MANDIANT
現在是 Google Cloud 的一員

M-TRENDS 2023

MANDIANT 特別報告

目錄

簡介

現實世界和網路領域之間的界限從未如此模糊。我們看到俄羅斯參與資訊行動，試圖影響關於其入侵烏克蘭的敘事，並試圖透過實體和網路攻擊來干擾關鍵基礎設施。我們看到入侵對更廣泛的網路犯罪生態系統產生了影響，特別是在歐洲，那裡的發動者正在選擇立場或完全中斷運作。我們看到發動者參與網路犯罪以資助間諜活動，支援北韓政權，以從核子到 COVID-19 等主題的相關資訊為攻擊目標。

Mandiant 回應人員每天都在調查和分析最新的攻擊和威脅，並瞭解如何以最佳方式來應對和緩解攻擊和威脅。我們透過各種服務將這些知識傳遞給我們的客戶，幫助他們在瞬息萬變的威脅環境中保持領先。

在發布我們的年度 M-Trends 報告時，我們旨在為更大的資安社群提供一些同樣的關鍵情報。M-Trends 2023 會一如既往地提供不斷演進的網路環境的詳細資訊、建議的緩解措施以及各種各樣的安全事件相關指標。

先來說說「數字會說話」部分的最大問題之一。答案為「是」，我們正在以比以往更快的速度偵測到攻擊。從 2022 年 1 月 1 日到 2022 年 12 月 31 日，全球停留時間中間值現在為 16 天，與我們 2022 年 M-Trends 報告的 21 天相比有所降低。這可能表明偵測攻擊的能力有所提高，但我們也認為勒索軟體攻擊是減少停留時間的一個驅動因素。2022 年涉及勒索軟體的入侵停留時間中間值為 9 天，相比之下，2022 年 M-Trends 所報告的時間為 5 天。

M-Trends 2023 的主題包括：

數字會說話：在 63% 的事件中，組織從外部實體收到入侵通知，而 2022 年 M-Trends 中這一比例為 47%，這使全球偵測率更接近防禦者在 2014 年所經歷的情況。我們有更多關於目標產業、攻擊類型、威脅組織和惡意軟體使用的特徵指標，以及基於趨勢和觀察結果的新詳細分解。

入侵烏克蘭：俄羅斯對烏克蘭的入侵幾乎消耗了俄羅斯國際關係的各個方面，並已經幾乎演變成 2022 年俄羅斯網路威脅活動的唯一推動因素。我們涵蓋了可追溯到二月的實體入侵之前的行動，包括使用破壞性和干擾性攻擊，以及資訊行動。

北韓經濟行動：據報導，多年來北韓進行了各種非法金融活動來資助該政權。加密貨幣的爆炸性成長正在與積極和持久的北韓網路能力彙聚，自然使至少一些北韓威脅組織會將行動延伸到該領域。

變化的重點和不常見的技術：2022 年，調查了一系列知名的入侵事件，儘管這些事件嚴重偏離常見的威脅發動者行為，但是這些入侵仍然取得成功，並對受攻擊的目標群組組織產生影響，強調了願意避開潛在交戰規則的持久型對手給組織造成的威脅。

M-Trends 2023 還包含一個紅隊案例研究、來自我們活動與全球事件團隊的威脅發動者與漏洞故事，以及我們 APT42 升級的詳細資訊。

M-Trends 以我們的奉獻精神為基礎，繼續為負責防禦的各類組織提供了關鍵資訊。本報告中的資訊已經過處理，以保護受害者的身分及其資料。

數字會說話

來自 Mandiant 調查的資料

M-Trends 2023 報告的指標是以 Mandiant Consulting 對 2022 年 1 月 1 日至 2022 年 12 月 31 日期間展開的針對性攻擊活動所進行的調查為基礎。注意，與 M-Trends 2022 報告的 15 個月期限相比，該版本的 M-Trends 期限為過去的 12 個月。

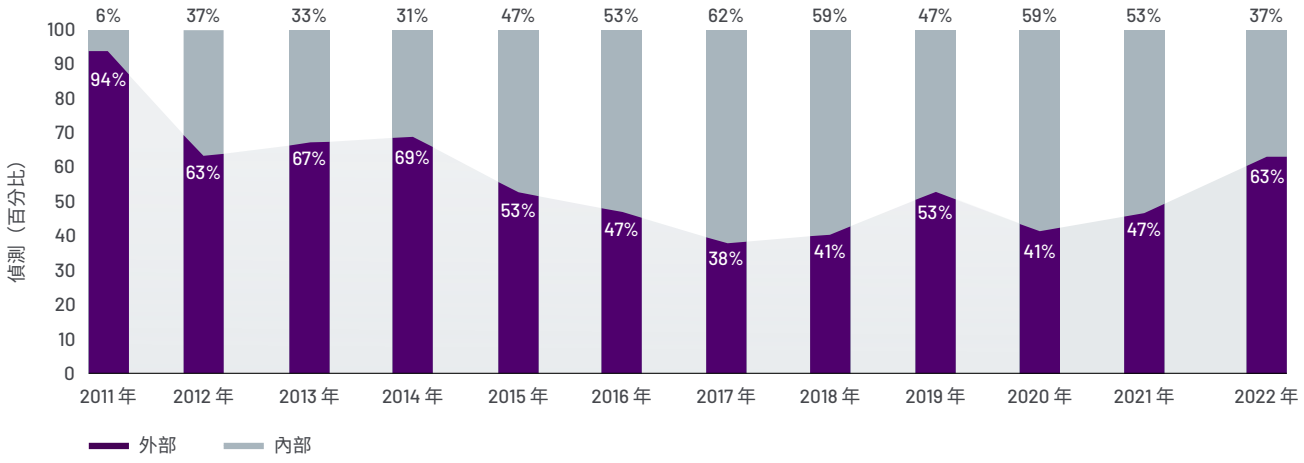
內部偵測是組織獨立發現其被入侵的情況。

外部偵測是外部實體通知組織其被入侵的情況。

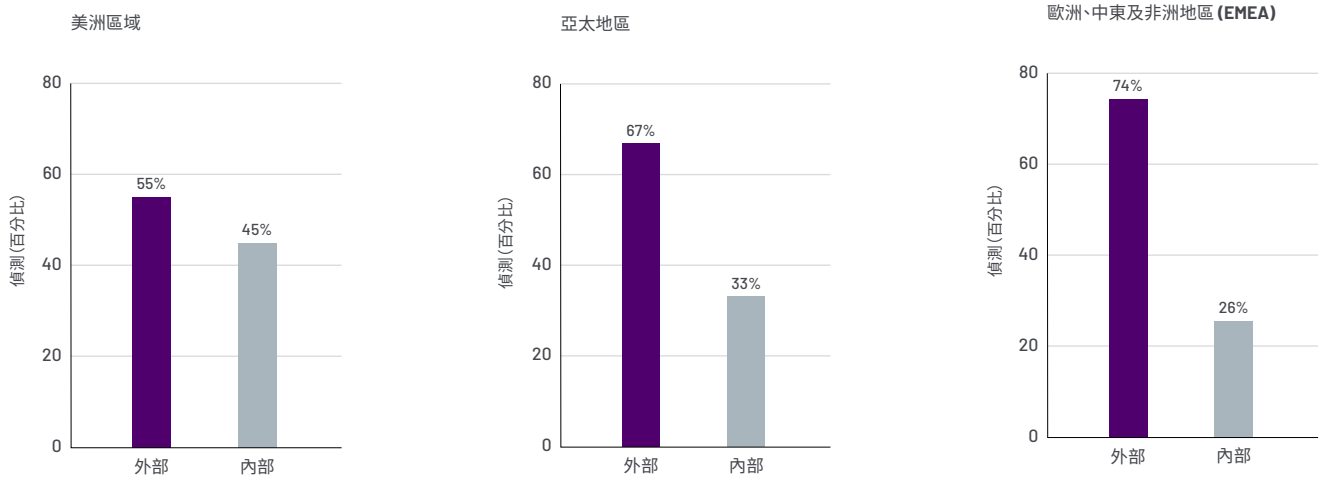
依來源偵測

2022 年，Mandiant 觀察到由外部實體警告存在以往或現今入侵的組織數量普遍增加。在 63% 的入侵事件中，組織收到了外部實體的通知。這延續了 2021 年觀察到的趨勢，使全球偵測率更接近防禦者在 2014 年經歷的情況。2022 年觀察到的外部通知的增加可能受到 Mandiant 對針對烏克蘭的網路威脅活動之調查支援，以及主動通知工作增加的影響。資安合作夥伴的主動通知使組織能更有效地啟動應對工作。入侵烏克蘭部分中重點分析了 Mandiant 在烏克蘭的工作：戰時的網路行動。

依來源偵測，2011-2022 年



地區偵測（按來源），2022 年



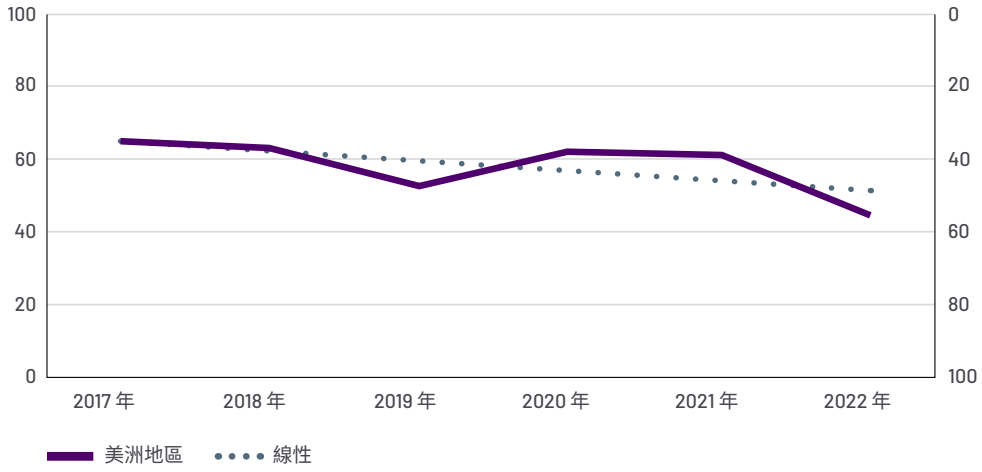
以往，Mandiant 觀察到總部位於美洲地區的組織偵測率相對穩定。然而，在 2022 年，組織在 55% 的事件中收到了外部實體通知，相比之下去年的比例為 40%。這是美洲地區在過去六年中所見過的最高比例的外部通知。雖然美洲地區的組織繼續提高偵測能力，但是來自可信資安合作夥伴的外部通知仍然是組織瞭解事件的主要方式。

2022 年，Mandiant 專家在亞太 (APAC) 區域回應的事件中有 33% 最初是由外部實體確認的。然而，在過去六年中，Mandiant 觀察到亞太區域的外部通知有增加的趨勢。與 2021 年相比，今年的內部偵測增加了 9%，這表明 Mandiant 在亞太區域觀察到的偵測源存在很大差異。

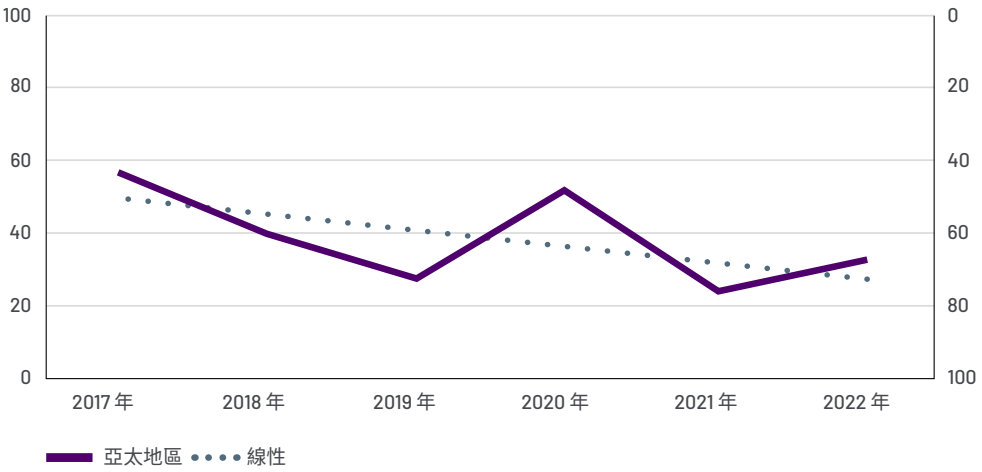
在 2022 年 74% 的調查中，歐洲、中東和非洲 (EMEA) 的組織收到了外部實體的入侵警報，而相比之下 2021 年這一比例為 62%。這一外部通知的顯著增長可以用 Mandiant 對烏克蘭的調查支援來解釋，並且很有可能是總體趨勢的異常值。在過去六年中，Mandiant 繼續看到 EMEA 區域轉向更多的外部通知，但由於 2022 年情有可原的情況，這一趨勢可能會在未來穩定下來。

地區偵測 (按來源)，2017–2022 年

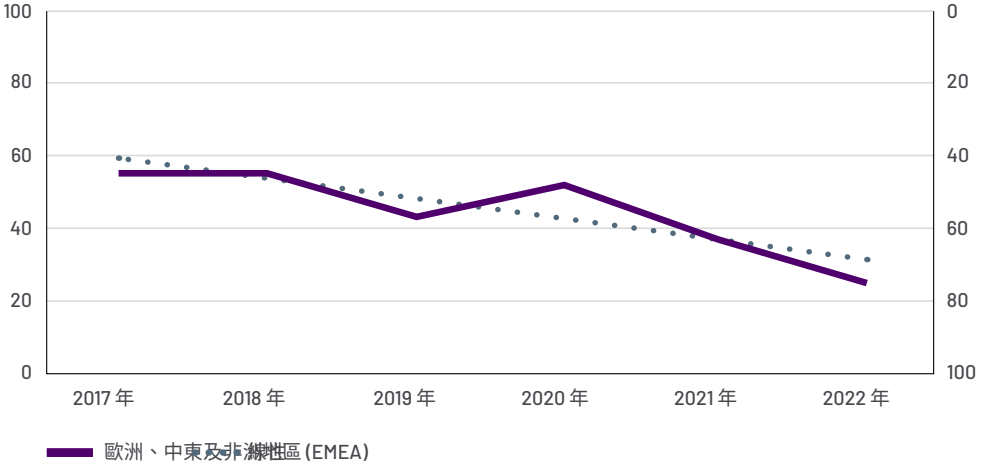
美洲區域



亞太地區



歐洲、中東及非洲地區 **(EMEA)**



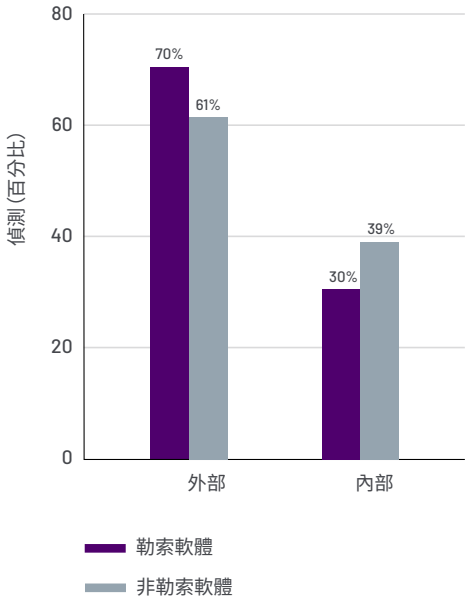
與勒索軟體相關的入侵為惡意發動者提供存取，或與惡意發動者相關，而該惡意發動者的主要目標是對資料進行加密，以便向目標索要贖金，從而避免進一步或撤銷惡意行為。

2022 年 無論調查類型如何 外部通知作為通知來源都更加普遍。在與勒索軟體有關的入侵中，組織在 70% 的調查中收到了外部實體通知。由於完整執行的勒索軟體事件有 67% 的調查（佔所有調查的 8%）是由於贖金備註而被偵測到，組織主要是從對手那裡收到通知。其餘 33% 的勒索軟體相關調查（佔所有調查的 4%）是由外部合作夥伴通知。

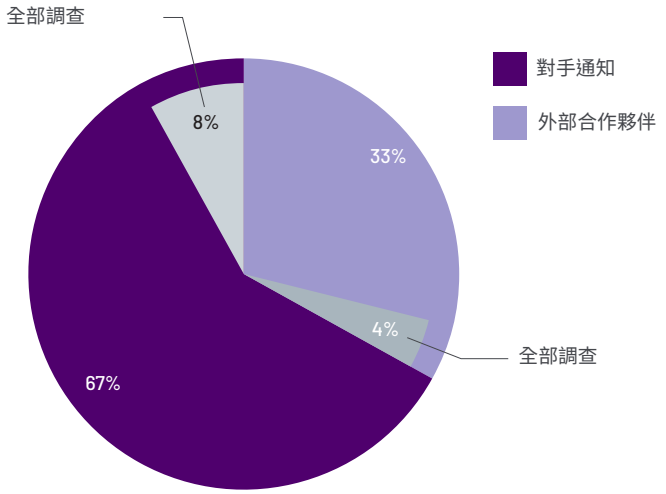
同樣地，外部實體向組織通知非勒索軟體相關入侵的頻率要高於組織能夠在內部確認類似入侵的頻率。然而，Mandiant 觀察到組織在 2022 年內部發現非勒索軟體入侵的頻率要高於發現勒索軟體入侵的頻率。這可能是由於可視性的增加造成的，允許組織在針對性攻擊生命週期內及早偵測入侵。雖然非勒索軟體行動通常會優先避免偵測機制，但是與勒索軟體操作者採用的相對較短週期相比，更長的行動週期會提供更多的偵測機會。

Mandiant 繼續看到組織與執行入侵通知的外部合作夥伴之間存在積極合作。這些外部方提供的有效資訊有助於組織更快地識別入侵，無論調查類型如何。

依來源偵測，按照調查類型劃分，2022 年



勒索軟體調查 —— 外部通知來源



停留時間

停留時間的計算方式為攻擊者在被偵測到之前，停留在受害環境的天數。中間值表示按大小排序的資料組中間點的數值。

停留時間中間值變化

21 → **16**

2021 年日數　　2022 年日數

全球停留時間

全球停留時間中間值繼續逐年改善，2022 年組織在兩週多的時間裡就偵測到事件。這是所有 M-Trends 報告期間內最短的全球停留時間中間值。

在外部實體為通知來源的情況下，全球停留時間中間值的顯著改善可能表明組織能更快地回應外部通知。這反映出人們越來越認識到合作關係和資訊交流在打造強韌的網路安全生態系統方面所發揮的關鍵作用。隨著資安合作夥伴正在改善外部通知中包含的關鍵資訊，資訊分享的改善將使組織能比獨自識別類似入侵時更加有效地採取行動。

防禦者繼續以比外部實體通知更快的速度偵測事件。2022 年內部偵測事件的全球停留時間中間值返回防禦者在 2020 年看到的類似時間框架。2022 年，內部偵測出的入侵的全球停留時間中間值為 13 天。2021 年，全球停留時間中間值是 18 天，2020 年為 12 天。

同樣地，Mandiant 專家觀察到，2022 年具有外部通知來源的調查的全球停留時間中間值再次顯著下降，與 2021 年相比下降了 32%。外部通知讓組織能在初步破壞後 19 天的中間值內發起對入侵的回應。

2022 年全球停留時間中間值的改善（如論偵測來源如何）使組織能以比以往更快的速度回應事件。

全球停留時間中間值，2011-2022 年

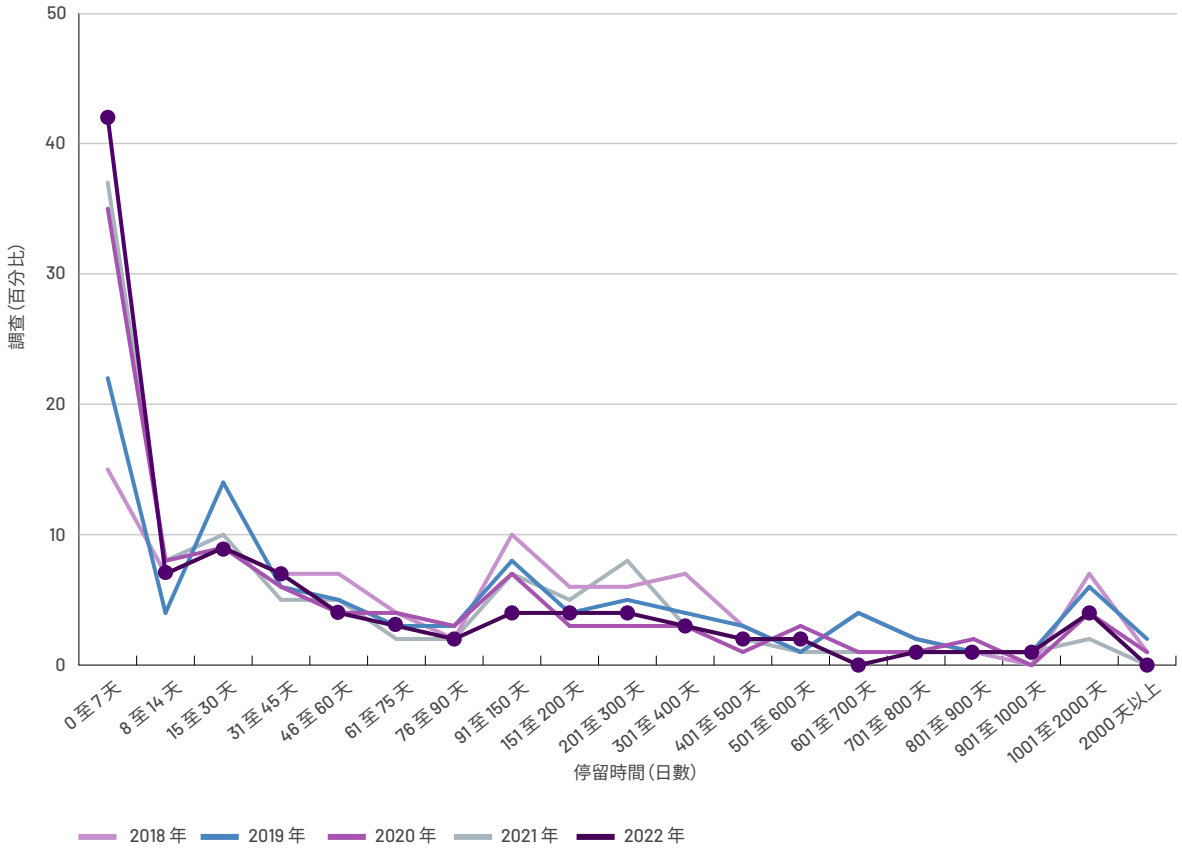
	2011 年	2012 年	2013 年	2014 年	2015 年	2016 年	2017 年	2018 年	2019 年	2020 年	2021 年	2022 年
全部	416	243	229	205	146	99	101	78	56	24	21	16
外部	–	–	–	–	320	107	186	184	141	73	28	19
內部	–	–	–	–	56	80	57.5	50.5	30	12	18	13

全球停留時間分布

全球停留時間分布繼續改善。42% 的入侵在一週或更短時間內被偵測到，相比之下上一個報告期內此類入侵的比例為 37%。與往年相比，Mandiant 在 2022 年的調查中發現停留時間分布更加均勻。這延續了上一個 M-Trends 報告期的趨勢，表明偵測正變得更加簡化，偵測能力已經得到改善，強調針對性攻擊生命週期的初始感染或事前勘查階段期間環境中的行動。

然而，隨著 Mandiant 繼續看到非勒索軟體相關調查的廣泛分布，組織仍然在面對長時間未被偵測到的入侵。受影響組織偵測能力的差異和他們所面臨的入侵類型有可能是這種分布擴散的促進因素。

全球停留時間分布，2018–2022 年



涉及勒索軟體的全球調查變化

23% → **18%**

在 2021 年　　在 2022 年

全球停留時間中間值變化 –– 勒索軟體

5 → **9**

2021 年日數　　2022 年日數

全球停留時間中間值變化 –– 非勒索軟體

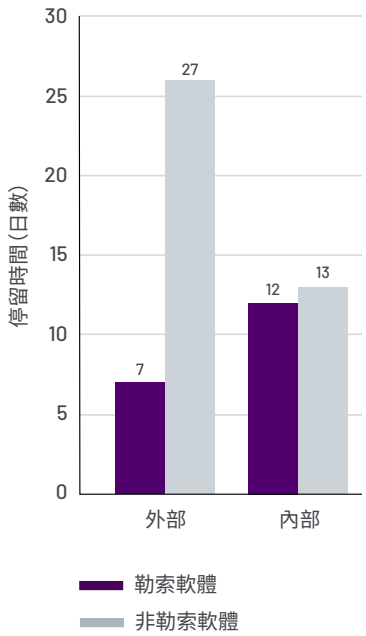
36 → **17**

2021 年日數　　2022 年日數

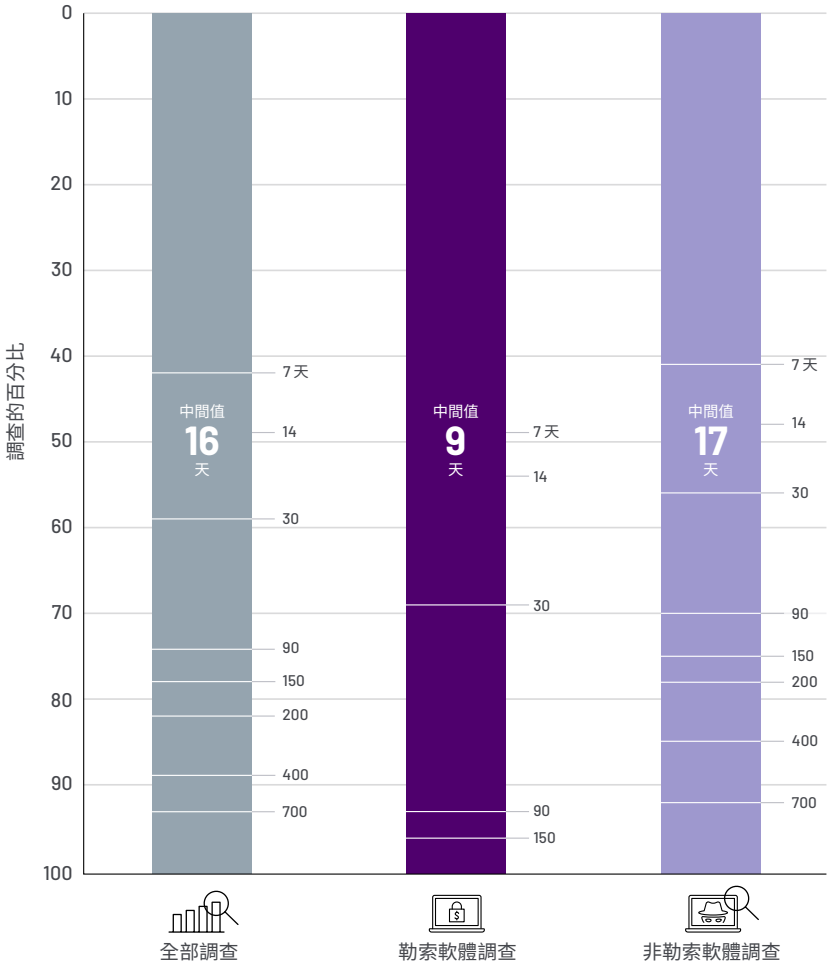
涉及勒索軟體的調查

Mandiant 專家指出，2021 到 2022 年間，涉及勒索軟體的全球入侵百分比有所下降。2022 年，有 18% 的入侵涉及到勒索軟體，相比而言，2021 年為 23%。勒索軟體攻擊仍然是停留時間減少的驅動因素。2022 年涉及勒索軟體的入侵停留時間中間值為 9 天，相比之下，2021 年為 5 天。Mandiant 觀察到在內部實體發出通知的例項中，涉及勒索軟體的入侵的全球停留時間中間值為 7 天，相比之下，組織在內部偵測到入侵時為 12 天。Mandiant 觀察到，與 2021 年相比，2022 年對手利用的勒索軟體未被偵測到的時間更長。

全球停留時間中間值（按偵測來源）



全球停留時間（按調查類型劃分），2022 年



美洲地區

美洲地區停留時間中間值變化

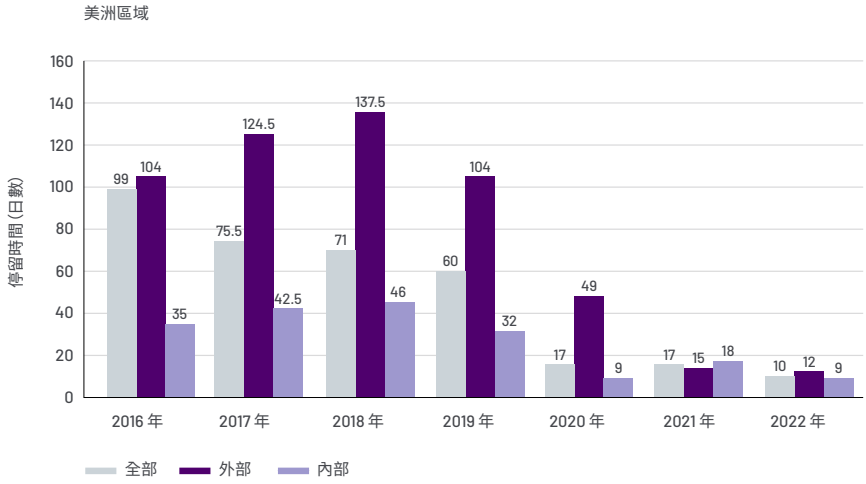
17 → **10**

2021 年日數　　2022 年日數

美洲地區停留時間中間值

2022 年，美洲地區調查的入侵的停留時間中間值下降一整週，達到 10 天，相比之下，2021 年和 2020 年為 17 天。Mandiant 觀察到美洲地區所有偵測類型的停留時間中間值具有一致性，其內部偵測降至 9 天，外部偵測降至其最低點 12 天。美洲地區的組織在比往年更快偵測到對手方面取得了進步，比之前在 2021 年觀察到的 17 天的最小時間範圍更快。

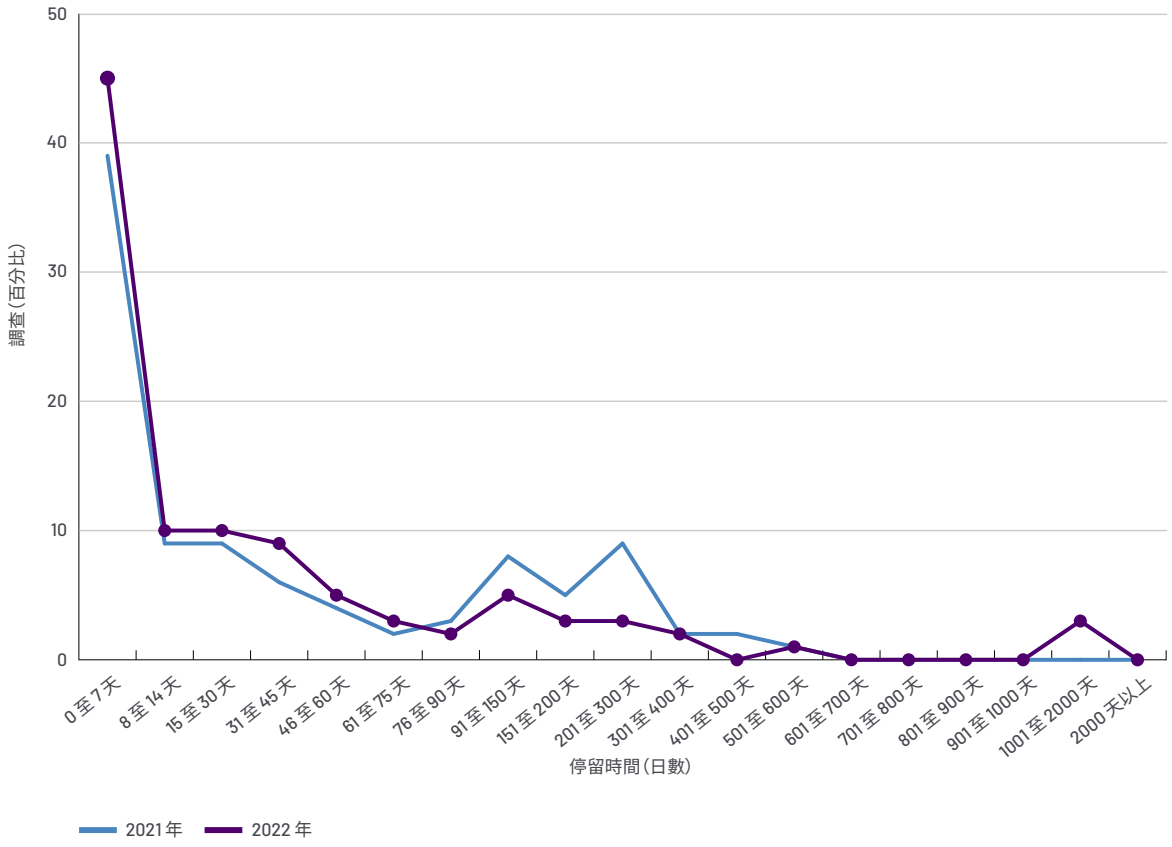
美洲地區停留時間中間值停留時間，2016-2022 年



美洲地區停留時間分布

在美洲地區，有 64% 的入侵是在 30 天或更少時間內偵測出，且其中有 70% 的入侵（美洲地區入侵總數的 45%）是在一週內偵測出。2022 年，美洲地區超過一半的入侵是在不到兩週的時間內偵測出。然而，Mandiant 觀察到長時間未被偵測到的入侵數量有小幅回升，美洲地區的入侵總數中有 7% 在超過一年的時間後仍未被偵測到。這與 M-Trends 2022 報告期中觀察到的 4% 有所增加。這表明，雖然美洲地區的組織能夠在兩週內偵測大部分入侵，但由於偵測改善，他們確認了原本會在更長時間內未被偵測到的對手入侵。

美洲地區停留時間分布，2021-2022 年



美洲地區涉及勒索軟體的調查變化

22% → **22%**

在 2021 年　　在 2022 年

雖然涉及勒索軟體的入侵百分比在全球範圍內都有所減少，但是 Mandiant 觀察到美洲地區涉及勒索軟體的調查百分比與去年具有一致性。同樣地，美洲地區的勒索軟體停留時間依舊保持不變。Mandiant 指出，無論是內部或外部偵測來源，這些調查都有類似的停留時間中間值，其中內部通知的調查停留時間中間值為五天，而外部實體通知的為六天。Mandiant 繼續觀察到非勒索軟體相關入侵的外部通知有所改善。2022 年，美洲地區的組織在 12 天內偵測到與勒索軟體不相關的入侵，相比之下 2021 年為 17 天。

