



資安 新常態

趨勢科技 2020 年資安預測



THE FUTURE IS

▶ **C** P.4 **OMPLEX**

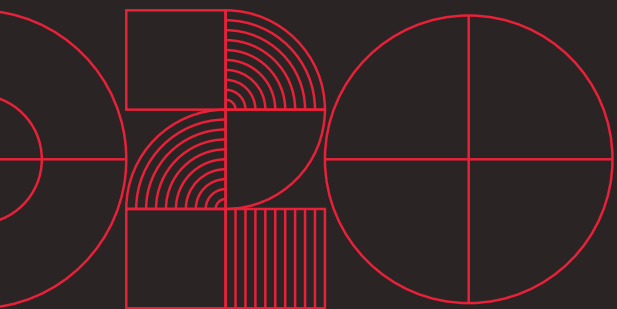
▶ **EX** P.8 **POSED**

▶ **MIS** P.12 **CONFIGURED**

▶ P.15 **DEFENSIBLE**

CYBERSECURITY IN

▶ **2020** P.18



資安 新常態

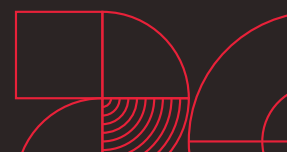
趨勢科技 2020 年資安預測

2020 年象徵著全新十年的開端，而從近期的知名資安事件與發展趨勢來看，威脅情勢同樣也即將出現重大轉變。2020 年及未來，網路資安必須就多重面向來加以檢視 — 從各式各樣的犯罪動機、網路犯罪武器，到不斷進步的科技潮流以及全球威脅情報。唯有如此，防守陣營才能隨時跟上並且預測網路犯罪的主流方向、潮流轉變，以及新興趨勢。

舊的典範，也就是企業網路隔絕在防火牆後方的時代，已經成為過去。企業環境不再只有少數特定企業應用程式。在新的典範之下，企業將有各式各樣的應用程式、服務及平台需要保護。因此，建置多重防護來因應生態系的轉變將是未來的關鍵，如此才能應付廣泛而多樣化的威脅。

儘管一些屢試屢驗的攻擊技巧，如：數位勒索、加密編碼、網路釣魚在今日的攻擊當中依然經常得逞，不過未來必然會有新的威脅崛起。譬如，雲端的日益普及將使得人為錯誤的風險變高，組態設定不當會讓駭客入侵的可能性大增。光是連網設備與基礎架構龐大的數量，就可能帶來各式各樣的漏洞，引來駭客的覬覦。企業未來所面臨的威脅只會更加複雜，同時還會結合傳統威脅與最新科技，例如人工智慧 (AI)，並從事商業詐騙。

我們的 2020 年資安預測彙整了趨勢科技專家對當今及未來新興威脅與技術的看法和分析。文中所描述的情境都是未來可能發生的狀況，而科技的進步與威脅的演變，更是推動情勢發展的主要力量。這份報告旨在提供詳細的資訊來協助企業在 2020 年及未來當面對關鍵資安領域的挑戰與契機時，能做出明智的決策。

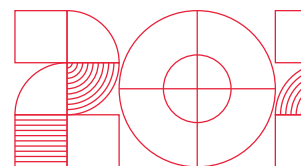


C O M P L E X

THE
FUTURE
IS

D H G C I R
I A N O N I
F R I M T S
F D L P R K
I P Z L I Y
C U Z E C E
U L T X A T

從資安威脅情勢近年來的演變即可證明，犯罪集團仍不斷入侵各類型系統以牟取暴利。而且他們不斷變換途徑、調整攻擊手法，這也提醒了使用者和企業必須隨時掌握最新的情勢。



駭客出招的速度讓那些修補不夠徹底 或急就章的修補更新捉襟見肘。

系統管理員必須特別留意修補更新部署的即時性與修補更新本身的品質。萬一部署的修補更新品質不佳，很可能導致一些關鍵系統的重要功能因而故障，甚至因為修補更新的缺陷而讓系統停擺。但如果延後套用修補更新，又可能讓駭客有充裕的時間來攻擊已知漏洞，使系統暴露在駭客入侵的風險中。

系統修補相關的問題，經常會造成一些空窗期讓駭客得以入侵系統。可預料地，當廠商釋出的修補如果不夠徹底，就有可能發生讓駭客直接越過修補程式碼的情況，例如，駭客可能只要修改幾行程式碼，就能觸發同樣的漏洞。去年，Microsoft Jet Database Engine 的某個零時差漏洞即被發現未完全修補，因此問題僅僅獲得控制，並未徹底排除¹。今年，駭客攻擊了 Cisco 路由器的某些漏洞，事後也被證明正是因為廠商的修補不完全所致²。

駭客會利用使用者通常不太注意開放原始碼程式庫更新訊息的心理，此外也會利用更新部署上的時間差，例如，在修補更新尚未實際到達至某個使用該程式庫的下游產品之前搶先攻擊未修補的漏洞³。

當修補更新未徹底修補漏洞，或者修補更新在部署上出現時間差時，就可利用虛擬修補來提供立即的漏洞防護，防堵已知及未知的漏洞。

網路犯罪集團將改用區塊鏈平台 來進行地下交易。

隨著駭客活動持續蓬勃發展，地下交易生態系也跟著不斷演進。在地下市場上，信賴將扮演更重要角色，例如一些高風險的交易，目前已開始出現背景審核與第三方託管機制⁴。未來，區塊鏈將被視為一種可在買家與賣家之間建立分散式信賴系統的新方法；而智慧合約則可讓網路犯罪集團將虛擬加密貨幣付款正常化，並記錄在區塊鏈上。那些希望維持匿名性並減少所謂「跑路詐騙」(exit scam) 風險的網路犯罪集團，未來將投入可提供去集中化交易的區塊鏈市場⁵。

惡意程式(如勒索病毒)商品化與犯罪服務(Crime-as-a-Service)商業模式，將使得網路犯罪攻擊變得輕鬆又有利可圖。

開放銀行與 ATM 惡意程式將使銀行系統成為攻擊目標。

2020 年，專門攻擊網路銀行與支付系統的行動惡意程式集團將如雨後春筍般冒出。在歐洲，線上支付將更加熱絡，因為有越來越多銀行表示將支援行動支付⁶。現在，隨著第二號支付服務指令 (Revised Payment Service Directive，簡稱 PSD2) 在歐盟正式生效，再加上其他國家也陸續跟進制定了自己的法規⁷，「開放銀行」普及之路不再遙遠。但這卻也意味著銀行業將面臨更多網路資安威脅：從銀行 API 漏洞到新的網路釣魚詐騙伎倆等等⁸。業界廠商不論新舊皆必須採取一些應對措施：從開發內建資安設計的軟體，到定期執行資安稽核。

