**29/1**

**xử lý process**

**gồm :**

* **ProcessID**
* **ParentPID**
* **CommandLine**
* **Image**
* **ProcessType**
* **Registry**
* **DroppedFiles**
* **DebugStrings**
* **Files**
* **Modules**
* **EventsCounters\_Network**
* **Scores\_Network**
* **nhiều ip -> type**
* **nhiều domain -> type**
* **nhiều http request -> type**
* **Priority ->type**
* **Autostart**
* **LowAccess**
* **FileType: (String)**

**-> 12 thuộc tính k cần xử lý**

**6 thuộc tính cần xử lý - > mục tiêu : trích thêm thuộc tính**

I. Trích thuộc tính

1. **pa1:**

* **IP** -> đã được phân loại 4 nhóm : 0 -> 4 -> có trong SYSMON

-> yêu cầu hệ thống đánh giá ip

* **Domain** -> đã được phân loại 4 nhóm : 0 -> 4 -> có trong SYSMON

-> yêu cầu hệ thống đánh giá domain

* **HttpRequests** -> đã được phân loại 4 nhóm : 0 -> 4 -> **không có trong SYSMON**

-> yêu cầu hệ thống trích xuất và đánh giá HttpRequests

**0: unknown**

**1: Suspicious**

**2: Malicious**

**3: whitelist**

**4: unsafe**

=> nhóm IP, Domain, HttpRequests trích 5x3= 15 thuộc tính tương ứng số lượng từng nhãn đánh giá được

ví dụ : d15ea029-37e4-4909-a687-f51a4ce8d2ae.json

"ProcessOID": "600aaa8c4be80029fe4188b5"

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0\_ip | 1\_ip | 2\_ip | 3\_ip | 0\_domain | 1\_domain | 2\_domain | 3\_domain | 0\_http | 1\_http | 2\_http | 3\_http |
| 0 | 7 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 |

1. pa2:

Tính giá trị sử dụng công thức entropy

x là sự kiện xảy ra (loại ip1, ip2,...)

p(x) là xác suất sảy ra sự kiện x

****

**=> tính được giá trị ip\_score = h(x)**

**dns, http tương tự…**

**tgv**

1. pa3:

chỉ lấy ip, domain, http có chỉ số max

vd:

|  |  |  |
| --- | --- | --- |
| ip | domain | http |
| 1 | 1 | 1 |

30/1

**II. registry :**

5 loại HKEY -> đếm

* **HKEY\_LOCAL\_MACHINE => hardware settings**
* **HKEY\_CLASSES\_ROOT**
* **HKEY\_USERS => settings for all users**
* **HKEY\_CURRENT\_CONFIG**
* **HKEY\_CURRENT\_USER**

**=> số lượng**

5 loại hành vi => có thể nhiều hơn

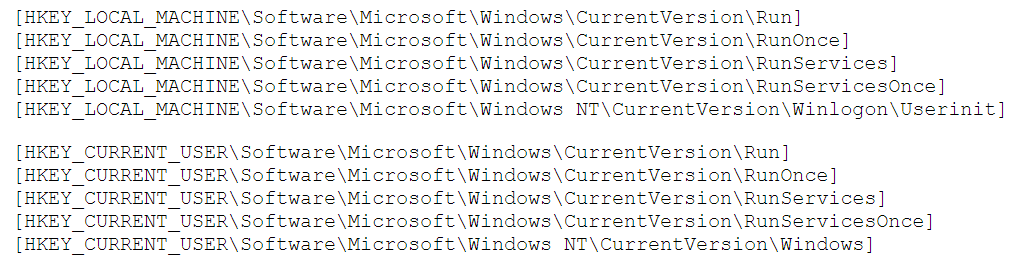
 => true/false

**C:/Users/Huong/Downloads/tajoddin2019.pdf**

7 nhóm security-sensitive registry keys

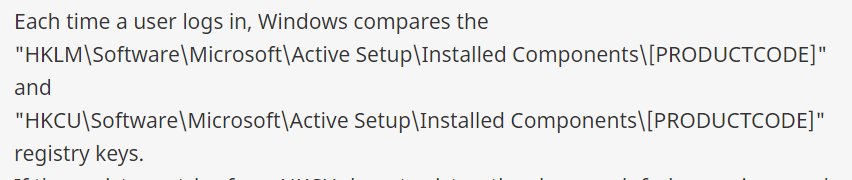
05/02

* ***Startup registry keys:***

**

* ***Active setup registry keys:***

*https://www.itninja.com/blog/view/active-setup-concept#:~:text=Using%20Active%20Setup%20registry%20keys,process%20to%20finish%20configuring%20it.*

**

* **Services registry keys:**
* *DLL injection registry keys:*

*https://en.wikipedia.org/wiki/DLL\_injection*

* *Shell spawning registry keys*
* *Internet settings registry keys:*
* *BHO registry keys:*

