

HỌC VIỆN KỸ THUẬT MẬT MÃ
KHOA AN TOÀN THÔNG TIN

MODULE THỰC HÀNH
MÃ ĐỘC

BÀI THỰC HÀNH SỐ 06

Phân tích một số hành vi của mã độc

Người thực hiện bài thực hành:

TS. Đặng Xuân Bảo

Hà Nội, 2020

MỤC LỤC

THÔNG TIN CHUNG VỀ BÀI THỰC HÀNH.....	3
CHUẨN BỊ BÀI THỰC HÀNH.....	4
Phân tích một số hành vi mã độc	5
1.1. Mô tả	5
1.2. Chuẩn bị	5
1.3. Phân tích Lab11-01	5
PHÂN TÍCH TĨNH.....	5
PHÂN TÍCH ĐỘNG.....	7

THÔNG TIN CHUNG VỀ BÀI THỰC HÀNH

Tên bài thực hành: Phân tích một số hành vi của mã độc

Học phần: Mã độc

Số lượng sinh viên cùng thực hiện:

Địa điểm thực hành: Phòng máy

Yêu cầu:

- Yêu cầu phần cứng:
 - + Máy tính với cấu hình tối thiểu: CPU 2.0 GHz, RAM 4GB, HDD 500GB
- Yêu cầu phần mềm trên máy:
 - + Hệ điều hành Windows 10
 - + VMware Workstation 15.0
- Yêu cầu kết nối mạng LAN: có
- Yêu cầu kết nối mạng Internet: có

CHUẨN BỊ BÀI THỰC HÀNH

Đối với giảng viên

Trước buổi học, giảng viên (người hướng dẫn thực hành) cần kiểm tra sự phù hợp của điều kiện thực tế của phòng thực hành với các yêu cầu của bài thực hành.

Ngoài ra không đòi hỏi gì thêm.

Đối với sinh viên

Trước khi bắt đầu thực hành, cần tạo các bản sao của máy ảo để sử dụng. Đồng thời xác định vị trí lưu trữ các công cụ đã chỉ ra trong phần yêu cầu.

Phân tích một số hành vi mã độc

1.1. Mô tả

Bài thực hành hướng dẫn sinh viên sử dụng một số công cụ trong việc phân tích động một số mẫu mã độc đơn giản..

1.2. Chuẩn bị

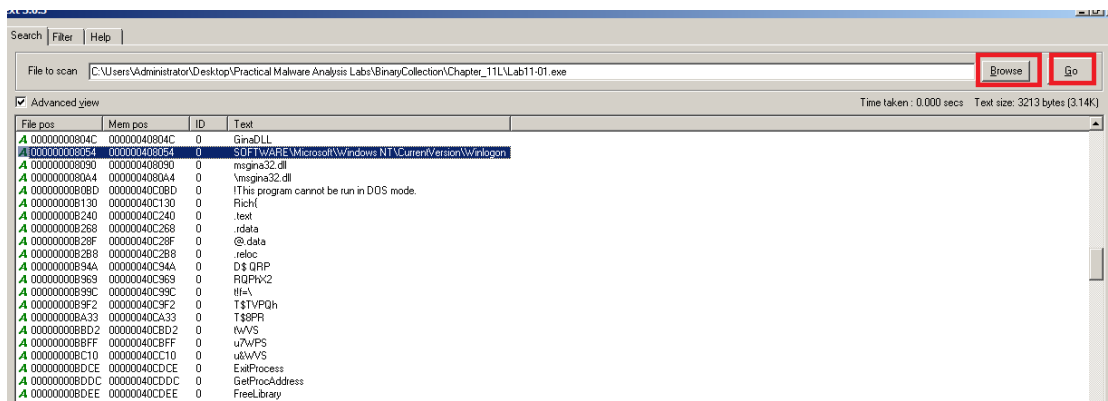
- Môi trường phân tích mã độc đã xây dựng trong Lab 1.

