Track the file

Description

드림이는 컴퓨터를 살펴보다가 수상한 점을 발견했습니다. 바로 malware.exe라는 프로그
컴퓨터에 생성되어 있다는 것이었어요. 드림이는 누군가가 USB를 연결해 파일을 복사해온
추측하고 있습니다.
시스템 로그를 분석해 malware.exe 파일이 시스템에 복사된 시간을 찾아보세요!

FLAG = DH{yyyy_MM_dd_hh_mm_ss}
yy, MM, dd, hh, mm, ss는 시간을 표현하는 방식으로 각각 연, 월, 일, 시, 분, 초를 나타
시간은 UTC+9를 기준으로 합니다.

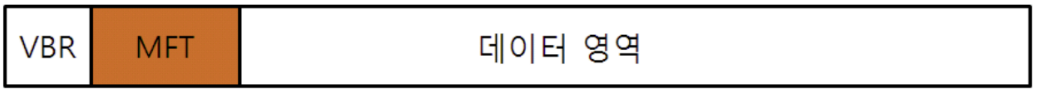
사용한 도구

FTK Imager, NTFS Log Tracker

Background

$MFT

- MFT 엔트리들의 집합



[그림1] NTFS 전체 구조

*NTFS는 VBR, MFT, 데이터 영역으로 나뉜다.

- VBR(Volume Boot Record) : 파일 시스템의 메타 데이터 저장
- MFT(Master File Table) : 각 파일과 디렉터리의 메타 데이터 저장
- 데이터 영역 : 실제 파일들의 데이터 저장

(메타 데이터 : 파일의 생성, 수정, 접근 시각 등)

$LogFile

- NTFS 트랜잭션 로그 파일
- MFT 엔트리 인덱스 2번에 주로 위치
- NFS가 정전이나 기타 오류로 인해 갑작스러운 중단시 주로 파일 손실 시 복구을 위해 사용된다

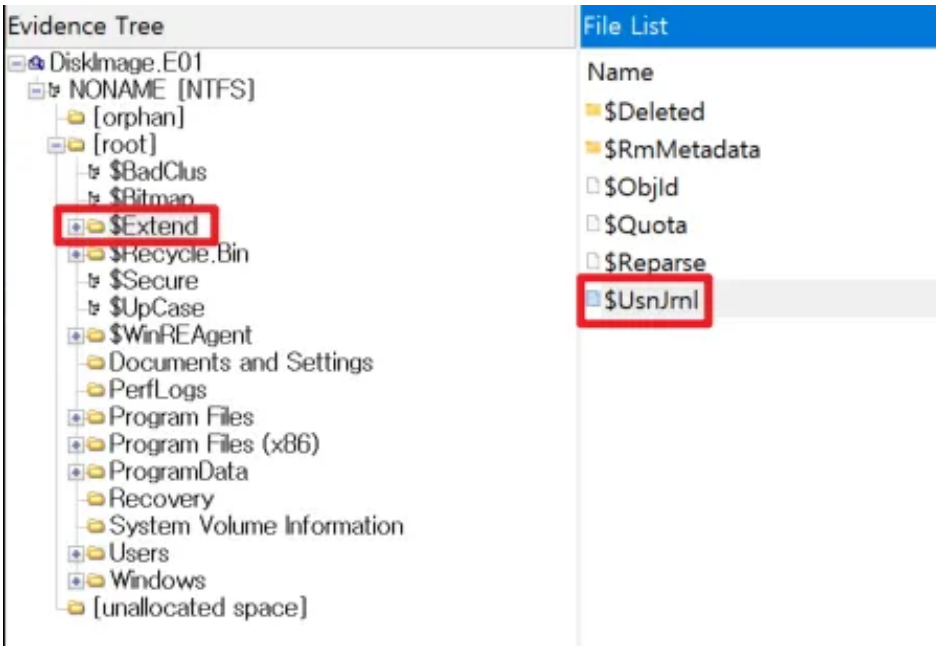
$UsnJrnl

- 응용 프로그램이 특정 파일의 변경 여부를 파악하기 위해 사용하는 로그
- NTFS 파일 시스템에서 지원하는 기능 중 하나
- LogFile과 달리 파일 복원 목적으로 기록되는 로그가 아닌 단순 파일에 작업이 있었음을 확인하기 위한 목적 → 시간 순서대로 엔트리를 저장하고 오래된 데이터는 삭제
- 파일 암호화, 이름 변경, 압축 등 다양한 이벤트를 확인 가능해 랜섬웨어 동작 분석에 많이 사용됨