美洲地區停留時間中間值變化 –– 勒索軟體

5 → **5**

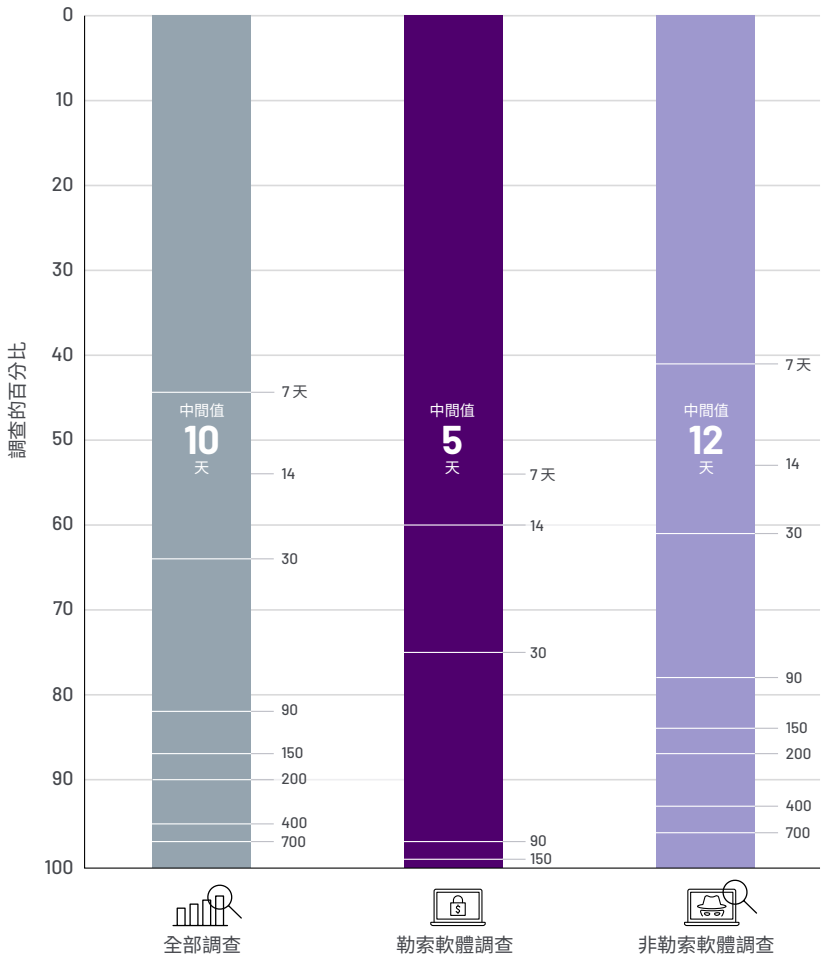
2021 年日數　　2022 年日數

美洲地區停留時間中間值變化 –– 非勒索軟體

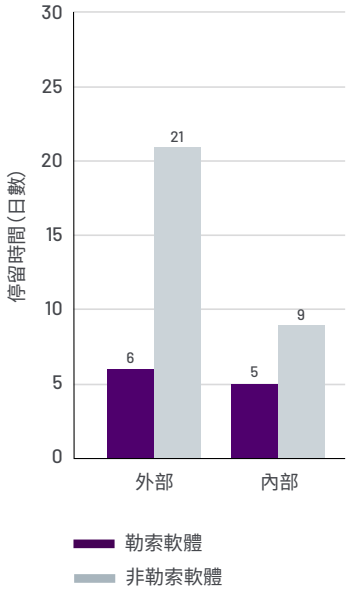
17 → **12**

2021 年日數　　2022 年日數

美洲停留時間（按調查類型劃分），2022 年



美洲地區停留時間中間值（按偵測來源）



亞太地區

亞太地區停留時間中間值變化

21 → **33**

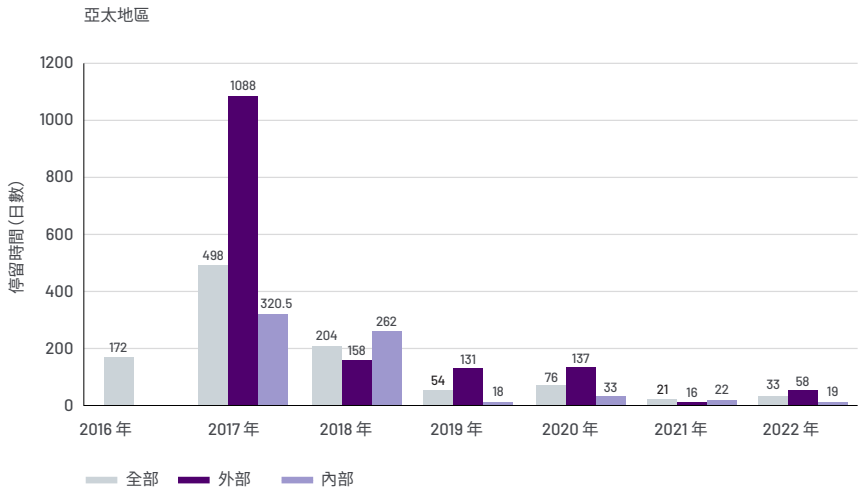
2021 年日數　　2022 年日數

亞太地區停留時間中間值

總體上，亞太地區的停留時間中間值與上一個 M-Trends 報告期相比有所下降。然而，亞太地區的組織仍在與比往年更快的速度偵測入侵，其內部確認的入侵停留時間中間值為 19 天，相比之下 2021 年為 22 天。在過去三年中，亞太地區的組織一直在不斷改善內部偵測能力。

來自外部實體的通知導致 2022 年的停留時間中間值為 58 天，相比之下 2021 年為 16 天。雖然這代表著停留時間中間值有所增加，但與 2020 年的 137 天外部通知停留時間中間值相比，仍減少了 58%。增加到 58 天可能是由於停留時間中間值從 2021 年觀察到的異常短的時間的正常化。

亞太地區停留時間中間值，2016-2022 年

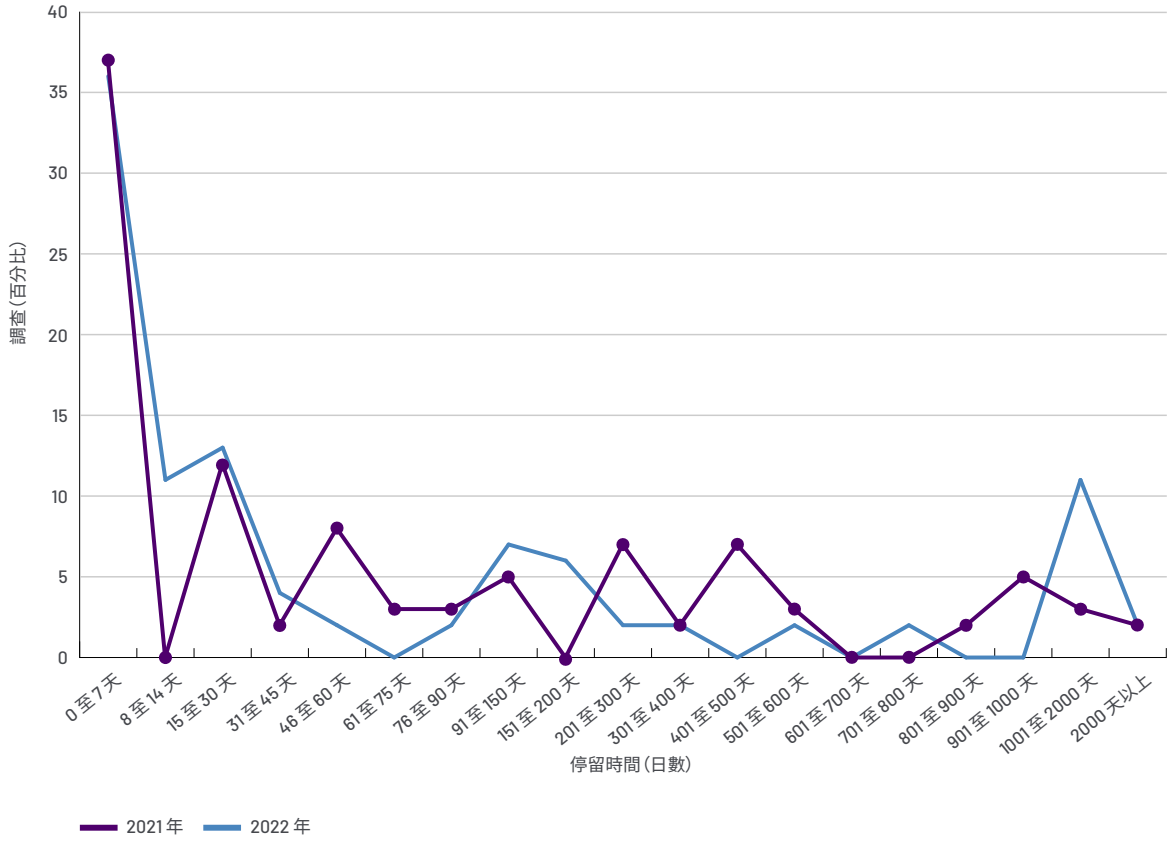


亞太地區停留時間分布

亞太地區停留時間分布繼續出現差異。停留時間分布圖顯示，亞太地區調查有 48% 的停留時間在 30 天內，且其中有 76% 的入侵（佔亞太地區總入侵數的 37%）是在一週內偵測出。在停留時間分布圖的另一面，亞太地區組織長時間未被偵測到的入侵分布更廣，其中有 30% 的調查在一年或更長的時間內未被偵測到，而 2021 年的調查只有 20%。

隨著偵測能力不斷提高，亞太地區的網路安全不斷成熟。這讓組織能發現原本會在長時間內未被偵測到的入侵，從而導致入侵分布更廣泛。

亞太地區停留時間分布，2021-2022



亞太地區涉及勒索軟體的調查變化

38% → **32%**

在 2021 年　　在 2022 年

與觀察到的涉及勒索軟體的全球調查減少類似，亞太地區的勒索軟體調查減少了 6%，2022 年為 32%，相比之下 2021 年為 38%。這個數字仍然幾乎是 2020 年 (12.5%) 和 2019 年 (18%) 調查百分比的兩倍。

亞太地區勒索軟體調查的停留時間中間值為 18 天，相比之下非勒索軟體調查為 60 天。無論調查類型如何，亞太地區的組織在內部偵測事件的速度比在外部更快。然而，觀察到的與勒索軟體停留時間中間值有關的時間範圍確實會對整體停留時間產生重大影響。

亞太地區停留時間中間值變化 —— 勒索軟體

9 → **18**

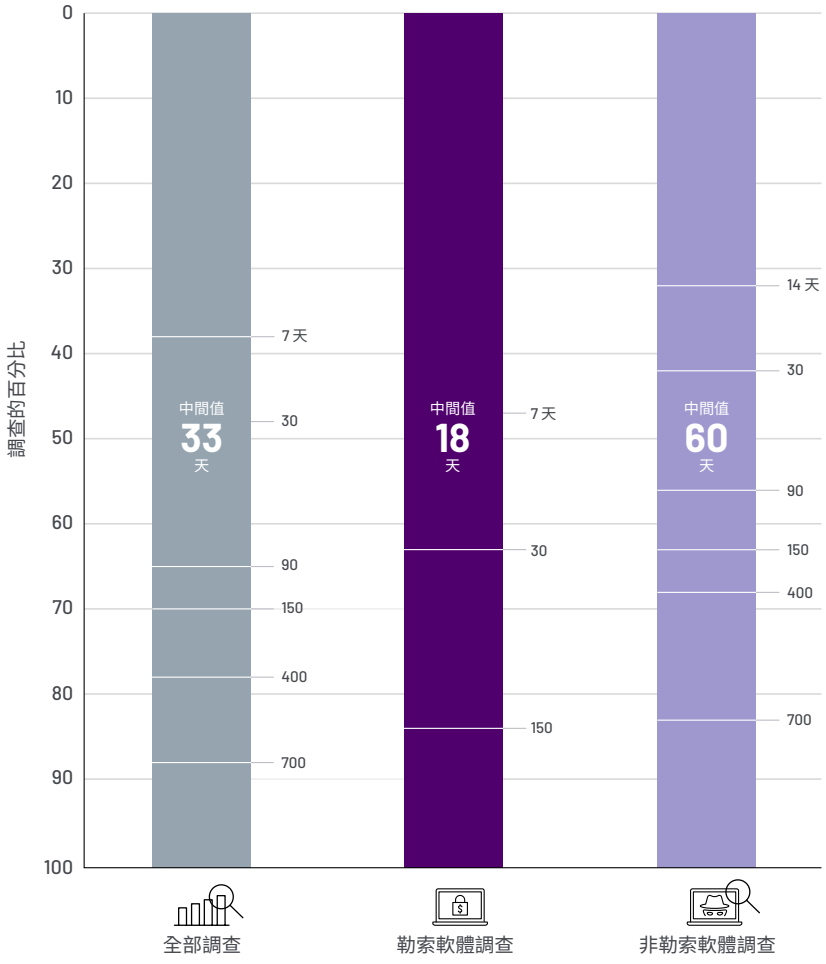
2021 年日數　　2022 年日數

亞太地區停留時間中間值變化 —— 非勒索軟體

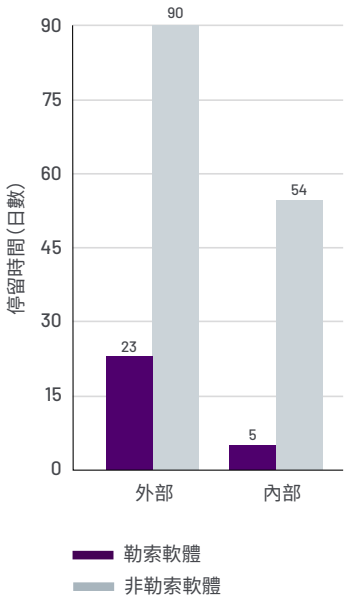
38 → **60**

2021 年日數　　2022 年日數

亞太地區停留時間 (按調查類型劃分)，2022 年



亞太地區停留時間中間值 (按偵測來源)



歐洲、中東及非洲地區 (EMEA)

EMEA 停留時間中間值變化

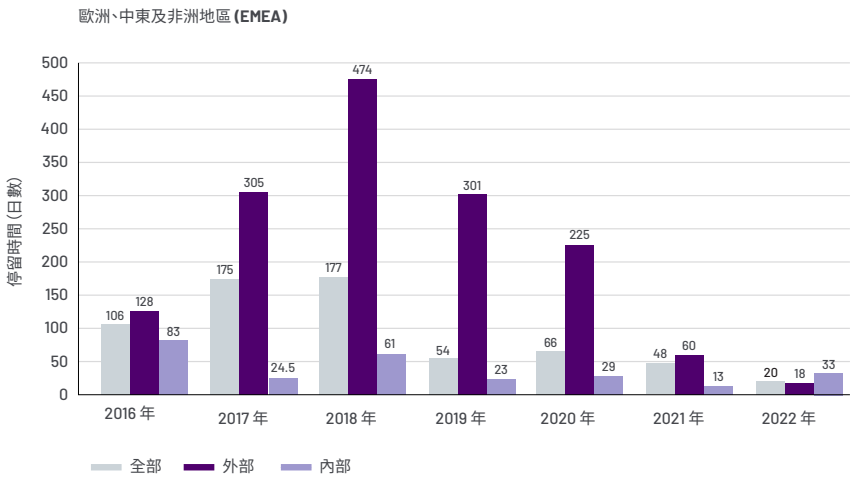
48 → **20**

2021 年日數　　2022 年日數

EMEA 停留時間中間值

EMEA 地區的組織在 2022 年偵測事件的速度比 2021 年要快 58%，其目前的總體停留時間中間值少於三週。仔細觀察偵測來源，被外部來源偵測到的入侵停留時間中間值從 2021 年的 13 天增加到 2022 年的 33 天。外部通知來源從 2021 年的 60 天降低到 2022 年的 18 天。這一巨大的變化可能收到 Mandiant 在烏克蘭的工作影響，該工作在 2022 年 EMEA 調查中佔了很大一部分。然而，即使在這項工作之外，總體趨勢表明停留時間中間值仍在逐年減少。

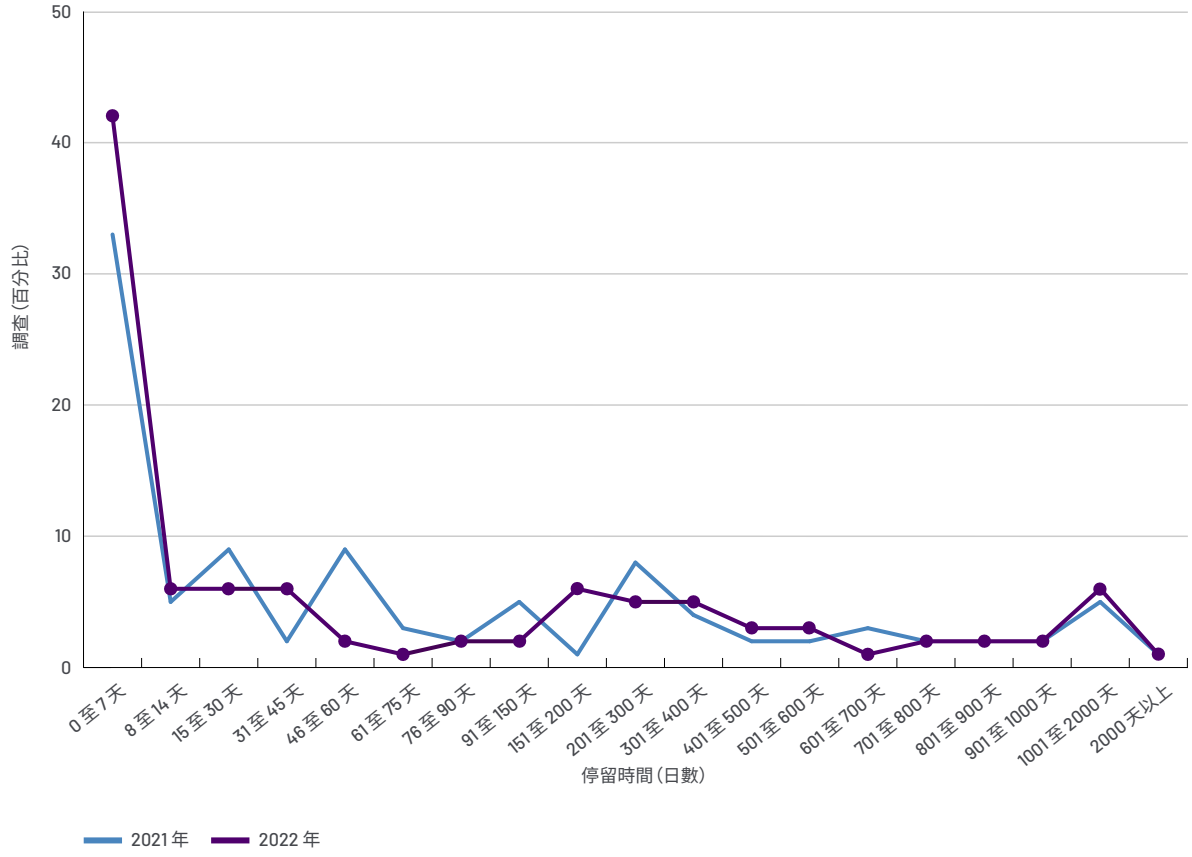
EMEA 停留時間中間值，2016-2022 年



EMEA 停留時間分布

EMEA 停留時間分布表明，Mandiant 調查的入侵中有 54% 是在 30 天內被確認，這些入侵中有 76%（佔 EMEA 調查總數的 42%）是在一週內被確認。EMEA 的組織在更快地偵測到絕大多數事件方面表現出改進。然而，入侵的總體分布仍與 2021 年保持一致，其中有 23% 的入侵時在最初入侵開始一年後被確認。

EMEA 停留時間分布，2021-2022 年



EMEA 涉及勒索軟體的調查變化

17% → **7%**

在 2021 年　　在 2022 年

EMEA 停留時間中間值變化 —— 勒索軟體

4 → **33**

2021 年日數　　2022 年日數

EMEA 停留時間中間值變化 —— 非勒索軟體

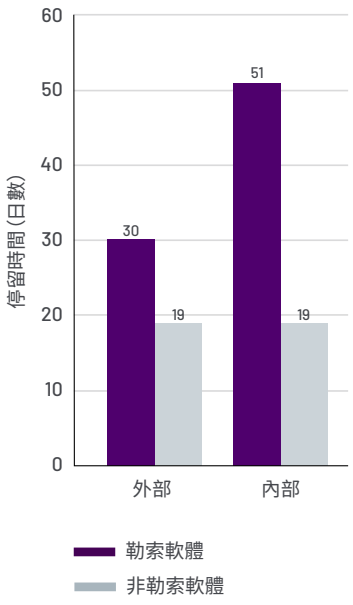
60 → **19**

2021 年日數　　2022 年日數

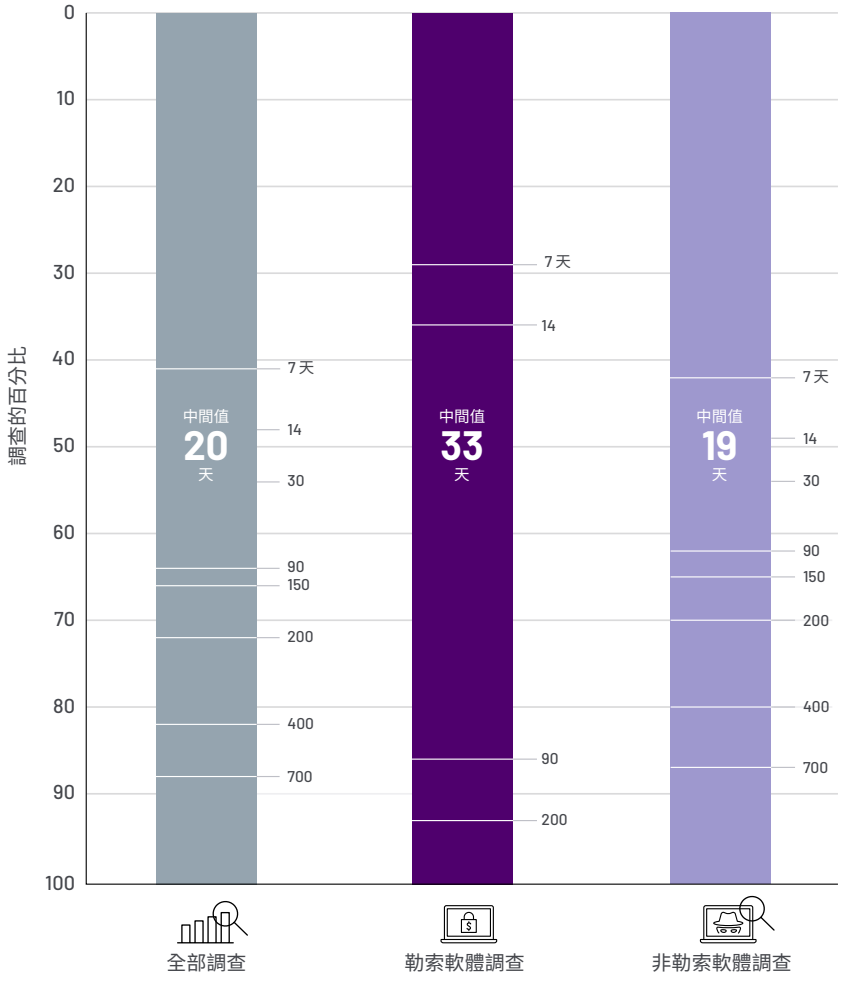
2022 年，Mandiant 發現與勒索軟體相關的 EMEA 調查下降了 10%。此外，Mandiant 指出，2022 年 EMEA 的勒索軟體特定調查的停留時間中間值增加到 33 天，僅從 2021 年上升了四天。這意味著，在 2022 年，利用勒索軟體攻擊 EMEA 組織的對手在被偵測到之前，在被入侵環境中花費的時間要長 89%。然而，2021 年 EMEA 的勒索軟體相關調查停留時間中間值異常短，因此該指標在 2022 年恢復也就不足為奇了。2022 年，外部實體向組織通知勒索軟體事件的速度比組織在內部偵測到事件的速度更快。EMEA 的組織會在勒索軟體相關入侵後 30 天內收到外部實體通知，而當類似入侵是在內部被確認時，對手會在 51 天內不被偵測到。

Mandiant 確實看到非勒索軟體停留時間出現顯著改善。EMEA 的組織偵測非勒索軟體入侵的速度要快三分之二，2022 年的停留時間中間值為 19 天，相比之下 2021 年為 60 天。

EMEA 停留時間中間值（按偵測來源）



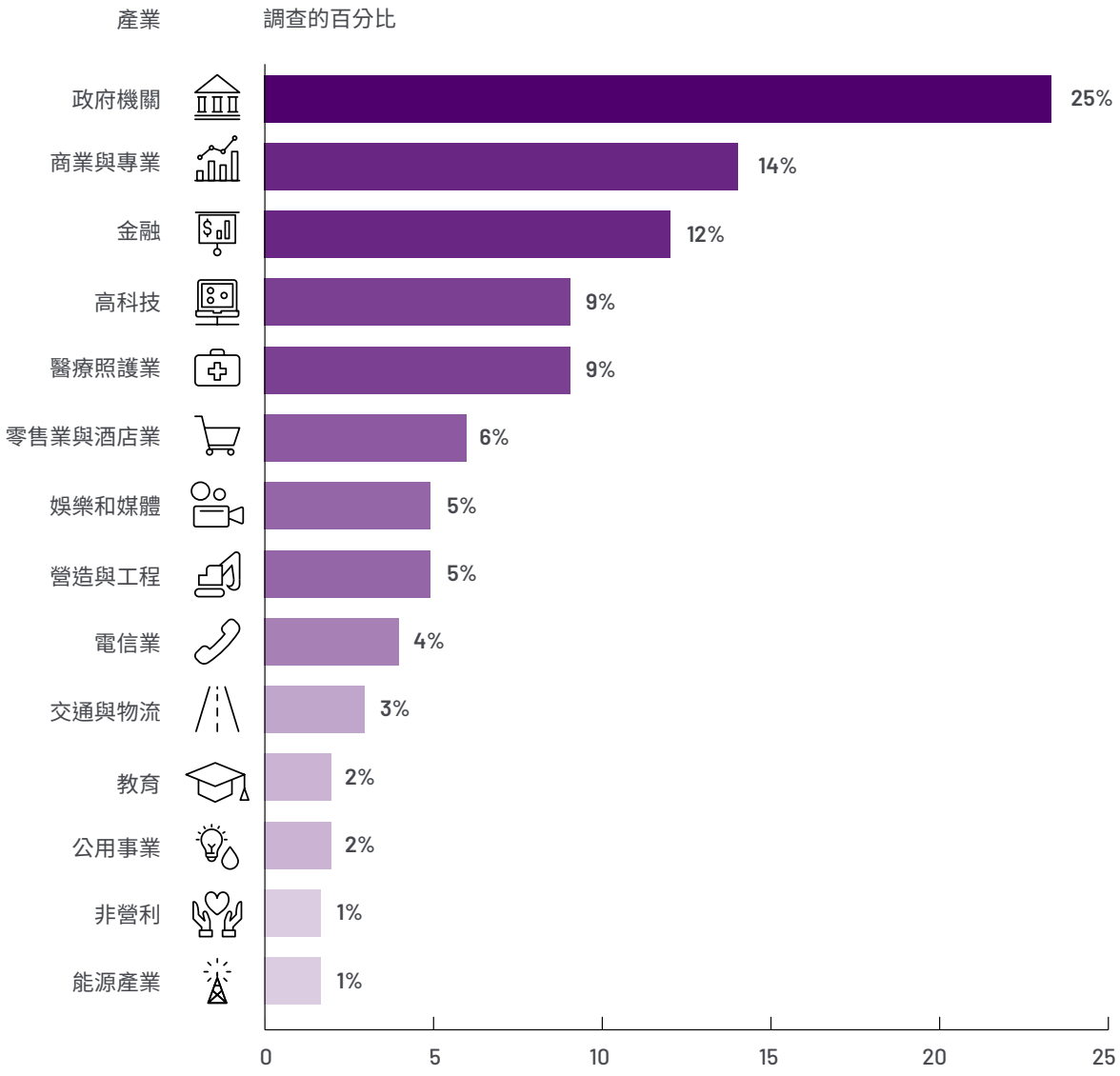
EMEA 停留時間（按調查類型劃分），2022 年



選擇目標產業

在 2022 年 Mandiant 調查的入侵中，政府相關組織的回應工作佔所有調查的四分之一。與 2021 年的 9% 相比，這主要反映了 Mandiant 為支援烏克蘭所做的大量工作。2022 年接下來的四大最被針對產業與 Mandiant 專家在 2021 年觀察到的保持一致。Mandiant 觀察到對手喜歡商業／專業服務、金融、高科技和醫療保健產業。這些產業對以金融和以間諜活動為動機的發動者而言都非常具有吸引力。

2022 年全球產業攻擊目標



針對性攻擊

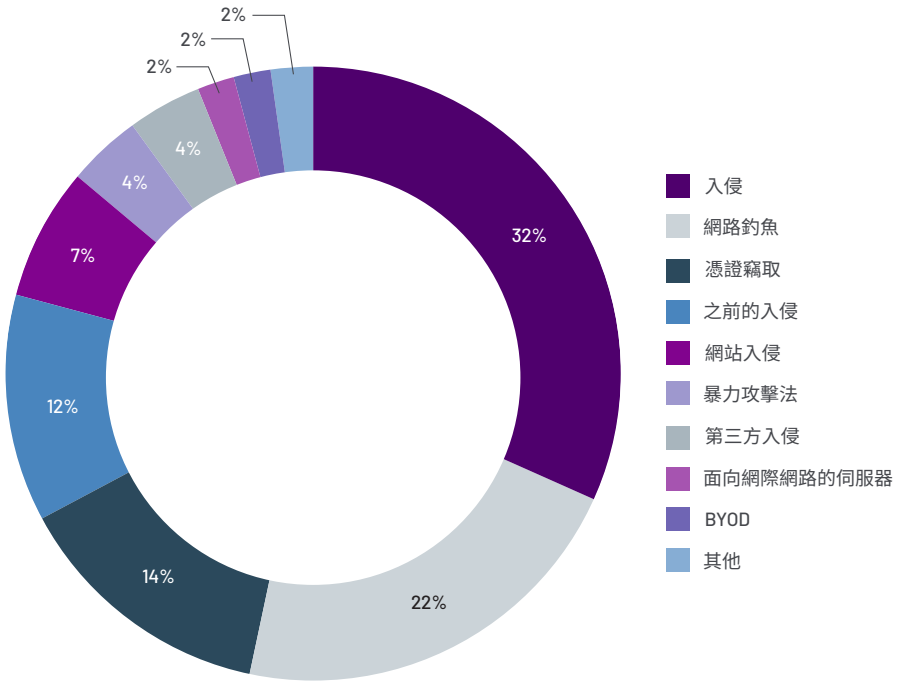
首次感染媒介

在 Mandiant 於 2022 年開展的調查中，漏洞攻擊依舊是對手最常使用的首次感染媒介。在首次感染媒介被確認的入侵中，32% 的入侵都是從漏洞攻擊開始。雖然這與 M-Trends 2022 報告期中確認的 37% 的入侵相比有所降低，但是漏洞攻擊仍是對手用來攻擊其目標的關鍵工具。

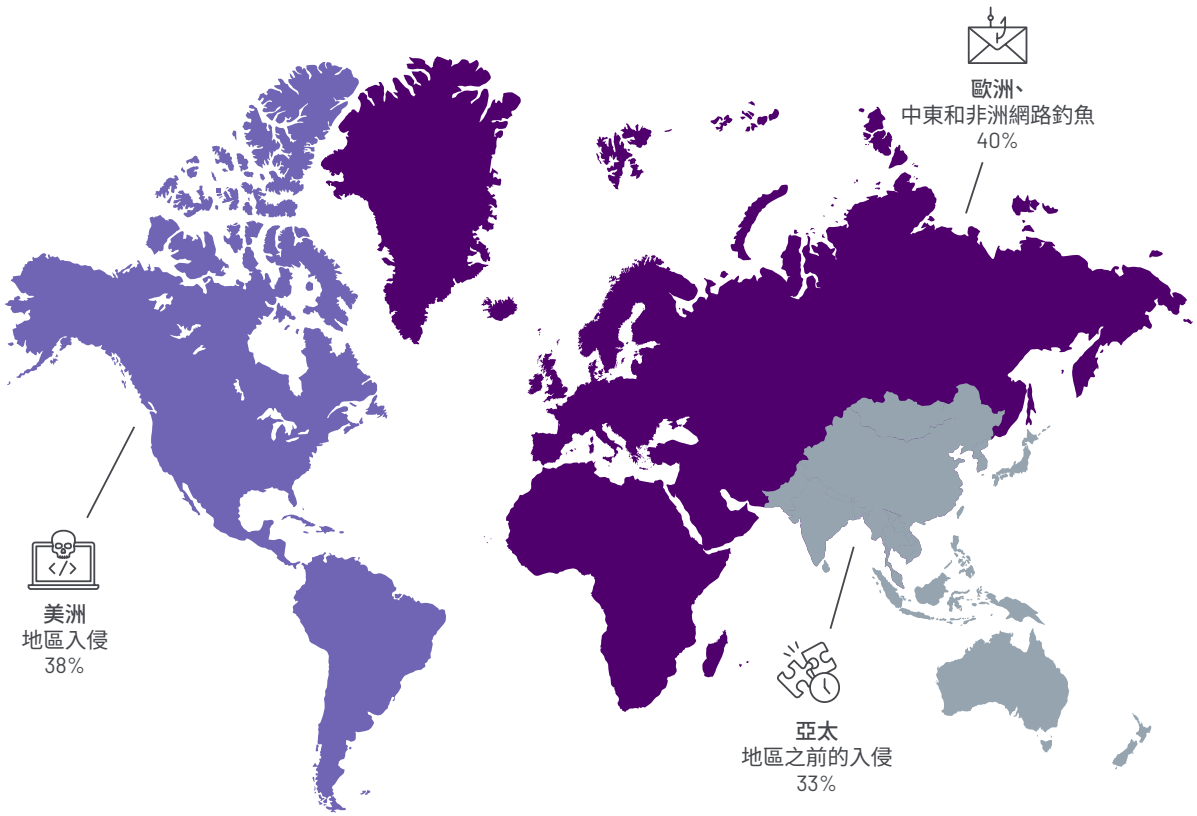
2022 年，網路釣魚重新成為入侵中觀察到的首次感染的第二大最常使用媒介，在首次感染媒介被確認的入侵中佔 22%。這與 2021 年 12% 的入侵相比有所增加。與去年同期相比，網路釣魚依然利潤豐厚，而且是對手的主要媒介。

