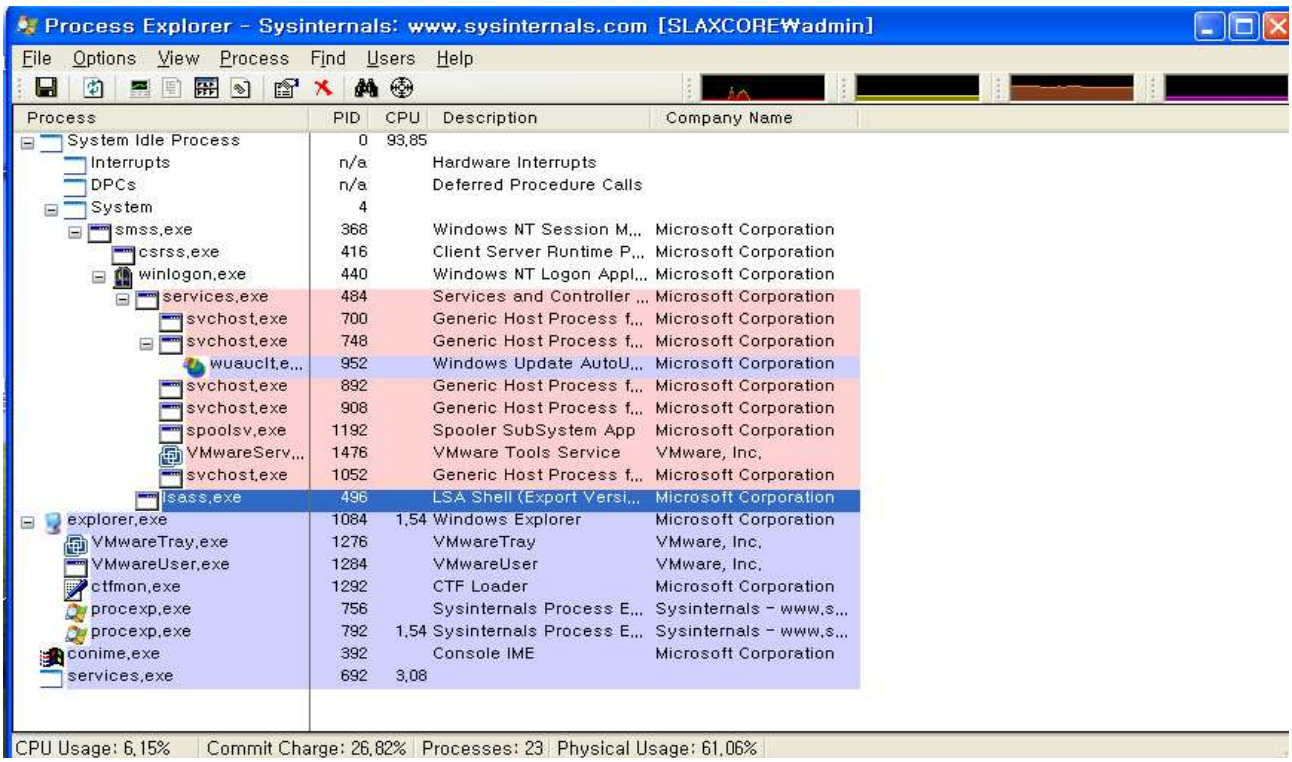
Process Explorer이란? Process Explorer는 프로세스를 관리할 수 있는 프로그램이다. 즉 실행중인 프로세스의 파악과 해당 프로세스의 우선권 변경, 정지, 강제 종료 등의 조치를 할 수 있다. 아울러 추가 설정을 통해 메모리 사용량 등을 파악할 수 있다. 참고적으로 윈도우(Windows)의 작업 관리자에서도 프로세스를 파악할 수 있으나 기능이 다양하지는 않다. 그리고 PC방과 같은 곳에서 윈도우의 작업 관리자를 사용할 수 없도록 조치했다면 Process Explorer 프로그램이 대안이 될 수도 있다.

