2020
第三季電子郵件安全趨勢

ASRC

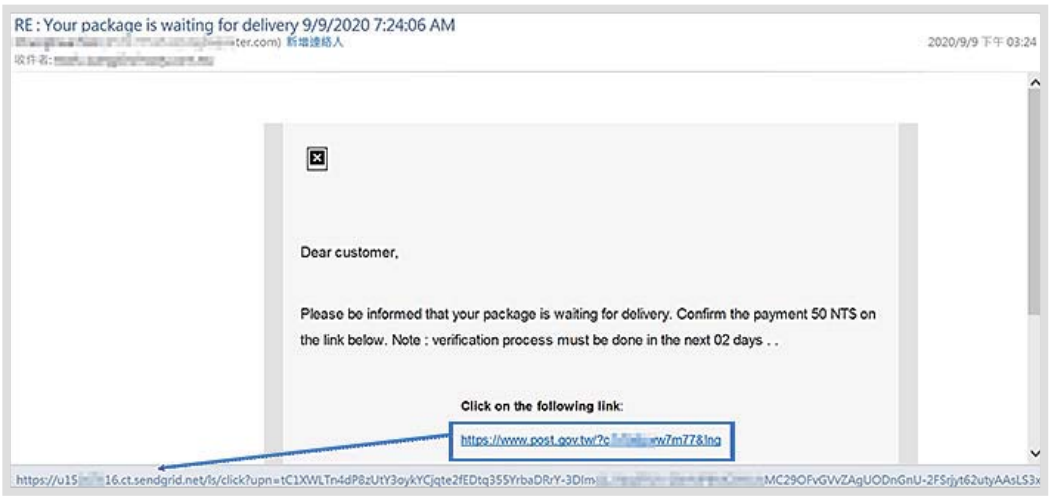
Spam Mail
Virus Mail
Malicious Mail

November 2020 released.

COVID-19對全球的影響橫跨了三季，上半年期盼完全解除在家工作的情況，在第三季仍無法得到完全實現，部分公司更保守預估這樣的情況可能會延續至明年的第一季，甚至更長的時間。而在電子郵件安全方面，第三季整體的郵件攻擊數量，相較於第二季稍有趨緩，但帶有惡意檔案的郵件則較上一季增加了約40%。本季明顯的電子郵件安全趨勢，多為合法服務遭到濫用，以下我們分別就幾個較值得注意的濫用趨勢分別說明。

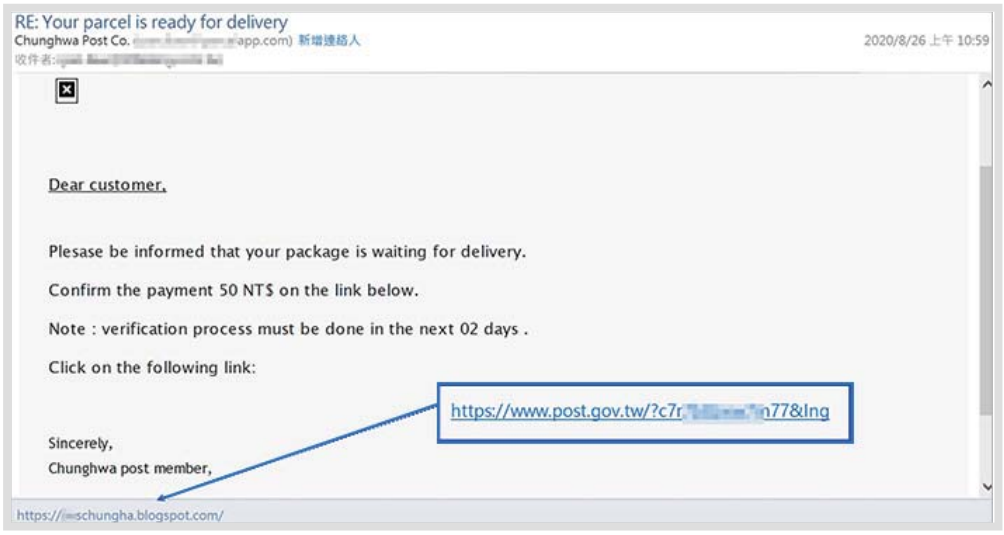
濫用公用服務的釣魚郵件

第三季最明顯的攻擊是濫用公用服務的釣魚郵件，其中數量最大的一波出現在8月份，來自SendGrid的釣魚郵件。SendGrid是一家位於科羅拉多州丹佛市的客戶交流平台，其服務包括了用於交易和營銷電子郵件。來自SendGrid的釣魚郵件可能與SendGrid在8月份發現的大批帳號密碼遭到破解，並且破解的帳號密碼被用以濫發垃圾與釣魚郵件的事件有關係。這批郵件發送自SendGrid的合法郵件伺服器，並且惡意頁面也寄宿在SendGrid所提供的網頁服務上。



