

악성코드 분석 보고서

-Drgep.exe-

2022-07-16

배준호

목차

1. 개요	3p
1-1. 개요	3p
1-2. 분석환경	3p
1-3. 파일정보	3p
2. 기초 분석(Virustotal)	4p
3. 정적 분석	5p
3-1. 패킹여부 확인 (Exeinfo PE)	5p
3-2. 패킹여부 확인 (PEiD)	5p
3-3. 언패킹 후 파일 확인 (GuNPACKer, PEiD)	6p
3-4. 문자열 확인 (Bintext)	7-8p
3-5. PE 구조 분석 (PEView)	9p
4. 동적 분석	10p
4-1. 파일 실행	10-11p
4-2. 프로세스 변화 확인	12p
4-3. 파일 및 레지스트리 변화 확인	13p
4-4. 네트워크 변화 확인	14p
5. 결론	15p
6. 대응 방안	16p

1.개요

1-1. 개요

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

1-2. 분석환경

구분	내용		
OS	Windows7		
Tools	정적분석 도구	Exeinfo PE, PEiD	패킹 여부 확인
		GunPacker	패킹 된 파일 언패킹
		BinText,	문자열 확인
		Pevview	pe구조 분석
	동적분석 도구	Process Explorer	프로세스 변화 확인
		Process monitor, Autoruns	레지스트리 변화 확인
		Currport	네트워크 변화 확인

[표1-1] OS와 악성코드 분석에 사용한 분석 툴

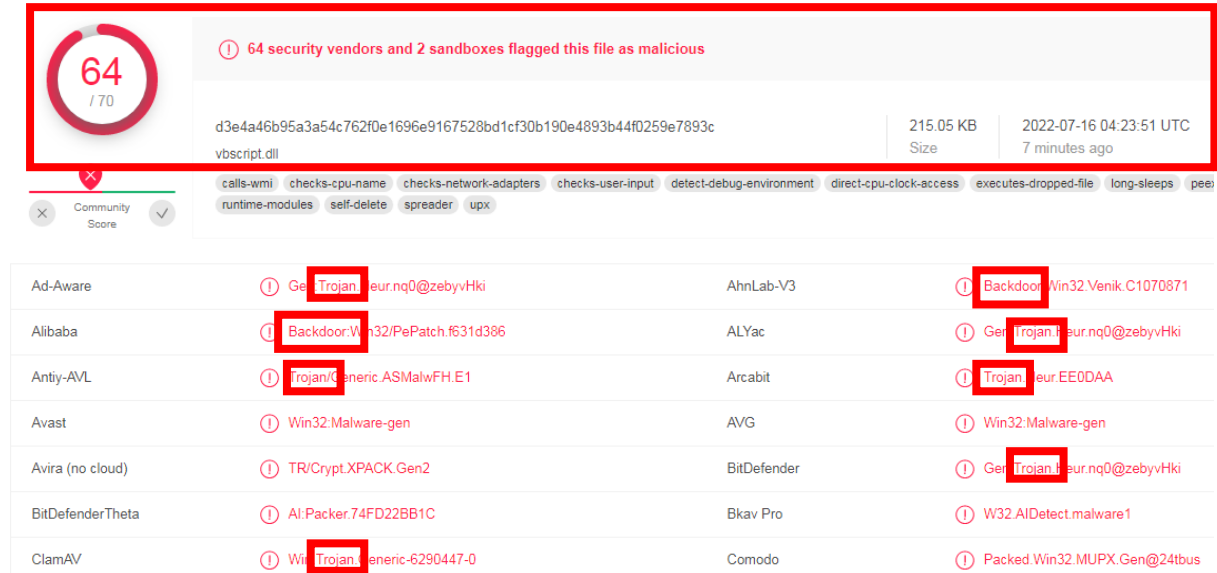
1-3.파일정보

구분	내용
파일명	Dgrep.exe
파일크기	215.05 KB (220214 bytes)
파일종류	Win32 EXE
생성시기	2015-10-09 03:43:26 UTC
MD5	68af0599e74d36bc2f39a2710754082c
SHA-1	c63f22e2d6feecbe9801c76a76f81589bce1b9a3
SHA-256	d3e4a46b95a3a54c762f0e1696e9167528bd1cf30b190e4893b44f0259e7893c
진단명	Adware.Agent.pvj
출처	리팩토링

