2020 DDoS攻擊現狀與趨勢調查

威睿DDoS安全防禦團隊

2020
DDoS攻擊現狀與
趨勢統計報告

前言

隨著網路科技的興起與普及，分散式阻斷服務攻擊(Distributed Denial of Service, DDoS)的規模與次數與日俱增，持續以更創新、複雜的攻擊手法，對企業組織帶來莫大的威脅。企業網路一旦因DDoS攻擊導致服務中斷或停機，除了營運受影響、機密資料外洩等問題外，也可能遭受駭客勒索贖金，讓公司面臨龐大的潛在損失。

混亂的2020年，更由於COVID-19全球性疫情的推波助瀾，順勢帶動了宅經濟、在家辦公、遠距教學等網路活動的迅速發展，但也因此成為網路駭客發動攻擊的絕佳契機，讓DDoS攻擊次數及規模達到前所未有的高峰。防堵DDoS攻擊不再是新話題，卻已經是任何企業組織都不可忽視的資安議題。

身為亞太區網路流量分析與DDoS安全的領導廠商，威睿科技(Genie Networks)持續專注於電信及網路運營商市場。有別於一般企業網路，這些電信等級的網路規模不僅更大，架構也更為複雜，因此需要高於一般市場規格與性能的檢測防禦系統以保障其安全性。威睿科技的DDoS防護解決方案，專門對應這些客戶的資安需求，在過去的20餘年，我們已成功協助全球數百家電信及網路運營商免於DDoS攻擊的威脅。

這份年度調查報告，由威睿科技針對2020年的DDoS攻擊活動進行觀測及統計，調查對象為亞太區數個大型電信及網路運營商(Internet Service Provider)網路，其服務類型包含：網際網路接取服務(Internet connection services) 、資料中心/雲中心/主機代管中心(Data center/co-location services)、以及行動數據服務(Mobile data network infrastructure)。

本調查報告以威睿科技的流量分析及DDoS偵測產品 – GenieATM所收集的數據資料進行分析，由於GenieATM主要針對網路第3、第4層的巨量型(Volumetric)DDoS攻擊檢測，因此本報告也將專注於呈現巨量型DDoS攻擊的相關統計數據。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，也會分享2020年前幾個規模最大的巨量攻擊案例剖析。

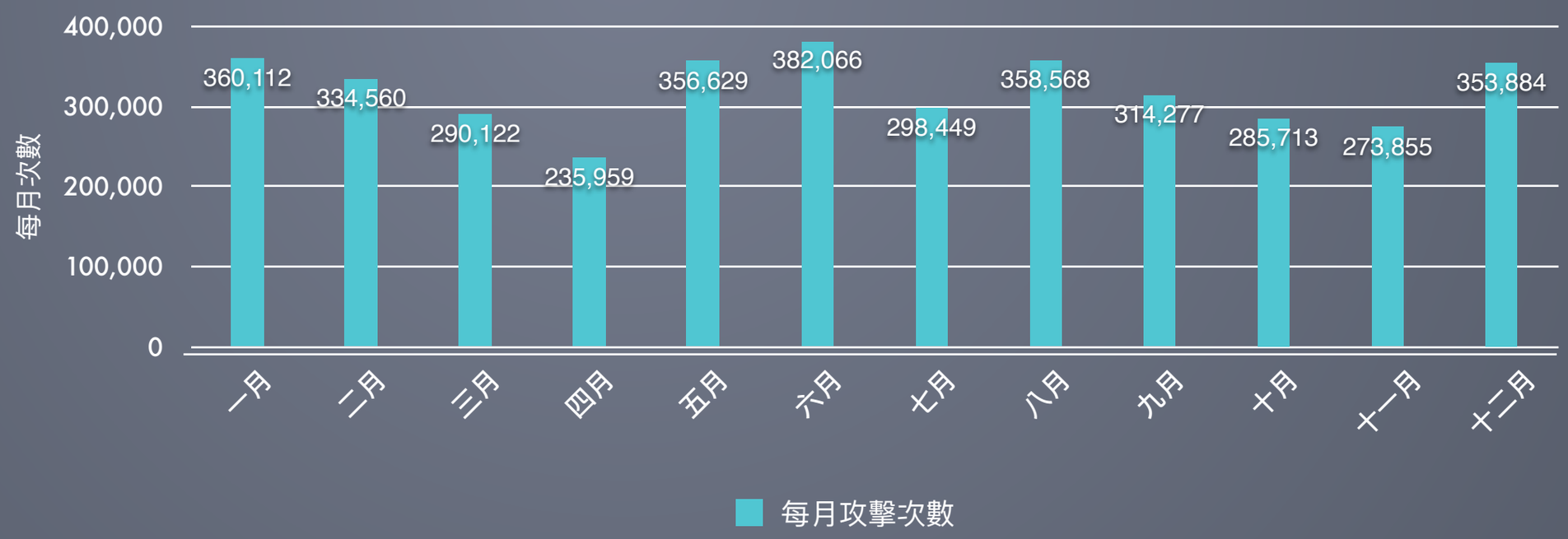
有別於市面上普遍的DDoS攻擊統計報告，其內容多半仰賴對調查對象的主觀式問卷調查，本調查報告採用現網的實際攻擊統計數據進行分析，使其呈現的資訊不受主觀記憶和觀點影響，盡可能提供最真實客觀的統計分析報告。

威睿DDoS安全防禦團隊

攻擊頻率趨勢

觀察2020年檢測到的DDoS攻擊事件頻率，全年總計約370萬次。每個月觀測的攻擊事件，約略在20萬到40萬次之間，以6月份到達最高峰的38萬多次，以4月份的次數最少為23萬多次。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-15%～+40%之間，平均每月約有30萬次的攻擊。相當於：

