



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。

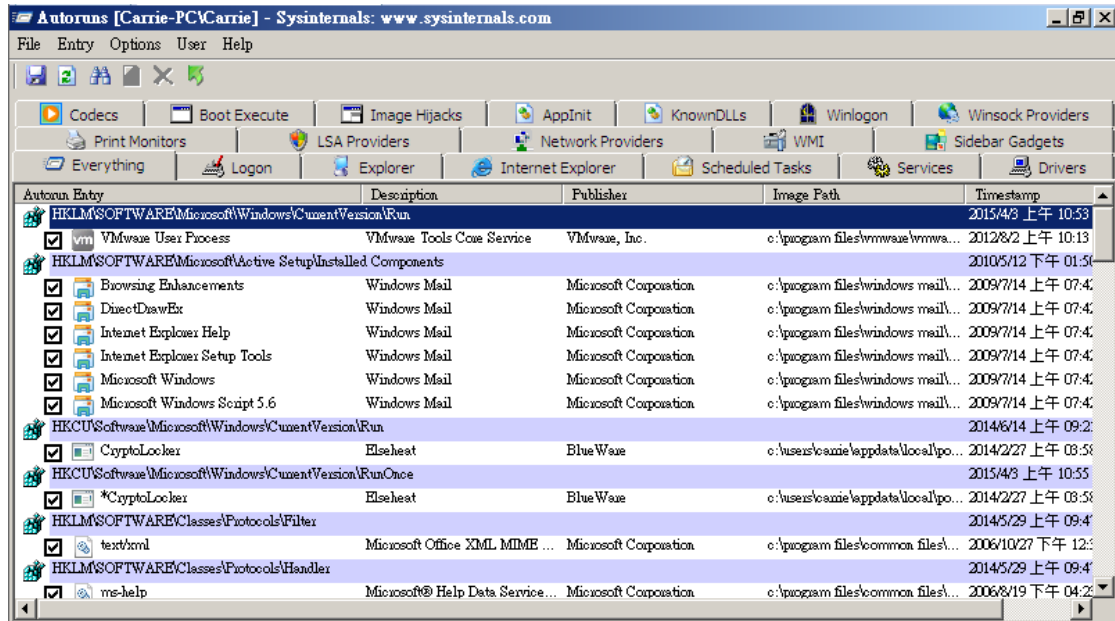
1. Autoruns
2. Process Explorer
3. Process Monitor