[표1-2] 악성코드 정보

2. 기초분석

2-1. VirusTotal



[그림 2-1] VirusTotal을 이용한 파일 분석

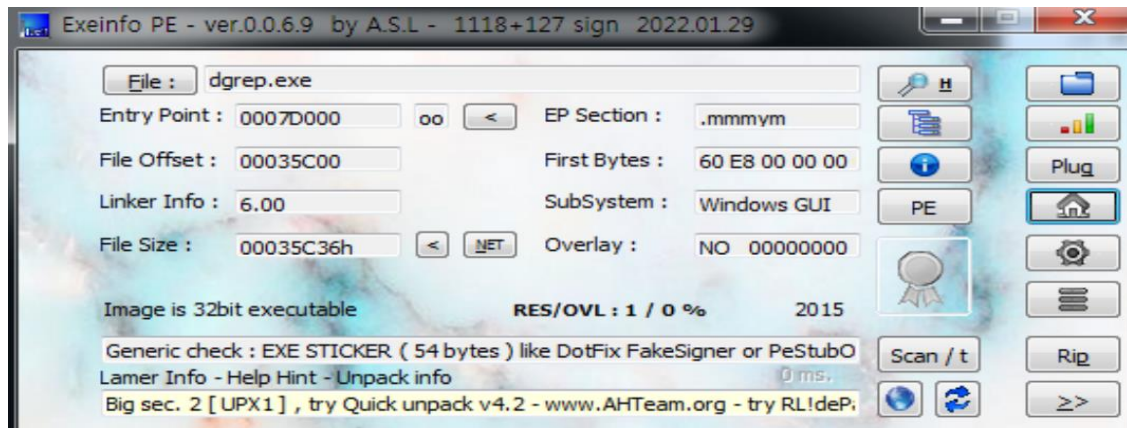
2022년 7월 16일 갱신 결과 70개 백신엔진 중 64개가 악성코드 의심파일임을 알 수 있다. 그 중 탐지 64개 중 25개가 *Trojan*¹이란 이름을 갖고 5개가 *Backdoor*²란 이름을 갖으므로 악성파일로 의심되는 파일이 트로이목마와 백도어의 성격을 가질 수 있다고 추측이 가능하다.

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

²Backdoor: 정상적인 인증 절차를 거치지 않고, 컴퓨터와 암호 시스템 등에 접근할 수 있도록 하는 장치

3. 정적분석

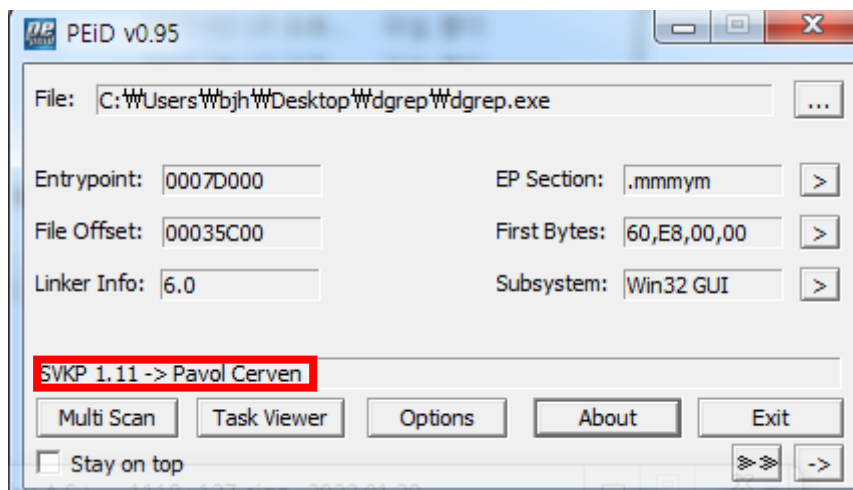
3-1. Exeinfo PE (패킹여부 확인)



[그림 3-1] Exeinfo PE 검사결과

[그림 3-1]을 보면 Exeinfo PE를 통하여 실행(EXE)파일의 ³패킹 여부를 확인한 결과 dgrep.exe 파일은 패킹된 파일임을 알 수 있다. 따라서 ⁴언패킹을 해야 한다.

3-2 PEiD (패킹여부 확인)



[그림 3-2] PEiD 검사결과

[그림 3-2]을 보면 ⁵프로텍터 종류가 SVKP로 패킹 되어 있다는 것을 알 수 있다.

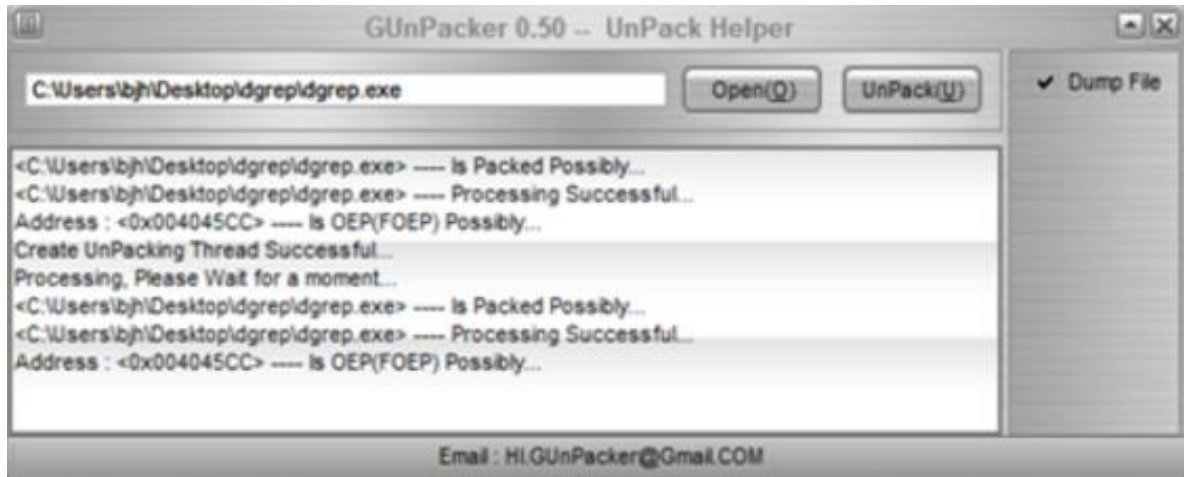
³패킹: 실행파일을 암호화하거나, 압축하여 소스코드를 볼 수 없도록 하는 것

