



HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
Posts and Telecommunications Institute of Technology

PHÂN TÍCH MÃ ĐỘC

KHOA AN TOÀN THÔNG TIN

TS. ĐÌNH TRƯỜNG DUY



HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
Posts and Telecommunications Institute of Technology

PHÂN TÍCH MÃ ĐỘC

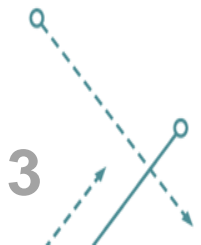
Một số lưu ý khi phân tích động

KHOA AN TOÀN THÔNG TIN
TS. ĐÌNH TRƯỜNG DUY

Giới thiệu

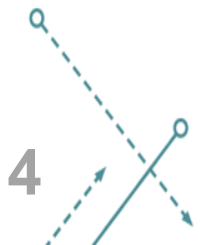
1. Qui trình thực hiện phân tích động

2. SYSINTERNALS TOOLS

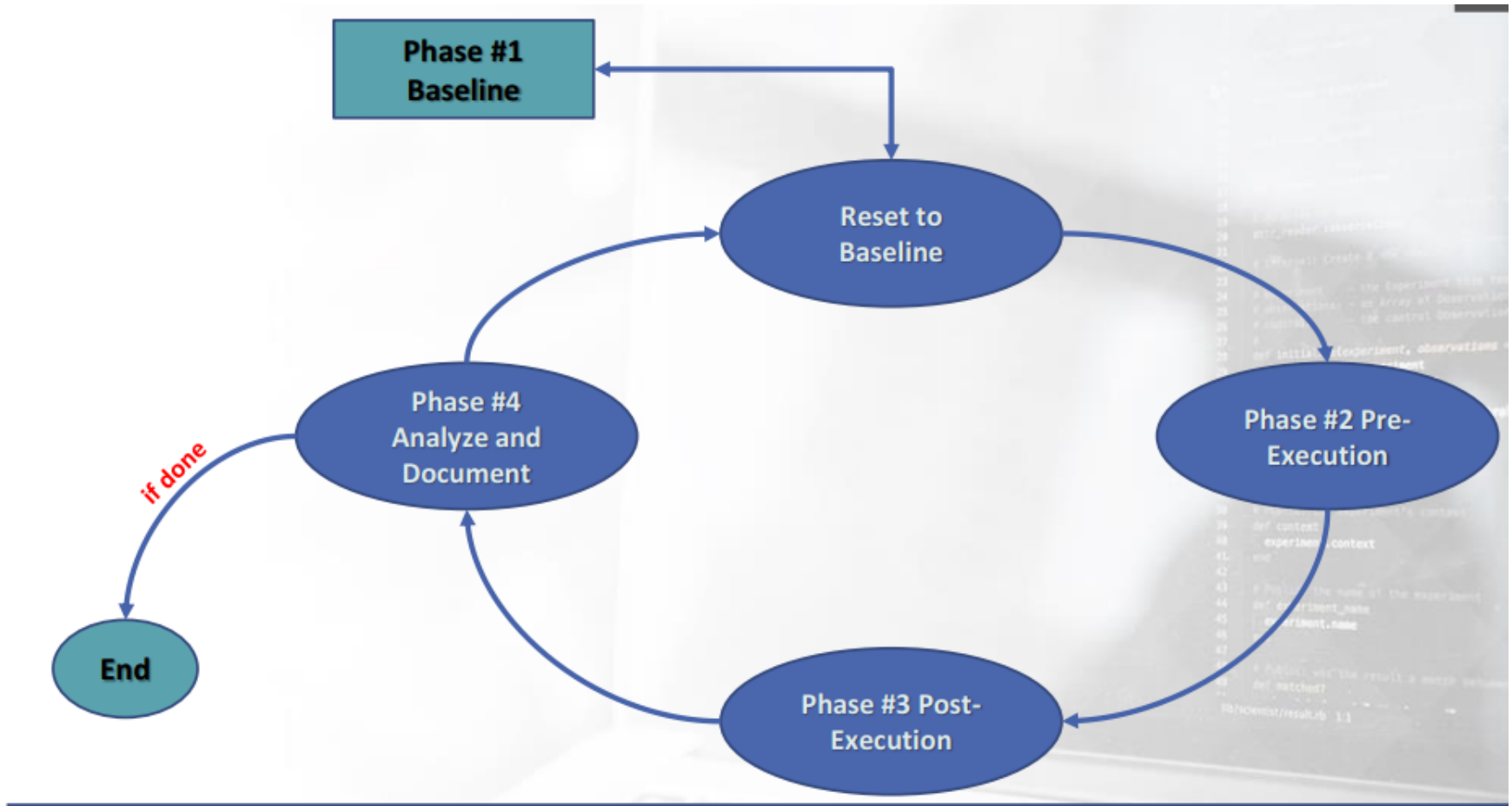


Quy trình thực hiện phân tích động

- Gồm 4 phase, mỗi giai đoạn lại có thể gồm nhiều bước khác nhau
 - **Phase 1: Baseline**
 - **Phase 2: Pre-Execution**
 - **Phase 3: Post-Execution**
 - **Phase 4: Analyze and Document**
- Thông thường phase 2, 3, 4 sẽ được lặp nhiều lần trước khi ra kết quả



Quy trình thực hiện phân tích động



Quy trình thực hiện phân tích động

- Tạo một máy ảo với hệ điều hành cần thiết.
 - Cài đặt tất cả các công cụ cần thiết.
 - Tạo một bản snapshot của máy ảo.
-
- ❖ Thực hiện bất kỳ cấu hình cụ thể nào nếu cần thiết.
 - ❖ Chuyển mẫu Malware vào máy ảo.
 - ❖ Khởi động các công cụ cần thiết (ví dụ: giám sát, theo dõi, gỡ lỗi, v.v.).



