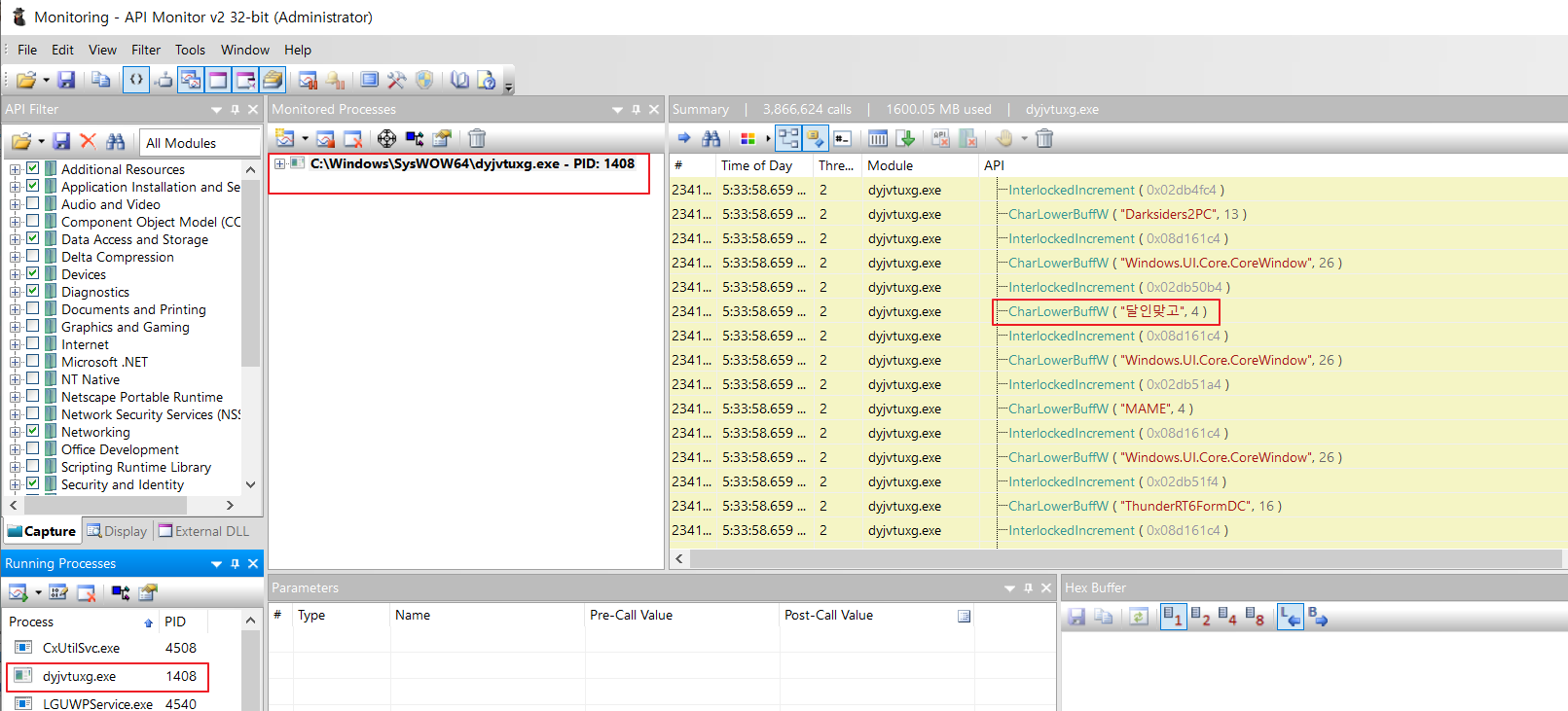


MultiByteToWideChar ( CP\_UTF8, 0, "SQL= INSERT INTO GR\_REGISTERUSER (GRKEY, GRMOMICODE, GRUSEREMAIL, GRUSERNAME, GRUSERTEL, MACADD, CREAT\_DT) VALUES ('25405f6b2f7e42d3ea16ae5bf3f3afd8jk90fx', 'MOMI01', 'kgyeongseong@gmail.com', 'ê¹ê²½ì±', '010-8345-5910', '34E12D3AC0C2^34E12D3AC0BE', GETDAT, 273, NULL, 0 )

