

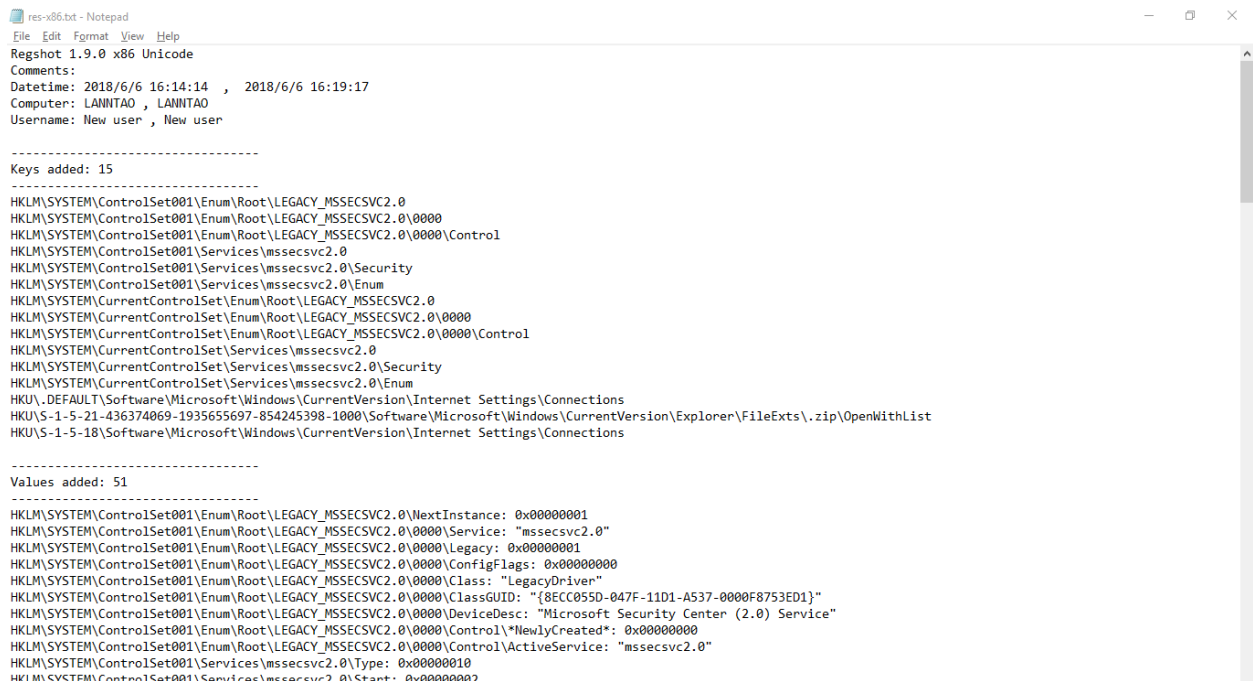
# MSSEVC.EXE

Sau khi bỏ kha khá thời gian ra re và hiểu hoạt động của con taskche.exe, mình nhanh chóng chuyển sang kiểm tra con mssecsvc.exe này. Qua phân tích sơ bộ thì có thể nhận định con này là 1 dropper với chức năng chính :

- + ) Drop con taskche.exe
- + ) Kill switch (đã bị xóa trong phiên bản này)
- + ) Khai thác lỗ hổng Eternal Blue

