**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**

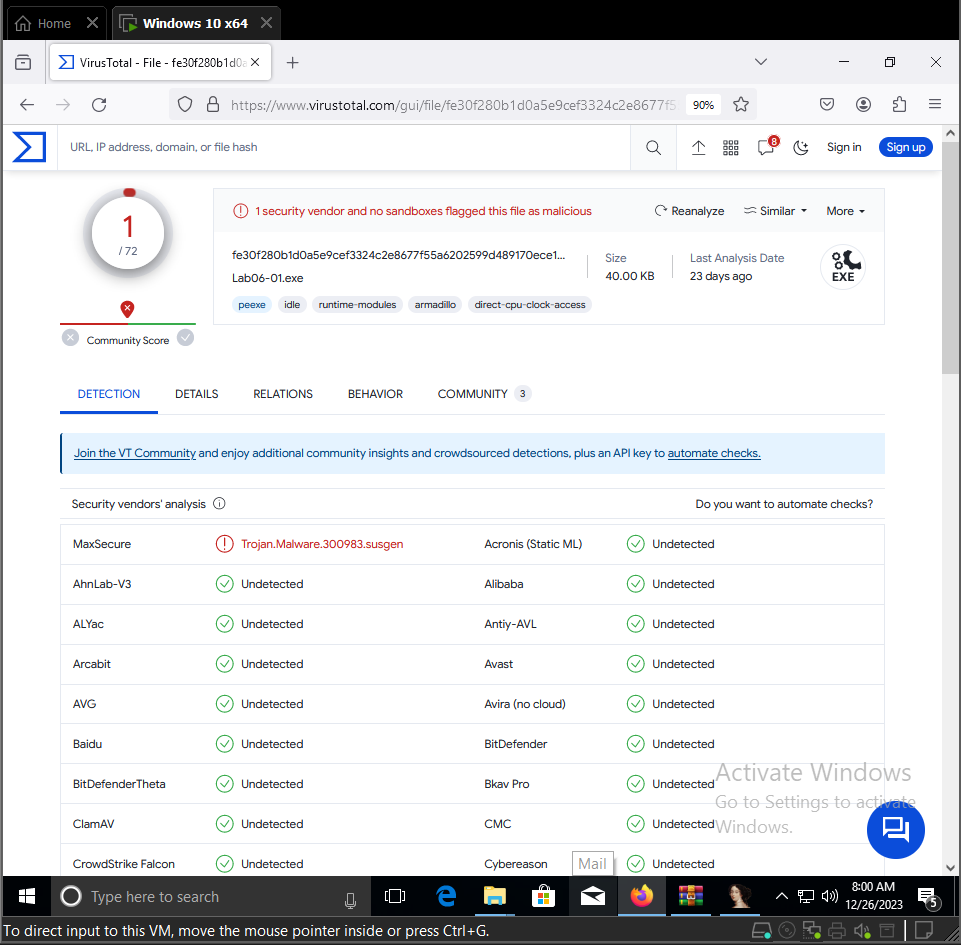
**MSSV: 2011770131**

**Lớp: 20DATA1**

**Báo cáo tuần 5**

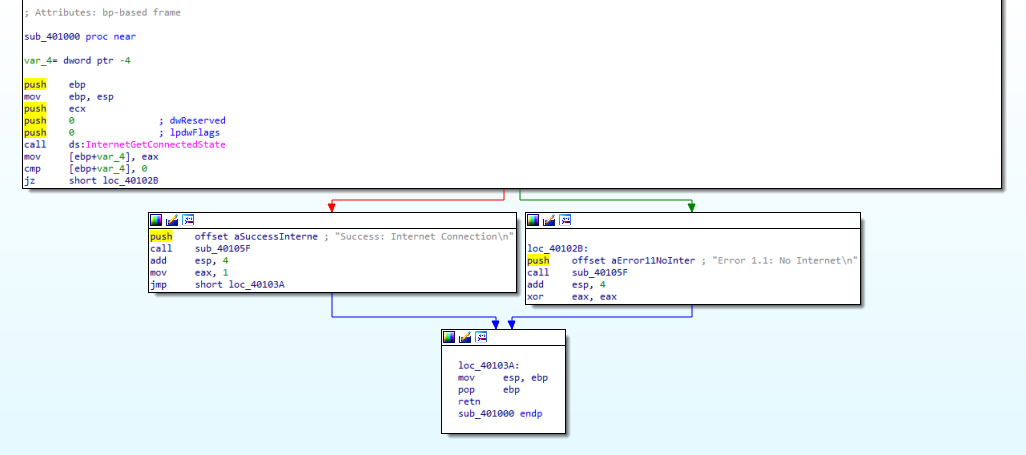
**Lab 6-01**

Dùng VirusTotal để kiểm tra tỉ lệ phát hiện của mẫu này và VT trả về kết quả là 1/72.



Dưới đây là đồ thị luồng của sub\_401000. Luồng chỉ ra 2 đường dẫn và đường dẫn sẽ được chọn dựa trên kết quả từ chức năng InternetGetConnectedState. Hàm trả về TRUE nếu có kết nối Internet hoặc FALSE nếu không có kết nối Internet.

