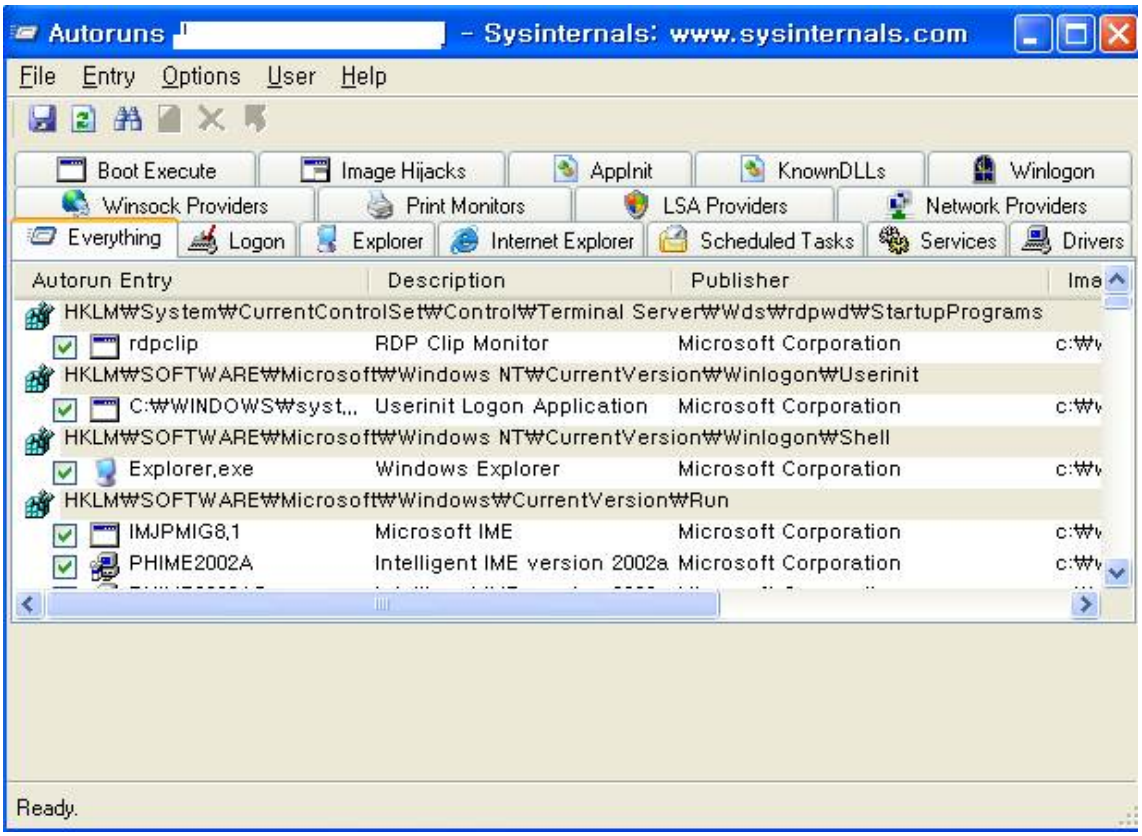
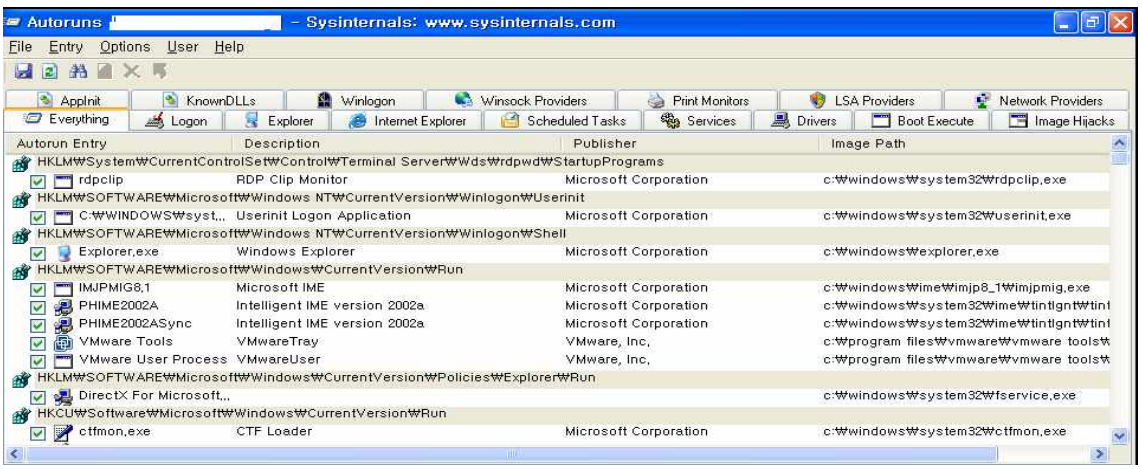
Autoruns란? sysinternals이라는 제작사에서 만든 프리웨어로 컴퓨터 내에서 자동으로 실행되게 설정되어있는 모든 시작프로그램을 보여주는 툴입니다.
프로그램의 다운로드는 제작사 사이트인 http://www.sysinternals.com/ 에서 다운로드가 가능합니다.
주의할 점은 Autoruns 프로그램은 시스템에 영향을 미치므로 사용 시 주의가 필요하며, 아울러 Autoruns 관련 파일을 함부로 삭제하지 않도록 해야 합니다.

