資訊安全講習-4

- 資 訊 科 技 與 競 爭 優 勢 -

李政峰 (James Lee)
經濟部工業局-能源管理系統輔導顧問
教育機構驗證中心ISCB個資講習顧問
Line：bear1858

- ISO 27001 主導稽核員
- ISO 20000 主導稽核員
- ISO 9001 內部稽核員
- BS 25999 主導稽核員
- BS 10012 主導稽核員
- SSCP 合格完訓
- CISSP合格完訓
- CCSP 合格完訓
- ECIH 合格完訓

Agenda

- 電子郵件社交工程
- BPC 商業流程入侵攻擊
- 7 個保護帳戶安全小提醒
- 8 個維護帳戶安全小秘訣
- 資訊安全案例分享
- 課後評量

電子郵件社交工程

- 資 訊 科 技 與 競 爭 優 勢 -

新釣魚信件，小心帳號密碼資料外洩

資料來源：2017.6.21 趨勢科技

釣魚網站竊取個資案件層出不窮，現在釣魚信件捲土重來，持續騙取被害者的網站登入帳號密碼等等資料。趨勢科技日前接獲回報，發現幾起釣魚信件的案件。

以往釣魚信件常直接將釣魚網站的惡意網址連結置於內文中，或將惡意連結偽冒為正常網址連結，誘使受害人信任而連線至釣魚網站，進而騙取受害人帳號密碼等個資。

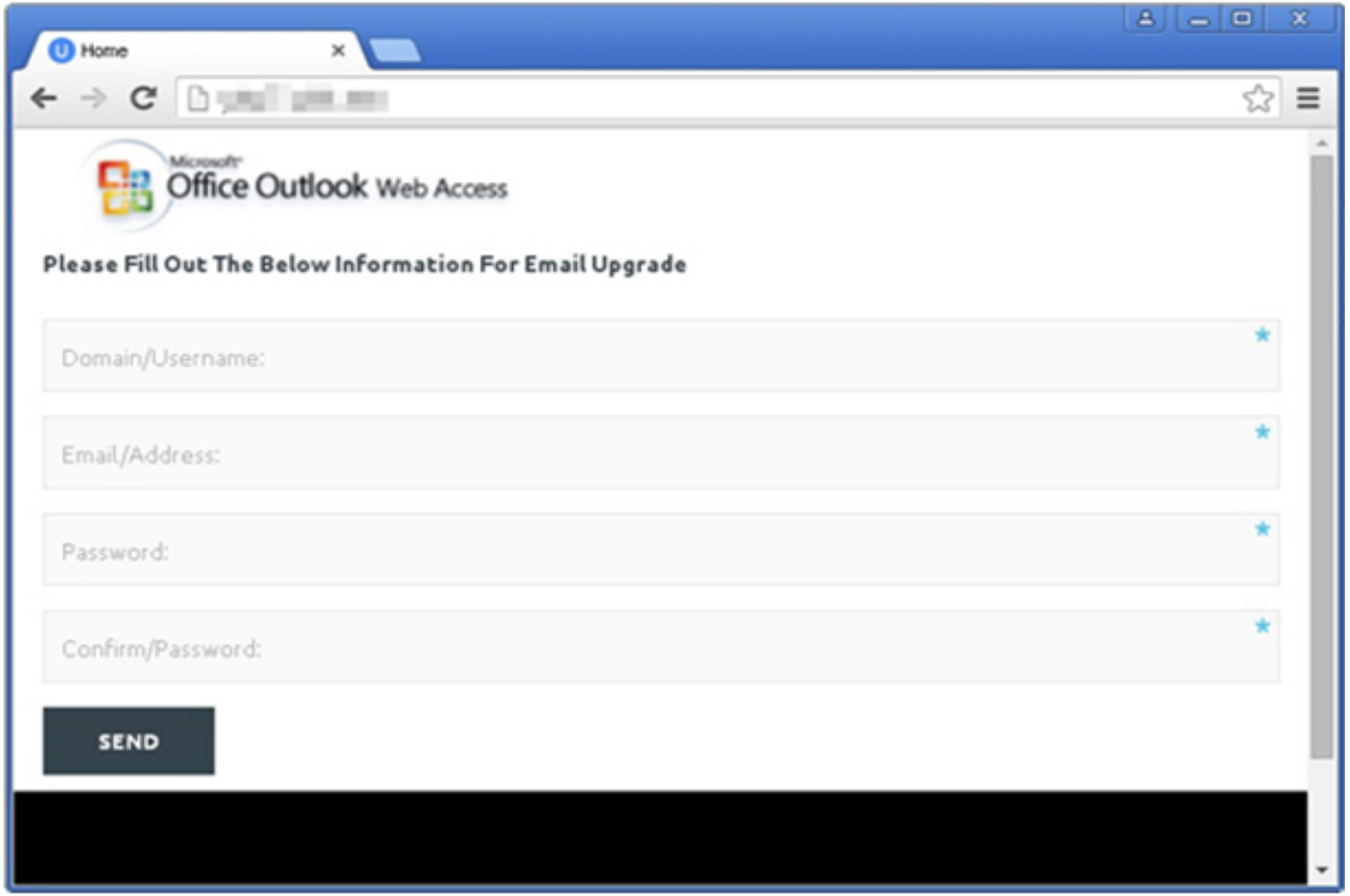
此次的釣魚信件案件與前述案件不同，釣魚信件中夾帶惡意附件，駭客誘使受害者下載執行附件後，再連線至釣魚網站。

新釣魚信件，小心帳號密碼資料外洩

〈案例一〉釣魚信件假冒 Word 檔案，誘使受害者點選，實為釣魚網站連結

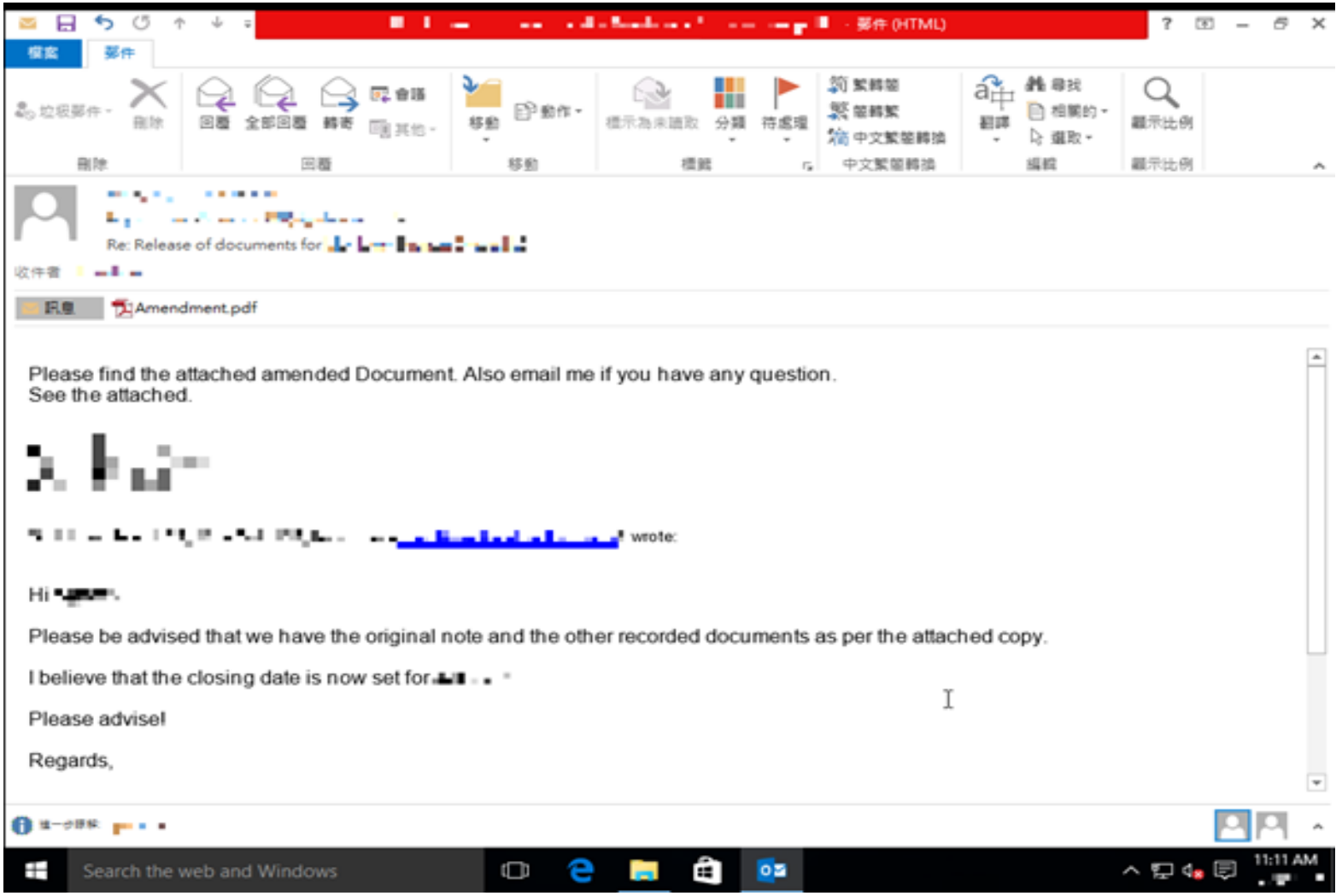
新釣魚信件，小心帳號密碼資料外洩

點選檢視或下載，會連線至釣魚網站誘使受害者輸入帳號密碼等資訊。



新釣魚信件，小心帳號密碼資料外洩

〈案例二〉釣魚信件夾帶惡意附件 pdf 檔。



新釣魚信件，小心帳號密碼資料外洩

下載並執行附件後，打開 pdf 檔，裡面要求使用者下載瀏覽 pdf 檔案的程式。

新釣魚信件，小心帳號密碼資料外洩

將滑鼠游標移至下載連結上方，發現真實連結網址並不是連線至 ADOBE 的網站，而是釣魚網站。

新釣魚信件，小心帳號密碼資料外洩

伺服器維修通知

新釣魚信件，小心帳號密碼資料外洩

Email信箱到期通知

Account

收件人：

Update Your Email Account Now (Do Not Ignore)

帐户更新

亲爱的用户，st

你的 电邮帐户 很快就会过期，导致它超过了配额/限额。

我们建议您现在更新并验证您的帐户，以避免暂停。

请立即更新您的帐户

不，我不会完成这个请求，取消

新釣魚信件，小心帳號密碼資料外洩

Email信箱使用空間已滿通知

电子邮件管理员

收件人：

您的邮件框已满（ 立即修复）

亲爱的 _____

您已经得到了您的存储限制，这将导致您的帐户暂停，无需升级。

立即升级以继续使用您的电子邮件帐户

帐户安全部门。

新釣魚信件，小心帳號密碼資料外洩

郵件違規通知

新釣魚信件，小心帳號密碼資料外洩

Email信箱升級通知

MailBox Service

收件人：

We will temporarily lock your email account (Last Notice!!!)