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。

| Process | CPU | Private Bytes | Working Set | PID | Description | Company Name |
|----------------------|-------|---------------|-------------|------|----------------------------------|-----------------------|
| System Idle Process | 82.10 | 0 K | 24 K | 0 | | |
| System | 1.34 | 44 K | 732 K | 4 | | |
| Interrupts | 0.34 | 0 K | 0 K | n/a | Hardware Interrupts and DPCs | |
| smss.exe | | 220 K | 608 K | 260 | Windows 工作階段管理員 | Microsoft Corporation |
| csrss.exe | | 1,380 K | 3,604 K | 360 | 用戶端伺服器執行階段處理... | Microsoft Corporation |
| wininit.exe | | 960 K | 3,052 K | 396 | Windows 啟動應用程式 | Microsoft Corporation |
| services.exe | | 3,068 K | 4,732 K | 464 | 服務及控制站應用程式 | Microsoft Corporation |
| svchost.exe | | 2,728 K | 5,868 K | 612 | Windows Services 的主機處理... | Microsoft Corporation |
| WmiPrvSE.exe | | 1,660 K | 4,648 K | 3216 | WMI Provider Host | Microsoft Corporation |
| svchost.exe | | 2,432 K | 4,964 K | 676 | Windows Services 的主機處理... | Microsoft Corporation |
| svchost.exe | | 8,312 K | 8,840 K | 724 | Windows Services 的主機處理... | Microsoft Corporation |
| svchost.exe | 0.02 | 28,616 K | 30,292 K | 820 | Windows Services 的主機處理... | Microsoft Corporation |
| dwm.exe | | 896 K | 2,716 K | 1300 | 桌面視窗管理員 | Microsoft Corporation |
| svchost.exe | 0.02 | 14,856 K | 20,472 K | 896 | Windows Services 的主機處理... | Microsoft Corporation |
| svchost.exe | 0.02 | 3,844 K | 6,276 K | 1056 | Windows Services 的主機處理... | Microsoft Corporation |
| svchost.exe | 0.16 | 11,864 K | 7,636 K | 1200 | Windows Services 的主機處理... | Microsoft Corporation |
| spoolsv.exe | | 5,132 K | 6,776 K | 1388 | 多工緩衝處理器子系統應用... | Microsoft Corporation |
| taskhost.exe | | 2,016 K | 5,460 K | 1424 | Windows 工作的主機處理程序 | Microsoft Corporation |
| svchost.exe | | 8,160 K | 6,168 K | 1432 | Windows Services 的主機處理... | Microsoft Corporation |
| vmtoolsd.exe | 0.09 | 7,064 K | 7,592 K | 1844 | VMware Tools Core Service | VMware, Inc. |
| SearchIndexer.exe | | 22,288 K | 12,464 K | 2044 | Microsoft Windows Search... | Microsoft Corporation |
| medtc.exe | | 2,400 K | 3,692 K | 1792 | Microsoft 分散式交易協調器... | Microsoft Corporation |
| svchost.exe | | 1,092 K | 3,460 K | 2852 | Windows Services 的主機處理... | Microsoft Corporation |
| svchost.exe | | 2,176 K | 5,432 K | 2920 | Windows Services 的主機處理... | Microsoft Corporation |
| TrustedInstaller.exe | | 35,228 K | 4,920 K | 796 | Windows 模組安裝程式 | Microsoft Corporation |
| lsass.exe | | 2,228 K | 5,332 K | 472 | Local Security Authority Process | Microsoft Corporation |
| lsmd.exe | | 1,152 K | 2,560 K | 480 | 本機工作階段管理員服務 | Microsoft Corporation |
| csrss.exe | 1.16 | 1,704 K | 11,940 K | 408 | 用戶端伺服器執行階段處理... | Microsoft Corporation |

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

| Options | View | Process | Find | Users | Help | | | |
|---|------|---------|---------------|-------------|------|------------------------------|-------------------|----------------------|
| Run At Logon | | | | | | | | |
| <input checked="" type="checkbox"/> Verify Image Signatures | | CPU | Private Bytes | Working Set | PID | Description | Company Na... | Verified Signer |
| <input type="checkbox"/> VirusTotal.com | | 8.66 | 0 K | 24 K | 0 | | | |
| <input type="checkbox"/> Always On Top | | 0.77 | 44 K | 1,400 K | 4 | | | |
| <input type="checkbox"/> Replace Task Manager | | 0.17 | 0 K | 0 K | n/a | Hardware Interrupts and DPCs | | |
| <input type="checkbox"/> Hide When Minimized | | | 220 K | 600 K | 260 | Windows 工作階段管理員 | Microsoft Corp... | (Verified) Microsoft |
| <input type="checkbox"/> Allow Only One Instance | | | 1,380 K | 3,200 K | 360 | 用戶端伺服器執行階段處理... | Microsoft Corp... | (Verified) Microsoft |
| <input checked="" type="checkbox"/> Confirm Kill | | | 960 K | 3,064 K | 396 | Windows 啟動應用程式 | Microsoft Corp... | (Verified) Microsoft |
| <input type="checkbox"/> Tray Icons | | | 3,068 K | 4,792 K | 464 | 服務及控制站應用程式 | Microsoft Corp... | (Verified) Microsoft |
| <input type="checkbox"/> Configure Symbols... | | | 2,792 K | 5,768 K | 612 | Windows Services 的主機處理... | Microsoft Corp... | (Verified) Microsoft |
| | | | 2,432 K | 4,840 K | 676 | Windows Services 的主機處理... | Microsoft Corp... | (Verified) Microsoft |
| | | | 8,456 K | 8,872 K | 724 | Windows Services 的主機處理... | Microsoft Corp... | (Verified) Microsoft |
| | | | 24,004 K | 26,416 K | 820 | Windows Services 的主機處理... | Microsoft Corp... | (Verified) Microsoft |
| | | | 912 K | 2,852 K | 1300 | 桌面組態管理員 | Microsoft Corp... | (Verified) Microsoft |

