2020 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

Jun 2020 released.

2020年第一季度很不平静，让世界各国都绷紧神经的莫过于新冠肺炎疫情相关的话题。不论是疫情扩散速度、防疫措施，抑或是物资采购、捐赠等都是热点话题。随着新冠肺炎疫情蔓延，出现许多诈骗邮件以提供防止被追踪的比特币钱包地址，以采购物资、资助研究的名义募捐，进行敛财。ASRC 研究中心 (Asia Spam-message Research Center) 在2020年第一季度观察到几个值得注意的邮件安全议题：

远程办公模式成为黑客攻击目标，造成各种诈骗泛滥

2020年第一季度，全球在新冠肺炎疫情的影响下，保持“社交距离 (Social Distancing)”改变了人类的生活方式。由于新冠肺炎极高的传染率，许多企业采取了居家上班的工作模式。这样的工作模式会带来如下影响：

网络流量的需求
在短时间急剧上升

远程连线、远程会议
VPN的需求量大增

人们直接见面接触的
概率大幅下降

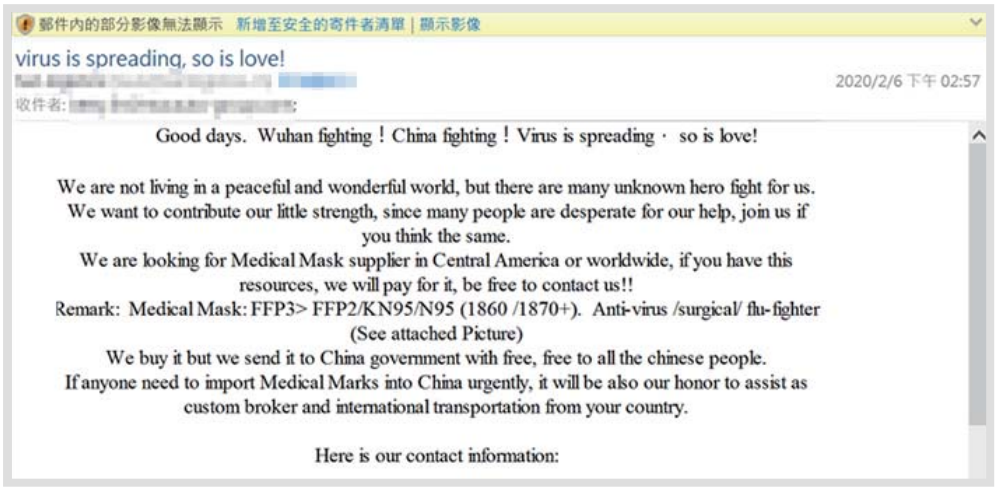
远程办公模式成为黑客攻击目标，造成各种诈骗泛滥。

病毒邮件比上一季度增加 340%、诈骗邮件爆增 400%

根据 ASRC 研究中心 (Asia Spam-message Research Center) 的观察，2020年第一季度的整体邮件量微幅上升，尤其是新冠肺炎疫情对全球影响最严重的三月；病毒邮件量明显激增，比上一季度，大约增加了340%；诈骗邮件的数量比上一季度增加约400%。

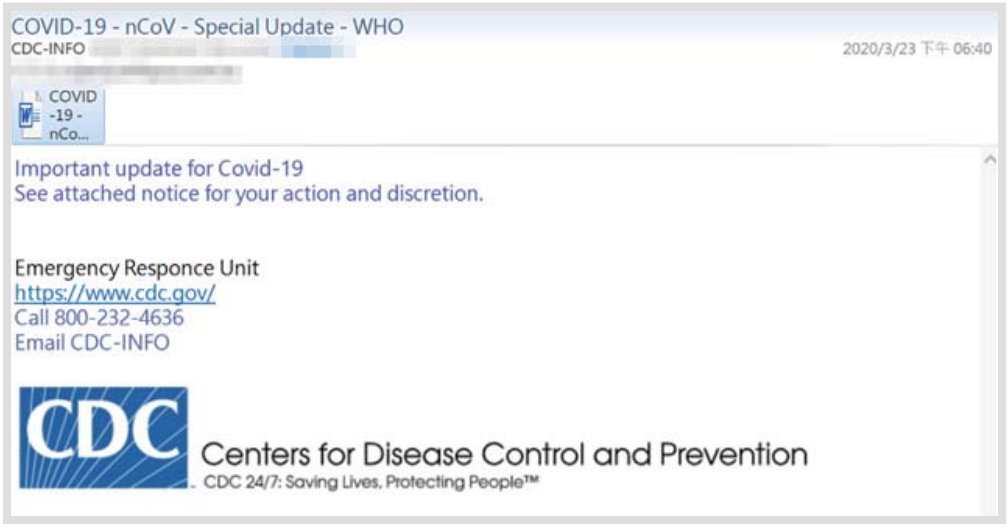
借新冠肺炎名义的攻击，以诈骗或入侵企业为目的

在新冠肺炎疫情逐渐蔓延的第一季度，许多攻击以疫情的名义，试图诱骗收件人打开恶意攻击邮件。这些攻击邮件，其邮件主题多半会带上cdc、covid、corona、spread这些关键字。
数量最多的是诈骗邮件，大部分是假冒研究机构或医疗单位，请求收件人捐钱；也有诈骗邮件谎称可购买疫苗或检测试剂，也是以骗财为目的。



募集捐款购买防疫物资的诈骗邮件

另一种目的是试图通过电子邮件尝试入侵企业内部，后续进行盗取信息、部署勒索软件等。这类攻击，多半直接发送可利用Office漏洞的恶意文件，并以疫情相关主题诱骗收件人开启，试图藉此提高攻击的成功机率。经统计，此类攻击常用的漏洞编号为：CVE-2012-0158、CVE-2017-11882、CVE-2017-0199以及CVE-2017-8570。



假冒CDC的通知，实际是利用CVE-2017-11882漏洞的恶意文件

在2020年3月，有大量以covid、corona相关的域名被注册，这些域名被用于售卖新冠肺炎病毒保健品与检测试剂，这些网站可能都是临时设立，其售卖的产品大多也是非法的。其他无附件的恶意邮件多半都夹带了一个以上的超链接用于钓鱼，或是以超链接的方式，诱骗收件人下载远程的恶意程序并执行。

伪装的附件以超链接的方式，诱骗收件人下载远程恶意程序并执行

为避免新冠肺炎群聚感染导致企业单位可能出现的人力损失，远程办公是普遍采取的应对措施。由于作业方式改变，彼此不见面、信息传递阻塞、中间人的窃听，可能出现冒名的情况（假冒老板要求通讯录、汇款、合约、订单等）；攻击者也利用此波疫情，搭配社交工程攻击的手法，进行财务相关的诈骗或入侵攻击，例如：Emotet银行木马等。新冠肺炎疫情对于全球来说，如同黑天鹅一般，大家未能预期它的出现，也不相信感染范围可与1918年西班牙流感匹敌，但新冠肺炎的严重性，也慢慢地变成了事实。那信息安全呢？我们可以看见信息安全所带来的可能性冲击，就如同灰犀牛一般，若我们忽视，则可能随时遭到猝不及防的攻击或损失！

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。