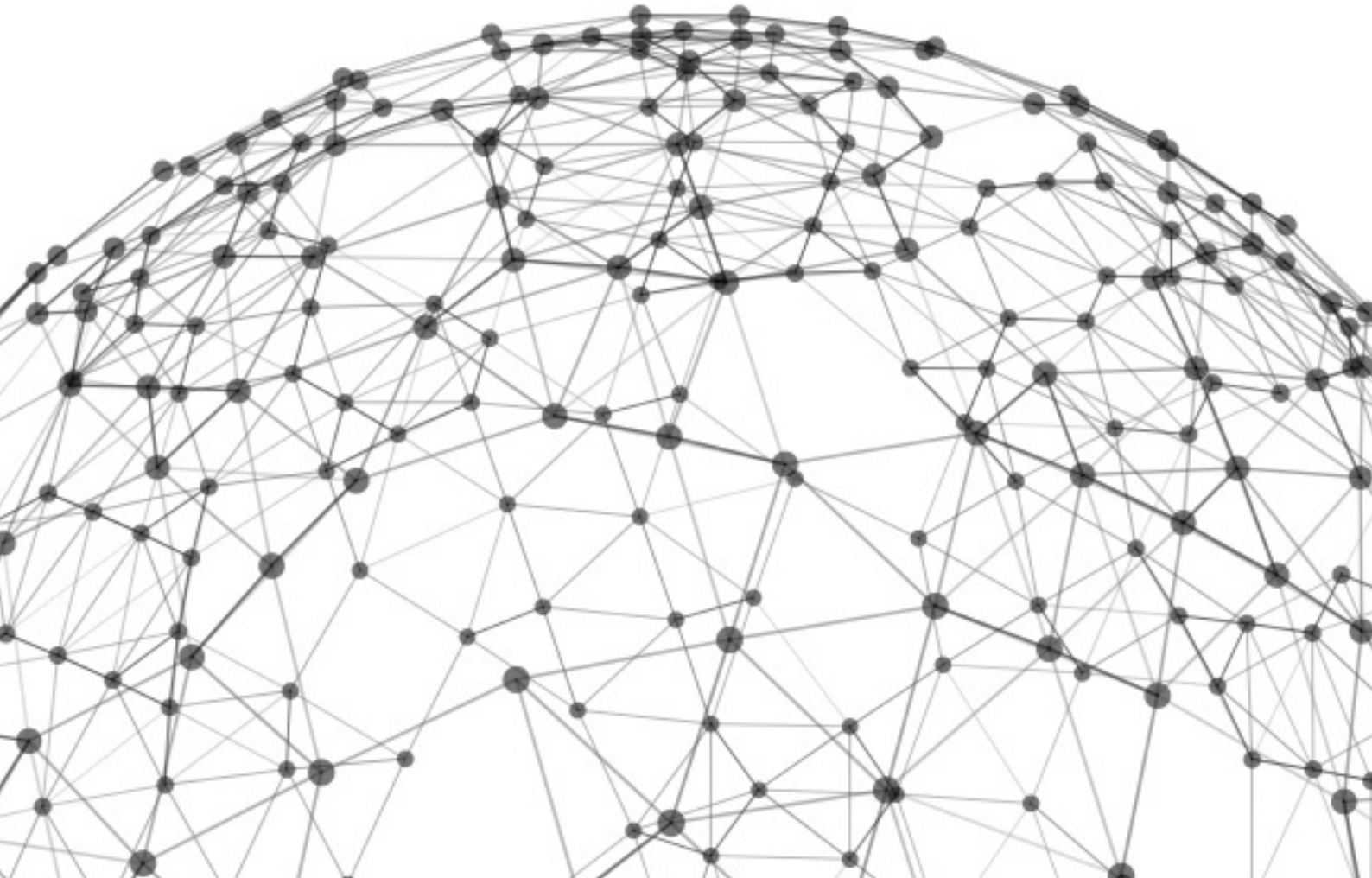
威睿科技

2021年

DDoS攻擊現狀與趨勢調查

威睿DDoS安全防禦團隊

genie 威睿科技



內容

P3 ..... 前言

P4 ..... 攻擊頻率

整體趨勢
類型分佈
類型趨勢
時長分佈

P8 ..... 攻擊規模

整體趨勢
類型分佈
規模分佈

P11 ..... 攻擊來源

地理位置分佈

P12 ..... 巨量攻擊

攻擊趨勢
案例分析(一)
案例分析(二)

P15 ..... 結語

前言

回顧2021年，網路駭客絲毫不曾停下腳步，持續為企業組織帶來各種資安威脅，這其中又以巨量規模的分散式阻斷服務攻擊(Distributed Denial of Service, DDoS)最受關注。儘管全球疫情逐漸得到控制，遠端工作與線上活動早已成為人們的新生活常態，企業數位轉型潮流加速延燒，加上各種新興網路技術如5G、IoT、及區塊鏈等推波助瀾下，不僅大幅降低了DDoS攻擊的門檻，更提供了駭客更多開闢新戰場的機會。在萬物連網的後疫情時代，DDoS防禦已然成為各大電信網路運營商及企業維持競爭力及永續經營的關鍵考量點。

相較於疫情剛爆發的2020年，2021年整體DDoS資安事件不減反增，整體攻擊流量也持續攀升創新紀錄，在攻擊規模與強度的增長趨勢下，攻擊手法也不斷進化，變得更多元複雜。相較於2020年，Tera bps等級規模的DDoS攻擊大幅增加，混合式攻擊(Multi-vector attack)也出現的更頻繁，並結合更多元的攻擊向量，創造出單月最大攻擊規模的新紀錄。

身為電信級DDoS檢測市場中的領導者，威睿科技每年針對DDoS攻擊活動的趨勢進行調查及統計。 本報告的調查對象涵括了亞太區數個指標性電信運營商網路，針對2021全年度進行持續性的DDoS攻擊資料收集與統計分析。這些運營商的網路服類型，包含了網際網路接取服務(Internet connection services) 、資料中心/主機代管中心(Data center/co-location services)、行動數據服務(Mobile data network infrastructure)等。

由於威睿科技的GenieATM解決方案，專精於針對網路第3、第4層的巨量型(Volumetric) DDoS攻擊檢測分析，因此本調查報告的統計分析對象也主要鎖定巨量型DDoS攻擊。除了攻擊方式的類型分佈、趨勢、規模、時長、來源分布等進行量化的統計外，也將分享2021年度規模最大的兩個巨量攻擊案例剖析。