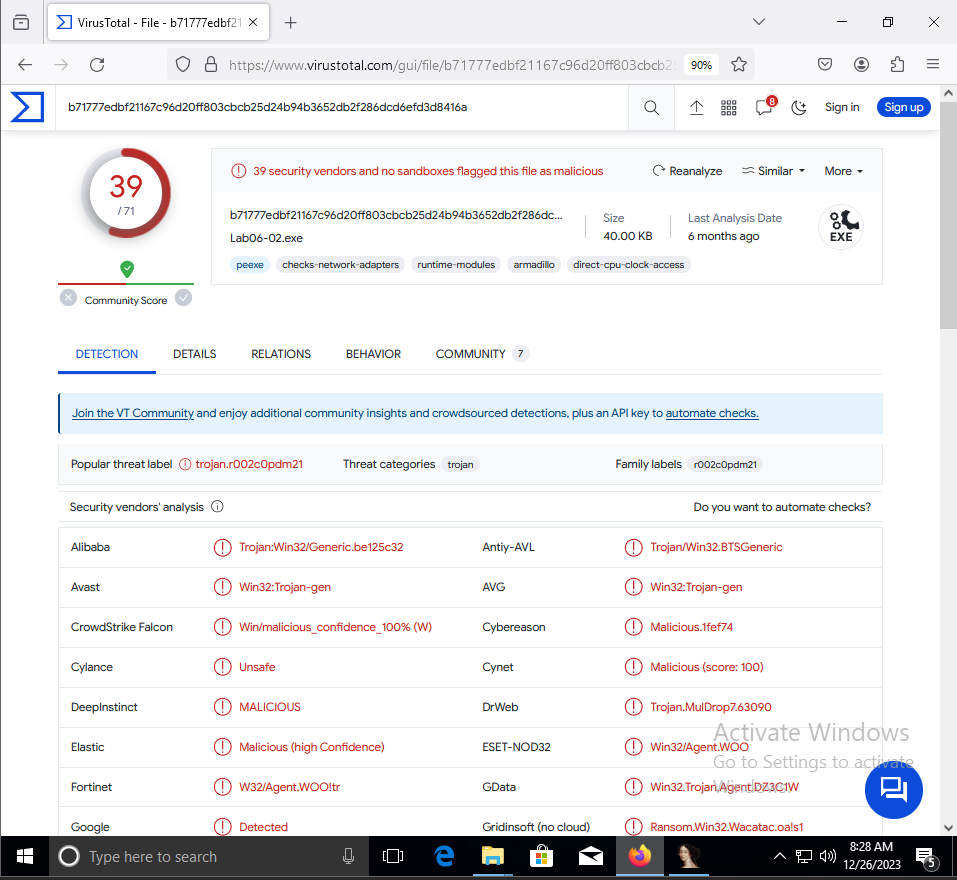
Nếu hàm trả về TRUE, chuỗi “Success: Internet Connection\n” được đẩy vào @0x40105F hoặc ngược lại nếu hàm trả về FALSE, chuỗi “Error 1.1: No internet\n” sẽ được đẩy vào hàm @0x40105F.



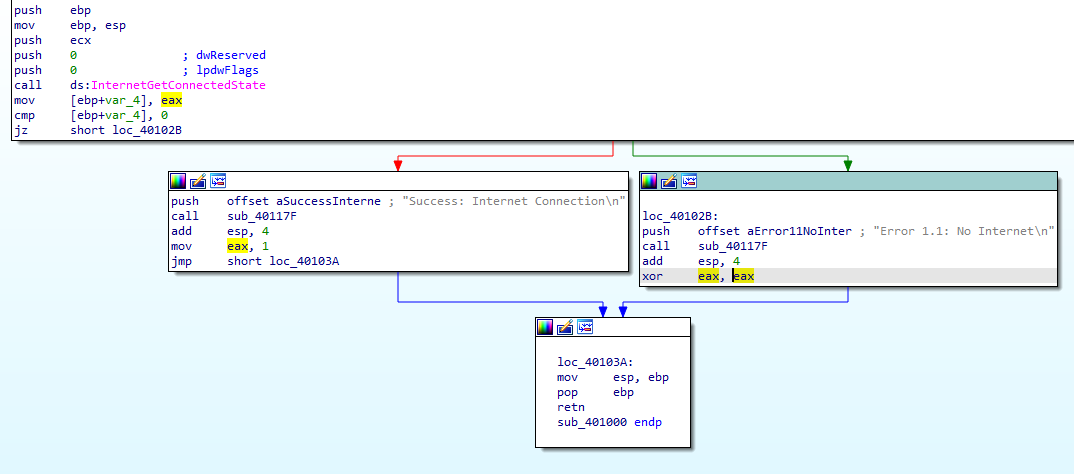
Mục đích của chương trình là để kiểm tra kết nối internet và đưa ra thông báo.

