TREND MICRO research

映對未來

對抗無所不在的持續性威脅

趨勢科技
2019年資安預測

內容

04 消費者

08 企業

12 政府機關

15 資安產業

18 工業控制系統

20 雲端基礎架構

23 智慧家庭

26 為接下來的一年預做準備

作者：Trend Micro Research

圖片授權：Shutterstock.com

趨勢科技
2019 年資安預測

2019 年及未來影響科技和資安產業最大的趨勢包括：不斷成長的大量資料促使人工智慧與機器學習技術崛起、雲端運算在全球企業更加普及，以及智慧裝置、智慧家庭、智慧工廠持續發展，更不用說還有即將於 2020 年上路並進一步提升網際網路速度的 5G 最新行動通訊技術。除此之外，2019 年也是政治社會發展的重要一年，包括：英國將正式退出歐盟，還有許多國家即將舉行大選。這些科技與政治上的演變，將直接左右 2019 年的資安情勢。

網路犯罪集團預料將如往常一樣，持續鎖定全球最新發展趨勢，鎖定容易下手、迅速海撈一票的機會。2019 年，數位入侵的影響層面和效應將更加深遠：利用外洩的帳號密碼從事詐騙的情況將越來越多、性勒索將危害更多生命、各國積極拓展網路勢力將間接造成一些傷害。不僅如此，網路宣傳與假新聞的盛行，某種程度上將左右一國的命運。因此，企業將面臨資安人才缺乏的全新挑戰，資安專家不僅難尋、而且昂貴，進而使得委外的情況增加。同時，資安險 (cyber insurance) 業務也將出現前所未有的成長，因為資料外洩與違反法規的罰鍰越來越高。

我們對未來一年的資安預測是根據我們內部研究專家對當前與新興科技、使用者行為、市場潮流以及這些因素對威脅情勢的影響所做的分析。我們考量其主要影響範圍以及科技與政治變革的擴散特性，將這些預測分成幾大領域。

消費者

04

社交工程網路釣魚將取代漏洞攻擊套件成為主要攻擊管道

網路釣魚案例在 2019 年將大幅增加。網路釣魚攻擊 (也就是歹徒假冒信譽良好的個人或企業機構，誘騙受害者提供個人敏感資訊的一種詐騙) 已經行之多年。然而經過多年的演進，歹徒已找到方法在犯罪過程當中盡可能避免與使用者接觸就能得逞。就好比漏洞攻擊套件之所以盛行，正因為這類攻擊能自動根據受害者的軟體版本來判斷該利用哪一個漏洞來進行攻擊。

然而近年來，絕大多數裝置使用相同軟體或作業系統的市場壟斷情況已逐漸瓦解。五年前，Windows 為王[1]，但現在，沒有單一作業系統能夠獨占百分之五十以上的市場[2]。網路犯罪集團必須做出抉擇：該花費好幾小時的時間來開發針對特定電腦族群的漏洞攻擊套件，並且面臨廠商可能推出修補更新來因應的情況，或者回歸到最歷久不衰、而且無真正解藥的詐騙伎倆，也就是社交工程詐騙。

未來，漏洞攻擊套件的活動將持續減少，這樣的情況我們觀察已經持續好一段時間。

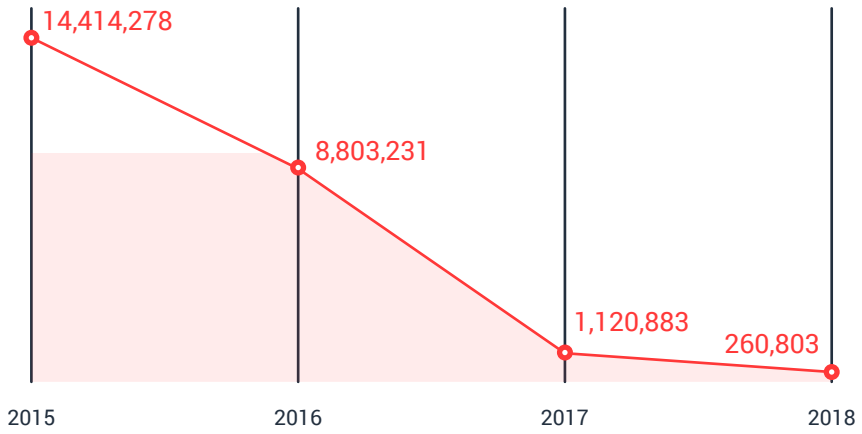


圖 1：已攔截的漏洞攻擊套件活動逐年減少 (根據趨勢科技 Smart Protection Network™ 全球威脅情報網 2018 年第三季的統計資料)。

根據我們所蒐集到的資料，網路釣魚攻擊正逐漸興起，而這樣的趨勢將持續至 2019 年。

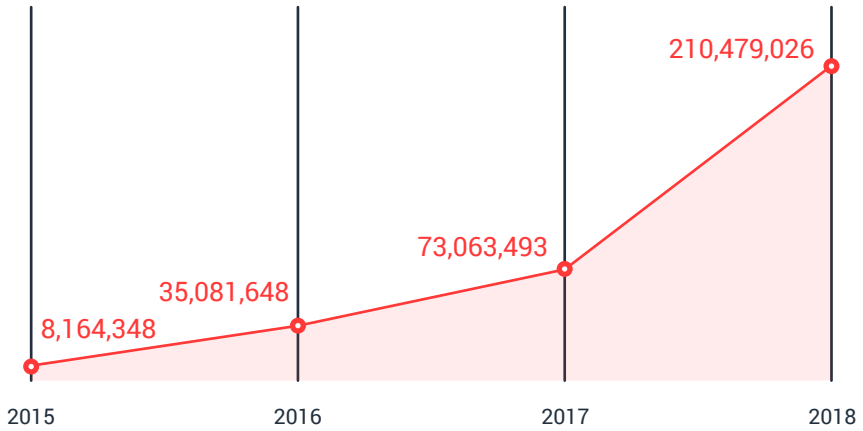


圖 2：已攔截的網路釣魚相關網址數量逐年攀升 (根據趨勢科技 Smart Protection Network 全球威脅情報網 2018 年第三季的統計資料)。

網路釣魚攻擊不僅出現在電子郵件，也出現在手機簡訊和即時通訊當中。一般來說，網路犯罪集團大多騙取使用者的網路銀行帳號登入憑證，但也會騙取雲端儲存或其他服務的帳號。除此之外，未來也將看到一些全新的攻擊型態，例如：SIM 卡劫持 (SIM-jacking)，這類攻擊非常仰賴社交工程技巧。在 SIM 卡劫持案件當中，歹徒會假冒受害者名義，向電信公司謊稱自己的 SIM 卡遺失，並說服電信公司技術支援人員將遺失的 SIM 卡移轉至歹徒自己的 SIM 卡上，如此一來就等於掌控了受害者的網路身分，因為網路帳號通常會與行動電話號碼連結[3]。

