ROT13 en *UserAssist*

Objetivo

Que el alumno conozca:

- Un uso del algoritmo de cifrado ROT13
- Parte del registro de Windows
- Cómo se cifran las entradas de la clave UserAssist en el registro de Windows.
- El funcionamiento de algunas herramientas para análisis forense

Requisitos

- Máquina virtual con Windows 10 proporcionada como material para esta práctica.
- VMware Workstation

Introducción

Cifrado por Desplazamiento

Consiste en sustituir cada letra del mensaje por otra situada ***k*** posiciones delante de ella, en el alfabeto que se esté utilizando.

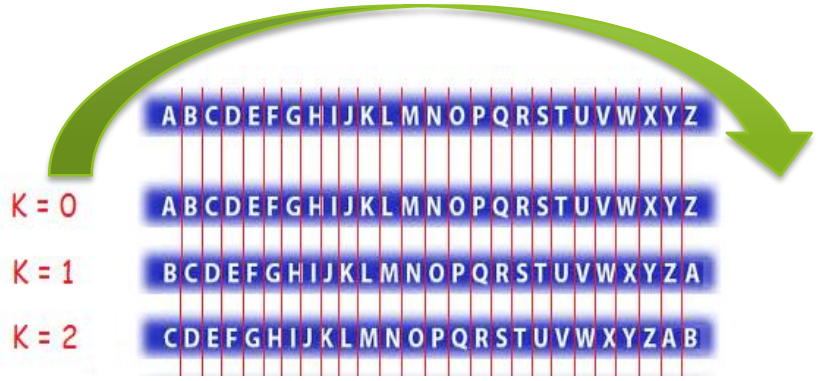

Fig. 1 Rotación del alfabeto para K=0, 1 y 2

También conocido como "Cifrado César"

Se considera que un cifrado por desplazamiento con llave **k=3** fue utilizado por el emperador Julio César (100 a.C – 44 a.C.).
"Suetonius, the gossip columnist of ancient Rome, says that Caesar wrote to Cicero and other friends in a cipher in which the plaintext letters were replaced by letters standing three places further down the alphabet. D for a, E for b, etc. Thus, the message *Omnia Gallia est divisa in partes tres* would be enciphered (using the modern 26-letter alphabet) to RPQLD JDOOLD HVW GLYLVD LQ SDUWHV WUHV"[1]

ROT13

Es un caso particular con **k=13**. La peculiaridad de esta llave radica en que, empleando el alfabeto inglés de 26 letras, al aplicar dos veces la función de cifrado se recupera el mensaje original. Con esto se tiene la ventaja de que con la misma función se puede cifrar y descifrar.

El Registro de Windows

El Registro de Windows contiene información de referencia que el sistema operativo consulta frecuentemente como información relacionada con las cuentas de cada usuario, el software instalado y su relación con los archivos creados por cada programa, propiedades de las carpetas, el hardware disponible en la computadora y los diferentes puertos de comunicación con el exterior.

Está dividido en **cinco claves** o carpetas predefinidas, que manejan distintos aspectos de la configuración del sistema operativo como se muestra en la siguiente tabla:

Clave o carpeta predefinida	Descripción
HKEY_CURRENT_USER	Contiene información de la configuración de usuario que ha iniciado sesión.
HKEY_USERS	Contiene los perfiles de los usuarios.
HKEY_LOCAL_MACHINE	Contiene información de configuración específica para el equipo.
HKEY_CLASSES_ROOT	Contiene la relación entre los distintos tipos de archivos y los programas utilizados para abrirlos.
HKEY_CURRENT_CONFIG	Contiene información del hardware cuando se inicia el sistema.

