

# Practical Malware Analysis

## Lab 01-01

Writer:    SÓI   

Mẫu lab01-01 được tải về từ:

<https://drive.google.com/file/d/1huaWDunvfT7cuaaZWMPocFOzW732rxiG/view?usp=sharing>

Trong Lab 01-01 có 2 phần đó là .exe và .dll

- Đầu tiên chúng ta đưa 2 file của Lab 01-01 này lên trang virustotal để check information của nó.

**38 engines detected this file**


SHA-256: 58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327bd6fe47  
File name: Lab01-01.exe  
File size: 16 KB  
Last analysis: 2018-10-02 04:23:57 UTC  
Community score: -26

**38 / 68**

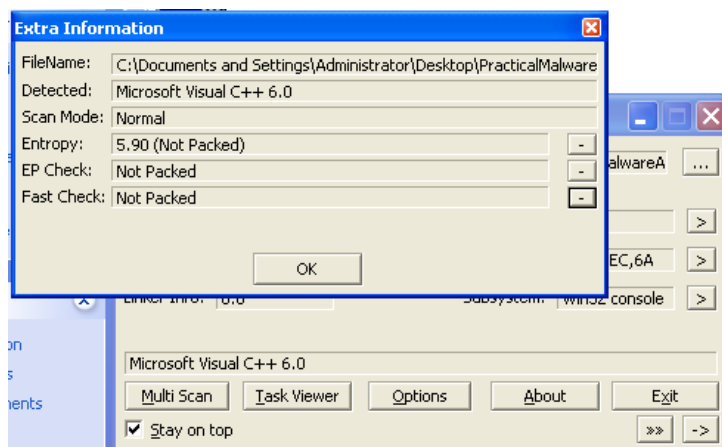
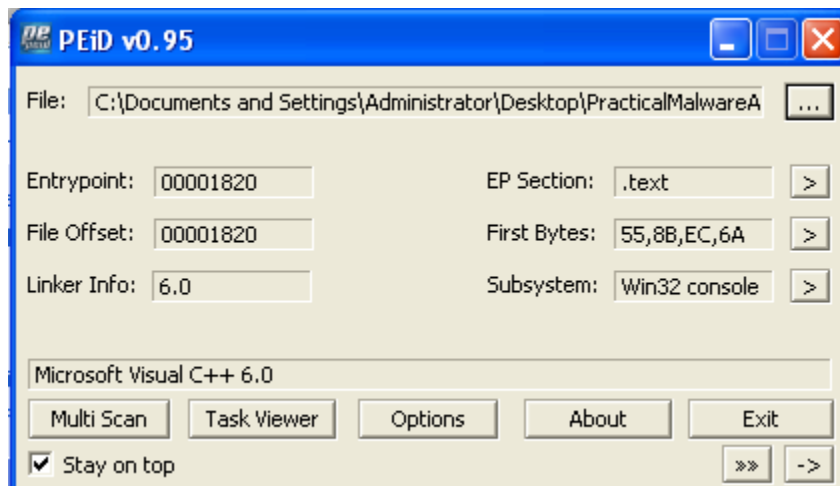
Detection	Details	Relations	Behavior	Community
AegisLab	Trojan.Win32.Generic.4!c	AhnLab-V3	Trojan/Win32.Agent.C957604	
ALYac	Trojan.Agent.1638455	Antiy-AVL	Trojan/Win32.TSGeneric	
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen	
Avira	HEUR/AGEN.1022518	AVware	Trojan.Win32.Generic!BT	
CAT-QuickHeal	Trojan.IGENERIC	ClamAV	Win.Malware.Agent-6342616-0	
Cylance	Unsafe	Cyren	W32/Trojan.CZAN-7287	
Endgame	malicious (high confidence)	ESET-NOD32	a variant of Win32/Agent.WOM	

Trên [www.virustotal.com](http://www.virustotal.com) 2018-10-02 phát hiện ra 38 phương tiện có thể phát hiện ra tệp này vd như Avira,Avast,AVG,... Điều này chứng tỏ lab 01-01 đã có từ lâu và độ phổ biến cũng cao.

### - Phát hiện Packer

Kiểm tra xem nó có bị packed hay không, sử dụng phần mềm PEID .

Để kiểm tra chúng ta add file đó vào chương trình PEID kích chọn vào phần Extra information kích vào phần entropy, EP check, Fast Check để xem có bị packed hay không. Và để ý phần Microsoft Visual C++ 6.0.



Như vậy 2 file này không hề bị pack

#### - **Xác định Mã băm :**

- Băm (hashing) là phương pháp phổ biến để định danh mã độc. Một file bất kì, không ngoại lệ một chương trình độc hại sau khi qua một hàm băm sẽ cho một chuỗi có giá trị không trùng lặp với bất kì một file nào khác. Chuỗi băm này có thể coi như “dấu vân tay” của file đó và có thể dùng để định danh file. SHA256 đang là hàm băm phổ biến nhất dùng cho việc định danh mã độc. Ngoài ra, MD5, SHA1 vẫn được sử dụng.

ta có thể sử dụng công cụ **certUtil** của PowerShell để thực hiện băm file lab01-01.exe ta dùng lệnh PowerShell:

**certUtil -hashfile .\Desktop\lab01-01.exe SHA256**

```
PS C:\Users\Administrator> certUtil -hashfile .\Desktop\Lab01-01.exe SHA256
SHA256 hash of .\Desktop\Lab01-01.exe:
58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327bd6fe47
CertUtil: -hashfile command completed successfully.
PS C:\Users\Administrator>
```

Khi đã có chuỗi băm của mã độc, ta có thể sử dụng để:

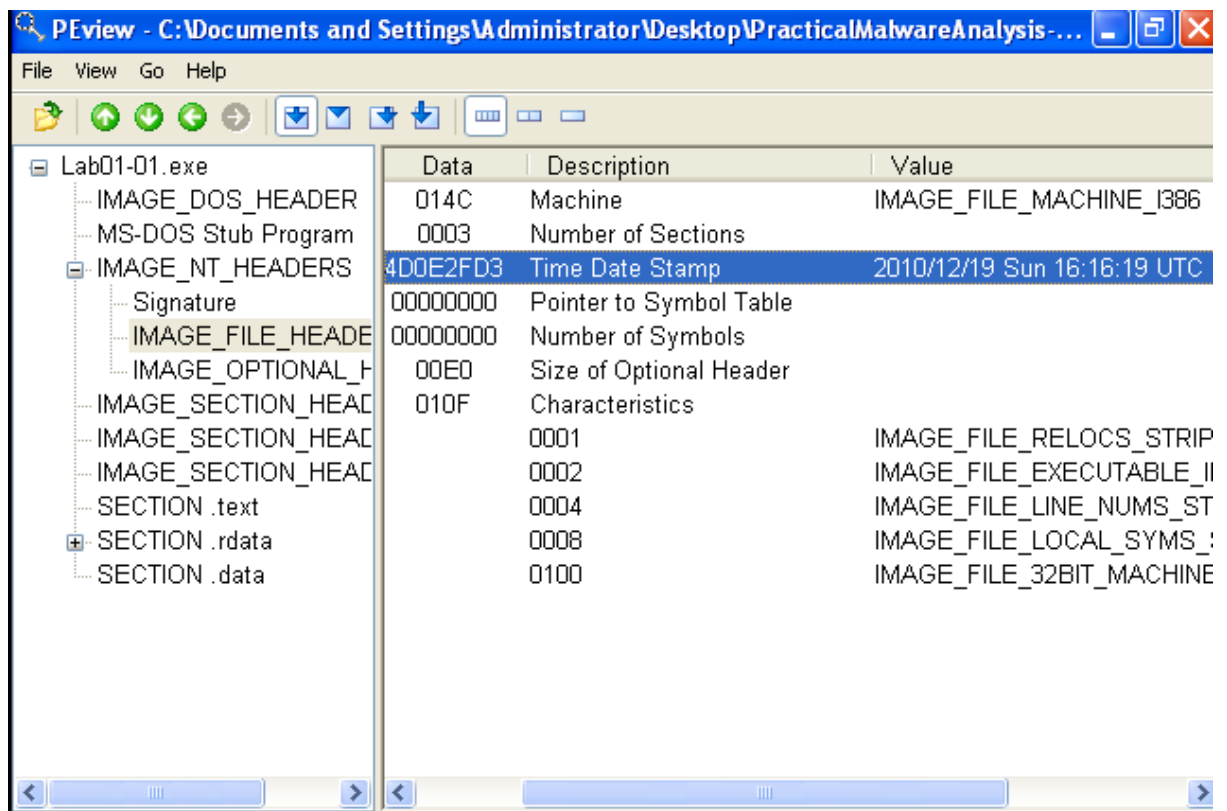
- Dùng như một nhãn, hoặc tên mã độc, tên biến thể.
- Chia sẻ với người khác để giúp họ nhận dạng mã độc.
- Tìm kiếm chuỗi này trên mạng, có thể mã độc đã được định danh từ trước đó

#### - PE file

**PEview** là công cụ đơn giản cho phép xem thông tin trong PE header

**IMAGE\_OPTIONAL\_HEADER** gồm kiến trúc bộ xử lý, thời điểm chương trình được biên dịch.

Ở đây ta thấy thời gian compiled của nó là 16:16:19



IMAGE\_SECTION\_HEADER.text và SECTION.text Chứa các tập lệnh CPU

IMAGE\_SECTION\_HEADER.rdata và SECTION.rdata Chứa các thông tin import và export như những gì ta thấy trong Dependency Walker

IMAGE\_SECTION\_HEADER.data và section.data Chứa dữ liệu toàn cục của chương trình, dữ liệu này có thể truy cập từ bất kì đâu trong chương trình. Dữ liệu cục bộ không được lưu trong section này hay bất kì đâu trong PE file

Trong phần **IMAGE\_OPTIONAL\_HEADER** để ý dòng **Subsystem** ta thấy giá trị **IMAGE\_SUBSYSTEM\_WINDOWS\_CUI** điều này có nghĩa chương trình là **console**.

00000140	00000000	Checksum	
00000144	0003	Subsystem	IMAGE_SUBSYSTEM_WINDOWS_CUI
00000146	0000	DLL Characteristics	
00000148	00100000	Size of Stack Reserve	

**IMAGE\_SECTION\_HEADER.text** dùng để mô tả mỗi section trong PE file, Trình biên dịch thường tạo và tự động đặt tên cho các section trong file thực thi, người dùng có ít quyền kiểm soát các tên này.

Ở đây **Virtual Size** có giá trị là 00000970 là không gian bộ nhớ cho section khi tải tiến trình. **Size of Raw Data** có giá trị 00001000 là kích thước của section trong ổ lưu trữ.

PEView - C:\Users\Administrator\Desktop\Lab01-01.exe

File View Go Help

	pFile	Data	Description	Value
Lab01-01.exe				
IMAGE_DOS_HEADER	000001E0	2E 74 65 78	Name	.text
MS-DOS Stub Program	000001E4	74 00 00 00		
IMAGE_NT_HEADERS	000001E8	00000970	Virtual Size	
Signature	000001EC	00001000	RVA	
IMAGE_FILE_HEADER	000001F0	00001000	Size of Raw Data	
IMAGE_OPTIONAL_HEADER	000001F4	00001000	Pointer to Raw Data	
<b>IMAGE_SECTION_HEADER.text</b>	000001F8	00000000	Pointer to Relocations	
IMAGE_SECTION_HEADER.rdata	000001FC	00000000	Pointer to Line Numbers	
IMAGE_SECTION_HEADER.data	00000200	0000	Number of Relocations	
SECTION .text	00000202	0000	Number of Line Numbers	
SECTION .rdata	00000204	60000020	Characteristics	
SECTION .data		00000020		IMAGE_SCN_CNT_CODE
		20000000		IMAGE_SCN_MEM_EXECUTE
		40000000		IMAGE_SCN_MEM_READ

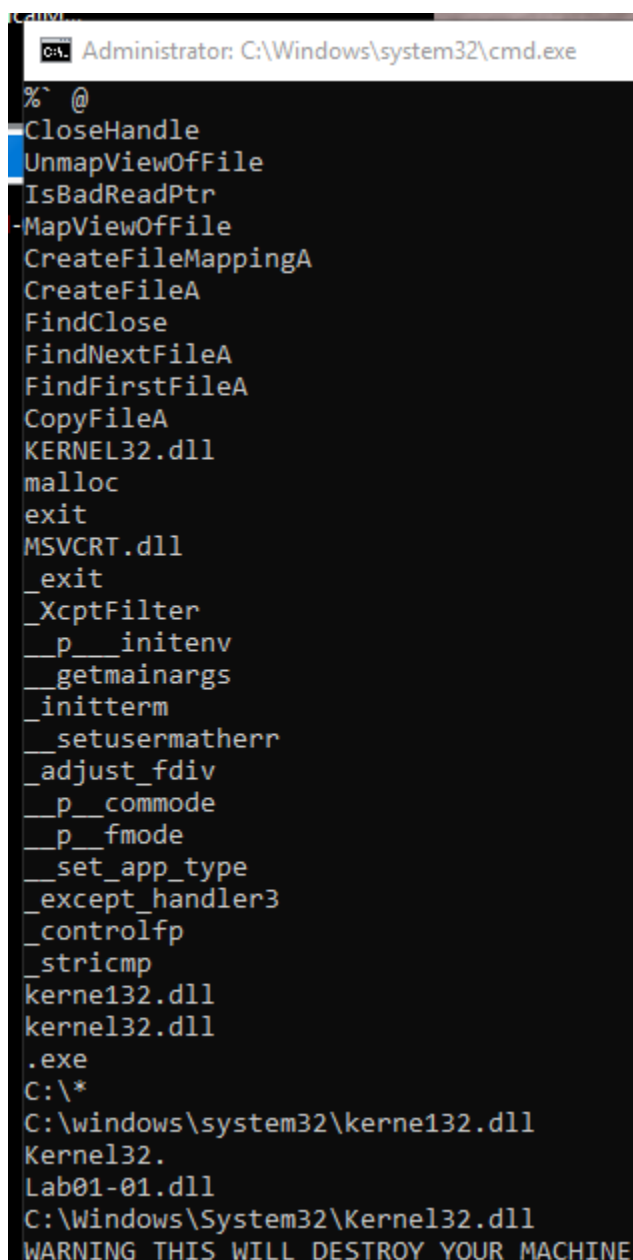
## - Kiểm Tra các chuỗi String

Một chương trình chứa các string nếu nó in ra các thông điệp, kết nối tới một URL hoặc copy một file tới một địa chỉ nào đó.

