2020
電子郵件安全趨勢回顧

ASRC

Spam Mail
Virus Mail
Malicious Mail

January 2021 released.

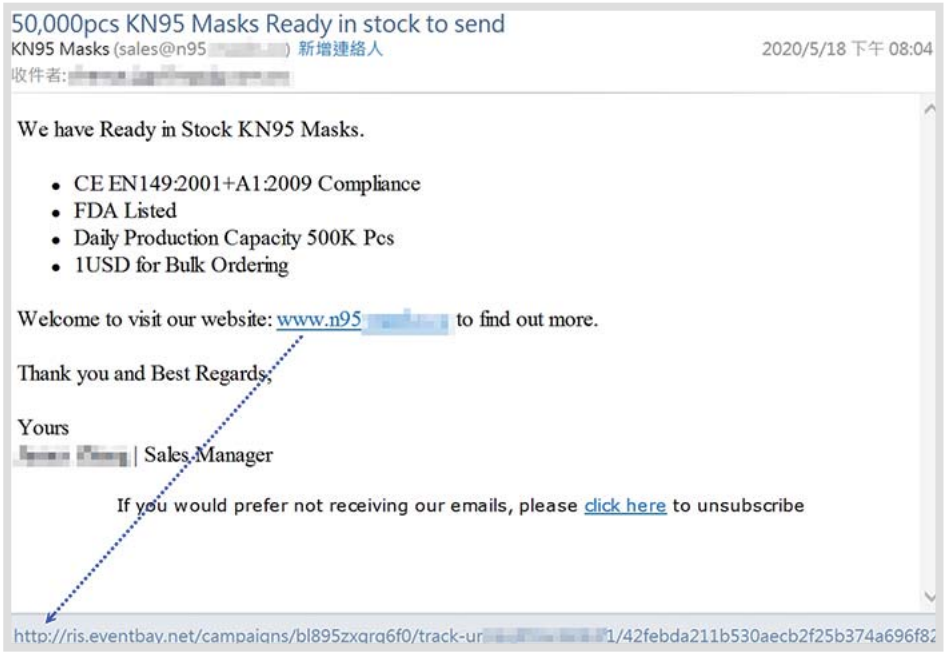
2020年幾乎全年都受到COVID-19疫情影響。疫情的出現改變了全球數位工作模式，為了降低疫情對工作人力的衝擊，遠距工作或在家學習成了重要選項，很可能也將成為今後的常態。

遠距工作挑戰了傳統的資安部署觀念，遠端存取不再有「可信任的區塊或空間場域」，因此，所有服務的存取都需要驗證迫使了零信任的架構要提早被實現。遠距工作也推動了雲端應用的加速，雲端服務商算是疫情下少數的受惠者；但雲端服務設定不當造成資料大批洩漏的情況，算是容易被忽視的資安弱點。此外，不論是安全人員或是攻擊者，面對遠距工作直覺可聯想到的資安問題，就是 VPN 連線的安全性保護及 DDoS 攻擊或任何可能阻斷服務取得的手段，這類攻擊在 2020 年算是最容易被觀察到的事件了。

2020 年郵件安全有哪些明顯的趨勢呢？

詐騙郵件

受到疫情的影響，在郵件安全方面防疫物資的詐騙經常出現。這些防疫物資的銷售廣告來自不明的公司與新註冊的域名，且出現的頻率與疫情的嚴重程度、防疫物資的匱乏程度有關係。2020年的第一季與第二季較常看到此類詐騙；第四季後就相對少了許多。

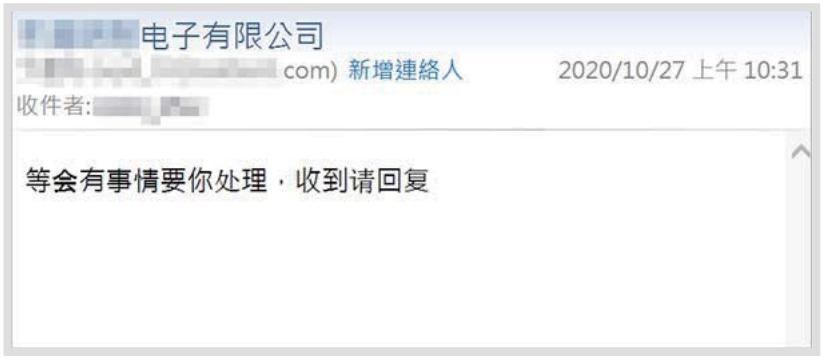


為了口罩銷售而指向一些新註冊的域名

除了與疫情有關的詐騙郵件外，還有內容以恫嚇收件人電腦遭到入侵與監控的比特幣詐騙郵件。詐騙的內容其實是杜撰的，但這樣的詐騙郵件內容依發送的地區與國別，融合了多國的在地化語言，以提高詐騙成功的機率。

