UserAssist: Reconstruyendo el Historial de Ejecución en Windows

En el análisis forense digital, a menudo nos enfrentamos al reto de demostrar que un usuario ejecutó un programa específico, incluso cuando el archivo original ha sido borrado o se encontraba en una unidad externa ya desconectada. Aquí es donde entra en juego **UserAssist**, uno de los artefactos más valiosos del registro de Windows para reconstruir la actividad del usuario.

¿Qué es UserAssist?

UserAssist es una característica del Explorador de Windows que registra los programas que un usuario ha ejecutado mediante la interfaz gráfica (GUI). A diferencia de otros registros que se centran en el sistema, UserAssist es específico de cada usuario, lo que permite atribuir acciones concretas a una identidad determinada.

Ubicación y Estructura

Este artefacto no se encuentra en el registro global del sistema, sino en el archivo **NTUSER.DAT** de cada perfil de usuario. La ruta técnica es:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist

Dentro de esta clave, encontraremos subclaves identificadas por **GUIDs** (Identificadores Únicos Globales). Los dos más relevantes para un analista son:

- **{CEBFF5CD...}**: Registra la ejecución de ejecutables directamente.
- **{F4E57C4B...}**: Registra la ejecución a través de accesos directos (.LNK).

El "truco" del cifrado: ROT13

Un detalle técnico fascinante de UserAssist es que los nombres de los programas no se guardan en texto claro, sino cifrados con un algoritmo simple llamado **ROT13** (una sustitución donde cada letra se desplaza 13 posiciones en el alfabeto). Por ejemplo, el nombre "Explorer.exe" se vería como "Rkcybere.rkr". Las

herramientas forenses modernas realizan este descifrado de forma automática.

Valor en la Investigación Forense (DFIR)

UserAssist proporciona tres datos críticos que permiten crear una línea de tiempo (timeline):

1. **Nombre completo del ejecutable y su ruta.**
2. **Contador de ejecuciones:** ¿Fue un evento único o un hábito?
3. **Marca de tiempo (Timestamp):** Cuándo fue exactamente la última vez que se lanzó.

Al combinar UserAssist con otros artefactos como **Prefetch** (que registra ejecuciones a nivel de sistema) o archivos **LNK** (que indican el origen del archivo), el analista obtiene una prueba irrefutable de la actividad humana tras la pantalla.

Ejercicio: "El Rastro del Intruso Interno"

Objetivo: Utilizar la lógica forense para identificar la ejecución de herramientas no autorizadas mediante el artefacto UserAssist.

Escenario:

El departamento de seguridad sospecha que un empleado de contabilidad utilizó una herramienta de recuperación de contraseñas (un archivo llamado PassView.exe) para acceder a archivos restringidos. El empleado afirma que "nunca ha oído hablar de ese programa" y el archivo no aparece en el escritorio ni en la carpeta de descargas.

Como analista, has obtenido un volcado del archivo **NTUSER.DAT** del usuario.

Tareas para el alumno:

1. **Localización:** Indica la ruta completa del registro donde buscarías las evidencias de UserAssist. ¿Por qué es importante analizar el NTUSER.DAT de ese usuario específico y no el de otro?
2. **Identificación de GUID:** Si el sospechoso utilizó un acceso directo en el escritorio para abrir el programa, ¿en qué

subclave (GUID) de UserAssist es más probable que encuentres el rastro?

3. **Descifrado manual (Desafío):** En el registro encuentras una entrada sospechosa con el nombre: CnffIvrj.rkr. Aplicando la lógica de ROT13, ¿a qué nombre de archivo corresponde?
4. **Correlación de Pruebas:** UserAssist te indica que el programa se ejecutó 15 veces y la última fue ayer a las 18:00h. Si además encuentras un archivo .LNK en la carpeta *Recent* apuntando a una unidad E:\ (un USB), ¿qué conclusión forense podrías redactar?