*https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=df7c2f3f-cac4-44cf-a2d3-72b5778ce057&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments*

|  |  |  |
| --- | --- | --- |
| security-sensitive registry key group | *keys* |  |
| ***Startup registry keys:*** | [HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices]  [HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce]  [HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]  [HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce]  [HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run]  [HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce]  [HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\RunServices]  HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnceEx | CurrentVersion\RunServices  CurrentVersion\RunServicesOnce  CurrentVersion\Run  CurrentVersion\RunOnce  CurrentVersion\RunOnceEx  *CurrentVersion\Policies\Explorer\Run* |
| ***Active setup registry keys:*** | *HKLM\Software\Microsoft\Active Setup, HKCU\Software\Microsoft\Active Setup*  *[HKEY\_LOCAL\_MACHINE\Software\Microsoft\Active Setup\Installed Components\KeyName]* | *Active Setup\Installed Components*  *Microsoft\Active Setup* |
| **Services registry keys:** | HKLM\SYSTEM\CurrentControlSet\Services\ | CurrentControlSet\Services\ |
| *DLL injection registry keys:* | *HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Windows\AppInit\_DLLs*  *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\AppCertDLLs*  *HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows\LoadAppInit\_DLLs*  *HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\LoadAppInit\_DLLs = 1* | *Windows\AppInit\_DLLs*  *Session Manager\AppCertDLLs*  *Windows\LoadAppInit\_DLLs* |
| *Shell spawning registry keys* | *[HKEY\_CLASSES\_ROOT\exefile\shell\open\command] @="\"%1\" %\*"*  *[HKEY\_CLASSES\_ROOT\comfile\shell\open\command] @="\"%1\" %\*"*  *[HKEY\_CLASSES\_ROOT\batfile\shell\open\command] @="\"%1\" %\*"*  *[HKEY\_CLASSES\_ROOT\htafile\Shell\Open\Command] @="\"%1\" %\*"*  *[HKEY\_CLASSES\_ROOT\piffile\shell\open\command] @="\"%1\" %\*"*  *[HKEY\_LOCAL\_MACHINE\Software\CLASSES\batfile\shell\open\command] @="\"%1\" %\*"*  *[HKEY\_LOCAL\_MACHINE\Software\CLASSES\comfile\shell\open\command] @="\"%1\" %\*"*  *[HKEY\_LOCAL\_MACHINE\Software\CLASSES\exefile\shell\open\command] @="\"%1\" %\*"*  *[HKEY\_LOCAL\_MACHINE\Software\CLASSES\htafile\Shell\Open\Command] @="\"%1\" %\*"*  *[HKEY\_LOCAL\_MACHINE\Software\CLASSES\piffile\shell\open\command] @="\"%1\" %\*"* | *exefile\shell\Open\command*  *comfile\shell\Open\command*  *batfile\shell\Open\command*  *htafile\Shell\Open\Command*  *piffile\shell\Open\command*  *open\command* |
| *Internet settings registry keys:* | *HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings* | *CurrentVersion\Internet Settings* |
| *BHO registry keys:* | *HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects* | *Explorer\Browser Helper Objects* |

4/2

* Danh sách các key cho registry

[**https://attack.mitre.org/techniques/enterprise/?fbclid=IwAR00NdaMSdIt-f2PIvpNC5HZqRYab8me-4mlW\_Jf0CnyRuoY3R3mT0YcCMU**](https://attack.mitre.org/techniques/enterprise/?fbclid=IwAR00NdaMSdIt-f2PIvpNC5HZqRYab8me-4mlW_Jf0CnyRuoY3R3mT0YcCMU)

[**https://attackevals.mitre-engenuity.org/APT29/results/reaqta/allresults.html**](https://attackevals.mitre-engenuity.org/APT29/results/reaqta/allresults.html)

**HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall**

[**https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=df7c2f3f-cac4-44cf-a2d3-72b5778ce057&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments**](https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=df7c2f3f-cac4-44cf-a2d3-72b5778ce057&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments)

1. *Startup registry keys:*

<https://www.picussecurity.com/resource/blog/picus-10-critical-mitre-attck-techniques-t1060-registry-run-keys-startup-folder>

<https://attack.mitre.org/techniques/T1547/001/>

***mitre : T1060 , T1547.001***

key: run, runonce, RunOnceEx, *Shell Folders….*

|  |
| --- |
| HKCU\Software\Microsoft\Windows\CurrentVersion\Run |
| HKLM\Software\Microsoft\Windows\CurrentVersion\Run |
| HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce |
| HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce |
| HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnceEx |
| HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Load |
| HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\Session Manager\BootExecute’từ *thành* để thực thi tải trọng của nó trong khi khởi động Windows. [[103]](https://www.welivesecurity.com/wp-content/uploads/2018/09/ESET-LoJax.pdf)‘autocheck autochk *’‘autocheck autoche* ’ |

|  |
| --- |
| *HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders* |
| *HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders* |
| *HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders* |
| *HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders* |

|  |
| --- |
| *HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices* |
| *HKCU\Software\Microsoft\Windows\CurrentVersion\RunServices* |
| *HKLM\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce* |
| *HKCU\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce* |

*HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run*

*HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run*

* *HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\Userinit*
* *HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\Shell*
* *HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\Notify*

1. *Active setup registry keys:*

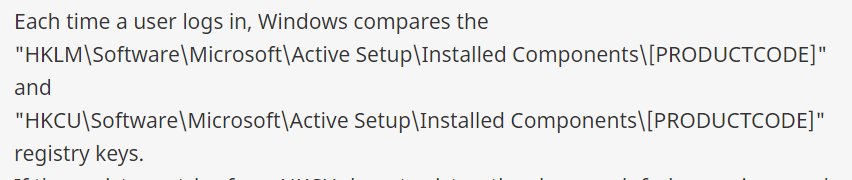
***mitre :***

***key :***

*HKLM\Software\Microsoft\Active Setup, HKCU\Software\Microsoft\Active Setup*

***link:***

[*https://www.itninja.com/blog/view/active-setup-concept#:~:text=Using%20Active%20Setup%20registry%20keys,process%20to%20finish%20configuring%20it*](https://www.itninja.com/blog/view/active-setup-concept#:~:text=Using%20Active%20Setup%20registry%20keys,process%20to%20finish%20configuring%20it)*.*

