3. USB 이동식 저장장치를 이용하여 전파되는 악성코드 분석

1. 개 요

최근 USB 이동식 저장장치를 통하여 전파되는 악성코드에 대한 감염피해가 증가하고 있어 주의가 필요하다. 이번에 확인된 ntion.exe 악성코드는 감염 시, 특정 사이트에 접속하여 추가 악성코드를 다운로드하는 Dropper 기능을 수행한다. 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.

2. USB 이동식 저장장치를 이용한 악성코드

■ 전파 방법

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

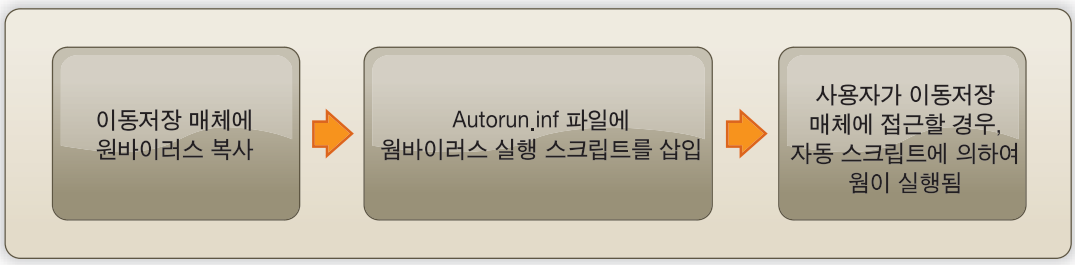
윈도우의 autorun.inf 기능 소개

윈도우에서는 CD나 USB를 이용한 이동저장매체가 시스템에 연결될 때 autorun.inf 파일을 이용하여 특정 프로그램을 자동으로 실행시킬 수 있다.

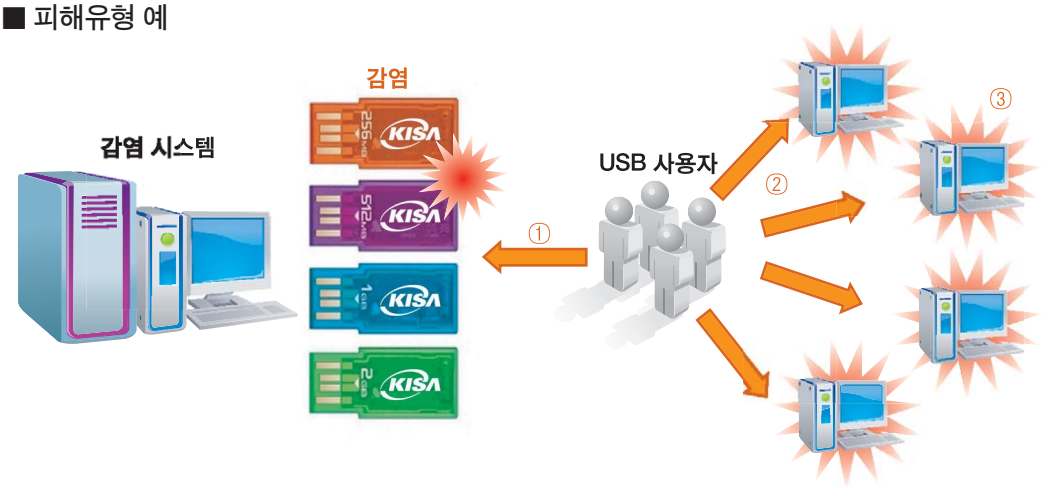
⊙ 일반적으로 사용자가 CD, 또는 USB 이동식 저장장치를 통하여 배포된 프로그램을 자동으로 설치할 수 있도록 하기 위함

이 기능을 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 감염된다.



■ 피해유형 예



[그림 1] 이동식 디스크를 이용한 악성코드 전파

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

3. 상세분석

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.

