$\frac{Registry forensik}{\text{by Koll, Michael}}$

Relative Pfade

%UserProfile% Pfad zum derzeitigen Benutzerprofil %SystemDrive% Laufwerksbuchstabe, auf dem Windows

installiert ist, i.d.R C:

%SystemRoot% Pfad zum Windows Ordner, i.d.R.

C:\Windows

Schlüssel & Werte

Ein Schlüssel enthält einen oder mehrere Werte sowie einen Zeitstempel des letzten Zugriffs

Jeder Wert hat 3 Felder:

Eindeutig innerhalb eines Schlüssels Name

Datentyp des Wertes (s.u.) Тур

kann leer oder null sein, Maximum 32767 Bytes, häu-Daten

fig in hexadezimaler Notation

Die wichtigsten Datentypen sind REG_NONE kein definierter Typ

REG_SZ Fixe Länge und NULL-Char am Ende REG_EXPAND_SZ Variable Länge und NULL-Char am Ende

REG_BINARY Binärdaten

REG DWORD Double-Word-Werte, häufig boolesche Werte

REG LINK

REG_MULTI_SZ Liste von Strings

Struktur

Wurzelschlüssel

HKLM	HKEY_LOCAL_MACHINE	Hauptschlüssel
HKU	HKEY_HKU	Hauptschlüssel
HKCR	HKEY_CLASSES_ROOT	Verweis
HKCU	HKEY_CURRENT_USER	Verweis
HKCC	HKEY_CURRENT_CONFIG	Verweis

Verweise

HKCC HKLM\SYSTEM\CurrentControlSet\Hardware Profiles\Current HKCU HKU\S-1-5-21-xxx (SID)

HKCR HKLM\SOFTWARE\Classes

HKU

Nutzerspezifische Einstellungen und Informationen für jeden aktiv geladenen Benutzer (Standardprofile und angemeldete Profile, keine abgemeldeten Nutzer)

.DEFAULT	Einstellungen, die Windows nutzt, bevor
	ein Nutzer sich eingeloggt hat
S-1-5-18	well-known SID für LocalSystem-
	Benutzer
S-1-5-19	well-known SID für LocalService-
	Benutzer, lokale Dienste, die den
	LocalSystem-User nicht benötigen
S-1-5-20	well-known SID für NetworkService-
	Benutzer, Netzwerkdienste, die den
	LocalService-Benutzer nicht benötigen
S-1-5-21-[]	SID des derzeit angemeldeten Benutzers
	(Link von HKCU)
0 1 5 01 5 7 07	Nuturana aniforda Datairranlaniin fun man

S-1-5-21-[...] Classe utzerspezifische Dateiverknüpfungen

HKCU

Link auf HKU\[SID]

Control-Panel

Spezifische Einstellungen und Informationen zum angemeldeten Benutzer (Umgebungsvariablen,

Desktopeinstellungen, Netzwerkverbindungen, Drucker und Präferenzen)

AppEvents Verknüpft Audiodateien mit Aktionen (z.B. Ton beim Öffnen eines Menüs) Console

Daten zum Console-Subsystem (z.B. zum MS-DOS-Command-Prompt)

Einstellungen der Systemsteuerung, u.a. regionale Einstellungen und Erschei-

nungsbild

Umgebungsvariablen, die Benutzer ge-Environment

setzt haben

Installierte Tastaturlayouts Keyboard-Layout

Network Jeder Unterschlüssel ein Netzlaufwerk,

> Name des Schlüssels ist Laufwerksbuchstabe, enthält Konfigurationsdaten zum

Verbinden

Präferenzen des Benutzers zum Drucken Printers Software Nutzerspezifische Einstellungen zu

installierten Programmen, je nach Programm Informationen zu Programmanbieter, Programm, on, Installationsdatum und zulegt zugegriffene Dateien. Ablage nach HKCU\Software\Programmanbieter\-

Programm\Version

Volatile Environment Umgebungsvariablen, die beim Login

definiert wurden

HKLM

Spezifische Einstellugen des lokalen Rechners, die für alle Benutzer geladen werden.

HARDWARE Speichert HW-Daten beim Systemstart, wird bei jedem Start erstellt und mit Informationen über

Geräte, Treiber und Ressourcen gefüllt

Lokale Windows-Sicherheitsdatenbank über SAM Benutzer- und Gruppeninformationen (Link zu

HKLM\SECURITY\SAM)

SECURITY Lokale Windows-Sicherheitsdatenbank (inklusive

SOFTWARE Einstellungen zu Applikationen des Rechners

(und Microsoft-Applikationen) Informationen zur Systemkonfiguration (z.B. Ge-

rätetreiber und Dienste). Derzeitiges Hardwareprofil ist Link von HKCC. Mehrere Sätze mit Schema ControlSetxxx. HKLM\SYSTEM\Select zeigt aktuelle verwendetes Profil in CurrentControlSet.

