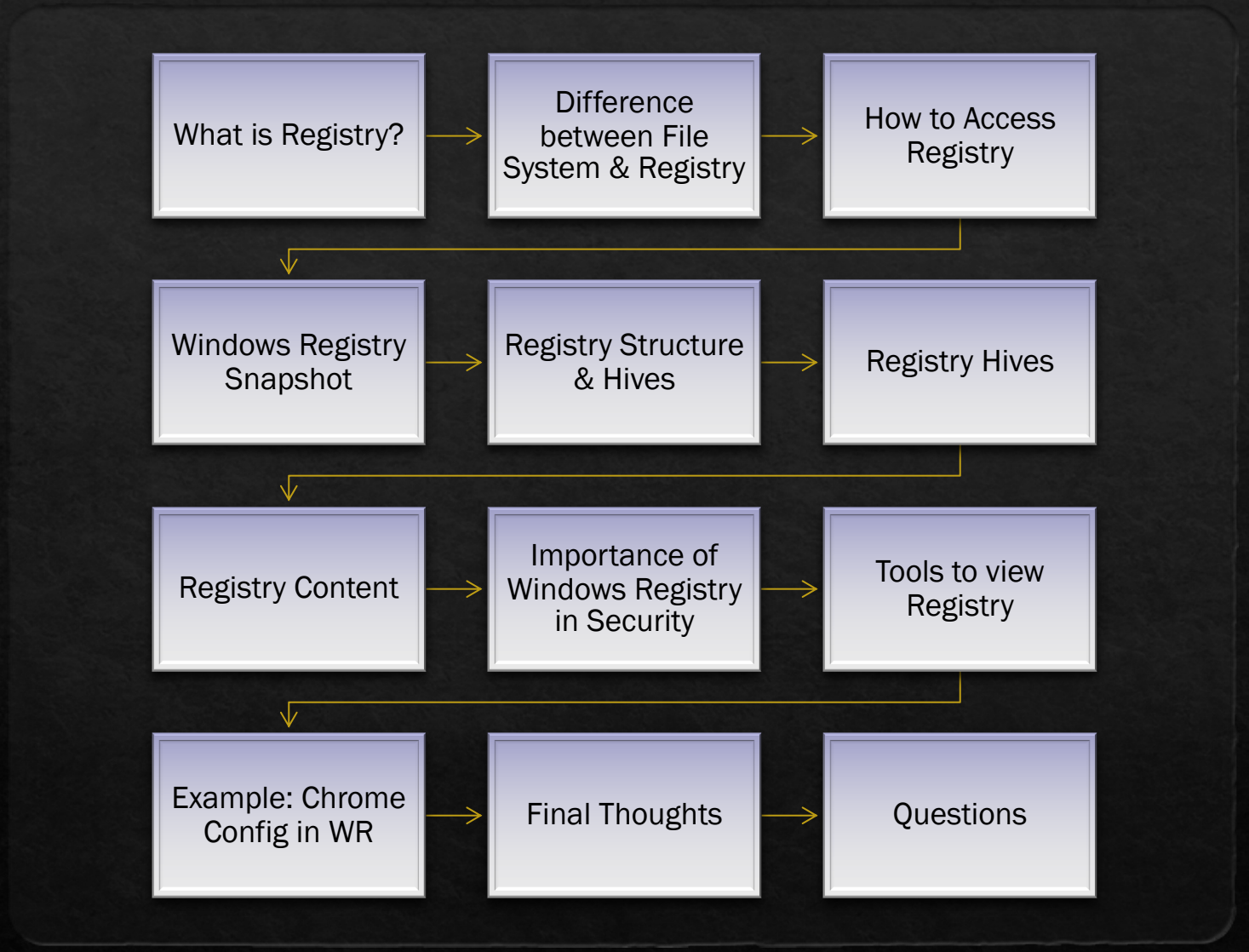
Windows Registry

By

Aastha Sahni

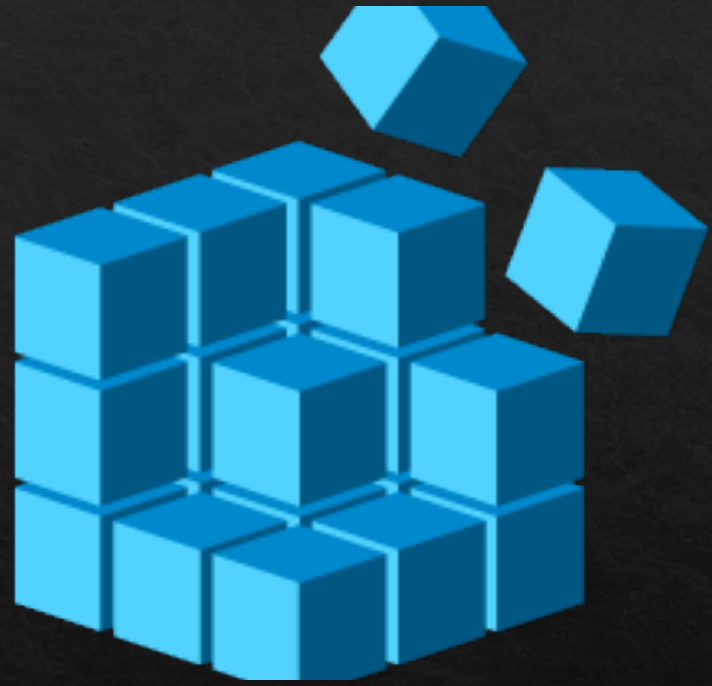
Agenda


What is Registry?
Difference between File System & Registry
How to Access Registry
Windows Registry Snapshot
Registry Structure & Hives
Registry Hives
Registry Content
Importance of Windows Registry in Security
Tools to view Registry
Example: Chrome Config in WR
Final Thoughts