■ 악성코드 Dropper 기능

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

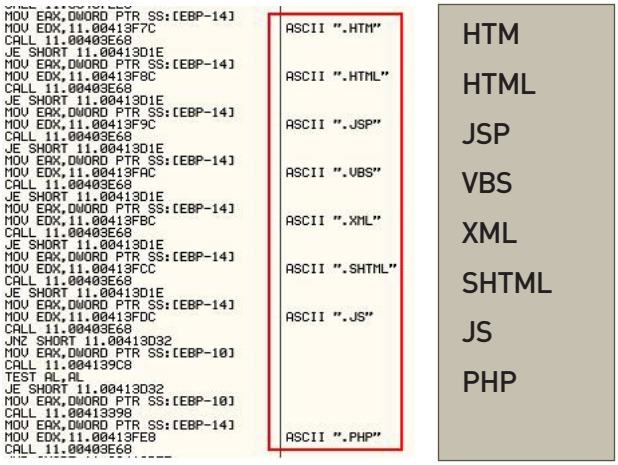
```
ASCII "hTTp://www.[redacted]down1/test.exe"
ASCII "hTTp://www.[redacted]down1/1.exe"
ASCII "hTTp://www.[redacted]down2/2.exe"
ASCII "hTTp://www.[redacted]down12/12.exe"
```

[그림 2] 악성코드로 의심되는 실행파일들에 대한 정보

⊙ 08.01.14 현재, 해당 사이트들은 이미 차단조치 되어 접속이 불가함

■ 웹 페이지 파일에 스크립트 코드삽입

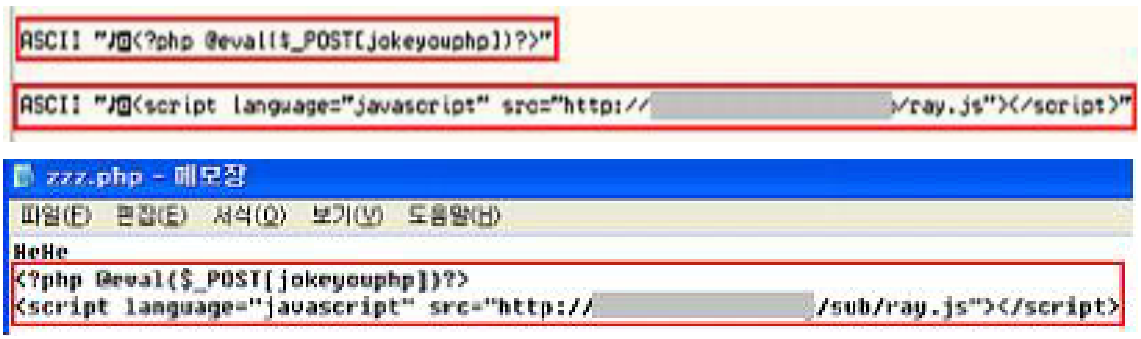
웜은 감염된 시스템의 모든 디렉토리를 검색하여 웹페이지 파일에 악성 스크립트 코드를 삽입한다. 웹 서버가 감염될 경우, 서비스 중인 웹 페이지 내에 악성 스크립트 코드가 삽입되어 해당 웹서버를 방문하는 사용자들에게 피해를 발생시킬 수 있다.



[그림 3] 감염된 시스템에서 검색하는 확장자 목록

[그림 4] 삽입된 자바스크립트 코드

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



[그림 5] 삽입된 PHP 및 자바스크립트 코드

■ 파일 생성

웜은 자신을 전파하기 위하여 이동식디스크에 "RECYCLER.EXE"라는 이름으로 자신을 복사하고 "autorun.inf" 파일에 의해 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 경고 창을 지속적으로 발생시켜 시스템 사용 시 불편을 초래한다.