⁴언패킹: 패킹 된 파일의 압축을 푸는 행위

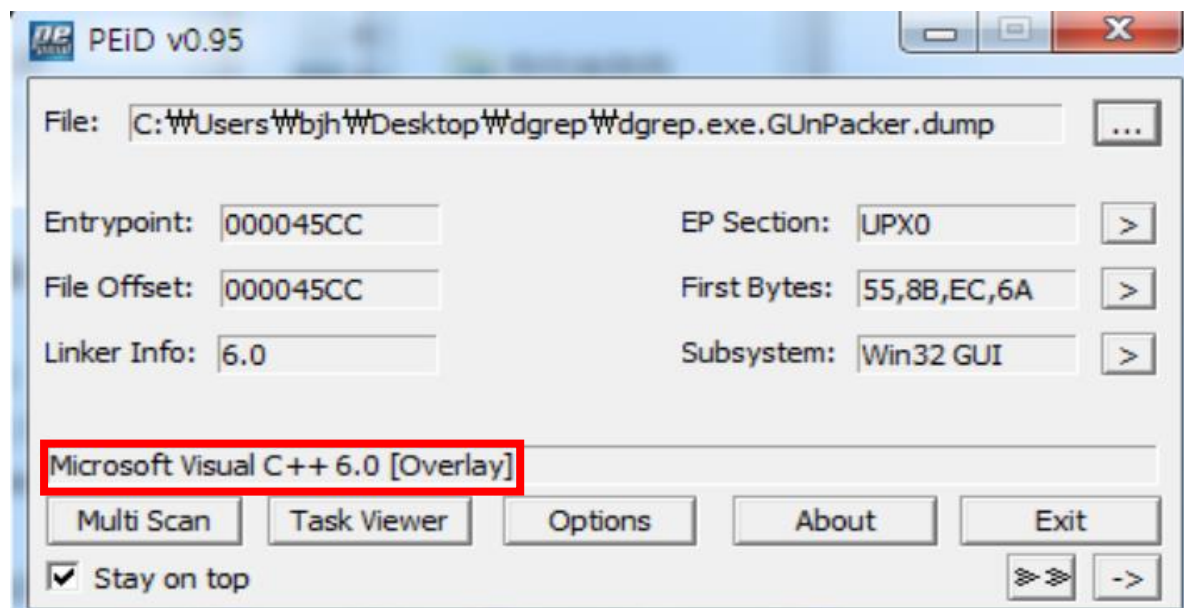
⁵프로텍터: PE 파일을 'Reverse Code Engineering'(분석) 으로부터 보호하기 위한 유틸리티

