NARLabs 國家實驗研究院

國家高速網路與計算中心

TWAREN異常使用與攻擊之即時偵測與告警通報

網路與資安組 **TWAREN NOC**

承諾·熱情·創新

www.narlabs.org.tw

研發宗旨與目標

NARLabs

- 利用大資料平台與自行開發的系統，結合TWAREN研究網路骨幹的 NetFlow 大資料、網路設備SNMP-Trap與SysLog、資安設備Log、伺服器SysLog、WebLog等多方面資料，即時偵測大規模大範圍掃瞄或攻擊、SYN flooding攻擊、DDoS攻擊、高量使用者等等，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，協防各連線學校或單位，降低學術網路整體損失，並留存偵測結果作為進一步研究的資料來源。

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

IP USER異常判斷1~初篩

NARLabs

- 正常日netflow約每秒一萬至三萬筆的產生速度，五分鐘可累積近千萬筆，內含 Unique IP 約百萬個。
- 利用自行開發的Netflow彙整排序引擎分別按照Flow、Byte、Packet、LinkPeer、SYN旗標數等五個方面查詢出Top-100，共500個IP各得一嫌疑分。(每次排序耗時都不到一秒，可頻繁查詢)
- 其中IP重複者合併且嫌疑分累加，合併後通常只會剩下三百多個嫌疑者IP。
- 進入第二階段判斷。

IP USER異常判斷2~判斷方向

NARLabs

- 依照**Flow**、**Packet**、**Byte**個別計算雙向差距比例以及方向，比例差值越大嫌疑越大，方向越明顯，以此判斷為攻擊者或受害者。
- 前述三項比例差值超過異常指標，或 **SYN**旗標占比超過異常指標，或是**Flow / Packet / Byte / LinkPeer** 數值超過異常指標，皆進入第三階段判斷。

IP USER異常判斷3~異常分類

NARLabs

- 攻擊者的LinkPeer IP數低於1000者，判斷為非廣域行為，DDoS可能性低，針對特定服務入侵或DoS可能性高，向ES查詢該IP所有LinkPeer與Flow數排名，若前幾名LinkPeer的Flow數占比極高，甚至高達90%以上，則該LinkPeer可能是被DoS或DDoS的集火目標，檢查該Peer是否已在三百多嫌疑者列表中，若無，則將該Peer補加入檢查列表。
- 向ES查詢各嫌疑者IP的Port、協定種類、封包數量、封包大小，各別彙整排序，根據前幾名的百分比，可判斷是否為特徵。
- 綜合多項特徵，評估推測異常類型。

IP USER異常判斷4~告警

NARLabs

- 經判斷為異常者，分析結果與詳細數據寫回ES，以便後續研究使用。
- 異常者的Flow、Packet、Byte、LinkPeer、雙向比例差等數據各有嚴重指標，超過一項得一告警分，告警分達二分則立即觸發告警信，餘者則僅進入追蹤列表。
- 追蹤列表中的異常者若持續6輪異常(每輪五分鐘)則觸發告警信，之後持續12、72、288輪異常會再發告警信，超過一天之後每天一次告警信。
- 追蹤列表中的異常者若持續6輪沒有異常，就會被移除追蹤。

