Microsoft

2022 年 Microsoft 數位防禦報告

釐清威脅形勢並賦予數位防禦能力。

內容

除非另行指出，否則這份報告中資料、深入解析和事件的涵蓋時間是從 2021 年 7 月到 2022 年 6 月 (Microsoft 2022 會計年度)。

為了在檢視和瀏覽本報告時獲得最佳體驗，我們建議使用 Adobe Reader，可從 Adobe 網站免費下載。

簡介者 Tom Burt
公司副總裁，客戶安全和信任部門

「從我們遍佈全球的產品與服務生態系統中，我們分析了數以兆計的訊號，發掘出全球數位威脅的肆虐程度、範圍和規模。」

我們的環境快照...

威脅形勢的範圍和規模

密碼攻擊的數量估計每秒提高到 921 次攻擊之多，光是一年就增加了 74%。

瓦解網路犯罪

到目前為止，Microsoft 移除了網路罪犯使用的 10,000 多個網域，以及國家級行為體使用的 600 多個網域。

解決漏洞

我們從 93% 的勒索軟體事件回應互動中發現了對權限存取和橫向移動的管控能力不足。

2022 年 2 月 23 日，網路安全世界進入了新時代，也就是混合戰時代。這一天，就在飛彈發射與坦克車跨越邊界的數小時前，俄羅斯行為體鎖定烏克蘭政府機構、科技和金融領域為目標，發動了大規模的毀滅性網路攻擊。您可以在此第三版年度《Microsoft 數位防禦報告》(MDDR) 的 < 國家威脅 > 一章中，了解更多有關這些攻擊的資訊以及從中汲取的教訓。這些教訓的關鍵在於，雲端提供了最佳的實體和邏輯安全性來抵禦網路攻擊，並且實現了威脅情報與端點防護方面的進展，同時在烏克蘭證明了其價值。

雖然年度網路安全性發展的任何調查都必須從這一點開始，但今年的報告則提供了更深入的探討。在報告的第一章中，我們聚焦在網路罪犯的活動，接著在第二章探討國家威脅。這兩個組織的攻擊複雜程度都大幅提升，進而大幅提升了其行動的影響層面。雖然俄羅斯佔盡了頭條新聞版面，但是，伊朗行為體在政權交替後將其攻擊行動升級，對以色列發動了毀滅性的攻擊，並且對美國的重大基礎設施發動了勒索軟體及駭入再洩露活動。中國同樣也增加了在東南亞及南半球其他地方的間諜活動，試圖反制美國勢力，並竊取關鍵資料和資訊。

而就如第三章內容所探討的，外國行為體也採用了高效技術在全球各地展開政治宣傳勢力活動。舉例來說，俄羅斯一直努力讓其公民和許多其他國家 / 地區的公民相信，入侵烏克蘭是合理作為，同時也一邊在西方散播抹黑 COVID 疫苗的政治宣傳，一邊在境內推廣其效用。此外，行為體更加鎖定物聯網 (IoT) 裝置或營運技術 (OT) 控制裝置為目標，做為入侵網路和重大基礎設施的進入點，這個部分將在第四章加以探討。在本報告的最後一章，我們回顧一年來的網路恢復力發展時，提供了過去一年來抵禦對 Microsoft 和客戶發動的攻擊所獲得的深入解析和汲取的教訓。

每一章都根據 Microsoft 獨特的優勢，提供汲取到的重要教訓與深入解析。從我們遍佈全球的產品與服務生態系統中，我們分析了數萬億的訊號，發掘出全球數位威脅的肆虐程度、範圍和規模。Microsoft 正採取行動保護我們的客戶和數位生態系統免受這些威脅的侵害，您可以深入閱讀以了解我們如何運用自身技術來識別並阻擋數十億的網路釣魚企圖、身分識別竊取和其他威脅。

簡介者 Tom Burt
續

我們也運用了法律和技術手段來查封和關閉遭到網路罪犯和國家級行為體利用的基礎結構，並通知客戶何時遭受到國家級行為體的威脅或攻擊。我們致力於不斷開發更有效的功能和服務，這些功能使用 AI/ML 技術來識別和封鎖網路威脅，同時有安全性專業人員能更快、更有效地抵禦和找出網路入侵。

也許最重要的是，在整個 MDDR 中，我們為個人、組織和企業提供了能夠付諸行動的最佳建議，幫助他們抵禦這些日益增加的數位威脅。採取良好的網路檢疫措施就是最佳防禦，能夠顯著降低網路攻擊的風險。

網路犯罪現況

網路罪犯繼續以複雜的營利企業做為行動的身分。攻擊者正不斷調整並尋找新方法來施展其技術，藉此增加其託管宣傳行動基礎結構的方式和位置的複雜性。同時，網路罪犯也越來越懂得節省開支。為了降低其額外負荷並大幅提升對外呈現的合法樣貌，攻擊者會入侵企業網路和裝置來從事網路釣魚活動、託管惡意軟體，甚至利用其運算能力來從事加密貨幣挖礦。

深入了解，前往 p6

「在烏克蘭的混合戰中網路武器部署的出現，正宣告著新的衝突時代來臨。」

國家威脅

國家級行為體發動的網路攻擊日益複雜，其主要目的在於避開偵測，並推進其策略性優先事項。在烏克蘭的混合戰中網路武器部署的出現，正宣告著新的衝突時代來臨。俄羅斯同樣以資訊勢力活動來支援其戰事，運用政治宣傳來影響俄羅斯、烏克蘭和全球的觀點。在烏克蘭以外地區，國家級行動體增加了活動，並開始利用先進的自動化、雲端基礎結構和遠端存取技術來擴大攻擊的目標。能夠存取最終目標的企業 IT 供應鏈經常遭到攻擊。網路安全性檢疫變得更加重要，因為行為體會迅速入侵未修補的漏洞，使用複雜的暴力破解技術竊取認證，並且使用開放來源或合法軟體來混淆其活動。此外，伊朗與俄羅斯一起使用包括勒索軟體在內的破壞性網路武器，做為其攻擊主力。

這些發展急需採用一致的全球架構，以優先處理人權和保護人們不受網路上魯莽國家的行為迫害。各國之間必須相互合作，共同實踐負責任的國家級行為規範與規則。

深入了解，前往 p6

裝置和基礎結構

在全球疫情之下，加上迅速採用各種面向網際網路的裝置成為加速數位轉型的一部分，大大增加了我們數位世界的攻擊面。因此，網路罪犯和各國都在迅速利用它。雖然近年來 IT 硬體和軟體的安全性已增強許多，但 IoT 和 OT 裝置的安全性仍無法跟上腳步。威脅執行者正利用這些裝置在網路上建立存取權並進行橫向移動，在供應鏈中打造立足點，或中斷目標組織的 OT 營運。

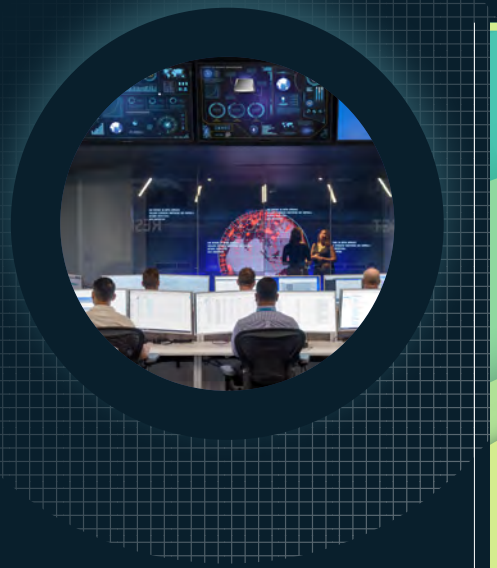
深入了解，前往 p56

簡介者 Tom Burt
續

網路勢力活動

各國無論是對內或在國際間使用複雜的勢力活動來散發政治宣傳及影響大眾觀點的情況日益增加。這些活動破壞了信任、推升極端化，並且威脅著民主進程。老練的進階持續滲透操控者行為體會利用傳統媒體搭配網際網路和社交媒體來大幅擴大其活動的範圍、規模並效率，並且在全球資訊生態系統中造成巨大的影響。在過去一年，我們看到俄羅斯在烏克蘭發動的混合戰當中運用了這些活動，同時也看到俄羅斯和包括中國和伊朗在內的其他國家部署越來越多透過社交媒體進行的政治宣傳活動，目的就是在各種議題上擴大其全球勢力。

深入了解，前往 p71



網路恢復力

安全性是技術成功的關鍵推手。唯有導入安全措施，讓組織盡可能具備抵禦現代攻擊的韌性，才能達成創新和提高生產力的目標。全球疫情讓我們面臨了挑戰，在 Microsoft，我們將安全性做法和技術轉而運用來保護我們的員工，無論他們在何處工作都能安全無虞。過去這一年中，威脅執行者繼續利用全球疫情爆發與轉換成混合式工作環境期間所暴露出的漏洞。此後，我們的主要挑戰一直是管理盛行且複雜的各種攻擊方法，以及越來越多的國家活動。在本章中，我們詳細探討了我們所面臨的挑戰，以及為了回應我們 15,000 多個合作夥伴而動員的防禦措施。

深入了解，前往 p86

我們獨特的優勢

370 億
成功封鎖的
電子郵件威脅

347 億
已封鎖的
身分識別威脅

43 兆
每天合成的訊號，運用複雜的資料分析和 AI 演算法來了解及防範數位威脅和網路犯罪活動。

25 億
每天分析的端點訊號

8,500+
工程師、研究人員、資料科學家、網路安全專家、威脅獵人、地緣政治分析師、調查人員及第一線回應人員，遍佈 77 個國家 / 地區。

15,000+
我們安全性生態系統中的合作夥伴，為客戶提高了網路恢復力。

2021 年 7 月 1 日到 2022 年 6 月 30 日

簡介者 Tom Burt
續

我們相信 Microsoft 無論是獨自進行，或是與私人產業、政府機關和民間社會團體中的其他人密切合作，都有責任保護數位系統，以鞏固我們社會的社交結構，並促進安全無虞的運算環境，讓每個人無論身在何處都能受到保護。就是這份責任心敦促我們自 2020 年以來，每年發佈 MDDR。這份報告正是集結 Microsoft 的大量資料與全方位研究的成果。報告中分享了我們對於數位威脅形勢演變的獨到見解，以及現今能夠採取的關鍵行動，以改善生態系統的安全性。

我們希望能傳達一股迫切感，讓讀者能夠根據在這裡以及我們一整年發行的眾多網路安全性刊物中呈現的資料和見解而立即行動。當我們思考威脅對於數位環境形成的重力時 (以及對於真實世界的意義)，必須記住，我們都有能力採取行動來保護自己、我們的組織和企業免受數位威脅的侵害。

感謝您撥冗回顧今年的《Microsoft 數位防禦報告》。希望您會覺得它提供了寶貴的深入解析和建議，幫助我們共同防禦數位生態系統。

Tom Burt 公司副總裁，客戶安全和信任部門

這份報告有雙重目標：

1. 讓整個生態系統中的客戶、合作夥伴和利益關係人清楚了解不斷演進的數位威脅形勢，並清楚呈現新的網路攻擊和過去持續存在威脅的演進趨勢。
2. 讓我們的客戶和合作夥伴有能力改善其網路恢復力並回應這些威脅。

網路犯罪現況

隨著網路防禦措施不斷改進，以及越來越多組織採取主動預防措施，攻擊者也會調整其技術。

概觀

網路犯罪現況

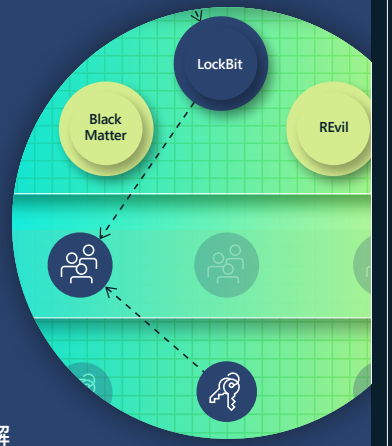
隨著網路防禦措施不斷改進，以及越來越多組織採取主動預防措施，攻擊者也會調整其技術。

網路罪犯繼續以複雜的營利企業做為行動的身分。攻擊者正不斷調整並尋找新方法來施展其技術，藉此增加其託管宣傳行動基礎結構的方式和位置的複雜性。同時，網路罪犯也越來越懂得節省開支。為了降低其額外負荷並大幅提升對外呈現的合法樣貌，攻擊者會入侵企業網路和裝置來從事網路釣魚活動、託管惡意軟體，甚至利用其運算能力來從事加密貨幣挖礦。

網路犯罪繼續上升，因為網路犯罪經濟透過提供更多利用工具和基礎結構的機會，降低了入行的技能障礙。

深入了解，前往 p18

勒索軟體和勒索的威脅越來越大膽，將攻擊目標鎖定在政府機關、企業和重大基礎設施。

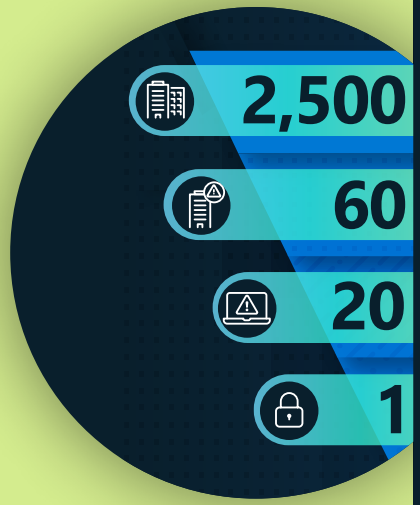


在 p9 深入了解

攻擊者越來越常以公開敏感資料做為威脅，促使受害者支付贖金。

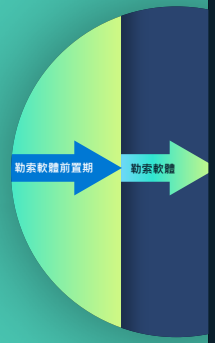
在 p10 深入了解

人為操作的勒索軟體最為普遍，因為罪犯利用這些攻擊成功入侵了三分之一的目標，而其中有 5% 遭到勒索。



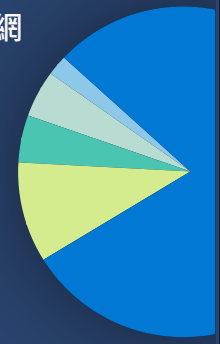
深入了解，前往 p9

打擊勒索軟體最有效的防禦措施包括跨網路架構的多因素驗證、頻繁的安全性修補程式及零信任原則。



深入了解，前往 p13

以無差別的方式鎖定所有收件匣的認證網路釣魚攻擊不斷增加，而商務電子郵件入侵（包括發票詐欺）為企業帶來了相當大的網路犯罪風險。



深入了解，前往 p21

為了打擊網路罪犯和國家級行為體的惡意基礎結構，Microsoft 採取了創新的法律措施並倚賴我們的公私合作夥伴關係。

深入了解，前往 p25

前言

網路犯罪繼續增加，隨機和目標式攻擊也不斷增加。

隨著網路防禦措施改進，以及越來越多政府機構和企業主動進行預防，我們看到攻擊者利用兩種策略來取得從事網路犯罪所需的存取權。一種方法是倚賴數量的廣泛目標活動。另一種方法是利用監視和更精選的目標來提高回報率。即使創造收入並非目標，例如出於地緣政治目的的國家活動，仍同時發動隨機和目標式攻擊。過去一年以來，網路罪犯繼續依賴社交工程和利用主題議題讓攻擊活動發揮最大的影響力。例如，雖然 COVID 為主題的網路釣魚誘餌使用頻率較低，但我們仍觀察到尋求捐款支持烏克蘭公民的誘餌不斷增加。

攻擊者正不斷調整並尋找新方法來施展其技術，藉此增加其託管宣傳行動基礎結構的方式和位置的複雜性。我們觀察到，網路罪犯越來越節省開支，而攻擊者也不再付錢購買技術。為了降低其額外負荷並大幅提升對外呈現的合法樣貌，有些攻擊者會更頻繁找機會入侵企業以從事網路釣魚活動、託管惡意軟體，甚至利用其運算能力來從事加密貨幣挖礦。

在本章中，我們也會探討激進駭客的崛起，這是私人公民採取網路攻擊手段以進一步達成社會或政治目標所造成的中斷情形。自 2022 年 2 月以來，世界各地有成千上萬名專家和新手以個人身分動員起來發動攻擊，例如造成網站停擺和洩漏竊得的資料，這些都是烏俄戰爭的一部分。這股趨勢是否會在積極抗爭結束之後延續下去，現在預測還言之過早。

組織必須定期審查並鞏固存取控制，以及實施安全性策略來抵禦網路攻擊。然而，他們能做的不只這些。我們會說明我們的數位犯罪部門 (DCU) 如何運用民事案例來查封遭到網路罪犯和國家級行為體利用的惡意基礎結構。我們必須透過公私夥伴關係共同打擊這個威脅。我們希望透過分享過去 10 年來所學到的知識，幫助其他人了解並思考能夠採取哪些主動措施來保護自己和整個生態系統，共同對抗不斷擴張的網路犯罪威脅。

Amy Hogan-Burney
數位犯罪部門總經理

勒索軟體與勒索：國家級威脅

勒索軟體攻擊對所有個體的危險性增加，因為犯罪分子利用不斷成長的網路犯罪生態系統發動攻擊，而重大基礎設施、所有規模的企業，以及州政府和地方政府都是他們的目標。

在過去兩年中，高調的勒索軟體事件（如涉及重大基礎設施、醫療保健和 IT 服務提供者的事件）引起了大眾相當程度的關注。隨著勒索軟體攻擊的範圍越來越大，其影響也越來越廣泛。以下是我們在 2022 年看到的攻擊範例：

- 2 月時，有兩家公司遭到攻擊，影響了德國北部數百個天然氣站的付款處理系統。[1]
- 3 月時，希臘的郵政服務遭到攻擊，使得郵遞工作暫時中斷，並影響了金融交易的處理。[2]
- 5 月底，哥斯大黎加政府機構遭到勒索軟體攻擊，造成醫院關閉及海關和稅收作業中斷，迫使該國政府宣告進入全國緊急狀態。[3]
- 同樣在 5 月，一起攻擊造成印度最大的航空公司之一航班延誤和取消，導致數百名旅客滯留。[4]

這些攻擊的成功，以及對真實世界的影響程度，都是網路犯罪經濟工業化的結果，從而取得工具和基礎結構，並透過降低入門的技能門檻來擴充網路罪犯的能力。

近年來，勒索軟體已從單一「犯罪集團」同時負責開發和散佈勒索軟體裝載模組的模式，轉向勒索軟體即服務 (RaaS) 模式。RaaS 可讓一個集團管理開發勒索軟體裝載模組的工作並提供付款和勒索的服務，透過將資料洩漏給稱為「同夥」的其他網路罪犯（也就是實際發動勒索軟體攻擊者）的方式，以從中分得利潤。這種分工合作的網路犯罪經濟擴大了攻擊者的版圖。網路犯罪工具的工業化使得攻擊者更容易進行入侵、洩漏資料及部署勒索軟體。

人為操作的勒索軟體[5]一詞，是由 Microsoft 研究人員所創造，用來描述人為發動的威脅，這些人會根據他們在目標網路所發現的內容在每一個攻擊階段做出決策，有別於商品勒索軟體攻擊的威脅，人為操作的勒索軟體對於組織來說仍是一大威脅。

模型以適用於端點的 Microsoft Defender (EDR) 資料為基礎 (2022 年 1 月至 6 月)。

勒索軟體與勒索：國家級威脅

續

隨著採取雙重勒索獲利策略成為標準做法，勒索軟體攻擊甚至變得更具影響力。這包括洩漏遭入侵裝置的資料、將裝置上的資料加密，然後張貼或威脅公開張貼竊得的資料，迫使受害者支付贖金。

雖然大多數勒索軟體攻擊者會利用投機取巧的方式將勒索軟體部署到取得存取權的任何網路，但有些攻擊者會利用存取代理人與勒索軟體操作者之間的人脈，向其他網路罪犯購買存取權。

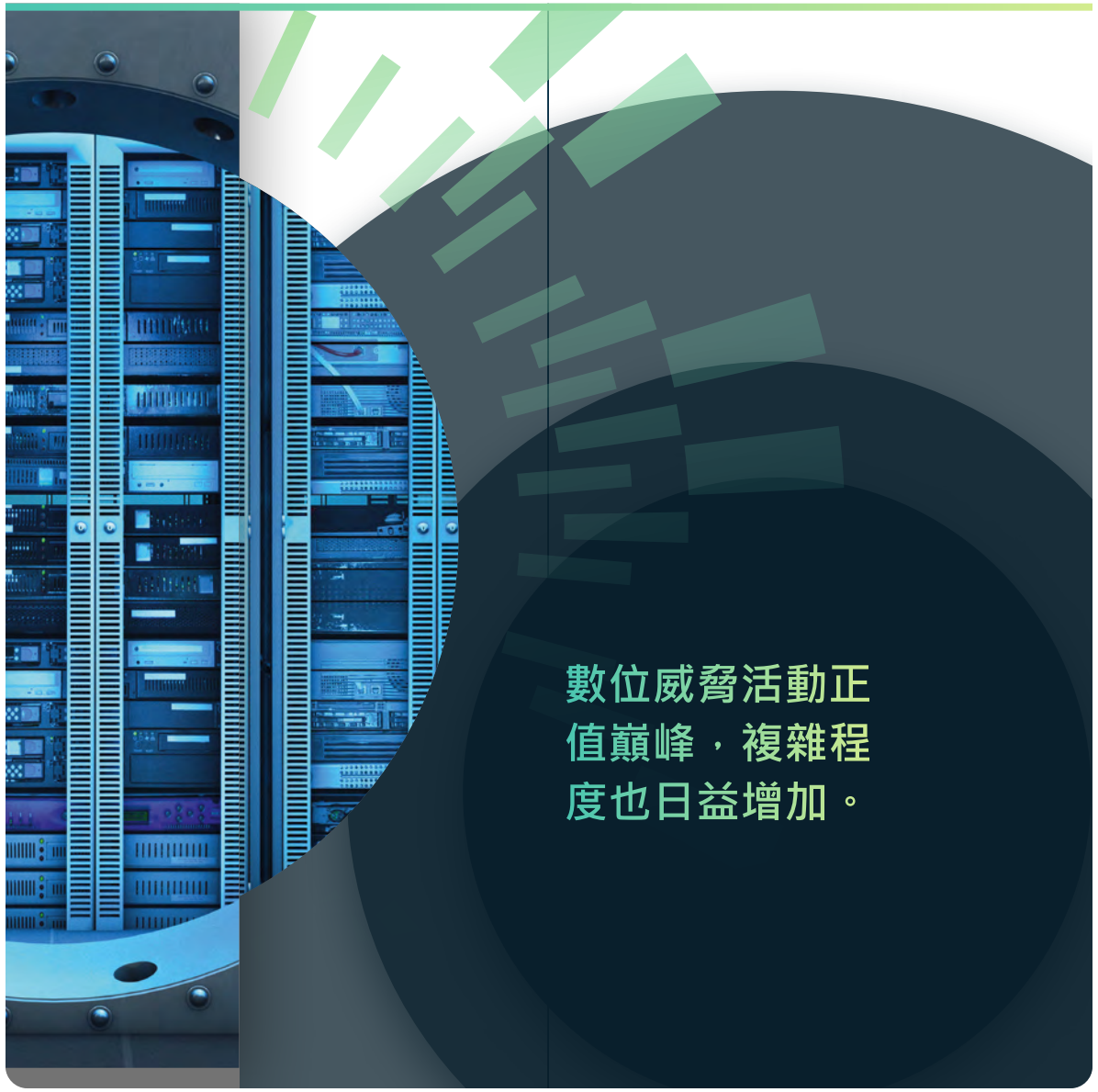
我們獨特的訊號廣度情報是從包括身分識別、電子郵件、端點和雲端等多個來源蒐集而來，並深入洞悉不斷成長的勒索軟體經濟與同夥體系，當中包括專為技術能力較低的攻擊者所設計的工具。

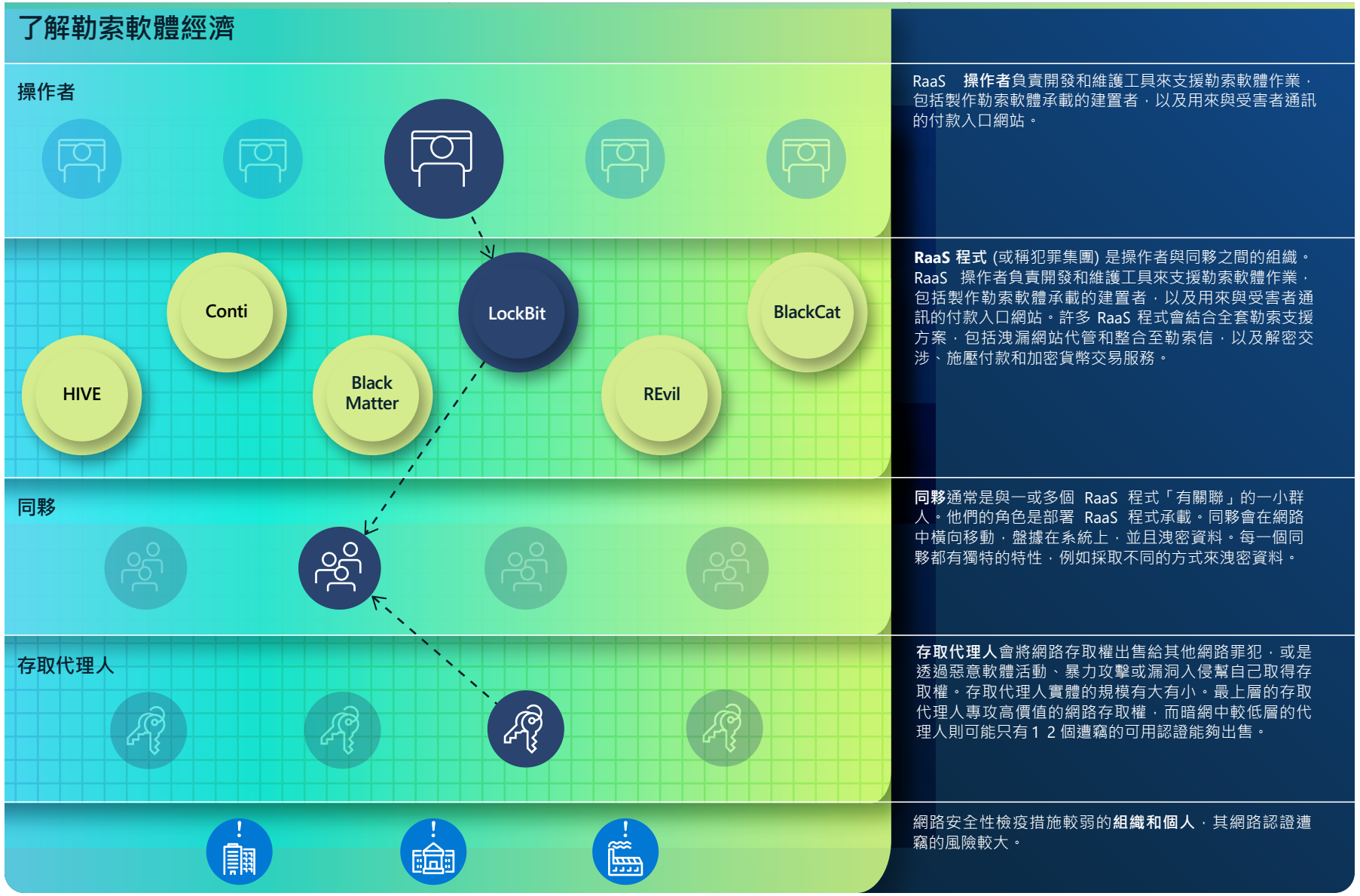
專業網路罪犯之間不斷擴大的關係，提高了勒索軟體攻擊的速度、複雜性和成功率。這種情況促使網路罪犯生態系統演變為具備不同技術、目標和技能的互聯玩家，他們在初始存取目標、付款服務，以及解密或發佈工具或網站方面相互支援。

勒索軟體操作者現在可以線上購買組織或政府網路的存取權，或透過主要目的單純是出售所取得存取權獲利的代理人之間的人際關係取得認證和存取權。

然後操作者會利用購得的存取權來部署購自暗網市場或論壇的勒索軟體裝載模組。在許多案例中，與受害者協商是由 RaaS 團隊進行，而不是操作者本身。這些犯罪交易過程順暢，參與者因為在暗網上匿名且跨國執法有其難度，而不容易遭到逮不和起訴。

為了持續並成功打擊此一威脅，便需要民營機構密切配合政府策略的執行。





勒索軟體有時與媒體描述的方式有所不同，單一勒索軟體變異鮮少由單一端對端「勒索軟體犯罪集團」所管理。反而是有單獨的實體會建置惡意軟體、取得受害者的存取權、部署勒索軟體，以及處理勒索協商。因犯罪生態系統工業化而出現了：

- 存取代理人，負責入侵並移交存取權 (存取權即服務)。
- 銷售工具的惡意軟體開發人員。
- 從事入侵的犯罪操作者與同夥。
- 從同夥 (RaaS) 手上接管獲利的加密和勒索服務提供者。

所有人為操作的勒索軟體活動都有共同的安全性弱點相依性。具體而言，攻擊者通常會利用組織的不良網路檢疫，這通常包括不常修補和無法實施多因素驗證 (MFA)。

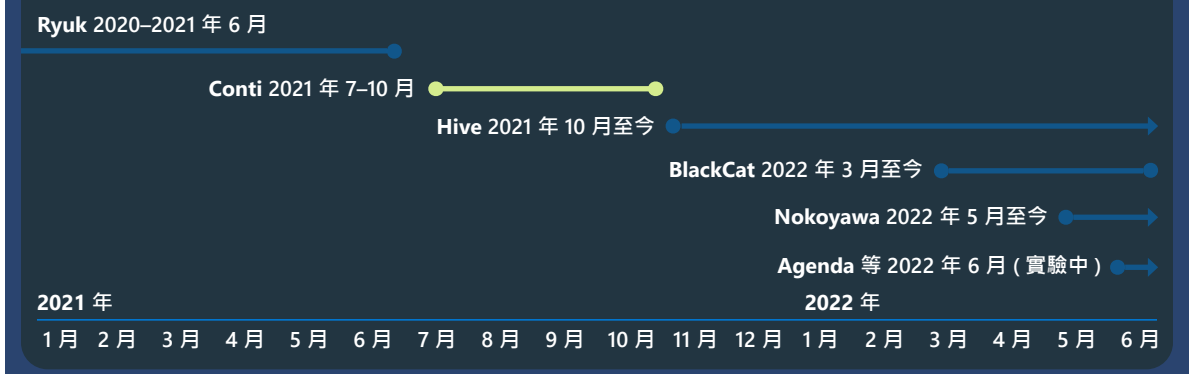
案例研究：瓦解 Conti

Conti 是過去兩年來最大型的勒索軟體變種之一，從 2022 年中開始停止運作，Microsoft 威脅情報中心 (MSTIC) 在 3 月底和 4 月初觀察到活動明顯減少。我們最後一次觀察到 Conti 勒索軟體部署是在 4 月中。不過，就像關閉其他勒索軟體運作一樣，Conti 的瓦解並未對勒索軟體部署造成明顯的衝擊，因為 MSTIC 觀察到 Conti 同夥轉向部署其他勒索軟體裝載模組，包括 BlackBasta、Lockbit 2.0、LockbitBlack 和 HIVE。這種情況與往年的資料一致，也暗示著勒索軟體犯罪集團會先銷聲匿跡，然後幾個月後又會重新出現，或將技術能力和資源重新分配到新組織。

我們的 Microsoft 情報團隊會根據勒索軟體威脅執行者的特定工具將其視為個別組織 (標記為 DEV) 進行追蹤，而不是依據他們使用的惡意軟體來進行追蹤。這表示，當 Conti 的同夥分散時，我們得以透過他們使用其他工具或 RaaS 套件來繼續追蹤這些 DEV。例如：

- DEV-0230 附屬於 Trickbot，一直是 Conti 的多發使用者。在 4 月底，MSTIC 使用 QuantumLocker 觀察到它。
- DEV-0237 從 Conti 的勒索軟體套件轉移到 HIVE 和 Nokoyawa，包括在 5 月 31 日對哥斯大黎加政府機構的攻擊中使用 HIVE。
- 我們使用 BlackBasta 觀察到 Conti 勒索軟體套件的另一個多發使用者 DEV-0506。

同夥 (DEV-0237) 在 RaaS 程式之間快速轉換的範例



在 Conti 等 RaaS 程式關閉後，勒索軟體同夥幾乎立即轉移到另一處 (Hive)。

RaaS 使得勒索軟體生態系統不斷進化並妨礙歸因

由於人為操作的勒索軟體是由個別操作者所推行，因此攻擊模式會因目標而不同，而且在整個攻擊過程中輪流發生。在過去，我們在單一勒索軟體攻擊的每一個活動中，觀察到初始進入媒介、工具和勒索軟體裝載模組選擇之間的密切關係。這讓歸因工作更容易進行。不過，RaaS 同夥模式解開了這層關係。因此，Microsoft 追蹤在特定攻擊中部署裝載模組的勒索軟體同夥，而不是將勒索軟體裝載模組開發人員視為操作者進行追蹤。

換句話說，我們不再假設 HIVE 開發人員是 HIVE 勒索軟體攻擊背後的操作者，而更有可能是同夥。

網路安全業一直努力要正確掌握開發人員和操作者的界線。但業界仍經常根據裝載模組名稱來通報勒索軟體事件，這會形成一種假像，以為單一實體 (或稱勒索軟體犯罪集團) 是使用該特定勒索軟體裝載模組的所有攻擊幕後的藏鏡人，而與之關聯的所有事件都採用共同的技術和基礎結構。為了支援網路防禦者，就必須深入了解不同的同夥攻擊的前置階段 (如資料洩密和其他持續性機制)，以及可能存在的偵測和防護機會。

除了惡意軟體，攻擊者還需要認證才能成功行動。要讓整個組織成功遭到人為操作的勒索軟體感染，有賴於存取高權限的帳戶。

聚焦人為操作的勒索軟體攻擊

在過去一年，Microsoft 的勒索軟體專家對超過 100 起人為操作的勒索軟體事件進行深入調查，以追蹤攻擊者的技術，並了解如何改善保護我們客戶的方式。

務必注意的是，我們在這裡分享的分析可能僅適用已上線、受管理的裝置。未上線且未管理的裝置代表組織硬體資產中最不安全的一環。

最普遍的勒索軟體階段技術：

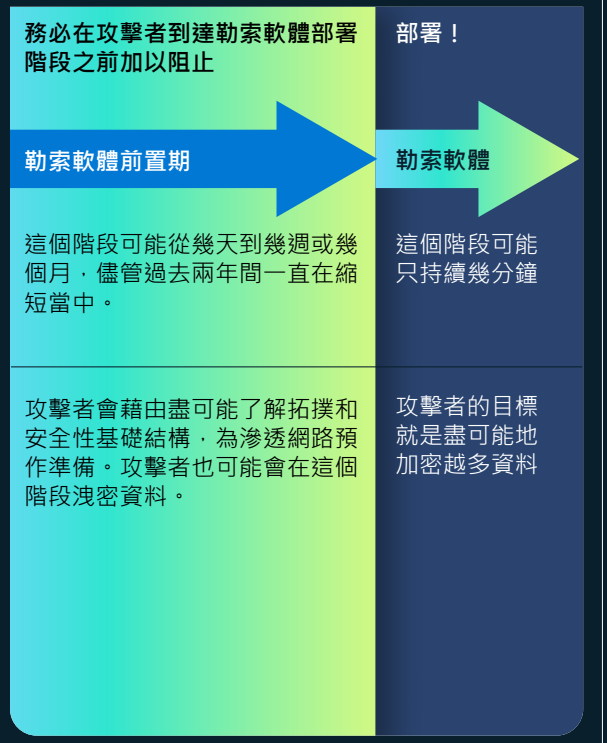
75%
使用管理工具。

75%
使用取得的高權限遭入侵使用者帳戶，透過 SMB 通訊協定散佈惡意裝載模組。

99%
嘗試使用作業系統建置工具竄改找到的安全性和備份產品。

典型的人為操作攻擊

人為操作的勒索軟體攻擊可分類為勒索軟體前置階段和勒索軟體部署階段。在勒索軟體前置階段，攻擊者會透過了解組織拓撲和安全性基礎結構，為滲透網路預作準備。



我們的調查發現，人為操作的勒索軟體攻擊背後大多數的執行者會利用類似的安全性弱點，而且有共同的攻擊模式和技術。

持久的安全性策略

對抗和防止這種性質的攻擊需要改變組織的觀念，轉而專注於所需的全方位防護，以減緩和阻止攻擊者，使其無法從勒索軟體前置階段進展到勒索軟體部署階段。

企業必須持續且積極地將安全性最佳做法應用於網路，以達到減少攻擊類型的目標。由於人為決策的關係，讓這些勒索軟體攻擊能夠產生多個看似不同的安全產品警示，因而可能很容易錯失或無法即時回應。警示疲勞會真正發生，而安全營運中心 (SOC) 可藉由查看警示的趨勢或依事件將警示分組，如此就能了解整體情勢，處理起來也變得更容易。接著 SOC 就能使用如受攻擊面縮小規則等強化功能來消除警示。強化以對抗常見威脅，不僅能減少警示量，還能在許多攻擊者取得網路存取權之前加以阻止。

組織必須持續維持高標準的安全性態勢和網路檢疫，以保護自己不受人為操作的勒索軟體攻擊。

可付諸行動的見解

勒索軟體攻擊者都是受容易獲利所激發，因此透過安全性強化來增加成本是顛覆網路犯罪經濟的關鍵。

1. 建立認證檢疫。除了惡意軟體，攻擊者還需要認證才能成功行動。要讓整個組織成功遭到人為操作的勒索軟體感染，有賴於存取高權限的帳戶，像是網域管理員，或是編輯群組原則的能力。
2. 稽核認證暴露。
3. 優先部署 Active Directory 更新。
4. 優先強化雲端。
5. 縮小受攻擊面。
6. 強化面向網際網路的資產，並了解您的周邊。
7. 強化您的網路以減少 SOC 警示疲勞的情形，就能減少高優先順序事件的數量並保留頻寬。

進一步資訊的連結

- RaaS：了解網路犯罪零工經濟以及如何自我保護 | Microsoft 安全性部落格 (英文)
- 人為操作的勒索軟體攻擊：可預防的災難 | Microsoft 安全性部落格 (英文)

來自一線應變人員的勒索軟體深入解析

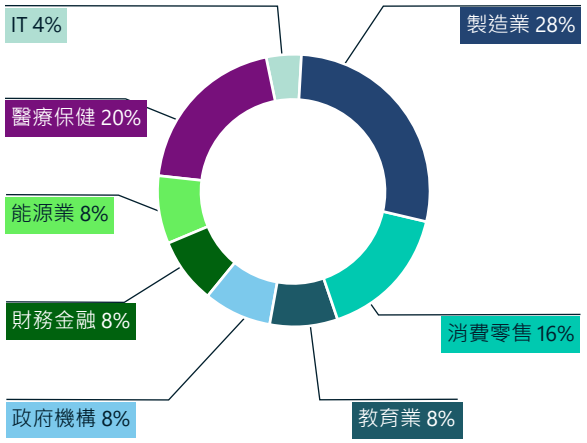
自 2019 年以來，全世界的組織都經歷了人為操作的勒索軟體攻擊穩定增加的情況。然而，去年的執法行動和地緣政治事件對網路犯罪組織有著重大的影響。

Microsoft 的 Security Service Line 在整個網路攻擊過程中，從調查到成功圍堵和復原活動一路為客戶提供支援。應變和復原服務是透過兩個高度整合的團隊提供，其中一個團隊專注於調查和復原的基礎工作，另一個團隊則專注於圍堵和復原。本節將摘要整理過去一年來勒索軟體活動的調查結果。

93%

的 Microsoft 勒索軟體事件復原活動調查中發現了存取和橫向移動的管控權限不足。

各產業的勒索軟體事件和復原活動

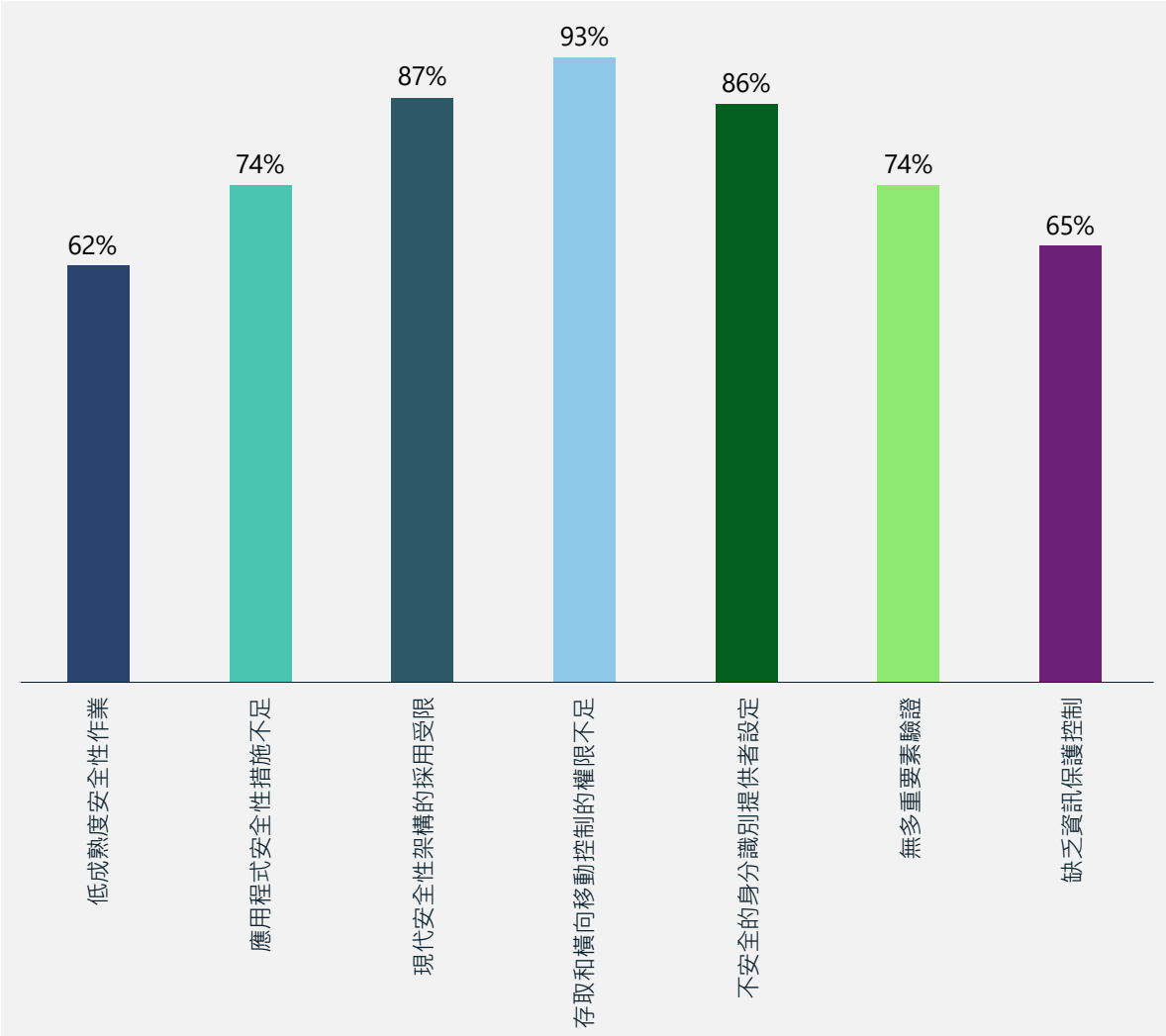


隨著新的小型組織和威脅出現，防禦團隊必須注意到不斷進化的勒索軟體威脅，同時防範之前未知的勒索軟體惡意軟體系列。犯罪集團利用的快速開發手段導致出現了利用簡單易用的套件來封裝情報勒索軟體的做法。如此一來，攻擊者就擁有更大的彈性，能夠對更多目標發動廣泛的攻擊。

下面幾頁將深入探討造成防護脆弱無力對抗勒索軟體最常觀察到的因素，調查結果可分成三類：

1. 脆弱的身分識別控制
2. 成效不彰的安全性作業
3. 資料防護有限

勒索軟體應變活動中最常見的調查結果摘要



勒索軟體事件應變活動中最常見的調查結果是存取和橫向移動控制的權限不足。

來自一線應變人員的勒索軟體深入解析

續

在我們的現場應變互動中看到的三個主要導因包括：

① **脆弱的身分識別控制：**
認證竊取攻擊仍是最大導因之一

② **成效不彰的安全性作業程序**
不僅讓攻擊者有機可趁，還會嚴重影響復原時間

③ **終究要回歸到資料：組織難以實施有效的資料防護策略來滿足其業務需要**

① 脆弱的身分識別控制

人為操作的勒索軟體持續進化，並採取傳統上與目標式攻擊相關的認證竊取和橫向移動方法。成功的攻擊通常是長時間活動的結果，這些活動涉及入侵身分識別系統，如 Active Directory (AD)，使人為操作者得以竊取認證、存取系統，並持續留在網路中。

Active Directory (AD) 和 Azure AD 安全性

88%

受影響的客戶未採用 AD 和 Azure AD 安全性最佳做法。這已成為常見的攻擊媒介，因為攻擊者利用重要身分識別系統中的不當組態和較弱的安全性態勢，來得到更廣泛的存取權並對企業造成衝擊。

最低權限存取和使用權限存取工作站 (PAW)

受影響的組織在管理其重要身分識別和高價值資產 (如專利系統和業務關鍵應用程式) 時，均未透過專用工作站實施適當的管理認證隔離和最低權限存取原則。

權限帳戶安全性

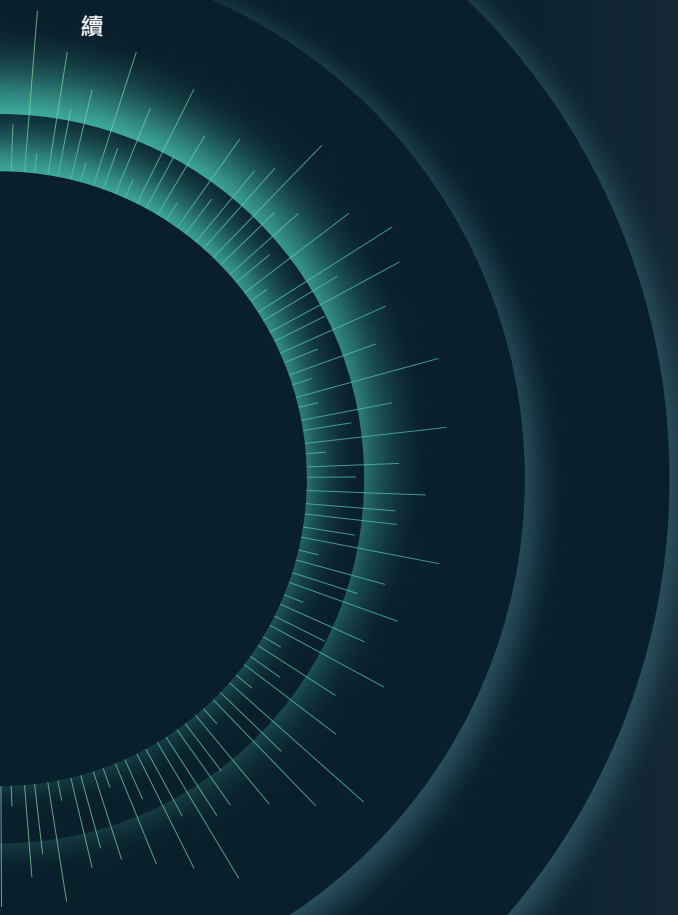
88%

MFA 的互動並未針對敏感和高權限的帳戶實施，因此讓攻擊者有安全性漏洞能夠入侵認證，並使用合法認證發動進一步的攻擊。

84%

有 84% 的組織管理員未使用權限身分識別控制 (如即時存取) 來防止入侵的權限認證遭到進一步惡意利用。

來自一線應變人員的勒索軟體深入解析



② 成效不彰的安全性作業

我們的資料顯示，遭到勒索軟體攻擊的組織在安全性作業、工具和資訊技術資產生命週期管理方面有明顯的落差。根據現有資料顯示，以下是最常觀察到的落差：

修補：

68%

受影響的組織沒有有效的漏洞和修補程式管理程序，而且高度倚賴手動程序而非自動化修補，導致出現嚴重的缺口。製造業和重大基礎設施持續與老舊營運技術 (OT) 系統的維護和修補工作艱苦奮鬥。

缺少安全性作業工具：

大多數組織表示，由於缺少安全性工具或設定不當，而缺乏端對端安全性可見度，導致偵測和回應的效率降低。

60%

的組織表示，未使用 EDR[6] 工具，這是偵測和回應的基本技術。

60%

未投資在安全性資訊與事件管理 (SIEM) 技術，導致監視孤島、偵測端對端威脅的能力有限，以及安全性作業效率低落。自動化依然是 SOC 工具和流程的關鍵落差，迫使 SOC 人員投入數不清的時間來了解安全性遙測。

84%

受影響的組織未將其多雲端環境整合到其安全性作業工具中。

回應和復原程序：

76%

在 76% 受影響的組織中觀察到缺乏有效的回應計畫是焦點領域，不但阻礙了適當的組織危機準備工作，同時也對回應和復原的時間造成負面影響。

③ 資料防護有限

許多遭到入侵的組織缺乏適當的資料防護程序，導致嚴重影響復原時間以及恢復企業營運的能力。最常遇到的漏洞包括：

不可變的備份：

44%

的組織沒有不可變的備份可用於受影響的系統。資料也顯示，管理員對於像是 AD 等關鍵資產並沒有備份和復原計畫。

資料遺失防護：

攻擊者通常會透過利用組織的漏洞來找出入侵系統的方式，進而洩露關鍵資料以進行勒索、竊取智慧財產或獲利。

92%

受影響的組織並未實施有效的資料遺失防護控制來降低這些風險，進而導致關鍵資料遺失。

有些地區的勒索軟體有減少的趨勢，有些區域則增加

今年我們觀察到，北美及歐洲的應變小組收到通報的勒索軟體案件整體數量與前一年相比有下降的趨勢。同時，在拉丁美洲通報的案件數量則是增加。

這項觀察可解釋為，網路罪犯從觸動執法單位審查風險較高的地區，轉向較寬鬆的目標地區。由於 Microsoft 未觀察到全世界企業網路安全有明顯改善能夠解釋勒索軟體相關支援電話減少的原因，因此我們認為，最可能的原因是 2021 年和 2022 年執法活動增加了犯罪活動的成本，加上 2022 年發生的一些地緣政治事件，共同導致這樣的結果。

最普遍的 RaaS 活動之一，要算是稱為 REvil（又稱為 Sodinokibi) 的俄語犯罪集團，自 2019 年以來一直十分活躍。2021 年 10 月，REvil 的伺服器在國際執法行動 GoldDust 中遭到斷線。[7] 2022 年 1 月，俄羅斯逮捕了 14 名聲稱 REvil 的成員，並掃蕩了與其有關聯的 25 個據點。[8] 這是俄羅斯第一次對境內勒索軟體操作者採取反制行動。

雖然執法行動可能會降低 2022 年的攻擊頻率，但威脅執行者也可能會制定新策略，以避免未來遭逮。此外，俄羅斯和美國之間因俄羅斯入侵烏克蘭而關係緊張，此情況似乎導致俄羅斯與全球打擊勒索軟體行動才剛開始的合作停擺。在 REvil 遭逮捕之後經過短暫不穩定的時期，美國與俄羅斯在追捕勒索軟體行為體方面停止合作，這表示網路罪犯可能再次將俄羅斯視為安全的避風港。

展望未來，我們預測勒索軟體活動的步調將取決於幾項關鍵問題的結果：

1. 各國政府會採取行動阻止勒索軟體罪犯在其境內活動，或是試圖阻止行為體從境外從事活動？
2. 勒索軟體組織是否會改變戰略，不再需要勒索軟體，而訴諸勒索形式的攻擊？
3. 組織能否比罪犯利用漏洞更快將其 IT 營運現代化並轉型？
4. 在追索和追蹤贖金方面的進展是否會迫使贖金接收方改變戰略和協商？

雖然執法行動可能會降低 2022 年的攻擊頻率，但威脅執行者也可能會制定新策略，以避免未來遭逮。

2X

有些地區的勒索軟體攻擊減少，但要求的贖金卻是兩倍以上。

可付諸行動的見解

1. 聚焦整體安全性策略，因為所有勒索軟體系列都是利用相同的安全性弱點來影響網路。
2. 更新和維護安全基礎知識，以提高深度防禦基礎防護層級，並將安全性作業現代化。移向雲端可讓您更快偵測到威脅並且更快做出回應。

