漫談後疫情時代之駭客攻擊趨勢

◆ 華梵大學特聘教授 — 朱惠中

全球疫情解封日已逐漸倒數，後疫情時代資安布局宜儘早開始。本文彙編FireEye、Check Point、TechRepublic、SANS、趨勢科技、安碁資訊、iThome等公司整理之駭客攻擊趨勢，下期續提出因應對策。

以 COVID-19 疫苗為誘餌的網路釣魚活動[1]

依 Paloalto Network 公司於今年 3 月 24 日報告指出，自 2020 年初以來，研究人員已觀察到與新冠疫情相關鏈接的釣魚 URL 有 69,950 個。由於新冠肺炎疫情仍未停歇，網路釣魚活動繼續偏向疫苗開發或各國新增限制措施的消息；有意竊取疫苗資訊的網路犯罪者也將持續鎖定開發疫苗公司作為攻擊目標。另針對以新冠疫情為主題所設計的網路釣魚網頁，這些攻擊大多為竊取用戶的商業憑證；例如，Microsoft、Webmail、Outlook 等，其中，Microsoft 登錄頁面佔 23%。其次發現自 2021 年 2 月以來，與新冠疫情相關的 Google 搜索和 URL 大量增加，亦發現網路駭客正在從這些發展趨勢竊取個資。此趨勢又可分為三階段：

[1] https://unit42.paloaltonetworks.com/covid-19-themed-phishing-attacks/。

疫情大流行初期，因新冠疫情測試工具嚴重不足，該期間相關之網絡釣魚攻擊亦大幅增加。

一、在疫情大流行初期（即 2020 年 3 月始），網路攻擊者著重在「新冠疫情檢測試劑盒」與「個人防護設備（PPE）」等領域。例如當時《紐約時報》報導美國新冠疫情測試工具嚴重不足，研究人員發現該期間與檢測工具相關之網絡釣魚攻擊大幅增加，很多都是以網上購物詐騙的形式出現，如設置偽造的 Microsoft Sharepoint 登錄網頁等。

二、接下來重點轉移到政府的經濟刺激與救濟計畫上（2020 年 4 月到 7 月）。2020 年 4 月起，美國國稅局開始向個人發放 1,200 美元，同時「薪資保護計劃」（PPP）付諸實施，這導致了網路釣魚攻擊的迅速猛增。駭客設置偽造之美國貿易委員會網站，冒充該會承諾為每個人提供高達 5,800 美元的臨時救濟基金，當用戶點擊「啟動驗證程序」按鈕後，會被重新導定某份表單，用戶憑證、社會安全號碼（SSN）和駕照號碼因而被竊取。

三、近期（2020 年秋末）則再次轉向疫苗的推出。由於攻擊者不間斷地留意最新趨勢且屢屢創建新的網路釣魚手法，故網路安全防禦亦應同步調整與精進。另駭客會迅速將新發現的漏洞轉化為攻擊武器，讓管理者難以及時修補。例如駭客利用仿造的輝瑞和 BioNTech 等品牌的網站，來

駭客設置偽造之美國貿易委員會網站，打著救濟基金的名號騙取使用者用戶資訊。（Source: http://ungodsrealnighchis.gq/us/protecting-americas-consumers-covid）

駭客利用仿造的 BioNTech 網站進行以 Covid-19 為主題的網路釣魚攻擊，釣魚網頁要求用戶使用 Office 365 憑證登錄，以進行疫苗註冊，藉機竊取用戶個資。（Source: pfizer-vaccine.online）

進行以 Covid-19 為主題的網路釣魚攻擊，釣魚網頁要求用戶使用 Office 365 憑證登錄，以進行疫苗註冊。此釣魚網站使用了一種越來越普遍的技術，即「客戶端偽裝」（Client-Side Cloaking）—該網站並沒有立即跳出意圖竊取用戶個資之表單，而是先要求用戶點擊「登錄」按鈕，以避開網路釣魚探測器。

鑑於新冠疫情仍為全球民眾關注議題，針對藥品和醫療公司之網路釣魚活動已不限美國，在世界各地亦普遍發生。文章指出，與藥房和醫院相關的網路釣魚攻擊呈倍數增加，例如魁北克最大製藥企業 Pharmascience、孟買的全球藥品製造商 Glenmark Pharmaceuticals、以及以上海為基地的醫藥研發公司 Junshi Biosciences 等公司均已淪為被攻擊的對象。

供應鏈攻擊與委外管理[2]

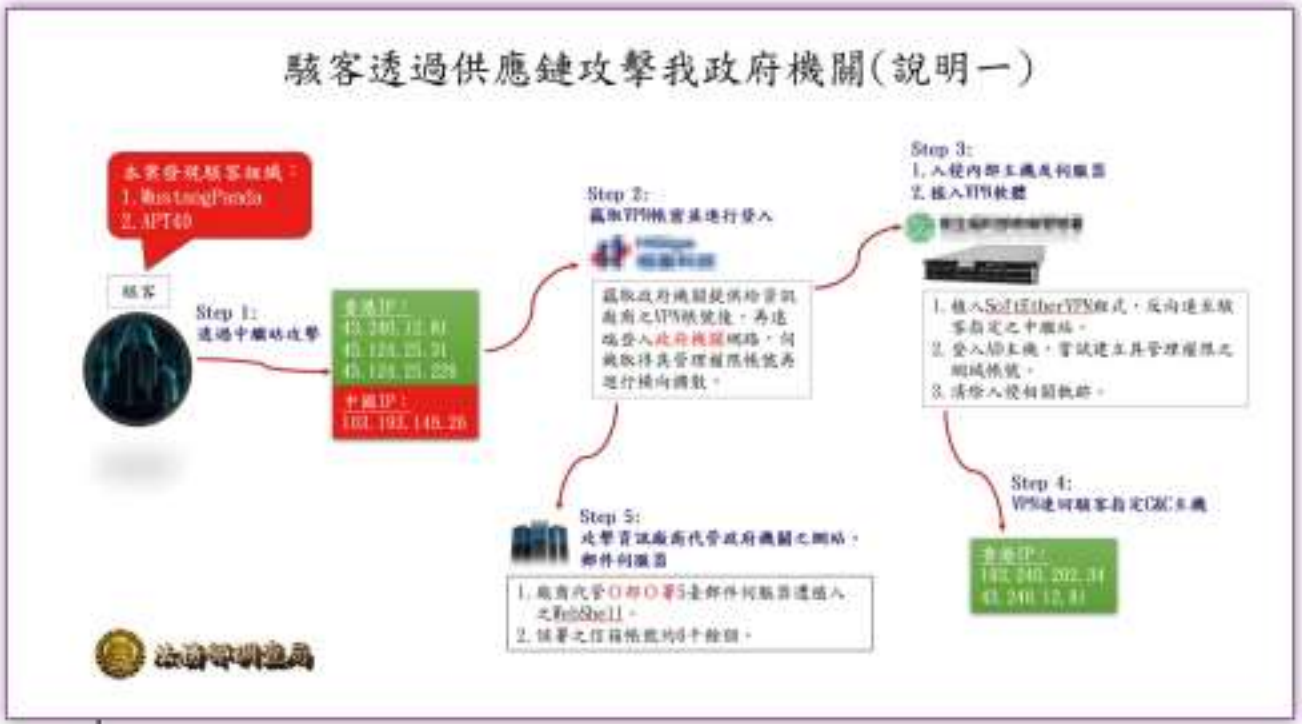
近年來，供應鏈攻擊手法越來越普遍，此類攻擊主要衝擊到被授權能存取系統和資料的委外廠商，故其不僅透過軟體供應鏈入侵，更是藉由委外廠商或合作廠商來進行滲透行為。由於與過往相比，有更多的供應商和服務商能接觸到政府與企業的敏感數據，因此，此類攻擊類型被視為 2021 年持續要留意的焦點。

[2] https://www.ithome.com.tw/news/142116。

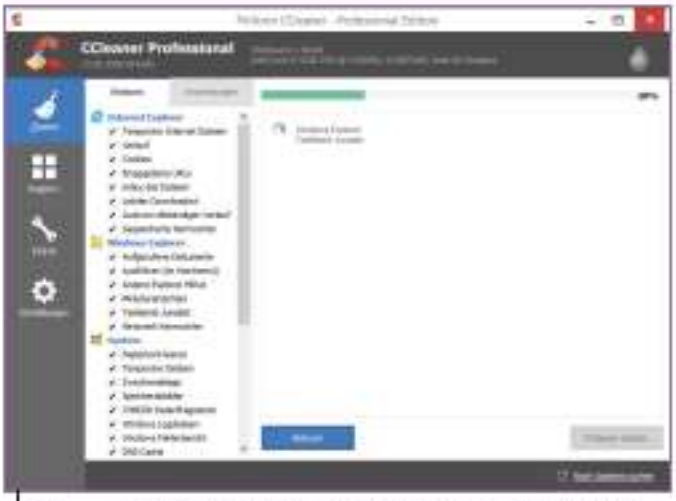
從另一個面向來看，供應鏈攻擊是一種以軟體開發人員或供應商為目標的新型態威脅與攻擊，其目標是要存取來源代碼、建置處理程序，或藉由具威脅的、新興的、感染合法的應用程式散布惡意程式碼來干擾機制。

若疫情未能衰減，在家工作或遠距教學成為日後主流，人類生活模式，將全然在線上進行，5G 布建就是達成上述需求的最佳解決方案。然在高速連網的環境下，駭客更易從某企業網路跳到其他企業網路，家用網路亦將成為歹徒的攻擊跳板：挾持家用電腦或藉由網路其他裝置，最終駭入企業內網。此類供應鏈攻擊還會波及下游廠商、需遠端存取企業機密或關鍵資訊的員工，進而讓人資、業務與技術支援等機敏資料，都將被駭客所竊取。

此外，遠端駭客在網路上的攻擊將轉以路由器為攻擊目標，入侵家用路由器將成為駭客的最新服務模式，繼而販售家用網路的存取權限，這種「存取服務」未來將成為駭客賺錢的商業模式。駭客將長期掌控裝置，將一些高價值目標（如高階主管或系統管理員）的家用網路存取權限賣給不法者；未來歹徒鎖定的最終目標，是已將資訊技術（IT）與營運技術（OT）網路整合的企業，網路罪犯將以藉銷售 OT 網路的存取權限營利為主要業務。



法務部調查局於 2020 年 8 月發出警示，提醒所有機關單位或企業重視 VPN 帳號委外維運風險，慎防駭客先入侵委外廠商再滲透到組織內部的情形。（圖片來源：法務部調查局）



CCleaner 為用於刪除不必要檔案和註冊表中最受歡迎的軟體之一，擁有眾多使用者，2017 年遭駭客入侵，使超過 200 萬的使用者電腦遭到感染。（Photo Credit: Tim Schulz, CCleaner, https://commons.wikimedia.org/wiki/File:CCleaner.png）

台積公司公布電腦病毒感染事件影響

發佈單位：台灣積體電路製造股份有限公司
發佈日期：2018年8月5日

台灣積體電路製造股份有限公司今（5）日針對電腦病毒感染事件提供進一步說明，台積公司於8月3日傍晚受到電腦病毒感染，影響台灣廠區部分電腦系統及廠房機台，受病毒感染的程度因工廠而異。台積公司已經控制此病毒感染範圍，同時找到解決方案，並台灣時間下午兩點為止，約90%受影響的機台已經恢復正常，台積公司預計在8月6日前，所有受影響機台皆能夠恢復正常。

台積公司預估此次病毒感染事件將導致晶圓出貨延遲以及成本增加，對台積公司第三季的營收影響約為百分之三，毛利率的影響約為一個百分點。台積公司有信心第三季晶圓出貨延遲數量將於第四季補回，全年業績展望以美元計仍將維持7月19日所說的高個位數成長。

台積公司多數客戶皆已收到相關事件的通知，我們也正與客戶緊密合作，溝通其晶圓交貨時程。台積公司將在未來幾天內與個別客戶溝通細部資訊。

此次病毒感染的原因為新機台在安裝軟體的過程中操作失誤，因此病毒在新機台連接到公司內部電腦網路時發生病毒擴散的情況。惟台積公司資料的完整性和機密資訊皆未受到影響，台積公司已採取措施彌補此安全問題，同時將進一步加強資訊安全措施。

台積電因新機臺安裝軟體爆發電腦病毒感染事件，造成台積電多家晶圓廠傳出產線當機，讓該公司遭受數十億元損失。（Source: tsmc, https://pr.tsmc.com/chinese/news/1969）

綜觀這幾年發生的供應鏈攻擊事件，我們可以發現企業若要做好相關的防護，必須重新思考對於各種委外服務的要求，亦即遵《資安管理法》第 4、9 條規定，將委外廠商與其合作廠商納入 ISMS 的導入範疇，以降低在家工作的風險及支援遠距上班的資安作為。

列舉近年間之供應鏈攻擊實例：

一、常用的工具軟體被駭客駭入，成為滲透企業的新利器，如「CCleaner」。

二、2018 年，台積電因新機臺安裝軟體爆發電腦病毒感染事件，導致產線停擺，加上橫向移動（Lateral Movement）影響，造成台積電多家晶圓廠傳出產線當機，讓該公司遭受數十億元損失。調查事故發生原因，係該公司既有機臺未修補安全漏洞，在新設備連入內部網路前，亦未照 SOP 要求實施掃描病毒的程序，相關網路（IT 與 OT）並未參考 PURDUE 參考模式作分層隔離，都是主因。

三、2018 年媒體揭露，大陸間諜透過美國科技的供應鏈，已經滲透到亞馬遜、蘋果等近 30 間美國企業，原因就出在這些公司採用的 Supermicro 伺服器主機板，被置入不明晶片。

總而言之，這幾年發生的供應鏈攻擊事件，委外廠商均扮演相當核心的角色，故委外廠商選任時，務必須落實監督（稽核）機制。

遠距工作與線上教學的弱點[3]

彙整相關資料，臚列遠距工作與線上教學的弱點如次：

一、不安全的設備。

二、疫情導致駭客行為增加。

三、駭客大力攻擊 VPN 與 RDP，以及遠端桌面的攻擊。

四、作業過度倚賴雲端工具。

五、缺乏培訓新的用戶，更無法說明安全性相關議題。

六、雲端代管系統遭未授權存取。

七、更容易接觸釣魚郵件與惡意網站。

八、公務與私務使用相同的帳密。

九、大量使用未經驗證的資訊工具。

十、缺乏遠距工作政策。

勒索軟體發展與防護實務

安克諾斯（Acronis）最新網路威脅報告示警，2020 年的網路攻擊有一半是勒索軟體，不僅透過檔案加密勒索贖金，甚至在加密前就先取機敏資料，威脅不付款就公開資料，故今年網路攻擊威脅從過去「資料加密」升級至「資料洩漏」，特別是對製造業之勒索；須從管理面來規劃防範勒索軟體的備份作業之標準作業程序。

重點彙整[4]

一、由於新冠肺炎疫情仍未停歇，網路釣魚活動將繼續利用疫苗開發或各國新增限制措施的消息；有意竊取疫苗資訊的網路犯罪分子或國家也將持續鎖定開發疫苗的製藥公司作為攻擊目標。

二、在全球各級學校大幅採用電子教學平臺後，統計資料顯示遭遇網路攻擊數量已明顯增加。未來，預期網路攻擊將繼續干擾遠距學習的進行。

三、2020 年第三季起，雙重勒索攻擊急遽增加，駭客先竊取企業大量敏感資料，再對受害企業的資料庫進行加密（據報導，暗網上可購買超過 4,000 個資料庫的存取密碼）。攻擊者威脅若不支付贖金，就將所竊取的資料公諸於眾（例如，在銷售收據上加印該公司已被勒索軟體入侵等訊息），造成企業難以拒絕駭客的要求。其中，醫院將是最容易遭到雙重勒索攻擊的目標之一。

[3] 扭轉潮流，趨勢科技 2021 年資安預測，https://www.trendmicro.com/zh_tw/security-intelligence/threat-report.html。

[4] https://www.checkpoint.com/press/2020/check-point-softwares-cyber-security-predictions-for-2021-securing-the-next-normal/.

為抑制疫情擴散，全球各級學校大幅採用電子教學平臺，未來預期網路攻擊將繼續干擾遠距學習的進行。

2020 年第三季起，雙重勒索攻擊急遽增加，駭客先竊取企業大量敏感資料，威脅若不支付贖金，就將所竊取的資料公諸於眾。

四、「水可以載舟，亦可覆舟」，5G 將打造一個萬物互聯的高速世界，卻也為犯罪分子和駭客提供了更多攻擊機會，如電子醫療裝置可監測使用者的健康狀況、聯網汽車服務能掌握使用者的移動路徑、智慧城市應用則會記錄使用者的生活方式等。因此，5G 時代中的大量資料，若遭洩漏、盜竊和篡改，後果將難以想像。資安管理者尤應注意許多資料可能繞過公司網路及其安全控制的情形。

五、手機應用程式有權廣泛存取聯絡人資料及訊息，因此個人資訊的洩漏問題已遠超出我們的想像。例如，追蹤新冠接觸者足跡的 App 就包含個資外洩的隱私問題。另外，竊取使用者銀行憑證或啟動廣告點擊詐欺的惡意軟體更已成為手機用戶日益嚴重的威脅。