악성 프로그램이 사용하는 자동 실행 설정 및 대응 방법

2002. 1. 31
이동련, ryuni@certcc.or.kr

본 문서에서는 윈도우 환경에서 윈도우 시작 시 사용자의 어떠한 행위 없이도 자동으로 실행하도록 설정하는 방법에 대해 설명한다. 프로그램 설치 시 윈도우를 시작 할 때마다 매번 실행하는 백신 프로그램이나 다른 여러 프로그램에서 이러한 설정 방법을 이용하는데 바이러스, 웜, 트로이목마와 같은 악성 프로그램들이 이러한 기능을 악용하고 있어 문제가 되고 있다. 이에 본 문서를 참고하여 윈도우 상의 악성 프로그램을 찾거나 분석하는데 유용하게 이용될 수 있다.

최근 제작되고 있는 거의 모든 웜을 비롯한 바이러스들이 바이러스 파일을 자동으로 실행하도록 설정하고 있어 한번 감염된 시스템에서는 사용자도 모르는 사이에 바이러스와 웜들이 계속적으로 자동 실행된다. 또한 바이러스나 웜은 사용자가 모르게 숨어서 활동하기 때문에 어떠한 액션을 취하지 않고도 자동으로 실행되는 이러한 방법을 선호한다. 이렇게 특정 파일의 실행 없이도 자동으로 실행되도록 설정하는 윈도우 환경에서의 설정방법에 대해 알아보자.

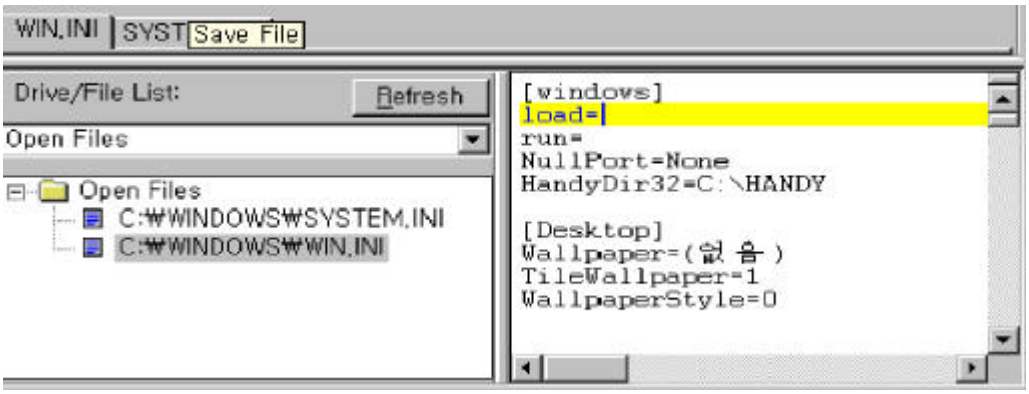
본 문서는 바이러스에 감염 된 경우 백신이 제작되지 않았거나 구할 수 없는 등의 여러 가지 이유에서 치료를 할 수 없을 때 이 문서에서 설명되어진 자동으로 실행되도록 설정 되었는지 여부를 확인하여 추가 설정된 바이러스 부분을 수동으로 삭제하여 치료할 수 있고, 특정 프로그램을 매번 실행시키기 번거로운 경우 필요에 따라 설정하는 등 유용하게 이용할 수 있을 것이다. 단, 레지스트리와 같은 시스템의 중요 정보를 다루므로 잘못 수정하여 시스템을 망가뜨리지 않도록 각별한 주의와 지식이 필요하다.

1. ini 파일을 이용하는 방법

INI 파일은 초기화라는 initialize의 약자로 윈도우나 여러 가지 프로그램의 최초 정보가 들어 있는 텍스트 기반의 크기가 64 KB로 제한되는 윈도우 초기화 파일이다. 주요 ini 파일로는 win.ini, system.ini 등이 있고 이들 파일은 윈도우의 기본 구동 설정을 담고 있으며 사용자에 의해 언제든지 수정 가능하다. 이러한 ini 파일의 설정을 변경하여 윈도우가 시작되는 초기에 특정 파일을 실행 시킬 수 있는데 주로 다음과 같은 세 가지 파일을 이용한다.

