

Cuckoo Sandbox and Noriben

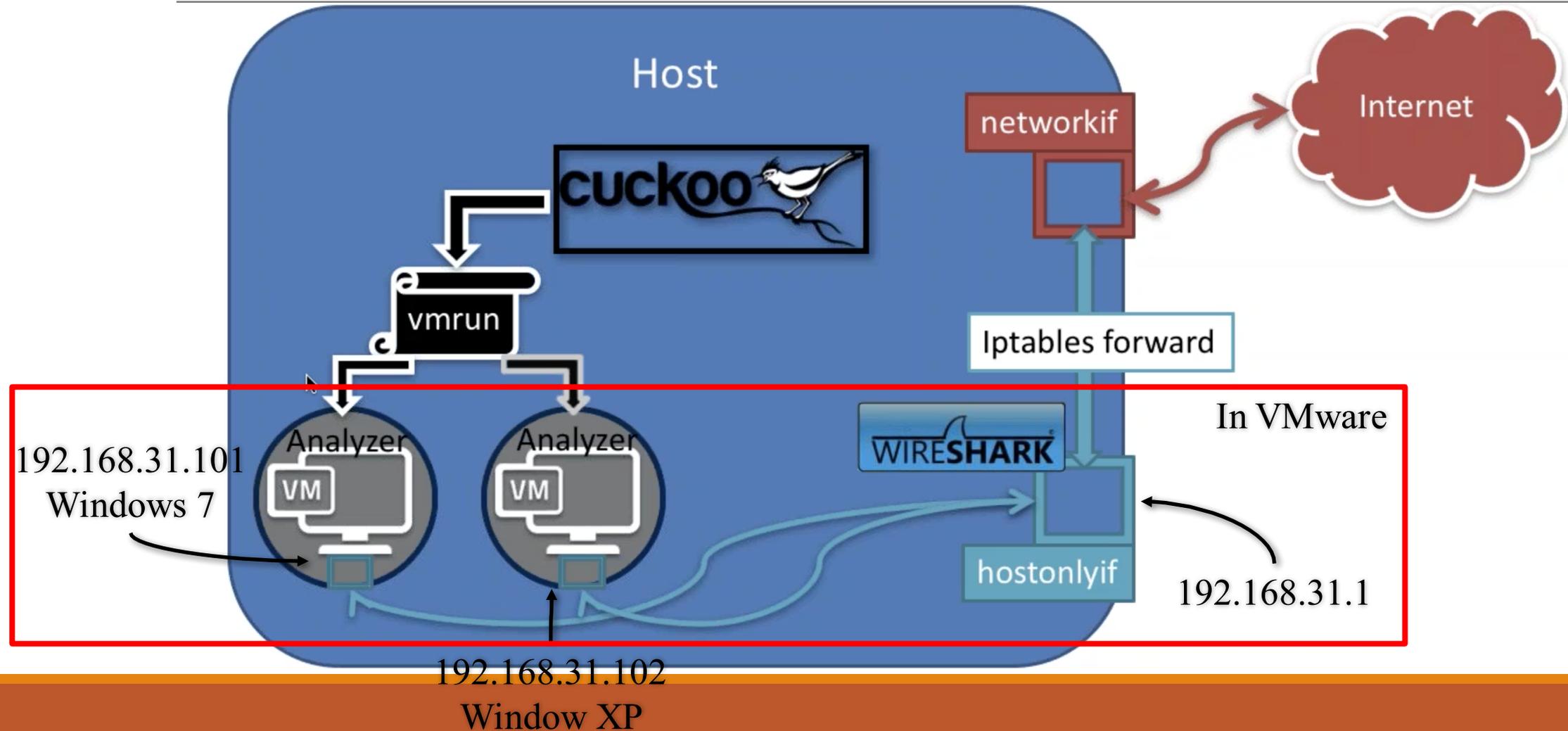
賴家民 SENALAI@III.ORG.TW

-
1. Cuckoo SandBox
 2. Procmon
 3. Noriben

Cuckoo Sandbox

- Traces of calls performed by all processes spawned by the malware.
- Files being created, deleted and downloaded by the malware during its execution.
- Memory dumps of the malware processes.
- Network traffic trace in PCAP format.
- Screenshots taken during the execution of the malware.
- Full memory dumps of the machines.

Architecture



Requirements

- Virtual Machine : VMware Fusion
- Host : Mac OS X 10.12.6
- Client : Windows 7 x64

Preparing Client

- Drop agent.py to Guset Client
- Python 2.7
 - <https://www.python.org/ftp/python/2.7.13/python-2.7.13rc1.msi>
 - For agent.py
 - Rename the file from agent.py to **agent.pyw** which will prevent the console window from spawning.
- Python Pillow
 - <http://effbot.org/downloads/PIL-1.1.7.win32-py2.7.exe>
 - For screenshot

Preparing Client

- Enable auto-logon
 - `reg add "hkml\software\Microsoft\Windows NT\CurrentVersion\WinLogon" /v DefaultUserName /d <USERNAME> /t REG_SZ /f`
 - `reg add "hkml\software\Microsoft\Windows NT\CurrentVersion\WinLogon" /v DefaultPassword /d <PASSWORD> /t REG_SZ /f`
 - `reg add "hkml\software\Microsoft\Windows NT\CurrentVersion\WinLogon" /v AutoAdminLogon /d 1 /t REG_SZ /f`
 - <https://support.microsoft.com/zh-tw/help/324737/how-to-turn-on-automatic-logon-in-windows>

Preparing Client

The image shows two overlapping Windows Control Panel windows. The background window is titled '自訂每個網路類型的設定' (Customize settings for each network type) and is located at 'Control Panel > System and Security > Windows Firewall > Custom Settings'. It contains two sections: 'Home or Work (Private) Network Location Settings' and 'Public Network Location Settings'. In both sections, the 'Turn off Windows Firewall (not recommended)' option is selected. The foreground window is titled 'Windows Update' and is located at 'Control Panel > System and Security > Windows Update'. It features a sidebar with navigation links like 'Check for updates' and 'Change settings'. The main content area shows a red shield icon with a white 'X' and the text 'Turn on automatic updates' and 'Do not automatically install updates'. A button labeled 'Turn on automatic updates (A)' is visible. Below this, it shows update status: 'Last update check: Never', 'Updates installed: Never', and 'Receive updates: Only for Windows'. A link for 'Get updates for other Microsoft products' is also present.

自訂每個網路類型的設定

您可以為您使用的每個網路位置類型修改防火牆設定。

[什麼是網路位置？](#)

家用或工作場所 (私人) 網路位置設定

- 開啟 Windows 防火牆
 - 封鎖所有連入連線，包括允許的程式清單中的連入連線
 - 當 Windows 防火牆封鎖新的程式時請通知我
- 關閉 Windows 防火牆 (不建議)

公用網路位置設定

- 開啟 Windows 防火牆
 - 封鎖所有連入連線，包括允許的程式清單中的連入連線
 - 當 Windows 防火牆封鎖新的程式時請通知我
- 關閉 Windows 防火牆 (不建議)

確定 取消

Windows Update

控制台首頁

檢查更新

變更設定

檢視更新記錄

還原隱藏的更新

更新: 常見問題集

請參閱

已安裝的更新

Windows Update

開啟自動更新
不會自動安裝更新

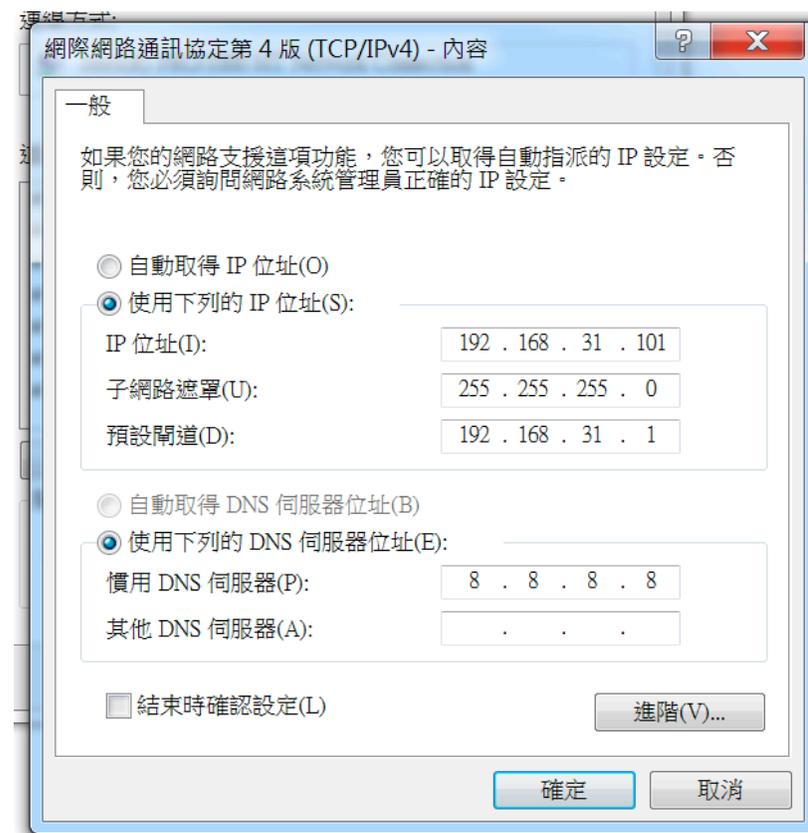
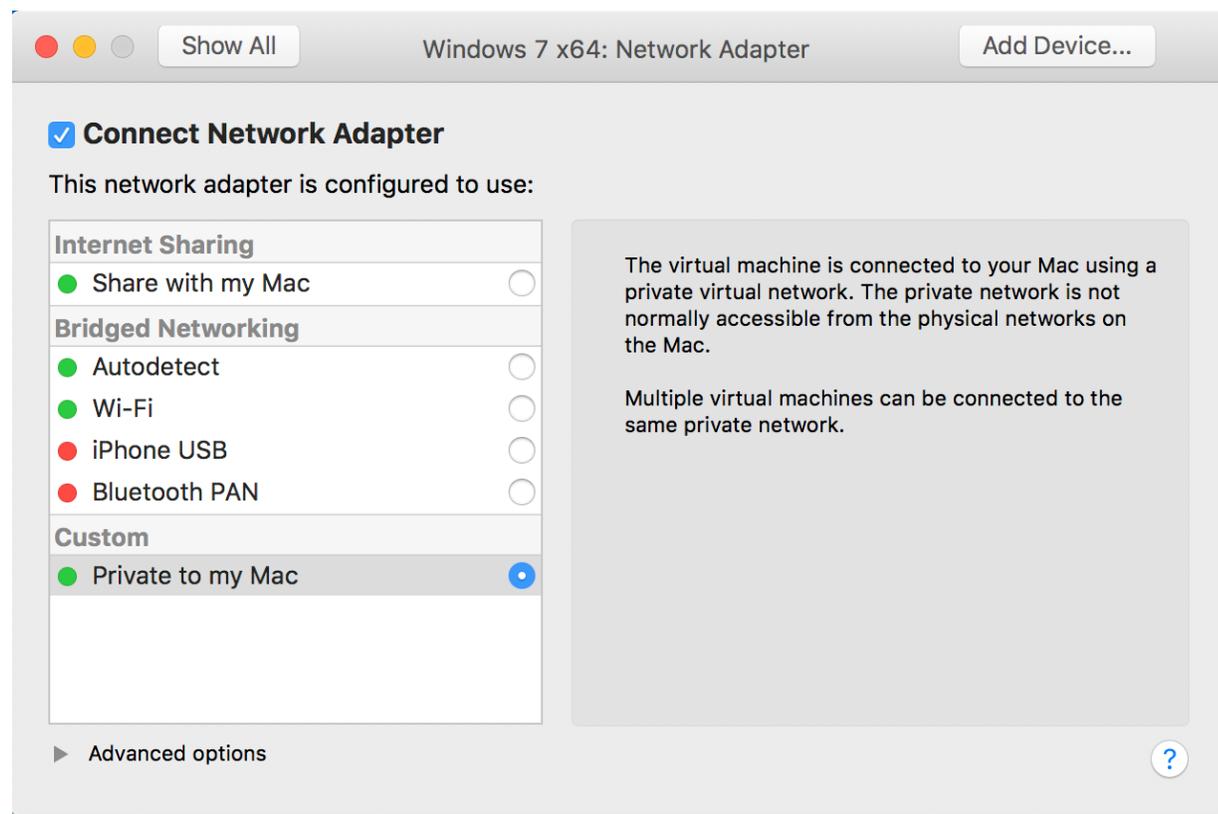
開啟自動更新以協助改善電腦的安全性和效能，並允許標準使用者在此電腦安裝更新。

