

AI LAB

악성 코드 분석 보고서

dgrep.exe

박주형

2020-3-27

목차

1. 개요	2
1-1. 개요	2
1-2. 파일 정보.....	2
1-3. 분석환경	2
1-4. 분석 도구.....	3
2. 기초 분석(Virustotal)	4
3. 정적 분석.....	5
3-1. 패킹여부 확인 (Exeinfo PE, GuNPACKer)	5
3-2. 문자열 확인 (Bintext).....	6
4. 동적 분석.....	7
4-1. 파일 실행.....	7
4-2. 프로세스 변화 확인 (Process Explorer).....	9
4-3. 파일 및 레지스트리 변화 확인 (autoruns, Process Monitor, System Explorer)	9
4-4. 네트워크 변화 확인 (TCPview, Wireshark)	11
5. 결론.....	12
6. 대응 방안.....	13

1. 개요

1-1. 개요

악성코드 파일로 의심되는 dgrep.exe 파일을 분석하여 결론 및 대응방안을 모색했습니다. 1-2.

파일 정보

구분		내용
파일 이름		dgrep.exe
생성 날짜		2015-10-09 03:43:26
파일 형식		Win32.exe
파일 크기		215.05 KB
해시값 ¹	MD5	68af0599e74d36bc2f39a2710754082c
	SHA-1	c63f22e2d6feecbe9801c76a76f81589bce1b9a3
	SHA-256 ²	d3e4a46b95a3a54c762f0e1696e9167528bd1cf30b190e4893b44f0259e7893c
1-3. 분석환경 (V3)가상환경 : VMware Workstation 15.5		Backdoor ³ /Win32.Venik.C1070871
출처 OS : Windows7 64bit		리팩토링스터디

¹해시값 : 해당 파일의 고유한 값.

²MD5, SHA - 1, SHA - 256 : 해시 함수

³Backdoor : 정상적인 인증 절차를 거치지 않고, 컴퓨터와 암호 시스템 등에 접근할 수 있도록 하는 장치

1-4. 분석 도구

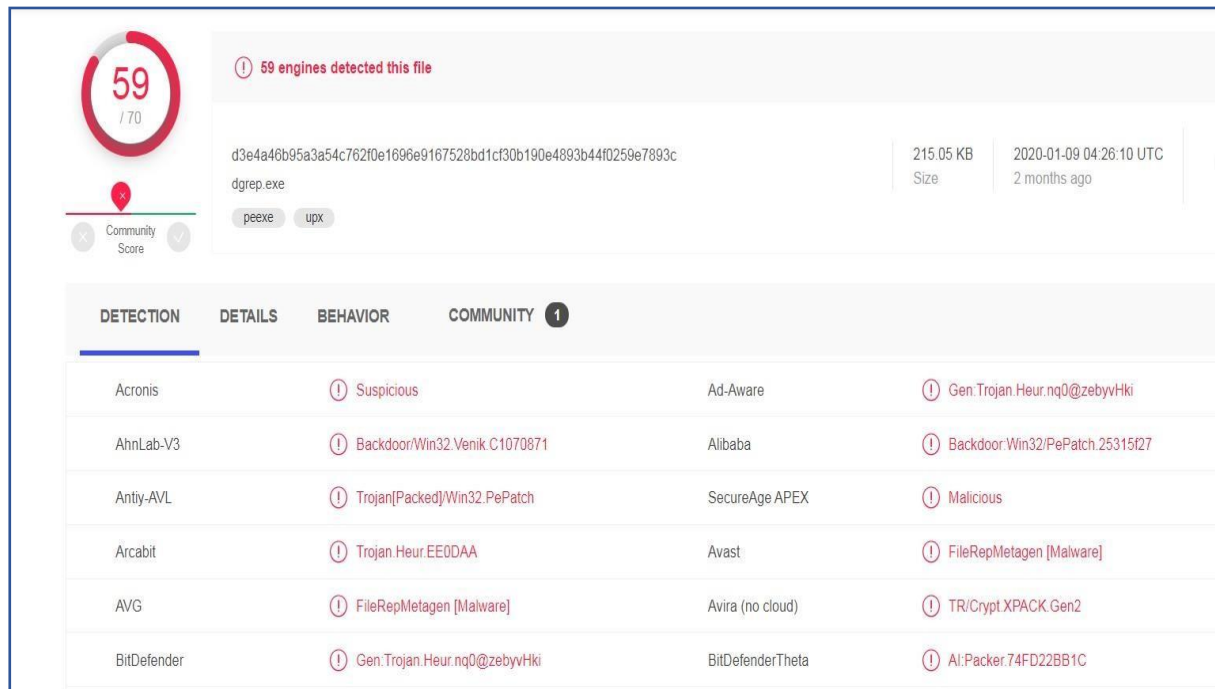
구분	Tool	내용
기초분석	VirusTotal	파일 검사 사이트
정적분석	Exeinfo PE	패킹 여부 확인
	GUnPacker	언패킹 도구
	Bintext	악성코드 문자열 확인
동적분석	Process Explorer,	프로세스 모니터링
	Process Monitor	실시간 레지스트리 변화 모니터링
	autoruns	윈도우 시작 프로그램 분석
	System Explorer	파일과 레지스트리 ⁴ 변화 비교 가능
	TCPview	실시간 네트워크 연결 분석
	Wireshark	네트워크 트래픽 ⁵ 및 패킷 ⁶ 분석

⁴ 레지스트리 : 윈도우계열 시스템에서 사용하는 시스템 구성 정보를 저장한 데이터베이스를 말한다.