至於社交工程詐騙的內容，我們預料網路犯罪集團將利用真實世界的運動賽事或政治事件，例如即將於日本舉行的 2019 年世界盃橄欖球賽 (Rugby World Cup)、2020 年東京夏季奧運 (Summer Olympics in Tokyo) 以及世界各國即將舉行的選舉活動。網路犯罪集團很可能架設一些假冒的網站來銷售一些預售門票、刊登一些宣稱提供免費或折價商品的廣告，或者散發假冒選舉或賽事相關內容的惡意連結。

▶ 聊天機器人將成為歹徒的利用工具

線上溝通已經不再侷限於電子郵件。隨著越來越多科技愛好者和上網成癮的年輕人整天黏在網際網路上，即時通訊應用程式已成為人們之間或是個人與企業之間一項廣為接受的通訊方式，可說是一種另類的線上客戶服務或支援。這項新的溝通形式，再加上先前所提歹徒開始回歸到社交工程詐騙伎倆，將為網路犯罪集團開拓新的機會。

我們預料利用聊天機器人 (Chatbot) 的詐騙攻擊在 2019 年將變得猖獗。同樣地，電話詐騙也會更加進步，開始利用預先錄製好的語音訊息與互動式語音應答 (IVR) 系統。歹徒會設計一個聊天機器人來先與受害者建立對話，創造一個自然的情境好讓後面可以發送一個網路釣魚連結給受害者，或者騙取受害者的個人資訊。歹徒會使出各式各樣的犯罪手法，包括：竄改訂單、在受害者電腦上安裝遠端遙控木馬程式 (RAT)，甚至進行勒索。

▶ 網路名人帳號將成為水坑式攻擊的工具

隨著社交工程手法越來越狡詐，**網路犯罪集團很可能會駭入知名 YouTuber 及其他「網紅」的社群媒體帳號來當成詐騙工具。**網路犯罪集團會專挑追隨人數上百萬的名人下手，利用針對性網路釣魚或類似手法來騙取這些帳號的密碼。當然，這類攻擊很可能會在主流媒體上引起軒然大波，但就算事件曝光，很可能也已有上百萬追隨者成為駭客的受害者。其電腦很可能已被植入資訊竊取程式或者變成殭屍網路的成員，暗中幫駭客發動分散式阻斷服務 (DDoS) 攻擊，或者在幫駭客挖礦賺取虛擬加密貨幣，甚至連他們自己的帳號都已變成歹徒的利用工具。

▶ 網路上將出現歹徒大規模運用外洩帳號密碼的實際案例

根據最近一份 Ponemon Institute 與 Akamai 所做的報告指出，密碼填充 (credential stuffing) 攻擊的情況日益嚴重，這是一種透過自動化方式將某處偷來的同一組帳號密碼嘗試登入多個其他熱門網站的攻擊手法[4]。由於過去所曾發生多次大規模資料外洩事件，再加上歹徒知道許多使用者習慣在不同網站上使用相同的帳號密碼，因此我們相信，**網路犯罪集團利用資料外洩事件偷來的帳號密碼從事非法交易的情況將會暴增。**

網路犯罪集團會使用偷來的帳號密碼在真實世界從事一些詐騙以獲取利潤，例如：註冊累積里程或點數回饋方案以竊取相關回饋。此外，也會利用這些帳號在社群媒體上註冊一些假鄉民帳號來發動網路宣傳，或者在一些消費性入口網站發送操弄評價的貼文，或者在一些社群民調上灌票等等，歹徒有無限的發展可能。

▶ 性勒索案例將會增加

青少年或青年遭到非錢財方式的勒索案例將會增加，例如「性勒索」即為一例。雖然，透過黑函的勒索行為不一定能夠得逞，但由於這類攻擊非常具針對性針，因此，受害者私下很可能會認真考慮歹徒的要求，不論是錢或性方面的要求。**隨著性勒索的案例更加常見[5、6、7]，這類攻擊在 2019 年所影響、甚至危害的生命將越來越多。**

企業

▶ 經由家用網路在家上班的情況將為企業帶來類似個人自備裝置 (BYOD) 的資安風險

企業 IT 人員將發現越來越多攻擊來自員工家中連上網際網路的裝置。這是兩大趨勢匯流 — 遠距工作逐漸興起，以及越來越多智慧裝置進入家庭 — 所帶來的一個令人意想不到但卻無可避免的結果。

越來越多員工因為公司提供彈性上班政策而在家工作 (亦稱為電子通勤、行動人力或在家上班)。根據 Gallup 的報告，美國 2016 年約有 43% 的員工在家工作，較 2012 年的 39% 略為成長[8]。此外，根據 Polycom 所做的一項全球人力調查顯示，2017 年有將近三分之二的員工善用「彈性上班地點」的政策，較 2012 年的 14% 大幅成長[9]。但如同 BYOD 個人自備裝置政策一樣，員工在家上班會帶來企業資料管理上的挑戰，因為員工會透過家用網路來連上雲端應用程式或協同作業軟體以便能夠聊天、視訊會議或分享檔案。

目前，家用網路通常會連接印表機及一些員工在家中和工作上都會用到的儲存裝置，造成工作和私人用途不分的情況。不僅如此，遠端工作者的家用網路也開始出現越來越多智慧家庭裝置。IDC 預測，所有類型的智慧家庭裝置從現在至 2022 年將呈現二位數成長[10]。不幸的是，對資安來說，這意味著員工「家用網路」上的每一個不安全的裝置都將對「企業網路」造成威脅，成為駭客可能利用的入侵點。

例如，我們的研究人員已經證明，智慧喇叭也可被用來外洩資料[11]。2019 年將出現一些針對性攻擊案例利用智慧喇叭的弱點來從員工家用網路進入企業網路。

▶ GDPR 監理機關將對第一個大型違規案件開罰年營業額 4% 的最高罰鍰

歐盟 (EU) 通用資料保護法 (General Data Protection Regulation，簡稱 GDPR) 的監理機關至今尚未立即展現其公權力。但不用多久，他們應該就會挑選一個違規的大型企業來開鍘，處以全球年營業額 4% 的最高罰鍰，藉此殺雞儆猴。

就隱私權保障而言，GDPR 是一個相對較為成熟的法規。事實上，過去十多年來已有許多企業在先前的資料保護規範 (Data Protection Directive) 底下挨罰[12]，因此，違規的企業應該很快就會感受到這項法規的威力。此外，由於 GDPR 的緣故，2019 年整體而言將出現比前一年更多的資料外洩通報案件，因為已有某些監理機關因需要調查的新通報案件過多而疲於奔命[13]。往好處想，向監理機關通報資料外洩事件，有助於企業更加了解歹徒如何駭入其企業。

除此之外，也無可避免地會讓一些法規當中較難遵守的細節浮上檯面，促使監理機關對此加以澄清或者進一步詳細說明企業需要建置哪些資安技術。**同時，企業也將被迫重新思考其目前以資料探勘 (data-mining) 為基礎的廣告模式是否值得，因為萬一不小心違反資料保護法，其代價相當可觀。事實上，我們預測，到了 2020 年，新的企業應用程式將有高達 75% 必須在法規遵循與安全之間做出艱難取捨。**儘管隱私權和安全兩者並非不能兼顧，但保障資料隱私權的一些做法將不利於企業徹底掌握資安威脅的來源並取得進一步的詳細資訊。

