(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0059540
(43) 공개일자 2020년05월29일

(51) 국제특허분류(Int. Cl.)
G06F 21/56 (2013.01) *G06F 21/55* (2013.01)
(52) CPC특허분류
G06F 21/566 (2013.01)
G06F 21/552 (2013.01)
(21) 출원번호 10-2018-0144399
(22) 출원일자 2018년11월21일
심사청구일자 2018년11월21일

(71) 출원인
충남대학교산학협력단
대전광역시 유성구 대학로 99 (궁동, 충남대학교)
(72) 발명자
원유재
대전광역시 유성구 온천로 45, 알파동 805호(봉명동)
서정훈
대전광역시 유성구 죽동로280번길 22, 301호(죽동)
(뒷면에 계속)
(74) 대리인
특허법인 공간

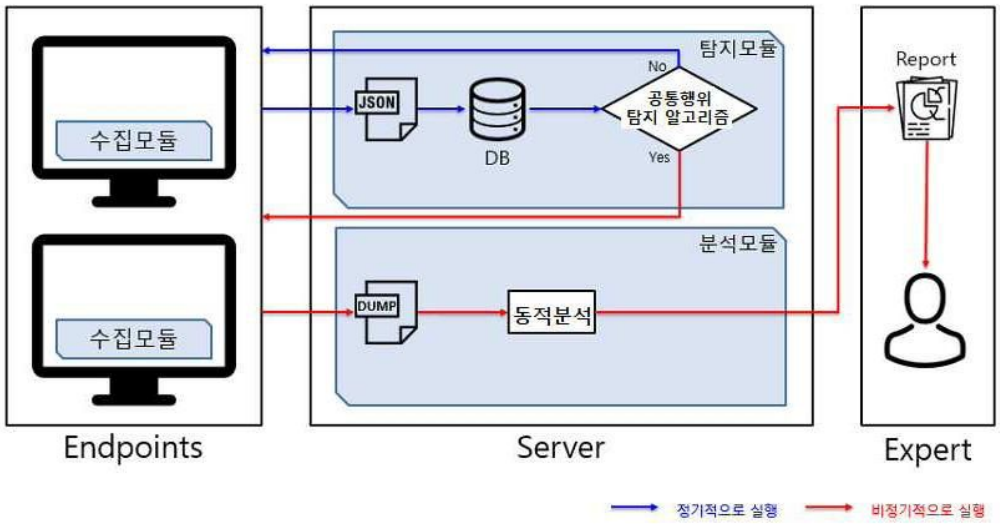
전체 청구항 수 : 총 3 항

(54) 발명의 명칭 **악성코드 감지시스템 및 감지방법**

(57) 요 약

본 발명에 의한 악성코드 감지시스템은, 다수의 엔드포인트; 각 엔드포인트에 설치되는 수집모듈; 탐지모듈; 분석모듈;을 포함하고, 상기 수집모듈은 정기적으로 각 엔드포인트의 네트워크 접속기록을 추출하여 탐지모듈로 전송하고, 탐지모듈로부터 전달받은 악성코드 후보 리스트에 있는 공통 행위와 관련된 프로세스의 정보를 통해 엔드포인트로부터 프로세스를 실행파일 형태로 추출하여 분석모듈로 전송하고, 상기 탐지모듈은 수집모듈로부터 받은 파일을 전처리한 후, 각 엔드 포인트의 공통행위를 탐지하여 악성코드 후보 리스트를 만든 후 악성코드 후보 리스트에 있는 공통 행위와 관련된 프로세스의 정보를 수집모듈로 전달하고, 상기 분석모듈은 전달받은 실행파일을 이용하여 동적 분석 진행 및 결과 리포트 생성하는 것을 특징으로 한다.

대 표 도



(72) 발명자

염철민

대전광역시 유성구 지족북로 33, 107동 1303호

연성화

대전광역시 유성구 농대로21번길 18, 201호

박종상

충청남도 아산시 음봉면 신휴길 157

이 발명을 지원한 국가연구개발사업

과제고유번호	2015-0-00930
부처명	과학기술정보통신부
연구관리전문기관	정보통신기술진흥센터
연구사업명	SW전문인력양성/정보통신창의인재양성
연구과제명	2018년 SW중심대학 지원사업_충남대
기 여 율	1/1
주관기관	충남대학교 산학협력단
연구기간	2018.01.01 ~ 2018.12.31

명 세 서

청구범위

청구항 1

다수의 엔드포인트;

각 엔드포인트에 설치되는 수집모듈;

탐지모듈;

분석모듈;

을 포함하고,

상기 수집모듈은 정기적으로 각 엔드포인트의 네트워크 접속기록을 추출하여 탐지모듈로 전송하고, 탐지모듈로부터 전달받은 악성코드 후보 리스트에 있는 공통 행위와 관련된 프로세스의 정보를 통해 엔드포인트로부터 프로세스를 실행파일 형태로 추출하여 분석모듈로 전송하고,

상기 탐지모듈은 수집모듈로부터 받은 파일을 전처리한 후, 각 엔드 포인트의 공통행위를 탐지하여 악성코드 후보 리스트를 만든 후 악성코드 후보 리스트에 있는 공통 행위와 관련된 프로세스의 정보를 수집모듈로 전달하고,

상기 분석모듈은 전달받은 실행파일을 이용하여 동적 분석 진행 및 결과 리포트 생성하는 것을 특징으로 하는 악성코드 감지시스템.

