IR-1

분야	포렌식
문제 파일 (zip)	https://drive.google.com/file/d/1KhkiZXagtpBXRQ63et2ZCyDtpvAIko87/view?usp=sharing
배포 완료	☐
출제자	이현

문제

랜섬웨어에 걸린 것 같다.

최초로 감염된 파일명과 감염 시간, 어떤 파일에 의해 감염되었는지 입력하라.

파일명은 소문자로 입력, 띄어쓰기는 언더바(_) 처리, 타임스탬프는 한국 시간인 UTC+9를 따르며, ISO 8601 표준에 의해 날짜와 시간 사이에 T 문자를 입력한다.

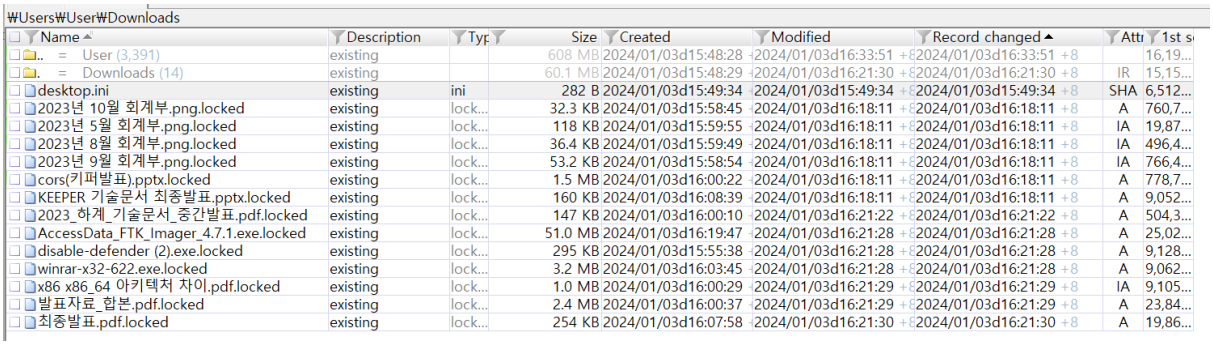
ex: KEEPER{asdf.asd_2024-12-23T12:34:56_example.exe}

답

KEEPER{2023년_10월_회계부.png_2024-01-03T17:18:11_0iajdngxorfo.exe}

풀이 과정

문제로 주어진 이미지 파일을 보면 암호화된 파일들이 보이며, 랜섬웨어에 걸렸음을 확인할 수 있다.



