(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2022-0080347
(43) 공개일자 2022년06월14일

(51) 국제특허분류(Int. Cl.)
G06F 21/56 (2013.01) *G06F 21/31* (2013.01)
G06F 21/55 (2013.01)
(52) CPC특허분류
G06F 21/56 (2013.01)
G06F 21/31 (2013.01)
(21) 출원번호 10-2020-0169362
(22) 출원일자 2020년12월07일
심사청구일자 2020년12월07일

(71) 출원인
주식회사 엔씨소프트
서울특별시 강남구 테헤란로 509 (삼성동)
(72) 발명자
김종수
경기도 성남시 분당구 대왕판교로 644번길 12
반규태
경기도 성남시 분당구 대왕판교로 644번길 12
(뒷면에 계속)
(74) 대리인
장영태

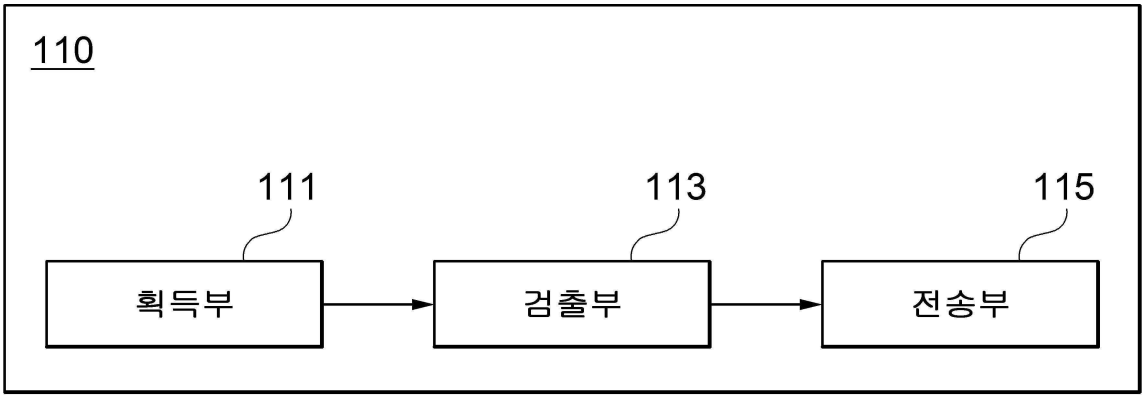
전체 청구항 수 : 총 12 항

(54) 발명의 명칭 **서버 모니터링 방법 및 장치**

(57) 요 약

서버 모니터링 방법 및 장치가 개시된다. 일 실시예에 따른 서버 모니터링 방법은 서버로부터 서버에서 실행 중인 하나 이상의 프로세스에 대한 리스트를 획득하는 동작, 서버로부터 하나 이상의 프로세스 중 기 정의된 화이트리스트에 속하지 않는 프로세스 각각에 대응되는 프로그램 정보를 획득하는 동작, 프로그램 정보에 기초하여, 화이트리스트에 속하지 않는 프로세스 중 서버에 대한 시스템 권한 및 다른 프로세스와 통신이 가능한 네트워크 통신 권한을 보유한 프로세스를 코드 인젝션(Code Injection)이 이루어진 타겟 프로세스로 검출하는 동작 및 타겟 프로세스의 코드 정보 중 적어도 일부를 포함하는 검출 결과를 서버로 전송하는 동작을 포함한다.

대 표 도 - 도2



(52) CPC특허분류
G06F 21/552 (2013.01)
G06F 21/554 (2013.01)
(72) 발명자
이충수
경기도 성남시 분당구 대왕판교로 644번길 12
조재익
경기도 성남시 분당구 대왕판교로 644번길 12

명 세 서

청구범위

청구항 1

서버로부터 상기 서버에서 실행 중인 하나 이상의 프로세스에 대한 리스트를 획득하는 동작;

상기 서버로부터 상기 하나 이상의 프로세스 중 기 정의된 화이트리스트에 속하지 않는 프로세스 각각에 대응되는 프로그램 정보를 획득하는 동작;

상기 프로그램 정보에 기초하여, 상기 화이트리스트에 속하지 않는 프로세스 중 상기 서버에 대한 시스템 권한 및 다른 프로세스와 통신이 가능한 네트워크 통신 권한을 보유한 프로세스를 코드 인젝션(Code Injection)이 이루어진 타겟 프로세스로 검출하는 동작; 및

상기 타겟 프로세스의 코드 정보 중 적어도 일부를 포함하는 검출 결과를 상기 서버로 전송하는 동작을 포함하는, 서버 모니터링 방법.

청구항 2

청구항 1항에 있어서,

상기 검출하는 동작은,

상기 화이트리스트에 속하지 않는 프로세스 중 읽기, 쓰기 및 실행 권한을 보유하고, 기 설정된 크기 이상의 메모리가 할당된 포괄적 호스트 프로세스(Generic Host Process)를 상기 시스템 권한 및 상기 네트워크 통신 권한을 받은 상기 타겟 프로세스로 검출하는, 서버 모니터링 방법.

청구항 3

청구항 1항에 있어서,

상기 검출 결과는,

상기 검출된 타겟 프로세스에 할당된 메모리 상의 코드 영역에서의 덤프 파일(Dump File)을 포함하는, 서버 모니터링 방법.

청구항 4

서버로부터 상기 서버에서 실행 중인 하나 이상의 프로세스에 대한 리스트를 획득하는 동작;

상기 서버로부터 상기 하나 이상의 프로세스 중 기 정의된 화이트리스트에 속하지 않는 프로세스 각각에 대응되는 프로그램 정보를 획득하는 동작;

상기 프로그램 정보에 기초하여, 상기 화이트리스트에 속하지 않는 프로세스에 속하는 복수의 스레드(Thread) 각각이 실행되는 영역 및 상기 복수의 스레드 각각이 보유한 권한을 기준으로 상기 복수의 스레드 중 코드 인젝션(Code Injection)이 이루어진 타겟 스레드를 검출하는 동작; 및

상기 타겟 스레드의 코드 정보 중 적어도 일부를 포함하는 검출 결과를 상기 서버로 전송하는 동작을 포함하는, 서버 모니터링 방법.

청구항 5

청구항 4항에 있어서,

상기 검출하는 동작은,

상기 복수의 스레드 중 읽기, 쓰기 및 실행 권한을 보유하고, 각 스레드가 속한 프로세스와 대응되는 프로그램 파일의 코드 영역 외의 영역 상에서 실행되는 스레드를 상기 타겟 스레드로 검출하는, 서버 모니터링 방법.

청구항 6

청구항 4항에 있어서,

상기 검출 결과는,

상기 검출된 타겟 스레드에 할당된 메모리 상의 영역에서의 덤프 파일(Dump File)을 포함하는, 서버 모니터링 방법.

청구항 7

서버로부터 상기 서버에서 실행 중인 하나 이상의 프로세스에 대한 리스트를 획득하고, 상기 서버로부터 상기 하나 이상의 프로세스 중 기 정의된 화이트리스트에 속하지 않는 프로세스 각각에 대응되는 프로그램 정보를 획득하는 획득부;

상기 프로그램 정보에 기초하여, 상기 화이트리스트에 속하지 않는 프로세스 중 상기 서버에 대한 시스템 권한 및 다른 프로세스와 통신이 가능한 네트워크 통신 권한을 보유한 프로세스를 코드 인젝션(Code Injection)이 이루어진 타겟 프로세스로 검출하는 검출부; 및

상기 타겟 프로세스의 코드 정보 중 적어도 일부를 포함하는 검출 결과를 상기 서버로 전송하는 전송부를 포함하는, 서버 모니터링 장치.

청구항 8

청구항 7항에 있어서,

상기 검출부는,

상기 화이트리스트에 속하지 않는 프로세스 중 읽기, 쓰기 및 실행 권한을 보유하고, 기 설정된 크기 이상의 메모리가 할당된 포괄적 호스트 프로세스(Generic Host Process)를 상기 시스템 권한 및 상기 네트워크 통신 권한을 받은 상기 타겟 프로세스로 검출하는, 서버 모니터링 장치.

청구항 9

청구항 7항에 있어서,

상기 검출 결과는,

상기 검출된 타겟 프로세스에 할당된 메모리 상의 코드 영역에서의 덤프 파일(Dump File)을 포함하는, 서버 모니터링 장치.

청구항 10

서버로부터 상기 서버에서 실행 중인 하나 이상의 프로세스에 대한 리스트를 획득하고, 상기 서버로부터 상기 하나 이상의 프로세스 중 기 정의된 화이트리스트에 속하지 않는 프로세스 각각에 대응되는 프로그램 정보를 획득하는 획득부;

상기 프로그램 정보에 기초하여, 상기 화이트리스트에 속하지 않는 프로세스에 속하는 복수의 스레드(Thread) 각각이 실행되는 영역 및 상기 복수의 스레드 각각이 보유한 권한을 기준으로 상기 복수의 스레드 중 코드 인젝션(Code Injection)이 이루어진 타겟 스레드를 검출하는 검출부; 및

상기 타겟 스레드의 코드 정보 중 적어도 일부를 포함하는 검출 결과를 상기 서버로 전송하는 전송부를 포함하는, 서버 모니터링 장치.