Khi kiểm tra các chuỗi string có thể dự đoán hành vi của chương trình. Có nhiều công cụ cho phép tìm kiếm các string trong một chương trình , đây chúng ta dùng chương trình **strings** trong cmd.

Đầu tiên tải **strings** trên trang trữ của windows, đặt nó vào trong file chứa file lab01-01 chạy chương trình **strings** lên chạy lệnh :

### Strings lab01-01.exe



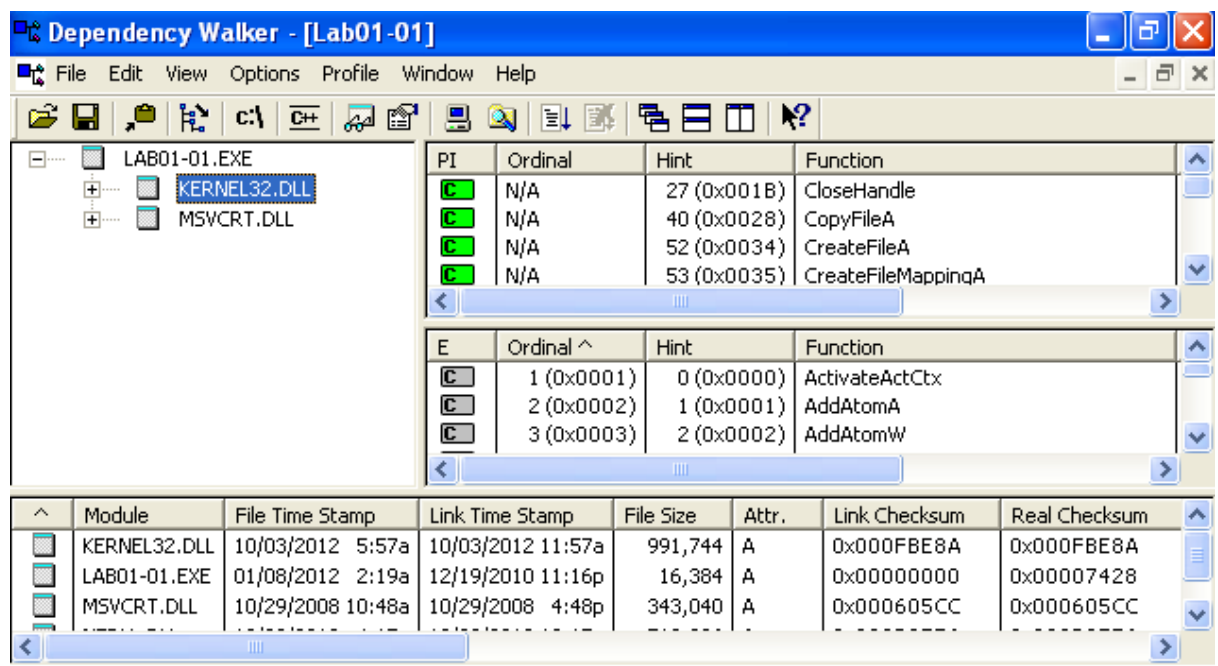
```
Administrator: C:\Windows\system32\cmd.exe
%~ @
CloseHandle
UnmapViewOfFile
IsBadReadPtr
-MapViewOfFile
CreateFileMappingA
CreateFileA
FindClose
FindNextFileA
FindFirstFileA
CopyFileA
KERNEL32.dll
malloc
exit
MSVCRT.dll
_exit
_XcptFilter
__p__initenv
__getmainargs
__initterm
__setusermatherr
__adjust_fdiv
__p__commode
__p__fmode
__set_app_type
__except_handler3
__controlfp
__stricmp
kerne132.dll
kernel32.dll
.exe
C:\*
C:\windows\system32\kerne132.dll
Kernel32.
Lab01-01.dll
C:\Windows\System32\Kernel32.dll
WARNING THIS WILL DESTROY YOUR MACHINE
```

Như đã thấy , lab01-01 sử dụng Kernel32.DLL và **Kerne132.DLL** mục đích để đánh lừa người sử dụng k nhận ra để phân biệt 2 DLL này, nó sẽ dùng Kerne132.DLL làm trung gian khi chúng ta gọi tới KEREL32. Địa chỉ file C:\Windows\system32\kerne132.dll

Warning this will destroy your machine!!!!

#### - Các hàm liên kết động

Ta sử dụng Dependency Walker (<http://www.dependencywalker.com/>) chỉ liệt kê các hàm được liên kết động trong một chương trình.



Trong lab01-01.exe có thể thấy Lab01-01 sử dụng 2 DLL để liên kết : KERNEL32.DLL và MSVCRT.DLL trong đó KERNEL32.DLL là DLL phổ biến nhất, chứa các hàm cốt lõi cho phép truy cập và sử dụng bộ nhớ, file, phần cứng,...

Click vào KERNEL32.DLL sẽ thấy danh sách các hàm được import. Hàm **CopyFileA** và **CreateFileA** là 2 hàm đáng chú ý nhất, CopyFileA là hàm thực hiện copy một file sang một file mới, CreateFileA là hàm thực hiện tạo một file mới.

**MapViewOfFile** là bản đồ chế độ xem ánh xạ tệp vào không gian địa chỉ của quá trình gọi. Lab01-01 có thể thực hiện thay đổi đối với tệp thực tế khi tệp được ánh xạ.




Từ đó ta có thể thấy con Lab01-01 này có chức năng sửa đổi file hệ thống cũng như sao chép các file để đánh cắp dữ liệu người dùng . Nó sẽ tạo một bản sao độc hại của dll bằng cách ngụy trang chính nó như kernel32.dll là kerne132.dll . Exe này sau đó sẽ cố gắng tìm kiếm một số tập tin và lây nhiễm nó để chạy dll này. Các dll có khả năng đảm bảo rằng chỉ có một ví dụ của mã độc hại đang chạy kể từ khi mutex đang được sử dụng. Sau đó nó sẽ giao tiếp đúng lúc (Sleep) tới máy chủ C & C với IP: 127.26.152.13 để nhận lệnh thực thi trên máy của nạn nhân.

### Lab 01-04

Writer:   SÓI  

Trong Lab 01-04 có 1 file Lab01-04.exe chúng ta sẽ bắt đầu đi phân tích tĩnh của con lab này qua file Lab01-04 này.

Đầu tiên thử kiểm tra nó trên [www.virustotal.com](http://www.virustotal.com) 2018-9-30 thì có 51/68 thiết bị có thể phát hiện ra nó.