HKCR.

SYSTEM

Link auf HKLM\Software\Classes & HKU\[SID] Classes

- Zuweisungen für Dateierweiterungen
- OLE-Datenbank

- Einstellungen für registrierte Anwendungen für COM-Objekte
- Nutzer- und systembasierte Informationen

Setzt sich aus HKLM\SOFTWARE\Classes und HKU\[SID]_Classes zusammen. Falls identischer Wert, hat HKCU Priorität. Beispiel: Was soll passieren, wenn eine .pptx-Datei geöffnet wird. HKCR macht einen erheblichen Teil der Registry und des Systemverhaltens aus

HKCC

Link auf HKLM\System\CurrenControlSet\Hardware Profiles\Current

Link zu den Konfigurationsdaten des derzeitigen

Hardwareprofils. Informationen werden bei iedem Booten neu erzeugt und daher nicht physisch in der Registry-Datei gespeichert.

System Software

Hives

User-Profile-Hives in %UserProfile%\NTUSER.DAT

Alle anderen Hives und Dateien in %SystemRoot%\System32\config HKU\.DEFAULT DEFAULT

HKLM\SAM SAM

HLKM\SECURITY SECURITY HKLM\SOFTWARE SOFTWARE HLKM\SYSTEM SYSTEM

Schlüssel HKLM\HARDWARE mit dynamischen Hive, wird beim

Systemstart erstellt aber nicht gespeichert

Liste zu Standard-Hive-Files:

HKLM\SYSTEM\CurrentControlSet\Control\hivelist Liste User-Hives: HLKM\SOFTWARE\Microsoft\Windows

NT\CurrentVersion\ProfileList

SID & SAM

Liste der SIDs

HKLM\Software\Microsoft\WindowsNT\CurrentVersion\ProfileList Pfad zu individuellen Profilen: ProfileImagePath

Aufbau der SID (S-1-5-21-[...]-1002):

Identifiziert den Schlüssel als SID

Revisionsnummer, Nummer der SID-Spezifikation

21-[...] Domänen-ID, identifiziert die Domäne oder den lo-

kalen Computer, Wert ist variabel

Benutzer-ID, relative ID (RID), >1000 für Profile 1002

die nicht standardmäßig generiert wurden

Informationen aus SAM

SAM\Domains\Account\Users\<Benutzernummer>\

Enthält Informationen wie Datum der letzten Passwortänderung und Datum der letzten Anmeldung vom Nutzer mit der Id <Benutzernummer>

Wichtige Pfade

Systeminfo

HKLM/Software/Microsoft/ Windows NT/CurrentVersion/ CurrentBuildNumber

Windows Buildnummer

(cmd: systeminfo)

Autorun

HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce HKLM\Software\Microsoft\Windows\CurrentVersion\Run HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce HKCU\Software\Microsoft\Windows\CurrentVersion\Run Pfade in Run bei jedem Systemstart, RunOnce nur einmal

MRU

HKU\<SID>\Software \Microsoft \Windows \

CurrentVersion \Explorer

ComDlg32 Zuletzt ausgeführte Anwendungen und deren

Pfade sowie geöffnete oder geänderte Dateien

Unterschlüssel mit Dateierweiterungen, zuletzt RecentDocs

geöffnete Dateien diesen Typs

Aufrufe, die via Run durchgeführt wurden RunMRU Werte von Objekten, auf der Nutzer zugegriffen UserAssist

hat (z.B. Optionen der Systemsteuerung, Datei-

verknüpfungen und Programme)

ROT13 verschlüsselt, es gibt mehrere MRU-Listen in unterschiedlichen Listen

Geschützter Speicher

HKU\<SID>\Software \Microsoft \ Protected Storage System Provider Verschlüsselte Passwörter für viele Anwendungen (Outlook Express, MSN-Explorer oder Internet Explorer)

Autovervollständigung oder Passwort merken

Internet Explorer

HKU\<SID>\Software \Microsoft \Internet Explorer

Download Informationen zu Downloads

Benutzereinstellungen (Search Bars, Startseite, Main

Zuletzt besuchte Seiten (z.B. EMail, Onlineban-TypedURLs

king)