ATM 犯罪軟體商品化的情形將更加普遍，Cutlet Maker、Hello World 及 WinPot 等惡意程式的變種皆已出現販售的廣告。我們預料這些 ATM 惡意程式家族將在地下市場上彼此爭奪霸主的地位⁹。

Deepfake 將成為歹徒詐騙企業的下一個新領域。

多年來，電子郵件詐騙以及各種衍生的技巧¹⁰大多來自西非的詐騙集團¹¹，這樣的情況短期內應該不會有所改變。不過，我們預料 2020 年將出現運用最新技術 (尤其是 AI 技術) 的進階詐騙。AI 技術已被巧妙運用在製作幾可亂真的照片、影片及音訊，這些內容當中所呈現的對話和動作，都是合成出來的，這就是目前正快速崛起的「Deepfake」深度偽造技術¹²。Deepfake 的崛起相當令人擔憂，因為這項原本只是用來移花接木製作影視名人色情影片的技术，未來無可避免地將變成歹徒冒充企業人員的工具。

2019 年已經有網路犯罪集團運用 AI 技術來假冒員工說話的聲音來從事社交工程詐騙。一家能源企業據報因此受騙損失了 243,000 美元，在該案例中，詐騙集團正是使用 AI 來模仿其執行長的聲音¹³。未來將有更多詐騙集團會使用 Deepfake 來假冒高層決策人員，詐騙企業員工匯出款項或做出某些關鍵決定。此外，傳統的變臉詐騙 (BEC)¹⁴ 及技術支援詐騙也將開始改懸易轍。歹徒再也不會單單只偽造電子郵件地址，還會搭配運用 Deepfake 影音來增加假冒郵件的可信度。企業的 CXX 級主管將是這類詐騙的頭號目標，因為這些人經常出現在各種電話、會議、媒體與網路影片當中¹⁵，因此取材方便。

Google 已提供了大量的 Deepfake 影片供研究人員分析，以了解該如何偵測這些深度合成的影音內容¹⁶。儘管 Deepfake 詐騙目前才剛要崛起，但員工們必須開始學會分辨一些 Deepfake 影音的特徵，例如：說話語調改變、速度放慢、皮膚質地不太自然等等。而未來企業的財務流程也應該要有額外的驗證步驟來應對才是。

歹徒可能入侵託管服務廠商 (MSP) 來散布惡意程式或駭入企業外部供應鏈。

今日的企業越來越仰賴委外服務來滿足其日常營運需求，因此也令人擔憂駭客會經由企業外部供應鏈來避開企業本身的管控流程與防護措施¹⁷。這樣的風險來自於企業對第三方廠商 (如 MSP) 的完全信任。



近年來已開始出現各種不同形態的供應鏈攻擊，例如假冒軟體更新或入侵第三方服務廠商，來將惡意程式植入目標企業¹⁸，我們預料 2020 年影響中小企業最大的會是第二種情況。假使中小企業將全部或部分的基礎架構或營運外包，那這第三方廠商很可能會變成歹徒入侵企業的跳板。

處於供應鏈中的 MSP 一旦遭到入侵，還可能連帶波及下游的其他廠商。歹徒會先入侵第三方服務廠商，然後在其網站內植入惡意程式碼來蒐集客戶的敏感資料等等。駭客會先尋找資安措施薄弱的代理商或供應商，然後再將惡意程式散播至廠商的企業客戶。例如，某家軟體供應商正因為資訊基礎架構遭駭客入侵，連帶使得其服務的數百家牙科診所的電腦系統遭勒索病毒感染¹⁹。未來，這樣的情況就算沒變嚴重，也會持續下去。

為了避免遭到這類惡意程式襲擊，企業應該定期執行漏洞與風險評估，並設置一些預防性措施，包括徹底調查對系統擁有存取權限的服務供應商及員工的背景。

駭客將利用「可蠕蟲化」與「反序列化」漏洞。

今年 5 月，Microsoft 釋出了一項更新來修補 CVE-2019-0708 這個重大的遠端程式碼執行 (RCE) 漏洞，這就是俗稱的「BlueKeep」漏洞。隨後，該公司又陸續釋出了多次類似更新來修補一些影響 Windows 遠端桌面服務的漏洞。由於這些漏洞具備了「可蠕蟲化」特性²⁰，任何惡意程式只要利用此漏洞就能像 2017 年橫掃全球、癱瘓數十萬台電腦的 WannaCry 勒索病毒一樣迅速擴散。不過，要開發出一套攻擊 BlueKeep 漏洞的手法其實相當複雜，而且需要相當高超的技術。之前就曾出現過一個宣稱可攻擊此漏洞的 Metasploit 模組，不過卻被證明難以運用，不像 EternalBlue 漏洞攻擊套件²¹ 那樣方便。

相信未來我們還會再聽到更多有關 BlueKeep 的消息，此外也會聽到有關其他重大漏洞的相關攻擊嘗試。一些應用廣泛的通訊協定，如 Server Message Block (SMB) 和 Remote Desktop Protocol (RDP) 未來都將成為駭客試圖入侵系統時的攻擊途徑。惡名昭彰的 WannaCry 和 NotPetya 勒索病毒就是利用 SMB 通訊協定。而 RDP 通訊協定的資安問題也是不惶多讓，除了 BlueKeep 會用到之外，亦經常成為勒索病毒的入侵途徑²²，例如 SamSam 勒索病毒就會掃描裝置是否存在著暴露在外的 RDP 連接埠²³。

另一個我們認將成為企業重大隱憂的漏洞就是反序列化 (Deserialization) 漏洞。這個將非信賴資料反序列化的漏洞，是一群極為重大的漏洞，如果被用來攻擊企業應用程式，歹徒將可修改原本被視為無法修改的安全資料，進而執行歹徒所植入的程式碼²⁴。序列化是一種許多程式語言都用到的技巧，其目的是將物件轉成一種可儲存或傳輸的格式。反序列化就是將這道程序反過來。該機制之所以存在風險，是因為接收序列化物件的應用程式在將物件反序列化之前，通常不會先檢查一下這些非信賴的輸入資料。所以有技巧的駭客會不斷嘗試利用這項漏洞來將惡意物件插入序列化資料當中，讓物件得以在應用程式伺服器上執行。