**

*ví dụ:*

*[HKEY\_LOCAL\_MACHINE\Software\Microsoft\Active Setup\Installed Components\KeyName]*

*StubPath=C:\PathToFile\Filename.exe*

1. *Services registry keys:*

[*https://attack.mitre.org/techniques/T1574/011/*](https://attack.mitre.org/techniques/T1574/011/)

[*https://attack.mitre.org/techniques/T1112/*](https://attack.mitre.org/techniques/T1112/)

|  |
| --- |
| *HKLM\system\\services\* |
| *HKLM\SYSTEM\CurrentControlSet\Services\<thông tin khác>*  *(Hijack Execution Flow: Services Registry Permissions Weakness)* |

*ví dụ:*

*HKLM\SYSTEM\CurrentControlSet\services\[service\_name]\Start*

1. *DLL injection registry keys:*

[*https://attack.mitre.org/techniques/T1546/009/*](https://attack.mitre.org/techniques/T1546/009/)

[*https://attack.mitre.org/techniques/T1546/010/*](https://attack.mitre.org/techniques/T1546/010/)

|  |
| --- |
| *HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows* |
| *HKEY\_LOCAL\_MACHINE\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows* |
| *HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows "AppInit\_DLLs"="pserver32.dll"* |
| *HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows\AppInit\_DLLs – %APPDATA%\Intel\ResN32.dllvà HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows\LoadAppInit\_DLLs – 0x1.* |
| *‘HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\BootExecute’ from ‘autocheck autochk ’ to ‘autocheck autoche ’* |

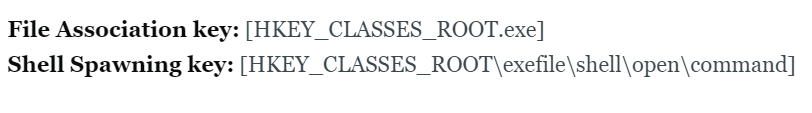
*ví dụ:*

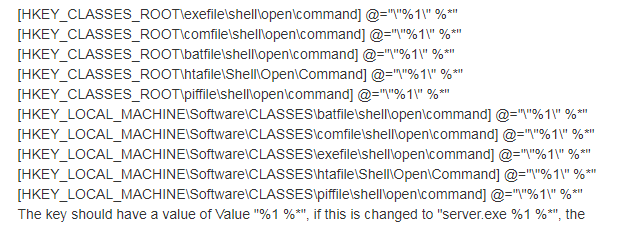
*HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows\lllt.dlll*

1. *Shell spawning registry keys*

[*https://omgdebugging.com/2015/08/10/file-associations-and-shell-spawning/*](https://omgdebugging.com/2015/08/10/file-associations-and-shell-spawning/)

**HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell**

**

**

1. *Internet settings registry keys:*

[*https://attack.mitre.org/techniques/T1012/*](https://attack.mitre.org/techniques/T1012/)

|  |
| --- |
| *HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings* |

*ví dụ*

*HKEY\_CURRENT\_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings\\Connections*

1. *BHO registry keys:*

[*https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=internet+explorer*](https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=internet+explorer)

[*https://social.msdn.microsoft.com/Forums/en-US/c0587dc6-17e3-4bd5-b0bc-8afc92106e5d/is-there-a-registry-setting-to-query-to-see-if-a-bho-has-been-disabled?forum=ieextensiondevelopment*](https://social.msdn.microsoft.com/Forums/en-US/c0587dc6-17e3-4bd5-b0bc-8afc92106e5d/is-there-a-registry-setting-to-query-to-see-if-a-bho-has-been-disabled?forum=ieextensiondevelopment)

|  |
| --- |
| *HKEY\_LOCAL\_MACHINE \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Policies \ Ext* |
| *HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\* |
| ***HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Settings\<BHO CLSID>*** |
| ***HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects*** |

*\*\* ngoài ví dụ cụ thể*

# *Credentials in Registry*

<https://resources.infosecinstitute.com/topic/mitre-attck-vulnerability-spotlight-credentials-in-registry/#:~:text=Why%20are%20credentials%20in%20the,privileges%20on%20a%20compromised%20system>.

|  |
| --- |
| *reg query HKLM /f password /t REG\_SZ /s*  *# or*  *reg query HKCU /f password /t REG\_SZ /s*  *HKLM:\SAM\SAM\Domains\Account\Users\* |

1. *modify:*

[*https://attack.mitre.org/techniques/T1112/*](https://attack.mitre.org/techniques/T1112/)

|  |
| --- |
| *HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ Path* |
| *SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfileGloballyOpenPorts\List* |
| *HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Pniumj* |
| *HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Load* |
| *HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System Enable LUA="0" and HKEY\_CURRENT\_USER\Software\DC3\_FEXEC* |
| *HKCU\Software\Classes\Applications\rundll32.exe\shell\open* |
| *HKCU\Software\Microsoft\Office\<version>\<product>\Security\VBAWarnings and HKCU\Software\Microsoft\Office\<version>\<product>\Security\AccessVBOM* |
| *HKCU\Software\Microsoft\Office\* |
| *HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\WABE\DataPath* |
| *‘HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\BootExecute’ from ‘autocheck autochk ’ to ‘autocheck autoche ’* |
| *HKCU\Software\Microsoft[dllname] and modifies Registry keys under HKCR\CLSID...\InprocServer32* |
| *HKEY\_CURRENT\_USER\SOFTWARE{{8 random characters}}* |
| *HKLM\SOFTWARE\Microsoft\DRM* |
| *SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LocalAccountTokenFilterPolicy* |
| *HKLM\SYSTEM\CurrentControlSet\services\[service\_name]\Start* |
| *SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers* |
| *HKEY\_CURRENT\_USER\Software\Classes\* |
| *HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Applications\laxhost.dll and HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\PrintConfigs* |
| *HKCU\Software\ApplicationContainer\Appsw64* |
| *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\WMI\Security* |
| *HKLM\System\CurrentControlSet\Control\SecurityProviders\WDigest* |
|  |

