Study on Security Auditing of Windows Registry Database

Jamyang Tashi
Associate Lecturer
Department of Information Technology
Jigme Namgyel Engineering College, Royal University of Bhutan, Bhutan

Abstract

Windows Operating System is the most widely used OS for computer systems in the digital world. With its popularity also comes in place the different kind of threats and malicious codes that affects the performance of the computer system where most Windows users are unaware of it. Any kind of malicious code that affects the performance of the Windows computer system affects the windows registry database. Therefore, it is important for computer users to have good knowledge of the Windows Registry Database where they can monitor the activities in the registry database. This paper basically explains the registry database, inbuilt tools in Windows OS, and open-source tools that can be used to investigate or monitor the malicious activities in the windows registry that affects the performance and smooth operation of the computer system. While monitoring and troubleshooting, it is important for users to gather and provide evidence of malicious activities on a Windows Operating system so that the system administrator of the organization can work smoothly without putting the system down.

Keywords: Windows Registry, Security Auditing, Investigation, Monitoring, Auditing

I. INTRODUCTION

Windows Operating System (OS) is the most widely used operating system in this world because of its simplistic Graphical User Interface where the user does not require much knowledge to use the OS. Microsoft Windows OS has become a significant OS for any organization and company for connecting users, resources, assets, and various IT resources in the organizations' network. Such significant usage has also brought about the increase in cybercrimes that are the Windows OS becomes the victims. Most users are unaware of the cybercrimes that are frequently being done on their system and as such has brought about a huge loss in most company's revenue due to data loss and thievery.

Windows System since its evolution from the Windows XP version since the year 2000, Microsoft introduced Windows Registry as the default treasury in which every configuration setting, Software, Hardware, User information, and settings are stored within in a categorized manner. The Windows Registry in a glance can be seen as only a database for storing the logs for every action done on the Windows system but for a Forensics specialist it is a treasure cove of evidence that can provide information on various kinds of criminal activities such as through malicious software deployed by Hackers to disrupt the Windows system leading to data loss and system failure. Other activities can also be analyzed through the registry such as when USB devices are used for data thievery and manipulations, As well as User account disruptions which cause users in an organizational network to be disabled from accessing their systems

The Windows Registry is set up in a hierarchical structure that stores all the configuration and information of every software application and hardware device that are currently configured to the system. The logs for any activities performed by the user or the system itself will make modifications to the Registry in real-time, thereby any pieces of evidence that can be availed from the registry will be valid for investigations. The only difficulty being that accessing certain data which is beneficial for investigation can be tough as the windows registry is huge in terms of content thereby using various open-source tools for auditing can help investigators easily extract evidence from the registry.

A. *Aim*

This study aims to explain the Windows Registry Database and different forms of investigation that could be performed using the tools to monitor the threats associated with the Windows OS because of which the system performance can be adversely affected.

B. *Objectives:*

The following pots were the main objectives of the study carried out:
- Explain Windows Registry Database and various tools used for conducting the auditing on the windows registry.
- Demonstrates the usage of the tools for auditing in the windows registry database.
- To collect and analyze the result after performing the auditing.
- Explains the backup and restoration methods for windows registry for the smooth operation of Windows OS system.

The Windows Registry Database will be set up in a hierarchical structure that stores all the configuration and information of every software application and hardware device that are currently configured to the system. The logs for any activities performed by the user or the system itself will make modifications to the registry in real-time, thereby any pieces of evidence that can be availed from the registry will be valid for investigations. While investigating the registry, there are log files to be checked in addition to the open-source tools available for users. Therefore, it is important to monitor the malicious code and activities running in the registry files of the computer system.

II. Literature review

The Windows Registry and its Hive structure provide information on how the configuration for the Windows OS is stored in the Registry and even summarizes how the Registry can be used as a treasury for forensics investigation (Carvey, 2011). As explained by Carvey, "The Windows Registry is a core component of the Windows operating system, and it maintains a considerable amount of configuration of the system. The Registry maintains historical information about user activity which is maintained similar to as a log file". Every configuration that is made as well as any changes to the system is directly logged in the Windows Registry in real-time thereby proving the evidence gathered from the Windows Registry to be valid for forensics investigation. Windows Registry may provide beneficial information for forensics investigators but without the set knowledge on how to access the Windows Registry can prove the forensics investigations to be a very difficult task indeed.

The Windows Registry is to be considered as a huge directory that has a hierarchical database of information based on many various system files such as autoexec.bat, config.sys, win.ini, and system.ini each having their own specific logs of the system configurations. The registry stores and organizes those data and displays them to users in its hierarchical structure if accessed by the default windows registry editing tool called the Regedit as explained and demonstrated (Yadav, 2020). He states the various locations or subkeys in the Registry which each have their own set of information for evidential uses. The evidence that can be gathered can relate to the following categories; User info, Hardware info, Software info, current system configuration info, etc.

