IR-2

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

문제

피해자는 윈도우 PC를 사용할 때 잦은 알림이 번거롭다고 느껴, 디펜더를 비활성화하는 프로그램을 항상 사용한다고 한다.

또한 피해자에게 들은 바로는 랜섬웨어가 감염되기 전에 컴퓨터가 이상한 행위를 했었다고 한다.

원인을 찾아내고, 어떤 경로로 유입되었는지 분석하라.

다운로드 유입 URL, 다운로드 받은 악성 파일, 다운로드 받은 악성 파일이 실행된 시간을 답으로 입력해야 한다.

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

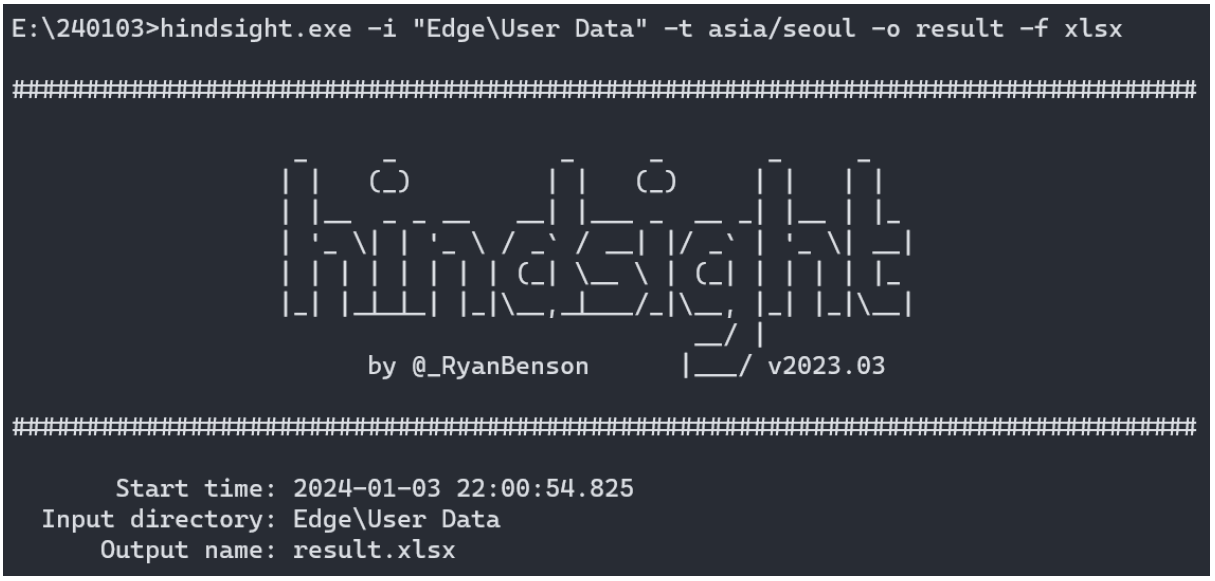
ex: KEEPER{https://www.example.com/_asdf.asd_2024-12-23T12:34:56}

답

KEEPER{https://keeper.or.kr/board/view/172731_11월_회계부.rar_2024-01-03T17:04:29}

풀이 과정

브라우저 분석 (Edge)



hindsight 도구 사용하여 브라우저 기록 분석 시작

크롬, 파이어폭스 등 다른 브라우저는 설치 흔적이 없었으므로 Edge 브라우저 분석 시작

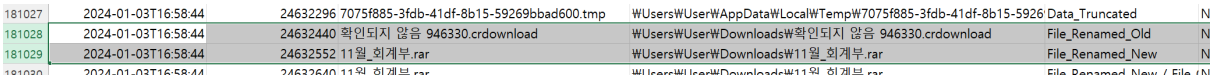
Hindsight Internet History Forensics (v2023.03)

