(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2008년05월30일
(11) 등록번호 10-0833958
(24) 등록일자 2008년05월26일

(51) Int. Cl.
G06F 11/00 (2006.01)
(21) 출원번호 10-2006-0073334
(22) 출원일자 2006년08월03일
심사청구일자 2006년08월03일
(65) 공개번호 10-2008-0011010
(43) 공개일자 2008년01월31일
(30) 우선권주장
1020060071495 2006년07월28일 대한민국(KR)
(56) 선행기술조사문헌
JP14342106 A*
JP2002342106 A*
US20050187740 A1
US5842002 A
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
고려대학교 산학협력단

(72) 발명자
한제헌

이희조

(74) 대리인
유미특허법인

전체 청구항 수 : 총 18 항 심사관 : 안철용

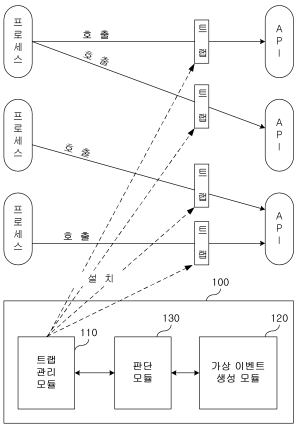
(54) 악성 프로그램을 탐지하는 프로그램이 저장된 기록 매체 및악성 프로그램 탐지 방법

(57) 요 약

대화형 스파이웨어를 효과적으로 탐지할 수 있는 스파이웨어 탐지 프로그램이 개시된다.

스파이웨어 탐지 프로그램은 악성 프로그램이 호출하는 함수에 트랩을 설치하고, 임의의 구간을 선택하여 통상 구간과 가상 이벤트 구간을 결정한 다음, 가상 이벤트 구간에서 하나 이상의 가상 이벤트를 발생시킨다. 그리고 스파이웨어 탐지 프로그램은 통상 구간 및 가상 이벤트 구간에서 트랩이 실행되는 밀도를 각각 계산하여 악성 프로그램의 존재 여부를 판단한다.

대표도 - 도2



특허청구의 범위

청구항 1

삭제

청구항 2

알려지지 않은 프로세스가 사용하는 함수에 트랩을 설치하는 기능;

임의의 시간 구간을 선택하여 통상 구간과 가상 이벤트 구간을 결정하는 기능;

상기 가상 이벤트 구간에서 하나 이상의 가상 이벤트를 발생시키는 기능;

상기 통상 구간에서 상기 트랩이 실행되는 밀도인 제1 밀도를 계산하는 기능;

상기 가상 이벤트 구간에서 상기 트랩이 실행되는 밀도인 제2 밀도를 계산하는 기능;

상기 제1 밀도 및 상기 제2 밀도를 통해 상기 알려지지 않은 프로세스가 악성 프로그램인가를 판단하는 기능을 컴퓨터에 실현하고,

상기 악성 프로그램인가를 판단하는 기능은

상기 제2 밀도가 상기 제1 밀도와 임계값의 합보다 큰 경우에 상기 알려지지 않은 프로세스를 악성 프로그램으로 판단하는 기능을 포함하는 프로그램이 저장된 기록 매체.

청구항 3

제2항에 있어서,

상기 제1 밀도를 계산하는 기능은 상기 트랩이 상기 통상 구간에서 실행되는 횟수를 상기 통상 구간의 길이로 나누어 상기 제1 밀도를 계산하는 기능을 포함하고,

상기 제2 밀도를 계산하는 기능은 상기 트랩이 상기 가상 이벤트 구간에서 실행되는 횟수를 상기 가상 이벤트 구간의 길이로 나누어 상기 제2 밀도를 계산하는 기능을 포함하는 프로그램이 저장된 기록 매체.

청구항 4

제3항에 있어서,

상기 트랩을 설치하는 기능은 상기 트랩을 함수 후킹 방법을 통해 상기 트랩을 설치하는 기능을 포함하는 프로그램이 저장된 기록 매체.

청구항 5

제2항 내지 제4항 중 어느 한 항에 있어서,

상기 트랩을 설치하는 기능은 메시지 후킹 함수, API 후킹 함수, 파일 기록 함수, 레지스트리 기록 함수에 상기 트랩을 설치하는 기능을 포함하고,

상기 악성 프로그램은 키로거이고,

상기 가상 이벤트는 키스트로크 이벤트인 프로그램이 저장된 기록 매체.

청구항 6

제2항 내지 제4항 중 어느 한 항에 있어서,

상기 트랩을 설치하는 기능은 웹페이지 연결 함수에 상기 트랩을 설치하는 기능을 포함하고,

상기 악성 프로그램은 사용자의 요청 웹페이지 주소를 변경하는 웹 리다이렉터이고,

상기 가상 이벤트는 웹페이지 요청 이벤트인 프로그램이 저장된 기록 매체.

청구항 7

제2항 내지 제4항 중 어느 한 항에 있어서,

상기 트랩을 설치하는 기능은 패킷 전송 함수에 상기 트랩을 설치하는 기능을 포함하고,

상기 악성 프로그램은 사용자의 패킷을 가로채는 패킷 스니퍼이고,

상기 가상 이벤트는 패킷 생성 이벤트인 프로그램이 저장된 기록 매체.

청구항 8

제2항 내지 제4항 중 어느 한 항에 있어서,

상기 트랩을 설치하는 기능은 에디트 콘트롤 함수에 상기 트랩을 설치하는 기능을 포함하고,

상기 악성 프로그램은 사용자의 패스워드를 탈취하는 패스워드 스틸러이고,

상기 가상 이벤트는 로그인 이벤트인 프로그램이 저장된 기록 매체.

청구항 9

제2항 내지 제4항 중 어느 한 항에 있어서,

상기 트랩을 설치하는 기능은 팝업창 생성 함수에 상기 트랩을 설치하는 기능을 포함하고,

상기 악성 프로그램은 일정 시간마다 팝엉창을 생성하는 팝업 광고 스파이웨어이고,

상기 가상 이벤트는 타이머 이벤트인 프로그램이 저장된 기록 매체.

