**Prefetch**

**Concept**

* 시스템에서 실행된 응용프로그램을 분석할 때 유용한 파일로 Windows에서만 존재하는 파일로 응용프로그램이 처음 사용되는 곳을 기준으로 Prefetch 파일을 만들고, 응용프로그램을 실행할 때 속도를 향상시키기 위해서 Prefetching 기법을 사용한다.

**Introduction**

* Usage
  + Windows 운영체제에서 부팅 및 응용 실행 시 프로세스의 메모리 적재 가속화를 생성
    - Windows XP 버전에서 처음 도입
    - 동일한 실행 파일이라도 특정 위치에서 처음 실행 시 Prefetching 수행
* Function
  + 프로세스 가속화
    - Windows 부팅 프로세스(Boot Prefetching)
      * 부팅 과정에서 로드되는 악성 코드 확인 가능
      * 윈도우는 부팅 중 다양한 파일을 사용
      * 부팅과 관련된 파일을 디스크내에 퍼져 있거나 단편화 되어 부팅속도를 저하시킴
      * 부팅 시 사용되는 코드와 데이터를 모니터링 한 후 결과를 파일에 저장
      * 부트 프리패칭된 파일을 이용해서 부팅시에 부팅 속도를 향상
    - Windows 응용 프로세스(Application Prefetching)
      * 악성코드가 활용하는 리소스 목록 확인 가능
      * ‘Process Hollowing’ 기법 탐지 가능
      * 응용프로그램을 처음 실행시키면 캐시 관리자가 처음 10초 동안 모니터링 진행
      * 모니터링 하는 10초동안 메모리에 로드한 코드와 데이터 일부 혹은 전체를 파일로 생성하는 이 파일을 프리패치 파일이라고 한다.
      * 프리패칭된 응용프로그램을 다시 실행 시 프리패치 파일을 이용해서 초기 실행 속도 향상
* Limit
  + Prefetch 최대 개수
    - Windows XP, Vista, 7 -> 128개로 제한
    - Windows 8 -> 1024개로 제한
    - 오래된 Prefetch 파일부터 순서대로 삭제

**Setting Prefetch function activate**

* Path
  + HKLM\System\ControlSet001\Control\SessionManager\Memory Management\PrefetchParameters
* Level
  + Level 0: 비활성화
  + Level 1: 응용 프로그램 프리패칭만 사용
  + Level 2: 부트 프리패칭만 사용
  + Level 3: 응용/부트 프리패칭 모두 사용(Default)
* Cf
  + Window 10에서는 Boot Prefetch 파일이 없기 때문에 위의 레지스트리 값이 큰 의미가 없다
  + Windows 운영체제 번호에 따라서 프리패치의 구조가 달라진다.

**Reason for Prefetch analysis**

* 프리패치 파일은 다양한 정보를 가지고 있다 -> 분석 했을 때 얻을 수 있는 정보가 많고 활용이 가능하다.
* MetaData
  + 응용프로그램 이름
  + 응용프로그램 실행 횟수
  + 응용프로그램 마지막 실행 시간
  + 참조목록(ex. DLL, SBD, NLS, INI등의 경로)
  + 파일 시스템 시간 정보를 이용한 통합 타임라인 분석

**Path**

* %SystemRoot%\Prefetch\\*

**Compressed Prefetch File Structure – MAM File Format**

* Consist
  + File header
  + Compressed Blocks
  + Block terminator
* Compressed Method
  + Microsoft XPRESS Huffman(or LZXPRESS)
  + Microsoft XPRESS (LZ77 + DIRECT2)
* FileHeader

|  |  |  |  |
| --- | --- | --- | --- |
| OFFSET | SIZE | VALUE | DESCRIPTION |
| 0 | 4 | MAM\x04 | Signature 0x4d, 0x41, 0x4d, 0x04; Does 0x80 in the last byte indicate the presence of a checksum |
| 4 | 4 | Untitled | Total uncompressed data size |

**Uncompressed Prefetch File – SCCA File Format**

* Windows XP Windows 2003

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **A** | **B** | **C** | **D** | **E** | **F** |
| **0x00** | **Prefetcher Version** | | | | **Signature** | | | | **Prefetcher Management**  **Service Version** | | | | **File Size** | | | |
| **0x10** | **Executable File Name**  **(길이가 58byte 넘는 경우, 파일이름 끝에 0x0000 기록)** | | | | | | | | | | | | | | | |
| **0x20** |
| **0x30** |
| **0x40** |  | | | | | | | | | | **파일이름**  **> 58, 0x0000** | | **Full Path**  **Hash Value** | | | |
| **0x50** | **0x00000000** | | | | **Section Info Offset** | | | | **Num Sections** | | | | **Page Info Offset** | | | |
| **0x60** | **Num Pages** | | | | **Filename**  **Info Offset** | | | | **Filename**  **Info Size** | | | | **Metadata**  **Info Offset** | | | |
| **0x70** | **Num**  **Metadata Records**  **(Disk Volume Numbers)** | | | | **Metadata**  **Info Size** | | | | **Last Launch Time**  **(Last Execution Time)** | | | | | | | |
| **0x80** | **Min RePrefetch Time** | | | | | | | | **Min ReTrace Time** | | | | | | | |
| **0x90** | **Num Launches**  **(Execution Numbers)** | | | | **Sensitivity** | | | |  |  |  |  |  |  |  |  |

