

악성코드 분석 보고서

(dgrep.exe / vpscript.dll)

Refactoring week18
2021. 2. 27 Kwon Moonjeong

목차

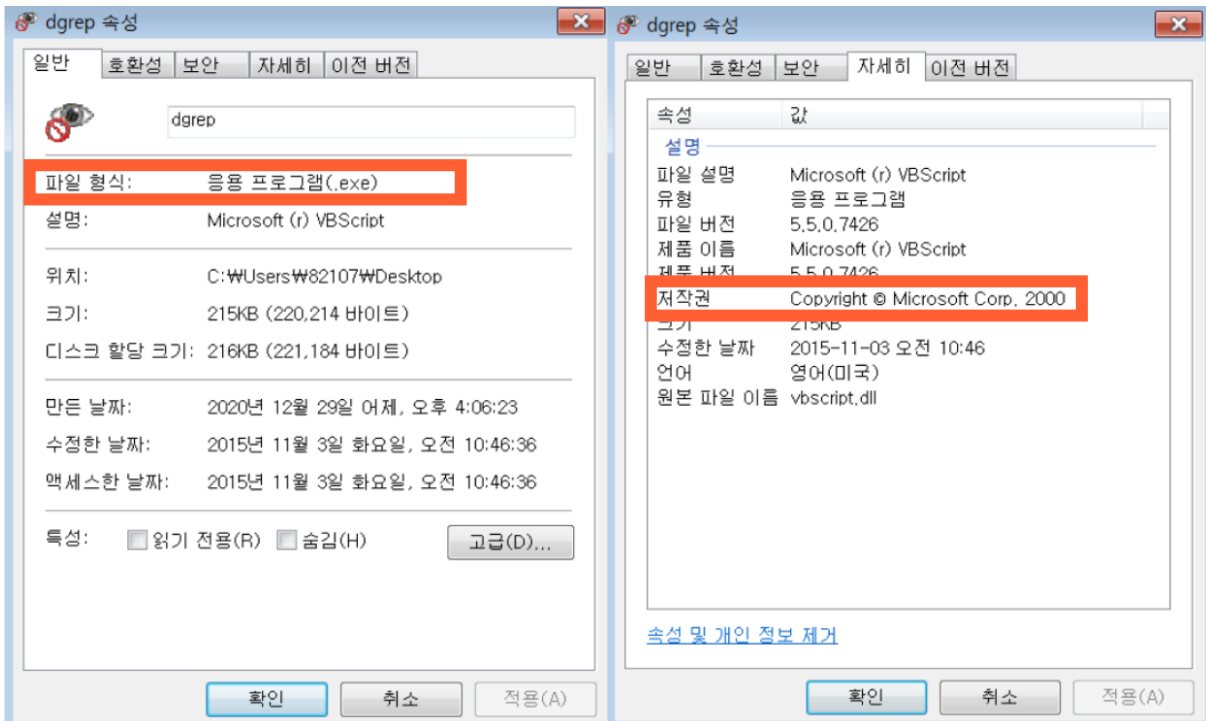
- 기초 분석 (3p)
 - 파일 정보
 - 파일 속성 살펴보기
 - VirusTotal 분석 결과
- 정적 분석 (7p)
 - EXE 파일 정보(Exeinfo PE)
 - EXE 파일 언패킹한 정보(Universal Extractor)
 - 텍스트 정보(Bintext)
 - PE 구조 분석(PEView)
- 동적 분석 (11p)
 - 파일 아이콘의 소멸
 - 신규 생성된 프로세스 분석(Process Explorer)
 - 레지스트리에서 신규 프로그램 생성(Autoruns)
 - 신규 생성된 포트(Currport)
 - 새로운 네트워크 패킷(Wireshark)
- 결론 및 대응 방안 (21p)

파일 정보

구분	내용
파일명	vbscript.dll, dgrep.exe
파일 버전	5.5.0.7426
파일 크기	215.05 KB
제작 시기	2015-10-09 03:43:26
파일 타입	Win32 EXE
제작사	Copyright © Microsoft Corp. 2000 : 정상적인 일반 파일인 것처럼 사용자를 속임
MD5	68af0599e74d36bc2f39a2710754082c
SHA-1	c63f22e2d6feecbe9801c76a76f81589bce1b9a3
SHA-256	d3e4a46b95a3a54c762f0e1696e9167528bd1cf3 0b190e4893b44f0259e7893c
포함 함수	KERNEL32.dll / GDI32.dll / MFC42.dll / WS32.dll MSVCRT.dll / SHLWAPI.dll / USER32.dll
악성코드 분류	백도어/트로이 목마
출처	실습 파일으로 소원석 멘토님께 Evernote를 통하여 전달 받음

[표 1-1] 악성코드 파일 정보를 축약한 표이다.

파일 속성 살펴보기



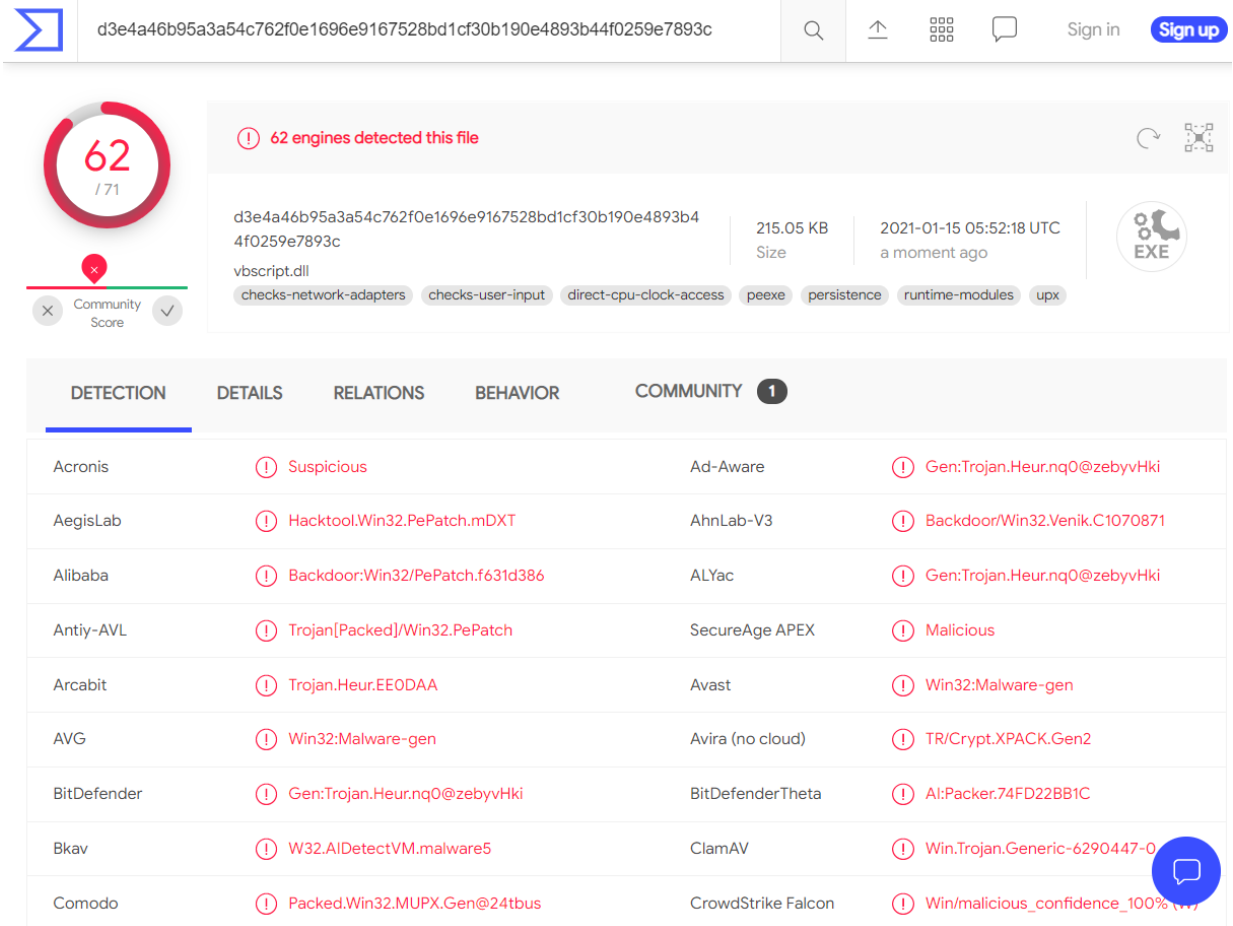
[그림 1-1] 파일 아이콘에서 오른쪽 클릭으로 속성창을 연 모습

악성코드 dgrep.exe를 분석하기 전에 속성을 살펴보았다.