2022 年，在首次感染媒介被確認的調查中，對手使用憑證竊取的頻率比 2021 年要高，分別為 14% 和 9%。與往年相比，Mandiant 調查發現 2022 年廣泛資訊竊取器惡意軟體和憑證購買的使用均日益普遍。在許多案例中，調查發現憑證有可能是在組織環境之外被竊取，然後用來攻擊組織，可能是因為重複使用的密碼或在公司裝置上使用個人帳戶。

首次感染媒介 (確認時)

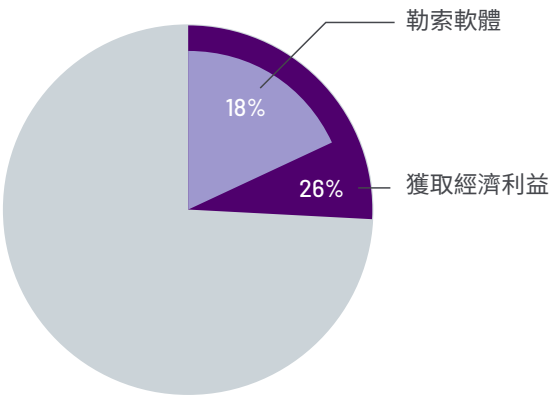


最常見的首次感染媒介（按地區）



從地區上來說，對手利用各種媒介來取得目標群組織存取權並完成其任務。在美洲地區，在首次感染媒介被確認的入侵追蹤，使用漏洞攻擊仍是最常用的媒介，佔調查的 38%。以亞太地區組織為目標的對手使用先前入侵的存取權來執行其入侵的頻率要比使用其他媒介高 10%。在 EMEA，在入侵媒介被確認的調查中，有 40% 的調查中的對手使用了網路釣魚。各地區內使用媒介的多樣化可能表明對手並非使用相同的攻擊路徑來完成其任務。對手繼續使用最有效的入侵媒介來獲得其位於每個區域內的目標存取權限。

對手行動



獲取經濟利益

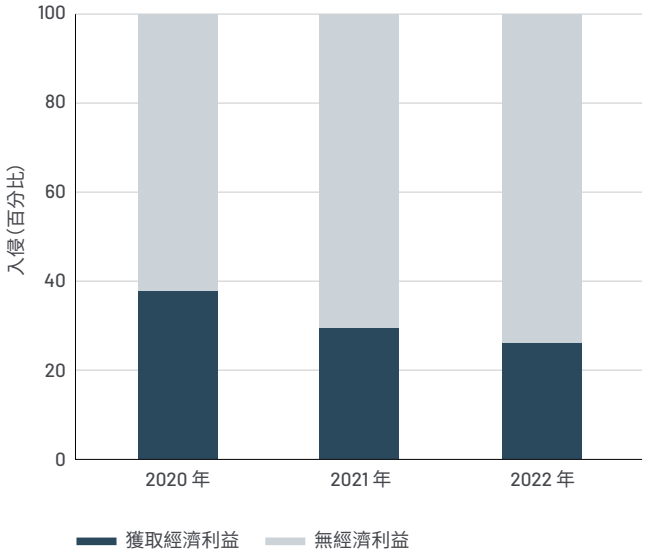
30% → **26%**

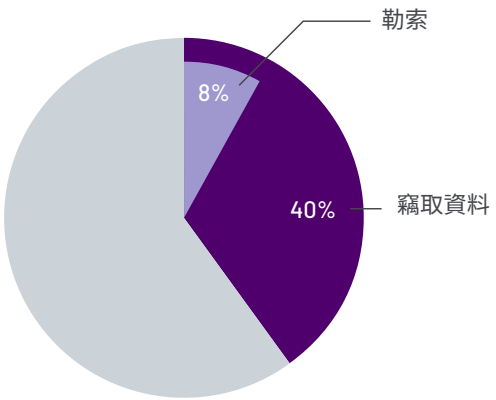
在 2021 年　　在 2022 年

2022 年 確認對手在獲取經濟利益的 Mandiant 調查有所減少。然而，以金融為動機的入侵在 Mandiant 調查的入侵中仍然佔據超過四分之一。在 2022 年的 Mandiant 調查中，26% 的入侵揭示了對手透過勒索、勒索軟體、出售存取權限、非法轉帳及盜竊支付卡來尋求經濟利益。

與 M-Trends 2022 報告期相比，Mandiant 開展的勒索軟體相關調查降低了 5%。2022 年，所有 Mandiant 調查中有 18% 與勒索軟體相關。自 2020 年以來，這是與勒索軟體相關的 Mandiant 調查的最小百分比。

獲取經濟利益，2020-2022 年





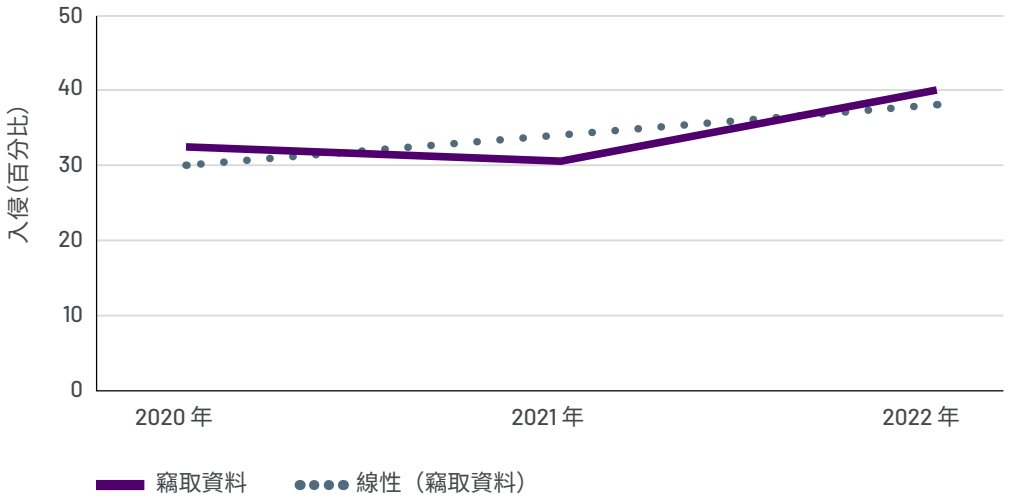
竊取資料

29% → **40%**

在 2021 年　　在 2022 年

2022 年，Mandiant 專家確認在 40% 的入侵中，對手優先使用資料竊取。與往年相比，Mandiant 防禦者觀察到威脅發動者在 2022 年嘗試竊取，或成功完成資料竊取行動的頻率更高。在其中 19% 的入侵（佔所有入侵的 8%）裡，威脅發動者在付款談判期間使用了被竊取的資料。Mandiant 繼續觀察到威脅發動者因眾多目標而執行資料竊取行動。然而，在 22% 的調查中，我們觀察到對手優先使用資料竊取，這可能表明其為智慧財產竊取或間諜活動相關最終目標。觀察到的資料竊取的持續增加有可能表明，組織正在改進其偵測資料竊取行動的能力，從而使調查人員能進行更全面的調查。

觀察到的資料竊取，2020-2022 年



被入侵架構

4% → **6%**

在 2021 年　　在 2022 年

作案手法

Mandiant 專家繼續觀察到，投機入侵被用作針對性攻擊活動之來源的情況略有上升。在某些情況下，大規模非針對性活動已經轉化成針對性攻擊活動，因為被入侵環境的存取權限被出售給針對性威脅發動者，或在攻擊期間收集到的關鍵資訊被用來完成針對性攻擊者的目標。

2022 年，Mandiant 專家在 6% 的入侵中確認了這種活動，相比之下 2021 年和 2020 年分別為 4% 和 3%。隨著漏洞攻擊的使用繼續增加，被入侵架構的使用也在增加也就不足為奇了。隨著概念驗證 (POC) 程式碼可用於新確認的漏洞攻擊，使入侵自動化的能力也增加了。從 POC 到大範圍攻擊之間較短的週期使發動者能夠速戰速決，這反過來又能為額外的非針對性攻擊提供必要的基礎設施。

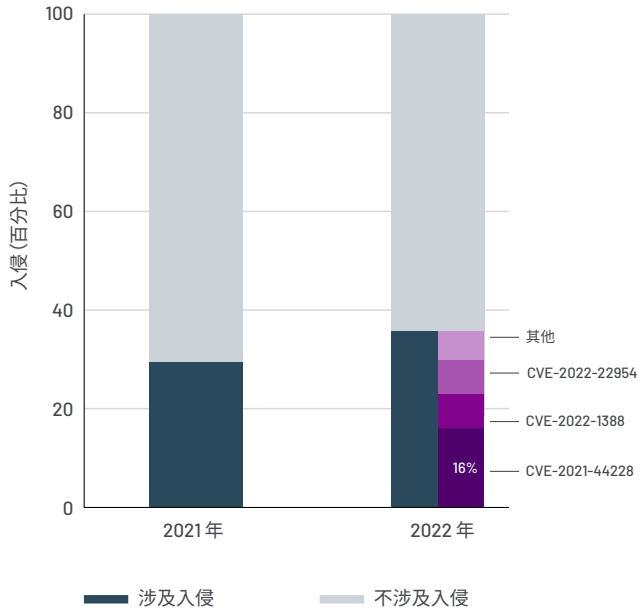
在觀察到被入侵架構的 Mandiant 調查中，大約 60% 的入侵導致了某些類型的加密貨幣挖掘活動。而在剩餘將近 40% 的入侵中，該架構被用於額外行動，包括持續的垃圾郵件和／或網路釣魚行動，以及進一步分發殭屍網路。與往年相似，與內部人員威脅相關的入侵在 2022 年的 Mandiant 調查中佔 1%。

2022 年漏洞攻擊活動

對手仍在使用漏洞攻擊來開展其行動。2022 年，Mandiant 在 36% 的調查中觀察到至少有一次漏洞攻擊的成功漏洞攻擊活動，相比之下 2021 年為 30% 的調查。Mandiant 繼續觀察到對手利用漏洞攻擊來發起和繼續入侵。可以透過網際網路存取的週邊裝置，包括防火牆、虛擬化解決方案及虛擬私人網路裝置，仍為備受追捧的攻擊目標。

在以漏洞為目標的所有調查中，濫用 Log4j[1] 漏洞佔 16% 的調查。所確認的第二和第三最值得注意的漏洞與 F5 Big-IP[2] 和 VMware Workspace ONE Access 及身分管理員 [3] 有關。

確認時的漏洞攻擊活動



確認了多個威脅組織（每個環境）

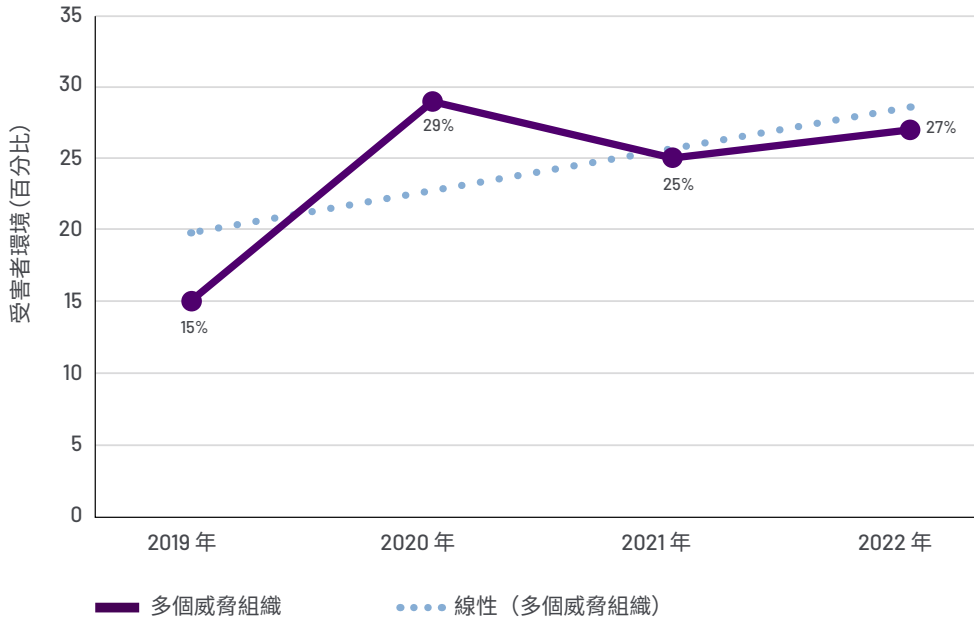
25% → **27%**

在 2021 年　　在 2022 年

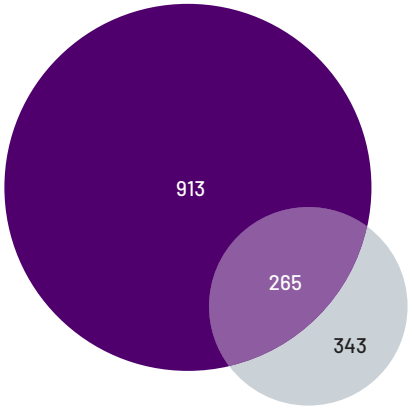
環境

在超過四分之一的調查中，Mandiant 專家在相同的環境內確認了多個威脅組織。在這些調查期間，Mandiant 觀察到有威脅組織合作完成中心目標，以及多個威脅組織獨立被目標環境吸引的例項。2022 年，多個威脅發動者被確認的調查百分比增加到與 2020 年觀察到的類似百分比水平。這種趨勢仍然不穩定，然而 Mandiant 觀察到過去四年內在相同的環境中確認的多個威脅組織普遍有所增加。

確認了多個威脅組織



威脅組織



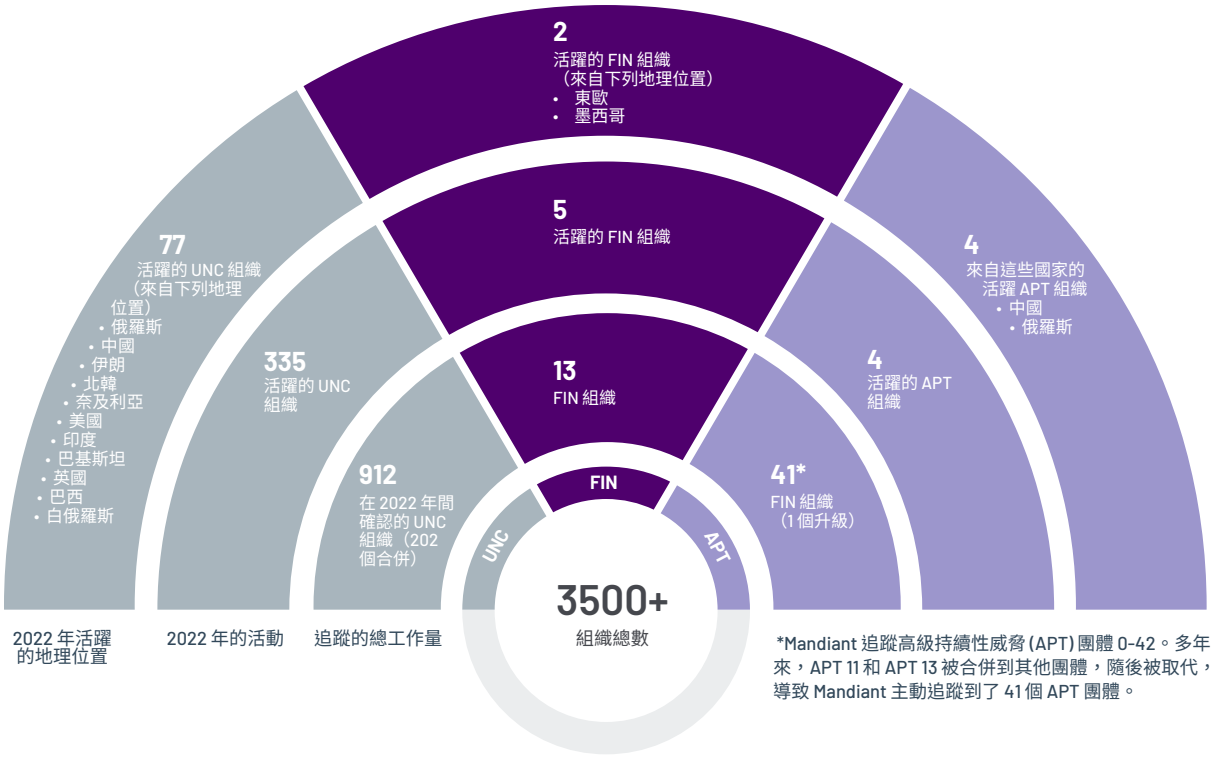
新追蹤到的威脅集團

新追蹤和觀察到的威脅集團

觀察到的威脅集團

Mandiant 專家追蹤了 3500 多個威脅組織，其中包括在 M-Trends 報告期間新追蹤的 900 多個威脅組織。在這些新追蹤的組織中，有 265 個威脅組織是在 2022 年 Mandiant 調查期間首次確認的。Mandiant 在 2022 年的所有入侵中確認了共計 343 個獨特的威脅組織。組織面臨著四個已命名進階持續性威脅 (APT) 組織的入侵。這包括中國和俄羅斯政府資助的組織、五個以經濟為動機的威脅 (FIN) 組織，以及 335 個未分類的威脅 (UNC) 組織。總體上，組織仍在面臨和回應成熟的威脅組織，同時也在應對新歸因的組織。

2022 年的威脅團體



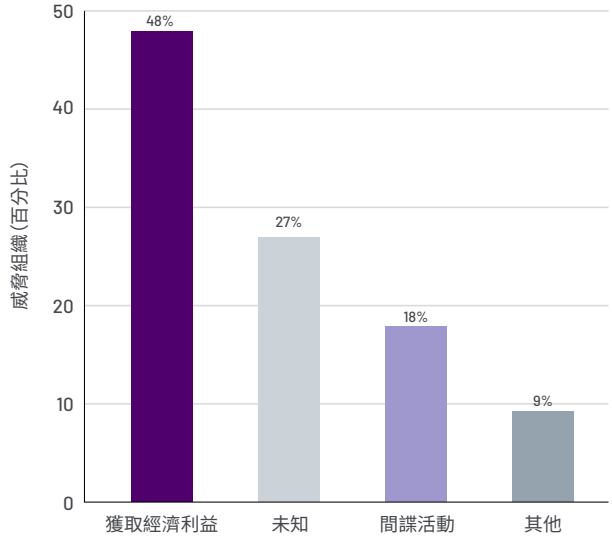
*Mandiant 追蹤高級持續性威脅 (APT) 團體 0-42。多年來，APT 11 和 APT 13 被合併到其他團體，隨後被取代，導致 Mandiant 主動追蹤到了 41 個 APT 團體。

破壞性行動 —— 威脅組織的評估目標是破壞或損壞目標的基礎設施，比如 DDoS 或破壞性 ICS 攻擊。

駭客入侵 —— 威脅組織的評估目標是損害名譽、獲得媒體報導和／或影響政策。

製造麻煩 —— 威脅組織的評估目標是獲取存取權限和透過受害環境傳播，比如殭屍網路與垃圾郵件。

觀察到的威脅集團（按目標劃分），2022 年

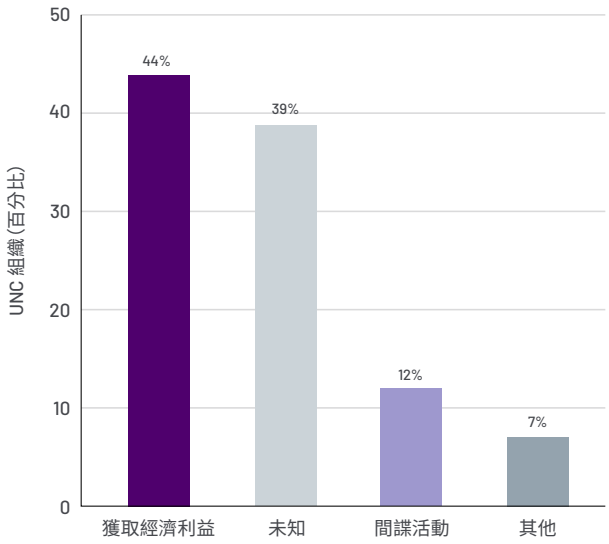


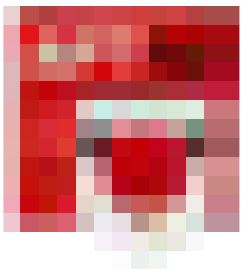
這些威脅組織是包含人工製品在內的威脅組織叢集，比如對手基礎設施、工具及間諜情報技術。在威脅組織首次被建立時，Mandiant 會評估該組織的首要目標。隨著我我們對威脅組織的知識變得足夠成熟，深入的研究有助於根據既定的 Mandiant 命名慣例來指派正式的名稱。

在 2022 年觀察到的所有威脅組織中，Mandiant 評估這些威脅組織中有 48% 具有以金融為動機的行動，18% 具有與間諜活動有關的動機，還有 9% 具有其他動機，比如破壞性行動、駭客入侵及製造麻煩。在剩餘 27% 的威脅組織中，動機無法評估。這通常是因為對手在他們能夠完成其任務之前就被發現了，或者沒有發現直接證據來建立可信的目標。

在 2022 年的活躍組織中，Mandiant 追蹤為未分類 (UNC) 組織的威脅組織裡有 335 個在入侵中被觀察到。Mandiant 評估表明這些威脅組織中有 44% 是以獲取經濟利益為動機，有 12% 是以間諜活動相關行動為動機。尤其是，這些 UNC 組織可能有不止一個動機。為了不斷完善我們對這些威脅組織及其活動的理解，Mandiant 不斷分析來自前線調查的對手行動，以便在所有 Mandiant 產品與服務中產生和整合可行情報。透過這項工作，以及對公開報告、資訊分享及其他研究的分析，Mandiant 繼續透過持續的聚類與合併來擴大其威脅發動者知識庫。

觀察到的威脅集團 (按目標劃分)，2022 年





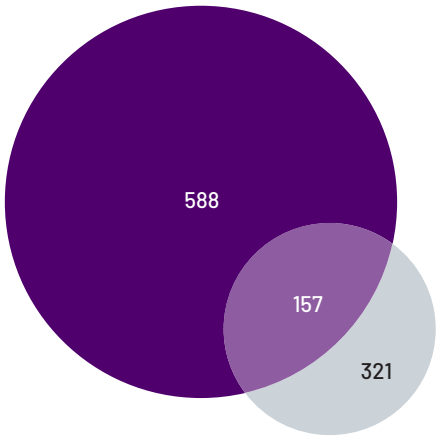
2022 年，Mandiant 基於對活動重疊的大量研究，把一個組織升級為一個命名的威脅組織 APT42，併將 202 個威脅組織合並入其他威脅組織。如需關於 Mandiant 如何定義和引用 UNC 組織和合併的詳細資訊，請參見「Mandiant 如何追蹤未分類的威脅發動者。[4]」

惡意軟體

惡意程式碼系列是一個程式或成員間有足夠的「程式碼重疊」的一組程式，FireEye 視其為同一種東西，即「系列」。「系列」一詞擴大了單一惡意軟體的範圍，因為它可以隨著時間的變化而變化，這反過來又會創造新的，但從根本上而言又是重疊的惡意軟體。

2022 年，Mandiant 開始追蹤 588 個新的惡意程式碼系列，以增加其惡意軟體知識庫。與涵蓋 15 個月的 M-Trends 2022 報告期中報告的 700 多個新追蹤的惡意軟體相比，Mandiant 在 2022 年新追蹤的惡意軟體相當於每個月確認大約 49 個新的惡意程式碼系列，相比之下 2021 年為每個月 45 個新的系列。這可能表明對手正在繼續以類似於往年的速度擴大其工具組。

在這些新的惡意程式碼系列追蹤，有 157 個系列是在 Mandiant 調查的入侵追蹤被觀察到。這在 Mandiant 調查中的惡意程式碼系列總數（321 個）中僅佔略少於一半。這表明，雖然對手在繼續部署新工具，但之前觀察到的惡意程式碼系列仍在其軍火庫中佔據很大一部分。



新追蹤到的惡意程式碼系列

新追蹤和觀察到的惡意程式碼系列

觀察到的惡意程式碼系列

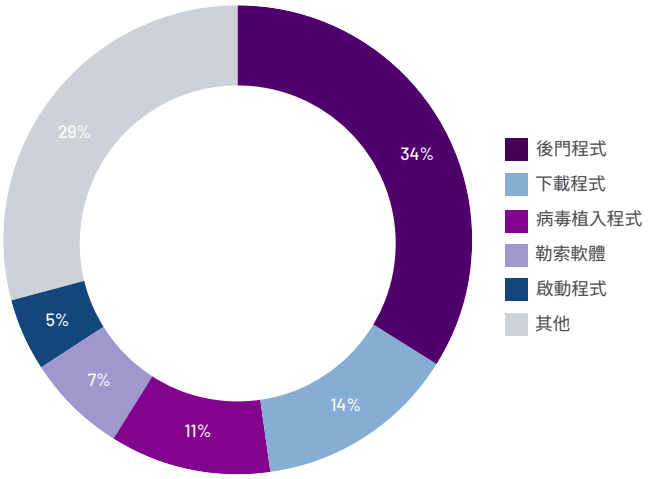
惡意軟體類別描述一個惡意程式碼系列的主要目標。每個惡意程式碼系列都只會分配一個最能描述其主要目的的類別，無論其功能是否不止適合一個類別。

新的惡意程式碼系列 (按類別劃分)

在新追蹤到的 588 個惡意程式碼系列中，前五大類別分別是後門(34%)、下載程式(14%)、植入程式(11%)、勒索軟體(7%)以及啟動程式(5%)。這些類別的惡意軟體在過去幾年裡保持一致，而後門繼續在新追蹤的惡意程式碼系列中佔據略微超過三分之一的比例。2022 年，新追蹤的憑證竊取器跌出 Mandiant 追蹤的前五大類別。考慮到被竊取憑證是首次出現在最常見的入侵媒介中，這似乎表明威脅發動者正在使用之前建立的憑證竊取器來獲取被竊取的憑證。

惡意軟體類別	主要目的
後門程式	該程式的主要目的是讓威脅發動者能互動式地向安裝了該程式的系統發出命令。
認證竊取器	該公用程式的主要目的是存取、複製或竊取身分驗證認證。
下載程式	該程式的唯一目的是從特定地址下載（也許還會啟動）一個檔案，並且不會提供任何額外的功能或支援任何其他互動式命令。
病毒植入程式	該程式的主要目的是擷取、安裝並可能會啟動或執行一個或多個檔。
啟動程式	該程式的主要目的是啟動一個和多個檔案。與植入程式或安裝程式的區別之處在於它不包含或不會對檔案進行配置，只是會執行或載入檔案。
勒索軟體	該程式的主要目的是執行一些惡意操作（如加密資料），其目標為牟取受害者付款，以避免或撤銷惡意操作。
隧道程式	代理或通道網路流量的程式。
其他	包括所有其他惡意軟體類別，如公用程式、鍵盤記錄器、銷售點(POS)、隧道器和資料採擷器。

最新追蹤到的惡意程式碼系列 (按類別劃分)，2022 年

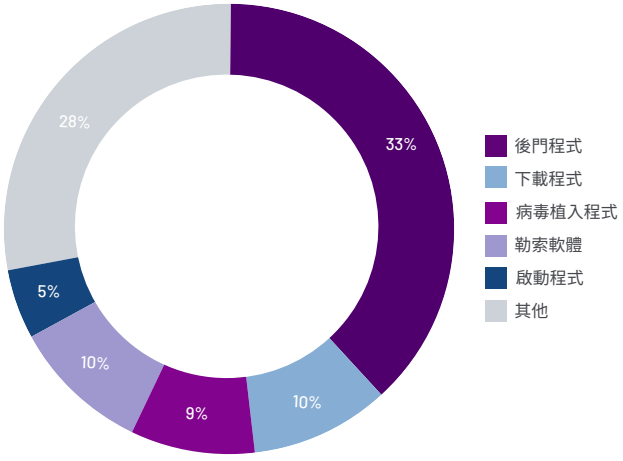


觀察到的惡意程式碼系列是 Mandiant 專家調查期間確認的惡意程式碼系列

觀察到的惡意程式碼系列 (按類別劃分)

在 2022 年中，Mandiant 專家在入侵中觀察到 321 個獨特的惡意程式碼系列。後門程式仍是主要的威脅組織，威脅發動者在 33% 的 Mandiant 調查中使用具備後門程式功能的惡意軟體。相比於 2021 年，這個資料降低了 7%，然而與下一個最常見的功能類型相比，具備後門程式功能的惡意程式碼系列仍在更多的調查中被觀察到。接下來的類別與 2021 年相比在順序上存在微小變化，前五位的剩餘類別為下載程式 (10%)、勒索軟體 (10%)、植入程式 (9%) 以及啟動程式 (5%)。

觀察到的惡意程式碼系列 (按類別劃分)，2022 年



後門程式

40% → **33%**

在 2021 年　在 2022 年

勒索軟體

10% → **10%**

在 2021 年　在 2022 年

啟動程式

4% → **5%**

在 2021 年　在 2022 年

其他

22% → **28%**

在 2021 年　在 2022 年

下載程式

7% → **10%**

在 2021 年　在 2022 年

病毒植入程式

12% → **9%**

在 2021 年　在 2022 年

隧道程式

4% → **5%**

在 2021 年　在 2022 年

在 2021 和 2022 年間的調查中，獨特的勒索軟體系列的使用仍然相對穩定。雖然勒索軟體入侵的百分比有所減少，但是對手仍在使用類似百分比的不同勒索軟體惡意程式碼系列來為獲取經濟利益而執行其任務。

與 2021 年觀察到的調查的 7% 相比，2022 年獨特的下載程式的使用增加了 3%。與此同時，獨特的植入程式的使用也減少了相同的數量，從 2021 年觀察到的 12% 減少到 2022 年觀察到的 9%。提供通道功能的獨特惡意軟體的使用（從 4% 增加）也可能是導致各種任務追蹤獨特的植入程式和後門程式減少的一個因素。

尤其是，憑證竊取器跌出了 2022 年前五大觀察到的惡意程式碼系列（按類別劃分）清單，儘管憑證竊取的使用出現在五大首次感染媒介中。然而，Mandiant 觀察到憑證和資訊竊取器類型惡意軟體暴增，比如透過濫用搜尋引擎最佳化 (SEO) 和惡意廣告提供的 RECORDSTEALER、VIDAR 和 RECORDSTEALER 等等。Mandiant 還觀察到其他類型的惡意軟體的使用可能表明對手在用於完成任務的工具使用上變得更加靈活。

RECORDSTEALER，亦稱為 Raccoon Stealer V2 (Sekoia)、Record Stealer (AhnLab) 和 RecordBreaker (Proofpoint)，是以 C 語言編寫的憑證竊取器，能從常見網頁瀏覽器、加密貨幣錢包獲取敏感性資料，並配置稱下載程式。

REDLINESTEALER，亦稱為 RedLine (Minerva Labs and Proofpoint) 和 Redlinestealer (Fortinet)，是一種憑證竊取器惡意軟體，能夠從網頁瀏覽器、檔案、FTP 應用程式及加密貨幣錢包竊取憑證。它還能收集廣泛的系統調查資訊，比如基礎硬體規格、桌面螢幕快照、使用者名稱、操作系統、語言、地理位置、安裝的軟體、程序清單及全球 IP 位址。惡意軟體可以下載並啟動額外的有效負載或為攻擊者啟動隱藏的命令 Shell。Redline Stealer 一直在駭客論壇上打廣告供出售。

VIDAR，亦稱為 Mosaicloader (Bitdefender)，是以 C++ 語言編寫的資料挖掘程式，以來自多個網頁瀏覽器、加密貨幣錢包、聊天軟體、Authy 雙因素身分驗證公用程式及各種其他應用程式的資料為目標。所收集的資料被壓縮並使用 HTTP 上傳到遠端伺服器。VIDAR 似乎是以一個名為 ARKEI 的類似資料挖掘程式為基礎。

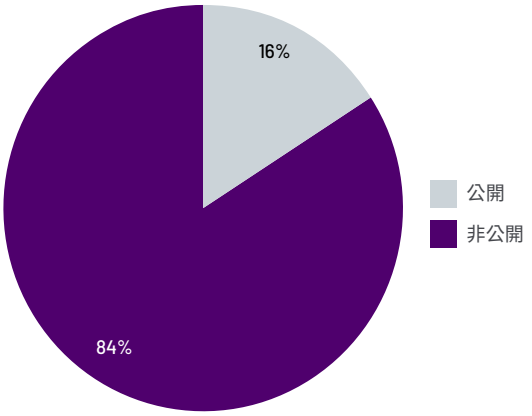
公開可用的工具或程式碼系列很容易獲取，沒有限制。這包括可以在網際網路上自由獲取的工具，以及出售或購買的工具，只要能被任何買家購買的工具都屬於該範疇。

非公開工具或程式碼系列，據我們所知，是無法公開獲取的（免費或出售）。它們可能包括私人開發、持有或使用的工具，以及在受限制的客戶群體中共用或出售的工具。

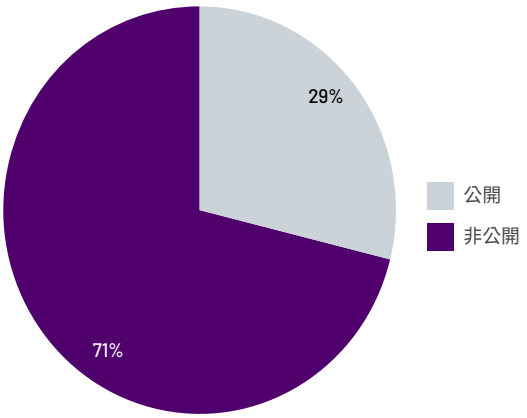
惡意軟體（按可用性劃分）

新追蹤和觀察到的惡意程式碼系列的可用性仍然每年都保持相對一致。在兩個類別追蹤，惡意程式碼系列往往是私人開發的，或者可用性有限。Mandiant 注意到，入侵期間使用的惡意程式碼系列有 29% 是公開可用的，與 2021 年的 28% 相比增加了 1%。雖然對手繼續使用各種非公開可用的惡意軟體，並根據目標環境開發惡意軟體來實現其目標，但是許多對手還在繼續使用相同的公開可用惡意程式碼系列（例如 BEACON）。

