(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2015년05월12일
(11) 등록번호 10-1518233
(24) 등록일자 2015년04월30일

(51) 국제특허분류(Int. Cl.)
H04L 12/22 (2006.01) *H04L 12/24* (2006.01)
H04L 12/26 (2006.01)
(21) 출원번호 10-2014-0038101
(22) 출원일자 2014년03월31일
심사청구일자 2014년03월31일
(56) 선행기술조사문헌
KR1020120006250 A*
KR1020080040921 A*
KR1020090052596 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
순천향대학교 산학협력단
충청남도 아산시 신창면 순천향로 22, 순천향대학교내
(72) 발명자
곽진
충남 천안시 서북구 한들3로 100, 101동 1401호 (백석동, 백석마을아이파크)
서진원
서울특별시 송파구 석촌호수로 169 잠실레이크펠리스아파트 111동 1404호
(74) 대리인
추혁, 박종경, 원성수

전체 청구항 수 : 총 3 항 심사관 : 석상문

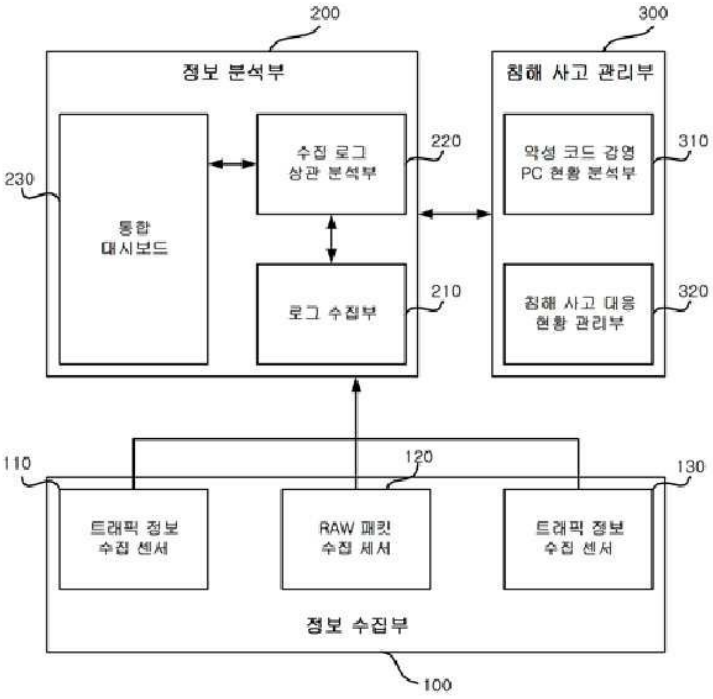
(54) 발명의 명칭 **기업 내부 전산환경의 위협탐지를 위한 보안 장치**

(57) 요 약

본 발명은 기업 내부 전산환경의 위협탐지를 위한 보안 아키텍처에 관한 것으로서, 네트워크에 흐르는 모든 트래픽에 대한 정보를 수집하는 트래픽 정보 수집 센서와, 상기 네트워크에서 전송되는 모든 트래픽을 패킷 형태로 저장하는 RAW 패킷 수집 센서와, 네트워크 패킷에서 실행파일 내역을 재조합하여 분석하는 실행파일 분석기를 포

(뒷면에 계속)

대 표 도 - 도1



함하는 정보 수집부; 상기 정보 수집부에서 수집되는 모든 로그를 통합하여 저장하는 로그 수집부와, 상기 로그 수집부에서 수집된 로그들 간의 연관성을 분석하는 로그 상관 분석기와, 상기 로그 상관 분석기에서 분석된 네트워크의 현재 상황을 보안 담당자에게 제공하는 통합 대시보드를 포함하는 정보 분석부; 및 기업 내부망의 악성 코드 감염 현황을 파악하는 악성 코드 감염 PC 현황 분석부와, 침해 사고에 대한 시작부터 종료까지의 대응 현황을 저장하는 침해 사고 대응 현황 관리부를 포함하는 침해 사고 관리부를 포함하여, 프로토콜 분석기를 이용하여 내부에서 외부로 향하는 모든 통신을 분석하고, 기업 내부망으로 유입되는 제로데이형 악성 코드를 탐지하기 위해 통신에서 모든 실행파일을 수집하여 행위 분석 기반의 분석을 실시함으로써, 특정 프로토콜에 종속적인 탐지, 특성 서비스에 종속적인 탐지, 우회가 손쉬운 시그니처 기반의 탐지, 네트워크 인프라에 대한 이상 징후 탐지 및 서비스망에 특화된 탐지 등 종래 기술이 지녔던 한계를 개선할 수 있다.

