臺灣大學計資中心網路組
北區學術資訊安全維運中心

資訊安全技術報告

看 CSI : CYBER 學電腦鑑識

臺灣大學計資中心網路組
北區學術資訊安全維運中心

摘要

CSI 犯罪現場為美國老牌刑事鑑識影集，影集內容描述一組刑事鑑識科學家調查傳統刑案的故事，有鑑於今日犯罪型態由實體轉為虛擬數位型態，美國 CBS 於今年推出專門講述網路犯罪與電腦鑑識之系列影集，名為 CSI : CYBER(網路犯罪)。

ASOC 依據相關劇情，撰寫實務之電腦鑑識技術，讓讀者更易瞭解實際電腦鑑識技術，本次推出為如何鑑識電腦內勒索軟體 CryptoLocker，讀者可透過本報告，逐步分析與發現 CryptoLocker 在電腦內之活動

案情簡介

許多集的 CSI : CYBER 都會看到受害者電腦遭到惡意程式入侵，而探員在調查時，採用數位鑑識方法，快速找到惡意程式，並完成破案，而現實生活中，實務的鑑識方法為何?本篇文章將說明數個能夠輕易取得的工具，觀察電腦中已知/未知程序的運作與行為模式，分析出潛藏在電腦中的惡意程式。

鑑識程式簡介

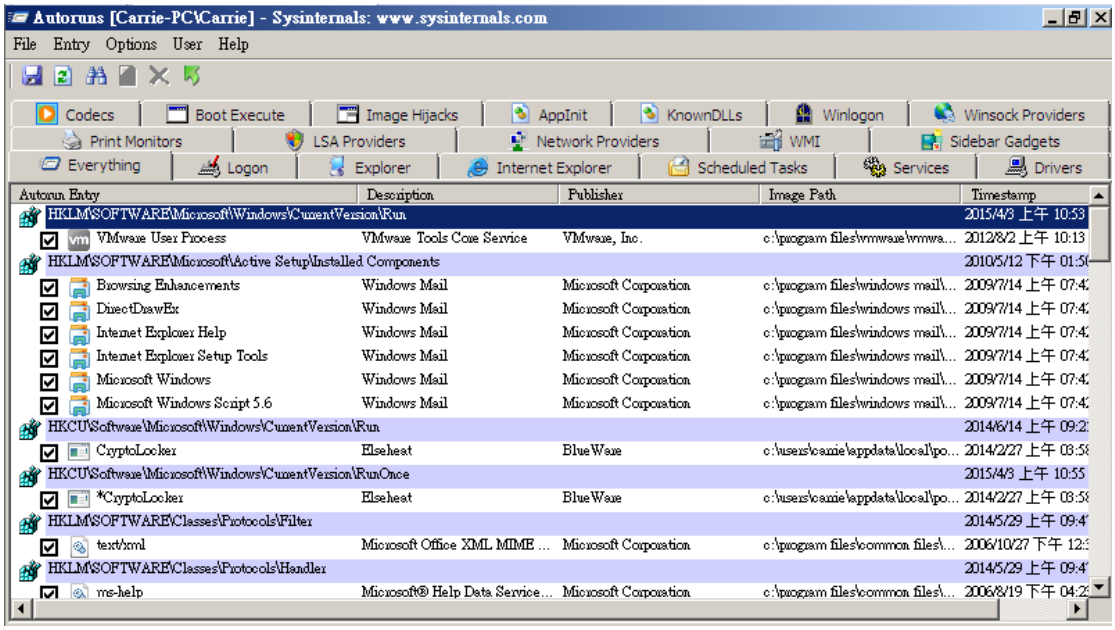
進行惡意程式的分析、鑑識時，我們需要用到數個工具來觀測與紀錄惡意程式行為。本篇將會介紹三個工具，並以一個實際案例來說明作用方式。