[開啟自動更新\(A\)](#)
[讓我選擇我的設定](#)

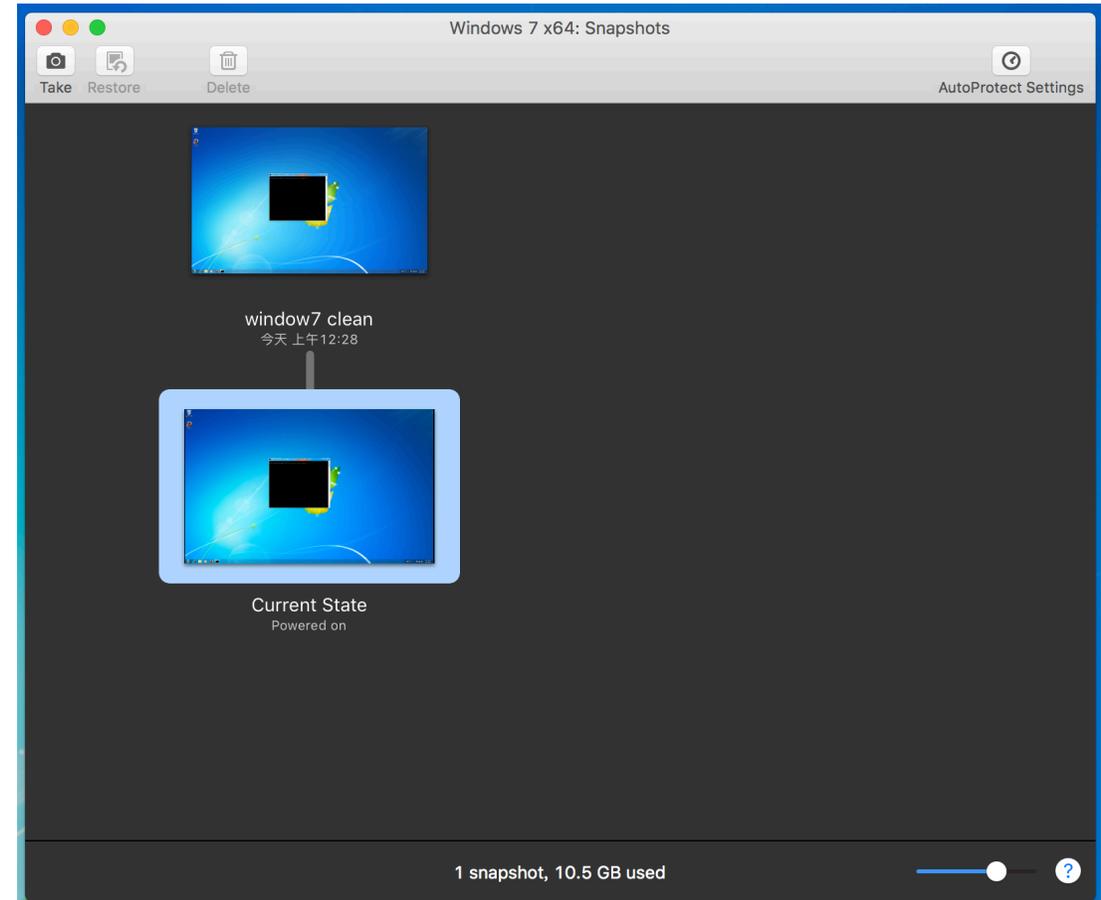
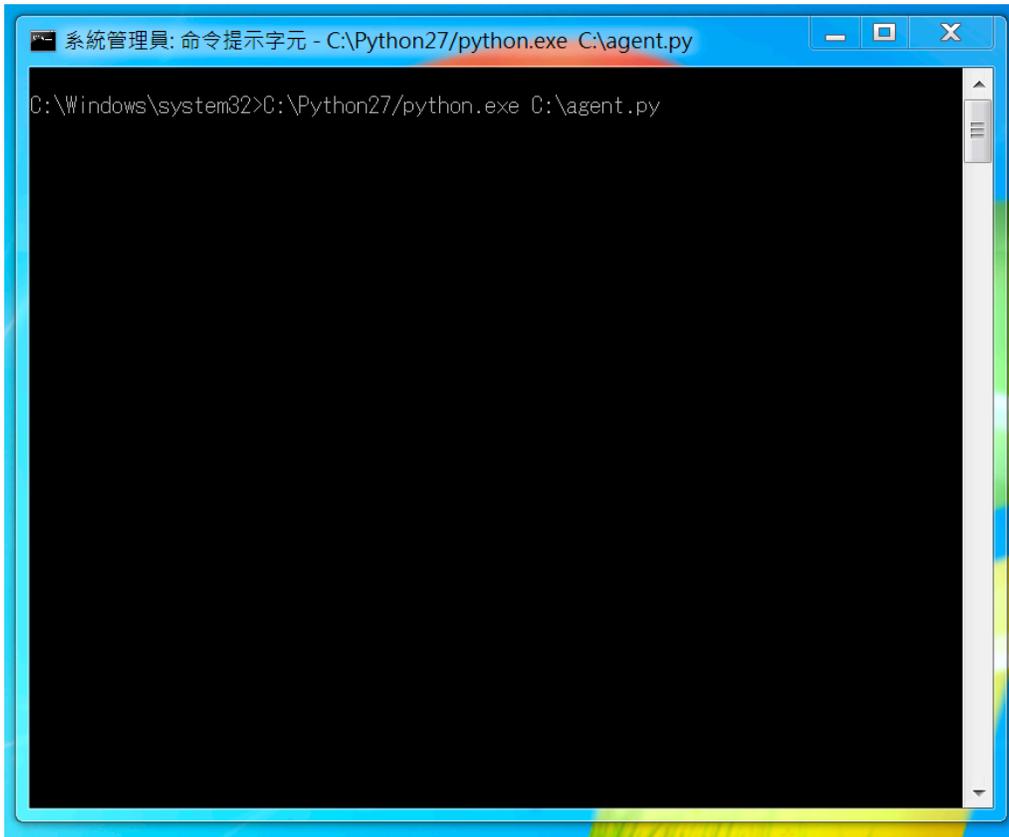
最近的更新檢查: 從未
已安裝更新: 從未
接收更新: 僅適用於 Windows。

取得其他 Microsoft 產品的更新。 [了解詳細資料](#)

Preparing Client



Preparing Guest Client



Preparing Host

```
$ sudo pip install -U pip setuptools
```

```
$ sudo pip install -U cuckoo
```

or

```
$ virtualenv cuckoo
```

```
$ source cuckoo/bin/activate
```

```
(cuckoo)$ pip install -U pip setuptools
```

```
(cuckoo)$ pip install -U cuckoo
```

Preparing Host(Ubuntu)

```
$ sudo apt-get install python python-pip python-dev libffi-dev libssl-dev
```

```
$ sudo apt-get install python-virtualenv python-setuptools
```

```
$ sudo apt-get install libjpeg-dev zlib1g-dev swig
```

```
$ sudo apt-get install mongodb
```

```
$ sudo apt-get install tcpdump apparmor-utils
```

```
$ sudo aa-disable /usr/sbin/tcpdump
```

```
$ sudo setcap cap_net_raw,cap_net_admin=eip /usr/sbin/tcpdump
```

<http://blog.csdn.net/mark20170902/article/details/53422384>

Preparing Host(Ubuntu)

- Setting IP Forwarding

```
1 iptables -A FORWARD -o ens33 -i ens38 -s 192.168.31.0/24 -m conntrack --ctstate NEW -j ACCEPT
2
3 iptables -A FORWARD -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
4
5 iptables -A POSTROUTING -t nat -j MASQUERADE
6
7 sysctl -w net.ipv4.ip_forward=1
```

Preparing Host (Mac)

```
$ brew install libmagic
```

Preparing Host (Mac)

- Setting ip Forwarding

```
sudo sysctl -w net.inet.ip.forwarding=1 #setting mac os x port forwarding
rules="nat on en0 from vmnet2:network to any ->(en0)
pass inet proto icmp all
pass in on vmnet2 proto udp from any to any port domain keep state
pass quick on en0 proto udp from any to any port domain keep state"
echo "$rules" > ./pfrules
sudo pfctl -e -f ./pfrules
```