在網路攻擊與數位科技同步發展的趨勢下，可以預見未來的攻擊數據將持續超越既有的紀錄。期盼這份調查報告，不僅能提供DDoS攻擊的相關趨勢及深入見解，也能協助提升運營商及企業的資安警覺意識，做為制定網路安全政策及防禦工作部署的參考依據。

威睿DDoS安全防禦團隊

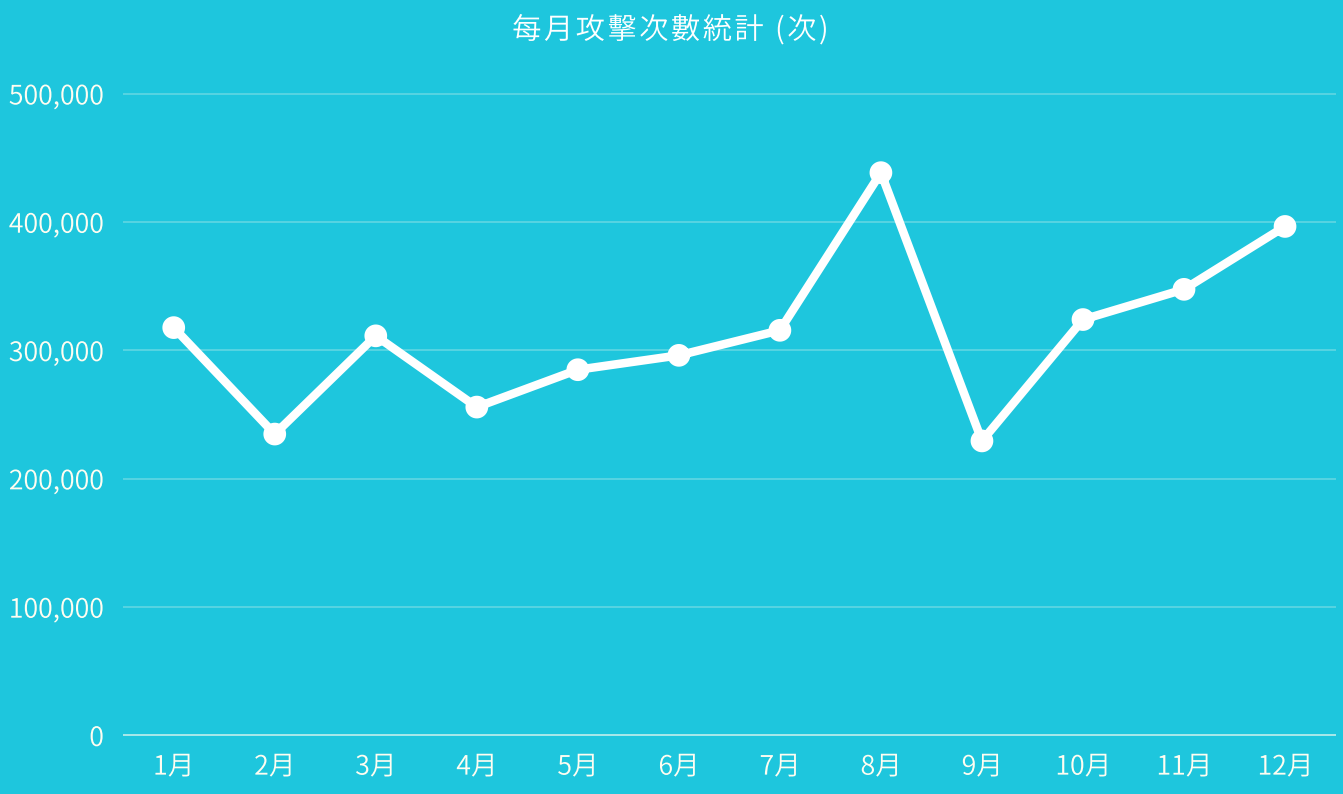
2022/3

攻擊頻率

攻擊頻率趨勢

觀察2021年參與本研究的電信運營商透過Genie產品檢測到的DDoS攻擊事件頻率，全年總計約375萬次，此結果和2020年觀測到的數字幾乎相當 (2020年約為370萬次)。每個月觀測的攻擊事件，約略在22萬到44萬次之間，以8月份到達最高峰的將近44萬次，以9月份的次數最少約為23萬次。逐月攻擊頻率有相當程度的波動，每月成長/衰退幅度(MoM+)約在-50%～+50%之間，平均每月約有31萬次的攻擊。相當於：

- 每日有10,283次；
- 每小時有428次；
- 每分鐘有7次攻擊發生。



攻擊頻率

攻擊類型佔比

在此次觀察報告中，我們統計數十種的DDoS攻擊類型(Attack Vector)，而這些攻擊主要又可分為幾大類別：TCP洪水攻擊(如SYN Flooding、RST Flooding、SYN-RST Flooding...等)、UDP洪水攻擊、協議濫用攻擊(如Malformed TCP封包、Malformed UDP封包、Land Attack、IP Protocol Null、ICMP濫用…等)、反射放大攻擊(如SSDP Amplification、NTP Amplification、CLDAP Amplification、DNS Amplification ...等)、 蠕蟲攻擊 (如SQL Slammer、Code Red、Sasser...等)、應用層洪水攻擊等。

觀察統計2021的DDoS攻擊事件頻率，前五大最常出現的攻擊類型分別為：

1 **30.6%** TCP SYN 洪水攻擊

2 **25.4%** SSDP反射 放大攻擊

3 **13.0%** NTP反射 放大攻擊

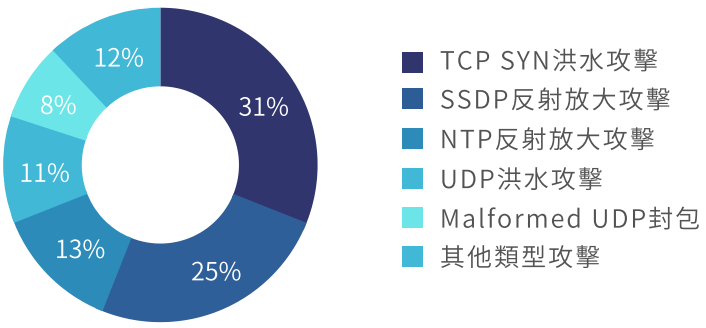
4 **10.6%** UDP 洪水攻擊

5 **8.4%** Malformed UDP封包 (埠號為0)