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。

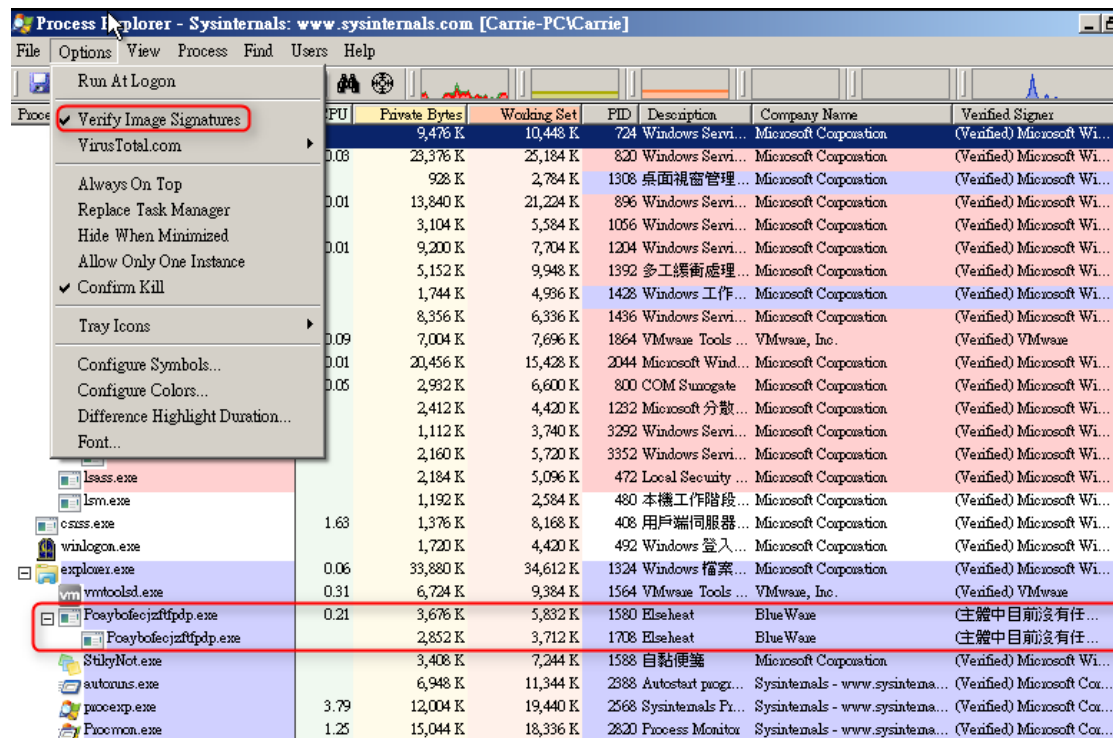
| Time of Day | Process Name | PID | Operation | Path | Result | Detail |
|---------------------|--------------|------|--------------------|--|--------------------|------------------------------|
| 上午 11:59:03 2297843 | Explorer.EXE | 1312 | CreateFile | C:\Users\Carmie\Desktop\SysinternalsSuite\p... | SUCCESS | Desired Access: Read Attibut |
| 上午 11:59:03 2308497 | Explorer.EXE | 1312 | QueryBasicInfor... | C:\Users\Carmie\Desktop\sysinternalsuite\pox... | SUCCESS | CreationTime: 2015/4/3 上午 |
| 上午 11:59:03 2309067 | Explorer.EXE | 1312 | CloseFile | C:\Users\Carmie\Desktop\sysinternalsuite\pox... | SUCCESS | |
| 上午 11:59:03 2317495 | Explorer.EXE | 1312 | CreateFile | C:\Users\Carmie\Desktop\SysinternalsSuite\pox... | SUCCESS | Desired Access: Read Attibut |
| 上午 11:59:03 2317719 | Explorer.EXE | 1312 | QueryBasicInfor... | C:\Users\Carmie\Desktop\sysinternalsuite\pox... | SUCCESS | CreationTime: 2015/4/3 上午 |
| 上午 11:59:03 2317789 | Explorer.EXE | 1312 | CloseFile | C:\Users\Carmie\Desktop\sysinternalsuite\pox... | SUCCESS | |
| 上午 11:59:03 2325755 | Explorer.EXE | 1312 | CreateFile | C:\Users\Carmie\Desktop\SysinternalsSuite\pox... | SUCCESS | Desired Access: Read Attibut |
| 上午 11:59:03 2326101 | Explorer.EXE | 1312 | QueryBasicInfor... | C:\Users\Carmie\Desktop\sysinternalsuite\pox... | SUCCESS | CreationTime: 2015/4/3 上午 |
| 上午 11:59:03 2326171 | Explorer.EXE | 1312 | CloseFile | C:\Users\Carmie\Desktop\sysinternalsuite\pox... | SUCCESS | |
| 上午 11:59:03 2330241 | Explorer.EXE | 1312 | CreateFile | C:\Users\Carmie\Desktop\SysinternalsSuite\pox... | SUCCESS | Desired Access: Generic Read |
| 上午 11:59:03 2330581 | Explorer.EXE | 1312 | CreateFileMapping | C:\Users\Carmie\Desktop\sysinternalsuite\pox... | FILE LOCKED WIT... | Sync Type: Sync TypeCreateSe |
| 上午 11:59:03 2331190 | Explorer.EXE | 1312 | CreateFileMapping | C:\Users\Carmie\Desktop\sysinternalsuite\pox... | SUCCESS | Sync Type: Sync TypeOther |
| 上午 11:59:03 2334119 | Explorer.EXE | 1312 | Load Image | C:\Users\Carmie\Desktop\sysinternalsuite\pox... | SUCCESS | Image Base: 0x620000, Image |
| 上午 11:59:03 2335292 | Explorer.EXE | 1312 | CloseFile | C:\Users\Carmie\Desktop\sysinternalsuite\pox... | SUCCESS | |