¥Users¥User¥Downloads

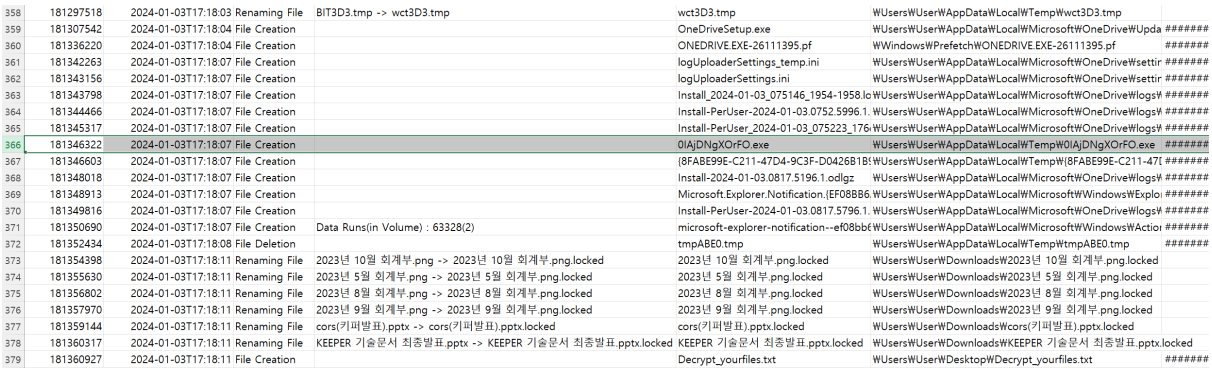
Name	Description	Typ	Size	Created	Modified	Record changed	Attr	1st s
.. = User (3,391)	existing		608 MB	2024/01/03d15:48:28	2024/01/03d16:33:51 +8	2024/01/03d16:33:51 +8		16,19...
. = Downloads (14)	existing		60.1 MB	2024/01/03d15:48:29	2024/01/03d16:21:30 +8	2024/01/03d16:21:30 +8	IR	15,15...
desktop.ini	existing	ini	282 B	2024/01/03d15:49:34	2024/01/03d15:49:34 +8	2024/01/03d15:49:34 +8	SHA	6,512...
2023년 10월 회계부.png.locked	existing	lock...	32.3 KB	2024/01/03d15:58:45	2024/01/03d16:18:11 +8	2024/01/03d16:18:11 +8	A	760,7...
2023년 5월 회계부.png.locked	existing	lock...	118 KB	2024/01/03d15:59:55	2024/01/03d16:18:11 +8	2024/01/03d16:18:11 +8	IA	19,87...
2023년 8월 회계부.png.locked	existing	lock...	36.4 KB	2024/01/03d15:59:49	2024/01/03d16:18:11 +8	2024/01/03d16:18:11 +8	IA	496,4...
2023년 9월 회계부.png.locked	existing	lock...	53.2 KB	2024/01/03d15:58:54	2024/01/03d16:18:11 +8	2024/01/03d16:18:11 +8	IA	766,4...
cors(키퍼발표).pptx.locked	existing	lock...	1.5 MB	2024/01/03d16:00:22	2024/01/03d16:18:11 +8	2024/01/03d16:18:11 +8	A	778,7...
KEEPER 기술문서 최종발표.pptx.locked	existing	lock...	160 KB	2024/01/03d16:08:39	2024/01/03d16:18:11 +8	2024/01/03d16:18:11 +8	A	9,052...
2023_하계_기술문서_중간발표.pdf.locked	existing	lock...	147 KB	2024/01/03d16:00:10	2024/01/03d16:21:22 +8	2024/01/03d16:21:22 +8	A	504,3...
AccessData_FTK_Imager_4.7.1.exe.locked	existing	lock...	51.0 MB	2024/01/03d16:19:47	2024/01/03d16:21:28 +8	2024/01/03d16:21:28 +8	A	25,02...
disable-defender (2).exe.locked	existing	lock...	295 KB	2024/01/03d15:55:38	2024/01/03d16:21:28 +8	2024/01/03d16:21:28 +8	A	9,128...
winrar-x32-622.exe.locked	existing	lock...	3.2 MB	2024/01/03d16:03:45	2024/01/03d16:21:28 +8	2024/01/03d16:21:28 +8	A	9,062...
x86 x86_64 아키텍처 차이.pdf.locked	existing	lock...	1.0 MB	2024/01/03d16:00:29	2024/01/03d16:21:29 +8	2024/01/03d16:21:29 +8	IA	9,105...
발표자료_합본.pdf.locked	existing	lock...	2.4 MB	2024/01/03d16:00:37	2024/01/03d16:21:29 +8	2024/01/03d16:21:29 +8	A	23,84...
최종발표.pdf.locked	existing	lock...	254 KB	2024/01/03d16:07:58	2024/01/03d16:21:30 +8	2024/01/03d16:21:30 +8	A	19,86...

추가로 Record changed 시간이 16시 18분, 16시 21분으로 나눠진 것으로 보아 랜섬웨어가 2번의 감염을 수행한 것으로 확인된다. (또는 단순히 랜섬웨어가 2번에 걸쳐 감염을 수행했을 수도 있다.)

더 확실하게 확인하기 위해선 $MFT, $LogFile, $UsnJrnl:J를 확인하여 디스크에 언제 생성되었고 실행되었는지 확인해야 한다.