進一步資訊的連結

- 保護您的組織免受勒索軟體威脅 | Microsoft 安全性
- 7 種強化環境對抗入侵的方式 | Microsoft 安全性部落格（英文）
- 改善以 AI 為基礎的防禦能力，以瓦解人為操作的勒索軟體 | Microsoft 365 Defender 研究團隊
- Security Insider：探索最新的網路安全性洞察和更新 | Microsoft 安全性

網路犯罪即服務

網路犯罪即服務 (CaaS) 是全世界客戶所面臨的日益成長且不斷進化的威脅。Microsoft 數位犯罪部門 (DCU) 觀察到 CaaS 生態系統持續成長，且有越來越多線上服務促進各種網路犯罪，包括 BEC 和人為操作的勒索軟體。網路釣魚仍是慣用的攻擊手段，因為網路罪犯成功竊取並出售竊得的帳戶存取權，就能得到相當大的價值。

為了因應不斷擴大的 CaaS 市場，DCU 強化了偵聽系統，以在整個生態系統 (包括網際網路、深層網路、經過審查的論壇、[9] 專用網站、線上討論論壇及傳訊平台) 中偵測並找出 CaaS 交易。

網路罪犯現在會跨時區和語言協作，以取得特定結果。例如，一個由位在亞洲的個人所管理的 CaaS 網站可在歐洲維持營運，並且在非洲建立惡意帳戶。這些跨管轄區性質的營運帶來了複雜的執法挑戰。為了因應這種情況，DCU 將重心放在讓用於協助 CaaS 攻擊的惡意犯罪基礎結構停擺，並與世界各地的執法機關合作，讓罪犯伏法。

網路罪犯越來越常利用分析來達到最大的觸及率、範圍和獲利。就像合法企業一樣，CaaS 網站必須確保產品和服務的有效性，才能維持穩固的名譽。例如，CaaS 網站會例行自動存取遭入侵的帳戶，確保遭入侵的認證有效。當密碼被重設或漏洞被修補時，網路罪犯就會停止銷售特定帳戶。我們找到越來越多 CaaS 網站，為買方提供隨需驗證做為品質控管的程序。因此，買方對於 CaaS 網站銷售的有效帳戶和密碼有信心，同時還能減少 CaaS 商家在銷售前，遭竊的認證被修復而伴隨的潛在成本。

DCU 同時發現，CaaS 網站可讓買方選擇購買特定地理位置、指定線上服務提供者的遭入侵帳戶，尤其是鎖定個人、職業和產業為目標。經常訂購的帳戶主要是處理發票的專業人員或部門，例如財務長或「應收帳款」。同樣地，參與公共事業合約的產業也經常成為目標，因為透過公開招標流程而能夠取得的資訊量相當大。

DCU 對於 CaaS 的調查當中發現了許多重要的趨勢：

服務的數量和複雜性日益增加。

其中一個範例是網頁殼層的演進，這些通常包含用來自動發動網路釣魚攻擊的遭入侵 Web 伺服器。DCU 還發現，CaaS 轉銷商會透過專用的 Web 儀表板簡化網路釣魚套件或惡意軟體的上傳作業。CaaS 罵方隨後通常會嘗試透過儀表板向威脅執行者銷售其他服務，例如垃圾郵件服務，以及根據定義的屬性 (包括地理位置或職業) 製作的專用垃圾郵件收件者清單。在某些實例中，我們觀察到單一網頁殼層用於多項攻擊活動的情形，這可能表示，威脅執行者可能保持對遭入侵伺服器的持續存取。我們還發現，CaaS 生態系統中提供的匿名服務增加，以及有提供虛擬私人網路 (VPN) 和虛擬私人伺服器 (VPS) 帳戶。在大多數實例中，提供的 VPN/VPS 一開始是透過竊得的信用卡購買。CaaS 網站也提供了更多的遠端桌面通訊協定 (RDP)、安全殼層 (SSH) 和 cPanels，這些都會用作協調網路犯罪攻擊的平台。CaaS 商家使用適當的工具和指令碼來設定 RDP、SSH 和 cPanels，以促進各種類型的網路攻擊。

有越來越多同形字網域建立服務要求以加密貨幣付款。

同形字網域會利用與另一個字元看起來一模一樣或幾乎一模一樣的字元來假冒合法網域名稱。其目的是欺騙觀看者，讓他們以為同形字網域是真正的網域。這些網域是無處不在的威脅，也是發動大量網路犯罪的管道。CaaS 網站現在會銷售自訂的同形字網域名稱，讓買方能夠要求要假冒的特定公司和網域名稱。收到付款後，CaaS 商家會使用同形字產生器工具來選取網域名稱，然後註冊惡意同形字。這種服務的款項幾乎完全以加密貨幣支付。

2,750,000

次，這是 DCU 今年成功封鎖的網站註冊次數，因而得以領先打算利用它們來從事全球網路犯罪的犯罪行為體。

網路犯罪即服務

續

CaaS 賣方有越來越多遭入侵的認證可供購買。

使用遭入侵的認證就能在未經授權的情況下存取使用者帳戶，包括電子郵件訊息服務、企業檔案共用資源，以及商務用 OneDrive。如果管理員認證遭到入侵，未經授權的使用者就可以存取機密檔案、Azure 資源和公司使用者帳戶。在許多實例中，DCU 調查發現了跨多部伺服器使用未經授權的相同認證做為自動驗證認證的手段。此模式可能表示，遭到入侵的使用者可能是多次網路釣魚攻擊的受害者，或是有裝置惡意軟體能讓殭屍網路鍵盤側錄程式收集認證。

具有強化功能的 CaaS 服務和產品正不斷出現，以規避偵測。

一個 CaaS 賣方提供網路釣魚套件，並增加了專為規避偵測和預防系統所設計的幾層複雜性與匿名功能，一天可能只收費 $6 美元。服務提供了一系列的重新導向，會在允許流量進入下一層或網站之前進行檢查。其中一項執行了 90 多次指紋辨識裝置的檢查，包括是否為虛擬機器，並收集有關所使用的瀏覽器和硬體的詳細資料等。如果所有檢查都通過，流量救回傳送至用於網路釣魚登陸頁面。

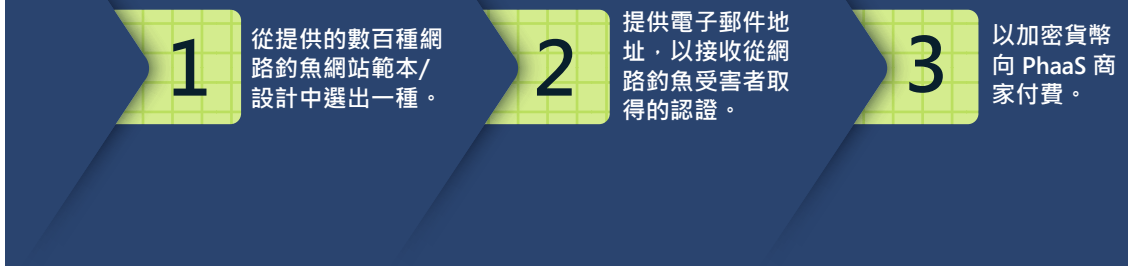
端對端網路犯罪服務正在出售受管理服務的訂閱。

一般來說，如果作業安全性不佳，從事線上犯罪的每一步都可能讓威脅執行者曝光。如果從多個 CaaS 網站購買服務，那麼曝光和遭逮的風險也會增加。DCU 觀察到一項令人擔憂的暗網趨勢，發現有越來越多提供軟體程式碼匿名化和網站文字通用化來減少曝光機率的服務。端對端網路犯罪訂閱服務提供者負責管理所有服務，並保證能進一步降低因訂閱 OCN 而曝光的風險。風險降低的結果使得這類端對端服務越來越受歡迎。

網路釣魚即服務 (PhaaS) 就是端對端網路犯罪服務的範例。PhaaS 是從稱為完全無法偵測到的服務 (FUD) 演變而來，並以訂閱模式提供。典型的 PhaaS 說法包括讓網路釣魚網站保持一個月有效。

DCU 還找到了以訂閱模式提供分散式拒絕服務 (DDoS) 的 CaaS 商家。此模式是將進行攻擊所需的殭屍網路的建立和維護工作外包給 CaaS 商家。每個 DDoS 訂閱客戶都會收到加密的服務來強化作業安全性，並享有一整年全天候的支援。DDoS 訂閱服務提供了不同的架構和攻擊方法，因此購買者只需選取要攻擊的資源，而賣方則在殭屍網路上提供各式各樣遭入侵裝置的存取權來發動攻擊。DDoS 訂閱的費用只要 $500 美元。

PhaaS，網路罪犯在單一訂閱內提供多項服務。一般而言，購買者只需執行三個動作：



完成這些步驟後，PhaaS 商家會建立內含三或四層重新導向和託管資源的服務，以鎖定特定使用者為目標。活動隨後展開，並獲取、驗證受害者的認證，然後傳送到購買者提供的電子郵件地址。許多 PhaaS 商家提供在公用區塊鏈上託管網路釣魚網站的服務以便進一步收費，如此一來，任何瀏覽器都可以存取這些網站，而且重新導向可將使用者指向分散式總帳上的資源。

DCU 持續致力於開發各種工具和技術來找出並瓦解 CaaS 網路罪犯。CaaS 服務的演進帶來了重大的挑戰，尤其是在瓦解加密貨幣支付方面。

使用加密貨幣的犯罪活動

隨著加密貨幣的使用成為主流，有越來越多犯罪分子利用加密貨幣來規避執法和反洗錢 (AML) 措施。這使得執法機關在追查和追溯支付給網路罪犯的加密貨幣時，面臨了更大的挑戰。

在過去四年中，全球區塊鏈解決方案支出成長約 340%，而新的加密貨幣錢包成長約 270%。截至 2022 年 7 月 28 日，全球有超過 8300 萬種專用電子錢包，而所有加密貨幣的總市值約為 $1.1 兆美元。[10]

資料來源：Twitter.com—@PeckShieldAlert (PeckShield 是一家位於中國的區塊鏈資安公司)。

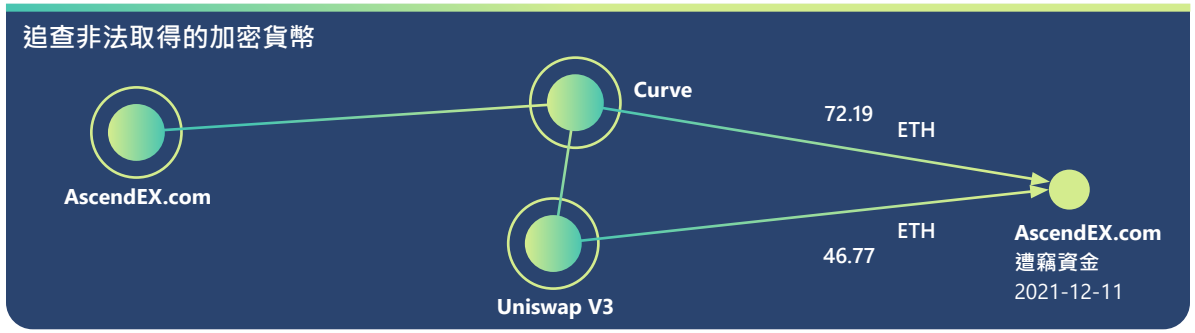
追查勒索軟體款項

勒索軟體是非法取得加密貨幣的最大來源之一。為了瓦解勒索軟體攻擊中使用的惡意技術基礎結構 (例如，2022 年 4 月瓦解 Zloader[11])，Microsoft 的 DCU 會追查罪犯電子錢包，以實現加密貨幣追蹤和復原功能。

DCU 調查人員觀察到，勒索軟體行為體不斷進化與受害者的通訊策略，以藏匿金錢的蹤跡。網路罪犯原本會在勒索信中包含比特幣位址。然而，這樣做很容易就能循線追溯到區塊鏈上的付款交易，因此勒索軟體行為體便停止包含電子錢包位址，而改為附加電子郵件地址或聊天網站的連結，藉此向受害者傳達贖金交付位址。某些行為體甚至為每一個受害者建立了專屬的網站和登入，防止安全性研究人員和執法機關偽裝成受害者來取得罪犯的電子錢包位址。儘管犯罪分子努力隱藏自己的蹤跡，但在執法機關與加密分析公司的合作之下，仍然可以透過追查區塊鏈上的動靜來找回部分贖金。

趨勢：DEX 非法所得洗錢

網路罪犯有一個關鍵問題是將加密貨幣轉換為法定貨幣。網路罪犯會利用幾種可能的途徑來進行轉兌，而每一種都會伴隨不同程度的風險。降低風險的方法之一，是透過分散式交易所 (DEX) 進行犯罪所得洗錢，後續再透過像是集中式交換所 (CEX)、點對點 (P2P) 和場外 (OTC) 交易所等可用的出金選項來兌現。DEX 是吸引人的洗錢地點，因為這些地方通常不會遵循 AML 措施。



透過使用加密貨幣調查工具 Chainalysis，Microsoft 的數位犯罪部門發現 AcendEX 駭客除了 Uniswap 之外，另外還在一家稱為 Curve 的較小型 DEX 上兌換竊得的資金。此圖說明團隊發現的洗錢路徑。每一個圓圈代表一個電子錢包叢集，而每一條線上的數字代表 Ethereum 轉匯的洗錢總金額。

2021 年 12 月，駭客攻擊了全球加密貨幣交易平台 AscendEx，並竊得其客戶所屬約 $7770 萬美元的加密貨幣。[12] AscendEx 聘請區塊鏈分析公司並聯絡其他 CEX，將收受遭竊資金的電子錢包列入黑名單。此外，傳送貨幣的位址在 Ethereum 區塊鏈總管工具 Etherscan 上也會有此標記，[13] 為了規避警示和黑名單，駭客於 2022 年 2 月 18 日在 Ethereum 上向全球最大的 DEX 之一 Uniswap 匯出了 $150 萬美元。[14]

DEX 採取更強硬的 AML 措施或許就能打擊其平台上的洗錢活動，並迫使網路罪犯使用其他模糊處理方法，如混幣或無授權交易。例如，Uniswap 近期宣布將開始使用黑名單來封鎖已知參與犯罪活動的電子錢包，禁止其在交易所進行交易。[15]

可付諸行動的見解

1. 如果您是網路犯罪的受害者，並且使用加密貨幣支付贖金給罪犯，請聯絡當地執法機關，他們可能可以協助追查和取回損失的資金。
2. 選擇 DEX 時，務必熟悉現行的 ALM 措施。

進一步資訊的連結

- 以硬體為主的威脅防禦措施來對抗日益複雜的挖礦劫持攻擊 | Microsoft 365 Defender 研究團隊

不斷演進的網路釣魚威脅環境

認證網路釣魚計劃不斷增加，並且持續對世界各地的使用者造成巨大的威脅，因為它們無差別地鎖定所有收件匣為目標。在我們的研究人員追查和防禦的威脅當中，網路釣魚攻擊的數量比所有其他威脅都多一級。

使用適用於 Office 的 Defender 提供的資料，就能幫助我們了解惡意電子郵件和遭入侵的身分識別活動。Azure Active Directory Identity Protection 還能透過遭入侵的身分識別事件警示提供更多資訊。使用 Defender for Cloud Apps，就能幫助我們了解遭入侵的身分識別資料存取事件，而 Microsoft 365 Defender (M365D) 提供了跨產品的相關性。橫向移動指標來自適用於端點的 Defender (攻擊行為警示和事件)、適用 Office 的 Defender (惡意電子郵件)，以及同樣來自 M365D (跨產品相關性)。

7 億 1 千萬
封每個星期遭到封鎖的網路釣魚電子郵件。

1 小時 12 分
當您落入網路釣魚電子郵件的陷阱成為受害者時，攻擊者存取您的私人資料所花的平均時間。[16]

1 小時 42 分
一旦裝置遭到入侵，攻擊者開始在您的企業網路內橫向移動的平均時間。[17]

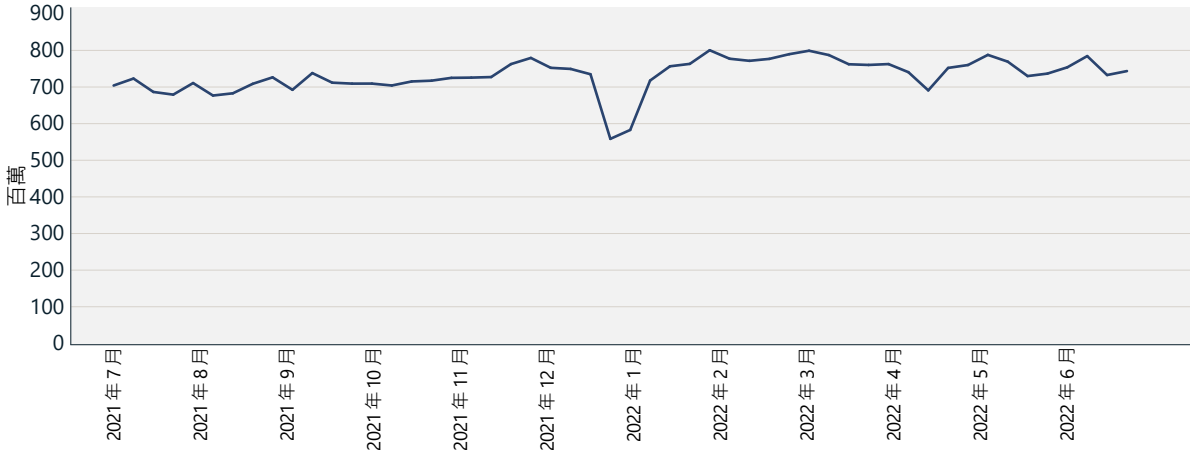
Microsoft 365 認證仍是攻擊者最搶手的帳戶類型之一。一旦登入認證遭到入侵，攻擊者就能登入與公司相關的電腦系統，促進利用惡意軟體和勒索軟體進行感染，藉由存取 SharePoint 檔案來竊取機密的公司資料和資訊，以及透過使用 Outlook 傳送其他惡意電子郵件等動作來繼續擴大網路釣魚。

除了鎖定更廣泛目標的活動，以及針對認證、捐款和個人資訊進行網路釣魚之外，攻擊者還會鎖定少數選定的企業勒索更大的贖金。對企業發動電子郵件網路釣魚攻擊以取財的行為，統稱為 BEC 攻擊。Microsoft 每個月偵測到數百萬封 BEC 電子郵件，相當於觀察到的所有網路釣魚電子郵件數量的 0.6%。2022 年 5 月發佈的 IC3[18] 報告指出，BEC 攻擊造成的損失有上升趨勢。

網路釣魚攻擊中使用的技術越來越複雜。為了回應反制對策，攻擊者調整新方法來施展其技術，並增加其託管宣傳行動基礎結構的方式和位置的複雜性。這意味著，組織必須定期重新評估實施安全性解決方案的策略，以封鎖惡意電子郵件，並加強對個別使用者帳戶的存取控制。

531,000
除了適用於 Office 的 Defender 所封鎖的 URL 之外，我們的數位犯罪部門還指示將託管於 Microsoft 外部的 531,000 個專用網路釣魚 URL 消滅殆盡。

偵測到的網路釣魚電子郵件



每個星期的網路釣魚偵測次數持續增加。去年的報告指出，12 月至 1 月次數減少是預期中的季節性下降。
資料來源：Exchange Online Protection 訊號。

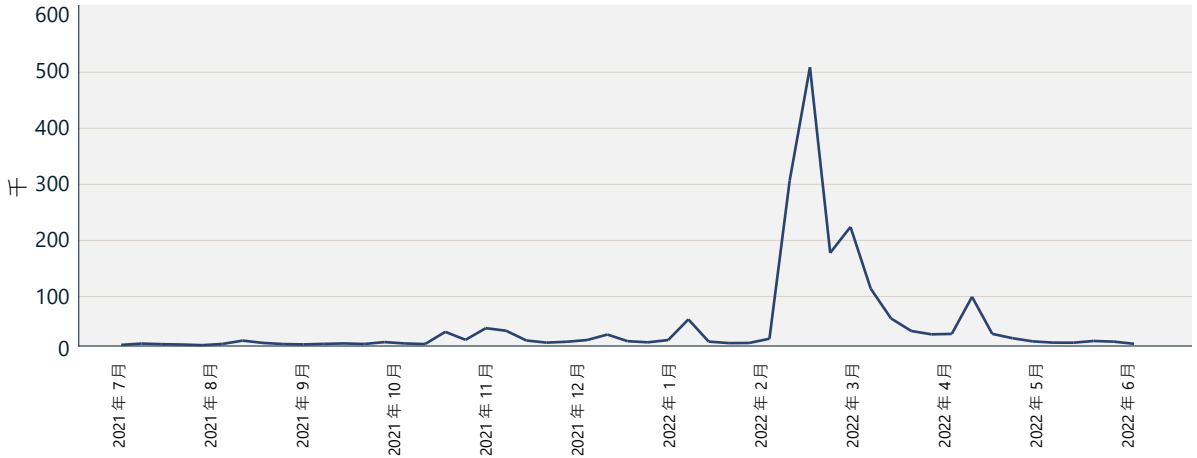
不斷演進的網路釣魚威脅環境

續

我們持續觀察到，網路釣魚電子郵件數量逐年穩定增加的趨勢。在 2020 年和 2021 年轉換為遠端工作的趨勢，使得網路釣魚攻擊大幅增加，目的是利用不斷變化的工作環境。網路釣魚操作者迅速採用新的電子郵件範本，並使用與世界大事 (如 COVID-19 全球疫情，以及與協作和生產力工具相關的主題，如 Google 雲端硬碟或 OneDrive 檔案共用) 相關的誘餌。雖然 COVID-19 主題已逐漸減少，但烏克蘭戰爭從 2022 年 3 月初開始成為了新的誘餌。我們的研究人員觀察到，假冒合法組織聲稱為了支援烏克蘭公民而進行比特幣和 Ethereum 等加密貨幣募款的電子郵件數量有了驚人的成長。

自 2022 年 2 月底烏克蘭開戰後，短短幾天就偵測到企業客戶之間包含 Ethereum 位址的網路釣魚電子郵件數量大幅增加。偵測到的總數在 3 月的第一週達到高峰，約有 50 萬封網路釣魚電子郵件包含 Ethereum 電子錢包位址。在開戰之前，偵測為網路釣魚的其他電子郵件中，Ethereum 電子錢包位址的數量明顯少了許多，每天平均為幾千封電子郵件。

包含 Ethereum 電子錢包位址的網路釣魚電子郵件



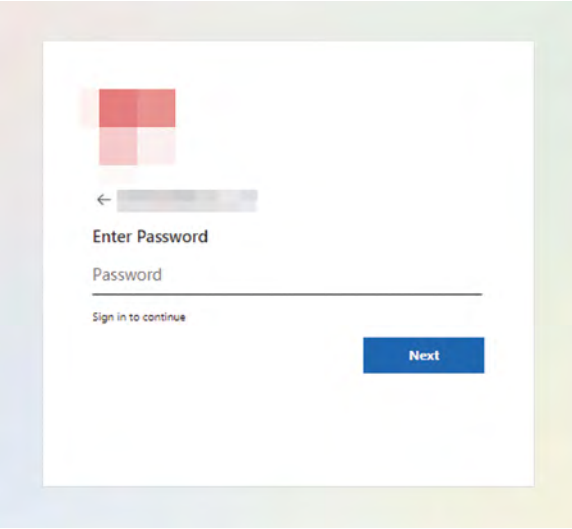
烏俄衝突展開之際，偵測為網路釣魚且包含 Ethereum 電子錢包位址的電子郵件總數便增加，並且在初次推送後逐漸減少。

網路釣魚者比以往更加依賴合法基礎結構來運作，因而使得網路釣魚活動增加，目的在於損害營運的各個層面，因此他們不需要購買、託管或自行操作。例如，惡意電子郵件可能來自遭入侵的寄件者帳戶。攻擊者受益於使用聲譽分數較高，而且比新建立的帳戶和網域更值得信任的電子郵件地址。在一些更進階的網路釣魚活動中，我們觀察到攻擊者偏好從 DMARC[19] 不當設定為「無動作」原則的網域傳送和詐騙，因為這項設定等於為電子郵件詐騙敞開大門。

大型網路釣魚作業通常使用雲端服務和雲端虛擬電腦 (VM) 來操控大規模的攻擊。攻擊者可以使用 SMTP 電子郵件中繼或雲端電子郵件基礎結構，將從 VM 部署和傳遞電子郵件的程序完全自動化，以受益於這些合法服務的高傳遞率及正面聲譽。如果允許透過這些雲端服務傳送惡意電子郵件，防禦端就必須依賴強大的電子郵件過濾功能來阻止電子郵件進入其環境。

Microsoft 帳戶一直是網路釣魚操作者的首要目標，大量假冒 Microsoft 365 登入頁面的網路釣魚登陸頁面就足以證明。例如，網路釣魚者會嘗試在其網路釣魚套件中產生針對收件者自訂的唯一 URL，藉此提供與 Microsoft 登入一致的體驗。此 URL 會指向為了獲取認證而開發的惡意網頁，但 URL 中的參數會包含特定收件者的電子郵件地址。一旦目標瀏覽至該頁面，網路釣魚套件就會預先填入使用者登入資料以及針對電子郵件收件者自訂的企業標誌，以仿造目標公司的自訂 Microsoft 365 登入頁面的外觀。

使用動態內容假冒 Microsoft 登入的網路釣魚頁面

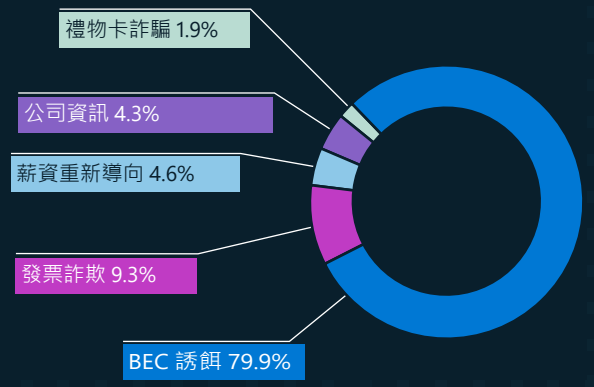


聚焦商務電子郵件入侵

網路罪犯正發展日益複雜的計劃和技術，以擊敗安全性設定並鎖定個人、企業和組織為目標。我們投入大量的資源，以進一步強化我們的 BEC 強制執行計劃做為因應。

BEC 是最昂貴的金融網路犯罪，估計 2021 年調整後損失為 $24 億美元，佔全球五大網際網路犯罪損失的 59% 以上。[20] 為了解問題的範圍，以及如何以最佳方式保護使用者對抗 BEC 攻擊，Microsoft 安全性研究人員一直在追查攻擊中最常使用的主題。

BEC 主題 (2022 年 1 月至 6 月)



BEC 主題 (依發生百分比排列)

BEC 趨勢

作為進入點，BEC 攻擊者通常會嘗試與潛在受害者展開對話，以建立密切關係。攻擊者假冒同事或業務熟人的身分，逐步引導對話走向金錢往來。我們追查作為 BEC 誘餌的簡介電子郵件，佔了近 80% 偵測到的 BEC 電子郵件。Microsoft 安全性研究人員過去一年找出的其他趨勢包括：

- 在 2022 年觀察到的 BEC 攻擊中，最常用的技術是詐騙 [21] 和假冒。[22]
- 對受害者造成最大財務損失的 BEC 子類型是發票詐欺 (根據我們的 BEC 活動調查中所看到的數量和要求金額)。
- 應付帳款報告和客戶連絡資訊等業務資訊竊取，讓攻擊者得以擬定出令人信服的發票詐欺行為。
- 大多數薪資重新導向請求都是從免費的電子郵件服務傳送，很少是來自遭入侵的帳戶。這些來源的電子郵件數量會在每月 1 日和 15 日 (最常見的付款日) 前後暴增。
- 儘管禮物卡詐騙是已知的詐騙手段，但在偵測到的 BEC 攻擊中僅佔了 1.9%。

可付諸行動的見解
對抗網路釣魚

為了減少組織暴露於網路釣魚攻擊的機會，建議 IT 管理員實施以下原則和功能：

1. 要求所有帳戶使用 MFA 以限制未經授權的存取。
2. 針對高權限的帳戶啟用條件式存取功能，以封鎖來自通常不會在您的組織產生硫量的國家 / 地區、區域和 IP 的存取。
3. 考慮對高階主管、涉及付款或採購活動的員工，以及其他權限帳戶使用實體安全性金鑰。
4. 強制使用支援如 Microsoft SmartScreen 這類服務的瀏覽器，以分析 URL 找出可疑的行為，並阻止存取已知的惡意網站。[23]
5. 使用機器學習為主的安全性解決方案，以便在電子郵件到達收件匣之前，隔離高度可疑的網路釣魚工具，並在沙箱內引爆 URL 和附件，例如適用於 Office 365 的 Microsoft Defender。[24]
6. 在整個組織中啟用假冒和詐騙防護功能。
7. 設定網域金鑰識別郵件 (DKIM) 和以網域為基礎的郵件驗證、報告與一致性 (DMARC) 行動原則，防止傳遞可能詐騙信譽良好寄件者的未經驗證電子郵件。
8. 稽核租用戶和使用者建立的允許規則，並移除寬鬆的網域和 IP 為主例外。這些規則通常優先順序較高，可能會讓已知的惡意電子郵件通過電子郵件篩選。
9. 定期執行網路釣魚模擬器，以衡量整個組織的潛在風險，並找出易受攻擊的使用者和進行教育。

進一步資訊的連結

- 從 Cookie 竊取到 BEC：攻擊者使用 AiTM 網路釣魚網站做為進入點來推進金融詐欺 | Microsoft 365 Defender 研究團，Microsoft 威脅情報中心 (MSTIC)

同形字欺騙

BEC 和網路釣魚是常見的社交工程戰術。社交工程在犯罪中扮演著相當重要的角色，負責取信於目標並說服目標與罪犯互動。

在實際商務中，商標用來保障對產品或服務來源的信任，而偽造產品則是濫用商標的行為。同樣地，在網路釣魚攻擊過程中，網路罪犯會以目標熟悉的連絡人名義，使用同形字來欺騙可能的受害者。

同形字是 BEC 中用於電子郵件通訊的網域名稱，其中字元會被看似一模一樣或幾乎一模一樣的字元取代，藉此欺騙目標。

BEC 嘗試中使用的同形字技術

BEC 通常分成兩個階段，第一個階段涉及入侵認證。這些類型的認證洩漏可能是網路釣魚攻擊或大型資料外洩所造成的結果。認證隨後會在暗網上出售或交易。

第二個階段是詐欺階段，攻擊者會使用遭到入侵的認證來利用同形字電子郵件網域從事複雜的社交工程。

BEC 攻擊的進展

技術	顯示同形字技術的網域 %
用 l 替換 I	25%
用 i 替換 l	12%
用 q 替換 g	7%
用 rn 替換 m	6%
用 .cam 替換 .com	6%
用 0 替換 o	5%
用 ll 替換 l	3%
用 ii 替換 i	2%
用 vv 替換 w	2%
用 l 替換 ll	2%
用 e 替換 a	2%
用 nn 替換 m	1%
用 ll 替換 I，用 l 替換 i	1%
用 o 替換 u	1%

2022 年 1 月至 7 月超過 1,700 個同形字網域的分析。雖然使用的同形字技術多達 170 種，但其中 75% 的網域只使用了 14 種技術。

同形字實際使用情況

與受害者認得的郵件網域看起來一模一樣的同形字網域在郵件提供者上註冊，且使用者名稱也一模一樣。接著從遭劫持的網域傳送一封遭劫持的電子郵件，當中包含新的付款指示。

罪犯利用開放原始碼情報和存取電子郵件往來內容，找出負責開立發票和付款的個人。然後他們會建立假冒傳送發票的個人電子郵件地址。此假冒內容包含一模一樣的使用者名稱和郵件網域，是真實寄件者的假分身。

攻擊者複製包含合法發票的電子郵件鏈結，然後更改發票以包含自己的銀行詳細資料。然後再次從同形假冒電子郵件將經過修改的這個新發票傳送給目標。由於內容看似合理，而且電子郵件看起來像真的一樣，因此目標通常會遵循詐欺指示。

可付諸行動的見解

1. 強制使用支援服務的瀏覽器來分析 URL，以找出可疑的行為，並阻止存取已知的惡意網站，例如 Safe Links 和 SmartScreen。[25]
2. 使用機器學習為主的安全性解決方案，以便在電子郵件到達收件匣之前，隔離高度可疑的網路釣魚工具，並在沙箱內引爆 URL 和附件。

進一步資訊的連結

- Internet Crime Complaint Center (IC3) | 商務電子郵件入侵：$430 億詐騙案
- 詐騙情報洞察— Office 365 | Microsoft Docs
- 假冒洞察— Office 365 | Microsoft Docs

自 Microsoft 早期協作以來的殭屍網路瓦解時程表

十多年來，DCU 一直努力主動阻止網路犯罪，促成了 26 個惡意軟體和國家級瓦解行動。隨著 DCU 團隊使用更先進的戰術和工具來阻斷這些不法活動，我們也看到網路罪犯不斷進化其手段，試圖保持領先。以下時程表顯示 DCU 瓦解的殭屍網路範例，以及 Microsoft 阻斷這些網路所採取的策略。

2008

Conficker 殭屍網路

描述：一種以 Windows 作業系統為目標的快速傳播蠕蟲，在公用網路中感染了數百萬台電腦和裝置；在全球造成網路中斷。

協作：成立 Conficker 工作小組，這是此類的第一個團隊。Microsoft 與全球 16 個組織合作，打擊殭屍。

Microsoft 回應：這個小組跨多個國際管轄區共同合作，並且成功瓦解了 Conficker。

2009

Waledac 殭屍網路

描述：使用美國網域的複雜垃圾郵件殭屍網路，它會收集電子郵件地址並散發垃圾郵件，感染了全球多達 90,000 台電腦。[26]

協作：成立另一個團隊，Microsoft 惡意軟體防護中心 (MMPC) 著重與學術人員密切合作。[27]

Microsoft 回應：Microsoft 使用 C2 的分層中斷方法，未經通知就截獲美國境內的網域，給了不良行為體意外一擊。[28] Microsoft 授與了近 280 個 Waledac 伺服器所使用網域的臨時擁有權。

2011

Microsoft 數位犯罪部門成立

協作：透過跨調查人員、律師及工程師之間的密切整合，專為打擊影響 Microsoft 生態系統的網路犯罪而設計。

Microsoft 方法：目標是更了解各種惡意軟體的技術層面，並將這些見解提供給 Microsoft 法務團隊來制定出有效的瓦解策略。

2013

Rustock 殭屍網路

描述：利用網際網路提供者做為主要 C2 的後門特洛伊木馬程式垃圾電子郵件機器人；專為銷售藥品所設計。

協作：Microsoft 與 Pfizer Pharmaceuticals 合作，以了解 Rustock 銷售的藥品，並與荷蘭執法機關的官員密切合作。[29]

Microsoft 回應：Microsoft 與美國法警和荷蘭執法機關合作，掃蕩了該國境內的 C2 伺服器。登記並封鎖所有未來的網域產生器演算法 (DGA)。

Sirefef/Zero Access 殭屍網路

描述：一種設計成將人們引導到危險網站，達到安裝惡意軟體或竊取個人資訊目的之廣告殭屍網路；受感染的電腦超過 200 萬台，每個月使廣告主花費超過 $270 萬美元；主要位於美國和西歐。

協作：與 FBI 和歐洲刑警組織的網路犯罪中心密切合作，共同破獲對等基礎結構。

Microsoft 回應：加入 Zero Access 網路，取代犯罪 C2 伺服器，並成功截獲下載伺服器網域。

2019

Trickbot 殭屍網路

描述：複雜的殭屍網路，其零散的基礎結構遍布全球，鎖定金融服務業為目標；入侵了 IoT 裝置。

協作：Microsoft 與金融服務資訊共用和分析中心 (FS-ISAC) 合作，共同打擊 Trickbot。[30]

Microsoft 回應：DCU 建置了一套系統來識別和追查殭屍基礎結構，並針對有效的網際網路提供者產生通知，同時將不同國家 / 地區的特殊法律納入考量。

2022

持續聚焦瓦解行動

描述：Microsoft 過去一年來，瓦解了七個威脅執行者的基礎架構，阻止他們散佈其他惡意軟體、控制受害者的電腦，並鎖定其他受害者。

協作：與網際網路服務提供者、政府機構、執法機關和私人產業合作，Microsoft 透過分享資訊來幫助全球超過 1700 萬個惡意軟體受害者進行修復工作。

展望未來

DCU 持續創新，並期待能運用其瓦解殭屍網路的經驗，進行超越惡意軟體的協調行動。我們需要有創意的工程、分享資訊、創新的法律理論，以及公私領域的夥伴關係，才能持續成功。

網路罪犯濫用基礎結構

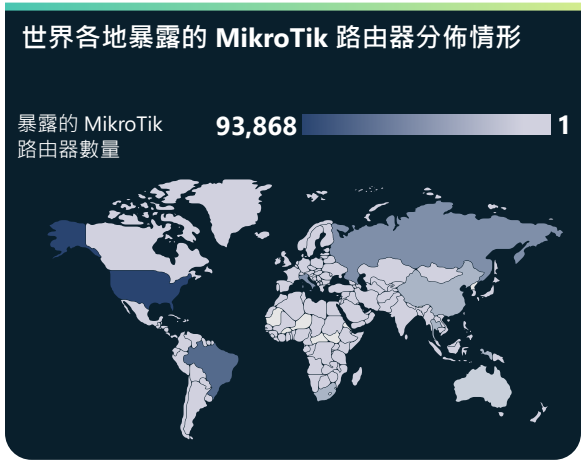
網際網路閘道作為犯罪命令和控制基礎結構

IoT 裝置逐漸成為使用普遍可見殭屍網路的網路罪犯青睞的目標。當路由器未經修補且直接暴露於網際網路時，威脅執行者就可能會濫用路由器來取得網路存取權、執行惡意攻擊，甚至支援其活動。

適用於 IoT 的 Microsoft Defender 團隊對各種設備進行研究，從舊版工業控制系統控制器到先進的 IoT 感應器。團隊會調查 IoT 和 OT 特有惡意軟體，並將資訊分享到共用入侵指標清單中。

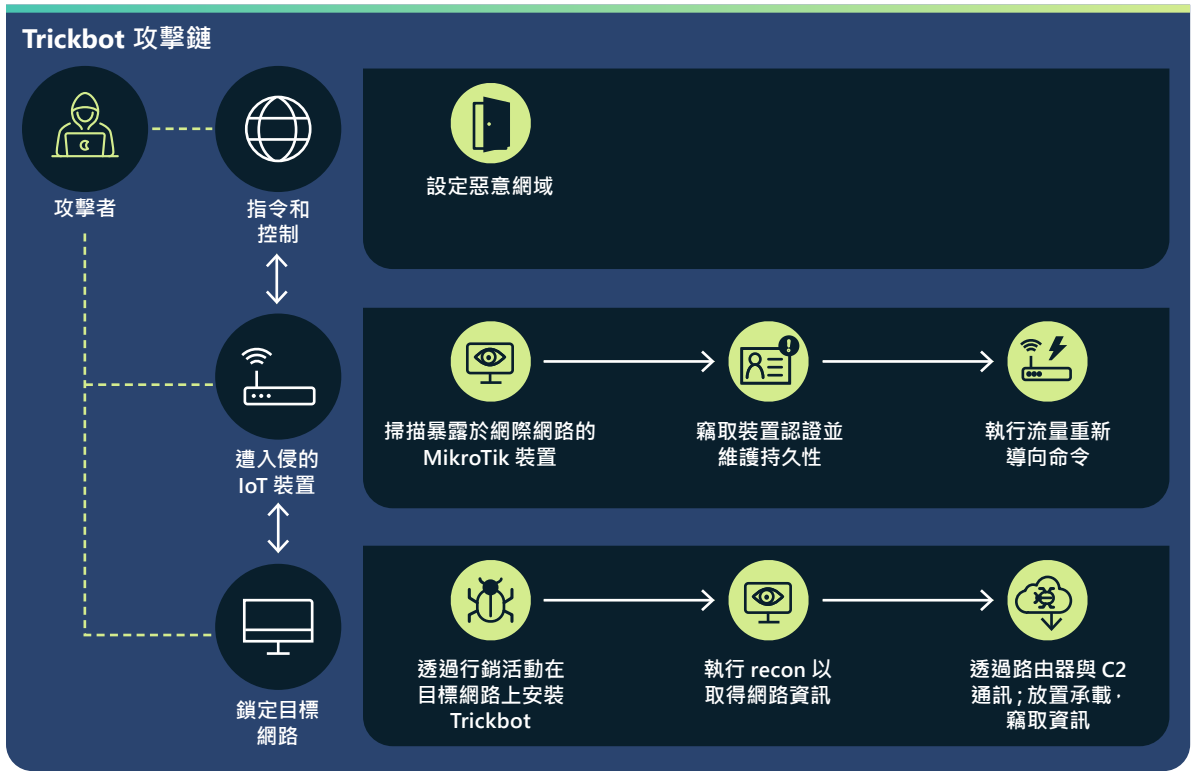
路由器是特別脆弱的攻擊媒介，因為它們在連接網際網路的住家和組織之間無所不在。MikroTik 路由器是世界各地居家和商務上普遍使用的路由器，我們一直在追查其活動，了解它們如何用於命令和控制 (C2)、網域名稱系統 (DNS) 攻擊，以及加密挖礦劫持。

更具體而言，我們識別出 Trickbot 操作者如何利用遭入侵的 MikroTik 路由器，並重新設定它們做為 C2 基礎結構的一部分。這些裝置受歡迎的程度使得 Trickbot 濫用的嚴重程度加劇，而其獨特的硬體和軟體讓威脅執行者得以規避傳統安全性措施、擴充其基礎結構，並且入侵更多裝置和網路。



暴露的路由器有著潛在漏洞遭利用的風險。

我們透過追查和分析包含安全殼層 (SSH) 命令的流量，觀察到攻擊者在取得裝置的合法認證後，會使用 MikroTik 路由器與 Trickbot 基礎結構進行通訊。這些認證可透過暴力破解攻擊、利用隨時可用的修補程式來入侵已知的漏洞，以及使用預設密碼來取得。一旦裝置遭到存取，攻擊者就會發出特定命令，將路由器中的兩個連接埠之間的流量重新導向，以在 Trickbot 所影響的裝置與 C2 之間建立通訊線路。



Trickbot 攻擊鏈，顯示使用 MikroTik IoT 裝置做為 C2 的 Proxy 伺服器。

我們將有關攻擊 MikroTik 裝置之各種方法的知識彙整在一起，不僅是 Trickbot 而已，還包括已知的常見漏洞和暴露風險 (CES)，並將這些知識納入適用 MikroTik 裝置的開放原始碼工具中，以便能夠擷取與這些裝置上的攻擊相關的鑑識成品。[31]

充當惡意軟體 C2 反向 Proxy 的裝置，並不是 Trickbot 和 MikroTik 路由器獨有的。我們與 Microsoft RiskQ 團隊協作，追溯到涉及的 C2，並透過觀察 SSL 憑證發現了同樣受到影響的 Ubiquiti 和 LigoWave 裝置。[32] 這明顯指出，IoT 裝置正成為國家級協調攻擊的有效環節，同時也是使用普遍可見殭屍網路之網路罪犯的熱門目標。

濫用 IoT 裝置的加密罪犯

閘道裝置對於威脅執行者來說，是越來越有價值的目標，因為已知漏洞的數量穩定地逐年增加。這些裝置會用於加密挖礦和其他類型的惡意活動。

隨著加密貨幣越來越受歡迎，許多個人和組織都會將路由器等裝置的運算能力和網路資源投入區塊鏈上進行的貨幣挖礦。不過，挖礦加密貨幣是既耗時又耗資源的過程，成功率也低。為了增加挖到貨幣的可能性，挖礦者會在分散式合作網路中彙集在一起，透過連線資源接收相對於他們成功挖到之代幣的一定比例的雜湊。

在過去一年，Microsoft 觀察到有越來越多的攻擊濫用路由器來重新導向加密貨幣挖礦工作。網路罪犯入侵連線到挖礦集區的路由器，並利用 DNS 毒害攻擊將挖礦流量重新導向至與其相關聯的 IP 位址，從而修改目標裝置的 DNS 設定。受影響的路由器會將錯誤的 IP 位址註冊到所指的網域名稱，以將挖礦資源（或雜湊）傳送至威脅執行者所使用的集區。這些集區可能會對與犯罪活動相關的匿名貨幣進行挖礦，或使用挖礦者所產生的合法雜湊來取得他們所挖到代幣的一定比例，進而獲得回報。

2021 年發現的已知漏洞當中，有超過一半都缺少修補程式，因此更新和保護公司與私人網路上的路由器一直是裝置擁有者和管理員的一大挑戰。

閘道裝置的 DNS 毒害攻擊會危害合法的挖礦活動，並將資源重新導向犯罪挖礦活動。

作為犯罪基礎結構的虛擬機器

普遍移向雲端的行動也包括網路罪犯在內，他們會利用網路釣魚或散佈惡意軟體認證竊取程式取得不知情受害者的私人資產。許多網路罪犯選擇將惡意基礎結構架設在雲端虛擬機器 (VM)、容器和微服務上。

一旦網路罪犯取得存取權，就可能發生一系列的事件來架設基礎結構，例如透過指令碼和自動化程式建立一系列的虛擬機器。這些指令碼式的自動化程序會用來發動惡意活動，包括大規模的電子郵件垃圾郵件攻擊、網路釣魚攻擊，以及裝載惡意內容的網頁。甚至還可能包括架設擴展的虛擬環境來執行加密貨幣挖礦，致使最終受害者在月底損失數十萬美元。

網路罪犯清楚知道，他們的惡意活動在被偵測到並遭到掃蕩之前，存留時間有限。因此，他們擴大了規模，現在會採取主動出擊的方式，並且隨時準備因應突發事件。目前觀察到，他們會提前準備遭到入侵的帳戶，並且監控其環境。一旦某一個帳戶被偵測到（使用數十萬台虛擬機器所設定），他們就會周遊到下一個帳戶（已利用指令碼備妥，可立即啟用），而且他們的惡意活動會繼續運作，幾乎不受干擾。

就像雲端基礎結構一樣，內部佈署基礎結構也可用於攻擊，方法是利用內部佈署使用者未察覺到的虛擬本機環境。這會需要初始存取點保持開放且可存取。網路罪犯同樣會濫用內部佈署私人資產來起始後續的雲端基礎結構鏈，架設的目的在於混淆其來源，以避開可疑基礎結構建立偵測。

可付諸行動的見解

1. 實施良好的網路檢疫，以及為員工提供網路安全訓練，指引他們避免成為社交工程攻擊的目標。
2. 透過大規模偵測定期進行自動化使用者活動異常檢查，協助減少這類攻擊的發生。
3. 更新及保護公司和私人網路上的路由器。

激進駭客是否持續存在？

雖然激進駭客不是新現象，但在烏克蘭戰爭中卻看到掀起了一波駭客志願軍潮，當中有一些是受政府指使，部署網路工具來破壞政治對手、組織，甚至國家的名譽或資產。

2022 年 2 月，烏克蘭政府號召世界各地的一般公民對俄羅斯發動網路攻擊，這些都隸屬於烏克蘭的 30 萬名「IT 大軍」。[33] 於此同時，既有的激進駭客團體（如 Anonymous、Ghostsec、Against the West、Belarusian Cyber Partisans 和 RaidForum2）也展開攻擊來支援烏克蘭。其他團體，包括一些 Conti 勒索軟體犯罪集團，則跟俄羅斯站在同一邊。[34]

在隨後的幾個月中，Anonymous 的活動非常高調、隨處可見。以該團體（或其附屬團體之一）的名義活動的駭客，讓數千個俄羅斯和白俄羅斯的網站暫時停擺、洩露數百 GB 竊得的資料、駭入了俄羅斯的電視頻道來播放親烏克蘭的內容，甚至提出願意支付比特幣給投降的俄羅斯坦克部隊。

公民駭客的崛起

社交媒體平台讓成千上萬名可能成為公民駭客的人能夠迅速組織和動員起來，他們得到指示發動容易進行的攻擊，像是 DDoS 攻擊。召集人利用 Twitter、Telegram 和私人論壇來召集駭客、組織行動，以及散發駭客指令手冊。

然而，這些駭客中，大多數可能僅具備有限的技能，即使按照指令行動也一樣。這暗示著兩種可能的未來情景：一種是有數百或數千名具有基礎技術能力的個人使用攻擊範本，在未來對目標發動協調或個別的激進駭客攻擊，另一種是烏克蘭的積極抗爭告終後，這些人便離開了激進駭客，至少在下一次政治或社會議題激發他們採取行動之前，不會再出現。

駭客的政治化

這種政治動員所帶來的更大風險，就是部署精通技術的駭客，他們可能會繼續對外國政府目標發動網路攻擊，以支援母國的優先事項，無論是自發性的行動，或是應政府要求的行動。

伊朗、中國和俄羅斯都已採用激進駭客做為養成者，以便招募進入該國的駭客組織。例如，親俄羅斯的駭客組織 Killnet 在 2022 年 4 月對捷克鐵路、區域機場和捷克的市民服務伺服器發動了 DDoS 攻擊，即使捷克並未直接參戰。[35] 於此同時，有些政府可能利用激進駭客來掩護傳統網路攻擊或惡意破壞活動，例如，伊朗對抗以色列的活動。

在越來越多 DDoS 攻擊與激進駭客有所關聯的環境中，科技業面臨了必須快速破解網站上正常和異常流量之間差異的挑戰。Microsoft 及其合作夥伴共同開發了一組工具，用來分辨惡意 DDoS 流量並追溯其來源。此外，Microsoft 的 Azure 平台還可找出平台上產生異常大量出埠流量的機器，並將其關閉。

抗議軟體的興起

抗議軟體的興起，是對烏俄戰爭的情緒反應直接造成的結果。某些開放原始碼軟體發展人員運用其軟體的普遍程度做為手段來發言或採取行動，以對抗逐漸展現的地緣政治局勢。其中包括桌面上或瀏覽器上出現的無害文字檔案，目的在於散播和平訊息，但也包括根據 IP 位址地理位置的目標式攻擊以及破壞行動，像是抹除硬碟。隨著其他全球事件逐漸展開，我們預期未來會再次看到抗議軟體出現。由於這些案例通常是備受尊敬的開放原始碼維護者利用自己的開放原始碼元件來發表個人聲明，因此目前並沒有防護措施可阻止這類變更在原始碼檔案套件中發生，使用者應持續關注可能的影響。

社交媒體平台讓成千上萬名可能成為公民駭客的人能夠組織和動員起來，他們得到指示發動容易進行的攻擊，像是 DDoS 攻擊。

可付諸行動的見解

1. 科技業必須共同合作，設計出一套回應此新威脅的應變措施。
2. 包括 Microsoft 在內的領先科技公司擁有工具可識別與 DDoS 攻擊相關的惡意流量，並停用負責的電腦。
3. 開放原始碼使用者應在地緣政治衝突期間，隨時保持高度警戒。