1. *querry registry*

[*https://attack.mitre.org/techniques/T1012/*](https://attack.mitre.org/techniques/T1012/)

|  |
| --- |
| *Software\Microsoft\Windows\CurrentVersion\Uninstall* |
| *HKEY\_CURRENT\_USER\Software\Microsoft\Terminal Server Client\Default* |
| *HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings* |
| *HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Load* |
| *HKCR\http\shell\open\command* |
| *HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run* |
| *SYSTEM\CurrentControlSet\Control\Lsa Name* |
| *HKEY\_CURRENT\_USER\Software\Bitcoin\Bitcoin-Qt* |
| *"HKEY\_CURRENT\_USER\Software\Microsoft\Terminal Server Client\Default"* |
| *HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces* |
| *HKLM\Software\Microsoft\Windows NT\CurrentVersion ProductName or HKLM\HARDWARE\DESCRIPTION\System\CentralProcessor\0 ProcessorNameString* |
| *reg query "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\InternetSettings"* |
| *HKLM\System\CurrentControlSet\Services\mssmbios\Data\SMBiosData* |
| *HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid* |
| *HKU\SOFTWARE\Microsoft\CTF* |
|  |
|  |

*6/2-7/2*

**Xử lý filetype vs processtype**

|  |  |
| --- | --- |
| **FileType** | **ProcessType** |
| **ADB** | **Child process** |
| **BRW-CHR** | **Dropped from another process** |
| **BRW-FF** | **Embedded COM++** |
| **BRW-IE** | **Injected** |
| **BRW-OPR** | **Main process** |
| **FLS** | **MSI Installer** |
| **INS-DRV** | **Probably manual launch or APC inject** |
| **INS-MSI** | **Runned from Explorer.exe** |
| **JVA** | **Suspicious** |
| **NKN** | **Was launched as a service** |
| **OFS** | **Was launched through Task Scheduler** |
| **OUTL** | **WMI Requests** |
| **SCR-CMD** |  |
| **SCR-HTA** |  |
| **SCR-PSH** |  |
| **SCR-WS** |  |
| **WIN-SYS** |  |
| **WIN-TOL** |  |
| **WIN-XPR** |  |
| **KHOANG TRANG “ ”** |  |

**III. Priority: 3 mức**

**1: Low**

**2: Medium**

**3: High**

=> độ ưu tiên tiến trình

31/1

**IV. image + cmd:**

1. **image**

**phương án 1:** chỉ lấy 1-2 thư mục đầu

vd : 0c8d54b4-1f6b-431d-b14d-304182e66428.json

"OID": "5b33bff03628a5337a057bc7" -> C:\\Windows

"OID": "5b33bff03628a5337a0582b5" -> C:\\Users\\admin hoặc C:\\Users

"OID": "5b33bff23628a5337a058aaa" -> C:\\Windows\\ hoặc C:\\Windows\\system32\\

**=> to categorical**

**phương án 2:**

1 image = 1 doc

1 thu muc = 1 word

**=> doc2vec**

**vd : 0c8d54b4-1f6b-431d-b14d-304182e66428.json**

**"OID": "5b33bff33628a5337a059845"**

C:\\Users\\admin\\AppData\\Local\\Temp\\297bin.exe\

**=> word list :** C:, Users, admin, AppData, Local, Temp

=> quan tâm đến thứ tự => **sử dụng mô hình CBOW**

1. **cmd**

C:/Users/Huong/Downloads/1905.09538.pdf

b1: loại hết đường dẫn trong cmd

b2: trích lệnh và tham số => word

**=> doc2vec ( CBOW)**

**vd:0c8d54b4-1f6b-431d-b14d-304182e66428.json**

**"OID": "5b33bffc3628a5337a05e418"**

reg add HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Run /v PncVoJCIlqX /t REG\_EXPAND\_SZ /d \"\\\"C:\\Users\\admin\\AppData\\Roaming\\Oracle\\bin\\javaw.exe\\\" -jar \\\"C:\\Users\\admin\\eNSBiwAwNEK\\hwZNrnKcIhn.dthUyf\\\"\" /f

**=> trích :** reg , add, /v, /t, /d, -jar, /f

V. **DroppedFiles => số lượng ……?**

01/02->06/02

mục tiêu :