Autoruns의 각종 기능

1. autoruns.exe 파일을 실행시키면 다음과 같은 좁은 화면이 표시됩니다.



와이드모니터나 최대화를 통해서 넓게 볼 수도 있습니다.



각 항목별로 의미하는 내용을 알아보겠습니다.

- Autorun Entry : 시작프로그램으로 등록된 항목을 표시합니다.
- Description : 어떠한 종류의 시작프로그램인지를 표시합니다.
- Publisher : 프로그램의 공급자를 표시합니다.
- Image Path : 프로그램의 드라이브 내 경로를 표시합니다.

2. 처음 설정된 화면은 모든 항목을 표시하게 되어있습니다. 중요한 운영체제의 항목도 표시가 되게 되있는데, 이것은 설정에서 변경이 가능합니다.

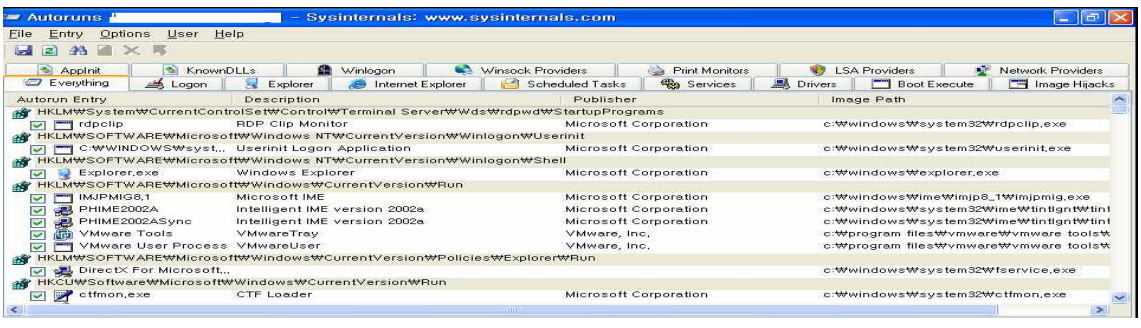
[Option]을 선택 -> [Hide Microsoft Entries]를 체크 -> F5나 [File]에서 [Refresh]를 선택

다음과 같이 중요 운영체제의 항목이 사라진 걸 확인 할 수 있습니다.

이 기능은 중요 운영체제를 숨김으로서 실수를 미연에 방지할 수 있으나, 운영체제로 위장한 악성코드를 찾아내는데에는 용이하지 못하므로 악성코드 탐색을 목적으로 하신다면 안하실 것을 권장드립니다.

