



## Addressing Computer Issues Using RegCure Pro

Product White Paper  
January, 2012



## **ParetoLogic RegCure Pro**

RegCure Pro is a software solution created for improving computer speed and performance. It targets not only the Windows registry, but also active malware, clutter, memory defragmentation and other PC performance problems. RegCure Pro was specifically developed to be utilized by computer users of all ability levels.

See: [www.regcure.com](http://www.regcure.com) for more information.

### **ParetoLogic – The Company**

ParetoLogic is an international software development company headquartered in Victoria, British Columbia, Canada. We specialize in providing advanced security applications and performance tools for business and personal computer users.

ParetoLogic creates solutions that combine sophisticated technology with a truly user-friendly interface. Our products empower people to secure and optimize their computers and are available in eight languages in 192 countries around the world. ParetoLogic has established partnerships on a global scale to ensure our products are available to all computer users regardless of location, language, or computing experience.

Attention to consumer needs coupled with a commitment to deliver exceptional software applications and resource-rich websites, guarantees that our products will exceed expectations.

## Addressed in this White Paper

This document provides information about the registry and makes recommendations to improve it. One area of contention with computer experts lies in the potential effects of unwanted items in the registry. What we will show in this paper is that there are instances when malicious items can be left in the registry. These can have a negative impact on computer functionality. Benchmark testing has been performed to demonstrate how RegCure technology improves registry functioning when working in conjunction with anti-malware software. In addition, this white paper discusses RegCure Pro's other functions and features as they pertain to the improvement of computer performance.

This document highlights the sensitive nature of registry modifications.

**The following topics are covered:**

Registry Information	4
Specific Registry Concerns	4
Scan and Removal	6
Issues, Concerns and Answers	8
RegCure Technology Benchmark Testing	10
Safety – The User Experience	12
Overall Performance Solution	13



This white paper includes information and recommendations about RegCure Pro. This document is not intended for instructional purposes. For detailed instructions, please refer to the RegCure Pro help file, which can be accessed via the program.



## Registry Information

The registry is a necessary component of the Windows operating system. In fact, Windows would not be able to run without a functional registry. Modifications to the registry occur every time an application is added or removed. Manual changes are not recommended and even experienced computer users proceed with caution when making changes.

The registry is stored on your computer in several files. Depending upon your version of Windows there will be different files and different locations for these files. The registry contains information "...such as profiles for each user, the applications installed on the computer and the types of documents that each can create, property sheet settings for folders and application icons, what hardware exists on the system, and the ports that are being used."<sup>1</sup> Whenever changes are made to the Control Panel settings, file associations, system policies, or installed software, the changes are reflected and stored in the registry. The operating system continually references this information during its operation.

## Specific Registry Concerns

There are advantages to a registry system. Some benefits include: machine configuration is separate from user configuration, setting group policies is easier for administrators to manage, the registry can be accessed as one item over a network, and it can be backed up easily due to the size and specific location of the files. However, a centralized registry system presents some problems as well. The registry is considered a single point of failure – modifications can lead to disrepair. The resulting damage can range from poor performance to not being able to boot up your computer. In the most extreme cases, data can become unrecoverable and a full reinstallation of the operating system is required.

Occasionally, applications do not uninstall properly. In such instances these programs are not equipped with uninstall capabilities or they leave items behind after uninstalling. As a result, left-over entries in the registry can lead to

---

<http://support.microsoft.com/kb/256986>



increased registry size. Some computer users spend a lot of time and effort going through the registry and editing it manually. Not only can this be a daunting task, it is also a risky one.

Most software programs are benign but there are many malicious programs that can be damaging to the computer system. These programs install files to the system and add items to the registry without consent or foreknowledge. Some anti-malware programs are efficient at removing malicious intruders but leave the corresponding registry entries. This will be covered in greater detail later in the paper.

*Making changes to the registry can cause irreversible damage. We recommend having foreknowledge of backup procedures. A good registry program provides safeguards and functionality for restore points.*



## Scan and Removal

There are several types of registry items that can be scanned using RegCure Pro. The following table lists these categories and describes invalid entries that can be contained within. The description column lists the effect, such as system crashes, application failure, incorrect functionality, and errors.