Quy trình thực hiện phân tích động

- Thực thi Malware.
 - Bắt đầu theo dõi và giám sát hành vi và hoạt động của nó.
 - Theo dõi cuộc gọi hệ thống.
 - Truy cập vào các tệp tin.
 - Ghi lưu lưu lượng mạng...
 - Ghi lại/Chụp ảnh màn hình, bộ nhớ, tệp cấu hình, tệp đăng ký, các tệp tin được giải nén, v.v.
-
- ❖ Phân tích và ghi chú về mọi thứ đã xảy ra.
 - ❖ Quan sát hành vi hiển thị.
 - ❖ Ghi lại sự kiện và hành động.



Quy trình thực hiện phân tích động

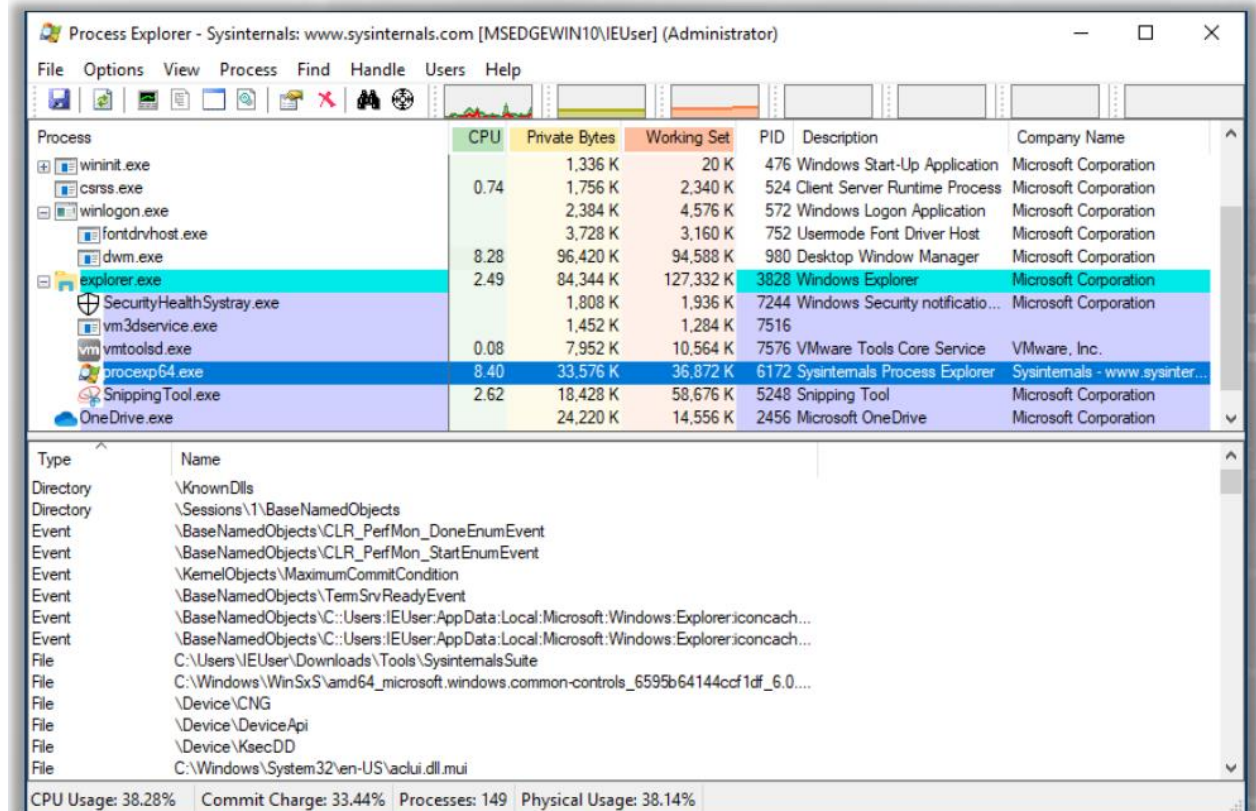
- Mã độc có thể sửa đổi thông tin registry để thay đổi hành vi hệ thống theo ý muốn của nó, và nó thực hiện điều này bằng cách sử dụng các API Win32.
- Những API thông thường nhất mà mã độc sử dụng là sửa đổi các giá trị registry được dùng để thực thi phần mềm trong quá trình khởi động hệ thống hoặc đăng nhập người dùng.
- Mã độc sửa đổi các giá trị này để hệ thống tự động khởi động mã độc trong quá trình khởi động hệ thống.
- Các kỹ thuật này được gọi là cơ chế duy trì tính bền vững (persistence mechanisms) trong Windows.
- Nếu hệ điều hành được cài đặt trên một máy ảo để phân tích mã độc, các dấu vết của máy ảo sẽ có trong registry.
- Mã độc có thể truy vấn các khóa registry này và tìm hiểu xem hệ điều hành mục tiêu của nạn nhân có được cài đặt trên máy ảo hay không.
- Trong trường hợp này, mã độc có thể không thể hiện hành vi thực sự của nó và có thể đánh lừa người phân tích.

