2020 守内安信息科技 & ASRC
第二季度邮件安全观察

ASRC

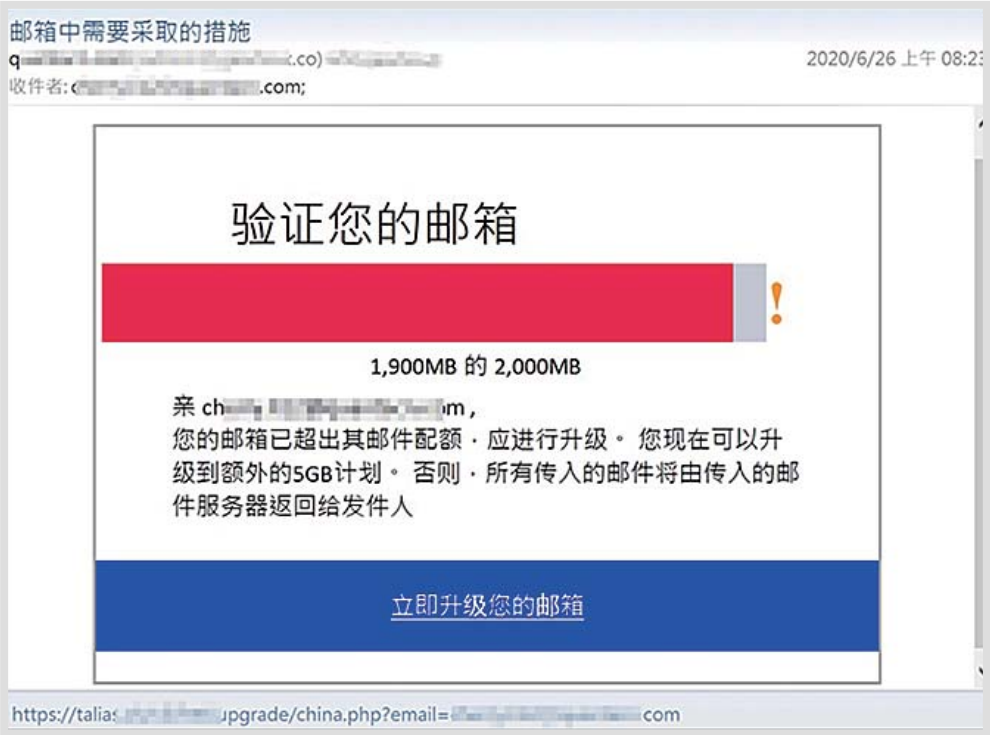
Spam Mail
Virus Mail
Malicious Mail

August 2020 released.

2020年第二季度，全球仍然笼罩在新冠肺炎的疫情中，疫情的影响程度已远超第一季度。许多企业开始采取远程居家的办公模式，以确保公司员工的健康以及特定服务项目的正常运作。工作模式的改变加重了对网络的依赖程度，也因为人与人彼此见不到面，各种诈骗、网络安全漏洞就容易被攻击者所利用。以下简要分享守内安与 ASRC 研究中心 (Asia Spam-message Research Center) 第二季度邮件安全观察概况。

伪造钓鱼邮件较上一季度增加，出现不少伪造企业管理者发送的钓鱼邮件

本季度伪造企业组织通知、收货确认通知等钓鱼邮件明显增多，较上季度大约增长了24%，并且集中在六月。其中为大多数的是伪造企业管理者发送邮件账号密码相关问题的钓鱼邮件，会在收件人点击链接后导向钓鱼页面，这个钓鱼页面通常寄宿于被入侵的Wordpress网站；其次为假的语音与文件发送通知，这些通知除了部分寄宿于被入侵的Wordpress网站，部分则是使用免费的窗体或网站生成器作为钓鱼页面，还有少量直接夹带恶意附件；最后是假的货物运送或商业交易确认，部分寄宿于被入侵的 Wordpress 网站、还有部分则直接将钓鱼页面的 HTML 放在附件文件内试图避开浏览器对网址的警示与检查，还有一部分则是直接夹带以 rar 压缩后的恶意执行文件。

