Dreamhack-Autoruns(level1)

문제

> 드림이의 컴퓨터에 누군가가 USB 저장장치를 연결했다가 해제한 후에, 컴퓨터를 재부팅할 때마다 계산기 프로그램이 실행되고 있어요. 도대체 어떻게 된 일일까요?
>
> Windows 레지스트리를 분석해 플래그를 찾아보세요.
>
> **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.

풀이

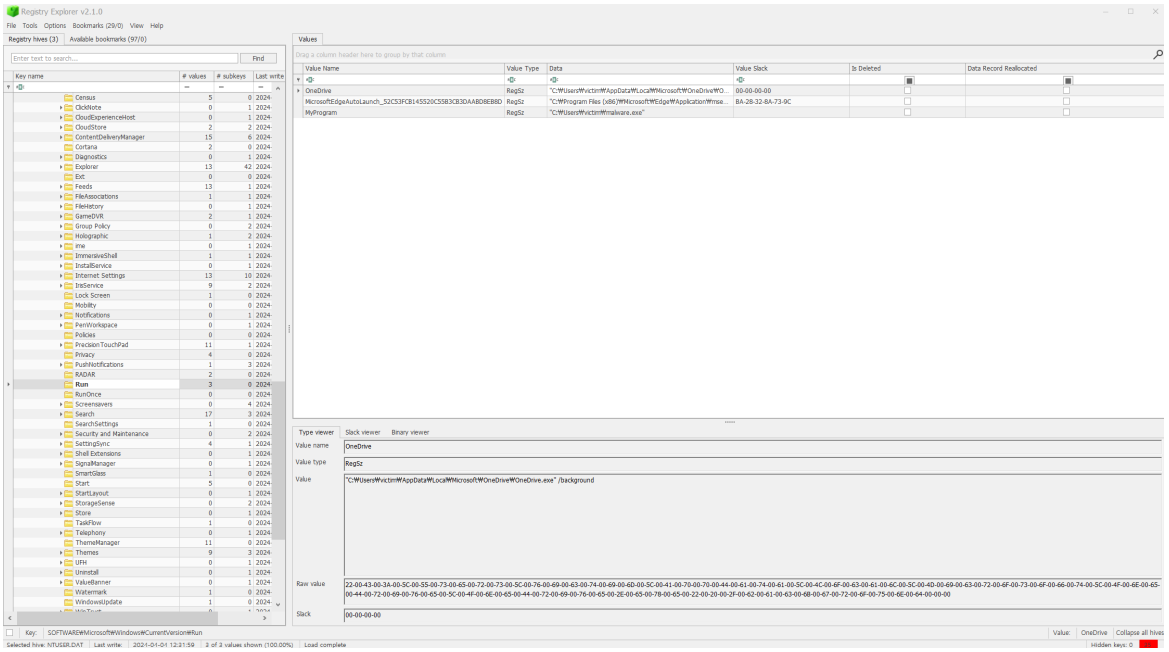
1. 문제 파악

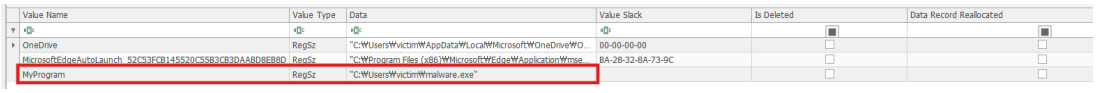
   자동 실행 설정된 .exe 파일의 이름 (또는 경로)을 레지스트리에서 찾아야 함