⁵ 트래픽 : 서버와 스위치 등 네트워크 장치에서 일정 시간 내에 흐르는 데이터의 양

⁶ 패킷 : 데이터를 일정 크기로 자른 것

2. 기초 분석(Virustotal)



[그림 1] Virustotal 검사 결과

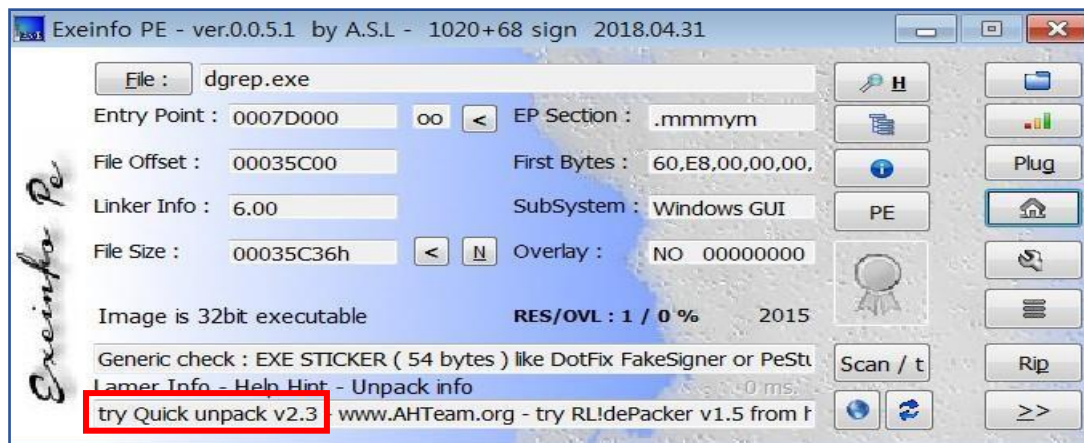
dgrep.exe 파일을 Virustotal에 업로드 하여 검사한 결과, 59개의 백신 엔진에서 악성코드로 진단했다. 진단명은 Backdoor, Trojan⁷등으로 해당 유형의 행동을 할 것으로 예상된다.

⁷Trojan : 유용한 프로그램으로 가장하여 사용자가 그 프로그램을 실행하도록 속이는 악성 코드로 트로이 목마라고 부른다.

3. 정적 분석

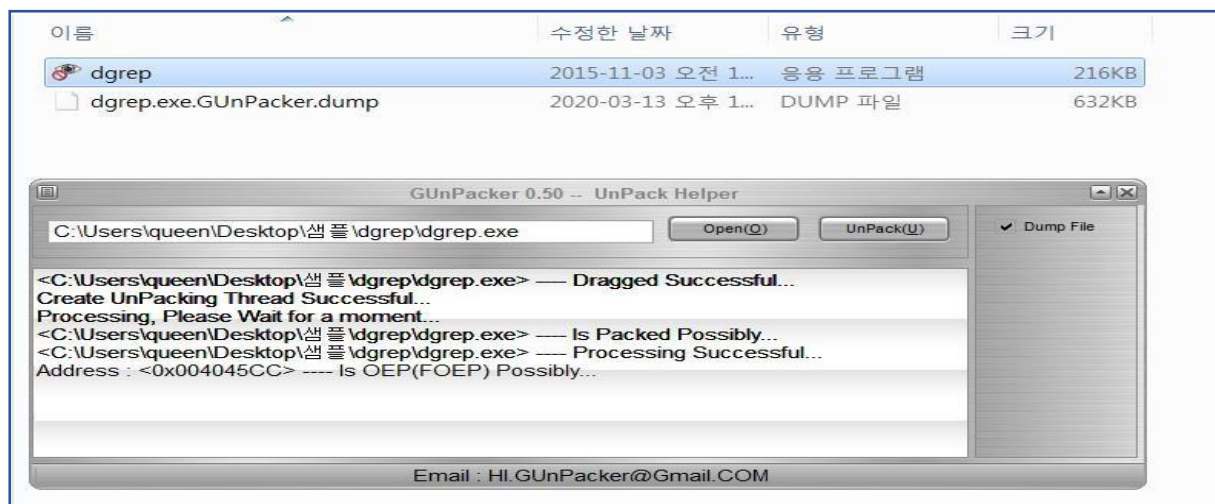
3-1. 패킹⁸여부 확인 (Exeinfo PE, GuNPACKer)

파일이 패킹 되어 있을 경우 문자열이나 함수 등이 난독화 되어 있어 분석하는데 어려움이 있다. 그렇기 때문에 악성코드 파일의 패킹 여부를 먼저 확인해야 한다. 그 후 패킹 되어 있는 파일의 경우 언패킹 해주어야 한다.



