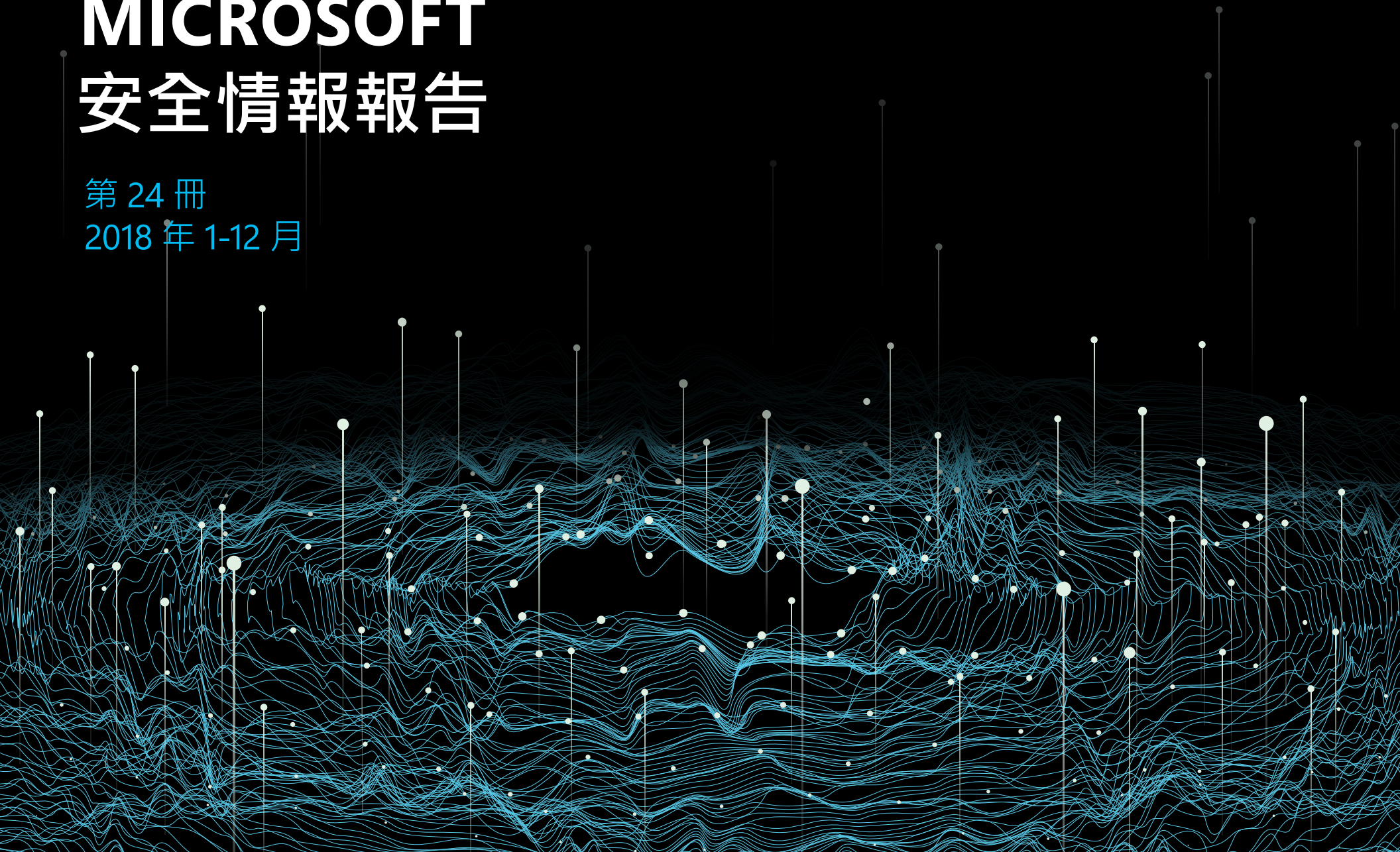
Microsoft

MICROSOFT 安全情報報告

第 24 冊
2018 年 1-12 月



目錄

作者和投稿者 3

前言 4

第一節：勒索軟體、加密貨幣挖礦和金錢. 6

勒索軟體攻擊逐漸式微 7

加密貨幣挖礦呈上升趨勢 10

瀏覽器型的加密貨幣挖礦軟體：一種新型態的威脅 11

未經請求之加密貨幣挖礦的影響 12

第二節：軟體供應鏈面臨風險 13

信任危機 16

超越軟體：透過雲端物件的供應鏈入侵 17

調查網路事件：專業服務 18

第三節：網路釣魚仍然猖獗. 19

網路釣魚在 2018 年仍然是首選攻擊媒介 20

調查網路事件：製造業 23

第四節：全球各地的惡意程式碼. 24

調查網路事件：金融服務 27

指引 28

資料來源 33

本文件僅供參考。MICROSOFT 對於本文件中的資訊，不作任何明示、默示或法定的保證。

本文件是依「現況」提供。本文件所呈現的資訊和觀點，包括 URL 及其他網際網路網站參考資料，如有變更恕不另行通知。
請自行承擔使用風險。

此處提及的實際公司和產品名稱可能是其各自擁有者的商標。

作者和投稿者

Abhishek Agrawal
Information Protection

David Fantham
Information Protection

Debraj Ghosh
Microsoft Security Marketing

Diana Kelley
Cybersecurity Solutions Group

Elia Florio
Windows Active Defense

Eric Avena
Windows Defender Research Team

Eric Douglas
Windows Defender Research Team

Francis Tan Seng
Windows Defender Research Team

Jonathan Trull
Cybersecurity Solutions Group

Joram Borenstein
Cybersecurity Solutions Group

Karthik Selvaraj
Windows Defender Research Team

Kasia Kaplinska
Microsoft Security Marketing

Kristina Laidler
Security Incident Response

Matt Duncan
Windows Active Defense Data Engineering and Analytic

Mark Simos
Cybersecurity Solutions Group

Paul Henry
Wadeware LLC

Pragya Pandey
Microsoft Security Marketing

Ram Pliskin
Azure Security

Ryan McGee
Microsoft Security Marketing

Seema Kathuria
Cybersecurity Solutions Group

Steve Wacker
Wadeware LLC

Tanmay Ganacharya
Windows Defender Research Team

Volv Grebennikov
Bing

Yaniv Zohar
Azure Security

前言

各位讀者好，歡迎閱讀第 24 期的 Microsoft 安全情報報告 (SIR)。身為從業者和安全架構師，我閱讀這樣的報告，希望更加了解資安局勢，並獲得有關如何利用知識更有效地捍衛及保護組織的實用建議。

SIR 團隊將提高網路復原力的教育精神引入到本報告中，並篩選了一年的資料，精煉出最重要的教訓。

您所閱讀的是從一年的安全性資料分析和實際經驗教訓中汲取的洞察。所分析的資料包括每天收集自 Microsoft 雲端的 6.5 兆個威脅訊號，以及我們在世界各地的數千名安全研究人員和回應人員的研究和真實經驗。2018 年，攻擊者在不斷尋求從客戶和組織竊取資料和資源的過程中，使用了各種骯髒的手段，包括新的 (虛擬貨幣挖礦) 和舊的 (網路釣魚)。類似 Ursnif 活動等混合攻擊，混合了社交和技術手段。隨著防禦方對勒索軟體 (強大且具破壞性的攻擊形式) 採取更聰明的保護措施，犯罪份子轉向了「匿蹤」但仍然有利可圖的虛擬貨幣挖礦軟體。

這種「轉向」令人挫折，好像攻擊者總是領先一步。但從不同的角度來看這個問題，有其正面意義。像您這樣的防禦者和網路安全性專業人員實施防禦技術，迫使攻擊者改變慣用的有效負載 (Payload)，使得勒索軟體不再是首選。

網路犯罪活動數量增加的另一個領域是供應鏈。其中最引人注目的是在 2018 年 3 月 6 日爆發、由一個有毒的對等應用程式引發的 Dofoil 虛擬貨幣挖礦軟體疫情。供應鏈的顧慮已超越應用程式而轉入雲端，包括惡意瀏覽器擴充功能、遭入侵的 Linux 存放庫，以及多個後門模組實例。為了因應這個威脅，各組織正在走向透明和可信的供應鏈模型。

資料很好，但有時了解發生在組織中的事件會有助益。這就是為什麼我們包含了偵測和回應團隊 (DART) 的實地經驗教訓。其中包括一家大型製造公司如何實施控制措施，阻止了困擾他們數月的多階段網路釣魚活動，以及數個金融服務組織使用先進的調查工具和端點監控，最終得以從其系統中根除威脅行為者。

最後但並非最不重要的是，網路釣魚點擊詐騙案件持續上升 – 但機器學習模型也進步了，在攻擊程式進入端點就先察覺攔截，並在點擊後防止傷害。更多好消息？越來越多的公司正在實施多因素解決方案，以防止認證竊盜網路釣魚電子郵件重演。

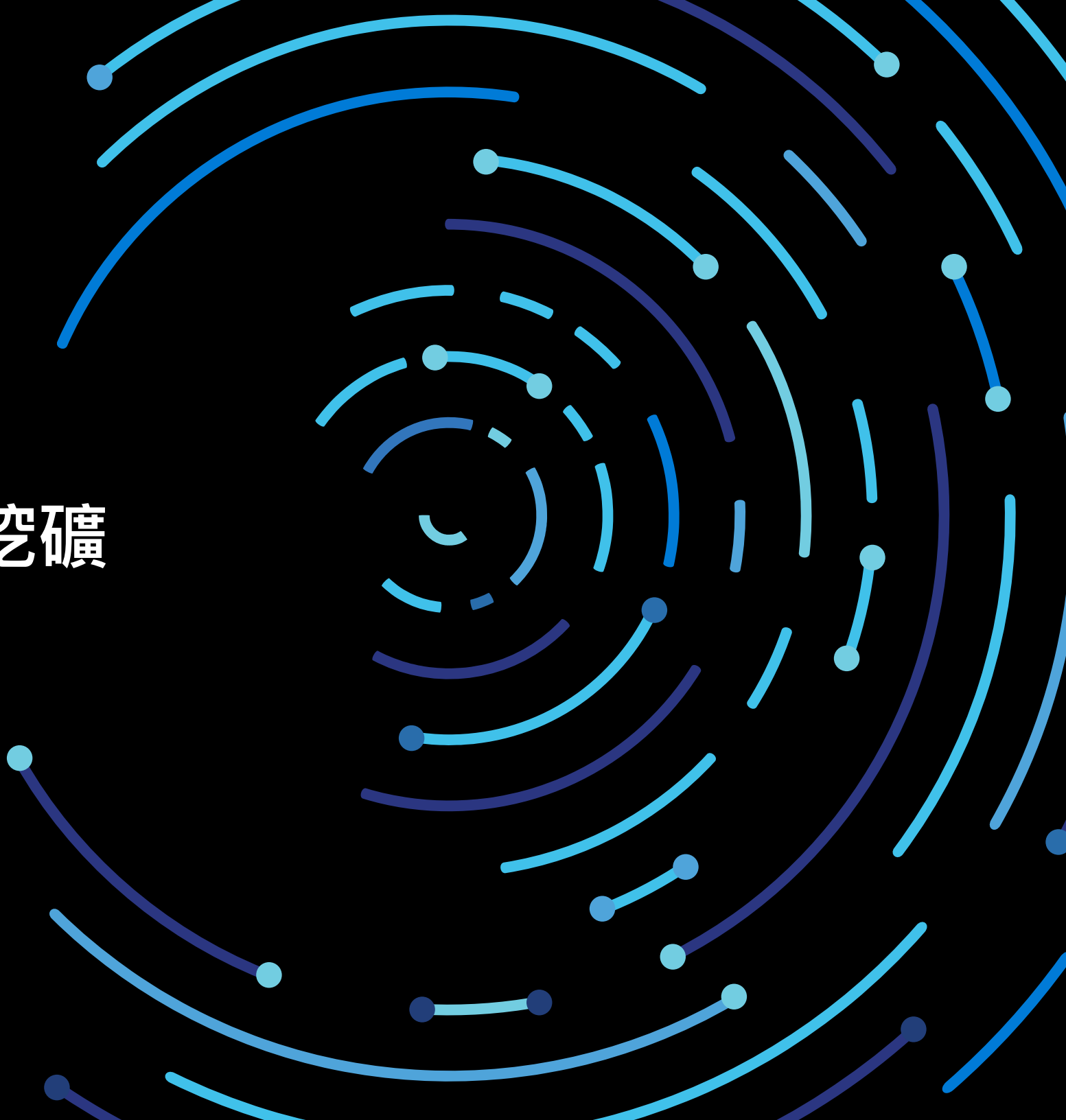
攻擊者尋找機會，所以我們對他們的技術和攻擊手法了解得越多，我們就會越有準備來建立防禦，迅速做出回應。重要的小步驟可以對組織的整體網路安全性健康狀況產生巨大的影響。這就是為什麼在本報告中，除了對不斷變化的惡意軟體和攻擊環境的深入洞察外，您還可以找到建議步驟和其他最佳做法指引。因為當我是從業者時，這正是我與壞人奮戰時所需要的。我們希望這也是您所需要的。

