風起「雲」湧

如何因應數位化的挑戰與驟增的資安事件

資策會 資安所鑄造廠⊙朱宇豐
資策會 資安所鑄造廠⊙竇瑋甄

數位化與資訊化的普及提高了資安威脅。資訊系統漏洞、風險往往會在運作中的設備發生，且系統設定不當也會造成資安風險。2021年4月臺灣疫情再度爆發，原有的生活方式發生改變，包含遠距辦公、遠距上課、遠距會議…等。然而攻擊事件的發生跟生活模式環環相扣，人們依賴數位化生活越高，資訊安全就顯得更為重要。

疫情驅動的資安風險

疫情使人與人的接觸產生距離，網路卻使我們更加靠近。遠距工作、線上購物以及宅娛樂確也為網路攻擊提供了更迅速的管道，衍生相當多資安問題。以金融業來說，因應疫情關係很多銀行等金融單位啟動遠距上班，大幅增加未授權存取及外部入侵的資安風險。近年來，金融業積極推動數位轉型，提供客戶更多的遠端服務，使企業面臨更多的資安威脅。[4]網路資安領導廠商Fortinet® 2020年10月發布《2020年遠距工作網路資安報告》（2020 Remote Workforce Cybersecurity Report），其報告指出，全球有超過 8 成的企業面臨推行遠距工作的挑戰，尤其在於確保網路的安全連接、業務連續性等層面。83% 企業指出在緊急推行遠距工作上，一定程度上遇到挑戰，而最大挑戰便是確保網路的安全連接、業務連續性及關鍵業務應用程式的存取。令人不得不注意的是，60% 的企業表示在轉移至遠距工作的過程中，發現針對安全漏洞的嘗試攻擊活動有所增加。

當企業員工的工作模式改變、與顧客的互動數位化，各產業面臨邊界愈來越模糊的議題，資安人員的防守線如修築長城，需建置最長最堅固的防衛，因資安威脅與攻擊將永遠存在。其中又可將疫情下的資安議題分為遠距工作、雲端安全、醫療資安三個面向探討。

一、遠距工作：遠距上班、爆量的網購訴說疫情下我們的生活，也掀起駭客新浪潮。遠距工作的模式出現更多的Business Email Compromise（BEC）商務電子郵件詐騙事件，駭客藉由惡意軟

體或網路釣魚入侵公司高階主管或委外廠商的郵件帳號，企圖誘使企業員工或投資者匯款。另外，疫情促成了另類的混合辦公型態，駭客利用家庭網路漏洞，利用VPN竊取企業機密資料，成為了資安漏洞。

二、數位雲端安全：疫情加速了企業推動數位轉型，相當多企業開始將基礎建設與資料移至雲端使用，依賴雲端進行資料的儲存與串聯處理。然而，地端防護機制無法滿足雲端控管，不正確的雲端設定引起資料外洩的情況常有耳聞，其風險多半來自用戶自身的操作不當，而被入侵者取得內部系統應用程式開發介面，而這也意味者駭客將輕易入侵企業。

三、醫療資安：國際網路資安大廠Check Point Software（NASDAQ：CHKP）最新研究指出，自2020年11月初起，全球鎖定醫療機構的攻擊遽增45%。2021年5月，愛爾蘭衛生健康署（Health Service Executive, HSE）宣布，由於遭受駭客綁架軟體攻擊，他們為預防國民資料受害，緊急關閉了所有的資訊系統，並且與資安團隊着手對應辦法。駭客的攻擊手法多樣，包括勒索軟體、僵屍病毒、木馬程式和 DDoS 攻擊等，其中，又以勒索軟體在醫療領域的增長幅度最大，也更具破壞性。在持續延燒的疫情下，醫院承受巨大的救援壓力，往往更願意直接支付贖金來換取醫療服務環境保障，這使網路駭客獲取大量利益外，也變得更加猖狂。

在COVID-19席捲全球的這兩年，打著疫情、COVID-19、快篩、分流上班旗號的釣魚郵件、勒索軟體、惡意網站、假新聞也隨之暴增。今年4月、5月短短兩個月的時間，宏碁、日月光、廣達等大廠接連傳出遭駭消息，被勒索高額贖金。廣達遭駭客團體REvil要求支付贖金5千萬美元，廣達雖營運未受影響，並採取緊急應變措施對公司整體提升網路安全等級，相似的資安事件發生卻影響其客戶與委託廠商的對其資安信任度。