[그림 2-1] Exeinfo PE 검사 결과

[그림 2-1]은 Exeinfo PE에 파일을 업로드 한 결과이다. dgrep.exe는 패킹 되어 있는 파일임을 확인할 수 있다.



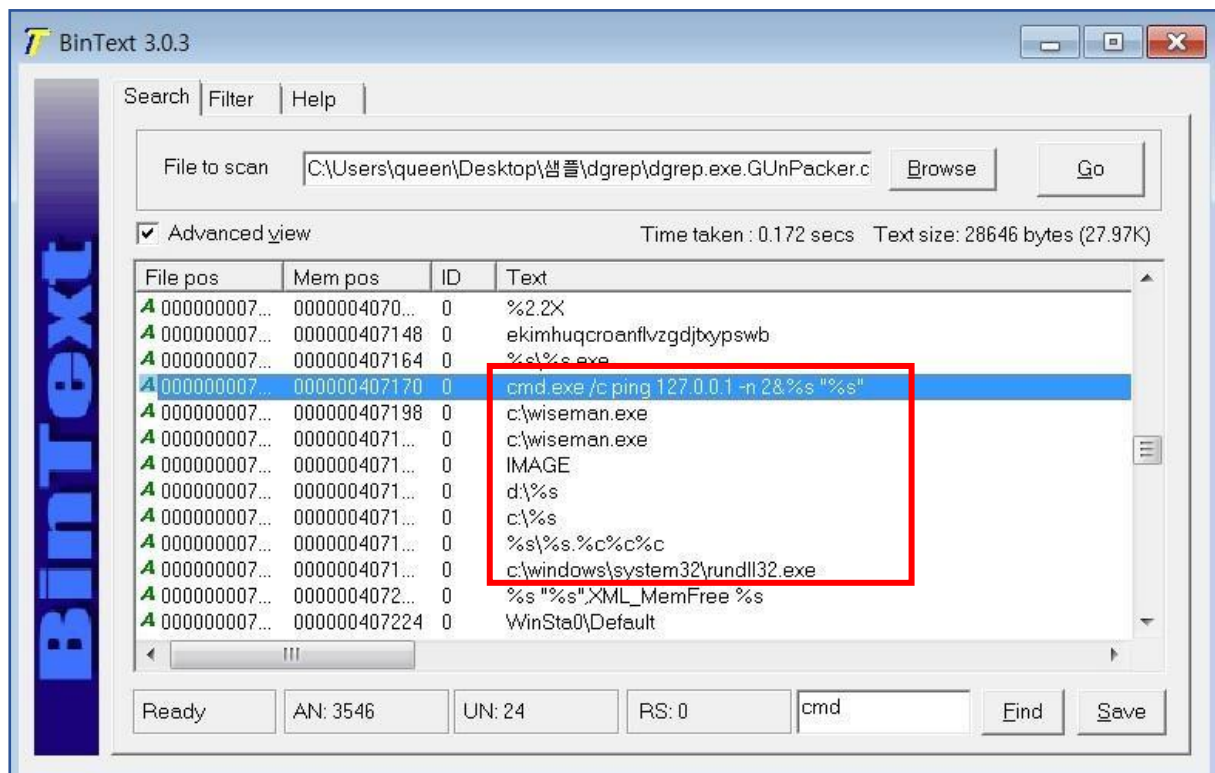
[그림 2-2] GUNPacker로 언패킹 한 결과

GUNPacker를 사용하여 패킹을 풀어주고 덤프 파일을 생성하였다.

⁸ 패킹 : 실행파일을 암호화하거나, 압축하여 소스코드를 볼 수 없도록 하는 것

3-2. 문자열 확인 (Bintext)

파일의 내부 문자열 확인을 통해 파일이 실행되면 어떠한 행동을 하는 지 유추할 수 있다.



[그림 3] Bintext 문자열

[그림 3]을 Bintext를 통해 내부 문자열을 확인한 결과이다.

- (가) cmd.exe /c ping 127.0.0.1 : 커맨드 창을 켜 ping을 보내 네트워크 연결 확인을 한다. 네트워크 연결을 시도할 것으로 추정된다.
- (나) C:\wiseman.exe : C 드라이브에 wiseman.exe 파일을 다운로드 할 것으로 추정된다.
- (다) C:\windows\system32\rundll32.exe : 해당 경로에 rundll32.exe⁹파일을 설치하거나 실행할 것으로 추정된다.