본 파일은 실행파일(확장자 .exe)로 실행했을 때 컴퓨터 상에 어떠한 행동이 나타날 것임을 추측할 수 있다.

또한 저작권 항목에서 마이크로소프트사에서 만든 파일이라고 나타나 있으나, 분석을 진행한 결과 이는 신뢰할 수 없는 정보라는 결론을 얻었다.

VirusTotal 분석 결과



[그림 1-2] 악성코드 기초분석 사이트 VirusTotal에 악성코드 dgrep.exe를 업로드한 결과

악성코드 dgrep.exe을 본격적으로 분석하기 전에 분석 방향을 세우고자 악성코드 기초분석 사이트 VirusTotal으로 기초 분석을 진행하여 6페이지 상단의 [표 1-2]와 같은 결과를 얻었다.

총 71개의 백신 엔진 중 악성코드로 탐지한 엔진이 62개인 것으로 보아 악성코드일 확률이 높고, 악성코드명에 “Trojan”, “Backdoor”가 빈번하게 나타나는 것으로 보아 백도어/트로이목마일 가능성이 높다고 판단하였다.

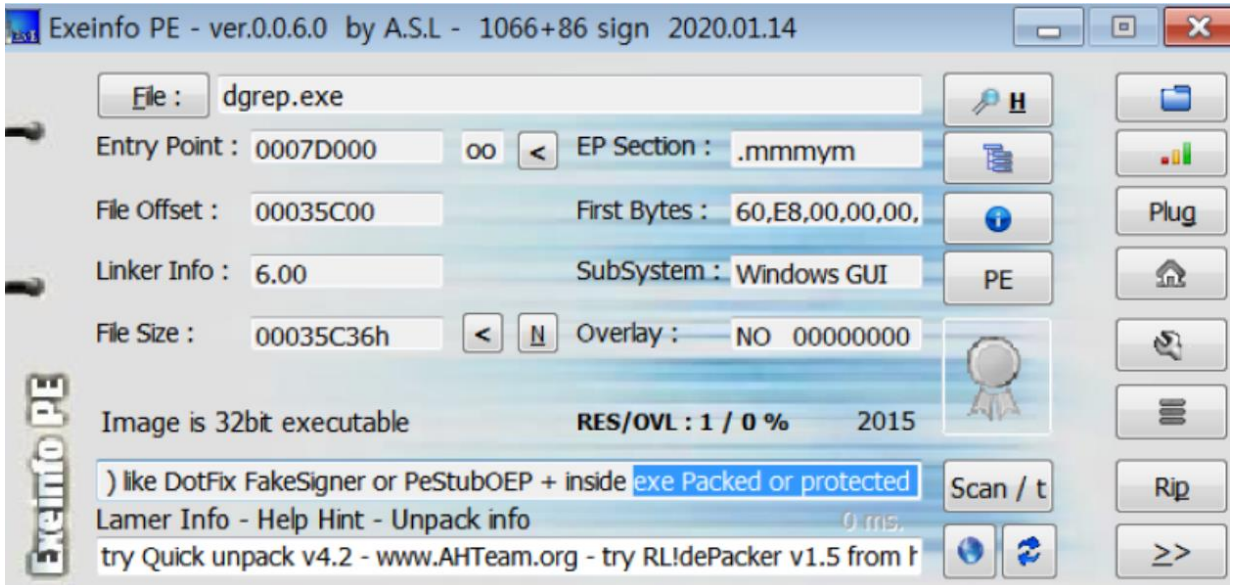
구분	내용
악성코드 탐지 백신	62 / 71
분석한 일시	2021-02-05 09:12
*HTTP Request	有 / 11개 IP주소 : 107.163.241.198
*DNS Resoultion	api.wisemansupport.com (211.110.207.188) api.admatching.co.kr (211.110.207.188)
악성코드 분류	백도어/트로이목마

[표 1-2] VirusTotal에서 획득한 정보를 축약한 표이다.

* **HTTP Request** : 웹 서버에 데이터를 요청하거나 전송할 때 보내는 패킷(데이터 한 덩어리). 네트워크 상의 활동이 발생중임을 확인할 수 있다.

* **DNS Resolution** : 네트워크 상에서 도메인 이름과 매핑(Mapping)되는 IP주소를 반환해주는 것. ex. 포털 사이트 '네이버'의 도메인 네임(<https://www.naver.com/>)을 입력했을 때 이와 대응하는 네이버의 IP인 125.209.222.141를 연결해주는 것이다.

EXE 파일 정보(Exeinfo PE)



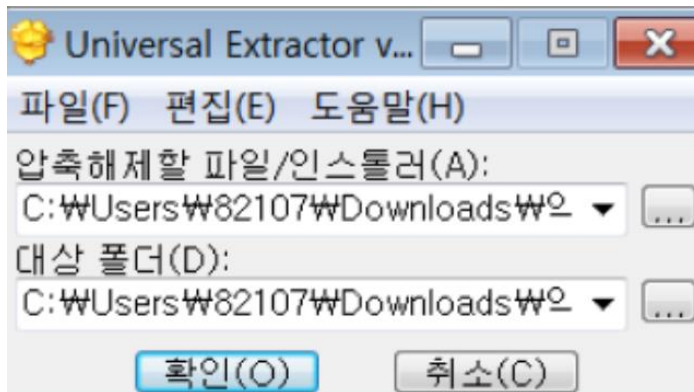
[그림 2-1] EXE 파일 정보를 보여주는 정적 분석 도구 Exeinfo PE에 악성코드 dgrep.exe를 업로드하여 얻은 결과

EXE 파일의 *패킹 여부를 확인할 수 있는 정적 분석 도구 Exeinfo PE를 사용하여 악성코드 dgrep.exe의 패킹 여부를 체크한 결과, Packed or protected로 패킹된 파일임을 알 수 있었다. 따라서 *언패킹이 필요하다.

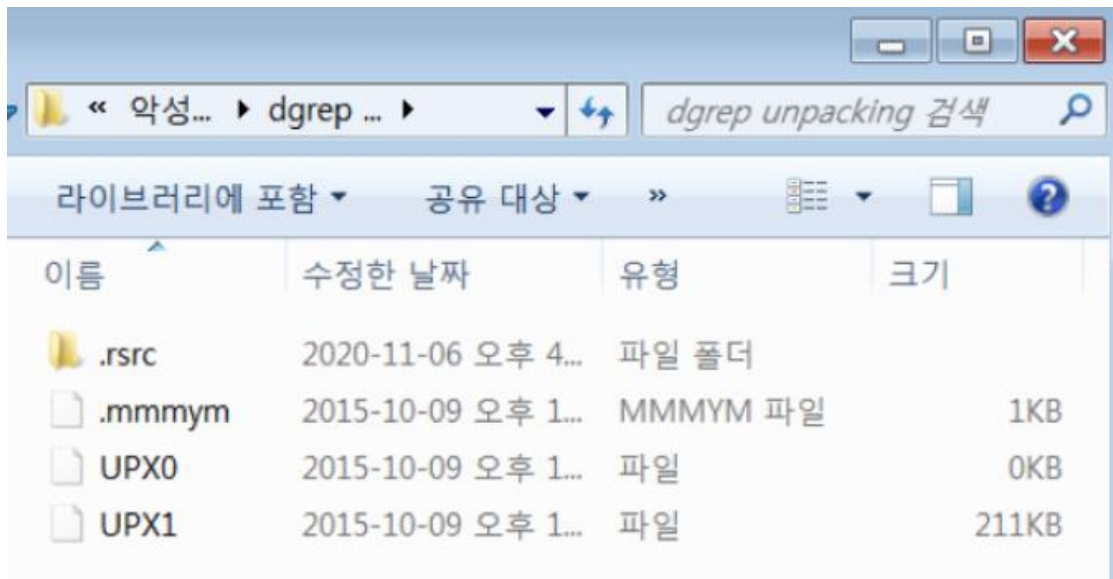
***패킹(Packing)** : 실행압축이라는 뜻으로, 실행파일(PE 파일) 압축하였으나 일반 프로그램처럼 실행 가능하다. 데이터 보호, 프로그램 크기 줄이기 등의 목적을 위하여 실행한다.