與其試圖串聯多項漏洞以便能執行某段程式碼，駭客直接利用這項反序列化漏洞，反而更容易取得系統完全的控制權，而且還能自動執行程式碼，即使面對複雜的環境也一樣。序列化與反序列化是 Java 應用程式當中的重要觀念，對許多網站應用程式和中介軟體來說也經常用到。企業只要是使用了支援這類機制的平台，就應隨時修補相關漏洞以及採用虛擬修補技術²⁵，並且應對這方面的系統與軟體漏洞多加了解。



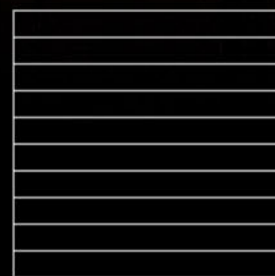


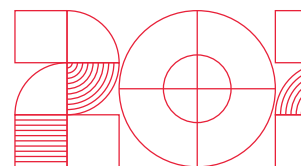
THE
FUTURE
IS

EXPOSED

U	V	O	E	B	U
N	U	P	X	R	N
S	L	E	P	O	P
A	N	N	O	A	R
F	E	L	S	D	O
E	R	B	E	T	T
B	A	R	D	C	E

未來，科技的匯流將帶來各種以資訊技術 (IT) 與營運技術 (OT) 資產為目標的新舊攻擊和技巧。





網路犯罪集團將瞄準 IoT 裝置 來從事間諜與勒索行動。

我們預料網路犯罪集團與駭客將運用機器學習與 AI 技術來竊聽企業內的連網裝置，例如：智慧電視與智慧喇叭。他們會利用語言辨識與物體識別技術來竊聽人員與業務上的對話。根據這些資料，再進一步找出可以勒索的目標，或者在企業內建立間諜行動據點。

至於其他藉由攻擊 IoT 裝置來獲利的方式，網路犯罪集團目前還沒找到能夠利用 IoT 來擴大攻擊面的有效商業模式，更遑論像 5G 網路所帶來的最新情勢。IoT 攻擊的獲利模式儘管仍在萌芽階段，但未來網路犯罪集團勢必會多方嘗試。其中，數位勒索²⁶是最可能的獲利模式之一。

目前，網路犯罪集團已經在地下論壇上不斷討論如何入侵各種連網裝置來獲利。這些獲利方式會先從消費性裝置下手，理所當然下一個目標就是連網的工業機械設備。我們已經可看到針對大型製造設備所用的可程式化邏輯控制器 (PLC) 相關的攻擊討論²⁷。

至於像路由器這類的 IoT 裝置，則可能被收編至駭客的殭屍網路當中，成為網路犯罪集團發動分散式網路攻擊的幫兇。除此之外，將路由器收編至殭屍網路，還可用來挾持網域名稱伺服器 (DNS hijacking)，而這還可當成犯罪工具或服務來販售，最主要是用於網路釣魚攻擊。不僅如此，地下市場上還販賣著網路攝影機畫面的存取權限，以及修改過韌體的智慧電表。這類暴露在外的裝置，也讓 IoT 資安相關的討論浮上檯面並成為焦點，尤其，並非所有 IoT 裝置都內建了資安防護或具備適當的攻擊防範能力。

5G 技術採用者將面臨移轉至 軟體定義網路的資安問題。

隨著 5G 技術在 2020 年逐漸開始布局，我們預料該領域將因技術太過新穎而出現各種不同的資安漏洞，包括其程式碼與不同環境之間的動態交換。就算是自動化管理，這項技術仍將帶來資安挑戰，不僅因為程式無可避免地會出現瑕疵，而廠商也尚未針對這項技術所帶來的相關威脅做好萬全準備。

由於 5G 環境是一種軟體定義的網路，為使用者和連網裝置帶來了高頻寬、低延遲的連線，因此可預見地 5G 網路服務將廣泛涵蓋各式各樣的應用與垂直市場。5G 網路相關的威脅將來自於軟體運作上的漏洞 (也就是管理 5G 網路的軟體或供應商本身的漏洞) 以及其分散式網路拓樸 (也就是更廣泛的攻擊途徑、大量的 IoT 裝置等等)。

駭客將試圖控制負責管理 5G 網路的軟體來操控網路本身。不僅如此，5G 相關的升級作業將如同智慧型手機的軟體更新一樣，無可避免地會存在著漏洞²⁸。研究人員已經展示了如何運用一些廉價的硬體與軟體平台來攻擊 5G 漏洞²⁹，因此相信網路犯罪集團的腳步應該也不會落後太多才對。5G 網路資安防護的不足，也使得某些資安問題更加惡化，包括：機密性 (如資料/流量遭到監聽)、一致性 (如資料在傳輸過程遭篡改) 與可用性 (如網路中斷可能引起連鎖效應)³⁰。

目前世界各國和各大廠商的成功指標似乎都是看誰能率先完成 5G 網路建置，因此基本上是犧牲安全來換取速度。但為了趕進度而造成組態設定上的缺失或打算事後再來補強 5G 的安全性，都會為資安帶來挑戰，因為日後仰賴這項技術的服務會越來越多。等 5G 基礎架構建置好後再來強化安全性，會比一開始就內建資安防護來得更加複雜³¹。而且要解決防護不足的問題，將需要擁有解決軟體定義網路問題能力的資安專業人才³²。如果網路提供了動態切換功能，那麼資安防護也必須具備動態能力。例如，在採用網路功能虛擬化 (NFV) 與應用程式虛擬化來動態部署網路服務的環境中，資安防護就必須要能隨應用程式而快速部署。

關鍵基礎架構將受到更多攻擊與停機事件的影響。

2020 年公共事業與其他關鍵基礎架構/基礎建設 (CI) 仍將是網路勒索集團的攻擊目標。而勒索病毒也依然是網路犯罪集團的首選利器，因為企業若不付款將面臨很高的風險。生產線可能因而癱瘓數星期，隨系統復原的時間長短而定，而生產線長期停擺將造成可觀的財務損失。此外，駭客也可能建立殭屍網路，對營運技術 (OT) 網路發動分散式阻斷服務 (DDoS) 攻擊。採用雲端服務的製造業，需面臨供應鏈攻擊的危險，若供應商的資安做得不好，很可能會變成駭客攻擊的跳板，使得生產線癱瘓。在基礎架構方面，其最迫切的問題則是因網路攻擊而使得服務中斷，因此對於導入工業物聯網 (IIoT) 的企業來說，強化網路資安的壓力只會越來越大³³。