章節附註

1. https://www.reuters.com/business/energy/shell-re-routes-oil-supplies-after-cyberattack-german-logistics-firm-2022-02-01/
2. https://www.bleepingcomputer.com/news/security/greeces-public-postal-service-offline-due-to- ransomware-attack/
3. https://www.bleepingcomputer.com/news/security/costa-rica-s-public-health-agency-hit-by-hive-ransomware/; https://www.reuters.com/world/americas/cyber-attack-costa-rica-grows-more-agencies-hit-president-says-2022-05-16/
4. https://www.bleepingcomputer.com/news/security/spicejet-airline-passengers-stranded-after-ransomware-attack/
5. https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/
6. 端點偵測及回應。 https://www.microsoft.com/en-us/security/business/threat-protection/
7. https://www.washingtonpost.com/national-security/cyber-command-revil-ransomware/2021/11/03/528e03e6-3517-11ec-9bc4-86107e7b0ab1_story.html
8. https://www.bbc.com/news/technology-59998925
9. 審查論壇是一個線上論壇，會要求現有成員對新成員的加入表達意見。
10. https://www.statista.com/statistics/800426/worldwide-blockchain-solutions-spending/; https://www.blockchain.com/charts/my-wallet-n-users; https://coinmarketcap.com
11. https://blogs.microsoft.com/on-the-issues/2022/04/13/zloader-botnet-disrupted-malware-ukraine/
12. https://www.coindesk.com/business/2021/12/13/crypto-exchange-ascendex-hacked-losses-estimated-at-77m/ ; https://www.zdnet.com/article/after-77-million-hack-crypto-platform-ascendex-to-reimburse-customers/
13. https://etherscan.io/address/0x73326b6764187b7176ed3c00109ddc1e6264eb8b
14. https://finance.yahoo.com/news/ethereum-worth-over-1-5m-160249300.html
15. https://news.bitcoin.com/decentralized-finance-crypto-exchange-uniswap-starts-blocking-addresses-linked-to-blocked-activities/
16. 資料來源：適用於 Office 的 Defender (惡意電子郵件 / 遭入侵的身分識別活動)、Azure Active Directory Identity Protection (遭入侵的身分識別事件 / 警示)、Defender for Cloud Apps (遭入侵的身分識別資料存取事件) 和 M365D (跨產品相關性)。
17. 資料來源：適用於端點的 Defender (攻擊行為警示 / 事件)、適用於 Office 的 Defender (惡意電子郵件) 和 M365D (跨產品相關性)。
18. https://www.ic3.gov/Media/Y2022/PSA220504
19. 以網域為基礎的郵件驗證、報告與一致性：一種電子郵件驗證、原則和報告通訊協定，其設計在於讓電子郵件網域擁有者有能力保護自己的網域，防止未經授權的使用。
20. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
21. https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/learn-about-spoof-intelligence?view=o365-worldwide
22. https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/impersonation-insight?view=o365-worldwide
23. https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-smartscreen/microsoft-defender-smartscreen-overview
24. https://www.microsoft.com/en-us/security/business/siem-and-xdr/microsoft-defender-office-365
25. https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-smartscreen/microsoft-defender-smartscreen-overview
26. Microsoft Corporation v. John Does 1-27, et. al., No. 1:10CV156, (E.D.Va.Feb 22, 2010)。
27. 請參閱 Bowden, Mark. 蠕蟲：第一次數位世界大戰 (Worm: The First Digital World War)。Grove/Atlantic, Inc., Sep 27, 2011。
28. 具體而言，聯邦民事訴訟程序第 65 條中，允許當事人在以下情況尋求此類救濟：1) 若未予以救濟，當事人將遭受立即且無法彌補的傷害，以及 2) 當事人嘗試及時提供另一方通知。此外，法律要求採用平衡原則，平衡原則用於權衡被告的通知權利與對公眾的損害程度。
29. Microsoft Corporation v. John Does 1-11, et. al., No. 2:11cv222, (W.D.Wa.Feb 9, 2011)。
30. Microsoft Corp. v. Does, No. 1:20-cv-01171 (AJT/IDD), 2021 U.S. Dist.LEXIS 258143, at *1 (E.D.Va.Aug. 12, 2021)。
31. https://github.com/microsoft/routeros-scanner
32. RiskQ：遭入侵並利用做為惡意軟體 C2 反向 Proxy 的 Ubiquiti 裝置 | RiskIQ 社群版
33. https://www.theguardian.com/world/2022/mar/18/amateur-hackers-warned-against-joining-ukraines-it-army
34. https://therecord.media/russia-or-ukraine-hacking-groups-take-sides/
35. https://www.expats.cz/czech-news/article/pro-russian-hackers-target-czech-websites-in-a-series-of-attacks

國家威脅

國家級行為體發動的網路攻擊日益複雜，其目的在於避開偵測，並推進其策略性優先事項。

概觀

國家威脅

國家級行為體發動的網路攻擊日益複雜，其目的在於避開偵測，並推進其策略性優先事項。在烏克蘭的混合戰中網路武器部署的出現，正宣告著新的衝突時代來臨。

俄羅斯同樣以資訊勢力活動來支援其戰事，運用政治宣傳來影響俄羅斯、烏克蘭和全球的觀點。這一場首度的大規模混合衝突帶來了其他重要的教訓。首先，移向雲端可讓數位營運和資料的安全性受到最妥善的保護，包括網路空間和實體空間。俄羅斯最初的攻擊目標是使用 wiper 惡意軟體鎖定內部佈署服務，以及使用最早發射的飛彈之一攻擊實體資料中心。

烏克蘭的應變方式是迅速將工作負載和資料移到烏克蘭境外資料中心的超大規模雲端。其次，雲端中採用資料與先進 AI 和 ML 服務技術的網路威脅情報和端點防護措施的精進，幫助烏克蘭防禦俄羅斯的網路攻擊。

在其他地區，國家級行動體增加了活動，並且利用先進的自動化、雲端基礎結構和遠端存取技術來擴大攻擊的目標。能夠存取最終目標的企業 IT 供應鏈經常遭到攻擊。網路安全性檢疫變得更加重要，因為行為體會迅速入侵未修補的漏洞，使用複雜的暴力破解技術竊取認證，並且使用開放來源或合法軟體來混淆其活動。伊朗與俄羅斯一起使用包括勒索軟體在內的破壞性網路武器，做為其攻擊主力。

這些發展急需採用一致的全球架構，以優先處理人權和保護人們不受網路上魯莽國家的行為迫害。各國之間必須相互合作，共同實踐達成共識的負責任國家級行為規範與規則。

保衛烏克蘭：網路戰的早期教訓 — Microsoft 問題焦點（英文）

以重大基礎設施為目標的攻擊日益增加，尤其是 IT 部門、金融服務、交通運輸系統及通訊基礎設施。

深入了解，前往 p35

IT 供應鏈遭利用做為存取目標的閘道。

NOBELIUM

深入了解，前往 p36

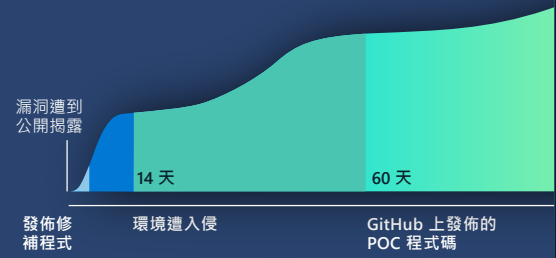
中國擴大全球目標，尤其是東南亞的小國，藉此獲得情報和競爭優勢。

深入了解，前往 p44

伊朗在政權交替後展現積極野心，將勒索軟體攻擊的範圍從區域對手擴大到美國和歐盟受害者，並且鎖定知名度高的美國重大基礎設施為目標。

深入了解，前往 p46

找出且迅速入侵未修補的漏洞已成為一大重要戰術。快速部署安全性修補程式是防禦的一大關鍵。



深入了解，前往 p39

北韓將目標鎖定在國防和航太公司、加密貨幣、新聞機構、脫北者及救援組織，以達到政權當局的目標：建構國防、提振經濟，以及確保國內穩定。

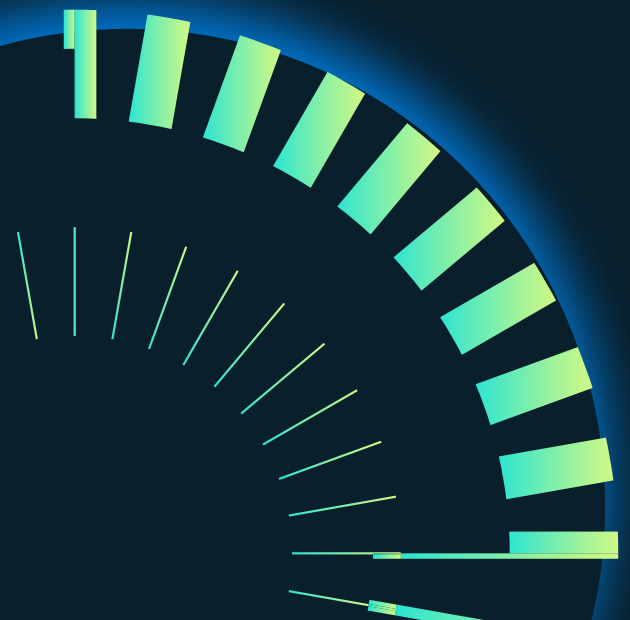
深入了解，前往 p49

網路傭兵威脅著網路世界的和平穩定，因為這個不斷成長的私有企業產業正著手開發並出售先進的工具、技術和服務，讓他們的客戶（通常是政府）能夠闖入網路和裝置。

深入了解，前往 p52

前言

在 2020 年和 2021 年的高調攻擊後，國家級威脅執行者耗費了大量資源來適應各組織為了抵禦複雜的威脅所實施的新安全防護措施。



就像企業組織一樣，敵手開始利用自動化、雲端基礎結構和遠端存取技術的進步來擴大其攻擊範圍，以鎖定更廣泛的目標。這些戰術性調整導致新方法出現，以及針對企業供應鏈的大規模攻擊發生。隨著行為體發展出新方式來迅速入侵未修補的漏洞、擴展技術來入侵企業網路，並且使用開放來源或合法軟體來混淆其活動，IT 安全性檢疫也變得更加重要。新的攻擊技術提供了更難偵測的新媒介來取得目標網路的存取權。最後，隨著戰時的實體攻擊提升，我們看到了網路攻擊成為軍事行動中的要角。

烏克蘭衝突提供了彌足珍貴的範例，說明了網路攻擊如何演變，在地面發生軍事衝突的同時對全世界造成衝擊。電力系統、電信系統、媒體級其他重大基礎設施全都成為實體攻擊和網路攻擊的目標。網路入侵嘗試常被視為間諜活動和資訊洩密活動的一部分，現已成為混合戰中的焦點，目的在於對重大基礎設施系統發動破壞性的 wiper 惡意軟體攻擊。將這些系統的安全性連接到雲端，就能進行提早偵測和阻斷可能的破壞性攻擊。[1]

在重大網路事件中首次有利用機器學習的行為偵測使用已知的攻擊模式，在事先不知道基礎惡意軟體的情況下，成功找出並阻止進一步攻擊，而人類甚至還未察覺到這些威脅。我們也認可與保護這些系統的防禦者即時分享威脅情報的價值，提供重要的資訊讓他們得以預測和防禦主動攻擊。

世界各地的國家級威脅執行者繼續以新舊方式擴展其活動。中國、北韓、伊朗和俄羅斯全都鎖定 Microsoft 客戶發動攻擊。隨著行為體將焦點轉移到可做為多個組織的存取點的上游服務，IT 服務供應鏈也成為常見的目標。我們預期行為體會繼續利用企業供應鏈中的信任關係，強調全面實施驗證規則、認真修補，以及遠端存取基礎結構的帳戶配置的重要性，並且經常稽核合作夥伴關係以確保真實性。

國家級行為體 (就像勒索軟體和犯罪份子) 已轉向以設定不當或未修補的企業系統 (VPN/VPS 基礎結構、內部佈署伺服器、協力廠商軟體) 為目標來因應曝光率增加的情況，以進行離地攻擊。許多人增加使用商品惡意軟體和開放原始碼 red 團隊工具來混淆其惡意活動。

因此，透過優先修補、啟用防篡改功能、使用 RiskIQ 等受攻擊面管理工具從外部查看受攻擊面，以及在整個企業中啟用多因素驗證，來維護強大的 IT 安全檢疫基準，已成為主動底綠許多複雜行為體的基準基礎知識。

國家級行為體也增加了使用勒索軟體做為攻擊戰術，經常在攻擊中重複使用該犯罪生態系統所建立的勒索惡意軟體。我們看到了伊朗與北韓兩國為主的行為體，利用商品勒索軟體工具破壞區域對手境內的目標系統，通常包括重大基礎設施。最後，我們看到了日益增加的網路傭兵威脅，他們開發和出售工具、技術和服務來擴大入侵易受攻擊的第三方解決方案。國家級行為體的公級複雜性和敏捷性將持續逐年進化。組織必須獲悉這些行為體的便化以便因應，同時在防禦上不斷進化。

John Lambert
Microsoft 威脅情報中心傑出工程師暨企業副總裁

國家級資料的背景

國家威脅是源自特定國家 / 地區的網路威脅活動，其明顯意圖是促進國家民族利益。國家級行為體代表著我們客戶面臨的最先進且持續的許多威脅，包括智慧財產權竊取、間諜活動、監視、認證竊取、破壞性攻擊等。

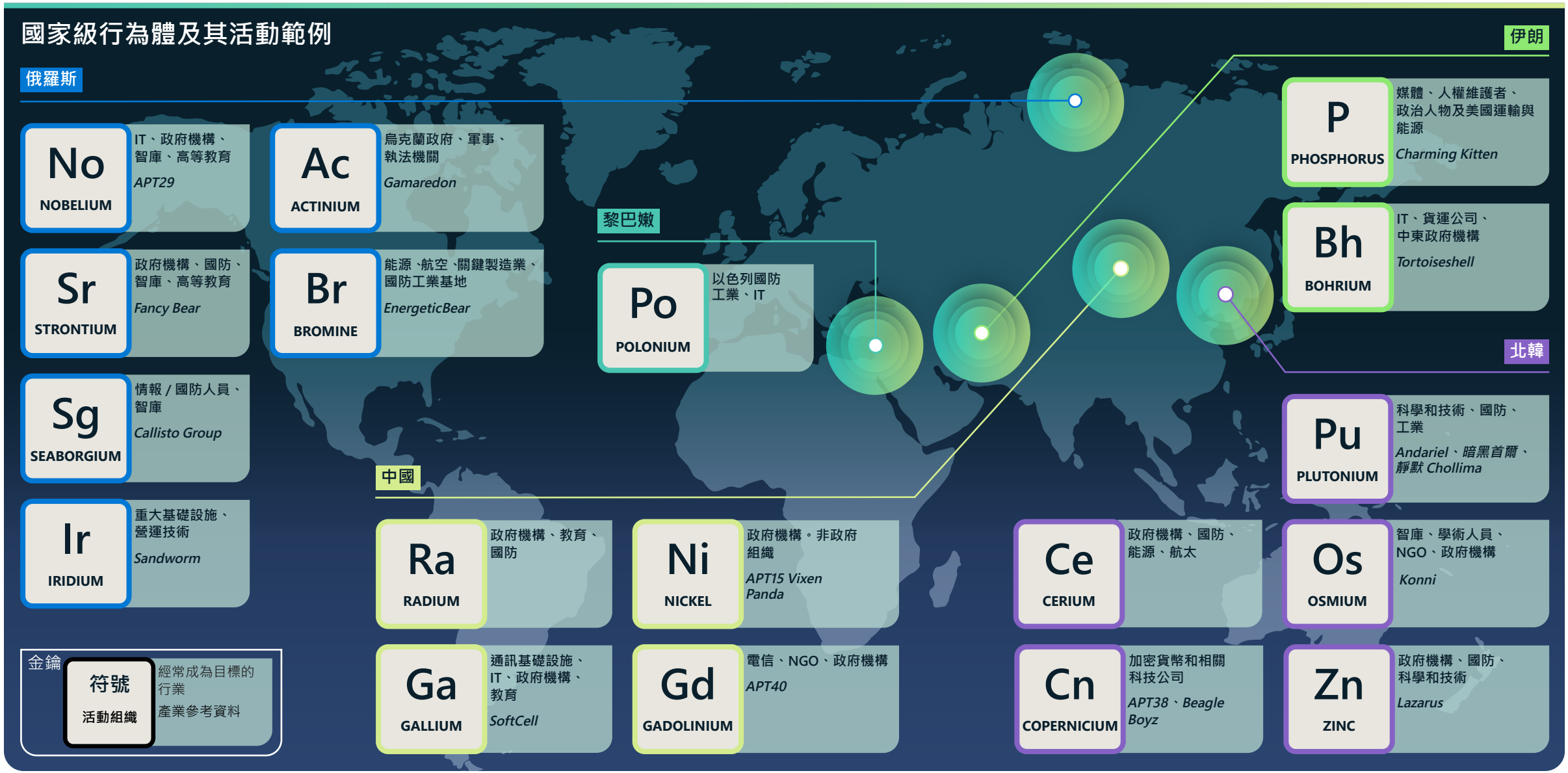
我們投入大量資源來探索、了解和反制這些威脅。當組織或個人帳戶持有者遭到觀察到的國家活動鎖定或入侵時，Microsoft 就會以國家通知 (NSN) 的形式直接向客戶發出警示，包括調查該活動所需的資訊。自 2018 年開始以來，截至 2022 年 6 月我們已發送了超過 67,000 則 NSN。

本章中呈現的 Microsoft NSN 警示資料提供了可衡量活動的視角。圖表中顯示的國家活動層級是根據 Microsoft 對客戶發出的 NSN 數量，用以回應偵測到至少鎖定客戶組織中一個帳戶為目標或進行入侵的國家級行為體。

我們在本報告中納入其威脅組織的四個主要國家為俄羅斯、中國、伊朗和北韓。這些代表過去一年來，最常觀察到鎖定 Microsoft 客戶為目標的來源國家。報告中還包括我們對於來自黎巴嫩和網路傭兵的威脅組織，或可雇用的民間攻擊行為體的觀察。

Microsoft 依化學元素名稱 (例如 NOBELIUM) 來識別國家級組織，下一頁僅顯示了其中一部分。我們使用 DEV-#### 名稱做為不明、新興或發展中威脅活動群集的臨時名稱，讓我們得以將他們做為一組獨特的資訊加以追查，直到我們對於掌握到的活動背後行為體來源或身分識別有高度信心。

一旦符合準則，DEV 就會轉換為具名行為體或與現有行為體合併。在本章中，我們引用了國家和 DEV 組織的範例，以提供更深入的角度來了解攻擊目標、技術和動機分析。雖然這些組織中有許多是使用與網路罪犯相同的工具，但是它們有著獨特的威脅，採取定製惡意軟體的形式、具備探索和利用零時差漏洞的能力，而且逍遙法外。


國家級行為體及其活動範例
俄羅斯
No
NOBELIUM
IT、政府機構、智庫、高等教育
APT29
Ac
ACTINIUM
烏克蘭政府、軍事、執法機關
Gamaredon
Sr
STRONTIUM
政府機構、國防、智庫、高等教育
Fancy Bear
Br
BROMINE
能源、航空、關鍵製造業、國防工業基地
EnergeticBear
Sg
SEABORGIUM
情報 / 國防人員、智庫
Callisto Group
Ir
IRIDIUM
重大基礎設施、營運技術
Sandworm
黎巴嫩
Po
POLONIUM
以色列國防工業、IT
伊朗
P
PHOSPHORUS
媒體、人權維護者、政治人物及美國運輸與能源
Charming Kitten
Bh
BOHRIUM
IT、貨運公司、中東政府機構
Tortoiseshell
北韓
Pu
PLUTONIUM
科學和技術、國防、工業
Andariel、暗黑首爾、靜默 Chollima
中國
Ra
RADIUM
政府機構、教育、國防
Ni
NICKEL
政府機構。非政府組織
APT15 Vixen Panda
Ce
CERIUM
政府機構、國防、能源、航太
Os
OSMIUM
智庫、學術人員、NGO、政府機構
Konni
Ga
GALLIUM
通訊基礎設施、IT、政府機構、教育
SoftCell
Gd
GADOLINIUM
電信、NGO、政府機構
APT40
Cn
COPERNICIUM
加密貨幣和相關科技公司
APT38、Beagle Boyz
Zn
ZINC
政府機構、國防、科學和技術
Lazarus
金鑰
符號
活動組織
經常成為目標的行業
產業參考資料

不斷演進的威脅環境

Microsoft 肩負追查國家級行為體活動，並且在我們發現客戶成為目標或遭到入侵時通知客戶的任務，而這正是我們根深蒂固的使命，矢志保護客戶不受攻擊。

這項通知是我們承諾通知客戶的關鍵環節，讓客戶得知我們的安全性產品防護是否成功阻止了觀察到的攻擊，或是攻擊是否因未知的安全性弱點而持續有效。長時間追查通知有助於 Microsoft 找出個別行為體不斷進化的威脅趨勢，並且聚焦產品防護，以主動消弭我們整體雲端服務中對客戶的威脅。

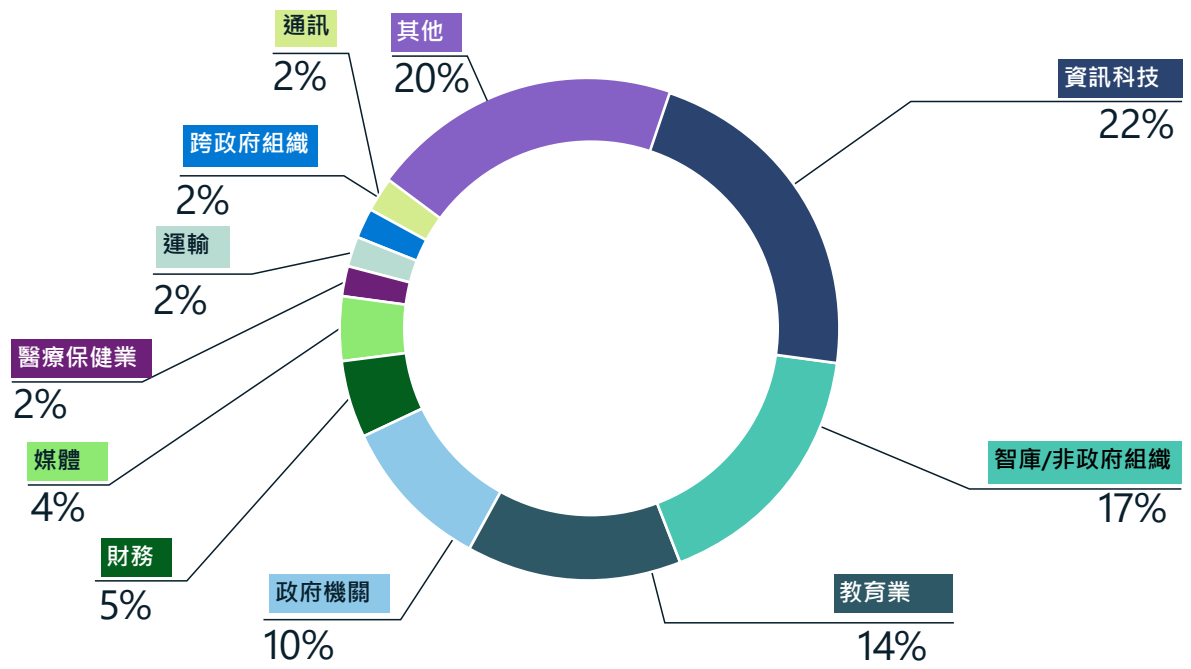
這個追查過程還能讓我們分享有關我們所見所聞的資料與見解。追查這些行為體並循線跟蹤其攻擊的分析師，需依賴各種技術指標和地緣政治專業知識相互結合來了解行為體的動機，進而結合技術和全球背景成為新的見解。這項精心策劃的行動提供了獨特的角度來深入了解國家級網路行為體的優先事項，以及他們的動機如何反映背後雇用國家的政治、軍事和經濟優先事項。

過去一年的政治發展在全世界塑造出了國家贊助的威脅組織的優先事項和風險承受能力。隨著地緣政治關係分崩離析，鷹派在某些國家取得了更多控制權，網路行為體也變得更加膽大而積極。例如：

- 俄羅斯持續不斷鎖定烏克蘭政府和該國重大基礎設施為目標，與其地面軍事行動相輔相成。[2]
- 伊朗積極尋求管道來進入美國重大基礎設施，例如港務當局。
- 北韓繼續進行從金融和科技公司竊取加密貨幣的活動。
- 中國擴大了其全球網路間諜活動。

雖然國家級行為體可能技術精熟，並且會運用各式各樣的戰術，但他們的攻擊也時常遭遇良好的網路檢疫而受阻。其中許多行為體依賴相對低技術的手段（如魚叉式網路釣魚電子郵件）來提供複雜的惡意軟體，而非投資於發展客製化的攻擊，或使用目標式社交工程來達到其目標。

國家級行為體鎖定目標的產業別



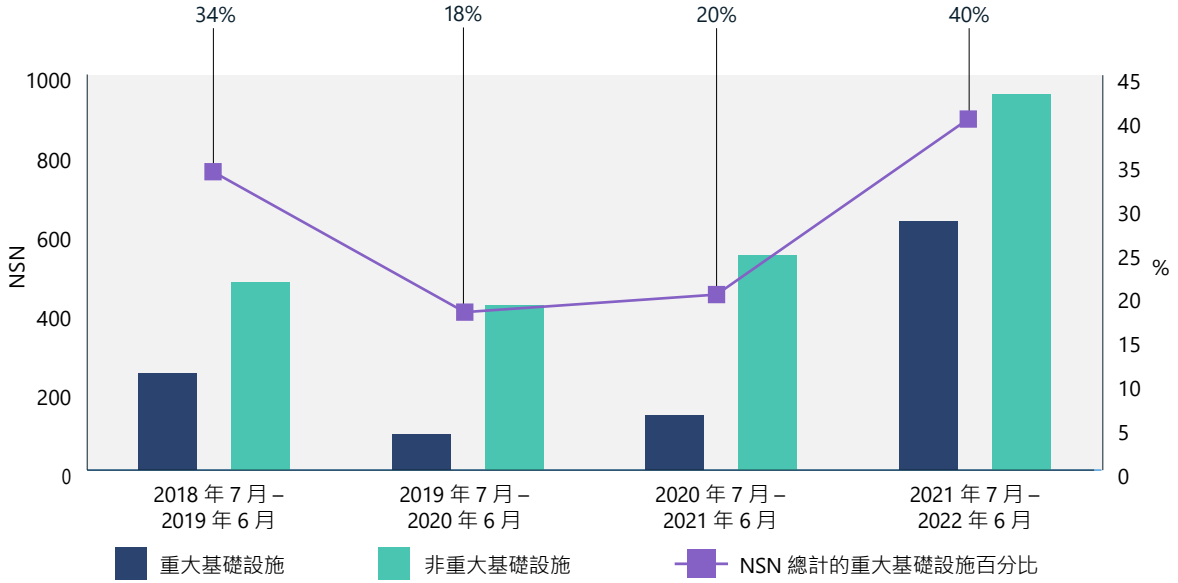
國家級組織會鎖定各種產業為目標。俄羅斯和伊朗國家級行為體就鎖定 IT 業為目標，做為接觸 IT 公司客戶的手段。智庫、非政府組織 (NGO)、大專院校及政府機構仍是國家級行為體的其他常見目標。

國家級行為體有著各種不同的目標，因此可能會鎖定特定的組織或個人團體為目標。過去一年的供應鏈攻擊增加，尤其是 IT 公司更顯著。透過入侵 IT 服務提供者，威脅執行者通常就能透過與管理連線系統的公司之間的信任關係到達其原始目標，或是可能藉由在一次攻擊中入侵數百個下游客戶，來發動更大規模的攻擊。在 IT 部門之後，最常成為目標的實體就是智庫、附屬於大專院校的學術人員，以及政府官員。這些是理想的「脆弱目標」，能讓間諜活動用來收集有關地緣政治議題的情報。

不斷演進的威脅環境

續

重大基礎設施趨勢

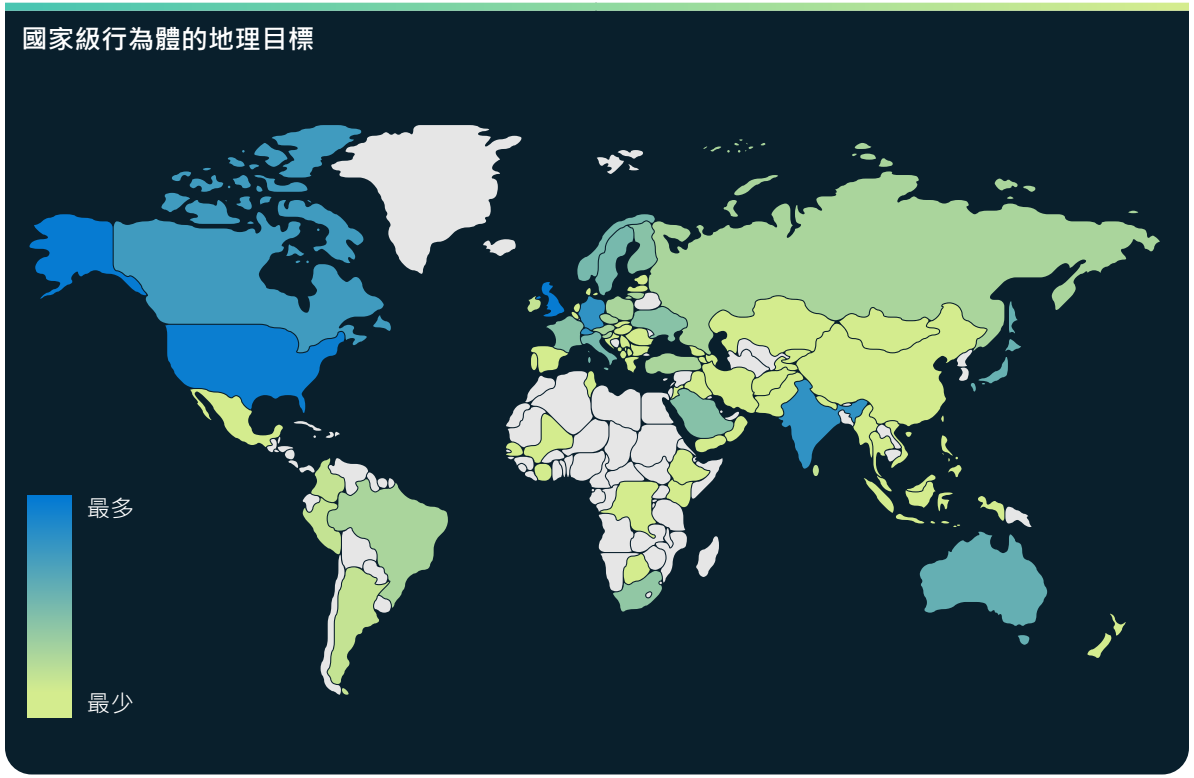


過去一年以來，國家級行為體鎖定重大基礎設施為目標的情況增加[3]，其中行為體將重點放在 IT 領域、金融服務、交通運輸系統及通訊基礎設施的公司。

「在烏克蘭遭到入侵之前，政府認為將資料保留在國內才能保障其安全。入侵發生之後，將資料遷移到雲端並移往境外，現在已是復原計劃和善治的一部分。」

Cristin Flynn Goodwin，
法律副總顧問，客戶安全和信任部門

國家級行為體的地理目標



過去一年，國家級組織的網路目標遍及全球，其中尤其著重在美國和英國企業。根據我們的 NSN 資料顯示，位於以色列、阿拉伯聯合大公國、德國、印度、瑞士和日本的組織也都是最常遭到鎖定的目標。

可付諸行動的見解

1. 找出可能合乎國家級組織的策略優先事項的潛在高價值資料目標、存在風險的技術、資訊及業務營運，並加以保護。
2. 實施雲端防護措施，以針對網路大規模提供已知和新型威脅的辨識能力和緩解措施。

IT 供應鏈做為數位生態系統的閘道

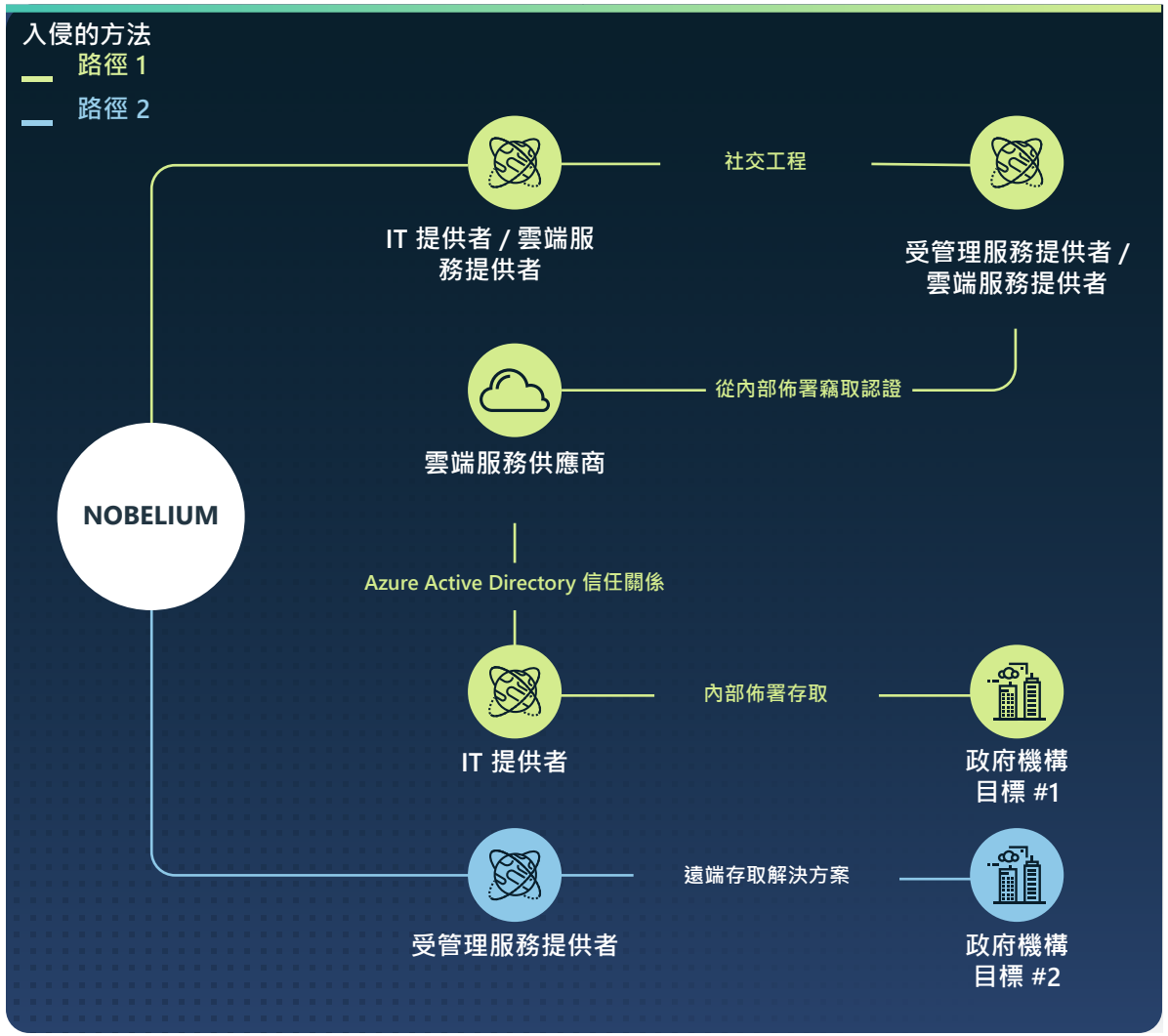
鎖定 IT 服務提供者為目標的國家可能會讓威脅執行者利用賦予這些供應鏈提供者的信任和存取權，入侵其他感興趣的組織。在過去一年，國家級網路威脅組織鎖定 IT 服務提供者為目標來攻擊第三方目標，並且得以接觸到政府、政策和重大基礎設施產業的下游客戶。

IT 服務提供者是吸引人的中間目標，因為它們服務的數百名直接客戶和數千名間接客戶是外國情報單位高度關注的對象。如果遭到入侵，這些公司享有的例行商業做法和委派的系統管理權限，都可能讓惡意行為體得以存取和操控 IT 服務提供者用戶端網路，而不會立即觸發警示。

在過去一年，NOBELIUM 企圖入侵和利用雲端解決方案和其他受管理服務提供者的權限帳戶，試圖鎖定下游存取權為目標以進一步接觸美國和歐洲政府與政策客戶。

NOBELIUM 展示了如何利用「入侵一個目標進而擴大入侵多個目標」方法對付認定的地緣政治敵手。過去一年以來，威脅行為體同時尋求第三方和直接入侵北大西洋公約組織 (NATO) 成員國境內的敏感組織，俄羅斯政府將他們視為生存上的威脅。在 2021 年 7 月到 2022 年 6 月初之間，Microsoft 收到客戶回報俄羅斯針對線上服務客戶的威脅活動通知中，NATO 成員國境內的 IT 產業公司就佔了 48%，很可能是中間存取點。整體來說，同一期間有關俄羅斯威脅活動的通知中，NATO 成員國境內的客戶就佔了 90%，主要為 IT、智庫和非政府組織 (NGO)，以及政府部門，這也暗示著尋求多種手段來初步接觸這些目標的策略。

從利用軟體供應鏈轉向利用 IT 服務供應鏈的趨勢持續進行中，鎖定了雲端解決方案和受管理服務提供者為目標以進一步接觸下游客戶。



此圖描述 NOBELIUM 採取多媒介方法入侵其最終目標，以及沿途對其他受害者的附帶破壞。除了上述行為之外，NOBELIUM 還對涉及的實體發動了密碼噴霧和網路釣魚攻擊，甚至鎖定了至少一名政府機構員工的個人帳戶為目標，做為另一個可能的入侵途徑。

IT 供應鏈做為數位生態系統的閘道

續

這一整年中，Microsoft 威脅情報中心 (MSTIC) 偵測到越來越多入侵 IT 公司的伊朗國家級和伊朗同夥行為體。在許多案例中偵測到行為體竊取登入認證來取得下游客戶的存取權，以達到各種目標，從收集情報到報復性的破壞攻擊等。

- 在 2021 年 7 月和 8 月，DEV-0228 入侵了一家以色列商務軟體提供者，並於隨後用來入侵以色列國防、能源和法務部門的下游客戶。[4]
- 從 2021 年 8 月到 9 月，Microsoft 偵測到鎖定印度境內 IT 公司為目標的伊朗國家級行為體激增。由於缺乏促使這股轉向的緊急地緣政治問題，因而意味著這個目標鎖定行動目的為間接存取印度境外的子公司和客戶。
- 在 2022 年 1 月，我們評估為與伊朗政府關係密切的組織 DEV-0198 入侵了一家以色列雲端解決方案提供者。Microsoft 評估此行為體很可能利用了提供者遭入侵的認證來進行驗證，而得以進入以色列物流公司。MSTIC 觀察到，當月稍後同一行為體試圖對該物流公司發動破壞性網路攻擊。
- 2022 年 4 月，我們評估與伊朗國家組織在 IT 供應鏈技術上密切合作、位於黎巴嫩的組織 POLONIUM，入侵了另一家以色列 IT 公司，進而得以進入以色列國防和法務組織。[5]

過去一年的活動顯示，像 NOBELIUM 和 DEV-0228 這樣的威脅行為體，他們比組織本身更了解組織的信任關係樣貌。這種日益增加的威脅，表示組織更加需要了解和強化其數位資產的邊界和進入點。同時也突顯出 IT 服務提供者嚴格監控自身網路安全狀況的重要性。例如，組織應實施多因素驗證和條件式存取原則，使惡意行為體更難擷取到權限帳戶或散播到整個網路。

徹底審查並稽核合作夥伴關係，有助於盡可能減少您組織和上游提供者之間任何不必要的權限，並且立即移除任何看似陌生關係的存取權。增加對活動記錄的熟悉程度並檢閱可用的活動，就能更容易發現可能觸動進一步調查的異常狀況。

> 鎖定第三方為目標的國家可能會讓他們得以利用供應鏈中的信任和存取權來入侵敏感組織。

可付諸行動的見解

1. 審查並稽核上游和下游服務提供者關係及委派的權限存取，以盡可能減少不必要的權限。移除任何看似陌生或未經過稽核的合作夥伴關係的存取權。[6]
2. 針對遠端存取基礎結構和虛擬私人網路 (VPN) 啟用記錄並審核所有驗證活動，並且聚焦在設定單因素驗證的帳戶，以確認真實性並調查異常活動。
3. 針對所有帳戶啟用 MFA（包括服務帳戶），並確保對所有遠端連線強制執行 MFA。
4. 使用無密碼解決方案保護帳戶的安全。[7]

進一步資訊的連結

- NOBELIUM 鎖定委派的系統管理權限為目標以促進規模更大的攻擊 | Microsoft 威脅情報中心 (MSTIC)
- 伊朗鎖定 IT 部門為目標的趨勢上升 | Microsoft 威脅情報中心 (MSTIC)，Microsoft 數位安全部門
- 公開鎖定以色列組織為目標的 POLONIUM 活動和基礎結構 | Microsoft 威脅情報中心 (MSTIC)

快速漏洞攻擊

隨著組織加強其網路安全性態勢，國家級行為體也做出了回應，他們尋求全新、獨特的戰術來發動攻擊和規避偵測。識別和利用先前已知的漏洞（也稱為零時差漏洞），就是這波行動當中的關鍵戰術。

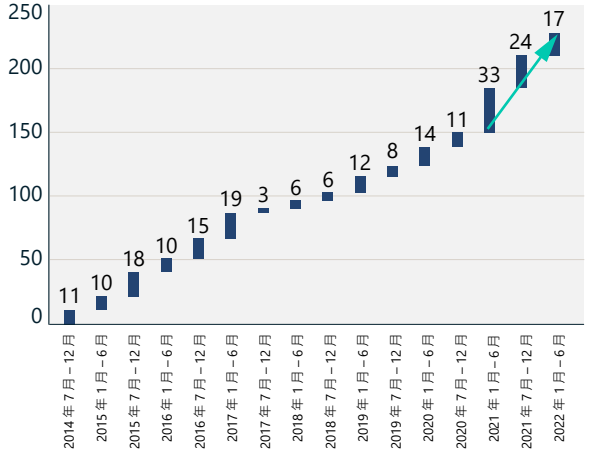
零時差漏洞是初步惡意探索相當有效的手段，一旦公開暴露，其他國家級和犯罪行為體就能迅速重複利用這些漏洞。過去一年公開揭露的零時差漏洞數量與前一年不相上下，是有史以來的最高記錄。

隨著網路威脅行為體（包括國家級和犯罪）越來越擅長利用這些漏洞，我們觀察到，從公布漏洞到該漏洞商品化，這個過程的時間縮短了。因此，組織修補漏洞刻不容緩。同樣重要的是，組織或個人一旦發現新漏洞，就應依照協議的漏洞揭露程序，負責盡快向受影響的廠商揭露或通報。

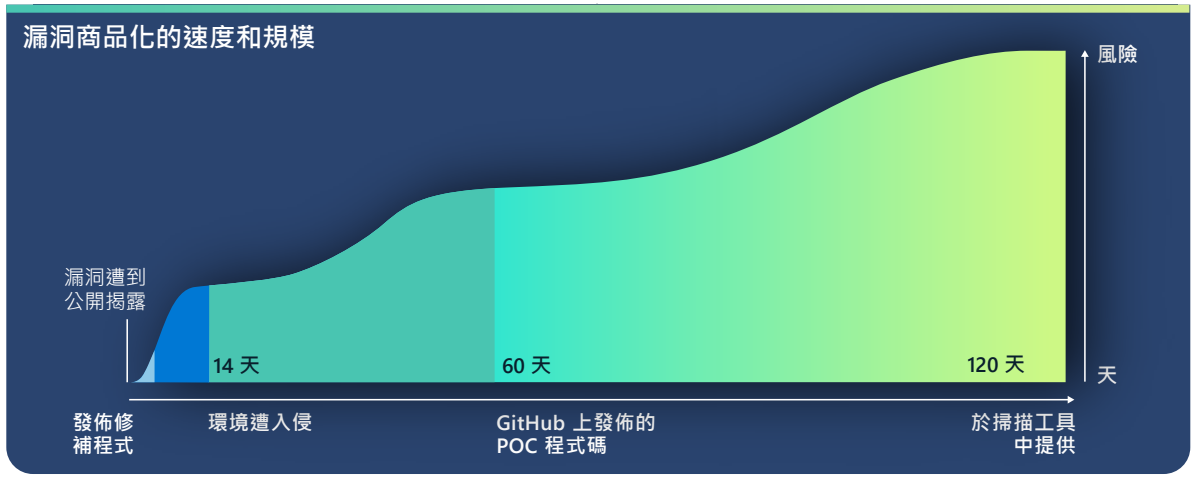
這樣就能確保找到漏洞，並及時開發修補程式，以保護客戶免於遭受先前未知的威脅侵害。

許多組織會假設，如果漏洞管理是其網路安全性整體的一部分，那麼他們就不太可能成為零時差攻擊的受害者。然而，漏洞商品化卻促使它們發展的速度更快。零時差漏洞經常被其他行為體發現，並在短時間內大規模重複利用，使得未修補的系統面臨風險。儘管零時差攻擊可能難以偵測到，但行為體的入侵後行動通常較容易偵測到，而且如果是來自完整修補的軟體，也可視為入侵的警告訊號。

針對零時差漏洞所發行的修補程式



常見的漏洞和暴露風險清單 (CVE) 公開揭露的零時差漏洞數量。



平均而言，漏洞被公開揭露後，只需 14 天就可在環境中用於入侵。此觀點提供了零時差漏洞利用時程表的分析，以及容易遭受所指入侵攻擊且自首次公開揭露起在網路上活動的系統數量。

雖然零時差漏洞攻擊一開始往往以一群有限的組織為目標，但很快就會納入更大規模的威脅行為體生態系統。這使得威脅行為體加快腳步，盡可能在潛在目標安裝修補程式之前擴大利用漏洞。

雖然我們觀察到許多國家級行為體從未知的漏洞發展成惡意探索漏洞，但中國為主的國家級威脅行為體在發現和發展零時差漏洞方面尤其精通。中國的漏洞報告法規於 2021 年 9 月生效，成為全世界首度有政府要求在向產品或服務擁有者分享漏洞情報之前，先向政府機構通報漏洞以進行審查。這項新法規可能讓中國政府機構中的要角得以積累通報的漏洞，並進一步發展成武器。過去一年來，中國為主的行為體使用零時差的情況增加，可能反映出中國首度一整年對中國安全社群的漏洞揭露需求，也是利用零時差漏洞做為國家優先事項方面的一大步。下面所述的漏洞最先是由中國為主的國家級行為體在攻擊中開發和部署，接著被發現並散播到更大規模威脅生態系統中的其他行為體。

快速漏洞攻擊

續

即使組織不是國家級攻擊的目標，在規模更大的行為體生態系統利用漏洞之前，能修補受影響系統中零時差漏洞的時間也有限。

這些新發現漏洞的範例顯示，從漏洞修補開始，組織平均有 60 天的時間，概念證明 (POC) 程式碼會線上提供，而且通常由其他行為體挑選來重複使用 同樣地 在自動漏洞掃描和惡意探索工具 (如 Metasploit) 找到漏洞之前，組織平均有 120 天的時間 這通常會導致大規模利用漏洞 。這也突顯出，即使組織不是國家級威脅行為體的目標，在規模更大的行為體生態系統利用漏洞之前，能修補受影響系統中零時差漏洞的時間也有限。

CVE-2021-35211 SolarWinds Serv-U

在 2021 年 7 月，SolarWinds 發佈 CVE-2021-35211 資訊安全公告，將此歸功於 Microsoft 通知。[8] 當時我們發現了與國家級一致的威脅行為體 DEV-0322 正積極利用 SolarWinds Serv-U 漏洞。我們的 RiskIQ 團隊在 6 月 15 日到 7 月 9 日之間，觀察到有 12,646 個 IP 位址裝載了受影響裝置的網際網路連線版本。

CVE-2021-40539 Zoho ManageEngine ADSelfService Plus

2021 年 9 月，我們的研究人員觀察到，中國附屬行為體利用了數個位於美國境內實體的 Zoho ManageEngine。此漏洞在 9 月 6 日公開通報為 CVE-2021-40539 Zoho ManageEngine ADSelfService Plus，組織通常會使用它來處理密碼重設。[9] DEV-0322 在 9 月底利用此漏洞做為初始媒介，以在網路中獲得立足點，並執行其他動作，包括認證傾印、安裝自訂二進位檔案，以及放置惡意軟體以維持持續性。在揭露時 RiskIQ 在網際網路上觀察到 4,011 個這些系統的活躍執行個體。

CVE-2021-44077 Zoho ManageEngine ServiceDesk Plus

在 2021 年 10 月底，我們觀察到 DEV-0322 利用另一項 Zoho ManageEngine 產品 ServiceDesk Plus 中的漏洞 (CVE-2021-44077)，此產品為具有資產管理功能的 IT 技術支援軟體。DEV-0322 利用此漏洞來鎖定醫療保健、資訊科技、高等教育和關鍵製造業當中的實體並進行入侵。在 12 月 2 日，美國聯邦調查局 (FBI) 與網路安全暨基礎設施安全局 (CISA) 發出了一份聯合公告，警告大眾有關國家級威脅行為體利用此漏洞的資訊。在揭露時，RiskIQ 在網際網路上觀察到 7,956 個這些系統的活躍執行個體。

CVE-2021-42321 Microsoft Exchange

在 2021 年 10 月 16 日和 17 日於中國成都舉辦的天府杯國際網路安全高峰會暨駭客競賽期間，揭露了 Exchange 漏洞 CVE-2021-42321 的零時差入侵活動。Microsoft 的安全研究人員在漏洞揭露之後經過僅三天時間，於 10 月 21 日就觀察到環境中使用 Exchange 漏洞的入侵活動。在揭露時，RiskIQ 在網際網路上觀察到 61,559 個這些系統的活躍執行個體。直到 2021 年 11 月，我們都持續觀察到入侵活動。

CVE-2022-26134 Confluence

中國附屬行為體可能在 6 月 2 日公開揭露 Confluence 漏洞 (CVE-2022-26134) 之前四天就已握有該漏洞的零時差入侵程式碼，並且可能利用此程式碼來對付美國境內實體。在揭露時，RiskIQ 在網際網路上觀察到 53,621 個易受攻擊的 Confluence 系統執行個體。

漏洞被挑選出，並且在相對更短的時間內遭到大規模利用。

可付諸行動的見解

1. 零時差漏洞一經發佈即優先修補，不要等到修補管理週期才部署。
2. 記載並清查所有企業硬體和軟體資源，以判斷風險，並迅速決定進行修補的時程。

俄羅斯國家級行為體的戰時網路戰術威脅烏克蘭及其他範疇

今年，俄羅斯國家級行為體展開網路活動來支援俄羅斯入侵烏克蘭期間的軍事行動，通常是使用相同的戰術和技術來打擊烏克蘭境外的目標。世界各地的組織必須採取措施來加強網路安全性，以對抗俄羅斯陣線的威脅行為體引發的數位威脅。

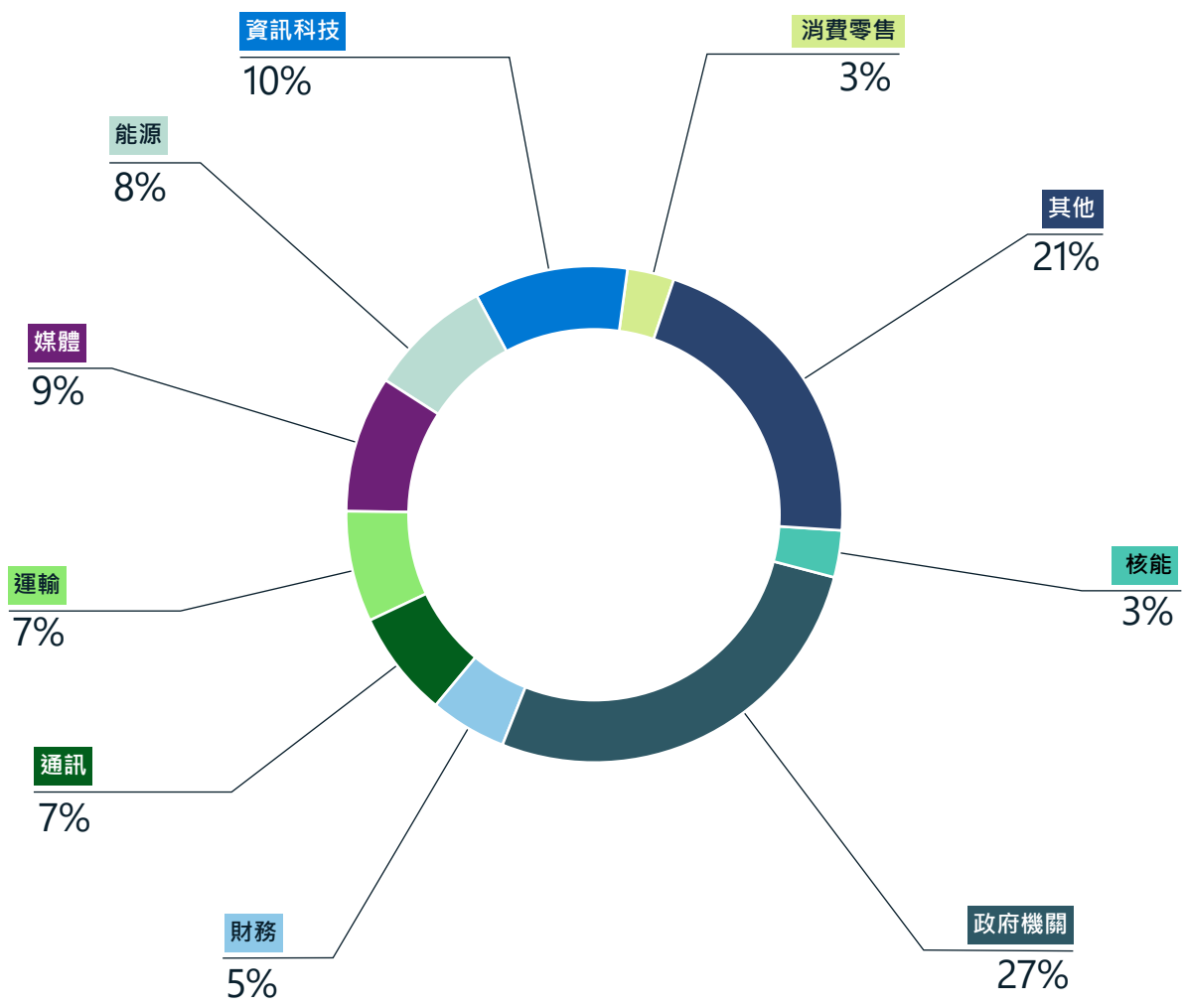
隨著軍事衝突持續造成地面情勢繼續動盪，假如俄羅斯國家級網路活動份子對準軍事目標提高入侵頻率或強度，那麼烏克蘭及其盟友也應準備好自我防禦。在戰事爆發後的四個月間，Microsoft 觀察到與俄羅斯軍事相關的威脅行為體對近 50 個不同的烏克蘭機構和企業發動了數波破壞性網路攻擊，以及對其他目標進行了間諜活動為主的入侵行動。若排除對網路服務客戶進行的活動，在 2 月底到 6 月間，有 64% 針對已知目標的俄羅斯威脅活動是朝向烏克蘭境內的組織發動。