SYSINTERNALS TOOLS

- Process

Explorer giúp theo dõi các DLL và handle được mở bởi một tiến trình.

Process Handles



Process Explorer - Sysinternals: www.sysinternals.com [MSEdgeWin10\IEUser] (Administrator)

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
wininit.exe		1,336 K	20 K	476	Windows Start-Up Application	Microsoft Corporation
csrss.exe	0.74	1,756 K	2,340 K	524	Client Server Runtime Process	Microsoft Corporation
winlogon.exe		2,384 K	4,576 K	572	Windows Logon Application	Microsoft Corporation
fontdrvhost.exe		3,728 K	3,160 K	752	Usermode Font Driver Host	Microsoft Corporation
dwm.exe	8.28	96,420 K	94,588 K	980	Desktop Window Manager	Microsoft Corporation
explorer.exe	2.49	84,344 K	127,332 K	3828	Windows Explorer	Microsoft Corporation
SecurityHealthSystray.exe		1,808 K	1,936 K	7244	Windows Security notificatio...	Microsoft Corporation
vm3dservice.exe		1,452 K	1,284 K	7516		
vmtoolsd.exe	0.08	7,952 K	10,564 K	7576	VMware Tools Core Service	VMware, Inc.
procexp64.exe	8.40	33,576 K	36,872 K	6172	Sysinternals Process Explorer	Sysinternals - www.sysinter...
SnippingTool.exe	2.62	18,428 K	58,676 K	5248	Snipping Tool	Microsoft Corporation
OneDrive.exe		24,220 K	14,556 K	2456	Microsoft OneDrive	Microsoft Corporation

Type	Name
Directory	\KnownDlls
Directory	\Sessions\1\BaseNamedObjects
Event	\BaseNamedObjects\CLR_PerfMon_DoneEnumEvent
Event	\BaseNamedObjects\CLR_PerfMon_StartEnumEvent
Event	\KernelObjects\MaximumCommitCondition
Event	\BaseNamedObjects\TermSrvReadyEvent
Event	\BaseNamedObjects\VC::Users\IEUser\AppData\Local\Microsoft\Windows\Explorer\iconcach...
Event	\BaseNamedObjects\VC::Users\IEUser\AppData\Local\Microsoft\Windows\Explorer\iconcach...
File	C:\Users\IEUser\Downloads\Tools\SysinternalsSuite
File	C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0....
File	\Device\NCG
File	\Device\DeviceApi
File	\Device\KsecDD
File	C:\Windows\System32\en-US\aclui.dll.mui

CPU Usage: 38.28% | Commit Charge: 33.44% | Processes: 149 | Physical Usage: 38.14%

SYSINTERNALS TOOLS

- Process

Explorer giúp theo dõi các DLL và handle được mở bởi một tiến trình.

DLLs Loaded by a Process

Process Explorer - Sysinternals: www.sysinternals.com [MSEDGEWIN10\IEUser] (Administrator)

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
wininit.exe		1,336 K	20 K	476	Windows Start-Up Application	Microsoft Corporation
csrss.exe	0.59	1,756 K	2,332 K	524	Client Server Runtime Process	Microsoft Corporation
winlogon.exe		2,384 K	4,576 K	572	Windows Logon Application	Microsoft Corporation
fontdrvhost.exe		3,728 K	3,168 K	752	Usemode Font Driver Host	Microsoft Corporation
dwm.exe	7.34	96,568 K	94,616 K	980	Desktop Window Manager	Microsoft Corporation
explorer.exe	4.28	85,876 K	128,032 K	3828	Windows Explorer	Microsoft Corporation
SecurityHealthSystray.exe		1,808 K	1,936 K	7244	Windows Security notificatio...	Microsoft Corporation
vm3dservice.exe		1,452 K	1,284 K	7516		
vmtoolsd.exe	0.08	7,952 K	10,564 K	7576	VMware Tools Core Service	VMware, Inc.
procexp64.exe	3.42	33,596 K	38,292 K	6172	Sysinternals Process Explorer	Sysinternals - www.sysinter...
SnippingTool.exe	4.15	19,084 K	58,340 K	5248	Snipping Tool	Microsoft Corporation
OneDrive.exe	< 0.01	24,220 K	14,556 K	2456	Microsoft OneDrive	Microsoft Corporation

Name	Description	Company Name	Path
advapi32.dll.mui	Advanced Windows 32 Base API	Microsoft Corporation	C:\Windows\System32\en-US\advapi32.dll.mui
apphelp.dll	Application Compatibility Client Libr...	Microsoft Corporation	C:\Windows\System32\apphelp.dll
apphelp.dll.mui	Application Compatibility Client Libr...	Microsoft Corporation	C:\Windows\System32\en-US\apphelp.dll.mui
bcrypt.dll	Windows Cryptographic Primitives ...	Microsoft Corporation	C:\Windows\System32\bcrypt.dll
bcrypt.dll.mui	Windows Cryptographic Primitives ...	Microsoft Corporation	C:\Windows\System32\en-US\bcrypt.dll.mui
bcryptprimitives.dll	Windows Cryptographic Primitives ...	Microsoft Corporation	C:\Windows\System32\bcryptprimitives.dll
cfgmgr32.dll	Configuration Manager DLL	Microsoft Corporation	C:\Windows\System32\cfgmgr32.dll
clbcatq.dll	COM+ Configuration Catalog	Microsoft Corporation	C:\Windows\System32\clbcatq.dll
combase.dll	Microsoft COM for Windows	Microsoft Corporation	C:\Windows\System32\combase.dll
combase.dll.mui	Microsoft COM for Windows	Microsoft Corporation	C:\Windows\System32\en-US\combase.dll.mui
comctl32.dll	User Experience Controls Library	Microsoft Corporation	C:\Windows\WinSxS\amd64_microsoft.windows.common-c...
comctl32.dll.mui	User Experience Controls Library	Microsoft Corporation	C:\Windows\WinSxS\amd64_microsoft.windows.c...control...
comdlg32.dll	Common Dialogs DLL	Microsoft Corporation	C:\Windows\System32\comdlg32.dll
comdlg32.dll.mui	Common Dialogs DLL	Microsoft Corporation	C:\Windows\SysWOW64\en-US\comdlg32.dll.mui