Microsoft Edge nutzt

HKCU/Software/Classes/Local Settings/Software/ Microsoft/Windows/CurrentVersion/AppContainer/Storage/

microsoft.microsoftedge_xxxxxx/MicrosoftEdge

Netzwerke

WLAN

HKLM/Software/Microsoft/Windows NT/ Netzwerkgeräte CurrentVersions/NetworkCards (Beschreibung und GUID)

HKLM/System/CurrentControlSet/ Services/Tcpip/Parameters/ Interfaces/<GUID>

Details zum Netzway, Domain)

werkgerät (IP, Gate-

P2P

HKLM/System/ControlSet001/ Services/SharedAccess/Parameters/ FirewallPolicy/StandardProfile/ AuthorizedApplications/List

Applikationen mit erlaubtem Zugriff auf ausgehende Verbindungen

Angeschlossene Geräte

HKLM/System/Mounted Devices

HKCU/Software/Microsoft/ Windows/CurrentVersion/Explorer/ MountPoints2

HKLM/System/CurrentControlSet/ Control/DeviceClasses

Unterschlüssel DeviceInstance CurrentControlSet/

HKLM/System/CurrentControlSet/Enum/Geräte im System mit <Enumerator>/<DeviceID>

HKLM/System/CurrentControlSet/Enum/Angeschlossene USB-USBSTOR

Mount eines Geräts bei Nutzerlogin Enthält für DeviceClass-GUID mit

Liste aller Geräte, die

im System gemountet

wurden

Geräten die verbunden waren oder sind. Pfad zu HKLM/System/ Enum. Durch Export Zeitstempel für ersten und letzten Zugriff Gerätebeschreibung

und IDs

Geräte

Antiforensische Maßnahmen

Zeitstempel fädlschen Prüfsumme häufig nur auf Inhalt

(Tool http://www.petges.lu/home/

download)

Pagefile.sys HKLM/System/ CurrentCOntrolSet/

Control/Session Manager/

Memory Management denWert ClearPagefileAtShutdown auf 1

Zeitstempel vermeiden HKLM/System/CurrentControlSet/

> Contol/FileSystem Wert. NtfsDisableLastAccessUpdate

auf 1 setzen

Einträge löschen Verlauf IE oder zuletzt genutzte Do-

kumente

UserAssist abstellen HKU/Software/Microsoft/Windows/

CurrentVersion/Explorer/ UserAssist Wert NoLog vom

Typ DWORD mit Wert 1 erstellen

Tools

FTK-Imager Erstellung von Abbildern, Kopien der Hive-Files (Live) (Files → Obtain Protec-

ted Files)

Registry-Editor Importieren und Exportieren von Datei-

> en, Struktur laden und entfernen, Verbinden mit der Registry eines Remotecomputers, Berechtiungen ändern, Regis-

try durchsuchen

Änderungen in der Registry aufzeichnen RegShot

(Erstellen eines ersten Abbildes und Ver-

gleich mit einem zweiten)

Forensic Registry Untersuchung und Bearbeitung von EDitor (fred) HIVE-Dateien, vorgefertige Berichtsvor-

RegRipper Extrahieren von spezifischen Informatio-

nen, Automatisierung durch Plugins und

Profile

DCODE Decodieren von Zeitstempeln (https://

www.dcode.fr/timestamp-converter)

Auslesen von Hive-Files (https: Access Data Registry Viewer //accessdata.com/product-download/

registry-viewer-1-8-0-5)

Auslesen von Hive-Files (https://www. RegView

gaijin.at/dlregview.php)

Fehler und Verbesserungen bitte melden:

https://github.com/michkoll/latex-template-cheatsheet/issues

Windows 10-Forensik

Allgemein

Buildnummer

Aktuelle Buildnummer über systeminfo (cmd.exe) oder HKLM\Software\Microsoft\Windows NT\CurrentVersion\CurrentBuildNumber

Zuletzt verwendete Elemente

 $\label{lem:c:wsername} $$C:\Users\le \arrang\Microsoft\Windows\Recent $$$

Überwachter Ordnerzugriff

Überwacht und blockiert den schreibenden Zugriff auf vorhandene Dateien für nicht-vertrauenswürdige Applikationen.