1. 프로그램 다운로드 및 실행 방법

제작사의 사이트인 http://www.sysinternals.com 에서 다운로드 하면 됩니다. 실행은 압축을 푼 뒤 procexp.exe만 실행하기만 하면 됩니다. 압축파일이기 때문에 따로 설치 과정은 필요하지 않습니다.



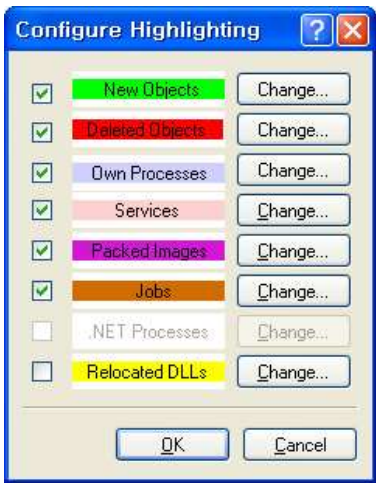
Process Explorer 구동화면

2. 프로그램화면 설명

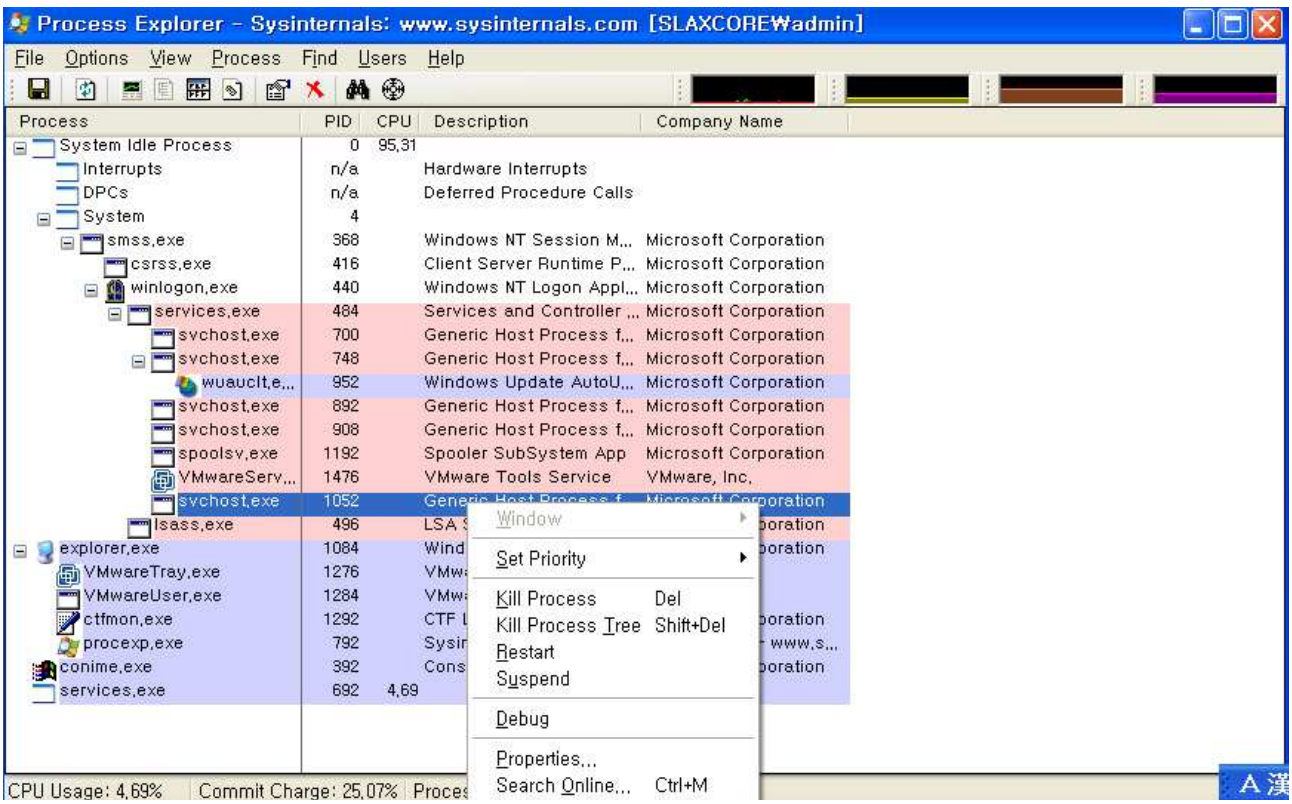
위의 그림을 기본으로 각 항목에 대해 설명하겠습니다.