## Phân tích thủ công :

- + ) Sử dụng RegShot để phân tích, compare registry thay đổi trước và sau khi chạy malware :



```
res-x86.txt - Notepad
File Edit Format View Help
Regshot 1.9.0 x86 Unicode
Comments:
Datetime: 2018/6/6 16:14:14 , 2018/6/6 16:19:17
Computer: LANNTAO , LANNTAO
Username: New user , New user

-----
Keys added: 15
-----
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_MSSECSVC2.0
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_MSSECSVC2.0\0000
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_MSSECSVC2.0\0000\Control
HKLM\SYSTEM\ControlSet001\Services\mssecsvc2.0
HKLM\SYSTEM\ControlSet001\Services\mssecsvc2.0\Security
HKLM\SYSTEM\ControlSet001\Services\mssecsvc2.0\Enum
HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_MSSECSVC2.0
HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_MSSECSVC2.0\0000
HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_MSSECSVC2.0\0000\Control
HKLM\SYSTEM\CurrentControlSet\Services\mssecsvc2.0
HKLM\SYSTEM\CurrentControlSet\Services\mssecsvc2.0\Security
HKLM\SYSTEM\CurrentControlSet\Services\mssecsvc2.0\Enum
HKU\S-1-5-21-436374069-1935655697-854245398-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.zip\OpenWithList
HKU\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections

-----
Values added: 51
-----
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_MSSECSVC2.0\NextInstance: 0x00000001
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_MSSECSVC2.0\0000\Service: "mssecsvc2.0"
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_MSSECSVC2.0\0000\Legacy: 0x00000001
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_MSSECSVC2.0\0000\ConfigFlags: 0x00000000
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_MSSECSVC2.0\0000\Class: "LegacyDriver"
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_MSSECSVC2.0\0000\ClassGUID: "{8ECC055D-047F-11D1-A537-0000F8753ED1}"
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_MSSECSVC2.0\0000\DeviceDesc: "Microsoft Security Center (2.0) Service"
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_MSSECSVC2.0\0000\Control\NewlyCreated*: 0x00000000
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_MSSECSVC2.0\0000\Control\ActiveService: "mssecsvc2.0"
HKLM\SYSTEM\ControlSet001\Services\mssecsvc2.0\Type: 0x00000010
HKLM\SYSTEM\ControlSet001\Services\mssecsvc2.0\Start: 0x00000002
```

- + ) Sử dụng wireshark phân tích gói tin :

2.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
18	53.912115	192.168.56.152	104.17.40.137	HTTP	154	GET / HTTP/1.1
20	53.916518	104.17.40.137	192.168.56.152	HTTP	412	HTTP/1.1 200 OK (text/plain)
25	56.974279	192.168.56.152	104.17.40.137	HTTP	154	GET / HTTP/1.1
27	56.979032	104.17.40.137	192.168.56.152	HTTP	412	HTTP/1.1 200 OK (text/plain)

> Internet Protocol Version 4, Src: 192.168.56.152, Dst: 104.17.40.137

> Transmission Control Protocol, Src Port: 56500, Dst Port: 80, Seq: 1, Ack: 1, Len: 100

> Hypertext Transfer Protocol

> GET / HTTP/1.1\r\n

Host: www.iuqerfsodp9ifjaposdfjhgosurijfaewrgwea.com\r\n

Cache-Control: no-cache\r\n

\r\n

[Full request URI: http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrgwea.com/]

ETHER 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

0018 01101110 11101111 11000000 10101000 00111000 10011000 01101000 00010001 n...8.h.

0020 00101000 10001001 11011100 10110100 00000000 01010000 00000000 11110100 {...P..

0022 10000010 00100010 10101011 01000111 01111101 00001110 01010000 00011000 ..G}.P.

0030 00000001 00000000 01001111 01011110 00000000 00000000 01000111 01000101 ..O^..GE

0038 01010100 00100000 00101111 00100000 01001000 01010100 01010100 01010000 T / HTTP

0040 00101111 00110001 00101110 00110001 00001010 00001010 01001000 01101111 /1.1..Ho

0048 01110011 01101000 00110100 00100000 01110111 01110111 01110111 00101110 st: www.

0050 01101001 01110101 01110001 01100101 01110010 01110010 01110011 01101111 iuqerfso

0058 01100100 01110000 00111001 01101001 01100110 01101010 01100001 01110000 dp9ifjap

0060 01101111 01110011 01100100 01100110 01101010 01101000 01100111 01101111 osdfjhgo

0068 01110011 01110101 01110010 01101001 01101010 01100110 01100001 01100101 surijfae

0070 01110111 01110010 01110111 01100101 01110010 01110111 01110111 01100101 wrgwe

0078 01100001 00101110 01100011 01101111 01101001 00001010 00001010 01000011 a.com..C

0080 01100001 01100011 01101000 01100101 00101001 01000011 01101111 01101110 ache-Con

0088 01101000 01110010 01101111 01101100 00110100 00100000 01101110 01101111 trol: no

0090 00101101 01100011 01100001 01100011 01101000 01100101 00001101 00001010 -cache..

0098 00001101 00001010 ..