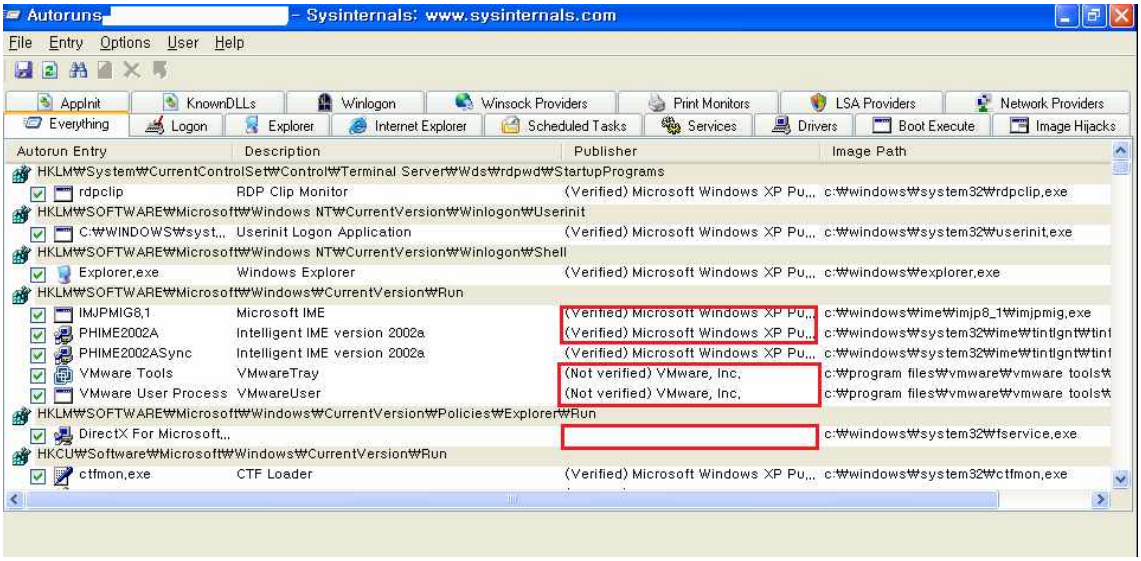
3. 이번에는 Autoruns에서 제공하는 Verify(verify digital signatures) 검증기능에 대해 소개해드리겠습니다. sysinternals는 마이크로소프트웨어 내에 속해있는 제작사로 마이크로소프트웨어사가 제공하는 소프트웨어가 맞는지 검증해주는 기능을 가지고 있습니다.

- 실행 전 기존 화면



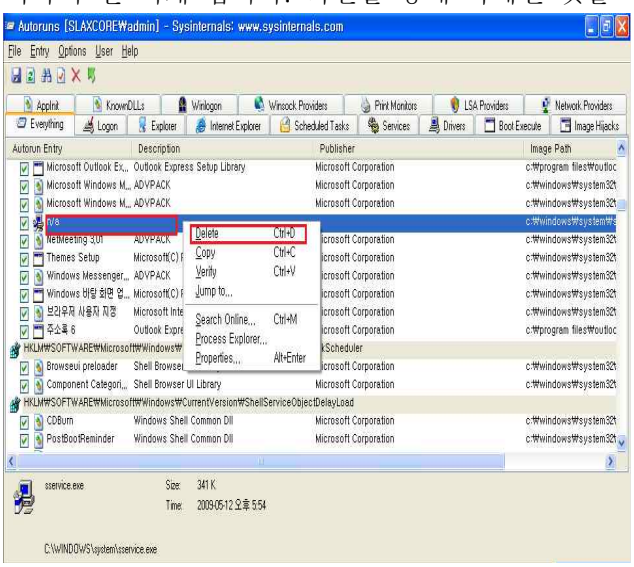
[Option]선택 -> [Verify Code Signature]항목체크 -> F5나 [File]에서 [Refresh]를 선택

- 실행 후 기존 화면과는 다르게 다음과 같이 화면이 변경된 것을 확인 할 수 있습니다.