청구항 10

제2항 내지 제4항 중 어느 한 항에 있어서,

상기 트랩을 설치하는 기능은 레지스트리 기록 함수에 상기 트랩을 설치하는 기능을 포함하고,

상기 악성 프로그램은 사용자의 시작 페이지 변경을 막는 시작 페이지 스파이웨어이고,

상기 가상 이벤트는 시작 페이지 변경 이벤트인 프로그램이 저장된 기록 매체.

청구항 11

제2항 내지 제4항 중 어느 한 항에 있어서,

상기 트랩을 설치하는 기능은 모뎀 제어 함수에 상기 트랩을 설치하는 기능을 포함하고,

상기 악성 프로그램은 사용 요금이 부과되는 전화 번호에 전화를 거는 다이얼러이고,

상기 가상 이벤트는 모뎀 상태 변화 이벤트인 프로그램이 저장된 기록 매체.

청구항 12

제2항 내지 제4항 중 어느 한 항에 있어서,

상기 트랩을 설치하는 기능은 에디트 콘트롤 함수, URL 콘트롤 함수, 및 웹사이트 연결 함수에 상기 트랩을 설치하는 기능을 포함하고,

상기 악성 프로그램은 사용자의 웹활동 정보를 수집하는 컬렉터이고,

상기 가상 이벤트는 웹사이트 연결 이벤트인 프로그램이 저장된 기록 매체.

청구항 13

제2항 내지 제4항 중 어느 한 항에 있어서,

상기 트랩을 설치하는 기능은 파일 기록 함수에 상기 트랩을 설치하는 기능을 포함하고,

상기 악성 프로그램은 웹페이지에 임의의 링크를 생성하는 링크 크리에이터이고,

상기 가상 이벤트는 히스토리 데이터베이스에서의 웹사이트 연결 이벤트인 프로그램이 저장된 기록 매체.

청구항 14

제2항 내지 제4항 중 어느 한 항에 있어서,

상기 트랩을 설치하는 기능은 레지스트리 수정 함수에 상기 트랩을 설치하는 기능을 포함하고,

상기 악성 프로그램은 툴바 중지를 방지하는 툴바 스파이웨어이고,

상기 가상 이벤트는 툴바 중지 이벤트인 프로그램이 저장된 기록 매체.

청구항 15

제2항 내지 제4항 중 어느 한 항에 있어서,

상기 트랩을 설치하는 기능은 레지스트리 수정 함수에 상기 트랩을 설치하는 기능을 포함하고,

상기 악성 프로그램은 BHO 중지를 방지하는 BHO 스파이웨어이고,

상기 가상 이벤트는 BHO 중지 이벤트인 프로그램이 저장된 기록 매체.

청구항 16

제2항 내지 제4항 중 어느 한 항에 있어서,

상기 트랩을 설치하는 기능은 레지스트리 함수에 상기 트랩을 설치하는 기능을 포함하고,

상기 악성 프로그램은 사용자 설정값을 변경하거나 사용자 설정값이 사용자에 의해 변경되는 것을 막는 사용자 설정 스파이웨어이고,

상기 가상 이벤트는 타이머 이벤트인 프로그램이 저장된 기록 매체.

청구항 17

제2항 내지 제4항 중 어느 한 항에 있어서,

상기 트랩을 설치하는 기능은 레지스트리 함수에 상기 트랩을 설치하는 기능을 포함하고,

상기 악성 프로그램은 시작 프로그램 리스트에서 소정의 시작 프로그램이 삭제되는 것을 막는 시작 프로그램 스파이웨어이고,

상기 가상 이벤트는 시작 프로그램 삭제 이벤트인 프로그램이 저장된 기록 매체.

청구항 18

삭제

청구항 19

알려지지 않은 프로세스가 사용하는 함수에 트랩을 설치하는 단계;

임의의 시간 구간을 선택하여 통상 구간과 가상 이벤트 구간을 결정하는 단계;

상기 가상 이벤트 구간에서 하나 이상의 가상 이벤트를 발생시키는 단계;

상기 통상 구간에서 상기 트랩이 실행되는 밀도인 제1 밀도를 계산하는 단계;

상기 가상 이벤트 구간에서 상기 트랩이 실행되는 밀도인 제2 밀도를 계산하는 단계;

상기 제1 밀도 및 상기 제2 밀도를 통해 상기 알려지지 않은 프로세스가 악성 프로그램인가를 판단하는 단계를 포함하고

상기 악성 프로그램인가를 판단하는 단계는

상기 제2 밀도가 상기 제1 밀도와 임계값의 합보다 큰 경우에 상기 알려지지 않은 프로세스를 악성 프로그램으로 판단하는 단계를 포함하는 악성 프로그램 탐지 방법.

청구항 20

제19항에 있어서,

상기 제1 밀도를 계산하는 단계는 상기 트랩이 상기 통상 구간에서 실행되는 횟수를 상기 통상 구간의 길이로 나누어 상기 제1 밀도를 계산하는 단계를 포함하고,

상기 제2 밀도를 계산하는 단계는 상기 트랩이 상기 가상 이벤트 구간에서 실행되는 횟수를 상기 가상 이벤트 구간의 길이로 나누어 상기 제2 밀도를 계산하는 단계를 포함하는 악성 프로그램 탐지 방법.

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

<5> 본 발명은 악성 프로그램을 탐지하는 프로그램 및 방법에 관한 것이다.

<6> 특히 본 발명은 대화형 스파이웨어를 효과적으로 탐지할 수 있는 프로그램 및 방법에 관한 것이다.

<7> 스파이웨어(Spyware)는 일반적으로 사용자의 PC(personal computer)에 설치되어 사용자의 행위를 감시(Monitoring)하거나, 사용자가 원하지 않는 광고를 제공하려는 목적으로 제작되며, 그 외에도 여러 가지 사용자가 원하지 않는 행위를 한다. 몇 년 전부터 스파이웨어는 많은 문제를 유발시켰으며, 특히 사용자의 행위를 감시하여 사용자의 중요한 정보를 가로채는 스파이웨어는 PC 자체의 자원을 소모시키거나 마비시키는 1차적인 피해뿐 아니라 금전적 피해나 여러 가지 2차 피해까지 유발하는 상황이다.