Diana Kelley
Microsoft 網路安全性領域首席技術官

附註：我們一直在尋求改進 SIR 的方法。如果您有任何意見，請聯繫我們，也請不吝指教。

第一節

勒索軟體、加密貨幣挖礦和金錢



2017 年的重大資安案件主要涉及勒索軟體。WannaCrypt 和 Petya 勒索軟體 (一種惡意軟體，它鎖定或加密電腦，然後要求贖金來恢復存取) 在全球爆發，引起媒體大篇幅報導，許多人推測，這個問題將會在未來加劇。相反地，勒索軟體遭遇率在 2018 年大幅下降。

勒索軟體遭遇率減少在一定程度上是由於改進的偵測和教育，使攻擊者更難以從中獲利。因此，攻擊者開始將精力從勒索軟體轉移到加密貨幣挖礦等方法上，利用受害者的運算資源為攻擊者賺取數位財。這一轉變從根本上展現了大多數以利潤為導向的網路罪犯的投機性質：他們傾向於追逐最容易獲得的金錢，當網路犯罪的經濟狀況發生變化時，他們很快跟進。

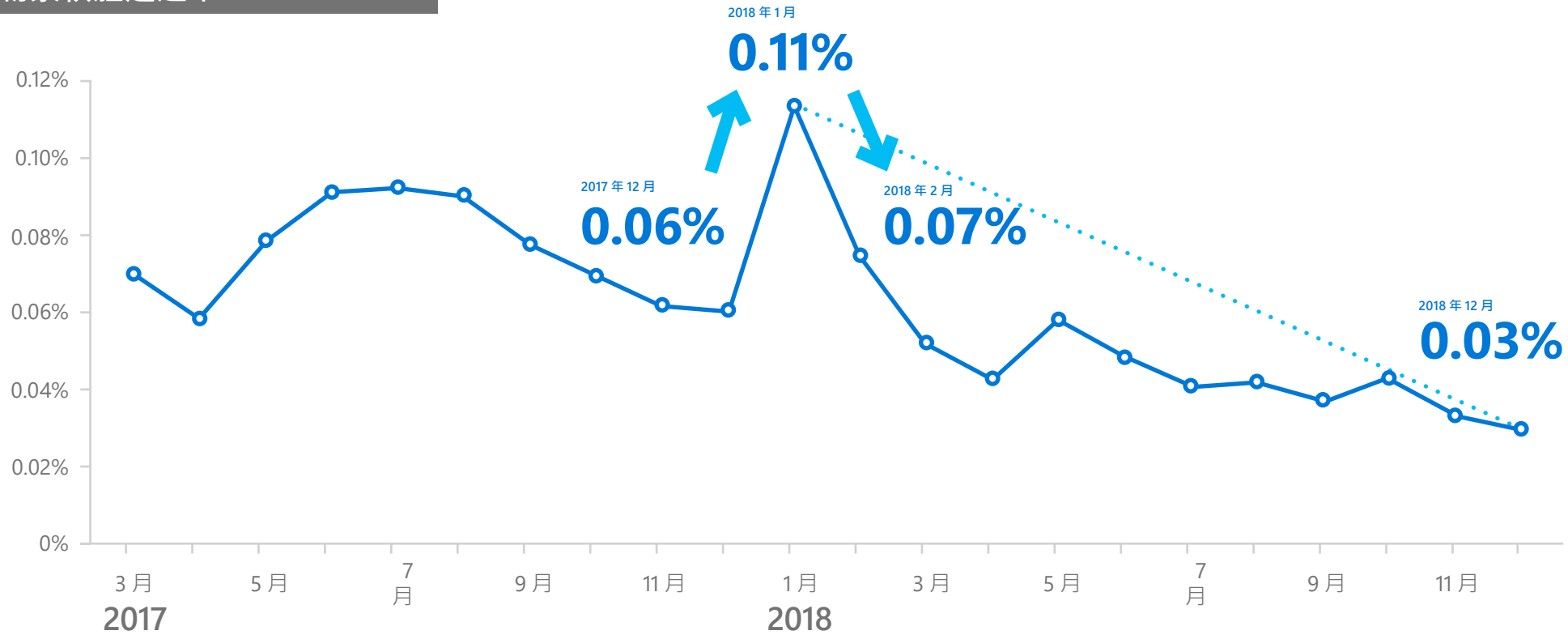
勒索軟體攻擊逐漸式微

十多年前，在地下主導早期惡意軟體的駭客和惡作劇者，被組織犯罪和其他以營利為導向的利益團體所取代。早期的惡意軟體疫情往往又快又猛，以利潤為導向的惡意軟體則更有可能悄悄地執行，避免引起注意，以便盡可能長時間繼續執行其功能：傳送垃圾郵件、竊取敏感資訊、進行阻斷服務攻擊和其他惡意活動。

勒索軟體逆勢而行。勒索軟體沒有試圖不被發現，而是公開拒絕受害者存取電腦和重要檔案，直到受害者支付贖金 (甚至在支付贖金之後，攻擊者並未釋放對電腦的控制)。

隨著勒索軟體在 2017 年達到頂峰，這種公開攻擊的風格似乎代表了攻擊者技術的一個新階段。但最近資料顯示，勒索軟體可能正在式微，攻擊者逐漸回到他們過去使用的匿蹤行動模式，試圖躲在雷達掃描不到的死角，以便更有效地進行加密貨幣挖礦這類的攻擊。雖然勒索軟體遭遇率有所下降，但這不一定意味著攻擊的嚴重程度有所銳減。

勒索軟體遭遇率



2017 年 3 月至 2018 年 12 月期間，勒索軟體遭遇率下降了約 60%，在此期間只有間歇性增加。

圖 1.

2017 年 3 月至 2018 年 12 月的勒索軟體遭遇

這種整體下降的原因可能有很多，不過 Microsoft 安全研究人員推測，主要因素是使用者和組織都越來越了解勒索軟體威脅，並更有智慧地處理這些威脅，包括更謹慎行事，備份重要檔案，以備在檔案遭到勒索軟體加密時可予以恢復。另外，如前所述，網路罪犯是投機份子。

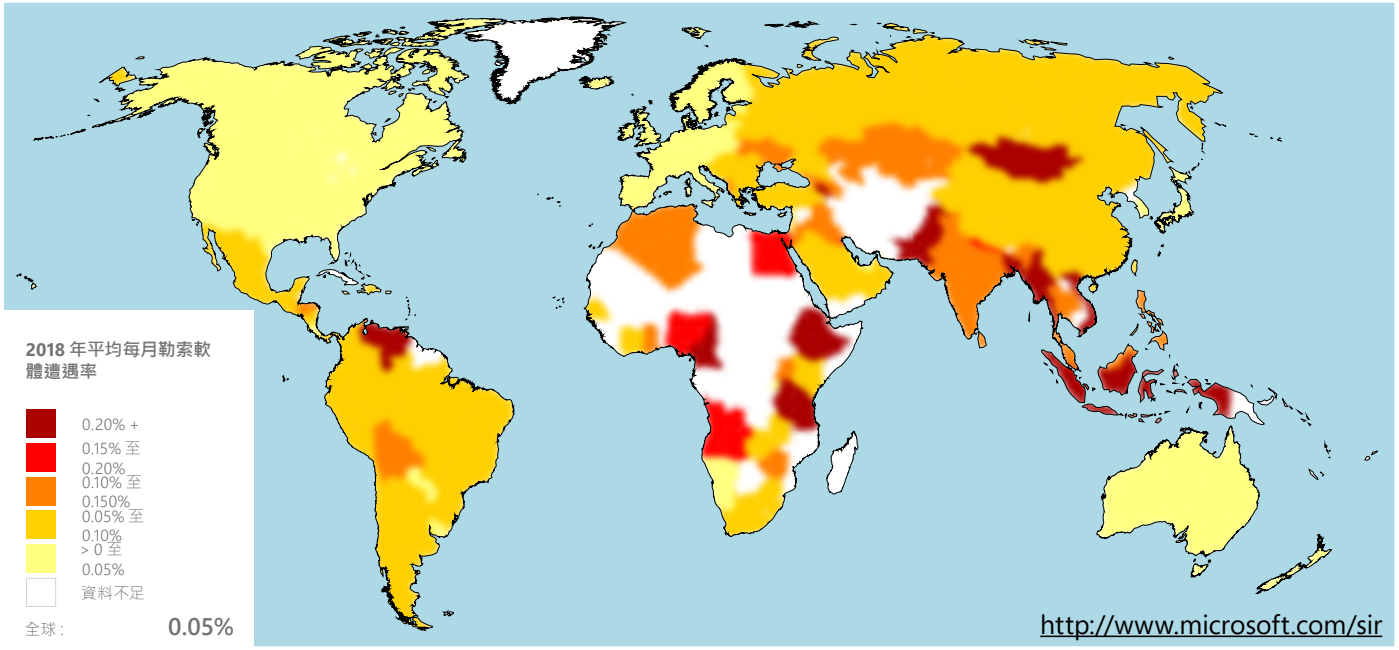
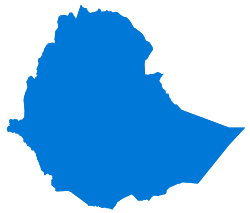


圖 2.

