

8 bits

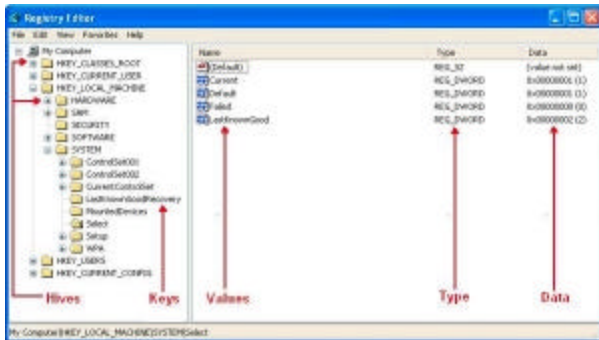
Techblog over IT, informatiebeveiliging en open source forensics

28-12-07

Forensische analyse van het Windows register

Ik kwam op het internet een uiteenzetting tegen hoe je het Windows register kunt analyseren. Het artikel kan een leidraad zijn tijdens onderzoek van het register.

Structuur van het Windows register



(c) www.forensicfocus.com

Volgens het artikel kan het register worden bekeken als een 'bestandssysteem op zich'. Als je de 'key pane' van de register editor bekijkt (Windows XP > START > regedit) dan zie je een georganiseerd rijtje met mappen staan. De vijf mappen die hiërarchisch gezien bovenaan staan worden 'hives' genoemd en beginnen allemaal met HKEY (wat een afkorting zou zijn van Handle to a Key).

Alhoewel vijf hives zichtbaar zijn zijn er slechts twee echt: HKEY_USERS (HKU) en HKEY_LOCAL_MACHINE (HKLM). De andere drie hives zijn snelkoppelingen of aliases van onderwerpen die binnen de twee 'echte' hives aanwezig zijn.

Elke hive is samengesteld uit een collectie keys, die op hun beurt waarden (values) en subkeys bevatten. Zoals je in het voorbeeld kunt zien worden de values gevormd door namen van bepaalde items binnen een key. Deze items vertegenwoordigen allerlei eigenschappen van het besturingssysteem en veel programma's zijn van de diverse items afhankelijk. Het Windows register wordt vaak vergeleken met de Windows Explorer.

Meer informatie over het register [vind je hier](#).

Gebruikte tools

Het artikel gaat uit van het gebruik van regedit.exe (de standaard register viewer van Windows XP). Ik heb zelf ook gebruik gemaakt van de [registry viewer van Werner Rumpeltesz](#), FTK Imager, het [offline registry parsing script](#) en [RegistryReport](#).

Bestanden kopiëren

Voor je het onderzoek gaat doen in het Windows register is het handig om met behulp van bijvoorbeeld FTK Imager de volgende bestanden naar een aparte map te kopiëren:

```
c:\Documents and Settings\gebruikersnaam\ntuser.dat
c:\Windows\system32\config\SYSTEM
c:\Windows\system32\config\SOFTWARE
c:\Windows\system32\config\SAM
```

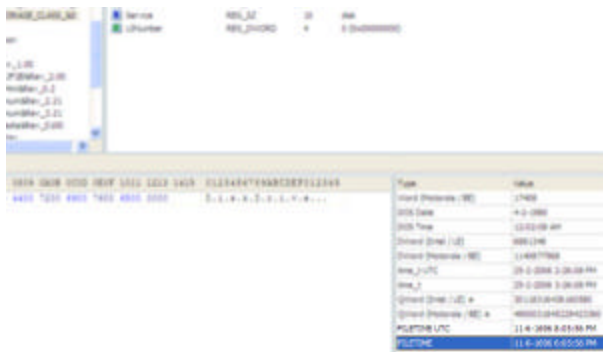
c:\Windows\system32\config\SECURITY

Algemene informatie

Ten eerste is het goed om een aantal zaken te weten te komen. Ik gebruik eerst RegistryReport van Werner Rumpeltesz. Na het downloaden van deze tool wordt een map aangemaakt met de naam Sys32Config. Als je de bovengenoemde bestanden SYSTEM, SOFTWARE, SAM en NTUSER.DAT naar deze map Sys32Config kopieert, en je start vervolgens het programma RegReport.exe, dan kun je een rapport opstellen met een schat aan informatie.

Het register als logboek

Alle keys in het register bevatten een waarde met de 'LastWrite' tijd. Je kunt het vergelijken met de last modified tijd van een bestand. Deze waarde wordt opgeslagen als FILETIME structuur en geeft aan wanneer de specifieke registersleutel voor het laatst is gewijzigd. Met de registry viewer van Rumpeltesz kun je dit FILETIME attribuut bijvoorbeeld zien.