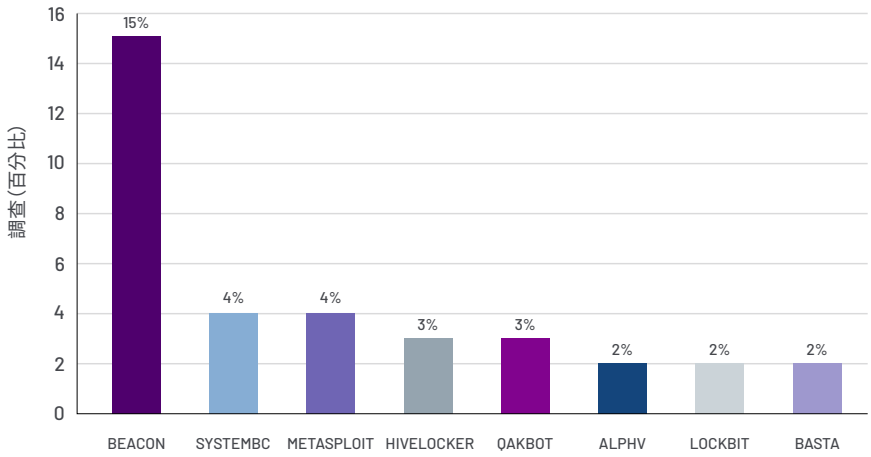
新追蹤的惡意程式碼系列（按可用性劃分），2022 年



觀察到的惡意程式碼系列（按可用性劃分），2022 年



2022 年最常見的惡意程式碼系列



與往年一致，Mandiant 在調查中確認的最常見惡意程式碼系列為 BEACON。Mandiant 調查的所有入侵中有 15% 確認了 BEACON，目前為止仍是各區域內調查中最常見的。它已經被 Mandiant 追蹤的各種威脅組織使用，包括歸因於中國、俄羅斯和伊朗的國家支援威脅組織，以及包括 FIN6、FIN7、FIN9、FIN11 和 FIN12 及超過 700 個 UNC 組織在內的以金融為動機的威脅組織。這種普遍性可能是由 BEACON 的普遍可用性，加上惡意軟體的高可定制性和易用性造成的。

雖然 2022 年 BEACON 的整體使用情況仍然最值得注意，但是使用情況與 2021 年相比下降了 10%，使之成為近年來觀察到的最小百分比的 BEACON 活動。在 2021 年和 2020 年的所有入侵中，BEACON 的使用分別佔所有入侵的 28% 和 24%。

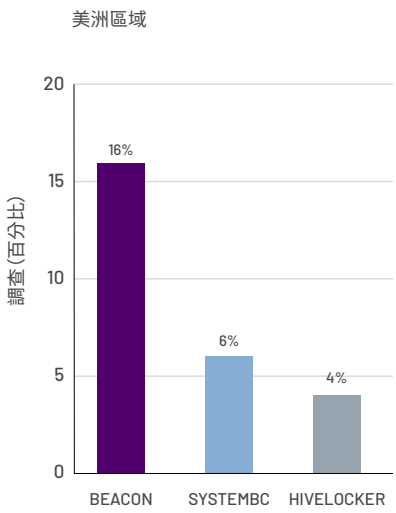
觀察到的第二和第三最常見惡意程式碼系列為 SYSTEMBC 和 METASPLOIT。這些惡意程式碼系列為對手提供了類似於 BEACON 的功能，然而功能具有各種限制。2022 年，作為隧道程式的惡意軟體使用有所增加。這可能反映了 SYSTEMBC 等惡意軟體使用的增加，部署勒索軟體的發動者大量使用這種惡意軟體。2022 年，Mandiant 觀察到四個不同的惡意程式碼系列對組織構成了巨大的威脅。Mandiant 觀察到 HIVELOCKER、ALPHAV、LOCKBIT 和 BASTA 等惡意程式碼系列構成了大部分的勒索軟體相關入侵。

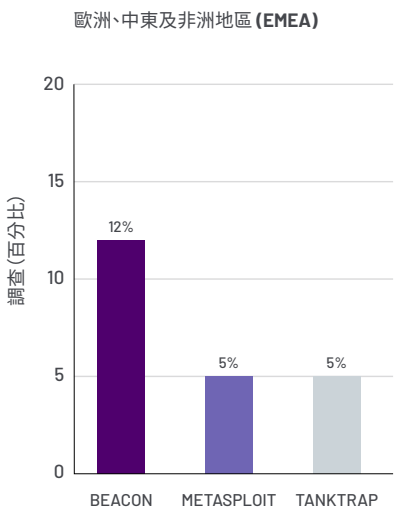
雖然勒索軟體相關入侵有所減少，但是 Mandiant 還觀察到，與 2021 年相比，2022 年新增到與所追蹤勒索軟體系列相關的資料洩露分享網站普遍減少。在最常見和最具破壞性的勒索軟體系列中，Mandiant 觀察到，新增到 LOCKBIT、ALPHV、BASTA、CONTI 和 HIVELOCKER 等勒索軟體系列相關的勒索軟體資料洩露網站的組織減少了將近 10%。

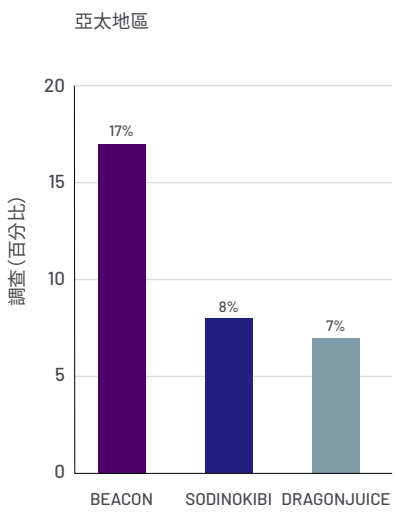
2022 年，Mandiant 觀察到 LOCKBIT 資料洩露分享網站與 2021 年的貼文相比發生了最大的變化。Mandiant 還評估，隨著 CONTI 組織在 2022 年初中斷，原關聯組織開始使用其他勒索軟體系列，如 BASTA、ROYALLOCKER 和 HIVELOCKER 來執行其行動。這可能解釋了與 2021 年相比，2022 年使用的勒索軟體系列種類更多的原因。

區域詳細分解

雖然 BEACON 是所有區域內最常見的惡意程式碼系列，但下一個最熱門的惡意程式碼系列因區域而異。在美洲地區，SYSTEMBC 和跨平台 HIVELOCKER 勒索軟體是 BEACON 之後出現頻率最高的。在亞太地區，SODINOKIBI 勒索軟體和事前勘查工具 DRAGONJUICE 是最常見的。在 EMEA，METASPLOIT 和 PowerShell 公用程式 TANKTRAP 也在前三之列。多年來，隨著對手逐步專營其任務，Mandianat 觀察到常見惡意程式碼系列的區域差異加大。







惡意軟體定義

BEACON 惡意軟體是一個商用後門程式，是 Cobalt Strike 軟體平台的一部分，通常用於對網路環境進行滲透測試。該惡意軟體支援好幾種功能，如注入和執行任意程式碼、上傳和下載檔案，以及執行 shell 命令。Mandiant 已發現許多已命名威脅團體使用過 BEACON，包括 APT19、APT32、APT40、APT41、FIN6、FIN7、FIN9、FIN11、FIN12 和 FIN13，以及超過 750 個 UNC 組織。

SYSTEMBC 是一個用 C 語言編寫的隧道程式，它使用基於 TCP 的自訂二進位通訊協定從 C2 伺服器擷取與代理相關的命令。C2 伺服器指示 SYSTEMBC 充當 C2 伺服器和遠端系統之間的代理。SYSTEMBC 還能夠透過 HTTP 擷取其他承載。某些變體可能會將 Tor 網路用於此目的。下載的承載可在執行前被寫入磁碟或直接對應到記憶體中。SYSTEMBC 通常用於隱藏與其他惡意程式碼系列相關的網路流量。觀察到的軟體系列包括 DANABOT、SMOKELOADER 和 URSNIF。Mandiant 發現 FIN12 和超過 20 個 UNC 組織在使用 SYSTEMBC，其目標與經濟利益相關。

METASPLOIT 是個滲透測試平台，使用者可以在平台上發現、利用及驗證漏洞。Mandiant 已發現 APT28、APT35、APT40、APT41、FIN6、FIN7、FIN11、FIN12、FIN13 和 152 個 UNC 組織使用過 METASPLOIT，其最終目標從間諜活動和經濟利益到滲透測試等。

HIVELOCKER 是一個影響 Windows 和 Linux 作業系統的勒索軟體系列。它最初是在 GoLang 中編寫的，但在 2022 年初用 Rust 重新編寫。它可以加密邏輯磁碟和遠端網路共用。在執行時，該勒索軟體將解析指定其行為的命令列參數，比如在加密前要終止的程序和要停止的服務。HIVELOCKER 能夠基於加密程序期間命令列參數中指定的檔案大小、檔案名稱或檔案副檔名來跳過檔案。Mandiant 追蹤超過 15 個 UNC 組織與 HIVELOCKER 勒索軟體的分發或使用相關聯。

QAKBOT 是用 C/C++ 語言編寫的後門程式，它會執行外掛程式框架，透過能提供鍵盤記錄、檔案傳輸和檔案執行等功能的嵌入式可下載外掛程式來延伸其功能。QAKBOT 還透過攔截瀏覽器活動、向瀏覽器工作階段注入惡意程式碼，以及擷取瀏覽器、電子郵件用戶端和 FTP 用戶端儲存的憑證來鎖定憑證。QAKBOT 能夠透過 SMB 傳播到網路上的其他系統，並透過 UPnP 通訊協定在連接的路由器上設定埠轉寄。Mandiant 發現超過 20 個 UNC 組織使用過 QAKBOT，包括為 BASTA 勒索軟體的使用提供存取的分發叢集。

惡意程式碼系列的**作業系統有效性**是可以在上面使用惡意軟體的作業系統。

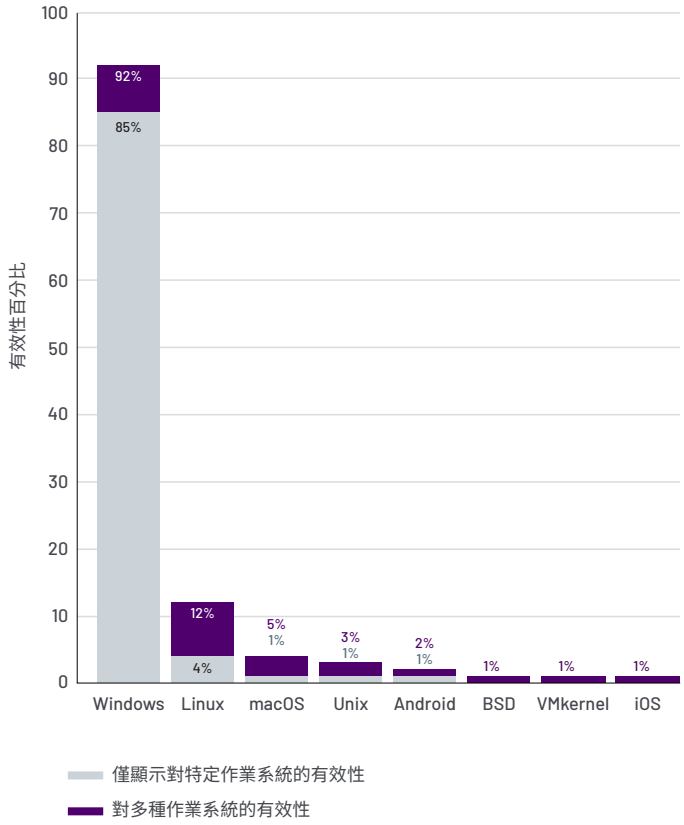
作業系統有效性

根據之前的 M-Trends 報告，在 Windows 上有效的惡意軟體是目前為止最常見的新追蹤和觀察到的惡意軟體，其中有 92% 新確認的惡意程式碼系列和 93% 觀察到的惡意軟體能夠在 Windows 上執行。與 2021 年相比，Mandiant 在 2022 年觀察到 Linux 平台上有效的新追蹤惡意軟體的使用相對穩定，觀察到的惡意軟體有略微減少，觀察到的惡意軟體中有 15% 在 Linux 上有效，相比之下 2021 年為 18%。

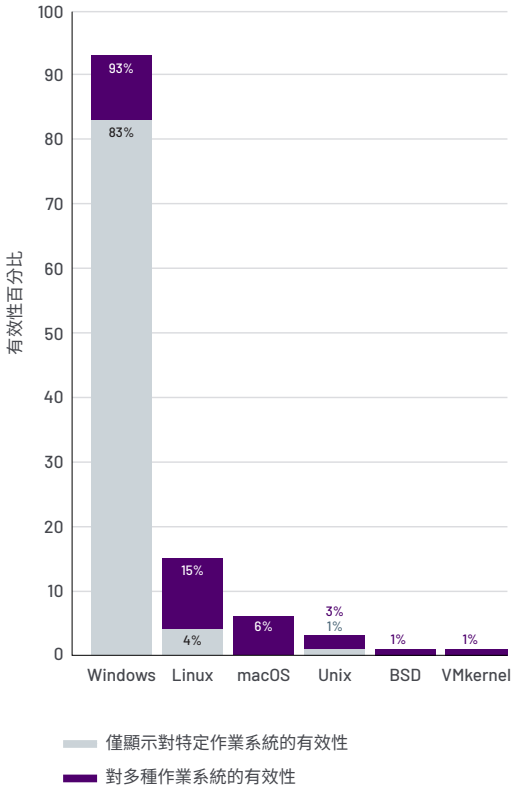
同樣地，與往年相比，Mandiant 觀察到對手使用在一種或更多作業系統上有效的惡意軟體的頻率比使用旨在專注於一種作業系統的惡意軟體更高。在惡意軟體僅在一種作業系統上有效的例項中，它可能會針對 Windows 作業系統。

今年是 Mandiant 首次強調在 VMWare 建立的作業系統 VMkernel 上有效的惡意軟體。雖然在該作業系統上有效的惡意軟體總體數量並不高，但由於 VMWare 架構，特別是 ESXi 主機的盛行，這對防禦者而言是值得注意的。這些類型的作業系統不具有端點偵測和回應 (EDR) 工具監控的強大功能。因此，對平台的監控和調查對防禦者而言充滿挑戰 。

2022 年新追蹤到的惡意程式碼系列的作業系統有效性



2022 年觀察到的惡意程式碼系列的作業系統有效性



威脅技術

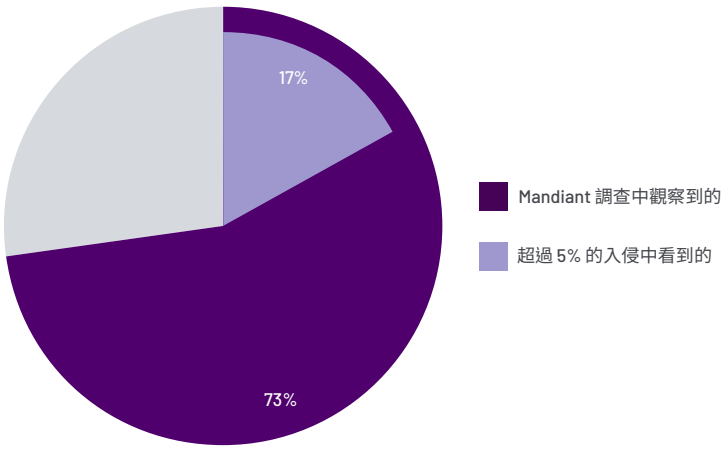
MITRE ATT&CK® 是個可以公開存取的對手戰術與技術知識庫，以現實生活中的觀察結果為基礎。在私營部門、政府及網路安全產品與服務社區內，ATT&CK 知識庫被用作特定威脅模型與方法的開發基礎。

Mandiant 繼續將其調查結果對應到 MITRE ATT&CK 架構，以支援社群。組織應該基於入侵期間使用的特定技術之可能性來優先考慮要實施的安全措施。Mandiant 將 150 項額外的 Mandiant 技術對應到更新後的 MITRE ATT&CK 架構中，使得與 ATT&CK 框架相關的 Mandiant 技術與後續發現總共達到 2300 多項。2022 年，MITRE ATT&CK 框架更新至 12 版本，導致企業版 ATT&CK 現在包含 193 項技術和 401 項子技術。

Mandiant 提供了關於最常觀察到的技術的指標，觀察到的對手在決定如何進一步改善其偵測能力時會使用這些技術作為組織資源。優先處理最常用技術的偵測可以幫助組織在打造更強大的資安生態系統途中奠定堅實基礎。

2022 年，Mandiant 觀察到調查中有 73% 的 MITRE ATT&CK 技術，相比之下，上一個 M-Trends 報告期為 70% 的技術。2022 年，觀察到的 71% 的技術（所有技術的 17%）出現在 5% 以上的入侵中，而 2021 年觀察到的技術有 43%（所有技術的 30%）。這種對手常用技術的結合強調了從優先實施安全措施到防止最常用的技術在內的防禦值。只有少量的技術具有較高普遍性，觀察到的技術中只有 4.3%（所有技術的 1%）出現在超過 30% 的入侵中。值得注意的是，頻率最高的技術與 Mandiant 在 2021 年觀察到的情況保持一致，表明偵測和減少其使用的工作具有持久的防禦者價值。

2022 年最常用的 MITRE ATT&CK 技術



在 Mandiant 於 2022 年開展的一半調查中，對手使用命令或指令碼語言解譯器來進一步推進入侵 (T1059)，其中有 65% 的案例（所有入侵的三分之一）涉事使用 PowerShell (T1059.001)。Mandiant 還繼續觀察到 Web 通訊協定 (T1071.001) 和遠端桌面 (T1021.001) 在各種入侵中的頻繁使用，這表明對手繼續在其行動中嚴重依賴組織現有的技術。這些子技術在過去三年裡一直位於前五之列。然而，這可能表明對這些技術的偵測在不斷改進，並且已經優先考慮其他證據來源來擷取額外技術的證據。

10 大最常見的技術

1.	T1059：命令與指令碼語言解譯器	**50.9%**
2.	T1027：混淆檔案或資訊	**43.5%**
3.	T1071：應用程式層通訊協定	**33.1%**
4.	T1082：系統資訊發現	**31.6%**
5.	T1070：指標移除	**31.5%**
6.	T1083：檔案和目錄發現	**29.5%**
7.	T1140：反混淆／解碼檔案或資訊	**27.3%**
8.	T1021：遠端服務	**26.4%**
9.	T1105：輸入工具轉送	**24.9%**
10.	T1543：建立或修改系統處理序	**24.7%**

最常見的 5 種子技術

1.	T1059.001：PowerShell	**33.2%**
2.	T1070.004：檔案刪除	**25.2%**
3.	T1071.001：Web 通訊協定	**24.3%**
4.	T1569.002：服務執行	**21.8%**
5.	T1021.001：遠端桌面通訊協定	**20.3%**

與 MANDIANT 針對性攻擊生命週期相關的 MITRE ATT&CK 技術，2022 年

Mandiant 的針對性攻擊生命週期是網路對手用於執行攻擊的可預測事件序列。欲瞭解更多資訊：https://www.mandiant.com/resources/targeted-attack-lifecycle

初步偵察

事前勘查

T1595：主動掃描	1.3%	T1595.002：漏洞掃描	0.5%
		T1595.001：掃描 IP 塊	0.5%
		T1595.003：詞資料表掃描	0.2%

資源開發

T1608：階段能力	8.8%	T1608.003：安裝數位憑證	6.0%
		T1608.005：連結目標	2.7%
		T1608.002：上傳工具	0.5%
		T1608.004：路過式目標	0.2%
		T1608.001：上傳惡意軟體	0.2%
T1583：獲得基礎設施	7.5%	T1583.003：虛擬私人伺服器	7.5%
T1584：入侵基礎設施	3.5%		
T1587：開發能力	2.6%	T1587.003：數位證書	1.3%
		T1587.002：編碼簽署憑證	1.3%
T1588：獲取能力	2.2%	T1588.003：編碼簽署憑證	1.6%
		T1588.004：數位證書	0.5%
T1585：建立帳戶	0.2%	T1585.002：電子郵件帳戶	0.2%

初步破壞

初始存取

T1190：利用面向公眾的應用程式	21.2%		
T1566：網路釣魚	16.5%	T1566.001：魚叉式網路釣魚附件	8.2%
		T1566.002：魚叉式網路釣魚連結	3.7%
		T1566.003：透過服務的魚叉式網路釣魚	0.2%
T1133：外部遠端服務	12.6%		
T1078：有效帳戶	9.3%		
T1189：路過式入侵	4.6%		
T1199：可信關係	2.4%		
T1091：透過可移動媒介複製	1.5%		
T1200：硬體新增	0.4%		
T1195：供應鏈入侵	0.2%	T1195.002：入侵軟體供應鏈	0.2%

建立據點

持續

T1543：建立或修改系統處理序	**24.9%**	T1543.003：Windows 服務	**13.6%**
		T1543.002：系統服務	**0.9%**
T1053：計畫的任務 / 工作	**18.3%**	T1053.005：計畫的工作	**12.8%**
		T1053.003：Cron	**0.9%**
T1098：帳戶操縱	**14.1%**	T1098.005：裝置註冊	**1.5%**
		T1098.004：SSH 授權索金鑰	**1.1%**
		T1098.001：額外雲端認證	**0.7%**
		T1098.002：額外電子郵件委派許可	**0.5%**
T1133：外部遠端服務	**12.6%**		
T1505：伺服器軟體元件	**11.9%**	T1505.003：網頁殼層	**11.7%**
		T1505.004：IIS 元件	**0.2%**
T1547：啟動或登入自動啟動執行	**10.8%**	T1547.009：快捷方式修改	**3.1%**
		T1547.004：Winlogon Helper DLL	**0.7%**
T1136：建立帳戶	**9.2%**	T1136.001：本機帳戶	**3.8%**
		T1136.003：雲端帳戶	**0.7%**
		T1136.002：網域帳戶	**0.7%**
T1574：劫持執行流	**8.2%**	T1574.001：登錄執行金鑰／開機資料夾	**7.7%**
		T1574.011：服務登錄權限弱點	**6.0%**
		T1574.002：DLL 側載	**1.8%**
		T1574.008：透過搜尋順序劫持的路徑攔截	**0.9%**
		T1574.010：服務檔案權限弱點	**0.2%**
		T1574.005：可執行安裝程式檔案權限弱點	**0.2%**
		T1574.001：DLL 搜尋命令劫持	**0.2%**
T1546：事件觸發執行	**4.8%**	T1546.003：Windows Management Instrumentation 事件訂閱	**2.4%**
		T1546.008：協助工具功能	**1.3%**
		T1546.012：影像檔執行選項插入	**0.4%**
		T1546.002：螢幕保護裝置	**0.4%**
		T1546.010：AppInit DLL	**0.4%**
		T1546.004：Unix Shell 設定修改	**0.4%**
		T1546.007：Netsh Helper DLL	**0.2%**
		T1546.001：變更預設檔案關聯	**0.2%**
T1037：啟動或登入初始化指令碼	**1.1%**	T1037.001：登入指令檔(Windows)	**0.4%**
		T1037.004：RC 指令碼	**0.2%**
T1542：作業系統前啟動	**0.2%**	T1542.002：元件固件	**0.2%**
T1176：瀏覽器擴充功能	**0.2%**		
T1137：Office 應用程式啟動	**0.2%**	T1137.006：增益集	**0.2%**

提升權限

提升權限

T1543：建立或修改系統處理序	**24.9%**	T1543.003：Windows 服務	**13.6%**
		T1543.002：系統服務	**0.9%**
T1055：處理序注入	**23.1%**	T1055.003：執行緒執行劫持	**1.5%**
		T1055.001：動態連結程式庫插入	**0.7%**
		T1055.002：可攜式執行檔插入	**0.5%**
		T1055.004：非同步程式呼叫	**0.5%**
		T1055.012：處理程式空白	**0.5%**
T1134：存取權杖操縱	**16.3%**	T1134.001：權杖偽裝 / 盜竊	**8.1%**
		T1134.004：上級 PID 欺騙	**0.4%**
		T1134.002：用權杖建立處理序	**0.4%**
T1547：啟動或登入自動啟動執行	**10.8%**	T1547.001：登錄執行金鑰／開機資料夾	**7.7%**
		T1547.009：快捷方式修改	**3.1%**
		T1547.004：Winlogon Helper DLL	**0.7%**
T1078：有效帳戶	**9.3%**		
T1574：劫持執行流	**8.2%**	T1574.011：服務登錄權限弱點	**6.0%**
		T1574.002：DLL 側載	**1.8%**
		T1574.008：透過搜尋順序劫持的路徑攔截	**0.9%**
		T1574.010：服務檔案權限弱點	**0.2%**
		T1574.005：可執行安裝程式檔案權限弱點	**0.2%**
		T1574.001：DLL 搜尋命令劫持	**0.2%**
T1546：事件觸發執行	**4.8%**	T1546.003：Windows Management Instrumentation 事件訂閱	**2.4%**
		T1546.008：協助工具功能	**1.3%**
		T1546.012：影像檔執行選項插入	**0.4%**
		T1546.002：螢幕保護裝置	**0.4%**
		T1546.010：AppInit DLL	**0.4%**
		T1546.004：Unix Shell 設定修改	**0.4%**
		T1546.007：Netsh Helper DLL	**0.2%**
		T1546.001：變更預設檔案關聯	**0.2%**
T1548：濫用提升控制機制	**2.7%**	T1548.002：繞開使用者帳戶控制	**1.8%**
		T1548.003：Sudo 和 Sudo 快取	**0.5%**
		T1548.001：Setuid 和 Setgid	**0.4%**
T1484：網域政策修改	**2.0%**	T1484.001：群組原則修改	**2.0%**
T1037：啟動或登入初始化指令碼	**1.1%**	T1037.001：登入指令檔(Windows)	**0.4%**
		T1037.004：RC 指令碼	**0.2%**
T1086：權限提升利用	**0.2%**		

內部偵察

發現

T1082：系統資訊發現	31.3%		
T1083：檔案和目錄發現	29.3%		
T1033：系統所有者／使用者發現	22.5%		
T1012：查詢登錄	22.3%		
T1622：Debugger 規避	21.1%		
T1057：程序發現	20.7%		
T1087：帳戶發現	18.3%	T1087.002：網域帳戶	5.5%
		T1087.002：本機帳戶	5.1%
		T1087.004：雲端帳戶	0.9%
		T1087.003：電子郵件帳戶	0.4%
T1016：系統網路設定發現	15.8%	T1016.001：發現網際網路連線	1.1%
T1518：軟體發現	15.4%		
T1497：虛擬化／沙箱 規避	13.7%	T1497.001：系統檢查	10.1%
		T1497.003：基於時間的規避	0.2%
T1007：系統服務發現	10.4%		
T1135：網路共用發現	9.7%		
T1069：權限群組發現	9.3%	T1069.002：網域群組	6.0%
		T1069.001：本機群組	1.8%
		T1069.003：雲端群組	0.9%
T1010：應用程式視窗發現	8.4%		
T1049：系統網路連接發現	8.2%		
T1482：網域信任探索	6.8%		
T1614：系統位置發現	5.9%	T1614.001：系統語言發現	5.7%
T1046：網路服務發現	2.7%		
T1580：雲端基礎設施發現	1.5%		
T1018：遠端系統發現	1.3%		
T1538：雲端服務儀表板	0.9%		
T1615：群組政策發現	0.9%		
T1040：網路監聽	0.5%		
T1201：密碼政策發現	0.4%		
T1124：系統時間發現	0.4%		
T1120：週邊裝置發現	0.2%		

橫向移動

橫向移動

T1021：遠端服務	**26.4%**	T1021.001：遠端桌面通訊協定	**20.3%**
		T1021.002：SMB / Windows 管理共用	**6.6%**
		T1021.004：SSH	**6.4%**
		T1021.005：VNC	**1.3%**
		T1021.006：Windows 遠端管理	**0.2%**
T1091：透過可移動媒介複製	**1.5%**		
T1570：橫向工具轉送	**1.5%**	T1550.002：雜湊傳遞	**0.5%**
		T1550.001：應用程式存取權杖	**0.2%**
		T1550.003：票證傳遞	**0.2%**
T1550：使用替代身分驗證材料	**1.1%**	T1550.002：雜湊傳遞	**0.7%**
		T1550.001：應用程式存取權杖	**0.4%**
T1534：內部魚叉式網路釣魚	**0.9%**		
T1563：遠端服務工作階段劫持	**0.2%**		

持續存取

持續

T1543：建立或修改系統處理序	**24.9%**	T1543.003：Windows 服務	**13.6%**
		T1543.002：系統服務	**0.9%**
T1053：計畫任務／工作	**18.3%**	T1053.005：計畫的工作	**12.8%**
		T1053.003：Cron	**0.9%**
T1098：帳戶操縱	**14.1%**	T1098.005：裝置註冊	**1.5%**
		T1098.004：SSH 授權索金鑰	**1.1%**
		T1098.001：額外雲端認證	**0.7%**
		T1098.002：額外電子郵件委派許可	**0.5%**
T1133：外部遠端服務	**12.6%**		
T1505：伺服器軟體元件	**11.9%**	T1505.003：網頁殼層	**11.7%**
		T1505.004：IIS 元件	**0.2%**
T1547：啟動或登入自動啟動執行	**10.8%**	T1547.001：登錄執行金鑰／開機資料夾	**7.7%**
		T1547.009：快捷方式修改	**3.1%**
		T1547.004：Winlogon Helper DLL	**0.7%**
T1136：建立帳戶	**9.2%**	T1136.001：本機帳戶	**3.8%**
		T1136.003：雲端帳戶	**0.7%**
		T1136.002：網域帳戶	**0.7%**
T1574：劫持執行流	**8.2%**	T1574.011：服務登錄權限弱點	**6.0%**
		T1574.002：DLL 側載	**1.8%**
		T1574.008：透過搜尋順序劫持的路徑攔截	**0.9%**
		T1574.010：服務檔案權限弱點	**0.2%**
		T1574.005：可執行安裝程式檔案權限弱點	**0.2%**
		T1574.001：DLL 搜尋命令劫持	**0.2%**
T1546：事件觸發執行	**4.8%**	T1546.003：Windows Management Instrumentation 事件訂閱	**2.4%**
		T1546.008：協助工具功能	**1.3%**
		T1546.012：影像檔執行選項插入	**0.4%**
		T1546.002：螢幕保護裝置	**0.4%**
		T1546.010：AppInit DLL	**0.4%**
		T1546.004：Unix Shell 設定修改	**0.4%**
		T1546.007：Netsh Helper DLL	**0.2%**
		T1546.001：變更預設檔案關聯	**0.2%**
T1037：啟動或登入初始化指令碼	**1.1%**	T1037.001：登入指令檔(Windows)	**0.4%**
		T1037.004：RC 指令碼	**0.2%**
T1542：作業系統前啟動	**0.2%**	T1542.002：元件固件	**0.2%**
T1176：瀏覽器擴充功能	**0.2%**		
T1137：Office 應用程式啟動	**0.2%**	T1137.006：增益集	**0.2%**

任務完成

收集

T1560：把收集到的資料存檔	17.2%	T1560.001：透過公用程式存檔	7.3%
		T1560.002：透過庫存檔	0.5%
T1213：來自資訊庫的資料	10.4%	T1213.002：Sharepoint	3.5%
		T1213.003：程式碼儲存庫	1.6%
		T1213.001：匯集	0.9%
T1056：輸入擷取	6.8%	T1056.001：鍵盤記錄	6.6%
		T1056.003：網路入口擷取	0.2%
T1113：螢幕擷取	5.1%		
T1115：剪貼簿資料	4.9%		
T1114：電子郵件收集	3.8%	T1114.002：遠端電子郵件收集	1.5%
		T1114.001：本機電子郵件收集	0.5%
		T1114.003：電子郵件轉寄規則	0.4%
T1074：資料已分級	3.8%	T1074.001：本機資料暫存	3.1%
		T1074.002：遠端資料暫存	0.4%
T1039：來自網路共用裝置的資料	2.9%		
T1005：來自本機系統的資料	1.1%		
T1602：來自設定存放庫的資料	0.7%	T1602.002：網路裝置設定傾印	0.7%
T1119：自動收集	0.4%		
T1530：來自雲端儲存的資料	0.4%		
T1125：視訊擷取	0.2%		
T1557：中間對手	0.2%	T1557.002：ARP 緩衝中毒	0.2%

滲透

T1567：Web 服務滲透	4.4%	T1567.002：滲透至雲端儲存	2.4%
T1020：自動滲透	1.3%		
T1041：透過 C2 管道滲透	0.7%		
T1030：資料轉送大小限制	0.2%		

影響			
T1486：為影響加密資料	**18.3%**		
T1489：服務停止	**13.0%**		
T1529：系統關閉／重啟	**7.5%**		
T1496：資源劫持	**5.3%**		
T1490：禁止系統復原	**5.1%**		
T1565：資料操縱	**2.0%**	T1565.001：儲存資料操縱	**2.0%**
T1485：資料銷毀	**1.8%**		
T1561：磁碟抹除	**0.7%**	T1561.001：磁碟內容清除	**0.4%**
		T1561.002：磁碟結構抹除	**0.2%**
T1531：帳戶存取移除	**0.7%**		
T1491：損壞	**0.7%**	T1491.002：外部損壞	**0.4%**
T1498：網路拒絕服務	**0.4%**	T1498.001：直接網路淹沒	**0.4%**
T1499：端點拒絕服務	**0.2%**	T1491.001：內部損壞	**0.2%**

額外惡意軟體定義

ALPHV，亦稱為 BlackCat（網際網路）和 Noberus(Symantec)，是以 Rust 編寫的勒索軟體。該勒索軟體可能包含指定勒索軟體功能的純文字 JSON 設定。ALPHV 或許能夠提升其特權並繞過 UAC，可能包含 AES 和 ChaCha20（或 Salsa）加密功能，或許使用重新啟動管理員作為其行動的一部分，會刪除磁碟區陰影複製，或許按比例枚舉磁碟區和網路共用，並且可能會終止處理程序與服務。

