漫談後疫情時代之駭害攻擊趨勢

華梵大學特聘教授／朱惠中

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://ungodsirealnighchis.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]

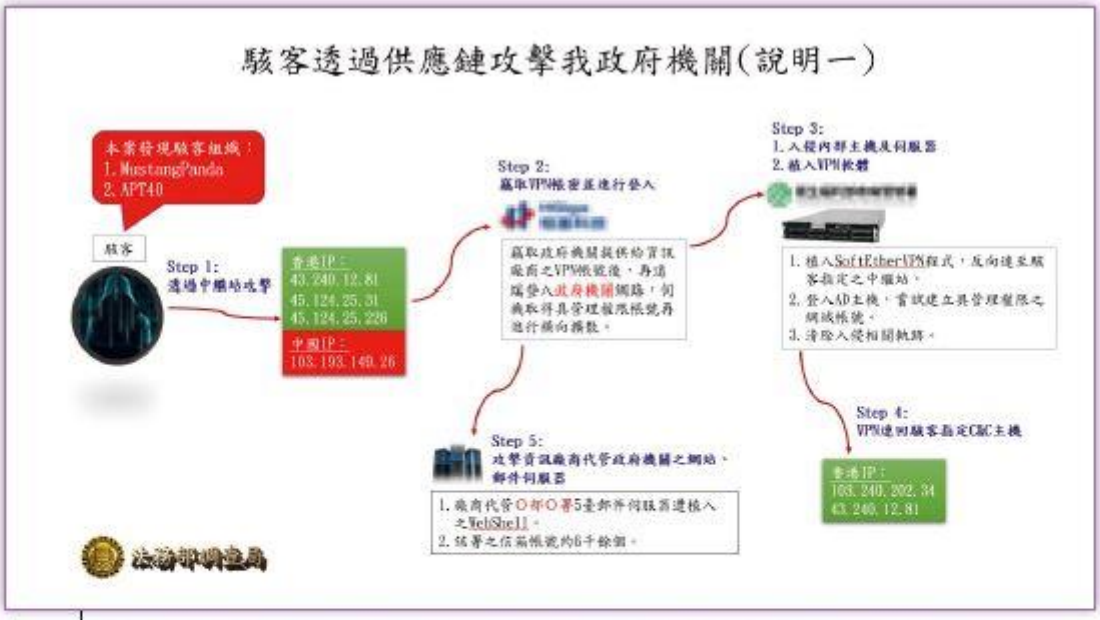
近年來，供應鏈攻擊手法越來越普遍，此類攻擊主要衝擊到被授權能存取系統和資料的委外廠商，故其不僅透過軟體供應鏈入侵，更是藉由委外廠商或合作廠商來進行滲透行為。由於與過往相比，有更多的供應商和服務商能接觸到政府與企業的敏感數據，因此，此類攻擊類型被視為 2021 年持續要留意的焦點。

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

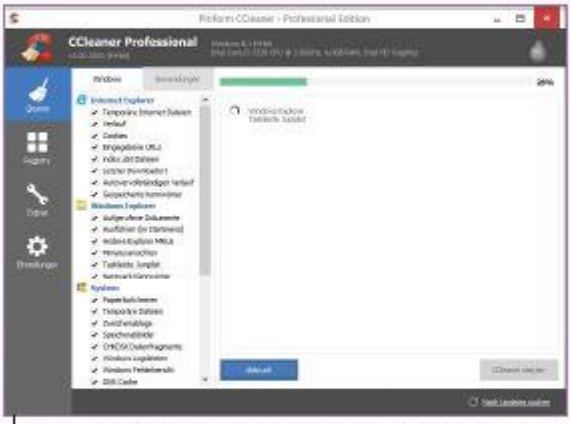
從另一個面向來看，供應鏈攻擊是一種以軟體開發人員或供應商為目標的新型態威脅與攻擊，其目標是要存取來源代碼、建置處理程序，或藉由具威脅的、新興的、感染合法的應用程式散布惡意程式碼來干擾機制。

