(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2012년03월09일
(11) 등록번호 10-1122650
(24) 등록일자 2012년02월24일

(51) 국제특허분류(Int. Cl.)
G06F 21/22 (2006.01)
(21) 출원번호 10-2010-0039335
(22) 출원일자 2010년04월28일
심사청구일자 2010년04월28일
(65) 공개번호 10-2011-0119918
(43) 공개일자 2011년11월03일
(56) 선행기술조사문헌
KR1020090130990 A*
US07234164 B2*
*는 심사관에 의하여 인용된 문헌
기술이전 희망 : **기술양도**, **실시권허여**, **기술지도**

(73) 특허권자
한국전자통신연구원
대전광역시 유성구 가정로 218 (가정동)
(72) 발명자
김요식
대전광역시 유성구 구즉로 25, 송강그린A 315동 103호 (송강동)
노상균
광주광역시 서구 죽봉대로38번길 23-6 (농성동)
(뒷면에 계속)
(74) 대리인
신영무

전체 청구항 수 : 총 13 항 심사관 : 엄인권

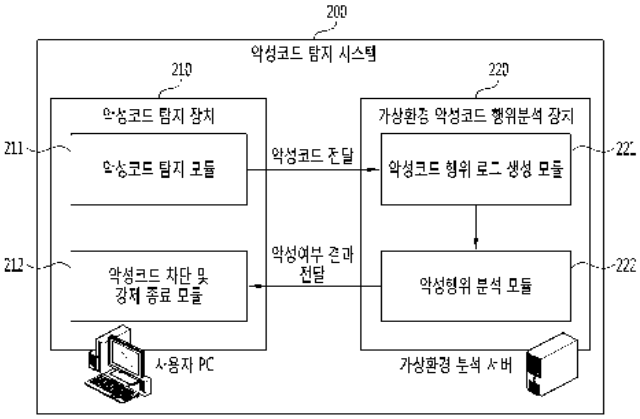
(54) 발명의 명칭 **정상 프로세스에 위장 삽입된 악성코드 탐지 장치, 시스템 및 방법**

(57) 요 약

본 발명은 정상 프로세스에 위장 삽입된 악성코드를 탐지하기 위한 장치, 시스템 및 방법에 관한 것이다.

본 발명에 따른 악성코드 탐지 장치는, 컴퓨터 시스템상에서 실행중인 프로세스로부터 생성된 쓰레드 정보를 추출하여 상기 쓰레드에 연관된 코드를 식별하고 상기 식별된 코드의 악성 여부를 추정하여 상기 악성으로 추정된 코드를 추출하는 악성코드 탐지모듈과, 상기 추출된 코드를 가상환경에서 실행하여 행위를 분석한 결과에 기반하여 상기 코드를 악성코드로 최종 판단하고 상기 코드의 실행을 강제 종료하는 악성코드 강제 종료 모듈을 포함한다.

대 표 도 - 도2



(72) 발명자

정윤정

경기도 성남시 중원구 은이로12번길 3-1 (은행동)

김동수

경상북도 포항시 남구 중앙로91번길 19-12 (대도동)

김원호

대전광역시 유성구 유성대로 1741, 111동 702호 (전민동, 세종아파트)

한유정

경기도 수원시 장안구 천천동 315-38 106호

윤영태

대전광역시 중구 태평로 35, 버드내A 211동 401호 (태평동)

손기욱

대전광역시 유성구 엑스포로 501, 청구나래A 109동 1506호 (전민동)

이철원

대전광역시 유성구 엑스포로 448, 207동 902호 (전민동, 엑스포아파트)

특허청구의 범위

청구항 1

컴퓨터 시스템상에서 실행중인 프로세스로부터 생성된 쓰레드 정보를 추출하여 상기 쓰레드에 연관된 코드 - 상기 쓰레드에 연관된 코드는 실행 파일이거나 DLL(Dynamic Link Library)임- 를 식별하고 상기 식별된 코드의 악성 여부를 추정하여 상기 악성으로 추정된 코드를 추출하는 악성코드 탐지모듈과,

상기 추출된 코드를 가상환경에서 실행하여 행위를 분석한 결과에 기반하여 상기 코드를 악성 코드로 최종 판단하고 상기 코드의 실행을 강제 종료하는 악성코드 강제 종료 모듈

을 포함하는 악성코드 탐지 장치.

청구항 2

삭제

청구항 3

제1항에 있어서, 상기 악성코드 탐지모듈은, 상기 프로세스의 가상 메모리, 상기 식별된 코드의 PE(Portable Executable) 속성, 상기 식별된 코드의 서비스 속성 및 쓰레드 스택중 적어도 하나를 검사함으로써 상기 식별된 코드의 악성 여부를 추정하는 악성코드 탐지 장치.