* mỗi mẫu -> 1 file csv gồm **nhiều ( không cố định )** process -> mỗi dòng 1 process
* mỗi process gồm **nhiều thuộc tính ( số lượng cố định )** như mô tả trên

kết quả :

file csv mẫu

1 process gồm các thuộc tính

|  |  |  |  |
| --- | --- | --- | --- |
| stt | tên | kiểu |  |
| f1 | ProcessID | string ( dựng cây ) |  |
| f2 | ParentPID | string ( dựng cây) |  |
|  | CreationTimestamp | number |  |
| f3 | CommandLine | String -> **categorical hoặc vector hoặc drop** |  |
| f4 | Image | String -> **drop hoặc vector** |  |
| f5 | ProcessType | String -> **categorical** |  |
| f6 | Registry | list - > 12 thuộc tính |  |
| HKEY\_LOCAL\_MACHINE | | number ( đếm số lượng ) |  |
| HKEY\_CLASSES\_ROOT | | number ( đếm số lượng ) |  |
| HKEY\_USERS | | number ( đếm số lượng ) |  |
| HKEY\_CURRENT\_CONFIG | | number ( đếm số lượng ) |  |
| HKEY\_CURRENT\_USER | | number ( đếm số lượng ) |  |
| Startup registry keys | | binary (true/false) |  |
| Active setup registry keys | | binary (true/false) |  |
| Services registry keys | | binary (true/false) |  |
| DLL injection registry keys | | binary (true/false) |  |
| Shell spawning registry keys | | binary (true/false) |  |
| Internet settings registry keys | | binary (true/false) |  |
| BHO registry keys | | binary (true/false) |  |
| f7 | DroppedFiles | number ( đếm số lượng ) |  |
| f8 | DebugStrings | number |  |
| f9 | Files | number |  |
| f10 | Modules | number |  |
| f11 | EventsCounters\_Network | number |  |
| f12 | Scores\_Network | binary (true/false) |  |
| f13 | ip | 5 thuộc tính theo 5 loại |  |
| unknown\_ip | | number ( đếm số lượng ) |  |
| Suspicious\_ip | | number ( đếm số lượng ) |  |
| Malicious\_ip | | number ( đếm số lượng ) |  |
| whitelist\_ip | | number ( đếm số lượng ) |  |
| unsafe\_ip | | number ( đếm số lượng ) |  |
| f14 | domain | 5 thuộc tính theo 5 loại |  |
| unknown\_domain | | number ( đếm số lượng ) |  |
| Suspicious\_domain | | number ( đếm số lượng ) |  |
| Malicious\_domain | | number ( đếm số lượng ) |  |
| whitelist\_domain | | number ( đếm số lượng ) |  |
| unsafe\_domain | | number ( đếm số lượng ) |  |
| f15 | http request | 5 thuộc tính theo 5 loại |  |
| unknown\_http\_request | | number ( đếm số lượng ) |  |
| Suspicious\_http\_request | | number ( đếm số lượng ) |  |
| Malicious\_http\_request | | number ( đếm số lượng ) |  |
| whitelist\_http\_request | | number ( đếm số lượng ) |  |
| unsafe\_http\_request | | number ( đếm số lượng ) |  |
| f16 | Priority | 3 mức ưu tiên |  |
| f17 | Autostart | binary (true/false) |  |
| f18 | LowAccess | binary (true/false) |  |
| f19 | FileType | String -> **categorical** |  |
| label | label | number 4 mức |  |

label 4 mức:

**0\_ no threats**

**1\_ suspicious**

**2\_malicious**

**không xác định**

code :

|  |  |
| --- | --- |
| **stt** | **note** |
| f3 | 2/2: drop |
| f4 | 2/2: drop |
| f6 | 4/2 oke 5 loại HKEY  còn 7 security-sensitive registry keys  6/2 oke |
| f7 | 2/2 oke |
| f13 | 3/2 list domain?  4/2 oke |
| f14 | 4/2 oke |
| f15 | 3/2 oke |
| f16 | 3/2 : đếm số lượng |
| lable | 3/2 oke |
| còn lại | 2/2 : oke |
| kết quả | 4/2 còn thiếu 7 security-sensitive registry keys  <https://drive.google.com/file/d/1BTeNJSiJ7P-F0UYrv5LRWchiZGtT_Nsg/view?usp=sharing>  6/2 oke  <https://drive.google.com/file/d/1cMDgv2fOOvfvpvk1iTYtEeYie-2ac7wx/view?usp=sharing>  bộ ~50k độc ~10k sạch  <https://drive.google.com/file/d/1bOmZnEF3S4aKImeTFE3TkZst4MQugbyv/view?usp=sharing> |

note:

|  |  |  |
| --- | --- | --- |
|  |  |  |
| 2/2 extract\_features | init() | * map các thuộc tính k cần xử lý và khởi tạo giá trị (0) cho các thuộc tính cần xử lý * input : list [{keys: values} ] => danh sách process * output: dict dict {OID: {features: values}}} => khởi tạo giá trị   features: nt |
| handel\_single\_task() | * map thuộc tính cho theo OID * input : json path * output: dict {OID: {feature: value}}} => đã gán giá trị tương ứng   feature: nt |
| 3/2 extract\_features | handle\_ip() | * input: list[{keys:values}] => danh sach ip * output: dict{OID:{feature:value} }   feature: "unknown\_ip", "Suspicious\_ip", "Malicious\_ip", "unsafe\_ip" : number (0->4)  “domain” : list String |
| handle\_http\_request() | - input: list[{keys:values}] => danh sach http\_request  - output:dict {OID:{feature:value} }  feature:"unknown\_http\_request", "Suspicious\_http\_request", "Malicious\_http\_request", "unsafe\_http\_request" : number (0->4) |
| handle\_label() | - input: list[{keys:values}] => danh sach Incident  - output:dict {OID:label }  label : number (0->4) |
| handle\_priority() | - input: list[{keys:values}] => danh sach Threat  - output:dict {OID:priority }  priority : number (0->3) |
| ……………….. | | |

