TWAREN 連線單位異常使用即時監控之設計與實作

梁明章
國家高速網路與計算中心
liangmc@narlabs.org.tw

摘要

本文將說明 TWAREN NOC 最近在 Netflow 網路通聯紀錄即時監控上的開發成果，使用連線單位的 Netflow 以及 ARP Table 或 MAC Address Table 資訊進行細緻的彙整、分析、綜合判斷，我們的設計方法與實作，在提供連線單位即時異常使用監控之餘，亦能為進行長時區間內微小規模動作的異常偵測研究累積資料，同時也累積骨幹層面惡意者的 IP 資料庫。

關鍵詞：TWAREN，骨幹網路，網路通聯紀錄，Netflow，異常使用偵測，即時監控告警。

1. 前言

TWAREN[1] NOC 的網管系統以自行開發為主，經歷十多年開發經驗，近年來由於大資料平台的開源與普及，NOC 利用 ElasticSearch[2]建立 Cluster 提供了足夠的運算力使得十幾年前只能用來做統計報表的 Netflow 網路通聯資料可以用來進行即時異常行為的偵測，並且將成果發表於 TANET2017 臺灣網際網路研討會論文「TWAREN 骨幹異常使用即時偵測與告警系統」[3]，歷年來也陸續發表更新的開發成果，然而我們的目標並非只是即時偵測到異常，而是希望能自動判斷是哪種異常，最好還能自動附帶對應的處置說明，甚至是自動應變，並且一直朝此目標前進。

目前我們的系統已經做到可以自動察覺大規模惡意行為的來源 IP 並自動下令全骨幹設備將其封包封鎖丟棄，也能自動察覺正被大規模攻擊的受害者 IP，只是因為自動清洗會影響受害者的正常服務，而受害者的承受能力上限也有差異，因此並不會自動執行清洗。

近幾年資安越發受到重視，NOC 除了維護骨幹網路運行之外，對於骨幹整體用戶的資安防護也希望能盡一分心力，而 NOC 擁有使用者單位所不具備的全網視角 Netflow 網路通聯記錄便是我們的切入點，既然我們已經對大規模的異常攻擊具備即時偵測封鎖的遏制能力，接下來我們就將目光投放到「以點及面，區域聯防」的方向研究，因為駭客除了對特定目標出手之外，大部分時候其實多是在廣泛探測收集可能入侵的弱點機器資訊，以擴充可控制的棋子兵團，因此我們嘗試針對某些連線單位做細緻的 Netflow 分析，做更複雜的綜合判斷，找到更明確的惡意者來源 IP，然後以點及面，擴及整個骨幹查找曾被該惡意者肆虐的網路通聯紀錄，當資料樣本越多之後，利用 AI 方法去學習分析該惡意者的行為特徵，或許也能牽扯出同家族的受害者或潛伏者，達到區域聯防的效果。

主要內容

本文主要報告這一兩年來 NOC 針對 Netflow 網路通聯紀錄應用在連線單位的細緻分析成果，我們選了有計畫合作的某連線單位開發加值服務，後文稱為試驗單位，在提供常規網路監控服務之後，接續開發異常使用的即時監控服務，另外將國網中心也列入連線單位異常使用監控服務的對象，下文開始說明我們的設計與實作。

1.1 連線單位的通聯記錄彙整分析與即時呈現

由於我們使用 nfdump 程式組[4]的 nfcapd 接收 netflow 封包分成一筆筆 netflow 紀錄來儲存，照預設值每五分鐘存成一個檔案，因此我們的程式讀取一個檔案資料就能進行五分鐘區間的彙整分析，若無特殊設定，路由器送出的每一筆 netflow 資料是單向的(要求路由器送雙向彙整的 netflow 會嚴重消耗資源，此非路由器的主要任務)，因此我們以連線單位為主視角稱為內部 inside，用 nfdump 讀取 netflow 資料檔分開列印成「內往外 egress」及「外往內 ingress」兩個方向暫時檔。

