惡意程式分析組

病毒不再神秘 - 讓我們支解惡意行為！

HITCON GIRLS 資安女孩

- **HITCON GIRLS**
  - 由一群對資安有興趣，想學習更多技術的女孩們所組成。
- 讀書會
  - 我們分成不同的組別，進行討論、學習和互補，惡意程式分析組針對 **Malware** 進行分析，內容其中包含各種動態工具以及反組譯的討論。

成員介紹

成員

Turkey
台灣駭客協會 秘書
唯一的台灣駭客協會正職XD

珣珣
輔仁大學資訊工程所 碩一
NISRA 成員

成員介紹

教練

Lucas
任職於趨勢科技

Charles
任職於Team T5

Joey
台灣科技大學 資訊管理所

資安學習地圖

- 資訊收集
  Information Gathering
- 網路安全
  Network Security
- 網站與網頁應用程式安全
  Web Security
- 系統安全
  System Security
- 加密與解密
  Cryptography
- 惡意程式檢測
  Malware Detection
- 逆向工程
  Reversing Engineering
- 數位鑑識
  Digital Forensics
- 行動裝置
  Mobile Devices

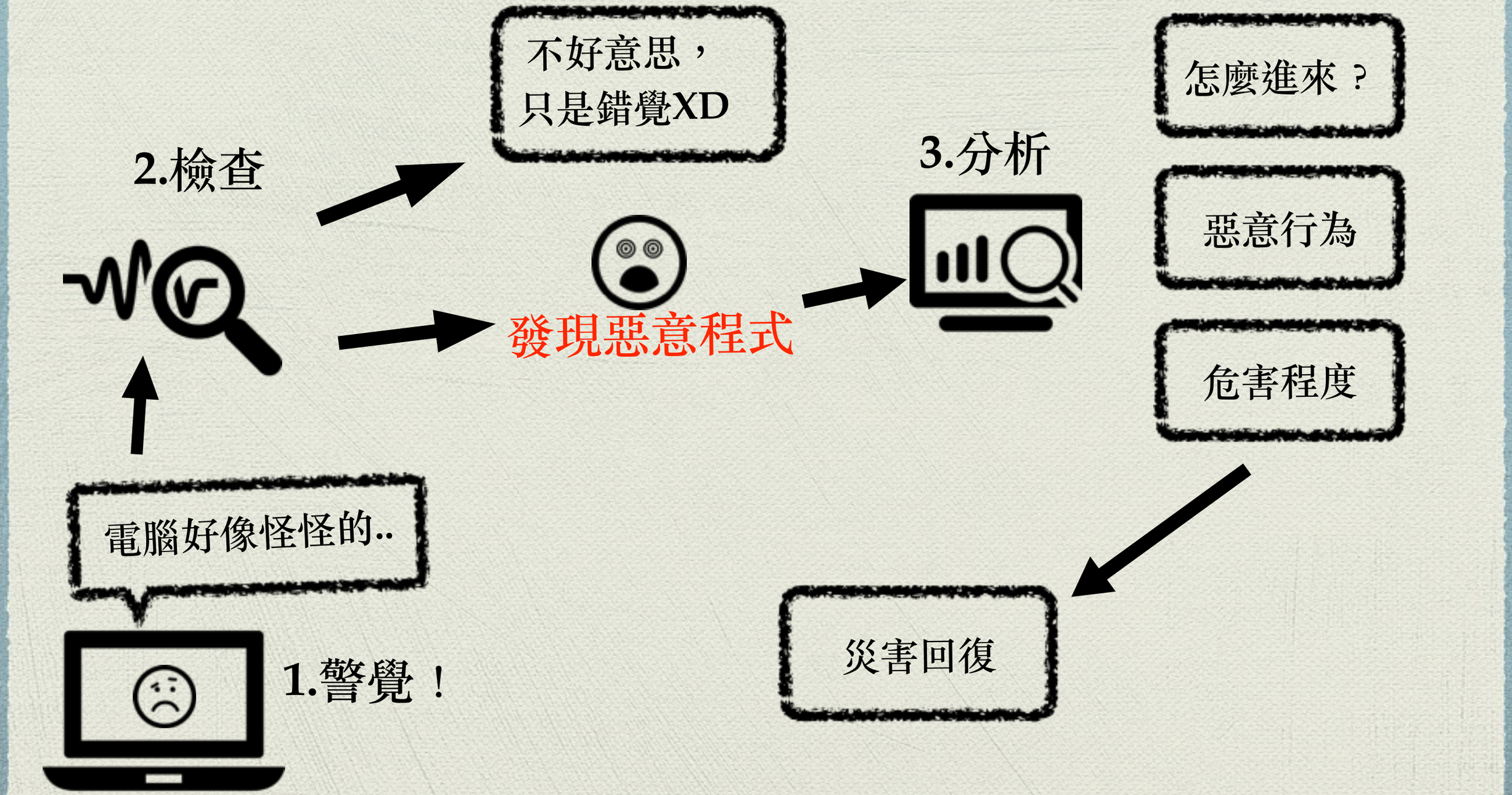
資安學習地圖

- 「數位鑑識」 **Digital Forensics**
  - 覺得家裡好像有被侵入過，於是做一些檢查。
- 「惡意程式檢測」 **Malware Detection**
  - 廚房地板上發現一顆炸彈，移動到安全環境做檢驗。
- 「逆向工程」 **Reversing Engineering**
  - 理解運作原理、威脅性，反向尋找兇手

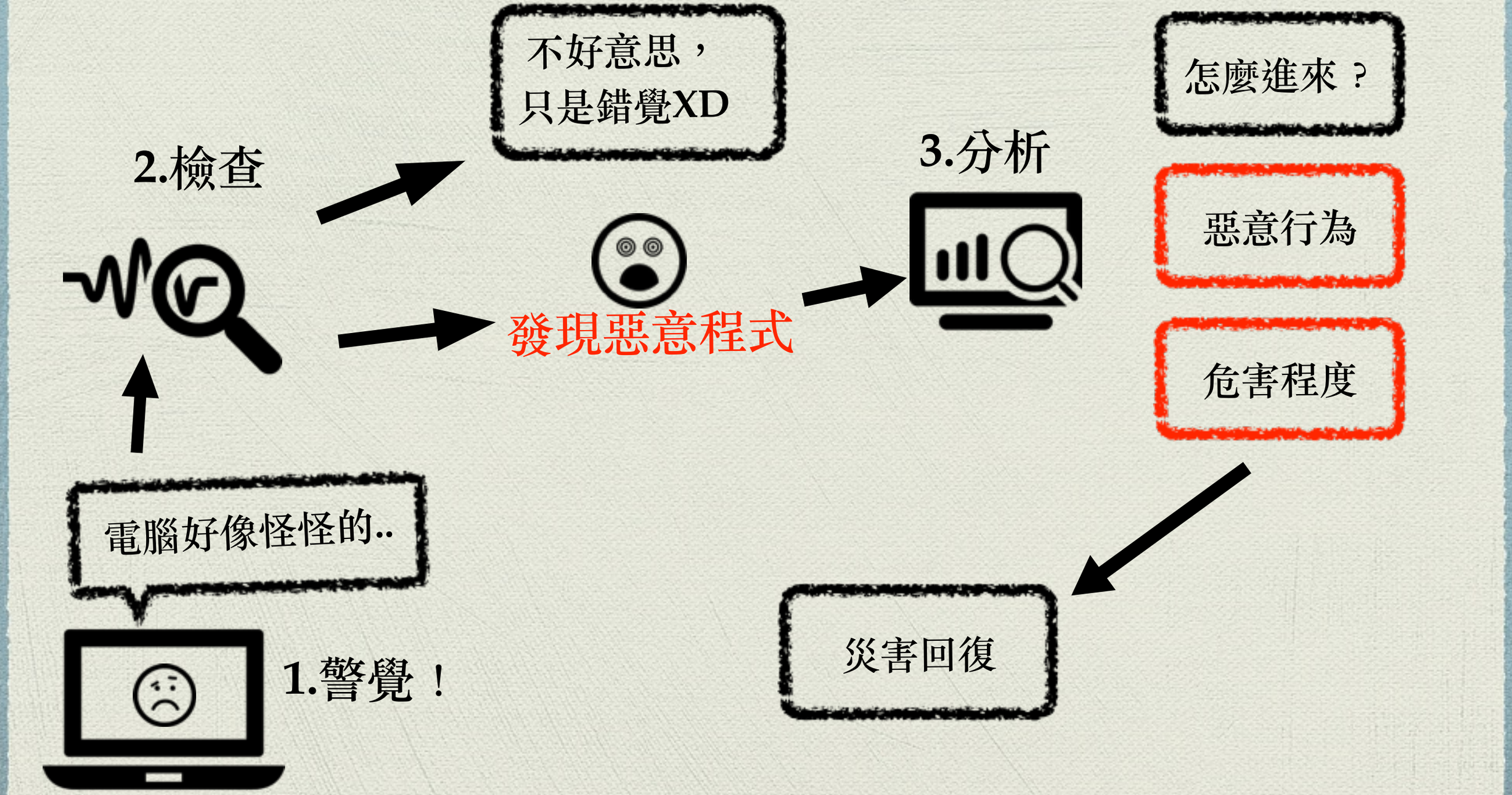
學習框架

- 惡意程式淺談
  - 何謂惡意程式？
- 【手動分析】從三大層面來分析惡意程式
  - **Registry、Process、網路**
  - 工具介紹
- 【自動分析】**SandBox**介紹
- 逆向工程

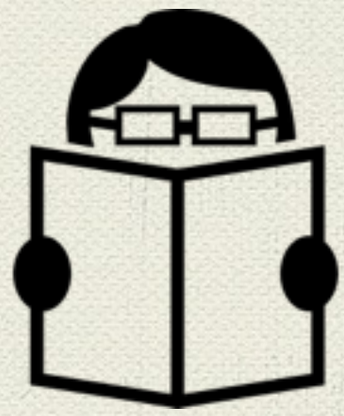
組別定位



組別定位



惡意程式淺談



何謂惡意程式(Malware)