| 上午 11:59:03 2407144 | Explorer.EXE | 1312 | CreateFile | C:\Windows\lhh.exe | SUCCESS | Desired Access: Read Attibut |
| 上午 11:59:03 2408908 | Explorer.EXE | 1312 | QueryBasicInfor... | C:\Windows\lhh.exe | SUCCESS | CreationTime: 2009/7/14 上午 |
| 上午 11:59:03 2409034 | Explorer.EXE | 1312 | CloseFile | C:\Windows\lhh.exe | SUCCESS | |
| 上午 11:59:03 2412569 | Explorer.EXE | 1312 | CreateFile | C:\Windows\lhh.exe | SUCCESS | Desired Access: Read Attibut |
| 上午 11:59:03 2414259 | Explorer.EXE | 1312 | QueryBasicInfor... | C:\Windows\lhh.exe | SUCCESS | CreationTime: 2009/7/14 上午 |
| 上午 11:59:03 2414340 | Explorer.EXE | 1312 | CloseFile | C:\Windows\lhh.exe | SUCCESS | |
| 上午 11:59:03 2418127 | Explorer.EXE | 1312 | CreateFile | C:\Windows\lhh.exe | SUCCESS | Desired Access: Read Attibut |
| 上午 11:59:03 2419810 | Explorer.EXE | 1312 | QueryBasicInfor... | C:\Windows\lhh.exe | SUCCESS | CreationTime: 2009/7/14 上午 |
| 上午 11:59:03 2419891 | Explorer.EXE | 1312 | CloseFile | C:\Windows\lhh.exe | SUCCESS | |
| 上午 11:59:03 2421837 | Explorer.EXE | 1312 | CreateFile | C:\Windows\lhh.exe | SUCCESS | Desired Access: Generic Read |
| 上午 11:59:03 2423629 | Explorer.EXE | 1312 | CreateFileMapping | C:\Windows\lhh.exe | FILE LOCKED WIT... | Sync Type: Sync TypeCreateSe |
| 上午 11:59:03 2425522 | Explorer.EXE | 1312 | CreateFileMapping | C:\Windows\lhh.exe | SUCCESS | Sync Type: Sync TypeOther |
| 上午 11:59:03 2427849 | Explorer.EXE | 1312 | Load Image | C:\Windows\lhh.exe | SUCCESS | Image Base: 0x2c8000, Image |
| 上午 11:59:03 2428112 | Explorer.EXE | 1312 | CloseFile | C:\Windows\lhh.exe | SUCCESS | |
| 上午 11:59:03 2472165 | Explorer.EXE | 1312 | CreateFile | C:\Users\Carmie\Desktop\SysinternalsSuite\p... | SUCCESS | Desired Access: Read Attibut |
| 上午 11:59:03 2472424 | Explorer.EXE | 1312 | QueryBasicInfor... | C:\Users\Carmie\Desktop\sysinternalsuite\pox... | SUCCESS | CreationTime: 2015/4/3 上午 |
| 上午 11:59:03 2472497 | Explorer.EXE | 1312 | CloseFile | C:\Users\Carmie\Desktop\SysinternalsSuite\p... | SUCCESS | |
| 上午 11:59:03 2480467 | Explorer.EXE | 1312 | CreateFile | C:\Users\Carmie\Desktop\SysinternalsSuite\p... | SUCCESS | Desired Access: Read Attibut |
| 上午 11:59:03 2480687 | Explorer.EXE | 1312 | QueryBasicInfor... | C:\Users\Carmie\Desktop\SysinternalsSuite\p... | SUCCESS | CreationTime: 2015/4/3 上午 |

