# 如何快速檢測是否有潛伏的惡意程式？


https://www.seekinfo.com.tw/
更新日期：2016/10/21

有時候，客戶會懷疑電腦是否有中毒，但防毒軟體未發現？或者公司收到某些單位的通知，對外連線有異常的情形？(這類的事件是否為真，在此略過不談，不是本文的重點。) 可是又不知道是哪一部電腦有問題？是否有什麼快速的方法可以進行檢測？如果您有這方面的需求，本文提供一個解決方案。

首先，很多人會認為那就用防毒軟體做一次徹底掃描？這通常是沒用的。試想一下，在有安裝防毒軟體的電腦，啟動之後，防毒軟體就進行持續性的監控，只要有檔案 I/O 發生，或者應用程式啟動，都會先被防毒軟體檢查一遍。如果某個病毒可以啟動，表示防毒軟體無法偵測到，那重覆再做一次掃描，會改變結果嗎？

那有更好的方法嗎？有的，接下來就說明我們的方法..

ESET 有一個工具程式 - SysInspector，如果電腦有安裝 ESET 防毒軟體(EEA、EES、EFSW…)，就有這個工具程式。SysInspector 的功能是收集電腦裡面的資訊，包括重要的檔案，像是執行中的程式、開機會啟動的程式、服務、驅動程式… 從 SysInspector 的報告，就可以分析目前電腦裡面是否有可疑的程式在執行。

ESET SysInspector 是免費的，如果您不是 ESET 用戶，也可以直接到 ESET 官方網站下載。

那要如何分析？用人工看是一個方法，可是除非經驗老到，否則一般人大概很難看出端倪，況且這樣的效率不高。如果用全球各地五十多套防毒軟體來掃描，這樣總是能將病毒抓出來吧！Google 旗下有一家公司叫 VirusTotal，它使用五十幾家的防毒軟體來掃描檔案，所以我們只要將 SysInspector 的報告加以分析，再比對 VirusTotal 上的資料，就可以得出結果。

但這裡有二個問題：

- 公司的電腦那麼多，要怎麼取得所有電腦的 SysInspector 報告？
- SysInspector 報告裡面所列出的檔案那麼多(估計一部電腦平均大概有 2000 ~ 3000 個檔案)，一個個到 VirusTotal 查，那可是會累死人。

很簡單，席克資訊提供**免費**的服務給有這種需求的 Premium 客戶..

如果您有使用 ERA Server v6.x 管理全公司的電腦，要取得全公司的 SysInspector 報告就非常容易了。從 Web Console 上，新增一個 **SysInspector 防護記錄要求** 的用戶端工作，然後指派給所有的電腦，建議不要設定立即執行，使用單次排程，指定執行的時間，並設定隨機延遲間隔，這樣才不會全公司的電腦全擠在一起上傳報告到 ERA Server。(**提醒您：如果沒有需要，不要做這個動作，因為大量的 SysInspector 報告，會使 SQL 資料庫變大許多，徒增備份的負擔。**)

當 SysInspector 的報告送回 ERA Server 之後，再執行我們提供的程式，即可自動將所有 SysInspector 的報告上傳到我們公司的伺服器。簡單輕鬆完成第一項工具。

當我們收到檔案後，我們有寫了一套程式，可以幫您做分析，如果發現檔案有被其他防毒軟體公司偵測是病毒，會加以記錄。最後，您就可以確認全公司電腦裡的檔案，被哪些防毒軟體認定是病毒。不過在此強調一下，防毒軟體有可能誤判，所以當您看到某個檔案被其他防毒軟體公司判定是病毒，請冷靜思考一下，是真的是病毒？或者只是誤判？

某些執行細節在此省略，實際有需要的客戶，我們會再和您討論執行的步驟。

如果對本文的內容有疑問，請聯絡**席克資訊 TEL: 04-22132276**