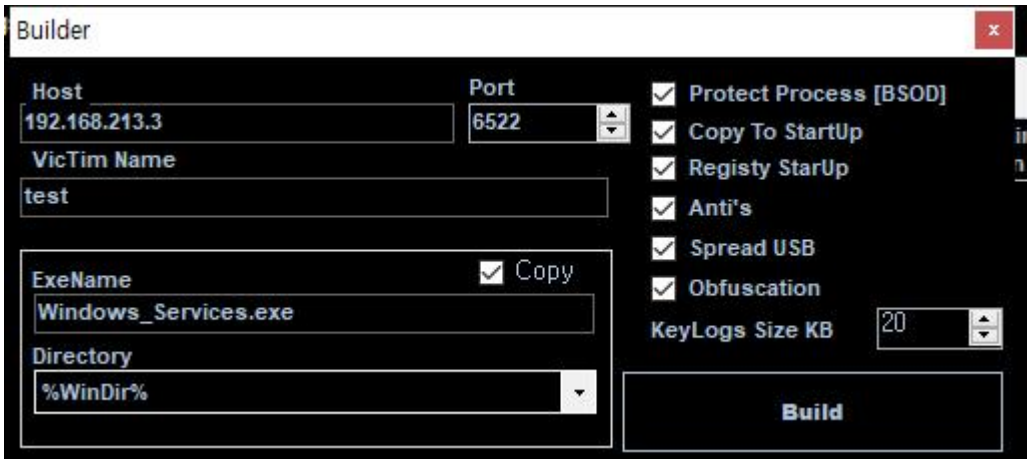
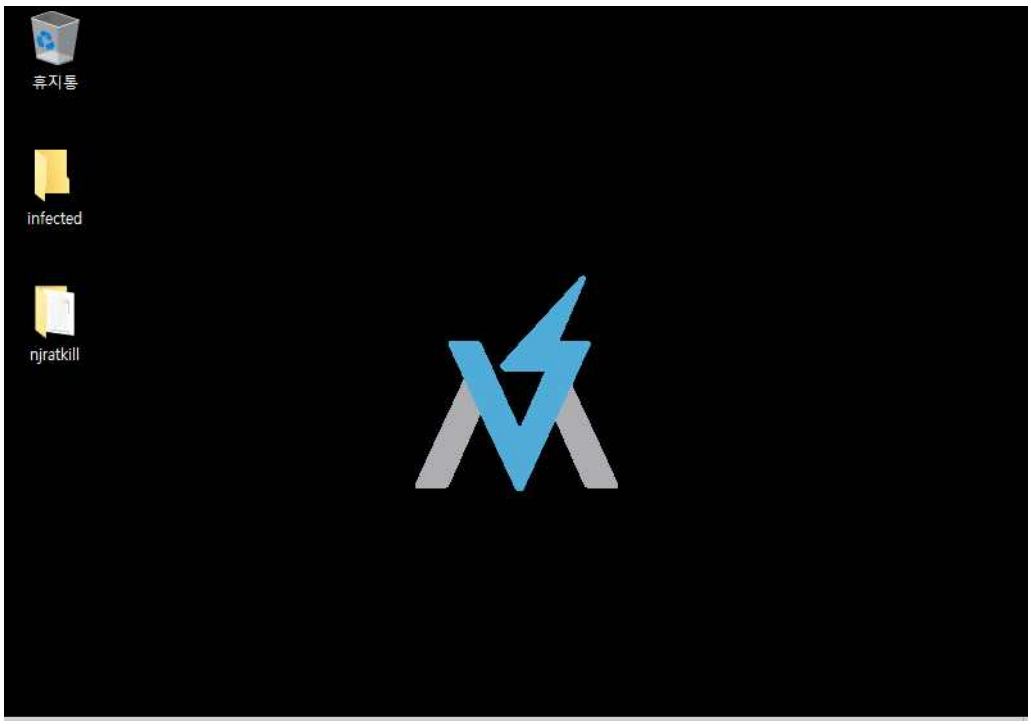
njratkill은 njrat 악성 코드를 쉽게 삭제할 수 있도록 하기 위해 제가 작성한 프로그램입니다. 파이썬3 으로 제작되었으며, 윈도우 10 FLARE VM 환경에서 테스트 되었습니다.

프로그램을 테스트하기 위해 서버에서 IP 주소를 확인하고 기능을 최대한 활성화시켜서 클라이언트에서 실행시킬 파일을 생성하였습니다.