NTFS Log Tracker를 사용하여 로그를 추출한 후 csv 파일로 뽑아낸다.

그 다음 `.locked` 확장자를 검색하고 그 주위 로그를 분석하면 된다. 랜섬웨어가 실행됨에 따라 `.locked`로 변한 것이기 때문이다.



358	181297518	2024-01-03T17:18:03	Renaming File	BIT3D3.tmp -> wct3D3.tmp	wct3D3.tmp	¥Users¥User¥AppData¥Local¥Temp¥wct3D3.tmp	
359	181307542	2024-01-03T17:18:04	File Creation		OneDriveSetup.exe	¥Users¥User¥AppData¥Local¥Microsoft¥OneDrive¥Upda	#######
360	181336220	2024-01-03T17:18:04	File Creation		ONEDRIVE.EXE-26111395.pf	¥Windows¥Prefetch¥ONEDRIVE.EXE-26111395.pf	#######
361	181342263	2024-01-03T17:18:07	File Creation		logUploaderSettings_temp.ini	¥Users¥User¥AppData¥Local¥Microsoft¥OneDrive¥settir	#######
362	181343156	2024-01-03T17:18:07	File Creation		logUploaderSettings.ini	¥Users¥User¥AppData¥Local¥Microsoft¥OneDrive¥settir	#######
363	181343798	2024-01-03T17:18:07	File Creation		Install_2024-01-03_075146_1954-1958.lo	¥Users¥User¥AppData¥Local¥Microsoft¥OneDrive¥logs¥	#######
364	181344466	2024-01-03T17:18:07	File Creation		Install-PerUser-2024-01-03.0752.5996.1.	¥Users¥User¥AppData¥Local¥Microsoft¥OneDrive¥logs¥	#######
365	181345317	2024-01-03T17:18:07	File Creation		Install-PerUser_2024-01-03_075223_176	¥Users¥User¥AppData¥Local¥Microsoft¥OneDrive¥logs¥	#######
366	181346322	2024-01-03T17:18:07	File Creation		0IAjDNgXOrFO.exe	¥Users¥User¥AppData¥Local¥Temp¥0IAjDNgXOrFO.exe	#######
367	181346603	2024-01-03T17:18:07	File Creation		{8FABE99E-C211-47D4-9C3F-D0426B1B	¥Users¥User¥AppData¥Local¥Temp¥{8FABE99E-C211-47(	#######
368	181348018	2024-01-03T17:18:07	File Creation		Install-2024-01-03.0817.5196.1.odlgz	¥Users¥User¥AppData¥Local¥Microsoft¥OneDrive¥logs¥	#######
369	181348913	2024-01-03T17:18:07	File Creation		Microsoft.Explorer.Notification.{EF08BB6	¥Users¥User¥AppData¥Local¥Microsoft¥Windows¥Explo	#######
370	181349816	2024-01-03T17:18:07	File Creation		Install-PerUser-2024-01-03.0817.5796.1.	¥Users¥User¥AppData¥Local¥Microsoft¥OneDrive¥logs¥	#######
371	181350690	2024-01-03T17:18:07	File Creation	Data Runs(in Volume) : 63328(2)	microsoft-explorer-notification--ef08bb6	¥Users¥User¥AppData¥Local¥Microsoft¥Windows¥Actio	#######
372	181352434	2024-01-03T17:18:08	File Deletion		tmpABE0.tmp	¥Users¥User¥AppData¥Local¥Temp¥tmpABE0.tmp	#######
373	181354398	2024-01-03T17:18:11	Renaming File	2023년 10월 회계부.png -> 2023년 10월 회계부.png.locked	2023년 10월 회계부.png.locked	¥Users¥User¥Downloads¥2023년 10월 회계부.png.locked	
374	181355630	2024-01-03T17:18:11	Renaming File	2023년 5월 회계부.png -> 2023년 5월 회계부.png.locked	2023년 5월 회계부.png.locked	¥Users¥User¥Downloads¥2023년 5월 회계부.png.locked	
375	181356802	2024-01-03T17:18:11	Renaming File	2023년 8월 회계부.png -> 2023년 8월 회계부.png.locked	2023년 8월 회계부.png.locked	¥Users¥User¥Downloads¥2023년 8월 회계부.png.locked	
376	181357970	2024-01-03T17:18:11	Renaming File	2023년 9월 회계부.png -> 2023년 9월 회계부.png.locked	2023년 9월 회계부.png.locked	¥Users¥User¥Downloads¥2023년 9월 회계부.png.locked	
377	181359144	2024-01-03T17:18:11	Renaming File	cors(키퍼발표).pptx -> cors(키퍼발표).pptx.locked	cors(키퍼발표).pptx.locked	¥Users¥User¥Downloads¥cors(키퍼발표).pptx.locked	
378	181360317	2024-01-03T17:18:11	Renaming File	KEEPER 기술문서 최종발표.pptx -> KEEPER 기술문서 최종발표.pptx.locked	KEEPER 기술문서 최종발표.pptx.locked	¥Users¥User¥Downloads¥KEEPER 기술문서 최종발표.pptx.locked	
379	181360927	2024-01-03T17:18:11	File Creation		Decrypt_yourfiles.txt	¥Users¥User¥Desktop¥Decrypt_yourfiles.txt	#######