Questions

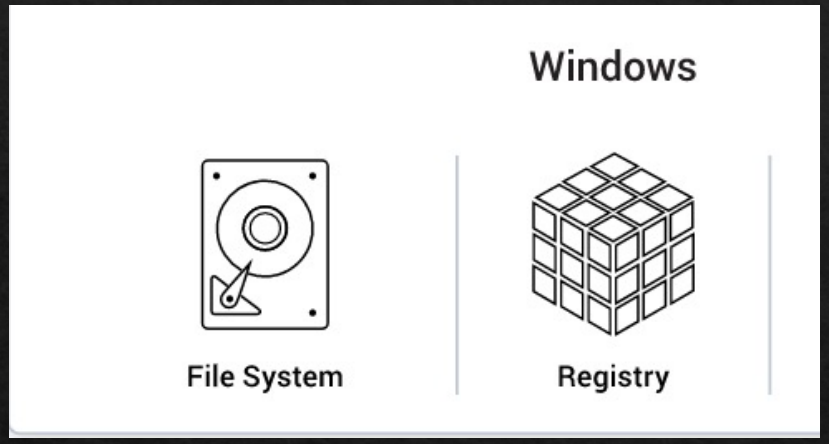
What is Registry?

- A central hierarchical database used in Windows used to store information that is necessary to configure the system for one or more users, applications, and hardware devices.
- The Registry contains information that Windows continually references during operation, 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.

