Copyright (C) 2000-2001, Diamond Computer Systems Pty. Ltd.

http://www.diamondcs.com.au support@diamondcs.com.au

Case Studies

What is RegistryProt ?

RegistryProt is a 100% free, standalone, compact, low-level realtime registry monitor and protector. From the same people who brought you TDS and WormGuard, RegistryProt adds another dimension to Windows security and intrusion detection.

How does it work ?

By monitoring important locations and keys in the Windows system registry, RegistryProt will alert whenever a key is added or changed, and then give the option of accepting the key change, reverting back to the original key setting, or deleting the key.

Many Registry monitors work by actively polling specific registry locations (you can confirm this with a tool such as SysInternals Registry Monitor). This is a task that must be executed every few seconds and demands resources from the system. RegistryProt v2.0 is unique in that it hooks into the registry, allowing it to sit and wait for changes/additions, using virtually no resources in doing so.

Why does the Registry need monitoring ?

In essence, the registry is a database. The registry itself does not need monitoring, but certain keys and locations within the registry can have a significant influence on the way that Windows runs. Some of these include keys that allow programs to start automatically when Windows is loaded.

By monitoring these locations and keys within the registry, it is possible to detect in realtime:
 * Trojan infection - the vast majority of trojans that have autostart capability use the registry to do so.
 * Spyware - a lot of autostarting spyware also install into the registry.
 * Malicious registry modifications
 * Other unauthorised auto-starting software.

Does RegistryProt consume many Resources ?

No! At only 20kb, the memory footprint of RegistryProt is tiny, and it has been specially engineered to be as small as possible - right down to the last byte. Running as a multi-threaded invisible background task, you will probably forget it is even there! RegistryProt does not even use any system tray or taskbar icons - there is no need. It is also 100% standalone, requiring no additional files or DLLs to run. We encourage you to compare RegistryProt with other registry monitors (some of which cost up to US$30) using the performance testing and monitoring software of your choice (even Task Manager will do!) - we're confident the results will both please and surprise.

RegistryProt is everything you need in a registry monitor/protector, and just as importantly - nothing you don't!

How do I install RegistryProt ?

Installation is easy - just run rpsetup.exe, and follow the directions. Then, simply run the rpadmin.exe program, and click Install, and then click Start. That's all!

Clicking Install will allow RegistryProt to start automatically every time Windows loads. Clicking Start will start RegistryProt.

The RPAdmin.exe simply allows you to Start/Stop RegistryProt and Install/Uninstall it's autostart capability.

NOTE : Users of earlier versions of RegistryProt should stop, and uninstall the old version before installing the new version - RegistryProt 2.0

Ok I've installed it, and RegistryProt is running, now what ?

That's all! You can now go about your normal business, just as if RegistryProt wasn't running. RegistryProt will not make itself known until the time comes that an important registry key has been added or modified. At that point, RegistryProt will alert you.

Where is your Homepage ?

We have a lot of security software for immediate download available at http://www.diamondcs.com.au

When I started RegistryProt, it alerted me to a few keys! Why ?

When you first run RegProt, if any autostart keys exist then RegistryProt will ask you if you want to allow their existance. You would probably click Yes to most if not all of these keys. After clicking Yes to confirm the presence of a key, you will never be alerted again on that particular key unless the actual data in it changes.

How do I know if a registry entry is safe or not ?

Ultimately you must decide for yourself if you want to allow a registry entry, and manually inspecting the file that the entry points to is usually the best way to start.

When you first start RegistryProt, you will be asked to allow/deny the existing auto-start registry keys. You would typically select 'Yes' to allow all of the existing entries (unless you recognise one to be a trojan or your anti-virus/anti-trojan software informs you accordingly). At this point you can typically forget about the registry entries.

However, when you run a program and RegistryProt springs into action and warns you with an alarm, this is an obvious tip-off that whichever program you just executed has modified or added to your registry.

I've deleted a key but it keeps coming back!

If you are experiencing this behavior, it is very likely that a trojan is resetting the key at a timed interval. It is also very likely that the file causing this behavior is referred to in the DATA field of the recurring RegistryProt alert.
To stop this behavior, the program that is resetting the key must be terminated before the key can be properly removed/reset.

TDS-3 users can easily accomplish this from the **System Analysis..|..Process List** window by selecting the malicious program and pressing Kill Process.

How can I manually edit registry entries ?