Aktivieren

Windows Defender Security Center \to Einstellungen für Virenund Bedrohungsschutz \to Überwachter Ordnerzugriff oder

Gruppenrichtlinien: Computerkonfiguration/Administrative Vorlagen/Windows/Windows Defender Antivir/Windows Defender Exploit Guard/Überwachter Ordnerzugriff oder

Registry (Besitzer vorher ändern): HKLM\Software\Microsoft\Windows Defender\Windows Defender Exploit Guard\ControlledFolderAccess\EnableControlledFolderAccess (DWORD) = 0x01

Erlaubte Anwendungen

HKLM\Software\Microsoft\Windows Defender\
Windows Defender Exploit Guard\ControlledFolderAccess\
AllowedApplications
Hinzufügen mit (PS): Add-MpPreference
-ControlledFolderAcessAllowedApplications

Geschützte Ordner

«Anwendungspfad>"

HKLM\Software\Microsoft\Windows Defender\
Windows Defender Exploit Guard\ControlledFolderAccess\
ProtectedFolders

Standardmäßig geschützte Ordner: Documents|Pictures|Videos|Music|Desktop|Favorites (<username> und Public)

Ereignisse

Einzusehen über EventVwr oder Powershell: Get-WinEvent -LogName "Microsoft-Windows-Windows Defender/Operational Where-Object {\$_..Id -in 1123,1124,5007}

Ereignis-IDs:

1123 Blockiertes Ereignis

1124 Überwachtes Ereignis (Auditmodus)

5007 Änderung von Einstellungen

Jumplists

Mehr Informationen als MRU/MFU:

- Dateiname, -pfad
- MAC Zeitstempel
- Name des Volumes
- Zeitlicher Verlauf von Down- und Uploads
- Informationen bleiben nach Löschen der Datei erhalten

Speicherort

Erstellt vom Betriebssystem: C:\User\<username>\AppData\ Roaming\Microsoft\Windows\Recent\AutomaticDestinations Erstellt von Softwareanwendungen:

C:\User\<username>\AppData\Roaming\Microsoft\Windows\
Recent\CustomDestinations

Dateiname: <appId>.<automatic|custom>Destinations-ms
Die AppId kann im ForensicsWiki nachgelesen werden https:
//www.forensicswiki.org/wiki/List_of_Jump_List_IDs

Automatic Destination JL

Aufbau der Datei:

Header (32 Byte) mit Versionssnummer (3=Win10, 1=Win7/8), Anzahl Einträge, Anzahl gepinnte Einträge, Zuletzt zugewiesene Entry-ID, Anzahl der Aktionen DestList-Entry:

Prüfsumme Fehlerhafter Eintrag wird nicht angezeigt (New|Birth) Bei Änderung des Volumes geänderte New-

Volume-ID ID

(New|Birth) Generiert aus Bootzeit,Sequenznummer und Object-ID MAC-Adresse. Bei Änderung des Volumes

neue New-ID

NetBios Name nbtstat -n
Entry ID Fortlaufende Nummer

Access Timestamp letzter Zugriff
Pinned Status angepinnt (ja/nein)
Access Count Zugriffszähler

variabel Unicode vollständiger Pfad zur Datei

Länge Unicode Länge Unicodepfad

CustomDestionations JL

einfachere Dateistruktur, zusammengesetzte MS-SHLINK-Segmente

Anfang eines LNK-Segments: 4C 00 00 01 14 02 00 00

00 00 00 C0 00 00 00 00 00 00 46

Ende: AB FB BF BA

QuickAccess/Schnellzugriff

Angepinnte Einträge im Schnellzugriff des Explorer. Dateiname 5f7b5f1e01b83767.automaticDestinations-ms

Tools

JumpListExt for grafische Oberfläche, nicht mehr stabil in ak-Windows 10 tuellen Versionen

JLECmd .exe -f <JLFile>

(-html|-csv|-json) <targetDir> (-ld)

Windows 10 Applications

SystemApps

vorinstalliert, können nicht deinstalliert werden C:\Windows\SystemApps\<appname>

WindowsApps

über Windows Store C:\Windows\WindowsApps\<appname>

Einstellungsdaten

C:\Users\<username>\AppData\Local\Packages\<appname> Haupteinstellungen in Datei/Registry-Hive settings.dat

Anwendungsdaten

Gespeichert in ESE-DB-Datenbanken, Aufbau nicht vollständig bekannt, teilweise möglich mit ESEDatabaseView von Nirsoft