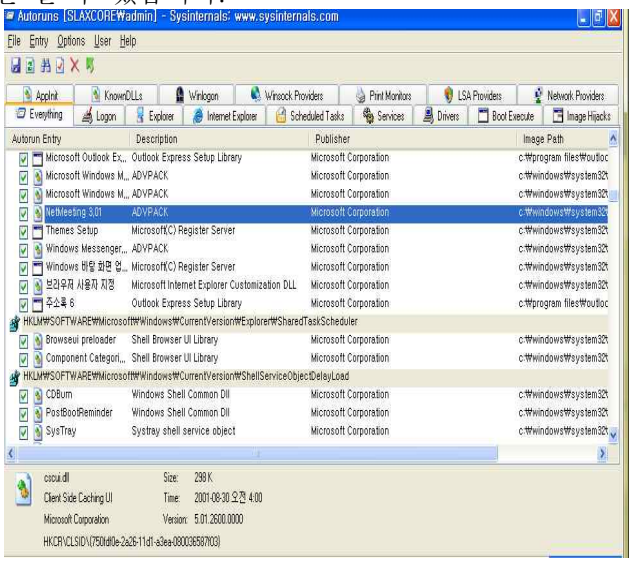


기존 Publisher항목에서는 없었던 Verifide가 공급자 앞에 붙은 것이 확인이 가능합니다.
여기서 Verifide는 마이크로소프트웨어사가 제공하는 소프트웨어란 것인 검증된 것으로 정상적인 프로그램을 말합니다.
반면에 Not Verifide나 아예 Publisher항목에 표시가 안 되는 경우는 악성프로그램이나 비정상적인 프로그램으로 의심할 수 있습니다. 하지만 간혹 정상적인 프로그램도 Not Verifide 표시되는 경우가 있으므로 주의가 필요합니다.

4. 다음은 [Entry]메뉴에 각 항목에 대해 설명하겠습니다.
-Delete : 선택한 프로그램을 시작프로그램에서 삭제합니다. 삭제된 항목은 윈도우 부팅 시 자동으로 시작이 안 되게 됩니다. 화면을 통해 삭제된 것을 확인 할 수 있습니다.

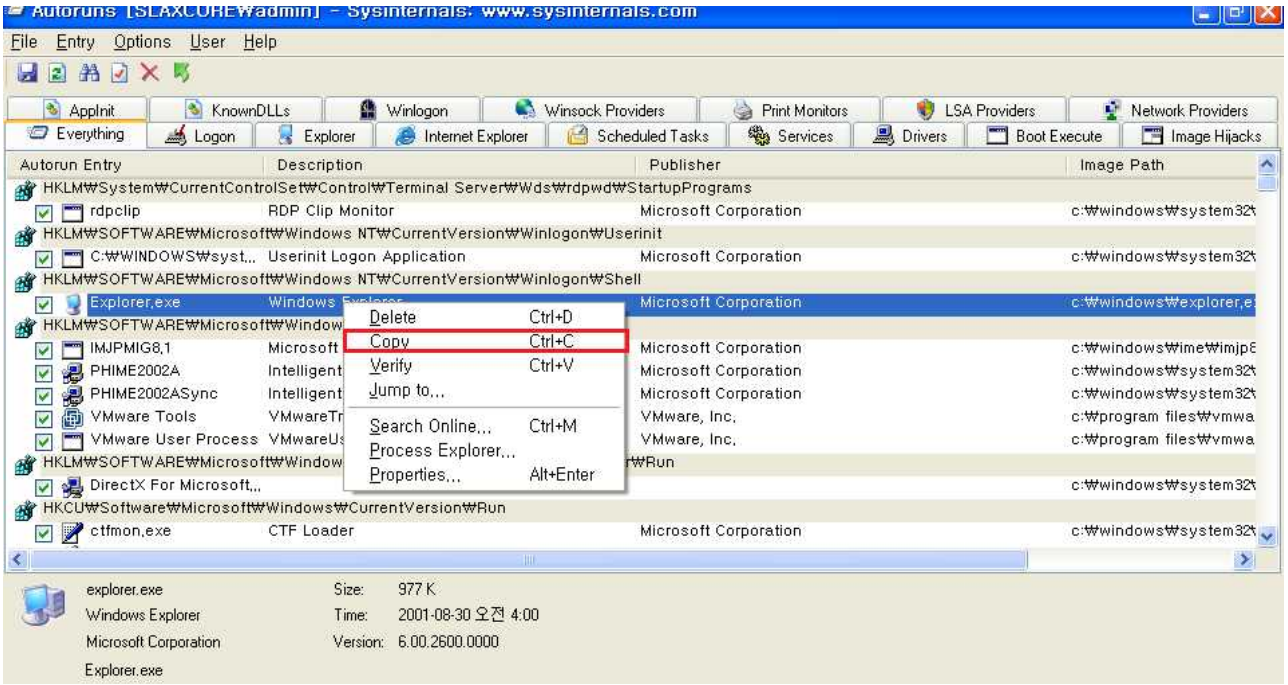


Delete 클릭!