The evolution of the Windows Operating system also came about with the change in hive structure of the Windows Registry database due to certain drawbacks as well as the unorganized manner of display of devices. Forensics Analysis that had been done on the Windows Registry during the time of Windows 7 as the main operating system for Windows is clearly portrayed (Alghafli, 2009) which also portrays the analytical research based on Software applications such as Windows Live Messenger, Skype, etc. and also the analysis is done over Network related configurations. Alghafli also stated the various evidential information that can be extracted for the various hardware devices connected to the system. "The information located under the subkey, HKEY_Local_Machine contains the various device information for every device that has been plugged into the system. Such information can be used to identify any unknown devices that may have been plugged into the system for malicious intent. The tool used to conduct the study was software programmed by the researchers themselves that allowed them to extract only specific information from the registry as per their filters and needs. The tool is winning 32-bit based and is infeasible for use for the current research as for the present system, the tool had legacy functions that were inapplicable for the research.

Dashora. 2010, introduces the various locations in the Windows Registry that can be used as a means for Evidence Gathering in a Windows Environment. Windows provide logs for any events that have occurred in the system in the Windows Event Log that can be used as forensics information, the Windows Registry as per Dashora's research has various locations that each provides information on various activities the user had done on the Windows system. Information examples can be like the commands input in the Run dialog box to execute certain actions in the system. Also, information such as the browser history as well as the searches done in the windows explorer can be known from those locations in the Windows Registry that helps to identify the intentions of the users as per their activity logs. The Regedit tool can be used to access that information if the location itself is known but due to updates in the windows Registry structure with every update of the Windows OS, the locations also change but the changes are usually not too dynamic thereby validating each of those locations for the usage of forensic analysis.

Detection and Monitoring of Malicious software with the help of an Intrusion Detection System had been done pr with which Registry findings had been analyzed in order to identify the Malicious code responsible. Apap had proceeded with the project by firstly setting up a virtual lab for the demonstration which then was equipped with intrusion detection software. When the malicious attack was initiated on the system, the audit was monitored using a RAD (Registry Anomaly Detection) tool which was designed by Apap and his research team which had three basic components namely; an audit sensor, model generator, and an anomaly detector. Each component provides various data for forensics analysis such as an alarm that detected the security intrusion on the system. The model generator provided general information of the various registry keys that were affected as per their process name, Query, Key info, Responses to the query, and result value. Though the tool used in his research had proper evaluations of the intrusion detection demonstration since the tool is of proprietary use, the tool was not publicly accessible thereby in the current research, a different tool was used to perform the security audit for detecting intrusions.

The tool used to perform the security detection in this report was the Process Monitor tool which was suggested (Russinovich, 2021) which allowed capturing of real-time changes in the windows registry database. The ProcMon tool allowed capturing the changes only when specified thereby allowing our research to specifically determine only the results for the intrusion that was conducted. The process monitor displayed only the relevant registry keys which were affected during the intrusion demonstration also the results displayed could also be filtered to display only the most relevant keys from the Windows registry for evidential data.

To compare the changes made by either the user activity or malicious attacks performed either by software or hardware-initiated attacks were checked and performed using the RegShot tool which was suggested and used in the forensics research (Farmer, 2013). The tool allowed taking snapshots of the windows registry before and after for any intrusion demonstrations and specified only the changes in the keys of the registry database based on the type of intrusion which allowed easier analysis of the changes made to the Registry. Other tools that were suggested for the research such as the ERUNT tool that was used to perform offline extraction of the registry hive files for analysis, not only did it allow extracting of data but also the extracted registry files could be used to perform a backup and restore which reverted any changes in the registry which resolved any errors that had occurred while a demonstration of intrusion analysis. As concluded by Farmer “Based on the using the registry activity on a Windows system, we were able to label all processes as either attacks or normal, with relatively high accuracy and low false-positive rate, for the experiments performed in the study”. (Roy, 2012) explains the various Registry locations that store the information of USB devices when installed on a Windows-operated system. The information that could be retrieved for the hardware devices was available via the setupapi.log file located in the system folder of the Windows explorer. With the log file, the specific information of the USB device was available which could be used as a filter for searching the relevant keys in the ProcMon tool. All information that was related to the USB drive was available starting from the device installation info to the last date and time of the device removed from the system that helped in concluding whether the Malicious activity was done through the specific USB drive or not. Roy also suggested that the Windows Registry provides every detailed information of the USB drive and can be identified as the culprit for the crime as per the comparison of information extracted from the registry with the drive information given from the device.

III. TOOLS AND PROCESS

A. *ERUNT Tool*

It stands for Emergency Recovery Utility NT. It's a tool for backing up and restoring the Windows Registry. This tool will back up and restore the Windows Registry in its entirety, including the protection hive, ensuring that permissions are properly backed up and restored.

