User-spezifische Computernutzung tracken

Valentin Lekov
Friedrich-Alexander-Universität
Erlangen-Nürnberg (FAU)

ABSTRACT

Mit der erhöhten Nutzung von elektronischen Geräte, gibt es auch eine erhöhte Anzahl von Cyberangriffen. Und nach jedem Cyberangriff gibt es Spuren, die hintergelassen werden, selbst wenn sie nicht leicht sichtbar sind. Die Windows Registry, eine Kernkomponente des Windows-Betriebssystem, ist die zentrale hierarchische Datenbank, die eine beträchtliche Menge an Konfigurationsinformationen über das System und seine Programme enthält. Es enthält auch historische Informationen zu den Benutzern, wie z.B. USB-Aktivitäten, zuletzt besuchte Webseiten, zuletzt aufgerufene Dateien, zuletzt verwendete Programme usw. Die Registry besteht aus mehreren Gruppen, die als Hives bezeichnet werden und jedes Hive besteht aus Schlüsseln, Unterschlüsseln und Werten. Mit digitaler Forensik, die ein Prozess zur Wiederherstellung und Untersuchung von Materialien in elektronischen Geräten ist, können viele Informationen über Benutzeraktivitäten extrahiert werden. Diese Informationen können manchmal entschiedend sein, um die Beteiligung eines Benutzers an einer bestimmten Cyberkriminalität zu beweisen oder zu wiederlegen.

KEYWORDS

Digitale Forensik, Windows Registry, Historische Informationen, Registry Editor, PowerShell, UserAssist, ExecutedProgramsList, RegRipper

1 EINLEITUNG

Dieses Paper soll einen überblick über die Arten historischer Informationen in der Windows Registry und deren Extraktion geben. In Abschnitt 2 sollen Hintergründe geklärt werden, welche für dieses Paper wichtig sind. In Abschnitt 3 werden die verschiedene Arten von historischen Informationen aufgezählt und es wird gezeigt, wo man diese Informationen im Registry finden kann. Der vierte Abschnitt beschäftigt sich mit den Werkzeuge und Methoden, die zur Extraktion von historischen Informationen benutzt werden können.

2 HINTERGRÜNDE UND GRUNDLAGEN

Während der Schwerpunkt dieses Papers ist, die verschiedenen Arten historischer Informationen zu zeigen und wie sie extrahiert werden können, sind einige Hintergrundinformationen erforderlich, um zu verstehen, wo und warum sie gespeichert werden. Daher finden Sie in diesem Abschnitt eine grundlegende Erläuterung der Windows Registry, sowie einige Tools zur Datenextraktion.

2.1 Windows Registry

Das Windows Registry ist eine zentrale hierarchische Datenbank zum Speichern von Informationen, die zur Konfigurieren des Systems für einen oder mehrere Benutzer, Anwendungen und Hardwaregeräte erforderlich ist [1].

Der obere Teil der Windows Registry besteht aus fünf Einträgen, sogenannte Hives [2]. Wie in **Abbildung 1** gezeigt wird, sind die

Hives *HKEY_LOCAL_MACHINE (HKLM)* und *HKEY_USERS (HKU)* die einzige richtigen Wurzeln. Während die anderen drei Hives nur Links zu bestimmten Schlüsseln der richtigen Wurzeln [2] sind.

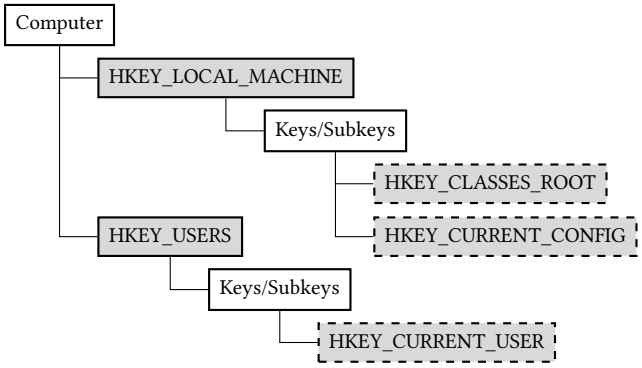

Abbildung 1: Struktur der Windows Registry

In der Windows Registry werden zahlreiche Informationen zu den Aktivitäten der Benutzer erfasst, die später für einen forensischen Analysten von Vorteil sein können. Solche Benutzeraktivitäten umfassen:

- USB-Aktivitäten
- zuletz besuchte Webseiten
- zuletz aufgerufene Dateien
- zuletz verwendete Programme usw. [1]

2.2 Werkzeuge zur Datenextraktion

In dieser Abschnitt werden verschiedene Werkzeuge zur Datenextraktion aufgezählt und erklärt.

