Addressing Registry Issues Using RegCure

White Paper
May, 2009

ParetoLogic – The Company

ParetoLogic is an international software development company headquartered in Victoria, British Columbia, Canada. We are a member of SIIA (Software Information Industry Association) and 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.

pareto
LOGIC

RegCure is a software solution created for the Windows registry. It identifies and safely removes invalid items including remnants left behind from failed installations, incomplete un-installations, disabled drivers, and malware. After removing these registry entries, restoration of the computer to a previous state can be made. See: www.regcure.com for more information.

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 improves registry functioning when working in conjunction with anti-malware software.

> *This document highlights the sensitive nature of registry modifications.*

The following topics are covered:

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."[1] 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 re-installation 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 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 backing-up and restoring files removed from the registry.*

[1] http://support.microsoft.com/kb/256986

Scan and Removal

There are several types of registry items that can be scanned using RegCure. 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.
Empty Registry Keys	Registry keys can be empty - they have no associated value.
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 then it shows up as an irregularity.

Table 1: Types of invalid registry entries

Scanning

Once the categories of registry items are selected a RegCure scan can be initiated. RegCure 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 scan you perform will typically detect hundreds of invalid registry entries. RegCure'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 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 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 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 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 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 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.[2] In this section we perform benchmark tests on a fresh installation of Windows XP with no other installed programs.

1. **RegCure scan and clean.** We set a baseline for the clean system by initiating the RegCure scan and removal process. We were able to arrive at a zero item detection of unwanted registry items.

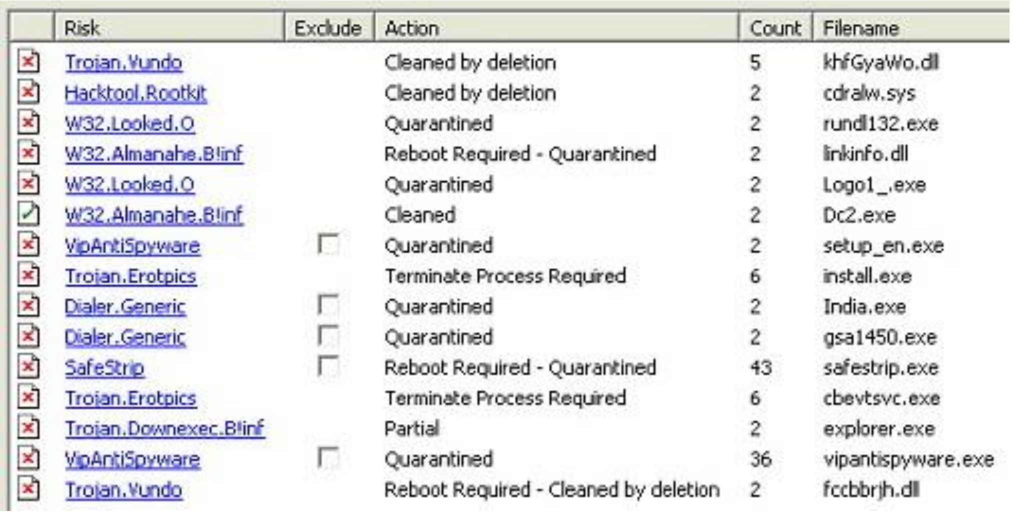
2. **Malware infection.** Ten malware samples were used to infect the computer.

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.

[2] For more information on malware see: “A CyberCrime Report”

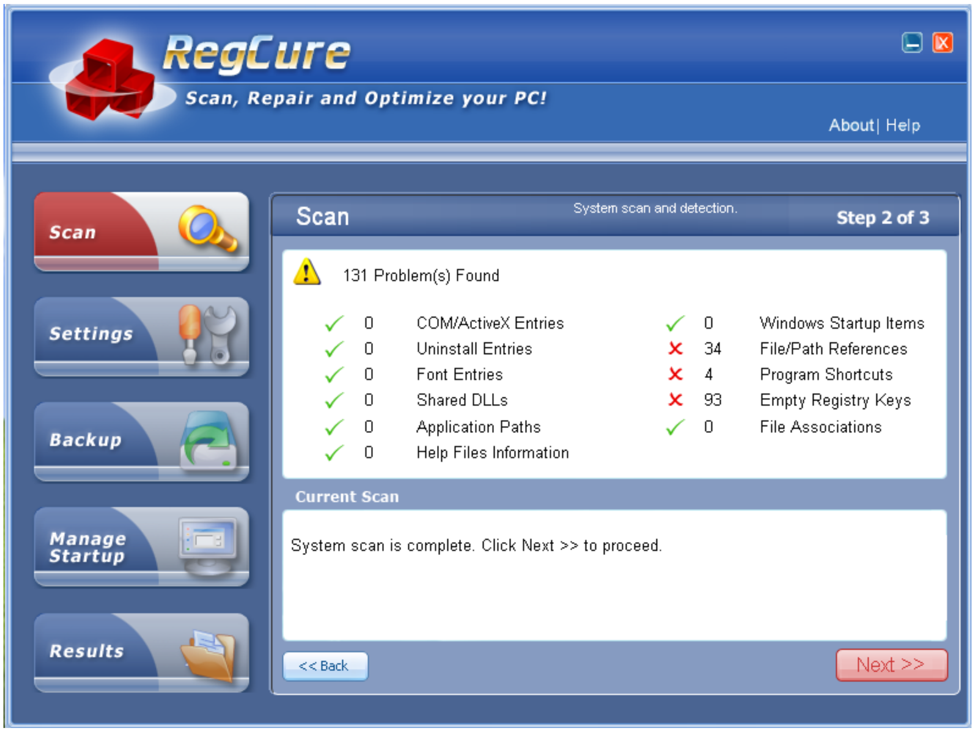
3. **Scan and clean using Symantec AntiVirus.** We used Symantec AntiVirus to remove the unwanted malware infecting the computer system.



