



# Vir.IT eXplorer Lite

-The free security software for Windows -

**Vir.IT eXplorer Lite** is the free version (for both private and corporate users) of the suite Vir.IT eXplorer PRO. Vir.IT eXplorer is an AntiVirus solution for Microsoft Windows® operating systems that includes an AntiSpyware, AntiMalware and AntiRootkit module protection.

The software can detect: viruses, spyware, trojans, backdoors, BHOs, dialers, adware, hijackers, keyloggers, worms, rootkits, fraudtools, ransomware and other malware. Among its key features stands out without a doubt the easy to use graphical interface and the low system resources footprint, making it ideal even on outdated computers. **Vir.IT eXplorer Lite** can be installed on Microsoft Windows® operating systems starting from Windows® 95 up to Windows® 8.

**Vir.IT eXplorer Lite** aims to increase the user's security experience, thanks to the ability to install it together with other AntiVirus and/or Internet Security products without having to uninstall or deactivate them.

This allows the user to dramatically increase the security of the computer without having to give up performance or the usual software solutions already installed on the computer.

All this is given for free, both in private and corporate realities, without having to register or give other private information before the download or during the installation process.

The latest release of **Vir.IT eXplorer Lite** can be downloaded directly from the official TG Soft's website (<http://www.tgsoft.it/>). TG Soft is the mind - the company - behind **Vir.IT eXplorer Lite**.



The installation process is very intuitive and straightforward, just choose the language (English or Italian) and follow the instructions on the screen as in a common wizard setup, after which you will be prompted to restart the computer.

Once **Vir.IT eXplorer Lite** is installed, it can be identified from the common "Spy Agent" icon, in the Windows® notification area.

**Vir.IT Lite Monitor** is in charge of monitoring the system and automatically download new updates.



The first thing to do after the installation is to update the AntiVirus, in order to have the latest virus signatures and scan engines. Only for the first time, right after the installation, it is suggested to update the software manually, generally new signature and engine updates are downloaded automatically, in a transparent way,

without user interaction from the **Vir.IT Lite Monitor** when the computer is connected to the Internet. **Vir.IT eXplorer Lite** is constantly updated to cope with next-generation viruses/malware, with a particular attention to those actually in the wild and to the ones sent by the PRO users and by the more than 2'000'000 users of the Lite version to the [TG Soft's C.R.A.M. team](#).

It is possible to manually update both the virus signatures and the scan engines of **Vir.IT eXplorer Lite** by clicking on the [Update Online] icon as shown in the image on the right.



The manual update can be done also from the **Vir.IT Lite Monitor** by clicking on the icon with the red and white arrows [Update Online] as displayed in the image on the left.

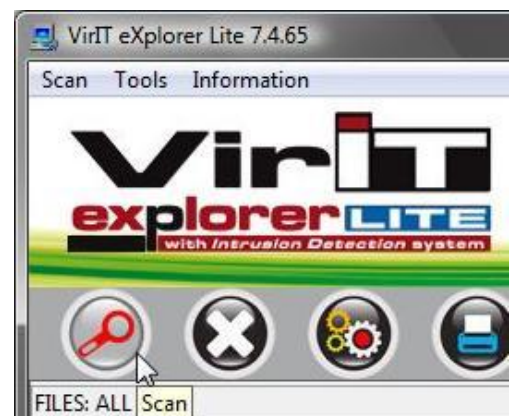
After retrieving the last update, it is good practice to start a full scan of the computer to check the eventual presence of unwanted software inside the computer, such as: spyware, viruses, rootkits, adware or other malware.

**Vir.IT eXplorer Lite** will start searching for bad applications inside the computer. On Windows® Vista, Windows® Server 2008, Windows® 7 and Windows® 8 operating system it is suggested to start the scan activity with Administrative privileges, by clicking with the right mouse button on the **Vir.IT eXplorer Lite** shortcut available on the Desktop or by following the path: Start -> All Programs -> VirIT eXplorer Lite[this is a folder] -> VirIT eXplorer Lite and selecting the item [Run as Administrator]. By running **Vir.IT eXplorer Lite** as Administrator, the scan will be able to check the Master Boot Record, the Boot Sectors of the Hard Disks and eventually remove infected files detected during the activity without any restriction action.

To start the scan simply press the red magnifying glass icon that will start the search activity.

By default, the scan is performed on all the available hard disks, network units mapped on the computer and all external storage devices connected at the time the scan starts (USB Drivers, external Hard Disks, [other]).

The default option is set to "Clean infected files automatically".