① Win.ini

윈도우의 시작 시 C:\WINDOWS(윈도우 98 기준) 폴더에 위치한 Win.ini 파일의 load 와 run 부분에 명시된 경우 해당 파일이 자동 실행된다.



위의 그림과 같이 윈도우 설치 후 디폴트로 "load="과 "run=" 부분은 비어있다. 이 win.ini 파일을 조심스럽게 다루지 않으면 부팅이 되지 않을 수 있으므로 함부로 수정하지 않는 것이 좋다.

☞ **사례**

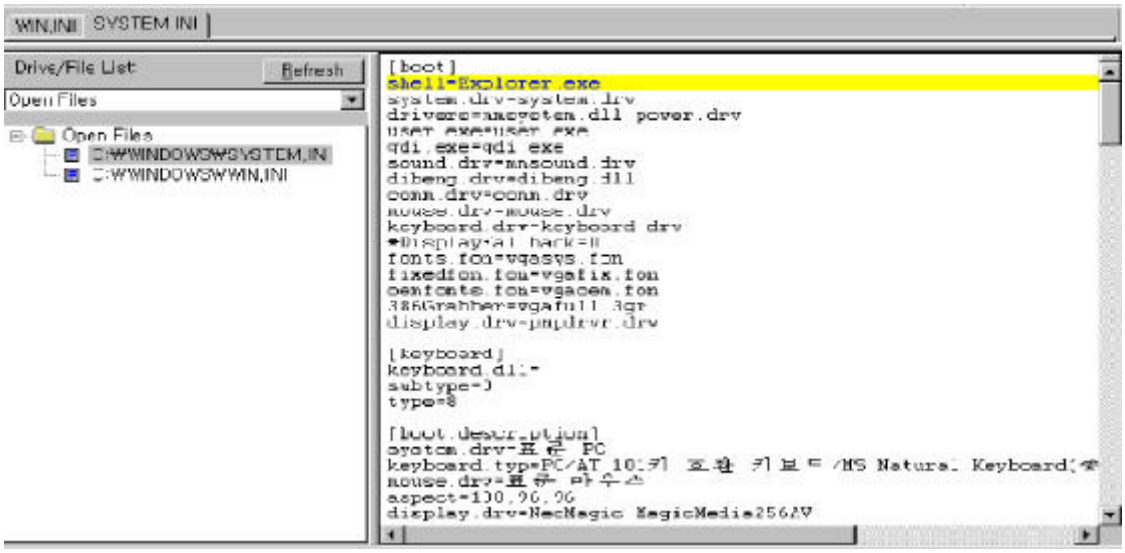
2000년 12월 발견된 화면에 커다란 회오리 모양의 그림을 출력하는 증상을 나타내어 많은 피해를 일으켰던 Hybris 웜에서 win.ini 파일의 [windows]의 run= 부분을 다음과 같이 수정하는 방법을 이용한다.

```
run=C:\Windows\System\amiaamia.exe
```

<※ 생성되는 파일명이 임의로 바뀌어 amiaamia.exe 라는 파일명은 변한다.>

② **System.ini**

윈도우 시작 시 C:\WINDOWS(윈도우 98 기준) 폴더에 위치한 System.ini 파일에서 시스템 정보를 읽어 오는데 이때 다음과 같은 boot 부분에 파일명을 명시한 경우 해당 파일이 자동 실행된다.



윈도우 설치 후 디폴트 설정은 위의 그림과 같다. system.ini 파일 역시 잘못 수정할 경우 아예 윈도우 부팅이 되지 않을 수 있으니 함부로 수정하지 않는 것이 좋다.

