



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2009년11월09일
(11) 등록번호 10-0925401
(24) 등록일자 2009년10월30일

(51) Int. Cl.

G06F 21/22 (2006.01) G06F 21/00 (2006.01)

(21) 출원번호 10-2008-0013596

(22) 출원일자 2008년02월14일

심사청구일자 2008년02월14일

(65) 공개번호 10-2009-0088198

(43) 공개일자 2009년08월19일

(56) 선행기술조사문헌

KR1020020097344 A*

KR1020070049511 A*

*는 심사관에 의하여 인용된 문헌

(73) 특허권자

주식회사 안철수연구소

서울 영등포구 여의도동 12 씨씨엠빌딩 6층

(72) 발명자

고향훈

강원 춘천시 퇴계동 현대1차아파트 107동 1104호

(74) 대리인

김문재

전체 청구항 수 : 총 13 항

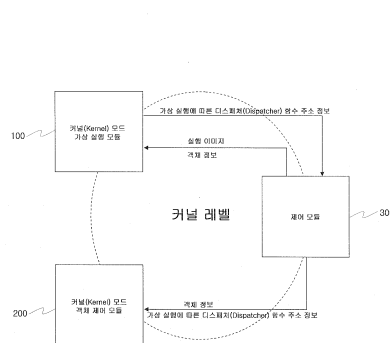
심사관 : 이우찬

(54) 커널 모드의 악성 행위 검출 시스템 및 그 방법

(57) 요약

본 발명은 커널(Kernel) 모드의 악성 행위 검출 시스템 및 그 방법을 개시한다. 즉, 임의의 커널 모드 드라이버에 대한 실행 이미지 파일 및 객체 정보를 전달받아 상기 임의의 커널 모드 드라이버를 메모리에 로드하여 가상으로 구동하고, 상기 임의의 커널 모드 드라이버의 가상 구동에 따라 산출되는 디스패처(Dispatcher) 함수의 상기 메모리 상 주소 정보를 반환하는 커널 모드 가상 실행 모듈; 및 상기 임의의 커널 모드 드라이버에 대한 객체 정보를 토대로 상기 임의의 커널 모드 드라이버의 실제 구동에 따라 산출되는 디스패처 함수의 메모리 상의 실제 주소를 파악하며, 상기 파악된 상기 디스패처 함수의 실제 주소 정보와 상기 커널 모드 가상 실행 모듈로부터 반환되는 주소 정보를 비교하여 상이할 경우, 상기 디스패처 함수의 주소를 상기 반환된 주소 정보로 변경하는 커널 모드 객체 제어 모듈을 포함함으로써, 커널 모드 객체 내 디스패처 함수 주소가 변경되는 악성 행위에 대한 감지 및 복구가 용이하다.

대표도 - 도1



특허청구의 범위

청구항 1

커널(Kernel) 모드의 악성 행위 검출 시스템에 있어서,

임의의 커널 모드 드라이버에 대한 실행 이미지 파일 및 객체 정보를 전달받아 상기 임의의 커널 모드 드라이버를 메모리에 로드하여 가상으로 구동하고, 상기 임의의 커널 모드 드라이버의 상기 커널 모드 가상 실행 모듈로부터 가상 구동에 따라 산출된 후 반환되는 주소 정보를 비교하여 상이할 경우를 반환하는 커널 모드 가상 실행 모듈; 및

상기 임의의 커널 모드 드라이버에 대한 객체 정보를 토대로 상기 임의의 커널 모드 드라이버의 실제 구동에 따라 산출되는 디스패처 함수의 메모리 상의 실제 주소를 파악하며, 상기 파악된 상기 디스패처 함수의 실제 주소 정보와 상기 커널 모드 가상 실행 모듈로부터 반환되는 주소 정보를 비교하여 상이할 경우, 상기 디스패처 함수의 주소를 상기 반환된 주소 정보로 변경하는 커널 모드 객체 제어 모듈을 포함하는 것을 특징으로 하는 커널 모드의 악성 행위 검출 시스템.

청구항 2

제 1 항에 있어서, 상기 시스템은,

상기 임의의 커널 모드 드라이버에 대한 실행 이미지 파일 및 객체 정보를 제공하며, 상기 커널 모드 가상 실행 모듈로부터 반환되는 디스패처 함수의 주소 정보를 상기 커널 모드 객체 제어 모듈로 전달하는 제어 모듈을 더 포함하는 것을 특징으로 하는 커널 모드의 악성 행위 검출 시스템.

청구항 3

제 1 항에 있어서, 상기 커널 모드 가상 실행 모듈은,

상기 실행 이미지 파일의 크기와 동일한 크기의 메모리를 할당하여 상기 실행 이미지를 로딩하며, 상기 메모리의 시작 주소를 기준으로 상기 로딩된 실행 이미지에 대한 실행 명령의 주소 값을 재배치하는 것을 특징으로 하는 커널 모드의 악성 행위 검출 시스템.

