악성코드 분석 보고서

-tber.exe-

2022-11-26

배준호

목차

1.개요

1-1. 개요

여러 분석 툴을 사용하여 악성코드로 추정되는 tber.exe 파일을 분석하고 분석한 결과를 바탕으로 어떠한 악성 코드인지 추측하고 예방법 및 대응 방안을 작성한다.

1-2. 파일정보

구분	내용
파일명	tber.exe
파일크기	3.60 MB (3777536 bytes)
파일종류	Win32 EXE
생성시기	2018-01-23 17:47:58 UTC
MD5	50d539a6390a4ebe0927f140dc1c06f2
SHA-1	d32b2802bfad11ffeec8579e385b2e7efffdcbc6
SHA-256	364040375650bf968b7503de130ecf17b8194f47825847e98149446acd741e50
진단명	PUP/Win32.InstMonster.R218831 (AhnLab-V3)
	Win32: Adware-gen [Adw] (AVG)
출처	Virusshare

[표1-1] 악성코드 정보

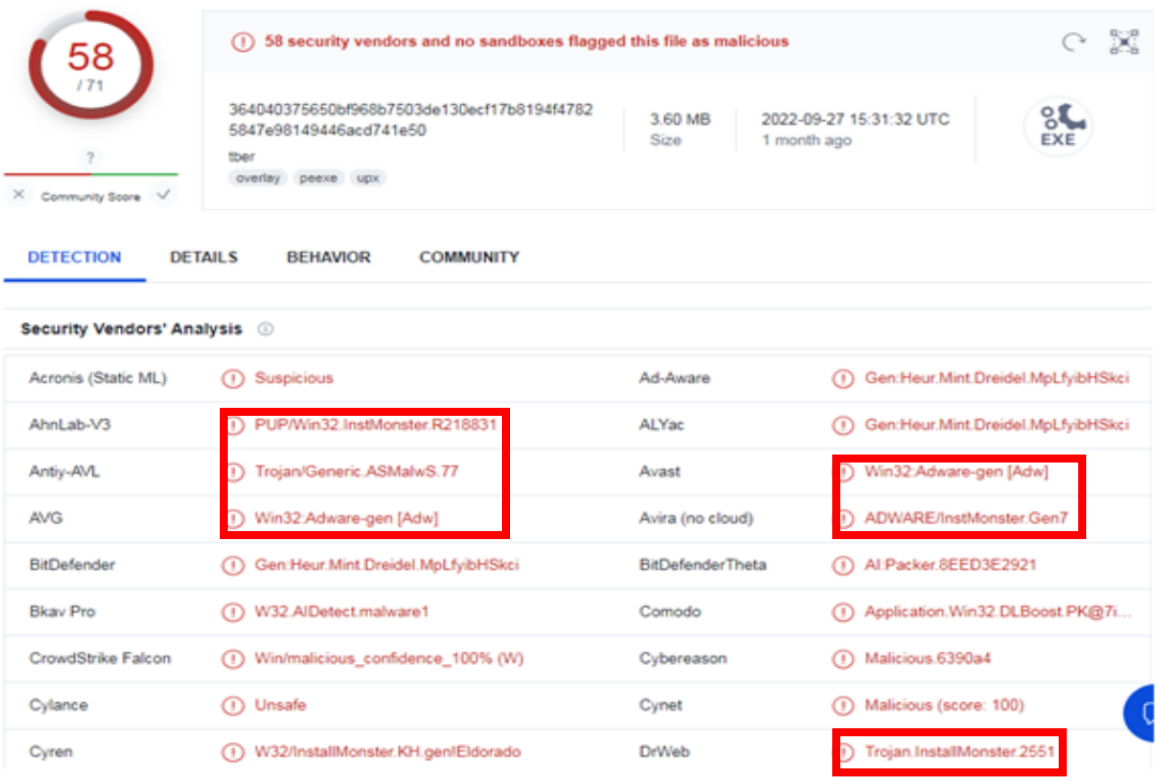
1-3. 분석환경

구분	내용	
Os	Windows7	
가상환경	Vmware Workstation 15.5.7	
기초분석	VirusaTotal	악성코드 진단 및 파일 정보
정적분석 도구	Exeinfo PE,	패킹 여부 확인
	Upx303w	패킹 된 파일 언패킹
	BinText,	문자열 확인
	Peview	pe구조 분석
동적분석 도구	Process Explorer	프로세스 변화 확인
	Process monitor, Autoruns	레지스트리 변화 확인
	Currport, WireShark	네트워크 변화 확인

[표1-2] OS와 악성코드 분석에 사용한 분석 툴

2.기초분석

2-1. VirusTotal (파일 감염여부 진단)

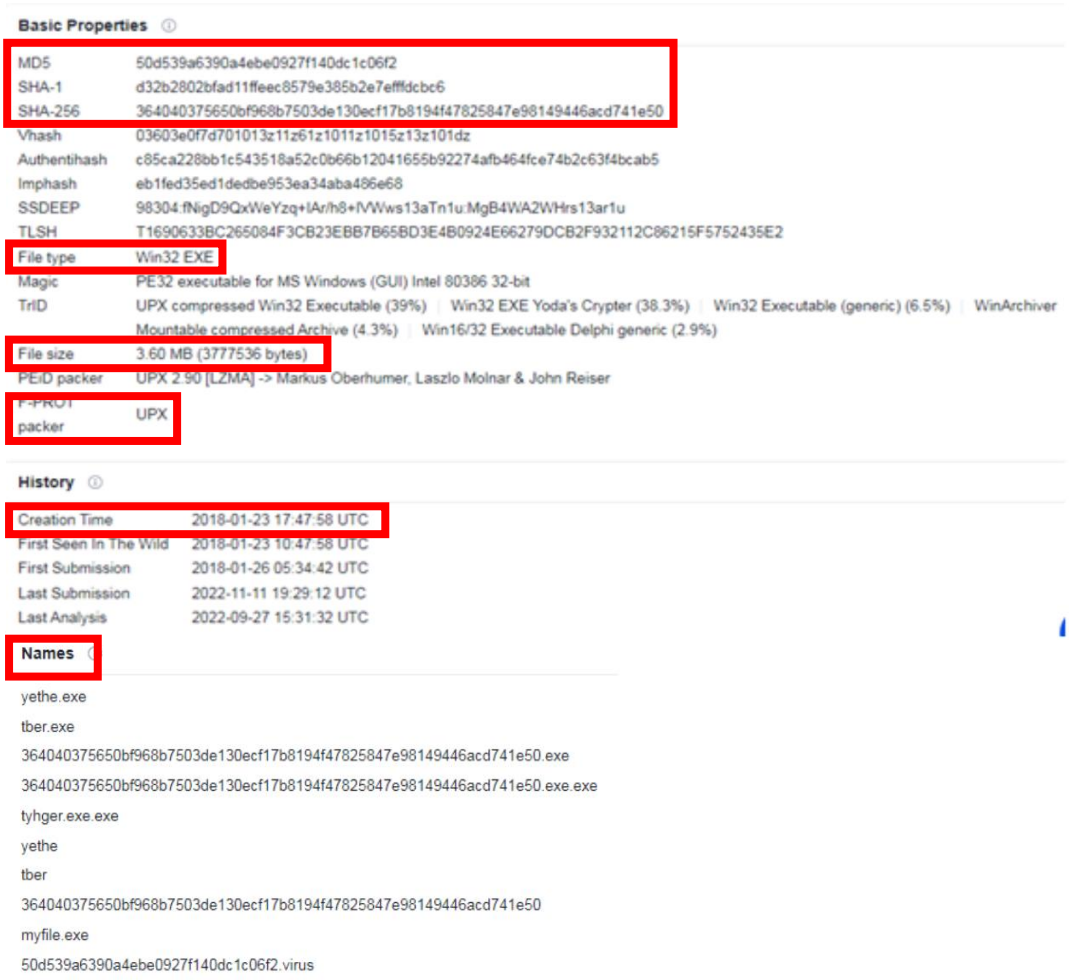


[그림 2-1] VirusTotal을 이용한 파일 분석(1)