**Lab 6-02**

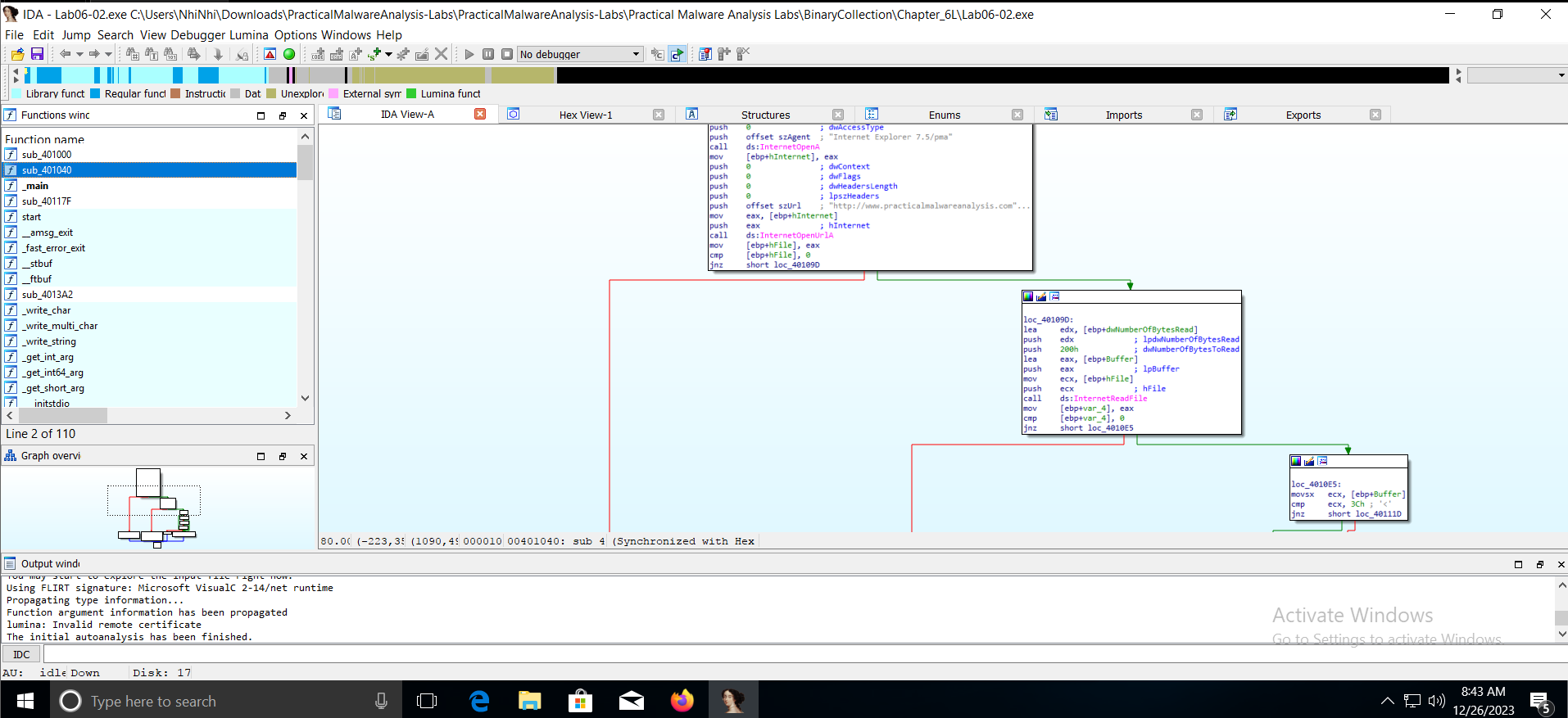
Đưa mẫu lên Virus Total để kiểm tra, tỉ lệ phát hiện của tập tin là 39/71. Được phân tích vào tháng 6 năm 2023.



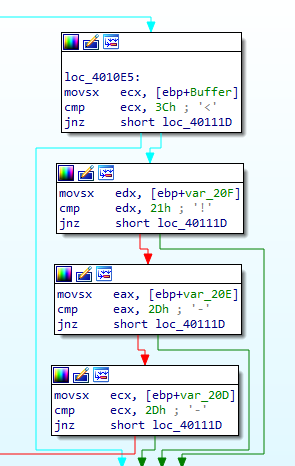
Chương trình con đầu tiên có địa chỉ 0x0401000. Kiếm tra kết nối internet nếu có trả về eax 1 và trả về 0 nếu không có kết nối.