Type	Timestamp (Asia/Seoul)	URL	Title / Name / Status	Data / Value / Path
url	2024-01-03 16:58:07.004	https://keeper.or.kr/	KEEPER	
url	2024-01-03 16:58:16.057	https://keeper.or.kr/board/%EA%B8%B0%EC%88%A0%EB%AC%B8%EC%8	KEEPER	
url	2024-01-03 16:58:16.620	https://keeper.or.kr/board/%EA%B8%B0%EC%88%A0%EB%AC%B8%EC%8	KEEPER	
url	2024-01-03 16:58:17.932	https://keeper.or.kr/board/%ED%9A%8C%EA%B3%84%EB%B6%80	KEEPER	
url	2024-01-03 16:58:19.299	https://www.google.com/	Google	
url	2024-01-03 16:58:19.468	https://keeper.or.kr/board/view/172731	KEEPER	
download	2024-01-03 16:58:22.209	blob:https://keeper.or.kr/33feaa89-fa2a-4c65-abe2-3e7b07e73350	Complete - 100% [1243505/1	C:₩Users₩User₩Downloads₩11월_회계부.rar
url	2024-01-03 16:58:27.589	https://github.com/qtkite/defender-control	GitHub - qtkite/defender-control: An open-source windows defender manager. Now	
url	2024-01-03 16:58:34.809	https://keeper.or.kr/board/%EA%B8%B0%EC%88%A0%EB%AC%B8%EC%8	KEEPER	
url	2024-01-03 16:58:35.188	https://keeper.or.kr/board/%EA%B8%B0%EC%88%A0%EB%AC%B8%EC%8	KEEPER	
url	2024-01-03 16:58:35.235	https://keeper.or.kr/board/%EA%B8%B0%EC%88%A0%EB%AC%B8%EC%8	KEEPER	
login (never save)	2024-01-03 16:58:36.693	https://keeper.or.kr/		
url	2024-01-03 16:58:41.550	https://github.com/qtkite/defender-control	GitHub - qtkite/defender-control: An open-source windows defender manager. Now	
url	2024-01-03 16:58:41.713	https://github.com/qtkite/defender-control	GitHub - qtkite/defender-control: An open-source windows defender manager. Now	
url	2024-01-03 16:58:42.172	https://keeper.or.kr/board/%ED%9A%8C%EA%B3%84%EB%B6%80	KEEPER	
site setting (hsts)	2024-01-03 16:58:42.436	Encoded domain: by3HYgXFJoQvTPlDd2zzpjW2gj+L2+egy4ezZdihpTo=	HSTS observed	{'expiry': 1735804722.436291, 'host': 'by3HYgXFJoQvTPl
url	2024-01-03 16:58:42.932	https://keeper.or.kr/board/view/172699	KEEPER	
download	2024-01-03 16:58:45.668	blob:https://keeper.or.kr/d1748001-a21b-4fc8-a31f-3c27e8b6815e	Complete - 100% [33042/330	C:₩Users₩User₩Downloads₩2023년 10월 회계부.png
url	2024-01-03 16:58:51.332	https://keeper.or.kr/board/%ED%9A%8C%EA%B3%84%EB%B6%80	KEEPER	
url	2024-01-03 16:58:51.494	https://keeper.or.kr/board/%ED%9A%8C%EA%B3%84%EB%B6%80?page=	KEEPER	
url	2024-01-03 16:58:51.531	https://keeper.or.kr/board/%ED%9A%8C%EA%B3%84%EB%B6%80?page=	KEEPER	
url	2024-01-03 16:58:52.630	https://keeper.or.kr/board/view/172659	KEEPER	
download	2024-01-03 16:58:54.577	blob:https://keeper.or.kr/e5395e36-5d78-471d-bdf7-4d15478fbe78	Complete - 100% [54504/545	C:₩Users₩User₩Downloads₩2023년 9월 회계부.png

아래 로그를 보면 일반적인 회계부의 경우 png 이미지 파일인데, 11월 회계부는 rar 파일을 다운로드 받음

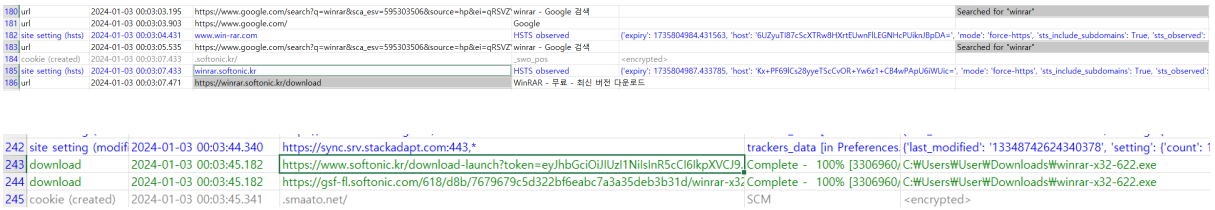
해당 게시글인 `https://keeper.or.kr/board/view/172731`에 현재는 `11월_회계부.rar` 파일이 존재하지 않음 (사이트 관리자가 롤백했을 수도, 작성자가 다시 수정했을 수도 이후 작업은 E01(이미지) 파일만으로는 확인할 수 없다.)