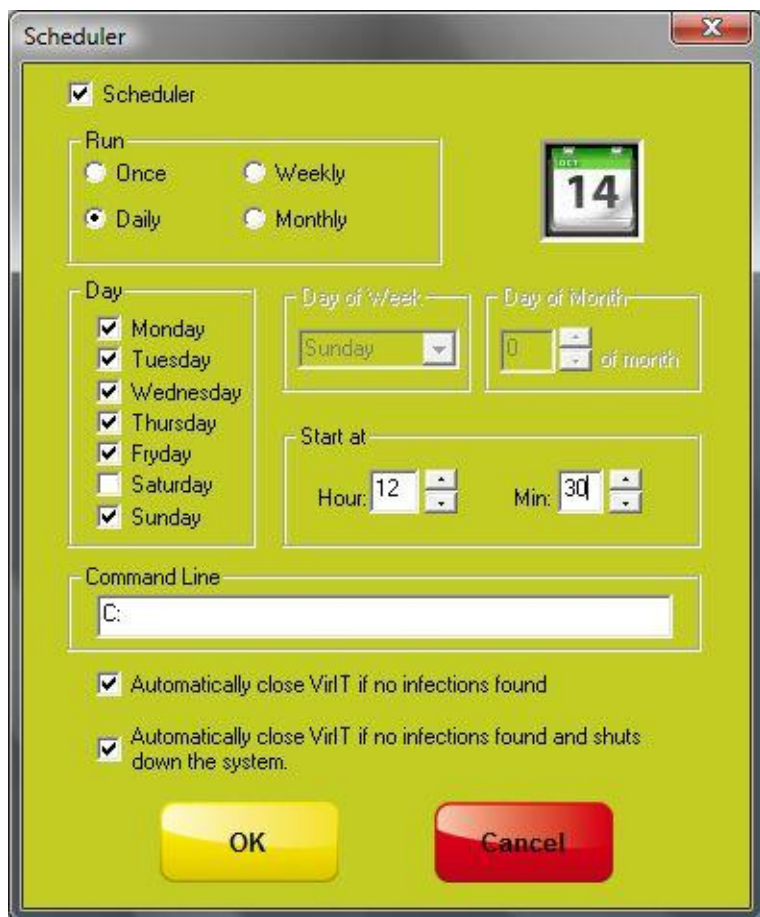


Automatic scheduled scans can be set in **Vir.IT eXplorer Lite** by clicking on the [SCHEDULER] icon as displayed in the image on the right.



To set the [SCHEDULER] it is also possible to execute it by clicking on the calendar/clock icon available on the **Vir.IT Lite Monitor** interface.

If correctly set, the [SCHEDULER] allows easier automate scans.



At startup: every time the computer powers on a scan is started;

Daily: the scan is performed on the selected days inside the Day group, at the set time (hour/minutes);

Weekly: a scan is started once a week, at the specific day set in the drop-down menu Day of the Week;

Monthly: a scan is started every month at the chosen day from the Day of the Month group.

It is also possible to specify the units where a scan is started, simply write the letter of the unit inside the Command Line space, separated by a space.

When **Vir.IT eXplorer Lite** (like its big brother **Vir.IT eXplorer PRO**) detects a virus/malware, it can adopt different techniques to properly remove it. For example, when a cleanup task is performed, even from a polymorphic virus, most of the AntiViruses on the market proceed to move the infected file to the quarantine or to delete it without checking whether the file is recoverable or not.



**Vir.IT eXplorer Lite**, instead, proceeds with the disinfection of the file, erasing only the tail of the file that is detected as a virus/malware. This process allows to restore the file to its original functionality, without caring to perform a substitution or re-installation of the file after being compromised by a virus/malware. Only in the case the file is detected as compromised and permanent unrecoverable, then **Vir.IT eXplorer Lite** proceeds to move the file to the quarantine or erase it on demand.

This philosophy is found by examining the removal methodology selectable from the [OPTIONS] window, accessible by clicking on colored gears icon as displayed on the right.



The ONLY SCAN options is the most neutral ones, it performs a scan only displaying the infected files, without further actions.

The remaining actions are divided in three different category:

- Clean infected files  
It is the standard action. Vir.IT eXplorer Lite will give priority to the removal of a virus from the infected file, when possible.
- Delete infected files (use with caution)  
It is the most aggressive option. Vir.IT eXplorer Lite will delete the infected file. The user needs to take care to substitute the file with a genuine one. In the case the infected file is fundamental for the operating system or for another application installed on the computer, the substitution of the file must be done before the computer reboot or before the application startup.
- Search and rename infected files  
When an infected file is detected, the infection is not removed, instead, it is renamed changing the file extension in .vir, leaving the file in its original path.

Each type of action has two different run mode:

Automatic: for each infected file detected during the scan, the chosen action is taken by the software without asking the user what to do.

Ask: for each infected file detected during the scan, the chosen action is asked the user.