3-3. GUnPakcer 언패킹 후 파일 확인

GUnpacker 툴을 이용해 grep.exe 실행 파일을 언패킹 하여 덤프파일 생성



[그림 3-3] dgrep.exe 파일 언패킹 진행

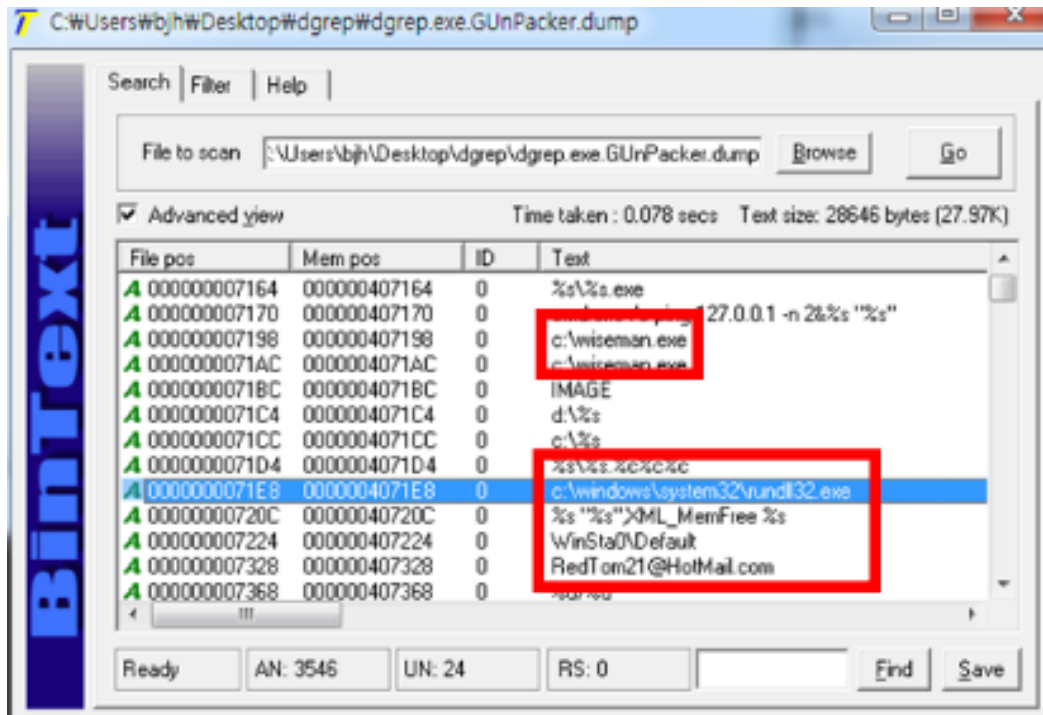


[그림 3-4] PEiD를 통해 언패킹 된 파일 확인

[그림 3-4]를 보면 PEiD를 통해 해당 파일이 언패킹 된 것을 확인할 수 있고 해당파일이 C++언어를 사용한 것을 알 수 있음

3-4. 문자열 확인 (BinText)

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

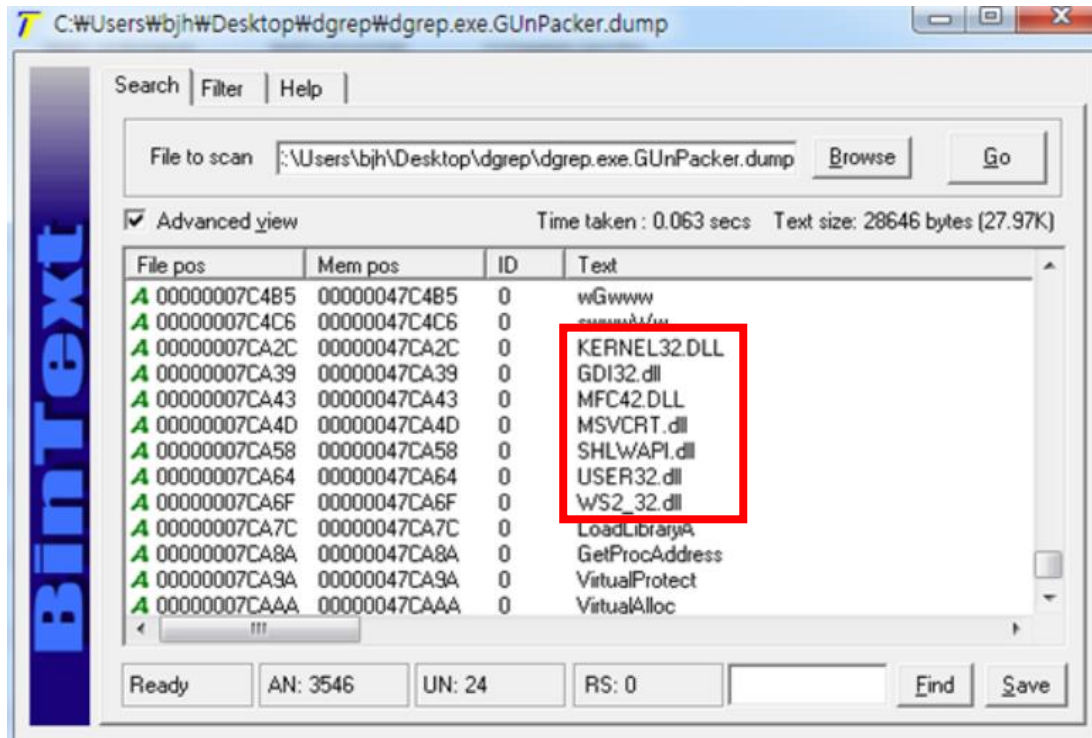


[그림 3-5] Bintext 문자열

다음은 [그림 3-5]를 통해 문자열을 분석한 결과이다.

- (가) cmd.exe /c ping 127.0.0.1: 명령 프롬프트를 실행시켜 해당 ip와 연결을 시도한 것으로 추정됨
- (나) c:\wiseman.exe: C드라이브에 wiseman.exe 파일을 다운받은 것으로 추정됨
- (다) c:\windows\system32\cmd.exe: 해당경로에 cmd.exe 파일을 설치하거나 실행한 것으로 추정됨
- (라) RedTom21@HotMail.com : 악성코드 배포자 혹은 제작자로 추정되는 이메일 확인

⁶rundll32.exe : 실행파일(.exe)이 실행되면, 그 실행파일이 필요로 하는 DLL 파일을 찾아서 실행파일과 연결을 시켜주는 역할을 한다.