   레지스트리 분석을 통해 해당 자동 실행 파일을 찾고 .exe 파일의 MD5 해시값 FLAG를 찾아야 함

2. 문제 풀이

   분석한 파일 : `SOFTWARE` , `NTUSER.DAT`



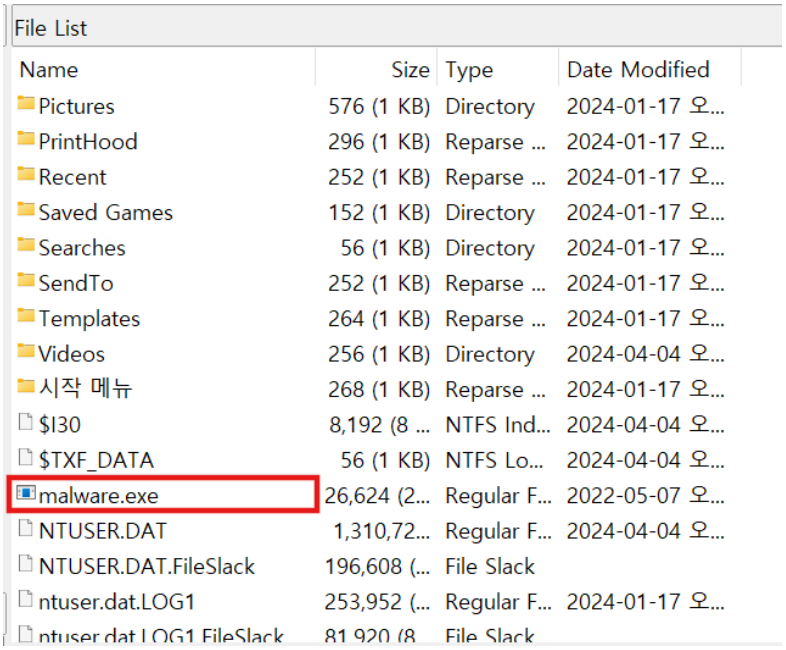


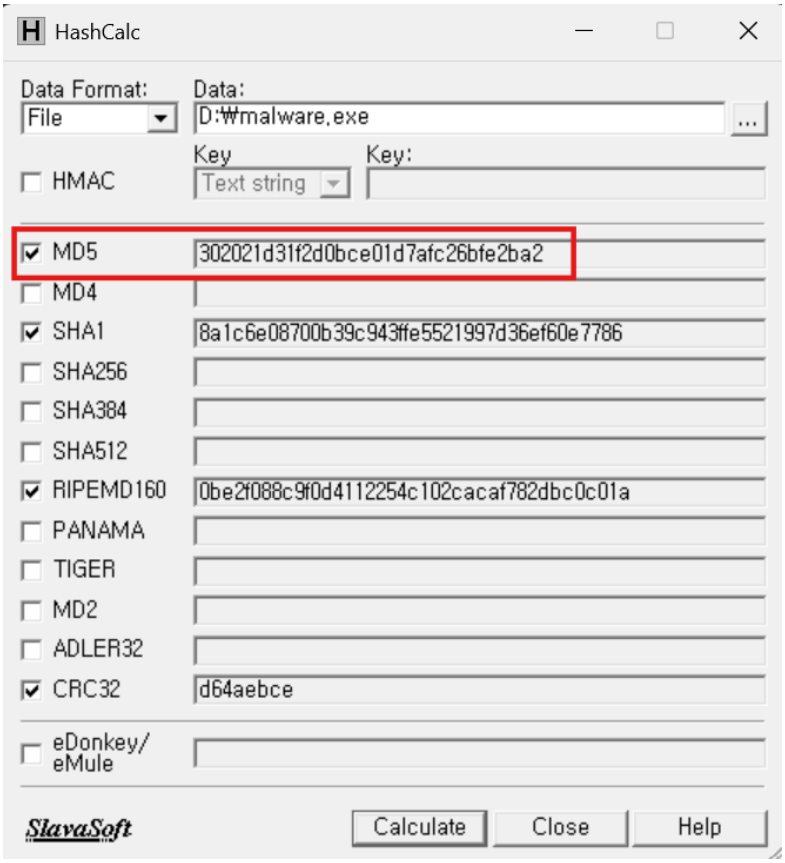
Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
OneDrive	RegSz	"C:₩Users₩victim₩AppData₩Local₩Microsoft₩OneDrive₩O...	00-00-00-00		
MicrosoftEdgeAutoLaunch_52C53FCB145520C55B3CB3DAABD8EB8D	RegSz	"C:₩Program Files (x86)₩Microsoft₩Edge₩Application₩mse...	BA-28-32-8A-73-9C		
MyProgram	RegSz	"C:₩Users₩victim₩malware.exe"			

(1) 경로 : `HKCU\Software\Microsoft\Windows\CurrentVersion\Run`

분석 내용 : 해당 레지스트리 경로는 사용자가 로그인할 때 자동으로 실행되는 프로그램을 설정하는 영역, `"MyProgram"` 이라는 이름의 실행 파일이 등록되어 있음.

(2) 분석 내용 : "MyProgram" 이 파일인 줄 알고 추출하여 해시값 입력했지만 틀려서 .exe 파일을 다시 찾아보았다,,





(3) 경로 : `C:\Users\victim\malware.exe`

분석 내용 : `malware.exe` HashCalc 도구를 이용하여 해당 실행 파일의 MD5 해시값을 계산

[MD5: 302021d31f2d0bce01d7afc26bfe2ba2]