NARLabs 國家實驗研究院

國家高速網路與計算中心

骨幹大規模異常行為特徵自動萃取與搜尋Botnet之開發報告

TWAREN NOC 平台開發組

梁明章

前言(1/3)

NARLabs

- TWAREN NOC維運團隊利用研究網路骨幹NetFlow開發的即時異常使用偵測系統，以ElasticSearch Cluster即時儲存NetFlow資料建立全文檢索，以C語言開發高速的彙整、統計、排序查詢系統作為前端輔助系統，結合兩者開發即時異常使用與攻擊偵測暨告警系統，即時偵測大規模大範圍掃瞄或攻擊、SYN flooding攻擊、DDoS攻擊、高流量使用者，說明實作方法，可自動告警並通報相關資訊以供NOC或各校網管人員快速反應處理，如攻擊入口過濾、特徵說明等，並留存偵測結果作為進一步研究的資料來源。

前言(2/3)

NARLabs

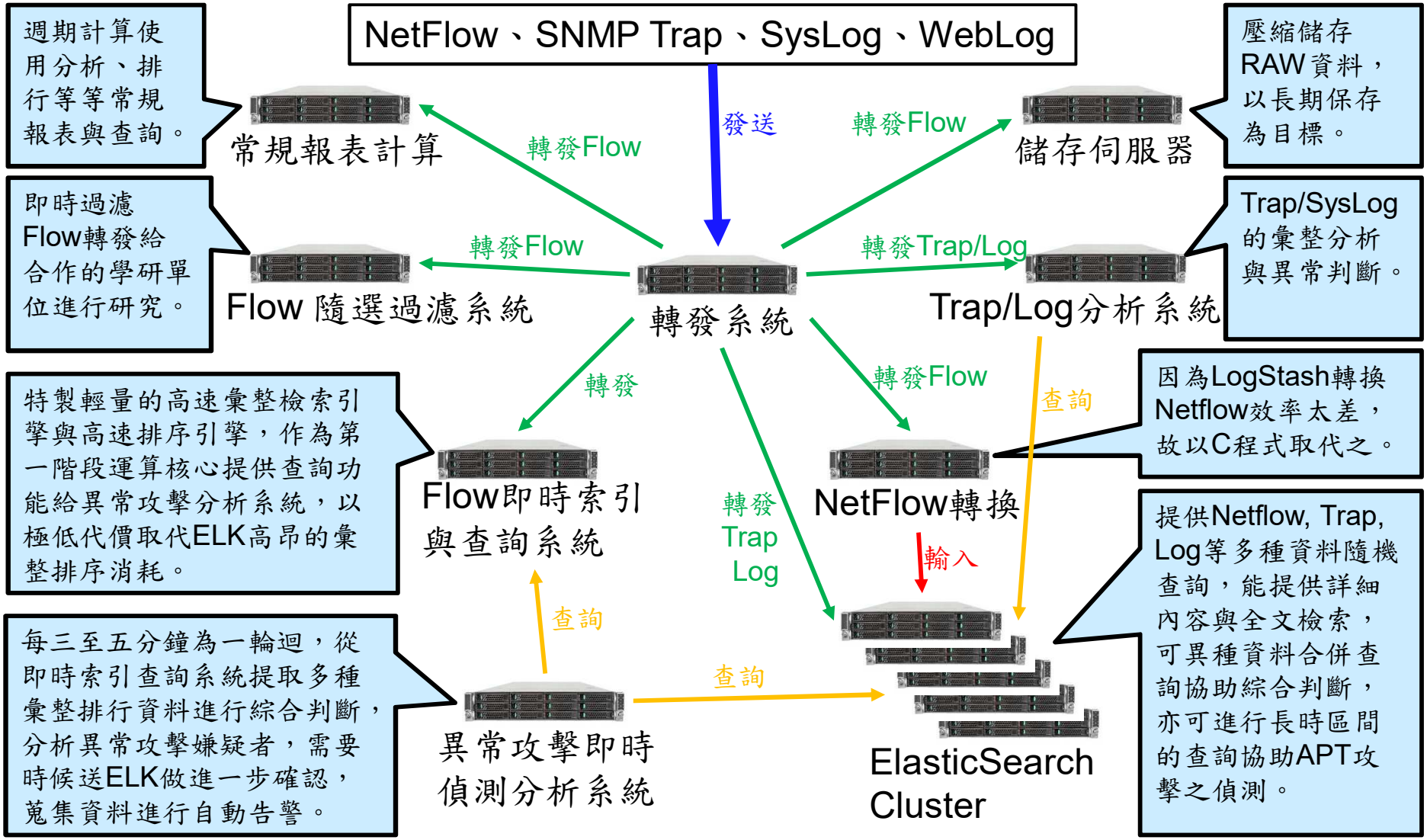
- 國網中心已有一個資安團隊利用HoneyPot及資安設備捕捉惡意軟體分析行為與C&C，但只能捕捉落入陷阱者或能複製到封包的線路，而我們想以「面」的方向進行，以骨幹Netflow做全面性的Botnet偵測，雖然精確度不如HoneyPot「點」的做法，但優點是涵蓋面廣，結果可以互補並互相參考，本文將要說明我們如何利用骨幹Netflow大資料來尋找Botnet的成員相關的研究。