1.3. Phân tích Lab11-01

Trong bài thực hành này, chúng ta sẽ thực hành file Lab11-1.exe.

PHÂN TÍCH TĨNH

Sử dụng công cụ Bintext



- Hai mục cần lưu ý:
 - SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon
 - Gina.DLL

File pos	Mem pos	ID	Text
00000000804C	00000040804C	0	Gina.dll
000000008054	000000408054	0	SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
000000008058	000000408058	0	msgina32.dll
0000000080A4	0000004080A4	0	\msgina32.dll
0000000080BD	00000040C0BD	0	!This program cannot be run in DOS mode.
000000008130	00000040C130	0	RichI
000000008240	00000040C240	0	.text
000000008268	00000040C268	0	.rdata
00000000828F	00000040C28F	0	@.data
0000000082B8	00000040C2B8	0	.reloc
00000000894A	00000040C94A	0	D\$ QRP
000000008969	00000040C969	0	RQPhx2
00000000899C	00000040C99C	0	tf=\
0000000089F2	00000040C9F2	0	T\$TVPQh
000000008A33	00000040CA33	0	T\$8PR
000000008BD2	00000040CBD2	0	twVS
000000008BEE	00000040CBE	0	u7WPS
000000008F42	00000040CF42	0	RegSetValueExW
000000008F54	00000040CF54	0	RegCreateKeyW
000000008F62	00000040CF62	0	ADVAPI32.dll
000000008F72	00000040CF72	0	wsprintfA
000000008F7C	00000040CF7C	0	USER32.dll
00000000C118	00000040D118	0	gina.dll
00000000C121	00000040D121	0	DllRegister
00000000C12D	00000040D12D	0	DllUnregister
00000000C13B	00000040D13B	0	ShellShutdownDialog
00000000C14F	00000040D14F	0	WlxActivateUserShell
00000000C164	00000040D164	0	WlxDisconnectNotify
00000000C178	00000040D178	0	WlxDisplayLockedNotice
00000000C18F	00000040D18F	0	WlxDisplaySASNotice
00000000C1A3	00000040D1A3	0	WlxDisplayStatusMessage
00000000C1BB	00000040D1BB	0	WlxGetConsoleSwitchCredentials
00000000C1DA	00000040D1DA	0	WlxGetStatusMessage
00000000C1EE	00000040D1EE	0	WlxInitialize
00000000C1FC	00000040D1FC	0	WlxLockOk

Những chuỗi này gợi ý đây là phần mềm độc hại có chứa thành phần tác động lên GINA.

Công cụ PReview

Chú ý đến những dòng sau đây.

- RegSetValueExA
- RegCreateKeyExA
- SizeofResource
- LockResource
- LoadResource

PEview - C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_11\Lab11-01.exe

	pFile	Data	Description	Value
Lab11-01.exe				
IMAGE_DOS_HEADER	00007000	000076AC	Hint/Name RVA	0186 RegSetValueExA
MS-DOS Stub Program	00007004	000076BE	Hint/Name RVA	015F RegCreateKeyExA
IMAGE_NT_HEADERS	00007008	00000000	End of Imports	ADVAPI32.dll
IMAGE_SECTION_HEADER	0000700C	00007632	Hint/Name RVA	0295 SizeofResource
IMAGE_SECTION_HEADER	00007010	00007644	Hint/Name RVA	01D5 LockResource
IMAGE_SECTION_HEADER	00007014	00007654	Hint/Name RVA	01C7 LoadResource
IMAGE_SECTION_HEADER	00007018	00007622	Hint/Name RVA	02BB VirtualAlloc
SECTION .text	0000701C	00007674	Hint/Name RVA	0124 GetModuleFileNameA
SECTION .idata	00007020	0000768A	Hint/Name RVA	0126 GetModuleHandleA
IMPORT Address Table	00007024	00007612	Hint/Name RVA	00B6 FreeResource
IMPORT Directory Table	00007028	00007664	Hint/Name RVA	00A3 FindResourceA
IMPORT Name Table	0000702C	00007604	Hint/Name RVA	001B CloseHandle
IMPORT Hints/Names & Ordinals	00007030	000076DE	Hint/Name RVA	00CA GetCommandLineA
SECTION .data	00007034	000076F0	Hint/Name RVA	0174 GetVersion
SECTION .rsrc	00007038	000076FE	Hint/Name RVA	007D ExitProcess
	0000703C	0000770C	Hint/Name RVA	019F HeapFree
	00007040	00007718	Hint/Name RVA	011A GetLastError
	00007044	00007728	Hint/Name RVA	02DF WriteFile
	00007048	00007734	Hint/Name RVA	029E TerminateProcess
	0000704C	00007748	Hint/Name RVA	00F7 GetCurrentProcess
	00007050	0000775C	Hint/Name RVA	02AD UnhandledExceptionFilter