## Phân tích bằng công cụ tổng hợp :

Ở đây mình sài công cụ online cho phép phân tích tổng hợp mấy “món” này là : <https://www.hybrid-analysis.com>

Link report : <https://www.hybrid-analysis.com/sample/112ad9dbab06d887ac3a5b7ca6a2ddd772762980f93926bd381efd7d34a251c0/5b17a0a27ca3e13fc5345ee8>

## System Security

### Modifies proxy settings

details "00000000")

"<Input Sample>" (Access type: "DELETEVAL"; Path: "HKCU\SOFTWARE\MICROSOFTWINDOWS\CURRENTVERSION\INTERNET SETTINGS"; Key: "PROXYSERVER")  
"<Input Sample>" (Access type: "DELETEVAL"; Path: "HKCU\SOFTWARE\MICROSOFTWINDOWS\CURRENTVERSION\INTERNET SETTINGS"; Key: "PROXYOVERRIDE")  
"<Input Sample>" (Access type: "DELETEVAL"; Path: "HKCU\SOFTWARE\MICROSOFTWINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP"; Key: "PROXYBYPASS")  
"<Input Sample>" (Access type: "DELETEVAL"; Path: "HKLM\SOFTWARE\WOW6432NODE\MICROSOFTWINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP"; Key: "PROXYBYPASS")  
"<Input Sample>" (Access type: "SETVAL"; Path: "HKU\SOFTWARE\MICROSOFTWINDOWS\CURRENTVERSION\INTERNET SETTINGS"; Key: "PROXYENABLE"; Value: "00000000")  
"<Input Sample>" (Access type: "DELETEVAL"; Path: "HKU\SOFTWARE\MICROSOFTWINDOWS\CURRENTVERSION\INTERNET SETTINGS"; Key: "PROXYSERVER")  
"<Input Sample>" (Access type: "DELETEVAL"; Path: "HKU\SOFTWARE\MICROSOFTWINDOWS\CURRENTVERSION\INTERNET SETTINGS"; Key: "PROXYOVERRIDE")  
"<Input Sample>" (Access type: "DELETEVAL"; Path: "HKU\SOFTWARE\MICROSOFTWINDOWS\CURRENTVERSION\INTERNET SETTINGS\ZONEMAP"; Key: "PROXYBYPASS")

source **Registry** Access

relevance 10/10

research [Show me all reports matching the same indicator](#)

### Queries sensitive IE security settings

details "<Input Sample>" (Path: "HKCU\SOFTWARE\MICROSOFT\INTERNET EXPLORER\SECURITY"; Key: "DISABLESECURITYSETTINGSCHECK")

source **Registry** Access

relevance 8/10

research [Show me all reports matching the same indicator](#)

Ở đây ta có thể thấy công cụ cho ra 2 kết quả hoạt động “khả nghi” với registry là :

1. Enable proxy => cái này để tạo môi trường cho TOR hoạt động
2. Tắt Security Check của IE

```
mssecsvc.exe
PID: 3880, Report UID: 00011949-00003880
Stream UID: 00011949-00003880-32850-42-004072AO
File Name: 00011949-00003880.00000000.12269.00400000.00000002.mdmp

-
@4072cc: push eax
@4072cd: call 004097D4h ;inet_addr@WS2_32.DLL
@4072d2: mov ecx, dword ptr [esp+00000434h]
@4072d9: mov dword ptr [esp+14h], eax
@4072dd: push ecx
@4072de: call 004097CEh ;htonl@WS2_32.DLL
@4072e3: push 00000000h
@4072e5: push 00000001h
@4072e7: push 00000002h
@4072e9: mov word ptr [esp+1Eh], ax
@4072ee: call 004097C8h ;socket@WS2_32.DLL
@4072f3: mov esi, eax
@4072f5: cmp esi, FFFFFFFFh
@4072f8: je 0040746Ch
@4072fe: lea edx, dword ptr [esp+10h]
@407302: push 00000010h
@407304: push edx
@407305: push esi
@407306: call 004097C2h ;connect@WS2_32.DLL
@40730b: cmp eax, FFFFFFFFh
@40730e: je 00407466h
@407314: push 00000000h
@407316: push 00000089h
@40731b: push 0042E544h
@407320: push esi
@407321: call 004097BCh ;send@WS2_32.DLL
@407326: cmp eax, FFFFFFFFh
@407329: je 00407466h
@40732e: push 00000000h
```

Các dll được import => dùng để tạo kết nối TCP => dùng trong khai thác lỗ hổng Eternal Blue