청구항 2

청구항 1에 있어서,

상기 탐지모듈은 탐지된 공통행위 중 화이트 리스트에 있는 공통행위는 악성코드 후보 리스트에서 제외하는 것을 특징으로 하는 악성코드 감지시스템.

청구항 3

다수의 엔드포인트, 각 엔드포인트에 설치되는 수집모듈, 탐지모듈, 분석모듈을 포함하는 악성코드 감지시스템을 이용한 악성코드 감지방법으로서,

상기 수집모듈이 정기적으로 각 엔드포인트의 네트워크 접속기록을 추출하여 탐지모듈로 전송하는 제1 단계;

상기 탐지모듈이 수집모듈로부터 받은 파일을 전처리한 후, 각 엔드 포인트의 공통행위를 탐지하여 악성코드 후보 리스트를 만든 후 악성코드 후보 리스트에 있는 공통 행위와 관련된 프로세스의 정보를 수집모듈로 전달하는 제2 단계;

상기 수집모듈이 탐지모듈로부터 전달받은 악성코드 후보 리스트에 있는 공통 행위와 관련된 프로세스의 정보를 통해 엔드포인트로부터 프로세스를 실행파일 형태로 추출하여 분석모듈로 전송하는 제3단계;

상기 분석모듈이 전달받은 실행파일을 이용하여 동적 분석 진행 및 결과 리포트 생성하는 제4 단계:를 포함하는 것을 특징으로 하는 악성코드 감지방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 악성코드 감지시스템 및 감지방법에 관한 것으로, 보다 상세하게는 엔드포인트의 접속기록을 추출하여 악성코드를 감지하는 악성코드 감지시스템 및 감지방법에 관한 것이다.

배 경 기 술

[0002] 최근 악성코드는 불특정 다수를 대상으로 무차별적으로 대량 배포하는 기존의 전략과 달리 특정 목표에 최적화하고 점점 더 지능적으로 진화하고 있다. 또한 악성코드의 목적이 해커 본인의 기량 과시가 아닌 금전적 이득으로 변화되고 있다.

[0003] 이에 따라 기업, 기관에 대한 공격이 증가하고 있는 추세이며 2016년 대기업 전산망 해킹 사건, 2017년 국내 웹호스팅 업체의 랜섬웨어 감염 사건, 2018년 가상화폐 거래소 해킹 사건 등 매년 관련 사고가 발생하고 있다.

[0004] 대표적으로 2016년 대기업 전산망 해킹 사고에 사용된 악성코드는 GhOst RAT이라는 악성코드로 대상 PC를 감염시킨 후 공격자의 C&C 서버와 통신을 하여 키로깅, 원격 제어, 추가 다운로드 기능 등을 제공한다.

[0005] 이러한 악성코드를 감지하기 위해 다양한 연구가 진행되고 있고, 비특허문헌 1은 그 예이다.

[0006] 또한 이러한 공격은 제로 데이 취약점을 이용하거나 변종 악성코드를 사용하는 경우가 많기 때문에 시그니처 기반 탐지 기법으로는 탐지에 한계가 있다.

선행기술문헌

비특허문헌

[0008] (비특허문헌 0001) Choi Bo Min, Kang Hong Koo, Lee Tae Jin. "A Study on the Method Variants Prediction using Malware API Information"

발명의 내용

해결하려는 과제

[0009] 본 발명이 해결하고자는 하는 과제는, 악성코드를 좀 더 효과적으로 감지하는 악성코드 감지시스템 및 감지방법을 제공하는 것이다.

과제의 해결 수단

[0011] 본 발명에 의한 악성코드 감지시스템은, 다수의 엔드포인트; 각 엔드포인트에 설치되는 수집모듈; 탐지모듈; 분석모듈;을 포함하고, 상기 수집모듈은 정기적으로 각 엔드포인트의 네트워크 접속기록을 추출하여 탐지모듈로 전송하고, 탐지모듈로부터 전달받은 악성코드 후보 리스트에 있는 공통 행위와 관련된 프로세스의 정보를 통해 엔드포인트로부터 프로세스를 실행파일 형태로 추출하여 분석모듈로 전송하고, 상기 탐지모듈은 수집모듈로부터 받은 파일을 전처리한 후, 각 엔드 포인트의 공통행위를 탐지하여 악성코드 후보 리스트를 만든 후 악성코드 후보 리스트에 있는 공통 행위와 관련된 프로세스의 정보를 수집모듈로 전달하고, 상기 분석모듈은 전달받은 실행파일을 이용하여 동적 분석 진행 및 결과 리포트 생성하는 것을 특징으로 한다.

[0012] 상기 탐지모듈은 탐지된 공통행위 중 화이트 리스트에 있는 공통행위는 악성코드 후보 리스트에서 제외할 수 있다.

