ROT13 En UserAssist

Jose Manuel Evangelista Tiburcio

18 de Agosto de 2024

Descripción Breve

El sistema de Cifrado de Cesar, nombrado así por el emperador Romano Julio César, es un método criptográfico "clásico" , simétrico que emplea una llave única para cifrar y descifrar, realizando un desplazamiento sobre los símbolos del alfabeto que son sustituidos k espacios a la derecha.
El objetivo es ocultar el mensaje original y generar confusión en aquellos que no deberían acceder al contenido.Un caso particular interesante es cuando k=13, conocido como cifrado **ROT13**.
Con este desplazamiento, aplicar dos veces el cifrado sobre el mismo mensaje permite recuperar el texto original, lo que convierte a ROT13 en una herramienta útil para cifrar y descifrar con la misma función. Por ello en esta práctica de forma instructiva y para ilustrar esto, realizamos un análisis sobre un caso hipotético, sobre un usuario sospechoso en una corporación donde se han realizado ataques con software malicioso, por ello se ilustra en la práctica, un caso sencillo de un "análisis forense" sobre los registros de usuario en Windows.

Respuestas a Preguntas

- **¿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.**
  Indagando un poco se pudo reconocer varias herramientas de malware, listadas a continuación:
  - njraT.lnk : NjRAT (también llamado como Bladabindi y Njw0rm) es un malware del tipo troyano que tiene como característica controlar de forma remota las máquinas infectadas
  - Poison Ivy 2.3: Es el nombre de una versión específica de una herramienta de administración remota (RAT) conocida como Poison Ivy. Caracterizado por la Difusión sigilosa, Ofuscación y Acceso remoto no autorizado.
  - ProRat.lnk: Hace referencia a un archivo .lnk (acceso directo) que está asociado con ProRat, otro tipo de herramienta de administración remota (RAT) que ha sido ampliamente utilizada para actividades maliciosas.

  - Revenge RAT:Es un Troyano de Acceso Remoto (RAT) relativamente simple y disponible de manera gratuita. Este malware está diseñado para recopilar automáticamente información del sistema infectado antes de permitir que los actores maliciosos accedan remotamente a componentes del sistema como cámaras web, micrófonos y diversas otras utilidades.

- **¿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?**
  Programas no maliciosos como Recortes, Notepad e inclusive Google Chrome se encontraban en direcciones convencionales como Accesorios, sin embargo el malware detectado, se encontraba ya en un directorio raíz, lo cual vislumbra que se intentaba dañar la computadora desde directorios directos al sistema.

- **¿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?**
  Podría deberse a que quizá el usuario que estuvo perpetrando los ataques intento ocultar su actividad, eliminándolos , o también debido a que como es malware, a través de alguna técnica este se oculto del panel de programas, aunque esto no descarta que quizá se sigue ejecutando.

- **¿Qué relación tiene esta práctica con el análisis forense?**
  El análisis Forense permite encontrar indicios de actividades irregulares, datos que se intentaron borrar e inclusive actividad sospechosa dentro (generalmente) de un equipo de cómputo, con el fin de proporcionar pruebas, a otros fines mediáticos en, comúnmente una investigación. Por lo tanto en esta práctica, ejemplifica como recuperar información almacenada en los registros del S.O. Windows permite, en este caso, descubrir que el equipo analizado era quien hacia uso de malware y por lo tanto ponía en peligro a la corporación.

- **Investigue por qué Windows usa ROT13 para cifrar esta información e indíquelo en su reporte**
  La razón por la cual Windows usa ROT13 para cifrar cierta información no es tanto por su seguridad, sino por su simplicidad y rapidez. ROT13 es un cifrado por sustitución muy básico que simplemente rota las letras del alfabeto 13 posiciones. Esto significa que el mismo algoritmo que cifra un mensaje puede ser usado para descifrarlo. En el contexto de Windows, ROT13 se ha utilizado históricamente para ofuscar información sensible en ciertos registros y configuraciones, principalmente como una forma rápida de evitar la visualización casual de datos, más que como una verdadera medida de seguridad

- **Investigue sobre las siguientes herramientas UserAssistView v1.02 y UserAssist v2.6.0, y emita un comentario sobre su utilidad.**

  Descripción: UserAssistView v1.02 es una herramienta de NirSoft que permite visualizar los datos almacenados en las claves de registro "UserAssist" de Windows.

Estas claves contienen información sobre las aplicaciones y archivos utilizados recientemente por los usuarios.

Funcionalidad:

- Muestra una lista detallada de los programas y archivos ejecutados por el usuario.
- Incluye información sobre el nombre del archivo, tiempo de ejecución, número de usos, y la última vez que fue ejecutado.
- Permite exportar la lista a un archivo de texto o CSV.

Utilidad: Es útil en análisis forense digital y auditorías de seguridad, permitiendo rastrear la actividad del usuario y verificar el uso de software en un sistema Windows.

