

3 December 2007

By: Ionut Ilascu, Editor, Software Reviews



ESET SysInspector

[Inside Look Into Your System](#)

See all that's running on your system

ESET is a great name in the world of computers, especially when it comes to protecting your machine against malware. From the first protection solution introduced on the market, they managed to attract the attention of many users due to low prices, increased detection and elimination rates, fast scans and low computer resources required. NOD32 is known all over the world for the good job it does and now its heftier brother, [Smart Security](#), is winning the world over. It is a complete solution for closing all doors for Internet nasty critters as it brings very good spam filtering, firewall, advanced heuristics and NOD32's smooth engine. A third product is on its way to get on the market and, judging by the way it feels and moves, I can't say it'll be adopted on installed applications list too soon. Unlike its predecessors, SysInspector is not an active tool but a monitor of the system. Its purpose consists in analyzing your computer and retrieving important intelligence on the running processes, registry entries or startup programs and network connections. It permits viewing all the details and, more than this, it'll analyze the threat level providing clues on the dangers lurking inside. SysInspector comes in handy when you want to investigate suspicious system behavior. All information is displayed in four sections of the interface reporting on the results of the initial scan of the computer. SysInspector does not need to be installed and a simple launch of the executable will suffice to get the program going. After a not too long period of time (on XP it took about 14" to load) the application will complete the analysis of your computer and will be ready to present all data gathered. The interface is nice and simple and there are no hidden settings. Once the inspection is over, you can navigate through all sections of the interface in search for the desired details. Program Controls section supplies the necessary means for saving the results into an XML log file for later investigation of the results, filtering the items (all details are included on a risk scale going from 1 to 9) or searching a particular item. SysInspector organizes gathered information into expandable nodes which are in fact the basic and most important sections of your computer: running processes, network connections, important registry entries, critical files, system information and file details. Each section is expandable in order to provide a more in-depth view. Users can have a detailed look at the running processes (all of them are displayed) and their modules. Description Window in the right shows a brief description of the module/process as well as the developing company while in the lower part you have more details (Details Window) presenting all the processes it is linked to. Regarding the risk level of an item, it can be easily identified by simply comparing its color with the one in Risk Level slider. The downside is that there will be a bunch of unknown applications (like Foobar or some Thunderbird or Total Commander modules) or even false positives (Feedreader is one of them) which need to be corrected; and you cannot make any change except for the items displayed. You cannot add a process and all its modules to a safe zone, so that at the next inspections SysInspector does not render them as unknown or risky. Network Connections node comprises all running TCP, UDP and DNS servers. SysInspector displays all current connections but you will not benefit from a refresh so it is kind of uncomfortable as you will not have an accurate view on the processes performing outbound/inbound connections. The same color coding is available here as well. Important Registry Entries section contains registry items that are usually prone to causing problems. It features entries related to autostart, BHOs (Browser Helper Objects), Internet related, Shell Open Commands, Network Desktop, Shell Execute Hooks, Protocols, etc. Services section contains a list of files registered as Windows Services. Users can benefit here from details like the way a service is set to start, a brief description and the company it pertains

to. You cannot make any modification in here, just take a look and, if there is a problem, use a different application to fix it. The same is available for Drivers as you will be presented with a list of drivers installed on your system. System Information node, as its name suggests, brings details on the system. Here you can find out about the amount of memory available, how much of it was in use during the scan, type of the CPU and its frequency, user language, environment variables, applications currently installed, list of hotfixes and updates (on Vista I could see only the latest updates), name of the current user and of the computer as well as allowed privileges. For a viewer, SysInspector gathers a lot of data in quite a short amount of time but it shows it is in beta stage, as there are details that need to be taken into consideration for such an application. Refresh is one of them as the processes on the system keep changing every minute. Also, you cannot manipulate the processes in any way from SysInspector (save for opening file location or in RegEdit). Searching online is a mighty good idea but it seems that the application uses Google so there isn't much functionality here (I was expecting more appropriate web locations). **The Good** SysInspector makes for a very good system checker and the fact that it labels the items as safe, unknown and risky on its own makes the users' job a lot easier. The information gathered is comprehensive enough to cover registry entries, running processes and network connections. **The Bad** It is a beta, so there can't be really bad things when it comes to a project in progress. We'll be waiting for the final version to come out and take a look at the improvements as there is plenty of room for them. **The Truth** As a computer administrator you should know at all times what's going on with the system. SysInspector scans the machine and rakes up important info on all running processes, network connections, registry entries, services and drivers. Applying color codes for making unknown and risky items stand out from the crowd is only for the better, although during our testing it labeled as unknown all non-system related connections (the same result came from testing it on two different Vista Business systems). SysInspector will retrieve important information on your computer but the downside is that it cannot be refreshed and you cannot introduce it to some of the items it lists so that next time they will no longer be marked with the color for "unknown". *Here are some snapshots of the application in action:*