異常偵測結果資料內容擷圖

NARLabs

Table JSON

View surrounding documents View single document

t	Abnormal	Attacker
#	AbnormalType	1
t	AncestorID	129.78.110.124_1505715422004
#	AvgPacketSizeIn	48
#	AvgPacketSizeOut	40
#	ByteAll	12,047,123
#	ByteIn	814,764
#	ByteOut	11,232,359
#	CountDstPort	11
#	CountOctet	49
#	CountPacket	34
#	CountProtocol	3
t	Description	嚴重超標：『五分鐘內連線不同IP數高達210,871個』 主要特徵：『攻擊協定：TCP（99.99%）』『攻擊應用埠：DNS-53（99.99%）』『封包特徵：99.16%以上的Flow內有封包1個共40(Bytes)』 綜合推測：『疑似正在進行大範圍感染入侵』『含SYN旗標的Flow高比例異常（95.83）%）』『疑似以TCP廣域連線』『重點攻擊TCP應用埠DNS-53（99.99%）』 資訊摘要：『使用協定共3個：TCP(99.99%)』『目的Port共11個：DNS-53(99.99%)』『Octet特徵共49個：40(98.94%)』『Packet特徵共34個：1(99.39%)』
#	Direction	-3
#	EsHits	318,083
#	FlowAll	288,456
#	FlowIn	12,042
#	FlowOut	276,414
t	Geoip.city	Sydney
🌐	Geoip.coordinates	151.1982, -33.8612
t	Geoip.country_code	AU
#	Geoip.latitude	-33.861
#	Geoip.longitude	151.198
t	ID	129.78.110.124_1505715722022
💻	IP	129.78.110.124
#	KeepMonitorContinueWarnTimes	2
t	KeepMonitorString	本IP開始異常時間已超過0日0時10分，其中100%時間超過告警標準，最近已持續0日0時10分超過告警標準
#	LinkIPs	210,871
?	ListDstPort	{ "Key": 53, "Count": 318044, "Note": "DNS-53",

告警信範例1

回覆 | 回覆全部 | 轉寄 | 備存 | 垃圾郵件 | 刪除 | 更多

主旨 **Netflow 五分鐘異常偵測 2 個嫌疑者達告警標準 (09/18/2017 13:02:05)** 13:02

給 [redacted]

副本 [redacted]

```
================================================================================
Netflow 五分鐘異常偵測 2 個嫌疑者達告警標準 (09/18/2017 13:02:05)
================================================================================
Victim：140.112.33.135
嚴重異常，立即告警
嚴重超標：『封包數21,386,205 (21,386,197/8) 高達全網2.44%』『用量29,939MB (29,939/0) 高達全網4.12%；平均速率 (798.40/0.00) (Mbps)』
綜合推測：『疑似被DoS攻擊，攻擊者IP為65.254.100.36』
資訊摘要：『使用協定共2個：TCP(72.41%)；UDP(27.59%)』『目的Port共13
個：51794(20.69%)：51807(18.39%)：63508(9.20%)：64287(8.05%)：51799(6.90%)：51782(5.75%)：51786(5.75%)：51790(5.75%)：51798(4.60%)：51802(4.60%)』『Octet特徵共38
個：1304(10.34%)：4811(9.20%)：632(8.05%)：52(3.45%)：312(3.45%)：364(3.45%)：4848(3.45%)：9632(3.45%)：40(2.30%)：416(2.30%)』『Packet特徵共33
個：1(24.14%)：15(9.20%)：2925750(4.60%)：6(3.45%)：7(3.45%)：10(3.45%)：12(3.45%)：59(3.45%)：8(2.30%)：17(2.30%)』
詳情網址： http://[redacted].twaren.net/[redacted]/?fddate=2017.09.18&fdtype=Victim&fdid=140.112.33.135_1505710921401
================================================================================
Attacker：65.254.100.36
嚴重異常，立即告警
嚴重超標：『封包數21,386,197 (0/21,386,197) 高達全網2.44%』『用量29,939MB (0/29,939) 高達全網4.12%；平均速率 (0.00/798.40) (Mbps)』
綜合推測：『疑似參與DDoS大軍會合攻擊 140.112.33.135，攻擊者可能是Botnet成員』
資訊摘要：『使用協定共2個：TCP(73.03%)；UDP(26.97%)』『目的Port共13
個：51794(22.47%)：51807(17.98%)：63508(8.99%)：64287(7.87%)：51799(6.74%)：51782(5.62%)：51786(5.62%)：51790(5.62%)：51798(4.49%)：51802(4.49%)』『Octet特徵共38
個：1304(12.36%)：4811(8.99%)：632(7.87%)：52(3.37%)：312(3.37%)：364(3.37%)：4848(3.37%)：9632(3.37%)：40(2.25%)：416(2.25%)』『Packet特徵共33
個：1(25.84%)：15(8.99%)：2925750(4.49%)：6(3.37%)：7(3.37%)：10(3.37%)：12(3.37%)：59(3.37%)：8(2.25%)：17(2.25%)』
詳情網址： http://[redacted].twaren.net/lmj/?fddate=2017.09.18&fdtype=Attacker&fdid=65.254.100.36_1505710921401
================================================================================
檢視本次偵測所有異常IP詳細資料 http://[redacted].twaren.net/[redacted]/?timerange=1505710861401-1505710981401
```

