2019
全球郵件安全趨勢回顧

ASRC

Spam Mail
Virus Mail
Malicious Mail

Feb 2020 released.

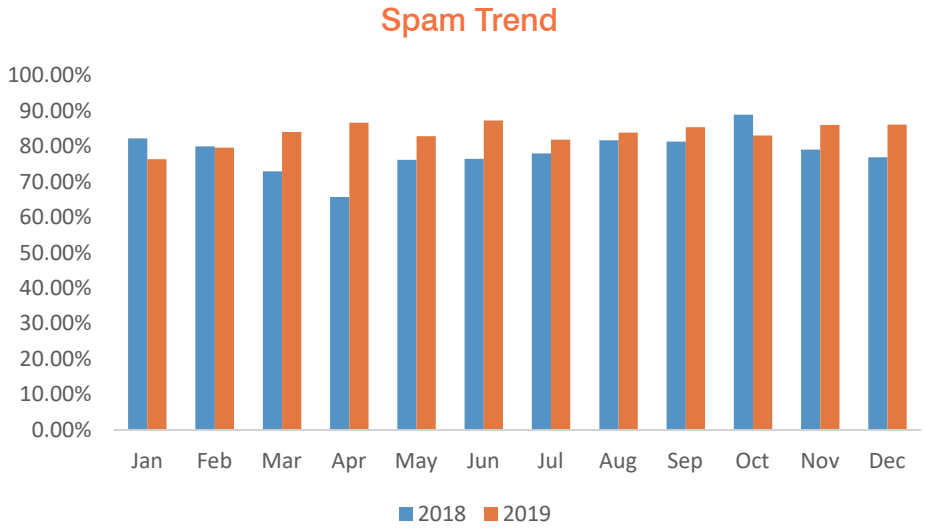
概觀

根據ASRC 研究中心 (Asia Spam-message Research Center) 與中華數位科技的觀察，2019 年整體來說，垃圾郵件與病毒郵件的數量呈現均勻分布，沒有哪個月份特別爆量，但是相較於2018年，數量稍有成長。郵件量爆發、詐騙郵件與釣魚攻擊在2019年第四季達到全年高峰；BEC詐騙郵件的數量雖然降低，但是BEC事件並未因此緩和。CVE-2014-4114、CVE-2018-0802、CVE-2017-11882這三個 Microsoft Office 文件漏洞利用全年可見；2019 年第一季被揭露的 WinRAR 漏洞 (包含CVE-2018-20250、CVE-2018-20251、CVE-2018-20252與CVE-2018-20253)，皆被用於APT攻擊或是滲透測試、紅隊演練。

統計

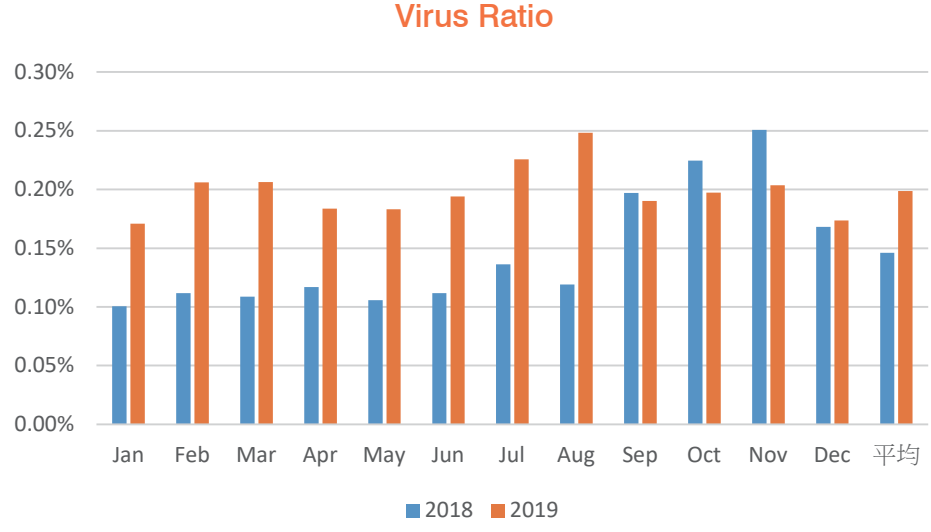
垃圾郵件佔比趨勢統計

2019年垃圾郵件平均約佔總體郵件的83.67%，相較於2018年的佔比增加了6%左右；2019年每個月的垃圾郵件佔比幾乎都在80%以上，月份之間的波動很平均，且多數月份垃圾郵件佔比都較 2018 年來得高。