청구항 11

청구항 10항에 있어서,

상기 검출부는,

상기 복수의 스레드 중 읽기, 쓰기 및 실행 권한을 보유하고, 각 스레드가 속한 프로세스와 대응되는 프로그램 파일의 코드 영역 외의 영역 상에서 실행되는 스레드를 상기 타겟 스레드로 검출하는, 서버 모니터링 장치.

청구항 12

청구항 10항에 있어서,

상기 검출 결과는,

상기 검출된 타겟 스레드에 할당된 메모리 상의 영역에서의 덤프 파일(Dump File)을 포함하는, 서버 모니터링 장치.

발명의 설명

기 술 분 야

[0001] 개시되는 실시예들은 악성 코드를 검출하기 위해 서버를 모니터링하는 기술에 관한 것이다.

배 경 기 술

[0002] 최근 서버의 보안 시스템을 피해 서버 내에 악성 코드를 유포함으로써 서버의 정상적인 운영을 방해하거나, 서버에 의해 관리되는 정보를 유출하려는 시도가 점차 증가하고 있다.

[0003] 서버의 보안이 까다로워질수록, 악성 코드 유포자들은 서버의 보안 시스템을 회피할 수 있는 다양한 수단을 강구해왔으며, 그 결과 블랙리스트만을 탐지하는 현재의 안티 바이러스(Anti-Virus) 제품을 통해서는 서버 내 유포된 악성 코드를 검출하지 못하는 문제가 발생했다.

선행기술문헌

특허문헌

[0004] (특허문헌 0001) 대한민국 공개특허공보 제10-2014-0035202호(2014.03.21. 공개)

발명의 내용

해결하려는 과제

[0005] 개시되는 실시예들은 예측 불가능한 악성 코드를 검출하고자 서버를 모니터링하는 수단을 제공하기 위한 것이다.

과제의 해결 수단

[0006] 개시되는 일 실시예에 따른 서버 모니터링 방법은, 서버로부터 서버에서 실행 중인 하나 이상의 프로세스에 대한 리스트를 획득하는 동작, 서버로부터 하나 이상의 프로세스 중 기 정의된 화이트리스트에 속하지 않는 프로세스 각각에 대응되는 프로그램 정보를 획득하는 동작, 프로그램 정보에 기초하여, 화이트리스트에 속하지 않는 프로세스 중 서버에 대한 시스템 권한 및 다른 프로세스와 통신이 가능한 네트워크 통신 권한을 보유한 프로세스를 코드 인젝션(Code Injection)이 이루어진 타겟 프로세스를 검출하는 동작 및 타겟 프로세스의 코드 정보 중 적어도 일부를 포함하는 검출 결과를 서버로 전송하는 동작을 포함한다.

[0007] 검출하는 동작은, 화이트리스트에 속하지 않는 프로세스 중 읽기, 쓰기 및 실행 권한을 보유하고, 기 설정된 크기 이상의 메모리가 할당된 포괄적 호스트 프로세스(Generic Host Process)를 시스템 권한 및 네트워크 통신 권한을 받은 타겟 프로세스로 검출할 수 있다.

[0008] 검출 결과는, 검출된 타겟 프로세스에 할당된 메모리 상의 코드 영역에서의 덤프 파일(Dump File)을 포함할 수 있다.

[0009] 다른 실시예에 따른 서버 모니터링 방법은, 서버로부터 서버에서 실행 중인 하나 이상의 프로세스에 대한 리스트를 획득하는 동작, 서버로부터 하나 이상의 프로세스 중 기 정의된 화이트리스트에 속하지 않는 프로세스 각각에 대응되는 프로그램 정보를 획득하는 동작, 프로그램 정보에 기초하여, 화이트리스트에 속하지 않는 프로세스에 속하는 복수의 스레드(Thread) 각각이 실행되는 영역 및 복수의 스레드 각각이 보유한 권한을 기준으로 복수의 스레드 중 코드 인젝션(Code Injection)이 이루어진 타겟 스레드를 검출하는 동작 및 타겟 스레드의 코드

정보 중 적어도 일부를 포함하는 검출 결과를 서버로 전송하는 동작을 포함한다.

[0010] 검출하는 동작은, 복수의 스레드 중 읽기, 쓰기 및 실행 권한을 보유하고, 각 스레드가 속한 프로세스와 대응되는 프로그램 파일의 코드 영역 외의 영역 상에서 실행되는 스레드를 타겟 스레드로 검출할 수 있다.

[0011] 검출 결과는, 검출된 타겟 스레드에 할당된 메모리 상의 영역에서의 덤프 파일(Dump File)을 포함할 수 있다.

[0012] 개시되는 일 실시예에 따른 서버 모니터링 장치는, 서버로부터 서버에서 실행 중인 하나 이상의 프로세스에 대한 리스트를 획득하고, 서버로부터 하나 이상의 프로세스 중 기 정의된 화이트리스트에 속하지 않는 프로세스 각각에 대응되는 프로그램 정보를 획득하는 획득부, 프로그램 정보에 기초하여, 화이트리스트에 속하지 않는 프로세스 중 서버에 대한 시스템 권한 및 다른 프로세스와 통신이 가능한 네트워크 통신 권한을 보유한 프로세스를 코드 인젝션(Code Injection)이 이루어진 타겟 프로세스로 검출하는 검출부 및 타겟 프로세스의 코드 정보 중 적어도 일부를 포함하는 검출 결과를 서버로 전송하는 전송부를 포함한다.

[0013] 검출부는, 화이트리스트에 속하지 않는 프로세스 중 읽기, 쓰기 및 실행 권한을 보유하고, 기 설정된 크기 이상의 메모리가 할당된 포괄적 호스트 프로세스(Generic Host Process)를 시스템 권한 및 네트워크 통신 권한을 받은 타겟 프로세스로 검출할 수 있다.

[0014] 검출 결과는, 검출된 타겟 프로세스에 할당된 메모리 상의 코드 영역에서의 덤프 파일(Dump File)을 포함할 수 있다.

[0015] 다른 실시예에 따른 서버 모니터링 장치는, 서버로부터 서버에서 실행 중인 하나 이상의 프로세스에 대한 리스트를 획득하고, 서버로부터 하나 이상의 프로세스 중 기 정의된 화이트리스트에 속하지 않는 프로세스 각각에 대응되는 프로그램 정보를 획득하는 획득부, 프로그램 정보에 기초하여, 화이트리스트에 속하지 않는 프로세스에 속하는 복수의 스레드(Thread) 각각이 실행되는 영역 및 복수의 스레드 각각이 보유한 권한을 기준으로 복수의 스레드 중 코드 인젝션(Code Injection)이 이루어진 타겟 스레드를 검출하는 검출부 및 타겟 스레드의 코드 정보 중 적어도 일부를 포함하는 검출 결과를 서버로 전송하는 전송부를 포함한다.

[0016] 검출부는, 복수의 스레드 중 읽기, 쓰기 및 실행 권한을 보유하고, 각 스레드가 속한 프로세스와 대응되는 프로그램 파일의 코드 영역 외의 영역 상에서 실행되는 스레드를 타겟 스레드로 검출할 수 있다.

[0017] 검출 결과는, 검출된 타겟 스레드에 할당된 메모리 상의 영역에서의 덤프 파일(Dump File)을 포함할 수 있다.

발명의 효과

[0018] 개시되는 실시예들에 따르면, 화이트리스트에 기반하여 서버 내에서 실행되는 악성 코드를 검출함으로써, 실행 가능한 모든 프로세스를 사전에 정의하지 않고도 서버의 무결성을 검증할 수 있다.

[0019] 또한 개시되는 실시예들에 따르면, 프로세스의 종류 및 부여된 권한을 바탕으로 악성 코드의 인젝션이 이루어진 프로세스를 검출함으로써, 별도의 프로세스로 실행되지 않고 은닉된 채로 실행 중인 악성 코드를 효과적으로 검출할 수 있다.

도면의 간단한 설명

[0020] 도 1은 일 실시예에 따른 서버 모니터링 시스템을 나타내는 블록도

도 2는 실시예에 따른 서버 모니터링 장치를 설명하기 위한 블록도

도 3은 제1 실시예에 따른 서버 모니터링 방법을 설명하기 위한 흐름도

도 4는 제1 실시예에 따른 서버 모니터링 방법을 보다 상세히 설명하기 위한 흐름도

도 5는 타겟 프로세스를 검출하는 동작을 보다 상세히 설명하기 위한 흐름도

도 6은 타겟 프로세스의 실행 패턴을 나타내는 예시도

도 7은 제2 실시예에 따른 서버 모니터링 방법을 설명하기 위한 흐름도

도 8은 제2 실시예에 따른 서버 모니터링 방법을 보다 상세히 설명하기 위한 흐름도

도 9는 타겟 스레드를 검출하는 동작을 보다 상세히 설명하기 위한 흐름도

도 10은 타겟 스레드의 실행 패턴을 나타내는 예시도

도 11은 일 실시예에 따른 컴퓨팅 장치를 포함하는 컴퓨팅 환경을 예시하여 설명하기 위한 블록도

발명을 실시하기 위한 구체적인 내용

[0021] 이하, 도면을 참조하여 구체적인 실시형태를 설명하기로 한다. 이하의 상세한 설명은 본 명세서에서 기술된 방법, 장치 및/또는 시스템에 대한 포괄적인 이해를 돕기 위해 제공된다. 그러나 이는 예시에 불과하며 개시되는 실시예들은 이에 제한되지 않는다.