近幾年來，有多個不同的駭客團體專門對全球各地的發電廠進行情報偵察³⁴。這些針對性勒索病毒攻擊活動的主要目標是希望取得工業控制系統 (ICS) 以及監控與資料擷取 (SCADA) 系統的登入憑證，並蒐集廠房設施運作的相關資料。這些入侵行動的衝擊不僅將在受攻擊的基礎架構內部擴散，更可能向外延伸至一些相互依賴的系統，因此影響深遠 (例如發電廠停止運作導致當地電力中斷³⁵)。

然而駭客攻擊所造成的系統故障還不只影響公共事業，舉凡食品生產、交通運輸以及製造設備，都會慢慢導入 IoT 並透過人機介面 (HMI) 來管理、診斷與控制相關設備，因此也會招來危險。

公共建設與政府 IT 基礎架構，都將比民間產業更容易暴露在駭客攻擊的威脅中，原因是公共事業的經費通常較為不足。駭客在偵查行動當中所獲得的資訊，能讓駭客有機會策劃更縝密的聯合攻擊，不僅可能中斷基礎架構服務，更可能影響政府與政治制度的運作。



家庭辦公室與其他遠端工作模式將改寫供應鏈攻擊的定義。

企業必須非常小心在家工作模式以及那些模糊了企業資安界線的家庭連網裝置所帶來的風險。畢竟，家庭辦公室不如企業環境來得安全。再者，其 Wi-Fi 無線網路如果不夠安全，就會像開放或公共場所一樣，提高遠端工作的風險。開放的網路會讓敏感的檔案與資訊暴露於被竊聽的危險³⁶。此外，原本在遠端使用的裝置有可能感染了惡意程式之後，再將惡意程式帶到企業內部網路散播，進而造成企業機密資訊外洩。

工作人力的行動化，已使得員工不再像從前那樣整天坐在辦公室內。在家工作的員工有別於自行攜帶裝置 (BYOD) 到公司上班的人員，會在不同裝置之間隨時切換，並且存取雲端應用程式與通訊軟體。因此，連網家用裝置變成駭客攻擊企業的入口，已經是無可避免的發展趨勢，而且員工在工作上也可能會用到智慧電視、喇叭、語音助理等裝置。企業必須決定該採取怎樣的資安政策來應對這樣的情境。

網路犯罪集團可利用他們蒐集來的個人資訊，假扮成員工，透過家用或公用網路發動一波精心策畫的攻擊。像這樣日趨精密的攻擊，已經遠遠超越單純地將款項匯到某個帳戶或者散播惡意程式。員工的家庭網路環境將成為歹徒發動供應鏈攻擊的入口。

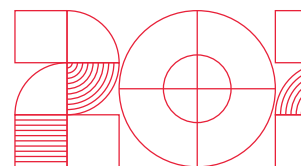


MISCONFIGURED

THE
FUTURE
IS

轉型至雲端和 DevOps 環境，不僅將帶來效益，也將帶來風險，突顯資安防護應涵蓋整個部署流程的必要性。

M I S C O N
B A T G E F
R L A L R I
O J K I R G
K G E T O U
E N H C R R
M E N T D E



容器元件的漏洞將成為 DevOps 團隊需要優先面對的資安問題。

容器³⁷ 是一個瞬息萬變的環境，不但應用程式經常推陳出新、架構越來越整合，其軟體更是不時推出新的版本，因此傳統的資安方法已無法跟上這樣的步調。

這正是為何當容器逐漸顛覆傳統、在企業內肩負更重要的使命時，開發資安營運 (DevSecOps) 原則對 DevOps 團隊變得相當重要。由於容器環境的部署週期很短，因此能保留給資安與漏洞測試的時間所剩不多。現在，企業光為了一個應用程式，可能就需要保護數百個橫跨多台虛擬機器、散置不同雲端服務平台的容器。企業將因為容器架構各元件的問題而忙得不可開交，包括：執行環境 (如 Docker、CRI-O、Containerd、runC³⁸)、協調工具 (如 Kubernetes) 以及建構環境 (如 Jenkins) 等等的漏洞。駭客會想盡辦法利用任何脆弱的環節來入侵 DevOps 流程。

一些普遍流行的容器映像若含有漏洞然後又被下載到企業內使用，將對企業流程造成不良影響。假使企業必須仰賴第三方來提供映像修補，那麼容器的修補將更加麻煩。容器化應用程式的漏洞，不只將影響容器程式碼或引擎，還會影響整個環境的許多其他單元，這些都是駭客可能試圖駭入及操控的目標。

無伺服器平台將因為組態設定錯誤以及含有漏洞的程式碼而擴大企業的受攻擊面。

有越來越多的企業正在擁抱無伺服器 (Serverless) 平台，藉此整合雲端應用程式並降低成本。Gartner 預測，至 2020 年全球約有 20% 以上的企業採用無伺服器運算技術³⁹。無伺服器平台可提供所謂的「功能服務」(Function as a Service)，讓企業不需支付整套伺服器或整個容器的成本，就能讓開發人員執行其程式碼⁴⁰。然而，採用無伺服器技術並非就能對資安問題免疫。

我們預料一些過時未更新的程式庫、組態設定錯誤，以及已知和未知的漏洞，都可能是無伺服器應用程式遭威脅入侵的破口。駭客可利用這些弱點來蒐集敏感資訊或滲透企業網路⁴¹。

除此之外，無伺服器平台包含了容器、無伺服器功能以及其他相關的元件，更加突顯潛在威脅來源的複雜性。既然無伺服器運算 (尤其是開放原始碼) 提供的是無狀態 (stateless) 功能，因此如何監控存取權限與儲存敏感資料，將是 2020 年的最重要考量。所以，除了提升網路透明度之外，執程序的改善與工作流程的詳實記載，對執行無伺服器應用程式來說顯得相當重要。

由於功能是位於容器式應用程式當中，因此無伺服器的部署環境也應將 DevSecOps 列為首要目標。此外，無伺服器環境也將受惠於 DevSecOps 所提倡的持續整合與易用性⁴²。一些專門解決無伺服器基礎架構資安問題(如開放原始碼應用程式相依性與漏洞)的資安工具，對採用無伺服器環境以及部署某些功能來說至關重要。

使用者造成的組態設定不當以及不安全的第三方廠商，將加深雲端平台的風險。

企業就算定期更新系統並採取適當的措施，如果應用程式的組態設定不當或者認證機制不足，仍然會帶來風險。一些基本的資安控管如果未建置妥當，將對企業的資料安全帶來巨大威脅。

