白皮書

Cloudflare 安全洞察：2021 年第四季度 DDoS 趨勢

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

2021 年的上半年見證了大量勒索軟體和 DDoS 勒索攻擊活動，中斷了全球關鍵基礎結構的各個方面（包括美國一家大型石油管道系統運營商），同時還出現了 IT 管理軟體方面的漏洞，對學校、公共事業、旅行組織、信用社等機構造成威脅。

2021 年下半年，在 Cloudflare 網路上觀察到，最強大的殭屍網路之一 (Meris) 的部署量不斷成長，HTTP DDoS 攻擊和網路層攻擊數打破記錄。除此之外，去年 12 月還發現了 Log4j2 漏洞 (CVE-2021-44228)，允許攻擊者在遠端伺服器上執行程式碼，這可以說是自 Heartbleed 和 Shellshock 出現以來，網際網路上最嚴重的漏洞之一。

上面列出的攻擊只是少數幾個範例，但這些重大攻擊的趨勢顯示：越來越嚴重的網路威脅影響到每個人，無論是科技公司、政府組織，還是酒廠和肉類加工廠都囊括在內。

以下是從 2021 年（第四季度）的情況中得出的一些 DDoS 攻擊趨勢和重點：

DDoS 勒索攻擊

- 在第四季度，DDoS 勒索攻擊較去年同期成長 29%，較上一季度成長 175%。
- 僅在 12 月份，就有三分之一的調查受訪者報告說成為 DDoS 勒索攻擊的目標或受到攻擊者的威脅。

應用程式層 DDoS 攻擊

- 在 2021 年第四季度，製造業成為攻擊的最大目標，攻擊數較前一季度成長達到 641% 的驚人數據。商務服務和博弈業是應用程式層 DDoS 攻擊的第二和第三大目標產業。
- 中國網路攻擊流量仍然佔據最高百分比，今年連續第四次位居榜首。
- 2021 年中旬出現了一種名為 Meris 殭屍網路的新型殭屍網路，並持續攻擊全球組織，發起了一些有史以來最大的 HTTP 攻擊，包括 Cloudflare 自動緩解的 17.2M rps 攻擊。

網路層 DDoS 攻擊

- 第四季度是 2021 年攻擊者最活躍的一個季度。僅在 2021 年 12 月份，發生的攻擊數就超過 2021 年第一季度和第二季度分別觀察到的所有攻擊數。
- 儘管大部分都是小規模攻擊，但 TB 強度的攻擊成為了 2021 年下半年的新常態。Cloudflare 自動緩解了幾十個峰值超過 1 Tbps 的攻擊，其中最大的一次攻擊峰值接近 2 Tbps，這是我們目前為止見過的最大攻擊。
- 2021 年第四季度，尤其是在 11 月份，記錄到一起針對全球 VoIP 提供者的持續性 DDoS 勒索攻擊活動。
- 源自摩爾多瓦的攻擊數在 2021 年第四季度較第三季度翻了四倍，使其成為網路層 DDoS 活動百分比最高的國家。
- SYN 洪水攻擊和 UDP 洪水攻擊是最常見的攻擊手段，而 SNMP 攻擊等新型威脅較前一季度成長了將近 5,800%。

本報告基於 Cloudflare 的 DDoS 防護系統自動偵測和緩解的 DDoS 攻擊數。如需深入瞭解該系統的運作方式，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

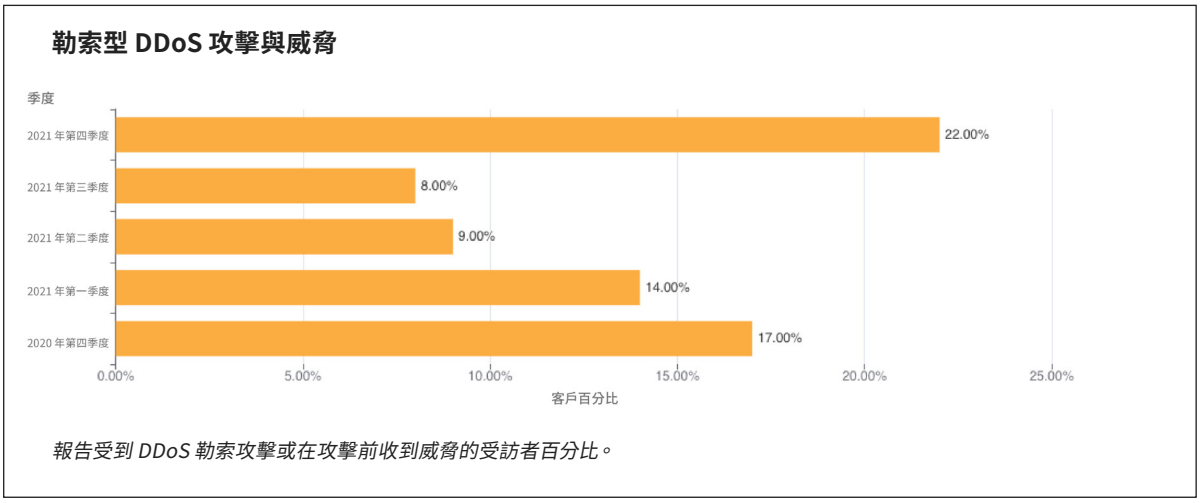
為分析攻擊趨勢，我們會計算「DDoS 活動」率，即攻擊流量在我們的全球網路中觀察到的總流量（攻擊流量+乾淨流量）中所佔的百分比。透過衡量攻擊數佔所觀察到的總流量的百分比，我們能夠標準化資料點並避免以絕對數字反映而出現的偏頗，例如，某個 Cloudflare 資料中心接收到更多的總流量，因而發現更多攻擊。