Dear info.[redacted],

We noticed that your email account has been outdated .
Your account will be placed on temporary block, it would be permanently blocked if you do not upgrade within 48hours.

Upgrade Account

Note: Failure to unblock your e-mail account. It will be permanently disabled.

Thank you for using our service.
E-Mail Service

新釣魚信件，小心帳號密碼資料外洩

上述案例皆為看似正當的通知信，信件中的連結皆導向釣魚網站

電子郵件社交工程

資料來源：2018年05月15日資安趨勢部落格快訊

趨勢科技2018年第一季封鎖了近95億筆的威脅 - 其中有82%與電子郵件有關

電子郵件對企業來說是特別脆弱的一環，因為它是一種溝通工具，同時也是網路犯罪份子最愛用的威脅載體。趨勢科技的Smart Protection Network在2018年第一季封鎖了近95億筆的威脅 - 其中有82%與電子郵件有關。

電子郵件會成為主要的攻擊途徑是因為這是種無處不在且被廣泛利用的通訊方式。根據市場調查公司Radicati Group在2017年所進行的研究顯示，該年每天發送了2,690億封電子郵件。除了數量外，電子郵件也被各種人士所使用，從年輕學生到跨國企業執行長都有。它已經成為日常生活的一部分，人們經常會打開電子郵件，滑動內容或點擊連結。網路犯罪分子也利用這樣的習慣來嘗試各種手法攻擊使用者。

網路釣魚

資料來源： 2018 年 05 月 16 日 BY TREND LABS 趨勢科技全球技術支援與研發中心

「帳號出現異常活動 請更新您的付款資料」一按下去，Apple ID 就被盜

新的 Apple ID 網路釣魚攻擊，利用社交工程技巧假藉可能必須終止服務的名義強迫使用者提供個人資料。這波網路釣魚電子郵件是假冒 Apple 的名義，通知客戶因為帳號出現異常活動而被鎖住，必點選郵件內的連結來更新付款資料。當受害者點選郵件中的「Update Your Payment Details」(更新您的付款資料)按鈕時，就會連上一個外觀類似 Apple 網站的假冒網站，網站上所使用的影像背景甚至跟正版的 Apple 網站一樣。

社交工程

資料來源： 2019 年 07 月 14 日 科技新報

駭客，竟然從廣達、Facebook 和 Google 3 家全球頂尖的高科技公司，盜走約新台幣 38 億元

- 這是一堂台灣公司都不能忽視的資安課。一名東歐駭客，竟然從廣達、Facebook 和 Google 3 家全球頂尖的高科技公司，盜走超過 1 億 2,100 萬美元（約新台幣 38 億元），整個過程有如電影《神鬼交鋒》。
- 2019 年 3 月 21 日，一則來自紐約的司法新聞，揭開這場騙局的真相：立陶宛男子黎瑪索斯卡（Evaldas Rimasauskas），因假冒台灣廣達公司身分，替廣達領取貨款，詐騙美國 Facebook 和 Google，被引渡到紐約受審。路透報導，黎瑪索斯卡在紐約曼哈頓法院認罪，同意歸還其中 4,970 萬美元，他騙走 Google 2,300 萬美元、Facebook 9,800 萬美元，創下全球社交工程被駭金額新紀錄，即使人抓到了，還有 1,730 萬美元不知去向。

社交工程

資料來源： 2019 年 07 月 14 日 科技新報

駭客，竟然從廣達、Facebook 和 Google 3 家全球頂尖的高科技公司，盜走約新台幣 38 億元

社交工程

資料來源： 2019 年 07 月 14 日 科技新報

駭客，竟然從廣達、Facebook 和 Google 3 家全球頂尖的高科技公司，盜走約新台幣 38 億元

關鍵 1：郵件帳號被駭客監控

這種犯罪手法可視為社交工程的進階運用，常見狀況是，犯罪者滲透進入郵件系統後，先只悄悄讀取這個人的往來信件。如果被駭的人是公司老闆，當他發現被害人的信箱收到預訂機票的信件，就可能趁他在飛機上，或是沒有辦法回信的短暫時間，替他發郵件向供應商「討債」，把錢匯進他的戶頭。

在歐洲，甚至有一種房仲詐騙，駭客入侵房仲的郵件系統，平常按兵不動，只默默讀取房仲的郵件，等到有房子成交，消費者要付款時，駭客就浮上水面，不但阻斷真房仲發出的郵件，還用他的身分發郵件，要消費者把買房子的錢匯到駭客指定的帳號，在英國，許多消費者因此被騙走終身積蓄。更可惡的是，駭客通常在英國時間星期五發動攻擊，等到錢一匯進假房仲的帳戶，就立刻把錢轉到亞洲等地的戶頭，利用銀行休假時間，創造洗錢的斷點。

社交工程

資料來源： 2019 年 07 月 14 日 科技新報

駭客，竟然從廣達、Facebook 和 Google 3 家全球頂尖的高科技公司，盜走約新台幣 38 億元

關鍵 2：真資訊加假帳號突破控管

犯罪者要花長時間才出手，因為他們鎖定有價值的對象後，就必須完全了解雙方交易的過程與節奏，甚至特定的專業術語，「就像在上另一個班」他形容，犯罪者必須讓自己就像參與這專案的一分子。等到時機成熟，犯罪者發出請款要求，因為專案名稱是真的，交易的過程都真實存在，而帳號資訊早透過正常程序動過手腳，才能通過所有流程，讓財會單位同意把錢付出去。

「你看過電影《神鬼交鋒》嗎？」他分析，很多高明的騙局，讓真訊息和假訊息糅合在一起，達成目的。「我辦過不少類似這樣的攻擊，其中一個案子，受害者、詐騙者和被冒名者，來往 2,000 封信，竟只有不到 5 封是真的，攻擊者完全融入整個供應鏈。」

社交工程

資料來源： 2019 年 07 月 14 日 科技新報

駭客，竟然從廣達、Facebook 和 Google 3 家全球頂尖的高科技公司，盜走約新台幣 38 億元

關鍵 2：真資訊加假帳號突破控管

「這麼高的交易金額，不用見面簽約嗎？」《財訊》記者問，林宏嘉推斷，駭客就是因為長時間監聽，知道付款規則、簽核等程序的複雜度，所以鎖定這些已經有穩定交易，要求付款不容易被起疑的供應鏈交易，再挑選一個雙方最難查證的時間點發動詐騙，這樣 3 分真 5 分像的情況下，往往容易一擊就成功得手。

錢轉入戶頭後，駭客集團最難的挑戰是如何創造斷點，阻絕國際警方追查。黎瑪索斯卡落網，是因為他就是扮演車手角色，不只廣達的假帳戶是用他的名義開的，他也曾直接從帳戶提款花用，因此被捕。但剩下的 7,000 多萬美元在哪裡？誰才是真正的主謀？目前不得而知。

社交工程

資料來源： 2019 年 07 月 14 日 科技新報

駭客，竟然從廣達、Facebook 和 Google 3 家全球頂尖的高科技公司，盜走約新台幣 38 億元

關鍵 3：製造斷點阻絕追查

勤業眾信聯合會計師事務所董事萬幼筠則觀察，「這種手法都經過非常精密的設計」，這類型的犯罪，犯罪者很了解業務內容才辦得到，有時，還可能涉及企業內部舞弊，請出關鍵人物出場配合，讓公司做出錯誤的判斷。

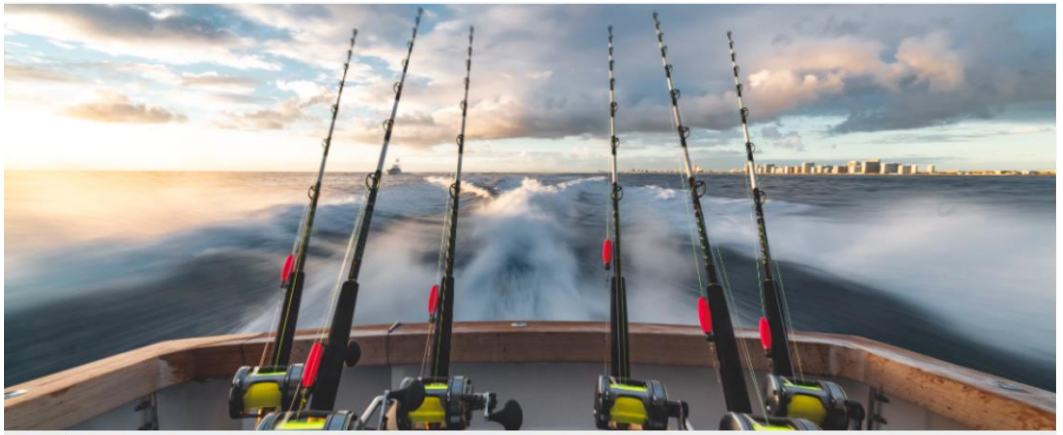
《財訊》調查發現，廣達絕不是唯一個案，當駭客攻擊愈來愈有規模、手法愈來愈精細，連全球大廠都難逃資安威脅。台灣風險正在上升，一股闇黑勢力正在擴散，已成為重要的國安問題。

