nikonikoni

Description

[함께실습] nikonikoni에서 실습하는 문제입니다.

당신은 고객에게서 해킹 사고를 분석해달라는 의뢰를 받았습니다.

의뢰 내용은, 갑자기 자신의 컴퓨터 배경화면이 애니메이션 캐릭터로 바뀌었다는 것이었습니다!

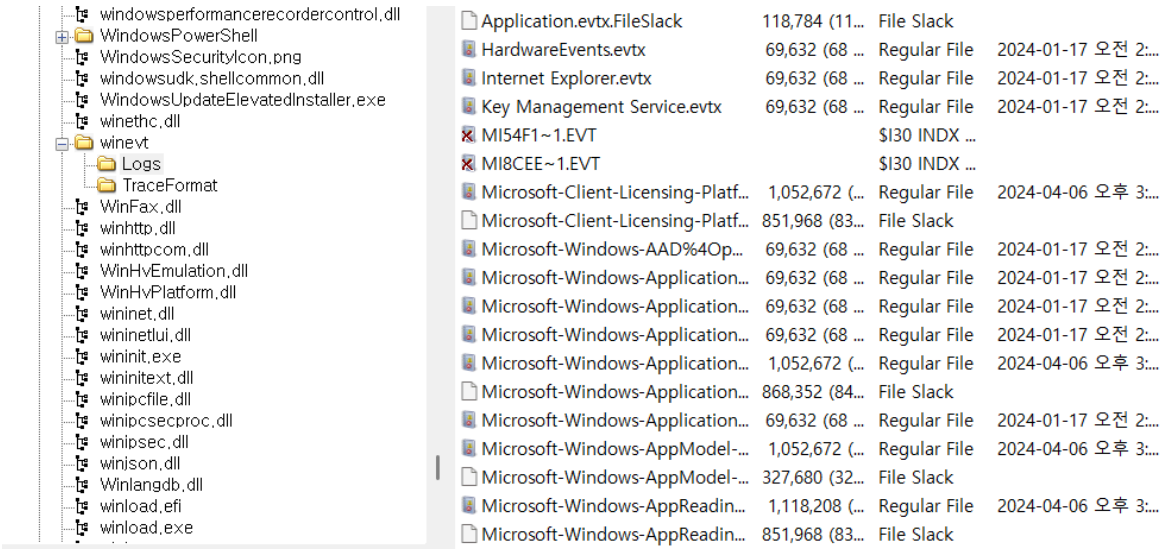
주어진 이미지의 이벤트 로그를 분석하여, 해당 PC에서 실행된 악성코드에 대해 분석해 주세요.

Info

FLAG = DH{A_B_C}
◦ A: 배경화면을 변경하는 프로그램의 이름 (경로 제외, 확장자 제외, PC에 저장된 이름 기준)
◦ B: 배경화면 이미지 파일 이름 (경로 제외, 확장자 제외, PC에 저장된 이름 기준)
◦ C: 악성 스크립트 실행 시간 (Unix Timestamp, seconds 단위)예를 들어 A가 dream, B가 hack, 그리고 C가 1712376008라면, FLAG는 DH{dream_hack_1712376008}입니다.

- FLAG = DH{A_B_C}
  - ◦ A: 배경화면을 변경하는 프로그램의 이름 (경로 제외, 확장자 제외, PC에 저장된 이름 기준)
  - ◦ B: 배경화면 이미지 파일 이름 (경로 제외, 확장자 제외, PC에 저장된 이름 기준)
  - ◦ C: 악성 스크립트 실행 시간 (Unix Timestamp, seconds 단위)
- 예를 들어 A가 dream, B가 hack, 그리고 C가 1712376008라면, FLAG는 DH{dream_hack_1712376008}입니다.