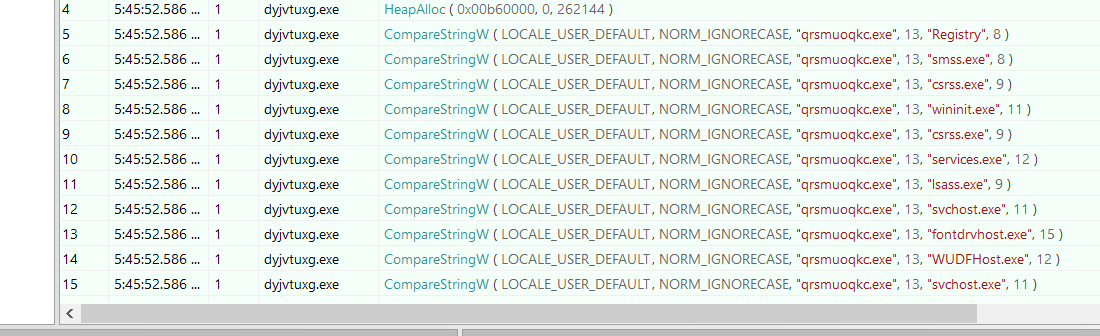
**프로세스 이름**

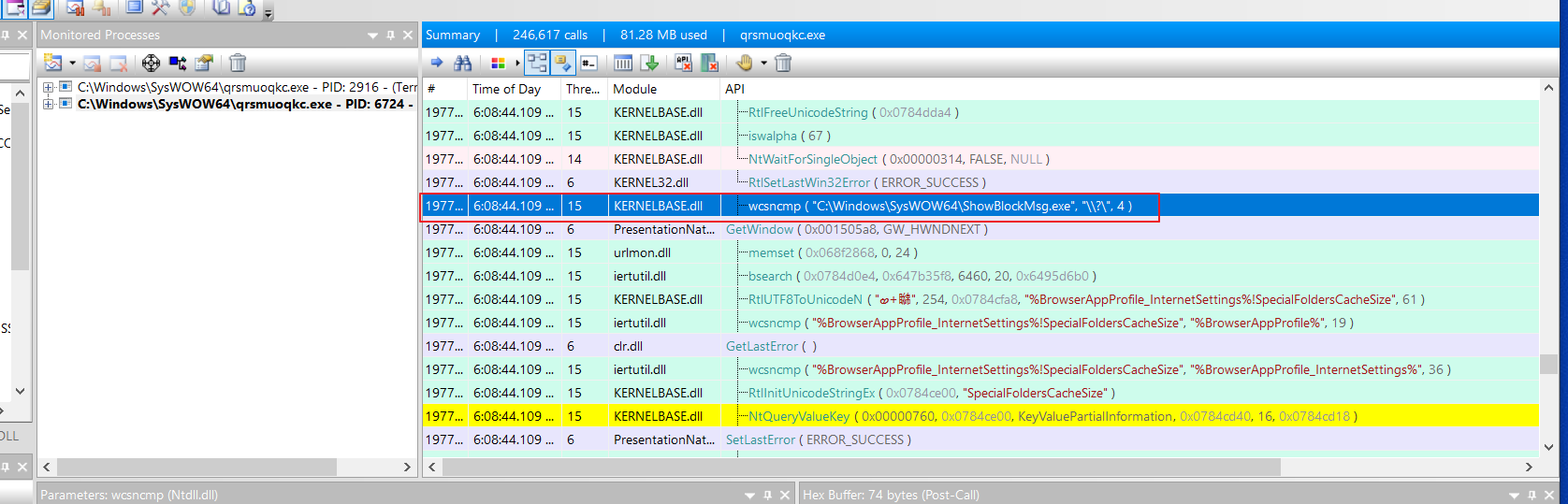
GRinspack.exe

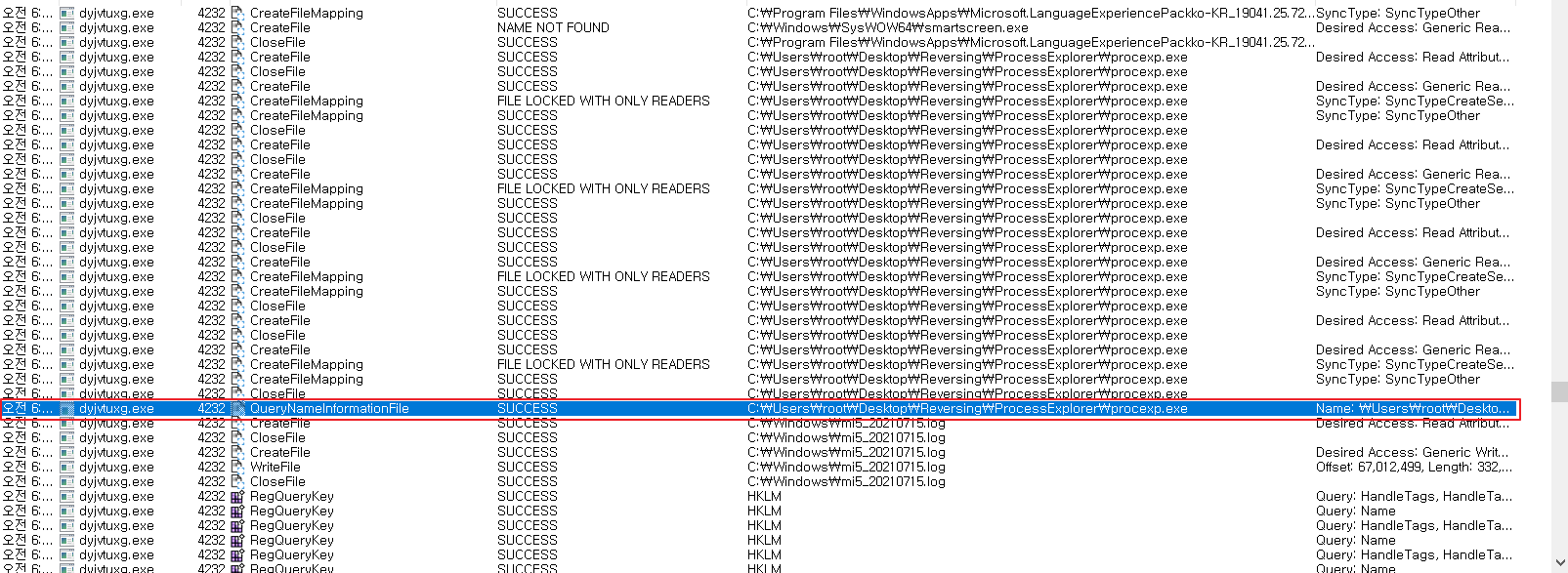


C:\Windows\SysWOW64\dyjvtuxg.exe

프로세스 찾아서 끄는 역할 담당인듯

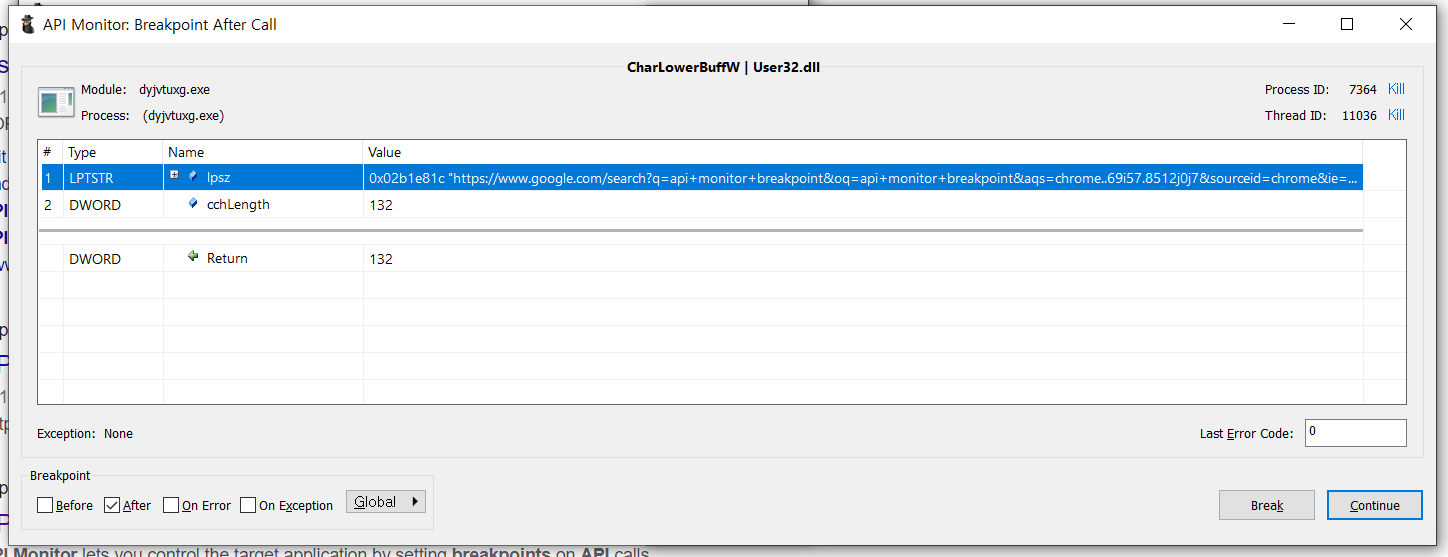






다른 파일들은 넘어가면서 차단하는 QueryNameInformationFile API를 호출한다(?)

후킹해보자



CharLowerBuffW API

0x02b1e81c "https://www.google.com/search?q=api+monitor+breakpoint&oq=api+monitor+breakpoint&aqs=chrome..69i57.8512j0j7&sourceid=chrome&ie=utf-8"