- Process : 현재 실행 중인 Process를 표시합니다.
- PID : PID(Process ID)로 각 프로세스에게 할당 된 ID를 말합니다.
- CPU : 현재 CPU의 자원을 얼마나 사용하고 있는지 백분율 단위로 표시합니다. 이 항목은 수시로 변하기 때문에 화면에 값이 절대적인 값은 아닙니다.
- Company Name : 프로세스에 공급자명을 표시합니다.

2-1. 화면을 보시면 프로세스들이 여러 가지의 색으로 구분되는 것을 알 수 있습니다. 이것은 Process Explorer에서 지원하는 Highlighting 기능으로 프로세스를 종류별로 쉽게 구분되게 해줍니다.
이에 대한 설정은 [Option] -> [Configure Highlighting] 메뉴에서 설정이 가능합니다.

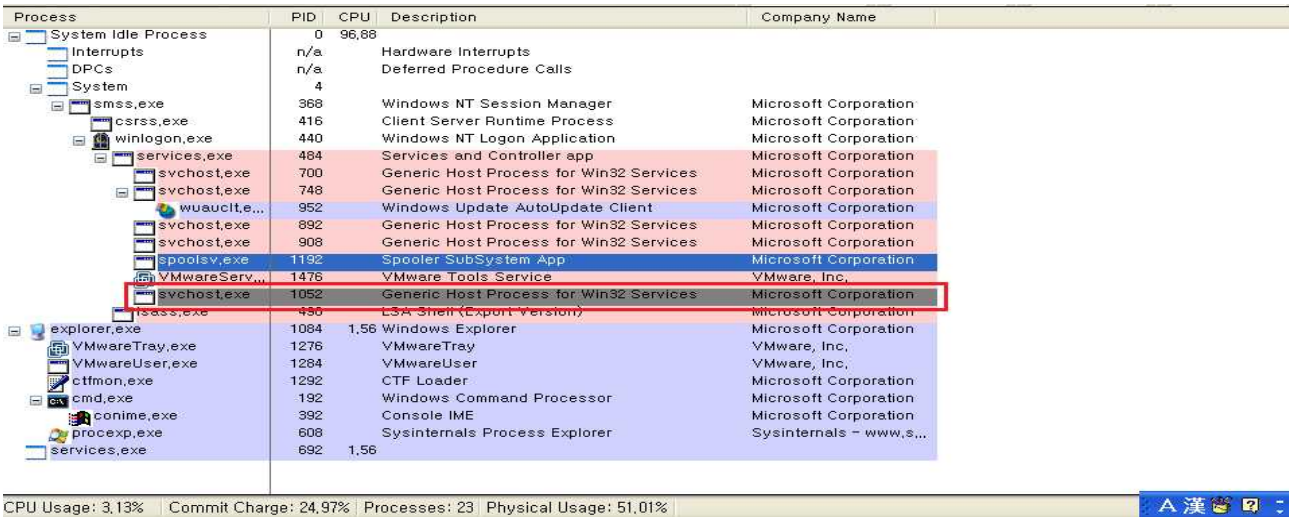


3. 실행 중인 프로세스를 관리하고자 할 경우, 해당 프로세스를 선택한 후 마우스 오른쪽 버튼을 누르면 메뉴가 나타납니다.



