TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TP HCM

KHOA CÔNG NGHỆ THÔNG TIN

Môn: Thực Hành Phân Tích Mã Độc

Họ Và Tên: Trần Hân Nhi

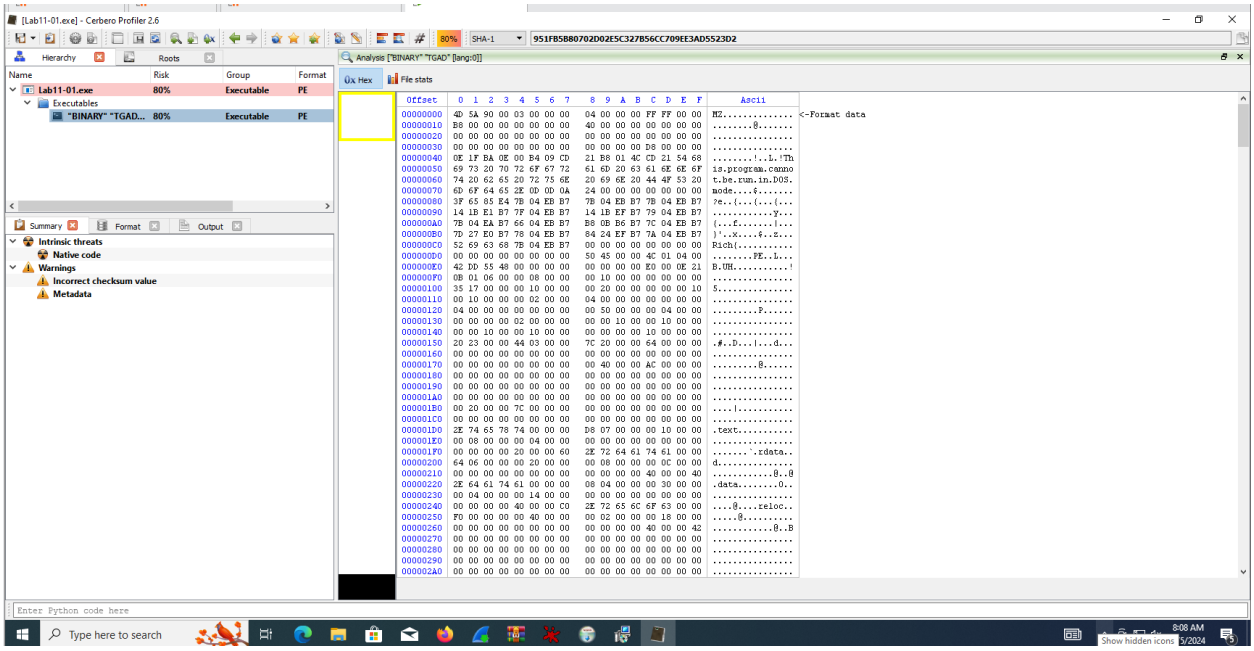
MSSV: 2011770131

Lớp: 20DATA1

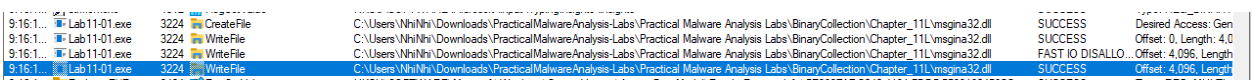
Báo cáo tuần 6

Lab 11-01:

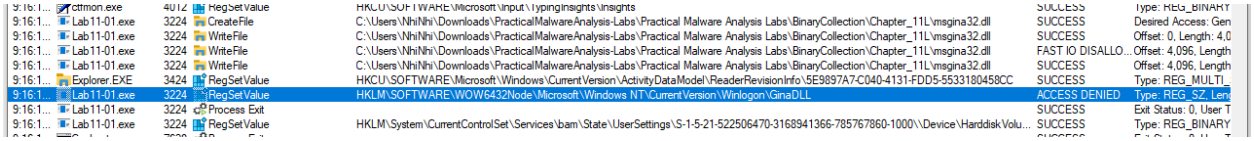
Tập tin nhị phân trong phần mã nguồn của Lab 11-01.exe