我們自行開發的彙整分析程式，本文後續以 nfdump2es 稱呼之，會先讀取 egress(內往外)的 netflow 紀錄，以來源 IP(Souce IP，即單位內部 IP)為基底進行彙整建立物件陣列，在此稱為陣列 A，如下**圖1**所示，陣列 A 內每個內部 IP(圖內稱為 iIPn)對外的連線目標 IP(Destination IP，圖內稱為 oIPn)在此內部 IP 物件內以其連線目標 IP 為基底建立 peer 物件陣列並做 netflow 彙整，但在此需要設下限制，如果一個內部 IP 在五分鐘內對外傳輸的 unique peer 數量超過臨界值就不再增加 peer 陣列元素，臨界值可以觀察單位對外的服務連線數量來定(例如 DNS、WEB 服務)，此外，以所有連線目標 IP 為基底另外建立一個物件陣列彙整數據，在此稱為陣列 B，陣列 B 每個 IP 物件會掛上與它有關的內部 IP 物件也以指標作為陣列，無須複製整個物件，以節省記憶體，因此，此階段將會建立一個內部 IP 為基底的雙層巢式物件陣列 A，以及一個外部目標 IP 為基底的物件陣列 B。

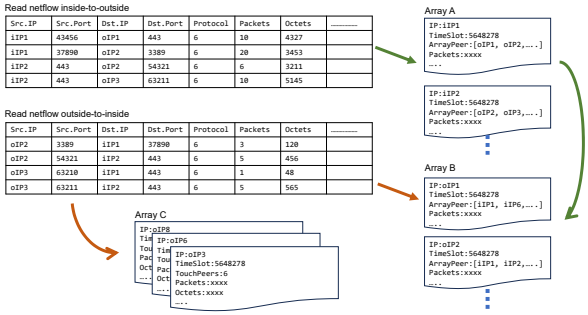

圖 1 netflow 讀取階段示意圖

參見上**圖1**在讀取第一筆 netflow 時，以其 Unix Epoch TimStamp 加上150秒後除以300秒取整數商做為本次所有物件的統一時間槽編號 TimeSlot，等於是從格林威治時間零點開始每五分鐘步進一個時間槽號碼，往後本文相關運算只要比對 TimeSlot 相等就代表是同時區間內的紀錄。

第二階段，nfdump2es 會讀取 ingress(外往內)的 netflow 紀錄檔，作法同樣參見上**圖1**，此階段就會開始浮現一些異常現象，說明幾種組合情況如下。

首先，將外部 IP(此時為 Source IP)與陣列 B 做比對，如果發現符合者，就與其所掛的內部 IP 陣列元素比對目標 IP(也就是內部 IP)，如果有符合的內部 IP，則將此 netflow 的數據合併入陣列 A 中該內部 IP 的數據以及其下的外部 IP 數據，這樣的情況將會放在所有資料讀完之後再做異常判斷，除此以外的其他情況會在讀資料時先做判斷處理。

舉例一，若在陣列 B 比對時就查無符合者，表示該外部 IP 並沒有任何內部 IP 的反向傳輸封包，表示它是逕自單向連線，如果它的連線目標內部 IP 有存在於陣列 A 中，代表內部 IP 拒絕回應它(無服務)或是被防火牆拋棄封包(非白名單)，有可能是惡意行為。

舉例二，如果它的連線目標內部 IP 並未出現在陣列 A 中，則該外部 IP 疑似故意調查單位內有使用的 IP，惡性概率高，故將此外部 IP 加入異常者陣列，後續稱為陣列 C，加總其數據。

某些外部 IP 可能同時犯有如上兩例情況，但因為 netflow 並無封包內容可分析，無法肯定例一必然異常，因此我們僅針對異常概率較高的例二做紀錄。

當兩個方向 netflow 資料讀取完後，進入第三階段，就前文已經建立好的三大陣列資料進行綜合判斷，此時陣列 A 代表五分鐘內有對外傳輸動作的內部 IP，陣列 B 代表與陣列 A 互有傳輸的外部 IP，而陣列 C 則是沒有陣列 A 關聯的外部 IP，此時會針對各陣列做下列分析判斷步驟：