Registry entries can be modified with any common registry editor, such as the one that comes with Windows - RegEdit. To start RegEdit, simply press the Windows Start button, then Run, then type "regedit" and press Enter.

Does RegistryProt create any logs ?

Yes, RegistryProt appends to the HISTORY.LOG file (in your RegistryProt directory). RegistryProt will log as many details as it can, including the time, the event, full registry path, and before/after settings when available.

Should I disable RegistryProt while I defrag my hard drives ?

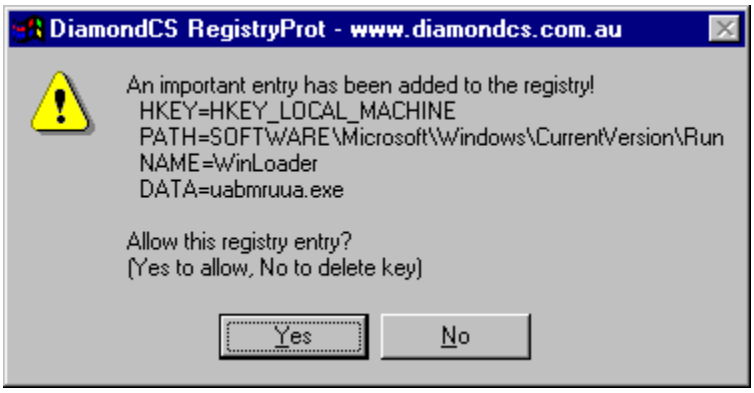
It is not necessary to disable RegistryProt during defragmentation or other intensive scans, but it is recommended and will also aid performance. In general, disabling all 'active' programs (not just RegistryProt) is a good idea - the less programs running the better!

I have a question you have not answered here, HELP!

If you have any other questions or feedback regarding our software, please do not hesitate to contact us at support@diamondcs.com.au

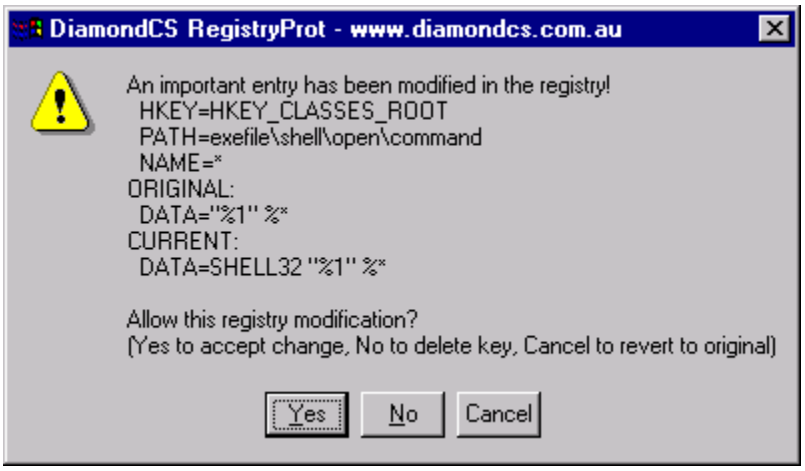
Subseven Detection

RegistryProt's most useful attribute is that it will detect the vast majority of trojans at the exact moment that they infect/install themselves into your system, and as such provides a new dimension in trojan and intrusion detection.

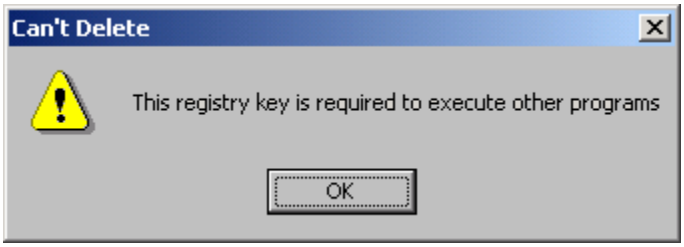


This picture is a screenshot of an actual SubSeven infection, as detected by RegistryProt. SubSeven usually installs into the common Run autostart registry keys. The moment it does this, RegistryProt alerts that an important key has been added.

Case Study - Drat Detection



This picture is a screenshot of an actual Drat infection, as detected by RegistryProt. Unlike SubSeven, the Drat trojan uses an existing registry key. Because of this, RegistryProt alerts that an important key has been modified. As this is a very important registry key, it cannot be deleted even if you select 'no'.



Replacing the original is the only option when this particular key is modified.