<8> 스파이웨어는 크게 침투형 스파이웨어(Penetration Spyware)와 대화형 스파이웨어(Dialog Spyware)로 분류할 수 있다. 침투형 스파이웨어는 사용자의 행위에 상관 없이 그 스스로 시스템에 피해를 입히는 스파이웨어로, 멀웨어(Malware), 다운로더(Downloader), 봇(BOT) 등이 이에 해당한다. 멀웨어는 PC의 성능을 저해 시키거나 마비시키는 스파이웨어이고, 봇은 외부에 있는 공격자의 명령을 받아 그 명령대로 동작하는 스파이웨어이다. 그에 반해 대화형 스파이웨어는 사용자의 행위가 방아쇠가 되어 동작을 시작하며, 사용자의 행위를 이용하여 악의적인 행동을 하는 스파이웨어를 말한다. 대화형 스파이웨어로는 키로거(Keylogger), 하이재커(Hijacker), 애드웨어(Adware) 등이 있다. 키로거는 사용자의 행위를 감시하거나 갈무리(Capture)하여 획득한 정보를 제3자에 전송하는 동작을 수행한다. 하이재커는 사용자의 입력 정보를 변경하여 원하지 않는 동작을 하게 하는데, 예를 들어 어떠한 웹 사이트에 접속 하려고 URL(uniform resource locator)을 넣었을 때 광고적인 목적으로 URL을 변경하는 등의 동작을 수행한다. 애드웨어는 사용자의 입력 정보가 있을 때 팝업창(Pop-up browser)을 생성하는 등의 동작을 수행한다.

<9> 대화형 스파이웨어는 사용자의 중요한 정보를 가로채거나 위조할 수 있으므로 심각한 금전적 피해를 입히는 등, 피해가 PC 자체에 그치지 않고 또 다른 2차 피해를 유발 시키고 있다. 최근에는 침투형 스파이웨어와 대화형 스파이웨어가 결합된 형태의 스파이웨어가 출현하고 있다. 예를 들어 봇과 키로거가 결합되어 봇의 전파력과, 키로거의 키스트로크 갈무리(Keystroke capturing) 기능이 결합되어 더 큰 피해를 유발시키고 있다.

<10> 다음은 도 1을 참조하여 대화형 스파이웨어의 동작을 설명한다.

<11> 도 1은 대화형 스파이웨어의 동작을 도시한 도면이다.

<12> 도 1에 도시된 바와 같이 대화형 스파이웨어는 키스트로크 이벤트, 타이머 이벤트, 네트워크 이벤트와 같은 사용자 이벤트에 반응하여 동작한다. 대화형 스파이웨어는 사용자 이벤트를 가로채(Hooking) 다양한 동작을 수행한다. 예를 들어 대화형 스파이웨어는 사용자 이벤트를 가로채고 파일 API(application program interface, 응용 프로그램 인터페이스) 또는 레지스트리 API를 호출하여 가로챈 사용자 이벤트를 파일 또는 레지스트리에 저장할 수도 있다. 또한, 대화형 스파이웨어는 네트워크 API 또는 프로세스 API를 호출하여 가로챈 사용자 이벤트를 네트워크 또는 특정 프로세스로 전송하는 동작을 수행할 수도 있다.

<13> 현재 스파이웨어를 탐지하는데 가장 많이 사용되는 알고리즘은 스파이웨어의 특징을 추출하여 PC에 해당 특징이 나타나면 스파이웨어로 탐지하는 방식이다. 여기서 스파이웨어의 특징에는 스파이웨어의 파일 이름, 프로세스

이름, 메모리 사용 정보, 레지스트리 이름, 데이터 등이 있다. 이러한 방법에 따라 스파이웨어를 탐지하기 위하여는 스파이웨어가 발견된 후 이를 분석하여 특징을 추출한 다음, 추출한 특징을 DB에 입력하여 이 DB를 사용자에게 배포해야 한다. 이때 스파이웨어 출현 시점과 발견 시점 사이의 시간 간격 동안, 그리고 발견 시점과 특징 추출 후 DB 배포 시점까지의 시간 간격 동안에는 사용자에게 스파이웨어의 존재를 통지할 수 없는 문제가 있다.

발명이 이루고자 하는 기술적 과제

<14> 본 발명이 이루고자 하는 기술적 과제는 대화형 스파이웨어를 효과적으로 탐지할 수 있는 프로그램 및 방법을 제공하는 것이다.

발명의 구성 및 작용

<15> 본 발명의 실시예에 따른 기록 매체에 저장된 프로그램은 악성 프로그램이 호출하는 함수에 트랩을 설치하는 기능과, 임의의 구간을 선택하여 통상 구간과 가상 이벤트 구간을 결정하는 기능과, 상기 가상 이벤트 구간에서 하나 이상의 가상 이벤트를 발생시키는 기능과, 상기 통상 구간에서 상기 트랩이 실행되는 밀도인 제1 밀도를 계산하는 기능과, 상기 가상 이벤트 구간에서 상기 트랩이 실행되는 밀도인 제2 밀도를 계산하는 기능과, 상기 제1 밀도 및 상기 제2 밀도를 통해 상기 악성 프로그램의 존재 여부를 판단하는 기능을 포함한다.

<16> 이때, 상기 악성 프로그램의 존재 여부를 판단하는 기능은 상기 제2 밀도가 상기 제1 밀도와 임계값의 합보다 큰 경우에 상기 악성 프로그램이 존재한다고 판단하는 기능을 포함할 수 있다.

<17> 또한 이때, 상기 제1 밀도를 계산하는 기능은 상기 트랩이 상기 통상 구간에서 실행되는 횟수를 상기 통상 구간의 길이로 나누어 상기 제1 밀도를 계산하는 기능을 포함하고, 상기 제2 밀도를 계산하는 기능은 상기 트랩이 상기 가상 이벤트 구간에서 실행되는 횟수를 상기 가상 이벤트 구간의 길이로 나누어 상기 제2 밀도를 계산하는 기능을 포함할 수 있다.

<18> 또한 이때, 상기 트랩을 설치하는 기능은 상기 트랩을 함수 후킹 방법을 통해 상기 트랩을 설치하는 기능을 포함할 수 있다.