`11월_회계부.rar` 파일 다운로드 버튼 클릭 시간은 2024-01-03T16:58:22



181027	2024-01-03T16:58:44	24632296 7075f885-3fdb-41df-8b15-59269bbad600.tmp	₩Users₩User₩AppData₩Local₩Temp₩7075f885-3fdb-41df-8b15-5926	Data_Truncated	N
181028	2024-01-03T16:58:44	24632440 확인되지 않음 946330.crdownload	₩Users₩User₩Downloads₩확인되지 않음 946330.crdownload	File_Renamed_Old	N
181029	2024-01-03T16:58:44	24632552 11월_회계부.rar	₩Users₩User₩Downloads₩11월_회계부.rar	File_Renamed_New	N

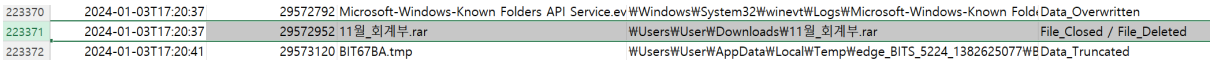
UsnJrnl 에서도 다운로드 기록을 확인할 수 있다. crdownload는 다운로드 중일 때 생성되는 파일인데 2024-01-03T16:58:44에 다운로드가 완료된 것으로 보인다.



180	url	2024-01-03 00:03:03.195	https://www.google.com/search?q=winrar&sca_esv=595303506&source=hp&ei=qRSVZ	winrar - Google 검색			Searched for "winrar"
181	url	2024-01-03 00:03:03.903	https://www.google.com/	Google			
182	site setting (hsts)	2024-01-03 00:03:04.431	www.win-rar.com	HSTS observed	{'expiry': 1735804984.431563, 'host': '6UZyuTI87cScXTRw8HXrtEUwnFILEGNHcPUiknJBpDA=', 'mode': 'force-https', 'sts_include_subdomains': True, 'sts_observed':		
183	url	2024-01-03 00:03:05.535	https://www.google.com/search?q=winrar&sca_esv=595303506&source=hp&ei=qRSVZ	winrar - Google 검색			Searched for "winrar"
184	cookie (created)	2024-01-03 00:03:07.433	.softonic.kr/	_swo_pos	<encrypted>		
185	site setting (hsts)	2024-01-03 00:03:07.433	winrar.softonic.kr	HSTS observed	{'expiry': 1735804987.433785, 'host': 'Kx+PF69ICs28yyeTScCvOR+Yw6z1+CB4wPApU6iWUic=', 'mode': 'force-https', 'sts_include_subdomains': True, 'sts_observed':		
186	url	2024-01-03 00:03:07.471	https://winrar.softonic.kr/download	WinRAR - 무료 - 최신 버전 다운로드			

242	site setting (modif	2024-01-03 00:03:44.340	https://sync.srv.stackadapt.com:443,*	trackers_data [in Preferences	{'last_modified': '13348742624340378', 'setting': {'count': 1	
243	download	2024-01-03 00:03:45.182	https://www.softonic.kr/download-launch?token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9	Complete -	100% [3306960/	C:₩Users₩User₩Downloads₩winrar-x32-622.exe
244	download	2024-01-03 00:03:45.182	https://gsf-fl.softonic.com/618/d8b/7679679c5d322bf6eabc7a3a35deb3b31d/winrar-x3	Complete -	100% [3306960/	C:₩Users₩User₩Downloads₩winrar-x32-622.exe
245	cookie (created)	2024-01-03 00:03:45.341	.smaato.net/	SCM	<encrypted>	

rar 파일을 열기 위해 winrar 검색 후 상단에 뜨는 softsonic 사이트에서 6.22 버전을 다운로드

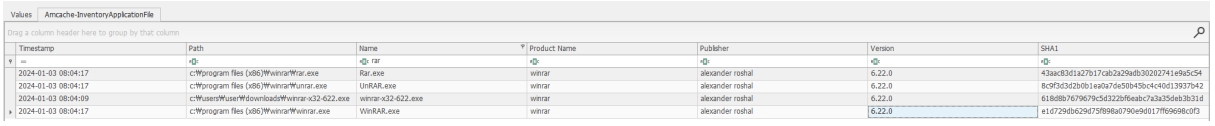


223370	2024-01-03T17:20:37	29572792 Microsoft-Windows-Known Folders API Service.ev	₩Windows₩System32₩winevt₩Logs₩Microsoft-Windows-Known Fold	Data_Overwritten
223371	2024-01-03T17:20:37	29572952 11월_회계부.rar	₩Users₩User₩Downloads₩11월_회계부.rar	File_Closed / File_Deleted
223372	2024-01-03T17:20:41	29573120 BIT67BA.tmp	₩Users₩User₩AppData₩Local₩Temp₩edge_BITS_5224_1382625077₩E	Data_Truncated

다운로드 받은 `11월_회계부.rar` 파일의 경로에 가면 존재하지 않는데, 이후에 계속 활용하는 파일 시스템 로그를 통해 2024-01-03T17:20:37에 삭제된 것을 확인할 수 있다.