社交工程

資料來源： 2019 年 09 月 17 日 iThome

網路釣魚攻擊事件頻傳，大學與匿名爆料平臺遭鎖定

- 暗網研究人員Sh1ttyKids在上周末發現，衛報（The Guardian）的SecureDrop匿名爆料平台遭到網釣駭客鎖定，駭客建立了一個假冒為衛報的SecureDrop平台，以騙取爆料者的代號，還在網釣頁面上推銷一個惡意的Android程式。
- 探索了網釣頁面所推銷的Android程式，結果發現此一標榜為可隱藏爆料者位置的Android程式，實為一遠端存取木馬程式，能夠來監控爆料者的活動、所在地、通話、文字、拍照、執行其它命令，或是竊取裝置上的資料。



情境示意圖，Photo by stephen momot on https://unsplash.com/photos/UivGzIDhVyw

社交工程

資料來源： 2019 年 09 月 16 日 iThome

伊朗駭客集團Cobalt Dickens於全球大學展開大規模網釣行動

- 資安業者Secureworks上周指出，由伊朗政府掌控的駭客集團Cobalt Dickens在今年7、8月間再度鎖定全球大學展開網釣攻擊，企圖竊取大學的智慧財產，光是這兩個月就有超過60所大學被Cobalt Dickens鎖定。

今年暑假發動的這波網釣攻擊，信中內容宣稱學生的圖書館帳號已經過期，並附上連結，要使用者點選登入才能取回服務存取權。在使用者輸入憑證之後，憑證一方面落入駭客之手，另一方面也會將使用者導至正常的校方網站，讓受害學生遭駭之後完全無法查覺有異。情境示意圖，Photo by Victuallers on shorturl.at/kGHK8 (CC BY-SA 3.0)

BPC 商業流程入侵攻擊

- 資 訊 科 技 與 競 爭 優 勢 -

商業流程入侵 (BPC)

進階目標式攻擊的下一個步驟！

資料來源：2017 年 06 月 28 日 BY TREND LABS 趨勢科技全球技術支援與研發中心

近幾年來，針對性攻擊/鎖定目標攻擊(Targeted attack) 已有長足發展，其會鎖定特定對象並採用越來越進階的技術來發動攻擊。一般來說，這類駭客會鎖定企業內的單一成員、竊取其憑證、登入帳戶，並冒用這個帳戶來尋找敏感資訊。變臉詐騙攻擊或稱為商務電子郵件入侵 (Business Email Compromise，簡稱 BEC)就是駭客將惡意活動推展到新境界的手法之一，其會運用密集研究與量身訂做的訊息來達到入侵目的。

不過，現在又有新的威脅曝光了：商業流程入侵 (BPC)。BPC 聽起來跟 BEC 很像，但卻是完全不同的概念。

商業流程入侵 (BPC)

進階目標式攻擊的下一個步驟！

資料來源：2017 年 06 月 28 日 BY TREND LABS 趨勢科技全球技術支援與研發中心

BPC 的運作方式

BPC 駭客並非鎖定受害組織中的特定成員，而是鎖定企業中的特定流程，這些流程是完成重要日常作業的關鍵環節。一旦侵入系統之後，駭客就會試圖透過活動、漏洞或整個系統進行滲透，並使用這項弱點作為攻擊主力。

這種攻擊模式的目的是要盡量取得組織的流程資訊，包括商業用的所有活動和系統。駭客可以從這裡查出相關流程和平台的漏洞，並進行巧妙的調整或操控。如此一來，從公司的角度來看，系統仍照常運作。但是，網路罪犯卻躲在背後竊取資料、詐取利潤，甚至盜取實際商品。

商業流程入侵 (BPC)

進階目標式攻擊的下一個步驟！

資料來源：2017 年 06 月 28 日 BY TREND LABS 趨勢科技全球技術支援與研發中心

BPC 有成功過嗎？

雖然 BPC 屬於相對新的駭客招數，但仍有幾件 BPC 攻擊案成功並詐取到高額利潤。其中包括孟加拉央行 (Bangladesh Bank) 攻擊案；在這個案件中，駭客入侵相關流程，並找出可以竊取銀行轉帳驗證憑證的漏洞。這一起 BPC 形式的活動造成了多起詐欺轉帳要求，金額超過一億美元。

該起案件後不久，越南先鋒銀行 (Tien Phong Bank) 也成為駭客的 BPC 攻擊目標。幸好，該組織識破了駭客的詐欺轉帳要求，順利攔阻一百多萬美元免遭盜領。

商業流程入侵 (BPC)

進階目標式攻擊的下一個步驟！

資料來源：2017 年 06 月 28 日 BY TREND LABS 趨勢科技全球技術支援與研發中心

防堵 BPC

由於這類攻擊仍屬新技術，因此防護的第一步是確保對 BPC 的高度警覺，尤其是 IT 團隊系統負責人應充分瞭解這類惡意活動，以更嚴密監控可疑的系統操縱，並阻擋不當的活動發生。

此外，應嚴密檢視網路、所有連接的元件，以及後續的稽核政策。這有助 IT 人員查明任何可能與 BPC 有關的系統調整。

BEC 商務電子郵件詐騙

BEC 商務電子郵件詐騙

資料來源：2018 年 09 月27 日 BY TREND LABS 趨勢科技全球技術支援與研發中心

- 在這些年來，駭客最容易賺錢的方法之一是勒索病毒攻擊。這些攻擊利用強有力的加密技術來讓受害者無法使用自己的檔案和資料 – 然後攻擊者再出售解密金鑰來換取無法追踪的比特幣贖金。
- 但是現在又有另一種高獲利的攻擊手法出現，特別是針對了企業。

BEC 商務電子郵件詐騙

資料來源：2018 年 09 月27 日 BY TREND LABS 趨勢科技全球技術支援與研發中心

- 雖然企業現在越來越意識到了BEC詐騙攻擊，但這攻擊策略其實已經讓駭客賺了好幾年。趨勢科技的研究報告指出，全球企業在2016年遭遇的BEC詐騙攻擊平均造成了14萬美元的損失。
- 在過去，BEC詐騙被稱為man-in-the-email詐騙，駭客利用看似真實的郵件來讓受害企業進行匯款。正如趨勢科技的研究人員所指出，這些攻擊可能以各種不同形式出現，像是假發票、CEO詐騙攻擊、帳號入侵或偽造，甚至是傳統的資料竊取。
- 而以駭客所賺到的錢以及他們攻擊成功的案例來看，BEC詐騙在可見的未來還是會繼續地發生。

BEC 商務電子郵件詐騙

資料來源：2018 年 09 月27 日 BY TREND LABS 趨勢科技全球技術支援與研發中心

- 駭客在兩年前的BEC詐騙攻擊平均造成14萬美元的商業損失，而這些網路犯罪分子一直以來都在精進自己獲利的能力。
- 到了2018年7月，美國聯邦調查局的網路犯罪投訴中心報告指出，BEC詐騙所造成的損失增加了136%，特別是在2016年12月到2018年5月之間。這意味著BEC詐騙攻擊已經造成美國企業達125億美元的損失，不管攻擊是來自國際還是國內。

BEC 商務電子郵件詐騙

資料來源：2018 年 10 月12 日 BY TREND LABS 趨勢科技全球技術支援與研發中心

- **沒有惡意程式,不綁架檔案,一封信竟騙走一棟房子!**
- 前陣子美國洛杉磯的一位男子將非法取得的律師電子郵件帳號提供給其共犯使用，歹徒假冒該律師發送電子郵件給房地產交易的買方，詐騙超過千萬台幣。一封信,騙走一棟房子，一點都不誇張。

BEC 詐騙難以防範的六個因素

資料來源：2018 年 09 月27 日 BY TREND LABS 趨勢科技全球技術支援與研發中心

- 隨著攻擊成功次數的增加，讓駭客賺取更多金錢也造成了更多受害公司。在這樣的情況下，企業高層和IT主管不僅要意識到這些攻擊正在發生，還必須要了解防護此類攻擊的困難性。這樣一來，企業才能採取主動行動，來更好地保護其郵件系統、重要資料、財務和其他資產。

BEC 詐騙難以防範的六個因素

資料來源：2018 年 09 月27 日 BY TREND LABS 趨勢科技全球技術支援與研發中心

- **使用複雜的社交工程攻擊**

  在BEC詐騙中，駭客不只是用一套說詞來製作泛用性的電子郵件就希望可以欺騙他們的目標。相反地，他們會花時間進行複雜的社交工程攻擊。讓他們可以選擇提高目標開啟和回應郵件機會的攻擊方式。

BEC 詐騙難以防範的六個因素

資料來源：2018 年 09 月27 日 BY TREND LABS 趨勢科技全球技術支援與研發中心

- **特製的電子郵件**

  由於使用了強大的社交工程技術，駭客可以製作出假以亂真的電子郵件，內容包含了目標的名字，甚至是企業內的其他人。例如，會計可能會收到來自公司執行長要求匯款的偽造詐騙郵件，使用了執行長的郵件地址甚至是執行長的郵件簽名檔。因此，他就更有可能會去轉出資金，因為郵件看起來非常真實。

BEC 詐騙難以防範的六個因素

資料來源：2018 年 09 月27 日 BY TREND LABS 趨勢科技全球技術支援與研發中心

- **沒有使用惡意連結或附件**

  雖然駭客的背景資料和基礎工作進行的很深入且精細，但送出的郵件卻相當簡單。BEC詐騙依賴於帶有強烈訊息、具有說服力的郵件，這代表著缺乏用來識別可能攻擊的常見可疑元素。