CPU Usage: 26.73% Commit Charge: 33.29% Processes: 147 Physical Usage: 37.86%

SYSINTERNALS TOOLS

- **Listdlls/Listdlls64** giúp hiển thị các DLL được tải vào một tiến trình

```

Administrator: Command Prompt
C:\Users\Client2>C:\Users\Client2\Desktop\3.SysinternalsSuite>Listdlls64.exe procexp64.exe

Listdlls v3.2 - Listdlls
Copyright (C) 1997-2016 Mark Russinovich
Sysinternals

-----
procexp64.exe pid: 2496
Command line: "C:\Users\Client2\Desktop\3.SysinternalsSuite\procexp64.exe"

Base                Size                Path
0x0000000040000000  0x190000  C:\Users\Client2\Desktop\3.SysinternalsSuite\procexp64.exe
0x0000000078e50000  0x19f000  C:\Windows\SYSTEM32\ntdll.dll
0x0000000078d20000  0x11f000  C:\Windows\system32\kernel32.dll
0x0000000038880000  0x6a000   C:\Windows\system32\KERNELBASE.dll
0x0000000074180000  0x71000   C:\Windows\system32\SHLWAPI.dll
0x000000007fd70000  0x67000   C:\Windows\system32\GDI32.dll
0x0000000078c20000  0xfa000   C:\Windows\system32\USER32.dll
0x0000000070410000  0xe000    C:\Windows\system32\LPK.dll
0x00000000760c0000  0xcb000   C:\Windows\system32\USP10.dll
0x00000000756a0000  0x9f000   C:\Windows\system32\msvcrt.dll
0x0000000071890000  0x27000   C:\Windows\system32\IPHLPAPI.DLL
0x0000000070310000  0x8000    C:\Windows\system32\NSI.dll
0x00000000700a0000  0xb000    C:\Windows\system32\WINNSI.DLL
0x000000007fde0000  0x12c000  C:\Windows\system32\RPCRT4.dll
  
```

SYSINTERNALS TOOLS

- **Handle/ Handle64** là các tham chiếu đến các đối tượng trong không gian kernel mà tiến trình có thể truy cập. Có thể liệt kê các handle của một tiến trình bằng cách sử dụng Process Explorer, nhưng cũng có một công cụ khác từ Sysinternals có tên là "**handles**".

```
Administrator: Command Prompt

C:\Users\Client2>C:\Users\Client2\Desktop\3.SysinternalsSuite\handle64.exe /?

Nthandle v4.22 - Handle viewer
Copyright (C) 1997-2019 Mark Russinovich
Sysinternals - www.sysinternals.com

usage: handle [[-a [-l]] [-u] | [-c <handle> [-y]] | [-s]] [-p <process>|<pid>] [name] [-nobanner]
-a          Dump all handle information.
-l          Just show pagefile-backed section handles.
-c          Closes the specified handle (interpreted as a hexadecimal number).
            You must specify the process by its PID.
            WARNING: Closing handles can cause application or system instability.
-y          Don't prompt for close handle confirmation.
-s          Print count of each type of handle open.
-u          Show the owning user name when searching for handles.
-p          Dump handles belonging to process (partial name accepted).
name        Search for handles to objects with <name> (fragment accepted).
-nobanner   Do not display the startup banner and copyright message.

No arguments will dump all file references.

C:\Users\Client2>C:\Users\Client2\Desktop\3.SysinternalsSuite\handle64.exe -p 2496

Nthandle v4.22 - Handle viewer
Copyright (C) 1997-2019 Mark Russinovich
```

SYSINTERNALS TOOLS: Procmon

- **Procmon/ Procmon64** là một công cụ giám sát nâng cao các tiến trình, cung cấp thông tin về các hoạt động và/hoặc sự kiện được thực hiện bởi các tiến trình trên tệp tin, tiến trình/luồng, registry và hoạt động mạng trong thời gian thực.
- **Procexp** chỉ cho thấy một tiến trình có một handle mở tới một tệp tin cụ thể, trong khi **Procmon** sẽ cho thấy các hoạt động cấp thấp được thực hiện bởi tiến trình đó trên tệp tin đó.