2022년 9월 27일 갱신 결과 71개 백신엔진 중 58개가 악성코드 의심파일임을 알 수 있다. 주된 악성코드 진단명은 Trojan[1], Adware[2]이었다. 또한 AhnLab-V3에서 나온 진단명 PUP/Win32.InstMonster.R218831은 광고성 웹페이지를 로딩 함으로써 공격자가 수익을 얻는 악성 프로그램이다. 따라서 해당 파일은 트로이목마와 에드웨어의 성격을 가지는 악성파일이라고 추측이 가능하다.

[1]Trojan: 유용한 프로그램으로 가장하여 사용자가 그 프로그램을 실행하도록 속이는 악성 코드로 트로이 목마라고 부른다.

[2]Adware: 특정 소프트웨어를 실행할 때 또는 설치 후 자동적으로 광고가 표시되는 프로그램



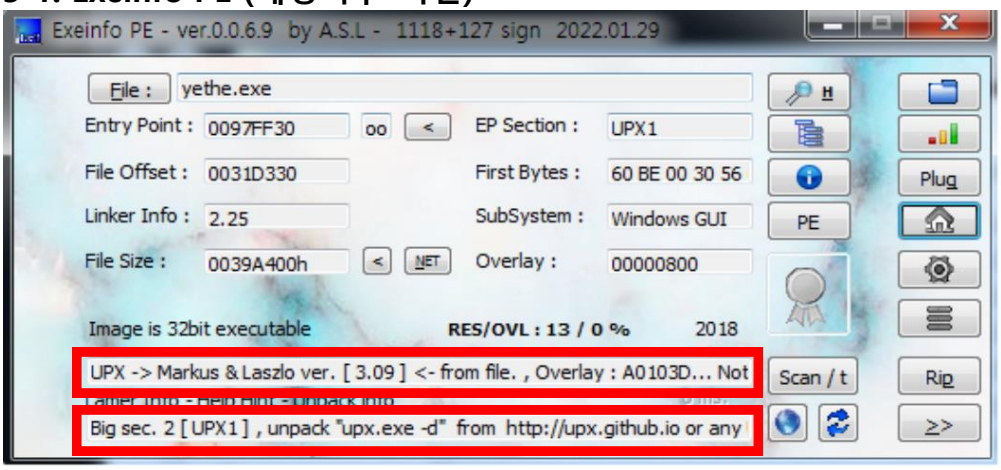
[그림 2-2] VirusTotal을 이용한 파일 분석(2)

분석을 통해 Hash값, 파일 타입 및 크기, 패킹[3] 기법, 생성시간, 파일 이름 등을 확인할 수 있다.
해당 파일의 유형은 Win32 EXE이며 UPX 패킹 기법으로 패킹 되었고 2018년 1월 23일에 생성되었음을 알 수 있다. 또한 VirusTotal에 여러 이름으로 보고된 것을 알 수 있다.

[3]패킹: 실행파일을 암호화하거나, 압축하여 소스코드를 볼 수 없도록 하는 것

3. 정적분석

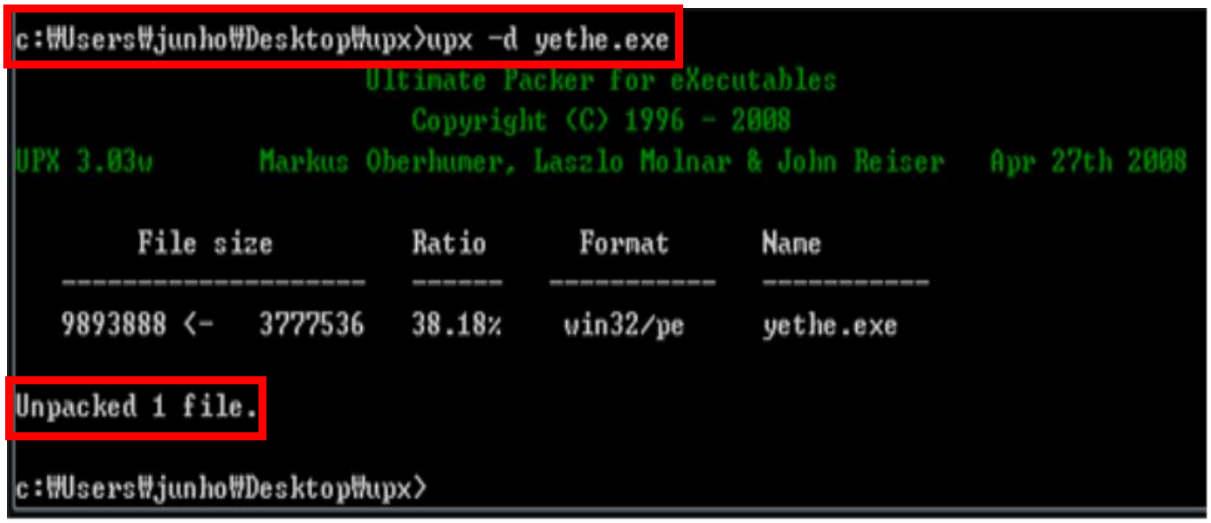
3-1. Exeinfo PE (패킹여부 확인)



[그림 3-1] Exeinfo PE 검사결과

[그림 3-1]을 보면 Exeinfo PE를 통하여 실행(EXE)파일의 패킹 여부를 확인한 결과 tber.exe 파일은 UPX로 패킹 된 파일임을 알 수 있다. 따라서 *언패킹*[4]을 해야 한다.

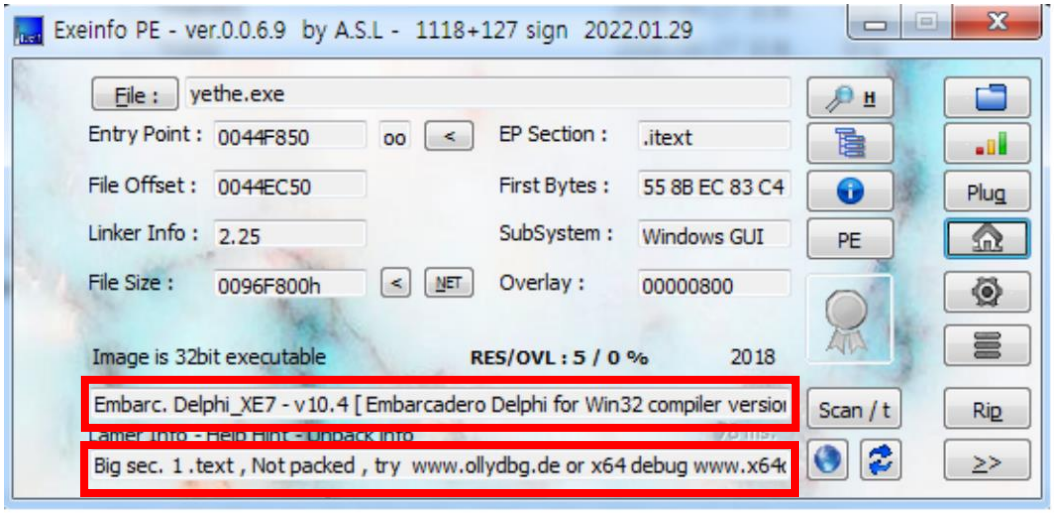
3-2 UPX 언패킹 후 파일 확인



[그림 3-2] UPX툴을 이용한 언패킹 과정

UPX(Ultimate Packer for eXecutables)는 여러 운영체제에서 수많은 파일 포맷을 지원하는 오픈 소스 실행 파일 압축 프로그램으로 UPX를 통해 파일을 패킹과 언패킹을 할 수 있다.
[그림 3-2]와 같이 UPX 실행프로그램을 cmd창에 명령어를 입력하여 언패킹하였다.

