

# Basic Dynamic Malware Analysis

For today, we're going to use **Procmon**.

Process Monitor, or "Procmon", is an advanced tool for Windows that allows **monitoring of active processes and threads**, network activity, file access, and system calls made on an operating system. It is widely used to monitor potential processes or activities created by malware running on a system.

First of all, we will setup the VM in order to **protect us from the malware** and we'll do that by disabling:

- Any network connectivity
- Any USB connectivity
- Any file sharing between host and VM
- Any drag and drop or share clipboard features

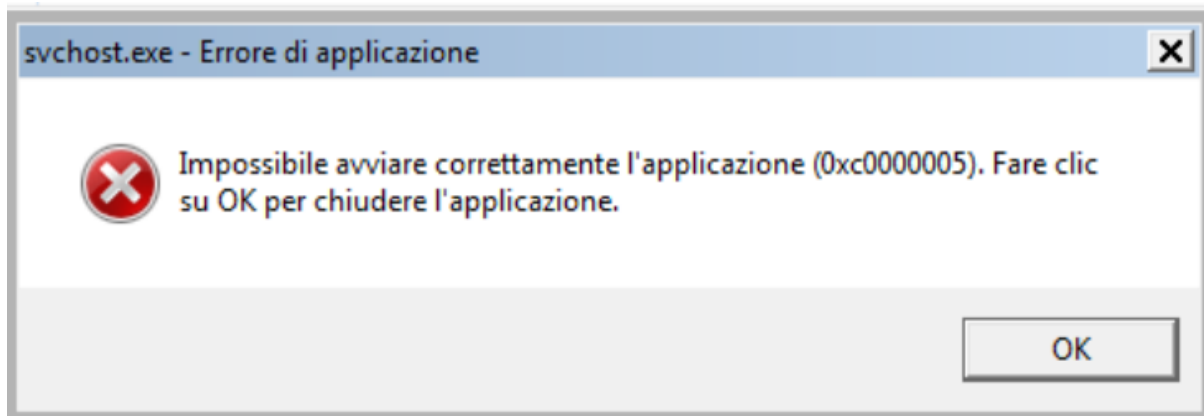
After all of that, we open up our Win7 VM and start Procmon.

Process Monitor - Sysinternals: www.sysinternals.com						
File Edit Event Filter Tools Options Help						
Time ...	Process Name	PID	Operation	Path	Result	Detail
16:27:...	Explorer.EXE	1320	RegCloseKey	HKCR\TypeLib\{EAB22AC0-30C1-11CF...	SUCCESS	
16:27:...	Explorer.EXE	1320	RegCloseKey	HKCR\TypeLib\{EAB22AC0-30C1-11CF...	SUCCESS	
16:27:...	Explorer.EXE	1320	CloseFile	C:\Windows\System32\ieframe.dll	SUCCESS	
16:27:...	services.exe	492	Thread Create		SUCCESS	Thread ID: 1868
16:27:...	svchost.exe	300	Thread Create		SUCCESS	Thread ID: 784
16:27:...	svchost.exe	1168	Thread Create		SUCCESS	Thread ID: 324
16:27:...	lsass.exe	500	RegOpenKey	HKLM\SAM\SAM\DOMAINS\Account\...	NAME NOT FOUND	Desired Access: R...
16:27:...	lsass.exe	500	RegOpenKey	HKLM\SAM\SAM\DOMAINS\Account\...	NAME NOT FOUND	Desired Access: R...
16:27:...	lsass.exe	500	RegOpenKey	HKLM\SAM\SAM\DOMAINS\Account\...	SUCCESS	Desired Access: R...
16:27:...	lsass.exe	500	RegQueryValue	HKLM\SAM\SAM\DOMAINS\Account\...	SUCCESS	Type: REG_BINA...
16:27:...	lsass.exe	500	RegCloseKey	HKLM\SAM\SAM\DOMAINS\Account\...	SUCCESS	
16:27:...	lsass.exe	500	RegOpenKey	HKLM\SAM\SAM\DOMAINS\Account\...	NAME NOT FOUND	Desired Access: R...
16:27:...	lsass.exe	500	RegOpenKey	HKLM\SAM\SAM\DOMAINS\Account\...	NAME NOT FOUND	Desired Access: R...
16:27:...	lsass.exe	500	RegOpenKey	HKLM\SAM\SAM\DOMAINS\Account\...	SUCCESS	Desired Access: R...
16:27:...	lsass.exe	500	RegQueryValue	HKLM\SAM\SAM\DOMAINS\Account\...	SUCCESS	Type: REG_BINA...
16:27:...	lsass.exe	500	RegCloseKey	HKLM\SAM\SAM\DOMAINS\Account\...	SUCCESS	
16:27:...	VBoxTray.exe	340	Thread Create		SUCCESS	Thread ID: 1212
16:27:...	VBoxTray.exe	340	Thread Exit		SUCCESS	Thread ID: 1212, ...
16:27:...	Explorer.EXE	1320	ReadFile	C:\Windows\explorer.exe	SUCCESS	Offset: 529.920, Le...
16:27:...	Explorer.EXE	1320	ReadFile	C:\Windows\explorer.exe	SUCCESS	Offset: 529.920, Le...
16:27:...	taskeng.exe	308	Thread Exit		SUCCESS	Thread ID: 2792, ...
16:27:...	svchost.exe	912	Thread Exit		SUCCESS	Thread ID: 2232, ...

Showing 238.991 of 357.412 events (66%)      Backed by virtual memory

As we can see, Procmon is registering any current process running in the system, their PID, file access and system calls.

Then we start the [Malware\\_U3\\_W2\\_L2](#) file but we get the following error message.



This message pops up because the malware targets outdated libraries that were present in Windows XP but patched in Windows 7. This shows us **how important it is to always update and patch the systems** in order to fight and prevent exploitation from malicious software and malicious attackers.

**Federico Biggi**