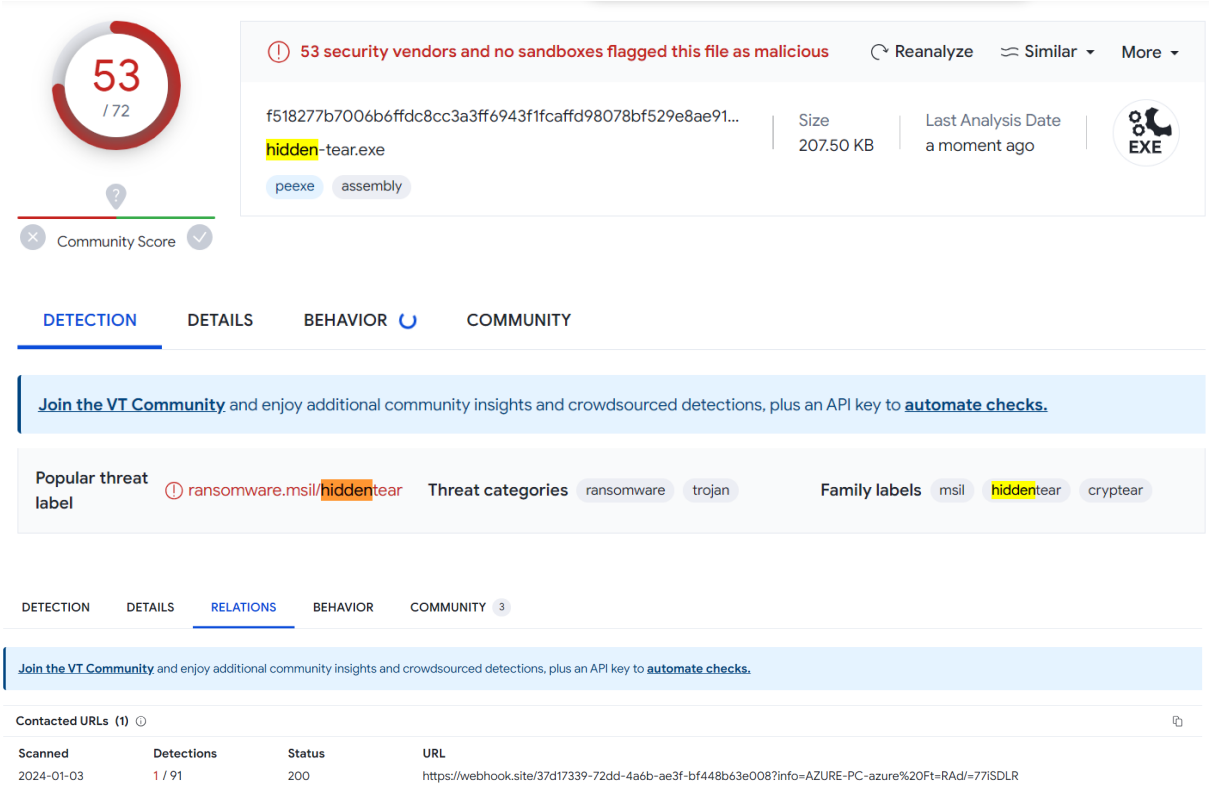
최초로 암호화된 파일은 `2023년 10월 회계부.png`

그 위에 Temp 폴더에 생성된 수상한 파일이 존재한다.

생성 시간(2024-01-03T17:18:07)과 암호화된 시간(2024-01-03T17:18:11)을 보면 매우 가깝다. 생성됨과 동시에 실행되었음을 추측할 수 있다.

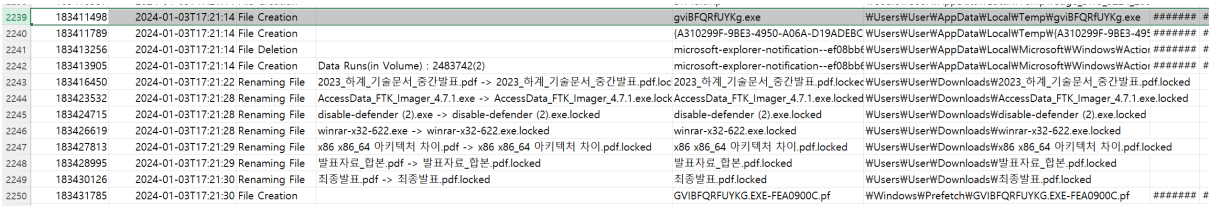