- Microsoft Documentation



Difference between File System & Registry



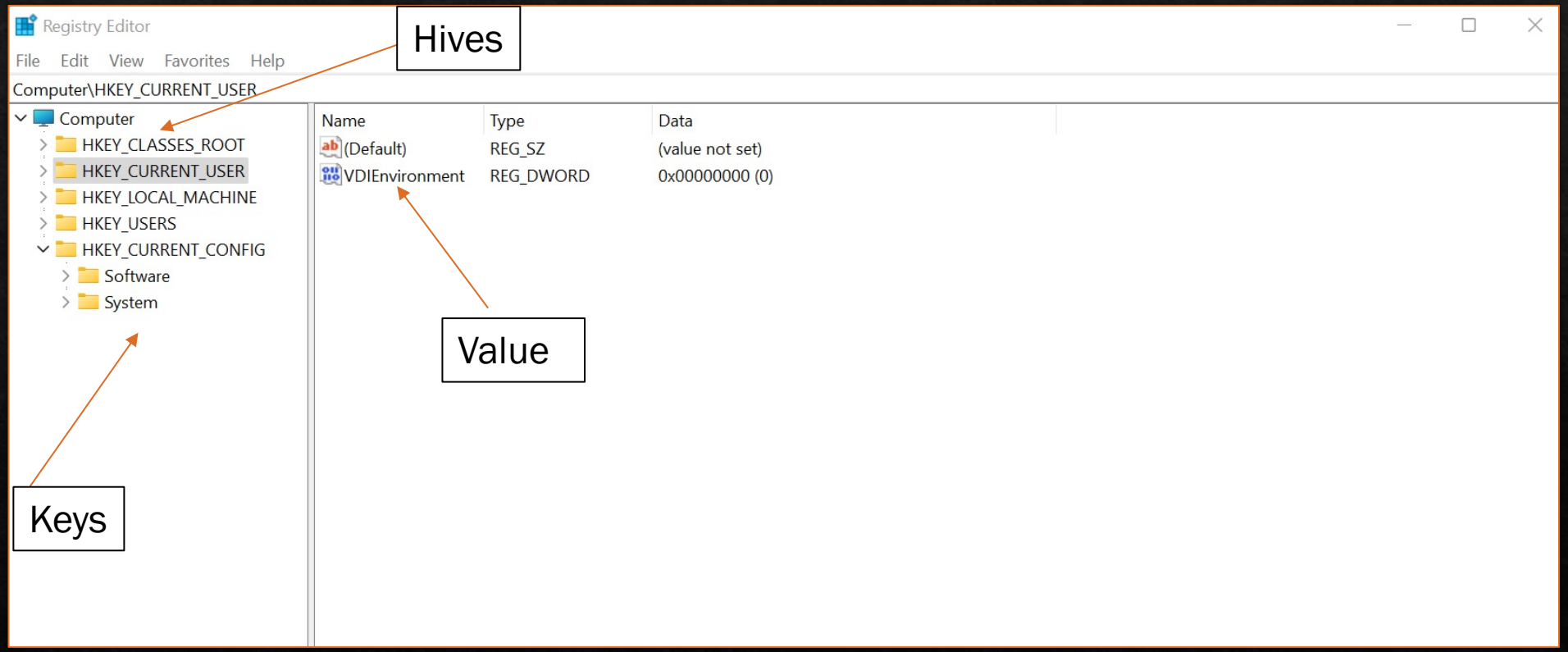
- The windows registry is like a file system.
- A file system has files and folders whereas registry has keys and within keys we have either more keys or key -value pairs, storing information.