레지스트리 및 파일 시스템 분석

일단 다운로드 받은 winrar가 설치되었는지 Amcache.hve를 통해 어느정도 확인 가능

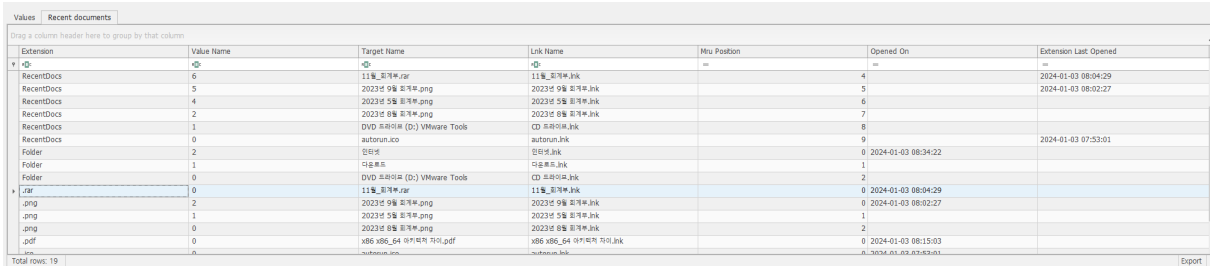


Values | Amcache-InventoryApplicationFile

Drag a column header here to group by that column

Timestamp	Path	Name	Product Name	Publisher	Version	SHA1
2024-01-03 08:04:17	c:₩program files (x86)₩winrar₩rar.exe	Rar.exe	winrar	alexander roshal	6.22.0	43aac83d1a27b17cab2a29adb30202741e9a5c54
2024-01-03 08:04:17	c:₩program files (x86)₩winrar₩unrar.exe	UnRAR.exe	winrar	alexander roshal	6.22.0	8c9f3d3d2b0b1ea0a7de50b45bc4c40d139370b42
2024-01-03 08:04:09	c:₩users₩user₩downloads₩winrar-x32-622.exe	winrar-x32-622.exe	winrar	alexander roshal	6.22.0	618d8b7679679c5d322bf6eabc7a3a35deb3b31d
2024-01-03 08:04:17	c:₩program files (x86)₩winrar₩winrar.exe	WinRAR.exe	winrar	alexander roshal	6.22.0	e1d729db629d75f998a0790e9d01 7ff69698c0f3

`C:\program files (x86)\winrar` 경로에 6.22 버전이 설치되었음을 확인



Values | Recent documents

Drag a column header here to group by that column

Extension	Value Name	Target Name	Lnk Name	Mru Position	Opened On	Extension Last Opened
RecentDocs	6	11월_회계부.rar	11월_회계부.lnk	4		2024-01-03 08:04:29
RecentDocs	5	2023년 9월 회계부.png	2023년 9월 회계부.lnk	5		2024-01-03 08:02:27
RecentDocs	4	2023년 5월 회계부.png	2023년 5월 회계부.lnk	6		
RecentDocs	2	2023년 8월 회계부.png	2023년 8월 회계부.lnk	7		
RecentDocs	1	DVD 드라이브 (D:) VMware Tools	CD 드라이브.lnk	8		
RecentDocs	0	autorun.ico	autorun.lnk	9		2024-01-03 07:53:01
Folder	2	인터넷	인터넷.lnk	0	2024-01-03 08:34:22	
Folder	1	다운로드	다운로드.lnk	1		
Folder	0	DVD 드라이브 (D:) VMware Tools	CD 드라이브.lnk	2		
.rar	0	11월_회계부.rar	11월_회계부.lnk	0	2024-01-03 08:04:29	
.png	2	2023년 9월 회계부.png	2023년 9월 회계부.lnk	0	2024-01-03 08:02:27	
.png	1	2023년 5월 회계부.png	2023년 5월 회계부.lnk	1		
.png	0	2023년 8월 회계부.png	2023년 8월 회계부.lnk	2		
.pdf	0	x86 x86_64 아키텍처 차이.pdf	x86 x86_64 아키텍처 차이.lnk	0	2024-01-03 08:15:03	

Total rows: 19 | Export

RecentDocs 확인 결과 `2024-01-03 08:04:29` → 9시간 더한 시간인 `2024-01-03 17:04:29` 실행 (바이너리에는 UTC+0으로 저장되어 있기 때문에 도구에서 UTC를 설정하는 기능이 별도로 존재하지 않는 한 UTC+0이라 생각하고 타임스탬프를 계산해야 한다.)