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。



| Process | Private Bytes | Working Set | PID | Description | Company Name | Verified Signer |
|----------------------|---------------|-------------|------|--------------------|----------------------------------|-----------------------------|
| lsass.exe | 9,476 K | 10,448 K | 724 | Windows Servi... | Microsoft Corporation | (Verified) Microsoft Wi... |
| csrss.exe | 23,376 K | 23,184 K | 820 | Windows Servi... | Microsoft Corporation | (Verified) Microsoft Wi... |
| vmtoolsd.exe | 928 K | 2,784 K | 1308 | 桌面視窗管理... | Microsoft Corporation | (Verified) Microsoft Wi... |
| explorer.exe | 13,840 K | 21,224 K | 896 | Windows Servi... | Microsoft Corporation | (Verified) Microsoft Wi... |
| vmtoolsd.exe | 3,104 K | 5,584 K | 1056 | Windows Servi... | Microsoft Corporation | (Verified) Microsoft Wi... |
| vmtoolsd.exe | 9,200 K | 7,704 K | 1204 | Windows Servi... | Microsoft Corporation | (Verified) Microsoft Wi... |
| vmtoolsd.exe | 5,152 K | 9,948 K | 1392 | 多工緩衝處理... | Microsoft Corporation | (Verified) Microsoft Wi... |
| vmtoolsd.exe | 1,744 K | 4,936 K | 1428 | Windows 工作... | Microsoft Corporation | (Verified) Microsoft Wi... |
| vmtoolsd.exe | 8,356 K | 6,336 K | 1436 | Windows Servi... | Microsoft Corporation | (Verified) Microsoft Wi... |
| vmtoolsd.exe | 7,004 K | 7,696 K | 1864 | VMware Tools ... | VMware, Inc. | (Verified) VMware |
| vmtoolsd.exe | 20,456 K | 15,428 K | 2044 | Microsoft Wind... | Microsoft Corporation | (Verified) Microsoft Wi... |
| vmtoolsd.exe | 2,932 K | 6,600 K | 800 | COM Surrogate | Microsoft Corporation | (Verified) Microsoft Wi... |
| vmtoolsd.exe | 2,412 K | 4,420 K | 1232 | Microsoft 分散... | Microsoft Corporation | (Verified) Microsoft Wi... |
| vmtoolsd.exe | 1,112 K | 3,740 K | 3292 | Windows Servi... | Microsoft Corporation | (Verified) Microsoft Wi... |
| vmtoolsd.exe | 2,160 K | 5,720 K | 3352 | Windows Servi... | Microsoft Corporation | (Verified) Microsoft Wi... |
| vmtoolsd.exe | 2,184 K | 5,096 K | 472 | Local Security ... | Microsoft Corporation | (Verified) Microsoft Wi... |
| vmtoolsd.exe | 1,192 K | 2,584 K | 480 | 本機工作階段... | Microsoft Corporation | (Verified) Microsoft Wi... |
| vmtoolsd.exe | 1,376 K | 3,168 K | 408 | 用戶端伺服器... | Microsoft Corporation | (Verified) Microsoft Wi... |
| vmtoolsd.exe | 1,720 K | 4,420 K | 492 | Windows 登入... | Microsoft Corporation | (Verified) Microsoft Wi... |
| vmtoolsd.exe | 33,880 K | 34,612 K | 1324 | Windows 檔案... | Microsoft Corporation | (Verified) Microsoft Wi... |
| Pcaybofecjzftfdp.exe | 6,724 K | 9,384 K | 1564 | VMware Tools ... | VMware, Inc. | (Verified) VMware |
| Pcaybofecjzftfdp.exe | 3,676 K | 5,832 K | 1580 | Elseheat | BlueWave | 主體中目前沒有任... |
| Pcaybofecjzftfdp.exe | 2,852 K | 3,712 K | 1708 | Elseheat | BlueWave | 主體中目前沒有任... |
| StikyNot.exe | 3,408 K | 7,244 K | 1588 | 自黏便箋 | Microsoft Corporation | (Verified) Microsoft Wi... |
| autoexec.exe | 6,948 K | 11,344 K | 2388 | Autostart progr... | Sysinternals - www.sysinterna... | (Verified) Microsoft Cor... |
| procexp.exe | 12,004 K | 19,440 K | 2568 | Sysinternals Pr... | Sysinternals - www.sysinterna... | (Verified) Microsoft Cor... |
| Procmon.exe | 15,044 K | 18,336 K | 2820 | Process Monitor | Sysinternals - www.sysinterna... | (Verified) Microsoft Cor... |