- Registry cannot be access by any user, it requires admin access!

How to Access Registry

To access windows registry, run utility **regedit.**

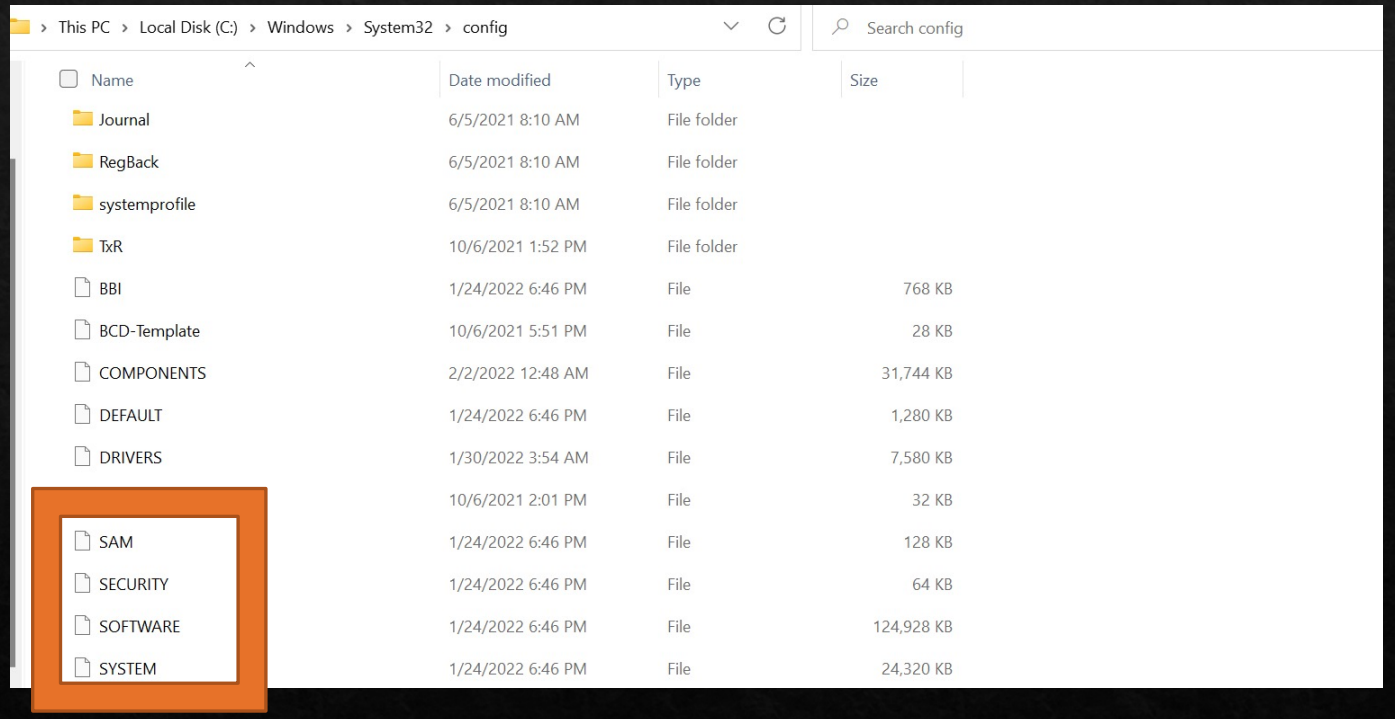
It is a graphical tool that lets you view and monitor the Windows operating system’s registry and edit if necessary.