해당 시간을 기점으로 MFT, UsnjrnI 분석 시작

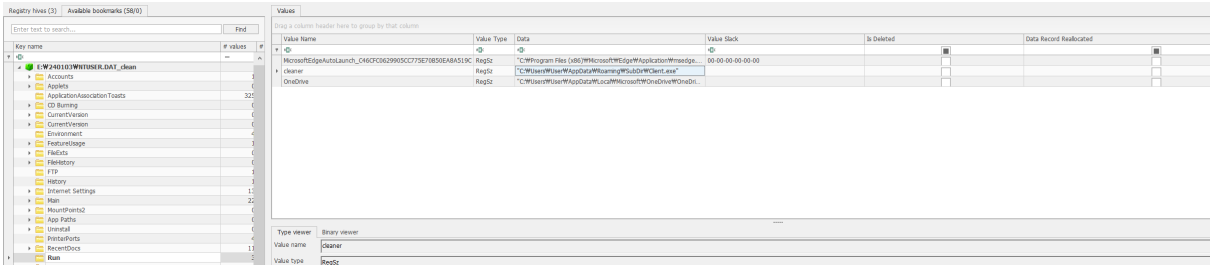
186443	2024-01-03T17:04:29	25219360	11월_회계부.rar	₩Users₩User₩Downloads₩11월_회계부.rar	Object_ID_Chang
186444	2024-01-03T17:04:29	25219448	11월_회계부.rar	₩Users₩User₩Downloads₩11월_회계부.rar	Object_ID_Chang
186445	2024-01-03T17:04:29	25219536	290532160612e071.automaticDestinations-ms	₩Users₩User₩AppData₩Roaming₩Microsoft₩Windows₩Recent₩Automat	File_Created / D
186446	2024-01-03T17:04:29	25219680	f01b4d95cf55d32a.automaticDestinations-ms	₩Users₩User₩AppData₩Roaming₩Microsoft₩Windows₩Recent₩Automat	Data_Overwritte
186447	2024-01-03T17:04:29	25219824	f01b4d95cf55d32a.automaticDestinations-ms	₩Users₩User₩AppData₩Roaming₩Microsoft₩Windows₩Recent₩Automat	Data_Overwritte
186448	2024-01-03T17:04:29	25219968	11월_회계부.lnk	₩Users₩User₩AppData₩Roaming₩Microsoft₩Windows₩Recent₩11월_회	File_Created
186449	2024-01-03T17:04:29	25220056	11월_회계부.lnk	₩Users₩User₩AppData₩Roaming₩Microsoft₩Windows₩Recent₩11월_회	File_Created / D
186450	2024-01-03T17:04:29	25220144	11월_회계부.lnk	₩Users₩User₩AppData₩Roaming₩Microsoft₩Windows₩Recent₩11월_회	File_Created / D

확인한 결과 레지스트리 데이터처럼 11월_회계부.lnk 파일이 생성되었고 시간도 맞았음.

lnk 파일이 생성되었다는 것 자체가 해당 파일을 실행하여 생성된 것이기 때문에 rar 파일을 실행한 시간이라고 봐도 무방함 (rar 파일을 받았다고 lnk 파일이 생성되진 않음, 또한 RecentDocs의 Extension Last Opened 시간과 같음을 확인할 수 있음)