[4]언패킹: 패킹 된 파일의 압축을 푸는 행위

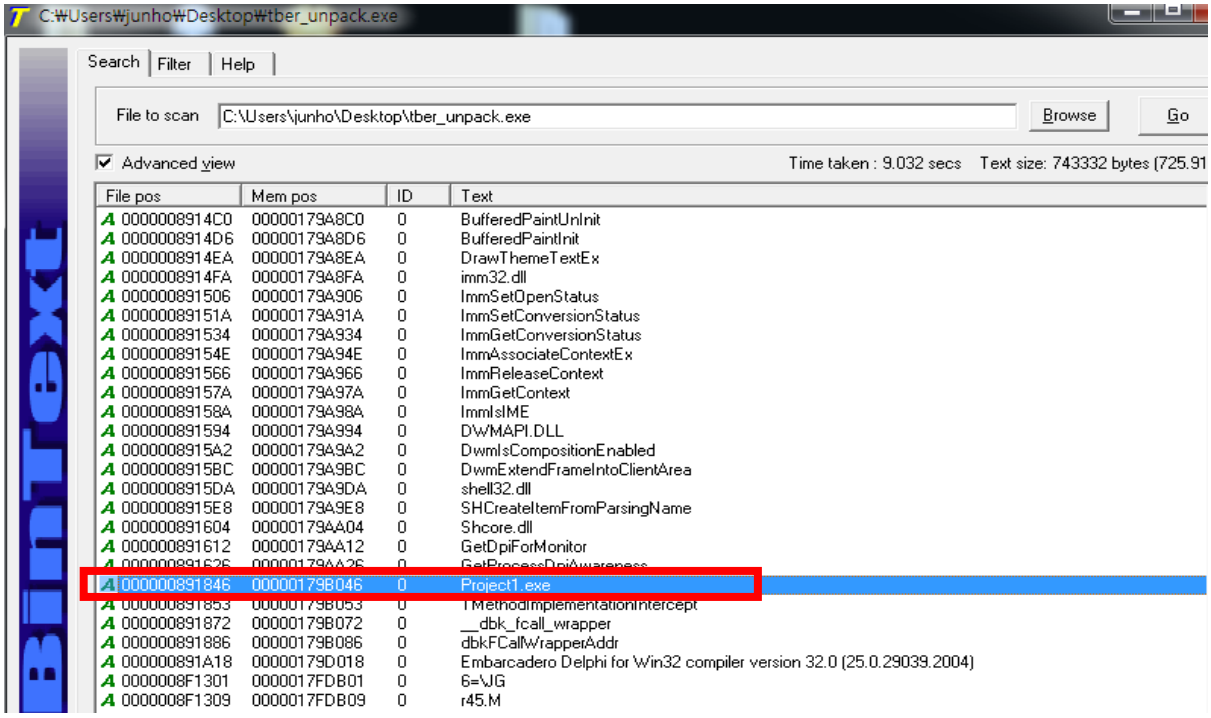


[그림 3-3] Exeinfo PE를 통해 언패킹된 파일 확인

Exeinfo를 통해 해당 파일은 delphi 언어로 만든 파일로 추측이 가능하다.

3-3. 문자열 확인 (BinText)

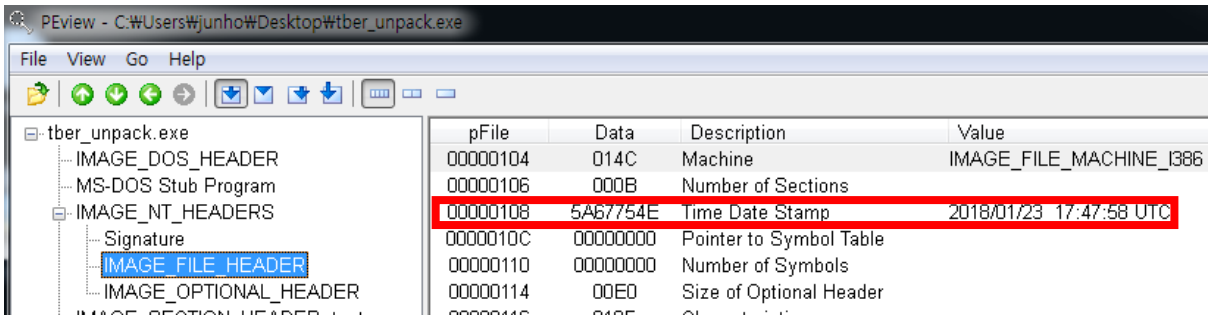
언패킹한 덤프파일을 BinText 툴을 이용하여 해당 문자열을 확인할 수 있고 문자열 확인을 통해서 어떠한 행동을 하는 지 유추할 수 있다.



[그림 3-5] Bintext 문자열

Bintext 분석 결과 파일 실행 시 Project1.exe가 실행할 수 있다고 예측할 수 있다.

3-4. PE 구조 분석 (PEView)



[그림 3-6] IMAGE_FILE HEADER 분석 결과

PE 구조를 분석해주는 PEView를 통해서 Time Date Stamp를 통해 생성시기는 2018년 1월 23일라는 것을 알 수 있다.

pFile	Data	Description	Value
00890C00	00000001	Attributes	
00890C04	0089A5EC	RVA to DLL Name	kernel32.dll
00890C08	0089A1E0	RVA to HMODULE	
00890C0C	0089A21C	RVA to Import Address Table	
00890C10	0089A32C	RVA to Import Name Table	
00890C14	0089A43C	RVA to Bound IAT	
00890C18	0089A514	RVA to Unload IAT	
00890C1C	00000000	Time Date Stamp	
00890C20	00000001	Attributes	
00890C24	0089A61C	RVA to DLL Name	user32.dll
00890C28	0089A1E4	RVA to HMODULE	
00890C2C	0089A220	RVA to Import Address Table	
00890C30	0089A334	RVA to Import Name Table	
00890C34	0089A440	RVA to Bound IAT	
00890C38	0089A518	RVA to Unload IAT	
00890C3C	00000000	Time Date Stamp	
00890C40	00000001	Attributes	
00890C44	0089A636	RVA to DLL Name	wtsapi32.dll
00890C48	0089A1E8	RVA to HMODULE	
00890C4C	0089A224	RVA to Import Address Table	
00890C50	0089A33C	RVA to Import Name Table	
00890C54	0089A444	RVA to Bound IAT	
00890C58	0089A51C	RVA to Unload IAT	
00890C5C	00000000	Time Date Stamp	
00890C60	00000001	Attributes	
00890C64	0089A68A	RVA to DLL Name	user32.dll
00890C68	0089A1EC	RVA to HMODULE	
00890C6C	0089A22C	RVA to Import Address Table	
00890C70	0089A348	RVA to Import Name Table	
00890C74	0089A44C	RVA to Bound IAT	
00890C78	0089A524	RVA to Unload IAT	
00890C7C	00000000	Time Date Stamp	