自2019年末開始，國內外有相當多企業頻傳嚴重的資安事件，如圖1所示，特別令人髮指連醫療體系都成為了駭客攻擊的首要目標，對於防疫行動雪上加霜。回顧臺灣2020年重大資安事件，5月中油、台塑等兩大石化公司受到勒索軟體攻擊；台灣國際航電（Garmin）遭勒索病毒入侵，線上服務被迫中斷。2020下半年，工業電腦大廠研華科技（Advantech）公司部分伺服器傳出遭到攻擊，而鴻海墨西哥廠也在12月驚傳遭勒索病毒入侵。事實上除了製造業，2020年新冠病毒肆虐全球，醫療體系卻接連遭到駭客攻擊，對於防疫行動雪上加霜。受到攻擊後，相關篩檢作業被迫延後，嚴重時，更是可能導致網路系統癱瘓，錯過急症患者的黃金救援時間。

「前事不忘，後事之師」，2020年至今發生的資安事件，在今年也繼續發生著，警惕著企業在資安防護上不得鬆懈，相關的預防措施與漏洞修補，都需踏實落實。

圖 1、疫情下資安事件　　圖片來源：本文章自行整理

企業網路邊界破壞之下資安技術探勘

疫情之下，遠距辦公打破原有疆界的企業網路環境。在疫情下的資安事件議題中，最被關注領域為，醫療、威脅式勒索軟體。因此，資安大廠開始推出一系列針對勒索軟體的解決方案，包含 Trend Micro、CISCO、FIREEYE…等。

Sophoslabs研究報告提出10個不同類型的勒索軟體[1]，分別為：WANNACRY、GANDCRAB、SAMSAM、DHARMA、BITPAYMER、RYUK、LOCKERGOGA、MEGACORTEX、ROBBINHOOD、SODINOKIBI。其中，最常見入侵接觸的方法為利用社交工程(Social Engineering)，透過電子信箱的方式，誘使開啟信箱點擊連結。其擴散感染方法大致可分為：加密蠕蟲（Cryptoworm）、勒索軟體即服務（RaaS）和自動主動攻擊。

- 加密蠕蟲（Cryptoworm）：為一種獨立的勒索軟體，將自行複製並感染於其他可執行的設備上，達到最大擴散。此種行為若僅利用防火牆或是端點設備將很難偵測到。
- 勒索軟體即服務（RaaS）：利用網路平台或是信箱傳送，偽裝成常見之軟體，降低受害者心防並點擊安裝，也是常見的攻擊手法，近期的 Microsoft Exchange 漏洞就為類似手法，漏洞為（CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 and CVE-2021-27065）。
- 主動式自動攻擊：此方法針對系統弱點，利用掃描後得到的資訊延伸分析，或初階判斷取得可進入點。

有趣的是，勒索軟體的生態好比一場商業行為，如圖2為例，經常為組織型態，首先會

有開發型駭客角色，此類型駭客主要是製作惡意攻擊腳本，並且大部分腳本類型為已知攻擊（舊手法），接下來由整合型駭客進行包裝成可執行的應用程式，並交由攻擊型駭客引誘受害者執行，受害者點擊後，會發送訊息向攻擊型駭客回報受害者狀態。在受害者取得款項交付的方式，金流管理駭客在收到款項後，對每個角色的駭客進行分潤。

