CLOUDFLARE

威脅報告

DDoS 攻擊威脅情勢

2022 年第二季 DDoS 趨勢

目錄

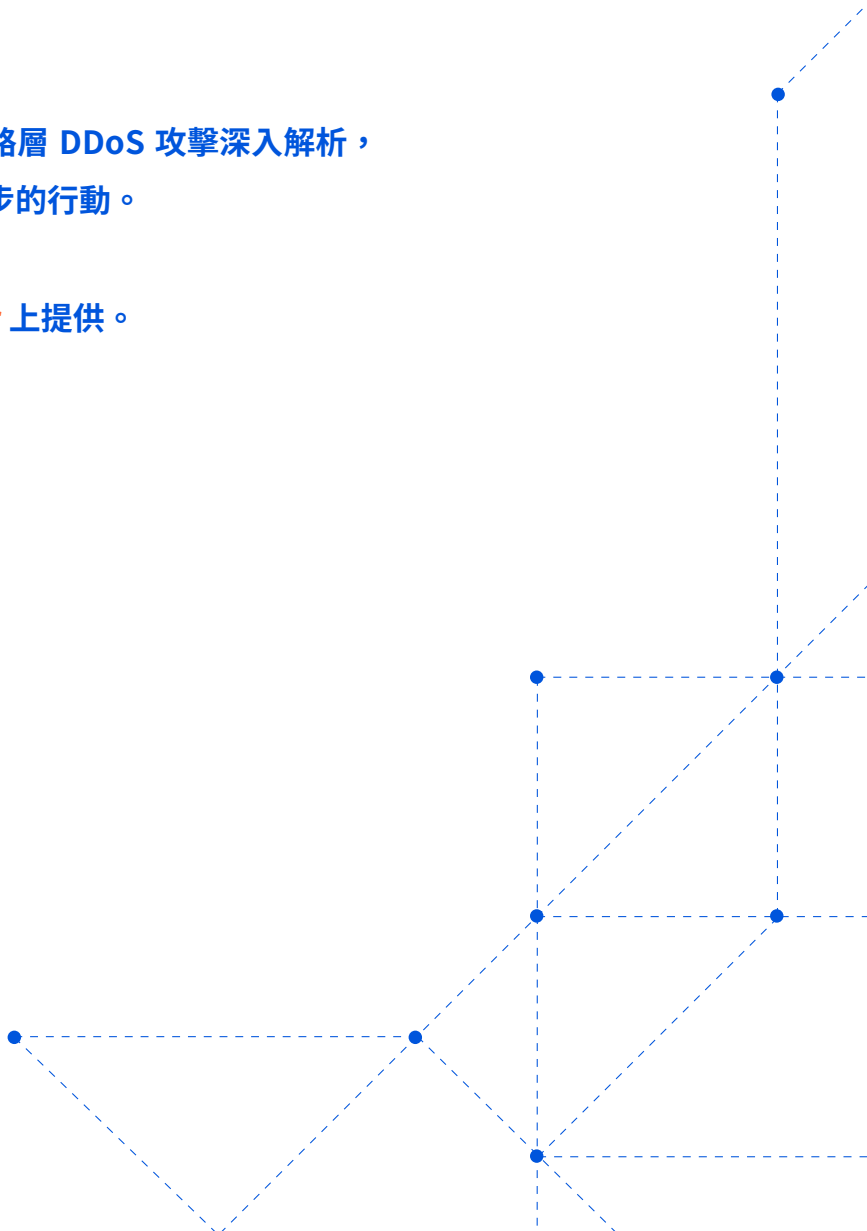
報告摘要

歡迎閱讀 Cloudflare DDoS 季度報告。本報告揭示了有關 2022 年第二季 DDoS 威脅情勢的深入解析與趨勢，這些資訊從全球 Cloudflare 網路中觀察所得。

在此期間，我們記錄了有史以來最大的一些攻擊，包括 Cloudflare 自動偵測並緩解的一次每秒 2,600 萬個請求的 HTTPS DDoS 攻擊。針對烏克蘭和俄羅斯的攻擊仍在繼續，同時又萌發了新的 DDoS 勒索攻擊活動。應用程式層及網路層攻擊數均在全面增長，並且產業和地理目標發生了顯著的變化。

在以下各節中，我們將概述應用程式層及網路層 DDoS 攻擊深入解析，以準備更好的應對之策，並告知各組織下一步的行動。

本報告的互動版本也會在 Cloudflare Radar 上提供。



重點內容

① 俄羅斯和烏克蘭網際網路

- 地面戰爭伴隨著針對資訊傳播的攻擊。
- 烏克蘭的廣播媒體公司成為第二季度 DDoS 攻擊的最大目標。事實上，前六大攻擊數最多的產業均為線上/網際網路媒體、出版業和廣播業。
- 另一方面，俄羅斯的線上媒體排名下降，在遭受攻擊較多的產業中位列第三。第二季度，俄羅斯的銀行、金融服務和保險業 (BFSI) 公司成為遭受攻擊最多的公司，躍居首位。
- 幾乎 45% 的應用程式層 DDoS 攻擊的目標都是 BFSI 產業。俄羅斯的加密貨幣公司遭受的攻擊數位列第二。

進一步瞭解 Cloudflare 如何讓開放式網際網路流量流入俄羅斯，同時避免向外展開攻擊。

② DDoS 勒索攻擊

- 我們觀察到新一波 DDoS 勒索攻擊，由自稱 Fancy Lazarus 的實體發出。
- 2022 年 6 月，勒索攻擊達到了今年以來的最高程度。每五名經歷過 DDoS 攻擊的調查受訪者中，就有一人報告受到 DDoS 勒索攻擊或其他威脅。
- 整體來說，第二季度的 DDoS 勒索攻擊數環比增長了 11%。

③ 應用程式層 DDoS 攻擊

- 第二季度，應用程式層 DDoS 攻擊數同比增長 72%。
- 位於美國的組織是此類攻擊的主要目標，其次是賽普勒斯、香港特別行政區及中國大陸。針對賽普勒斯組織的攻擊數環比增長 166%。
- 第二季度，航空和太空業遭受此類攻擊最多，其次是網際網路產業以及銀行、金融服務和保險業，而遊戲/博彩業位居第四。

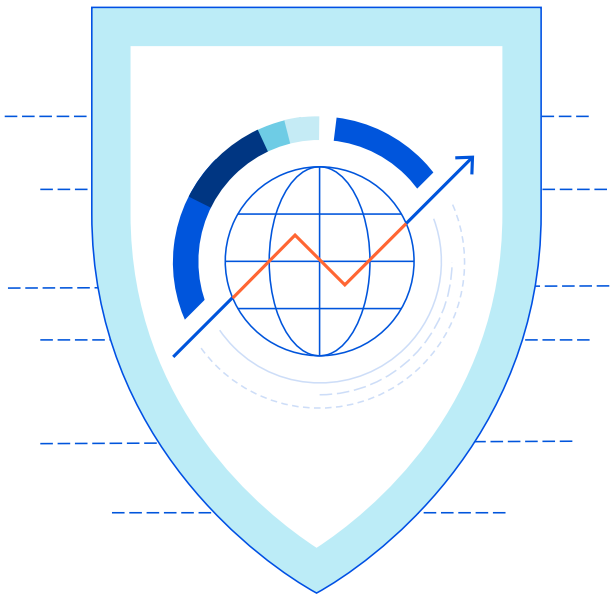
④ 網路層 DDoS 攻擊

- 第二季度，網路層 DDoS 攻擊數同比增長 109%。
- 100 Gbps 及以上的攻擊數環比增長 8%。
- 持續三小時以上的攻擊數環比增長 12%。
- 遭受此類攻擊最多的產業分別是電信業、遊戲/博彩業以及資訊科技和服務業。
- 位於美國的組織是此類攻擊的主要目標，其次是中國、新加坡及德國。

本報告基於 Cloudflare DDoS 防護系統自動偵測和緩解的 DDoS 攻擊數。如需深入瞭解 DDoS 緩解措施的運作方式，請查看此深度剖析部落格貼文。

有關我們如何衡量在網路中觀察到的 DDoS 攻擊的說明

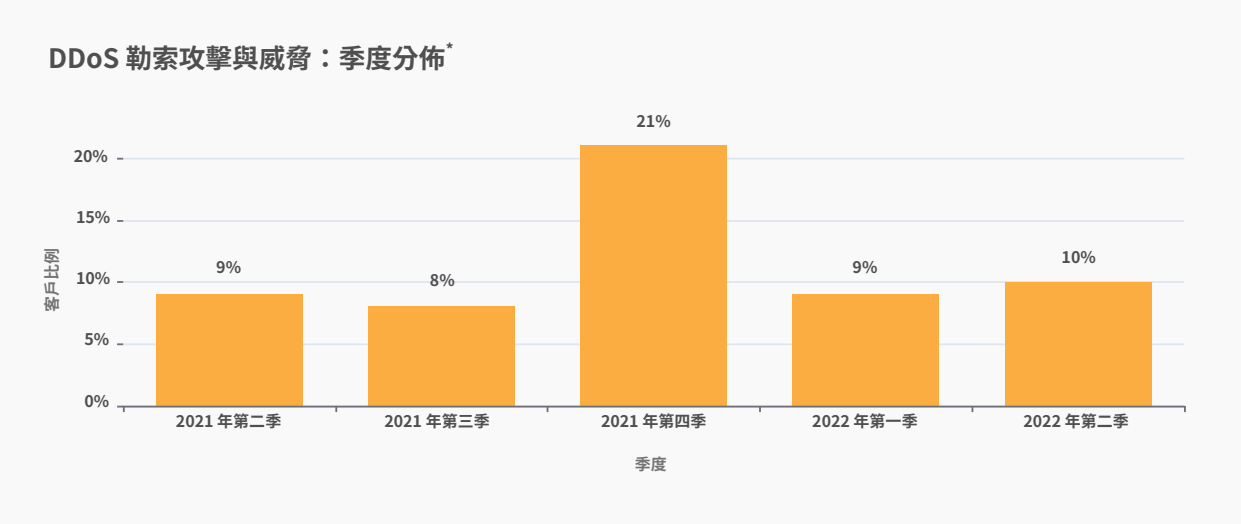
為分析攻擊趨勢，我們會計算「DDoS 活動」率，即攻擊流量在我們的全球網路中、特定位置或特定類別（如行業或帳單國家/地區）觀察到的總流量（攻擊流量+潔淨流量）中所佔的百分比。透過衡量這些百分比，我們能夠標準化資料點並避免以絕對數字反映而出現的偏頗，例如，某個 Cloudflare 資料中心接收到更多的總流量，因而發現更多攻擊。



