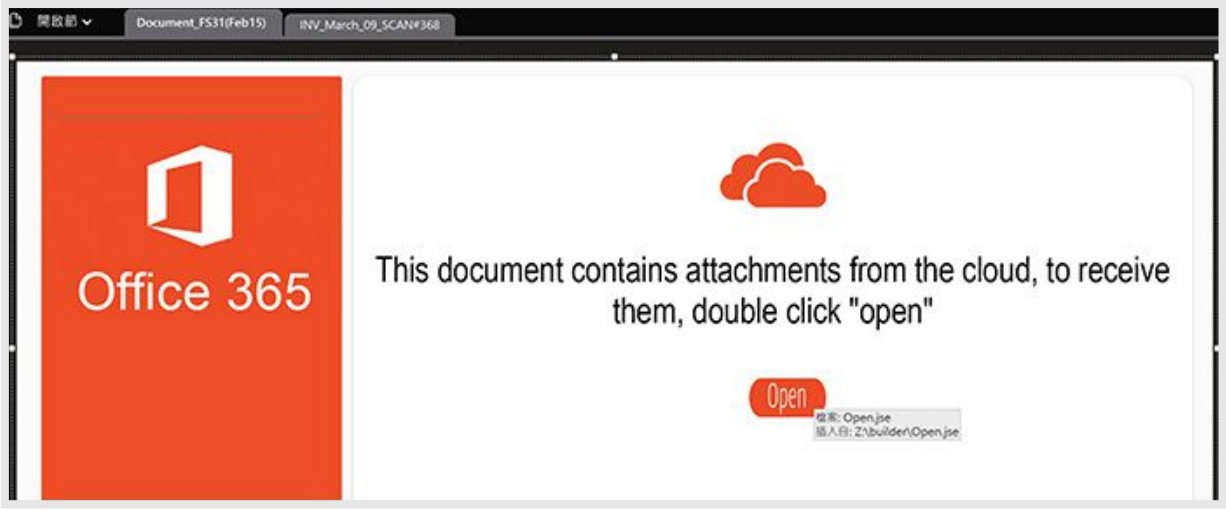
针对 Microsoft OneNote 的攻击

Qbot 于今年第一季有一波通过电子邮件流窜的恶意攻击，名为 QakNote。

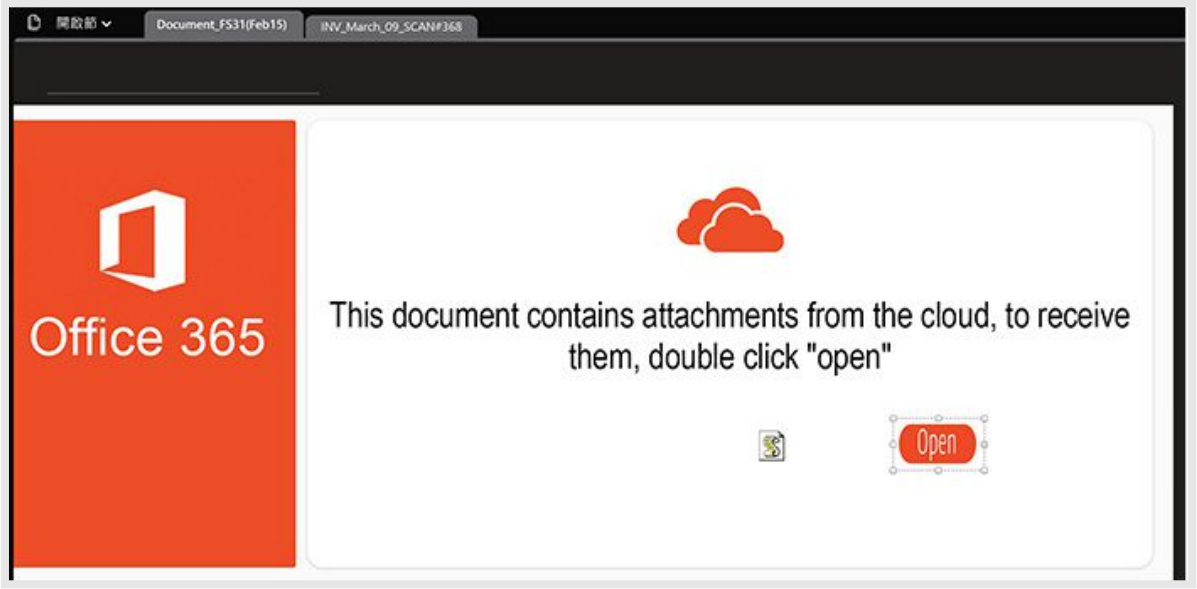
这个攻击主要的特性是使用 .one 的恶意文件试图攻破 Microsoft OneNote，为后续的恶意行动打开受感染装置的入侵大门。