2018 年依國家/地區列出的全球平均每月勒索軟體遭遇率

受勒索軟體影響最嚴重的國家/地區：衣索比亞



平均每月遭遇率：

0.77%

2018 年平均每月勒索軟體遭遇率最高的五個地點是衣索比亞 (平均每月勒索軟體遭遇率 0.77%)、蒙古 (0.46)、喀麥隆 (0.41)、緬甸 (0.33) 和委內瑞拉 (0.31)，在此期間每個地點的平均每月勒索軟體遭遇率為 0.31% 或更高。[1] 幾年前，勒索軟體遭遇往往聚集發生在歐洲和北美的富裕國家/地區，但隨著攻擊者已經開始不再使用勒索軟體，遭遇模式已經變得與惡意軟體的整體模式更加相似。

2018 年勒索軟體遭遇率最低的地點是愛爾蘭 (0.01)、日本 (0.01)、美國 (0.02)、英國 (0.02) 和瑞典 (0.02%)，在同一時期每個國家/地區的平均每月勒索軟體遭遇率為 0.02% 或更低。遭遇率較低的地區往往擁有成熟的網路安全性基礎設施，以及用於保護關鍵基礎設施和向民眾宣導基本安全性的完善方案。

註腳

[1] 遭遇率是執行 Microsoft 即時安全性產品並報告惡意軟體遭遇的電腦百分比。遭遇威脅並不表示電腦已被感染。唯有使用者選擇提供資料給 Microsoft 的電腦，才會在計算遭遇率時考慮進去。

加密貨幣挖礦呈上升趨勢

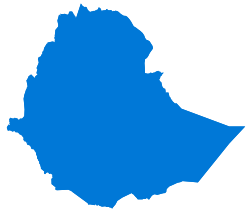
加密貨幣是一種虛擬貨幣，可以用來在網路和實體世界中匿名買賣商品和服務。存在許多不同類型的加密貨幣，藉由區塊鏈技術，每筆交易都記錄在由全世界數千台或數百萬台電腦維護的分散式帳本中。新虛擬貨幣是由執行複雜計算，並同時驗證區塊鏈交易的電腦所創造或「開採」。

開採虛擬貨幣相當有利可圖—在 2018 年，一枚比特幣 (最古老且最流行的加密貨幣) 價值數千美元，但執行必要的計算非常耗資源，並隨著每一枚新虛擬貨幣被開採，進一步加劇。對於比特幣等流行貨幣來說，如果無法獲得龐大計算資源 (大多數個人和小團體無法獲得的)，開採虛擬貨幣就幾乎無利可圖。基於這個原因，尋求非法獲利的攻擊者逐漸轉向惡意軟體，藉以使用受害者的電腦，幫助開採加密貨幣。透過這種方法，他們可以利用幾十萬台電腦的處理能力 (而不只是一兩台電腦)。即使發現了輕微感染，加密貨幣的匿名性質也使追蹤工作更為複雜。

2018 年，全球平均每月加密貨幣挖礦遭遇率為 0.12%，相較於勒索軟體的 0.05% 低遭遇率。許多因素導致挖礦做為惡意軟體的有效負載越來越受歡迎。與勒索軟體不同，加密貨幣挖礦不需要使用者輸入：它會在使用者正在執行其他工作或離開電腦時，同時在背景運作，而且除非電腦效能顯著降低，否則可能完全不會被注意到。因此使用者不太可能採取任何動作來消除威脅，也因此可能繼續長時間挖礦，讓攻擊者得利。

可用於秘密開採許多加密貨幣的「現成」產品，是這個趨勢的另一個驅動因素。進入的門檻低，因為虛擬貨幣挖礦軟體的廣泛可用性，網路罪犯將其重新包裝為惡意軟體，以傳遞到毫無戒心的使用者的電腦。然後，使用攻擊者用來傳遞其他威脅的許多相同技術，如社交工程、惡意探索和路過式下載，將武器化的挖礦軟體散發給受害者。挖礦軟體安裝後，將在受害者的電腦上於背景中執行 (執行區塊鏈計算)，讓攻擊者得利。

受加密貨幣挖礦影響最嚴重的國家/地區的平均每月遭遇率



衣索比亞：5.58%

坦尚尼亞：1.83%

巴基斯坦：1.47%

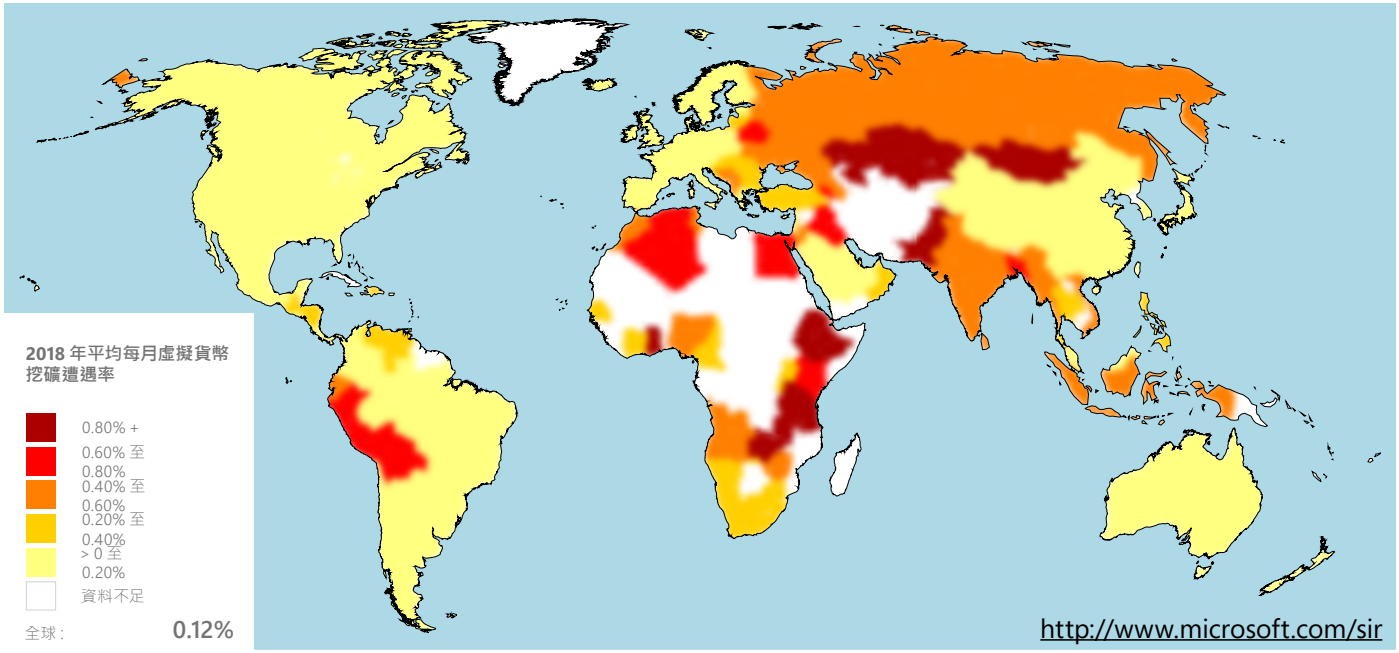


圖 3.

2018 年依國家/地區列出的全球平均每月虛擬貨幣挖礦軟體遭遇率

受加密貨幣挖礦影響最小的國家/地區的平均每月遭遇率

愛爾蘭：0.02%

日本：0.02%

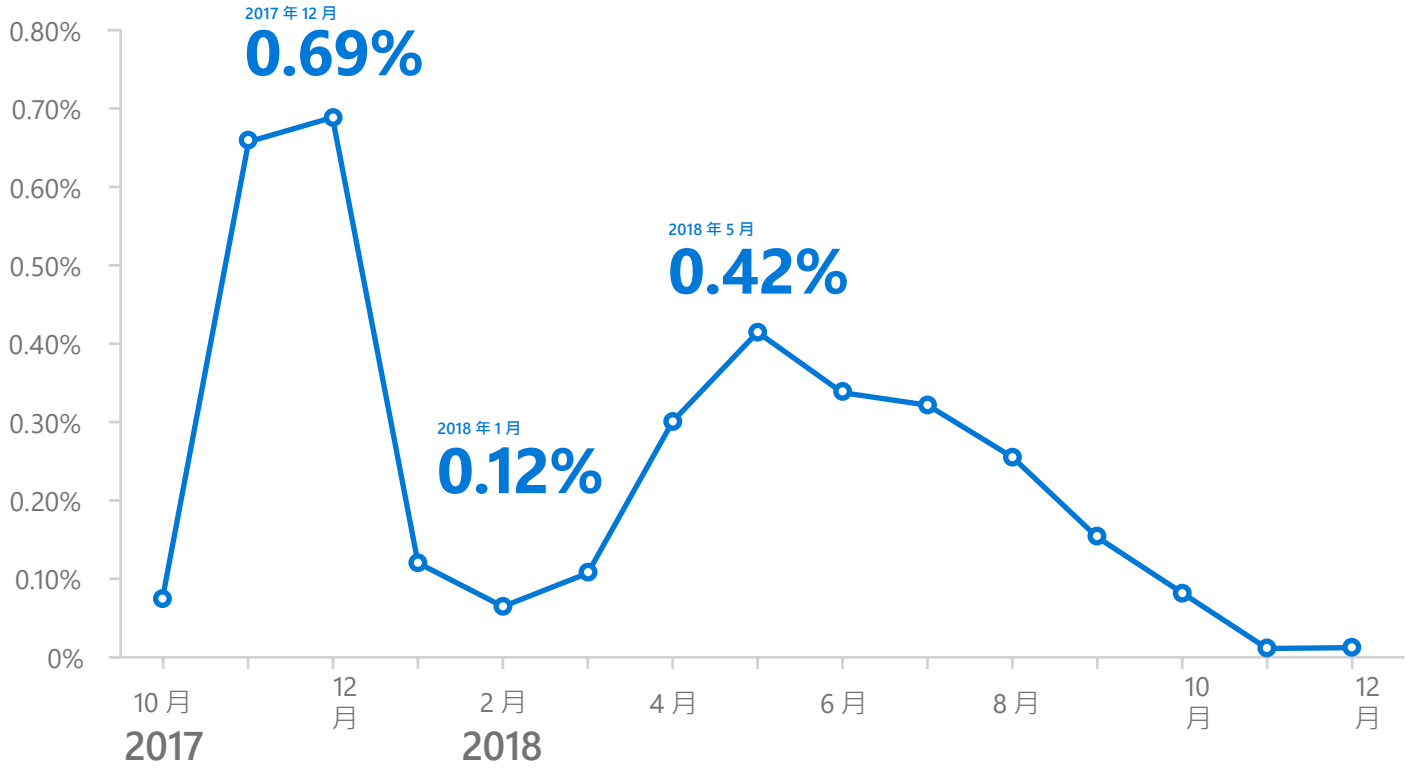
美國：0.02%

2018 年加密貨幣挖礦遭遇率最高的五個地點是衣索比亞 (5.58)、坦尚尼亞 (1.83)、巴基斯坦 (1.47)、哈薩克 (1.24) 和尚比亞 (1.13)，在此期間每個地點的平均每月虛擬貨幣挖礦遭遇率約為 1.13% 或更高。2018 年虛擬貨幣挖礦遭遇率最低的地點是愛爾蘭、日本、美國和中國，在此期間每個國家/地區的平均每月虛擬貨幣挖礦遭遇率都在 0.02% 左右。