- 定義
  - 蓄意撰寫來破壞電子裝置或竊取資料的程式

何謂惡意程式(Malware)

- 條件特徵

強行安裝

抵制移除

強行彈出廣告

干擾、佔用系統資源

停用防毒軟體或其他電腦管理程式來做進一步的破壞

強行修改使用者軟體設定

非允許之下，紀錄使用者資訊

與電腦病毒聯合侵入用戶電腦

……

何謂惡意程式(Malware)

- **Grayware 的存在**
  - 具備下列特徵的應用程式
    - 具有擾人的行為模式
    - 令人排斥
    - 令人難以察覺
- 介於「好軟體」與「壞病毒」的灰色地帶
- 就跟槍一樣，拿來打壞人就是伸張正義，拿來打好人就是惡意

【手動分析】

從三大層面來分析惡意程式

惡意程式分析的層面

- **Registry Key**
- **Process**
- 網路連線

惡意程式分析的層面

- **Registry Key → 使用工具：AutoRuns**
- Process
- 網路連線

惡意程式的分析- Registry Key

- 惡意程式為了隨系統自動啟動，會在**Registry**建立啟動項

- **Registry小知識**

名稱	作用
HKEY_CLASSES_ROOT	儲存Windows可辨識的檔案類型的詳細清單，以及相關聯的程式。
HKEY_CURRENT_USER	儲存當前使用者設定的資訊。
HKEY_LOCAL_MACHINE	包括安裝在電腦上的硬體和軟體的資訊。
HKEY_USERS	包含使用電腦的使用者的資訊。
HKEY_CURRENT_CONFIG	這個分支包含電腦當前的硬體配置資訊。

前備小知識 - Registry

- 登錄檔/註冊表
- 惡意程式為了隨系統自動啟動，會在Registry建立啟動項
- **Registry小知識**
  - 用於儲存系統和應用程式的設計資訊
  - **C:\Windows\regedit.exe**

前備小知識 - 啟動項

- 每次開機就會有一個人自動出現，準備做事
- 這就是啟動項！
- **Registry 中開機先執行的項目，就是啟動項**

前備小知識 - 啟動項

- **HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run**
- 使用者一登入，該程式就自動執行

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				
webHancer Agent	webHancer Customer Companion	(Not verified) webHancer C...	c:\program files\webhancer\programs\whagent.exe
webHancer Survey Companion	webHancer Survey Companion	(Not verified) webHancer C...	c:\program files\webhancer\programs\whsurvey.exe
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects				
WhleHelperObj Class	webHancer IE Helper Module	(Not verified) webHancer C...	c:\program files\webhancer\programs\whiehlpr.dll
HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries				
000000000001	webHancer Winsock2 SPI	(Not verified) webHancer C...	c:\windows\webhdll.dll
000000000001	Microsoft Windows Sockets 2.0 Service Provider	Microsoft Corporation	c:\windows\system32\mswsock.dll
000000000002	webHancer Winsock2 SPI	(Not Verified) webHancer C...	c:\windows\webhdll.dll
000000000002	Microsoft Windows Sockets 2.0 Service Provider	Microsoft Corporation	c:\windows\system32\mswsock.dll
000000000004	Microsoft Windows Rsvp 1.0 Service Provider	Microsoft Corporation	c:\windows\system32\rsvpsp.dll
000000000005	Microsoft Windows Rsvp 1.0 Service Provider	Microsoft Corporation	c:\windows\system32\rsvpsp.dll
000000000006	Microsoft Windows Sockets 2.0 Service Provider	Microsoft Corporation	c:\windows\system32\mswsock.dll
000000000007	Microsoft Windows Sockets 2.0 Service Provider	Microsoft Corporation	c:\windows\system32\mswsock.dll
000000000012	VSockets Library	VMware, Inc.	c:\program files\vmware\vmware tools\vsock sdk\bin\win32\vsocklib.dll
000000000013	VSockets Library	VMware, Inc.	c:\program files\vmware\vmware tools\vsock sdk\bin\win32\vsocklib.dll
000000000014	VSockets Library	(Not Verified) VMware, Inc.	c:\program files\vmware\vmware tools\vsock sdk\bin\win32\vsocklib.dll
000000000015	VSockets Library	(Not Verified) VMware, Inc.	c:\program files\vmware\vmware tools\vsock sdk\bin\win32\vsocklib.dll
000000000016	webHancer Winsock2 SPI	(Not Verified) webHancer C...	c:\windows\webhdll.dll

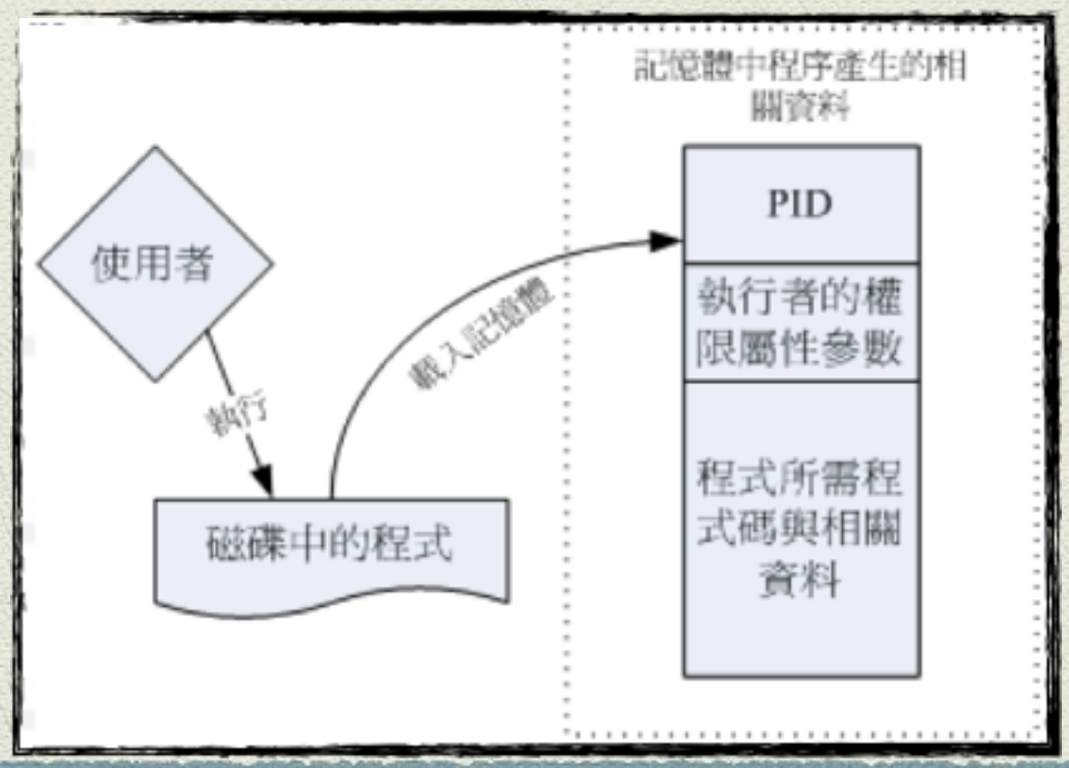
惡意程式分析的層面

- Registry Key
- **Process → 使用工具：ProcessExplorer**
- 網路連線

前備小知識 - Process

- 觸發程式 → 被載入記憶體 → 產生程序了！
- 程序 (process)