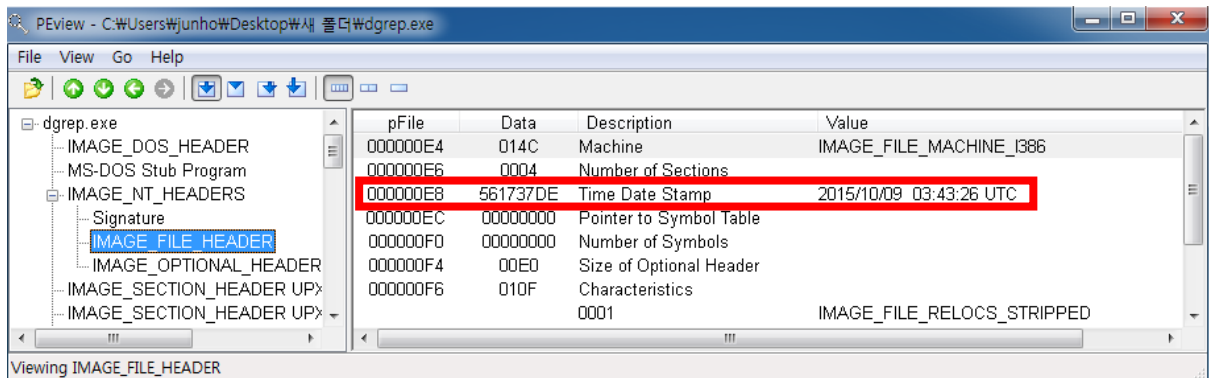


[그림 3-6] Bintext 문자열 DLL파일 확인

다음은 [그림 3-6]를 통해 알 수 있는 각 DLL파일의 설명이다.

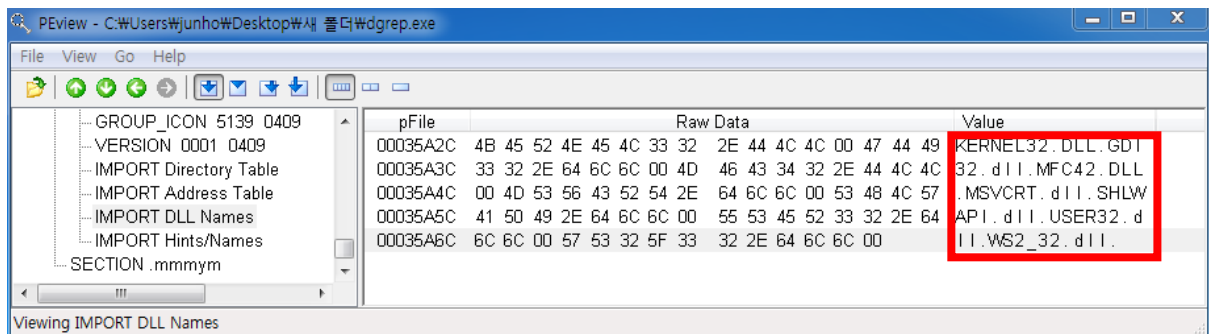
- (가) Kernel32.DLL: Windows XP (32 비트 및 64 비트), Vista 및 Windows 10, 8.1, 8, 7 용으로 설계된 32 비트 동적 링크 라이브러리
- (나) GDI32.DLL: 마우스 움직임, 그림, 화면, GUI의 기본이 된다.
- (다) MFC42.DLL: MFC (Microsoft Foundation Class Library)는 Windows 용 데스크톱 응용 프로그램을 개발하기 위한 C++ 개체 지향 라이브러리
- (라) MSVCRT.DLL: stdio.h, string.h, stdlib.h, etc등등 호출되지 않는 에러가 발생했을 때 실행
- (마) USER32.DLL: 윈도우 USER 구성 요소를 구현한다. 즉 프로그램들에게 그래픽 사용자 인터페이스 (GUI)를 구현할 수 있게 해준다
- (바) WS2_32.DLL: TCP/IP 네트워킹 기능을 제공하고 다른 네트워크 API와 부분적으로 깨진 호환성을 제공하는 Winsock API를 구현합니다

3-4. PE 구조 분석 (PEView)



[그림 3-7] IMAGE_FILE HEADER 분석 결과

PE 구조를 분석해주는 PEView를 통해서 Time Date Stamp를 통해 생성시기는 2015년 10월 9일라는 것을 알 수 있다.




[그림 3-8] IMPORT DLL Names 분석 결과

[그림 3-8]를 통해 Dgrep.exe의 DLL파일을 알 수 있다. (KERNEL32.dll / GDI32.dll / MFC42.dll / MSVCRT.dll / SHLWAPI.dll / USER32.dll / WS32.dll). 이는 BinText에서 나온 결과와 같은 것을 알 수 있다.