<19> 본 발명의 실시예에 따른 악성 프로그램 탐지 방법은 악성 프로그램이 호출하는 함수에 트랩을 설치하는 단계와, 임의의 구간을 선택하여 통상 구간과 가상 이벤트 구간을 결정하는 단계와, 상기 가상 이벤트 구간에서 하나 이상의 가상 이벤트를 발생시키는 단계와, 상기 통상 구간에서 상기 트랩이 실행되는 밀도인 제1 밀도를 계산하는 단계와, 상기 가상 이벤트 구간에서 상기 트랩이 실행되는 밀도인 제2 밀도를 계산하는 단계와, 상기 제1 밀도 및 상기 제2 밀도를 통해 상기 악성 프로그램의 존재 여부를 판단하는 단계를 포함한다.

<20> 아래에서는 첨부한 도면을 참고로 하여 본 발명의 실시예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

<21> 또한 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다.

<22> 또한, 본 명세서에서 기재한 모듈(module)이란 용어는 특정한 기능이나 동작을 처리하는 하나의 단위를 의미하며, 이는 하드웨어나 소프트웨어 또는 하드웨어 및 소프트웨어의 결합으로 구현할 수 있다.

<23> 이하에서는 스파이웨어 대신에 악성 프로그램이라는 용어를 사용하도록 한다.

<24> 다음은 도 2 내지 도 4를 참조하여 본 발명의 실시예에 따른 악성 프로그램 탐지 프로그램(100)을 설명한다.

<25> 도 2는 본 발명의 실시예에 따른 악성 프로그램 탐지 프로그램(100)의 블록도이다.

<26> 도 2에 도시된 바와 같이, 악성 프로그램 탐지 프로그램(100)은 트랩 관리 모듈(110), 가상 이벤트 발생 모듈(120), 판단 모듈(130)을 포함한다.

<27> 트랩 관리 모듈(110)은 알려지지 않은 프로세스(unknown process)가 사용하는 API 함수에 트랩을 설치하고, 설치된 트랩에 걸린 프로세스의 정보, API를 호출할 때 사용하는 인자값, 그리고 설치된 트랩의 실행 횟수에 대한 정보를 판단 모듈(130)에 제공한다. 여기서 알려지지 않은 프로세스는 현재 실행중인 프로세스 중에서 운영체제

가 통상적으로 사용하는 프로세스와 같은 알려진 프로세스를 제외한 것을 말한다. 그리고, 가상 이벤트 발생 모듈(120)은 가상 이벤트를 생성하여 악성 프로그램이 트랩에 빠지도록 한다. 판단 모듈(130)은 임의의 프로세스가 트랩에 빠지는 밀도를 통해 악성 프로그램의 존재를 파악한다.

<28> 도 3은 본 발명의 실시예에 따른 악성 프로그램 탐지 방법의 흐름도이다.

<29> 먼저, 트랩 관리 모듈(110)은 알려지지 않은 프로세스가 사용하는 하나 이상의 API 함수에 트랩을 설치한다(S110). 트랩 관리 모듈(110)은 API Hooking(API 가로채기) 수단 등을 통해 API 함수에 트랩을 설치할 수 있다.

<30> 다음으로, 가상 이벤트 발생 모듈(120)은 통상 구간과 가상 이벤트 구간을 결정한다(S120). 이때, 가상 이벤트 발생 모듈(120)은 악성 프로그램이 통상 구간과 가상 이벤트 구간을 파악하지 못하도록 임의의 구간을 선택하여 통상 구간과 가상 이벤트 구간을 결정할 수 있다.

<31> 그리고 나서, 가상 이벤트 발생 모듈(120)은 가상 이벤트 구간에서 하나 이상의 가상 이벤트를 발생시킨다(S130). 악성 프로그램이 설치되어 있다면, 이 악성 프로그램은 발생한 가상 이벤트를 처리하기 위하여 트랩이 설치된 API 함수를 실행하게 된다. 악성 프로그램은 계속적으로 발생하는 가상 이벤트를 처리하여야 하므로 가상 이벤트가 발생에 실시간으로 반응하여 발생한 가상 이벤트를 처리하여야 한다. 즉, 가상 이벤트의 발생 시점과 악성 프로그램이 가상 이벤트를 처리하기 위한 API 함수 호출 시점 사이의 간격은 매우 짧다. 따라서 악성 프로그램은 가상 이벤트 구간에서 발생된 가상 이벤트를 해당 가상 이벤트 구간에서 처리한다고 볼 수 있다. 악성 프로그램은 가상 이벤트가 발생된 가상 이벤트 구간에서 트랩에 빠지게 되고 트랩을 실행하게 된다.

<32> 그리고, 판단 모듈(130)은 다음의 수학식 1과 같이 통상 구간에서 트랩 실행 밀도(A)를 계산한다(S140).

수학식 1

<33> $$\text{통상 구간에서 트랩 실행 밀도}(A) = \frac{\text{트랩 실행 횟수}}{\text{통상 구간의 길이}}$$

<34> 다음으로, 판단 모듈(130)은 다음의 수학식 2와 같이 가상 이벤트 구간에서 트랩 실행 밀도(B)를 계산한다(S150).

수학식 2

<35> $$\text{가상 이벤트 구간에서 트랩실행밀도}(B) = \frac{\text{트랩 실행 횟수}}{\text{가상 이벤트 구간의 길이}}$$

<36> 그리고 나서, 판단 모듈(130)은 다음의 수학식 3과 같이 가상 이벤트 구간에서의 트랩 실행 밀도가 통상 구간에서의 트랩 실행 밀도보다 임계값 이상으로 큰 경우(S160) 트랩 실행 밀도(A 및 B)에 해당하는 알려지지 않은 프로세스를 악성 프로그램이라고 판단한다(S170).

수학식 3

<37> $if(B \geq A + TH)$ 스파이웨어 탐지

<38> 수학식 3에서 TH는 임계값(Threshold value)이다.

<39> 그리고, 판단 모듈(130)은 악성 프로그램으로 판단된 알려지지 않은 프로세스를 중지시킨다(S180).

