



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

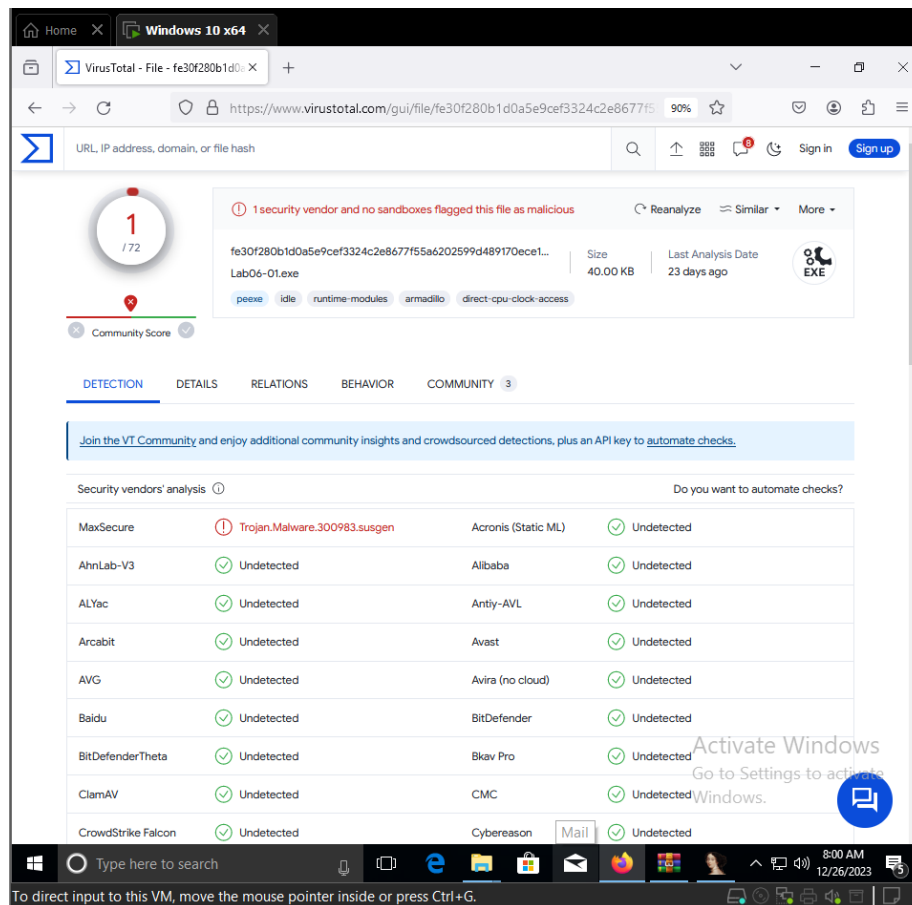
MSSV: 2011770131

Lớp: 20DATA1

Báo cáo tuần 5

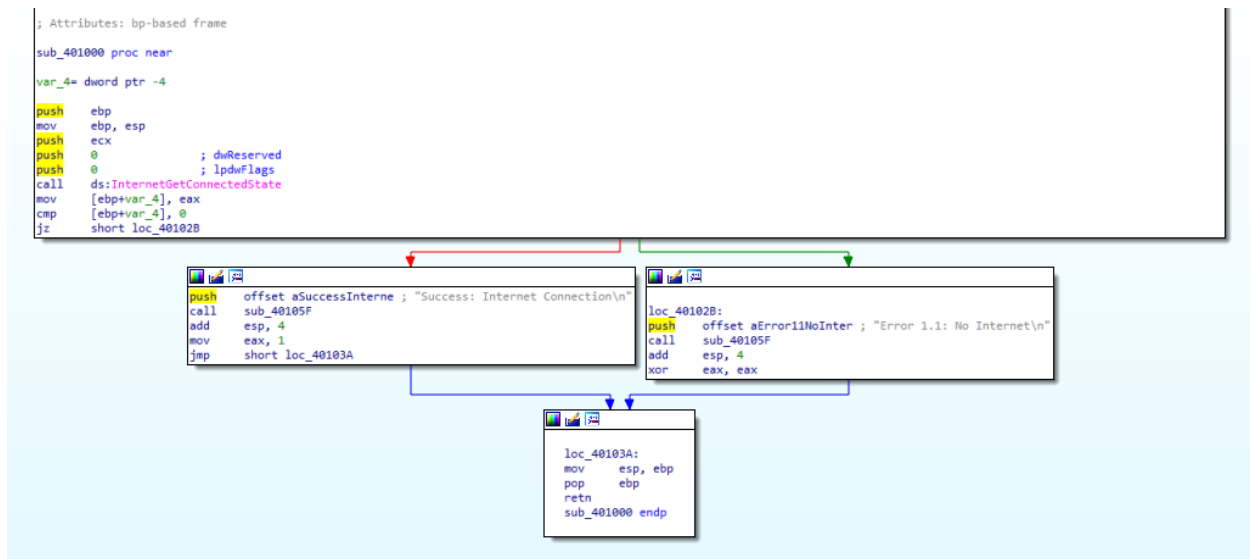
Lab 6-01

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.

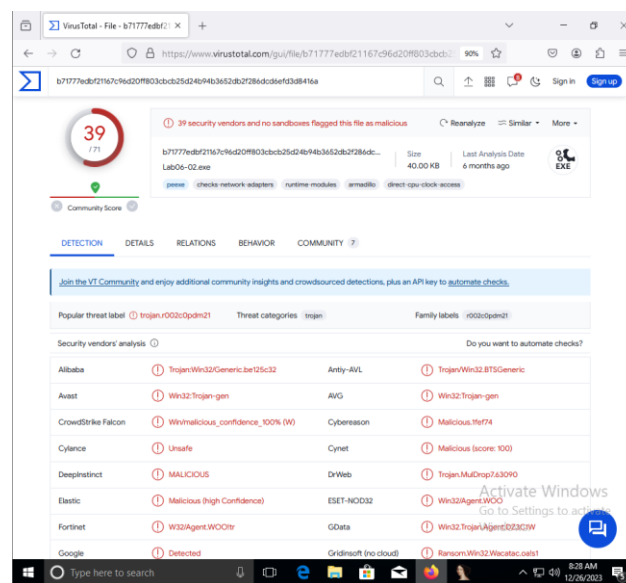