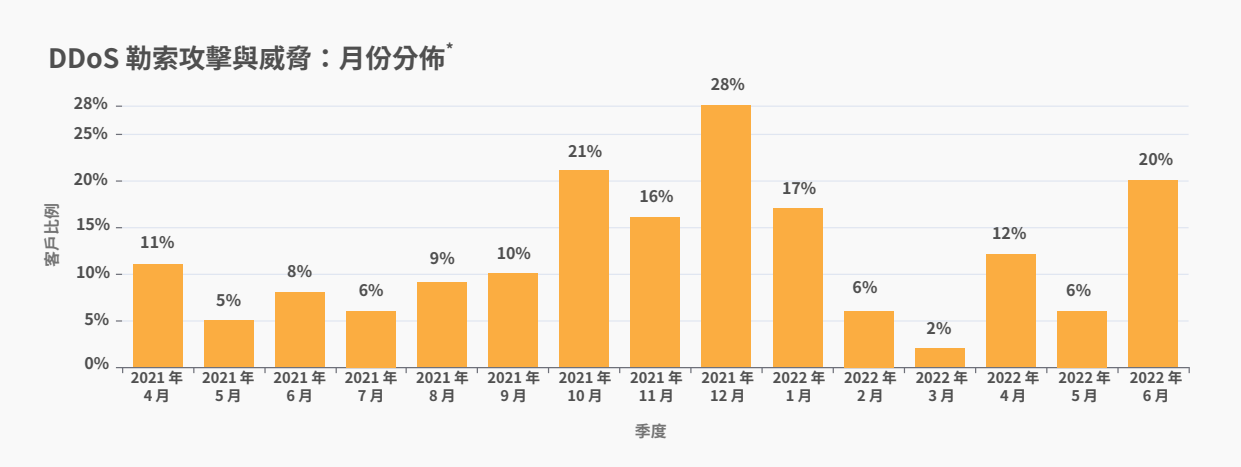
勒索攻擊趨勢

我們的系統會持續分析流量，並自動偵測及緩解 DDoS 攻擊。每個受影響的客戶都會收到提示，請求參與一個自動化調查，以幫助我們更好地瞭解該攻擊的性質以及緩解措施的成功率。調查中的一個問題是，受訪者是否收到威脅或勒索信，要求付款以換得停止 DDoS 攻擊。

第二季度報告威脅或勒索信的受訪者數量環比和同比均增長 11%。本季度，我們一直在緩解 DDoS 勒索攻擊，這些攻擊由自稱是進階持續威脅 (APT) 組織 Fancy Lazarus 的實體發起。而金融機構和加密貨幣公司成為這起活動的主要目標。



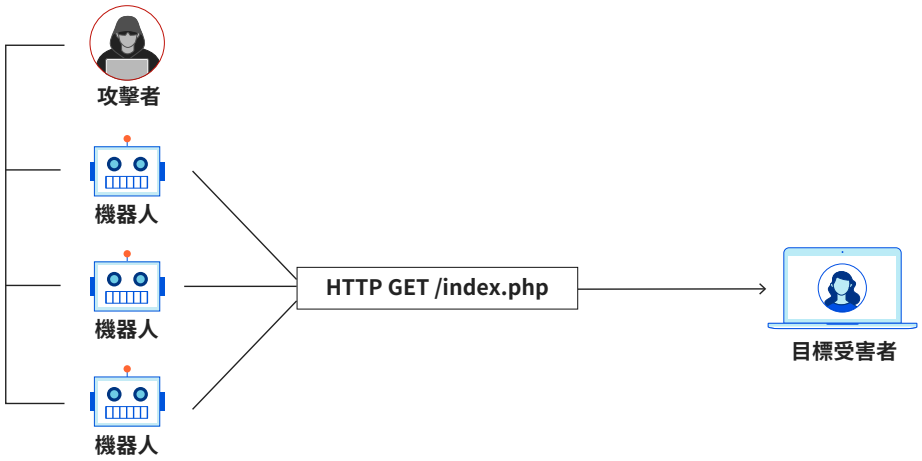
6 月份，每五名受訪者中就有一人報告收到 DDoS 勒索攻擊或威脅 — 這是自 2021 年 12 月以來的最高比率。



*來源：https://radar.cloudflare.com/notebooks/ddos-2022-q2

應用程式層 DDoS 攻擊

應用程式層 DDoS 攻擊，特別是 HTTP DDoS 攻擊，旨在透過使網頁伺服器無法處理合法使用者請求來破壞它。如果伺服器收到的請求數量超過其處理能力，伺服器將丟棄合法請求甚至崩潰，導致對合法使用者的服務效能下降或中斷。

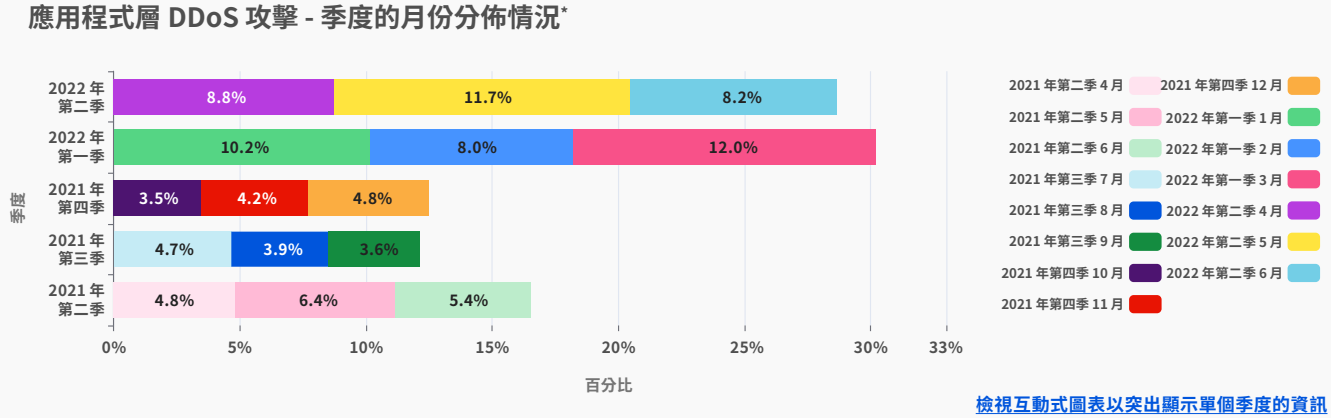


應用程式層 DDoS 攻擊

應用程式層 DDoS 攻擊：月份分佈

第二季度，應用程式層 DDoS 攻擊數同比增長 72%。

整體來說，第二季度的應用程式層 DDoS 攻擊數量同比增長 72%，但環比下降 5%。5 月是本季度最繁忙的月份。幾乎 41% 的應用程式層 DDoS 攻擊發生在 5 月。6 月發生的攻擊數最少，只有 28%。