<40> 한편, 판단 모듈(130)은 가상 이벤트 구간에서의 트랩 실행 밀도가 통상 구간에서의 트랩 실행 밀도와 임계값의 합보다 작은 경우(S160) 트랩 실행 밀도(A 및 B)에 해당하는 알려지지 않은 프로세스를 악성 프로그램이 아니라고 판단한다(S190).

<41> 악성 프로그램은 통상 구간에서도 필요에 따라 트랩이 설치된 API를 실행하게 된다. 따라서 통상 구간이더라도 트랩 실행 밀도는 소정의 값을 갖게 된다. 그러나 가상 이벤트 구간에서는 가상 이벤트가 발생하므로 악성 프로그램은 이 가상 이벤트를 처리하기 위하여 트랩이 설치된 API를 가상 이벤트 만큼 추가로 실행하게 된다. 따라서 악성 프로그램이 아닌 알려지지 않은 프로세스라면 통상 구간에서의 트랩 실행 밀도와 가상 이벤트 구간에서의 트랩 실행 밀도는 거의 비슷한 값을 갖는다. 반면, 악성 프로그램의 경우에는 이 악성 프로그램이 가상 이벤트를 처리하기 위한 API를 실행하므로 트랩 실행 밀도가 증가하게 된다. 따라서 악성 프로그램의 경우에는 가상

이벤트 구간에서의 트랩 실행 밀도(B)가 통상 구간에서의 트랩 실행 밀도(A)보다 큰 값을 갖게 된다. 다만, 오차가 있을 수 있으므로 판단 모듈(130)은 소정의 임계값을 설정하여 가상 이벤트 구간에서의 트랩 실행 밀도(B)와 통상 구간에서의 트랩 실행 밀도(A)를 비교하여 악성 프로그램의 존재 여부를 판단한다.

<42> 다음은 도 4를 참조하여 다양한 악성 프로그램에 따라 트랩이 설치되는 API 함수를 설명한다.

<43> 도 4는 본 발명의 실시예에 따라 탐지하고자 하는 악성 프로그램과 트랩이 설치되는 API 함수 간의 관계를 나타낸다.

<44> 먼저, 키로거에 대해서 설명한다.

<45> 키로거는 키스트로크 이벤트를 가로채므로 메시지 후킹 함수(Message Hooking Function)나 API 후킹 함수(API Hooking Function)를 실행한다. 또한 키로거는 가로챈 키스트로크 이벤트를 파일 또는 레지스트리에 저장하는 경우도 있으므로 파일 기록 함수(File Write Function)나 레지스트리 기록 함수(Registry Write Function)를 호출할 수도 있다. 뿐만 아니라 키로거는 가로챈 키스트로크 이벤트를 네트워크로 전송하는 경우도 있으므로 네트워크 전송 함수(Network Send Function)를 호출할 수 있다.

<46> 따라서 키로거가 설치되어 있는 경우라면 다음과 같이 키로거의 존재를 파악할 수 있다. 트랩 관리 모듈(110)은 메시지 후킹 함수, API 후킹 함수, 파일 쓰기 함수, 레지스트리 기록 함수 및 네트워크 전송 함수에 트랩을 설치한다. 그리고 가상 이벤트 발생 모듈(120)은 가상 이벤트 구간에서 하나 이상의 키스트로크 이벤트를 발생시킨다. 그리고 나서, 판단 모듈(130)은 통상 구간 및 가상 이벤트 구간에서의 트랩 실행 밀도를 계산하여 키로거의 존재 여부를 파악한다.

<47> 다음으로 웹 리다이렉터(web redirector)에 대해서 설명한다.

<48> 웹 리다이렉터는 사용자가 요청한 웹 페이지의 주소를 가로채서, 사용자의 요청 웹페이지를 광고 등을 위한 웹페이지의 주소로 변경한다. 즉, 웹 리다이렉터는 사용자의 웹페이지 요청 이벤트를 가로채고, 웹페이지 연결 함수를 호출하여 자신이 원하는 웹페이지에 브라우저를 연결시킨다. 이때 웹페이지 연결 함수는 윈도우즈 운영체제에서 브라우저 지원 개체(Browser Helper Object, BHO)라는 확장 프레임워크일 수 있다. 이 BHO는 브라우저가 실행될 때마다 자동으로 실행되는 작은 프로그램으로, 브라우저 내의 이벤트를 효과적으로 제어함으로써 브라우저의 기능을 확장하는데 사용된다.

<49> 웹 리다이렉터가 설치되어 있는 경우라면 다음과 같이 키로거의 존재를 파악할 수 있다. 트랩 관리 모듈(110)은 웹페이지 연결 함수에 트랩을 설치하고, 가상 이벤트 발생 모듈(120)은 웹페이지 요청 이벤트를 발생시킨다. 그리고 나서, 판단 모듈(130)은 트랩 실행 밀도를 계산하여 웹 리다이렉터의 존재 여부를 파악한다.

<50> 다음으로 패킷 스니퍼(packet sniffer)에 대해서 설명한다.

<51> 패킷 스니퍼는 사용자의 패킷을 가로채서 원격의 악성 이용자가 패킷을 엿볼수 있도록 한다. 이를 위하여 패킷 스니퍼는 패킷 생성 이벤트에 반응하고, 가로챈 패킷을 전송하기 위하여 패킷 전송 함수를 호출한다.

<52> 따라서 트랩 관리 모듈(110)은 패킷 전송 함수에 트랩을 설치하고, 가상 이벤트 발생 모듈(120)은 패킷 생성 이벤트를 발생시켜, 판단 모듈(130)은 트랩 실행 밀도를 통해 패킷 스니퍼의 존재 여부를 파악할 수 있다.

<53> 다음으로 패스워드 스틸러(Password stealer)에 대해서 설명한다.

<54> 패스워드 스틸러는 사용자가 웹사이트에 로그인할 때 아이디와 패스워드를 탈취한다. 이를 위하여 패스워드 스틸러는 웹사이트 또는 특정한 응용 프로그램을 이용한 서버로의 로그인에 해당하는 로그인 이벤트에 반응하며, 아이디와 패스워드가 기록된 에디트 콘트롤로부터 정보를 읽어 오기 위하여 에디트 콘트롤 함수를 호출한다. 따라서 악성 프로그램 탐지 프로그램(100)은 에디트 콘트롤 함수에 트랩을 설치하고, 로그인 이벤트를 발생시켜, 트랩 실행 밀도를 통해 패스워드 스틸러의 존재를 파악할 수 있다.