真實世界所發生的事件將成為社交工程攻擊的誘餌

在前一節，我們預測網路釣魚攻擊將越來越猖獗。在企業環境當中，**真實世界所發生的事件，例如許多國家 2019 年即將舉行的大選、2020 年東京夏季奧運，甚至像政治局勢不穩以及英國脫歐的議題，都將成為歹徒對企業發動社交工程攻擊的誘餌。**我們預測這類事件和議題將引來許多網路犯罪活動，運用在一些針對企業的網路犯罪、電子郵件詐騙、社交工程攻擊等等。

除此之外，網路犯罪集團也將投入更多心力，透過員工的社群媒體帳號挖掘更多關於員工的資訊，藉此精心策畫更具說服力的網路釣魚攻擊。

變臉詐騙的對象將轉向比現在低兩階的員工

變臉詐騙 (Business Email Compromise，簡稱 BEC) 依然是歹徒向企業詐財非常強大且獲利豐厚的犯罪手法。我們相信，由於企業 CXX 高層主管遭到變臉詐騙的新聞經常在媒體上曝光[14]，因此，**網路犯罪集團未來將降低其攻擊對象的層級。**例如，網路犯罪集團可能會轉而攻擊 CxO 的秘書、助理，或是財務部門總監、經理之類的職務。

企業自動化將是商業流程入侵的最新難題

商業流程入侵 (Business Process Compromise，簡稱 BPC) 是一種歹徒暗中竄改企業流程以從中獲利的詐騙手法，同時也是未來企業仍將面對的風險之一。**而企業自動化將使得企業更難保護其商業流程以防範 BPC 攻擊。**根據 Forrester 預測，2019 年，企業自動化將導致 10% 的工作流失[15]。

隨著企業有越來越多監控相關的工作皆透過軟體或線上應用程式來達成，企業若未在一開始就做好防範措施，歹徒將有更多機會可以駭入這類流程。自動化軟體很可能本身就含有漏洞，而且在與現有系統整合時也可能形成資安缺口。不僅如此，由於歹徒也會試圖尋找企業的供應商、合作夥伴或外包廠商的弱點來達成其目的，因此自動化也將為供應鏈帶來資安風險。

歹徒將持續探索數位勒索的應用領域

根據我們前瞻研究團隊針對網路黑函 (也就是數位勒索) 的深入調查結果[16]，我們預料這項網路犯罪獲利模式將出現更細膩的犯罪手法。2019 年，**網路犯罪集團將根據企業可能被 GDPR 開罰的最高罰鍰來做為他們向該企業勒索的贖金參考。**歹徒所打的如意算盤是：企業在驚嚇、惶恐之餘，很可能寧願支付贖金也不願因資料外洩曝光而受罰。

除此之外，也將出現一些以毀損企業品牌聲譽為要脅的網路勒索案例，歹徒可能會以停止製造不利企業的假新聞作為交換條件來向企業勒索一筆金額。

政府機關

▶ 在各種選舉的壓力之下，政府對抗假新聞的行動將被迫讓步

根據 Carnegie Europe 指出，2019 年歐盟即將經歷一場讓歐洲議會 (European Parliament) 徹底改組的選舉[17]，而希臘、波蘭和烏克蘭等國也將舉行自己的國內大選。此外，奈及利亞、南非以及亞洲地區的印度和印尼等多個國家也將舉行選舉。**2019 年，我們認為社群媒體在 2016 年之後所做的一些對抗假新聞的改善措施，仍不足以抗衡網路犯罪集團在這些選舉當中如洪水般的網路宣傳攻勢。**

如同我們的報告「The Fake News Machine: How Propagandists Abuse the Internet and Manipulate the Public」(假新聞製造機：宣傳者如何濫用網際網路來操弄大眾) 一文所指出，假新聞成功散播的三大要素：平台、動機、工具，只要其中一項被瓦解或失去操控能力就會破功[18]。然而，歹徒的動機永遠不會消失，而工具也很難禁止，因為同樣的工具很可能也用於正當用途。儘管各國政府已經出現管制社群媒體平台的聲音[19]，但我們相信這些網站應該不會有足夠的時間來徹底清除這些製造假新聞的網際網路頻道。除了取締假新聞的技術困難之外，任何一個幅員廣大的地區 (如歐盟) 都可能包含多種不同語言，而非如美國的社群媒體網站，基本上大多以英文的內容為主。

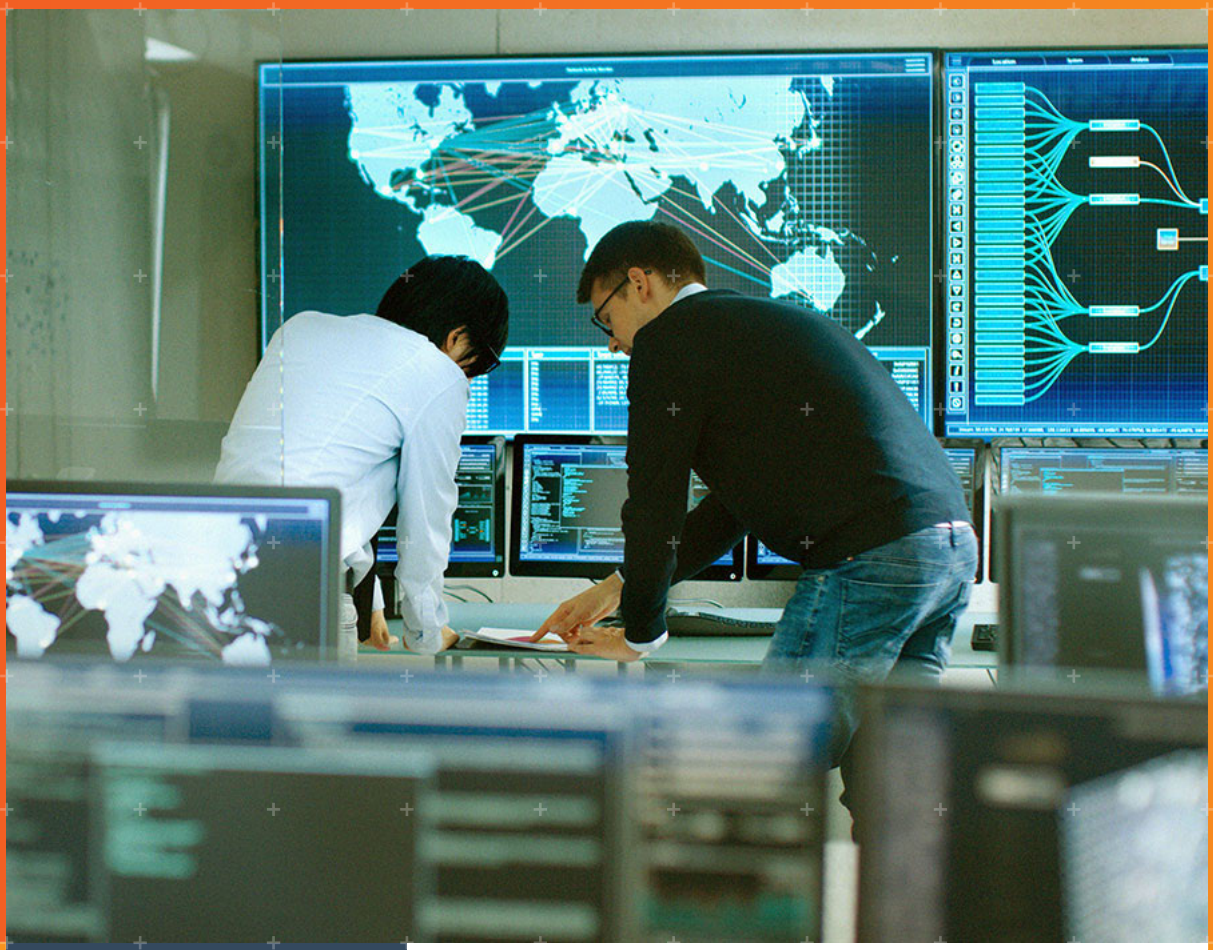
更不幸的是，歹徒用來散布假新聞以操弄大眾輿論的技術，甚至變得越來越強大。一個很好的例子就是 Adobe 所稱的「Photoshop for audio」語音編輯軟體[20]，就很可能被拿來當成欺騙的工具。雖然 Adobe 尚未釋出更多有關該軟體的相關資訊，但卻已預告了一個更真假難辨的未來。