Nếu hàm trả về TRUE, chuỗi “Success: Internet Connection\n” được đẩy vào @0x40105F hoặc ngược lại nếu hàm trả về FALSE, chuỗi “Error 1.1: No internet\n” sẽ được đẩy vào hàm @0x40105F.



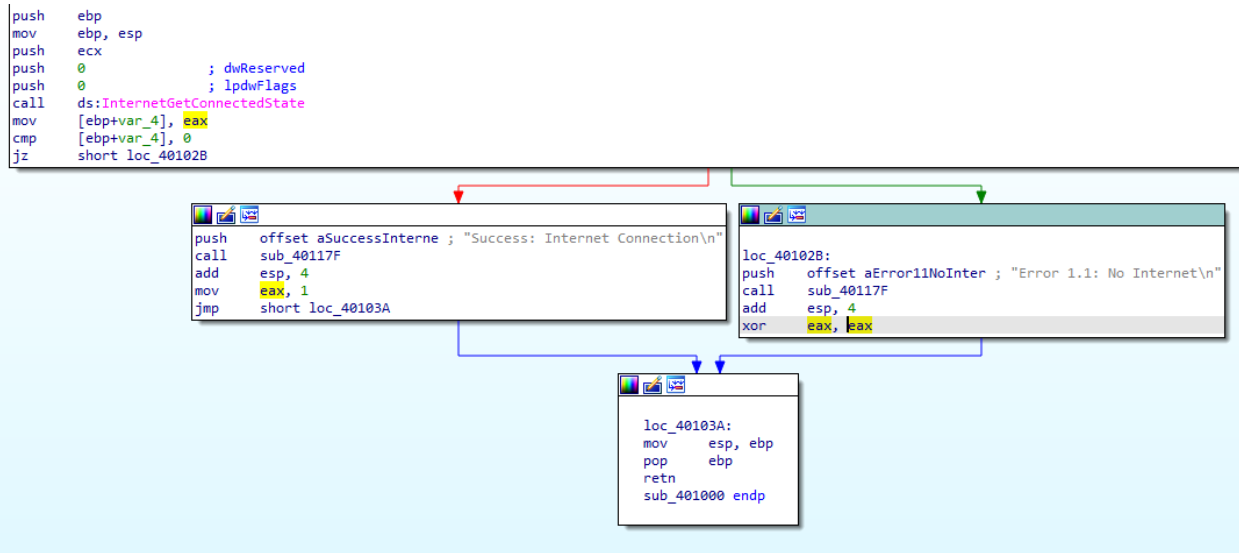
Mục đích của chương trình là để kiểm tra kết nối internet và đưa ra thông báo.