12.0% 其他類型 攻擊

若以大類別歸納，2021年最主要的攻擊型態為反射放大攻擊，其次為UDP及TCP SYN洪水攻擊。

攻擊頻率的類型佔比



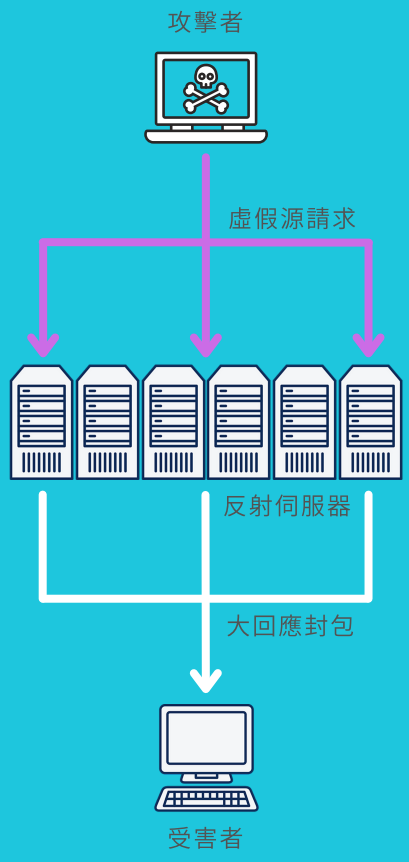
觀察2021年前五大常出現的攻擊向量(Attack Vector)，和前一年(2020)的觀測結果完全相同，只有排名和佔比上的稍微改變。TCP SYN洪水攻擊躍升成為最常見的攻擊型態(由2020年的18.2%到2021的30.6%)，而SSDP反射放大攻擊和NTP反射放大攻擊的排名也超越UDP洪水攻擊。

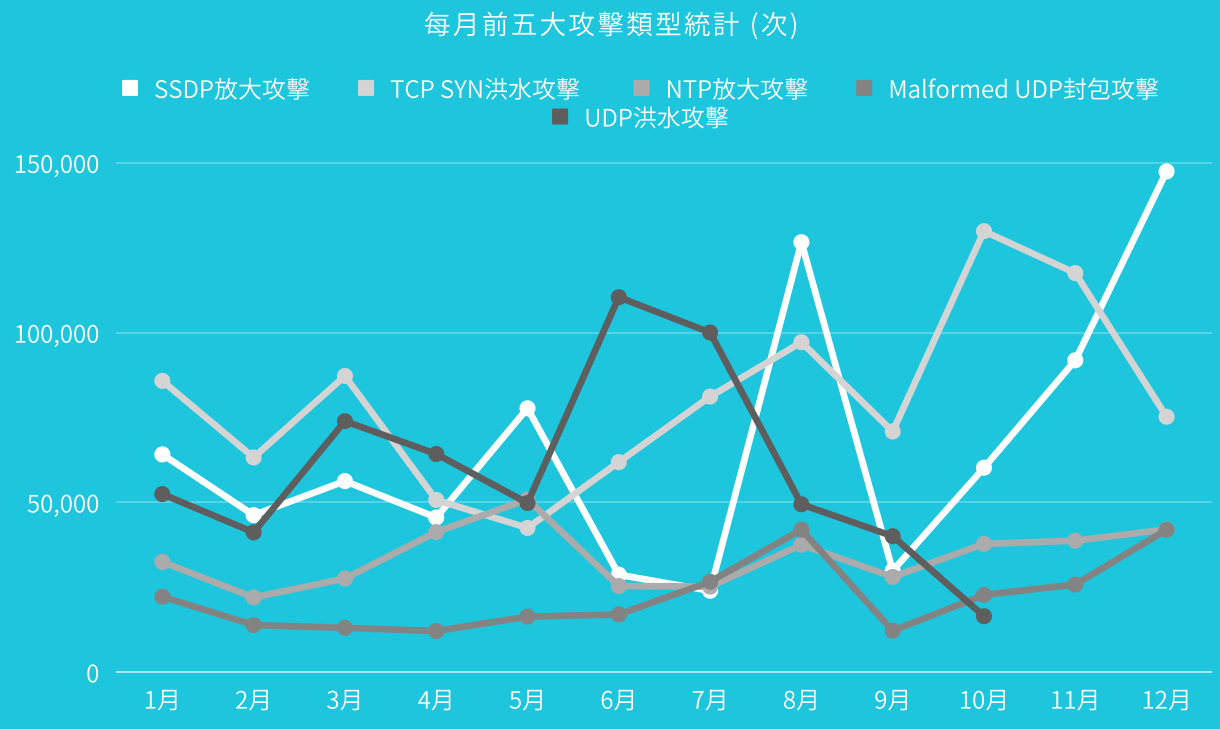
攻擊頻率

攻擊類型趨勢

2021年的逐月Top5攻擊向量(Attack Vector)類型沒有太大變動，大致上都是UDP洪水攻擊、TCP洪水攻擊、SSDP反射放大攻擊、NTP反射放大攻擊及 Malformed UDP封包攻擊分佔前5名，除了在11，12月份DNS反射放大攻擊擠進前5名之外。

此外，排名第5的Malformed UDP 封包(埠號為0)攻擊流量的形成，經觀察分析發現，主要是反射放大攻擊的伴隨效應。因為在如SSDP、NTP等反射放大攻擊的攻擊過程中，通常會使得反射伺服器以極大的UDP封包回應攻擊者的虛假請求 (Spoofed IP Requests)，而這些被利用作為反射放大攻擊的反射伺服器通常會回應以放大倍率(Amplification Factor)極高的大封包。而過大的UDP封包在傳送時需要被切段(Fragmentation)成較小的IP封包傳送，使得除了首個IP封包片段(fragment)帶有UDP封包標頭(header)的完整的資訊外，其他後續的IP片段封包則會被路由器視為沒有UDP封包標頭，造成後續IP片段封包被路由器等識別統計為UDP源/目的埠號均為0的通訊協定異常封包。所以，Malformed UDP封包攻擊流量常高居第5名，是反映出主要攻擊型態為反射放大攻擊的現況。





