**Flowviewer產品特色與優點**

原理

Flowviewer採用具備auto-bypass功能之網路卡與優化後的系統。系統搭載由本公司獨立開發的異常偵測系統，包含能快速辨別異常流量（駭客入侵與攻擊）的特殊演算法與能快速收集網卡上封包的驅動程式，透過多線程/執行序（multi-thread）的方式可迅速收集封包；利用多核心處理的概念來提升整體處理效率，可在本機端或是透過ACL (Access Control List) 在核心路由交換器(目前支援的廠牌有Alcatel、Cisco、Foundry、Extreme)，阻斷惡意流量。由於軟、硬體搭配得宜，Flowviewer並不會像市面上IPS(Intrusion Prevention System)設備，在面對頻寬消耗型或是資源消耗型的攻擊便發生硬體故障的問題。

**Port 1**

**Port 2**

**I/O RX**

**CPUs**

**Packet processing**

**CPU core 1**

**Packet processing**

**CPU core 2**

**NIC RX Buffer**

**Ring Buffer**

**NIC**

**CPUs**

**RSS**

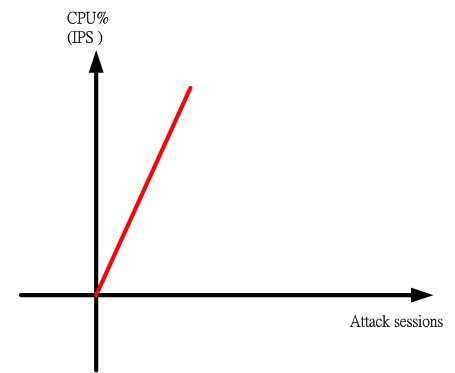
**CPUs**

圖一 利用多核心及多執行序方式提升處理封包效率

Flowviewer設備與IPS(Intrusion Prevention System)設備之技術的比較

IPS設備之技術採用深層檢測（deep packet inspection），此技術必須要過濾經過此設備上多數封包才能準確比對特徵碼（Signature）提高防止駭客入侵的準確率，此技術的架構一定是採用有session原理。此設備另一項功能防禦值（Threshold）是計算經過設備上每秒有多少封包及sessions數，防禦值（Threshold）由使用單位自行設定，此技術相同是採用有session原理。

採用有session原理的缺點，當使用單位遇到駭客DDoS攻擊時產生巨大sessions數經過IPS設備會導致此設備CPU使用率滿載讓設備當機，雖然IPS設備廠商宣稱是採用ASIC晶片技術，但是ASIC晶片也是屬於CPU的種類。不相信此說法的人可以拿任何一種廠牌的IPS設備來實驗，以軟體模擬DDoS攻擊製造大量Flow（Session）攻擊IPS設備，觀察設備的CPU使用率跟Flow（Session）攻擊數的比率情況，也就是X軸是Flow(Session)攻擊數，Y軸是設備的CPU使用率，並繪出座標圖。如果數據做的越多，應該是趨近直線，成線性關係也就是正比，再從二度空間推到三度空間，當Z軸是時間，在何時IPS設備會當機？



圖二 攻擊session數與IPS CPU使用率比例示意圖

Flowviewer設備是採用non session原理，為何可以達到non session架構？設備是接收取樣率1:1的Netflow（或sFlow）資料所以可以達到non session架構，藉由分析來源位址、目的位址、通訊協定、通訊埠號、封包數、傳輸量大小等資料來找出異常流量。如同大數據採用的全樣本原理，我們相信唯有利用大量的流量數據資料，並針對個別IP去進行分析，方得精準找出其行為規律性。在IEEE的論文期刊中也都可以看到有人發表與這項技術原理相關的文章。因此，我們誠摯建議客戶將1:1的Netflow資料轉送至Flowviewer進行分析，透過全部數據樣本的解析，便可精確判斷出哪些是屬於異常流量。雖然透過分析全部數據資料來作辨識是最完善的解決方案，然而在實務上，設備能不能接受海量的數據卻成了另一個問題，這就是此技術無法產品化真正原因，Flowviewer設備採用自行開發的數學演算法與判別式，還有就是透過分析完整的流量資料，才能突破此技術的瓶頸。以我們的實際經驗來說，某A廠牌字母開頭的設備僅能接受取樣率1:1000的Netflow。換句話說，就是從一百萬個封包中只取樣一千個出來做樣本分析，這樣的話又怎麼能精準判別出來呢？這表示有設備廠商是認同此技術，只是無法克服此技術的瓶頸。