`0IAjDNgXOrFO.exe`인데 도구에 따라서 대문자로만 보여주는 경우도 있으므로 flag 통일을 위해 소문자로 인증 요구

더 나아가서 해당 파일을 추출하고 virustotal의 결과를 확인하면 HiddenTear Ransomware 임을 확인할 수 있다.



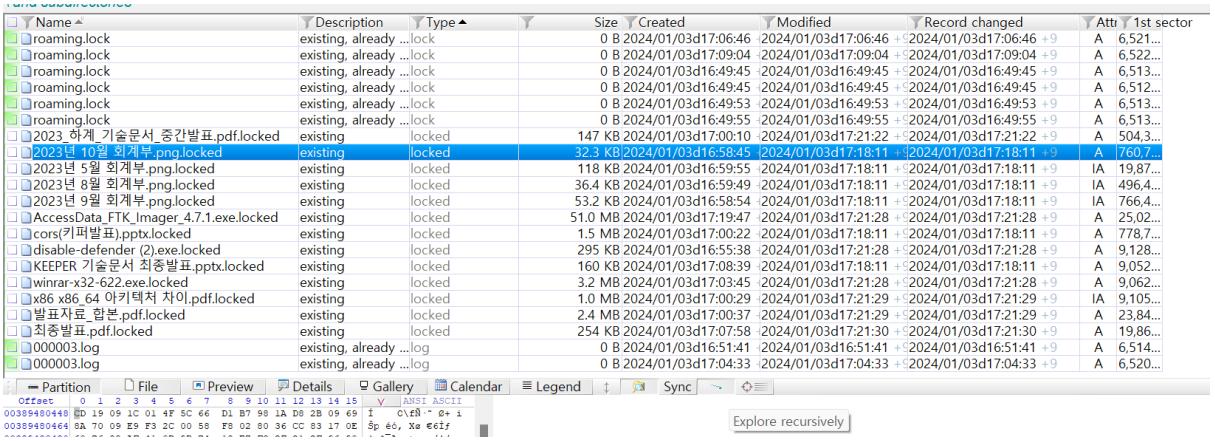
webbhook.site 사이트를 통해 사용자 정보 및 decrypt key가 전송됨을 유추할 수 있다.