Fast Startup und Ruhezustand

Datei: hiberfil.sys

Zustände

HIBR Im Ruhezustand RSTR Wird fortgesetzt WAKE Nach Fortsetzung

Forensische Bewertung

Änderung des Formats ab Win8

- Header bleibt auch nach Fortsetzen verfügbar
- Daten nur zwischen Versetzen in Ruhezustand bis zur Fortsetzung
- Vor Win8 zeitlich weit zurückreichende Daten
- Sichern der hiberfil.sys im laufenden Zustand keine forensisch relevanten Daten
- Größte Menge Daten shutdown /h
- HIBR2BIN ermöglicht dekomprimieren der Daten im neuen Format
- Fast Startup liefert keine interessanten Daten, da alle Applikationen beendet sind

Edge Browser / ESE-DB

Anwendungspfad

C:\Windows\SystemApps\Microsoft.MicrosoftEdge_ 8wekyb3d8bbwe\MicrosoftEdge

ESE-Datenbank

Transaktionsflow

- 1. Transaction in RAM (Log Cache)
- 2. Seiten aus DB in RAM (Page Cache)
- 3. Transaktion im RAM anwenden (LC⇒PC)
- 4. Aktualiserte Daten in Logdatei (LC→Datei)
- 5. Datenbank aktualisieren

Dirty-DB

Datenbank, die nicht vollständig aktualisiert wurde.

Zeitpunkt der Transaktion V01.chk

Transaktionsdaten, hexadezimale Dateinamen *.log

Wiederherstellung mit esentutl

esentutl /mh database.dat Überprüfung der Datenbank

(Feld State=Dirty)

Reparatur der Datenbank esentutl /r database.dat

(Feld State=Clean)

WebCacheV01.dat

Pfade

→C:\Users\<username>\AppData\Local\Packages\

Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\MicrosoftEdge\

(enthält v.a. Verweise und Speicherorte)

→C:\Users\<username>\AppData\Local\Packages\

Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\#!<number> \MicrosoftEdge\

Aufbau

Tabelle Containers

ContainerId Referenz auf Tabelle Container n Pfad zum Verzeichnis mit zwischen-

Directory gespeicherten Daten

Zufällige Zeichenfolge, in 8er-SecureDirectories

Gruppen teilbar

(Coo-Name Containertyp

kies|Content|History|...)

Integritätslevel, (Protected= Inter-PartitionId

net=Low | lokal=medium)

Tabelle Container_n

SecureDirectory Unterverzeichnis im Cachepfad

Type z.B. Ïn PrivateModus (siehe Chivers) Anzahl wie oft URL referenziert wird AccessCount

<Timestamps> Sync, Creation, Expiry, Modified, Accessed Time

URL Quelle der Informationen Filename Name der Cachedatei

Cache-Speicherort ermitteln

SecureDirectories in 8er-Blöcke aufteilen

zeigt auf x-ten Block (in Container n) SecureDirectory

Zeichenfolge anhängen Directory

Zeitstempel

CreationTime Erstellungzeit der Cachedatei/-objekt ExpiryTime

vom Webserver vorgegeben, Cache wird un-

vom Webserver, Zeitpunkt der letzten Ände-ModifiedTime

rung der Ressource

AccessTime Letzter Zugriff des Nutzers auf Datei

Werkzeuge

Fazit: Tools gute Unterstützung, manuell bringt mehr

Zeigt Cachedateien von IE und Edge **IECacheView**

(Dateiname, -größe, -typ, URL, Zeit-

stempel, Cachedateipfad)

BrowsingHistoryView Zeigt Browserverlauf mehrerer Browser

OneDrive

Anwendungspfad

C:\User\<username>\AppData\Local\Microsoft\OneDrive\

Registry

HKU\Software\Microsoft\OneDrive\

Version.UserFolder

.\Accounts\Personal ClientFirstSignInTimestamp,

UserCID, UserFolder

Konfigurations- und Diagnostikdaten

Ausgehend vom One-Drive-Verzeichnis:

.\logs\Personal\ Down-\Uploadgeschwindigkeit,

SyncDiagnostics.log Ausstehende Down-\Uploads, verfügbarer Speicherplatz lokal, UserCID (siehe REG), Anzahl

Dateien und Verzeichnisse

.\settings\Personal\ bisher kein Parser, mit Hexeditor

<usercid>.dat Dateinamen einsehen

.\settings\Personal\ Während Download temporär Da-<uploads|downloads>.txt ten wie Dateiname und User-CID

Logdateien

.\logs\Personal\

*.aodl, *.odlsent, *.odl enthalten Clientaktivitäten Die Datei ObfuscationStringMap.txt enthält verschleierte Dateinamen, die in den Logs gefunden werden können.