UserAssist v2.6.0

Descripción: UserAssist v2.6.0 es otra herramienta diseñada para extraer y mostrar los datos de las claves "UserAssist" en el Registro de Windows, comúnmente utilizada en análisis forense.

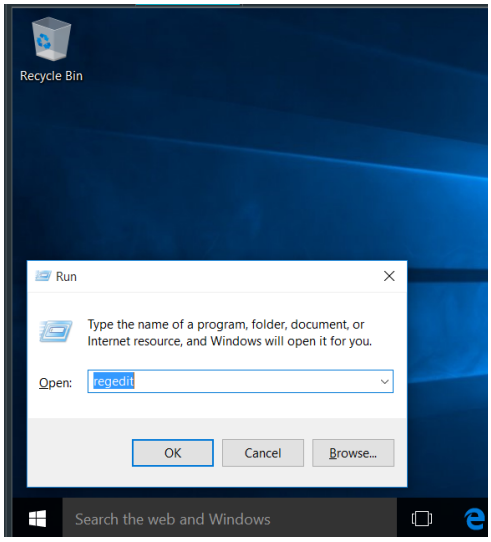
Funcionalidad:

- Muestra información sobre las aplicaciones y archivos ejecutados recientemente.
- Ofrece visualización detallada con opciones para filtrar y analizar los datos.

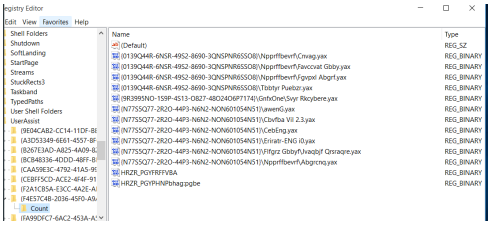
Utilidad: Al igual que UserAssistView, es valiosa en análisis forense digital y monitoreo del uso del sistema, facilitando la identificación de actividades inusuales o sospechosas.

Ambas herramientas son esenciales en la seguridad informática y el análisis forense digital, proporcionando acceso a datos de uso del sistema que son cruciales para monitorear actividades y detectar posibles amenazas o incumplimientos de políticas de uso en entornos Windows.

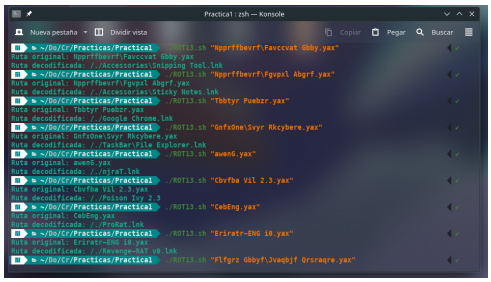
Imágenes en Secuencia



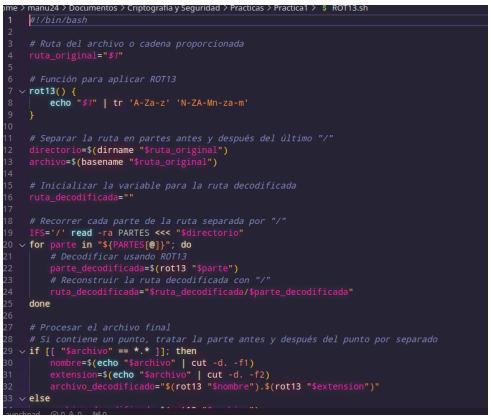
(a) Ingreso al Registro de Windows



(b) Redireccionamiento a la ruta especificada



(c) Descifrado de las rutas con ayuda del script en bash



```bash
#!/bin/bash

# Ruta del archivo o cadena proporcionada
ruta_original="$1"

# Función para aplicar ROT13
rot13() {
    echo "$1" | tr 'A-Za-z' 'N-ZA-Mn-za-m'
}

# Separar la ruta en partes antes y después del último "/"
directorio=$(dirname "$ruta_original")
archivo=$(basename "$ruta_original")

# Inicializar la variable para la ruta decodificada
ruta_decodificada=""

# Recorrer cada parte de la ruta separada por "/"
IFS='/' read -ra PARTES <<< "$directorio"
for parte in "${PARTES[@]}"; do
    # Decodificar usando ROT13
    parte_decodificada=$(rot13 "$parte")
    # Reconstruir la ruta decodificada con "/"
    ruta_decodificada="$ruta_decodificada/$parte_decodificada"
done

# Procesar el archivo final
# Si contiene un punto, tratar la parte antes y después del punto por separado
if [[ "$archivo" == *.* ]]; then
    nombre=$(echo "$archivo" | cut -d. -f1)
    extension=$(echo "$archivo" | cut -d. -f2)
    archivo_decodificado="$(rot13 "$nombre").$(rot13 "$extension")"
else
```

(d) Fragmento del Script

Figure 1: Secuencia realizada para el "análisis"