청구항 4

제1항에 있어서, 상기 악성코드 탐지모듈은 상기 쓰레드 정보를 추출하기 위해 상기 컴퓨터 시스템상에서 동작하는 프로세스 목록 및 각 프로세스에 의해 생성된 쓰레드 정보를 추출하는 악성코드 탐지 장치.

청구항 5

제1항에 있어서, 상기 악성코드 탐지모듈은 상기 쓰레드를 생성한 프로세스의 가상메모리에 상기 쓰레드에 연관된 상기 코드에 해당하는 파일이름의 문자열이 존재하는지 검사하여 해당 문자열이 존재한다면 상기 코드를 악성으로 추정하는 악성코드 탐지 장치.

청구항 6

제1항에 있어서, 상기 악성코드 탐지모듈은 상기 식별된 코드의 PE 속성을 검사하여 알려지지 않은 섹션이 존재하는 경우에 상기 코드를 악성으로 추정하는 악성코드 탐지 장치.

청구항 7

제1항에 있어서, 상기 악성코드 탐지모듈은 상기 식별된 코드의 PE 속성을 검사하여 체크섬이 올바르지 않거나, 상기 PE 속성내의 파일 크기와 탐색기에서 나온 파일 크기가 상이한 경우에 상기 코드를 악성으로 추정하는 악성코드 탐지 장치.

청구항 8

제1항에 있어서, 상기 악성코드 탐지모듈은 상기 식별된 코드에 의해 수행되는 서비스 속성을 검사하고, 상기 서비스가 다른 서비스와의 연관성 및 종속성이 없거나 자동 시작으로 설정되어 있는 경우에 상기 코드를 악성으로 추정하는 악성코드 탐지 장치.

청구항 9

제1항에 있어서, 상기 악성코드 탐지모듈은 상기 쓰레드에 연관된 코드가 식별되지 않을 경우에 쓰레드 스택을 추적하여 상기 쓰레드가 사용중인 DLL 목록을 획득하고 상기 획득된 DLL의 PE 속성을 검사함으로써 상기 DLL의 악성 여부를 추정하는 악성코드 탐지 장치.

청구항 10

제1항에 있어서, 상기 악성코드 강제 종료 모듈은 상기 코드의 행위 분석결과가 운영체제 방화벽 및 백신 무력화 행위, 가상환경 식별행위, 파일 및 레지스트리에 대한 생성/변경행위중 하나에 해당하는 경우 상기 코드를 악성코드로 최종 판단하는 악성코드 탐지 장치.

청구항 11

컴퓨터 시스템상에서 실행중인 프로세스로부터 생성된 쓰레드 정보를 추출하여 상기 쓰레드에 연관된 코드를 식별하고 상기 식별된 코드의 악성 여부를 추정하여 상기 악성으로 추정된 코드를 추출하는 악성코드 탐지모듈과, 상기 추출된 코드의 가상환경 행위 분석 결과에 기반하여 상기 코드를 악성코드로 최종 판단하고 상기 코드의 실행을 강제 종료하는 악성코드 강제 종료 모듈을 구비하는 악성코드 탐지 장치와,

상기 악성코드 탐지모듈에 의해 추출된 코드를 가상환경에서 실행하여 상기 코드의 행위에 대한 로그를 생성하는 로그생성모듈과, 상기 로그를 이용하여 상기 코드의 행위가 운영체제 방화벽 및 백신 무력화 행위, 가상환경 식별행위, 파일 및 레지스트리에 대한 생성 또는 변경행위중 하나에 해당하는지 분석하고 상기 분석 결과를 상기 악성코드 강제 종료 모듈에 전달하는 악성행위 식별모듈을 구비하는 가상환경 악성코드 행위분석 장치를 포함하고,

상기 악성코드 탐지 장치는 클라이언트에서 동작하고 상기 가상환경 악성코드 행위분석 장치는 서버에서 동작하는 악성코드 탐지 시스템.

청구항 12

삭제

청구항 13

제11항에 있어서, 상기 악성코드 탐지 모듈은 상기 가상환경 악성코드 행위분석장치에 상기 추출된 코드의 가상환경 행위 분석을 요청하는 악성코드 탐지 시스템.

청구항 14

컴퓨터 시스템상에서 실행중인 프로세스 목록 및 각 프로세스에 종속된 쓰레드 정보를 추출하는 단계;

상기 쓰레드에 연관된 코드를 식별하고, 상기 프로세스의 가상 메모리, 상기 코드의 PE 속성, 상기 코드와 서비스 프로세스와의 연관성 및 쓰레드 스택중 적어도 하나를 검사함으로써 상기 식별된 코드의 악성 여부를 추정하는 단계;

상기 악성으로 추정된 코드의 악성 위협도를 산출하는 단계;

상기 산출된 악성 위협도가 임계값 이상인 코드를 추출하여 가상환경 악성코드 행위 분석 장치에 분석 요청하는 단계;

상기 가상환경 악성코드 행위 분석 장치로부터 수신된 분석 결과에 기반하여 상기 코드를 악성코드로 최종 판단

하는 단계; 및

상기 악성 코드로 최종 판단된 코드의 실행을 강제 종료하는 단계

를 포함하는 악성코드 탐지 방법.