1. FTK Imager로 winevt 로그파일 확인



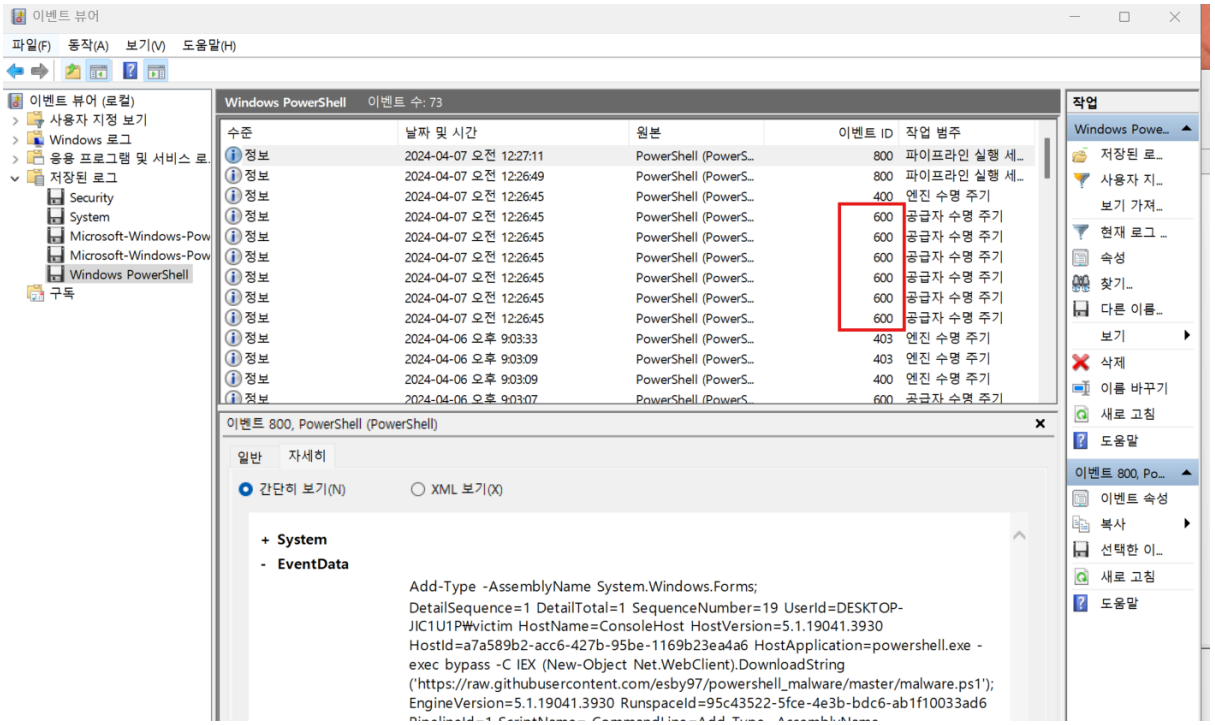
2. 이벤트 뷰어를 통해 각 로그 확인하기

https://isacacia.tistory.com/111

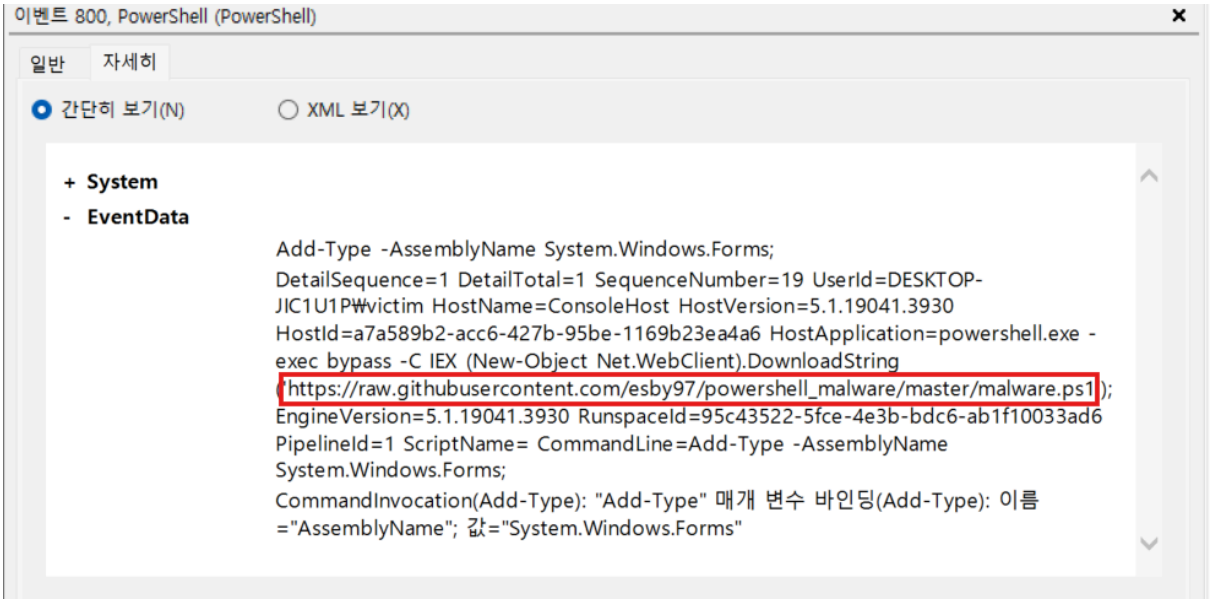
확인 해야 할 이벤트들은 아래와 같다.Windows Powershell이벤트 ID 400 - Powershell 시작이벤트 ID 600 - Powershell 코드 실행이벤트 ID 403 - Powershell 중지

powershell 을 통해 시작이벤트는 600번대 인것을 확인할 수 있다.

Windows PowerShell에서 이벤트 ID가 600번대인 것을 찾을 수 있다.



3. 해당 이벤트를 자세히 보면 malware url 경로를 확인할 수 있다



즉, 이벤트 ID가 600번대인 로그들을 보면 날짜 및 시간이 2024년 04월 07일 12:26:45초인 것을 확인할 수 있다.

4. 해당 URL를 타고 들어가면 배경화면을 변경하는 프로그램의 이름, 배경화면 이미지 파일 이름까지 확인할 수 있다.