I：陣列 B 每個外部 IP 其下都掛有與其關聯的內部 IP 列表，逐一計算跟每個內部 IP 的傳輸特徵，例如平均封包大小若沒大於48Bytes 顯然毫無有效傳輸內容，明確異常，如果關聯的內部 IP 僅有一個或數個，封包量又大，可懷疑其為 TCP flooding 類型攻擊。如果關聯的內部 IP 非常多，過半或甚至接近全部，則可懷疑其為掃瞄探測攻擊，對於陣列 B 中被判斷為惡意者的，就納入陣列 C 中。

II：分析陣列 A，如果某內部 IP 的對外連線 peer 數量已達臨界值且非已知服務器，就是需要告警的異常，也可綜合平均封包大小、netflow 總數量、內外傳輸量的比例等幾個面向的數據是否超過設定臨界值的組合狀況來判斷是否需注意的異常與類型。

實務上可以先收集單位對外的網路服務與其行為特徵列為白名單，使在分析陣列 A 時可以避免告警已知服務器，藉此可將各項臨界值降低以提高靈敏度，抓出非人類行為的異常，舉個例子，雙方向傳輸量皆大且平均封包小、peer 數又多的，有可能是 p2p 行為。異常判斷結果會記錄回陣列 A 的欄位中。

III：分析陣列 C，陣列 C 的主要作用在於累積惡意者 IP 到骨幹範圍的資料中，未來作為 NOC 異常偵測自動封鎖與解鎖機制的參考，慣犯就要更嚴苛對待。

第四階段就是將上述分析判斷結果寫回陣列中的欄位之後，開始轉換陣列物件資料為 JSON 文件以寫入 NoSQL 大資料平台，以及準備填入 SQL 的紀錄，下**圖2**略舉一些陣列 A 轉換的欄位例子，下**圖3**略舉一些陣列 B 轉換的欄位例子。

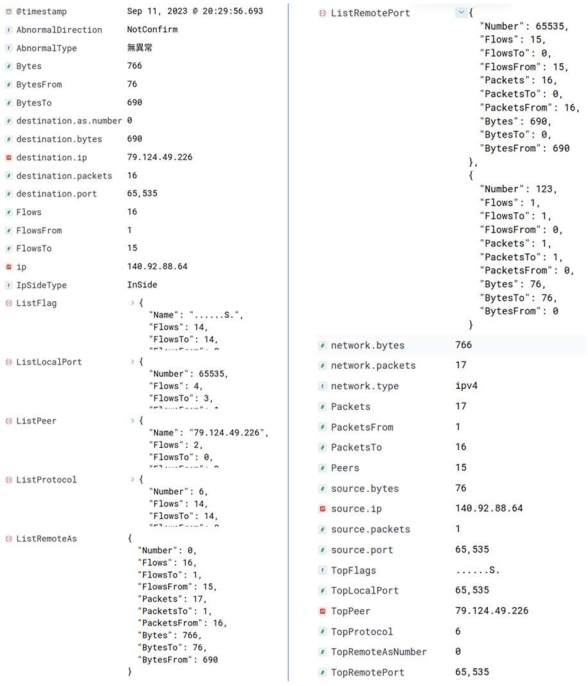

圖 2 陣列 A 欄位例圖

@timestamp	Sep 12, 2023 @ 00:20:00.270
AbnormalDirection	Attacker
AbnormalType	掃瞄探測者
Bytes	6,280
BytesFrom	6,240
BytesTo	40
Flows	157
FlowsFrom	156
FlowsTo	1
ip	107.170.234.40
IpSideType	OutSide
Packets	157
PacketsFrom	156
PacketsTo	1
Peers	156

