Betriebssysteme
Forensik: ntuser.dat

Die NTUSER.DAT befindet sich als versteckte Systemdatei im Ordner des jeweiligen Benutzers unter C:\Benutzer\<benutzer>\NTUSER.DAT
Ausserdem gibt es eine gleichnamige .log1 und log2 als Zwischenspeicher, bevor die Änderungen final in der NTUSER.DAT landen.
Diese sollten in die Analyse einbezogen werden.
Da jeder Benutzer eine eigene NTUSER.DAT besitzt, können gefundene Spuren exakt einem Benutzerkonto zugewiesen werden.

Im Live-Betrieb mit REGEDIT unter Computer\HKEY_CURRENT_USER\ (andere User unter HKU).
ID des angemeldeten Users ermitteln (HKCU): Dosbox: whoami /logonid

HKCU eines anderen Benutzers laden / editieren:
Registry: HKU/ markieren, Datei -> Struktur laden, ntuser.dat aus dem betreffenden Userprofils laden.

Offline Tool: Registry Explorer

MS Office

- legt die zuletzt aufgerufenen Dateien und Speicherorte ab
- nicht vertrauenswürdige Speicherorte (default: alles außer lokale Festplatte) werden gesondert gespeichert
- Schlüssel in NTUSER.DAT\Software\Microsoft\Office\
- ...\Word\User MRU\ listet die letzten 50 Word-Dokumente auf
- ...\Word\Place MRU\ listet die letzten 50 Word Speicherorte auf

Dateien und Ordner

- NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs - speichert die letzten 150 zugegriffenen Dateien ab
  - besitzt für jeden Dateityp einen Subschlüssel
  - Datei MRUListEx speichert jeweils die Reihenfolge, in der die Dateien geöffnet wurden
- NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU - speichert Dateien, die mit „Öffnen“ oder „Speichern unter“ Dialoges geöffnet bzw. geschlossen wurden
  - je Dateityp gibt es einen Subschlüssel und eine MRUListEx wie oben
- NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU - speichert Programm im Ausführen-Dialog

Fernzugriff

- NTUSER.DAT\SOFTWARE\Microsoft\Terminal Server Client\Servers - enthält Ziele (IP + Anmeldename) der RDP-Verbindungen

Betriebssysteme

siehe auch:

- Windows Registry: https://uwe-kernchen.de/phpmyfaq/index.php?solution_id=1069
- Forensik: https://uwe-kernchen.de/phpmyfaq/index.php?solution_id=1045

Eindeutige ID: #1420
Verfasser: Uwe Kernchen
Letzte Änderung: 2023-01-26 15:38