00890CA0	00000001	Attributes	
00890CA4	0089A71A	RVA to DLL Name	kernel32.dll
00890CA8	0089A1F4	RVA to HMODULE	
00890CAC	0089A244	RVA to Import Address Table	
00890CB0	0089A368	RVA to Import Name Table	
00890CB4	0089A464	RVA to Bound IAT	
00890CB8	0089A53C	RVA to Unload IAT	
00890CBC	00000000	Time Date Stamp	
00890CC0	00000001	Attributes	
00890CC4	0089A796	RVA to DLL Name	advapi32.dll
00890CC8	0089A1F8	RVA to HMODULE	
00890CCC	0089A258	RVA to Import Address Table	
00890CD0	0089A380	RVA to Import Name Table	
00890CD4	0089A478	RVA to Bound IAT	
00890CD8	0089A550	RVA to Unload IAT	
00890CDC	00000000	Time Date Stamp	
00890CE0	00000001	Attributes	
00890CE4	0089A7B6	RVA to DLL Name	rpcrt4.dll
00890CE8	0089A1FC	RVA to HMODULE	
00890CEC	0089A25C	RVA to Import Address Table	
00890CF0	0089A388	RVA to Import Name Table	
00890CF4	0089A47C	RVA to Bound IAT	
00890CF8	0089A554	RVA to Unload IAT	
00890CFC	00000000	Time Date Stamp	
00890D00	00000001	Attributes	
00890D04	0089A7D0	RVA to DLL Name	windowscodecs.dll
00890D08	0089A200	RVA to HMODULE	
00890D0C	0089A260	RVA to Import Address Table	
00890D10	0089A390	RVA to Import Name Table	
00890D14	0089A480	RVA to Bound IAT	
00890D18	0089A558	RVA to Unload IAT	
00890D1C	00000000	Time Date Stamp	
00890D20	00000001	Attributes	
00890D24	0089A7FC	RVA to DLL Name	uxtheme.dll
00890D40	00000001	Attributes	
00890D44	0089A8FA	RVA to DLL Name	imm32.dll
00890D48	0089A208	RVA to HMODULE	
00890D4C	0089A28C	RVA to Import Address Table	
00890D50	0089A3C4	RVA to Import Name Table	
00890D54	0089A4AC	RVA to Bound IAT	
00890D58	0089A584	RVA to Unload IAT	
00890D5C	00000000	Time Date Stamp	
00890D60	00000001	Attributes	
00890D64	0089A994	RVA to DLL Name	DWMAPI.DLL
00890D68	0089A20C	RVA to HMODULE	
00890D6C	0089A2A8	RVA to Import Address Table	
00890D70	0089A3E4	RVA to Import Name Table	
00890D74	0089A4C8	RVA to Bound IAT	
00890D78	0089A5A0	RVA to Unload IAT	
00890D7C	00000000	Time Date Stamp	
00890D80	00000001	Attributes	
00890D84	0089A9DA	RVA to DLL Name	shell32.dll
00890D88	0089A210	RVA to HMODULE	
00890D8C	0089A2B0	RVA to Import Address Table	
00890D90	0089A3F0	RVA to Import Name Table	
00890D94	0089A4D0	RVA to Bound IAT	
00890D98	0089A5A8	RVA to Unload IAT	
00890D9C	00000000	Time Date Stamp	
00890DA0	00000001	Attributes	
00890DA4	0089AA04	RVA to DLL Name	Shcore.dll
00890DA8	0089A214	RVA to HMODULE	

0088D478	00000000	Import Name Table RVA	
0088D47C	00000000	Time Date Stamp	
0088D480	00000000	Forwarder Chain	
0088D484	0089724C	Name RVA	ole32.dll
0088D488	00897024	Import Address Table RVA	
0088D48C	00000000	Import Name Table RVA	
0088D490	00000000	Time Date Stamp	
0088D494	00000000	Forwarder Chain	
0088D498	00897256	Name RVA	oleaut32.dll
0088D49C	00896D2C	Import Address Table RVA	
0088D4A0	00000000	Import Name Table RVA	
0088D4A4	00000000	Time Date Stamp	
0088D4A8	00000000	Forwarder Chain	
0088D4AC	00897263	Name RVA	shell32.dll
0088D4B0	00896A2C	Import Address Table RVA	
0088D4B4	00000000	Import Name Table RVA	
0088D4B8	00000000	Time Date Stamp	
0088D4BC	00000000	Forwarder Chain	
0088D4C0	0089726F	Name RVA	user32.dll
0088D4C4	00896A34	Import Address Table RVA	
0088D4C8	00000000	Import Name Table RVA	
0088D4CC	00000000	Time Date Stamp	
0088D4D0	00000000	Forwarder Chain	
0088D4D4	0089727A	Name RVA	version.dll
0088D4D8	00896D1C	Import Address Table RVA	
0088D4DC	00000000	Import Name Table RVA	
0088D4E0	00000000	Time Date Stamp	
0088D4E4	00000000	Forwarder Chain	
0088D4E8	00897286	Name RVA	winspool.drv
0088D4EC	00896984	Import Address Table RVA	