청구항 4

제 3 항에 있어서, 상기 커널 모드 가상 실행 모듈은,

IAT(Import Address Table)의 함수 목록을 검색하여 지원 가능한 함수를 선별하고, 상기 선별된 함수의 주소를 자체 처리를 위한 지원 대상 주소로 변환하여 상기 메모리에 저장하는 것을 특징으로 하는 커널 모드의 악성 행위 검출 시스템.

청구항 5

제 4 항에 있어서, 상기 커널 모드 가상 실행 모듈은,

상기 객체 정보에 포함된 상기 임의의 커널 모드 드라이버의 구동에 따른 호출 대상 함수 목록을 토대로, 해당 함수의 상기 지원 대상 주소를 상기 메모리 상의 실제 함수 주소로 변경하는 것을 특징으로 하는 커널 모드의 악성 행위 검출 시스템.

청구항 6

제 5 항에 있어서, 상기 커널 모드 가상 실행 모듈은,

상기 객체 정보에 포함된 인수 정보를 통해 메모리 상의 실제 함수 주소로 변환된 상기 해당 함수의 실행 명령을 실행하는 것을 특징으로 하는 커널 모드의 악성 행위 검출 시스템.

청구항 7

제 1 항에 있어서, 상기 커널 모드 객체 제어 모듈은,

상기 객체 정보에 포함된 상기 임의의 커널 모드 드라이버에 대한 이름 정보를 토대로 상기 임의의 커널 모드

드라이버에 대한 실제 구동에 따른 메모리 상의 로딩 위치를 확인하여 상기 임의의 커널 모드 드라이버의 실제 구동에 따라 산출되는 상기 디스패처 함수의 메모리 상의 실제 주소를 파악하는 것을 특징으로 하는 커널 모드의 악성 행위 검출 시스템.

청구항 8

제 1 항에 있어서, 상기 커널 모드 객체 제어 모듈은,

상기 파악된 상기 디스패처 함수의 실제 주소 정보와 상기 커널 모드 가상 실행 모듈로부터 반환되는 주소 정보를 동일 기준의 절대 주소로 변환하여 상호 비교하는 것을 특징으로 하는 커널 모드의 악성 행위 검출 시스템.

청구항 9

커널(Kernel) 모드의 악성 행위 검출 방법에 있어서,

a) 임의의 커널 모드 드라이버에 대한 실행 이미지 파일 및 객체 정보를 전달받아 상기 임의의 커널 모드 드라이버를 메모리에 로드하여 가상으로 구동하는 단계;

b) 상기 임의의 커널 모드 드라이버의 가상 구동에 따라 산출되는 디스패처(Dispatcher) 함수의 상기 메모리 상의 주소 정보를 반환하는 단계;

c) 상기 임의의 커널 모드 드라이버에 대한 객체 정보를 토대로 상기 임의의 커널 모드 드라이버의 실제 구동에 따라 산출되는 디스패처 함수의 메모리 상의 실제 주소를 파악하는 단계; 및

상기 파악된 상기 디스패처 함수의 실제 주소 정보와 상기 커널 모드 가상 실행 모듈로부터 가상 구동에 따라 산출된 후 반환되는 주소 정보를 비교하는 단계를 포함하는 것을 특징으로 하는 커널 모드의 악성 행위 검출 방법.

청구항 10

제 9 항에 있어서, 상기 방법은,

e) 상기 'd) 단계'를 통한 비교 결과, 상이할 경우 상기 디스패처 함수의 주소를 상기 반환된 주소 정보로 변경하는 단계를 더 포함하는 것을 특징으로 하는 커널 모드의 악성 행위 검출 방법.

청구항 11

제 9 항에 있어서, 상기 a) 단계는,

a-1) 상기 실행 이미지 파일의 크기와 동일한 크기의 메모리를 할당하여 상기 실행 이미지를 로딩하는 단계;

a-2) 상기 메모리의 시작 주소를 기준으로 상기 로딩된 실행 이미지에 대한 실행 명령의 주소 값을 재배치하는 단계;

a-3) IAT(Import Address Table)의 함수 목록을 검색하여 지원 가능한 함수를 선별하는 단계;

a-4) 상기 선별된 함수의 주소를 자체 처리를 위한 지원 대상 주소로 변환하여 상기 메모리에 저장하는 단계;

a-5) 상기 객체 정보에 포함된 상기 임의의 커널 모드 드라이버의 구동에 따른 호출 대상 함수 목록을 토대로, 해당 함수의 상기 지원 대상 주소를 상기 메모리 상의 실제 함수 주소로 변경하는 단계; 및

a-6) 상기 객체 정보에 포함된 인수 정보를 통해 메모리 상의 실제 함수 주소로 변환된 상기 해당 함수의 실행 명령을 실행하는 단계를 포함하는 것을 특징으로 하는 커널 모드의 악성 행위 검출 방법.