Lab 6-02

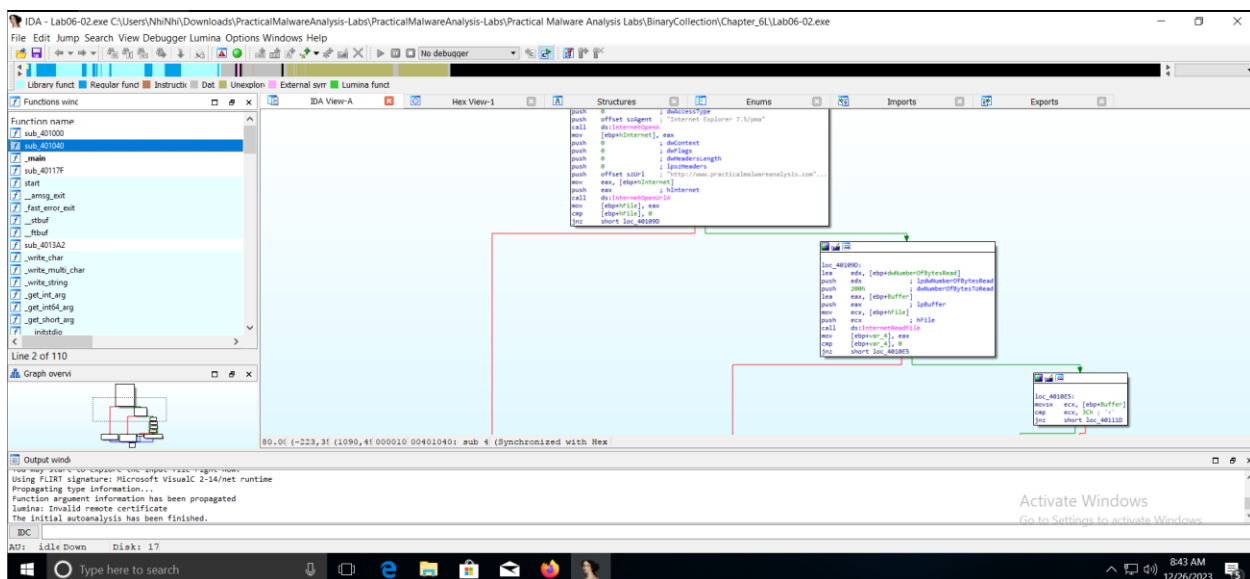
Đưa mẫu lên Virus Total để kiểm tra, tỉ lệ phát hiện của tập tin là 39/71. Được phân tích vào tháng 6 năm 2023.