[0022] 실시예들을 설명함에 있어서, 관련된 공지기술에 대한 구체적인 설명이 개시되는 실시예들의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략하기로 한다. 그리고, 후술되는 용어들은 개시되는 실시예들에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다. 상세한 설명에서 사용되는 용어는 단지 실시예들을 기술하기 위한 것이며, 결코 제한적이어서는 안 된다. 명확하게 달리 사용되지 않는 한, 단수 형태의 표현은 복수 형태의 의미를 포함한다. 본 설명에서, "포함" 또는 "구비"와 같은 표현은 어떤 특성들, 숫자들, 단계들, 동작들, 요소들, 이들의 일부 또는 조합을 가리키기 위한 것이며, 기술된 것 이외에 하나 또는 그 이상의 다른 특성, 숫자, 단계, 동작, 요소, 이들의 일부 또는 조합의 존재 또는 가능성을 배제하도록 해석되어서는 안 된다.

[0023] 도 1은 일 실시예에 따른 서버 모니터링 시스템(100)을 나타내는 블록도이다.

[0024] 도시된 바와 같이, 일 실시예에 따른 서버 모니터링 시스템(100)은 서버 모니터링 장치(110) 및 서버(120)를 포함한다.

[0025] 서버 모니터링 장치(110)는 서버(120)의 무결성을 검증하는 장치로서, 구체적으로는 서버(120)의 시스템을 점검하여 서버(120) 내 유포된 악성 코드를 검출한다.

[0026] 일 실시예에 따르면, 서버 모니터링 장치(110)는 점검-수집-관리-대응으로 이루어진 모니터링 프로세스에 따라 주기적으로 서버(120)의 시스템을 점검하여, 악성 코드의 특징만으로 서버(120) 내 유포된 악성 코드를 식별하고, 해당 악성 코드와 관련된 상세한 정보를 서버(120)의 관리자에게 보고할 수 있다.

[0027] 구체적으로, 서버 모니터링 장치(110)의 모니터링 프로세스는 다음과 같이 구성될 수 있다.

[0028] (1) 점검 프로세스: 서버 모니터링 장치(110)가 제공하는 점검 프로그램을 통한 주기적인 서버 시스템 점검

[0029] (2) 수집 프로세스: 점검 결과를 서버로 수집

[0030] (3) 관리 프로세스: 서버의 시스템 무결성 검증을 위한 화이트리스트 관리

[0031] (4) 대응 프로세스: 서버의 시스템 내 탐지된 악성 코드의 특징 패턴 생성

[0032] 보다 상세하게, 상술한 점검 프로세스 상에서, 서버 모니터링 장치(110)가 제공하는 점검 프로그램은 서버(120)의 시스템 상에서 스케줄러(Scheduler)로서 등록 및 실행될 수 있다.

[0033] 일 실시예에 따르면, 서버 모니터링 장치(110)는 서버(120)에 구비된 에이전트(미도시)와 통신 네트워크를 통해 정보를 교환함으로써, 서버(120) 내 유포된 악성 코드를 검출할 수 있다.

[0034] 이때, 통신 네트워크는 인터넷, 하나 이상의 로컬 영역 네트워크(local area networks), 광역 네트워크(wire area networks), 셀룰러 네트워크, 모바일 네트워크, 그 밖에 다른 종류의 네트워크들, 또는 이러한 네트워크들의 조합을 포함할 수 있다.

[0035] 서버(120)는 하나 이상의 클라이언트(미도시)와 연결되어, 웹 상으로 또는 각 클라이언트에 구비된 애플리케이션을 통해 클라이언트 각각에게 서비스를 제공하는 장치이다.

[0036] 비록, 도 1에서 서버(120)는 단일한 개체로 도시되어 있으나, 실시예에 따라서 서버 모니터링 장치(110)에 의해 모니터링되는 서버는 복수 개일 수 있음에 유의해야 한다.

[0037] 도 2는 실시예에 따른 서버 모니터링 장치(110)를 설명하기 위한 블록도이다.

[0038] 도시된 바와 같이, 실시예에 따른 서버 모니터링 장치(110)는 획득부(111), 검출부(113) 및 전송부(115)를 포함한다.

[0039] 제1 실시예에 따르면, 서버 모니터링 장치(110)는 프로세스(Process)를 검출 단위로 하여 기 설정된 조건을 만

족하는 타겟 프로세스를 검출함으로써 서버를 모니터링할 수도 있으나, 또 다른 제2 실시예에 따라서는 프로세스를 구성하는 스레드(Thread)를 검출 단위로 하여 기 설정된 조건을 만족하는 타겟 스레드를 검출함으로써 서버를 모니터링할 수도 있다.

[0040] 이하에서는, 제1 실시예와 제2 실시예를 구분하여 각 실시예에 따른 세부 구성의 역할을 설시하기로 한다.

[0041] [제1 실시예]

[0042] 획득부(111)는 서버(120)로부터 서버(120)에서 실행 중인 하나 이상의 프로세스에 대한 리스트를 획득하고, 서버(120)로부터 하나 이상의 프로세스 중 기 정의된 화이트리스트에 속하지 않는 프로세스 각각에 대응되는 프로그램 정보를 획득한다.

[0043] 이하의 실시예들에서, '화이트리스트'는 실행이 허용되는 프로세스의 목록을 의미하며, 이러한 목록은 사용자에 의해 사전에 정의될 수 있다.

[0044] 종래의 악성 코드 방지를 위한 장치들은 사전에 설정된 유해 소프트웨어의 실행을 차단하거나, 특정 게임을 플레이할 수 없게 하거나, 특정 증권 거래 프로그램을 사용할 수 없게 하는 등, 블랙리스트에 해당하는 프로세스의 실행만을 차단함으로써 서버의 무결성을 유지하려 하였다. 그러나, 이러한 블랙리스트 기반의 방법으로는 예측 불가능한 새로운 악성 코드로 인한 피해를 예방할 수 없기 때문에, 서버 모니터링 장치(110)는 상술한 화이트리스트를 기반으로 악성 코드를 검출한다.

[0045] 검출부(113)는 획득된 프로그램 정보에 기초하여, 기 정의된 화이트리스트에 속하지 않는 프로세스 중 기 정의된 패턴에 따라 실행 중인 타겟 프로세스를 검출한다.

[0046] 제1 실시예에 따르면, 검출부(113)는 기 정의된 패턴에 기초하여, 기 정의된 화이트리스트에 속하지 않는 프로세스 중 코드 인젝션(Code Injection)이 이루어진 프로세스를 타겟 프로세스로 검출할 수 있다.

[0047] 구체적으로, '코드 인젝션'은 정상적인 프로세스에 악성 코드를 주입하는 행위를 의미하며, 이렇게 주입된 악성 코드는 별도의 프로세스를 생성하지 않고 정상적인 프로세스의 메모리 영역에 추가되어 은닉된 채로 동작하게 된다. 이로 인해, 종래의 보안 프로그램이 프로세스의 목록을 조사하거나, 프로세스의 이름을 기반으로 필터링을 수행하더라도 악성 코드가 주입된 프로세스를 탐지할 수 없게 된다.

[0048] 제1 실시예에 따르면, 검출부(113)는 기 정의된 화이트리스트에 속하지 않는 프로세스 중 서버(120)에 대한 시스템 권한 및 다른 프로세스와 통신이 가능한 네트워크 통신 권한을 보유한 프로세스를 코드 인젝션이 이루어진 타겟 프로세스로 검출할 수 있다.

[0049] 제1 실시예에 따르면, 검출부(113)는 화이트리스트에 속하지 않는 프로세스 중 읽기, 쓰기 및 실행 권한을 보유하고, 기 설정된 크기 이상의 메모리가 할당된 포괄적 호스트 프로세스(Generic Host Process)를 시스템 권한 및 네트워크 통신 권한을 받은 타겟 프로세스로 검출할 수 있다.

[0050] 구체적으로, '포괄적 호스트 프로세스'는 일련의 윈도우 기반 Win32 서비스를 처리하기 위한 프로세스를 의미한다. 예를 들어, 포괄적 호스트 프로세스는 'svchost.exe' 파일을 통해 수행될 수 있다.

[0051] 한편 구체적으로, '읽기, 쓰기 및 실행 권한을 보유한 프로세스'라 함은, 프로세스의 사용 권한 중 읽기 권한, 쓰기 권한 및 실행 권한이 모두 '허용'으로 설정된 프로세스를 의미할 수 있다.

[0052] 또한 구체적으로, 타겟 프로세스 검출의 기준이 되는 '기 설정된 크기 이상의 메모리'라 함은 서버(120)의 시스템에 유의미한 영향을 주기 위한 악성 코드가 주입되기 위해서 필요한 최소 크기 이상의 메모리를 의미할 수 있다. 예를 들어, 검출부(113)는 4096 바이트를 할당되는 메모리의 최소 크기 조건으로 설정할 수 있다.

[0053] 전송부(115)는 검출된 타겟 프로세스의 코드 정보 중 적어도 일부를 포함하는 검출 결과를 서버(120)로 전송한다.

[0054] 제1 실시예에 따르면, 서버(120)로 전송되는 검출 결과는 검출부(113)에 의해 검출된 타겟 프로세스에 할당된 메모리 상의 코드 영역에서의 덤프 파일(Dump File)을 포함할 수 있다.