⁹ rundll32.exe : 실행파일(.exe)이 실행되면, 그 실행파일이 필요로 하는 DLL 파일을 찾아서 실행파일과 연결을 시켜주는 역할을 한다

4. 동적 분석

4-1. 파일 실행

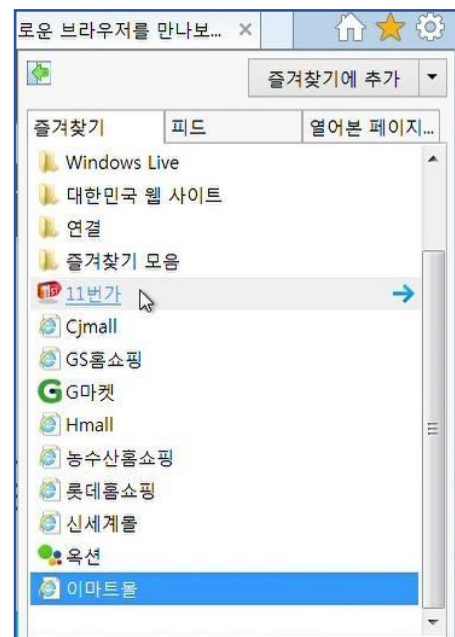
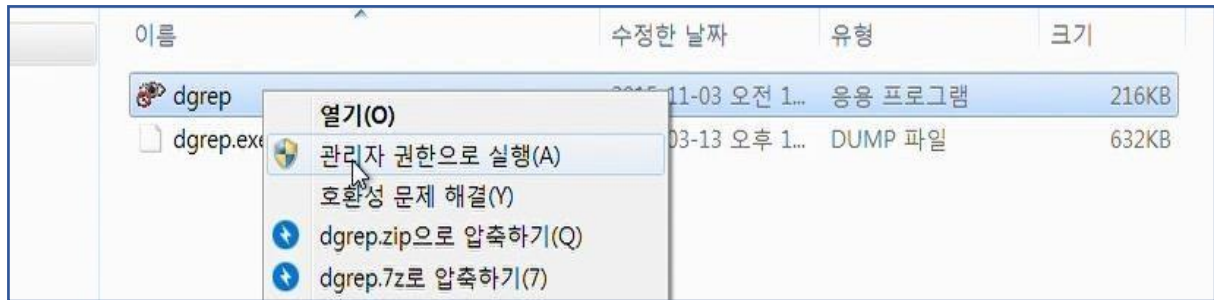
이름	수정한 날짜	유형	크기
dgrep	2015-11-03 오전 1...	응용 프로그램	216KB
dgrep.exe.GUnPacker.dump	2020-03-13 오후 1...	DUMP 파일	632KB



이름	수정한 날짜	유형	크기
dgrep.exe.GUnPacker.dump	2020-03-13 오후 1...	DUMP 파일	632KB

[그림 4] 파일 실행 후

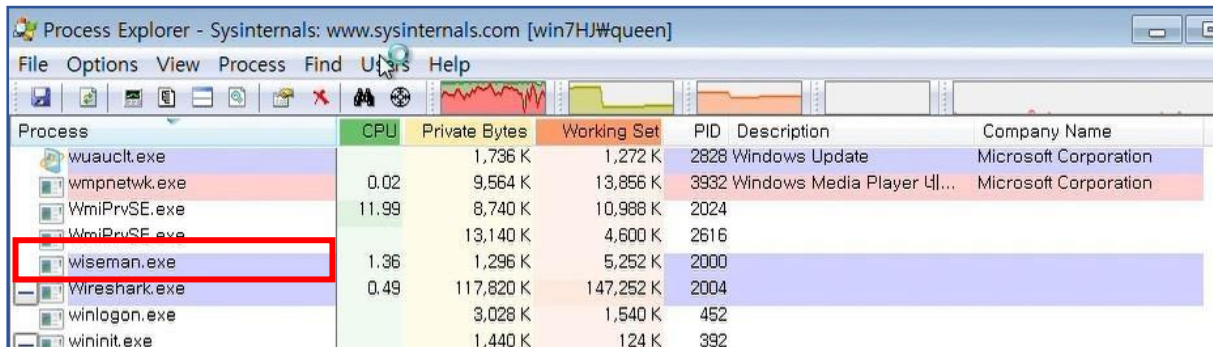
일반 사용자 권한으로 실행 시 파일이 사라지는 것 외에는 특별한 변화를 찾아볼 수 없었다.



[그림 5] 관리자 권한으로 실행

관리자 권한으로 실행 시 dgreg.exe파일이 사라지고 바탕화면에 바로가기 아이콘이 생성되었다. 또한 즐겨찾기에 다양한 쇼핑물들이 추가되었다.