Volgens de Microsoft Knowledge Base vertegenwoordigt een FILETIME structuur het aantal '100 nanoseconden intervals' dat is verstreken sinds January 1, 1601. De LastWrite tijd wordt geupdated op het moment dat een registerkey wordt aangemaakt, gewijzigd, gebruikt of gewist. Als er niet veel is gebeurd met de registerkey kan het dus zijn dat een datum ergens in het jaar zestienhonderdzoveel wordt getoond in plaats van de werkelijke datum. Helaas kan alleen de LastWrite tijd van een key worden verkregen en niet de LastWrite tijd van de value die de key vertegenwoordigt. Via programma's zoals de registry viewer kan de LastWrite tijd niet worden verkregen.

De LastWrite tijd van elke afzonderlijke registerkey heb ik kunnen verkrijgen met het offline registry parsing script.

Na het downloaden van het offline registry parsing script kun je met FTK Imager een registerbestand (bijvoorbeeld Windows > system32 > config > system) kopiëren naar de map waarin regp.pl staat. Vervolgens voer je met een dosbox het commando in:

```
perl regp.pl c:\mijnmap\system > mijnlogbestand.log
```

Vervolgens kun je het logbestand uitstekend met een programma als Windows WordPad bekijken. Het kan eigenlijk niet eenvoudiger.

Het kan voor een onderzoek van belang zijn om de LastWrite tijd van een key te kennen, want die gegevens kunnen met een gebeurtenis of tijdstip in verband worden gebracht. Helaas blijft het wel altijd vaag wat er

precies is gewijzigd, want alleen de LastWrite tijd van de key wordt geregistreerd en niet die van de value die de key vertegenwoordigt. In elk geval kan het interpreteren van het "register als log", in combinatie met andere gegevens zoals MAC tijden (Modified, Accessed, Created) soms helpen om meer duidelijkheid te krijgen.

Autorun lokaties

Autorun lokaties zijn registerkeys die programma's of applicaties op kunnen starten tijdens het bootproces. Het is altijd een goed idee om hiernaar te kijken tijdens een onderzoek. Bijvoorbeeld, als via een bepaalde computer vermoedelijk is ingebroken op een systeem, dan moet gekeken worden naar de autorun lokaties. Via de autorun lokaties kan bijvoorbeeld aan het licht komen dat de computer zelf was besmet met een trojan / backdoor.

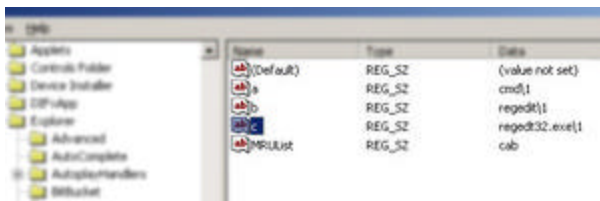
Een aantal bekende autorun lokaties:

HKLM\Software\Microsoft\Windows\CurrentVersion\Runonce
HKLM\Software\Microsoft\Windows\CurrentVersion\policies\Explorer\Run
HKLM\Software\Microsoft\Windows\CurrentVersion\Run
HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Run
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
(ProfilePath)\Start Menu\Programs\Startup

MRU lijst

MRU, ofwel de 'most recently used' lijst bevat items die zijn aangemaakt ten gevolge van handelingen van de gebruiker. In feite zijn er in het gehele register talrijke MRU lijsten aanwezig. Het register bewaart deze lijsten voor het geval dat de gebruiker deze in de toekomst weer nodig heeft. Een voorbeeld van een MRU lijst in het Windows register is de RunMRU key. Als een gebruiker een commando uitvoert via 'run' ('uitvoeren') in het Start menu, dan wordt deze handeling opgeslagen in deze registerkey

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU



Dit voorbeeld geeft aan dat via 'run' de volgende commando's zijn ingevoerd:

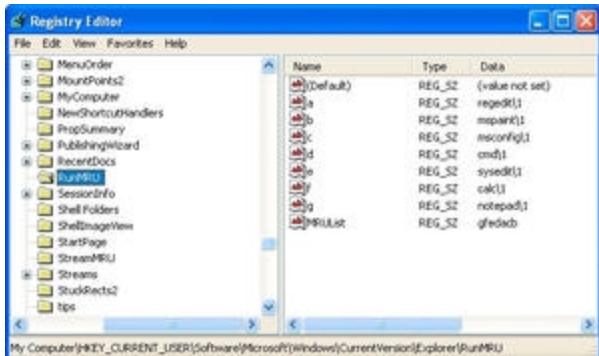
cmd
regedit
regedt32.exe

Via de key MRUList kun je zelfs zien in welke volgorde de commando's zijn gegeven:

cab
a = cmd
b = regedit

c = regedt32.exe

Oftewel, eerst is het commando regedt32.exe gegeven, daarna het commando cmd en als laatste het commando regedit.