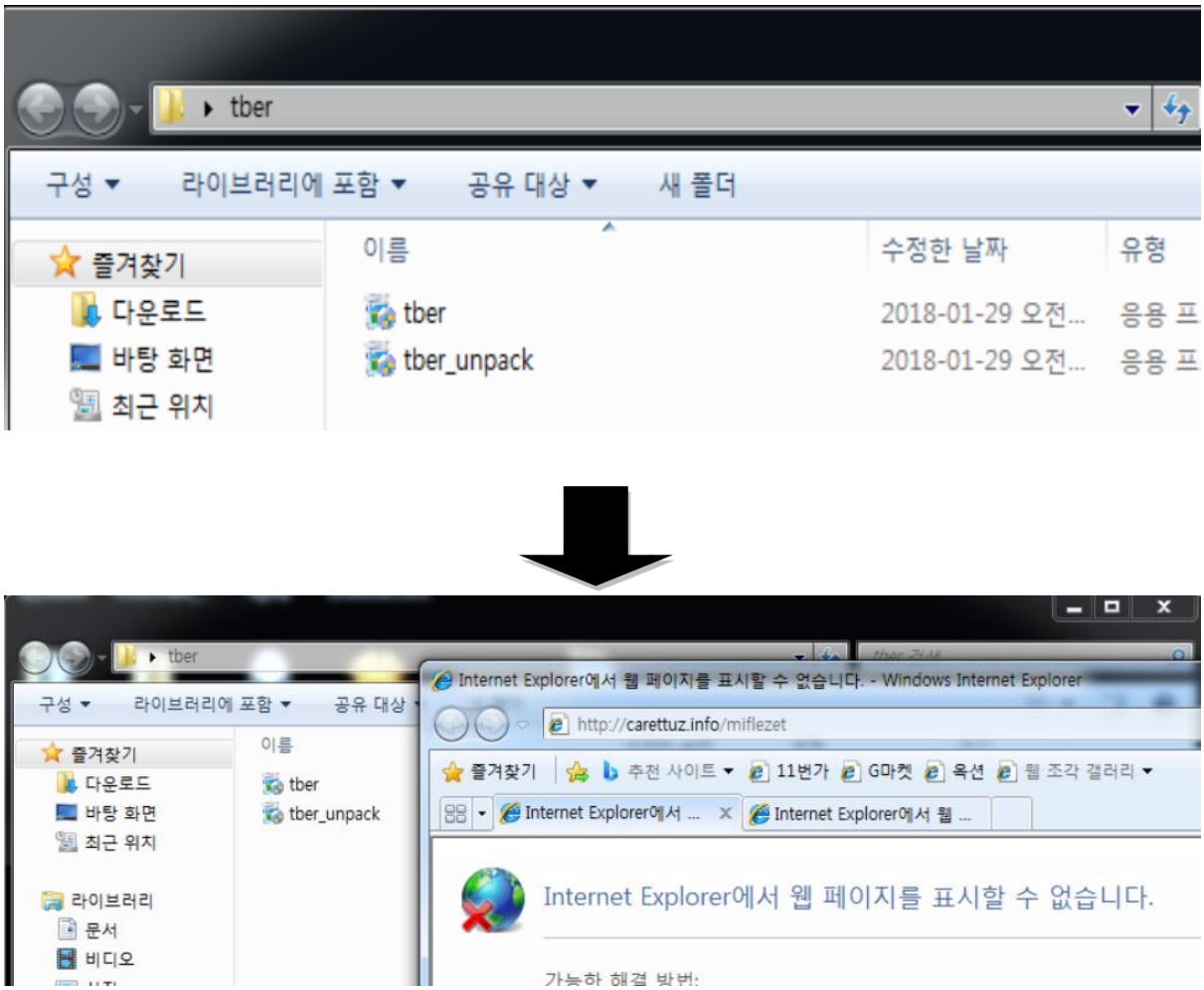
pFile	Data	Description	Value
0088D400	00000000	Import Name Table RVA	
0088D404	00000000	Time Date Stamp	
0088D408	00000000	Forwarder Chain	
0088D40C	00897204	Name RVA	KERNEL32.DLL
0088D410	00896E54	Import Address Table RVA	
0088D414	00000000	Import Name Table RVA	
0088D418	00000000	Time Date Stamp	
0088D41C	00000000	Forwarder Chain	
0088D420	00897211	Name RVA	advapi32.dll
0088D424	00896D84	Import Address Table RVA	
0088D428	00000000	Import Name Table RVA	
0088D42C	00000000	Time Date Stamp	
0088D430	00000000	Forwarder Chain	
0088D434	0089721E	Name RVA	comctl32.dll
0088D438	0089699C	Import Address Table RVA	
0088D43C	00000000	Import Name Table RVA	
0088D440	00000000	Time Date Stamp	
0088D444	00000000	Forwarder Chain	
0088D448	0089722B	Name RVA	gdi32.dll
0088D44C	00897068	Import Address Table RVA	
0088D450	00000000	Import Name Table RVA	
0088D454	00000000	Time Date Stamp	
0088D458	00000000	Forwarder Chain	
0088D45C	00897235	Name RVA	netapi32.dll
0088D460	00896E48	Import Address Table RVA	
0088D464	00000000	Import Name Table RVA	
0088D468	00000000	Time Date Stamp	
0088D46C	00000000	Forwarder Chain	
0088D470	00897242	Name RVA	ntdll.dll
0088D474	008971FC	Import Address Table RVA	

[그림 3-7] IMPORT DLL Names 분석 결과

[그림 3-7]를 통해 tber.exe의 DLL파일을 알 수 있다. (kernel32.dll / advapi32.dll / comctl32.dll / gdi32.dll / netapi32.dll / ntdll.dll / ole32.dll / oleaut32.dll / shell32.dll / user32.dll / version.dll / winspool.drv / wtsapi32.dll / msimg32.dll / rpcrt4.dll / windowscodecs.dll / uxtheme.dll / imm32.dll / DWMAPI.DLL / Shcore.dll). 이는 BinText에서 나온 결과와 같은 것을 알 수 있다.

4. 동적분석

4-1 파일실행

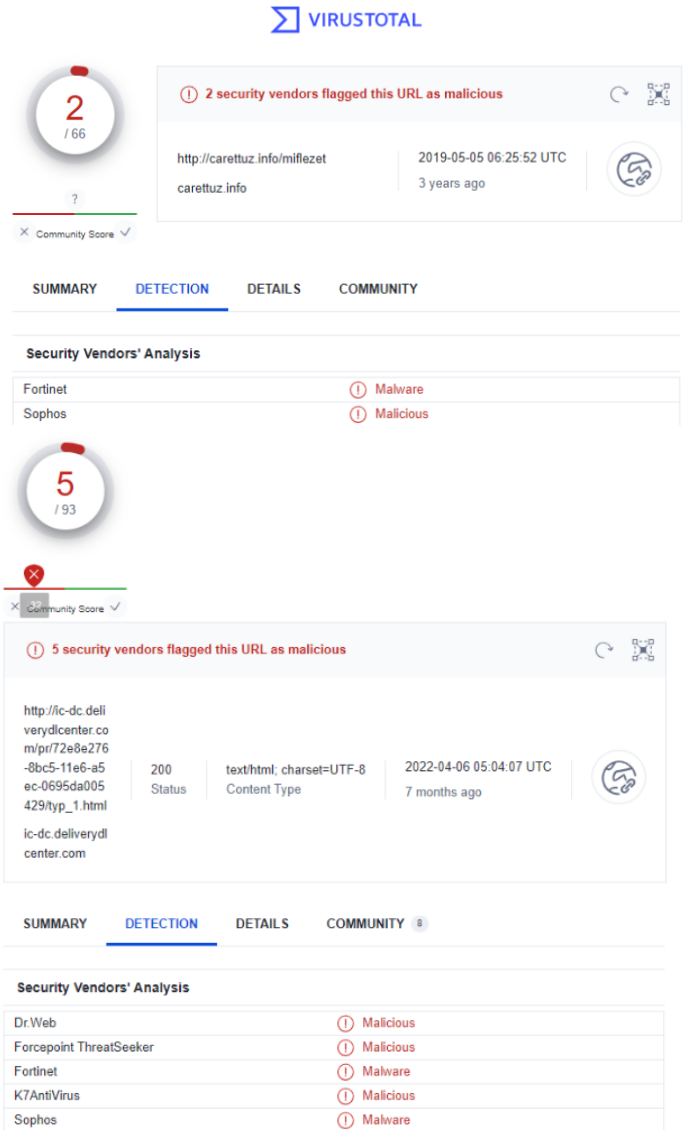


[그림 4-1] 파일 실행 전 후

파일 실행 시 아래 두 링크의 인터넷창이 생성된다.