由於雲端服務的弱點，我們預見將來會看到更多網路入侵事件。因雲端儲存組態設定不當而造成資料外洩，仍將是 2020 年企業常見的資安問題。存取控管不足、權限管理不當、事件記錄未妥善監控、企業資產暴露在公共網路上，這些都只不過是企業在建置雲端網路可能會犯的其中幾項疏失。雲端服務相關的錯誤和疏失，將使企業的眾多資料暴露在外，甚至被政府懲罰或罰款。要消除這些風險，企業可提升雲端整體的資安狀況(如正確設定及部署基礎架構)，並採取最佳實務原則，確實遵循產業規範。

隨著越來越多企業和生產線(亦即生產製造流程)⁴³移轉至雲端，未來將牽涉更多的第三方服務廠商。而這些廠商可能帶來一些隱藏風險，因為他們或許沒有太多的雲端經驗(換句話說仍習慣於傳統的流程和系統)，而且也不具備適當的基礎架構防護。所以駭客很可能會利用殭屍網路來發動 DDoS 攻擊，試圖干擾雲端服務的運作。

雲端平台將因其採用的第三方程式庫而遭到程式碼注入攻擊。

2020 年將出現更多雲端平台遭到程式碼注入攻擊的案例，不論是直接攻擊雲端平台或是經由第三方程式庫。駭客注入惡意程式的目的大多是為了竊聽流量或者掌控使用者的雲端檔案及資訊。這類從雲端服務網站應用程式下手的駭客攻擊，最常使用的手法就是跨網站腳本攻擊(Cross-Site Scripting)以及 SQL 資料隱碼攻擊(SQL Injection)。駭客一旦得逞，就能從遠端取得敏感資訊並篡改資料庫內容。另一方面，駭客也可以繞道第三方程式庫來達成相同目的，只要使用者下載了被篡改的程式庫，就會執行被注入的惡意程式碼⁴⁴。

在此同時，我們也預見將有更多駭客的目光跟隨著企業的资料移轉到雲端。可預期地，當軟體服務(SaaS)、基礎架構服務(IaaS)及平台服務(PaaS)運算模式更加普及，雲端入侵的案例也將增加。當有越多企業將資料放在雲端，就會引來越多駭客的覬覦。要防範雲端入侵必須多管齊下：開發人員應善盡自己的職責、企業應仔細評估自己採用的供應商及平台，同時也要改善雲端資安狀況的管理。

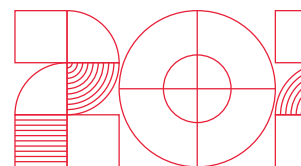


DEFENSE IS RESPONSIBLE

THE
FUTURE
IS

S P R O T D
E I F E E E
C T I L C F
U R A B T E
R O E A E N
E F L B L S
S A E L B I

網路資安人才的短缺與不良的資安習慣，也進一步助長了資安的問題。要建立一個安全的環境，關鍵就在於風險管理與完整的威脅情報。



預判式偵測及行為偵測將是對抗持續性威脅與無檔案式威脅的重要關鍵。

無檔案式威脅未來仍將是傳統黑名單機制的漏網之魚⁴⁵。企業必須考慮採用具備行為偵測、沙盒模擬分析與流量監控能力的解決方案。由於這類威脅會潛藏在系統登錄或系統記憶體內，或利用系統白名單上的正常工具，如 PowerShell 和 Windows Management Instrumentation (WMI)，因此，非檔案式偵測指標 (例如特定的執行事件或行為) 就變得非常重要。無檔案式攻擊技巧一直都是其他攻擊形態的重要元素，駭客會利用這類技巧在系統植入木馬程式⁴⁶、虛擬加密貨幣挖礦程式⁴⁷、勒索病毒⁴⁸ 等等。

除了專門感染 IoT 裝置、讓裝置變成 DDoS 殭屍網路成員的 Linux 威脅之外⁴⁹，以 Linux 為基礎的惡意程式也將因為開放原始碼在企業內日漸位居要角 (儘管並非企業平台主要元件⁵⁰) 而持續穩定成長。除此之外，具備資訊竊取能力的惡意程式變種數量也會成長，因為這些都是駭客蒐集資訊的可靠工具，可讓他們進一步滲透網路。我們預料這些威脅將經由各種途徑 (如無檔案式技巧) 長期潛伏在企業系統內部，隨時準備發動下一波攻擊。

MITRE ATT&CK 資安框架將在企業資安評估當中扮演更重要的角色。

MITRE ATT&CK 資安框架提供了一整套的資安評估指標。其公開的知識庫採用已知攻擊的相關資料來對攻擊的手法與技巧進行分類和說明⁵¹。我們預料未來將有更多企業採用這套框架來進行威脅模型、資安產品以及企業風險的評估。除了讓威脅追蹤人員更容易掌握駭客的攻擊和模式之外，也讓防守陣營更方便評估防範措施與資安工具的成效。此外，MITRE ATT&CK 知識庫也可作為一套資安管理員與網路資安廠商的共同資源，進一步簡化駭客攻擊技巧與防禦手段相關情報的分享。

威脅情報必須透過資安數據分析專業知識來發揮效果，層層防護企業資安架構。

展望 2020 年及未來，我們預料駭客攻擊在計劃上將更加周詳、目標將更加分散、手法也將更多變化。威脅情報與資安分析將有助於企業主動守護其環境的安全、發掘資安漏洞、消除脆弱的環節，並且了解駭客的攻擊策略。對於希望能夠降低資安風險、事先預防任何攻擊事件發生的企業來說，能確實融入資安及相關風險評估流程的完整威脅情報，將是企業的無價之寶。

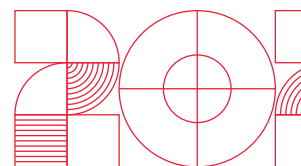
只要分析情報能隨手可得，讓資安防護隨時做好準備，不論是進階威脅、長期潛伏的惡意程式、常見的網路釣魚，或是潛在的零時差漏洞以及其他攻擊手法，都能事先加以預防。企業若能全方位掌握整個環境的資安狀況，就能擁有一套能即時偵測威脅並有效攔截攻擊的預防方法。這意味著企業的情報掌握必須超越端點的層次，將電子郵件、伺服器、雲端工作負載以及網路也納入整體情報網的範圍。