前言(3/3)

NARLabs

- 本文將說明TWAREN NOC利用骨幹Netflow大資料研究骨幹大規模異常行為的特徵萃取，然後利用這些特徵從Netflow大資料中尋找同類的小規模異常者進行判斷與紀錄，並將這些程序實作為自動化機制，以協助相關學術研究或使學術單位網管可以依此清除受感染者或進行Botnet傳輸內容研究，同時也說明一些在節省硬體經費的前提下優化大資料演算的心得跟各校分享。

現行系統架構


NetFlow、SNMP Trap、SysLog、WebLog
發送
常規報表計算
轉發Flow
轉發Flow
儲存伺服器
週期計算使用分析、排行等等常規報表與查詢。
壓縮儲存RAW資料，以長期保存為目標。
即時過濾Flow轉發給合作的學研單位進行研究。
轉發Flow
轉發Trap/Log
Flow 隨選過濾系統
轉發系統
Trap/Log分析系統
Trap/SysLog的彙整分析與異常判斷。
轉發
轉發Flow
查詢
因為LogStash轉換Netflow效率太差，故以C程式取代之。
特製輕量的高速彙整檢索引擎與高速排序引擎，作為第一階段運算核心提供查詢功能給異常攻擊分析系統，以極低代價取代ELK高昂的彙整排序消耗。
Flow即時索引與查詢系統
轉發
Trap
Log
NetFlow轉換
輸入
提供Netflow, Trap, Log等多種資料隨機查詢，能提供詳細內容與全文檢索，可異種資料合併查詢協助綜合判斷，亦可進行長時區間的查詢協助APT攻擊之偵測。
查詢
每三至五分鐘為一輪迴，從即時索引查詢系統提取多種彙整排行資料進行綜合判斷，分析異常攻擊嫌疑者，需要時候送ELK做進一步確認，蒐集資料進行自動告警。
查詢
異常攻擊即時偵測分析系統
ElasticSearch Cluster

骨幹異常行為即時偵測告警

NARLabs

- 大規模廣域掃瞄
  - 服務掃瞄
    - 特定IP對大量IP,大量Port,小封包
  - 特定弱點探測或入侵
    - 特定IP對大量IP少量Port，小封包探測，大封包入侵
- 大規模攻擊
  - 網域癱瘓攻擊
    - 大量Flow/Pkt/Bytes集中輸出到特定網域內
  - 服務阻斷攻擊
    - 少量IP大量FLOW集中輸出到特定IP
    - 大量Fake IP大量FLOW集中輸出到特定IP，找出攻擊路徑，作為防禦或清洗參考
- 嚴重超量行為
  - 所有異常都會被記錄並進入追蹤程序，追蹤結果符合告警條件才觸發告警。
  - 若異常數據符合嚴重規模者立即告警，以求快速處置。