Các lệnh API này cho thấy phần mềm độc hại đăng ký key vào registry và trích xuất phần tài nguyên.

– BINARY TGAD 0000.

PEview - C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_11\Lab11-01.exe

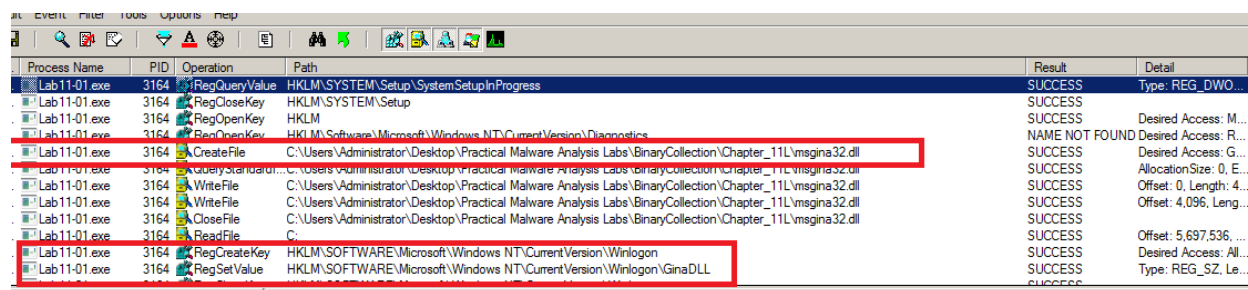
	pFile	Raw Data	Value
Lab11-01.exe			
IMAGE_DOS_HEADER	0000B1E0	00 00 00 00 00 00 00 00 00 40 00 00 AC 00 00 00@.....
MS-DOS Stub Program	0000B1F0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
IMAGE_NT_HEADERS	0000B200	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
IMAGE_SECTION_HEADER	0000B210	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
IMAGE_SECTION_HEADER	0000B220	00 20 00 00 7C 00 00 00 00 00 00 00 00 00 00 00
IMAGE_SECTION_HEADER	0000B230	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
IMAGE_SECTION_HEADER	0000B240	2E 74 65 78 74 00 00 00 D8 07 00 00 00 10 00 00	..text.....
SECTION .text	0000B250	00 08 00 00 00 00 04 00 00 00 00 00 00 00 00 00
SECTION .idata	0000B260	00 00 00 00 20 00 00 60 2E 72 64 61 74 61 00 00rdata..
IMPORT Address Table	0000B270	64 06 00 00 00 20 00 00 00 08 00 00 00 0C 00 00	d.....
IMPORT Directory Table	0000B280	00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40@..@
IMPORT Name Table	0000B290	2E 64 61 74 61 00 00 00 08 04 00 00 00 30 00 00	..data.....0..
IMPORT Hints/Names & Ordinals	0000B2A0	00 04 00 00 00 14 00 00 00 00 00 00 00 00 00 00
SECTION .data	0000B2B0	00 00 00 00 40 00 00 C0 2E 72 65 6C 6F 63 00 00@...reloc..
SECTION .rsrc	0000B2C0	F0 00 00 00 00 40 00 00 00 02 00 00 00 18 00 00@.....
IMAGE_RESOURCE_DATA_ENTRY	0000B2D0	00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42@..B
IMAGE_RESOURCE_DATA_ENTRY	0000B2E0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
IMAGE_RESOURCE_DATA_ENTRY	0000B2F0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
IMAGE_RESOURCE_DATA_ENTRY	0000B300	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
IMAGE_RESOURCE_DATA_ENTRY	0000B310	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
BINARY TGAD 0000	0000B320	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
	0000B330	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
	0000B340	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
	0000B350	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
	0000B360	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
	0000B370	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Đây là tệp PE, được giấu trong phần resource.