청구항 12

제 9 항에 있어서, 상기 c) 단계는,

c-1) 상기 객체 정보에 포함된 상기 임의의 커널 모드 드라이버에 대한 이름 정보를 토대로 상기 임의의 커널 모드 드라이버의 실제 구동에 따른 메모리 상의 로딩 위치를 확인하는 단계; 및

c-2) 상기 확인된 메모리 상의 로딩 위치를 토대로, 상기 임의의 커널 모드 드라이버의 실제 구동에 따라 산출되는 상기 디스패처 함수의 메모리 상의 실제 주소를 파악하는 단계를 포함하는 것을 특징으로 하는 커널 모드

의 악성 행위 검출 방법.

청구항 13

제 10 항에 있어서, 상기 d) 단계는,

상기 파악된 상기 디스패처 함수의 실제 주소 정보와 상기 커널 모드 가상 실행 모듈로부터 반환되는 주소 정보를 동일 기준의 절대 주소로 변환하여 상호 비교하는 것을 특징으로 하는 커널 모드의 악성 행위 검출 방법.

명세서

발명의 상세한 설명

기술 분야

- <1> 본 발명은 커널(Kernel) 모드의 악성 행위를 검출하고, 이를 복구하기 위한 것으로, 보다 상세하게는, 가상 실행을 산출된 디스패처(Dispatcher) 함수 주소와 실제 커널 모드 드라이버의 구동에 따른 디스패처 함수 주소를 비교하여 변조 여부를 확인하고 이를 복구하는 커널 모드의 악성 행위 검출 시스템 및 그 방법에 관한 것이다.

배경 기술

- <2> 근래의 악성 프로그램들은 과거 응용 프로그램 형태로 동작하거나 특정 응용 프로그램을 감염시켜 악성 행위를 하던 것과 달리 커널 모드(Kernel Mode) 라는 운영체제의 관리 기능이 동작하는 특별한 환경에서 동작하도록 만들어져 그 악성 행위가 더욱 강력해짐에 따라, 안티 바이러스(Anti-Virus) 프로그램에서 이를 진단하거나 치료하기가 어려워지고 있는 실정이다.
- <3> 특히, 커널 모드 드라이버의 객체내에 있는 디스패처(Dispatcher) 함수 주소를 변경하여 악성 행위를 하는 경우, 예컨대, 정상적인 운영체제의 드라이버간 I/O를 자신의 함수로 변경함으로써 이를 가로채고 악성 행위를 수행하는 경우에는 이를 진단 및 치료하기가 더욱 어렵다.
- <4> 이와 관련하여, 지금까지는 이러한 악성 프로그램에 의해 변경된 커널 모드 드라이버 객체내의 디스패처 함수 주소에 대해 악성 프로그램의 실행 명령을 분석하여 원본 함수 주소를 찾아내고 이를 다시 커널 모드 드라이버 객체내에 저장해 주는 방법을 통해 해당 악성 행위에 대응하였다.
- <5> 그러나, 상술한 방법은 악성 행위 진단 및 치료하는데 있어서 많은 시간이 소요된다는 단점이 있으며, 더욱이, 상술한 악성 행위의 진단 및 치료 동작에 대한 분석 결과를 그대로 반영하는 프로그램이 존재하지 않아 커널 모드에서 이루어지는 악성 행위에 대한 대응에 한계가 있다.
- <6> 이에 따라, 현재 커널 모드에서의 악성 행위, 보다 구체적으로 커널 모드 객체 내 디스패처 함수 주소가 변경되는 것에 대해 이를 감지하여 빠르고 원래 함수 주소로 안정되게 복구하여 주는 방안이 시급히 필요한 실정이다.

발명의 내용

해결 하고자하는 과제

- <7> 본 발명은 상기한 바와 같이 선행 기술에 내재되었던 문제점을 해결하기 위해 창작된 것으로, 본 발명의 목적은 가상 실행을 통해 산출된 디스패처(Dispatcher) 함수 주소를 토대로 실제 커널 모드 드라이버의 구동에 따른 디스패처 함수 주소의 변조 여부를 확인하고 이를 복구하는 커널 모드의 악성 행위 검출 시스템 및 그 방법을 제공함에 있다.