在每一波活動中，俄羅斯威脅行為體都利用我們在對烏克蘭境內和境外目標進行入侵前，觀察到的許多戰術、技術和程序 (TTP)。這些行為體主要目的在於破壞資料，使烏克蘭政府機構在衝突初期失去制衡能力。此後，他們試圖切斷對烏克蘭的軍事運輸和人道救援行動，中斷大眾存取服務和媒體的能力，並竊取對俄羅斯的長期情報或經濟價值的資訊。

鎖定交通運輸為目標，對試圖在衝突中倖存的烏克蘭公民而言至關重要的區域造成了威脅。根據 5 月 UNICEF 贊助的一項調查顯示，受衝突影響的城市地區受訪者最憂心的是運輸和燃料、供應中斷、安全性，以及能獲得的食物、醫療服務和金融服務有限。[10] 6 月時，聯合國烏克蘭危機協調員表示，烏克蘭境內至少有 1570 萬人急需人道救援，而且隨著戰事持續，這個數字將會增加。[11]

在烏克蘭境外，Microsoft 在 2 月底到 6 月間偵測到有 42 個國家 / 地區的 128 個組織遭到俄羅斯網路入侵攻擊。美國是俄羅斯頭號目標。在此期間，借道波蘭進入烏克蘭的許多國際軍事支援和人道救援同樣也是主要的目標。在 4 月和 5 月間，隸屬於俄羅斯政府的威脅行為體也追擊了波羅的海國家的組織，以及丹麥、挪威、芬蘭和瑞典等國的電腦網路。

入侵以來烏克蘭境內最主要的目標產業別



在整個衝突期間，烏克蘭境內的聯邦、州和地方政府組織一直是俄羅斯政府和附屬威脅組織的優先目標。交通運輸、能源、金融和媒體業組織成為焦點，突顯了這些網路活動對烏克蘭公民所依賴的服務構成風險。

俄羅斯國家級行為體的戰時網路戰術威脅烏克蘭及其他範疇

續

我們也看到，NATO 國家的外交部門成為類似活動目標的情況增加。

在過去一年，俄羅斯國家級威脅組織持續保持對烏克蘭境內和境重大基礎設施的高度入侵行動。IRIDIUM 在一次失敗的行動中部署了 Industroyer2 惡意軟體，企圖破壞烏克蘭的電力系統造成數百萬人無電可用。在烏克蘭境外，BROMINE 在 2022 年初對參與製造業和工業控制系統的組織發動入侵。

今年，俄羅斯政府與附屬行為體利用許多下列 TTP 對烏克蘭、其盟友和其他有情報價值的目標進行了網路行動：

利用惡意附件或連結的魚叉式網路釣魚

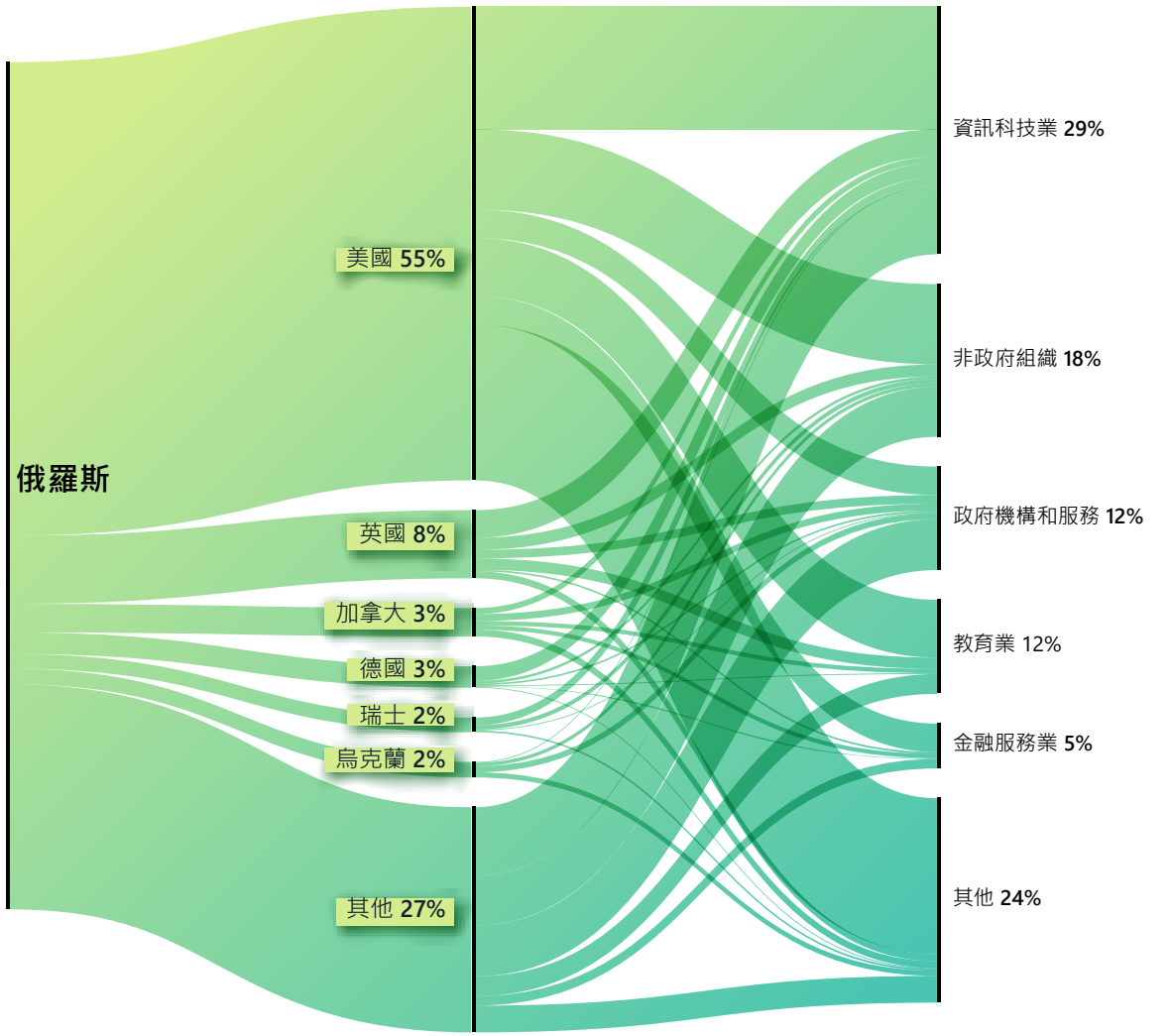
俄羅斯政府及附屬於俄羅斯的組織，如 ACTINIUM、DEVIUM、STRONTIUM、DEV-0257、SEARIDIUM 和 IRIDIUM，全都利用網路釣魚活動來初步存取烏克蘭境內和境外組織中所需的帳戶和網路。許多活動利用目標組織或同業內遭入侵或詐騙的帳戶及吸引人的主題來誘騙受害者。NOBELIUM 利用遭入侵的外交官員帳戶來傳送網路釣魚郵件，偽裝成外交官員對全球的外交部門員工進行通訊。STRONTIUM 根據美國智庫公開提供的帳戶擁有者名稱建立了詐騙帳戶，並傳送網路釣魚訊息來取得智庫內帳戶的存取權。SEAIUMIUM 利用與烏克蘭衝突相關的報告為誘餌進行網路釣魚，而得以初步存取北歐國家國際事務智庫的帳戶。

利用 IT 服務供應鏈影響下游客戶

在 2021 年底，俄羅斯國家級行為體入侵了 IT 服務提供者，並利用存取權從事進一步的網站竄改，並於 1 月時藉由 DEV-0586 部署 Whispergate 破壞性惡意軟體。[12] DEV-0586 還入侵了一家為烏克蘭國防部建置資源管理系統的 IT 公司網路，以及通訊與交通運輸部門中的其他組織，表示該組織同時在這些部門中探索第三方攻擊的選項。

在 2021–2022 年間，NOBELIUM 在全世界鎖定 IT 服務提供者為目標，取得政府機構和其他敏感網路的存取權，其中又以美國和西歐為主要目標 (請參閱本章前段有關供應鏈弱點的討論)。

俄羅斯：主要目標國家 / 地區與產業別



儘管自 2022 年初以來更加聚焦烏克蘭境內的組織，但位於北美和西歐的企業仍然是俄羅斯行為體最主要攻擊的線上服務客戶。NOBELIUM 攻擊 IT 業的活動，使該產業成為去年度最主要的目標。

俄羅斯國家級行為體的戰時網路戰術威脅烏克蘭及其他範疇

續

利用對外公開的應用程式取得網路的初步存取權

至少自 2021 年底以來，STRONTIUM 致力發展並優化其利用公眾服務的能力（例如 Microsoft Exchange 伺服器）來竊取資訊。STRONTIUM 利用了未修補的 Exchange 伺服器來存取烏克蘭政府機構的帳戶，以及進入美國、黎巴嫩、祕魯和羅馬尼亞境內的軍事和國防工業相關組織，還有亞美尼亞、波士尼亞、科索沃和馬來西亞境內的其他政府機構。DEV-0586 也夥同俄羅斯軍事組織，利用 Confluence 伺服器漏洞而得以初步進入烏克蘭和其他東歐國家 / 地區的政府和 IT 部門組織。

在戰時及和平時期，俄羅斯政府與其附屬威脅行為體使用了許多相同的 TTP 來入侵鎖定的組織。

使用系統管理帳戶和通訊協定以及原生公用程式進行網路探索和橫向移動

在取得初步存取網路的權限後，Microsoft 觀察到，俄羅斯國家級行為體會利用執行基本維護工作所使用的合法帳戶和軟體公用程式來盡可能規避偵測。他們依賴具有系統管理功能的遭入侵身分識別，以及有效的系統管理通訊協定、工具和方法在網路內橫向移動，而不會立即吸引自動化監控和網路防禦者的注意。

基本網路檢疫及採用端點偵測和應變工具，有助於減輕這些類型的活動在平時和戰時造成的負面影響。

持續衝突的不可預測性促使世界各地的組織必須採取措施來加強網路安全性，以對抗俄羅斯國家級和俄羅斯附屬威脅行為體引發的數位威脅。

可付諸行動的見解

1. 透過實施 MFA 身分識別防護工具來保護使用者的身分識別，以及強制執行最低權限存取來保護最敏感的權限帳戶和系統，將認證竊取和帳戶濫用的情形降至最低。
2. 套用更新以確保所有系統盡快獲得最高層級的防護，並保持最新狀態。
3. 在組織中部署防惡意軟體、端點偵測和身分識別防護解決方案。結合各種深度防禦安全性解決方案，並搭配經訓練且有能力的人員，就能讓組織有能力識別、偵測及防止影響業務的入侵行為。
4. 藉由備份關鍵系統和啟用記錄，在偵測到或收到有關環境威脅的通知時進行調查並復原。強烈建議制定出事件應變計畫。

進一步資訊的連結

- 保衛烏克蘭：網路戰的早期教訓 | Microsoft 問題焦點（英文）
- 烏克蘭的混合戰 | Microsoft 問題焦點（英文）
- 烏克蘭的網路威脅活動：分析和資源分析 | Microsoft 安全回應中心 (MSRC)
- 中斷鎖定烏克蘭為目標的網路攻擊 | Microsoft 問題焦點（英文）
- 鎖定烏克蘭政府為目標的惡意軟體攻擊 | Microsoft 問題焦點（英文）
- MagicWeb：NOBELIUM 以任意身分進行驗證的入侵後誘騙手段 | Microsoft 威脅情報中心 (MSTIC)、偵測及回應團隊 (DART)、Microsoft 365 Defender 研究團隊

中國擴大全球目標以提升競爭優勢

在現今複雜的地緣政治情勢中，進行網路活動的中國國家級和國家附屬威脅行為體的目的通常在於推進國家的策略性軍事、經濟和對外關係目標，這是中國獲得競爭優勢的目標之一。過去一年，Microsoft 觀察到以世界各地國家 / 地區為目標的大規模中國威脅活動。

自 2021 年中以來，中國一直在操控局勢，以在最糟的 COVID-19 疫情爆發情況下確保經濟與財務穩定。[13] 中國繼續努力維護在地緣政治事件上的立場，例如努力在與俄羅斯的「不設限」夥伴關係 [14] 以及在國際舞台上維持立場之間取得平衡。[15] 此外，中國對美國與其盟友在台灣議題上提出嚴正抗議 [16]，以及在南海議題上持續與許多國家 / 地區的對外關係造成壓力。[17]

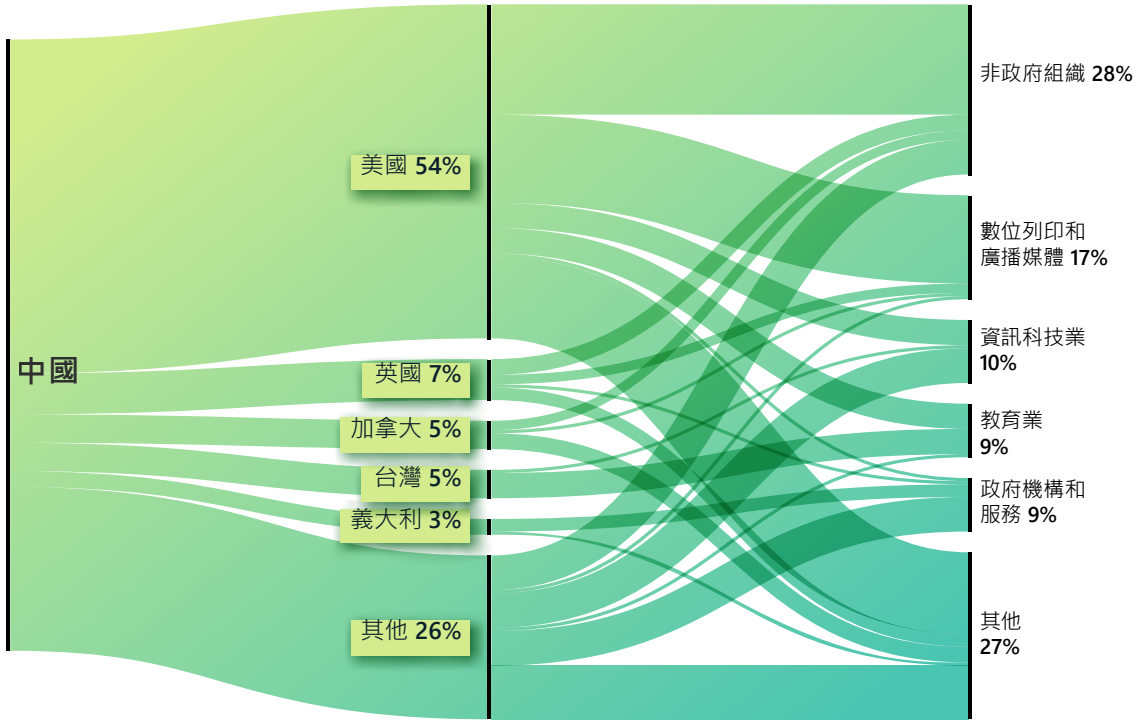
中國國家級和國家附屬威脅組織增加了鎖定全世界小國為目標，並且將重點放在東南亞，以在所有方面獲得競爭優勢。

中國同時透過先前制定的一帶一路倡議 (BRI) 繼續擴大本身在全球的經濟影響力，試圖重新制定與歐盟 (EU) 的全面投資架構 [18]，並與亞太地區的 15 個國家協商新的區域貿易協定，稱為區域全面經濟夥伴協定。[19] Microsoft 評估，從觀察到的網路活動和廣泛鎖定的實體目標規模來看，中國將繼續利用網路收集做為工具，協助推進其策略性政治、軍事和經濟目標。

網路目標可能促進經濟和軍事利益。

Microsoft 觀察到，中國國家級和國家附屬威脅組織擴大將目標鎖定在世界各地的小國，這暗示著中國很可能利用網路間諜活動做為其擴大全球經濟和軍事影響力的一環。

中國：主要目標國家 / 地區與產業別



智庫 /NGO、媒體、IT、政府機構和教育部門，都是最常成為中國為首威脅組織鎖定目標的產業，其目的可能是持續情報收集和偵察。

目標範圍包括 (但不限於) : 位於非洲、加勒比海、中東、大洋洲和南亞的國家 / 地區，其中的重點則是在東南亞各國和太平洋島國。

根據中國的 BRI 策略，中國為首的威脅組織將目標鎖定在阿富汗、哈薩克、模里西斯、納米比亞和千里達及托巴哥。[20] 例如，千里達及托巴哥是 2018 年第一個為中國 BRI 策略背書的加勒比海國家，而中國將其視為該區域的重要合作夥伴。NICKEL 自 2021 年以來，一直以千里達及托巴哥為網路活動的目標。例如，2022 年 3 月，NICKEL 已政府機構為目標進行了偵察活動，目的可能是收集情報。

中國擴大全球目標以提升競爭優勢

續

同時，Microsoft 觀察到中國國家級和國家附屬威脅組織將其網路活動的重點放在東南亞地區的實體，並且擴及太平洋島國，因為中國將其軍事和經濟優先事項轉為處理美國重新關注該區域所帶來的挑戰。2022 年 1 月，Microsoft 觀察到 RADIUM 鎖定越南一家能源公司和能源相關政府機構，以及印尼的政府機構為目標。RADIUM 的活動很可能與中國在南海的策略目標一致。[21] 在 2 月底到 3 月初，GALLIUM 入侵了附屬於東南亞地區一個著名的跨政府組織 (IGO) 的 100 多個帳戶。GALLIUM 攻擊該區域 IGO 的時機，適逢美國與區域領導人宣佈敲定會面的時間。GALLIUM 行為體的任務很可能就是在事件之前監控通訊並收集情報。

中國擴大在太平洋島國的影響力同時，中國威脅組織的活動也隨之而來。4 月時，中國和索羅門群島簽署了一項安全協定，旨在「促進和平與安全」。這項協定可能讓中國得以在索羅門群島上部署武警和軍隊。[22] 5 月時，中國在斐濟主辦了第二次中國與太平洋島國 (PICs) 外長會議，並提議推動「全面策略夥伴關係」，以進一步促進政治、文化、社會、安全和氣候變遷利益，同時對抗全球疫情[23] 大約在 5 月同一時間，Microsoft 在索羅門群島政府系統上發現了 GADOLINIUM 惡意軟體。此外，RADIUM 也在巴布亞紐幾內亞境內一家電信公司的系統上執行惡意程式碼。我們評估，這些活動可能出於情報收集目的，以支援中國的整體區域策略。

Microsoft 中斷了 NICKEL 活動，但威脅組織仍持續存在。

2021 年 12 月，Microsoft 數位犯罪部門 (DCU) 向美國維吉尼亞州東區的美國聯邦地區法院提交訴狀，要求當局查封 42 個由 NICKEL 掌控的命令和控制 (C2) 網域。這些 C2 網域自 2019 年 9 月起，在針對中南美洲、加勒比海、歐洲和北美洲的政府、外交實體和 NGO 的活動中使用。[24] NICKEL 自 2019 年底以來，透過這些活動得以長期存取數個實體並持續洩漏這些受害者的資料。

隨著中國繼續與更多國家（通常簽訂了 BRI 相關協定）建立雙邊經濟關係，中國的全球影響力將持續擴大。我們評估，中國國家級和國家附屬威脅行為體將追擊其政府機構、外交和 NGO 領域的目標，以獲得新見解，可能是為了達成經濟上的間諜活動或傳統的情報收集目的。自 Microsoft 的中斷行動以來，NICKEL 鎖定了數個政府機構為目標，可能試圖重新取得失去的存取權。在 2022 年 3 月底到 5 月間，NICKEL 再次入侵了全世界至少五個政府機構。這暗示著，該組織取得了這些實體的其他進入點，或是透過新的 C2 網域重新取得存取權。NICKEL 持續在全球重複入侵相同的政府機構，意味著這項任務的重要性相當高。

中國對於其對外政策的立場越來越有自信。我們評估，透過網路進行的經濟間諜活動和情報收集工作很可能會繼續。

可付諸行動的見解

1. 大幅提升網路防禦能力，以主動消弭網路威脅。由於中國威脅行為體持續存在，因此各組織必須及時找出、保護、偵測及回應可能的入侵。
2. 威脅行為體會濫用排定的工作[25] 做為慣用手段來維持其持續性並規避防禦，您務必確保環境採行額外的安全指導方針來防範這種常用的伎倆。[26]
3. 我們會繼續觀察使用 Web Shell 做為進入目標網路的初始媒介的情況。[27] 組織應強化其系統，以抵禦 Web Shell 攻擊，這類攻擊可能讓攻擊者得以進入並執行遠端命令。[28]

進一步資訊的連結

- NICKEL 鎖定整個拉丁美洲及歐洲的政府機構為目標 | Microsoft 威脅情報中心 (MSTIC)、Microsoft 數位安全部門 (DSU)
- 保護人員免受近期的網路攻擊 | Microsoft 問題焦點（英文）

伊朗在政權交替後展現積極野心

Microsoft 觀察到，伊朗國家級組織和附屬行為體加快了對以色列進行網路攻擊的步調並加大範圍，將勒索軟體攻擊對象從區域敵手擴大到美國和歐盟受害者，並鎖定知名的美國重大基礎設施為目標，至少預先佈局進行可能的破壞性網路攻擊。

隨著伊朗政權交替，其國家級行為體的網路活動也更加積極。2021 年夏季，伊朗強硬派總統 Ibrahim Raisi 上位，取代了溫和派總統 Hassan Rouhani。Raisi 是最高領袖的接班人，也是伊朗伊斯蘭革命衛隊 (IRGC) 的親密盟友，與前總統 Rouhani 的外交作風形成了鮮明的對比，前總統經常與最高領袖和 IRGC 資深領導人意見相左。[29] Raisi 政府的鷹派觀點似乎促使伊朗行為體提高意願，對以色列與西方採取更大膽的行動，尤其是美國，儘管美國重新加入外交行動，以恢復伊朗核協議。

伊朗加快對以色列網路攻擊的步調並加大範圍

在 Raisi 組成其外交政策團隊後的數星期內 [30]，伊朗國家級行為體恢復對以色列的破壞性網路攻擊，且速度較前一年更快。這些勒索軟體和駭入再洩露攻擊從 9 月開始每隔幾星期便會發動，至少涉及 3 個伊朗附屬行為體，暗示著這些攻擊可能與報復以色列的全國性活動有所關聯。至少在一個案例中，Microsoft 評估 2021 年底對以色組織發動的勒索軟體攻擊，目的是為了掩護背後的資料刪除攻擊。Microsoft 惡意軟體分析確定了傳送至受害者的勒索軟體設計，是在加密後執行 wiper 惡意軟體。

到了 2022 年，伊朗網路攻擊在目標選定和攻擊形式上有所提升。2 月時，DEV-0198 試圖對以色列重大基礎設施發動破壞性攻擊。Microsoft 也評估，一個伊朗附屬行為體最有可能是一項複雜網路攻擊背後的主謀，該次攻擊可能使用軟體調整 IP 網路音訊，在 6 月造成以色列緊急防空警報誤發。

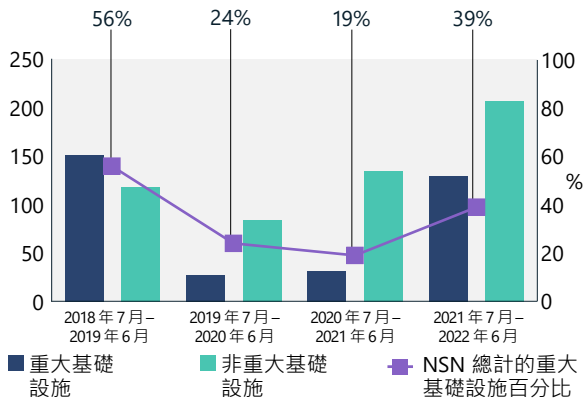
伊朗一整年間對美國和以色列重大基礎設施的威脅不斷增加

Microsoft 評估，伊朗國家級行為體附屬於 IRGC (PHOSPHORUS 和 DEV-0198)，從 2021 年後期到 2022 年中鎖定知名的美國和以色列重大基礎設施為目標。可能的目標是讓德黑蘭得以呼應資深 IRGC 長官將伊朗發生的中斷事件歸咎於美國和以色列，而展開報復針對相同領域進行報復。[31] 我們評估，此活動與 2021 年 10 月底 IRGC 伊朗民防組織首長 Gholamreza Jalali 將軍的聲明有關，他呼應了政權內其他勢力人士的指控，認為美國和以色列對伊朗的港口、鐵路和加油站發動網路攻擊。[32] Jalali 在一場精心準備的主麻日演說中，於講台上第二度傳達了這項指控，並播放飛彈擊中「USA」字樣的影像，暗示著高階人員與他抱持相同的觀點。[33]

2021 年 10 月，PHOSPHORUS 開始大規模掃描美國組織，企圖找出未修補的 Fortinet 和 ProxyShell 漏洞。一旦遭到入侵，這些未修補的系統就會用來執行勒索軟體攻擊，在數個案例中，其目標鎖定美國和其他西方國家的重大基礎設施。這些活動首度證實了在中東以外地區發動的伊朗國家附屬勒索軟體攻擊事件。在 10 月底伊朗發生的加油站網路攻擊事件後，Microsoft 觀察到，對美國企業的伊朗勒索軟體攻擊激增，暗示著兩者之間可能的關聯性。

於此同時，PHOSPHORUS 進入了目標式攻擊，經常透過魚叉式網路釣魚鎖定知名的美國重大基礎設施公司為目標，包括入境的主要港口和機場、運輸系統、公用事業公司，以及石油和天然氣公司。此目標式攻擊經常透過魚叉式網路釣魚進行，一直持續到 2022 年中。這些目標直接與德黑蘭當局歸咎美國和以色列對伊朗發動攻擊的領域不謀而合，很可能為伊朗提供了報復的選項。對幾乎相同的目標進行入侵可能提供機會來嚇阻未來這類攻擊，同時藉由指出攻擊原因但不承認犯罪的方式，試圖避免衝突升級。

伊朗基礎設施再次成為目標



伊朗鎖定重大基礎設施為目標的情況增加，觀察到的最高程度介於 2018 年下半到 2019 年初。我們使用美國第 21 號總統政策指令 (PPD-21) 來判斷一家公司是否符合重大基礎設施的標準。(2021 年 7 月 –2022 年 6 月)。

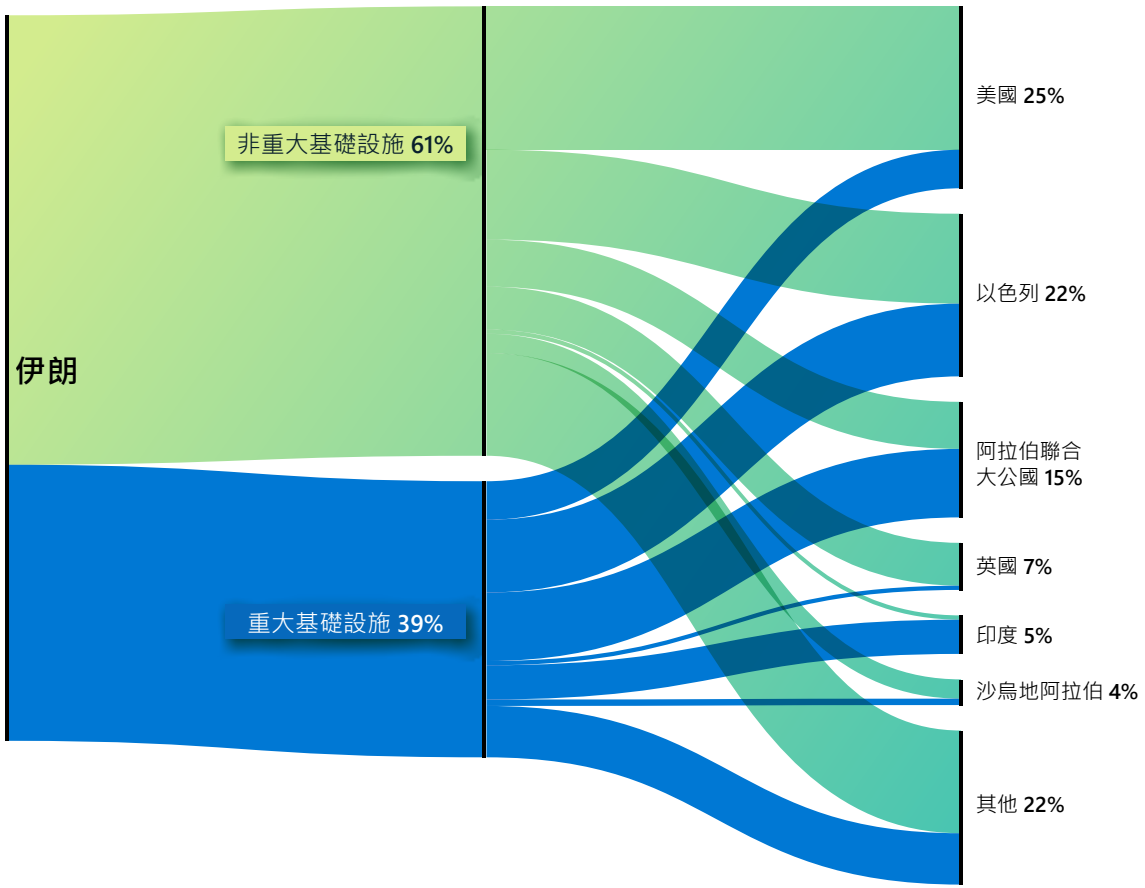
伊朗在政權交替後展現積極野心

續

在以色列，DEV-0198 將目標鎖定以色列的鐵路、物流公司 ·物流公司的軟體提供者 ·以及燃料公司，並將重點放在加油站。2022 年初，該組織對以色列主要物流公司發動了破壞性攻擊，迫使該公司關閉電腦和部分營運以圍堵攻擊。在另一個案例中，我們觀察到該組織企圖透過竊得或重複使用的認證，存取以色列主要交通運輸提供者的網路。同時，另一個伊朗行為體 DEV-0343，其目標鎖定國防、航運和衛星影像公司暗示著與 IRGC 有所關聯，該行為體在 2021 年初入侵了以色列交通運輸和港口相關實體的帳戶。

以色列威脅組織很可能持續威脅美國和以色列的交通運輸和能源公司，尤其是在恢復伊朗核協議的外交行動式微之際，華盛頓、特拉維夫和德黑蘭當局都在尋求替代的強制手段來制衡讓步。

伊朗鎖定重大基礎設施為目標的國家別



伊朗鎖定重大基礎設施為目標的情況，最主要是針對以色列、阿拉伯聯合大公國及美國組織。

在接下來的一年，伊朗行為體很可能持續威脅美國和以色列的交通運輸和能源公司。

伊朗組織將勒索軟體攻擊從區域對手向外擴大，並鎖定知名的美國和以色列重大基礎設施為目標。

可付諸行動的見解

1. 藉由啟用如 MFA 等無密碼解決方案，並且針對所有遠端連線強制使用，以加強組織的整體網路檢疫，進而減少任何可能遭入侵的認證出現。
2. 評估所有入埠電子郵件流量的真實性，確保寄件者位址合法。
3. 及早並經常修補。[34]
4. 審查並稽核您與服務提供者之間的每一項合作夥伴關係，以盡可能減少組織與上游提供者之間任何不必要的權限。Microsoft 建議，立即移除任何看似陌生或未經過稽核的合作夥伴關係的存取權。[35]

進一步資訊的連結

- 伊朗鎖定 IT 部門為目標的趨勢上升 | Microsoft 威脅情報中心 (MSTIC)，Microsoft 數位安全部門 (DSU)
- 伊朗相關的 DEV-0343 鎖定國防、GIS 及航運部門為目標 | Microsoft 威脅情報中心 (MSTIC)，Microsoft 數位安全部門 (DSU)

黎巴嫩境內與伊朗攻擊以色列相關的組織

Microsoft 不分平台、目標受害者或地理區域一致監控網路威脅活動。我們在全世界維持可見度並積極找尋威脅，為客戶提供更強大的偵測能力。

雖然來自俄羅斯、中國、伊朗和北韓的威脅佔了我們所觀察到的國家級行為體活動的大多數，但是我們也會追查並傳達來自 NATO 成員國和民主國家的威脅。在去年，我們在土耳其境內行為體 (SILICON) 和越南境內行為體 (SILICONTH) 的活動中起了作用。今年我們將擴大追查先前公開揭露的黎巴嫩境內組織的詳細情形。[36]

Microsoft 發現了先前未記載的黎巴嫩境內組織，我們有適度信心評估，該組織與伊朗情報暨安全局 (MOIS) 附屬的行為體共同協調行動。自 2020 年底以來，這類來自德黑蘭的合作或指令與揭露的真相一致，指出伊朗政府正利用第三方來執行網路活動，很可能為了強化伊朗的合理推諉。

在觀察到的活動中，POLONIUM 在 2022 年 2 月至 5 月間於黎巴嫩境內採取行動，鎖定或入侵了 20 多個以色列境內的組織和一個 IGO，隨後遭到 Microsoft 阻斷並公開揭露其活動。有近一半的以色列組織屬於以色列國防工業的一部分，或與以色列國防企業有所關聯，這表示該組織與伊朗在收集情報和 / 或直接反擊以色列方面有著類似的共同利益。[37]

POLONIUM 與 MOIS 組織之間有所關聯的評估依據，是觀察到的受害者重疊，以及工具和技術的共通性。

- 受害者重疊：一個與伊朗 MOIS 有所關聯的伊朗國家級組織，Microsoft 以 MERCURY 追查其行動，該組織先前入侵了多個 POLONIUM 受害者，指出任務需求的融合，或雙方組織之間可能會「移交」受害者。
- 共同的工具和技術：類似 POLONIUM，MSTIC 觀察到 DEV-0588 (也稱為 CopyKittens) 經常使用 AirVPN 從事活動，而 DEV-0133 (也稱為 Lyceum[38]) 使用 OneDrive 作為 C2 並進行洩密。與伊朗國家行為體類似，POLONIUM 利用雲端服務提供者入侵以色列一家航空公司和律師事務所。[39]

POLONIUM 部署了一系列的客製化植入器，以使用雲端服務作為 C2 並進行洩密，最明顯就是 OneDrive 和 DropBox。POLONIUM 經常針對目標建立專屬的 OneDrive 應用程式，很可能是為了規避偵測。

截至 2022 年 6 月，Microsoft 讓 20 多個 POLONIUM 建立的 OneDrive 應用程式停擺，通知受影響的組織，並且部署一系列的安全性情報更新來隔離 POLONIUM 開發的工具。

Microsoft 成功偵測到並阻斷了 POLONIUM 濫用 OneDrive 作為 C2 的行為。

可付諸行動的見解

1. 更新防毒工具[40]，並確保開啟雲端防護[41]以偵測相關指標。
2. 對於具有服務提供者關係的客戶，務必落實所有合作夥伴關係審查和稽核，以盡可能將組織與上游提供者之間不必要的權限降到最低。[42] 立即移除任何看似陌生或未經過稽核的合作夥伴關係的存取權。

進一步資訊的連結

- 公開鎖定以色列組織為目標的 POLONIUM 活動和基礎結構 | Microsoft 威脅情報中心 (MSTIC)、Microsoft 數位安全部門 (DSU)
- MERCURY 利用未修補的系統中的 Log4j 2 漏洞來鎖定以色列組織為目標 | Microsoft 威脅情報中心 (MSTIC)、Microsoft 365 Defender 研究團隊、Microsoft Defender 威脅情報

北韓運用網路能力實現政權當局的三大目標

過去一年來，北韓的網路優先事項反映出當權政府所稱的全球優先事項。金正恩在幾次重要演說中強調了三項優先事項，包括建造國防能力、振興國家岌岌可危的經濟，以及確保國內穩定。[43] 北朝國家級行為體採取的行動清楚顯示，他們利用網路來實現這三個目標。

北韓國家級威脅組織（主要是 CERIUM 和 ZINC）利用各種戰術試圖侵入全球各地國防和航太公司的網路。隨著北韓在 2022 年上半年展開歷來最積極的飛彈試射，它同時利用了網路間諜活動來幫助北韓研究人員在發展自主防禦系統和對策上取得優勢，以利反制對手所取得的進展。

我們觀察到，COPERNICIUM 鎖定全世界各種加密貨幣相關公司為目標，且通常能成功，以協助支持北韓岌岌可危的經濟。雖然我們無法確認該組織是否能在入侵後將貨幣外洩，但我們觀察到，COPERNICIUM 會傳送惡意文件來偽裝成其他加密貨幣公司發出的提案，藉此感染數十台電腦。

最後，Microsoft 以 DEV-0215 追查的一個組織，藉由鎖定報導北韓議題的新聞組織為目標，努力捍衛北韓的穩定與忠誠度。這些機構在北韓和脫北者社群內都有來源，而平壤當局將他們視為生存上的威脅。此外，該組織努力取得進入韓語基督教團體網路的存取權，這些團體往往發表公開反對北韓的言論，並積極與脫北者合作。

北韓國家級行為體利用各種戰術試圖侵入世界各地的航太公司。

鎖定國防和航太公司為目標

由 CERIUM 和 ZINC 領導的北韓國家級行為體，大量投入發展以侵入國防和航太公司為目標的戰術。CERIUM 藉由下載用戶端和尋找弱點的方式，不斷探測南韓的虛擬私人網路 (VPN)。另外還下載了南韓軍事和政府客戶常用的應用程式，很可能是為了要尋找漏洞。該組織密切關注目前的活動，並撰寫新的誘餌文件，利用高認知度的主題做為誘餌，吸引目標點按其惡意軟體執行檔和連結。

ZINC 和 CERIUM 都在活動中使用社交媒體和社交工程。ZINC 尤其擅長在 LinkedIn 和其他專業社交媒體網站上建立假的個人資料，背後的主謀則假冒主要國防和航太公司的招聘人員。他們使用這些個人資料，利用社交媒體上的直接訊息或電子郵件傳送連結或惡意檔案附件給可能的受害者。

除了企業員工之外，CERIUM 還廣泛鎖定南韓國軍事成員，並且特別關注南韓軍事學校和從事學術工作的軍事成員。

鎖定加密貨幣以平衡損失

自聯合國於 2016 年對北韓實施制裁以來，北韓的經濟便持續萎縮，加上天災（如洪水[44] 和乾旱[45]）以及 2020 年初爆發 COVID-19 全球疫情以來幾乎完全封鎖邊境停止進口，使得經濟情況雪上加霜。[46] 儘管北韓於 2022 年初開放邊境與中國進行貿易，但很快又再次關閉。[47] 5 月中，北韓通報了第一例 COVID-19 國內病例。[48] 此後便採行了中國式大規模封鎖的「COVID 清零」政策來對抗病毒，但此舉卻對北韓已然岌岌可危的經濟造成了負面衝擊。

北韓國家級組織 COPERNICIUM 試圖利用從能夠侵入其網路的任何公司竊取金錢（通常是加密貨幣）來彌補部分收益損失。我們在美國、加拿大、歐洲和整個亞洲都發現了數十台屬於加密貨幣相關公司的電腦遭到入侵。COPERNICIUM 甚至入侵了北韓最強大盟友，也就是中國所屬的加密貨幣相關公司的電腦，包括中國本土和香港。該組織大量倚賴社交媒體作為早期偵察和接近目標的方法。行為體會建立個人資料來假冒與加密貨幣相關的企業內的開發人員或資深主管。接著與業界人士建立關係，而一旦建立密切關係後，就會傳送惡意連結或檔案。

北韓運用網路能力實現政權當局的三大目標

續

一個與 PLUTONIUM 相關的組織負責開發和部署勒索軟體

Microsoft 以 DEV-0530 追查一個來自北韓的行為體組織，該組織在 2021 年 6 月開始開發並使用勒索軟體發動攻擊。這個自稱為 H0lyGh0st 的團體早在 2021 年 9 月就已利用同名的勒索軟體承載從事活動，並成功入侵了許多國家的小型企業。

Microsoft 評估，DEV-0530 與另一個作為 PLUTONIUM（也稱為 DarkSeoul 或 Andariel）追查的北韓境內組織有關。雖然在活動中使用 H0lyGh0st 勒索軟體是 DEV-0530 獨特的手法，但 MSTIC 觀察到了兩個組織之間的通訊，以及 DEV-0530 使用由 PLUTONIUM 專門製作的工具。

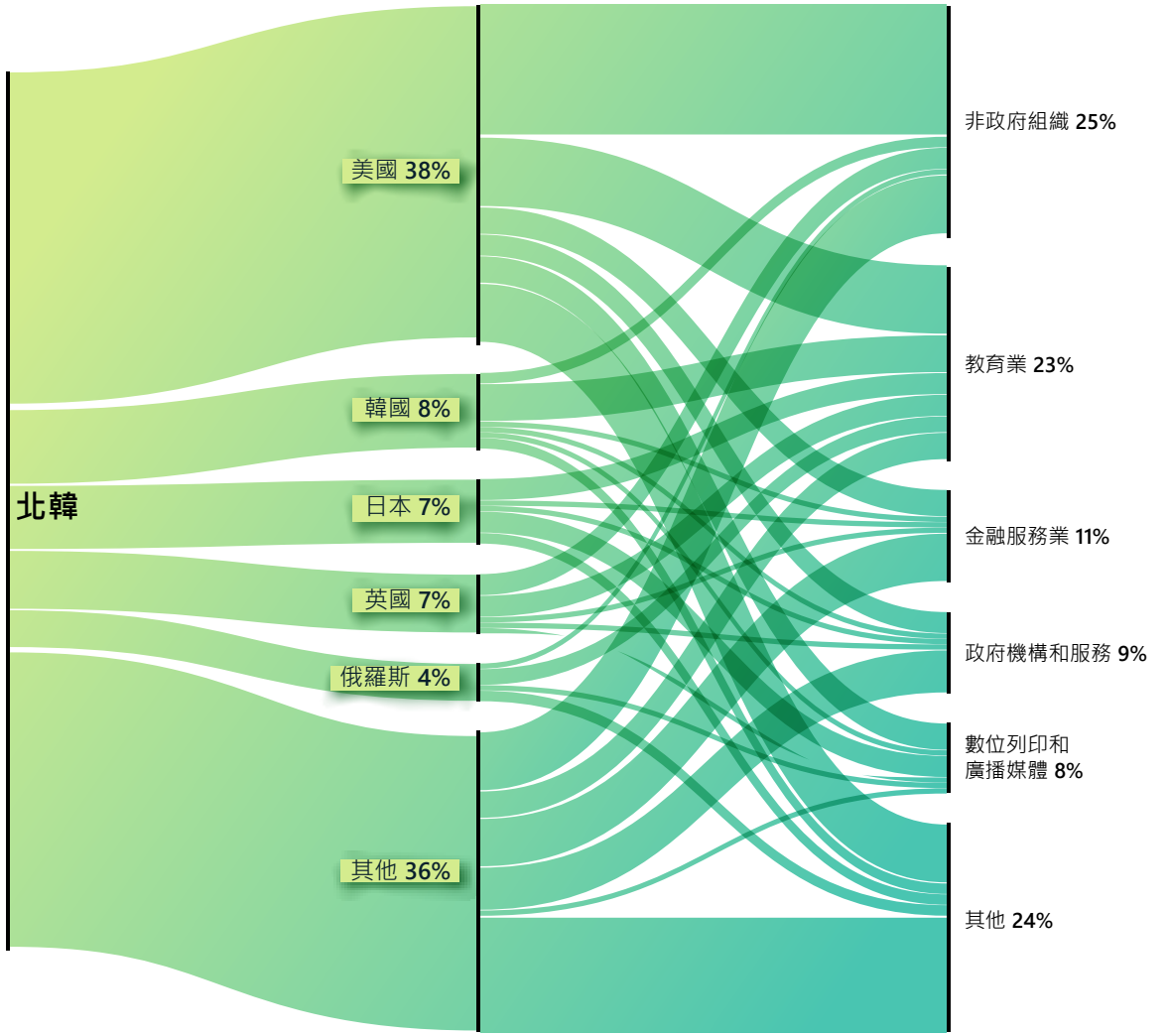
目前還不確定 DEV-0530 活動是否由政府贊助。儘管出於贊助竊取加密貨幣公司的相同理由，勒索軟體攻擊很可能是由政府下令發動，但是 DEV-0530 背後的行為體也可能是單獨行動，目的只為了賺錢。如果是北韓駭客的單獨行動，就可解釋為何相較於政府贊助的加密貨幣公司竊取行動，該活動的規模並不大。

鎖定北韓的新聞機構、脫北者、宗教團體和救援組織為目標

在過去一年，最高領導人金正恩在公開場合更加關注內部安全性與忠誠度，而不是飛彈和核武。為了反映對這種內需問題的關注，至少有兩個北韓國家級組織將重點放在政權當局視為國內威脅的各層面。

第一個是 Microsoft 作為 DEV-0215 追查的組織，其目標是密切關注北韓新聞的媒體組織。這種目標鎖定的可能原因之一，就是這些媒體機構的新聞來源是脫北者、與北韓密切往來的中國公民，甚至是北韓境內的一些公民，他們會透過各種手段與外界通訊。北韓政府認為，這些組織是生存上的威脅，尤其北韓境內的公民會被視為賣國賊和間諜。DEV-0215 可能試圖找出這些機構來源，以便消除潛在的資訊洩漏。

北韓：最主要的目標國家和行業別



北韓將美國、南韓及日本視為主要敵手。雖然俄羅斯是長期盟友，但北韓威脅行為體仍會鎖定俄羅斯智庫、學術人員及外交官員為目標，以取得有關俄羅斯對全球事務看法的情報。

北韓運用網路能力實現政權當局的三大目標

續

Microsoft 也看到了 DEV-0215 鎖定韓語基督教社群為目標的證據。基督教福音派韓語教會往往會批評北韓和南韓政府進行有利北韓的互動。這些教會很可能與脫北者接觸，有些也會參與北韓的人道主義工作。北韓將他們視為威脅，因為即使在全球疫情期間，脫北者從北韓逃離的路線幾乎中斷[49]，但是這些基督教團體經常扮演協助脫北者逃離的重要角色。DEV-0215 製作了有關基督教聚會的假文件，作為以韓語人士為對象的誘餌，鎖定該團體為目標並找出協助安排投誠的人。

最後，國家級組織 OSMIUM 一整年持續關注國際救援組織，包括過去協助過北韓的組織在內。雖然北韓始終迴避外國的協助提議，尤其自 COVID-19 疫情爆發以來更是如此[50]，但北韓可能考慮接受協助提議，卻對允許外國救援工作者進入國內的安全後患感到憂心。本含可能侵入全世界援助組織的網路，以判斷是否允許該援助進入其國內。

可付諸行動的見解

1. 北韓國家級行為體技術純熟、毫不留意且富有創造力，但組織仍可以防禦他們。
2. 即使最成功的攻擊也能透過基本的網路檢疫阻止，例如雙因素驗證，或是在虛擬環境中，不要開啟不明人士傳送的附件。

進一步資訊的連結

- 北韓威脅行為體利用 H0lyGh0st 勒索軟體鎖定中小企業為目標 | Microsoft 威脅情報中心 (MSTIC)、Microsoft 數位安全部門 (DSU)

在北韓方面的專家之間，長期以來一直持續爭論北韓政府是認真看待公開聲明的內容，還是表態做樣子而已。與北韓聲稱的優先事項一致的網路攻擊，證實了相信北韓公開聲明其目標時，會說到做到的一方。

網路傭兵威脅網路世界的和平穩定

著手開發並出售工具、技術和服務的私有企業產業正不斷成長，他們讓客戶 (通常是政府) 能夠闖入網路、電腦、手機和網路連線裝置。這些實體是國家級行為體的資產，經常危害持不同政見者、人權鬥士、新聞記者、公民社會擁護者和其他一般平民。我們將這些實體稱為網路傭兵或民間攻擊行為體。

民間企業可製造和出售網路武器的世界，對於消費者、各種規模的企業及政府機構來說更加危險。這些攻擊工具能使用的方式有許多種，而且與善治和民主的規範與價值相左。Microsoft 認為，保護人權是根本義務，我們藉由在全球減少「監視即服務」來表達我們的重視程度。

Microsoft 評估，在民主與威權政體中，某些國家級行為體向外尋求開發和利用「監視即服務」技術。他們利用這種方式規避責任和監督，以及獲得原本難以開發的能力。

這些網路武器為國家級行為體提供了他們無法單獨開發的監視功能。

網路傭兵營運的市場是不透明的。儘管如此，我們持續觀察到這些組織利用零時差攻擊，甚至零點擊攻擊，這種攻擊完全不需要受害者互動，就能實現監視即服務。

Microsoft 近期公告了一個歐洲民間攻擊行為體，我們稱為 KNOTWEED，是奧地利境內的 PSOA，稱為 DSIRF。有多則新聞報導指出，該公司與開發和試圖銷售稱為 Subzero 的惡意軟體工具組有關。[51] 受害者包括許多國家如奧地利、英國和巴拿馬境內的法律事務所、銀行和策略諮詢公司。[52]

由於這些攻擊性監視功能不再是國防和情報機構所建立的高度機密功能，而是現在提供給公司和個人的商業產品，因此任何網路武器的監管制度都需要超越出口管制。這些網路武器的影響可能極具破壞性。

當網路傭兵利用產品或服務中的漏洞時，會讓整個運算生態系統面臨風險。當漏洞公開確立時，公司將與時間賽跑，必須在廣泛攻擊發生之前發佈防護措施 (請參閱前面有關漏洞惡意探索的討論)。這對於軟體供應商 (必須迅速開發修補程式) 和產品消費者 (必須立即實作修補程式) 兩方面來說，都是既危險又困難的循環。

Microsoft 身為網路安全技術協議 [53] (由 150 多家科技公司共同組成的領導聯盟) 的創始成員，承諾不參與網路上的攻擊行動。我們遵守這項承諾，也在這個領域中履行我們的人權責任。我們參與了技術中斷和法律挑戰，以突顯網路傭兵提供的服務所造成的負面影響，並且在發現濫用行為時，繼續保護我們的客戶。

網路傭兵建立並提供技術複雜且普遍可得的「監視即服務」功能，包括先進的惡意軟體和各種不同的技術。

政府可付諸行動的見解

1. 針對監視即服務實現透明度和監督的要求，尤其在採購方面，包括禁止這些攻擊行為體，如同美國商務部將黑名單企業列入「實體清單」的做法一樣。
2. 對此部門離職員工制定離職後的限制。
3. 首先從履行「了解您的客戶」義務開始著手，並鼓勵企業堅守其人權承諾。

進一步資訊的連結

- 了解 KNOTWEED：利用 0 時差惡意探索的歐洲民間攻擊行為體 | Microsoft 威脅情報中心 (MSTIC)、Microsoft 安全回應中心 (MSRC)、RiskIQ (Microsoft Defender 威脅情報) (英文)
- 繼續打擊民間網路武器 | Microsoft 問題焦點 (英文)

實施網路安全規範以維護網路世界的和平與安全

我們急需一致的全球架構，以優先處理人權和保護人們不受網路上魯莽國家的行為迫害。這點在烏克蘭持續的戰事當中更清楚展現。除了全球策略的努力之外，各國政府現在還可以用行動帶來立即的正面影響。

五年前，Microsoft 呼籲訂定「數位日內瓦公約」(Digital Geneva Convention) 以促進跨領域的責任和義務來捍衛網路和平與安全。網路環境逐漸成為各國之間衝突與競爭的獨特且動盪的領域，攻擊變得更加普遍，即使在和平時期也一樣。

如今，從俄羅斯入侵行動中，俄羅斯對烏克蘭發動的網路攻擊就能清楚證明，這樣的架構顯然有其必要性。這場戰事闢出了一個新戰場，顛覆了我們以往所知的一切。

若要為網路環境帶來和平，將會需要強化和重新打造全球治理機構，讓它們與時俱進。網路環境與其他領域有著根本上的差異，它無邊無界、人造合成，而且主要由民營產業所維護。這意味著要求科技業對產品與服務的安全性，甚至規模更大的數位生態系統承擔更大的責任。雖然所有領域都有明顯的進展，但挑戰也大幅增加。

我們必須加倍共同努力，保衛網路環境的安全。我們不能將我們期望從網路上得到的權利和自由視為理所當然。當我們努力應付挑戰時，惡意行為體也正在規劃下一次的攻擊方式和地點，使用 AI、利用假資訊，並尋找方法來破壞剛起步的元宇宙。人權鬥士、科技業和尊重權利的政府必須共同努力，實現安全有保障的網路世界的希望願景。未來的道路雖然漫長，但政府現在就可採取多種行動來立即改善網路安全生態系統：