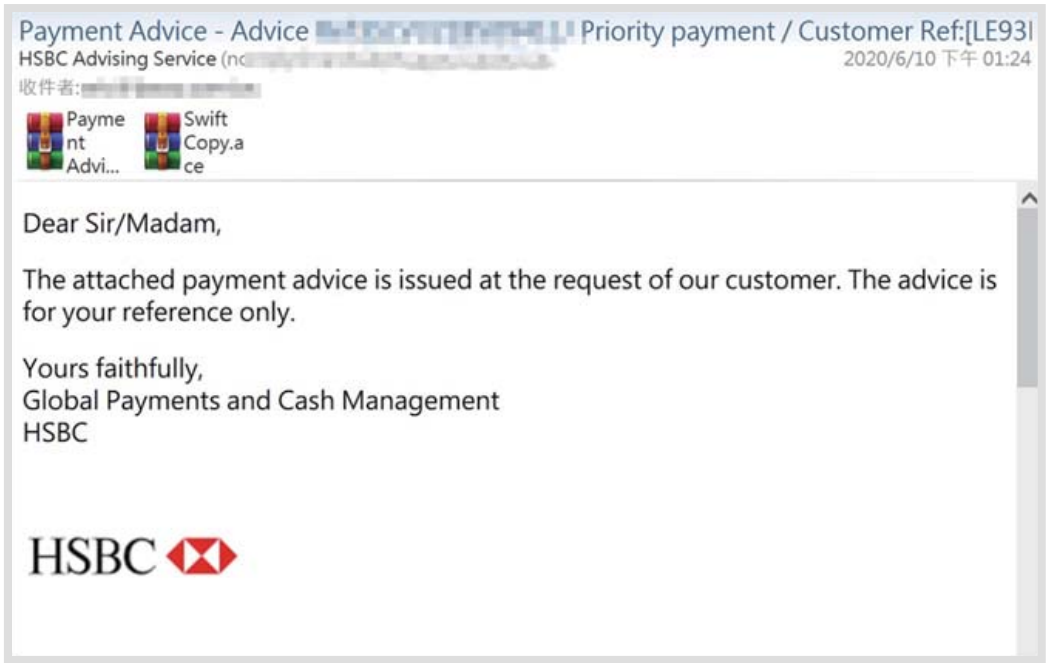


钓鱼页面通常寄宿于被入侵的 Wordpress 网站

病毒邮件数量明显增加，夹带恶意镜像文件或压缩格式文件居多

病毒邮件数量较上一季度增长了约 60%，同样集中在六月。以夹带恶意 .img 文件为多，占了总量 1/3 以上。这些 .img 文件中包含了一个恶意 .exe 可执行文件，在 Windows 环境下被双击后，会自动挂载成为一个虚拟光盘，便可读取其中的 .exe 文件；此外，网络上也有人教学如何以 7-zip 解出镜像文件内的内容，若收到此类恶意攻击时缺乏安全意识，而以如何开启该类文件的目的在网络上寻找答案，也可能因此涉险！