http://carettuz.info/miflezet

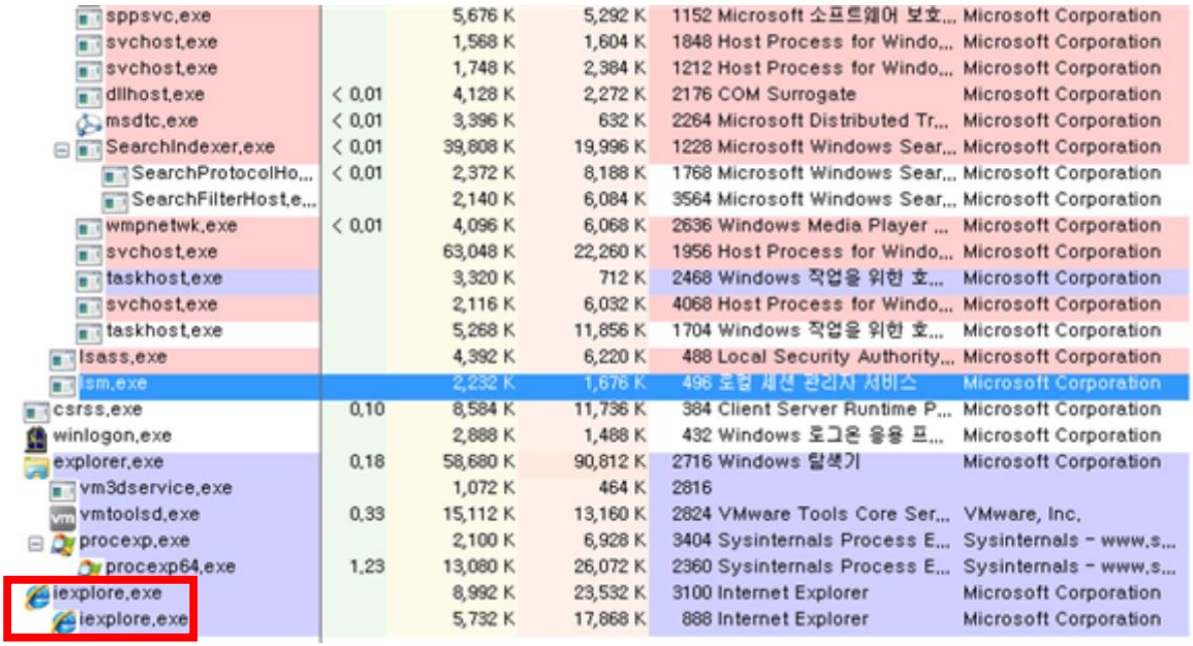
http://ic-dc.deliverydlcenter.com/pr/72e8e276-8bc5-11e6-a5ec-0695da005429/typ_1.html



[그림 4-2] 생성된 사이트 기초분석 결과

tber.exe 파일을 실행 시 생성된 사이트를 기초 분석한 결과 [그림 4-2]와 같이 악성코드가 탐지되었다. 그 외의 활동은 발견되지 않았다.

4-2 프로세스 변화 확인 (Procexp)

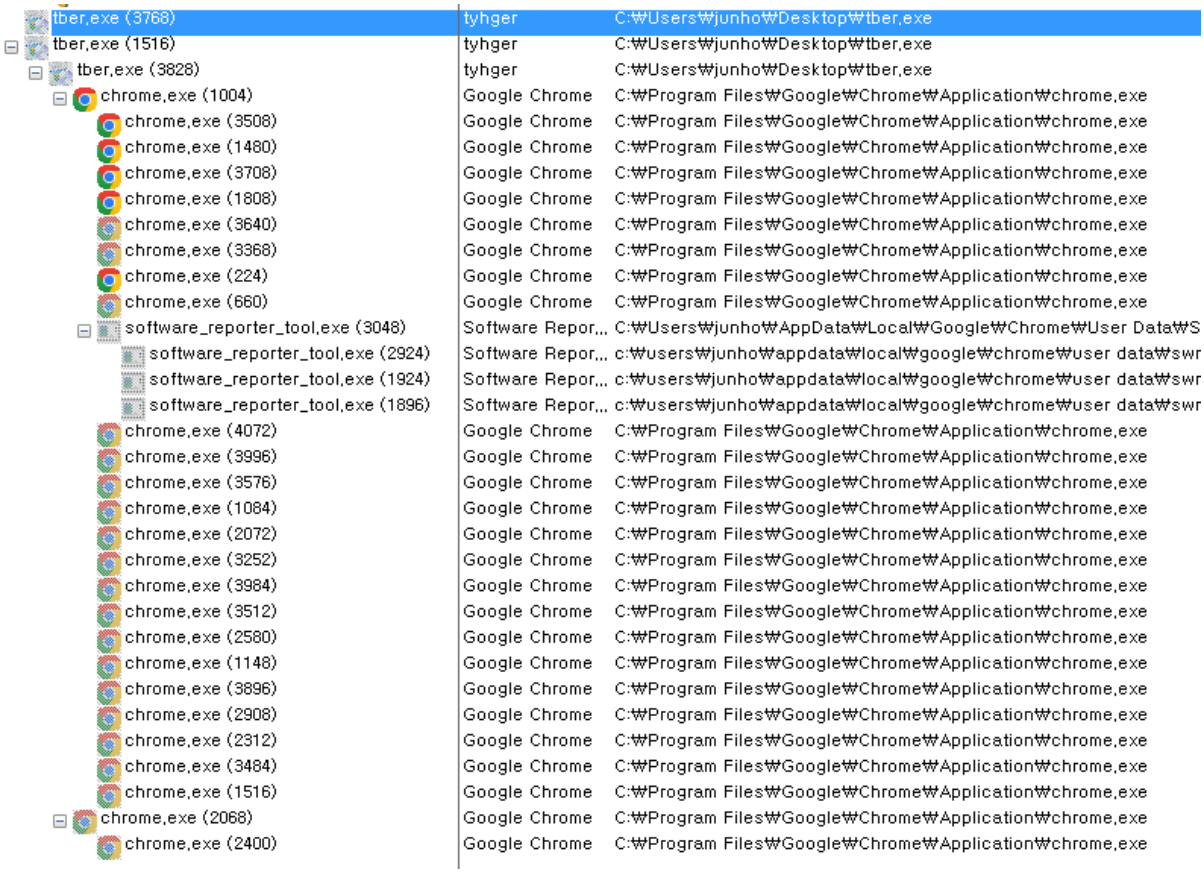


sppsvc.exe		5,676 K	5,292 K	1152 Microsoft 소프트웨어 보호...	Microsoft Corporation
svchost.exe		1,568 K	1,604 K	1848 Host Process for Windo...	Microsoft Corporation
svchost.exe		1,748 K	2,384 K	1212 Host Process for Windo...	Microsoft Corporation
dllhost.exe	< 0.01	4,128 K	2,272 K	2176 COM Surrogate	Microsoft Corporation
msdtc.exe	< 0.01	3,396 K	632 K	2264 Microsoft Distributed Tr...	Microsoft Corporation
SearchIndexer.exe	< 0.01	39,808 K	19,996 K	1228 Microsoft Windows Sear...	Microsoft Corporation
SearchProtocolHo...	< 0.01	2,372 K	8,188 K	1768 Microsoft Windows Sear...	Microsoft Corporation
SearchFilterHost.e...		2,140 K	6,084 K	3564 Microsoft Windows Sear...	Microsoft Corporation
wmpnetwk.exe	< 0.01	4,096 K	6,068 K	2636 Windows Media Player ...	Microsoft Corporation
svchost.exe		63,048 K	22,260 K	1956 Host Process for Windo...	Microsoft Corporation
taskhost.exe		3,320 K	712 K	2468 Windows 작업을 위한 호...	Microsoft Corporation
svchost.exe		2,116 K	6,032 K	4068 Host Process for Windo...	Microsoft Corporation
taskhost.exe		5,268 K	11,856 K	1704 Windows 작업을 위한 호...	Microsoft Corporation
lsass.exe		4,392 K	6,220 K	488 Local Security Authority...	Microsoft Corporation
lsm.exe		2,232 K	1,676 K	496 로컬 세션 관리자 서비스	Microsoft Corporation
csrss.exe	0.10	8,584 K	11,736 K	384 Client Server Runtime P...	Microsoft Corporation
winlogon.exe		2,888 K	1,488 K	432 Windows 로그온 응용 프...	Microsoft Corporation
explorer.exe	0.18	58,680 K	90,812 K	2716 Windows 탐색기	Microsoft Corporation
vm3dservice.exe		1,072 K	464 K	2816	
vmtoolsd.exe	0.33	15,112 K	13,160 K	2824 VMware Tools Core Ser...	VMware, Inc.
procexp.exe		2,100 K	6,928 K	3404 Sysinternals Process E...	Sysinternals - www.s...
procexp64.exe	1.23	13,080 K	26,072 K	2360 Sysinternals Process E...	Sysinternals - www.s...
iexplore.exe		8,992 K	23,532 K	3100 Internet Explorer	Microsoft Corporation
iexplore.exe		5,732 K	17,868 K	888 Internet Explorer	Microsoft Corporation