과제 해결수단

- <8> 상술한 목적을 달성하기 위한 본 발명의 일면에 따라, 커널(Kernel) 모드의 악성 행위 검출 시스템이 제공되며: 이 시스템은, 임의의 커널 모드 드라이버에 대한 실행 이미지 파일 및 객체 정보를 전달받아 상기 임의의 커널 모드 드라이버를 메모리에 로드하여 가상으로 구동하고, 상기 임의의 커널 모드 드라이버의 가상 구동에 따라 산출되는 디스패처(Dispatcher) 함수의 상기 메모리 상 주소 정보를 반환하는 커널 모드 가상 실행 모듈; 및 상기 임의의 커널 모드 드라이버에 대한 객체 정보를 토대로 상기 임의의 커널 모드 드라이버의 실제 구동에 따라 산출되는 디스패처 함수의 메모리 상의 실제 주소를 파악하며, 상기 파악된 상기 디스패처 함수의 실제 주소 정

보와 상기 커널 모드 가상 실행 모듈로부터 반환되는 주소 정보를 비교하여 상이할 경우, 상기 디스패처 함수의 주소를 상기 반환된 주소 정보로 변경하는 커널 모드 객체 제어 모듈을 포함하는 것을 특징으로 한다.

- <9> 바람직하게는, 상기 시스템은, 상기 임의의 커널 모드 드라이버에 대한 실행 이미지 파일 및 객체 정보를 제공하며, 상기 커널 모드 가상 실행 모듈로부터 반환되는 디스패처 함수의 주소 정보를 상기 커널 모드 객체 제어 모듈로 전달하는 제어 모듈을 더 포함하는 것을 특징으로 한다.
- <10> 바람직하게는, 상기 커널 모드 가상 실행 모듈은, 상기 실행 이미지 파일의 크기와 동일한 크기의 메모리를 할당하여 상기 실행 이미지를 로딩하며, 상기 메모리의 시작 주소를 기준으로 상기 로딩된 실행 이미지에 대한 실행 명령의 주소 값을 재배치하는 것을 특징으로 한다.
- <11> 바람직하게는, 상기 커널 모드 가상 실행 모듈은, IAT(Import Address Table)의 함수 목록을 검색하여 지원 가능한 함수를 선별하고, 상기 선별된 함수의 주소를 자체 처리를 위한 지원 대상 주소로 변환하여 상기 메모리에 저장하는 것을 특징으로 한다.
- <12> 바람직하게는, 상기 커널 모드 가상 실행 모듈은, 상기 객체 정보에 포함된 상기 임의의 커널 모드 드라이버의 구동에 따른 호출 대상 함수 목록을 토대로, 해당 함수의 상기 지원 대상 주소를 상기 메모리 상의 실제 함수 주소로 변경하는 것을 특징으로 한다.
- <13> 바람직하게는, 상기 커널 모드 가상 실행 모듈은, 상기 객체 정보에 포함된 인수 정보를 통해 메모리 상의 실제 함수 주소로 변환된 상기 해당 함수의 실행 명령을 실행하는 것을 특징으로 한다.
- <14> 바람직하게는, 상기 커널 모드 객체 제어 모듈은, 상기 객체 정보에 포함된 상기 임의의 커널 모드 드라이버에 대한 이름 정보를 토대로 상기 임의의 커널 모드 드라이버에 대한 실제 구동에 따른 메모리 상의 로딩 위치를 확인하여 상기 임의의 커널 모드 드라이버의 실제 구동에 따라 산출되는 상기 디스패처 함수의 메모리 상의 실제 주소를 파악하는 것을 특징으로 한다.
- <15> 바람직하게는, 상기 커널 모드 객체 제어 모듈은, 상기 파악된 상기 디스패처 함수의 실제 주소 정보와 상기 커널 모드 가상 실행 모듈로부터 반환되는 주소 정보를 동일 기준의 절대 주소로 변환하여 상호 비교하는 것을 특징으로 한다.
- <16> 본 발명의 또 다른 일면에 따라, 커널(Kernel) 모드의 악성 행위 검출 방법이 제공되며: 이 방법은, a) 임의의 커널 모드 드라이버에 대한 실행 이미지 파일 및 객체 정보를 전달받아 상기 임의의 커널 모드 드라이버를 메모리에 로드하여 가상으로 구동하는 단계; b) 상기 임의의 커널 모드 드라이버의 가상 구동에 따라 산출되는 디스패처(Dispatcher) 함수의 상기 메모리 상의 주소 정보를 반환하는 단계; c) 상기 임의의 커널 모드 드라이버에 대한 객체 정보를 토대로 상기 임의의 커널 모드 드라이버의 실제 구동에 따라 산출되는 디스패처 함수의 메모리 상의 실제 주소를 파악하는 단계; 및 d) 상기 파악된 상기 디스패처 함수의 실제 주소 정보와 상기 커널 모드 가상 실행 모듈로부터 반환되는 주소 정보를 비교하는 단계를 포함하는 것을 특징으로 한다.
- <17> 바람직하게는, 상기 방법은, e) 상기 'd) 단계'를 통한 비교 결과, 상이할 경우 상기 디스패처 함수의 주소를 상기 반환된 주소 정보로 변경하는 단계를 더 포함하는 것을 특징으로 한다.
- <18> 바람직하게는, 상기 a) 단계는, a-1) 상기 실행 이미지 파일의 크기와 동일한 크기의 메모리를 할당하여 상기 실행 이미지를 로딩하는 단계; a-2) 상기 메모리의 시작 주소를 기준으로 상기 로딩된 실행 이미지에 대한 실행 명령의 주소 값을 재배치하는 단계; a-3) IAT(Import Address Table)의 함수 목록을 검색하여 지원 가능한 함수를 선별하는 단계; a-4) 상기 선별된 함수의 주소를 자체 처리를 위한 지원 대상 주소로 변환하여 상기 메모리에 저장하는 단계; a-5) 상기 객체 정보에 포함된 상기 임의의 커널 모드 드라이버의 구동에 따른 호출 대상 함수 목록을 토대로, 해당 함수의 상기 지원 대상 주소를 상기 메모리 상의 실제 함수 주소로 변경하는 단계; 및 a-6) 상기 객체 정보에 포함된 인수 정보를 통해 메모리 상의 실제 함수 주소로 변환된 상기 해당 함수의 실행 명령을 실행하는 단계를 포함하는 것을 특징으로 한다.
- <19> 바람직하게는, 상기 c) 단계는, c-1) 상기 객체 정보에 포함된 상기 임의의 커널 모드 드라이버에 대한 이름 정보를 토대로 상기 임의의 커널 모드 드라이버의 실제 구동에 따른 메모리 상의 로딩 위치를 확인하는 단계; 및 c-2) 상기 확인된 메모리 상의 로딩 위치를 토대로, 상기 임의의 커널 모드 드라이버의 실제 구동에 따라 산출되는 상기 디스패처 함수의 메모리 상의 실제 주소를 파악하는 단계를 포함하는 것을 특징으로 한다.
- <20> 바람직하게는, 상기 d) 단계는, 상기 파악된 상기 디스패처 함수의 실제 주소 정보와 상기 커널 모드 가상 실행