☞ **사례**

2001년 9월에 등장하여 최고의 피해를 일으킨 Nimda에서 system.ini 파일을 수정하여 자동 실행되도록 다음과 같이 수정하였다.

```
Shell = explorer.exe load.exe -dontrunold
```

<※ Nimda에 감염된 경우 생성되는 파일명이 load.exe 이다.>

③ wininit.ini

C:\WINDOWS\(윈도우 98 기준) 폴더에 wininit.ini 파일이 존재하면 시작 프로그램에 의해 한번 실행된 후 삭제된다. 예를 들어 wininit.ini 파일의 내용이 다음과 같을 때

```
[Rename]
NUL=c:\windows\picture.exe
```

NUL=c:\windows\picture.exe 문장은 c:\windows\picture.exe를 NUL 로 보낸다는 뜻이며 이것은 삭제한다는 것을 의미한다. 이러한 행동은 은밀하게 일어나므로 사용자는 의식하지 못하는 것이 대부분이기 때문에 악성 코드의 실행 흔적을 감추는 방법으로 많이 사용된다.

☞ **사례**

2001년 제작된 Nimda에서도 wininit.ini 파일을 이용하여 윈도우 재부팅 시 자동으로 삭제되도록 다음과 같이 설정한다.

```
[Rename]
NUL = 실행되었던 경로\파일이름 .EXE

<※ 이때 파일이름은 임의로 정해진다.
```

2. 레지스트리를 이용하는 방법

레지스트리를 이용하는 방법은 최근 나타나는 웜들이 가장 많이 사용하는 방법으로 특히 스크립트 언어로 제작된 경우 아주 손쉽게 레지스트리를 다룰 수 있다. 이러한 레지스트리를 이용한 자동 실행 설정 방법을 알아보기 전에 먼저 레지스트리에 대한 이해가 필요하다.

1) 레지스트리 이해하기

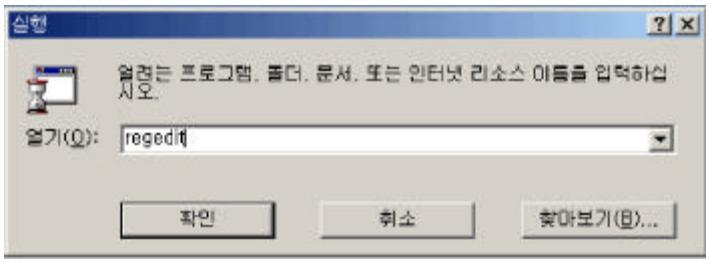
레지스트리란 윈도우 환경설정에 대한 모든 정보가 저장되어있는 일종의 데이터 베이스라 할 수 있다. 윈도우 3.x 버전에서의 INI 파일이 수행했던 역할을 윈도우95부터 레지스트리가 대신하게 되었는데 INI 파일은 인쇄 가능한 파일이므로 텍스트 편집기만 있으면 초기화 설정을 바꿀 수 있다. 파일의 크기는 64KB로 제한되어 PC에 프로그램을 설치하면 win.ini 파일이 더욱 길어져 결국 설치 할 수 있는 프로그램의 수가 제한된다. 또한 프로그램이 첫 32KB를 초과하는 엔트리를 제대로 읽지 못하는 경우가 발생하여 64KB라는 제한에도 불구하고 사용하는 모든 프로그램이 제대로 실행될 수 있도록 하려면 사용하는 ini 파일의 크기가 32KB을 넘지 못하게 된다.

INI 파일에 저장되어 있는 모든 정보는 비구조적이고 섹션 머리글과 추가 텍스트만 몇 줄 들어 있는 구조이다. 이로 인하여 프로그램 속도가 느려지는 것을 막기 위해 소프트웨어 개발자들은 각 프로그램에 대해 별도의 IN파일을 만들기 시작했다. 그 결과, 테스트를 끝낸 각각의 프로그램은 윈도우 디렉토리에 사용하지 않는 IN파일을 하나씩 남기게 되어 사용자들은 구성이 엉망이 된 파일 구조를 관리해야 하게 되었고 각 INI 파일은 컴퓨터 전반에 걸쳐 영향을 미치는 설정을 초기화하므로 단일 IN파일에 사용자에 따라 다른 정보를 저장하는 것이 어려워졌다.