攻擊目標為中國，則以簡體字為內容

有些詐騙並非以直接騙取金錢為目的，而是騙取企業內部的資訊，再作後續利用。這樣的詐騙在2020年居家辦公，不便直接確認的情況下，特別容易奏效。



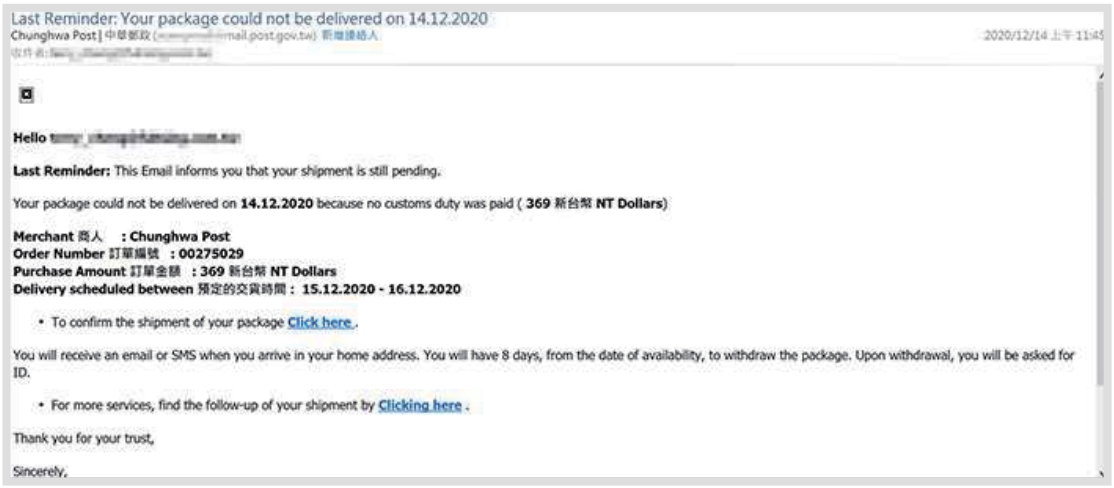
冒充企業高層，向員工索討企業內部資訊，或冒名令其執行不該執行的事務

釣魚郵件

2020年最大宗的攻擊，非釣魚郵件莫屬了。通常釣魚的目標，是希望能釣取企業服務的各種憑證，尤其在遠距工作的情況下，若能釣到一組企業電子郵件的帳號密碼，很可能就能遠距取用企業的所有服務！

意圖騙取郵件帳號密碼的釣魚郵件

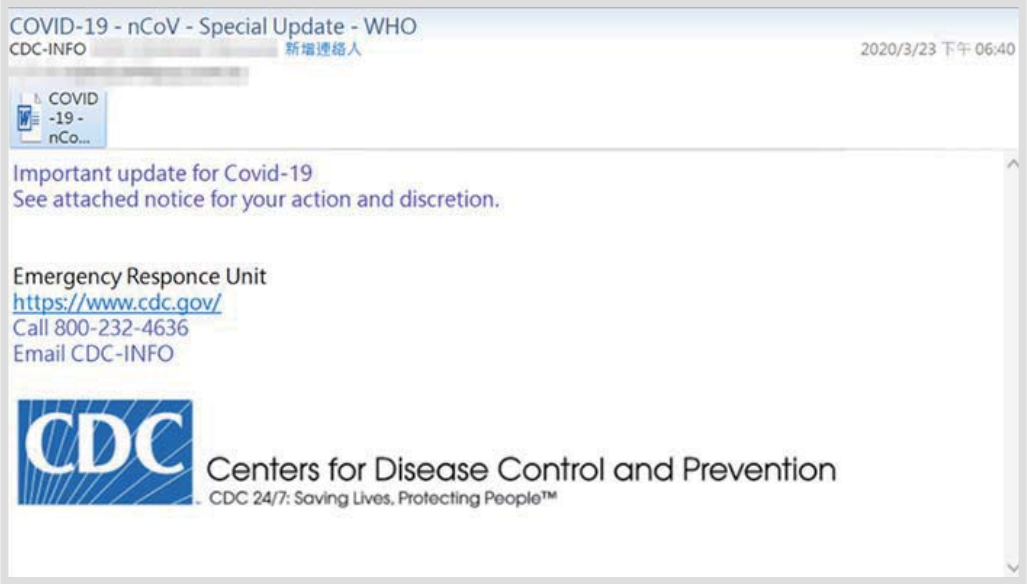
在2020年第四季，我們也觀察到了聲稱未付稅金導致郵件包裹延遲的釣魚郵件。這種釣魚郵件的目的是藉由假的刷卡付稅，釣取信用卡資訊。在受疫情影響仰賴物流的情況之下，這種釣魚郵件將使受害者更容易上勾！