Delete 클릭 후

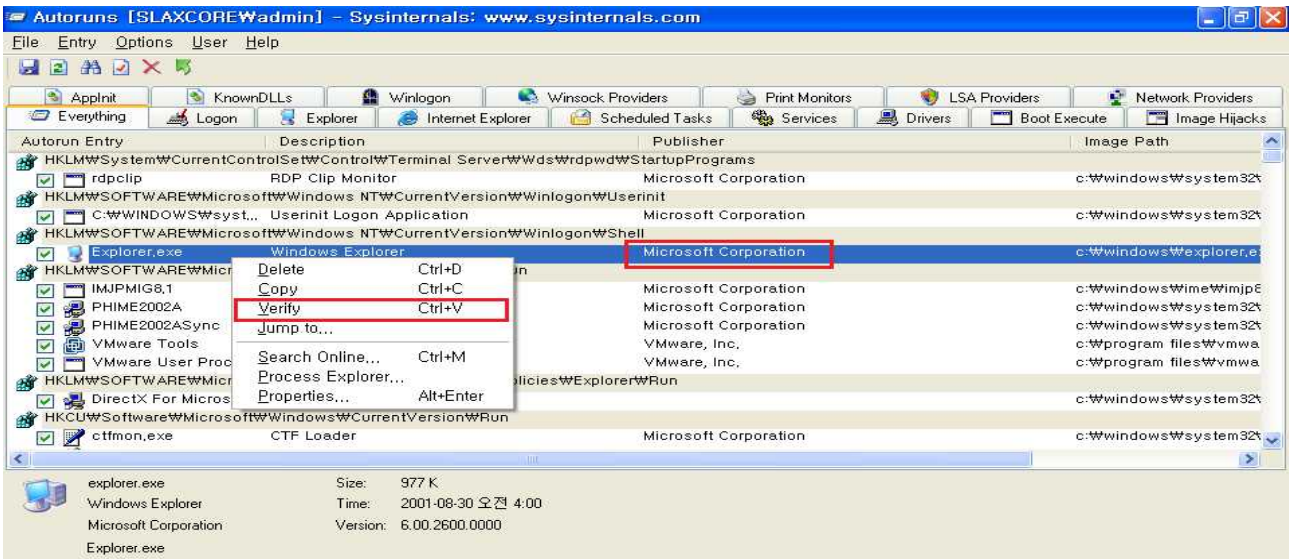
-Copy : 선택한 프로그램의 이름, 프로그램 종류, 제공자, 시스템경로를 복사합니다.