为了防范宏在 Office 文件中被恶意滥用，微软去年七月宣布关闭宏功能的措施会部署到 Windows 平台的 Access、Excel、PowerPoint、Word 和 Visio。今年一月我们就发现了攻击者瞄准 Microsoft OneNote 发动新的恶意攻势。

.one 的恶意文件中可包含恶意的 VBS 、HTA 或 LNK 快捷方式作为附件，也可以携带恶意的 .js或 .jse，当受害者不慎点击其中的携带附件，就可能触发一连串请求 powershell.exe 执行的恶意行为。



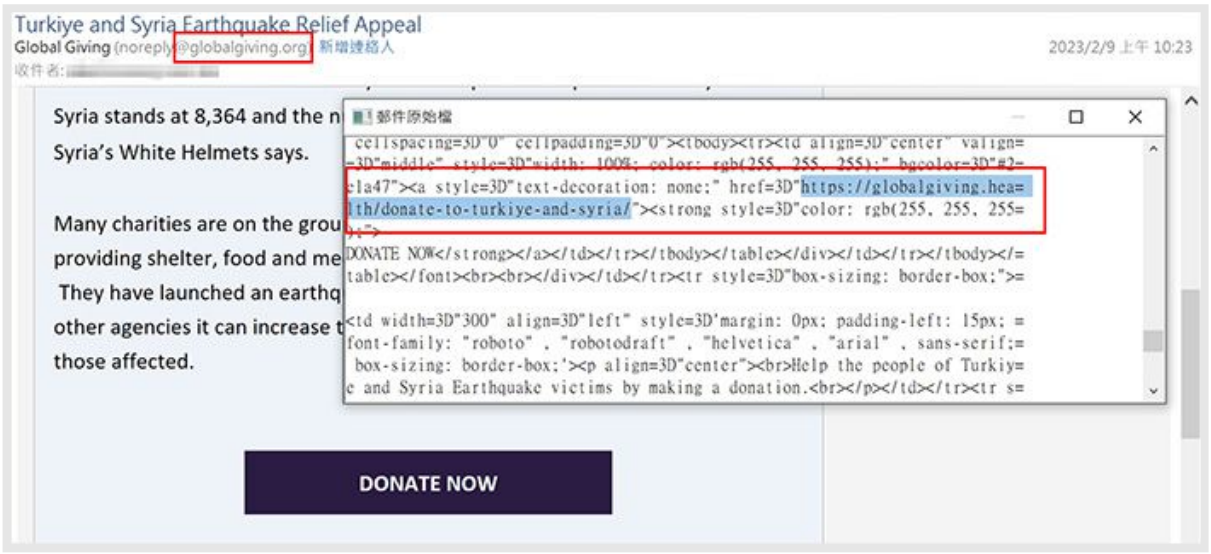
OneNote 允许在笔记中插入各种附件



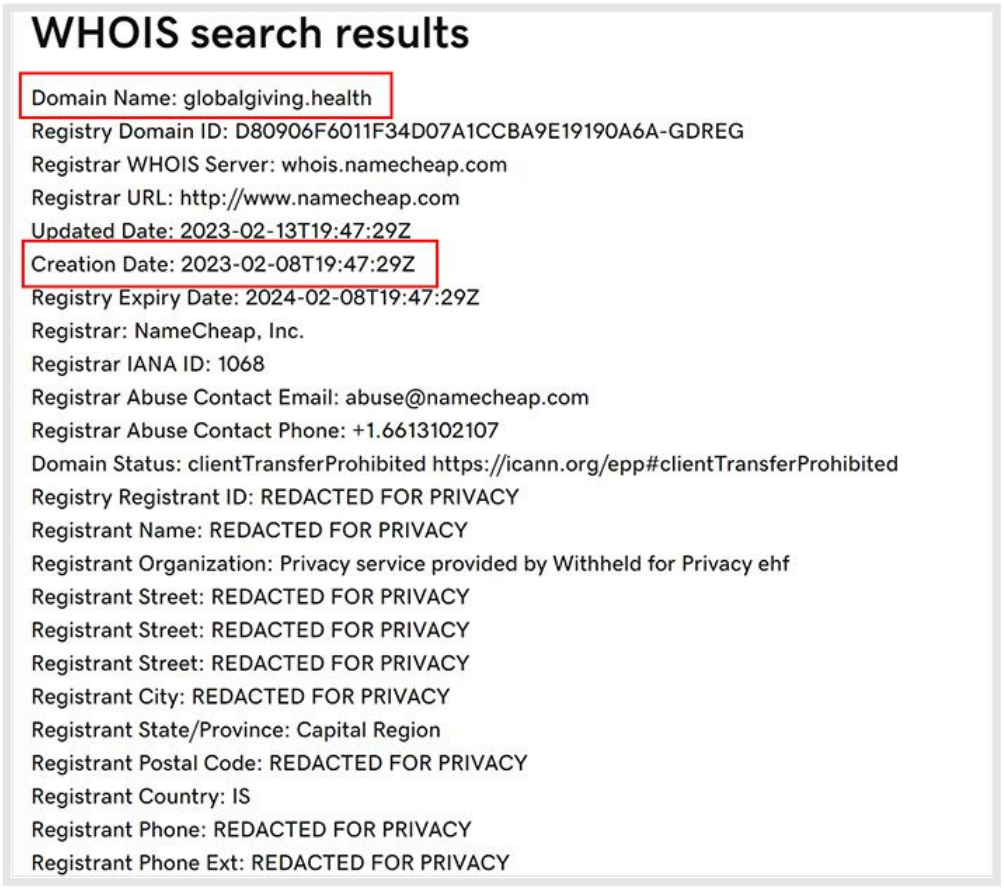
插入的附件成为一个个组件，这些组件可以移动或排序前后位置，原始的攻击刻意将攻击程序代码藏在图片后方

土耳其震灾募款诈骗邮件

2023 年 2 月 6 日凌晨 4 时 17 分，土耳其发生强烈地震，受灾规模巨大引起世界关注，同样也引起了黑客的关注。在初期，我们观测到的诈骗邮件通过假冒全球捐赠网（globalgiving.org）的捐款信息，搭配带有二维码的钓鱼页面进行虚拟货币的捐款诈骗。



假冒全球捐赠网的诈骗



WHOIS search results

Domain Name: globalgiving.health
Registry Domain ID: D80906F6011F34D07A1CCBA9E19190A6A-GDREG
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 2023-02-13T19:47:29Z
Creation Date: 2023-02-08T19:47:29Z
Registry Expiry Date: 2024-02-08T19:47:29Z
Registrar: NameCheap, Inc.
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.6613102107
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: Privacy service provided by Withheld for Privacy ehf
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: Capital Region
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: IS
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY

但其来信的网域却是在 2023/02/08 注册

钓鱼页面本身不具备交易或骗取敏感数据的功能，只提供三个指向诈骗用虚拟钱包地址的 QR code：

BTC

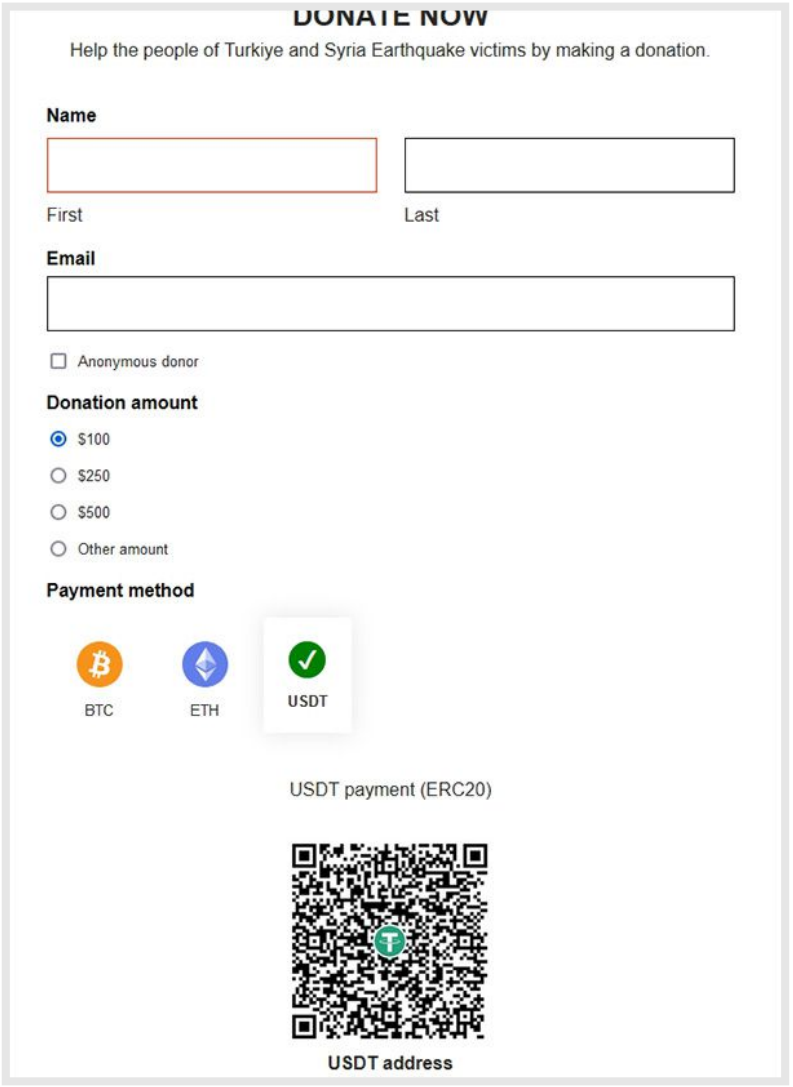
bitcoin:15euPhVcHmSP1kHeq2EyWvf9NXS12hmcWN

ETH

ethereum:0xFb9217f10569a60A352b26A22fD99a1719c1bCd7@1

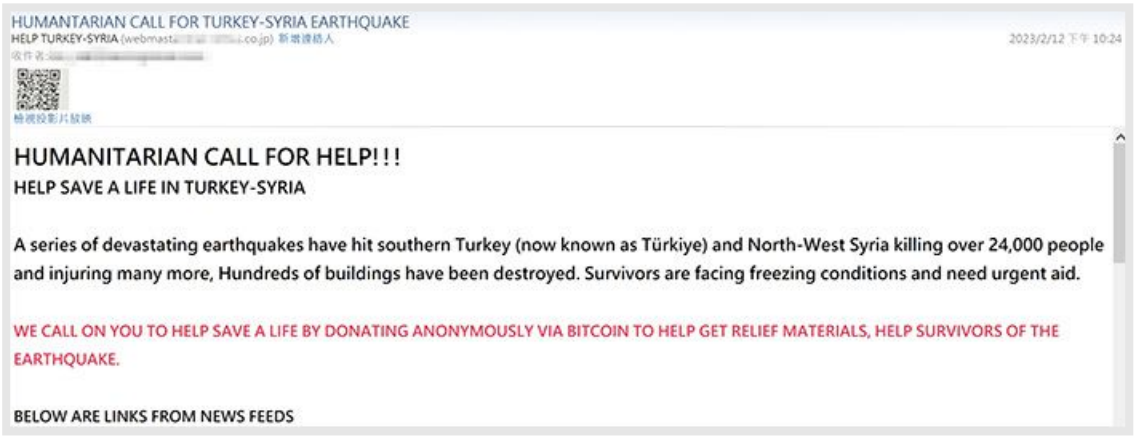
USDT

ethereum:0xdAC17F958D2ee523a2206206994597C13D831ec7@1/transfer?address=0xFb9217f10569a60A352b26A22fD99a1719c1bCd7



