2020
第二季電子郵件安全趨勢

ASRC

Spam Mail
Virus Mail
Malicious Mail

August 2020 released.

2020年第二季，全球仍然籠罩在新冠肺炎的疫情中。疫情的嚴重及影響程度已遠超第一季。許多企業開始採取分梯次在家上班的模式，以確保公司人員的健康以及特定服務項目的正常運作。工作模式的改變加重了對網路的依賴程度，也因為人與人彼此見不到面，各種詐騙、資安破口就容易被攻擊者所利用。以下簡要分享ASRC研究中心(Asia Spam-message Research Center) 第二季郵件安全觀察概況。

偽造釣魚郵件相較上季增加，出現不少偽造企業管理者發送的釣魚郵件

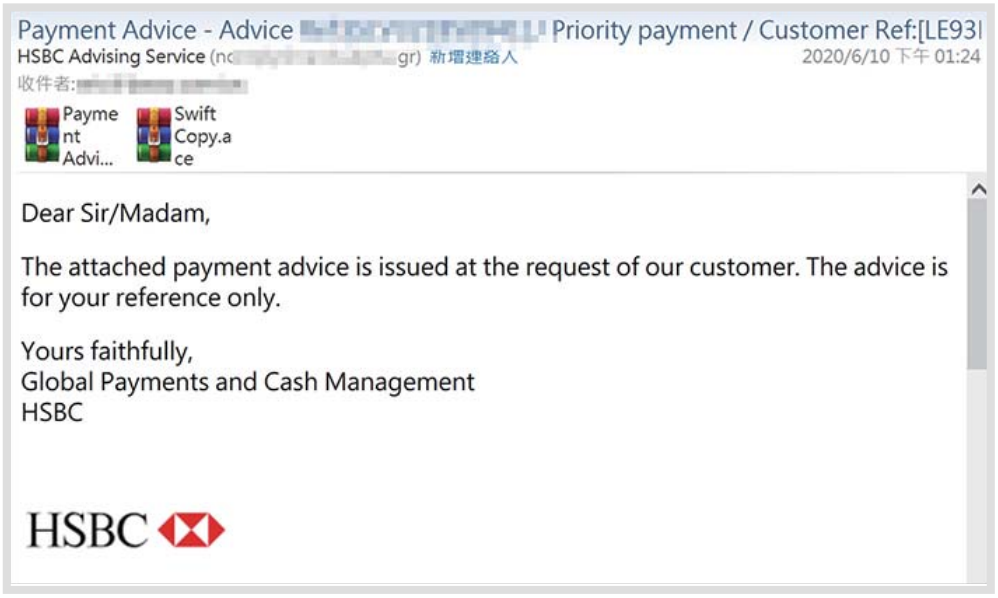
本季偽造企業組織通知、收貨確認通知...等釣魚郵件明顯增長，相較於上季大約成長了24%，並且集中在六月份。其中為數最多的是偽造企業管理者發送郵件帳號密碼相關問題的釣魚郵件，會在收信者點擊連結後導向釣魚頁面，這個釣魚頁面通常寄宿於被入侵的 WordPress 網站；其次為假的語音與檔案遞送通知，這些通知除了部分寄宿於被入侵的 WordPress 網站，部分則是使用免費的表單或網站生成器做為釣魚頁面，還有少量直接夾帶惡意附件檔案；最後是假的貨物運送或商業交易確認，部分寄宿於被入侵的 WordPress 網站、還有部分則直接將釣魚頁面的 HTML 放在附件檔內試圖避開瀏覽器對網址的警示與檢查，還有一部分則是直接夾帶以 RAR 壓縮後的惡意執行檔。

釣魚頁面通常寄宿於被入侵的 WordPress 網站

病毒郵件數量明顯增加，夾帶惡意映像檔或壓縮格式檔案居多

病毒郵件數量較上一季成長了約60%，同樣集中在六月份。以夾帶惡意 .img 檔為最大宗，佔了總量 1/3 以上。這些 .img 檔中包含了一個惡意 .exe 可執行檔案，在 Windows 環境下被雙擊後，會自動掛載成為一個虛擬光碟，便可讀取其中的 .exe 檔；此外，網路上也有人教學如何以7-Zip 解出映像檔內的內容，若收到此類惡意攻擊時缺乏資安意識，而以如何開啟該類檔案的目的在網路上尋找答案，也可能因此曝險！