4-2. 프로세스 변화 확인 (Process Explorer)

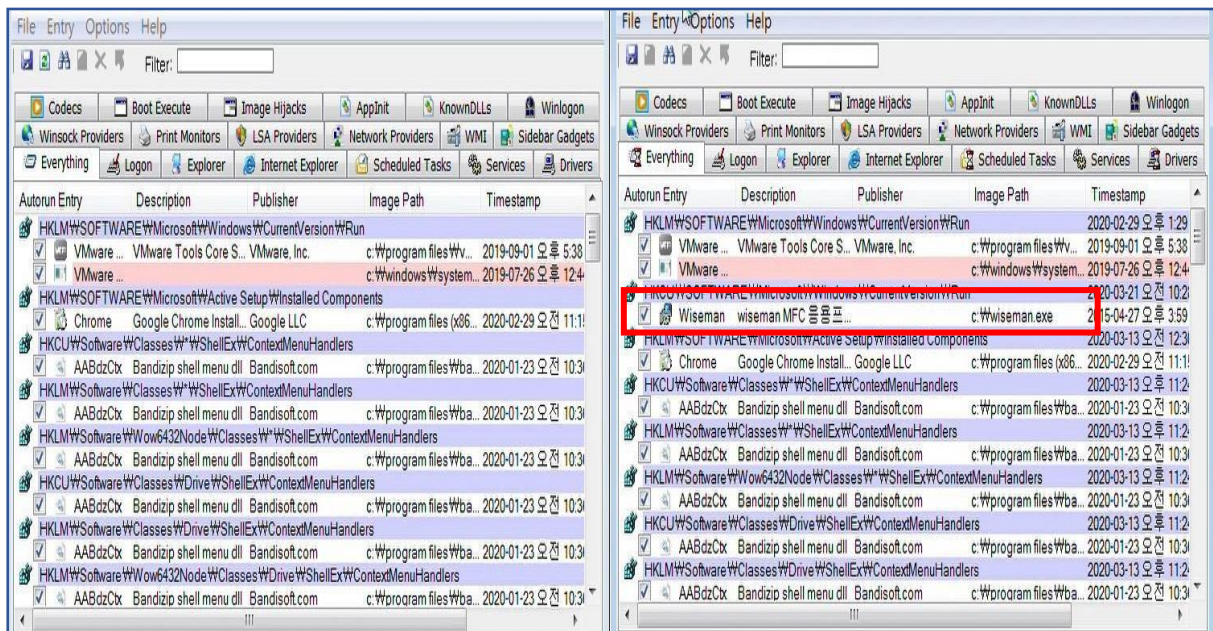


Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
wuauclt.exe		1,736 K	1,272 K	2828	Windows Update	Microsoft Corporation
wmpnetwk.exe	0.02	9,564 K	13,856 K	3932	Windows Media Player Network...	Microsoft Corporation
WmiPrvSE.exe	11.99	8,740 K	10,988 K	2024		
WmiPrvSE.exe		13,140 K	4,600 K	2616		
wiseman.exe	1.36	1,296 K	5,252 K	2000		
Wireshark.exe	0.49	117,820 K	147,252 K	2004		
winlogon.exe		3,028 K	1,540 K	452		
wininit.exe		1,440 K	124 K	392		

[그림 6] Process Explorer 분석 결과

[그림 6]은 dgrep.exe 파일을 관리자 권한으로 실행 후 Process Explorer로 확인한 프로세스 변화이다. wiseman.exe 프로세스가 생성되었다.

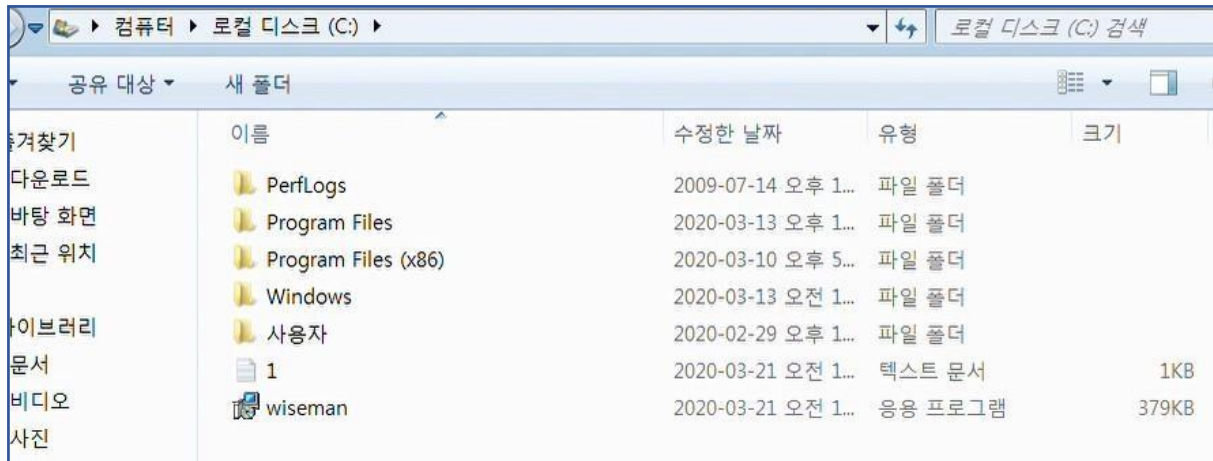
4-3. 파일 및 레지스트리 변화 확인 (autoruns, Process Monitor, System Explorer)



