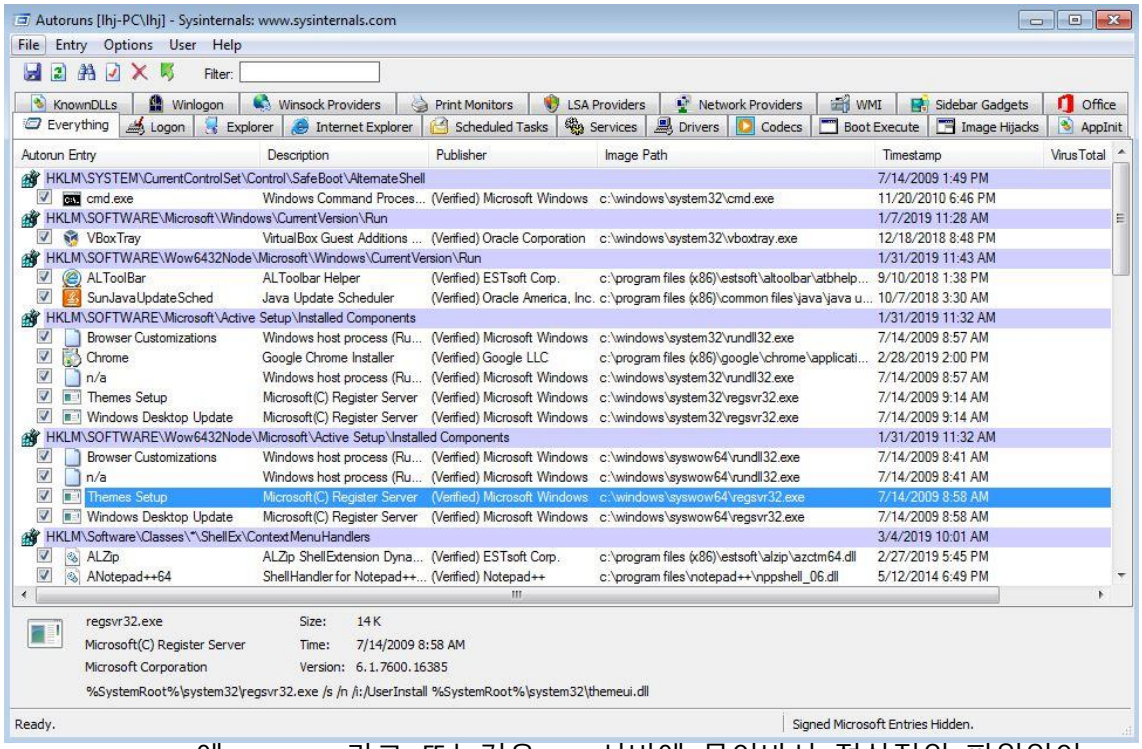
1. 마이크로소프트에서 제공하는 sysinternals 패키지 안에 들어가있는 툴이다.
   윈도우가 실행 될때 실행되는 프로그램을 일목요연하게 보여주는 프로그램이다.



- Publisher 에 'Verified'라고 뜨는것은 MS 서버에 물어봐서 정상적인 파일임이 확인된 파일
- 'Not verified' 라고 뜨는 파일이 알 수 없는 위험도가 높은 파일이지만 회사에 따라서는 원가 절감을 위해서 MS 인증을 받지 않고 배포 되는 경우도 있음.

2. 항목 설명

- Everything : 낱개항목에서 볼수 있는 정보를 한군데 가져다 리스팅 해놨다. 이곳에서 다 분석하기가 힘드니까 페이지를 돌아다니면서 이상한 점을 찾으면 된다.