1. Autoruns
2. Process Explorer
3. Process Monitor

透過下列網址能夠下載到這些工具：
https://technet.microsoft.com/en-us/sysinternals/bb545027

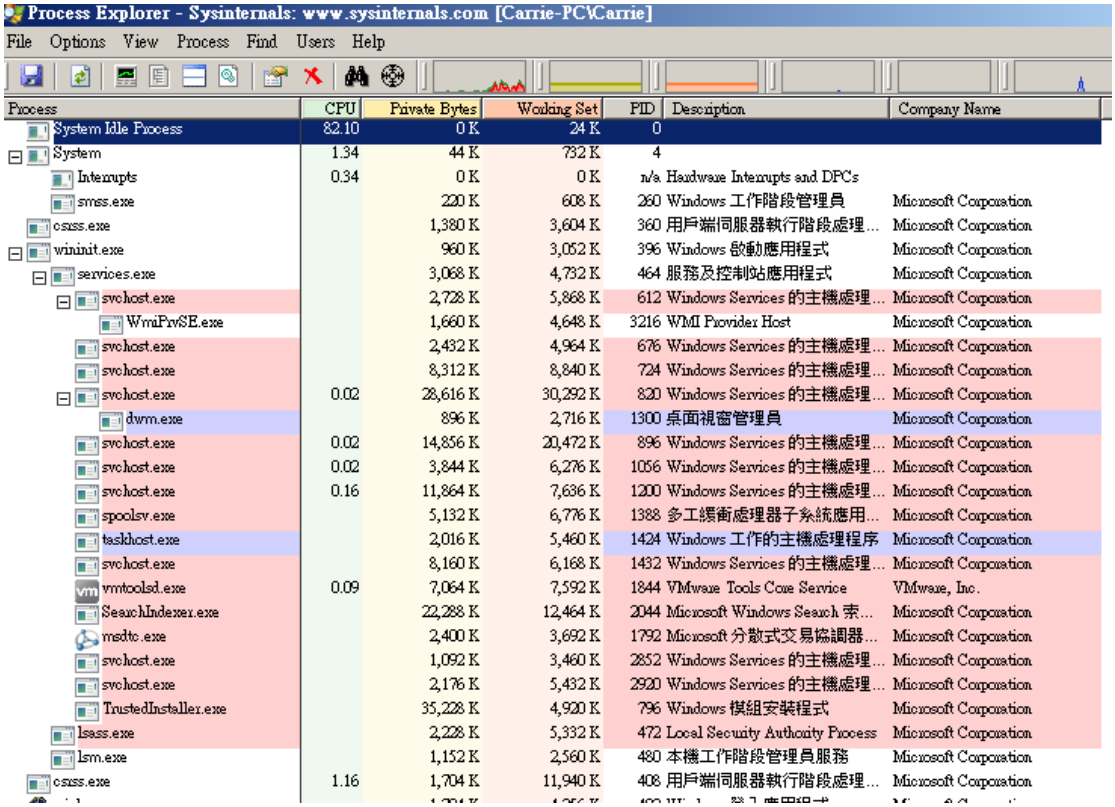
Autoruns 簡介

惡意程式必須被執行，才能發揮其功能，故多數惡意程式，會於電腦開機時，利用作業系統的 Autorun 功能，自動將惡意程式帶起，Sysinternals Autoruns 工具可協助我們查找此區之細部設定。

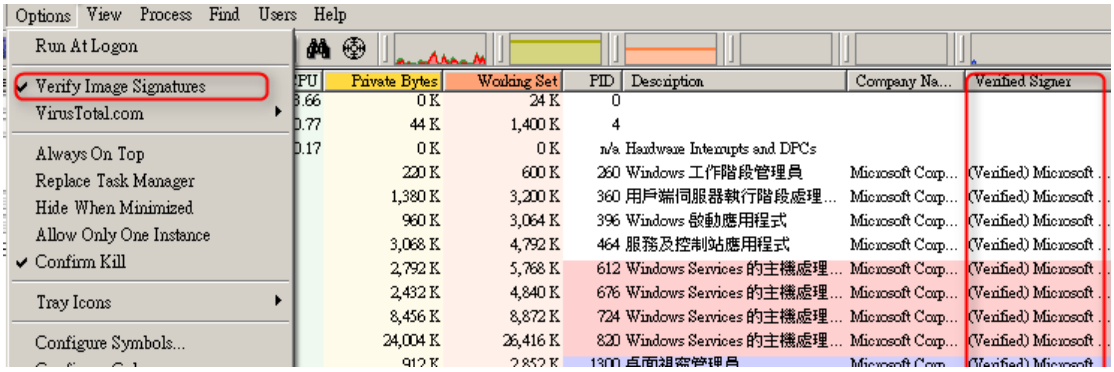


Process Explorer 簡介

Process Explorer 能快速檢視程序中的 Parent/Children 關係，最多的應用方式還是屬於管理層面。若是以系統管理員權限開啟程式，它能傳送訊息至其他使用者帳戶，甚至登入/登出/Remote 該帳戶。對程序本身能夠提高/降低優先度、凍結、關閉單一程序或整個關連程序，以及以系統管理員/受限制的帳戶來執行新程序。