  「由於這些詐騙沒有使用任何惡意連結或附件，它們可以躲避傳統解決方案，」趨勢科技指出。

BEC 詐騙難以防範的六個因素

資料來源：2018 年 09 月27 日 BY TREND LABS 趨勢科技全球技術支援與研發中心

- **訊息內的緊迫感**

  除了利用社交工程來包含正常姓名、地址及其他細節來欺騙受害者外，駭客還會在BEC詐騙郵件內加入強烈的緊迫感來讓攻擊更容易成功。趨勢科技研究人員分析許多郵件後發現，它們都包含了強烈的用語如“緊急”、“付款”、“轉帳”、“要求”及其他可以加強整體訊息的詞語。

- 駭客會偽裝成合作廠商、律師事務所代表或甚至是執行長來聯繫公司員工或高階主管，操縱目標員工/高階主管來秘密進行資金的轉移。

BEC 詐騙難以防範的六個因素

資料來源：2018 年 09 月27 日 BY TREND LABS 趨勢科技全球技術支援與研發中心

- **各種不同方式來針對不同的受害者**

  此外，攻擊者建立了各種不同的攻擊範本，讓他們可以根據社交工程研究來用最有可能成功的方式針對目標。比方說，想攻擊公司執行長的駭客可能會偽裝成合作廠商來為逾期發票要求付款。想針對一家公司發動攻擊的駭客可能並不會偽裝成外部廠商，而是偽裝成需要個人身份資料的內部人力資源員工。

  有了這麼多不同的攻擊範本，駭客有可以精心挑選來製作出最假以亂真的郵件，讓詐騙成功的機會更加提高。

BEC 詐騙難以防範的六個因素

資料來源：2018 年 09 月27 日 BY TREND LABS 趨勢科技全球技術支援與研發中心

- **進一步利用入侵帳號：繼續循環下去**

  最後且不幸的是，受害者被騙進行匯款並不代表著BEC詐騙的結束。一旦帳號被入侵，就可以被用來進行進一步的BEC詐騙，將釣魚郵件或其他BEC詐騙郵件寄給入侵帳號通訊錄上的其他人。

  根據美國聯邦調查局IC3的報告，駭客也會利用受害者來作為“錢騾（money mule）”。這些是來自愛情詐騙或勒索詐騙的受害者，駭客用來開設BEC詐騙所需的新帳戶。雖然這些帳戶可能只開啟短短的時間，卻已經替駭客帶來更多賺錢的機會。

7個保護帳戶安全小提醒

- 資 訊 科 技 與 競 爭 優 勢 -

7 個保護帳戶安全小提醒

資料來源：2019-03-22趨勢科技全球技術支援與研發中心

1. 不要在金融服務應用程式或瀏覽器登入頁面，使用自動填寫登入名稱和密碼的功能。

7 個保護帳戶安全小提醒

資料來源：2019-03-22趨勢科技全球技術支援與研發中心

2. 不要在瀏覽器或不安全的記事應用程式儲存密碼。請使用密碼管理工具。

7 個保護帳戶安全小提醒

資料來源：2019-03-22趨勢科技全球技術支援與研發中心

3. 帳戶使用高強度的專屬密碼，並使用密碼管理工具產生密碼。依據您使用帳戶的頻率，每 30-90 天變更一次密碼，以將密碼遭駭的風險降到最低。

7 個保護帳戶安全小提醒

資料來源：2019-03-22趨勢科技全球技術支援與研發中心

4. 在銀行帳戶啟用雙重認證，並安裝認證應用程式（如果您的銀行有支援）。登入銀行之前必須輸入一組認證碼，該認證碼會透過 SMS 傳送，或是傳送到註冊的認證應用程式。

7 個保護帳戶安全小提醒

資料來源：2019-03-22趨勢科技全球技術支援與研發中心

5. 使用完金融服務應用程式後，請先登出，再讓手機進入睡眠模式。

7 個保護帳戶安全小提醒

資料來源：2019-03-22趨勢科技全球技術支援與研發中心

6. 定期檢查帳戶是否有可疑活動；設定交易的提醒。

7 個保護帳戶安全小提醒

資料來源：2019-03-22趨勢科技全球技術支援與研發中心

7. 不要回覆要求提供 PIN 碼、帳號、簽帳卡或信用卡號碼的網路釣魚簡訊或電子郵件。

8 個維護帳戶安全小秘訣

- 資 訊 科 技 與 競 爭 優 勢 -

8 個維護帳戶安全小秘訣

資料來源：2019-04-30趨勢科技全球技術支援與研發中心

- 不要在金融服務應用程式或瀏覽器登入頁面，使用自動填寫登入名稱和密碼的功能。
- 不要在瀏覽器或不安全的記事應用程式儲存密碼。請使用密碼管理工具。
- 帳戶使用高強度的專屬密碼，並使用密碼管理工具產生密碼。依據您使用帳戶的頻率，每 30-90 天變更一次密碼，以將密碼遭駭的風險降到最低。

8 個維護帳戶安全小秘訣

資料來源：2019-04-30趨勢科技全球技術支援與研發中心

- 在銀行帳戶啟用雙重認證，並安裝認證應用程式（如果您的銀行有支援）。登入銀行之前必須輸入一組認證碼，該認證碼會透過 SMS 傳送，或是傳送到註冊的認證應用程式。
- 使用完金融服務應用程式後，請先登出，再讓手機進入睡眠模式。
- 定期檢查帳戶是否有可疑活動；設定交易的提醒。

8 個維護帳戶安全小秘訣

資料來源：2019-04-30趨勢科技全球技術支援與研發中心

- 不要回覆要求提供 PIN 碼、帳號、簽帳卡或信用卡號碼的網路釣魚簡訊或電子郵件。
- 如果您的帳戶遭入侵，請登入並變更帳戶密碼，然後到銀行更換簽帳卡或信用卡。

資訊安全案例分享

- 資 訊 科 技 與 競 爭 優 勢 -

地平線掃描報告2019

資料來源：2019-03-21 bsi

地平線掃描報告2019

資料來源：2019-03-21 bsi

前 10 大營運衝擊（disruptions）- 過去 12 個月

1
無預警的資通訊中斷
Unplanned IT and telecom outages

2
健康與安全事件
Health and safety incident

3
缺乏人才／關鍵技術
Lack of talent/Key skills

4
網路攻擊與資料外洩
Cyber attack & data breach

5
產品品質事件／產品回收下架
Product quality incident/ product recall

6
異常氣候／自然災害
（如：颶風／地震）
Adverse weather/natural disaster

7
匯率波動
Exchange rate volatility

8
自然資源短缺
Natural resources shortage

9
法規變更
Regulatory changes

10
借貸成本提高
Higher cost of borrowing

地平線掃描報告2019

資料來源：2019-03-21 bsi

前 10 大營運威脅（threats）- 未來 12 個月

1
網路攻擊與資料外洩
Cyber attack & data breach

2
資訊與通訊中斷
IT and telecom outage

3
異常氣候／自然災害
Adverse weather/natural disaster

4
關鍵基礎設施失效
Critical infrastructure failure

5
聲譽事件
Reputation incident

6
法規變更
Regulatory changes

7
缺乏人才／關鍵技術
Lack of talent/key skills

8
供應鏈中斷
Supply chain disruption

9
公共服務中斷
Interruption to utility supply

10
政局變化
Political change

地平線掃描報告2019

資料來源：2019-03-21 bsi

最昂貴的營運衝擊（以美元計算的累積金額）

1
健康與安全事件
Health and safety incidents
11.86億

2
聲譽事件
Reputation incidents
10.36億

3
惡劣氣候
Adverse weather
5億

4
資訊與通訊中斷
IT and telecom outage
3億700萬

5
缺乏人才
Lack of talent
2億5400萬

6
公共服務中斷
Interruption to utility supply
2億4400萬

7
供應鏈中斷
Supply chain disruption
1億8100萬

8
網路攻擊
Cyber attack
1億4400萬

9
新科技的引進
Introduction of new technology
9700萬

10
匯率波動
Exchange rate volatility
9600萬

GPS追蹤器的安全漏洞將允許駭客得知用戶位置或竊聽

資料來源：2019-05-13 iThome

- 英國資安業者Fidus Information Security最近披露，由某家中國業者製造的GPS追蹤器含有多個重大的安全漏洞，將允許遠端駭客得知用戶位置、啟用麥克風以進行竊聽，或是重置裝置設定，而且該業者與多個品牌合作，在全球市場皆有舖貨，估計光是在英國就有超過1萬臺含有相關漏洞的GPS追蹤器。
- GPS追蹤器通常是為老人或小孩所設計的，可在超出活動範圍時傳送警報予緊急聯絡人，電池續航力高達數月。新款的GPS追蹤器配有獨立的電話號碼，可透過行動網路建立連結，允許親友藉由文字簡訊傳送命令以得知用戶位置，撥打電話以啟用用戶的麥克風，設定警報，還能鎖住裝置，變更裝置密碼，重啟或是重置裝置等。

Google利用Gmail蒐集用戶網上購物的紀錄

資料來源：2019-05-20 iThome

- 要刪除Google透過掃瞄Gmail紀錄到的用戶網購清單資訊，用戶必須逐條點入清單中的購物項目按下「移除購物交易」。但是按下去後，使用者會被帶到Gmail信箱中的原始信件處，他必須刪掉信件才能刪除Google帳號中的紀錄。

全球最大加密貨幣交易中心幣安遭駭

資料來源：2019-05-16 iThome

- 數位貨幣交易所遭駭的情況不斷發生，全球最大交易所幣安（Binance）在5月7日公告，駭客藉由安全漏洞，取得大量的用戶金鑰、雙因素認證碼等資料，然後一口氣領走超過7,000個比特幣，相當於4,200萬美元。
- 幣安執行長趙長鵬（Changpang Zhao）表示，駭客使用了網路釣魚、病毒等手法入侵，並且耐心等待最佳出手時機，再透過多個看似獨立的帳號，一次領走大量比特幣。遺憾的是，直到駭客盜走比特幣時，觸發多個警報系統，他們才發現遭到攻擊。