Flowviewer設備上有一項功能可以阻斷Domain Name，使用單位只要將想封鎖的Domain Name輸入設備上即可，此功能的技術的確要分析經過設備上的封包，但是此技術只要分析1個封包就可以判斷出Domain Name，不需要使用深層檢測（deep packet inspection）技術，所以可以達到non session的技術。

IPS這類採用session的設備在阻斷時，同樣是要使用深層檢測的技術去分析流經設備的封包，因此在面對大量封包時，必定會大量消耗CPU等硬體資源，進而導致設備當機；而Flowviewer採用non session技術，因此不必擔心大量異常流量消耗硬體資源的問題，當然也不會因此而引發當機的問題。

實際案件說明

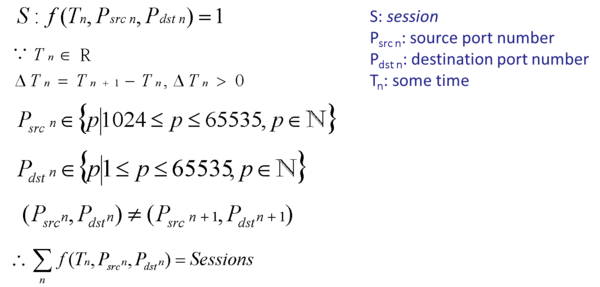
台灣新北市某知名私立大學因為某些原因被駭客以DDoS攻擊導致全校網路癱瘓，台灣電視新聞及網路新聞都有報導，駭客還透過網路發佈在哪一天要發動第二次攻擊，剛好此學校有購買Flowviewer設備所以網路管理者跟我們抱怨為什麼購買Flowviewer設備，還會造成網路癱瘓？我們來分析原因，此學校的網路設備架構是Router放置在最出口端，接著對內設備有IPS設備、Flowviewer設備、Core Switch設備，在學校網路癱瘓的時間Core Switch設備並沒有當機而且Netflow資料還有傳送到Flowviewer設備上，在從Flowviewer設備上有看到IP資料只是資料內容只有內對內的IP資料，並沒有內對外及外對內的IP資料，這表示Flowviewer設備也沒有當機，等於說明Router跟IPS設備有一台設備當機而導致全校網路對外癱瘓，Flowviewer設備是每5分鐘收集一次Netflow資料後，在下1秒內以數學演算法快速分析判斷出攻擊的IP並且直接在設備上阻斷攻擊的IP，而IPS設備竟然不到5分1秒內就當機導致全校對外網路癱瘓，我們不相信Router會在5分1秒內就當機，經過我們分析給網路管理者了解，而且駭客還會發動第二次攻擊，建議網路管理者將IPS設備卸下讓Flowviewer設備來判斷駭客攻擊並自動阻斷來攻擊的IP，結果駭客還是有發動第二次攻擊而Flowviewer設備也順利阻斷來攻擊的IP，否則駭客又要在網路發佈另一次的攻擊。網路管理者將IPS設備卸下就沒有將IPS設備再上線。所以你們可以模擬駭客使用大量sessions攻擊IPS設備，跟上述座標圖是否相同？