[0013] 본 발명에 의한 악성코드 감지방법은, 다수의 엔드포인트, 각 엔드포인트에 설치되는 수집모듈, 탐지모듈, 분석모듈을 포함하는 악성코드 감지시스템을 이용한 악성코드 감지방법으로서, 상기 수집모듈이 정기적으로 각 엔드포인트의 네트워크 접속기록을 추출하여 탐지모듈로 전송하는 제1 단계; 상기 탐지모듈이 수집모듈로부터 받은 파일을 전처리한 후, 각 엔드 포인트의 공통행위를 탐지하여 악성코드 후보 리스트를 만든 후 악성코드 후보 리스트에 있는 공통 행위와 관련된 프로세스의 정보를 수집모듈로 전달하는 제2 단계; 상기 수집모듈이 탐지모듈로부터 전달받은 악성코드 후보 리스트에 있는 공통 행위와 관련된 프로세스의 정보를 통해 엔드포인트로부터 프로세스를 실행파일 형태로 추출하여 분석모듈로 전송하는 제3단계; 상기 분석모듈이 전달받은 실행파일을 이용하여 동적 분석 진행 및 결과 리포트 생성하는 제4 단계:를 포함하는 것을 특징으로 한다.

발명의 효과

[0015] 본 발명에 의한 악성코드 감지시스템 및 감지방법은, 종래의 악성코드 감지시스템 및 감지방법보다 보다 효과적으로 악성코드를 감지한다.

도면의 간단한 설명

[0017] 도 1은 GRR의 구조도

도 2는 공통 행위 탐지 시스템의 개념도

도 3은 탐지모듈의 탐지 동작 순서도

도 4는 실시예 1의 헌트 수행 화면

도 5는 실시예 1에서의 화이트리스트 적용 전 결과 화면

도 6은 실시예 1에서의 화이트리스트 적용 후 결과 화면

발명을 실시하기 위한 구체적인 내용

[0018] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세하게 설명하고자 한다. 그러나 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변환, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 본 발명을 설명함에 있어서 관련된 공지 기술에 대한 구체적인 설명이 본 발명의 요지를 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다.

[0019] 본 출원에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다.

[0021] 본 발명은 Google Rapid Response(이하 GRR)라는 오픈 소스 프레임워크를 통해 기업, 기관 환경 등에서 각 엔드포인트의 네트워크 접속 기록을 이용하여 공통적인 행위를 탐지할 수 있도록 한다.

[0022] GRR 은 Google에서 개발한 침해사고 대응 원격 포렌식 도구로 다수의 PC에서 동시에 아티팩트를 수집하는 기능을 제공한다.

[0023] 도 1은 GRR의 구조도이다.

[0024] GRR은 크게 클라이언트(Client), 프론트엔드(Frontend Server) 서버, 워커(Worker), AFF4 서브시스템(AFF4 Subsystem), 데이터 스토어(Data Store)로 구성되어 있다. 클라이언트는 HTTP 프로토콜을 이용하여 프론트엔드 서버와 메시지를 교환한다. 프론트엔드 서버는 AFF4 서브시스템과 통신하여 데이터를 데이터 스토어에 저장한다. 워커는 데이터를 분석하거나 클라이언트에게 새로운 작업을 부여하기 위하여 AFF4 서브시스템과 통신한다.

[0025] 워커가 단일 클라이언트로부터 아티팩트를 수집하는 수집하는 작업을 플로우라고 한다. 워커가 수집하고자 하는 아티팩트를 선택하여 실행 명령을 내리면 명령은 클라이언트에게 전달되고, 클라이언트는 해당하는 아티팩트를 추출하여 HTTP 프로토콜을 통해 프론트엔드 서버에 전송한다. 프론트엔드 서버는 수집한 아티팩트를 데이터스토어에 저장하고 워커는 데이터 스토어에서 아티팩트를 얻을 수 있다.

[0026] 플로우는 단일 클라이언트로부터 아티팩트를 수집할 수 있는데, 플로우를 프론트엔드 서버와 연결된 모든 클라이언트에게 전송하여 그들로부터 아티팩트를 동시에 수집하는 기능을 헌트라고 한다.

[0027] 악성코드는 스팸 메일, 웹 방문 등 네트워크 활동을 통해 유포되는 경우가 많으며 대상 PC를 감염 시킨 후에 공격자의 C&C 서버와 통신하여 명령 및 제어를 받는 경우가 많다. 감염된 PC들의 네트워크 활동 기록을 조사하면 악성코드의 유포 경로나 공격자의 C&C 서버와의 통신 기록이 공통적으로 나타날 수 있다. 만약 다수의 PC가 같은 망에 존재하는 기업 환경에 위와 같은 악성코드를 이용한 공격이 시도되었다면 감염된PC들에서 악성코드 유

포지 또는 공격자의 C&C 서버와의 공통적인 네트워크 통신이 감지될 것이다. 이는 공격을 탐지하고 빠른 대응을 위한 중요한 단서가 될 수 있다.

[0028] 따라서 본 발명에서는 GRR을 통해 다수의 엔드포인트로부터 네트워크 접속 기록을 수집한 후 그들의 공통점을 탐지하여 해당 정보를 보안 전문가에게 제공하도록 한다.

[0030] 도 2는 공통 행위 탐지 시스템의 개념도이다.

[0031] 본 발명의 악성코드 감지시스템은 각 엔드포인트로부터 네트워크 접속 기록을 수집하는 수집 모듈과 데이터 전처리 후 알고리즘을 통해 공통 행위를 탐지하는 탐지 모듈을 포함된다. 탐지 모듈은 탐지된 공통 네트워크 행위의 주체 프로세스의 정보를 보안 전문가에게 제공하여 적절한 조치를 취할 수 있도록 한다.