06/02->..../02

Dữ liệu bình thường

//sẽ cập nhật thêm số lượng

|  |  |
| --- | --- |
| LOẠI | Số lượng |
| Adobe Flash | 2784 |
| JAVA | 2367 |
| Microsoft Office | 4939 |
| PE EXE | 16407 |
| PE DLL | 9564 |
| HTML Documents | 8824 |
| Adobe PDF | 7783 |
| Scripts | 27807 |
| Email files | 7929 |
| Archive files | 50684 |
| Tổng | 139138 |

Dữ liệu mã độc

|  |  |
| --- | --- |
| Tên mã độc | Số lượng |
| ursnif | 2856 |
| formbook | 1881 |
| covid19 | 1506 |
| nanocore | 1451 |
| agenttesla | 1381 |
| emotet | 1331 |
| hawkeye | 1321 |
| azorult | 1165 |
| fareit | 1130 |
| keylogger | 1126 |
| lokibot | 1098 |
| gandcrab | 1060 |
| troldesh | 1036 |
| pony | 1016 |
| Khác | 27531 |
| tổng | 46890 |

Dữ liệu nghi ngờ

|  |  |
| --- | --- |
| LOẠI | Số lượng |
| Adobe Flash | 46 |
| JAVA | 278 |
| Microsoft Office | 498 |
| PE EXE | 498 |
| PE DLL | 370 |
| HTML Documents | 467 |
| Adobe PDF | 366 |
| Scripts | 412 |
| Email files | 511 |
| Archive files | 300 |
| Tổng | 3746 |

dựng model phân loại process: RF, MLP

* trước khi train :
  + 100% drop : 'task', 'CreationTimestamp', 'ProcessID', 'ParentPID',
  + nếu k có ý định xử lý -> drop : 'CommandLine',

'Image'

file csv : <https://drive.google.com/file/d/1mHjTmU7ZXsRAVKFTKXL46a93m9X7Bj2l/view?usp=sharing>

code RF : <https://colab.research.google.com/drive/1Hj0nmbq5tmBiK1baZFInSzc_laruk_Pb?usp=sharing>

|  |  |  |  |
| --- | --- | --- | --- |
| Xử lý data | RF | | |
|  | 10 | 50 | 100 |
| - 'CommandLine': drop  - ‘Image’ : drop  - k train nhãn 0  - test cả nhãn 0 | acc: 55.46 | acc: 55.48 | acc: 55.48 |
| - 'CommandLine': drop  - ‘Image’ : drop  - train 4 nhãn  - test 4 nhãn | acc:95.92 | acc: 96.09 | acc:96.01 |
| - 'CommandLine': drop  - ‘Image’ : drop  - gộp nhãn 0 với nhãn 1  - train 3 nhãn  - test 3 nhãn | acc: 98.83 | acc: 98.93 | acc: 98.93 |
| - 'CommandLine': drop  - ‘Image’ : drop  - k train nhãn 0  - k test nhãn 0  Tỉ lệ nhãn 0 / Tổng số: 55.89% | acc: 97.88 | acc: 98.03 | acc: 98.05 |
| - 'CommandLine': drop  - ‘Image’ : drop  - gộp nhãn 0 với nhãn 2  - train 3 nhãn  - test 3 nhãn | acc: 98.83 | acc: 98.93 | acc: 98.93 |

Using Knn to replace label ’0’

Tổng số bản ghi nhãn 0/Tổng số bản ghi: 540094/1224332

Chia data gốc thành 3 phần:

* Phần 1:

|  |  |  |  |
| --- | --- | --- | --- |
| Label | Số lượng | % trên SL nhãn 0 | % trên tổng số |
| 0 | 194426 | 100% | 47.64% |
| 0=>1 | 5880 | 3.02% | 1.44% |
| 0=>2 | 33707 | 17.34% | 8.26% |
| 0=>3 | 154839 | 79.64% | 37.51% |

Total: 408110

* Phần 2:

|  |  |  |  |
| --- | --- | --- | --- |
| Label | Số lượng | % trên SL nhãn 0 | % trên tổng số |
| 0 | 163400 | 100% | 40.04% |
| 0=>1 | 3678 | 2.25% | 0.9% |
| 0=>2 | 27056 | 16.56% | 6.63% |
| 0=>3 | 132666 | 81.19% | 32.51% |

Total: 408110

* Phần 3:

|  |  |  |  |
| --- | --- | --- | --- |
| Label | Số lượng | % trên SL nhãn 0 | % trên tổng số |
| 0 | 182266 | 100% | 44.66% |
| 0=>1 | 5190 | 2.85% | 1.27% |
| 0=>2 | 35027 | 19.22% | 8.58% |
| 0=>3 | 142051 | 77.94% | 34.81% |