XLoader變種假冒行動電話電信商,進行簡訊釣魚,Android及 iOS 皆為攻擊目標

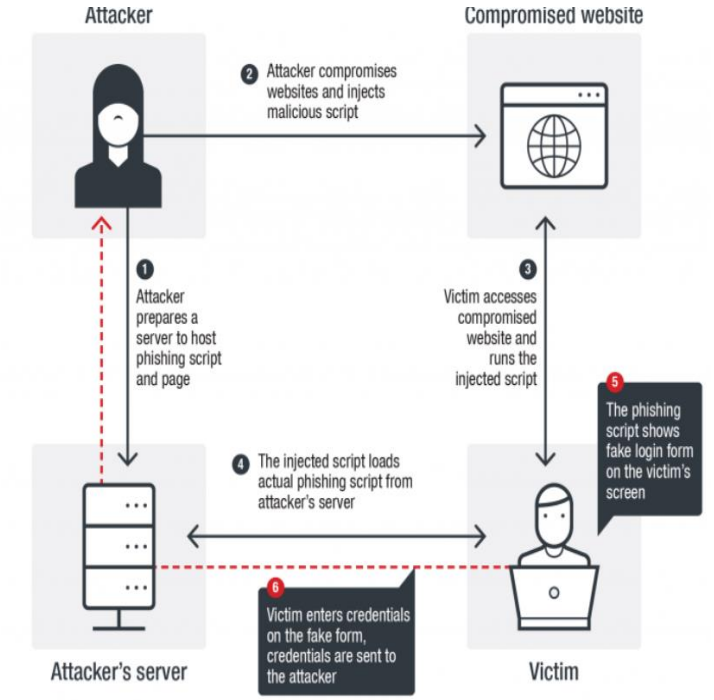
資料來源：2019 年 04 月 17 日 Trend Labs 趨勢科技全球技術支援與研發中心

- 惡名昭彰的XLoader之前曾偽裝成Facebook、Chrome及其他合法應用程式來誘騙使用者下載它的惡意應用程式。
- XLoader變種會偽裝成Android上的安全防護軟體，同時還會利用惡意iOS描述檔(Configuration Profile)來攻擊iPhone和iPad裝置。
- 新變種還會山寨日本行動電話電信商的網站), 透過簡訊釣魚(smishing),誘騙使用者下載假的手機安全防護應用程式APK檔。

「Soula」偽造搜尋引擎登入畫面，針對韓國網站發動水坑攻擊，竊取帳密

資料來源：2019 年 04 月 17 日 Trend Labs 趨勢科技全球技術支援與研發中心

- 透過網路釣魚活動利用注入假登入表單來竊取使用者帳密，至少有四家韓國網站受害，包括了該國訪問量最大的商務網站。
- 利用水坑攻擊進行網路釣魚



Soula的攻擊鏈。

Office 365被入侵帳號

資料來源：2019 年 05 月 15 日 Trend Labs 趨勢科技全球技術支援與研發中心

- Microsoft Office 365仍是相當吸引網路犯罪分子的目標，因為全世界有越來越多企業持續在使用中。
- 光是2019年3月就有超過150萬封惡意和垃圾郵件從數千個被入侵的Office 365帳號寄送出去。據說帳號盜用（account takeover）攻擊的增加是造成此巨大影響的原因。
- 網路犯罪分子盜用Office 365帳號的各種方法。最常見的一種是用釣魚郵件誘騙使用者連到偽造的Office 365登入表單。當使用者登入後，網路犯罪分子就能夠取得其電子郵件帳號。

Office 365被入侵帳號

資料來源：2019 年 05 月 15 日 Trend Labs 趨勢科技全球技術支援與研發中心

- 除了網路釣魚郵件外，其他入侵郵件帳號的方法還包括使用之前從同一使用者個人郵件帳號所竊取的密碼、暴力破解及利用之前資料外洩流出的帳密來嘗試登入。網路和應用程式管道也都被用來入侵郵件帳號。
- 當帳號被入侵之後，網路犯罪分子不會立即發動攻擊。他們會先進行偵察以最大程度地提高攻擊成功機會。所以他們會設定信箱規則來隱藏或刪除他們使用被入侵帳號寄送的郵件。
- 一旦網路犯罪分子獲得企業相關的重要資訊，如企業用的郵件簽名檔及處理財務交易的方式，就會開始針對其他有高價值的帳號，重點放在財務部門的高階主管和員工。

近一半的組織網路安全技術人才短缺,該怎麼辦?

資料來源：2019 年 06 月 04 日 Trend Labs 趨勢科技全球技術支援與研發中心

- 根據(ISC)^2，一家網路安全及IT安全專家組織所指出，全球的網路安全技術人員短缺在2018年達到了近300萬。人才短缺問題也反映在趨勢科技委託進行的調查裡。在1,125名資訊安全長(CISO)中，有近50%的人認為這是他們組織所擔心的重點之一。隨著資安威脅的持續增加(趨勢科技在2018年阻止了超過480億次威脅)且變得更加先進，全球技術人才短缺也讓組織面臨更高的風險。

近一半的組織網路安全技術人才短缺,該怎麼辦?

資料來源：2019 年 06 月 04 日 Trend Labs 趨勢科技全球技術支援與研發中心

- 來自美國、英國、德國、西班牙、義大利、瑞典、芬蘭、法國、荷蘭、波蘭、比利時及捷克的資訊安全長在接受訪談時評估網路安全的挑戰，包括了技術人才短缺。
- 調查顯示，在人員方面，資訊安全長不僅面臨組織內部缺乏網路安全意識的問題，還面臨著技術人才短缺的問題。有33%的受訪者表示在招聘新人才時面臨問題，49%的受訪者擔心人才短缺會讓自己的組織面臨更大的風險。美國的資訊安全長裡有54%(被調查國家裡的最高比例)承認很難請到熟練的專業人才。

承包商來催款,才驚覺175萬美元都匯給假廠商!

資料來源：2019 年 05 月 08 日 Trend Labs 趨勢科技全球技術支援與研發中心

- BEC詐騙造成俄亥俄州教會175萬美元的損失

  變臉詐騙攻擊或稱為商務電子郵件入侵（Business Email Compromise，簡稱BEC)持續危害了許多組織。根據美國聯邦調查局的報告，僅在2018一年就讓企業損失了12億美元。而BEC詐騙也正在從傳統企業受害者擴展到了非營利組織與宗教團體，最新的一起案例就跟教會有關。

承包商來催款，才驚覺175萬美元都匯給假廠商!

資料來源：2019 年 05 月 08 日 Trend Labs 趨勢科技全球技術支援與研發中心

- 在4月17日，俄亥俄州布倫瑞克的聖安布羅斯天主教會發現自己成為BEC詐騙的受害者。他們接到承包商Marous Brothers工程公司因為修建計畫未付款帳單的聯繫後發現。這些帳單總額為175萬美元 – 與 BEC詐騙取走的金額相同。
- 根據美國聯邦調查局的說法，聖安布羅斯教會被騙以為Marous Brothers變更了銀行帳戶。駭客入侵了兩名員工的電子郵件帳號。接著利用這些帳號來欺騙教會的其他人將付款匯到詐騙份子的銀行帳戶。教會並不知道自己一直將付款送到詐騙份子使用的銀行帳戶。由於原收款者（Marous Brothers）沒有收到付款，工程公司不得不詢問教會為何拖欠付款。

勒索病毒襲擊美政府辦公室，迫使氣象頻道斷線

資料來源：2019 年 05 月 01 日 Trend Labs 趨勢科技全球技術支援與研發中心

- 四月底美國氣象頻道（Weather Channel）遭到勒索軟體攻擊，導致其直播暫停了一個多小時。FBI發言人證實，這是一起勒索病毒攻擊案件。

ITHOME.COM.TW

美國氣象電視台也成勒索軟體受害者，導致節目無法準時開播

美國The Weather Channel遭勒索軟體攻擊，導致晨間新聞開天窗，...

美國又有兩個地方政府感染了勒索軟體

資料來源：2019 年 05 月 09 日　iThome

- 美國德州的波特郡（Potter County）才在4月下旬遭到勒索軟體攻擊，迄今尚未完全復原，5月馬里蘭州的巴爾的摩市（Baltimore City）又傳出遭到勒索軟體攻擊，已關閉多數的伺服器，尚在評估受災規模。
- 由於波特郡認為若支付贖金取回檔案的可能性只有1%，決定自行修復系統，但從遭到攻擊迄今已經過18天，波特郡仍只復原了部份系統，造成許多員工仍只能仰賴最傳統的紙筆來工作，而且不能上網。

美國巴爾的摩市政府示意圖。圖片來源:Marylandstater (https://commons.wikimedia.org/wiki/File:1city_hall_baltimore.jpg)