이 발명을 지원한 국가연구개발사업

과제고유번호	NRF-2012R1A2A2A01010886
부처명	미래창조과학부
연구관리전문기관	한국연구재단
연구사업명	중견연구자지원사업 핵심연구
연구과제명	유무선 통합 환경에서의 안전한 클라우드 데이터센터 구축을 위한 지능형보안관제 기술 개발
기 여 율	1/1
주관기관	순천향대학교 산학협력단
연구기간	2012.05.01 ~ 2015.04.30

명 세 서

청구범위

청구항 1

네트워크에 흐르는 모든 트래픽에 대한 정보를 수집하는 트래픽 정보 수집 센서와, 상기 네트워크에서 전송되는 모든 트래픽을 패킷 형태로 저장하는 RAW 패킷 수집 센서와, 네트워크 패킷에서 실행파일 내역을 재조합하여 분석하는 실행파일 분석기를 포함하는 정보 수집부;

상기 정보 수집부에서 수집되는 모든 로그를 통합하여 저장하는 로그 수집부와, 상기 로그 수집부에서 수집된 로그들 간의 연관성을 분석하는 로그 상관 분석기와, 상기 로그 상관 분석기에서 분석된 네트워크의 현재 상황을 보안 담당자에게 제공하는 통합 대시보드를 포함하는 정보 분석부; 및

기업 내부망의 악성 코드 감염 현황을 파악하는 악성 코드 감염 PC 현황 분석부와, 침해 사고에 대한 시작부터 종료까지의 대응 현황을 저장하는 침해 사고 대응 현황 관리부를 포함하는 침해 사고 관리부를 포함하며,

상기 실행파일 분석기는,

상기 네트워크에서 실행파일의 내역이 존재하는 패킷들을 재조합하여 실행파일을 추출하는 기능과 상기 실행파일을 가상 환경에서 분석하는 행위 기반 분석 기능을 보유하는, 기업 내부 전산환경의 위협탐지를 위한 보안 장치.

청구항 2

청구항 제1항에 있어서,

상기 트래픽 정보 수집 센서는,

네트워크 트래픽에서 프로토콜별로 분류하여 정보를 수집하는 것을 특징으로 하는, 기업 내부 전산환경의 위협탐지를 위한 보안 장치.

청구항 3

삭제

청구항 4

청구항 제1항에 있어서,

상기 로그 상관 분석기는,

정보 수집 대상의 모든 정보 기기의 시간이 동일하고, IP의 정보가 동일한 조건 하에서 상기 로그들 간의 연관성을 분석하는 것을 특징으로 하는, 기업 내부 전산환경의 위협탐지를 위한 보안 장치.

발명의 설명

기 술 분 야

[0001] 본 발명은 보안 아키텍처에 관한 것으로, 더욱 상세하게는 최근 가장 심각한 문제로 떠오른 APT 공격을 탐지하고 대응할 수 있는 기업 내부 전산환경의 위협탐지를 위한 보안 아키텍처에 관한 것이다.

배 경 기 술

[0002] 인터넷 인프라의 급속한 발전과 인터넷 보급율의 확대에 따라 이제 인터넷은 더 이상 낯선 환경이 아니다. 한국인터넷진흥원이 제공하는 2012년 5월 개인 인터넷이용통계에 의하면 10대 99.9%, 20대 99.9%, 30대는 99.5%로 나타났다. 10대 미만의 이용률도 88.2%에 이르고 있어 앞으로 10년 후에는 우리나라의 인터넷 이용률은 인구대비 90%에 육박할 것이다.

[0003] 이렇듯 인터넷의 기하급수적인 증가는 순기능 이외에도 개인정보 유출, DDoS 공격, 해킹 사고 등의 부작용 및

역기능 역시 증가하고 있다. 가장 심각한 것은 사용자 PC의 보안을 위협하는 악성 프로그램이 갈수록 지능화, 다양화되고 있고, 악성 프로그램에 의한 피해는 나날이 커지고 있다.

[0004] 멀리는 2003년 1.25 인터넷 침해사고를 일으킨 Slammer Worm에서 2009년 7.7 DDoS, 2011년 3.4 DDoS 해킹사고는 모두 악성코드에 의해서 발생한 대형 해킹사고로 알려져 있다.