IPS (Intrusion Prevention System) / IDS (Intrusion Detection System) 設備是採用特徵碼（signature）方式去進行比對、過濾的。除了需要定期更新特徵碼外，在面對未知型的攻擊與入侵/零時差攻擊時，這樣的設備也難以在第一時間防護網路安全。駭客使用機器人程式在雲端網路對使用單位網路進行入侵每兩、三天就會變更使用的特徵碼，**事實上實際的說法是駭客使用入侵程式，而此入侵程式就是在對使用單位的網路進行猜測密碼的動作，如果成功就可植入木馬程式成為駭客的殭屍網路(botnet)，駭客也會針對特定埠號（Port number）來進行猜測密碼的動作，因為某些特定埠號比較容易進行內對內入侵**，再擴大殭屍網路(botnet)，而IPS設備就是收集這些機器人程式的特徵碼來過濾，防止駭客的入侵程式到使用單位的網路來猜測密碼的動作，駭客也會從內對內入侵來竊取軍事/商業機密資料。例：facebook被竊取使用者資料，美國的資訊安全專家完全沒有分析到駭客是如何使用內對內入侵方式，都只探討駭客是如何找到軟體漏洞，最後結論是facebook員工下載app software讓駭客成功入侵到facebook內部網路然後成功竊取使用者資料，facebook員工的電腦有facebook使用者的資料嗎？當然沒有，駭客一定是使用最新木馬程式進行內對內入侵並成功躲避保護server farm的IPS設備，駭客使用的木馬程式是最新程式在IPS設備的資料庫當然沒有，所以很容易躲避偵測並成功竊取使用者資料。如果我所敘述的觀念不是事實，那麼為什麼美國在2017年又會發生Equifax公司的使用者資料被竊取的事件？我猜想2015年Hello Kitty網站被駭，造成330萬用戶資料被竊，駭客也是使用此種方式。如果你是駭客知道這種方式可以成功竊取資料一定會使用此方式，而且駭客寫最新的木馬程式並不難；至於軍事/商業間諜也一定會採用新型的特徵碼去進行入侵行為，因此採用特徵碼的設備對於這類未知特徵的攻擊與入侵是束手無策的。利用特徵碼的方式去比對、過濾並非是完全不好的，但是在面對資源消耗型的攻擊時，系統效能會因為異常大量的封包而耗費甚鉅，進而引發當機的問題，上述已經有用數學座標圖概念來說明當機現象。部分IPS / IDS設備採用門檻值（threshold）去辨別駭客攻擊，由於門檻值設定太低會造成嚴重誤判、造成管理者的額外負擔。因此管理者並不會將門檻值設定太低，作為代價的結果便是讓駭客有機可乘。

另一方面，絕大多數的IPS / IDS設備都聚焦於「內部網路對外部網路」與「外部網路對內部網路」的入侵與攻擊，對於「內部網路對內部網路」的入侵與攻擊是不太著重的。金融與軍事單位常為了防範外部網路入侵與攻擊，都會採用封閉的網路環境。但也因為採用封閉網路的關係，造成管理者往往忽視了內部入侵的嚴重性與威脅性。當Flowviewer的分析資料來源是採用Netflow時，其資料包含內部對傳的流量，因此Flowviewer可利用獨有的inner intrusion功能去分析出內部入侵(insider intrusion)。

Flowviewer設備判斷駭客入侵及攻擊之IP規律性分析

我們也創造出相關的數學方程式來做為判斷駭客入侵及攻擊的規律性機制，再加上實際單位的使用經驗。因為使用單位會告知設備是否有誤判情況。如果有誤判發生，我們會修正判斷式，直到使用單位說沒有誤判情況發生為止。



圖三 利用數學公式作判別準則

關於上述方程式，我們的Youtube頻道有簡單的解說

<https://www.youtube.com/watch?v=yX_wp2oedYM>

裡面也有關於「Simulate hacker attack\_ Top 6 ways of hack attacks and how to protect」的影片：<https://www.youtube.com/watch?v=vKweWU82okI>