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。

| Time of Day | Process Name | PID | Operation | Path | Result | Detail |
|---------------------|--------------------|------|---------------|--|---------|---------|
| 上午 11:07:44.1943279 | Pooybafecjzftpd... | 1584 | RegQueryValue | HKCU\Software\Microsoft\Windows\CurrentVersion\Run\CryptoLocker | SUCCESS | Type: R |
| 上午 11:07:44.1943440 | Pooybafecjzftpd... | 1584 | RegCloseKey | HKCU\Software\Microsoft\Windows\CurrentVersion\Run | SUCCESS | |
| 上午 11:07:44.1943601 | Pooybafecjzftpd... | 1584 | RegOpenKey | HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce | SUCCESS | Desired |
| 上午 11:07:44.1943720 | Pooybafecjzftpd... | 1584 | RegQueryValue | HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce*CryptoLocker | SUCCESS | Type: R |
| 上午 11:07:44.1943786 | Pooybafecjzftpd... | 1584 | RegCloseKey | HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce | SUCCESS | |
| 上午 11:07:44.3023354 | Pooybafecjzftpd... | 1584 | RegOpenKey | HKCU\Software\Microsoft\Windows\CurrentVersion\Run | SUCCESS | Desired |
| 上午 11:07:44.3023578 | Pooybafecjzftpd... | 1584 | RegQueryValue | HKCU\Software\Microsoft\Windows\CurrentVersion\Run\CryptoLocker | SUCCESS | Type: R |
| 上午 11:07:44.3023711 | Pooybafecjzftpd... | 1584 | RegCloseKey | HKCU\Software\Microsoft\Windows\CurrentVersion\Run | SUCCESS | |
| 上午 11:07:44.3023855 | Pooybafecjzftpd... | 1584 | RegOpenKey | HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce | SUCCESS | Desired |
| 上午 11:07:44.3023967 | Pooybafecjzftpd... | 1584 | RegQueryValue | HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce*CryptoLocker | SUCCESS | Type: R |
| 上午 11:07:44.3024080 | Pooybafecjzftpd... | 1584 | RegCloseKey | HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce | SUCCESS | |
| 上午 11:07:44.4121125 | Pooybafecjzftpd... | 1584 | RegOpenKey | HKCU\Software\Microsoft\Windows\CurrentVersion\Run | SUCCESS | Desired |
| 上午 11:07:44.4121374 | Pooybafecjzftpd... | 1584 | RegQueryValue | HKCU\Software\Microsoft\Windows\CurrentVersion\Run\CryptoLocker | SUCCESS | Type: R |
| 上午 11:07:44.4121510 | Pooybafecjzftpd... | 1584 | RegCloseKey | HKCU\Software\Microsoft\Windows\CurrentVersion\Run | SUCCESS | |
| 上午 11:07:44.4121650 | Pooybafecjzftpd... | 1584 | RegOpenKey | HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce | SUCCESS | Desired |
| 上午 11:07:44.4121762 | Pooybafecjzftpd... | 1584 | RegQueryValue | HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce*CryptoLocker | SUCCESS | Type: R |