[0033] 수집 모듈은 각 엔드포인트에 설치되며 정기적으로 각 엔드포인트 네트워크 접속 기록을 추출하여 서버로 전송하는 역할을 한다. 다수의 엔드포인트로부터 동시에 네트워크 접속 기록을 수집하기 위해서 GRR의 헌트 기능을 사용한다. 수집 모듈의 결과물은 모든 엔드포인트의 네트워크 접속 기록 데이터를 가진JSON 파일이며, 이를 탐지 모듈로 전송한다.

[0035] 도 3은 탐지모듈의 탐지 동작 순서도이다.

[0036] 탐지 모듈은 데이터 전처리 과정과 알고리즘을 통한 탐지 과정으로 나눌 수 있다. 데이터 전처리 과정은 수집 모듈로부터 받은 JSON 파일을 파싱하여 데이터베이스에 저장하는 과정이다. 수집 모듈로부터 받은 JSON 파일은 각 엔드포인트 별로 네트워크와 관련된 여러 가지 데이터를 포함하고 있다. 그 중 값이 존재하지 않거나 공통 행위 탐지에 도움이 되지 않는 데이터들이 많이 존재한다. 전처리 과정은 이와 같은 데이터들을 제거하고 공통 행위 탐지에 도움이 되는 데이터들을 선정하여 데이터베이스에 보관한다. 데이터베이스에 저장되는 데이터는 전송 받은 클라이언트의 ID, 네트워크 행위를 하는 프로세스의 이름, Local IP, Local Port, Remote IP, Remote Port이다.

[0037] 데이터 전처리가 완료되면 데이터베이스에 저장된 데이터들을 이용하여 공통 행위를 탐지한다. 공통 행위는 전체 50% 이상의 엔드포인트에서 같은 IP에 접속 기록이 존재하거나 또는 같은 Port로 통신을 하는 것으로 정의한다. 이 조건에 맞는 공통 행위 중 발견된 엔드포인트의 수에 따라 비중을 다르게 두어 우선순위를 둔다.

[0038] 탐지된 공통 행위의 주체 프로세스에는 각 엔드포인트가 실행한 프로세스와 시스템 프로세스가 모두 존재한다. 시스템 프로세스의 경우 시스템을 구성하는 데 필수적이고 안전성이 검증되었기 때문에 모든 탐지 결과에 포함될 수밖에 없다. 안전성이 검증된 시스템 프로세스 같은 경우에는 탐지 대상에서 제외하는 것이 속도 향상 및 부하를 줄일 수 있는 방법이다. 이를 위해 관리자는 보고받은 공통 행위 중 시스템 프로세스를 구별하여 화이트리스트를 구성하고 이를 탐지 대상에 적용하는 과정이 필요하다.

[0039] 공통 행위가 탐지되면 수집 모듈은 해당 행위의 주체 프로세스를 엔드포인트로부터 추출하여 분석 모듈로 전송한다. 분석 모듈에선 해당 프로세스의 덤프 파일을 분석하고 리포트를 작성하여 전문가에게 제공함으로써 악성여부 판단을 돕는다. 덤프파일은 오픈소스인 Cuckoo Sandbox를 이용하여 분리된 가상 환경에서 동적 분석을 진행한 후 결과 리포트를 출력한다. 즉, 공통 행위를 일으킨 프로세스를 덤프한 후 동적 분석을 통해 악성여부 판단을 돕는다.

[0040]

[0041] (실시예 1)

[0042] 실시예 1에서는, 공통 행위 탐지 실험을 위해 4대의 엔드포인트를 이용한 실험 환경을 구성하였다. 각 엔드포인트는 1대의 리얼 머신과 3대의 가상 머신이며 운영체제는 모두 Windows10으로 설정하였고 각 엔드포인트마다 수집모듈을 설치하였다. 또한 엔드포인트들과 연결된 Ubuntu서버를 구축하고 탐지 모듈을 설치하였다.

[0043] 우선 공통 행위를 확인하기 위해 인위적으로 각 엔드포인트에서 공통적으로 프로그램을 실행 시킨다. 실행하는 프로그램은 다운로드 폴더 내에 존재하는 파일을 특정 서버로 전송하는 client.exe, 원격 제어를 지원하는 TeamViewer.exe, 웹 브라우저인 Chrome.exe이다. client.exe는 실험을 위해 임의로 제작한 프로그램이다.

[0044] 각 엔드포인트에서 프로그램을 실행하고 나면 수집 모듈을 가동시킨다. 수집 모듈은 헌트를 실행하여 각 엔드포인트로부터 네트워크 접속 기록을 추출한다. 수집 주기는 60분으로 설정하였다.

[0045] 수집이 완료되면 데이터는 탐지 모듈로 전송되어 데이터베이스에 저장되고 이 데이터를 알고리즘에 입력하여 실행한 프로그램들이 공통 행위로 탐지되는지를 확인해 보았다. (예를 들어, 모든 엔드포인트에서 Chrome 브라우저를 통해 구글 웹사이트에 접속한 것이 발견되면, 공통행위로 탐지될 수 있다)

[0047] 도 4는 실시예 1의 헌트 수행 화면이다.