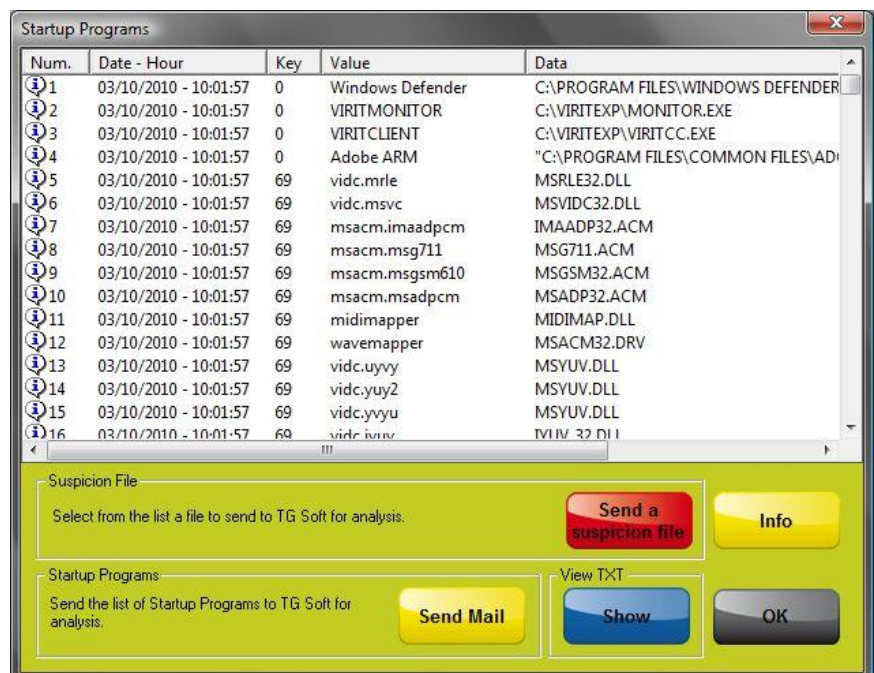
TG Soft is proud to introduce Intrusion Detection™, the innovative intrusion detection solution which is able to analyze and monitor software that puts itself in auto-execution, integrated in the **Vir.IT Lite Monitor**.



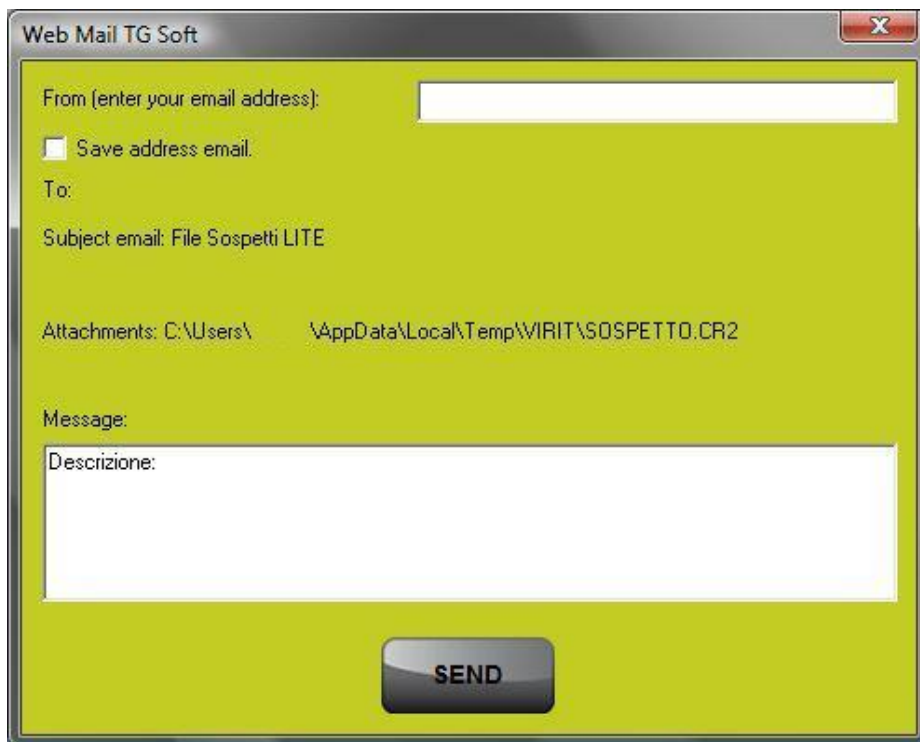
If an unwanted program puts itself in auto-execution without asking for the user permission, using one of dozens of possible methods in Windows®, a window is displayed informing the user about what is happening on the computer. In this way, the user can decide which further actions to take. If the suspicious file is a well-known virus/malware, a window is displayed reporting the possibility to remove directly the infection. If AntiVirus is asking attention for a suspicious file, it is suggested to send it to the [TG Soft's C.R.A.M. team](#).