[그림 7] 이동식 디스크가 연결되지 않은 경우

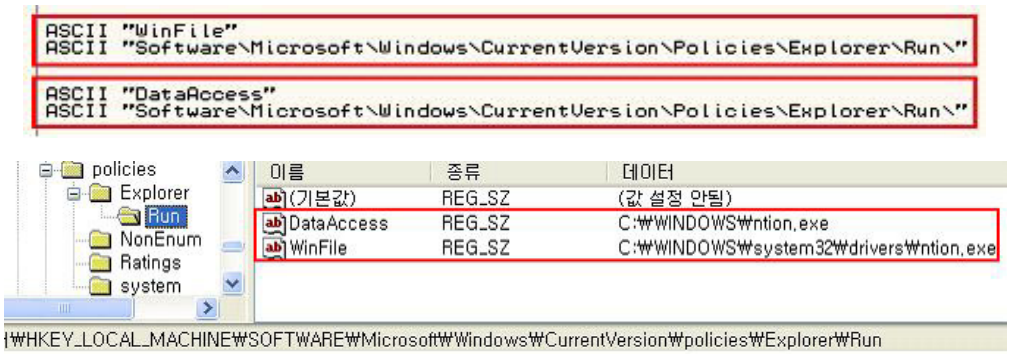
또한, 웜은 감염된 시스템에 자신의 복사본인 "ntion.exe"와 Explorer 프로세스에 인젝션 되는 "ntion.dll"을 생성한다.

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

[그림 8] 감염된 시스템에 생성되는 악성코드들

■ 레지스트리 변경

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

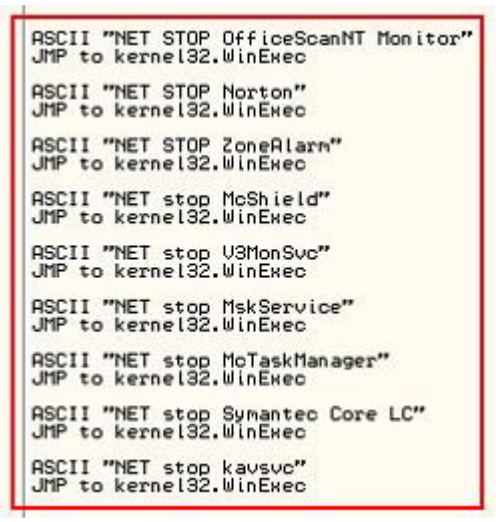


- HKLM/SOFTWARE/Microsoft/Windows/CurrentVersion/policies/Explorer/Run/DataAccess (C:\Windows\ntion.exe)
- HKLM/SOFTWARE/Microsoft/Windows/CurrentVersion/policies/Explorer/Run/WinFile (C:\Windows\system32\drivers\ntion.exe)

[그림 9] 재부팅 후 활동을 위한 Explorer 레지스트리 등록

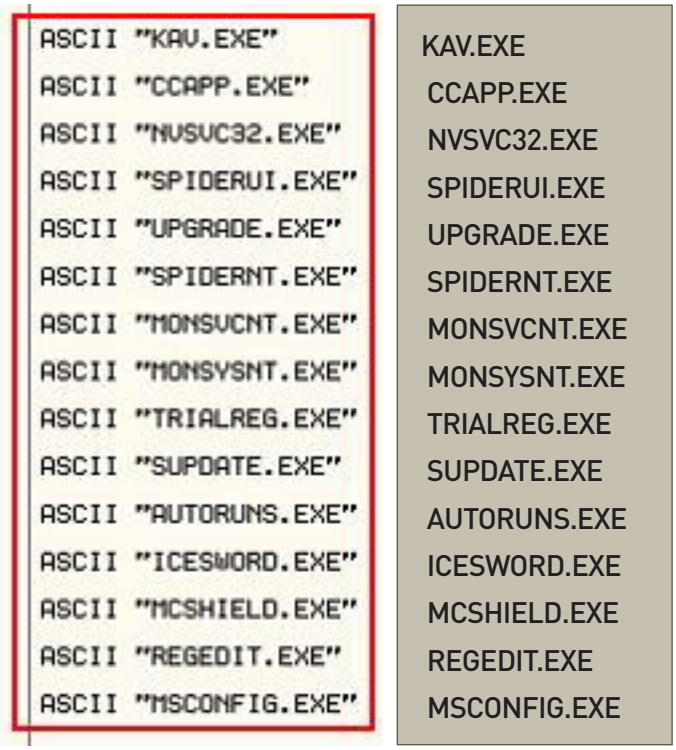
■ 자기보호 기능

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.