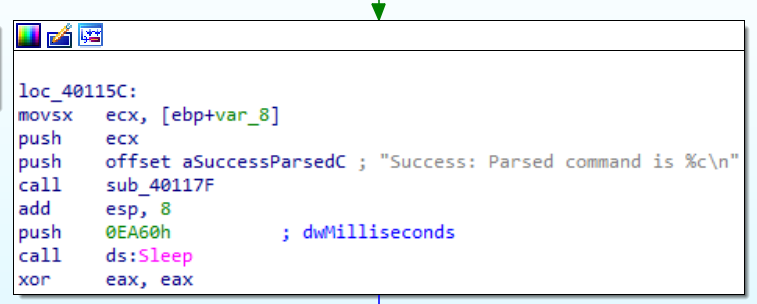


Nếu chương trình con trên trả về 1, chương trình con thứ 2 sẽ được gọi



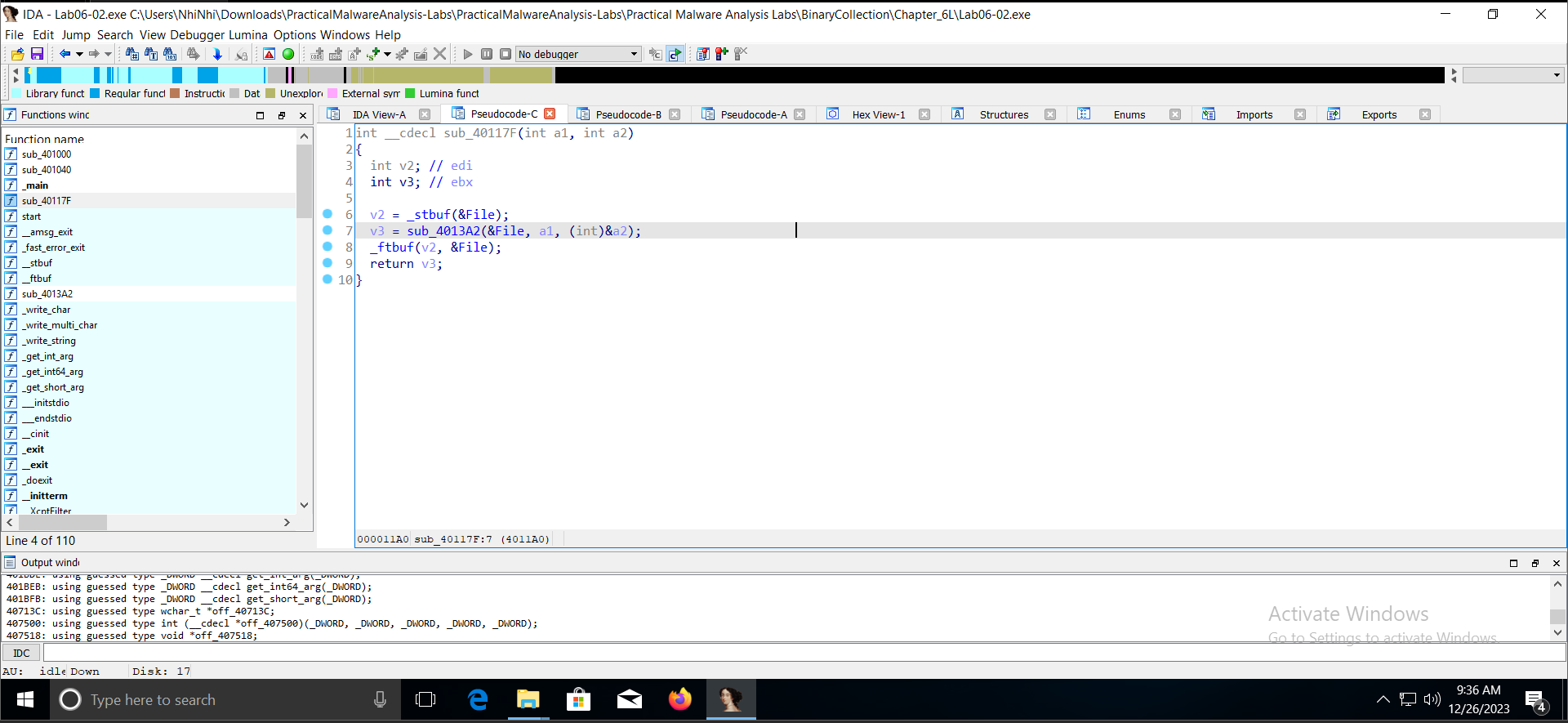
InternetOpenURLA gọi qua “'http://www.practicalmalwareanalysis.com/cc.htm'”. Tập tin từ URL được đọc và kiểm tra ký tự, nếu khớp với 4 ký tự đầu tiên “< , !, -, -”. Nếu có sẽ tiếp tục thực hiện hàm tiếp theo là lệnh, nếu không sẽ in ra thông báo “Error 2.3: Fail to get command\n”.

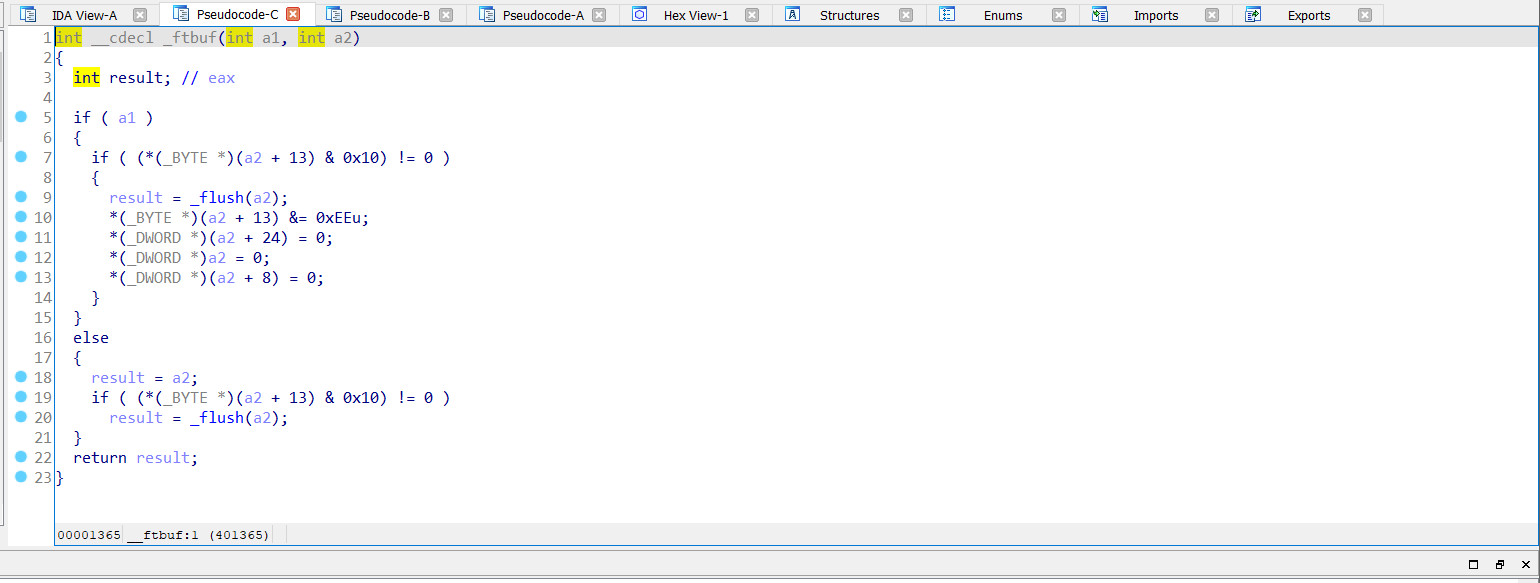
  
Sau khi phân tích cú pháp trang đã tải xuống và kiểm tra các ký tự đầu, các ký tự tiếp theo sẽ được phân tích cú pháp dưới dạng lệnh. Nếu thành công nó sẽ sleep và kết thúc