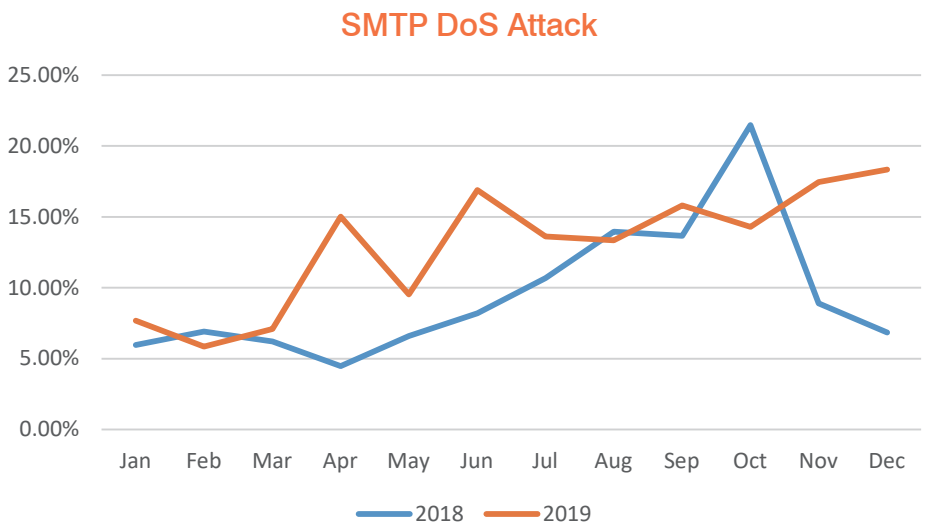
垃圾郵件中的病毒郵件

垃圾郵件中，一般病毒的佔比大約在0.1~0.2%之間。2018年第四季的波動幅度較大，2019年平均佔比都維持在0.15%之上。



SMTP DoS攻擊

同一個IP集中發送大量郵件，並可能造成SMTP服務阻塞或中斷的攻擊，多半發生在第四季，可能因為第四季為消費旺季，雙11、雙12、聖誕節與跨年接踵而來，搭配 EDM 與 Phishing 一起出現。但是2019年除了第四季外，在四月份及六月份類型的攻擊也都有明顯上升的跡象。



郵件附檔類型

電子郵件中，常用的附件類型，可能被用以攻擊的機率大概有多少呢？我們統計了2018、2019年的數據，最常用來攻擊的常用作業文件檔為Word檔(註：凡含有不當目的的Word檔皆從嚴認定)，其次為Excel檔；多數作業系統都可以直接支援ZIP解壓縮，因此ZIP壓縮格式較常被用來夾帶惡意檔案。

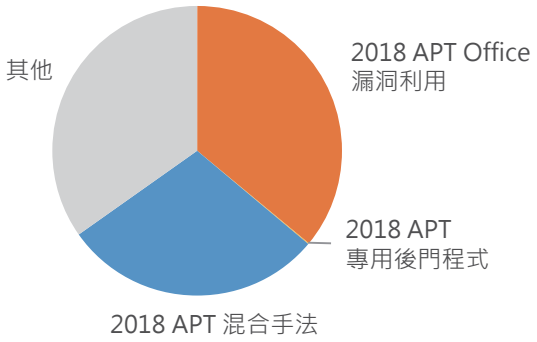
	2018	2019
文書作業類型		
Word	28.65%	24.90%
Excel	5.86%	3.33%
PDF	2.69%	3.12%
PowerPoint	0.82%	1.40%
壓縮檔類型		
ZIP	14.03%	9.98%
RAR	4.99%	9.51%

APT 攻擊郵件

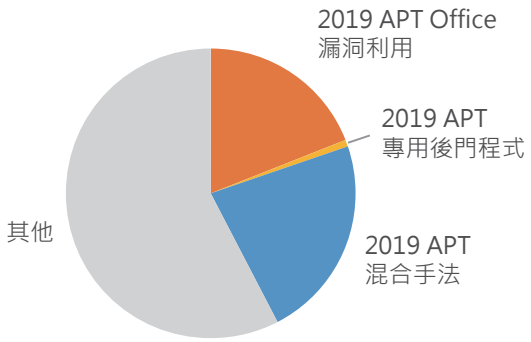
2018年APT攻擊郵件最常見的是Office漏洞利用的手法，較常被利用的漏洞編號分別是OLE漏洞(CVE-2014-4114)與方程式漏洞 (CVE-2017-11882)。

2019年APT攻擊郵件最常見利用的Office漏洞編號為CVE-2014-4114、CVE-2018-0802、CVE-2017-11882，大致上承繼了2018年的利用情況。

2018



2019

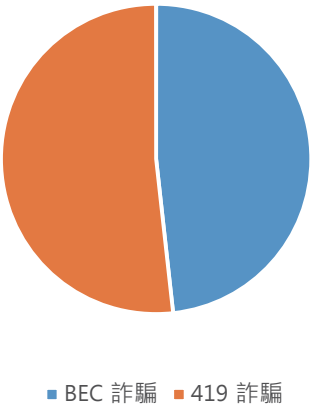


詐騙郵件

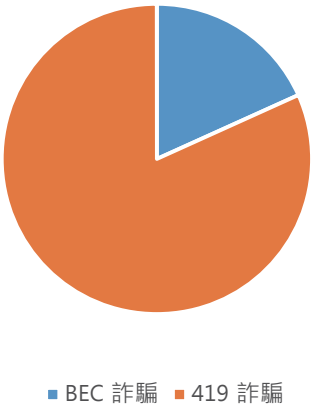
2018年的BEC與419詐騙佔比大約各占一半。2019年BEC與419詐騙佔比發生了不一樣的變化，BEC詐騙與419 詐騙郵件總量相較2018年的總量下降；雖然BEC詐騙郵件下降的幅度高於419詐騙，並不表示BEC詐騙的風險跟著下降了。