Categories	Invalid Entry Description
COM/ActiveX Entries	The COM/ActiveX section of the Windows registry can contain invalid entries that can cause application failure, system crashes, or errors when opening documents.
Uninstall Entries	The Uninstall Entries Section of the Windows registry can contain invalid entries or point to one or more missing entries. Typically this is due to incorrect installing or uninstalling of applications.
Font Entries	The Font section of the Windows registry can contain one or more missing font files that can cause application errors (for example, Word processing applications).
Shared DLLs	The Shared DLLs section of the Windows registry can contain invalid entries that cause application failure due to DLL conflict.
Application Paths	The Application Paths section of the Windows registry can contain invalid disk directories that can cause application failure.
Help Files Information	The Help section of the Windows registry can point to invalid help files that can cause application help files to open incorrectly.
Windows Startup Items	The Run section of the Windows registry can contain missing program entries that can be due to incorrect installing or uninstalling of an application.
File/Path References	Some registry items can be associated with non-existing files and folders such as when temporary files are used for storage. These entries may still be valid and required for use. Only remove entries that you know are invalid.
Program Shortcuts	Program shortcuts that are files with a ".lnk" extension may no longer be linked to an application.
File Associations	The File Associations section of the registry can contain invalid file associations. If a file type is associated with a program that does not exist, it shows up as an irregularity.

*Table 1: Types of invalid registry entries*



## **Scanning**

Once the categories of registry items are selected a RegCure Pro scan can be initiated. RegCure Pro provides a step-by-step process that includes displaying the scan progress. After the scan is completed the list of errors will be displayed. Although a computer may already have several scanning tools, the first RegCure Pro scan you perform will typically detect hundreds of invalid registry entries. RegCure Pro's detection of registry items is specific to invalid entries as described in Table 1.

*Registry items that are listed could be associated with non-existing folders or files and, as such, are invalid registry items. However, some entries may be valid. It is important to know an item is invalid before removing it.*

## **Removal of Detected Items**

By default, all the identified errors are selected for removal. Information for each error is provided including an error description and the location of each item. There is the option to select only items the user wants to remove and items can also be sent to the Ignore list.

## **Ignore List**

When an item is added to the Ignore list, RegCure Pro does not remove the item and it ignores it in future scans. The items that are listed in the results window have associated information about their location in the registry and there is also a link so they can easily be sent to the Ignore list. The Ignore list can be displayed and reviewed. Any of the items can be removed from the list so that they are once again available to be scanned, detected, and removed.



## Issues, Concerns, and Answers

*Why does RegCure Pro detect items on a brand new computer?*

When a computer system is built and sold it comes with applications and the operating system installed. From the moment applications begin writing to the registry the potential exists for unnecessary registry data to begin accumulating. This occurs when applications shipped within the operating system start running during the latter stages of the install.

Although this type of registry data will usually be more benign in nature, it still fits with the overall classification of being potentially unnecessary to system functioning and redundant to normal computer operations. It is also important to keep in mind that two freshly installed computer systems are not necessarily going to have the same registry entries.

*Why does RegCure Pro detect items immediately after performing a subsequent scan and removal?*

There are applications and processes constantly running in the background when a computer is active. Some applications have associated keys in the registry that appear to have no value associated with them. These items are unused or can be considered unwanted for regular computer functioning. After these items are removed from the registry, the associated program detects that the entry is missing and then replaces it. The item is again replaced with an empty value associated with it leaving it open to detection and removal when performing a new scan.

*Why do items get left in the registry and why do programs create empty keys?*

In the case of uninstalling applications, poor programming practices lead to leaving registry items orphaned. In other situations, programs remove their associated data from the registry and leave the registry key with no associated value; the item is null or empty. It is difficult to say for certain whether the registry key is still serving a purpose. It could be that a null or empty-value key has some meaning to the associated application. In these cases the registry item should remain. Frequently, anti-malware applications remove malicious programs such as viruses and spyware but will leave behind registry items originally created from these malware intruders. These items and those orphaned due to an inefficient uninstall procedure can safely be removed.

*What about issues and concerns involving users having to perform system*



*restores?*

There are many instances of computers facing severe system issues or failure that can be the result of faulty hardware or lack of hard disk drive space. Another major cause of dysfunctional system performance is based on software limitations including outdated drivers, missing or corrupt files, and the like. Also, having malicious software installed on the system without the user's knowledge or permission can result in system failures and slowdowns. RegCure Pro is not a cure-all solution. It addresses issues to the registry and removes unwanted items there but it does not provide a cure for all system issues. It does offer the ability to restore the system to a previous state should undesirable results occur. RegCure Pro is designed to work with the Microsoft Windows restore function to ensure the user can return their system to the state prior to registry changes even if that was a dysfunctional state.