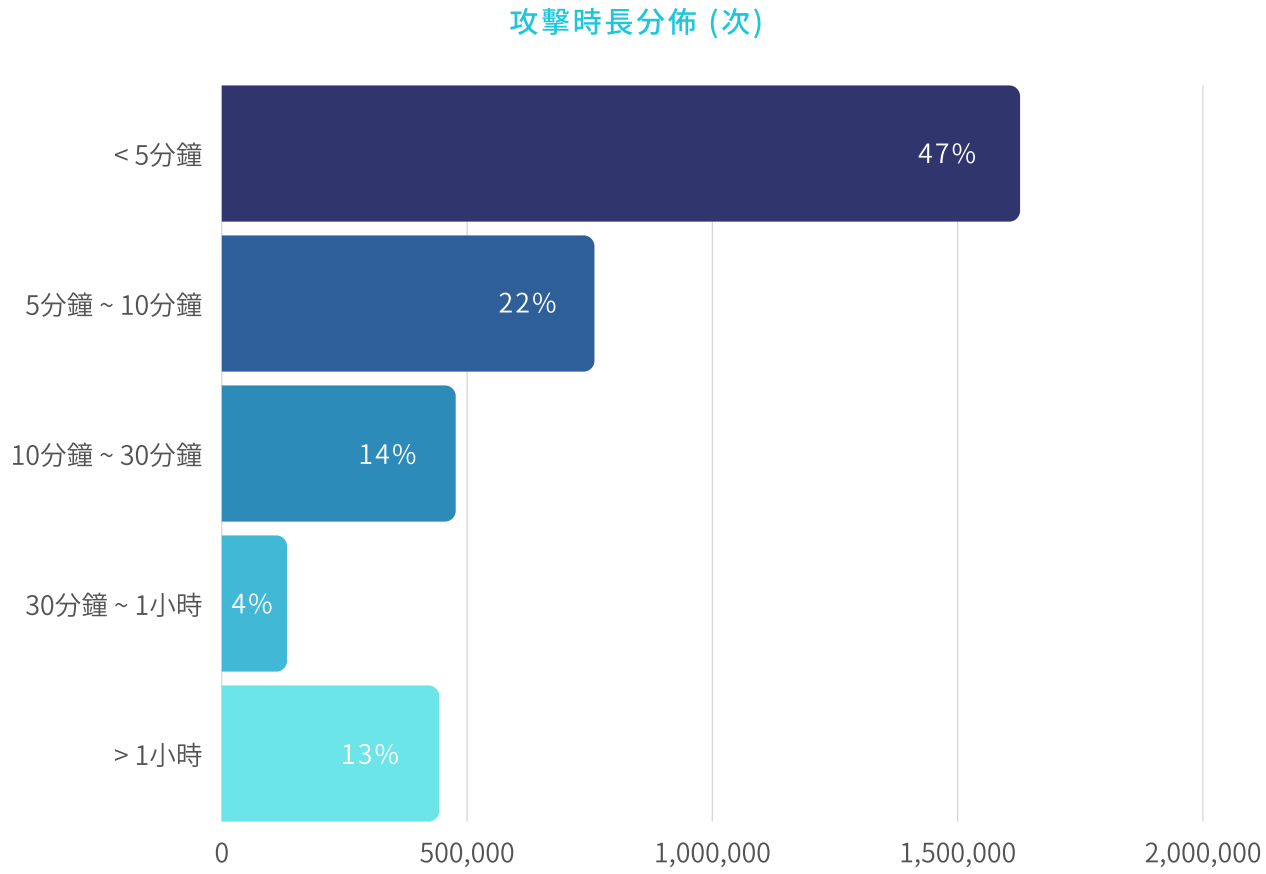
攻擊頻率

攻擊時長分佈

統計2021觀測的DDoS攻擊事件，每次攻擊的持續時間平均為62.7分鐘 (約1小時)。

我們觀察到將近半數的攻擊事件持續時間都在短於5分鐘內就會結束，約有36%的攻擊事件持續時間都在5到30分鐘之間，而長於1小時的攻擊僅佔全部事件的13%，然而平均攻擊時長卻長達一個小時。這是因為雖然長於1小時的攻擊次數僅佔少數，但其持續時間往往不只是1個多小時，部份攻擊甚至持續了數十小時、數日的時間，因此在統計上會大幅拉高整體時長的平均值。

此外，極大比例的攻擊從出現、產生大規模流量、到攻擊流量結束，時間持續不過短短數分鐘。因此能否在流量巨增之初，就能以最快的時間檢測、告警及處理，將會是對巨量DDoS攻擊防禦的重要關鍵之一。