[0005] 하지만 불특정 다수를 대상으로 유포하는 악성코드 같은 경우 보안 관리자 또는 백신제작자에게 쉽게 탐지가 되어 공격자가 확보한 좀비PC들을 손쉽게 제거가 가능한 반면에, 특정 목표를 대상으로 유포되는 타켓형 악성코드의 경우 탐지가 불가능하여 기업 내부망의 커다란 위협으로 대두되었으며 최악의 경우 기업의 업무가 마비되는 상황이 발생할 수 있는 것이다.

[0006] 이미 국내에서도 이런 사례가 존재한다. 최근 3년 동안 발생한 가장 큰 해킹사고인 2011년 4월 농협금융의 금융서버 침해사고 사례를 보면 공격이 파괴형으로까지 변하였으며 당시 금융업무가 수 일 동안 멈춘 것을 돌이켜 보면 기업 내부망에 대한 위협이 얼마나 큰 파급효과를 가져오는지 알 수 있다.

[0007] 당시 검찰수사결과의 발표에 의하면 이 노트북은 2010. 9. 4. 경 좀비PC가 되었으며 범인들은 7개월 이상 노트북을 집중 관리하면서 필요한 정보를 획득한 뒤 원격조종으로 공격을 한 것임으로 언급하고 있다.

[0008] 이러한 경향을 보았을 때 공격자는 다수가 아닌 특정 공격 목표 대상 1개 사이트에 대한 공격을 수행하고 있으며, 이러한 성격을 가지고 있는 공격을 지능형 지속 공격(APT, Advanced Persistent Threat, 이하 APT)이라 칭하고 있다.

[0009] 그러나 APT라는 용어는 SQL Injection, XSS(Cross Site Script)와 같은 특정 공격기법을 지칭하는 것이 아니므로, 이러한 단어로서 공격자의 공격 기법과 공격 성격을 규정할 수는 없다. 하지만 APT라는 용어에 대해서 설명하는 문서를 살펴보면 Advanced는 진보된 공격 기법을 의미한다. 이 말은 자동화된 공격도구를 사용하는 것이 아닌 숙련된 전문가에 의한 수동 공격을 의미하는 것이며, Persistent라는 의미는 지속적인 공격을 의미하는 것이다. 즉, 오직 공격의 성공을 목표로 가지고 장시간을 소요하더라도 공격을 수행하는 것이다. 마지막으로 Threat은 말 그대로 앞서 언급한 두 단어의 성격을 포함하는 위협이라는 것이다.

[0010] 이렇게 고수준의 공격자에 의해서 실행되는 공격인 APT는 숙련된 보안 관리자 및 방어자가 부족한 국내 환경에서는 방어가 쉽지 않다고 볼 수 있다. 또한 공격자들이 공격을 수행하는데 사용하는 가장 보편적인 방법은 악성코드를 기업 내부망에 유포하는 것이다.

[0011] 공격자 역시 공격 성공률을 높이기 위해서 백신에 탐지되지 않는 악성코드를 기업 내부망에 침투시키기 위해서 노력하고 있다. 이러한 악성코드는 수많은 제로데이(Zero-Day) 공격을 발생시키며 보안 관리자의 대응을 매우 어렵게 한다.

[0012] 아쉽게도 국내 기업이 운영 중인 대부분의 보안장비는 인터넷에서 내부 기업으로 유입되는 유해 트래픽 및 허가되지 않은 접근을 차단하는데 효율적인 장비들이다. 하지만 기업 내부망에서 발생하는 제로데이형 악성코드 탐지 및 감염PC의 행위를 탐지하기에는 역부족인 것이 사실이므로 최근 발생하는 내부망 위협에 대한 새로운 탐지 및 대응 기법의 구축이 절실히 요구되고 있다.

[0013] 최근까지도 보안담당자들은 보안성을 강화하기 위해서 기존 보안장비인 침입차단시스템, 침입탐지시스템, PC백신, PC보안 등을 도입하여 보안 시스템을 구축하고 있다. 하지만 이러한 보안 장비들은 기업 내부망을 대상으로 발생하는 침해사고를 탐지하고 대응하기에는 다음과 같은 분명한 한계가 존재한다.

[0014] 안티 바이러스 제품은 악성코드 샘플이 수집되어야 탐지 패턴을 만들 수 있다. 이것은 숙주를 찾아서 병균을 분리하고 해당 백신을 만드는 것과 동일한 원리이다. 즉, 알려지지 않은 악성코드는 탐지가 불가능하다는 것이다. 따라서 이 문제는 안티 바이러스 제품 자체의 문제가 아니라 해당 제품이 동작하는 생명주기의 문제점으로 보아야 한다.