Autorun Entry	Description	Publisher	Image Path	Timestamp
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2020-02-29 오후 1:29
VMware ...	VMware Tools Core S...	VMware, Inc.	c:\program files\Wv...	2019-09-01 오후 5:38
VMware ...			c:\windows\system...	2019-07-26 오후 12:4
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				2020-03-21 오전 10:2
Chrome	Google Chrome Install...	Google LLC	c:\program files (x86...	2020-02-29 오전 11:1
HKCU\Software\Classes*\ShellEx\ContextMenuHandlers				2020-03-13 오전 12:3
AABdzCtx	Bandizip shell menu dll	Bandisoft.com	c:\program files\Wba...	2020-01-23 오전 10:3
HKLM\Software\Classes*\ShellEx\ContextMenuHandlers				2020-03-13 오후 11:2
AABdzCtx	Bandizip shell menu dll	Bandisoft.com	c:\program files\Wba...	2020-01-23 오전 10:3
HKLM\Software\Wow6432Node\Classes*\ShellEx\ContextMenuHandlers				2020-03-13 오전 11:2
AABdzCtx	Bandizip shell menu dll	Bandisoft.com	c:\program files\Wba...	2020-01-23 오전 10:3
HKCU\Software\Classes\Drive\ShellEx\ContextMenuHandlers				2020-03-13 오전 11:2
AABdzCtx	Bandizip shell menu dll	Bandisoft.com	c:\program files\Wba...	2020-01-23 오전 10:3
HKLM\Software\Classes\Drive\ShellEx\ContextMenuHandlers				2020-03-13 오전 11:2
AABdzCtx	Bandizip shell menu dll	Bandisoft.com	c:\program files\Wba...	2020-01-23 오전 10:3
Wiseman	wiseman MFC 응용 프...		c:\wiseman.exe	2020-04-27 오후 3:59

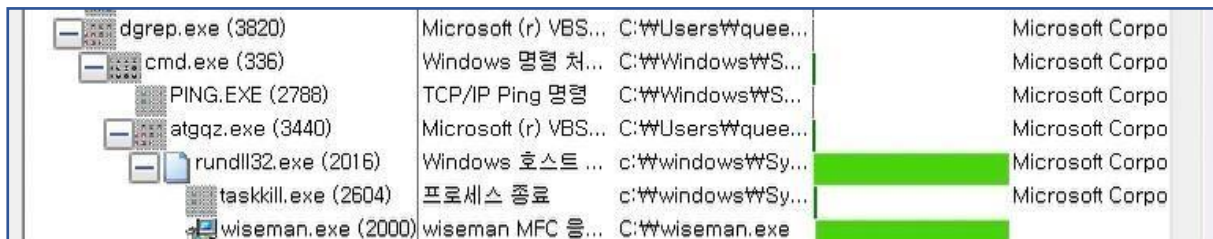
[그림 7] autoruns 분석 결과

[그림 7]의 왼쪽은 파일 실행 전이며 오른쪽은 관리자 권한으로 실행한 후의 이미지이다. Wiseman.exe 파일이 해당 경로에 생성되었다.



[그림 8] 관리자 권한으로 실행 후 c
드라이브

[그림 8]은 dgrep.exe 파일을 관리자 권한으로 실행 후의 c드라이브이다. Wiseman.exe 파일이 생성된 것을 볼 수 있다.



[그림 9] Process Monitor 분석 결과

[그림 9]는 dgrep.exe 파일을 관리자 권한으로 실행 후 Process Monitor에 Process Tree이다. (가)