Mögliche Aktionen in den Logs:

Datei lokal hinzugefügt FILE_ACTION_ADDED FILE_ACTION_REMOVED Datei lokal entfernt FILE_ACTION_RENAMED Datei umbenannt

Arbeitsspeicher

Username und Passwort liegen im Klartext vor, nach Parameter &passwd= und &loginmft= suchen

Benachrichtigungen und Kacheln Datenbank

C:\Users\<username>\AppData\Local\Microsoft\Windows\ Notifications

wpndatabase.db Datenbank (Signatur 53 51 4C 69

74 65 20 66 6F 72 6D 61 74 20

Writhe Ahead Log (Signatur 37 7F wpndatabase.db-wal 06 82 oder 37 7F 06 83)

Shared Memory File, keine spezifiwpndatabase.db-shm

sche Signatur

SQLite-Datenbank mit WAL-Verfahren: Änderungen in Datei, bei Erreichen des Checkpoints (manuell oder automatisch) synchronisiert. WAL-Dateien bei der Untersuchung einbeziehen (PRAGMA wal_checkpoint).

Struktur und Inhalt

Notification

Relevante Tabellen in wpndatabase.db

NotificationHandler Anwendungen, die zu Benachrichtigungen berechtigt sind (Zuordnung

über PrimaryID→ AppID,GUID) Benachrichtigunginhalt \rightarrow Payload

Kacheln

Datenbank wie Benachrichtigungen, Zeitstempel ArrivalTime und ExpiryTime Rückschlüsse auf Verwendung des Computers Einige Anwendungen legen in dem DB-Verzeichnis Cacheordner an, die sehr lange zurückreichen

Cortana

%localAppData%\Packages\Microsoft\Microsoft.Windows. Cortana_cw5n1h2txyewy

Artefakte

 \rightarrow .\AppData\Indexed DB\ 11 Tabellen, Tabelle HeaderTable IndexedDB.edb enthält createdTime. lastOpenTime \rightarrow .\LocalState\ [Veraltet] Geofences mit Standortdaten. Reminders benutzerspe-ESEDatabase CortanaCoreInstance\ zifische Erinnerungen, Triggers CortanaCoreDb.dat LocationTriggers, TimeTriggers,

ContactTriggers

keine Dokumentation, Infos über \rightarrow .\LocalState\ DeviceSearchCache\ Programmeinträgen, -aufrufen,

Zeitstempel und JL-Einträge vollständige HTML-Seite von Su-

<randomnumber> chen über Cortana HTML- und JavaScript Dateien \rightarrow .\AC\AppCache\

<randomnumber> für Cortana-Suche \rightarrow .\LocalState\ Aufgezeichnete Sprachbefehle LocalRecorder\Speech

→.\LocalState\Cortana\ Falls Synchronisierung mit Andro-Uploads\Contacts id. Kontaktdaten und Mobilnum-

mern

URLs die über Cortane-Suche aus- \rightarrow 9d1f905ce5044aee. automaticDestinations-ms gelöst wurden

 \rightarrow WebCacheV01.dat

URLs die über Cortana aufgerufen wurden

→%SystemDrive%\Windows\ Letzte Ausführungszeit(en) Prefetch\SEARCHUI.

EXE-14F7ADB7.pf

 \rightarrow .\AC\INetCache\

→%SystemDrive%\Windows\ Erstellungs- und Änderungszeitappcompat\Programs\ stempel der Anwendung

Amcache.hve

Deaktivieren von Cortana

Parameter in

HKLM\Software\Policies\Microsoft\Windows\Windows Search

AllowCortana dword:00000000 DisableWebSearch dword:00000001 AllowSearchToUseLocation dword:00000000 ConnectedSearchUseWeb dword:00000000 ConnectedSearchPrivacv dword:00000003

Fehler und Verbesserungen bitte melden:

https://github.com/michkoll/latex-template-cheatsheet/issues

Betriebssystemforensik (allgemein)

by Koll, Michael

Betriebssystem

Architektur

Monolithisch (S.22)

schnell, minimaler Overhead; Funktio-Geschwindigkeit nen optim. abgestimmt

Sicherheit Risiko: ganzes BS im priv. Modus; Probleme einzerln Komp. Auswirkung auf

ganzes BS

Schlecht, ganzes BS im Speicher gehal-Speichereffizienz

Schlecht, da bei Änderungen viele Kom-Wartbarkeit.