實際案例

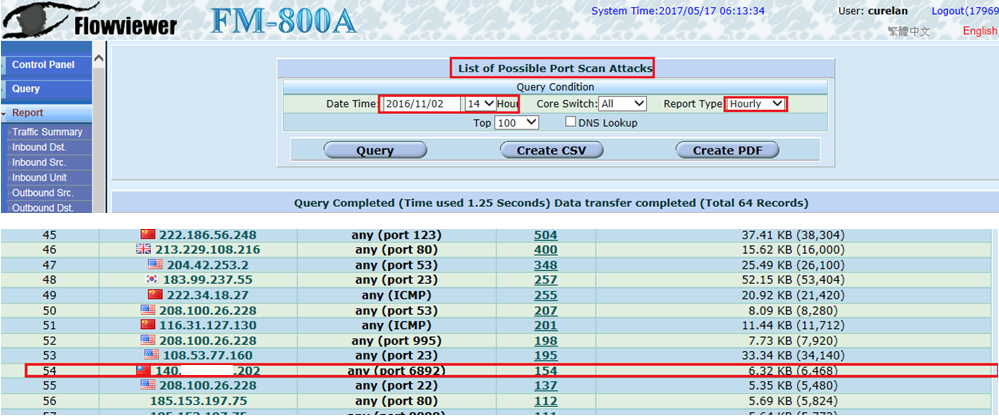
案例一：WannaCry勒索病毒

2017年5月該病毒於全球大規模傳播，利用微軟SMB協定中的數個漏洞進行主動傳播。透過利用漏洞，病毒可以獲得作業系統的特權，並隨機透過445或是139埠自我傳播，嘗試感染區域網路中其他設備。當時建議的應對防禦方式除了更新微軟釋出的更新檔外，就是建議透過防火牆關閉445埠。然而關閉445埠這個手段卻可能影響其他正常Windows共用完全停止工作，並且可能會影響其它應用程式的執行。我們觀察幾個部屬Flowviewer的單位後，發現在5月時透過445埠的入侵/攻擊行為有明顯的增加。這可以證明Flowviewer能確實抵禦該病毒主動傳播的行為。

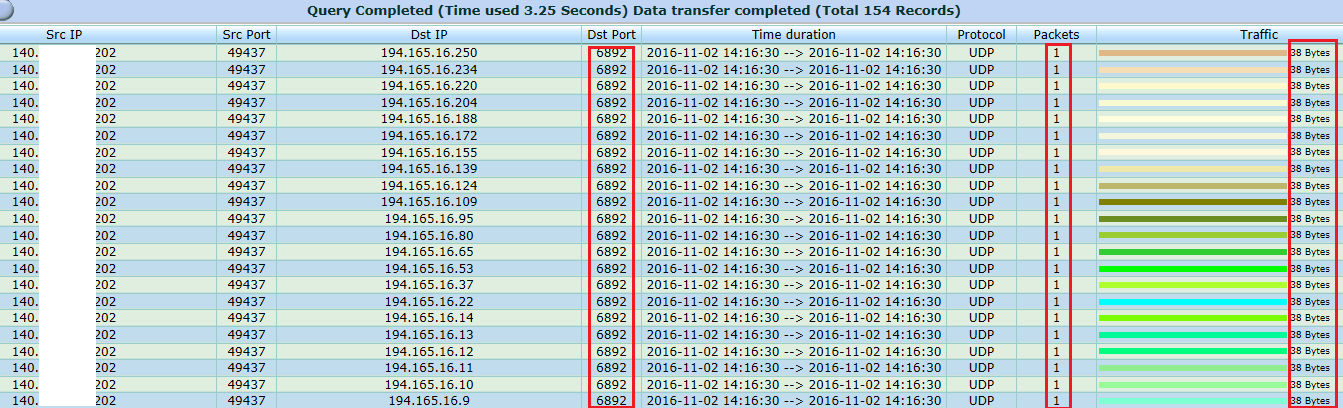
|  |  |  |  |
| --- | --- | --- | --- |
| **A 校** | | **B 校** | |
| **日期** | **攻擊數量 / 每日** | **日期** | **攻擊數量 / 每日** |
| 2017/5/1 | 6 | 2017/5/1 | 69 |
| 2017/5/2 | 14 | 2017/5/2 | 75 |
| 2017/5/3 | 19 | 2017/5/3 | 82 |
| 2017/5/4 | 24 | 2017/5/4 | 80 |
| 2017/5/5 | 29 | 2017/5/5 | 84 |
| 2017/5/6 | 25 | 2017/5/6 | 118 |
| 2017/5/7 | 20 | 2017/5/7 | 60 |
| 2017/5/8 | 15 | 2017/5/8 | 85 |
| 2017/5/9 | 18 | 2017/5/9 | 61 |
| 2017/5/10 | 18 | 2017/5/10 | 83 |
| 2017/5/11 | 18 | 2017/5/11 | 75 |
| 2017/5/12 | **309** | 2017/5/12 | **328** |
| 2017/5/13 | 286 | 2017/5/13 | 278 |
| 2017/5/14 | 94 | 2017/5/14 | 140 |
| 5月12日前每日平均攻擊數：19個  5月12日當日攻擊數：309個 | | 5月12日前每日平均攻擊數：80個  5月12日當日攻擊數：328個 | |