- OfficeScanNT
- Norton
- ZoneAlarm
- McShield
- V3MonSvc
- MskService
- McTaskManager
- Symantec Core LC
- kavsvc (Kaspersky)

[그림 10] 안티 바이러스 프로세스의 종료



[그림 11] 특정 프로그램 검색

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

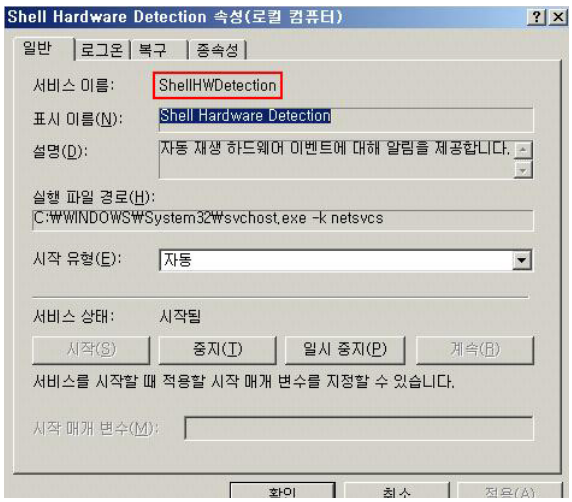
[그림 12] 폴더속성 변경

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

4. 예방방법 (USB 저장장치 자동실행 방지)

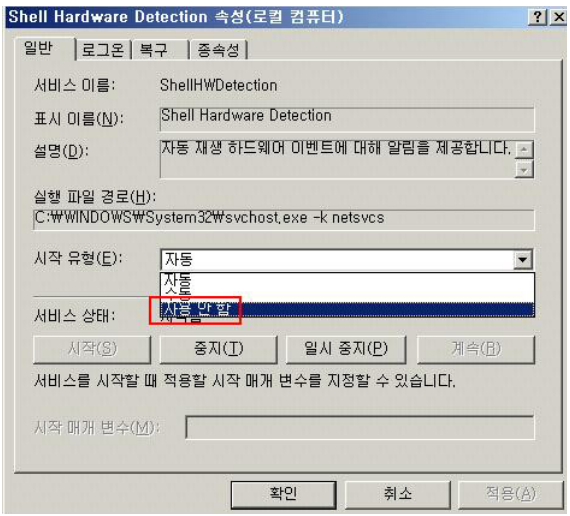
윈도우즈의 특정 서비스 항목을 사용하지 않는 것으로 감염된 이동식 디스크에서 악성코드가 실행되는 것을 막을 수 있다.

① 시작→설정→제어판→성능 및 유지관리→관리도구→서비스로 들어가 'Shell Hardware Detection' 을 선택



[그림 13] ShellHWDetection 서비스의 속성

② ①의 '일반탭' 에서 시작유형을 사용안함으로 설정한다.

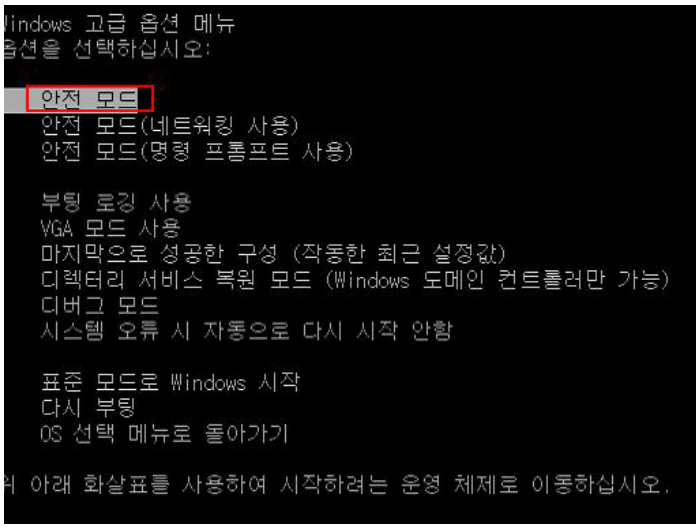


[그림 14] ShellHWDetection 서비스의 속성변경

③ 재부팅 한다.

