# Windows Registry Attacks Cheat Sheet

The Windows Registry Editor, commonly referred to as **regedit**, is a graphical tool in the Microsoft Windows operating system that allows authorized users to view and modify the Windows registry. The registry itself is a hierarchical database that stores configuration settings and options for the operating system, including information about hardware, software, user preferences, and system settings. Here is a table summarizing the function and description of each HKEY hive in the Windows Registry:

| **HKEY Hive** | **Function and Description** |
|---|---|
| **HKEY_CLASSES_ROOT (HKCR)** | This hive contains information about registered applications, including file associations and OLE Object Class IDs that tell Windows which programs to use for opening specific files. It merges data from `HKEY_LOCAL_MACHINE\Software\Classes` and `HKEY_CURRENT_USER\Software\Classes`, prioritizing user-specific settings over system defaults |
| **HKEY_CURRENT_USER (HKCU)** | This hive stores configuration information related to the currently logged-in user, including personalized settings like desktop background, screensavers, and application settings. It is dynamically linked to a specific subkey in `HKEY_USERS` that corresponds to the user |
| **HKEY_LOCAL_MACHINE (HKLM)** | This hive contains configuration data that applies to the computer regardless of who is logged in. It includes information about the system's hardware, installed software, security settings, and other system-wide settings . |
| **HKEY_USERS (HKU)** | This hive includes subkeys corresponding to each user profile on the system. Each subkey contains the same type of information as `HKEY_CURRENT_USER` for each user. It serves as a master list of user settings on the computer |
| **HKEY_CURRENT_CONFIG (HKCC)** | This hive contains information about the hardware profile that is currently in use by the system. It is used primarily for system configuration details such as which hardware profile is active |

This table provides a simplified overview of the primary functions and roles of each major registry hive in the Windows operating system.

Registry hives are logical containers within the Windows Registry, designed to group related information together. Each hive contains a specific set of keys, subkeys, and values, organizing configuration data in a way that supports the management of system and user settings. Hives play a crucial role in the functioning of Windows by organizing and storing configuration data, making it easier to manage and troubleshoot system and user settings.

Here's a detailed table summarizing the top 20 different examples of **Windows Registry attacks**, outlining the purpose of each attack and providing specific details along with examples of how each is executed:

| Attack Purpose | Detail of Execution | Example of Execution |
|---|---|---|
| Persistence of Kovter Malware | Kovter writes its code directly into the Registry to ensure it executes upon system startup. | Kovter modifies `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` to execute its script each time the computer boots. |
| Malware Installation via Fake Update | A fake Adobe Flash update pop-up writes malicious code into the Registry, which then executes further harmful scripts. | A user clicks on a pop-up, leading to a Registry change at `HKCU\Software\Classes\clsid` that triggers malware execution. |
| Privilege Escalation via Service Modification | Modifies the `ImagePath` registry key under services to redirect a legitimate service to execute a malicious binary. | An attacker changes `HKLM\System\CurrentControlSet\Services\svcname\ImagePath` to point to a malicious executable. |
| Remote Access via RAT Installation | Installs RATs and modifies the Registry to ensure the RAT executes at every system start. | A RAT modifies `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` to add itself, ensuring it runs on startup. |

| | | |
|---|---|---|
| Ransomware Activation (Ryuk) | Ryuk ransomware modifies run keys to load the ransomware during system startup. | Ryuk adds a new value in `HKLM\Software\Microsoft\Windows\CurrentVersion\Run` to execute its encryption routine. |
| Anti-Forensics via System Restore Manipulation | Alters Registry settings controlling System Restore to hide malicious activities or prevent recovery from backups. | Malware modifies `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore` to disable System Restore functionality. |
| Disabling Security Tools | Modifies registry keys associated with antivirus software to disable it. | Malware sets the `HKLM\Software$$Antivirus Name]\RealTime Protection` key to `0` to turn off antivirus protection. |
| User Logon Hijacking | Changes `UserInit` or `Shell` keys to execute malicious scripts at user logon. | Malware modifies `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit` to include a malicious script. |
| Early Malware Execution | Adds entries to `BootExecute` to execute malware before the operating system fully loads. | A rootkit adds itself to `HKLM\System\CurrentControlSet\Control\Session Manager\BootExecute` for early system execution. |

| | | |
|---|---|---|
| Persistence via Startup Folder | Adds links to malicious programs in the Startup folder through the Registry. | Malware adds a new entry in `HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders` pointing to its executable. |
| Fileless Malware Execution | Uses registry keys to store and execute next-step code for malware after initial deployment. | A fileless virus stores its payload in `HKCU\Software\Classes\clsid` and schedules execution using WMI events. |
| DLL Hijacking | Replaces a legitimate DLL file with a malicious one by modifying the registry to point to the bogus DLL. | An attacker modifies `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\SharedDLLs` to load a malicious DLL instead of the legitimate one. |
| Command Interception via PATH Modification | Modifies the PATH environment variable in the Registry to redirect the execution of legitimate commands to malicious executables. | Malware appends a malicious directory to `HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Environment\Path`. |
| Service Hijacking via Weak Permissions | Exploits weak permissions on service-related registry keys to launch malicious code when a service starts. | An attacker grants themselves modify permissions on `HKLM\System\CurrentControlSet\Services\svcname` and changes the service binary path. |

| | | |
|---|---|---|
| Credential Dumping via SAM Keys | Dumps the Security Account Manager (SAM) database from the registry to extract password hashes. | Tools like Mimikatz modify `HKLM\SYSTEM\CurrentControlSet\Control\Lsa` to dump credentials stored in the SAM. |
| Data Hiding in Registry | Stores malicious payloads in the Registry to evade detection by signature-based security software. | Malware hides its data in `HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache`. |
| Lateral Movement Preparation | Modifies or deletes registry keys to disrupt normal system operations or to prepare the system for further attacks. | An attacker deletes `HKLM\Software\Policies\Microsoft\WindowsFirewall\DomainProfile` to disable firewall rules before moving laterally. |
| Information Gathering via Registry | Remotely queries the registry to gather information about installed remote access tools. | An external script queries `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall` to find installed software for exploitation. |
| Evading Application Whitelisting | Uses the registry to bypass application whitelisting by modifying keys that control which applications can run. | Malware modifies `HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers` to whitelist its executable. |
| Malware Configuration Storage | Stores configuration settings for malware in the Registry to maintain flexibility and stealth. | A Trojan stores its C&C server addresses in `HKCU\Software$$Malware Name]\Settings` to dynamically update its behavior. |

This table provides a comprehensive overview of the diverse and sophisticated ways in which attackers can leverage the Windows Registry to conduct malicious activities, emphasizing the need for vigilant monitoring and robust security measures to protect against such threats.