



2019 上半年資安總評

隱匿的威脅、 瀰漫的衝擊



趨勢科技法律免責聲明

本文之內容僅供一般資訊及教育用途。不作為也不應視為法律諮詢建議。本文之內容可能不適用於所有情況，也可能未反映出最新的情勢。在未就特定事實或所呈現之情況而徵詢法律建議之前，不應直接採信本文之所有內容或採取行動。趨勢科技保留隨時修改本文內容而不事先知會之權利。

所有翻譯成其他語言之內容僅供閱讀之方便。翻譯之準確性無法保證。若有任何關於翻譯準確性的問題，請參考本文件原始語言的官方版本。任何翻譯上的不一致與差異皆不具約束力，且在法規與執法上不具法律效力。

儘管趨勢科技已盡合理之努力確保本文內容之準確性與時效性，但趨勢科技對其準確性、時效性與完整性不提供任何擔保或聲明。在您存取、使用及採納這份文件內容時，即同意自行承擔任何風險。趨勢科技不提供任何形態之擔保，不論明示或隱含之擔保。趨勢科技或建立、製作或供應此文件之任何相關對象，對於存取、使用、無法使用、因使用本文、因本文內容之錯誤或遺漏而引起之任何後果、損失、傷害皆不承擔責任，包括直接、間接、特殊、連帶、營利損失或特殊損害賠償。使用本文之資訊即代表接受本文之「原貌」。

發行：

Trend Micro Research

圖片授權：Shutterstock.com

內容

04

勒索病毒依然到處肆虐並造成嚴重損失

09

威脅逐漸朝「就地取材」的方向發展

14

針對性攻擊更常採用經過千錘百鍊的技巧而非全新技巧

15

犯罪集團依然仰賴虛擬加密貨幣挖礦來獲利

19

訊息威脅更多元化

25

無所不在的漏洞讓修補更新顯得更加重要

29


IoT 和 IIoT 資安依然是一項重大問題

31

多層式防禦有助於解決今日多重面向的威脅

32

威脅情勢回顧



在一個不斷演變的威脅情勢下，網路資安再也不單只是防止駭客及網路犯罪集團入侵網路、系統、裝置以及底層技術以確保敏感資料和其他數位資產的安全就好。現在更需要的是，主動追蹤駭客攻擊路徑，甚至在其建立據點與營運之前預先加以攔截。

2019 上半年最令人矚目的一些威脅即充分印證了這點，例如：能夠「就地取材」的無檔案式威脅，經常利用一些普遍列於白名單內的正常系統工具來從事不法行動。此外，還有大量的惡意程式與網路釣魚攻擊正在結合資安漏洞與人性弱點並朝多樣化發展。

勒索病毒犯罪集團的目標相當明確，那就是：癱瘓企業機構來從事勒索。事實證明，勒索病毒攻擊甚至能嚴重到讓受害者就算再不情願也必須屈服於網路犯罪集團的勒索。在虛擬加密貨幣挖礦威脅方面，運算效能較端點裝置更強且資源更豐富的伺服器與雲端環境，已經成為歹徒的新天堂。而許多企業賴以為生的訊息平台，也正充斥著各式各樣的威脅，包括：變臉詐騙、性愛勒索、網路釣魚等等，這些詭計都不單只是利用人性弱點而已。

過去這半年以來，許多犯罪集團似乎正在分散投資風險，這一點，顯現在他們的針對性攻擊行動似乎廣泛涵蓋多種平台且突然重拾對漏洞攻擊套件的興趣，再加上他們對路由器和物聯網 (IoT) 裝置持續不懈的攻擊。有不少的威脅甚至運用了多重階段或多重層次的感染程序。無可否認，這些威脅所採用的手法、技巧及程序或許並無創新之處，但卻更穩當且更不易出錯，這一點值得注意。

漏洞的問題依然令人擔憂，不論是網路資安永遠得面對的軟體漏洞，或是最近開始引起關注的硬體漏洞。更有甚者，一些普遍存在的漏洞，如熱門桌面軟體服務與容器平台所發現的漏洞，充分突顯出資安漏洞一旦放任不管將衍生出多大的問題。

對企業與資安系統管理員來說，光是確保網路、系統、裝置及技術的正確設定或定期修補就是一件艱鉅的任務，更遑論採取一些措施來縮小受攻擊面，並主動監控及遏止駭客每一階段或每一層面的入侵活動。但考慮到企業所面臨的風險，不論是網路資安或實體安全的風險，若能成功做到這點，一切的辛苦都將因其帶來的效益而變得值得。

這份年度期中資安總評報告，重新回顧了 2019 上半年的資安情勢，探討了這段期間出現的重大威脅以及伴隨而來的問題和風險，希望能為企業提供一些分析建議，協助企業在剩下的半年及未來能妥善因應前述的各項挑戰。

勒索病毒依然到處肆虐並造成嚴重損失

重大攻擊事件寫下鉅額損失

當 2019 上半年接近尾聲時，已經獲利超過 20 億美元的 GandCrab 勒索病毒集團在其銷售「勒索病毒服務」(Ransomware as a service, 簡稱 RaaS) 的駭客論壇上宣布引退¹。GandCrab 以服務化的商業模式聞名：任何網路犯罪集團，不論技術水準如何，只需付費訂閱這項服務就能取得自己專屬的客製化勒索病毒。接下來，就能透過其偏好的管道散布這個專屬版本的 GandCrab 勒索病毒，例如經由垃圾郵件或漏洞攻擊套件。儘管如此，勒索病毒集團一直以來大多採用亂槍打鳥的方式，並將其惡意程式賣給一些嘗試進入該領域的新手²，試圖招攬更多業務夥伴並擄獲更多受害者來提高其獲利潛力。

不過這半年來，他們卻出現了一些改弦易轍的跡象。也許，網路犯罪集團覺得他們若將攻擊目標換成一些超大型跨國集團，甚至政府機構，或許也可以很穩定地獲得同樣、甚至更高的報酬。其犯罪手法有一貫的模式：勘查目標、發送精心製作的電子郵件給目標的員工、搜尋可利用的資安漏洞來進入目標，然後在目標內部的各網路與系統之間橫向移動。

一個例子就是 6 月份襲擊美國佛羅里達州湖市 (Lake City) 的 Ryuk 勒索病毒。由於 Ryuk 勒索病毒挾持了湖市的市民服務系統，因此市府官員被迫支付了 46 萬美元的贖金⁴。其實不到二週之前佛羅里達州的里維埃拉海灘 (Riviera Beach) 才剛遭到勒索病毒攻擊，而該市府官員被迫支付了 60 萬美元的贖金³。

毫不意外地，Ryuk 勒索病毒也因這筆龐大的金額而登上今年的最高贖金排行榜⁵。此勒索病毒自去年 8 月首度現身至今年 1 月為止已經賺了至少 705 個比特幣 (當時的市值至少 370 萬美元以上)⁶。其惡名昭彰的程度也反映在該病毒的流行程度上，根據趨勢科技 Smart Protection Network™ 全球情報網的資料，2019 上半年它是偵測數量最多的勒索病毒之一。

這些驚人的贖金，似乎也與 2018 下半年至 2019 上半年勒索病毒相關威脅 (檔案、電子郵件及網址) 的偵測數量大幅成長 77% 的態勢吻合 (儘管新的勒索病毒家族數量減少了 55%)。偵測數量的增加，可能不僅反映出我們在電子郵件與網址層次主動攔截勒索病毒相關活動的方法有所提升，也反映了在勒索病毒下載階段之後資安攔截技術的整體改善。此外，活動數量的增長也呼應了這半年來媒體上曝光的各種針對性勒索病毒攻擊事件，這些事件不僅造成了軒然大波，更帶來了巨大的損害。

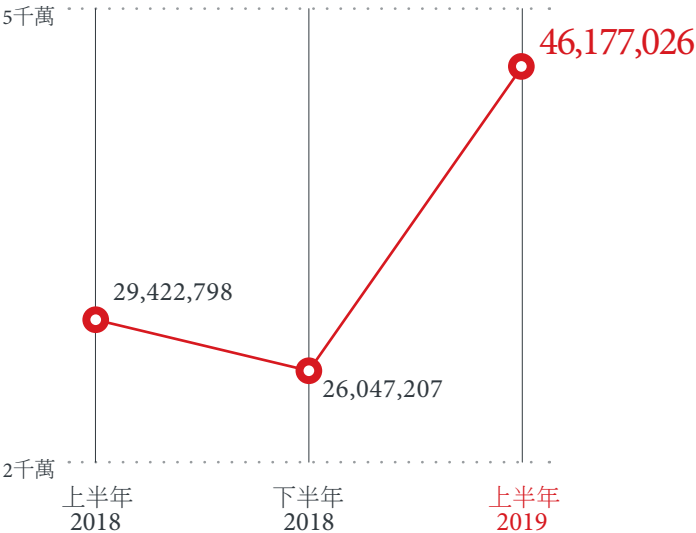


圖 1：勒索病毒相關威脅偵測數量大幅成長：
勒索病毒相關威脅 (檔案、電子郵件及網址) 偵測數量半年期比較。

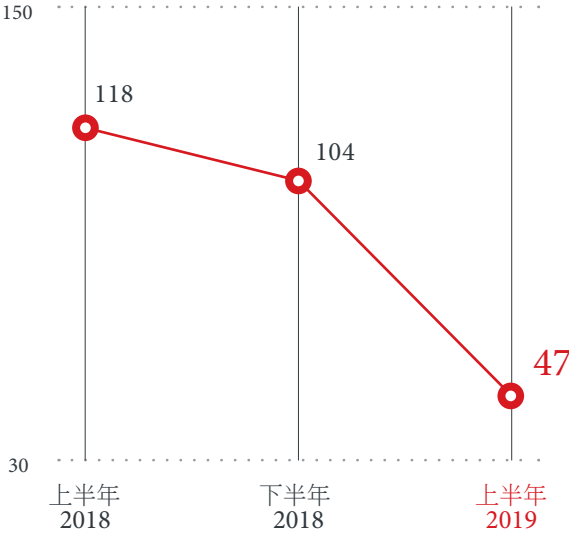


圖 2：新的勒索病毒家族數量進一步減少：
新的勒索病毒家族數量半年期比較。

今年 3 月，LockerGoga 勒索病毒襲擊了挪威的一家製造商，造成該公司多家工廠生產停擺，同時也迫使該公司其他工廠改用人工作業⁷。三個月後，當一切都塵埃落定⁸，其財務損失已超過 5,500 萬美元⁹。同樣地，今年 5 月發生的 RobbinHood 勒索病毒攻擊事件，也造成美國馬里蘭州巴爾的摩 (Baltimore) 市損失 530 萬美元，儘管損失金額少很多，但同樣相當可觀¹⁰。除此之外，RobbinHood 勒索病毒也是今年 4 月攻擊美國北卡羅來納州格林維爾 (Greenville) 市的元兇，使得該市所有遭感染的系統久久無法使用¹¹。

勒索病毒家族	入侵途徑與攻擊管道	散布方式	其他重要行為
Clop (CryptoMix)	網路上遭入侵的 Active Directory ¹² 。	駭入遠端桌面服務 ¹³ 。	利用含有合法數位簽章的執行檔來散布以躲避偵測。
Dharma ¹⁴ (亦稱 Crysis ¹⁵)	垃圾郵件。	暴力破解遠端桌面登入 (Crysis) ¹⁶ 。	利用防毒軟體安裝流程來引開注意力。
NamPoHyu 病毒 (亦稱 MegaLocker 病毒) ¹⁷	暴露在外的 Samba 伺服器。	暴力破解 Samba 伺服器登入。	先前的版本會將網路連接儲存 (NAS) 裝置加密。
GandCrab	垃圾郵件、漏洞攻擊套件、惡意廣告、已遭入侵的網站、暴露在外的資料庫 ¹⁸ 、含有漏洞的軟體 ¹⁹ 。	經由合作夥伴的客製化。	採用勒索病毒服務 (RaaS) 的商業模式。
MongoLock ²⁰	暴露在外或安全性不佳的 MongoDB 資料庫。	利用 Shodan 之類的搜尋引擎來尋找暴露在外或安全性不佳的 MongoDB 伺服器。	將資料庫加密之後即刪除原始資料，若有備份磁碟存在，則一併將它格式化 ²¹ 。
Ryuk ²²	垃圾郵件。	已遭入侵的路由器、Trickbot 與 Emotet (惡意程式載入器) ²³ 、EternalBlue。	可讓感染的系統無法開機 ²⁴ 。
LockerGoga ²⁵	遭外洩的登入憑證。	系統管理工具、滲透測試工具以及其他駭客工具 ²⁶ ，利用合法憑證來避開偵測以入侵系統。	修改受感染系統的使用者帳號密碼，不讓系統被重新開機。
Nozelesn ²⁷	含有惡意附件的垃圾郵件。	Emotet 惡意程式 (利用網路共用管理權限將自己複製到其他電腦)。	其檔案下載器 Nymaim 木馬程式會利用無檔案技巧載入該勒索病毒。
RobbinHood ²⁸	已遭入侵或無安全保護的遠端桌面、木馬程式載入器。	網域控制器或架構 (如：Empire PowerShell 與 PsExec)。	加密每個檔案，使用一個非重複的金鑰。
BitPaymer ²⁹	已遭入侵的系統管理員帳號、含有 Dridex 的電子郵件 ³⁰ 。	Dridex (竊取網路資訊)、供應鏈攻擊 ³¹ 、已遭入侵的遠端桌面伺服器 ³² 。	利用 PsExec 工具。
MegaCortex ³³	已遭入侵的網域控制器。	重新命名的 PsExec 工具。	停用某些執行程序。

表 1：上半年，重大勒索病毒攻擊除了將檔案加密之外還使用了其他攻擊技巧：
2019 上半年重大勒索病毒家族的攻擊行為比較。

這些事件告訴我們勒索病毒集團如何入侵攸關企業營運和生存的關鍵系統來迫使他們就範。歹徒之所以敢採取更大膽的攻擊並要求更高的贖金，正因為他們的惡意程式除了將檔案加密之外，還會試圖藉由某些破壞行為來讓企業無法復原以發揮最大的威脅效果。一旦受害者的系統或檔案復原機會變得渺茫，勒索病毒集團就更能對受害者予取予求，並要求巨額的贖金。

WannaCry 依然獨占鰲頭

根據趨勢科技 Smart Protection Network 全球威脅情報網的資料顯示 2019 上半年有多個相當活躍的勒索病毒家族。受害情況最嚴重的產業包括：製造、政府、教育及醫療。除此之外，金融、科技、能源、食品飲料以及石油天然氣等產業，也同樣傳出災情。

惡名昭彰的 WannaCry 再次展現強韌的生命力，自從 2017 年 5 月首次現身並在全球各地造成嚴重災情之後³⁴，至今仍是這段期間偵測最多的勒索病毒，其數量甚至大幅超越所有其他勒索病毒家族的總和。與去年的情況一樣，絕大多數的 WannaCry 勒索病毒都是在使用 Microsoft Windows 7 的系統上發現。顯然，系統漏洞的修補依然是一項艱鉅的挑戰，尤其對大型企業而言，因為 WannaCry 所攻擊的漏洞早在 2017 年釋出的修補更新當中即已解決，而且 Windows 7 的支援要到 2020 年 1 月才會終止³⁵。

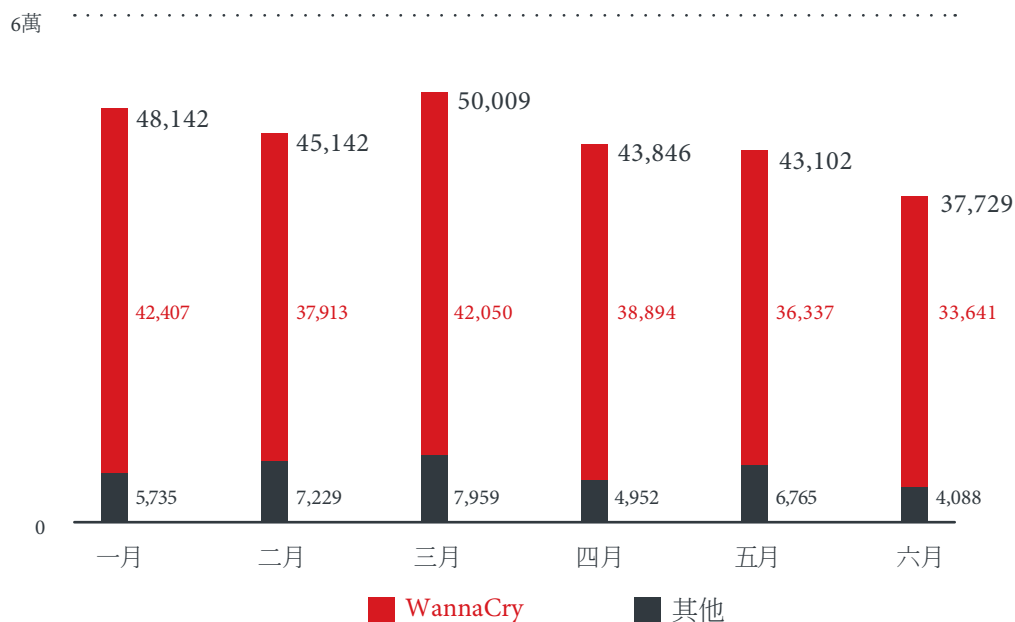


圖 3：WannaCry 依然占了大部分的勒索病毒偵測數量：
WannaCry 與所有其他勒索病毒家族偵測數量逐月比較 (2019 上半年)。



圖 4：超過 90% 的 WannaCry 偵測數量都是來自使用 Windows 7 的系統：
WannaCry 偵測數量依作業系統分布 (2019 上半年)。

儘管勒索病毒家族數量仍在持續減少，但一些新發現的獲利手段顯然將促使勒索病毒持續成為一項常態性的威脅，特別是針對大型企業。事實上，異軍突起的 Sodinokibi (亦稱為 Sodin 或 REvil) 似乎有取代 GandCrab 的態勢，同時也採用了類似的散布方法^{36、37}。

當網路犯罪集團有太多的途徑和攻擊面可入侵企業的網路時，光保護端點裝置是不夠的。若能部署一套多層式的威脅防禦，涵蓋閘道、伺服器、網路到端點，就能在企業網路基礎架構的每一層面遏止勒索病毒的入侵。

威脅逐漸朝「就地取材」的方向發展

無檔案式威脅活動較 2018 一整年多出 18%；巨集惡意程式仍歷久不衰

2019 上半年，我們偵測到無檔案式威脅活動突然暴增，甚至較 2018 一整年多出 18%，印證了我們對今年資安情勢的預測：網路犯罪集團和其他駭客會逐漸朝「就地取材」的方向發展³⁸，利用合法系統管理工具或滲透測試工具來避免引人注目。

相較於寫入磁碟的傳統惡意程式，就地取材的威脅(如無檔案式威脅)較不容易被發現，因為它們可在系統記憶體內執行，隱藏在系統登錄內部，或者利用一般列於白名單上的系統工具，如：PowerShell、PsExec、Windows Management Instrumentation (WMI)³⁹ 以及 AutoHotKey⁴⁰ 來執行。儘管如此，我們還是可以藉由追蹤一些徵兆來偵測無檔案式威脅相關活動，例如某些程式執行事件或行為。

就某方面來說，我們在上半年發現的許多重要威脅皆採用無檔案式技巧在系統植入或執行惡意檔案，最典型的就虛擬加密貨幣挖礦惡意程式⁴¹ 以及勒索病毒⁴²，有時也會出現銀行木馬程式⁴³。這些威脅都有一個共通特徵，那就是：使用 PowerShell。雖然對系統管理員來說 PowerShell 是一個強大又彈性方便的工具，但問題是一旦落入網路犯罪者手中也是同樣強大。