<55> 다음으로 팝업 광고(Popup advertisement) 스파이웨어에 대해서 설명한다.

<56> 팝업 광고 스파이웨어는 일정 시간마다 팝업창(pop-up window)을 생성한다. 이를 위하여 팝업 광고 스파이웨어는 타이머 이벤트에 반응하며, 팝업창 생성 함수를 호출한다. 따라서 악성 프로그램 탐지 프로그램(100)은 팝업창 생성 함수에 트랩을 설치하고, 타이머 이벤트를 발생시켜, 트랩 실행 밀도를 통해 팝업 광고 스파이웨어의 존재를 파악할 수 있다.

<57> 다음으로 시작 페이지(Start page) 스파이웨어에 대해서 설명한다. 시작 페이지 스파이웨어는 사용자가 시작 페

이지를 변경하는 것을 막는다. 이를 위하여 시작 페이지 스파이웨어는 시작 페이지 변경 이벤트에 반응하며, 레지스트리 기록 함수를 호출한다. 따라서 악성 프로그램 탐지 프로그램(100)은 레지스트리 기록 함수에 트랩을 설치하고, 시작 페이지 변경 이벤트를 발생시켜, 트랩 실행 밀도를 통해 시작 페이지 스파이웨어의 존재를 파악할 수 있다. 한편, 시작 페이지 스파이웨어는 특정한 이벤트 없이도 주기적으로 계속 시작 페이지 설정을 변경할 수있기 때문에, 악성 프로그램 탐지 프로그램(100)은 가상 이벤트를 발생시키지 않고 트랩만을 설치하여 트랩 실행 밀도를 통해 시작 페이지 스파이웨어를 탐지할 수 있다.

<58> 다음으로 애드웨어의 일종인 다이얼러(Dialer)에 대해서 설명한다. 다이얼러는 사용 요금이 비싼 전화 번호에 전화를 걸기 위하여 사용자의 모뎀을 사용한다. 이를 위하여 다이얼러는 모뎀 상태 변화 이벤트에 반응하며, 모뎀 제어 함수를 호출한다. 따라서 악성 프로그램 탐지 프로그램(100)은 모뎀 제어 함수에 트랩을 설치하고, 모뎀 상태 변화 이벤트를 발생시켜, 트랩 실행 밀도를 통해 다이얼러의 존재를 파악할 수 있다.

<59> 다음으로 애드웨어의 일종인 컬렉터(Collector)에 대해서 설명한다. 컬렉터는 사용자의 웹활동 정보를 수집한다. 즉, 컬렉터는 사용자가 연결하는 웹사이트, 사용자가 웹사이트를 검색하기 위하여 사용하는 키워드, 사용자가 인터넷을 사용하는 시간 등에 대한 정보를 수집한다. 이를 위하여 컬렉터는 웹사이트 연결 이벤트에 반응한다. 그리고, 컬렉터는 에디트 콘트롤에 기록된 정보를 얻기 위하여 에디트 콘트롤 함수를 호출할 수도 있고, URL 콘트롤에 기록된 URL 정보를 얻기 위하여 URL 콘트롤 함수를 호출할 수도 있다. 그리고, 컬렉터는 웹사이트 연결 함수를 호출할 수도 있다. 따라서 악성 프로그램 탐지 프로그램(100)은 에디트 콘트롤 함수, URL 콘트롤 함수, 웹사이트 연결 함수에 트랩을 설치하고, 웹사이트 연결 이벤트를 발생시켜, 트랩 실행 밀도를 통해 컬렉터의 존재를 파악할 수 있다.

<60> 다음으로 애드웨어의 일종인 링크 크리에이터(Link creator)에 대해서 설명한다. 링크 크리에이터는 바탕화면과 같은 PC의 특정한 위치에 광고 등의 목적을 위한 링크를 생성한다. 링크 크리에이터는 특정한 웹사이트 접속에 반응하기 때문에 사용자가 이전에 접속했던 히스토리 데이터베이스에서의 웹사이트 연결 이벤트에 반응하고, 해당 웹페이지에 링크를 추가하기 위하여 파일 기록 함수를 호출한다. 따라서 악성 프로그램 탐지 프로그램(100)은 파일 기록 함수에 트랩을 설치하고, 히스토리 데이터베이스에서의 웹사이트 연결 이벤트를 발생시켜, 트랩 실행 밀도를 통해 링크 크리에이터의 존재를 파악할 수 있다.

<61> 다음으로 애드웨어의 일종인 툴바(Toolbar) 스파이웨어와 BHO 스파이웨어에 대해서 설명한다. 툴바와 BHO는 악의적 목적으로 사용될 수 있다. 사용자는 악의적으로 사용되는 툴바나 BHO를 발견하는 경우 이를 중지시키게 되는데, 툴바 스파이웨어와 BHO 스파이웨어는 중지되는 툴바나 BHO를 다시 활성화시킨다. 이를 위하여 툴바 스파이웨어와 BHO 스파이웨어는 각각 툴바 중지 이벤트, BHO 중지 이벤트에 반응하며, 중지된 툴바 또는 BHO를 활성화하기 위하여 레지스트리 수정 함수를 호출한다. 따라서 악성 프로그램 탐지 프로그램(100)은 레지스트리 수정 함수에 트랩을 설치하고, 툴바 중지 이벤트 또는 BHO 중지 이벤트를 발생시켜, 트랩 실행 밀도를 통해 툴바 스파이웨어 또는 BHO 스파이웨어의 존재를 파악할 수 있다. 툴바 스파이웨어와 BHO 스파이웨어는 특정한 이벤트가 없어도 주기적으로 계속 자신을 실행 가능하도록 설정을 변경할 수 있기 때문에, 악성 프로그램 탐지 프로그램(100)은 가상 이벤트를 발생시키지 않고 트랩만을 설치하여 트랩 실행 밀도를 통해 툴바 스파이웨어나 BHO 스파이웨어를 탐지할 수 있다.