청구항 15

제14항에 있어서, 상기 코드를 악성코드로 최종 판단하는 단계는, 상기 가상환경 악성코드 행위 분석 장치의 분석 결과가 운영체제 방화벽 및 백신 무력화 행위, 가상환경 식별행위, 파일 및 레지스트리에 대한 생성/변경행위중 하나에 해당하는 경우에 상기 코드를 악성코드로 최종 판단하는 악성코드 탐지 방법.

명 세 서

기 술 분 야

[0001] 본 발명은 정상 프로세스에 위장 삽입된 악성코드를 탐지하기 위한 장치, 시스템 및 방법에 관한 것으로, 더욱 상세하게는 컴퓨터 시스템상에서 실행중인 프로세스들의 쓰레드 정보를 추출하여 악성코드에 의해 생성된 쓰레드인지를 식별하고 가상환경에서의 악성코드 행위를 분석하여 정상 프로세스에 위장 삽입된 악성코드를 탐지하는 시스템 및 방법에 관한 것이다.

배 경 기 술

[0002] 최근 인터넷 서비스가 다양화됨에 따라 인터넷 사용률이 증가하고 있으며, 이에 따라 컴퓨터 바이러스나 인터넷 웜 등과 같은 악성코드들이 인터넷을 통해 널리 확산되어 사용자들에게 많은 피해를 야기시키고 있다. 특히, 2009년 77대란을 유발한 봇(bot)과 같은 악성코드에 의한 피해가 속출하고 있다. 이런 악성코드는 자신이 서버(server) 역할을 하기 위해 정상 프로세스에 쓰레드를 삽입하여 C&C(Command and Control)에 의해 통제를 받으며 사용자 PC에서 악성 행위를 수행한다. 이런 악성코드는 자신의 존재를 숨기기 위해 DLL 인젝션 또는 코드 인젝션 기법을 통해 정상 프로세스로 가장하여 자신을 은닉한다.

[0003] 종래의 악성코드 탐지 방법은 바이너리 해쉬값 또는 특정 영역의 연속된 바이트 시퀀스(byte sequence)를 시그니처로 생성비교하여 악성여부를 판단하여 해당 프로세스를 강제 종료시키고 파일을 삭제한다. 그러나, 바이너리 패턴 비교 방식에 의존하므로 이미 알려져서 악성코드의 바이너리 패턴 데이터베이스에 등록되어 있는 악성코드에 대해서는 확실한 진단율을 기대할 수 있지만, 아직 알려지지 않은 악성코드에 대해서는 진단 자체가 불가능하다는 단점이 있다.

[0004] 또한, 악성코드의 탐지 및 처리를 위해 특정 API를 후킹(hooking)하거나 커널 계층에서의 후킹을 이용하는 방법이 있으나, 전자의 경우 특정 API만을 대상으로 후킹하여 악성코드의 행위를 중간에서 모니터링하고 사용자의 판단에 의해 악성여부를 판단하고 차단여부를 결정하여야 하고, 후자의 경우에는 시스템 오동작에 따른 심각한 장애를 유발할 수도 있다는 문제점이 있다.

[0005]

발명의 내용

해결하려는 과제

[0006] 본 발명은 전술한 문제점을 해결하기 위한 것으로, 컴퓨터 시스템상에서 실행중인 프로세스로부터 생성된 쓰레드들이 악성코드에 의해 생성된 쓰레드인지를 1차적으로 판단하고 악성으로 의심되면 가상환경에서의 악성코드 행위를 추가적으로 분석함으로써 정상 프로세스로 가장된 악성코드를 탐지하는 시스템 및 방법에 관한 것이다.

과제의 해결 수단

[0007] 본 발명의 일 실시예에 따른 악성코드 탐지 장치는, 컴퓨터 시스템상에서 실행중인 프로세스로부터 생

성된 쓰레드 정보를 추출하여 상기 쓰레드에 연관된 코드를 식별하고 상기 식별된 코드의 악성 여부를 추정하여 상기 악성으로 추정된 코드를 추출하는 악성코드 탐지모듈과, 상기 추출된 코드를 가상환경에서 실행하여 행위를 분석한 결과에 기반하여 상기 코드를 악성코드로 최종 판단하고 상기 코드의 실행을 강제 종료하는 악성코드 강제 종료 모듈을 포함한다.