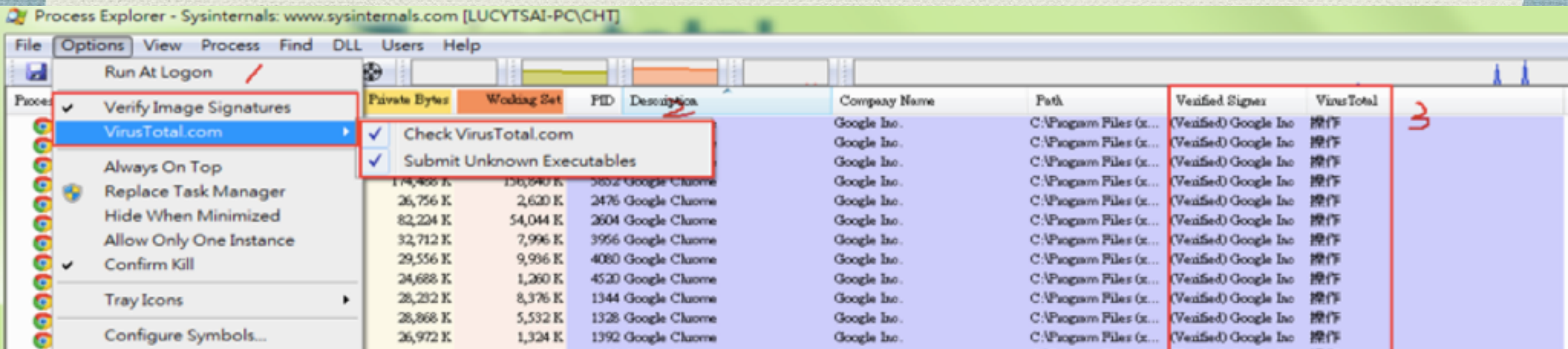
可以說就是一個正在運作中的程式。



分析惡意程式工具 - ProcessExplorer

- **ProcessExplorer -** 記憶體中在執行的所有程序及其目錄

- 作用類似於工作管理員，優點在於可以顯示

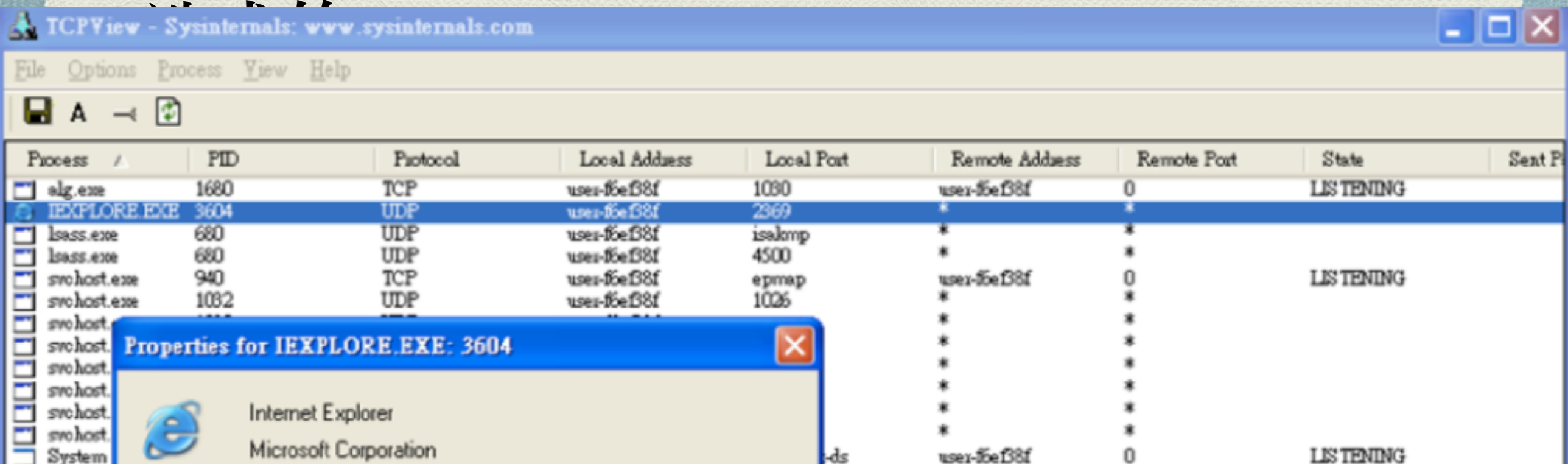


惡意程式分析的層面

- Registry Key
- Process
- 網路連線 → 使用工具：**TCPView**

分析惡意程式工具 - TCPView

- **TCPView - 記錄對外連線**
- **顯示連線記錄、每筆連線記錄是由哪支程式**



小節

- **Registry Key → 使用工具：AutoRuns**
- **Process → 使用工具：ProcessExplorer**
- 網路連線 → 使用工具：**TCPView**

【自動分析】

從三大層面來分析惡意程式

線上的自動分析網站

- 線上 **SandBox**
  - **Virustotal**
  - **Anubis**
  - **Comodo**

SandBox 介紹

- 是一個受限制的環境，是一種安全機制，為執行中的程式提供的隔離環境。
- 通常是作為一些來源不可信、具破壞力或無法判定程式意圖的程式提供實驗之用。

SandBox 線上服務 - Anubis

Anubis - Malware Analysis for Unknown Binaries

Home | Advanced Submission | Clustering | News | About | Sample Reports | Links

register / login

Task Overview

Task ID:	11e4f35b66d743584e906d2b7802a794a
File Name:	01.exe
MD5:	39870818c55a5212c06fda94b0228b27
Analysis Submitted:	2015-06-28 03:47:52
Analysis Started:	2015-06-28 03:47:58
Analysis Ended:	2015-06-28 03:47:58
Created New Analysis Report:	No - The Analysis report was created on 2013-12-27 20:35:03.
Available Report Formats:	HTML XML PDF Text

- Monitored Registry Keys:

Key Name	Watch subtree	Notify Filter	Count
HKLM\Software\Classes	1	Key Change,Value Change	3
HKLM\Software\Classes\CLSID	1	Key Change,Value Change	2
HKLM\Software\Microsoft\COM3	1	Key Change,Value Change	6
HKLM\system\CurrentControlSet\control\NetworkProvider\HwOrder	0	Value Change	1
HKU	1	Key Change,Value Change	3

SandBox 線上服務 - Comodo

Comodo Instant Malware Analysis

- **File Info**

Name	Value
Size	32768
MD5	39870818c55a5212c06fda94b0228b27
SHA1	075c5f1126c1fc91830a6aa3440fc8bfeae94331
SHA256	bce767fa626065f5aa10d23be05041b9efc9e3eb74d9a555131500ee214aa858
Process	Active

- **Keys Created**
- **Keys Changed**
- **Keys Deleted**
- **Values Created**

Name	Type	Size	Value
LM\Software\Microsoft\Windows\CurrentVersion\Run\redirect	REG_SZ	44	"C:\TEST\redirect2.exe"

SandBox 線上服務 - Virustotal

分析 | 檔案詳細資料 | 其他資訊 | 評論 0 | 投票

防毒	結果	更新
AVG	Clicker.EIV	20141006
AVware	DotComToolbar	20141004
Ad-Aware	Gen:Trojan.Heur.VP.cm0@a0oDWFni	20141006
Agnitum	Trojan.CL.DotComToolBar!8rDzAaBuGh4	20141005
AhnLab-V3	Win-Trojan/Dotcomtoolbar.32768.B	20141006
Antiy-AVL	Trojan[Clicker]/Win32.DotComToolBar	20141006
Avast	Win32:VB-FOQ [Wrm]	20141006
Avira	TR/VB.Downloader.Gen	20141006
Baidu-International	Trojan.Win32.DotComToolBar.aLT	20141006
BitDefender	Gen:Trojan.Heur.VP.cm0@a0oDWFni	20141006
Bkav	W32.Clodce3.Trojan.028b	20141003
CMC	Generic.Win32.39870818c5!MD	20141004
Comodo	TrojWare.Win32.TrojanClicker.DotComToolBar.A	20141006

聽到這邊你一定會有疑惑……

- 為什麼需要手動又自動化？用一種方法測試不就好了嗎？

聽到這邊你一定會有疑惑……

- 為什麼需要手動又自動化？用一種方法測試不就好了嗎？
  - 部分行為是模糊的，正常軟體有此行為，惡意程式也會有，因此很難單純以行為做為是否惡意的評斷
  - 比較狡猾的惡意程式可能會躲避常用的工具、或是讓 SandBox 無法檢測出

篩選的能力	加殼	經驗不足
透過工具可以收集到很多資訊，卻不確定是否相關，需要培養篩選資訊的能力	惡意程式進行加殼，會是新的關卡	一次分析需要大量的時間反覆確認

中場小結

如果遇到無法分析的狀況

- 假設狀況是，工具無法分析、**SandBox** 沒有結果，就需要...最後的絕招

- 每個主角都有不想祭出的最後絕招
- 可能會對自身造成傷害
  - ……最後拿出來才帥啊！！！
  - 啊就傲嬌嘛

「啊啊，我本來不想用這招的」

「天啊！是逆向工程！」

逆向工程

- 逆向工程 **Reverse Engineering**
- 泛稱對目標進行逆向分析及研究，得出其流程、結構

逆向工程

- 逆向工程 **Reverse Engineering**
- 泛稱對目標進行逆向分析及研究，得出其流程、結構

Sourcecode……你們在哪裡？

- 惡意程式 **.EXE** 居多
- **.exe (executable file)** 通稱執行檔

他……看不到原始碼啊啊啊！

逆向工程……我們要分析的是？

- 遠古時代嗚嘎嚇嘎 - 機器語言
  - 系統a呢，其實只認得 0 和 1
- 我們稱做為 Binary

```
B8  000001100
05  000000400
2D  000000200
```

?

逆向工程……我們要分析的是？

- 喔喔喔已知用火！ - 組合語言
  - 從 0 和 1 延伸出一種神奇的東西
  - 簡短的指令，讓人類能讀能寫

```
B8  00000100    MOV EAX,10000
05  00000400    ADD EAX,40000
2D  00000200    SUB EAX,20000
```

? → !

逆向工程……我們要分析的是？

- 組合語言挑戰了人類閱讀的極限
- 所以現在有許多高階語言，好讀好寫好親切

機器語言 → 組合語言 → 高階語言

逆向工程……我們要分析的是？

- 組合語言挑戰了人類閱讀的極限
- 所以現在有許多高階語言，好讀好寫好親切

機器語言 → 組合語言 → 高階語言

.EXE

逆向工程……我們要分析的是？

- 組合語言挑戰了人類閱讀的極限
- 所以現在有許多高階語言，好讀好寫好親切

機器語言 → 組合語言 → 高階語言

.EXE

「啊啊，我本來不想用這招的」

因為你們可能會睡著

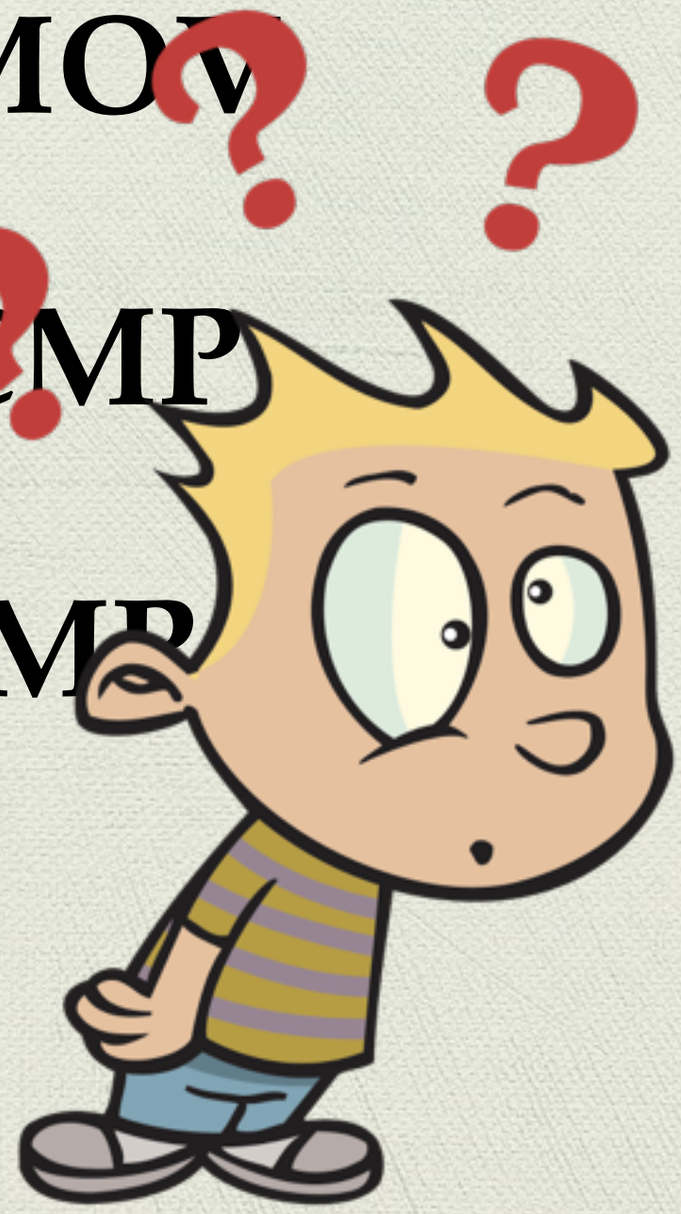
我們進入鑽木取火時代囉ಠ_ಠ

親愛的程式碼我們來惹

ヾ(*´∀｀*)...