Windows Registry



Registry Files

C:/windows/system32/config/

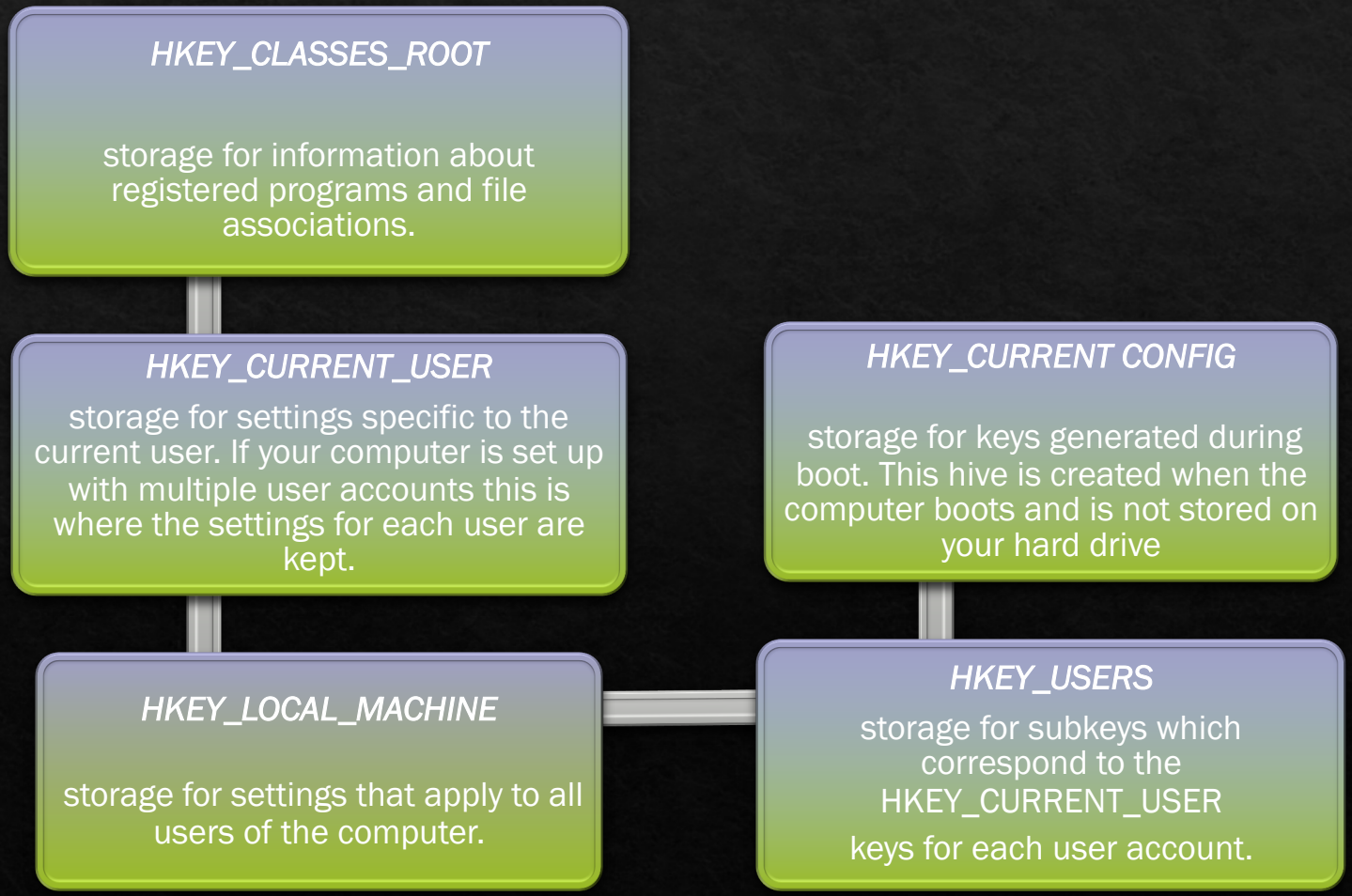


Registry Structure & Hives

Components of Windows Registry

- Hives
- Root Keys
- Keys
- Sub-Keys
- Value

Registry Hives



Registry Content

The registry stores critical system information about user, system and installed applications.

- Operating system information - build number, version user and registered user.
- Information about properly installed applications
- Installed services
- Maps network addresses to host machines
- Security information - trojan, ransomware, malware

Importance of Windows Registry in Security.

Windows registry is a great source of forensic evidence.

- Images of windows registry are extracted for more detailed analysis of incident by DFIR teams.
- Identifying malware and ransomware information for forensic analysis
- Tools for extracting detailed information which otherwise not possible with usual editor.
- Window Registry is often used by attackers to hide malwares and APTs

Tools to Access Windows Registry

- RegScanner
- RegistryChangesView
- RegFromApp
- RegDllView
- ActiveXHelper
- RegFileExport

Where to find these tools https://www.nirsoft.net/

Example: How attackers can misuse Registry

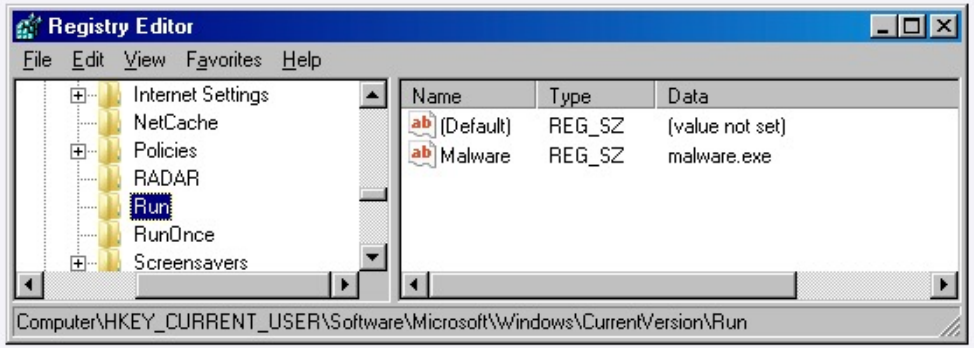


Figure 1: A malicious actor creates a value in the Run key

At a later point in time the malware is removed from the system. The registry value is overwritten before being deleted.

