Dreamhack-Autoruns(level1)

[forensics]

Description

드림이의 컴퓨터에 누군가가 USB 저장장치를 연결했다가 해제한 후에, 컴퓨터를 재부팅할 때마다 계산기 프로그램이 실행되고 있어요. 도대체 어떻게 된 일일까요?

Windows 레지스트리를 분석해 플래그를 찾아보세요. (2024.10.02)

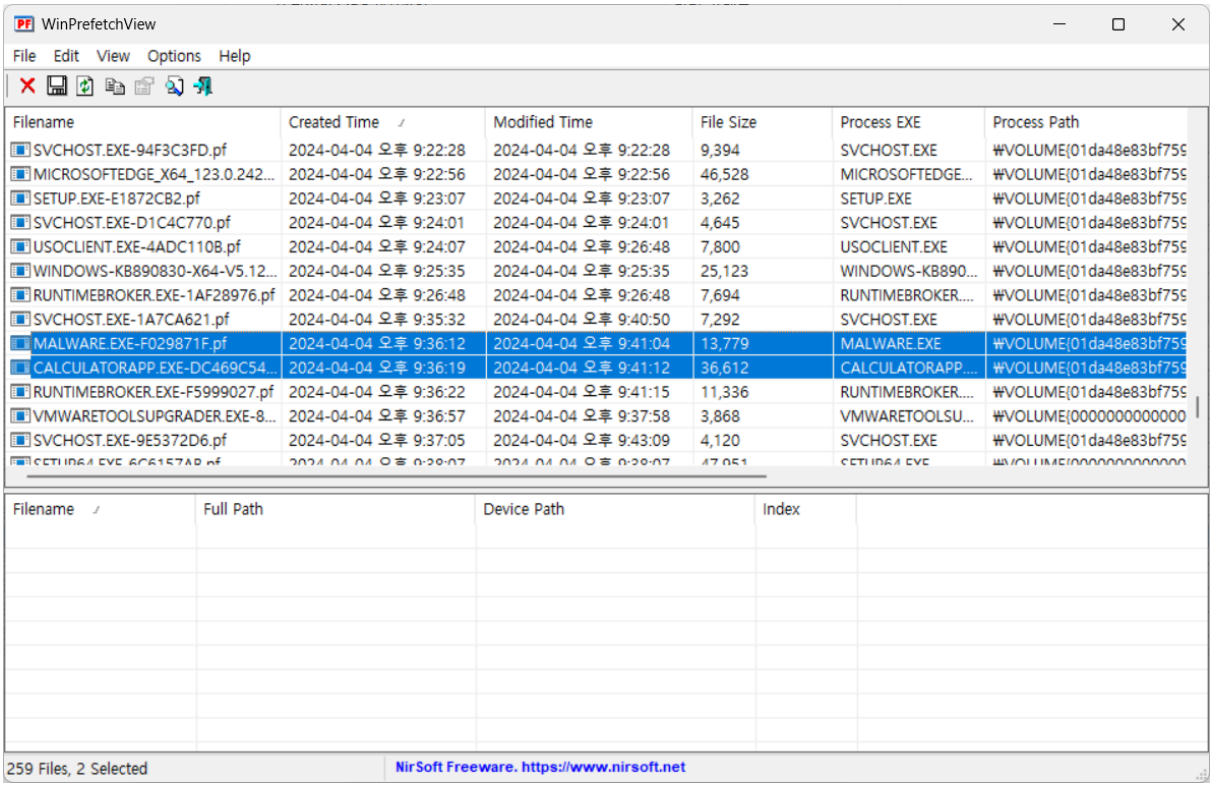
Info

FLAG = `DH{ MD5(File) }` FLAG는 자동 실행되고 있는 `exe` 파일을 MD5 해시로 계산한 값을 이용해 만듭니다. 예를 들어 대상 파일의 MD5 해시값이 `00112233445566778899AABBCCDDEEFF` 라면, 플래그는 `DH{00112233445566778899AABBCCDDEEFF}` 입니다.