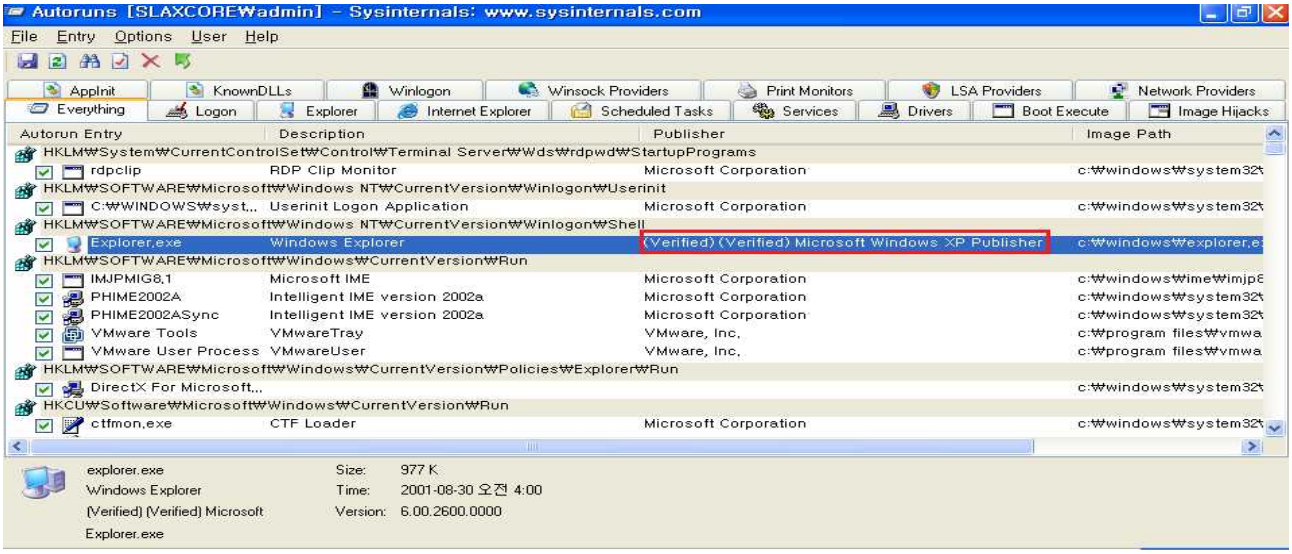
Copy를 클릭 후 메모장에 붙여넣기

메모장에 복사된 이름, 프로그램 종류, 제공자, 시스템경로

-Verify : 선택한 프로그램의 Verify(검증)을 실행합니다.