51 / 68

51 engines detected this file

SHA-2560fa1498340fca6c562cfa389ad3e93395f44c72fd128d7ba08579a69aaf3b126

File nameLab01-04.exe

File size36 KB

Last analysis2018-09-30 03:34:35 UTC

Community score-159

Detection

Details

Relations

Behavior

Community

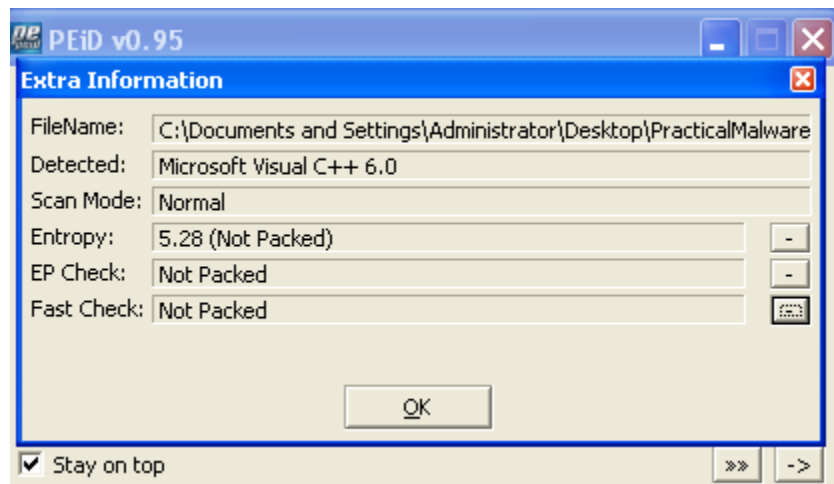
Ad-Aware	⚠ Gen:Trojan.Heur.RPcqW@aqlk5pji	AegisLab	⚠ Trojan.Win32.Generic.a!c
Antiy-AVL	⚠ Trojan[Downloader]/Win32.Unknown	Arcabit	⚠ Trojan.Heur.RPE9A4ED
Avast	⚠ Win32:Malware-gen	AVG	⚠ Win32:Malware-gen
Avira	⚠ TR/Dropper.Gen	AVware	⚠ Trojan.Win32.Generic!BT
BitDefender	⚠ Gen:Trojan.Heur.RPcqW@aqlk5pji	Bkav	⚠ W32.eHeur.Malware01
CAT-QuickHeal	⚠ TrojanDownloader.Small	ClamAV	⚠ Win.Trojan.Agent-375080
CrowdStrike Falcon	⚠ malicious_confidence_70% (D)	Cybereason	⚠ malicious.fd47ad



Tiếp theo kiểm tra xem file .exe này có bị pack hay không bằng phần mềm



PEiD



Như vậy file .exe này không hề bị pack.

Chuỗi băm: là phương pháp phổ biến để định danh mã độc. Một file bất kì, không ngoại lệ một chương trình độc hại sau khi qua một hàm băm sẽ cho một chuỗi có giá trị không trùng lặp với bất kì một file nào khác.

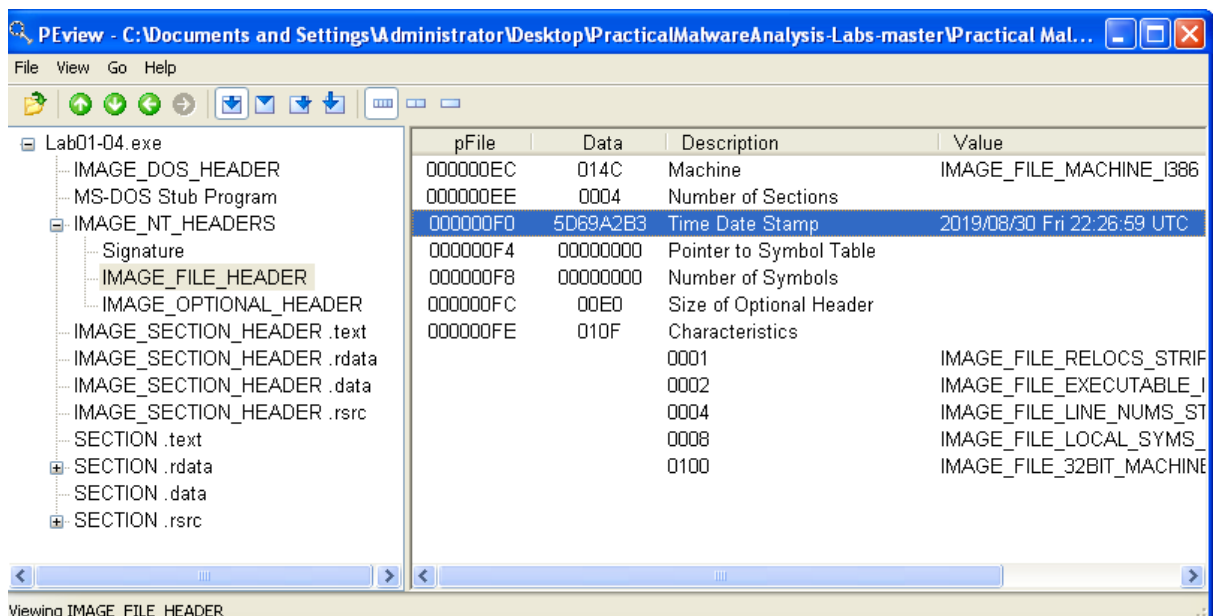
Chuỗi băm này có thể coi như “dấu vân tay” của file đó và có thể dùng để định danh file. SHA256 đang là hàm băm phổ biến nhất dùng cho việc định danh mã độc. Ngoài ra, MD5, SHA1 vẫn được sử dụng.

Ta có thể sử dụng công cụ **certUtil** của PowerShell để thực hiện băm file Lab01-04.exe bằng lệnh

**certUtil -hashfile .\Desktop\lab01-04.exe SHA256**

```
PS C:\Users\Administrator> certUtil -hashfile .\Desktop\Lab01-04.exe SHA256
SHA256 hash of .\Desktop\Lab01-04.exe:
0fa1498340fca6c562cfa389ad3e93395f44c72fd128d7ba08579a69aaf3b126
CertUtil: -hashfile command completed successfully.
PS C:\Users\Administrator>
```

Dùng Preview ta thấy :



Thời gian compiled của nó là 2019/08/30 Fri 22:26:59 UTC

Trong phần **IMAGE\_OPTIONAL\_HEADER** để ý dòng **Subsystem** ta thấy giá trị **IMAGE\_SUBSYSTEM\_WINDOWS\_GUI** điều này có nghĩa chương trình là **GUI**.