相反的，BEC詐騙郵件顯得更有策略性，不會過早介入商談中的交易，也減少接觸不必要收到BEC郵件的人員，大幅提高BEC詐騙的成功機率。

2018



2019



重要趨勢

信任來源飽受挑戰

電子郵件的可信度，在近年來不停的受挑戰，尤其 BEC 事件頻傳的情況下，對於郵件中提及異常的變更事項，都需要特別留意，尤其是匯款帳號的變更，一定要透過電子郵件以外的管道再次進行確認。

其次需要特別注意的是在電子郵件內的超連結。並不是超連結帶有可信賴的網域名稱，就表示這樣的超連結不帶有威脅！也不是所有惡意的超連結都必然會下載惡意程式，或需要被攻擊者配合輸入帳號密碼相關資料，畢竟，並非所有人使用網路服務都會隨手登出。在 2017 年開始出現釣魚郵件結合 Google OAuth，就是企圖矇騙收信人透過點擊一個共享文件的連結，授與攻擊者存取Google App的權限，如今類似的手法也開始出現在Office 365。

最後，白名單一定要慎用，看似來自熟知的同事、供應商的郵件，也有可能隱藏惡意攻擊！

供應鏈攻擊是國家級資助的APT攻擊常用的手段。攻擊者的主要目標可能具備了很高的警戒意識與防護能力，因此攻擊者可從主要目標的合作對象下手，之後再透過主要目標對合作對象的信任，直接穿過各種防護措施進行攻擊。

合法域名空間遭到濫用的實例

釣魚郵件與詐騙郵件氾濫

2019年電子郵件中，帶有惡意連結的數量，大約是2018年的2.8倍。釣魚郵件為了取信收件者點擊，多半會使用一些在地化用語及社交工程的手法。由於釣魚郵件主要目的是騙取網路服務的帳號密碼或其他機敏資料，因此多半在點擊之後，會透過瀏覽器連往一個收集這些機敏資料的釣魚網站或釣魚表單，再誘騙受害者輸入其機敏資料。

瀏覽器的開發商也注意到類似的問題，於是紛紛在網址列加入了檢查與提醒的功能，希望能藉此保護使用者。

然而攻擊者也開始改變做法，在電子郵件中直接夾入一個惡意的靜態 HTML 頁面，誘騙收信人填入機敏資料，但是這個頁面透過瀏覽器打開時，網址列顯示的是本地端的儲存位址而非遠端的釣魚網站。當收信人填完資料按下送出後，瀏覽器即以POST搭配加密連線的方式，將機敏資料送往釣魚網站，這樣的釣魚手段能略過多數的瀏覽器保護措施。這類型的攻擊郵件，在2019年第四季大量出現。

惡意的靜態HTML釣魚檔案

Office 文件漏洞充滿威脅

經典穩定的Office文件檔漏洞，一直是攻擊者愛用的武器之一。除了作業人員、防毒軟體對文件型檔案的警覺性較低外，許多人所使用的Office不會經常性的更新。除了公司編列預算的問題外，原本就使用了非正版Windows，或擔心相容性、使用上的適應性，以及缺乏漏洞修補的概念，都是使用者不願更新的原因。

根據ASRC的統計，2018年最常見的郵件漏洞利用攻擊為OLE漏洞(CVE-2014-4114)與方程式漏洞(CVE-2017-11882)。

2019年，CVE-2014-4114仍持續被利用，且在第三季爆發相當大量的攻擊樣本，主要目標產業為電子、食品、醫療相關產業；CVE-2018-0802則做為CVE-2017-11882其後續的衍生變形攻擊持續存在。2020年初甫被披露的CVE-2020-0674及其後續影響力，我們也將持續關注。

結論

2020年會是5G基礎建設部署、成熟加速的一年，隨著整體網速的加快，行動應用服務將更趨複雜化，因此，個人資訊遭到刺探、洩資的速度與規模、攻擊的速度及頻率，都會跟著大幅的提高；而惡意程式也可以不必再拘泥檔案大小的限制，更可朝向功能完備的方向作發展；加上量子電腦、雲端運算的推波助瀾，資安事故的發生與危害程度可能是過去難以想像的。電子郵件仍會是網路攻擊重要的入侵管道，單純的帳號密碼防護力漸趨薄弱，多因素驗證已是勢在必行。

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