資訊處
Office of Information Technology

資安事件宣導

使用TCPVIEW
找到網路異常連線

TCPView介紹

- TCPView是由微軟公司提供的圖形化小工具，可用於監看目前電腦網路連線情形。

- TCPView顯示程序名稱、連線IP位址、連線埠及連線狀態等訊息，並可進一步查詢程式安裝目錄及網域名稱註冊資訊，方便使用者判斷是否有異常連線，並提供結束程序功能。

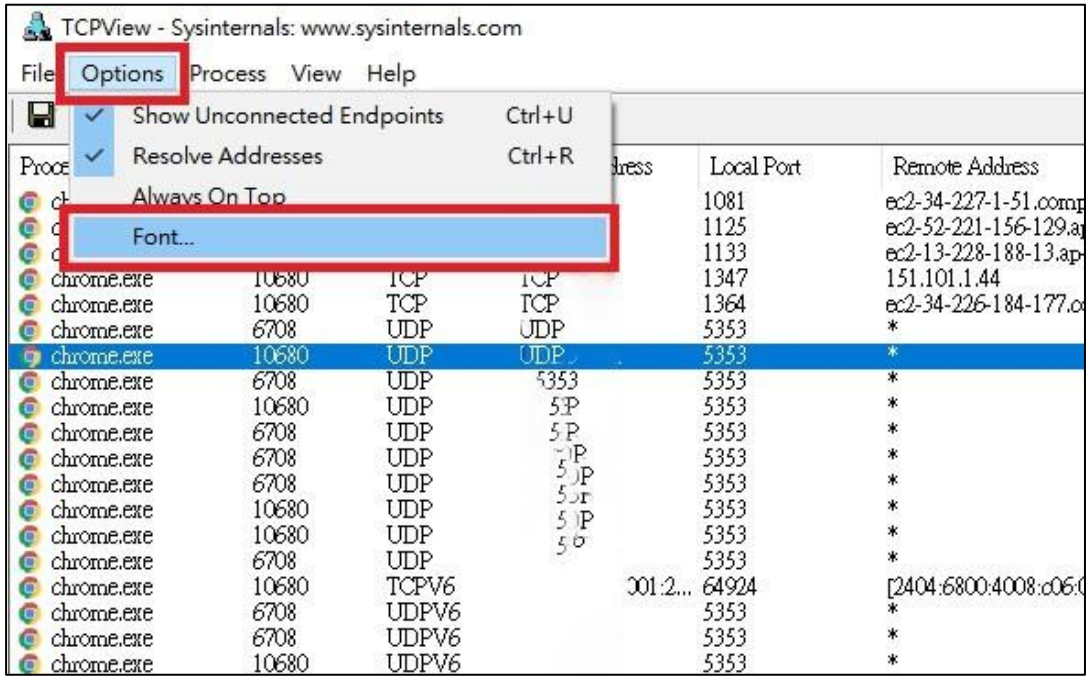
- TCPView免安裝，下載後解壓縮即可執行。