逆向工程 - 組合語言

- MOV
- CMP
- JMP



你在說什麼？
呼嘎蝦嘎呼嚕達？

逆向工程 - 組合語言

- **MOV** → **(Move) 移動**
- **CMP** → **(Compare) 比較**
- **JMP** → **(Jump) 跳躍**

逆向工程 - 組合語言

- **MOV (Move) 移動**

```
mov  edx,8000h
mov  eax,4h
```

逆向工程 - 組合語言

- **MOV (Move) 移動**

```
mov  edx,8000h
mov  eax,4h
```

EDX

EAX

逆向工程 - 組合語言

- **MOV (Move) 移動**

```
mov  edx,8000h
mov  eax,4h
```

8000h

EDX

EAX

逆向工程 - 組合語言

- **MOV (Move) 移動**

```
mov  edx,8000h
mov  eax,4h
```

EDX = 8000h

EAX

逆向工程 - 組合語言

- **MOV (Move) 移動**

```
mov  edx,8000h
mov  eax,4h
```

EDX = 8000h

EAX

4h

逆向工程 - 組合語言

- **MOV (Move) 移動**

```
mov  edx,8000h
mov  eax,4h
```

EDX = 8000h

EAX = 4h

逆向工程 - 組合語言

- **MOV (Move) 移動**

```
mov  edx,8000h
mov  eax,4h
```

EDX = 8000h

EAX = 4h

換句話說

edx = 8000h

eax = 4h

h 是 16 進位的意思

逆向工程 - 組合語言

- **CMP (Compare) 比較**
- **JMP (Jump) 跳躍**

```
cmp edx,eax
ja NextLoop
```

逆向工程 - 組合語言

- **CMP (Compare) 比較**
- **JMP (Jump) 跳躍**

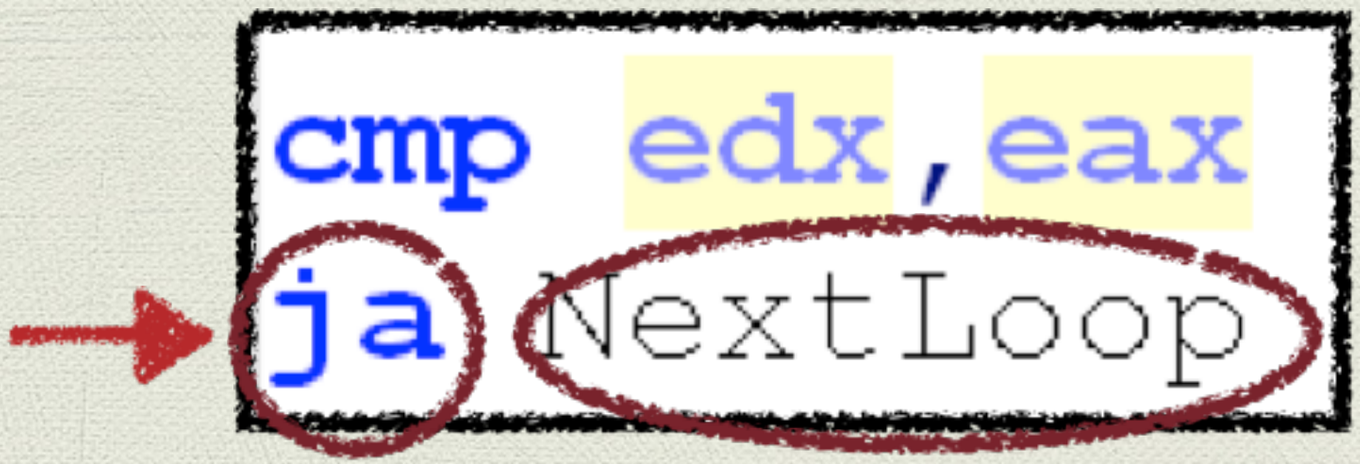
```
cmp edx,eax
ja NextLoop
```

EDX = 8000h

EAX = 4h

逆向工程 - 組合語言

- **CMP (Compare) 比較**
- **JMP (Jump) 跳躍**



EDX = 8000h **VS** **EAX = 4h**

If Above, Jump to NextLoop

逆向工程 - 組合語言

- **CMP (Compare) 比較**
- **JMP (Jump) 跳躍**

NextLoop

```
cmp edx,eax
ja NextLoop
```

EDX = 8000h **VS** **EAX = 4h**

If Above, Jump to NextLoop

逆向工程 - 組合語言

- **CMP (Compare) 比較**
- **JMP (Jump) 跳躍**

EDX = 8000h **VS** **EAX = 4h**

If Above, Jump to NextLoop

逆向工程 - 組合語言

NextLoop

- **CMP (Compare) 比較**
- **JMP (Jump) 跳躍**

```
cmp edx,eax
ja NextLoop
```

EDX = 8000h **VS** **EAX = 4h**

If Above, Jump to NextLoop

逆向工程 - 組合語言

- **CMP (Compare) 比較**
- **JMP (Jump) 跳躍**

NextLoop

```
cmp  edx,eax
ja   NextLoop
```

EDX = 8000h **VS** **EAX = 4h**

If Above, Jump to NextLoop

逆向工程 - 組合語言

- **JMP (Jump) 跳躍**
  - 數字一定是正號或負號
- 兩個數字的關係一定是三一律
  - 等於 =
  - 大於 >
  - 小於 <

逆向工程 - 組合語言

- **JMP (Jump) 跳躍**
  - 數字一定是正號或負號
- 兩個數字的關係一定是三一律
  - 等於 =
  - 大於 >
  - 小於 <

	意義	無號	有號
x = y	Equal	JE	JE
x > y	Above, Greater	JA	JG
x < y	Below, Less	JB	JL

逆向工程 - 組合語言

- **MOV (Move) 移動**
- **CMP (Compare) 比較**
- **JMP (Jump) 跳躍**
  - **如果有需要，不妨回頭查表格！**
  - **不一定與 CMP 並存**

逆向工程 - 組合語言

- **Push 與 Pop**

- **Call 呼叫**
  - 呼叫副程式！

逆向工程

- 反組譯
  - 逆向工程應用在軟體裡的其中一種方法
  - 把機器碼轉換成組合語言
- 分成動態和靜態兩種手法
  - 動態分析，必須運作該程式
  - 靜態分析，不運作該程式

逆向工程 - 靜態與動態分析優缺點

	動態分析	靜態分析
優	• 可知執行時的真實行為 • 可信度高	• 分析範圍較大、較完整 • 不受特定招數影響 • 不需要運行程式
缺	• 容易被躲避 • 需要運行程式	• 被混淆的程式碼分析困難 • 無法得知執行時的資訊

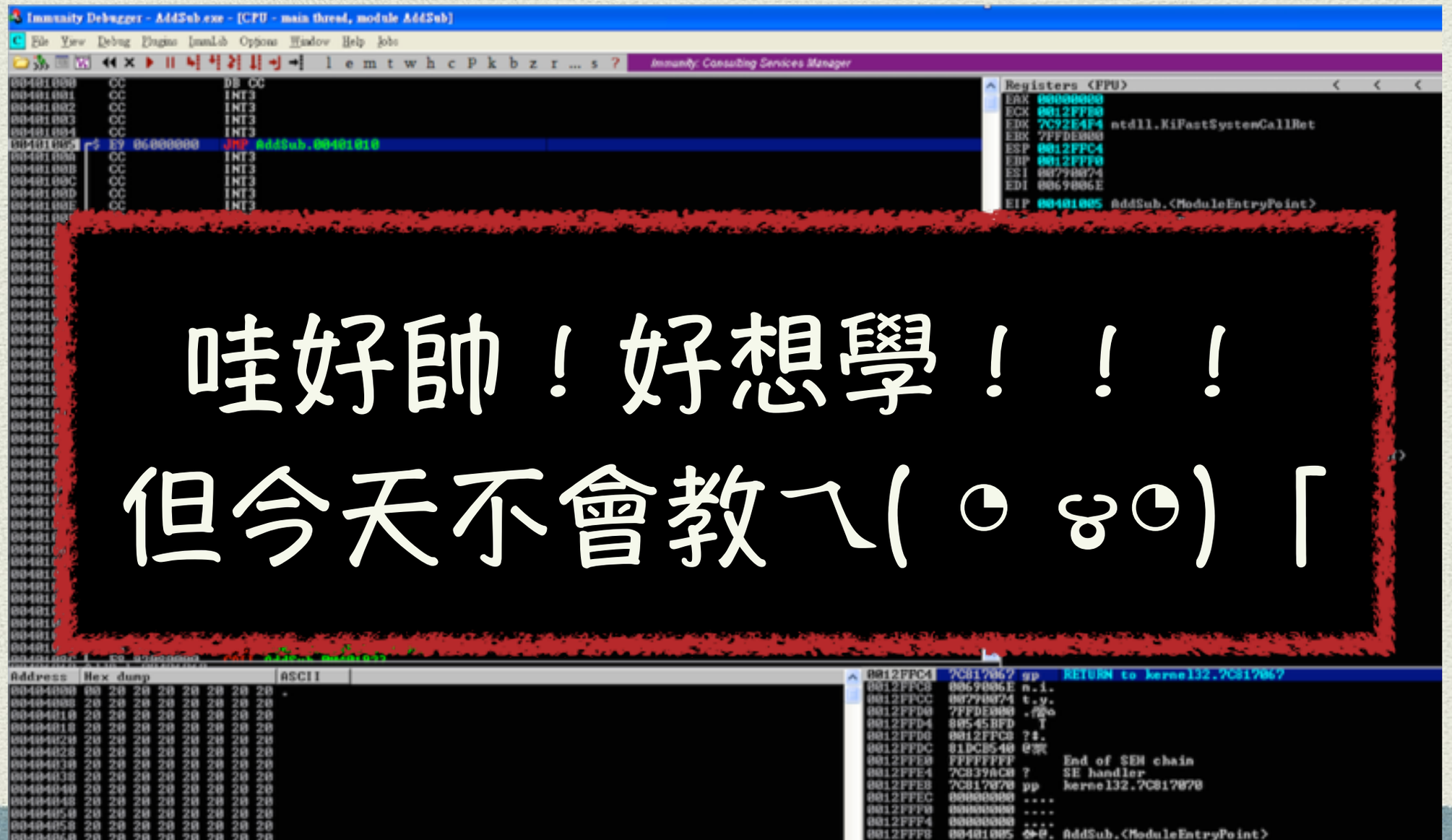
動態分析 - 工具

- **Immunity Debugger 哈囉！、(´∀`)…**

- **Olly Dbg 說你好！、(◦∀◦)…**

動態分析 - 工具

- **Immunity Debugger 哈囉！、(´∀`)…**



靜態分析 - 工具

- IDA 安安！、(´∀`)...