4. 동적분석

4-1 파일실행

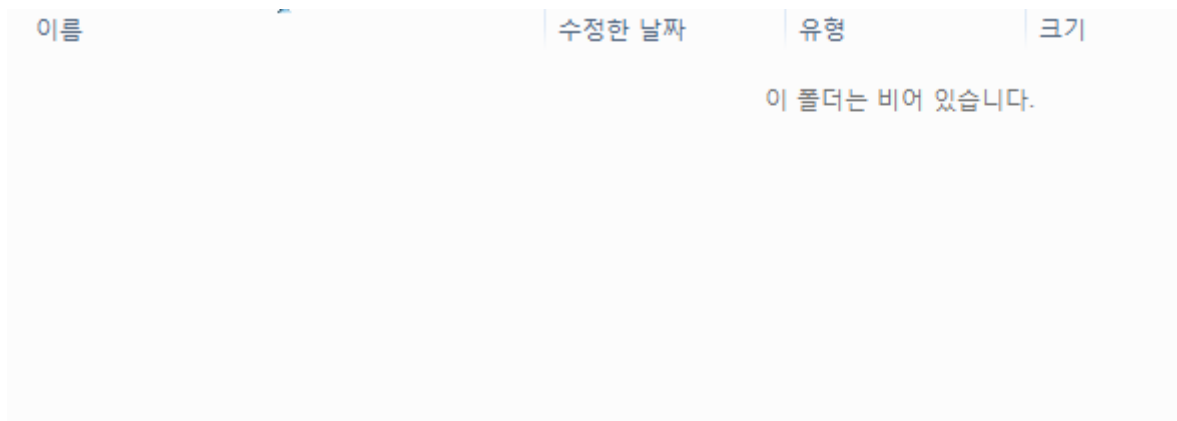
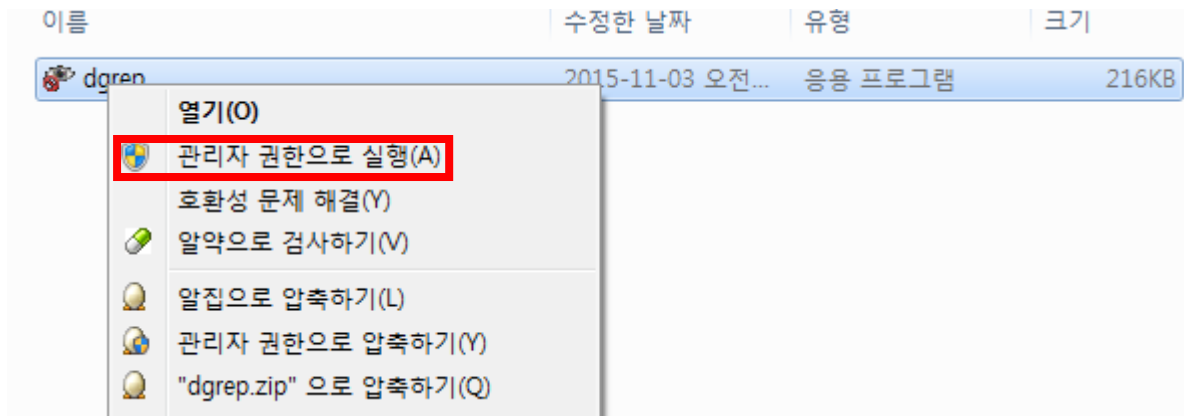
이름	수정한 날짜	유형	크기
 dgrep	2015-11-03 오전...	응용 프로그램	216KB



이름	수정한 날짜	유형	크기
이 폴더는 비어 있습니다.			

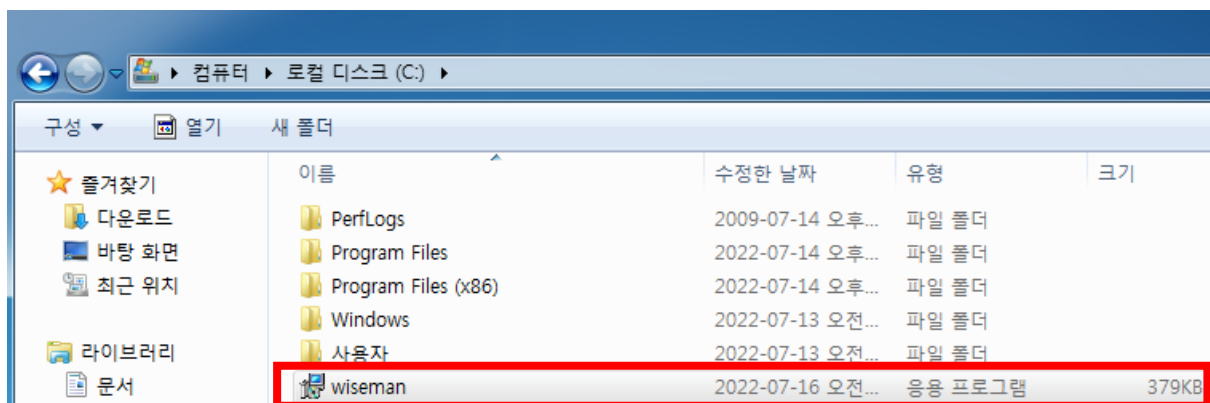
[그림 4-1] 파일 실행 전 후

Dgrep.exe 파일을 일반 사용자 권한으로 실행 시 파일이 사라지는 것 외에는 변화가 없다.