[0048] 도 4는 수집 모듈에서 주기적으로 헌트를 실행하여 각 엔드포인트로부터 네트워크 접속 기록을 수집하는 화면이다. 60분을 주기로 헌트를 실행하고 데이터를 다운로드하여 데이터베이스에 저장하는 것을 확인할 수 있다.

[0050] 도 5는 실시예 1에서의 화이트리스트 적용 전 결과 화면이다.

[0051] 도 5의 결과 화면은 각각 프로세스의 이름, 접속하는 IP주소, 통신에 사용하는 Port번호와 해당 행위를 하는 클라이언트의 수를 출력해주고 있다.

[0052] 결과를 보면 각종 시스템 프로그램이 탐지된 모습을 볼 수 있다. 안전성이 검증된 시스템 프로그램의 경우 보안 전문가에게 보고 시 시간적 자원 낭비가 될 수 있다. 따라서 보안 전문가는 최초의 시스템 프로그램 탐지 시 안전성을 검증한 후 화이트리스트에 해당 프로그램을 추가하여 분석 과정에 시간을 절약 할 수 있다. 하지만 화이트리스트는 공통 행위 탐지 시스템의 정확도를 떨어뜨리는 수 있는 요소이므로 신중히 운용할 필요가 있다.

[0053] 도 6은 실시예 1에서의 화이트리스트 적용 후 결과 화면이다.

[0054] 시스템 프로세스가 화이트리스트를 통해 필터링 되고 사용자가 실행한 일반 프로세스들의 공통 행위가 탐지되는 것을 확인할 수 있다.

[0055] 즉, 상기 탐지모듈은 수집모듈로부터 받은 파일을 전처리한 후, 각 엔드 포인트의 공통행위를 탐지하여 악성코드 후보 리스트(또는 '악성코드 행위 후보 리스트'라고 할 수도 있다)를 만들고, 악성코드 후보 리스트에 있는 공통 행위와 관련된 프로세스의 정보를 수집모듈로 전달한다.(예를 들어, 탐지 모듈은 수집모듈에 Chrome 프로세스에 대한 덤프파일을 전송할 수 있다.)

[0056] 그 후에 수집 모듈은 전달받은 프로세스의 정보를 통해 엔드포인트로부터 프로세스를 실행 파일 형태로 추출하여 분석 모듈로 전달한다.(예를 들어, 수집 모듈은 엔드포인트로부터 Chrome.exe 파일을 추출하여 분석 모듈로 전달한다.)

[0057] 그 후에 분석 모듈은 전달받은 실행파일을 이용하여 Cuckoo Sandbox를 통해 동적 분석 진행 및 결과 리포트를 생성하고 전문가에게 전달할 수 있다.(예를 들어, 분석 모듈은 Chrome.exe의 동적 분석을 할 수 있다.)

[0058] 보안 전문가는 전달된 동적 분석 진행 및 결과 리포트를 보고 이 프로세스들의 행위의 악성 여부를 판단하여 차단 여부를 결정한다.

[0060] 탐지 모듈에서 사용하는 데이터는, 수집모듈로부터 받은 네트워크 접속 기록, 실행중인 프로세스 목록 등이다.

[0061] 분석 모듈에서 사용하는 데이터는, 수집모듈로부터 받은 실행 파일(덤프 파일)이다.

[0062] 행위의 주체 프로세스는, 탐지된 공통 행위를 일으킨 프로세스이다. 예들 들어,모든 엔드포인트에서 Chrome 브라우저를 통해 같은 웹사이트에 접속하였다면 해당 웹사이트로의 네트워크 연결의 주체 프로세스는 Chrome이 된다.

[0063] 덤프파일은 엔드포인트로부터 파일을 추출한 것을 의미한다.

[0065] 본 발명은 오픈소스인 GRR을 활용하여 다수의 PC로부터 네트워크 접속 기록을 수집한다. 수집한 데이터는 전처리를 통해 데이터베이스에 저장하고 알고리즘을 통해 공통점을 찾아 전문가에게 보고한다.

[0066] 본 발명은 기업, 기관 등 다수의 엔드포인트를 감염시키고 C&C 서버를 이용하여 엔드포인트들을 조종하는 공격에 대해 감염된 엔드포인트들이 공격자의 C&C 서버와 통신하는 과정을 탐지하므로 빠른 탐지가 가능하다.

[0068] 따라서 본 발명에 의한 악성코드 감지시스템은 다수의 엔드포인트, 각 엔드포인트에 설치되는 수집모듈, 탐지모듈을 포함한다.

[0069] 상기 수집모듈은 정기적으로 각 엔드포인트의 네트워크 접속기록을 추출하여 탐지모듈로 전송한다.

[0070] 상기 탐지모듈은 수집모듈로부터 받은 파일을 전처리한 후, 각 엔드 포인트의 공통행위를 탐지하여 악성코드 후보 리스트로 저장해둔다.

[0071] 상기 탐지모듈은 탐지된 공통행위 중 화이트 리스트에 있는 공통행위는 악성코드 후보 리스트에서 제외할 수 있다.

[0073] 본 발명에 의한 악성코드 감지방법은 다음의 2단계를 포함한다.