- ✓ 每日 10,146次；
- ✓ 每小時有 423次；
- ✓ 每分鐘就有 7次攻擊發生。



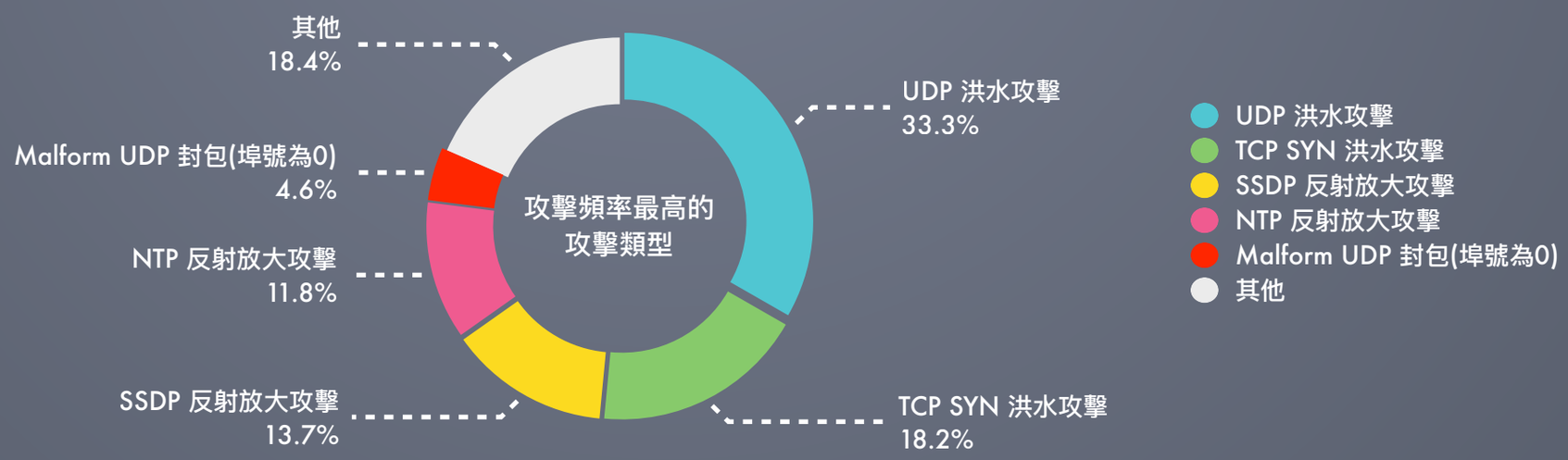
攻擊頻率｜攻擊類型(ATTACK VECTOR)佔比

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)、應用層洪水攻擊等等。

觀察統計2020年的DDoS攻擊事件頻率，前五大常出現的攻擊類型分別為：

- ✓ 1st, UDP洪水攻擊, 佔約總次數的33.3%
- ✓ 2nd, TCP SYN洪水攻擊, 佔約總次數的18.2%
- ✓ 3rd, SSDP反射放大攻擊, 佔約總次數的13.7%
- ✓ 4th, NTP反射放大攻擊, 佔約總次數的11.8%
- ✓ 5th, Malformed UDP封包 (埠號為0), 佔約總次數的4.6%
- ✓ 其他類型攻擊次數合計，約佔總次數的18.4%

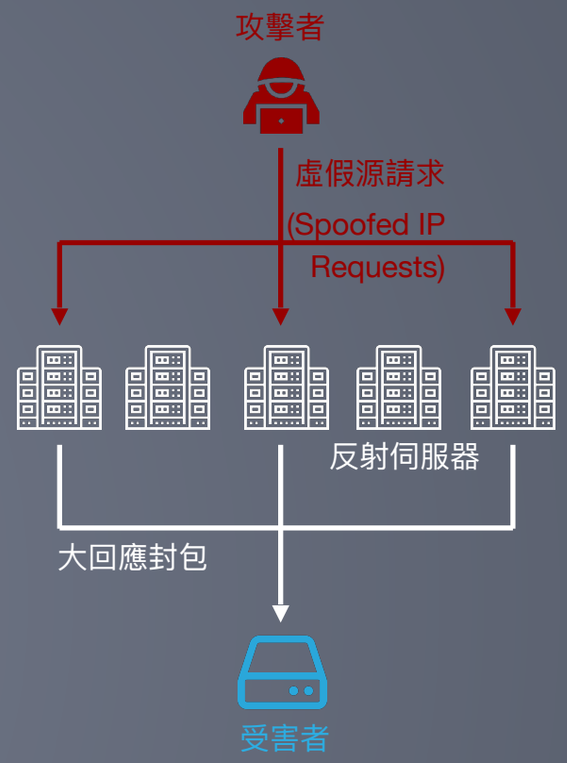
若以大類別歸納，2020年最主要的攻擊型態為反射放大攻擊，其次為UDP及TCP SYN洪水攻擊。