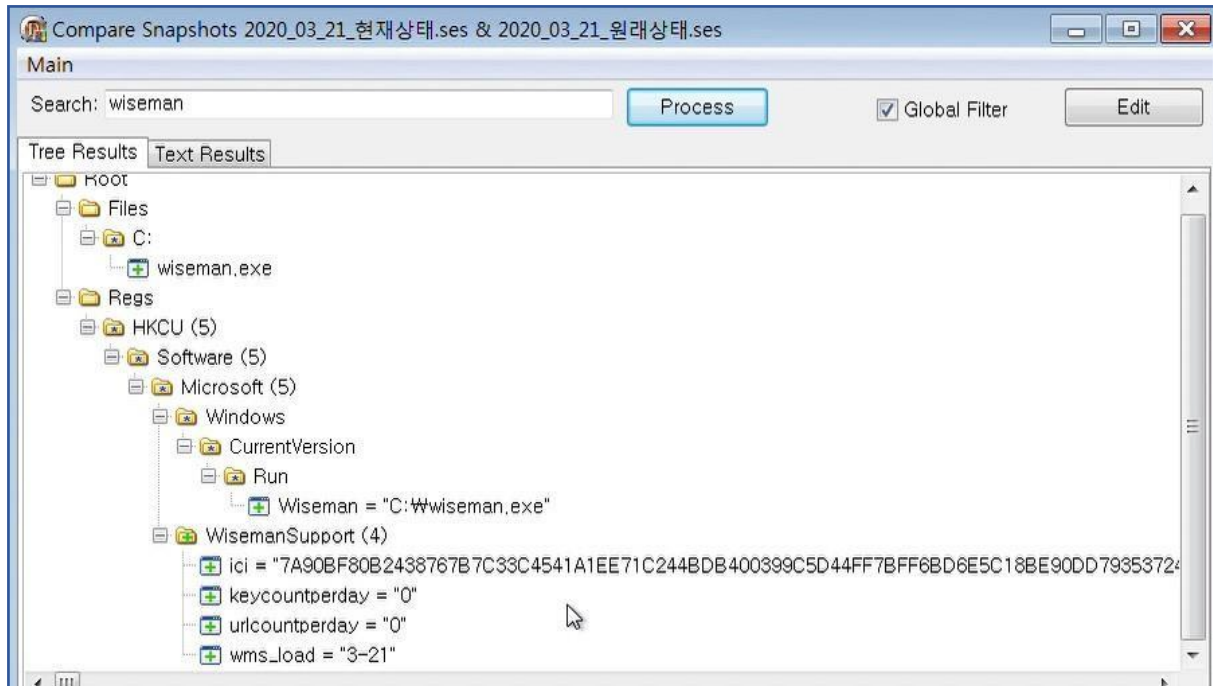
dgrep.exe 실행 후 cmd.exe를 생성한다.

(나) cmd.exe 하위에 PING.EXE를 생성한다. Ping¹⁰을 보내 네트워크 연결을 시도한 것으로 추정된다.

(다) 임의의 파일 atgqz.exe 생성 후 하위에 rundll32.exe 파일을 생성한다.

(라) Rundll32.exe 파일에 하위에 taskkill.exe와 wiseman.exe를 생성한다. taskkill.exe는 자동 종료 도구로, 파일 실행 후 이 프로세스를 이용해 자동으로 삭제된 것으로 추정된다. rundll32.exe는 공유된 dll 파일에 저장된 기능을 실행하기 위해 사용되는데 wiseman.exe 파일 실행을 도와줄 것으로 추정된다.

¹⁰ Ping : IP 네트워크를 통해 특정한 호스트가 도달할 수 있는지 여부를 테스트하는 데 쓰인다.



[그림 10] System Explorer 분석결과

[그림 10]은 관리자 권한으로 파일 실행 전과 후에 system explorer 분석 결과를 비교한 것이다. C 드라이브에 wiseman.exe파일이 생성된 것을 볼 수 있다. 레지스트리 Run¹¹키에 wiseman이 추가 된 것을 볼 수 있다. 윈도우 다시 시작 시 Wiseman.exe도 자동으로 실행될 것으로 추측된다. 그 외에 wiseman레지스트리들이 추가된 것을 볼 수 있다.

4-4. 네트워크 변화 확인 (TCPview, Wireshark)

System	4	UDP	win7hj.locald...	netbios-ns	*	*		121	6,770
System	4	UDP	win7hj.locald...	netbios-dgm	*	*		12	2,226
wininit.exe	392	TCP	win7HJ	49152	win7HJ	0	LISTENING		
wininit.exe	392	TCPV6	win7HJ	49152	win7HJ	0	LISTENING		
wiseman.exe	2000	TCP	win7hj.locald...	49216	211.110.207.188	http	ESTABLISHED	1	113
wiseman.exe	2000	TCP	win7hj.locald...	49216	211.110.207.188	http	ESTABLISHED	1	113
wmpnetw...	3932	TCP	win7HJ	rtsp	win7HJ	0	LISTENING		
wmpnetw...	3932	UDP	win7HJ	5004	*	*			
wmpnetw...	3932	UDP	win7HJ	5005	*	*			
wmpnetw...	3932	TCPV6	win7HJ	rtsp	win7HJ	0	LISTENING		

[그림 11] TCPview 분석 결과

[그림 11]은 관리자 권한으로 파일 실행 후 TCPview로 본 네트워크 변화이다. 특정 ip(211.110.207.188)에 연결하는 것을 볼 수 있다.