- 引用規範、法律和後果來歸因。過去五年中的一項重大改進，就是政府咎責網路攻擊的速度和協調過程。這些聲明不只是點名和指責，還需要突顯違反了哪些國際法或規範，以及將要承擔哪些後果，以協助鞏固國際間期望的認可。
- 明確對國際法釋義。雖然各國政府同意國際法適用於網路，但問題在於如何在特定實例當中應用。這尤其與烏克蘭遭入侵的善後工作有關。各國政府能夠努力不懈地設定期望值、避免誤解，並聲明自己如何理解遵循國際法所應盡的義務來建立信任。
- 諮詢其他利益關係人。國際論壇持續探索促進健全的多方關係人包容性的最佳方式，各國政府可透過諮詢多方關係人社群 (尤其是科技業) 來支持明智的對話，確保對話受益於具備寶貴專業知識的人。
- 組成常設機構，以支援網路環境中負責任的國家級行為。國際外交論壇在推動負責任的網路國家級行為方面的重要性前所未見。顯然需要一套永久的聯合國機制，將網路環境視為衝突領域來處理。
- 定義新規範來對抗不斷演進的威脅。網路環境的威脅會隨著技術創新而不斷進化。雖然國際規範應保持技術性中立，但也需要根據威脅形式的改變以及我們使用技術的方式而更新和細部修訂。即使在今天，我們也看到現有國際架構中的落差遭到濫用。各國應承諾明確保護支撐數位生態系統但目前未受保護的核心程序，像是軟體更新程序。此外，某些特定領域值得額外的保護。例如，正如我們在全球疫情下所學到的，保護醫療保健的規範至關重要。

國家級行為體和攻擊的數量與複雜性不斷增加，使得情況難以維持。

立即行動勢在必行，政府現在就可採取多種行動來立即改善網路安全生態系統，包括在網路環境中針對國家級行為實施達成共識的規範和規則，以及擴大與多方關係人社群合作，共同解決新出現的差距。

必須重新打造多邊機構，以因應國家級網路攻擊的巨大挑戰。

進一步資訊的連結

- 抉擇的時刻：需要強大的全球網路安全應變能力 | Microsoft 問題焦點 (英文)
- 必須阻止鎖定醫療保健的網路攻擊 | Microsoft 問題焦點 (英文)
- 聯合國的網路外交下一篇章召喚著我們 | Microsoft 問題焦點 (英文)

章節附註

1. https://www.microsoft.com/en-us/cybersecurity/content-hub/cloud-security
2. https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks/
3. 3 本章中的重大基礎設施依照美國第 21 號總統政策指令 (PPD-21)，重大基礎設施的安全性與韌性 (2013 年 2 月) 所定義。
4. https://www.microsoft.com/security/blog/2021/11/18/iranian-targeting-of-it-sector-on-the-rise/
5. https://www.microsoft.com/security/blog/2022/06/02/exposing-polonium-activity-and-infrastructure-targeting-israeli-organizations/
6. https://www.microsoft.com/security/blog/2021/10/25/nobelium-targeting-delegated-administrative-privileges-to-facilitate-broader-attacks/
7. https://www.microsoft.com/en-us/security/business/identity-access/azure-active-directory-passwordless-authentication
8. https://www.solarwinds.com/trust-center/security-advisories/cve-2021-35211
9. https://pitstop.manageengine.com/portal/en/community/topic/adselfservice-plus-6114-security-fix-release
10. https://reliefweb.int/report/ukraine/unicef-ukraine-humanitarian-situation-report-no-13-10-17-may-2022
11. https://news.un.org/en/story/2022/06/1119672
12. https://zetter.substack.com/p/dozens-of-computers-in-ukraine-wiped?s=r ; https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/
13. https://www.cnn.com/2022/03/14/economy/china-jan-feb-economy-challenges-ahead-intl-hnk/index.html
14. https://www.wsj.com/articles/russias-vladimir-putin-meets-with-chinese-leader-xi-jinping-in-beijing-11643966743
15. https://www.washingtonpost.com/world/2022/04/01/china-eu-summit/
16. https://twitter.com/MoNDefense
17. https://news.usni.org/2022/01/24/2-u-s-aircraft-carriers-now-in-south-china-sea-as-chinese-air-force-flies-39-aircraft-near-taiwan
18. https://ec.europa.eu/trade/policy/in-focus/eu-china-agreement/; https://www.usnews.com/news/world/articles/2022-02-28/eu-plans-summit-with-china-on-april-1-to-address-tensions
19. https://www.wsj.com/articles/u-s-on-sidelines-as-china-and-other-asia-pacific-nations-launch-trade-pact-11641038401
20. https://greenfdc.org/chinas-two-sessions-2022-what-it-means-for-economy-climate-biodiversity-green-finance-and-the-belt-and-road-initiative-bri/
21. https://www.cfr.org/global-conflict-tracker/conflict/territorial-disputes-south-china-sea
22. https://www.theguardian.com/world/2022/apr/30/the-china-solomons-security-deal-has-been-signed-time-to-move-on-from-megaphone-diplomacy
23. https://www.fmprc.gov.cn/eng/zxxx_662805/202205/t20220531_10694928.html
24. https://blogs.microsoft.com/on-the-issues/2021/12/06/cyberattacks-nickel-dcu-china/; https://www.microsoft.com/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe/
25. https://www.microsoft.com/security/blog/2022/04/12/tarrask-malware-uses-scheduled-tasks-for-defense-evasion/
26. https://attack.mitre.org/techniques/T1053/
27. https://www.microsoft.com/security/blog/2022/07/26/malicious-iis-extensions-quietly-open-persistent-backdoors-into-servers/
28. https://www.microsoft.com/security/blog/2021/02/11/web-shell-attacks-continue-to-rise/
29. https://www.timesofisrael.com/in-rare-criticism-of-irgc-rouhani-slams-anti-israel-slogans-on-test-missiles/; https://www.theguardian.com/world/2017/may/05/iran-president-hassan-rouhani-nuclear-agreement-sabotaged; https://d2071andvip0wj.cloudfront.net/184-iran-s-priorities-in-a-turbulent-middle-east_1.pdf; https://www.aljazeera.com/news/2016/3/9/iran-launches-ballistic-missiles-during-military-drill; https://www.usatoday.com/story/news/world/2015/04/25/iran-yemen-weapons/26367493/; https://www.armscontrol.org/blog/ArmsControlNow/2016-03-14/The-Iranian-Ballistic-Missile-Launches-That-Didnt-Happen; https://www.reuters.com/world/middle-east/iran-parliament-approves-most-raisi-nominees-hardline-cabinet-2021-08-25/;
30. https://www.reuters.com/world/middle-east/iran-parliament-approves-most-raisi-nominees-hardline-cabinet-2021-08-25/; https://www.france24.com/en/live-news/20210825-iran-s-parliament-approves-president-s-cabinet-choices

章節附註續

31. https://www.janes.com/defence-news/news-detail/iranian-irgc-consolidates-primacy-inintelligence-operations; https://www.proofpoint.com/us/blog/threat-insight/badblood-ta453-targets-us-and-israeli-medical-research-personnel-credential; https://miburo.substack.com/p/iran-disinfo-privatized?s=r.
32. https://www.reuters.com/business/energy/iran-says-israel-us-likely-behind-cyberattack-gas-stations-2021-10-30/
33. https://www.tasnimnews.com/en/news/2021/11/05/2602361/us-military-action-off-the-table-iranian-general
34. 特別是指修補適用 ProxyShell 的 Exchange 伺服器漏洞 (CVE-2021-26855、CVE-2021-26857、CVE-2021-26858 和 CVE-2021-27065、CVE-2021-34473)。此外，務必修補有漏洞的 Fortinet FortiOS SSL VPN 設備。
35. https://docs.microsoft.com/en-us/microsoft-365/commerce/manage-partners?view=o365-worldwide
36. https://www.microsoft.com/security/blog/2022/06/02/exposing-polonium-activity-and-infrastructure-targeting-israeli-organizations/
37. https://www.microsoft.com/security/blog/2022/06/02/exposing-polonium-activity-and-infrastructure-targeting-israeli-organizations/
38. https://www.secureworks.com/blog/lyceum-takes-center-stage-in-middle-east-campaign
39. https://www.microsoft.com/security/blog/2021/11/18/iranian-targeting-of-it-sector-on-the-rise/
40. https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/manage-updates-baselines-microsoft-defender-antivirus?view=o365-worldwide
41. https://docs.microsoft.com/microsoft-365/security/defender-endpoint/cloud-protection-microsoft-defender-antivirus
42. https://docs.microsoft.com/microsoft-365/commerce/manage-partners?view=o365-worldwide
43. https://www.marketwatch.com/story/kim-jong-un-calls-for-improved-living-conditions-in-north-korea-01633920099
https://www.bbc.com/news/world-asia-59845636
https://kcnawatch.org/newstream/1650963237-449932111/respected-comrade-kim-jong-un-makes-speech-at-military-parade-held-in-celebration-of-90th-founding-anniversary-of-kpra/
44. https://www.theguardian.com/world/2021/aug/06/north-korea-homes-wreckeddamaged-and-and-bridges-washed-away-in-floods
45. https://www.reuters.com/world/asia-pacific/nkorea-mobilises-office-workers-fight-drought-amid-food-shortages-2022-05-04/
46. https://www.washingtonpost.com/world/asia_pacific/north-korea-kim-pandemic/2021/09/08/31adfd74-ff53-11eb-87e0-7e07bd9ce270_story.html
47. https://news.yahoo.com/china-halts-freight-train-traffic-102451425.html
48. https://www.cnn.com/2022/05/11/asia/north-korea-covid-omicron-coronavirus-intl-hnk/index.html
49. https://www.csis.org/analysis/number-north-korean-defectors-drops-lowest-level-two-decades
50. https://www.aljazeera.com/economy/2022/5/20/north-korea-shuns-outside-help-as-covid-catastrophe-looms
51. Jan-Philipp Hein，在怪異間諜軟體之謎中，蹤跡經由 Wirecard 引導至克里姆林宮，FOCUS Online (2022)，https://www.focus.de/politik/vorab-aus-dem-focus-volle-kontrolle-ueber-zielcomputer-das-raetsel-um-die-spionage-app-fuehrt-ueber-wirecard-zu-putin_id_24442733.html；Sugar Mizzy，我們推出來自奧地利的「Subzero」邦特洛伊木馬程式 (2021 年)，https://europe-cities.com/2021/12/17/we-unveil-the-subzero-state-trojan-from-austria/；Andre Meister，我們推出來自奧地利的「Subzero」邦特洛伊木馬程式，Netzpolitik.org (2022 年)，https://netzpolitik.org/2021/dsirf-wir-enthuellen-den-staatstrojaner-subzero-aus-oesterreich。
52. 如同我們在技術部落格中指出，確認某一國家 / 地區的目標不一定表示 DSIRF 客戶位於同一國家 / 地區，因為跨國目標鎖定很常見。
53. 首頁 | 網路安全技術協議 (cybertechaccord.org)

裝置和基礎結構

隨著數位轉型加速，數位基礎結構的安全性比以往更加重要。

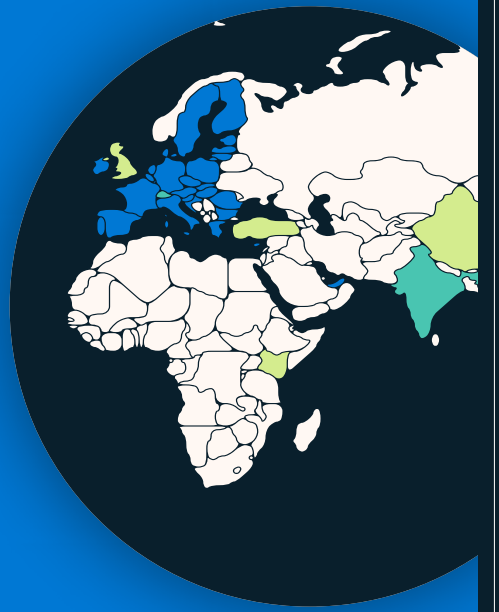
概觀

裝置和基礎結構

在全球疫情之下，加上迅速採用各種面向網際網路的裝置成為加速數位轉型的一部分，大大增加了數位世界的攻擊面。

網路罪犯和各國都在迅速利用它。雖然近年來 IT 硬體和軟體的安全性已增強許多，但物聯網 (IoT) 和營運技術 (OT) 裝置的安全性仍無法跟上腳步。威脅執行者正利用這些裝置在網路上建立存取權並進行橫向移動，在供應鏈中打造立足點，或中斷目標組織的 OT 營運。

世界各國政府都轉為藉由改善 IoT 和 OT 安全性來保護重大基礎設施。

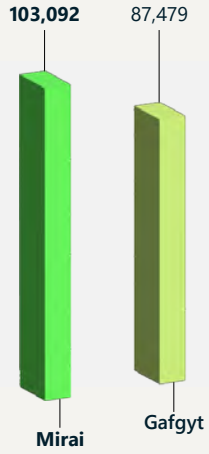


深入了解，前往 p59

需要全球一致且可互通的安全性政策，才能確保廣泛採用。

深入了解，前往 p59

惡意軟體即服務已轉向對基礎設施和公用事業以及企業網路中的 IoT 和 OT 採取大規模行動



深入了解，前往 p63

對遠端管理裝置的攻擊不斷增加，在 2022 年 5 月便觀察到超過 1 億次攻擊，比過去一年增加了五倍。

深入了解，前往 p62

攻擊者越來越常利用 IoT 裝置韌體中的漏洞來滲透企業網路並發動破壞性攻擊。

深入了解，前往 p65

據分析，有 32% 的韌體映像包含至少 10 個已知的重大漏洞。

深入了解，前往 p66

前言

加速數位轉型使得重大基礎設施和網路實體系統的網路安全風險提高。

過去幾年以來，我們看到數位世界發生了前所未有的變化。組織不斷進化，以期從智慧雲端和智慧邊緣納入運算功能的進展。全球疫情迫使實體必須數位化才得以生存，加上全世界所有產業採用面向網際網路裝置的速度，使得數位世界的受攻擊面呈指數增加。

這種快速變遷已讓安全性社群沒有能力跟上步調。在過去一年，我們觀察到組織內各個角落都有惡意利用裝置的威脅，從傳統 IT 設備到營運技術 (OT) 控制器，甚至是簡單的物聯網 (IoT) 感應器。雖然近年來 IT 設備的安全性已增強許多，但 IoT 和 OT 裝置安全性仍無法跟上腳步。威脅執行者正利用這些裝置在網路上建立存取權並進行橫向移動，或中斷組織的 OT 營運。我們看到了對電網的攻擊、勒索軟體攻擊導致 OT 營運中斷、IoT 路由器遭到利用來增加持續性，以及鎖定韌體中漏洞為目標的攻擊。

雖然 IoT 和 OT 漏洞普遍存在對於所有組織來說是一大挑戰，但是重大基礎設施的風險也逐漸升高，因為威脅執行者已得知，停用關鍵服務會是相當有力的控制手段。2021 年對 Colonial Pipeline Company 進行的勒索軟體攻擊，展現了犯罪分子如何中斷關鍵服務來提高支付贖金的可能性。而俄羅斯對烏克蘭發動的網路攻擊顯示，部分國家為了達到其軍事目的，將針對重大基礎設施的網路攻擊視為可接受的破壞行為。

然而，希望就在前方。政策制定者和網路防禦者正採取行動改善重大基礎設施的網路安全性，包括它們所依賴的 IoT 和 OT 裝置。政策制定者正加速制定法律和法規，以建立大眾對於重大基礎設施和裝置網路安全的信任。

Microsoft 正與世界各地的政府機構合作，將把握這個機會強化網路安全，同時我們也歡迎各方的參與。然而，另我們憂心的是，不一致、客製化或複雜的需求可能產生非預期的作用，包括在某些情況下，將有限的安全性資源轉換成遵循多項重複認證而導致安全性降低。

從安全性作業的立場來看，網路防禦者會採行多種方法來改善組織的 IoT/OT 安全性態勢。其中一種方法是對 IoT 和 OT 裝置實施持續監視。另一種方法是「左移」，意思是針對 IoT 和 OT 裝置本身要求並實施更好的網路安全做法。第三種方法是實施跨 IT 和 OT 網路的安全性監視解決方案。這種整體方法對於促進關鍵組織流程帶來相當大的附加益處，例如「打破 OT 和 IT 之間的孤島」，進而讓組織達到更強化的安全性態勢，同時滿足業務目標。

Michal Braverman-Blumenstyk
副總裁暨雲端和 AI 安全性部門技術長

政府採取行動改善重大基礎設施的安全性與韌性

世界各國政府正制定並改進政策，以管理重大基礎設施的網路安全風險。有許多政府也制定政策來改善 IoT 和 OT 裝置的安全性。這波全球政策計畫浪潮不斷推升，創造了巨大的機會來強化網路安全性，但也對整個生態系統的利益關係人帶來挑戰。

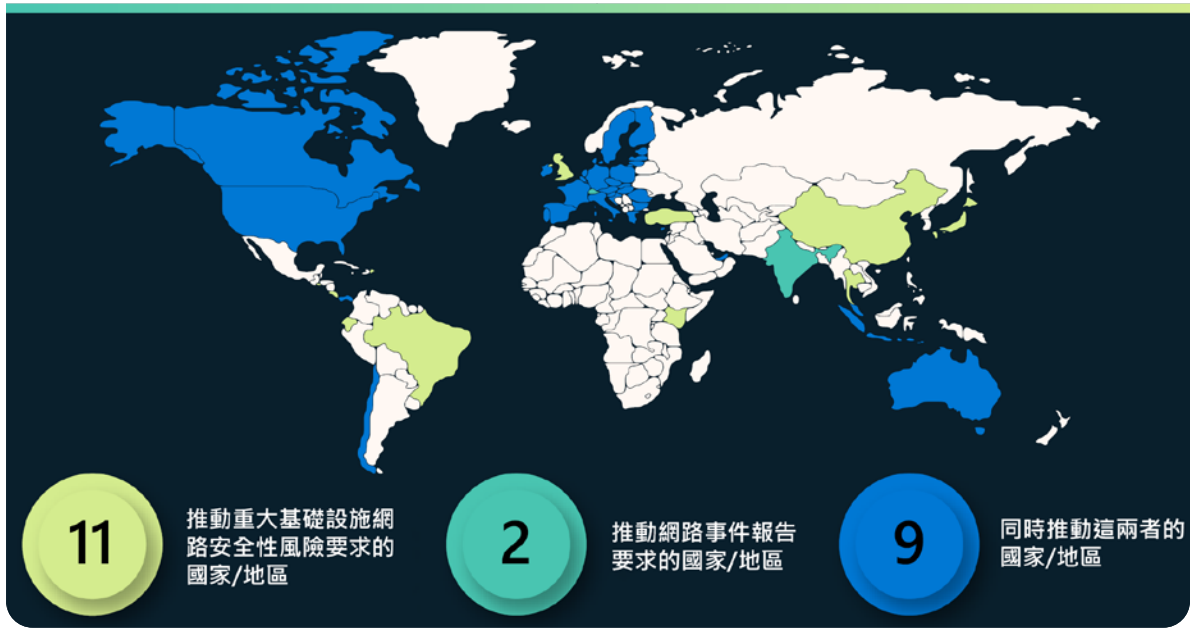
發展管理重大基礎設施網路風險的整體願景至關重要，卻也很複雜，尤其有鑒於技術和全球供應商之間的互連程度、技術用途和相關風險的範圍，以及同時投入短期和長期策略的需要。有效界定範圍的政策能推動反覆學習和改進，並支援全球、跨部門的互通性，因此有助於管理複雜性並實現更在乎安全的數位轉型。然而，零星的立法作為可能導致法規需求重疊且不一致。這可能會影響資源，最終破壞安性全目標。例如，組織可能將資源從創新和安全性轉向形式上的合規性做法。

Microsoft 尋求與世界各地的政府機構合作，以推行有效的重大基礎設施網路安全性政策、增進對挑戰和機會的了解，並支援強化共同風險態勢的作為。

重大基礎設施網路安全性風險管理的政策發展

在過去一年，包括澳洲、智利、歐盟 (EU)、日本、新加坡、英國 (UK) 和美國等多個司法管轄區都發展、更新或實施了跨領域或特定領域的網路安全性需求。[1] 當中許多政府 (以及其他如印度 [2] 和瑞士 [3]) 都已針對重大基礎設施和重要的服務提供者發出或正在發展網路安全性事件報告需求。[4]

過去一年，澳洲、EU、印尼和美國發生了一些值得注意的政策發展。澳洲制定了兩項法律，有助於管理跨部門的重大基礎設施網路安全性風險。除此之外，法律還指定新的重大基礎設施領域，要求制定風險管理計劃、要求網路安全性事件報告，以及讓政府有權在判定重大基礎設施業者不願意或無法適當回應事件時介入。



EU 努力更新其 2016 年 NIS 指令，該指令為 EU 成員國提供了一個架構，用來規範視為對經濟和社會運作至關重要的技術服務和產品。提議的 NIS 2 包括修訂，將制定一個新的重大數位基礎設施類別、增加對網路事件報告的需求，並施加額外的網路安全性風險管理需求。EU 同時也發展了對其數位營運韌性管制框架法案 (DORA) 的建議更新，為金融服務部門所使用的資訊通訊技術創造了新的需求。

印尼在 5 月發布了一項有關保護重要資訊基礎設施 (「IIV」) 的法規，將於 2024 年 5 月生效，涵蓋了能源、交通運輸、金融和醫療保健等行業。印尼的法規目標是保護 IIV 實施的持續性、防止網路攻擊，並增加處理網路事件的整備度。IIV 提供者將負責進行安全可靠的保護、實施有效的網路風險管理，以及向對應的政府機構報告網路風險結果。該法規包括要求在 24 小時內報告網路事件。

政府採取行動改善重大基礎設施的安全性與韌性

續

美國國會通過了一項法律，授權網路安全暨基礎設施安全局 (CISA) 發佈法規，要求重大基礎設施業者通報網路事件，同時美國運輸安全管理局 (TSA) 也針對交通運輸業發出了新的產業特定網路安全性需求。在 2021 年，TSA 針對有害液體和天然氣管線業者發佈了兩項安全指令，以因應 Colonial Pipeline Company 遭受的勒索軟體攻擊：

- 第一項指令要求業者指定網路安全協調員，在 12 小時內通報網路事件，並對其系統進行漏洞評估。
- 第二項指令是 TSA 在 2022 年所修訂，要求業者實施具體的緩解措施，以防範勒索軟體攻擊和其他針對 IT 和 OT 系統的已知威脅，在 30 天內制定並實施網路安全應變和回應計劃，以及每年審查網路安全性架構設計。

基於針對管道的法規，TSA 在 2021 年稍後再發佈了另外兩項安全性指令，對鐵道運輸、旅客鐵路運輸業者，或鐵路和公共運輸系統頒布網路安全性需求。這些指令要求涵蓋的業者指定網路安全協調員，在 24 小時內通報網路安全性事件，制定並實施網路安全性事件應變計劃，以及完成網路安全性漏洞評估。TSA 同時宣佈，另外更新了航空安全計畫，要求機場和航空公司執行前兩項規定，也就是指派協調員，以及在 24 小時內通報事件。

IoT 和 OT 裝置安全性的政策發展

有數十個國家 / 地區的政府積極發展需求，以提升包括 IoT 和 OT 裝置在內的資訊與通訊技術 (ICT) 產品和服務的網路安全性。在 ICT 產品與服務環境中，最大的隱憂就是軟體供應鏈安全性和 IoT 安全性。

- 歐盟提出了網路韌性法案，針對獨立軟體和連線裝置以及輔助服務建立網路安全性需求。[5] 軟體廠商的相關做法包括利用安全的軟體開發生命週期 [6] 及提供軟體物料清單。[7] 新的安全性需求將適用於連線裝置，並且所有製造商都應負責管理已發行產品的協調漏洞揭露流程 [8]。

政策制定者也將注意力集中在 IoT 裝置和聯網 OT 裝置的持續激增。

- 在英國，《產品安全及電信基礎設施法案》草案將要求消費者連線產品 (如智慧電視) 的製造商停止使用容易成為網路罪犯目標的預設密碼，建立漏洞揭露原則 (例如收到安全缺陷通知的方式)，以及公開其提供安全性更新所需的最短時間。[9]
- 歐盟正透過多項立法文件實施新的安全性標準或要求，包括無線電設備指令授權法，將應用到無線網路裝置，並尋求改善網路復原能力、保護消費者隱私權及降低金融詐騙的風險。[10] 此外，可能因實施 2019 年歐盟網路安全法 [12] 而必須使用目前發展中的雲端認證計劃 [11]。

一致性需求

在許多案例中，活動的範圍不斷追求跨區域、產業、技術及營運風險管理區域，導致尋求利用指導方針或展現合規性的組織面臨範圍、需求和複雜性方面可能重疊或不一致的情形若沒有普遍接受的 IoT 定義，那麼 IoT 和 OT 裝置法規的範圍更是一大挑戰。上述範例可能適用於「連線產品和輔助服務」、「消費者連線產品」及「無線網路裝置」。同時，許多政府旨在實施更健全的評估機制，以更了解組織和產品是否符合以及如何遵循目前、新出現及不斷進化的需求。隨著這些趨勢的融合，複雜性也將增加。令人振奮的是，歐盟網路韌性法案協商期間提出的問題，探討了新法規如何與現有的網路安全法規互動，表示有意避免網路安全性需求出現衝突。

以風險為基礎和成果或流程導向 (相對於具體實施) 的反覆運算方法能夠促進增強網路安全性與持續改進。同樣地，專注於實現跨產業、區域和政策領域的互通性，便能跨互聯的全球供應鏈一致提高網路安全性。

政府採取行動改善重大基礎設施的安全性與韌性

續

跨區域、產業和主題領域的發展中重大基礎設施網路安全性政策日益複雜。此活動帶來了巨大的機會和重大的挑戰。各國政府如何進行，將對數位轉型和整個生態系統安全性的未來有著至關重要的影響力。

加快軟體供應鏈安全性和零信任架構方面的整個生態系統投資

有關改善網路安全性的美國行政命令 (EO) 14028 一直扮演催化劑的角色，有助於加快 Microsoft 持續投資自有供應鏈和整個生態系統供應鏈安全性的計劃，並且讓客戶能夠實現零信任目標。

我們始終相信，若要增強軟體供應鏈，就需要分享學習經驗和最佳做法，我們早在 15 年前公開發行安全性開發生命週期便已開始這樣做。

此外，我們與國家網絡安全卓越中心密切合作，展示適用於內部佈署和雲端技術零信任架構做法，並建立新的產品功能，包括針對混合和多雲端環境強制實施防範網路釣魚驗證的能力。

如今，我們超越了 EO 的要求，證明符合軟體供應鏈安全性需求，並以兩種方式提供軟體物料清單 (SBOM) 資訊：

1. 第一種是，我們分享開放原始碼版本的 SBOM 產生器工具，建置此工具的目的在於輕鬆與 CI/CD 管道整合，以支援在 Windows、Linux、Mac、iOS 和 Android 平台上建置。[13]
2. 第二種是，我們投入供應鏈完整性、透明度和信任 (SCITT) 的產業標準開發工作。如此將能實現自動交換可驗證的供應鏈資訊，包括證明符合需求的成品，例如從 EO 軟體供應鏈指導方針產生的需求。

可付諸行動的見解

1. 必須重新打造多邊機構，以因應國家級網路攻擊的巨大挑戰。
2. 發展跨區域、產業和主題領域一致且互通的網路安全性政策。

進一步資訊的連結

- 持續投資供應鏈安全性，以支援網路安全性行政命令 | Microsoft 技術社群 (英文)
- 美國政府提出了 Zero Trust 架構策略和要求 | Microsoft 安全性部落格 (英文)
- 網路行政命令 | Microsoft Federal (英文)
- 供應鏈完整性、透明度和信任 | github.com (英文)
- 實施 Zero Trust 架構 | NCCoE (nist.gov) (英文)

IoT 和 OT 暴露：趨勢和攻擊

日益緊密相連的數位世界意味著裝置很快就連上網路、與規模更大的系統通訊、收集資料，並且創造出過去隱蔽空間的可見度。這為組織和威脅行為體帶來了機會，使得網路犯罪事業成為數十億美元的產業，同時也形成風險。

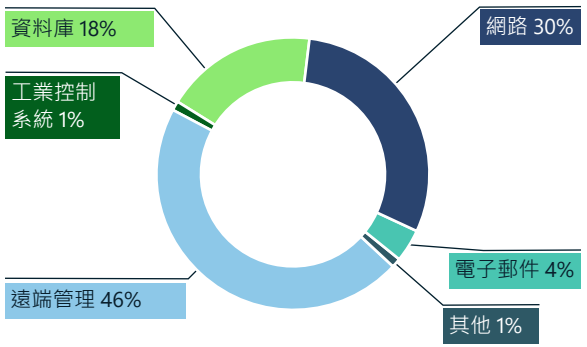
IoT 裝置（包括從印表機到網路相機、空調控制裝置及建築物門禁控制等所有一切）對個人、組織和網路都構成獨特的安全性風險。雖然對於許多組織的營運至關重要，但很快就會成為負擔和安全性風險。幾乎所有產業都快速採用 IoT 解決方案，同時使得攻擊媒介的數量和組織暴露的風險增加。

惡意軟體即服務已轉向對公眾基礎設施和公用設施（包括醫院、石油和天然氣、電網、交通運輸服務及其他重大基礎設施）以及企業網路採取大規模行動。威脅行為體需要進行大量的研究，才能發現和利用運作環境和嵌入式 IoT 和 OT 裝置的設定。

IoT 裝置會構成獨特的安全性風險，成為網路中的進入點和樞紐。有數百萬的 IoT 裝置未經修補或遭到暴露。

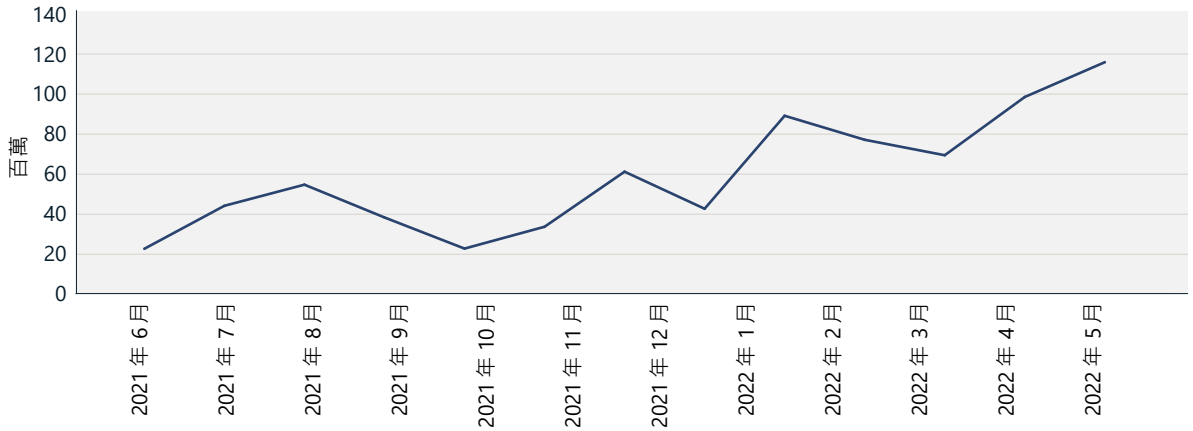
只要在開放網路連接埠上偵聽以找出服務，就可透過網際網路搜尋工具發現暴露的裝置。這些連接埠常用於裝置的遠端管理。若未正確保護，暴露的 IoT 裝置就可能成為進入另一層企業網路的樞紐，因為未經授權的使用者能夠從遠端存取連接埠。我們觀察到，有各種威脅行為體試圖利用在網際網路上暴露的裝置中的漏洞，這些裝置從相機、路由器到控溫器都有。然而，儘管存在風險，仍有數百萬部裝置未經修補或已暴露。

摘要整理 IoT/OT 上的攻擊類型



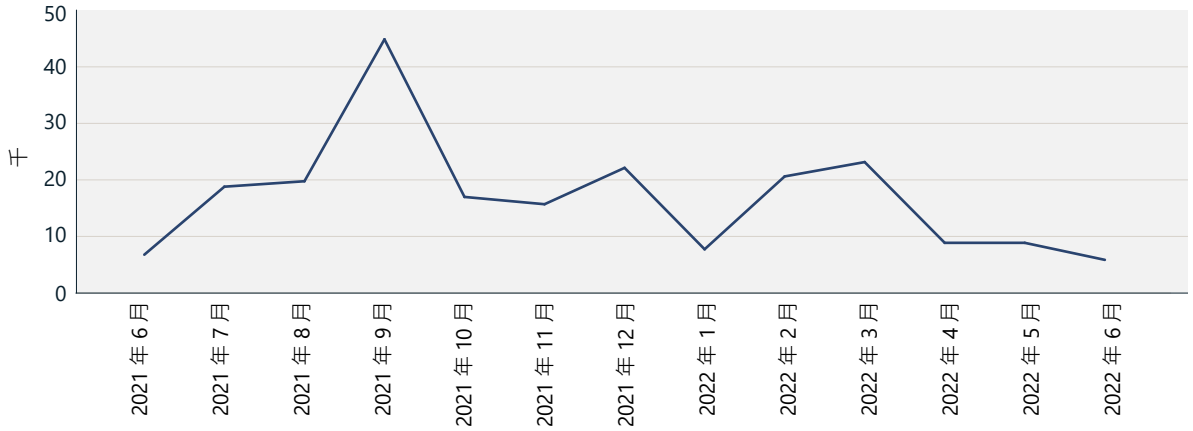
透過 MSTIC 感應器網路觀察到的攻擊類型。最普遍的是對遠端管理裝置的攻擊、透過網路發動的攻擊，以及對資料庫的攻擊（暴力破解或惡意探索）。

對遠端管理裝置的攻擊



隨時間增加對遠端管理連接埠的攻擊，如 MSTIC 感應器網路上所見。

針對 IoT 和 OT 的網路攻擊



一段時間的網路攻擊量，如 MSTIC 感應器網路所見。隨著直接連線到網路的裝置數量持續減少，攻擊者最終可能會減少探查這些裝置。

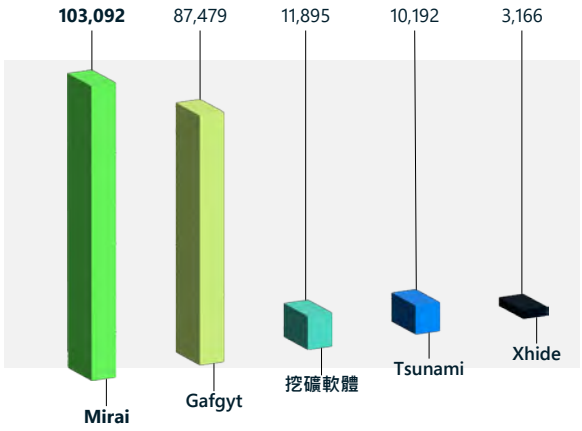
IoT 和 OT 暴露：趨勢和攻擊

續

改造過的惡意軟體公用程式

隨著網路犯罪集團不斷進化，其惡意軟體的部署和目標的選擇也與時俱進。在過去一年，我們觀察到對常見 IoT 通訊協定 (如 Telnet) 的攻擊大幅減少，在某些案例中減少達 60%。而同時，網路犯罪集團和國家級行為體重新利用了殭屍網路。惡意軟體 (如 Mirai) 持續存在，突顯了這些攻擊的模組化和現有威脅的適應能力。

環境中偵測到的前幾名 IoT 惡意軟體



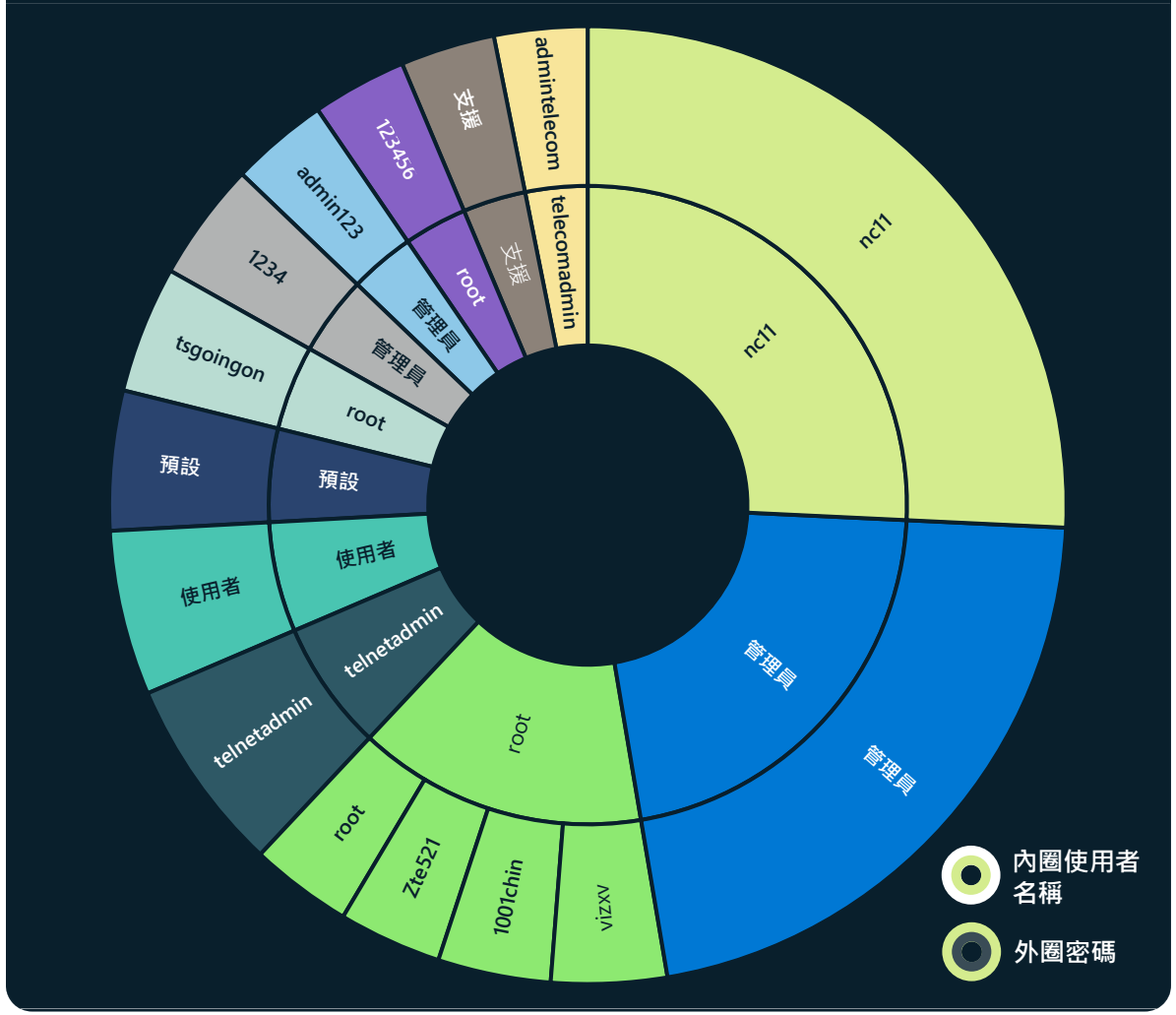
Mirai 進化後能感染更廣泛的 IoT 裝置，包括網際網路通訊協定相機、安防攝影機數位錄影機及路由器。攻擊媒介繞過了舊式安全性控制，並且利用其他漏洞和橫向移動對網路內的端點構成風險。Mirai 經過多次重新設計，其變種可適應不同的架構，並利用已知和零時差漏洞來入侵新的攻擊媒介。

在過去一年，Mirai 的使用在 32 位元和 64 位元 x86 CPU 架構中都已增加，且惡意軟體還有了國家級和犯罪集團能夠快速採用的新功能。現在國家級攻擊會在分散式拒絕服務 (DDoS) 攻擊中利用現有殭屍網路的新變種來對付外國對手。

隨著 2022 年對 IoT 裝置的攻擊獲利減少，我們觀察到有數個濫用漏洞 (如 Log4j 和 Spring4Shell) 的威脅行為體組織將惡意承載傳送至伺服器等裝置、進行感染，並招募成為大型殭屍網路的一員，用來執行 DDoS 攻擊。經改造的惡意軟體公用程式的目標是易受攻擊的 IoT 裝置，它會對組織和國家造成嚴重的影響，因為橫向移動可能會對其他承載和網路上的其他裝置暴露後門。

許多工業控制系統通訊協定未受監視，因此容易遭受專門針對 OT 的攻擊。這可能表示重大基礎設施的風險增加。

在為期 45 天的感應器訊號中 IoT/OT 裝置上看到的使用者名稱和密碼配對相對普遍程度



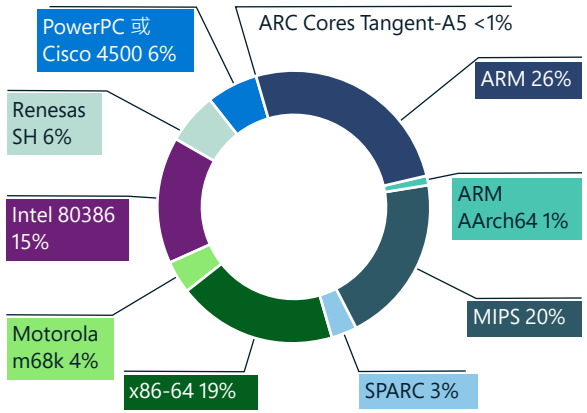
使用常見的使用者名稱和密碼配對會增加入侵的風險。根據規模超過 3900 萬部 IoT 和 OT 裝置的取樣，使用相同使用者名稱和密碼的裝置約佔了 20%。

IoT 和 OT 暴露：趨勢和攻擊

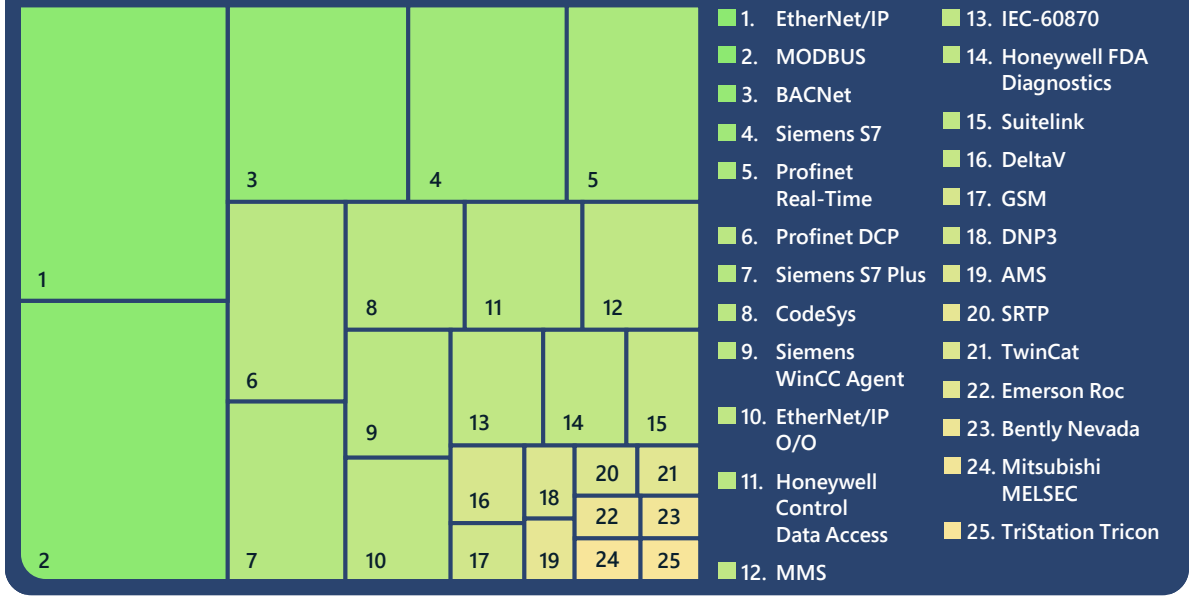
續

雖然脆弱的設定和預設認證仍對網路構成風險，但 Microsoft 觀察到許多網路上的惡意探索是利用 HTTP。我們觀察到這種情況在使用舊式殭屍網路對 Web 服務發動的攻擊中有增加的趨勢。同時，網際網路上開放 telnet 連接埠的數量減少，這對於網路安全來說是正面徵兆，因為過去對裝置構成風險的殭屍網路正逐漸失去相關性。儘管開放 telnet 連接埠數量減少，我們仍觀察到感應器網路中持續存在殭屍網路。

不同 CPU 架構的 IoT 惡意軟體分佈情形



工業控制系統通訊協定的普遍現象



Microsoft 觀察到，執行 ARM 的 IoT 裝置最容易成為惡意軟體攻擊的目標，其次是 MIPS、X86-64 和 Intel 80386 CPU。

工業控制系統通訊協定的漏洞

我們從雲端連線感應器深入查看 OT 資料，發現了最常見的工業控制系統 (ICS) 通訊協定。這些通訊協定可深入洞悉這些裝置的本質及其受攻擊面。尤其與重大基礎設施的安全性息息相關。這裡分享一些學到的重要經驗：

1. 呈現的大多數通訊協定都是專用，因此標準 IT 監視工具無法在這些裝置和通訊協定之間擁有充分的安全性可見度。因此，網路未受監視，而且更容易遭受專門針對 OT 的攻擊。
2. 有大量各種不同的廠商專屬通訊協定。這表示，廠商專屬安全性解決方案將無法充分涵蓋整個網路。Microsoft 優先採取無關廠商的方法，為廣泛的各種不同裝置提供安全性保護。
3. 組織應確保這些通訊協定不會直接從其網路暴露到網際網路上。由於這些通訊協定的漏洞和不安全的本質，這種暴露可能構成重大安全性風險。

Mirai 等惡意軟體會持續發展新功能，而且正由網路犯罪集團和國家級行為體所採用，在 DDoS 攻擊中利用現有殭屍網路的新變種來攻擊外國對手。

可付諸行動的見解

1. 藉由套用修補程式、變更預設密碼和預設 SSH 連接埠確保裝置健全。
2. 藉由消除不必要的網際網路連線和開放連接埠、封鎖連接埠以限制遠端存取、拒絕遠端存取，以及使用 VPN 服務來減少受攻擊面。
3. 使用 IoT/OT 感知網路偵測及回應 (NDR) 解決方案，以及安全性資訊與事件管理 (SIEM)/ 安全性協調流程和回應 (SOAR) 解決方案，以監控裝置中是否有異常或未經授權的行為，例如與陌生的主機通訊。
4. 分割網路以限制攻擊者在初始入侵後進行橫向移動和入侵資源的能力。IoT 裝置和 OT 網路應該透過防火牆與公司 IT 網路隔離。
5. 確保 ICS 通訊協定不會直接暴露於網際網路。

供應鏈和韌體駭客攻擊

幾乎每一部與網際網路連線的裝置都有韌體，也就是內嵌於裝置硬體或電路板中的軟體。在過去幾年中，我們看到鎖定韌體為目標發動破壞性攻擊的情況增加。由於韌體很可能持續是威脅行為體認為有價值的目標，因此組織必須保護韌體以防遭到駭客入侵。

韌體負責裝置的主要功能，像是連線到網路或儲存資料。舉凡企業 (IoT) 中使用的路由器、相機、電視和其他裝置，以及重大基礎設施使用的工業控制設備 (OT) 中都可找到韌體。在過去，韌體是使用不安全的程式碼編寫，因此製造了嚴重的漏洞，這些漏洞可能遭到利用，以進一步接管裝置或在韌體中植入惡意程式碼。

若是涉及供應鏈，這種風險便會加劇。大多數裝置都是使用許多製造商的硬體和軟體元件以及開放原始碼程式庫所建置。在許多情況下，裝置操作員無法查看硬體和軟體物料清單 (H/SBOM) 以評估其網路上裝置的供應鏈風險。2020 年 6 月，許多不同製造商使用的網路堆疊中發現了漏洞，影響了消費者和工業設備領域數億部 IoT 裝置。[14] 在某些案例中，網路堆疊會由其他廠商進行品牌重塑，且無法得知裝置是否容易受到攻擊。我們看到惡意行為體鎖定這個 IoT/OT 裝置硬體和軟體供應鏈為目標來入侵組織的威脅增加。

不同裝置的韌體更新程序會有很大的差異，而執行上的複雜度和後勤挑戰則影響著更新頻率。因為有時不一定能判斷裝置是否執行最新的韌體，使得安全性專業人員難以監視並確保其 IoT 和 OT 裝置的安全性態勢。此外，某些裝置的韌體並未以密碼編譯方式簽署，因此能夠在未經使用者驗證的情況下進行更新。這些弱點進一步讓裝置在生產和配銷鏈中更容易遭到供應鏈攻擊。

為了解決這些威脅，Microsoft 大量投資以確保韌體在供應鏈各階段移動時維持安全性和完整性，並隨時證明在擷取期間或過程中未遭到篡改。如此一來，我們就能驗證每個管道區段之間的信任，並針對我們出貨給客戶的每一個元件提供經認證且可證實的端對端監管鏈。我們與合作夥伴共同努力，將這項晶片到雲端的安全性帶給企業和 OT 網路上的所有裝置。

「ICT 基礎設施供應商成為目標的情況越來越普遍，因為他們能夠大量複製單一攻擊。同時，全球立法、法規和客戶對供應鏈安全性與復原能力的需求不斷增加，往往在他們的要求中出現分歧。

解決方法就是合作。Microsoft 與供應商和全球政府機構合作，共同致力於解決供應鏈生態系統的安全性，以期超乎客戶和監管機構的要求。為達此目的，我們正推動一套全面的方法來確保跨整個供應鏈彈性部署安全性和營運復原能力。

推動從設計到裝置運作的韌體完整性，是我們整體方法的關鍵所在。確保供應商的 SDL 流程並部署硬體根信任創新，正是我們「內建」供應鏈完整性的做法範例。

我們的社群利用涵蓋全新防篡改技術和加密機制的共同研究與開發，並結合持續監控和異常偵測。我們一起攜手進步，撕除被稱為供應鏈受攻擊面的標籤。」

Edna Conway，
副總裁暨雲端基礎結構部門安全與風險控管長

聚焦韌體漏洞

攻擊者越來越常利用 IoT 裝置韌體中的漏洞來滲透企業網路。與使用 XDR 代理程式找出弱點的傳統 IT 端點不同的是，IoT/OT 裝置內的漏洞識別更加難以捉摸。

在 Microsoft 和 Ponemon Institute 共同進行的一項近期調查中，突顯了企業中 IoT/OT 裝置的機會和安全性挑戰。[15] 雖然有 68% 的受訪者認為，採用 IoT/OT 對於其策略性數位轉型來說至關重要，但有 60% 的受訪者承認 IoT/OT 安全性是 IT/OT 基礎結構中最不安全的層面之一。

攻擊者利用 IoT 裝置韌體中的漏洞來滲透網路的範例，就是 Trickbot 特洛伊木馬程式，它利用 Mikrotik 路由器中的預設密碼和漏洞 [16] 來繞過企業防禦系統。IoT 裝置韌體面臨的基本挑戰，就是缺乏對裝置安全性態勢和漏洞的可見度。

雖然有可用於建置安全裝置的解決方案，但已有數十億部裝置進入市場並部署於企業中。這些稱為舊廠裝置。在 2021 年，Microsoft 收購了 ReFirm Labs，為舊廠裝置安全性帶來了一線希望，並且讓裝置製造商能夠改善其產品的安全性。ReFirm Labs 會分析裝置的二進位韌體映像，並製作有關潛在安全性弱點的詳細報告。[17] 這項技術將納入適用於 IoT 的 Microsoft Defender 未來的版本中。

在過去一年，我們檢驗了客戶掃描唯一韌體彙整的結果。雖然並非每一個發現的弱點都可能遭到利用，但它們突顯了裝置韌體安全性的基本挑戰。

但要注意，在傳統 Windows 或 Linux 端點上，絕不可能接受 IoT/OT 裝置中存在的弱點類型。

- 弱式密碼：掃描的韌體映像中，有 27% 包含的帳戶具有使用弱式演算法 (MD5/DES) 編譯的密碼，這些密碼很容易遭到攻擊者破解。

分析的韌體映像中的安全性弱點

- 已知漏洞：與其他系統一樣，IoT/OT 裝置韌體廣泛利用開放原始碼程式庫。不過，裝置出貨時，這些元件的版本經常已經過時。在我們的分析中，有 32% 的映像包含至少 10 個評為重大 (9.0 或更高) 的已知漏洞 (CVE)。有 4% 至少包含 10 個存在超過 6 年的重大漏洞。
- 憑證過期：憑證是用來驗證連線和身分識別，以及保護敏感資料，但分析的映像中，有 13% 包含至少 10 個已過期超過三年的憑證。
- 軟體元件：有 36% 的映像包含 Microsoft 建議 IoT 裝置應排除的軟體元件 (如封包擷取工具 (tcpdump、libpcap))，這些可能遭到利用，在攻擊鏈當中進行網路偵察。