***언패킹(Unpacking)** : 패킹된 파일의 압축을 푸는 행위이다.

EXE 파일 언패킹한 정보(Universal Extractor)



[그림 2-2] 악성코드 dgrep.exe를 언패킹 프로그램 Universal Extractor에 업로드한 모습

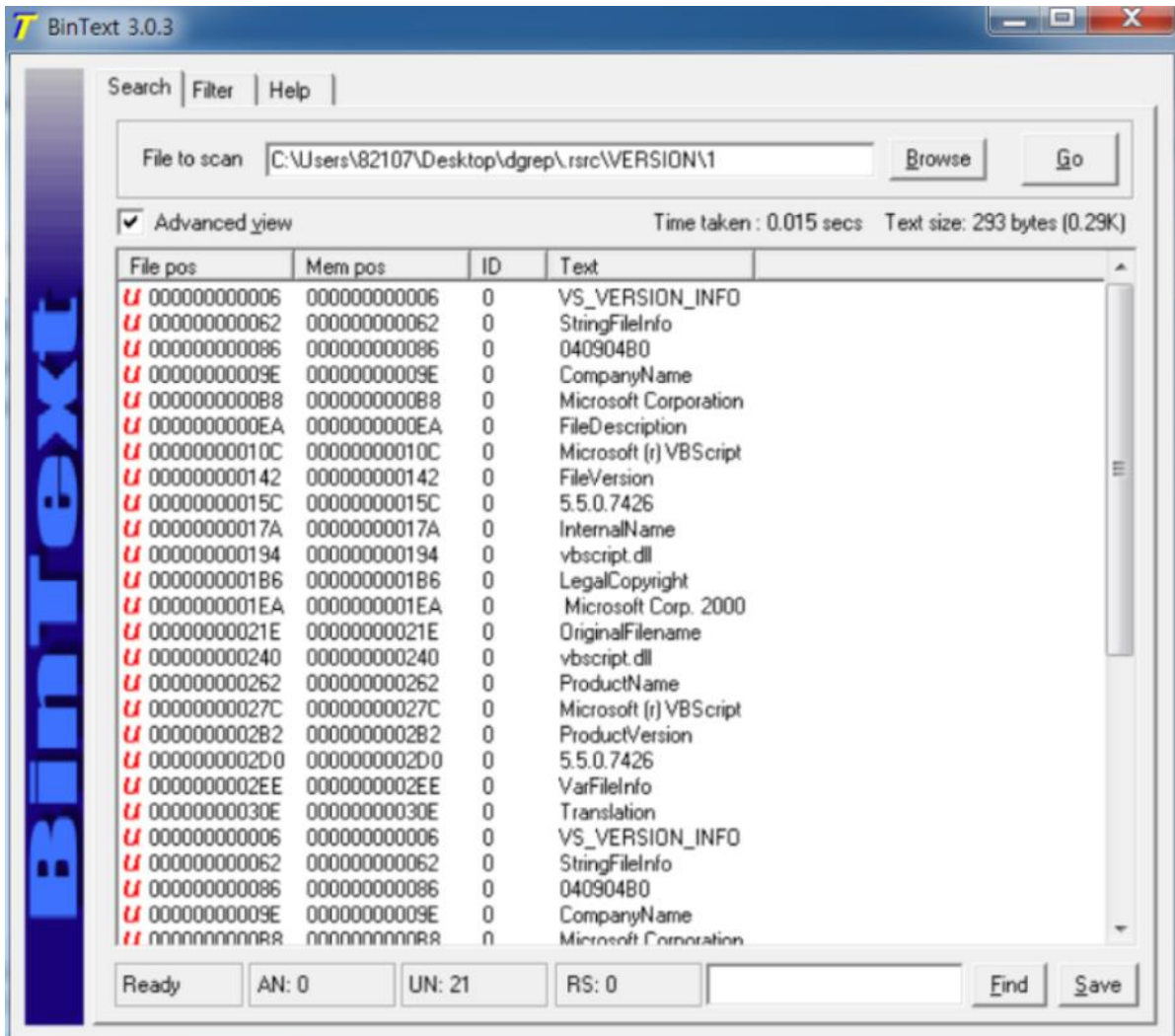


[그림 2-3] 악성코드 dgrep.exe를 언패킹하여 나온 폴더와 파일들

패킹된 EXE 파일을 언패킹하는 **Universal Extractor**를 사용하여 악성코드 dgrep.exe을 언패킹하였다. [그림 2-2]

그 결과 1개의 폴더 .rsrc와 3개의 파일 .mmmy, UPX0, UPX1을 획득하였다. [그림 2-3]

텍스트 정보(Bintext)



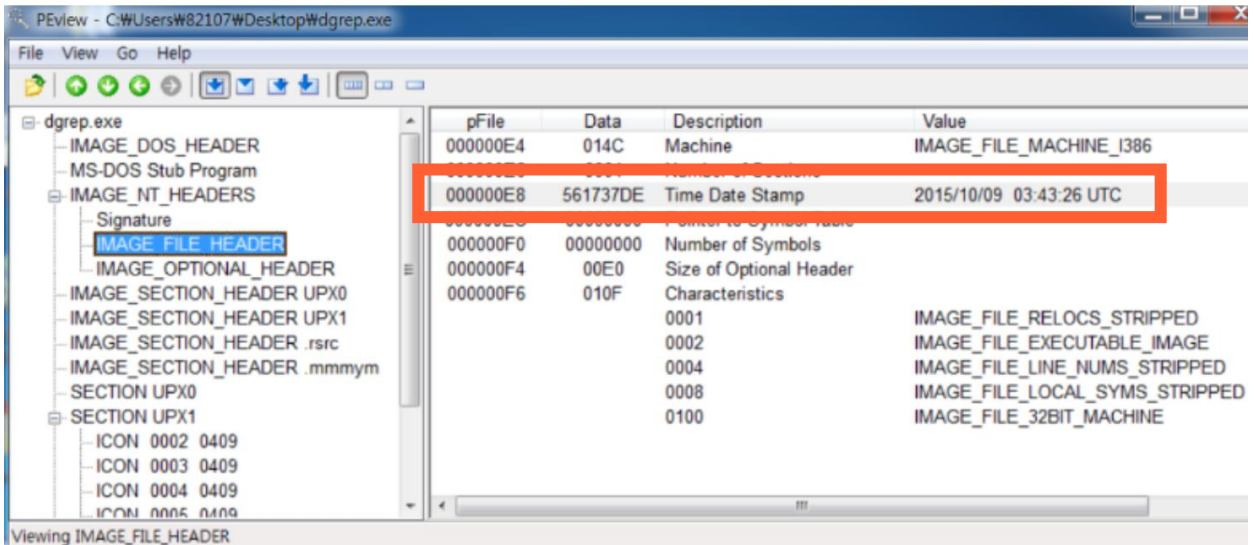
[그림 2-4] 악성코드 dgrep.exe를 언패킹한 파일을 Bintext에 업로드하여 얻은 결과

파일에서 문자열 정보를 추출하는 Bintext를 사용하여 [그림 2-4]와 같이 텍스트 정보를 얻었다.

언패킹 전에는 알 수 없는 문자들이 나와 해독이 불가능했으나, 언패킹 후에는 사용된 함수와 퍼블리셔명을 확인할 수 있었다.