2.2.1 Registry Editor. Das am häufigsten verfügbare Tool zum Anzeigen und Ändern des Inhalts des Windows Registry ist der Registry Editor, auch als *regedit* bezeichnet [1]. Diese Editor bietet ein grafiches Interface und wird mit allen Windows-Installationen verteilt [1]. Der Registry Editor bietet auch die Möglichkeit, alle Einträge der Registry einfach in eine Registry-Data-Datei (*.reg*) zu exportieren.

Teile des Windows Registry, die über Registry Editor sichtbar sind, sind "flüchtig"[1]. Dies bedeutet, dass sie beim Booten des Systems oder beim Anmelden eines Benutzers ausgefüllt werden und beim Herunterfahren des Systems nicht auf der Festplatte gespeichert werden [1]. Ein Beispiel für flüchtige Daten ist das Hive *HKEY_CURRENT_USER* [1].

2.2.2 PowerShell. Die PowerShell ist eine aufgabenbasierte Befehlszeilen-Shell und Skriptsprache, die speziell für Systemadministratoren entwickelt wurde [2]. Die PowerShell basiert sich auf .NET Framework und hilft IT-Fachleuten, die Verwaltung des Windows-Betriebssystems und der darauf ausgeführten Anwendungen zu steuern und zu automatisieren [2].

Der Basisbefehl in PowerShell besteht aus einem Cmdlet im Format Verb-Noun, z. B. *Get-File* [2]. Im Gegensatz zu herkömmlichen Befehlszeilenschnittstellen sind die Cmdlets von PowerShell für den Umgang mit Objekten ausgelegt [2].

2.2.3 UserAssist. UserAssist [7] ist ein hilfreiches Programm, das von Didier Stevens entwickelt wurde. Dieses Programm wird benutzt, um alle zuletzt verwendete Programme anzuzeigen und es gibt Informationen darüber wie oft ein Programm ausgeführt und wann es zuletzt ausgeführt wurde.

2.2.4 ExecutedProgramsList. Ein weiteres hilfreiches Tool zum Extrahieren aller zuletzt verwendeten Programmen ist *ExecutedProgramsList*. Im Vergleich zu UserAssist zeigt ExecutedPrograms-List mehr Programme an, die zuletzt ausgeführt wurden, sowie mehr Informationen zu jedem dieser Programme (z.B. wann es erstellt wurde, wann es zuletzt geändert wurde usw).

2.2.5 RegRipper. RegRipper ist ein SSuperparser"für die Windows Registry [1]. Es ist ein Framework, das verschiedene Plugins (einzeln oder in Gruppen) ausführt, wobei die Plugins verwendet werden, um bestimmte Daten nach Bedarf zu extrahieren und die Ergebnisse dann dem Analysten angezeigt werden [1].

3 ARTEN VON HISTORISCHEN INFORMATIONEN

Eine Schlüsselaufgabe bei Untersuchungen ist es zu bestimmen, welche Dateien, Ordner oder Softwareanwendungen zuletzt verwendet wurden [5]. Diese Fähigkeit zu zeigen, dass eine Person eine Datei geöffnet, gespeichert oder gesucht hat, kann beweisen, dass der Verdächtige diese Datei kennt [5].

Diesen Abschnitt beschäftigt sich mit den verschiedenen Arten von historischen Informationen, sowie deren Stellen in dem Windows Registry.

3.1 Installierte Programme

Diese Art von historischen Informationen zeigt welche Programme auf dem System installiert sind [4, 5]. Eine solche Stelle in dem Windows Registry ist **HKLM:\Software\Microsoft\Windows\CurrentVersion\Uninstall** [4, 5]. Jedes Programm hat einen eigenen Unterschlüssel und jeder dieser Unterschlüsseln enthält verschiedene Informationen über das Programm [5].

Immer wenn man ein Programm durch *Programm deinstallieren* in der *Systemsteuerung* deinstallieren möchte, werden alle dort angezeigten Informationen (wie der Programmname oder Deinstallationspfad) von diesem Schlüssel abgeholt [5].

3.2 Zuletzt verwendete Programme

Die zuletzt verwendeten Programme sind unten dem Schlüssel **HKCU:\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\<GUID>\Count** gespeichert. Ein *GUID* ist ein 128-Bit Wert, der aus einer Gruppe von 8 hexadezimalen Ziffern besteht, gefolgt von drei Gruppen mit jeweils 4 hexadezimalen Ziffern, gefolgt von einer Gruppe von 12 hexadezimalen Ziffern [6]. Die Informationen im Schlüssel **Count** sind rot13 verschlüsselt. Mit Hilfe von *UserAssist* können diese Informationen sehr leicht extrahiert und entschlüsselt werden.