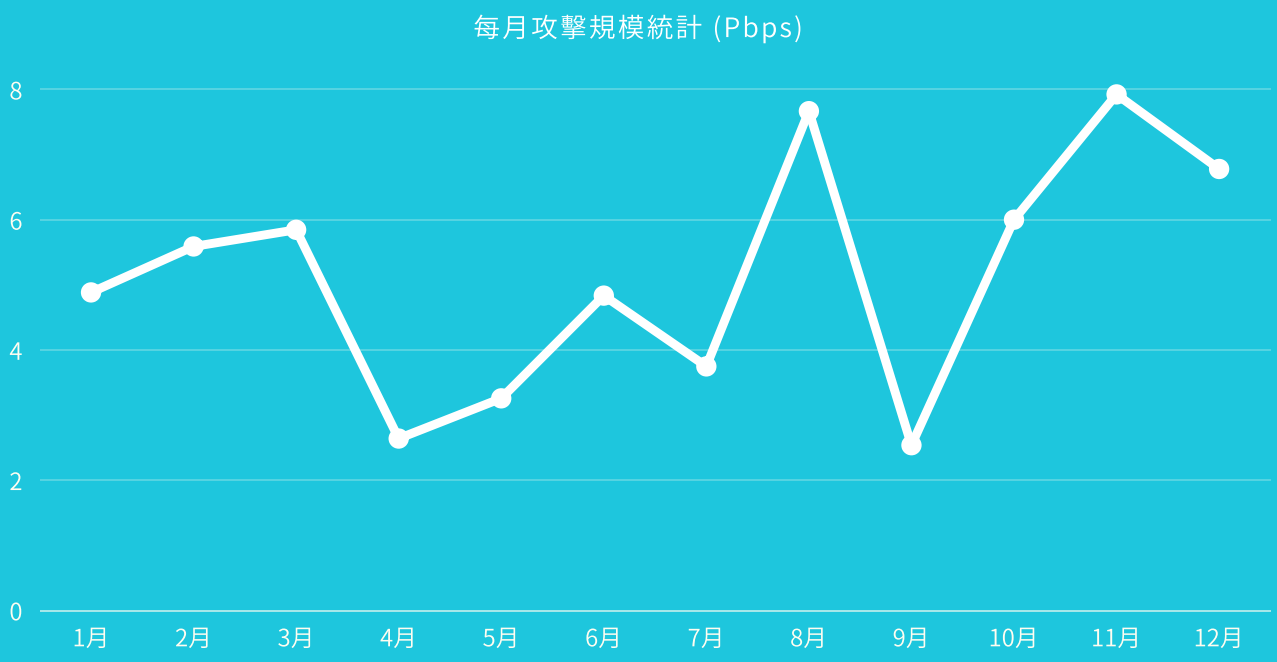
攻擊規模

攻擊規模趨勢

觀察2021年參與本研究的電信運營商透過Genie產品檢測到的DDoS攻擊事件流量，全年總計約61.7 Peta bps。每個月觀測的攻擊事件，約略在2 Pbps到8 Pbps之間，以11月份到達最高峰的將近8 Pbps，以9月份的次數最少為近2.5 Pbps。逐月攻擊頻率有相當程度的波動，每月攻擊流量大小成長/衰退幅度(MoM+)較次數頻率波動更大，約在-70%～+140%之間，平均每月約有5.1 Pbps的攻擊。相當於：

- 每日約有169 Tbps的攻擊流量；
- 每小時有 7 Tbps的攻擊流量；
- 每分鐘就有 117.4 Gbps的攻擊流量在網路上流竄。

和前一年(2020)檢測到的攻擊流量相比，我們可以觀察到約有 21%的成長。而相較於在參與本研究的電信運營商檢測到的攻擊次數全年僅有1.3%成長的前提下，我們可以發現在2021年的DDoS攻擊的模式為單次攻擊流量的規模較過去更為巨大。



攻擊規模

攻擊類型分佈

2021觀測到的DDoS攻擊事件，以攻擊流量的規模統計，前五大攻擊向量類型(Attack Vector)分別為：

1 **30.1%** TCP SYN 洪水攻擊

2 **25.6%** SSDP反射 放大攻擊

3 **13.9%** Malformed UDP封包 (埠號為0)

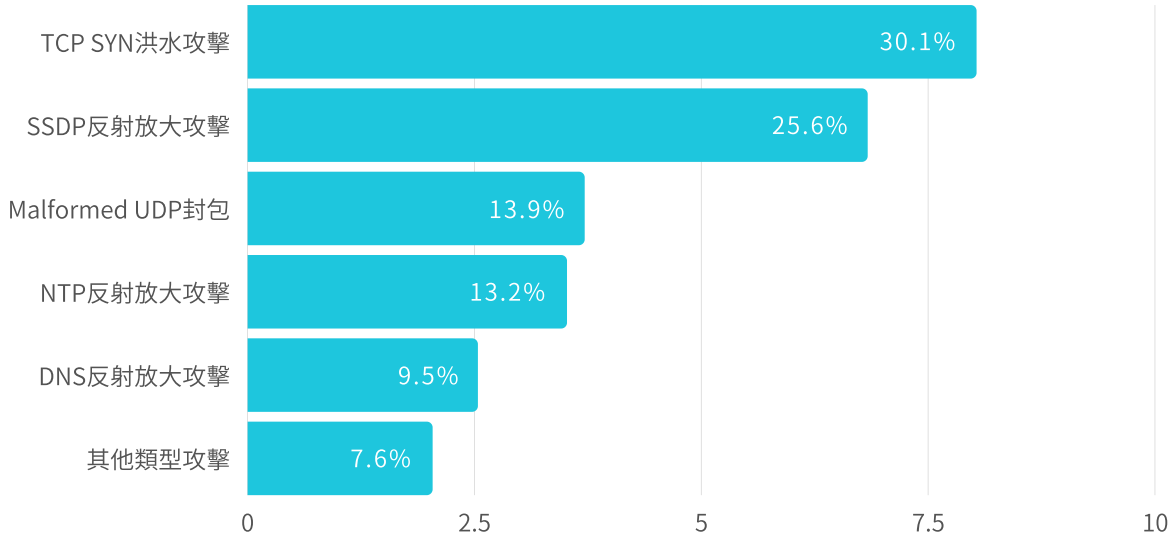
4 **13.2%** NTP反射 放大攻擊

5 **9.5%** DNS 反射 放大攻擊

7.6% 其他類型 攻擊

由統計結果可以發現，2021年的攻擊流量規模佔比前五名與攻擊頻率佔比前五名極為相似，尤其第一與第二名皆為TCP SYN洪水攻擊及SSDP反射放大攻擊，且其攻擊規模佔比與攻擊頻率佔比幾乎相同。

攻擊規模的類型佔比 (Pbps)