*What is the impact to a system as a result of registry junk left on the system?*

Windows registry systems accumulate junk data over time especially as a result of un-installation software limitations. Generally speaking, with modern computer systems performing at higher speeds, "junk" in the registry will not likely have a noticeable impact on system performance when it comes to speed.

However, it is our contention that certain leftover registry junk and unwanted items can cause malfunctions and system stability issues. These problems are indeed noticeable and in some cases can cause significant disruption to computer functioning. From the user perspective the system appears to be slow because programs are malfunctioning. The user has no way of knowing if this is actually due to malfunctioning applications, registry error, or a combination of both.

An example of problem data is a remnant of a program in the registry that results in the operating system or an application (for example, Internet Explorer), attempting to run the absent program. Depending on what the remnant is, there may be no resulting issues. However, we do not want to rule out the possibility that a system slowdown can result as the operating system waits for a timeout period to use the nonexistent program or an error messages appears indicating files are unexpectedly missing. A registry cleaner that is able to eliminate the problem data can assist programs to resume normal functioning and, from the user perspective, the system functionality is returned to expected levels of operation.

## RegCure Technology Benchmark Testing

In the previous section we pointed out that “junk” registry items are potential causes for malfunction. If this is true for miscellaneous benign applications with poor uninstall procedures, it is even more likely with malware. These items can be installed to a computer system without the user’s knowledge by simply visiting a website.<sup>2</sup> In this section we perform benchmark tests on a fresh installation of Windows XP with no other installed programs.

1. **RegCure Pro scan and clean.** We set a baseline for the clean system by initiating the RegCure Pro scan and removal process. We were able to arrive at a zero item detection of unwanted registry items.
2. **Malware infection.** Ten malware samples were used to infect the computer.

cz_265_1825.exe	Trojan.Win32.Dialer.qn (v)
gsa1450.exe	Trojan.Win32.Dialer.cj
India.exe	Porn-Dialer.Win32.EzDial.a (not a virus)
install.exe	Trojan-Downloader.Win32.Exchanger.nd
Instant-Access.exe	Dialer.InstantAccess.A
is.exe	Trojan.Vundo.FEA
ok.exe	Trojan-Downloader.Win32.Agent.vqd
rfx8.exe	Trojan.Win32.Patcher.ar
safestrip_setup(1).exe	Rogue Security Program
setup_en.exe	Rogue Security Program

*Table 2: Malware items used to infect the test computer.*

3. **Scan and clean using Symantec AntiVirus.** We used Symantec AntiVirus to remove the unwanted malware infecting the computer system.

---

<sup>2</sup> For more information on malware see: [“A CyberCrime Report”](#)

Risk	Exclude	Action	Count	Filename
Trojan.Vundo		Cleaned by deletion	5	khfGyaWo.dll
Hacktool.Rootkit		Cleaned by deletion	2	cdraw.sys
W32.Looked.O		Quarantined	2	rundl132.exe
W32.Almanahc.Blinf		Reboot Required - Quarantined	2	linkinfo.dll
W32.Looked.O		Quarantined	2	Logo1_.exe
W32.Almanahc.Blinf		Cleaned	2	Dc2.exe
VipAntiSpyware	<input type="checkbox"/>	Quarantined	2	setup_en.exe
Trojan.Erotpics		Terminate Process Required	6	install.exe
Dialer.Generic	<input type="checkbox"/>	Quarantined	2	India.exe
Dialer.Generic	<input type="checkbox"/>	Quarantined	2	gsa1450.exe
SafeStrip	<input type="checkbox"/>	Reboot Required - Quarantined	43	safestrip.exe
Trojan.Erotpics		Terminate Process Required	6	cbvtsvc.exe
Trojan.Downexec.Blinf		Partial	2	explorer.exe
VipAntiSpyware	<input type="checkbox"/>	Quarantined	36	vipantispyware.exe
Trojan.Vundo		Reboot Required - Cleaned by deletion	2	fccbbrjh.dll

Image 1: Symantec AntiVirus results.