0000013C	00001000	Size of Headers	
00000140	00000000	Checksum	
00000144	0002	Subsystem	IMAGE_SUBSYSTEM_WINDOWS_GUI
00000146	0000	DLL Characteristics	
00000148	00100000	Size of Stack Reserve	

**Kiểm tra các chuỗi String:** kiểm tra các chuỗi string có thể là cách đơn giản để dự đoán hành vi của chương trình.

Đầu tiên tải **strings** trên trang trữ của windows, đặt nó vào trong file chứa file lab01-01 chạy chương trình **strings** lên chạy lệnh :

**Strings lab01-04.exe**

```

CloseHandle
OpenProcess
GetCurrentProcess
CreateRemoteThread
GetProcAddress
LoadLibraryA
WinExec
WriteFile
CreateFileA
SizeofResource
LoadResource
FindResourceA
GetModuleHandleA
GetWindowsDirectoryA
MoveFileA
GetTempPathA
KERNEL32.dll
AdjustTokenPrivileges
LookupPrivilegeValueA
OpenProcessToken
ADVAPI32.dll
_snprintf
MSUCRT.dll
_exit
XcptFilter
exit
_p__initenv
_getmainargs
_initterm
_setusermatherr
_adjust_fdiv
_p__commode
_p__fmode
_set_app_type
_except_handler3
_controlfp
_stricmp
winlogon.exe
<not real>
SeDebugPrivilege
sfc_os.dll
\system32\wupdmgr.exe
%s%s
BIN
#101
EnumProcessModules
psapi.dll
GetModuleBaseNameA
psapi.dll
EnumProcesses
psapi.dll
\system32\wupdmgr.exe
%s%s
\winup.exe
%s%s
BIN
!This program cannot be run in DOS mode.
Rich

```

Chúng ta có thể thấy rằng thực sự có khá nhiều thông tin được tìm thấy. Nó có lẽ là không đóng gói hoặc obfuscated

Ở đây có đường dẫn vào file

`\system32\wupdmgrd.exe`

`\system32\wupdmgr.exe`

`\winup.exe`

<http://www.practicalmalwareanalysis.com/updater.exe> là một chỉ báo dựa trên mạng rằng phần mềm độc hại này có mặt.

Nó sử dụng KERNEL32.dll , MSVCRT.dll và urlmon.dll

Để kiểm tra các chức năng được imports trong chương trình ta sử dụng IDA kiểm tra

IDAPro không có vấn đề gì khi tải tệp sao cho không có cảnh báo về đóng gói hoặc làm xáo trộn.

Address	Ordinal	Name	Library
00402000		OpenProcessToken	ADVAPI32
00402004		LookupPrivilegeValueA	ADVAPI32
00402008		AdjustTokenPrivileges	ADVAPI32
00402010		GetProcAddress	KERNEL32
00402014		LoadLibraryA	KERNEL32
00402018		WinExec	KERNEL32
0040201C		WriteFile	KERNEL32
00402020		CreateFileA	KERNEL32
00402024		SizeofResource	KERNEL32
00402028		CreateRemoteThread	KERNEL32
0040202C		FindResourceA	KERNEL32
00402030		GetModuleHandleA	KERNEL32
00402034		GetWindowsDirectoryA	KERNEL32
00402038		MoveFileA	KERNEL32
0040203C		GetTempPathA	KERNEL32
00402040		GetCurrentProcess	KERNEL32

ở đây có 1 số imports đáng chú ý:

**LoadResource, FindResourceA** : cho biết rằng dữ liệu được tải từ phần tài nguyên

**GetWindowsDirectoryA** : chỉ ra rằng các tệp tin có thể được ghi vào thư mục hệ thống

**WinExec** : chỉ ra rằng một chương trình được thực hiện

**WriteFileA, CreateFileA, MoveFileA**: cho biết rằng một tệp được tạo, ghi vào và có thể di chuyển

**OpenProcessToken, LookupPrivilegeValueA, AdjustTokenPrivileges, CreateRemoteThread, FindResourceA**

Name	Address	Ordinal
BeginFileMapEnumeration	10007B70	1
CloseFileMapEnumeration	10007BD0	2
GetNextFileMapContent	10007C00	3
SRSetRestorePointA	10007D50	4


ở trên cho thấy phần mềm độc hại đang cố tăng đặc quyền của nó lên SeDebugPrivilege. Sau khi điều chỉnh, nó bắt đầu gọi hàm thứ 2 của sfc\_os.dll là hàm CloseFileMapEnumeration.

## Lab 01-02

Writer: \_\_SÓI\_\_

Trong Lab 01-02 có 1 file Lab01-02.exe chúng ta sẽ bắt đầu đi phân tích tĩnh của con lab này qua file Lab01-02 này.

Đầu tiên thử kiểm tra nó trên [www.virustotal.com](http://www.virustotal.com) 2018-10-04 thì có 42/68 thiết bị có thể phát hiện ra nó. Do đó đây là 1 con malware đã cũ và khá phổ biến.



**42 engines detected this file**  
SHA-256 c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b54eaa362674a2a48f64a6  
File name Lab01-02.exe  
File size 3 KB  
Last analysis 2018-10-04 13:44:37 UTC  
Community score -165

42 / 69

tectionDetailsRelationsBehaviorCommunity6

AegisLab	Trojan.Win32.Generic.4!c	AhnLab-V3	Trojan/Win32.StartPage.C26214
ALYac	Trojan.Startpage.3072	Antiy-AVL	Trojan/Win32.SGeneric
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira	TR/Downloader.Gen	AVware	Trojan.Win32.Generic!BT
Baidu	Win32.Trojan-Clicker.AgentLad	CAT-QuickHeal	Trojan.Dynamer!ac
ClamAV	Win.Malware.Agent-6350563-0	CrowdStrike Falcon	malicious_confidence_100% (W)
Cybereason	malicious.cbcb77	Cylance	Unsafe
Cyren	W32/Trojan.UCOC-9169	DrWeb	Trojan.Click3.12740
Endgame	malicious (moderate confidence)	ESET-NOD32	Win32/TrojanClicker.AgentLNVM
Fortinet	W32/Agent.NVM!tr	GData	Win32.Trojan.AgentLJV4QJM
Ikarus	Trojan.Win32.TrojanClicker	Jiangmin	Trojan.Generic.fxlq
MAX	malware (ai score=98)	McAfee	Generic.ait

## Kiểm tra packed hoặc obfuscated

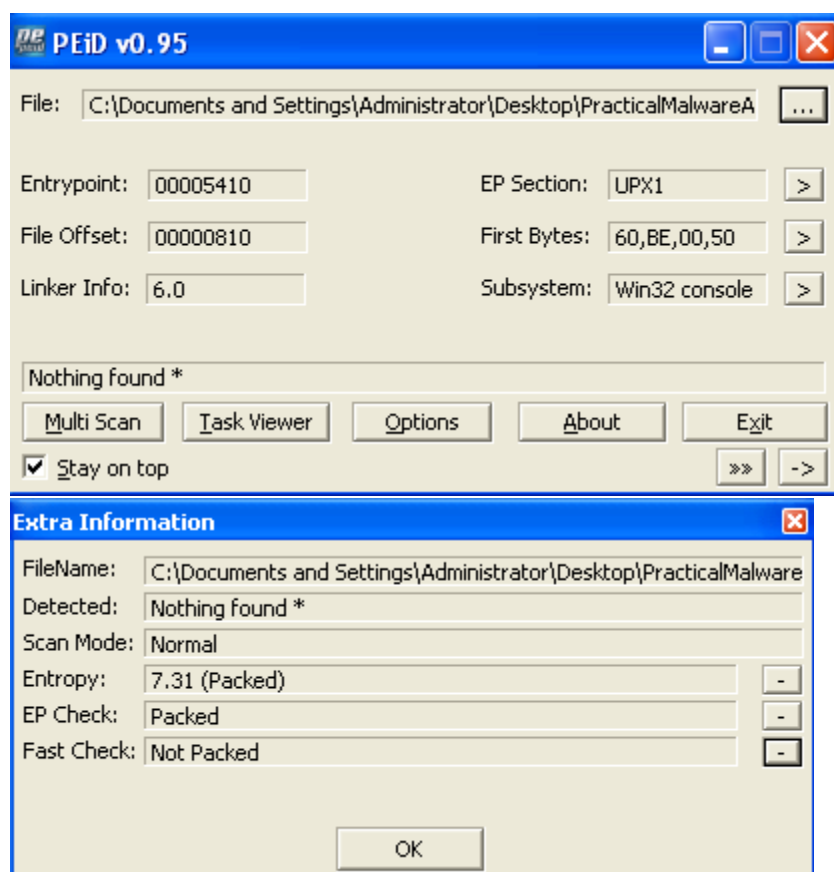
- Sử dụng Strings:  
Strings lab01-02.exe

```
8P1PSW
KERNEL32.DLL
ADVAPI32.dll
MSUCRT.dll
WININET.dll
LoadLibraryA
GetProcAddress
VirtualProtect
VirtualAlloc
VirtualFree
ExitProcess
CreateServiceA
exit
InternetOpenA

C:\Documents and Settings\Administrator\Desktop\PracticalMalwareAnalysis-Labs-master\Practical Malware Analysis Labs\BinaryCollection\Chapter_1L>
```