[0008] 본 발명의 다른 실시예에 따른 악성코드 탐지 시스템은, 컴퓨터 시스템상에서 실행중인 프로세스로부터 생성된 쓰레드 정보를 추출하여 상기 쓰레드에 연관된 코드를 식별하고 상기 식별된 코드의 악성 여부를 추정하여 상기 악성으로 추정된 코드를 추출하는 악성코드 탐지모듈과, 상기 추출된 코드의 가상환경 행위 분석결과에 기반하여 상기 코드를 악성코드로 최종 판단하고 상기 코드의 실행을 강제 종료하는 악성코드 강제 종료 모듈을 구비하는 악성코드 탐지 장치와, 상기 악성코드 탐지모듈에 의해 추출된 코드를 가상환경에서 실행하여 상기 코드의 행위에 대한 로그를 생성하는 로그생성모듈과, 상기 로그를 이용하여 상기 코드의 행위가 운영체제 방화벽 및 백신 무력화 행위, 가상환경 식별행위, 파일 및 레지스트리에 대한 생성 또는 변경행위중 하나에 해당하는지 분석하고 상기 분석 결과를 상기 악성코드 강제 종료 모듈에 전달하는 악성행위 식별모듈을 구비하는 가상환경 악성코드 행위분석 장치를 포함한다.

[0009] 본 발명의 또다른 실시예에 따른 악성코드 탐지 방법은, 컴퓨터 시스템상에서 실행중인 프로세스 목록 및 각 프로세스에 종속된 쓰레드 정보를 추출하는 단계; 상기 쓰레드에 연관된 코드를 식별하고, 상기 프로세스의 가상메모리, 상기 코드의 PE 속성, 상기 코드와 서비스 프로세스와의 연관성 및 쓰레드 스택중 적어도 하나를 검사함으로써 상기 식별된 코드의 악성 여부를 추정하는 단계; 상기 악성으로 추정된 코드의 악성 위협도를 산출하는 단계; 상기 산출된 악성 위협도가 임계값 이상인 코드를 추출하여 가상환경 악성코드 행위 분석 장치에 분석 요청하는 단계; 상기 가상환경 악성코드 행위 분석 장치로부터 수신된 분석 결과에 기반하여 상기 코드를 악성코드로 최종 판단하는 단계; 및 상기 악성 코드로 최종 판단된 코드의 실행을 강제 종료하는 단계를 포함한다.

발명의 효과

[0010] 본 발명에 의한 악성코드 탐지 시스템 및 방법을 이용하면, 이미 발견된 악성코드뿐만 아니라 아직까지 발견되지 않은 악성코드나 기 발견된 악성코드의 변형된 코드도 탐지할 수 있게 되어, 악의적 행위의 가능성이 있는 알려지지 않은 악성코드에도 효과적으로 대응할 수 있으며, 사고조사용으로 활용할 수 있다.

[0011] 또한, 컴퓨터 시스템상에서 실행중인 프로세스로부터 생성된 쓰레드를 추출하여 악성코드에 의해 생성된 쓰레드인지를 1차적으로 판단하고 악성으로 의심되면 가상환경에서의 악성코드 행위를 추가적으로 분석함으로써 악성코드의 오탐율을 줄일 수 있다.

도면의 간단한 설명

[0012] 도 1은 본 발명에 따른 악성코드 탐지 시스템을 이용하여 정상프로세스에 위장 삽입된 악성코드를 탐지하는 개념을 설명한 도면이다.

도 2는 본 발명의 일실시예에 따른 악성코드 탐지 시스템의 구성을 도시한 블록도이다.

도 3는 본 발명의 일실시예에 따라 정상프로세스에 위장 삽입된 악성코드를 탐지하는 방법을 도시한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0013] 아래에서는 첨부한 도면을 참고로 하여 본 발명의 실시예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명하겠다. 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.

[0014] 명세서 전체에서, 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. 또한, 명세서에 기재된 "…부", "모듈" 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨

어나 소프트웨어 또는 하드웨어 및 소프트웨어의 조합으로 구현될 수 있음을 의미한다.

[0015] 도 1은 본 발명에 따른 악성코드 탐지 장치를 이용하여 정상프로세스에 위장 삽입된 악성코드를 탐지하는 개념을 설명한 도면이다. 도시된 바와 같이, 일반 프로세스(1,3)는 일반 쓰레드를 생성한다. 한편, 악성 프로세스(2)는 자신의 프로세스를 은닉하기 위해 다른 정상 프로세스(1,3)에 악성행위를 하는 악성코드를 DLL 인젝션 또는 코드 인젝션 기법을 이용하여 삽입한다. 삽입된 악성코드는 정상 프로세스의 일부분과 같이 동작하게 되어 식별이 어려우며, 삽입된 악성코드에 의해 악성행위를 담당하는 악성 쓰레드(20,30) 가 생성된다.

[0016] 본 발명에 따른 악성코드 탐지 시스템(100)은 이러한 정상 프로세스에 삽입된 악성 쓰레드(20, 30)을 탐지하기 위한 것이다.

[0017]

[0018] 도 2는 본 발명의 일실시예에 따른 악성코드 탐지 시스템의 구성을 도시한 블록도이다.