## Phân tích dữ liệu lấy được từ 2 cái trên và phân tích binary :

### 1. Kill switch bị NOP :

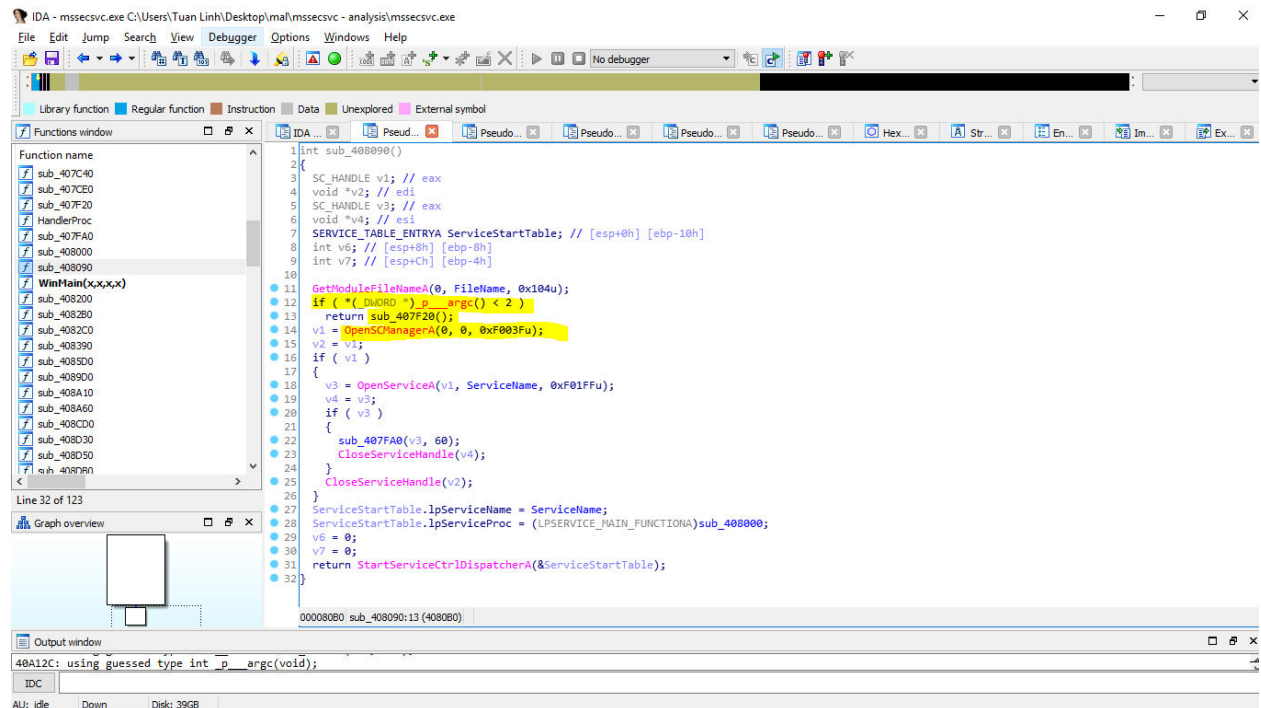
<http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com> .

Kết nối thành công => malware sẽ quit, theo phiên bản đầu tiên là sẽ thế, nhưng trong phiên bản này có vẻ ai đó đã xóa kill switch. Code không bị thay đổi (ví dụ thay đổi url, xóa phần check Url, etc...) mà dường như là patch (nop) lại phần code của kill switch nên có lẽ không phải tác giả chỉnh sửa.

```
int stdcall WinMain(HINSTANCE hInstance, HINSTANCE hPrevInstance, LPSTR lpCmdLine, int nShowCmd)
{
    void *v4; // esi
    CHAR szUrl; // [esp+8h] [ebp-50h]
    int v7; // [esp+41h] [ebp-17h]
    int v8; // [esp+45h] [ebp-13h]
    int v9; // [esp+49h] [ebp-Fh]
    int v10; // [esp+4Dh] [ebp-8h]
    int v11; // [esp+51h] [ebp-7h]
    __int16 v12; // [esp+55h] [ebp-3h]
    char v13; // [esp+57h] [ebp-1h]

    strcpy(&szUrl, "http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com");
    v7 = 0;
    v8 = 0;
    v9 = 0;
    v10 = 0;
    v11 = 0;
    v12 = 0;
    v13 = 0;
    v4 = InternetOpenA(0, 1u, 0, 0, 0);
    InternetOpenUrlA(v4, &szUrl, 0, 0, 0x84000000, 0);
    InternetCloseHandle(v4);
    InternetCloseHandle(0);
    sub_408090();
    return 0;
}
```