Từ Proc Mon, chúng ta có thể quan sát thấy msgina32.dll

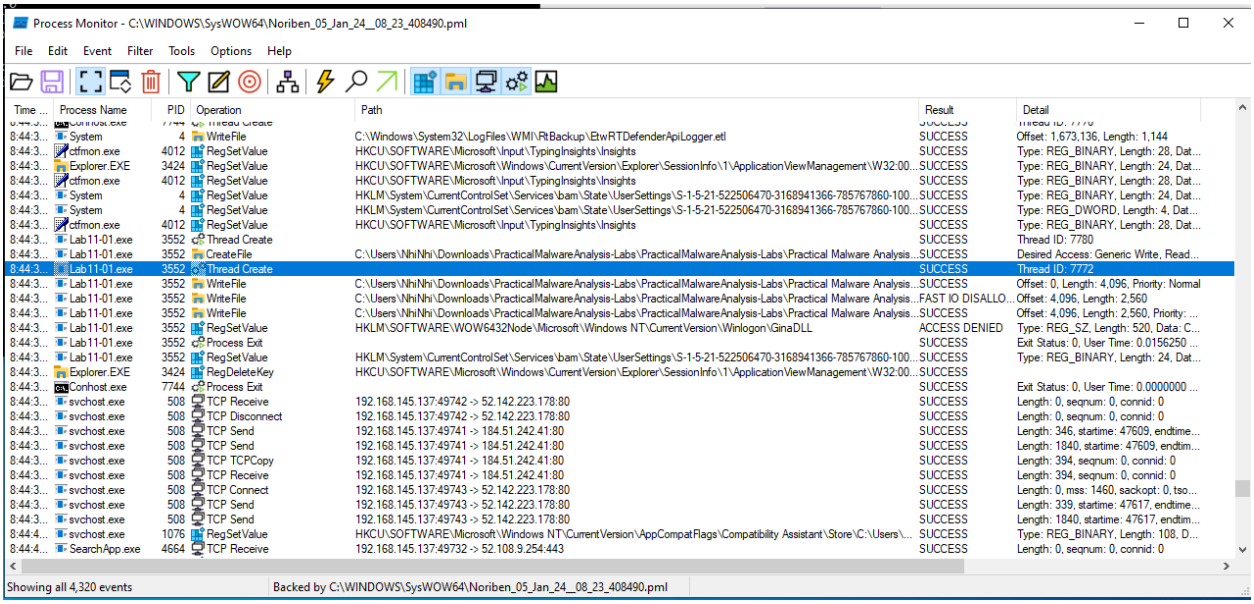


Trong hình trên, mã độc thêm “HKLM \ SOFTWARE \ Microsoft \ Windows NT \ CurrentVersion \ Winlogon \ GinaDLL” vào sổ đăng ký.



9:16:1...	ctfmon.exe	4012	RegSetValue	HKCU\SOFTWARE\Microsoft\Input\TypingInsights\Insights	SUCCESS	Type: REG_BINARY
9:16:1...	Lab11-01.exe	3224	CreateFile	C:\Users\NhiNhi\Downloads\PracticalMalwareAnalysis-Labs\Practical Malware Analysis Labs\BinaryCollection\Chapter_11L\msgina32.dll	SUCCESS	Desired Access: Gen
9:16:1...	Lab11-01.exe	3224	WriteFile	C:\Users\NhiNhi\Downloads\PracticalMalwareAnalysis-Labs\Practical Malware Analysis Labs\BinaryCollection\Chapter_11L\msgina32.dll	SUCCESS	Offset: 0, Length: 4,0
9:16:1...	Lab11-01.exe	3224	WriteFile	C:\Users\NhiNhi\Downloads\PracticalMalwareAnalysis-Labs\Practical Malware Analysis Labs\BinaryCollection\Chapter_11L\msgina32.dll	FAST IO DISALLO...	Offset: 4,096, Length
9:16:1...	Lab11-01.exe	3224	WriteFile	C:\Users\NhiNhi\Downloads\PracticalMalwareAnalysis-Labs\Practical Malware Analysis Labs\BinaryCollection\Chapter_11L\msgina32.dll	SUCCESS	Offset: 4,096, Length
9:16:1...	Explorer.EXE	3424	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\ActivityDataModel\ReaderRevisionInfo\5E9897A7-C040-4131-FDD5-5533180458CC	SUCCESS	Type: REG_MULTI
9:16:1...	Lab11-01.exe	3224	RegSetValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon\GinaDLL	ACCESS DENIED	Type: REG_SZ, Len
9:16:1...	Lab11-01.exe	3224	Process Exit		SUCCESS	Exit Status: 0, User T
9:16:1...	Lab11-01.exe	3224	RegSetValue	HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-522506470-3168941366-785767860-1000\\Device\HarddiskVolu...	SUCCESS	Type: REG_BINARY

Winlogon , GINA và các nhà cung cấp mạng là các phần của mô hình đăng nhập tương tác. Thủ tục đăng nhập được kiểm soát bởi Winlogon, MSGina.dll và các nhà cung cấp mạng. Để thay đổi quy trình đăng nhập, MSGina.dll có thể được thay thế bằng GINA DLL tùy chỉnh. Winlogon sẽ kích hoạt việc sử dụng dll độc hại và đó là cách mã độc đạt được sự bền bỉ.