Erweiterbarkeit ponenten

Geschichtet (S.23)

Geschwindigkeit Langsamer, da Funktionen Overhead,

häufiger Kontextwechsel

Sicherheit Teile des BS im User Mode, z.B. Trei-

ber; Probleme Komponenten → BS

Speichereffizienz Gut, einzelne Module dynamisch nach-

geladen und entladen

Besser, da Änderungen meist nur bei Wartbarkeit,

einzelnen Komponenten Erweiterbarkeit

Mikrokernel (S.24)

schlechte Performance, häufige Prozess-Geschwindigkeit

wechsel und Interprozesskommunikati-

Sicherheit sicherheitskritischer Teil relativ klein:

Dienste außerhalb Kern können Sicherheit und Stabilität nicht beeinflussen

Gut, einzelne Module dynamisch nach-Speichereffizienz

geladen und entladen

Wartbarkeit. Sehr gut, einzelne Module können aus-Erweiterbarkeit getauscht werden (z.T. während Be-

trieb)

Vorteile virtuelles BS

Sandbox verbesserte Sicherheit durch Abschottung: bessere Ausnutzung des Systems durch mehrere VMs; herstellen kompatibler Laufzeitumgebungen

Ziele (S.12)

Unterstützung des

Anwenders

Abstraktion der Hardware (Nummerierte Datenblöcke der HDD werden durch Reihenfolge, Verkettung und Verknüpfung zu Datei), Bereitstellen von Dienstfunktionen (Dateien öffnen, lesen, schreiben, schließen),

Verbergen irrelevanter Details (Nummerierung Datenblöcke für

Anwender nicht sichtbar)

Optimierung der Rechnerauslastung Zuverlässigkeit

Parallele Nutzung Rechnerkomponenten, mehrere Aufgaben quasiparallel Schutzmechanismus gegenseitig störender Prozesse. Abfangen von Ausnahmesituationen, Verhindern von blockieren-

den Prozessen

Portabilität Programme auf verschiedenen Plattfor-

men lauffähig

Nicht erfüllte Zuverlässigkeit

Prozess belegt zu viel Speicher, so dass andere Prozesse nicht ausgeführt werden können

Abbruch mit Ctrl+C funktioniert nicht, da Signal auf

Ignorieren steht

Prozess zieht alle Prozessorleistung, so dass andere Prozesse

blockiert sind (unfaires Scheduling)

Aufgaben (S.14)

Programm- und Prozessverwaltung

Steuern, Erzeugen, Starten, Entfernen von Prozessen; Laden von Programmen von HDD in RAM; Leerlaufprozess; Kommunikation und Synchronisation von Prozessen

Kommandoebene, graphische Be-Anwenderschnittstelle

dienoberfläche, Systemaufrufe zwischen BS und Programmen Aufteilen der Betriebsmittel, Tren-

Verwalten von Betriebsmitteln nung Benutzerbereiche, Schutz. Prüfung Zugang

Verbindungen mit anderen

Rechnern

Begriffe

Parallel Gleichzeitige Abarbeitung von Prozessen,

jeder Prozess läuft auf eigener CPU

Abwechselnde Abarbeitung, alle Prozesse Quasiparallel

laufen auf gleicher CPU

besteht aus Vorschriften/Anweisungen in Programm

formaler Sprache; Ausführen zur Bewälti-

gung bestimmter Aufgaben

Prozess ablaufendes Programm mit konkreten Daten, besitzt Rechte, Registerinhalte und

Speicher: Zustände running, ready oder

waiting

Untereinheit von Prozessen, teilen sich den-Threads

selben virtuellen Adressraum, Prozesswech-

sel schneller

Leerlaufprozess Prozessor führt ständig Befehlszyklen aus,

Leerlaufprozess verbraucht diese mit NOP-

Anweisungen

Dateisystem

Zusammenhängende Belegung (S.104)

Belegungstabelle Datei, Start, Länge

Verteilte Belegung verkettete Listen (FAT) (S.105)

Belegungstabelle Datei, Start

Verweis auf nächste Adresse, Dateiende Hilfstabelle (FAT)

mit EOF

Verteilte Belegung mittels Index-Liste (S.106)

Belegungstabelle

Datei, Index-DU

Index-DU

Verweise auf DUs (falls zu lang Verweis

auf weitere Index-DU)

Windows

Allgemein

Windows Stations, Desktops und Session (S.34)

Authentifizierung Session-orientiert, Session beinhaltet mehrere Stations, Stations beinhalten Desktops mit Fenstern und GDI-Objekten. Sicherheitsbeschreiber eines Objekts ist mit Station verbunden, darüber Kontrolle von Benutzer zum Desktop

Prozesse und Dienste

svchost.exe (Dienste) (S.138)

