Autoruns

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

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

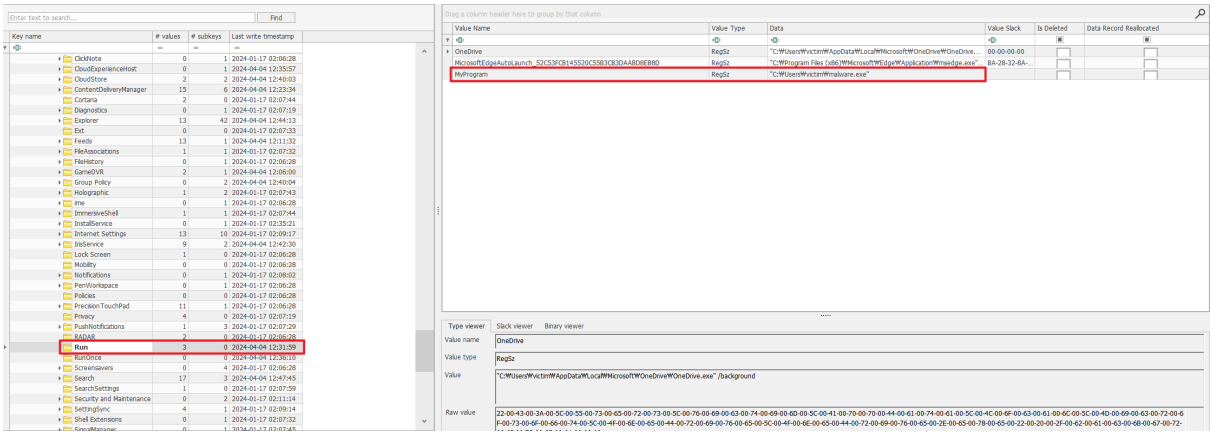
사용한 도구

FTK Imager, Registry Explorer

1. NTUSER.DAT 분석

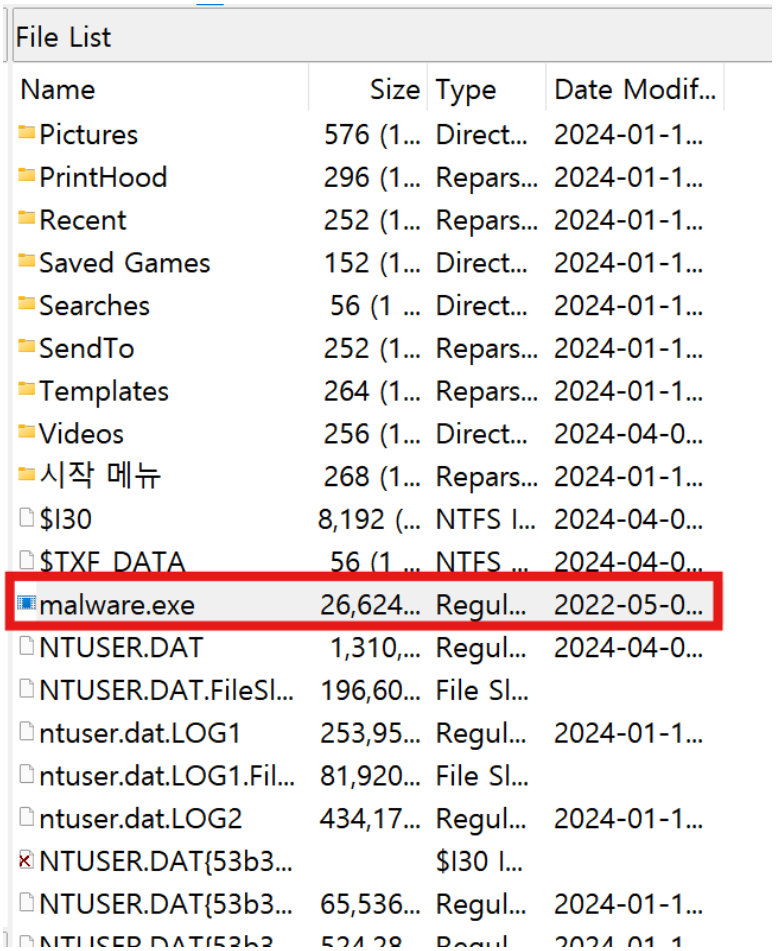
   경로: `C:Windows\Users\victim\NTUSER.DAT` 추출

   분석 내용: `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run` 내부에 존재하는 MyProgram을 확인해보면 C:\Users\victim\malware.exe가 부팅될때마다 실행되는 걸 확인할 수 있다.



2. malware.exe의 hash값 추출

- FTK Imager에서 malware.exe의 hash 값 추출




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