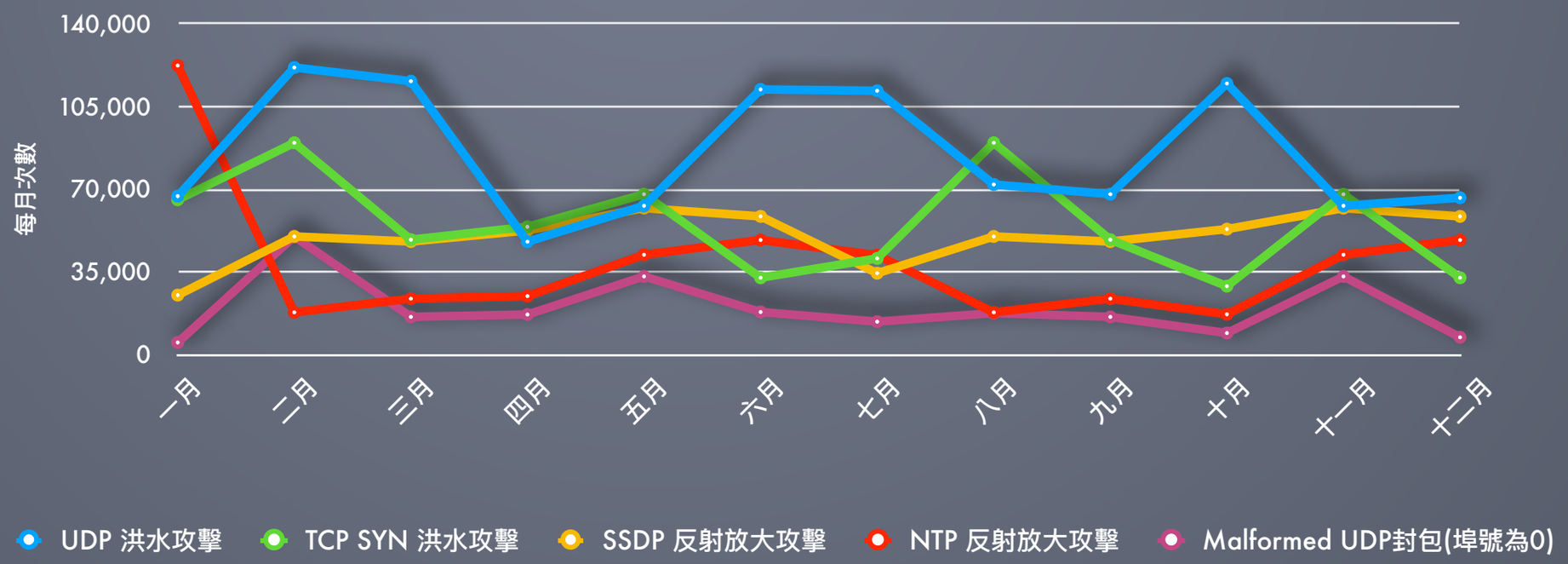


攻擊頻率｜攻擊類型(ATTACK VECTOR)趨勢

2020年的逐月Top5攻擊類型沒有太大變動，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，除了在少數月份有TCP RST洪水攻擊及DNS反射放大攻擊擠進前5名，以及1月時DNS反射放大攻擊擠進第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。因為在反射放大攻擊如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封包攻擊流量常高踞第5名，是反映出主要攻擊型態為反射放大攻擊的現況。



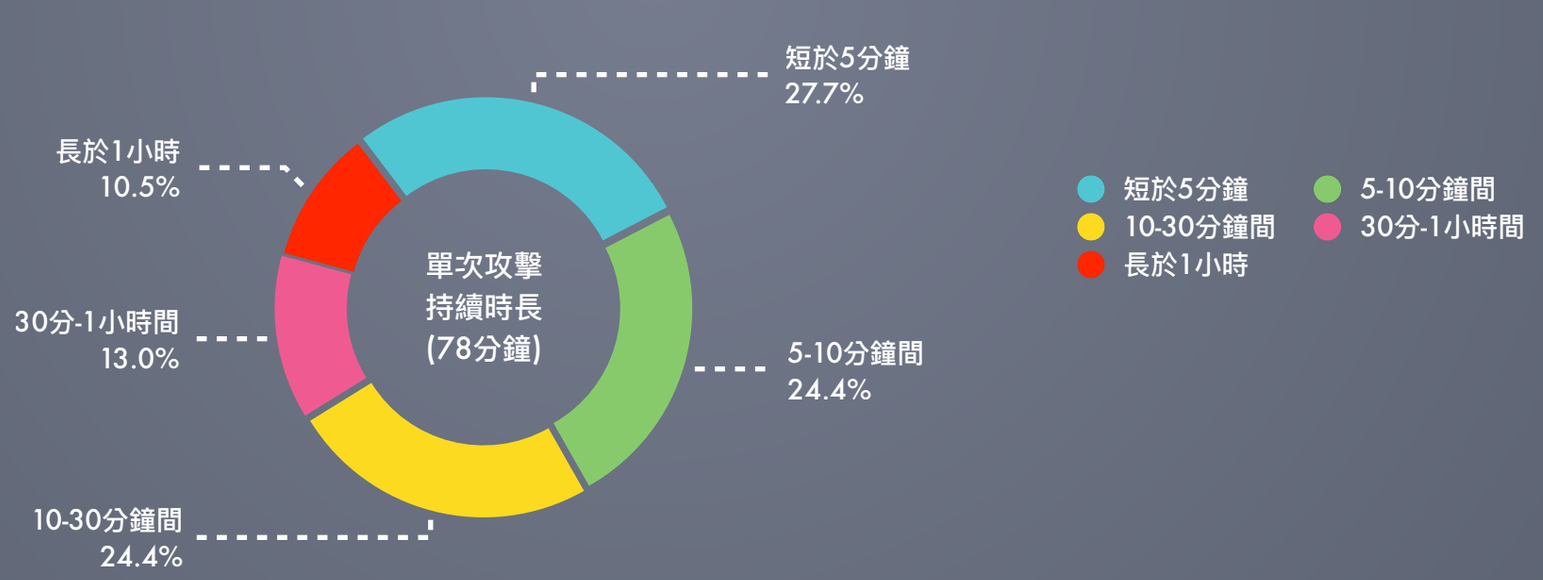


攻擊頻率｜攻擊時長分佈

統計2020年觀測到的DDoS攻擊事件，每次攻擊的持續時間平均約 78分鐘(1.3小時)，而大多數的攻擊常在5分鐘內結束。

我們觀察到將近半數的攻擊事件持續時間都在5到30分鐘之間，約有28%的攻擊事件持續時間則短於5分鐘，而長於1小時的攻擊僅佔全部事件的11%，然而總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，極大比例的攻擊由出現、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。