[0015] 그리고 대다수의 기업이 침입탐지시스템/침입방지시스템을 운영하고 있으나 이러한 제품은 단일 이벤트만을 탐지하는 제품이다. 즉, 탐지 패턴에 명시된 이상 징후를 탐지하는 것이다. 만일 공격자가 탐지 패턴에 없는 새로운 공격을 수행하여 침투를 수행하고, 이후 정상적인 접속을 가장하여 공격을 진행하는 경우 공격의 탐지가 불가능하다는 것이다. 침입탐지시스템/침입방지시스템의 가장 큰 문제는 초기 탐지가 실패하면 이후 연관된 탐지가 모두 실패한다는 점이다.

[0016] 침입차단시스템을 운영하는 경우 내부직원의 외부행 접속은 모두 허용하여 운영하는 것이 일반적이다. 이것은

내부와 외부를 경계선으로 구분하고 해당 경계선의 유일한 통로를 통제하는 전통적인 보안 모델에 기인하는 것이다. 즉 인터넷으로 통칭되는 외부망을 위협의 근원으로 판단하고, 자사 직원인 기업 내부 직원들을 신뢰하기 때문에 외부로 향하는 접속을 100% 신뢰한다는 가정 사항에서 출발하는 보안모델인 것이다. 만일 이러한 가정 사항이 무너지는 경우 해당 보안모델 자체의 신뢰성이 무너질 수 있을 수 있다는 것이다.

[0017] 이렇듯 전통적인 보안장비들의 운영에서는 탐지가 어려운 내부망 보안 위협을 대응하기 위해서는 새로운 보안 모델이 필요하고 이에 적합한 내부망 위협 탐지용 보안 아키텍처가 필요한 것이다.

선행기술문헌

특허문헌

[0018] (특허문헌 0001) 대한민국 공개특허공보 제10-2010-0075480호(공개일 2010.07.02.)

발명의 내용

해결하려는 과제

[0019] 따라서, 본 발명은 상기한 종래 기술의 문제점을 해결하기 위해 이루어진 것으로서, 본 발명의 목적은 전통적인 보안 아키텍처에서 탐지가 어려운 기업 내부 업무망 대상 해킹 공격을 탐지하고 대응하기 위한 새로운 보안 아키텍처를 제공하는데 있다.

과제의 해결 수단

[0020] 상기와 같은 목적을 달성하기 위한 본 발명의 기업 내부 전산환경의 위협탐지를 위한 보안 아키텍처는, 네트워크에 흐르는 모든 트래픽에 대한 정보를 수집하는 트래픽 정보 수집 센서와, 상기 네트워크에서 전송되는 모든 트래픽을 패킷 형태로 저장하는 RAW 패킷 수집 센서와, 네트워크 패킷에서 실행파일 내역을 재조합하여 분석하는 실행파일 분석기를 포함하는 정보 수집부; 상기 정보 수집부에서 수집되는 모든 로그를 통합하여 저장하는 로그 수집부와, 상기 로그 수집부에서 수집된 로그들 간의 연관성을 분석하는 로그 상관 분석기와, 상기 로그 상관 분석기에서 분석된 네트워크의 현재 상황을 보안 담당자에게 제공하는 통합 대시보드를 포함하는 정보 분석부; 및 기업 내부망의 악성 코드 감염 현황을 파악하는 악성 코드 감염 PC 현황 분석부와, 침해 사고에 대한 시작부터 종료까지의 대응 현황을 저장하는 침해 사고 대응 현황 관리부를 포함하는 침해 사고 관리부를 포함하는 것을 특징으로 한다.

발명의 효과

[0021] 상술한 바와 같이, 본 발명에 의한 기업 내부 전산환경의 위협탐지를 위한 보안 아키텍처에 따르면, 프로토콜 분석기를 이용하여 내부에서 외부로 향하는 모든 통신을 분석하고, 기업 내부망으로 유입되는 제로데이형 악성 코드를 탐지하기 위해 통신에서 모든 실행파일을 수집하여 행위 분석 기반의 분석을 실시함으로써, 타겟형 공격을 탐지하여 내부망의 위협을 조기에 탐지할 수 있다.

도면의 간단한 설명

[0022] 도 1은 본 발명의 일 실시예에 의한 기업 내부 전산환경의 위협탐지를 위한 보안 아키텍처의 전체 구성도이다.

도 2는 본 발명의 일 실시예에 의한 통합 대시보드에 세션 기반의 정보를 시각화하는 방법 중 링크형 차트를 예시한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0023] 이하, 본 발명의 기업 내부 전산환경의 위협탐지를 위한 보안 아키텍처에 대하여 첨부된 도면을 참조하여 상세히 설명하기로 한다.