瀏覽器型的加密貨幣挖礦軟體：一種新型態的威脅

本節中提供的統計資訊涉及惡意加密貨幣挖礦軟體，這些挖礦軟體旨在做為惡意軟體安裝在受害者的電腦上。但一些最重大的加密貨幣挖礦威脅完全基於網頁瀏覽器，根本不需要安裝。一些服務為瀏覽器型的加密貨幣挖礦做廣告，讓網站擁有者在不依賴廣告的情況下，將網站流量變現。網站擁有者據稱在頁面中加入 JavaScript 程式碼，以供使用者存取網站時在背景中開採加密貨幣，其收益則由網站擁有者和服務分配。遺憾的是，攻擊者在沒有獲得使用者同意的情況下，迅速利用這些服

Brocoiner 遭遇率



務開採加密貨幣，通常是透過入侵合法網站及惡意地將挖礦程式碼插入其原始程式碼。這些瀏覽器型的挖礦軟體根本不需要入侵使用者的電腦，就能使用支援 JavaScript 的網頁瀏覽器在任何平台上執行。如同加密貨幣挖礦特洛伊木馬程式，瀏覽器型的挖礦軟體在使用者瀏覽受影響的網頁時，會顯著降低電腦效能並浪費電力。

圖 4.

最猖獗的瀏覽器型的加密貨幣挖礦軟體 Brocoiner 遭遇率

未經請求之加密貨幣挖礦的影響

惡意加密貨幣挖礦的受害者面臨的最明顯威脅是運算資源的消耗，這可能會浪費電力，並顯著降低電腦效能。使用者和組織還面臨虛擬貨幣挖礦帶來的其他風險，包括：

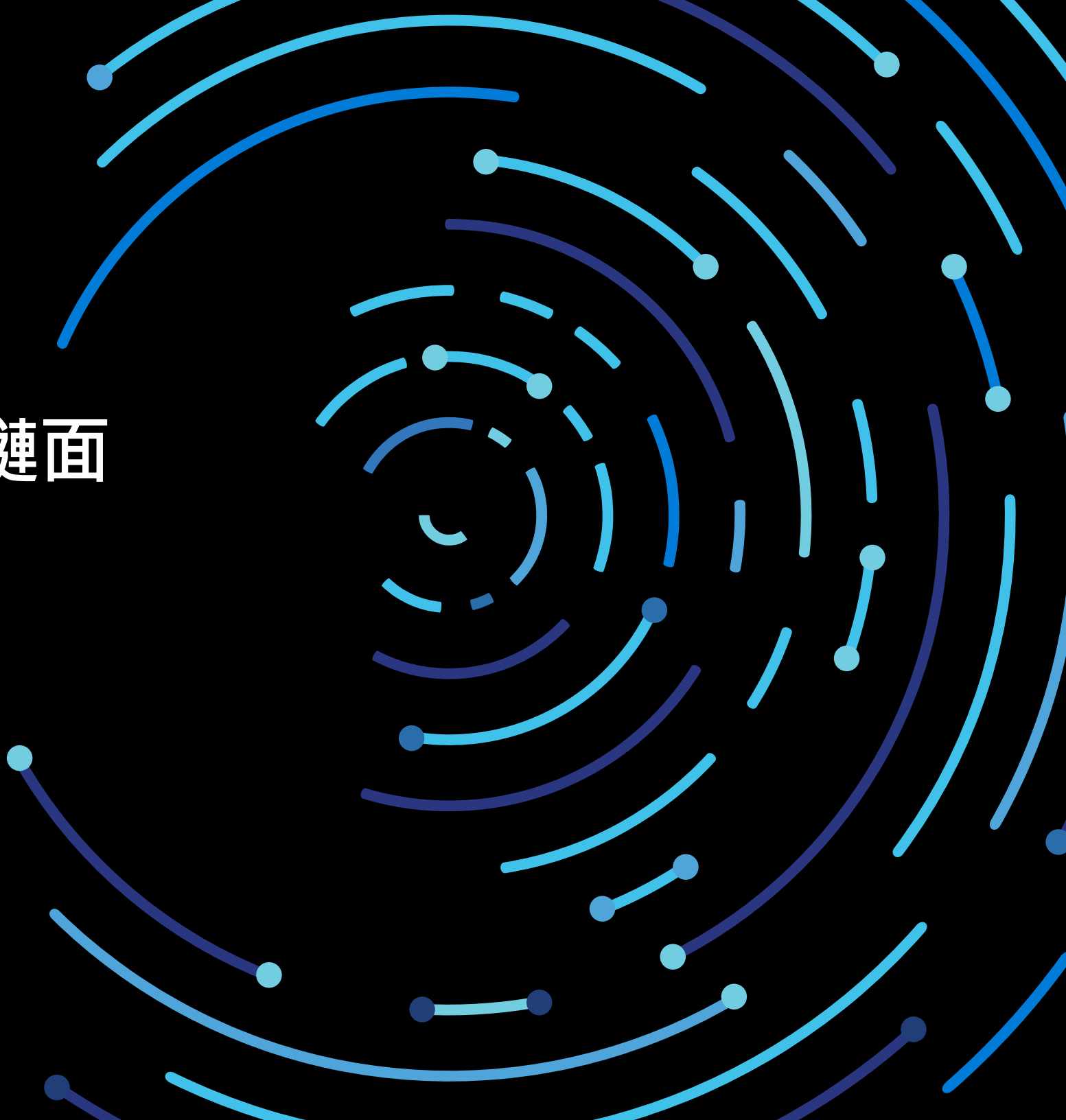
獲得立足點，在未來造成更大的傷害。
如同其他型態的惡意軟體，加密貨幣挖礦可以成為攻擊者的進入點。當電腦在背景中開採加密貨幣時，網路罪犯可以了解環境，並可能發現安全漏洞，以便利用為其他目的。

網際網路連線的裝置可能遭入侵，並變成加密貨幣挖礦的機器人。
許多此類裝置缺乏內建的安全性，如惡意軟體威脅偵測，可能因此成為攻擊者的理想目標。

傷害機器。
加密貨幣挖礦軟體連續執行數月或更長時間可能會影響效能，而過度功耗和 CPU 利用率所產生的熱量可能會損害電腦。

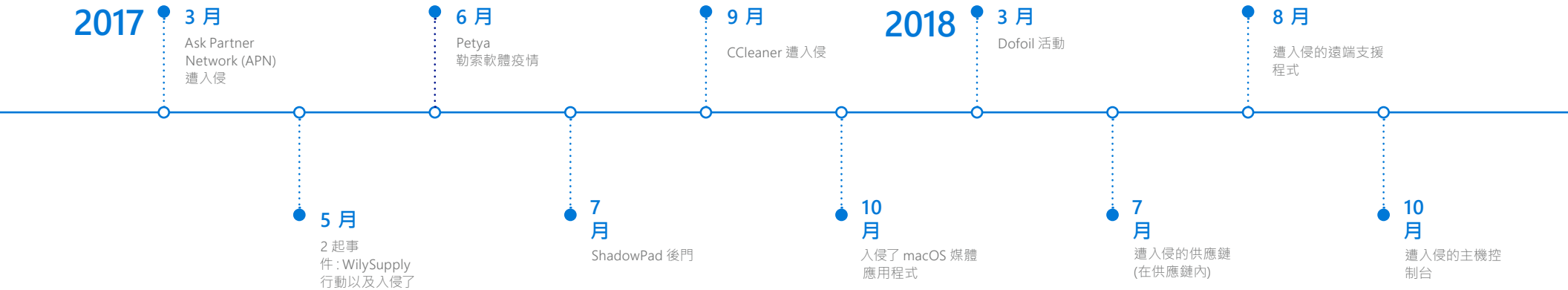
第二節

軟體供應鏈面臨風險



多年來，Microsoft 一直在追蹤那些將供應鏈入侵做為攻擊進入點的威脅行為者。在供應鏈攻擊中，攻擊者集中入侵合法軟體發行者的開發或更新程序。

如果得逞，攻擊者會將遭入侵的元件合併到合法的應用程式或更新套件中，然後將其散發給軟體的使用者。然後，惡意程式碼就會透過與軟體相同的信任度和權限來執行。過去幾年軟體供應鏈攻擊次數的增加，已成為許多網路安全性對話的重要話題，也是許多 IT 部門關注的主要問題。



2017 年主要軟體供應鏈攻擊

▲ **圖 5.**

2017 年和 2018 年軟體供應鏈攻擊

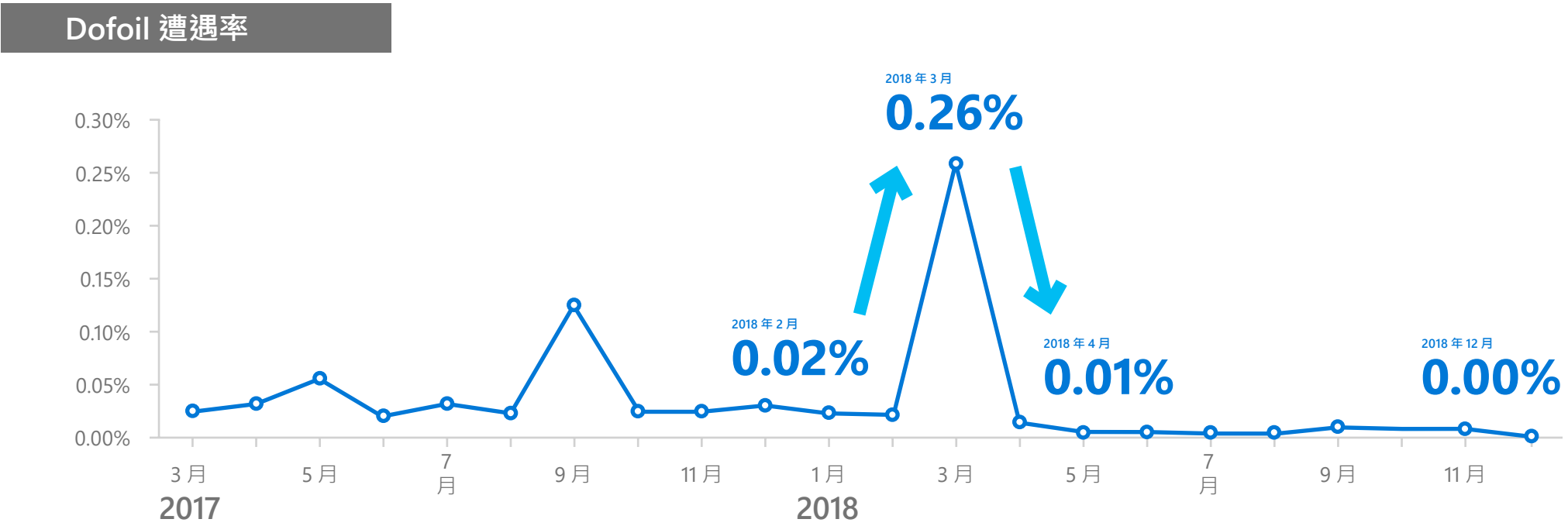
2017 年，一些供應鏈攻擊事件引發媒體大篇幅報導，其中最引人注目的是 6 月 Petya 勒索軟體疫情，該事件可追溯到烏克蘭一款熱門稅務會計應用程式更新程序遭入侵，所造成的初步感染。5 月，WilySupply 行動使文字編輯器的軟體更新程式遭入侵，在金融和 IT 領域的目標組織上安裝後門。7 月，一個名為 ShadowPad 的後門隱藏在伺服器管理軟體套件中，並允許攻擊者安裝額外的惡意軟體有效負載，以進行資料竊取和其他惡意活動。在 9 月，流行的免費軟體工具 CCleaner 的基礎設施遭入侵，一個後門版本傳遞到其使用者群。