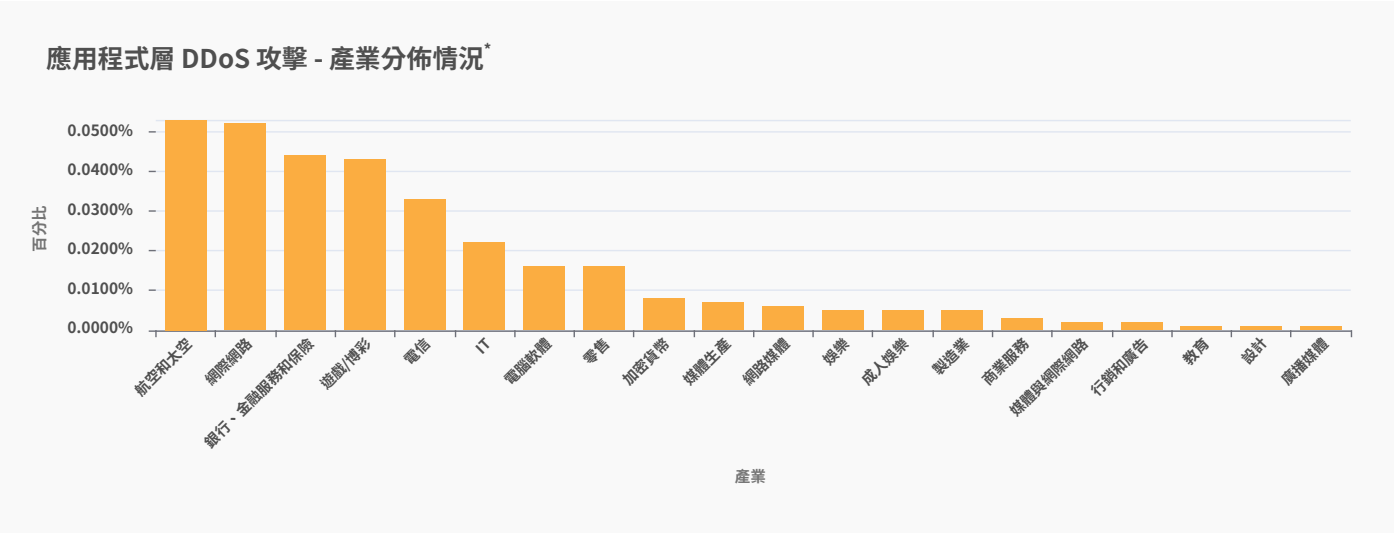
檢視互動式圖表以突出顯示單個季度的資訊

*來源：https://radar.cloudflare.com/notebooks/ddos-2022-q2

應用程式層 DDoS 攻擊：產業分佈

針對航空和太空業的攻擊數環比增長 493%。

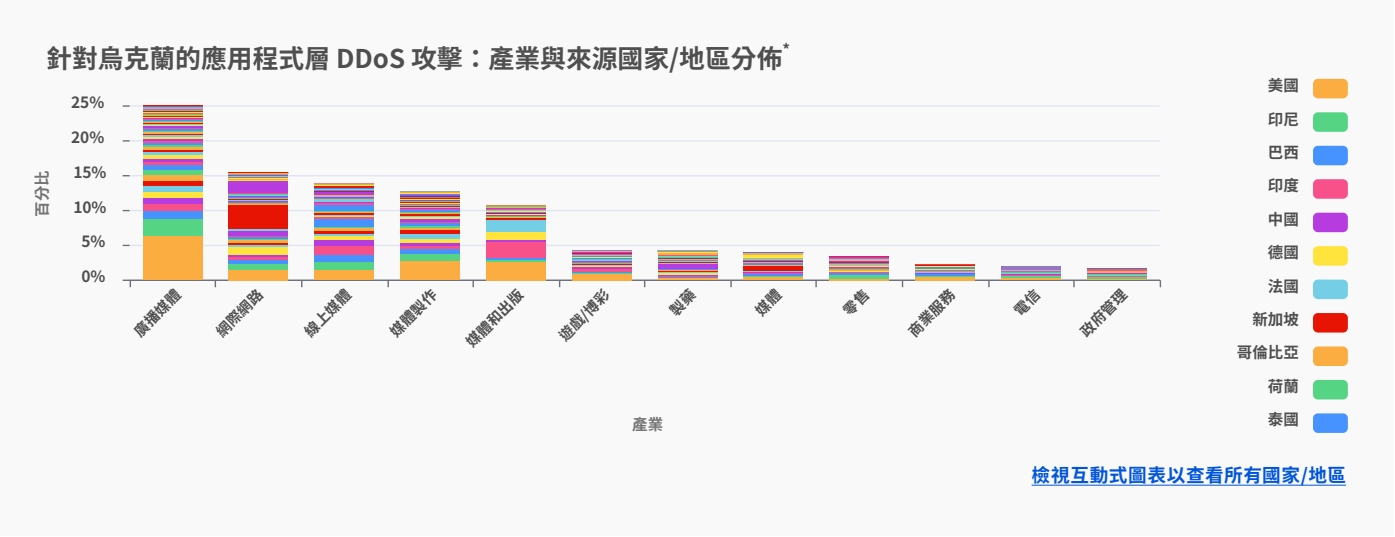
第二季度，航空和太空業是遭受應用程式層 DDoS 攻擊最多的產業。其他遭受攻擊最多的產業按順序分別為銀行、金融機構和保險業 (BFSI) 以及遊戲/博彩業。



烏克蘭和俄羅斯的網路空間

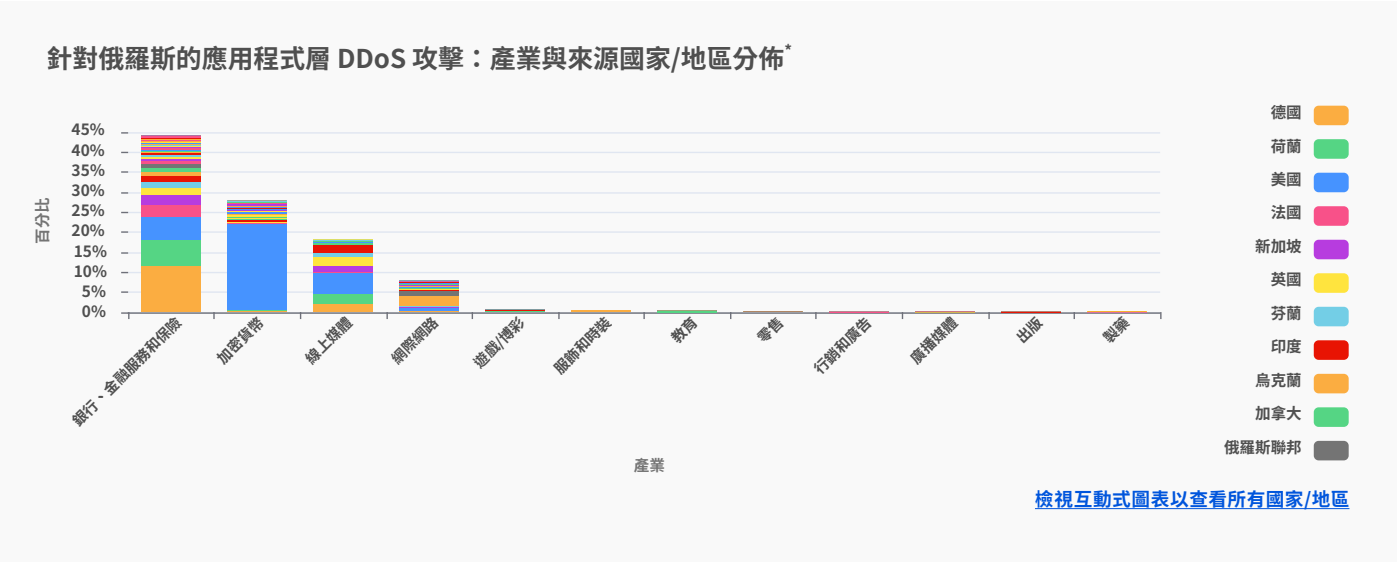
媒體和出版公司是烏克蘭遭受攻擊最多的公司。

隨著烏克蘭戰爭在地面、空中和水面繼續進行，網路空間的戰爭也在繼續展開。將烏克蘭公司作為攻擊目標的實體似乎在嘗試掩蓋資訊，因為烏克蘭遭受攻擊最多的前六大產業均屬於廣播、網際網路、網路媒體和出版業。在所有針對烏克蘭的 DDoS 攻擊中，僅以上產業便幾乎佔了 80%。



*來源：https://radar.cloudflare.com/notebooks/ddos-2022-q2

而戰爭的另一方，俄羅斯的銀行、金融機構和保險業 (BFSI) 公司受到的攻擊最多。實際上，幾乎 45% 的 DDoS 攻擊的目標都是 BFSI 產業。第二大目標是加密貨幣產業，然後是線上媒體。



在戰爭雙方，我們可以看到攻擊都是高度分散的，這表明使用了全球分散式殭屍網路。

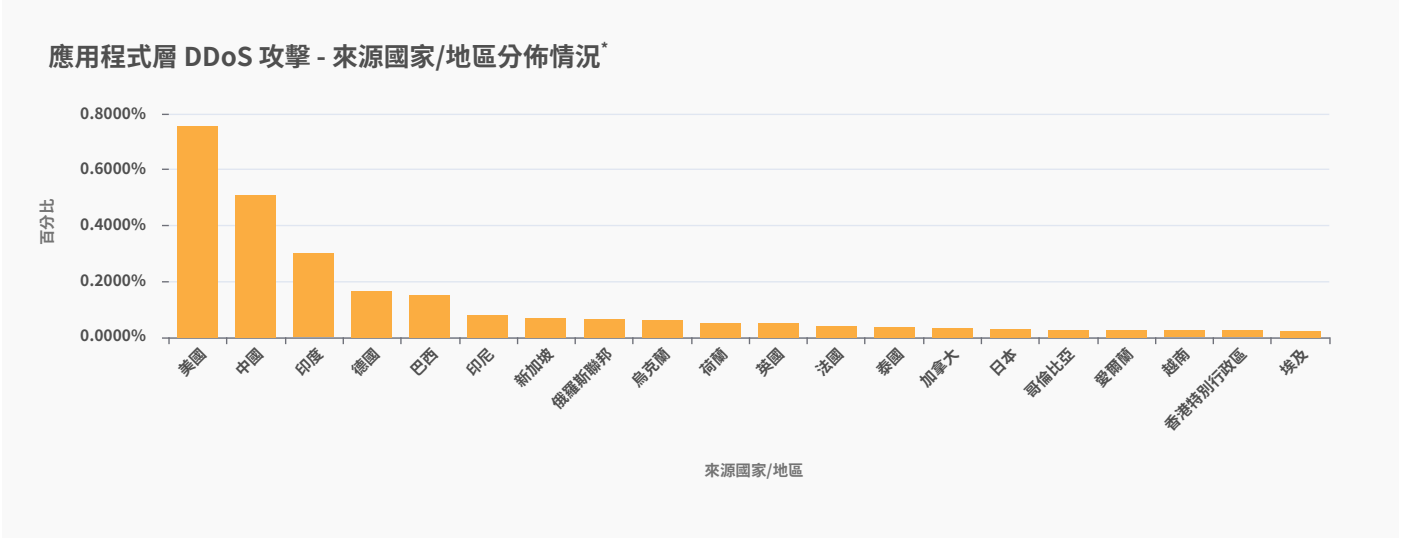
應用程式層 DDoS 攻擊：來源國家/地區分佈

第二季度，來自中國的攻擊數減少了 78%，而來自美國的攻擊數則減少了 43%。

為瞭解 HTTP 攻擊的來源，我們研究了屬於產生攻擊 HTTP 請求之用戶端的來源 IP 位址的地理位置。與網路層攻擊不同，HTTP 攻擊中的來源 IP 位址無法偽造。特定國家/地區的 DDoS 活動百分比較高，這並不意味著該特定國家/地區正在發起攻擊，而是表明有殭屍網路在其境內運作。