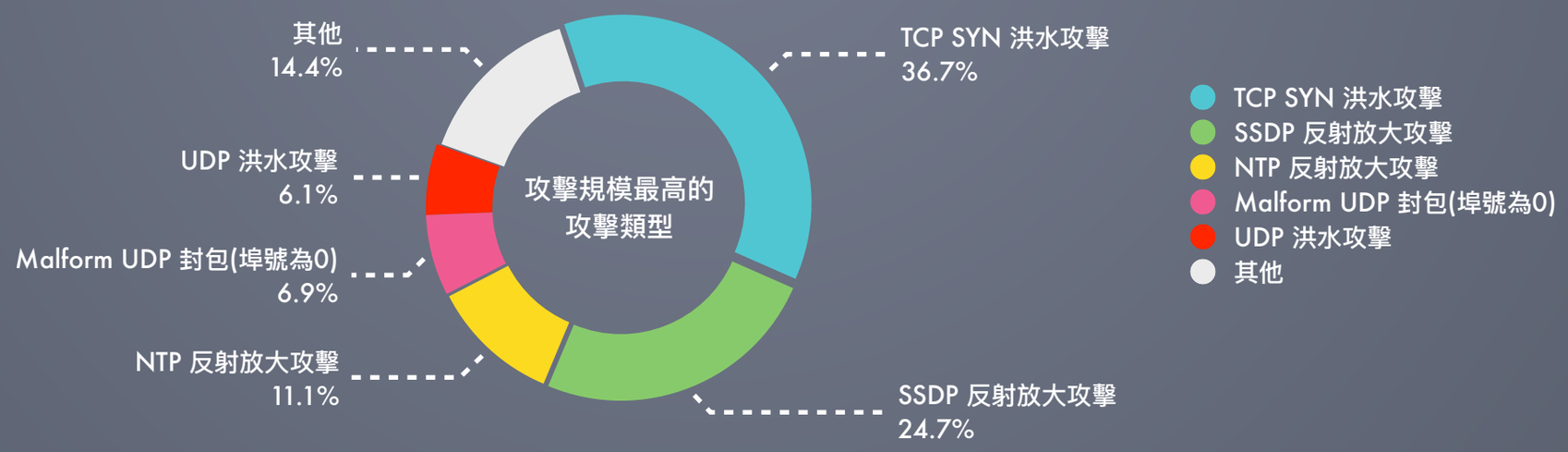


攻擊規模｜攻擊類型(ATTACK VECTOR)分佈

2020年觀測到的DDoS攻擊事件，以攻擊流量的規模計算，前五大攻擊類型分別為：

- ✓ 1st, TCP SYN洪水攻擊, 佔約總攻擊流量的36.7%
- ✓ 2nd, SSDP反射放大攻擊, 佔約總攻擊流量的24.7%
- ✓ 3rd, NTP反射放大攻擊, 佔約總攻擊流量的11.1%
- ✓ 4th, Malformed UDP封包(埠號為0), 佔約總攻擊流量的6.9%
- ✓ 5th, UDP洪水攻擊, 佔約總攻擊流量的6.1%
- ✓ 其他類型攻擊流量總合，約佔總攻擊流量14.4%

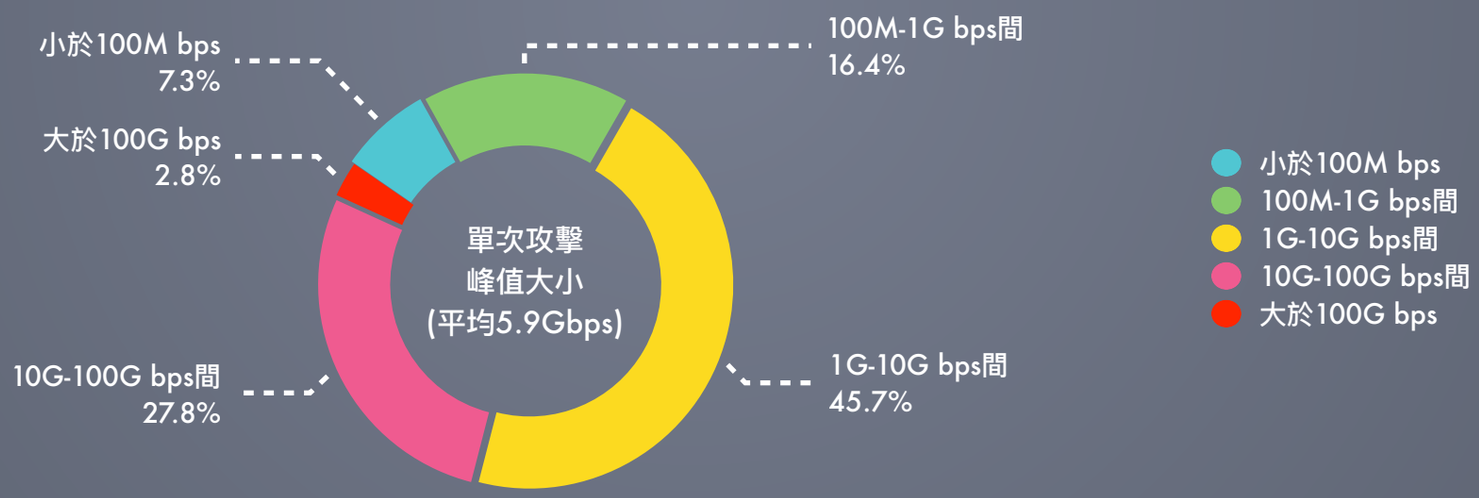
將攻擊流量規模佔比Top 5 和 攻擊頻率佔比Top 5 兩相對照比較，可以發現：UDP洪水攻擊的單次攻擊規模，相較於反射放大攻擊或TCP SYN洪水攻擊等，一般而言單次攻擊規模較小，因而使得前 5 大的攻擊雖然類型不變，但以攻擊流量規模論，排名上UDP洪水攻擊的排名由頻率最高的第一名降到第五名。