環境中的韌體攻擊

Viasat：利用韌體漏洞鎖定衛星通訊為目標

在 2022 年 2 月，一起衛星網路事件中斷了策略通訊網路，整個歐洲都感受到衝擊。Viasat 的 KA-SAT 系統收到大量流量，造成許多數據機中斷，同時網路也遭到拒絕服務攻擊。隨著固網寬頻中斷，操作員便無法從遠端存取數千座風力發電機，同時惡意 wiper 惡意軟體也被部署到受影響的數據機上。這次中斷影響了企業和組織用於通訊的 30,000 多個衛星終端機。

Cyclops Blink：利用韌體供應鏈攻擊鎖定防火牆閘道為目標

對於威脅行為體而言，發展並擴展命令和控制 (C2) 及攻擊基礎結構，是獲得成功的關鍵要素。隨著對於穩定 C2 基礎結構的需求增加，路由器因不常修補且缺乏全面的安全性解決方案，而成為理想的攻擊媒介。

Microsoft 正與政府機構和業界合作開發韌體分析技術，以更深入了解裝置安全性，並為裝置製造商和操作者提供完整生命週期的安全性。

自 2019 年 6 月以來，一個國家附屬的進階持續威脅 (APT) 組織藉由執行惡意韌體更新，隨後再納入大型殭屍網路中的方式，使用模組化的惡意軟體 Cyclops Blink 鎖定易受攻擊的 WatchGuard 防火牆裝置和 ASUS 路由器為目標。惡意軟體透過利用已知漏洞的方式進行權限提升，藉此成功感染裝置，進而讓威脅行為體能夠管理裝置。一旦被感染，惡意軟體就會進一步安裝更多模組，並且規避韌體更新。目前已觀察到，遭入侵的裝置連線到裝載於其他 WatchGuard 裝置上的 C2 伺服器。Cyclops Blink 操作者發出許多 SSL 憑證給他們位在各種不同的 TCP 連接埠上的 C2，藉由執行惡意韌體更新及規避傳統安全性方法 (如掃描) 取得具有權限的遠端存取權來進入網路。

Microsoft 如何改善供應鏈安全性

Microsoft 正與政府機構和業界合作，共同因應這些 IoT 和 OT 裝置安全性挑戰 (請參閱第 66 頁的討論)。我們的貢獻將包括利用韌體分析技術為裝置操作員提供可見度，以深入了解其網路上裝置的安全性態勢。如此將能讓客戶找出需要額外防護、升級或更換的裝置並優先處理，並且促進裝置製造商投資裝置安全性的需求。同時，我們以全方位的解決方案支援製造商來架構安全的裝置並採用安全的開發生命週期。

另一個關鍵要素，就是為製造商和操作員提供健全的基礎結構，以便在發現安全性問題時更新韌體並解決問題。Microsoft 將韌體分析和適用於 IoT 的 Defender 與適用於 IoT 中樞的裝置更新相互結合，提供解決方案來因應 IoT 和 OT 裝置安全性的整個生命週期。這些都是實現我們對於客戶的願景過程中的重要步驟，藉由採用支援其 IoT 和 OT 解決方案的零信任方法的裝置來保護基礎結構的安全。[18]

攻擊者越來越常鎖定 IoT 裝置韌體中的漏洞為目標來滲透企業網路。

可付諸行動的見解

1. 取得您網路上 IoT/OT 裝置更深入的可見度，並依照遭入侵時，對企業構成的風險排列其優先順序。
2. 使用韌體掃描工具來了解潛在的安全性弱點，並與廠商合作找出如何降低高風險裝置的風險。
3. 要求您的廠商採用安全開發生命週期最佳做法，以利提高 IoT/OT 裝置的安全性。

進一步資訊的連結

- 評估支援美國資訊與通訊科技業的關鍵供應鏈

偵察式 OT 攻擊

複雜的供應鏈使用特定設計資訊來規劃實際系統。在構成這些設計資訊的無數資產當中，最敏感的就是專案檔案，它定義了環境及其資產。這個檔案是威脅行為體想要取得存取權並針對環境部署完全量身打造的成功攻擊時，最關鍵的策略目標。

鎖定工業系統為目標以中斷運作流程的行動包含兩個步驟。

1. 首先，攻擊者必須存取 OT 網路。經由企業端網路上的 IoT 裝置 (Purdue 模型第 4 層) 進入網路，並越過傳統上以防火牆和網路設備分隔的 IT-OT 邊界進入營運和控制層，就能達成這個目的。
2. 其次，必須識別網路裝置。工業系統使用專為其環境所設計的客製化架構中的標準裝置和元件。其中一種標準裝置就是可程式設計邏輯控制器 (PLC)。每個製造商都會為自己的 PLC 開發專屬的介面和功能，這是工業系統的關鍵元件，而這些裝置會進一步設定，以採用專為客戶環境所設計的自訂架構。

每個 PLC 的專屬設定都會在專案檔案中描述，當中包含環境及其資產的定義、階梯邏輯等。

在顯示攻擊證據的大多數環境中，分析顯示攻擊之前的時程遠遠超過攻擊本身的時間長度。威脅行為體常常花上數個月時間從遠端模擬環境及其資產，並且多次嘗試建構模型並準備其目標攻擊。隨著環境持續變化並整合新裝置，專案中的資料和設定檔案尤其容易產生許多漏洞。竊取專案檔案就能縮短攻擊時程達數星期或數個月，讓攻擊者能夠迅速且準確地建立目標環境的模型，因而增加了偵測到惡意活動的難度。

Industroyer 和 Incontroller

我們觀察到，國家贊助的行為體使用模組化惡意軟體和攻擊架構對組織、重大基礎設施和政府機構目標發動攻擊的情況增加。為了干擾烏克蘭關鍵營運的新嘗試，突顯了針對目標環境高度量身打造的偵察式 OT 攻擊的威脅增加。國家級網路行為體執行的擴大偵察和研究手段，指出了在混合的網路活躍行動和政策中，使用網路戰從遠端削弱基礎結構以達成特定策略性或行動目標的策略。

我們觀察到，對目標環境高度量身打造的偵察式 OT 攻擊的威脅越來越多。

偵察式 OT 攻擊

續

在 2022 年初，發現了兩次適應性高的關鍵 OT 攻擊。對烏克蘭境內的變電所和保護繼電器發動的網路實體攻擊，採用了客製化的惡意軟體，包括 Industroyer 的變種，這個惡名昭彰的惡意軟體自 2016 年部署後，造成了烏克蘭境內多次電力中斷。

Industroyer2 是在新目標上第一個已知的重新部署 OT 攻擊惡意軟體。它利用專為 Industroyer 開發的 IEC104 通訊協定 (用於電力系統監視和控制的標準通訊協定) 外掛程式，並且主要鎖定類似 PLC 的遠端終端機設備為目標，其模型編號為 ABB RTU540/560。此惡意軟體的編寫者利用對受害者環境的知識，對預定的輸出重複發出命令，確保它們無法手動打開。這樣就能確保電力中斷時間更長，造成更具破壞性的影響。

Incontroller 是同一時期確認的模組化攻擊架構，它是一個模組化工具組，可大幅縮短侵入和攻擊 OT 裝置的前置期，並繞過舊版安全性解決方案。一般用途工具組具有資料收集、偵察和攻擊功能，可針對不同環境高度自訂，並且能夠大幅影響 OT 攻擊的研究階段，減少執行偵察所需的時間，藉由擷取有關裝置及其設定的資訊來支援環境模擬。

Incontroller 架構支援 Schneider Electric 和 Omron PLC 的通訊協定，並且會收集資訊，例如韌體版本、機型和連線裝置。工具組可發出命令來變更設定，並且開啟和關閉輸出。一旦進入環境，架構就會支援在裝置中植入後門用來傳送更多承載、利用漏洞來增加存取點、上傳梯形邏輯，並且能夠發動 DoS 攻擊。工具組的通用特性可讓威脅行為者快速攻擊環境，而不需要針對每個 PLC 或位置編寫新的攻擊。這樣行為者就能輕鬆與可能跨許多產業的不同類型機器互動。

可付諸行動的見解

1. 避免透過不安全的管道傳送包含系統定義的檔案，或傳送給非必要人士。
2. 若無法避免要傳送這類檔案時，請務必監視網路上活動並確保資產的安全。
3. 使用 EDR 解決方案進行監視來保護工程站。
4. 主動對 OT 網路進行事件回應。
5. 部署持續監視，如適用於 IoT 的 Defender。

章節附註

1. 請參閱，例如網路與資訊系統安全性修訂指令 (NIS2) | Shaping Europe’s digital future (打造歐洲的數位未來) (europa.eu) (英文)；https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2020:595:FIN&rid=1; 2022 年安全性立法修正案 (重大基礎設施保護) 法案 (homeaffairs.gov.au) (英文)；智利：參議院引進網路安全宇關鍵資訊基礎設施法案 | News post | DataGuidance (英文); 日本通過經濟安全法案來保護敏感技術 | The Japan Times (英文); 網路安全法案審查及針對 CII 的網路安全行為準則更新 (csa.gov.sg) (英文)；改善英國網路韌性立法提案—GOV.UK (www.gov.uk) (英文); 2021 年電信 (安全性) 法 (legislation.gov.uk) (英文); 更新 NIST 網路安全架構—邁向 CSF 2.0 之旅 | NIST (英文)
2. Cert-In—首頁
3. 引發有關引入網路攻擊通報義務的諮詢 (admin.ch)
4. 請參閱，例如無標題 (house.gov)
5. 網路韌性法案 | 打造歐洲的數位未來 (europa.eu) (英文)
6. 請參閱，例如 Microsoft 安全性開發週期 (英文)
7. 請參閱 例如Microsoft 使用 SPDX 產生軟體物料清單 (SBOM)—Engineering@Microsoft (英文); 另請參閱 例如軟體物料清單 (SBOM) 的最低標準 | 美國國家電信暨資訊管理局 (ntia.gov) (英文)
8. 請參閱，例如 https://www.microsoft.com/en-us/msrc/cvd
9. 產品安全及電信基礎設施 (PSTI) 法案—產品安全資料表—GOV.UK (www.gov.uk) (英文)
10. 委員會強化無線網路裝置和產品的網路安全性 (europa.eu) (英文)
11. 雲端認證計劃：跨全歐洲打造受信任的雲端服務 — ENISA (europa.eu) (英文)
12. 認證 — ENISA (europa.eu) (英文)
13. https://github.com/microsoft/sbom-toolGitHub - Microsoft/sbom-tool：SBOM 工具是一種可高度擴展且專供企業使用的工具，可針對各種成品建立 SPDX 2.2 相容的 SBOM。
14. https://www.zdnet.com/article/ripple20-vulnerabilities-will-haunt-the-iot-landscape-for-years-to-come
15. IoT/OT 創新至關重要，但也伴隨著巨大的風險 (2021 年 12 月)：https://www.microsoft.com/security/blog/2021/12/08/new-research-shows-iot-and-ot-innovation-is-critical-to-business-but-comes-with-significant-risks/ (英文)
16. 揭露 Trickbot 在 C2 基礎結構中使用 IoT 裝置的情形 (2022 年 3 月)：https://www.microsoft.com/security/blog/2022/03/16/uncovering-trickbots-use-of-iot-devices-in-command-and-control-infrastructure/ (英文)
17. Channel 9 上有關 IoT 韌體掃描的 IoT 節目秀 (2022 年 5 月)：https://docs.microsoft.com/en-us/shows/internet-of-things-show/iot-device-firmware-security-scanning-with-azure-defender-for-iot (英文)
18. 如何將零信任方法應用於您的 IoT 解決方案 (2021 年 5 月)：https://www.microsoft.com/security/blog/2021/05/05/how-to-apply-a-zero-trust-approach-to-your-iot-solutions/ (英文)

網路勢力活動

當今的外國勢力活動會利用新的方法和技術，使其專為破壞信任所設計的活動更有效率且更具成效。

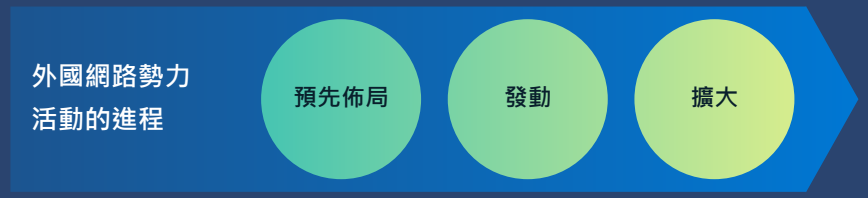
概覽：

網路勢力活動

當今的外國勢力活動會利用新的方法和技術，使其專為破壞信任所設計的活動更有效率且更具成效。

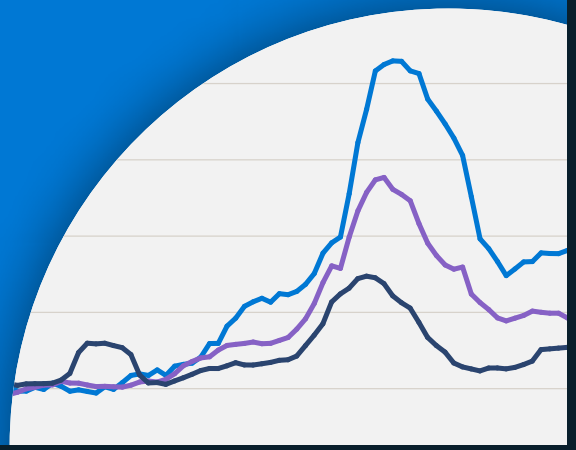
各國無論是對內或在國際間使用複雜的勢力活動來散發政治宣傳及影響大眾觀點的情況日益增加。這些活動破壞了信任、推升極端化，並且威脅著民主進程。老練的進階持續滲透操控者行為體會利用傳統媒體搭配網際網路和社交媒體來大幅擴大其活動的範圍、規模並效率，並且在全球資訊生態系統中造成巨大的影響。在過去一年，我們看到俄羅斯在烏克蘭發動的混合戰當中運用了這些活動，同時也看到俄羅斯和包括中國和伊朗在內的其他國家越來越常改採透過社交媒體進行的政治宣傳活動，目的就是擴大其全球勢力。

網路勢力活動越來越複雜，因為有越來越多政府和國家利用這些活動來帶風向、打擊對手名聲，以及製造分歧。



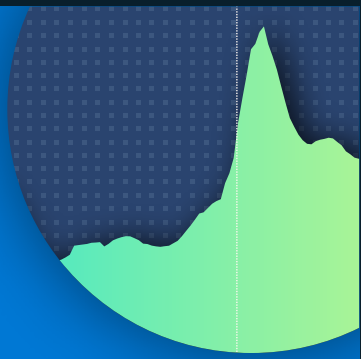
深入了解，前往 p74

俄羅斯入侵烏克蘭的行動證明了，網路勢力活動與較為傳統的網路攻擊和活躍的軍事行動相互結合，發揮最大的影響力。



深入了解，前往 p76

俄羅斯、伊朗和中國在整個全球疫情期間經常採用政治宣傳和勢力活動做為策略性工具，以實現更廣泛的政治目的。



深入了解，前往 p76

合成媒體因為工具的普及而變得越來越普遍，這些工具能輕易製造並散播極為逼真的人造影像、影片和音訊。證明媒體資產來源的數位出處技術能確保打擊濫用。

深入了解，前往 p80

防禦網路勢力活動的整體方法

Microsoft 在已成熟的網路威脅情報基礎結構上持續努力提升，以打擊網路勢力活動。我們的策略是偵測、中斷、防禦和阻止外國侵略者的政治宣傳活動。

深入了解，前往 p83

前言

民主需要值得信賴的資訊才得以蓬勃發展。Microsoft 著重的重要領域之一，就是國家所發展和延續的勢力活動。這些活動破壞了信任、推升極端化，並且威脅著民主進程。

外國勢力活動一直對資訊生態系統構成威脅。然而，在網際網路和社交媒體時代的不同之處，就在於大幅擴大活動的範圍、規模和效率，並且對全球資訊生態系統的健全狀態造成巨大的影響。

「在真相穿上鞋子之前，謊言早已跑遍半個世界」，這句古老的格言現在透過資料得到證實。麻省理工學院 (MIT) 的一項研究[1] 發現，人們轉傳虛假內容的機率比真相高出 70%，而且觸及前 1,500 人的速度快上 6 倍。隨著政治宣傳活動在網際網路和社交媒體上日益猖獗，並且破壞對傳統新聞的信任，資訊生態系統也變得越來越盲目。2021 年的一項研究[2] 指出，只有 7% 的美國成人表示他們對報紙、電視和廣播等新聞報導「非常信任」，而有 34% 的人表示「完全不信任」。

Microsoft 一直努力找出外國網路勢力環境中的主要行為體、威脅和戰術，並且分享學到的經驗教訓。今年 6 月，我們出了一份全面報告，分享從烏克蘭汲取的教訓，當中詳細介紹了俄羅斯的網路勢力活動。[3]

我們也正在研究深度偽造等先進技術是如何被武器化並用來破壞新聞記者的可信度。同時我們也與業界、政府機構和學術人員合作，發展更好的方法來偵測合成媒體並恢復信任，例如可找出偽造的人工智慧 (AI) 系統。

資訊生態系統和國家級網路政治宣傳迅速變化的性質，包括將傳統網路攻擊與勢力活動融為一體，以及干預民主選舉，這些都需要有社會整體的做法來對抗網路上和實體上對民主的威脅。

Microsoft 致力於支援健全的資訊生態系統，讓受信任的新聞和資訊得以蓬勃發展。我們開發工具和威脅偵測功能，以對抗國家推動的勢力活動不斷進化和擴大的風險。為了完成這項工作，我們近期收購了 Miburo Solutions，我們與第三方驗證機構 (如 Global Disinformation Index 和 NewsGuard) 合作，並參與且時而領導多方關係人夥伴關係，包括內容出處與真實性聯盟 (C2PA)。唯有共同努力，我們才能成功對抗試圖破壞民主進程和機構的惡意份子。

Teresa Hutson

技術與企業責任部門副總裁

網路勢力活動的趨勢

隨著技術迅速發展的步調，網路勢力活動也變得越來越複雜。我們看到在傳統網路攻擊中使用的工具被重複利用並擴大運用到網路勢力活動。此外，我們還看到國家之間的協調與強化增加。

Microsoft 今年透過收購專門分析外國勢力活動的 Miburo Solutions，以投入打擊外國勢力活動的行動。這些分析師與 Microsoft 的威脅情境資訊分析師相互結合，共同成立了 Microsoft 數位威脅分析中心 (DTAC)。DTAC 負責分析和報告國家級威脅，包括網路攻擊和勢力活動，將資訊和威脅情報與地緣政治分析相互結合，提供深入解析並提出有效的應變和防護措施。

全世界有超過四分之三的人表示，他們擔心資訊武器化[4]，而我們的資料能夠支援這些擔憂。Microsoft 及其合作夥伴持續追查國家級行為體如何使用勢力活動來實現其策略目標與政治目標。除了破壞性網路攻擊和網路間諜活動之外，威權政體也越來越常利用網路勢力活動來帶風向、打擊對手名聲、推升恐懼、製造分歧及扭曲事實。

這些外國網路勢力活動通常分成三個階段：

預先佈局

就像惡意軟體在組織的電腦網路內預先佈局一樣，外國網路勢力活動也會在網際網路上的公共領域中預先佈局虛假敘事。預先佈局戰術長期以來一直協助較為傳統的網路活動，尤其是 IT 管理員掃描其最近的網路活動時。長期蟄伏在網路上的惡意軟體可讓後續利用更加有效。網際網路上未被注意到的虛假敘事可能讓後續引用看起來更令人信服。

發動

通常在達成行為體的目標最有利的時間點，便會透過政府支持和影響的媒體機構和社交媒體管道發動協調的活動來傳播敘事。

擴大

最後，國家控制的媒體和代理會在目標受眾內部擴大敘事。通常，不知情的技術推動者會延伸敘事觸及的範圍。例如，網路廣告可能有助於金融活動，而協調的內容傳遞系統可能大量湧入搜尋引擎。

這個三步驟的方法在 2021 年後期被用來支援俄羅斯在烏克蘭境內散播有關謠傳的生化武器和生物實驗室的虛假敘事。此敘事最初於 2021 年 11 月 29 日上傳到 YouTube，由一名位於莫斯科的美國僑民在固定播出的英語節目中，聲稱烏克蘭境內美國資助的生物實驗室與生化武器有所關聯。這個故事流傳了數個月都沒有引起注意。在 2022 年 2 月 24 日，正當俄羅斯坦克跨過邊界之時，這則敘事便投入了戰事。Microsoft 的資料分析團隊找到了 10 個受俄羅斯控制或影響的新聞網站，這些新聞網站在 2 月 24 日同步發佈報導來回顧「去年的報導」，並試圖賦予它可信度。此外，俄羅斯外交部官方舉行記者會，進一步植入資訊環境中有關美國生物實驗室的假宣稱。隨後俄羅斯贊助的團隊努力在社交媒體和網際網路網站上廣為擴大敘事。

我們看到世界各地的威權政體為了彼此利益，一起破壞資訊生態系統。例如，在整個 COVID-19 全球疫情期間，俄羅斯、伊朗和中國採取政治宣傳和勢力活動的手段，混合利用公開、半隱蔽和隱蔽的散播方法來鎖定民主國家為目標，並推進地緣政治目標 (在第 76 頁進一步討論)。這三個政體在彼此的訊息和資訊生態系統上操弄，以推動偏好的敘事。這篇報導大部分內容是有關美國及其盟友的批評或陰謀論，加上政府官員在官方聲明中加油添醋，同時宣傳自家 COVID-19 疫苗與應變措施優於美國和其他民主國家。這些國營媒體機構藉由彼此大肆報導，創造了一個報導民主國家負面新聞，或者說是報導俄羅斯、伊朗和中國正面新聞的生態系統，只要當中某一個官方媒體機構發出報導，另外兩個國家就會跟進大肆報導。

有關美國生物實驗室和生化武器的敘事，透過許多外國勢力活動的三大階段傳播：預先佈局、發動和擴大。

網路勢力活動的趨勢

續

民間機構技術實體可能在不知情的情況下推動了這些活動，因而增加挑戰性。推動者可能包括註冊網際網路網域、主機網站、在社交媒體和搜尋網站上推廣素材、促進管道流量，以及透過數位廣告支付這些活動的公司。組織必須清楚威權政體針對網路勢力活動採用的工具和方法，以便偵測進而防止活動擴散。另外，幫助消費者發展更複雜能力的需求不斷增加，目的就是能夠識別外國勢力活動，並限制與其敘事或內容互動。

網路勢力活動（包括威權政治宣傳）對於全世界民主國家構成威脅，因為這些活動會破壞信任、促進極端化，並且威脅民主化進程。

需要增加跨政府、民間機構和民間社會之間的協調與資訊分享，才能提高透明度，以及揭露並瓦解這些勢力活動。

在全球有超過四分之三的人擔心資訊如何遭到武器化。

聚焦在 COVID-19 及俄羅斯入侵烏克蘭期間的勢力活動

許多國家試圖在整個全球疫情及俄羅斯入侵烏克蘭的期間控制資訊環境，這些都明確證明了威權政體如何混合進行網路與資訊活動。

COVID-19 政治宣傳

俄羅斯、伊朗和中國在整個 COVID-19 全球疫情期間進行了政治宣傳和勢力活動。COVID-19 在這些活動中主要以兩種方式成為顯著特色：

1. 代表全球疫情本身。
2. 利用 COVID-19 做為策略性裝置的活動，為了實現更廣泛的政治目標。

這些類型活動的廣泛目標有兩方面：其一是破壞民主國家、民主機構，以及美國與其盟友在全球舞台上的形象；其二是在國內和國際上提升自身的地位。

從已知的俄羅斯報導機構和媒體組織鎖定英語讀者傳遞的訊息，對照俄羅斯政府如何向自己的人民傳達有關疫苗和 COVID-19 嚴重性的訊息，就能清楚窺見一二。

試圖掩蓋 COVID-19 病毒來源的活動就是另一個例子。自全球疫情爆發以來，俄羅斯、一喇和中國的 COVID-19 政治宣傳便大量增加彼此的報導來擴大這些中心主題。這些報導內容大多是在宣傳有關美國的批評或陰謀論。這些官方媒體機構經常彼此大肆報導，發展出了一個報導民主國家負面新聞，或者說是報導俄羅斯、伊朗和中國正面新聞的生態系統，當中某一個官方媒體機構發出報導，另外兩個國家就會跟進大肆報導，並且不斷循環重複。

RT.com 上前 10 名最多觀看次數的冠狀病毒相關報導的標題 (2021 年 10 月 –2022 年 4 月)

反疫苗政治宣傳鎖定非俄文讀者為目標

俄文（以下翻譯成英文）	英文
「Lockdowns and boosters prevent transmission (封鎖和疫苗能阻止病毒傳播)」	「Vaccinations fail to curb transmission and are ineffective against new strains (接種疫苗無法遏止病毒傳播，對抗新的病毒變種無效)」
「Russian public figures are testing positive (俄羅斯公眾人物篩檢結果陽性)」	「Pfizer vaccine has dangerous side effects (輝瑞疫苗伴隨危險的副作用)」
「Cases and deaths are increasing in Russia (俄羅斯境內確診和死亡數增加)」	「Mass vaccination is politically motivated (大規模疫苗接種具政治意圖)」
「The Sputnik V vaccine is highly effective (Sputnik V 疫苗非常有效)」	「Pfizer and Moderna conduct unregulated trials (輝瑞和莫德納從事非法試驗)」
「Vaccine proof needed on public transport (搭乘大眾交通工具須出示疫苗接種證明)」	

俄羅斯 COVID-19 訊息內容隨語言而不同。

這類範例之一就是，俄羅斯和伊朗官方媒體很早就暗示 COVID-19 可能是美國製造的生化武器。這項宣稱於全球疫情初期，一名法律教授受訪時聲稱自己相信 COVID-19 是做為武器而製造，此後便在邊緣共謀網站上流傳。[6] 這段訪問在少數網站上發佈後並未廣為傳開，直到國有媒體機構將它挑出利用才廣為人知。伊朗政府贊助的伊朗英語和法語媒體機構 PressTV[7] 在 2020 年 2 月發佈了一篇英語報導，標題為「Is coronavirus a US biowarfare weapon as Francis Boyle believes? (冠狀病毒是否如 Francis Boyle 所相信，是美國生化戰武器？)」，這篇文章指出，美國是 COVID-19 疫情爆發的幕後黑手，並寫到：「在所有美國參與的戰爭中，都使用了輻射、化學、生物和其他禁止使用的武器，對目標地區的人造成極大的傷亡。」[8] 俄羅斯官方媒體機構和中國政府報導機構對於此論調皆表達了支持立場。Russia Today (RT) 這家官方媒體機構就是以傳播克里姆林宮政治宣傳著名[9]，至少發佈過一篇宣傳伊朗官方聲明的報導，宣稱 COVID-19 可能是「『美國生化攻擊』的產物，目標瞄準伊朗和中國」[10]，並推出社交媒體貼文暗指此陳述。例如，RT 於 2020 年 2 月 27 日的推文寫道：「Show of hands, who isn’t going to be surprised if it ever gets revealed that #coronavirus is a bioweapon? (假如發現冠狀病毒是生化武器，誰是那個不會感到意外的人？請舉手」[11]

烏克蘭戰爭—以政治宣傳做為戰爭的武器

俄羅斯入侵烏克蘭就是明確的例子，證明了網路勢力活動如何融入較為傳統的網路攻擊和地面軍事活動，以發揮最大的影響力。

在入侵烏克蘭之前，Microsoft 威脅情報分析師發現，至少有六個不同的俄羅斯同夥行為體對烏克蘭發動超過 237 次網路攻擊。這些活動試圖破壞服務和機構、阻止烏克蘭人取得可靠的資訊，並植入對烏克蘭領導層的懷疑。

聚焦在 COVID-19 及俄羅斯入侵烏克蘭期間的勢力活動

續

在 Microsoft 於 2022 年 4 月發佈的一份報告中，我們展示了俄羅斯如何基於控制基輔資訊環境的明顯意圖，發射了一枚飛彈擊中基輔電視塔，並於同日對烏克蘭主要媒體公司發動破壞性惡意軟體攻擊 [12]

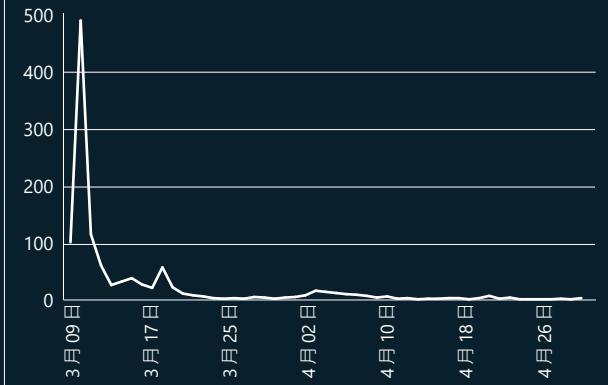
另一個說明網路攻擊和勢力活動如何發佈報導的範例，就是俄羅斯威脅行為體向烏克蘭公民發送一封電子郵件，偽裝成來自 Mariupol 的居民，責怪烏克蘭政府加劇戰事，並號召國民反抗政府。這些電子郵件（依姓名）專門寄給接收電子郵件的人，指出他們的資訊可能在之前的間諜活動相關網路攻擊中遭竊。郵件中未包含惡意連結，表示其意圖是純粹的勢力活動。

以聲稱遭駭客入侵、洩漏或其他敏感資料為特色，是俄羅斯行為體進行勢力活動時常見的策略。在整場烏克蘭戰事中，親俄羅斯的社交頻道不斷宣傳自稱來自烏克蘭來源的洩漏或敏感資料。親俄羅斯的社交頻道和機構利用洩漏或敏感資料做為更大規模的勢力策略的一部分，用來打擊對機構的信任，並讓大眾對主流報導產生懷疑。這些資訊可能遭到操控用來製作政治宣傳，鎖定烏克蘭和西方國家為目標，打擊對數位安全性的信任，並且削弱西方國家對烏克蘭的支援。

在地面活動發生後，俄羅斯利用其他資訊攻擊來塑造公眾意見帶風向，以掩蓋或破壞事實。例如，在 3 月 7 日俄羅斯透過向聯合國 (UN) 提出的陳述預先佈局，指出烏克蘭 Mariupol 的一家產婦醫院遭到淨空並做為軍事基地使用。於 3 月 9 日，俄羅斯轟炸了該醫院。在新聞報導轟炸的消息後，俄羅斯的 UN 代表 Dmitry Polyanskiy 隨即推文指出，該則有關轟炸的報導是「假新聞」，並引述俄羅斯稍早宣稱該醫院遭利用為軍事基地的說法。在該醫院遭到攻擊後兩星期，俄羅斯接著將這項陳述廣泛推送到俄羅斯控制的網站，

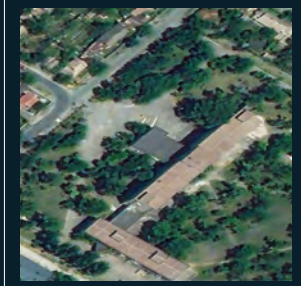
有流量的網域

(2022 年 3 月 9 日 –2022 年 4 月 30 日)



政治宣傳網站發佈有關產婦醫院的報導持續約兩星期，之後於 2022 年 4 月 1 日又再短暫復活。資料來源：Microsoft AI 為善 (AI For Good) 實驗室。

2022 年 2 月和 3 月 Mariupol 一家產婦醫院的衛星影像



Microsoft 自有的衛星影像分析顯示，這家產婦醫院遭到轟炸。第一張照片拍攝於 2022 年 2 月 24 日，第二張拍攝於 2022 年 3 月 24 日。照片來源：Planet Labs。

隨著戰事持續進行，俄羅斯也不斷洗白自己的暴行。例如，在 2022 年 6 月底，俄羅斯媒體機構和意見領袖將轟炸購物商場的行為描述成合理且必要，假裝宣稱這座商場並不是真正營運的商場，而是烏克蘭國土防衛隊的兵工廠 [13] 有數名親俄的部落客在 Telegram 上貼文並大肆宣傳強調此「栽贓行動」陳述的內容，這些部落客全都指向聲稱的製造指標，包括現場影片中出現穿著軍服的人 [14]，以及影片中消失的女性。[15] 俄羅斯倚賴打造出的政治宣傳信差和媒體系統來發起這些活動。在網路上大肆宣傳這些報導，讓俄羅斯能夠推卸國際間的指責，並避免承擔責任。

像俄羅斯這樣的國家了解利用封閉來源的資訊影響公眾認知，以及利用「駭入再洩露」活動來散播反制陳述並造成不信任能獲得的價值。

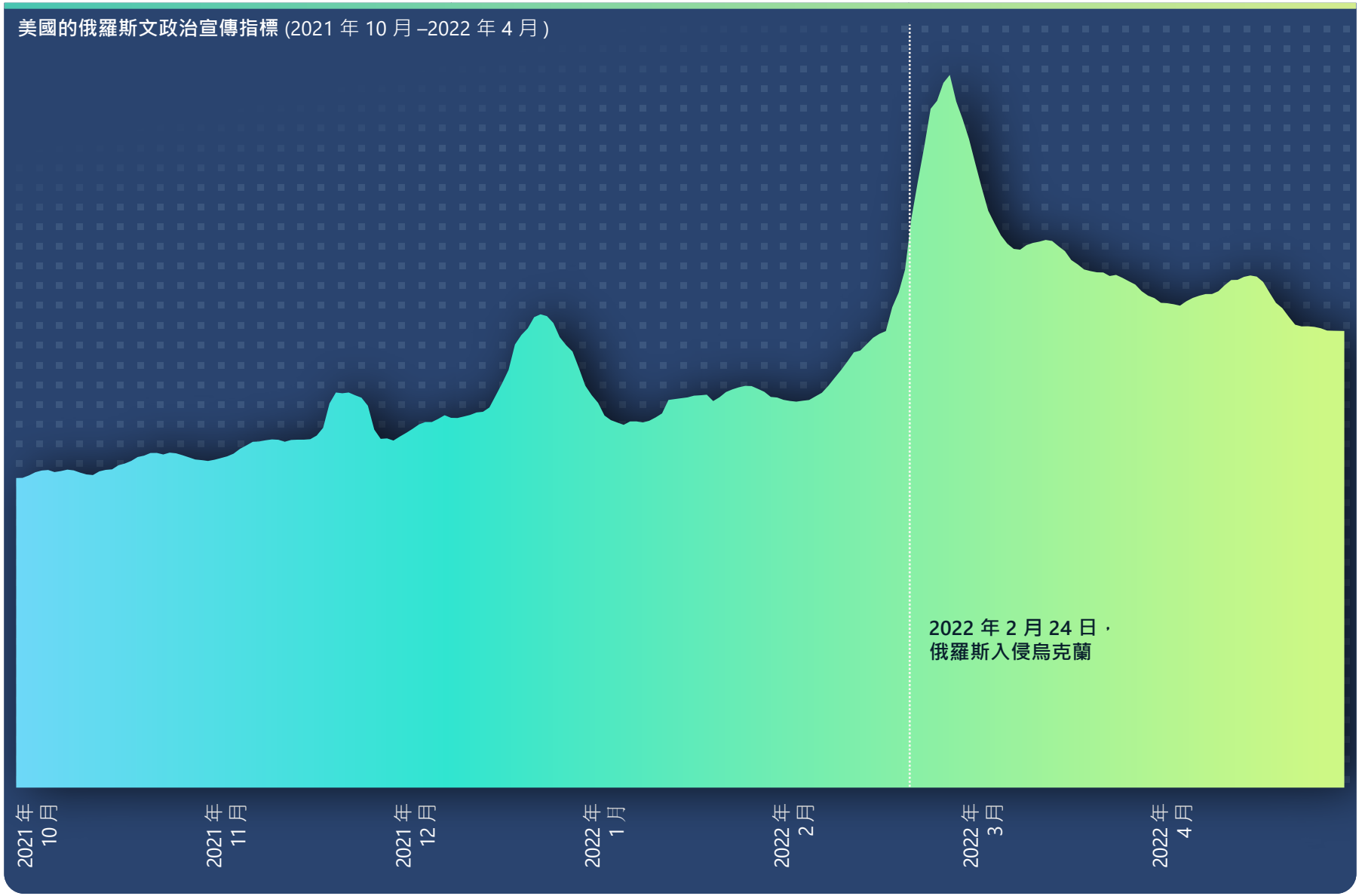
進一步資訊的連結

- 保衛烏克蘭：網路戰的早期教訓 | Microsoft 問題焦點（英文）
- 俄羅斯在烏克蘭的網路攻擊活動概觀 | Microsoft 特別報告
- 中斷鎖定烏克蘭為目標的網路攻擊 | Microsoft 問題焦點（英文）

追蹤俄羅斯文政治宣傳指標

2022 年 1 月，近 1000 個美國網站將流量導向俄羅斯政治宣傳網站。以美國讀者為目標的俄羅斯政治宣傳網站最常見的主題包括烏克蘭的戰事、美國本土政治 (親川普或親拜登)，以及 COVID-19 與疫苗相關敘述。

俄羅斯文政治宣傳指標 (RPI) 會監視來自俄羅斯官方控制和贊助的新聞機構與宣傳者的新聞流量，佔網際網路上整體新聞流量的比例。RPI 可用於在精確的時程表上繪製出跨網際網路和不同地理區的俄羅斯文政治宣傳消耗量的圖表。然而，Microsoft 注意到，我們只能觀察張貼在先前確定的網站上的俄羅斯文政治宣傳。我們無法深入洞悉其他類型網站上的政治宣傳，包括權威新聞網站、未確定身分的網站，以及社交網路群組。



追蹤俄羅斯文政治宣傳指標

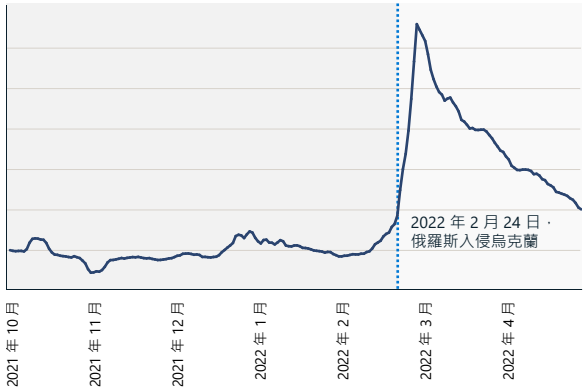
續

俄羅斯文政治宣傳指標：烏克蘭

當烏克蘭戰爭爆發時，我們看到俄羅斯文政治宣傳增加了 216%，並於 3 月 2 日達到高峰。下圖顯示此驟增現象與入侵同時發生的巧妙時間點。這兩個圖顯示，在爆發入侵不久，俄羅斯文政治宣傳便驟增。

RPI，烏克蘭

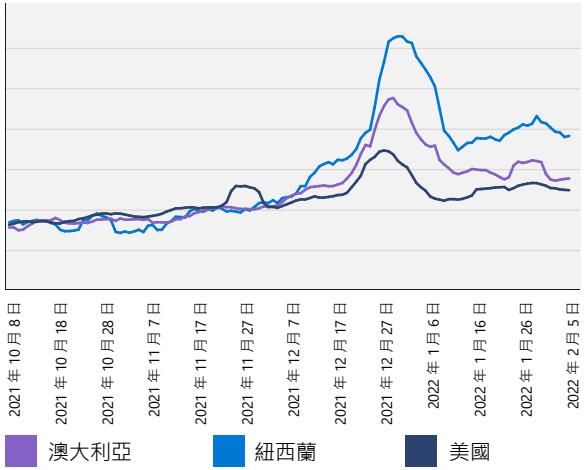
(2021 年 10 月 7 日 –2022 年 4 月 30 日)



俄羅斯文政治宣傳指標：紐西蘭與澳洲和美國的比較

對紐西蘭的 RPI 評估顯示，2021 年底有一波與 COVID-19 政治宣傳有關的驟增現象。2022 年初於威靈頓爆發的公開示威行動之前，紐西蘭境內就出現這波俄羅斯文政治宣傳消耗量驟增的現象。第二波驟增現象明顯與俄羅斯入侵烏克蘭有關，且超過了澳洲和美國的 RPI。

RPI，紐西蘭與澳洲和美國的比較



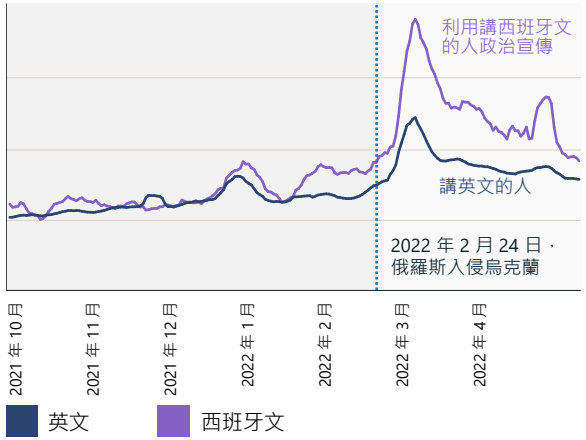
紐西蘭境內的俄羅斯文政治宣傳消耗量類似澳洲，直到 2021 年 12 月的第一周才有所改變。12 月之後，相較於澳洲和美國的消耗量，紐西蘭境內的俄羅斯文政治宣傳消耗量增加超過 30%。

美國的俄羅斯文政治宣傳指標：英文和西班牙文

RPI 也會跨語言追蹤政治宣傳。包括 RT 和 Sputnik News 在內的多個媒體機構提供了超過 20 種語言的報導。這些包括英語、西班牙語、德語、法語、希臘語、義大利語、捷克語、波蘭語、塞爾維亞語、拉脫維亞語、立陶宛語、摩爾多瓦語、白俄羅斯語、亞美尼亞語、奧塞提語、喬治亞語、亞塞拜然語、阿拉伯語、土耳其語、波斯語和達利語。

下圖顯示美國境內西班牙語新聞的 RPI 比英語新聞高出許多。

俄羅斯文政治宣傳消耗量在講西班牙語的人之中高出 2 倍



在美國的俄羅斯文政治宣傳消耗量在講西班牙語的人之間高出 2 倍。

在拉丁美洲的俄羅斯文政治宣傳很活躍

西班牙文的 RT 是擁有最高頁面瀏覽次數和最多 Facebook 追蹤人數的國際新聞機構。

資料來源：Microsoft AI 為善 (AI For Good) 研究實驗室

合成媒體

我們正進入支援 AI 的媒體創造與操控的黃金時代。Microsoft 分析師指出，這是由兩項關鍵趨勢所推動：容易使用的工具和服務十分普遍，方便用於人工製作出相當逼真的合成影像、影片、音訊和文字，以及快速傳播針對特定受眾最佳化之內容的能力。

這兩項發展本質上都存在問題。AI 為基礎的技術可用來製作有趣、刺激的數位內容，無論是製作純粹合成或強化現有素材都能做得到。這些工具正由企業廣泛用於廣告和通訊，以及個人用於為跟隨者製作吸引人的內容。然而，若是惡意製作並散佈的合成媒體，則可能對個人、公司、機構和社會造成嚴重的損害。Microsoft 持續在內部和規模更大的媒體生態系統中推動開發技術與做法，以限制這種損害行為。

本節探討 Microsoft 分析中對於目前製作破壞性合成內容的最先進技術、假設此內容廣泛傳播可能造成的傷害，以及可防禦以合成媒體為基礎的網路威脅的技術緩解措施等方面的深入解析。

製作合成媒體

合成文字和媒體的領域發展速度驚人，因為以往只有大型電影製片廠的龐大運算資源才能實現的技術，現在已整合到手機應用程式當中。同時，工具的越來越容易使用，並且能夠產生相當逼真的內容，甚至可以騙過鑑識媒體專家。我們非常接近實現任何人都能製作出任何人說任何話或做任何事的合成影片的境界。我們正進入一個時代，此時我們看到的網路內容當中有相當大量是完全或部分使用 AI 技術合成的，而這樣的想法不無道理。

> 有了更複雜、更容易使用且更普遍可用的工具，製作出的合成內容自然不斷增加，而且很快就會與實境相去不遠。

有許多高品質的商用影像、影片和音訊編輯工具可免費使用。這些工具可用來對數位內容進行簡單但可能具破壞性的變更，例如加入誤導文字、換臉，以及移除或修改背景。這類「廉價偽造」廣泛用於散佈惡意內容、宣傳政治意識形態，以及損害名譽。有一個知名的範例是 2019 年美國眾議院議長 Nancy Pelosi 的影片[16]，影片中她說話含糊不清，看起來像喝醉了一樣。雖然很快就確定該影片是為了製造效果而調慢播放速度，但「廉價偽造」卻在原始影片和背景出現之前就已廣為散佈。

用來修改媒體內容的更複雜方法包括應用先進的 AI 技術來 (a) 製作純合成媒體，以及 (b) 對現有媒體進行更複雜的編輯。「深偽」一詞常用來形容這類使用尖端 AI 技術製作出的合成媒體 (其名稱來自有時使用的深度神經網路)。這些技術經發展成為獨立應用程式、工具和服務，並整合到既有的商用和開放原始碼編輯工具中。

惡意行為體將這類技術武器化，以期損害個人與機構。深偽技術的範例包括：

- **換臉 (影片、影像)**—將影片中的臉孔換成另一張臉。這項技術可用於嘗試勒索個人、公司或機構，或讓個人處於尷尬地點或情境中。
- **操縱傀儡 (影片、影像)**—使用影片將靜止影像或另一段影片製作成動畫。這樣可能看起來像某個人說了尷尬或令人誤解的話。
- **生成對抗網路 (影片、影像)**—這一系列的技術用於產生逼真的圖像。
- **Transformer 模型 (影片、影像、文字)**—從文字描述製作豐富的圖像。

這類以 AI 為基礎進階技術尚未廣泛運用在現今的網路勢力活動中，但我們預期這個問題會隨著工具越來越容易使用且越來越普遍可得而擴大。

操控合成媒體的影響

使用資訊活動造成損害或擴大勢力並非新鮮事。然而，資訊傳播的速度飛快，加上我們無法從假象中快速找出事實，這些都意味著偽造和其他合成產生的惡意媒體所造成的影響和損害可能會更嚴重，就如 Pelosi 的例子所示。

我們考慮的損害類別有下列幾種：市場操控、付款詐欺、語音釣魚、冒充、品牌損害、名譽受損及殭屍網路。這些類別中有許多都是真實世界廣泛通報的範例，有可能損及我們分辨事實與假象的能力。

如果我們無法再相信眼見或耳聞的一切，那麼長期且更為險惡的威脅就會是我們對真實的理解。因此，任何危害公眾人物或私人形象的影像、音訊或影片都能視同造假，這是一種稱為「說謊者紅利」的結果。[17] 近期的研究[18] 顯示，這種技術濫用的情況已用於攻擊金融系統，儘管許多其他濫用情況也可能發生。

合成媒體

續

偵測合成媒體

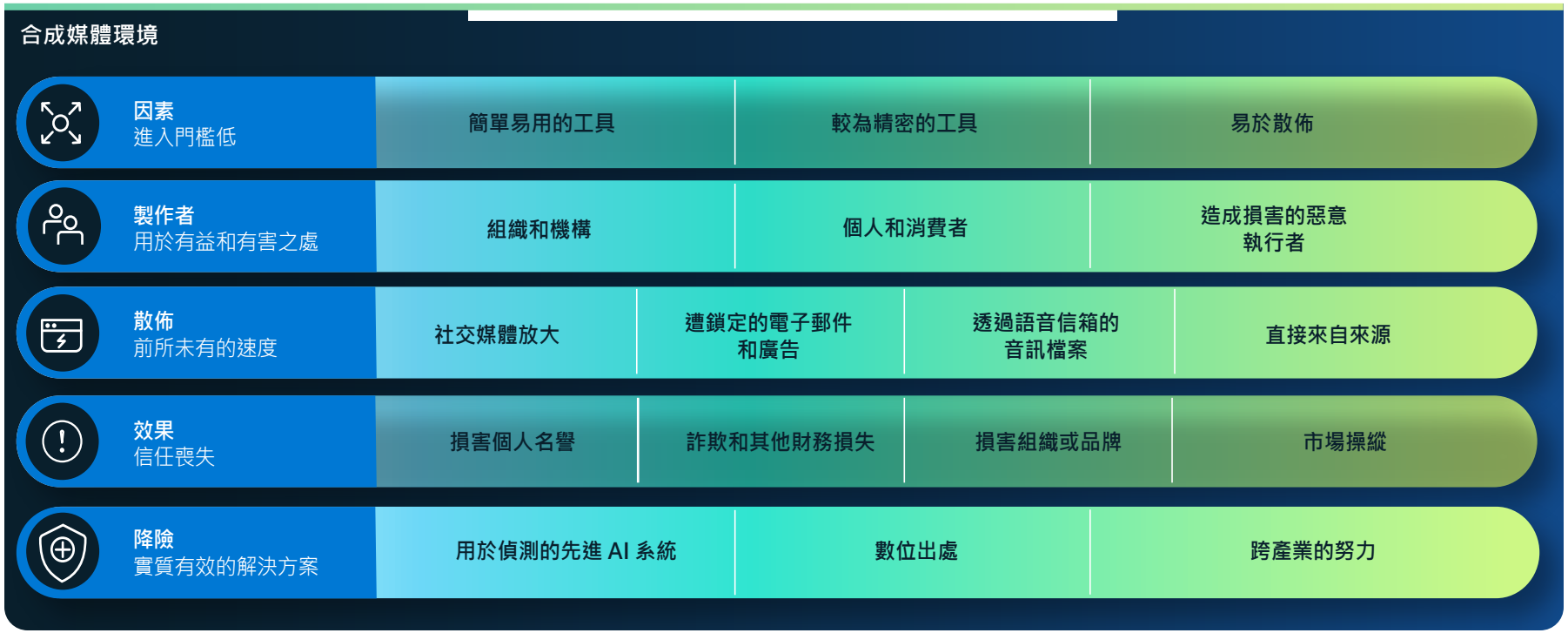
業界、政府機構和學術人員正共同努力，發展更好的方法來偵測和緩解合成媒體並恢復信任。有幾種有效的可行途徑，以及值得考慮的阻止方式。

其中一種方法是建置以 AI 為基礎的系統來找出造假，基本上就是「防禦性」AI 系統，用來對抗攻擊性 AI 系統。這是一個積極研究的領域，其中目前製作合成音訊和影片的系統留下了洩漏蹤跡的成品，透過受過訓練的媒體鑑識分析師和自動化工具就能找出。

不幸的是，雖然目前的造假顯露出瑕疵，但精確的成品往往是特定工具或演算法所專屬。這表示，有關已知造假的訓練通常不會概括其他演算法，如同 2020 年一場打造深偽影像偵測器的公開賽中所示。[19] 雖然擴大投資在開發更多進階偵測器是很吸引人的想法，但 Microsoft 對於這樣是否能帶來有意義的改進抱持高度懷疑的態度，原因有兩個：

首先，我們有反映真實世界的出色實體模型。目前的造假者抄捷徑，因而產生可偵測到的成品，但較新的模型將變得更加逼真。電腦無法將相機拍攝的真實世界場景製作成模型，這種情況本來就毫無特別之處。

其次，進階偽造演算法在製作過程中使用稱為生成對抗網路 (GAN) 的技術。GAN 會扮演兩套 AI 系統來相互對抗，使用產生器來造假，以及使用判別器來偵測偽造影像並訓練產生器。任何在開發更厲害偵測器方面的投資，都只會讓產生器改善造假的品質。



合成媒體

續

數位資產的出處

如果偵測造假並不可靠，那麼要怎麼做才能防止惡意利用合成媒體呢？有一項重要的新興技術就是數位出處，這是一種機制，可讓數位媒體創作者有能力認證資產，並幫助消費者識別數位資產是否經過竄改。數位出處在現今社交媒體網路環境中尤其重要，因為內容在網際網路上迅速傳播，而不良行為者有機會輕鬆操控內容。

數位出處技術是現代版的密碼編譯文件簽署，其設計目的是在現今網路上流傳的途徑中，擷取物件的來源、編輯歷程記錄及中繼資料。實現這種類型的媒體端對端防篡改認證的視覺和技術方法，是由 Microsoft 跨團隊的研究人員和科學家共同開發。我們共同領導跨產業合作夥伴關係，旨在將媒體出處技術實際應用到 Project Origin 中（由 Microsoft、BBC、CBC/ 加拿大廣播公司及紐約時報共同創立），並參與 Content Authenticity Initiative（內容真實性計劃，由 Adobe 創立）。Microsoft 同時與科技業和媒體服務業的合作夥伴一起建立了「內容出處與真實性聯盟」(C2PA)。C2PA 是一個標準組織，近期發佈了最先進的數位出處規範，以應用於媒體資源，包括影像、影片、音訊和文字。