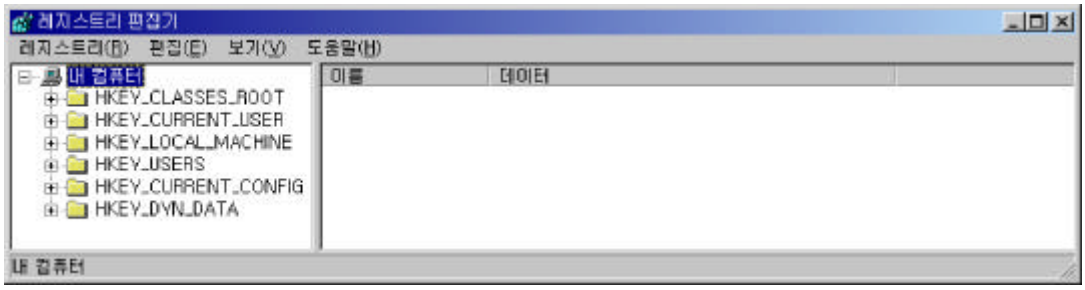
이러한 문제점은 Windows 3.1에서 더욱 부각되어 개발자들은 Windows 3.1에서 OLE기능을 사용할 때 필요한 정보를 저장하기 위해 다른 구조를 만들게 되었으며 그것이 레지스트리이다. 다시 말해 레지스트리는 한마디로 '윈도우가 실행되는데 필요한 모든 정보가 등록되

어 있는 데이터베이스'로 PC에 설치된 하드웨어를 비롯하여 소프트웨어, 사용자, 네트워크 설정 등에 관한 드라이버의 설치 위치, 환경 변수 등 모든 정보가 기록되어 있는 중요한 요소로 레지스트리 파일이 손상되면 시스템이 다운되거나 부팅조차 할 수 없는 심각한 문제가 발생한다.

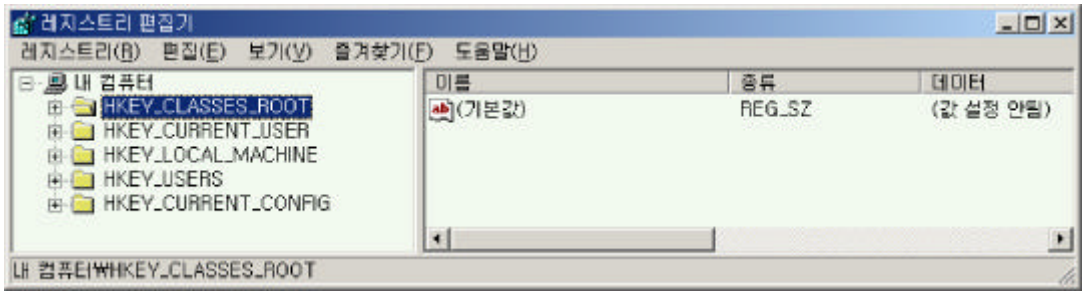
레지스트리의 구조를 구경하기 위해서는 레지스트리 편집기를 이용하는데 시작메뉴의 실행에서 "regedit"라고 입력한 후 확인 버튼을 클릭하면 편집기가 실행된다.



윈도우 98의 경우 편집기를 실행하면 다음 그림과 같이 내 컴퓨터 안에 6개의 폴더가 존재하는데



윈도우 2000에서는 HKEY_DYN_DATA 가 없어지고 5개의 폴더로 이루어져 있다.



레지스트리는 트리구조로 되어 있으며 각 폴더들을 키(key)라고 하고 키 이름과 키 데이터로 구성된다.

이제부터는 전체 레지스트리를 구성하는 서브 레지스트리에 대하여 간략히 살펴보자.