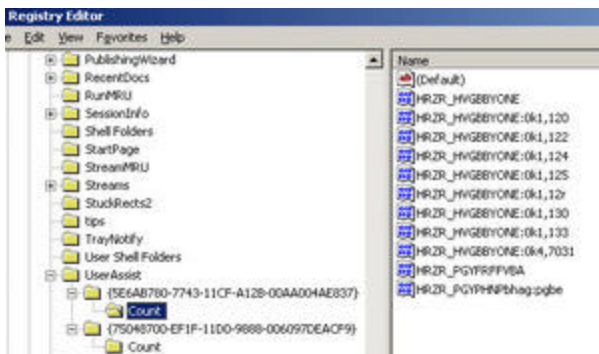
Met de informatie die RunMRU geeft kan een beter beeld gevormd worden van de gebruiker en de applicaties die hij heeft gebruikt. Bijvoorbeeld, als je in de RunMRU lijst ziet staan dat de gebruiker commando's heeft gebruikt zoals msconfig, cmd, sysedit en regedit kan worden aangenomen dat hij meer dan gemiddeld met een computer om kan gaan.

UserAssist

De UserAssist key,

HCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist

bevat twee of meer subkeys met lange hexadecimalen namen. Deze subkeys hebben de functie van globally unique identifiers (GUIDs). Elke subkey bevat waarden die verwijzen naar specifieke objecten die de gebruiker op het systeem heeft benaderd, zoals het Control Panel, snelkoppelingbestanden, programma's etc. Deze waarden zijn echter encrypted via het ROT-13 (ofwel Caesar) algoritme. Deze encryptie is eenvoudig te ontcijferen, want elk karakter wordt vertegenwoordigd door een letter uit het alfabet dat dertien letters verderop staat in de ASCII tabel. Een tooltje om de code te ontcijferen [vind je hier](#).



Een voorbeeld, in mijn geval vind ik de tekst HRZR_HVGBBYONE. Ik kopieer deze tekst en ik ga naar de pagina <http://edoceo.com/utilitas/rot13>. Hier plak ik de tekst in het juiste veldje en ik decodeer, waarna ik de tekst UEME_UITOOLBAR zie verschijnen.

Met de UserAssist key kun je een beter beeld krijgen van het soort bestanden of applicaties zijn benaderd op een bepaald systeem.

Draadloze netwerken

Een wifikaartje (draadloze ethernet card) zoekt contact met allerlei access points in de omgeving, die

gevonden kunnen worden dankzij hun SSID (service set identifier). Wanneer iemand contact maakt via een netwerk of een hotspot, dan wordt de SSID gelogd door Windows XP als voorkeursnetwerk. Deze SSID's kunnen worden teruggevonden in

HKLM\SOFTWARE\Microsoft\WZC\Parameters\Interfaces key

Onder deze key kunnen een aantal subkeys staan, welke lijken op GUIDs. De inhoud moet in elk geval de waarden 'ActiveSettings' en 'Static#0000' bevatten. In de binaire data van de 'Static#' waarden staan de netwerk SSIDs van alle draadloze access points waarmee het systeem verbinding heeft gemaakt. Om dit te zien moet je met de rechtermuisknop 'modify' selecteren.

Naast de naam van de SSID logt Windows ook de instellingen van het netwerk tijdens de specifieke verbinding, zoals het IP adres, dhcp domein, subnet mask etc. Deze gegevens staan in:

HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\

Op basis van deze draadloze netwerkinformatie kan een onderzoeker vaststellen of iemand verbinding heeft gemaakt met een specifiek draadloos netwerk, inclusief de timeframe, IP adres dat door de dhcp server werd toegekend etc. Dit kan bijvoorbeeld van pas komen als moet worden aangetoond dat iemand zich schuldig heeft gemaakt aan een strafbaar feit tijdens wardriving.

LAN Computers

Windows XP bevat een netwerk mapping tool met de naam My Network Place. Hiermee kunnen gebruikers eenvoudig andere gebruikers op een LAN (Local Area Network) vinden. Een computer die goed is aangesloten op een LAN moet via My Network Place alle andere gebruikers van het netwerk kunnen zien. Deze lijst met gebruikers of computers is opgeslagen in het register. Ook als iemand niet meer verbonden is met een LAN kun je de lijst nog wel vinden in het register:

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComputerDescriptions

De ComputerDescriptions key is bruikbaar wanneer vastgesteld moet worden of een gebruiker verbinding met een bepaald netwerk heeft gemaakt.