Cloudflare Radar 上提供了本報告的互動版本。

勒索攻擊

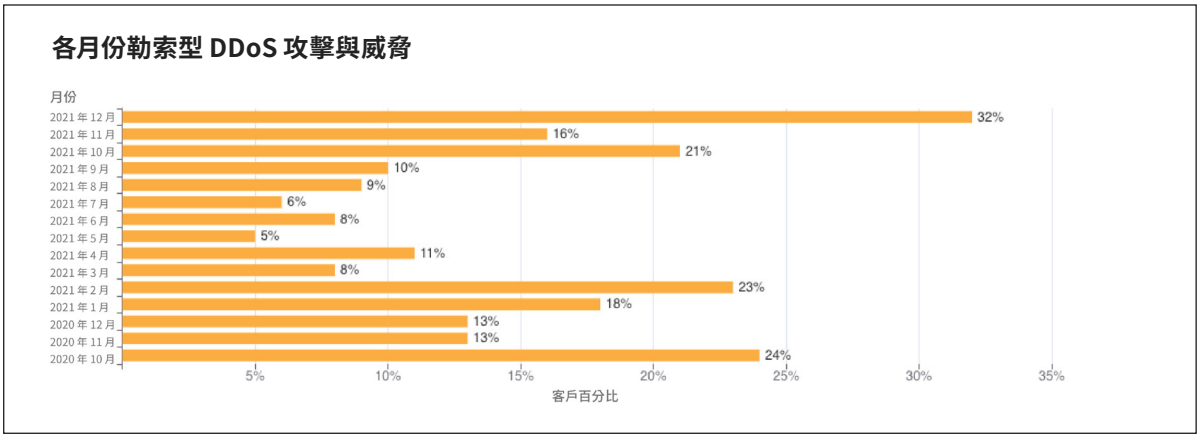
我們的系統會持續分析流量，並在偵測到 DDoS 攻擊時自動套用緩解措施。每個受到 DDoS 攻擊的客戶都會收到提示，請求參與一個自動化調查，以幫助我們更好地瞭解該攻擊的性質以及緩解措施的成功率。

兩年多以來，Cloudflare 一直在對受到攻擊的客戶進行調查，調查中的一個問題是，他們是否收到勒索信，要求付款以換得停止 DDoS 攻擊。2021 年第四季度記錄到有史以來表明勒索威脅的最高調查回應數，勒索攻擊較去年同期成長了 29%，較上一季度成長了 175%。更具體地說，每 4.5 個受訪者中，就有一個 (22%) 報告收到攻擊者要求付款的勒索信。



