Enhancing Security through Continuous Threat Assessment

NetApe

網路封包解析與 Log 解析軟體

NSGUARD
NSGUARD Technology, Inc.
捷睿智能股份有限公司

簡介

由 App/網站角度進行分析的專業網路封包鑑識工具。不只辨識常見網路協定，更支援超過三百種以上通訊或社交 app(表列如附件所示)，並定期更新。整合公開情資網站最新資訊及 Wireshark，提供更全面化資訊。另外，簡易且直覺的操作介面，為使用者省下熟悉如何操作工具的寶貴時間。

4G 行動網路帶動通訊 App 的蓬勃發展，通訊 App 豐富的多媒體影音訊息，加上其免費、方便性及通訊加密性，頓時成為時下最熱門的通訊方式。

各類 App 開發團隊水準良莠不齊，對於個資的保護與資訊加密的要求並不相同，往往因為疏忽或貪圖方便而導致資訊的外流。使用者可藉助 NetApe 來分析 App 的安全性，了解 App 是否有洩漏個資的可能性。另外一個問題是其隱密性容易成為大量犯罪者隱匿不法的溫床，執法機關可使用 NetApe 來分析疑犯網路行為與證據蒐集。此外惡意程式的網路行為有其特定的模式，資安分析人員可藉由 NetApe 發現異常的網路行為進而找出隱藏在網路中各類惡意程式。

封包是構成網路世界的最基本元素，所有網路問題皆來自於此，在封包層面上瞭解越多，越能掌控網路世界的瞬息萬變。使用者僅需將擷取的網路封包檔案交由 NetApe 進行解析，即能掌握網路世界的脈動與蛛絲馬跡。

功能說明

- 概觀 (統計資訊)
  - 服務伺服器連線統計 – 用以統計使用者與各服務伺服器連線數，可得知使用者對於各類服務的需求程度
  - HTTP 用戶代理連線統計 – 統計 HTTP user-agent 連線資訊，可從中得知各種瀏覽器與設備使用的頻率
  - 網域名稱系統使用統計 – 透過 DNS 查詢網域名稱(Domain name)的 IP 次數統計

- HTTP 回應代碼統計 – HTTP 回應(response)的狀態碼(Http status code)統計，可從中察覺是否出現大量的不正常狀態碼

- 連線資訊 (Conversation)
  - 依據 5-tuple (Source IP, Destination IP, Source Port, Destination Port, Protocol)資訊將 IPv4 或 IPv6 的封包合併成一條一條的連線(Connection)，並針對連線內的封包進行深層封包檢視(DPI)
- 網域名稱系統 (DNS)
  - 從 DNS 查詢的歷程看出目標經常瀏覽的網站或使用的 Mobile 有哪些，以及在甚麼時間使用這些服務
- 超文字傳輸協定 (HTTP)
  - 條列所有的內容符合 HTTP 通訊協定的連線，並將 Header 中重要的欄位解析出來，包含 請求方法(Method)、目的地主機名(Hostname)稱、請求 URI、用戶代理(User-agent)、狀態碼(Status Code)等
- 網路電話(VoIP)
  - 將 SIP/RTP VoIP 電話封包解譯後彙整於此
- 圖片 (Picture)
  - 將封包中所有被解譯還原成圖片的檔案以使用者可以快速瀏覽的方式呈現
  - 封包中的圖片來源通常包含瀏覽網站上的圖片、Mobile App 的大頭貼、或者是照片
- 傳輸層安全協定 (SSL/TLS)
  - 目前許多網站與 Mobile App 都是使用 HTTPS 加密傳輸內容，雖然無法看到資料傳輸內容，但是還是可以分析這些加密連線的 IP、Domain Name、憑證內容、以及連線數量與次數等，得知目標經常瀏覽的網站或經常使用的 Mobile App。
- 文字 (Text)
  - 呈現解譯後的文字的資料。資料來源主要來於：HTTP, FTP, Web-Email 三種。
- 電子郵件 (Email)

- 可支援 SMTP、POP3、IMAP4 等通訊協協定解譯功能。可解譯電子郵件的標題、寄件人、收件人、發送時間、接收時間、內容、附件等重要資訊。

- 檔案 (File)
  - 所有被解譯出來的檔案都可以在這裡找到，包含圖片、Email 附件、FTP 傳輸檔案、HTML 網頁、影像、聲音或 VoIP 語音檔…等。
- 元素解析 (Element decoder)
  - 可利用正規表示式(regular expression)搜尋關鍵字詞，將封包中可能含有敏感資訊的內容，如使用者的經緯度或地址資訊…等找出來，並以表格方式呈現

應用場景

- 安全分析
  - APP 開發商往往為了縮短產品上市時間或是降低研發成本，加入第三方軟體來實現某些產品功能，如 GPS 定位功能、甚至是帳號密碼認證…等。
  - 利用內建的關鍵字查找或是自行定義的正規表示式(regular expression)搜尋，可分析該 APP 是否有洩漏個資的疑慮。
- 犯罪偵查
  - 能還原封包內未加密之圖片/電子郵件，使這類資訊有機會成為證據的數位資料
  - 觀察犯罪嫌疑人之封包中所含 APP 種類及操作時間長短，瀏覽網站歷程及地理位置等資訊，便能進行罪犯側寫 (offender profile ng)推敲該對象之性格喜好及作息模式，方便規劃之後追蹤策略，如高鐵訂票、Ubike、計程車、捷運或火車等，一旦該目標利用手機查詢交通班次、購買訂票或叫車，從封包分類就能有效縮小搜尋範圍。
- 惡意程式分析
  - 惡意程式泛指會破壞電腦正常運作的程式。
  - 可由如 DNS 封包的請求與回應、或是 SSL 安全性憑證…等網路連線行為、封包內容分析可以找出可能的惡意程式，並由連線紀錄找出受害的終端設備，進行損害控管。

系統需求

產品名稱	NetApe 封包解析軟體
硬體需求	● CPU: Intel® Core™ i5 以上 ● RAM: 8 GB 以上 ● HD: 500 GB 以上
軟體需求	● Microsoft Windows 7 Service Pack 1 (SP1) 64-bit ● Microsoft Windows 10 64-bit

NSGUARD

NSGUARD Technology, Inc.