[0055] 이후, 서버(120)의 관리자는 전송된 덤프 파일 내 코드 정보를 분석하고, 추가 확인이 필요하다 판단되는 경우 서버(120)에 직접 접근하여 서버(120)를 점검할 수 있다. 즉 다시 말하면, 서버 모니터링 장치(110)를 이용하여 검출 및 전송되는 검출 결과를 통해, 일부 악성 코드는 관리자의 개입 없이도 자동적으로 검출할 수 있다.

[0056] 제1 실시예에 따르면, 전송부(115)는 타겟 프로세스에 대응되는 프로그램에 있어서, 프로그램 식별을 위한 해시

값, 프로그램 사이즈, 프로세스 실행 차단이 이루어지는 시간, 프로그램 이름, 프로그램 공급사 이름, 프로세스 실행 경로 중 적어도 하나 이상에 대한 정보를 더 포함하는 검출 결과를 서버(120)로 전송할 수 있다.

[0057] [제2 실시예]

[0058] 획득부(111)는 서버(120)로부터 서버(120)에서 실행 중인 하나 이상의 프로세스에 대한 리스트를 획득하고, 서버(120)로부터 하나 이상의 프로세스 중 기 정의된 화이트리스트에 속하지 않는 프로세스 각각에 대응되는 프로그램 정보를 획득한다.

[0059] 검출부(113)는 획득된 프로그램 정보에 기초하여, 기 정의된 화이트리스트에 속하지 않는 프로세스에 속하는 복수의 스레드 중 기 정의된 패턴에 따라 실행 중인 타겟 스레드를 검출한다.

[0060] 제2 실시예에 따르면, 검출부(113)는 기 정의된 패턴에 기초하여, 복수의 스레드 중 코드 인젝션이 이루어진 스레드를 타겟 스레드로 검출할 수 있다.

[0061] 제2 실시예에 따르면, 검출부(113)는 복수의 스레드 각각이 실행되는 영역 및 복수의 스레드 각각이 보유한 권한에 기초하여 코드 인젝션이 이루어진 타겟 스레드를 검출할 수 있다.

[0062] 구체적으로, 검출부(113)는 복수의 스레드 중 읽기, 쓰기 및 실행 권한을 보유하고, 각 스레드가 속한 프로세스와 대응되는 프로그램 파일의 코드 영역 외의 영역 상에서 실행되는 스레드를 타겟 스레드로 검출할 수 있다.

[0063] 즉 다시 말하면, 검출부(113)는 각 스레드가 실행되는 메모리 영역을 식별한 후, 식별된 메모리 영역이 각 스레드에 따른 프로그램 파일의 코드 영역이 아닌 경우, 해당 스레드 중 읽기, 쓰기 및 실행 권한을 보유한 스레드를 타겟 스레드로 검출할 수 있다.

[0064] 전송부(115)는 검출된 타겟 스레드의 코드 정보 중 적어도 일부를 포함하는 검출 결과를 서버(120)로 전송한다.

[0065] 제2 실시예에 따르면, 서버(120)로 전송되는 검출 결과는 검출부(113)에 의해 검출된 타겟 스레드에 할당된 메모리 상의 영역에서의 덤프 파일을 포함할 수 있다.

[0066] 제2 실시예에 따르면, 전송부(115)는 타겟 스레드에 대응되는 프로그램에 있어서, 프로그램 식별을 위한 해시값, 프로그램 사이즈, 스레드 실행 차단이 이루어지는 시간, 프로그램 이름, 프로그램 공급사 이름, 스레드 실행 경로 중 적어도 하나 이상에 대한 정보를 더 포함하는 검출 결과를 서버(120)로 전송할 수 있다.

[0067] 도시된 제1 및 제2 실시예에서, 각 구성들은 이하에 기술된 것 이외에 상이한 기능 및 능력을 가질 수 있고, 이하에 기술된 것 이외에도 추가적인 구성을 포함할 수 있다.

[0068] 또한, 제1 및 제2 실시예에서, 획득부(111), 검출부(113) 및 전송부(115)는 물리적으로 구분된 하나 이상의 장치를 이용하여 구현되거나, 하나 이상의 프로세서 또는 하나 이상의 프로세서 및 소프트웨어의 결합에 의해 구현될 수 있으며, 도시된 예와 달리 구체적 동작에 있어 명확히 구분되지 않을 수 있다.

[0069] 도 3은 제1 실시예에 따른 서버 모니터링 방법을 설명하기 위한 흐름도이다.

[0070] 도 3에 도시된 방법은 예를 들어, 상술한 서버 모니터링 장치(110)에 의해 수행될 수 있다.

[0071] 우선, 서버 모니터링 장치(110)는 서버(120)로부터 서버(120)에서 실행 중인 하나 이상의 프로세스에 대한 리스트를 획득한다(310).

[0072] 이후, 서버 모니터링 장치(110)는 서버(120)로부터 하나 이상의 프로세스 중 기 정의된 화이트리스트에 속하지 않는 프로세스 각각에 대응되는 프로그램 정보를 획득한다(320).

[0073] 이후, 서버 모니터링 장치(110)는 획득된 프로그램 정보에 기초하여, 화이트리스트에 속하지 않는 프로세스 중 기 정의된 패턴에 따라 실행 중인 타겟 프로세스를 검출한다(330).

[0074] 이후, 서버 모니터링 장치(110)는 검출된 타겟 프로세스의 코드 정보 중 적어도 일부를 포함하는 검출 결과를 서버(120)로 전송한다(340).

[0075] 도 4는 제1 실시예에 따른 서버 모니터링 방법을 보다 상세히 설명하기 위한 흐름도이다.

[0076] 도 4에 도시된 방법은 예를 들어, 상술한 서버 모니터링 장치(110)에 의해 수행될 수 있다.

[0077] 우선, 서버 모니터링 장치(110)는 서버(120)로부터 서버(120)에서 실행 중인 하나 이상의 프로세스에 대한 리스트를 획득한다(410).

[0078] 이후, 서버 모니터링 장치(110)는 획득된 리스트 내 각 프로세스가 기 정의된 화이트리스트에 속하는지 여부를 판단한다(420).

[0079] 이후, 서버 모니터링 장치(110)는 판단 대상이 된 프로세스가 화이트리스트에 속한다고 판단된 경우, 해당 프로세스의 실행을 허용한다(430).

[0080] 한편, 서버 모니터링 장치(110)는 판단 대상이 된 프로세스가 화이트리스트에 속하지 않는다고 판단된 경우, 해당 프로세스에 대응되는 프로그램 정보를 획득한다(440).

[0081] 이후, 서버 모니터링 장치(110)는 획득된 프로그램 정보에 기초하여, 화이트리스트에 속하지 않는다고 판단된 프로세스가 기 정의된 패턴에 따라 실행됨으로써 코드 인젝션이 이루어진 프로세스인지 여부를 판단한다(450).

[0082] 이후, 서버 모니터링 장치(110)는 판단 대상이 된 프로세스가 코드 인젝션이 이루어지지 않은 프로세스로 판단된 경우, 해당 프로세스의 실행을 허용한다(430).

[0083] 한편, 서버 모니터링 장치(110)는 판단 대상이 된 프로세스가 코드 인젝션이 이루어진 프로세스로 판단된 경우, 해당 프로세스를 타겟 프로세스로 검출한다(460).

[0084] 이후, 서버 모니터링 장치(110)는 검출된 타겟 프로세스의 코드 정보 중 적어도 일부를 포함하는 검출 결과를 서버(120)로 전송한다(470).

[0085] 도 5는 타겟 프로세스를 검출하는 동작(450)을 보다 상세히 설명하기 위한 흐름도이다.

[0086] 도 5에 도시된 방법은 예를 들어, 상술한 서버 모니터링 장치(110)에 의해 수행될 수 있다.

[0087] 우선, 서버 모니터링 장치(110)는 화이트리스트에 속하지 않는 프로세스에 대응되는 프로그램 정보를 획득한 후, 획득된 프로그램 정보에 기초하여 해당 프로세스가 포괄적 호스트 프로세스인지 여부를 판단한다(510).

[0088] 이후, 서버 모니터링 장치(110)는 판단 대상이 된 프로세스가 포괄적 호스트 프로세스로 판단된 경우, 해당 프로세스가 읽기, 쓰기 및 실행 권한이 있는지 여부를 판단한다(520).

[0089] 이후, 서버 모니터링 장치(110)는 판단 대상이 된 프로세스가 읽기, 쓰기 및 실행 권한이 있는 것으로 판단된 경우, 해당 프로세스에 기 설정된 크기 이상의 메모리가 할당되었는지 여부를 판단한다(530).

[0090] 이후, 서버 모니터링 장치(110)는 판단 대상이 된 프로세스에 기 설정된 크기 이상의 메모리가 할당된 것으로 판단된 경우, 해당 프로세스를 타겟 프로세스로 검출한다.

[0091] 한편, 서버 모니터링 장치(110)는 상술한 동작 510 내지 530을 통해 판단 대상이 된 프로세스가 하나의 조건이라도 만족하지 못하는 것으로 판단된 경우, 해당 프로세스를 타겟 프로세스가 아닌 것으로 판단하여 실행을 허용한다.

