WatchDog (워치독) 구현

사이버보안학과 정보보안 학술소학회

김형찬

2018.01.28.(일)

CONTENTS

워치독이란 ?

W h o I s

- WatchDog (감시견)

- 시스템이 기계적인 고장으로 인한 중단 상태
  프로그램의 오류로 인한 무한루프 상태가 되는 것을 감시

- 비정상적인 동작을 할 경우 자동으로 시스템을 리셋하여
  정상적으로 동작하도록 해주는 것

활용 사례

- 드론으로 개의 배설물 청소
  - 주변 보다 온도가 높은 곳의 GPS좌표를 수집 (https://www.anadronestarting.com/%EC%99%80%EC%B9%98%EB%8F%85/)

- 홈페이지에 수상한 접근 시도 감시
  - 코스콤 내 정보보호센터에서 관제 (http://news.mt.co.kr/mtview.php?no=2011051915223888456&outlink=1&ref=https%3A%2F%2Fsearch.naver.com)

워치독 구현

- 윈도우 서비스 생성 및 실행
- 프로세스 리스트를 불러와 특정 프로세스의 실행 여부 판단
- 특정 프로세스가 실행 중이지 않을 경우 다시 실행

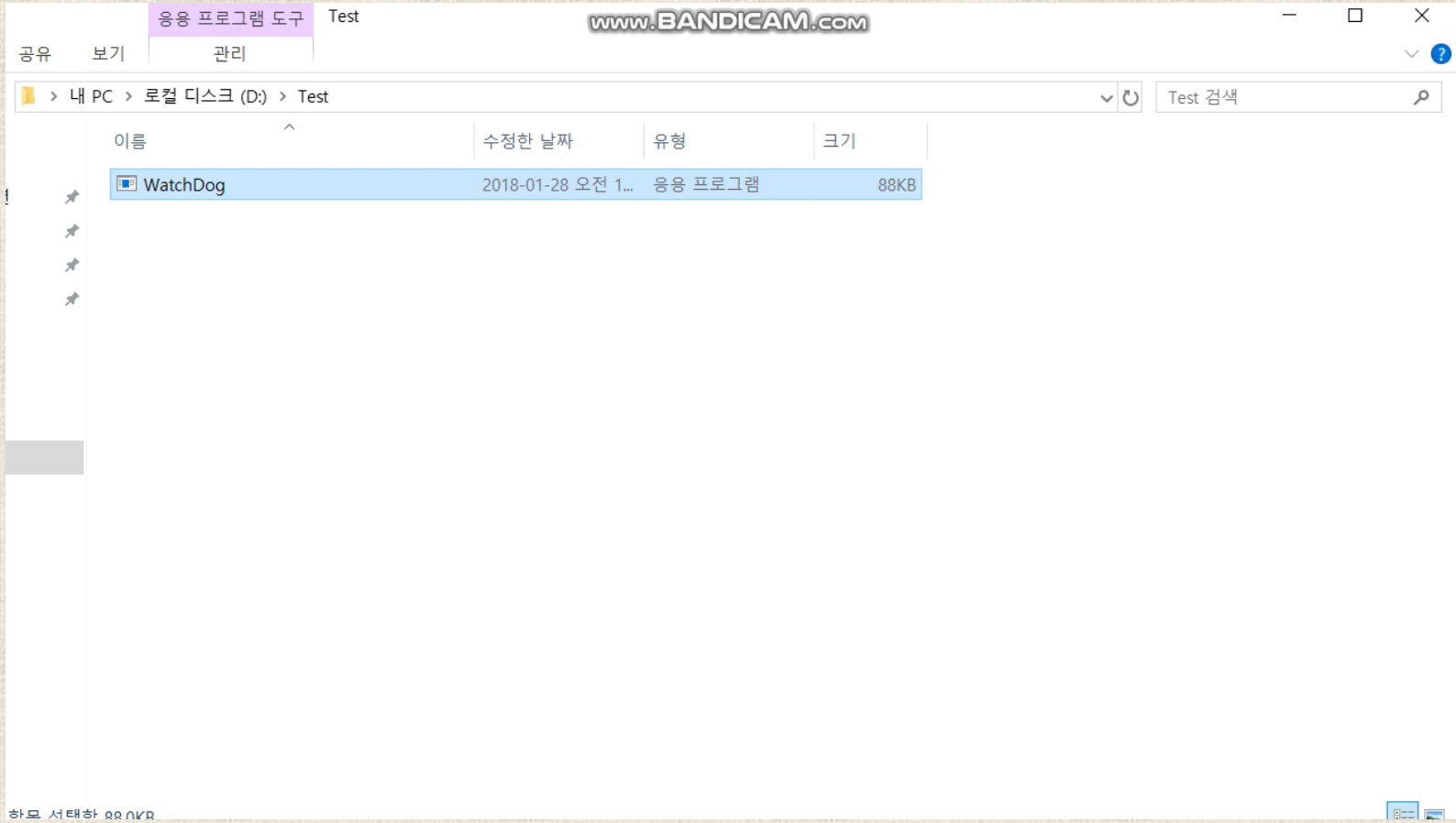
워치독 구현 – 서비스에서 일반 프로그램 실행

W h o I s

- 서비스의 실행 영역 ≠ 일반 프로그램의 실행 영역

- 서비스를 유저의 권한으로 실행해야 한다.
  - 프로세스 아이디 값(PID) 가져오기
  - PID로 프로세스 핸들 값 가져오기
  - 프로세스 핸들 값으로 토큰 핸들 가져오기
  - 토큰 복사
  - 프로세스 실행

시연 영상



https://youtu.be/SZ0RwgYzfKM

Q & A