위장 가상 머신 정보를 이용한 인텔리전트 봇 대응 방법 및 장치

■ 보유기관 한국전자통신연구원

■ 주요 발명자

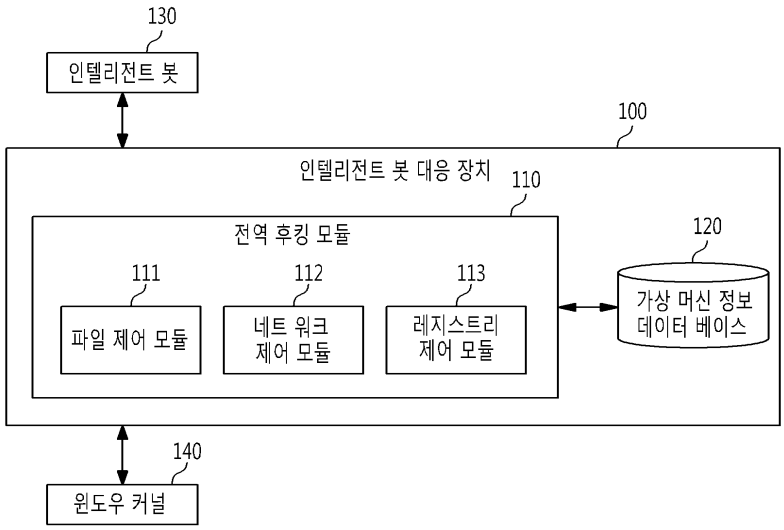
■ 권리사항	
· 출원번호	10-2010-0039358
· 출원일	2010년 4월 28일
· 현재상태	■ 등록 □ 공개(심사중) □ 미공개
■ 기술완성도	□ 기초연구단계 ■ 실험단계 □시작품단계 □ 제품화단계

■ 적용가능분야 및 목표시장 인텔리전트 봇

■ 기술 개요

위장 가상 머신 정보를 이용한 인텔리전트 봇 대응 방법 및 장치로 인텔리전트 봇의 악성 프로세스를 중단하도록 하는 위장 가상 머신 정보를 이용한 인텔리전트 봇 대응 방법 및 장치에 관한 기술임

■ 기술 개념도



[그림] 본 기술에 따른 위장 가상 머신 정보를 이용한 인텔리전트 봇 대응 장치의 구성도

■ 기술 내용 및 동향

[기술의 특 · 장점]

- 본 기술에 따르면 가상 머신의 동작을 탐지하는 인텔리전트 봇이 가상 머신 상에서 동작하는 것으로 판단하도록 위장 가상 머신 정보를 제공하여 인텔리전트 봇이 악성 프로세스를 중단하도록 함
- 그래서 사용자 단말이 인텔리전트 봇에 감염되더라도 악성 프로세스를 수행하지 않도록 하여 DDos(Distributed denial of service) 공격 또는 정보 유출 등의 2차 피해를 예방할 수 있음
- 또한 사용자 컴퓨터에서 실행되는 프로세스가 위장 가상 머신 정보를 리턴 받고 자신이 가상 머신 상에서 동작하는 것으로 판단하여 악성행위를 중단하도록 함
- 따라서 인텔리전트 봇이 악성 행위에 사용되는 것을 원천 차단하여 인털레전트 봇에 의한 사이버 테러 행위를 미연에 방지할 수 있음

[기술동향]

- 일반적으로 인텔리전트 봇(Intelligent Bots)은 사용자의 직접적인 참여 없이 정규적으로 정보를 수집하거나 또는 서비스를 수행하는 프로그램으로, 사용자가 제공한 파라미터를 사용해 인터넷에 접속된 단말을 검색하고 사용자가 관심을 가지고 있는 정보를 수집하여 사용자에게 제공함
- 그러나 이와 같은 인텔리전트 봇은 그 특성상 사용자의 의도에 따라 악성 행위에 사용될 수도 있음
- 따라서, 보안 전문가들은 이와 같은 인텔리전트 봇을 이용한 악성 행위를 분석하기 위하여 가상 머신(Virtual Machine)을 실행하고 가상 머신 상에서 인텔리전트 봇이 실행되게 하여 악성 행위를 분석 및 추적하고 있음
- 인텔리전트 봇의 제작자들은 이러한 가상 머신 실행을 통한 방법에 대응하기 위하여 가상 머신의 동작을 탐지하는 방법을 사용하고 있음
- 이와 같은 가상 머신의 동작을 탐지하는 방법에 의하면 인텔리전트 봇이 가상 머신 상에서 동작하게 되는지를 탐지하고, 인텔리전트 봇이 가상 머신 상에서 동작하는 것으로 판단하면 악성 행위를 실행하지 않고 종료함
- 그러나 이러한 기존의 기술에 따르면, 사용자 단말이 인텔리전트 봇에 감염될 경우에는 인텔리전트 봇이 악성 프로세스를 수행하게 되어 정보 유출 등의 피해를 막을 수 없다는 문제가 있음