2018 年的軟體供應鏈攻擊 – 根源和衝擊

2018 年第一件重大的軟體供應鏈攻擊事件發生在 3 月 6 日，Windows Defender ATP 在這次攻擊當中封鎖了傳遞 Dofoil 特洛伊木馬程式 (又稱 Smoke Loader) 的龐大活動。此一大規模的惡意軟體活動可追溯到有毒的對等應用程式。應用程式的更新套件遭到已下載入侵碼的惡意程式所取代，該程式隨後安裝了 Dofoil 惡意軟體。複雜的特洛伊木馬程式附帶虛擬貨幣挖礦負載，並呈現先進的跨程序注入技術、持久性機制和規避方法。

圖 6.

2018 年 Dofoil (Smoke Loader) 遭遇趨勢在 3 月顯示遭封鎖的事件高峰



在該活動的前 12 個小時，Windows Defender 防毒軟體在全球封鎖了 400,000 多次感染嘗試。俄羅斯佔全球遭遇的 73%，土耳其和烏克蘭分別佔 18% 和 4%。

2018 年，又偵測到利用遭入侵軟體供應鏈做為交付機制的數起攻擊，包括下表所述的攻擊：

期間	攻擊	描述	受影響的軟體
2018 年 3 月	Dofoil 虛擬貨幣挖礦活動 (由 Microsoft 報告)。	攻擊者毒化了一個對等應用程式的更新過程以安裝 Dofoil，進而安裝虛擬貨幣挖礦惡意軟體。	對等應用程式。
2018 年 7 月	供應鏈中遭入侵的供應鏈 (由 Microsoft 報告)。	攻擊者入侵 PDF 編輯器應用程式廠商與其中一個軟體廠商合作夥伴之間的共用基礎結構。	PDF 編輯器應用程式和第三方合作夥伴廠商。
2018 年 8 月	遭入侵的遠端支援程式 (Operation Red Signature，由 Trend Micro 和 IssueMakersLab 報告)。	遠端支援解決方案提供者的更新伺服器遭入侵，傳遞一個稱為 9002 RAT 的遠端存取工具。	遠端支援程式。
2018 年 10 月	遭入侵的主機控制台解決方案 (由 ESET 報告)。	主機控制台解決方案的安裝指令碼遭竄改，以竊取認證。	主機控制台解決方案。

圖 7.

2018 年的其他軟體供應鏈攻擊

信任危機

供應鏈攻擊極為險惡，因為它們利用了使用者和 IT 部門對所使用軟體的信任。遭入侵的軟體通常由廠商簽署認證，可能沒有問題跡象，這使得偵測感染的難度大大增加。這類攻擊可能會破壞供應鏈與其客戶之間的關係，無論後者是企業使用者還是家庭使用者。透過毒化軟體和破壞交付或更新基礎設施，供應鏈攻擊可能會影響組織所提供之商品和服務的完整性和安全性。

供應鏈攻擊影響到不同產業和地理位置的各種軟體和目標組織。供應鏈攻擊的威脅是整個產業範圍的問題，需要多個利害關係人關注，包括編寫程式碼的軟體開發人員和廠商、管理軟體安裝的系統管理員，以及發現這些攻擊並建立解決方案，以保護人員和軟體的資安社群。

超越軟體：透過雲端物件的供應鏈入侵

供應鏈攻擊破壞信任的能力，在雲端中被擴大，變得更為複雜。2018 年發生的幾起雲端物件、服務和基礎架構遭入侵事件突顯了這個複雜性：

- 中毒的 Chrome 擴充功能安裝點擊欺詐惡意軟體 (由 ICEBRG 報告)
- 各種遭入侵的 Linux 存放庫 (在一些線上論壇中報告)
- 惡意 WordPress 外掛程式用於各種惡意活動，包括允許攻擊者在 WordPress 網站上發佈內容 (由 Wordfence 報告)
- 惡意 Docker 映像，其中包含下載加密貨幣挖礦惡意軟體並上傳到 Docker Hub 帳戶的指令碼 (由 Fortinet 和 Kromtech 報告)
- Python 官方存放庫中的域名搶註 (Typo Squatting) 惡意套件，其中的惡意指令碼會下載惡意軟體，用以劫持剪貼簿中之虛擬貨幣挖礦位址 (在 Medium 上報告)
- StatCounter 中遭入侵的指令碼允許攻擊者在使用 StatCounter 的網站中注入惡意指令碼 (由 ESET 報告)
- 多起後門 npm 模組事件 (npm 部落格、Medium)，如果被利用，可能會導致攻擊者能夠將任意程式碼輸入到執行中伺服器並執行惡意程式碼等情況。

這些事件顯現供應鏈入侵如何大幅擴大攻擊面。雲端物件如果不安全，可能會成為意外的進入媒介。例如，Docker Hub 事件涉及一個惡意帳戶上傳 Docker 映像，其中包含隱藏的虛擬貨幣挖礦後門。Docker 映像裝載於 Docker Hub 近一年，由毫無戒心的管理員和使用者下載數百萬次並使用。

供應鏈風險擴展到雲端中的程式碼、開放原始碼、Web 程式庫、容器，以及雲端中的其他物件。這些風險，再加上已曝光軟體和硬體供應鏈入侵事件之間的高度差異，使供應鏈攻擊成為一個廣泛的威脅類別。儘管對於這些攻擊類型的整個光譜沒有一個合適的解決方案，但是組織需要為遭入侵硬體和軟體供應商、廠商和收購目標、開放原始碼軟體供應商，以及雲端服務和基礎設施供應商建立供應鏈攻擊的預防性保護和外洩後偵測機制。

透過 DART 調查網路事件

Microsoft 偵測和回應團隊 (DART) 是一個由網路安全性專家和事件回應人員組成的全球團隊，可幫助組織偵測、調查和回應網路安全性事件。本節重點介紹 DART 在過去一年處理的一些客戶案例；說明常見的攻擊者趨勢以及 Microsoft 和客戶是如何阻止它們。

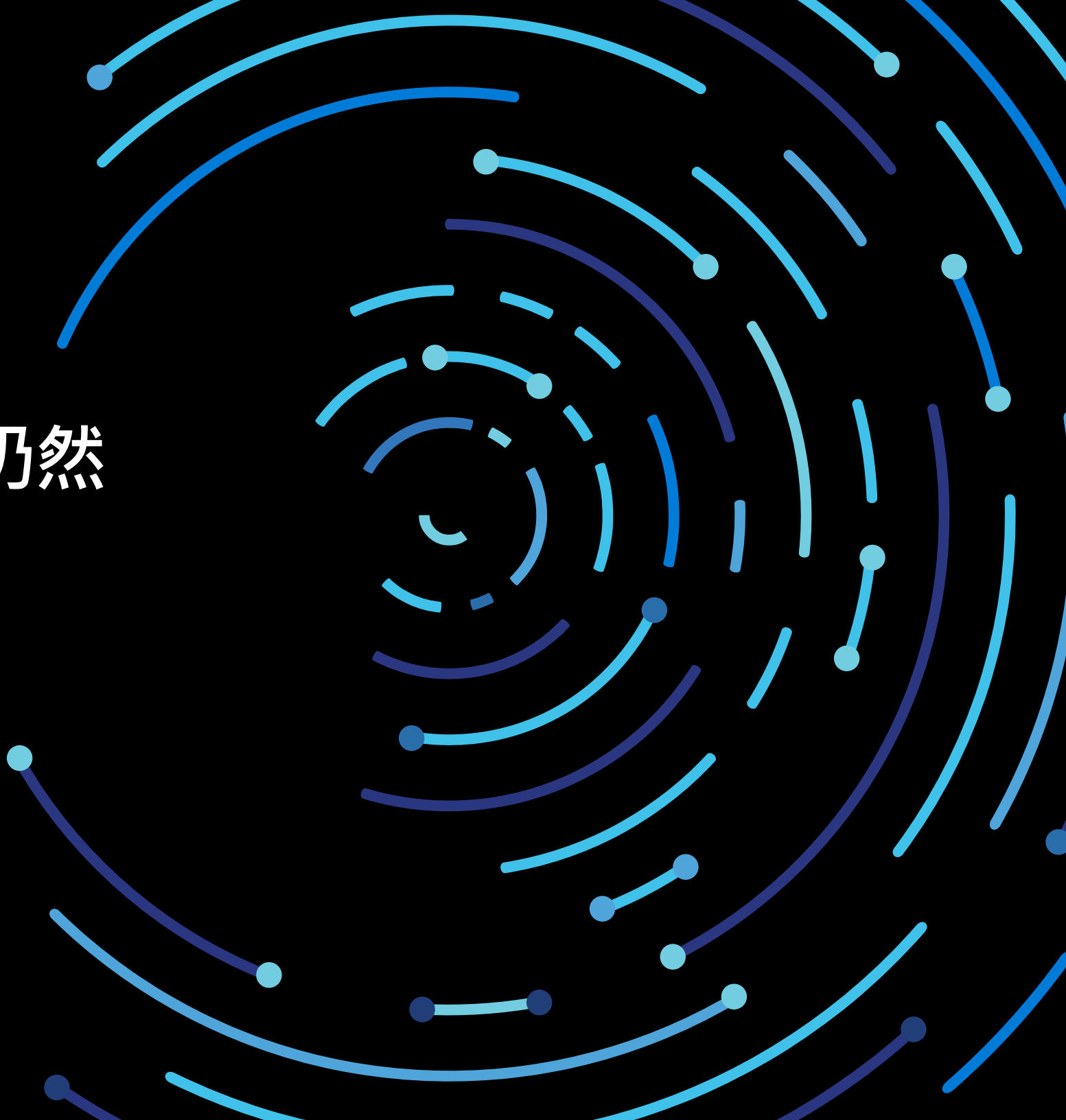
專業服務組織經歷了洩露資料的國家級攻擊

一個專業服務組織受到了一個有國家級贊助的複雜進階持續威脅 (APT) 的影響，該威脅獲得了該組織的特殊權限認證。攻擊者透過密碼噴濺攻擊，使用少量弱式密碼或廣泛使用的密碼 (如「p@ssword」或「123456」) 來鎖定大量使用者帳戶並獲取 Office 365 管理認證，獲得了對網路的存取 (密碼噴濺攻擊用來避免每個帳戶登入嘗試次數限制的偵測)。在滲透網路後，APT 對員工信箱精心策劃並執行自動洩露資料。儘管內部多次試圖驅逐，但對手仍在網路中停留了 200 多天。做為攻擊的一部分，對手利用了組織的供應鏈軟體和自動洩露資料。

由於推測客戶資料洩露，該組織聘請 DART 小組進行調查，協拽防止進一步的損害。DART 確定了目標 Office 365 信箱搜尋、遭入侵的帳戶，以及攻擊者的命令和控制通道。這次事件給客戶帶來的主要教訓是部署控制，以保護雲端服務不受身分識別的威脅和攻擊者的攻擊。該組織採用了多重要素驗證 (MFA)、某些雲端應用程式的條件式存取原則，以及 Office 365 記錄。為了進一步保護自己在未來免受類似的威脅，該組織還可能採用端點威脅偵測和回應 (EDR) 解決方案，來偵測可能試圖利用其網路的攻擊者。此外，我們還建議該組織任命一個雲端治理機構或全球身分識別團隊，負責管理和實施適當的使用者驗證原則，以便該組織對其安全狀態進行監督，並更有效地降低風險。

第三節

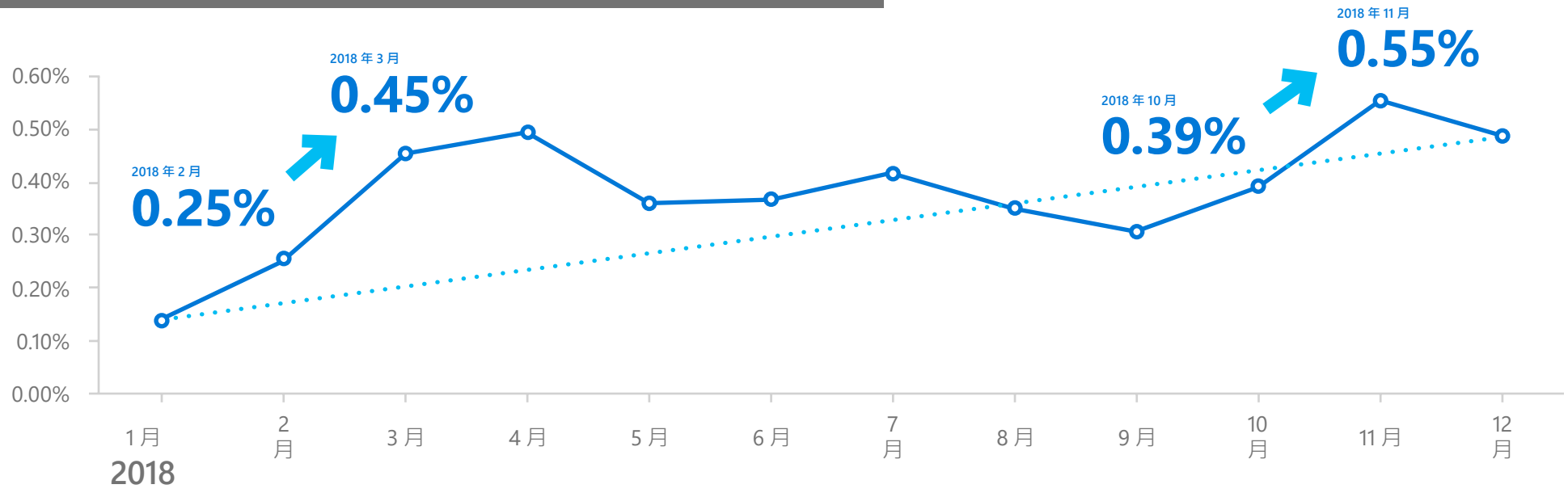
網路釣魚仍然猖獗



2018 年，Microsoft 威脅分析師看到證據，指出攻擊者繼續將網路釣魚做為首選攻擊方法。網路釣魚在可預見的未來仍然是個問題，因為在面對網路罪犯的持續攻擊，使受害者陷入誘餌圈套時，涉及人性決策和判斷。

網路釣魚率仍在上升

網路釣魚電子郵件在傳入電子郵件總數中所佔百分比



▲ **圖 8.**

2018 年網路釣魚電子郵件

網路釣魚在 2018 年仍然是首選攻擊媒介

Microsoft 每月在 Office 365 中分析和掃描超過 4,700 億封電子郵件，以偵測網路釣魚和惡意軟體，從而使分析師對攻擊者趨勢和技術有相當深入的了解。2018 年 1 月至 12 月，做為網路釣魚郵件的傳入電子郵件所佔比例增加了 250%。網路釣魚仍然是用於向使用者傳遞惡意零日有效負載的最大攻擊媒介之一。Microsoft 透過額外的反網路釣魚保護、偵測、調查和回應功能，繼續強化抵禦能力，協助保護使用者的安全。

網路釣魚攻擊方法的演變

隨著保護人們不受網路釣魚攻擊的工具和技術變得更加複雜，攻擊者被迫自我適應。網路釣魚攻擊已逐漸轉變為多型態，這意味著攻擊者不使用單個 URL、網域或 IP 位址傳送郵件，而是使用具有多個攻擊點的各種基礎結構。攻擊本身的性質也發生了變化，有各種現代網路釣魚活動，從幾分鐘的短跨距攻擊到更長時間的大量攻擊。另一些是序列變種攻擊，其中攻擊者連續幾天傳送少量郵件。

此外，Microsoft 還觀察到攻擊者使用託管基礎結構和其他公有雲基礎結構的趨勢，透過隱藏在合法網站和資產之間，更難以被發現。例如，攻擊者逐漸使用流行的文件共用和協作網站和服務，來散發惡意有效負載和用於竊取使用者認證的假登入表單。在組織內外使用遭入侵的帳戶，進一步散發惡意電子郵件的情況也有所增加。

網路釣魚活動從針對性到廣泛不等

如同一般的惡意軟體散發，網路釣魚活動從針對性的攻擊到廣泛的通用攻擊不等。儘管高度複雜的攻擊在每個被釣帳戶產生更大的金錢收益，更一般的攻擊則在每個遭入侵的帳戶產生較少收益，但鎖定更廣泛的使用者群組。

一個複雜、針對性的活動範例是 Ursnif，在其中攻擊者將文件檔案名稱本地化為熟悉組織或目標產業的專有名稱。這類攻擊與廣泛的活動有很大不同，看起來更合法、更值得信賴。

2018 年的一些廣泛活動涉及商業電子郵件入侵 (BEC)、在目標組織內冒充知名品牌、網域或使用者以及複雜的欺騙活動。網域模擬是一種常見的攻擊策略，用於引誘組織相信電子郵件是可信的，而應該開啟。

網路釣魚誘餌以多種形式出現

Microsoft 研究人員發現，有許多不同類型的網路釣魚誘餌或有效負載在活動中使用，其中包括：

- **網域詐騙** (電子郵件網域與原始網域名稱完全相符)
- **網域模擬** (電子郵件網域與原始網域名稱類似)[2]
- **使用者模擬** (電子郵件看似來自您信任的人)
- **簡訊誘餌** (簡訊看似來自銀行、政府機構或其他公司等合法來源，以賦予其宣稱的合法性，通常要求受害者提供敏感的資訊，例如使用者名稱、密碼或敏感財務資料)
- **認證網路釣魚連結** (電子郵件包含的頁面連結類似於合法網站的登入頁面，讓使用者輸入其登入認證)
- **網路釣魚附件** (電子郵件包含送件者誘使受害者開啟的惡意檔案附件)
- **指向假雲端儲存位置的連結** (電子郵件看似來自合法來源，並誘使使用者授予權限和/或輸入個人資訊，如認證，以換取存取假的雲端儲存位置)

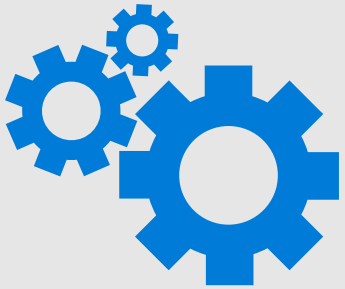
攻擊者可能使用這麼多種誘餌，增加了組織必須面對的網路釣魚威脅的複雜性。

註腳

[2] 在特殊情況下，網域模擬可能類似於網域詐騙(與原始網域名稱完全相符)，亦即網域出現在電子郵件顯示名稱中。

透過 DART 調查網路事件

大型製造組織受到針對性網路釣魚事件的攻擊

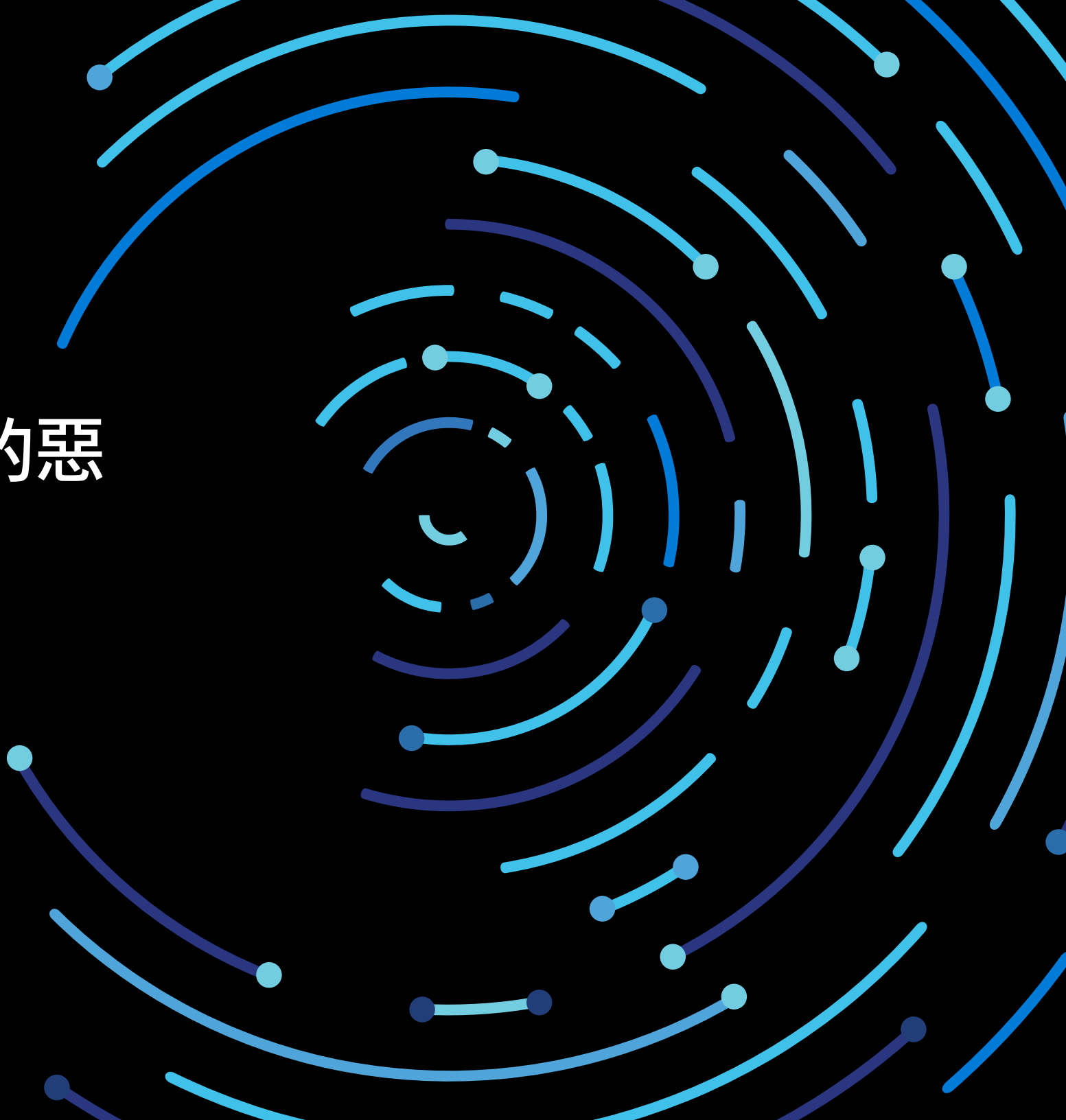


一個製造組織在幾個月的時間內經歷了一場多階段的網路釣魚活動。這種方法並不罕見。在第一階段，攻擊者執行偵察，在第二階段鎖定高價值資產。此活動的第一階段利用了一個眾所周知的網路釣魚詐騙，亦即在傳送給組織內一個小型目標群組的電子郵件中內嵌了網頁連結。電子郵件宣稱，目標有一個重要的電子文件等待審查，收件人要做的就是用他們的網域認證進行驗證才能存取。這個假的登陸頁面設定為供目標審查所謂的「重要文件」，實際上收集認證，並允許攻擊者從世界任何地方存取 Office 365 帳戶。網路釣魚活動的第二階段旨在向目標製造組織內的高價值資產傳送類似的網路釣魚電子郵件，希望能夠存取更有價值的資料。Microsoft 在網路釣魚活動的第二階段與此客戶進行合作。從這一事件中，客戶的主要教訓是：網路釣魚仍然是最有效的攻擊方法之一，使用者仍然是最薄弱的環節。訓練使用者對網路釣魚詐騙要有警覺、有工具來識別攻擊者和行動，以及定期修補系統都很重要；如果不解決其中一個問題，組織還是一樣脆弱。

在這種情況下，客戶最重要的關切是立即需要阻止對遭入侵帳戶的存取。DART 與 Azure 身分識別和 Office 365 團隊合作，設計了一個計劃，透過使用新部署的 Microsoft Azure Log Analytics 解決方案，從網路中消滅攻擊者，並監視到命令和控制通道的任何流量。團隊能夠在短短 3 個小時內協助解決這個情況。攻擊者的存取遭封鎖，而且組織可以將注意力轉向損壞評估和復原。DART 使用 Azure Log Analytics 工具來尋找攻擊者行為，這有助於發現組織面臨的許多設定挑戰。例如，DART 發現了關鍵伺服器上的修補漏洞、發現網路上的電腦與網際網路上已知的壞主機進行通訊，也發現了幾部沒有惡意程式碼防護的重要伺服器。

第四節

全球各地的惡意程式碼



惡意軟體以可用性受損、資料遺失、智慧財產竊盜、金錢損失、精神痛苦等形式給組織和個人帶來風險，甚至可能危及人命。Microsoft 使用廣泛的工具和技術來識別、阻止和消除惡意軟體感染，無論這些感染在何處發現。

2017 年，惡意軟體遭遇率從 5% 左右到 7% 以上不等。2018 年初又上升，之後的大部分時間都下降到僅超過 4%。2018 年惡意軟體遭遇率整體下降的一些潛在原因是 Windows 10 的採用率成長，以及 Windows Defender 保護功能的使用增加。遭遇率是執行 Windows Defender 防毒軟體的電腦在當月報告遇到惡意軟體的百分比，包括 Defender 封鎖的感染嘗試。

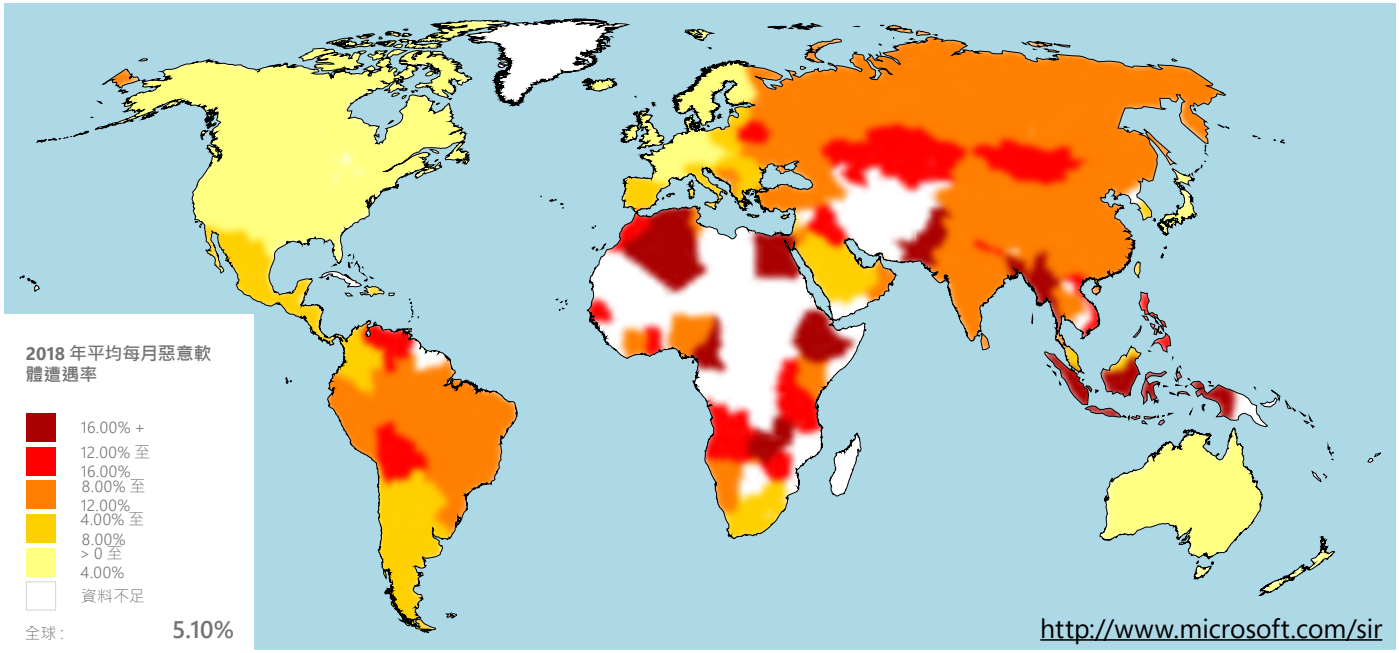


圖 9.

2018 年依國家/地區列出的全球平均每月惡意軟體遭遇率

2018 年 1 月至 12 月期間惡意軟體遭遇率最高的五個地點是衣索比亞 (平均每月遭遇率 26.33%)、巴基斯坦 (18.94)、巴勒斯坦地區 (17.50)、孟加拉 (16.95) 和印尼 (16.95)，在此期間所有這些地點都有平均每月遭遇率約 16.59% 或更高。感染率往往與社會中的人類發展因素和技術整備情況密切相關。在聯合國國際電信聯盟 (ICT) 公佈的 2017 年資訊和通訊技術 (ICT) 指數中，2018 年遭遇率最高的所有地點都排在國家/地區的倒數 40% 之列。

同一期間惡意軟體遭遇率最低的五個地點是愛爾蘭 (1.26)、日本 (1.51)、芬蘭 (1.74)、挪威 (1.79) 和荷蘭 (1.82)，在此期間所有這些地點的平均每月遭遇率都在 1.82% 或更低。這些地點往往擁有成熟的網路安全性基礎設施，以及用於保護關鍵基礎設施和向民眾宣導基本安全性的完善方案。

受惡意軟體影響最嚴重的國家/地區的平均每月遭遇率

衣索比亞： 26.33%

巴基斯坦： 18.94%

巴勒斯坦地區： 17.50%

透過 DART 調查網路事件

多個金融服務組織經歷了國家級攻擊，中斷了營運

在 DART 看到的一個較具破壞性的事件中，幾個金融服務組織成為受國家級贊助之 APT (不同於前面所提及、鎖定專業服務組織的群組) 的目標。

這種 APT 使用高度針對性、模糊的後門植入程式 (可能是透過魚叉式網路釣魚電子郵件傳遞)，感染了零號患者電腦 (Patient Zero) 之後，獲得了管理存取權限。隨後，APT 進行了多次欺詐交易，將大量現金轉入外國銀行帳戶。在某些情況下，攻擊者在 100 多天內沒有被發現。攻擊者意識到他們被偵測到後，迅速部署了預演攻擊，將破壞性惡意軟體傳送到環境中一半以上的系統，因此這些客戶的營運關閉了好幾天。

從這些事件中，有一些關鍵的教訓。首先，軟體生命週期管理特別重要，其中包括確保系統定期更新 (作業系統和安全性)、修補和稽核。在某種情況下，一個組織的 Linux 系統環境中執行的工作負載數量異常多，完全不受管理，面臨著極高的攻擊風險。第二個教訓是，務必將系統資料的備份儲存在離線位置，以防主要資料遺失。另一個教訓是，如果您需要了解對手活動，傳統的防毒解決方案可能還不夠。

恢復正常運作模式是這些組織的最高優先要務。DART 透過首先調查影響，然後採取必要的緩解措施 (例如從受影響的系統中刪除惡意軟體，並使系統處於健全狀態)，以協助恢復服務。該團隊還對客戶進行如何使用 Microsoft 威脅調查工具 (包括 EDR 和其他工具) 的訓練，以便他們可以在網路中尋找異常行為和攻擊者活動。DART 強調，端點監視對於抵禦傳統防毒解決方案可能無法偵測到的複雜、針對性的攻擊至關重要。

指引

指引

要建立組織復原能力和有意義的風險降低措施，就需要採取包括預防、偵測和回應在內的安全做法。我們將以下建議的安全性最佳做法和控制整理到這些類別中。

預防：

預防性控制在整體防禦策略中發揮著關鍵作用，因為正確的投資會增加網路罪犯的攻擊成本，並隨著時間維持這些增加的攻擊成本 (不需要專家分析師來監測和解譯輸出)。預防性控制投資應以成本最低的技術為目標，穩定移除低廉和有效的攻擊技術。