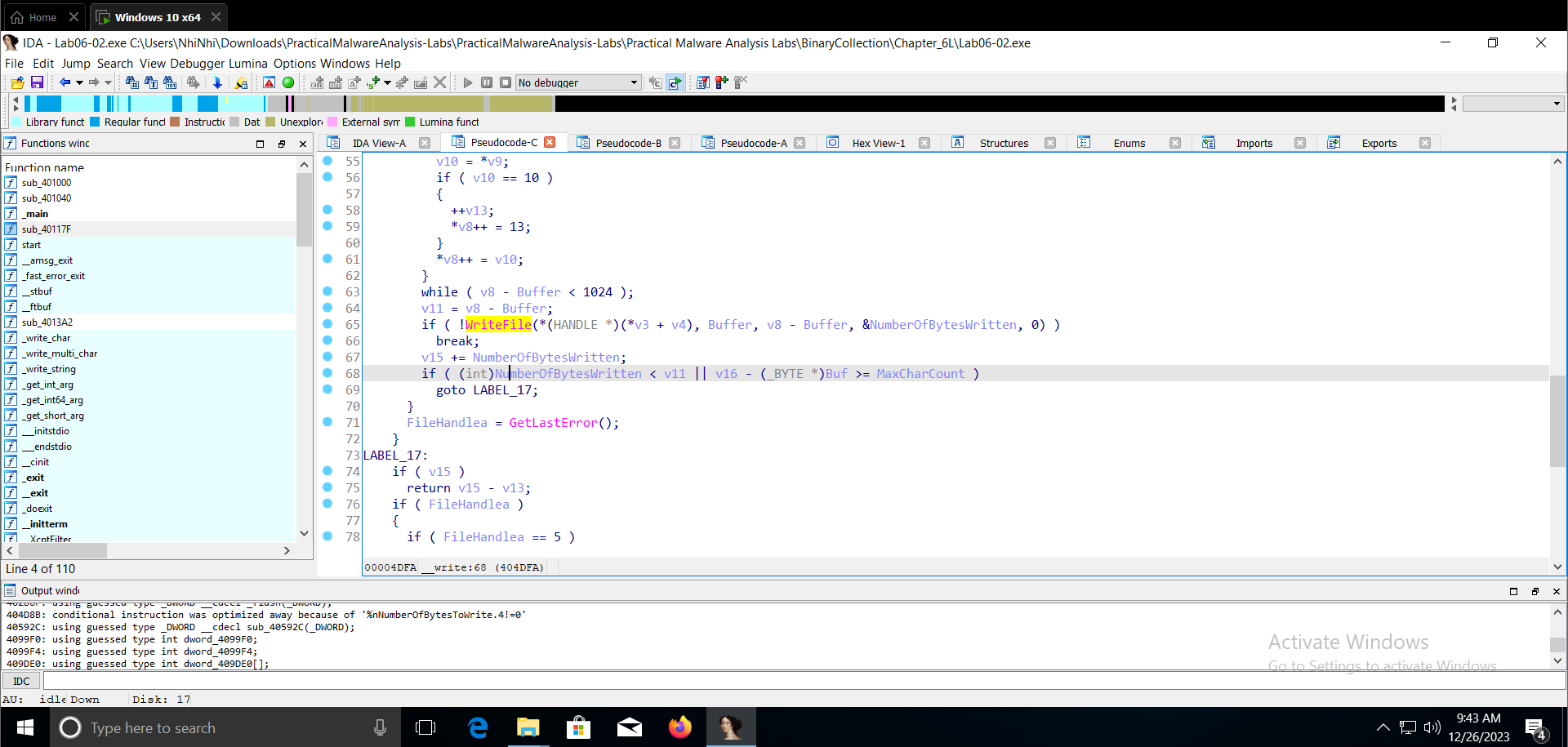


Chương trình con đầu tiên được gọi bởi main thực hiện kiểm tra internet và in thông báo về kết nối

Sub\_0x40117F gọi \_stbuf và \_ftbuf. Sub\_4013A2 liên quan đến hoạt động độc/ ghi file và gán kết quả vào v3. Kiểm tra các hàm \_ftbuf, flush, \_write, ta thấy chương trình gọi hàm WriteFile. Có thể suy ra được hàm con 0x40117F thực thi một loạt các thao tác kiểm tra để thực hiện hành vi ghi dữ liệu ra file.