▶ 無辜的受害者將受困在國與國之間的網路戰火當中

原本就敵對的國家，其彼此間的針對性網路攻擊仍將持續下去，但 2019 年，一些通常不會被點名的國家也將投入這場戰爭。不論原因為何，世界各國正不斷強化自己的網路攻防能力，因此會在背後支持其國內的駭客，不管是為了攻擊而做準備，或者是為了因應可能或即將遭到的攻擊。**壞消息是，這樣的發展將波及與這類網路攻防毫不相干的無辜受害者。**不論個人、企業，甚至一些對社會大眾影響深遠的大型企業，都很可能受困在國與國之間的紛爭與戰火當中。這樣的情況，已經出現在 WannaCry[21] 和 NotPetya[22] 的案例當中，但這類連帶傷及無辜的情況只會增加不會減少。

▶ 監理機關將加強管制

今日資安相關的對話將促使政府加強管制，不單針對隱私權的事物，也將涵蓋消費性和工業用物聯網 (IoT & IIoT)。在美國，加州法律要求智慧裝置製造商必須強制使用高強度的密碼[23]，但這只不過是朝此方向邁進的一小步而已。我們預料 2019 年將會有某些國家開始著手立法禁止消費者和產業機構使用不安全的 IoT 裝置。



資安產業

▶ 網路犯罪集團將運用更多魚目混珠的技巧

為了因應資安廠商推出的新技術，尤其是機器學習在網路資安領域重新獲得青睞，**網路犯罪集團將運用更高的技巧來「魚目混珠」。**歹徒將不斷開發出所謂「就地取材」的技巧，也就是將一些日常運算裝置用於原本設計之外的用途，並且在網路上流傳。目前我們所看到的這類技巧有：

- 使用一些非傳統常見副檔名的惡意檔案，例如：URL、.IQY、.ISO、.PUB 及 .WIZ。
- 減少對一般執行檔的依賴，例如採用「無檔案式」元件、PowerShell、腳本以及巨集。
- 採用經過數位簽章的惡意程式，如同我們的研究報告「Exploring the Long Tail of (Malicious) Software Downloads」一文所指出[24]，這類技巧目前已經相當普遍，而且由於成效良好，因此未來仍將持續下去。
- 採用超越先前發現技巧的最新惡意程式啟動方法，如：Mshta、Rundll32、Regasm 或 Regsvr32。[25]
- 利用電子郵件帳號或雲端儲存服務和應用程式來當成幕後操縱 (C&C) 的存取點、下載點或資料外傳匯集點。
- 以最小幅度篡改或感染正常的系統檔案。

當網路犯罪集團採用上述技巧來感染系統時，單靠機器學習技術來防禦資安威脅的企業將面臨嚴重考驗。我們預料這些網路犯罪技巧在 2019 年將越來越盛行。

▶ 99.99% 的漏洞攻擊依然不會是零時差漏洞攻擊

零時差漏洞攻擊，也就是惡意程式利用軟體廠商所不知情的漏洞來發動攻擊，一直是資安界的注目焦點之一。每當有這類新的攻擊出現，必定也會登上媒體版面，因為這類攻擊少之又少。

一方面，網路犯罪集團要在軟體當中發現從未被發掘的漏洞，不是一件容易的事，因為像趨勢科技 Zero Day Initiative (ZDI) 這類的漏洞懸賞計畫，已讓漏洞研究人員有一個正常揭發漏洞又能獲得適當回報的管道。而且就算駭客真的發現這樣的漏洞，軟體廠商只要一發現，就會立即採取適當的措施來因應。但從另一個角度看，網路犯罪集團下手的最佳時機，其實正是廠商發布新的修

補更新到企業真正將更新部署到系統上的這段空窗期。負責修補更新的系統管理員，須擬定一套妥善的策略再加上充足的時間來全面套用修補更新，而這就給了網路犯罪集團足夠的時間來發動攻擊。由於漏洞相關的細節在漏洞公開時也隨之發布，因此，讓歹徒節省了很多研究該如何運用漏洞的時間。

2019年，漏洞攻擊的成功方程式是：利用一些已經釋出修補更新、但企業卻尚未套用更新的漏洞。這些漏洞可能有數週、甚至數個月的時間可以讓歹徒利用。未來，這類利用修補空窗期的漏洞攻擊，將是網路資安的一大禍源。

極具針對性的攻擊將利用人工智慧開發的技巧

一些財力雄厚的犯罪集團所發動的針對性攻擊，將開始使用人工智慧 (AI) 所開發的技巧來進行情蒐偵查。歹徒將利用 AI 來預測目標機構高階主管或其他關鍵人物的動向。讓 AI 幫助他們判斷這些企業高階主管未來將會出現在什麼地方，例如：公司幫他們訂的飯店、會議舉辦的餐廳，以及其他有助於預測他們未來出席地點的偏好。

同樣地，資安廠商也會開始提升其 AI 防禦技巧，而企業資安團隊也會開始利用 AI，透過像機器學習這類的方式更深一層了解企業日常的活動，以便在企業活動出現異樣而有資安疑慮的第一時間立即提供警示。像這樣的未來場景，都讓我們有機會一窺 AI 技術的未來發展以及對資安的意義。

PRODUCTION
Dashboard
Monitoring
Problems
Group and tag
Tactical views
System
Configuration
External

工業控制系統

▶ 針對真實世界工業控制系統 (ICS) 的攻擊將成為一項日益嚴重的問題

一些正在培養及鍛鍊網路攻防技巧的國家，會拿較小國家的關鍵基礎架構來當成攻擊對象。他們可能利用這種方式來獲得一些政治或軍事上的優勢，或針對一些尚無報復能力的國家測試其攻擊能力，或是任何其他可能的動機。至於攻擊目標是水、電力設施或製造業的工業控制系統 (ICS)，將視攻擊者的意圖或機會而定。但不管怎樣，這類事件所突顯的正是歐盟網路資訊安全規範 (NIS Directive) 所希望管制的弱點，該規範的適用對象正是管理國家基礎關鍵設施的營運單位[26]。