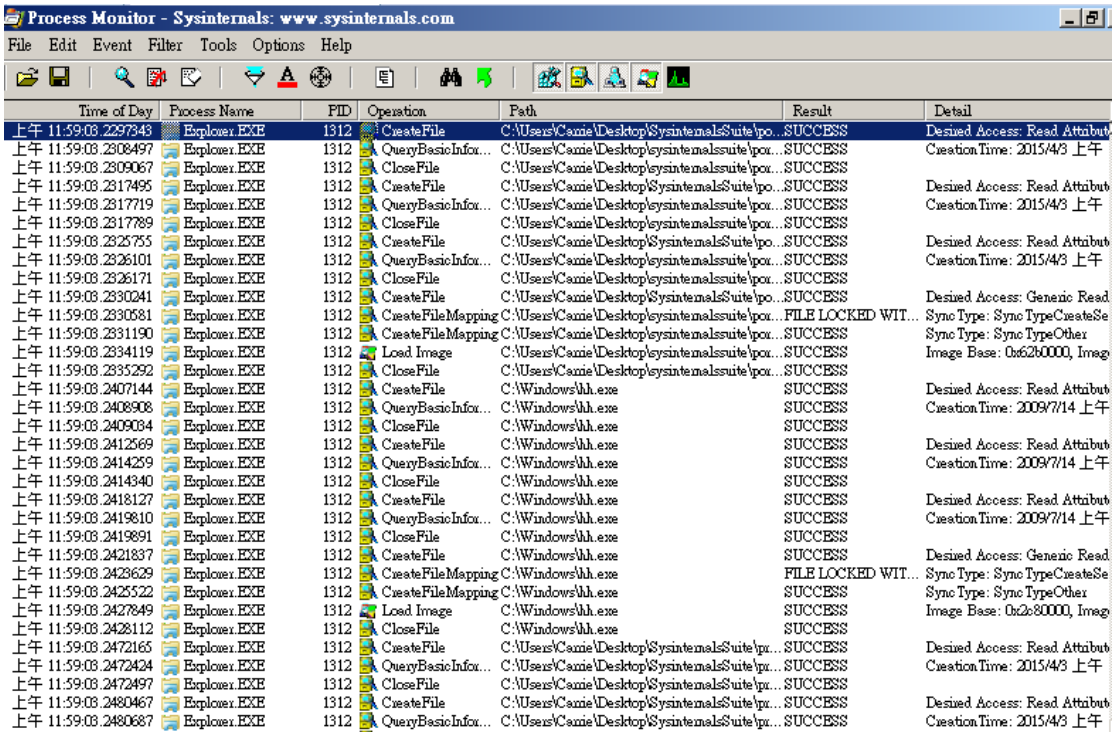


具有檢測簽章的功能，作為初步的惡意程式判斷是非常好用的功能



Process Monitor 簡介

Process Monitor 能夠記錄應用程式在電腦中的行為。電腦中的程序繁多，在預設檢視的情況下會看到所有運作中程式的行為，記錄的精確度有至百萬分之一秒。

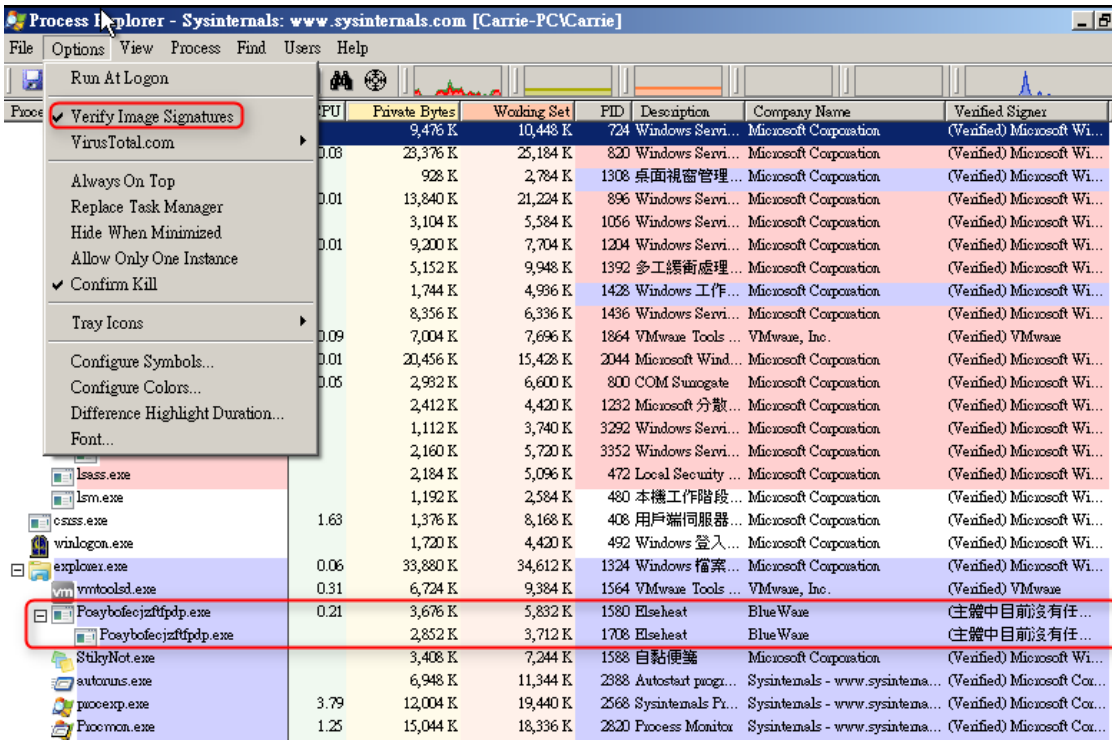