¹¹ Run: Run 키에 등록된 파일은 Windows OS 가 시작할 때 자동으로 실행된다.

No.	Time	Source	Destination	Protocol	Length	Info
7919	451.100194	211.110.207.188	192.168.175.128	HTTP	951	HTTP/1.1 200 OK (text/html)
7921	451.102405	192.168.175.128	211.110.207.188	HTTP	140	GET /wms/bc.php?pid=defapp&mac=000c29b10432 HTTP/1.1
7926	451.125269	211.110.207.188	192.168.175.128	HTTP	838	HTTP/1.1 200 OK (text/html)
7928	451.137194	192.168.175.128	211.110.207.188	HTTP	167	GET /wms/ico/auction.ico HTTP/1.1
7975	452.491066	211.110.207.188	192.168.175.128	HTTP	1141	HTTP/1.1 200 OK (image/x-icon)
8016	456.244215	192.168.175.128	211.110.207.188	HTTP	164	GET /wms/ico/11st.ico HTTP/1.1
8025	456.263024	192.168.175.128	211.110.207.188	HTTP	164	GET /wms/ico/11st.ico HTTP/1.1
8046	456.320000	211.110.207.188	192.168.175.128	HTTP	453	HTTP/1.1 200 OK (image/x-icon)
8048	457.022967	192.168.175.128	152.195.11.6	HTTP	402	GET /c/msdownload/update/software/secu/2017/11/windows6.1-kb4054518-x64_8bc38e3ac0bf6d5c5a90cff6ee5bb6255...
8064	457.209746	152.195.11.6	192.168.175.128	HTTP	1380	HTTP/1.1 206 Partial Content
8128	464.413025	192.168.175.128	211.110.207.188	HTTP	167	GET /wms/ico/gmarket.ico HTTP/1.1
8158	466.006475	211.110.207.188	192.168.175.128	HTTP	1141	HTTP/1.1 200 OK (image/x-icon)
8168	468.932887	192.168.175.128	211.110.207.188	HTTP	141	GET /wms/upd.php?pid=defapp&cid=000c29b10432 HTTP/1.1
8178	468.951974	211.110.207.188	192.168.175.128	HTTP	324	HTTP/1.1 200 OK (text/html)
8180	468.953281	192.168.175.128	211.110.207.188	HTTP	154	GET /wms/files/WisemanUpdate.exe HTTP/1.1
8182	468.961326	192.168.175.128	152.195.11.6	HTTP	402	GET /c/msdownload/update/software/secu/2017/11/windows6.1-kb4054518-x64_8bc38e3ac0bf6d5c5a90cff6ee5bb6255...
8210	469.611339	152.195.11.6	192.168.175.128	HTTP	1168	HTTP/1.1 206 Partial Content

[그림 12] Wireshark 분석 결과

[그림 12]는 파일을 관리자 권한으로 실행한 후 네트워크 패킷 분석 결과이다. 특정 ip(211.110.207.188)주소와 통신이 오고 간 것을 볼 수 있다. GET 메소드를 사용하여 옥션, 11번 가, G마켓 아이콘을 생성할 것으로 추정된다. 또한 wisemanUpdate.exe를 생성하는 것을 보니 자동으로 업데이트 될 것으로 추정된다.

5. 결론

dgrep.exe파일은 패킹 되어 있는 파일이다. 관리자 권한으로 실행 시에 악성 행위를 하는 것으로 추정된다. 실행 후 dgrep.exe파일은 자동으로 삭제되었으며 바탕화면과 작업표시줄에 쇼핑몰 아 이콘이 생성되었다. 애드웨어¹² 기능이 있는 것으로 추정된다. 파일이 실행되면 cmd창을 켜 ping 을 보내 네트워크 연결을 시도한 후 wiseman.exe파일을 생성하는 것으로 추정된다. 또한 레지스 트리 run키에 wiseman.exe를 추가하여 윈도우가 시작할 때 wiseman.exe도 자동으로 실행될 것으 로 추정된다. wisemanUpdate.exe 파일도 생성하여 자동으로 업데이트 할 것으로 추정된다. 자동 으로 파일이 삭제되고 네트워크 연결 확인을 하는 등 원격 제어된 것을 보니 백도어, 트로이 목 마 성격을 띄고 있다.

따라서 dgrep.exe 파일은 트로이목마, 애드웨어, 백도어 유형의 악성코드 파일로 추정된다.

¹² 애드웨어 : 특정 소프트웨어를 실행할 때 또는 설치 후 자동적으로 광고가 표시되는 프로그램

6. 대응 방안

1. 신뢰할 수 없는 사이트는 이용하지 않는다.
2. 정기적으로 중요한 파일들은 백업해 놓는다.
3. 비정상적인 실행 파일이나 첨부 파일 실행을 금지한다.
4. 최신 버전의 백신 프로그램을 사용한다.