這類攻擊就如同針對性攻擊，一開始會先對攻擊目標進行一番偵查，直到情蒐目的達成為止。工業控制系統一旦遭到攻擊，其可能影響將包括營運停擺、設備損壞、間接財務損失等等，最糟的情況還可能造成人員傷亡。

▶ 人機介面 (HMI) 的弱點依然是工業控制系統最主要的漏洞根源

根據 ZDI 漏洞懸賞計畫的資料，工業控制系統中有很大一部分的漏洞都出現在其監控與資料擷取 (SCADA) 系統軟體的人機介面 (HMI) [27、28]，這是廠房內各種不同診斷與控制器模組的主要管理界面。一般來說，工業控制系統包含了分散式控制系統 (DCS) 和各種現場裝置以及 SCADA 系統，而所有的系統都有自己的 HMI。**預料 2019 年將有更多關於 HMI 的漏洞被揭露。**

目前，這類軟體是漏洞研究人員比較能夠掌握的部份。眾所周知，基於各種因素，這類 HMI 軟體不像 Microsoft 和 Adobe 的軟體那樣受到嚴密保護，而且也不如大眾所想像的，會在自己獨立隔離的環境當中執行[29]。除此之外，HMI 軟體的維護和升級也會受到原廠被併購或區域性廠商互相整併這類的市場變化所影響或阻礙。

雲端基礎架構

▶ 移轉至雲端時的安全設定錯誤將導致更多資料外洩發生

將資料移轉至雲端，是一項牽涉到整個企業的工作，需要完備的規劃、人力資源以及多方參與，就如同將辦公室遷移到另一個地點一樣，甚至可能更多。每一家公司移轉至雲端的情況 (包括規模和步調) 皆不盡相同，此外，就算是業界最佳實務原則也需視企業的個別情況和實際需求而微調。

我們預料將看到更多大型資料外洩事件是因為移轉至雲端時的組態設定錯誤而直接導致。將企業內系統或私有雲上的資料遷移至某家雲端服務，很可能讓企業因而暴露在資安風險當中，除非企業能確切掌握其資料所面臨的狀況。或許雲端資料庫在預設的情況下會設為私密，但如果是來自外部的資料庫，有可能就會保留著原本的權限設定。因此，資料庫的存取政策在整個過程當中就必須確實掌握、貫徹並維持。

▶ 雲端運算實體將可能被歹徒用來挖礦

雲端挖礦是當今虛擬加密貨幣掏金熱下另一個合法挖礦的選擇。挖礦者不必自己投資硬體設備，只須向雲端廠商購買 CPU 運算能力就能開始挖礦。這類商業模式有各種不同的資費方案可供選擇，但雲端挖礦最吸引人的一點是容易入門且容易維護，這對那些在硬體設備和電力供應方面有困難的人來說確實方便。

然而換個角度想像一下，**網路犯罪集團也有越來越多人想要躍躍欲試，他們將竊取一些雲端帳號來從事挖礦，或者暗中掌控一些挖礦帳號。**換句話說，2018 年媒體上報導的雲端資源遭駭客挾持用來挖礦的事件[30]，其實已預告了未來的發展趨勢，而非僅是網路犯罪集團一時興起的嘗試而已。網路上已經有現成的雲端資料庫掃瞄工具，再加上每一個雲端部署環境都有許多資安設定必須正確設定，因此網路犯罪集團自然會朝這個方向來尋找可利用的漏洞。此外，我們也預料挖礦惡意程式也會盡可能調節其占用的資源來降低被人發現的機會。

▶ 更多雲端相關的軟體漏洞將被發現

就駭客的偏好程度來看，網路犯罪集團還是會挑選一些較容易下手的方式，例如竊取雲端帳號登入憑證來掌控資料庫。然而，針對雲端基礎架構弱點的研究也不會停滯不前。**隨著雲端更加普及，針對雲端基礎架構漏洞的研究將開始獲得一些進展**，尤其，開放原始碼社群對於 Docker 這類容器化軟體以及 Kubernetes 這類容器協調系統的使用率及研究正日益成長。

Docker[31] 和 Kubernetes[32] 目前在雲端部署環境的使用率相當普遍。近年來 Kubernetes 已被發現數個漏洞[33]，其中一個「重大」等級的漏洞出現在 2018 年 12 月[34]。根據一位專門研究雲端基礎架構漏洞的專家「Kromtech」發現，有數十個惡意的 Docker 映像在上架的一年內至少被不知情的開發人員下載了五百萬次[35]。

智慧家庭

▶ 網路犯罪集團將競相角逐 IoT「蠕蟲戰爭」的霸主

隨著越來越多智慧裝置連上家庭網路，家用路由器對於想要掌控智慧家庭裝置的網路犯罪集團來說，仍是一個非常誘人的攻擊目標。**智慧家庭環境將重現 2000 年早期一個資安史上名為「蠕蟲戰爭」的重要時代[36]。**

近年來一些利用路由器所發動的智慧裝置攻擊 (亦稱 IoT 攻擊) 大致上不是根據網路上流傳的 Mirai 惡意程式原始碼[37]，就是根據其他行為類似的惡意程式所衍生而來 (前者現身於 2016 年 8 月[38]，最早感染的是連網的 Linux 裝置)。這些惡意程式會利用幾個已知的漏洞攻擊手法，以及一些容易猜測的登入帳號和密碼來駭入裝置。換句話說，它們會自動掃瞄網際網路來發掘同一款裝置來下手。由於裝置的數量是有限的，而且一台裝置只能接受一個惡意程式的指揮來執行某些惡意程式或從事像 DDoS 之類的惡意攻擊，因此，網路犯罪集團便開始在程式內加入一些程式碼不讓其他駭客操控裝置，或者將其他駭客的惡意程式剔除，以便能夠獨占裝置的控制權。資安專家對這種情況應不陌生：Netsky 當年的作者就和其他知名蠕蟲 (如 Mydoom 和 Bagle) 的作者掀起了一場蠕蟲大戰。

▶ 銀髮族將出現第一個遭到智慧醫療裝置攻擊的案例

研究人員、業餘專家和網路駭客都將不斷發現智慧裝置的漏洞。但是在明確、容易獲利的方法出現之前，未來幾年頂多只會出現一些零星的實際攻擊案例。2019 年之後，我們不難想像研究人員甚至駭客都會紛紛試圖駭入一些智慧裝置和系統，尤其是一些在研究和市場上已有一定成果的領域，如自動駕駛汽車[39]。但就目前而言，網路犯罪集團眼中只有錢，既然目前還有許多其他獲利管道，全球性的智慧裝置攻擊在 2019 年還不太可能發生。

不過在範圍較小的健康追蹤裝置方面，我們相信**首樁智慧醫療裝置攻擊的真實受害案例將會是銀髮族**。企業目前正試圖開發智慧追蹤裝置和其他連網醫療裝置的銀髮族客群[40]，例如一些可監視心跳或者在年長者滑倒或跌倒時緊急通知某個網路帳號的智慧裝置。過去，年長者因為身體大多有些狀況，再加上身邊存有一筆養老積蓄，因此經常成為電話詐騙的對象[41]。我們認為，銀髮族在 2019 年很可能成為智慧裝置攻擊的第一個受害者。理由是，使用健康追蹤裝置的年長者不見得非常熟悉電腦操作，因此不會去檢查這些裝置的隱私權設定，使得自己的敏感醫療資料因而外洩，或者不知如何保護自己的帳號，讓駭客能夠竊取其健康資訊或其他個人資料。