Time ...	Process Name	PID	Operation	Path	Result	Detail
8:44:3...	System	4	WriteFile	C:\Windows\System32\LogFiles\WMI\RtBackup\EtwRTDefenderApiLogger.etl	SUCCESS	Offset: 1,673,136, Length: 1,144
8:44:3...	ctfmon.exe	4012	RegSetValue	HKCU\SOFTWARE\Microsoft\Input\TypingInsights\Insights	SUCCESS	Type: REG_BINARY, Length: 28, Dat...
8:44:3...	Explorer.EXE	3424	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00...	SUCCESS	Type: REG_BINARY, Length: 24, Dat...
8:44:3...	ctfmon.exe	4012	RegSetValue	HKCU\SOFTWARE\Microsoft\Input\TypingInsights\Insights	SUCCESS	Type: REG_BINARY, Length: 28, Dat...
8:44:3...	System	4	RegSetValue	HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-522506470-3168941366-785767860-100...	SUCCESS	Type: REG_BINARY, Length: 24, Dat...
8:44:3...	System	4	RegSetValue	HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-522506470-3168941366-785767860-100...	SUCCESS	Type: REG_DWORD, Length: 4, Dat...
8:44:3...	ctfmon.exe	4012	RegSetValue	HKCU\SOFTWARE\Microsoft\Input\TypingInsights\Insights	SUCCESS	Type: REG_BINARY, Length: 28, Dat...
8:44:3...	Lab11-01.exe	3552	Thread Create		SUCCESS	Thread ID: 7780
8:44:3...	Lab11-01.exe	3552	CreateFile	C:\Users\NhiNhi\Downloads\PracticalMalwareAnalysis-Labs\PracticalMalwareAnalysis-Labs\Practical Malware Analysis...	SUCCESS	Desired Access: Generic Write, Read...
8:44:3...	Lab11-01.exe	3552	Thread Create		SUCCESS	Thread ID: 7772
8:44:3...	Lab11-01.exe	3552	WriteFile	C:\Users\NhiNhi\Downloads\PracticalMalwareAnalysis-Labs\PracticalMalwareAnalysis-Labs\Practical Malware Analysis...	SUCCESS	Offset: 0, Length: 4,096, Priority: Normal
8:44:3...	Lab11-01.exe	3552	WriteFile	C:\Users\NhiNhi\Downloads\PracticalMalwareAnalysis-Labs\PracticalMalwareAnalysis-Labs\Practical Malware Analysis...	FAST IO DISALLO...	Offset: 4,096, Length: 2,560
8:44:3...	Lab11-01.exe	3552	WriteFile	C:\Users\NhiNhi\Downloads\PracticalMalwareAnalysis-Labs\PracticalMalwareAnalysis-Labs\Practical Malware Analysis...	SUCCESS	Offset: 4,096, Length: 2,560, Priority: ...
8:44:3...	Lab11-01.exe	3552	RegSetValue	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon\GinaDLL	ACCESS DENIED	Type: REG_SZ, Length: 520, Data: C...
8:44:3...	Lab11-01.exe	3552	Process Exit		SUCCESS	Exit Status: 0, User Time: 0.0156250 ...
8:44:3...	Lab11-01.exe	3552	RegSetValue	HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-522506470-3168941366-785767860-100...	SUCCESS	Type: REG_BINARY, Length: 24, Dat...
8:44:3...	Explorer.EXE	3424	RegDeleteKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00...	SUCCESS	
8:44:3...	Conhost.exe	7744	Process Exit		SUCCESS	Exit Status: 0, User Time: 0.0000000 ...
8:44:3...	svchost.exe	508	TCP Receive	192.168.145.137:49742 -> 52.142.223.178:80	SUCCESS	Length: 0, seqnum: 0, connid: 0
8:44:3...	svchost.exe	508	TCP Disconnect	192.168.145.137:49742 -> 52.142.223.178:80	SUCCESS	Length: 0, seqnum: 0, connid: 0
8:44:3...	svchost.exe	508	TCP Send	192.168.145.137:49741 -> 184.51.242.41:80	SUCCESS	Length: 346, startime: 47609, endtime...
8:44:3...	svchost.exe	508	TCP Send	192.168.145.137:49741 -> 184.51.242.41:80	SUCCESS	Length: 1840, startime: 47609, endtim...
8:44:3...	svchost.exe	508	TCP TCPCopy	192.168.145.137:49741 -> 184.51.242.41:80	SUCCESS	Length: 394, seqnum: 0, connid: 0
8:44:3...	svchost.exe	508	TCP Receive	192.168.145.137:49741 -> 184.51.242.41:80	SUCCESS	Length: 394, seqnum: 0, connid: 0
8:44:3...	svchost.exe	508	TCP Connect	192.168.145.137:49743 -> 52.142.223.178:80	SUCCESS	Length: 0, mss: 1460, sackopt: 0, tso...
8:44:3...	svchost.exe	508	TCP Send	192.168.145.137:49743 -> 52.142.223.178:80	SUCCESS	Length: 339, startime: 47617, endtime...
8:44:3...	svchost.exe	508	TCP Send	192.168.145.137:49743 -> 52.142.223.178:80	SUCCESS	Length: 1840, startime: 47617, endtim...
8:44:4...	svchost.exe	1076	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store\C:\Users\...	SUCCESS	Type: REG_BINARY, Length: 108, D...
8:44:4...	SearchApp.exe	4664	TCP Receive	192.168.145.137:49732 -> 52.108.9.254:443	SUCCESS	Length: 0, seqnum: 0, connid: 0

Các đầu vào được chuyển cho hàm WlxLoggedOutSAS ban đầu và một bản sao của các đầu vào được chuyển cho một hàm để ghi vào tập tin.