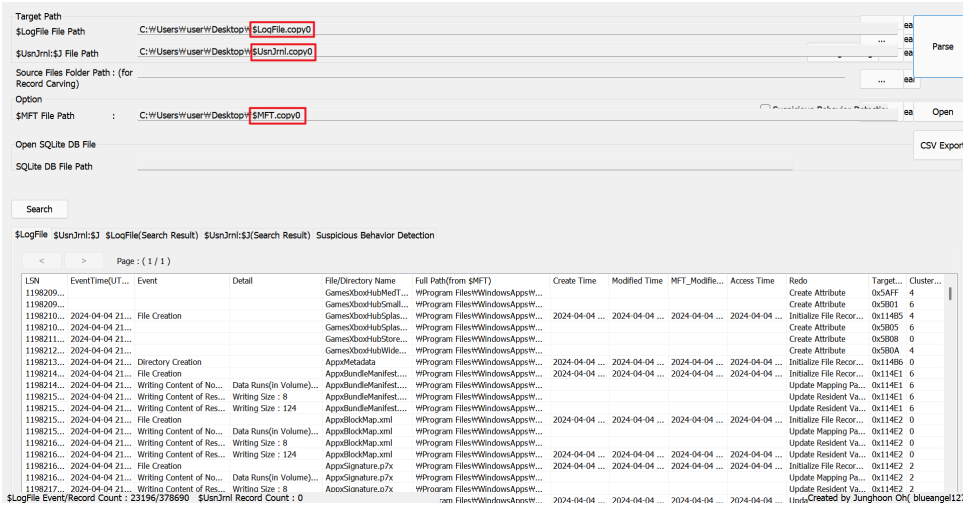
https://blog.naver.com/jsky10503/221329429863

→ 자세한 설명

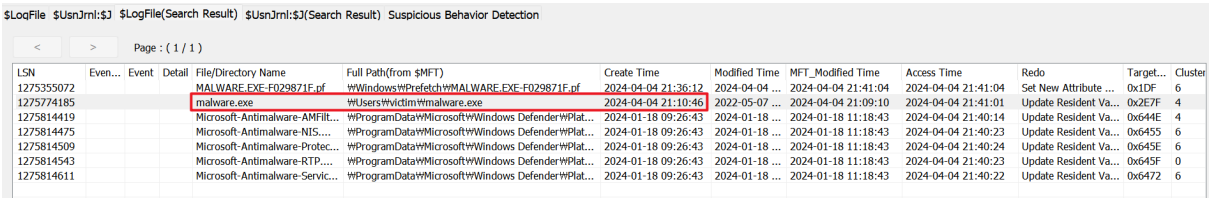
1. FTK Imager로 MFT, LogFile, JsnJrnl 추출



2. NTFS Log Tracker에 파일 3개 넣은 후 Parse



3. Search를 활용해 malware검색



LSN	Even...	Event	Detail	File/Directory Name	Full Path(from $MFT)	Create Time	Modified Time	MFT_Modified Time	Access Time	Redo	Target...	Cluster
1275355072				MALWARE.EXE-F029871F.pf	₩Windows₩Prefetch₩MALWARE.EXE-F029871F.pf	2024-04-04 21:36:12	2024-04-04 ...	2024-04-04 21:41:04	2024-04-04 21:41:04	Set New Attribute ...	0x1DF	6
1275774185				malware.exe	₩Users₩victim₩malware.exe	2024-04-04 21:10:46	2022-05-07 ...	2024-04-04 21:09:10	2024-04-04 21:41:01	Update Resident Va...	0x2E7F	4
1275814419				Microsoft-Antimalware-AMFilt...	₩ProgramData₩Microsoft₩Windows Defender₩Plat...	2024-01-18 09:26:43	2024-01-18 ...	2024-01-18 11:18:43	2024-04-04 21:40:14	Update Resident Va...	0x644E	4
1275814475				Microsoft-Antimalware-NIS....	₩ProgramData₩Microsoft₩Windows Defender₩Plat...	2024-01-18 09:26:43	2024-01-18 ...	2024-01-18 11:18:43	2024-04-04 21:40:23	Update Resident Va...	0x6455	6
1275814509				Microsoft-Antimalware-Protec...	₩ProgramData₩Microsoft₩Windows Defender₩Plat...	2024-01-18 09:26:43	2024-01-18 ...	2024-01-18 11:18:43	2024-04-04 21:40:24	Update Resident Va...	0x645E	6
1275814543				Microsoft-Antimalware-RTP....	₩ProgramData₩Microsoft₩Windows Defender₩Plat...	2024-01-18 09:26:43	2024-01-18 ...	2024-01-18 11:18:43	2024-04-04 21:40:23	Update Resident Va...	0x645F	0
1275814611				Microsoft-Antimalware-Servic...	₩ProgramData₩Microsoft₩Windows Defender₩Plat...	2024-01-18 09:26:43	2024-01-18 ...	2024-01-18 11:18:43	2024-04-04 21:40:22	Update Resident Va...	0x6472	6

malward.exe의 생성시간을 확인할 수 있다.

FLAG

DH{2024_04_04_21_10_46}