PHÂN TÍCH ĐỘNG

Công cụ Procmon

- Trong Procmon chọn Filter, Reset Filter.
- Chọn Filter, Filter, Filter tên cần lọc là Lab11-01.exe.
- Ta được kết quả sau:
 - CreateFile ... msgina32.dll or IRP_MU_CREATE ... msgina.dll
 - RegCreateKey
HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon
 - RegSetValue
HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\GinaDLL

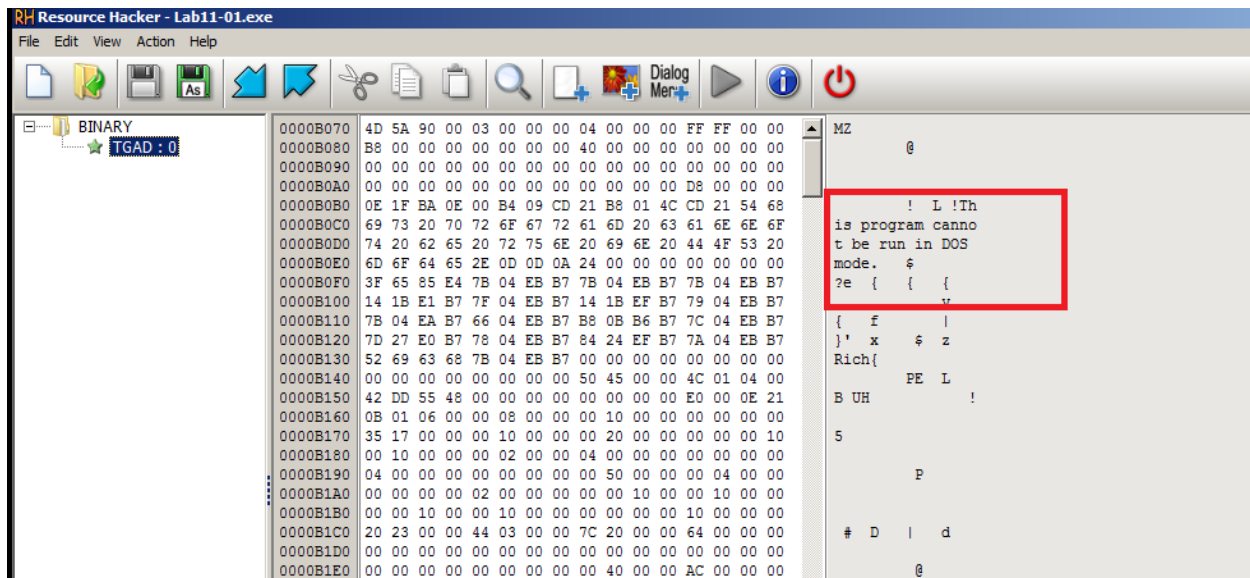


Process Name	PID	Operation	Path	Result	Detail
Lab11-01.exe	3164	RegQueryValue	HKLM\SYSTEM\Setup\SystemSetupProgress	SUCCESS	Type: REG_DWO...
Lab11-01.exe	3164	RegCloseKey	HKLM\SYSTEM\Setup	SUCCESS	
Lab11-01.exe	3164	RegOpenKey	HKLM\SYSTEM\Setup	SUCCESS	
Lab11-01.exe	3164	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Diagnostics	NAME NOT FOUND	Desired Access: R...
Lab11-01.exe	3164	CreateFile	C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_11\msgina32.dll	SUCCESS	Desired Access: G...
Lab11-01.exe	3164	QueryStandard...	C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_11\msgina32.dll	SUCCESS	AllocationSize: 0, E...
Lab11-01.exe	3164	WriteFile	C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_11\msgina32.dll	SUCCESS	Offset: 0, Length: 4...
