WFA: The ACMru Key Explained

Windows systems record a great deal of user activity, under the guise of optimizing the "user experience" (Note: Windows XP gets its name from the "user eXPerience"). This information is recorded and maintained automatically, without any user interaction (though some specifics steps may be taken to prevent the data from being recorded) and can be extremely valuable to a forensic analyst.

When a user performs a search on a Windows system, they may do so using the Search Assistant, accessed by clicking Start, then Search (via the Classic Start Menu display in Windows XP), and then choosing For Files and Folders…, as illustrated in figure 1.

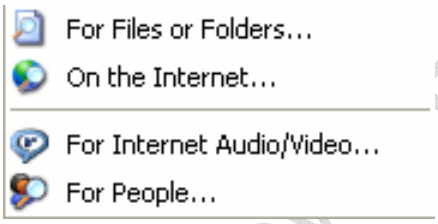

Figure 1

Note that the Search Assistant can be brought up by clicking on the desktop and hitting the F3 key.

When clicking on For Files and Folders…, the user is presented with a dialog that provides options for the search, as illustrated in figure 2.

Figure 2

Entries entered in for each of the choices next to the green icons with the white arrows are recorded in the Registry within the following key:

HKCU\SOFTWARE\Microsoft\
Search Assistant\ACMru*nnnn*

Registry keys specific to a user are most often found in the NTUSER.DAT Registry hive file located within the user's profile. The "HKCU" tag refers to the HKEY_CURRENT_USER hive, which corresponds to the Registry hive file for the currently logged on user.

The Registry subkey name "*nnnn*" is a placeholder for one of four numbers (each 4 digits long) that pertains to a specific search option. The subkeys are illustrated in figure 3.

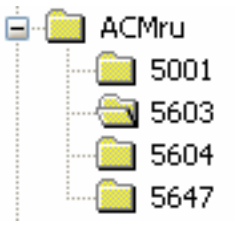

Figure 3

The 5603 subkey contains entries that the user enters into the search function when searching for "All or part of a document name:", as illustrated in figure 4.

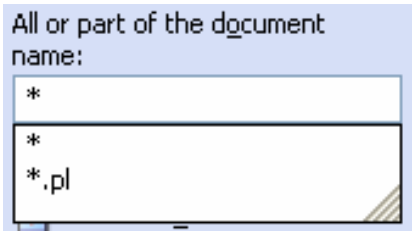

Figure 4

These entries appear in the drop-down list as shown in figure 4, and can be found in the Registry within the 5603 subkey, as illustrated in figure 5.

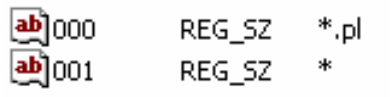

Figure 5

As illustrated in figure 5, the search terms entered by the user are saved as values named with three digits, beginning with "000". The most recent search term used is saved as "000". This indicates that the LastWrite time for the key should then correspond to the date on which the search terms were entered, and the search was run.

The 5604 subkey is populated when the user enters choices into the "A word or phrase in a file" textfield, as illustrated in figure 6.

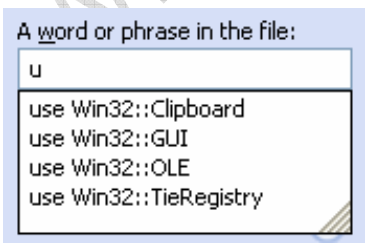

Figure 6

A forensic analyst had determined that an intruder had gained unauthorized access to a network infrastructure apparently using an employee's compromised credentials. Logs indicated that the intruder had use the Remote Desktop client to access systems within the infrastructure. The contents of the NTUSER.DAT Registry hive file within the user profile illustrated items that the intruder had searched for on the systems, providing a clue to their intentions and activities.

The 5647 subkey contains search terms entered when the user chooses to search for "Computers or People".

The 5001 subkey is populated when the user chooses to enter search terms by clicking on the "Search the Internet" choice, as illustrated in figure 7.

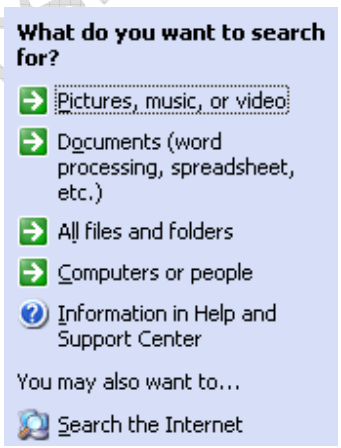

Figure 7

The 5001 subkey may also be populated by the user by opening Internet Explorer version 6.0 and hitting the Control + E key combination, or by choosing View -> Explorer Bar -> Search from the menu bar.

SrchAsst.pl

The srchasst.pl Perl script uses the Parse::Win32Registry[1] module to extract

[1] http://search.cpan.org/~jmacfarla/Parse-Win32Registry-0.30/

and display information from the ACMRu Registry key found within an NTUSER.DAT Registry hive file. A simple command line displays the information as follows:

```
C:\Perl\forensics>srchasst.pl d:\cases\ntuser.dat
Search Assistant\ACMru [Mon Sep 26 23:02:08
  2005 (UTC)]
5603 [Mon Sep 26 23:32:56 2005 (UTC)]
000  port*
001  sol.exe
002  hacker*
003  hack*
004  lad*

5604 [Mon Sep 26 23:33:30 2005 (UTC)]
000  disk
001  ha*
```

As you can see, the Perl script takes the path to an NTUSER.DAT Registry hive file as its one argument. The script then attempts to locate the ACMru key within the specified path, and if it does (the key itself may exist, but may not have subkeys if the user hasn't run any searches) extracts the LastWrite time for the key, as well as any of the subkeys that may exist. In this case, the 5603 and 5604 subkeys were located, indicating that the user had searched not only for files with specific names (i.e., "port*", sol.exe) but also for content within files (i.e., "port"). Within each subkey, the value name that is the smallest number (i.e., "0000") indicates the most recently searched for term – the date and time that this search was conducted corresponds to the LastWrite time for the key. Therefore, we are not only able to see past activity (i.e., earlier search terms) but also establish a more direct timeline for recent activity. In this case, apparently two searches had been run seconds apart, or were perhaps part of the same search.

Registry key LastWrite times are analogous to file last modification times, as they indicate when a key had last been modified, such as when a value or subkey had been added or removed, or when a value within that key had been modified. If a value is modified within a subkey (in this case, 5603), the LastWrite time for that subkey is updated, whereas the LastWrite time from the ACMru key is not affected.

Summary

Windows systems record a great deal of user activity, to include files accessed and searches run by the user. In cases involving intruder access to system via Remote Desktop or malicious insider activity, clues to their intentions can be derived from information regarding items that they search for.

Harlan is a forensic analyst located in the metro DC area, and is the author of three books related to live response and forensic analysis of Windows systems. He also presents at conferences and provides training on those same topics, as well. Comments, questions, and requests for code should be directed to him at keydet89@yahoo.com.