■ 관련 기술

1	출원번호	10-2004-0097474
	발명의 명칭	이상 트래픽 분석을 위한 네트워크 시뮬레이션 장치 및 그 방법
2	출원번호	10-2006-0028732
	발명의 명칭	가상의 인라인 네트워크 보안방법

■ 시장 동향

- 2009년 발생한 DDoS 사건의 경우, 미국과 한국 정부를 비롯해 다수의 금융 및 미디어 웹사이트를 대상으로 하여 벌어졌으며, 시만텍 보안 연구소는 DDoS 공격의 원인이 마이둠(MyDoom) 웜의 변종 및 w32.dozer라는 악성 코드임을 밝혀냄
- W32.dozer는 주로 이메일의 첨부 파일로 확산되는 보안 위협으로 사용자가 첨부 파일을 클릭하면 악성 코드가 사용자 시스템에 다운로드 되도록 하는 것임
- 특히 DDoS는 그 자체가 바이러스는 아니며, 다수의 컴퓨터를 악성코드로 감염시킨 후, 특정 컴퓨터에서 명령을 내리면, 감염된 컴퓨터(즉 좀비PC)에서 명령을 수행하여 특정 사이트에 과도한 트래픽을 보내게 되는 것으로, 결과적으로 공격을 받은 사이트는 정상적인 이용이 불가능해지고, 최악의 경우 서버가 다운되어 이용 불능 상태에 빠질 수 있는 것임
- 그러나 악성코드에 감염되었을 경우, 사용자는 알아채기 힘들고, 사용자 컴퓨터는 영향이 없는 채로 공격에 가담되어, 결론적으로는 대규모 공격이 주요 국가기관 사이트나 대형 포털 사이트에 가해지면서, 국가적으로 큰 손실이 야기될 수 있음
- DDoS에 의한 사이버테러와 정보유출 사건은 지속적으로 발생하고 있는데, 2013년 8월 말, 중국의 인터넷이 대규모 DDoS 공격을 받았고 이로 인해 .cn 도메인 내에 있는 사이트를 접속할 때 잠시 중단되고 느려졌음
- 국가 코드 최상위 도메인(country code top level domain, ccTLD)인 중국의 .cn을 공격한 이번 DDoS 공격은 역사상 가장 큰 규모로 중국 도메인 관리자인 중국 인터넷 네트워크 정보 센터(CNNIC)에 따르면, 첫번째 공격은 베이징 시간으로 일요일 12시를 전후로 시작됐으며, CNNIC은 이 공격으로 인해 다수의 사이트가 중단되었다고 말했다고 함
- 이와 같이 현재 전 세계 네트워크망이 확대됨에 따라 DDoS 공격에 의한 피해 역시 끊임없이 발생하고 있으며, 이러한 시장 상황에서 사용자 컴퓨터에 설치된 악성 프로세스의 구동을 원천 차단할 수 있는 기술의 필요성이 점차 강조되고 있음
- 또한 한국의 경우 북한 세력의 사이버테러로 인해 DDoS의 공격 발생 빈도가 점점 증가하고 있고, 일본의 경우 지난 2011년 3월 청와대와 국가정보원 등 한국 정부 기관을 겨냥해 일어난 DDoS 공격에 일본의 서버와 PC가 이용됐다는 사실이 밝혀짐에 따라 일본과 한국 또한 보안 프로세스의 중요성이 강조되고 있음

■ 문의처	
· 소속	기술사업화실
· 담당자	유준상
· 연락처	042-870-4827, yjs39@ensec.re.kr