ASICI

Asociación Internacional de Ciberseguridad

Guía de la herramienta PeCmd

PECmd

PECmd (Prefetch Explorer Command Line) es una herramienta de línea de comandos desarrollada por Eric Zimmerman, un reconocido experto en forenses digitales. Está diseñada específicamente para analizar archivos Prefetch de Windows, que son artefactos valiosos en una investigación forense.

¿Qué son los Archivos Prefetch?

Los archivos Prefetch son creados por el sistema operativo Windows (desde Windows XP) para acelerar el proceso de arranque y la carga de aplicaciones. Cuando una aplicación se ejecuta por primera vez, Windows registra los archivos y recursos que la aplicación utiliza y los guarda en un archivo `.pf` en el directorio `C:\Windows\Prefetch`.

Estos archivos contienen información crucial para los forenses:

- **Nombre de la aplicación ejecutada:** El nombre del ejecutable principal.
- **Ruta de la aplicación:** La ubicación completa desde donde se ejecutó la aplicación.
- **Fechas y horas de ejecución:** Las marcas de tiempo de las últimas ocho (o más, dependiendo de la versión de Windows) veces que la aplicación fue ejecutada.
- **Recursos y archivos a los que accedió:** Una lista de los archivos `.dll`, `.exe`, y otros recursos a los que la aplicación accedió durante su ejecución. Esto puede indicar, por ejemplo, si una aplicación maliciosa cargó otras herramientas.
- **Volumenes y dispositivos:** Información sobre los volúmenes o dispositivos desde los cuales se accedieron los archivos.

¿Por qué son importantes para el Análisis Forense?

Los archivos Prefetch son una fuente de inteligencia vital para un investigador forense porque pueden:

1. **Confirmar la ejecución de programas:** Proporcionan evidencia de que un programa específico (incluyendo malware o herramientas de ataque) fue ejecutado en el sistema.
2. **Determinar cuándo se ejecutó algo:** Las marcas de tiempo de las últimas ejecuciones son fundamentales para establecer una línea de tiempo de eventos.
3. **Identificar la ubicación del ejecutable:** La ruta de la aplicación revela si se ejecutó desde una ubicación esperada (ej. `C:\Program Files`) o una sospechosa (ej. `C:\Users\Public` o una unidad USB).
4. **Descubrir actividad sospechosa:** La ejecución de herramientas de hacking, software de borrado seguro, o malware a menudo deja un rastro en los archivos Prefetch.

Descarga e Instalación

PECmd es una herramienta portátil y no requiere instalación. Puedes descargar el ejecutable directamente desde el GitHub de Eric Zimmerman (busca "PrefetchExplorer" o "PECmd"):

- **URL de descarga:** Busca en GitHub el repositorio "EricZimmerman/PECmd" o el repositorio "EricZimmerman/ForensicsTools".
- Una vez descargado, descomprime el archivo ZIP. El ejecutable `PECmd.exe` estará dentro. Es recomendable colocarlo en una carpeta de fácil acceso, como `C:\Tools\PECmd`.

Sintaxis Básica de PECmd

La sintaxis general de PECmd es:

PECmd.exe [opciones]

Opciones Principales de PECmd

Estas son las opciones más comunes y útiles para el análisis forense con PECmd.

- **`-d <directorio>` / `--directory <directorio>`:** Especifica el directorio que contiene los archivos Prefetch a procesar. Si no se especifica, PECmd buscará en el directorio Prefetch por defecto de la unidad actual (`C:\Windows\Prefetch`).
    - Ejemplo: `PECmd.exe -d "C:\Windows\Prefetch"`
    - Ejemplo para analizar prefetch de una imagen forense montada: `PECmd.exe -d "E:\Windows\Prefetch"`
- **`-f <archivo_prefetch>` / `--file <archivo_prefetch>`:** Procesa un único archivo Prefetch.
    - Ejemplo: `PECmd.exe -f "C:\Windows\Prefetch\WINWORD.EXE-F0F66683.pf"`
- **`-csv <directorio>` / `--csv <directorio>`:** Exporta los resultados a un archivo CSV en el directorio especificado. Cada archivo Prefetch analizado generará una fila en el CSV. Este es el formato de salida más útil para análisis posteriores en hojas de cálculo o herramientas como Excel/Timeline Explorer.
    - Ejemplo: `PECmd.exe -d "C:\Windows\Prefetch" -csv "C:\resultados_forenses"`
- **`-json <directorio>` / `--json <directorio>`:** Exporta los resultados a un archivo JSON en el directorio especificado. Útil para integraciones programáticas.
    - Ejemplo: `PECmd.exe -d "C:\Windows\Prefetch" -json "C:\resultados_forenses"`
- **`-html <directorio>` / `--html <directorio>`:** Exporta los resultados a un archivo HTML en el directorio especificado. Genera una vista más amigable para una rápida revisión.