* Windows Vista, Windows 7

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **A** | **B** | **C** | **D** | **E** | **F** |
| **0x00** | **Prefetcher Version** | | | | **Signature** | | | | **Prefetcher Management**  **Service Version** | | | | **File Size** | | | |
| **0x10** | **Executable File Name**  **(길이가 58byte 넘는 경우, 파일이름 끝에 0x0000 기록)** | | | | | | | | | | | | | | | |
| **0x20** |
| **0x30** |
| **0x40** |  | | | | | | | | | | **파일이름**  **> 58, 0x0000** | | **Full Path**  **Hash Value** | | | |
| **0x50** | **0x00000000** | | | | **Section Info Offset** | | | | **Num Sections** | | | | **Page Info Offset** | | | |
| **0x60** | **Num Pages** | | | | **Filename**  **Info Offset** | | | | **Filename**  **Info Size** | | | | **Metadata**  **Info Offset** | | | |
| **0x70** | **Num**  **Metadata Records**  **(Disk Volume Numbers)** | | | | **Metadata**  **Info Size** | | | | **Unknown** | | | | | | | |
| **0x80** | **Last Launch Time**  **(Last Execution Time)** | | | | | | | | **UnKnown** | | | | **0x00000000** | | | |
| **0x90** | **UnKnown** | | | | **0x00000000** | | | | **Num Launches**  **(Execution Numbers)** | | | | **Sensitivity** | | | |

* Windows 10

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **A** | **B** | **C** | **D** | **E** | **F** |
| **0x00** | **Prefetcher Version** | | | | **Signature** | | | | **Prefetcher Management**  **Service Version** | | | | **File Size** | | | |
| **0x10** | **Executable File Name**  **(길이가 58byte 넘는 경우, 파일이름 끝에 0x0000 기록)** | | | | | | | | | | | | | | | |
| **0x20** |
| **0x30** |
| **0x40** |  | | | | | | | | | | **파일이름**  **> 58, 0x0000** | | **Full Path**  **Hash Value** | | | |
| **0x50** | **0x00000000** | | | | **Section Info Offset** | | | | **Num Sections** | | | | **Page Info Offset** | | | |
| **0x60** | **Num Pages** | | | | **Filename**  **Info Offset** | | | | **Filename**  **Info Size** | | | | **Metadata**  **Info Offset** | | | |
| **0x70** | **Num**  **Metadata Records**  **(Disk Volume Numbers)** | | | | **Metadata**  **Info Size** | | | | **Unknown** | | | | | | | |
| **0x80** | **LastLaunchTime1** | | | | | | | | **LastLaunchTime2** | | | | | | | |
| **0x90** | **LastLaunchTime3** | | | | | | | | **LastLaunchTime4** | | | | | | | |
| **0xA0** | **LastLaunchTime5** | | | | | | | | **LastLaunchTime6** | | | | | | | |
| **0xB0** | **LastLaunchTime7** | | | | | | | | **LastLaunchTime8** | | | | | | | |
| **0xC0** | **UnKnown** | | | | **0x00000000** | | | | **UnKnown** | | | | **0x00000000** | | | |
| **0xD0** | **Num Launches**  **(Execution Numbers)** | | | | **Sensitivity** | | | |  | | | |  | | | |

**Uncompressed Prefetch File Structure – File Header(Window 10)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Address Range** | **Size** | **Field Name** | **Description** |
| 0x00~0x03 | 4 Byte | Prefetch Version | Windows XP: 0x11, Windows 7: 0x17  Windows 8.1: 0x1A, Windows 10: 0x1E |
| 0x04~0x07 | 4 Byte | Signature | Signature: “SCCA” |
| 0x80~0x0B | 4 Byte | Prefetch Management  Service Version | unKnown |
| 0x0c~0x0F | 4 Byte | File Size | 파일 크기 |
| 0x10~0x49 | 58 Byte | Executable File Name | 파일 이름 |
| 0x4A~0x4B | 2 Byte | 0x0000 with filename size 58 or higher | 길이가 58byte를 넘을 경우 파일이름 끝에 0x0000을 기록 |
| 0x4C~0x4F | 48 Byte | Full Path Hash Value | 파일의 경로 해시값  <Filename>-<PathHash>.pf |
| 0x50~0x53 | 4 Byte | 0x00000000 | 0x00000000 |

**Uncompressed Prefetch File Structure**

**– File Information(Window10)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Address Range** | **Size** | **Value** | **Description** |
| 0x54~0x57 | 4 Byte | Section Info Offset | Section 정보의 위치 |
| 0x58~05B | 4 Byte | Num Sections | Section의 개수 |
| 0x5C~0x5F | 4 Byte | Page Info Offset | Page 정보의 위치 |
| 0x60~0x63 | 4 Byte | Num Pages | Page의 개수 |
| 0x64~0x67 | 4 Byte | Filename Info Offset | 파일 이름 정보의 위치 |
| 0x68~0x6B | 4 Byte | Filename Info Size | 파일 이름 정보의 크기 |
| 0x6C~0x6F | 4 Byte | Metadata Info Offset | 메타 데이터 정보의 위치 |
| 0x70~0x73 | 4 Byte | Num Metadata Records | 메타 데이터 정보의 개수 |
| 0x74~0x77 | 4 Byte | Metadata Info Size | 메타 데이터 정보의 크기 |
| 0x78~0x7F | 8 Byte | Unknown | 알 수 없음 |
| 0x80~0x8F | 64 Byte | Last Launch Time | 마지막 실행 시간 8개 |
| 0xC0~0xCF | 16 Byte | Unknown | 알 수 없음 |
| 0xD0~0xD3 | 4 Byte | Num Launches | 실행 횟수 |
| 0xD4~0x-- | - Byte | Sensitivity | 알 수 없음 |