- 4. Scan the system with RegCure Pro.** After Symantec AntiVirus was used to clean the system, we ran another RegCure Pro scan. The results: 131 items were detected.
- 5. Clean the system with RegCure Pro.** We once again used RegCure Pro to clean the registry. The results: 131 detected problems were cleaned.



## Safety – The User Experience

*According to Wikipedia<sup>3</sup>, “Poorly designed registry cleaners may not know for sure whether a key is still being used by Windows or what detrimental effects removing it may have. This has led to examples of registry cleaners causing loss of functionality and/or system instability.” What measures has ParetoLogic taken to ensure that the system is not negatively affected?*

RegCure Pro was tested using a comprehensive suite of function and regression tests to ensure that the product performs as designed. These tests are run both on new and populated systems. This suite of tests covers all aspects of user interaction including: scanning, cleaning, backup, and managing startup functionality. Testing was performed on the 64-bit Windows<sup>®</sup> 7 operating system platform as well as 32-bit Windows platforms that RegCure Pro supports including: Windows 7, XP (Service Pack 3), and Vista (Service Pack 2). With every program update, these tests are rerun to ensure the highest quality standards are met.

*How is the System Restore Point for Windows 7, Vista and XP incorporated?*

With restore point capabilities you can return your system to a previous working state. This method involves backing up system files as well as registry entries. The settings section of RegCure includes an option to create a restore point. When this is selected a system restore point is automatically generated each time the process of fixing errors is initiated.

### Safety and Peace of Mind

While removing items from the registry is a delicate matter, having the right tool in hand makes the task a safe and efficient process. The creators of RegCure Pro have designed a registry cleaning tool with safety in mind. By maintaining a clean registry free of junk items and malicious entries, a computer system is both stable and free of any performance constraints caused by these items remaining in the registry.

---

<sup>3</sup> [http://en.wikipedia.org/wiki/Registry\\_cleaner](http://en.wikipedia.org/wiki/Registry_cleaner)

Note: Restoring the registry can affect the functionality of your software. There are instances when incremental backups are beneficial over a complete backup of the registry.



## Overall Performance Solution

There are many reasons why a computer might be performing poorly or slowly. The Windows registry plays a large role in PC performance, but it is just one of the factors. RegCure Pro also tackles other performance problem areas, including:

**Malware:** There are all kinds of malicious programs that can sneak onto your computer. These viruses, spyware, adware, keyloggers, Trojan downloaders and other malware can hijack your web browser, annoy you with ads, attempt to steal confidential information, try to take over your computer or other unscrupulous tasks. They also can cause major performance programs. These programs were not designed to get along well with your operating system and other software. RegCure Pro finds active malware and gets it off your computer.

**Disk fragmentation:** When files are recalled and saved again, they often do not fit into their original physical locations. Your PC will split a file into parts and save those pieces where they fit best. However, this can place parts of the same file far away from each other. This means when you recall a file, your PC must take time to hunt down each part and bring them back together. Disk defragmentation, often known as defragging, puts all of the parts of a file in contiguous locations. This means your files can be recalled and saved faster.

**Too much demand on resources:** Computers can do many things seemingly at once, but there is a limit to their resources. When too many applications or processes are trying to run, there are not enough resources to go around. RegCure Pro helps stop unneeded programs that steal resources from valuable processes. As well, this program helps users select only the programs they want to launch at startup. This improves startup times.

**Clutter:** Your computer saves all kinds of files. These temporary items, junk files and general clutter are unneeded and can take up needed disk space. RegCure Pro also removes web browser privacy files, as well as ones generated by other applications. These items are not needed and they also can contain confidential information. As well, RegCure Pro can disable web browser add-ons, such as toolbars, that use resources and can diminish your browser's appearance.



*All information contained in this document is the proprietary information of ParetoLogic, Inc. and is protected by international copyright treaties. This document contains information that is privileged and confidential. Any disclosure, distribution or copying of this document without the prior written consent of ParetoLogic is strictly prohibited under applicable law. ParetoLogic and RegCure Pro are registered trademarks or trademarks of ParetoLogic, Inc. in Canada, the United States, and in other countries. All other trademarks are the property of their respective owners.*

*Copyright © 2012 ParetoLogic, Inc. All rights reserved.*