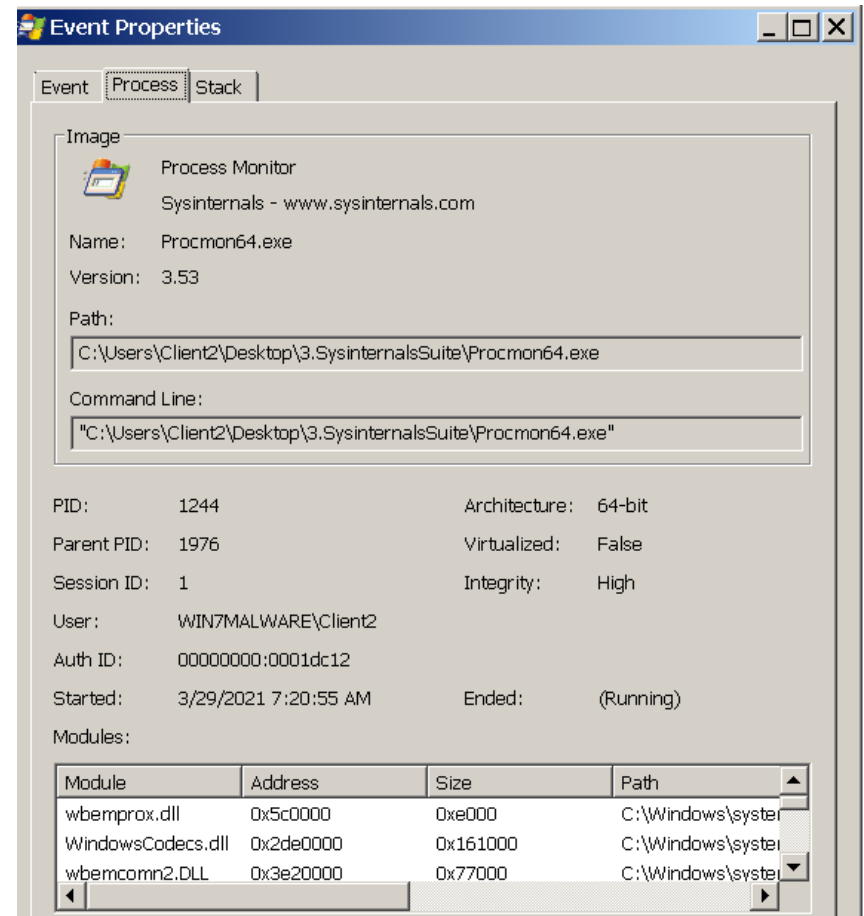
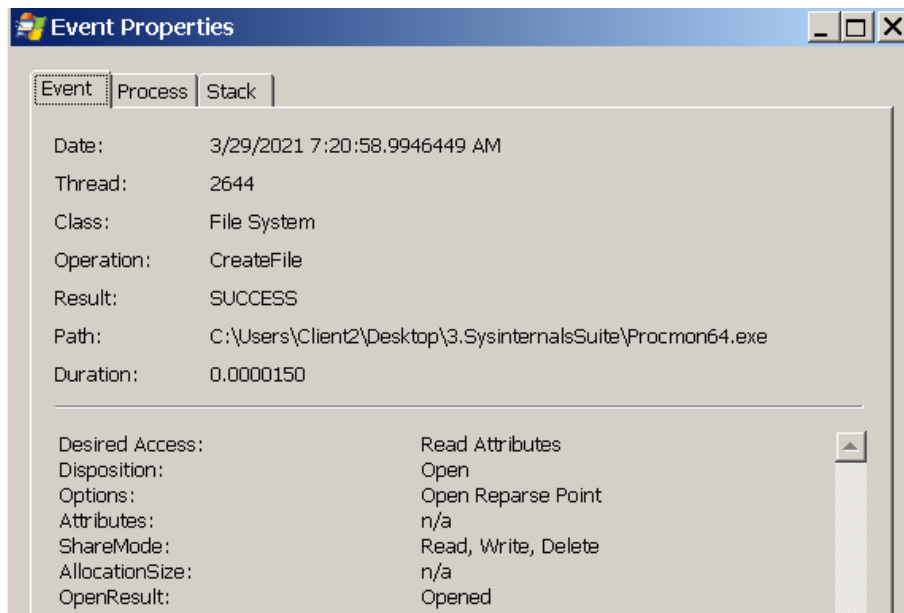