모듈로부터 반환되는 주소 정보를 동일 기준의 절대 주소로 변환하여 상호 비교하는 것을 특징으로 한다.

효 과

<21> 본 발명에 따른 커널(Kernel) 모드의 악성 행위 검출 시스템 및 그 방법은 커널 모드 드라이버를 가상으로 실행하여 그 실행 결과로 저장된 임의의 커널 모드 드라이버의 구동에 따른 디스패처(Dispatcher) 함수의 주소를 구하고, 이를 실제 커널 모드 드라이버의 구동에 따른 디스패처 함수의 주소와 비교하여 다를 경우, 이를 가상 실행에 따른 주소 값으로 변경함으로써, 커널 모드 객체 내 디스패처 함수 주소가 변경되는 악성 행위를 빠르게 감지하고 원래 함수 주소로 복구할 수 있다.

<22> 아울러, 본 발명에 따른 커널(Kernel) 모드의 악성 행위 검출 시스템 및 그 방법은 변경 전 디스패처 함수의 주소를 찾기 위해 가상 실행 환경을 적용함에 따라 실제 실행 중인 컴퓨터 환경에는 아무런 영향을 주지 않아 안정적으로 동작할 수 있다

발명의 실시를 위한 구체적인 내용

<23> 이하에서는 첨부한 도면을 참조하여 본 발명의 바람직한 실시예를 상술하기로 한다.

<24> 도 1에는 본 발명의 실시예에 따른 커널(Kernel) 모드의 악성 행위 검출 시스템의 개략적인 구성도를 도시한다.

<25> 도 1에 도시한 바와 같이, 상기 시스템은 임의의 커널 모드 드라이버에 대한 실행이미지 파일을 메모리에 로드하고, 이를 가상 환경에서 실행함으로써 산출되는 디스패처(Dispatcher) 함수의 주소를 반환하는 커널 모드 가상 실행 모듈(100); 상기 임의의 커널 모드 드라이버 객체 내 디스패처 함수 주소의 변경 여부를 확인하고, 이를 원래 값으로 복구하는 커널 모드 객체 제어 모듈(200); 및 상기 커널 모드 가상 실행 모듈(100)과 커널 모드 객체 제어 모듈(200)의 구동을 제어하며 상기 임의의 커널 모드 드라이버에 대한 실행 이미지 파일 및 객체 정보를 제공하며, 상기 커널 모드 가상 실행 모듈(100)로부터 반환되는 디스패처 함수의 주소 정보를 커널 모드 객체 제어 모듈(200)로 전달하는 제어 모듈(300)을 포함하는 구성을 갖는다.