美國作為 HTTP DDoS 攻擊的主要來源，已經連續第二個季度位居榜首，排在其後的分別是中國、印度及德國。有趣的是，儘管美國連續兩個季度排名第一，但來自美國的攻擊數環比下降了 48%，而來自其他地區的攻擊數卻有所增長。來自印度、德國及巴西的攻擊數分別增長了 87%、33% 和 67%。

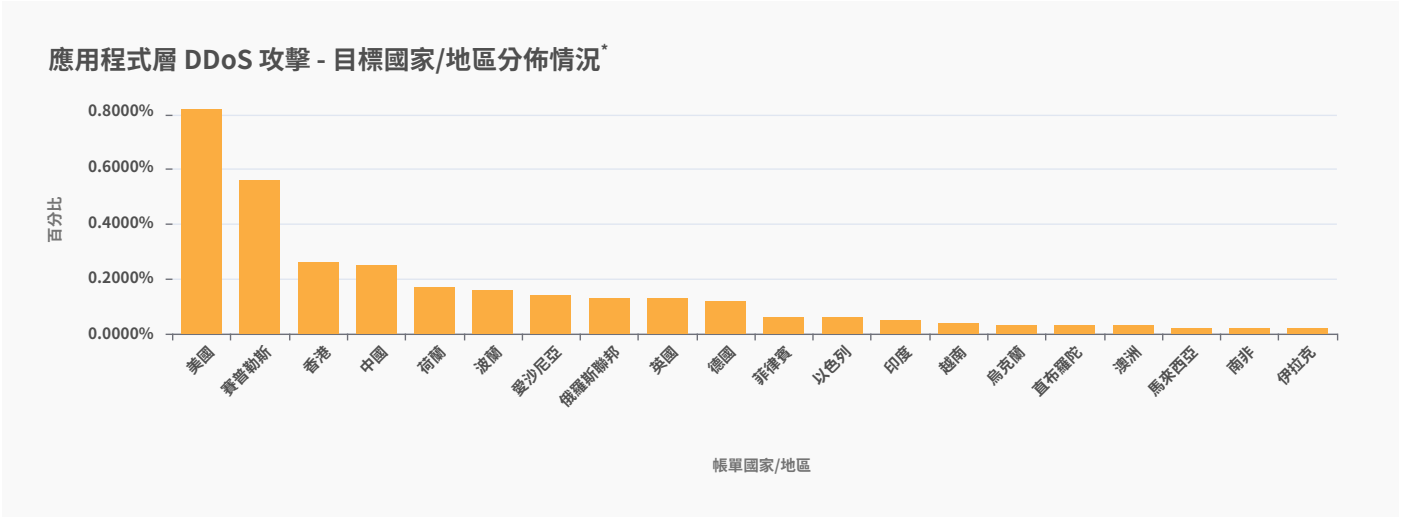
*來源：https://radar.cloudflare.com/notebooks/ddos-2022-q2



應用程式層 DDoS 攻擊：目標國家/地區分佈

為確定哪些國家/地區遭受最多的 HTTP DDoS 攻擊，我們按客戶的帳單國家/地區對 DDoS 攻擊進行了分類，並以其佔據所有 DDoS 攻擊數的百分比進行表示。

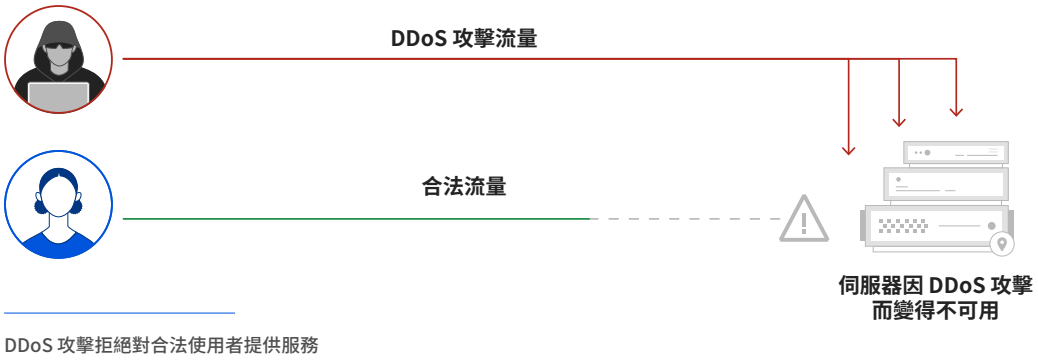
針對美國境內目標的 HTTP DDoS 攻擊數環比增長了 67%，使美國成為應用程式層 DDoS 攻擊的首要目標國家/地區。針對中國公司的攻擊數環比下降了 80%，使中國從第一位下降到第四位。針對賽普勒斯的攻擊數增長了 167%，使其成為第二季度遭受攻擊第二多的國家/地區，排在其後的分別是香港特別行政區、中國大陸及荷蘭。



*來源：https://radar.cloudflare.com/notebooks/ddos-2022-q2

網路層 DDoS 攻擊

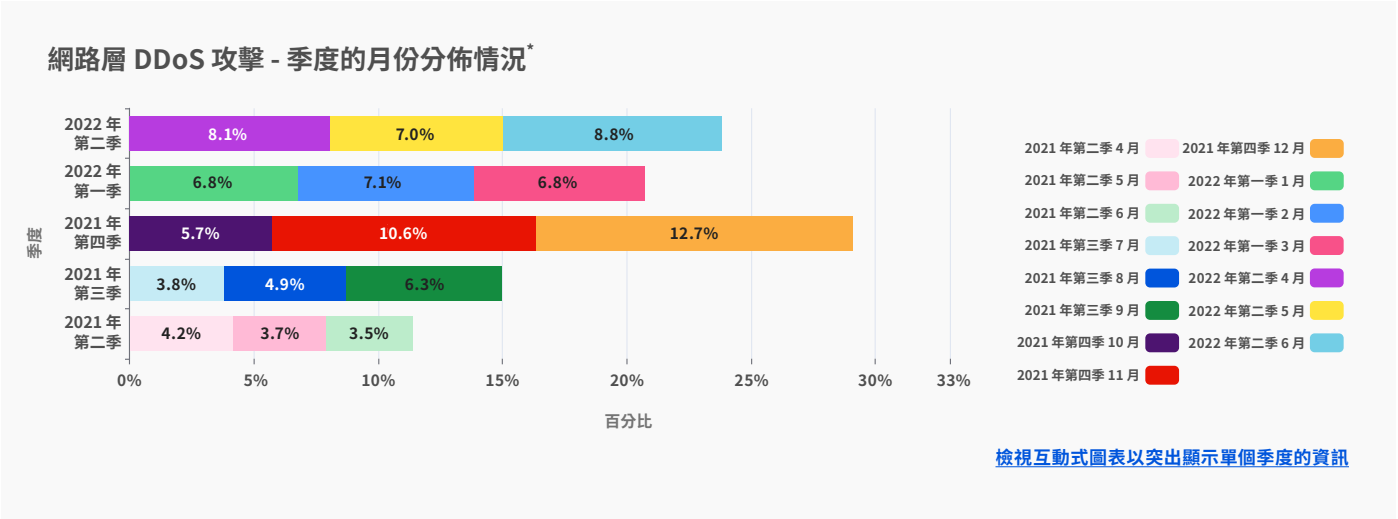
應用程式層攻擊的目標是執行最終使用者嘗試存取之服務（本例中為 HTTP/S）的應用程式（OSI 模型的第 7 層）。相較之下，網路層攻擊則以壓垮網路基礎結構（例如聯網路由器和伺服器）和網際網路鏈路本身為目標。