Tabla 1 Organización del Registro de Windows

Por ejemplo, cuando se instala un programa, éste realiza cambios en el Registro de Windows para indicarle al sistema operativo los tipos de archivos asociados a dicho programa. En este caso, se modifica la clave HKEY_CLASSES_ROOT

Existe una clave del registro de Windows llamada **UserAssist**, la cual contiene una lista de programas que se usan con frecuencia y que aparecen en el menú de inicio, da información sobre cuantas veces fueron ejecutados un programa y las fechas de acceso. Dicha clave se localiza en ***HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist***.

[1] Kahn, David (1967). "The Codebreakers", p. 84

Desarrollo

En el tráfico de red de una organización se han detectado diversos ataques provenientes de un equipo de cómputo perteneciente a la misma organización. Se sospecha que el empleado al que se la ha asignado el equipo ha estado realizando actividades maliciosas contra la infraestructura de la empresa.

Se aseguró el equipo de cómputo del empleado, se analizó con herramientas antivirus/antimalware alguna evidencia que demuestre que ha instalado y empleado software malicioso para llevar a cabo estos ataques, sin embargo, no se ha logrado demostrar su culpabilidad. Le han turnado el caso a usted, y ha tenido a bien revisar el acceso a los programas a través de las claves de registro de Windows de UserAssist.

Analice la llave de registro de UserAssist y determine si el empleado ha utilizado software malicioso en su equipo (en la máquina virtual).

1. Ejecutar el comando regedit para abrir el Editor del registro de Windows, esto se logra con las teclas **Windows + R**, en la ventana escribir el comando `regedit`, dar clic en el botón **Aceptar**.

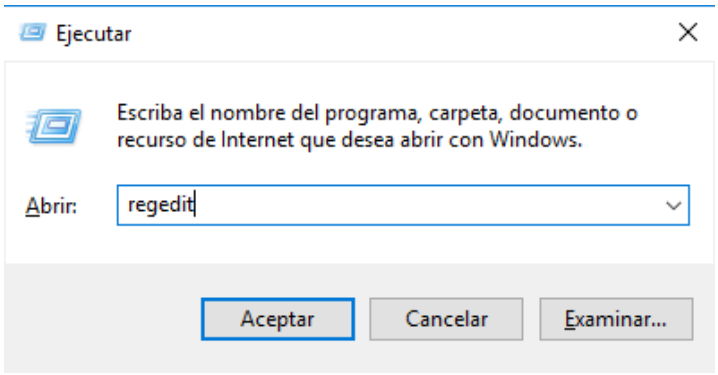

Fig. 2 Ejecutar el comando *regedit*

2. Se abrirá un cuadro de diálogo del Control de Cuentas de Usuario (User Account Control) en donde solicitará permiso para ejecutar el Editor del registro de Windows, dar clic en el botón **Sí**.

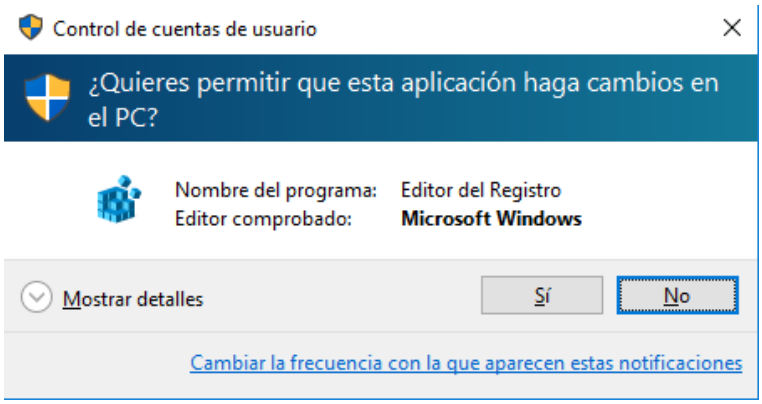

Fig. 3 Control de cuentas de usuario

3. Una vez abierto el Editor del registro de Windows buscar el registro **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}\Count**