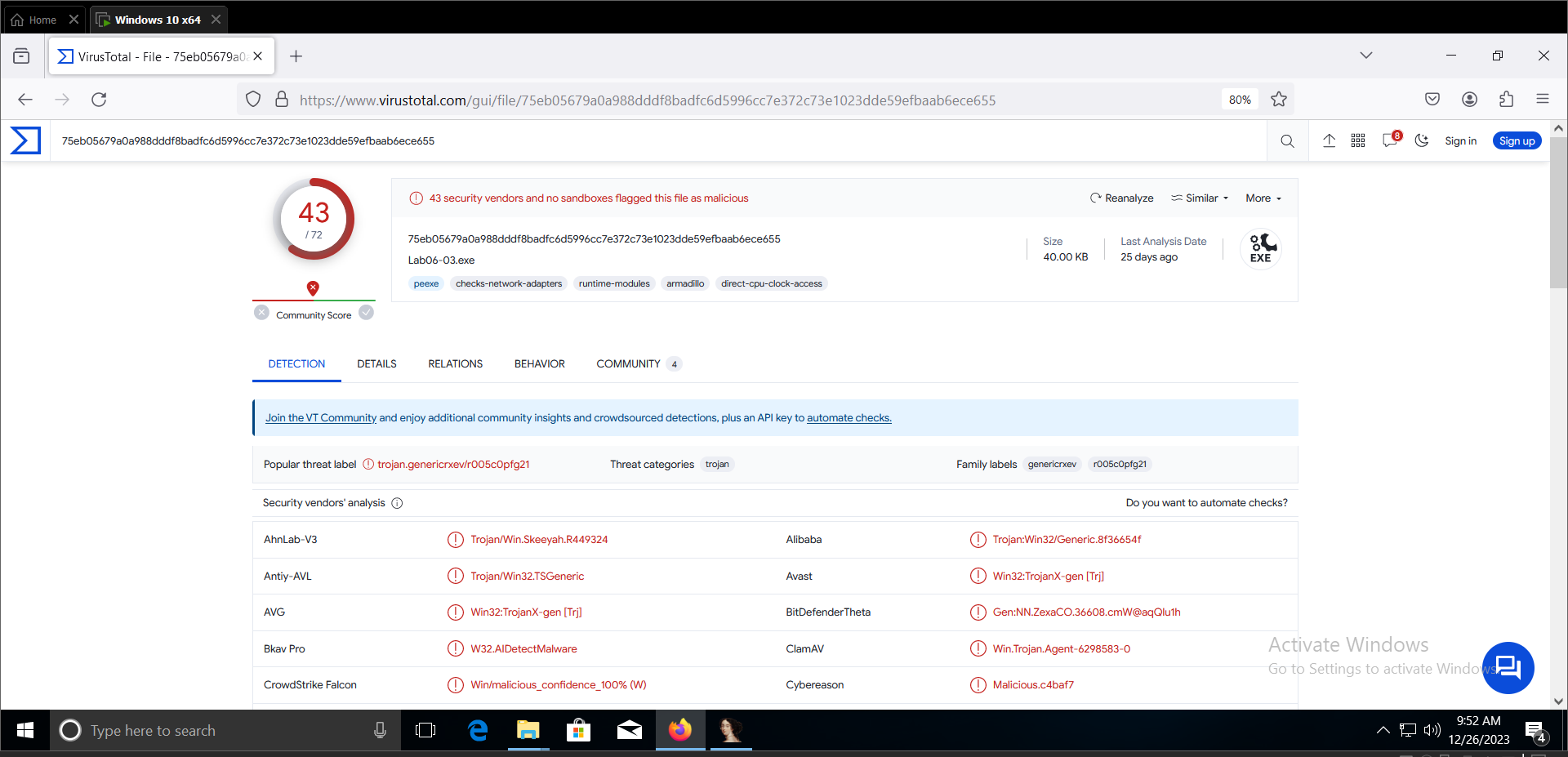
Chương trình con thứ hai được gọi bởi main đọc và kiểm tra kí tự đầu tiên của chuỗi URL nếu khớp sẽ thực hiện lệnh và ngược lại sẽ kết thúc. Sau khi kiểm tra trùng khớp, hàm phân tích cú pháp các ký tự tiếp theo dưới dạng lệnh, nếu thành công nó sẽ sleep và và kết thúc.

Loại cấu trúc mã được sử dụng trong chương trình con này là lệnh if

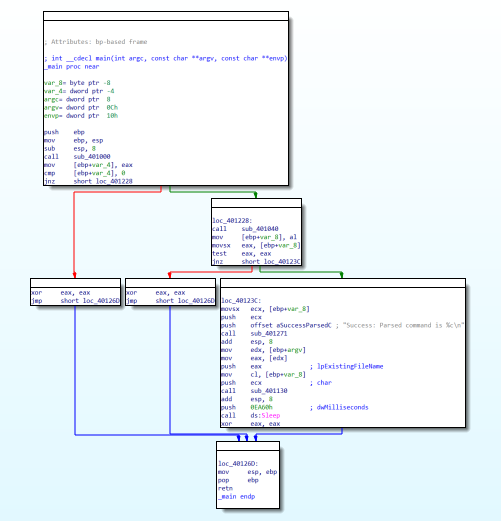
Mục đích của mã độc này là chương trình kết nối tới địa chỉ <http://www.practicalmalwareanalysis.com/cc.htm>, sử dụng Agent là Internet Explorer 7.5/pma, kiểm tra kết nối và lấy HTML comment trong đoạn đầu file cc.htm sau đó in nội ký tự đầu tiên trong HTML comment nhận được ra màn hình. Sau khi hoàn tất thực thi, chương trình sẽ Sleep

**Lab 6-03**

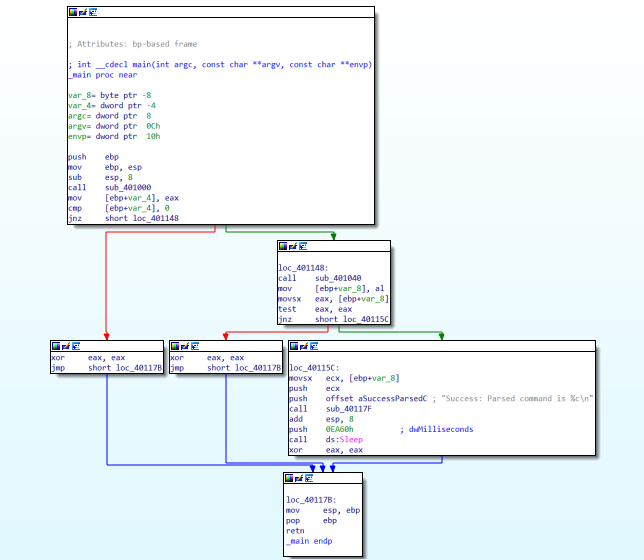
Dùng VirusTotal để kiểm tra tỉ lệ phát hiện của mẫu này và VT trả về kết quả là 43/72. Được phân tích vào 25 ngày trước