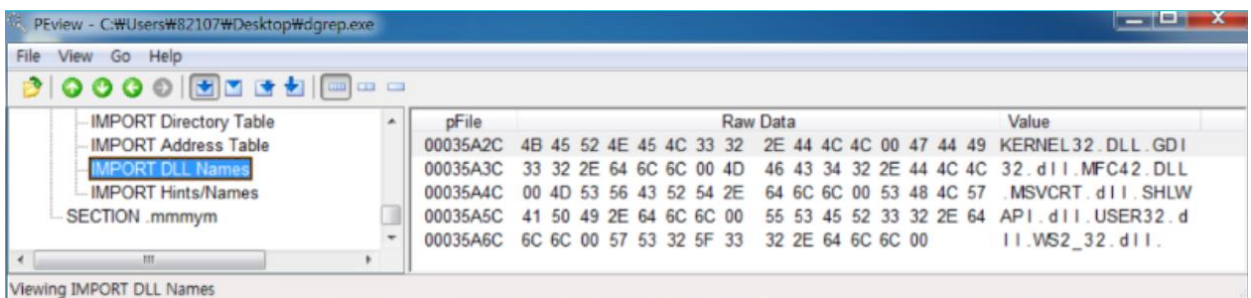
파일 속성에서 살펴본 바와 같이 마이크로소프트사에서 만든 파일이라고 나와있다.

PE 구조 분석(PEView)



[그림 2-5] 악성코드 dgrep.exe를 PEView에 업로드하여 [IMAGE_FILE_HEADER] 를 확인

*PE구조체를 분석하는 정적분석 툴 PEView를 활용하여 PE파일로서의 정보를 알아냈다. [IMAGE_FILE_HEADER]에서 타임스탬프 항목을 참고하여 본 파일의 생성 시기를 알아냈다. (생성 시기 : 2015/10/09)



[그림 2-6] PEView에서 [Import DLL Names] 를 확인

또한 [Import DLL Names]에서 사용된 *DLL 함수가 다음과 같음을 발견하였다. (KERNEL32.dll / GDI32.dll / MFC42.dll / MSVCRT.dll / SHLWAPI.dll / USER32.dll / WS32.dll)

*PE : Portable Executable은 윈도우 운영 체제에서 사용되는 실행 파일이다.

* DLL : Dynamic-Link Library는 마이크로소프트 윈도우에서 구현된 동적 라이브러리로, 내부에는 다른 프로그램이 불러서 쓸 수 있는 다양한 함수들을 가지고 있다.

파일 아이콘의 소멸



[그림 3-1] 악성코드 dgreg.exe 실행 전



[그림 3-2] 악성코드 dgreg.exe 실행 후

악성코드 dgreg.exe(vbscript.dll) 실행 시 파일 아이콘이 사라지는 것을 확인할 수 있다.

이는 사용자가 파일을 발견하지 못하도록 함으로써 악성코드 중 사용자 몰래 악성 행위를 하는 백도어(Backdoor)라는 추측을 할 수 있다.

신규 생성된 프로세스 분석(Process Explorer)

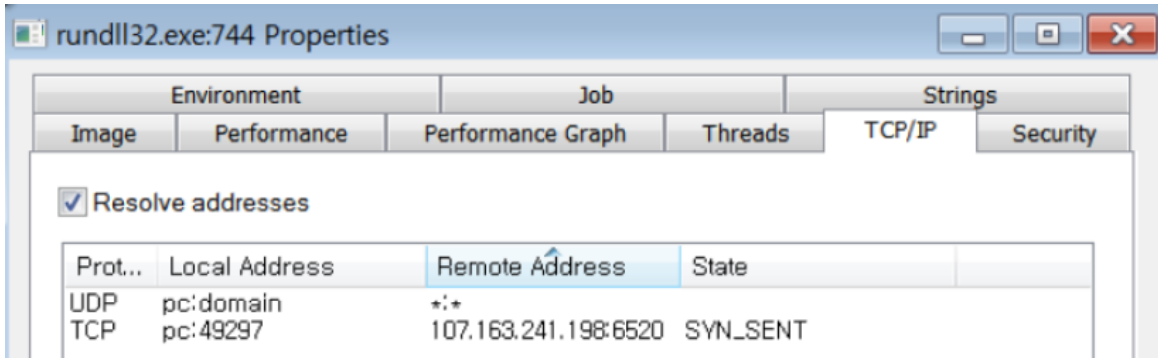
Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	56.35	0 K	24 K	0		
System	0.65	156 K	164 K	4		
Interrupts	1.27	0 K	0 K	n/a	Hardware Interrupts and D...	
smss.exe		352 K	100 K	260		
csrss.exe	< 0.01	1,896 K	1,964 K	348		
wininit.exe		1,436 K	192 K	400		
services.exe	0.05	6,000 K	5,244 K	500		
lsass.exe	0.10	3,772 K	3,664 K	508	Local Security Authority Pro...	Microsoft Corporation
lsmon.exe		2,328 K	1,540 K	516		
csrss.exe	0.42	10,648 K	10,544 K	408		
conhost.exe	0.84	1,400 K	4,640 K	3952		
vmtoolsd.exe		2,828 K	1,328 K	464		
explorer.exe	0.09	33,316 K	41,372 K	1392	Windows 탐색기	Microsoft Corporation
vm3dservice.exe		1,076 K	520 K	1668		
vmtoolsd.exe	0.25	8,540 K	10,432 K	1680	VMware Tools Core Service	VMware, Inc.
procexp.exe		2,044 K	6,992 K	3140	Sysinternals Process Expl...	Sysinternals - www.sysi...
procexp64.exe	2.19	9,816 K	20,552 K	1716	Sysinternals Process Expl...	Sysinternals - www.sysi...
GoogleCrashHandler.exe		1,400 K	68 K	836		
GoogleCrashHandler64.exe		1,388 K	112 K	884		
cmd.exe	1.20	1,984 K	3,436 K	3996		
PING.EXE	0.60	996 K	3,540 K	3868		
rundll32.exe	4.21	5,172 K	11,104 K	4084		
wiseman.exe	0.65	1,288 K	4,760 K	1876		

CPU Usage: 43.65% | Commit Charge: 34.86% | Processes: 50 | Physical Usage: 46.12%

[그림 3-3] 동적 분석 도구 Process Explorer에서 악성코드 dgrep.exe를 실행한 모습

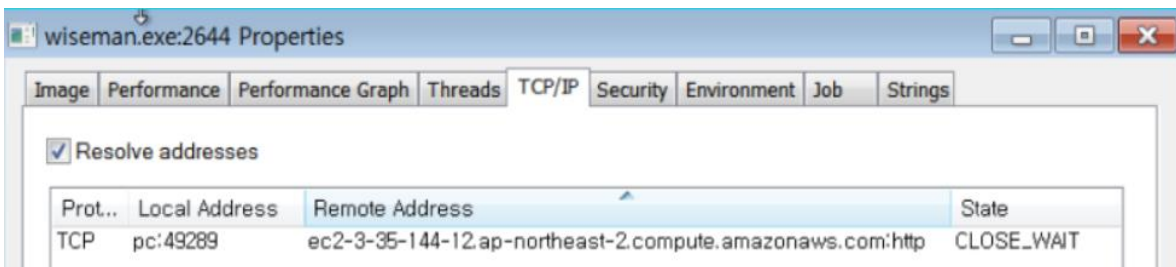
프로세스의 변화와 흐름을 파악할 수 있는 Process Explorer라는 동적 분석 툴을 활용하였다.

악성코드 dgrep.exe 실행 중 총 5개의 프로세스(conhost.exe, cmd.exe, PING.EXE, rundll32.exe, wiseman.exe)가 생성되며, 실행 된 후에는 rundll32.exe와 wiseman.exe만 남는다는 사실을 파악하였다.



[그림 3-4] 동적 분석 도구 Process Explorer에서 악성코드 dgrep.exe를 실행하여 생성된 2개의 프로세스 중 rundll32.exe의 TCP/IP 속성을 확인한 모습

*TCP 포트(원격 IP 주소 107.163.241.198, 포트 번호 6520)이 *3-way-handshake 중 SYN_SENT 상태이다. 따라서 네트워크 활동을 하기 위하여 세션 연결 중인 것으로 추정된다.