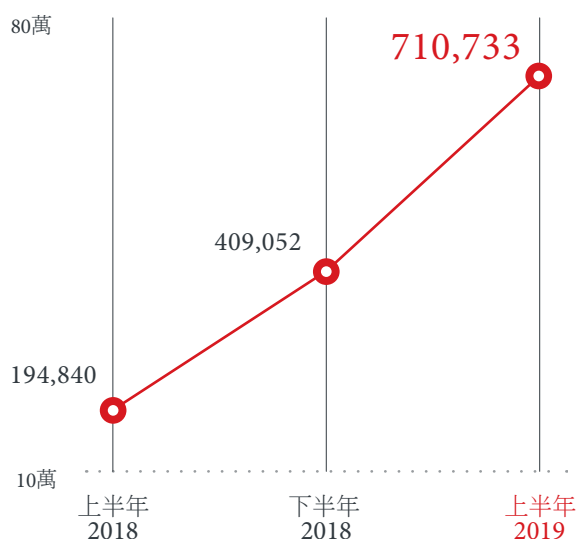


圖 5：無檔案式威脅活動較 2018 一整年多出 18%：已攔截的無檔案式威脅活動半年期比較。

巨集惡意程式儘管偵測數量較 2018 下半年稍微減少，但仍歷久不衰。如同去年一樣，本期偵測到的巨集惡意程式大多是 Powload，主要經由垃圾郵件散布。

Powload 除了會散播各種惡意檔案 (如 Ursnif 和 Bebloh 資訊竊取程式) 之外，其本身這幾年來亦不斷持續演進。例如，它開始使用圖像隱碼術 (steganography，一種將程式碼隱藏在圖像當中的技術)，或是模仿區域性品牌與用語來瞄準特定目標。Powload 還有一點值得注意的就是經常使用 PowerShell 來搭配巨集惡意程式，作為另一種感染途徑以掩護其惡意活動⁴⁴。

除了 Powload 之外，我們也看到巨集惡意程式出現在垃圾郵件攻擊行動當中，散布像 Trickbot⁴⁵ 之類的資訊竊取程式，有時甚至會搭配一些網路間諜使用的惡意程式⁴⁶。

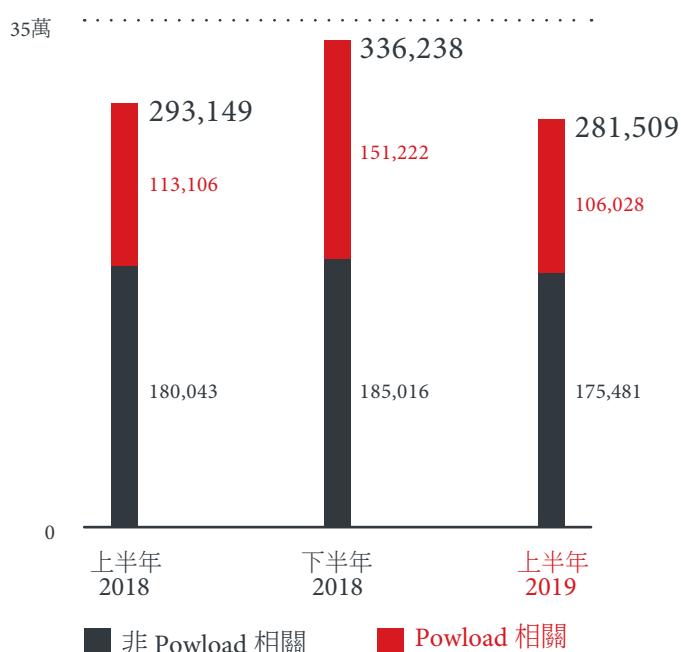


圖 6：絕大部分偵測到的巨集仍舊和 Powload 有關：
Powload 相關與非 Powload 相關巨集惡意程式偵測數量半年期比較。

多重階段與多重層次的容錯措施

除了無檔案式技巧和巨集惡意程式之外，上半年出現的一些重要威脅還會運用多重階段或多重層次的感染程序。

採用多重階段方式來散布惡意程式，有助於降低被徹底封鎖的風險。惡意程式感染的第一階段通常看起來無任何異常 (例如下載某個第二階段用的腳本)，因此不會引起注意。但是，將一大段惡意程式碼內嵌至 Microsoft Office 文件當中，就很容易起人疑竇。對駭客來說，多重階段的散布方式是他們躲避資安偵測的一種容錯措施。我們曾經在虛擬加密貨幣挖礦攻擊行動當中看到這樣的策略，其感染程序包含了三個下載與執行 PowerShell 腳本的階段，最後才會下載真正的惡意程式，並複製到其他電腦⁴⁷。

另一方面，多重階段的攻擊也讓惡意程式有更多機會可以入侵系統。就算不採用新的惡意程式，只要在攻擊當中盡可能包含更多漏洞的攻擊手法，就能增加感染系統的機會。BlackSquid 虛擬加密貨幣挖礦程式就是採用這種作法，它內建了高達 8 種漏洞的攻擊手法來散布、植入及執行最終的惡意程式，並讓駭客從遠端執行程式碼⁴⁸。更誇張的是某個 Mirai 的變種在單一攻擊當中就運用了 13 種漏洞攻擊手法來感染路由器和其他物聯網 (IoT) 裝置。如果這樣還不夠，那它還具備暴力破解能力，會使用一些常見的登入憑證來試圖登入這些裝置⁴⁹。

多重階段和多重層次的惡意程式感染很難被偵測，因為它們可會隱身在一些常用的檔案或程式當中，所以容易被忽略，尤其若資安防護機制只單看某些特定惡意行為的話。更糟糕的是，隨著這些進階而隱匿的威脅層出不窮，能夠對付它們的人才卻嚴重不足。根據我們所委託調查並在 3 月發表的一份研究報告指出，將近 50% 的企業機構目前皆面臨網路資安人才短缺的問題⁵⁰。

此外，我們還看到另一個有趣且相關的趨勢：行動勒索病毒會定期在加密檔案與竊取資訊兩種行為之間切換。例如，Anubis 就具備了勒索病毒的能力⁵¹，但也可以當成銀行惡意程式來使用⁵²。其最新版本事實上同時兼具了兩種能力，使用它的駭客似乎會視攻擊當下的行動和目標而選擇使用其中一種能力。有時候，歹徒也許只是看怎樣運用才賺得到錢⁵³。畢竟，也有一些舊的勒索病毒家族 (如 SMSLocker 和 Svpeng) 曾經被當成銀行惡意程式來使用⁵⁴。

漏洞攻擊套件依然是揮之不去的威脅

ShadowGate 攻擊行動在沉寂了一段時間之後，今年 6 月又再次捲土重來，使用升級版的 Greenflash Sundown 漏洞攻擊套件來散布虛擬加密貨幣挖礦程式，新的套件現在可就地取材使用新版的 PowerShell 以無檔案方式執行惡意程式。ShadowGate 上一次頻繁活動是在 2018 年 4 月，當時它利用漏洞攻擊套件在東亞地區短暫散播了一陣子的虛擬加密貨幣挖礦惡意程式⁵⁵。

Greenflash Sundown 漏洞攻擊套件重新獲得犯罪集團青睞，似乎也預告了漏洞攻擊套件未來的情勢發展。因此，一般使用者和企業切勿因為駭客缺乏零時差漏洞攻擊套件可用，或者已經較不仰賴漏洞攻擊套件所針對的平台而掉以輕心。

根據趨勢科技 Smart Protection Network 的監測資料顯示，2019 上半年漏洞攻擊套件相關活動依然延續著 2018 年的成長趨勢。只不過就算進一步成長，跟前幾年全盛時期動輒數以百萬計的漏洞攻擊套件散布網址攔截次數相比，仍有一段很大的差距⁵⁶。但話雖如此，活動數量的增加，意味著儘管只是攻擊舊有的漏洞，漏洞攻擊套件仍獲得了相當程度的斬獲，這有可能是因為搭配了各種惡意程式與概念驗證攻擊的緣故。

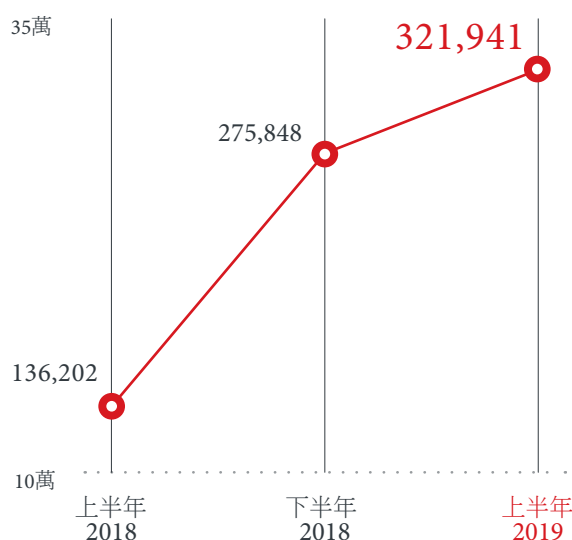


圖 7：儘管只有零星的活動出現，但漏洞攻擊套件仍占有一席之地：
已攔截的漏洞攻擊套件散布網址存取次數半年期比較。

利用社群媒體與社交平台來掩護網路犯罪

社群媒體遭犯罪集團濫用早已不是新聞。2017 年我們曾經針對假新聞發表了一份研究，指出歹徒如何利用假新聞來煽動群眾抗議、抹黑新聞記者，甚至影響國家政策或操弄選舉⁵⁷。但在 2019 上半年我們觀察到一個重要的趨勢轉變，威脅在攻擊或詐騙過程當中開始結合一些社群媒體頻道與協作平台和網路，甚至包括一些開發人員與資安專業人士所使用的平台。

例如，Slub 後門程式就會利用 Slack 和 Github 兩大平台。前者是一個熱門的網站式協作與訊息平台，被犯罪集團當成與受害者溝通的橋樑；後者是開發人員專用的網頁式協作與版本控制平台，被犯罪集團當成了惡意程式碼的儲存庫⁵⁸。除此之外，還有一個駭客團體的犯罪手法是利用網路釣魚來竊取 Instagram 熱門帳號，然後再詆毀、破壞這些帳號以藉機勒索錢財或裸照⁵⁹。

還有另外一個熱門的社群媒體網站 Twitter 也成為 XLoader Android 惡意程式的利用工具，該程式會將其幕後操縱 (C&C) 伺服器的位址編碼之後包含在 Twitter 帳號的名稱當中⁶⁰。此外，技術支援詐騙也開始逐漸盛行，這類詐騙會利用社群媒體頻道來引誘不幸的使用者提供個人身分識別資訊 (PII)、下載可疑的軟體，甚至被騙支付所謂的服務費用⁶¹。

對資安研究人員而言，社群媒體提供了一個功能完整、內容豐富的平台來蒐集有用的威脅情報⁶²。但正如前述的案例所示，社群媒體同樣也可能讓犯罪集團用來掩護其活動。因此，有鑑於社群媒體頻道所牽涉的資安及隱私風險，包括：資料外洩、身分冒用、網路釣魚等等，企業在運用社群媒體來經營品牌或提升知名度時，務必將社群媒體頻道也納入網路資安策略的一環。

針對性攻擊更常採用經過千錘百鍊的技巧而非全新技巧

針對性攻擊一向被視為網路犯罪集團運用最新攻擊手法、技巧與程序的先驅。然而從 2019 上半年的重大攻擊行動看來，情況似乎有所轉變。歹徒明顯地更常使用相對老舊但卻更為可靠的攻擊手法、技巧和程序，也許是因為這麼做更有效率，畢竟，開發採用全新攻擊技巧的惡意程式需耗費相當的時間和資源。再者，針對性攻擊可以就地取材，利用系統現有的工具就能從事網路間諜行動。

Bouncing Golf 攻擊行動就是一個例子，它採用的是重新包裝合法應用程式的常見技巧。不過其應用程式散布的管道倒很特別，它不經由官方或第三方應用程式市集來散布，反而是先放在一個獨立的網站上，然後再透過社群媒體來宣傳該網站⁶³。同樣地，TA505 網路犯罪集團也不需在攻擊行動當中加入新的技巧，因為他們已經擁有一整套經過千錘百鍊的武器：駭客工具、巨集惡意程式 (含 Microsoft Excel 4.0 檔案內嵌的惡意巨集)、木馬程式、檔案下載器，以及後門程式^{64、65}。該集團會經常發動大規模垃圾郵件攻擊行動，並定期翻新其散播的機制，因此對大型企業來說永遠是一項威脅。

MuddyWater 網路間諜行動同樣也仰賴一些眾所周知的技巧：網路釣魚郵件、水坑式攻擊、巨集惡意程式，以及 PowerShell 工具⁶⁶。其攻擊或許並未用到零時差漏洞或精密惡意程式，但卻能一再誘惑受害者上當，下載並開啟含有後門程式的文件⁶⁷。最近一次，該行動使用了一種名為「Powerstats v3」的多重階段 PowerShell 後門程式以及 13 種開放原始碼漏洞攻擊後續輔助工具來協助他們在成功入侵系統之後進一步蒐集登入憑證或取得系統管理權限⁶⁸。

明顯老舊的攻擊技巧至今仍屢試不爽，這突顯出一項事實，那就是企業需要重新檢討或制定新的網路資安策略：從提升員工的資安意識和修補系統漏洞、到嚴格控管整個網路基礎架構，並且僅開放絕對必要的存取權限。

犯罪集團依然仰賴虛擬加密貨幣挖礦來獲利

虛擬加密貨幣挖礦惡意程式依然是偵測數量最多的威脅

儘管自 2018 年以來虛擬加密貨幣挖礦惡意程式的偵測數量一直在持續減少，但根據 Smart Protection Network 全球威脅情報網的資料顯示，這類惡意程式仍是 2019 上半年偵測數量最多的威脅。

近來，虛擬加密貨幣再度抬頭，使得市場瀰漫著一股樂觀的情緒，也促使網路犯罪集團再次投入挖礦的行列，暗中從事非法挖礦行動。例如全世界最廣為人知的比特幣 (Bitcoin)，其價值在過去 7 個月來不斷上漲，在今年 6 月達到 12,000 美元的高峰，較年初翻了三倍⁶⁹。

門羅幣 (Monero) 的價值從今年年初至 6 月也同樣翻了三倍，儘管其最高點只到 117 美元⁷⁰，但它在網路犯罪集團之間依舊相當受到歡迎，甚至逐漸成為挖礦惡意程式偏愛的虛擬加密貨幣⁷¹。由於門羅幣幾乎能提供完全的匿名性，因此受到網路犯罪集團的青睞也就不令人意外⁷²。而且門羅幣不像比特幣需要使用專門的硬體或客製化專屬設備來挖礦⁷³。

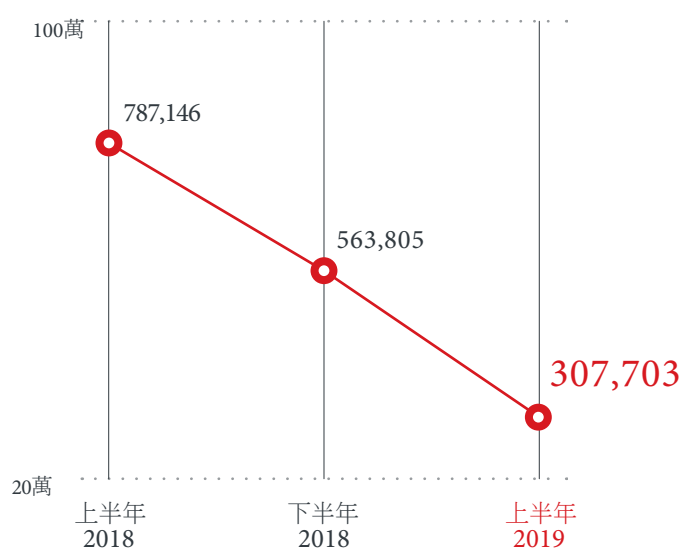


圖 8：儘管趨勢正在下滑，但虛擬加密貨幣挖礦惡意程式仍是偵測數量最多的威脅 (就檔案式威脅來看)：
虛擬加密貨幣挖礦惡意程式相關的檔案式威脅偵測數量半年期比較。

虛擬加密貨幣挖礦威脅進一步演化出複雜的行為

此外，虛擬加密貨幣挖礦威脅也更加成熟。有許多威脅開始採用一些原本只有針對性攻擊或資訊竊盜攻擊行動才會使用的進階駭客工具、模組化惡意程式，以及錯綜複雜的感染程序。

今年 2 月，我們曾經分析過一個顯然模仿 Korkerds 的 Linux 威脅會將受害系統原本感染的虛擬加密貨幣挖礦程式移除，然後再安裝自己的挖礦惡意程式⁷⁴。同月，我們也發表了一篇研究指出某個虛擬加密貨幣挖礦威脅會使用 Radmin 和 Mimikatz 駭客工具來蒐集登入憑證以取得系統管理權限，它甚至會大費周章地利用隨機命名的檔案來隱藏自己的活動並且只在假日才發動攻擊 (以盡可能避免企業發現)，這一切都是為了掩蓋自己的痕跡⁷⁵。

正如我們在 4 月份的一份報告中指出，有個運用多重散布技巧來執行 PCastle 腳本的攻擊行動會進一步在受害系統植入門羅幣挖礦程式⁷⁶。雖然我們在幾個國家都偵測到這項攻擊行動，但其 5 月份的一波後續攻擊最後還是回到了一開始的目標，也就是中國境內的系統。不過這一次它採用了一種多重層次的無檔案手法來執行 PCastle⁷⁷。

許多虛擬加密貨幣挖礦威脅顯然都是利用資安上的漏洞。比方說，駭客利用了知名協作軟體 Confluence 的一個漏洞來散布某個虛擬加密貨幣挖礦程式，該程式甚至還內含一個專門用來掩蓋其活動的 Rootkit⁷⁸。此外，也有一些專門從事挖礦的殭屍網路 (Botnet) 惡意程式變種會透過開放的連接埠來擴散至其他 Android 裝置⁷⁹，並內含一個以 Perl 撰寫的後門程式元件具備發動分散式阻斷服務 (DDoS) 攻擊的能力⁸⁰。還有另一種演化路線是使用開放原始碼程式設計語言 Go (也就是 Golang) 撰寫的惡意程式來掃描是否有電腦還在使用含有漏洞的軟體，進而散布虛擬加密貨幣挖礦程式⁸¹。

伺服器 and 雲端環境成為惡意虛擬加密貨幣挖礦活動的賺錢工具

2017 與 2018 年，惡意虛擬加密貨幣挖礦活動的重心在於利用各種技巧試圖讓系統感染挖礦程式，然而 2019 上半年，加密虛擬貨幣挖礦程式很明顯地將目標轉向伺服器以及我們所預言的雲端環境⁸²。越來越多網路犯罪集團開始利用雲端基礎架構來挖礦，包括使用已入侵的容器平台以及惡意的 Docker 容器映像等等⁸³。

正如我們在 3 月中指出，有某項服務利用 Docker Control API 來散布門羅幣挖礦程式。該服務的惡意行徑包括：搜尋暴露在外或組態設定不當的容器映像，然後讓駭客利用此 API 來執行一些指令，例如使用駭客指定的映像建立新的容器⁸⁴。今年 5 月我們也曾發表過一個類似案例：我們發現某個公開的 Docker Hub 儲存庫正在提供內含虛擬加密貨幣挖礦軟體二進位檔案的映像，該映像甚至內含一個腳本，疑似用來搜尋更多 API 暴露在外的 Docker 主機進而加以感染⁸⁵。

同樣在 5 月，某個虛擬加密貨幣挖礦攻擊行動據稱會利用 Jenkins 自動化伺服器網站架構中的一個漏洞來執行 Kerberods 惡意程式，該程式接著會在受害系統植入門羅幣挖礦惡意程式⁸⁶。在更早之前 2018 年初發生的一個事件當中，歹徒也曾利用一個 Jenkins 漏洞來散布 JenkinsMiner 惡意程式，據稱歹徒因而獲利 10,800 個門羅幣 (在事件曝光當時至少值 300 萬美元)⁸⁷。

近來這波趨勢轉變的原因有幾點：首先，端點防護在偵測及攔截本機虛擬加密貨幣挖礦程式的能力已更上層樓。其次，專門提供腳本讓網站經營者內嵌到自家網站以利用訪客的瀏覽器來挖礦的知名 Coinhive 服務在今年 3 月遭到關閉⁸⁸，讓網路犯罪集團損失了一項重要工具。