One of the issues with the Registry is that the resources offered by Windows are insufficient for backing it up. For example, Regedit's "Export registry" feature is not useful for creating a full registry backup. It doesn't export the entire registry (no details from the "SECURITY" hive, for example), and the exported file can't be used to replace the new registry with the old one later. Instead, re-importing the file merges it with the existing register without removing anything added after the export, leaving you with a jumble of old and new entries.

System Restore is another method that backs up the Registry. Though this tool is much more useful for backing up and restoring data than Regedit, it is still vulnerable to malware that can disable System Restore and erase all of your restore points.

B. *RegShot Tool*

It not only lists the changes but also goes into great detail about which keys were changed as a result of modifying your screen context. This is helpful if you want to manually access certain buttons. Regshot is an excellent tool for comparing the number of registry entries that have been modified after an upgrade or a change in your device settings. Although most PC users would never need to do this, it is a useful method for troubleshooting and keeping track of your registry.

Regshot is a SourceForge-hosted open-source (LGPL) project. M. Buecher, XhmikosR, and TiANWEi built and registered it in January 2001. It has been changed and updated several times since its introduction to enhance its functionality.

C. *Process Monitor Tool*

Process Monitor is the free monitoring tool for windows that help in monitoring the file system, Registry, and process/thread activity in windows. When the process monitoring system is run on the system it helps in capturing all the system events like the session ID, user names, reliable process information, full thread stacks, logging to a file, and much more.

It is used to detect the attempt that fails to read, write the registry keys and record all the action attempt against the Microsoft Windows Registry, it also allows for filtering on specific keys, processes, process IDs, and values.

Through Process Monitor we can observe, view, and capture windows files, registry key activity, network activity, profile events, process, thread activity, and system activity in real-time. We can use it as our own and combine it with other tools to create an automatic monitoring system.

D. *Windows Registry Back-up*

The Windows Registry database can be backed up using the default windows registry editing tool known as Regedit but the backup feature of Regedit allows only backing up of certain hive files of the registry thereby its limitation doesn’t provide a feasible method of backing up of the Registry.

The ERUNT tool allows the whole backing up of the Registry database even when the Registry is extracted from an offline system. The backup can even be performed as per user specifications such as backing up of only a few hive files.

E. Windows Registry Modifications with Regedit

The Windows Operating System since the Vista version has introduced the default Registry editor known as the Regedit which can be simply accessed by typing the keyword ‘Regedit in the run command box.
The Regedit app provides a unique set of functionalities that can allow users to alter, modify delete, or even backup the Registry database with user preferences. The Regedit displays the entire Windows Registry in a tree-based hierarchical structure whereby the user can specify the registry that is to be modified by simply locating the subkey within the registry structure.

F. Security Auditing on User activity logs

The user activities that are performed on a Windows Operating system are audited with the help of the Process Monitor tool which allowed capturing of registry changes in real-time whenever any modifications are made to the system.

The following common actions which users usually perform were analyzed and checked to know whether certain actions were performed or not.

- Run command: The shortcut commands that were used to open certain applications or directories
- Browser typed URLs: the URL of websites that were accessed by the user
- Search history in Windows Explorer: Any searches that were performed in the Windows File explorer
- Start-up Objects: The various applications that are set to run on start up
- Last accessed registry key: Log information on the last modified registry key by the user
- Last uploaded directory in browser: The recent directory that was uploaded through the Internet Browser

G. Restoration of the Windows Registry

The restoration of the Windows Registry can be done by either with the regedit tool or the ERUNT tool. The regedit application does not allow the whole registry database to be restored as certain processes that are running cannot be modified as it can lead to system failure. The ERUNT tool features backing up and restoration of the whole registry database whereby the restoration is completed on the next reboot of the system.

IV. RESULT AND DISCUSSIONS

A. Gathering of Security Auditing Tool

The various tools that were suggested in few research papers that are related to the report were mostly infeasible as most of the tools were legacy-type tools that were compatible only with older versions of the Windows Operating system. The tools that were feasible for the following report are the ones that were mentioned & explained earlier.

Also, in order for the Security Audit to be conducted, learning the usage of those tools became a prerequisite as each tool had its user manual teaching the basic information on how to use the tool and its features. The Process Monitor tool was capable of capturing real-time registry changes but the process monitor was not efficient in terms of intrusion detection method as with each capture of Registry data, the RAM usage of the system would exceed tremendously.

The RegShot Application provided a better filter for registry changes which allowed easier analysis of the Registry. Not only does the RegShot provide a comparison study but also had the feature of restoring the Windows Registry with the help of a snapshot that was taken by the tool.

ERUNT tool is a reliable tool for restoration of the Windows Registry database as it provided the function of restoring the whole registry database, unlike the Regedit which does not allow restoration of the currently running system processes. On reboot, the ERUNT tool restores the system changes to their earlier state with the backup it had created of the registry database.