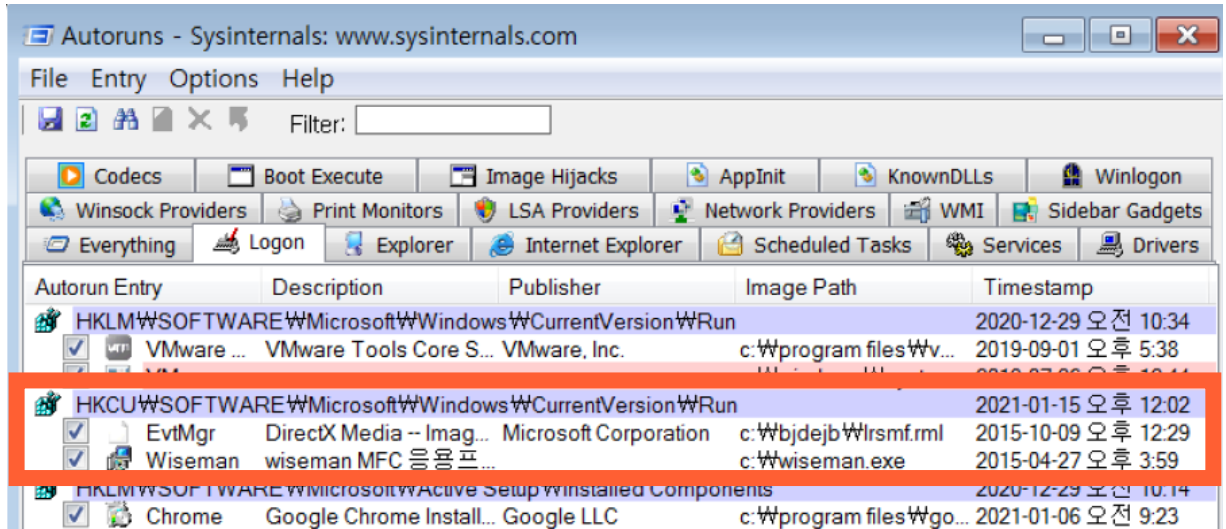


[그림 3-5] 동적 분석 도구 Process Explorer에서 악성코드 dgrep.exe를 실행하여 생성된 2개의 프로세스 중 wiseman.exe의 TCP/IP 속성을 확인한 모습

TCP 포트가 *4-way-handshake 중 CLOSE-WAIT 상태로, 네트워크 세션을 끊는 중이다. 따라서 rundll32.exe와 wiseman.exe는 네트워크 활동을 한다고 추정할 수 있다.

- * 포트(Port) : 각 응용프로그램에 할당된 논리적 주소로, 데이터를 전달하고 받는다.
- * TCP : Transmission Control Protocol의 약어로, 데이터 흐름과 전송 시 오류를 제어하여 데이터가 안정적으로 전송될 수 있도록 하는 네트워크 프로토콜
- * 3-way-handshake : TCP에서 통신하는 장치 간에 네트워크 연결을 설정하는 과정
- * 4-way-handshake : TCP에서 통신하는 장치 간에 네트워크 연결을 끊는 과정

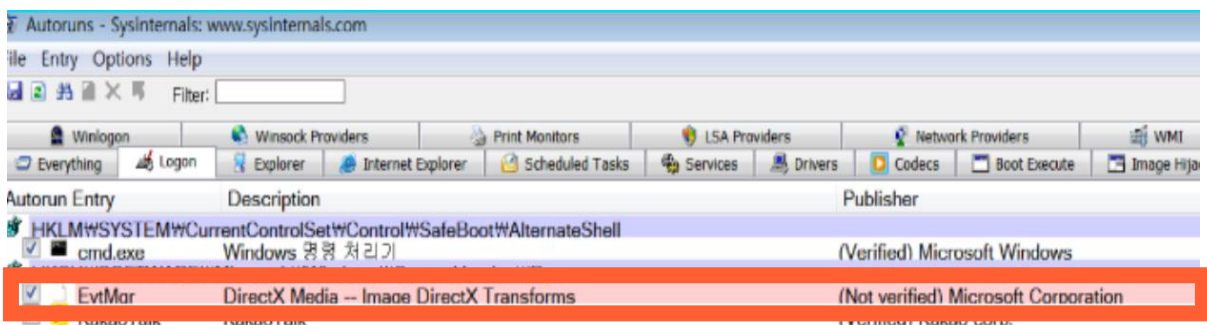
레지스트리에서 신규 프로그램 생성(Autoruns)



[그림 3-6] Autoruns에서 악성코드 dgrep.exe 실행으로 신규 생성된 프로그램 확인

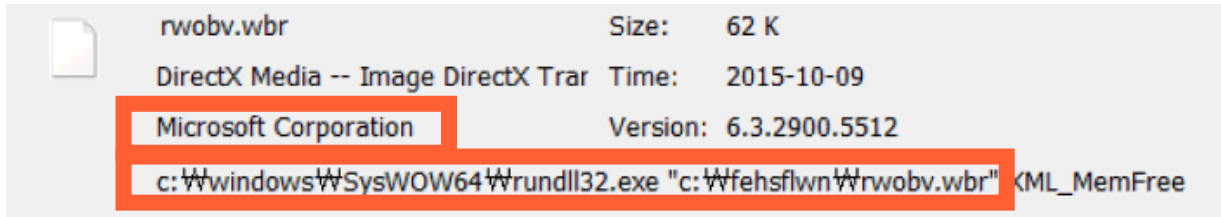
레지스트리 확인하는 동적분석 도구인 Autoruns로 확인한 결과, 새로운 프로그램 “Wiseman.exe”와 “EvMar”이 생성됨을 알 수 있다.

레지스트리의 경로인 CurrentVersion\Run에 있는 프로그램은 PC가 재부팅 될 때 자동 실행되므로, 사용자가 PC를 켤 때 저절로 실행되는 프로그램이다.



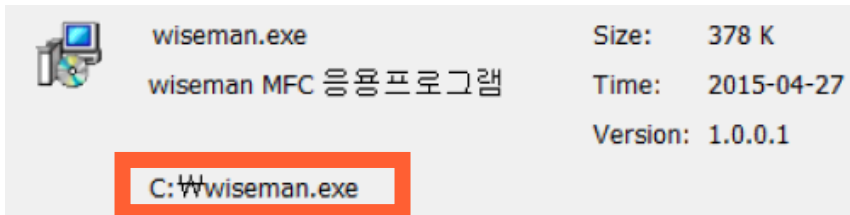
[그림 3-7] Autoruns에서 EvMar의 퍼블리셔를 검증한 모습

또한 Autoruns에 내장된 기능으로 퍼블리셔를 검증한 결과, **EvMar**의 퍼블리셔가 마이크로소프트라고 되어있으나 **Not verified**로 되어 있어 신뢰할 수 없다. 이는 사용자가 악성코드를 실행하여 설치된 프로그램이 마이크로소프트사의 프로그램이라 인지하도록 속이는 사회공학적 기법이라 할 수 있다.