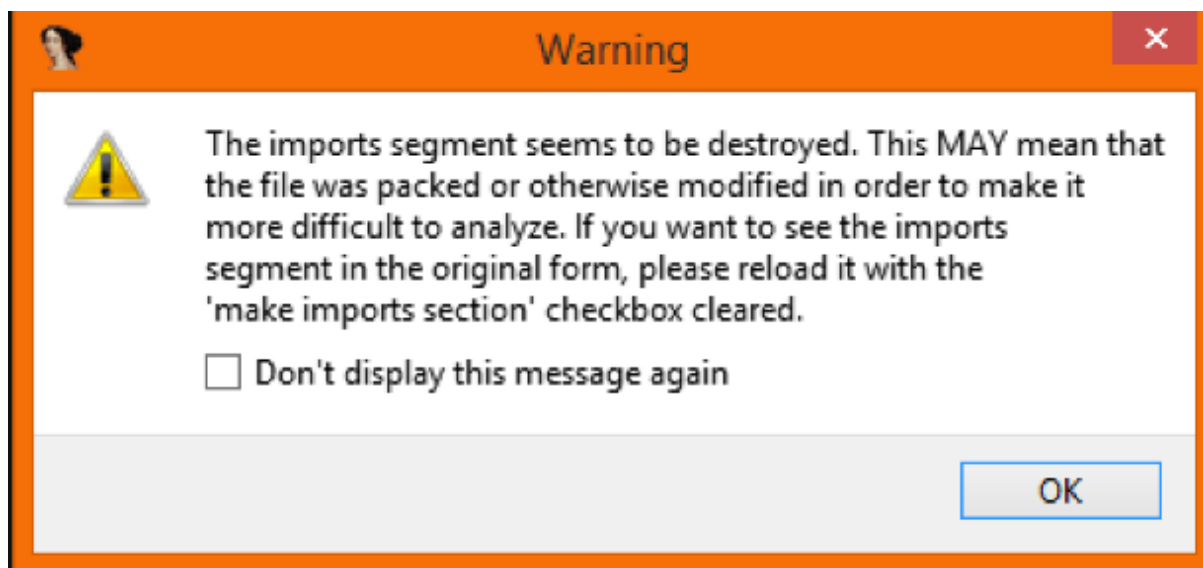
Ở đây ta thấy nó hiển thị rất ít các chuỗi có thể file này đã bị pack. Để kiểm tra ta sẽ sử dụng thêm những phần mềm khác để kiểm tra.

- Sử dụng PEID



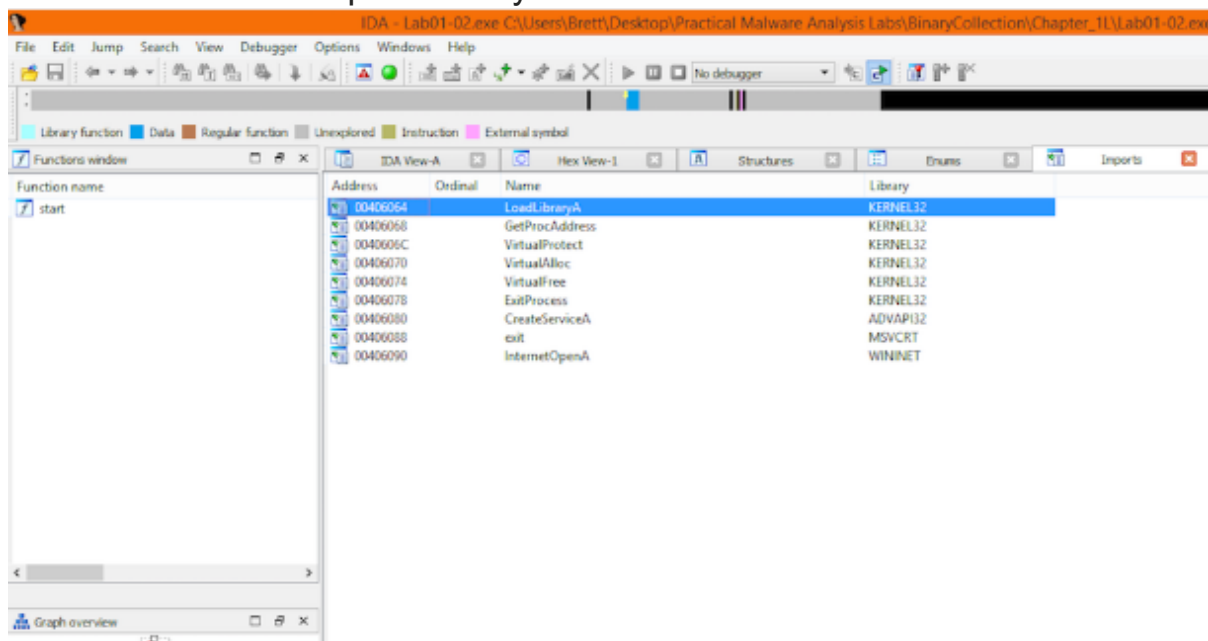
Khi chạy PEid, nó không tìm thấy cách packed cụ thể nhưng "EP Section" cho thấy UPX1 đây chính là cách đã packed file

## - Sử dụng PEView



Thông báo này xuất hiện chứng tỏ rằng file này đã bị pack hoặc bị obfuscated.

Khi mở danh sách imports ở đây có khá ít .