B. Evidences gathered from User activity log

When the registry keys are modified or deleted, the changes to the system due to the modifications can be seen in real-time. Not only that but when system changes are made on the Windows Operated system, the Registry database is also modified as per the system changes made. (Dashora, Tomar and Rana, 2010) stated that Computer forensics is the analysis of a computer device or network that is suspected of being used in illegal activity. The investigation's main goal is to discover data and facts relevant to the case under review or research the inquiry focuses on "convicting information present in the system" and "entry points for the convicting information. The Windows Forensics Process examines the evidence collected during the operation of the operating system. These traces can be found in Event Logs, Slack Space, Windows Registry, and Temporary Files, among other places.

The Windows Registry keeps track of recently accessed files/folders, user's preferences. Windows Registry also includes valuable details about the applications installed on the device. Keeps track of the user's actions, which is crucial for forensics. Some keys in the registry are application-specific, while others are generic. The registry contains a number of essential keys, including the following:

C. Run Command input logs

This Registry Key keeps track of the commands you've recently typed in the Run window. This data is crucial for the investigation of a computer forensics operation.
Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU

D. Start-up Objects

These are the objects that are set to start automatically when Windows starts. This data is kept in a number of registry hives.
Computer\HKCU\\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

E. Last accessed key in Registry

This key gives the information about what registry key was accessed last time.
Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Applets\Regedit

F. Internet Explorer Typed in Address

This key gives the user information about what were the typed in websites from the Internet Explorer Address Bar.
Computer\HKEY_CURRENT_USER\Software\Microsof t\Internet Explorer\TypedUrls

G. Last Saved Directory in Internet Explorer

This key gives the user information about in which folder was the last downloaded file saved.
Computer\HKEY_CURRENT_USER\Software\Microsof t\Internet Explorer – Download Directory.

V. Conclusion

With the help of various open-source tools that were mentioned and demonstrated above provided a feasible means for conducting a security audit over a Windows Operated system through the windows registry database. The findings of the research proved to be a beneficial resource for forensic investigators as most investigators are unaware of the information that can be availed from the windows registry. Though understanding the values of the keys in the registry can be a difficult task as well but if the evidence can be gathered from the specified file paths from the registry, then any forensic investigation can acquire valid evidence from the Security audits if conducted.

Commonly used commands such as the Run, Win explorer search, browser search history, etc are also some of the useful locations for extracting beneficial evidence for forensic analysis. With each of these pieces of evidence, conclusions can be drawn on whether the user performed any malicious activity or not.

The USB device information that can be obtained from the registry with the help of the auditing tools was beneficial as such information can be used to deduce whether the drive is the culprit for the cybercrime or not. Not only USB devices but also any other devices that are connected to the system can be identified with the help of the evidential information that can be extracted from the registry.

Also, for any system failures and registry errors, Using the ERUNT tool to perform an initial full backup of the registry then restoration of the backup can remediate any system errors, as well as recovery of data, can be possible if the backup of the registry contains the data which was undeleted then.

References

[1] Alghafli, K. A. (2009). Forensic Analysis of the Windows 7 Registry. Perth. Australia: Edith Cowan University.
[2] Apap, F. (2003). Detecting Malicious Software by Monitoring Anomalous Windows Registry Accesses. New York: Columbia University.
[3] Bots, G. (Director). (2018, March 4). Windows 10 Create and Edit Registry File [Motion Picture].
[4] Carvey, H. (2011). Windows Registry Forensics. Burlington: Elsevier Incorporated.
[5] Dashora, K. (2010). A Practical Approach for Evidence Gathering in Windows Environment. Bhopal, India: International Journal of Computer Appliances.
[6] Farmer, D. J. (2013). A Forensic Analysis of the Windows Registry. Retrieved from Corradoroberto: https://secure.corradoroberto.it/doc/Registry_Forensics.pdf
[7] Izhar, S. (2018, May 22). USB Forensics: Find the History of Every Connected USB Device on Your Computer. Retrieved from CYBRARY
[8] Khan, K. A. (Director). (2016, December 31). How to Delete Search History Directly from Registry [Motion Picture].
[9] Russinovich, M. (2021, April 21). Process Monitor. Retrieved from Microsoft: https://docs.microsoft.com/en-us/sysinternals/downloads/procmon
[10] Shaver, J. S. (2015). Exposing Vital Forensic Artifacts of Usb Devices in The Windows 10 Registry. Monterey, California: Naval Postgraduate School.
[11] TechHut (Director). (2020, June 15). How to Backup Registry in Windows 10 [Motion Picture].
[12] Yadav, A. (2020, March 18). Registry Forensics. Retrieved from Tutorials point: https://www.tutorialspoint.com/registry-forensic