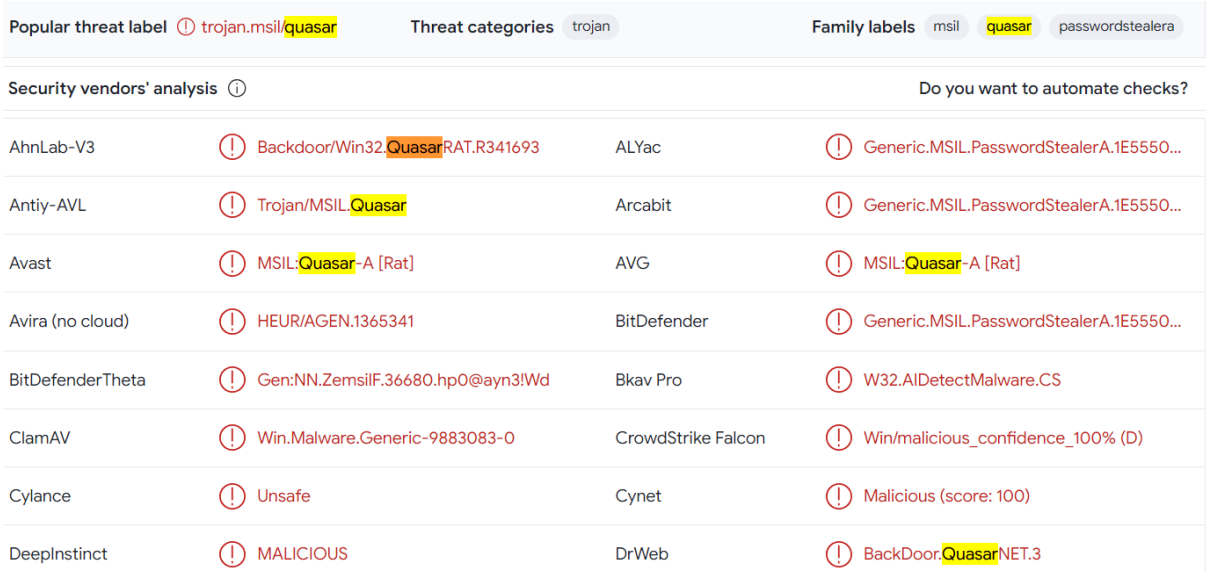
187256	2024-01-03T17:04:34	25296336	₩Users₩User₩AppData₩Local₩Microsoft₩Windows₩WebCache₩V01.chk	Data_Overwritten
187257	2024-01-03T17:04:35	25296416	Rar$DIa5732.5826	₩Users₩User₩AppData₩Local₩Temp₩Rar$DIa5732.5826	File_Created
187258	2024-01-03T17:04:35	25296512	Rar$DIa5732.5826	₩Users₩User₩AppData₩Local₩Temp₩Rar$DIa5732.5826	File_Created / File
187259	2024-01-03T17:04:35	25296608	11.pdf	₩Users₩User₩AppData₩Local₩Temp₩Rar$DIa5732.5826₩11.pdf	File_Created
187260	2024-01-03T17:04:35	25296680	11.pdf	₩Users₩User₩AppData₩Local₩Temp₩Rar$DIa5732.5826₩11.pdf	File_Created / Da
187261	2024-01-03T17:04:35	25296752	11.pdf	₩Users₩User₩AppData₩Local₩Temp₩Rar$DIa5732.5826₩11.pdf	File_Created / Bas
187262	2024-01-03T17:04:35	25296824	11.pdf	₩Users₩User₩AppData₩Local₩Temp₩Rar$DIa5732.5826₩11.pdf	File_Created / Bas
187263	2024-01-03T17:04:35	25296896	11.pdf	₩Users₩User₩AppData₩Local₩Temp₩Rar$DIa5732.5826₩11.pdf	Basic_Info_Chang
187264	2024-01-03T17:04:35	25296968	11.pdf	₩Users₩User₩AppData₩Local₩Temp₩Rar$DIa5732.5826₩11.pdf	Basic_Info_Chang
187265	2024-01-03T17:04:35	25297040	11.pdf .cmd	₩Users₩User₩AppData₩Local₩Temp₩Rar$DIa5732.5826₩11.pdf .cmd	File_Created
187266	2024-01-03T17:04:35	25297128	11.pdf .cmd	₩Users₩User₩AppData₩Local₩Temp₩Rar$DIa5732.5826₩11.pdf .cmd	File_Created / Da
187267	2024-01-03T17:04:35	25297216	11.pdf .cmd	₩Users₩User₩AppData₩Local₩Temp₩Rar$DIa5732.5826₩11.pdf .cmd	File_Created / Bas
187268	2024-01-03T17:04:35	25297304	11.pdf .cmd	₩Users₩User₩AppData₩Local₩Temp₩Rar$DIa5732.5826₩11.pdf .cmd	File_Created / Bas
187269	2024-01-03T17:04:35	25297392	test.exe	₩Users₩User₩AppData₩Local₩Temp₩Rar$DIa5732.5826₩test.exe	File_Created
187270	2024-01-03T17:04:35	25297472	test.exe	₩Users₩User₩AppData₩Local₩Temp₩Rar$DIa5732.5826₩test.exe	File_Created / Da
187271	2024-01-03T17:04:35	25297552	test.exe	₩Users₩User₩AppData₩Local₩Temp₩Rar$DIa5732.5826₩test.exe	File_Created / Da

내리다보면 Temp 폴더에 rar 파일을 실행함에 따라 생성된 것으로 보이는데(Temp 폴더 경로를 보면 짐작할 수 있다. - `Temp\Rar$~~~`) cmd 파일, `test.exe` 등 수상한 파일들이 Temp 폴더에 생성됨



윈도우 부팅 시 자동 실행되는 레지스트리 경로인 Run에 수상한 파일 존재
`C:\Users\User\AppData\Roaming\SubDir\Client.exe`

다행히 해당 파일은 존재함, 컴퓨터가 꺼지더라도 계속 유지할 수 있게 등록되어 있어서 파일이 존재했음



Popular threat label	trojan.msil/quasar	Threat categories	trojan	Family labels	msil	quasar	passwordstealera

Security vendors' analysis — Do you want to automate checks?

AhnLab-V3	Backdoor/Win32.QuasarRAT.R341693	ALYac	Generic.MSIL.PasswordStealerA.1E5550...
Antiy-AVL	Trojan/MSIL.Quasar	Arcabit	Generic.MSIL.PasswordStealerA.1E5550...
Avast	MSIL:Quasar-A [Rat]	AVG	MSIL:Quasar-A [Rat]
Avira (no cloud)	HEUR/AGEN.1365341	BitDefender	Generic.MSIL.PasswordStealerA.1E5550...
BitDefenderTheta	Gen:NN.ZemsilF.36680.hp0@ayn3!Wd	Bkav Pro	W32.AIDetectMalware.CS
ClamAV	Win.Malware.Generic-9883083-0	CrowdStrike Falcon	Win/malicious_confidence_100% (D)
Cylance	Unsafe	Cynet	Malicious (score: 100)
DeepInstinct	MALICIOUS	DrWeb	BackDoor.QuasarNET.3

virustotal 결과 Quasar RAT 파일이며, 피해자가 말한 이상한 행위는 좀비PC에 감염되어 이상한 행위를 했을 수 있음.

