2020
第一季電子郵件安全趨勢

ASRC

Spam Mail
Virus Mail
Malicious Mail

Jun 2020 released.

2020年第一季過得十分不平靜，讓世界各國都繃緊神經的話題，莫過於防疫相關問題。不論是疫情的擴散速度、防疫保護的措施，抑或是物資採買、捐贈等都是被熱烈討論的話題。正當疫情蔓延時，出現許多詐騙郵件以提供防止被追蹤的比特幣錢包位址，假藉採買物資、幫助研究的名義募款行斂財之舉。這樣的捐款並不能真正幫助防疫的任何作為，反而飽了攻擊者的口袋。ASRC 研究中心 (Asia Spam-message Research Center) 在2020年第一季觀察到幾個值得注意的郵件安全議題：

遠端工作模式成為駭客攻擊目標，造就各種詐騙氾濫

2020第一季，全球在新冠肺炎影響下，保持「社交距離 (Social Distancing)」改變了人類生活接觸的方式。由於新冠肺炎的極高的傳染率，及對高齡、體弱、慢性病患者不可忽視的致死能力，許多企業為保住相關服務與業務能量，在可行的情況下紛紛採行在家上班的工作模式。這樣的工作模式帶來了下列的影響：

網路流量的需求
在短時間劇烈上升

遠端連線、遠距會議
VPN的需求大增

人們直接見面接觸的
情況大幅下降

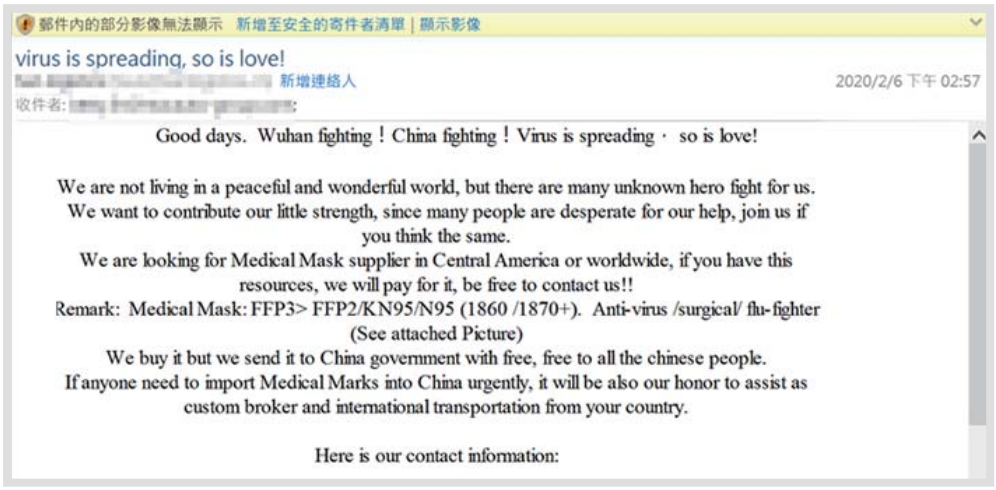
這些影響，可能會帶來針對遠端作業軟體的攻擊嘗試，以及各種詐騙的氾濫。

病毒郵件相較上季增加 340%、詐騙郵件爆增 400%

根據 ASRC 研究中心 (Asia Spam-message Research Center) 的觀察，第一季的整體郵件量微幅上升，尤其是新冠肺炎對全球影響最劇烈的三月份；病毒郵件量則明顯激增，相較於上一季，大約增加了340%，增加幅度最高也是在三月；詐騙郵件的數量在本季也較上季增加約400%。

藉名新冠肺炎的攻擊，目的以詐財或入侵企業為大宗

在疫情逐漸蔓延的第一季，許多攻擊也藉著疫情之名，試圖誘騙收件者開啟惡意攻擊郵件。這些假藉疫情之名的攻擊郵件，其主旨多半會帶上cdc、covid、corona、spread這些關鍵字眼。
以目的來說，數量最大宗的為詐騙郵件，多半假藉研究或衛生單位，以研究或幫助世界的名義，請求收件人捐錢；當然也有詐騙郵件誆稱可購買疫苗或篩檢試劑，一樣是以詐騙金錢為目的。


郵件內的部分影像無法顯示 新增至安全的寄件者清單 | 顯示影像

virus is spreading, so is love!