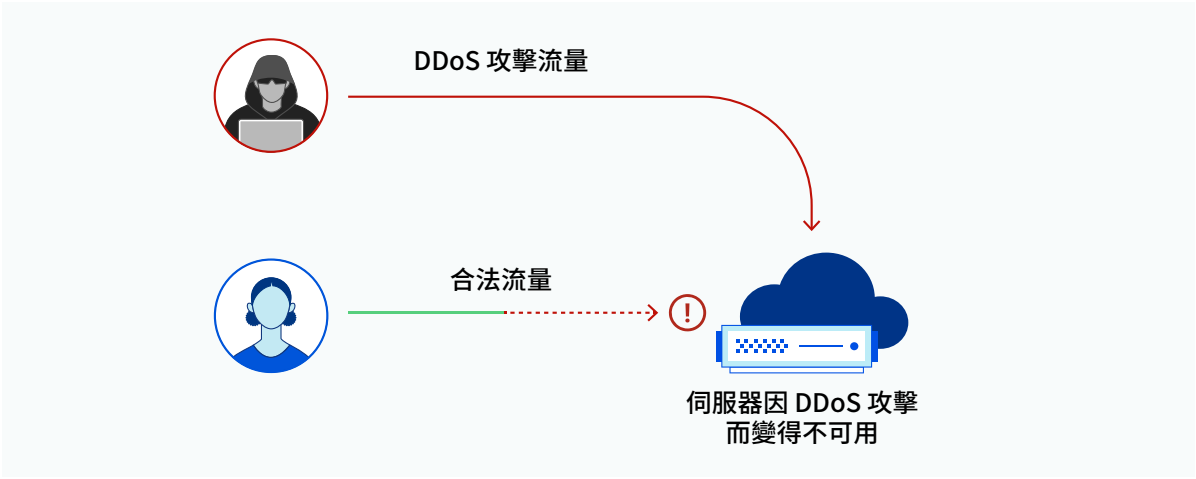
報告受到 DDoS 勒索攻擊或在攻擊前收到威脅的受訪者百分比。

當我們按月份細分，可以發現 2021 年 12 月位居榜首，有 32% 的受訪者報告收到勒索信，幾乎是所有調查受訪者的三分之一。



應用程式層 DDoS 攻擊

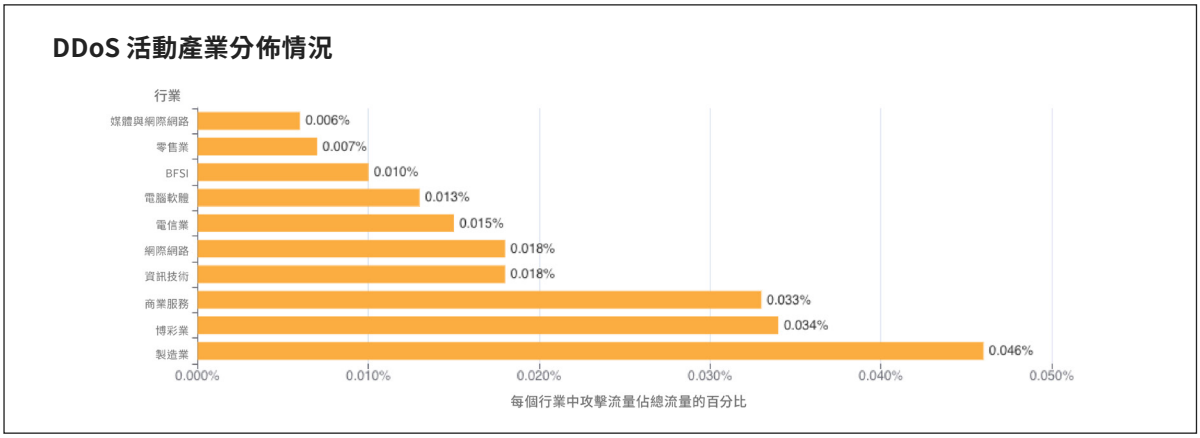
應用程式層 DDoS 攻擊，特別是 HTTP DDoS 攻擊，旨在透過使網頁伺服器無法處理合法使用者請求來破壞它。如果伺服器收到的請求數量超過其處理能力，伺服器將丟棄合法請求甚至崩潰，導致對合法使用者的服務效能下降或中斷。



應用程式層 DDoS 攻擊：行業分佈

在第四季度，製造公司的 DDoS 攻擊數較前一季度成長了 641%，商業服務業的 DDoS 攻擊數成長了 97%。

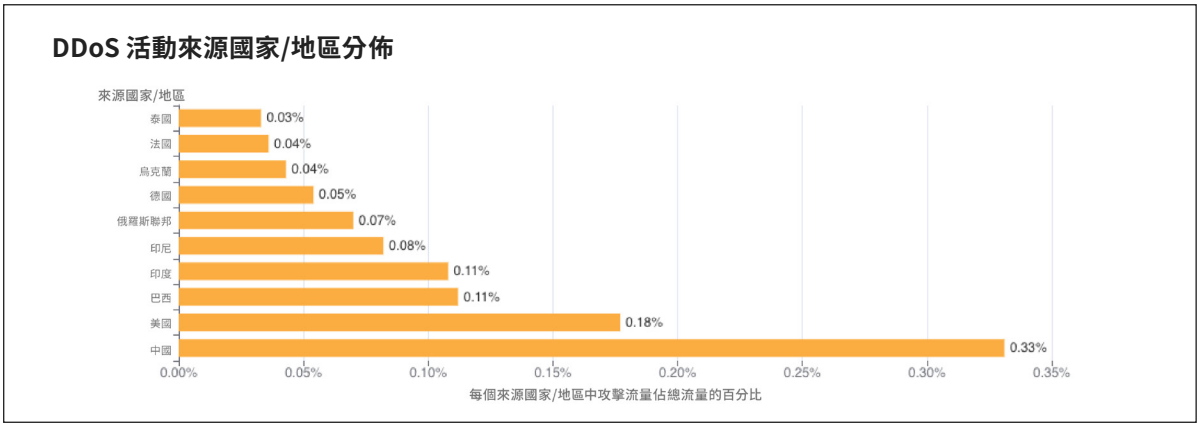
按行業細分受到的應用程式層攻擊，可以發現在 2021 年第四季度，製造業、商業服務和博彩業是受到攻擊最多的行業。



應用程式層 DDoS 攻擊：來源國家/地區分佈

為瞭解 HTTP 攻擊的來源，我們研究了產生攻擊 HTTP 請求之用戶端的來源 IP 位址地理位置。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/地區的高 DDoS 活動百分比通常表明大型殭屍網路在其境內運行。

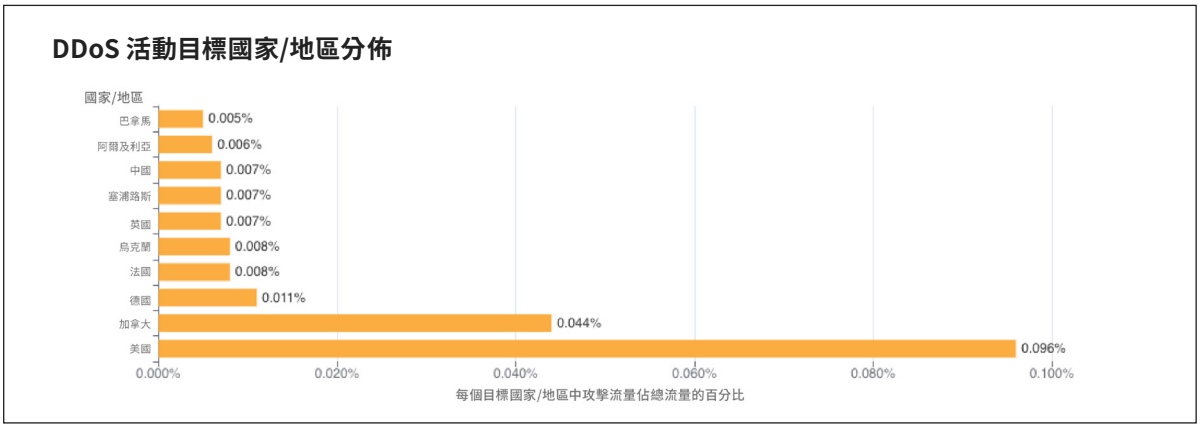
中國仍然是境內 DDoS 攻擊百分比最高的國家，已連續第四個季度位居榜首。每一千個源自中國 IP 位址的 HTTP 請求中，就有超過三個是 HTTP DDoS 攻擊的一部分。美國仍然佔據第二位，之後是巴西和印度。