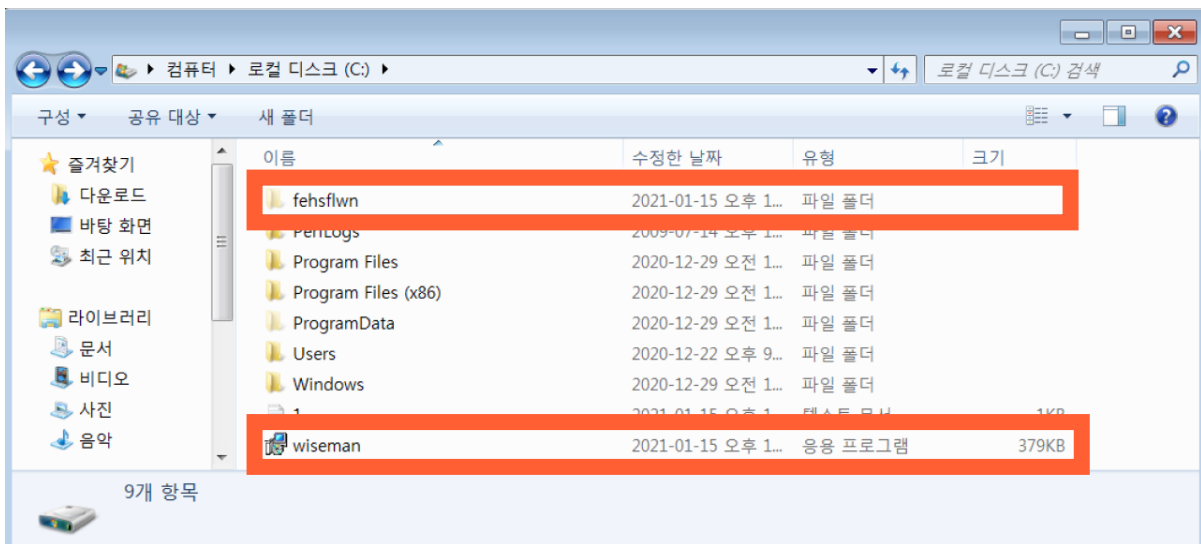


[그림 3-8] 프로그램 EvMar의 상세 정보

상세 정보에 표시된 경로에 “fehsflwn”이라는 폴더 안에 “rwobv”라는 파일이 존재한다. 또한 앞서 확인한 바와 같이 마이크로소프트사에서 제작된 것처럼 사용자를 속이려는 것으로 보인다.



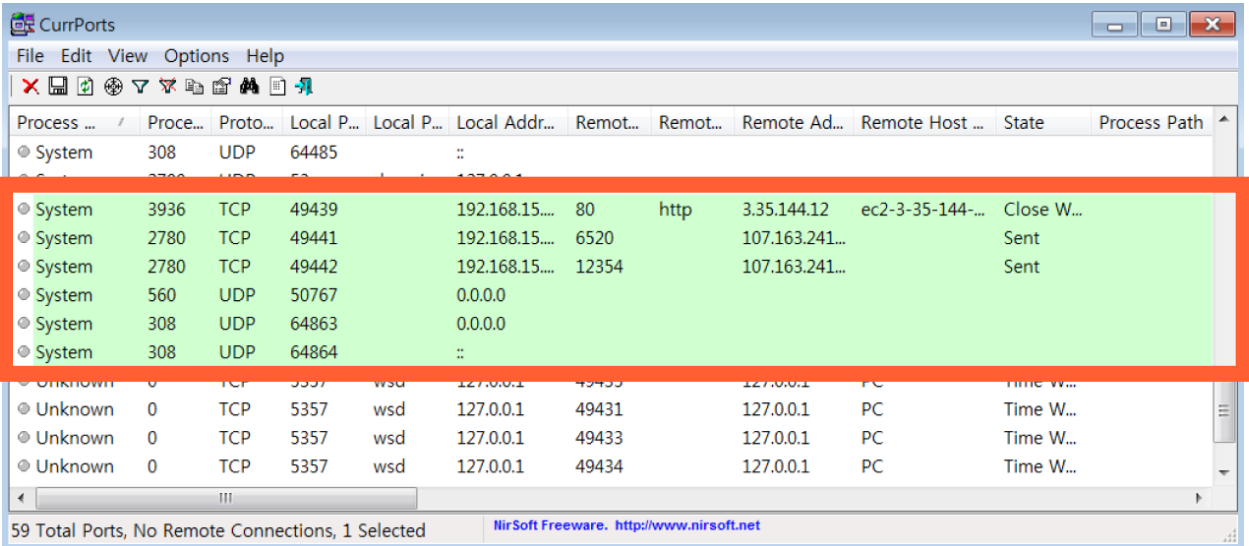
[그림 3-9] 프로그램 wiseman.exe의 상세 정보. C드라이브에 wiseman.exe가 존재한다



[그림 3-10] C드라이브에서 숨김 파일 해제를 적용한 모습

해당 경로에 fehsflwn폴더(숨김 폴더)와 Wiseman.exe가 생성됨을 확인할 수 있다. Wiseman.exe와 관련한 내용은 17페이지부터 Wireshark를 통하여 발견한 새로운 네트워크 패킷에서도 발견할 수 있다.

신규 생성된 Port(Currport)



Process ...	Proce...	Proto...	Local P...	Local P...	Local Addr...	Remot...	Remot...	Remote Ad...	Remote Host ...	State	Process Path
System	308	UDP	64485		::						
System	3936	TCP	49439		192.168.15....	80	http	3.35.144.12	ec2-3-35-144-...	Close W...	
System	2780	TCP	49441		192.168.15....	6520		107.163.241...		Sent	
System	2780	TCP	49442		192.168.15....	12354		107.163.241...		Sent	
System	560	UDP	50767		0.0.0.0						
System	308	UDP	64863		0.0.0.0						
System	308	UDP	64864		::						
Unknown	0	TCP	5357	wsd	127.0.0.1	49431		127.0.0.1	PC	Time W...	
Unknown	0	TCP	5357	wsd	127.0.0.1	49433		127.0.0.1	PC	Time W...	
Unknown	0	TCP	5357	wsd	127.0.0.1	49434		127.0.0.1	PC	Time W...	

59 Total Ports, No Remote Connections, 1 Selected

NirSoft Freeware. <http://www.nirsoft.net>

[그림 3-10] 동적 분석 도구 Currport에서 dgrep.exe 실행 후 신규 생성된 포트 6개가 발견됨

네트워크 연결을 확인하는 동적 분석 도구 Currport를 활용하여 악성코드 실행 시 TCP 포트 80, 12354, 6520가 새로 생성됨을 발견하였다.

이는 악성코드가 네트워크 활동을 할 가능성이 있음을 시사하여 추가 조사가 필요함을 뜻한다.

신규 생성된 네트워크 패킷(Wireshark)