<26> 상기 커널 모드 가상 실행 모듈(100)은 임의의 커널 모드 드라이버에 대한 실행 이미지 파일 및 객체 정보를 제어 모듈(300)로부터 전달받아 상기 임의의 커널 모드 드라이버를 메모리에 로드하여 가상으로 구동한다.

<27> 보다 구체적으로 커널 모드 가상 실행 모듈(100)은 제어 모듈(300)로부터 전달되는 실행 이미지 파일의 크기와 동일한 크기의 메모리를 할당하여 상기 실행 이미지를 해당 위치에 로딩한다.

<28> 이때, 커널 모드 가상 실행 모듈(100)은 할당된 메모리의 시작 주소를 기준으로 상기 로딩된 실행 이미지에 대한 실행 명령의 주소 값을 재배치함으로써 메모리 상에서 실행 가능하도록 한다.

<29> 이와 더불어, 커널 모드 가상 실행 모듈(100)은, IAT(Import Address Table)의 함수 목록을 검색하여 지원 가능한 함수를 선별하고, 상기 선별된 함수의 주소를 자체 처리를 위한 지원 대상 주소로 변환하여 메모리에 저장한다. 여기서, 상기 메모리에 저장되는 함수는 주로 커널이 제공하는 함수로써, 예컨대, 'KeInitializeSpinLock' 등을 커널 모드 가상 실행 모듈(100)의 동작 환경에 맞도록 구현한 함수이다. 한편, IAT 영역에는 프로그램이 필요한 함수의 주소뿐만 아니라 그 함수가 포함된 다른 모듈의 이름을 포함하고 있으므로 커널 모드 가상 실행 모듈(100)은 IAT에 포함된 다른 모듈도 상술한 방식을 통해 메모리에 저장함이 바람직하다.

<30> 또한, 커널 모드 가상 실행 모듈(100)은 제어 모듈(300)로부터 전달되는 객체 정보에 포함된 상기 임의의 커널 모드 드라이버의 구동에 따른 호출 대상 함수 목록(주소 정보 포함)을 토대로, 해당 함수의 상기 지원 대상 주소를 상기 메모리 상의 실제 함수 주소로 변경한다.

<31> 아울러, 커널 모드 가상 실행 모듈(100)은, 제어 모듈(300)로부터 전달되는 객체 정보에 포함된 인수 정보를 통해 메모리 상의 실제 함수 주소로 변환된 상기 해당 함수의 실행 명령을 실행한다.

<32> 또한, 커널 모드 가상 실행 모듈(100)은 상기 임의의 커널 모드 드라이버의 가상 구동에 따라 산출되는 디스패처(Dispatcher) 함수의 상기 메모리 상의 주소 정보를 제어 모듈(300)로 반환한다. 즉, 해당 함수의 실행이 종료되거나 또는 커널 모드 가상 실행 모듈(100)의 미구현 함수의 문제 등으로 인한 오류가 발생할 경우, 커널 모드 가상 실행 모듈(100)은 구동을 종료하고 해당 결과 값을 반환한다.

<33> 상기 커널 모드 객체 제어 모듈(200)은 제어 대상인 상기 임의의 커널 모드 드라이버의 실제 구동에 따라 산출되는 상기 디스패처 함수의 메모리 상의 실제 주소를 파악한다.