	Risk	Exclude	Action	Count	Filename
☒	Trojan.Vundo		Cleaned by deletion	5	khfGyaWo.dll
☒	Hacktool.Rootkit		Cleaned by deletion	2	cdralw.sys
☒	W32.Looked.O		Quarantined	2	rundl132.exe
☒	W32.Almanahe.B!inf		Reboot Required - Quarantined	2	linkinfo.dll
☒	W32.Looked.O		Quarantined	2	Logo1_.exe
✓	W32.Almanahe.B!inf		Cleaned	2	Dc2.exe
☒	VipAntiSpyware	□	Quarantined	2	setup_en.exe
☒	Trojan.Erotpics		Terminate Process Required	6	install.exe
☒	Dialer.Generic	□	Quarantined	2	India.exe
☒	Dialer.Generic	□	Quarantined	2	gsa1450.exe
☒	SafeStrip	□	Reboot Required - Quarantined	43	safestrip.exe
☒	Trojan.Erotpics		Terminate Process Required	6	cbevtsvc.exe
☒	Trojan.Downexec.B!inf		Partial	2	explorer.exe
☒	VipAntiSpyware	□	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.** After Symantec AntiVirus was used to clean the system, we ran another RegCure scan. The results: 131 items were detected.



131 Problem(s) Found

✓	0	COM/ActiveX Entries	✓	0	Windows Startup Items
✓	0	Uninstall Entries	✗	34	File/Path References
✓	0	Font Entries	✗	4	Program Shortcuts
✓	0	Shared DLLs	✗	93	Empty Registry Keys
✓	0	Application Paths	✓	0	File Associations
✓	0	Help Files Information			

Current Scan

System scan is complete. Click Next >> to proceed.

Image 2: RegCure scan results after removing malware using Symantec.

5. **Clean the system with RegCure.** We once again used RegCure to clean the registry. The results: 131 detected problems were cleaned.

Safety – The User Experience

According to Wikipedia [3]*, "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 lead 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 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. This also includes testing across 32-bit Window platforms that RegCure supports: Windows 98, SE, ME, 2000 (Service Pack 4), XP (Service Pack 3), and Vista (Service Pack 1). With every program update, these tests are rerun to ensure the highest quality standards are met.

What Backup and Restore functions are offered?

If you are operating Windows 2000 (SP4), Windows 98 SE, or Windows ME, you will need to refer to the system help instructions on how to create a backup of the registry. For these systems, RegCure offers automatic backup file capabilities. If you are running a Windows Vista or Windows XP operating system, there are two backup mechanisms available with RegCure:

- System Restore Point
- Backup Files

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

The system restore point option is available if you are using Windows Vista or Windows XP. 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.

What are RegCure Backup Files?

Every time you use RegCure to remove registry items a backup file is automatically created. RegCure saves these backups so that deleted items can be restored. With this option, a group of registry entries can be reinstated rather than having to restore the whole registry or an out-dated set of files. There is also an option to restore one or more backup files at a time.

[3] 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.

Is RegCure safe to use?

RegCure was tested by Softpedia [4], an independent reviewer, and found to be a 100% clean. It can be installed by any user with no concern; "…it does not contain any form of malware, including but not limited to: spyware, viruses, Trojans, and backdoors."

Safety can also be substantiated by the success RegCure has experienced:

- Over 3.5 million customers have purchased RegCure.
- Currently, over a million users run RegCure on a weekly basis.
- 70% of RegCure customers are so satisfied with the product they have purchased other ParetoLogic products.

RegCure is one of the most popular and best-selling registry cleaners available.

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 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.

[4] http://www.softpedia.com/get/Tweak/Registry-Tweak/RegCure.shtml