① **HKEY_CLASSES_ROOT**

이 곳에 저장되는 것은 OLE 데이터와 파일의 각 확장자에 대한 정보, 각 파일과 프로그램간의 연결에 대한 정보가 들어 있다. HKEY_CLASSES_ROOT안에는 파일의 확장자들에 대한 서브 트리로 구성되는데 일반적으로 각 확장자는 파일 타입과 연결되어 있고, 왼쪽 패널의 한 파일 타입을 선택하면 오른쪽 패널에 그 타입의 파일이 어떤 프로그램과 연결되어 있는지 알 수 있다.

② **HKEY_CURRENT_USER**

윈도우가 설치되어 있는 컴퓨터의 환경에 대한 설정이 담겨 있는 곳으로 하나의 윈도우를 여러명이 사용할 경우, 사용자들이 각각에 대한 ID 와 패스워드를 이용하여 윈도우에 접속했을 때 접속한 사용자가 맞추어 놓은 설정을 반영하기 위한 곳이다. 각각의 사용자가 자신의 세팅을 설정하면 그 정보는 HKEY_USER에 저장된다.

③ **HKEY_LOCAL_MACHINE**

컴퓨터에 설치된 하드웨어와 하드웨어를 구동 시키는데 필요한 드라이버나 설정 사항에 관련된 정보를 모아 둔 곳이다. 프린터와 화면 설정 등과 같이 컴퓨터를 켜고 윈도우를 부팅할 시에 필요한 설정, 컴퓨터에 설치된 하드디스크 드라이브나 플로피 드라이브, 플러그앤 플레이를 지원하는 하드웨어에 관한 정보, 디바이스 드라이버나 시스템에서 사용하는 소프트웨어에 관한 전반적인 정보를 담고 있다.

④ **HKEY_USER**

HKEY_CURRENT_USER에 저장된 정보와 데스크 탑 설정, 네트워크 연결 등의 정보가 저장되어 있으며 USER.DAT에 저장한다. 즉, 윈도우를 사용하는 사람이 한사람일 경우 모든 설정 사항이 HKEY_CURRENT_USER의 내용과 일치하게 된다.

⑤ **HKEY_CURRENT_CONFIG**

레지스트리 중에서 가장 단순한 부분으로 HKEY_LOCAL_MACHINE에 서브로 존재하는 Config의 내용이 담겨 있다. 즉, 디스플레이와 프린터에 관한 설정만을 볼 수 있다.

⑥ **HKEY_DYN_DATA**

윈도우 2000에서는 없어진 레지스트리로 자주 사용하는 하드웨어 장치의 정보를 따로 저장하는 윈도우의 모니터 역할의 정보가 담겨있다.

2) 레지스트리를 이용한 자동 실행 설정 방법

윈도우의 시작 시 자동 시작 되는 레지스트리의 위치는 다음과 같으므로 원할 경우 해당 레지스트리에 파일을 등록한다.

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices]
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce]
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices]

다음의 레지스트리 값은 실행 파일 쉘들의 디폴트 값이다.

[HKEY_CLASSES_ROOT\exefile\shell\open\command] @="\"%1\" %*"
[HKEY_CLASSES_ROOT\comfile\shell\open\command] @="\"%1\" %*"
[HKEY_CLASSES_ROOT\batfile\shell\open\command] @="\"%1\" %*"
[HKEY_CLASSES_ROOT\htafile\Shell\Open\Command] @="\"%1\" %*"
[HKEY_CLASSES_ROOT\piffile\shell\open\command] @="\"%1\" %*"
[HKEY_LOCAL_MACHINE\Software\CLASSES\batfile\shell\open\command] @="\"%1\" %*"
[HKEY_LOCAL_MACHINE\Software\CLASSES\comfile\shell\open\command] @="\"%1\" %*"
[HKEY_LOCAL_MACHINE\Software\CLASSES\exefile\shell\open\command] @="\"%1\" %*"
[HKEY_LOCAL_MACHINE\Software\CLASSES\htafile\Shell\Open\Command] @="\"%1\" %*"
[HKEY_LOCAL_MACHINE\Software\CLASSES\piffile\shell\open\command] @="\"%1\" %*"

여기서 각 키들은 디폴트로 "%1 %*" 값을 갖는데 이들을 "server.exe %1 %*" 로 변경할 경우 exe, com, bat, hta, pif 파일들의 실행 시 매번 server.exe 파일이 자동으로 실행된다.