****

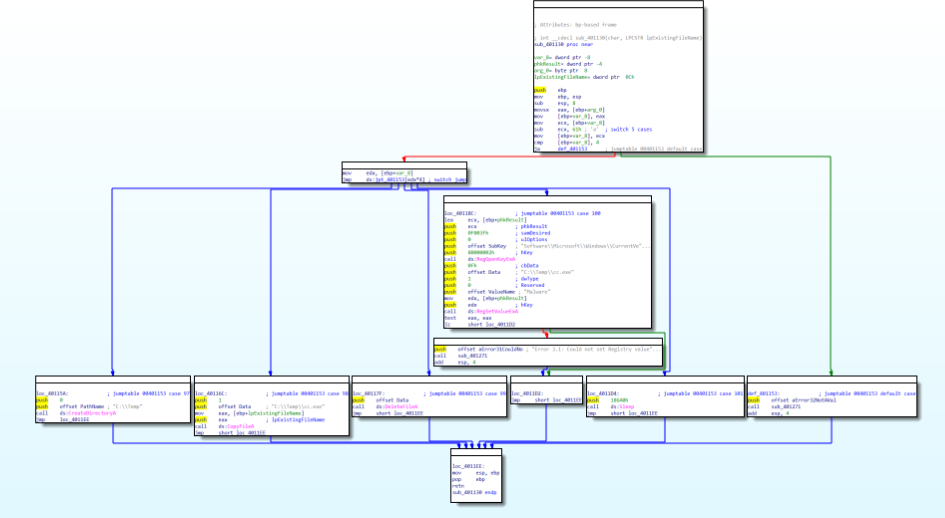
Cấu trúc luồng lab 6-03



Cấu trúc luồng lab6-02



Các câu lệnh trong lab 6-03 giống như bài 2 nhưng có một hàm gọi bổ sung tới sub\_401130.

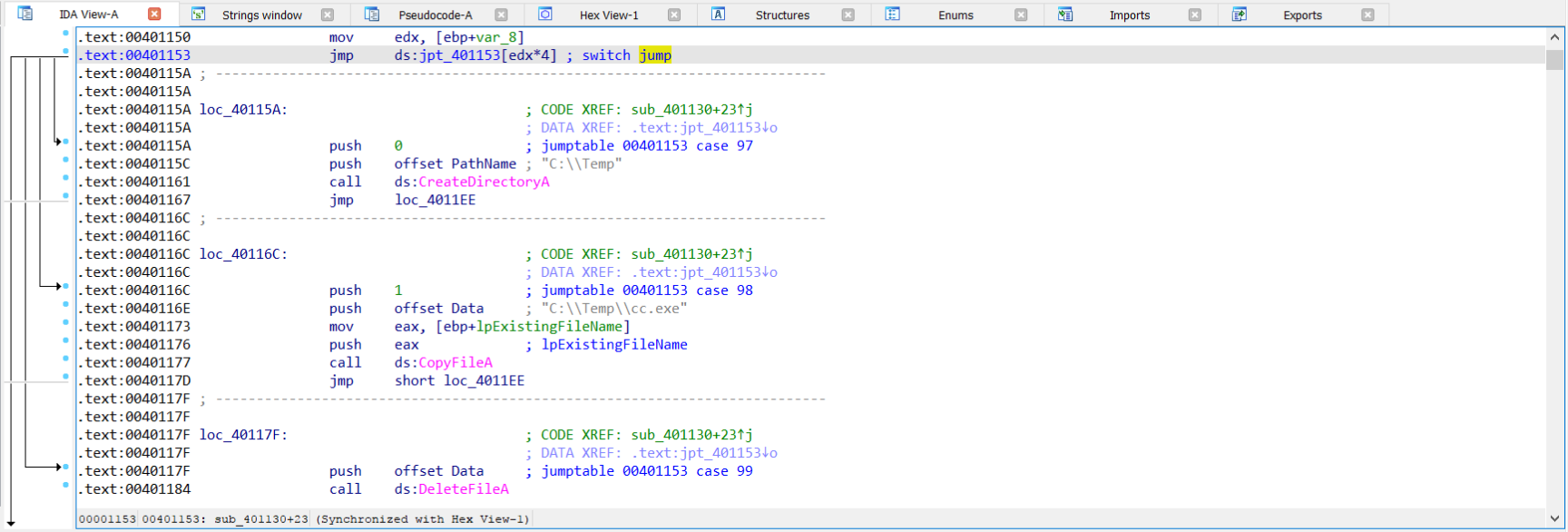


Cấu trúc mã chính là bảng chuyển đổi thông qua bảng jump. Xem xét các câu lệnh trước khi thực hiện bước nhảy

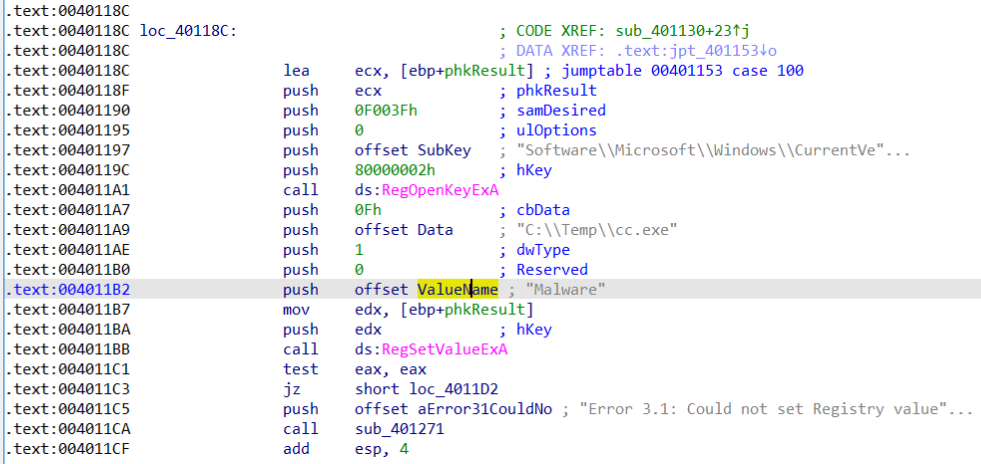
Thư mục “C:\\temp” được tạo thông qua chức năng CreateDirectoryA

Tập tin thực thi hiện tại được sao chép sáng “C:\\Temp\\cc.exe” thông qua CopyFileA

“C:\\Temp\\cc.exe” bị xoá thông qua chức năng DeleteFileA



Khoá đăng ký “Mã độc” có giá trị “C:\\Temp\\cc.exe” được thêm vào Software\\Microsoft\\Windows\\CurrentVersion\\Run thông qua chức năng RegSetValueExA, làm cho mã độc tồn tại.