對歹徒而言，伺服器和雲端平台不單只是可行的替代方案而已，公有雲基礎架構其實是很誘人的攻擊目標。就算集結了大量的裝置或端點，也無法與雲端基礎架構幾乎取之不盡、用之不竭的資源相提並論。對網路犯罪集團來說，這根本就是一座金礦，而且是一座無人看守、無人戒備的寶藏。所以他們當然非常樂意利用這類因為組態設定不當而造成的漏洞來植入並散布惡意程式。

虛擬加密貨幣挖礦活動的破壞性或許不如勒索病毒那樣驚人，但對企業的影響卻不單只是運算資源遭人盜用或是系統效能問題而已。尤其對雲端部署環境來說，它可能造成雲端運算帳單爆表，尤其當用量超過原先設定的配額時。此外，還可能造成企業內部署的伺服器或資料中心硬體設備耗損與耗電量增加。不但如此，當企業環境內被植入虛擬加密貨幣挖礦程式時，一些用來執行定期作業或特定工作的系統，很可能會出現服務異常、不規律或不穩定的狀況⁸⁹。

網路犯罪集團當然希望他們的挖礦程式可以散布得越廣越好，而且要盡可能不被發現。這些程式躲藏得越久，就能幫歹徒賺更多的錢。隨著資安威脅的精密度與擴散能力日益增強，企業若能提高對系統的掌握與監控能力，將有助於發現其網路基礎架構當中暗藏的惡意活動和進行中的威脅。

暴露在外及不安全的雲端環境造成連鎖反應

雲端相關的威脅，包括虛擬加密貨幣挖礦威脅，通常都是利用組態設定上的錯誤或不安全的登入憑證來駭入雲端。這類經常被忽略的風險，事實上已演變成一大資安問題，尤其對應用程式元件與 API 而言⁹⁰。而且除了立即的風險之外，組態設定錯誤還可能造成連鎖反應。例如，不安全的 API 很可能引來一些利用網路掃瞄工具來尋找受害者的駭客，他們隨時都在搜尋含有漏洞或組態設定錯誤的 API，進而加以利用。

在一個雲端環境當中，組態設定錯誤意味著雲端運算實體很可能暴露在駭客入侵的危險當中。例如，2019 上半年就出現過不少儲存敏感資訊的雲端基礎架構被人發現缺乏密碼保護⁹¹ 或是缺乏安全認證及防火牆機制⁹² 的案例。

雖然組態設定錯誤的問題聽起來似乎不難修正，但要正確設定一個雲端運算實體的組態，其實是一件相當複雜且需要專業知識的工作，更何況是設定整個雲端基礎架構。而且，這項工作一旦沒有確實做好，會讓雲端內的任何資安機制都無法徹底遏止駭客的入侵。採用 DevOps 的企業更是如此，因為 DevOps 是一種強調靈活性以縮短開發及交付週期的方法⁹³，因此一方面要盡量提高開發與交付應用程式或產品的速度，一方面又要遵守稽核、監控及資料隱私規範，如歐盟通用資料保護法 (GDPR)⁹⁴。

訊息威脅更多元化

假冒 Office 365 的網路釣魚網站顯著增加

根據趨勢科技 Smart Protection Network 的資料，網路釣魚活動在 2019 上半年仍持續減少。相較於 2018 下半年，我們發現已攔截的網路釣魚網址存取次數 (也就是所有試圖瀏覽這類網站的次數) 減少了 9%；另外，已攔截的非重複用戶端 IP 存取網路釣魚網址次數 (也就是原本可能因此遭到感染的使用者數量) 減少了 18%。

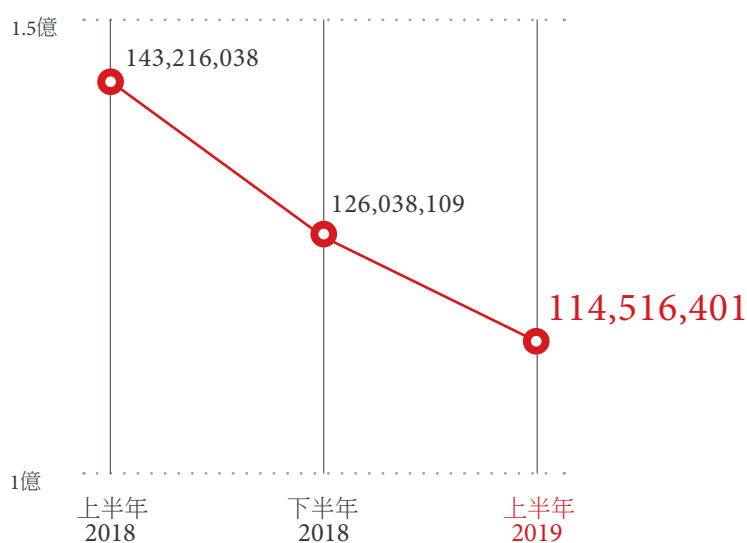


圖 9：已偵測到的網路釣魚網站試圖瀏覽次數持續減少：
已攔截的網路釣魚網址存取次數半年期比較 (同一個被攔截的網址若被存取三次仍算三次)。

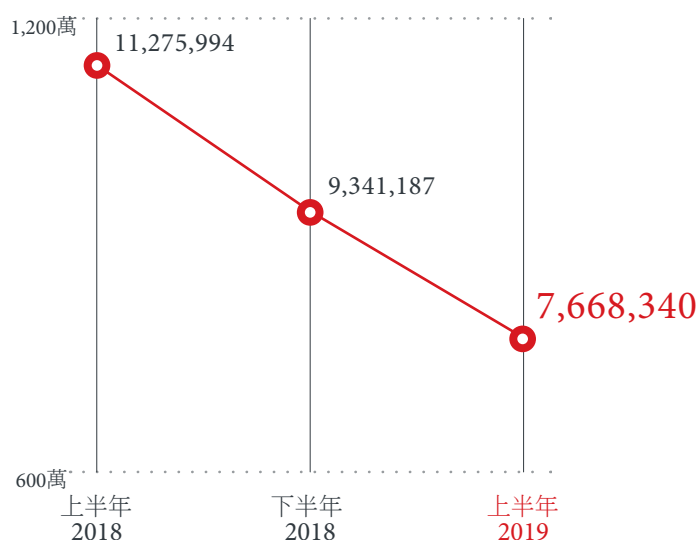


圖 10：原本可能遭網路釣魚網站感染的使用者數量進一步減少：

已攔截的非重複用戶端 IP 存取網路釣魚網址次數半年期比較 (同一台電腦若試圖存取同一個網址三次則只算一次)。

這股下滑的趨勢背後可能有部份原因是使用者對網路釣魚詐騙的防範意識提升。但有趣的是，在對比 2018 下半年與 2019 上半年的資料之後，我們發現這些已攔截的非重複網路釣魚網址當中，假冒 Microsoft Office 365 的網址增加了 76%，尤其是 Outlook。這股趨勢的具體證明之一就是一項研究指出今年三月有 29% 的企業機構，其 Office 365 帳號遭駭客入侵，因此光該月就有 150 萬封惡意垃圾郵件是利用這些被駭的帳號所散發⁹⁵。而推升這股趨勢的網路犯罪集團有可能是偏愛使用雲端或行動平台 (如 Office 365) 來詐騙使用者和企業。

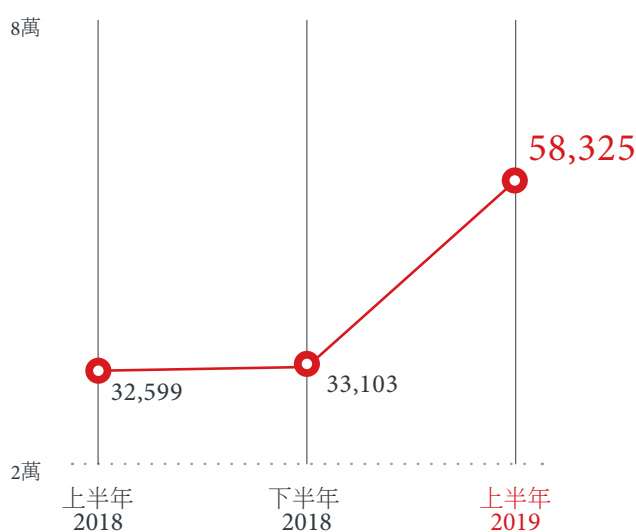


圖 11：假冒 Office 365 (含 Outlook) 的網址數量增加 76%：已攔截的 Office 365 相關非重複網路釣魚網址半年期比較。

就網路犯罪集團而言，如此涇渭分明地重新定位，意味著他們正朝著開發多重樣貌、多重平台的社交工程威脅方向發展⁹⁶。正如我們在 1 月的時候指出，某些 Android 應用程式宣稱提供美肌修圖功能，但其實卻會將不知情的使用者帶到網路釣魚網站，然後竊取他們所要修的圖⁹⁷。今年 3 月，我們發現了一起網路釣魚行動利用水坑式攻擊技巧，先透過情蒐偵查來入侵目標網站，然後在網站植入假冒的登入畫面來騙取使用者的登入憑證⁹⁸。還有另一起我們在 4 月份披露的攻擊行動，網路釣魚駭客使用 Google Chrome 和 Mozilla Firefox 瀏覽器的 SingleFile 擴充元件來將其惡意的登入網頁加密編碼，甚至包括了一個假冒知名支付流程處理網站的網頁⁹⁹。

同樣在 3 月份，美國俄勒岡州民眾服務部 (Oregon Department of Human Services) 宣布有超過 35 萬名民眾的個人醫療資訊遭到外洩，原因很可能是駭客藉由網路釣魚駭入了員工的電子郵件帳號所造成¹⁰⁰。此外，網路犯罪集團也不斷利用受害人電子郵件信箱內既有的討論串來散布惡意程式，例如今年 4 月出現的某個 Emotet 變種就是最好的例子¹⁰¹，這種手法最早出現在去年某個專門散布 Ursnif 惡意程式的攻擊行動¹⁰²。

駭客將惡意郵件混入既有的電子郵件討論串中，可讓收件人較不容易起疑，不像新的郵件那麼容易被判定成詐騙郵件。駭客利用企業自身的資料或資產來對企業員工發動攻擊，就不容易讓人起疑。不僅如此，這些攻擊還可運用一些更複雜的技巧，例如使用一些罕見的檔案類型¹⁰³、老舊的通訊協定¹⁰⁴，甚至使用原本被認為安全的通訊協定¹⁰⁵。

變臉詐騙仍蓬勃發展

使用變臉詐騙 (BEC) 技巧的攻擊，或許比使用進階惡意程式的網路釣魚或針對性攻擊在技術上單純許多，至少變臉詐騙只須熟悉並企業內部運作，然後假裝成內部人員來啟動內部流程即可。不過，歹徒卻相當仰賴所謂的社交工程技巧，例如假裝成企業高層主管 (通常是執行長)，利用一種緊急的口吻來促使電子郵件收件人 (通常是財務部門) 執行其要求。若要說美國聯邦調查局 (FBI) 最新的報告能給我們什麼樣的教訓，那就是：這類詐騙的受害代價越來越高。

根據 FBI 網際網路犯罪申訴中心 (Internet Crime Complaint Center，簡稱 IC3) 所發布的數字顯示，變臉詐騙已成為犯罪集團獲利非常豐厚的詐騙手法。該單位估計，2018 年美國境內企業因變臉詐騙 (BEC) 或電子郵件帳號入侵 (EAC) 所蒙受的損失就超過了 12 億美元，該單位這一整年當中共接獲了 2 萬多起相關的通報案例¹⁰⁶。

根據我們的資料，變臉詐騙從 2018 下半年一直活躍至 2019 上半年，其詐騙嘗試攻擊活動數量大約成長了 52%。而且和去年下半年的情況一樣，受害企業大多分布於美國、澳洲和英國。雖然這或許也呼應了我們客群的分布情況，但這些國家確實是許多大型與跨國企業總部所在之處，因此詐騙集團鎖定這些地區也算相當合理。

不令人意外地，執行長依然是變臉詐騙最常假冒的對象，遠遠超越其他企業高層人士。

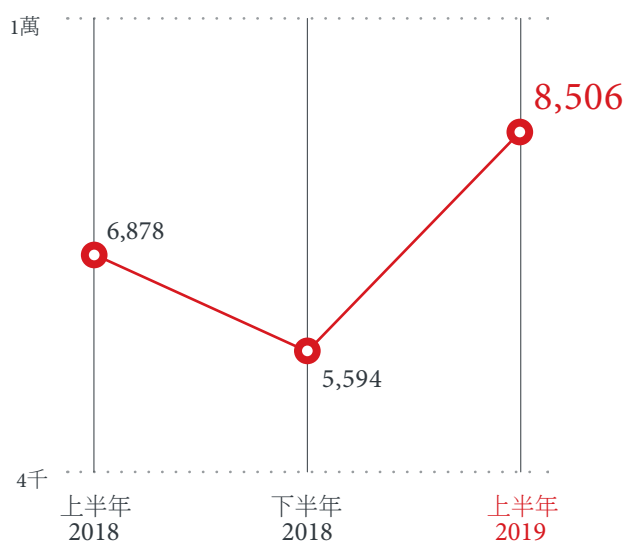


圖 12：變臉詐騙出現成長：

變臉詐騙嘗試攻擊數量半年期比較。

註：這項資料代表偵測到的變臉詐騙所有嘗試攻擊案例，不論攻擊成功與否。

變臉詐騙包括了執行長 (CEO) 詐騙。

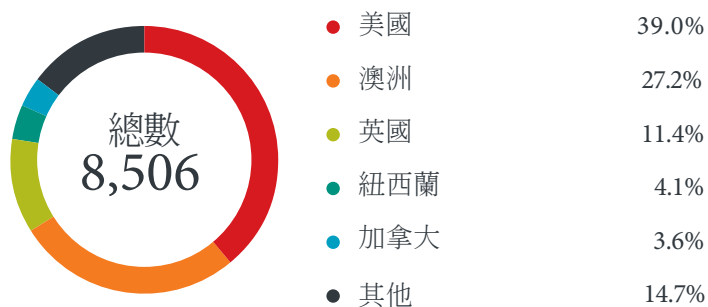


圖 13：2019 上半年，一些被視為全球商業中心的國家，其變臉詐騙嘗試攻擊案例也較多：

變臉詐騙分布國家。

註：這項資料代表偵測到的變臉詐騙所有嘗試攻擊案例，不論攻擊成功與否。

變臉詐騙包括了執行長 (CEO) 詐騙。



圖 14：執行長 (CEO) 依然是變臉詐騙最常假冒的對象：

2019 上半年變臉詐騙假冒的職務對象分布。

註：這項資料代表偵測到的變臉詐騙所有嘗試攻擊案例，不論攻擊成功與否。
變臉詐騙包括了執行長 (CEO) 詐騙。

變臉詐騙集團一開始採用的方法相對簡單，通常只需駭入或假冒 CXX 級高階主管的電子郵件，就能誘騙受害人匯款。但從 2019 上半年的一些案例就可看出其活動範圍已經擴大，包括：公關公司¹⁰⁷、跨國企業區域辦公室¹⁰⁸，甚至是學區單位¹⁰⁹。

最知名的變臉詐騙集團 London Blue 這些年來也開始以其他員工為假冒的對象，例如：財務總監與高階主管助理¹¹⁰，而其他的詐騙集團也曾鎖定人事部門人員¹¹¹。這一點符合我們之前的預測：變臉詐騙集團將開始鎖定企業內一些層級較低的員工¹¹²。除此之外，受害機構也開始出現明顯的變化：從傳統企業移轉至非營利機構和宗教機構，例如美國俄亥俄州的某個教會就在 4 月份遭變臉詐騙攻擊而損失 175 萬美元，歹徒駭入了數名員工的電子郵件帳號，再利用這些帳號詐騙該機構內的其他人員將款項匯入某個假冒的外包商帳戶¹¹³。

垃圾郵件所帶來的性愛勒索案例暴增

今年 4 月¹¹⁴，FBI 指出其 2018 年所接獲的勒索案件仍以性愛勒索為大宗¹¹⁵。我們在去年年底左右發表的 2019 年資安預測指出，數位勒索 (尤其是性愛勒索) 的案例將會增加¹¹⁶。毫無意外地，趨勢科技 Smart Protection Network 全球威脅情報網的資料也顯示性愛勒索相關的垃圾郵件偵測數量從 2018 下半年至 2019 上半年大幅成長了 319%。

2019 上半年最著名的性愛勒索案例就是 4 月份的一波以義大利文使用者為主要目標的垃圾郵件攻擊，歹徒威脅受害者若不在指定期限內支付贖金，就要將性愛影片寄給其通訊錄上的聯絡人¹¹⁷。

性愛勒索通常會利用被害人的恐懼心理來逼迫他們遵從歹徒的要求。這類詐騙在短期之內不會消失，就近期的資料來看，甚至可能會出現更大規模的行動。

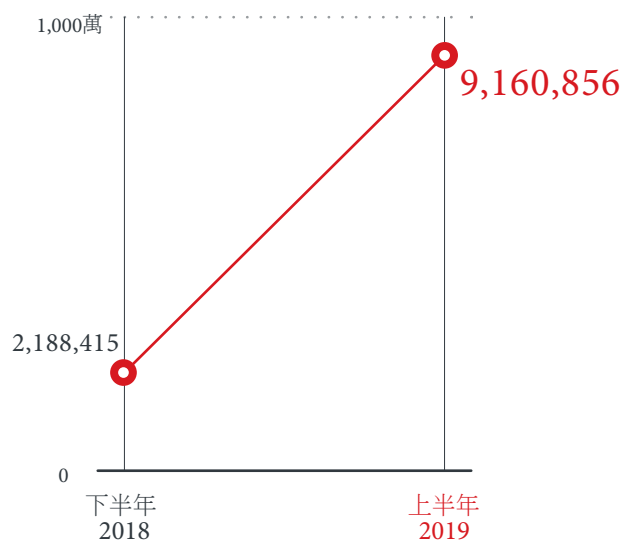


圖 15：垃圾郵件所帶來的性愛勒索案例翻了四倍以上：
性愛勒索相關垃圾郵件偵測數量半年期比較。

無所不在的漏洞讓修補更新顯得更加重要

更多硬體層次的漏洞曝光

2018 年初，Meltdown 和 Spectre 這兩個涉及微處理器 CPU 指令推測執行 (speculative execution) 技術上的資安漏洞相繼被揭露¹¹⁸，為資安漏洞的防範與修補帶來全新境界的挑戰。事實上，甚至連早在 1995 年所生產的處理器都受到波及¹¹⁹，使得這兩項漏洞的衝擊幾乎無所不在。這兩項看似突然冒出來的硬體層次漏洞，其實與網路資安界經常看到的軟體漏洞有一定程度的關聯。

今年 2 月，研究人員示範了一項概念驗證攻擊，利用 Intel Core 和 Xeon 系列 CPU 的軟體保護擴展 (SGX) 指令集當中的安全區 (Enclave) 來隱藏惡意程式，躲避防毒軟體的偵測。安全區原本的設計用意是為了讓資料保護在安全區內以管制其存取，但卻反而可能遭駭客濫用，將惡意程式碼放入安全區內，然後再將惡意程式碼嵌入使用者在不知情下安裝的應用程式內¹²⁰。

今年 5 月，研究人員揭露了數個現代 Intel 處理器的微架構資料取樣 (Microarchitectural Data Sampling，簡稱 MDS) 漏洞。從 ZombieLoad、Fallout 和 Rogue In-Flight Data Load (RIDL) 這些旁路攻擊 (side-channel attack) 手法就可看出這類漏洞的威脅性，其攻擊方式與 Meltdown 和 Spectre 漏洞類似。這些旁路攻擊手法可讓駭客執行程式碼或讀取原本應該被處理器的架構保護的資料¹²¹。

高危險的漏洞揭露狀況更受到關注

從影響層面來看，2019 上半年所揭露的漏洞，可說是「無所不在」。的確，經由我們 Zero Day Initiative (ZDI) 漏洞懸賞計畫所揭露的漏洞絕大多數都屬於高嚴重性等級。