- IDA Pro，為Interactive Disassembler公司的反組譯與除錯產品。常用於逆向工程。

靜態分析 - 工具

```
.text:00401010 ; Attributes: noreturn
.text:00401010
.text:00401010 start_0          proc near               ; CODE XREF: startîj
.text:00401010                  mov     edx, offset aHelloWorld ; "Hello World!\n\r"
.text:00401015                  call    sub_401933
.text:0040101A                  mov     edx, offset aHowTallAreYou? ; "How tall are you?\n\r"
.text:0040101F                  call    sub_401933
.text:00401024                  call    sub_401580
.text:00401029                  call    sub_4010BF
.text:0040102E                  cmp     eax, 0BEh
.text:00401033                  jb      short loc_401041
.text:00401035                  mov     edx, offset aYesYouHave190Y ; "Yes! You have 190! You are Gay!
.text:0040103A                  call    sub_401933
.text:0040103F                  jnb     short loc_40104B
.text:00401041
.text:00401041 loc_401041:                              ; CODE XREF: start_0+23îj
.text:00401041                  mov     edx, offset aNoYouCanNotPla ; "No! You can not play :<\n\r"
.text:00401046                  call    sub_401933
.text:0040104B
.text:0040104B loc_40104B:                              ; CODE XREF: start_0+2Fîj
.text:0040104B                  mov     edx, offset aILoveNisra ; "I love nisra!\n\r"
.text:00401050                  call    sub_401933
.text:00401055                  push    0               ; uExitCode
.text:00401057                  call    ExitProcess
.text:00401057 start_0          endp
.text:00401057
.text:00401057 ; ---------------------------------------------------------------------------
.text:0040105C                  db 14h dup(0CCh)
.text:00401070 ; ---------------------------------------------------------------------------
```

靜態分析 - 工具

記憶體位置

```
text:004 return
text:00401010
text:00401010 start_0         proc near               ; CODE XREF: start↑j
text:00401010                 mov     edx, offset aHelloWorld ; "Hello World!\n\r"
text:00401015                 call    sub_401933
text:0040101A                 mov     edx, offset aHowTallAreYou? ; "How tall are you?\n\r"
text:0040101F                 call    sub_401933
text:00401024                 call    sub_401580
text:00401029                 call    sub_4010BF
text:0040102E                 cmp     eax, 0BEh
text:00401033                 jb      short loc_401041
text:00401035                 mov     edx, offset aYesYouHave190Y ; "Yes! You have 190! You are Gay!
text:0040103A                 call    sub_401933
text:0040103F                 jnb     short loc_40104B
text:00401041
text:00401041 loc_401041:                             ; CODE XREF: start_0+23↑j
text:00401041                 mov     edx, offset aNoYouCanNotPla ; "No! You can not play :<\n\r"
text:00401046                 call    sub_401933
text:0040104B
text:0040104B loc_40104B:                             ; CODE XREF: start_0+2F↑j
text:0040104B                 mov     edx, offset aILoveNisra ; "I love nisra!\n\r"
text:00401050                 call    sub_401933
text:00401055                 push    0               ; uExitCode
text:00401057                 call    ExitProcess
text:00401057 start_0         endp
text:00401057
text:00401057 ; ---------------------------------------------------------------------------
text:0040105C                 db 14h dup(0CCh)
text:00401070 ; ---------------------------------------------------------------------------
```

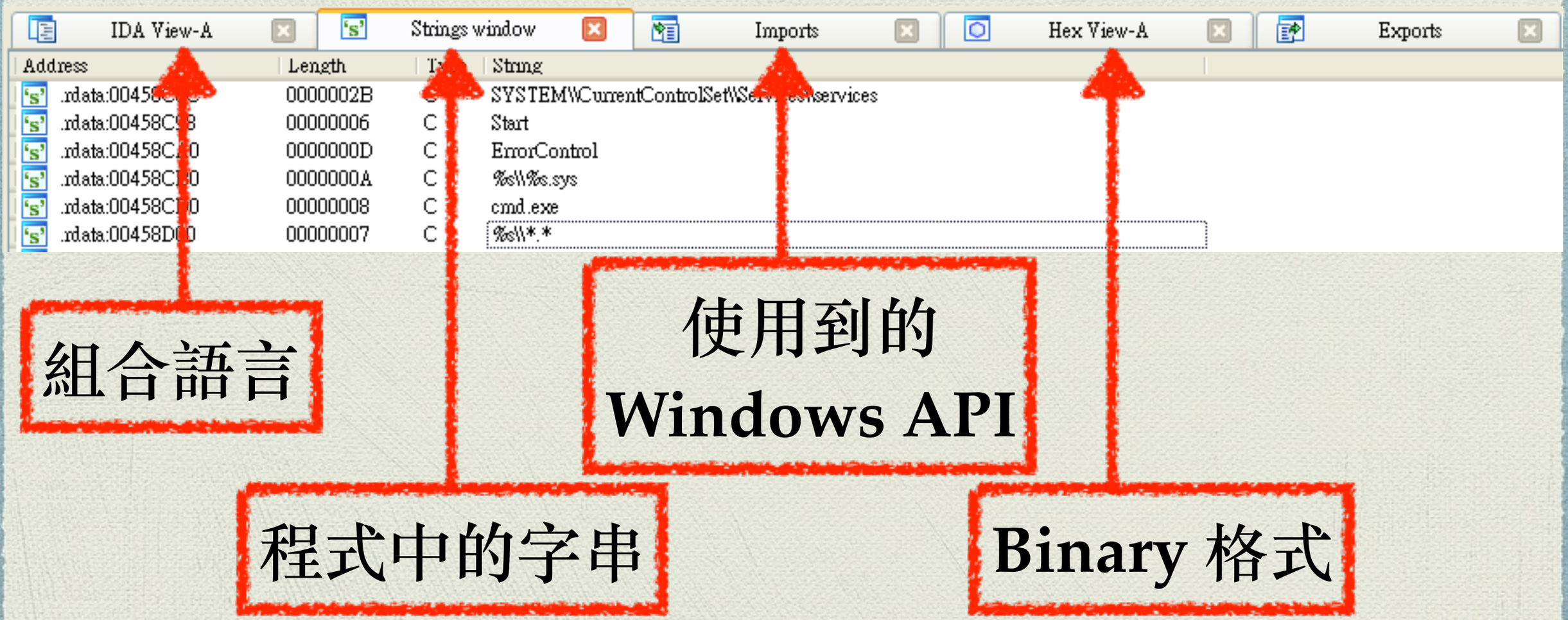
靜態分析 - 工具

這裡都是組合語言啊啊啊

```
.text:00401010 start_0         proc near               ; CODE XREF: startîj
.text:00401010                 mov     edx, offset aHelloWorld ; "Hello World!\n\r"
.text:00401015                 call    sub_401933
.text:0040101A                 mov     edx, offset aHowTallAreYou? ; "How tall are you?\n\r"
.text:0040101F                 call    sub_401933
.text:00401024                 call    sub_401580
.text:00401029                 call    sub_4010BF
.text:0040102E                 cmp     eax, 0BEh
.text:00401033                 jb      short loc_401041
.text:00401035                 mov     edx, offset aYesYouHave190Y ; "Yes! You have 190! You are Gay!
.text:0040103A                 call    sub_401933
.text:0040103F                 jnb     short loc_40104B
.text:00401041
.text:00401041 loc_401041:                             ; CODE XREF: start_0+23îj
.text:00401041                 mov     edx, offset aNoYouCanNotPla ; "No! You can not play :<\n\r"
.text:00401046                 call    sub_401933
.text:0040104B
.text:0040104B loc_40104B:                             ; CODE XREF: start_0+2Fîj
.text:0040104B                 mov     edx, offset aILoveNisra ; "I love nisra!\n\r"
.text:00401050                 call    sub_401933
.text:00401055                 push    0               ; uExitCode
.text:00401057                 call    ExitProcess
.text:00401057 start_0         endp
.text:00401057
.text:00401057 ; ---------------------------------------------------------------------------
.text:0040105C                 db 14h dup(0CCh)
.text:00401070 ;
```