告警信範例2

回覆 | 回覆全部 | 轉寄 | 備存 | 垃圾郵件 | 刪除 | 更多

從 [redacted]

主旨 **Netflow 五分鐘異常偵測 2 個嫌疑者達告警標準 (09/16/2017 00:27:03)**　　西元2017年09月16日 00:27

給 [redacted]

副本 [redacted]

==========

Netflow 五分鐘異常偵測 2 個嫌疑者達告警標準 (09/16/2017 00:27:03)

==========

Attacker：202.118.69.89

本IP開始異常時間已超過1日0時0分，其中100%時間超過告警標準，最近已持續1日0時0分超過告警標準

異常超標：『五分鐘內連線不同IP數高達50,221個』

主要特徵：『攻擊協定：TCP（100.00%）』『封包特徵：93.57%以上的Flow內有封包1個共40(Bytes)』

資訊摘要：『使用協定共2個：TCP(100.00%)』『目的Port共181個：60151(2.43%)：60152(2.40%)：60145(2.39%)：60142(2.20%)：60191(2.10%)：60186(1.92%)：60160(1.88%)：60192(1.81%)：60141(1.78%)：60144(1.72%)』『Octet特徵共12個：40(93.45%)：152(4.00%)：80(1.53%)』『Packet特徵共4個：1(93.69%)：3(4.01%)：2(2.16%)』

詳情網址：http://[redacted].twaren.net/[redacted]/?fddate=2017.09.16&fdtype=Attacker&fdid=202.118.69.89_1505492822124

==========

Attacker：199.48.164.35

本IP開始異常時間已超過0日0時30分，其中66%時間超過告警標準，最近已持續0日0時10分超過告警標準

異常超標：『五分鐘內連線不同IP數高達36,817個』

主要特徵：『攻擊協定：UDP（100.00%）』『攻擊應用埠：5060（100.00%）』

資訊摘要：『使用協定共1個：UDP(100.00%)』『目的Port共1個：5060(100.00%)』『Octet特徵共79個：435(27.58%)：434(23.22%)：436(19.78%)：433(14.13%)：432(7.12%)：437(3.38%)：431(2.86%)：430(1.08%)』『Packet特徵共23個：1(99.66%)』

詳情網址：http://[redacted].twaren.net/[redacted]/?fddate=2017.09.16&fdtype=Attacker&fdid=199.48.164.35_1505492822124

==========

檢視本次偵測所有異常IP詳細資料 http://[redacted].twaren.net/[redacted]/?timerange=1505492762124-1505492882124