<62> 다음으로 애드웨어의 일종인 사용자 설정(configureation) 스파이웨어에 대하여 설명한다. 사용자 설정 스파이웨어는 사용자 설정값을 변경하거나 사용자에 의한 변경을 막는다. 이를 위하여 사용자 설정 스파이웨어는 타이머 이벤트에 반응하며, 사용자 설정값을 변경하기 위하여 레지스트리 함수를 호출한다. 따라서 악성 프로그램 탐지 프로그램(100)은 레지스트리 함수에 트랩을 설치하고, 타이머 이벤트를 발생시켜, 트랩 실행 밀도를 통해 사용자 설정 스파이웨어의 존재를 파악할 수 있다.

<63> 다음으로 애드웨어의 일종인 시작 프로그램(Start Programs) 스파이웨어에 대해서 설명한다. 시작 프로그램 스파이웨어는 시작 프로그램 리스트에서 특정 프로그램을 삭제하는 경우 삭제된 프로그램을 다시 시작 프로그램 리스트에 추가하는 동작을 수행한다. 이를 위하여 시작 프로그램 스파이웨어는 시작 프로그램 삭제 이벤트에 반응하고, 레지스트리 함수를 호출한다. 따라서 악성 프로그램 탐지 프로그램(100)은 레지스트리 함수에 트랩을 설치하고, 시작 프로그램 삭제 이벤트를 발생시켜, 트랩 실행 밀도를 통해 시작 프로그램 스파이웨어의 존재를 파악할 수 있다. 시작 프로그램 스파이웨어는 특정한 이벤트가 없어도 주기적으로 계속 자신을 실행 가능하도록 설정을 변경할 수 있기 때문에, 악성 프로그램 탐지 프로그램(100)은 가상 이벤트를 발생시키지 않고 트랩만을 설치하여 트랩 실행 밀도를 통해 시작 프로그램 스파이웨어를 탐지할 수 있다.

<64> 이상에서 설명한 본 발명의 실시예는 장치 및 방법을 통해서만 구현이 되는 것은 아니며, 본 발명의 실시예의

구성에 대응하는 기능을 실현하는 프로그램 또는 그 프로그램이 기록된 기록 매체를 통해 구현될 수도 있으며, 이러한 구현은 앞서 설명한 실시예의 기재로부터 본 발명이 속하는 기술분야의 전문가라면 쉽게 구현할 수 있는 것이다.

<65> 이상에서 본 발명의 실시예에 대하여 상세하게 설명하였지만 본 발명의 권리범위는 이에 한정되는 것은 아니고 다음의 청구범위에서 정의하고 있는 본 발명의 기본 개념을 이용한 당업자의 여러 변형 및 개량 형태 또한 본 발명의 권리범위에 속하는 것이다.

발명의 효과

<66> 본 발명의 실시예에 따르면, 다양한 악성 프로그램이 용이하게 탐지될 수 있다.

<67> 또한, 본 발명의 실시예에 따르면 악성 프로그램이 실시간으로 탐지될 수 있으므로, 기존 탐지 방법이 가지는 스파이웨어를 탐지하지 못하는 시간 간격이 없다.

<68> 뿐만 아니라, 본 발명의 실시예에 따르면 알려지지 않은 스파이웨어도 탐지할 수 있는 장점이 있다.

도면의 간단한 설명

<1> 도 1은 대화형 스파이웨어의 동작을 도시한 도면이다.

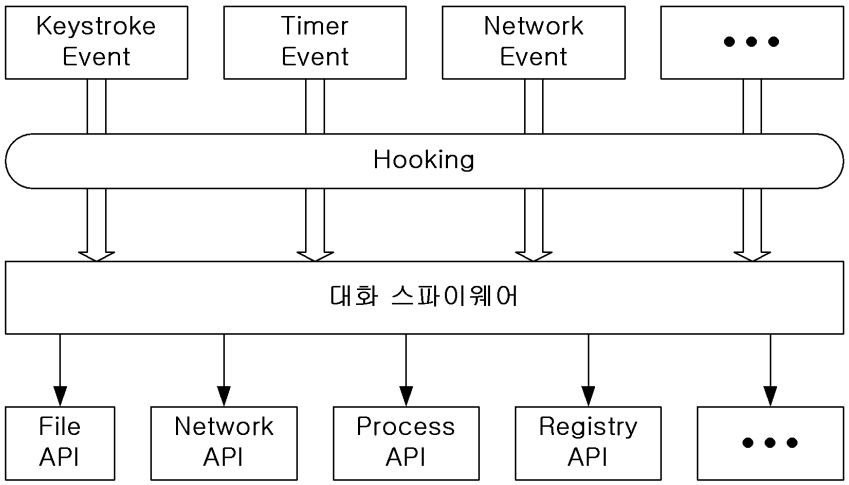
<2> 도 2는 본 발명의 실시예에 따른 악성 프로그램 탐지 프로그램의 블록도이다.

<3> 도 3은 본 발명의 실시예에 따른 악성 프로그램 탐지 방법의 흐름도이다.