TCPView介面

- TCPView畫面如下，分為功能區及顯示區介紹。

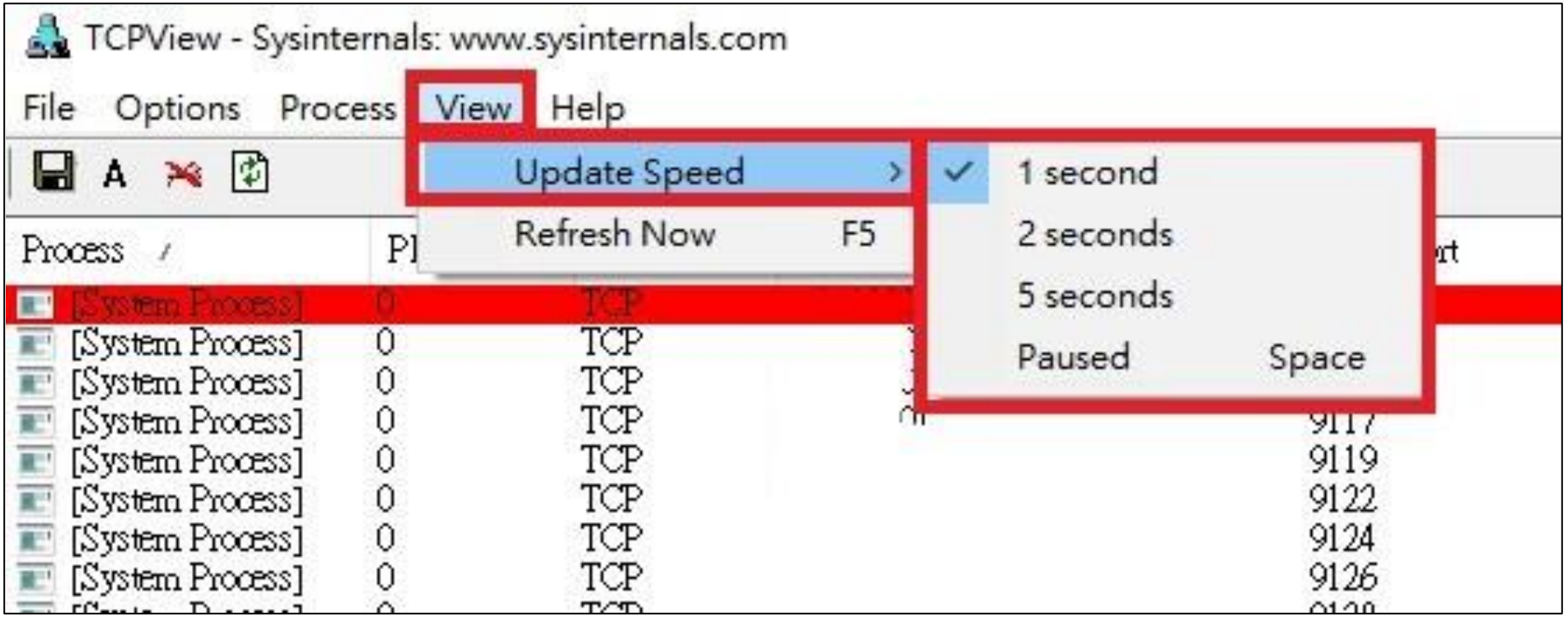
TCPView介面-功能區(1)

- 點選【Options->Font】，可調整顯示區字型大小



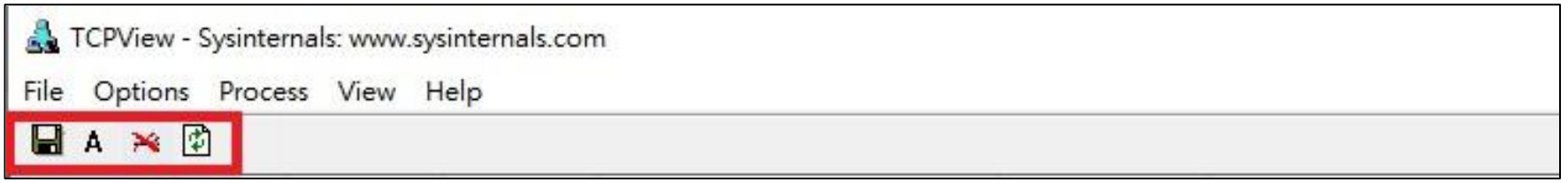
TCPView介面-功能區(2)

- 點選【View->Update Speed】可設定更新頻率或暫停更新，預設每秒更新。



TCPView介面-功能區(3)