☞ **사례**

2001년 7월 발생하여 많은 피해를 일으켰으며 특히 정보유출로 인한 사회적인 피해를 초래한 Sircam의 경우 다음과 같이 윈도우가 시작될 때마다 웜이 실행되고 exe 파일이 실행될 때마다 매번 자동 실행되도록 하는 두 가지 방법의 레지스트리 설정을 이용한다.

다음과 같이 설정하여 윈도우 시작마다 자동 실행되고

> HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
> 에 Driver32=C:\Windows\System\scam32.exe 값 추가

exe 파일이 실행될 때 마다 자동 실행된다.

HKEY_CLASSES_ROOT\exefile\shell\open\command 에 C:\recycled\sirc32.exe "%1" %* 값 설정

Sircam과 같이 레지스트리를 설정하는 방법을 이용하는 웜은 쉽게 찾을 수 있을 것이다.

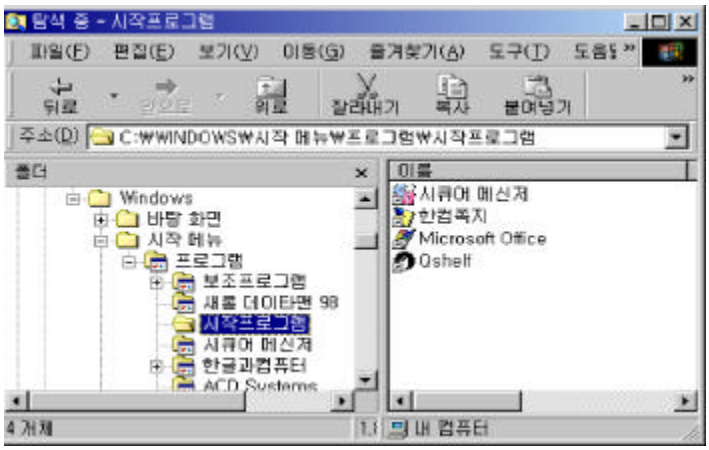
3. 자동 시작 폴더를 이용하는 방법

윈도우의 재시작 시 이 폴더 안에 있는 모든 프로그램들은 자동으로 실행된다. 윈도우에서 이러한 자동 시작 폴더는 다음과 같으며 여기서는 한글 윈도우와 영문윈도우 경우만 명시한다.

◆ Win 98에서

한글 윈도우 : C:\WINDOWS\시작 메뉴\프로그램\시작프로그램

영문 윈도우 : C:\windows\start menu\programs\startup



그림에서 보는 바와 같이 시큐어 메신저나 한컴 쪽지 등과 같은 프로그램들이 자동시작 폴더에 위치시켜 윈도우 시작 시 마다 자동으로 실행되도록 설정한다.

◆ Win 2000에서

한글 윈도우 : C:\Documents and Settings\Administrator\시작 메뉴\프로그램\시작프로그램

영문 윈도우 : C:\Documents and Settings\Administrator\start menu\programs\startup

이러한 폴더는 다음과 같이 레지스트리에 등록되어 있어 이러한 기능이 제공되는 것이다.

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders에

서 Startup의 데이터 값으로 한글 윈도우 경우 C:\WINDOWS\시작 메뉴\프로그램\시작프로그램 로 설정되어 있을 것이다.

이러한 방법은 임의의 프로그램이 자동 시작 폴더에 특정 파일을 복사함으로써 윈도우 시작마다 자동으로 동작하도록 설정할 수 있는 쉬운 방법이다.

