治科資訊公司(Curelan)Flowviewer FM-800A
網路異常行為偵測系統: 1Gbps throughput
The professional security solution provider

流量分析與限額管控零時差

產品概述：

Flowviewer FM-800A技術服務核心，其核心技術可針對網路流量進行分析，透過本公司自行開發的演算法分析找出異常流量，偵測到異常流量時，可使用Email通知管理者。採用行為模式(不採用特徵碼方式)有效判斷，無須更新特徵碼可用於偵測未知特徵碼的攻擊與入侵行為，提供多樣入侵與攻擊報表，所提供之網路服務流量報表具備動態調整時間區段來查詢每個IP，並可追蹤每個IP之流入/流出位址，所以可提供疑似犯罪記錄給電信警察。

駭客入侵之途徑

- 疑似SSH密碼猜測攻擊。
- 疑似RDP攻擊。
- 未知之微軟作業系統漏洞及PHP,C++資料庫漏洞，此種方式之途徑連原廠都不知道他們程式漏洞在那兒，這是高段駭客手法所以全世界對此途徑都是無解，只能等原廠發現自動更新漏洞。

※ 解決方案：Flowviewer FM-800A有提供SSH及RDP入侵偵測及自動阻斷功能。

駭客透過非SSH及RDP之途徑入侵後之補救方式

- 如果駭客不是從這二種方式入侵而產生攻擊事件是否有補救方式？
- 在此提出目前所知道的駭客攻擊手法：
  - UDP Flood Attacks：產生大量偽造UDP封包去惡意攻擊想要攻擊的IP，讓此IP達到癱瘓不能正常運作，此IP可以是Http File Server、Web Server、DNS Server等。
  - DOS Relay Attacks：透過跳板產生大量TCP封包去攻擊想要攻擊的IP，此IP可以是Http File Server、Web Server、DNS Server等。

※ 解決方案：Flowviewer FM-800A有提供此二種攻擊偵測及自動阻斷功能。

Flowviewer FM-800A 產品敘述：

1、系統支援動態查詢流量報表功能。
2、具備針對整體網路進行監看功能，方便網路服務分析。
3、支援Behavior(行為模式)方式來進行IP網路封包的檢測。
4、支援role based 之設定管理方式。
5、具備IPv4/IPv6雙協定(Dual Stack)技術，同時提供IPv4與IPv6處理能力。

產品功能特色

- **Netflow 或 sFlow 流量報表：**
  支援接收Netflow 或 sFlow，並且可以透過動態查詢追蹤網路犯罪。
- **動態查詢功能：**
  可任意調整時間區段來查詢每個IP間的聯繫。
- **疑似DNS攻擊報表：**
  可偵測出透過此通訊協定攻擊的IP。
- **流量配額管理及即時流量監控：**
  可以設定每一個IP可使用的網路流量大小。
- **蠕蟲偵測(NBAD)：**
  採用網路行為異常偵測技術，不需IPS設備(Intrusion Prevention System)做病毒碼辨識。
- **疑似SSH密碼猜測攻擊報表：**
  此功能可以偵測出駭客欲透過此通訊協定入侵的是哪個來源IP。
- **疑似RDP攻擊報表：**
  Remote Desktop Protocol(RDP)是一種由Microsoft所使用的遠端桌面通訊協定，可以藉此提供使用者遠端操控另一台電腦上的功能。此功能可以偵測出駭客欲透過此通訊協定入侵的是哪個來源IP。
- **疑似UDP Flood攻擊報表：**
  UDP Flood攻擊是一種用透過傳送大量UDP封包的阻斷式攻擊。此功能可以偵測出哪些IP已受到駭客控制而去攻擊別人。
- **疑似DOS跳板攻擊報表：**
  透過跳板產生大量TCP封包去攻擊想要攻擊的IP，此IP可以是Http File Server、Web Server、DNS Server等。此功能可以偵測出哪些IP已受到駭客控制而去攻擊別人。

採購資訊

廠牌：Curelan
軟體名稱：FM-800A

Curelan Technology Co., Ltd. http://www.curelan.com blue@curelan.com TEL：886-73115186

The professional security solution provider