Total: 408112

18/02

|  |  |  |  |
| --- | --- | --- | --- |
| stt | tên | kiểu | Mô tả |
| f1 | ProcessID | string ( dựng cây ) | The identifier of process that triggers the event |
| f2 | ParentPID | string ( dựng cây) | Like ProcessId but for parent process |
|  | CreationTimestamp | number | Timestamp when the process created |
| f3 | CommandLine | String -> **categorical hoặc vector hoặc drop** | The command line string contains all arguments passed to the process upon execution |
| f4 | Image | String -> **drop hoặc vector** | The file path of the executable associated with the process |
| f5 | ProcessType | String -> **categorical** | Loại tiến trình |
| f6 | Registry | list - > 12 thuộc tính | The Windows Registry, or simply the registry, is a hierarchical database that stores configuration information that is crucial for the operation of Windows and the applications and  services that run on Windows [20] |
| HKEY\_LOCAL\_MACHINE | | number ( đếm số lượng ) | HKLM stores information about hardware settings, installed applications, Windows startup, and so on. Actually, it stores local machine-specific configuration information that is valid for all user profiles. |
| HKEY\_CLASSES\_ROOT | | number ( đếm số lượng ) | HKCR stores information about file type associations and COM (for Component Object Model) objects. |
| HKEY\_USERS | | number ( đếm số lượng ) | HKU stores Windows settings for all users and its subkeys contain information about all user profiles. |
| HKEY\_CURRENT\_CONFIG | | number ( đếm số lượng ) | HKCC stores the current  hardware profile settings |
| HKEY\_CURRENT\_USER | | number ( đếm số lượng ) | HKCU stores all information related to the profile of the user who is currently logged into Windows. |
| Startup registry keys | | binary (true/false) | Startup registry keys (for example, Run and RunOnce) are some registry entries that store paths to executable programs on Windows. Programs listed in these registry keys are automatically run after Windows is loaded. Malware writers often abuse  this feature to automatically launch their malicious code on the victim’s machine without any user intervention. |
| Active setup registry keys | | binary (true/false) | Active setup is a mechanism to trigger one or more actions to be run once per user early during login into Windows. More specifically, the Windows logon process compares the Active Setup area of the machine profile (HKLM) with that of the current  user profile (HKCU), and if the HKCU registry entries do not exist or match, then the specified program is run for the current user. The registry keys are of great interest for both malware writers as well as professional programmers, because they launch programs before startup registry entries are evaluated. |
| Services registry keys | | binary (true/false) | A Windows service is a program that runs in the background with minimal or no user interaction by either svchost.exe or by Windows directly launching the program. Recall that  svchost.exe, also known as Service Host, is a generic host process that acts as a launcher for DLLbased services. Services registry keys store information about Windows services and drivers, including where they are located and how they should be started. Many malware samples register themselves as a Windows  service to run automatically at Windows startup. This allows them to perform their malicious activities  without being detected |
| DLL injection registry keys | | binary (true/false) | DLL injection is the process of loading code into the address space of a running program through a DLL, making it possible to hook system APIs and implement alternate  functionality. There are some registry keys, such as AppInit DLLs, that can be used to implement usermode DLL injection in Windows. While only a small set of modern benign programs use these registry keys to load DLLs, a large majority of malware uses them for malicious purposes |
| Shell spawning registry keys | | binary (true/false) | Shell spawning refers to the procedure that spawns a child process to execute a command or series of commands. The shell spawning capability of the registry enables a specified program to be automatically launched whenever a file with a particular extension is opened. Malware writers often exploit this capability by adding certain registry entries. This allows them to launch their malicious code even  when other files are opened |
| Internet settings registry keys | | binary (true/false) | There are some registry entries, called Internet Settings, that store connection and proxy settings as well as cache configuration, allowed file types, security zones, and so on. Some malware samples tend to modify these entries to disable normal Internet access and to avoid being detected or removed. |
| BHO registry keys | | binary (true/false) | A browser helper object (BHO) is a module (often a DLL) designed as a plugin for either Windows Explorer or Internet Explorer to provide added functionality. Whenever a new instance of Windows Explorer or Internet Explorer is launched, it reads a specific registry key, namely Browser Helper Objects, to locate and then load BHOs whose CLSID  is stored there. Recall that a CLSID or Class Identifier is a globally unique identifier that identifies a COM  class object. Because BHOs have unrestricted access to the Internet Explorer event model, many instances of malware have also been created as BHOs that perform malicious activities such as gathering sensitive data and capturing login credentials. To prevent these malware  threats, the new browser of Microsoft, officially called Microsoft Edge, provides no support for BHOs. |
| f7 | DroppedFiles | number ( đếm số lượng ) | Số lượng file xóa bởi tiến trình |
| f8 | DebugStrings | number số lượng | enable debug logging |
| f9 | Files | number số lượng | số lượng file |
| f10 | Modules | number số lượng | Số lượng modun sử dụng |
| f11 | EventsCounters\_Network | number số lượng | số lần kết nối mạng của tiến trình |
| f12 | Scores\_Network | binary (true/false) | tiến trình có kết nối mạng hay không. |
| f13 | ip | 5 thuộc tính theo 5 loại | địa chỉ ip mà tiến trình kết nối tới. |
| unknown\_ip | | number ( đếm số lượng ) |  |
| Suspicious\_ip | | number ( đếm số lượng ) |  |
| Malicious\_ip | | number ( đếm số lượng ) |  |
| whitelist\_ip | | number ( đếm số lượng ) |  |
| unsafe\_ip | | number ( đếm số lượng ) |  |
| f14 | domain | 5 thuộc tính theo 5 loại | dns mà tiến trình liên kết đến |
| unknown\_domain | | number ( đếm số lượng ) |  |
| Suspicious\_domain | | number ( đếm số lượng ) |  |
| Malicious\_domain | | number ( đếm số lượng ) |  |
| whitelist\_domain | | number ( đếm số lượng ) |  |
| unsafe\_domain | | number ( đếm số lượng ) |  |
| f15 | http request | 5 thuộc tính theo 5 loại |  |
| unknown\_http\_request | | number ( đếm số lượng ) |  |
| Suspicious\_http\_request | | number ( đếm số lượng ) |  |
| Malicious\_http\_request | | number ( đếm số lượng ) |  |
| whitelist\_http\_request | | number ( đếm số lượng ) |  |
| unsafe\_http\_request | | number ( đếm số lượng ) |  |
| f16 | Priority | 3 mức ưu tiên |  |
| f17 | Autostart | binary (true/false) | Tiến trình có tự khởi động hay không. |
| f18 | LowAccess | binary (true/false) | Tiến trình có mức độ truy cập thấp hay không. |
| f19 | FileType | String -> **categorical** | Loại file |
| label | label | number 4 mức |  |