[그림 4-2] 관리자 권한으로 실행 시

Dgrep.exe 파일을 관리자 권한으로 실행 시 파일이 사라진다. 또한 [그림 4-3]과 같이 로컬디스크 c에 wiseman.exe 실행파일이 생성된 것을 확인할 수 있다.



[그림 4-3] 관리자 권한으로 실행 후 파일 생성

4-2 프로세스 변화 확인 (Procexp)

Process Name	PPID	PID	Private Bytes	Working Set	Session ID	Company Name
csrss.exe	0,38	8,704 K	13,336 K	396	Client Server Runtime P...	Microsoft Corporation
conhost.exe	0,95	1,392 K	4,456 K	3536	콘솔 창 호스트	Microsoft Corporation
winlogon.exe	0,12	3,044 K	1,588 K	432	Windows 로그인 응용 프...	Microsoft Corporation
explorer.exe	0,12	44,576 K	40,164 K	1212	Windows 탐색기	Microsoft Corporation
vm3dservice.exe	0,12	1,092 K	752 K	1808		
vmtoolsd.exe	0,12	11,664 K	7,452 K	1820	VMware Tools Core Ser...	VMware, Inc.
procexp.exe	4,22	2,468 K	6,692 K	1920	Sysinternals Process E...	Sysinternals - www.s...
procexp64.exe	4,22	13,816 K	30,028 K	448	Sysinternals Process E...	Sysinternals - www.s...
AYAgent.aye	0,04	5,636 K	6,764 K	832	Tray Application	ESTsecurity Corp.
AYPop.aye	0,29	8,180 K	23,036 K	2336	Popup Application	ESTsecurity Corp.
cmd.exe	0,96	2,056 K	3,404 K	2868	Windows 명령 처리기	Microsoft Corporation
PING.EXE	0,74	992 K	3,556 K	3832	TCP/IP Ping 명령	Microsoft Corporation
rundll32.exe	4,77	5,292 K	10,844 K	964	Windows 호스트 프로세스...	Microsoft Corporation
wiseman.exe	0,64	1,320 K	4,072 K	2856	Wiseman NFC 응용 프로그램	Microsoft Corporation

[그림 4-4] Process Explorer 분석 결과

[그림 4-4]과 같이 conhost.exe를 생성하고 cmd 명령어를 통해 PING.EXE를 생성하고 사라졌으며 rundll32.exe와 wiseman.exe를 생성한다는 것을 확인했다.

Prot...	Local Address	Remote Address	State
TCP	bjh,localdomain:49874	107.163.241.198:6520	SYN_SENT
UDP	bjh:domain	:::	

[그림 4-5] Process Explorer에서 dgrep.exe 실행 후 생성된 rundll32.exe TCP/IP의 속성

State(상태)가 3-way-handsake 중 하나인 SYN_SENT인 것을 보아 원격 주소 107.163.241.198, 포트번호 6520로 TCP 통신을 위해 세션 연결 중인 것으로 추정된다.

Prot...	Local Address	Remote Address	State
TCP	bjh,localdomain:49871	ec2-3-35-144-12.ap-northeast-2.compute.amazonaws.com:http	SYN_SENT

[그림 4-6] Process Explorer에서 dgrep.exe 실행 후 생성된 wiseman.exe TCP/IP의 속성

wiseman.exe 파일 또한 해당 주소로 TCP통신을 하기 위해 세션 연결 중인 것으로 추정된다.

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

dgrep.exe (2724)	Microsoft (r) V... C:\Users\bjh...	Microsoft Corp...	bjh\junho	"C:\Users\bjh...	2022-07-16 오전...	2022-07-16 오전...
cmd.exe (2236)	Windows 명령 ... C:\Windows\...	Microsoft Corp...	bjh\junho	cmd.exe /c pin...	2022-07-16 오전...	2022-07-16 오전...
PING.EXE (3756)	TCP/IP Ping 명령 C:\Windows\...	Microsoft Corp...	bjh\junho	ping 127.0.0.1 -...	2022-07-16 오전...	2022-07-16 오전...
kyewbuoo.exe (964)	Microsoft (r) V... C:\Users\bjh...	Microsoft Corp...	bjh\junho	C:\Users\bjh...	2022-07-16 오전...	2022-07-16 오전...
rundll32.exe (3912)	Windows 호스... c:\windows\...	Microsoft Corp...	bjh\junho	c:\windows\...	2022-07-16 오전...	n/a
taskkill.exe (14...	프로세스 종료 c:\windows\...	Microsoft Corp...	bjh\junho	taskkill /f /im a...	2022-07-16 오전...	2022-07-16 오전...
wiseman.exe (1...	wiseman MFC ... C:\wiseman.exe		bjh\junho	"C:\wiseman,e...	2022-07-16 오전...	n/a

[그림 4-7] Process Monitor 분석 결과

Process Monitor를 통해 프로세스 트리를 확인한 결과 dgrep.exe 파일을 실행했을 때 과정을 알 수 있다.