過了 2019 年，隨著具備語音辨識功能的智慧裝置以及智慧助理在智慧家庭環境更加普及，「語音式攻擊」的案例將開始增加[42]，所有年齡層都可能成為受害者。

為接下來的一年預做準備

▶ 面對更多未知威脅企業需要聰明的多層式防護

今日混合式資料中心架構與不斷演變的端點/使用者及行動裝置，包括合作夥伴以及其他可能連上企業網路的第三方對象，都將使得資安團隊在 2019 年需付出很大的心力來確保企業安全。相形之下，資安人才的短缺問題將更加嚴峻[43]，因此，採用聰明、高效率的多層式資安技術來彌補現有人力的不足，將更加重要。

想要防範不斷變化的威脅以確保企業網路安全，需要對資安風險管理有敏銳的認知。想要單靠一套所謂的新式技術來防範所有已知和未知的威脅絕對不可能，因為每種新型態的威脅都是針對資安的不同層面。企業不應追求所謂的「萬靈丹」，而是應該挑選跨世代融合的威脅防禦技巧，並且在適當時機套用適當技巧，包括：

- 惡意程式防護 (惡意程式偵測、行為分析、機器學習、網站信譽評等)。
- 網路防護 (入侵防護、防火牆、漏洞分析)。
- 電子郵件與協同作業防護 (垃圾郵件防護)。
- 系統防護 (應用程式控管、一致性監控、記錄檔檢查)。
- 特化偵測引擎、客製化沙盒模擬分析、全球威脅情報 (針對未知威脅)。
- 端點防護。
- 整合式資料外洩防護。

此外，這套解決方案還應針對使用者實際連上企業網路的地點和方式而最佳化，包括平台和裝置。最後，資安團隊也必須能夠利用這些技術來檢視網路活動、評估威脅並採取適當的措施。

▶ 開發人員必須擁抱開發營運 (DevOps) 文化並以資安為焦點

開發營運 (DevOps) 是一種結合軟體開發 (Dev) 流程與 IT 營運 (Ops) 流程以縮短系統開發生命週期以改善效率並提升整合的方法。此外，目前正興起所謂的「開發資安營運」(DevSecOps) 方法，也就是以資安為焦點的開發營運流程，藉此改善資安作業，並將資安融入流程的每一步驟當中。軟體開發人員應該採取這樣的心態，然後再配合各種實用工具，才能既發揮其資安效益、又降低成本。

通常，軟體設計上的弱點以及其他可能外洩個人資訊的漏洞，都是在軟體已經安裝到生產環境的電腦和裝置之後才發現，因此如果能提早在規劃階段就將資安納入考量，就能大幅減少這類問題發生。

▶ 使用者必須肩負起數位公民的責任並養成良好資安習慣

使用者能否分辨真假，尤其分辨網際網路內容的真假，在 2019 年將越來越重要。如果能盡量散播有關假新聞運作機制的訊息，或許能讓社會大眾對各種輿論操作具備一定免疫能力。中央與地方政府可將網路資安意識教育融入學校教育當中，並且將對象擴大到整個社會。

社交工程詐騙基本上利用的就是人類心理上的相同弱點，使用者在面對社群媒體上的內容時應該隨時抱持著一定程度的懷疑。同樣地，在收到電子郵件或接到電話時也應抱持相同的心態，再次確認其來源是否可靠。

電腦、平板、智慧型手機等消費性裝置必須受到妥善保護以防範勒索病毒、危險網站、身分盜用等各種威脅，而最重要的就是務必採用一套能提供完整防護的資安解決方案。這類防護還應該包括資料防護，以便保護珍貴檔案、防範最新威脅、確保線上交易安全。

除此之外，使用者也應定期更換密碼、避免在不同的帳號使用相同密碼、盡可能啟用多重認證功能，或者使用一套密碼管理工具來妥善保護自己的各種登入憑證。

智慧家庭的系統管理員應確實檢查產品的預設值來確保路由器和連網裝置安全，並且了解如何開啟安全設定、定期更新韌體、僅連上安全的網路、架設防火牆並僅開放特定連接埠來管制流量、設定一個「訪客專用網路」來避免不必要的裝置任意連上您的網路。如果可以的話，也應定期檢查裝置的歷史記錄檔。當然，不論是路由器或連網裝置都應該強制使用高強度且非重複的密碼。

2019 年，幾乎所有會用到網際網路的產業都將面臨各種不同的網路資安挑戰，即使未來 5G 行動網路帶來了更快的網際網路 (不論是好是壞)，情況依然不會有所改變。不過，現有的工具和技術應該足以讓使用者和企業提升自己對抗網路犯罪集團與其他新興犯罪的能力。唯有更進一步認識這些問題，才是保護資訊安全的正確方向。