攻擊規模｜攻擊大小分佈

統計2020年觀測到的DDoS攻擊事件，單次攻擊的平均峰值大小約5.5G bps，單次攻擊峰值大小最多落在1Gbps到10Gbps間。

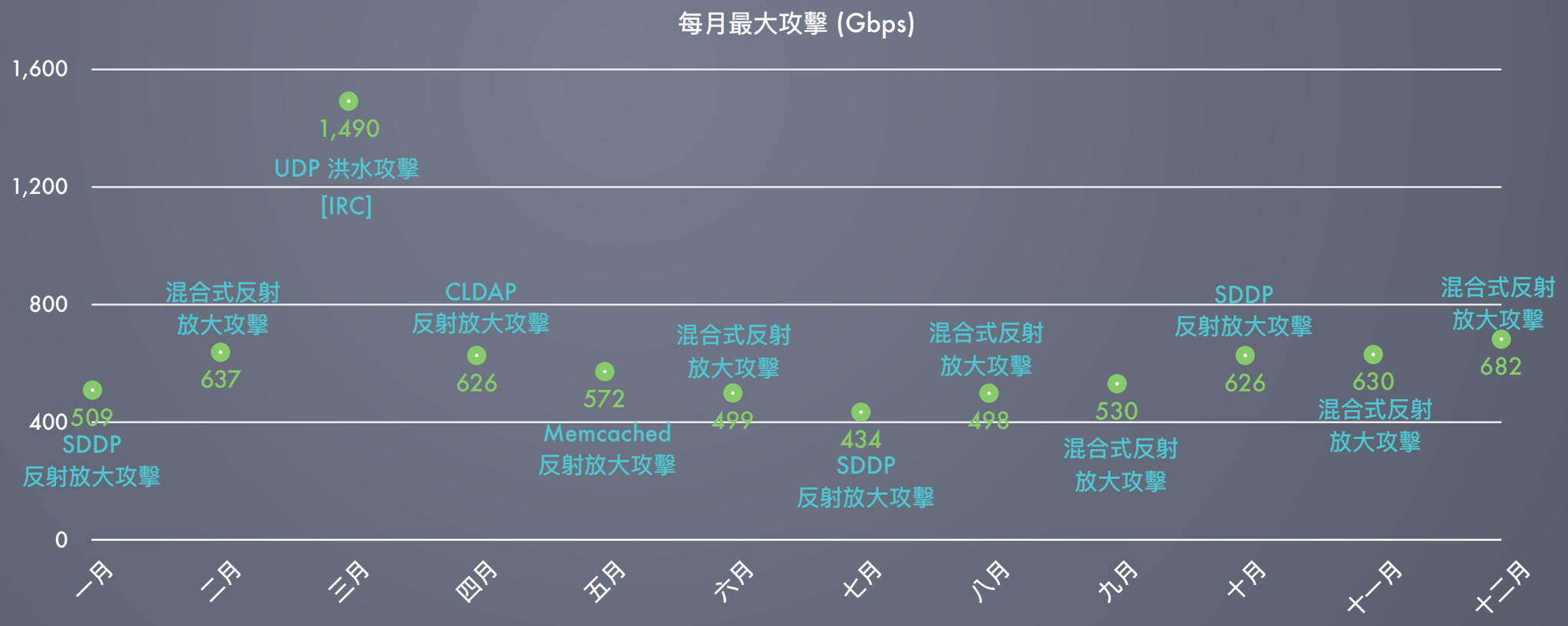
進一步分析不同攻擊類型的單次攻擊規模，發現不同攻擊類型單次攻擊峰值平均規模差異極大。單次攻擊峰值平均規模較大的攻擊類型有反射放大攻擊、TCP SYN 洪水攻擊、Malformed TCP 或UDP封包攻擊等，其單次攻擊平均規模都高達20Gbps以上；而單次攻擊峰值平均規模較小的攻擊類型則有像蠕蟲攻擊及特定協議誤用攻擊等，其單次攻擊一般在數百Mbps的規模。故可以發現因類型的不同，一般大規模的攻擊類型和一般小規模的攻擊，其攻擊平均規模大小可達數百倍。



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，2020全年每月檢測到的最大攻擊，除了三月間發生的最大攻擊事件，其攻擊流量規模高達1.49T bps外，每月最大攻擊的規模一般落於 400G bps至700G bps之間。

此外，觀察發現巨量攻擊類型主要多為反射放大式攻擊、或由反射放大攻擊組合而成的混合式攻擊(Multi-vector attack)。唯獨在三月檢測到的攻擊為一個鎖定特定目的地埠號的UDP洪水攻擊。接下來，我們將進一步剖析數個2020年巨量規模攻擊的流量特性。