4. bat 파일을 이용하는 방법

배치파일의 기능은 순차적이고 반복된 동일한 과정을 몇 개의 혹은 수십, 수백 개의 연관된 명령어를 하나의 파일로 집약하여 그 하나의 파일만 실행함으로써 원하는 작업 과정을 수행하도록 만든 것이다. 텍스트 형식으로 이루어져 있으며, 응용 프로그램 실행 시 관련파일의 실행 순서와 옵션을 지정한다. bat는 도스용 파일로 윈도우에서는 자주 사용되지는 않으나 autoexec.bat 파일과 같이 시스템 부팅 시 중요하게 이용되기도 한다.

① Autoexec.bat

C:\ 에 위치한 BAT 파일인 Autoexec.bat은 운영체제의 사용 환경을 설정하는데 사용되는 파일로 프롬프트의 형식이나 기본 경로를 설정하며 여러 가지 유틸리티의 환경 설정을 부팅과 동시에 자동으로 이루어지도록 한다. 부팅 시 필요한 중요한 파일로 악성 프로그램에서 사용하는 BAT 파일 중 가장 많이 이용되며 이 파일에 등록된 경우 윈도우 시작 시 도스레벨에서 매번 자동 실행된다. 웜이나 바이러스와 같은 악성 코드들이 C 드라이브를 삭제하는 등의 명령을 autoexec.bat 파일에 삽입하여 심각한 피해증상을 나타내는데 주로 사용된다.

☞ **사례**

2002년 1월 발견된 Gigger 웜은 C 드라이브의 모든 파일을 삭제하는 증상을 갖는데 이때 autoexec.bat 파일을 이용한다. 다음과 같은 명령어를 추가하여 C 드라이브를 포맷하며 비슷한 방법으로 사용하는 웜들이 많이 존재한다.

```
ECHO y|format c:
```

② Winstart.bat

C:\WINDOWS(윈도우 98 기준) 폴더에 위치한 winstart.bat 파일은 일반 BAT 파일과 같은 기능을 하며 윈도우 시작마다 자동 실행된다.

☞ **사례**

2001년 8월에 발견된 Cuerpo와 같은 웜에서 winstart.bat 파일을 생성하여 레지스트리 파일을 생성하기도 하며 2001년 7월 국내에서 제작된 Reality 에서는 다음과 같이 특정 파일을 생성하여 실행하도록 설정한다.

```
@echo off
debug < c:\Windows\System\System.dll > nul
copy c:\Command32.com c:\Windows\Cammand\Command32.com
c:\Windows\Cammand\Command32.com
```

5. 응용 프로그램 ICQ의 설정을 이용하는 방법

특정 응용 프로그램을 설치하는 경우 응용 프로그램에 사용에 맞게 자동으로 실행되도록 설정하는 경우가 있다. 악성 프로그램에서 이러한 점을 이용하여 다른 응용 프로그램에서 설정된 사항을 사용하기도 하는데 본 문서에서는 세계적으로 많이 사용되고 있는 대표적인 채팅 프로그램 ICQ의 설정 방법을 이용하는 것에 대하여 알아본다.

시스템에 채팅 프로그램 ICQ의 설치 시 다음 레지스트리에 등록된 모든 값은 ICQNET 이 인터넷 연결을 확립할 경우 실행된다.
이때 다음과 같은 값을 등록하여 자동 실행되도록 만들 수 있다.

```
[HKEY_CURRENT_USER\Software\Mirabilis\ICQ\Agent\Apps\test]
    "Path"="test.exe"
    "Startup"="c:\\test"
    "Parameters"=""
    "Enable"="Yes"
```

☞ 사례

2001년 1월에 발견된 Leave에서 다음과 같은 설정을 이용한다.

```
HKEY_CURRENT_USER\Software\Mirabilis\ICQ\Agent\Apps\에

icqrun    C:\WINDOWS\regsv.exe 값 추가
```