[그림 4-3] Process Explorer 분석 결과

tber.exe 실행 시 tber.exe 실행 파일은 실행되었다 바로 사라지면서 다음 빨간 박스와 같이 사이트 두개를 생성한다.

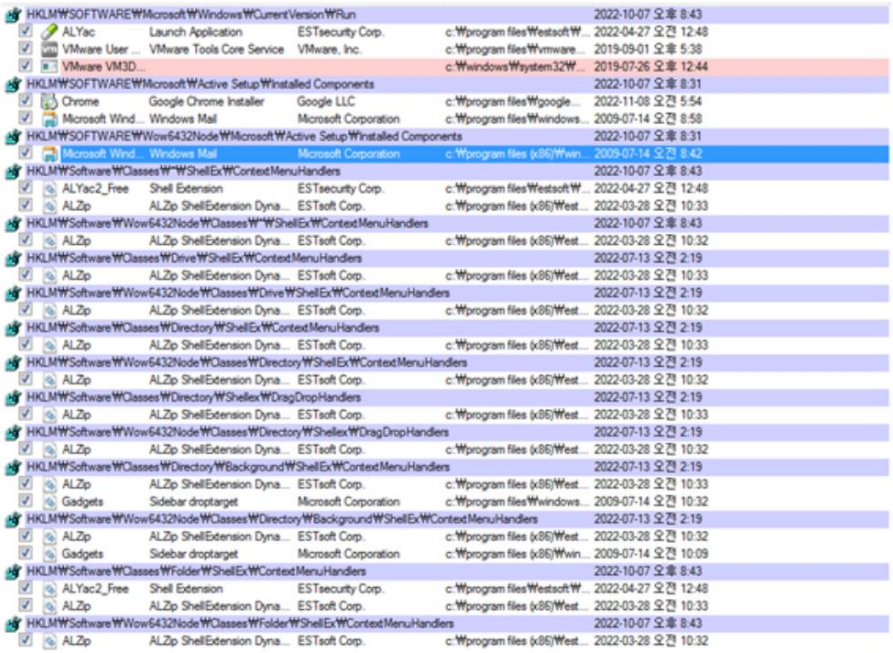
4-3. 파일 및 레지스트리 변화 확인 (Procmon, Autoruns)



tber.exe (3768)	tyhger	C:₩Users₩junho₩Desktop₩tber.exe
tber.exe (1516)	tyhger	C:₩Users₩junho₩Desktop₩tber.exe
tber.exe (3828)	tyhger	C:₩Users₩junho₩Desktop₩tber.exe
chrome.exe (1004)	Google Chrome	C:₩Program Files₩Google₩Chrome₩Application₩chrome.exe
chrome.exe (3508)	Google Chrome	C:₩Program Files₩Google₩Chrome₩Application₩chrome.exe
chrome.exe (1480)	Google Chrome	C:₩Program Files₩Google₩Chrome₩Application₩chrome.exe
chrome.exe (3708)	Google Chrome	C:₩Program Files₩Google₩Chrome₩Application₩chrome.exe
chrome.exe (1808)	Google Chrome	C:₩Program Files₩Google₩Chrome₩Application₩chrome.exe
chrome.exe (3640)	Google Chrome	C:₩Program Files₩Google₩Chrome₩Application₩chrome.exe
chrome.exe (3368)	Google Chrome	C:₩Program Files₩Google₩Chrome₩Application₩chrome.exe
chrome.exe (224)	Google Chrome	C:₩Program Files₩Google₩Chrome₩Application₩chrome.exe
chrome.exe (660)	Google Chrome	C:₩Program Files₩Google₩Chrome₩Application₩chrome.exe
software_reporter_tool.exe (3048)	Software Repor...	C:₩Users₩junho₩AppData₩Local₩Google₩Chrome₩User Data₩S
software_reporter_tool.exe (2924)	Software Repor...	c:₩users₩junho₩appdata₩local₩google₩chrome₩user data₩swr
software_reporter_tool.exe (1924)	Software Repor...	c:₩users₩junho₩appdata₩local₩google₩chrome₩user data₩swr
software_reporter_tool.exe (1896)	Software Repor...	c:₩users₩junho₩appdata₩local₩google₩chrome₩user data₩swr
chrome.exe (4072)	Google Chrome	C:₩Program Files₩Google₩Chrome₩Application₩chrome.exe
chrome.exe (3996)	Google Chrome	C:₩Program Files₩Google₩Chrome₩Application₩chrome.exe
chrome.exe (3576)	Google Chrome	C:₩Program Files₩Google₩Chrome₩Application₩chrome.exe
chrome.exe (1084)	Google Chrome	C:₩Program Files₩Google₩Chrome₩Application₩chrome.exe
chrome.exe (2072)	Google Chrome	C:₩Program Files₩Google₩Chrome₩Application₩chrome.exe
chrome.exe (3252)	Google Chrome	C:₩Program Files₩Google₩Chrome₩Application₩chrome.exe
chrome.exe (3984)	Google Chrome	C:₩Program Files₩Google₩Chrome₩Application₩chrome.exe
chrome.exe (3512)	Google Chrome	C:₩Program Files₩Google₩Chrome₩Application₩chrome.exe
chrome.exe (2580)	Google Chrome	C:₩Program Files₩Google₩Chrome₩Application₩chrome.exe
chrome.exe (1148)	Google Chrome	C:₩Program Files₩Google₩Chrome₩Application₩chrome.exe
chrome.exe (3896)	Google Chrome	C:₩Program Files₩Google₩Chrome₩Application₩chrome.exe
chrome.exe (2908)	Google Chrome	C:₩Program Files₩Google₩Chrome₩Application₩chrome.exe
chrome.exe (2312)	Google Chrome	C:₩Program Files₩Google₩Chrome₩Application₩chrome.exe
chrome.exe (3484)	Google Chrome	C:₩Program Files₩Google₩Chrome₩Application₩chrome.exe
chrome.exe (1516)	Google Chrome	C:₩Program Files₩Google₩Chrome₩Application₩chrome.exe
chrome.exe (2068)	Google Chrome	C:₩Program Files₩Google₩Chrome₩Application₩chrome.exe
chrome.exe (2400)	Google Chrome	C:₩Program Files₩Google₩Chrome₩Application₩chrome.exe