[0019] 악성코드 탐지 시스템(200)은, 컴퓨터 시스템상에서 실행중인 프로세스로부터 생성된 쓰레드 정보를 추출하여 상기 쓰레드에 연관된 코드를 식별하고 상기 식별된 코드의 악성 여부를 검사하여 악성으로 의심되는 코드를 추출하는 악성코드 탐지 장치(210)와, 악성코드 탐지 장치(210)에 의해 추출된 코드를 가상환경에서 실행하여 악성행위를 분석하는 가상환경 악성코드 행위분석 장치(220)를 포함한다. 구체적으로, 악성코드 탐지 장치(210)는 악성코드 탐지모듈(211)과 악성코드 강제 종료 모듈(212)을 포함한다. 일실시예에서, 악성코드 탐지 장치(210)는 사용자 PC에서 실행되는 것으로 기재되어 있으나, 이외에도 랩탑, 휴대용 컴퓨터 또는 타블렛 등 네트워크 기능을 구비한 다양한 유형의 기기중 하나에서 수행될 수 있으며 이에 한정되지 않는다.

[0020] 악성코드 탐지모듈(2110)은 컴퓨터 시스템상에서 실행중인 프로세스로부터 생성된 쓰레드 정보를 추출하여 쓰레드에 연관된 코드를 식별하고 상기 식별된 코드의 악성 여부를 추정하여 상기 악성으로 추정되는 코드를 추출하여 악성코드 행위분석 장치(220)로 전달한다. 상기 쓰레드에 연관된 코드는 컴퓨터상에서 실행중인 실행파일이거나 프로세스에 동적으로 링크된 DLL(Dynamic Link Library)이다. 악성코드 탐지모듈(210)은, 상기 프로세스의 가상 메모리, 상기 식별된 코드의 PE(Portable Executable) 속성, 상기 식별된 코드의 서비스 프로세스와의 연관성 및 상기 쓰레드에 연관된 쓰레드 스택중 적어도 하나를 검사함으로써 상기 코드의 악성 여부를 추정한다. 본 발명에 따른 악성 여부 추정 과정은 이하 도 3을 참조하여 좀더 상세히 설명될 것이다.

[0021] 악성코드 강제 종료 모듈(212)은 악성코드 행위분석 장치(220)의 분석결과에 기반하여 상기 코드를 악성코드로 최종 판단하고 상기 코드의 실행을 강제 종료한다. 또한, 상기 악성 코드를 클라이언트의 메모리로부터 삭제할 수 있다.

[0022] 가상환경 악성코드 행위분석 장치(220)는 악성코드 탐지 장치(210)로부터 전달된 코드를 가상 환경에서 실행시켜 코드의 행위를 분석하고 분석결과를 악성코드 탐지 장치(210)에 제공하는 역할을 한다. 도면상에서 가상환경 악성코드 행위분석 장치(220)는 악성코드 탐지 장치(210)가 실행되는 사용자 PC와 물리적으로 구별되는 서버상에서 실행되는 것으로 기재되어 있으며, 이러한 실시예에 국한되는 것은 아니며, 구현에 따라서는 악성코드 탐지 장치(210)와 동일한 시스템 상에 구현가능하다.

[0023] 구체적으로, 가상환경 악성코드 행위분석 장치(220)는 악성코드 행위 로그 생성 모듈(221)과 악성행위 식별모듈(222)을 포함한다.

[0024] 악성코드 행위 로그 생성 모듈(221)은 악성코드 탐지 장치(210)로부터 전달된 코드를 가상환경에서 실행하여 코드의 행위에 대한 로그를 생성한다. 악성코드 행위 분석 모듈(222)은 로그를 분석하여 상기 코드의 행위가 운영체제 방화벽 및 백신 무력화 행위, 가상환경 식별행위, 파일 및 레지스트리에 대한 생성 또는 변경 행위인지 분석하고 상기 분석 결과를 악성코드 탐지 장치(210)에 악성코드 차단 및 강제 종료 모듈(112)로 전송한다.

[0025] 가상환경을 에뮬레이션하여 코드의 행위를 분석하는 과정은 샌드박스(Sandbox) 등 본 기술분야에 공지된 도구를 이용하여 구현될 수 있으므로 이에 대한 자세한 설명은 본 명세서에서 생략하겠다.

[0026]

[0027] 도 3은 본 발명의 일실시예에 따라 정상프로세스에 위장 삽입된 악성코드를 탐지하는 방법을 도시한 흐름도이다. 도 3에는 편의상 단계(S311) 내지 단계(S319)는 악성코드 탐지 장치(210)에서 수행되고 단계(S321)

내지 단계(S323)는 가상환경 악성코드 행위분석 장치(220)에서 수행되는 것으로 도시되어 있으나, 이는 일 예에 불과하며, 본 발명의 단계(S311 내지 S319)와 단계(S321 내지 S323)가 반드시 물리적으로 분리된 장치상에서 구현되는 것에 한정되는 것은 아니다.