美國亞特蘭大市遭勒索軟體攻擊災情超乎預期

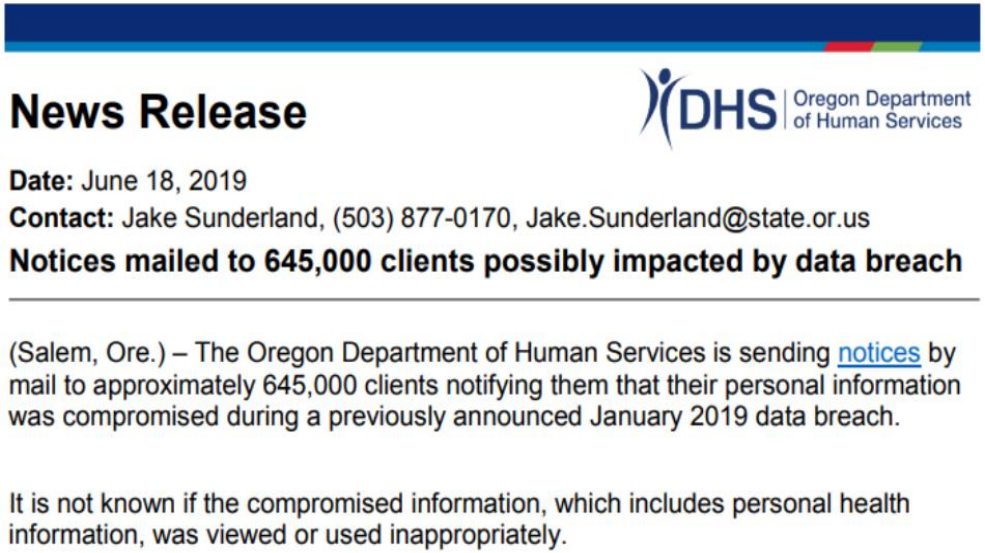
資料來源：2019 年 06 月 11 日 iThome

- 亞特蘭大市資訊管理主管Daphne Rackley在公開會議上提到，由於今年3月市政機關遭遇勒索病毒攻擊，除了之前分配3,500萬美元的IT預算外，還需要額外追加950萬美元來恢復受衝擊的服務。
- 在3月22日亞特蘭大市政府遭到勒索病毒攻擊，公家機關被要求關閉無線網路以及電腦5天，8千名市政府員工受到影響。這個勒索病毒加密了部分市政資料，導致公家服務受到嚴重衝擊，包括市民無法使用支付帳單或是查詢法院相關資訊等線上服務。駭客向亞特蘭大市政府勒索市值5.1萬美元的比特幣，但是市政府並沒有支付贖金。

美奧勒岡州健保署員工誤點網釣信件，害64萬人個資外洩！

資料來源：2019 年 06 月 20 日 iThome

- 美國奧勒岡州健保署（Department of Human Services，DHS）年初遭網釣攻擊，有9名員工不慎開啟郵件，點入郵件挾帶的惡意網站連結。這些員工於隔天起分別通報，健保署並在1月28日前確認所有受影響帳號並予以關閉。根據安全小組調查，雖然沒有惡意程式植入到員工桌機或筆電，但確認網釣攻擊已經造成資料外洩。



News Release

DHS Oregon Department of Human Services

Date: June 18, 2019

Contact: Jake Sunderland, (503) 877-0170, Jake.Sunderland@state.or.us

Notices mailed to 645,000 clients possibly impacted by data breach

(Salem, Ore.) – The Oregon Department of Human Services is sending notices by mail to approximately 645,000 clients notifying them that their personal information was compromised during a previously announced January 2019 data breach.

It is not known if the compromised information, which includes personal health information, was viewed or used inappropriately.

駭客任務中東版!

資料來源：2019 年 06 月 23 日　風傳媒

川普下令對伊朗發動網路攻擊-伊朗駭客鎖定美國政府

伊朗日前宣稱擊落美國「全球之鷹」無人偵察機侵犯領空，因此擊落，而美國媒體揭露，總統川普原批准對伊朗採取報復性反擊，在戰機和艦艇已就位的狀態下臨時喊停，目前仍不清楚川普為何改變心意，但《美聯社》引述消息指出，川普隨後授權對伊朗展開網路攻擊，不過美國網路安全公司指出，隨著美國與伊朗緊張關係加劇，伊朗也擴大對美國的網路攻擊。

美國資訊安全公司CrowdStrike把伊朗進行的網攻行為稱作「優雅小貓」（Refined Kitten），鎖定美國政府機構發送網路釣魚郵件。

AESDDoS 殭屍網路變種,經由暴露在外的 Docker API 滲透容器!

資料來源：2019 年 06 月 19 日 Trend Labs 趨勢科技全球技術支援與研發中心

- 組態設定錯誤的問題早已不是新聞，不過對網路犯罪集團來說，這類問題卻是他們入侵企業電腦資源以從事惡意活動的一項有效管道， Docker Engine-Community 這套熱門的開放原始碼 DevOps 工具如何因為組態設定上的錯誤，而讓駭客滲透到容器內部並執行 Linux 殭屍網路惡意程式 AESDDoS 的某個變種。
- 在容器主機上運作的 Docker API 可讓主機接收所有容器相關的指令，然後交由具備系統管理（root）權限執行的容器引擎來執行。如果這些 API 的連接埠因為蓄意或組態設定上的錯誤而提供給外部存取，就可能讓駭客有機會掌控主機，在主機上的容器內植入惡意程式，然後從遠端存取使用者的伺服器與硬體資源。(如：暴露在外的 Docker 主機遭歹徒植入虛擬加密貨幣挖礦惡意程式。)

弱密碼惹的禍!

資料來源：2019 年 07 月 11 日 Trend Labs 趨勢科技全球技術支援與研發中心

Silex 一天就癱瘓數千台物聯網設備

- 這是個特別有破壞性的惡意軟體，需要重新安裝韌體才能回復受感染的設備。惡意軟體使用已知的預設帳密（物聯網設備出廠時的標準使用者名稱和密碼）進入受害者系統。Cashdollar指出他所發現的病毒會針對ARM設備。他還看到了針對類Unix作業系統的版本。這代表如果Linux伺服器使用預設帳密，Silex也會對其造成影響。
- 它會先清空儲存裝置來癱瘓設備。接著會移除防火牆規則、刪除網路設定，最終完全停止設備。Silex受害者可能會以為是硬體故障，而不知道是遭到惡意軟體感染。

社交工程

資料來源： 2019 年 07 月 14 日 科技新報

駭客，竟然從廣達、Facebook 和 Google 3 家全球頂尖的高科技公司，盜走約新台幣 38 億元

- 這是一堂台灣公司都不能忽視的資安課。一名東歐駭客，竟然從廣達、Facebook 和 Google 3 家全球頂尖的高科技公司，盜走超過 1 億 2,100 萬美元（約新台幣 38 億元），整個過程有如電影《神鬼交鋒》。
- 2019 年 3 月 21 日，一則來自紐約的司法新聞，揭開這場騙局的真相：立陶宛男子黎瑪索斯卡（Evaldas Rimasauskas），因假冒台灣廣達公司身分，替廣達領取貨款，詐騙美國 Facebook 和 Google，被引渡到紐約受審。路透報導，黎瑪索斯卡在紐約曼哈頓法院認罪，同意歸還其中 4,970 萬美元，他騙走 Google 2,300 萬美元、Facebook 9,800 萬美元，創下全球社交工程被駭金額新紀錄，即使人抓到了，還有 1,730 萬美元不知去向。

社交工程

資料來源： 2019 年 07 月 14 日 科技新報

駭客，竟然從廣達、Facebook 和 Google 3 家全球頂尖的高科技公司，盜走約新台幣 38 億元

社交工程

資料來源： 2019 年 07 月 14 日 科技新報

駭客，竟然從廣達、Facebook 和 Google 3 家全球頂尖的高科技公司，盜走約新台幣 38 億元

關鍵 1：郵件帳號被駭客監控

- 這種犯罪手法可視為社交工程的進階運用，常見狀況是，犯罪者滲透進入郵件系統後，先只悄悄讀取這個人的往來信件。如果被駭的人是公司老闆，當他發現被害人的信箱收到預訂機票的信件，就可能趁他在飛機上，或是沒有辦法回信的短暫時間，替他發郵件向供應商「討債」，把錢匯進他的戶頭。
- 在歐洲，甚至有一種房仲詐騙，駭客入侵房仲的郵件系統，平常按兵不動，只默默讀取房仲的郵件，等到有房子成交，消費者要付款時，駭客就浮上水面，不但阻斷真房仲發出的郵件，還用他的身分發郵件，要消費者把買房子的錢匯到駭客指定的帳號，在英國，許多消費者因此被騙走終身積蓄。更可惡的是，駭客通常在英國時間星期五發動攻擊，等到錢一匯進假房仲的帳戶，就立刻把錢轉到亞洲等地的戶頭，利用銀行休假時間，創造洗錢的斷點。

社交工程

資料來源： 2019 年 07 月 14 日 科技新報

駭客，竟然從廣達、Facebook 和 Google 3 家全球頂尖的高科技公司，盜走約新台幣 38 億元

關鍵 2：真資訊加假帳號突破控管

- 犯罪者要花長時間才出手，因為他們鎖定有價值的對象後，就必須完全了解雙方交易的過程與節奏，甚至特定的專業術語，「就像在上另一個班」他形容，犯罪者必須讓自己就像參與這專案的一分子。等到時機成熟，犯罪者發出請款要求，因為專案名稱是真的，交易的過程都真實存在，而帳號資訊早透過正常程序動過手腳，才能通過所有流程，讓財會單位同意把錢付出去。
- 「你看過電影《神鬼交鋒》嗎？」他分析，很多高明的騙局，讓真訊息和假訊息糅合在一起，達成目的。「我辦過不少類似這樣的攻擊，其中一個案子，受害者、詐騙者和被冒名者，來往 2,000 封信，竟只有不到 5 封是真的，攻擊者完全融入整個供應鏈。」

社交工程

資料來源： 2019 年 07 月 14 日 科技新報

駭客，竟然從廣達、Facebook 和 Google 3 家全球頂尖的高科技公司，盜走約新台幣 38 億元

關鍵 2：真資訊加假帳號突破控管

- 「這麼高的交易金額，不用見面簽約嗎？」《財訊》記者問，林宏嘉推斷，駭客就是因為長時間監聽，知道付款規則、簽核等程序的複雜度，所以鎖定這些已經有穩定交易，要求付款不容易被起疑的供應鏈交易，再挑選一個雙方最難查證的時間點發動詐騙，這樣 3 分真 5 分像的情況下，往往容易一擊就成功得手。
- 錢轉入戶頭後，駭客集團最難的挑戰是如何創造斷點，阻絕國際警方追查。黎瑪索斯卡落網，是因為他就是扮演車手角色，不只廣達的假帳戶是用他的名義開的，他也曾直接從帳戶提款花用，因此被捕。但剩下的 7,000 多萬美元在哪裡？誰才是真正的主謀？目前不得而知。