圖 3 陣列 B 欄位例圖

第五階段就是通報或告警，不過因為試驗單位並不希望採用告警或通報的方式，因此我們採用 Dashboard 網頁呈現圖表的方式提供給試驗單位的網管人員，當他們感覺網路怪怪時即可上 Dashboard 查看狀況，擷取其中兩塊圖表如下**圖4**，此圖例發生當下，試驗單位網管人員通報他們對外傳輸卡卡不順暢，而 Dashboard 正好呈現出有外部 IP 正在進行短時間高頻率惡意行為影響了該單位的邊界資安設備。因為我們使用的 ES 平台資料進入後就可即時查詢，因此 Dashboard 的查詢結果約只比案發時間晚五分鐘(因為五分鐘一輪統計分析的緣故)。

圖 4 連線單位即時異常監控 Dashboard 部分截圖

1.2 ARP 與 MAC 的資料協助

由於我們使用的 netflow 只從骨幹到試驗單位的邊界路由器為止，我們僅能記錄到單位內傳出來的封包來源 IP，然而該 IP 是否真實卻不得而知，被駭客控制的電腦要作案時也未必會使用自己的 IP，有可能臨時假冒他人 IP，因此，如果要更加細緻的監察單位內的異常，可以蒐集 ARP table 與 MAC-address table 來進行輔助。

下**圖5**顯示我們能從 Layer2/3 switch 上收集 IP 與 MAC 來自哪個 switch port 的資訊。

Collect ARP information from layer3 switch

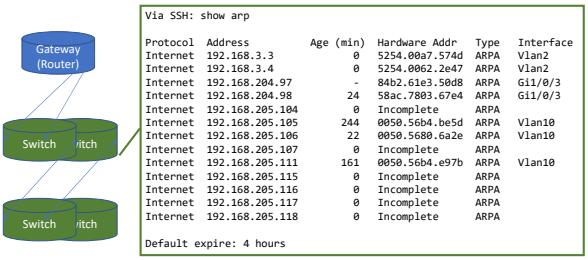

圖 5 連線單位 Layer3 switch ARP 擷取圖

而純粹的 Layer2 swicth 或僅啟用 Layer2功能的 Layer3 switch 沒有 ARP table 可查，下**圖6**顯示我們可以改查 mac-address table 的資訊來替代，只是無法獲得 IP 資訊，但可以記錄 MAC address 的實體位置，以桌機或伺服器而言，這位置不會經常變動，但筆電或行動裝置較可能改變無線接取位置，但大致來說資料還是有參考價值的。

Collect MAC information from layer2 switch

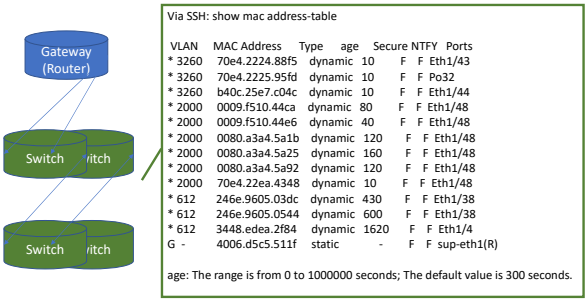

圖 6 連線單位 Layer2 switch MAC table 擷取圖

在 Gateway 設備上同樣也可取得 ARP table 資訊，如下**圖7**，一個內部 IP 若與外部有傳輸行為，必然要在 Gateway 設備的 ARP table 存在資訊，而從圖中可見 State 欄位有幾種狀況，其中 Incomplete 狀態的 IP 查無 MAC address，而 Age 是四秒，表示有外部 IP 想送封包給211.79.60.29，而 Gateway 送出 ARP request 之後已經過了4秒還沒收到任何機器回應，如無意外，此 IP 當下是沒有設備在使用的，換言之有外部 IP 正企圖連線未使用的 IP 211.79.60.29，那個外部 IP 有可能在惡意探測，可結合前章節的判斷，將此 IP 列入陣列 C 當中。