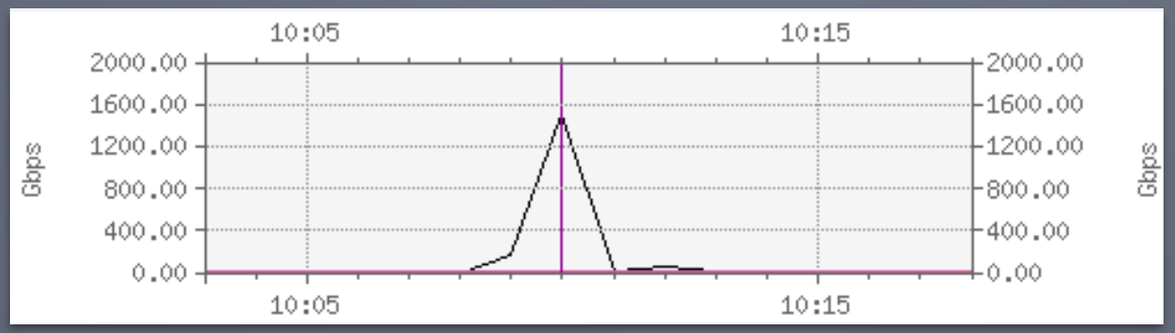


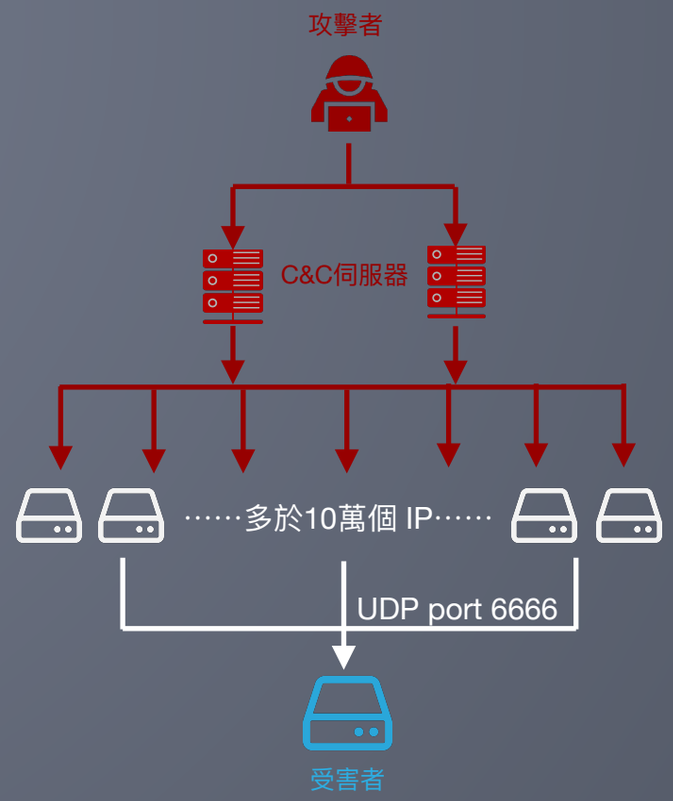
巨量攻擊｜案例分析 1

2020年檢測到的最大攻擊，發生在3月22日上午10時08分，攻擊峰值高達1,490G bps，攻擊持續僅5分鐘26秒。該攻擊是一個來源位址極分散的大規模UDP洪水攻擊，由超過10個路由器灌入受害網路，在兩分鐘內攻擊流量就暴衝到近1.5T bps的峰值。在攻擊達峰值時，評估約有超過10萬個攻擊IP位址同時發送大小約 408 Bytes的封包，到受害主機的UDP埠號6666。受害主機為一雲服務中心的服務伺服器，而這些攻擊流量的源位址都來自於亞太國內。

進一步探討這個攻擊的流量行為：它使用的UDP埠號6666一般被用於Internet Relay Chat (IRC)通訊。IRC協定通常被用於在主從式架構(client-server model)下傳送文本(text)形式的資料，目前已知UDP埠號6666常是Kali Linux木馬工具使用的通訊埠號之一。在這次的巨量攻擊中，單一受害主機受到超過10萬個源IP以高於3.6G pps的速度發送流量封包，是一次規模極為可觀的殭屍網路(Botnet)攻擊。

所謂的殭屍網路是由許多受到惡意程式感染的連網設備所組成，駭客常利用這些因感染而可以遠端控制的裝置來發動大規模攻擊，而殭屍網路的威力主要由受感染設備的數量規模來決定。過往要實現一個DDoS攻擊並不容易，但隨著物聯網(IoT)的問世，促使聯網的裝置數量大幅度增長，再加上物聯網設備普遍資安標準較為鬆散的特性，正好讓殭屍網路駭客找到了征服大量設備的新寶地。以3月發生的這個巨量攻擊為例，同一時間能發動數萬個源IP進行攻擊，創下每秒Tb級的攻擊流量，正符合IoT殭屍網路的攻擊場景。