SYSINTERNALS TOOLS: Procmon

Process Monitor - Sysinternals: www.sysinternals.com							
File Edit Event Filter Tools Options Help							
Time of D...	Process Name	PID	TID	Operation	Path	Result	Detail
7:20:58.856...	Procmon64.exe	1244	940	CreateFile	C:\Windows\System32\api-ms-win-appm...	NAME NOT FOUND	Desired Access: R...
7:20:58.857...	Procmon64.exe	1244	940	CreateFile	C:\Windows\System32\ext-ms-win-kernel...	NAME NOT FOUND	Desired Access: R...
7:20:58.858...	Procmon64.exe	1244	940	RegQueryValue	HKLM\HARDWARE\DESCRIPTION\Sy...	SUCCESS	Type: REG_DWO...
7:20:58.858...	Procmon64.exe	1244	940	RegQueryValue	HKLM\System\CurrentControlSet\Control...	SUCCESS	Type: REG_DWO...
7:20:58.859...	Procmon64.exe	1244	940	RegQueryValue	HKLM\System\CurrentControlSet\Control...	SUCCESS	Type: REG_SZ, Le...
7:20:58.859...	Procmon64.exe	1244	940	RegQueryValue	HKLM\System\CurrentControlSet\Control...	SUCCESS	Type: REG_DWO...
7:20:58.859...	Procmon64.exe	1244	940	RegQueryValue	HKLM\System\CurrentControlSet\Control...	SUCCESS	Type: REG_BINAR...
7:20:58.859...	Procmon64.exe	1244	940	RegQueryValue	HKLM\System\CurrentControlSet\Control...	SUCCESS	Type: REG_SZ, Le...
7:20:58.859...	Procmon64.exe	1244	940	RegQueryValue	HKLM\System\CurrentControlSet\Control...	SUCCESS	Type: REG_DWO...
7:20:58.859...	Procmon64.exe	1244	940	RegQueryValue	HKLM\System\CurrentControlSet\Control...	SUCCESS	Type: REG_BINAR...
7:20:58.859...	Procmon64.exe	1244	940	RegQueryValue	HKLM\HARDWARE\DESCRIPTION\Sy...	SUCCESS	Type: REG_DWO...
7:20:58.859...	Procmon64.exe	1244	940	RegQueryValue	HKLM\System\CurrentControlSet\Control...	SUCCESS	Type: REG_DWO...
7:20:58.859...	Procmon64.exe	1244	940	RegQueryValue	HKLM\System\CurrentControlSet\Control...	SUCCESS	Type: REG_SZ, Le...
7:20:58.859...	Procmon64.exe	1244	940	RegQueryValue	HKLM\System\CurrentControlSet\Control...	SUCCESS	Type: REG_DWO...
7:20:58.859...	Procmon64.exe	1244	940	RegQueryValue	HKLM\System\CurrentControlSet\Control...	SUCCESS	Type: REG_BINAR...
7:20:58.859...	Procmon64.exe	1244	940	RegQueryValue	HKLM\System\CurrentControlSet\Control...	SUCCESS	Type: REG_SZ, Le...
7:20:58.859...	Procmon64.exe	1244	940	RegQueryValue	HKLM\System\CurrentControlSet\Control...	SUCCESS	Type: REG_DWO...
7:20:58.859...	Procmon64.exe	1244	940	RegQueryValue	HKLM\System\CurrentControlSet\Control...	SUCCESS	Type: REG_BINAR...
7:20:58.860...	Procmon64.exe	1244	940	RegQueryValue	HKLM\HARDWARE\DESCRIPTION\Sy...	SUCCESS	Type: REG_DWO...
7:20:58.981...	Procmon64.exe	1244	940	RegSetInfoKey	HKLM\SOFTWARE\Microsoft\COM3	SUCCESS	KeySetInformation...
7:20:58.981...	Procmon64.exe	1244	940	RegQueryValue	HKLM\SOFTWARE\Microsoft\COM3\Co...	SUCCESS	Type: REG_DWO...
7:20:58.982...	Procmon64.exe	1244	940	CreateFile	C:\Windows\Registration\R00000000000...	SUCCESS	Desired Access: G...
7:20:58.983...	Procmon64.exe	1244	940	RegSetInfoKey	HKCR\Wow6432Node\CLSID\{4590F811...	SUCCESS	KeySetInformation...
7:20:58.987...	Procmon64.exe	1244	940	CreateFile	C:\Windows\System32\wbemcomn2.dll	SUCCESS	Desired Access: R...
7:20:58.987...	Procmon64.exe	1244	940	CreateFile	C:\Windows\System32\wbemcomn2.dll	SUCCESS	Desired Access: R...

SYSINTERNALS TOOLS

- Right-click vào bất cứ dòng vào và chọn Properties để xem được Event Properties



SYSINTERNALS TOOLS: Procmon

- Process Monitor cung cấp năm công cụ chính cho việc phân tích:



- Hoạt động Registry (Registry Activity): Bao gồm các sự kiện được thực hiện trên registry, chẳng hạn như tạo, liệt kê, truy vấn và xóa các khóa và giá trị (RegCreateKey, RegEnumKey, RegSetValue, RegDeleteValue, RegQueryValue, RegCloseKey, RegOpenKey).

SYSINTERNALS TOOLS: Procmon

- Hoạt động Hệ thống tệp tin (File System Activity): Bao gồm các hoạt động trên hệ thống tệp tin và thiết bị cục bộ và từ xa, chẳng hạn như mở tệp tin, đóng tệp tin, liệt kê thư mục, ghi tệp tin, truy vấn kích thước tệp tin, thời điểm dấu thời gian của tệp tin hoặc thư mục ...
- Sự kiện Phân tích (Profiling Events): Tạo nhật ký cho sự kiện của mỗi tiến trình và luồng trên hệ thống, chẳng hạn như thời gian xử lý của bộ xử lý và bộ nhớ lưu trữ được sử dụng.