其中最值得注意的就是 BlueKeep 漏洞 (CVE-2019-0708)，這是一個遠端桌面服務的重大漏洞，在 5 月份登上媒體版面，以其「蠕蟲化」特性聞名，因為這項漏洞可讓惡意程式像 WannaCry 利用 EternalBlue 漏洞那樣四處繁衍，有如蠕蟲一般¹²²。其所帶來的風險大到讓 Microsoft 甚至針對原本已終止支援的作業系統 (Windows 2003 和 Windows XP) 都釋出修補更新¹²³。

無獨有偶，同樣在 5 月，一位網路代號「SandboxEscaper」的研究人員公布了一份針對 Windows 10 工作管理員 (Task Manager) 當時的零時差漏洞 (CVE-2019-1069) 的攻擊程式碼。受影響的作業系統包括：32 及 64 位元 Windows 10、Windows Server 2016 和 2019，甚至連 Windows 8 也未能逃過一劫，此漏洞可讓駭客提升權限來存取原本受到保護的檔案¹²⁴。

無 (0.0)	低 (0.1-3.9)	中 (4.0-6.9)	高 (7.0-8.9)	重大 (9.0-10.0)
0	107	101	335	40

表 2：雖然歸類為「重大」等級的漏洞相對少數，但許多被揭露的漏洞其衝擊層面都很廣：
2019 上半年經由我們 ZDI 漏洞懸賞計畫揭露的漏洞嚴重等級分布狀況。
依據 Common Vulnerability Scoring System (CVSS) v3.0 的標準。

除此之外，容器平台與 DevOps 工具的漏洞揭露狀況更令人擔憂。隨著這類軟體的日益普及，這一點不令人意外。但這些漏洞所衍生的風險，卻也突顯出盡可能在工作流程或開發流程早期融入資安防護的重要。

在這類所有漏洞當中，最值得注意的是 Docker 和 Kubernetes 等容器平台執行時期元件 runC 的一個漏洞 (CVE-2019-5736)。這項漏洞一旦遭攻擊得逞，駭客就能完全掌控容器所在的主機，並且將惡意容器部署到線上生產環境¹²⁵。另一個重要漏洞是 CVE-2019-1002101，這是一個 Kubernetes 指令列介面工具的漏洞，可用來執行指令並管理前一個漏洞 (CVE-2018-1002100) 所衍生出來的資源¹²⁶。此漏洞一旦遭攻擊得逞，駭客就能引誘使用者下載一個惡意的容器映像，或者再配合另一個漏洞來非法存取某個容器¹²⁷。

此外，DevOps 團隊經常使用的知名工作流程自動化工具 StackStorm 也被發現了一個漏洞 (CVE-2019-9580)。此漏洞可讓駭客非法存取暴露在外的伺服器，並在伺服器上執行任意指令¹²⁸。

Microsoft 揭露的漏洞數量最多；工業控制系統 (ICS) 的資安公告數量減少

根據我們擁有 3,500 多名獨立研究人員參與的 ZDI 漏洞懸賞計畫所統計的資料，2019 上半年，在所有家用與辦公室軟體廠商當中，Microsoft 所發出的資安公告是最多的，其中許多都和 Windows、Office 及 Internet Explorer 有關。然而，這上半年所揭露的漏洞絕大部分卻都與工業控制系統 (ICS) 軟體有關。

即便如此，2019 上半年所揭露的 ICS 軟體相關漏洞數量還是比 2018 下半年減少 36%，減少的原因可能有幾點，包括：業界整體的網路資安意識提升、更新修補生態體系更加完備，以及廠商為了遵從法規而適時負責任地揭露資訊，例如歐盟網路資訊安全規範 (NIS Directive) 即要求歐盟的關鍵基礎架構廠商必須改善自身的資安情況¹²⁹。

有趣的是，ICS 軟體相關的漏洞，包括監控與資料擷取 (SCADA) 環境的漏洞，有半數都出現在 LAquis SCADA 軟體以及 Advantech WebAccess。前項軟體產品當中即包含了人機介面 (HMI)，而後者則是網頁版的人機介面。在 SCADA 環境中，人機介面基本上就是負責關鍵基礎架構管理與各項控制系統監控的中樞，直接左右生產環境的運作。也因此才會成為犯罪集團覬覦的重要目標，足以讓歹徒切斷企業的營運。但麻煩的是，要確保人機介面的安全並非一件容易的事，因為人機介面不僅用來管理營運技術 (OT) 基礎架構，更會連接工業物聯網 (IIoT) 上的裝置，甚至連接傳統的資訊技術 (IT) 系統，如此一來將使得駭客有更大的攻擊面可入侵關鍵基礎架構。

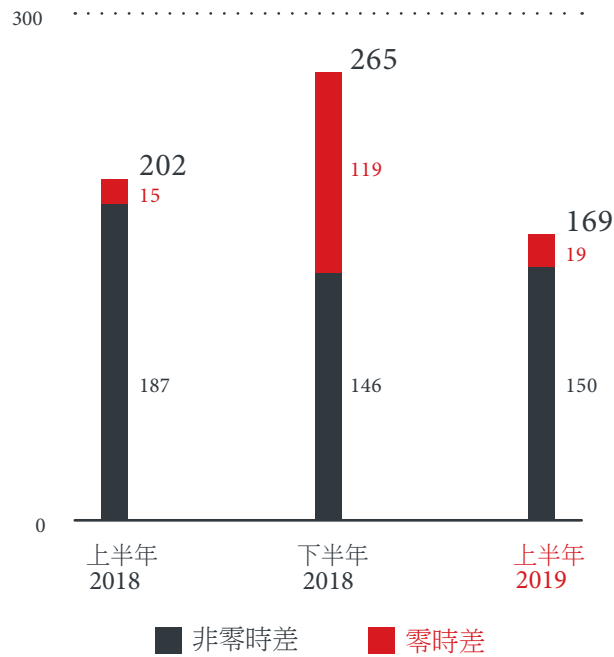


圖 16：ICS 軟體相關的漏洞減少：
經由我們 ZDI 漏洞懸賞計畫揭露的 ICS 相關漏洞半年期比較。

漏洞 — 不論是未知、已知 (n-day) 或是老舊系統與軟體上發現的漏洞，對企業來說都是一種無形的警惕，讓企業無時無刻都不能掉以輕心。基本上，網路犯罪集團沒有理由不會重新攻擊已知的舊漏洞，因為歹徒永遠能夠利用漏洞修補的空窗期來發動攻擊。例如今年 4 月，駭客就攻擊了 Oracle WebLogic 的一個零時差漏洞 (CVE-2019-2725)，當時 Oracle 甚至都還來不及發布修補更新。此外，還有像 BlueKeep 遠端桌面服務漏洞，以及資安研究人員 SandboxEscaper 所揭露的重大漏洞，都只需一台未能即時修補的系統，就能讓更多其他的系統也遭池魚之殃。

立即修補零時差漏洞和已知漏洞的作法確實很好，但事情卻不如想像中的容易。事實上，根據今年 4 月發表的一份調查報告顯示，絕大多數的企業都會為了避免造成停機而延後更新修補¹³⁰。這問題如果遇上一些老舊及內嵌式系統，例如 ICS 所用的系統，那問題更將雪上加霜，因為這些系統的廠商很可能早已不再釋出更新¹³¹。除了採用一些其他機制 (如虛擬修補) 來消彌這方面的資安漏洞之外，很重要的一點是企業必須確實掌握哪些漏洞會對他們的系統造成衝擊，包括是否可被攻擊¹³² 以及實際的風險與影響有多大¹³³，如此企業才能更準確地評估哪些漏洞需要立即處理。

IoT 和 IIoT 資安依然是一項重大問題

IoT 已成為殭屍網路與蠕蟲大戰的主戰場

據估計，至 2021 年，全球使用中的 IoT 裝置總數將達 250 億之譜¹³⁴，也難怪駭客已經開始在該領域蠢蠢欲動。

的確，2019 上半年充斥著各種針對這類裝置的惡意程式，專門利用這類裝置的組態設定錯誤與其他資安弱點。事實上，根據趨勢科技 Smart Home Network 解決方案的監測資料，可能遭駭客用來對內發動攻擊的路由器數量 (駭客從網際網路駭入路由器，然后再攻擊與路由器連接的裝置) 與 2018 下半年相比仍持續穩定成長，目前已超過 50 萬。

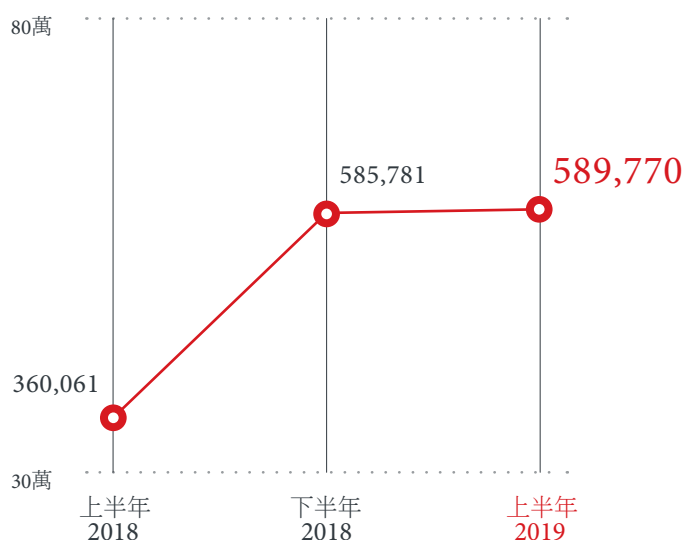


圖 17：路由器上的活動 (包含可能為駭客攻擊的活動) 依然維持穩定：可能遭駭客用來對內發動攻擊的路由器數量半年期比較。

註：可能為駭客攻擊的活動在偵測上會判定為與威脅活動密切關聯的高風險事件。

正如我們先前所預測¹³⁵，IoT 已成為殭屍網路與蠕蟲開拓感染裝置的最新戰場。目前參與這場 IoT 殭屍網路與蠕蟲大戰的包括 Bashlite¹³⁶ 以及數個 Mirai 變種^{137、138} (如 Omni¹³⁹、Hakai 及 Yowai¹⁴⁰)，它們的共同特徵都是會先掃描感染裝置上是否有其他競爭對手的惡意程式或檔案，若有則將它刪除，然後再植入自己的惡意程式。在這場彼此互打的 IoT 蠕蟲大戰當中，我們也觀察到另一股趨勢：惡意程式們還會進一步利用這些已經變成殭屍的裝置來挖礦，試圖榨出更多利潤¹⁴¹。

至於其他的 IoT 威脅，則避開了這些衝突，試圖走出自己的路。例如今年 5 月出現的 HiddenWasp 惡意程式，就是用於針對性攻擊的第二階段，用來感染已遭到入侵的系統¹⁴²。而一個月後出現的 Silex 則是破壞了數以千計 IoT 裝置的韌體，讓裝置變成磚塊，根本無法使用，除非重新安裝韌體¹⁴³。

隨著物聯網在家庭¹⁴⁴、辦公場所¹⁴⁵ 以及各種產業¹⁴⁶ 的日漸普及 (從食品生產¹⁴⁷、製造¹⁴⁸，到電信¹⁴⁹、醫療照護¹⁵⁰ 等等)，IoT 資安已成為一項重要的資安議題。然而，只要使用者和企業就連最簡單的更換或更新裝置密碼都一直無法做到，那麼 IoT 裝置的資安將只是緣木求魚。

針對真實世界關鍵基礎架構的攻擊突顯 IIoT 資安的重要性

IIoT 已徹底改變了工業環境和關鍵基礎架構的運作方式¹⁵¹。而營運技術 (OT) 和資訊技術 (IT) 的結合，也讓企業得以將營運簡化及自動化，並且更加透明。在這樣的發展下，至 2021 年全球 IIoT 市場預計將達到 1,230 億美元的規模¹⁵²。

然而，這股技術匯流風潮卻也帶來了資安上的風險。一般來說，IIoT 裝置會分散在各個廠房設施，跨區分享各自的資料，並從彼此共用的基礎架構存取資料，然後透過與企業網路甚至與傳統 IT 系統相連的主控台來管理。如此錯綜複雜的關係，很可能形成資安上的漏洞，讓駭客有機可乘。事實上，根據今年 3 月發表的一份調查指出，有 50% 的企業機構在過去兩年當中曾經發生關鍵基礎架構遭駭客攻擊的事件¹⁵³。

最具代表性的 IIoT 惡意程式就是 2017 年攻擊石油及天然氣產業的 Triton 惡意程式 (又名 Trisis)，它會駭入並修改工廠內的「安全儀控系統」(Safety Instrumented System，簡稱 SIS)，此系統算是一種保護措施，可在生產作業發生問題時讓系統進入「安全模式」。駭客一旦入侵了 SIS，就有可能中斷工廠運作，甚至造成實體損害¹⁵⁴。今年 4 月，Triton 惡意程式背後的犯罪集團被發現又攻擊了某個關鍵基礎架構¹⁵⁵。到了 6 月，這個名為「Xenotime」的犯罪集團被發現試圖刺探美國和亞太地區電力公司的工業控制系統¹⁵⁶。

對於關鍵基礎架構來說，導入 IIoT 可確保運作的順暢及安全，這也正是為何 IIoT 的資安至關重要：從實施嚴格的修補政策 (特別是針對老舊系統) 到強制貫徹認證及授權機制，並且確保工業環境裝置之間的資料通道安全¹⁵⁷。

多層式防禦有助於解決今日多重面向的威脅

2019 上半年所見到的威脅，大多為持續性、隱匿且專門利用科技、流程及人員弱點的威脅。

針對能夠就地取材或造成額外資安風險的威脅，一套多層式的縱深防禦能協助企業機構從閘道、網路、伺服器到端點全面削弱或遏止威脅。例如，專門利用 PowerShell 及巨集惡意程式的無檔案式威脅，可透過行為監控來攔截惡意程式相關的行為、透過沙盒模擬分析來將可疑腳本隔離，或是透過入侵防護來防止幕後操縱通訊或資料外傳之類的可疑流量。但是，既要主動監控網路和端點上任何細微的異常狀態或惡意程式感染的徵兆，同時又要兼顧警示通知和修補更新，系統管理員很可能會疲於奔命。為了解決這項複雜問題，企業可尋找一些結合資安專家與資安技術的解決方案，來提供更好的威脅偵測、交叉關聯分析、回應以及矯正。

目前正朝數位轉型邁進的企業，尤其是採用 DevOps 流程的機構，都被迫將許多營運作業或系統移轉或整合至最新的技術或某種形式的雲端基礎架構，但這卻可能帶來一些資安上的風險。雲端基礎架構天生就是瞬息萬變，因此其資安的強化是一項相當挑戰的工作。再加上底層的系統和網路萬一態設定不當、認證機制不足或缺乏，或是與一些老舊的基礎架構整合，就很容易遭到駭客存取或篡改。為此，企業應該將資安融入其採用的技術、工作流程以及程式開發週期當中，或將資安盡可能建置在流程的上游，如此就能降低下游的資安與隱私風險。

此外，社交工程攻擊的防範，也應列為企業網路資安策略的重要一環。在電子郵件閘道部署一些資安解決方案，例如採用機器學習技術來協助偵測可疑的電子郵件內容，就能大幅遏阻威脅。不過，培養一種網路資安的企業文化，包括：提升人員對惡意郵件典型異常狀況的警覺以及定期執行網路釣魚模擬訓練，皆有助於對抗惡意程式，防範網路犯罪集團試圖竊取個人身分識別資訊與財產。

除此之外，企業和一般使用者皆可採用一些資安技術來保護自己的裝置，尤其是實施個人自備裝置 (BYOD) 政策的環境。當然，一些基本的資安措施也很重要，例如：啟用認證功能、強化密碼安全、確保路由器安全、切勿點選或下載意圖或用途曖昧不明的連結或應用程式。任何訊息、產品、服務及好康優惠，只要是看起來太過誘人或太過於急迫，絕大多數都是詐騙。

威脅情勢回顧

2019 上半年，趨勢科技 Smart Protection Network™ 全球威脅情報網總共幫使用者攔截了 268 億次以上的威脅，包含各式各樣的電子郵件、檔案及網址。

26,804,076,261

2019 上半年整體威脅攔截總數

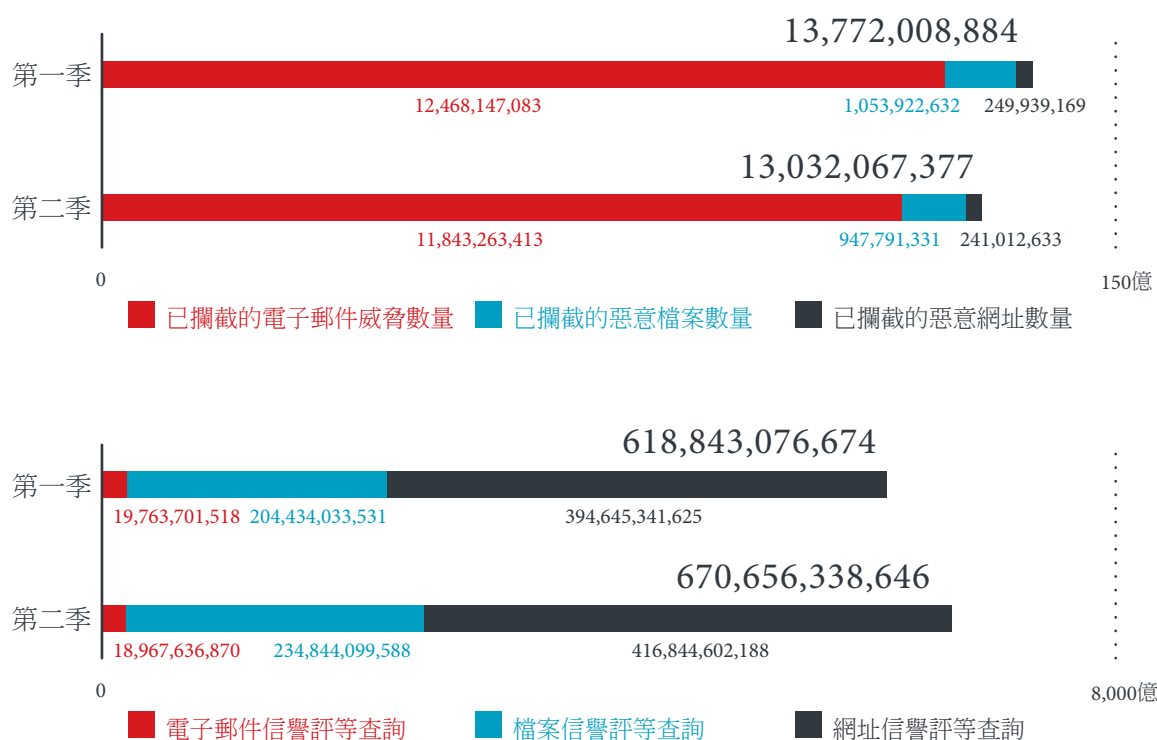


圖 18：該年第二季所攔截的電子郵件、檔案與網址威脅數量略為減少：

已攔截的電子郵件、檔案與網址威脅數量，以及電子郵件、檔案與網址信譽評等查詢數量逐季比較 (2019 上半年)。

網路犯罪與詐騙集團仍持續利用 Android 平台的普及率。根據趨勢科技行動應用程式信譽評等服務 (MARS) 的資料，已攔截的惡意 Android 應用程式，包括惡意應用程式以及可能有害的應用程式 (PAU)，從 2019 年第一季至第二季略為減少，但上半年的整體數量仍相當可觀。

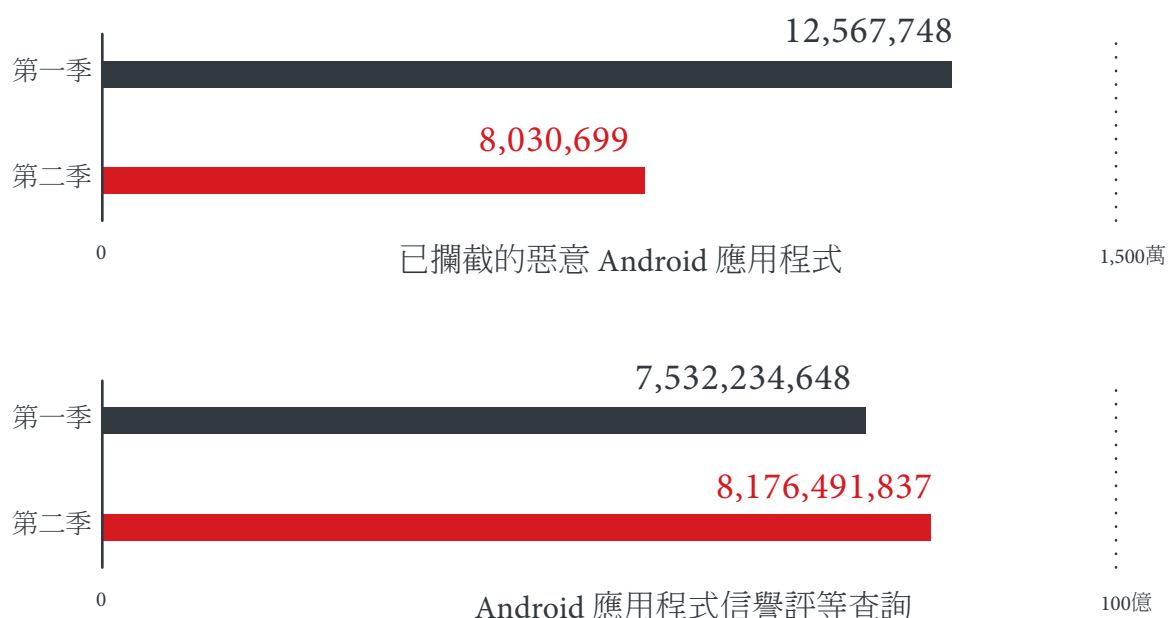


圖 19：該年第二季 Android 平台的威脅數量減少：
已攔截的惡意 Android 應用程式數量以及 Android 應用程式信譽評等查詢數量逐季比較 (2019 上半年)。
根據趨勢科技行動應用程式信譽評等服務 (MARS) 的資料。

儘管新的勒索病毒家族數量較 2018 下半年減少，但從 2019 上半年的重大事件卻能看出勒索病毒仍將是威脅情勢中的常客。

新的勒索病毒家族					
ANATOVA	CLOP	DOGOJOKER	JUWON	RABBIT	TIONE
BIGBORB	CORTEX	FCRYPT	LOCKERGOGA	RANNOH	TREE
BITLOCKED	CRAZYCRYPT	FREEZING	LOOCIPHER	RAPID	TUNCA
BLACKROUTER	CRAZYZIP	GOLDENAXE	MAOLOA	REDKEEPER	VEGA
BLUEEAGLE	CRYPONY	GORGON	MONGOLOCK	ROBBINHOOD	XCRY
BONE	CRYPTO	HOLA	PAPJ	SEEDLOCKER	YATRON
BROWEC	CRYPTGO	JAMPER	PHOBOS	SEON	YFISNIFFER
CHATER	CYMRANSOM	JCRY	PONY	SODINOKIBI	

表 3：本期發現 47 個新的勒索病毒家族：
新的勒索病毒家族數量 (2019 上半年)。

根據我們的資料，PDF 是 2019 上半年垃圾郵件附件最常使用的檔案類型，微幅領先 2018 年最流行的 XLS (Microsoft Excel)。

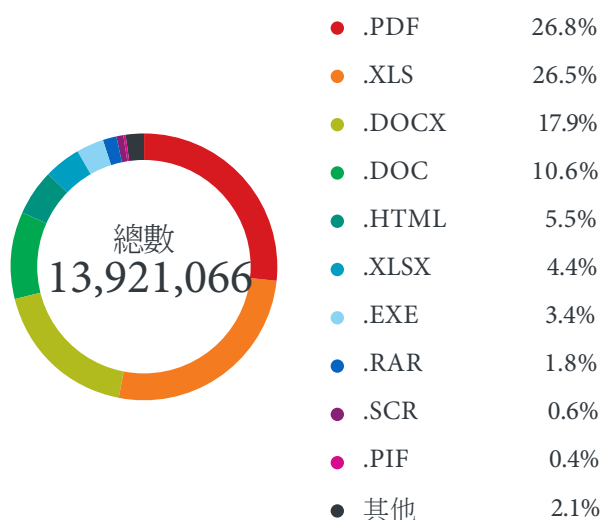


圖 20：PDF 微幅領先 XLS，成為垃圾郵件附件最常用的檔案類型：
垃圾郵件附件檔案類型分布 (2019 上半年)。

漏洞攻擊套件活動儘管增加，但仍舊是攻擊一些舊的漏洞來散布惡意程式，再次突顯系統定期修補與更新的重要。

漏洞攻擊套件	攻擊的漏洞	散佈的勒索病毒	散佈的殭屍網路惡意程式
Magnitude	CVE-2018-8174 (Internet Explorer) CVE-2018-4878 (Adobe Flash Player)	Magniber	
Rig	CVE-2018-8174 CVE-2018-4878	GandCrab Paradise Sodinokibi GetCrypt Buran VegaLocker	Amadey AZORult K POT Predator the Thief PurpleFox SmokeLoader Vidar
GrandSoft	CVE-2018-15982 (Adobe Flash Player) CVE-2018-4878		Ramnit
GreenFlash Sundown	CVE-2018-15982 CVE-2018-8174 CVE-2018-4878	Seon	
Fallout	CVE-2018-15982 CVE-2018-8174 CVE-2018-4878	GandCrab Paradise Maze	Amadey AZORult K POT SmokeLoader Vidar
Spelevo	CVE-2018-15982 CVE-2018-8174	Shade Troidash	Amadey IcedID PsiXBot Vidar

表 4：儘管漏洞攻擊套件似乎又熱絡了起來，但依然是仰賴一些舊的漏洞：
2019 上半年重大漏洞攻擊套件、其攻擊的漏洞，以及散佈的勒索病毒與殭屍網路惡意程式。

2019 上半年殭屍網路惡意程式的肆虐程度，從我們今年第一季至第二季偵測到的殭屍網路連線數量暴增 91% 即可看出端倪。殭屍網路相關的活動，主要源自遭駭客已入侵或挾持的電腦和裝置向駭客的 C&C 伺服器連線。

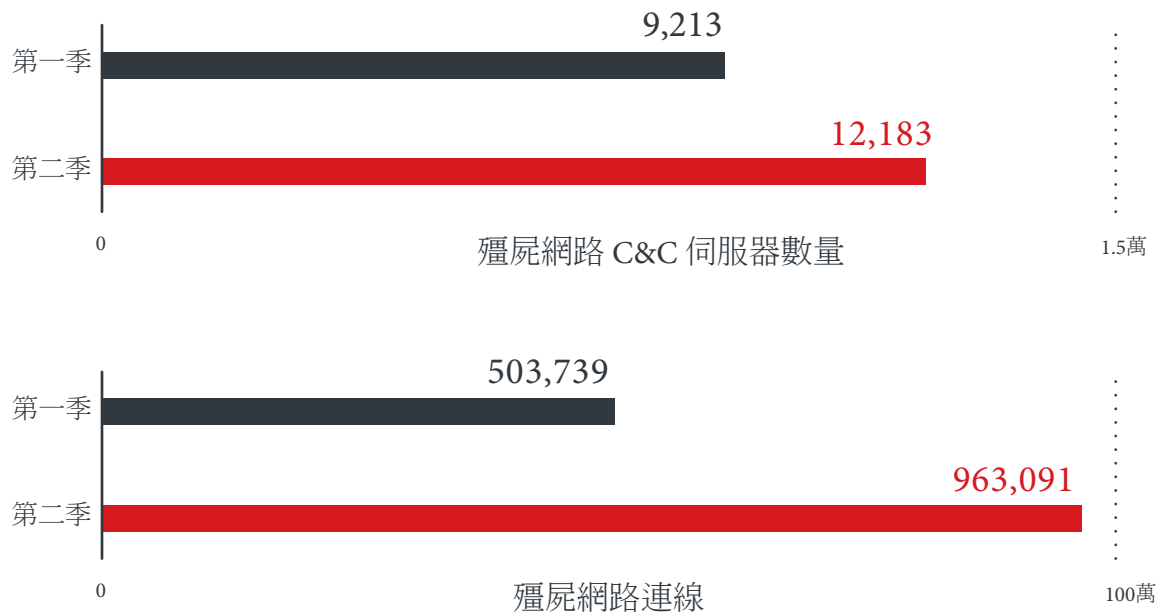


圖 21：殭屍網路相關活動維持上揚的趨勢：

殭屍網路 C&C 伺服器數量與偵測到的殭屍網路連線數量逐季比較 (2019 上半年)。

註：殭屍網路 C&C 伺服器數量為端點查詢或連線的非重複且活躍的 C&C 伺服器數量；殭屍網路連線數量為向 C&C 伺服器查詢或連線的非重複端點數量。

跟去年一樣，Telnet 預設密碼登入活動是該期間觸發最多次的偵測規則 (根據趨勢科技 Smart Home Network 解決方案回報的資料)，再次印證了變更、更新、強化裝置登入憑證的重要性。此外，EternalBlue 及 WannaCry 相關活動的數量亦不容小覷，顯示 EternalBlue 所攻擊的 Server Message Block (SMB) 漏洞，儘管 Microsoft 已透過 MS17-010 安全性公告加以修正，但仍舊是一項持續性的資安風險，為使用者招來 WannaCry 之類的威脅。



圖 22：Telnet 預設密碼登入、虛擬加密貨幣挖礦活動以及 SMB 漏洞攻擊等活動依然相當頻繁：智慧家庭網路主要的對內與對外活動分布 (2019 上半年)。

根據趨勢科技 Smart Home Network 解決方案回報的資料。

註：這些是惡意、處於灰色地帶、或可能有害的應用程式觸發偵測規則時所記錄的活動，意味著駭客攻擊或許正在發生。而與威脅活動密切關聯的事件則歸類在可能為駭客攻擊的活動。

根據趨勢科技 Deep Security™ 和趨勢科技 TippingPoint® Threat Protection System 兩項解決方案所回報的資料顯示，已知 (n-day) 漏洞仍是一項重大的資安問題。針對 SMB 漏洞的攻擊 (也就是 EternalBlue 和 EternalChampion) 仍是最普遍的威脅之一。

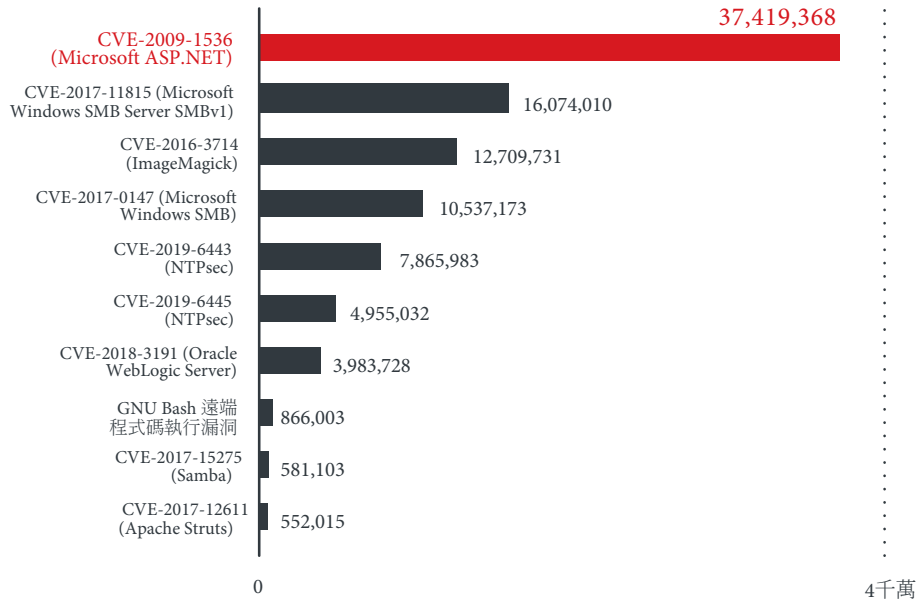


圖 23：一些老早就已釋出修補更新的舊漏洞，依然對企業造成資安風險：
惡意活動偵測規則觸發次數排行榜 (2019 上半年)。
根據趨勢科技 Deep Security 解決方案回報的資料。
註：當駭客試圖攻擊某個漏洞而遭到攔截時就會觸發偵測規則。

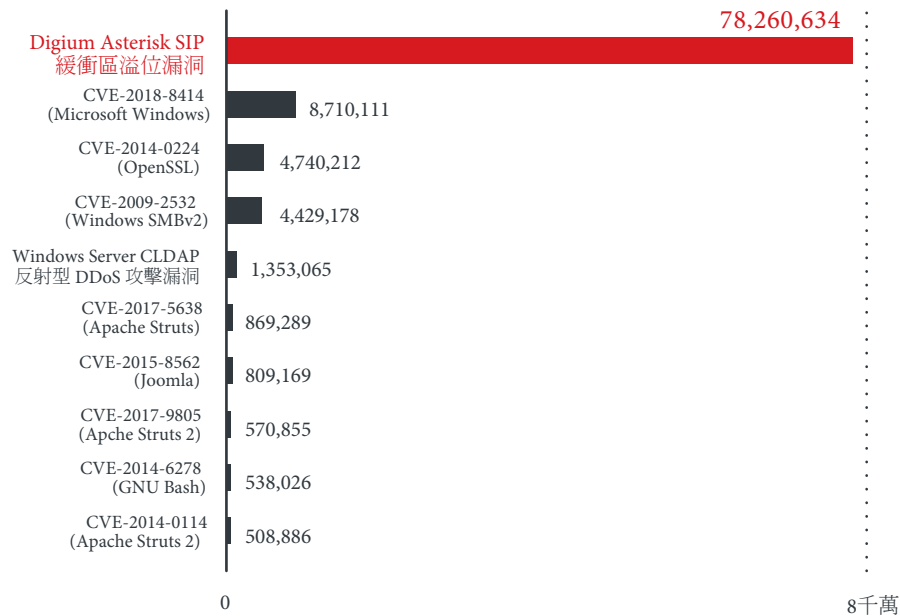


圖 24：經由已修補漏洞的駭客入侵或攻擊依然猖獗：
惡意活動偵測規則觸發次數排行榜 (2019 上半年)。
根據趨勢科技 TippingPoint Threat Protection System 解決方案回報的資料。
註：當駭客試圖攻擊某個漏洞而遭到攔截時就會觸發偵測規則。

參考資料

- 1 Catalin Cimpanu。(2019年6月1日)。ZDNet。「GandCrab勒索病毒犯罪集團表示即將終止營運」(GandCrab ransomware operation says it's shutting down)。上次存取時間2019年7月24日：<https://www.zdnet.com/article/gandcrab-ransomware-operation-says-its-shutting-down/>。
- 2 趨勢科技。(2016年9月7日)。趨勢科技資訊安全新聞。「深層網路上的勒索病毒服務 (RaaS)：對企業的意義為何」(Ransomware as a Service Offered in the Deep Web: What This Means for Enterprises)。上次存取時間2019年7月24日：<https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-as-a-service-what-this-means-for-enterprises>。
- 3 Patricia Mazzei。(2019年6月19日)。The New York Times。「美國佛羅里達州城市遭勒索病毒襲擊，同意支付歹徒60萬美元」(Hit by Ransomware Attack, Florida City Agrees to Pay Hackers \$600,000)。上次存取時間2019年7月24日：<https://www.nytimes.com/2019/06/19/us/florida-riviera-beach-hacking-ransom.html>。
- 4 Patricia Mazzei。(2019年6月27日)。The New York Times。「美國佛羅里達州又一城市遭駭，此次支付了46萬美元贖金」(Another Hacked Florida City Pays a Ransom, This Time for \$460,000)。上次存取時間2019年7月24日：<https://www.nytimes.com/2019/06/27/us/lake-city-florida-ransom-cyberattack.html>。
- 5 Coveware。(2019年7月15日)。Coveware。「Ryuk與Sodinokibi肆虐使得第二季勒索病毒受害金額成長三倍」(Ransomware Amounts Rise 3x in Q2 as Ryuk & Sodinokibi Spread)。上次存取時間2019年7月24日：<https://www.coveware.com/blog/2019/7/15/ransomware-amounts-rise-3x-in-q2-as-ryuk-amp-sodinokibi-spread>。
- 6 Alexander Hanel。(2019年1月10日)。CrowdStrike Blog。「專門鎖定大型目標的Ryuk：又一個獲利豐厚的針對性勒索病毒」(Big Game Hunting with Ryuk: Another Lucrative Targeted Ransomware)。上次存取時間2019年7月24日：<https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/>。
- 7 趨勢科技。(2019年3月20日)。趨勢科技資訊安全新聞。「有關LockerGoga勒索病毒您該知道的事」(What You Need to Know About the LockerGoga Ransomware)。上次存取時間2019年7月24日：<https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware>。
- 8 Joe Tidy。(2019年6月25日)。BBC News。「勒索病毒攻擊如何讓一家公司損失4,500萬英鎊」(How a ransomware attack cost one firm £45m)。上次存取時間2019年8月1日：<https://www.bbc.com/news/business-48661152>。
- 9 Pound Sterling Live。(日期不詳)。Pound Sterling Live。「2019年6月25日：英鎊兌美元歷史匯率」(Historical Rates for the GBP/USD currency conversion on 25 June 2019 [25/06/2019])。上次存取時間2019年8月1日：<https://www.poundsterlinglive.com/best-exchange-rates/british-pound-to-us-dollar-exchange-rate-on-2019-06-25>。
- 10 Manny Fernandez、David E. Sanger與Marina Trahan Martinez。(2019年8月22日)。The New York Times。「勒索病毒攻擊正在考驗美國城市的決心」(Ransomware Attacks Are Testing Resolve of Cities Across America)。上次存取時間2019年8月23日：<https://www.nytimes.com/2019/08/22/us/ransomware-attacks-hacking.html>。
- 11 Doug Olenick。(2019年4月26日)。SC Media。「美國北卡羅來納州格林維爾(Greenville)正從Robbinhood勒索病毒攻擊事件中復原」(Greenville in recovery phase from Robbinhood ransomware attack)。上次存取時間2019年8月13日：<https://www.scmagazine.com/home/security-news/ransomware/greenville-in-recovery-phase-from-robbinhood-ransomware-attack/>。
- 12 Janus Agcaoli與Miguel Ang。(2019年6月6日)。趨勢科技資訊安全新聞。「縮小目標、獲利更大：2019年勒索病毒發展」(Narrowed Sights, Bigger Payoffs: Ransomware in 2019)。上次存取時間2019年8月2日：<https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/narrowed-sights-bigger-payoffs-ransomware-in-2019>。
- 13 Lawrence Abrams。(2019年3月5日)。BleepingComputer。「CryptoMix Clop表示其攻擊的目標是網路而非電腦」(CryptoMix Clop Ransomware Says It's Targeting Networks, Not Computers)。上次存取時間2019年7月24日：<https://www.bleepingcomputer.com/news/security/cryptomix-clop-ransomware-says-its-targeting-networks-not-computers/>。
- 14 Raphael Centeno。(2019年5月8日)。TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)。「Dharma勒索病毒使用防毒工具來分散注意力以掩護惡意活動」(Dharma Ransomware Uses AV Tool to Distract from Malicious Activities)。上次存取時間2019年7月24日：<https://blog.trendmicro.com/trendlabs-security-intelligence/dharma-ransomware-uses-av-tool-to-distract-from-malicious-activities/>。
- 15 趨勢科技。(2019年5月9日)。趨勢科技資訊安全新聞。「最新勒索病毒總整理：仍在發展當中的病毒在網路現身」(Ransomware Recap: Still in Development, Found in the Wild)。上次存取時間2019年7月24日：<https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-recap-still-in-development-found-in-the-wild/>。
- 16 Jon Oliver。(2016年9月19日)。TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)。「暴力破解展示：Crysis勒索病毒鎖定澳洲及紐西蘭企業」(A Show of [Brute] Force: Crysis Ransomware Found Targeting Australian and New Zealand Businesses)。上次存取時間2019年8月1日：<https://blog.trendmicro.com/trendlabs-security-intelligence/crysis-targeting-businesses-in-australia-new-zealand-via-brute-forced-rdps/>。
- 17 趨勢科技。(2019年4月18日)。趨勢科技資訊安全新聞。「NamPoHyu(亦稱MegaLocker Virus)勒索病毒從遠端加密Samba伺服器」(NamPoHyu aka MegaLocker Virus Ransomware Found Remotely Encrypting Samba Servers)。上次存取時間2019年8月2日：<https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/nampohyu-aka-megalocker-virus-ransomware-found-remotely-encrypting-samba-servers>。