新增連絡人 2020/2/6 下午 02:57

收件者:

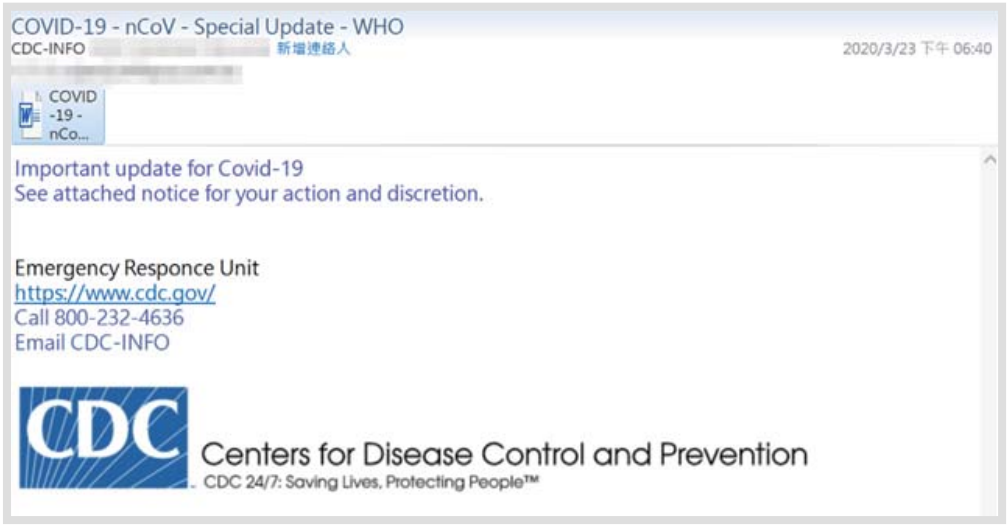
Good days. Wuhan fighting ! China fighting ! Virus is spreading， so is love!

We are not living in a peaceful and wonderful world, but there are many unknown hero fight for us.
We want to contribute our little strength, since many people are desperate for our help, join us if you think the same.
We are looking for Medical Mask supplier in Central America or worldwide, if you have this resources, we will pay for it, be free to contact us!!
Remark: Medical Mask: FFP3> FFP2/KN95/N95 (1860 /1870+). Anti-virus /surgical/ flu-fighter (See attached Picture)
We buy it but we send it to China government with free, free to all the chinese people.
If anyone need to import Medical Marks into China urgently, it will be also our honor to assist as custom broker and international transportation from your country.

Here is our contact information:

募款購買防疫物資的詐騙郵件

另一種目的則是試圖透過電子郵件嘗試入侵企業單位內部，以利進行後續的竊資、部署勒索軟體等目的。這類攻擊，多半直接寄送可利用Office漏洞的惡意文件，並以疫情相關主題誘騙收信人開啟，試圖藉此提高攻擊成功機率。經統計，此類型攻擊常用的漏洞編號為：CVE-2012-0158、CVE-2017-11882、CVE-2017-0199以及CVE-2017-8570。


COVID-19 - nCoV - Special Update - WHO

CDC-INFO 新增連絡人 2020/3/23 下午 06:40

COVID -19 - nCo...

Important update for Covid-19
See attached notice for your action and discretion.

Emergency Responce Unit
https://www.cdc.gov/
Call 800-232-4636
Email CDC-INFO

CDC Centers for Disease Control and Prevention
CDC 24/7: Saving Lives, Protecting People™

冒名CDC的通知，事實上為一可利用CVE-2017-11882漏洞的惡意文件

在 2020 年 3月，有大量以covid、corona相關的域名被註冊，這些域名被用於販賣新冠病毒保健品與檢測試劑，這些販售網站可能都是臨時設立，其販售物多半是不合法的贗品。其他無附件檔的惡意郵件多半都夾帶了一個以上的超連結用於釣魚，或是以超連結的方式，誘騙收件者下載遠端的惡意程式並執行。

偽裝的附檔以超連結的方式，誘騙收件者下載遠端的惡意程式並執行

為避免新冠肺炎群聚感染導致企業單位所可能出現的人力損失，遠距上班是普遍採取的應對措施。由於作業方式改變，彼此見不到面、資訊傳遞的塞車、中間人的竊聽，就可能出現冒名的號令 (假冒老闆要求通訊錄、匯款、合約、訂單...)；攻擊者也利用此波疫情，搭配社交工程攻擊的手法，進行財務相關的詐騙或入侵攻擊，比方：Emotet銀行木馬...等。新冠肺炎對於全球來說，可說是如黑天鵝般，大家未能預期它的出現，也不相信他的感染範圍可與1918年西班牙流感匹敵，但新冠肺炎的嚴重性，從大家的懷疑慢慢地變成了現實。資訊安全呢？我們可以看見資訊安全所帶來的可能性衝擊，它就如同灰犀牛般，若我們忽視，則可能隨時遭到猝不及防的攻勢或損失！

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