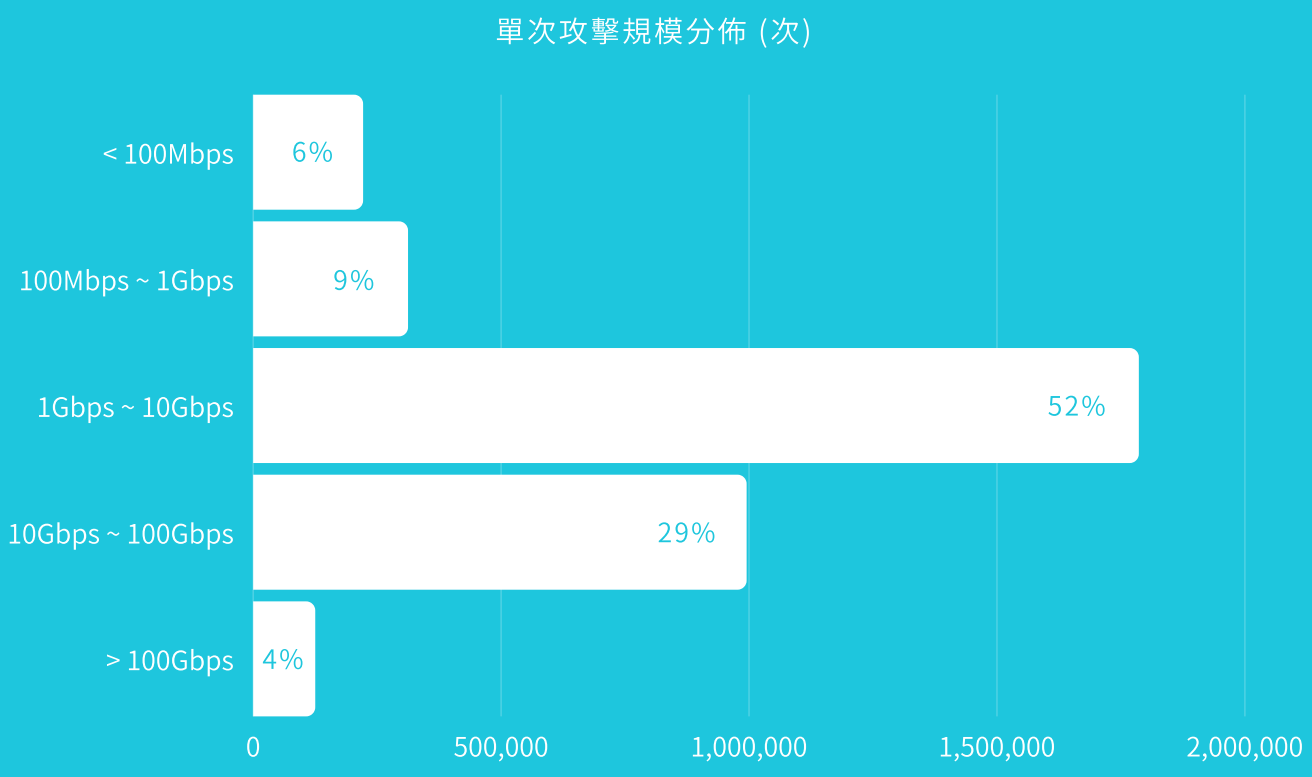
攻擊規模

攻擊大小分佈

統計2021年觀測到的DDoS攻擊事件，

- 單次攻擊的平均峰值大小約17.5 Gbps，
- 單次攻擊峰值大小最多落在1 Gbps到10 Gbps間。

進一步分析不同攻擊類型的單次攻擊規模，發現不同攻擊類型單次攻擊峰值平均規模差異極大。單次攻擊峰值平均規模較大的攻擊類型有IP Protocol錯誤(Null)、Memcached攻擊、反射放大攻擊、Malformed TCP 或UDP封包攻擊等，其單次攻擊平均規模高達50 Gbps以上；而單次攻擊峰值平均規模較小的攻擊類型則有像蠕蟲攻擊及特定協議誤用攻擊等，其單次攻擊一般在數百Mbps的規模。



攻擊來源

地理位置分佈

觀察2021年檢測到的DDoS攻擊事件，統計攻擊源IP的地理區域，約有24.6%的攻擊來自於中國，其餘高排名地區為美國、日本、香港、新加坡及澳洲等。

需注意的是，這項統計是由攻擊流量的源IP位址去查找攻擊流量的來源國家分佈。但這樣的資訊並不一定真實反應一般人心目中所想像的「攻擊者位置」。首先，許多的DDoS攻擊會使用假造源位址(Source IP Spoofing)的技巧，以躲避資安防禦技術的追蹤查找。要能辨識出某一攻擊流量是否有虛假源地址，常需以源IP位址搭配網路設備介面和相關網路配置等資訊進行查找。但因此次統計分析的涵蓋規模極廣且跨越不同的電信運營商網路，故尚未對攻擊流量源是否為假造進行分析。

此外，在反射放大攻擊中，本報告所統計的攻擊流量源IP位置代表的是反射伺服器(Reflection Server)的所在位置(如圖1所示)；又或是在殭屍網路(Botnet)攻擊中，本報告統計的是被感染主機(Bots)(又名「肉雞」)的位置(如圖2所示)，並不代表發起駭客或C&C伺服器的所在地理位置分佈。

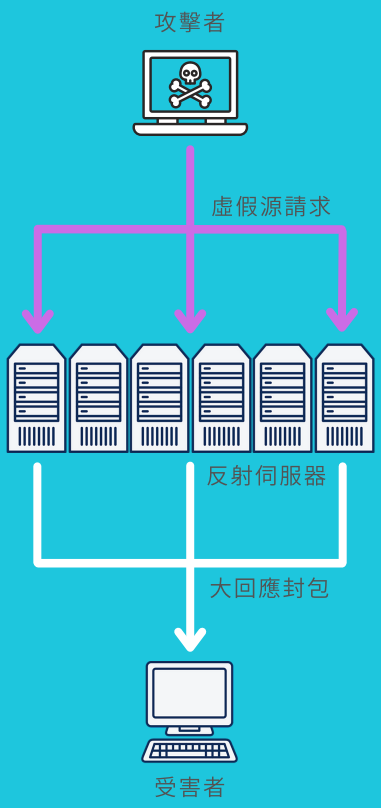


圖1

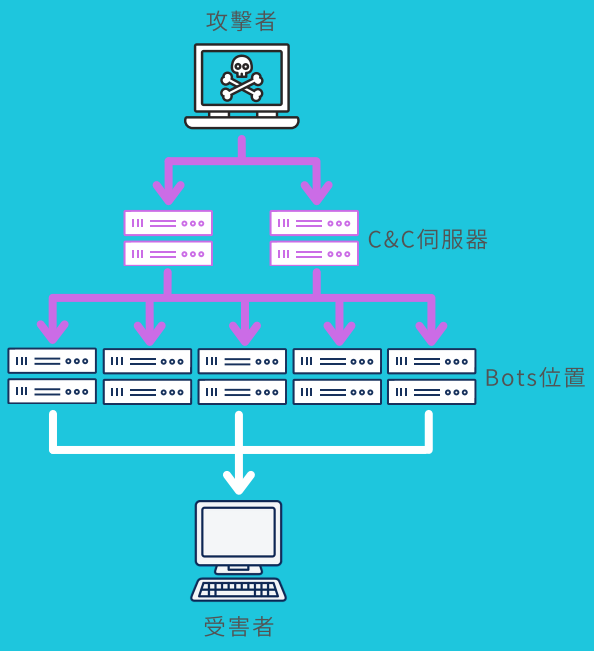
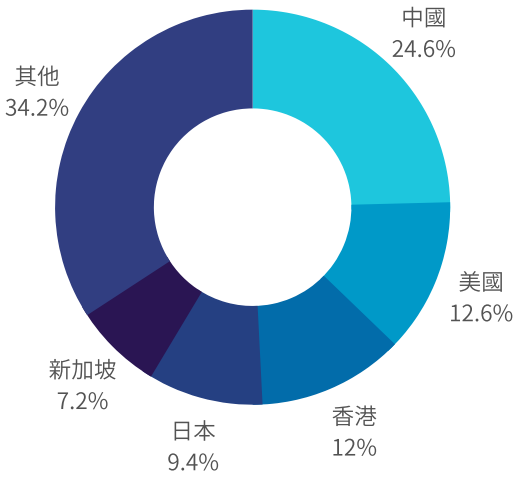