랜섬웨어 감염 역시 RAT Builder 배포자가 실행시켰을 가능성도 존재

`test.exe`는 무엇인지, `Client.exe`는 무엇인지 확인이 필요함 → 역시 MFT, UsnJrnl에서 확인

187267	2024-01-03T17:04:35	25297216	11.pdf .cmd	₩Users₩User₩AppData₩Local₩Temp₩Rar$DIa5732.5826₩11.pdf .cmd	File_Created / E
187268	2024-01-03T17:04:35	25297304	11.pdf .cmd	₩Users₩User₩AppData₩Local₩Temp₩Rar$DIa5732.5826₩11.pdf .cmd	File_Created / E
187269	2024-01-03T17:04:35	25297392	test.exe	₩Users₩User₩AppData₩Local₩Temp₩Rar$DIa5732.5826₩test.exe	File_Created
187270	2024-01-03T17:04:35	25297472	test.exe	₩Users₩User₩AppData₩Local₩Temp₩Rar$DIa5732.5826₩test.exe	File_Created / D
187271	2024-01-03T17:04:35	25297552	test.exe	₩Users₩User₩AppData₩Local₩Temp₩Rar$DIa5732.5826₩test.exe	File_Created / D
187272	2024-01-03T17:04:35	25297632	test.exe	₩Users₩User₩AppData₩Local₩Temp₩Rar$DIa5732.5826₩test.exe	File_Created / E
187273	2024-01-03T17:04:35	25297712	test.exe	₩Users₩User₩AppData₩Local₩Temp₩Rar$DIa5732.5826₩test.exe	File_Created / E
187274	2024-01-03T17:04:36	25297792	CloudStore	₩Users₩User₩AppData₩Roaming₩Microsoft₩Windows₩CloudStore	Access_Right_C
187275	2024-01-03T17:04:36	25297872	CloudStore	₩Users₩User₩AppData₩Roaming₩Microsoft₩Windows₩CloudStore	Access_Right_C
187323	2024-01-03T17:04:40	25304408	Network Persistent State	₩Users₩User₩AppData₩Local₩Microsoft₩Edge₩User Data₩Default₩Net	Basic_Info_Char
187324	2024-01-03T17:04:40	25304520	Network Persistent State~RF1b3a46.TMP	₩Users₩User₩AppData₩Local₩Microsoft₩Edge₩User Data₩Default₩Net	File_Renamed_N
187325	2024-01-03T17:04:40	25304656	Network Persistent State	₩Users₩User₩AppData₩Local₩Microsoft₩Edge₩User Data₩Default₩Net	Basic_Info_Char
187326	2024-01-03T17:04:40	25304768	Network Persistent State~RF1b3a46.TMP	₩Users₩User₩AppData₩Local₩Microsoft₩Edge₩User Data₩Default₩Net	File_Closed / Fi
187327	2024-01-03T17:04:40	25304904	SubDir	₩Users₩User₩AppData₩Roaming₩SubDir	File_Created
187328	2024-01-03T17:04:40	25304976	SubDir	₩Users₩User₩AppData₩Roaming₩SubDir	File_Created / F
187329	2024-01-03T17:04:40	25305088	Client.exe	₩Users₩User₩AppData₩Roaming₩SubDir₩Client.exe	File_Created
187330	2024-01-03T17:04:40	25305168	Client.exe	₩Users₩User₩AppData₩Roaming₩SubDir₩Client.exe	File_Created / D
187331	2024-01-03T17:04:40	25305248	Client.exe	₩Users₩User₩AppData₩Roaming₩SubDir₩Client.exe	File_Created / D
187332	2024-01-03T17:04:40	25305328	Client.exe	₩Users₩User₩AppData₩Roaming₩SubDir₩Client.exe	File_Created / E
187333	2024-01-03T17:04:40	25305408	Client.exe	₩Users₩User₩AppData₩Roaming₩SubDir₩Client.exe	File_Created / E

2024-01-03T17:04:35 → 2024-01-03T17:04:40 (`test.exe`, `Client.exe`)

두 파일의 생성 시간이 매우 유사한 것과, `test.exe` 파일이 Temp 경로에 있었다는 것을 기반으로 `test.exe` 파일이 실행되면서 `C:\Users\User\AppData\Roaming\SubDir` 경로에 `Client.exe`라는 파일이 생성된 것으로 추측할 수 있다.

