2020 守内安信息科技 & ASRC
邮件安全趋势回顾报告

ASRC

Spam Mail
Virus Mail
Malicious Mail

January 2021 released.

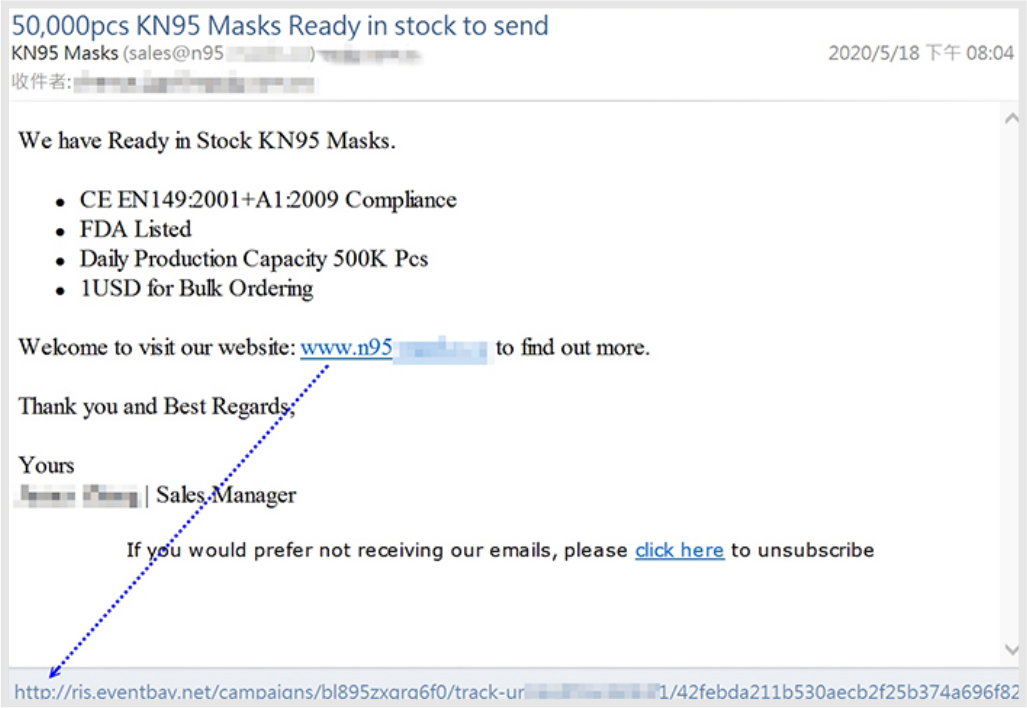
2020年近乎全年都受到Covid-19疫情影响。疫情的出现改变了全球数字工作模式，为了降低疫情对正常工作生活的影响，远程办公或在家学习成了首选，这很可能将成为今后的常态。

远程办公给网络安全部署带来了新的挑战，远程访问不再有「可信任的区域或空间场域」，因此，所有服务的存取都需要验证，迫使提早实现零信任架构。远程办公也推动了云应用的加速，云服务商算是疫情下少数获利者；但云服务设定不当造成数据大批泄漏是容易被忽略的网络安全问题。此外，不论是安全人员或是攻击者，面对远程办公可联想到的网络安全问题，就是VPN联机的安全性保护及DDoS攻击或任何可能的阻断服务取得的手段，这类攻击在2020年很常见。

2020年邮件安全有哪些明显的趋势呢?

诈骗邮件

受到疫情的影响，在邮件安全方面，有关抗疫物资的诈骗邮件经常出现。这些抗疫物资的销售广告来自来路不明的公司与新注册的域名，且出现的频率与疫情的严重程度、抗疫物资的匮乏程度有关。第一季度与第二季度常见此类诈骗邮件；第四季度就相对减少了。



为了口罩销售而指向一些新注册的域名

除了与疫情有关的诈骗邮件外，还有内容以恫吓收件人计算机遭到入侵与监控的比特币诈骗邮件。诈骗的内容其实是杜撰的，但这样的诈骗邮件内容依发送的地区与国别，融合了多国语言，以提高诈骗成功的机率。