企業必將意識到，網路資安人才短缺與不良的資安習慣，仍是影響 2020 年威脅情勢的重要因素。決策者與 IT 主管必須要能掌握其企業環境整體的資安狀況。至於資安專家，如資安營運中心 (SOC) 的分析師，則能協助企業掌握問題的全貌，並且將企業內所發現的情況與全球威脅情報進行交叉比對。



CYBERSECURITY IN 2020

I N F O R M
C N O I T A
O N N E C T
C Y B E R S
T I R U C E
Y 2 0 2 0 2
D A T A O O



與資安專家合作，是企業從網路資安基礎架構各層面下手以防範各種風險的必要條件。如此才能讓防禦者與開發人員都能進一步掌握及掌控其連網的裝置並解決資安上的弱點。即時、零時差的偵測能力，也將是主動發掘已知及未知威脅的關鍵。

面對瞬息萬變的威脅情勢，企業需要一套跨世代融合且環環相扣的多層式防禦，並以下列資安能力為基礎：

- ▶ **全方位掌握**。利用專業工具和專家知識提供最佳化、優先次序分明的威脅調查，進而降低衝擊並矯正風險。
- ▶ **威脅預防與有效遏止**。自動遏止已偵測到並以視覺化方式呈現的威脅，此外更搭配惡意程式防護、AI/機器學習、應用程式控管、網站信譽評等以及垃圾郵件防護技巧。
- ▶ **託管式偵測及回應**。提供資安專業能力來交叉關聯警示通知與偵測資料，藉由最佳化威脅情報工具來進行威脅追蹤、全方位分析與立即矯正。
- ▶ **行為監控**。主動攔截進階惡意程式與進階攻擊技巧，偵測異常行為與惡意程式相關的攻擊手法。
- ▶ **端點防護**。保護使用者，利用沙盒模擬分析、入侵偵測、端點感應等功能來預防攻擊並保護資料。
- ▶ **入侵防護**。阻止可疑流量，如幕後操縱 (C&C) 通訊與資料外傳。