USB Devices

Iedere keer als een device wordt aangesloten aan een Universal Serial Bus (USB) dan zorgt Windows ervoor dat drivers worden geactiveerd en dat informatie over het device wordt opgeslagen in het register. Je kunt bijvoorbeeld informatie vinden in:

HKLM\SYSTEM\ControlSet00x\Enum\USBSTOR

Deze sleutel bewaart informatie over USB devices die ooit op het systeem aangesloten zijn geweest. Onder elk device staat het Device ID, dat meteen ook het serienummer van het device is. Deze serienummers zijn uniek en worden door de fabrikant verstrekt. Niet elke USB device heeft een serienummer, dit zie je over het algemeen aan het '&' symbool voor het tweede karakter van de device ID. Met andere woorden, als het tweede karakter van het device ID een & is, dan heb je geen uniek identificatienummer.

Mounted volumes

De sleutel

HKLM\SYSTEM\MountedDevices

laat alle drives zien die met het systeem verbonden zijn (geweest). De key bewaart een database (met mounted volumes) dat door het NTFS bestandssysteem wordt gebruikt. De binaire data voor elke \DosDevices\x: waarde bevat informatie waarmee elk volume herkend kan worden. Dit is de reden waarom een externe schijf weer dezelfde driveletter wordt toegekend als deze weer aan het systeem wordt gekoppeld. Deze informatie kan handig zijn om aan te tonen welke hardware met het systeem verbonden is geweest.

Webbrowsers

Internet Explorer is de vaste webbrowser van Windows. Internet Explorer slaat veel data op in het Windows register:

HKCU\Software\Microsoft\Internet Explorer

Drie subkeys in deze key zijn het meest interessant:

HKCU\Software\Microsoft\Internet Explorer\Main

Deze subsleutel bewaart de gebruikersinstellingen zoals search bars, start pagina, formulierinstellingen etc.

De tweede, en waarschijnlijk meest belangrijke subkey is:

HKCU\Software\Microsoft\Internet Explorer\TypedURLs

Uit deze data kan blijken dat de gebruiker wellicht een gmail, hotmail of hyves account heeft alsmede welke interesses iemand heeft.

De derde subkeys is:

HKCU\Software\Microsoft\Internet Explorer\Download Directory

Deze key laat de meest recente directory zien die is gebruikt om een bestand naar te downloaden. Dit kan een beeld geven in welke map de gedownloadde bestanden staan.

Andere browsers zoals Opera, Netscape en Firefox gebruiken het register niet zoals Internet Explorer. Als deze browsers gebruikt worden worden er geen sporen achtergelaten in de TypedURLs key. Internet Explorer slaat geschiedenis op in een bestand dat bij het register bekend is: index.dat. De andere browsers hebben daar hun eigen methode voor, die niet bij het register bekend hoeft te zijn. Opera slaat geschiedenis bijvoorbeeld op in een bestand met de naam opera.dir (standaard in C:\Documents and Settings\User Profile\Application Data\Opera\Opera\profile\). Net als Opera laten Netscape en Firefox ook minimaal gegevens achter in het register. Netscape en Firefox slaan geschiedenis op in een bestand met de naam history.dat (ASCII, bijvoorbeeld in C:\Documents and Settings\User Profile\Application Data\Mozilla\Firefox\Profiles\x.default\)

P2P programma's

Peer-to-Peer (P2P) netwerken staan bekend om de uitwisseling van illegaal materiaal. Limewire laat, behoudens gegevens over de lokatie waarin het programma geïnstalleerd is, heel weinig gegevens achter in het register. Kazaa laat wat meer gegevens achter. Twee registerkeys zijn hier het meest interessant:

HKCU\Software\Kazaa

HKLM\Software\Kazaa

Een programma dat een log in het register bijhoudt is Morpheus. In dit log staat een overzicht van meest

recente zoektermen:

HKCU\Software\Morpheus\GUI\SearchRecent

Een registerkey houdt informatie over alle P2P programma's bij:

HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\
FirewallPolicy\StandardProfile\AuthorizedApplications\List

In deze lijst staan alle applicaties die toestemming hebben om de Windows Firewall te passeren. Mocht een P2P programma niet in de lijst staan, dan wordt deze automatisch geblokkeerd. Deze lijst is dus een goede plek om te zien of iemand gebruik heeft gemaakt van een P2P programma of andere downloadsoftware.

Uitgebreid overzicht

Een uitgebreid overzicht met registersleutels die voor het onderzoek van systemen van belang kunnen zijn [vind je hier](#). De lijst is samengesteld door AccessData, bekend van o.a. FTK.