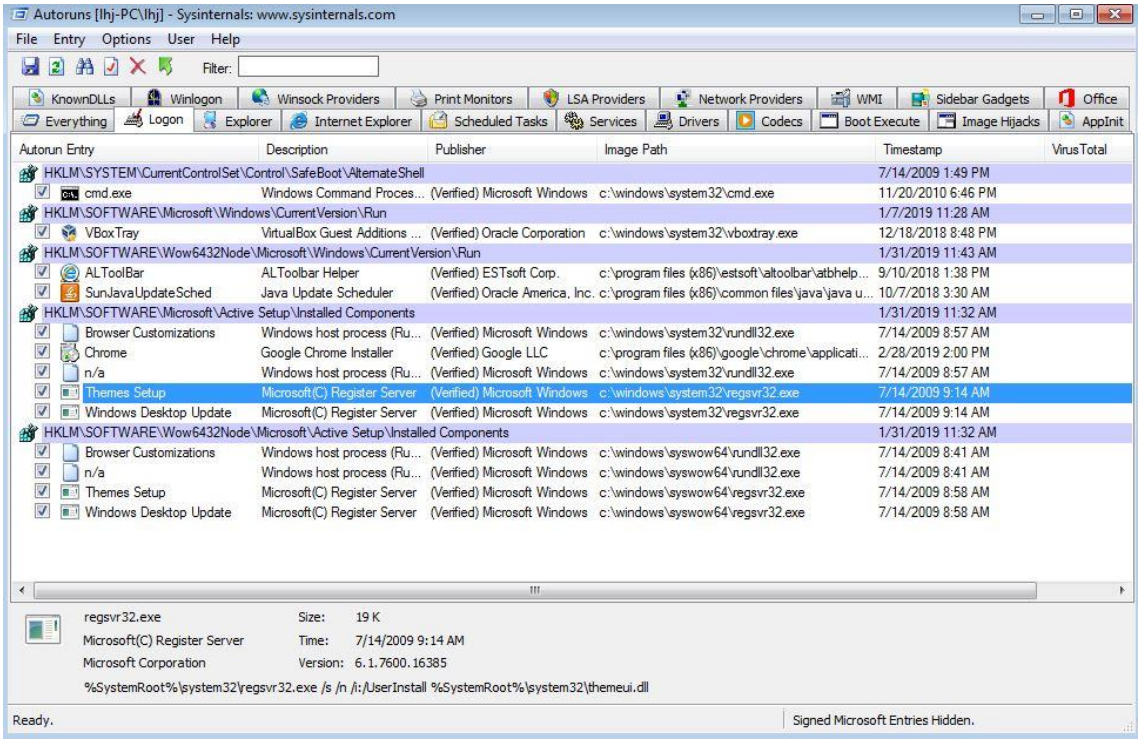
- LogOn : 윈도우 실행시 자동으로 실행되는 프로그램의 리스트

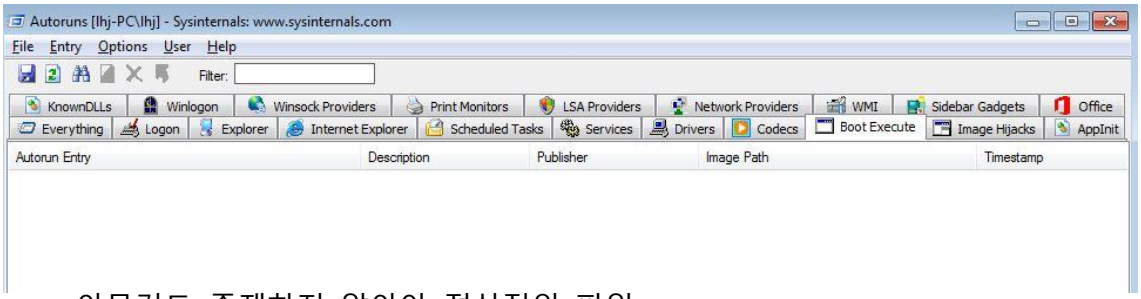
- Internet Explorer : IE 에 붙어서 동작하는 BHO 관련 프로그램의 리스트
(이곳에 매우 많은 리스트가 있다면 IE 에 문제가 있다는 소리이고, 알수 없는 파일이 존재한다면 애드웨어나 스파이웨어일 가능성이 높음)

- Service : 윈도우에 서비스로 돌아가는 프로그램의 리스트
악성코드의 경우 서비스에 등록 되어 동작하는 경우도 있다. 이 경우 회사이름을 위장 하는 경우도 많으므로 'Not verified'의 경우 주의 해야 한다.

- Drivers : 임시로 혹은 영구적으로 윈도우에서 돌아가는 서비스 드라이버 파일 리스트

- Boot Execute, Image Hijacks, Appinit : 이부분은 정상적인 윈도우라면 비어있는것이 정상이다. 파일이 등록되어 있으면 의심해봐야 함. (Appinit 에 Himym.dll 파일이 붙어있다면 악성코드 100%)





- 아무것도 존재하지 않아야 정상적인 파일.