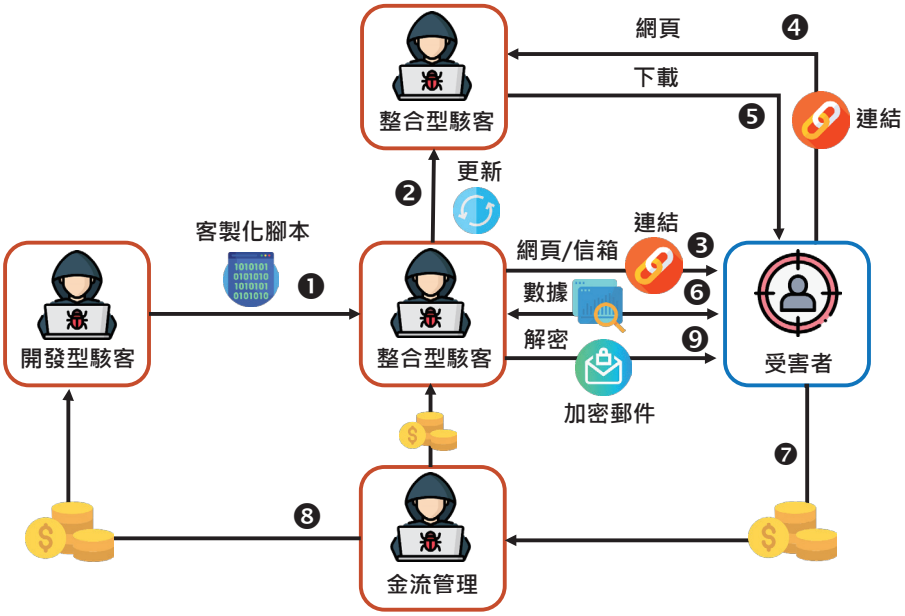

圖 2、勒索軟體生態系　　圖片來源：How Ransomware Attacks[1]

防範方法&結論

疫情加速數位化浪潮，不可否認，數位化的擴展與資安趨勢有正面成長關係[3]。[2]IBA對疫情底下可注意的安全方式分為個人、系統/雲端和移動設備。個人面向中資訊設備須隨時保持更新，包含防毒軟體，針對已知的風險抵制；遠距工作在網路連線安全也不可忽視，連線回公司可利用VPN加密通道方式，減少使用來路不明的WIFI，避免中間人攻擊竊聽中間傳輸資料，造成資料外洩；在家工作的過程中，員工將敏感資料各自保存，因此需更加注意瀏覽網頁安全，以免惡意人士透過網站瀏覽器做為入侵途徑，呼籲員工在家遠距上班，來路不明網頁千萬不要點擊，若遇到可疑的網站連結，可先至與Virustotal相似的網頁進行安全確認（https://www.virustotal.com/）。

此外，網路上免費的信箱服務許多，建議減少註冊來路不明的信箱帳號，以免變成駭客跳板主機。並在系統/雲端中建置資料備援機制與快速恢復機制，若主機還置放於無

人看管的公司，硬體安全恐有缺口，備援機制和快速復原機制不可缺少，須隨時準備快速復原規劃。更進一步來看，系統/雲端服務的傳輸過程，需透過資料加密與傳輸加密，提升雲端存取安全。人員方面，系統管理員要對敏感資料更加嚴謹和建置可隨時銷毀的機制。雲端設備/儲存體服務選擇可信賴的大廠，因大廠為了讓各企業資安合規都會導入ISO，管理上會比較嚴謹可減少風險發生。在系統管理上，連線管理可利用黑白名單，強化存取的安全。國內自主研發單位資策會資安所也推出資安快篩服務，在疫情之下多一個保障（https://esm.secbuzzer.co/）。

多數企業措手不及因應疫情浪潮下的資安風險[5]，本文在此建議四個層面的防護建議：

一、標示重要資產做首要保護與緊急修復，減少重災發生；

二、防範隔離不可少，降低遠端連線造成內部系統感染；

三、防範未然，購買時選用合適的資安防護設備；

四、以「人」為本，提升員工資安意識。

資安防護有很多方法達到，缺少預算與資源，可以透過時間投入從人員的意識與習慣去改善現況。資安不應該僅是「駭」人聽聞，而是融入工作甚至生活中的一道防線，更進一步提升企業品牌形象。 CNFA

參考資料

[1]. (SophosLabs, How Ransomware Attacks, 2019)。檢自https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophoslabs-ransomware-behavior-report.pdf

[2]. (Bana, IBA cybersecurity guidelines for law firms during the Covid-19 crisis, 2020) 。檢自https://www.ibanet.org/article/25FA3B61-C5EE-4EB7-A987-5C795B911DCD

[3]. (EY, Technology resiliency: key considerations, 2020)。檢自Technology and information security(https://www.ey.com/en_lu/covid-19/technology-information-security#technology)

[4]. (Fortinet, Fortinet 發表「2020 年遠距工作網路資安報告」：8成企業遇極大挑戰, 2020)。檢自https://www.fortinet.com/tw/corporate/about-us/newsroom/press-releases/2020/fortinet-publishes-remote-work-security-report-2020

[5]. (周維忠, 疫情下遠距工作成常態　資安風險如影隨形, 2021)。檢自https://www.netadmin.com.tw/netadmin/zh-tw/trend/16BB571CE86E478DAF08CDC45099301F