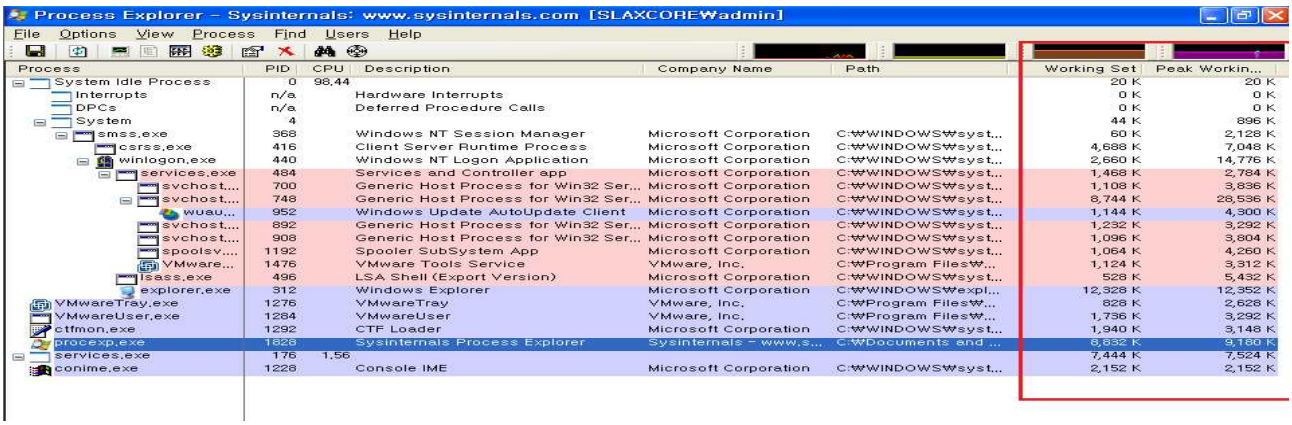
각 메뉴를 설명하면 다음과 같습니다.

- Set Priority : 프로세스의 우선순위를 설정하는 메뉴입니다. Realtime(실시간), High(높음), Above Normal(보통 초과), Normal(보통), Below Normal(보통 미만), Idle(낮음)으로 설정 가능합니다.
- Kill Process : 선택한 프로세스를 종료합니다.
- Kill Process Tree : 선택한 프로세스의 하부 구조까지 종료합니다.
- Restart : 선택한 프로세스를 재시작합니다.
- Suspend : 선택한 프로세스를 정지합니다. 그림을 보시면 정지한 프로세스의 색이 바뀐걸 알 수 있습니다.

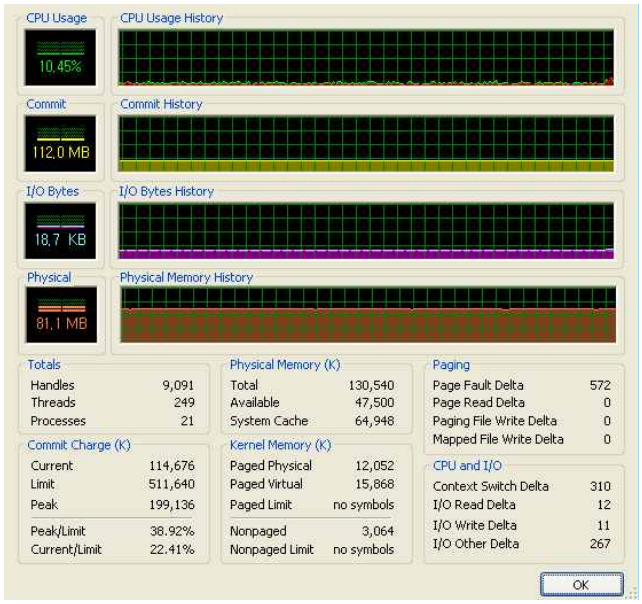


- Debug : 선택한 프로세스를 Debug 합니다.
- Properties : 선택한 프로세스의 등록정보를 봅니다.
- Search Online : 선택한 프로세스를 온라인에서 검색합니다.