Verify클릭 전 Publisher의 상태

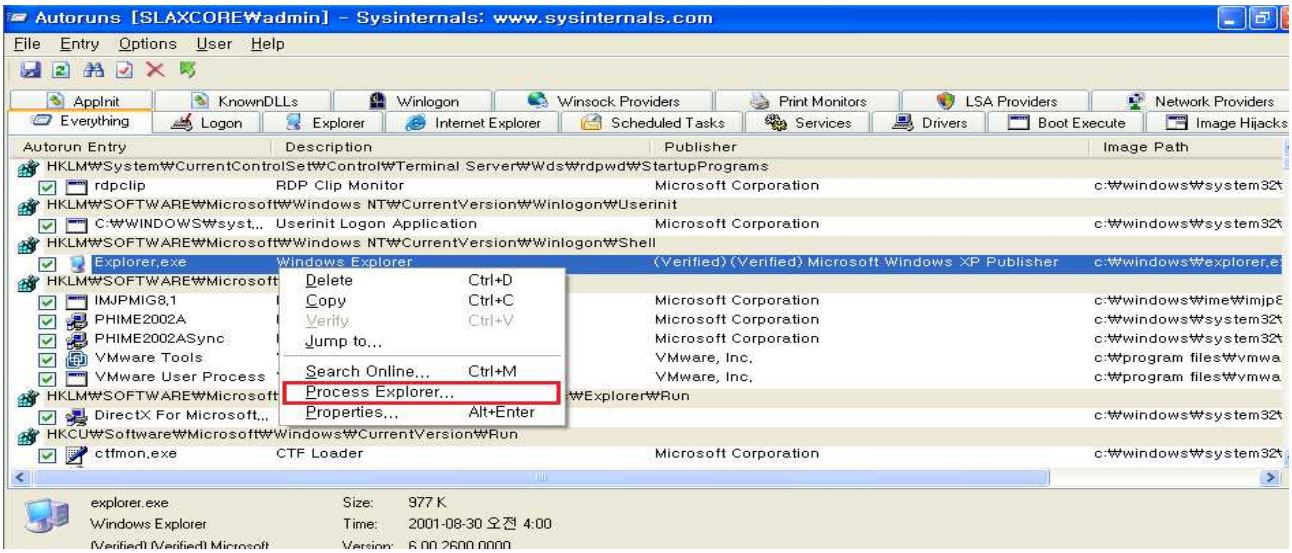


Verify 클릭 후 변화된 Publisher

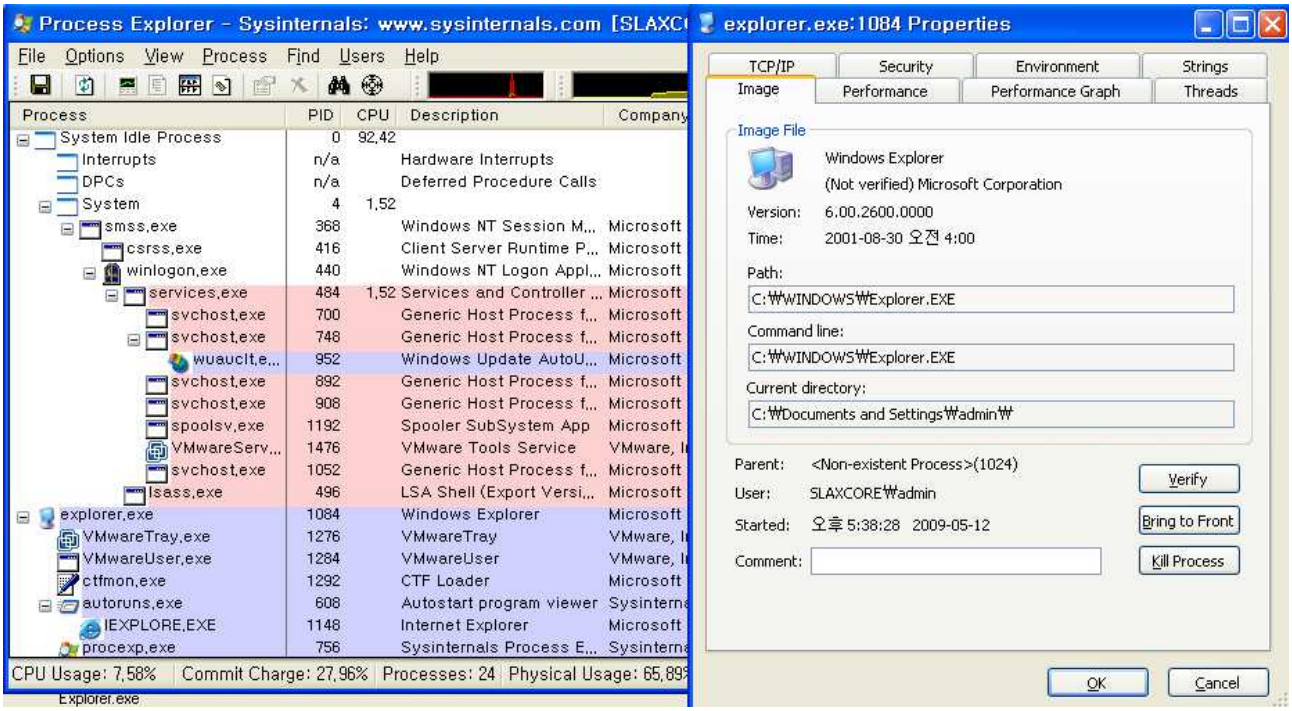
-Jump to : 선택한 프로그램의 레지스트리 편집기의 해당 항목으로 이동됩니다. 레지스트리를 수정 또는 삭제할 경우에는, 반드시 미리 백업을 해둔 상태에서 진행하기 바랍니다. 레지스트리를 잘못 건드릴 시 시스템에 심각한 문제가 발생 할 수도 있습니다. 레지스트리 백업 방법은 윈도우의 [시작] -> [실행] -> regedit를 입력한 후, 파일 메뉴에서 내보내기(*.reg)를 하면 됩니다. 단, 악성코드로 판명된 레지스트리의 경우 완전삭제하시기 바랍니다.

-Search Online : 선택한 프로그램에 대해 인터넷에서 검색합니다. 마이크로소프트웨어사의 프로그램이므로 자동으로 msn으로 검색합니다.

-Process Explorer : 선택한 프로그램을 Process Explorer프로그램과 연동하여 실행합니다.
Process Explorer는 같은 제작사에서 만든 프로그램으로 시스템상의 실행되고 있는 프로세스를 보여주는 프로그램으로 연동하여 사용하고자 할 경우. 프로그램을 미리 실행시켜 놓거나 autoruns가 들어있는 동일 경로에 Process Explorer를 놓고 사용하면 됩니다.