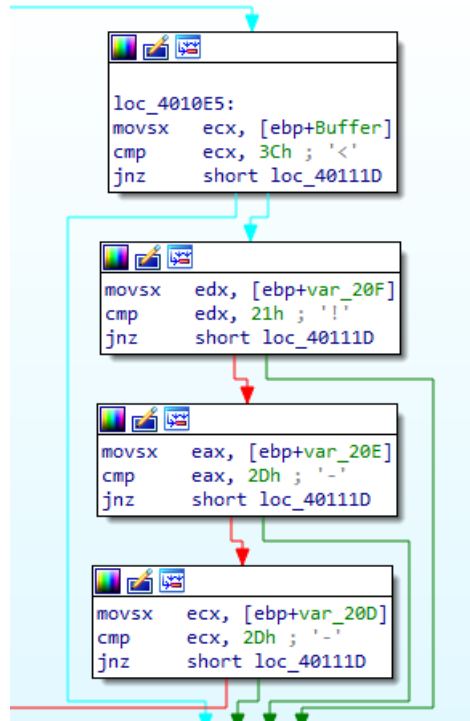
Chương trình con đầu tiên có địa chỉ 0x0401000. Kiểm tra kết nối internet nếu có trả về eax 1 và trả về 0 nếu không có kết nối.



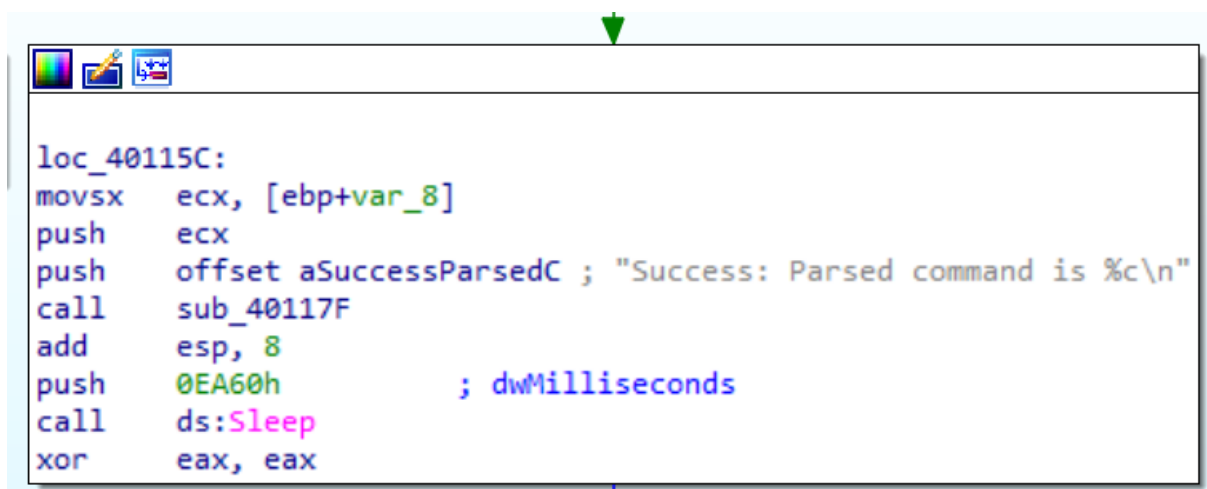
Nếu chương trình con trên trả về 1, chương trình con thứ 2 sẽ được gọi



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”.