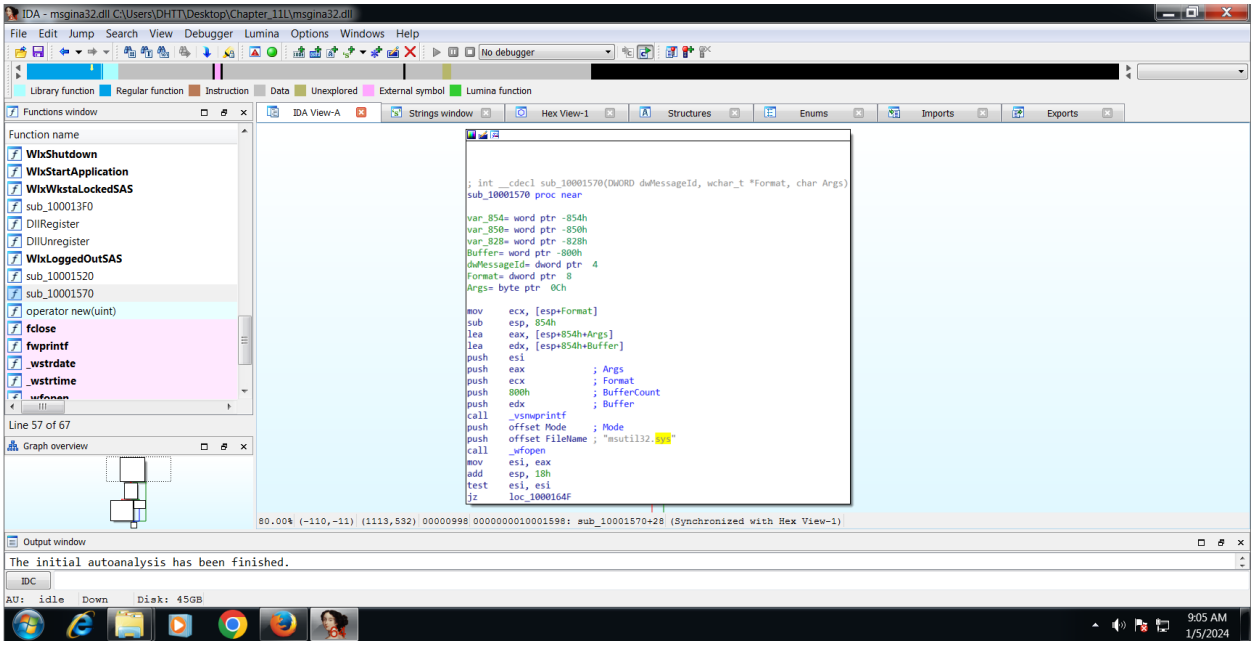
```
; Exported entry  41. WlxLoggedOutSAS


; int __stdcall WlxLoggedOutSAS(PVOID pWlxContext, DWORD dwSasType, PLUID pAuthenticationId, PSID pLogonSid, PDWORD pdwOptions, PHANDLE phToken, PWLX_MPR_NOTIFY_INFO pNprNotifyInfo
public WlxLoggedOutSAS
WlxLoggedOutSAS proc near

pWlxContext= dword ptr  4
dwSasType= dword ptr  8
pAuthenticationId= dword ptr  0Ch
pLogonSid= dword ptr  10h
pdwOptions= dword ptr  14h
phToken= dword ptr  18h
pNprNotifyInfo= dword ptr  1Ch
pProfile= dword ptr  20h

push    esi
push    edi
push    offset aWlxloggedoutsa_0 ; "WlxLoggedOutSAS"
call    sub_10001000
push    64h ; 'd'       ; unsigned int
mov     edi, eax
call    ??2@YAPAXI@Z    ; operator new(uint)
mov     eax, [esp+0Ch+pProfile]
mov     esi, [esp+0Ch+pNprNotifyInfo]
mov     ecx, [esp+0Ch+phToken]
mov     edx, [esp+0Ch+pdwOptions]
add     esp, 4
push    eax
mov     eax, [esp+0Ch+pLogonSid]
push    esi
```

Hình trên cho thấy dll độc hại ghi các giá trị bị đánh cắp vào tập tin c: \ windows \ system32 \ msutil32.sys.



1. Mã độc nào lây nhiễm vào ổ đĩa nào? Ổ C:\
2. Làm thế nào để mã độc đạt được sự bền bỉ?

   MSGina.dll có thể được thay thế bằng GINA DLL tùy chỉnh. Winlogon sẽ kích hoạt việc sử dụng dll độc hại và đó là cách mã độc đạt được sự bền bỉ.

3. Mã độc đánh cắp thông tin đăng nhập của người dùng như thế nào?

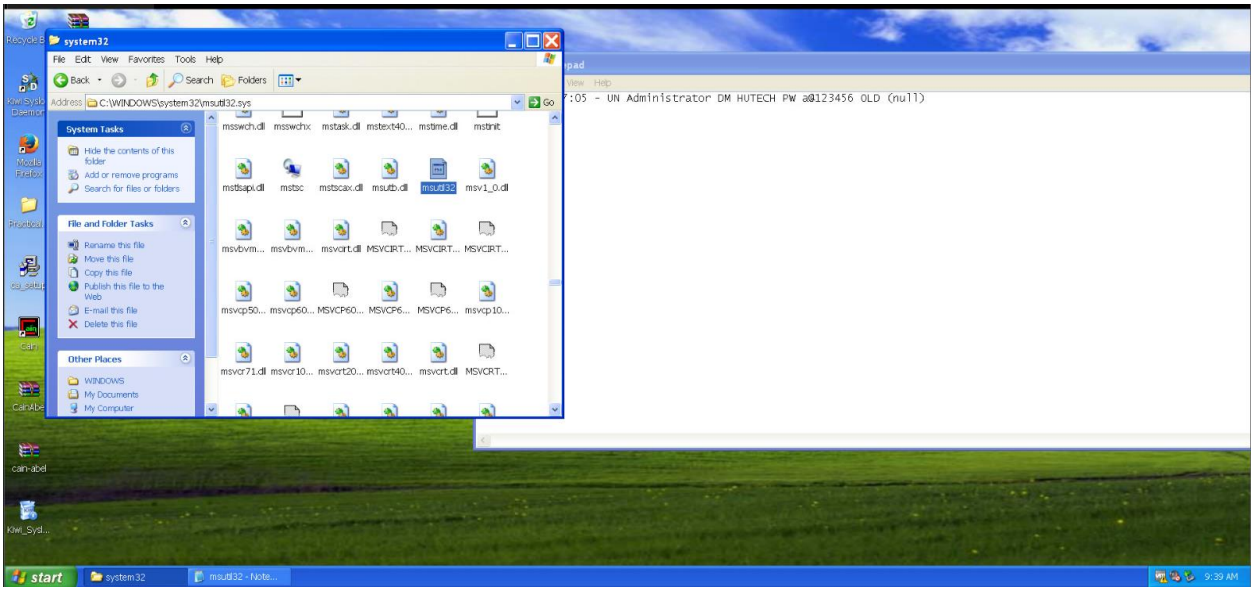
   Dll độc hại ghi lại các giá trị bị đánh cắp vào tập tin c: \ windows \ system32 \ msutil32.sys và gửi thông tin đăng nhập được ghi lại đến một máy chủ từ xa do kẻ tấn công kiểm soát.