[0024] 도 1은 본 발명의 일 실시예에 의한 기업 내부 전산환경의 위협탐지를 위한 보안 아키텍처의 전체 구성도이다.

[0025] 도 1에 도시된 바와 같이, 본 발명의 바람직한 실시예에 따른 기업 내부 전산환경의 위협탐지를 위한 보안 아키텍처는 크게 정보 수집부(100), 정보 분석부(200) 및 침해 사고 관리부(300)를 포함하여 구성된다.

[0026] 보다 구체적으로 살펴보면, 정보 수집부(100)는 다시 네트워크 트래픽에서 프로토콜별 정보를 수집하는 트래픽 정보 수집 센서(110), RAW 패킷 수집 센서(120) 및 네트워크 트래픽에서 실행파일을 수집하여 자동으로 분석하는 실행파일 분석기(130)를 포함한다.

[0027] 여기서, 트래픽 정보 수집 센서(110)는 내부망 대상 공격 징후를 탐지하기 위해서 내부망에 흐르는 모든 트래픽에 대한 정보를 수집하는 부분이다. 내부망의 정보 수집을 위한 수집 위치는 네트워크 트래픽에서 직접 수집을 하는 것을 원칙으로 해야 한다. 최고로 숙련된 공격자라고 할지라도 네트워크를 우회하여 공격을 진행시킬 수는 없기 때문이다.

[0028] 네트워크 계층에서 정보를 수집하는 것은 여러 가지 장점을 제공하게 되는데 우선 첫 번째로 공격자가 정보 수집 자체를 인식하지 못한다는 점이다. 이것은 정보 수집 시 은닉성이 보장된다는 점에서 공격자들에게 무형의 압박을 제공하는 요소이기도 한다. 두 번째는 우회 패킷이 발생하지 않는다는 점이다. 호스트 레벨에서 에이전트를 이용하고 정보를 수집하는 경우, 에이전트의 가용성이 로그 수집의 신뢰성과 직결된다. 즉, 에이전트가 안정적이지 못하면 로그 수집 역시 안정성이 떨어지며, 호스트를 점령한 공격자가 언제든지 해당 에이전트를 제거하는 경우 수집이 불가능해지는 사태도 발생하기 때문이다.

[0029] 과거 전체 정보를 수집하기 어려운 상황에서는 침입차단시스템, 침입탐지시스템 등 보안장비의 이벤트 로그를 설치하고 이후 ESM으로 로그를 수집하는 구조로 운영되었다. 그러나 이러한 모델은 1차 로그를 생성하는 장비들이 전수 조사가 아닌 탐지 정보만을 수집한다는 점과 원본 로그가 아니라 제조사에 특화된 로그 포맷 형태로 저장이 되어 수집로그의 정규화가 반드시 필요하다는 단점이 존재하였다.

[0030] 본 발명의 트래픽 정보 수집 센서(110)에 있어서, 네트워크 정보에서 공격 정보를 추출하기 위해서는 L3 레벨의 침입차단시스템과 같은 출발지 IP, 포트, 목적지 IP, 포트 등의 정보로는 부족하고, 적어도 L7 레벨의 어플리케이션 정보가 필요하며, 기업 내부망 이용자들이 사용하는 프로토콜 수준의 분석이 수행되는 것이 바람직하다. 그러므로 네트워크 트래픽 정보를 수집하기 위해서는 트래픽 전수 조사, 프로토콜별 트래픽 분석을 수행해야 한다. 프로토콜 분석기는 실제 프로토콜을 직접 분석할 줄 알아야 한다. 이에, 단순히 패킷에 명시된 목적지 포트 번호 만을 가지고 분석하는 것이 아니라 트래픽 자체의 프로토콜의 헤더를 분석하는 것이 바람직하다. 이렇게 함으로써, 본 발명의 트래픽 정보 수집 센서(110)는 특정 프로토콜과 특정 서비스에 종속하여 탐지하는 종래 기법을 극복하여 서비스를 특정 포트 번호와 연관시키는 오류 등을 발생시키지 않을 수 있다.