[0092] 상기 도시된 도 3 내지 도 5에서는 상기 방법을 복수 개의 동작으로 나누어 기재하였으나, 적어도 일부의 동작들은 순서를 바꾸어 수행되거나, 다른 동작과 결합되어 함께 수행되거나, 생략되거나, 세부 동작들로 나뉘어 수행되거나, 또는 도시되지 않은 하나 이상의 동작이 부가되어 수행될 수 있다.

[0093] 도 6은 타겟 프로세스의 실행 패턴을 나타내는 예시도이다.

[0094] 도 6을 참조하면, 좌측의 작업 관리자 창의 프로세스 탭 상에 현재 실행 중인 프로세스의 리스트가 도시되어 있다.

[0095] 도시된 프로세스들 중, 사각형 박스로 구분된 프로세스들은 포괄적 호스트 프로세스에 해당하는 'svchost.exe'를 통해 수행되는 복수의 프로세스들을 나타낸다.

[0096] 이어서 우측 창은, 상기 사각형 박스로 구분된 프로세스들 중 최상단의 'svchost.exe'에 대한 속성 창의 보안 탭을 도시한 것으로, 사각형 박스로 표시된 부분은 해당 프로세스에 부여된 사용 권한을 나타낸다.

[0097] 이를 통해, 해당 프로세스에는 읽기 권한 및 실행 권한이 '허용' 상태로 부여되어 있음을 알 수 있다. 이를 통해, 해당 프로세스에는 쓰기 권한이 부여되어 있지 않으므로, 서버 모니터링 장치(110)는 해당 프로세스가 비록 'svchost.exe'를 통해 수행되는 프로세스이나, 타겟 프로세스로 검출하지는 않을 것임을 예상할 수 있다.

[0098] 도 7은 제2 실시예에 따른 서버 모니터링 방법을 설명하기 위한 흐름도이다.

[0099] 도 7에 도시된 방법은 예를 들어, 상술한 서버 모니터링 장치(110)에 의해 수행될 수 있다.

[0100] 우선, 서버 모니터링 장치(110)는 서버(120)로부터 서버(120)에서 실행 중인 하나 이상의 프로세스에 대한 리스트를 획득한다(710).

[0101] 이후, 서버 모니터링 장치(110)는 서버(120)로부터 하나 이상의 프로세스 중 기 정의된 화이트리스트에 속하지 않는 프로세스 각각에 대응되는 프로그램 정보를 획득한다(720).

[0102] 이후, 서버 모니터링 장치(110)는 획득된 프로그램 정보에 기초하여, 화이트리스트에 속하지 않는 프로세스에 속하는 복수의 스레드 중 기 정의된 패턴에 따라 실행 중인 타겟 스레드를 검출한다(730).

[0103] 이후, 서버 모니터링 장치(110)는 검출된 타겟 스레드의 코드 정보 중 적어도 일부를 포함하는 검출 결과를 서버(120)로 전송한다(740).

[0104] 도 8은 제2 실시예에 따른 서버 모니터링 방법을 보다 상세히 설명하기 위한 흐름도이다.

[0105] 도 8에 도시된 방법은 예를 들어, 상술한 서버 모니터링 장치(110)에 의해 수행될 수 있다.

[0106] 우선, 서버 모니터링 장치(110)는 서버(120)로부터 서버(120)에서 실행 중인 하나 이상의 프로세스에 대한 리스트를 획득한다(810).

[0107] 이후, 서버 모니터링 장치(110)는 획득된 리스트 내 각 프로세스가 기 정의된 화이트리스트에 속하는지 여부를 판단한다(820).

[0108] 이후, 서버 모니터링 장치(110)는 판단 대상이 된 프로세스가 화이트리스트에 속한다고 판단된 경우, 해당 프로세스의 실행을 허용한다(830).

[0109] 한편, 서버 모니터링 장치(110)는 판단 대상이 된 프로세스가 화이트리스트에 속하지 않는다고 판단된 경우, 해당 프로세스에 대응되는 프로그램 정보를 획득한다(840).

[0110] 이후, 서버 모니터링 장치(110)는 획득된 프로그램 정보에 기초하여, 화이트리스트에 속하지 않는다고 판단된 프로세스에 속하는 복수의 스레드 각각이 기 정의된 패턴에 따라 실행됨으로써 코드 인젝션이 이루어진 스레드인지 여부를 판단한다(850).

[0111] 이후, 서버 모니터링 장치(110)는 판단 대상이 된 스레드가 코드 인젝션이 이루어지지 않은 스레드로 판단된 경우, 해당 프로세스(스레드)의 실행을 허용한다(830).

[0112] 한편, 서버 모니터링 장치(110)는 판단 대상이 된 스레드가 코드 인젝션이 이루어진 스레드로 판단된 경우, 해당 스레드를 타겟 스레드로 검출한다(860).

[0113] 이후, 서버 모니터링 장치(110)는 검출된 타겟 스레드의 코드 정보 중 적어도 일부를 포함하는 검출 결과를 서버(120)로 전송한다(870).

[0114] 도 9는 타겟 스레드를 검출하는 동작(850)을 보다 상세히 설명하기 위한 흐름도이다.

[0115] 도 9에 도시된 방법은 예를 들어, 상술한 서버 모니터링 장치(110)에 의해 수행될 수 있다.

[0116] 우선, 서버 모니터링 장치(110)는 화이트리스트에 속하지 않는 프로세스에 대응되는 프로그램 정보를 획득한 후, 획득된 프로그램 정보에 기초하여 화이트리스트에 속하지 않는다고 판단된 프로세스에 속하는 복수의 스레드 각각이 프로그램 파일의 코드 영역 외에서 실행되는지 여부를 판단한다(910).

[0117] 이후, 서버 모니터링 장치(110)는 판단 대상이 된 스레드가 프로그램 파일의 코드 영역 외에서 실행되는 것으로 판단된 경우, 해당 스레드가 읽기, 쓰기 및 실행 권한이 있는지 여부를 판단한다(920).

[0118] 이후, 서버 모니터링 장치(110)는 판단 대상이 된 스레드가 읽기, 쓰기 및 실행 권한이 있는 것으로 판단된 경우, 해당 스레드를 타겟 스레드로 검출한다.

[0119] 한편, 서버 모니터링 장치(110)는 상술한 동작 910 및 920을 통해 판단 대상이 된 스레드가 하나의 조건이라도 만족하지 못하는 것으로 판단된 경우, 해당 스레드를 타겟 스레드가 아닌 것으로 판단하여 실행을 허용한다.

[0120] 상기 도시된 도 7 내지 도 9에서는 상기 방법을 복수 개의 동작으로 나누어 기재하였으나, 적어도 일부의 동작들은 순서를 바꾸어 수행되거나, 다른 동작과 결합되어 함께 수행되거나, 생략되거나, 세부 동작들로 나뉘어 수행되거나, 또는 도시되지 않은 하나 이상의 동작이 부가되어 수행될 수 있다.

[0121] 도 10은 타겟 스레드의 실행 패턴을 나타내는 예시도이다.

[0122] 도 10을 참조하면, 사각형 박스로 표시된 부분에 예시적으로 메모장(notepad) 프로그램이 실행된 경우에 실행되는 스레드들이 도시되어 있다.

[0123] 구체적으로 'Start Address' 항목을 참조하면, 각 스레드가 어떠한 프로그램 파일의 코드 영역에서 실행되는지 확인할 수 있다. 예를 들어, 스레드 ID가 15056인 스레드의 경우, 'PIProtectorAPI64.dll' 파일의 코드 영역에서 실행되며, 스레드 ID가 39044인 스레드 및 46784인 스레드의 경우, 'ntdll.dll' 파일의 코드 영역에서 실행되고 있음을 알 수 있다.

[0124] 이를 통해, 상술한 파일과 같이 메모장 프로그램을 구성하는 파일의 코드 영역이 아닌 영역에서 실행되는 스레드를 구분할 수 있고, 그 경우 해당 스레드가 읽기, 쓰기 및 실행 권한을 갖고 있다면 서버 모니터링 장치(110)는 해당 스레드를 타겟 스레드로 검출하게 된다.

[0125] 도 11은 일 실시예에 따른 컴퓨팅 장치를 포함하는 컴퓨팅 환경(10)을 예시하여 설명하기 위한 블록도이다. 도시된 실시예에서, 각 컴포넌트들은 이하에 기술된 것 이외에 상이한 기능 및 능력을 가질 수 있고, 이하에 기술된 것 이외에도 추가적인 컴포넌트를 포함할 수 있다.

[0126] 도시된 컴퓨팅 환경(10)은 컴퓨팅 장치(12)를 포함한다. 일 실시예에서, 컴퓨팅 장치(12)는 서버 모니터링 장치(110)일 수 있다.

[0127] 컴퓨팅 장치(12)는 적어도 하나의 프로세서(14), 컴퓨터 판독 가능 저장 매체(16) 및 통신 버스(18)를 포함한다. 프로세서(14)는 컴퓨팅 장치(12)로 하여금 앞서 언급된 예시적인 실시예에 따라 동작하도록 할 수 있다. 예컨대, 프로세서(14)는 컴퓨터 판독 가능 저장 매체(16)에 저장된 하나 이상의 프로그램들을 실행할 수 있다. 상기 하나 이상의 프로그램들은 하나 이상의 컴퓨터 실행 가능 명령어를 포함할 수 있으며, 상기 컴퓨터 실행 가능 명령어는 프로세서(14)에 의해 실행되는 경우 컴퓨팅 장치(12)로 하여금 예시적인 실시예에 따른 동작들을 수행하도록 구성될 수 있다.