[0028] 단계(S311)에서, 시스템상에서 동작하는 프로세스 목록을 추출하고, 각 프로세스에 종속된 쓰레드 정보, 예를 들면, 쓰레드 개수, 각 쓰레드의 시작주소 및 베이스 주소를 추출한다.

[0029] 단계(S312)에서 쓰레드에 대한 악성 여부를 검사한다. 세부적으로, 악성 여부는 쓰레드를 생성한 주체 식별(S3121), 가상 메모리 검사(S3122), PE(Portable Executable) 분석(S3123), 서비스 프로세스 검사(S3124) 및 쓰레드 스택 검사(S3125) 단계들을 포함한다.

[0030] 우선, 단계(S3121)에서 쓰레드를 생성한 코드, 즉, 실행파일 또는 DLL을 식별한다. DLL을 식별하기 위해서는, 쓰레드를 생성한 프로세스에 링크된 DLL 중 동적 링크된 DLL을 추출하고, DLL의 베이스 주소와 메모리에 맵(mapped)된 크기를 구한다. 실행 파일 또는 동적 링크된 DLL중 베이스 주소와 메모리에 맵된 범위가 해당 쓰레드의 시작주소를 포함하고 있는 실행 파일 또는 DLL을 검색하여 해당 쓰레드를 생성한 실행파일 또는 DLL을 식별한다.

[0031] 가상 메모리 검사(S3122)에서, 쓰레드를 생성한 프로세스의 가상메모리에 단계(S3122)에서 식별된 DLL 파일이름의 문자열이 있는지 검사하고, DLL 파일이름의 문자열이 존재할 경우 해당 DLL이 DLL 인젝션 기술을 이용하여 정상 프로세스에 위장 삽입된 악성 코드일 가능성이 있다고 판단한다.

[0032] PE 분석 단계(S3123)에서, 상기 식별된 DLL의 PE 포맷을 검사하여 비정상적인 요소가 있는지 판단한다. 일예에서, PE 포맷에 많이 사용되는 비주얼 스튜디오, C++ 빌더, 델파이, 비쥬얼 베이직 등의 범용 컴파일러에 의해 생성된 데이터 외의 알려지지 않은(unknown) 섹션이 포함되어 있다면 해당 DLL이 정상 프로세스에 위장 삽입된 악성 코드일 가능성이 있다고 판단한다. 또한, 체크섬이 올바르지 않거나, PE 속성내의 파일 크기와 탐색기에서 나온 파일 크기가 상이한 경우에도 해당 DLL이 악성일 가능성이 있다고 판단한다.

[0033] 서비스 프로세스 검사(S3124)에서, 상기 식별된 DLL이 윈도우 운영체제에서 실행 중인 서비스 프로세스에 동적 링크되어 있는지와 서비스 정보가 포함되어 있는 레지스트리에 해당 DLL을 포함하는 서비스가 있는지 검사한다. DLL을 포함하고 있는 서비스가 있을 경우, 해당 서비스의 속성, 예를 들면 서비스 타입, 시작유형, 종속성, 속한 그룹 정보 등을 검사한다. 검사 결과, DLL을 포함하고 있는 서비스가 다른 서비스와의 연관성 및 종속성이 없거나 자동 시작이 설정되어 있는 경우에 악성 DLL에 의해 생성된 서비스일 가능성이 있다고 판단한다.

[0034] 쓰레드 스택 검사 단계(S3125)에서 단계(S3121)에서 해당 쓰레드를 생성한 DLL이 발견되지 않을 경우, 쓰레드 스택을 추적하여 쓰레드가 사용 중인 DLL 목록을 순차적으로 획득한 후 DLL의 PE 속성을 검사하여 알려지지 않은 섹션이 있는지 검사한다. DLL의 PE 검사는 전술한 단계(S3123)과 동일하다. 검사결과, 알려지지 않은 섹션이 있는 DLL을 정상 프로세스에 위장 삽입된 악성 코드일 가능성이 있다고 판단한다(S3125).

[0035] 단계(S3123)에서 악성 코드에 의해 생성된 것으로 추정되는 DLL의 악성 위협도를 산출한다. 일 예에서, 전술한 단계(S3121 내지 S3125)의 검사과정에서는 해당 DLL이 악성일 가능성이 있을 경우 판단된 경우에 이에 대응하는 플래그를 설정한다. 예를 들어, 가상메모리 검사 단계(S3122)에서 해당 DLL 파일이름의 문자열이 존재하면 DLL 인젝션 플래그를 설정한다. PE 분석 단계(S3123)에서는, PE 포맷내에 알려지지 않은(Unknown) 섹션이 있으면 Unknown섹션 플래그를 설정하고, 체크섬이 올바르지 않을 경우 체크섬 플래그를 설정하고, PE 속성내의 파일 크기와 탐색기에서 나온 파일 크기가 다르면 파일크기 플래그를 설정한다. 서비스 프로세스 검사 단계(S3124)에서는 서비스 플래그를, 쓰레드 스택 검사 단계(S3125)는 쓰레드 스택 플래그를 설정한다.