案例分析 – CryptoLocker 登錄檔活動

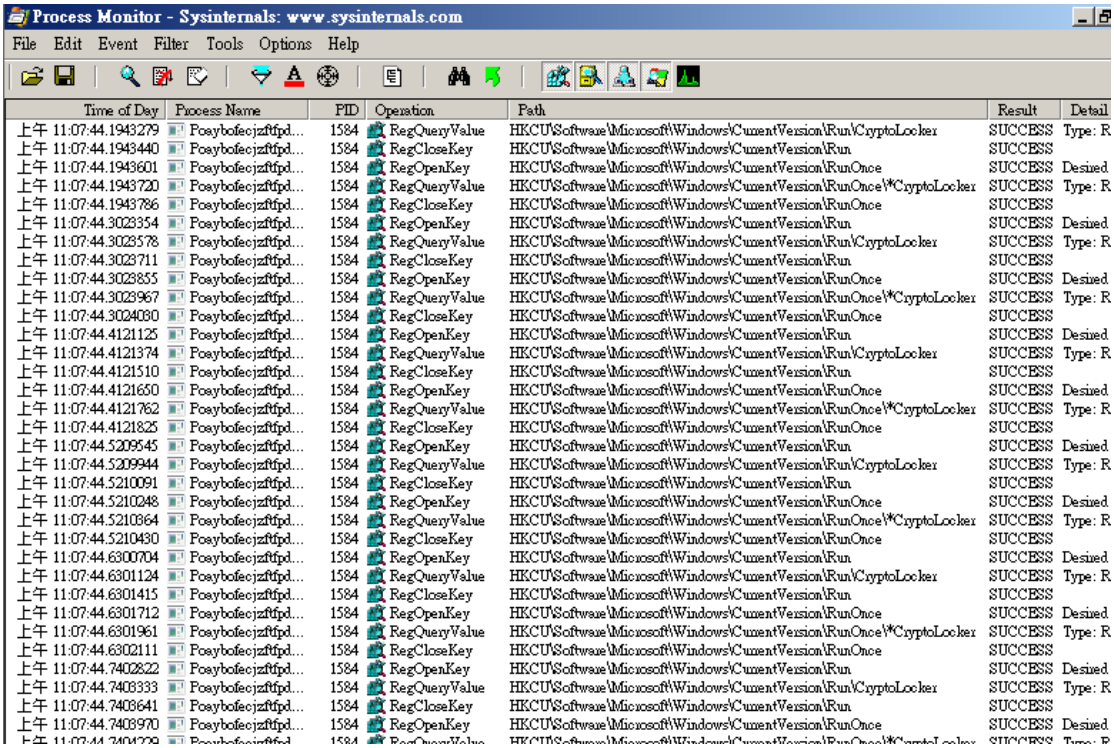
2013 年下半年出現的 CryptoLocker 是一種惡意程式，其最大特性會將使用者硬碟加密，並勒索使用者，若使用者不支付贖金，遭加密的硬碟資料無法解開，對硬碟內有重要資料的使用者而言影響頗巨，而 CryptoLocker 主要鎖定 Microsoft Windows 作業系統為攻擊目標。