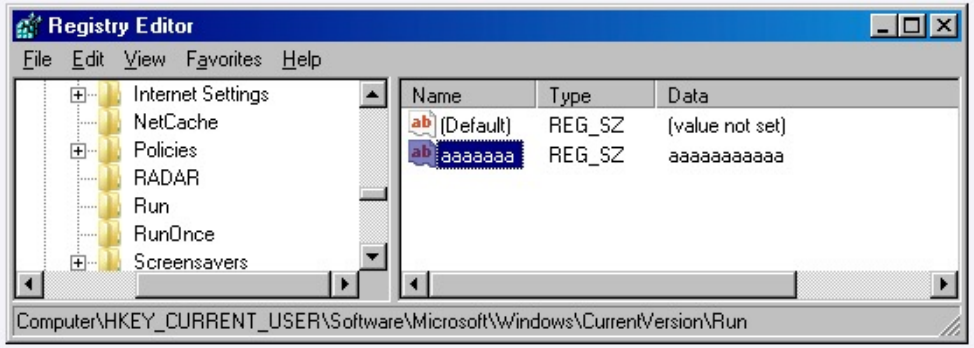


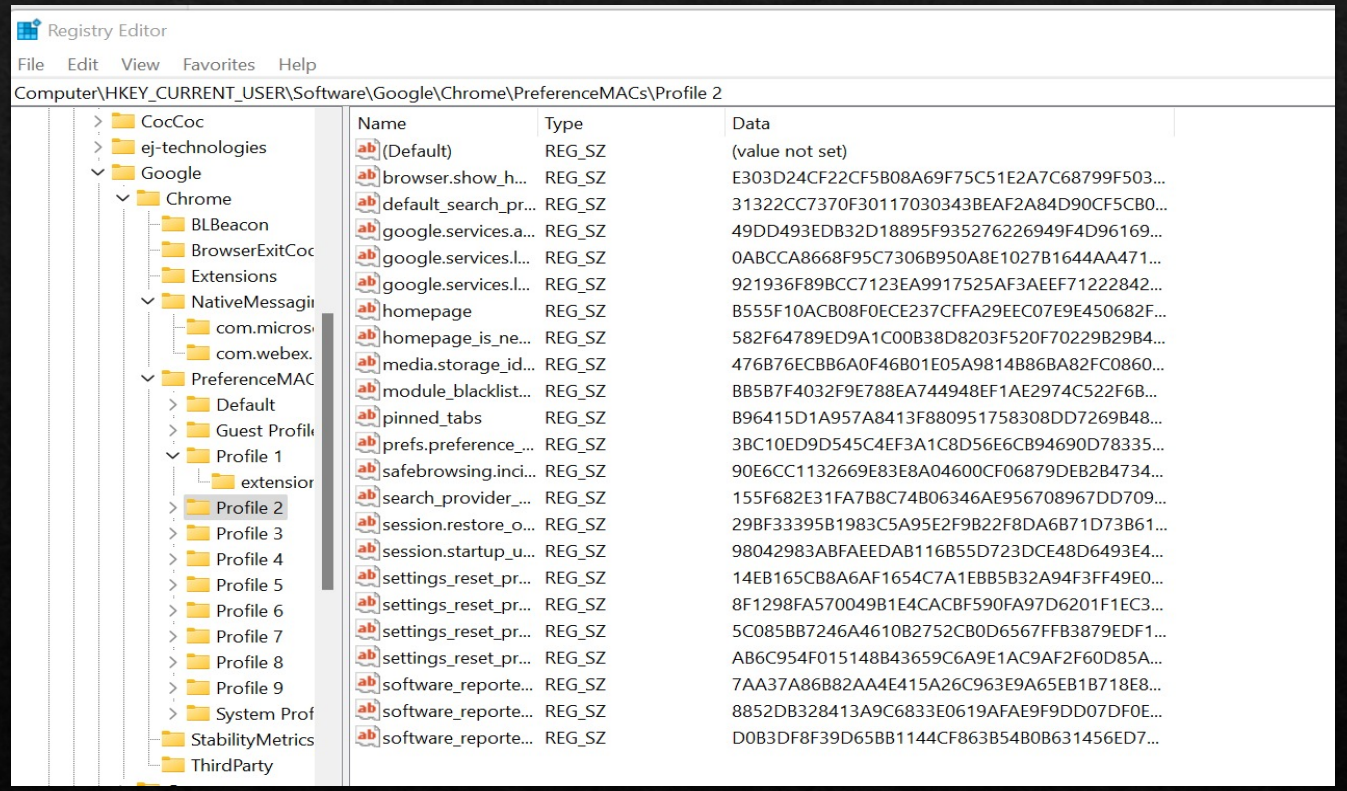
Figure 2: The malicious value is overwritten and deleted

Example: Chrome Config in WR

To check your Chrome setting you can go to:

1. Type Regedit in your search

2. It will open the windows registry and HKEY_CURRENT_USER\Software\Google\Chrome contains the Chrome settings



Final Thoughts!

Can we change settings in Windows Registry?

YES !!!!!!! If you know what you are doing and carefully changing values, there should not be and problem.

BUT - If you starting editing, deleting or adding registry keys with no proper knowledge you might damage you whole windows installation

Questions

References

- https://docs.microsoft.com/en-us/troubleshoot/windows-server/performance/windows-registry-advanced-users
- https://www.nirsoft.net/
- https://medium.com/@lucideus/windows-registry-forensic-analysis-part-1-windows-forensics-manual-2018-2cb4da210125
- https://docs.microsoft.com/en-us/troubleshoot/windows-server/performance/windows-registry-advanced-users
- https://www.mandiant.com/resources/digging-up-the-past-windows-registry-forensics-revisited

Questions