支援 C2PA 的物件會附帶資訊清單，其能夠保護物件和中繼資料免於篡改，並且會隨附識別發行者的憑證。

合成媒體原本的設計並非造成損害，但不良行為者卻將其武器化，用來破壞對個人與機構的信任。

數位出處是一項前景看好的新興技術，能夠藉由認證媒體資產的來源，協助恢復人們對網路媒體內容的信任。

遵循 C2PA 規範的公用版解決方案正以現有產品中的新功能，或新的獨立應用程式和服務的形式出現。我們預期大多數常用的擷取、編輯和編寫工具將在幾年後支援 C2PA。這為企業提供了一個機會來確定本身對於數位出處的需求和用途，並且在他們於現有工作流程中使用的工具內增添這一層額外的保護。

可付諸行動的見解

1. 透過主動考慮您的 PR 和通訊應變措施，採取主動的步驟來保護您的組織防範錯誤資訊的威脅。
2. 利用出處技術保護正式通訊。

進一步資訊的連結

- 在對抗假資訊上邁進堅定的一步 | Microsoft 問題焦點（英文）
- 達成里程碑，2022 年 1 月 31 日
- Project Origin | Microsoft ALT 創新
- 內容出處與真實性聯盟 (C2PA)
- 探索與 Project Origin 用於媒體驗證的系統相關的技術詳細資料 | Microsoft ALT 創新（英文）

900%

自 2019 年以來，深偽的年增率。[20]

防禦網路勢力活動的整體方法

Microsoft 在已成熟的網路威脅情報基礎結構上持續努力提升，以發展更廣泛、更具包容性的網路勢力活動視野。

我們使用架構來提供建議的應變和緩解策略，以對抗活動構成的威脅，這可分成四個關鍵支柱：偵測、中斷、防禦和阻止。

此外，Microsoft 已採行四項原則，以奠定我們在這個領域的工作。首先，我們承諾尊重言論自由，並維護客戶透過我們的平台、產品及服務建立、發佈和搜尋資訊的能力。其次，我們積極防止我們的平台和產品遭利用來大肆宣傳外國網路勢力網站和內容。第三，我們不願意從外國網路勢力內容或行為體營利。最後，我們利用我們產品中的內部和信任的第三方資料，優先呈現對抗外國勢力活動的內容。

偵測

如同網路防禦一樣，對抗外國網路勢力活動的第一步，就是發展偵測能力。任何單一公司或組織都無法期望單獨取得所需的進展。跨技術領域的嶄新、更廣泛的協作將會至關重要，包括在分析和報告大量倚賴民間社會角色的網路勢力活動方面將有所進展，包括學術機構和非營利組織中的角色。

分別來自 Princeton University 和 Carnegie Endowment for International Peace 的研究人員 Jake Shapiro 和 Alicia Wanless 在辨識出這個角色後，制定出各項計畫來開設新的「Institute for Research on the Information Environment」（資訊環境研究機構，IRIE）。在 Microsoft、Knight Foundation 和 Craig Newmark Philanthropies 的支援下，IRIE 將以歐洲核物理研究中心 (CERN) 為模型建立一個具包容性的多方關係人研究機構。它將結合資料處理和分析方面的專業知識，以加快和擴展此領域的新發現。調查結果將更廣泛分享給政策制定者、科技公司和消費者。

防禦

第二個策略支柱是鞏固民主防禦，這是需要投資和創新的長期優先事項。它應將科技對民主造成的挑戰，以及科技為了更有效地保衛民主社會所創造的機會納入考量。

Microsoft 的策略架構旨在協助跨領域的利益關係人偵測、中斷、防禦和阻止政治宣傳，尤其是外國侵略者的活動。

從我們這個時代的重大技術挑戰之一開始著手最為理想，那就是網際網路和數位廣告對傳統新聞業的影響。自 1700 年以來，自由且獨立的報章媒體一直在支援地球上每一個民主國家方面扮演著特殊的角色：揭發貪腐、記錄戰亂，以及時時清楚呈現最大的社會挑戰。然而，網際網路吞食了廣告收入並帶走了付費訂閱者，使得地方媒體陷入絕境。許多地方報業都已倒閉。我們近期工作的許多深入解析之一，就是缺乏報章的城鎮，在不知情的情況下暴露於外國政治宣傳的數量，無可避免地遠高於平均數量。基於這些原因，民主國家的關鍵防禦論調之一，必須是鞏固傳統新聞業和自由媒體，尤其是在地方上。這就需要持續的投資和創新，且必須反映不同國家 / 地區和各大洲的當地需求。這些問題並不容易，而且需要採取多方關係人的做法，而 Microsoft 和其他科技公司正逐漸增加這方面的支援。

我們還需要在公共政策方面進行新的創新，而且需要成為公共優先事項。這可包括讓出版商能與科技公司共同協商廣告收入的法律，以及立法提供優惠稅率，讓當地新聞媒體因為雇用記者而得以減輕一部分薪資稅賦。記者需要其他許多工具來製作報導內容，包括分辨合法和詐欺來源內容的能力。

另外，幫助消費者發展更複雜能力的需求迅速進化，目的就是能夠識別國家推動的資訊活動。雖然看起來可能令人望而卻步，但這類似科技業長期追求打擊其他網路威脅的工作。考慮教育消費者仔細查看電子郵件地址，協助發現垃圾郵件或其他詐欺性通訊。美國的一些倡議，例如 News Literacy Project 和 Trusted Journalism。

如果我們無法再相信眼見或耳聞的一切，那麼長期且更為險惡的威脅就會是我們對真實的理解。

防禦網路勢力活動的整體方法

續

計畫—正在協助發展更明智的新聞和資訊消費者。從全球來看，像是來自 NewsGuard 的瀏覽器外掛程式這類新技術有助於更快推動這項工作。

這也應能提醒我們，公民教育是民主基礎的一部分。如同以往，這項工作需要從學校開始。但是，我們生活的世界要求我們終其一生持續接受公民教育。戰略與國際研究中心所領導的新 Civics at Work 承諾，Microsoft 也是初始簽署人暨合作夥伴，這項承諾尋求在企業社群內振興公民素養。這個例子正好展現了我們進一步鞏固民主防禦的機會。

中斷

近年來，Microsoft 數位犯罪部門 (DCU) 運用了更精細的戰略和開發工具來阻斷網路威脅，範圍從勒索軟體到殭屍網路，乃至於國家級攻擊。我們學到了許多重要的教訓，首先是扮演積極瓦解的角色來對抗各種不同的網路攻擊。

當我們考慮對抗網路勢力活動時，瓦解可能扮演更重要的角色，而最有效的瓦解方法也變得越來越明確。打擊大規模欺詐最有效的方法就是公開透明。正因如此，Microsoft 收購了在網路威脅分析和研究方面處於領先地位的公司 Miburo Solutions，借重他們偵測和回應外國網路勢力活動的專長，以提高我們自身偵測和中斷國家級勢力活動的能力。

我們的經驗顯示，政府機構、科技公司及 NGO 都應該謹慎處理並利用充分的證據來究責網路攻擊。我們了解到，這種瓦解行動的影響至關重要，甚至能在瓦解網路勢力方面更有助益。在俄羅斯入侵烏克蘭之前，親眼看到美國政府分享資訊，將公開透明化為有效行動，例如揭露俄羅斯的計畫，包括像是利用假造影片來密謀特定活動。

去年夏天，位於日內瓦的 CyberPeace Institute 發佈有關烏克蘭內外持續網路攻擊的內容中顯示，廣大的民間社會和民間組織有機會進一步提高有關網路勢力活動的透明度。有關新發現且記載完整活動的可靠報告，有助於大眾更準確評估所閱讀、看到和聽到的資訊，尤其是在網際網路上。為了達到此目的，Microsoft 將建置並擴充其現有網路報告，並且將發佈有關我們發現的網路勢力活動的新報告、資料和更新，包括適時的究責聲明。我們將發佈一份年度報告，使用資料導向的方法來綜觀整個公司內外國資訊活動的普遍程度，以及確保逐步改進的後續行動。我們也將考慮強化此類透明度的其他行動。

例如，數位廣告的角色尤其重要，因為廣告宣傳可能幫助外國活動募資，同時為外國贊助的政治宣傳網站塑造合法的樣貌。將會需要做出新的努力來中斷這些金流。

阻止

最後，假如對於違反國際規則沒有責任感，我們就無法期望國家改變行為。強制實施這種責任制是唯一要由政府承擔的責任。然而，多方關係人行動在鞏固和擴展國際規範方面扮演著越來越重要的角色。有 30 多個網路平台、廣告主和發行者 (包括 Microsoft 在內) 簽署了近期更新的歐盟不實資訊行為守則，一致同意堅守承諾，以應對這項日益增長的挑戰。就像最近的「巴黎宣言」、「基督城宣言」和「未來網際網路宣言」一樣，多邊和多方關係人行動能夠將民主國家的政府與公眾集結在一起。隨後政府就能以這些規範和法律為基礎擴大建置，以進一步推動世界民主國家所需且理應承擔的責任制。

透過快速且根本的公開透明，民主國家政府機構和社會都可透過究責國家級攻擊的來源、公告週知並建立對機構的信任，以有效打擊勢力活動。

我們提高了偵測和瓦解外國勢力活動的技術能力，並致力於公開透明地通報這些活動，例如我們的網路攻擊報告。

可付諸行動的見解

1. 在組織中實施強大的數位檢疫措施。
2. 考量不同的方式來減少員工或業務措施在無意間促進網路勢力活動的情況。這包括減少供應已知外國政治宣傳網站。
3. 支援資訊素養和公民參與活動，做為協助社會防禦政治宣傳和外國勢力的關鍵要素。
4. 與同業相關團體直接互動，努力因應勢力活動。

章節附註

1. https://mitsloan.mit.edu/ideas-made-to-matter/mit-sloan-research-about-social-media-misinformation-and-elections?msclkid=8dc75d6abcfe11ecad9946a058d581c9
2. https://news.gallup.com/poll/355526/americans-trust-media-dips-second-lowest-record.aspx
3. 保衛烏克蘭：網路戰的早期教訓 (microsoft.com)
4. https://www.edelman.com/sites/g/files/aatuss191/files/2022-01/2022 Edelman Trust Barometer_FullReport.pdf
5. 俄羅斯外交部發言人 Maria Zakharova：https://tass.com/politics/1401777；Lavrov：https://www.cnn.com/2022/05/05/opinions/sergey-lavrov-hitler-comments-ukraine-kauders/index.html,Kirill Kudryavtsev/Pool/AFP/Getty Images
6. https://apnews.com/article/conspiracy-theories-iran-only-on-ap-media-misinformation-bfca6d5b236a29d61c4dd38702495ffe
7. https://www.justice.gov/opa/pr/united-states-seizes-websites-used-iranian-islamic-radio-and-television-union-and-kata-ib
8. https://www.presstv.ir/Detail/2020/02/04/617877/Is-the-coronavirus-a-US-bioweapon
9. https://www.state.gov/wp-content/uploads/2022/01/Kremlin-Funded-Media_January_update-19.pdf
10. https://www.rt.com/news/482405-iran-coronavirus-us-biological-weapon/
11. https://web.archive.org/web/20220319124125/https://twitter.com/RT_com/status/1233187558793924608?s=20
12. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd
13. 俄羅斯 Kremenchuk 的宣稱與證據—bellingcat
14. https://t.me/oddr_info/39658
15. https://t.me/voenacher/23339
16. 事實查證：Nancy Pelosi「喝醉」的影片是操弄的結果 | 路透社
17. https://lawcat.berkeley.edu/record/1136469
18. https://carnegieendowment.org/2020/07/08/deepfakes-and-synthetic-media-in-financial-system-assessing-threat-scenarios-pub-82237
19. 深偽偵測挑戰結果：進一步推動 AI 的公開倡議 (facebook.com)
20. 深偽 2020：轉折點，作者 Johannes Tammekänd、John Thomas 和 Kristjan Peterson，2020 年 10 月

網路恢復力

了解現代化的風險與回報，對於全面復原方法來說至關重要。

概覽：

網路恢復力

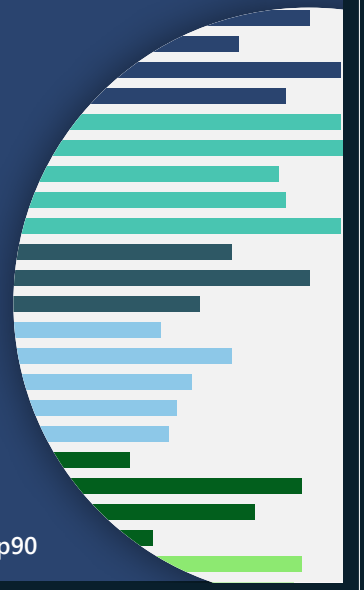
網路安全性是技術成功的關鍵推手。唯有導入安全措施，讓組織盡可能具備抵禦現代攻擊的韌性，才能達成創新和提高生產力的目標。

全球疫情已讓我們面臨挑戰，我們將安全性做法和技術轉而運用來保護 Microsoft 的員工，無論他們在何處工作都能安全無虞。過去這一年中，威脅執行者繼續利用全球疫情爆發與轉換成混合式工作環境期間所暴露出的漏洞。此後，我們的主要挑戰一直是管理盛行且複雜的各種攻擊方法，以及越來越多的國家活動。

有效的網路恢復力需要採取全面、適應性強的方法，來抵禦針對核心服務和基礎結構不斷進化的威脅。

深入了解，前往 p89

現代化的系統和架構對於管理超連結世界的威脅來說非常重要。

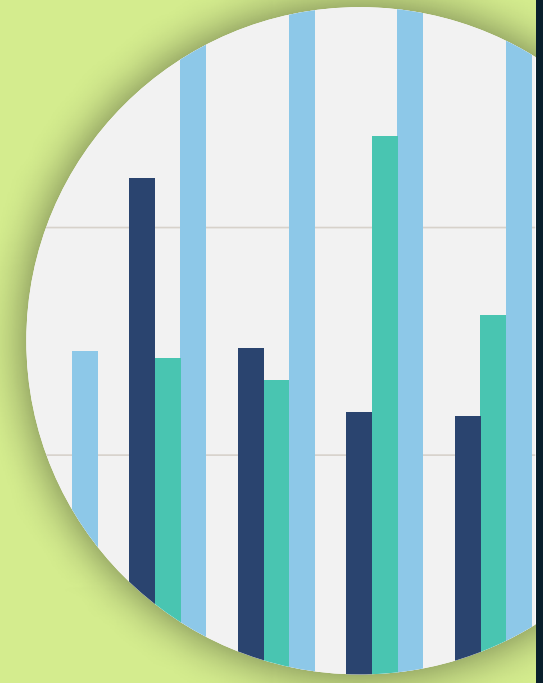


深入了解，前往 p90

基本安全性態勢是先進解決方案效益的判斷因素

深入了解，前往 p92

密碼型攻擊仍是身分識別攻擊的主要來源，而其他類型的攻擊正在興起。



深入了解，前往 p93

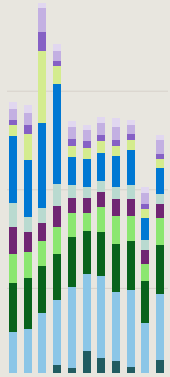
我們有能力在恢復力的人性層面上協作並作的，以對抗網路勢力活動。

深入了解，前往 p102

絕大多數成功的網路攻擊都可利用基本的安全性檢疫加以防止。

深入了解，前往 p108

在過去一年，全球經歷的 DDoS 活動在數量、複雜度和頻率上都是前所未見。



深入了解，前往 p98

前言

全球疫情讓我們面臨挑戰，我們將安全性做法和技術轉而運用來保護 Microsoft 的員工，無論他們在何處工作都能安全無虞。過去這一年中，威脅執行者繼續利用全球疫情爆發與轉換成混合式工作環境期間所暴露出的漏洞。此後，我們的主要挑戰一直是管理盛行且複雜的各種攻擊方法，以及越來越多的國家活動。

數位威脅活動和網路攻擊的複雜程度日益增加。當今許多複雜的攻擊都著重於採取不同程度安全性控制來入侵身分識別架構、供應鏈和第三方。具體而言，我們觀察到身分識別網路釣魚攻擊就是明確存在的威脅。然而，這些類型的攻擊通常因良好的身分識別管理、網路釣魚控制和端點管理做法而失敗。因此，我們必須記住這些基本知識：只要制定基本檢疫措施，就能阻止 98% 的攻擊。在 Microsoft，我們在採取的零信任方法當中管理身分識別和裝置，其中包括最低權限存取和防範網路釣魚認證，以有效阻止威脅行為體並保護我們的資料。

今天，即使是沒有複雜技術技能的威脅行為體都能發動令人難以置信的破壞性攻擊，因為在網路犯罪經濟中已廣泛提供了先進的戰術、技術和程序。烏克蘭的戰事證明了國家級行為體如何透過增加使用勒索軟體來升高其攻擊性網路活動。勒索軟體現已發展成一個複雜的產業，其中威脅行為體利用兩倍或三倍的勒索策略來索取贖金，而開發人員則提供勒索軟體即服務 (RaaS)。有了 RaaS，威脅行為體就能利用同夥網路進行攻擊，降低了技術較不熟練的網路罪犯入門的障礙，最終擴展了攻擊者的版圖。

因此，Microsoft 設計出一個勒索軟體消除計畫。這個計畫的目標是補救控制和覆蓋範圍的落差、促進服務的功能改進，以及為我們的安全性營運中心和工程團隊開發應對勒索軟體攻擊事件的復原劇本。

最近的供應鏈和第三方供應商攻擊指出了業界的主要轉捩點。這些攻擊對客戶、合作夥伴、政府機構和企業造成的破壞，以及 Microsoft 繼續擴展，說明了將注意力集中在網路恢復力以及與安全性利益關係人之間的協作極其重要。敵手也會將目標鎖定在內部佈署系統，提高了組織管理舊有系統所構成漏洞的需求，因而必須將基礎結構現代化並移至更安全穩健的雲端。

在我們生活的時代裡，安全性是技術成功的關鍵推手。唯有導入安全措施，讓組織盡可能具備抵禦現代攻擊的韌性，才能達成創新和提高生產力的目標。隨著數位威脅不斷增加和進化，將網路復原能力融入每個組織的架構中便是至關重要。

Bret Arsenault
資訊安全長

網路恢復力：互聯社會的關鍵基礎

我們在數位技術革命過程中看到了組織在經營方式和提供的服務方面轉型，因而變得越來越緊密相連。隨著網路環境的威脅增加，將網路恢復力融入組織架構中的做法，已經與財務和營運恢復力同等重要。

數位轉型永遠改變了組織與客戶、合作夥伴、員工和其他利益關係人互動的方式。新技術提供了與人互動、改造產品和最佳化營運的巨大機會。全球疫情加速了數位轉型，藉由促進創新技術使得人們得以採取全新的方式從任何地點協作。

隨著網路威脅變得盛行，要在我們這個「永遠連線」的世界裡阻止威脅入侵組織變得更加困難。網路恢復力代表著組織即使遭到攻擊，仍持續營運並維持加速成長的能力。預防措施必須與生存和復原能力相互平衡，而政府機構和企業正在開發超越安全性和隱私權的全方位模型，以在網路恢復力當中納入保護資產、資料和其他資源的能力。

開發全面的方法來實現網路恢復力

網路恢復力需要採取全面、適應性強且全球通用的方法，能夠抵禦針對核心服務和基礎結構不斷進化的威脅，包括：

- 基本網路檢疫，如網路恢復力貝爾曲線中所述。
- 了解並管理數位轉型的風險 / 回報權衡。
- 即時回應能力，能夠主動偵測威脅和漏洞。
- 防範已知攻擊的措施，以及對抗新的和預測的攻擊媒介的預防活動，包括自動補救的能力。
- 透過錯誤隔離和分割，降低攻擊和災難的影響。
- 發生中斷事件時自動復原和備援。
- 優先處理營運測試以找出落差，以及了解外部資源的共同責任和相依性，例如雲端式安全性解決方案。

有效的網路復原計畫是從資源基礎知識開始，例如了解可用的服務，以及擁有可靠的資源目錄，能夠在發生中斷時取用。以此為基礎進行後續建置之下，計畫必須能夠評估本身的有效性、衡量關鍵服務的效能及其相依性、跨內部佈署和雲端服務進行測試和驗證，以及在組織的數位生命週期中持續改進。

為了提供整體方法，我們與組織合作以確定其最關鍵的內部佈署和線上服務、業務流程、相依性、人事、廠商和供應商。另外，我們也期望找出合乎客戶與市場期望、法規與合約義務及內部營運的資產和資源。確定這些關鍵資源後，應同步進行偵測和監視威脅、中斷、潛在攻擊媒介以及系統和程序漏洞的工作。為了能夠在目前技能短缺情況下執行這些工作，便需要根據組織面臨的整體風險，嚴謹地規劃出優先順序。

這種整體方法需要能夠適應不斷進化的威脅形勢，目標是推動可衡量的績效提升、縮短偵測、回應和復原的時間，以及縮小發生中斷時的影響範圍。這個方法也必須辨識威脅之間日益增加的關聯性。例如，安全性事件可能導致資料外洩並伴隨隱私權問題，因此需要許多內外部團隊共同合作，以快速回應並儘量減少影響。

> 網路恢復力是企業即使遭遇包括網路攻擊在內的中斷情況，仍能持續營運並維持加速成長的能力。

可付諸行動的見解

1. 建置和管理技術系統以限制資料外洩的影響，讓它們能持續安全且有效地運作，即使資料外洩成功也一樣。專注於常見的關鍵資產、支援敏捷性，以及建構適應能力構 (例如混合和多雲端、多平台)、減少受攻擊面 (例如，移除未使用的應用程式和過度佈建的存取權)、假設遭入侵的資源，並預期敵手將會進化。
2. 在規劃數位專案時，同時考量可能的威脅與機會，以及跨數位技術供應鏈復原的共同責任，包括雲端式安全性解決方案。
3. 建置系統時，在設計中融入安全性，並逐步預測、偵測、抵抗、適應及回應未來不斷進化的威脅。
4. 企業領導者必要時應確實諮詢安全性團隊，以了解與新發展相關的風險。同樣地，安全性團隊應考慮業務目標，並建議領導者如何安全地追求這些目標。
5. 確保針對組織復原能力制定清楚的營運做法和程序，以因應網路事件。

將系統和架構現代化的重要性

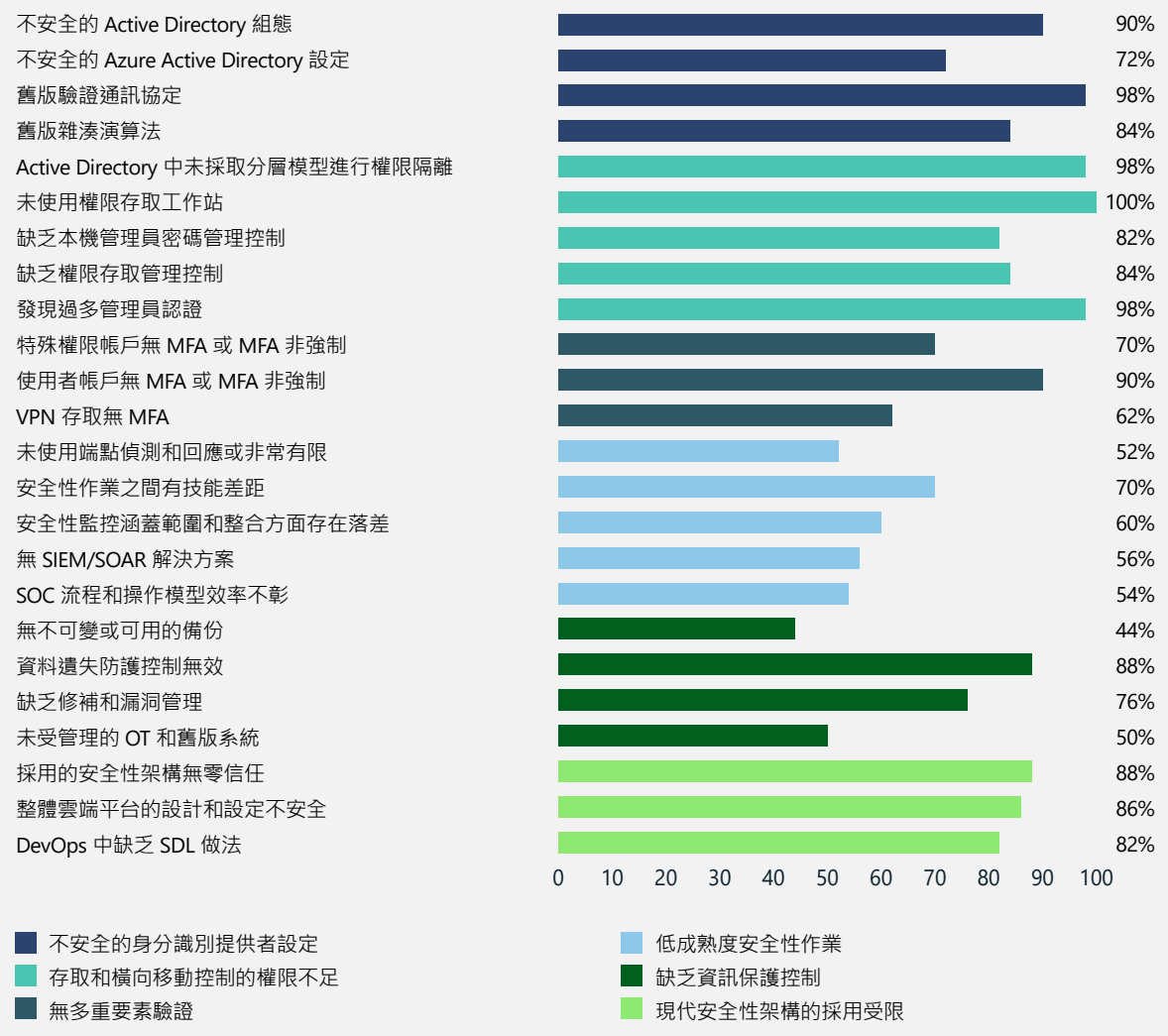
當我們針對超連結世界發展新的功能時，必須管理舊式系統和軟體所帶來的威脅。

舊式系統是指現代連線工具 (如智慧手機、平板電腦和雲端服務) 成為常態之前所開發的系統，若組織仍在使用這些系統，便會帶來風險。這種風險暴露可透過 Microsoft Security Services for Incident Response 團隊的調查結果進一步了解，這個團隊由一群安全性專業人員所組成，目的在於協助客戶回應攻擊並進行復原。

在過去一年中，從攻擊中復原的客戶當中發現的問題可分成六大類，如本頁圖表所示。下一頁概述可採取哪些實質步驟來提高恢復力。

有 80% 以上的安全性事件可追溯到幾個缺乏的元素，這些可透過現代安全性方法加以解決。

影響網路恢復力的關鍵問題



這個圖表顯示，缺乏基本安全性控制的受影響客戶百分比，這點對於提高組織網路恢復力至關重要。調查結果是根據 Microsoft 過去一年的互動情形。

「領導者應該將網路恢復力視為企業韌性的關鍵層面。他們應對網路中斷進行規劃，就像處理天災或其他無法預見的事件一樣，並且集結如營運、通訊、法務等內部利益關係人共同擬定策略。這樣做將有助於確保組織能夠盡速讓關鍵業務系統再次上線運作，以恢復正常業務營運。

但這不止於此。由於許多組織依賴第三方供應商和服務提供者，因此領導者應將網路恢復力規劃延伸到其端對端價值鏈，以進一步確保業務續航力和恢復力。」

Ann Johnson，
企業副總裁，安全性、合規性、身分識別和管理業務開發部門

將系統和架構現代化的重要性

續

其中有一些組織能夠處理以將其方法現代化並防範威脅的明確領域：

問題	實質步驟
不安全的身分識別提供者設定 設定不當和暴露身分識別平台及其元件，是取得未經授權的高權限存取權常見的媒介。	部署和維護身分識別系統 (如 AD 和 Azure AD 基礎結構) 時，務必遵循安全性設定基準和最佳做法。 藉由強制執行權限隔離、最低權限存取，並利用特殊權限存取工作站 (PAW) 來管理身分識別系統，以實施存取限制。
存取和橫向移動控制的權限不足 管理員在數位環境中擁有過多權限，且經常在受到網際網路和工作效率風險限制的工作站上公開管理認證。	保護並限制管理存取權，讓環境更具恢復力並限制攻擊的範圍。採用權限存取管理控制，例如即時存取和限制權限管理。
無多重要素驗證 (MFA) 現在的攻擊者不會侵入，而是登入。	MFA 是關鍵且基本的使用者存取控制，所有組織都應該啟用。MFA 搭配條件式存取運作，就能在對抗網路威脅上發揮無比珍貴的價值。
低成熟度安全性作業 受衝擊最大的組織使用傳統威脅偵測工具，並且無法得到相關深入解析以及時回應和補救。	全方位的威脅偵測策略需要在擴充式偵測和回應 (XDR) 和採用機器學習的現代雲端原生工具方面進行投資，以便將訊號與雜訊分開。納入 XDR 就能跨整個數位環境提供深入的安全性見解，實現安全性作業工具現代化。
缺乏資訊保護控制 組織持續努力地建立全面的資訊保護控制，期望能完整涵蓋資料位置，並在整個資訊生命週期中維持有效性，同時與資料的業務關鍵性保持同調。	找出您的關鍵業務資料及其所在位置。檢閱資訊生命週期流程並實施資料保護，同時確保業務續航力。
現代安全性架構的採用受限 身分識別是新的安全性周邊，可存取不同的數位服務和運算環境。整合零信任原則、應用程式安全性和其他現代網路架構，就能讓組織主動管理可能難以想像的風險。	零信任架構會強制實施最低權限的概念、明確驗證所有存取權，並且永遠假設入侵狀況。組織也應該在 DevOps 和應用程式生命週期流程中實施安全性控制和做法，以提高其商務系統中的保證層級。

基本安全性態勢是先進解決方案效益的判斷因素

透過我們的分析，我們發現組織防禦中常見的盲點相當普遍，使攻擊者得以初步存取、建立立足點並實施攻擊，即使有先進的安全性解決方案也未能阻止。

在許多案例中，網路攻擊的結果早在攻擊開始之前就已確定。攻擊者利用易受攻擊的環境取得初步存取權、進行監視，並透過橫向移動和加密或外洩造成破壞。及早阻止攻擊者就能增加降低整體衝擊的機會。

Microsoft 研究安全性態勢中的特定設定，以找出這些環境中實際做法內最常見的缺點。如此讓我們得以看見人為操作勒索軟體攻擊期間利用的最常見漏洞，這些漏洞讓威脅行為體得以存取並在網路中移動，而不會被偵測到。

基本安全性設定必須開啟

未加入或過時的組織裝置（都與漏洞和安全性代理程式狀態有關）會成為攻擊者的可能進入點及存取建立路徑。我們發現，雖然確保組織裝置加入更新的端點偵測和回應[1] (EDR) 及端點保護平台[2] (EPP) 解決方案是一個重要的步驟，但不保證能阻止勒索軟體。

EDR 和 EPP 等進階解決方案對於在攻擊流程中及早偵測到攻擊者，以及實現自動化補救和防護來說，非常重要。然而，由於這些進階解決方案倚賴偵測攻擊的基本能力，因此需要開啟基本安全性設定。事實上，我們觀察到一種普遍的情況，那就是即使已有進階解決方案，仍因為沒有基本安全性設定而遭到破壞。

相較於安全營運中心 (SOC) 分析師回應時間，安全性設定的最佳做法是更能代表恢復力的指標。

我們在整個客戶和合作夥伴群體觀察到，在六個月期間，SOC 分析師查看相關警示並採取行動所需的時間縮短了 70%。這代表意識提高，是好現象。不過，雖然安全性設定可見度提高了 SOC 分析師的效能，但透過讓組織的裝置上線並更新來實現產品可見度，是更好的成功預防預測指標。

未知裝置所帶來的風險

與雲端網路（客戶知道哪些資產在哪些作業系統上執行）不同的是，內部佈署網路可能包含廣泛的各種組織未監視或管理的裝置，如 IoT、桌上型電腦、伺服器和網路裝置。

企業網路平均有 3,500 多部連線裝置未受到 EDR 代理程式保護，並且可能可以存取企業資源，甚至可存取高價值資產。適用於端點的 Microsoft Defender (MDE) 使用網路偵查來探索裝置，並提供這些連線到網路之裝置的相關裝置分類資訊，例如裝置名稱、作業系統分佈情形及裝置類型。

3,500 部

企業中未受端點偵測和回應代理程式保護的平均連線裝置數。

對於 EDR 代理程式不支援的裝置，務必至少知道其存在，並採取行動來評估漏洞及限制網路存取以保護它們。

可付諸行動的見解

1. 若缺乏基本安全性設定，就連先進的解決方案都可能遭到破壞。
2. 投資安全性態勢設定的最佳做法，以防範未來的攻擊。這些基本設定會在組織防禦攻擊方面，產生巨大的投資報酬。
3. 讓所有適用的裝置都採用 EDR 解決方案。
4. 務必更新安全性代理程式，並確實防止篡改，讓產品獲得更深入的可見度及更完整的保護優勢。

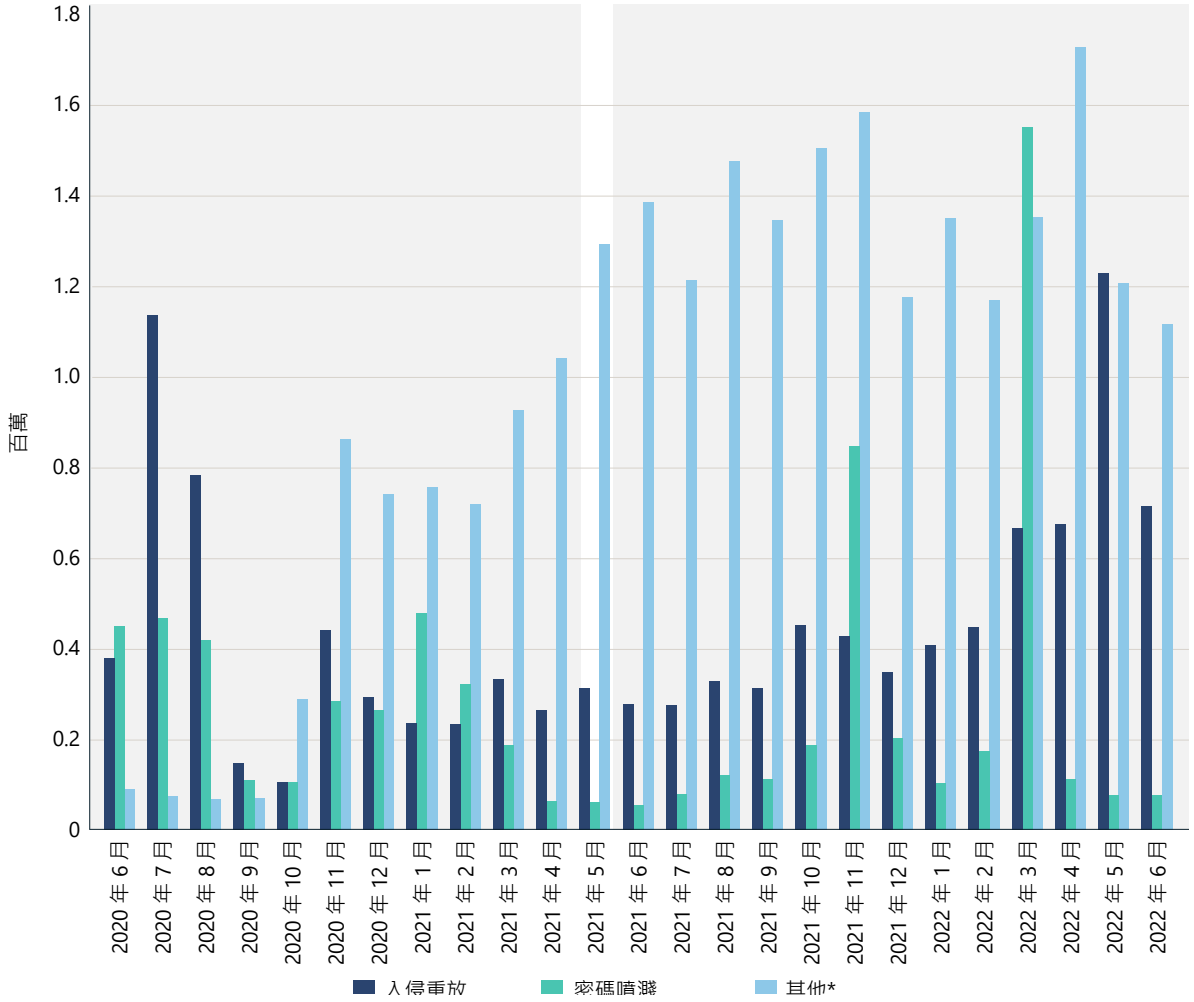
維護身分識別健全是組織福祉的基礎

保護身分識別比以往更加重要。密碼型攻擊仍是身分識別攻擊的主要來源，而其他類型的攻擊正在興起。相較於先前的密碼噴濺和入侵重新執行的常態，複雜攻擊的數量持續增加。

密碼型攻擊仍然很常見，有超過 90% 未受到強式驗證保護的帳戶是經由這些方法遭到入侵。強式驗證會使用一種以上的驗證要素，例如密碼 + 簡訊和 FIDO2 安全性金鑰。

我們看到目標式密碼噴濺攻擊增加，其中有相當大量驟增的攻擊者流量分散到數千個 IP 位址。

遭入侵的使用者 (依攻擊類別)



每月遭入侵的使用者 (依攻擊類別)。密碼噴濺攻擊的數量波動很大，如同 2021 年 11 月與 2022 年 3 月觀察到的驟增一樣。這些驟增代表觸及了數千名使用者和數千個 IP 位址。*「其他」表示與密碼噴濺和入侵重新執行不同的攻擊，包括網路釣魚、惡意軟體、中間人、內部佈署權仗簽發者入侵等。資料來源：Azure AD 身分識別保護。

4,500

在您閱讀此聲明的同時，我們抵禦了 4,500 次密碼攻擊。

維護身分識別健全是組織福祉的基礎

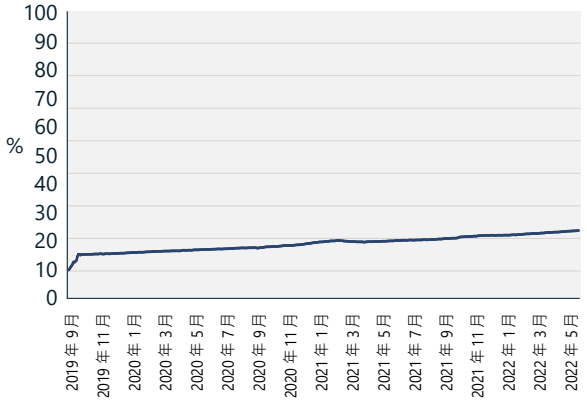
續

採用強式驗證

從積極面來看，我們看到 Azure Active Directory (Azure AD) 企業客戶群中採用強式驗證的趨勢穩定成長。對於 Azure AD，去年強式驗證每月有效使用者 (MAU) 從 19% 成長到 26%，同時管理帳戶的強式驗證 MAU 從 30% 成長到約 33%。

這是正向趨勢，但仍需要大幅成長才能達到強式驗證的大多數覆蓋範圍；尚未在環境中使用強式驗證的客戶應開始規劃和部署強式驗證以保護其使用者。[3] 在設計強式驗證部署的同時，也應考量無密碼驗證，因為它提供了最安全的可用體驗，消除了密碼攻擊的風險。

使用強式驗證
(2019 年 9 月 –2022 年 5 月)

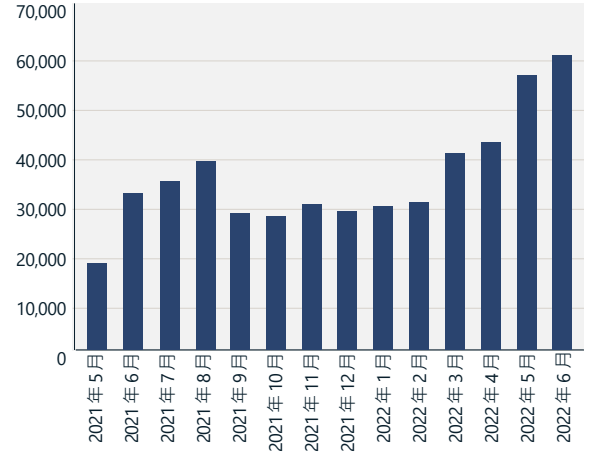


雖然自 2019 年以來，強式驗證使用率已倍增，但只有 26% 的使用者和 33% 的管理員使用強式驗證。資料來源：Azure Active Directory。

權杖重新執行攻擊持續上升

其他形式攻擊的佔比在 2022 年有所增加。我們看到了目標式攻擊增加，尤其是避開密碼型驗證來降低偵測機率的情況。這些攻擊會利用瀏覽器單一登入 (SSO) Cookie，或重新整理透過惡意軟體、網路釣魚和其他方法取得的權仗。在某些案例中，攻擊者會選擇與目標使用者所在地理位置接近的位置，以進一步降低偵測的機率。我們看到了權杖重新執行攻擊持續增加，在 Azure AD Identity Protection 中每月達到 40,000 多次偵測。權杖重新執行是指發出給合法使用者的權杖遭到攻擊者擁有並利用。權杖通常是透過惡意軟體取得，例如將使用者瀏覽器中的 Cookie 外洩，或透過進階網路釣魚方法。

偵測到的權杖重新執行攻擊數量



每月偵測到的權杖重新執行攻擊。資料來源：Azure AD Identity Protection，由異常權杖偵測標記的唯一工作階段。

維護身分識別健全是組織福祉的基礎

續

擷取權杖

除了惡意軟體，攻擊者還需要認證才能達成目標。事實上，所有人為操作的勒索軟體攻擊中都有遭竊的認證。許多複雜的入侵都有從暗網購買的認證，一開始是從簡單且廣泛分散的認證竊取惡意軟體竊得。這類惡意軟體已進化成竊取權杖，包括工作階段資訊和 MFA 請求。這表示，使用者登入企業資產所在的本地系統上的感染，可能會導致企業網路上發生嚴重事件。

攻擊者也可透過中間人攻擊從受害者的裝置中擷取權杖，受害者只要按一下網路釣魚電子郵件或簡訊中的惡意連結，就會被導向看似身分識別提供者的合法登入頁面的網站。實際上，它是攻擊者營運的 Web 服務，會轉送和攔截使用者與身分識別提供者之間的所有流量。攻擊者能夠攔截使用者名稱和密碼，也能轉送 MFA 挑戰；導致身分識別提供者所簽發且遭攻擊者攔截的權杖，可能包含 MFA 請求，進一步讓攻擊者得以用來滿足 MFA 需求。

Microsoft Defender for Cloud Apps 自 2022 年初以來，每月平均偵測到 895 次此類攻擊。這種形式的攻擊可藉由使用 MFA 的防範網路釣魚要素加以避免，例如憑證式驗證、商務用 Windows Hello 或 FIDO2 安全性金鑰。

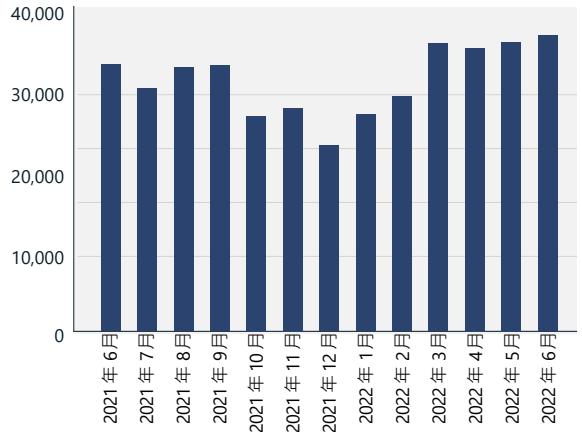
> 密碼型攻擊是帳戶遭到入侵的主要方法。

MFA 倦怠

攻擊者利用「MFA 倦怠」的概念，對受害者的裝置產生多個 MFA 要求，希望受害者會不小心或因為倦怠而接受要求。這種攻擊只要使用現代驗證器應用程式 (例如 Microsoft Authenticator) 結合幾項功能，如編號比對 [4] 和啟用其他相關內容，就能加以避免。[5] Azure AD Identity Protection 估計每月有 30,000 次 MFA 倦怠攻擊發生。

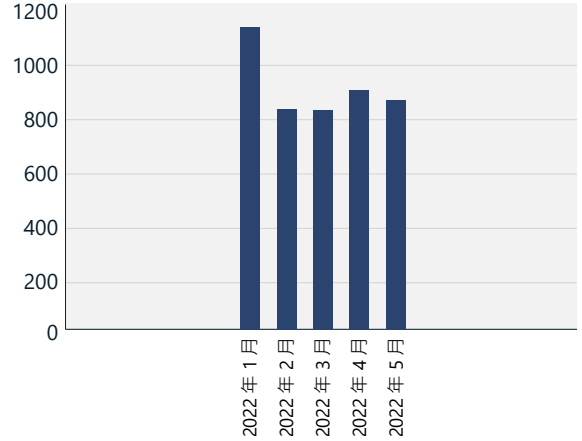
> 複雜攻擊的佔比繼續上升，突顯了對於多重要素驗證的防範網路釣魚要素的需求。

估計的 MFA 倦怠攻擊執行個體



資料來源：Azure AD 身分識別保護。

偵測到的中間人攻擊後續網路釣魚執行個體數



資料來源：Microsoft Defender for Cloud Apps。

可付諸行動的見解

1. 確認整個組織內的所有帳戶都受到強式驗證措施的保護。
2. 無密碼驗證提供了最安全且使用者易用的體驗，消除了密碼攻擊的風險。
3. 停用整個組織內的舊式驗證。
4. 透過防範網路釣魚形式的強式驗證來保護高價值的管理帳戶。
5. 將內部佈署身分識別提供者現代化，成為雲端身分識別提供者，並將所有應用程式連線到雲端式身分識別提供者，以提供一致的使用者體驗和安全性。

進一步資訊的連結

- 就在這個世界密碼日，考慮一併擺脫密碼吧 | Microsoft 安全性

作業系統預設安全性設定

隨著安全性威脅形勢持續進化，我們看到對於預設設定的電腦安全性需求日益增加，目的在於改善網路恢復力。儘管作業系統安全性比以往更加急迫、複雜且更關乎業務，但正確處理並進行管理可能相當具有挑戰性。

在過去，電腦和裝置安全性包括了內建安全性功能，而客戶或 IT 專業人員都預期能依需求自行設定這些功能。這種方法不再適用，因為攻擊者利用在自動化、雲端基礎結構和遠端存取技術上更先進的工具來達成其目標。從晶片到雲端，所有安全層都進行預設設定因而變得相當關鍵。Microsoft 已進化到預設設定 Windows 作業系統安全性。[6]

注重深度防禦的客戶 (包括分層安全性態勢、新的安全性功能、定期和一致的修補和更新，以及通報網路釣魚和其他詐騙的安全性訓練和認知) 可以預期惡意軟體減少的情況。

為了簡化深度防禦，Windows 11 預設開啟了緊密整合的硬體和軟體防護，包括記憶體完整性、安全開機，以及信賴平台模組 2.0。Windows 10 使用者擁有同等能力的硬體時，也可以在 Windows「設定」應用程式或 BIOS 功能表中將這些功能開啟。

一般而言，較舊的裝置在硬體安全性和軟體安全性技術之間常常無法同樣的強度。對於未預設啟用安全性的裝置，務必盡可能在設定中進行手動設定。[7]

對於未預設啟用安全性的裝置，Microsoft 建議盡可能在設定中手動設定這些裝置。

主動套用持續的作業系統更新和安全性修補程，有助於在整個硬體和軟體生命週期提供保護。

可付諸行動的見解

1. 使用在信賴平台模組中綁定登入認證的無密碼解決方案，特別是尋找符合 Faster Identity Online (FIDO) 聯盟[8] 業界標準的無密碼解決方案。
2. 及時清除組織裝置上所有未使用和過時的可執行檔。
3. (如果未預設啟用) 透過啟用記憶體完整性、安全開機和信賴平台模組 2.0 來防範進階韌體攻擊，這將會使用現代 CPU 內建的功能來強化開機。
4. 開啟資料加密和認證防護。
5. 啟用應用程式和瀏覽器控制來增強保護以防止不受信任的應用程式，以及其他內建的入侵程式防護。
6. 啟用記憶體存取保護，以協助防範臨時起意的實體攻擊，例如有人將惡意裝置插入可從外部存取的連接埠。

進一步資訊的連結

- Windows 安全性書籍 | 商務
- Windows 11 的新安全性功能將有助於保護混合式工作 | Microsoft 安全性部落格 (英文)

軟體供應鏈集中程度

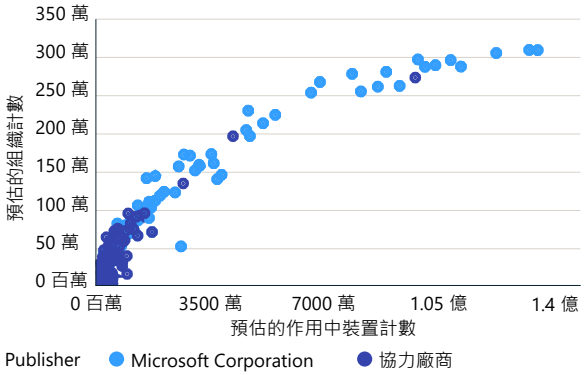
對第三方應用程式、外掛程式和延伸模組發動的攻擊，可能破壞客戶對供應生態系統中扮演主要角色的供應商的信任。使用網路理論來查看軟體集中程度，有助於清楚了解修補的關鍵性，尤其是對於中央應用程式。

擁有 1800 萬個應用程式可執行檔的 Windows App Network 已在 500 萬個組織內安裝和使用，提供了最上層的視野來綜觀我們的軟體生態系統。在 100,000 個最常用的應用程式中，有 97% 是由協力廠商組織所製作，其更新和安全修補程式也是由他們維護。這顯示了我們商業應用程式生態系統的兩項重要特性。

首先，Windows 商業應用程式生態系統具有集中性。只有前 100,000 (總數 1800 萬) 個應用程式會在 1,000 部左右的裝置上使用。換言之，這些應用程式在裝置生態系統中具有這種廣泛觸及效益者，只佔了其中 1% 的一半多。

其次，這些應用程式的管理能力具有多樣性，其中排名前 10,000 的應用程式供應商會管理這些最常用商業應用程式的更新和安全性修補程式。這證明了一家公司在多樣化的軟體供應商安全性、合規性和管理控制方面具備相互依存關係。

最常用應用程式的商業滲透情形



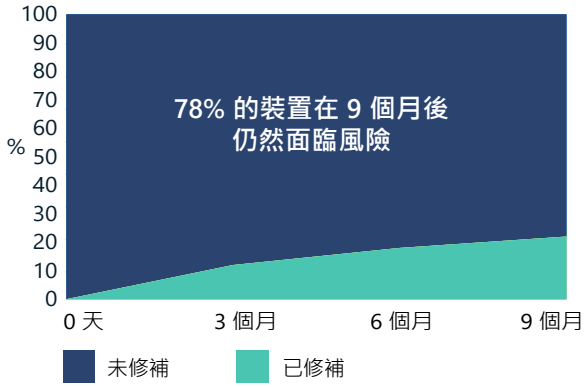
最熱門的應用程式會有數百萬個組織和數千萬部裝置使用。由於它們幾乎無所不在，因此敵手不斷尋找機會利用這些熱門應用程式中的漏洞，這可能會影響使用者群中的數百萬部裝置。

我們觀察到，有數百萬部商用裝置在修補程式發行後數個月，或甚至在產品支援終止後數年，仍在使用易受攻擊的應用程式版本。例如，有 100 多萬部作用中 Windows 商用裝置執行的 PDF 讀取器版本，自 2017 年後就不再支援。

不支援的舊版應用程式仍在數百萬部商用裝置上使用中。因此，組織便面臨了有漏洞卻無法修補的風險。

對於仍支援的應用程式版本，我們看到採用關鍵修補程式的速度正在下降，這種情況正好與提升恢復力的趨勢背道而馳。這個曲線本應呈現的是修補程式月增率呈指數上升，以達到所需的恢復力。

關鍵修補程式部署率



我們檢查了影響一組瀏覽器的 134 個版本的關鍵漏洞後，發現在修補程式發行後 9 個月，仍有 78% (相當於數百萬部裝置) 使用其中一個受影響的版本。

我們使用 InterpretML[9] 工具組來找出與可能有使用舊版應用程式的組織具有相互關聯的特性。這些預測指標中最重要的包括：與裝置互動的時數低；地理區域，如亞太地區和拉丁美洲；以及汽車、化學、電信、運輸與物流、保健付款人 (索賠處理人) 和保險等產業。