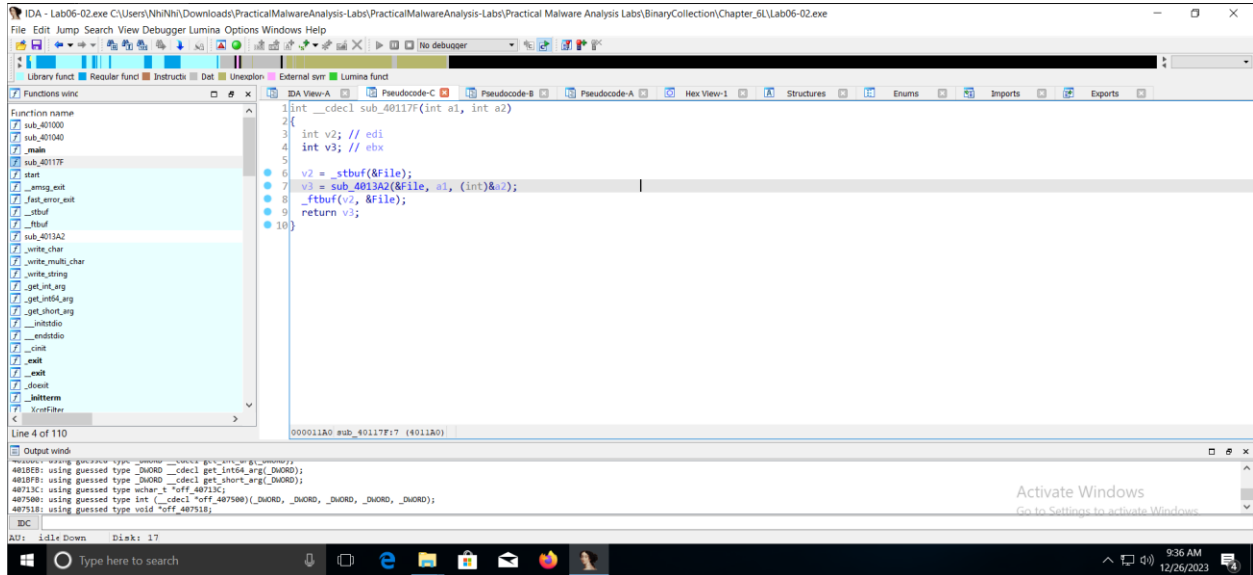


Sau khi phân tích cú pháp trang đã tải xuống và kiểm tra các ký tự đầu, các ký tự tiếp theo sẽ được phân tích cú pháp dưới dạng lệnh. Nếu thành công nó sẽ sleep và kết thúc



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 đọc/ 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.



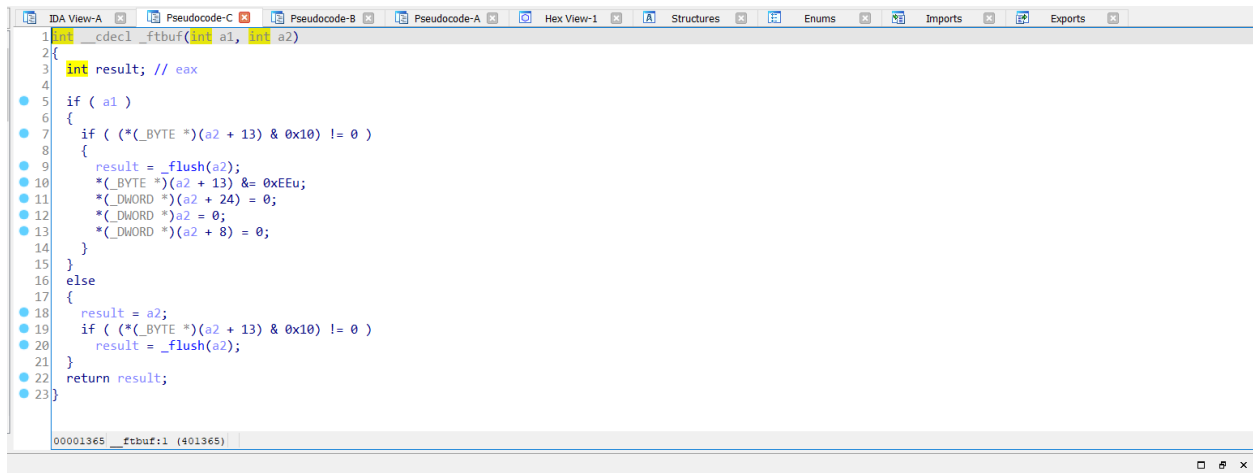
```
int __cdecl sub_40117F(int a1, int a2)
{
    int v2; // edi
    int v3; // ebx
    v2 = _stbuf(&file);
    v3 = sub_4013A2(&file, a1, (int)&a2);
    _ftbuf(v2, &file);
    return v3;
}
```

Line 4 of 110

000011A0: sub_40117F+7 (4011A0)