Eine weitere Stelle, an der eine Liste der zuletzt ausgeführten Programme, die mit dem Befehl *Start\Run* ausgeführt werden, verwaltet wird, ist **HKCU:\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU** [5]. Die *MRUList* verwaltet eine Liste von Alphabeten, die sich auf die jeweiligen Werte beziehen [5]. Diese Alphabete sind in der Reihenfolge angeordnet, in der die Einträge hinzugefügt wurden [5]. Der zuletzt hinzugefügte Eintrag impliziert jedoch nicht den zuletzt verwendeten Befehl, da der Verdächtige möglicherweise frühere Befehle erneut ausgeführt hat [5].

3.3 Zuletzt geöffnete, gespeicherte und gesuchte Dateien

Manchmal löscht ein Verdächtiger eine Datei, nachdem er sie benutzt hat [5]. Insofern die Datei nicht ausdrücklich gelöscht wurde, wird der Dateiname möglicherweise weiterhin in dem *Most Recently Used (MRU)* Registry-Schlüssel angezeigt [5].

Es gibt mehrere Stellen in der Windows Registry, die Infos über die zuletzt geöffnete, gespeicherte oder gesuchte Dateien enthalten. Dieser Abschnitt zeigt nur Einige davon.

3.3.1 Zuletzt geöffnete Dateien. Der Schlüssel **HKCU:\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs** speichert alle Dateien, die durch den *Dateimanager* geöffnet waren [5].

Die Informationen sind in einer Form von Eigenschaften und jede Eigenschaft hat eine entsprechende *.lnk* Datei im Ordner **C:\Users\User\AppData\Roaming\Microsoft\Windows\Recent**. Das System benutzt später diese Informationen, um die zuletzt geöffnete Dateien unter *Schnellzugriff* im *Dateimanager* zu zeigen.

3.3.2 Zuletzt gespeicherte Dateien. Die Stelle, die die zuletzt gespeicherten Dateien beibehaltet

ist **HKCU:\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU** [5]. Die Informationen von diese Stelle werden später benutzt um Namensvorschläge zu geben, wenn man eine Datei speichern möchte [5].

Abhängig von der Dateierweiterung der zuletzt gespeicherten Dateien kann dieser Schlüssel verschiedene Unterschlüssel enthalten, wie z.B. *reg* oder *txt*. Wichtiger ist aber der Schlüssel namens *. Dieser beinhaltet alle zuletzt gespeicherten Dateien, unabhängig von der Dateierweiterung.

Interessanterweise kann dieser Schlüssel auch dazu verwendet werden alle zuletzt geöffneten Dateien anzuzeigen.

3.3.3 Zuletzt gesuchte Dateien. **HKCU:\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery** ist dafür verantwortlich, alle Suchanfragen des *Dateimanager* beizubehalten. Die letzten zehn Abfragen werden immer dann gezeigt, wenn der Benutzer sich auf das Sucheingabefeld im *Dateimanager* konzentriert. Sobald der Benutzer jedoch mit der Eingabe beginnt, werden zehn oder weniger relevante Abfragen gezeigt.

3.4 Verbundete Geräte

Der Schlüssel **HKLM:\SYSTEM\MountedDevices** enthält eine Liste der bereitgestellten Geräte [5]. Dieser listet alle Datenträger auf, denen ein Laufwerksbuchstabe zugewiesen wurde, einschließlich von UBS-Speichergeräten und externen DVD/CD-ROM-Laufwerken [5]. Die Regisitrierungswerte, deren Name mit **DosDevices**\ beginnt und dem zugehörigen Laufwerksbuchstaben endet, enthalten Informationen zu den bereitgestellten Geräten [5]. Durch Korrelieren des Eintrags mit dem Registrierungsschlüssel LastWrite-Time, kann der Ermittler herausfinden, wann das Wechselmedium verbunden war [5].

4 EXTRAKTION HISTORISCHER INFORMATIONEN

4.1 PowerShell

Da die Powershell bereits installiert ist, kann man diese sofort verwenden. Mit dem in **Abbildung 2** gezeigten Skript kann man alle Informationen aus dem Schlüssel **HKCU:\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\<GUID>\Count** extrahieren.

```powershell
$path = "HKCU:\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}\Count"

Get-Item -Path $path | ForEach-Object { $_.Property } | ForEach-Object {
    Write-Output "$_"
}
```