결론

지금까지 추출한 타임스탬프를 나열하면 다음과 같다.

2024-01-03T16:58:19 - `https://keeper.or.kr/board/view/172731` 접속

2024-01-03T16:58:22 - `11월_회계부.rar` 파일 다운로드 클릭

2024-01-03T16:58:44 - `11월_회계부.rar` 파일 다운로드 완료

2024-01-03T17:04:29 - `11월_회계부.rar` 파일 실행

2024-01-03T17:04:35 - rar 압축파일 내부에 존재하는 `11.pdf` 실행과 동시에 `11.pdf .cmd`, `test.exe` 파일 생성 (실행되었을 가능성 높음)

2024-01-03T17:04:40 - `Client.exe` 생성 (test.exe 파일에 의해 생성되었다고 추측 가능)

2024-01-03T17:20:37 - `11월_회계부.rar` 파일 삭제 (피해자에게 물어봐서 삭제하지 않았다고 한다면, RAT Builder 배포자가 삭제했거나 지금까지 발견된 악성코드에 의해 삭제되었거나 둘 중 하나임 → 이 부분은 상세한 악성코드 분석 필요)

IR-1 타임라인까지 합치면

2024-01-03T17:18:07 - `0IAjDNgXOrFO.exe` 파일 생성

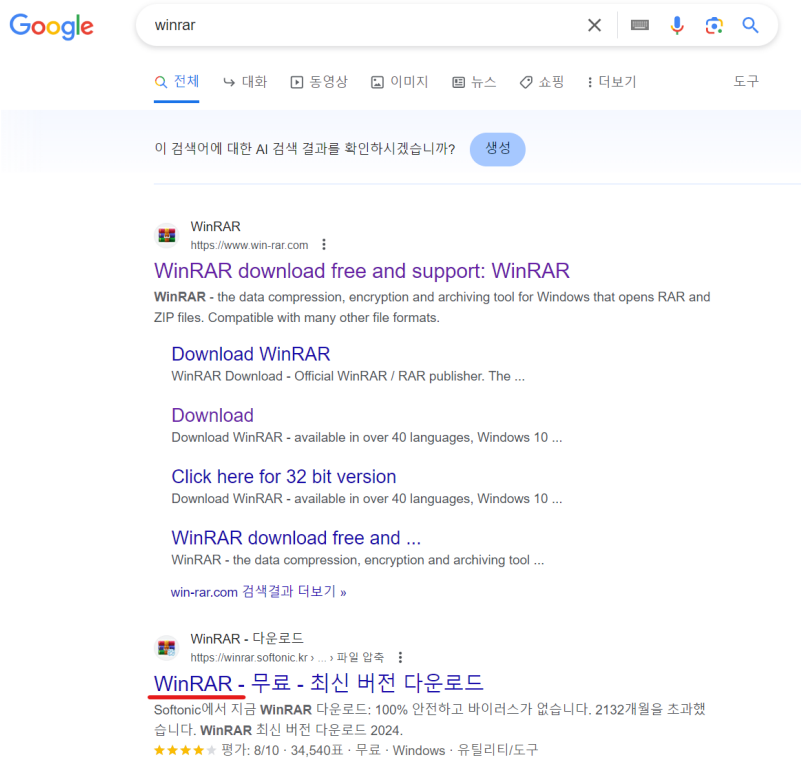
2024-01-03T17:18:11 이후 - `2023년 10월 회계부.png` 등 암호화

2024-01-03T17:21:14 - `gviBFQRfUYKg.exe` 파일 생성

2024-01-03T17:21:22 이후 - `2023_하계_기술문서_중간발표.pdf` 등 암호화

난독화되지 않은 파일이 있는 것을 확인하고 핵심 유입 파일인 rar 파일을 삭제하고 재감염시켰다고 추측할 수도 있음

실제 감염 경로



keeper 홈페이지에 올라온 rar 파일을 열어보기 위해 softsonic 사이트에서 winrar 설치 (위 링크를 통해 다운로드 받은 버전은 cve-2023-38831 취약점이 존재한다.)

rar 파일 내부에 `11.pdf` 파일을 열면서 QuasarRAT 파일이 실행됨 (실제로 `test.exe` 파일이 실행되면서 `client.exe` 파일로 복사되며, 지속성을 유지하기 위해 윈도우가 실행될 때마다 계속 실행되게 레지스트리 등록된다. `test.exe`와 `client.exe`는 같은 파일이다.)

RAT Builder 배포자가 RAT를 통해 2번에 걸쳐 랜섬웨어 배포 (감염되지 않은 확장자가 있어서 코드에 확장자 추가 및 재컴파일 후 배포)

cve-2023-38831 취약점 분석 글: HDCE-inc group-ib

QuasarRAT - The Best Windows RAT? - Remote Administration Tool for Windows