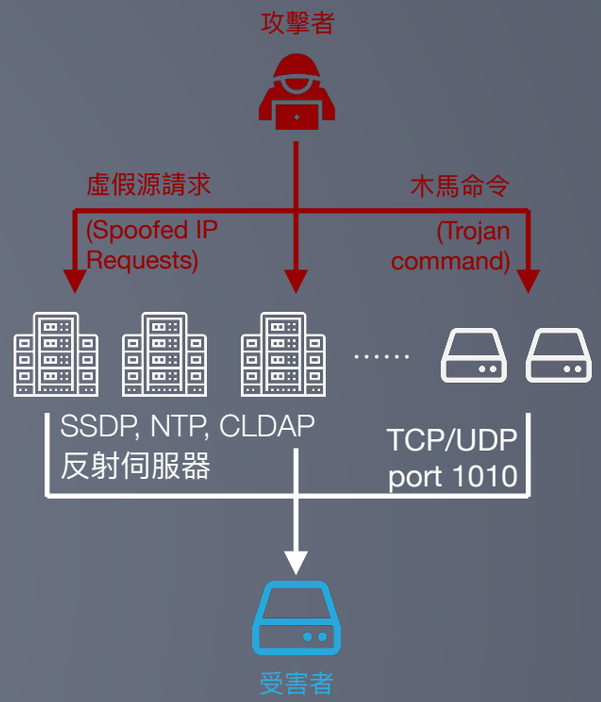


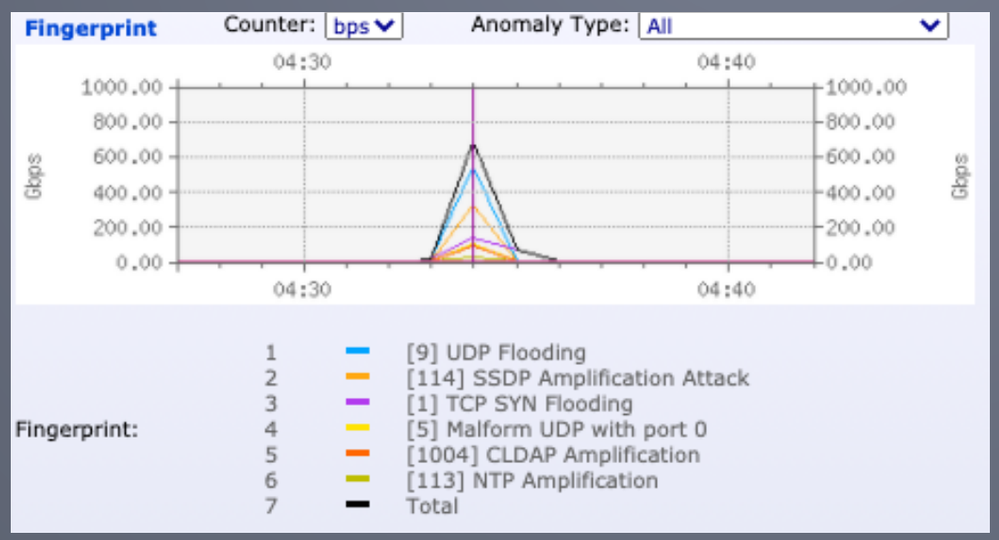
巨量攻擊｜案例分析 2

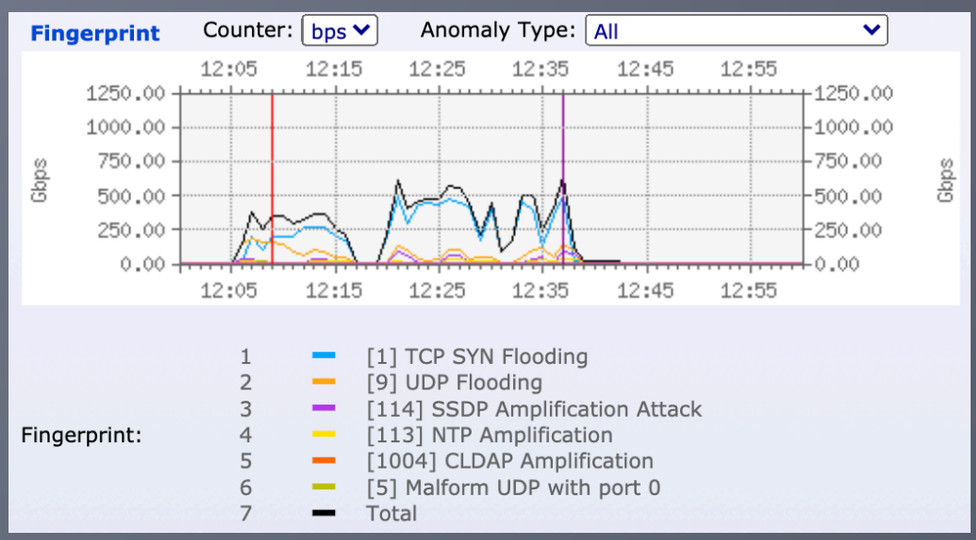
除了一次高達將近1.5Tbps的巨量攻擊外，2020年次大及第三大攻擊均為大規模的混合型攻擊，分別發生在年末的12月3日凌晨4時和年初的2月12日上午10時，攻擊峰值各高達682G bps及637G bps。在攻擊時長上，則一短一長，一個僅持續約5分鐘，而另一巨量攻擊則持續了約42分鐘之久。

這兩個巨量攻擊型態，都屬於大規模的混合型攻擊攻擊。攻擊結合了數種常見的反射放大攻擊，包含有SSDP反射放大攻擊、NTP反射放大攻擊、CLDAP反射放大攻擊和反射放大攻擊伴隨的Malformed UDP封包流量等等。除了反射放大攻擊，這個混合攻擊還包含了相當的TCP SYN洪水攻擊流量，瞄準如目的地端口80， 甚或以數個高埠號源端口流量瞄準特定的TCP/UDP1010目的地端口的Doly木馬程式攻擊。

這樣的巨量攻擊在攻擊流量最猛烈時，有超過數百個的攻擊IP位址同時以不同的通訊協定(TCP, SSDP, NTP, CLDAP等)，經由數十個路由器鏈路將攻擊流量，灌入受害網路。而這兩個巨量攻擊則分別的源自於國內它家電信業者的網路，以及來自於亞太國內外。