表一 A、B兩單位於五月1-14日透過 445埠進行入侵的IP數量統計

就算關閉445埠，WannaCry這類的勒索軟體還是會從其他埠入侵。例：台灣嘉義縣某私立大學在2016年11月2日就發現有內部主機受到感染，通過6892埠對外進行大規模掃描的動作。圖四、五分別顯示Flowiewer當時偵測到的結果。由此案例可知，針對特定埠號去進行阻擋、防禦無法有效防止入侵與攻擊行為。

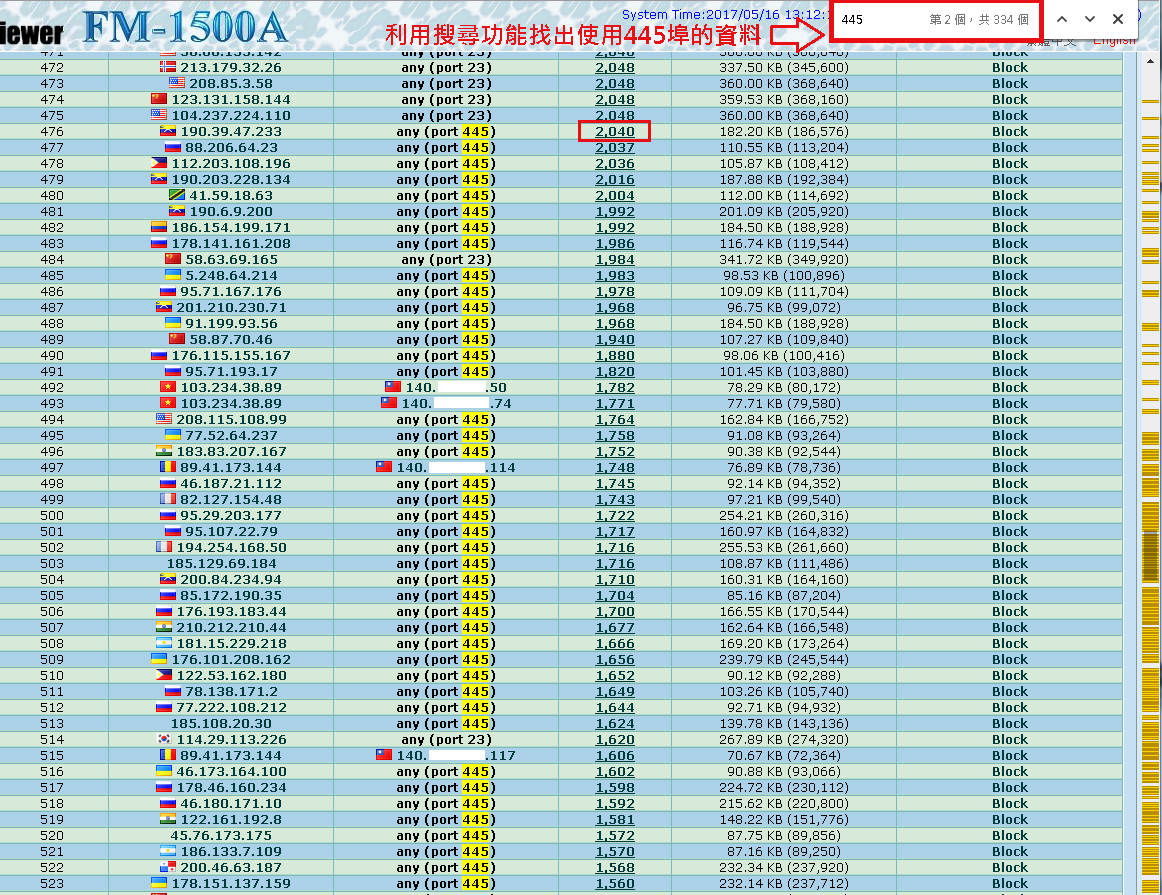