參考資料

1. Catalin Cimpanu。(2018年10月13日)。ZDNet。「Microsoft JET 漏洞雖然最近已經被修復，但仍然可能遭到攻擊」(Microsoft JET vulnerability still open to attacks, despite recent patch)。上次存取時間 2019年10月8日：<https://www.zdnet.com/article/microsoft-jet-vulnerability-still-open-to-attacks-despite-recent-patch/>。
2. Ionut Arghire。(2019年3月29日)。Security Week。「Cisco 路由器漏洞修補不完全」(Cisco Improperly Patched Exploited Router Vulnerabilities)。上次存取時間 2019年10月30日：<https://www.securityweek.com/cisco-improperly-patched-exploited-router-vulnerabilities>。
3. Catalin Cimpanu。(2019年9月9日)。ZDNet。「資安研究人員披露另一起 Chrome 修補缺失」(Security researchers expose another instance of Chrome patch gapping)。上次存取時間 2019年10月8日：<https://www.zdnet.com/article/security-researchers-expose-another-instance-of-chrome-patch-gapping/>。
4. Vladimir Kropotov、Fyodor Yarochkin 與 Michael Ofiaza。(2019年1月7日)。趨勢科技資訊安全新聞。「一諾千金：地下論壇上的信賴與倫理」(Your Word is Your Bond: Trust and Ethics in Underground Forums)。上次存取時間 2019年10月8日：<https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/your-word-is-your-bond-trust-and-ethics-in-underground-forums>。
5. Europol。(2019年10月9日)。Europol。「網路犯罪越來越大膽，資料已成為犯罪的焦點」(Cybercrime Is Becoming Bolder With Data At The Centre Of The Crime Scene)。上次存取時間 2019年10月11日：<https://www.europol.europa.eu/newsroom/news/cybercrime-becoming-bolder-data-centre-of-crime-scene>。
6. Apple。(2019年10月1日)。Apple。「歐洲及中東支援 Apple Pay 的銀行」(Apple Pay participating banks in Europe and the Middle East)。上次存取時間 2019年10月8日：<https://support.apple.com/en-gb/HT206637>。
7. PwC。(日期不詳)。PwC Italia。「開放銀行...所以呢?」(Open Banking... so what?)。上次存取時間 2019年10月28日：<https://www.pwc.com/it/en/industries/banking/future-open-banking.html>。
8. Feike Hacquebord、Robert McArdle、Fernando Mercês 與 David Sancho。(2019年9月17日)。趨勢科技資訊安全新聞。「開放銀行的風險」(The Risks of Open Banking)。上次存取時間 2019年10月8日：<https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-risks-of-open-banking-are-banks-and-their-customers-ready-for-psd2>。
9. Numaan Huq、Vladimir Kropotov、Mayra Rosario、David Sancho 與 Fyodor Yarochkin。(2019年6月28日)。趨勢科技資訊安全新聞。「犯罪軟體求售：ATM 惡意程式在網路犯罪地下市集的商品化」(Crimeware for Sale: The Commoditization of ATM Malware in the Cybercriminal Underground)。上次存取時間 2019年10月8日：<https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/crimeware-for-sale-the-commoditization-of-atm-malware-in-the-cybercriminal-underground>。
10. Europol。(2018年)。Europol。「2018年網際網路組織犯罪威脅評估」(Internet Organised Crime Threat Assessment 2018)。上次存取時間 2019年10月16日：<https://www.europol.europa.eu/sites/default/files/documents/iocta2018.pdf>。
11. The United States Department of Justice。(2019年9月10日)。US Department of Justice。「鎖定數百名變臉詐騙犯的全球聯合執法行動在世界各地逮捕 281 人」(281 Arrested Worldwide in Coordinated International Enforcement Operation Targeting Hundreds of Individuals in Business Email Compromise Schemes)。上次存取時間 2019年10月16日：<https://www.justice.gov/opa/pr/281-arrested-worldwide-coordinated-international-enforcement-operation-targeting-hundreds>。
12. J.M. Porup。(2019年4月10日)。CSO Online。「Deepfake 影片的運作原理與引發的風險」(How and why deepfake videos work — and what is at risk)。上次存取時間 2019年10月11日：<https://www.csoonline.com/article/3293002/deepfake-videos-how-and-why-they-work.html>。
13. Catherine Stupp。(2019年8月30日)。The Wall Street Journal。「犯罪集團在某個罕見的案例當中使用 AI 來假冒執行長聲音」(Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case)。上次存取時間 2019年10月11日：<https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402>。
14. 趨勢科技。(日期不詳)。趨勢科技。「變臉詐騙 (BEC)」(Business Email Compromise (BEC))。上次存取時間 2019年10月11日：[https://www.trendmicro.com/vinfo/us/security/definition/business-email-compromise-\(bec\)](https://www.trendmicro.com/vinfo/us/security/definition/business-email-compromise-(bec))。
15. Liam Tung。(2019年9月4日)。ZDNet。「別管電子郵件了：詐騙集團利用 Deepfake 技術模仿執行長的聲音詐騙員工匯款」(Forget email: Scammers use CEO voice 'deepfakes' to con workers into wiring cash)。上次存取時間 2019年10月16日：<https://www.zdnet.com/article/forget-email-scammers-use-ceo-voice-deepfakes-to-con-workers-into-wiring-cash/>。
16. Nick Dufour 與 Andrew Gully。(2019年9月24日)。Google AI Blog。「提供 Deepfake 偵測研究資料」(Contributing Data to Deepfake Detection Research)。上次存取時間 2019年10月23日：<https://ai.googleblog.com/2019/09/contributing-data-to-deepfake-detection.html>。
17. 趨勢科技。(日期不詳)。趨勢科技。「商業流程入侵 (BPC)」(Business Process Compromise (BPC))。上次存取時間 2019年10月11日：<https://www.trendmicro.com/vinfo/us/security/definition/business-process-compromise>。
18. Chaoying Liu 與 Joseph C. Chen。(2019年1月16日)。趨勢科技資訊安全情報部落格 (Security Intelligence Blog)。「新的 Magecart 攻擊經由網路廣告供應鏈來散布惡意程式」(New Magecart Attack Delivered Through Compromised Advertising Supply Chain)。上次存取時間 2019年10月11日：<https://blog.trendmicro.com/trendlabs-security-intelligence/new-magecart-attack-delivered-through-compromised-advertising-supply-chain/>。
19. Catalin Cimpanu。(2019年8月29日)。ZDNet。「勒索病毒襲擊美國數百家牙醫診所」(Ransomware hits hundreds of dentist offices in the US)。上次存取時間 2019年10月24日：<https://www.zdnet.com/article/ransomware-hits-hundreds-of-dentist-offices-in-the-us/>。
20. Simon Pope。(2019年8月13日)。Microsoft Security Response Center。「修補新的遠端桌面服務可蠕蟲化漏洞 (CVE-2019-1181/1182)」(Patch new wormable vulnerabilities in Remote Desktop Services (CVE-2019-1181/1182))。上次存取時間 2019年10月8日：<https://msrc-blog.microsoft.com/2019/08/13/patch-new-wormable-vulnerabilities-in-remote-desktop-services-cve-2019-1181-1182/>。
21. Dan Goodin。(2019年9月7日)。Ars Technica。「Windows 平台 BlueKeep 可蠕蟲化漏洞攻擊手法在網路上流傳」(Exploit for wormable BlueKeep Windows bug released into the wild)。上次存取時間 2019年10月24日：<https://arstechnica.com/information-technology/2019/09/exploit-for-wormable-bluekeep-windows-bug-released-into-the-wild/>。
22. Jay Yaneza。(2017年2月9日)。趨勢科技資訊安全情報部落格 (Security Intelligence Blog)。「RDP 暴力破解攻擊在系統植入 CRYISIS 勒索病毒」(Brute Force RDP Attacks Plant CRYISIS Ransomware)。上次存取時間 2019年10月8日：<https://blog.trendmicro.com/trendlabs-security-intelligence/brute-force-rdp-attacks-plant-cryisis-ransomware/>。
23. 趨勢科技。(2018年3月23日)。趨勢科技資訊安全新聞。「亞特蘭大網路攻擊疑似出現 SAMSAM 勒索病毒」(SAMSAM Ransomware Suspected in Atlanta Cyberattack)。上次存取時間 2019年10月8日：<https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/samsam-ransomware-suspected-in-atlanta-cyberattack>。
24. MITRE。(2019年9月19日)。Common Weakness Enumeration。「CWE-502：非信賴資料反序列化」(CWE-502: Deserialization of Untrusted Data)。上次存取時間 2019年10月8日：<https://cwe.mitre.org/data/definitions/502.html>。
25. 趨勢科技。(2018年10月25日)。趨勢科技資訊安全新聞。「虛擬修補：在漏洞遭到攻擊之前預先加以修補」(Virtual Patching: Patch Those Vulnerabilities before They Can Be Exploited)。上次存取時間 2019年10月24日：<https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/virtual-patching-patch-those-vulnerabilities-before-they-can-be-exploited>。
26. 趨勢科技。(日期不詳)。趨勢科技。「數位勒索」(Digital Extortion)。上次存取時間 2019年10月7日：<https://www.trendmicro.com/vinfo/us/security/definition/digital-extortion>。

