Basic Dynamic Malware Analysis

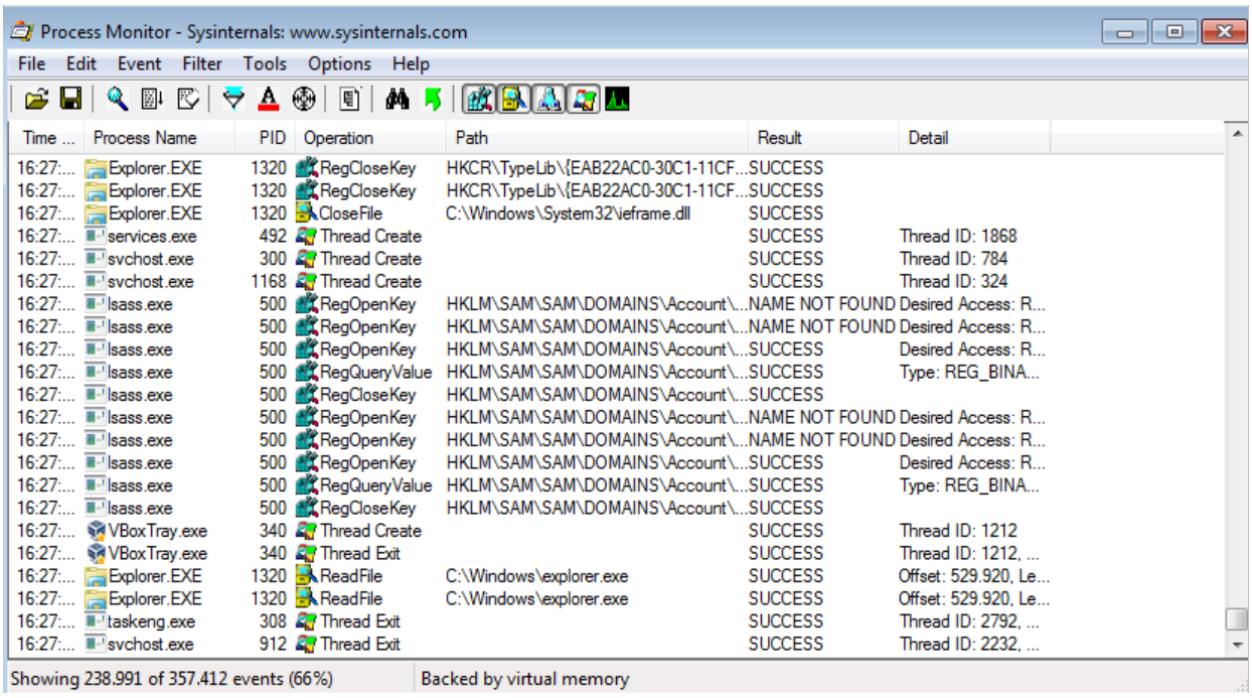
For today, we’re going to use **Procmon.**

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:

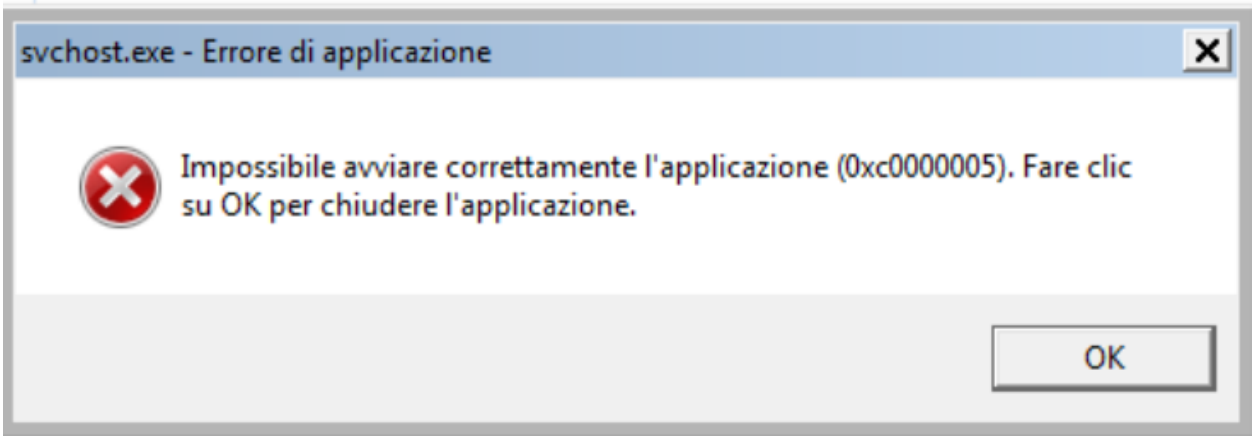
- Any network connectivity
- Any USB connectivity
- Any file sharing between host and VM
- Any drag and drop or share clipboard features

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



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This message pops up because the malware targets outdated libraries that were present in Windows XP but patched in Windows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.