Preparing Host

- Initial Cuckoo
 - (cuckoo) \$ cuckoo -d

```

      .-.-.      .-.-.      .-.-.      .-.-.      .-.-.
     /  /  \    /  /  \    /  /  \    /  /  \    /  /  \
    /  /  \    /  /  \    /  /  \    /  /  \    /  /  \
   /  /  \    /  /  \    /  /  \    /  /  \    /  /  \
  /  /  \    /  /  \    /  /  \    /  /  \    /  /  \
 /  /  \    /  /  \    /  /  \    /  /  \    /  /  \
/  /  \    /  /  \    /  /  \    /  /  \    /  /  \
\  \  /    \  \  /    \  \  /    \  \  /    \  \  /
 \  \  /    \  \  /    \  \  /    \  \  /    \  \  /
  \  \  /    \  \  /    \  \  /    \  \  /    \  \  /
   \  \  /    \  \  /    \  \  /    \  \  /    \  \  /
    \  \  /    \  \  /    \  \  /    \  \  /    \  \  /
     \  \  /    \  \  /    \  \  /    \  \  /    \  \  /
      \  \  /    \  \  /    \  \  /    \  \  /    \  \  /

Cuckoo Sandbox 2.0.2
www.cuckoosandbox.org
Copyright (c) 2010-2017

=====

Welcome to Cuckoo Sandbox, this appears to be your first run!
We will now set you up with our default configuration.
You will be able to see and modify the Cuckoo configuration,
Yara rules, Cuckoo Signatures, and much more to your likings
by exploring the /home/gun/.cuckoo directory.

Among other configurable items of most interest is the
new location for your Cuckoo configuration:
/home/gun/.cuckoo/conf

=====

Cuckoo has finished setting up the default configuration.
Please modify the default settings where required and
start Cuckoo again (by running `cuckoo` or `cuckoo -d`).

```

Preparing Host

- Configuring general behavior and analysis options
 - (cuckoo) \$ vim ~/.cuckoo/conf/cuckoo.conf
- Modify part
 - ip = 192.168.31.1
 - machinery = vmware

Preparing Host

- Enabling and configuring auxiliary modules
 - (cuckoo) \$ vim ~/.cuckoo/conf/auxiliary.conf
- Modify part
 - None

Preparing Host

- Volatility configuration
 - (cuckoo) \$ vim ~/.cuckoo/conf/memory.conf
- Modify part
 - None

Preparing Host

- Enabling and configuring processing modules
 - (cuckoo) \$ vim ~/.cuckoo/conf/processing.conf
- Modify part
 - [Virustotal]
 - enable = yes

Preparing Host

- Enabling or disabling report formats
 - (cuckoo) \$ vim ~/.cuckoo/conf/reporting.conf
- Modify part
 - [mongodb]
 - enable = yes

Preparing Host

- Enabling or disabling report formats
 - (cuckoo) \$ vim ~/.cuckoo/conf/vmware.conf
- Modify part
 - path = /Applications/VMware Fusion.app/Contents/Library/vmrun
 - interface = vmnet2
 - machines = windows7
 - [windows7]
 - vmx_path =
/Users/scml/Documents/VirtualMachines.localized/Cuckoo.vmwarevm/Cuckoo1.vmx
 - Snapshot = Cuckoo Clean
 - ip = 192.168.31.101

Preparing Host

- (cuckoo) \$ cuckoo community
- (cuckoo) \$ git clone --recursive <https://github.com/VirusTotal/yara-python>
- (cuckoo) \$ cd yara-python
- (cuckoo) \$ python setup.py build
- (cuckoo) \$ python setup.py install

Wannacry @ Cuckoo

The screenshot displays a Windows desktop environment within a Cuckoo sandbox. A red ransomware notification window is the central focus, with the title "Oops, your files have been encrypted!". The window contains the following text:

我的電腦出了什麼問題？
您的一些重要文件被我加密保存了。照片、圖片、文檔、壓縮包、音頻、視頻文件、exe文件等，幾乎所有類型的文件都被加密了，因此不能正常打開。這和一般文件損壞有本質上的區別。您可在網上找找恢復文件的方法，我敢保證，沒有我們的解密服務，就算老天爺來了也不能恢復這些文檔。

有沒有恢復這些文檔的方法？
當然有可恢復的方法。只能通過我們的解密服務才能恢復。我以人格擔保，能夠提供安全有效的恢復服務。但是收費的，也不能無限期的推遲。請點擊 <Decrypt> 按鈕，就可以免費恢復一些文檔。請您放心，我是絕不會騙您的。但想要恢復全部文檔，需要付款點費用。是否隨時都可以固定金額付款，就會恢復的嗎，當然不是，推遲付款時間越長對你不利。最好3天之內付款費用，過了三天費用就會翻倍。還有，一個禮拜之內未付款，將會永遠恢復不了。對了，忘了告訴你，對半年以上沒錢付款的窮人，會有活動免費恢復，能否輪到你，就靠您的運氣加點緣分。

Send \$300 worth of bitcoin to this address:
129YDPgwueZHyMgw518p7AABnjr65Mw

Buttons: Check Payment, Decrypt

In the background, a command prompt window shows the following log output:

```
C:\Windows\System32\cmd.exe - C:\Python27\python.exe C:\a...
or functions of: 32-bit kernel32.dll (with timestamp 0x445b0bde)
2017-08-28 11:49:05,342 [analyzer] DEBUG: Loaded monitor into process with pid 2038
2017-08-28 11:49:29,875 [analyzer] INFO: Added new file to list with pid 2038 and path C:\Windows\TaskSch...
2017-08-28 11:49:29,921 [analyzer] INFO: Injected into process with pid 3048 and name u' tasksche.exe'
2017-08-28 11:49:30,000 [analyzer] WARNING: Unable to find the correct offsets for functions of: 32-bit kernel32.dll (with timestamp 0x445b0bde)
2017-08-28 11:49:30,000 [analyzer] WARNING: Unable to find the correct offsets for functions of: 32-bit kernel32.dll (with timestamp 0x445b0bde)
2017-08-28 11:49:30,094 [analyzer] DEBUG: Loaded monitor into process with pid 3048
2017-08-28 11:49:32,266 [lib.api.process] INFO: Memory dump of process with pid 2038 completed
2017-08-28 11:49:32,290 [analyzer] INFO: Process with pid 2038 has terminated
2017-08-28 11:50:00,345 [analyzer] DEBUG: Received request to inject pid=3048, but it we are already injected there.
2017-08-28 11:50:00,484 [lib.api.process] INFO: Memory dump of process with pid 3048 completed
2017-08-28 11:50:01,141 [analyzer] INFO: Process with pid 3048 has terminated
2017-08-28 11:50:01,141 [analyzer] INFO: Process list is empty, terminating analysis.
2017-08-28 11:50:02,187 [analyzer] INFO: Analysis completed.
```

Process Monitor

Process Monitor



Process Monitor是windows系統的即時監控程式,可以對process, activity, File, Registry, Network...等等進行分析