[0036] 악성여부에 따른 위협도 산출 단계(S313)에서는 전술한 검사 단계들에서 설정된 플래그에 따라 점수를 높음, 중간, 낮음의 3단계로 위협 점수를 계산한다. 예를 들어, 인젝션된 DLL인 경우 높음(10점), Unknown 섹션의 경우 낮음(1점), 서비스로 동작하는 DLL의 경우 중간(5점) 등과 같은 방식으로 위협도를 산출한다.

[0037] 단계(S314)에서, 단계(S3123)에서 구해진 악성 위협도가 임계값 이상인 경우 상기 쓰레드를 악성 쓰레드로 판단하며, 그렇지 않은 경우에는 다음 쓰레드에 대하여 악성여부를 검사하기 위해 단계(S312)로 돌아간다.

[0038] 단계(S315)에서, 악성 쓰레드로 판단된 쓰레드에 연관된 실행파일 또는 DLL 파일을 추출한다.

[0039] 단계(S316)에서, 추출된 실행파일 또는 DLL(이하, “코드”라 함)을 가상환경 악성코드 행위분석 장치

(220)로 전송하여 분석을 요청한다.

[0040] 단계(S321)에서, 가상환경 악성코드 행위분석 장치(220)는 악성코드 탐지 장치(210)에 의해 악성 위협도가 높다고 판단된 코드를 수신한다.

[0041] 단계(S322)에서, 가상환경에서 해당 코드를 실행하여 파일 및 레지스트리 접근, 네트워크 송수신 행위에 대한 로그를 생성하고, 로그 분석을 통해 상기 코드의 행위가 운영체제 방화벽 및 백신 무력화하는 행위인지, 자신이 실행되는 환경인지 가상환경인지 확인하는 행위, 파일 및 레지스트리를 생성하거나 변경하는 행위를 포함하는 악성행위중 하나에 해당하는지 판단한다.

[0042] 단계(S323)에서 상기 분석 결과를 악성코드 탐지 장치(210)에 전송한다.

[0043] 단계(S317)에서 분석 결과를 수신하고, 단계(S318)에서 분석 결과가 악성행위에 해당하는 경우 상기 실행 코드를 악성코드로 최종 판단한다.

[0044] 단계(S319)에서 상기 악성 코드의 실행을 강제종료하고, 해당 코드를 삭제한다.

[0045]

[0046] 이제까지 본 발명에 대하여 그 바람직한 실시예들을 중심으로 살펴보았다. 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로 개시된 실시예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 동등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

