

Malware Analysis

악성코드 분석



이다영

Contents



정적 분석



동적 분석

정적 분석



파일의 겉면을 보고 판단하는 것.
악성코드 내의 어떠한 함수가 사용되는지,
어떠한 라이브러리가 이용되는지가 주요 분석 대상

정적 분석

#무엇을 찾을 수 있을까?

1. 파일의 컴파일 시기는 언제인가?
2. 파일의 패킹 여부
3. 임포트를 통해 악성코드 행위를 알 수 있는가?
4. 시스템에서 검색할 수 있는 다른 파일이 존재하는가?
5. 감염된 장비에 해당 악성코드를 발견하기 위한 네트워크 기반의 증거는 무엇인가?
6. 악성코드의 목적은 무엇인가?

정적 분석



실습 파일



실습 환경



Lab01-01.dll



Lab01-01

Windows 7

정적 분석

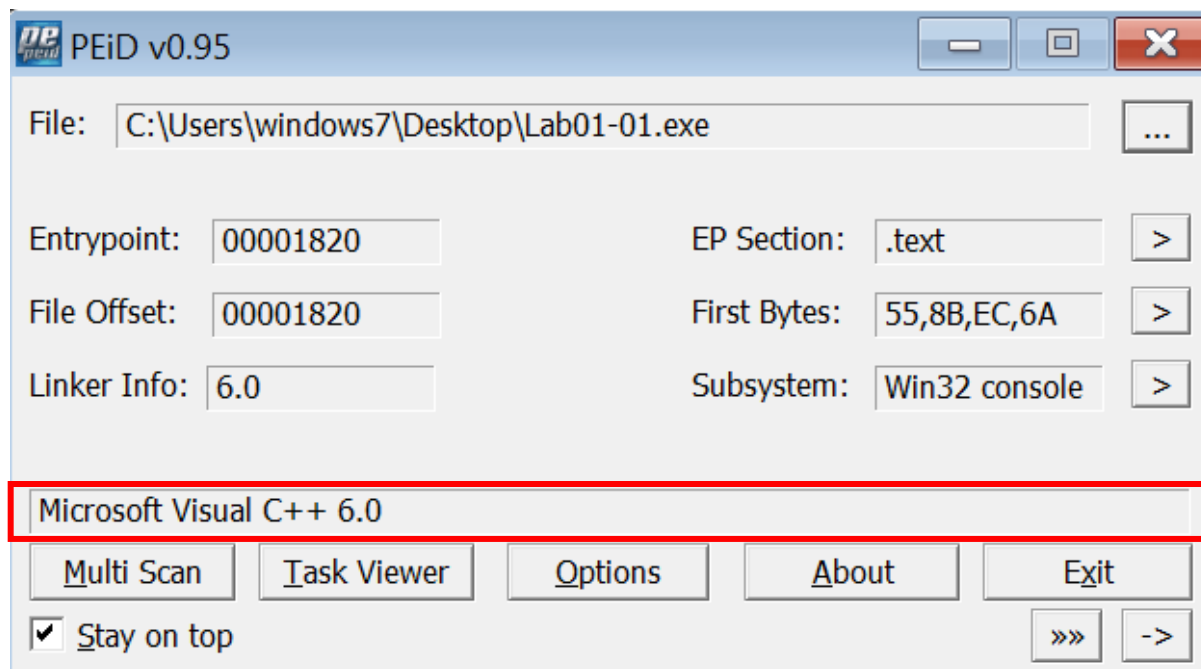
1. 파일의 컴파일 시기는 언제인가?

pFile	Data	Description	Value
000000EC	014C	Machine	IMAGE_FILE_MACHINE_I386
000000EE	0003	Number of Sections	
000000F0	4D0E2FD3	Time Date Stamp	2010/12/19 Sun 16:16:19 UTC
000000F4	00000000	Pointer to Symbol Table	
000000F8	00000000	Number of Symbols	
000000FC	00E0	Size of Optional Header	

IMAGE NT HEADERS -> IMAGE FILE HEADER

정적 분석

2. 파일의 패킹 여부



정적 분석

3. 임포트를 통해 악성코드 행위를 알 수 있는가?

pFile	Data	Description	Value
000020B8	00002124	Hint/Name RVA	001B CloseHandle
000020BC	00002132	Hint/Name RVA	02B0 UnmapViewOfFile
000020C0	00002144	Hint/Name RVA	01B5 IsBadReadPtr
000020C4	00002154	Hint/Name RVA	01D6 MapViewOfFile
000020C8	00002164	Hint/Name RVA	0035 CreateFileMappingA
000020CC	0000217A	Hint/Name RVA	0034 CreateFileA
000020D0	00002188	Hint/Name RVA	0090 FindClose
000020D4	00002194	Hint/Name RVA	009D FindNextFileA
000020D8	000021A4	Hint/Name RVA	0094 FindFirstFileA
000020DC	000021B6	Hint/Name RVA	0028 CopyFileA
000020E0	00000000	End of Imports	KERNEL32.dll

SECTION -> IMPORT NAME TABLE

정적 분석

3. 임포트를 통해 악성코드 행위를 알 수 있는가?

pFile	Data	Description	Value
000020B8	00002124	Hint/Name RVA	001B CloseHandle
000020BC	00002132	Hint/Name RVA	02B0 UnmapViewOfFile
000020C0	00002144	Hint/Name RVA	01B5 IsBadReadPtr
000020C4	00002154	Hint/Name RVA	01D6 MapViewOfFile
000020C8	00002164	Hint/Name RVA	0035 CreateFileMappingA
000020CC	0000217A	Hint/Name RVA	0034 CreateFileA
000020D0	00002188	Hint/Name RVA	0090 FindClose
000020D4	00002194	Hint/Name RVA	009D FindNextFileA
000020D8	000021A4	Hint/Name RVA	0094 FindFirstFileA
000020DC	000021B6	Hint/Name RVA	0028 CopyFileA
000020E0	00000000	End of Imports	KERNEL32.dll

SECTION -> IMPORT NAME TABLE

정적 분석

3. 임포트를 통해 악성코드 행위를 알 수 있는가?

pFile	Data	Description	Value
000020B8	00002124	Hint/Name RVA	001B CloseHandle
000020BC	00002132	Hint/Name RVA	02B0 UnmapViewOfFile
000020C0	00002144	Hint/Name RVA	01B5 IsBadReadPtr
000020C4	00002154	Hint/Name RVA	01D6 MapViewOfFile
000020C8	00002164	Hint/Name RVA	0035 CreateFileMappingA
000020CC	0000217A	Hint/Name RVA	0034 CreateFileA
000020D0	00002188	Hint/Name RVA	0090 FindClose
000020D4	00002194	Hint/Name RVA	009D FindNextFileA
000020D8	000021A4	Hint/Name RVA	0094 FindFirstFileA
000020DC	000021B6	Hint/Name RVA	0028 CopyFileA
000020E0	00000000	End of Imports	KERNEL32.dll

SECTION -> IMPORT NAME TABLE

정적 분석

3. 임포트를 통해 악성코드 행위를 알 수 있는가?

pFile	Data	Description	Value
000020B8	00002124	Hint/Name RVA	001B CloseHandle
000020BC	00002132	Hint/Name RVA	02B0 UnmapViewOfFile
000020C0	00002144	Hint/Name RVA	01B5 IsBadReadPtr
000020C4	00002154	Hint/Name RVA	01D6 MapViewOfFile
000020C8	00002164	Hint/Name RVA	0035 CreateFileMappingA
000020CC	0000217A	Hint/Name RVA	0034 CreateFileA
000020D0	00002188	Hint/Name RVA	0090 FindClose
000020D4	00002194	Hint/Name RVA	009D FindNextFileA
000020D8	000021A4	Hint/Name RVA	0094 FindFirstFileA
000020DC	000021B6	Hint/Name RVA	0028 CopyFileA
000020E0	00000000	End of Imports	KERNEL32.dll

SECTION -> IMPORT NAME TABLE

정적 분석

3. 임포트를 통해 악성코드 행위를 알 수 있는가?

pFile	Data	Description	Value
000020B8	00002124	Hint/Name RVA	001B CloseHandle
000020BC	00002132	Hint/Name RVA	02B0 UnmapViewOfFile
000020C0	00002144	Hint/Name RVA	01B5 IsBadReadPtr
000020C4	00002154	Hint/Name RVA	01D6 MapViewOfFile
000020C8	00002164	Hint/Name RVA	0035 CreateFileMappingA
000020CC	0000217A	Hint/Name RVA	0034 CreateFileA
000020D0	00002188	Hint/Name RVA	0090 FindClose
000020D4	00002194	Hint/Name RVA	009D FindNextFileA
000020D8	000021A4	Hint/Name RVA	0094 FindFirstFileA
000020DC	000021B6	Hint/Name RVA	0028 CopyFileA
000020E0	00000000	End of Imports	KERNEL32.dll

SECTION -> IMPORT NAME TABLE

정적 분석

3. 임포트를 통해 악성코드 행위를 알 수 있는가?

pFile	Data	Description	Value
000020B8	00002124	Hint/Name RVA	001B CloseHandle
000020BC	00002132	Hint/Name RVA	02B0 UnmapViewOfFile
000020C0	00002144	Hint/Name RVA	01B5 IsBadReadPtr
000020C4	00002154	Hint/Name RVA	01D6 MapViewOfFile
000020C8	00002164	Hint/Name RVA	0035 CreateFileMappingA
000020CC	0000217A	Hint/Name RVA	0034 CreateFileA
000020D0	00002188	Hint/Name RVA	0090 FindClose
000020D4	00002194	Hint/Name RVA	009D FindNextFileA
000020D8	000021A4	Hint/Name RVA	0094 FindFirstFileA
000020DC	000021B6	Hint/Name RVA	0028 CopyFileA
000020E0	00000000	End of Imports	KERNEL32.dll

SECTION -> IMPORT NAME TABLE

파일을 불러온 뒤 복사하여 메모리에 등재하는 루틴

정적 분석

4. 시스템에서 검색할 수 있는 다른 파일이 존재하는가?

명령어: strings.exe [파일] > [파일.txt]

```
C:\Users\windows7\Desktop>strings.exe Lab01-01.exe > Lab01-01.txt  
  
Strings v2.53 - Search for ANSI and Unicode strings in binary images.  
Copyright (C) 1999-2016 Mark Russinovich  
Sysinternals - www.sysinternals.com
```

정적 분석

4. 시스템에서 검색할 수 있는 다른 파일이 존재하는가?

```
kerne132.dll 악의적인 파일
kerne132.dll 원본 시스템 파일
.exe
C:\*
C:\windows\system32\kerne132.dll Kernel132.dll 경로
Kerne132.
Lab01-01.dll Lab01-01.dll 참고
C:\Windows\System32\Kerne132.dll
WARNING_THIS_WILL_DESTROY_YOUR_MACHINE
```

원본 시스템 파일 명칭 kernel32.dll과 유사한
kernel132.dll을 생성할 것이며 이때 Lab01-01.dll을 참조할 것

정적 분석

5. 감염된 장비에 해당 악성코드를 발견하기 위한 네트워크 기반의 증거는 무엇인가?

pFile	Data	Description	Value
000020AC	00002116	Hint/Name RVA	0296 Sleep
000020B0	0000211E	Hint/Name RVA	0044 CreateProcessA
000020B4	00002130	Hint/Name RVA	003F CreateMutexA
000020B8	00002140	Hint/Name RVA	01ED OpenMutexA
000020BC	00002108	Hint/Name RVA	001B CloseHandle
000020C0	00000000	End of Imports	KERNEL32.dll
000020C4	0000219C	Hint/Name RVA	009D _adjust_fdiv
000020C8	00002192	Hint/Name RVA	0291 malloc
000020CC	00002186	Hint/Name RVA	010F _initterm
000020D0	0000217E	Hint/Name RVA	025E free
000020D4	00002168	Hint/Name RVA	02C0 strcmp
000020D8	00000000	End of Imports	MSVCRT.dll
000020DC	80000017	Ordinal	0017
000020E0	80000073	Ordinal	0073
000020E4	8000000B	Ordinal	000B
000020E8	80000004	Ordinal	0004
000020EC	80000013	Ordinal	0013
000020F0	80000016	Ordinal	0016
000020F4	80000010	Ordinal	0010
000020F8	80000003	Ordinal	0003
000020FC	80000074	Ordinal	0074
00002100	80000009	Ordinal	0009
00002104	00000000	End of Imports	WS2_32.dll

SECTION -> IMPORT NAME TABLE

정적 분석

5. 감염된 장비에 해당 악성코드를 발견하기 위한 네트워크 기반의 증거는 무엇인가?

pFile	Data	Description	Value
000020AC	00002116	Hint/Name RVA	0296 Sleep
000020B0	0000211E	Hint/Name RVA	0044 CreateProcessA
000020B4	00002130	Hint/Name RVA	003F CreateMutexA
000020B8	00002140	Hint/Name RVA	01ED OpenMutexA
000020BC	00002108	Hint/Name RVA	001B CloseHandle
000020C0	00000000	End of Imports	KERNEL32.dll
000020C4	0000219C	Hint/Name RVA	009D _adjust_fdiv
000020C8	00002192	Hint/Name RVA	0291 malloc
000020CC	00002186	Hint/Name RVA	010F _initterm
000020D0	0000217E	Hint/Name RVA	025E free
000020D4	00002168	Hint/Name RVA	02C0 strcmp
000020D8	00000000	End of Imports	MSVCRT.dll
000020DC	80000017	Ordinal	0017
000020E0	80000073	Ordinal	0073
000020E4	8000000B	Ordinal	000B
000020E8	80000004	Ordinal	0004
000020EC	80000013	Ordinal	0013
000020F0	80000016	Ordinal	0016
000020F4	80000010	Ordinal	0010
000020F8	80000003	Ordinal	0003
000020FC	80000074	Ordinal	0074
00002100	80000009	Ordinal	0009
00002104	00000000	End of Imports	WS2_32.dll

SECTION -> IMPORT NAME TABLE

정적 분석

5. 감염된 장비에 해당 악성코드를 발견하기 위한 네트워크 기반의 증거는 무엇인가?

pFile	Data	Description	Value
000020AC	00002116	Hint/Name RVA	0296 Sleep
000020B0	0000211E	Hint/Name RVA	0044 CreateProcessA
000020B4	00002130	Hint/Name RVA	003F CreateMutexA
000020B8	00002140	Hint/Name RVA	01ED OpenMutexA
000020BC	00002108	Hint/Name RVA	001B CloseHandle
000020C0	00000000	End of Imports	KERNEL32.dll
000020C4	0000219C	Hint/Name RVA	009D _adjust_fdiv
000020C8	00002192	Hint/Name RVA	0291 malloc
000020CC	00002186	Hint/Name RVA	010F _initterm
000020D0	0000217E	Hint/Name RVA	025E free
000020D4	00002168	Hint/Name RVA	02C0 strcmp
000020D8	00000000	End of Imports	MSVCRT.dll
000020DC	80000017	Ordinal	0017
000020E0	80000073	Ordinal	0073
000020E4	8000000B	Ordinal	000B
000020E8	80000004	Ordinal	0004
000020EC	80000013	Ordinal	0013
000020F0	80000016	Ordinal	0016
000020F4	80000010	Ordinal	0010
000020F8	80000003	Ordinal	0003
000020FC	80000074	Ordinal	0074
00002100	80000009	Ordinal	0009
00002104	00000000	End of Imports	WS2_32.dll

SECTION -> IMPORT NAME TABLE

정적 분석

5. 감염된 장비에 해당 악성코드를 발견하기 위한 네트워크 기반의 증거는 무엇인가?

pFile	Data	Description	Value
000020AC	00002116	Hint/Name RVA	0296 Sleep
000020B0	0000211E	Hint/Name RVA	0044 CreateProcessA
000020B4	00002130	Hint/Name RVA	003F CreateMutexA
000020B8	00002140	Hint/Name RVA	01ED OpenMutexA
000020BC	00002108	Hint/Name RVA	001B CloseHandle
000020C0	00000000	End of Imports	KERNEL32.dll
000020C4	0000219C	Hint/Name RVA	009D _adjust_fdiv
000020C8	00002192	Hint/Name RVA	0291 malloc
000020CC	00002186	Hint/Name RVA	010F _initterm
000020D0	0000217E	Hint/Name RVA	025E free
000020D4	00002168	Hint/Name RVA	02C0 strncmp
000020D8	00000000	End of Imports	MSVCRT.dll
000020DC	80000017	Ordinal	0017
000020E0	80000073	Ordinal	0073
000020E4	8000000B	Ordinal	000B
000020E8	80000004	Ordinal	0004
000020EC	80000013	Ordinal	0013
000020F0	80000016	Ordinal	0016
000020F4	80000010	Ordinal	0010
000020F8	80000003	Ordinal	0003
000020FC	80000074	Ordinal	0074
00002100	80000009	Ordinal	0009
00002104	00000000	End of Imports	WS2_32.dll

Sleep을 통해 일정시간 프로세스를 멈추다가,
WS2_32.dll로 네트워크 통신을 하여
프로세스를 생성하는 백도어로 추측

정적 분석

6. 악성코드의 목적은 무엇인가?

Backdoor(백도어)

: 시스템 접근에 대한 사용자 인증 등 정상적인 절차를 거치지 않고
응용 프로그램 또는 시스템에 접근하여
컴퓨터 속의 정보를 빼내거나 특정 작업을 하도록 제작된 프로그램

동적 분석



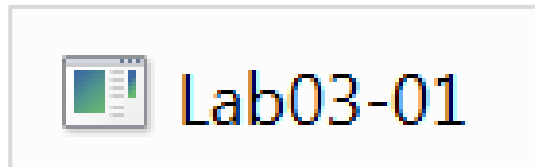
파일을 실행시키면서 분석하는 과정.
악성코드 실행 시 발생하는 파일, 프로그램, 레지스트리 등
각종 서비스 및 시스템 관련 항목의 변경 사항을 확인해야한다.
실행 시 발생하는 네트워크 트래픽 또한 주요 관건이다.

동적 분석

#무엇을 찾을 수 있을까?

1. 악성코드임을 의미하는 호스트 기반 표시자는 무엇인가?
2. 악성코드를 인식할 수 있는 네트워크 기반의
시그니처가 존재하는가?
3. 악성코드의 목적은 무엇인가?

동적 분석



Windows XP

동적 분석

```
<2f
StubPath
SOFTWARE\Classes\http\shell\open\commandv
Software\Microsoft\Active Setup\Installed Components\
test
  www.practicalmalwareanalysis.com   악성코드가 실행되면서 접근할 주소
admin
VideoDriver
WinVMX32-
vmx32to64.exe
SOFTWARE\Microsoft\windows\CurrentVersion\Run   부팅시에 실행되는 것들
Ph?
V5h
V)V
SOFTWARE\Microsoft\windows\CurrentVersion\Explorer\Shell Folders
PWj
AppData
```


동적 분석

1. 악성코드임을 의미하는 호스트 기반 표시자는 무엇인가?

호스트 기반 표시자

: 감염 PC에서 일어나는 모든 파일 행위나 레지스트리 변경 행위

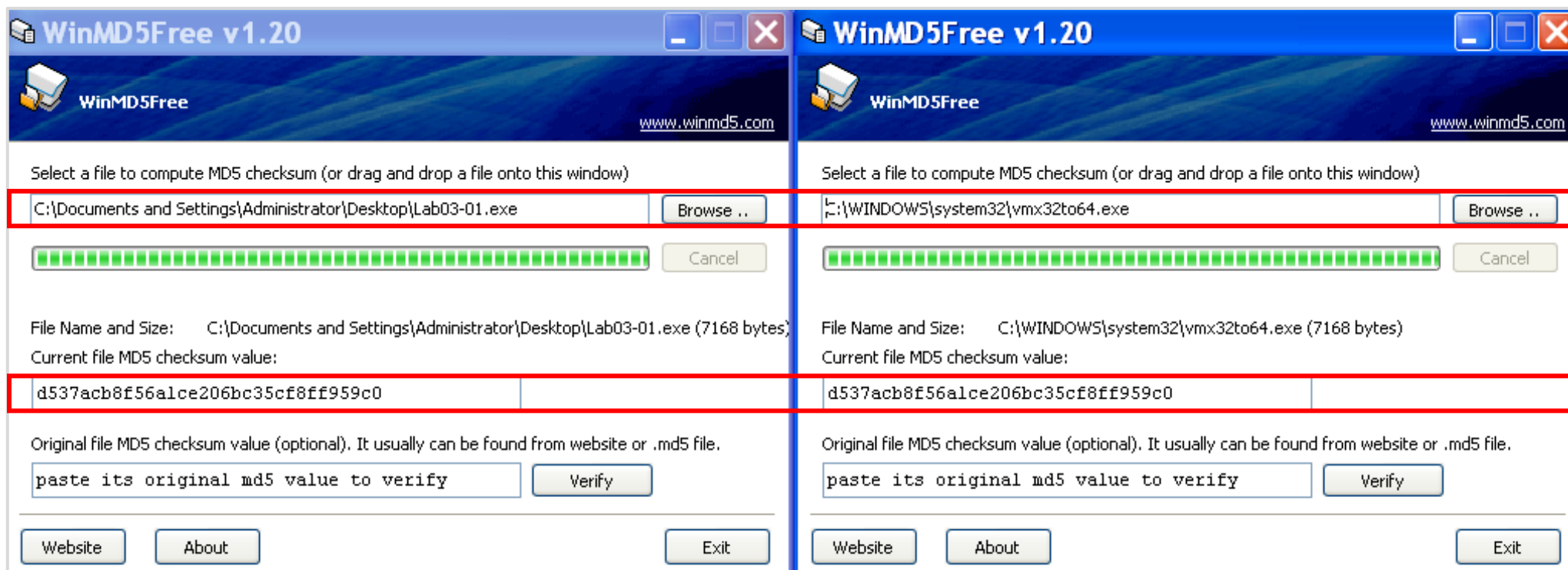
동적 분석

1. 악성코드임을 의미하는 호스트 기반 표시자는 무엇인가?

Time of Day	Process Name	PID	Operation	Path	Result	Detail
3:06:09.3029958 AM	Lab03-01.exe	2864	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\ RNG\Seed	SUCCESS	Type: REG_...
3:06:09.5895610 AM	Lab03-01.exe	2864	WriteFile	C:\WINDOWS\system32\vmx32to64.exe	SUCCESS	Offset: 0, Le...
3:06:09.6154520 AM	Lab03-01.exe	2864	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\VideoDriver	SUCCESS	Type: REG_...
3:06:10.2731479 AM	Lab03-01.exe	2864	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\ RNG\Seed	SUCCESS	Type: REG_...
3:06:10.2732820 AM	Lab03-01.exe	2864	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\ RNG\Seed	SUCCESS	Type: REG_...
3:06:10.2733803 AM	Lab03-01.exe	2864	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\ RNG\Seed	SUCCESS	Type: REG_...
3:06:10.2734770 AM	Lab03-01.exe	2864	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\ RNG\Seed	SUCCESS	Type: REG_...
3:06:10.2735896 AM	Lab03-01.exe	2864	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\ RNG\Seed	SUCCESS	Type: REG_...
3:06:10.2736971 AM	Lab03-01.exe	2864	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\ RNG\Seed	SUCCESS	Type: REG_...
3:06:10.2737935 AM	Lab03-01.exe	2864	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\ RNG\Seed	SUCCESS	Type: REG_...

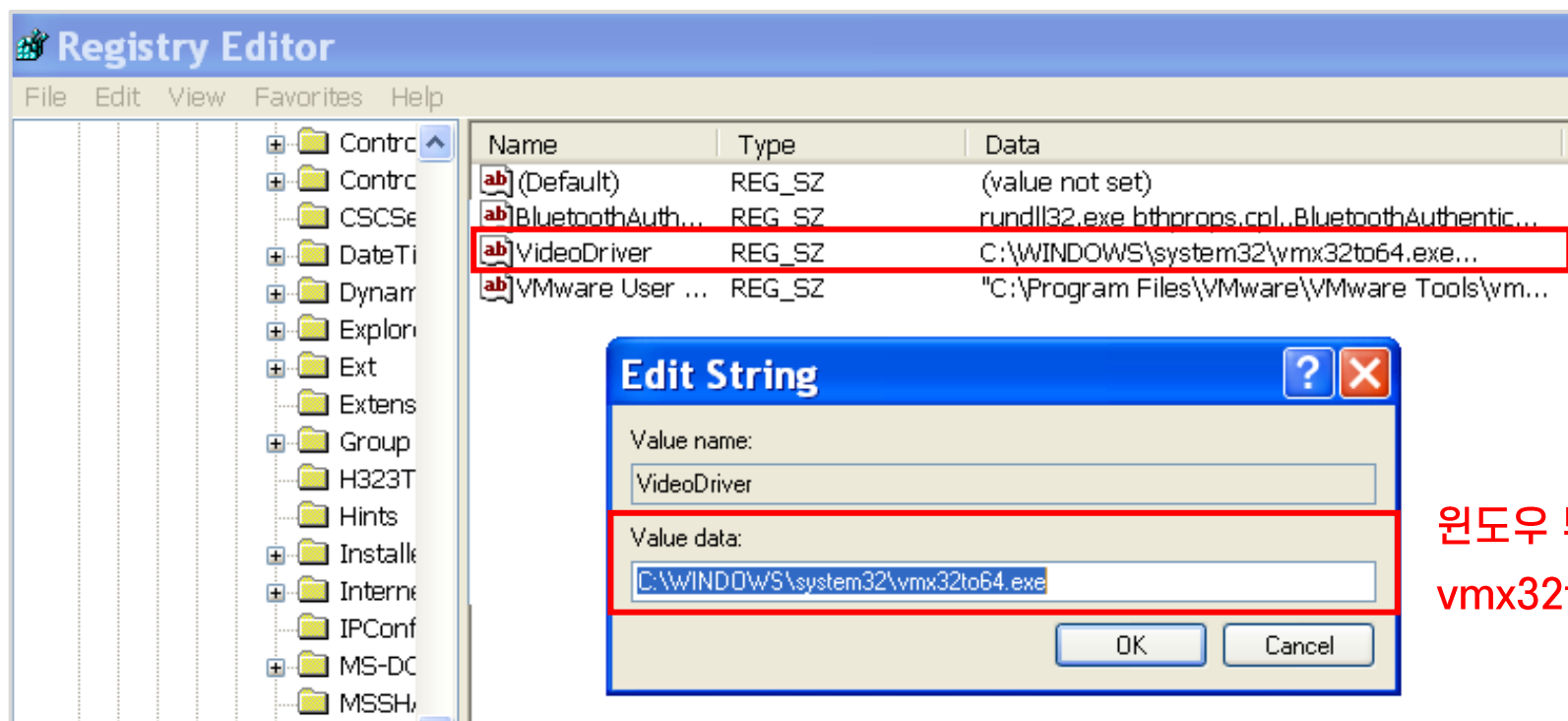
동적 분석

1. 악성코드임을 의미하는 호스트 기반 표시자는 무엇인가?



동적 분석

1. 악성코드임을 의미하는 호스트 기반 표시자는 무엇인가?



동적 분석

2. 악성코드를 인식할 수 있는 네트워크 기반의 시그니처가 존재하는가?

Lab03-01.exe		868 K	2,372 K 2864
Name	Description	Company Name	Path
secur32.dll	Security Support Provi...	Microsoft Corpor...	C:\WINDOWS\system32\secur32.dll
setupapi.dll	Windows Setup API	Microsoft Corpor...	C:\WINDOWS\system32\setupapi.dll
shlwapi.dll	Shell Light-weight Utilit...	Microsoft Corpor...	C:\WINDOWS\system32\shlwapi.dll
sortkey.nls			C:\WINDOWS\system32\sortkey.nls
sorttbls.nls			C:\WINDOWS\system32\sorttbls.nls
unicode.nls			C:\WINDOWS\system32\unicode.nls
user32.dll	Windows XP USER A...	Microsoft Corpor...	C:\WINDOWS\system32\user32.dll
usp10.dll	Uniscribe Unicode scri...	Microsoft Corpor...	C:\WINDOWS\system32\usp10.dll
version.dll	Version Checking and ...	Microsoft Corpor...	C:\WINDOWS\system32\version.dll
winmr.dll	LDAP RnR Provider DLL	Microsoft Corpor...	C:\WINDOWS\system32\winmr.dll
wldap32.dll	Win32 LDAP API DLL	Microsoft Corpor...	C:\WINDOWS\system32\wldap32.dll
ws2_32.dll	Windows Socket 2.0 3...	Microsoft Corpor...	C:\WINDOWS\system32\ws2_32.dll
ws2help.dll	Windows Socket 2.0 H...	Microsoft Corpor...	C:\WINDOWS\system32\ws2help.dll
wshbth.dll	Windows Sockets Hel...	Microsoft Corpor...	C:\WINDOWS\system32\wshbth.dll
wshtcpip.dll	Windows Sockets Hel...	Microsoft Corpor...	C:\WINDOWS\system32\wshtcpip.dll

네트워크 관련 dll

동적 분석

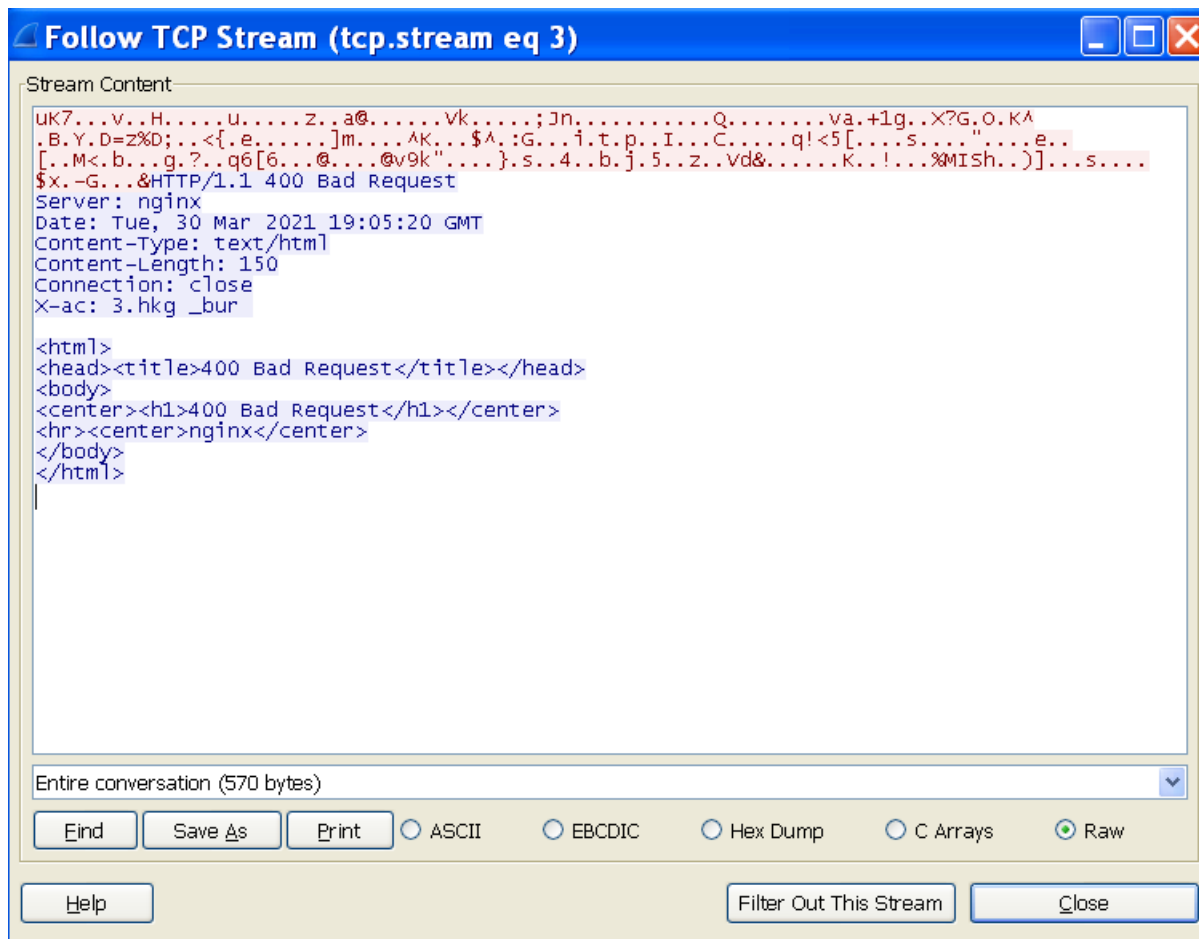
2. 악성코드를 인식할 수 있는 네트워크 기반의 시그니처가 존재하는가?

```
<2f
StubPath
SOFTWARE\Classes\http\shell\open\commandv
Software\Microsoft\Active Setup\Installed Components\
test
  www.practicalmalwareanalysis.com
admin
VideoDriver
WinVMX32-
vmx32to64.exe
SOFTWARE\Microsoft\windows\CurrentVersion\Run
Ph?
V5h
V)V
SOFTWARE\Microsoft\windows\CurrentVersion\Explorer\Shell Folders
PWj
AppData
```

악성코드가 실행되면서 접근할 주소

동적 분석

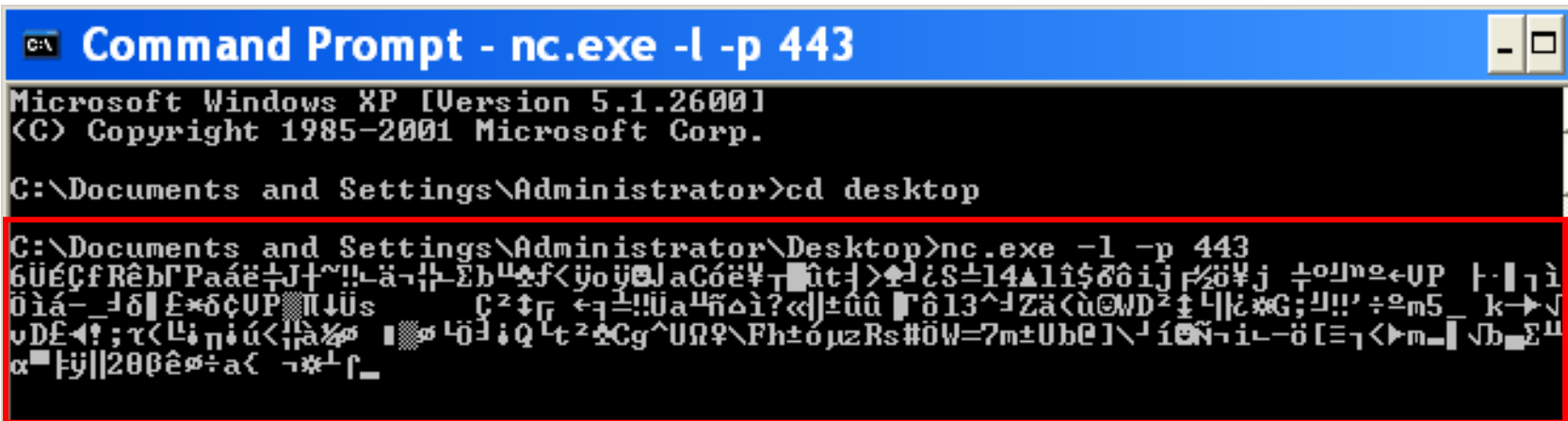
2. 악성코드를 인식할 수 있는 네트워크 기반의 시그니처가 존재하는가?



443번 포트를 통해 전송되는 데이터

동적 분석

2. 악성코드를 인식할 수 있는 네트워크 기반의 시그니처가 존재하는가?



```
C:\> Command Prompt - nc.exe -l -p 443
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

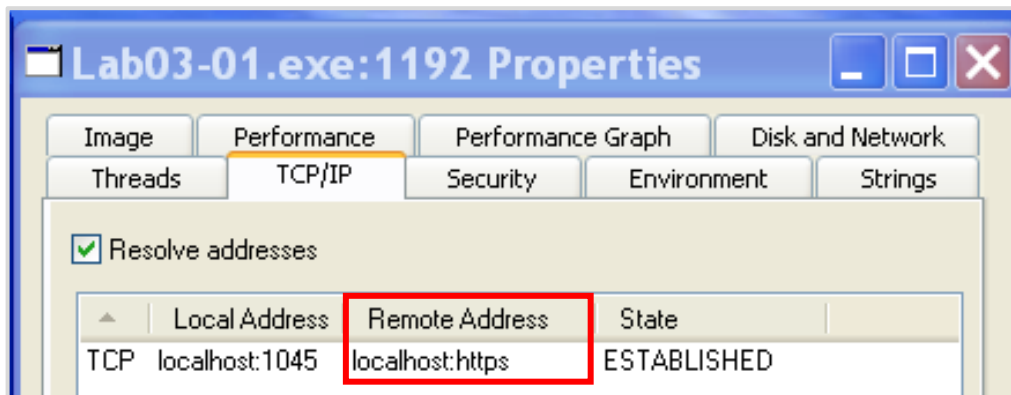
C:\Documents and Settings\Administrator>cd desktop

C:\Documents and Settings\Administrator\Desktop>nc.exe -l -p 443
6ÜÉÇfRêbΓPaáë÷J†~!!-ä-γ-Σbμ±f<ÿoÿËJaCöë¥T■û†>±¿¿S±14▲1î$ôôijf/ö¥j ÷oJn±UP |·|γì
öìá- ÿδ||£*δçUP■Π↓Üs C²†Γ ←γ±!!üaμñΔì?«||±ûû Γô13^¿Zä<ù@WD²±||¿*G;γ!!'÷±m5 k→√
υD£◄!;τ<L;Π;ú<||à%σ ■σ L0¿;Q L†²±Cg^UΩ♀\Fh±óμzRs#öW=7m±Ubc] \¿í@ÑγiL-ö [≡γ<▷m-|√bΣμ
α■†ÿ||20βêσ÷α< γ*†Γ_
```

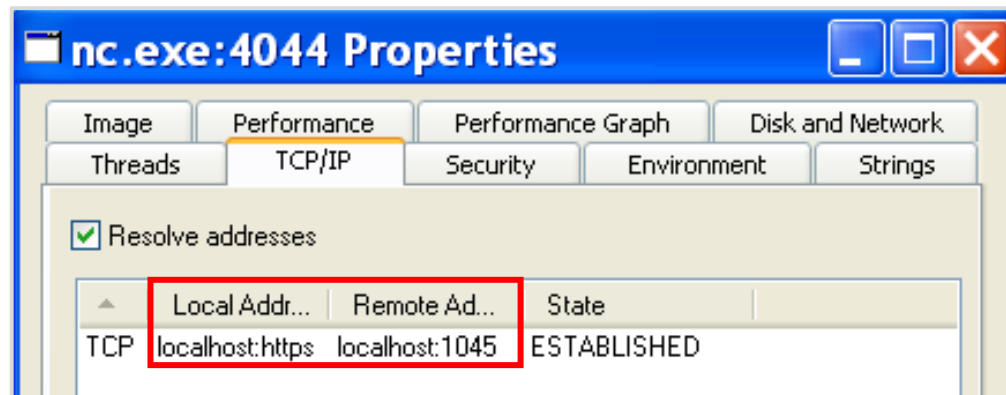
포트를 443으로 지정하고 리스닝

동적 분석

2. 악성코드를 인식할 수 있는 네트워크 기반의 시그니처가 존재하는가?



HTTPS : 443번 포트



Lab03-01.exe가 www.practicalmalwareanalysis.com으로 데이터를 보내면,
로컬에서 그에 맞는 어떠한 명령어를 다시 exe 파일쪽으로 넘겨준다

동적 분석

3. 악성코드의 목적은 무엇인가?

Backdoor(백도어)

: 시스템 접근에 대한 사용자 인증 등 정상적인 절차를 거치지 않고
응용 프로그램 또는 시스템에 접근하여
컴퓨터 속의 정보를 빼내거나 특정 작업을 하도록 제작된 프로그램

감사합니다 😊