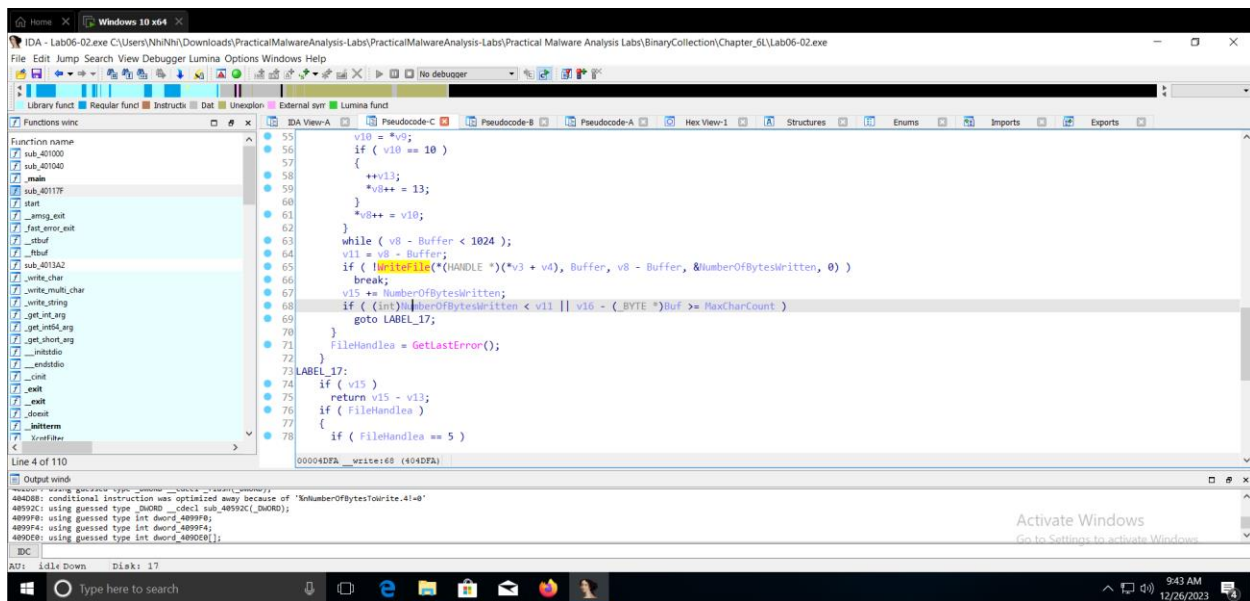
Output window:

```
4010B8: using guessed type _DWORD __cdecl get_int6_arg(_DWORD);
4010B8: using guessed type _DWORD __cdecl get_short_arg(_DWORD);
40113C: using guessed type uchar_t __off_40713C;
407500: using guessed type int (__cdecl __off_407500)(_DWORD, _DWORD, _DWORD, _DWORD, _DWORD);
407518: using guessed type void __off_407518;
```



```
int __cdecl _ftbuf(int a1, int a2)
{
    int result; // eax
    if ( a1 )
    {
        if ( (*(_BYTE *) (a2 + 13) & 0x10) != 0 )
        {
            result = _flush(a2);
            *(_BYTE *) (a2 + 13) &= 0xEEu;
            *(_DWORD *) (a2 + 24) = 0;
            *(_DWORD *) a2 = 0;
            *(_DWORD *) (a2 + 8) = 0;
        }
        else
        {
            result = a2;
            if ( (*(_BYTE *) (a2 + 13) & 0x10) != 0 )
            {
                result = _flush(a2);
            }
            return result;
        }
    }
}
```

00001365: _ftbuf+1 (401365)



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 kết thúc.