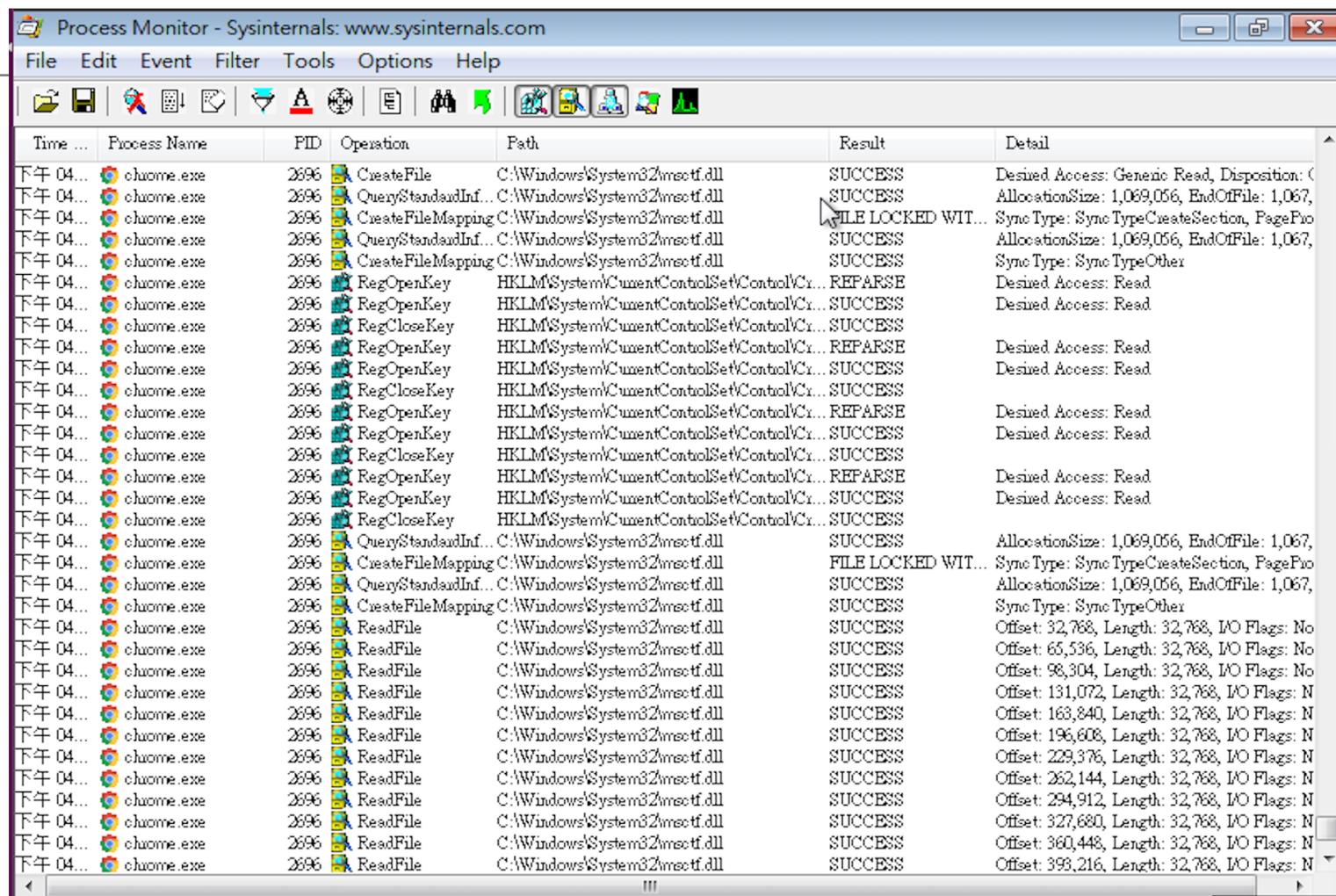
➤ 同時監控Registry和Process

Process Monitor v3.33

免安裝, 直接執行exe檔

下載網址: <https://technet.microsoft.com/en-us/sysinternals/processmonitor.aspx>

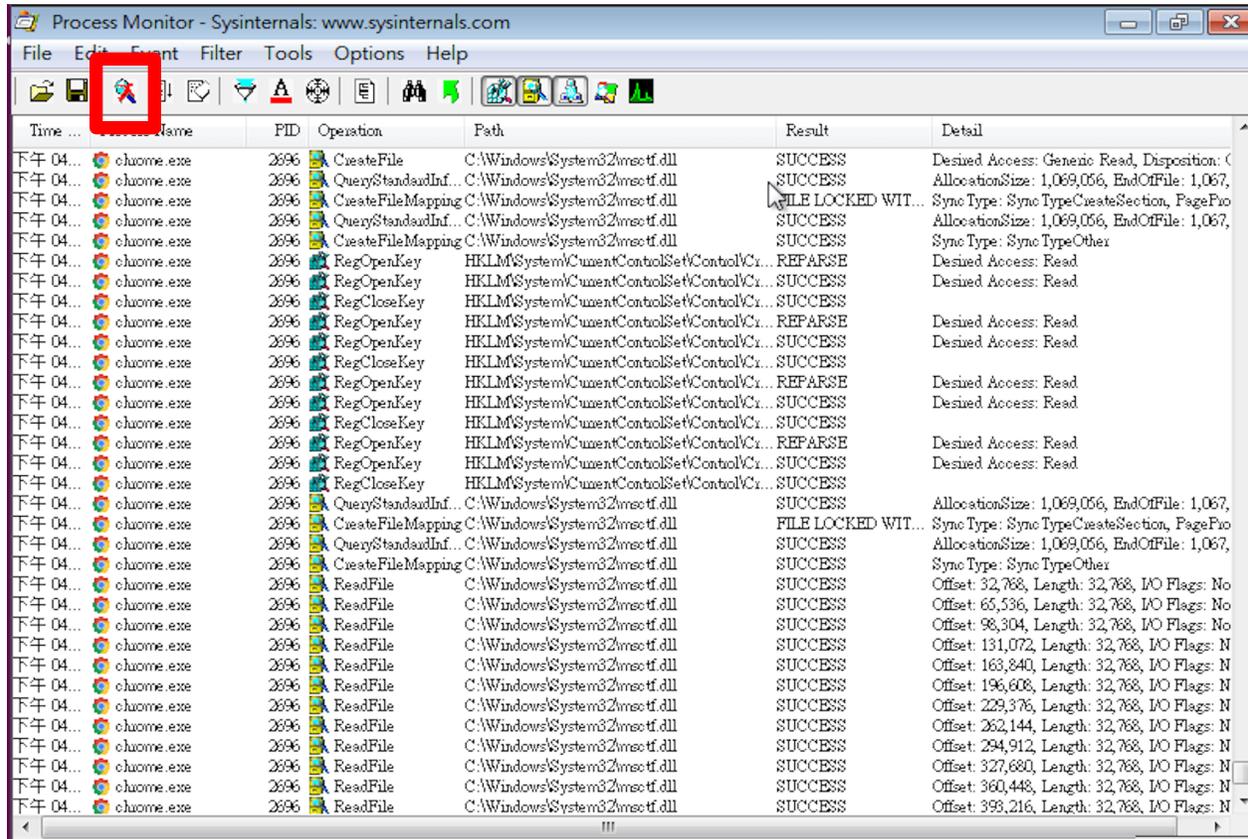
主畫面



The screenshot shows the Process Monitor application window with a list of system events. The events are filtered to show operations performed by chrome.exe (PID 2896) on the file C:\Windows\System32\msctf.dll. The operations include file creation, mapping, and reading, as well as registry operations. The results are mostly successful, with some 'FILE LOCKED WITH OTHER APPLICATIONS' errors during file mapping attempts.

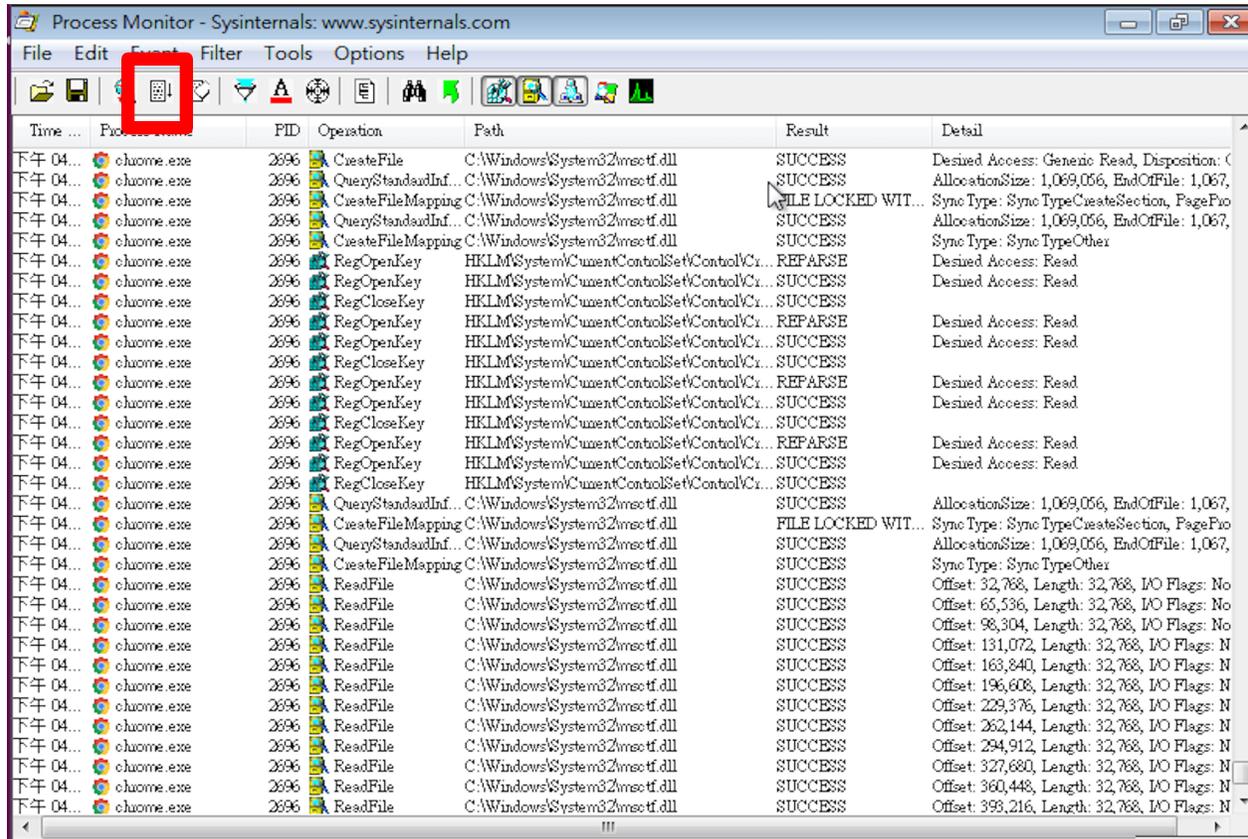
Time ...	Process Name	PID	Operation	Path	Result	Detail
下午 04...	chrome.exe	2896	CreateFile	C:\Windows\System32\msctf.dll	SUCCESS	Desired Access: Generic Read, Disposition: (
下午 04...	chrome.exe	2896	QueryStandardInf...	C:\Windows\System32\msctf.dll	SUCCESS	AllocationSize: 1,069,056, EndOfFile: 1,067,
下午 04...	chrome.exe	2896	CreateFileMapping	C:\Windows\System32\msctf.dll	FILE LOCKED WIT...	Sync Type: Sync TypeCreateSection, PagePro
下午 04...	chrome.exe	2896	QueryStandardInf...	C:\Windows\System32\msctf.dll	SUCCESS	AllocationSize: 1,069,056, EndOfFile: 1,067,
下午 04...	chrome.exe	2896	CreateFileMapping	C:\Windows\System32\msctf.dll	SUCCESS	Sync Type: Sync TypeOther
下午 04...	chrome.exe	2896	RegOpenKey	HKLM\System\CurrentControlSet\Control\Cr...	REPARSE	Desired Access: Read
下午 04...	chrome.exe	2896	RegOpenKey	HKLM\System\CurrentControlSet\Control\Cr...	SUCCESS	Desired Access: Read
下午 04...	chrome.exe	2896	RegCloseKey	HKLM\System\CurrentControlSet\Control\Cr...	SUCCESS	
下午 04...	chrome.exe	2896	RegOpenKey	HKLM\System\CurrentControlSet\Control\Cr...	REPARSE	Desired Access: Read
下午 04...	chrome.exe	2896	RegOpenKey	HKLM\System\CurrentControlSet\Control\Cr...	SUCCESS	Desired Access: Read
下午 04...	chrome.exe	2896	RegCloseKey	HKLM\System\CurrentControlSet\Control\Cr...	SUCCESS	
下午 04...	chrome.exe	2896	RegOpenKey	HKLM\System\CurrentControlSet\Control\Cr...	REPARSE	Desired Access: Read
下午 04...	chrome.exe	2896	RegOpenKey	HKLM\System\CurrentControlSet\Control\Cr...	SUCCESS	Desired Access: Read
下午 04...	chrome.exe	2896	RegCloseKey	HKLM\System\CurrentControlSet\Control\Cr...	SUCCESS	