BASTA，亦稱為 Basta Ransomware，是以 C++ 語言編寫的勒索軟體，會加密本機檔案。該惡意軟體使用 .basta 作為加密檔案的副檔名。

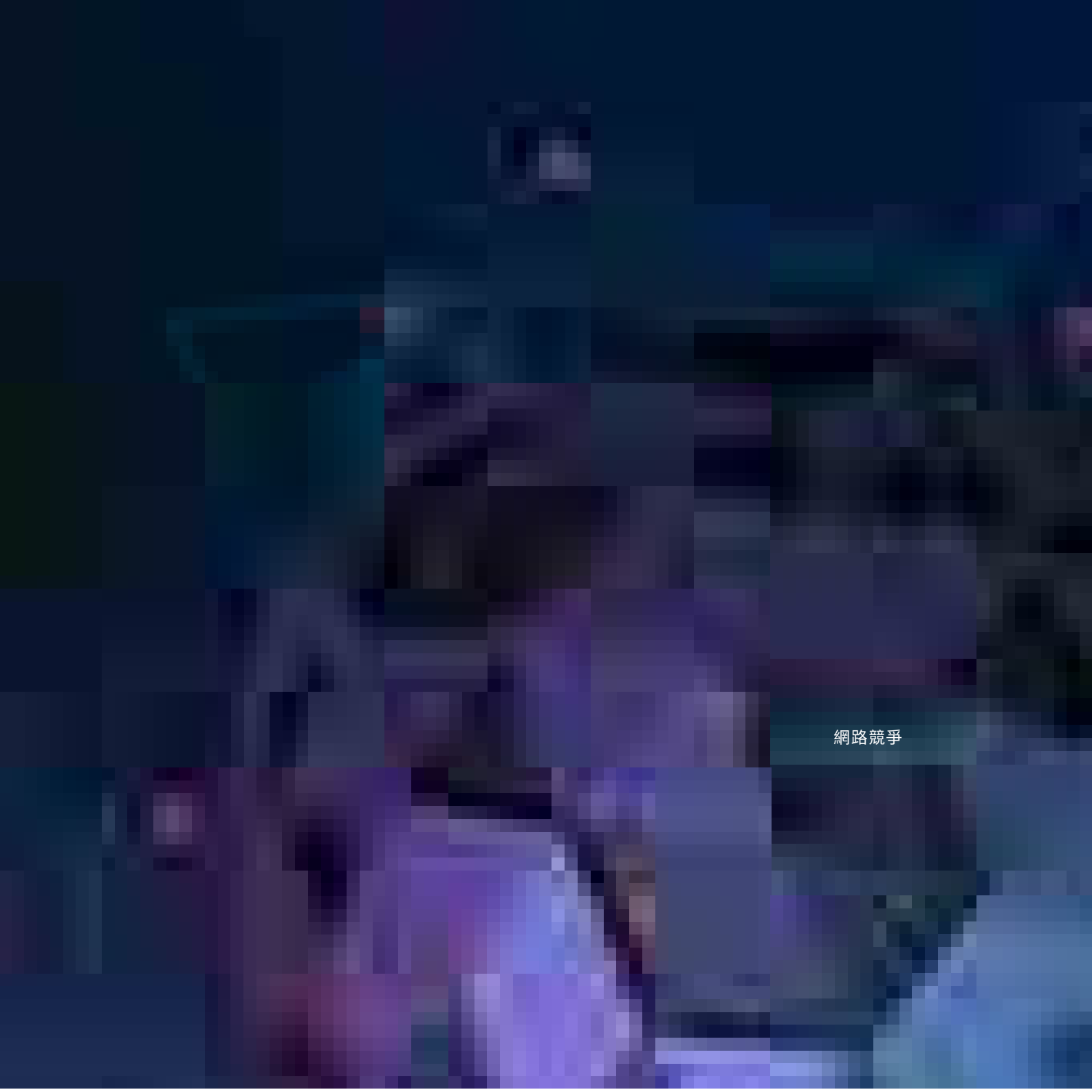
DRAGONJUICE 是基於「Ladon」專案的全面、模組化、跨平台、可自訂掃描工具。

LOCKBIT 是用 C 語言編寫的勒索軟體，對儲存在本機和網路共用上的檔案進行加密。LOCKBIT 還可以識別網路上的其他系統並透過 SMB 傳播。在加密檔案之前，LOCKBIT 會清除事件記錄檔，刪除磁碟區陰影複製，並終止可能影響其加密檔案能力的處理序和服務。據觀察，LOCKBIT 已經使用檔案副檔名「.lockbit」來加密檔案。

ROYALLOCKER 是私人管理的 Windows 型勒索軟體，能夠加密本機檔案，停用執行中程序並刪除陰影複製。該勒索軟體還能夠加密 VMDK 磁碟格式。

SODINOKIBI 亦稱為 Revil（網際網路）Sodin（網際網路）和 Trickgate（檢查點），是以 C 語言編寫的勒索軟體，能加密本機存放和網路上分享的檔案。它會從指定目錄、備份檔案及磁碟區陰影複製中刪除檔案。SODINOKIBI 可以設定成透過 HTTP 向遠端伺服器發送基本系統資訊。系統資訊包括目前使用者名稱、主機名稱、網域名稱和地區設定。

TANKTRAP 是以 PowerShell 編寫的公用程式，會使用 Windows 群組政策來擴散和啟動清除程式。我們有觀察到 NEARMISS、SDELETE、PARTYTICKET 和 CADDYWIPER 使用了 TANKTRAP。



入侵烏克蘭：戰時的網路行動

俄羅斯於 2021 年秋季開始在其與烏克蘭的邊界沿線集結軍隊，這促使美國和歐洲官員就俄羅斯入侵的威脅發出警告。Mandiant 確定了在 2022 年 2 月 24 日俄羅斯入侵烏克蘭之前和之後發生的廣泛的網路間諜活動、干擾性與破壞性網路攻擊，以及資訊行動。

克里姆林宮不斷升級將烏克蘭納入俄羅斯勢力範圍的企圖最終以俄羅斯的入侵告終，並為網路威脅活動創造了前所未有的環境。入侵烏克蘭代表著主要網路強國在廣泛、活躍的軍事行動的同時，開展破壞性攻擊、間諜活動和資訊行動的首批例項之一。在俄羅斯入侵的前幾個月內，Mandiant 從未觀察到與攻擊數量、威脅發動者種類及工作協調相匹配的威脅發動者活動。此次入侵還對俄語網路犯罪生態系統造成了暫時性破壞，在某些情況下還沿著政治路線分裂了犯罪組織，而且它似乎還觸發了自 2015 年以來駭客入侵中最大的復興。

衝突期間俄羅斯網路行動的演變可以大致劃分為五個主要階段：

- **戰略網路間諜活動和入侵前的預先部署 (2022 年 2 月之前)**
- **初步的破壞性網路行動和軍事入侵 (2022 年 2 月至 2022 年 4 月)**
- **持續的目標鎖定與攻擊 (2022 年 5 月至 2022 年 7 月)**
- **為獲取戰略優勢而保持據點 (2022 年 8 月至 2022 年 9 月)**
- **新的破壞性攻擊活動 (2022 年 10 月至 2022 年 12 月)**

Mandiant 還觀察到中國、白俄羅斯及伊朗威脅組織在每個階段中將目標鎖定烏克蘭。我們認為中國和烏克蘭組織的入侵旨在為其政府收集情報，而白俄羅斯組織則既收集情報，又利用入侵來啟動資訊行動。

在入侵的所有階段中，Mandiant 已經透過事件回應、補救、情報、託管服務、網路防禦及一般諮詢來支援烏克蘭的數十個組織，我們將在 2023 年繼續回應烏克蘭各地的事件。雖然 Mandiant 幾乎與烏克蘭工業的每個部門都進行了接觸，但我們的絕大多數的調查都支援烏克蘭國家政府組織。

Mandiant 還確認了在每個階段進行的相關資訊行動，包括那些使用傳統網路威脅活動的行動。

2022 年烏克蘭戰爭期間俄羅斯網路行動的五個階段
2022 年 1 月到 9 月

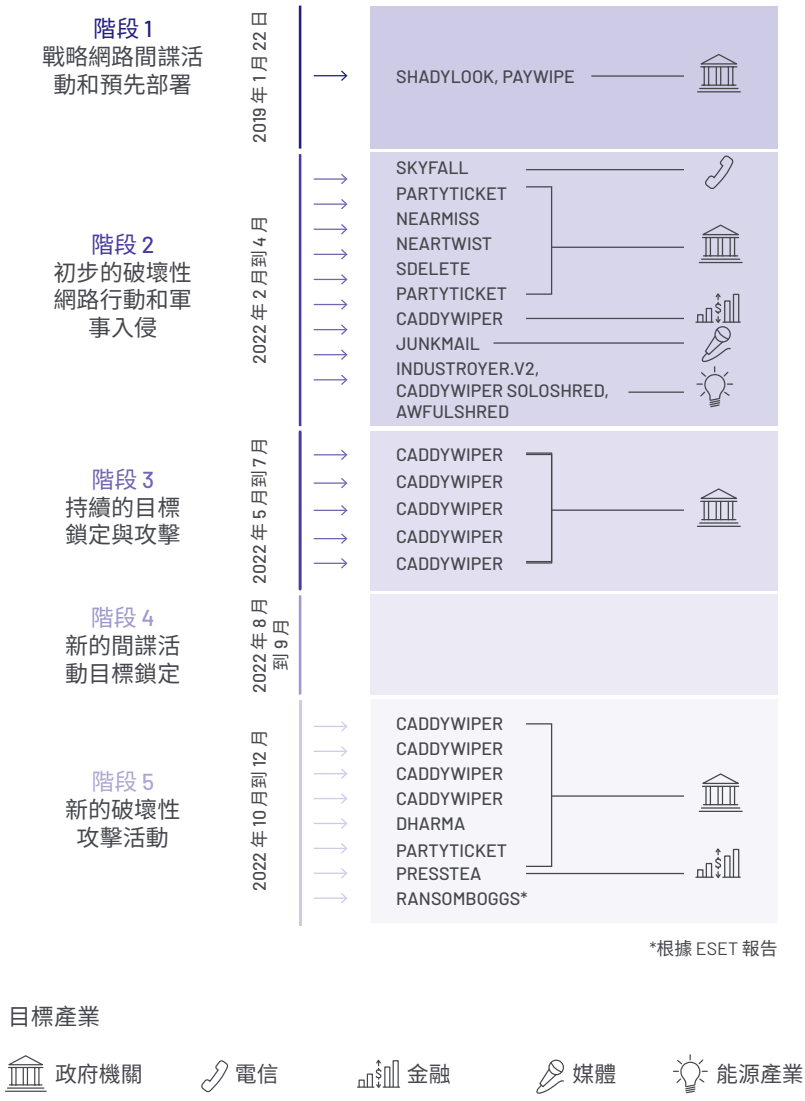


圖 1. 2022 年觀察到的俄羅斯在烏克蘭網路行動的各個階段。

戰略網路間諜活動和入侵前的預先定位

入侵活動

Mandiant 觀察到多個威脅組織在入侵前的時間範圍內進行入侵活動。最值得注意的是，我們在入侵烏克蘭之前觀察到了 UNC2589 和 APT28 的活動。

UNC2589

UNC2589（Mandiant 懷疑其代表俄羅斯政府的利益行事）在烏克蘭進行了大量的間諜活動收集行動，尤其是在俄羅斯入侵前的 2021 年底和 2022 年初。尤其是，我們評估 UNC2589 於 2022 年 1 月 14 日透過 PAYWIPE（亦稱為 WHISPERGATE）對烏克蘭實體進行了破壞性攻擊。這或許是初步但不成熟的攻擊，俄羅斯軍事準則稱之為武裝衝突「在資訊領域的準備」，目的是動搖烏克蘭人民對其政府的信任，並破壞對針對俄羅斯侵略的強大防禦的支援。2022 年 1 月和 2 月，針對烏克蘭關鍵基礎設施的額外 UNC2589 行動也支援這一目標，然而也針對金融機構進行了分散式阻絕服務（DDoS）攻擊。

APT28 和其他 GRU 叢集

Mandiant 確認了在多個例項中，俄羅斯聯邦武裝部隊總參謀部情報總局（GRU）相關叢集依賴於歷史上入侵的投機性存取，以便在戰爭開始後獲得目前的持續存取。2022 年 2 月下旬，GRU 資助的威脅組織 APT28 重新啟動了休眠的 2019 EMPIRE 感染，使其在環境內橫向移動，並使用 SDELETE 公用程式來在受感染的系統中刪除檔案和目錄。在另一個案例中，APT28 把目標瞄準 VPN，以獲得存取權限，並在 2021 年 4 月向多個受害者部署了 FREETOW 植入程式。在至少一個案例中，在取得據點後，攻擊者進入休眠狀態，直到在戰爭的第二階段期間，於 2022 年 2 月和 3 月開展了一系列的清除攻擊。自戰爭開始以來，APT28 一直是俄羅斯在烏克蘭最活躍的活動叢集，並且將破壞性網路攻擊置於在烏克蘭的間諜活動之上。

初步的破壞性網路行動和軍事入侵
(2022 年 2 月至 2022 年 4 月)

在 2022 年前四個月內，Mandiant 在烏克蘭觀察到的破壞性網路攻擊比過去八年內的更多。在戰爭的前幾個階段內，烏克蘭組織受到使用六種獨特清除程式的威脅發動者的影響。這些破壞性網路攻擊的時間恰逢，並且很可能支援俄羅斯於 2022 年 2 月 24 日入侵烏克蘭，而且沒有針對與戰爭直接相關或支援戰爭的組織。雖然破壞性網路攻擊最初確實在一些烏克蘭網路中造成了廣泛的破壞，但它們的影響力可能不如之前針對烏克蘭的一些俄羅斯網路攻擊。相比之下，俄羅斯在 2015 年和 2016 年成功以破壞電網為目標而發動了網路攻擊，使數十萬烏克蘭人在數小時內無電可用，而 2017 年的 NOTPETYA 攻擊破壞了整個烏克蘭及其他地區的行動。

APT28 清除攻擊和 GRU Living on the Edge

Mandiant 觀察到 APT28 以多個烏克蘭實體為目標，進行破壞性和間諜活動行動，類似於戰爭開始時的行動。APT28 的戰時行動已經偏離了歷史上的 APT28 活動。該組織已經表現出傾向於入侵邊緣基礎設施，進行各種行動，我們稱這一技術為「Living on the Edge」。APT28 還在短時間內使用了各種破壞性和間諜活動惡意軟體，並在戰爭期間使用了幾個近期發布的漏洞攻擊，包括 PROXYSHELL、PROXYSHELL 漏洞鏈，以及幾個 Exchange 漏洞。

「Living on the Edge」已經成為戰爭期間 GRU 行動的關鍵部分。自烏克蘭戰爭開始以來，GRU 一直試圖對烏克蘭境內的關鍵服務和組織進行連續且幾乎不變的網路間諜活動與破壞活動。目標群組織的存取權限和針對目標群組織的行動之間的平衡依賴於對路由器和其他網際網路連接裝置等邊緣基礎設施的入侵。在破壞性行動導致無法直接存取端點的情況下，被入侵的邊緣裝置會允許持續重新進入網路。由於大部分的 EDR 技術沒有涵蓋這些類型的裝置，因此防禦者也更難入侵這些路由器。

俄羅斯對個工業控制系統能力的新興趣

2022 年 2 月到 4 月期間，軟體公司 ESET 報告了一名疑似俄羅斯威脅發動者在一次行動中針對烏克蘭電力設施，導致部署了多個清除惡意程式碼系列。此次攻擊還涉及面向工業控制系統 (ICS) 破壞框架 INDUSTROYER.V2 的一種變體，2016 年 12 月的一次類似攻擊中使用了該框架的先前版本，在烏克蘭造成停電。雖然尚不清楚該行動是否有效地影響了電力設施的電力傳輸與分配行動，但該事件強化了一種觀念，即俄羅斯具有影響電力系統的可重複使用能力。

駭客人物和網路資訊行動的重新出現

Mandiant 觀察到入侵烏克蘭後，駭客入侵顯著增加，包括來自俄羅斯支援的組織的活動。俄羅斯情報部門在使用虛假的駭客人物來支援資訊行動，以及幹擾性和破壞性網路活動方面有著悠久的歷史。特別是，Mandiant 專注於分析一系列自稱的駭客組織 ——XakNet Team、Infoccentr 和 CyberArmyofRussia_Reborn—— 所有這些組織都可能至少與 GRU 資助的 APT28 協調過行動。Mandiant 直接觀察到 APT28 在多個烏克蘭組織的網路上部署了清除程式，隨後在 24 小時內自稱是駭客主義者的威脅發動者在 Telegram 上洩露了資料，這些發動者很可能是源自該組織。我們從這些組織確認了至少 16 次數據洩露，其中有四次與 APT28 的清除攻擊同時發生。

在 Telegram 通道上，威脅發動者聲稱透過 DDoS 攻擊、網站塗改及駭客和洩密行動等傳統駭客活動來攻擊受害者。此類活動有兩個可能的影響目標，有利於俄羅斯入侵烏克蘭。這些組織透過其威脅活動在海外宣傳俄羅斯的利益，他們透過聲稱自己是愛國志願者來向國內受眾宣傳普通俄羅斯人支援政府的想法。這兩項工作都被俄羅斯媒體，在社交媒體平台，以及在其他線上平台上放大了。

在這個階段，Mandiant 還觀察到 KillNet 集體的駭客活動有所增加。KillNet 聲稱對針對波蘭、立陶宛及其他 NATO 國家的活動負責，這似乎符合俄羅斯政府的優先事項。然而，Mandiant 尚未發現將 KillNet 與俄羅斯情報部門相關聯的直接證據。

使用實體存取實現網路行動

在針對烏克蘭政府組織網路的活動進行調查時，Mandiant 發現證據表明入侵是俄羅斯軍事單位於 2022 年初實際存取網路之後發生。發動者（Mandiant 追蹤為 UNC3762）使用了該實際存取來進行網路偵查、收集憑證，並使用遠端桌面和網頁殼層橫向移動。UNC3762 還入侵了 PROXYSHELL 漏洞鏈（CVE-2021-34473、CVE-2021-34523、CVE-2021-31207），部署了 THRESHGO 惡意軟體，並從環境中竊取資料。

持續的目標鎖定與攻擊
(2022 年 5 月至 2022 年 7 月)

在最初幾波破壞性攻擊後，針對烏克蘭的網路行動的速度和種類都發生了變化。Mandiant 觀察到有人持續嘗試部署清除惡意軟體，但這些攻擊與 2022 年 2 月最初一波攻擊相比協調性更低。這些攻擊通常在攻擊者獲得或重新獲得存取權限後更快發生，而存取權限通常是透過入侵邊緣基礎設施獲得。在許多例項中，烏克蘭防禦者能夠在發生任何破壞之前確認並緩解攻擊企圖。Mandiant 還看到在各波破壞性活動之間的存取權限和收集行動企圖，這表明俄羅斯要求持續存取之前被清除的實體。

持續入侵和行動節奏

在戰爭的這個階段中，俄羅斯網路發動者繼續企圖透過入侵邊緣基礎設施重新獲得多個受害網路存取權限，或透過 GRE 通道，在持續緩解的情況下維持在網路上的存取。這種模式證明了與俄羅斯結盟的威脅發動者開展的週期性收集和破壞性活動。GRU 叢集透過採用新發布的漏洞攻擊來保持其較高的行動節奏，同時也在努力將其破壞行動標準化。在各波破壞活動之間，有一個使用被入侵的合法電子郵件伺服器的網路釣魚活動企圖入侵 Follina 漏洞，以使用 EARLYBLOOM 和 DARKCRYSTALRAT 後門程式支援 APT28 存取與收集行動。GRU 還從使用多種不同清除程式轉向嚴重依賴 CADDYWIPER 及其變體來在快速週轉行動中清除組織。這種高行動節奏導致行動人員犯下幾個錯誤。在一個例項中，一個威脅發動者企圖使用 NEARMISS 參數來部署 PARTYTICKET 有效載荷。他們能夠調整並成功部署 NEARMISS，但是錯誤導致延誤並有可能影響其有效性。

GRU 入侵行動在其於戰爭開始時的行動，以及那些發生在這個持續的目標鎖定階段的行動之間保持了幾個主題。總體上，GRU 繼續針對和使用邊緣基礎設施來獲取戰略目標的存取權限。一旦進入環境，GRU 叢集使用 IMPACKET 和公開可用的後門程式來維持據點。Mandiant 還觀察到另一個 GRU 叢集 UNC3810 展示了在 Linux 系統上鎖定目標和行動的熟練程度。UNC3810 在很大程度上使用了 GoGetter 和 Chisel 等代理工具來維持存取並在目標環境內橫向移動。

為獲取戰略優勢而保持據點
(2022 年 8 月至 2022 年 9 月)

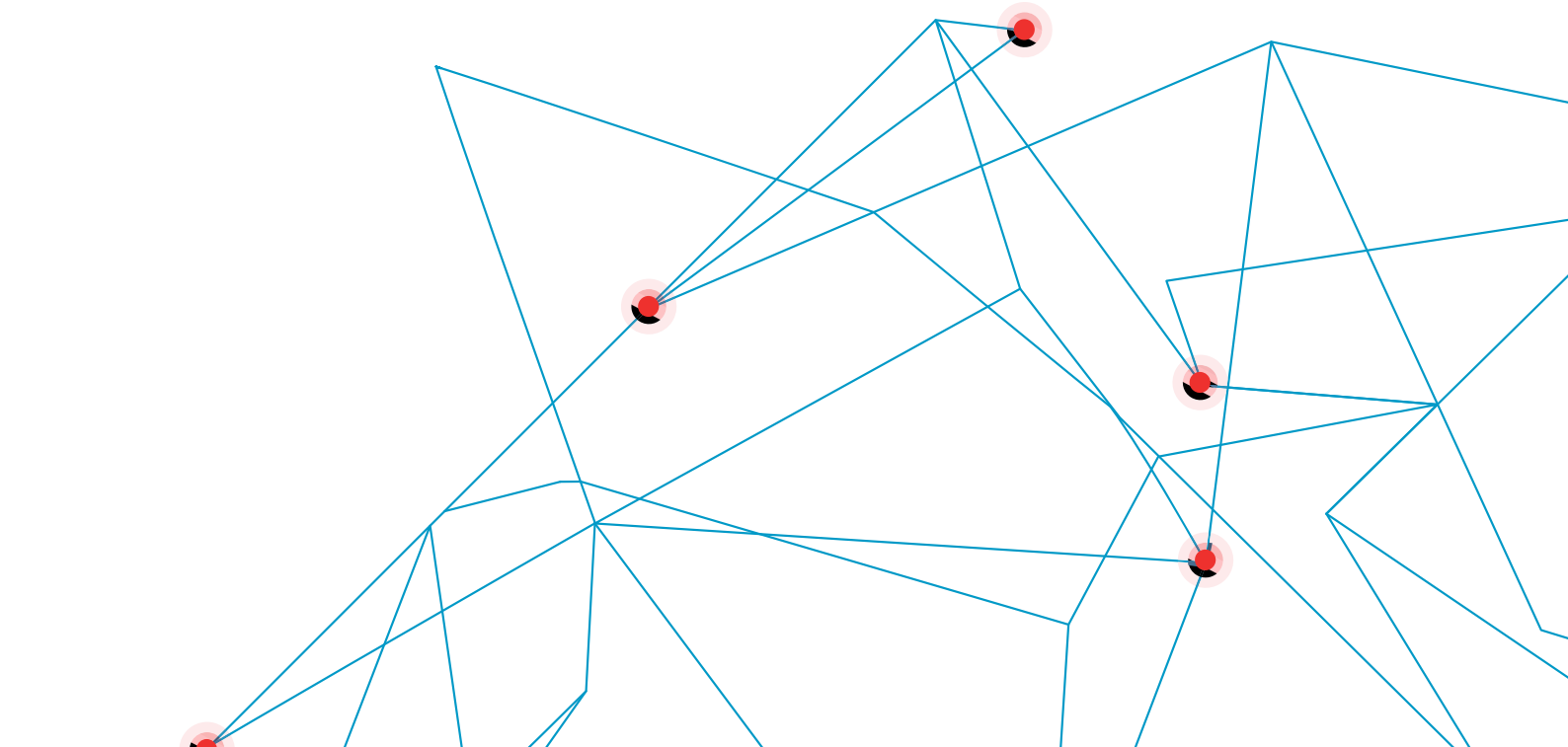
在前一階段結束時，我們沒有觀察到與可疑 FSB 網路威脅發動者 Turla 或 Temp.Isotope 相關活動的任何直接證據。然而，在八月到九月之間，GRU 叢集停止了針對烏克蘭的破壞性活動，而且與 FSB（俄羅斯的聯邦安全局）相關的叢集開始出現。雖然一個 GRU 相關叢集 UNC3810 仍然活躍在間諜活動領域，但 Mandiant 觀察到與俄羅斯有關聯的威脅組織 TEMP.Armageddon 將目標鎖定烏克蘭的不同政府實體。儘管我們主要觀察到自戰爭開始以來，GRU 叢集掌舵針對烏克蘭的網路行動，但是 TEMP.Armageddon—— 一個與俄羅斯有關的威脅發動者，收集關於烏克蘭國家安全和執法實體的資訊，以支援俄羅斯的國家利益，完全專注於烏克蘭目標 —— 一直在透過不斷演變的工具與技術來針對烏克蘭與其他歐洲組織。從 TEMP.Armageddon 觀察到的行動範圍與該組織在過去幾年內開展的大量活動一致。

除了以烏克蘭政府實體為目標的 TEMP.Armageddon，Mandiant 還在八月和九月確認了可疑的 Turla 活動。Turla 是俄羅斯網路間諜活動發動者，自 2006 年以來就一直保持活躍，以針對外交、政府及防禦實體而聞名。Mandiant 確認了一次可追溯至 2021 年底的入侵，該入侵發生在一家符合 Turla 的戰術、技術與程序的烏克蘭政府機構。

破壞性攻擊的新節奏
(2022 年 10 月至 2022 年 12 月)

行動最新階段的特點是烏克蘭破壞性網路攻擊的死灰復燃。儘管一些攻擊看起來與前幾個階段中看到的破壞性攻擊類似，但是這一波新的破壞性攻擊似乎偏離了歷史常態。早期嘗試依賴於使用 CADDYWIPER 變體的快速週轉行動，但是在十月到十二月進行的攻擊中，CRU 叢集在目標網路上部署了勒索軟體變體。這一轉變與 Microsoft 關於 IRIDIUM 在波蘭部署的 Prestige (PRESSTEA) 勒索軟體的報告一致。儘管在此階段的存取和行動迴圈似乎仍在繼續，但 GRU 轉向使用勒索軟體可能表明他們正在經歷工具轉變，且沒有資源去以來編寫或修改自訂惡意軟體。

在此階段中，Mandiant 還觀察到針對烏克蘭能源部門的破壞性行動與針對烏克蘭能源基礎設施的更廣泛的俄羅斯活躍活動同時發生。雖然網路行動有可能在支援活躍活動，但我們沒有足夠的見解來確認它。



關於俄羅斯入侵烏克蘭的資訊行動

俄羅斯針對烏克蘭的戰爭在這個話題上產生了過多的虛假資訊。Mandiant 觀察到各種虛假資訊活動，從網路資訊行動，到利用協調過的不真實帳戶網路來在線上媒體中推廣捏造的內容之活動。Mandiant 已經確認了多個與俄羅斯結盟的資訊行動，這些行動和宣傳與衝突有關敘事的已知發動者有關，包括與白俄羅斯有關聯的 Ghostwriter 活動、Secondary Infektion 活動，以及據報導與隸屬於俄羅斯網路研究社的個人有關之活動。

俄羅斯的虛假資訊活動似乎具有雙重目的，即在戰術上回應或塑造現場事件，並在戰略上影響不斷變化的地緣政治格局。正在宣傳的敘事旨在打擊烏克蘭人的士氣並煽動內部動盪，將烏克蘭與其盟友孤立開來，並加強對俄羅斯的正面看法。雖然大部分的虛假資訊活動是以烏克蘭和歐洲的受眾為目標，但是 Mandiant 已經確認了針對俄羅斯國內受眾的資訊宣傳活動，這進一步強調了俄羅斯向本國人民推銷戰爭的必要性。

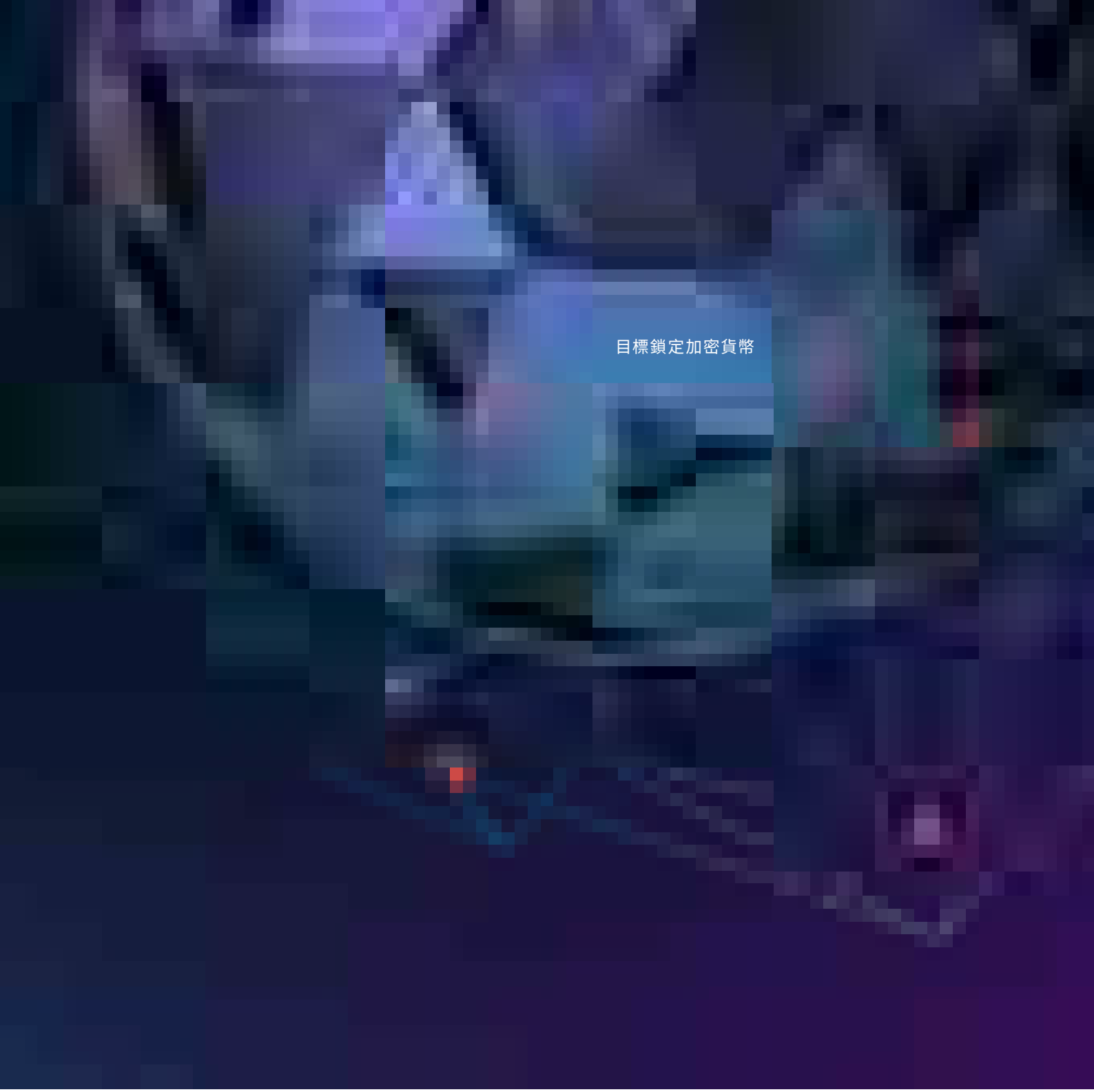
Mandiant 預計此類行動，包括那些涉及網路威脅活動及具有潛在干擾性和破壞性攻擊的行動，將隨著衝突的開展而繼續。與此同時，Mandiant 還觀察到親中國和親伊朗的活動適時地利用俄羅斯入侵來進一步推進長期戰略目標。儘管其中一些行動推動了似乎符合俄羅斯利益的敘事，但它們也展示了具有全球意義的事件如何能夠吸引第三方發動者。Mandiant 預計這種動態將會繼續下去，並且正在積極監控其圍繞衝突的資訊行動活動範圍的擴大。

重點

俄羅斯對烏克蘭的入侵表明，網路行動和作為新的事實標準的活躍戰爭可能存在重疊。戰爭幾乎消耗了俄羅斯國際關係的各個方面，並已經幾乎演變成 2022 年俄羅斯網路威脅活動的唯一推動因素。雖然俄羅斯威脅發動者為絕大多數的間諜活動和 Mandiant 調查的所有干擾性和破壞性行動負責，但是中國和伊朗國家資助的組織也一直活躍於該區域，凸顯了各國將如何利用網路來獲取關於情報重點的資訊。

俄羅斯發動者的戰術與戰略選擇展示了網路行動與權衡的多功能性。俄羅斯使用之前的入侵來進行清除行動，這表明了在地緣政治形勢發生變化的情況下，為間諜活動目的而開始的入侵如何能用於攻擊，並表明防禦者必須對入侵進行確認與全面修復。俄羅斯發動者專注於邊緣裝置的戰術性選擇也實現了靈活性，並使發動者能在破壞性活動後繼續收集資訊。這些裝置很難被防禦者監控，但是它們應該立即被修補，而且任何源自它們的可疑流量都應接受全面調查。

任何武裝衝突都有可能會帶來針對民眾和重負的破壞性行動。政府和私有部門組織在一個國家的運作中都發揮著重要作用。為了抵禦此類攻擊和從中恢復的而做的準備工作應該是標準的，因為如果被認為支援了其中一方，即便是沒有直接受到敵對行動直接影響的國家也可能會被針對。



北韓的經濟行動繼續升級

除了傳統情報收集任務外，2022 年 DPRK 行動人員對竊取和使用加密貨幣表現出了更大的興趣，隨著該政權尋求減輕制裁的經濟影響，他們的活動延伸到數位資產生態系統新的部分。

至少從 2016 年開始，與朝鮮民主主義人民共和國 (DPRK) 相關的威脅發動者已經將網路行動延伸到傳統的間諜活動收集與破壞性攻擊之外，以利用他們的能力進行以金融為動機的活動與入侵。從歷史上看，北韓威脅發動者將目標鎖定為全球的金融實體、投資服務、電子商務、加密貨幣使用者以及交易所和交易處理組織。這些活動包含對傳統金融實體 (其中最著名的目標是孟加拉中央銀行)，以及新興的加密貨幣和數字資產部門的入侵。2022 年，Mandiant 觀察到北韓威脅發動者繼續發展他們的目標鎖定，作為確認替代收入來源和減輕制裁影響之工作的一部分。