| 上午 11:07:44.4121825 | Pooybafecjzftpd... | 1584 | RegCloseKey | HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce | SUCCESS | |
| 上午 11:07:44.5209545 | Pooybafecjzftpd... | 1584 | RegOpenKey | HKCU\Software\Microsoft\Windows\CurrentVersion\Run | SUCCESS | Desired |
| 上午 11:07:44.5209944 | Pooybafecjzftpd... | 1584 | RegQueryValue | HKCU\Software\Microsoft\Windows\CurrentVersion\Run\CryptoLocker | SUCCESS | Type: R |
| 上午 11:07:44.5210091 | Pooybafecjzftpd... | 1584 | RegCloseKey | HKCU\Software\Microsoft\Windows\CurrentVersion\Run | SUCCESS | |
| 上午 11:07:44.5210248 | Pooybafecjzftpd... | 1584 | RegOpenKey | HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce | SUCCESS | Desired |
| 上午 11:07:44.5210364 | Pooybafecjzftpd... | 1584 | RegQueryValue | HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce*CryptoLocker | SUCCESS | Type: R |
| 上午 11:07:44.5210490 | Pooybafecjzftpd... | 1584 | RegCloseKey | HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce | SUCCESS | |
| 上午 11:07:44.6300704 | Pooybafecjzftpd... | 1584 | RegOpenKey | HKCU\Software\Microsoft\Windows\CurrentVersion\Run | SUCCESS | Desired |
| 上午 11:07:44.6301124 | Pooybafecjzftpd... | 1584 | RegQueryValue | HKCU\Software\Microsoft\Windows\CurrentVersion\Run\CryptoLocker | SUCCESS | Type: R |
| 上午 11:07:44.6301415 | Pooybafecjzftpd... | 1584 | RegCloseKey | HKCU\Software\Microsoft\Windows\CurrentVersion\Run | SUCCESS | |
| 上午 11:07:44.6301712 | Pooybafecjzftpd... | 1584 | RegOpenKey | HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce | SUCCESS | Desired |
| 上午 11:07:44.6301961 | Pooybafecjzftpd... | 1584 | RegQueryValue | HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce*CryptoLocker | SUCCESS | Type: R |
| 上午 11:07:44.6302111 | Pooybafecjzftpd... | 1584 | RegCloseKey | HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce | SUCCESS | |
| 上午 11:07:44.7402822 | Pooybafecjzftpd... | 1584 | RegOpenKey | HKCU\Software\Microsoft\Windows\CurrentVersion\Run | SUCCESS | Desired |
| 上午 11:07:44.7403333 | Pooybafecjzftpd... | 1584 | RegQueryValue | HKCU\Software\Microsoft\Windows\CurrentVersion\Run\CryptoLocker | SUCCESS | Type: R |
| 上午 11:07:44.7403641 | Pooybafecjzftpd... | 1584 | RegCloseKey | HKCU\Software\Microsoft\Windows\CurrentVersion\Run | SUCCESS | |
| 上午 11:07:44.7403970 | Pooybafecjzftpd... | 1584 | RegOpenKey | HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce | SUCCESS | Desired |
| 上午 11:07:44.7404299 | Pooybafecjzftpd... | 1584 | RegQueryValue | HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce*CryptoLocker | SUCCESS | Type: R |