Hàm mới nhận các tham số: đối số các kí tự trong url, argv - tên chương trình thực thi

Hàm chứa cấu trúc mã chính switch – case

Chức năng của cấu trúc mã chính

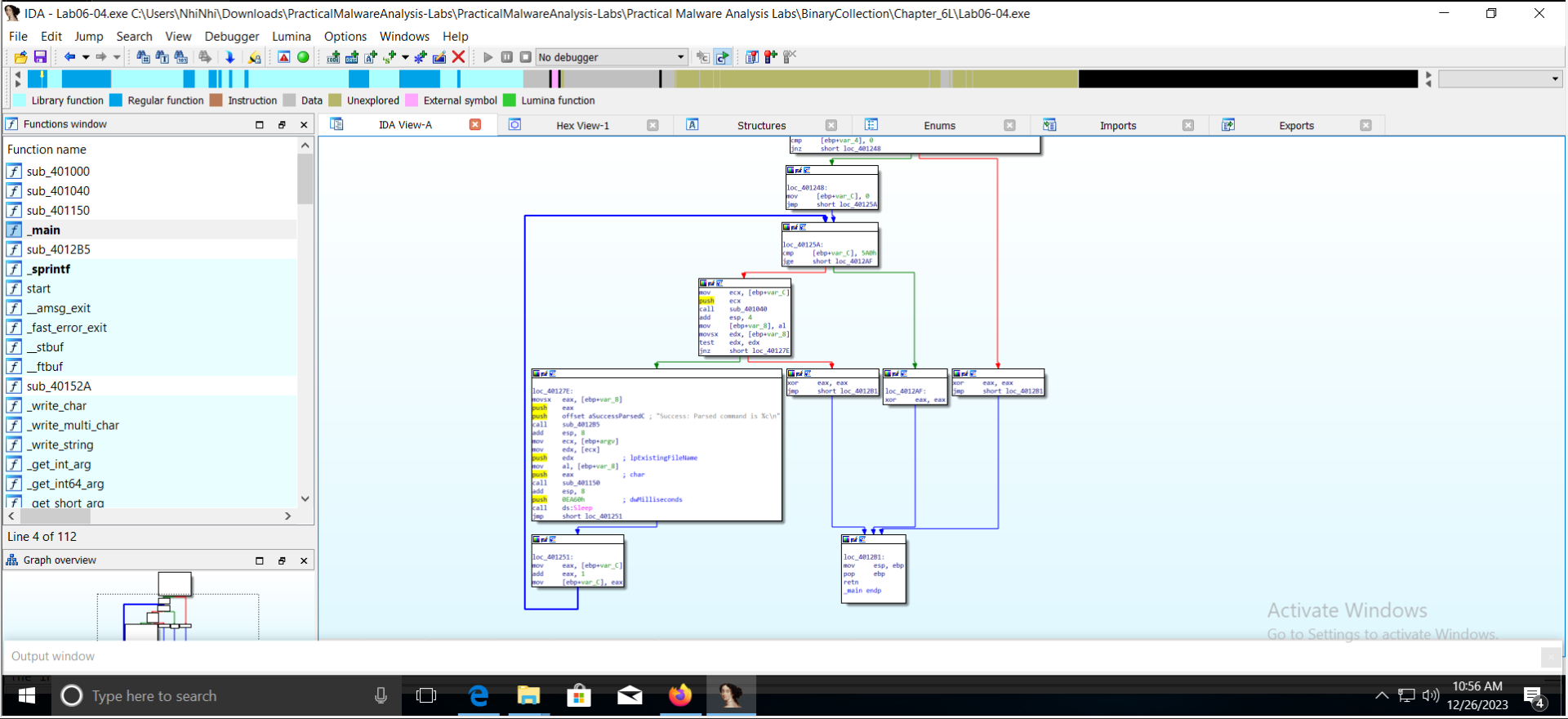
* Tạo thư mục
* Sao chép tập tin thực thi
* Xoá tập tin
* Tạo key mới “Malware” có giá trị “C:\temp\cc.exe” thêm vào Software\\Microsoft\\Windows\\CurrentVersion\\Run
* Sleep

Mục đích của mã độc:

Mã độc thực hiện kết nối tới <http://www.practicalmalwareanalysis.com/cc.htm> , sử dụng UA là “Internet Explorer 7.5/pma”, kiểm tra kết nối và kiểm tra HMTL file. Nếu thỏa mãn, mã độc thực hiện lấy ký tự đầu tiên trong HMTL comment và coi ký tự đó là điều kiện nhảy switch case, thực hiện một trong các hành vi:

* Tạo thư mục
* Sao chép tập tin thực thi
* Xoá tập tin
* Tạo key mới “Malware” có giá trị “C:\temp\cc.exe” thêm vào Software\\Microsoft\\Windows\\CurrentVersion\\Run
* Sleep

**Lab 6-04**

****