雖然這些組織似乎在繼續利用各種金融目標，但是 Mandiant 觀察到 2022 年對加密貨幣生態系統的關注度越來越高。威脅發動者使用創造性手段為北韓政權及其自己的行動提供資金。尤其是，在過去一年裡，Mandiant 還觀察到從針對更少、更大的組織轉向針對更大的數量的較小實體，從而獲取適度的經濟利益。媒體報導強調了北韓行動人員在 2022 年竊取了大約 17 億美元的加密貨幣，超過了 2021 年竊取的 4.28 億美元。此外，據說該政權還持有 1.7 億美元的未洗錢加密貨幣，這些加密貨幣可能被儲存為儲備金。聯合國 (UN) 表示，這些非法資金正被用於資助該國的導彈計畫。

NFT、跨鏈橋、勒索軟體等等：2022 年北韓網路犯罪

Mandiant 對北韓加密貨幣行動的早期分析強調了他們以針對加密貨幣交易所為中心，並且主要由 TEMP.Hermit 和疑似與 APT38 有關聯的叢集驅動。自那以後，加密貨幣盜竊中涉及的可疑 DPRK 組織數量，及其目標的性質繼續不斷擴大。北韓威脅發動者已經將目標對準加密貨幣的跨學科層面，包括非同質化代幣 (NFT)、跨區塊鏈連接機制，甚至網路遊戲。

在疑似與北韓有關的組織 UNC4469 發起的一場長達數月的廣泛加密貨幣網路釣魚活動中，數千份智慧合約被用來向超過一百萬毫無戒心的使用者提供惡意 NFT。UNC4469 使用惡意的大規模 NFT 空頭到使用者錢包、網路釣魚頁面及社交媒體平台，其主題旨在透過社交工程讓受害者連接他們的錢包。一旦連接到錢包，UNC4469 能夠收集並轉移資產（包括 NFT）至 UNC4469 控制的錢包。從網路釣魚受害者那裡竊取的資產很快就被出售，資金透過各種區塊鏈轉移，以進行洗錢並掩蓋它們的痕跡。跨越多個區塊鏈的活動自動化、持續時間及數量表明正在進行複雜且成熟的執行。

除了 NFT，「跨鏈橋」是加密貨幣生態系統的另一部分，今年來使用量不斷增長。跨鏈橋有助於不同區塊鏈之間的資產流動，無需使用加密貨幣交易所。隨著跨鏈橋的使用更加廣泛，它們可以積累價值，使其成為有吸引力的目標。2022 年，發動者對 Harmony 的 Horizon 跨鏈橋的 1 億美元入侵就證明了這一點，FBI 將其歸因於北韓 [5]。

隨著加密貨幣的興起，以加密貨幣和區塊鏈為主要特徵的網路遊戲也流行起來，也因此獲得了北韓團體的興趣。2022 年 4 月，美國財政部聲稱，北韓的威脅發動者應對網路遊戲 Axie Infinity 玩家使用的數位分類帳中 6 億美元被盜事件負責。美國政府成功扣押了與此次盜竊有關的 3,000 萬美元加密貨幣，並將其歸因於「Lazarus」網路犯罪團夥。北韓發動者 TEMP.Hermit 展示了針對加密貨幣服務的歷史，其中許多事件被歸因於 Lazarus。

2022 年北韓值得注意的針對加密貨幣的威脅活動

		可疑組織	使用的惡意程式碼系列
2022 年	一月	UNC1130	COINTOSS
		UNC1130	不適用
	三月	TEMP.HERMIT	不適用
		不適用	不適用
	四月	不適用	不適用
	五月	不適用	不適用
	六月	UNC1069	LONEJOGGER
	七月		
	八月	UNC1130	LOGCABIN
	秋季	UNC1758	AppleJeus

此外，Mandiant 在 2022 年 4 月和 5 月調查了多起疑似 DPRK 在以加密貨幣為重點的組織中獲得工作機會的努力的開源報告。這些說法似乎與 2022 年 5 月的美國政府諮詢一致，該諮詢是關於北韓 IT 工作者冒充非北韓國民在有機會為 DPRK 計畫創收的領域內獲得工作機會。

雖然這些行動的規模和性質表明它們的存在主要是為了促進為北韓政權的原子核計畫野心提供資金，但 Mandiant 觀察到的一些活動表明它們也可能起到支援發動者進一步網路行動的作用。例如，Mandiant 已經觀察到與公開報導的 Kimsuky 活動集相一致的活動叢集 UNC1130 使用針對性金融資料和被竊取的加密貨幣來購買基礎設施與裝置。UNC1130 行動人員採用各種線上人物角色來從多個供應商處購買基礎設施、硬體及編碼簽署憑證。在至少一個確認的購買中，威脅發動者使用了美國地址。這些購買是透過 PayPal、American Express 信用卡及源自之前行動的加密貨幣進行的。Mandiant 此前曾觀察到 DPRK 控制的錢包向加密貨幣付款服務提供者付款。

最後，2022 年底，敏感及開源報告表明，一些與公開追蹤為 Andariel 的威脅組織相關叢集涉及在影響全球組織的活動中使用勒索軟體。對這些活動的分析，保安閾 UNC4131 和 UNC4369 的活動，表明它們的目標似乎以金融為動機，至少部分目標是透過自籌資金進行進一步行動。相比其他賺錢計畫，UNC4131 和 UNC4369 開展的活動數量有限。

不只是金錢：在環境中持續的情報收集行動

如今，北韓相關威脅叢集承擔著雙重任務。儘管他們越來越關注以金融為動機的活動，但是 Mandiant 繼續看到傳統間諜活動性質的 DPRK 活動與行動。2022 年，Mandiant 觀察到影響政府、航太與國防、教育、法律、媒體、製藥及技術部門的入侵，以及南韓、日本和美國的其他組織。這些行動持續的事前勘查和社交工程工作，以定制存取戰略資訊的魚叉式網路釣魚活動。

2022 年初，北韓間諜活動組織進行了針對專業學者、記者、政治人物、博客主及其他私有部門個人的憑證盜竊行動，主要是在南韓。Mandiant 觀察到目標與 2021 年年中持續存在的類似活動一致，儘管與前幾個月相比，它們反映出私有部門受害者有所增加，且針對宗教組織的行動有所減少。對惡意軟體發布資料、誘餌檔案語言及誘餌內容的分析表明，南韓和日本的實體成為了一場以軟體發展為主題的網路釣魚電子郵件活動的目標。其中一個檔案提到了一家銷售資安裝置的日本科技公司，包括資安攝影機。

對電子郵件內容、詐騙實體及目標的分析表明，UNC1130 在持續開展戰略情報收集與竊取憑證活動。這些最有可能是為了讓北韓領導層瞭解地緣政治問題，以及從各國對 DPRK 武器試驗的興趣到對感知的 DPRK 活動的潛在回應等問題。

Mandiant 觀察到另一個北韓威脅發動者 UNC2970 透過 LinkedIn 訊息向媒體產業的目標發送訊息。一旦建立了聯繫，媒介就變成了簡訊服務。隨後一份武器化工作描述誘餌檔案被發送給受害者，從而實現初始存取。在獲得目標環境存取權限後，UNC2970 利用各種惡意程式碼系列來執行傳統的間諜活動行動。

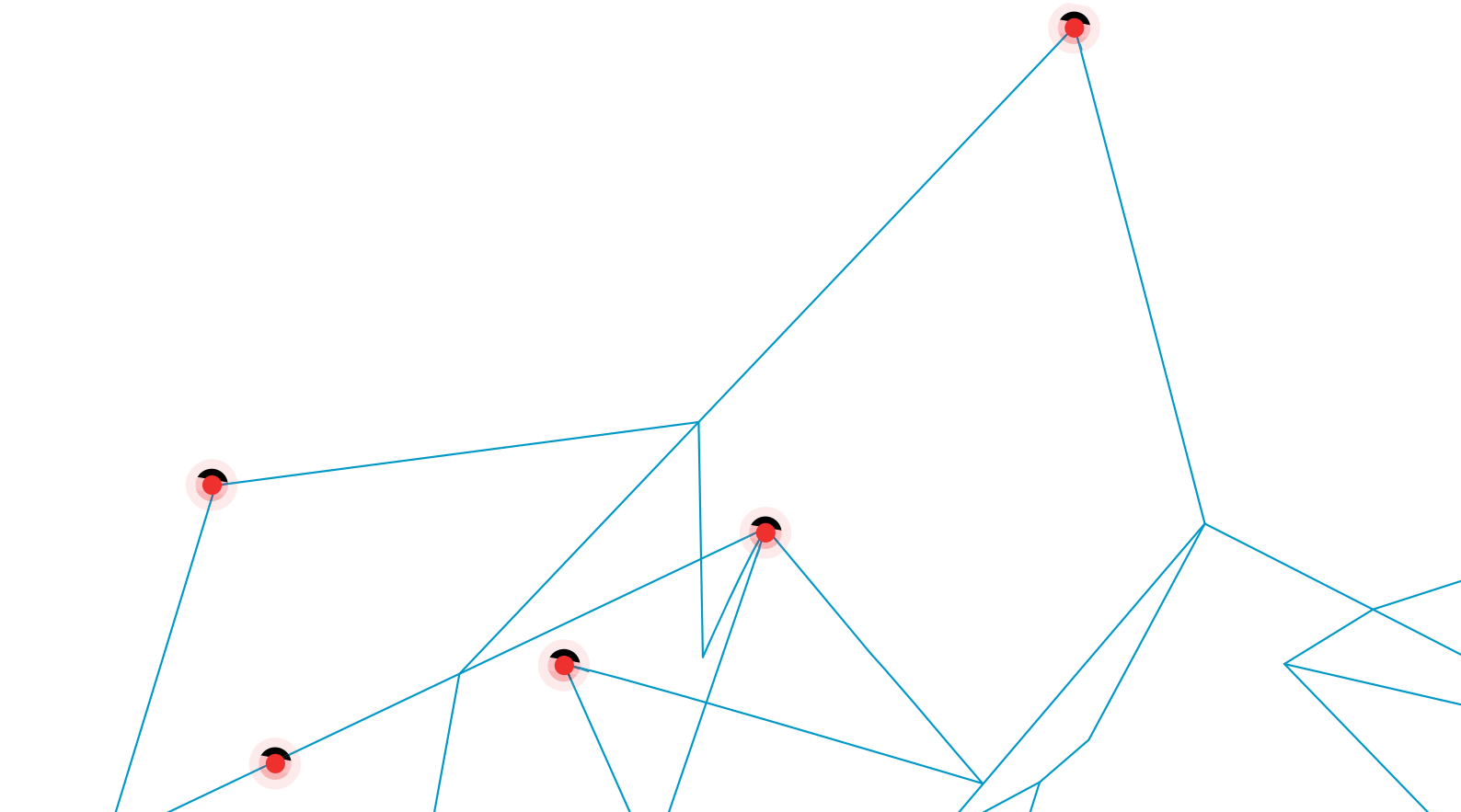
雖然傳統的網路間諜活動仍然是北韓的首要任務，但在 2022 年對資金的需求更加強烈，並一致決心將獲取經濟利益放在首位。北韓對西方利益的目標鎖定將有可能繼續與國家優先事項相稱，例如該政權的原子核野心，以及在區域上集中的地緣政治事件。

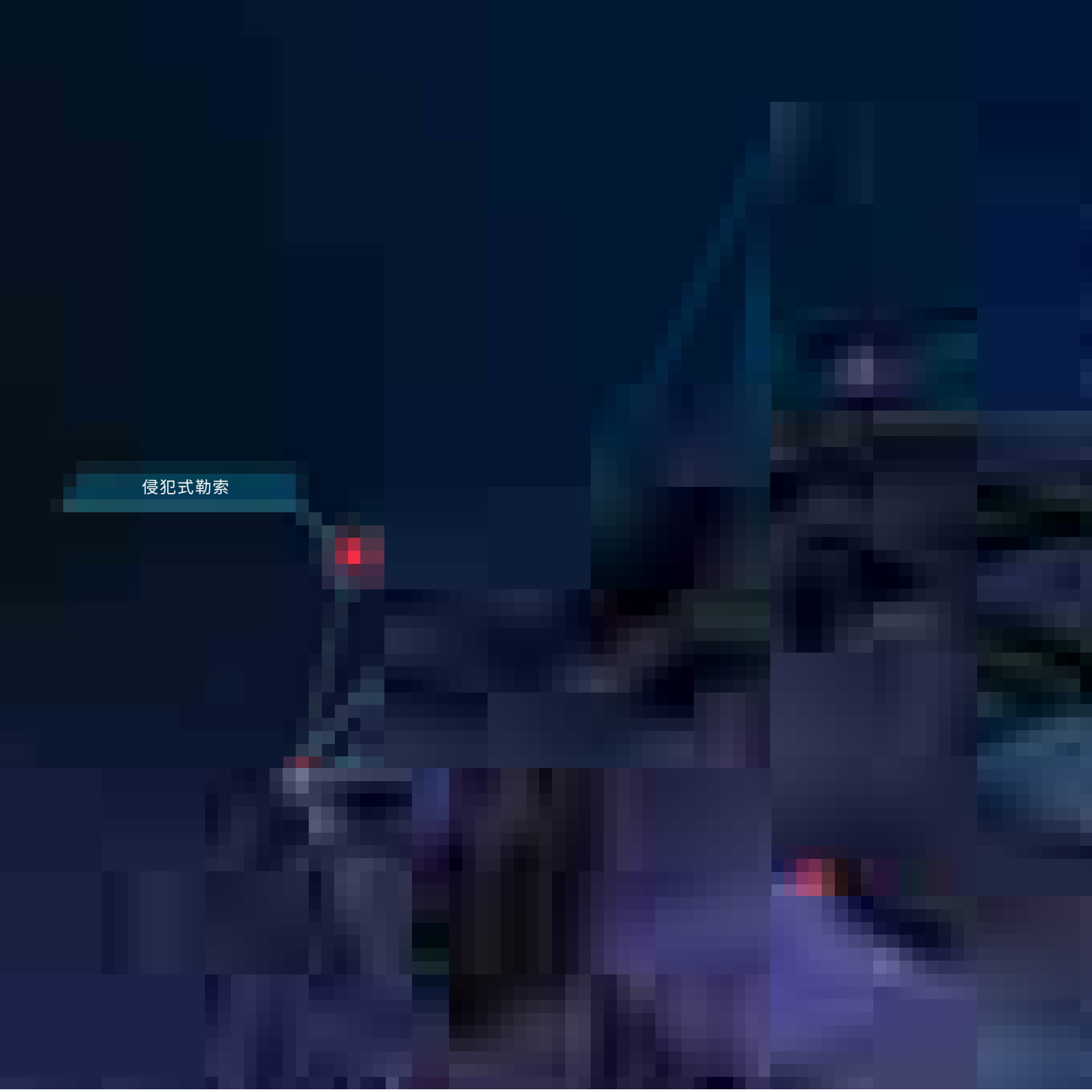
結論

據報導，多年來北韓進行了各種非法金融活動來資助該政權。加密貨幣的爆炸性成長正在與積極和持久的北韓網路能力彙聚，自然使至少一些北韓威脅組織會將行動延伸到該領域。APT38、TEMP.Hermit 和 UNC1130 等 DPRK 發動者持續表現出願意探索新的方式來入侵不斷發展的加密貨幣生態系統，而 Mandiant 在 2022 年對 DPRK 活動趨勢的分析也加強了這一點。由於 DPRK 行動在為網路活動提供資金和支援政權方面取得了巨大成功，這些專注的工作將有可能在整個 2023 年繼續有增無減。Mandiant 追蹤的許多 DPRK 威脅組織已經將目標鎖定加密貨幣，或以某種形式使用加密貨幣。這種潛在目標的延伸為其他部門的網路防禦者提供了機會，讓他們能夠獲得有關北韓戰術、技術與程式的寶貴見解。

北韓人員在不透露其真實國籍的情況下謀求就業的努力滿足了該政權的戰略需求，同時也給目標群組織帶來了巨大風險。除了為政權提供資金外，這些人員還會洩露敏感和專有資訊、引入漏洞，或促進網路入侵。就業企圖也會將 DPRK 利益傳遞給網路防禦者，從而提供準備視窗。

Mandiant 於 2023 年 3 月將 UNC1130 升級成 APT43。完整的 APT43 報告可從 https://www.mandiant.com/resources/blog/apt43-north-korea-cybercrime-espionage 下載取得





2022 年變化的重點和不常見的技術帶來的威脅發動者成功

2022 年，調查了一系列了知名的入侵事件，儘管這些事件嚴重偏離常見的威脅發動者行為，但是這些入侵仍然取得成功，並對受攻擊的目標群組織產生影響。雖然與 Mandiant 定期調查的政府資助與犯罪威脅發動者相比，威脅發動者展現出的技術複雜性相對較低，但對目標群組織的影響不成比例。這些事件強調了願意避開潛在交戰規則持久型對手給組織造成的威脅。Mandiant 觀察到威脅發動者利用地下網路犯罪市場中可用的資料、巧妙的社交工程計畫，甚至還用賄賂在執行入侵和帳戶接管。此外，這些對手錶現出與他們的目標進行個人接觸的意願，對他們中的許多人進行欺凌和威脅。

2022 年初，一群網路犯罪分子開始針對高知名度的大型國際公司，其入侵經常引起轟動，從而成為新聞頭條。該組織被 Mandiant 追蹤為 UNC3661，並被公開稱為「Lapsus」，在目標群組織內開展了各種惡意活動。UNC3661 最初以南美洲的組織為目標，但很快將範圍擴大到包含全球組織。UNC3661 開展的入侵導致原始程式碼、智慧財產被盜，並在多個例項中造成重大聲譽損害。

儘管入侵造成的損害和範圍很廣，但 UNC3661 的動機並不僅限於經濟利益。實際上，他們在入侵期間的行動廣泛地表達了對惡名的渴望，而不是為了增加利潤而進行最佳化。UNC3661 經常要求公司將智慧財產作為開源發布，而不是根據其財務潛力而選擇目標，經常會在 Telegram 聊天中進行投票，以確定下一次要針對的組織。

最近，Mandiant 遇到了另一個被追蹤為 UNC3944 的組織，它表現出的特徵與 UNC3661 類似。UNC3944 是以金融為動機的威脅叢集，其活躍期可追溯至 2022 年 5 月，經常使用從 SMS 網路釣魚行動中獲得的被竊取憑證來獲取初始網路存取權限。在極少數情況下，隸屬於 UNC3944 的發動者參與了互動式社交工程行動，主動威脅個人，並嘗試賄賂個人，以獲取系統存取權限。

這兩個威脅叢集的一個共同主題是，在不依賴零時差、自訂惡意軟體或新工具的情況下，它們的入侵會產生過大的影響。組織務必要瞭解這種新的、更加直言不諱的威脅的潛在後果，並相應地調整保護和預期。

初步入侵

UNC3661 和 UNC3944 都依賴被竊取憑證和巧妙的社交工程的組合來獲取目標環境的出示存取權限。雖然 Mandiant 尚未確認額外的首次攻擊媒介，但 UNC3661 已經向內部人員徵求 VPN 憑證，而開源報告表明他們是透過網路釣魚電子郵件活動來獲取這些憑證。UNC3661 還使用被竊取的 cookie 來獲取目標群組織的網路存取權限。在接受記者採訪時，威脅發動者表示他們是從地下市場 Genesis Market 購買這些被竊取的 cookie。

Mandiant 觀察到 UNC3661 使用被竊取或非法的憑證來對組織的 VPN 基礎設施進行驗證，並管理社交工程活動，以在多因素驗證 (MFA) 平台中註冊新裝置。UNC3944 也利用有效憑證進行驗證；然而，當遇到 MFA 限制時，他們會對幫助台操作員進行社交工程，以啟用訂閱者身分模組 (SIM) 交換攻擊並註冊新手機。SIM 交換允許將現有手機的服務轉移到新的手機。威脅組織可以使用 SIM 卡交換攔截 MFA 驗證訊息，從而劫持 SMS 訊息。

四處走動，然後離開

一旦植入到組織的網路，UNC3661 和 UNC3944 都喜歡使用他們已經獲得存取權限的各種端點上可用的工具。這種行動模式有時候被稱為「離地攻擊」，消除了攻擊者在將工具或惡意軟體運輸到環境時被偵測到的機會。同樣地，隨著威脅發動者在事前勘查或橫向移動期間採取的行動與已經在環境中很常見的活動相混合，偵測機會會進一步混淆。然而，在某些案例中，環境中已有的簡單工具是不夠的，Mandiant 觀察到 UN3944 和 UNC3661 多使用了更加複雜的工具。

UNC3944 通常會依賴虛擬機器器 (VM) 來實現入侵後的任務目標。在一個例項中，威脅組織在利用 MFA 漏洞後，在 Citrix 桌面上安裝了 VMware，隨後使用 VM 在被入侵的網路中執行大規模的內部事前勘查活動。Mandiant 還確認了證據表明，UNC3944 獲取了組織的 Azure 入口網站存取，並建立了設定為接受來自外部攻擊者控制的 IP 位址遠端桌面通訊協定 (RDP) 連接的 VM。透過遠端連接到 Azure VM，攻擊者濫用了存取控制政策，使其能從 Azure 租戶進入客戶網路。UNC3944 對 VM 的使用也提供了部分的反鑑識功能。如果 UNC3944 刪除了 VM，它們就創造了必須從網路內部收集次要觀察的證據。

UNC3944 還非常小心地確保，即使它們從網路中被刪除，它們也能夠透過各種技術重新獲得存取權限。雖然它們通常會避免使用持久性後門，但為了重新獲取存取權限的工作仍然有效。例如，UNC3944 能夠濫用各種密碼重設服務，如 ServiceNow 和 ManageEngine 來重設已經修補的帳戶密碼。利用帳戶在修補期間已經成功重設並接受保護這一假設，UNC3944 不用冒著在新攻擊中被偵測的風險，而是會因其持續存取目標環境而獲得回報。

相比之下，UNC3661 會使用 Mimikatz 或 Impacket 等常見惡意軟體來在需要的時候為憑證收集提供援助。Mandiant 確認了證據表明，UNC3661 使用這兩種工具來存取組織的 ntds.dit，以及執行 DCSync 行動。Mandiant 還觀察到 UNC3661 使用 Mandiant 追蹤為 DOUBLEJUMP 的公共公用程式來入侵 CVE-2022-21919，從而提升環境內的權限。CVE-2022-21919 是 Windows User Profile Service 追蹤的漏洞，被入侵時，能在 NT AUTHORITY\SYSTEM 使用者情景下執行惡意 DLL。

雖然 UNC3661 有時能夠利用作業系統弱點和漏洞來提升權限，該組織更喜歡的技術是使用已經提升權限的被竊取憑證。Mandiant 觀察到絕大多數與 UNC3661 有關的橫向移動都是在 RDP 上使用有效憑證發生，而且威脅組織已經證明能夠將目標對準環境所有者認為安全的憑證資料商店。Mandiant 觀察到 UNC3661 存取內部資料、傳訊平台及管理系統，它們對其進行了嚴格的純文字憑證和存取權杖搜尋。

兩個組織之間的一個共同主題是在它們入侵的環境中將目標鎖定端點偵測和回應 (EDR) 能力。UNC3661 和 UNC3944 都採取積極措施，在可能的情況下移除 EDR 工具，以限制對其活動的可見性。Mandiant 觀察到 UNC3661 使用 ProcessHacker 來獲取在端點上停用 EDR 服務所需的權限，儘管它們也會在需要的時候依靠簡單地解除安裝服務。UNC3944 別觀察到使用簡單又有效的定制惡意軟體來在端點上停用 EDR 服務，以便阻止偵測並禁止修補活動。

使事情私人化

多年來，網路犯罪中出現了一種隱含的專業化趨勢，令人驚訝。勒索軟體操作者很早就瞭解到，在協商勒索需求和協調解密時，不良的客戶服務會影響他們的營收。在網路間諜活動領域行動的威脅組織很少（如果有的話）與他們的目標群組織的員工進行除社交工程或魚叉式網路釣魚之外的互動。另一方面，UNC3661 和 UNC3944 不惜成本去騷擾，並在某些情況下恐嚇他們所入侵組織的成員。通常，這些爆發與修補活動同時發生，使攻擊者的進展被逆轉，但同樣常見的是，這種戰術是為了服務勒索需求而部署的。在一個案例中，UNC3944 透過變更全球地址清單中的頭銜來針對組織的個別員工，在另一個案例中，使用各種內部工具向員工發送淫穢垃圾訊息。UNC3661 甚至加入了被入侵組織員工舉行的電話會議，以推動向勒索需求屈服。UNC3661 還厚顏無恥地使用相同的通訊平台向資安和營運團隊告知在環境內進行的破壞性行動。

雖然在網路犯罪從勒索軟體到多方面敲詐行動的演變過程中，與目標群組織成員的直接互動有所增加，但 UNC3661 和 UNC3944 等組織所進行的互動則完全不同。這些組織展示的活動更多地說明了金融動機與對惡名之渴望的融合。

汲取的經驗教訓

Lapsus 和 UNC3944 之間的共同點很簡單；兩個組織都意識到與針對端點相比，針對憑證與帳戶有什麼價值。儘管缺乏成熟度和複雜性，但是這兩個組織都能獲得具有成熟資安組織的大型實體存取權限。這兩個組織都忽視了在網路上建立據點的想法，而是專注於針對合法個人用戶的存取權限和帳戶。

除了針對憑證而不是端點，還有另一個更加險惡的執行緒將這些發動者綁定在一起。UNC3944 和 UNC3661 在入侵期間都有意將高管和權限管理員作為目標，並且帶有威脅、強迫或以其他方式刺激這些高高優先順序員工支付贖金或向發動者的需求屈服的個人意圖。這種以威脅和其他惡意活動針對個人的有意意願構成了攻擊面的演變；現在，個人及其家人被視為惡意發動者從入侵中牟利過程中的嘲弄物件。為了應對這種演變飛躍，防禦者應擴大其對「攻擊面」的定義，並考慮為員工提供保護可能會成為保護組織免受惡意發動者侵害的必要組成部分。

在短期內，組織將不得不與威脅發動者抗衡，這些發動者會尋找新的方式，透過社交工程和商品資訊竊取器組合，以及針對其內部資料儲存的資訊收集行動來竊取使用者身分身分資訊。隨著 MFA 變得更加常見，攻擊者會尋找新的方式，在不依賴惡意軟體的情況下繞過 MFA。短期內身分和存取管理 (IAM) 系統預計也會出現同樣的情況，因為攻擊者和研究人員都在探索此類平台提供的功能。

尤其是，政府和執法部門為破壞和組織勒索軟體行動而採取的行動可能會導致其他發動者將其重點轉向資料竊取和勒索行動。近期為追回勒索軟體贖金、發出起訴書和進行逮捕而採取的行動，以及加密貨幣市場的戲劇性衰退期，可能會消除網路犯罪使用勒索軟體的一些動機。雖然其他組織可能會比 UNC3661 和 UNC3944 更加複雜，但它們的惡名和有效性可能會激勵使用許多相同戰術的後續攻擊。當組織準備並努力安置他們的資安團隊和基礎設施時，留意防範簡單又持久的攻擊者應該是其設計目標的一部分。

紅隊案例研究

Mandiant 紅隊演練幫助組織評估他們的安全計畫應對現實世界攻擊場景的能力，並改善其安全態勢。Mandiant 與從金融機構到製造商到全球醫療保健公司在內的各種客戶合作。

本文章中概述的場景反映了一家大型公共事業公司擔心工地辦公室被入侵，從而使攻擊者能夠獲得關鍵雲端和營運技術 (OT) 環境資源的存取權限。他們請求 Mandiant 嘗試在 Azure 中獲取全球管理員存取權限，並測試其軟體發展生命週期 (SDLC) 控制的有效性，從而幫助他們評估此次風險。

初步破壞

Mandiant 觀察到威脅組織使用非傳統社交工程管道，包括透過 WhatsApp 和 LinkedIn 等平台，以及使用 SMS 和語音網路釣魚（電話釣魚）來將使用者作為目標。基於客戶的威脅模型，紅隊以電話釣魚活動將目標鎖定分公司辦公室。使用基於以雲端為基礎的服務，他們建立了一個自訂呼叫中心，其電話號碼與客戶自己的 IT 幫助台號碼類似。這意味著來自該號碼的來電呼叫者 ID 看起來會很熟悉，而且任何回電的分公司辦公室都不太可能會認為該號碼看起來可疑。

紅隊打電話給幾個分公司辦公室的接待處，安排預約「技術人員」到現場安裝一些新的軟體。實際上，「技術人員」可能是 Mandiant 員工，而「軟體」則是 Mandiant 建立的自訂惡意軟體，用於遠端存取網路，同時透過防禦性控制來規避偵測。透過自訂呼叫中心設定，來電被路由給一群紅隊成員。後續通話似乎是由不同的呼叫代理接聽，為回電確認或提出進一步問題的目標創造了令人信服的展示。

一旦分公司辦公室確認了預約，紅隊就會指派該區域內的顧問在當週拜訪該辦公室。顧問帶著徽章抵達現場，徽章內容是根據紅隊在開源情報收集 (OSINT) 期間收集到的員工徽章圖像編織而成。區域辦公室內的客戶員工為紅隊操作員提供了每個工作站的無監督存取權限。操作員使用該存取權限在每台機器上安裝了 Mandiant 的自訂命令與控制 (C2) 惡意軟體，確保如果裝置透過執行「COM 劫持」攻擊而重新開機，惡意軟體也會重新開機。這種持久性技術涉及修改 Windows 註冊表，以引導使用 Microsoft 元件物件模型 (COM) 的應用程式載入惡意程式碼，而不是合法二進位檔。

橫向移動到 Azure

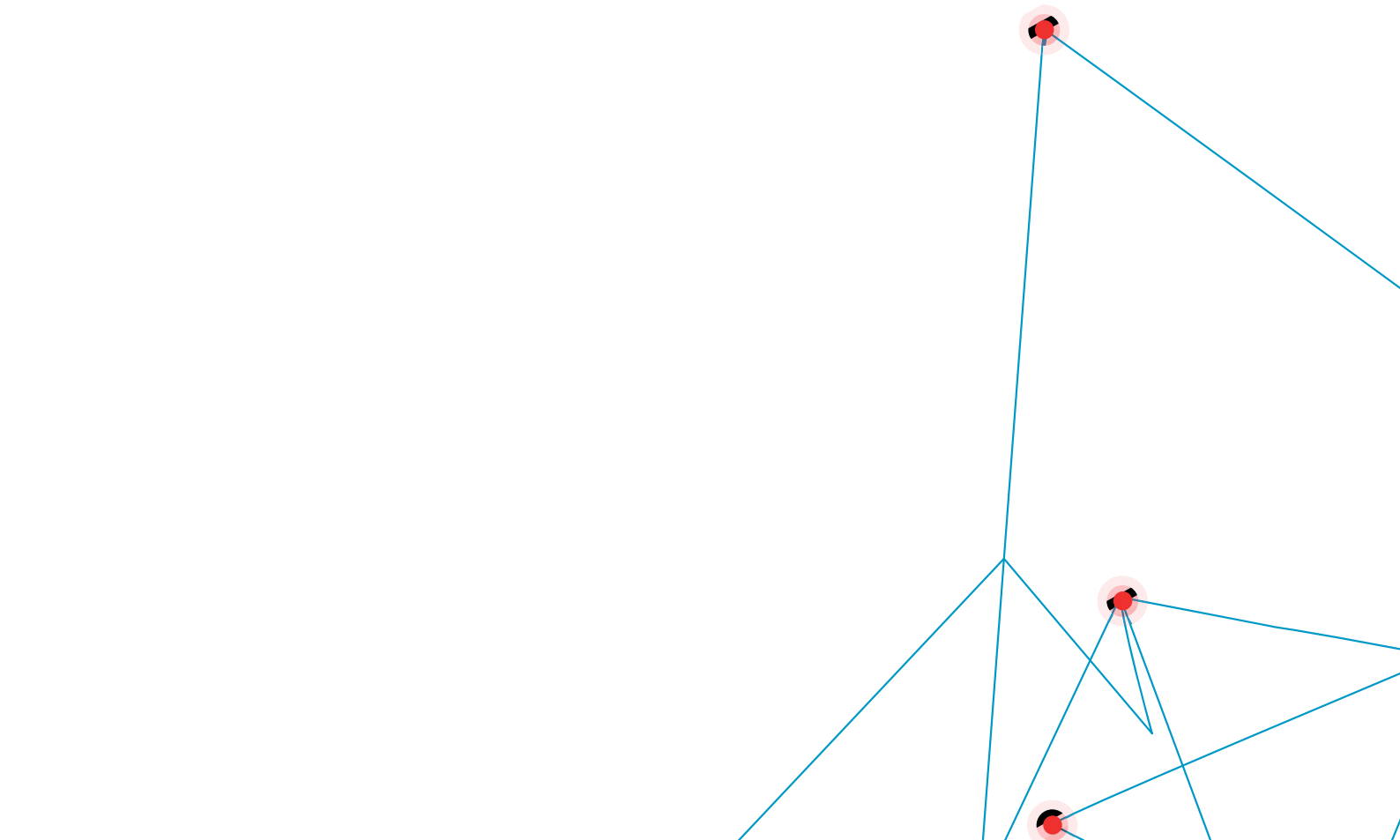
紅隊獲得了客戶內部網路的存取權限，但尚未取得他們可以用來在內部網路中行動的任何內部使用者憑證。Mandiant 諮詢了客戶的內部網域控制站的 Kerberos 服務，並取得了數千個有效使用者名稱清單。該使用者名稱清單隨後被用於針對客戶的 Azure 雲端基礎設施的密碼噴灑攻擊。密碼噴灑攻擊與傳統的暴力密碼猜測攻擊不同，在後者中，攻擊者會在每個帳戶上嘗試數千個密碼，以期找到有效的憑證。在密碼噴灑攻擊中，攻擊者反而會嘗試用多個使用者帳戶的一個常見密碼登入。Mandiant 使用內部工具執行了攻擊，而該內部工具會使用 API Gateway 來嘗試對每隔 25 次嘗試後輪轉的無法追蹤 IP 位址進行驗證。

密碼噴灑攻擊與暴力密碼攻擊相比更難偵測。我們很經常看到環境使用的政策會在一定數量的失敗嘗試後將帳戶鎖定，但密碼噴灑攻擊不會觸發這種鎖定。由於單個帳戶僅嘗試一次，因此確認密碼噴灑攻擊的最常見方式是對單個 IP 位址的失敗驗證數量進行統計分析。為了避免這種偵測，Mandiant 設定了一個捲動的 IP 位址集區（請求可能會源自這些地址），並在一定數量的請求後變更了源地址。使用這種技術，Mandiant 能夠確認使用常見密碼的多個帳戶，包括幾個百都使用相同密碼的帳戶。以往，Mandiant 在為新帳戶或密碼重設後配置預設密碼的組織中觀察到這一現象。Mandiant 隨後使用所收集到的憑證來針對常見服務，而這可能會提供關於組織的進一步見解或甚至存取權限。