圖2

攻擊來源地區分佈



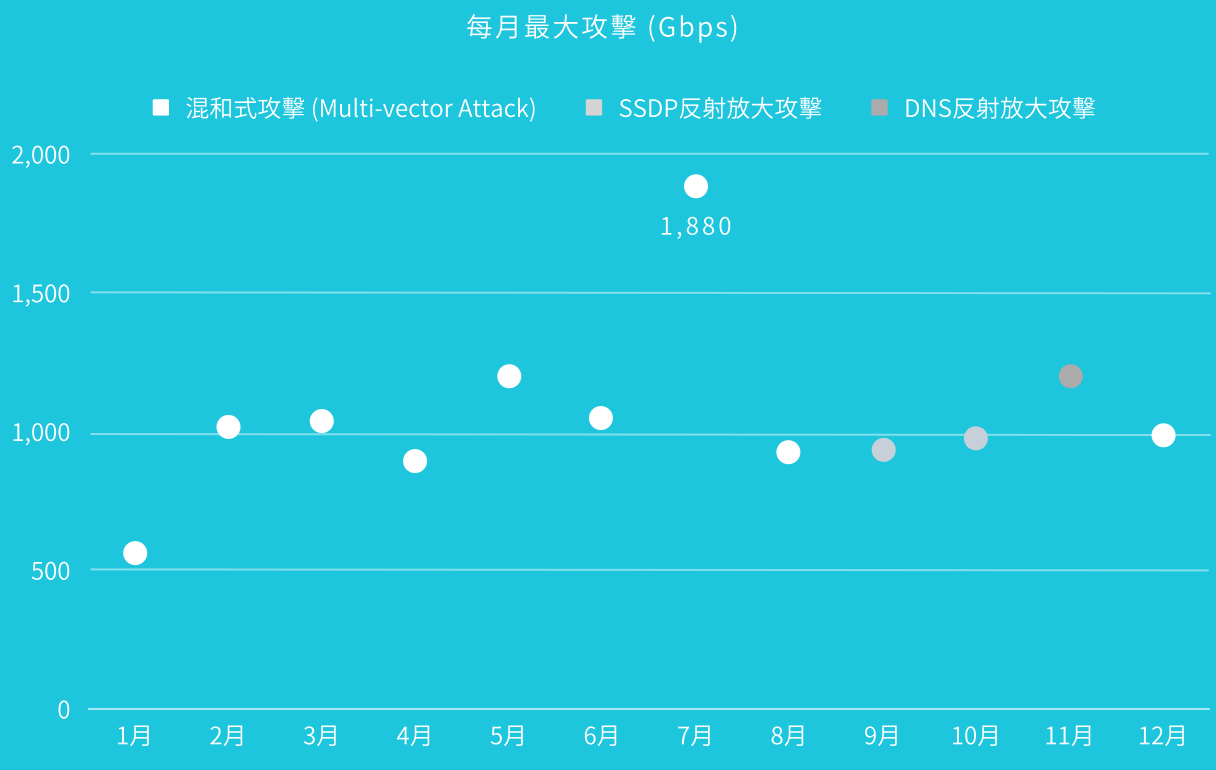
巨量攻擊

逐月巨量攻擊趨勢

以每個月為單位，我們記錄了每月的最大攻擊規模及其類型。由下圖表可見，參與本研究的電信運營商2021全年透過Genie產品檢測到的最大攻擊事件發生在7月間，其攻擊流量規模高達1.88Tbps，而每月最大攻擊的規模一般落於500Gbps至1.2Tbps之間。

與2020年的觀測結果相比，
巨量攻擊在2021年的規模平均成長了約65%，
清楚地呈現出DDoS巨量攻擊逐年成長的趨勢。

觀察發現巨量攻擊的型態主要多為由UDP反射放大攻擊向量組合而成的混合式攻擊(Multi-vector attack)、或特定類型的反射放大式攻擊向量(SSDP和DNS反射放大攻擊)。此外，不同於以往，我們發現2021年的混合式攻擊，除了UDP的反射放大攻擊外，也常有TCP洪水攻擊的攻擊向量摻雜其中，促成單次攻擊的巨量規模。



巨量攻擊

案例分析 (一)

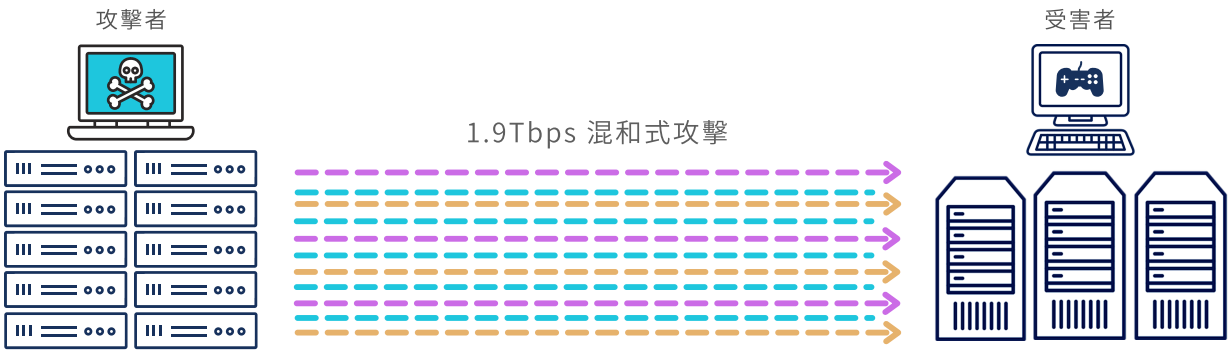
參與本次2021年研究的電信運營商全年檢測到的最大攻擊事件發生於7月12日上午7時59分，

- **攻擊峰值高達1,880Gbps，**
- **攻擊持續僅8分鐘3秒，**
- **攻擊類型為混合式攻擊(Multi-vector attack)，**

主要攻擊方式為SSDP反射放大式攻擊，另搭配DNS反射放大式攻擊、NTP反射放大式攻擊、CLDAP反射放大式攻擊、以及UDP洪水攻擊和TCP洪水攻擊組合而成。由超過10個路由器灌入受害網路，在僅兩分鐘內攻擊流量即暴衝到近1.9Tbps的峰值。在攻擊達峰值時，評估約有超過數百個攻擊IP位址同時個別發送高達數Giga bps的流量至受害主機的UDP或TCP埠號80。