下午 04...	chrome.exe	2896	RegOpenKey	HKLM\System\CurrentControlSet\Control\Cr...	REPARSE	Desired Access: Read
下午 04...	chrome.exe	2896	RegOpenKey	HKLM\System\CurrentControlSet\Control\Cr...	SUCCESS	Desired Access: Read
下午 04...	chrome.exe	2896	RegCloseKey	HKLM\System\CurrentControlSet\Control\Cr...	SUCCESS	
下午 04...	chrome.exe	2896	QueryStandardInf...	C:\Windows\System32\msctf.dll	SUCCESS	AllocationSize: 1,069,056, EndOfFile: 1,067,
下午 04...	chrome.exe	2896	CreateFileMapping	C:\Windows\System32\msctf.dll	FILE LOCKED WIT...	Sync Type: Sync TypeCreateSection, PagePro
下午 04...	chrome.exe	2896	QueryStandardInf...	C:\Windows\System32\msctf.dll	SUCCESS	AllocationSize: 1,069,056, EndOfFile: 1,067,
下午 04...	chrome.exe	2896	CreateFileMapping	C:\Windows\System32\msctf.dll	SUCCESS	Sync Type: Sync TypeOther
下午 04...	chrome.exe	2896	ReadFile	C:\Windows\System32\msctf.dll	SUCCESS	Offset: 32,768, Length: 32,768, I/O Flags: No
下午 04...	chrome.exe	2896	ReadFile	C:\Windows\System32\msctf.dll	SUCCESS	Offset: 65,536, Length: 32,768, I/O Flags: No
下午 04...	chrome.exe	2896	ReadFile	C:\Windows\System32\msctf.dll	SUCCESS	Offset: 98,304, Length: 32,768, I/O Flags: No
下午 04...	chrome.exe	2896	ReadFile	C:\Windows\System32\msctf.dll	SUCCESS	Offset: 131,072, Length: 32,768, I/O Flags: N
下午 04...	chrome.exe	2896	ReadFile	C:\Windows\System32\msctf.dll	SUCCESS	Offset: 163,840, Length: 32,768, I/O Flags: N
下午 04...	chrome.exe	2896	ReadFile	C:\Windows\System32\msctf.dll	SUCCESS	Offset: 196,608, Length: 32,768, I/O Flags: N
下午 04...	chrome.exe	2896	ReadFile	C:\Windows\System32\msctf.dll	SUCCESS	Offset: 229,376, Length: 32,768, I/O Flags: N
下午 04...	chrome.exe	2896	ReadFile	C:\Windows\System32\msctf.dll	SUCCESS	Offset: 262,144, Length: 32,768, I/O Flags: N
下午 04...	chrome.exe	2896	ReadFile	C:\Windows\System32\msctf.dll	SUCCESS	Offset: 294,912, Length: 32,768, I/O Flags: N
下午 04...	chrome.exe	2896	ReadFile	C:\Windows\System32\msctf.dll	SUCCESS	Offset: 327,680, Length: 32,768, I/O Flags: N
下午 04...	chrome.exe	2896	ReadFile	C:\Windows\System32\msctf.dll	SUCCESS	Offset: 360,448, Length: 32,768, I/O Flags: N
下午 04...	chrome.exe	2896	ReadFile	C:\Windows\System32\msctf.dll	SUCCESS	Offset: 393,216, Length: 32,768, I/O Flags: N