- 18 趨勢科技。(2019年5月27日)。趨勢科技資訊安全新聞。「GandCrab 勒索病毒攻擊 MySQL 資料庫」(GandCrab Ransomware Found Targeting MySQL Databases)。上次存取時間 2019年7月24日：<https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/gandcrab-ransomware-found-targeting-mysql-databases/>。
- 19 Augusto Remillano II 與 Robert Malagad。(2019年5月7日)。TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)。「CVE-2019-3396 Redux：Confluence 漏洞遭駭客用於散布虛擬加密貨幣挖礦程式及 Rootkit」(CVE-2019-3396 Redux: Confluence Vulnerability Exploited to Deliver Cryptocurrency Miner With Rootkit)。上次存取時間 2019年7月24日：<https://blog.trendmicro.com/trendlabs-security-intelligence/cve-2019-3396-redux-confluence-vulnerability-exploited-to-deliver-cryptocurrency-miner-with-rootkit/>。
- 20 Lawrence Abrams。(2018年9月11日)。BleepingComputer。「MongoLock 勒索病毒刪除 MongoDB 進行勒索」(Mongo Lock Attack Ransoming Deleted MongoDB Databases)。上次存取時間 2019年8月2日：<https://www.bleepingcomputer.com/news/security/mongo-lock-attack-ransoming-deleted-mongodb-databases/>。
- 21 趨勢科技。(2019年1月8日)。趨勢科技資訊安全新聞。「MongoLock 勒索病毒立即刪除檔案並格式化備份硬碟」(Ransomware MongoLock Immediately Deletes Files, Formats Backup Drives)。上次存取時間 2019年8月2日：<https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-mongolock-immediately-deletes-files-formats-backup-drives/>。
- 22 Buddy Tancio、Ryan Maglaque、Cenen Enalbes 與 Jay Yaneza。(2019年3月14日)。趨勢科技資訊安全新聞。「從託管式偵測及回應服務的角度看 Ryuk 勒索病毒」(Examining Ryuk Ransomware Through the Lens of Managed Detection and Response)。上次存取時間 2019年8月2日：<https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/examining-ryuk-ransomware-through-the-lens-of-managed-detection-and-response/>。
- 23 趨勢科技。(2019年5月21日)。趨勢科技資訊安全新聞。「Ryuk 勒索病毒攻擊目標多元化使不法獲利穩定提高」(Ryuk Ransomware Shows Diversity in Targets, Consistency in Higher Payouts)。上次存取時間 2019年7月24日：<https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ryuk-ransomware-shows-diversity-in-targets-consistency-in-higher-payouts/>。
- 24 Alexander Hanel。(2019年1月10日)。CrowdStrike Blog。「專門鎖定大型目標的 Ryuk：又一個獲利豐厚的針對性勒索病毒」(Big Game Hunting with Ryuk: Another Lucrative Targeted Ransomware)。上次存取時間 2019年7月24日：<https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/>。
- 25 趨勢科技。(2019年3月20日)。趨勢科技資訊安全新聞。「有關 LockerGoga 勒索病毒您該知道的事」(What You Need to Know About the LockerGoga Ransomware)。上次存取時間 2019年7月24日：<https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware/>。
- 26 Kevin Beaumont。(2019年3月22日)。Double Pulsar。「LockerGoga 如何搗倒 Hydro：瞄準大型企業的勒索病毒針對性攻擊」(How Lockergoga took down Hydro — ransomware used in targeted attacks aimed at big business)。上次存取時間 2019年8月2日：<https://doublepulsar.com/how-lockergoga-took-down-hydro-ransomware-used-in-targeted-attacks-aimed-at-big-business-c66551f5880>。
- 27 Erika Mendoza、Jay Yaneza、Gilbert Sison、Anjali Patil、Julie Cabuhat 與 Joelson Soares。(2019年3月29日)。TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)。「趨勢科技 MDR (託管式偵測及回應服務) 發現 Emotet 散播的 Nozelesn 勒索病毒載入程式」(Emotet-Distributed Ransomware Loader for Nozelesn Found via Managed Detection and Response)。上次存取時間 2019年7月24日：<https://blog.trendmicro.com/trendlabs-security-intelligence/emotet-distributed-ransomware-loader-for-nozelesn-found-via-managed-detection-and-response/>。
- 28 Lawrence Abrams。(2019年4月26日)。BleepingComputer。「RobbinHood 勒索病毒深入研究」(A Closer Look at the RobbinHood Ransomware)。上次存取時間 2019年7月24日：<https://www.bleepingcomputer.com/news/security/a-closer-look-at-the-robbinhood-ransomware/>。
- 29 Gilbert Sison 與 Ryan Maglaque。(2019年4月15日)。TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)。「系統管理員帳號遭駭客利用，透過 PsExec 安裝 BitPaymer 勒索病毒」(Account With Admin Privileges Abused to Install BitPaymer Ransomware via PsExec)。上次存取時間 2019年8月2日：<https://blog.trendmicro.com/trendlabs-security-intelligence/account-with-admin-privileges-abused-to-install-bitpaymer-ransomware-via-psexec/>。
- 30 NJCCIC。(2017年8月29日)。NJCCIC。「Bit Paymer」。上次存取時間 2019年7月24日：<https://www.cyber.nj.gov/threat-profiles/ransomware-variants/bitpaymer/>。
- 31 Arnold Osipov。(2019年7月18日)。Morphisec。「BitPaymer 勒索病毒採用新的客製化封裝架構攻擊美國目標」(Bitpaymer Ransomware Leveraging New Custom Packer Framework Against Targets Across the U.S.)。上次存取時間 2019年7月24日：<http://blog.morphisec.com/bitpaymer-ransomware-with-new-custom-packer-framework>。
- 32 Threat Team。(2018年8月13日)。BluVector。「BitPaymer 勒索病毒侵襲美國職業高爾夫球員協會 (PGA) 與某阿拉斯加小鎮」(BitPaymer Ransomware Freezes the PGA and an Alaskan Town)。上次存取時間 2019年7月24日：<https://www.bluvektor.io/threat-report-bitpaymer-ransomware-freezes-the-pga-and-an-alaskan-town/>。
- 33 趨勢科技。(2019年5月7日)。趨勢科技資訊安全新聞。「MegaCortex 勒索病毒攻擊企業網路」(MegaCortex Ransomware Spotted Attacking Enterprise Networks)。上次存取時間 2019年7月24日：<https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/megacortex-ransomware-spotted-attacking-enterprise-networks/>。
- 34 趨勢科技。(2017年5月12日)。TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)。「大規模 WannaCry/Wcry 勒索病毒攻擊數個不同國家」(Massive WannaCry/Wcry Ransomware Attack Hits Various Countries)。上次存取時間 2019年7月24日：<https://blog.trendmicro.com/trendlabs-security-intelligence/massive-wannacrywcrw-ransomware-attack-hits-various-countries/>。
- 35 Microsoft。(2019年8月3日)。Windows Help。「Windows 7 支援將於 2020 年 1 月 14 日終止」(Windows 7 support will end on January 14, 2020)。上次存取時間 2019年8月1日：<https://support.microsoft.com/en-us/help/4057281/windows-7-support-will-end-on-january-14-2020>。
- 36 Lawrence Abrams。(2019年6月24日)。BleepingComputer。「Sodinokibi 勒索病毒現在開始經由漏洞攻擊套件和惡意廣告散布」(Sodinokibi Ransomware Now Pushed by Exploit Kits and Malvertising)。上次存取時間 2019年7月24日：<https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-now-pushed-by-exploit-kits-and-malvertising/>。
- 37 Brian Krebs。(2019年7月15日)。Krebs on Security。「REvil 是不是新的 GandCrab 勒索病毒？」(Is 'REvil' the New GandCrab Ransomware?)。上次存取時間 2019年7月24日：<https://krebsonsecurity.com/2019/07/is-revil-the-new-gandcrab-ransomware/>。
- 38 Trend Micro Research。(2018年)。趨勢科技。「映對未來：對抗無所不在的持續性威脅」(Mapping the Future: Dealing With Pervasive and Persistent Threats)。上次存取時間 2019年7月24日：<https://documents.trendmicro.com/assets/rpt/rpt-mapping-the-future.pdf>。
- 39 趨勢科技。(2019年7月29日)。趨勢科技資訊安全新聞。「檯面下的風險：認識無檔案式威脅」(Risks Under the Radar: Understanding Fileless Threats)。上次存取時間 2019年8月2日：<https://www.trendmicro.com/vinfo/us/security/news/security-technology/risks-under-the-radar-understanding-fileless-threats/>。

- 40 Hiroyuki Kakara 與 Kazuki Fujisawa。(2019 年 4 月 17 日)。TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)。「潛在的針對性攻擊使用 AutoHotkey 和 Excel 檔案內嵌惡意腳本來躲避偵測」(Potential Targeted Attack Uses AutoHotkey and Malicious Script Embedded in Excel File to Avoid Detection)。上次存取時間 2019 年 7 月 24 日：<https://blog.trendmicro.com/trendlabs-security-intelligence/potential-targeted-attack-uses-autohotkey-and-malicious-script-embedded-in-excel-file-to-avoid-detection/>。
- 41 Augusto Remillano II 與 Arvin Macaraeg。(2019 年 4 月 12 日)。TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)。「挖礦惡意程式擴散至中國之外，使用 EternalBlue 與 Powershell 等多種散布方法」(Miner Malware Spreads Beyond China, Uses Multiple Propagation Methods Including EternalBlue, Powershell Abuse)。上次存取時間 2019 年 8 月 2 日：<https://blog.trendmicro.com/trendlabs-security-intelligence/miner-malware-spreads-beyond-china-uses-multiple-propagation-methods-including-eternalblue-powershell-abuse/>。
- 42 Erika Mendoza、Jay Yaneza、Gilbert Sison、Anjali Patil、Julie Cabuhat 與 Joelson Soares。(2019 年 3 月 29 日)。TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)。「趨勢科技 MDR (託管式偵測及回應服務) 發現 Emotet 散播的 Nozelesn 勒索病毒載入程式」(Emotet-Distributed Ransomware Loader for Nozelesn Found via Managed Detection and Response)。上次存取時間 2019 年 7 月 24 日：<https://blog.trendmicro.com/trendlabs-security-intelligence/emotet-distributed-ransomware-loader-for-nozelesn-found-via-managed-detection-and-response/>。
- 43 Henry Alarcon, Jr. 與 Raphael Centeno。(2019 年 3 月 4 日)。TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)。「無檔案式銀行木馬程式攻擊巴西銀行，可能下載殭屍網路病毒與資訊竊取程式」(Fileless Banking Trojan Targeting Brazilian Banks Downloads Possible Botnet Capability, Info Stealers)。上次存取時間 2019 年 7 月 24 日：<https://blog.trendmicro.com/trendlabs-security-intelligence/fileless-banking-trojan-targeting-brazilian-banks-downloads-possible-botnet-capability-info-stealers/>。
- 44 Augusto Remillano II 與 Kiyoshi Obuchi。(2019 年 3 月 12 日)。TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)。「Powload 的演進：從無檔案式技巧到圖像隱碼術」(From Fileless Techniques to Using Steganography: Examining Powload's Evolution)。上次存取時間 2019 年 7 月 24 日：<https://blog.trendmicro.com/trendlabs-security-intelligence/from-fileless-techniques-to-using-steganography-examining-powloads-evolution/>。
- 45 Miguel Ang。(2019 年 5 月 20 日)。TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)。「Trickbot 觀察：透過垃圾郵件中的重導網址散布」(Trickbot Watch: Arrival via Redirection URL in Spam)。上次存取時間 2019 年 7 月 24 日：<https://blog.trendmicro.com/trendlabs-security-intelligence/trickbot-watch-arrival-via-redirection-url-in-spam/>。
- 46 Hiroyuki Kakara 與 Kazuki Fujisawa。(2019 年 4 月 17 日)。TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)。「潛在的針對性攻擊使用 AutoHotkey 和 Excel 檔案內嵌惡意腳本來躲避偵測」(Potential Targeted Attack Uses AutoHotkey and Malicious Script Embedded in Excel File to Avoid Detection)。上次存取時間 2019 年 7 月 24 日：<https://blog.trendmicro.com/trendlabs-security-intelligence/potential-targeted-attack-uses-autohotkey-and-malicious-script-embedded-in-excel-file-to-avoid-detection/>。
- 47 Janus Agcaoli。(2019 年 6 月 5 日)。TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)。「門羅幣挖礦惡意程式 PCASTLE 再度瞄準中國，這回採用多重層次的無檔案式感染技巧」(Monero-Mining Malware PCASTLE Zeroes Back In on China, Now Uses Multilayered Fileless Arrival Techniques)。上次存取時間 2019 年 7 月 24 日：<https://blog.trendmicro.com/trendlabs-security-intelligence/monero-mining-malware-pcastle-zeroes-back-in-on-china-now-uses-multilayered-fileless-arrival-techniques/>。
- 48 Johnlery Triunfante。(2019 年 6 月 3 日)。TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)。「BlackSquid 利用八種知名漏洞攻擊手法潛入伺服器與磁碟當中並植入 XMRig 挖礦程式」(BlackSquid Slithers Into Servers and Drives With 8 Notorious Exploits to Drop XMRig Miner)。上次存取時間 2019 年 7 月 24 日：<https://blog.trendmicro.com/trendlabs-security-intelligence/blacksquid-slithers-into-servers-and-drives-with-8-notorious-exploits-to-drop-xmrig-miner/>。
- 49 Augusto Remillano II 與 Jakub Urbanec。(2019 年 5 月 23 日)。TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)。「新的 Mirai 變種使用多種漏洞攻擊手法瞄準路由器和裝置」(New Mirai Variant Uses Multiple Exploits to Target Routers and Other Devices)。上次存取時間 2019 年 7 月 24 日：<https://blog.trendmicro.com/trendlabs-security-intelligence/new-mirai-variant-uses-multiple-exploits-to-target-routers-and-other-devices/>。
- 50 趨勢科技。(2019 年 3 月 25 日)。趨勢科技資訊安全新聞。「將近 50% 的企業面臨網路資安人才短缺的問題」(Cybersecurity Skills Shortage a Problem for Nearly 50 Percent of Organizations)。上次存取時間 2019 年 7 月 24 日：<https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/cybersecurity-skills-shortage-a-problem-for-nearly-50-percent-of-organizations/>。
- 51 趨勢科技。(2019 年 3 月 5 日)。趨勢科技資訊安全新聞。「2018 年行動威脅情勢」(2018 Mobile Threat Landscape)。上次存取時間 2019 年 8 月 2 日：<https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/2018-mobile-threat-landscape>。
- 52 Kevin Sun。(2019 年 1 月 17 日)。TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)。「Google Play 出現會在手機上植入 Anubis 銀行惡意程式的應用程式並利用動作感應資料來躲避偵測」(Google Play Apps Drop Anubis Banking Malware, Use Motion-based Evasion Tactics)。上次存取時間 2019 年 7 月 24 日：<https://blog.trendmicro.com/trendlabs-security-intelligence/google-play-apps-drop-anubis-banking-malware-use-motion-based-evasion-tactics/>。
- 53 Tony Bao。(2019 年 7 月 8 日)。TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)。「Android 惡意程式 Anubis 強勢回歸，已出現超過 17,000 個樣本」(Anubis Android Malware Returns with Over 17,000 Samples)。上次存取時間 2019 年 7 月 24 日：<https://blog.trendmicro.com/trendlabs-security-intelligence/anubis-android-malware-returns-with-over-17000-samples/>。
- 54 行動裝置威脅應變團隊。(2017 年 1 月 18 日)。TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)。「2016 年回顧：行動威脅多樣性、規模和範圍更加擴大」(In Review: 2016's Mobile Threat Landscape Brings Diversity, Scale, and Scope)。上次存取時間 2019 年 7 月 24 日：<https://blog.trendmicro.com/trendlabs-security-intelligence/2016-mobile-threat-landscape/>。
- 55 Joseph C. Chen。(2019 年 6 月 27 日)。TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)。「ShadowGate 重返世界舞台，採用進化版 Greenflash Sundown 漏洞攻擊套件」(ShadowGate Returns to Worldwide Operations With Evolved Greenflash Sundown Exploit Kit)。上次存取時間 2019 年 7 月 24 日：<https://blog.trendmicro.com/trendlabs-security-intelligence/shadowgate-returns-to-worldwide-operations-with-evolved-greenflash-sundown-exploit-kit/>。
- 56 趨勢科技。(2016 年)。趨勢科技。「是時候了：資安情勢演變已迫使威脅因應策略面臨調整」(Setting the Stage: Landscape Shifts Dictate Future Threat Response Strategies)。上次存取時間 2019 年 8 月 1 日：<https://documents.trendmicro.com/assets/rpt/rpt-setting-the-stage.pdf>。
- 57 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 2019 年 7 月 24 日：<https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/fake-news-cyber-propaganda-the-abuse-of-social-media/>。
- 58 Cedric Pernet、Daniel Lunghi、Jaromir Horejsi 與 Joseph C. Chen。(2019 年 3 月 7 日)。TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)。「運用 GitHub 並透過 Slack 來通訊的最新 SLUB 後門程式」(New SLUB Backdoor Uses GitHub, Communicates via Slack)。上次存取時間 2019 年 7 月 24 日：<https://blog.trendmicro.com/trendlabs-security-intelligence/new-slub-backdoor-uses-github-communicates-via-slack/>。
- 59 Jindrich Karasek 與 Cedric Pernet。(2019 年 2 月 28 日)。TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)。「駭客集團如何盜取 Instagram 名人帳號」(How a Hacking Group is Stealing Popular Instagram Profiles)。上次存取時間 2019 年 7 月 24 日：<https://blog.trendmicro.com/trendlabs-security-intelligence/how-a-hacking-group-is-stealing-popular-instagram-profiles/>。