4. Mã độc làm gì với thông tin đăng nhập bị đánh cắp?

   Kẻ tấn công có thể sử dụng thông tin đăng nhập bị đánh cắp để truy cập trái phép vào tài khoản của người dùng.

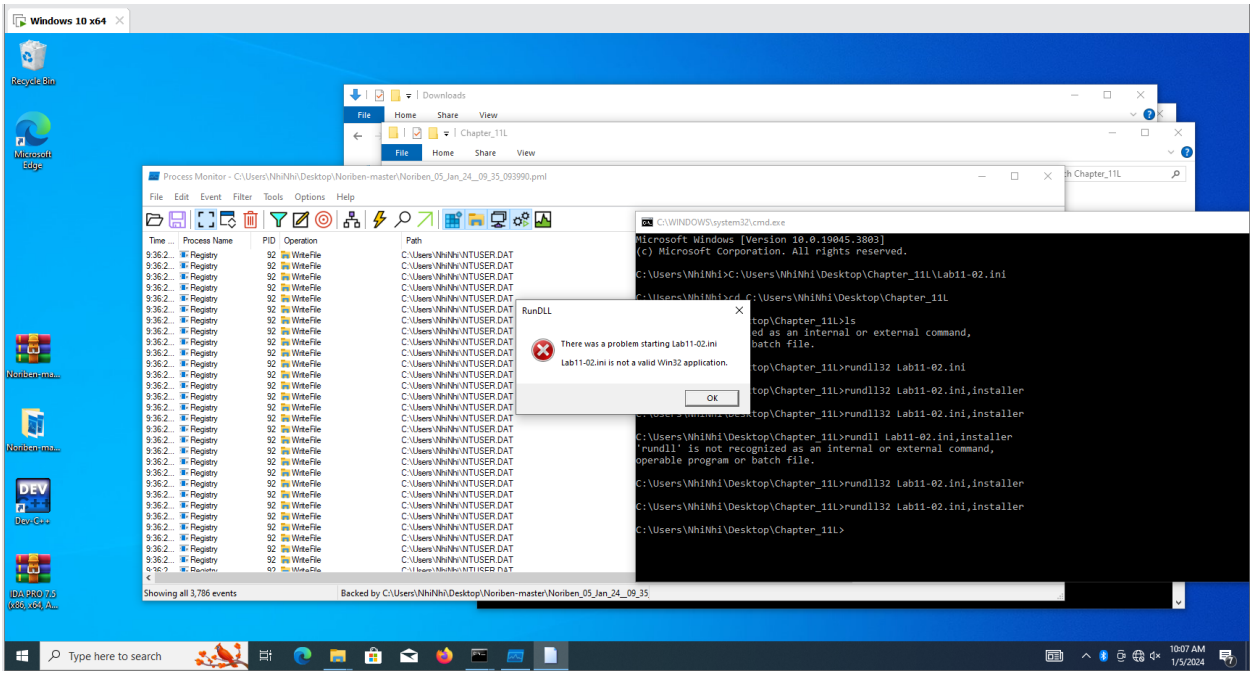
5. Làm cách nào bạn có thể sử dụng mã độc này để lấy thông tin đăng nhập của người dùng từ môi trường thử nghiệm của bạn?

   Khởi động lại máy và đăng nhập lại

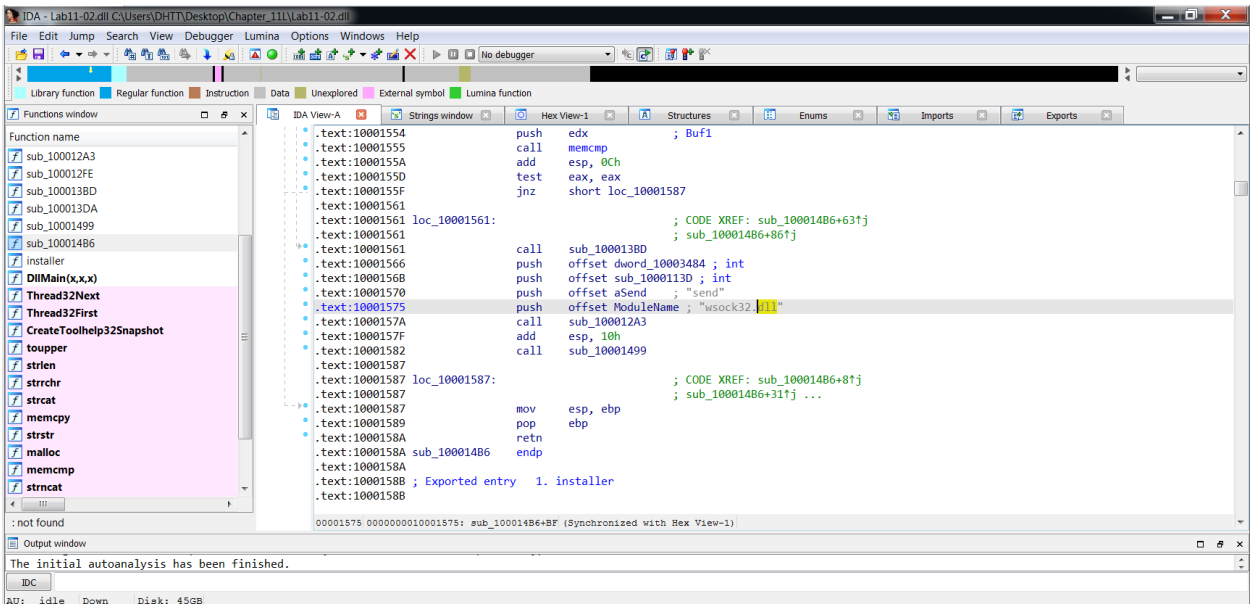


Lab 11-02:

Đoạn này em lỗi chạy hong được anh ơi

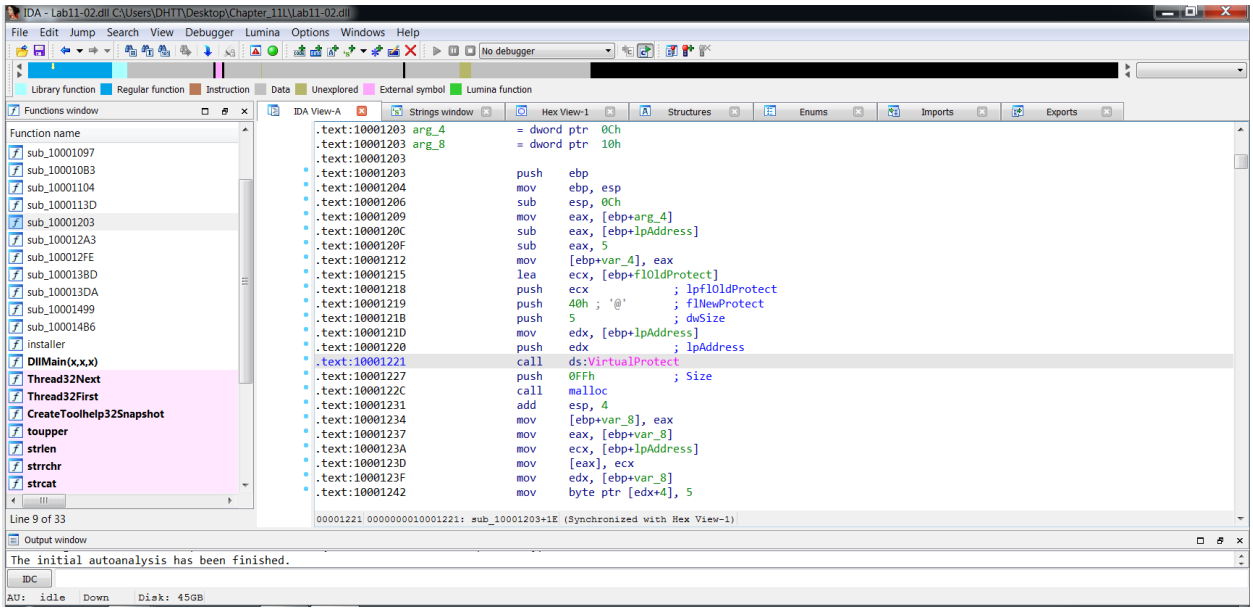


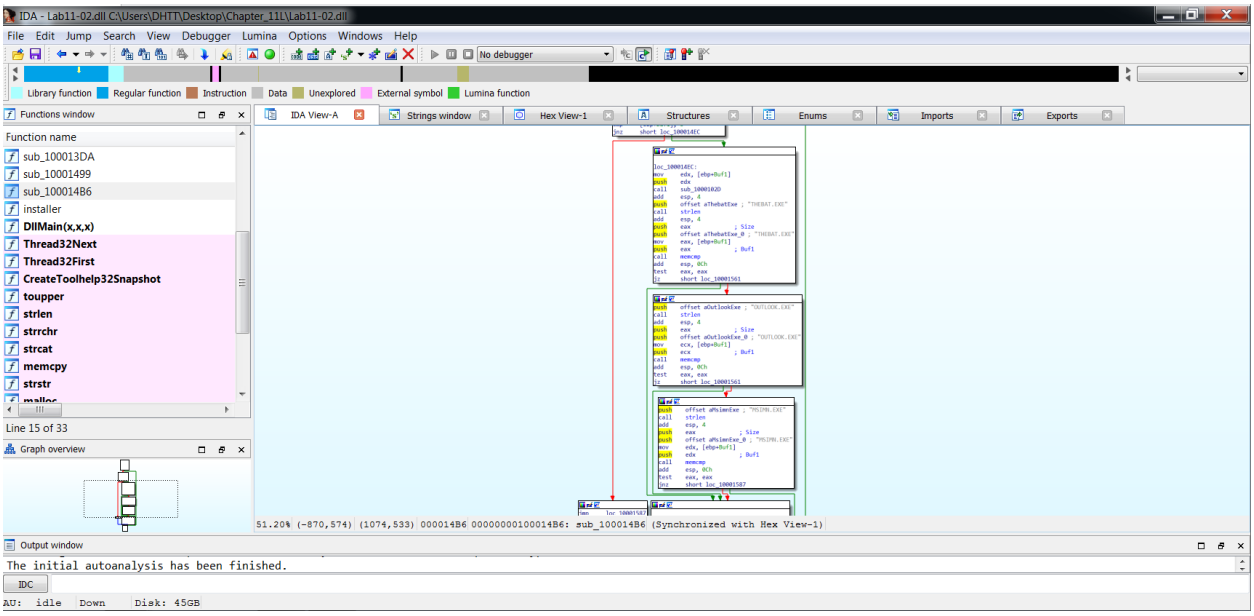
Nếu chúng ta nhìn vào chương trình con @ 0x100014B6 sẽ thấy rằng nó đang cố gắng lấy địa chỉ gửi từ wscock32.dll.