功能介紹



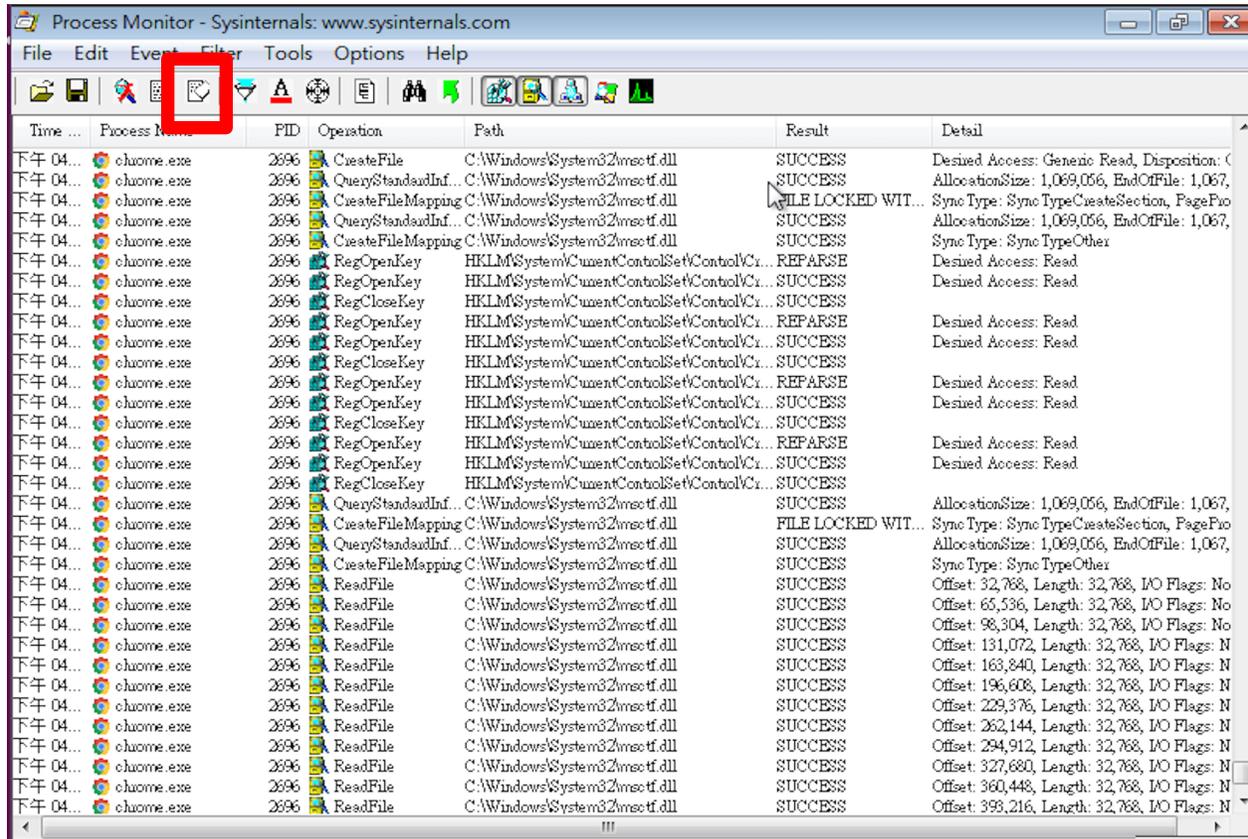
開啟/停止捕捉: 開始/停止捕捉行為

功能介紹



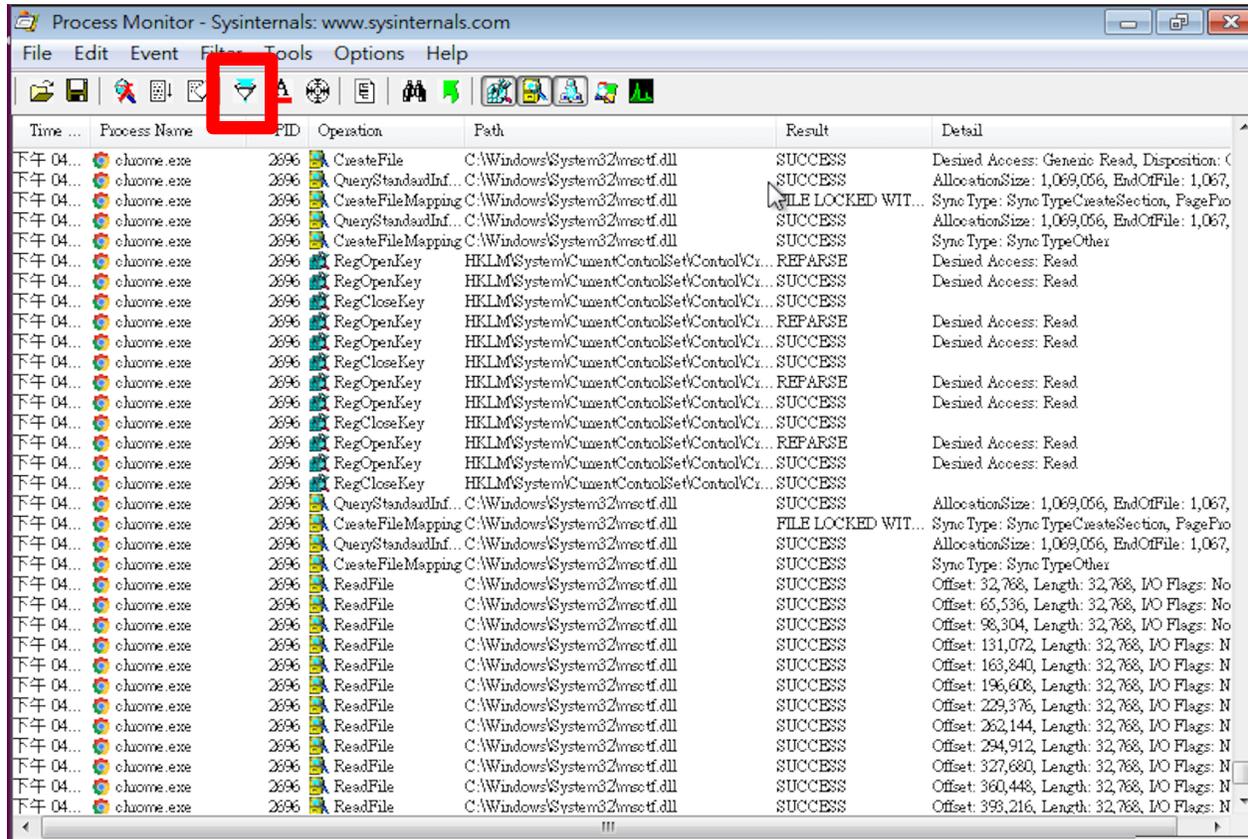
自動下拉: 保持在最下(新)的紀錄

功能介紹



清除記錄: 清除目前的紀錄

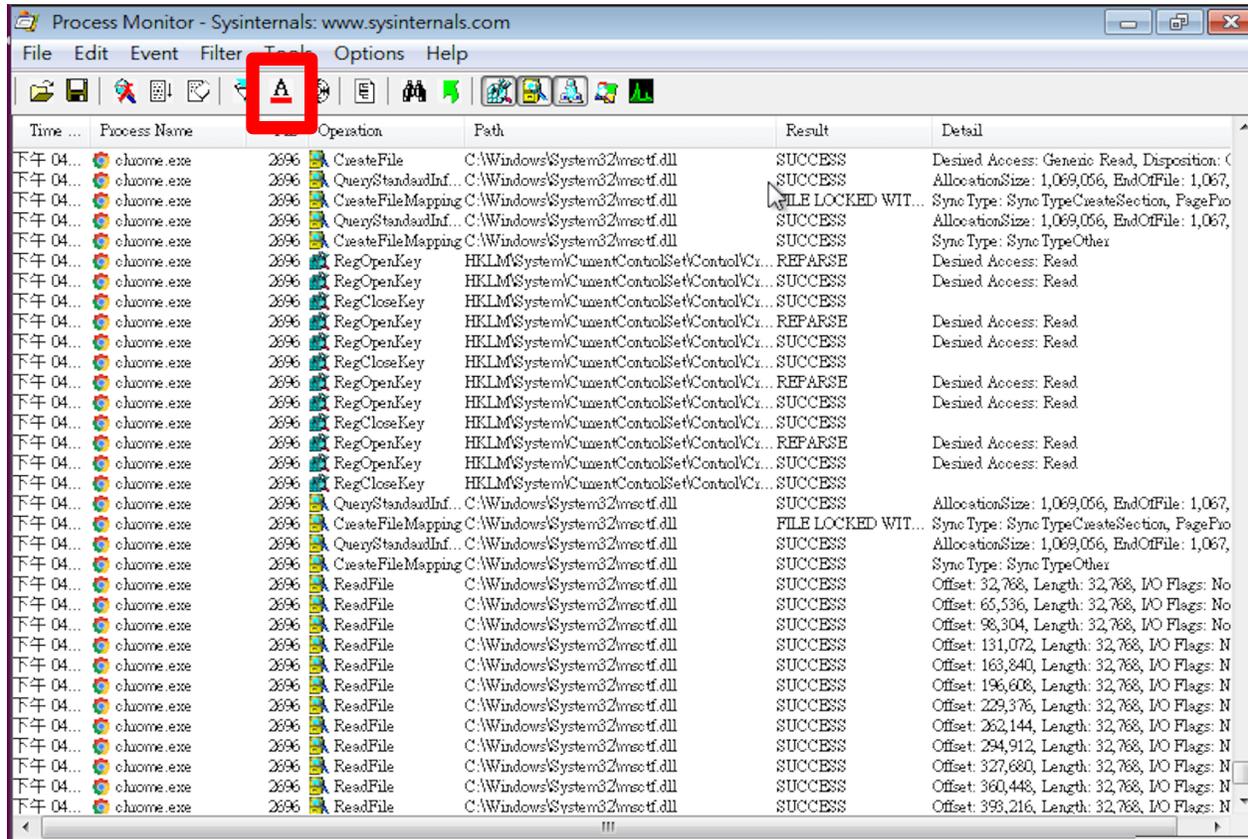
功能介紹



設定過濾: 可用PID, Operation, Process Name... 等等來設定過濾紀錄

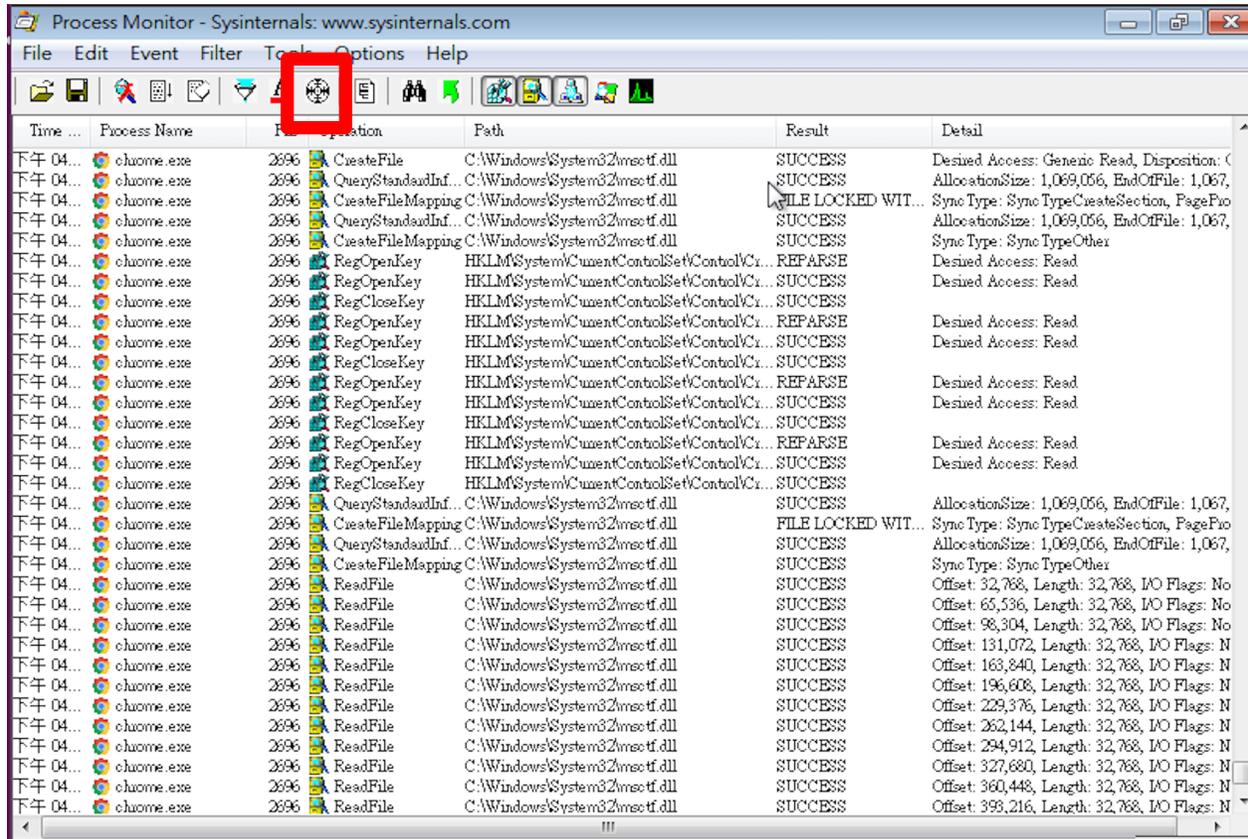
- Operation is "TCP Connect"
- Operation is "RegSetValue"
- Operation is "WriteFile"
- "Category" is "Write"