即時異常偵測系統產生第一階段資料(例1)

NARLabs

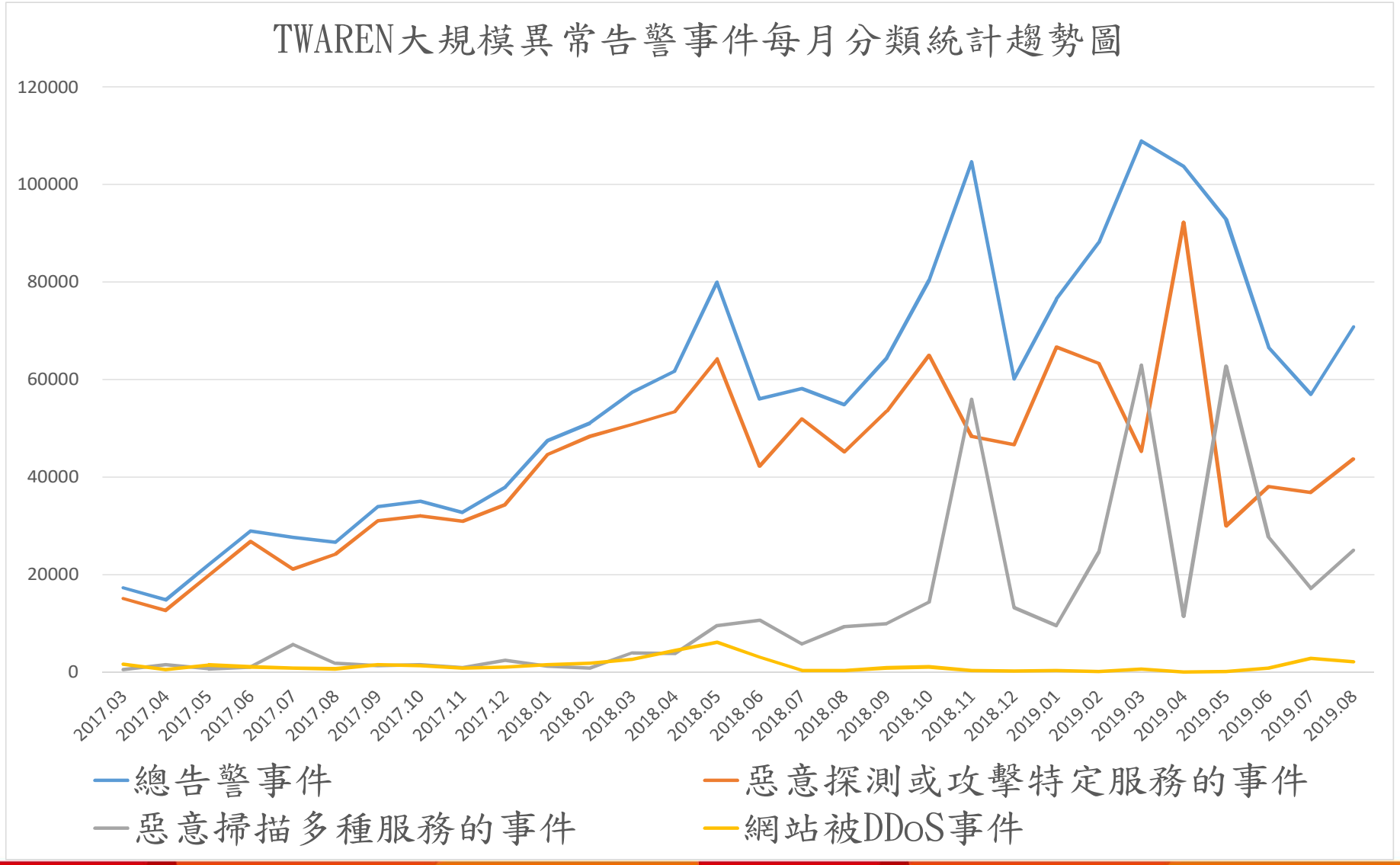
- ※Attacker：203.xxx.xxx.115 (xx中心)
- ※異常類型：連線對象過多
- ※異常超標：五分鐘內連線不同IP數高達61,812個
- ※主要特徵：『協定：TCP（99.98%）』『應用埠：SSH-22（99.94%）』
- ※資訊摘要：
- ＊使用協定共3個：TCP(99.98%)
- ＊目的Port共23個：SSH-22(99.94%)
- ＊Octet特徵共1054個：180(13.49%)：120(8.43%)：1915(7.64%)：60(7.50%)：244(6.65%)：40(6.49%)：240(5.95%)：1931(4.45%)：1811(2.92%)：220(2.38%)
- ＊Packet特徵共34個：3(15.74%)：1(15.06%)：5(13.55%)：14(12.54%)：2(9.51%)：4(7.07%)：12(5.23%)：11(4.51%)：7(4.12%)：13(4.06%)
- ＊本IP開始異常時間已超過0日0時5分，其中100.0%時間超過告警標準，最近已持續0日0時5分超過告警標準

