Exercise 12

16/11/2021

Windows Registry Forensics

The registry is a database of stored configuration information about the users, hardware, and software on a Windows system. It can be a treasure trove of evidence of what, where, when, and how something occurred on the system. The registry was designed to configure the system, but to do so, it tracks a plethora of information about the user's activities, the devices connected to system, what software was used and when, etc. All these can be useful for the forensic investigator. The registry on a Windows system varies a bit from version to version. A skilled, professional digital forensic investigator needs to be able to work with nearly all versions of Windows and other operating systems.

Inside the registry, there are root folders. These root folders are referred to as hives. There are five registry hives.

HKEY_USERS: contains all the loaded user profiles

HKEYCURRENT_USER: profile of the currently logged-on user

HKEYCLASSES_ROOT: configuration information on the application used to open files

HKEYCURRENT_CONFIG: hardware profile of the system at start-up

HKEYLOCAL_MACHINE: configuration information including hardware and software settings

Information that can be found in the registry includes:

1) Users and the time they last used the system
2) Most recently used software
3) Any devices mounted to the system including unique identifiers of flash drives, hard drives, phones, tablets, etc.
4) When the system connected to a specific wireless access point
5) What and when files were accessed
6) A list of any searches done on the system
7) And much, much more

Exercise

1) Many hackers crack a local wireless access point and use it for their intrusions. In this way, if the IP address is traced, it will lead back to the neighbour's or other wireless AP and not them. However, evidence about wireless can be got from the registry. The forensic investigator simply has to look in the registry for

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles

There, you will find a list of GUIDs of wireless access points the machine has been connected to. When you click on one, it reveals information including the SSID name and the date last connected in hexadecimal.

2) The "RecentDocs" key tracks the most recent documents used or opened on the system by file extension. It can be found at:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

3) When the user types a URL in Internet Explorer, this value is stored in the registry at:

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs

When we open that key in the registry, it lists the last URLs that the user visited with Internet Explorer. This could reveal the source of malicious malware that was used in the breach, or in civil or policy violation types of investigations, may reveal what the user was looking for/at. The registry also tracks the IP addresses of the user interfaces. Note that there may be numerous interfaces and this registry key tracks each interface's IP address and related information.

HKEY_LOCAL_MACHINE\System\Services\CurrentControlSet\services\Tcpip\Parameters\Interfaces

We can find the IP address assigned to the interface, the subnet mask, and the time when the DHCP server leased the IP. In this way, we can tell whether the suspect was using that particular IP at the time of the intrusion or crime.

4) As a forensic investigator, we often need to find what applications or services were set to start when the system starts. Malware is often set to start each time the system restarts to keep the attacker connected. This information can be located in the registry in literally tens of locations. Probably the most used location is:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

Any software/locations designated in these subkeys will start every time the system starts. Rootkits and other malicious software can often be found here and they will start each time the system starts. If the hacker just wanted the software to run once at start up, the subkey may be set here.

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce

5) Often, the suspect will use a Flash drive or hard drive for their malicious activities and then remove them so as not to leave any evidence. The skilled forensic investigator, though, can still find traces of evidence of those storage devices within the registry, if they know where to look.

How would we find evidence that a USB storage device was inserted and used? To find evidence of USB storage devices, we want to look at the following key.

HKEY_Local_Machine\System\ControlSet00x\Enum\USBSTOR

In this key, we will find evidence of any USB storage device that has ever been connected to this system. Expand USBSTOR to see a listing of every USB storage device ever connected to this system.

If the suspect used any hardware device that must be mounted to either read or write data (CD-ROM, DVD, hard drive, flash drive, etc.), the registry will record the mounted device. This information is stored at:

HKEY_LOCAL_MACHINE\System\MountedDevices

Refer https://forensicswiki.xyz/wiki/index.php?title=Windows_Registry for more details about the registry and also tools to use it.

Use the tool **regedit** available in Windows and then search for the keys mentioned above. Include screenshots in your submission.