SharePoint 和 Outlook 等服務通常託管在 Azure 中，是名副其實的敏感性資料寶藏庫。雖然 Mandiant 確實持有多組有效的憑證，但是客戶已經將多因素驗證 (MFA) 設定為存取最常用服務的一項要求。然而，Microsoft Graph API 尚未設定相同的要求。使用 Microsoft Graph API，Mandiant 列舉了更多關於目標環境組織結構的資訊，以及租戶的條件式存取原則。Mandiant 對條件式存取原則的分析揭露了存在一組免於 MFA 的帳戶。透過以進一步的密碼噴灑攻擊來攻擊這些帳戶，Mandiant 能夠收集額外的憑證，使其能存取更大範圍的服務，無需嘗試繞過 MFA。

攻擊密碼管理員解決方案

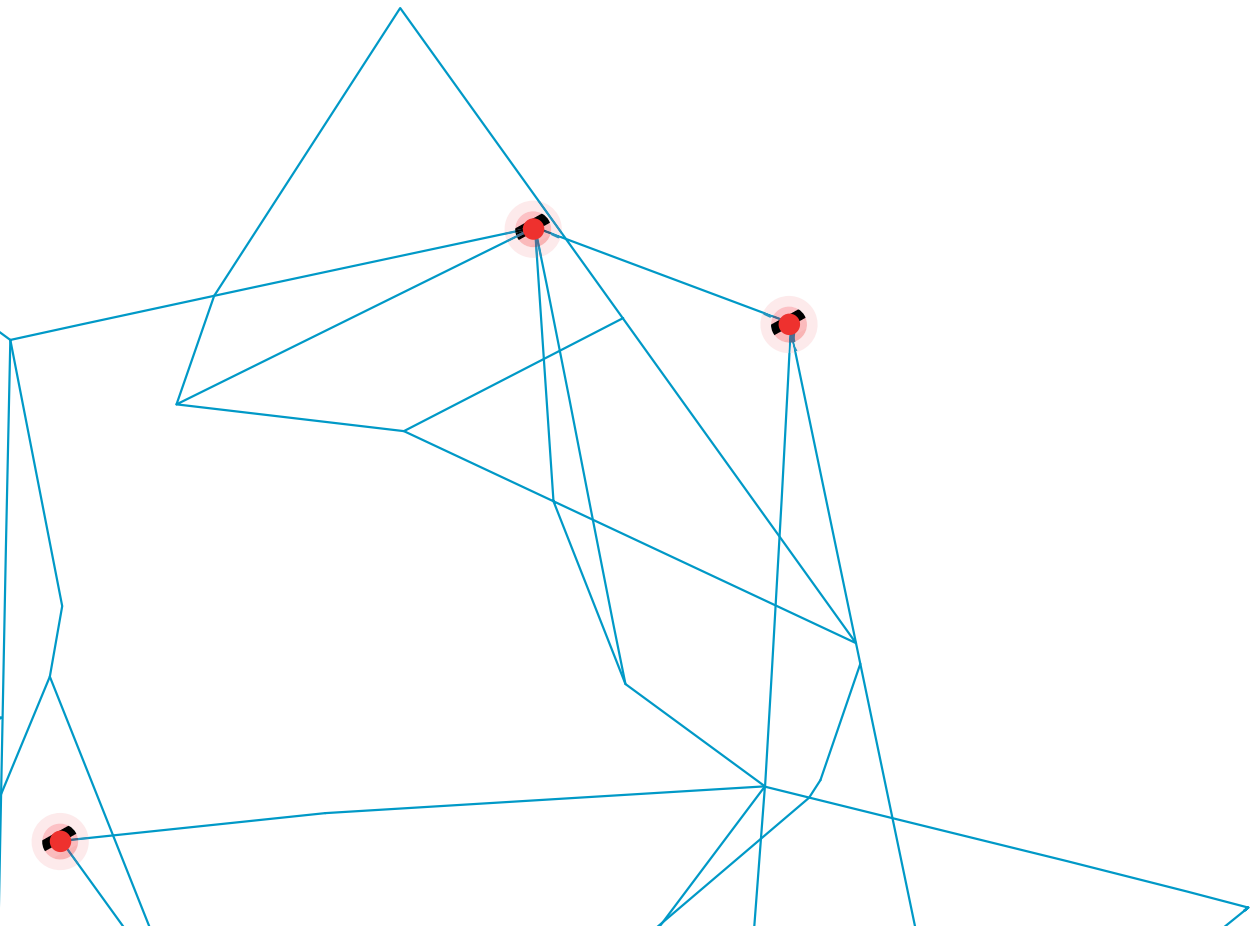
Mandiant 現在可以存取分公司辦公室現場差不多數十個端點的存取權限，以及 Azure 存取權限。在其中一個端點上，Mandiant 確認了熱門密碼管理員軟體 KeePass 使用的加密資料庫檔案。雖然資料庫使用強式密碼加密，但 KeePass 設定檔案的存取權限並不安全。透過修改設定檔案，Mandiant 使用 KeePass 中的漏洞在 KeePass 用戶端中建立惡意觸發程式。每次解密 KeePass 密碼資料庫時，被解密的密碼會被寫入檔案。一旦使用者解鎖資料庫，且未加密密碼被寫入檔案，Mandiant 會擷取檔案，從 KeePass 中移除觸發程式，並刪除檔案。在未加密密碼中，Mandiant 確認了用戶端環境內幾個關鍵系統的管理憑證，包括用於存取敏感 OT 網路和內部伺服器的跳轉框。Mandiant 使用這些憑證來橫向移動，並在相關機器上安裝惡意軟體。在一個例項中，一個網域系統管理員登入了其中一個伺服器，而 Mandiant 使用 NanoDump 在沒別偵測到的情況下從記憶體中擷取其憑證。NanoDump 是一個複雜的工具，實施的功能與眾所週知的 Mimikatz 公用程式類似，但包含的進階選項和功能可以透過防毒 (AV) 和端點偵測和回應 (EDR) 解決方案幫助規避偵測。



在 Azure 內獲得可視性

雖然 Mandiant 處理了有效的網域管理員憑證，但是限制了管理帳戶存取權限的條件式存取原則被證明是一個障礙。然而，大量的內部網域事前勘查揭露了存在幾個內建 Microsoft On-Line (MSOL) 帳戶，這些帳戶被用來將內部部署活動目錄和 Azure 活動目錄相同步。如果具有充足權限的攻擊者可以獲取執行同步的系統存取權限，則攻擊者有可能擷取純文字的 MSOL 帳戶憑證。MSOL 帳戶權限因部署選項而異，但通常包括 Azure 內的全域讀取者角色。借助全域讀取者角色，帳戶具有租戶內所有資源與特性的可見性。此外，由於 MSOL 是一個服務帳戶，它通常被排除在具有條件式存取原則的 MFA 執行之外。

Mandiant 使用了網域管理員憑證來在執行同步的網域控制站上獲取工作階段。Mandiant 使用僅在記憶體中運作的開源工具收集純文字 MSOL 帳戶密碼。



權限提升至全球管理員權限

Mandiant 擁有存取權限的 MSOL 帳戶是 Azure 內提升權限的完美位置，因為它具有雲端內所有資源的可見性。Mandiant 透過 C2 植入程式代理瀏覽器流量，以使用 MSOL 帳戶憑證直接存取 Azure 入口網站，收集關於租戶的應用程式、使用者及組織等級體系的寶貴資訊。Mandiant 能夠確認，雖然客戶為所有權限帳戶實施了強條件式存取原則，但是 MSOL 帳戶並未受到限制。

Mandiant 確認 Microsoft Office 365 應用程式在 Azure 內具有全球管理員角色。如果 Mandiant 可以確認有權向 Microsoft Office 365 應用程式新增擁有者的內部部署服務帳戶，那麼它就能提供一條通往全球管理員角色的路徑。使用此漏洞的一個關鍵條件是易受攻擊的使用者為內部部署帳戶，而不是僅存在於 Azure AD 中的帳戶。Mandiant 對網域管理員的存取權限可以建立通常被稱為任何同步內部部署帳戶的銀級票證。銀級票證讓攻擊者能夠為一項能在傳遞票證攻擊中使用之服務的授予票券服務 (TGS) 票券。負責 AD 和 Azure AD 同步的系統機器雜湊用於簽署 Azure 網頁入口網站驗證的票證。在該例項中，Mandiant 為一個具有向 Microsoft Office 365 應用程式新增擁有者的內部部署服務帳戶偽造了票證。一旦在具有 Azure 入口網站存取權限的瀏覽器工作階段內載入了銀級票證，Mandiant 會將編輯帳戶新增為 Microsoft Office 365 應用程式的擁有者。借助對服務原則 (SP) 的完全所有權，Azure 內的使用者可以透過為 SP 建立證書或憑證來奪取服務的身分。Mandiant 能夠冒充 Microsoft Office 365 SP 並獲取與全球管理員角色相關的所有權限。

攻擊軟體發展生命週期(SDLC)

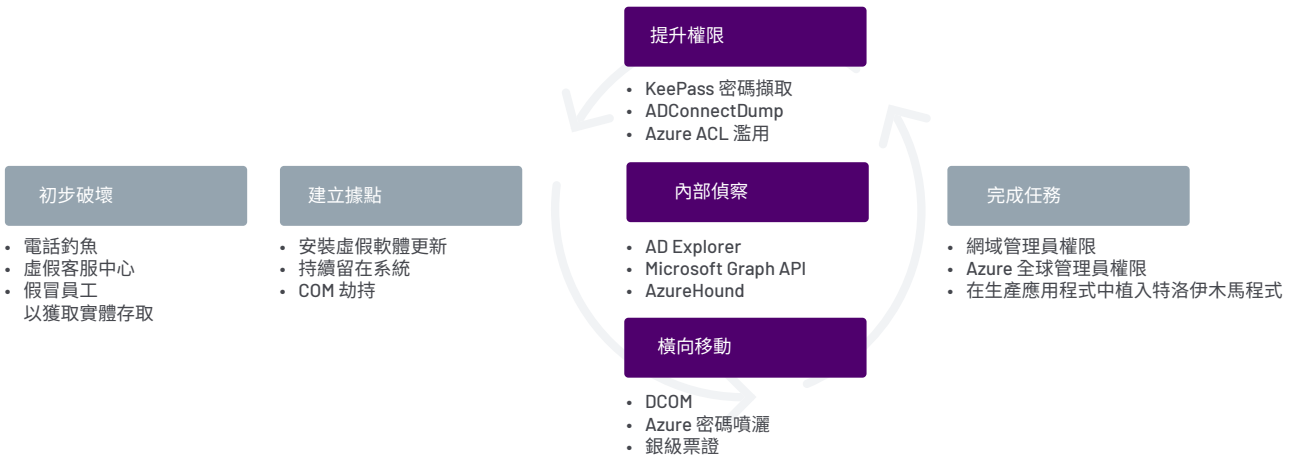
在獲得客戶環境的完全全球管理員存取權限後，Mandiant 已經準備好應對演練的終極目標，即透過將惡意程式碼注入應用程式來對客戶的 SDLC 植入病毒。客戶環境內的許多業務程序透過自訂應用程式執行。Mandiant 將目標鎖定基於 JavaScript 的內部網頁應用程式，該應用程式通常會包含在內部應用程式中，以產生與技術支援人員的聊天提示。聊天提示的程式碼託管在 Azure Blob 儲存空間內，允許儲存文字、圖像、視聽元件，甚至還有二進位大型物件(BLOB)等非結構化資料。這種架構提供了必要的手段，Mandiant 可以透過這種手段來對儲存了聊天提示 JavaScript 原始程式碼的 Blob 儲存空間植入病毒。

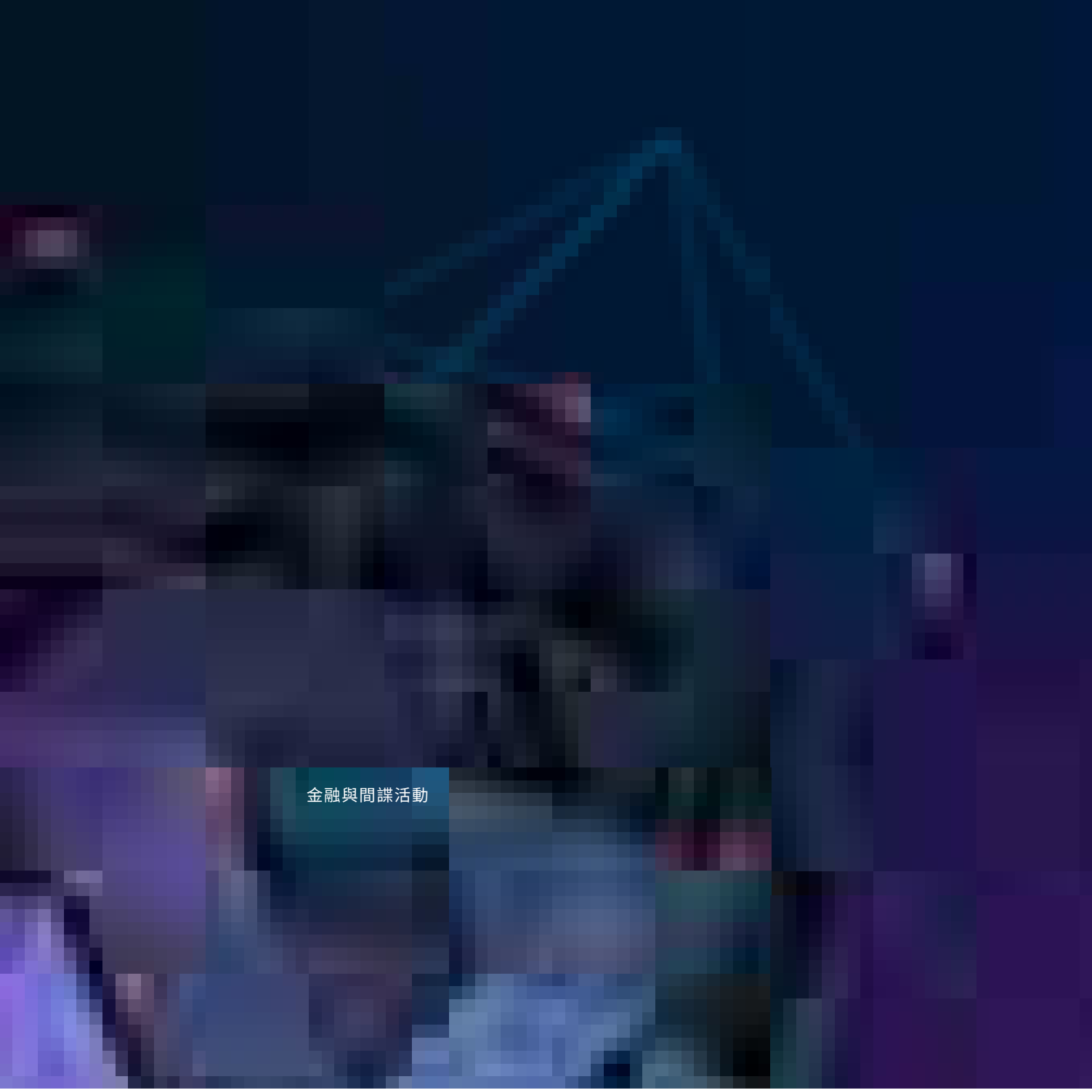
Mandiant 與客戶合作設計了一個後門程式，該後門會提供逼真的概念驗證示範，且不會破壞使用聊天提示的應用程式。注入 JavaScript 原始程式碼的惡意程式碼會傳播到多個內部應用程式，從而啟動符合用戶端設定的參數的狀態變更過。造訪客戶網路內數十個被被影響的網路應用程式中任意一個的使用者會將被植入病毒的 JavaScript 程式碼載入他們的瀏覽器工作階段。大量的內部監控和變更控制系統允許及早偵測植入的程式碼，而客戶的資安團隊在 15 分鐘內就將變更恢復，並重新開機其事件回應程序。

結果

不斷演化的網路安全態勢不斷為防禦者和攻擊者帶來新的挑戰。威脅發動者不斷創新他們的社交工程方法，而這反過來又促使資安人員為其使用者制定更好的保護和訓練。連接到雲端的混合內部部署網路在資安方面帶來了獨特的挑戰，需要進行大量的規劃和操作變化才能解決，而攻擊者的操作沒有類似限制，並且僅受其目標指引。同樣地，多層身分管理和應用程式部署為必須嚴密看管的客戶環境建立了新的垂直度。隨著雲端服務遷移的實施和設計階段滿足業務營運的嚴峻現實，錯誤設定的出現並不少見。組織應考慮測試其雲端架構部署，以提高抵禦有動機、敏捷對手的能力。

針對性攻擊生命週期對應





2022 年活動與全球事件

Mandiant 在前線調查、分析公開報告、資訊分享及其他研究期間獲取了關於威脅發動者的知識。2022 年，Mandiant Intelligence 成立了活動與全球事件 (CGE) 團隊來揭露高影響、多目標入侵活動，並向防禦者提供可行的威脅情報。每個活動或全球事件概況都包含入侵指標、值得注意的對手主機命令，以及關於威脅發動者使用的戰術、技術與程序 (TTP) 的深度分析與背景資料，以及 MITRE ATT&CK 框架對應。透過提供與背景資料和分析相結合的資訊，防禦者能夠更高效地回應這些威脅。

活動 —— 威脅發動者

2022 年，Mandiant 防禦者回應了從國家資助的間諜活動和以金融為動機的勒索行動在內的極具影響力的活動。Mandiant 防禦者與涉及被入侵的 USB 及其他外部裝置的多個活動正面交鋒，這些裝置都在目標環境內廣泛傳播惡意軟體。這些活動的確認為 Mandiant 服務提供了可行的資料，用以建立新的即時偵測、制定和延伸現有的威脅獵捕任務，並建立高保真度自動遏制指南，以便在新興威脅活動開始時隔離受影響的系統。2022 年，在 CGE 團隊追蹤的最值得注意的活動中，APT29、BASTA 勒索軟體操作員及使用基於 USB 的惡意軟體的威脅組織提供了透過該計畫，將複雜的威脅發動者活動提煉為可行情報的例證。

APT29

APT29 是一個網路間諜活動威脅組織，它使用創新的 TTP 來攻擊歐洲和北美洲的人道主義組織、智庫、國防部門及外交機構。繼 2022 年初俄羅斯和烏克蘭之間的緊張局勢之後，Mandiant 成立了烏克蘭危機資源中心，以監控更廣泛的社區，並使其做好準備應對可能會增加的俄羅斯網路活動。該中心為客戶和社區提供寶貴的資源，以主動加強其環境對破壞性攻擊的抵禦能力，強調俄羅斯資訊行動，並提供俄羅斯網路能力概觀。考慮到歷史上俄羅斯針對烏克蘭和西方目標的活動，Mandiant 通知該社區，俄羅斯各種網路威脅組織的報復行動疑似有所增加。該通知包括對能源、金融和運輸部門等高價值產業之各種破壞性影響的展望，以及值得注意的威脅組織和每個組織值得注意的技術。

2022 年，Mandiant 繼續透過非傳統部門追蹤 APT29 的目標群組織，以保持不被偵測並實現其任務目標。2022 年 1 月，俄羅斯入侵烏克蘭約一個月前，APT29 發起了針對主要位於歐洲地區的外交實體的網路釣魚活動。在接下來幾個月內，APT29 繼續以的獨特的戰術針對私有部門內的多個組織，特別專注於獲取電子郵件地址。Mandiant 發起了兩個活動，追蹤特定 APT29 活動。

亮點活動

APT29 開展針對多個國家政府機構的網路釣魚活動

APT29 發送的網路釣魚電子郵件旨在偽裝成與目標群組織有關的大使館相關的行政通知。網路釣魚電子郵件使用了合法但被增選的電子郵件地址來發送包含惡意附件的電子郵件。這些附件最終導致了使用合法服務進行命令和控制 (C2) 的後門程式。以往，APT29 大量使用從第三方雲端服務擷取 BEACON 的植入程式。Mandiant 在 2022 年 2 月觀察到作業轉變，當時 APT29 開始部署依賴於增選基礎設施的更簡單植入程式。

APT29 以 QUIETEXIT 隧道程式攻擊組織

APT29 的第二波活動針對了多個組織，該組織透過被入侵的視訊會議錄影機（主要為 LifeSize TelePresence 裝置）代理了他們的流量。APT29 部署了 QUIETEXIT 隧道程式來路由透過被入侵環境的流量。QUIETEXIT 是公開可用的 Dropbear 軟體的修改版本，可以提供 SSH 逆向 shell。APT29 精心將目標鎖定一部分特定的信箱 將注意力集中在涉及公司發展、兼併與收購、大規模業務交易，以及 IT 安全的高管團隊和關鍵員工。該組織使用被入侵的權限交換帳戶的使用者名稱和密碼來獲得存取權限，並使用「GetFolder」和「FindFolder」請求來列舉感興趣的信箱。透過對目的檔案夾使用「FindItem」查詢篩選器，APT29 能夠收集自上次資料開採以來建立的所有信箱項目。

展望

APT29 是高度活躍和複雜的威脅組織，在全球範圍內開展了無數知名的入侵事件。最值得注意的是，影響了全球各地政府和企業的 SolarWinds 供應鏈入侵已經被 Mandiant 歸因於 APT29。在整個 2022 年，隨著俄羅斯持續入侵烏克蘭，APT29 的行動集中在歐洲外交實體，幾乎肯定是為了滿足俄羅斯的持續情報優先任務，即西方對戰爭的回應及提供給烏克蘭的經濟與軍事援助。隨著戰爭進入第二年，西方政府加深支援烏克蘭的承諾，俄羅斯可能會加強這些網路間諜活動，以便收集情報，並塑造俄羅斯在烏克蘭和全球各地的姿態。

APT29 透過使用進階端點偵測緩解技術，以及在某些活動中使用有效載荷一次性加密，將 C2 有效載荷可用性降到最低，從而持續改進和監控其行動，最大限度地提高效率和規避偵測。隨著它們試圖避免偵測和完成其任務，APT29 的入侵技術將有可能會繼續。

BASTA 勒索軟體

2022 年中，Mandiant 觀察到疑似位於東歐的威脅發動者以金融為動機的的活動發生了重大轉變。隨著公開報導的增加及對隸屬於 CONTI 的發動者的審查增加，BASTA（亦稱為 BlackBasta）勒索軟體出現了。CONTI 操作者發展了一個多產的犯罪集團，該集團積極利用勒索軟體來勒索受害者。當時，Mandiant 懷疑 BASTA 是由 CONTI 勒索軟體操作者和關聯組織改名而來，作為避免審查增加的合乎邏輯的後續步驟。Mandiant 發現的證據表明，至少有一個威脅發動者將 BASTA 勒索軟體整合到它們的他們的行動中，直接替換了 CONTI 勒索軟體。CONTI 行動於 2022 年 5 月下旬正式停止，而 BASTA 行動是在不久之前的 2022 年 4 月出現。Mandiant 建立了兩個活動來追蹤活躍的 BASTA 勒索軟體部署工作。

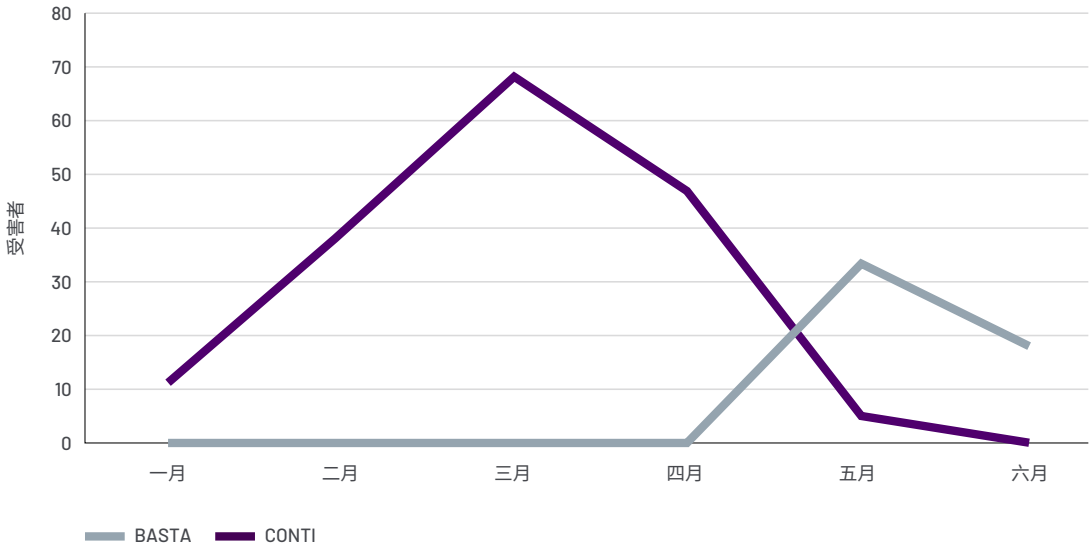


圖 2. 新增到 CONTI 和 BASTA DLS 網站的受害者（2022 年）

亮點活動

以金融為動機的發動者透過第三方獲取組織存取權限，從而部署 BASTA 勒索軟體並勒索受害者

六月，Mandiant 獲悉有有一次供應鏈入侵透過共用服務提供者託管的基礎設施影響了加拿大西部的信用社。雖然透過第三方獲取存取權限並非新鮮事，但這對勒索行動而言較為罕見。在其中一些案例中，負責的發動者（Mandiant 追蹤為 UNC3973）使用了 SYSTEMBC 隧道程式進行入侵後行動，並嘗試部署 BASTA 勒索軟體。利用集中存取，UNC3973 使用被入侵的 MSSP 和目標群組織之間共用的一個具有網域管理員權限的未經授權服務帳戶來獲取每個環境的存取權限。隨後，攻擊者使用了一批指令碼來嘗試停用防毒軟體，並建立了排程工作來部署 SYSTEMBC（一種透過受感染端點來代理流量的工具）。然而，系統的防毒軟體偵測到並隔離了 SYSTEMBC 二進位檔。為了進一步嘗試對網路進行勒索，攻擊者建立了一個 Windows 服務來啟動 BASTA 勒索軟體。幸運的是，無論 UNC3973 如何嘗試進行干擾，系統的端點防毒軟體仍然能夠偵測並隔離惡意軟體。

疑似以金融為動機的發動者透過 QAKBOT 獲取存取權限，以部署 BASTA 勒索軟體

2022 年 10 月，Mandiant 回應了多次入侵，在這些入侵中，攻擊者在進行大範圍的 QAKBOT 網路釣魚活動後部署了 BASTA 勒索軟體。Mandiant 觀察到發布威脅叢集 UNC2633 使用 QAKBOT 來獲取目標環境的初始存取。隨後，QAKBOT 入侵被用來向第二個威脅叢集 UNC4393 提供感興趣的環境的存取。隨後，UNC4393 繼續部署各種工具，包括 BEACON 和 SYSTEMBC 隧道程式，然後使用 Rclone 來從環境中竊取資料並部署 BASTA 勒索軟體。在一些案例中，UNC4393 僅在獲得存取後的幾天內就從其在環境中的存取獲利。這種快節奏與其他 CONTI 相關威脅叢集一致。以往，UNC2633 也經常與 Mandiant 在 CONTI 生態系統中追蹤到的叢集進行合作。

展望

Mandiant 繼續根據獨特的 TTP 來追蹤並建立勒索軟體活動叢集，以便評估地下罪犯的演變。雖然這兩個活動代表了 BASTA 勒索軟體的使用，但事件的組成部分闡明不同發動者是如何使用相同的勒索軟體變體完成任務。隨著執法工作繼續阻礙犯罪生態系統，勒索軟體操作員在迴圈使用勒索軟體變體執行任務時，改造了保持營運速度和一致性的方法。

基於 USB 的入侵導致以金融為動機和間諜活動相關威脅發動者活動

在整個 2022 年，Mandiant 觀察到一些活動涉及使用受感染的 USB 磁碟機和其他外部裝置來傳播惡意有效負載。負責的發動者包括以金融為動機的組織，該組織被認為與更大的 Evil Corp 生態系統，以及根據中國民族國家利益行事的間諜活動組織有關。作為回應，Mandiant 發起了多起活動來追蹤與基於 USB 的入侵有關的活動與威脅叢集。

亮點活動

未知動機發動這種透過受感染的 USB 磁碟機分發 BIRDBAIT

該活動涉及執行由 Mandiant 追蹤為 UNC3840 的威脅叢集從基於 USB 的存儲媒介傳播的蠕蟲。該蠕蟲會建立並啟動一個包含內建命令的快捷方式檔案，該命令會執行 Windows Standard Installer 二進位 Msiexec.exe 來下載並執行遠端託管的有效載荷。Mandiant 觀察到一個包含 BIRDBAIT LNK 下載程式、DENSEDROP 和 DENSELAUNC 的惡意軟體鏈。DENSEDROP 是一個高度混淆的 PE 32 位元記憶體中植入程式，最終會啟動 DENSELAUNCH，一個 C++ Win32 DLL 載入程式，能將任意程式碼寫入指定的程序記憶體空間。尤其是，在 UNC3840 使用 BIRDBAIT LNK 下載程式的事件中，C2 基礎設施通常會解析似乎為被入侵網路連接儲存 (NAS) 裝置的 IP 位址。

在活動初期，幾乎沒有證據表明在部署 DENSELAUNCH 和 DENSEDROP 之後有重大後續活動，但在整個 2022 年對活動的追蹤導致確認了 FRUITBIRD 等額外的惡意程式碼系列。DENSEDROP 在滿足多項環境檢查後推出的 FRUITBIRD 很有可能被用來分發額外的有效負載，包括惡意軟體、廣告軟體及 HOLA VPN 安裝程式。該活動表明，UNC3840 背後的威脅發動者可能在利用其惡意軟體作為安裝付費 (PPI) 服務，為其他威脅發動者提供入侵媒介。

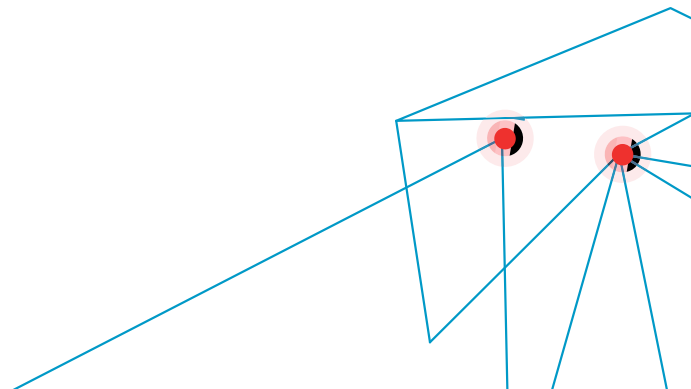
雖然 Mandiant 對 UNC3840 行動的瞭解有限，但是 UNC3840 非常有可能在分發有效負載，並向多個第三方提供安裝付費存取等服務。Mandiant 對 UNC3840 和其他以金融為動機的威脅發動者使用的惡意軟體的分析揭露了與其他追蹤的叢集可能存在重疊。這些重疊包括在分發 URSNIF 的活動中使用封包程式，以使用 LONGFALL 加密程式（亦稱為 CryptOne），各種惡意程式碼系列都使用過該加密程式，包括與 Evil Corp 相關的系列。Mandiant 觀察到在少量案例中，在 UNC3840 感染後部署了 FAKEUPDATES 惡意軟體。經常使用 FAKEUPDATES 提供之存取權限的威脅發動者還包含與 Evil Corp 重疊。

使用那個包含 URI 的命令列參數啟動的 Msiexec.exe 處理程式的確認被證明是偵測可能存在惡意有效負載之下載的有效方式。Mandiant 確認後來被叢集到 UNC3840 下的活動早在 2021 年 9 月就已經發生了。

與中國有關的涉嫌間諜活動發動者透過受感染的 USB 裝置傳播惡意軟體

Mandiant 確認了追蹤為 UNC4191 的惡意活動針對公共和私有部門，這些部門主要位於東南亞，還有美國、歐洲和大洋洲。該活動於 2022 年 4 月開始，並持續一整年，同時還使用受感染的 USB 裝置作為活動的首次感染媒介。在成功的感染中，惡意軟體部署包括啟動程式 MISTCLOAK 和 BLUEHAZE，後者執行 ncat 網路公用程式副本來建立反向 shell 到硬編碼網域。Mandiant 還確認了 DARKDEW 植入程式的證據，該植入程式能夠從氣隙系統上收集檔案，並透過感染連接的可攜式磁碟機來進行進一步傳播。Mandiant 懷疑這一活動表明中國行動旨在獲取和保持公共和私有部門的存取權限，以便收集情報，支援中國的戰略性政治與商業利益。基於與 TWOPIPE 植入程式的惡意軟體相似性，有跡象表明 UNC4191 活動與中國有關的行動相關，而這些行動又與追蹤為 UNC53 的發動者有關。UNC53 亦稱為 TEMP.Hex，是一個多產的威脅發動者，以全球範圍內的公共和私有部門組織為目標，並且疑似與中國國家安全部有關。

在最初發現 UNC4191 活動之後，Mandiant 在多個組織內確認了使用 MISTCLOAK、DARKDEW 和 BLUEHAZE 進行入侵的證據。在分析人員對受影響的系統進行試驗並通知客戶的過程中，Mandiant 確認了一種目標鎖定模式，該模式受影響的系統都位於菲律賓。這為 Mandiant 觀察到的與各種中國網路間諜活動一致的區域目標鎖定提供了更多背景資料。



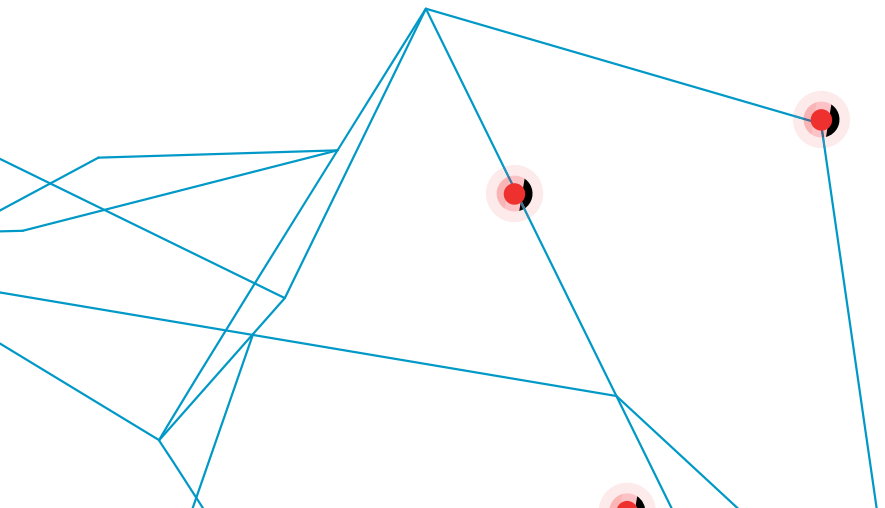
疑似與中國有關的間諜活動組織開展 USB 行動

在整個 2022 年，Mandiant 觀察到疑似與中國有關的發動者 UNC53 針對全球各地的各種產業。在某些案例中，UNC53 透過受感染的 USB 磁碟機獲取目標環境的初始存取，利用合法二進位檔來側載惡意 DLL 並加密植入 SOGU 變體的有效負載。該活動可能是獲取全球多個部門存取權限並從中收集戰略資料之長期工作的一部分，涉及該 SOGU 變體的活動最早可追溯至 2020 年。此前觀察到的疑似與 UNC53 相關的行動還在 2021 年使用 SOGU 變體針對東南亞地區的多個部門。