- 常用功能區，從左到右功能如下：



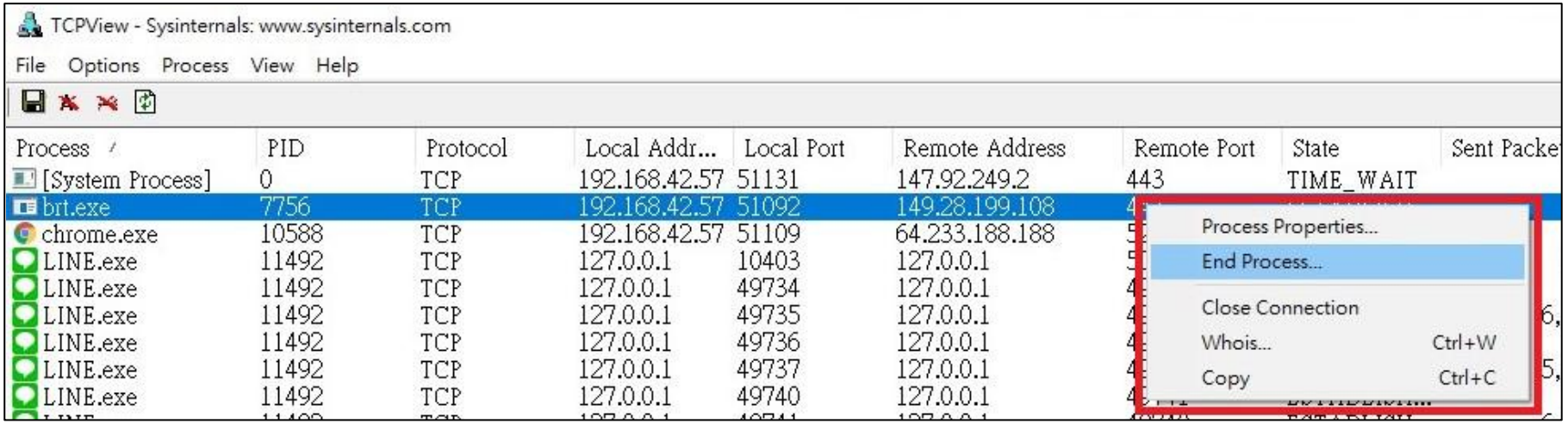
  - 將目前連線資訊另存為文字檔。
  - 切換連線位址及連線埠顯示方式
    - 連線位址預設是網域名稱，可改為IP位址。
    - 連線埠預設是服務，可改為埠號。
  - 預設顯示電腦所有程序，建議點選，改為僅顯示連線中的程序。
  - 重新整理連線資訊。

TCPView介面-顯示區(1)

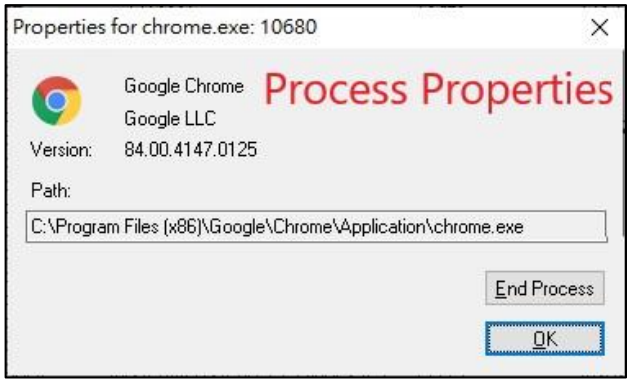
- 顯示區列出目前電腦網路連線狀態，查找惡意程式時主要參考下列欄位：
  - Process：條列連線中的程序名稱。
  - Remote Address：該筆連線的目的網域名稱或IP位址，localhost(127.0.0.1)代表本機。
  - Remote Port：該筆連線的目的連線埠，常見的連線埠如下：
    - 瀏覽網頁：http(80)、https(443)。
    - 電子郵件：POP3(110)、POP3S(995)、SMTP(25/587)、SMTPS(465)、IMAP(143)、IMAPS(993)等。

TCPView介面-顯示區(2)