부호의 설명

[0047] 1,3: 일반 프로세스

2: 악성 프로세스

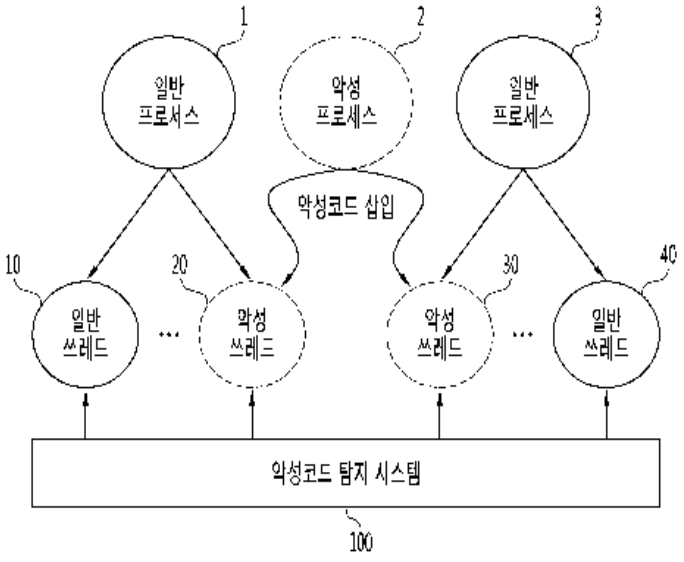
10,40: 일반 쓰레드

20,30: 악성 쓰레드

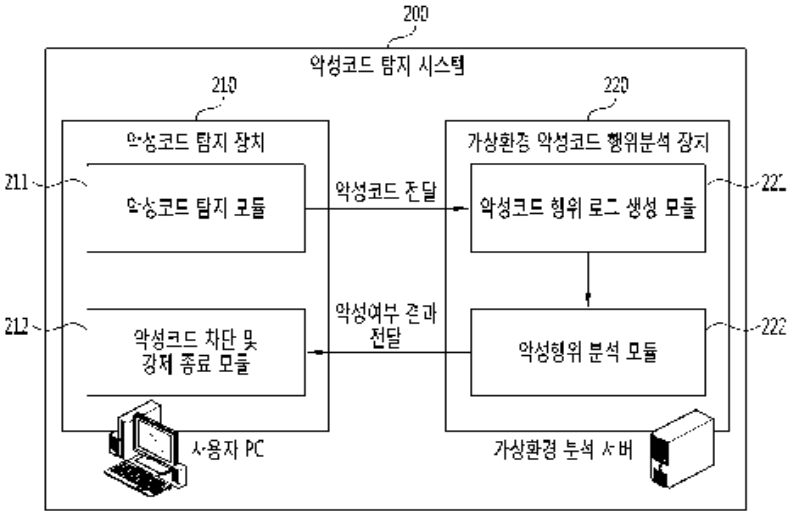
100: 악성코드 탐지 시스템

도면

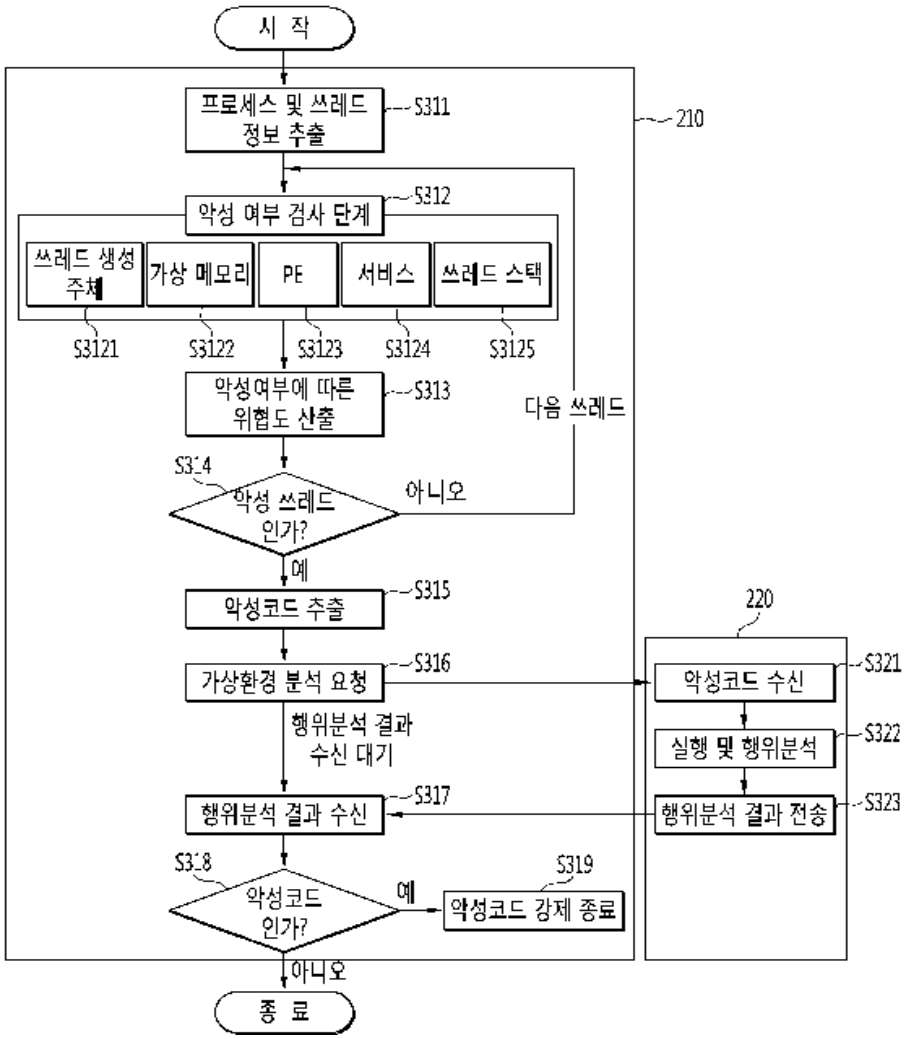
도면1



도면2


200
악성코드 탐지 시스템
210
악성코드 탐지 장치
211
악성코드 탐지 모듈
212
악성코드 차단 및 강제 종료 모듈
사용자 PC
악성코드 전달
악성여부 결과 전달
220
가상환경 악성코드 행위분석 장치
221
악성코드 행위 로그 생성 모듈
222
악성행위 분석 모듈
가상환경 분석 서버

도면3


시 작
프로세스 및 쓰레드 정보 추출
S311
210
악성 여부 검사 단계
S312
쓰레드 생성 주체
가상 메모리
PE
서비스
쓰레드 스택
S3121
S3122
S3123
S3124
S3125
악성여부에 따른 위협도 산출
S313
다음 쓰레드
S314
악성 쓰레드 인가?
아니오
예
악성코드 추출
S315
220
가상환경 분석 요청
S316
악성코드 수신
S321
행위분석 결과 수신 대기
실행 및 행위분석
S322
행위분석 결과 수신
S317
행위분석 결과 전송
S323
S318
악성코드 인가?
예
S319
악성코드 강제 종료
아니오
종 료