[0128] 컴퓨터 판독 가능 저장 매체(16)는 컴퓨터 실행 가능 명령어 내지 프로그램 코드, 프로그램 데이터 및/또는 다른 적합한 형태의 정보를 저장하도록 구성된다. 컴퓨터 판독 가능 저장 매체(16)에 저장된 프로그램(20)은 프로세서(14)에 의해 실행 가능한 명령어의 집합을 포함한다. 일 실시예에서, 컴퓨터 판독 가능 저장 매체(16)는 메모리(랜덤 액세스 메모리와 같은 휘발성 메모리, 비휘발성 메모리, 또는 이들의 적절한 조합), 하나 이상의 자기 디스크 저장 디바이스들, 광학 디스크 저장 디바이스들, 플래시 메모리 디바이스들, 그 밖에 컴퓨팅 장치(12)에 의해 액세스되고 원하는 정보를 저장할 수 있는 다른 형태의 저장 매체, 또는 이들의 적합한 조합일 수 있다.

[0129] 통신 버스(18)는 프로세서(14), 컴퓨터 판독 가능 저장 매체(16)를 포함하여 컴퓨팅 장치(12)의 다른 다양한 컴포넌트들을 상호 연결한다.

[0130] 컴퓨팅 장치(12)는 또한 하나 이상의 입출력 장치(24)를 위한 인터페이스를 제공하는 하나 이상의 입출력 인터페이스(22) 및 하나 이상의 네트워크 통신 인터페이스(26)를 포함할 수 있다. 입출력 인터페이스(22) 및 네트워크 통신 인터페이스(26)는 통신 버스(18)에 연결된다. 입출력 장치(24)는 입출력 인터페이스(22)를 통해 컴퓨팅 장치(12)의 다른 컴포넌트들에 연결될 수 있다. 예시적인 입출력 장치(24)는 포인팅 장치(마우스 또는 트랙패드 등), 키보드, 터치 입력 장치(터치패드 또는 터치스크린 등), 음성 또는 소리 입력 장치, 다양한 종류의 센서 장치 및/또는 촬영 장치와 같은 입력 장치, 및/또는 디스플레이 장치, 프린터, 스피커 및/또는 네트워크 카드와 같은 출력 장치를 포함할 수 있다. 예시적인 입출력 장치(24)는 컴퓨팅 장치(12)를 구성하는 일 컴포넌트로서 컴퓨팅 장치(12)의 내부에 포함될 수도 있고, 컴퓨팅 장치(12)와는 구별되는 별개의 장치로 컴퓨팅 장치(12)와 연결될 수도 있다.

[0131] 한편, 본 발명의 실시예는 본 명세서에서 기술한 방법들을 컴퓨터상에서 수행하기 위한 프로그램, 및 상기 프로그램을 포함하는 컴퓨터 판독 가능 기록매체를 포함할 수 있다. 상기 컴퓨터 판독 가능 기록매체는 프로그램 명령, 로컬 데이터 파일, 로컬 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체는 본 발명을 위하여 특별히 설계되고 구성된 것들이거나, 또는 컴퓨터 소프트웨어 분야에서 통상적으로 사용 가능한 것일 수 있다. 컴퓨터 판독 가능 기록매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM, DVD와 같은 광 기록 매체, 및 롬, 램, 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 상기 프로그램의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함할 수 있다.

[0132] 이상에서 본 발명의 대표적인 실시예들을 상세하게 설명하였으나, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자는 상술한 실시예에 대하여 본 발명의 범주에서 벗어나지 않는 한도 내에서 다양한 변형이 가능함을 이해할 것이다. 그러므로 본 발명의 권리범위는 설명된 실시예에 국한되어 정해져서는 안 되며, 후술하는 청구범위뿐만 아니라 이 청구범위와 균등한 것들에 의해 정해져야 한다.