## 2. OpenCSManager :



Nếu argc >= 2 thì sẽ chạy OpenCSManager(), cụ thể argc ở đây là “-m security”

```
-----
Values added: 51
-----
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_MSSECSVC2.0\NextInstance: 0x00000001
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_MSSECSVC2.0\0000\Service: "mssecsvc2.0"
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_MSSECSVC2.0\0000\Legacy: 0x00000001
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_MSSECSVC2.0\0000\ConfigFlags: 0x00000000
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_MSSECSVC2.0\0000\Class: "LegacyDriver"
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_MSSECSVC2.0\0000\ClassGUID: "{8ECC055D-047F-11D1-A537-0000F875ED1}"
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_MSSECSVC2.0\0000\DeviceDesc: "Microsoft Security Center (2.0) Service"
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_MSSECSVC2.0\0000\Control\*NewlyCreated*: 0x00000000
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_MSSECSVC2.0\0000\Control\ActiveService: "mssecsvc2.0"
HKLM\SYSTEM\ControlSet001\Services\mssecsvc2.0\Type: 0x00000010
HKLM\SYSTEM\ControlSet001\Services\mssecsvc2.0\Start: 0x00000002
HKLM\SYSTEM\ControlSet001\Services\mssecsvc2.0\ErrorControl: 0x00000001
HKLM\SYSTEM\ControlSet001\Services\mssecsvc2.0\ImagePath: "C:\Documents and Settings\New user\Desktop\mssecsvc.exe -m security"
HKLM\SYSTEM\ControlSet001\Services\mssecsvc2.0\DisplayName: "Microsoft Security Center (2.0) Service"
HKLM\SYSTEM\ControlSet001\Services\mssecsvc2.0\ObjectName: "LocalSystem"
HKLM\SYSTEM\ControlSet001\Services\mssecsvc2.0\FailureActions: 00 00 00 01 00 00 01 00 00 01 00 00 00 00 00 01 00 00 60 EA 00 00
HKLM\SYSTEM\ControlSet001\Services\mssecsvc2.0\Security\Security: 01 00 14 80 90 00 00 00 9C 00 00 00 14 00 00 00 30 00 00 00 02 00 1C 00 01 00 00 00 02 80 14 00 FF 01
```

Vậy OpenCSManager() là gì và làm gì? :

## Service Control Manager

The service control manager (SCM) is started at system boot. It is a remote procedure call (RPC) server, so that service configuration and service control programs can manipulate services on remote machines.

Thực ra ngoài phương pháp để khởi động cùng start up như ta đã nói trong khi phân tích file tasksche.exe, thì còn phương pháp khác là register application như một Service trong windows , cụ thể ở đây là tasksche.exe

Đầu tiên nó drop file này vào %WINDIR%

Installation/Persistence
<p>Creates a system file in windows directory</p> <p><b>details</b> "&lt;Input Sample&gt;" created file "%WINDIR%\tasksche.exe"</p> <p><b>source</b> API Call</p> <p><b>relevance</b> 7/10</p> <p><b>research</b> <a href="#">Show me all reports matching the same indicator</a></p>
<p>Drops executable files to the Windows system directory</p> <p><b>details</b> File type "PE32 executable (GUI) Intel 80386 for MS Windows" was dropped at "%WINDIR%\tasksche.exe"</p> <p><b>source</b> Extracted File</p> <p><b>relevance</b> 7/10</p> <p><b>research</b> <a href="#">Show me all reports matching the same indicator</a></p>

Sau đó thì đăng ký cho nó thành một services.

```
v1 = OpenSCManagerA(0, 0, 0xF003Fu);
v2 = v1;
if ( v1 )
{
    v3 = OpenServiceA(v1, ServiceName, 0xF01FFu);
    v4 = v3;
    if ( v3 )
    {
        sub_407FA0(v3, 60);
        CloseServiceHandle(v4);
    }
    CloseServiceHandle(v2);
}
ServiceStartTable.lpServiceName = ServiceName;
ServiceStartTable.lpServiceProc = (LPSERVICE_MAIN_FUNCTIONA)sub_408000;
v6 = 0;
v7 = 0;
return StartServiceCtrlDispatcherA(&ServiceStartTable);
}
```