靜態分析 - 工具

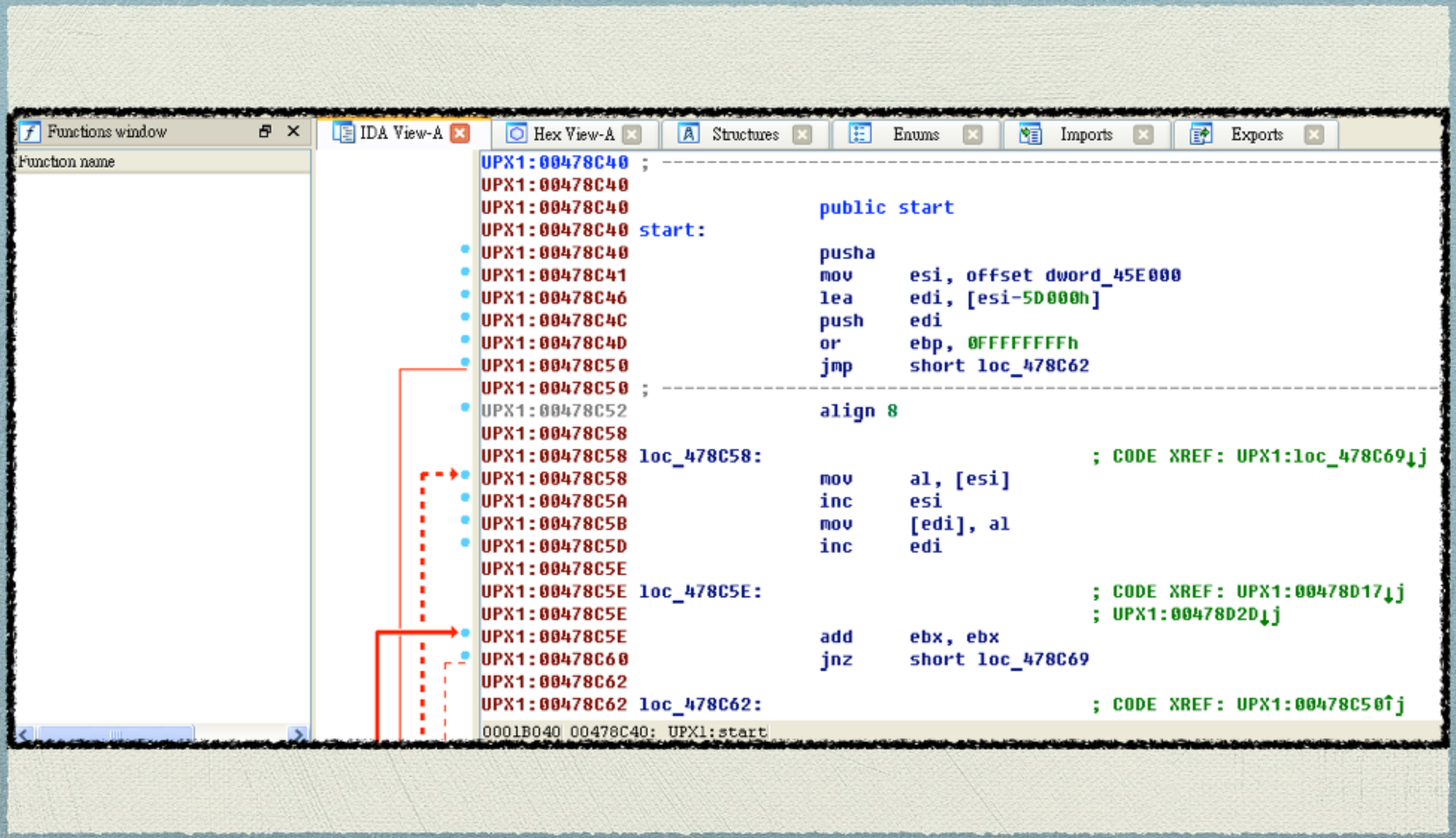
- 選擇 Subviews 可以看到各種子分頁



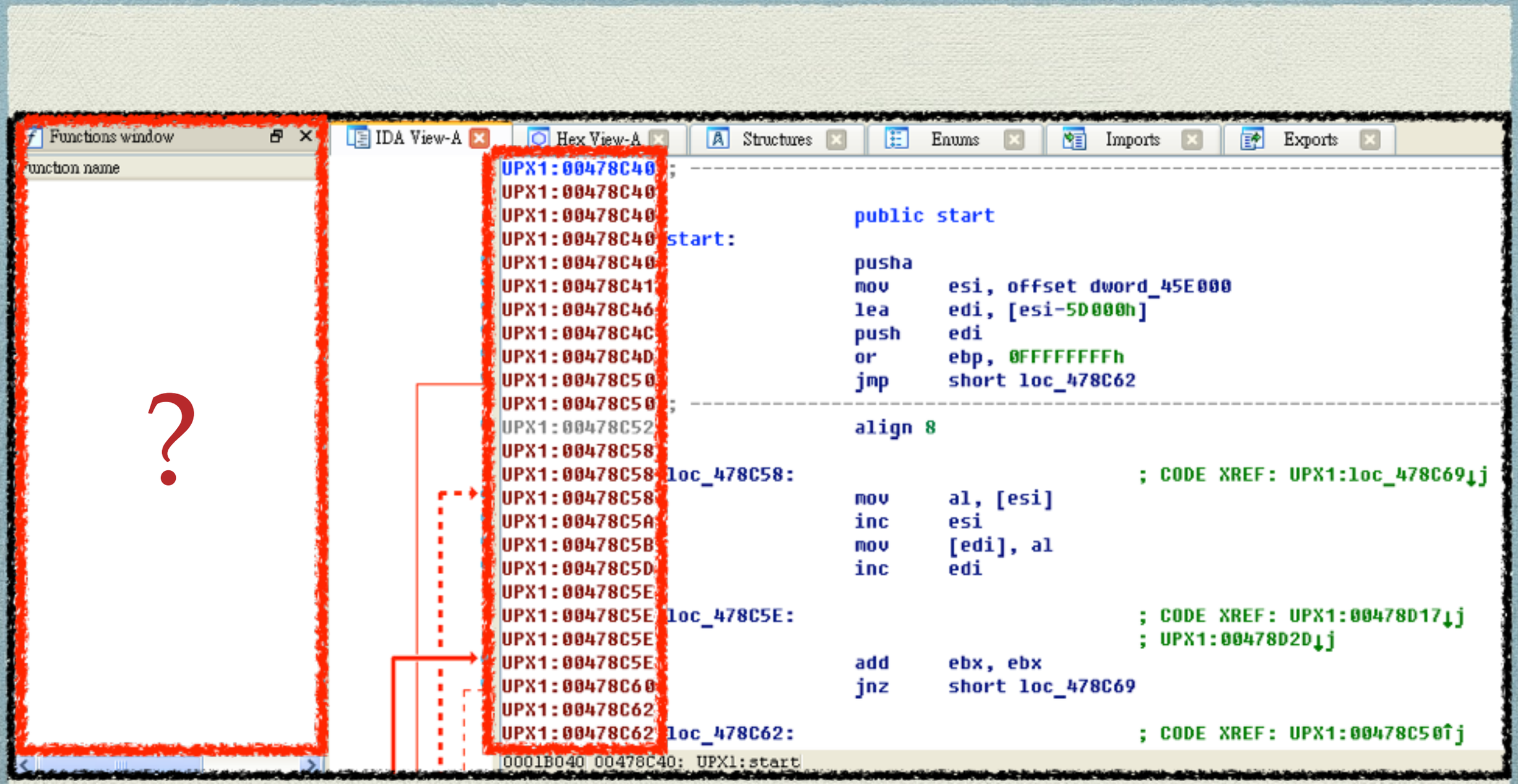
實例分析之 IDA - Honeynet Q2

- 目標
  - Malware 的行為
    - Malware 下載的檔案
    - 該檔案的行為
- 首先把 trivus.exe 把它扔進 IDA ！
  - 好希望解答自己跑出來(´;ω;`)