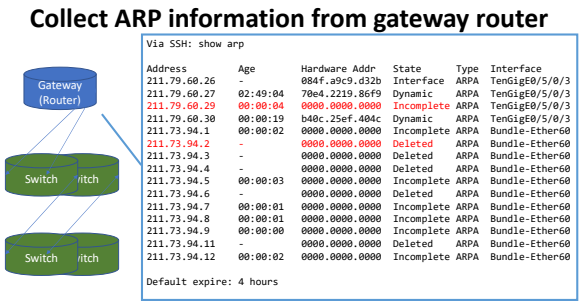

圖 7 連線單位 Geteway Router ARP table 擷取圖

我們將收集到的資料分別以 IP address 跟 MAC address 為基底彙整成一個個物件，並且轉換成如下**圖8**的 JSON 文件記錄並送入大資料平台儲存，即可在前面章節的綜合判斷中以 TimeSlot 為時間戳記來提取加入判斷。

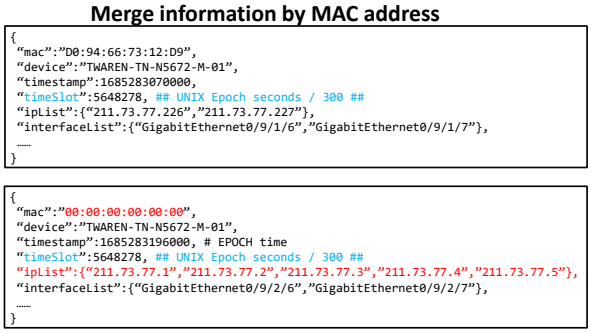

圖 8 連線單位 ARP & MAC 彙整資訊示意圖

1.3 長時區間彙整分析

前文所提的每輪彙整分析結果存入大資料平台，還可利於長時區間的彙整分析，藉著資料分階段準備的方式，可避免一次性運算海量 netflow 資料的超大算力需求。

我們將試驗單位每日的彙整結果查詢出來以內部 IP 為基底再做全日的彙整陣列時，可以用來查找一些極小規模的不正常行為，舉個例子，將陣列用 flow 總數做反向排序，浮現在前的就會出現一些不正常現象，某些內部 IP 整天下來僅會連線一兩個外部 IP 一次並送出一些封包，或是僅從某外部 IP 抓回一些封包，次數只有一兩次，這樣的行為是相當怪異的，疑似在跟 C&C 聯繫，可以註記該 IP 疑似已被入侵或請單位網管進行檢查。

而前章節提到的 ARP/MAC table 的儲存，在積累一段時間之後，也能透過搜尋查出一個 MAC address 使用多個 IP 的設備，如果該設備並非行動裝置，那其行為就甚為可疑，可能是冒用 IP 進行攻擊或聯絡 C&C，即使他的動作規模或次數很微小，也會被這方法探查到。

1.4 未來工作

當我們研究哪些特徵組合是異常時，或許可以反向思考，正常人類操作會有哪些特徵組合，如此反而樣態較少更容易列舉，那麼不符合這些人類組合的就是異常了，排除掉已知的服務器，剩下的可以導入 AI 方式去學習異常的分類，這也是我們團隊正在進行的研究之一。

本文提到的多種資料收集來源與方式，我們仍在開發中，以往我們優先開發即時偵測的機制，往後會持續往長時間累積資料的分析偵測進行研究，試著找出潛伏或小規模小動作的異常者，拔除隱患，未來若有進展將會持續報告成果。

參考文獻

[1] TWAREN，TaiWan Advanced Research and Education Network，台灣高品質學術研究網路，http://www.twaren.net/

[2] https://www.elastic.co/

[3] 梁明章, "TWAREN 骨幹異常使用即時偵測與告警系統", TANET2017 臺灣網際網路研討會, 2017.

[4] https://github.com/phaag/nfdump/