## The 삽: User Function Monitoring Tool



장기헌 nvdark 2014.07.05



# The 삽



#### 배경

◎ 동적, 정적 분석: 삽, 삽, 삽, 삽 그리고 삽

◎ 분석을 하다 보면 누구나 하는 생각: 아...없나?

○ 검색 중 API모니터링 도구는 있지만 USER 함수 모니터링 도구가 없었음!!!

◎ 그래서!! 있으면 편하겠다!!

#### 컨샙

1. DLL

② 2. User Function 찾기

◎ 3. 함수 내부 연결 점 찾기

4. 원하는 포인트 모니터링

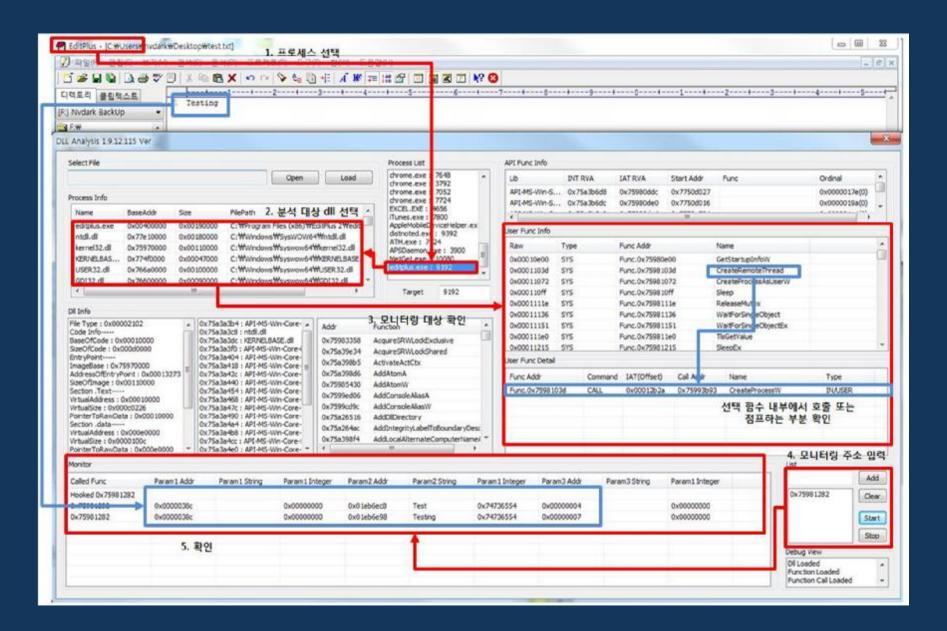
#### 개발

● API, User Function 및 함수 이외의 부분 포함

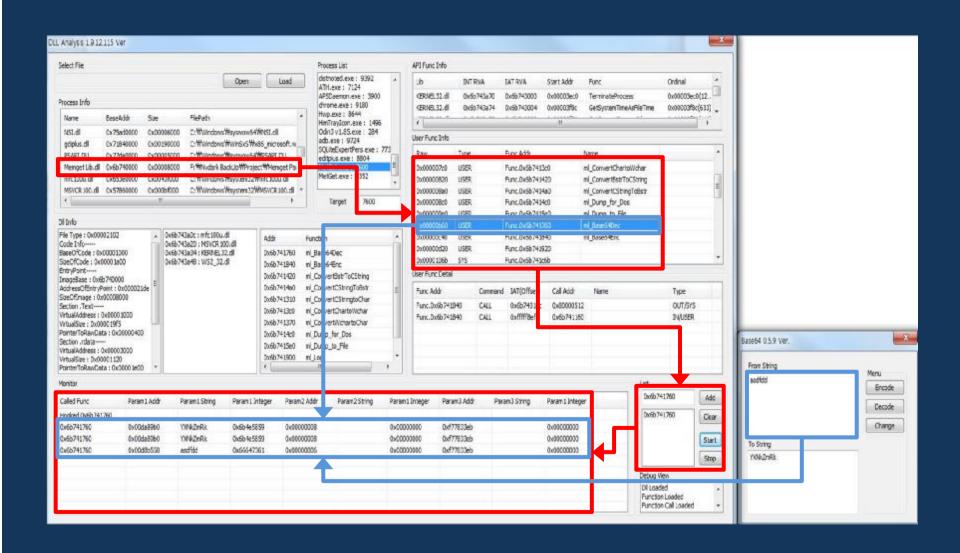
◎ 동적 분석에 기반한 모니터링

◎ 출력 할 결과 값 구분

#### 예시 1: API



#### 예시 2: User Function



#### 문제

◎ 분석의 정확성

◎ 늘어나는 요구사항

◎ 아....이건 뭐 쓸때마다...

## 그래서...

○ 목적: 삽 제작

◎ 아이디어 듬뿍 담긴 머리

● 방향:손맛 있는 삽 만들기

# Code Engn UNSIGNED