[0074] (1) 제1 단계: 상기 수집모듈이 정기적으로 각 엔드포인트의 네트워크 접속기록을 추출하여 탐지모듈로 전송하는 단계

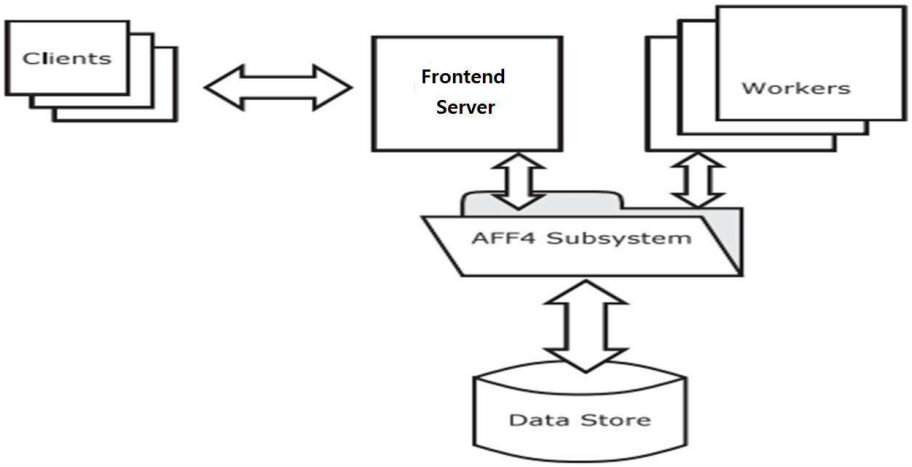
[0075] (2) 제2 단계: 상기 탐지모듈이, 수집모듈로부터 받은 파일을 전처리한 후, 각 엔드 포인트의 공통행위를 탐지하여 악성코드 후보 리스트를 만든 후 악성코드 후보 리스트에 있는 공통 행위와 관련된 프로세스의 정보를 수집모듈로 전달하는 단계

[0076] (3) 제3 단계: 상기 수집모듈이, 탐지모듈로부터 전달받은 악성코드 후보 리스트에 있는 공통 행위와 관련된 프로세스의 정보를 통해 엔드포인트로부터 프로세스를 실행파일 형태로 추출하여 분석모듈로 전송하는 단계

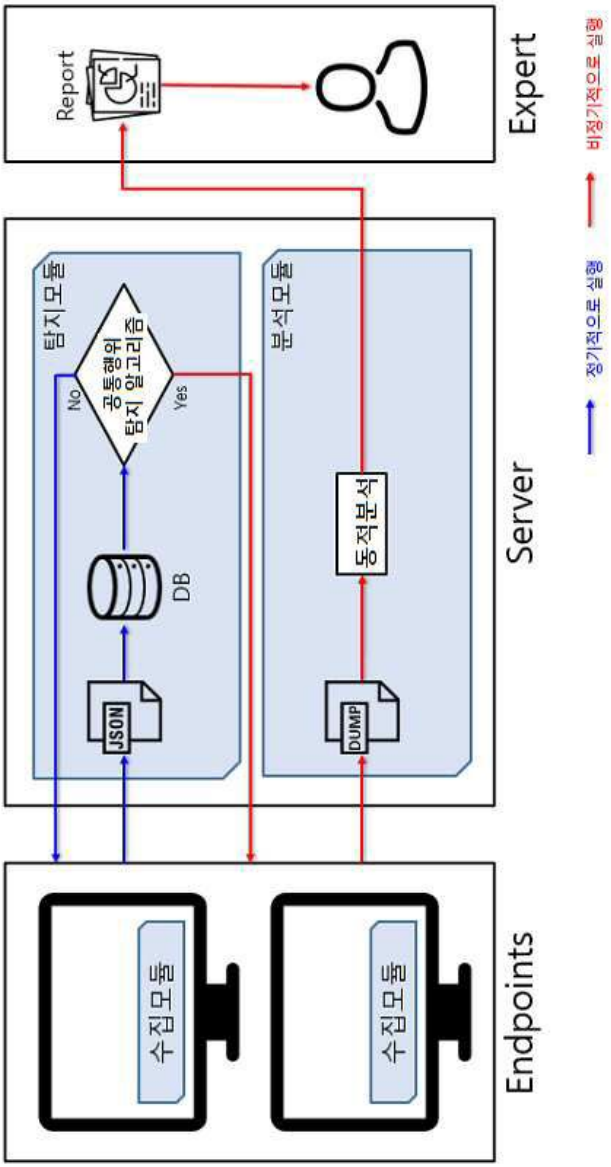
[0077] (4) 제4 단계: 상기 분석모듈이 전달받은 실행파일을 이용하여 동적 분석 진행 및 결과 리포트 생성하는 단계