拉長觀察時間，發現同一個受害主機，不僅在7月12日遭受了如此大規模的攻擊，在7月份12日附近兩週間，光針對該主機就發生了有十幾起規模超過 1 Tera bps的巨量DDoS攻擊。且攻擊形態大部份是相同的混合式攻擊組合，或是單純的UDP洪水攻擊(攻擊最烈時，有數源IP同時個別發送數高達數Giga bps的流量至受害主機的UDP或TCP埠號80)，而這些攻擊的持續時間全都在10分鐘內結束。

受害主機為一雲服務中心的伺服器，提供線上遊戲服務，常成為DDoS攻擊的標的，攻擊雖然在2021全年均零星可見，但在6、7間除了遭受的攻擊流量規模都特別巨大外，其被攻擊的頻率也異常的高。



巨量攻擊

案例分析 (二)

UDP一直是最常被用來做為大規模DDoS攻擊的通訊協定，因為一般而言，相較於TCP需要有狀態的(stateful)連線，UDP更容易被攻擊者濫用來經由發送較少的流量，就引起被利用的反射放大伺服器(Amplification Reflection server)，對被鎖定的攻擊目標發送出極大的流量，使得攻擊者只需有較小的頻寬條件，就能更有效率地癱瘓攻擊目標的連線頻寬。這種攻擊者發出的虛假請求 (Spoofed IP Requests)和反射放大伺服器回應封包的流量大小比率，一般被稱之為攻擊放大倍率(Amplification Factor)。以本研究在2021年觀測到的數種常見UDP反射放大攻擊為例，依其被觀測到的年度攻擊量排名，各個攻擊頻寬放大倍率如下表所示。

從下表中可以看到，雖然攻擊放大倍率越大對攻擊者而言，該項攻擊向量會是越有效率的攻擊工具，但實際上我們觀測到的攻擊向量排名卻和攻擊放大倍率的由大到小排名並不相同。這原因在於除了要考慮攻擊放大倍率之外，還要考慮在網路上該攻擊向量的反射放大服務伺服器是不是容易在公開網路上被取得和利用。

此外，雖說相較於UDP ，使用TCP的服務應用因有三方握手(3-way handshaking)機制，較難被做為反射放大攻擊之用，但也並非全然不可行。或許它們的攻擊頻寬放大倍率不如UDP通訊協定的反射放大攻擊來得有效率，引發的攻擊流量規模不如UDP通訊協定的反射放大攻擊規模，然而一直以來我們仍可在網路上觀測到運用TCP通訊協定的反射放大攻擊。值得注意的是，運用TCP的反射放大攻擊在放大每秒封包數 (Packe per seond, pps)上的放大倍率上有不錯的效果，同樣能造成被攻擊目標的服務癱瘓。例如一種新的TCP反射放大攻擊手法就在2021年的USENIX Security研討會中被提出，它主要是利用像防火牆與深度封包分析(DPI)系統等中繼設備(Middlebox)的安全弱點，將反射與放大的 TCP 流量灌注到被攻擊目標上，造成DDoS流量攻擊的效果。雖然這類TCP反射放大攻擊的攻擊放大倍率會依中繼設備的型態甚至廠牌有所不同，但據該研究指出，它一般可造成100x~200x的放大倍率，最高甚或超過50,000x的放大倍率，因此在2022年這類的TCP反射放大攻擊的發展也值得持續關注。

累計攻擊量排名	攻擊向量	攻擊頻寬放大倍率
1	SSDP	~28X
2	NTP	~200X
3	DNS	~100X
4	CLDAP	~50,000X
5	Memcached	~60X
6	SNMP	~600X
7	Chargen	~400X

結語

雖然以攻擊事件頻率來看，本計畫在2021年觀測到的巨量型(Volumetric)DDoS攻擊次數和2020年相較沒有太大的成長(YoY+ 1.3%)，但以總體攻擊事件流量來看，全年有約 21%的YoY成長，可以發現在2021年有單次攻擊流量的規模較過去更為巨大的攻擊模式；此一模式也反應在超大型巨量攻擊的出現頻率上。相較於2020年只觀測到一次超過 1 Tera bps的攻擊，在2021年則觀測單次攻擊規模超過 1 Tera bps的卻有高達12次之多。

觀測2021年的DDoS攻擊活動，以攻擊向量(Attack Vector)類型來看，除了數種反射放大攻擊(e.g., SSDP, NTP, etc.)和其伴隨的UDP埠號0封包片段流量，洪水式攻擊(Flooding attacks)持續是DDoS攻擊的主要類型。以攻擊規模而言，攻擊峰值大小主要在1～10Gbps之間，而大於100Gbps規模的巨量攻擊次數也有12多萬次。以攻擊時長來看，將近半數的攻擊事件持續時間都在不到5分鐘內就結束。進一步觀察每月規模具代表性的巨量DDoS攻擊，發現混合型攻擊(Multi-vector attacks)是超巨量攻擊的主流，通常由數種反射放大攻擊再加上TCP/UDP洪水(Flooding)攻擊所組合而成。

由這份大規模DDoS攻擊觀察報告，除了能瞭解到DDoS攻擊持續不減的威脅頻率外，也能看到攻擊流量規模的快速成長。巨大的DDoS攻擊流量，不僅造成被攻擊目標無法正常運作以提供其原有的服務，也會對受害者的連網運營商網路資源造成具大的耗損，甚至進一步使得同一運營商網路的其他網路服務用戶也受到殃及。而攻擊源分散的巨大攻擊流量規模，也使得傳統in-line部署的邊界式DDoS攻擊防護產品的系統效能遭受嚴峻的挑戰。一個產品效能無法跟上攻擊規模持續成長的in-line安全解決方案，在面對不斷提升的攻擊流量規模時反而可能成為網路安全的漏洞和突破點。

因此，一個能夠全網分散式快速檢測、並完善支援Out-Of-Path (OOP)負載分散攻擊流量清洗功能的解決方案，對現今DDoS安全防禦更顯重要。

威睿科技(Genie Networks)自2000年成立以來，持續站在電信級IP網路流量分析與DDoS防禦的最前線，以採用智能流量分析技術的OOP解決方案協助數百家世界頂尖的電信網路運營商及企業防禦DDoS攻擊。面對處處是資安風險的後疫情時代，做好防禦刻不容緩，威睿科技將與運營商及企業組織並肩作戰，以領先市場的資安防護解決方案，確保客戶免於各種DDoS威脅，維持服務不中斷。

請上www.genie-networks.com了解更多，或聯絡sales@genie-networks.com與我們的專人對談。