圖四 11月2日當日的portscan報表

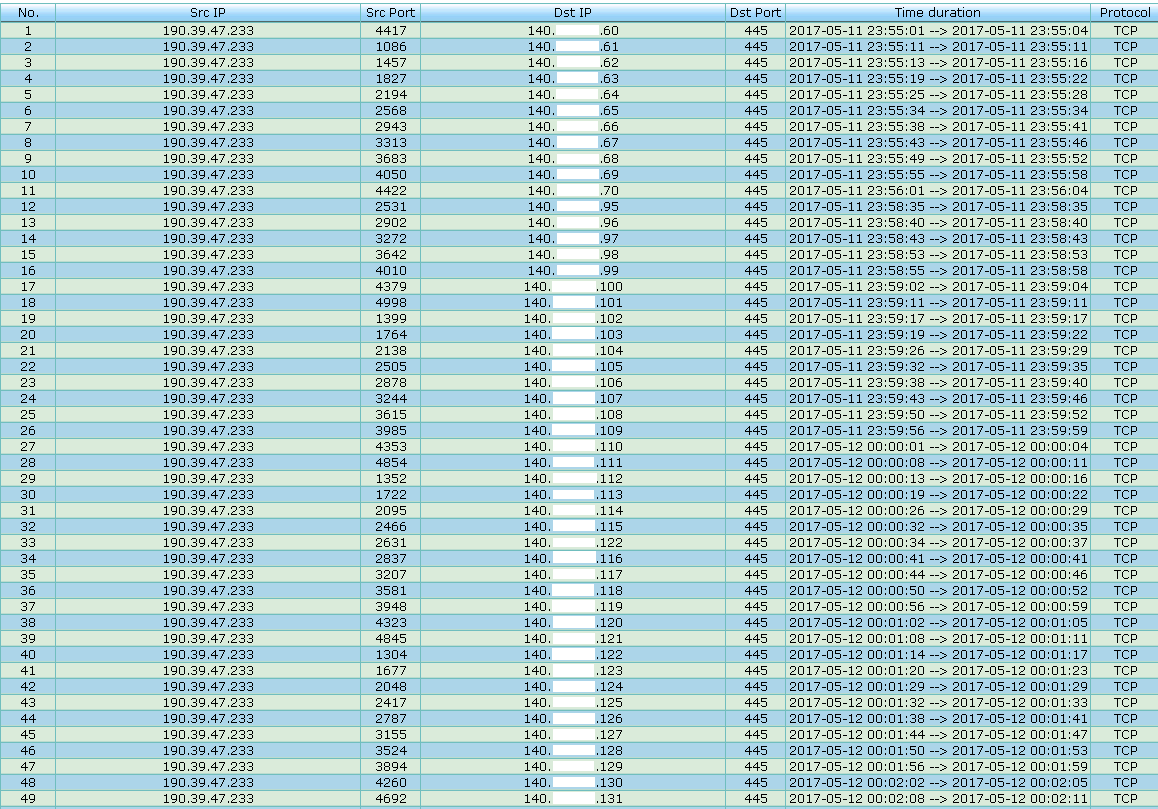


圖五 針對受到感染設備發出入侵封包 zoom in觀察結果

除了能夠自動偵測與阻斷入侵與攻擊，Flowviewer也能夠提供相關報表。圖六、七分別為B校在5月12日當天的portscan報表與針對特定IP(190.39.47.233) zoom in的結果。