功能介紹



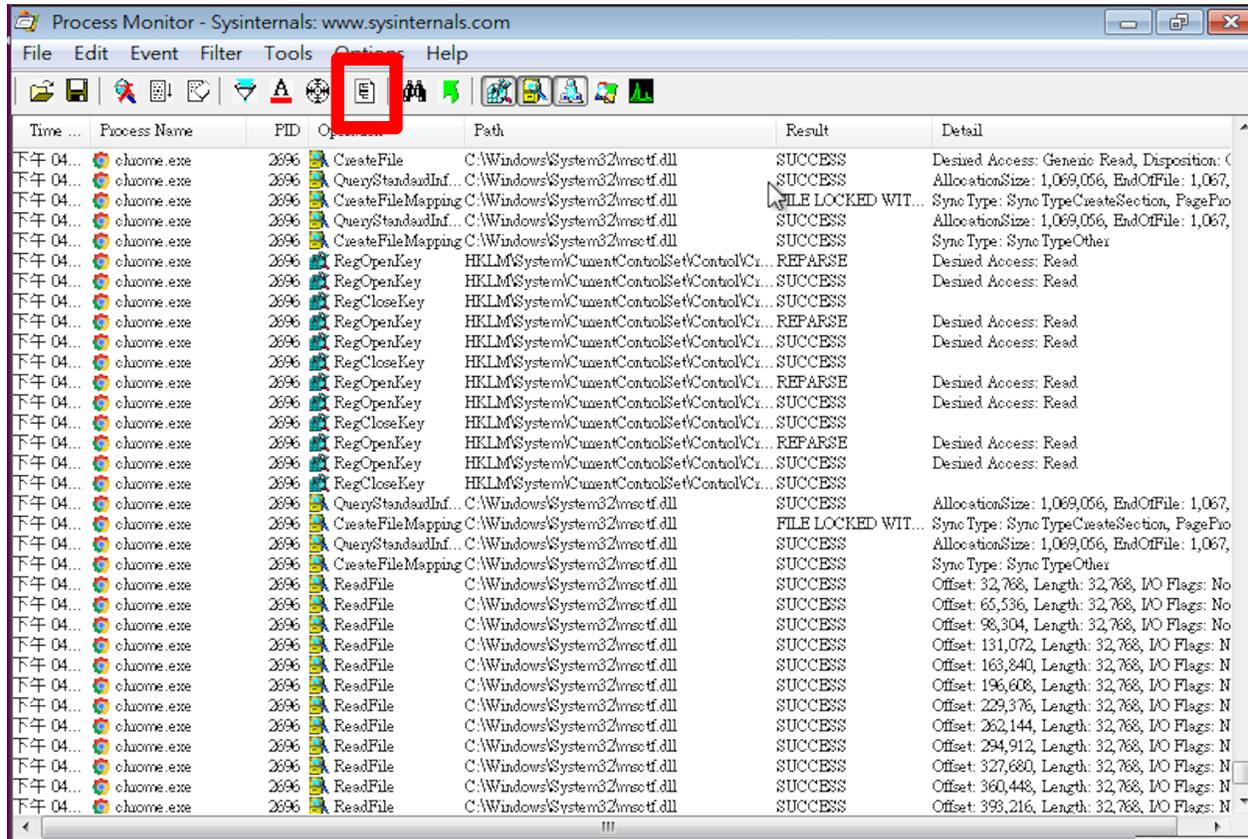
突出標示: 標示出所設定的紀錄

功能介紹



指定程式: 直接拖曳到指定的程式, Procmon會過濾此程式的紀錄

功能介紹



Process樹: 畫出Process樹

功能介紹

Process Tree

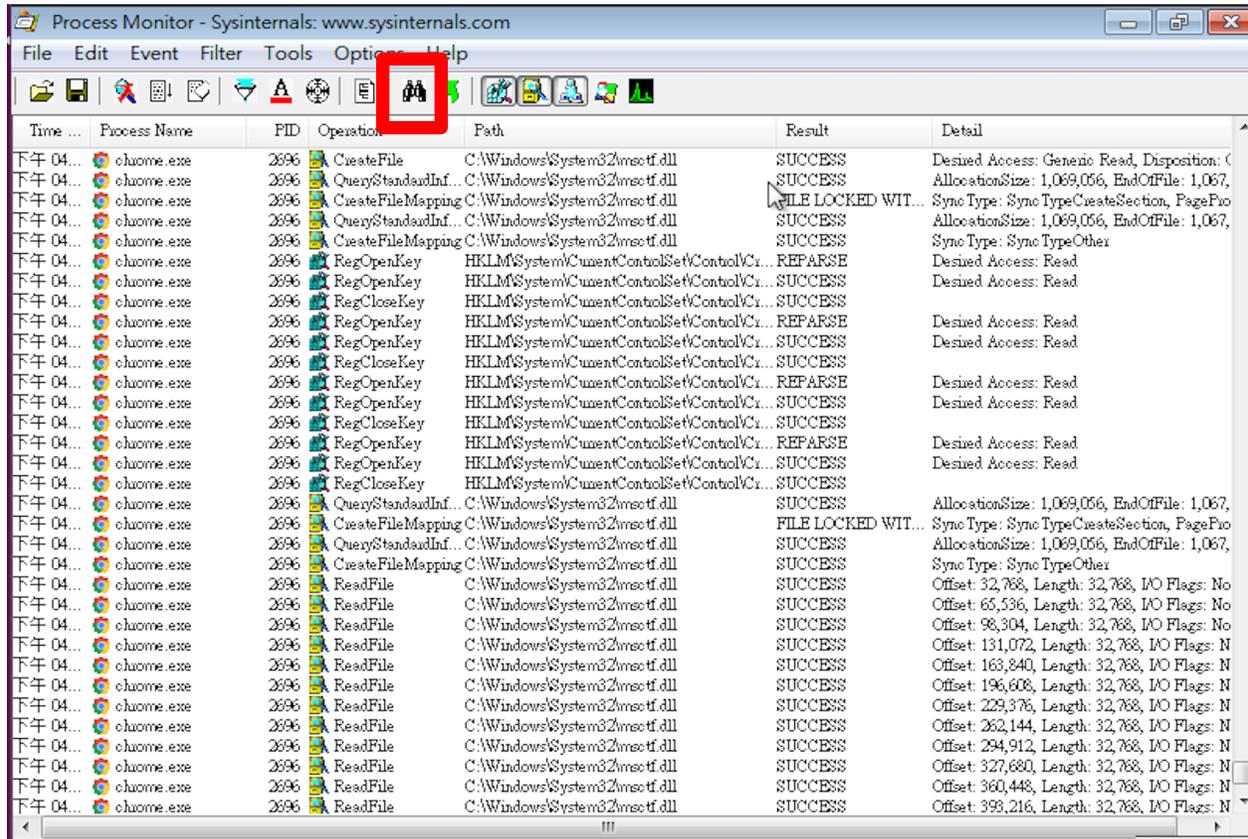
Only show processes still running at end of current trace
 Timelines cover displayed events only

Process	Description	Image Path	Life Time	Company	Owner
Idle (0)		Idle			
System (4)		System			NT AUTHORITY\SYSTEM
smss.exe (232)	Windows 工作階段...	C:\Windows\System...		Microsoft Corporation	NT AUTHORITY\SYSTEM
csrss.exe (300)	用戶端伺服器執...	C:\Windows\system...		Microsoft Corporation	NT AUTHORITY\SYSTEM
csrss.exe (348)	用戶端伺服器執...	C:\Windows\system...		Microsoft Corporation	NT AUTHORITY\SYSTEM
wininit.exe (356)	Windows 啟動應用...	C:\Windows\system...		Microsoft Corporation	NT AUTHORITY\SYSTEM
services.exe (444)	服務及控制站應...	C:\Windows\system...		Microsoft Corporation	NT AUTHORITY\SYSTEM
svchost.exe (556)	Windows Services ...	C:\Windows\system...		Microsoft Corporation	NT AUTHORITY\SYSTEM
wmiprvse.exe (1404)	WMI Provider Host	C:\Windows\system...		Microsoft Corporation	NT AUTHORITY\SYSTEM
DllHost.exe (2648)	COM Surrogate	C:\Windows\system...		Microsoft Corporation	NT AUTHORITY\SYSTEM
DllHost.exe (536)	COM Surrogate	C:\Windows\system...		Microsoft Corporation	NT AUTHORITY\SYSTEM
svchost.exe (636)	Windows Services ...	C:\Windows\system...		Microsoft Corporation	NT AUTHORITY\SYSTEM
svchost.exe (724)	Windows Services ...	C:\Windows\System...		Microsoft Corporation	NT AUTHORITY\SYSTEM
AUDIODG.EXE (2768)	Windows Audio Dev...	C:\Windows\system...		Microsoft Corporation	NT AUTHORITY\SYSTEM
svchost.exe (760)	Windows Services ...	C:\Windows\System...		Microsoft Corporation	NT AUTHORITY\SYSTEM
Dwm.exe (1836)	桌面視窗管理員	C:\Windows\system...		Microsoft Corporation	currentUser

Description:
Company:
Path: Idle
Command:
User:
PID: 0 Started: 2017/6/23 下午 04:25:14

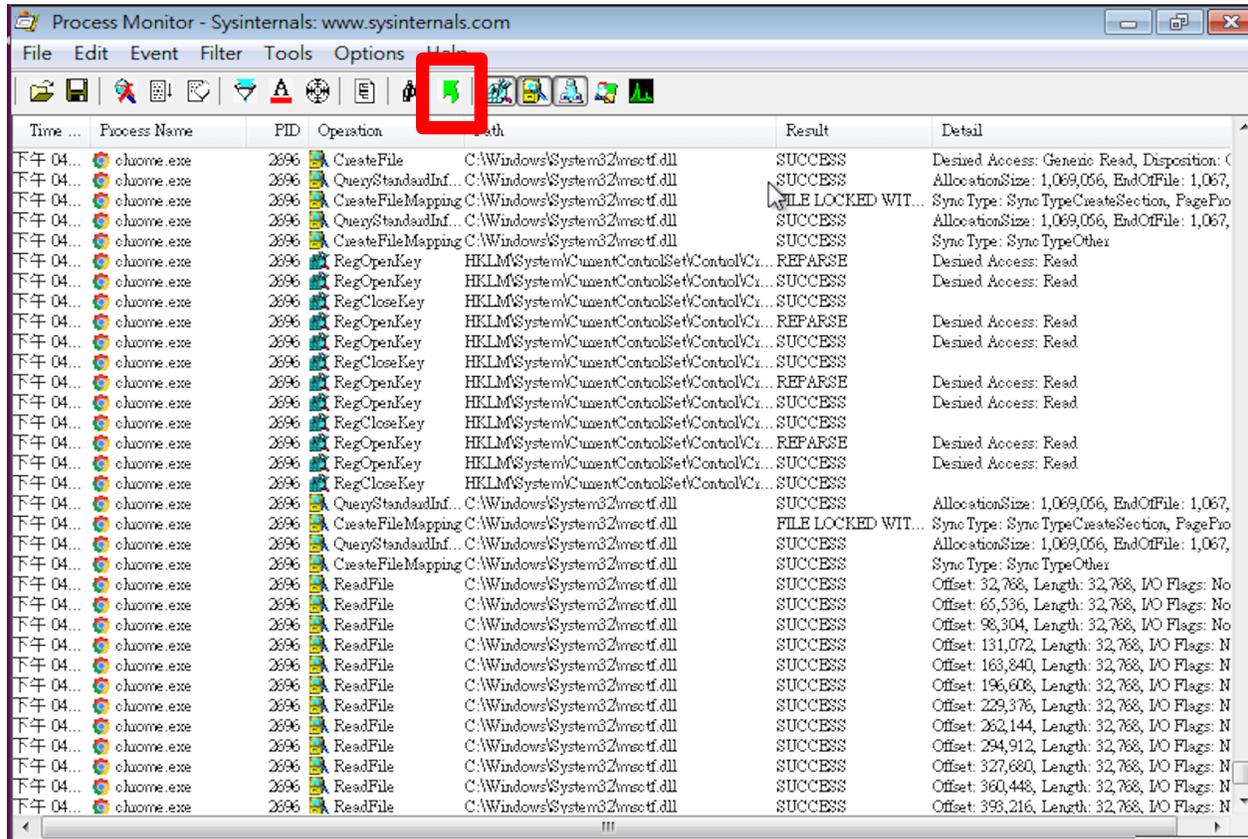
Go To Event Include Process Include Subtree Close