- mit tlist laufende Prozesse mit Diensten auflisten (tlist -m svchost.exe -s)
- ullet mit Process-Explorer farblich gekennzeichnete Dienste ightarrowProperties \rightarrow Services
- spezielle Programme wie z.B. svchost-Analyzer

Gestartete Dienste in Registry

HKLM\System\CurrentControlSet\Services als Unterschlüssel

laufende Prozesse PIDs und TIDs

mit Process Explorer; PID in Liste laufende Prozesse; TID $Prozesseigenschaften \rightarrow Threads$

Registryzugriffe von Prozessen

Mit Process Explorer und Process Hacker: Möglichkeit über Process Monitor Registryzugriffe zu protokollieren (Software $installieren \rightarrow mit Process Monitor analysieren)$

Ausgeführte Dienste

z.B. über msc (services) oder Registry (siehe oben)

Mandatorische Zugriffsregeln (S.153)

No-<Write|Read>-Up Kein schreibender/lesender Zugriff von Prozessen mit niedrigem Level auf Objekte mit höherem Level

(gleiches Level zugelassen)

No-<Write|Read>-Down Kein schreibender/lesender Zugriff von Prozessen mit höherem Level

auf Objekte mit niedrigerem Level (gleiches Level zugelassen)

Default: No-Write-Up (für alle Objekte), No-Read-Up (für Prozesse und Threads)

DACL (S.156)

Sicherheitsdeskriptor besteht aus Header, SID Besitzer, SID Gruppe, DACL, SACL

DACL besteht aus ACEs mit <Allow|Denv>, SID User, ACE-Bitmapp

Regeln DACL: Erst Einzel-ACE, dann Gruppe; Erst Verbote, dann Erlaubnisse: Reihenfolge von oben nach unten Hinweis: Beim Ändern bzw. lesen aufpassen auf Gruppenzugehörigkeit (Jeder)

Festplatten und Drucker

Option 1 In regedit HKEY LOCAL MACHINE\SYSTEM exportie-

ren, in RegRipper Report erstellen

Option 2 Systemwerkzeuge wie msinfo

Forensische Anwendungsfälle

Suchen mit X-Ways

Image einbinden. Datei nach hex-Nach Hexwert in Bild Wert durchsuchen

Nach ASCII-String in Image einbinden, nach Text-Wert su-

chen mit ASCII-Codepage Dokument Nach Unicode-String in Image einbinden, nach Text-Wert suchen mit Unicode-Codepage Dokument

in docx-Datei

Carving

Image einbinden, Indexieren, Index nach Text-Wert durchsuchen mit ASCII- oder Unicode-Codepage

Carving-Programm durchsucht Dokument von Anfang nach Anfangssignatur, Markierung, Suchen Richtung Ende nach Endesignatur; Bereich dazwischen in Datei kopieren

Schattenkopie

Volume-Shadow-Copy-Service (VSS) hält Dateien in mehreren Versionen, Versionen können über Eigenschaften \rightarrow Versionen eingesehen werden. Zur Analyse Schattenkopie mounten

Thumbs.db

Inhalte können mit Thumb.db-Viewer sichtbar gemacht werden (bildlich oder als Liste): Ungefähres Erscheinungsbild. Speicherort des Originals und Veränderungsdatum kann eingesehen werden

Überwachter Ordnerzugriff

(Details auf eigenem CheatSheet) Angriffsmöglichkeiten prüfen, dazu:

Ist überwachter Windows Defender, Registry oder

Ordnerzugriff aktiviert? Gruppenrichtlinien

Falls aktiviert, sind diese geschützt Standardverzeichnisse Zusätzliche VerzeichnisseSchauen ob Verzeichnis hinzuge-

fügt (in Registry oder Windows

Defender)

Schauen ob Anwendungen erlaubt Erlaubte Anwendungen

sind (in Registry)

Nutzung OneDrive

Anhaltspunkte zur Nutzung

UserFolder

ClientFirstSignInTimestamp

UserCID

Logdateien

Schauen ob vorhanden Erster Login des Nutzers Falls vorhanden muss genutzt worden sein

Infos zu Anzahl Dateien, Up-/Downloadgeschwindigkeit,

UserCID

UNIX

Systemzustand

Werkzeuge verwenden Informationen aus /proc-Verzeichnis

Uptime /proc/cpuinfo Systemauslastung /proc/stat Speicherauslastung /proc/meminfo Version BS /proc/version Dateisysteme /proc/filesystem

Fehler und Verbesserungen bitte melden:

https://github.com/michkoll/latex-template-cheatsheet/issues