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。

| Autorun Entry | Description | Publisher | Image Path | Timestamp |
|--|--------------------------|-----------------------|-------------------------------------|--------------------|
| <input checked="" type="checkbox"/> VMWae User Pr... | VMWae Tools Core Service | VMWae, Inc. | c:\program files\vmwae\vmwa... | 2012/8/2 上午 10:13 |
| HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components | | | | |
| <input checked="" type="checkbox"/> Browsing Enhanc... | Windows Mail | Microsoft Corporation | c:\program files\windows mail\... | 2009/7/14 上午 07:42 |
| <input checked="" type="checkbox"/> DirectDrawEx | Windows Mail | Microsoft Corporation | c:\program files\windows mail\... | 2009/7/14 上午 07:42 |
| <input checked="" type="checkbox"/> Internet Explorer... | Windows Mail | Microsoft Corporation | c:\program files\windows mail\... | 2009/7/14 上午 07:42 |
| <input checked="" type="checkbox"/> Internet Explorer... | Windows Mail | Microsoft Corporation | c:\program files\windows mail\... | 2009/7/14 上午 07:42 |
| <input checked="" type="checkbox"/> Microsoft Windo... | Windows Mail | Microsoft Corporation | c:\program files\windows mail\... | 2009/7/14 上午 07:42 |
| <input checked="" type="checkbox"/> Microsoft Windo... | Windows Mail | Microsoft Corporation | c:\program files\windows mail\... | 2009/7/14 上午 07:42 |
| <input checked="" type="checkbox"/> HKCU\Software\Microsoft\Windows\CurrentVersion\Run | | | | 2015/4/4 上午 11:15 |
| <input checked="" type="checkbox"/> CryptoLocker | Elseheat | Blue Wave | c:\users\kazmie\appdata\local\po... | 2014/2/27 上午 08:58 |
| <input checked="" type="checkbox"/> HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce | | | | 2015/4/4 上午 11:15 |
| <input checked="" type="checkbox"/> *CryptoLocker | Elseheat | Blue Wave | c:\users\kazmie\appdata\local\po... | 2014/2/27 上午 08:58 |

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。