DDoS 攻擊拒絕對合法使用者提供服務

網路層 DDoS 攻擊：月份分佈

第二季度，網路層 DDoS 攻擊數同比增長 109%，100 Gbps 及以上的巨流量攻擊數環比增長 8%。



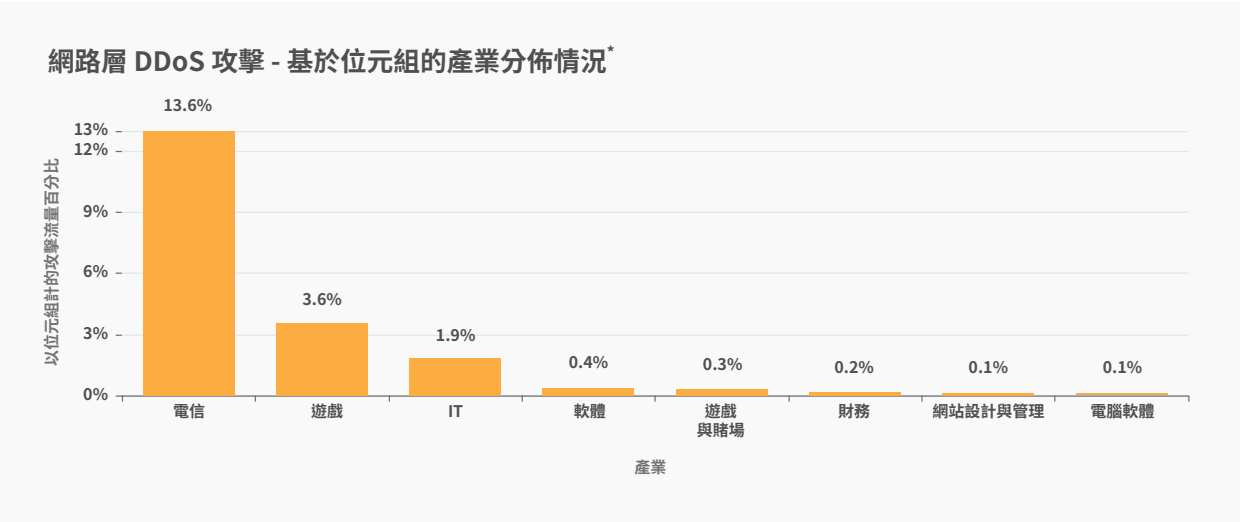
第二季度，網路層 DDoS 攻擊總數同比增長 109%，環比增長 15%。在所有網路層攻擊中，僅 6 月份便幾乎佔了 36%。

*來源：https://radar.cloudflare.com/notebooks/ddos-2022-q2

網路層 DDoS 攻擊：產業分佈

第二季度，針對電信公司的攻擊數環比增長 66%。

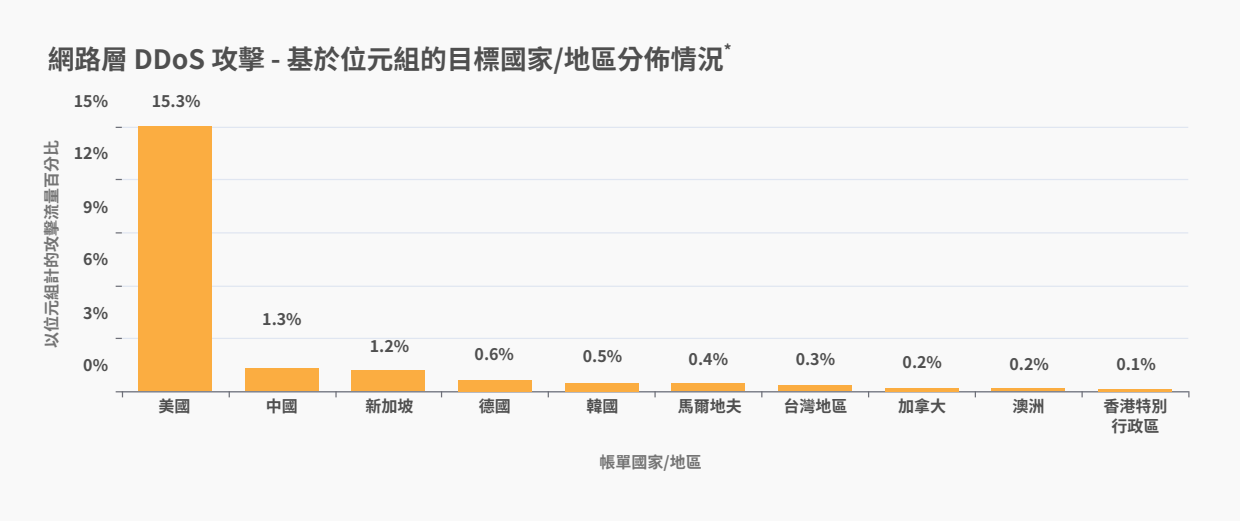
電信產業已經連續第二個季度成為網路層 DDoS 攻擊的最主要目標。此外，針對電信公司的攻擊數環比增長了 66%。遊戲產業位居第二，緊跟其後的是資訊科技和服務公司。



網路層 DDoS 攻擊：目標國家/地區分佈

針對美國網路的攻擊數環比增長了 95%。

第二季度，美國仍是遭受攻擊最多的國家/地區且以較大的優勢遙遙領先，排在其後的分別是中國、新加坡及德國。



*來源：https://radar.cloudflare.com/notebooks/ddos-2022-q2

網路層 DDoS 攻擊：輸入國家/地區分佈情況

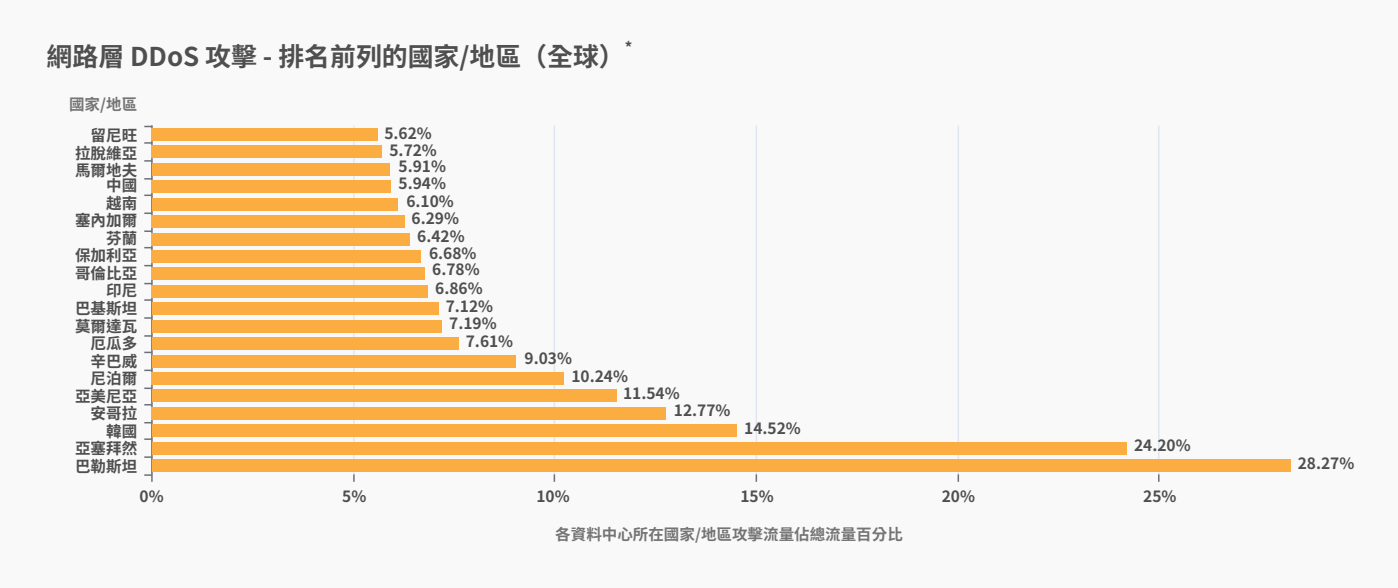
第二季度，Cloudflare 在巴勒斯坦觀察到的近三分之一的流量以及在亞塞拜然觀察到的近四分之一的流量都屬於網路層 DDoS 攻擊。

在試圖弄清網路層 DDoS 攻擊的來源時，我們不能使用與進行應用程式層攻擊分析相同的方法。要發起應用程式層 DDoS 攻擊，用戶端與伺服器之間必須成功握手，以建立 HTTP/S 連線。為實現成功握手，攻擊不能偽造其來源 IP 位址。雖然攻擊者可能會使用殭屍網路、代理或其他方法來掩蓋自己的身分，但攻擊用戶端的來源 IP 位置確實就是應用程式層 DDoS 攻擊的攻擊來源。

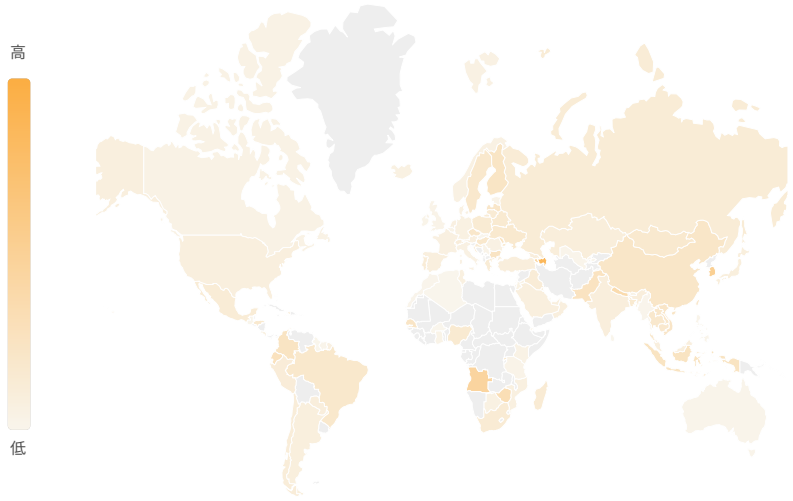
相較而言，發起大多數網路層 DDoS 攻擊都無需握手。攻擊者可以偽造來源 IP 位址來混淆攻擊來源並在攻擊屬性中引入隨機性。像這樣的技術可能會使簡單的 DDoS 防護系統更難攔截攻擊。如果我們根據「偽造的」來源 IP 位址推導出來源國家/地區，我們將得到一個「偽造的國家/地區」。