Labs

請選擇功能

TWAREN Netflow 異常偵測紀錄區間查詢結果，時間點：2017/09/16 週六 00:27:02.176

- 140.112.50.233 (Victim) 2017/09/16 週六 00:27:02.176
- 136.172.30.85 (Attacker) 2017/09/16 週六 00:27:02.176
- 202.118.69.89 (Attacker) 2017/09/16 週六 00:27:02.124
  - DocumentID：202.118.69.89_1505492822124
  - 異常超標：『五分鐘內連線不同IP數高達50,221個』
  - 主要特徵：『攻擊協定：TCP（100.00%）』『封包特徵：93.57%以上的Flow內有封包1個共40(Bytes)』
  - 資訊摘要：『使用協定共2個：TCP(100.00%)』『目的Port共181個：60151(2.43%)：60152(2.40%)：60145(2.39%)：60142(2.20%)：60191(2.10%)：60186(1.92%)：60160(1.88%)：60192(1.81%)：60141(1.78%)：60144(1.72%)』『Octet特徵共12個：40(93.45%)：152(4.00%)：80(1.53%)』『Packet特徵共4個：1(93.69%)：3(4.01%)：2(2.16%)』
  - 本IP開始異常時間已超過1日0時0分，其中100%時間超過告警標準，最近已持續1日0時0分超過告警標準，本異常追蹤系列可＜按此＞查詢
  - 對 50221 個 IP 位址連線
  - Protocol種類：2種
    - TCP：391938個Flows（100.00%）
  - 攻擊Port：181個
    - Port 60151：9506個Flows（2.43%）
    - Port 60152：9398個Flows（2.40%）
    - Port 60145：9352個Flows（2.39%）
    - Port 60142：8615個Flows（2.20%）
    - Port 60191：8237個Flows（2.10%）
    - Port 60186：7518個Flows（1.92%）
    - Port 60160：7382個Flows（1.88%）
    - Port 60192：7095個Flows（1.81%）
    - Port 60141：6989個Flows（1.78%）
    - Port 60144：6737個Flows（1.72%）
  - Octet Per Flow 特徵：12種
    - 40 Bytes：366253個Flows（93.45%）
    - 152 Bytes：15664個Flows（4.00%）
    - 80 Bytes：5998個Flows（1.53%）
  - Packets Per Flow 特徵：4種
    - 1 Packets：367189個Flows（93.69%）
    - 3 Packets：15720個Flows（4.01%）
    - 2 Packets：8473個Flows（2.16%）
  - 詳細數據
  - 地理資訊
    - 國碼：CN
    - 城市：Dalian
    - 經緯度： 121.6022, 38.9122
  - Flow 流過的 Router 與 Interface，從多至少排序
- 31.192.105.26 (Attacker) 2017/09/16 週六 00:27:02.124
- 199.48.164.35 (Attacker) 2017/09/16 週六 00:27:02.124
  - DocumentID：199.48.164.35_1505492822124
  - 異常超標：『五分鐘內連線不同IP數高達36,817個』
  - 主要特徵：『攻擊協定：UDP（100.00%）』『攻擊應用埠：5060（100.00%）』
  - 資訊摘要：『使用協定共1個：UDP(100.00%)』『目的Port共1個：5060(100.00%)』『Octet特徵共79個：435(27.58%)：434(23.22%)：436(19.78%)：433(14.13%)：432(7.12%)：437(3.38%)：431(2.86%)：430(1.08%)』『Packet特徵共23個：1(99.66%)』
  - 本IP開始異常時間已超過0日0時30分，其中66%時間超過告警標準，最近已持續0日0時10分超過告警標準，本異常追蹤系列可＜按此＞查詢
  - 對 36817 個 IP 位址連線
  - Protocol種類：1種
    - UDP：67402個Flows（100.00%）
  - 攻擊Port：1個
    - Port 5060：67402個Flows（100.00%）
  - Octet Per Flow 特徵：79種
    - 435 Bytes：18591個Flows（27.58%）
    - 434 Bytes：15651個Flows（23.22%）
    - 436 Bytes：13335個Flows（19.78%）
    - 433 Bytes：9522個Flows（14.13%）
    - 432 Bytes：4797個Flows（7.12%）
    - 437 Bytes：2276個Flows（3.38%）
    - 431 Bytes：1931個Flows（2.86%）
    - 430 Bytes：728個Flows（1.08%）
  - Packets Per Flow 特徵：23種
    - 1 Packets：67175個Flows（99.66%）
  - 詳細數據
  - 地理資訊
    - 國碼：US
    - 城市：Jacksonville
    - 經緯度： -81.6516, 30.3304
  - Flow 流過的 Router 與 Interface，從多至少排序

Copyright © 2017 國家實驗研究院國家高速網路與計算中心. All rights reserved.

告警通報服務

NARLabs

- TWAREN連線單位皆有IP範圍資料，系統可依據異常者IP判斷組織單位，自動通報該單位聯絡窗口，或由NOC值班人員進行通知。
- TANet學校單位可根據WHOIS資料判斷異常者單位。
- Fake Source IP 異常攻擊者無法根據IP判斷來源學校單位，需針對學校骨幹連接埠做異常偵測才行，因NOC目前計算資源有限，無法服務所有單位。

集思廣益

NARLabs

- 告警信通報頻率探討
  - 目前：30分/1小時/6小時/1天，可修改設定
  - 移除追蹤之時間(目前30分)與移除通報
  - 其他告警信運作方式?
- 其他通報方式?
  - 輔以NOC值班人員電話通報?
- 臨界值
  - 多嚴重才需要告警? 各家忍受程度不同

NARLabs

Q&A