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。

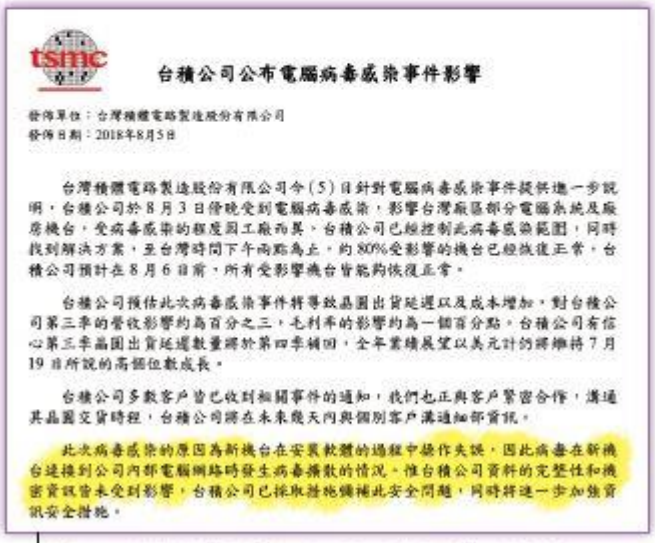
此外，遠端駭客在網路上的攻擊將轉以路由器為攻擊目標，入侵家用路由器將成為駭客的最新服務模式，繼而販售家用網路的存取權限，這種「存取服務」未來將成為駭客賺錢的商業模式。駭客將長期掌控裝置，將一些高價值目標（如高階主管或系統管理員）的家用網路存取權限賣給不法者；未來歹徒鎖定的最終目標，是已將資訊技術（IT）與營運技術（OT）網路整合的企業，網路罪犯將以藉銷售 OT 網路的存取權限營利為主要業務。



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，至台灣時間下午兩點為止，約 80%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的將維持 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。

本文摘自清流雙月刊中華民國110年5月 號P49-P55

你夠在意嗎？考驗人性的社交工程誘惑

社團法人臺灣E化資安分析管理協會、逢甲大學創能學院／林子煒

你夠在意嗎？考驗人性的社交工程誘惑

◆ 社團法人臺灣 E 化資安分析管理協會、逢甲大學創能學院 — 林子煒

社交工程形形色色，若不夠留意，騙到你會怕。

社交工程—駭客最有效且省錢之攻擊方式

自從人們可以利用網際網路互通有無，每個人至少都擁有多個網路服務帳號，包括個人或其所屬單位的電子郵件帳號；正因如此，利用資訊科技便利之社交工程犯罪行為層出不窮，且趨勢逐年上升。

社交工程即為人與人之間的攻擊。過去關於此類攻擊定義為「攻擊者藉由社交手法取得系統或網路的資訊」，然而現今攻擊者的目標，已逐漸轉到個人擁有之資訊。此攻擊管道，最常見的為電子郵件、簡訊、即時通訊軟體（如 Messenger、Skype、Line、Instagram、Whats App）等