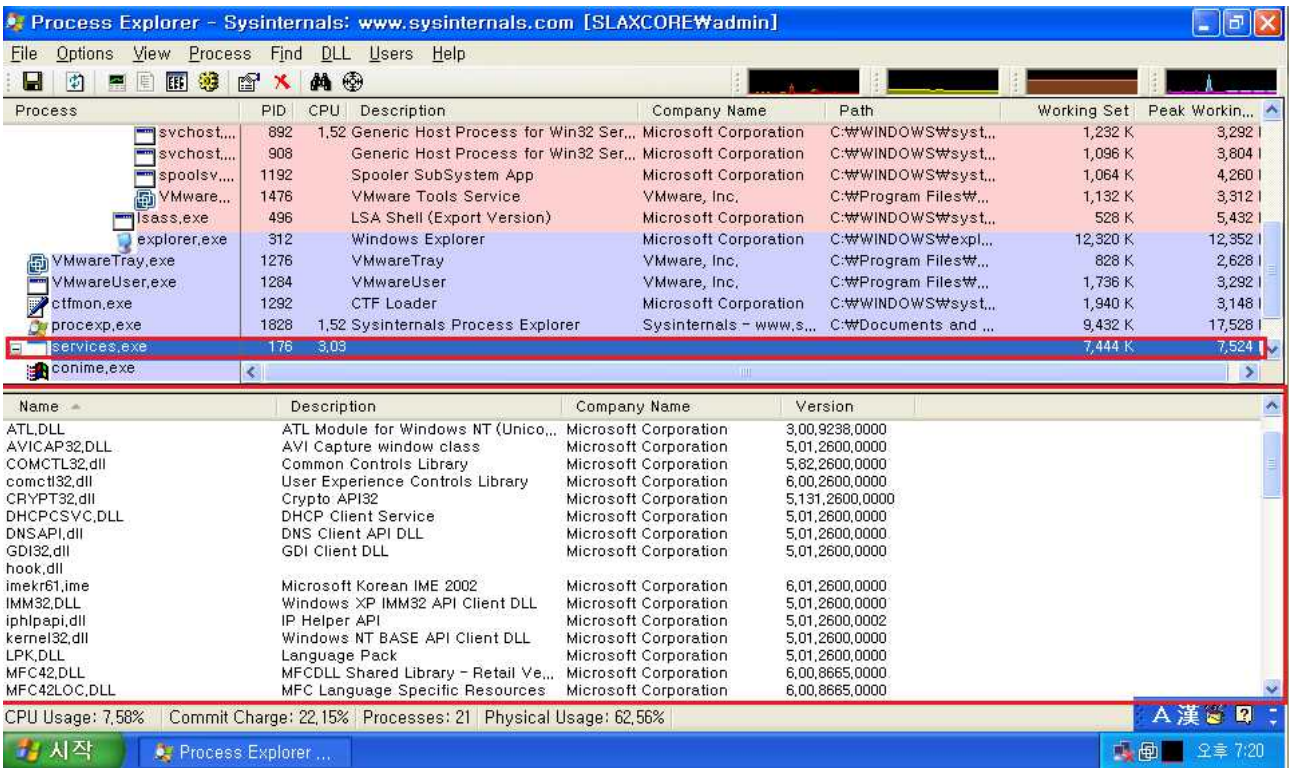
3-1. 기본화면에서의 출력항목 외에 다른 항목을 추가하고 싶다면 [View] -> [Select Columns]에서 설정이 가능합니다. 프로세스의 메모리 사용양이 알고 싶다면 다음과 같이 하면 됩니다.
[View] -> [Select Columns] -> [Process Memory] -> [Working Set Size]와 [Peak Working Set Size]를 체크한 후 확인을 하면 됩니다. 그림을 보면 메모리 사용양이 나오는 것을 확인 할 수 있습니다. 이 밖에도 Tread, Handle, Path 등의 많은 설정을 할 수가 있습니다.



마지막으로 [View] → [System Information]를 선택하면 CPU 점유율과 메모리 (전체) 사용량 등을 그래프로 확인할 수 있습니다. 수치는 달라지므로 유의하시기 바랍니다.



3-2. 다음은 실행중인 프로세스의 Dll이나 Handle의 무엇이 있는지 확인하는 방법을 알려드리겠습니다. [View] -> [Show Lower Pane]를 체크 후 하단의 [Lower Pane View]에서 Dll 이나 Handle을 체크하시면 됩니다.