Mandiant 開發了針對這些惡意程式碼系列的即時偵測特徵碼，以及專注於透過卸載式媒介確認惡意軟體複製的額外偵測內容。這些工作導致額外發現 UNC53 在多個組織內開展基於 USB 的入侵，同時還部署了 SOGU、KORPLUG 和 FLOOPYSTAMP。Mandiant 的偵測能力不僅導致越來越多的 UNC53 入侵被偵測到，還導致發現了不相關的蠕蟲感染。

展望

被入侵的卸載式裝置是獲取目標環境存取權限的有效技術，並導致了有影響力的入侵。以金融為動機的威脅發動者，以及負責為間諜活動而收集情報的威脅發動者都使用過這種首次感染媒介和傳播機制。威脅發動者受益於入侵偏離其預定目標一到兩度的系統，比如酒店業務辦公室和個人電腦，這些系統存在於組織的技術控制和監控之外。在沒有對可攜式磁碟機使用進行嚴格技術控制的情況下，這種接近性為威脅發動者提供持續的機會來獲取環境存取權限。



全球事件 —— 值得注意的漏洞

漏洞披露一直是資安社群的重要支柱。隨著技術的發展、傳播並嵌入世界各地人們的生活，對這些技術內漏洞進行確認和負責任的披露有助於保護人們及其資料。漏洞的公開披露變得越來越常見，並引發了關於維護和修補的必要對話，不僅在技術領域，在公眾當中也是如此。多年來，評估潛在影響、保護行動並最終保護使用者資料和體驗的需求變得越來越重要。不出所料，每種類型的威脅發動者都吸取了類似的教訓。

隨著新漏洞被發現，通常會出現攻擊者是否已經在使用漏洞來實現其目標的問題。如果不存在資料來支援這麼一種想法，即已經有攻擊者成功使用該漏洞來攻擊組織，那麼這通常不是因為攻擊者缺少嘗試。由於解決新發布的漏洞的過程是一項成本效益分析工具，因此對使用者構成風險的漏洞對威脅發動者來說可能是一個不平等的機會。雖然行動團隊必須在可用性方面遵守服務等級協議，但是威脅發動者不會受到此類限制。如果系統管理員需要時間來測試和驗證修補程式，威脅發動者只需要概念驗證 (PoC) 程式碼中最基本的覆蓋範圍即可開始攻擊這些組織。

這種需要反應和攻擊機會的相互作用在 Mandiant 內產生了一個程序，我們稱之為「全球事件」。當披露的漏洞所造成的威脅足夠大，並且觀察到的惡意發動者嘗試在外入侵它時，Mandiant 會發起全球事件。在 2022 年披露和公布為 CVE 的超過 20,000 個漏洞中，Mandiant 根據各種評估標準發起了九個全球事件。在整個 2022 年，Mandiant 努力追蹤幾個重大漏洞的入侵事件，並為其提供偵測，包括 Log4Shell、Follina 及一系列影響 VMWare 的漏洞。

Log4Shell

2021 年 12 月 9 日，Lunasec 團隊公布了 Java 記錄框架中的漏洞 Log4j，並將其命名為 Log4Shell。在透過 Log4j 中的 Java 命名和目錄介面 (JNDI) 功能進行處理時，該漏洞允許透過惡意使用者輸入執行任意 Java 程式碼。負責 Log4j 專案的 Apache 在常見漏洞評分系統 (CVSS)，以及公布為 CVE-2021-44228 的漏洞打出了最高的 10 分。由於自 2013 年以來在 Log4j 中存在的漏洞 以及 Log4j 作為記錄框架的廣泛使用 ，對潛在影響的估計似乎很普遍，因此有必要審查全球產品和平台中的現有程式碼庫。根據 PoC 程式碼的公開可用性和入侵的細微性質，Mandiant 將與 Log4Shell 相關的風險評定為關鍵風險，並預測對該漏洞的入侵將要開始，並在強度和範圍上迅速擴大。Mandiant 於 2021 年 12 月 10 日針對 Log4Shell 發起了全球事件，並且由於所確認的入侵具有廣泛性質，將該事件延續到 2022 年。

有預測稱 Log4Shell 所帶來風險將是全球性的，而這種預測很快就被證明是準確的。Mandiant 觀察到，許多不同的威脅發動者在各種客戶當中進行了廣泛的掃描與入侵嘗試，從而導致部署了各種惡意軟體。在 PoC 程式碼公布後，幾乎沒有垂直產業（如果有）在幾乎不停的掃描和後續入侵嘗試中倖免於難。到全球事件工作流結束時，Mandiant 的指標集合中已經發布了 1,000 多個與 Log4Shell 的嘗試與成功入侵相關的 IP 位址。

Log4j 作為大型應用程式的支援函式庫無處不在，而這又使確保環境安全的工作變得更加複雜。雖然供應商優先考慮確認和修補易受攻擊的產品，但遺留產品對業務營運的連續性和它們所存在之環境的安全性都構成了巨大風險。使用 Log4j 的遺留應用程式的修補程式通常被延遲，或在某些情況下從來都不會提供。在遺留產品無法修補的情況下，組織依賴於需要定期維護和審查的重大緩解措施。Mandiant 建議對 Log4j 的任何易受攻擊版本採取隔離和監控形式的緩解措施。當組織對 Log4Shell 漏洞進行初始範圍界定時，無法離線的業務關鍵型產品可能會限制網路入口和出口，以便在尋求解決方案或替代選擇時限制風險。限制對受影響產品應用程式介面的存取有助於減少潛在的攻擊面，同時限制出口流量可以防止 Java 服務存取在入侵期間使用的惡意檔案。當與受影響產品的出埠 DNS 請求和入埠 HTTP 請求的監控和篩選相結合時，隨著 Log4Shell 入侵嘗試開始加劇，在近期內無法修補的組織將擁有相當於潛在影響的預警系統。

Log4Shell 的入侵遵循了大規模部署產品中高關鍵性漏洞的常見模式。投機性攻擊者快速透過漏洞攻擊組織，以便輕鬆取勝，並在大規模攻擊中安裝加密貨幣挖礦程式。然而，在短時間內，發動者將勒索軟體活動中的漏洞作為在更有價值的目標中取得初步據點的一種方式。雖然 Log4Shell 影響了從 Minecraft 到 Apple iCloud 在內的大量 Java 型平台，但是行動裝置管理平台 MobileIron 等服務在目標鎖定方面脫穎而出。Mandiant 觀察到 UNC961 等組織在漏洞發布後數日內就使用了 HTTP 標頭 Cookie 值內的 Log4Shell 漏洞。以金融為動機的威脅發動者 UNC961 以其利用漏洞的能力而著稱，而這些漏洞代表著廣泛的目標選擇機會，該組織也傾向於將網頁型攻擊作為初始存取的方式。UNC961 精心製作了針對 MobileIron 例項的惡意請求，一旦透過 Log4j 處理了請求，就會向威脅發動者提供逆向 shell 功能 。一旦在尋求於環境內建立持續性之前成功入侵，則 UNC961 會採取措施來阻礙鑑識分析。UNC961 還將從一個簡單的逆向 shell 轉變成 HOLEPUNCH 隧道程式的變體，能夠將連接多路傳輸回命令和控制節點。

最後，網路間諜活動組織爭分奪秒地入侵關鍵服務，包括使用 Log4j 來取得初步據點並朝著目標前進。Mandiant 觀察到中國國家贊助的間諜活動組織 APT41 以類似於 UNC961 的方式針對易受攻擊的 MobileIron 部署。APT41 被觀察到攻擊政府實體、電信公司及金融組織。同樣地，APT41 的入侵後活動包括防鑑定技術，以及從簡單的逆向 shell 轉向功能更豐富的後門程式。雖然在這些例項中，UNC961 和 APT41 等組織的方法存在相似之處，但這種差別主要是由環境的限制和 Log4Shell PoC 程式碼上的快速週轉時間所驅動的。

在全球事件期間，Mandiant 總共發布了 1,632 個威脅發動者 Log4Shell 活動相關指標。

Follina

在 2022 年三月下旬，Mandiant 觀察到多個疑似中國間諜活動叢集入侵 Microsoft 診斷工具 (MSDT) 中的零時差漏洞，使其能執行任意程式碼。該漏洞由 Microsoft 在 2022 年 5 月 30 日發布，其 CVE 識別字為 CVE-2022-30190，後來被稱為「Follina」。雖然該漏洞獲得了 7.8 的 CVSS 評分，但是它要求攻擊者精心製作一個特殊的 URL 來調用 MSDT，要求使用者在易受攻擊的系統上開啟它，而這又會影響 Mandiant 的「中等風險」評估。在 Microsoft 發布後，Mandiant 觀察到更多政府支援的威脅組織和以金融為動機的攻擊者入侵 Follina。

用於在這些行動期間提供 Follina 入侵的文件都可能都是透過魚叉式網路釣魚提供，而且根據文件建立日期和樣本提交，使用該漏洞的行動是從 2022 年三月下旬或四月上旬開始。儘管缺少廣泛的入侵，但是 Mandiant 觀察到 UNC3347、UNC3784 和 UNC3819 使用 Follina 漏洞來攻擊印度、尼泊爾、白俄羅斯、俄羅斯和菲律賓的組織。雖然這些威脅叢集各不相同，但所有三者都與疑似中國網路間諜活動有關。向涵蓋廣闊地理區域的多個中國威脅組織分發零時差入侵與支援中國網路間諜活動的集中式數字軍需官理論相一致。同樣地，惡意軟體在多個叢集的分布對歸因提出了挑戰，使之更難區分特定中國威脅組織活動。

俄羅斯和疑似中國間諜活動組織 UNC3784 和 APT28 在其攻擊政府組織的嘗試中使用了 Follina。2022 年 6 月初，APT28 使用密碼噴灑攻擊入侵了 EMEA 的一個政府組織，並使用被入侵的電子郵件帳戶來向烏克蘭的組織發送魚叉式網路釣魚電子郵件。UNC3784 針對東南亞地區的政府組織部署了後門程式和下載程式。

雖然入侵難度的提高可能限制了選擇性地攻擊目標的威脅組織對 Follina 的使用，但是 Mandiant 確實也觀察到為潛在的經濟利益而使用 Follina 的情況。Mandiant 追蹤為 UNC2633 的分發威脅叢集於 2022 年 6 月初開始使用 Follina 來提供後門程式 QAKBOT 的變體。UNC2633 歷來以廣泛的產業為目標，通常被視為勒索軟體行動的前兆。Mandiant 還觀察到在地下論壇中作業的威脅發動者推銷私人入侵方式，這些入侵方式使其他威脅發動者能使用 Follina。入侵程式碼的可用性意味著其他發動者可能會嘗試在未來活動中使用 Follina。

Mandiant 發布了 84 個 Follina 威脅發動者活動相關的指標。

VMware 漏洞鏈

2022 年 5 月 18 日，美國網路安全與基礎設施局 (CISA) 發布了一項緊急指令[4]，涉及威脅發動者鏈結 VMware 產品中的漏洞，以獲取目標系統的特權存取。VE-2022-22954、CVE-2022-22960、CVE-2022-22972 和 CVE-2022-22973 等有問題的漏洞影響了多個 VMware 產品，而且一同使用時，可能會導致權限提升或遠端程式碼執行。具體而言，2022 年 4 月 6 日公布的 CVE-2022-22954 詳述了一個漏洞，該漏洞使攻擊者能在 VMware 的 Workspace ONE Access 產品的易受攻擊執行個體追蹤執行伺服器端範本注入。鑒於入侵程式碼的公開可用性及經確認的在外漏洞入侵，Mandiant 對 CVE-2022-22954 的分析提供了高風險評級。

CISA 的指令要求聯邦機構在廣泛入侵報告後緩解相關風險，並引發了對政府實體和私有組織潛在影響的猜測。鑒於 VMware 的普遍性，對漏洞的高度關注及對潛在入侵嘗試進行分類的嘗試，導致 Mandiant 在 2022 年 5 月 23 日發起了全球事件。早在 2022 年 4 月 8 日，即 VMware 披露漏洞兩天之後，Mandiant 就觀察到證據表明就存在成功的 CVE-2022-22954 入侵。初始入侵嘗試似乎透過存取 /etc/shadow 和 /etc/passwd 檔案而從易受攻擊的 VMware 應用程式成功傾印憑證。

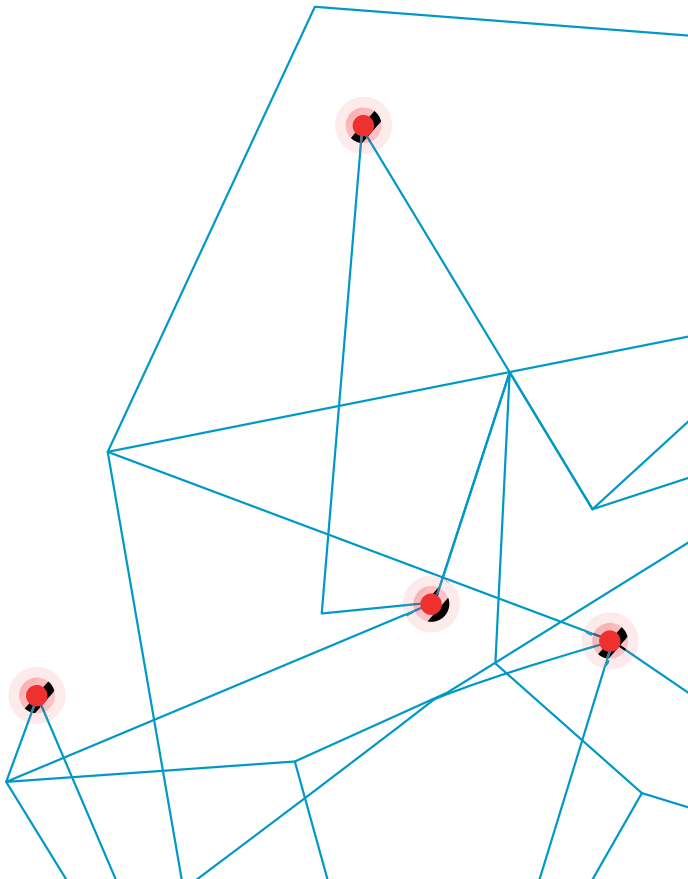
Mandiant 觀察到以金融為動機的攻擊者和疑似與俄羅斯有關的攻擊者使用 CVE-2022-22954。UNC3905 也入侵了該漏洞，該組織是個勒索軟體即服務關聯組織，已經對美國組織執行過資料洩露行動。至少有兩次提供了目標群組織存取權限的 UNC961 以易受攻擊的 VMware 應用程式為目標，並在 2022 年 4 月 16 日使用指令碼語言 Perl 從攻擊者控制的基礎設施下載第二階段惡意軟體。另一方面，威脅叢集 UNC3711 和疑似俄羅斯威脅發動者 UNC3810 似乎因國際行動而使用了 CVE-2022-22954。早在 2022 年 4 月 19 日，就觀察到 UNC3711 和 UNC3810 利用該漏洞來向烏克蘭組織提供破壞性惡意軟體。

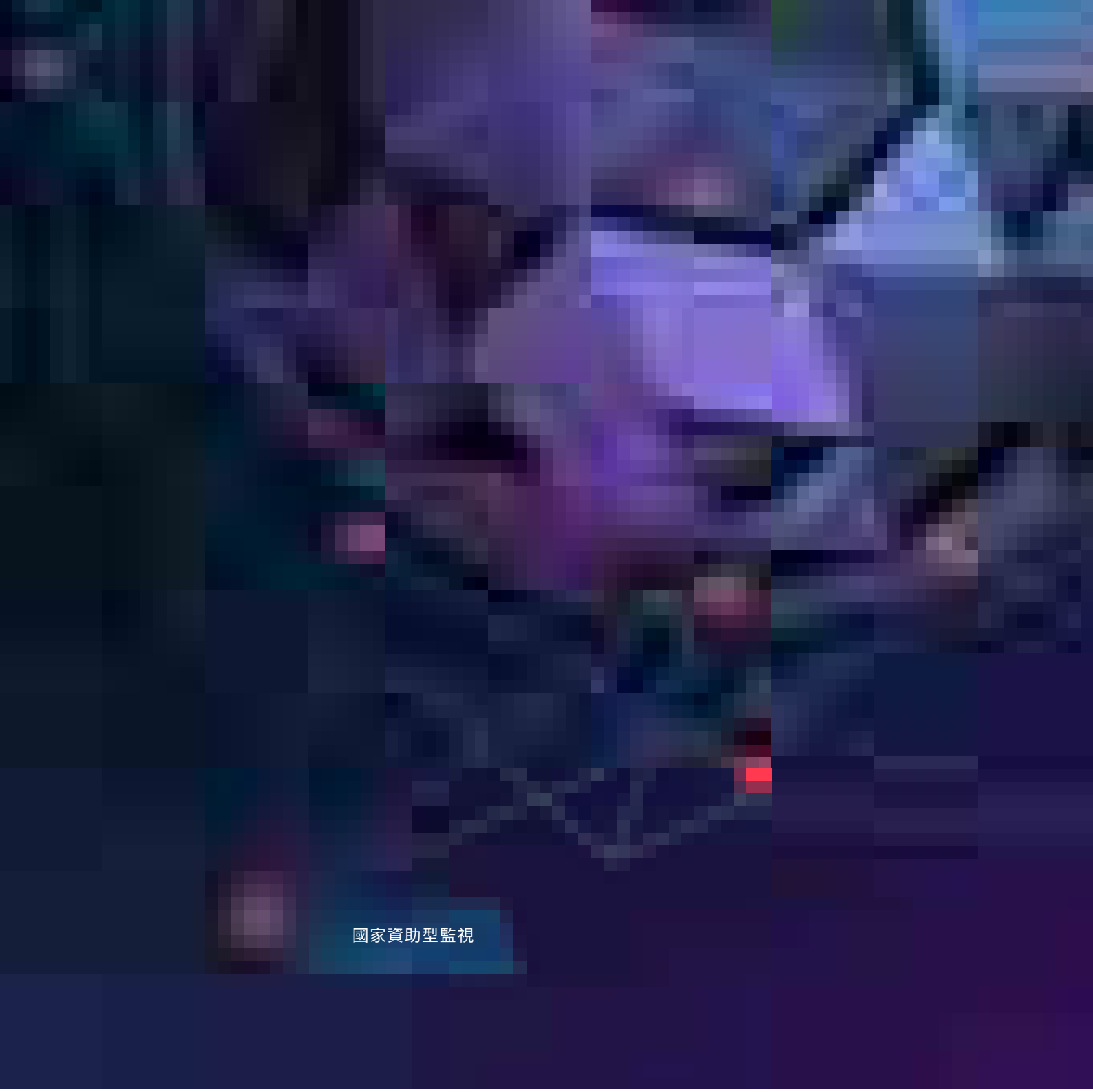
在全球事件期間，Mandiant 發布了 67 個 IP 位址、七個 URL 及兩個與觀察到的攻擊者活動相關的檔案雜湊，以幫助組織嘗試對其潛在入侵嘗試進行分類。

結論

每個資安組織都明白，在維護業務營運時，有太多的威脅發動者和漏洞需要追蹤、緩解或以其他方式解決。組織必須使用資料驅動的方法，根據相對風險和現場情報確定安全工作的優先順序。Mandiant 的活動與全球事件計畫旨在集中處理威脅發動者活動的可行指標，以幫助組織確認有可能會影響多個組織的活動。雖然追蹤威脅發動者的活動和追蹤潛在漏洞入侵的全球事件略有不同，但這二者背後的意圖都是為了能夠有效地確認影響組織的入侵。

Mandiant 組建了來自威脅情報、鑑識、事件回應服務等領域的跨職能團隊，以整合從活動或全球事件範圍內一系列有影響的入侵開始時可用的盡可能多的資訊。活動和全球事件貢獻者的任務是評估對組織的潛在影響，收集和評估新情報，以及開發和部署新偵測。向潛在受害者提供情報分析使他們能夠就如何及在何時實施安全措施做出更明智的決定。Mandiant 的 Managed Defense 服務既有助於為聚合的全球事件帶來威脅情報，也有助於從其中擷取威脅情報，以直接保護客戶網路，而且在許多情況下，能在客戶受威脅影響之前提供分析。





值得注意和最近升級的威脅組織

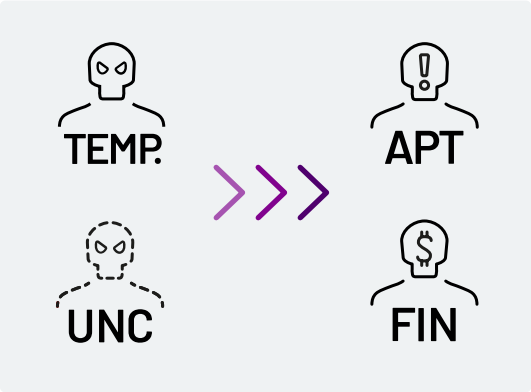
威脅叢集如何成為給 APT 或 FIN 組織

Mandiant 分析人員審查了各種來源的威脅活動資料，例如 Mandiant 事件回應接洽、Managed Defense 調查，以及資安產品遙測資料，以確認值得注意的叢集。當有足夠的活動，但沒有足夠證據來立即將其歸因於現有的威脅發動者或組織，Mandiant 會建立一個未分類 (UNC) 威脅叢集來追蹤新確認的活動。

UNC（原稱為 TEMP）是一個網路活動叢集，包含對手基礎設施、工具和間諜情報技術等可觀察的人工製品。UNC 是以通常在單一事件中發現的定義性、錨固特性為基礎。例如，一個常見的錨定是連接到發動者控制網域的惡意軟體樣本。

隨著我們對威脅叢集的知識不斷成熟，我們可能會將其提升為進階持續性威脅 (APT) 組織或以金融為動機 (FIN) 的組織。APT 組織通常以專注間諜活動行動為特徵，而 FIN 組織的特徵為專注於透過了勒索軟體部署、支付卡資料盜竊或業務電子郵件入侵等方式的牟利活動的犯罪行動。

2022 年，Mandiant 將一個追蹤的威脅叢集從「TEMP」提升到「APT」。在本報告中，我們審查了伊朗相關間諜活動威脅組織 APT42。



APT42 進行高度鎖定的監視作業

2022 年 8 月 Mandiant 將 UNC788 提升為 APT42。APT42 的活躍期可追溯至至少 2015 年，是一個複雜的網路威脅組織，使用高度鎖定的魚叉式網路釣魚和社交工程技術開展間諜活動行動。APT42 有可能是基於符合組織的行動要求和優先事項的目標鎖定模式而代表伊斯蘭革命衛隊 (IRGC) 情報組織 (IRGC-IO) 運作，包括為該政權抵禦內部和外部威脅、追捕認知的國內敵人，以及與來自西方的「革命」思想對抗。

伊朗政權對手的全球目標鎖定

APT42 組織主要集中在中東地區，並且主要針對被視為伊朗政權對手的組織與個人。APT42 一直以西方智庫、研究人員、記者、現任西方政府官員、前伊朗政府官員，以及海外伊朗僑民為目標。

一些 APT42 相關活動表明，隨著伊朗的優先事項演變，該組織變更了其行動重點。隨著 2020 年 3 月 COVID-19 疫情爆發，Mandiant 觀察到一個轉變，包括將目標鎖定製藥產業的行動。在伊朗總統選舉之前，APT42 同樣將目標轉向國內和外國反對組織。

建立信任和融洽關係

APT42 經常嘗試透過冒充記者或研究人員，並在發送惡意連結之前與目標進行數日或數週的友好對話，從而與其目標建立融洽關係。在某些情況下，該組織滲透電子郵件帳戶，隨後以初始受害者的同事、熟人和親屬為目標。APT42 行動還包含憑證收集，以收集多因素驗證 (MFA) 程式碼來繞過驗證方法。

2021 年 3 月到 6 月期間，APT42 使用一個屬於美國智庫員工的被入侵電子郵件帳戶來攻擊其他智庫和學術組織的中東研究人員、參與中東和伊朗政策的美國政府官員、一位前伊朗政府官員，以及一個伊朗反對組織的高級成員。APT42 冒充一位知名記者要求採訪，並與初始目標接觸了 37 天，以獲得其信任，並最最終將他們引導到憑證收集頁面。

在其他情況下，APT42 提供了一個 Dropbox 連結，指向一個 PDF 檔案，裡面帶有通往憑證收集頁面的內建 URL 短連結。在從被入侵收件匣發送電子郵件後，他們嘗試從受害者的「已發送」資料夾中刪除訊息以掩蓋它們的蹤跡。他們還仔細嘗試存取其目標的個人電子郵件帳戶。APT42 透過擷取 SMS 型一次性密碼並設定雙因素身分驗證來繞過多因素驗證。

監視作業

APT42 還使用行動惡意軟體來監視感興趣的個人。目標包括那些與伊朗的綠色運動有關人士及其他政治目標。

APT42 還針對那些聲稱能夠提供可以繞過政府限制之工具的人。在監視作業期間，APT42 部署了 VINETHORN 和 PINEFLOWER Android 行動惡意軟體來追蹤受害者位置、錄製電話交談、存取視訊和圖像及擷取整個 SMS 收件匣。

自訂工具的使用

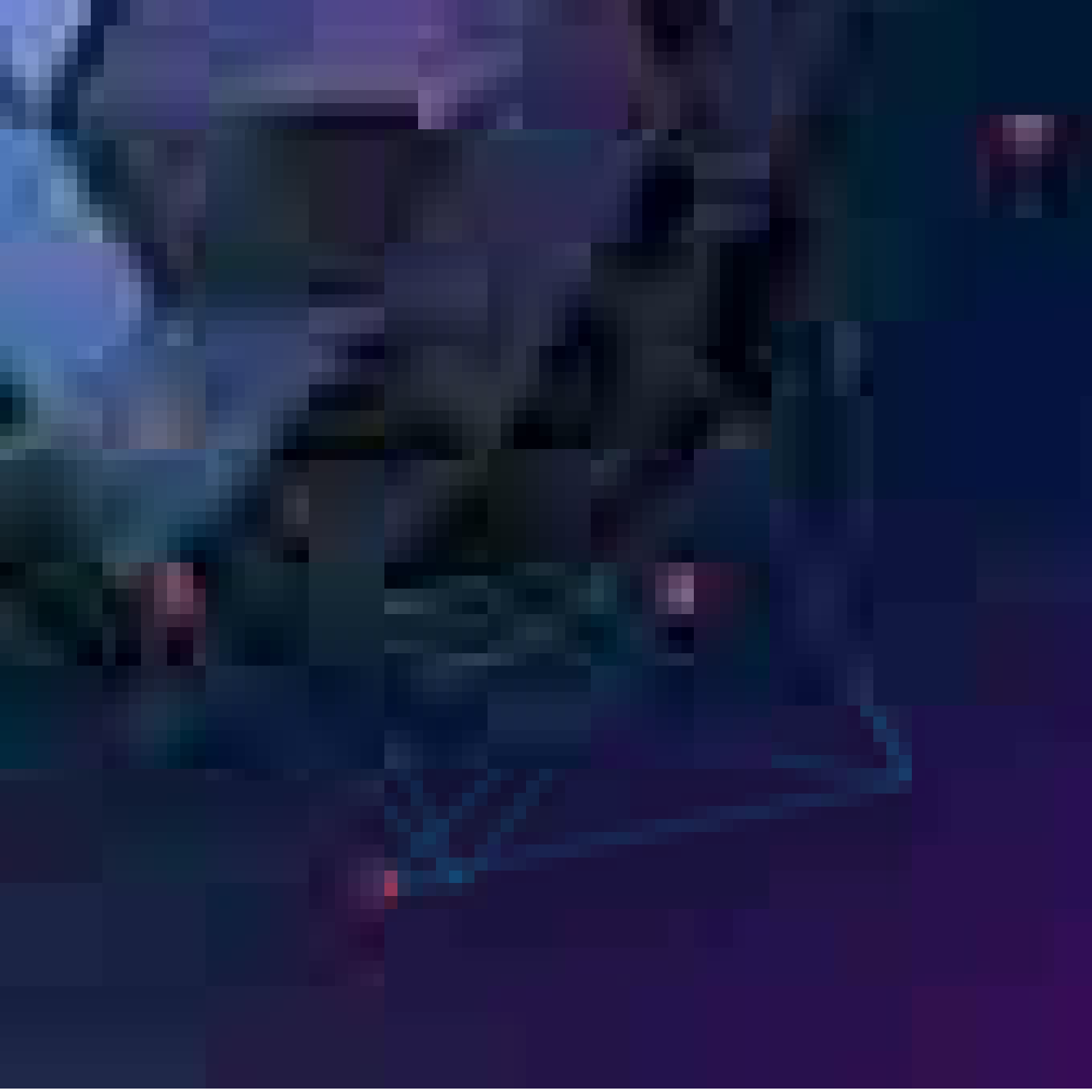
APT42 行動嚴重依賴憑證收集，但它們還使用好幾個自訂後門程式和工具。2021 年 9 月，APT42 使用了一個被入侵的歐洲政府電子郵件帳戶來向將近 150 個與世界各地的民間團體、政府或政府間組織雇用或有關聯的個人或實體相關電子郵件地址發送了網路釣魚電子郵件。該電子郵件聲稱與德黑蘭大使館的組織結構圖有關，並包含一個指向惡意巨集文件的連結，該文件可導致 TAMECAT 惡意軟體，一種 PowerShell 小立足點後門程式。

從 1 月到 3 月 22 日，APT42 使用了各種攻擊手法，包括在檔案分享平台上託管惡意 Office 檔案以提供魚叉式網路釣魚電子郵件，以及託管旨在擷取有效負載的惡意 PowerShell 程式碼，包括用於收集系統資訊和本機帳戶名稱的自訂事前勘查工具。

展望

APT42 活動從事伊朗相關專案的外交政策官員、評論員和記者構成威脅，尤其是在美國、英國和以色列地區。此外，該組織的監控活動也凸顯了個人目標面臨的現實風險，包括伊朗的雙重國籍人士、前政府官員，以及伊朗境內和之前離開該國的持不同政見者。

鑒於活動歷史悠久且不受基礎設施拆除和媒體報導影響，我們預計 APT42 的行動戰術和任務不會發生重大變化。儘管如此，隨著伊朗的優先事項隨著國內和地緣政治局勢的變化而不斷變化，該組織已經展示出迅速修改其行動重點的能力。



結論

在 M-Trends 2023 中，我們強調了偵測事件改善等積極趨勢，以及烏克蘭局勢和現實世界與網路世界融合等更具挑戰的趨勢。但這些並不是唯一的觀察與重點。

總體上，攻擊者並沒有放棄。實際上，我們看到攻擊者以更少的技能造成更大的影響。他們也更加無所顧忌，並且願意為了實現目標而變得更加激進和個人化。他們會欺凌和威脅，並忽視傳統的網路作業規則。如今，僅保護系統是不夠的，我們也需要保護員工。

為了確保我們的客戶免受最新且最相關的戰術、技術與程式影響，我們在紅隊演練中也採用了這些相同的無所顧忌的戰術。正如在我們的案例研究中所分享的，我們部分是透過偽裝成技術人員親自露面來獲取初始存取，這是一種大膽的戰術。我們看到人們越來越關注網路衛生，這很好，但組織必須繼續對各方面的安全保持警惕。

準備至關重要，但進行紅隊演練並非做好準備的唯一途徑。組織應考慮桌面演練、訓練練習及其他技巧。良好的基礎知識，如漏洞和暴露管理、最低權限和強化，也在構建強大的防禦中發揮作用。雲端考量因素也很重要。我們的紅隊案例研究證明了在與雲端相連的混合網路中，資安是多麼具有挑戰性。

Mandiant 的使命是確保每個組織都免受網路威脅，並對其準備就緒充滿信心。我們的活動與全球事件文章重點介紹了 Mandiant 如何分享有價值的情報和指標，以幫助我們的客戶和社群保護自身免受重大活動與漏洞的影響。

年度 M-Trends 報告以我們參與中的資料和學習成果為特色，在推進我們的任務方面也發揮重要作用。

任何網路防禦能力的核心都是驅動它的情報，而最好的威脅情報是直接從一線收集的。Mandiant 將繼續分享其在 M-Trends 中的前沿知識，以提高我們的集體安全意識、理解和能力，並確保組織能夠堅持不懈地進行網路安全工作。

參考書目

1.「Apaache Log4j 漏洞指南」。網路安全與基礎設施安全局，https://www.cisa.gov/news-events/news/apache-log4j-vulnerability-guidance

2.「威脅發動者使用 F5 BIG-IP CVE-2022-1388」。網路安全與基礎設施安全局，https://www.cisa.gov/news-events/ cybersecurity-advisories/aa22-138a

3.「威脅發動者鏈結未修補的 VMware 漏洞以實現全面系統控制」。網路安全與基礎設施安全局，https://www.cisa. gov/news-events/cybersecurity-advisories/aa22-138b

4. Vanderlee, Kelli。「DebUNCing 歸因：Mandiant 如何追蹤未分類的威脅發動者」。Mandiant，https://www.mandiant.com/resources/blog/how-mandiant-tracks-uncategorized-threat-actors

5. Franceschi-Bicchierai, Lorenzo。「FBI 指控北韓政府駭客在 Harmony 跨鏈橋盜竊案中竊取 1 億美元」。TechCrunch，https://techcrunch.com/2023/01/24/north-korea-fbi-harmony-horizon-crypto/

請前往 www.mandiant.com 瞭解更多資訊

Mandiant

11951 Freedom Dr, 6th Fl, Reston, VA
20190 (703) 935-1700
833.3MANDIANT (362.6342)
info@mandiant.com

關於 Mandiant

Mandiant 是動態網路防禦、威脅情報和事件應對服務等領域公認的領導者。Mandiant 透過拓展數十年的第一線經驗，幫助組織在抵禦及應對網路威脅上，對自己做好的準備抱有信心。Mandiant 現在是 Google Cloud 的一部分。

MANDIANT
現在是 Google Cloud 的一員