## - Tiến hành unpack



Sử dụng **UPX**, để file upx.exe chung với thư mục chứa file Lap01-02.exe sau đó chạy dòng lệnh

Upx -o trung.exe -d lab01-02.exe

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator\Desktop>upx -o trung.exe -d Lab01-02.exe

      Ultimate Packer for eXecutables
      Copyright (C) 1996 - 2018
UPX 3.95w      Markus Oberhumer, Laszlo Molnar & John Reiser   Aug 26th 2018

-----
File size      Ratio      Format      Name
-----
16384 <-      3072      18.75%      win32/pe      trung.exe
Unpacked 1 file.
```

Đề ý lúc này file lab01-02.exe có dung lượng là 3kb còn file trung.exe có dung lượng là 16kb. Như vậy file lab01-02.exe đã được unpack thành file trung.exe

Giờ chúng ta thử kiểm tra lại các chuỗi strings của trung.exe



```

KERNEL32.DLL
ADVAPI32.dll
MSUCRT.dll
WININET.dll
SystemTimeToFileTime
GetModuleFileNameA
CreateWaitableTimerA
ExitProcess
OpenMutexA
SetWaitableTimer
WaitForSingleObject
CreateMutexA
CreateThread
CreateServiceA
StartServiceCtrlDispatcherA
OpenSCManagerA
_exit
_XcptFilter
exit
__p__initenv
__getmainargs
__initterm
__setusermatherr
__adjust_fdiv
__p__commode
__p__fmode
__set_app_type
__except_handler3
__controlfp
InternetOpenUrlA
InternetOpenA
MalService
MalService
HGL345
http://www.malwareanalysisbook.com
Internet Explorer 8.0

C:\Documents and Settings\Administrator\Desktop\PracticalMalwareAna
ster\Practical Malware Analysis Labs\BinaryCollection\Chapter_1L>

```

Có khá nhiều các chuỗi string ở đây, có 1 số string đáng chú ý là

**CreateServiceA**

**StartServiceCtrlDispatcherA**

**OpenSCManager**

**InternetOpenUrlA**

**InternetOpenA**

**CreatThread**

có vẻ như phần mềm độc hại này đã thiết lập dịch vụ Windows. Nó cũng xuất hiện để liên hệ với một url.

Nó được giao tiếp với mạng tại địa chỉ:

<http://www.malwareanalysisbook.com>

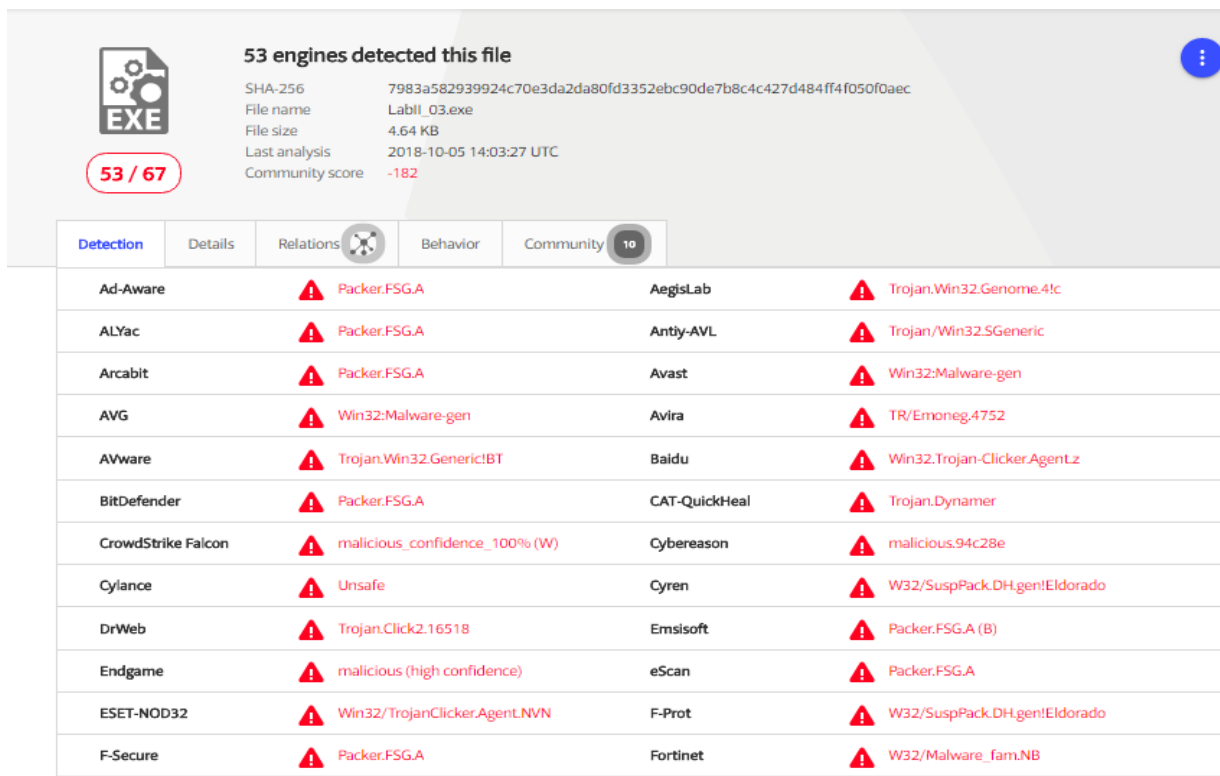
và sử dụng Internet Explorer 8.0

## Lab 01-03

Writer: \_\_SÓI\_\_

Trong Lab 01-03 có 1 file Lab01-03.exe chúng ta sẽ bắt đầu đi phân tích tĩnh của con lab này qua file Lab01-03 này.

Đầu tiên thử kiểm tra nó trên [www.virustotal.com](http://www.virustotal.com) 2018-10-05 thì có 53/67 thiết bị có thể phát hiện ra nó.



The screenshot shows the VirusTotal analysis interface for a file named Lab01-03.exe. The file is identified as a PE32 executable (EXE) with a size of 4.64 KB. It was last analyzed on 2018-10-05 at 14:03:27 UTC. The community score is -182. The analysis shows that 53 out of 67 engines detected the file as malicious. The detected signatures are listed in a table below.

Detection	Details	Relations	Behavior	Community
Ad-Aware	⚠ Packer.FSG.A	AegisLab	⚠ Trojan.Win32.Genome.4!c	
ALYac	⚠ Packer.FSG.A	Antiy-AVL	⚠ Trojan/Win32.SGeneric	
Arcabit	⚠ Packer.FSG.A	Avast	⚠ Win32:Malware-gen	
AVG	⚠ Win32:Malware-gen	Avira	⚠ TR/Emonneg.4752	
AVware	⚠ Trojan.Win32.Generic!BT	Baidu	⚠ Win32:Trojan-Clicker.AgentLz	
BitDefender	⚠ Packer.FSG.A	CAT-QuickHeal	⚠ Trojan.Dynamer	
CrowdStrike Falcon	⚠ malicious_confidence_100% (W)	Cybereason	⚠ malicious.94c28e	
Cylance	⚠ Unsafe	Cyren	⚠ W32/SuspPack.DH.gen!Eldorado	
DrWeb	⚠ Trojan.Click2.16518	Emsisoft	⚠ Packer.FSG.A (B)	
Endgame	⚠ malicious (high confidence)	eScan	⚠ Packer.FSG.A	
ESET-NOD32	⚠ Win32/TrojanClicker.AgentLNVN	F-Prot	⚠ W32/SuspPack.DH.gen!Eldorado	
F-Secure	⚠ Packer.FSG.A	Fortinet	⚠ W32/Malware_fam.NB	

Tiếp theo chúng ta sẽ kiểm tra xem nó có bị pack hay obfusacated không.

### - Kiểm tra chuỗi Strings

```
C:\WINDOWS\system32\cmd.exe
ster\Practical Malware Analysis Labs\BinaryCollection\Chapter_1L>strings Lab01-0
3.exe