即時異常偵測系統產生第一階段資料(例2)

NARLabs

- ※Attacker：140.1xx.26.68（xx區網中心）
- ※本IP開始異常時間已超過0日0時25分，其中100.0%時間超過告警標準，最近已持續0日0時30分超過告警標準
- ※嚴重超標：『五分鐘內連線不同IP數高達606,723個』
- ※主要特徵：『協定：TCP（100.00%）』『應用埠：2375（99.34%）』『封包數與大小：98.54%以上的Flow內有封包1個共40(Bytes)』『SYN比例超過95%』
- ※異常類型：疑似大範圍掃瞄或入侵
- ※資訊摘要：五分鐘內『連線對象606723個』『使用協定共2個：TCP(100.00%)』『目的Port共5個：2375(99.34%)』『Octet特徵共311個：40(98.49%)』『Packet特徵共26個：1(98.60%)』

異常特徵萃取方法研究(1/3)



異常特徵萃取方法研究(2/3)

	2019-05		2019-06		2019-07		2019-08	
異常重點	事件數	異常者IP數	事件數	異常者IP數	事件數	異常者IP數	事件數	異常者IP數
疑似大範圍掃瞄或入侵	55723	1110	54296	1326	47268	1063	62048	1157
連線對象過多	35976	443	10958	562	5587	444	7756	454
輸出流量過高	99	11	147	18	790	24	101	25
疑似SYN攻擊	88	23	157	32	94	19	90	13
疑似被DoS攻擊	64	11	29	9	1997	14	72	10
下載流量過高	44	6	801	16	552	14	943	18
Flow數量過多	13	7	42	8	221	33	648	14
疑似被分散式攻擊特定服務Port			26	7				
疑似大範圍傳出資料			14	3	13	2	307	19
疑似被分散式掃描服務或癱瘓主機網路							35	1
傳輸量過多							1	1
封包數量過多	1	1	11	6	14	13	12	6
連線對象超級多			1	1	7	2	3	1
Flow數量超級多	15	5	17	3	7	2	69	2
封包數量超級多	2	2	1	1			4	2
傳輸量超級多							1	1
尚未定義	1	1	3	3			1	1

異常特徵萃取方法研究(3/3)

NARLabs

- Port 22 | 發現特徵12種
  - 1＃22-1-52：8個攻擊者：103.207.36.130(@Hanoi[VN])…
  - 2＃22-4-240：5個攻擊者：185.232.67.11(@Timisoara[RO])…
  - 3＃22-1-48：76個攻擊者：139.220.192.57(@Beijing[CN])…
  - ……
  - ……
- Port 1433 | 發現特徵9種
  - 1＃1433-1-40：55個攻擊者：125.64.94.220(@Chengdu[CN])…
  - ……
  - 5＃1433-3-152：2個攻擊者：222.74.48.230(@Baotou[CN])
    218.4.133.202(@Nanjing[CN])……
  - ……
  - ……
- 高頻率TCP探測攻擊者通常無法經由系統SOCKET程序，需透過SOCKET_RAW或網卡驅動程式自行創造封包並維護管理回傳封包，封包構成與大小可能具有家族特色。