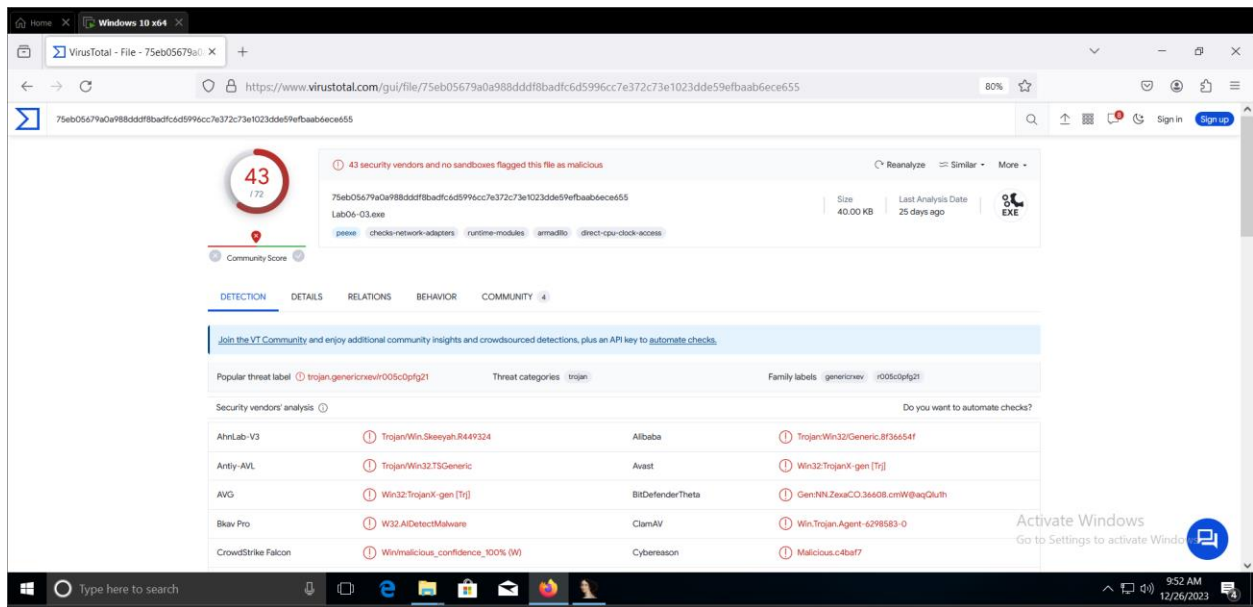
Loại cấu trúc mã được sử dụng trong chương trình con này là lệnh if

Mục đích của mã độc này là chương trình kết nối tới địa

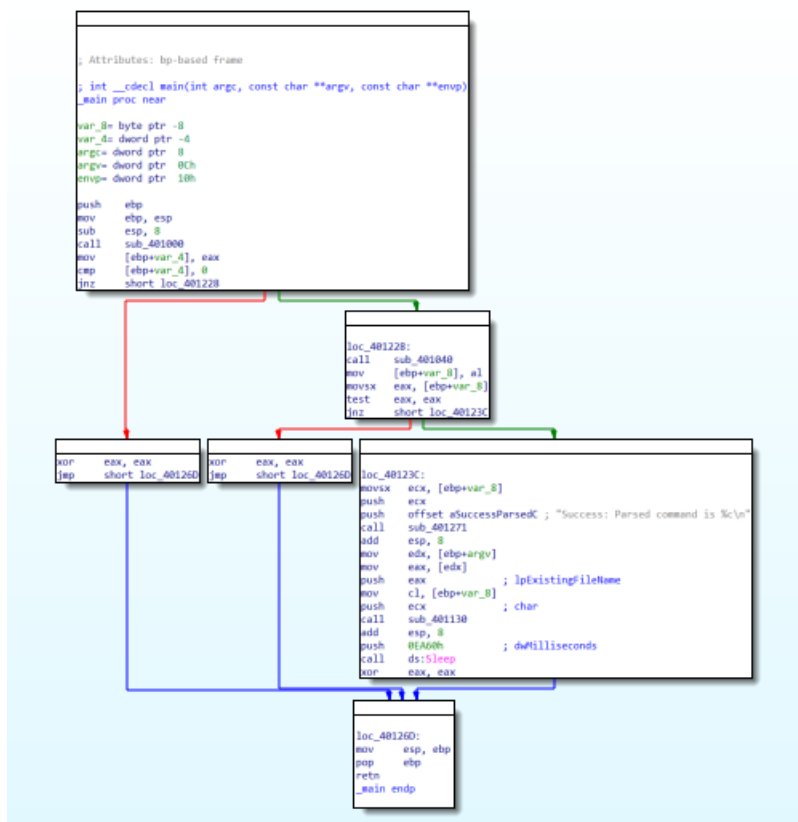
chỉ <http://www.practicalmalwareanalysis.com/cc.htm>, sử dụng Agent là Internet Explorer 7.5/pma, kiểm tra kết nối và lấy HTML comment trong đoạn đầu file cc.htm sau đó in nội ký tự đầu tiên trong HTML comment nhận được ra màn hình. Sau khi hoàn tất thực thi, chương trình sẽ Sleep