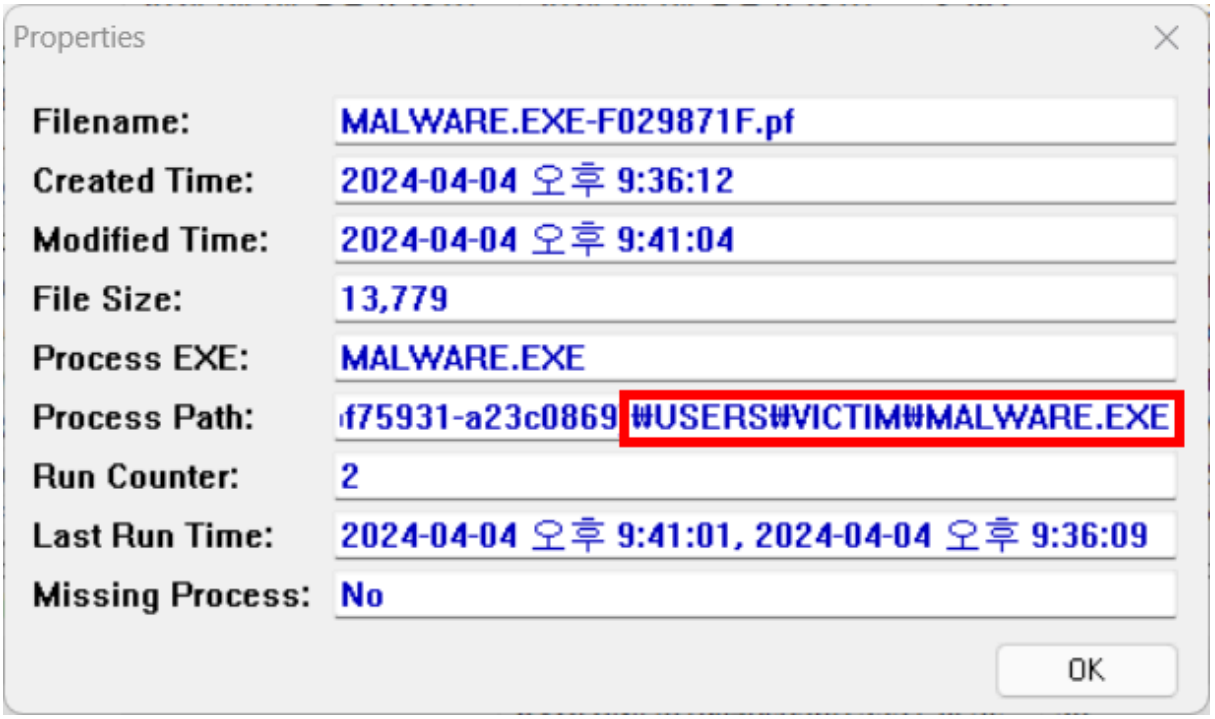
- FLAG = `DH{ MD5(File) }`
- FLAG는 자동 실행되고 있는 `exe` 파일을 MD5 해시로 계산한 값을 이용해 만듭니다. 예를 들어 대상 파일의 MD5 해시값이 `00112233445566778899AABBCCDDEEFF` 라면, 플래그는 `DH{00112233445566778899AABBCCDDEEFF}`입니다.

Write up

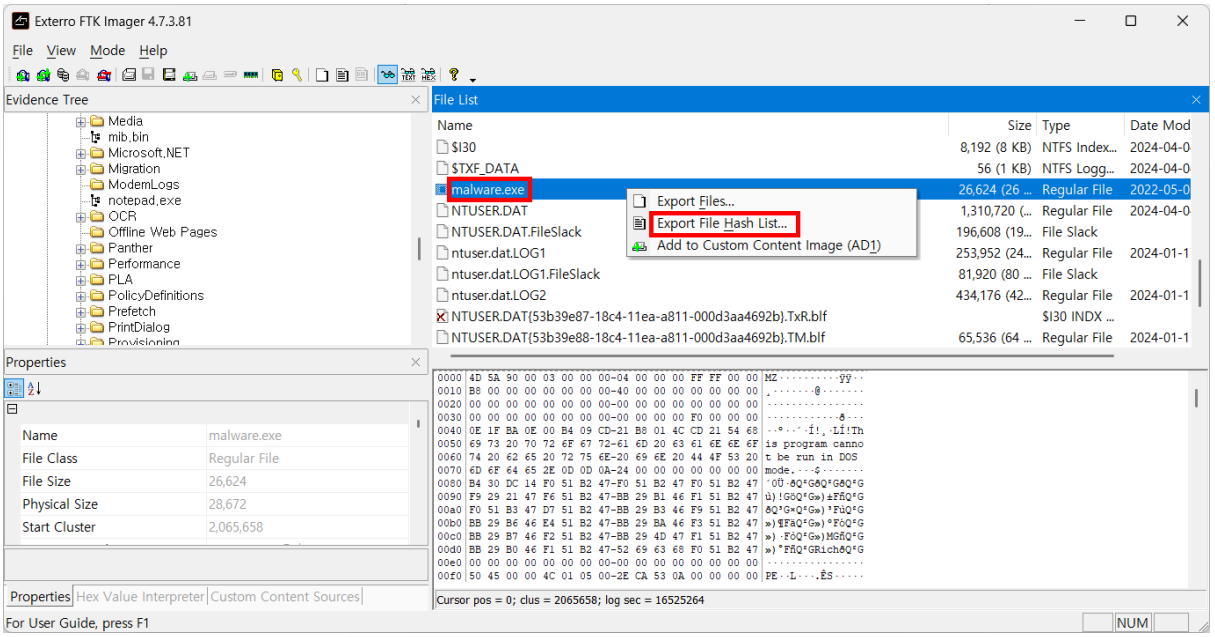
- 사용 도구: FTK Imager, WinPrefetchView
- `C:\Windows\Prefetch` 파일 추출
- USB를 통해 파일을 심고 실행을 했다면, 공격자가 심은 트리거 파일이 실행된 후 계산기가 실행되었을 가능성이 높음
- calc 키워드 검색 → 계산기가 2024-04-04 오후 9:36에 실행된 흔적 발견
- 계산기 실행 시점과 유사한 시간대에 실행된 다른 파일을 함께 확인함 (`malware.exe`)



- 의심 파일 `malware.exe`의 실제 경로를 Prefetch 분석을 통해 식별함
  - `C:\Users\victim\malware.exe`



- FTK Imager를 통해 해당 파일의 Hash List 추출



- 추출한 Hash List

MD5	302021d31f2d0bce01d7afc26bfe2ba2
SHA1	8a1c6e08700b39c943ffe5521997d36ef60e7786
FileNames	DiskImage.E01\NONAME [NTFS]\[root]\Users\victim\malware.exe

- malware.exe.의 MD5 해시를 추출한 결과, MD5: 302021d31f2d0bce01d7afc26bfe2ba2
- FLAG 형식으로는, DH{302021d31f2d0bce01d7afc26bfe2ba2}

FLAG

DH{302021d31f2d0bce01d7afc26bfe2ba2}