Chương trình con @ 0x10001203 đang sử dụng kỹ thuật kết nối nội tuyến. Đầu tiên, nó lấy offset từ vị trí hook đến hàm mà nó muốn nhảy tới. Sau đó, nó sử dụng VirtualProtect để tạo 5 byte không gian từ đầu địa chỉ chương trình con đến

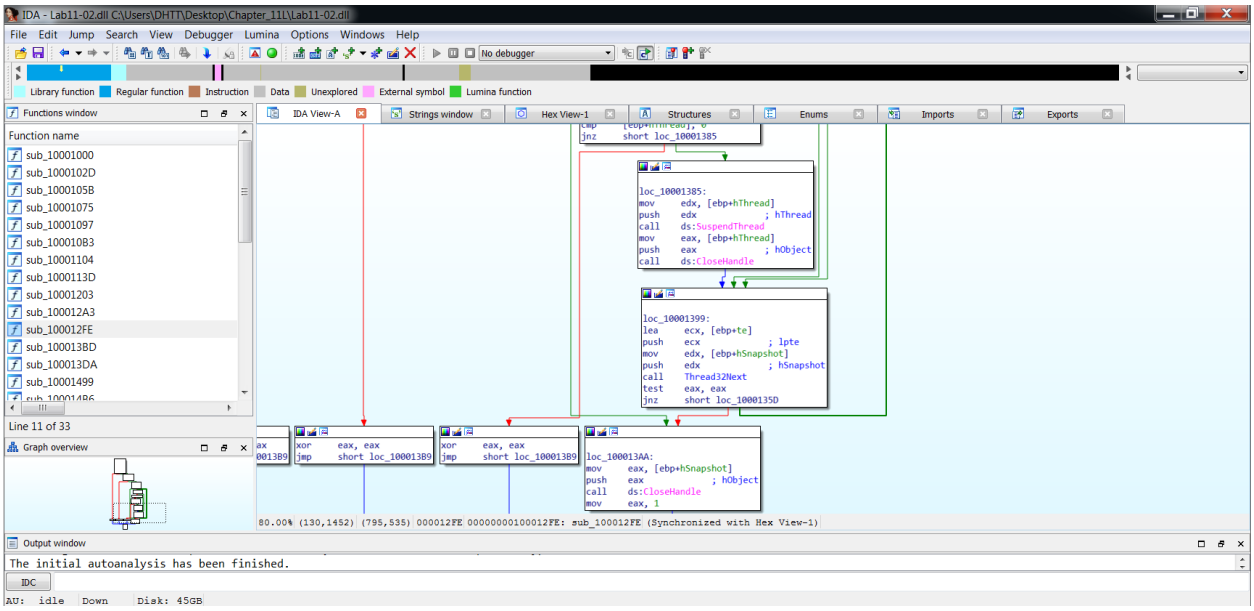
PAGE_EXECUTE_READWRITE. Khi nó được thực hiện, nó sẽ viết lại mã để jmp vào hàm hook. Cuối cùng, nó thiết lập lại 5 byte không gian bộ nhớ trở lại các thuộc tính bảo vệ cũ.



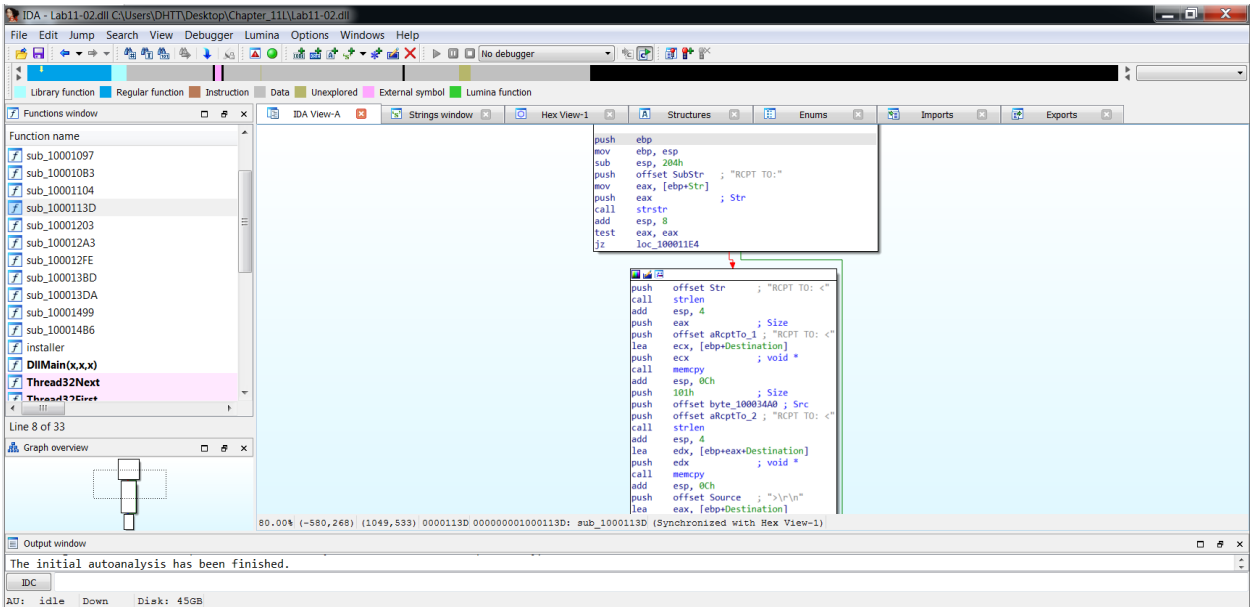


Tuy nhiên, mã độc chỉ kết nối được 3 chương trình; THEBAT.EXE, OUTLOOK.EXE, MSIMM.EXE.

Để kết luận, mã độc đang cố gắng thực hiện một kết nối nội tuyến trên chức năng gửi của wsock32.dll cho các chương trình đã chọn. Xem xét mã độc đang truy xuất những gì từ tập tin cấu hình.