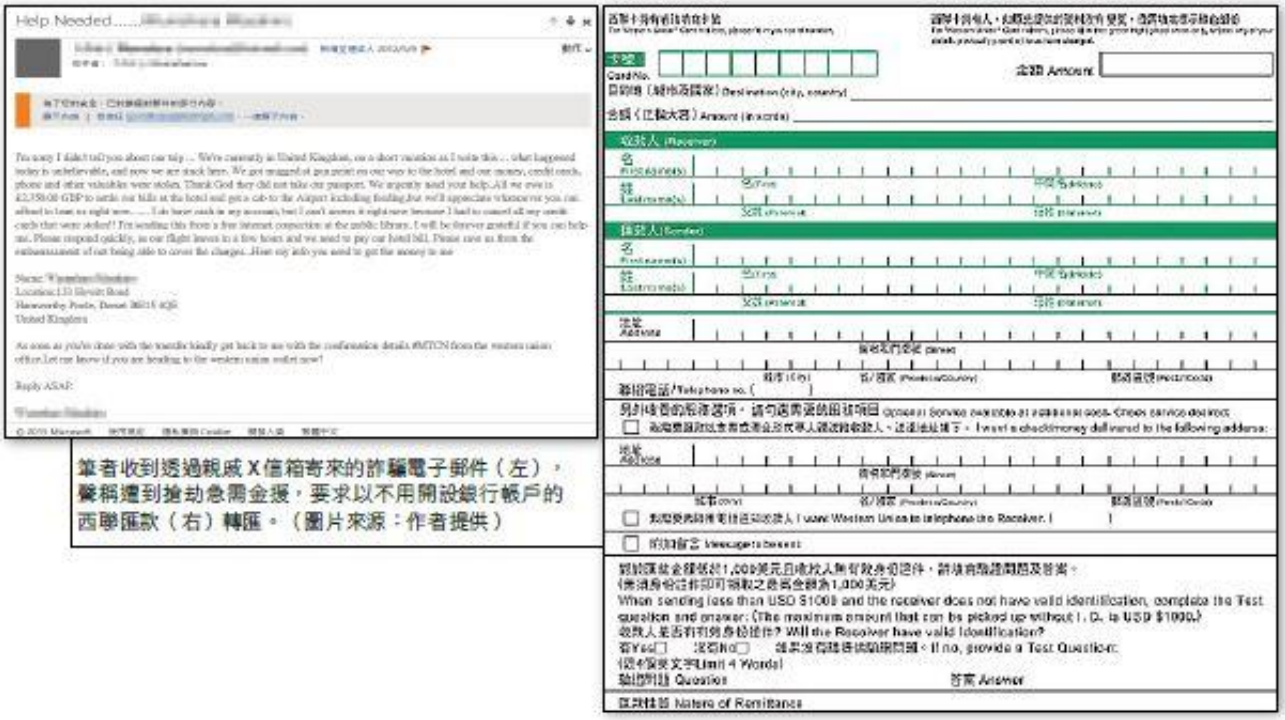
等。為何此種攻擊趨勢會逐年上升？因為對駭客而言，這是最有效、最省成本的攻擊方法。

親身經歷之詐騙案例

以自身經驗為例，某天上午收到親戚X寄來的英文信，信中述說他「正在英國旅遊，但被當地歹徒持槍威脅交出身上所有財產，包括金錢、信用卡、行動電話等。這封信是透過當地的免費網路寄出，現在急需金錢援助，請用西聯匯款（Western Union）匯2,350英鎊（約新臺幣9萬元）給我」。

信中附上姓名與地址，我抱著好奇心利用Google地圖查詢，結果發現那家英國旅館竟然地處在杳無人煙的社區。另個親戚Y也在詢問是否有收到這封信，所以我們研判親戚X的信箱帳戶應該已被盜用，而盜用者寫了這封信，並寄給信箱內所有的聯絡人。

詐騙者指定西聯匯款[1]的原因，係因其匯、收款的雙方都不用開設銀行帳戶，只要填寫雙方英文姓名與出示身分證明即可匯款。作法是在匯款人填妥表格後，系統會產生一組10位數密碼，匯款人只要將



筆者收到透過親戚X信箱寄來的詐騙電子郵件（左），聲稱遭到搶劫急需金援，要求以不用開設銀行帳戶的西聯匯款（右）轉匯。（圖片來源：作者提供）

[1] 成立於1851年，號稱是世界最大的電子匯款公司，在全球超過200個國家與地區設置至少21萬個據點，提供各地收、匯款服務，https://www.westernunion.com/us/en/home.html。

密碼給收款人，收款人就能憑藉英文姓名及密碼進行提款。時至今日，全球已有相當多利用西聯匯款而被詐騙的案例，警方與銀行都無法追蹤及攔截詐騙款。

社交工程郵件之包含要素

以電子郵件來詐騙至少已有十年歷史，然至今仍有民眾上當，因為民眾輕忽或無知，易讓駭客達到欺騙目的。社交工程電子郵件不乏利用聳動的郵件主旨、偽造受害者熟悉的寄件者、以假亂真的郵件內容等等，試圖吸引使用者上鉤。社交工程電子郵件中會有幾個要素，包含超連結、附件、圖片、郵件內容內嵌程式碼。

- **超連結**：有可能會讓受害者連至攻擊者所架設之惡意網站，藉此收集受害者相關資訊。
- **附件**：多含惡意程式，開啟並執行後會潛藏在受害電腦裡，直接將電腦內資料對外傳輸、偷偷側錄用戶使用電腦的任何行為、接續下載惡意程式至受害電腦再執行各項行為等。
- **圖片及郵件內容內嵌程式碼**：能回報給攻擊者表示「登陸成功」，更甚者直接讓受害者電腦自動從中繼站下載小程式(諸如鍵盤側錄工具、螢幕側錄工具等)，記錄受害者使用電腦行為，再進行下一步攻擊。

以上要素不一定會同時出現，亦可能交互搭配使用，曾有僅憑單一內容即欺騙成功的案例，造成受害者損失。例如，假冒會議邀請信函，成功欺騙到受害者出門參加會議，加害者利用這段時間闖空門等。

勒索軟體通常包裹著社交工程郵件外衣

近幾年造成全球重大災情的勒索軟體，大部分行為模式即透過社交工程電子郵件，讓受害者點擊後自動下載並執行一個看似無害的小程式，連線至外部中繼站下載勒索軟體主程式，此主程式會開始掃描電腦所存文件[2]後加密，跳出警告訊息，指示受害者利用比特幣付款至指定帳戶以換取解密提示。

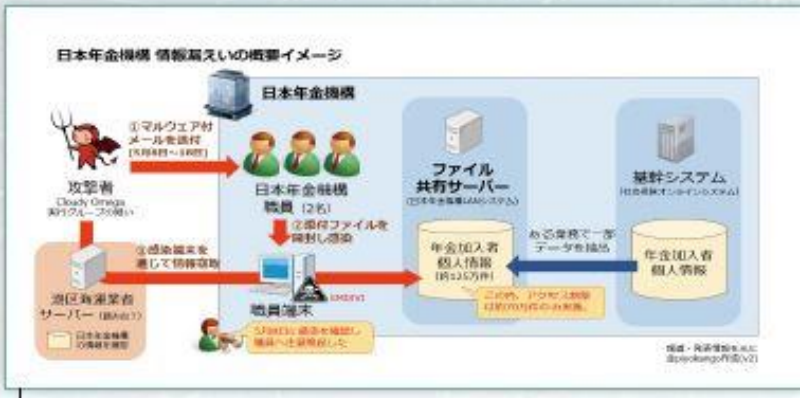
日本年金機構之個資外洩事件

若讀者認為，就算有人「運氣這麼不好」開啟了社交工程電子郵件，造成傷害也不過是個人財產及聲譽。其實損失的嚴重性，絕非想像中的那般簡單。

掌管日本全國國民年金的組織「日本年金機構」（相當於勞動部勞工保險局國

[2] 多為 Office 系列，以及 PDF 或 JPEG 圖檔等企業常見之檔案格式。

大部分勒索軟體的行為模式，即是透過社交工程電子郵件誘惑使用者點擊，而成為受害者。



日本年金機構個資外洩事件示意圖，遭駭主因係員工不慎打開含病毒之社交工程電子郵件所致。（Photo Credit: piyokango, https://piyolog.hatenadiary.jp/entry/20150601/1433166675）

民年金組），於 2015 年 6 月召開記者會，坦誠因員工電腦受駭客攻擊，導致民眾個人資料外洩[3]；整起事件的起因，即為員工不慎打開含病毒之社交工程電子郵件所致。

剛開始是該機構九州分部員工收到社交工程電子郵件，點選超連結後，即被自動下載惡意程式，並開始不正常的電腦連線。

雖然日本國家網路安全中心（National Information Security Center, NISC）[4]於第一時間發出通報，但因為日本年金機構檢測不出原因，因此僅更新個人電腦的防毒軟體，直到東京本部也有員工收到同樣的社交工程電子郵件並開啟，偵測到儲存年金的資料庫有異常連線行為後，才驚覺事態嚴重。日本年金機構事後雖通知警方，且 NISC 亦緊急派員處理，然已造成所屬 5 個單位內有多達 19 臺的個人電腦遭受感染，最後清查出竟然有高達 125 萬筆的個資外洩，嚴重影響到仰賴年金度日之日本民眾的生活。

社交工程之攻擊方式

由日本年金機構案例可知，只要個人一時疏忽，即使只是小小電子郵件，就有很大機會對企業、群體，甚至國家安全造成危害。

另外，即時通訊軟體也成為社交工程攻擊管道之一。在 COVID-19 疫情高峰時，國內採取口罩預購制，意外出現「口罩釣魚簡訊」，佯稱口罩到貨，引誘使用者點擊簡訊

[3] 《病毒入侵！日本年金機構 125 萬件個資遭外洩》，https://news.ltn.com.tw/news/world/breakingnews/1335620。