### 3. Service Control Dispatcher : (SMB Exploit)

```
loc_408101:
lea     eax, [esp+14h+ServiceStartTable]
mov     [esp+14h+ServiceStartTable.lpServiceName], offset ServiceName ; "mssecsvc2.0"
push    eax ; lpServiceStartTable
mov     [esp+18h+ServiceStartTable.lpServiceProc], offset sub_408000
mov     [esp+18h+var_8], 0
mov     [esp+18h+var_4], 0
call    ds:StartServiceCtrlDispatcherA
pop     edi
add     esp, 10h
retn
sub_408090 endp
```

## StartServiceCtrlDispatcher function

Connects the main thread of a service process to the service control manager, which causes the thread to be the service control dispatcher thread for the calling process.

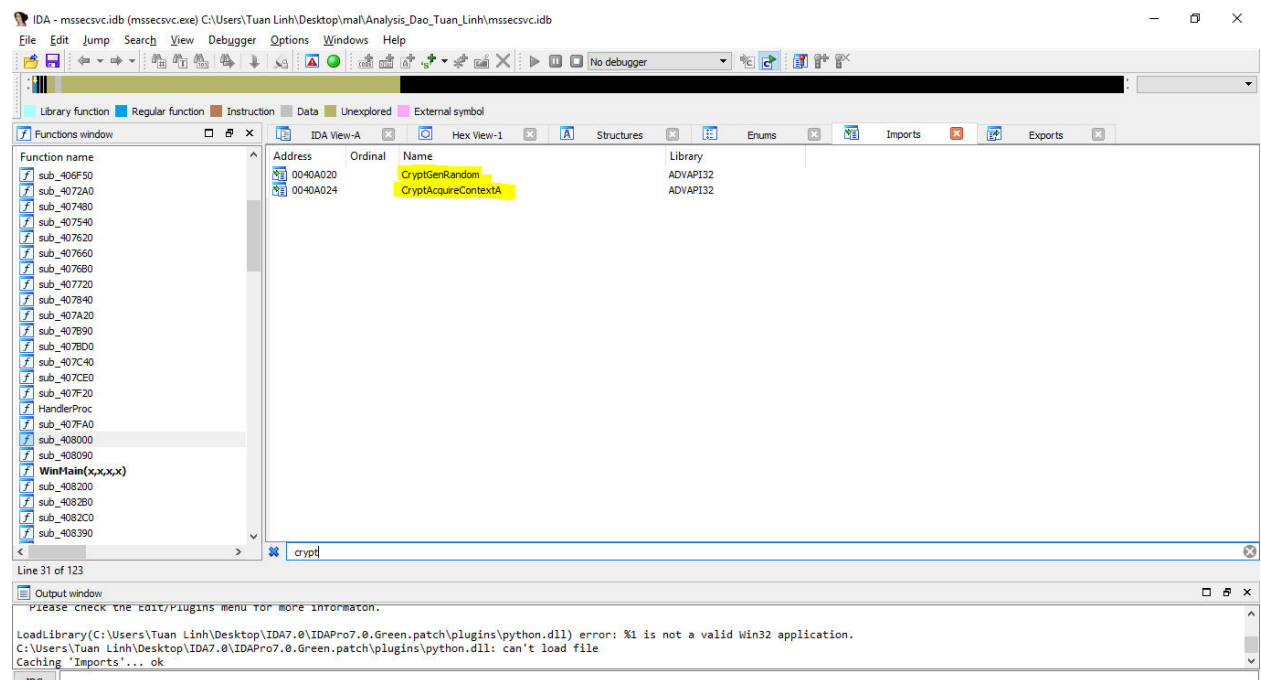
## 4. Chi tiết về phương thức sử dụng SMB Exploit (Eternal Blue)

:

<https://cloudblogs.microsoft.com/microsoftsecure/2017/06/30/exploring-the-crypt-analysis-of-the-wannacrypt-ransomware-smb-exploit-propagation/>

**Encryption method : RSA 2048, using Windows API ☺**

Vì cái này khá phổ biến và hầu như ransomware nào cũng dùng chung cách nên cũng không có gì đáng để analysis, có thể dễ dàng nhận ra qua việc kiểm tra các function được import vào



Chi tiết : <https://medium.com/threat-intel/wannacry-ransomware-decryption-821c7e3f0a2b>