The C.R.A.M. (Anti-Malware Research Center) team will take care of the sent files. Sending a suspicious file is completely safe and free, without any charges. The file is automatically encrypted before it is sent, so that it cannot harm anyone.

Vir.IT Lite Monitor also provides powerful diagnostic tools, such as the list of running programs on the computer, accessible via the "secret agent" icon. By clicking on the latter one, a window similar to the one here on the right will be displayed.



It is possible to send any startup program to the C.R.A.M. research team, by simply selecting the corresponding number of the suspicious file and clicking on the [SEND SUSPICION FILE] button. The same action can be taken when the Intrusion Detection™ identifies a new program that has put itself in automatic run mode.



It is not mandatory to put a valid email address when a suspicious file is sent. However, by using a valid email address, one will receive via email the result of the analysis of the sent file together with the actions to take. The email addresses are not used for commercial communications and are not provided to other companies, indeed they are only used for communications regarding the required analysis.

To the so far described characteristics, **Vir.IT eXplorer Lite** also adds some diagnostic and advanced removal specific virus/malware features, which other AntiVirus solutions present nowadays on the market have shown some difficulty to implement.

Below, an introduction and a brief description of some of these features is provided.

Process Manager: list of active processes, with the possibility to kill them.

Device Manager: list of the Device Drivers loaded in the kernel, with the possibility to save the memory dump.

System report: LOG file storing the list of the last modified or created files in sensible system directories, LOG file storing a list of all software with an entry in the automatic run module of Windows®, LOG file storing a list of all active services set in auto run mode at Windows® startup. All these reports give the user information like the ones that can be retrieved from the HijackThis™ software solution.

ADS look: allows to detect ADSs (Alternated Data Streams) hidden in files or directories.

Fix IE + Windows settings:

this tool is particularly useful, after a virus/malware has infected the computer disabling some Windows functions necessary to react after the attack.

In additions, it allows to: restore the Windows Task Manger, the regedit execution, restore the default desktop wallpaper, restore the default Internet Explorer web page, restore the default Windows Group Policy disabled as a result of the attack.

Move file and Vir.IT Agent System: provides powerful advanced features for manipulating files and the Windows registry. Their use is suggested only to advanced users.

It is suggested to left always installed **Vir.IT eXplorer Lite** on the computer, preferably in advance (not when the computer is overwhelmed by infections), so to quickly use the Intrusion Detection™ technology for reporting any virus/malware of next-generation, thanks to the send suspicious module made available by TG Soft with no extra charges. In this way, if a new virus/malware is detected, the C.R.A.M. research team can easily create a specific update with signatures and removal instructions for the user infection, even in this case with no extra charges.

**Vir.IT eXplorer Lite** is used by many IT assistance center as a diagnostic and removal virus/malware tool, since, in addition to being particularly efficient, it is able to identify and remove malicious software, also thanks to its pro-active update characteristics. This is possible through the send suspicious file tool that allows for free the transmission of a suspicious file to the [TG Soft's C.R.A.M. team](#).

For the most demanding users, private or corporate ones, that have the necessity to protect in real time their work and all the computer's files, there is the possibility to buy the commercial version, **Vir.IT eXplorer PRO**, that is a complete and efficient, low resources footprint software solution. In the one year license, it is included a technical assistance in English language via email and an ad-hoc update in the case the user is infected by a virus/malware of next generation, allowing the end user to get protected in the shortest possible time.

## SUMMARIZING

Install **Vir.IT eXplorer Lite** on the computer is quick and painless showing the great advantage of being able to be used simultaneously with other AntiVirus solutions (AntiMalware, AntiSpyware, [other]) already installed on the PC. This features allows to crosscheck the computer in an easy way, nowadays is no longer a habit for "hypochondriacs" but a handy tip for all users.

Thanks to the choice made by TG Soft to give for free with no extra charges **Vir.IT eXplorer Lite – Free Edition**, not only for private use, as common for other software distributed as Free Edition solutions but also and especially for corporate use, the installation is not only allowed but, as you might guess, it is highly recommended. We remind that **Vir.IT eXplorer Lite** has built inside different engines in order to identify and remove the following types of family: viruses, spyware, trojans, backdoors, BHOs, dialers, adware, hijackers, keyloggers, worms, rootkits, fraudtools and other malware.

The latest release of **Vir.IT eXplorer Lite** it is always available on the TG Soft's official website ([www.tgsoft.it](http://www.tgsoft.it)), without having to register. The last version of the AntiVirus is downloadable from the [Download](#) area, directly achievable by clicking on the link on the right.