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。

位於美國的企業今年連續第三次成為 HTTP DDoS 攻擊的最大目標，其次為加拿大和德國。

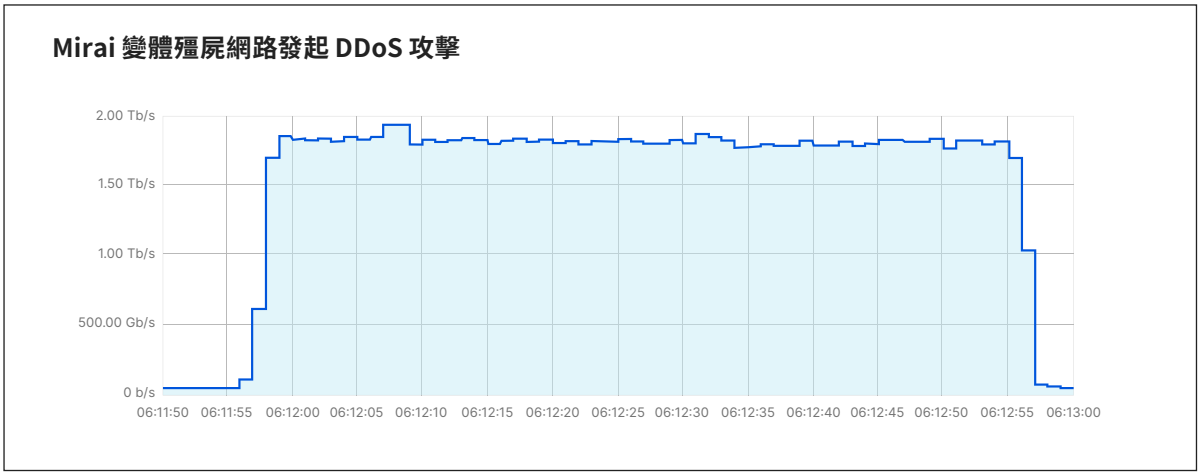


網路層 DDoS 攻擊

應用程式層攻擊的目標是最終使用者嘗試存取的服務所在的應用程式（OSI 模型的第 7 層），而網路層攻擊以網路基礎結構（例如聯網路由器和伺服器）和網際網路鏈路本身為目標。

Cloudflare 阻止了一個接近 2 Tbps 的攻擊

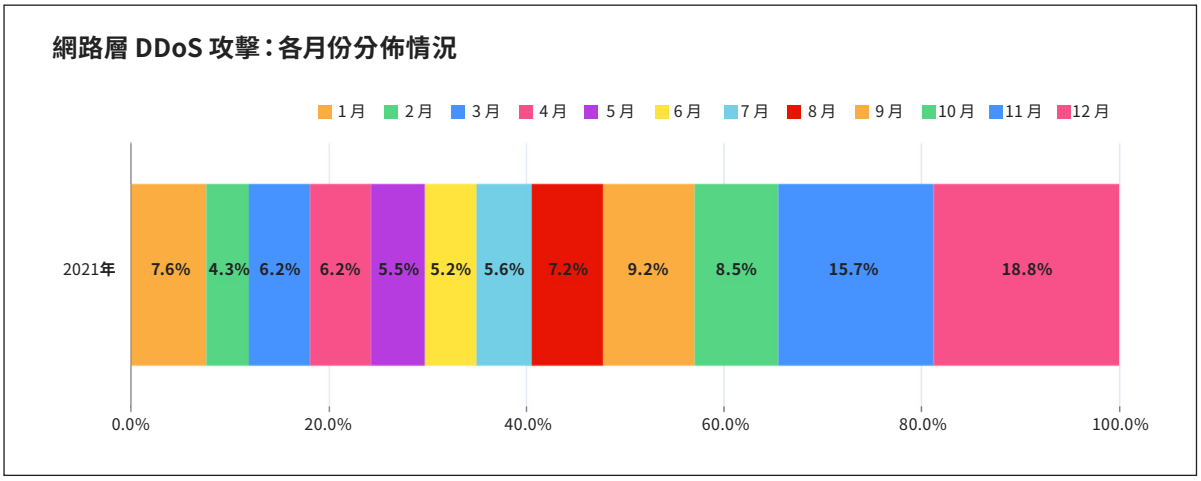
11 月，我們的系統自動偵測到並緩解了一次接近 2 Tbps 的 DDoS 攻擊。這是一次多方位攻擊，結合了 DNS 放大攻擊和 UDP 洪水攻擊。整個攻擊僅持續了一分鐘。攻擊由大約 15,000 個機器人發起，這些機器人在 IoT 裝置和未修補的 GitLab 執行個體上執行原始 Mirai 程式碼的變體。



網路層 DDoS 攻擊：月份分佈

12 月是 2021 年攻擊者最活躍的月份。

第四季度是 2021 年攻擊者最活躍的季度。在 2021 年的所有網路層 DDoS 攻擊中，超過 43% 發生在第四季度。10 月是相對平靜的一個月，11 月，即中國光棍節、美國感恩節假日、黑色星期五和網路星期一所在的這個月，網路層 DDoS 攻擊數幾乎翻倍。在 2021 年 12 月的最後幾天，由於全世界都在為一年的結束做準備，觀察到的攻擊數有所成長。事實上，僅 12 月的總攻擊數就高於 2021 年第二季度的所有攻擊數，幾乎等於 2021 年第一季度的所有攻擊數。