攻击目标为中国，邮件内容为中文

有些诈骗并非以直接骗取金钱为目的，而是骗取企业内部的信息，再作后续利用。这样的诈骗在2020年居家办公，不便直接确认的情况下，特别容易奏效。

冒充企业高层，向员工索要企业内部信息，或冒名令其执行不该执行的事务

钓鱼邮件

2020年最多的攻击，非钓鱼邮件莫属了。通常钓鱼的目标，是希望能钓取企业服务的各种凭证，尤其在远程办公的情况下，若能钓到一组企业电子邮件的账号密码，很可能远程取用企业的所有服务！

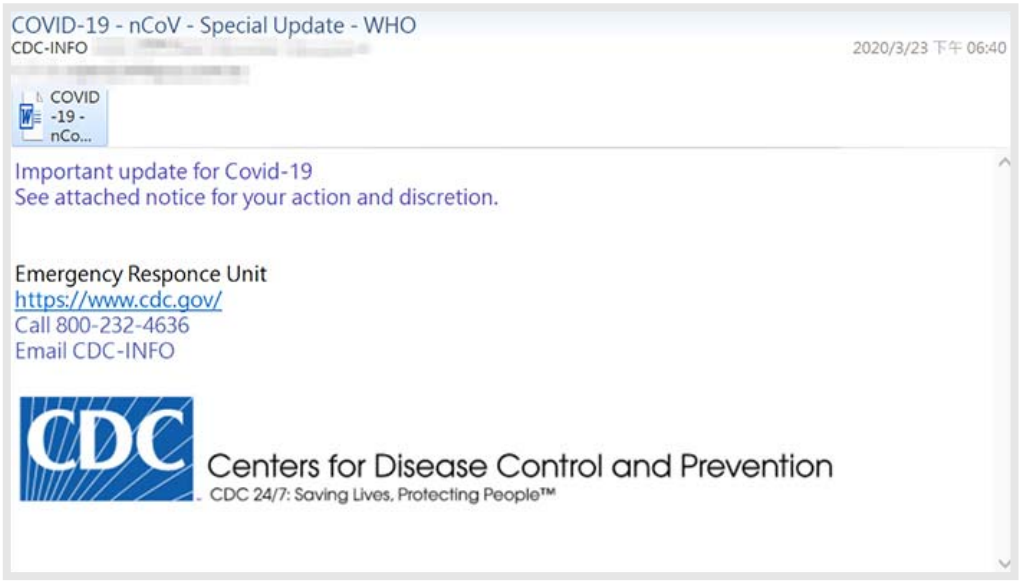
意图骗取邮件账号密码的钓鱼邮件

在2020年第四季度，我们也观察到了声称未付税金导致邮件包裹延迟的钓鱼邮件。这种钓鱼邮件的目的是藉由假的刷卡付税，钓取信用卡信息。在疫情之下，这种钓鱼邮件使受害者更容易上勾！

假冒物流公司发送的钓鱼攻击邮件

漏洞利用

试图通过电子邮件尝试入侵企业单位内部，以进行后续窃取信息、部署勒索软件等目的。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，试图藉此提高攻击成功机率。经统计，此类型攻击常用的漏洞编号为：CVE-2012-0158、CVE-2017-11882、CVE-2017-0199、CVE-2017-8570以及CVE-2018-0802。



冒名 CDC 的通知，事实上是可利用 CVE-2017-11882 漏洞的恶意文件

针对性攻击

在2020年我们也观察到了多起与疫情有关的针对性攻击，与国家资助有关的APT族群尝试以电子邮件攻击则在五月份最为频繁，其中有许多与疫情信息、设备发放、公告通知或口罩相关信息有关。此外，BEC攻击事件以一月份为基准作比对，在2020年11月份达到全年最高峰，这些BEC攻击邮件中都存在着被攻击对象才知道的机密信息。

结论

2021年仍无法明确预测何时可以完全摆脱疫情，而许多企业已将远程办公视为未来可能的常态。远程办公为网络安全带来了新的挑战，在家办公的计算机及所使用的网络也难以确保安全性，因此具备合理访问权限的零信任架构势必是未来趋势。由于远程办公的关系，非实时同步确认事项，多半依靠电子邮件或其他即时通信软件，各种诈骗事件将层出不穷。除了应避免公司数据外泄外，重要事项的联络，最好能设立第二通信渠道作确认；而重大决策也必须落实复核机制，才能避免BEC事件的发生。

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。