[4] 是日本負責網路危機應變處理之政府單位，為 2015 年 1 月由「內閣官房資訊安全中心」升格而成，代表將網路安全提高到國家安全層次。

內連結，當時亦有不少臺灣民眾受駭[5]。以下再列舉其他社交工程之攻擊種類。

一、**濫發電子訊息**：諸如惡意電子郵件、釣魚簡訊、即時通訊等文字訊息。此類攻擊通常一次廣發給多名使用者，因此亦稱為「垃圾郵件」。

二、**釣魚**：此類攻擊通常會讓使用者「信以為真」，透過話術讓人誤信，進而騙取錢財。近期常見「假交友」、「假投資」即屬此類。

三、**願者上鉤**：經典手法為攻擊者在公司門口隨意丟棄一個隨身碟，該公司不知情員工撿到後，誤以為是公司內有人不小心遺失，為了順利歸還，故而將該隨身碟插進自己的電腦內，殊不知惡意程式就此開始執行。

四、**搭順風車**：尾隨員工進入外人不該進去的區域，進而竊取到公司內部機密資訊。

五、**水坑攻擊**：利用網頁藏惡意程式碼的方式，讓使用者的電腦中毒。只要入侵或偽造目標受害者常瀏覽的網站，植入惡意程式，當受害者瀏覽該網站，即會下載惡意程式。

社交工程攻擊之防範措施

社交工程攻擊防不勝防，面對攻擊，可行的防範措施包含：

一、**使用垃圾郵件過濾器**：現行的郵件伺服器（包括 Gmail）皆有此機制。

二、**定期更新**：隨時更新防毒軟體、防火牆與電腦及手機的作業系統，以防任何安全性漏洞被利用。

三、**仔細確認**：確認訊息與自己是否相關，並查證訊息來源，有必要時打電話向來源確認。

釣魚簡訊經常引誘使用者點擊簡訊內連結，進而竊取民眾個資、詐騙錢財。（圖片來源：內政部 FB 粉絲專頁，https://www.facebook.com/moi.gov.tw/photos/a.105361604800013l/3275894322438948）

[5] 《台灣詐騙網址暴增 4 倍　駭客冒用口罩預購行騙》，https://www.cna.com.tw/news/ait/202009220313.aspx。

人是最大的零日漏洞，只要使用者資安意識稍有不足，即為攻擊者打開一扇自由進出的大門。

四、**提高警覺**：個人應提防不明電子郵件，並且勿任意點選附檔及超連結。

人是最大的 Zero-Day

社會生活中形形色色的誘惑，即是社交工程對於網路用戶的最佳詮釋，諸如「清不完的木馬，無知與恐懼也；補不完的系統，人腦也」、「人是最大的 Zero-Day[6]」等，雖然只是玩笑話，也道出了防範社交工程的最關鍵要素是「人」。資訊技術發展這麼多年，為何電子郵件社交工程依然是攻擊者的攻擊手段首選，乃因為電子郵件是阻力最小的攻擊路徑，只要使用者資安意識稍有不足，**開啟惡意電子郵件，即為攻擊者打開一扇自由進出的大門，也開闢了一條讓使用者或其所屬組織邁向毀滅的道路。**因此，在日常生活中一定會接觸到電子訊息的我們，勢必要多加瞭解是類攻擊，且必須養成習慣、提防不明電子訊息。相信你只要夠「在意」，必當能防範形形色色且誘惑人性之社交工程攻擊。

社團法人台灣 E 化資安分析管理協會（ESAM）

[6] 在電腦領域中，零日漏洞或零時差漏洞（zero-day vulnerability、0-day vulnerability）通常是指還沒有修補程式的安全漏洞，而零日攻擊或零時差攻擊（zero-day exploit、zero-day attack）則是指利用這種漏洞進行的攻擊。「零時差漏洞」是軟體或硬體的瑕疵，如未能及時修補，駭客就能在不被察覺的情況下透過網路侵犯個人隱私、偷取商業機密與摧毀公共設施等。

本文摘自清流雙月刊中華民國111年5月 號P65-P70