此範例主要的用意在於以實際案例展示各個工具的搭配使用，以分析 CryptoLocker 惡意程式。

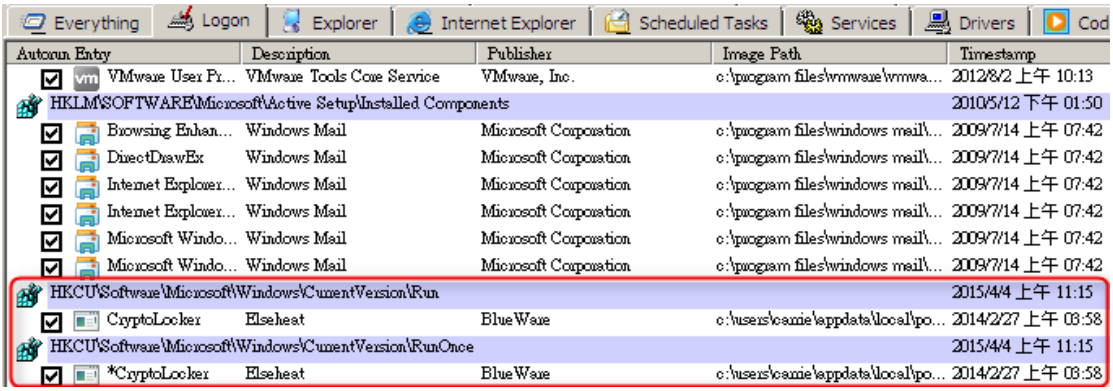
使用 Process Explorer 檢查目前運作程序，可發現一個特殊名稱的程式，針對此程序使用 Verify Image Signatures，但沒有任何簽章被發現，此程序十分可疑。



此可疑程序亦對兩個登錄檔持續監測，目的為確保開機後，該可疑程序能持續存活於作業系統，另可發現 CryptoLocker 此關鍵字。



接下來採用 Autoruns 工具觀測 Logon 設定，此設定為作業系統開機時會帶起的程序，惡意程式設計時，為避免重新開機時無法啟用，多會刻意在此處設定，下圖出現兩個由可疑程式所建立的登錄值，手動刪除並重新整理後，兩個登錄值出現，再次刪除，又再出現，惡意程式不斷監控並確保這兩個登錄值存在，使自己能於系統開啟時執行，至此我們已可確認此電腦遭 CryptoLocker 感染。



總結

本文件簡介 Sysinternals 三項知名工具 AutorunsProcess、ExplorerProcess、Process Monitor 並說明透過這三項工具，如何發現電腦中是否存在 CryptoLocker 惡意程式，透過這樣的解說，相信讀者應能瞭解基礎數位鑑識概念。

CSI : CYBER 影集中，幹員採用數位鑑識技術快速找到受害者電腦內惡意程式，而現實的數位鑑識環境，有許多干擾因素，如證物無法取得，或是證物遭破壞等因素，而能否快速找到惡意程式，分析人員經驗與素質，直接影響鑑識工作品質。

孫子兵法曰：「知彼知己，百戰不殆。」，分析者對駭客手法與作業系統知識瞭解越多，越能精準與快速分析，而這也是每位數位鑑識人員應平日充實的重點。