軟體恢復力維護應包括定期停用或解除安裝未使用的應用程式。

組織的安全性和合規性有賴於本身的努力，以及其軟體供應商的付出。

可付諸行動的見解

1. 及時更新組織內的所有應用程式和端點。
2. 及時清除組織裝置上所有未使用和過時的可執行檔。

進一步資訊的連結

- Microsoft Intune 文件 | Microsoft Docs
- 管理應用程式 | Microsoft Docs
- 適用於端點的 Microsoft Defender | Microsoft 安全性
- OSS 安全供應鏈架構 | Microsoft 安全性工程
- Microsoft 開放原始碼軟體安全供應鏈架構 | GitHub

培養對抗新興 DDoS、Web 應用程式和網路攻擊的韌性

加速的數位轉型終結了傳統網路和安全性周邊模型。移向雲端意味著企業必須採用雲端原生網路安全性來保護數位資產。

攻擊複雜度、頻率和數量持續增加，而且不再限於假期，表示已轉向全年攻擊。這突顯持續保護的重要性超越了傳統尖峰流量季節。

分散式阻斷服務 (DDoS) 攻擊

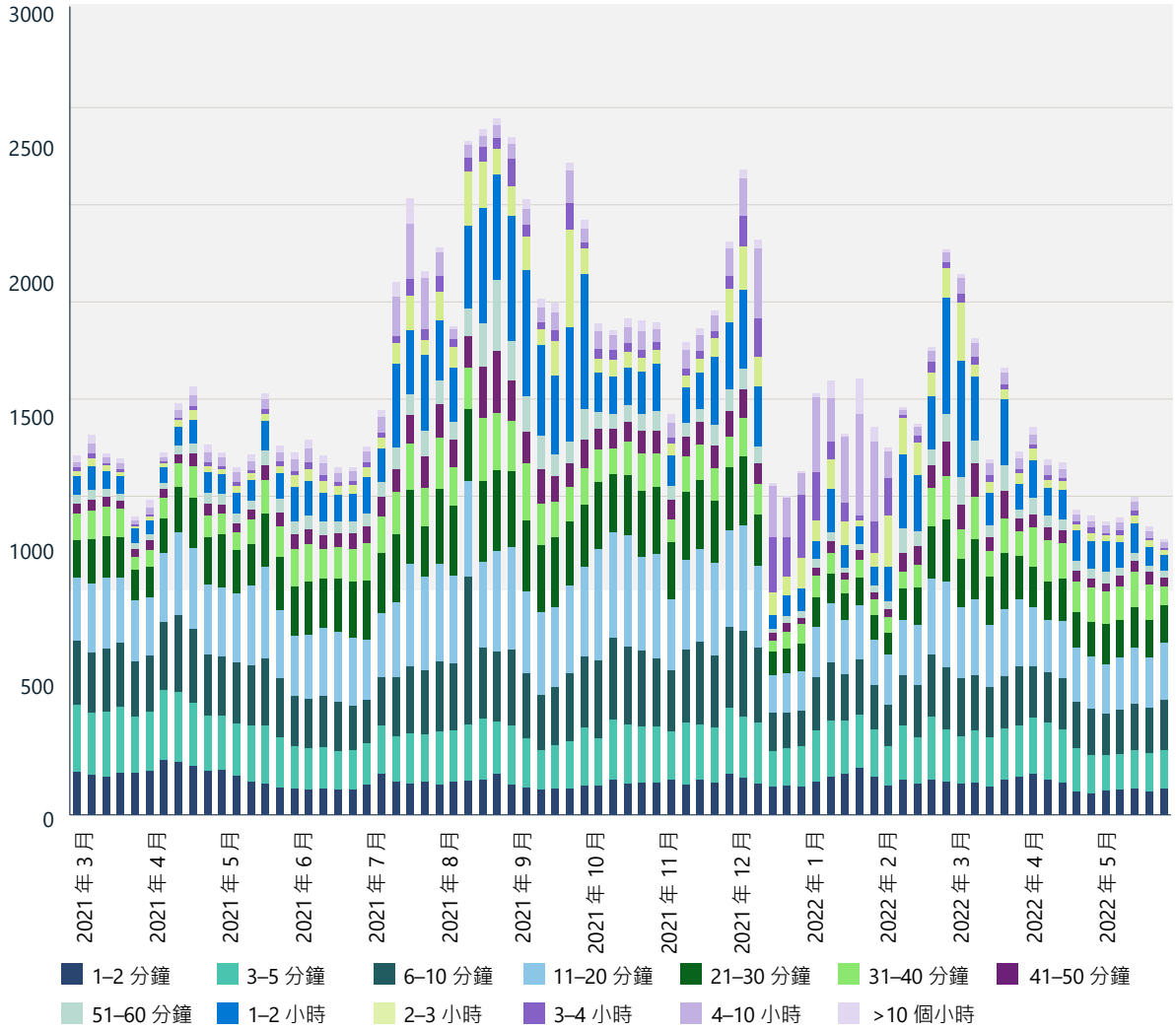
在過去一年，全球經歷的 DDoS 活動在數量、複雜度和頻率上都是前所未見。此 DDoS 暴增是因國家級攻擊大量增加，以及低成本的受雇型 DDoS 服務持續擴散所致。Microsoft 每天平均阻擋了 1,955 次攻擊，比去年增加了 40%。先前攻擊的尖峰數量通常發生在年底的假期。然而，今年記錄最高的一天是在 2021 年 8 月 10 日。這可能表示轉向全年攻擊，並突顯持續保護的重要性超越了傳統尖峰流量季節。

2021 年 11 月，Microsoft 阻止了來自多個國家 / 地區約 10,000 個來源的容積式 DDoS 攻擊，其每秒輸出量為 3.4 TB (Tbps)。在 2022 年也削減了 2+Tbps 以上類似的高容積式攻擊，突顯出不只是攻擊的複雜度和頻率在增加，攻擊的容積 (頻寬) 也在增加。

攻擊持續時間

過去一年觀察到的大多數攻擊持續時間都很短。約 28% 的攻擊持續不到 10 分鐘，26% 持續 10–30 分鐘，14% 持續 31–60 分鐘。32% 的攻擊持續超過一小時。

DDoS 攻擊數量和持續時間分佈情形
(2021 年 3 月 –2022 年 5 月)



過去一年大多數攻擊持續時間都很短。約 28% 的攻擊持續不到 10 分鐘。

培養對抗新興 DDoS、Web 應用程式和網路攻擊

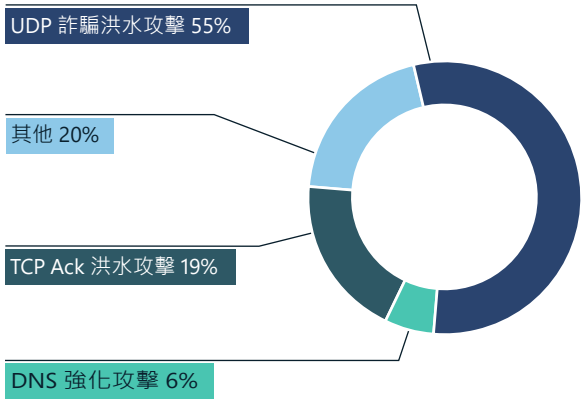
續

DDoS 攻擊媒介

在過去一年，常用的攻擊媒介是連接埠 80 上的使用者資料包通訊協定 (UDP) 反射，這是使用簡單服務探索通訊協定 (SSDP)、非連線式輕量型目錄存取通訊協定 (CLDAP)、網域名稱系統 (DNS)，以及包含單一尖峰的網路時間通訊協定 (NTP)。我們也看到鎖定網站為目標的應用程式層 DDoS 攻擊增加 ·包含 1630 萬個尖峰 RPS (每秒要求數) 和 9.89 Tbps 尖峰流量。

在 2022 年，Microsoft 每天消除了將近 2,000 次 DDoS 攻擊，並阻止了史上最大宗的 DDoS 攻擊。

DDoS 攻擊媒介



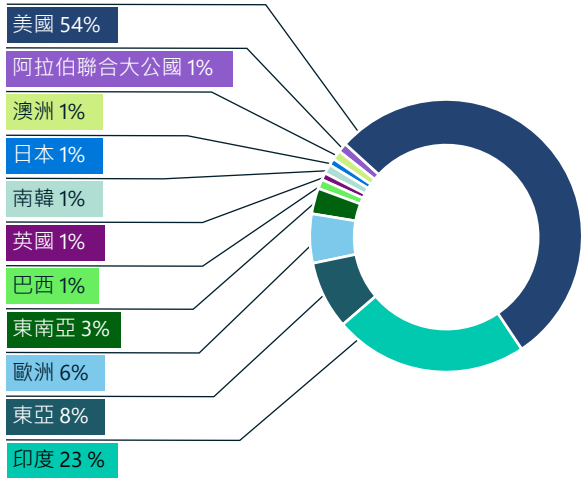
UDP 詐騙洪水攻擊在 2022 年上半躍升為首要媒介，從 16% 上升到 55%。TCP Ack 洪水攻擊從 54% 下降至 19%。

遊戲產業持續成為 DDoS 攻擊的首頁目標，這些攻擊大多來自 Mirai 殭屍網路和低流量 UDP 通訊協定攻擊的變種。由於 UDP 常用於遊戲和串流應用程式，因此絕大多數的攻擊媒介是 UDP 詐騙洪水，而有一小部分是 UDP 反射和放大攻擊。

地理目標區域

過去一年偵測到的 DDoS 攻擊中，有 54% 是鎖定美國為目標而發動，這個趨勢的形成有一部分可能是因為大多數 Azure 和 Microsoft 客戶都位於美國。我們還看到對印度的攻擊大幅上升，從 2021 年下半僅佔所有攻擊的 2%，到 2022 年上半已增加至 23%。東亞 (尤其是香港) 仍然是熱門目標，佔 8%。而在歐洲，我們看到了對阿姆斯特丹、維也納、巴黎和法蘭克福地區的集中攻擊。

DDoS 攻擊目的地

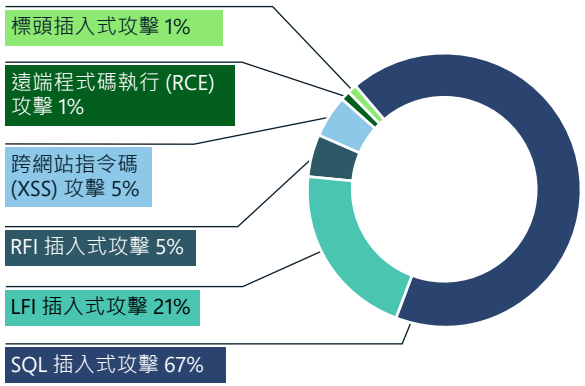


我們將亞洲大量攻擊歸因於該區域廣大的遊戲覆蓋範圍，尤其是在中國、日本、韓國和印度。這個覆蓋範圍將繼續擴大，因為智慧型手機越來越普及使得手機遊戲的熱門程度提升，這也暗示著這個地理目標未來只會繼續成長。

Web 應用程式入侵

Web 應用程式防火牆 (WAF) 結合 DDoS 保護，形成了保護 Web 和應用程式設計介面 (API) 資產的深度防禦策略的一部分。Microsoft 觀察到，每月透過 Azure WAF 觸發超過 3000 億條 WAF 規則。

最猖獗的攻擊類型分佈情形



Azure WAF 每天偵測到數十億次 Open Web Application Security Project (OWASP) 前 10 大[10] 攻擊。根據我們的訊號，攻擊者大多試圖發動 SQL 注入攻擊，接著再進行本機檔案注入和遠端檔案注入攻擊。這符合 OWASP 十大清單，顯示注入攻擊是排名第三的最常見 Web 攻擊類型。

另外，針對 Azure Web 應用程式的機器人攻擊也有所增加，每月平均有 17 億個機器人請求，而該流量中有 4.6% 包含惡意機器人。

培養對抗新興 DDoS、Web 應用程式和網路攻擊的韌性

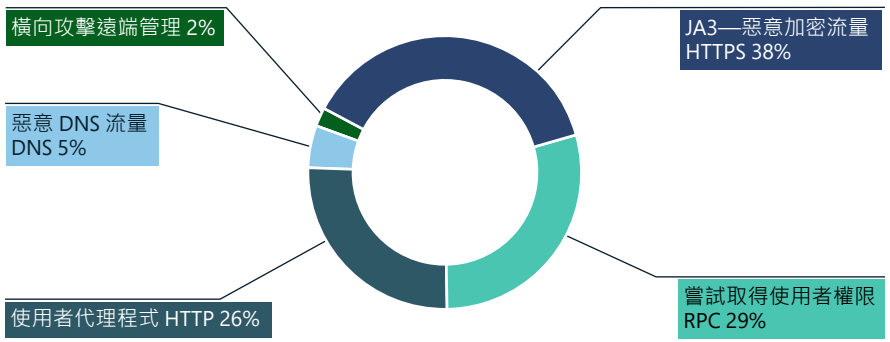
續

由於執行認證填充攻擊、信用卡詐欺、網路勢力活動及供應鏈攻擊的機器人數量不斷增加，我們預期對 Web 應用程式的機器人攻擊也會持續增加。

網路入侵：偵測和預防

我們觀察到 2022 年的網路層入侵 (尤其是惡意軟體) 大幅增加。光是在 6 月，Azure 防火牆入侵偵測和預防系統 (IDPS) 就封鎖了超過 1.5 億個連線。

IDPS 拒絕流量原因



IDPS 流量警示原因

對 IDPS 警示和拒絕流量的分析顯示下列攻擊者使用的方法。在拒絕流量中，我們看到攻擊者使用 SSL 來隱藏其活動，而遠端執行攻擊也變得越來越普遍。在警示流量中，我們看到 SMB/SMB2 通訊協定用來執行遠端執行攻擊。

可付諸行動的見解

1. 檢查資料中心或雲端服務內系統之間的所有流量，以及試圖存取的流量。
2. 制定健全的全年網路安全姓回應策略。
3. 使用雲端原生安全性服務來實施健全的零信任網路安全性態勢。

進一步資訊的連結

- 使用 Azure 防火牆改善您對勒索軟體攻擊的安全性防禦 | Azure 部落格和更新 | Microsoft Azure (英文)
- 剖析 DDoS 放大攻擊 | Microsoft 安全性部落格 (英文)
- 使用 Azure Web 應用程式防火牆實現從邊緣到雲端的智慧型應用程式防護 | Azure 部落格和更新 | Microsoft Azure (英文)

發展平衡的方法來實現資料安全性和網路恢復力

數位轉型加速了資料資產的大幅擴充，並促使安全性、合規性和隱私權的風險升高。具網路恢復力的組織必須在資料保護、合規性和復原能力方面權衡投資，並將這些與專門的法規回應程序整合，以因應獨特的違規類型。

資料外洩不是問題，何時發生才是問題。IBM 和 Ponemon Institute 的「2021 年資料外洩成本」研究報告指出，全球平均資料外洩成本為 $424 萬美元 (比前一年增加 10%)，而美國則為 $905 萬美元。當中發現，合規性錯誤是成本擴大的最大因素。反之，資料外洩成本降低則與像是事件回應 (IR) 規劃、零信任部署成熟度、安全性 AI 和自動化，以及使用加密等最佳做法關聯。

資料外洩在所難免。組織若採取平衡的復原方法，將能減少資料外洩的頻率、影響和成本。

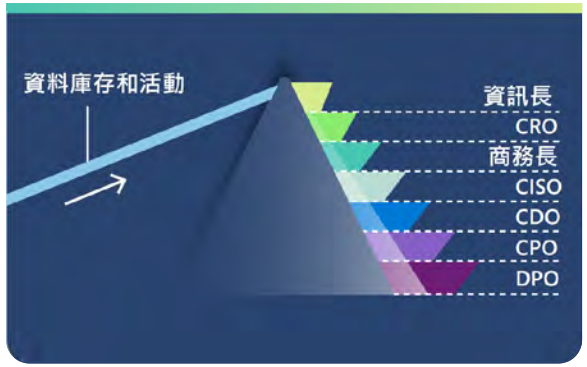
資料治理、安全性、合規性和隱私相互依存

我們已看到，資料在近幾年越來越重要，成為組織創造價值的關鍵引擎。同時，要求資料治理和安全性的隱私權法規興起，讓風險角色的界線變得模糊。像是資料長 (CDO) 或隱私權主管 (CPO) 等新興的高階主管角色特別關注安全性和合規性，但資料保護的實施和運作通常是倚賴資訊長 (CIO) 和 / 或資訊安全長 (CISO) 帶領的團隊。這不是一條單行道，因為 CDO 所帶領的資料治理計畫也具有安全性效益。由於這種相互關聯性，使得 IT、資料治理、安全性、合規性和隱私權團隊需要更密切地合作，以提高效率和管理風險。

整個組織資料資產的未來，就是統一資料風險管理平台

由於每一個領域都有客製化應用程式，且整個傳統組織混合、多雲端資料蔓生的擴及範圍不一致，在這樣的環境中，很難統整 IT、資料治理、安全性、合規性和隱私權管理流程。我們認為，組織需要單一窗口來尋找和了解其資料、保護其資料、控管資料的存取、使用和生命週期，以及在整個資料資產內防止資料遺失發生。

從相同的資料庫存和活動資訊著手處理，可促進跨團隊的流程、產生更全面的風險視野，並且讓組織更妥善準備和簡化對資料外洩的回應。



「單一窗口」應像稜鏡一樣。若團隊在資料安全性、合規性和隱私權方面面臨風險，就需要從不同卻一致的視角來了解相同的資料庫存和活動，以協調一致並協作。資料活動包括資料存取、修改和移動事件，這是資料安全性方程式非常寶貴的部分。

有效的資料治理、安全性、合規性和隱私是相互依存，並且需要跨團隊協作。

可付諸行動的見解

1. 投資合規性、資料保護和回應功能，以便在防禦與復原之間取得平衡，並將資料外洩的影響降到最低。
2. 開發並採用能跨越資料風險孤島並涵蓋完整資料資產的流程和工具。

進一步資訊的連結

- Microsoft Purview—資料保護解決方案 | Microsoft 安全性 (英文)
- 合規性和資料治理的未來已經發生：Microsoft Purview 簡介 | Microsoft 安全性部落格 (英文)

網路勢力活動的韌性：人性層面

在過去五年中，圖形和機器學習方面的進步引入了容易使用的工具，這些工具能夠快速產生高品質的逼真內容，而且幾秒鐘內就能廣泛散播到網際網路上。

而在透過文字、音訊和視覺內容通報的事件方面，我們來到了無論人類或演算法都無法可靠地分辨虛實的境界。這些工具及其輸出的激增，令人懷疑所有數位媒體的可信度，擾亂了我們對地方和世界事件的理解。技術進步所推動的新形式勢力活動已對民主進程造成嚴重的影響。[11]

問題在於，我們如何做好準備迎接更具韌性的未來，以對抗這些網路勢力活動。技術只是整張拼圖的一小塊。需要多方共同努力，包括注重媒體素養、意識和警戒的教育、對高品質新聞報導的投資 (在地方上、全國和國際上都有值得信賴的記者在現場)、分享和警示勢力活動的網路，以及新型態的法規，能夠處罰製作或操控數位媒體從事欺騙的惡意行為體。

我們也認知到，恢復對數位資訊的信任是一項遠大的目標，需要多元的觀點和參與。沒有任何一家公司、機構或政府能夠自行解決這些威脅。我們身為人類的強大動力，就是彼此協作和合作的能力。這一點現在尤其重要，因為需要所有人 (全球政府、產業、學術機構，以及特別是新聞、社會和媒體組織) 一起努力改善並促進健康的社會。

進一步資訊的連結

- 國防部網路任務中人工智慧的應用情形 | Microsoft 問題焦點 (英文)
- 人工智慧與網路安全性：新興挑戰與展望的方向。網路安全小組委員會前人工智慧應用於網路行動相關聽證會，參議院軍事委員會第 117 屆代表大會 (2022 年 5 月 3 日；Eric Horvitz 的證詞)

透過技能培養來鞏固人為因素

解決人為因素是任何網路安全性技能策略的重要環節。根據 Kaspersky Human Factor in IT Security (IT 安全性的人為因素) 研究[12] 顯示，46% 的網路安全性事件涉及粗心或制服員工不小心促成攻擊。

在數位安全性與韌性組織中的 Microsoft 教育與認知團隊負責鞏固網路安全性的人為因素，藉由賦予員工保護自身和客戶的系統與資料的能力來履行這項責任。我們的目標是：

- 在員工群體中建立集中的企業核心安全技能，藉此降低 Microsoft 和客戶面臨的風險。
- 透過多階段的訓練強化方法提升員工的安全性知識，以支援期望的行為成果。
- 每年舉辦必要的安全訓練和活動，將安全心態融入 Microsoft 的文化當中，以促進文化變革。
- 推廣一站式集中 Web 資源來納入最佳實務做法、公司政策資訊和事件報告，以獲得有關網路安全性的一切知識。

每年至少對每一位 Microsoft 員工實施一次目標式的集中網路安全技能計畫。訓練方案經過最佳化，可支援目前的網路安全計畫，並提供可衡量的行為成果。Microsoft 資訊風險管理委員會 (IRMC) 在確認要藉由訓練來達成的重要網路安全行為改變成果方面發揮著關鍵作用。

我們利用所有的網路安全技能計畫，盡可能衡量解決方案的效率、效益和成果。例如，我們的內部威脅技能方案具有 95% 的訓練合規性、出色的學習者滿意度，並且透過公司的「立即通報」(Report It Now) 工具達到大幅增加主管通報可能的內部威脅案例。計畫內容包括：

安全性基礎：集中式企業網路安全認知與合規性訓練，目的在於因應核心安全性和隱私權做法。這項高度預期的訓練系列採用寓教於樂的模式，讓學習網路安全性的過程具吸引力又有趣。

STRIKE：建置和維護企業營運解決方案的工程師必修的 Microsoft 技術訓練。這項僅限受邀參加的訓練目的在於因應網路安全檢疫最佳做法中及時且關鍵的層面，並採取專為目標對象需求量身打造的現場授課模式進行。

計畫專屬：目標式訓練計畫支援特定網路安全性計畫，包括影子 IT、內部威脅和 Microsoft Federal。這些方案透過高階主管支持與計分卡報告緊密整合到個別網路安全性計畫的整體互動策略中，以避免敷衍了事的「打勾」訓練方法。

MSProtect：Microsoft 的集中 Web 資源提供了最佳實務做法、公司政策資訊和事件報告，以獲得有關網路安全性的一切知識。這項隨選資源是員工在正式訓練方案以外的首選。

> 安全技能不得視為為了合規而敷衍了事的打勾活動。而是應著重行為改變以觀察確立的目標行為成果，並建立傾聽系統來判斷方案的影響。

可付諸行動的見解

1. 提供安全性訓練和資源，因應員工任何時候、任何地點的需要。
2. 制定集中式的技能策略，在整個企業中透過利益關係人告知。
3. 確實追蹤並分析訓練的影響，了解其效率 (數量)、效益 (品質) 和成果 (業務影響)。

進一步資訊的連結

- 在協助了 3000 萬人後，Microsoft 展開了下一階段的技能計畫

從我們的勒索軟體消滅計畫洞察先機

在過去五年中，Microsoft 始終在自己的零信任之旅[13] 不斷邁進，以確保身分識別和裝置受到健全的管理並保持良好狀態。隨著勒索軟體風險增加，我們發展出更深入的觀點來支援保護自己和客戶的方法。

經過深度的外部評估後，我們制定了勒索軟體消除計畫來補救控制和涵蓋範圍之間的差距，促進如適用於端點的 Defender、Azure 和 M365 等服務的功能改進，並且為我們的 SOC 和工程團隊開發劇本，以應對勒索軟體攻擊事件的復原工作。

第一步就是了解我們應對 Microsoft 遭到勒索軟體攻擊時的防護範圍。雖然我們在部署適用於端點的 Defender 以及確保所有裝置受到管理且符合我們的零信任原則方面，已做出相當大的努力，但我們仍需找出方法來了解我們是否能從攻擊中有效復原這個問題的所有面向。為了深入洞悉，我們評估了 NIST 8374：勒索軟體風險管理：網路安全性架構 (CSF) 設定檔[14]，這與我們遵循已知控制清單的整體企業政策相符。這項分析很快就找出涵蓋範圍的缺口。

我們隨後將 CSF 的識別、偵測、保護、回應及復原功能的缺口劃分出優先順序。我們找到對零信任和其他計畫的策略調整，也發現沒有現有工作流的缺口。在評估補救這些缺口所需的工作和付出的努力程度後，我們將其分成兩大支柱：

- **保護企業 (PtE)**：定義我們身為企業為了保護自己並能夠從攻擊 (假如成功的話) 中復原所需進行的工作項目。
- **保護客戶 (PtC)**：將功能內建到我們的方案中，以保護客戶及業務。

將調查結果嵌入自己的企業中

為了補救主要風險並保護我們的關鍵服務，以防範勒索軟體攻擊，我們計畫未來 6 到 12 個月將投資重點放在實現專屬勒索軟體計畫中的下面五個案例。一旦我們在每一個案例獲得成功，就會逐步將計畫的範圍擴展到企業的各個層面。

案例 1：安全性團隊成員了解有關勒索軟體攻擊的整體風險，並建立流程來對高階主管提供控制差距和風險狀態的認知。

案例 2：安全性團隊成員可存取專為他們和其他 Microsoft 內部團隊所設計的劇本，協助他們回應勒索軟體攻擊並從攻擊中復原關鍵服務。

案例 3：企業復原能力團隊成員擁有能依循的標準，幫助他們進行關鍵系統備份。有劇本存在，以及定期進行備份和復原的練習，就能確保在發生勒索軟體攻擊時復原資料。

案例 4：服務擁有者了解和實施必要的安全性和營運控制與政策，以保護其服務、客戶資料、端點和網路資源，避免遭受勒索軟體攻擊，並特別著重優先處理劃分為 Microsoft 關鍵服務的服務。

案例 5：所有員工都能存取教育和訓練資源，這些資源描述如何辨識勒索軟體攻擊，以及如何通知安全性團隊並展開回應。

可付諸行動的見解

1. 記載和驗證對關鍵服務所發動的勒索軟體攻擊相關的端對端復原和補救活動。
2. 讓利益關係人參與更新您的企業危機管理劇本來納入勒索軟體特定活動，以及判斷是否 / 何時支付勒索軟體的決策流程和指導方針。
3. 透過在部署的安全性產品中提供可用功能 (例如 Defender for Endpoint Attack Surface Reduction 規則) 來改善偵測和防護的涵蓋範圍。
4. 與安全性標準團隊合作，定義防範勒索軟體攻擊的基準，並為工程團隊提供如何防範勒索軟體攻擊的訓練和文件。
5. 實施自動化，讓 DevOps 團隊更容易部署安全性和營運策略，並確保在系統偏離合規性時能夠迅速發現和補救。

進一步資訊的連結

- 分享 Microsoft 如何防範勒索軟體 | Microsoft Inside Track

立即採取行動解決量子安全性問題

管理量子運算對當今加密及其保護的一切所造成威脅的壓力正在增加。近期發佈的「改善國家安全局國防與情報社群系統網路安全性備忘錄」[15] 擴大延伸了第 10428 號美國行政命令[16]「改善國家網路安全性」，突顯軟體供應鏈安全性對於因應未來國家級攻擊來說至關重要。

什麼是量子電腦？

量子電腦是使用量子物理特性來儲存資料和執行運算的機器。這對於某些工作來說是非常有利的，因為其表現能夠大幅超越我們最厲害的超級電腦。量子運算已開拓了資料加密和處理的新領域。研究預測，量子運算最快將在 2030 年成為一個價值數十億美元 (USD) 的量子工業。[17] 事實上，量子運算和量子通訊準備在多種產業中發揮改革作用，範圍涵蓋從醫療保健與能源到金融與安全性。

量子運算對於當今加密及其保護的一切構成威脅。

對當今加密的威脅

只要利用 Shor 的 1994 演算法和一台具有數百萬個物理量子位元的工業規模量子電腦，就可能有效破解我們目前廣泛部署的所有公開金鑰加密演算法。重要的是，務必考慮、評估和標準化「量子安全」加密系統在對抗敵手量子攻擊時的效率、敏捷性和安全性。軟體轉向「後量子加密」，也就是現有的典型演算法和通訊協定對抗量子攻擊達到健全狀態，將需要數年時間 (即使不需十年或更久時間) 才能達成。[18]

這表示，管理對當今加密及其保護的一切所造成威脅的壓力正在增加。敵手現在能夠記錄加密資料，並且在之後量子電腦可用時利用它。等待量子運算到來才處理其加密問題，便為時已晚。

由於加密技術在整個網路生態系統中普遍使用，這表示我們的加密型安全性服務可能遭到入侵。例如，這些服務包括通訊 (TLS、IPSec)、傳訊 (電子郵件、網路會議)、身分識別和存取管理、網路瀏覽、程式碼簽署、付款交易，以及其他依賴加密保護的服務。

隨著量子電腦成為現實，實作加密演算法和功能的第三方軟體元件也需要額外的審查。這就需要價值鏈中的所有組織克盡義務，確保供應鏈安全無虞。產業機構和政府機構正投入更多努力來定義軟體供應鏈安全性需求，並且在某些案例中導入新的要求來保護供應鏈。國家安全備忘錄 NSM-8[19] 針對在國家安全系統 (NSS) 中實施後量子加密制定了需求和時程表。它提出在 180 天內對「現代化規劃、使用不支援的加密、核准的任務特有通訊協定、抗量子通訊協定，以及規劃必要時使用抗量子加密」的時程預期。

標準化是過渡到量子安全加密的長期前置活動。標準機構原先處理使用公開金鑰加密的標準，現在則必須開始試驗並適應後量子演算法。

新的後量子加密 (PQC) 演算法 (一般認為傳統演算法能有效防禦量子攻擊) 現在正由 NIST 的後量子標準化專案進行審查。[20] 這項工作將影響標準機構內的全球工作。雖然與美國政府的演算法選擇有部分重疊，但對於符合標準的演算法，不同的國家級機構 / 法規選擇可能會帶來國際挑戰。這種支離破碎的情況將反而使得產品和服務工程更加複雜。

NIST 的後量子加密標準化計畫正在審查新的後量子加密演算法。這項工作將影響標準機構到的全球工作。

可付諸行動的見解

除了 SAFECode 和合作夥伴成員之外，業界也應立即進行短期活動，為 PQC 過渡做好準備。[21] 包括：

1. 選擇使用加密的產品 / 程式碼庫存。
2. 在組織中實施加密敏捷性策略，包括將加密變更時所需的程式碼流失率降到最低。
3. 在使用加密的產品或服務中試用候選的量子安全演算法。
4. 準備好使用不同的公開金鑰演算法進行加密、金鑰交換和簽名。
5. 測試您的應用程式，了解非常大的金鑰大小、密碼和簽名的影響。

進一步資訊的連結

- Microsoft 證明了建立新型量子位元所需的基礎物理學 | Microsoft 研究

整合商務、安全性和 IT 以提高韌性

健全的網路恢復力有賴於企業領導者與安全性團隊相互合作來實施安全性。根據 Microsoft 的經驗，安全性領導力是一個具有挑戰性的專業領域，需要來自組織領導者的支援，才能最有效地保護組織。

安全性負責人面對一系列動態挑戰，涵蓋風險、技術、經濟、組織流程、商業模式、文化轉型、地緣政治利益、間諜活動及國際制裁合規性等相關主題。其中每一項都伴隨需要理解和密切管理的細微變化。

安全性負責人還肩負了打擊智慧型、資金充沛且懷有強烈動機的人類攻擊者，以及技能不純熟但有效的網路罪犯。他們的團隊必須保衛從安全性優先順序低、甚至不存在的年代以來，歷經 30 年以上的時間逐漸累積起來的複雜技術資產。數年前做出的決策可能在今日帶來風險，直到還清技術債務並填補安全性方面的差距為止。

組織領導者和政策制定者能夠透過主動支援安全性負責人，並協助搭起整體安全性與組織其餘部分之間的橋樑，對安全性產生積極正面的影響。當 Microsoft 與具有此共識的客戶合作時，我們看到他們打造出更具韌性的組織，同時改善敏捷性來適應和創新。

組織領導層可專注於三個關鍵領域來支援安全性負責人：

1. 從設計建立安全性

安全性有時被視為業務流程中的障礙或事後考量，常常只有在來不及避免風險或只能便宜行事地修正時，才會納入決策考量。

組織領導者和政策制定者應確保：

在新計畫初期即納入安全性。新的數位計畫和雲端採用應優先處理安全性，以確保組織風險不會隨著每一個新的應用程式或數位功能而增加。一旦可靠地納入安全性，您就可以使用這些流程將舊版系統現代化，同時獲得安全性和工作效率方面的優勢。

將安全性的預防性維護正常化。確保基本安全性維護 (如套用安全性更新和修補程式及保護設定) 分配到完整的組織支援，包括預算、排定的停機時間、為廠商產品提供支援的收購需求。

不幸的是，許多組織一再延遲、延後或僅部分應用這些常見做法。這就讓攻擊者得到相當大的機會來進行入侵。安全性正常化的需求已納入 US NIST 800-40 中。[22]

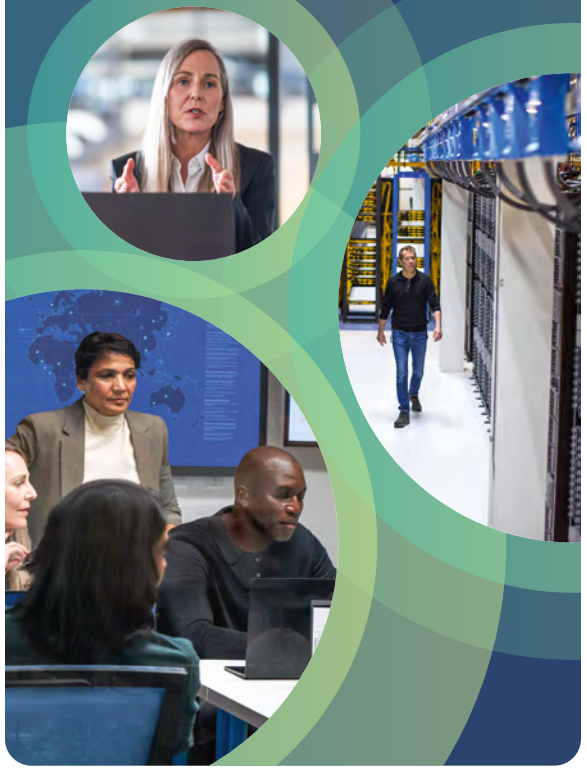
2. 參與安全性

組織領導者應積極參與和贊助關鍵安全性流程，確保優先處理資源和整備度以因應安全性嚴重損害。這包括參與：

確定關鍵業務資產。安全性負責人和團隊需要知道哪些是關鍵業務資產，以便將安全性資源的重點放在最重要的環節。這通常是一種新作為，包括提出和回答先前未處理過的新問題。

網路安全性業務續航力和嚴重損壞修復作為。網路攻擊可能成為大多數或所有業務營運中斷或停擺的重大事件。確保整個組織的團隊都以準備好處理這些情況，就能縮短恢復業務營運的時間、限制對組織造成的損害，並且協助維持客戶、市民和選民的信任和信心。這個做法應整合到現有的業務續航力和嚴重損壞修復流程中。

安全性風險的決策者，最好是具備所有風險和機會的完整可見度的業務或任務負責人。



整合商務、安全性和 IT 以提高復原力

續

3. 正確定位安全性

組織建構安全性風險責任制的方式，往往令他們無法做出良好的安全性風險決策。風險決策者最好是具備所有風險和機會的完整可見度的業務或任務負責人，但組織通常（有意或無意地）將安全性風險責任交給安全性團隊中的主題專家負責。這種做法為安全性團隊帶來不良負擔，同時使得企業負責人失去對業務關鍵風險的可見度和掌控力。組織可以修正這一點：

讓企業負責人做好準備：教育企業負責人全面了解安全性風險，以及這些威脅如何影響其業務。直接與安全性團隊接觸，也能增進安全性與整體業務敏捷性的協作關係。

將安全性風險交給企業負責人負責：隨著企業負責人獲得足夠的資訊得以了解並接受安全性風險，組織應明確將安全性風險的責任轉移給他們，同時仍由安全性團隊負責管理該風險，並為負責人提供資訊充足的專業知識和指導方針。

「從良好的資料備份開始，網路復原能力正從傳統業務續航力和嚴重損壞修復逐步進展到流程、技術及其相依性（包括人員和第三方）的復原功能；並且朝向持續運作、自我修復服務、關鍵角色的復原能力，以及關鍵第三方的容錯移轉前進。最具韌性的組織會促進 IT、業務主管和安全性專業人員之間的整合。出色的復原能力會在一開始就將復原能力納入設計之中、進行安全的變更管理，並且實現細微的錯誤隔離。網路恢復力只是良好的萬全準備計畫中的一個環節。隨著網路風險增加，網路安全性和復原能力之間的交集變得更加重要，資訊安全長 (CISO) 與企業復原能力計畫的關係也越來越穩固。每年都有越來越多的 CIO 接管全公司的復原能力。」

Lisa Reshaur
Microsoft 風險管理部門總經理

進一步資訊的連結

- 從復原能力到數位毅力：組織如何使用數位技術在前所未逢的時代開拓新頁 | Microsoft 官方部落格（英文）
- IT 和安全性團隊如何相互合作以提高端點安全性 | Microsoft 安全性

網路恢復力貝爾曲線

每個組織都應採行恢復力成功因素

如我們所見，許多網路攻擊會成功，只是因為組織未遵循基本安全性檢疫。每個組織應採行的最低限度標準包括：

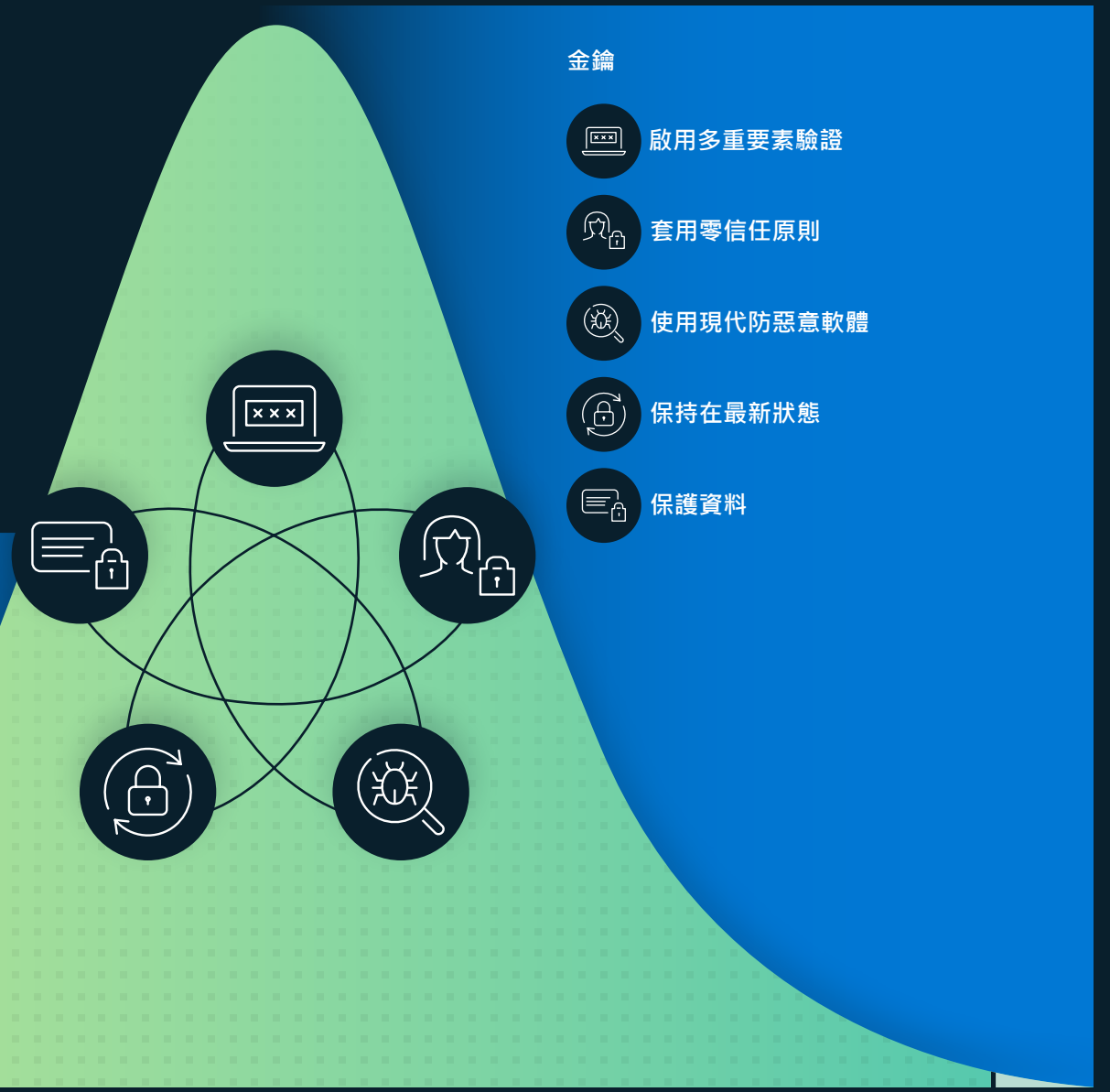
- **啟用多重要素驗證 (MFA)**：為了保護遭到入侵的使用者密碼，並協助為身分識別提供額外的恢復力。
- **套用零信任原則**：任何限制對組織所造成影響的恢復力計畫的基石。這些原則包括：

1. 明確驗證—確認使用者和裝置處於良好狀態，再允許存取資源。
2. 使用最低權限存取—僅允許存取資源所需的權限，別無其他。
3. 假設資料外洩—假設系統防禦遭到破壞，而系統可能遭到入侵。這表示持續監視環境是否發生可能的攻擊。

- **使用擴大偵測和回應防惡意軟體**：實作軟體來偵測並自動封鎖攻擊，以及提供安全性作業的深入見解。監視從威脅偵測系統獲得的深入見解，對於能及時回應威脅來說至關重要。
- **保持在最新狀態**：未修補和過時的系統是許多組織成為攻擊受害者的主要原因。務必確保所有系統處於最新狀態，包括韌體、作業系統和應用程式在內。
- **保護資料**：清楚您的重要資料、所在位置以及是否實作適當的系統，對於實施適當的防護措施來說至關重要。

98%

基本安全性檢疫仍能抵禦 98% 的攻擊。



章節附註

1. 端點偵測及回應 (EDR) 是企業端點安全性平台，其設計目的是為了幫助企業網路防止、偵測、調查及回應進階威脅。端點偵測及回應功能提供了近即時且可付諸行動的進階攻擊偵測能力。安全性分析師可有效地劃分警示的優先順序、深入洞察資料外洩的完整範圍，並做出回應行動來修復威脅。
2. 端點保護平台 (EPP) 是部署在端點裝置上的解決方案，目的是防止檔案型惡意軟體、偵測和封鎖來自信任和不信任應用程式的惡意活動，以及提供動態回應安全性事件和警示所需的調查和修復功能。
3. https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted
4. https://docs.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-number-match
5. https://docs.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-additional-context
6. Windows 安全性書籍：商務
7. Windows 11 的新安全性功能將有助於保護混合式工作 | Microsoft 安全性部落格 (英文)
8. FIDO 聯盟：開放式驗證標準比密碼更安全
9. https://interpret.ml/
10. OWASP 十大 | OWASP 基礎
11. https://blogs.microsoft.com/on-the-issues/2022/05/03/artificial-intelligence-department-of-defense-cyber-missions/
12. https://www.kaspersky.com/blog/the-human-factor-in-it-security/
13. https://aka.ms/ZTatMSFT
14. https://csrc.nist.gov/publications/detail/nistir/8374/final
15. https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/
16. 第 14028 號行政命令「改善國家網路安全性」
17. https://thequantumdaily.com/2020/02/18/the-quantum-computing-market-size-superpositioned-for-growth
18. 「The Long Road Ahead to Transition to Post-Quantum Cryptography」(迎接後量子加密的未來之前漫長的過渡期) (英文)，https://cacm.acm.org/magazines/2022/1/257440-the-long-road-ahead-to-transition-to-post-quantum-cryptography/fulltext
19. https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/
20. https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization
21. https://safecode.org/blog/preparing-for-post-quantum-cryptography-roadmap-initial-guidance/
22. https://csrc.nist.gov/publications/detail/sp/800-40/rev-4/final

參與團隊

參與團隊

本報告中的資料和見解是由一群具有多元背景並以安全性為重點的專業人士所提供，這些人任職於多個不同的 Microsoft 團隊。他們的共同目標是保護 Microsoft、其客戶和全世界免受網路攻擊的威脅。我們很自豪能以透明的精神分享這些見解，共同目標是讓世界成為一個對所有人來說都更安全的地方。

AI 為善 (AI for Good) 研究實驗室：擁抱資料和 AI 的威力以因應世界上的許多挑戰。該實驗室與 Microsoft 以外的組織共同合作，應用 AI 來改善生計和環境。重點領域包括網路安全 (假資訊、網路安全性、兒童安全)、災害應變、永續性和 AI 健康服務 (AI for Health)。

Azure Edge 與平台、企業和作業系統安全性：負責跨 Windows、Azure 及其他 Microsoft 產品的核心作業系統與平台安全性。該團隊打造出業界領先的安全性和硬體解決方案並納入 Microsoft 平台中，用以阻止從晶片到雲端的各種惡意探索、身分識別和惡意軟體入侵。跨 PC、邊緣和伺服器、Microsoft Pluton 安全性處理器等的 Microsoft 安全核心平台創作者。

Azure 網路，核心：這個雲端網路團隊專注於 Microsoft WAN、資料中心網路及 Azure 的軟體定義網路基礎結構，包括 DDoS 平台、網路邊緣平台及網路安全性產品，如 Azure WAF、Azure 防火牆和 Azure DDoS 保護標準。

雲端安全性研究團隊：這個團隊致力於保護 Microsoft 雲端、打造創新的安全性功能和產品，並從事研究，以保護客戶並讓客戶能夠安全地進行組織轉型。

客戶安全性與信任 (CST)：這個團隊負責推動 Microsoft 產品和線上服務的客戶安全性持續提升。CST 與公司內的工程和安全性團隊合作，確保合規性、增強安全性，並提供更公開透明的方式來保護我們的客戶，以及促進全球對 Microsoft 的信任。

客戶成功：客戶成功部門的安全性團隊會直接與客戶合作，分享最佳做法、學到的經驗教訓和指導方針，以加速安全性轉型和現代化。這個團隊會組合和組織從 Microsoft 之旅 (以及我們的客戶身上) 學到的最佳做法和經驗較續，將其融入參考策略、參考架構、參考計畫等之中。

網路防禦營運中心 (CDOC)：Microsoft 的網路安全性和防禦設施是一個融合中心，彙集了公司內的安全性專業人員，以保護我們的企業基礎結構及客戶有權存取的雲端基礎結構。事件回應人員與來自 Microsoft 服務、產品和裝置群組的資料科學家和資訊安全工程師合作，協助全天候保護、偵測及回應威脅。

Democracy Forward Initiative (民主進程倡議)：這個 Microsoft 團隊致力於維護、保護及推動民主化的基礎知識，方法包括促進健全的資訊生態系統、保衛開放且安全民主進程，以及宣導企業公民責任。

數位犯罪部門 (DCU)：一個由律師、調查人員、資料科學家、工程師、分析師和商務人士組成的團隊，透過技術、鑑定、民事訴訟、刑事轉介及公私合作關係，在全球打擊網路犯罪。

數位外交：一個由前外交官、政策制定者和法務專家所組成的國際團隊，致力於在不斷升級的國家級衝突下，推動和平、穩定且安全的網路環境。

數位安全性與復原能力 (DSR)：這個組織致力於讓 Microsoft 能夠建置最值得信賴的裝置和服務，同時確保我們的公司安全，以及公司和客戶的資料受到保護。

數位安全部門 (DSU)：一個由網路安全性律師和分析師組成的團隊，提供法律、地緣政治和技術專業知識，以保護 Microsoft 及其客戶。DSU 建立了對 Microsoft 企業安全性防禦措施的信任，有效對抗全世界先進的網路敵手。

數位威脅分析中心 (DTAC)：這個專家組成的團隊負責分析和通報國家級威脅，包括網路攻擊和勢力活動在內。這個團隊將資訊和網路威脅情報與地緣政治分析相互結合，為我們的客戶和 Microsoft 提供深入解析，以提出有效的應變和防護措施。

企業和安全性：這個團隊專注於為智慧雲端和智慧邊緣提供現代、安全且可管理的平台。

企業行動化：這個團隊協助提供現代工作場所和現代管理方式，以確保雲端和內部佈署的資料安全無虞。Endpoint Manager 納入了 Microsoft 和客戶用來管理和監視行動裝置、桌上型電腦、虛擬機器、嵌入式裝置及伺服器的服務和工具。

參與團隊

續

企業風險管理：一個跨營業單位運作的團隊，其任務是依照 Microsoft 資深領導層劃分風險討論的優先順序。ERM 會連接多個營運風險團隊、管理 Microsoft 的企業風險架構，以及使用 NIST 網路安全性架構促進公司的內部安全性評估。

全球網路安全性政策：一個與政府、非政府組織和產業夥伴合作的團隊，旨在推廣網路安全性公共政策，讓客戶能夠在採納 Microsoft 技術時，增強安全性和復原能力。

身分識別和網路存取 (IDNA) 安全性：一個致力於保護所有 Microsoft 客戶避免遭受未經授權的存取和詐欺的團隊。IDNA 安全性是一個跨專業領域的團隊，由工程師、商品經理、資料科學家和安全性調查人員共同組成。

M365 安全性：負責開發安全性解決方案的組織，包括適用於端點的 Microsoft Defender (MDE)、適用於身分識別的 Microsoft Defender (MDI) 等，目的在於保護企業客戶的安全。

Microsoft AI, Ethics and Effects in Engineering and Research (AETHER)：一個 Microsoft 諮詢委員會，其使命是確保以負責任的方式開發及佈署新技術。

Microsoft Bing 搜尋與發佈：一個專門提供世界級網際網路搜尋引擎的團隊，讓世界各地的使用者能夠快速找到值得信賴的搜尋結果和資訊，包括追蹤他們關心的主題和趨勢事件，同時讓使用者控制其隱私權。

Microsoft 客戶與合作夥伴解決方案：Microsoft 整合的商業上市組織，負責現場角色，例如安全性和技術銷售專家和顧問。

Microsoft Defender 專家：Microsoft 最大的全球組織，成員包括以產品為重點的安全性研究人員、應用科學家和威脅情報分析師。Defender 專家在 Microsoft 365 安全性產品和 Microsoft Defender 專家所管理的服務中提供創新偵測及回應功能。

適用於 IoT 的 Microsoft Defender：一個由網域專家研究人員所組成的團隊，專門研究 IoT/OT 惡意軟體、通訊協定和韌體的反向工程。這個團隊會尋找 IoT/OT 威脅，以揭露惡意趨勢和活動。

Microsoft Defender 威脅情報 (RiskIQ)：這個團隊透過分析 Microsoft 廣泛的外部遙測資料集合、隨著威脅形勢演進偵查以找出先前未知的威脅基礎結構，並且加入威脅行為體和活動的背景，藉此產生戰略情報。該團隊會定期發佈及時且獨特的研究，為防禦者提供關鍵的戰略情報。

Microsoft 安全性業務開發團隊：這個團隊負責領導我們 Microsoft 網路安全性成長策略、合作夥伴關係及策略性投資。

Microsoft 安全回應中心 (MSRC)：這個團隊會與安全性研究人員合作，致力於保護 Microsoft 客戶和合作夥伴生態系統。MSRC 是 Microsoft 網路防禦作業中心 (CDOC) 不可或缺的一部分，集結了安全性回應專家，共同即時保護、偵測及回應威脅。

Microsoft Security Services for Incident Response：一個由網路安全性專家組成的團隊，會在整個網路攻擊過程中，從調查到成功圍堵和復原相關活動一路為客戶提供支援。服務是透過兩個高度整合的團隊提供，一個是偵測及回應團隊 (DART)，專注於調查和復原的基礎工作，另一個是入侵復原安全性做法 (CRSP) 團隊，專注於圍堵和復原層面。

Microsoft 威脅情報中心 (MSTIC)：這個團隊專注於識別影響 Microsoft 客戶的最複雜的敵手，並追蹤和收集相關情報，包括國家級威脅、惡意軟體和網路釣魚等。

One Engineering System (1ES)：這個團隊的使命在於提供世界級的工具，幫助 Microsoft 開發人員盡情發揮工作效率且安全無虞。該團隊負責保護 Microsoft 端對端軟體供應鏈安全的核心策略。

營運威脅情報中心 (OpTIC)：這個團隊負責管理及散發網路威脅情報來支援 Microsoft 網路防禦營運中心 (CDOC) 的任務，以保護 Microsoft 和客戶。

Microsoft

釐清威脅形勢並賦予數位防禦能力。

- 深入了解 https://microsoft.com/mddr
- 深入探討：https://blogs.microsoft.com/on-the-issues/
- 保持聯繫：@msftissues and @msftsecurity