- 60 Hara Hiroaki、Lilang Wu 與 Lorin Wu。(2019年4月2日)。TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)。「新版 XLoader 偽裝成 Android 應用程式：某 iOS 設定檔內含指向 FakeSpy 的新連結」(New Version of XLoader That Disguises as Android Apps and an iOS Profile Holds New Links to FakeSpy)。上次存取時間 2019 年 7 月 24 日：<https://blog.trendmicro.com/trendlabs-security-intelligence/new-version-of-xloader-that-disguises-as-android-apps-and-an-ios-profile-holds-new-links-to-fakespy/>。
- 61 趨勢科技。(2019年2月28日)。TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)。「改變策略：在技術支援詐騙當中應用社群媒體與 SEO 搜尋引擎毒化技巧」(Shifting Strategies: Using Social Media, SEO in Tech Support Scams)。上次存取時間 2019 年 7 月 24 日：<https://blog.trendmicro.com/trendlabs-security-intelligence/shifting-strategies-using-social-media-seo-in-tech-support-scams/>。
- 62 Vladimir Kropotov 與 Fyodor Yarochkin。(2019年7月30日)。趨勢科技資訊安全新聞。「在 Twitter 上追蹤威脅：如何透過社群媒體來蒐集有用的威脅情報」(Hunting Threats on Twitter: How Social Media Can Be Used to Gather Actionable Threat Intelligence)。上次存取時間 2019 年 8 月 2 日：<https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/hunting-threats-on-twitter/>。
- 63 Ecular Xu 與 Grey Guo。(2019年6月18日)。TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)。「手機網路間諜行動 Bouncing Golf 肆虐中東地區」(Mobile Cyberespionage Campaign 'Bouncing Golf' Affects Middle East)。上次存取時間 2019 年 7 月 24 日：<https://blog.trendmicro.com/trendlabs-security-intelligence/mobile-cyberespionage-campaign-bouncing-golf-affects-middle-east/>。
- 64 Hara Hiroaki 與 Loseway Lu。(2019年6月12日)。TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)。「變換手法：剖析 TA505 駭客團體如何在最新的攻擊行動當中運用 HTML、RAT 及其他技巧」(Shifting Tactics: Breaking Down TA505 Group's Use of HTML, RATs and Other Techniques in Latest Campaigns)。上次存取時間 2019 年 7 月 24 日：<https://blog.trendmicro.com/trendlabs-security-intelligence/shifting-tactics-breaking-down-ta505-groups-use-of-html-rats-and-other-techniques-in-latest-campaigns/>。
- 65 Hara Hiroaki 與 Loseway Lu。(2019年7月4日)。TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)。「TA505 近期的垃圾郵件攻擊開始採用新的惡意程式工具 Gelup 及 FlowerPippi」(Latest Spam Campaigns from TA505 Now Using New Malware Tools Gelup and FlowerPippi)。上次存取時間 2019 年 7 月 24 日：<https://blog.trendmicro.com/trendlabs-security-intelligence/latest-spam-campaigns-from-ta505-now-using-new-malware-tools-gelup-and-flowerpippi/>。
- 66 Jaromir Horejsi。(2018年3月12日)。TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)。「中東與中亞地區出現疑似與 MuddyWater 有所關聯的攻擊行動」(Campaign Possibly Connected to "MuddyWater" Surfaces in the Middle East and Central Asia)。上次存取時間 2019 年 7 月 24 日：<https://blog.trendmicro.com/trendlabs-security-intelligence/campaign-possibly-connected-muddywater-surfaces-middle-east-central-asia/>。
- 67 Jaromir Horejsi 與 Daniel Lunghi。(2018年11月30日)。TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)。「土耳其出現以 PowerShell 為基礎的後門程式，酷似 MuddyWater 工具」(New PowerShell-based Backdoor Found in Turkey, Strikingly Similar to MuddyWater Tools)。上次存取時間 2019 年 7 月 24 日：<https://blog.trendmicro.com/trendlabs-security-intelligence/new-powershell-based-backdoor-found-in-turkey-strikingly-similar-to-muddywater-tools/>。
- 68 Daniel Lunghi 與 Jaromir Horejsi。(2019年6月10日)。TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)。「MuddyWater 再度現身，採用多重階段的後門程式 POWERSTATS V3 與新的漏洞攻擊後端工具」(MuddyWater Resurfaces, Uses Multi-Stage Backdoor POWERSTATS V3 and New Post-Exploitation Tools)。上次存取時間 2019 年 7 月 24 日：<https://blog.trendmicro.com/trendlabs-security-intelligence/muddywater-resurfaces-uses-multi-stage-backdoor-powerstats-v3-and-new-post-exploitation-tools/>。
- 69 CoinDesk。(日期不詳)。CoinDesk。「比特幣價格指數：比特幣即時價格表」(Bitcoin Price Index — Real-time Bitcoin Price Charts)。上次存取時間 2019 年 7 月 24 日：<https://www.coindesk.com/price/bitcoin/>。
- 70 CoinDesk。(日期不詳)。CoinDesk。「門羅幣價格指數：門羅幣 (XMR) 即時價格表」(Monero Price Index — Real-time Monero (XMR) Price Charts)。上次存取時間 2019 年 7 月 24 日：<https://www.coindesk.com/price/monero/>。
- 71 Sergio Pastrana 與 Guillermo Suarez-Tangil。(2019年1月3日)。ArXiv。「虛擬加密貨幣挖礦惡意程式生態系初探：十年淘金夢」(A First Look at the Crypto-Mining Malware Ecosystem: A Decade of Unrestricted Wealth)。上次存取時間 2019 年 8 月 2 日：<https://arxiv.org/pdf/1901.00846.pdf>。
- 72 Tom Wilson。(2019年5月15日)。Reuters。「觀念解說：近乎完全匿名的『私密貨幣』門羅幣」(Explainer: 'Privacy coin' Monero offers near total anonymity)。上次存取時間 2019 年 8 月 2 日：<https://www.reuters.com/article/us-crypto-currencies-altcoins-explainer/explainer-privacy-coin-monero-offers-near-total-anonymity-idUSKCN1SL0F0>。
- 73 Danny Palmer。(2018年2月20日)。ZDNet。「網路駭客利用虛擬加密貨幣挖礦大發利市卻刻意避開比特幣的原因」(Cyber attackers are cashing in on cryptocurrency mining - but here's why they're avoiding bitcoin)。上次存取時間 2019 年 8 月 2 日：<https://www.zdnet.com/article/cyber-attackers-are-cashing-in-on-cryptocurrency-mining-but-heres-why-theyre-avoiding-bitcoin/>。
- 74 Augusto Remillano II 與 Jakub Urbanec。(2019年2月8日)。TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)。「抄襲 KORKERDS 腳本且會清除系統上所有其他惡意程式的 Linux 挖礦程式」(Linux Coin Miner Copied Scripts From KORKERDS, Removes All Other Malware and Miners)。上次存取時間 2019 年 7 月 24 日：<https://blog.trendmicro.com/trendlabs-security-intelligence/linux-coin-miner-copied-scripts-from-korkerds-removes-all-other-malware-and-miners/>。
- 75 Don Ovid Ladores、Michael Jhon Ofiaza 與 Gilbert Sison。(2019年2月20日)。TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)。「門羅幣挖礦惡意程式使用 RADMIN 和 MIMIKATZ 來感染並經由漏洞散布」(Monero Miner-Malware Uses RADMIN, MIMIKATZ to Infect, Propagate via Vulnerability)。上次存取時間 2019 年 7 月 24 日：<https://blog.trendmicro.com/trendlabs-security-intelligence/monero-miner-malware-uses-radmin-mimikatz-to-infect-propagate-via-vulnerability/>。
- 76 Augusto Remillano II 與 Arvin Macaraeg。(2019年4月12日)。TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)。「挖礦惡意程式擴散至中國之外，使用 EternalBlue 與 Powershell 等多種散布方法」(Miner Malware Spreads Beyond China, Uses Multiple Propagation Methods Including EternalBlue, Powershell Abuse)。上次存取時間 2019 年 7 月 24 日：<https://blog.trendmicro.com/trendlabs-security-intelligence/miner-malware-spreads-beyond-china-uses-multiple-propagation-methods-including-eternalblue-powershell-abuse/>。
- 77 Janus Agcaoli。(2019年6月5日)。TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)。「門羅幣挖礦惡意程式 PCASTLE 再度瞄準中國，這回採用多重層次的無檔案式感染技巧」(Monero-Mining Malware PCASTLE Zeroes Back In on China, Now Uses Multilayered Fileless Arrival Techniques)。上次存取時間 2019 年 7 月 24 日：<https://blog.trendmicro.com/trendlabs-security-intelligence/monero-mining-malware-pcastle-zeroes-back-in-on-china-now-uses-multilayered-fileless-arrival-techniques/>。
- 78 Augusto II Remillano 與 Robert Malagad。(2019年5月7日)。TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)。「CVE-2019-3396 Redux：Confluence 漏洞遭駭客用於散布虛擬加密貨幣挖礦程式及 Rootkit」(CVE-2019-3396 Redux: Confluence Vulnerability Exploited to Deliver Cryptocurrency Miner With Rootkit)。上次存取時間 2019 年 7 月 24 日：<https://blog.trendmicro.com/trendlabs-security-intelligence/cve-2019-3396-redux-confluence-vulnerability-exploited-to-deliver-cryptocurrency-miner-with-rootkit/>。
- 79 Jindrich Karasek。(2019年6月20日)。TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)。「虛擬加密貨幣殭屍網路經由 ADB 感染並透過 SSH 散布」(Cryptocurrency-Mining Botnet Malware Arrives Through ADB and Spreads Through SSH)。上次存取時間 2019 年 7 月 24 日：<https://blog.trendmicro.com/trendlabs-security-intelligence/cryptocurrency-mining-botnet-arrives-through-adb-and-spreads-through-ssh/>。

- 80 Augusto Remillano II。(2019年6月13日)。TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)。「Outlaw 駭客團體殭屍網路散布挖礦程式以及使用 Perl 撰寫的後門程式」(Outlaw Hacking Group's Botnet Observed Spreading Miner, Perl- Based Backdoor)。上次存取時間 2019 年 7 月 24 日：<https://blog.trendmicro.com/trendlabs-security-intelligence/outlaw-hacking-groups-botnet-observed-spreading-miner-perl-based-backdoor/>。
- 81 Augusto Remillano II 與 Mark Vicente。(2019年6月28日)。TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)。「虛擬加密貨幣挖礦惡意程式行動採用以 Go 撰寫的散布程式」(Golang-based Spreader Used in a Cryptocurrency-Mining Malware Campaign)。上次存取時間 2019 年 7 月 24 日：<https://blog.trendmicro.com/trendlabs-security-intelligence/golang-based-spreader-used-in-a-cryptocurrency-mining-malware-campaign/>。
- 82 Trend Micro Research。(2018年)。趨勢科技。「映對未來：對抗無所不在的持續性威脅」(Mapping the Future: Dealing With Pervasive and Persistent Threats)。上次存取時間 2019 年 7 月 24 日：<https://documents.trendmicro.com/assets/rpt/rpt-mapping-the-future.pdf>。
- 83 Chris Doman 與 Tom Hegel。(2019年3月14日)。AT&T Cybersecurity。「烏雲密布：雲端虛擬加密貨幣挖礦攻擊」(Making it Rain - Cryptocurrency Mining Attacks in the Cloud)。上次存取時間 2019 年 7 月 24 日：<https://www.alienvault.com/blogs/labs-research/making-it-rain-cryptocurrency-mining-attacks-in-the-cloud/>。
- 84 Alfredo Oliveira。(2019年3月1日)。TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)。「暴露在外面的 Docker Control API 與社群分享的映象遭駭客用來散布虛擬加密貨幣挖礦惡意程式」(Exposed Docker Control API and Community Image Abused to Deliver Cryptocurrency-Mining Malware)。上次存取時間 2019 年 7 月 24 日：<https://blog.trendmicro.com/trendlabs-security-intelligence/exposed-docker-control-api-and-community-image-abused-to-deliver-malware/>。
- 85 Alfredo Oliveira。(2019年5月30日)。TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)。「已遭感染的虛擬加密貨幣挖礦容器透過暴露在外面的 API 攻擊 Docker 主機並利用 Shodan 來搜尋更多受害者」(Infected Cryptocurrency-Mining Containers Target Docker Hosts With Exposed APIs, Use Shodan to Find Additional Victims)。上次存取時間 2019 年 7 月 24 日：<https://blog.trendmicro.com/trendlabs-security-intelligence/infected-cryptocurrency-mining-containers-target-docker-hosts-with-exposed-apis-use-shodan-to-find-additional-victims/>。
- 86 趨勢科技。(2019年5月10日)。趨勢科技資訊安全新聞。「Jenkins 漏洞遭駭客用來植入 Kerberos 惡意程式並啟動門羅幣挖礦程式」(Jenkins Vulnerability Exploited to Drop Kerberos Malware and Launch Monero Miner)。上次存取時間 2019 年 7 月 24 日：<https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/jenkins-vulnerability-exploited-to-drop-kerberos-malware-and-launch-monero-miner/>。
- 87 Check Point Research。(2018年2月15日)。Check Point Research。「Jenkins 挖礦程式：有史以來最大的挖礦行動之一」(Jenkins Miner: One of the Biggest Mining Operations Ever Discovered)。上次存取時間 2019 年 7 月 24 日：<https://research.checkpoint.com/jenkins-miner-one-biggest-mining-operations-ever-discovered/>。
- 88 Jon Porter。(2019年2月28日)。The Verge。「熱門虛擬加密貨幣挖礦服務 Coinhive 下周將關門大吉」(Popular 'cryptojacking' service Coinhive will shut down next week)。上次存取時間 2019 年 7 月 24 日：<https://www.theverge.com/2019/2/28/18244636/coinhive-cryptojacking-cryptocurrency-mining-shut-down-monero-date/>。
- 89 Radiflow。(2018年2月8日)。Radiflow。「Radiflow 揭露史上第一起針對 SCADA 網路的虛擬加密貨幣惡意程式攻擊」(Radiflow Reveals First Documented Cryptocurrency Malware Attack on a SCADA Network)。上次存取時間 2019 年 7 月 24 日：<https://radiflow.com/news/radiflow-reveals-first-documented-cryptocurrency-malware-attack-on-a-scada-network/>。
- 90 Dave Shackelford。(2019年4月30日)。SANS Institute。「SANS 2019 年雲端資安問卷調查」(SANS 2019 Cloud Security Survey)。上次存取時間 2019 年 7 月 24 日：<https://www.sans.org/reading-room/whitepapers/analyst/2019-cloud-security-survey-38940/>。
- 91 趨勢科技。(2019年4月2日)。趨勢科技資訊安全新聞。「超過 13,000 個組態設定不當的 iSCSI 儲存叢集遭駭客從公開的網際網路存取」(More than 13,000 Misconfigured iSCSI Storage Clusters Accessible via the Public Internet)。上次存取時間 2019 年 7 月 24 日：<https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/more-than-13-000-misconfigured-iscsi-storage-clusters-accessible-via-the-public-internet/>。
- 92 趨勢科技。(2019年5月14日)。趨勢科技資訊安全新聞。「缺乏安全保護的伺服器造成巴拿馬將近 90% 的人民個人身分識別資訊外流」(Unsecured Server Leaks PII of Almost 90% of Panama Residents)。上次存取時間 2019 年 7 月 24 日：<https://www.trendmicro.com/vinfo/us/security/news/online-privacy/unsecured-server-leaks-pii-of-almost-90-of-panama-residents/>。
- 93 趨勢科技。(日期不詳)。趨勢科技資訊安全新聞。「開發營運」(DevOps)。上次存取時間 2019 年 7 月 24 日：<https://www.trendmicro.com/vinfo/us/security/definition/devops/>。
- 94 趨勢科技。(日期不詳)。趨勢科技資訊安全新聞。「歐盟通用資料保護法 (GDPR)」(EU General Data Protection Regulation (GDPR))。上次存取時間 2019 年 7 月 24 日：<https://www.trendmicro.com/vinfo/us/security/definition/eu-general-data-protection-regulation-gdpr/>。
- 95 Asaf Cidon。(2019年5月2日)。Barracuda Journey Notes。「威脅聚光燈：帳號被盜」(Threat Spotlight: Account Takeover)。上次存取時間 2019 年 7 月 24 日：<https://blog.barracuda.com/2019/05/02/threat-spotlight-account-takeover/>。
- 96 Abhishek Agrawal、David Fantham、Debraj Ghosh、Diana Kelley、Elia Florio、Eric Avena、Eric Douglas 等人。(2019年)。Microsoft Corporation。「Microsoft 資安情報報告，第 24 期，2018 年 1 月至 12 月」(Microsoft Security Intelligence Report, Volume 24, January - December 2018)。上次存取時間 2019 年 7 月 24 日：<https://clouddamcdnprod.azureedge.net/gdc/gdc09FrGq/original>。
- 97 Lorin Wu。(2019年1月30日)。TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)。「Google Play 上多款相機修圖軟體會發送色情內容，並將使用者重導至網路釣魚網站以蒐集其照片」(Various Google Play 'Beauty Camera' Apps Send Users Pornographic Content, Redirect Them to Phishing Websites and Collect Their Pictures)。上次存取時間 2019 年 7 月 24 日：<https://blog.trendmicro.com/trendlabs-security-intelligence/various-google-play-beauty-camera-apps-sends-users-pornographic-content-redirects-them-to-phishing-websites-and-collects-their-pictures/>。
- 98 Joseph C. Chen。(2019年3月28日)。TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)。「電腦及手機網路釣魚行動瞄準南韓網站，利用水坑式攻擊竊取登入憑證」(Desktop, Mobile Phishing Campaign Targets South Korean Websites, Steals Credentials Via Watering Hole)。上次存取時間 2019 年 7 月 24 日：<https://blog.trendmicro.com/trendlabs-security-intelligence/desktop-mobile-phishing-campaign-targets-south-korean-websites-steals-credentials-via-watering-hole/>。
- 99 Samuel P. Wang。(2019年4月4日)。TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)。「網路釣魚攻擊使用瀏覽器擴充元件 SingleFile 來將惡意登入網頁加密編碼」(Phishing Attack Uses Browser Extension Tool SingleFile to Obfuscate Malicious Log-in Pages)。上次存取時間 2019 年 7 月 24 日：<https://blog.trendmicro.com/trendlabs-security-intelligence/phishing-attack-uses-browser-extension-tool-singlefile-to-obfuscate-malicious-log-in-pages/>。
- 100 趨勢科技。(2019年3月29日)。趨勢科技資訊安全新聞。「美國俄勒岡州民眾服務部 (DHS) 遭網路釣魚攻擊導致 35 萬名民眾的醫療資訊外洩」(Health Information of 350,000 Oregon DHS Clients Exposed After Phishing Attack)。上次存取時間 2019 年 7 月 24 日：<https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/health-information-of-350-000-oregon-dhs-clients-exposed-after-phishing-attack/>。
- 101 Catalin Cimpanu。(2019年4月11日)。ZDNet。「Emotet 攔截電子郵件對話串並插入惡意程式連結」(Emotet hijacks email conversation threads to insert links to malware)。上次存取時間 2019 年 7 月 24 日：<https://www.zdnet.com/article/emotet-hijacks-email-conversation-threads-to-insert-links-to-malware/>。