預防需要考慮的四件事是：

1. **安全衛生至關重要。如本報告中分享的一些網路事件所示，常見的衛生問題可能會破壞進階安全功能，因此遵循以下提示有助於降低風險：**

- 避免使用不熟悉的免費和/或盜版軟體。僅使用來自受信任來源的軟體。
- 降低認證竊盜風險，包括保護特殊權限管理員帳戶。若要了解方法，請閱讀此部落格，其中概述了 Microsoft 用來指導和增強自身安全性狀態的一些原則和工具，以及一些規範性藍圖，以協助您制定自己的計劃。
- 應用軟體廠商提供的安全設定基線。
- 透過快速將最新更新應用於作業系統和應用程式，並立即為作業系統、瀏覽器和電子郵件部署關鍵安全性更新，使電腦保持最新狀態。隔離 (或淘汰) 無法更新或修補的電腦。
- 實施進階電子郵件和瀏覽器保護。部署具有進階威脅防護功能的安全電子郵件閘道，以抵禦現代網路釣魚變種。
- 啟用主機反惡意軟體和網路防禦，以獲得近乎即時的雲端封鎖回應 (如果在您的解決方案中可用)。

2. 實作存取控制。請考慮以下事項：

- 應用最小特殊權限原則，包括實現網路分段、從使用者中刪除本機管理員權限，以及在向電腦上執行的應用程式授予任何權限時謹慎行事。
- 僅下載來自可靠來源 (官方應用程式商店) 的應用程式。
- 部署強大的程式碼完整性原則，包括限制使用者可以執行的應用程式。如果可能，請採用安全性解決方案，限制在系統核心 (內核) 中執行的程式碼，並可以阻止未簽署的指令碼和其他形式的不受信任的程式碼。使用應用程式白名單。
- 若要了解軟體供應鏈攻擊以及如何防範這些攻擊，請閱讀 Microsoft 研究人員的這個部落格。

3. 保留備份。

- 為您的關鍵系統和資料建立抗毀損的備份。
- 使用雲端儲存服務，在線上自動備份資料。對於內部佈署的資料，請使用 3-2-1 規則定期備份重要資料。將資料的三個備份保留在兩種不同的儲存類型上，並在異地保留至少一個備份。

4. 提高警覺，一旦有懷疑，立即行動。

- 教導員工對要求敏感資訊的可疑通訊要有警覺，並指示他們如何立即回應並向組織的安全作業團隊報告這些資訊。訓練還可以協助減輕社交工程和魚叉式網路釣魚攻擊。
- 點擊網頁連結時要小心。養成安全網頁瀏覽習慣，並使用提供有關不安全網站的警告或封鎖存取不安全網站的解決方案，有助於降低遇到與加密貨幣挖礦相關之網站的可能性。
- 如果電腦執行速度異常緩慢，請尋找正在執行的任何可疑檔案，並隨時向作業系統廠商提交樣本。您可以將檔案提交給 Microsoft (https://www.microsoft.com/wdsi/filesubmission) 以進行惡意軟體分析。

偵測和回應：

偵測和回應透過限制攻擊者存取資源的時間來提升復原能力。這將透過增加攻擊者的成本 (他們必須重試或修改其作業)，並降低報酬率 (限制實現其目標的機率)，來降低攻擊者的投資報酬率。

使企業組織能夠更加滿足市場需求的雲端技術，也可以協助安全作業更有效地抵禦攻擊者。

圖 10.

SOC 的演化軌跡

當我們看到安全作業中心 (SOC) 的發展軌跡時，我們看到技術不斷提高 SOC 決策和行動的速度和品質。許多這些創新可以對應到美國空軍上校 John Boyd 記載的「觀察、定向、決定、行動」(OODA) 循環的每個階段。[3]

觀察 – SOC 可以利用大量可用的安全情報 (來自 Microsoft 和其他來源)，在組織內和外部環境中顯著增加其視野。

定向 – 隨著這些新資料來源可用於已經超載的 SOC，機器學習 (人工智慧的子集) 成為推理這些巨量資料集並識別值得調查之異常的重要工具。安全性廠商 (包括 Microsoft) 採用了機器學習技術來快速確定事件的優先順序 (並協助將這些個別事件融合為整體事件)。

決定 – 由於攻擊量和複雜性可能會使 SOC 快速超載，因此分析師和事件回應人員需要做出許多決策，並快速採取行動來回應警示和偵測。Microsoft 和其他廠商整合了自動調查功能和指引，以協助分析師快速做出正確的決策 (例如，隔離可能受感染或遭入侵的裝置)。目前，自動化的重點是快速解決低優先順序事件，以便將專門技能應用於更複雜的問題。

行動 – 回應需要在許多技術和平台上快速、準確的執行力，這正是安全性協調流程和回應自動化技術所實現的。Microsoft 和其他許多公司正在繼續投資於這些技術，包括現代威脅偵測和自動回應解決方案。

註腳

[3] http://www.militaryhistoryveteran.com/colonel-john-boyd-ooda-loop/

適用於現代 SOC 的一些其他趨勢包括：

- **警示饋送的品質優於數量** – 隨著組織從管理「不夠的資訊」轉向管理「過多的資訊」，高度專業化的 SOC 分析師的時間和注意力變得越來越有價值。這促使對警示品質的需求增加 (需要 1 級和 2 級分析師參與)。雖然額外的資料饋送總是有助於調查和主動搜尋，但 Microsoft 的企業 IT SOC 衡量的是需要分析師回應之警示饋送的真正率 (目前需要 90% 或更高的真正率)。

- 資料重力 – 如果不存取基礎原始資料，就很難對大型資料集 (包括安全性資料) 進行分析。隨著更多安全性資料的可用，相較於將資料回傳到內部佈署系統，在雲端中執行安全分析變得更加經濟實用。這可能會導致 SIEM 和 SOC 架構的演變，其中可能包括混合 SIEM 方法或將原生雲端 SIEM 做為服務。

- **高脈絡** – 這些類型的偵測更有用，因為它們能夠更有效地與資料集建立關聯。雖然傳統的網路流量型偵測仍然提供了一些安全性價值，但原始網路流量通常缺乏區分合法活動和異常活動的脈絡。我們看到 SOC 在脈絡豐富的偵測中獲得了更多的價值，例如：

  - **端點偵測和回應 (EDR)** 解決方案，對主機活動具有深層脈絡
  - 身分識別型偵測，包括對一般使用者驗證模式 (位置、時間、存取的服務等) 的洞察，並應用行為分析

對手更難以避免這些脈絡豐富的偵測，因為他們必須模擬更複雜的作業 (相對於 IP 流量的一些技術屬性)。

我們從客戶的重大外洩事件中吸取的另一個教訓是，當 IT 功能有一部分或全部外包時，將很難快速回應事件。我們建議您審查 IT 外包合約和服務等級協定 (SLA) 以及供應鏈廠商，以確保其相容於快速安全性回應。如需有關客戶事件調查的更多資訊，請參閱事件回應參考指南 (IRRG)，網址為 https://aka.ms/IRRG。

資料來源

資料來源

Microsoft 在提供廣泛 Microsoft 產品和服務的過程中 (如 Microsoft 隱私權聲明中所討論)，收集了 Microsoft 安全情報報告中包含的資料。這些資料為我們提供了有關產品和服務安全性和作業的寶貴資訊，以及對網路安全性威脅環境的整體洞察。這些資料包括來自以下來源的分析：[4]

- **Azure 資訊安全中心**服務對於雲端工作負載安全性提供更高的可見度，並運用進階分析和威脅情報來偵測攻擊，藉此協助組織防止、偵測及回應威脅。
- **Bing** 搜尋與決策引擎，每年執行數十億次網頁掃描，以找出惡意內容。偵測到此類內容後，Bing 便會向使用者顯示警告，以協助防止感染。
- **Exchange Online** 是 Microsoft 管理的電子郵件和生產力服務。Exchange Online 反惡意程式碼和反垃圾郵件服務每年掃描數十億封訊息，以識別並封鎖垃圾郵件和惡意程式碼。
- **惡意軟體移除工具** (MSRT) 是免費工具，Microsoft 設計用來協助從客戶電腦識別和移除特定普遍的惡意程式碼系列。MSRT 主要是透過 Windows Update、Microsoft Update 和自動更新發佈的重要更新。此工具版本也可從 Microsoft 下載中心取得。MSRT 並非最新即時防毒解決方案的取代品。
- **Microsoft 安全掃描工具**是可下載的免費安全性工具，提供視需要掃描功能，有助於移除惡意程式碼及其他惡意軟體。Microsoft 安全掃描工具並非要取代最新的防毒解決方案，因為這無法提供即時保護，也無法防止電腦遭受感染。

註腳

[4]重要的是，基於安全性考量，在使用之前，這些資料始終要經過嚴格的隱私權和合規性邊界管制。

- **Microsoft Security Essentials** 是免費、容易下載的即時保護產品，可為 Windows Vista 和 Windows 7 提供基本、有效的防毒和反間諜保護。

- **Microsoft System Center Endpoint Protection** (前身為 Forefront Client Security 和 Forefront Endpoint Protection) 是整合式產品，可為企業桌上型電腦、筆記型電腦及伺服器作業系統提供惡意程式碼和垃圾軟體防護。此產品運用 Microsoft Malware Protection Engine 和 Microsoft 防毒特徵碼資料庫，提供即時、排程和視需求保護。

- **Office 365** 是 Microsoft Office 訂閱服務，適用於組織和家庭使用者。精選訂閱方案包括存取 Office 365 進階威脅防護。

- Windows 安全性包含在 Windows 10 中，提供惡意程式碼和垃圾軟體的即時掃描和移除功能。此外，最新版本的 Windows 利用豐富的脈絡資料 (如電腦設定、裝置效能和健康情況等) 和其他這類資訊來增強客戶的安全性。同時，我們讓客戶在 Windows 10 中更加了解其隱私權。請閱讀此部落格，了解 Microsoft 這樣做的一些方法。

- **Windows Defender 進階威脅防護**是 Windows 10 年度更新版和更新版本內建的服務，可讓企業客戶偵測、調查及修復網路上的進階持續威脅和資料外洩。

- **Windows Defender Offline** 是可下載的工具，可用於建立可開機的 CD、DVD 或 USB 快閃磁碟機，以掃描電腦是否存在惡意程式碼和其他威脅。此產品未提供即時保護，也不是最新反惡意程式碼解決方案的替代品。

- **Windows Defender SmartScreen** 是 Microsoft Edge 和 Internet Explorer 中的功能，提供使用者防範網路釣魚網站和裝載惡意程式碼網站的保護。Microsoft 維護由 Microsoft Edge、Internet Explorer 及其他 Microsoft 產品和服務回報的釣魚網站和惡意程式碼網站的資料庫。在啟用篩選器後，當使用者嘗試瀏覽資料庫中的網站時，瀏覽器會顯示警告並封鎖頁面瀏覽。