- 在各筆連線點選滑鼠右鍵後，常用功能如下：

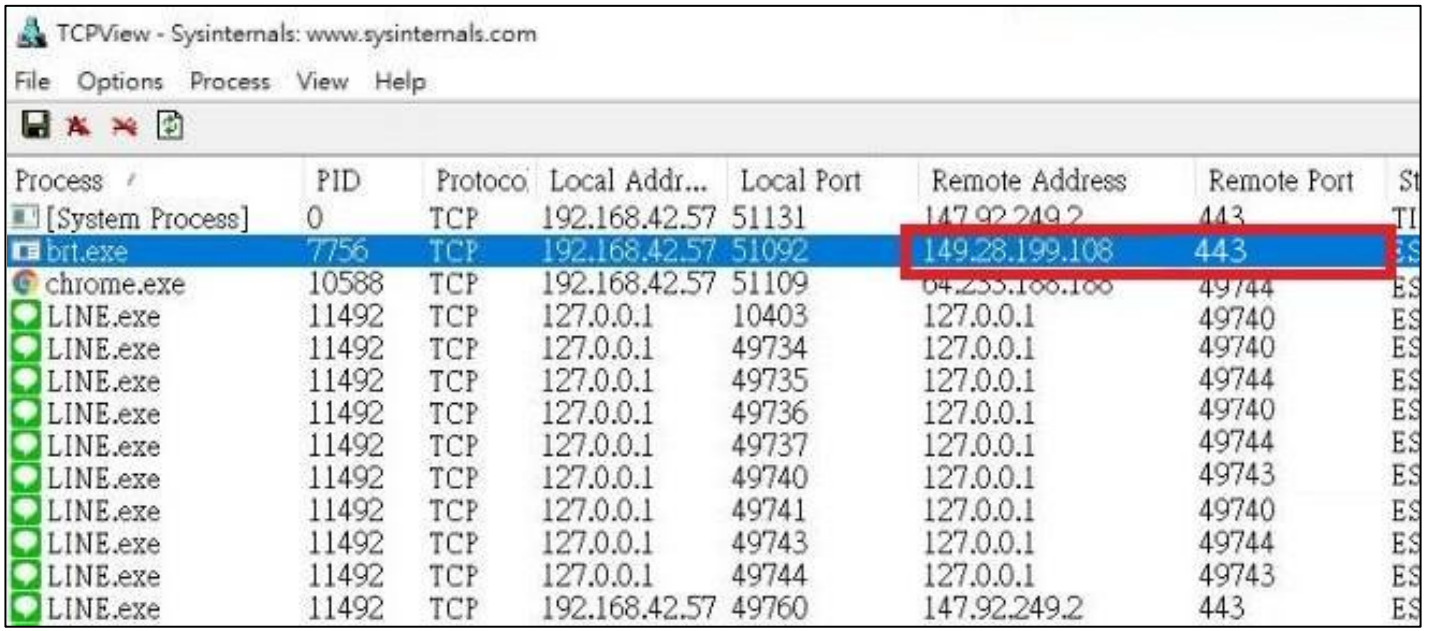


- Process Properties：可查看該程序使用的程式資訊及安裝目錄。
- End Process：判斷屬異常連線，可使用此功能終止程序。
- Whois：可查詢whois註冊資訊。



如何找出異常連線(1)

- 依據收到的斷線通知提供的IP及連線埠資訊，比對連線中程序的Remote Address及Remote Port
  - 如本校常見的Ohsoft軟體暗藏的挖礦程式，通常是連線149.28.199.108的443port。



Process	PID	Protoco	Local Addr...	Local Port	Remote Address	Remote Port	St
[System Process]	0	TCP	192.168.42.57	51131	147.92.249.2	443	TI
brt.exe	7756	TCP	192.168.42.57	51092	149.28.199.108	443	ES
chrome.exe	10588	TCP	192.168.42.57	51109	64.233.188.188	49744	ES
LINE.exe	11492	TCP	127.0.0.1	10403	127.0.0.1	49740	ES
LINE.exe	11492	TCP	127.0.0.1	49734	127.0.0.1	49740	ES
LINE.exe	11492	TCP	127.0.0.1	49735	127.0.0.1	49744	ES
LINE.exe	11492	TCP	127.0.0.1	49736	127.0.0.1	49740	ES
LINE.exe	11492	TCP	127.0.0.1	49737	127.0.0.1	49744	ES
LINE.exe	11492	TCP	127.0.0.1	49740	127.0.0.1	49743	ES
LINE.exe	11492	TCP	127.0.0.1	49741	127.0.0.1	49740	ES
LINE.exe	11492	TCP	127.0.0.1	49743	127.0.0.1	49744	ES
LINE.exe	11492	TCP	127.0.0.1	49744	127.0.0.1	49743	ES
LINE.exe	11492	TCP	192.168.42.57	49760	147.92.249.2	443	ES

如何找出異常連線(2)

- 依程序名稱或連線埠判斷，不是熟悉的程式名稱(如：brt.exe)或常見連線埠(如：3333、7777)，可能是惡意程式，可嘗試以程序名稱搜尋程式資訊及處理方式。

小結

- TCPView顯示電腦目前連線狀態，如查無異常連線，不代表無惡意程式，可能是目前該惡意程式沒有活動，所以未建立連線。
  - 如查無異常連線，但電腦明顯變慢或有其他異常情形，建議可再搭配微軟提供之小工具Process Explorer檢查執行中程序。

- 找到惡意程式後，可透過【Process Properties】查看程式安裝目錄，並建議先搜尋惡意軟體移除方式，確保問題徹底解決。

資料參考來源

- Microsoft Docs
  - https://docs.microsoft.com/en-us/sysinternals/downloads/tcpview
- TCPView下載網址
  - https://download.sysinternals.com/files/TCPView.zip
- iThome-搶救Windows疑難雜症Windows Sysinternals Suite
  - https://www.ithome.com.tw/node/44794