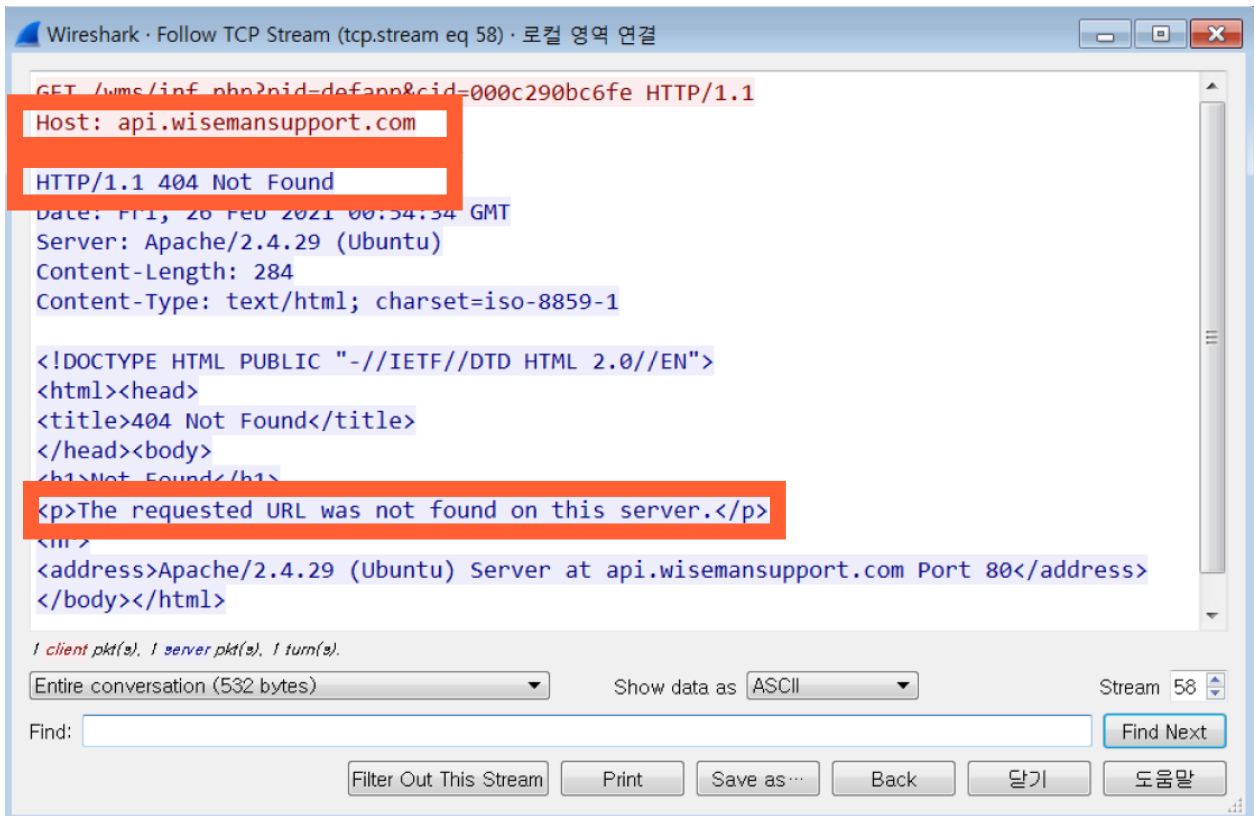
No.	Time	Source	Destination	Protocol	Length	Info
578	71.526691	192.168.15.133	3.35.144.12	TCP	66	49444 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SAC
580	71.534107	192.168.15.133	3.35.144.12	TCP	54	49444 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
581	71.534774	192.168.15.133	3.35.144.12	HTTP	141	GET /wms/inf.php?pid=defapp&cid=000c290bc6fe HTTP/1.1
585	71.642446	192.168.15.133	3.35.144.12	TCP	54	49444 → 80 [ACK] Seq=88 Ack=446 Win=63795 Len=0
588	76.549569	192.168.15.133	3.35.144.12	TCP	54	49444 → 80 [ACK] Seq=88 Ack=447 Win=63795 Len=0
2303	671.555690	192.168.15.133	3.35.144.12	TCP	54	49444 → 80 [FIN, ACK] Seq=88 Ack=447 Win=63795 Len=0
2304	671.555907	192.168.15.133	3.35.144.12	TCP	66	49472 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SAC
2307	671.574502	192.168.15.133	3.35.144.12	TCP	54	49472 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
2308	671.574618	192.168.15.133	3.35.144.12	HTTP	141	GET /wms/inf.php?pid=defapp&cid=000c290bc6fe HTTP/1.1
2312	671.692304	192.168.15.133	3.35.144.12	TCP	54	49472 → 80 [ACK] Seq=88 Ack=446 Win=63795 Len=0
2314	676.586991	192.168.15.133	3.35.144.12	TCP	54	49472 → 80 [ACK] Seq=88 Ack=447 Win=63795 Len=0
2688	1271.604078	192.168.15.133	3.35.144.12	TCP	54	49472 → 80 [FIN, ACK] Seq=88 Ack=447 Win=63795 Len=0
2689	1271.604301	192.168.15.133	3.35.144.12	TCP	66	49495 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SAC
2692	1271.609574	192.168.15.133	3.35.144.12	TCP	54	49495 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
2693	1271.609678	192.168.15.133	3.35.144.12	HTTP	141	GET /wms/inf.php?pid=defapp&cid=000c290bc6fe HTTP/1.1
2697	1271.722204	192.168.15.133	3.35.144.12	TCP	54	49495 → 80 [ACK] Seq=88 Ack=446 Win=63795 Len=0
2700	1276.623858	192.168.15.133	3.35.144.12	TCP	54	49495 → 80 [ACK] Seq=88 Ack=447 Win=63795 Len=0

[그림 3-11] 네트워크 패킷을 분석하는 도구 Wireshark를 사용하여 앞서 Currport로 발견한 악성코드의 TCP 포트의 IP주소인 3.35.144.12로 검색한 결과

No.	Time	Source	Destination	Protocol	Length	Info
38	179.959875	192.168.15.130	3.35.144.12	TCP	66	49179 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4
39	179.966170	3.35.144.12	192.168.15.130	TCP	60	80 → 49179 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 M
			3.35.144.12	TCP	54	49179 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
			192.168.15.130	HTTP	141	GET /wms/inf.php?pid=defapp&cid=000c290bc6fe HTTP/1
			192.168.15.130	TCP	60	80 → 49179 [ACK] Seq=1 Ack=88 Win=64240 Len=0
			192.168.15.130	HTTP	499	HTTP/1.1 404 Not Found (text/html)
			192.168.15.130	TCP	499	[TCP Retransmission] 80 → 49179 [PSH, ACK] Seq=1 Ac
			3.35.144.12	TCP	54	49179 → 80 [ACK] Seq=88 Ack=446 Win=63795 Len=0
			192.168.15.130	TCP	60	80 → 49179 [FIN, PSH, ACK] Seq=446 Ack=88 Win=64240
			3.35.144.12	TCP	54	49179 → 80 [ACK] Seq=88 Ack=447 Win=63795 Len=0
			192.168.15.130	TCP	54	49179 → 80 [FIN, ACK] Seq=88 Ack=447 Win=63795 Len=
			192.168.15.130	TCP	60	80 → 49179 [ACK] Seq=447 Ack=89 Win=64239 Len=0
			3.35.144.12	TCP	66	49200 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4
			192.168.15.130	TCP	60	80 → 49200 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 M
			3.35.144.12	TCP	54	49200 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0 M
			3.35.144.12	HTTP	141	GET /wms/inf.php?pid=defapp&cid=000c290bc6fe HTTP/1
			192.168.15.130	TCP	60	80 → 49200 [ACK] Seq=1 Ack=88 Win=64240 Len=0
			192.168.15.130	HTTP	499	HTTP/1.1 404 Not Found (text/html)
			192.168.15.130	TCP	499	[TCP Retransmission] 80 → 49200 [PSH, ACK] Seq=1 Ac

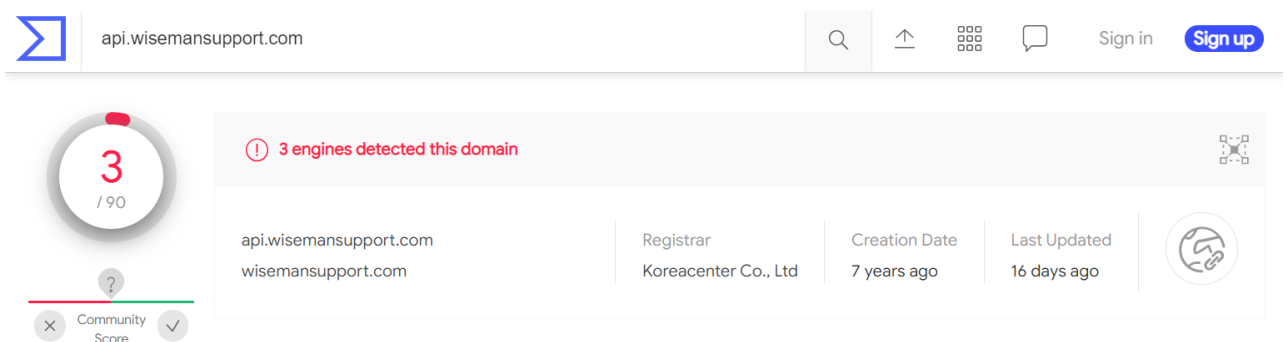
[그림 3-12] 아까 확인한 TCP 포트 중 80번의 네트워크 패킷 *Stream을 확인

* Stream : 어떤 데이터의 일관된 신호 흐름



[그림 3-13] 네트워크 패킷 *Stream을 확인하는 모습

앞서 Autoruns를 통하여 발견한 Wiseman.exe와 동일한 이름의 웹사이트(api.wiseman.support.com)와 네트워크 활동을 하는 것을 알 수 있다. 그러나 URL을 서버에서 찾을 수 없는 것으로 보아 현재 정상적인 네트워크 활동을 하고 있지는 않은 것으로 추정된다.