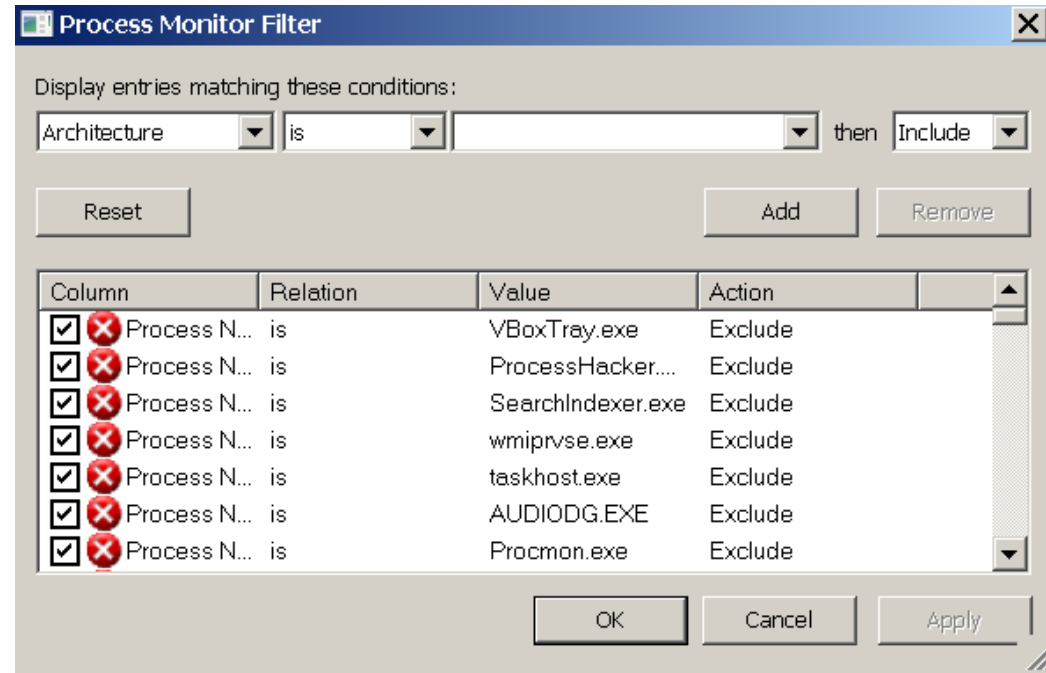


SYSINTERNALS TOOLS: Procmon

- Hoạt động Mạng (network Activity): Bao gồm địa chỉ nguồn và đích của tất cả hoạt động mạng UDP và TCP. Bạn có thể cấu hình ProcMon để giải quyết tên mạng từ địa chỉ mạng hoặc chỉ hiển thị địa chỉ IP. Để hiển thị tên mạng đã giải quyết, chọn "Hiển thị Địa chỉ Mạng đã Giải quyết" từ menu Tùy chọn.
- Hoạt động Tiến trình và Luồng (Process and Thread Activity): Bao gồm các sự kiện như việc tạo, khởi động hoặc hủy bỏ một tiến trình, việc tạo hoặc hủy bỏ một luồng, một chương trình tải một DLL, các hình ảnh thực thi và tệp tin dữ liệu được tải vào không gian địa chỉ của một tiến trình.

SYSINTERNALS TOOLS: Procmon

- Chúng ta có thể thực hiện việc lọc cụ thể hơn bằng cách sử dụng menu Filter hoặc cái phễu màu xanh dương trên cửa sổ chính của Procmon. Chọn bất kỳ cách nào sẽ dẫn đến cửa sổ (hiển thị bên phải).
- Có thể áp dụng bộ lọc dựa trên CommandLine, PID, Image Path, Process Name, User...

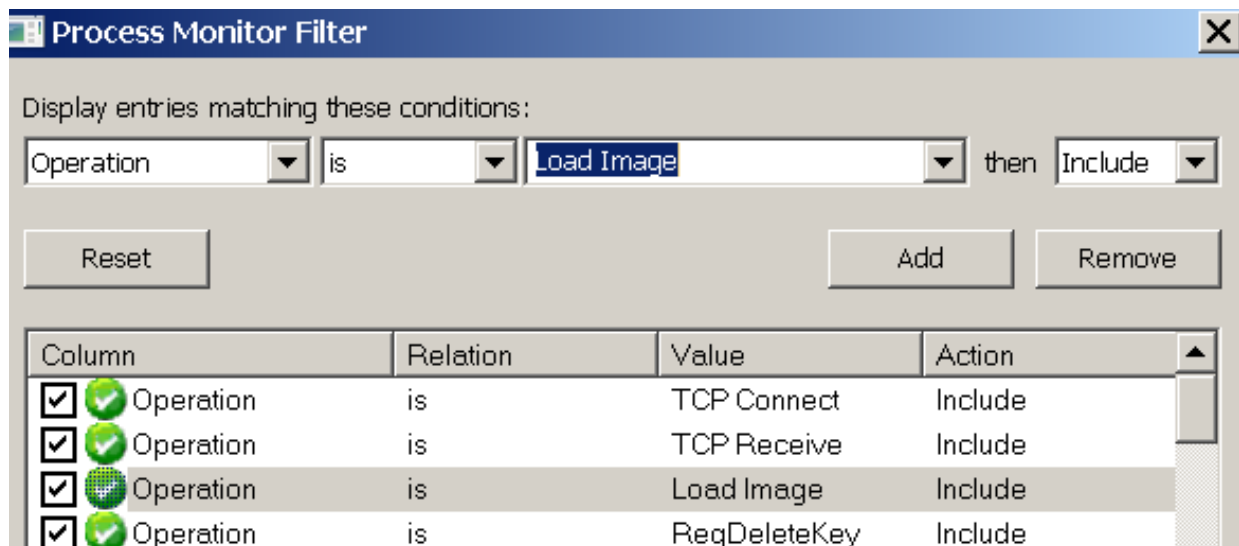


SYSINTERNALS TOOLS: Procmon

- Procmon Operation filters rất hữu dụng cho phân tích mã độc vì:
 - ✓ Có thể gửi và nhận cho cả giao thức TCP và UDP: có thể bắt được tất cả các kết nối có thể được sử dụng bởi mã độc trong khi nó chạy.