도면

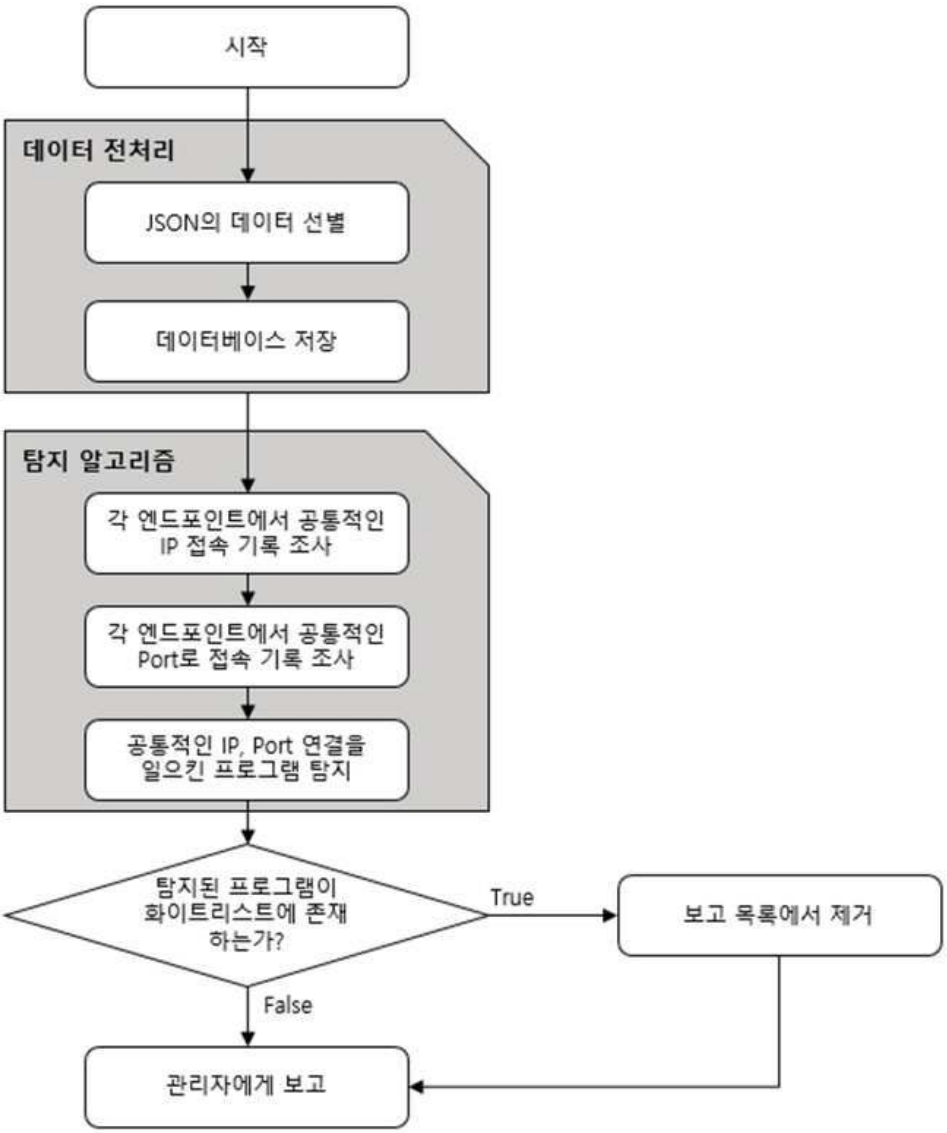
도면1



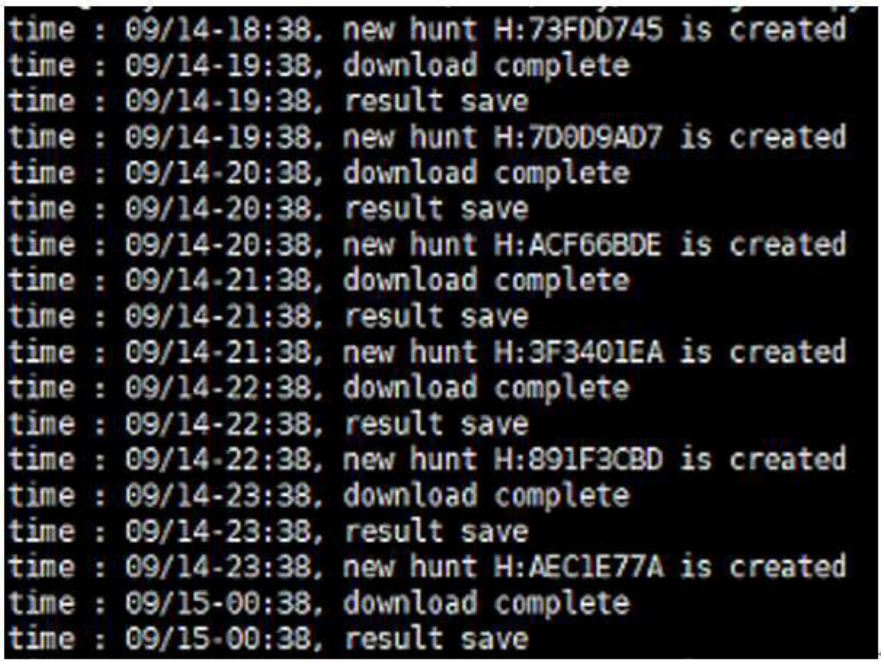
도면2


Expert
Report
Server
탐지 모듈
No
공통행위
탐지 알고리즘
Yes
DB
JSON
분석모듈
동적분석
DUMP
Endpoints
수집모듈
수집모듈
비정기적으로 실행
정기적으로 실행