여기서는 여러 상황에서 잘 작동하는지 최대한 확인하기 위해 기본값을 조금 변경하고, 기능을 최대한 활성화했습니다.



클라이언트에 윈도우의 공유 폴더 기능으로 앞에서 생성한 파일을 전송하였으며, 제작한 njratkill.py 파일 역시 복사해 두었습니다.

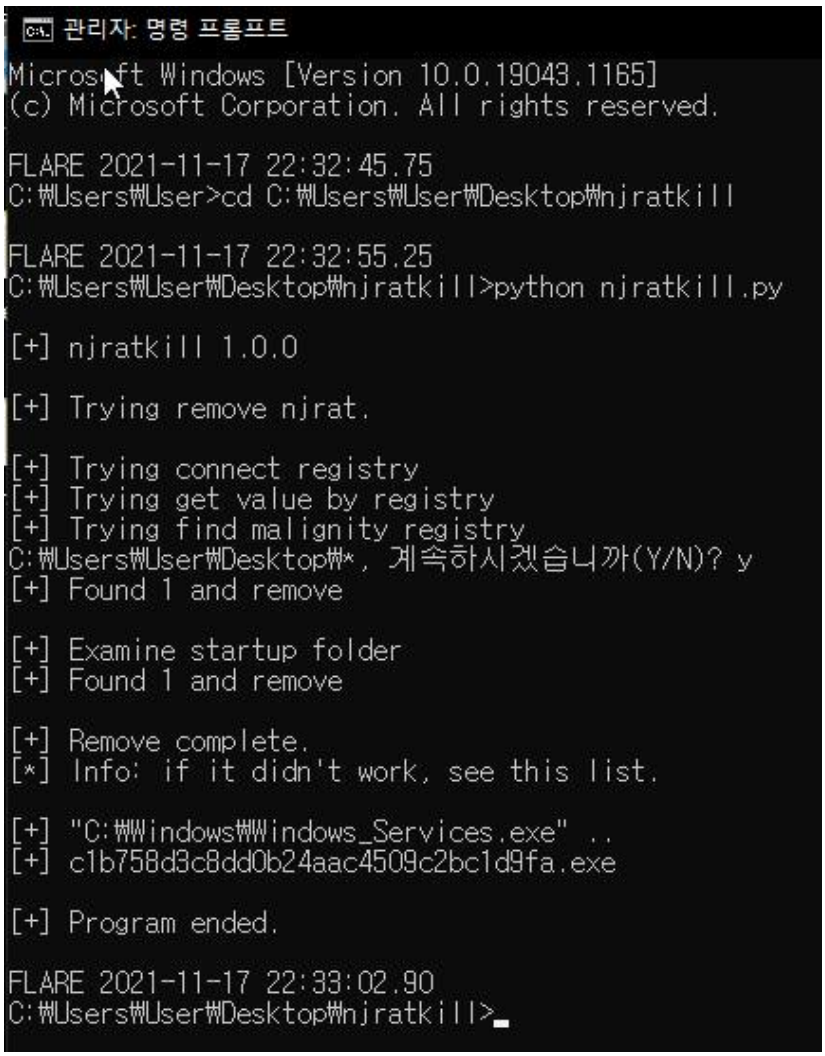
njrat 악성 코드에는 가상 머신과 디버깅 도구가 실행된 상태에서 실행되는 것을 막는 기능이 있기 때문에 여기서는 해당 기능을 비활성화시키고 생성하는 대신, 클라이언트에서 문제가 되는 프로세스를 종료시키기로 하였습니다.