부호의 설명

[0133] 10: 컴퓨팅 환경

12: 컴퓨팅 장치

14: 프로세서

16: 컴퓨터 판독 가능 저장 매체

18: 통신 버스

20: 프로그램

22: 입출력 인터페이스

24: 입출력 장치

26: 네트워크 통신 인터페이스

100: 서버 모니터링 시스템

110: 서버 모니터링 장치

111: 획득부

113: 검출부

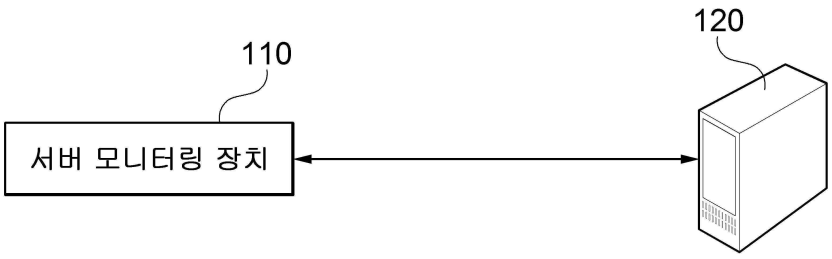
115: 전송부

120: 서버

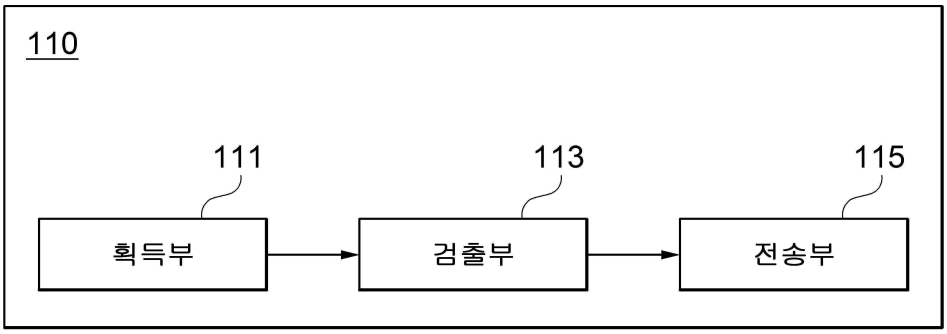
도면

도면1

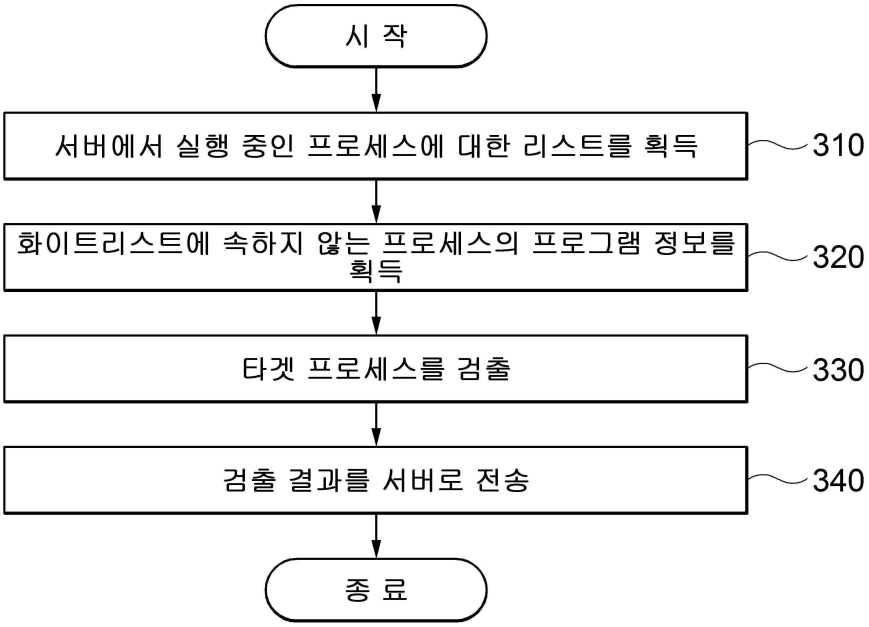
100



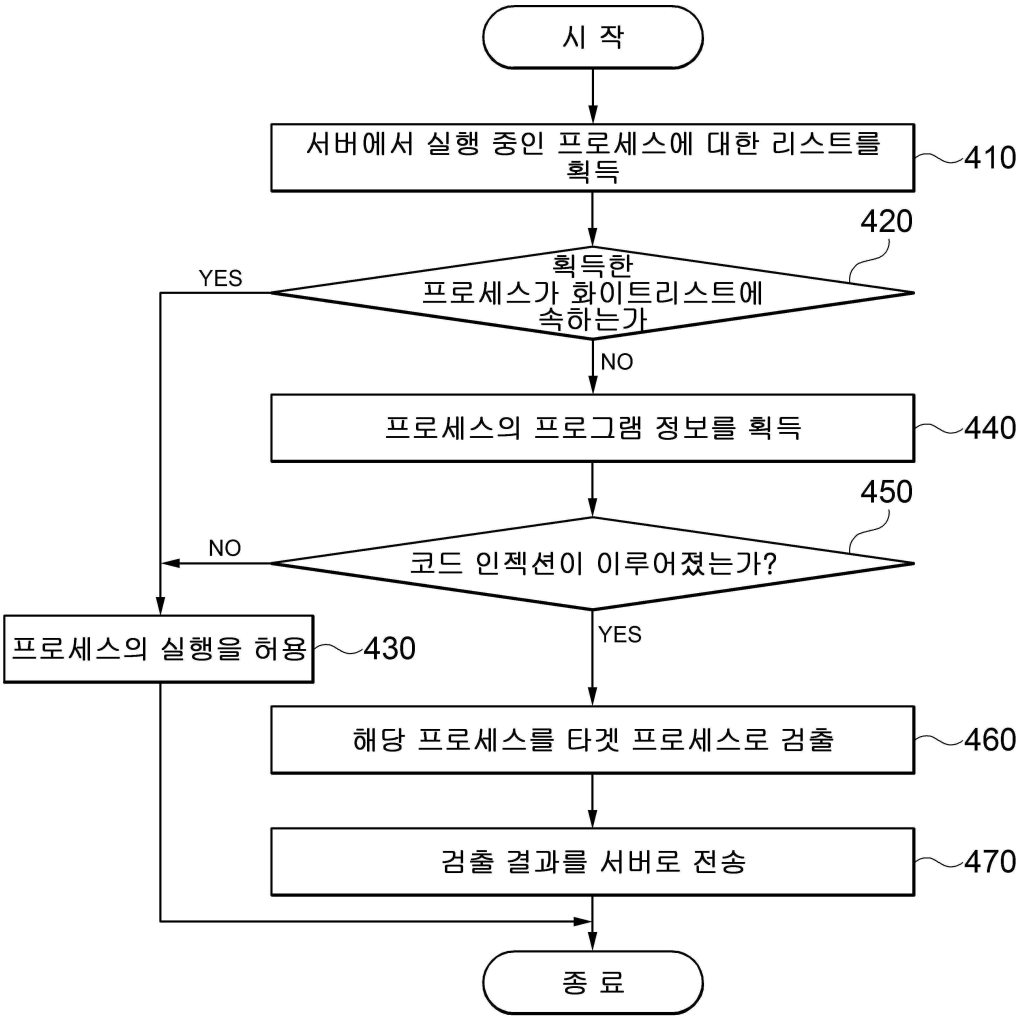
도면2


110
111
113
115
획득부
검출부
전송부

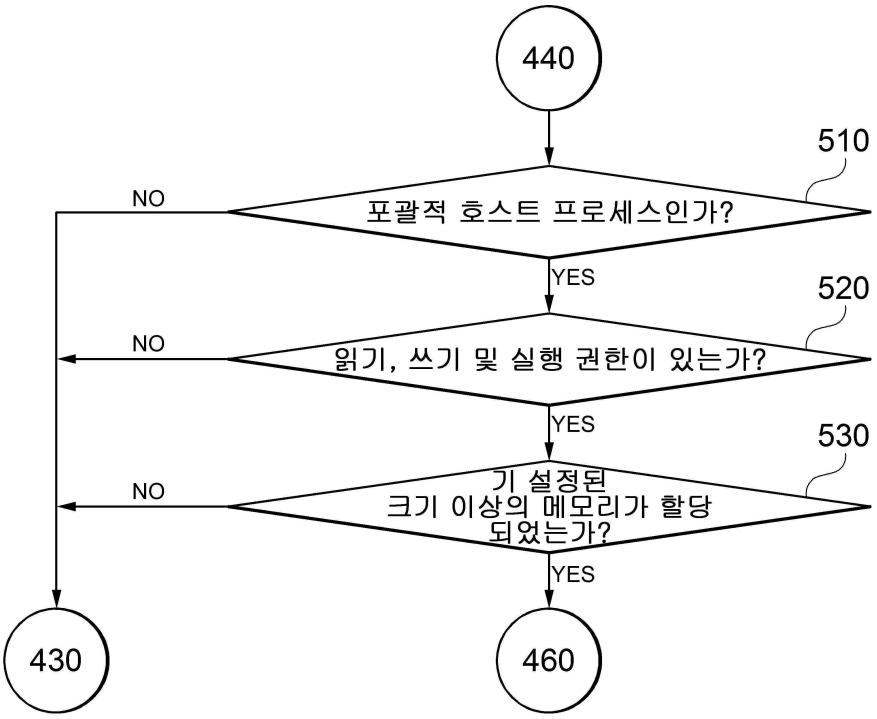
도면3


시 작
서버에서 실행 중인 프로세스에 대한 리스트를 획득
310
화이트리스트에 속하지 않는 프로세스의 프로그램 정보를 획득
320
타겟 프로세스를 검출
330
검출 결과를 서버로 전송
340
종 료

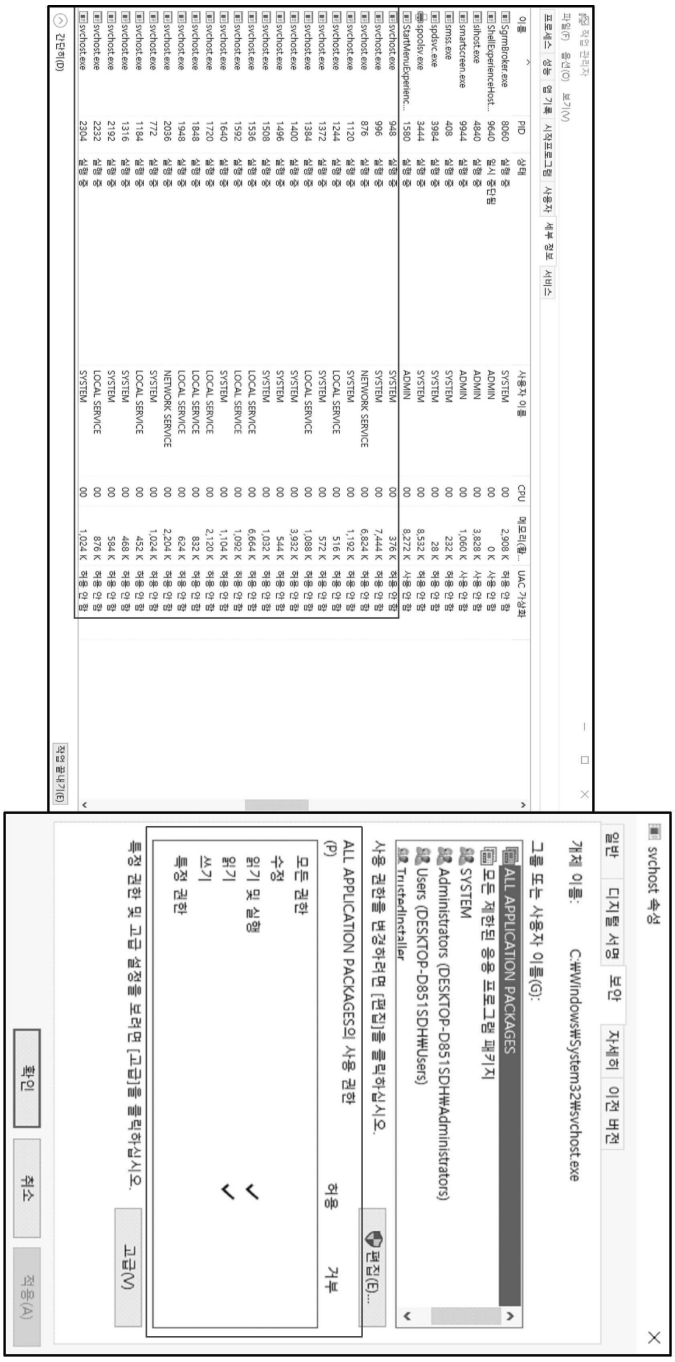
도면4


시 작
서버에서 실행 중인 프로세스에 대한 리스트를 획득
410
420
획득한 프로세스가 화이트리스트에 속하는가
YES
NO
프로세스의 프로그램 정보를 획득
440
450
코드 인젝션이 이루어졌는가?
NO
YES
프로세스의 실행을 허용
430
해당 프로세스를 타겟 프로세스로 검출
460
검출 결과를 서버로 전송
470
종 료

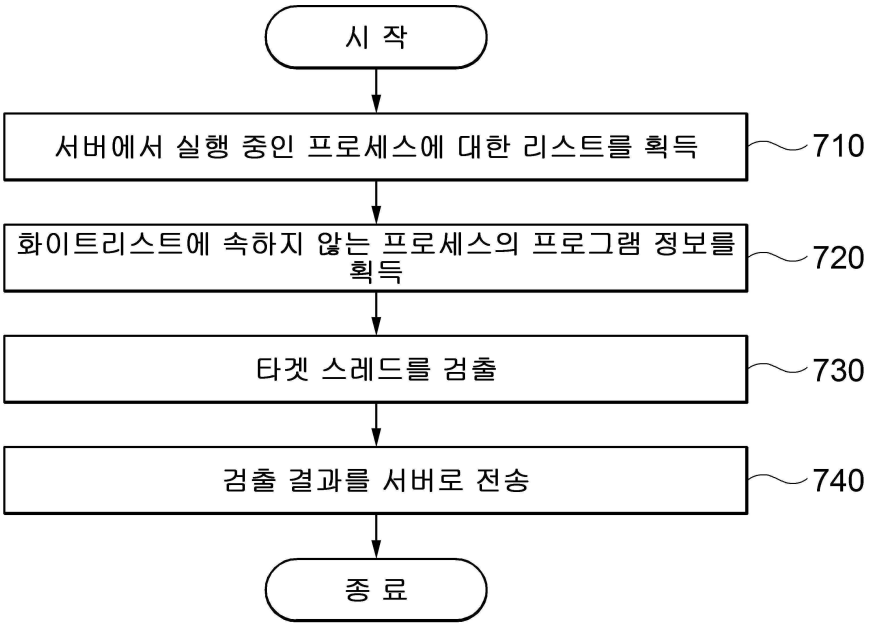
도면5


440
510
포괄적 호스트 프로세스인가?
NO
YES
520
읽기, 쓰기 및 실행 권한이 있는가?
NO
YES
530
기 설정된 크기 이상의 메모리가 할당 되었는가?
NO
YES
430
460