- <34> 보다 구체적으로, 커널 모드 객체 제어 모듈(200)은 제어 모듈(300)로부터 전달되는 객체 정보에 포함된 임의의 커널 모드 드라이버에 대한 이름 정보를 토대로 상기 임의의 커널 모드 드라이버에 대한 실제 구동에 따른 메모리 상의 로딩 위치를 확인한다. 더 나아가, 커널 모드 객체 제어 모듈(200)은 상기 확인된 임의의 커널 모드 드라이버의 메모리 상의 로딩 위치를 토대로, 상기 임의의 커널 모드 드라이버의 실제 구동에 따라 산출되는 상기 디스패처 함수의 메모리 상의 실제 주소를 파악한다.
- <35> 또한, 커널 모드 객체 제어 모듈(200)은 상기 파악된 디스패처 함수의 실제 주소 정보와 커널 모드 가상 실행 모듈(100)로부터 반환되는 주소 정보를 비교하여 서로 상이할 경우, 상기 실제 구동에 따른 디스패처 함수의 주소를 커널 모드 가상 실행 모듈(100)로부터 반환된 주소 정보로 변경한다. 이때, 커널 모드 객체 제어 모듈(200)은 상기 디스패처 함수의 실제 주소 정보와 상기 커널 모드 가상 실행 모듈(100)로부터 반환되는 주소 정보를 동일 기준의 절대 주소로 변환하여 상호 비교한다.
- <36> 이하, 도 2를 참조하여 본 발명의 실시예에 따른 커널(Kernel) 모드의 악성 행위 검출 방법을 설명하기로 한다. 여기서, 도 2는 커널 모드의 악성 행위 검출 방법을 설명하기 위한 개략적인 순서도이다.
- <37> 먼저, 임의의 커널 모드 드라이버에 대한 실행 이미지 파일 및 객체 정보를 전달받아 상기 임의의 커널 모드 드라이버를 메모리에 로드하여 가상으로 구동한다. 바람직하게는, 커널 모드 가상 실행 모듈(100)이 제어 모듈(300)로부터 전달되는 실행 이미지 파일의 크기와 동일한 크기의 메모리를 할당하여 상기 실행 이미지를 해당 위치에 로딩한다(S110-S120). 이때, 커널 모드 가상 실행 모듈(100)은 할당된 메모리의 시작 주소를 기준으로 상기 로딩된 실행 이미지에 대한 실행 명령의 주소 값을 재배치함으로써 메모리 상에서 실행 가능하도록 한다(S130). 이와 더불어, 커널 모드 가상 실행 모듈(100)이, IAT(Import Address Table)의 함수 목록을 검색하여 지원 가능한 함수를 선별하고, 상기 선별된 함수의 주소를 자체 처리를 위한 지원 대상 주소로 변환하여 메모리에 저장한다(S140-S150). 한편, IAT 영역에는 프로그램이 필요한 함수의 주소뿐만 아니라 그 함수가 포함된 다른 모듈의 이름을 포함하고 있으므로 커널 모드 가상 실행 모듈(100)은 IAT에 포함된 다른 모듈과 아울러, 제어 모듈(100)이 지정한 실행 이미지가 더 있을 경우 상술한 단계 'S110' 내지 단계 'S150'을 통해 메모리에 저장함이 바람직하다(S160). 또한, 커널 모드 가상 실행 모듈(100)이 제어 모듈(300)로부터 전달되는 객체 정보에 포함된 상기 임의의 커널 모드 드라이버의 구동에 따른 호출 대상 함수 목록(주소 정보 포함)을 토대로, 해당 함수의 상기 지원 대상 주소를 상기 메모리 상의 실제 함수 주소로 변경한다(S170). 아울러, 커널 모드 가상 실행 모듈(100)이 제어 모듈(300)로부터 전달되는 객체 정보에 포함된 인수 정보를 통해 메모리 상의 실제 함수 주소로 변환된 상기 해당 함수의 실행 명령을 실행한다(S180).
- <38> 다음으로, 임의의 커널 모드 드라이버의 가상 구동에 따라 산출되는 디스패처(Dispatcher) 함수의 상기 메모리 상의 주소 정보를 반환한다. 바람직하게는, 커널 모드 가상 실행 모듈(100)이 상기 임의의 커널 모드 드라이버의 가상 구동에 따라 산출되는 디스패처(Dispatcher) 함수의 상기 메모리 상의 주소 정보를 제어 모듈(300)로 반환한다(S190). 즉, 해당 함수의 실행이 종료되거나 또는 커널 모드 가상 실행 모듈(100)의 미구현 함수의 문제 등으로 인한 오류가 발생할 경우, 커널 모드 가상 실행 모듈(100)은 구동을 종료하고 해당 결과 값을 반환한다.
- <39> 그리고 나서, 상기 임의의 커널 모드 드라이버에 대한 객체 정보를 토대로 상기 임의의 커널 모드 드라이버의 실제 구동에 따라 산출되는 상기 디스패처 함수의 메모리 상의 실제 주소를 파악한다. 바람직하게는, 커널 모드 객체 제어 모듈(200)이 제어 모듈(300)로부터 전달되는 객체 정보에 포함된 임의의 커널 모드 드라이버에 대한 이름 정보를 토대로 상기 임의의 커널 모드 드라이버에 대한 실제 구동에 따른 메모리 상의 로딩 위치를 확인한다(S200). 이후, 커널 모드 객체 제어 모듈(200)은 상기 확인된 메모리 상의 로딩 위치를 토대로, 상기 임의의 커널 모드 드라이버의 실제 구동에 따라 산출되는 디스패처 함수의 메모리 상의 실제 주소를 파악한다(S210).
- <40> 그런 다음, 상기 파악된 상기 디스패처 함수의 실제 주소 정보와 상기 커널 모드 가상 실행 모듈로부터 반환되는 주소 정보를 비교한다. 바람직하게는, 커널 모드 객체 제어 모듈(200)이 상기 파악된 디스패처 함수의 실제 주소 정보와 커널 모드 가상 실행 모듈(100)로부터 반환되는 주소 정보를 비교한다(S220). 이때, 커널 모드 객체 제어 모듈(200)은 상기 디스패처 함수의 실제 주소 정보와 상기 커널 모드 가상 실행 모듈(100)로부터 반환되는 주소 정보를 동일 기준의 절대 주소로 변환하여 상호 비교한다.
- <41> 이후, 상기 단계 'S220'를 통한 비교 결과, 상이할 경우 상기 디스패처 함수의 주소를 상기 반환된 주소 정보로 변경한다. 바람직하게는, 커널 모드 객체 제어 모듈(200)이 상기 파악된 디스패처 함수의 실제 주소 정보와 커널 모드 가상 실행 모듈(100)로부터 반환되는 주소 정보를 비교하여 서로 상이할 경우, 상기 실제 구동에 따른

디스패처 함수의 주소를 커널 모드 가상 실행 모듈(100)로부터 반환된 주소 정보로 변경한다(S230).