[그림 4-4] Process Monitor 분석 결과

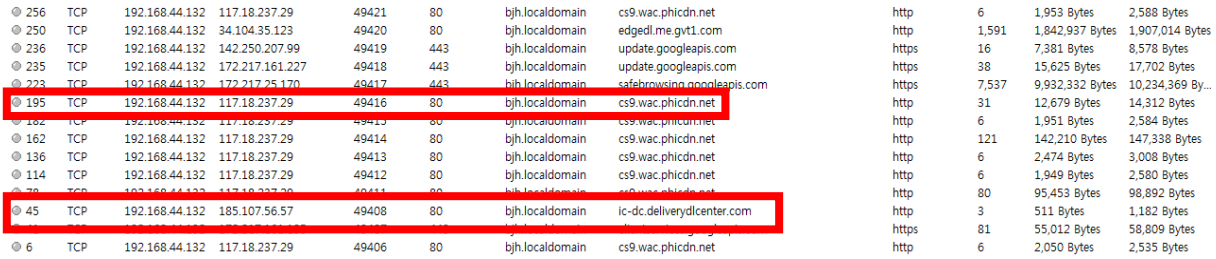
Process Monitor를 통해 프로세스 트리를 확인한 결과 tber.exe 파일을 실행했을 때 chrome.exe 파일만 실행했음을 알 수 있다.



[그림 4-8] Autoruns 분석 결과

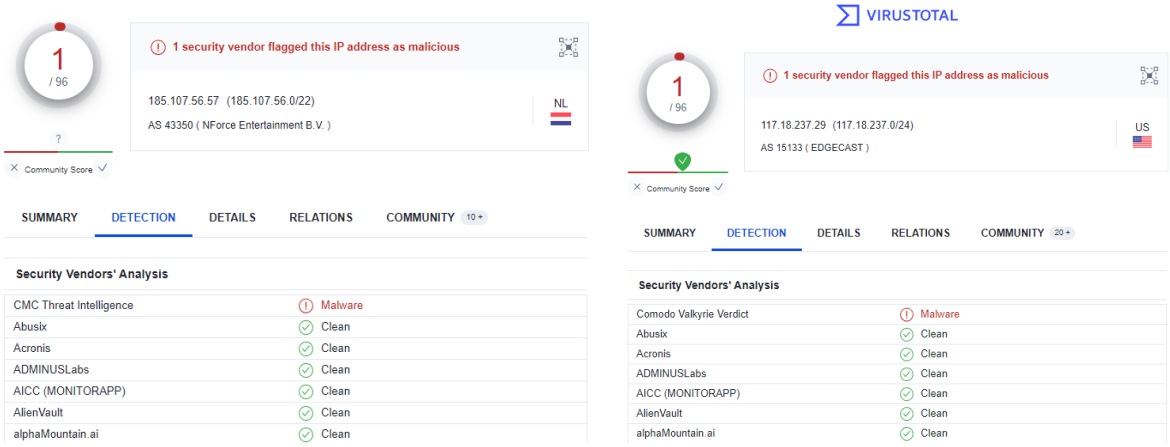
레지스트리 변화를 확인할 수 있는 도구인 Autoruns를 통해 분석한 결과 실행 전 후 변화가 없었다. 따라서 tber.exe 실행 파일은 레지스트리에 큰 영향이 없음을 알 수 있다.

4-4. 네트워크 변화 확인 (Smsniff, WireShark)



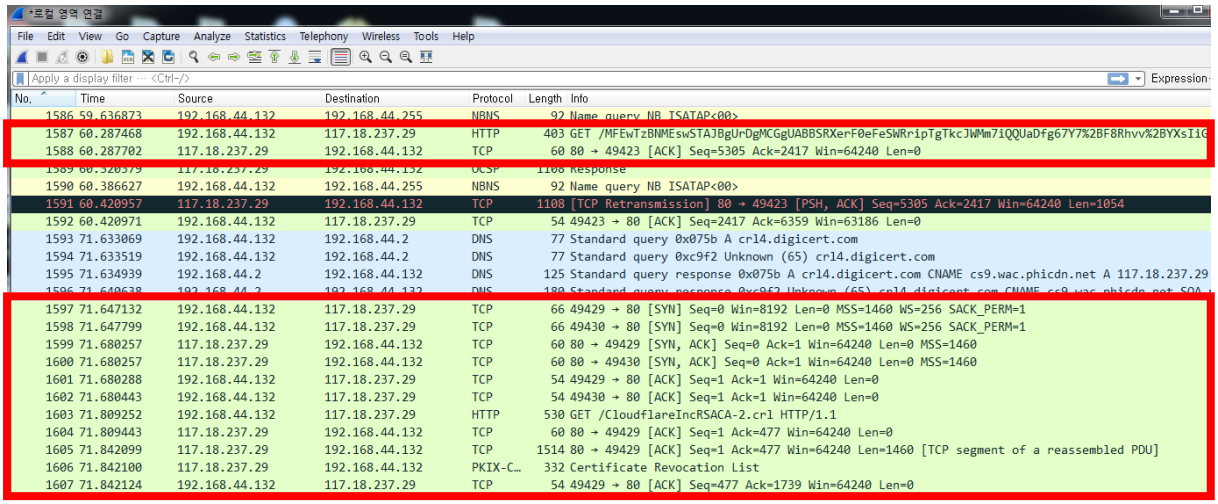
[그림 4-9] Smsniff 분석결과

Tber.exe 파일 실행 시 다음과 같이 TCP 통신을 하는 것을 알 수 있다.



[그림 4-9] VirusTotal 기초분석 결과

박스안의 IP주소를 통해 기초분석해 본 결과 악성코드가 탐지되었다. 따라서 tber.exe 실행 시 악성코드ip와 네트워크 행위를 한다고 추측할 수 있다.



[그림 4-10] WireShark 분석 결과

WireShark 분석을 통해 3-way handshaking이 일어나는 것을 알 수 있고 이 과정을 통해서 네트워크 활동을 하고 있음을 알 수 있다. 또한 GET 메소드 함수를 통하여 데이터를 받음을 알 수 있다.

5. 결론

해당 악성코드는 2018년에 1월 23일에 최초로 만들어졌으며 윈도우 환경에서 실행할 수 있는 파일이다. 기초분석 결과 Trojan과 Adware 유형의 악성코드가 진단되었다. 파일은 UPX기법으로 패킹 되어 있으며 언패킹 결과 delphi 언어로 만든 파일인 것을 알 수 있었다. 정적분석과 동적분석을 통하여 분석한 결과 파일을 임의로 설치하거나 레지스트리 변화의 흔적은 없었다. 파일 실행 시 광고성 사이트 2개가 열리는 것을 확인할 수 있었다. 또한 악성으로 추정되는 ip와 네트워크 통신을 하는 것을 확인할 수 있었다. 결과적으로 파일실행 시 팝업 창이 실행되는 Adware 유형의 악성코드로 보이고 악성 ip와 통신을 통해 정보를 훔쳐가는 Trojan 유형의 악성코드로도 추측이 가능하다.

6. 대응 방안

1. 최신 백신을 설치하고 주기적인 점검을 한다.
2. 부팅 화면 및 윈도우 시스템의 비밀번호를 설정한다.
3. 네트워크 공유 시 비밀번호를 설정하고, 읽기 기능만 공유한다.
4. 자료를 다운받을 때는 백신으로 먼저 확인을 한다.
5. 출처가 불분명한 링크, 메일, 애플리케이션 등을 열거나 설치하지 않는다
6. 불법 파일과 프로그램, 영상 등을 다운받지 않는다.
7. 개인 PC에 방화벽을 사용한다.