[그림 3-14] VirusTotal에 확인해본 결과, api.wisemansupport.com을 악성 도메인으로 판단한 백신 엔진이 3개이다.



api.wisemansupport.com

Communicating Files ⓘ

Scanned	Detections	Type	Name
2021-01-14	54 / 68	Win32 EXE	vbscript.dll
2021-01-13	58 / 71	Win32 EXE	vbscript.dll
2021-01-13	52 / 65	Win32 EXE	vbscript.dll
2021-01-12	59 / 71	Win32 EXE	vbscript.dll
2021-01-12	57 / 70	Win32 EXE	vbscript.dll
2021-01-12	57 / 70	Win32 EXE	vbscript.dll
2021-01-12	59 / 71	Win32 EXE	vbscript.dll
2021-01-12	55 / 70	Win32 EXE	vbscript.dll
2021-01-12	54 / 68	Win32 EXE	vbscript.dll
2021-01-13	51 / 71	Win32 EXE	vbscript.dll
2021-01-12	57 / 71	Win32 EXE	vbscript.dll
2021-01-12	59 / 71	Win32 EXE	vbscript.dll
2021-01-12	59 / 71	Win32 EXE	vbscript.dll
2021-01-12	58 / 70	Win32 EXE	vbscript.dll
2021-01-11	58 / 71	Win32 EXE	vbscript.dll
2021-01-11	56 / 68	Win32 EXE	vbscript.dll
2021-01-11	56 / 70	Win32 EXE	vbscript.dll
2021-01-11	58 / 70	Win32 EXE	vbscript.dll
2021-01-11	57 / 70	Win32 EXE	vbscript.dll
2021-01-11	56 / 70	Win32 EXE	vbscript.dll

[그림 3-15] api.wisemansupport.com이 교신하는 대부분의 파일이 악성코드로 판명되었다.

api.wisemansupport.com		Q	↑	☰	💬	Sign in	Si
Files Referring ⓘ							
Scanned	Detections	Type	Name				
2021-01-14	53 / 70	Win32 EXE	Korea Contents Network				
2020-12-18	52 / 71	Win32 EXE	wiseman.exe				
2020-12-17	52 / 71	Win32 EXE	wiseman.exe				
2020-12-07	49 / 69	Win32 EXE	wiseman				
2020-11-09	41 / 72	Win32 EXE	WisemanUpdate				
2020-10-31	49 / 72	Win32 EXE	Wiseman.exe				
2020-10-17	49 / 70	Win32 EXE	WisemanUpdate				
2020-10-03	49 / 68	Win32 EXE	Wiseman.exe				
2020-09-12	48 / 68	Win32 EXE	200.exe				
2020-08-20	43 / 66	Win32 EXE	Korea Contents Network				
2020-12-24	2 / 60	Text	da8163d47c95443c4f71dd36bcadea7e2a692fd171f84694249f35d2cf319ca3				
2021-01-06	6 / 70	Win32 EXE	MCleanup ToolKit				
2020-12-04	4 / 58	Text	cfe51af4e2085ef4f48ae215cee25c8f612fec83e2ad3bfff99227dfbfe19d8fc				
2021-01-06	18 / 69	Win32 EXE	AntiMalwarePro.exe				
2021-01-06	28 / 67	Win32 EXE	PC Cleaner.exe				
2020-12-11	3 / 71	Win32 EXE	MSecure DenyWall Total Security 360				
2020-08-21	1 / 58	Text	1266d8f2626505baacea965d194b38b473cfad404d51eb6ebea4197418ca30fd				
2021-01-14	4 / 59	Text	320bd65bf9b5533749f2de4d39a1978fdd56ace51dd386a667d3302a1b5a6a0				
2020-10-03	1 / 54	unknown	file-6824164_				
2020-07-24	3 / 59	Text	8f3e2755abe08fbbba1e1008e6093cb8f3fd4736c1e29c5aa47256f424c51502a				

[그림 3-16] api.wisemansupport.com이 포함하는 대부분의 파일 또한 악성코드로 판명되었다. 따라서 이 도메인은 악성 활동을 할 가능성이 높은 것으로 추정된다.

api.wisemansupport.com과 교신하는, 또는 포함하는 대부분의 파일이 많은 백신 엔진에서 악성코드로 판명되었다.

따라서 실행 시에 api.wisemansupport.com와 네트워크 활동을 하는 dgrep.exe는 악성 활동을 한다고 추측할 수 있다.

결론

본 악성코드는 다음 특징을 통하여 **백도어/트로이목마**로 분류할 수 있다.

- 패키징이 되어 있어 언패킹하지 않으면 파일의 정보를 알 수 없다.
- 실행 시 악성코드 파일의 아이콘이 사라지고, 악성코드를 실행하여 생성된 폴더도 숨김 처리되어 사용자가 찾을 수 없도록 한다.
- 컴퓨터를 재부팅하면 악성코드가 자동으로 실행된다.
- 악성코드 파일 및 악성코드 실행 시에 신규 생성된 파일의 퍼블리셔가 Microsoft사로 되어 있어 안전한 파일인 것처럼 사용자를 속인다. (사회공학적 기법)
- 악성 파일들을 포함한 홈페이지와 교신하여 악성 활동을 했던 것으로 추정되나, 현재는 활성화되어 있지 않은 상태이다.

유형	특징
바이러스	감염대상이 되는 프로그램 또는 코드를 감염시키므로 숙주가 필요
웜	실행 시 파일이나 코드를 네트워크와 전자우편 등을 통해 다른 시스템으로 자기 복제
트로이목마	정상적인 일반 파일인 것처럼 클릭을 유도하여 악의적 기능을 수행
기타	<ul style="list-style-type: none"> - 스파이웨어 (Spyware) : 사용자의 동의 없이 설치되어 정보 유출 등 악의적 행동 - 애드웨어 (Adware) : 사용자의 동의를 구하고, 광고를 목적으로 실행됨 - 백도어 : 해커가 해킹한 서버에 다시 쉽게 접근하기 위해 뒷문을 만드는 것으로, 여기에 트로이목마가 포함됨

[표 4-1] 악성코드의 유형별 특징

	자기 복제	감염 대상	형태	복구 방법
바이러스	O	O	기생/겹침	치료
트로이목마	X	X	독립	삭제
웜	O	X	독립	삭제

[표 4-2] 주요 악성코드 유형 3가지의 특징별 비교

대응 방안

본 악성코드는 백도어/트로이목마로 추정되어 감염된 컴퓨터를 복구하기 위해서는 악성코드를 삭제하여야 한다.
그러나 실행될 시에 파일 아이콘이 삭제되므로 찾기 쉽지 않아 예방이 중요하다.

본 악성코드 예방법으로 다음이 권장된다.

- 1) OS와 인터넷 방화벽 활성화
- 2) 신뢰할 수 없는 EXE파일 다운로드 및 실행 금지
- 3) 백신으로 탐지하여 삭제 (보편적으로 알려진 바이러스이므로 AhnLab-V3를 비롯한 *대부분의 백신으로 예방이 가능하다.)

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY 1
Acronis	Suspicious			Ad-Aware
AegisLab	Hacktool.Win32.PePatch.mDXT			AhnLab-V3
Alibaba	Backdoor:Win32/PePatch.f631d386			ALYac
Antiy-AVL	Trojan[Packed]/Win32.PePatch			SecureAge APEX
Arcabit	Trojan.Heur.EE0DAA			Avast
AVG	Win32:Malware-gen			Avira (no cloud)
BitDefender	Gen:Trojan.Heur.nqQ@zebyvHki			BitDefenderTheta
				Gen:Trojan.Heur.nqQ@zebyvHki
				Backdoor/Win32.Venik.C1070871
				Gen:Trojan.Heur.nqQ@zebyvHki
				Malicious
				Win32:Malware-gen
				TR/Crypt.XPACK.Gen2
				AI:Packers.74FD22BB1C

[그림 4-1] VirusTotal에서 악성코드 dgrep.exe를 탐지할 수 있는 백신을 보여준다

* 기초분석 사이트인 VirusTotal 사용 결과, 71개 중 62개의 백신 엔진이 악성코드로 분류하였다.

* 미탐 백신 엔진 : Baidu, CMC, Malwarebytes, TACHYON, Zoner, TotalDefense, SUPERAntiSpyware, Cyren, CAT-QuickHeal