钓鱼页面本身不具备交易或骗取机敏数据的功能

另一型态则是在内文要求直接捐款至特定比特币钱包账户：bc1q2ta3f85kyd6ez6gtz45agxfxwp7007wdnzvg4n。



附带 QRcode 的善款诈骗邮件

这封诈骗信夹带了 QRcode 图片附件，经过解码，结果为另一个比特币钱包：
bitcoin:bc1qfpehxeppc9yd2farrxxq5mlr4xr82ezwevu7uf，这个钱包过去就被广泛用于各种诈骗与恐吓取财。

提醒您，若要响应各种善款的捐助，请直接寻找官方统一的捐款单位；务必提防通过诈骗邮件要求任何捐款指示的操作，许多网络诈骗行动并非一次性的损失，食髓知味的攻击者会记录容易上当的受害者并且持续攻击！

漏洞利用：CVE-2023-21716、CVE-2023-23397

Microsoft 于 2 月 14 日发布重大漏洞 CVE-2023-21716，同时影响了多个版本的 Microsoft Office，此为远程执行任意程序代码 (RCE，Remote Code Execution) 漏洞，CVSS 评分值高达 9.8。这个漏洞的入侵方式为攻击者通过电子邮件携带特制的 RTF 文件，若使用者开启 RTF 文件；或以带有预览窗口的 Office 应用程序 (如: Microsoft Outlook) 浏览，黑客可藉此漏洞执行任意程序代码。

而在 Microsoft 3 月发布的安全性更新中 CVE-2023-23397 (CVSS评分值9.8) 为Microsoft Outlook 特权提升 (EoP) 漏洞，可利用 Outlook 的日历提醒功能来窃取受害者的 Net-NTLMv2 哈希。黑客通过发送利用此漏洞的恶意邮件后，Outlook 客户端只要接收并处理邮件，即便使用者没有开启或预览这封恶意邮件，都会自动触发该漏洞并泄漏 Net-NTLMv2 哈希。2022 年 4 月 1 日从乌克兰上传 VirusTotal 的样本，试图攻击乌克兰国家移民局；一家经营军舰、国防科技的土耳其公司，2022 年底便遭受到漏洞攻击。漏洞早在一年前便开始被滥用。

这两个漏洞都可让黑客通过恶意电子邮件进行攻击，应尽速修补。

邮件炸弹

邮件炸弹 (Email bomb) 是一种恶意滥用电子邮件的行为，其目的是使目标邮箱超额或使目标邮件服务器瘫痪，其中一种手段是利用压缩文件来进行。通过修改压缩文件，可让商业邮件服务器、反垃圾机制或是防病毒软件在解压缩检查压缩文件内容物时，拒绝服务或其他问题。在今年三月份我们看见了一种融合了过去邮件炸弹手法的新攻击手段。

压缩文件里的 WORD 文件有着超高比例的压缩

这种攻击在 Office Word 文件的前半段嵌入恶意攻击的程序代码；而后半段则全填为 0。当网络安全设备试图解压缩进行扫描检查时，解压缩后的文件大小过大很容易将缓存空间塞满，或造成其他包括内存方面未预期的错误；也可能因为文件过大而被略过某些扫描。所幸，这波攻击只持续了一小段时间便消失了。

结语

这一季最受瞩目的信息相关新闻，应该就是面向大众的 AI 实用功能推出与应用，由 OpenAI 的 ChatGPT 为全球展示了生成式AI为人类生产效率提升的可能性；可预见的，也可能提高攻击者的攻击效率。虽然目前还未看到较具体的攻击应用，但生成式 AI 可在短时间内生成较以往更令人信服的文案、翻译、以假乱真的图片，社交工程方面的攻击将会是未来的一大隐患。

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。