SendGrid服務被濫用於偽冒中華郵政進行釣魚

Google所提供的網誌服務也遭到濫用。網誌服務被用來發佈騙取帳號密碼的釣魚頁面。值得注意的是，遭到偽冒的對象，皆為台灣的中華郵政。



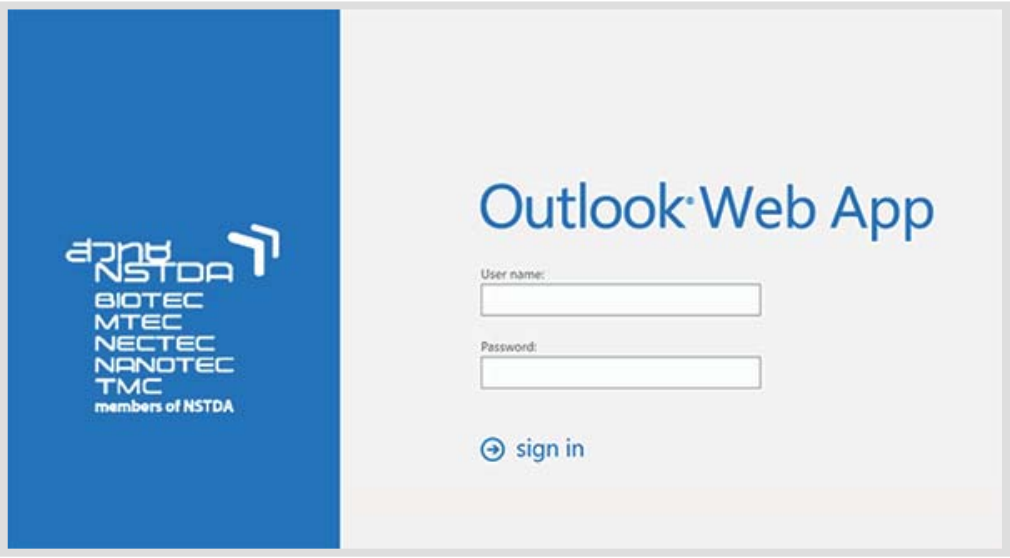
Google 網誌服務被濫用於偽冒中華郵政進行釣魚

網際網路檔案館 (archive.org) 快照存放釣魚頁面

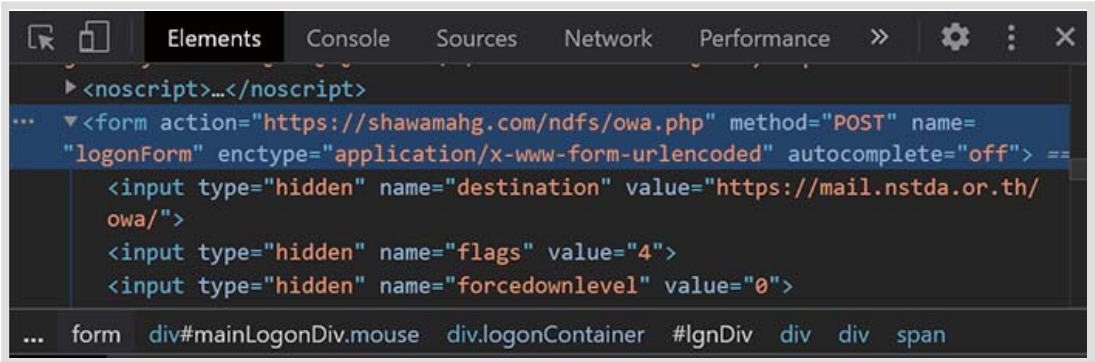
我們也發現網際網路檔案館 (archive.org) 的網頁快照服務遭到釣魚攻擊的濫用。這並不是過去的釣魚頁面被快照服務無意的保存下來，而是攻擊者蓄意利用快照服務的功能，先讓釣魚頁面存在於快照服務中；之後發送釣魚郵件，直接將釣魚頁面指向快照服務的特定頁面。

釣魚郵件，直接將釣魚頁面指向快照服務的特定頁面

這個攻擊希望騙取的標的是Outlook服務的帳號密碼。網際網路檔案館快照服務被濫用於提供一個惡意頁面存放的空間；而盜取帳號密碼的網頁端程式，則是在另一個地方。如此一來，瀏覽器及上網安全的保護措施，或許無法在拜訪惡意頁面時，直接警示所拜訪的網站為惡意來源，因為網際網路檔案館快照服務是一個知名的功用服務。



當拜訪這個頁面時，會發現這個釣魚頁面試圖騙取Outlook服務的帳號密碼



填入帳號密碼按下sign in後，帳號密碼即遭到盜取

恐嚇郵件詐騙比特幣

在9月初，突然出現大量的比特幣詐騙，其內容為恐嚇收件人電腦遭到入侵與監控，並威脅若不遵照指示匯入比特幣至對應的錢包，私密的影音照片將被公開外流。這個恐嚇詐騙聲稱的內容其實是杜撰的，但這個詐騙內容以各種語言分別分送給許多不同國家地區的人。

攻擊對象為中國，內容以簡體中文撰寫

攻擊對象為日本，內容以日文撰寫

這個類型的詐騙郵件，本身並不帶有任何惡意檔案或超連結，純粹只是以內容來讓受害人心生害怕進而匯比特幣到指定的帳戶，發送來源也十分多元，甚至利用了Gmail服務，來躲避來源偵測或信譽評價。

總結

詐騙、釣魚以及各種社交工程的手法，作為入侵、獲取利益的手段越來越普遍，雖然其中的技術含量低，但防不勝防，對於攻擊者而言，是一個獲取利益的便利手段。事實上，要以人工的方式辨識一個郵件內或網頁中存在的異常，本來就是件十分困難的事；若是這些異常點，全都被遭到濫用的「正常」服務所取代，那識別起來就更加的困難了。

因此，我們建議，人員可提防的部分，應該著眼在當悖離標準作業規範、約定的作業方式以及自身角色應接觸的事務時，採取更高的警戒或查證的工作；其他部分，則應採取更安全的資安措施或設備做為輔助才能事半功倍。

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