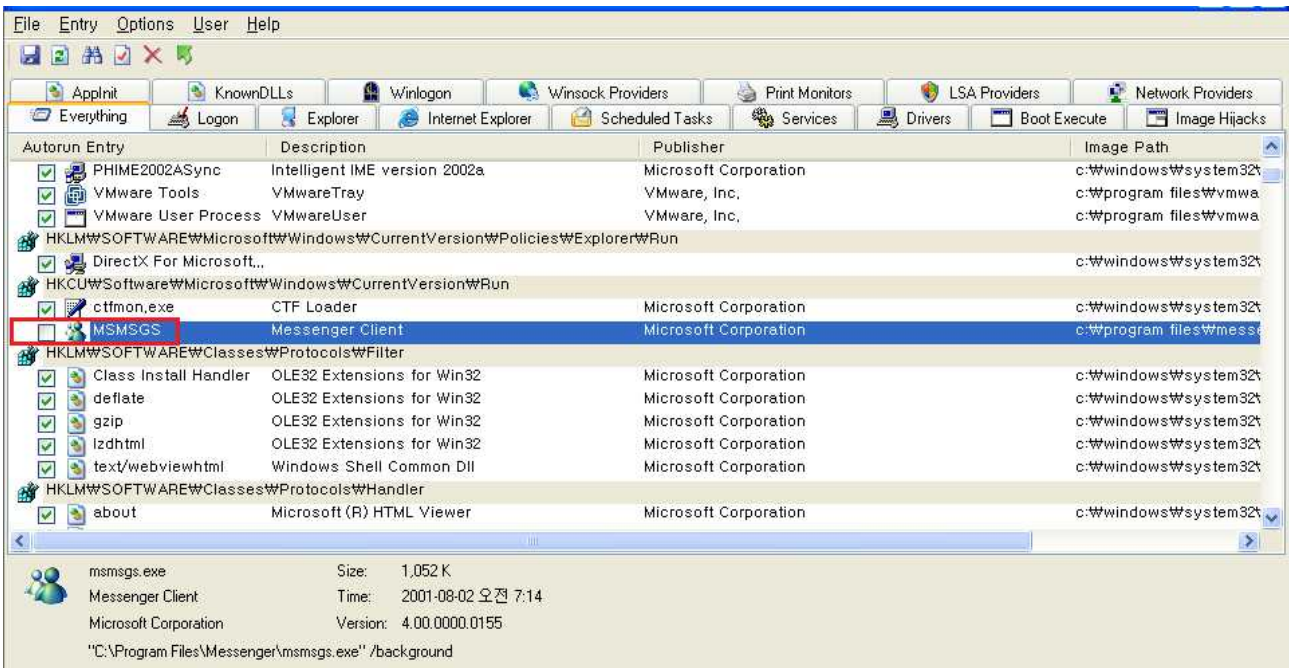
Process Explorer 클릭



Pocess Explorer와 연동되어 실행된 모습

-Properties : 선택한 프로그램의 등록정보를 보여줍니다.

4-1. 시작프로그램을 삭제하지 않고 구동을 원치 않는 개체의 체크박스를 해제해주면 간단하게 윈도우 시작 시 구동이 안 되게 할 수 있습니다. 그림과 같이 체크박스를 해제하면 간단하게 시작프로그램에서 제외할 수 있습니다. 이외에도 웹브라우저 툴바나 윈도우 탐색기에서 마우스 오른쪽 버튼 메뉴(Context Menu)를 체크박스 해제만으로 가볍게 제어가 가능합니다.



5. Auturuns 프로그램을 활용하여 바이러스 등의 유해 요소 파악이 가능 합니다.
악성프로그램의 경우 기본적으로 시작 프로그램에 등록할 가능성이 높기 때문에 Logon, Service 항목을 파악해 보도록 합니다. Description과 Publisher 부분이 누락되어 있다면 우선 의심해 봐야합니다. 그러나 정상 프로그램도 누락하는 경우가 있으므로 주의가 필요합니다. 그리고 경로가 정상적인 것인지도 파악해 봅니다. 악성프로그램의 경우 시스템 폴더나 설치 폴더 등에 위장할 가능성이 높습니다.

5-1. 툴바의 경우 Internet Explorer 웹브라우저를 숙주로 삼는 경우가 대부분이므로 이 항목을 조사해 보도록 합니다.

5-2. Winsock Providers, Drivers, Printer Monitor 등도 악용할 수 있으므로 확인이 필요합니다. 다만 초보자들의 경우 쉽게 파악하기 힘들 수도 있습니다.

5-3. 만약 악성코드를 분석하는 입장이라면 악성코드를 실행하기 전에 [File] -> [Export]를 통하여 시스템 로그를 저장한 뒤, 악성코드 실행 후 로그와 비교·분석을 하는 것이 좋습니다.

6. Autoruns 프로그램의 활용에 대해 알아보았습니다. 기타 추가적인 내용은 Help(도움말)을 통해 확인하거나 포럼에서 정보를 얻을 수 있을 것입니다.
http://forum.sysinternals.com/forum_topics.asp?FID=16

참조사이트 : http://blog.naver.com/hahaj1
작성자 : 중부대학교 SCP회장 정혜성