IDA - Honeynet Q2



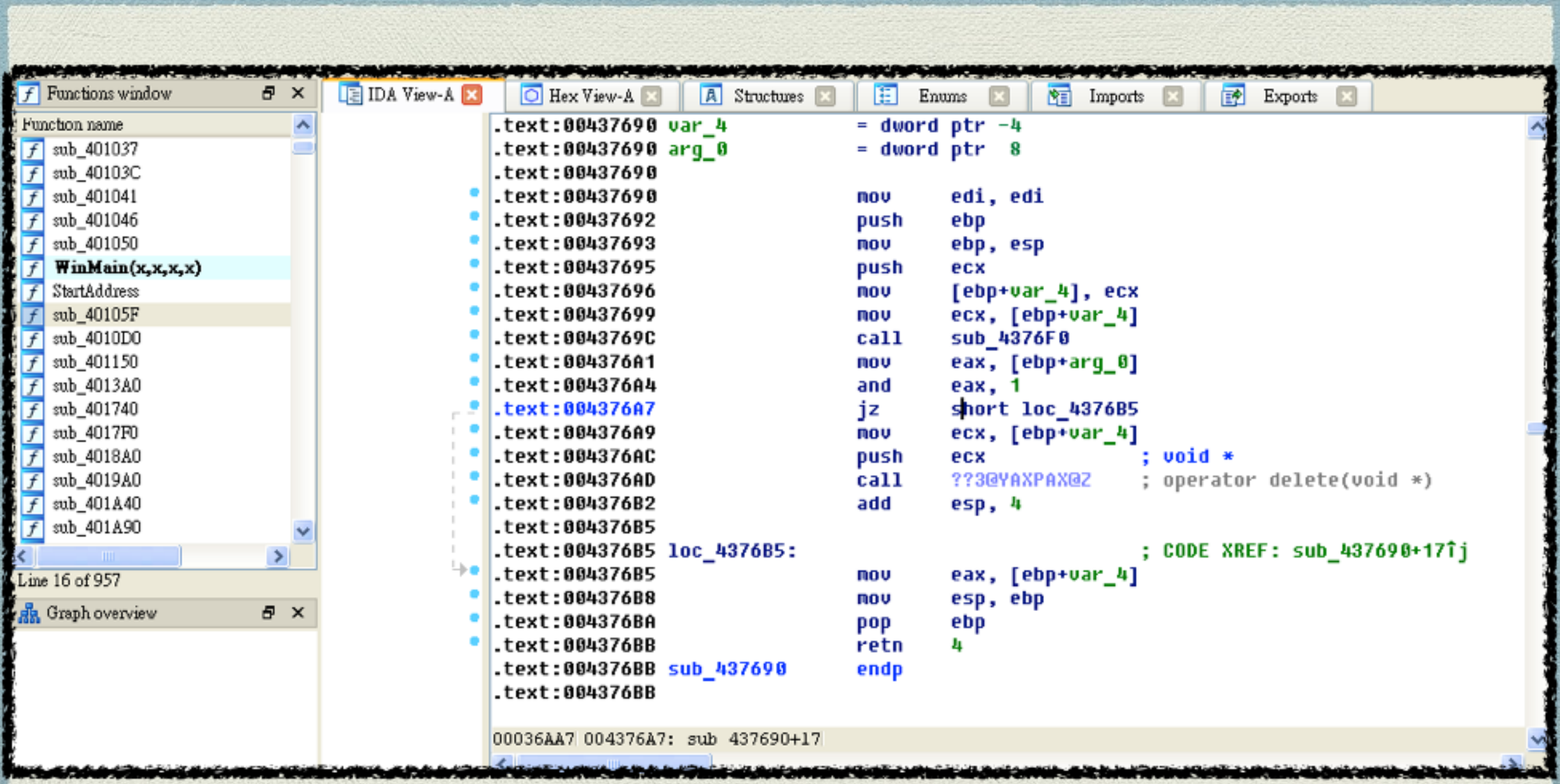
IDA - Honeynet Q2



實例分析之 IDA - Honeynet Q2

- 第一個難關：加殼！
  - 這個是未來讀書會要延伸的研究之一
  - 此處先跳過OAQ
- 加入我們一起研究吧！

IDA - Honeynet Q2



實例分析之 IDA - Honeynet Q2

- 第二個難關：怎麼看？
  - 發現程式碼很長……很長……
- 使用 String Windows 起手！
  - 字串大多會明碼留在程式裡！

IDA - Honeynet Q2

IDA View-A | Strings window | Imports | Hex View-A

Address	Length	Type	String
.rdata:00458D00	00000007	C	%s*.*
.rdata:00458D08	00000013	C	%s\userinit.exe,%s
.rdata:00458D1C	00000037	C	SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\
.rdata:00458D54	00000009	C	Userinit
.rdata:00458D60	00000007	C	Driver
.rdata:00458D68	0000003F	C	SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\services.sys
.rdata:00458DA8	00000007	C	Driver
.rdata:00458DB0	0000003F	C	SYSTEM\CurrentControlSet\Control\SafeBoot\Network\services.sys
.rdata:00458DF0	00000009	C	Userinit
.rdata:00458DFC	00000010	C	%s:*:Enabled:%s
.rdata:00458E10	00000075	C	SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\St···
.rdata:00458E88	0000003A	C	SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system
.rdata:00458EC4	0000000F	C	disabletaskmgr
.rdata:00458ED8	0000003C	C	SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced
.rdata:00458F14	00000007	C	hidden
.rdata:004590EC	0000000F	C	IsWow64Process
.rdata:00459110	0000000D	C	\service.exe
.rdata:00459120	0000000C	C	malware.exe
.rdata:0045912C	00000009	C	services
.rdata:00459138	0000000C	C	service.exe
.rdata:00459144	0000000D	C	\service.exe
.rdata:00459154	0000000C	C	service.exe
.rdata:00459474	00000007	C	(null)
.rdata:004594B1	00000008	C	(8PX\a\b
.rdata:004594B9	00000007	C	700WP\a
.rdata:004594C8	00000008	C	\b`b····

IDA - Honeynet Q2

IDA View-A | Strings window | Imports | Hex View-A

Address	Length	Type	String
.rdata:00458D00	00000007	C	%s*.*
.rdata:00458D08	00000013	C	%s\userinit.exe,%s
.rdata:00458D1C	00000037	C	SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\
.rdata:00458D54	00000009	C	Userinit
.rdata:00458D60	00000007	C	Driver
.rdata:00458D68	0000003F	C	SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\services.sys
.rdata:00458DA8	00000007	C	Driver
.rdata:00458DB0	0000003F	C	SYSTEM\CurrentControlSet\Control\SafeBoot\Network\services.sys
.rdata:00458DF0	00000009	C	Userinit
.rdata:00458DFC	00000010	C	%s:*:Enabled:%s
.rdata:00458E10	00000075	C	SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\St···
.rdata:00458E88	0000003A	C	SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system
.rdata:00458EC4	0000000F	C	disabletaskmgr
.rdata:00458ED8	0000003C	C	SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced
.rdata:00458F14	00000007	C	hidden
.rdata:004590EC	0000000F	C	IsWow64Process
.rdata:00459110	0000000D	C	\service.exe
.rdata:00459120	0000000C	C	malware.exe
.rdata:0045912C	00000009	C	services
.rdata:00459138	0000000C	C	service.exe
.rdata:00459144	0000000D	C	\service.exe
.rdata:00459154	0000000C	C	service.exe
.rdata:00459474	00000007	C	(null)
.rdata:004594B1	00000008	C	(8PX\a\b
.rdata:004594B9	00000007	C	700WP\a

實例分析之 IDA - Honeynet Q2

- Trivus.exe 小結

```
.rdata:00458F20                 unicode 0, <https://docs.google.com/uc?authuser=0&id=0BwwdBzXoIL8
.rdata:00458F20                 unicode 0, <pNUhJMnVXOUU&export=download>,0
.rdata:00458FCC                 align 10h
.rdata:00458FD0 aHttpsDocs_go_0:                        ; DATA XREF: sub_401B40+2C↑o
.rdata:00458FD0                 unicode 0, <https://docs.google.com/uc?authuser=0&id=0BwwdBzXoIL8
.rdata:00458FD0                 unicode 0, <BVE0wRzhWc1U&export=download>,0
.rdata:0045907C ; const WCHAR aSMalware_exe
.rdata:0045907C aSMalware_exe:                          ; DATA XREF: sub_401B40+52↑o
.rdata:0045907C                 unicode 0, <%s\malware.exe>,0
.rdata:0045909A                 align 4
.rdata:0045909C ; const WCHAR aSServices_sys
.rdata:0045909C aSServices_sys:                         ; DATA XREF: sub_401B40+80↑o
.rdata:0045909C                 unicode 0, <%s\services.sys>,0
.rdata:004590BC ; const WCHAR aSDriversServic
.rdata:004590BC aSDriversServic:                        ; DATA XREF: sub_401B40+AE↑o
.rdata:004590BC                 unicode 0, <%s\drivers\services.sys>,0
.rdata:004590EC ; char ProcName[]
.rdata:004590EC ProcName        db 'IsWow64Process',0   ; DATA XREF: sub_401C90+B↑o
.rdata:004590FB                 align 4
.rdata:004590FC ; const WCHAR ModuleName
.rdata:004590FC ModuleName:                             ; DATA XREF: sub_401C90+10↑o
.rdata:004590FC                 unicode 0, <kernel32>,0
.rdata:0045910E                 align 10h
.rdata:00459110 ; char aService_exe[]
.rdata:00459110 aService_exe    db '\service.exe',0     ; DATA XREF: _WinMain@16_0+68↑o
```

實例分析之 IDA - Honeynet Q2

- Trivus.exe 小結
  - service.exe
  - malware.exe
  - services.sys

IDA - Honeynet Q2

- 透過點擊
- 移動到該 String 出現的地方

```
push    offset aService_exe_0 ; "service.exe"
lea     ecx, [ebp+NewFileName]
push    ecx
call    sub_401041
add     esp, 8
movzx   edx, al
test    edx, edx
jnz     short loc_401EA9
push    offset aService_exe_1 ; "\\service.exe"
lea     eax, [ebp+NewFileName]
push    eax                   ; char *
call    _strcat
add     esp, 8
push    0                     ; bFailIfExists
lea     ecx, [ebp+NewFileName]
push    ecx                   ; lpNewFileName
lea     edx, [ebp+ExistingFileName]
push    edx                   ; lpExistingFileName
call    ds:CopyFileA
lea     eax, [ebp+NewFileName]
push    eax
call    sub_401037
add     esp, 4
push    0                     ; uCmdShow
push    offset CmdLine  ; "service.exe"
call    ds:WinExec
lea     ecx, [ebp+NewFileName]
push    ecx
```

IDA - Honeynet Q2

- 透過點擊
- 移動到該 String 出現的地方
- 在 IDA 裡粉紅色的都是 Windows API

```
push    offset aService_exe_0 ; "service.exe"
lea     ecx, [ebp+NewFileName]
push    ecx
call    sub_401041
add     esp, 8
movzx   edx, al
test    edx, edx
jnz     short loc_401EA9
push    offset aService_exe_1 ; "\\service.exe"
lea     eax, [ebp+NewFileName]
push    eax                   ; char *
call    _strcat
add     esp, 8
push    0                     ; bFailIfExists
lea     ecx, [ebp+NewFileName]
push    ecx                   ; lpNewFileName
lea     edx, [ebp+ExistingFileName]
push    edx                   ; lpExistingFileName
call    ds:CopyFileA
lea     eax, [ebp+NewFileName]
push    eax
call    sub_401037
add     esp, 4
push    0                     ; uCmdShow
push    offset CmdLine  ; "service.exe"
call    ds:WinExec
lea     ecx, [ebp+NewFileName]
push    ecx
```

什麼是 API ？

- API (Application Programming Interface)
  - 應用程式開發介面
- 為了方便使用
- 提供 Function ，直使呼叫便可使用

實例分析之 IDA - Honeynet Q2

- 第三個難關：Windows API
  - 我怎麼知道這個 API 是什麼？
- 就……查吧！除非你是人體字典！
  - CopyFile
  - WinExec

```
call    ds:CopyFileA
lea     eax, [ebp+NewFileName]
push    eax
call    sub_401037
add     esp, 4
push    0                       ; uCmdShow
push    offset CmdLine  ; "service.exe"
call    ds:WinExec
lea     ecx, [ebp+NewFileName]
push    ecx
```

IDA - Honeynet Q2

CopyFile function

Copies an existing file to a new file.

The **CopyFileEx** function provides two additional capabilities. **CopyFileEx** can call a specified callback function each time a portion of the copy operation is completed, and **CopyFileEx** can be canceled during the copy operation.

To perform this operation as a transacted operation, use the **CopyFileTransacted** function.