7:21:01.946...	svchost.exe	780	0	UDP Receive	192.168.1.160:68 -> 192.168.1.254:67	SUCCESS
7:21:01.967...	svchost.exe	672	0	UDP Send	192.168.1.160:50247 -> 192.168.1.2:53	SUCCESS
7:21:01.977...	svchost.exe	672	0	UDP Receive	#02:0:0:0:0:1:3:5355 -> fe80:0:0:0:3128:14...	SUCCESS
7:21:01.977...	svchost.exe	672	0	UDP Receive	224.0.0.252:5355 -> 192.168.1.1:50603	SUCCESS
7:21:02.205...	svchost.exe	672	0	UDP Send	192.168.1.160:61912 -> 192.168.1.2:53	SUCCESS

- ✓ Xem được các DLL và Executables mà mã độc cố gắng tải



SYSINTERNALS TOOLS: Procmon

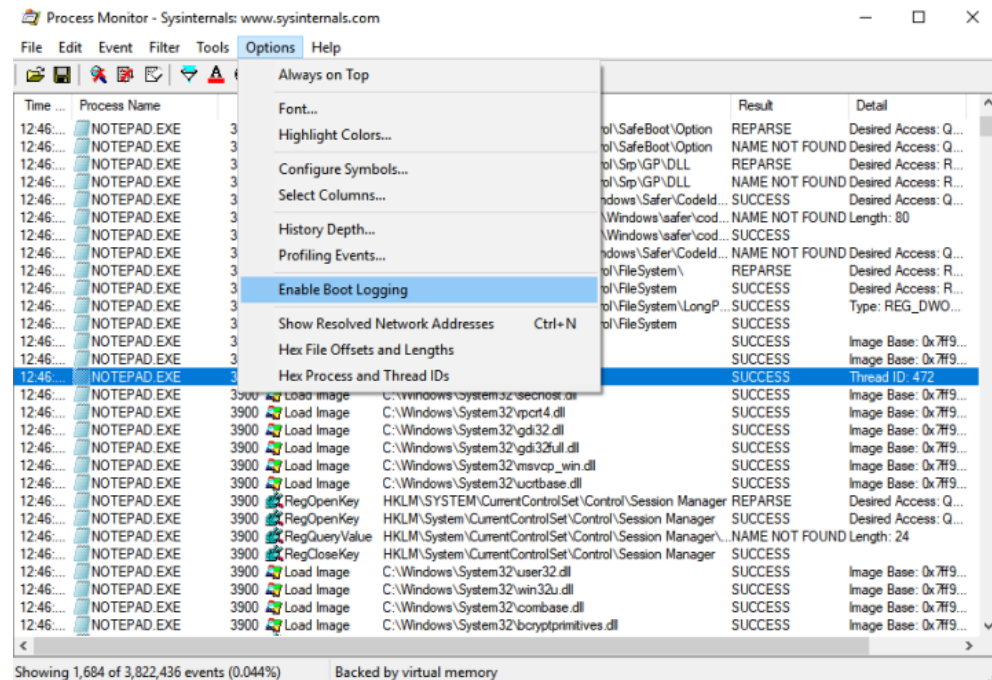
- Procmon Operation filters rất hữu dụng cho phân tích mã độc vì:
 - ✓ **Create File:** có thể bắt được các sự kiện tạo tệp của mã độc. Chú ý không phải tất cả các lệnh CreateFile đều chỉ tạo files/directories. Nó có thể sử dụng để đọc, viết, di chuyển và thậm chí xóa file.
 - ✓ **Registry activities:** những dạng hoạt động của mã độc như để duy trì tính bền vững trên máy sau khi khởi động lại, phần mềm độc hại có thể tạo ra các khóa registry.
 - ✓ **Process Create, Process Start, and Thread Create:** bao gồm việc tạo, bắt đầu các tiến trình và các luồng trong quá trình thực thi.



SYSINTERNALS TOOLS: Procmon

Procmon Tricks:

1. Boot Logging: Procmon có thể được cấu hình để bắt đầu ghi lại hoạt động hệ thống ở một giai đoạn sớm trong quá trình khởi động. Đối với phân tích phần mềm độc hại, điều này giúp theo dõi các sự kiện xảy ra trước, trong quá trình hoặc trong trường hợp không có đăng nhập người dùng, chẳng hạn như các trình điều khiển thiết bị buộc khởi động, chuỗi đăng nhập, các dịch vụ tự động khởi động hoặc khởi tạo shell.



SYSINTERNALS TOOLS: Procmon

Procmon Tricks:

2. Drop Filtered Events: Tùy chọn này trong menu Filter sẽ giảm số lượng nhật ký được ghi lại bởi Procmon. Chỉ sử dụng tùy chọn này khi bạn chắc chắn về những gì bạn cần. Vì bất kỳ sự kiện nào không đáp ứng bộ lọc đã chỉ định sẽ không bao giờ được ghi lại và không thể khôi phục sau này

3. History Depth

Procmon theo dõi việc sử dụng bộ nhớ và sẽ ngừng ghi lại các sự kiện nếu bộ nhớ ảo của hệ thống cạn kiệt. Bạn có thể điều khiển số lượng mục được lưu giữ bằng cách chọn hộp thoại "History Depth" từ menu Tùy chọn.

4. Backing Files

Để tiếp tục ghi lại sự kiện của Procmon trong trường hợp hết bộ nhớ ảo, chúng ta có thể cấu hình nó để lưu các sự kiện đã ghi lại vào một tệp tin cụ thể trên đĩa bằng cách chọn "Backing Files" từ menu File.