為此，在分析網路層 DDoS 攻擊來源時，我們會根據吸收流量的 Cloudflare 資料中心位置（而不是潛在的偽造來源 IP）對流量進行分類，來瞭解攻擊來源。我們的資料中心遍及全球超過 270 個城市，因此能夠在本報告中實現地理上的準確性。然而，即便是這種方法也不能達到 100% 的準確性，因為出於各種原因，比如降低成本、網路壅塞或管理不善，流量可能會透過不同的網際網路服務提供者和國家/地區回傳或路由。

第二季度，巴勒斯坦成為網路層 DDoS 攻擊佔比最高的 Cloudflare 位置，從第二位躍升至首位。排在巴勒斯坦之後的是亞塞拜然、南韓和安哥拉。



*來源：https://radar.cloudflare.com/notebooks/ddos-2022-q2



要檢視所有國家和地區，請查看互動式地圖。

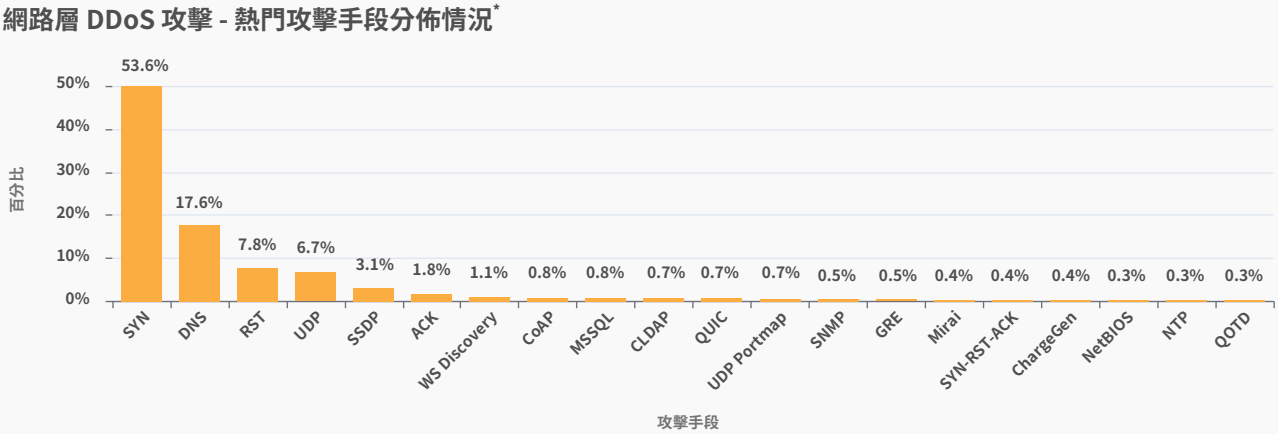
攻擊手段

第二季度，DNS 攻擊數有所增長，使其成為第二常見的攻擊手段。

攻擊手段是攻擊者用來發起攻擊的方法（如 IP 通訊協定、封包屬性、洪水方法和其他條件）。

第二季度，SYN 洪水在所有網路層攻擊中佔 53%。SYN 洪水濫用具狀態 TCP 握手的初始連線要求。在這個初始連線要求期間，伺服器沒有關於該新 TCP 連線的任何背景資訊，因此無法緩解初始連線要求的氾濫。這使得攻擊者更容易消耗未受保護的伺服器的資源。

在 SYN 洪水之後，針對 DNS 基礎結構的攻擊位居第二，接下來分別是濫用 TCP 連線流程的 RST 洪水及一般的 UDP 攻擊。



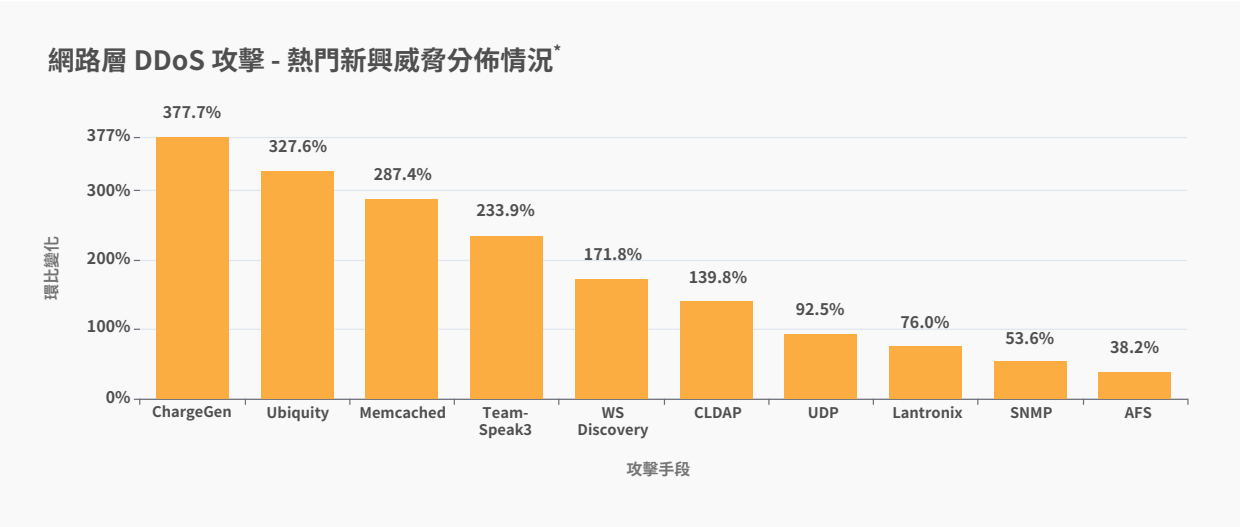
*來源：https://radar.cloudflare.com/notebooks/ddos-2022-q2

新興威脅

第二季度，主要的新興威脅包括 CHARGEN、Ubiquiti 和 Memcached 攻擊。

識別主要攻擊手段有助於組織更好地瞭解威脅情勢，進而改善其安全狀態。同樣地，瞭解新興威脅 — 甚至那些在攻擊中佔比較小的威脅 — 可協助組織主動保護其網路及資料。

第二季度，主要的新興威脅是濫用 Character Generator 通訊協定 (CHARGEN) 的放大攻擊、反映暴露 Ubiquiti 裝置流量的放大攻擊，以及臭名昭著的 Memcached 攻擊。



濫用 CHARGEN 通訊協定發起放大攻擊

第二季度，濫用 CHARGEN 通訊協定的攻擊數環比增長了 378%。

字元產生器通訊協定 (CHARGEN) 最初於 RFC 864 (1983) 中定義，是網際網路通訊協定套件的一項服務。它會任意產生字元，並在用戶端關閉連線之前，不斷地向用戶端傳送字元。最初開發 CHARGEN 是為了協助測試和偵錯，但它卻更常用於產生放大/反射攻擊。

在放大/反射攻擊中，攻擊者會偽造其受害者的來源 IP，並強制世界各地的支援伺服器將任意字元串流「重新」導向至受害者的伺服器。如果並行 CHARGEN 串流足夠多，則受害者的伺服器（如果未受保護）會遭受惡意流量的洪水攻擊，進而無法應對合法流量，導致使用者阻斷服務事件。

*來源：https://radar.cloudflare.com/notebooks/ddos-2022-q2

利用 Ubiquiti 發現通訊協定的放大攻擊

第二季度，Ubiquiti 攻擊數環比增長了 327%。

Ubiquiti 總部位於美國，該公司為消費者和企業提供網路和物聯網 (IoT) 裝置。您可以在使用 Ubiquiti 探索通訊協定 的網路上透過 UDP/TCP 連接埠 10001 探索 Ubiquiti 裝置。

與 CHARGEN 攻擊手段類似，攻擊者會偽造來源 IP，並針對開啟連接埠 10001 的 IP 位址發起攻擊。如果流量足夠大，則那些 IP 會回應受害者，並向其傳送大量的惡意流量。

Memcached DDoS 攻擊

第二季度，Memcached DDoS 攻擊數環比增長了 287%。

Memcached 是一個資料庫快取系統，可用於加速網站和網路。與 CHARGEN 和 Ubiquiti 類似，支援 UDP 的 Memcached 伺服器可能會被濫用，以發起放大/反射 DDoS 攻擊。在 Memcached 攻擊中，攻擊者會從快取系統請求內容，並偽造受害者的 IP 位址作為 UDP 封包中的來源 IP。Memcached 回應可放大最高 51,200 倍，因此會淹沒受害者。

網路層 DDoS 攻擊：攻擊率分佈

超過 100 Gbps 的巨流量攻擊數環比增長 8%。

衡量 L3/4 DDoS 攻擊規模有不同的方法。

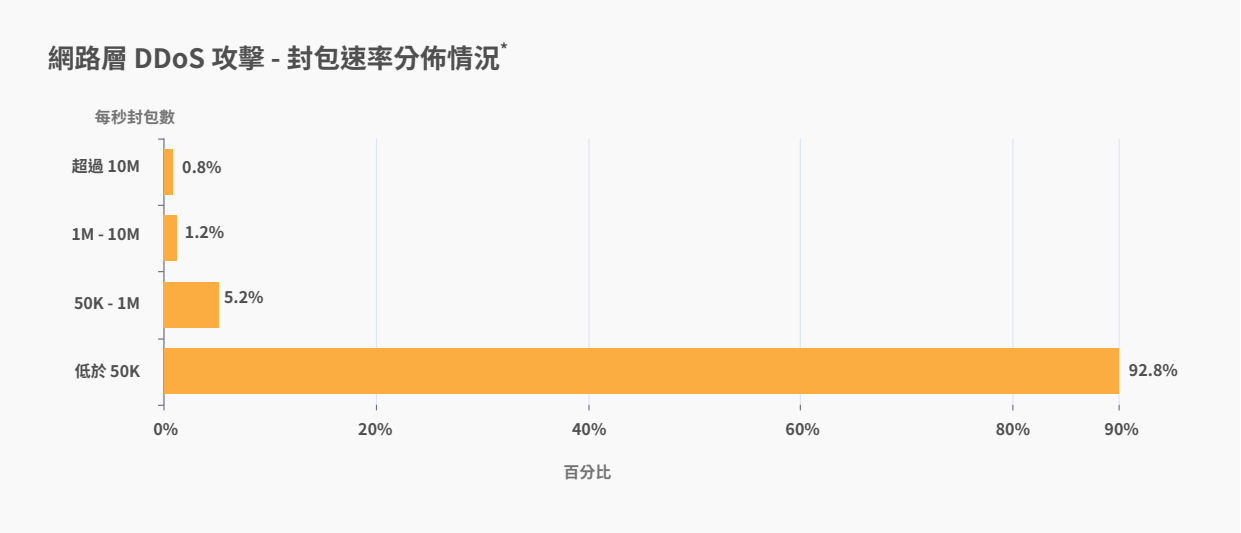
一種方法是測量它傳遞的流量大小 — 換言之即位元速率（具體而言，是每秒 TB 數或每秒 GB 數）。位元速率較高的攻擊會嘗試透過阻塞網際網路連結，來造成阻斷服務事件。

測量這些攻擊的另一種方法是追蹤它傳遞的封包數 — 也稱為封包速率（具體而言，是每秒百萬封包數）。封包速率較高的攻擊會嘗試壓垮伺服器、路由器或其他內聯硬體裝置。這些裝置會分配一定的記憶體量和計算能力來處理每個封包，因此，透過向裝置傳送大量封包，就會耗盡其處理資源。在這種情況下，封包會被「丟棄」，這表示裝置無法處理封包。對使用者而言，這會導致發生服務中斷和阻斷服務事件。

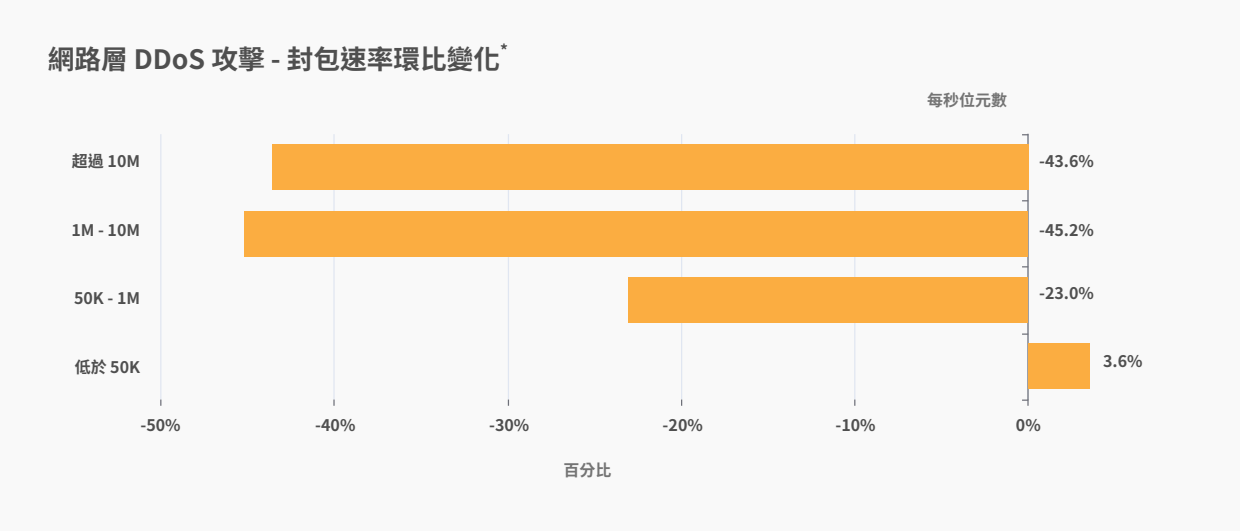
*來源：https://radar.cloudflare.com/notebooks/ddos-2022-q2

封包速率分佈情況

大部分網路層 DDoS 攻擊仍低於每秒 50,000 個封包。考量到 Cloudflare 網路的規模，50 kpps 在整個範圍內處於較低的一端，但它仍可輕鬆摧毀未受保護的網際網路設備，並造成標準千兆位元級乙太網路連線的壅塞。



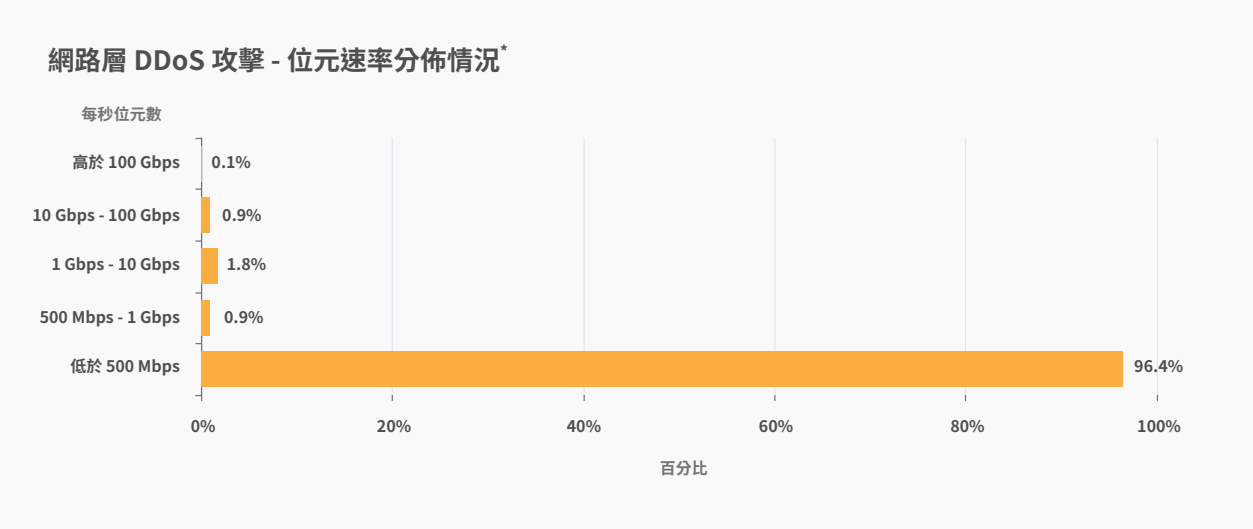
分析攻擊規模的變化時，我們可以看到，第二季度超過 50 kpps 的高封包量攻擊有所減少，導致小型攻擊增長 4%。



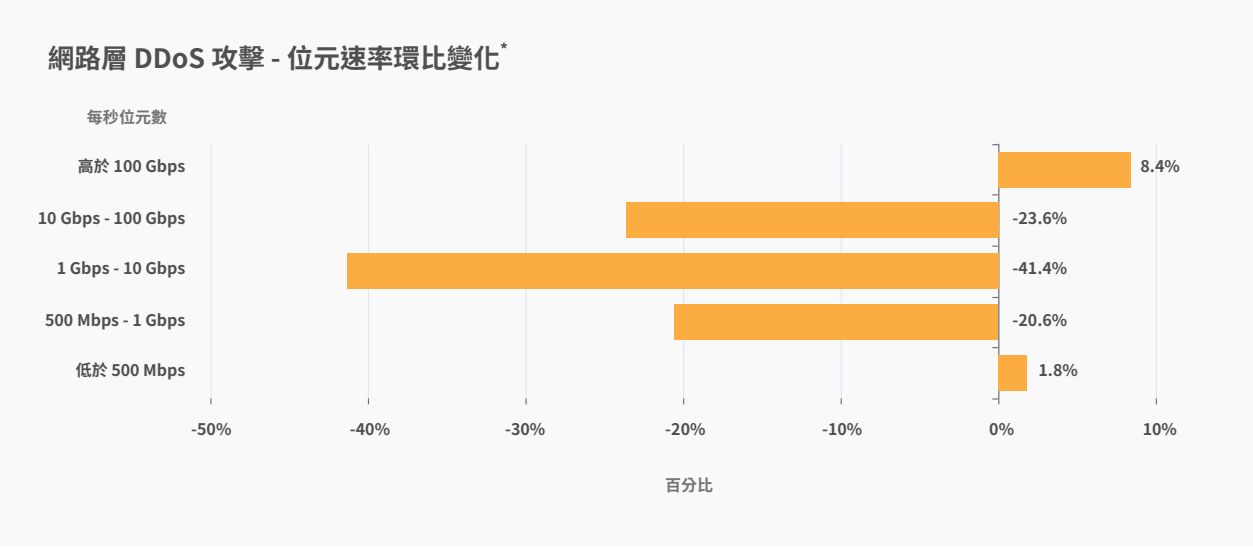
*來源：https://radar.cloudflare.com/notebooks/ddos-2022-q2

位元速率分佈情況

第二季度，大部分網路層 DDoS 攻擊仍低於 500 Mbps。與 Cloudflare 的網路規模相比，此數據同樣不足掛齒，但此類攻擊仍能夠快速地關閉未受保護且網路處理能力較低的網際網路設備，或者至少能夠造成標準千兆位元級乙太網路連線的壅塞。



有趣的是，介於 500 Mbps 和 100 Gbps 之間的大型攻擊數環比減少了 20-40%，但 100 Gbps 以上的巨流量攻擊數卻增長了 8%。



*來源：https://radar.cloudflare.com/notebooks/ddos-2022-q2

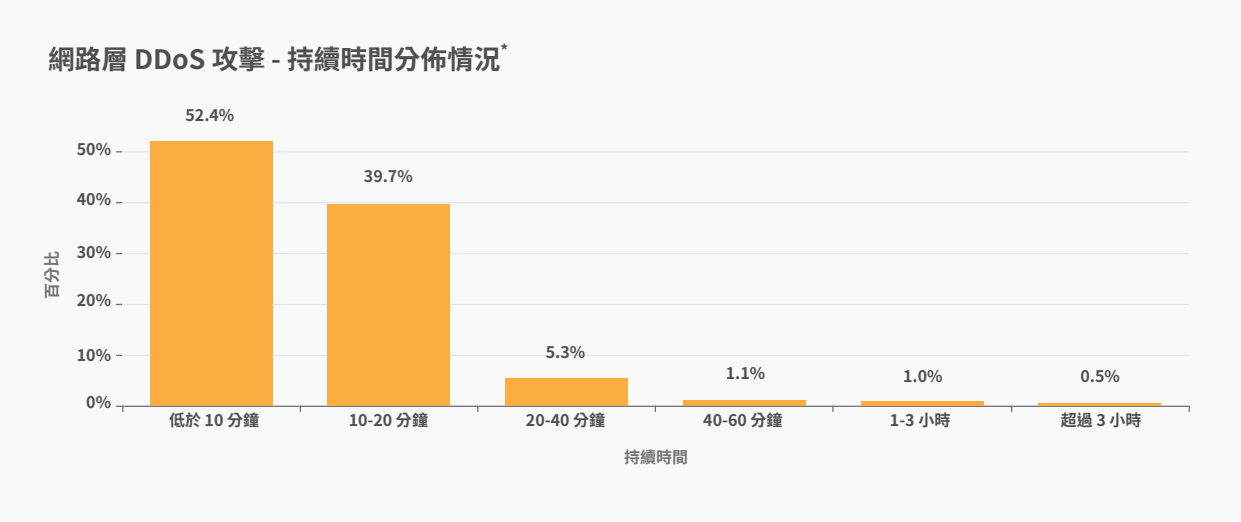
網路層 DDoS 攻擊：持續時間分佈

第二季度，持續超過三小時的攻擊數增長了 9%。

我們測量攻擊持續時間的方式是：記錄系統首次偵測到攻擊與具備攻擊特徵且前往特定目標的最後一個封包之間的時間差。

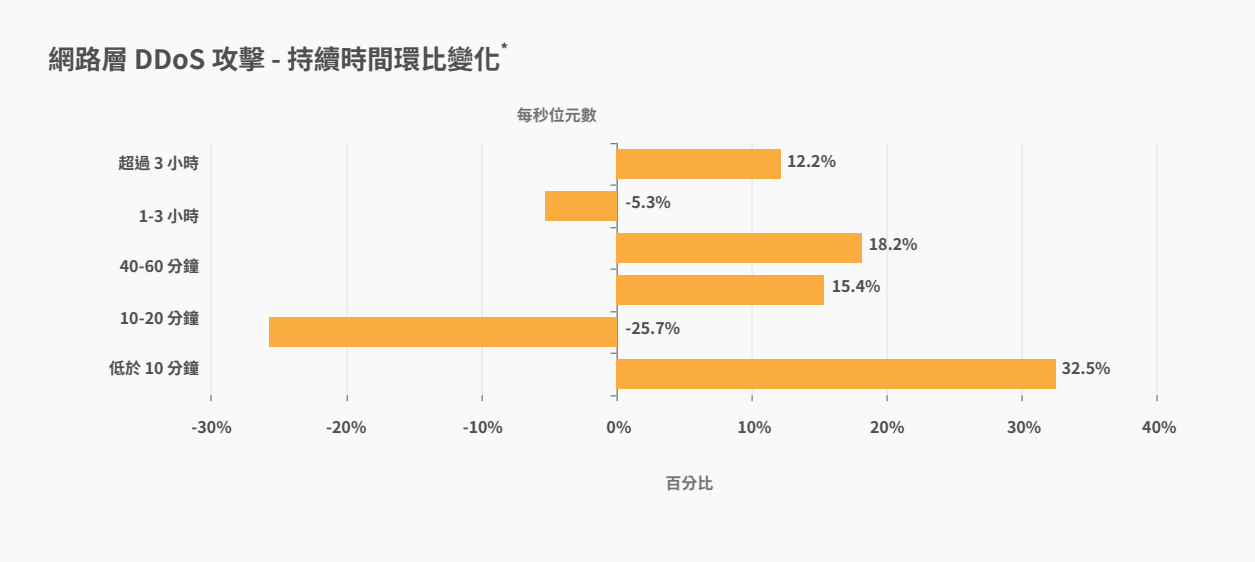
第二季度，52% 的網路層 DDoS 攻擊持續時間不足 10 分鐘。另有 40% 的攻擊持續了 10-20 分鐘。剩下 8% 的攻擊則持續了 20 分鐘到三小時以上。

重要注意事項：一次成功的攻擊即使只持續幾分鐘，造成的影響也會遠遠超過最初的攻擊時長。針對成功的 DDoS 攻擊，IT 人員可能需要幾小時 — 甚至幾天 — 的時間進行回應，才能恢復服務。終端使用者很難不注意到這種規模的中斷。成功的 DDoS 攻擊通常會導致巨大的收入損失，並可能導致客戶流失。



儘管第二季度記錄的大多數攻擊時間很短暫，但我們發現 20-60 分鐘之間的攻擊增長了 15% 以上，而持續時間超過三小時的攻擊則增長了 12%。

*來源：https://radar.cloudflare.com/notebooks/ddos-2022-q2



時間較短的攻擊很難偵測到，特別是爆發攻擊。爆發攻擊會在幾秒鐘內用大量的封包、位元組或請求轟擊目標。在這種情況下，依賴於手動緩解的 DDoS 防護服務幾乎不可能及時地緩解攻擊。此類服務只能從攻擊後分析中吸取教訓，然後部署篩選該攻擊特征的新規則，期望下次能捕捉到它。

同樣，使用「按需」服務（即安全團隊僅在已偵測到攻擊時，將流量重新導向至 DDoS 提供者）也無濟於事。在大多數情況下，在流量到達按需 DDoS 提供者之前，攻擊就已經結束了。

為此，建議公司使用始終啟用的自動化 DDoS 防護服務來分析流量，並足夠快速地套用即時特征識別以封鎖持續時間短暫的攻擊。

*來源：https://radar.cloudflare.com/notebooks/ddos-2022-q2

結論

2022 年第二季度，DDoS 攻擊仍在各種組織中發生。

隨著烏克蘭戰爭的繼續，DDoS 攻擊試圖透過將烏克蘭廣播媒體及通訊相關組織作為目標，來停止傳播資訊。而在戰爭的另一邊，銀行及金融服務業則成為俄羅斯遭受攻擊最多的產業。

除了俄烏衝突以外，新一波 DDoS 勒索攻擊達到了今年以來的最高程度。應用程式層 DDoS 攻擊數逐年增加，且大多數攻擊的目標是美國以及航空和太空業。網路層 DDoS 攻擊數也逐年增加，且大流量攻擊數 (100 Gbps) 和持續時間超過三小時的攻擊數增長尤為顯著。對於網路層攻擊而言，其首要目標產業是電信業，而遭受攻擊最多的國家/地區是美國。

顯而易見，DDoS 攻擊的規模、複雜程度及持續時間均在增長。正如世界各地的組織都受益於更簡單、更便宜、更快速的計算、儲存及網路功能，攻擊者也同樣受益匪淺。我們看到每個季度的攻擊數都在打破紀錄，包括 Cloudflare 最近阻止的一次每秒 2600 萬個請求的 HTTPS DDoS 攻擊。

作為 Cloudflare 使命的一部分，自 2017 年開始，我們一直在為所有應用程式服務客戶免費提供非計量、無限制的 DDoS 防護。這些年來，攻擊者越來越容易發起 DDoS 攻擊。我們希望提供幫助，以確保所有規模的組織都能夠獲得更加輕鬆且更具成本效益的保護，從而避免遭受各種各樣的 DDoS 攻擊。

尚未使用 Cloudflare？立即開始吧，您可以使用我們的 Free 和 Pro 方案保護您的網站，也可以連絡我們，以使用 Magic Transit 為您的整個網路提供全面的 DDoS 保護。

CLOUDFLARE

+ 886 8 0185 7030 | enterprise@cloudflare.com | www.cloudflare.com

REV:BDES-3514.2022JUL18