클라이언트에서 생성된 악성 파일을 실행시키자 위의 스크린샷처럼 서버에서 클라이언트를

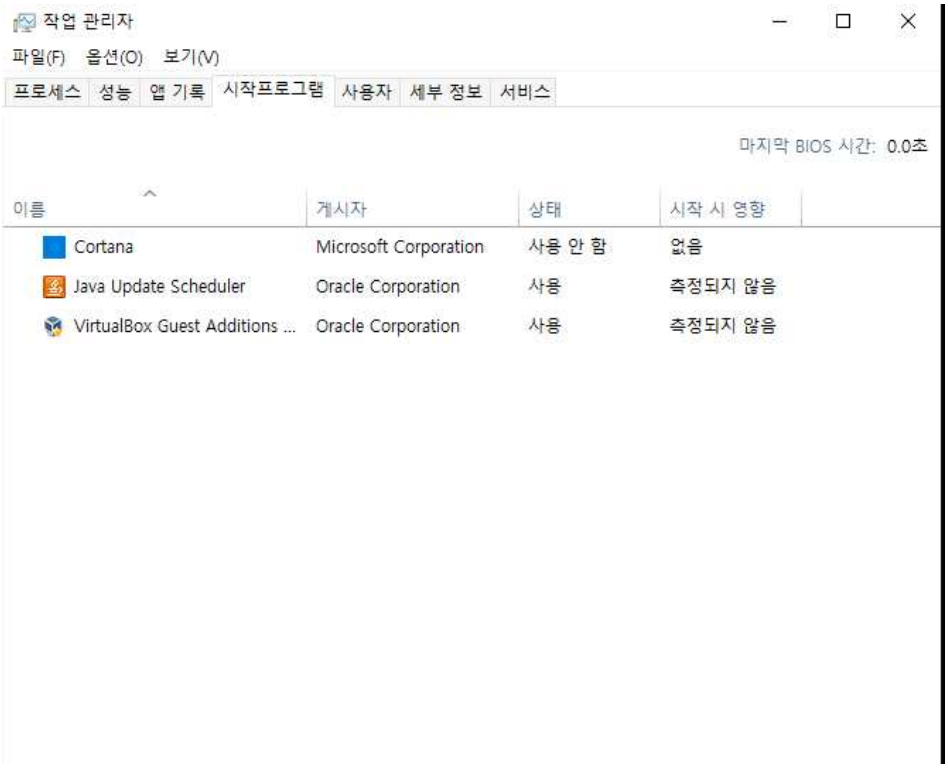
클라이언트에서 시작 프로그램을 확인해 보면 3개의 항목이 상당히 의심이 간다는 것을 알 수 있습니다. 이 3개의 항목이 악성 코드입니다.

일반적인 환경에서 치료를 시도하게 되면 악성 코드의 프로세스가 실행 중이고, 프로세스 보호 기능이 있으며, 공격자가 방해할 수 있기 때문에 안전모드로 부팅해야 합니다.

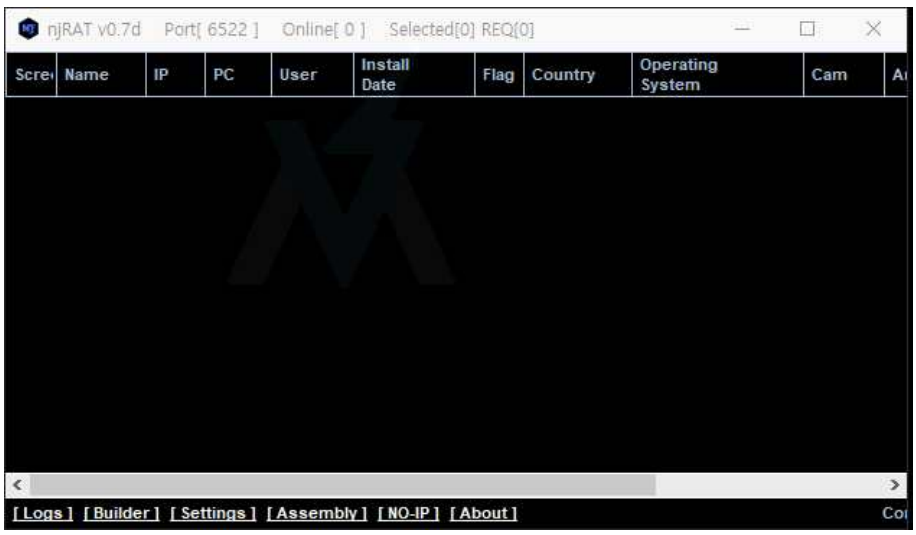
안전모드로 클라이언트를 부팅하면 위와 같이 되었습니다.



이 프로그램은 관리자 모드의 CMD 에서 실행하여야 합니다. 실행시키면 위의 스크린샷과 같이 성공적으로 치료가 진행되었습니다.



다시 시작 프로그램 목록을 확인해 보면 악성 코드로 의심되었던 3가지 항목이 모두 제거되었다는 점을 알 수 있습니다.



클라이언트를 재부팅 한 후 서버를 확인해 봐도 클라이언트를 조종할 수 없는 것으로 보아 성공적으로 치료가 되었다는 점을 확인할 수 있습니다.