[0031] 또한, 트래픽 정보 수집 센서(110)에서, 트래픽 정보를 추출하기 위한 프로토콜 분석기는 네트워크에서 흐르는 트래픽을 사용자가 알기 쉽게 텍스트 기반으로 변환하여 저장하는 기능을 지원하는 것이 바람직하다. 이를 위해서 트래픽 정보 수집 센서(110)는 네트워크에 전송되는 정보를 어플리케이션 프로토콜별로 구분하여 저장할 수 있어야 한다. 2000년대 중반까지도 프로토콜 해석기는 매우 고가인 QoS(Quality of Service) 장비에서나 수행할 수 있었다. 하지만 최근 기술의 발달로 L7 스위치와 같은 어플리케이션을 직접 제어할 수 있는 장비들이 대거 등장하고 있다. 특히 인터넷의 가장 기본이라고 할 수 있는 DNS, HTTP, FTP에 대해서는 반드시 지원하고, 여전히 공격자에 의해서 많이 사용되고 있는 IRC, SSH 등도 지원하는 경우 향후 분석에 좋은 효과를 얻을 수 있다.

[0032] 또한, 트래픽 정보 수집 센서(110)의 프로토콜 분석기는 외부로 로그를 전송하는 기능을 보유해야 한다. 프로토콜 분석기에서 자체적으로 로그를 저장하고 검색하는 등의 기능을 보유하면 좋겠지만 최근에는 성능 좋은 로그 검색기와 같은 제품이 많이 나오게 되므로, 이런 장비들과의 연동을 고려한다면 로그의 외부 전송 그리고 가독성이 좋도록 텍스트 형태로 저장하는 기능을 보유하면 분석이 더 용이할 것이다.

[0033] 이와 같이, 본 발명에 있어서 트래픽 정보 수집 센서(110)에서의 프로토콜 분석기의 사용은 기존 보안 장비에서 탐지하지 못하는 비정상 프로토콜, 비정상 포트 사용 등으로 탐지 범위가 비약적으로 확대되는 결과를 가질 수 있다.

[0034] 다음으로, RAW 패킷 수집 센서(120)는 비상 시 상황 재현, 패킷 재조합을 통한 악성 파일 추출 등의 대응을 손쉽게 진행하기 위해 RAW 패킷을 저장한다.

[0035] 앞서 살펴본 트래픽 정보 수집 센서(110)는 모든 트래픽을 텍스트로 변환하여 저장하는 것을 권고하였다. 물론 충분히 많은 정보를 수집하고 저장함으로써 대부분의 이상 징후는 트래픽 정보 수집 센서(110)에서 모두 저장된다고 볼 수 있다. 그러나, 트래픽 정보만을 저장하는 경우는 내부망 위협 대응에서 커다란 위협에 노출되는 경우에 직접 대응에는 정보 수집의 한계가 발생할 수 있다. 대표적인 경우로는 내부에서 유통되는 악성코드에 대한 샘플 수집과 같은 경우이다. 대부분의 악성코드 초기 파일은 PC에 설치된 후 외부에서 실제 악성코드를 다운

받는 Dropper인 경우가 많으므로 감염된 PC에서는 추출하기가 어렵기 때문이다.

[0036] 이에, RAW 패킷 수집 센서(120)는 네트워크에서 전송되는 모든 트래픽을 패킷 형태인 바이너리(binary) 형식으로 저장하는 것으로 대단히 방대한 저장 공간과 저장된 패킷에서 이를 손쉽게 검색하기 위한 바이너리 인덱스(index) 기술이 필요하다. 이것은 일반 텍스트 파일의 인덱싱 기술과는 다른 기술로 분류되는데 그 이유는 텍스트 파일과 달리 패킷은 이더넷 MTU(Maximum Transfer Unit)이라는 제약으로 인하여 최대 1,500byte의 개별 패킷으로 저장되기 때문이다.

[0037] 이러한 패킷에서 의미 있는 값을 구분하기 위해서는 패킷 기반의 정보 인덱스가 아닌 세션 기반의 정보 인덱스를 제공하는 것이 바람직하다. 세션 기반이 필요한 가장 큰 이유는 단방향의 트래픽은 사실 보안에서 그리 크게 문제가 되지 않기 때문이다. 단방향의 트래픽은 출발지와 목적지가 통신을 하지 않고 보통 출발지의 연결 시도만 보이기 때문이다. 이러한 정보는 대부분이 SYN 스캔이나 SYN Flooding과 같은 트래픽에서 보이며 이러한 정보는 보안상 특별히 문제가 되지 않는 트래픽이다. 반면 세션 단위에서 추출하는 정보는 출발지와 목적지가 서로 주고받았던 통신 내역을 모두 담고 있기 때문에 보안 분석에 많은 도움이 된다.