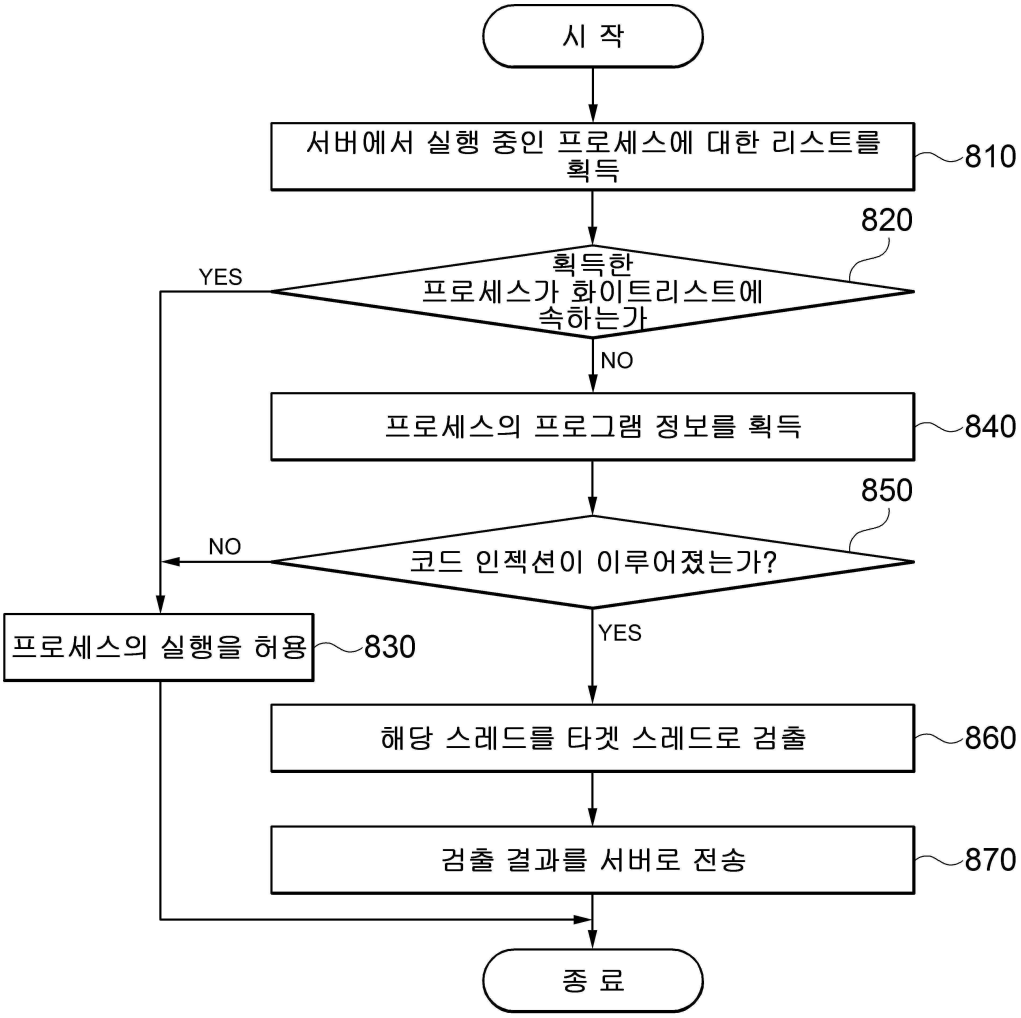
도면6


600
svchost 속성
일반
디지털 서명
보안
자세히
이전 버전
개체 이름: C:₩Windows₩System32₩svchost.exe
그룹 또는 사용자 이름(G):
ALL APPLICATION PACKAGES
모든 제한된 응용 프로그램 패키지
SYSTEM
Administrators (DESKTOP-D851SDH₩Administrators)
Users (DESKTOP-D851SDH₩Users)
TrustedInstaller
사용 권한을 변경하려면 [편집]을 클릭하십시오.
편집(E)...
ALL APPLICATION PACKAGES의 사용 권한(P)
허용
거부
모든 권한
수정
읽기 및 실행
읽기
쓰기
특정 권한
특정 권한 및 고급 설정을 보려면 [고급]을 클릭하십시오.
고급(V)
확인
취소
적용(A)

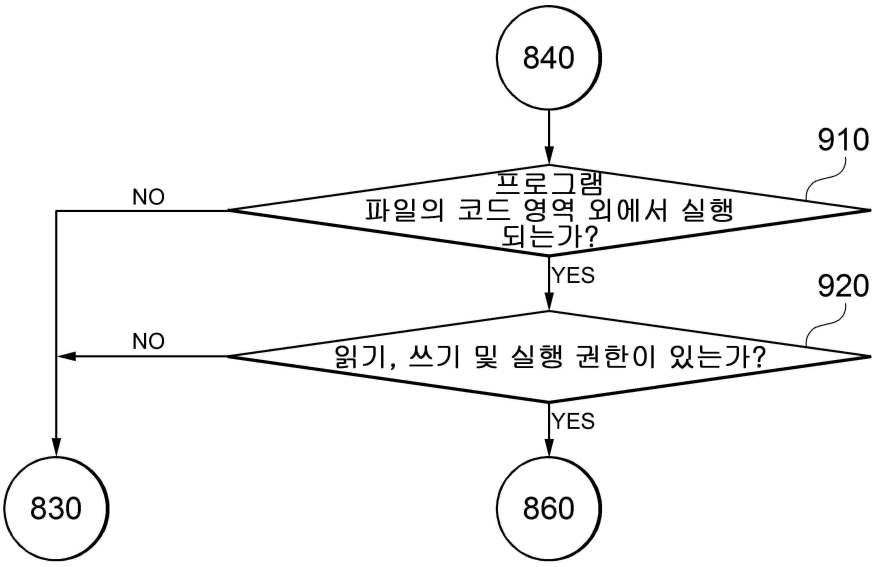
도면7


시 작
서버에서 실행 중인 프로세스에 대한 리스트를 획득
710
화이트리스트에 속하지 않는 프로세스의 프로그램 정보를 획득
720
타겟 스레드를 검출
730
검출 결과를 서버로 전송
740
종 료

도면8


시 작
서버에서 실행 중인 프로세스에 대한 리스트를 획득
810
820
획득한 프로세스가 화이트리스트에 속하는가
YES
NO
프로세스의 프로그램 정보를 획득
840
850
코드 인젝션이 이루어졌는가?
NO
YES
프로세스의 실행을 허용
830
해당 스레드를 타겟 스레드로 검출
860
검출 결과를 서버로 전송
870
종 료

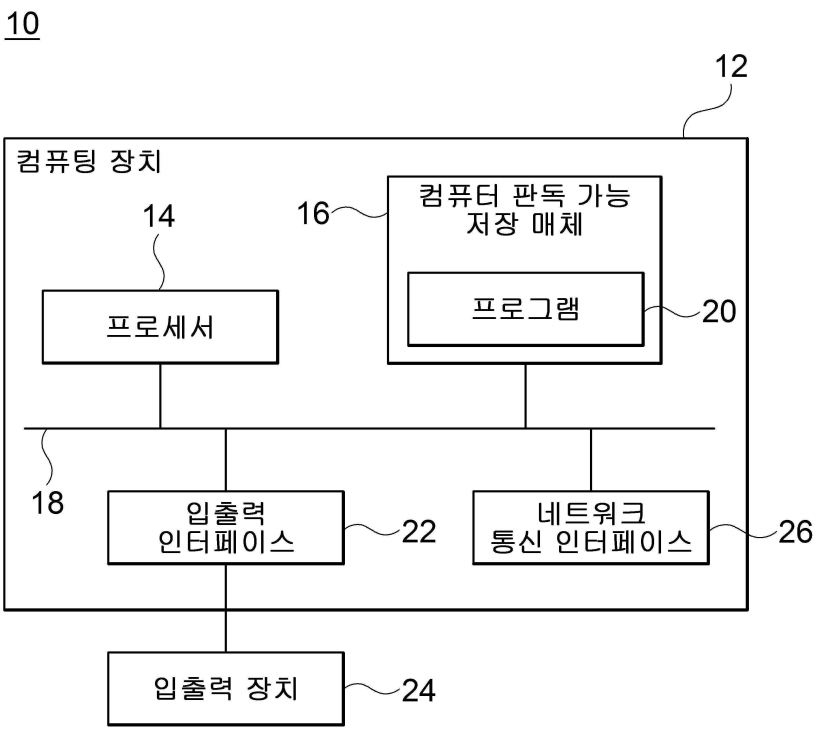
도면9



도면10

1000

도면11


10
12
컴퓨팅 장치
14
프로세서
16
컴퓨터 판독 가능
저장 매체
프로그램
20
18
입출력
인터페이스
22
네트워크
통신 인터페이스
26
입출력 장치
24