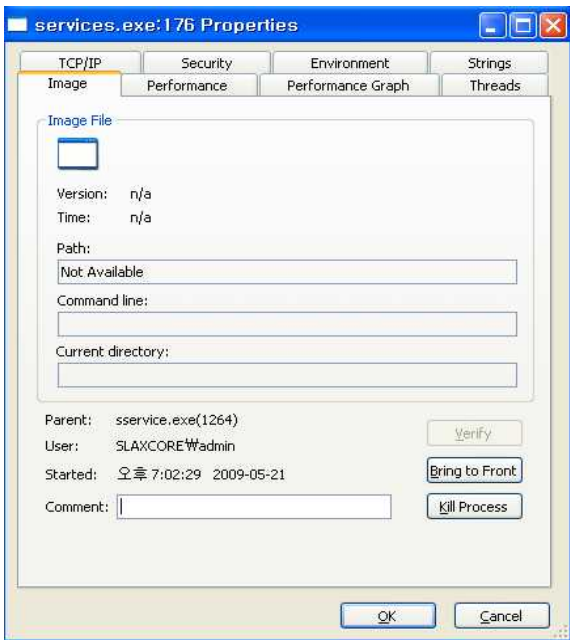


그림을 보시면 선택한 프로세스에 대한 실행중인 Dll파일을 확일 할 수 있습니다. [Lower Pane View]에서 Handle를 선택하면 프로세스에 대한 실행중인 Handle을 확인 할 수 있습니다.

4. 악성코드분석과 관련하여 Process Explorer의 활용

Process Explorer를 사용하여 시스템을 파악할 경우, 1차적으로 눈을 통해 이상한 프로세스를 파악할 수 있으며, 2차적으로 개별 프로세스의 속성 확인이나 의심가는 파일을 검색하여 조치가 가능합니다. 그러나 후자의 방법은 쉽지는 않은 방법입니다.

위에서도 언급했다시피 프로세스를 눈으로 쉽게 파악할 수 있는 경우, 바이러스나 스파이웨어 등의 활동을 파악할 수 있고 프로세스를 강제 종료(Kill Process)시킬 수 있습니다. 하위 프로세스까지 종료할 경우에는 Kill Process Tree를 선택하여 종료할 수 있습니다. 그러나 시스템 깊숙히 침투한 경우에는 단순히 프로세스를 종료하는 것만으로는 해결할 수 없는 경우도 있습니다. 또는 눈으로 파악할 수 없는 경우도 있을 것이다. 그럴 경우에는 그 프로세서를 구동시키는 악성프로그램 자체를 삭제하여야 합니다. 프로세스의 위치파악의 경우 프로세스의 속성(Properties)을 선택(메인 화면의 아이콘 클릭, 혹은 마우스 오른쪽 버튼 활용, 또는 원하는 프로세스 더블 클릭)하게 되면 해당 프로세스에 대한 상세 내용을 파악할 수 있습니다. 정상적인 경우가 아니라면, 그림과 같이 경로가 이상하거나 필수 정보가 제대로 표기되지 않을 것입니다.



악성프로세스의 정보

의심가는 파일을 정확하게 찾을 수 없는 경우 메인 아이콘의 쌍안경 아이콘을 클릭하거나 [Find] → [Fine Handle or DLL]을 선택하여 검색할 수 있습니다.

자신의 컴퓨터에서 실행중인 프로그램의 프로세스를 잘 알 수 없다면 메인 화면의 [Fine Window's Process] 아이콘을 드래그하여 원하는 프로그램 위에 올려놓으면 알 수 있습니다.(해당 프로세스는 파란색 배경으로 표시). 만약 스파이웨어와 같은 악성 프로그램이라면 프로세스를 강제 종료시키는 등의 조치를 취할 수 있습니다.

마지막으로 위에서 언급했던 [System Information] 화면(메인 아이콘 클릭, 혹은 화면 오른쪽 상단의 그래프 클릭)에서는 CPU 사용량(Usage) 등을 확인할 수 있습니다. 활동 중 인 프로세스의 확인은 그래프 위에 마우스를 올리면 된다. 만약 특정 부분이 심하게 치솟거나 혹은 과다하게 CPU를 점유하는 경우, 의심 여부를 판단하는 데 도움이 될 것입니다.

5. Porcess Explorer 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