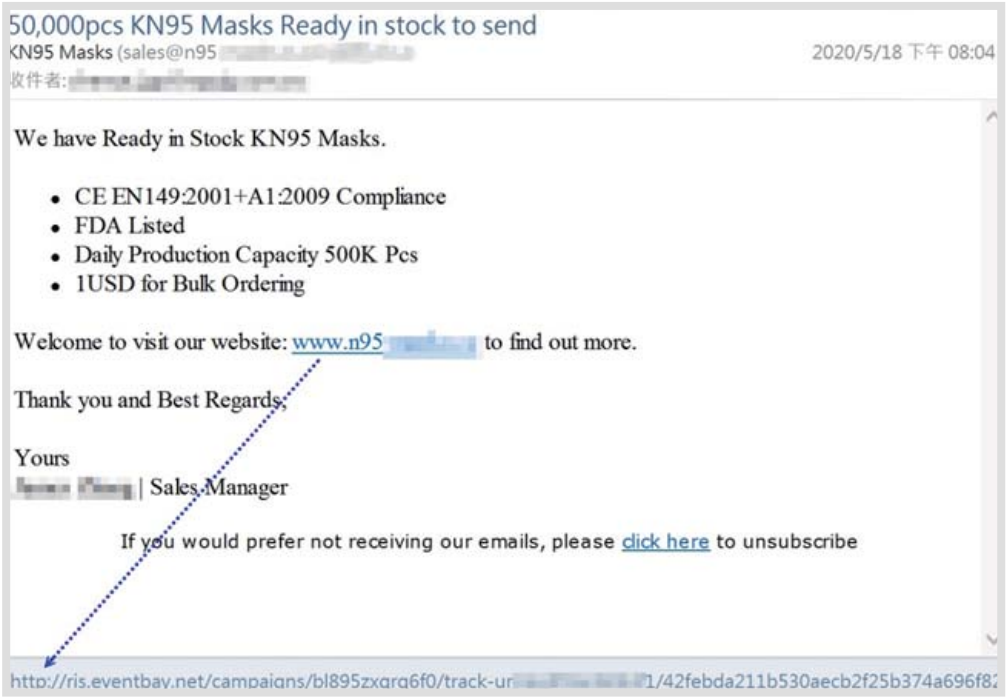
在第二季度，比较特别的是病毒邮件常用的压缩文件格式分别为 .ace 与 .rar，甚至比 Windows 内能解压缩的.zip压缩格式还要多。WinRAR 自 2015 年即对中国个人用户开放免费，许多中国的 PC 安装完成后也会安装免费的 WinRAR 作为预设的压缩或解压缩的工具；但是自 CVE-2018-20250、CVE-2018-20251、CVE-2018-20252、CVE-2018-20253 被揭露以来，常见的免费或可免费试用的解压缩软件诸如：WinRAR、7-Zip、Peazip 等，均已不再支持 .ace 的解压缩，.ace 的病毒附件会不会是刻意面向某些人群?值得玩味。



夹带 .ace 压缩文件的病毒邮件仍四处散播

来自新域名的邮件，假藉口罩售卖进行诈骗

全球第二季度仍在新冠肺炎的笼罩之中，许多地区对于口罩的供应还是匮乏，第二季度我们发现有许多口罩销售的电子邮件，指向一些新注册的域名。这些域名注册的时间都在半年内，甚至更短，并且在一段时间后就无法访问，极可能是诈骗。这类邮件较上一季度增长了约3.7倍，集中在六月。



口罩销售的电子邮件，指向一些新注册的域名

漏洞利用在四月达到高峰，受国家资助的 APT 族群利用疫情发动邮件攻击

附件使用已被揭露的 Office 漏洞的电子邮件攻击，在四月份达到高峰。

受到国家资助支持的 APT 族群，也在5月频繁地尝试以电子邮件发动攻击，且大多假藉疫情的议题发送公告通知、口罩相关信息，或伪冒 CDC 免费分发防疫物资，要求相关人员开启并填写附件调查表，藉以诱导收件者开启恶意附件！

总结

我们综合整理了第二季度恶意邮件社交工程特征，其中一大部分是促使人“发急”，例如：很急的订单、要求尽快回复或查看附件、电子邮件有状况将被停用、被入侵了等。因为很急，所以后续的作为就可能脱离原有的标准作业流程，加上远程办公的因素，再确认的工作可能因此变得难以落实，就很容易落入攻击者的陷阱。远程办公期间，别忘了“急事缓办，事缓则圆”，对于任何有疑虑的邮件都应当给予最小的信任，充分再确认才能免除后续网络安全危机。

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。