參考資料

1. StatCounter。*Statcounter Global Stats*。「2013 年 1 月至 12 月全球作業系統市場占有率」(Operating System Market Share Worldwide, Jan-Dec 2013)。上次存取時間 2018 年 11 月 13 日： http://gs.statcounter.com/os-market-share/all/worldwide/2013.
2. StatCounter。*Statcounter Global Stats*。「2017 年 10 月至 2018 年 10 月全球作業系統市場占有率」(Operating System Market Share Worldwide, Oct 2017 – Oct 2018)。上次存取時間 2018 年 11 月 13 日： http://gs.statcounter.com/os-market-share.
3. Lorenzo Franceschi-Bicchierai。(2018 年 7 月 17 日)。*Motherboard*。「SIM 卡劫持犯罪集團」(The SIM Hijackers)。上次存取時間 2018 年 11 月 13 日：https://motherboard.vice.com/en_us/article/vbqax3/hackers-sim-swapping-steal-phone-numbers-instagram-bitcoin.
4. Ponemon Institute。(2018 年 6 月)。*Akamai*。「密碼填充攻擊所帶來的成本：亞太地區」(The Cost of Credential Stuffing: Asia-Pacific)。上次存取時間 2018 年 11 月 13 日：https://www.akamai.com/us/en/multimedia/documents/white-paper/the-cost-of-credential-stuffing-asia-pacific.pdf.
5. Donna Freydkin。(2018 年 2 月 9 日)。*Today*。「網路『性勒索』如何導致一位年輕男子自殺」(How online 'sextortion' drove one young man to suicide)。上次存取時間 2018 年 11 月 28 日： https://www.today.com/parents/how-online-sextortion-drove-one-young-man-suicide-t122735.
6. Lizzie Dearden。(2018 年 5 月 4 日)。*Independent*。「警方透露已有五位英國男子因遭到網路『性勒索』而自殺」(Five British men have killed themselves after falling victim to online 'sextortion', police reveal)。上次存取時間 2018 年 11 月 28 日： https://www.independent.co.uk/news/uk/crime/blackmail-online-sextortion-suicides-videos-photos-sexual-police-advice-a8337016.html.
7. David Goodwin。(2018 年 11 月 8 日)。*Greenock Telegraph*。「因弗克萊德區年輕人遭黑幫『性勒索』」(Inverclyde youngsters fall victim to 'sextortion' gangs)。上次存取時間 2018 年 11 月 28 日： https://www.greenocktelegraph.co.uk/news/17204102.inverclyde-youngsters-fall-victim-to-sextortion-gangs/.
8. Gallup。(2017 年)。*Gallup*。「美國工作場所狀況」(State of the American Workplace)。上次存取時間 2018 年 11 月 27 日：https://news.gallup.com/file/reports/199961/SOAW_Report_GEN_1216_WEB_FINAL_rj.pdf.
9. Polycom。(2018 年)。*Polycom*。「變遷中的職場環境」(The Changing World of Work)。上次存取時間 2018 年 11 月 13 日：http://www.polycom.com/content/dam/polycom/common/documents/whitepapers/changing-needs-of-the-workplace-whitepaper-enus.pdf
10. IDC。(2018 年 10 月 1 日)。*IDC*。「IDC 預測所有類別的智慧家庭裝置至 2022 年將呈現二位數成長」(All Categories of Smart Home Devices Forecast to Deliver Double-Digit Growth Through 2022, Says IDC)。上次存取時間 2018 年 11 月 13 日： https://www.idc.com/getdoc.jsp?containerId=prUS44361618.
11. Stephen Hilt。(2018 年 12 月 27 日)。*趨勢科技資訊安全情報部落格 (Security Intelligence Blog)*。「IoT 裝置需提升內建安全性」(The Need for Better Built-in Security in IoT Devices)。上次存取時間 2018 年 11 月 13 日： https://blog.trendmicro.com/trendlabs-security-intelligence/iot-devices-need-better-builtin-security/.
12. Greg Young 與 William J. Malik。(2018 年 5 月 3 日)。*趨勢科技 Simply Security 部落格*。「HIPAA 和其他法規所教我們的 GDPR 現實問題」(What HIPAA and Other Compliance Teaches Us About the Reality of GDPR)。上次存取時間 2018 年 11 月 13 日： https://blog.trendmicro.com/what-hipaa-and-other-compliance-teaches-us-about-the-reality-of-gdpr/.
13. Phil Muncaster。(2018 年 9 月 14 日)。*Infosecurity Magazine*。「英國資訊委員會 (ICO) 因 GDPR 資料外洩通報案件過多而忙翻」(ICO Swamped with GDPR Breach Over-Reporting)。上次存取時間 2018 年 11 月 28 日： https://www.infosecurity-magazine.com/news/ico-swamped-with-gdpr-breach/.
14. David Meyer。(2018 年 12 月 4 日)。*Fortune*。「電子郵件詐騙如何利用市場商人的手段來對付企業財務長」(How Email Scammers Are Using Marketeer Methods to Target CFOs)。上次存取時間 2018 年 12 月 5 日： http://fortune.com/2018/12/04/targeted-email-fraud/.
15. Forrester Research。(2018 年 11 月 14 日)。*ZDNet*。「自動化將成為企業策略和營運的核心」(Automation will become central to business strategy and operations)。上次存取時間 2018 年 11 月 14 日： https://www.zdnet.com/article/automation-will-become-central-to-business-strategy-and-operations/.
16. David Sancho。(2018 年 1 月 30 日)。*趨勢科技資訊安全情報部落格 (Security Intelligence Blog)*。「數位勒索：前瞻觀點」(Digital Extortion: A Forward-looking View)。上次存取時間 2018 年 11 月 13 日： https://blog.trendmicro.com/trendlabs-security-intelligence/digital-extortion-forward-looking-view/.
17. Alberto Alemanno。(2018 年 6 月 27 日)。*Carnegie Europe*。「任人宰割的歐洲：2019 年歐洲議會大選即將引爆的戰線」(Europe Up for Grabs: The Looming Battle Lines of the 2019 European Parliament Elections)。上次存取時間 2018 年 11 月 13 日： https://carnegieeurope.eu/2018/06/27/europe-up-for-grabs-looming-battle-lines-of-2019-european-parliament-elections-pub-76691.
18. Lion Gu、Vladimir Kropotov 與 Fyodor Yarochkin。(2017 年 6 月 13 日)。*趨勢科技資訊安全新聞*。「假新聞與網路宣傳如何運用及操弄社群媒體」(Fake News and Cyber Propaganda: The Use and Abuse of Social Media)。上次存取時間 2018 年 11 月 13 日： https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/fake-news-cyber-propaganda-the-abuse-of-social-media.
19. Charles Hymas。(2018 年 9 月 20 日)。*The Telegraph*。「Telegraph 事件之後政府擬定了社群媒體管制計畫」(Government draws up plans for social media regulator following Telegraph campaign)。上次存取時間 2018 年 11 月 13 日： https://www.telegraph.co.uk/news/2018/09/20/government-draws-plans-social-media-regulator-following-telegraph/.
20. Sebastian Anthony。(2018 年 11 月 7 日)。*Ars Technica*。「Adobe 示範『photoshop for audio』讓您編輯語音就像編輯文字一樣簡單」(Adobe demos "photoshop for audio," lets you edit speech as easily as text)。上次存取時間 2018 年 11 月 13 日：https://arstechnica.com/information-technology/2016/11/adobe-voco-photoshop-for-audio-speech-editing/.
21. Lily Hay Newman。(2017 年 5 月 12 日)。*Wired*。「Meltdown 漏洞研究專家所警告的勒索病毒已經來臨」(The Ransomware Meltdown Experts Warned About Is Here)。上次存取時間 2018 年 11 月 28 日： https://www.wired.com/2017/05/ransomware-meltdown-experts-warned/.
22. Andy Greenberg。(2018 年 8 月 22 日)。*Wired*。「Notpetya 勒索病毒不為人知的故事，史上最具破壞力的網路攻擊」(The Untold Story of Notpetya, The Most Devastating Cyberattack in History)。上次存取時間 2018 年 11 月 28 日： https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

23. Adi Robertson。(2018 年 9 月 28 日)。*The Verge*。「加州成為第一個制定物聯網 (IoT) 網路攻擊法律的州」(California just became the first state with an Internet of Things cybersecurity law)。上次存取時間 2018 年 11 月 13 日： https://www.theverge.com/2018/9/28/17874768/california-iot-smart-device-cybersecurity-bill-sb-327-signed-law.

24. 趨勢科技前瞻威脅研究團隊。(2018 年 4 月 5 日)。*趨勢科技資訊安全情報部落格 (Security Intelligence Blog)*。「了解惡意程式攻擊如何濫用程式碼簽署機制」(Understanding Code Signing Abuse in Malware Campaigns)。上次存取時間 2018 年 11 月 13 日： https://blog.trendmicro.com/trendlabs-security-intelligence/understanding-code-signing-abuse-in-malware-campaigns/.