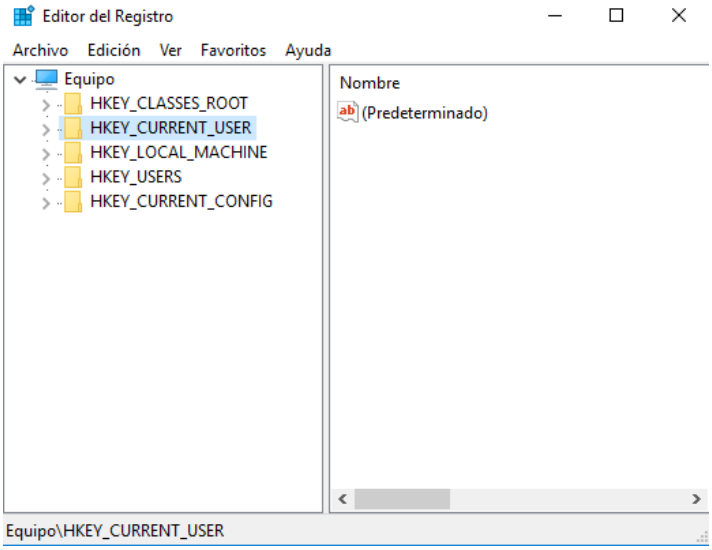

Fig. 4 Editor del registro de Windows

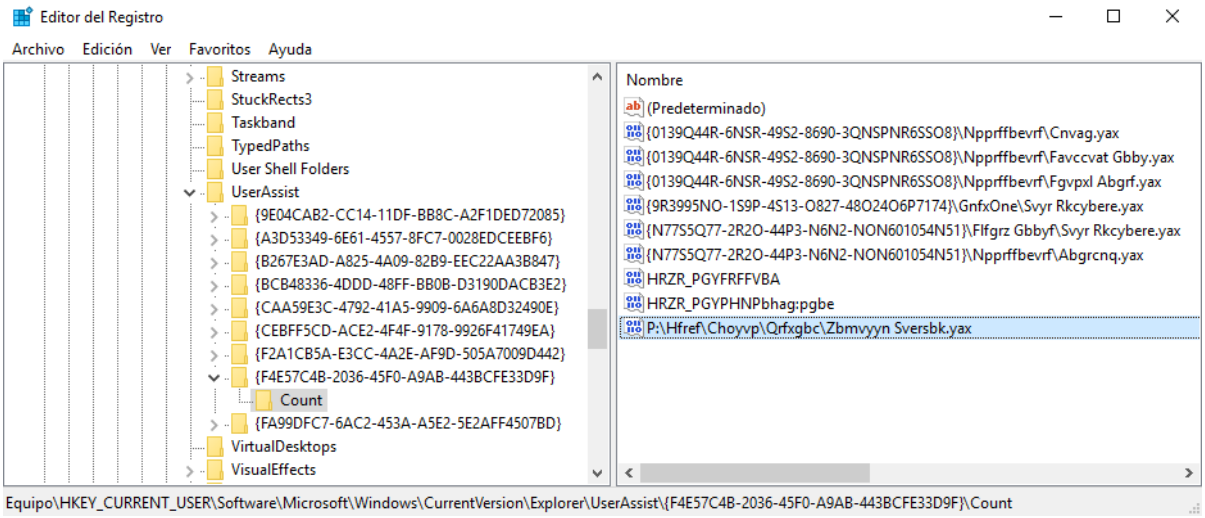

Fig. 5 Registro del User Assist

4. Una vez abierta la ruta del registro dar doble clic en uno de los registros, por ejemplo, en **P:\Hfref\Choyvp\Qrfxgbc\Zbmvyyn Sversbk.yax**.