**F5: processtype:**

|  |  |
| --- | --- |
| ProcessType |  |
| Child process |  |
| Dropped from another process |  |
| Embedded COM++ |  |
| Injected |  |
| Main process |  |
| MSI Installer |  |
| Probably manual launch or APC inject |  |
| Runned from Explorer.exe |  |
| Suspicious |  |
| Was launched as a service |  |
| Was launched through Task Scheduler |  |
| WMI Requests |  |

**F13: IP:** ip address to search. this param can search IPs found during analyzing in sandbox.

* Whitelisting IP is a cybersecurity strategy under which a user can only take actions on their computer that an administrator has explicitly allowed in advance.

<https://www.csoonline.com/article/3562429/whitelisting-explained-how-it-works-and-where-it-fits-in-a-security-program.html>

Whitelisting IP addresses enables you to control who can (or cannot) access your WordPress website.

<https://www.malcare.com/blog/how-to-whitelist-an-ip-address/>

* Unknown IP refers to the IP address of the device that is discovered from seed routers, but cannot be accessed by using Telnet/SSH and SNMP.
* IP suspicious: Sending a lot of spam, being associated with a device that is swarmed with malware, being associated with adware, showing different behaviour patterns and such.
* IP blacklisting is a method used to filter out illegitimate or malicious IP addresses from accessing your networks. Blacklists are lists containing ranges of or individual IP addresses that you want to block.
* unsafe IP- IP addresses associated with phishing websites, sites infected with malware, or otherwise malicious sites, have a 'bad' reputation in the GTI database. So, they are blocked from connecting to your PC and show up as risky connections in your McAfee software.

**F14: domain:** domain name to search. this param can search domains found during analyzing in sandbox.

* A whitelist is a list of domains approved for authorized access to data.
* If the host is unknown, then it means that the primary domain name server is not registered for the given domain. Because the domain name server cannot be found, it is not possible to tell the IP address of the given hostname.
* Domain suspicious…
* is located on a network with a bad reputation
* is newly registered
* has network connections to bad domains (like nameservers, etc)
* is a cousin domain to some regular domain
* has a name pattern like snowshoers use
* has network connections to individuals with bad reputations
* has network connections to sources of bad traffic
* is sent through a MTA with bad behaviour (holding open idle connections, retrying too frequently, etc)
* malicious domains?
* Unsafe domains are external links to websites that could contain phishing, malware, or unwanted software. ... Unwanted software: The site might attempt to trick users into installing programs that harm user experience

**F15: http request**

* A whitelist: các req hợp lệ đc gửi đi
* unknown: The SecureSphere HTTP Module has detected an HTTP Request which does not match any existing request in the profile.
* suspicious…

<https://help.fortinet.com/fweb/582/Content/FortiWeb/fortiweb-admin/recognize_suspicious_requests.htm>

* malicious:
* Unsafe:

**F16: Priority:** Priority determines where a task ranks in order relative to all the other tasks that need to be completed. Priority is the measure you’ll use to assign what is most important to get done now and what might be able to wait until later. Priority has the assignments of High, Medium, and Low.

|  |  |
| --- | --- |
| 1. Low | Should be fixed if time permits but can be postponed.Should be fixed if time permits but can be postponed. |
| 1. Medium | A core functionality that your product is explicitly supposed to perform is compromised. |
| 1. High | An urgent problem that blocks the system use until the issue is resolved. |

**F19: File type:**

|  |  |
| --- | --- |
| FileType |  |
| ADB |  |
| BRW-CHR |  |
| BRW-FF |  |
| BRW-IE |  |
| BRW-OPR |  |
| FLS |  |
| INS-DRV |  |
| INS-MSI |  |
| JVA |  |
| NKN |  |
| OFS |  |
| OUTL |  |
| SCR-CMD |  |
| SCR-HTA |  |
| SCR-PSH |  |
| SCR-WS |  |
| WIN-SYS |  |
| WIN-TOL |  |
| WIN-XPR |  |
| KHOANG TRANG “ ” |  |

**Label**: nhãn cho từng tiến trình gồm 4 mức

|  |  |
| --- | --- |
| 0 - unknow |  |
| 1 - no threats |  |
| 2 - suspicious |  |
| 3 - malicious |  |

Nhóm thuộc tính

|  |  |  |
| --- | --- | --- |
| Nhóm | stt | Tên feature |
| **Process creation** | f1 | ProcessID |
| f2 | ParentPID |
| f3 | CommandLine |
| f4 | Image |
| f5 | ProcessType |
| f19 | FileType |
| **RegistryEvent (12,13,14)** | f6 | Registry |
| **File (id 23, 11)** | f7 | DroppedFiles |
| f9 | Files |
|  | f8 | DebugStrings |
|  | f10 | Modules |
| **Network connection** (id 22, 3) | f11 | EventsCounters\_Network |
| f12 | Scores\_Network |
| f13 | ip |
| f14 | domain |
| f15 | http request |
|  | f16 | Priority |
| f17 | Autostart |
| f18 | LowAccess |
|  | label | label |