- (가) Dgrep.exe 파일 실행 후 cmd.exe 생성
- (나) Cmd.exe에서 ping.exe를 생성하여 ping을 통한 네트워크 연결시도
- (다) Kyewbuoo.exe 생성 후 하위에 rundll32.exe 파일 생성
- (라) Rundll32.exe 파일 하위에 taskkill.exe 파일과 wiseman.exe 파일 생성

Autoruns [bjh\junho] - Sysinternals: www.sysinternals.com						
File Entry Options User Help						
Filter:						
Everything Logon Explorer Internet Explorer Scheduled Tasks Services Drivers Codecs Boot Execute Image Hijacks						
Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal	
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2022-07-14 오후 4:20		
ALYac	Launch Application	ESTsecurity Corp.	c:\program files\Westsoft\...	2022-04-27 오전 12:48		
VMware User ...	VMware Tools Core Service	VMware, Inc.	c:\program files\vmware...	2019-09-01 오후 5:38		
VMware VM3D...			c:\windows\system32\...	2019-07-26 오후 12:44		
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2022-07-16 오전 9:21		
EvtMgr	DirectX Media - Image Dire...	Microsoft Corporation	c:\wofba\ssawc.sws	2015-10-09 오후 12:29		
Wiseman	wiseman MFC 응용프로그램		c:\wiseman.exe	2015-04-27 오후 3:59		

[그림 4-8] Autoruns 분석 결과

레지스트리 변화를 확인할 수 있는 도구인 Autoruns를 통해 EvtMgr과 Wiseman이 생성된 것을 알 수 있다. 레지스트리의 경로 중 CurrentVersion\Run에 있는 프로그램은 PC가 재부팅 할 때마다 자동실행 된다. 따라서 재부팅 시 EvtMgr과 Wiseman가 실행된다는 것을 알 수 있다.

4-4. 네트워크 변화 확인 (Cports)

Process Name	Process ID	Protocol	Local Port	Local Process	Local Address	Remote Process	Remote Address	Remote Host Name	State	Process Path
lsass.exe	500	TCP	49157		0.0.0.0		0.0.0.0		Listening	C:\Windows\system32\lsass.exe
rundll32.exe	1572	TCP	49874		192.168.44.135	6520	107.163.241.1...		Sent	c:\windows\SysWOW64\rundll32.exe
rundll32.exe	1572	TCP	49875		192.168.44.135	12354	107.163.241.1...		Sent	c:\windows\SysWOW64\rundll32.exe
rundll32.exe	1572	TCP	49876		192.168.44.135	12354	107.163.241.1...		Sent	c:\windows\SysWOW64\rundll32.exe
rundll32.exe	1572	UDP	53	domain	127.0.0.1					c:\windows\SysWOW64\rundll32.exe
System	4	UDP	138	netbios-...	192.168.44.135					
Unknown	0	TCP	5357	wsd	127.0.0.1	49865	127.0.0.1	bjh	Time Wait	
Unknown	0	TCP	5357	wsd	127.0.0.1	49866	127.0.0.1	bjh	Time Wait	
Unknown	0	TCP	5357	wsd	127.0.0.1	49867	127.0.0.1	bjh	Time Wait	
Unknown	0	TCP	49862		192.168.44.135	443	https	125.209.218.1...	Time Wait	
Unknown	0	TCP	49863		192.168.44.135	80	http	172.217.161.2...	Time Wait	
Unknown	0	TCP	49864		192.168.44.135	443	https	172.217.161.2...	Time Wait	
wininit.exe	388	TCP	49152		0.0.0.0		0.0.0.0		Listening	C:\Windows\system32\wininit.exe
wiseman.exe	2924	TCP	49877		192.168.44.135	80	http	3.35.144.12	Sent	C:\wiseman.exe

[그림 4-9] Cports 분석결과

Dgrep.exe 파일 실행 시 다음과 같이 rundll32.exe와 wiseman.exe가 신규 생성되는 것을 알 수 있다. 이때 TCP 포트 6520, 12354, 80번으로 네트워크 활동을 하기 위해 시도하는 것으로 추정된다.

5. 결론

1. 악성코드는 exe형식이고 언어는 c++ 이다.
2. 정상적인 파일인 것처럼 위장하는 것과 실행 시 아이콘이 사라지고 악성 코드가 실행되는 특징을 보아 백도어와 트로이목마의 성격을 가지고 있다.
3. 패킹이 되어 있어 언패킹을 하지 않으면 정보를 알 수 없다.
4. 해당 파일 실행 시 레지스트리에 파일을 생성하여 시작프로그램에도 영향을 준다.
5. Rundll32.dll과 wiseman.exe를 통하여 악성코드 개발자 혹은 유포자가 특정 ip나 도메인으로 네트워크 활동을 하려고 연결을 시도하는 것으로 추정된다.

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. 불법 파일과 프로그램, 영상 등을 다운받지 않는다.