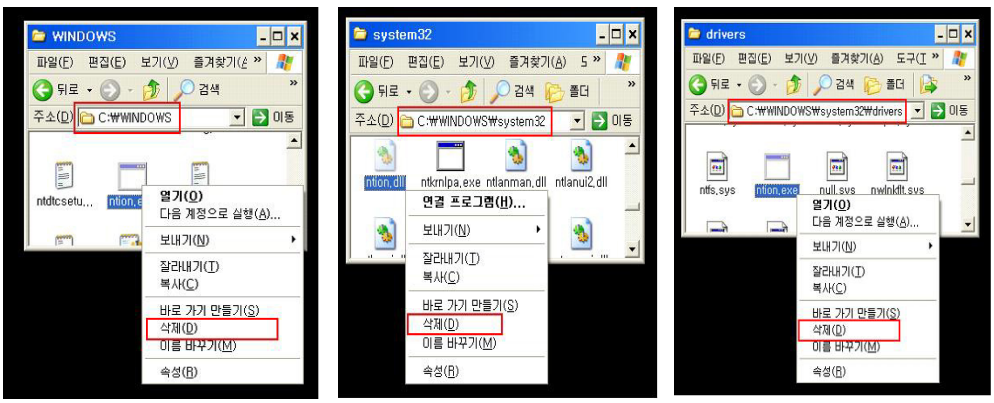
5. 감염 시 조치방법

① 부팅 시 F8을 눌러 안전모드를 선택한다.



[그림 15] 안전모드 선택 화면

② 아래 윈도우즈 하위 폴더에서 악성코드 파일들을 삭제한다.

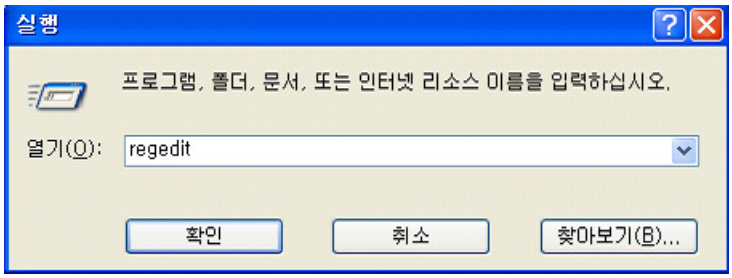


폴더에서 삭제할 파일들

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

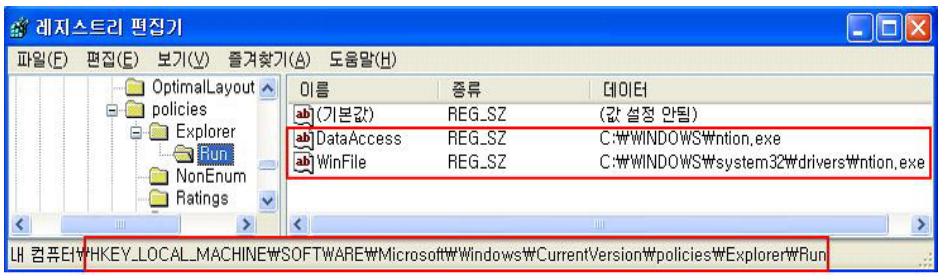
[그림 16] 악성코드 삭제

③ “시작” → “실행” 에서 regedit 를 입력한다.



[그림 17] 레지스트리 편집기 실행

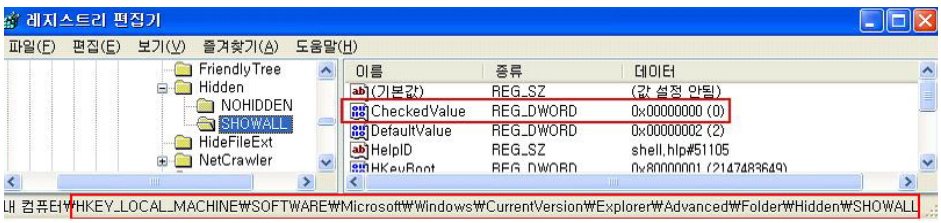
④ 아래의 레지스트리 항목들을 삭제 한다.



[그림 18] 레지스트리 삭제

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\policies\Explore\Run\DataAccess
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\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.

⑤ 재부팅 한다.