藉由假的刷卡付稅，釣取信用卡的刷卡資訊

漏洞利用

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、CVE-2017-8570以及CVE-2018-0802。



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

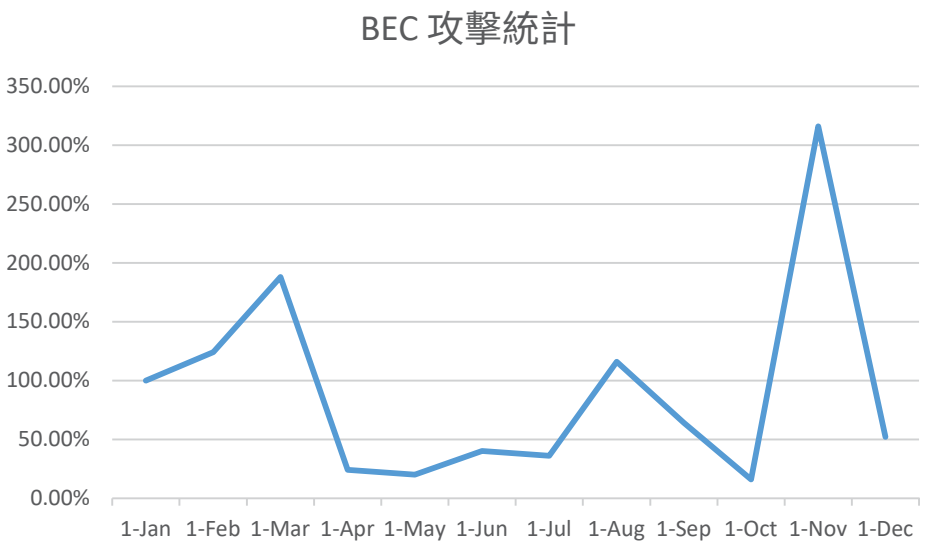
針對性攻擊

在2020年我們也觀察到了多起與疫情有關的針對性攻擊，與國家資助有關的APT族群嘗試以電子郵件攻擊則在五月份最為頻繁，其中有許多與疫情資訊、設備發放、公告通知或口罩相關資訊有關。

假防疫設備支援名義，試圖攻擊相關業者

搭配當時發生的時事，對特定單位發動的針對性攻擊

此外，BEC 攻擊事件以一月份為基準做為比對的話，在 2020 年 11 月份達到全年最高峰，這些 BEC 攻擊郵件中都存在著被攻擊對象才能知道的機敏資訊。



結論

2021 年仍無法明確預測何時可以完全擺脫疫情，而許多企業已將遠距工作視為未來可能的常態。遠距工作為資安帶來了新的挑戰，在家辦公的電腦及所使用的網路也難以確保安全性，因此具備合理存取權限的零信任的架構勢必是未來趨勢。由於遠距工作的關係，非即時同步確認事項的聯繫，多半倚賴電子郵件或其他傳訊軟體，各種詐騙事件將層出不窮。除了應避免公司資料外洩外，重要事項的聯絡，最好能設立第二通訊管道作確認；而重大決策也必須落實複核機制，才能避免 BEC 事件的發生。

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