Prefetch

Guida approfondita del prefetch e del suo uso in forensica

Il prefetch è un sistema pensato per originariamente per aumentare la velocità con cui un programma si avvia, e tutto questo è possibile perché ad ogni avvia di un programma, un file prefetch (.pf) viene salvato nella cartella "C:\Windows\Prefetch" con nome il nome dell'eseguibile, seguito da una serie di 8 cifre esadecimali. Questi due blocchi sono separati da "-". All'interno di questo file prefetch, vengono immagazzinate le seguenti informazioni:

- Il nome dell'eseguibile
- La hash del programma (che sarebbero le 8 cifre esadecimali)
- Le dimensioni del programma originale
- La versione/i di windows supportata dal programma
- Il numero di volte che è stato eseguito (in generale, non nella sessione del pc)
- L'ultima esecuzione (Data formato yyyy-mm-dd hh:mm:ss)
- Fino a 7 altre ultime date di esecuzione (Data formato yyyy-mm-dd hh:mm:ss)
- Il nome del volume dove quel file si trova
- Il numero seriale del volume
- La data di creazione del volume
- La lista di cartelle aperte dal programma
- La lista di file (risorse) caricate dal programma

Queste informazioni sono molto utili per permettere a noi di avere una timeline abbastanza accurata dei programmi che sono stati eseguiti nel tempo. Tramite programmi come WinPrefetchView, noi possiamo analizzare in modo accurato i file presenti nella cartella prefetch, selezionarli e vedere ulteriori loro caratteristiche, come la lista di risorse di cui il programma ha fatto uso. Se invece dobbiamo analizzare in modo ancora più avanzato il prefetch, possiamo usare tool come PECmd, che ci permette di vedere ogni informazione di un file prefetch o di un insieme. Come suggerisce il nome quest'ultimo è un tool per command line, che risulta comunque molto potente e pieno di informazioni. A volte potremmo riscontrare errori nell'analisi di questi artifatti. Nel caso l'utente abbia disabilitato il prefetch, bisogna controllare la seguente chiave di registro, che è responsabile per lo stato attivo/inattivo del prefetch:

- "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters".

Il servizio che si occupa della gestione del prefetch è il “sysmain”. La persona sotto controllo potrebbe aver stoppato il servizio. Nel caso controllare con il comando “sc query sysmain”, per controllare lo stato di esso. A volte però la persona controllata potrebbe giocare uno scherzo con i permessi. Prima cosa bisogna controllare che i permessi della cartella permettano la scrittura di file al suo interno. In caso contrario la persona potrebbe usare un noto metodo bypass detto cacls. Per verificare l’esecuzione del metodo cacls, abbiamo delle query al journal che possiamo fare per verificare la modifica dei permessi alla cartella del prefetch. A volte però invece di permormare modifiche di permessi su tutta la cartella, il controllato potrebbe modificare la visibilità di un singolo file prefetch, per non dare nell’occhio. In questo caso bisogna controllare che non ci siano file nascosti, con il comando “dir /ah”, che mostra ogni file, indipendentemente dalle impostazioni sui permessi di visualizzazione.