[AF] Análisis forense en sistemas Windows

Artefactos

Un aterfacto se refiere a cualquier objeto, dato o elemento almacenado en un sistema que pueda proporcionar información valiosa a una investigación. Hay 2 tipos:

- de aplicación
- de sistema operativo

Logs

Los archivos de registro o logs son artefactos interesantes en cualquier SO.

Registro de eventos

Sirve para obtener inicios de sesión, camibos de configuración, fechas, etc... Antiguamente se guardaban en %SystemRoot%\System32\config en formato .evt y actualmente van en %SystemRoot%\System32\winevt\Logs en formato evtx

NOTA: %WinDir% lleva al directorio de instalación de windows(legacy) y %SystemRoot% hace lo mismo, pero se usa en la actualidad, se recomienda usar el segundo.

Registros de aplicaciones

Pueden estar en varios sitios:

- Carpeta de instalación de la aplicación
- %AppData%: Ajustes de aplicación de un usuario
- %ProgramData%: Ajustes de aplicación comunes de todos los usuarios

Registros sobre la instalación

- %SystemRoot%\setupact.log: Información de las acciones de instalación
- %SystemRoot%\setuperr.log: Información sobre errores de instalación
- %SystemRoot%\WindowsUpdate.log: Registra información sobre actualización del sistema y aplicaciones
- %SystemRoot%\Debug\mrt.log: Resultados de la herramienta de eliminación de software malintencionado de windows (MSRT)
- %SystemRoot%\INF\setupapi.dev.log: Información de cada vez que se ha instalado un dispositivo nuevo
- %SystemRoot%\INF\setupapi.app.log: Instalación de componentes o aplicaciones
- %SystemRoot%\INF\setupapi.setup.log
- %SystemRoot%\INF\setupapi.offline.log

- %SystemRoot%\PANTHER*.log,xml: Info de errores cuando se actualiza desde otra versión

Y muchos más que están en las traspas

Papelera de Reciclaje

Almacena información de interés como archivos borrados e información sobre la fecha, hora y ubicación de los que fueron eliminados. La ruta de la papelera es C:\RECYCLED (Win 9x), C:\RECYCLER (W2000 hasta Svr2003) y C\$Recycle.bin (Vista en adelante). puede ser consultada con comandos de powershell. Dentro de la papelera hay 2 tipos de archivos

- comienzan con $I: Nombre, ruta original y algunos datos del archivo
- Comienzan por $R: Interior del archivo original