Lab11-01.exe	3164	CloseFile	C:\Users\Administrator\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_11\msgina32.dll	SUCCESS	Offset: 4,096, Leng...
Lab11-01.exe	3164	ReadFile	C:	SUCCESS	Offset: 5,697,536, ...
Lab11-01.exe	3164	RegCreateKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS	Desired Access: All...
Lab11-01.exe	3164	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GinaDLL	SUCCESS	Type: REG_SZ, Le...

Những hành động tạo ra một tệp có tên là msgina.dll và chèn một đường dẫn đến tệp đó vào các khóa đăng ký sẽ khởi chạy DLL khi hệ thống khởi động.

Công cụ Resource Hacker

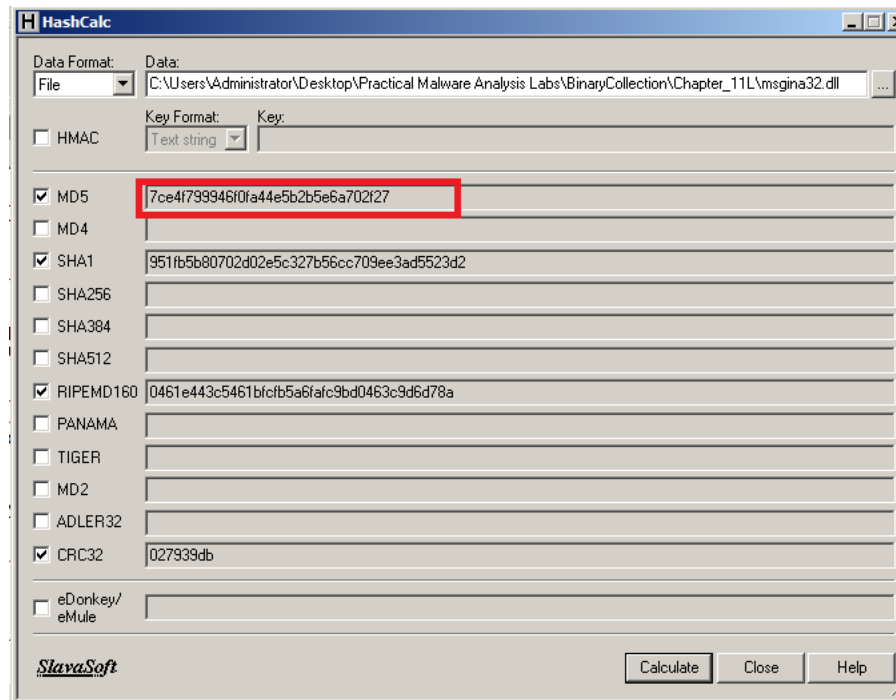
- Sử dụng công cụ Resource Hacker để trích xuất file gina.dll
- Sau khi mở file Lab11-01.exe ta được kết quả:
 - BINARY TGAD 0 bắt đầu với MZ và chứa một thông báo “Chương trình này không thể chạy trong chế độ DOS, đây là tệp exe.



- Chọn Action, Save resource as a binary file ...
- Lưu tên file có dạng YOURNAME-TGAD0.exe

Công cụ HashCalc

- Tính toán hàm băm MD5 của file msgina32.dll được tạo bằng các chạy phần mềm độc hại (thực hiện ở Procmon), ta được kết quả mã MD5 bắt đầu với 7ce4:



- Tính toán MD5 của tệp tin YOURNAME-TGAD0.exe (được tạo ở công cụ Resource Hacker), ta được kết quả mã MD5 cũng được bắt đầu với 7ce4:

