

기술문서	'09. 10. 19. 작성
------	-----------------

Windows 악성코드 분석 가이드

소속 : 동명대학교 THINK동아리

작성자 : 강동현 cari2052@gmail.com

Contents

1. 개요	p.03
2. 분석 도구	
가. 가상 컴퓨팅 환경 VMware, VirtualPC	p.04
나. 분석 도구	p.04
3. 악성코드 분석 준비	
가. 샘플 악성코드 (키로거_Backdoor)	p.06
4. 악성코드 분석	
가. 샘플 악성코드 바이너리 분석	p.07
나. 샘플 악성코드 실행 분석	p.09
다. 샘플 악성코드 임의 실행 분석	p.16
5. 맺음말	p.19
부록 A VMware workstaion 스냅샷 설정	p.20
부록 B 샘플 악성코드 언패킹	p.21

1. 개요

악성코드 분석에서 사용 가능한 도구를 이용한 분석환경 설정, 효율적인 분석 방법 그리고 악성코드 분석 과정을 통해 간접 분석 경험을 할 수 있도록 작성했다.

문서 열람 이전 악성코드 분석에 필요한 기본 지식들은 「[기술문서]악성코드 분석 방법론_태인규」, 「[기술문서]PE구조 분석, 구조_강동현」에서 참고할 수 있다.

또한 Windows 악성코드를 분석하기 위해서는 Windows 프로그래밍의 기본적인 지식, Windows 시스템, OS Windows 에 관한 전반적인 지식을 쌓은 후 분석을 시도하기를 바란다.

악성코드 분석은 가상 컴퓨터 내에서 분석하는 것이 가장 적절하다. 악성코드의 내부 동작 방식을 미리 알고 있으면 좋겠지만 확인되지 않은 악성코드들을 분석하기에는 어떠한 상황이 발생하는지는 예상하기 힘들기 때문에 가상 컴퓨터 내에서 네트워크 설정을 제외하거나 프락시 서버를 이용하여 가상 컴퓨터의 네트워크를 조절할 수 있어야한다.

2. 분석 도구

악성코드 분석에 필요한 도구

가. 가상 컴퓨팅 환경 VMware, VirtualPC

가상 컴퓨팅 환경을 제공하는 도구들로 실제 사용하는 시스템들과 동일한 환경을 제공한다. 하드웨어적인 설정들은 가상 인터페이스를 이용하여 연동할 수 있고, 실제 사용하는 CD-ROM이나 USB와 같은 디바이스들도 직접 연결 가능하다.

특히 스냅샷(Snapshot) 기능을 통해 분석환경에서 분석 후 다시 기존 스냅샷 지점으로 되돌릴 수 있으며, 이 스냅샷을 이용하여 특정 환경을 재설치 없이 사용할 수 있다.

1) VMware Workstation, VMware Player

VMware사에서 개발한 가상 솔루션으로 이미지를 통해 가상 컴퓨팅을 제공한다.

- o VMware Workstation은 상용 프로그램으로 30일간 평가버전으로 사용가능하고 이후 라이선스를 구입해야 사용할 수 있다.

- o VMware Player는 무료 프로그램으로 VMware Workstation과 비슷한 구성이지만 몇 가지 기능을 제외한 프로그램이다.

VMware 솔루션에 관한 내용은 <http://www.vmware.com> 에서 얻을 수 있다.

2) Virtual PC

Microsoft사에서 개발한 가상 솔루션으로 위의 VMware와 유사한 컴퓨팅을 제공한다.

나. 분석 도구

악성코드를 단계별 분석을 위해 각각의 분석 도구를 상황에 맞게 사용한다.

1) 시스템 분석 도구

시스템 환경이나 악성 코드로부터 변경사항들을 분석할 수 있다.

- o Filemon

악성코드가 외부 파일을 오픈, 생성, 제거, 변조 하는 등의 행동을 실시간으로 분석 할 수 있다.

- o Regmon

악성코드가 시스템의 레지스터 값을 이용하는 것을 실시간으로 분석할 수 있다.

- o winalysis

시스템의 주요 파일이나 레지스트리, 프로세스 등과 같은 정보를 미리 저장해 두었다가 악성코드 실행 후 변경된 사항을 확인할 수 있다.

- o procexp

실행중인 프로세스를 트리형식으로 나열한다.

2) 파일 분석 도구

윈도우즈 파일 형식의 악성코드를 분석할 수 있다.

- o Strings

파일 내부 문자열을 모두 찾아내어 특정 옵션 조합을 통해 결과를 보여준다.

- o dumpbin

파일의 정보를 옵션에 맞게 출력해준다. Header 정보, Section 정보 그리고 간략한 디스어셈블 까지 내용들을 확인할 수 있다.

- o Ollydbg

디버깅 도구로 직관적인 프로그램 디버깅이 가능하다. 디스어셈블 기능으로 분석에 도움이 되기도 하고 플러그인을 통해 기능 확장이 가능하다.

- o IDA Pro

상용의 디스어셈블러이며, 파일 로드와 동시에 상당한 디스어셈블 기능을 확인할 수 있다. 또한 기본적인 내용 이외에도 분석에 도움이 되는 정보들을 제공한다.

3) 네트워크 분석 도구

네트워크 연결 상태확인 및 패킷 분석을 할 수 있다.

- o TCPView

실행중인 프로세스의 포트정보와 프로토콜 정보(TCP or UDP) 등을 출력한다.

- o TDImon

프로세스로부터 발생하는 패킷 정보를 실시간으로 출력한다.

- o Fopen, openports

실행 중인 프로세스가 열어둔 포트 목록을 출력한다.

- o Wireshark

네트워크 인터페이스를 통한 패킷을 분석한다. 각 패킷을 직접 확인 가능하다.

- o Paros

웹 어플리케이션을 위한 프락시 도구. 웹 패킷의 내용을 확인 할 수 있고 패킷 내용을 수정할 수 있다.

3. 악성코드 분석 준비

샘플 악성코드(키로거_Backdoor)를 통해 악성코드 분석을 간접 경험을 할 수 있다.

가. 샘플 악성코드 (키로거_Backdoor)

1) 샘플 악성코드 정의

<http://www.virustotal.com>에서 샘플 바이러스를 백신 프로그램들의 바이러스 정의를 확인할 수 있다.

- o AhnLab-V3
 - Win-Trojan/Prorat.349228.0
- o Avast
 - Win32:Prorat-FE
- o Kaspersky
 - Backdoor.Win32.Prorat.dz
- o McAfee
 - BackDoor-AWV
- o nProtect
 - Backdoor/W32.Prorat.349228.W
- o ViRobot
 - Backdoor.Win32.Prorat.349228.G

2) 분석 환경

실제 샘플 악성코드 분석을 위해 설정한 분석 환경이다.

- o VMware workstation 6.0
기본적인 윈도우 설치한 후 분석이 끝난 이후 기본 설치로 되돌리기 위해 스냅샷(snapshot) 기능을 이용하였다. (부록 A VMware workstaion 스냅샷 설정 참고)
- o 분석 도구
 - strings : 실행파일 내부 문자열 확인
 - PEid v0.95 : Packing, 컴파일 정보
 - PView v0.9 : 윈도우 파일 구조 확인
 - Stud_PE v2.4 : 종합적 파일 정보 확인
 - winalysis v3.0 : 시스템 변경사항 확인
 - Filemon v7.03 : 프로세스로부터 파일 사용 내역 확인
 - Regmon v7.03 : 프로세스로부터 레지스트리 사용 내역 확인
 - IceSword v1.20en : Rootkit 탐색기
 - BinText v3.00 : strings와 유사

4. 악성코드 분석

준비된 환경에 샘플 악성코드를 옮기고 아래 분석 절차에 따라 분석한다.

가. 샘플 악성코드 바이너리 분석

악성코드 바이너리상의 아스키 코드, PE구조 확인, Import & Export, 패킹 등과 같이 악성코드를 실행하지 않고 확인 할 수 있는 내용들을 분석한다.

1) strings.exe

명령 프롬프트 상에서 strings.exe 파일을 실행한다.

```
strings>strings.exe -a services.exe>string.service.exe.txt
```

생성된 string.service.exe.txt 파일을 분석해 보면 내부 아스키 값을 확인할 수 있다.

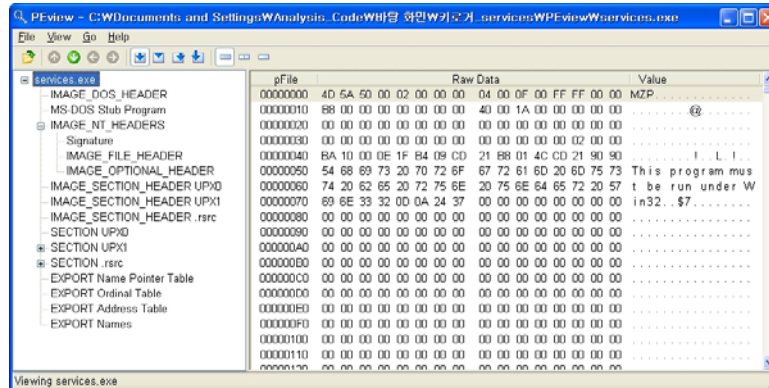
2) peid v0.95

샘플 악성코드를 open하면 패킹정보 또는 컴파일 정보를 확인할 수 있다.



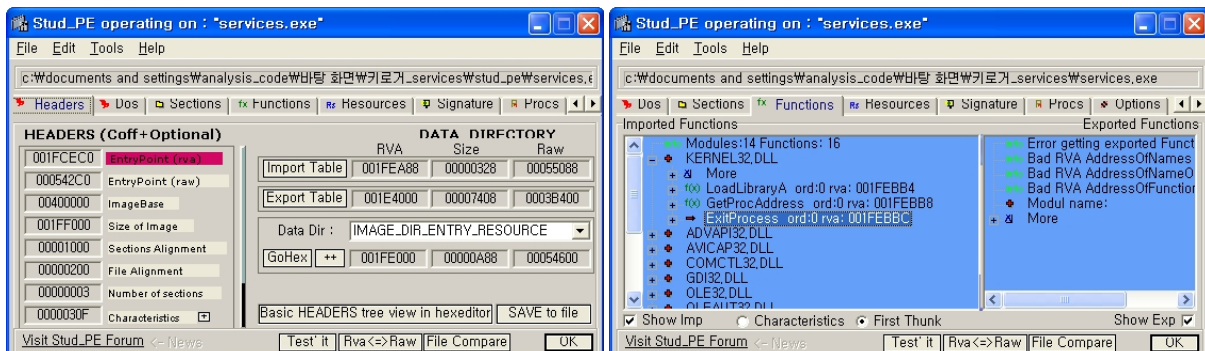
3) PView v0.9

샘플 악성코드의 바이너리 전체 분석한다. PE구조 형태로 분류하여 hexa코드와 아스키코드 값으로 분석할 수 있다.



4) Stud_PE v2.4

샘플 악성코드의 바이너리 값을 사용자가 보기 쉽도록 정렬되어 있다. Import, Export 함수 목록을 상세히 정리 되어 있으므로 자주 사용하는 것을 추천한다.

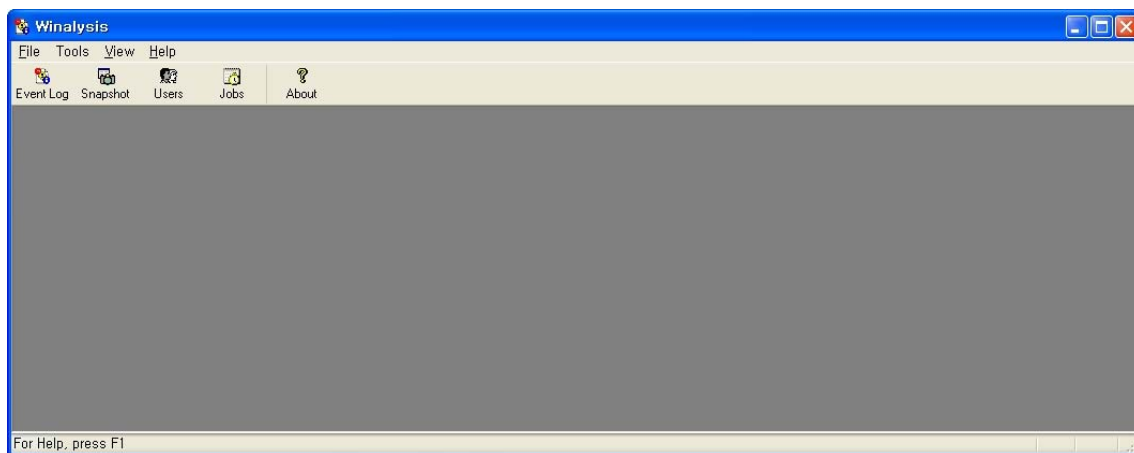


나. 샘플 악성코드 실행 분석

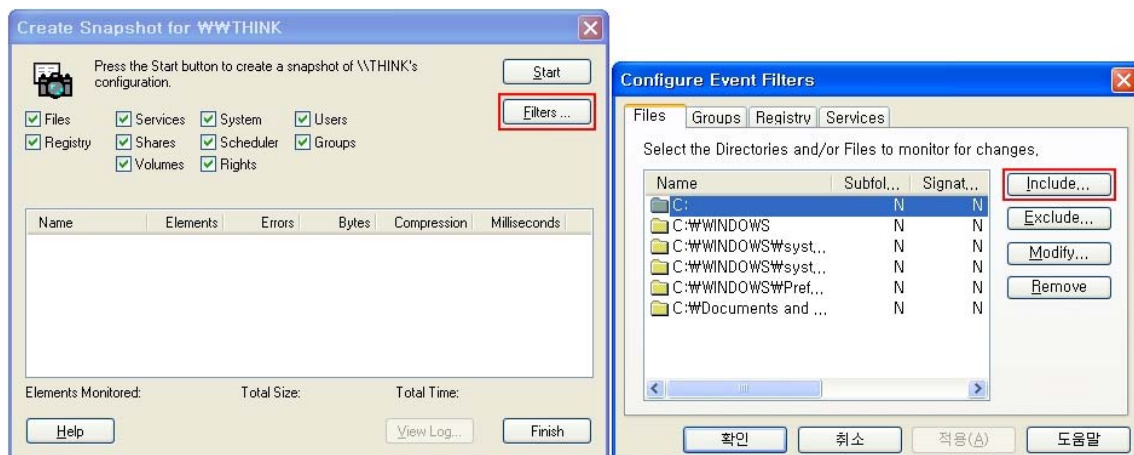
악성코드를 실행하여 어떤 행동을 하는지를 실시간으로 확인 한다.

1) winalysis v3.0

시스템 스냅샷에 사용하는 도구이다. 악성코드가 실행하기 전, 후를 비교할 수 있고 어떤 파일이 생성, 수정, 삭제되었는지에 시간차를 두고 분석할 수 있다.

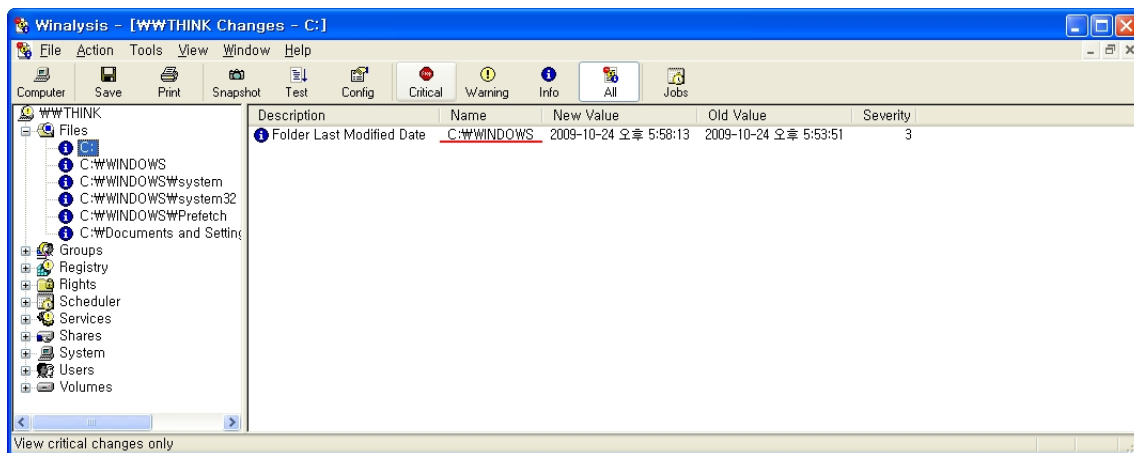


상단의 Snapshot 버튼을 클릭하면 시스템을 스냅샷을 할 수 있다.



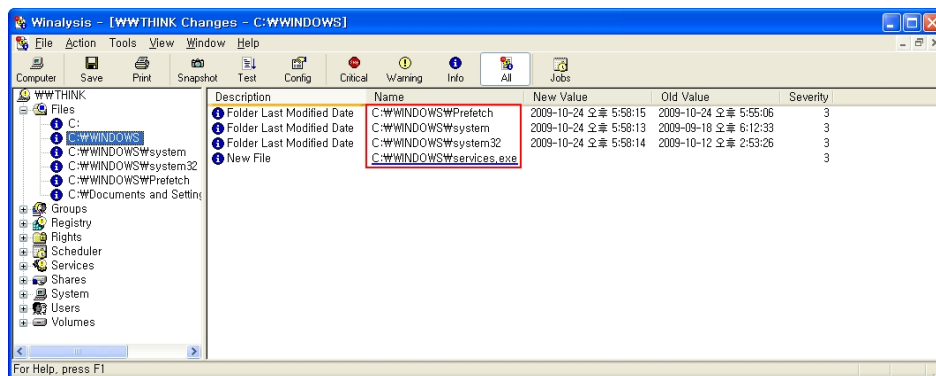
위 그림의 Filters 버튼을 클릭하면 Files, Groups, Registry, Services를 설정하여 이후 변경되는 정보를 설정 할 수 있다.

(디폴트로 C: , C:WINDOWS\SYSTEM32 로 설정되어 있으며 사용에 맞게 Include 버튼으로 추가 할 수 있다.)



스냅샷을 한 이후 악성코드를 실행하고, 다시 Snapshot 버튼 옆의 Test를 버튼을 클릭하면 변경된 내용을 찾아준다.

위 그림을 통해 C:에서 WINDOWS 폴더가 변경되었음을 확인할 수 있다.



위 그림을 통해 C:\WINDOWS에서 Prefetch, system, system32폴더가 변경되었고, WINDOWS 폴더 내에 services.exe 파일이 새로 생성되었음을 확인할 수 있다.

같은 방식으로 Prefetch, system, system32폴더 내부 파일을 확인하면 악성코드가 어떤 파일들을 생성했는지 알 수 있다.

파일 이외 변경된 Groups, Registry, Rights, Scheduler, Services, Shares, System, Users, Volumes를 확인 할 수 있다.

아래는 변경, 생성된 파일 정보들 이다.

- o WINDOWS\
 - services.exe
- o WINDOWS\Prefetch\
 - CONIME.EXE-13EEEA1A.pf
 - CMD.EXE-087B4001.pf
 - FSERVICE.EXE-2E4F6E14.pf
 - NET.EXE-01A53C2F.pf
 - NET1.EXE-029B9DB4.pf
 - RUNDLL32.EXE-2313F110.pf
 - SERVICES.EXE-14D2412D.pf
 - SERVICES.EXE-2B0DD057.pf

(Prefetch폴더는 MS Windows에서 메모리 미리 읽기 기능을 통한 빠른 실행을 위해 존재한다. 변경 사항들의 정보로 Forensic분야에서 활용되고 있다.)

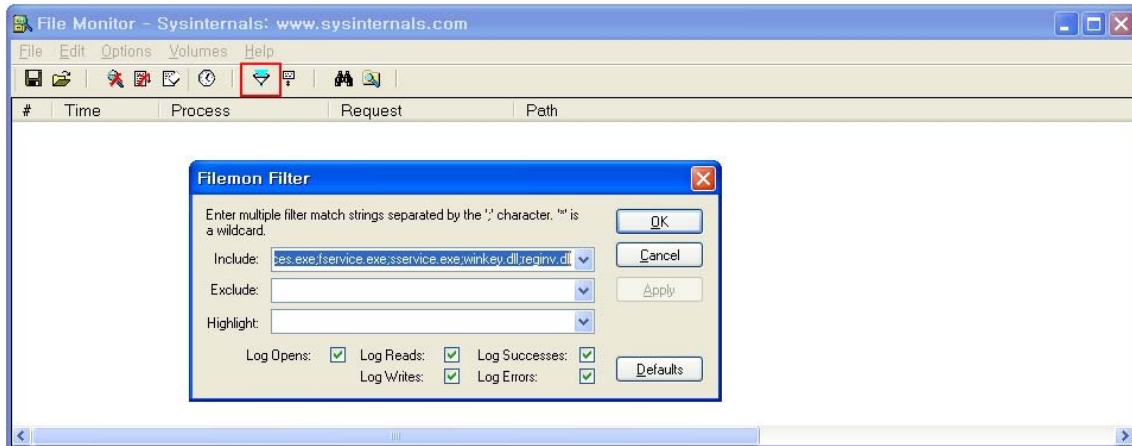
- o WINDOWS\system\
 - sservice.exe
- o WINDOWS\system32\
 - fservice.exe
 - reginv.dll
 - winkey.dll

아래는 변경, 생성된 레지스트리 정보들 이다.

Description	Name	New Value	Old Value	Severity
X Key Last Modified Date	HKLM\SYSTEM\CurrentControlSet\Services\Wsr...	2009-10-26 오후 10:28:10	2009-10-12 오후 2:52:43	4
X Key Last Modified Date	HKLM\SYSTEM\CurrentControlSet\Services\Wsr...	2009-10-26 오후 10:28:12	2009-10-12 오후 2:52:43	4
X Key Last Modified Date	HKLM\SYSTEM\CurrentControlSet\Services\Wsr...	2009-10-26 오후 10:28:12	2009-09-18 오후 6:26:04	4
X Key Last Modified Date	HKLM\SYSTEM\CurrentControlSet\Services\Wsr...	2009-10-26 오후 10:28:13	2009-09-18 오후 6:56:23	4
X Key Last Modified Date	HKLM\SYSTEM\CurrentControlSet\Services\Wsr...	2009-10-26 오후 10:28:13	2009-10-26 오후 10:25:14	4
X Key Last Modified Date	HKLM\SYSTEM\ControlSet001\Services\Wsr...	2009-10-26 오후 10:28:10	2009-10-12 오후 2:52:43	4
X Key Last Modified Date	HKLM\SYSTEM\ControlSet001\Services\Wsr...	2009-10-26 오후 10:28:12	2009-10-12 오후 2:52:43	4
X Key Last Modified Date	HKLM\SYSTEM\ControlSet001\Services\Wsr\Pa...	2009-10-26 오후 10:28:12	2009-09-18 오후 6:26:04	4
X Key Last Modified Date	HKLM\SYSTEM\ControlSet001\Services\WShare...	2009-10-26 오후 10:28:13	2009-09-18 오후 6:56:23	4
X Key Last Modified Date	HKLM\SYSTEM\ControlSet001\Services\WShare...	2009-10-26 오후 10:28:13	2009-10-26 오후 10:25:14	4
X Key Last Modified Date	HKLM\SOFTWARE\Microsoft\Windows NT\Cur...	2009-10-26 오후 10:28:09	2009-10-12 오후 2:53:29	4
X Key Last Modified Date	HKLM\SOFTWARE\Microsoft\Windows NT\Cur...	2009-10-26 오후 10:28:12	2009-09-18 오후 6:28:37	4
X Key Last Modified Date	HKLM\SOFTWARE\Microsoft\Windows NT\Cur...	2009-10-26 오후 10:28:10	2009-10-26 오후 10:25:14	4
X Key Last Modified Date	HKLM\SOFTWARE\Microsoft\Windows\Current...	2009-10-26 오후 10:28:09	2009-09-18 오후 6:17:10	4
X Key Last Modified Date	HKLM\SOFTWARE\Microsoft\Cryptography\WRNG	2009-10-26 오후 10:28:11	2009-10-26 오후 10:27:34	4
X Key Last Modified Date	HKLM\SOFTWARE\Microsoft\Active Setup\Inst...	2009-10-26 오후 10:28:09	2009-09-18 오후 6:18:35	4
New Key	HKLM\SOFTWARE\Microsoft\Windows\Current...			3
New Key	HKLM\SOFTWARE\Microsoft\Windows\Current...			3
New Key	HKLM\SOFTWARE\Microsoft\Active Setup\Inst...			3
New Value	HKLM\SYSTEM\CurrentControlSet\Services\W...	C:\WINDOWS\services.exe;-Enabled:services		3
New Value	HKLM\SYSTEM\ControlSet001\Services\WShare...	C:\WINDOWS\services.exe;-Enabled:services		3
New Value	HKLM\SOFTWARE\Microsoft\Windows\Current...	C:\WINDOWS\system32\sservice.exe		3
New Value	HKLM\SOFTWARE\Microsoft\Active Setup\Inst...	C:\WINDOWS\system\sservice.exe		3
Number of Subkeys	HKLM\SOFTWARE\Microsoft\Windows\Current...	4	3	3
Number of Subkeys	HKLM\SOFTWARE\Microsoft\Active Setup\Inst...	38	37	3
Number of Values	HKLM\SYSTEM\CurrentControlSet\Services\W...	5	4	3
Number of Values	HKLM\SYSTEM\ControlSet001\Services\WShare...	5	4	3
Value Changed	HKLM\SYSTEM\CurrentControlSet\Services\Wsr...	4	2	2
Value Changed	HKLM\SYSTEM\CurrentControlSet\Services\Wsr...	4	0	2
Value Changed	HKLM\SYSTEM\CurrentControlSet\Services\Wsr...	1	0	2
Value Changed	HKLM\SYSTEM\CurrentControlSet\Services\W...	15	13	2
Value Changed	HKLM\SYSTEM\ControlSet001\Services\Wsr...	4	2	2
Value Changed	HKLM\SYSTEM\ControlSet001\Services\Wsr\Start	4	0	2
Value Changed	HKLM\SYSTEM\ControlSet001\Services\Wsr\Wm...	W\SystemRoot\system32\DRIVERS\Wsr.sys	system32\DRIVERS\Wsr.sys	2
Value Changed	HKLM\SYSTEM\ControlSet001\Services\Wsr\Pa...	15	13	2
Value Changed	HKLM\SYSTEM\ControlSet001\Services\WShare...	15	13	2
Value Changed	HKLM\SOFTWARE\Microsoft\Windows NT\Cur...	Explorer.exe C:\WINDOWS\system32\sservice.exe	Explorer.exe	2
Value Changed	HKLM\SOFTWARE\Microsoft\Windows NT\Cur...	1	0	2
Value Changed	HKLM\SOFTWARE\Microsoft\Windows NT\Cur...	1	2	2
Value Changed	HKLM\SOFTWARE\Microsoft\Cryptography\WRNG	47 f6 11 91 60 b6 6e d1 f7 75 9c 26 83 94 24 52 77 80 ...	50 76 88 1e f1 f6 c8 f8 58 86 ca f9 67 f2 32 f2 05 87 a6 ...	2

2) Filemon v.7.03

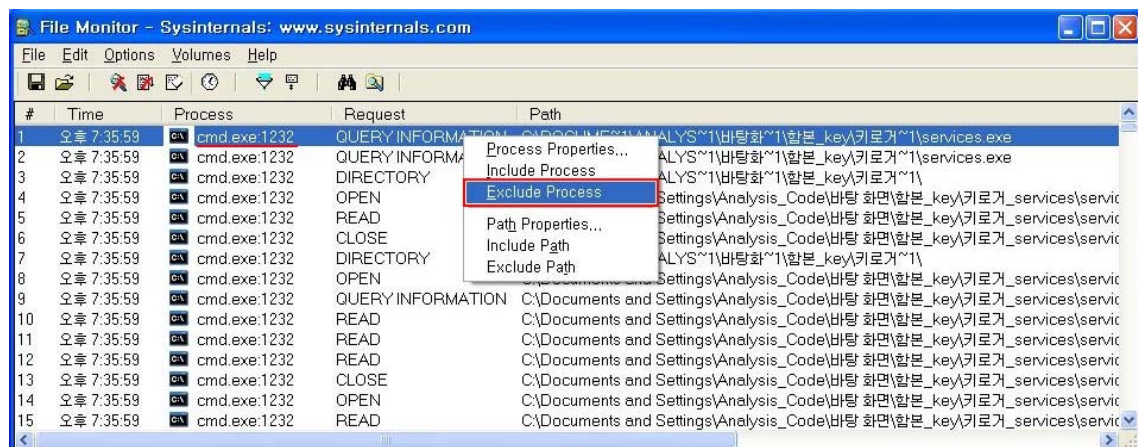
실행파일의 프로세스들이 파일을 통해 어떤 작업을 하는지를 실시간으로 분석할 수 있다. 실시간으로 분석되어지고 있는 파일 목록들을 필터링하여 필요한 정보들로 설정 가능하다.




winalysis 도구로부터 얻은 파일 목록을 필터링하여 분석하고 어떤 행동을 하는지 확인 한다.

(글자가 보이지 않으면, Options->Font...에서 폰트 크기를 변경해준다.)

(Include : services.exe;fsservice.exe;sservice.exe;winkey.dll;reginv.dll)



분석에 필요하지 않는 내용들은 Exclude Process를 통해 분석에 제외시킬 수 있다.(필터 설정에 자동 추가된다.)



File Monitor - Sysinternals: www.sysinternals.com

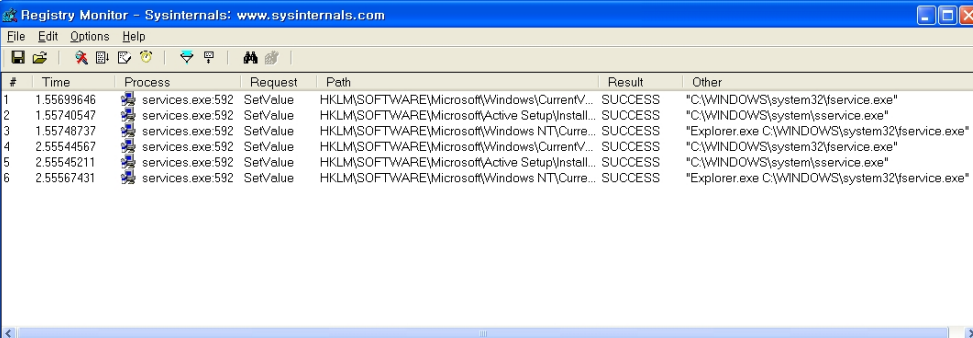
#	Time	Process	Request	Path
1	오후 7:57:06	services.exe:592	OPEN	C:\WINDOWS\services.exe
2	오후 7:57:06	services.exe:592	QUERY INFORMATION	C:\WINDOWS\services.exe
3	오후 7:57:06	services.exe:592	QUERY INFORMATION	C:\WINDOWS\services.exe
4	오후 7:57:06	services.exe:592	QUERY INFORMATION	C:\WINDOWS\services.exe
5	오후 7:57:06	services.exe:592	QUERY INFORMATION	C:\WINDOWS\services.exe
6	오후 7:57:06	services.exe:592	QUERY INFORMATION	C:\WINDOWS\services.exe
7	오후 7:57:06	services.exe:592	QUERY INFORMATION	C:\WINDOWS\services.exe
8	오후 7:57:06	services.exe:592	CREATE	C:\WINDOWS\system32\service.exe
9	오후 7:57:06	services.exe:592	CLOSE	C:\WINDOWS\services.exe
10	오후 7:57:06	services.exe:592	OPEN	C:\WINDOWS\services.exe
11	오후 7:57:06	services.exe:592	QUERY INFORMATION	C:\WINDOWS\services.exe
12	오후 7:57:06	services.exe:592	QUERY INFORMATION	C:\WINDOWS\services.exe
13	오후 7:57:06	services.exe:592	QUERY INFORMATION	C:\WINDOWS\services.exe
14	오후 7:57:06	services.exe:592	QUERY INFORMATION	C:\WINDOWS\services.exe
15	오후 7:57:06	services.exe:592	QUERY INFORMATION	C:\WINDOWS\services.exe
16	오후 7:57:06	services.exe:592	QUERY INFORMATION	C:\WINDOWS\services.exe
17	오후 7:57:06	services.exe:592	CREATE	C:\WINDOWS\system\service.exe
18	오후 7:57:06	services.exe:592	CLOSE	C:\WINDOWS\services.exe
19	오후 7:57:06	services.exe:592	QUERY INFORMATION	C:\WINDOWS\system32\service.exe
20	오후 7:57:06	services.exe:592	OPEN	C:\WINDOWS\system32\service.exe
21	오후 7:57:06	services.exe:592	QUERY INFORMATION	C:\WINDOWS\system32\service.exe
22	오후 7:57:06	services.exe:592	CLOSE	C:\WINDOWS\system32\service.exe
23	오후 7:57:07	services.exe:592	OPEN	C:\WINDOWS\services.exe
24	오후 7:57:07	services.exe:592	QUERY INFORMATION	C:\WINDOWS\services.exe
25	오후 7:57:07	services.exe:592	QUERY INFORMATION	C:\WINDOWS\services.exe
26	오후 7:57:07	services.exe:592	QUERY INFORMATION	C:\WINDOWS\services.exe
27	오후 7:57:07	services.exe:592	QUERY INFORMATION	C:\WINDOWS\services.exe
28	오후 7:57:07	services.exe:592	QUERY INFORMATION	C:\WINDOWS\services.exe
29	오후 7:57:07	services.exe:592	QUERY INFORMATION	C:\WINDOWS\services.exe
30	오후 7:57:07	services.exe:592	CREATE	C:\WINDOWS\system32\service.exe
31	오후 7:57:07	services.exe:592	CLOSE	C:\WINDOWS\services.exe
32	오후 7:57:07	services.exe:592	OPEN	C:\WINDOWS\services.exe
33	오후 7:57:07	services.exe:592	QUERY INFORMATION	C:\WINDOWS\services.exe
34	오후 7:57:07	services.exe:592	QUERY INFORMATION	C:\WINDOWS\services.exe
35	오후 7:57:07	services.exe:592	QUERY INFORMATION	C:\WINDOWS\services.exe
36	오후 7:57:07	services.exe:592	QUERY INFORMATION	C:\WINDOWS\services.exe
37	오후 7:57:07	services.exe:592	QUERY INFORMATION	C:\WINDOWS\services.exe
38	오후 7:57:07	services.exe:592	QUERY INFORMATION	C:\WINDOWS\services.exe
39	오후 7:57:07	services.exe:592	CREATE	C:\WINDOWS\system\service.exe
40	오후 7:57:07	services.exe:592	CLOSE	C:\WINDOWS\services.exe
41	오후 7:57:07	services.exe:592	QUERY INFORMATION	C:\WINDOWS\system32\service.exe
42	오후 7:57:07	services.exe:592	OPEN	C:\WINDOWS\system32\service.exe
43	오후 7:57:07	services.exe:592	QUERY INFORMATION	C:\WINDOWS\system32\service.exe
44	오후 7:57:07	services.exe:592	CLOSE	C:\WINDOWS\system32\service.exe

분석 확인 결과 1초마다 services.exe 프로세스가 fservice.exe, sservice.exe 파일을 생성하고 있음을 알 수 있다.

(Filemon의 해당라인을 더블클릭을 하면 파일 탐색기를 실행하여 자동으로 위치를 검색한다.)

3) Regmon v.7.03

Filemon과 같이 실행파일의 프로세스들이 레지스트리를 통해 어떤 작업을 하는지를 실시간으로 분석할 수 있다. 실시간으로 분석되어지고 있는 파일 목록들을 필터링하여 필요한 정보들로 설정 가능하다.

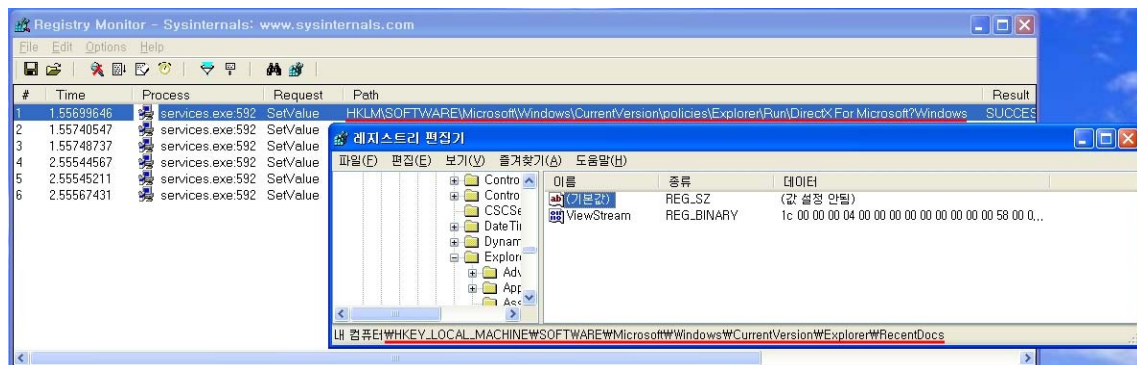


Registry Monitor - Sysinternals: www.sysinternals.com

#	Time	Process	Request	Path	Result	Other
1	1.55699646	services.exe:592	SetValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentV...	SUCCESS	"C:\WINDOWS\system32\service.exe"
2	1.55740547	services.exe:592	SetValue	HKLM\SOFTWARE\Microsoft\Active Setup\Install...	SUCCESS	"C:\WINDOWS\system\sservice.exe"
3	1.55748737	services.exe:592	SetValue	HKLM\SOFTWARE\Microsoft\Windows NT\Curre...	SUCCESS	"Explorer.exe C:\WINDOWS\system32\service.exe"
4	2.55544567	services.exe:592	SetValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentV...	SUCCESS	"C:\WINDOWS\system32\service.exe"
5	2.55545211	services.exe:592	SetValue	HKLM\SOFTWARE\Microsoft\Active Setup\Install...	SUCCESS	"C:\WINDOWS\system\sservice.exe"
6	2.55567431	services.exe:592	SetValue	HKLM\SOFTWARE\Microsoft\Windows NT\Curre...	SUCCESS	"Explorer.exe C:\WINDOWS\system32\service.exe"

위 그림에서는 fservice.exe;sservice.exe를 필터링 한 것이다. 악성코드 프로세스가 1초 간격으로 레지스트리를 변경하는 것을 확인할 수 있다.

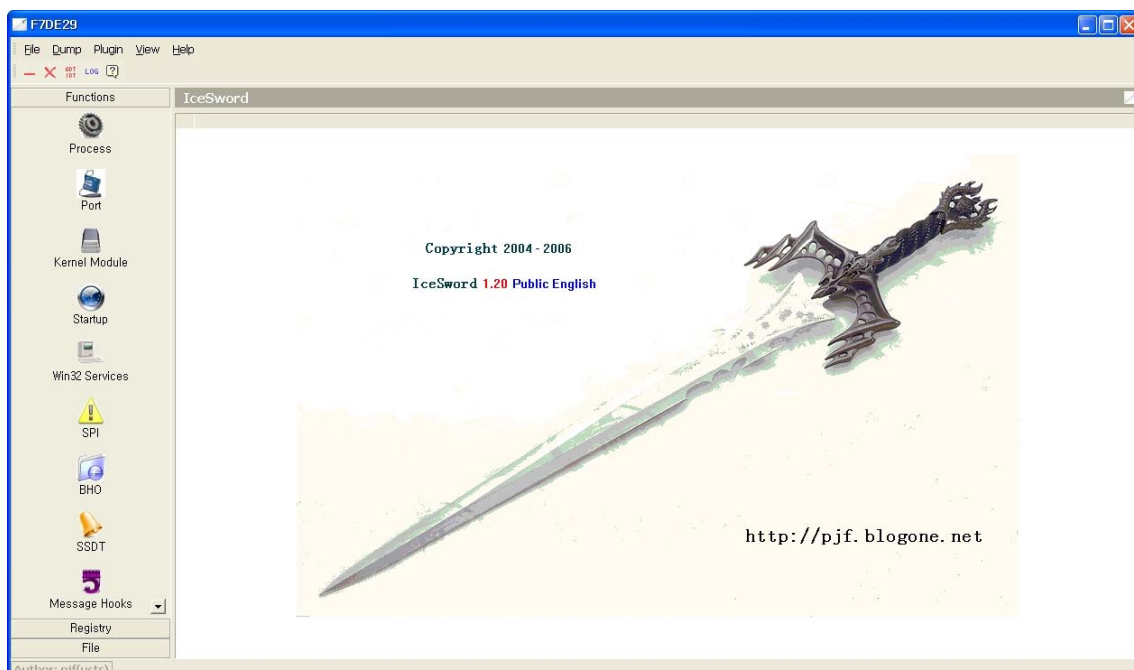
(글자가 보이지 않으면, Options->Font...에서 폰트 크기를 변경해준다.)



하지만 WindowsXP에서 제공하는 레지스트리 편집기로 해당 레지스트리를 확인할 수 없다.

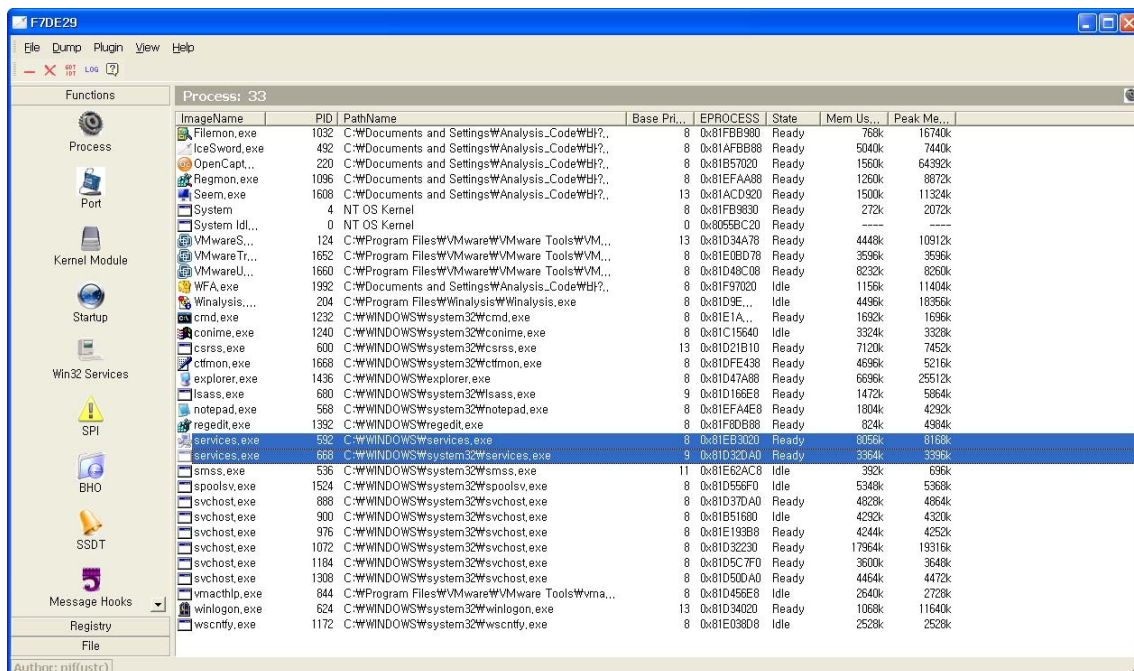
(Regmon의 해당라인을 더블클릭하면 레지스트리 편집기를 실행하여 자동으로 위치를 검색한다.)

4) IceSword v1.20en

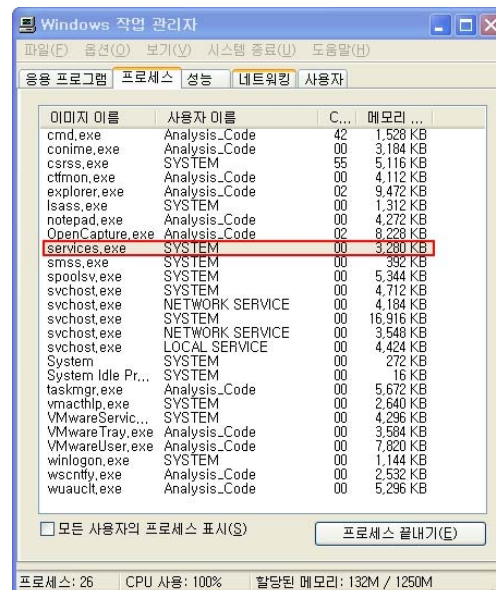


북경과학기술대학교에서 개발한 루트킷 탐색기능이 있는 안티 루트킷 도구이다.

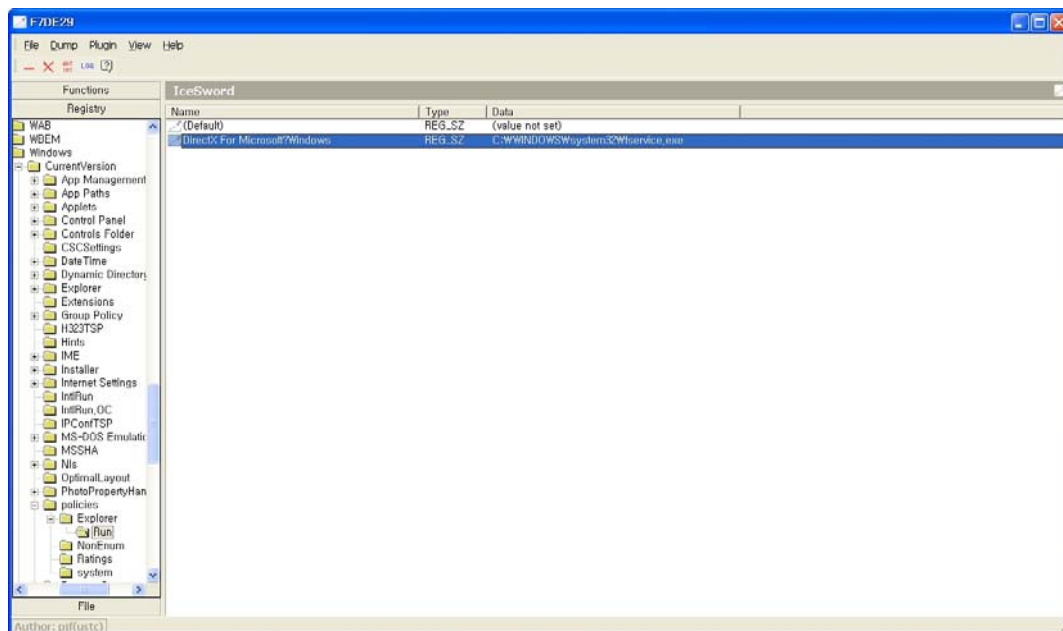
Functions, Registry, File로 구분하여 악성코드를 탐색할 수 있다.



악성코드 실행 후 Icesword로 프로세스(Process)를 확인해 보면 일반 작업관리자 윈도우에서 확인하지 못한 프로세스를 찾을 수 있다.



실제 샘플 악성코드를 실행하여 작업관리자로 프로세스를 찾아보면 위 그림과 같이 악성코드의 프로세스는 찾을 수 없다. 또한 위 그림에 악성코드가 있다고 하더라도 사용자가 강제 프로세스 종지를 할 수 없도록 제약을 걸어둘 수 있다.(시스템 중요 프로세스는 사용자임의 종료를 하지 못하도록 구성되어 있다.)



Icesword는 숨겨진 레지스트리 값을 모두 탐색이 가능하다.

이전 Regmon을 통해 자동으로 레지스트리 편집기 내에서 검색된 레지스트리 값이 확인이 안됐지만 Icesword로 찾을 수 있다.

(그림의 주소 :

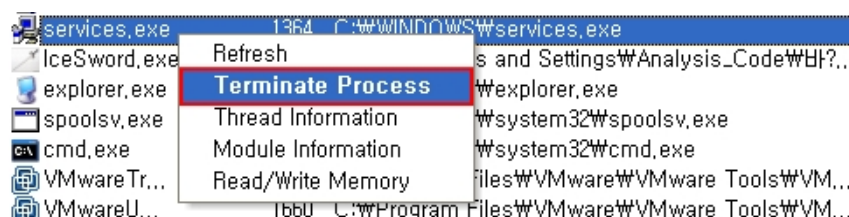
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\DirectXForMicrosoft\Windows)

다. 샘플 악성코드 임의 실행 분석

악성코드와 그 파생 파일, 레지스트리를 임의로 수정, 삭제하여 그 결과를 확인한다.

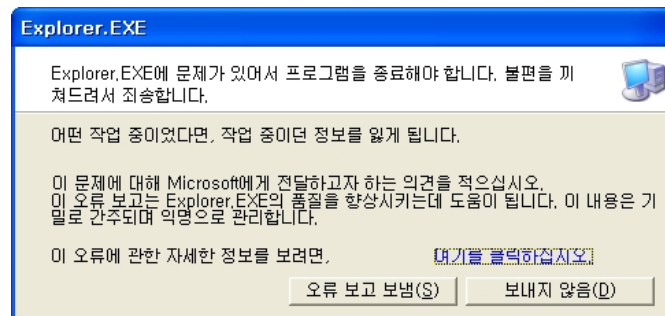
이전 **샘플 악성코드 실행 분석**에서 확인된 1초마다 파일, 레지스트리 생성하는 것을 확인했다. 생성된 파일과 레지스트리가 어떻게 사용되어 지는지 확인해 보아야 한다.

생성된 파일, 레지스트리는 샘플 악성코드의 프로세스가 1초마다 생성하므로 해당파일, 레지스트리를 수정, 삭제 하더라도 1초마다 다시 생성된다. 샘플 악성코드 프로세스를 kill하면 1초마다 생성하는 행동을 멈출 수 있다는 것을 예측할 수 있다.



Icesword 도구로 샘플 악성코드 프로세스를 제거한다. Icesword 도구 내에 표시된 프로세스를 선택하여 Terminate Process를 클릭한다.

샘플 악성코드 프로세스를 제거 하고나면 Explorer 오류 창이 뜨면서 오류 관련 단추 클릭 후 바탕화면이 잠시 깜빡거리는 것을 확인할 수 있다.



이전 레지스트리를 생성할 때 확인했던 explorer관련 레지스트리가 관련 있음을 추측할 수 있다. Explorer를 새로 실행하면서 동시에 System32폴더의 fservice.exe를 실행하고, fservice.exe는 Windows폴더 내부에 services.exe 파일 생성할 것이다.

악성코드가 두 개의 실행파일을 생성시키고 레지스트리를 통해 각각의 실행파일을 특정 패턴에서 실행하도록 구현되어 있다. 어느 하나가 없으면 나머지 파일을 통해 수정되거나 삭제된 파일을 생성하는 구성이다.

이 연결 고리를 끊기 위해 파일 생성, 레지스트리 등록 위치를 찾아서, 샘플 악성코드 프로세스를 제거하는 즉시 삭제해주면 그 연결고리를 끊을 수 있을 것이다.

1) 생성된 파일, 레지스트리

샘플 악성코드 프로세스가 생성하는 파일, 레지스트리를 확인하여 프로세스 재실행을 막아준다.

o Filemon에서 확인된 생성 파일

- C:\WINDOWS\system\sservice.exe
- C:\WINDOWS\system32\fservice.exe

o Regmon에서 확인된 생성 레지스트리

- "C:\WINDOWS\system32\fservice.exe"

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\DirectXForMicrosoft?Windows

- "C:WINDOWSsystemWsservice.exe"
HKLM\SOFTWARE\Microsoft\ActiveSetup\InstalledComponents\{5Y99AE78-58TT-11dW-BE53-Y67078979Y}\StubPath
- "Explorer.exe C:WINDOWSsystemWsservice.exe"
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell

2) 샘플 악성코드 프로세스 제거

샘플 악성코드 프로세스 제거 후 Iceword 도구를 이용하여 1) 생성된 파일, 레지스트리를 삭제하거나 이름을 수정한다.

3) 샘플 악성코드 파생 파일 및 레지스트리 제거

이전 Winalysis 도구로 변경되거나 생성된 파일, 레지스트리 그리고 이외 변경된 속성들을 확인하여 원래의 값으로 변경해준다. 삭제된 파일이나 레지스트리는 외부로 통해 원본 파일을 복사한다.

5. 맺음말

[기술문서]Windows 악성코드 분석 가이드 내용에서는 악성코드 내부 역어셈블리를 통한 리버싱 기술을 서술하지 않았다. 이유인즉, 샘플 악성코드에 대한 상세한 분석이 필요로 하지 않았기 때문이다.

악성코드는 하루에 수십 개에서 수백 개까지 발견되어지고 분석되어진다. 물론 정확한 분석도 중요하지만 새로운 악성코드에 따른 대처가 시급한 것이 우선이다. 또한 한 가지 악성코드 패턴이 여러 종류의 변종 악성코드가 생겨나면서 분석의 반복으로 인한 비효율적 분석이 될 가능성이 있기 때문이다.

하지만 무조건적으로 역어셈블리를 통한 리버싱을 제외하는 것 역시 위험한 행동이다.

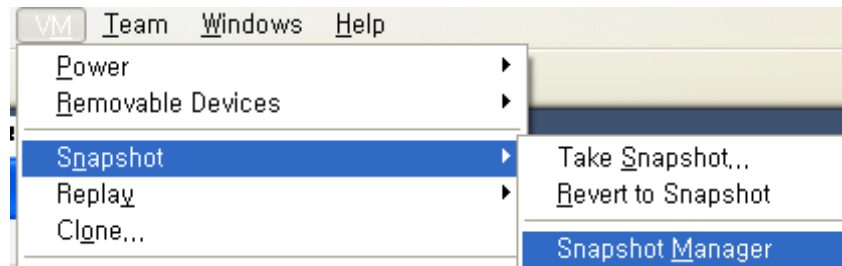
만일 샘플 악성코드의 내부 소스를 확인하고자 한다면 언패킹(참고:부록 B 샘플 악성코드 언패킹)을 한 후 소스를 확인하길 바란다.

상황에 맞게 효율적인 분석을 선택하는 것은 분석가의 몫이며, 그에 따른 정보의 책임 역시 분석가에 있음을 명심해야 할 것이다.

부록 A VMware workstation 스냅샷 설정

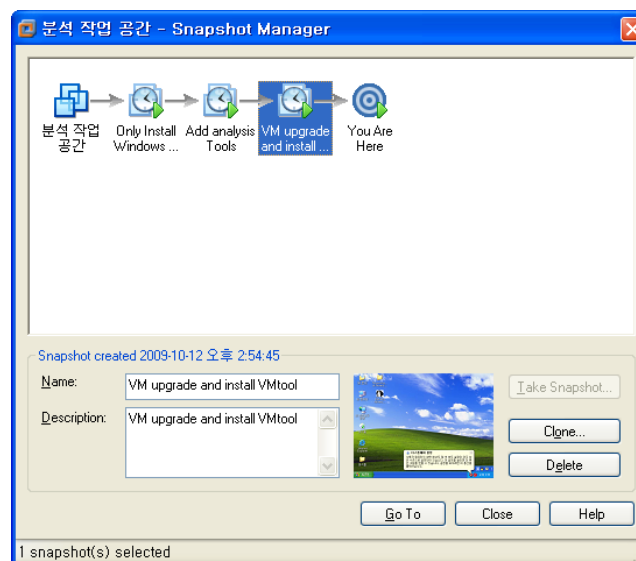
본 가이드에서는 VMware workstation v6.0.1로 가상 컴퓨팅 환경을 구성하였다.

분석환경인 OS와 분석 도구들을 미리 구축을 한 상태에서 VM -> Snapshot를 선택하면 아래 그림과 같이 나올 것이다.



Take Snapshot...를 선택하면 가상 이미지의 현재 상태를 그대로 저장된다.

Snapshot Manager를 선택하면 아래 그림과 같이 관리 윈도우가 나타나며, 기존 스냅샷을 순서대로 배열되어 보여준다.



각각의 스냅샷을 선택하여 Go To 박스를 클릭하면 기존의 설정으로 되돌릴 수 있다.

많은 악성코드들을 분석하기 위해 자신이 사용하는 운영체제, 분석 도구들을 가상이미지를 통해 구성한 후, 위 기능을 통해 스냅샷을 하기를 바란다.

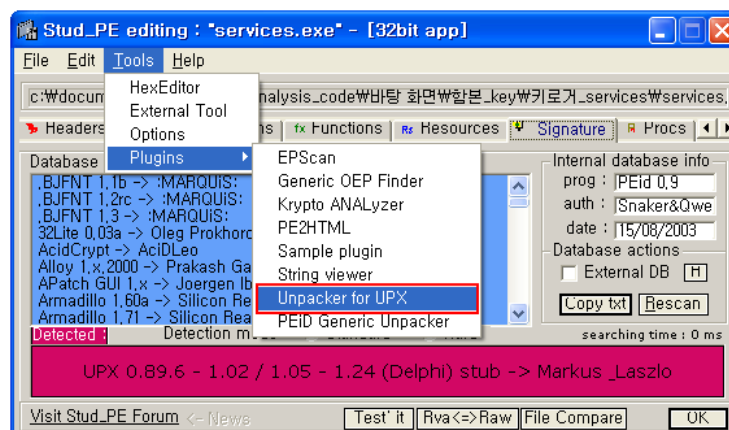
부록 B 샘플 악성코드 언패킹

샘플 악성코드는 UPX패킹이 되어 있다. UPX는 각종 파일의 용량을 줄일 수 있는 패킹기법 중 하나이다. UPX관련 자료들을 찾아보면 쉽게 패킹, 언패킹을 할 수 있는 도구들을 찾을 수 있을 것이다.

본 가이드에서는 Stud_PE를 이용하여 간단하게 언패킹을 했으며, 언패킹된 샘플 악성코드를 역어셈블러나 디버깅 도구를 통해 샘플 악성코드의 세부적인 행동사항들을 분석할 수 있다. (Download: <http://www.cgsoftlabs.ro/>)

Stud_PE 도구를 사용하기 전에 실행파일과 같은 폴더상에 ImpREC.dll 파일을 복사해주길 바란다.

Stud_PE -> Tools -> Plugins -> Unpacker for UPX를 선택하여 샘플 악성코드의 UPX 패킹을 풀어준다.



그 다음 패킹된 샘플 악성코드를 선택해 주면 언패킹 후 성공 메시지 창을 확인 할 수 있다.

언패킹된 파일은 Stud_PE.exe 파일과 동일한 폴더 내에 unpacked.exe 라는 파일이름으로 저장된다.

이름	크기	종류	수정한 날짜
services.exe	342KB	응용 프로그램	2009-05-12 오후 ...
unpacked.exe	2,048KB	응용 프로그램	2009-11-02 오후 ...

UPX 패킹을 통해 약 85% 압축이 되었다는 것을 확인할 수 있다.