Abbildung 2: Extrahieren von Informationen für zuletzt verwendete Programme

Wie bereits erwähnt, sind die Informationen in diesem Schlüssel rot13-verschlüsselt. Um sie zu entschlüsseln, kann die folgende Funktion verwendet werden:

```powershell
function rot13([string]$s) {
    $s_dec = ""

    for ($i = 0; $i -lt $s.length; $i++) {
        $c = [int][char]($s.Substring($i, 1))

        if ($c -ge 97 -And -c -le 122) {
            $c = [int][char]'a' + (($c - [int][char]'a') + 13) % 26)
        } elseif ($c -ge 65 -And $c -le 90) {
            $c = [int][char]'A' + (($c - [int][char]'A') + 13) % 26)
        }

        $s_dec += [char]$c
    }

    return $s_dec
}
```

Abbildung 3: Quellcode für die Funktion rot13

Zeile 4 aus **Abbildung 2** muss dann wie folgt geändert werden:

```
$s_dec = rot13($_)
Write-Output "$s_dec"
```

Abbildung 4: Verwendung der Funktion rot13

Das endgültige Skript gibt alle zuletzt verwendeten Programme in entschlüsselter Form aus.

4.2 RegRipper

Um RegRipper nutzen zu können muss es zuerst heruntergeladen werden. Derzeit ist es unter Github verfügbar.

Es gibt zwei ausführbare Versionen: eine mit GUI (*rr.exe*) und eine, die über *Command Prompt* ausgeführt werden kann (*rip.exe*). Der Unterschied besteht darin, dass die erste Version alle Informationen extrahiert die sie kann, ohne das gefiltert werden kann. In diesem Projekt wird die zweite Version verwendet.

Um zu sehen, welche Argumente RegRipper erwartet, kann man **rip** (oder **rip -h**) eingeben.

```
> rip

Rip v.3.0 - CLI RegRipper tool
Rip [-r Reg hive file] [-f profile] [-p
↪  plugin] [options]
...
```

Abbildung 5: RegRipper - Verwendung

Der Befehl **rip -l** listet alle verfügbaren Plugins auf. Das Plugin **comdlg32** erhält den gesamten Inhalt vom Schlüssel **HKCU:\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32**.

```
> rip -r Path\To\Registry\Hive\File -p
↪  comdlg32

Launching comdlg32 v.20200517
...
```

Abbildung 6: Extrahieren von Informationen aus ComDlg32

Wenn man die Ausgabe in einer Datei speichern möchte, kann man die Umleitungsoperatoren (> oder >>) verwenden.

5 ZUSAMMENFASSUNG

Windows Registry, eine Kernkomponente des Windows-Betriebssystem, ist die zentrale hierarchische Datenbank, die eine beträchtliche Menge an Konfigurationsinformationen über das System und seine Programme enthält. Es enthält auch historische Informationen zu den Benutzern, wie z.B. USB-Aktivitäten, zuletz besuchte Webseiten, zuletz aufgerufene Dateien und zuletz verwendete Programme.

Mit digitaler Forensik können viele Informationen über Benutzeraktivitäten extrahiert werden. Diese Informationen können manchmal entschiedend sein, um die Beteiligung eines Benutzers an einer bestimmten Cyberkriminalität zu beweisen oder zu wiederlegen.

Dieses Paper zeigt einige Beispiele dafür, wo Informationen zu Benutzeraktivitäten in dem Windows Registry enthalten sind. Es werden auch einige Tools gezeigt, mit denen ein Ermittler diese Informationen extrahieren kann.

LITERATUR

(1) H. Carvey, Windows Registry Forensics, 2nd ed. Cambridge: Elsevier, 2016.

(2) K.D. Cook and N. Shashidhar, Üsing PowerShell to Capture and Compare Windows Registry and Live Memory Artifacts with Online Databases to Identify Suspect Files.", 2018

(3) C. Leube, K. Bellin and R. Creutzburg, Ïmplementation of a forensic tool to examine the Windows registry", The International Society for Optical Engineering, 2014, 10.1117/12.2037020.

(4) Patil, Dinesh N., and Bandu B. Meshram. Ëxtraction Of Forensic Evidences From Windows Volatile Memory". 2nd International Conference For Convergence In Technology (I2CT), 2017.
(5) K. Youngsoo and D. Hong, "Windows Registry and Hiding Suspects' Secret in Registry", International Conference on Information Security and Assurance, 2008. Available: 10.1109/ISA.2008.8 [Accessed 19 October 2020].
(6) "GUID - Win32 apps", Docs.microsoft.com, 2020. [Online]. Available: https://docs.microsoft.com/en-us/windows/win32/api/guiddef/ns-guiddef-guid. [Accessed: 25 Oct, 2020].
(7) "My Software", Didier Stevens, 2020. [Online]. Available: https://blog.didierstevens.com/my-software/#UserAssist. [Accessed: 26 Oct, 2020].