25. MITRE ATT&CK。*MITRE*。「戰術：執行」(Tactic: Execution)。上次存取時間 2018 年 11 月 13 日： https://attack.mitre.org/tactics/TA0002/.

26. European Union Agency for Network and Information Security。*ENISA*。「網路資訊安全規範」(NIS Directive)。上次存取時間 2018 年 12 月 5 日： https://www.enisa.europa.eu/topics/nis-directive.

27. 趨勢科技。(2017 年 5 月 23 日)。*趨勢科技資訊安全新聞*。「SCADA 人機介面 (HMI) 漏洞的現況」(The State of SCADA HMI Vulnerabilities)。上次存取時間 2018 年 11 月 13 日： https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/the-state-of-scada-hmi-vulnerabilities.

28. Brian Gorenc。(2018 年 7 月 9 日)。*Zero Day Initiative*。「定期回報：2018 上半年回顧」(Checking In: A Look Back at the First Half of 2018)。上次存取時間 2018 年 11 月 28 日： https://www.zerodayinitiative.com/blog/2018/7/9/checking-in-a-look-back-at-the-first-half-of-2018.

29. 趨勢科技。(2017 年 5 月 23 日)。*趨勢科技資訊安全新聞*。「SCADA 人機介面 (HMI) 漏洞的現況」(The State of SCADA HMI Vulnerabilities)。上次存取時間 2018 年 11 月 13 日： https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/the-state-of-scada-hmi-vulnerabilities.

30. Charlie Osborne。(2018 年 5 月 15 日)。*ZDNet*。「針對企業雲端環境的虛擬加密貨幣挖礦攻擊暴增」(Cryptojacking attacks surge against enterprise cloud environments)。上次存取時間 2018 年 11 月 28 日： https://www.zdnet.com/article/cryptojacking-attacks-surge-against-enterprise-cloud-environments/.

31. Steven J. Vaughan-Nichols。(2018 年 3 月 21 日)。*ZDNet*。「何謂 Docker 以及為何它這麼熱門？」(What is Docker and why is it so darn popular?)。上次存取時間 2018 年 11 月 28 日： https://www.zdnet.com/article/what-is-docker-and-why-is-it-so-darn-popular/.

32. Udi Nachmany。(2018 年 11 月 1 日)。*Forbes.com*。「Kubernetes：IT 革命的演進」(Kubernetes: Evolution of an IT Revolution)。上次存取時間 2018 年 11 月 28 日： https://www.forbes.com/sites/udinachmany/2018/11/01/kubernetes-evolution-of-an-it-revolution/#366fcb4554e1.

33. CVE Details。*CVE Details*。「Kubernetes：資安漏洞清單」(Kubernetes: List of security vulnerabilities)。上次存取時間 2018 年 11 月 28 日： https://www.cvedetails.com/vulnerability-list/vendor_id-15867/product_id-34016/Kubernetes-Kubernetes.html.

34. Steven J. Vaughan-Nichols。(2018 年 12 月 3 日)。*ZDNet*。「Kubernetes 被發現第一個重大資安漏洞」(Kubernetes' first major security hole discovered)。上次存取時間 2018 年 12 月 3 日： https://www.zdnet.com/article/kubernetes-first-major-security-hole-discovered/.

35. Security Center。(2018 年 6 月 12 日)。*KromTech Security Center*。「數位加密貨幣挖礦攻擊入侵雲端：駭客如何利用今日容器化的趨勢」(Cryptojacking invades cloud. How modern containerization trend is exploited by attackers)。上次存取時間 2018 年 11 月 28 日： https://kromtech.com/blog/security-center/cryptojacking-invades-cloud-how-modern-containerization-trend-is-exploited-by-attackers.

36. 趨勢科技。*趨勢科技資訊安全情報部落格 (Security Intelligence Blog)*。「威脅成形：數位威脅背後動機的轉變」(Threat Morphosis: The Shifting Motivations Behind Digital Threats)。上次存取時間 2018 年 11 月 13 日： http://blog.trendmicro.com/threat-morphosis/.

37. Brian Krebs。(2016 年 10 月 1 日)。*Krebs on Security*。「Mirai 物聯網殭屍網路病毒原始程式碼遭公開」(Source Code for IoT Botnet 'Mirai' Released)。上次存取時間 2018 年 11 月 28 日： https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/.

38. 趨勢科技。(2016 年 9 月 13 日)。*趨勢科技資訊安全新聞*。「Linux 安全：深入探討最新 Linux 威脅」(Linux Security: A Closer Look at the Latest Linux Threats)。上次存取時間 2018 年 11 月 28 日： https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/linux-security-a-closer-look-at-the-latest-linux-threats.

39. Spencer Hsieh。(2018 年 10 月 5 日)。*Virus Bulletin*。「IoV 裝置資安問題」(Security issues of IoV devices)。上次存取時間 2018 年 11 月 28 日： https://www.virusbulletin.com/conference/vb2018/abstracts/security-issues-iov-devices/.

40. Christina Farr 與 Jillian D'Onfro。(2018 年 7 月 23 日)。*CNBC*。「Google 正在為 Nest 智慧家庭產品構思新市場：銀髮族」(Google is mulling a new market for Nest smart home products: seniors)。上次存取時間 2018 年 11 月 13 日： https://www.cnbc.com/2018/07/20/google-nest-senior-living-aging.html.

41. McCall Robison。(2018 年 11 月 15 日)。*MarketWatch*。「針對銀髮族的常見攻擊：該如何預防」(These common scams target seniors—how to avoid them)。上次存取時間 2018 年 11 月 28 日： https://www.marketwatch.com/story/these-common-scams-target-the-elderlyhow-to-avoid-them-2018-11-15.

42. 趨勢科技。(2018 年 4 月 11 日)。*趨勢科技資訊安全新聞*。「語音 IoT 與 IIoT 裝置所將面臨的威脅」(Threats to Voice-Based IoT and IIoT Devices)。上次存取時間 2018 年 11 月 28 日： https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/threats-to-voice-based-iot-and-iiot-devices.

43. Jon Oltsik。(2018 年 1 月 11 日)。*CSO Online*。「研究指出網路資安人才短缺問題日益嚴重」(Research suggests cybersecurity skills shortage is getting worse)。上次存取時間 2018 年 11 月 13 日： https://www.csoonline.com/article/3247708/security/research-suggests-cybersecurity-skills-shortage-is-getting-worse.html.

獻給 Raimund Genes (1963-2017 年)

TREND MICRO™ | research

TREND MICRO™ RESEARCH

趨勢科技為網路資安解決方案全球領導廠商，致力建立一個安全的資訊交換世界。

Trend Mico Research 背後擁有一群熱情的專家為後盾，他們熱衷發掘最新威脅、分享重要分析情報、全力為遏止網路犯罪而努力。我們的全球團隊每天都協助客戶偵測數以百萬計的威脅，為業界漏洞研究揭露的先驅，經常發表有關最新威脅偵測技巧的創新研究。我們不斷鑽研並預測最新威脅，發表令人深思的研究。

www.trendmicro.tw

©2018 年版權所有。趨勢科技股份有限公司保留所有權利。Trend Micro、t 字球形標誌與 Trend Micro Smart Protection Network 是趨勢科技股份有限公司的商標或註冊商標。所有其他公司和產品名稱為各該公司的商標或註冊商標。