`.locked` 로 암호화된 파일들을 더 찾아보면 풀이 과정 처음에 말했던 것처럼 2개의 랜섬웨어 파일이 사용되었음을 파일 시스템 로그를 통해 증명할 수 있다.



2239	183411498	2024-01-03T17:21:14	File Creation		gviBFQRfUYKg.exe	₩Users₩User₩AppData₩Local₩Temp₩gviBFQRfUYKg.exe
2240	183411789	2024-01-03T17:21:14	File Creation		{A310299F-9BE3-4950-A06A-D19ADEBC	₩Users₩User₩AppData₩Local₩Temp₩{A310299F-9BE3-495
2241	183413256	2024-01-03T17:21:14	File Deletion		microsoft-explorer-notification--ef08bb6	₩Users₩User₩AppData₩Local₩Microsoft₩Windows₩Actio
2242	183413905	2024-01-03T17:21:14	File Creation	Data Runs(in Volume) : 2483742(2)	microsoft-explorer-notification--ef08bb6	₩Users₩User₩AppData₩Local₩Microsoft₩Windows₩Actio
2243	183416450	2024-01-03T17:21:22	Renaming File	2023_하계_기술문서_중간발표.pdf -> 2023_하계_기술문서_중간발표.pdf.loc	2023_하계_기술문서_중간발표.pdf.locke	₩Users₩User₩Downloads₩2023_하계_기술문서_중간발표.pdf.locked
2244	183423532	2024-01-03T17:21:28	Renaming File	AccessData_FTK_Imager_4.7.1.exe -> AccessData_FTK_Imager_4.7.1.exe.lock	AccessData_FTK_Imager_4.7.1.exe.locked	₩Users₩User₩Downloads₩AccessData_FTK_Imager_4.7.1.exe.locked
2245	183424715	2024-01-03T17:21:28	Renaming File	disable-defender (2).exe -> disable-defender (2).exe.locked	disable-defender (2).exe.locked	₩Users₩User₩Downloads₩disable-defender (2).exe.locked
2246	183426619	2024-01-03T17:21:28	Renaming File	winrar-x32-622.exe -> winrar-x32-622.exe.locked	winrar-x32-622.exe.locked	₩Users₩User₩Downloads₩winrar-x32-622.exe.locked
2247	183427813	2024-01-03T17:21:29	Renaming File	x86 x86_64 아키텍처 차이.pdf -> x86 x86_64 아키텍처 차이.pdf.locked	x86 x86_64 아키텍처 차이.pdf.locked	₩Users₩User₩Downloads₩x86 x86_64 아키텍처 차이.pdf.locked
2248	183428995	2024-01-03T17:21:29	Renaming File	발표자료_합본.pdf -> 발표자료_합본.pdf.locked	발표자료_합본.pdf.locked	₩Users₩User₩Downloads₩발표자료_합본.pdf.locked
2249	183430126	2024-01-03T17:21:30	Renaming File	최종발표.pdf -> 최종발표.pdf.locked	최종발표.pdf.locked	₩Users₩User₩Downloads₩최종발표.pdf.locked
2250	183431785	2024-01-03T17:21:30	File Creation		GVIBFQRFUYKG.EXE-FEA0900C.pf	₩Windows₩Prefetch₩GVIBFQRFUYKG.EXE-FEA0900C.pf

해당 파일도 virustotal에 업로드한 결과 동일한 랜섬웨어임을 확인할 수 있었다.



x-ways에서 Explore recursively 기능을 사용하면 폴더 내부에 존재하는 파일들을 한 화면에 볼 수 있으며, Type으로 정렬 후 locked를 검색하면 위와 같은 결과가 나온다.

이전에 확인된 감염 파일들을 제외하면 추가로 감염된 파일은 없는 것으로 보인다.