以特徵尋找小規模異常者

NARLabs

- 以1433-3-152做過濾條件，隨機對某個上班日萃取出符合條件的Netflow，然後以sourceIPAddress做彙整Bucket，然後每個Bucket內再針對destinationIPAddress與sourceTransportPort做彙整，計算每個sourceIPAddress以這種特徵連線了多少個destinationIPAddress

來源IP	目標IP數量	Netflow筆數	來源Port數
1.170.36.229	63788	73274	13409
140.130.93.101	10076	31483	6936
122.165.92.180	6238	6542	5698
113.16.174.66	1295	1577	1318
202.127.28.58	1166	1556	1166
140.130.46.118	753	1277	753

- 除了第一名超過告警臨界值會被注意，第二名之後量都很小，整天下來才幾千筆，資安設備根本不會感覺異常，然而它們確實是有問題的，當我們繼續分析前後幾日資料，發現這些異常IP的雷同度相當高，而且整日數量也都是一兩千，真正的細水長流，屬於Botnet Master口袋內的預備兵，而這些小規模的異常者正是本文研究抓取的目標。

ES使用心得(1/4)

NARLabs

- TWAREN NOC團隊使用ElasticSearch作為大資料平台(後文簡稱為ES)，使用16台中階伺服器，每台320GB記憶體，六顆4TB硬碟，所以每台機器運行六個ES Data-Node，每個JVM的Heap-Memory設定為31GB，根據ES官方建議，每個Node需要另外一倍的記憶體作為Lucene引擎的IO緩衝記憶體，實際上六個Node需求360GB記憶體，所以我們算是超載使用，但是TWAREN的Netflow資料量使我們不得不如此做。

ES使用心得(2/4)

NARLabs

- ES將一個資料庫稱為一個INDEX，可以隨意命名，一個INDEX拆分成多個Shard(分片)，原則上一個運算單位(Data-Node)最多收容一個Shard是最安全的分配。當Client-Node接收到來自使用者的Search-Request時，Client-Node會先分析該查詢涉及到哪些INDEX，然後查出每個INDEX有哪些Shard，哪個Shard目前位於哪個Data-Node，再來就把Request分發到那些Shard所在的Data-Node，每個Shard獨立運行一個Lucene Engine來計算，然後將結果送回給Client-Node進行彙整。

ES使用心得(3/4)

NARLabs

- JVM HEAP
  - 小於32GB時以Compressed OOPS技術壓縮物件的定址(32位元)
- Shard大小與數量
  - 假如Heap size設定32GB的話，Shard不宜超過10GB，否則會對JVM內其他工作的記憶體擠壓太嚴重
  - Shard太小會造成Cluster內Shard總數過多增加Cluster管理負荷
  - 資料龐大的ES Index宜以每日一個Index為佳，然後將Index內Primary Data總大小除以10GB得到的商值就是適當的Shard數
  - Shard數不需要一成不變，可以隨著資料增長而調整，但是每個Index的Primary Shard數量不可超過Data-Node總數

ES使用心得(4/4)

NARLabs

- 每一次的統計彙整不要產生數千萬甚至億等級的**Bucket**數量。
- 將複雜的複合查詢拆開成多階段，階段之間的成果可以導出給自己寫的程式進行適當的篩選、計算成為濃縮的結果，再進行下一階段查詢。
- 根據查詢之間的相依關係調整順序，盡量使前次查詢產生的中途陣列或**IO**緩衝區資料可以被下次查詢引用。

NARLabs

Q&A