<42> 지금까지 본 발명을 바람직한 실시예를 참조하여 상세히 설명하였지만, 본 발명이 상기한 실시예에 한정되는 것은 아니며, 이하의 특허청구범위에서 청구하는 본 발명의 요지를 벗어남이 없이 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자라면 누구든지 다양한 변형 또는 수정이 가능한 범위까지 본 발명의 기술적 사상이 미친다 할 것이다.

산업이용 가능성

<43> 본 발명에 따른 커널(Kernel) 모드의 악성 행위 검출 시스템 및 그 방법은 변경 전 디스패처 함수의 주소를 찾기 위해 가상 실행 환경을 적용함에 따라 실제 실행 중인 컴퓨터 환경에는 아무런 영향을 주지 않아 안정적인 동작 환경을 제공하며, 이를 토대로 커널 모드 객체내 함수 주소를 변경하는 파일, 네트워크, 레지스트리, 키보드, 게임 해킹 프로그램 등 다양한 악성 프로그램의 행위의 진단 및 차단에 효과적으로 적용할 수 있다는 점에서 기존의 기술의 한계를 뛰어 넘음에 따라 관련 기술에 대한 이용만이 아닌 적용되는 장치의 시판 또는 영업의 가능성이 충분할 뿐만 아니라 현실적으로 명백하게 실시할 수 있는 정도이므로 산업상 이용가능성이 있는 발명이다.

도면의 간단한 설명

<44> 본 명세서에서 첨부되는 다음의 도면들은 본 발명의 바람직한 실시예를 예시하는 것이며, 후술하는 발명의 상세한 설명과 함께 본 발명의 기술사상을 더욱 이해시키는 역할을 하는 것이므로, 본 발명은 그러한 도면에 기재된 사항에만 한정되어 해석되어서는 아니된다.

<45> 도 1은 본 발명의 실시예에 따른 커널 모드의 악성 행위 검출 시스템의 개략적인 구성도.

<46> 도 2는 본 발명의 실시예에 따른 커널 모드의 악성 행위 검출 방법을 설명하기 위한 개략적인 순서도.

<47> *도면의 주요 부분에 대한 부호의 설명*

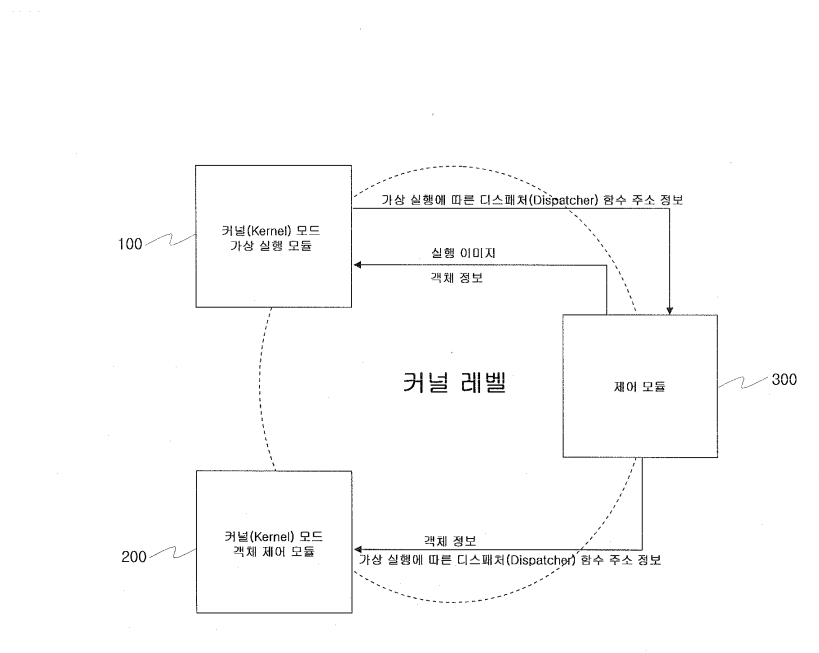
<48> 100: 커널 모드 가상 실행 모듈

<49> 200: 커널 모드 객체 제어 모듈

<50> 300: 제어 모듈

도면

도면1



도면2