[0038] 마지막으로 실행파일 분석기(130)는 네트워크 패킷에서 실행파일 내역을 재조립하여 분석하는 기능을 담당한다. 그러므로 해당 실행파일 분석기(130)는 네트워크에서 실행파일의 내역이 존재하는 패킷들을 재조합하여 실행파일을 추출하는 기능과 해당 실행파일을 가상 환경에서 분석하는 행위 기반 분석 기능을 보유한다.

[0039] 행위 기반 분석 기능은 특정한 시그니처가 존재하는 탐지 기법이 아니라 네트워크상에서 어떤 행위를 하는 호스트를 분석하고 악성여부를 판단하는 것이다. 시그니처가 패킷 내에 존재하는 특정 값의 유무를 판단하는 것이라면 행위 분석은 허가받지 않은 PC가 지속적으로 DB 서버에 접속을 시도하거나, 전혀 접속한 적이 없는 외국 사이트로 접속을 시도하는 등의 행위를 탐지하는 것이다. 이러한 탐지를 위해서는 악성 행위를 탐지하는 것보다 네트워크에서 발생할 수 있는 정상 행위를 먼저 정의하고 이 정상 행위를 벗어나는 행위를 탐지하는 것이 더 효과적이다.

[0040] 이에, 행위 기반 분석기는 호스트 내에서 해당 파일이 실행되기 전과 실행 이후에 발생하는 변화를 추적하여 이상 징후를 판단하게 되는데, 주로 과거 악성코드의 행위 기반에 대한 휴리스틱(heuristic) 정보를 기반으로 한다. 대표적인 것으로는 레지스트리의 변경을 들 수 있다. 악성코드는 설치되면 호스트가 부팅될 때 악성코드 자신이 자동으로 실행되도록 시작 프로그램에 등록하거나 서비스에 등록하여 호스트를 껐다가 켜더라도 동작하게 만든다. 또한 실행 시 외부로 접속을 시도하는 네트워크 행위를 보여주는 경우가 많다. 이것은 설치 후 악성코드 자체를 업데이트 하거나, C&C 서버로 자신의 감염사실을 알리기 위해서이다. 이러한 행위들을 분석하는 것이 바로 실행파일 분석기(130)이다.

[0041] 실행파일의 행위 기반 분석에서는 그 외 다음의 항목을 점검하여 의심 항목으로 도출하도록 한다.

[0042] · 레지스트리에 시작프로그램으로 등록

[0043] · 설치 후 외부 사이트 접속 시도

[0044] · 프로그램에 일정부분 실행 지체 코드 내재

[0045] · 설치 후 설치 프로그램 스스로 삭제하기

[0046] · 특정 파일 삭제하기

[0047] · 백신, 업데이트 기능 변조

[0048] · 임시 파일의 시간 관련 정보 조작

[0049] · 시스템 서비스 내용 변경

[0050] · 실행압축 형태 파일, 마우스/키보드 내용 후킹 함수

[0051] · 디버거, 가상환경 탐지 시도

[0052] 물론 실행파일 분석기(130)의 결과가 모두 악성코드를 의미하는 것은 아니다. 정상 파일도 업데이트를 위해서 업데이트 서버에 접속하여 파일을 다운로드 받는 경우도 많기 때문이다. 예를 들어, 마이크로소프트에서 제공하는 윈도우즈 업데이트 역시 인터넷에서 파일을 다운로드 받는 것이기 때문이다. 이를 위해 실행파일 분석기(130)는 다운로드 받는 도메인을 기반으로 화이트리스트(White List) 처리를 하는 것이 필요하다.

[0053] 이와 같이, 본 발명의 바람직한 실시예에 따른 실행파일 분석기(130)는 시그니처 기반 탐지 기법에 행위 기반 분석 기법을 추가함으로써, 공격에 대한 특징 값을 이용하는 탐지 기법으로서 우회가 손쉬운 시그니처 기반 탐지의 한계를 개선할 수 있다.

[0054] 정보 분석부(200)는 정보 수집부(100)에서 수집되는 모든 로그를 통합하여 저장하는 로그 수집부(210)와 이를 검색할 수 있는 검색 엔진을 위치시켜 공격자의 공격 행위를 분석하는 수집 로그 상관 분석부(220)를 포함한다. 또한, 통합 대시보드(230)를 설치하여 분석 결과 특히, 보안 분석 결과를 단순 차트가 아닌 시각화하여 제공함으로써 보안 담당자들에게 직관적인 화면을 제시하도록 한다.