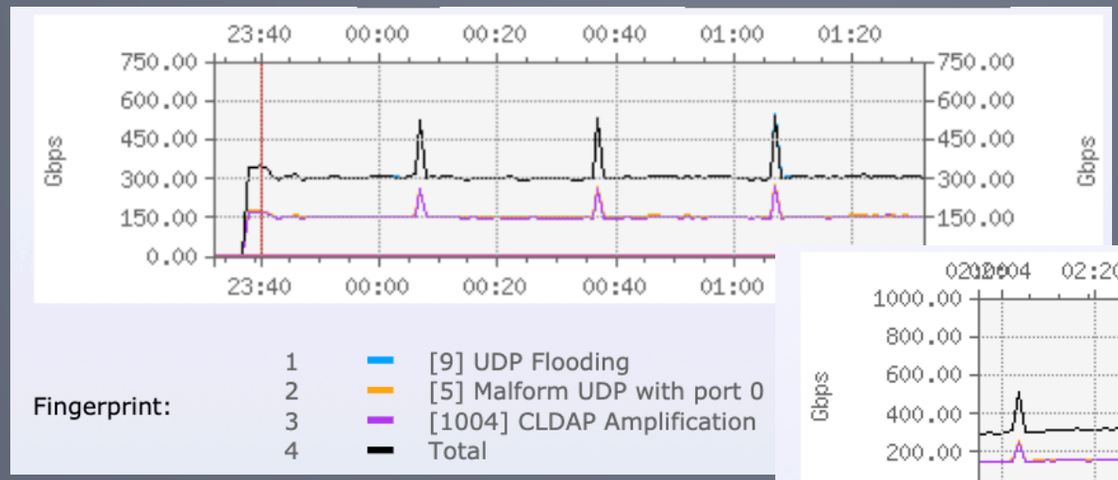


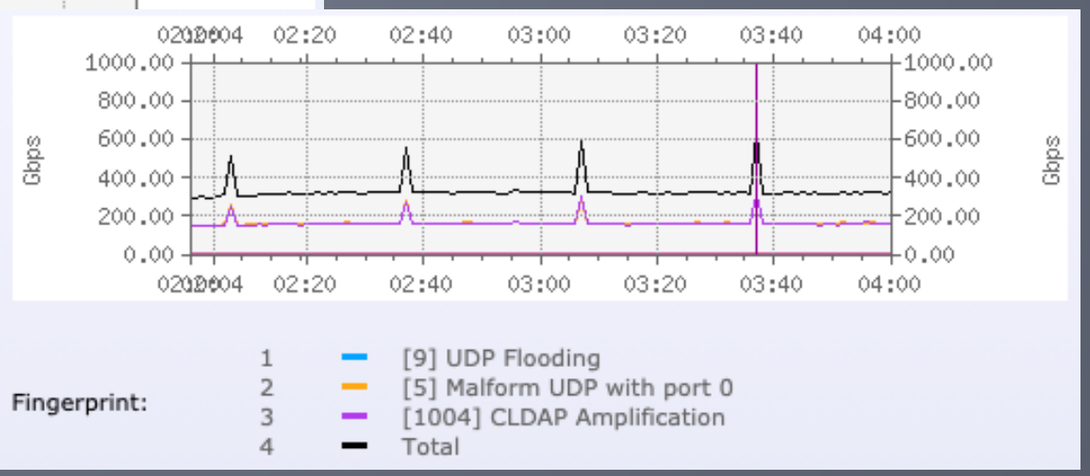


巨量攻擊｜案例分析 3

2020年檢測到的第四大攻擊，發生在今年4月18日晚間23時37分，攻擊峰值達626G bps。該攻擊是一個大規模的CLDAP反射放大攻擊，伴隨著大量的Malformed UDP封包流量。這次攻擊在異常流量出現半小時後流量達到短暫的峰值，在攻擊達峰值時，評估約有超過上千個反射攻擊伺服同時以CLDAP通訊協定攻擊受害主機。

這個巨量攻擊和前述幾個巨量攻擊相比，另有三大特別之處：首先，它攻擊源的反射攻擊伺服器主要多來自於國外運營商，如Microsoft、Amazon、瑞典、南非等等；第二，它的攻擊時長持續了3天又11小時多後，流量才回歸一般正常水準；第三，這個反射放大攻擊流量並非持續地處於流量高原，而是一種規律出現流量突刺的脈衝波型攻擊(Pulse Wave attack)。在這次巨量攻擊中，我們可觀察到固定每隔半小時就會出現流量突刺，流量的突刺峰值高達600多Gbps。這樣的流量突刺模式持續了約三天，突刺流量值逐漸衰減，最終歸於無突刺的流量高原，並於三天後流量值恢復正常。





結語

觀察2020年的DDoS攻擊活動，以攻擊事件頻率而言，巨量型DDoS攻擊在2020年共有多達370萬次，平均每月多達30萬次，其中最大的攻擊規模高達1.5Tbps，最長的攻擊甚至持續了三日之久。以單一攻擊類型的頻率來看，UDP洪水攻擊高居榜首，佔總頻率的3成之多，以大類別的攻擊頻率計算，最常出現的類型為反射放大攻擊，若以攻擊規模而言，則是TCP SYN洪水攻擊佔最多數。統計2020整年度發生的DDoS攻擊事件，平均攻擊峰值的大小大多落在1～10Gbps之間，而大於100Gbps規模的巨量攻擊次數也有高達10萬多次。 以攻擊時長來看，將近半數的攻擊事件持續時間均落在5到30分鐘之間，多數攻擊甚至持續不到5分鐘，而長於1小時的攻擊僅佔10.5%。

進一步觀察每月規模具代表性的巨量DDoS攻擊，發現混合型攻擊為巨量攻擊的主流，通常由數種反射放大攻擊甚或TCP/UDP洪水攻擊所組合而成。我們也在報告中分享了2020年的前幾大巨量攻擊案例，其攻擊類型包含：由物聯網裝置驅動的殭屍網路攻擊；結合反射放大攻擊與洪水攻擊的混合型攻擊；以及規律、持續性的脈衝波攻擊。

由這份觀察報告不難發現，DDoS攻擊手法越變越多元複雜，攻擊力度越來越猛烈的趨勢，這都會使傳統防禦解決方案遭受到嚴峻的挑戰。一個有效對應的解決方案，必須在防禦技術上與時俱進，提供趨近即時的回應速度、異常流量行為聚合、以及完善的檢測判定機制。

展望未來，疫情終究會結束，但物聯網等高速網路應用的發展已成為全球大勢，我們認為，DDoS攻擊將持續是各大電信網路運營商的重大資安威脅。期待這份DDoS現況與趨勢觀察報告，除了能讓電信網路運營商進一步了解網路攻擊的整體趨勢與攻擊屬性，做為制定網路安全政策及防禦工作部署的參考外，也期許對複雜攻擊流量行為的深入探察，也能做為評估、乃至於開發DDoS防禦解決方案時的一項重要依據，做為機器學習、AI智能化檢測等新型防禦技術研究應用的背景資訊。身為電信網路運營商最信賴的DDoS安全伙伴，威睿科技將持續以更貼近市場的產品線及分析研究報告，提供更完善的資安解決方案與專業洞見。

歡迎對本報告內容提出您寶貴的批評指教，請將您的反饋意見郵寄至：sales@genie-network.com