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

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 sang “C:\\Temp\\cc.exe” thông qua CopyFileA

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

```
.text:00401150 mov     edx, [ebp+var_8]
.text:00401153 jmp     ds:jpt_401153[edx*4] ; switch jump
;-----
.text:0040115A ;
.text:0040115A loc_40115A: ; CODE XREF: sub_401130+231j
.text:0040115A ; DATA XREF: .text:jpt_4011534o
; jump table 00401153 case 97
.text:0040115A push     0 ; offset PathName ; "C:\\Temp"
.text:0040115C call     ds:CreateDirectoryA
.text:00401161 jmp     loc_4011EE
;-----
.text:0040116C ;
.text:0040116C loc_40116C: ; CODE XREF: sub_401130+231j
.text:0040116C ; DATA XREF: .text:jpt_4011534o
; jump table 00401153 case 98
.text:0040116C push     1 ; offset Data ; "C:\\Temp\\cc.exe"
.text:0040116E mov     eax, [ebp+lpExistingFileName]
.text:00401173 push     eax ; lpExistingFileName
.text:00401176 call     ds:CopyFileA
.text:00401177 jmp     short loc_4011EE
;-----
.text:0040117F ;
.text:0040117F loc_40117F: ; CODE XREF: sub_401130+231j
.text:0040117F ; DATA XREF: .text:jpt_4011534o
; jump table 00401153 case 99
.text:00401184 push     offset Data ; ds>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.

```

.text:0040118C
.text:0040118C loc_40118C:                                ; CODE XREF: sub_401130+23↑j
.text:0040118C                                ; DATA XREF: .text:jpt_401153↓o
.text:0040118C      lea     ecx, [ebp+phkResult] ; jumtable 00401153 case 100
.text:0040118F      push    ecx                ; phkResult
.text:00401190      push    0F003Fh           ; samDesired
.text:00401195      push    0                  ; ulOptions
.text:00401197      push    offset SubKey      ; "Software\\Microsoft\\Windows\\CurrentVe"...
.text:0040119C      push    80000002h          ; hKey
.text:004011A1      call    ds:RegOpenKeyExA
.text:004011A7      push    0Fh                ; cbData
.text:004011A9      push    offset Data         ; "C:\\Temp\\cc.exe"
.text:004011AE      push    1                   ; dwType
.text:004011B0      push    0                   ; Reserved
.text:004011B2      push    offset ValueName    ; "Malware"
.text:004011B7      mov     edx, [ebp+phkResult]
.text:004011BA      push    edx                ; hKey
.text:004011BB      call    ds:RegSetValueExA
.text:004011C1      test    eax, eax
.text:004011C3      jz      short loc_4011D2
.text:004011C5      push    offset aError31CouldNo ; "Error 3.1: Could not set Registry value"...
.text:004011CA      call    sub_401271
.text:004011CF      add     esp, 4

```

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
- Xóa 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 HTML file. Nếu thỏa mãn, mã độc thực hiện lấy ký tự đầu tiên trong HTML comment và coi ký tự đó là điều kiện nhảy switch case, thực hiện một trong các hành vi:

- ## Lab 6-04