圖六 5月12日當日的portscan報表



圖七 針對特定IP(190.39.47.233) zoom in觀察結果

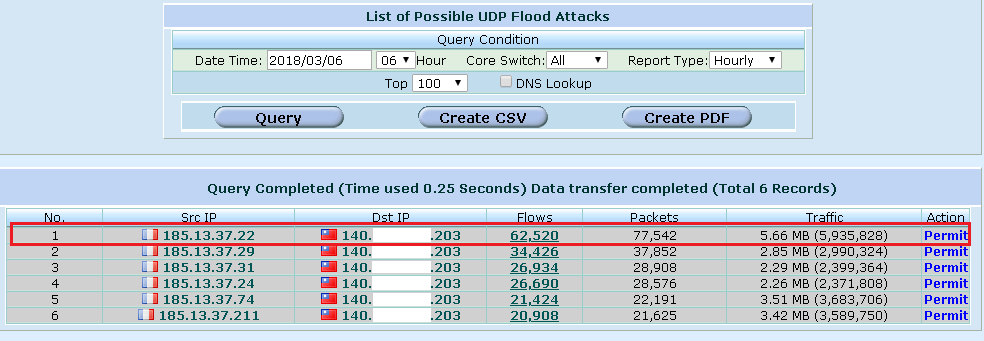
案例二：記憶體快取 DDoS放大攻擊

2018年2月時，某安全機構發現有透過UDP協定之11211埠產生記憶體快取DDoS放大攻擊（Memcached amplification attack），據指出其放大倍數高達50000倍以上，受害者包含開源碼（open-source）社群GitHub等多處，而當時湧入GitHub的流量最大值高達1.35 Tbps，這也是自從2016之後看到最大的攻擊。在面對此種類型的攻擊，使用流量清洗之類防禦手段並無法阻止實體物理頻寬擁塞的問題，因此必須在網路架構的上一層（上游ISP或是區網中心）設備進行阻斷，方得有效控制。這個論點我們在2017年9月已於國外資訊安全雜誌：SECURITY發表過相關廣告說明。這樣的處理方式是相當正確的，但如果能在持續放大攻擊前阻斷那就更好了。如下圖所示，角色A為發起攻擊的攻擊方，角色B為放大攻擊的角色，角色C為受害者。那麼有可能找到一個解決方案在A、B之間阻擋這樣惡意的流量嗎？答案是肯定的，在我們觀察部屬在某單位的Flowviewer之後，發現我們的演算法依舊適用於偵測尚未被放大的異常流量。透過Flowviewer的報表，也可以得知在五分鐘之內，其流量並不會迅速成長到50000倍以上。

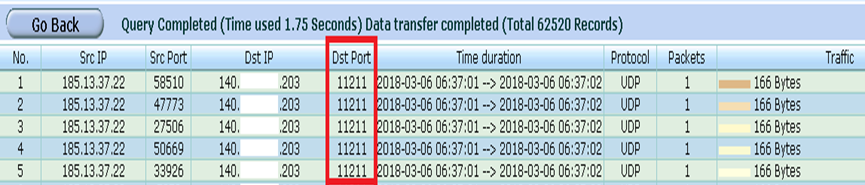


圖八 記憶體快取 DDoS放大攻擊簡單示意圖

如圖九所示，從報表上可以看到Flowviewer可以偵測並阻擋這些惡意流量。此外，還可以藉由點擊連線數（Flows）來觀察相關詳細資料，如圖十。從該報表可以明顯看到該攻擊在IP行為上是有明顯規律性的。



圖九 記憶體快取 DDoS放大攻擊會透過發送大量包含小傳輸量的封包



圖十 zoom in後可觀察到其規律性

結論

綜觀以上所述，可總結Flowviewer的優點包含：

1. 可依據網路環境彈性配置設備：設備提供四種模式給網路管理者選擇，管理者可以網路環境實際需求來配置設備。設備介面採人性化、直覺操作，可在短時間內熟悉系統操作。

2. 可與其他網路設備做配合，有效提升網路安全：偵測到惡意流量時，可依網路管理者選擇自動在本機進行阻斷或是利用ACL在核心交換器阻斷。

3. 利用分析IP行為辨別惡意流量：透過收集五分鐘內的流量資料，針對各IP去分析其流量的來源位址、目的位址、來源埠號、目的埠號、傳輸量、封包數、時間、傳輸協定等欄位，並利用本公司獨立開發之演算法判別，可針對IP行為辨別惡意流量。利用此方式可精準判別攻擊與入侵，也不須額外購買新的特徵碼。

4. 可提供詳細流量資料報表作為犯罪追查之證據：提供多樣化報表（包含流量與各類型攻擊/入侵報表）可供查詢，並提供動態查詢功能供管理者能快速檢索特定條件的流量資料。