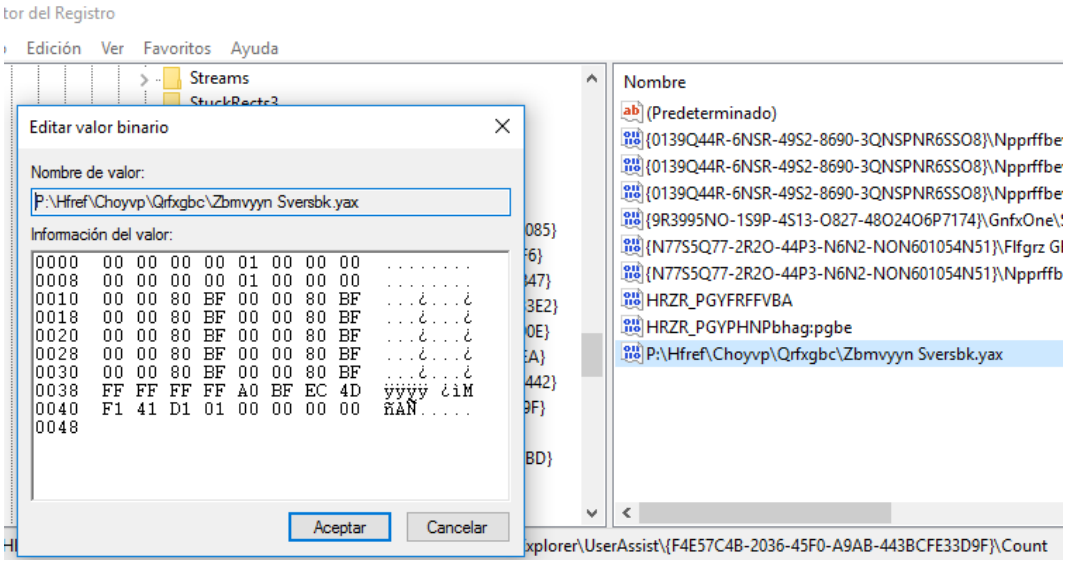

Fig. 6 Editor del valor del registro

Copiar el "Nombre de valor" de este registro y descifrar su contenido. Repita el procedimiento para cada registro.

Cuestionario

1. ¿Encontró indicios de la ejecución de software malicioso?
    a. En caso afirmativo, liste el software considerado malicioso y explique brevemente para que se usa cada uno.
2. ¿En qué directorios se encontraba cada link (*.lnk*) de los programas de reciente uso listados en el UserAssist? ¿Por qué cree que se encontraban en esas ubicaciones?
3. ¿Por qué cree que en un análisis previo no se encontraron los programas instalados en el equipo asegurado?, y ¿Por qué cree que, aunque se tienen los rastros del acceso al software malicioso, ya no se encuentra ese software instalado en el equipo?
4. ¿Qué relación tiene esta práctica con el análisis forense?
5. Investigue por qué Windows usa ROT13 para cifrar esta información e indíquelo en su reporte
6. Investigue sobre las siguientes herramientas UserAssistView v1.02 y UserAssist v2.6.0, y emita un comentario sobre su utilidad.

Elementos a calificar

1. Redacte un reporte en el que indique los pasos que considere necesarios para explicar cómo realizó la práctica, incluyendo capturas de pantalla que justifiquen su trabajo.
2. Incluya en su reporte tanto las respuestas del Cuestionario, como un apartado de conclusiones referentes al trabajo realizado.
3. Puede agregar posibles errores, complicaciones, opiniones, críticas de la práctica o del laboratorio, o cualquier comentario relativo a la misma.
4. Deberá subir el reporte en formato PDF a Classroom.

Referencias

- Microsoft. *Información del Registro de Windows para usuarios avanzados.*
- Aldeid. Windows-userassist-keys
- Microsoft. Generating Interface UUIDs

Universidad Nacional Autónoma de México

Paulo Contreras Flores
paulo.contreras.flores@ciencias.unam.mx

Jonathan Banfi Vázquez
jbanfi@ciencias.unam.mx

Tonatihu Sánchez Neri
tonatihus@ciencias.unam.mx