27. Stephen Hilt、Vladimir Kropotov、Fernando Mercès、Mayra Rosario 與 David Sancho。(2019年9月10日)。*趨勢科技資訊安全新聞*。「揭開網路犯罪地下市集的IoT威脅」(Uncovering IoT Threats in the Cybercrime Underground)。上次存取時間2019年10月7日：<https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-internet-of-things-in-the-cybercrime-underground>。
28. Tom Wheeler 與 David Simpson。(2019年9月3日)。*The Brookings Institution*。「為何5G需要新的網路資安方法」(Why 5G requires new approaches to cybersecurity)。上次存取時間2019年10月16日：<https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/>。
29. Altaf Shaik 與 Ravishankar Borgaonkar。(2019年)。*Black Hat*。「5G網路的新漏洞」(New Vulnerabilities in 5G Networks)。上次存取時間2019年10月16日：<https://i.blackhat.com/USA-19/Wednesday/us-19-Shaik-New-Vulnerabilities-In-5G-Networks-wp.pdf>。
30. 趨勢科技。(2019年10月14日)。*趨勢科技資訊安全新聞*。「歐盟報告點出5G網路的網路犯罪風險」(EU Report Highlights Cybersecurity Risks in 5G Networks)。上次存取時間2019年10月17日：<https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/eu-report-highlights-cybersecurity-risks-in-5g-networks>。
31. Tom Wheeler 與 David Simpson。(2019年9月3日)。*The Brookings Institution*。「為何5G需要新的網路資安方法」(Why 5G requires new approaches to cybersecurity)。上次存取時間2019年10月6日：<https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/>。
32. Craig Gibson、Vladimir Kropotov、Philippe Lin、Rainer Vosseler 與 Fyodor Yarochkin。(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10月16日：<https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/securing-enterprises-for-5g-connectivity>。
33. 趨勢科技。(2019年8月15日)。*趨勢科技資訊安全新聞*。「保護工業物聯網：保護能源、自來水與石油基礎架構」(Securing the Industrial Internet of Things: Protecting Energy, Water and Oil Infrastructures)。上次存取時間2019年10月30日：<https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/securing-the-industrial-internet-of-things-protecting-energy-water-and-oil-infrastructures>。
34. 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10月24日：<https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/new-critical-infrastructure-facility-hit-by-group-behind-triton>。
35. 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10月7日：<https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/triton-wielding-its-trident-new-malware-tampering-with-industrial-safety-systems/>。
36. Alfred Ng。(2019年9月19日)。*CNET*。「WeWork的Wi-Fi安全性不足導致敏感文件外洩」(WeWork's weak Wi-Fi security leaves sensitive documents exposed)。上次存取時間2019年10月31日：<https://www.cnet.com/news/weworks-weak-wi-fi-security-leaves-sensitive-documents-exposed/>。
37. 趨勢科技。(日期不詳)。*趨勢科技*。「容器」(Container)。上次存取時間2019年10月10日：<https://www.trendmicro.com/vinfo/us/security/definition/container>。
38. 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10月10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>。
39. Gartner, Inc.。(2018年12月4日)。*Gartner*。「Gartner公布2019年影響基礎架構與營運的十大趨勢」(Gartner Identifies the Top 10 Trends Impacting Infrastructure and Operations for 2019)。上次存取時間2019年10月24日：<https://www.gartner.com/en/newsroom/press-releases/2018-12-04-gartner-identifies-the-top-10-trends-impacting-infras>。
40. Scott Fulton III。(2019年4月9日)。*ZDNet*。「無伺服器運算的真正意義與其他您該知道的一切」(What serverless computing really means, and everything else you need to know)。上次存取時間2019年10月24日：<https://www.zdnet.com/article/what-serverless-computing-really-means-and-everything-else-you-need-to-know/>。
41. Guy Podjarny。(2018年5月15日)。*The Register*。「哇！好酷，您邁入了無伺服器時代。現在您只要操心那些壞掉的功能就行」(Hey cool, you went serverless. Now you just have to worry about all those stale functions)。上次存取時間2019年10月10日：https://www.theregister.co.uk/2018/05/15/stale_serverless_functions/。
42. 趨勢科技。(2018年4月13日)。*趨勢科技資訊安全新聞*。「無伺服器應用程式：它們對DevOps的意義為何」(Serverless Applications: What They Mean in DevOps)。上次存取時間2019年10月10日：<https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/serverless-applications-what-they-mean-in-devops>。
43. Willem Sundblad。(2019年7月18日)。*Forbes*。「智慧製造：建立一套混合雲邊界策略」(Smart Manufacturing: Creating a Hybrid Cloud-Edge Strategy)。上次存取時間2019年10月10日：<https://www.forbes.com/sites/willemsundbladeurope/2019/07/18/smart-manufacturing-creating-a-hybrid-cloud-edge-strategy/#77fc5816af5a>。
44. 趨勢科技。(2018年11月29日)。*趨勢科技資訊安全新聞*。「駭客感染Node.js套件來竊取比特幣錢包」(Hacker Infects Node.js Package to Steal from Bitcoin Wallets)。上次存取時間2019年10月10日：<https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/hacker-infects-node-js-package-to-steal-from-bitcoin-wallets>。
45. 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10月8日：<https://www.trendmicro.com/vinfo/us/security/news/security-technology/risks-under-the-radar-understanding-fileless-threats>。
46. Henry Alarcon Jr. 與 Raphael Centeno。(2019年3月4日)。*趨勢科技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10月8日：<https://blog.trendmicro.com/trendlabs-security-intelligence/fileless-banking-trojan-targeting-brazilian-banks-downloads-possible-botnet-capability-info-stealers/>。
47. Augusto Remillano II 與 Arvin Macaraeg。(2019年4月12日)。*趨勢科技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10月8日：<https://blog.trendmicro.com/trendlabs-security-intelligence/miner-malware-spreads-beyond-china-uses-multiple-propagation-methods-including-eternalblue-powershell-abuse/>。
48. Erika Mendoza、Jay Yaneza、Gilbert Sison、Anjali Patil、Julie Cabuhat 與 Joelson Soares。(2019年3月29日)。*趨勢科技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Nozeless勒索病毒載入程式」(Emotet-Distributed Ransomware Loader for Nozeless Found via Managed Detection and Response)。上次存取時間2019年10月8日：<https://blog.trendmicro.com/trendlabs-security-intelligence/emotet-distributed-ransomware-loader-for-nozeless-found-via-managed-detection-and-response/>。
49. Mark Vicente、Byron Galera 與 Augusto Remillano II。(2019年4月3日)。*趨勢科技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10月8日：<https://blog.trendmicro.com/trendlabs-security-intelligence/bashlite-iot-malware-updated-with-mining-and-backdoor-commands-targets-wemo-devices/>。
50. Steven Vaughan-Nichols。(2019年7月1日)。*ZDNet*。「根據Microsoft開發人員披露，目前Linux在Azure上的使用率高於Windows Server」(Microsoft developer reveals Linux is now more used on Azure than Windows Server)。上次存取時間2019年10月30日：<https://www.zdnet.com/article/microsoft-developer-reveals-linux-is-now-more-used-on-azure-than-windows-server>。
51. The MITRE Corporation。(日期不詳)。*MITRE*。「ATT&CK」。上次存取時間2019年10月11日：<https://attack.mitre.org/>。



獻給 Raimund Genes (1963-2017 年)



趨勢科技 2020 年資安預測

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。我們的創新解決方案，能為客戶的資料中心、雲端工作負載、網路、端點裝置提供多層式資安防護。

我們的研究機構 Trend Mico Research 是我們領先市場的核心關鍵，其背後擁有一群熱情的專家為後盾，他們熱衷發掘最新威脅、與外界分享重要分析情報、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，經常發表有關針對性攻擊、人工智慧、物聯網 (IoT)、網路犯罪集團等等的創新研究。我們不斷鑽研並預測最新威脅，發表令人深思、影響產業策略方向的研究。

www.trendmicro.com

©2019 年版權所有。趨勢科技股份有限公司保留所有權利。Trend Micro 與 t 字球形標誌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。