6. 파일 확장자 숨김 방법

바이러스나 웜과 같은 악성 프로그램들이 지능화 되면서 여러 가지 방법들을 이용하는데 확장자명이 제대로 보이지 않도록 하여 실행파일을 그림 파일이나 일반 문서파일로 혼동할 수가 있다. 사용자의 잘못된 설정이나 디폴트 설정을 그대로 이용하여 이러한 결과를 초래하게 되는데 파일 확장자가 보이지 않도록 설정되어 있는 것을 모두 해제하여 실수를 막을 수 있도록 해야한다. 본 문서에서는 윈도우 설치 시 디폴트로 설정되어 확장자명이 보이지 않도록 하는 두 가지 방법을 살펴본다.

① 레지스트리 설정

다음과 같이 레지스트리값을 설정할 경우

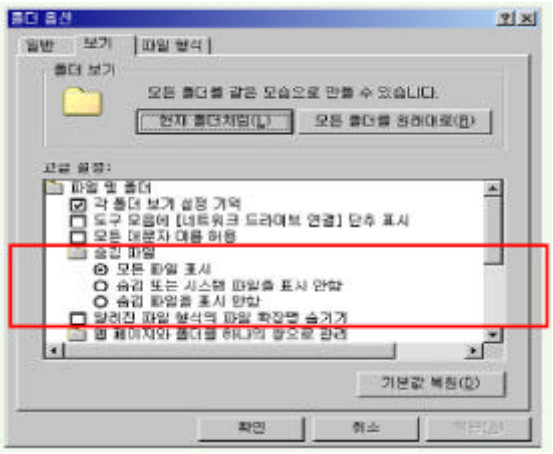
[HKEY_LOCAL_MACHINE\Software\CLASSES\ShellScrap]
(기본값)="스크랩 개체" "NeverShowExt"=“”

SHS 파일의 확장자가 보이지 않게 된다. NeverShowExt 키는 파일의 확장자를 숨기는 기능을 갖는데 이 경우는 .SHS 파일이 보이지 않게 된다. 이는 Girl.jpg.shs 파일이 존재할 경우 마치 그림 파일 Girl.jpg인 것처럼 위장할 수 있다는 것이다.
따라서 사용자는 NeverShowExt 키에 등록된 내용은 전부 삭제하여 모든 확장자명이 숨겨지지 않도록 해야한다.

② 탐색기 설정

탐색기에서 알려진 확장자명이 보이지 않도록 숨기는 기능이 제공되는데 이를 해지하여 모든 확장자명이 정확히 보이도록 해야한다.

그림과 같이 탐색기를 실행하여 도구 메뉴의 폴더옵션에서 그림과 같이 알려진 파일 형식의 파일 확장명 숨기기 선택을 해지 한 후 현재 폴더처럼 버튼을 클릭 한 후 확인 하여 종료한다. 추가적으로 모든 파일의 숨김 속성을 이용하여 일부 파일이 보이지 않을 수 있는데 숨김 파일도 표시되도록 한다.



☞ **사례**

2001년 2월 발견된 Anna Kournikova는 메일로 전파 시 첨부 파일명이 Anna Kournikova.jpg.vbs 이다. 이때 확장자명이 보이지 않도록 설정되어 있는 경우 Anna Kournikova.jpg 까지만 보이게 되므로 그림파일로 혼동하도록 유도한 것이다.

7. 참고 문헌

http://www.tlsecurity.net/auto.html
http://www.cert.org/incident_notes/IN-2000-07.html
http://www.nbinside.com/study/090.htm
http://myang2.hihome.com/right3.htm
http://members.tripod.lycos.co.kr/j2814/extention.htm
http://my.dreamwiz.com/bicter/study/boot/boot_9.htm
http://v3.netpia.com/newvirusdetail.asp?virus_id=652
http://securityresponse.symantec.com/avcenter/venc/data/pwsteal.coced240b.tro.html