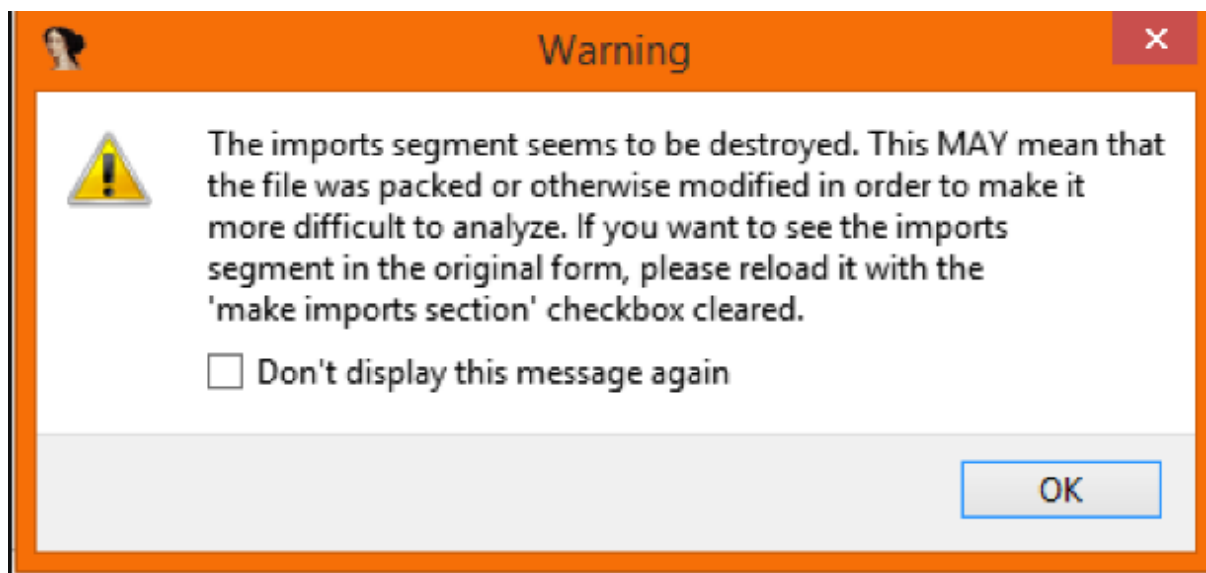
Strings v2.53 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

!Windows Program
$PE
b!@
`.rdata
@.data
$S!
;Ot
<Q@
KERNEL32.dll
LoadLibraryA
GetProcAddress
H @
Ph8
0IX
":Ll
3Bt>0
UQ<8
2l<,M
:R,
P@M^
S>UW
AQ=h
"Z,
5pg
k,
^J%
I*G9>
<*T
p@l
e%nN
kQc
H @
ole32.vd
Init
FoCr
U!C
>OLEAUTL
IMSVCRTI"b
_getmas
yrce
iP2r3Us
p!uuy
fmod
xP*1
9mU
dj
C:\Documents and Settings\Administrator\Desktop\PracticalMalwareAnalysis-Labs-ma
```

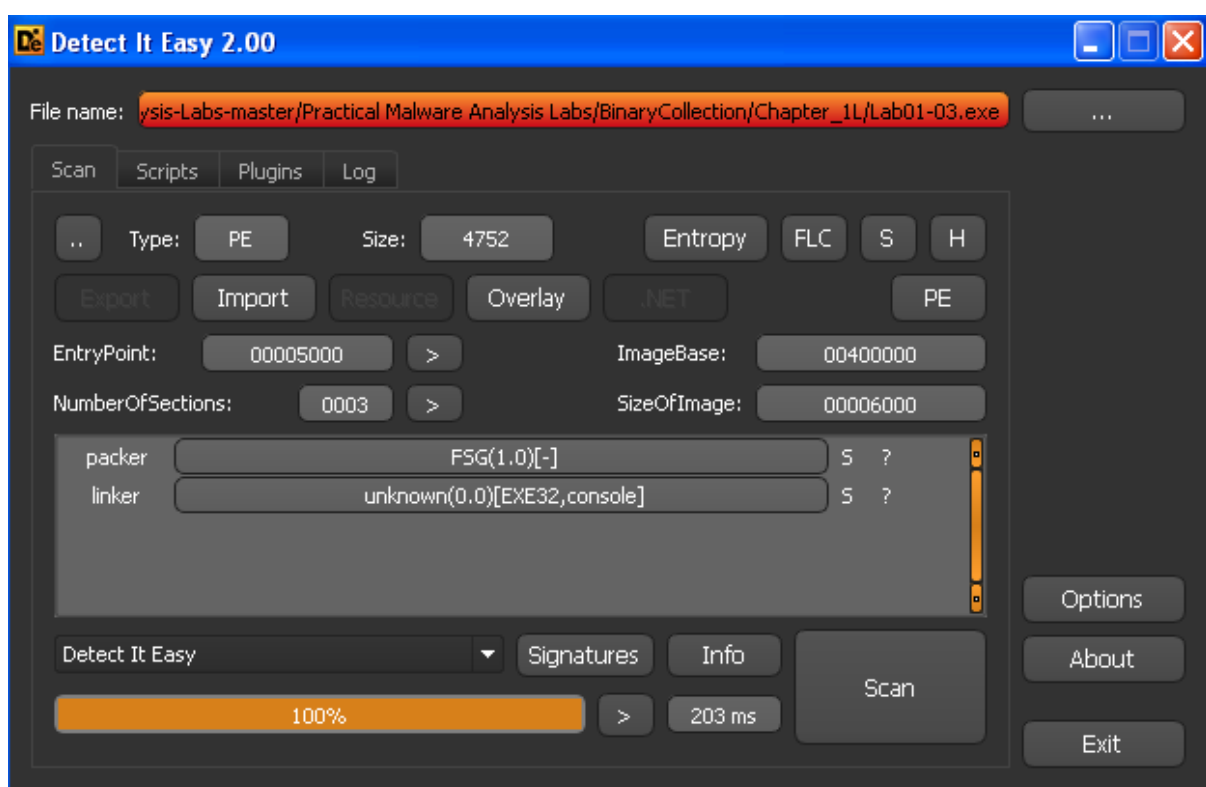
Chạy chuỗi dường như chỉ tiết lộ một vài chuỗi cơ bản là LoadLibraryA và GetProcAddress. Vì các chức năng này thường được gọi là phần mềm độc hại đóng gói và có một vài chuỗi dễ đọc khác, có vẻ như phần mềm độc hại này có thể được đóng gói.

## - IDAPro

Thông báo này chứng tỏ file này đã bị pack hoặc Obfuscated.



## - Detect it Easy



Ở đây chúng ta có thể thấy lab01-03.exe đã bị pack bằng phương thức FSG 1.0

Để biết thêm về lab01-03 chúng ta buộc phải unpack nó bằng fsg 1.0, tuy nhiên cho đến thời điểm hiện tại thì mình chưa thể unpack nó nên chúng ta tạm dừng phân tích nó ở đây chờ tới phần sau mình unpack nó và sẽ phân tích nó tiếp ^^

Cảm Ơn Mọi Người Đã Theo Dõi Bài Viết Của Mình ^^

\_\_SÓI\_\_