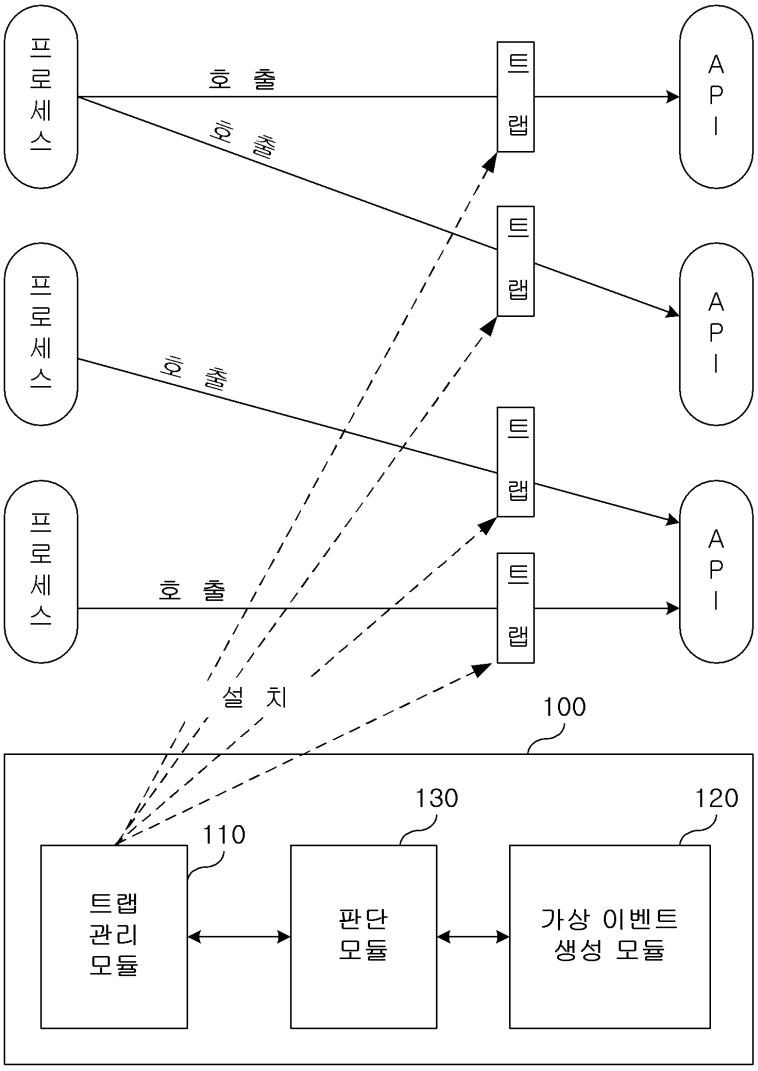
<4> 도 4는 본 발명의 실시예에 따라 탐지하고자 하는 악성 프로그램과 트랩이 설치되는 API 함수 간의 관계를 나타낸다.

도면

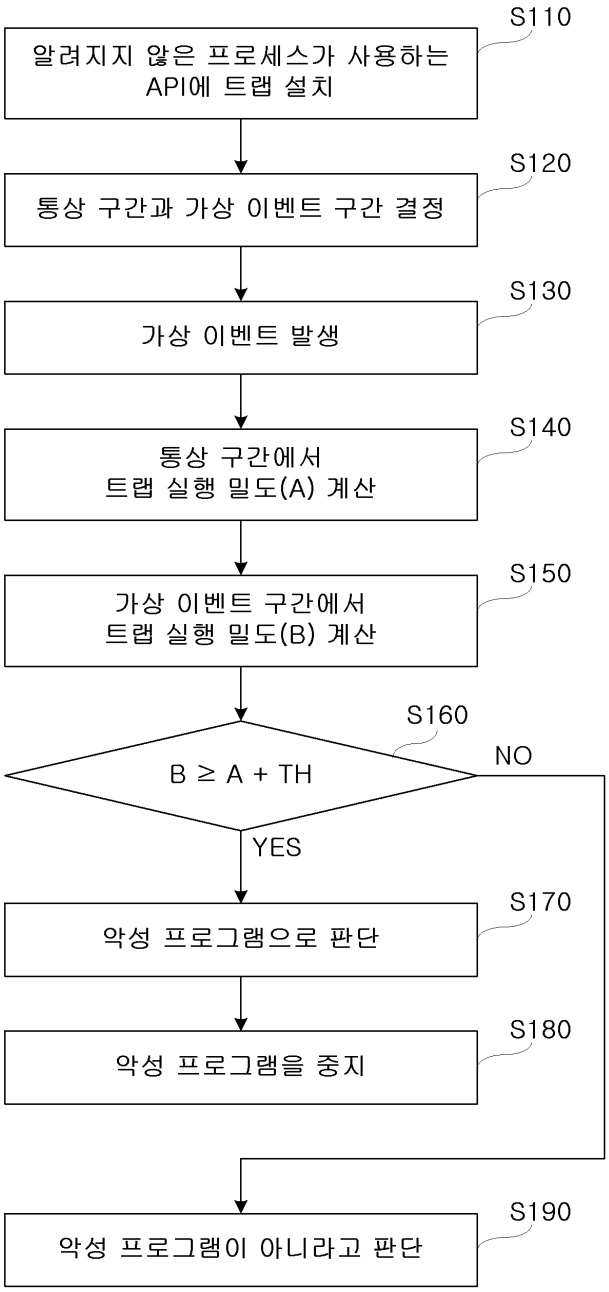
도면1



도면2


프로세스
호 출
호 출
트랩
API
프로세스
호 출
트랩
API
프로세스
호 출
트랩
트랩
API
설 치
100
110
130
120
트랩 관리 모듈
판단 모듈
가상 이벤트 생성 모듈

도면3


S110
알려지지 않은 프로세스가 사용하는 API에 트랩 설치
S120
통상 구간과 가상 이벤트 구간 결정
S130
가상 이벤트 발생
S140
통상 구간에서 트랩 실행 밀도(A) 계산
S150
가상 이벤트 구간에서 트랩 실행 밀도(B) 계산
S160
B ≥ A + TH
NO
YES
S170
악성 프로그램으로 판단
S180
악성 프로그램을 중지
S190
악성 프로그램이 아니라고 판단

도면4

Dialog Spywares	HoneyID	Trap
Keylogger	Keystroke Event	Message Hooking Function API Hooking Function File, Registry Write Function Network Send Function
Web redirector	To connect to the website using a web browser	Connecting function of web browser helper module
Packet sniffer	Generating TCP, UDP packet event	TCP, UDP send function
Password stealer	Making web login situation	Edit control function
Popup advertisement	Timer event	Creating popup windows function
Start page	Changing default start page on web browser	Writing to registry function (It should be used the parameters of function call)
Dialer	Turning on and off continuously modem status	Connecting functions that used for the modem.
Collector	To connect to the website using a web browser and surf Internet	Edit control function URL control function Web connection function
Link creator	To connect web site among history database	File write function
Malicious Toolbar, BHO	Turning off toolbar and BHO on web browser	Modifying registry function (It should be used the parameters of function call)
Holding configuration	Timer event	Registry function (It should be used the parameters of function call)
Start programs	To remove one from auto start extensibility points list of operating system	Registry function (It should be used the parameters of function call)