- 102 Erika Mendoza、Anjali Patil 與 Jay Yaneza。(2018 年 10 月 9 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「網路釣魚行動利用已遭駭入的電子郵件帳號，回覆現有的對話串來散發 URSNIF 惡意程式」(Phishing Campaign uses Hijacked Emails to Deliver URSNIF by Replying to Ongoing Threads)。上次存取時間 2019 年 7 月 24 日：<https://blog.trendmicro.com/trendlabs-security-intelligence/phishing-campaign-uses-hijacked-emails-to-deliver-ursnif-by-replying-to-ongoing-threads/>。
- 103 Miguel Ang 和 Donald Castillo。(2018 年 10 月 29 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「舊瓶裝新酒：垃圾郵件惡意程式附件暗藏新的檔案類型」(Same Old yet Brand-new: New File Types Emerge in Malware Spam Attachments)。上次存取時間 2019 年 7 月 24 日：<https://blog.trendmicro.com/trendlabs-security-intelligence/same-old-yet-brand-new-new-file-types-emerge-in-malware-spam-attachments/>。
- 104 Proofpoint Information Protection Research Team。(2019 年 3 月 14 日)。*Proofpoint*。「歹徒藉由竊取登入憑證、網路釣魚及老舊的電子郵件通訊協定來避開多重驗證 (MFA) 並入侵全球各地的雲端帳號」(Threat actors leverage credential dumps, phishing, and legacy email protocols to bypass MFA and breach cloud accounts worldwide)。上次存取時間 2019 年 7 月 24 日：<https://www.proofpoint.com/us/threat-insight/post/threat-actors-leverage-credential-dumps-phishing-and-legacy-email-protocols/>。
- 105 APWG。(2019 年 5 月 15 日)。*APWG*。「2019 年第一季網路釣魚活動趨勢報告」(Phishing Activity Trends Report, 1st Quarter 2019)。上次存取時間 2019 年 7 月 24 日：https://docs.apwg.org/reports/apwg_trends_report_q1_2019.pdf。
- 106 趨勢科技。(2019 年 4 月 25 日)。*趨勢科技資訊安全新聞*。「IC3：2018 年變臉詐騙造成企業損失 12 億美元」(IC3: BEC Cost Organizations US\$1.2 Billion in 2018)。上次存取時間 2019 年 7 月 24 日：<https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ic3-bec-cost-organizations-us-1-2-billion-in-2018/>。
- 107 Katia Moskvitch。(2019 年 3 月 20 日)。*Wired UK*。「網路犯罪集團瞄準企業人事部門以竊取您的薪水」(Cyber criminals are targeting HR departments to steal your salary)。上次存取時間 2019 年 8 月 1 日：<https://www.wired.co.uk/article/hr-email-scam-phishing-impersonating-employees>。
- 108 Sachin Dave。(2019 年 1 月 10 日)。*The Economic Times*。「偷天換日：13 億印度盧比的詐騙，中國駭客是如何得逞」(How Chinese hackers pulled off the Italian con job, a Rs 130-crore heist)。上次存取時間 2019 年 8 月 1 日：<https://economictimes.indiatimes.com/tech/internet/how-chinese-hackers-pulled-off-the-italian-con-job-a-rs-130-crore-heist/articleshow/67464588.cms>。
- 109 Nick Wooten。(2019 年 1 月 8 日)。*Shreveport Times*。「更新訊息：Caddo 各學校被騙的 100 萬美元目前已部分追回」(Update: Some of \$1M scammed from Caddo schools has been found)。上次存取時間 2019 年 8 月 1 日：<https://www.shreveporttimes.com/story/news/2019/01/08/scammer-get-nearly-1-million-meant-caddo-charter-school/2514083002/>。
- 110 趨勢科技。(2019 年 4 月 10 日)。*趨勢科技資訊安全新聞*。「London Blue 集團的變臉詐騙技巧不斷演進」(London Blue Group Using Evolving BEC Techniques in Attacks)。上次存取時間 2019 年 7 月 24 日：<https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/london-blue-group-using-evolving-bec-techniques-in-their-attacks/>。
- 111 趨勢科技。(2019 年 4 月 16 日)。*趨勢科技資訊安全新聞*。「新的變臉詐騙手法利用自動轉帳竊取員工薪資」(New Business Email Compromise Scheme Reroutes Paycheck by Direct Deposit)。上次存取時間 2019 年 7 月 24 日：<https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/new-business-email-compromise-scheme-reroutes-paycheck-by-direct-deposit/>。
- 112 Trend Micro Research。(2018 年)。*趨勢科技*。「映對未來：對抗無所不在的持續性威脅」(Mapping the Future: Dealing With Pervasive and Persistent Threats)。上次存取時間 2019 年 7 月 24 日：<https://documents.trendmicro.com/assets/rpt/rpt-mapping-the-future.pdf>。
- 113 趨勢科技。(2019 年 5 月 2 日)。*趨勢科技資訊安全新聞*。「變臉詐騙集團從美國俄亥俄州某教會騙取 175 萬美元」(BEC Scammers Steal US\$1.75 Million From an Ohio Church)。上次存取時間 2019 年 7 月 24 日：<https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/bec-scammers-steal-us-1-75-million-from-an-ohio-church/>。
- 114 FBI National Press Office。(2019 年 4 月 22 日)。*FBI*。「美國 FBI 網際網路犯罪申訴中心 (IC3) 公布 2018 年網際網路犯罪報告」(FBI Releases the Internet Crime Complaint Center 2018 Internet Crime Report)。上次存取時間 2019 年 8 月 13 日：<https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-the-internet-crime-complaint-center-2018-internet-crime-report>。
- 115 Federal Bureau of Investigation Internet Crime Complaint Center。(日期不詳)。*Federal Bureau of Investigation Internet Crime Complaint Center (IC3)*。「2018 年網際網路犯罪報告」(2018 Internet Crime Report)。上次存取時間 2019 年 7 月 24 日：https://pdf.ic3.gov/2018_IC3Report.pdf。
- 116 Trend Micro Research。(2018 年)。*趨勢科技*。「映對未來：對抗無所不在的持續性威脅」(Mapping the Future: Dealing With Pervasive and Persistent Threats)。上次存取時間 2019 年 7 月 24 日：<https://documents.trendmicro.com/assets/rpt/rpt-mapping-the-future.pdf>。
- 117 趨勢科技。(2019 年 4 月 24 日)。*趨勢科技資訊安全新聞*。「新的性勒索詐騙要求支付比特幣現金」(New Sextortion Scheme Demands Payment in Bitcoin Cash)。上次存取時間 2019 年 7 月 24 日：<https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/new-sex-tortion-scheme-demands-payment-in-bitcoin-cash/>。
- 118 Vit Sembera。(2018 年 1 月 5 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「危險的一知半解：了解 Meltdown 和 Spectre」(When Speculation Is Risky: Understanding Meltdown and Spectre)。上次存取時間 2019 年 8 月 1 日：<https://blog.trendmicro.com/trendlabs-security-intelligence/speculation-risky-understanding-meltdown-spectre/>。
- 119 Graz University of Technology。(2018 年)。*Graz University of Technology*。「Meltdown 和 Spectre」(Meltdown and Spectre)。上次存取時間 2019 年 8 月 1 日：<https://meltdownattack.com/>。
- 120 趨勢科技。(2019 年 2 月 14 日)。*趨勢科技資訊安全新聞*。「概念驗證攻擊示範惡意程式如何利用 Intel SGX 安全區 (Enclave) 躲避防毒軟體偵測」(Proof of Concept Shows How Malware Can Hide From AV Solutions via Intel's SGX Enclaves)。上次存取時間 2019 年 7 月 24 日：<https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/proof-of-concept-shows-how-malware-can-hide-from-av-solutions-via-intel-s-gsx-enclaves/>。
- 121 趨勢科技。(2019 年 5 月 15 日)。*趨勢科技資訊安全新聞*。「RIDL、Fallout 及 ZombieLoad 旁路攻擊影響數百萬 Intel 處理器」(Side-Channel Attacks RIDL, Fallout, and ZombieLoad Affect Millions of Vulnerable Intel Processors)。上次存取時間 2019 年 8 月 1 日：<https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/side-channel-attacks-ridl-fallout-and-zombieload-affects-millions-of-vulnerable-intel-processors/>。
- 122 趨勢科技。(2019 年 5 月 29 日)。*趨勢科技資訊安全新聞*。「BlueKeep 蠕蟲化漏洞 (CVE-2019-0708) 影響將近百萬台系統」(Nearly 1 Million Systems Affected By 'Wormable' BlueKeep Vulnerability [CVE-2019-0708])。上次存取時間 2019 年 7 月 24 日：<https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/nearly-1-million-systems-affected-by-wormable-bluekeep-vulnerability-cve-2019-0708/>。
- 123 Simon Pope。(2019 年 5 月 14 日)。*Microsoft Security Response Center*。「更新遠端桌面服務漏洞 (CVE-2019-0708) 以防範蠕蟲」(Prevent a worm by updating Remote Desktop Services [CVE-2019-0708])。上次存取時間 2019 年 7 月 24 日：<https://msrc-blog.microsoft.com/2019/05/14/prevent-a-worm-by-updating-remote-desktop-services-cve-2019-0708/>。

- 124 趨勢科技。(2019年5月31日)。趨勢科技資訊安全新聞。「SandboxEscaper 發表針對工作排程器零時差漏洞的攻擊手法」(SandboxEscaper Releases Exploit for Zero-Day Vulnerability in Task Scheduler)。上次存取時間 2019 年 7 月 24 日：<https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/sandboxescaper-releases-exploit-for-zero-day-vulnerability-in-task-scheduler/>。
- 125 趨勢科技。(2019年2月28日)。趨勢科技資訊安全新聞。「CVE-2019-5736：RunC 容器逃逸漏洞讓駭客取得目標主機系統管理權限」(CVE-2019-5736: RunC Container Escape Vulnerability Provides Root Access to the Target Machine)。上次存取時間 2019 年 7 月 24 日：<https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/cve-2019-5736-runc-container-escape-vulnerability-provides-root-access-to-the-target-machine/>。
- 126 趨勢科技。(2019年4月4日)。趨勢科技資訊安全新聞。「先前已修補的 Kubernetes 路徑瀏覽漏洞仍可能造成重大危險」(Previously Patched, Still Potentially Critical: Kubernetes' Path Traversal Vulnerability)。上次存取時間 2019 年 7 月 24 日：<https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/previous-patched-still-potentially-critical-kubernetes-path-traversal-vulnerability/>。
- 127 Ariel Zeligovsky。(2019年3月28日)。Twistlock。「揭露 Kubernetes 複本的目錄瀏覽漏洞 - CVE-2019-1002101」(Disclosing a directory traversal vulnerability in Kubernetes copy - CVE-2019-1002101)。上次存取時間 2019 年 7 月 24 日：<https://www.twistlock.com/labs-blog/disclosing-directory-traversal-vulnerability-kubernetes-copy-cve-2019-1002101/>。
- 128 趨勢科技。(2019年3月12日)。趨勢科技資訊安全新聞。「StackStorm DevOps 軟體漏洞 CVE-2019-9580 允許遠端程式碼執行」(StackStorm DevOps Software Vulnerability CVE-2019-9580 Allows Remote Code Execution)。上次存取時間 2019 年 7 月 24 日：<https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/stackstorm-devops-software-vulnerability-cve-2019-9580-allows-remote-code-execution/>。
- 129 趨勢科技。(日期不詳)。趨勢科技資訊安全新聞。「網路資訊安全規範 (NIS Directive)」(Network and Information Security (NIS) Directive)。上次存取時間 2019 年 8 月 1 日：[https://www.trendmicro.com/vinfo/us/security/definition/network-and-information-security-\(nis\)-directive/](https://www.trendmicro.com/vinfo/us/security/definition/network-and-information-security-(nis)-directive/)。
- 130 Keumars Afifi-Sabet。(2019年4月4日)。IT Pro。「IT 主管正為了營運的順暢而犧牲安全」(IT chiefs are compromising security for smoother business operations)。上次存取時間 2019 年 7 月 24 日：<https://www.itpro.co.uk/security/33384/it-chiefs-are-compromising-security-for-smoother-business-operations>。
- 131 趨勢科技。(2019年6月25日)。趨勢科技資訊安全新聞。「資安基礎觀念：虛擬修補」(Security 101: Virtual Patching)。上次存取時間 2019 年 7 月 24 日：<https://www.trendmicro.com/vinfo/us/security/news/security-technology/security-101-virtual-patching>。
- 132 John Simpson。(2019年5月29日)。TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)。「CVE-2019-0725：攻擊手法分析」(CVE-2019-0725: An Analysis of Its Exploitability)。上次存取時間 2019 年 7 月 24 日：<https://blog.trendmicro.com/trendlabs-security-intelligence/cve-2019-0725-an-analysis-of-its-exploitability/>。
- 133 John Simpson。(2019年5月24日)。TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)。「CVE-2019-11815：小心看待 CVSS 評分」(CVE-2019-11815: A Cautionary Tale About CVSS Scores)。上次存取時間 2019 年 7 月 24 日：<https://blog.trendmicro.com/trendlabs-security-intelligence/cve-2019-11815-a-cautionary-tale-about-cvss-scores/>。
- 134 Gartner。(2018年11月7日)。Gartner。「Gartner 選出 10 大 IoT 策略性技術與趨勢」(Gartner Identifies Top 10 Strategic IoT Technologies and Trends)。上次存取時間 2019 年 7 月 24 日：<https://www.gartner.com/en/newsroom/press-releases/2018-11-07-gartner-identifies-top-10-strategic-iot-technologies-and-trends/>。
- 135 Trend Micro Research。(2018年)。趨勢科技。「映對未來：對抗無所不在的持續性威脅」(Mapping the Future: Dealing With Pervasive and Persistent Threats)。上次存取時間 2019 年 7 月 24 日：<https://documents.trendmicro.com/assets/rpt/rpt-mapping-the-future.pdf>。
- 136 Mark Vicente、Byron Galera 與 Augusto Remillano。(2019年4月3日)。TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)。「Bashlite IoT 惡意程式新增挖礦與後門功能，專門攻擊 WeMo 品牌裝置」(Bashlite IoT Malware Updated with Mining and Backdoor Commands, Targets WeMo Devices)。上次存取時間 2019 年 7 月 24 日：<https://blog.trendmicro.com/trendlabs-security-intelligence/bashlite-iot-malware-updated-with-mining-and-backdoor-commands-targets-wemo-devices/>。
- 137 趨勢科技。(2019年4月4日)。趨勢科技資訊安全新聞。「Mirai 變種使用多種漏洞攻擊手法瞄準各類型路由器」(Mirai Variant Spotted Using Multiple Exploits, Targets Various Routers)。上次存取時間 2019 年 7 月 24 日：<https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/mirai-variant-spotted-using-multiple-exploits-targets-various-routers/>。
- 138 Augusto Remillano II 與 Jakub Urbanec。(2019年5月23日)。TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)。「新的 Mirai 變種使用多種漏洞攻擊手法瞄準路由器和目標裝置」(New Mirai Variant Uses Multiple Exploits to Target Routers and Other Devices)。上次存取時間 2019 年 7 月 24 日：<https://blog.trendmicro.com/trendlabs-security-intelligence/new-mirai-variant-uses-multiple-exploits-to-target-routers-and-other-devices/>。
- 139 Ruchna Nigam。(2018年7月20日)。Unit 42。「Unit 42 發現新的 Mirai 與 Gafgyt IoT/Linux 殭屍網路攻擊行動」(Unit 42 Finds New Mirai and Gafgyt IoT/Linux Botnet Campaigns)。上次存取時間 2019 年 8 月 1 日：<https://unit42.paloaltonetworks.com/unit42-finds-new-mirai-gafgyt-iotlinux-botnet-campaigns/>。
- 140 Augusto Remillano II。(2019年1月25日)。TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)。「Hakai 和 Yowai 殭屍網路攻擊 ThinkPHP 漏洞」(ThinkPHP Vulnerability Abused by Botnets Hakai and Yowai)。上次存取時間 2019 年 7 月 24 日：<https://blog.trendmicro.com/trendlabs-security-intelligence/thinkphp-vulnerability-abused-by-botnets-hakai-and-yowai/>。
- 141 Augusto Remillano II。(2019年4月26日)。TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)。「AESDDoS 殭屍網路惡意程式攻擊 CVE-2019-3396 漏洞，執行遠端程式碼並從事 DDoS 攻擊與虛擬加密貨幣挖礦」(AESDDoS Botnet Malware Exploits CVE-2019-3396 to Perform Remote Code Execution, DDoS Attacks, and Cryptocurrency Mining)。上次存取時間 2019 年 8 月 1 日：<https://blog.trendmicro.com/trendlabs-security-intelligence/aesddos-botnet-malware-exploits-cve-2019-3396-to-perform-remote-code-execution-ddos-attacks-and-cryptocurrency-mining/>。
- 142 趨勢科技。(2019年5月31日)。趨勢科技資訊安全新聞。「HiddenWasp 惡意程式攻擊 Linux 系統並借用 Mirai 和 Winnti 的程式碼」(HiddenWasp Malware Targets Linux Systems, Borrows Code from Mirai, Winnti)。上次存取時間 2019 年 7 月 24 日：<https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/hiddenwasp-malware-targets-linux-systems-borrows-code-from-mirai-winnti/>。
- 143 趨勢科技。(2019年6月27日)。趨勢科技資訊安全新聞。「Silex 惡意程式利用安全性薄弱的密碼破壞 IoT 裝置」(Silex Malware Bricks IoT Devices with Weak Passwords)。上次存取時間 2019 年 8 月 1 日：<https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/silex-malware-bricks-iot-devices-with-weak-passwords/>。
- 144 Trend Micro Research。(2019年3月5日)。趨勢科技資訊安全新聞。「複雜 IoT 環境的網路資安風險：智慧家庭、建築與其他設施面臨的威脅」(Cybersecurity Risks in Complex IoT Environments: Threats to Smart Homes, Buildings and Other Structures)。上次存取時間 2019 年 8 月 1 日：<https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/threats-and-risks-to-complex-iot-environments/>。

- 145 趨勢科技。(2019年5月2日)。趨勢科技資訊安全新聞。「工作場所IoT裝置：個人自備裝置(BYOD)環境的資安風險與威脅」(IoT Devices in the Workplace: Security Risks and Threats to BYOD Environments)。上次存取時間2019年8月1日：<https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/iot-devices-in-the-workplace-security-risks-and-threats-to-byod-environments/>。
- 146 趨勢科技。(日期不詳)。趨勢科技資訊安全新聞。「工業物聯網(IIoT)」(Industrial Internet of Things [IIoT])。上次存取時間2019年8月1日：<https://www.trendmicro.com/vinfo/us/security/definition/industrial-internet-of-things-iiot/>。
- 147 Ryan Flores、Stephen Hilt 與 Akira Urano。(2019年3月6日)。趨勢科技資訊安全新聞。「食品生產業的資安養成：防範IoT風險與威脅於未然」(Cultivating Security in the Food Production Industry: Nipping IoT Risks and Threats in the Bud)。上次存取時間2019年7月24日：<https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/cultivating-security-in-the-food-production-industry/>。
- 148 Trend Micro Research。(2019年4月3日)。趨勢科技資訊安全新聞。「工業4.0時代的資安：解決智慧製造環境的威脅」(Security in the Era of Industry 4.0: Dealing With Threats to Smart Manufacturing Environments)。上次存取時間2019年7月24日：<https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/security-in-the-era-of-industry-4-dealing-with-threats-to-smart-manufacturing-environments>。
- 149 趨勢科技。(2019年4月4日)。趨勢科技資訊安全新聞。「確保5G連線下的企業安全」(Securing Enterprises for 5G Connectivity)。上次存取時間2019年7月24日：<https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/securing-enterprises-for-5g-connectivity>。
- 150 趨勢科技。(2018年4月5日)。趨勢科技資訊安全新聞。「暴露在外的裝置與供應鏈攻擊：遭忽略的醫療網路風險」(Exposed Devices and Supply Chain Attacks: Overlooked Risks in Healthcare Networks)。上次存取時間2019年7月24日：<https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/exposed-medical-devices-and-supply-chain-attacks-in-connected-hospitals>。
- 151 趨勢科技。(2019年6月27日)。趨勢科技資訊安全新聞。「IIoT 攻擊面：威脅與資安解決方案」(The IIoT Attack Surface: Threats and Security Solutions)。上次存取時間2019年7月24日：<https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/-the-iiot-attack-surface-threats-and-security-solutions/>。
- 152 Louis Columbus。(2018年6月6日)。Forbes。「10張圖挑戰您對IoT成長的看法」(10 Charts That Will Challenge Your Perspective Of IoT's Growth)。上次存取時間2019年7月24日：<https://www.forbes.com/sites/louiscolumnbus/2018/06/06/10-charts-that-will-challenge-your-perspective-of-iots-growth/>。
- 153 Ponemon Institute。(2019年3月)。Tenable。「營運技術的網路資安：您必須知道的7點分析」(Cybersecurity in Operational Technology: 7 Insights You Need to Know)。上次存取時間2019年7月24日：https://static.tenable.com/marketing/research-reports/PonemonReport-Cybersecurity_in_Operational_Technology.pdf。
- 154 趨勢科技。(2017年12月22日)。趨勢科技資訊安全新聞。「揮動三叉戟的海神之子：TRITON 惡意程式破壞工業安全系統」(TRITON Wielding its Trident – New Malware tampering with Industrial Safety Systems)。上次存取時間2019年8月1日：<https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/triton-wielding-its-trident-new-malware-tampering-with-industrial-safety-systems/>。
- 155 趨勢科技。(2019年4月11日)。趨勢科技資訊安全新聞。「新的關鍵基礎架構設施遭到TRITON 背後的駭客集團襲擊」(New Critical Infrastructure Facility Hit by Group Behind TRITON)。上次存取時間2019年8月1日：<https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/new-critical-infrastructure-facility-hit-by-group-behind-triton/>。
- 156 趨勢科技。(2019年6月17日)。趨勢科技資訊安全新聞。「Triton 背後的駭客集團 Xenotime 試圖駭入美國電網的工業控制系統」(Xenotime, Hacking Group Behind Triton, Found Probing Industrial Control Systems of Power Grids in the US)。上次存取時間2019年7月24日：<https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/xenotime-hacking-group-behind-triton-found-probing-industrial-control-systems-of-power-grids-in-the-us>。
- 157 趨勢科技。(2019年6月27日)。趨勢科技資訊安全新聞。「IIoT 攻擊面：威脅與資安解決方案」(The IIoT Attack Surface: Threats and Security Solutions)。上次存取時間2019年7月24日：<https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/-the-iiot-attack-surface-threats-and-security-solutions/>。



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.com