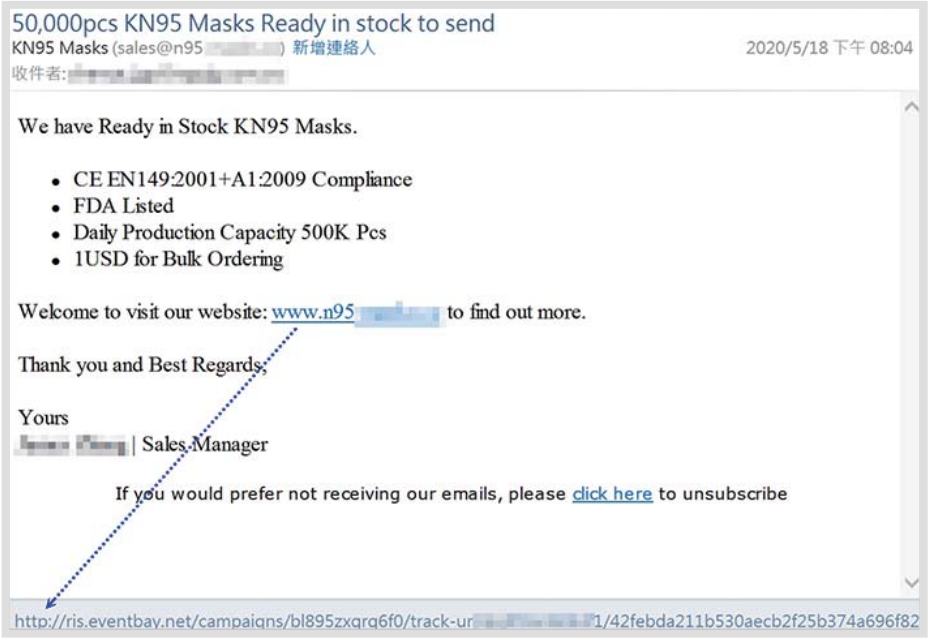
在第二季，比較特別的是病毒郵件較常用的壓縮檔格式分別為 .ace 與 .rar，甚至比 Windows 內建能解壓縮的.zip壓縮格式還要多。WinRAR 自 2015 年即對中國個人用戶開放免費，許多中國的 PC 安裝完成後也會安裝免費的 WinRAR 作為預設的壓縮或解壓縮的工具；但是自 CVE-2018-20250、CVE-2018-20251、CVE-2018-20252、CVE-2018-20253 被揭露以來，常見的免費或可免費試用的解壓縮軟體諸如：WinRAR、7-Zip、Peazip ...等，均已不再支援 .ace 的解壓縮，.ace 的病毒附件會不會是刻意面向某些族群？值得玩味。



夾帶 .ace 壓縮檔的病毒郵件仍四處散播

來自新域名的郵件，假藉口罩販售進行詐騙

全球第二季仍在新冠肺炎的籠罩之中，許多地區對於口罩的供應還是匱乏的，第二季我們發現有許多口罩銷售的電子郵件，指向一些新註冊的域名。這些域名被註冊的時間都在半年內，甚至更短，並且在一段時間後就無法拜訪，極可能是詐騙。這類郵件較上一季成長了約3.7倍，集中在六月份。



口罩銷售的電子郵件，指向一些新註冊的域名

漏洞利用在四月達到高峰，受國家資助的 APT 族群利用疫情發動郵件攻擊

附件使用已被揭露的 Office 漏洞的電子郵件攻擊，在四月份達到高峰。受到國家資助支持的 APT 族群，也在5月份頻繁地嘗試以電子郵件發動攻擊，且大多假藉疫情的議題寄發公告通知、口罩相關資訊，或偽冒 CDC 免費分發防護設備，要求相關人員開啟並填寫附件調查表格，藉以誘導收件者開啟惡意附件！

假防疫設備支援名義，試圖攻擊相關業者

總結

我們綜整了第二季惡意郵件社交工程特徵，其中一大部分是促使人「發急」，例如：很急的訂單、要求盡快回覆或查看附檔、電子信箱有狀況將被停用、被入侵了...等。因為很急，所以後續的作為就可能脫離原有的標準作業流程，加上遠距上班的因素，再確認的工作可能因此變得難以落實，就很容易落入攻擊者的陷阱。遠距上班的期間，別忘了「急事緩辦，事緩則圓」，對於任何有疑慮的來信都應當給予最小的信任，充分再確認才能免除後續資安危機。

關於ASRC 垃圾訊息研究中心

ASRC 垃圾訊息研究中心 (Asia Spam-message Research Center)，長期與中華數位科技合作，致力於全球垃圾郵件、惡意郵件、網路攻擊事件等相關研究事宜，並運用相關數據統計、調查、趨勢分析、學術研究、跨業交流、研討活動..等方式，促成產官學界共同致力於淨化網際網路之電子郵件使用環境。

更多資訊請參考 www.asrc-global.com

ASRC垃圾訊息研究中心