功能介紹



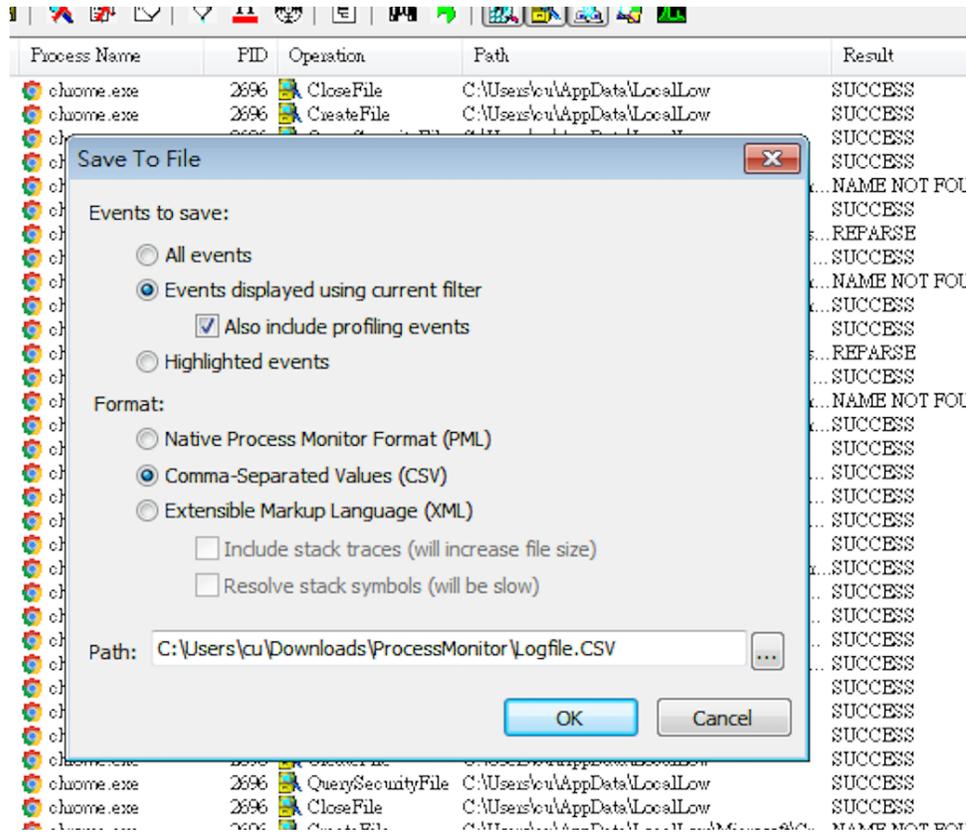
搜尋: 搜尋指定文字

功能介紹



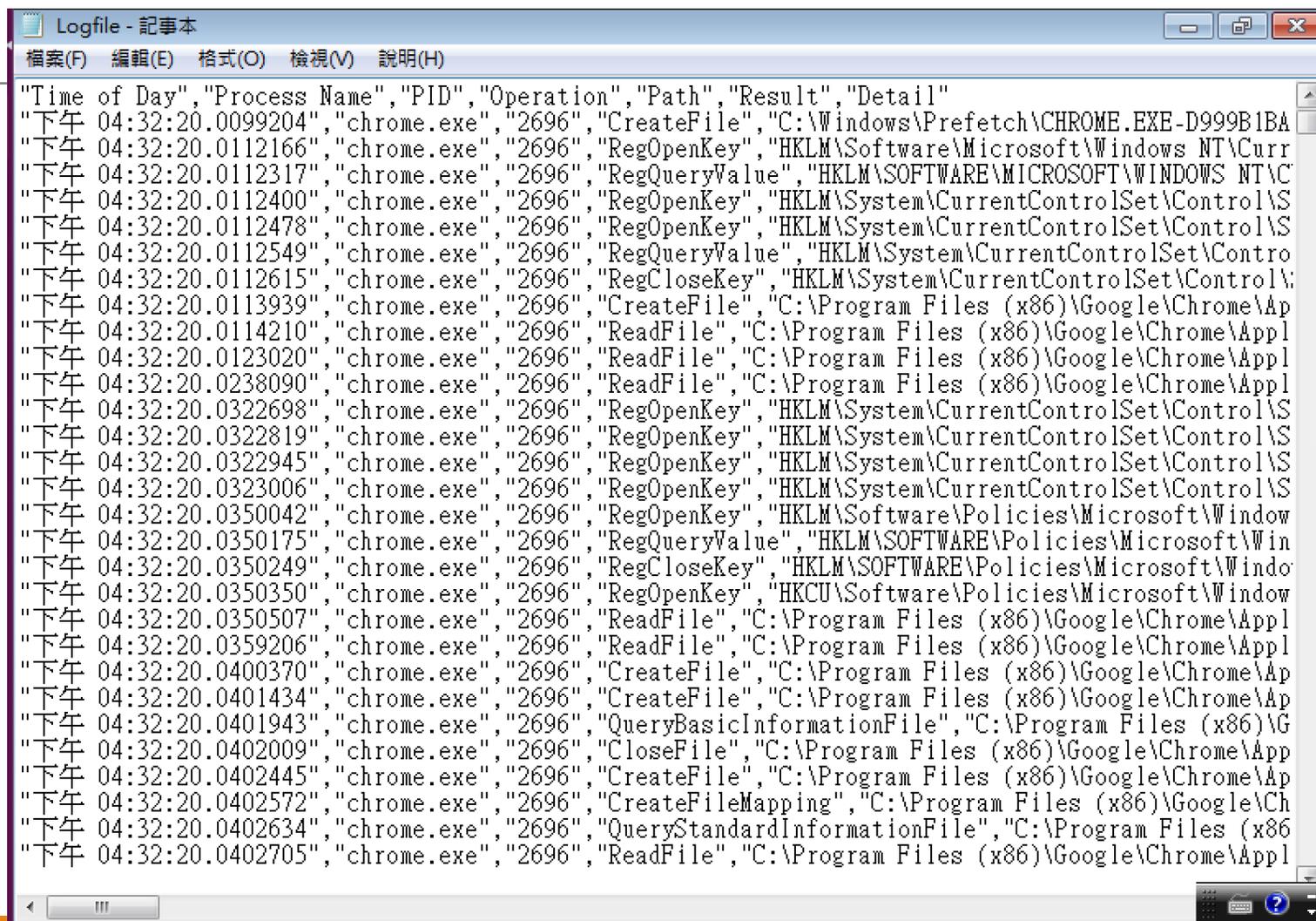
跳至File/ Registry: 跳至File檔案位置/
登陸編輯程式該Registry Key

檔案儲存



可以將所有或部分的紀錄儲存, 可以儲存為不同的格式(PML, CSV, XML)

儲存結果



```
Logfile - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)

"Time of Day","Process Name","PID","Operation","Path","Result","Detail"
"下午 04:32:20.0099204","chrome.exe","2696","CreateFile","C:\Windows\Prefetch\CHROME.EXE-D999B1BA
"下午 04:32:20.0112166","chrome.exe","2696","RegOpenKey","HKLM\Software\Microsoft\Windows NT\Curr
"下午 04:32:20.0112317","chrome.exe","2696","RegQueryValue","HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\C
"下午 04:32:20.0112400","chrome.exe","2696","RegOpenKey","HKLM\System\CurrentControlSet\Control\S
"下午 04:32:20.0112478","chrome.exe","2696","RegOpenKey","HKLM\System\CurrentControlSet\Control\S
"下午 04:32:20.0112549","chrome.exe","2696","RegQueryValue","HKLM\System\CurrentControlSet\Contro
"下午 04:32:20.0112615","chrome.exe","2696","RegCloseKey","HKLM\System\CurrentControlSet\Control\
"下午 04:32:20.0113939","chrome.exe","2696","CreateFile","C:\Program Files (x86)\Google\Chrome\Ap
"下午 04:32:20.0114210","chrome.exe","2696","ReadFile","C:\Program Files (x86)\Google\Chrome\Appl
"下午 04:32:20.0123020","chrome.exe","2696","ReadFile","C:\Program Files (x86)\Google\Chrome\Appl
"下午 04:32:20.0238090","chrome.exe","2696","ReadFile","C:\Program Files (x86)\Google\Chrome\Appl
"下午 04:32:20.0322698","chrome.exe","2696","RegOpenKey","HKLM\System\CurrentControlSet\Control\S
"下午 04:32:20.0322819","chrome.exe","2696","RegOpenKey","HKLM\System\CurrentControlSet\Control\S
"下午 04:32:20.0322945","chrome.exe","2696","RegOpenKey","HKLM\System\CurrentControlSet\Control\S
"下午 04:32:20.0323006","chrome.exe","2696","RegOpenKey","HKLM\System\CurrentControlSet\Control\S
"下午 04:32:20.0350042","chrome.exe","2696","RegOpenKey","HKLM\Software\Policies\Microsoft\Window
"下午 04:32:20.0350175","chrome.exe","2696","RegQueryValue","HKLM\SOFTWARE\Policies\Microsoft\Win
"下午 04:32:20.0350249","chrome.exe","2696","RegCloseKey","HKLM\SOFTWARE\Policies\Microsoft\Windo
"下午 04:32:20.0350350","chrome.exe","2696","RegOpenKey","HKCU\Software\Policies\Microsoft\Window
"下午 04:32:20.0350507","chrome.exe","2696","ReadFile","C:\Program Files (x86)\Google\Chrome\Appl
"下午 04:32:20.0359206","chrome.exe","2696","ReadFile","C:\Program Files (x86)\Google\Chrome\Appl
"下午 04:32:20.0400370","chrome.exe","2696","CreateFile","C:\Program Files (x86)\Google\Chrome\Ap
"下午 04:32:20.0401434","chrome.exe","2696","CreateFile","C:\Program Files (x86)\Google\Chrome\Ap
"下午 04:32:20.0401943","chrome.exe","2696","QueryBasicInformationFile","C:\Program Files (x86)\G
"下午 04:32:20.0402009","chrome.exe","2696","CloseFile","C:\Program Files (x86)\Google\Chrome\App
"下午 04:32:20.0402445","chrome.exe","2696","CreateFile","C:\Program Files (x86)\Google\Chrome\Ap
"下午 04:32:20.0402572","chrome.exe","2696","CreateFileMapping","C:\Program Files (x86)\Google\Ch
"下午 04:32:20.0402634","chrome.exe","2696","QueryStandardInformationFile","C:\Program Files (x86
"下午 04:32:20.0402705","chrome.exe","2696","ReadFile","C:\Program Files (x86)\Google\Chrome\Appl
```

Noriben

Nori-Ben = seaweed lunchbox

Simplest "box" to make

Cheap

Minimal ingredients



Noriben

- Simple Malware Analysis Sandbox:
 - Wrapper for Microsoft SysInternals Process Monitor(ProcMon)
- Build a Sandbox VM with just:
 - Noriben.py
 - Procmin.exe

Optional:

- Extra Procmon binary filter
- YARA signature files
- Virustotal API Key
- Add new filter to the script

Goal of Noriben

- Quick malware analysis results
- Flexibility for open-ended runs (manually stopped analysis)
- Allow for user interaction
- Analysis of
 - GUI apps
 - Command line args
 - Malware requiring debugging (Z-flag, code/memory altering)
 - Long sleeps (hours, days)

Noriben focus on:

- Processes, File activity, Registry Activity, Network Activity
- Log high level API calls while filtering out known noise
 - Thumbnail creation
 - Prefetch creation
 - Explorer registry key(MRUs)
 - RecentDocs
 - Malware analysis tools (CaptureBat, IDA, FakeNet)
 - VMWare tools
 - Java updater

Strat Noriben

Open "CMD" with administration

Run `path/to/python.exe path/to/noriben.py`

Compare with cuckoo sandbox

	Cuckoo Sandbox	Noriben
Spend time(sample/sec) time-out 120s	140s	230s
Simulate human activity	Yes(just random move mouse)	No
Memory dump	Plugin(volatility)	No
Static Analysis(Strings, PE header, ...)	Yes	No
Interface	Web and console	Just console
Network Analysis	Use wireshark catch package and analysis	Just analysis windows api
Report	Json and use web present	Just CSV
Portable	Slightly complicated	Very easy to use
Analysis range	Only Malware and process spawned by Malware	Whole systems