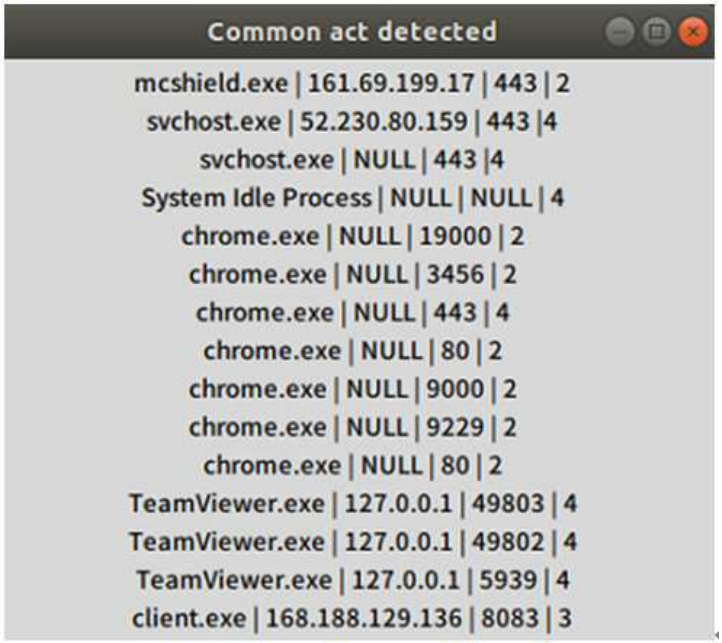
도면3


시작
데이터 전처리
JSON의 데이터 선별
데이터베이스 저장
탐지 알고리즘
각 엔드포인트에서 공통적인 IP 접속 기록 조사
각 엔드포인트에서 공통적인 Port로 접속 기록 조사
공통적인 IP, Port 연결을 일으킨 프로그램 탐지
탐지된 프로그램이 화이트리스트에 존재하는가?
True
보고 목록에서 제거
False
관리자에게 보고

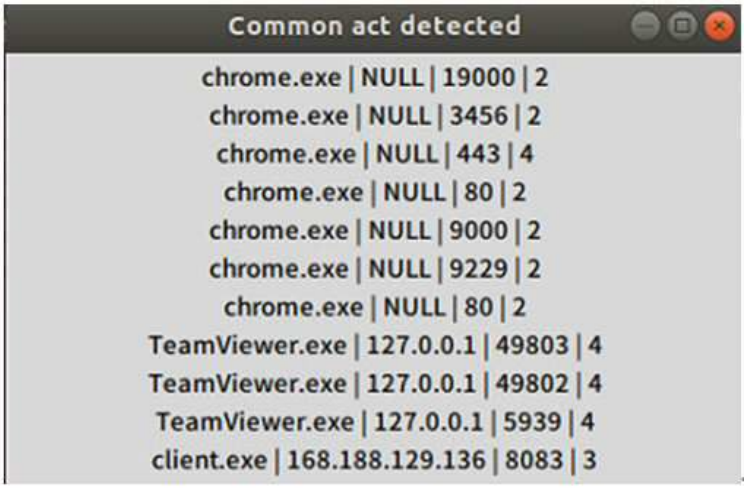
도면4


time : 09/14-18:38, new hunt H:73FDD745 is created
time : 09/14-19:38, download complete
time : 09/14-19:38, result save
time : 09/14-19:38, new hunt H:7D0D9AD7 is created
time : 09/14-20:38, download complete
time : 09/14-20:38, result save
time : 09/14-20:38, new hunt H:ACF66BDE is created
time : 09/14-21:38, download complete
time : 09/14-21:38, result save
time : 09/14-21:38, new hunt H:3F3401EA is created
time : 09/14-22:38, download complete
time : 09/14-22:38, result save
time : 09/14-22:38, new hunt H:891F3CBD is created
time : 09/14-23:38, download complete
time : 09/14-23:38, result save
time : 09/14-23:38, new hunt H:AEC1E77A is created
time : 09/15-00:38, download complete
time : 09/15-00:38, result save

도면5


Common act detected
mcshield.exe | 161.69.199.17 | 443 | 2
svchost.exe | 52.230.80.159 | 443 |4
svchost.exe | NULL | 443 |4
System Idle Process | NULL | NULL | 4
chrome.exe | NULL | 19000 | 2
chrome.exe | NULL | 3456 | 2
chrome.exe | NULL | 443 | 4
chrome.exe | NULL | 80 | 2
chrome.exe | NULL | 9000 | 2
chrome.exe | NULL | 9229 | 2
chrome.exe | NULL | 80 | 2
TeamViewer.exe | 127.0.0.1 | 49803 | 4
TeamViewer.exe | 127.0.0.1 | 49802 | 4
TeamViewer.exe | 127.0.0.1 | 5939 | 4
client.exe | 168.188.129.136 | 8083 | 3

도면6


Common act detected
chrome.exe | NULL | 19000 | 2
chrome.exe | NULL | 3456 | 2
chrome.exe | NULL | 443 | 4
chrome.exe | NULL | 80 | 2
chrome.exe | NULL | 9000 | 2
chrome.exe | NULL | 9229 | 2
chrome.exe | NULL | 80 | 2
TeamViewer.exe | 127.0.0.1 | 49803 | 4
TeamViewer.exe | 127.0.0.1 | 49802 | 4
TeamViewer.exe | 127.0.0.1 | 5939 | 4
client.exe | 168.188.129.136 | 8083 | 3