    - Ejemplo: `PECmd.exe -d "C:\Windows\Prefetch" -html "C:\resultados_forenses"`
- **`-k` / `--jsonk`:** Incluye una clave "KnowledgeBase" en la salida JSON, que puede ser útil para correlacionar con otras herramientas de Zimmerman.
- **`-l` / `--timeline`:** Muestra la salida en un formato adecuado para herramientas de línea de tiempo, como plaso.
- **`-q` / `--quiet`:** Suprime la salida en pantalla. Útil cuando solo te interesa la salida a archivo.
- **`-s` / `--splunk`:** Formatea la salida JSON de manera compatible con Splunk.
- **`-v` / `--verbose`:** Muestra información adicional durante el procesamiento.
- **`-h` / `--help`:** Muestra la ayuda del comando.

Ejemplos de Uso Práctico

Aquí hay algunos escenarios comunes y cómo usar PECmd para extraer información valiosa:

1. **Analizar todos los archivos Prefetch de un sistema y exportarlos a CSV:**

   PECmd.exe -d "C:\Windows\Prefetch" -csv "C:\Forensics_Output"

   Esto creará un archivo CSV llamado `PECmd_<fecha_y_hora>.csv` en `C:\Forensics_Output` que contendrá todos los detalles de los archivos Prefetch.

2. **Analizar un archivo Prefetch específico para ver sus detalles:**

   PECmd.exe -f "C:\Windows\Prefetch\CHROME.EXE-E6822B22.pf"

   Esto mostrará los detalles de ejecución de Chrome directamente en la consola.

3. **Buscar si una herramienta sospechosa fue ejecutada (ej. `nc.exe` para Netcat):**

   PECmd.exe -d "C:\Windows\Prefetch" -csv "C:\Forensics_Output"
   # Luego, abre el CSV y busca por "nc.exe" en la columna 'Executable Name'

   Alternativamente, puedes usar `findstr` (equivalente a `grep` en Windows) si no quieres el CSV completo:

   PECmd.exe -d "C:\Windows\Prefetch" | findstr /i "nc.exe"

4. **Identificar cuándo se ejecutó por última vez una aplicación sospechosa y desde dónde:**

   PECmd.exe -d "C:\Windows\Prefetch" -csv "C:\Forensics_Output"

   Una vez generado el CSV, busca el nombre del ejecutable sospechoso. Las columnas como `Last Run 0`, `Last Run 1`, etc., te darán las marcas de tiempo, y `Application Path` te dirá la ubicación.

5. **Correlacionar ejecuciones de programas con la actividad de una unidad USB:**

   Si se sospecha que se ejecutó malware desde una unidad USB, los archivos Prefetch pueden mostrar la `Application Path` apuntando a una letra de unidad extraíble (ej. `E:\malware.exe`).

   Ejemplo de cómo se vería una línea en el CSV: `Executable Name: MALWARE.EXE, Application Path: E:\MALWARE\MALWARE.EXE, Last Run 0: 2023-07-28 14:30:15`

Consideraciones al Usar PECmd

- **Permisos:** Debes ejecutar PECmd con privilegios de administrador para acceder al directorio `C:\Windows\Prefetch`.
- **Antivirus:** Algunos antivirus pueden marcar PECmd como una herramienta de hacking o "potencialmente no deseada" debido a su naturaleza forense. Esto es un falso positivo. Es posible que debas añadirlo a las exclusiones del antivirus.
- **Volatility:** La información de Prefetch es volátil y puede ser sobrescrita o eliminada. Por ello, es crucial obtener una imagen forense del disco lo antes posible en una investigación.
- **Confiabilidad:** Las marcas de tiempo en los archivos Prefetch se basan en el reloj del sistema. Si el reloj del sistema fue alterado, las marcas de tiempo pueden ser engañosas. Siempre verifica con otras fuentes de tiempo (ej. logs del sistema, eventos de registro, marcas de tiempo de archivos).
- **Límites de tiempo:** Los archivos Prefetch guardan las últimas 8 (o más) marcas de tiempo de ejecución. Esto significa que si un programa se ejecuta muchas veces, las ejecuciones más antiguas se perderán.
- **Sistemas operativos:** Los archivos Prefetch existen en Windows XP, Vista, 7, 8, 8.1, 10 y 11. El formato puede variar ligeramente entre versiones, pero PECmd suele manejar la mayoría de ellos.

PECmd es una herramienta esencial en el kit de herramientas de cualquier analista forense, proporcionando una visión rápida y detallada de la actividad de ejecución de programas en un sistema Windows.