網路層 DDoS 攻擊：攻擊速度分佈

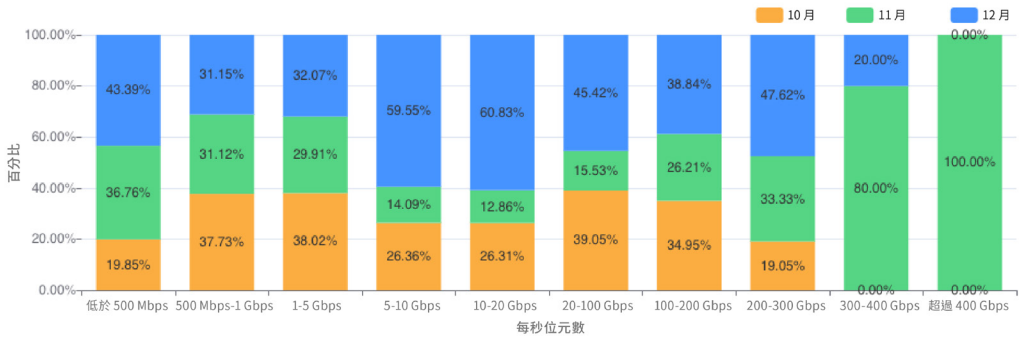
儘管大部分攻擊的規模都相對「較小」，但 TB 強度的攻擊正在成為常態。

衡量第 3/4 層 DDoS 攻擊規模有多種不同的方法。一種方法是測量它傳遞的流量大小，以位元速率為單位（例如，Tbps 或 Gbps）。另一種是測量它傳遞的資料封包數，以封包速率為單位（例如，Mpps：百萬封包/每秒）。

高位元速率的攻擊試圖使網際網路鏈路飽和，而高封包速率的攻擊會使伺服器、路由器或其他聯網硬體裝置不堪重負。這些裝置分配一定的記憶體和計算能力來處理每個封包。因此，透過向裝置發送大量封包，該裝置的處理資源就可能被耗盡。在這種情況下，封包就會「被丟棄」，即裝置無法再處理封包。對使用者而言，這會導致服務中斷和阻斷服務。

下面顯示了按規模（以位元速率為單位）和月份劃分的攻擊分佈。從上面的圖表中可以看到，大部分攻擊都發生在 12 月。然而，下圖則表明，規模超過 300 Gbps 的較大型攻擊都發生在 11 月。介於 5-20 Gbps 之間的大部分攻擊都發生在 12 月。

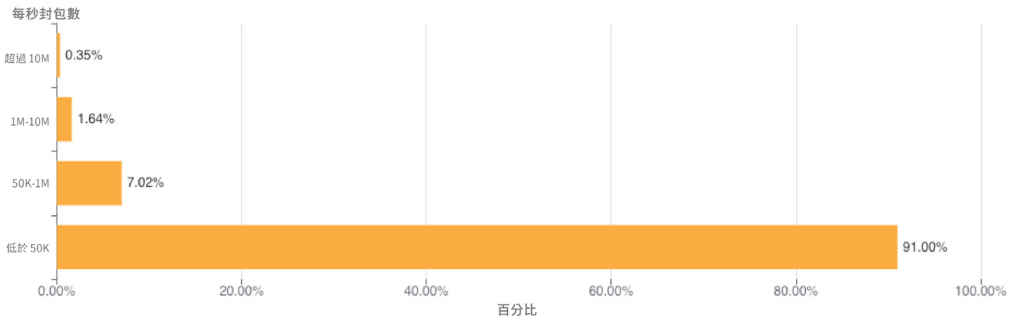
網路層 DDoS 攻擊：各月份規模分佈情況



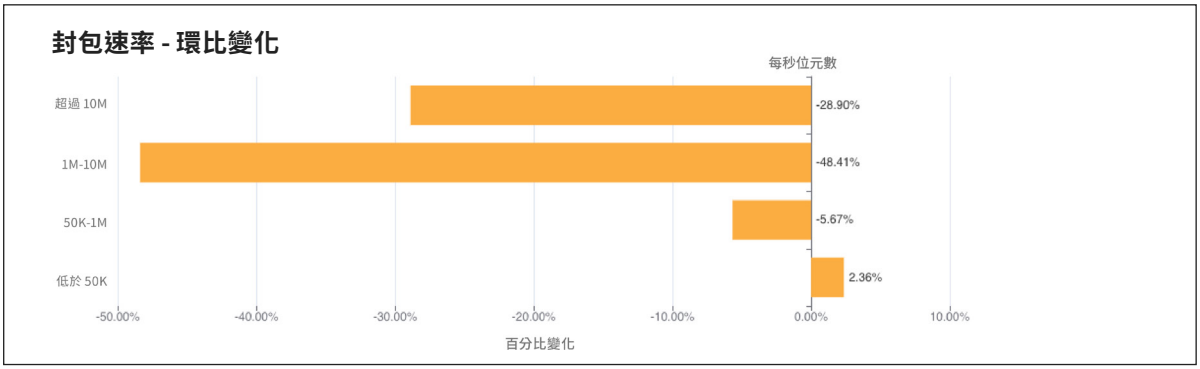
基於封包速率的分佈情況

Cloudflare 觀察到的一個有趣關聯是，當攻擊數量增加時，它們的規模和持續時間會降低。在 2021 年的前八個月，攻擊數相對較少，相應地，它們的速率有所增加。例如，在 2021 年第三季度，攻擊範圍從 1-10 百萬封包每秒 (mpps) 增加了 196%。2021 年第四季度，攻擊數有所增加，但 Cloudflare 觀察到，攻擊規模有所降低。在所有攻擊中，91% 的攻擊峰值低於 50,000 封包數每秒 (pps)，這足以輕而易舉地摧毀未受保護的網際網路財產。