Syntax

C++

```
BOOL WINAPI CopyFile(
  _In_ LPCTSTR lpExistingFileName,
  _In_ LPCTSTR lpNewFileName,
  _In_ BOOL    bFailIfExists
);
```

WinExec function

Runs the specified application.

Note This function is provided only for compatibility with 16-bit Windows. Applications should use the **CreateProcess** function.

Syntax

C++

```
UINT WINAPI WinExec(
  _In_ LPCSTR lpCmdLine,
  _In_ UINT   uCmdShow
);
```

IDA - Honeynet Q2

- 先來個人類語言版本說明
- CopyFile
  - 複製一個已存在檔案，另外成為一個新檔
- WinExec
  - 運作指定的應用程式

IDA - Honeynet Q2

- 再來個挑戰版本
- CopyFile
  - lpExistingFileName
  - lpNewFileName
  - bFailIfExists
- WinExec
  - lpCmdLine
  - uCmdShow

```
push    offset aService_exe_0 ; "service.exe"
lea     ecx, [ebp+NewFileName]
push    ecx
call    sub_401041
add     esp, 8
movzx   edx, al
test    edx, edx
jnz     short loc_401EA9
push    offset aService_exe_1 ; "\\service.exe"
lea     eax, [ebp+NewFileName]
push    eax                   ; char *
call    _strcat
add     esp, 8
push    0                     ; bFailIfExists
lea     ecx, [ebp+NewFileName]
push    ecx                   ; lpNewFileName
lea     edx, [ebp+ExistingFileName]
push    edx                   ; lpExistingFileName
call    ds:CopyFileA
lea     eax, [ebp+NewFileName]
push    eax
call    sub_401037
add     esp, 4
push    0                     ; uCmdShow
push    offset CmdLine  ; "service.exe"
call    ds:WinExec
lea     ecx, [ebp+NewFileName]
push    ecx
```

IDA - Honeynet Q2

- 再來個挑戰版本
- CopyFile
  - lpExistingFileName
  - lpNewFileName
  - bFailIfExists
- WinExec
  - lpCmdLine
  - uCmdShow

```
push    offset aService_exe_0 ; "service.exe"
lea     ecx, [ebp+NewFileName]
push    ecx
call    sub_401041
add     esp, 8
movzx   edx, al
test    edx, edx
jnz     short loc_401EA9
push    offset aService_exe_1 ; "\\service.exe"
lea     eax, [ebp+NewFileName]
push    eax                   ; char *
call    _strcat
add     esp, 8
push    0                     ; bFailIfExists
lea     ecx, [ebp+NewFileName]
push    ecx                   ; lpNewFileName
lea     edx, [ebp+ExistingFileName]
push    edx                   ; lpExistingFileName
call    ds:CopyFileA
lea     eax, [ebp+NewFileName]
push    eax
call    sub_401037
add     esp, 4
push    0                     ; uCmdShow
push    offset CmdLine  ; "service.exe"
call    ds:WinExec
lea     ecx, [ebp+NewFileName]
push    ecx
```

IDA - Honeynet Q2

- WinExec
  - 運作指定的應用程式
- 其中一個參數還可以隱藏！

WinExec function

Runs the specified application.

Note This function is provided only for compatibility with 16-bit Windows. Applications should use the **CreateProcess** function.

Syntax

C++

```
UINT WINAPI WinExec(
  _In_ LPCSTR lpCmdLine,
  _In_ UINT   uCmdShow
);
```

實例分析之 IDA - Honeynet Q2

- Trivus.exe 小結
  - 生成檔案
  - 其中一個檔案會偷偷運作
- 似乎離發現行為還有段距離？

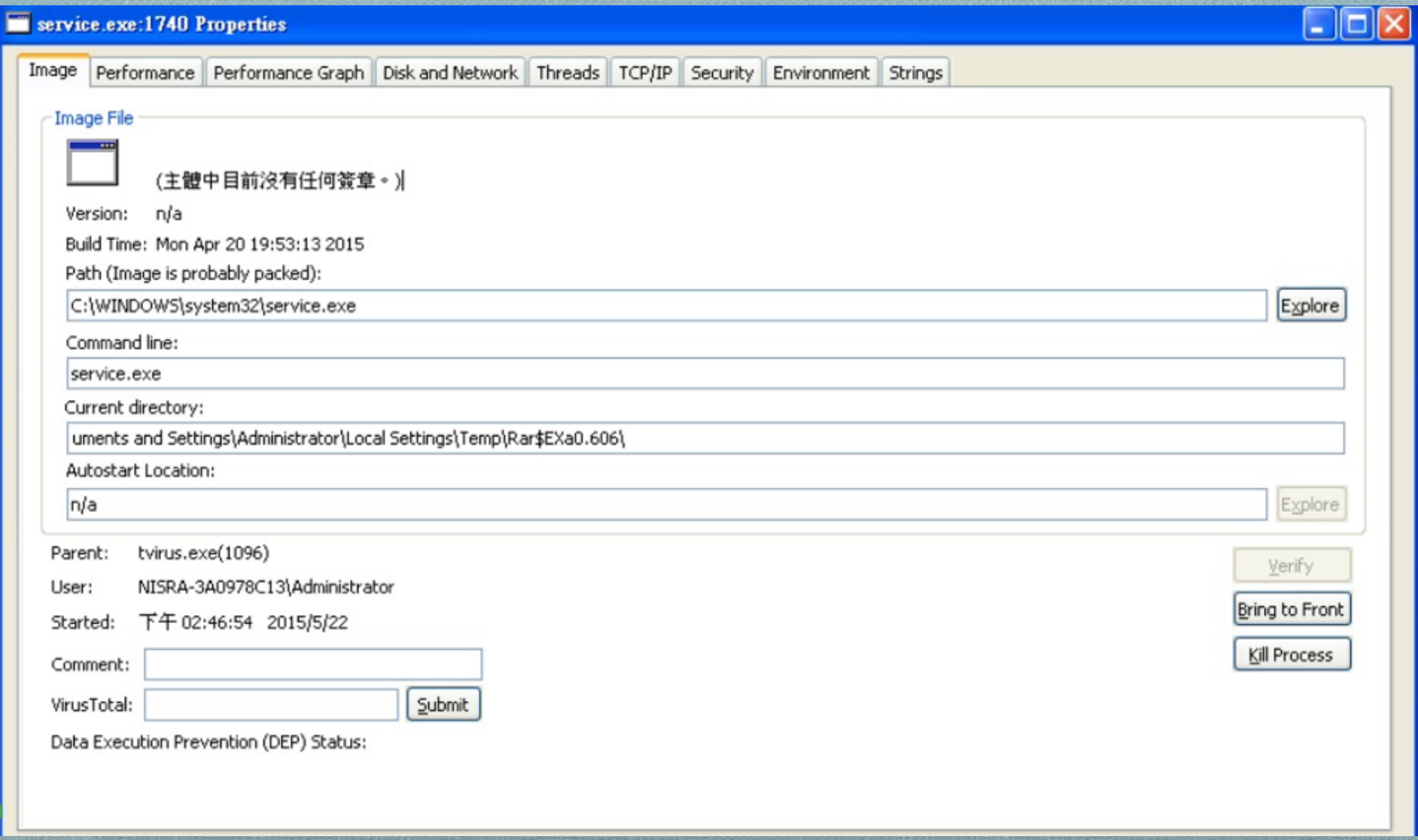
IDA - Honeynet Q2

- 前呼後應！讓我用用看前面的工具！
  - ProcessExplorer
  - TCPView

IDA - Honeynet Q2

- 前呼後應！讓我用用看前面的工具！
  - ProcessExplorer
  - TCPView
- 絕對不是偷懶 T_T 同學們快醒來啊 ~

IDA - Honeynet Q2



IDA - Honeynet Q2

TCPView - Sysinternals: www.sysinternals.com

File Options Process View Help

Process	PID	Protocol	Local Address	Local Port	Remote Address
alg.exe	720	TCP	nisra-3a0978c13	1028	nisra-3a0978c13
lsass.exe	516	UDP	nisra-3a0978c13	isakmp	*
lsass.exe	516	UDP	nisra-3a0978c13	4500	*
service.exe	1740	TCP	nisra-3a0978c13	3307	nisra-3a0978c13
svchost.exe	768	TCP	nisra-3a0978c13	epmap	nisra-3a0978c13
svchost.exe	812	UDP	nisra-3a0978c13	ntp	*
svchost.exe	892	UDP	nisra-3a0978c13	1900	*
System	4	TCP	nisra-3a0978c13	microsoft-ds	nisra-3a0978c13
System	4	UDP	nisra-3a0978c13	microsoft-ds	*

IDA - Honeynet Q2

- 前呼後應！讓我用用看前面的工具！
  - ProcessExplorer
    - 多了一個service.exe 在 C:\WINDOWS\system32
    - 備註：正常XP下該資料夾位置下有 services.exe
  - TCPView
    - 發現一個由 service.exe 建立的連線，3307port

實例分析之 IDA - Honeynet Q2

- 目標
  - Malware 的行為
  - Malware 下載的檔案
  - 該檔案的行為

實例分析之 IDA - Honeynet Q2

- 目標
  - Malware 的行為
  - Malware 下載的檔案
  - 該檔案的行為
- 把剛剛的動作 LOOP 一遍

什麼？！那還要多久？！

實例分析之 IDA - Honeynet Q2

- 心得
  - 需要相當有程度耐心
  - 不懂的資訊，就去查！需要反覆操作才會熟悉！
  - 看久你就會變成組合語言之神啦！！！！！
- 教練：「要多累積經驗！」

總結

- 無法預測有什麼樣的惡意行為
  - 對於舊的威脅，需要經驗和資料
  - 對於新的威脅，需要耐心和人力
- 複數工具交叉比對，增加分析正確的機率

快樂懶人包\(´∀`)/

- 初步了解惡意程式
- 從三個層面去評估該軟體會有什麼行為
  - Registry、Process、網路行為
- Online Sandbox
- IDA Pro 使用方法
- 面對分析需要耐心、細心和一些基本知識

QA 時間

- 希望有興趣的女生可以加入我們！
- 開放提問「不困難的問題」XDDD
- 感謝三位教練提攜！