Kết nối nhảy đến chức năng trên. Nó bắt đầu bằng việc kiểm tra xem bộ đệm gửi có chứa chuỗi “RCPT TO” hay không. Nếu có, nó sẽ tạo một bộ đệm mới “RCPT TO: <billy@malwareanalysisbook.com> \ r \ n ” và gửi nó đi qua chức năng gửi ban đầu. Sau đó, hàm sẽ kết thúc bằng cách chuyển tiếp dữ liệu gốc đến hàm gửi. Mã độc chỉ kết nối 3 chương trình; THEBAT.EXE, OUTLOOK.EXE, MSIMM.EXE. Đây đều là ứng dụng khách qua email, config.ini chứa địa chỉ email của kẻ tấn công được mã hóa. Nó được sử dụng để thay thế địa chỉ người nhận khiến email được gửi đến kẻ tấn công. Thiết lập inetsim và chỉ cần gửi email từ outlook express sau khi cài đặt mã độc.



1. Export cho mã độc DLL này là gì?

2. Điều gì xảy ra sau khi bạn cố gắng cài đặt mã độc này bằng cách sử dụng rundll32.exe?

Khi sử dụng rundll32.exe để thực thi mã độc DLL, hàm "DllInstall" sẽ được gọi. Hàm thực hiện các bước cài đặt mã độc vào hệ thống.

3. Lab11-02.ini phải nằm ở đâu để mã độc có thể cài đặt đúng cách?

Ở địa chỉ C:\WINDOWS\system32 ProcMon hiển thị truy cập tệp của C:\WINDOWS\system32\Lab11-02.ini. Đồng thời tập tin phải nằm cùng với tập tin mã độc DLL

4. Mã độc này được cài đặt như thế nào để tồn tại lâu dài?

DLL đặt giá trị khóa đăng ký AppInit_DLLs cho chính nó để nó được tải bằng User32.dll. Khóa đăng ký: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Windows\AppInit_DLLs: "spoolvxx32.dll" Đã khởi động lại máy ảo để các thay đổi đăng ký

AppInit_DLLs có hiệu lực. Nó tạo một dịch vụ Windows mới để đảm bảo nó được thực thi liên tục.

5. Mã độc này sử dụng kỹ thuật rootkit không gian người dùng nào?

Trên ws2_32.send(). Khi DLL độc hại được tải vào quy trình:

Tạm dừng chuỗi nếu quy trình gốc là mục tiêu.

Cài đặt hook.

Tiếp tục chuỗi.

Khởi chạy Outlook Express trong phần Immunity, được đặt cấu hình để ngắt trên mỗi lần tải DLL.

6. Mã hooking làm gì?

Hook nội tuyến trên ws2_32.send() gửi bản sao của email đến người nhận độc hại, billy@malwareanalysisbook.com. Nó được kích hoạt khi đáp ứng các điều kiện sau: Một trong những ứng dụng email khách được xác định trước được sử dụng. Lệnh RCPT TO SMTP đang được gửi qua ws2_32.send(). Móc thêm một lệnh RCPT TO bổ sung.

7. Mã độc này tấn công (các) quy trình nào và tại sao?

Các ứng dụng thư sau: thebat.exe, outlook.exe, msimn.exe

The Bat không còn nhập trực tiếp ws2_32 hoặc wsock32 nữa. Khi các điểm ngắt được đặt trên các hàm đó trong Immunity, chúng sẽ không được kích hoạt và hook không bao giờ được gọi. Mẫu này không hoạt động với phiên bản hiện tại của The Bat.

8. Ý nghĩa của tập tin .ini là gì?

Chứa địa chỉ email được mã hóa để gửi tin nhắn được sao chép tới. Mỗi lần DLL được tải, điểm vào sẽ đọc 256 byte từ tệp .ini.

9. Làm cách nào để bạn có thể nắm bắt động hoạt động của mã độc này với Wireshark?

Cài đặt phần mềm độc hại.

Thiết lập phiên bản REMNUX chạy inetsim và wireshark.

Sử dụng ứng dụng khách Outlook Express, msimn.exe để gửi email.

Lab 11-03

1. Bạn có thể khám phá những dẫn phân tích quan tâm nào bằng cách sử dụng phân tích tĩnh cơ bản?

EXE khởi động một ứng dụng.

String: net start cisvc

DLL nhập keylogger thăm dò và một chuỗi gợi ý.

Import: GetForegroundWindow

Import: GetAsyncKeyState

String: <SHIFT>

Các tệp cần chú ý

String: C:\WINDOWS\System32\inet_epar32.dll

String: C:\WINDOWS\System32\kernel64x.dll

String: Lab1103dll.dll

2. Điều gì xảy ra khi bạn chạy mã độc này?

Tập tin sao chép DLL vào C:\WINDOWS\System32\inet_epar32.dll

3. Làm thế nào để Lab11-03.exe cài đặt liên tục Lab11-03.dll?

EXE tấn công tệp nhị phân C:\Windows\System32\cisvc.exe, tệp này thực thi khi. Ứng dụng lập chỉ mục nội dung khởi động.

4. Mã độc đã lây nhiễm mã độc vào tập tin hệ thống Windows nào?

5. Lab11-03.dll làm gì?

Tạo một chuỗi chạy keylogger thăm dò ý kiến. Tiêu đề windows và tổ hợp phím ở dạng hex được lưu vào C:\WINDOWS\System32\kernel64x.dll. Sleep trong 10ms giữa các cuộc thăm dò.

6. Mã độc lưu trữ dữ liệu mà nó thu thập được ở đâu?

Tập tin C:\WINDOWS\System32\kernel64x.dll.