網路層 DDoS 攻擊：封包速率分佈情況

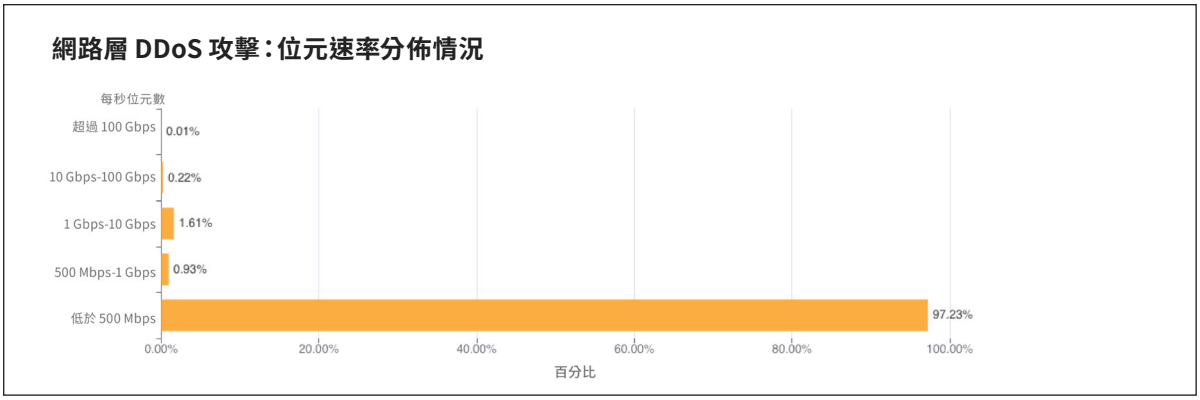


超過 1 mpps 的較大型攻擊較前一季度從 48% 降低至 28%，而峰值低於 50K pps 的攻擊數則較前一季度成長 2.36%。

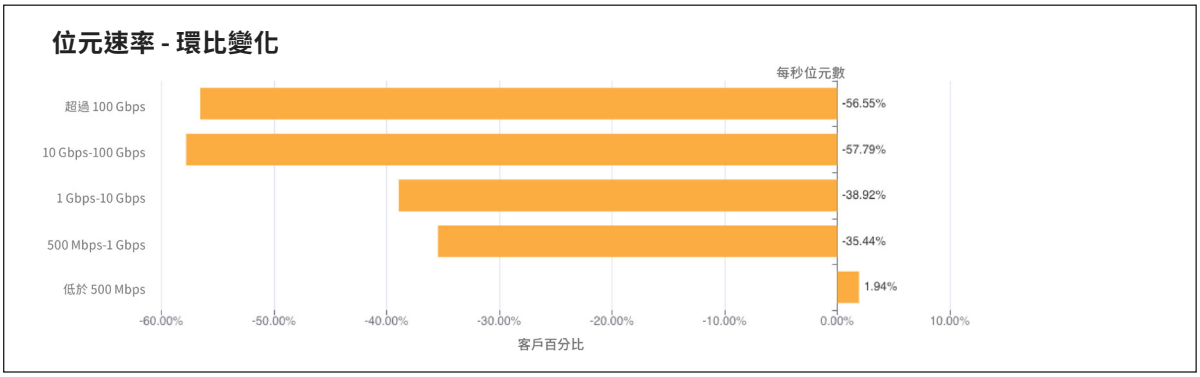


基於位元速率的分佈情況

與高封包量攻擊中觀察到的趨勢相似，高流量攻擊的數量也在減少。儘管超過 1 Tbps 的攻擊正在成為常態，我們目前為止觀察到的最大攻擊峰值已接近 2 Tbps，但大部分攻擊仍然規模較小，且峰值低於 500 Mbps (97.2%)。



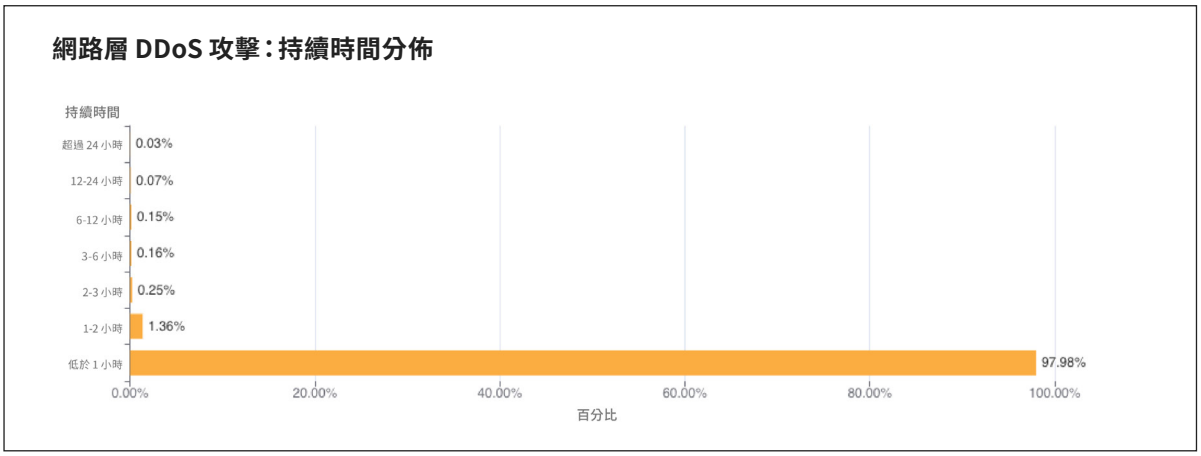
在 2021 年第四季度，高於 500 Mbps 的所有範圍的較大型攻擊都從 35% 減少至 57%，尤其是超過 100 Gbps 的攻擊。



網路層 DDoS 攻擊：持續時間分佈

大多數攻擊的持續時間都在 1 小時以內，再次表明有必要採取始終啟用的自動 DDoS 緩解解決方案。

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該攻擊特徵且前往該特定目標的最後一個封包之間的時間差。在 2021 年的最後一個季度，98% 的網路層攻擊持續時間不到一個小時。這十分常見，因為大部分攻擊持續時間很短。有意思的是，我們發現一個趨勢，當攻擊數量增加時，它們的速率和持續時間會降低。



短時間的攻擊很可能不被察覺，特別是爆發攻擊，此類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，依賴于安全分析來手動緩解的 DDoS 保護服務沒有機會及時緩解攻擊。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指紋的新規則，期望下次能捕捉到它。同樣，使用「按需」服務（即安全團隊在遭到攻擊時將流量重定向至 DDoS 保護提供商）也無濟於事，因為在流量到達按需 DDoS 保護提供商前，攻擊就已經結束了。

建議公司使用常駐的自動化 DDoS 防護服務來分析流量，並足夠快速地套用即時指紋識別以封鎖持續時間短暫的攻擊。

攻擊手段

SYN 洪水依然是攻擊者最喜歡使用的攻擊方法，而基於 SNMP 的攻擊則出現激增，較前一季度成長了將近 5,800%。

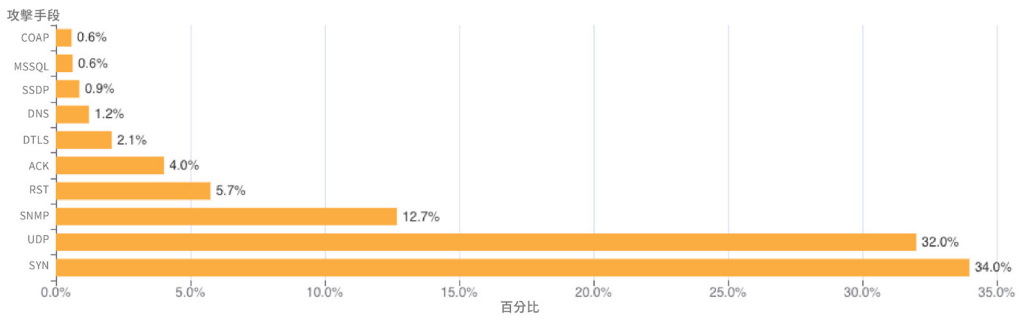
「攻擊手段」一詞用於描述攻擊者用來發起 DDoS 攻擊的方法，如 IP 通訊協定、TCP 旗標等封包屬性、洪水方法和其他條件。

SYN 洪水攻擊在 2021 年首次出現大幅減少。整個 2021 年，SYN 洪水攻擊平均佔據所有網路層攻擊的 54%。儘管仍然佔據最常見攻擊手段的席位，但其份額從上一季度的 38% 降低到 34%。

然而，SYN 攻擊和 UDP 攻擊勢均力敵。UDP 洪水攻擊是一種阻斷服務攻擊，會將大量使用者資料包通訊協定 (UDP) 封包傳送至目標伺服器，旨在擊垮該裝置處理和回應的能力。通常，保護該目標伺服器的防火牆也會因 UDP 洪水攻擊而變得精疲力盡，導致阻斷為合法流量提供服務。UDP 攻擊從 2021 年第三季度的第四位一躍成為第四季度的第二位，佔據總網路層攻擊的 32%，較上一季度成長了 1,198%。

排在第三位的是 SNMP，這是一匹黑馬，2021 年才首次出現在主要攻擊手段中，短短時間取得了巨大的飛躍。

網路層 DDoS 攻擊：熱門攻擊手段分佈



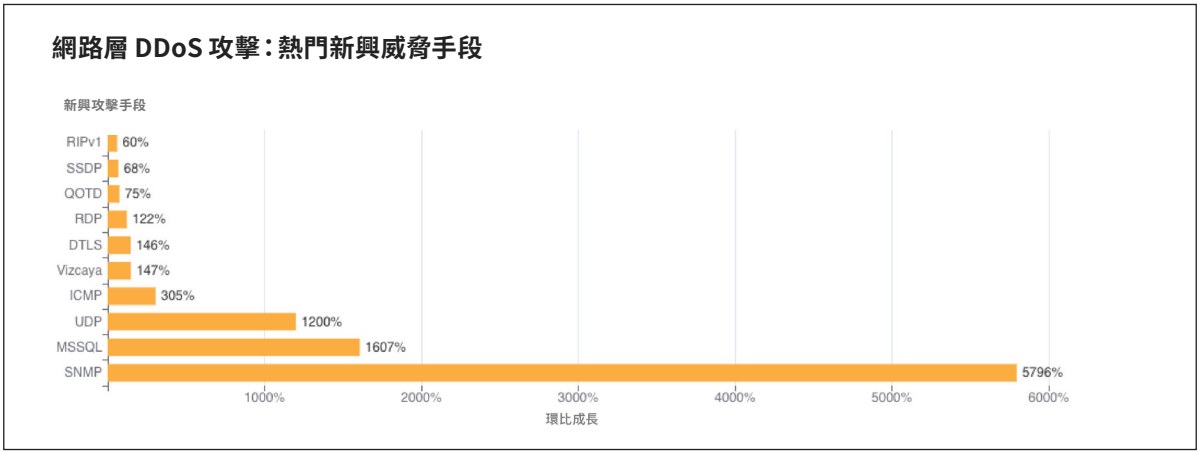
新興威脅

當我們研究新出現的攻擊手段時（這能幫助我們瞭解攻擊者正使用什麼新手段來發動攻擊），我們發現 SNMP、MSSQL 和基於 UDP 的泛型 DDoS 攻擊出現了激增。

SNMP 和 MSSQL 攻擊都透過偽造目標的 IP 位址作為用於觸發攻擊的封包中的來源 IP，從而在目標上反射和放大流量。

簡單網路管理通訊協定 (SNMP) 是基於 UDP 的通訊協定，通常用於在 UDP 知名連接埠 161 上探索和管理家庭或企業網路中的印表機、交換器、路由器和防火牆等網路裝置。在 SNMP 反射攻擊中，攻擊者傳送大量 SNMP 查詢，並在封包中偽造來源 IP 位址作為網路中裝置的目標，這樣，反過來回覆到該目標的位址。來自裝置的大量回應會導致目標網路受到 DDoS 攻擊。

與 SNMP 放大攻擊相似，Microsoft SQL (MSSQL) 攻擊基於一種技術，濫用 Microsoft SQL Server 解析通訊協定發起基於反射的 DDoS 攻擊。當 Microsoft SQL Server 回應用戶端查詢或請求時就會發生攻擊，嘗試利用 Microsoft SQL Server 解析通訊協定 (MC-SQLR) 接聽 UDP 連接埠 1434。



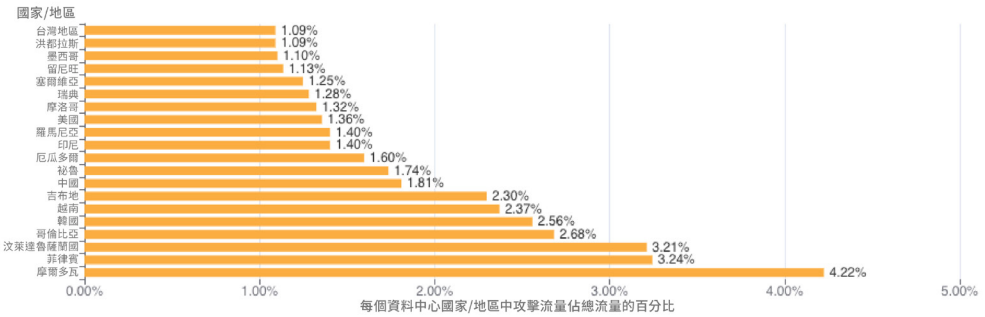
網路層 DDoS 攻擊：國家/地區分佈

源自摩爾多瓦的攻擊數翻了四倍，使其成為網路層 DDoS 活動百分比最高的國家。

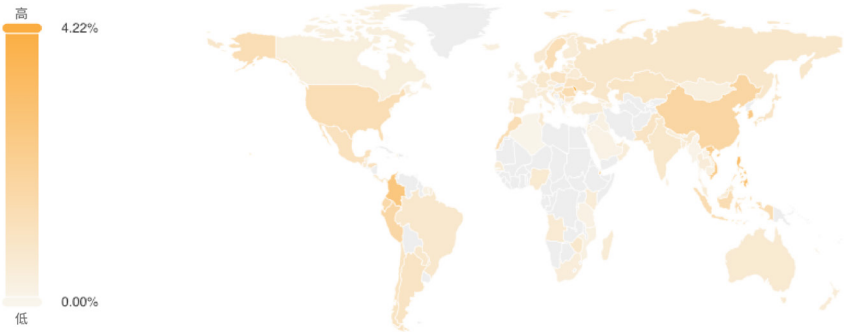
在分析網路層 DDoS 攻擊時，我們統計流量的依據是接收流量的 Cloudflare 邊緣資料中心位置，而不是源 IP。這樣做的原因在於，攻擊者在發起網路層攻擊時，可以通過偽造來源 IP 位址來混淆攻擊來源並在攻擊屬性中引入隨機性，這可能會使簡單的 DDoS 防護系統更難攔截攻擊。因此，如果我們根據偽造的源 IP 推導出源國家/地區，我們將得到一個偽造的國家/地區。

Cloudflare 能夠透過根據觀察到攻擊的資料中心位置顯示攻擊資料來克服偽造 IP 帶來的挑戰。我們在全球 250 多個城市擁有資料中心，因而能夠在報告中體現準確的地理位置。

DDoS 活動 Cloudflare 資料中心國家/地區分佈



網路層 DDoS 攻擊 - 排名前列的國家/地區 (全球)



要檢視所有國家和地區，請查看互動式地圖。

概述

Cloudflare 的使命是幫助建構更好的網際網路，讓所有人擁有更快速、更安全、更可靠的體驗，即使在面臨 DDoS 攻擊時也是如此。作為我們使命的一部分，自 2017 年開始，我們一直在為所有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。為反擊攻擊者的優勢，我們想要確保所有規模的組織都能夠簡單且免費地保護他們自身，防禦所有類型的 DDoS 攻擊。

尚未使用 Cloudflare？立即開始。