社交工程

資料來源： 2019 年 07 月 14 日 科技新報

駭客，竟然從廣達、Facebook 和 Google 3 家全球頂尖的高科技公司，盜走約新台幣 38 億元

關鍵 3：製造斷點阻絕追查

- 勤業眾信聯合會計師事務所董事萬幼筠則觀察，「這種手法都經過非常精密的設計」，這類型的犯罪，犯罪者很了解業務內容才辦得到，有時，還可能涉及企業內部舞弊，請出關鍵人物出場配合，讓公司做出錯誤的判斷。
- 《財訊》調查發現，廣達絕不是唯一個案，當駭客攻擊愈來愈有規模、手法愈來愈精細，連全球大廠都難逃資安威脅。台灣風險正在上升，一股闇黑勢力正在擴散，已成為重要的國安問題。

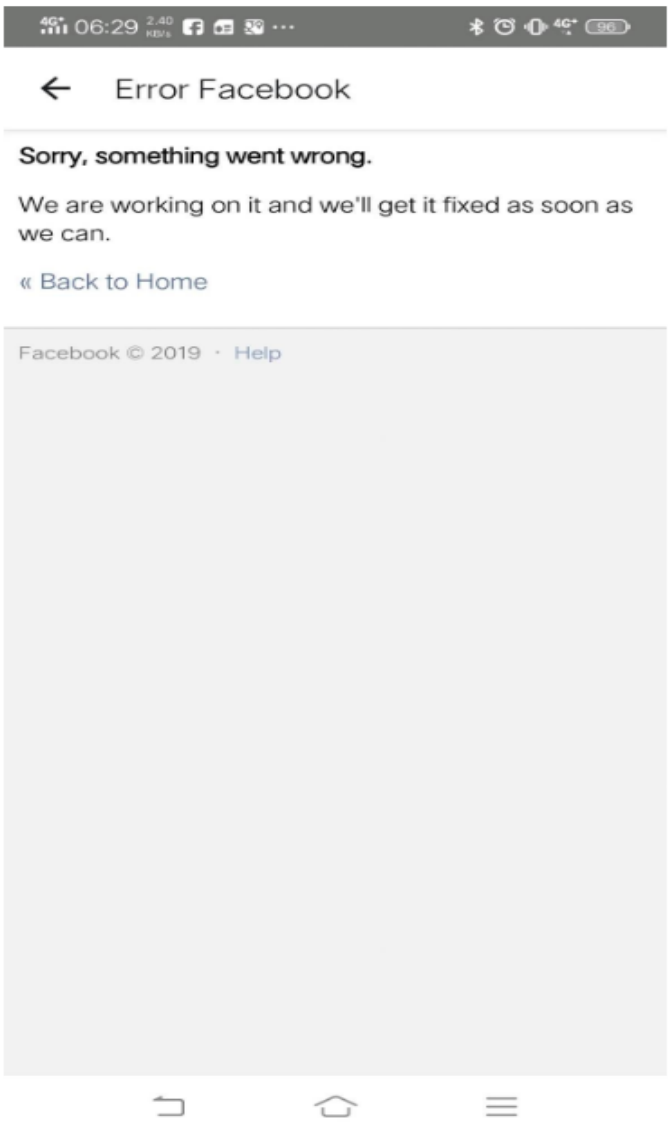
臉書當機13mins「動態全消失」...桌機手機都掛！

資料來源： 2019 年 07 月 18 日 ETTODAY新聞雲

臉書桌面板在今日早上約6點25分開始，出現大當機現象，隨後手機板也不能用，動態牆上直接一片空白，或是看不到新的貼文，更有人的頁面顯示「抱歉，有某些錯誤發生」，不只在台灣，國外也有許多網友轉戰推特哀嚎，目前臉書官方尚未有回應。

▼桌機或手機板都出現錯誤訊息。（圖／翻攝自臉書）

臉書當機13mins「動態全消失」...桌機手機都掛！



資料來源： 2019 年 07 月 18 日 ETTODAY新聞雲

駭客賺錢

資料來源： 2019 年 08 月 06 日 TVBS新聞網

北韓四度射彈！路透：駭客網攻偷走638億

- 北韓今天凌晨又發射兩枚飛彈，這是兩星期來第4度試射，北韓顯然是對美韓聯合軍演表達不滿。不過遭制裁的北韓，為何有錢發展新武器？路透社取得一份聯合國機密報告，顯示北韓駭客對17個國家的金融機構、加密貨幣交易所發動35次網攻，竊取資金跟洗錢，偷了至少20億美元，約台幣638億，來突破制裁造成的經濟困境。

圖 / 達志影像美聯社

別亂用充電線！

資料來源： 2019 年 08 月 19 日 科技報橘

駭客在 USB 接頭植入晶片，遠距入侵電腦竊取資料！

- 駭客入侵電腦的方式千奇百怪，任何看似無害的東西都可以變成工具。在 USB 充電線裡面置入無線網路晶片，只要接上電腦，就會被電源啟動，讓駭客可以遠距存取資料或載入惡意軟體。
- 不只是充電線，任何有 USB 的裝置都可以植入該晶片，例如 USB 小檯燈、USB 電風扇等等，都是潛在的風險。

可入侵電腦的傳輸線，首圖來源：_MG_ Twitter

帶動家中Wi-Fi成長的動力是智慧家庭

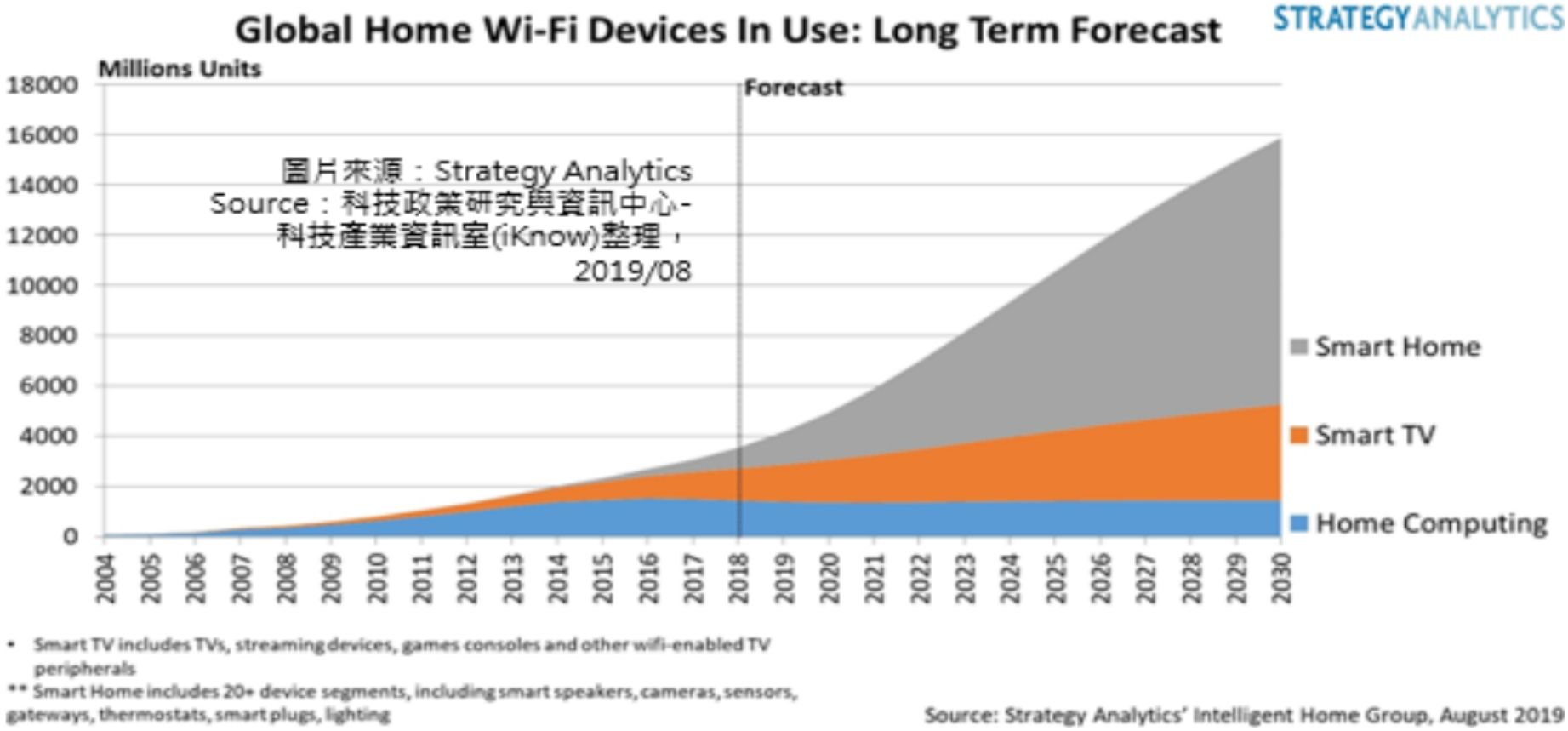
資料來源： 2019 年 08 月 14 日 國家實驗研究院

- 現今全球家庭中正在使用的Wi-Fi裝置數高達50億台。未來幾年隨著Wi-Fi從Wi-Fi 5（802.11ac）轉換至Wi-Fi 6（802.11ax）勢必帶動Wi-Fi裝置的起飛，至2030年之時，全球使用Wi-Fi裝置數將成長至170億台。也就是說，無線家庭將成為21世紀初帶動Wi-Fi起飛的關鍵因素之一。
- 進入2020年，智慧家庭裝置將取代智慧電視佔據第二名的位子，甚至長期看起來，智慧家庭裝置將佔所有家中使用WiFi的比例達到60%以上。內建Wi-Fi功能的智慧家庭裝置包含：智慧音箱，智慧家電，攝像機和恆溫器等。

帶動家中Wi-Fi成長的動力是智慧家庭

資料來源： 2019 年 08 月 14 日 國家實驗研究院

全球家庭WiFi裝置使用趨勢



圖、全球家庭WiFi裝置使用趨勢

勒索軟體驚傳大規模攻擊臺灣醫療院所!

資料來源：2019 年 09 月 05 日 iThome

臺灣22家醫療院所驚傳勒索軟體攻擊

8月31日國內傳出10多家醫療院所遭受勒索軟體攻擊，遇害時間自29日凌晨開始，衛生福利部資訊室發出公告，說明初步清查結果，至9月1日止，受到本次病毒影響的機構，共有22家醫院。

衛生福利部資訊室指出，初步查證結果顯示，部分醫院主機被駭客當成跳板，經由VPN網路進行攻擊。

北韓網攻攫飛彈資金-美制裁3駭客團

資料來源： 2019 年 09 月 15 日 聯合新聞網

- 美國財政部13日宣布制裁3個由北韓官方所支持的駭客團體(Lazarus Group、Bluenoroff以及Andariel)，並且揭露其透過攻擊關鍵基礎設施攫取非法資金，最終全挹注到武器與飛彈計畫，也令受害美國企業面臨是否支付贖金的兩難。

美國財政部13日宣布制裁3個由北韓官方所支持的駭客團體，並且揭露其透過攻擊關鍵基礎設施攫取非法資金，最終全挹注到武器與飛彈計畫，也令受害美國企業面臨是否支付贖金的兩難， 美聯社

北韓網攻攫飛彈資金-美制裁3駭客團

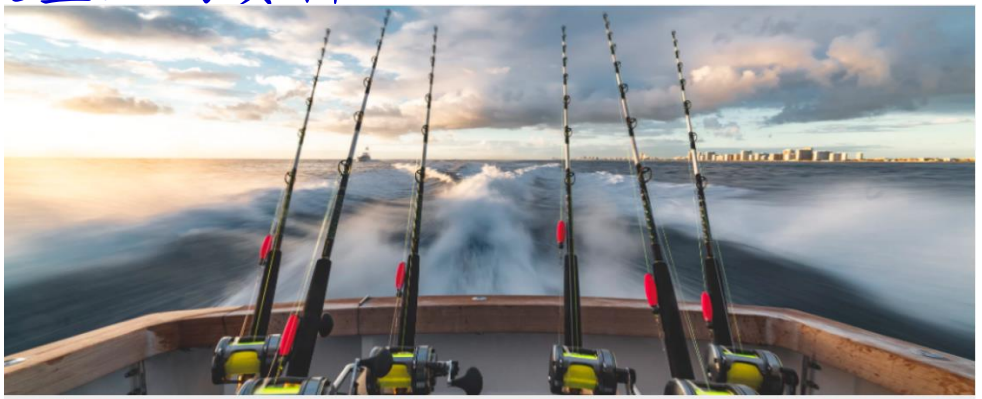
資料來源： 2019 年 09 月 15 日 聯合新聞網

- Lazarus Group兩年前以惡意軟體WannaCry發動網攻，造成全球性的廣泛破壞，英國國家醫療保健服務（NHS）轄下的醫院與救護車運作癱瘓，估計逾1.9萬次預約看診被迫取消，損失成本逾1.12億美元；日產（Nissan）、雷諾（Renault）等車商的汽車生產，以及聯邦快遞（FedEx）海運等都一度中斷，另還有多間公司受害。
- Bluenoroff自2014年以來透過各種手段，從全球各金融機構竊得超過10億美元，包含攻擊環球銀行金融電信協會（SWIFT）；Anadriel則被資安公司發現，企圖駭入自動提款機竊取信用卡資訊並搬走現金，或是竊取銀行的顧客資料向黑市兜售。

網路釣魚攻擊頻傳，大學與匿名爆料平臺遭鎖定

資料來源： 2019 年 09 月 17 日 iThome

- 暗網研究人員Sh1ttyKids在上周末發現，衛報（The Guardian）的SecureDrop匿名爆料平台遭到網釣駭客鎖定，駭客建立了一個假冒為衛報的SecureDrop平台，以騙取爆料者的代號，還在網釣頁面上推銷一個惡意的Android程式。
- 探索了網釣頁面所推銷的Android程式，結果發現此一標榜為可隱藏爆料者位置的Android程式，實為一遠端存取木馬程式，能夠來監控爆料者的活動、所在地、通話、文字、拍照、執行其它命令，或是竊取裝置上的資料。



情境示意圖，Photo by stephen momot on https://unsplash.com/photos/UivGzIDhVyw

伊朗駭客集團Cobalt Dickens於全球大學展開大規模網釣行動

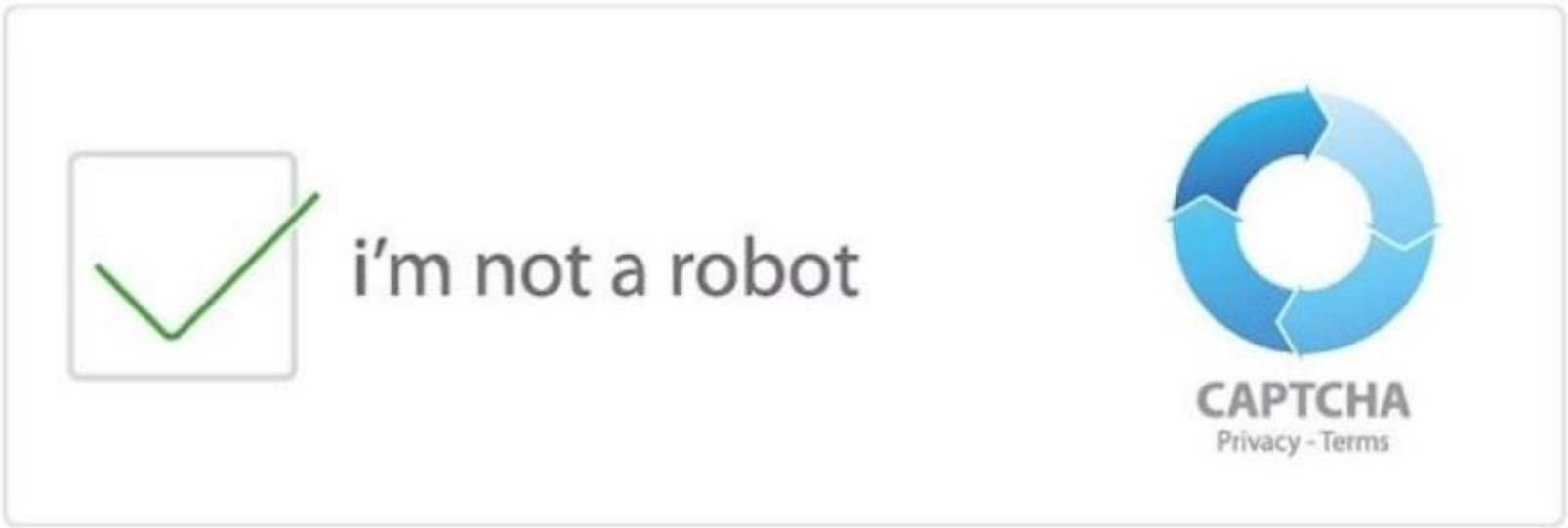
資料來源： 2019 年 09 月 16 日 iThome

- 資安業者Secureworks上周指出，由伊朗政府掌控的駭客集團Cobalt Dickens在今年7、8月間再度鎖定全球大學展開網釣攻擊，企圖竊取大學的智慧財產，光是這兩個月就有超過60所大學被Cobalt Dickens鎖定。

今年暑假發動的這波網釣攻擊，信中內容宣稱學生的圖書館帳號已經過期，並附上連結，要使用者點選登入才能取回服務存取權。在使用者輸入憑證之後，憑證一方面落入駭客之手，另一方面也會將使用者導至正常的校方網站，讓受害學生遭駭之後完全無法查覺有異。情境示意圖，Photo by Victuallers on shorturl.at/kGHK8 (CC BY-SA 3.0)

驗證真人機制遭駭客利用變釣魚網頁新工具

資料來源： 2019 年 09 月 18 日 聯合新聞網



驗證真人機制遭駭客利用變釣魚網頁新工具

資料來源： 2019 年 09 月 18 日 聯合新聞網

- Captcha是用來認證使用者是否是真人的圖靈測試機制，過去最常見的就是在數張圖片中點選一張正確的圖片。不過，最近有公司發現，有駭客利用Captcha這個機制，來繞資安過電子郵件的安全防護機制，讓原本電子郵件用來過濾釣魚網頁的機器人檢查機制無法檢查這個釣魚網頁，然後如果你是真的人類的話，就會將你導引到釣魚網頁上。
- 防毒軟體要能夠發揮阻擋釣魚網頁的前提有兩個，第一就是他必須要有一個知道有哪些釣魚網頁的網址資料庫，第二就是他必須要知道你的Email中是否有含有這個網址，或是要將你導向這個網址。

我如何讓 50 個惡意文件騙過 AI 安防系統？

資料來源： 2019 年 09 月 27 日 大數據文摘

- AI 當道，許多企業與政府單位開始在安防系統內導入 AI，提升安全性。然而道高一尺魔高一丈，不管系統在怎麼嚴密，就是有駭客可以破解這些系統。
- 網絡安全平台 Endgame、MRG-Effitas 和 VM-Ray 舉辦一場駭客大賽，邀請工程師來破解他們的安防系統。有個工程師成功破解他們的 AI 系統，讓 50 個惡意程式成功運作。

台大醫院證實遭駭疑有資料外洩 調查局介入調查

資料來源： 2019年09月28日自由時報

- 教育部在今年8月初接到台大醫院通報，指遠端系統疑似被駭，駭客是從分院駭入總院資料庫，因為沒有資料外洩，故依資安規定通報為一級事件，但9月20日再接到台大醫院通報，因駭入權限提高且疑似有資料外洩，因此從1級事件升級為3級事件，教育部速依規定向行政院通報，已由行政院技術服務處協助調查。

台大醫院（圖）系統傳遭駭客入侵，教育部已依規定向行政院通報，經證實已升級為3級資安事件。（資料照）

課後評量

- 資 訊 科 技 與 競 爭 優 勢 -

感謝您的聆聽！