[0055] 보다 구체적으로, 로그 수집부(210)는 내부망 위협 대응을 위해서 가장 기본적으로 로그 수집을 수행한다. 로그는 사용자 또는 공격자의 네트워크 행위에 대한 흔적으로서, 만일 로그 수집에 문제가 생기는 경우 이상 징후를 정확하게 판단하는 것이 매우 어려워지기 때문이다. 또한, 로그 수집부(210)는 해당 로그가 변조되지 않았음을 보증하는 절차를 통해 수집된 로그의 무결성을 확보하여 침해사고 발생 시 추적 과정에서 매우 중요하게 활용한다.

[0056] 로그 수집을 위한 방법은 직접 로그를 전송 받는 방법, 에이전트를 통하여 수집하는 방법 등을 이용할 수 있다. 로그를 전송 받는 방법은 개별 장비가 생산되는 로그를 중앙 로그 저장 시스템에 전송하는 것을 의미한다. 이 경우 대부분 시스템 경과 기록(SYSLOG; system log)을 이용하여 로그를 전송하는 방법을 사용한다. 그러나, 개별 장비의 경우 드물지만 SYSLOG를 지원하지 않는 장비도 있으며, 여러 장비에 동시에 동일한 로그를 전송하는 기능이 없는 장비도 있다. 이러한 경우 장비가 생산하는 로그를 저장하는 별도 장비에서 로그를 수집해야 하는 상황이 발생하므로, 해당 장비에 로그 수집 에이전트를 설치하여 로그를 수집한다. 에이전트는 로그가 저장되는 장비에 설치되는 소형 어플리케이션이며 정해진 규칙에 따라 로그를 별도의 정규화 과정을 거치지 않고 바로 저장하는 방식을 사용하는 것이 바람직하다.

[0057] 여기서, 전체 트래픽 현황을 텍스트 로그로 저장하여 로그를 분석하는 경우의 장점은 다음을 들 수 있다.

[0058] · 유실 없는 모든 로그는 침입탐지시스템이 놓친 공격자의 행위까지도 저장한다.

[0059] · 저장된 모든 로그를 기반으로 분석하는 경우 진행 중인 공격자의 공격행위 탐지가 가능하다.

[0060] · 모든 로그의 저장은 기업 네트워크 현황 파악 및 장애처리에도 도움이 된다.

[0061] 또한, 이것을 텍스트 인덱스 기반의 검색엔진을 이용하여 검색하는 경우 다음의 장점이 있다.

[0062] · 수집 시 로그에 대한 파싱(parsing)과 같은 정규화가 필요 없어 고속 수집이 가능하다.

[0063] · 로그 검색 시 로그 포맷에 대한 구조 이해를 선행할 필요가 없어 사용자 편의성이 증대된다.

[0064] · 원하는 경우 후처리를 통하여 로그를 파싱할 수 있다.

[0065] · 각 장비별 동일 IP 탐지 등이 매우 손쉽게 진행될 수 있다.

[0066] 대부분의 텍스트 색인 기반 검색 엔진은 로그를 파싱하여 저장하는 것이 아니라 수집된 로그를 변환 없이 그대로 저장하고 이를 색인한다. 그러므로 파싱에 대한 시간이 소요되지 않아 고속 수집이 가능해진다. 또한 파싱을 하지 않고 수집 로그를 그대로 저장하는 것은 파싱 시에 발생하는 로그 왜곡을 차단할 수 있는 점도 장점으로 볼 수 있다.

[0067] 다음으로, 수집 로그 상관 분석부(220)는 네트워크에서 발생한 로그를 통합 수집한 후에 각 로그들 간의 연관성을 분석한다. 상관 분석이란 정보의 연관성을 파악하여 위협 여부를 판단하는 것이다. 이러한 상관분석을 위해서는 다음과 같은 선행조건이 필수적이다.

[0068] · 정보 수집대상의 모든 정보기기의 시간이 동일해야 한다.

[0069] · NAT, PAT의 환경이더라도 IP의 정보가 동일해야 한다.

[0070] · 수집대상 정보기기들의 목록에 대한 정보가 구축되어야 한다.

[0071] 여기서, 모든 정보기기의 시간이 동일해야 한다는 것은 시간이 동일하지 않으면 수집된 장비의 이벤트와의 1차 연관성이 모두 사라지고 이를 추적하는 것은 거의 불가능하기 때문이다.

[0072] NAT, PAT 환경이더라도 IP의 정보가 동일해야 한다는 점은 다양한 정보를 수집하고 상관분석을 하기 위해서는 정보들 간의 연결고리가 있어야 한다는 것을 의미한다. 정보보호 장비들의 모든 로그는 가장 기본적인 통신정보

인 IP 주소와 포트번호가 저장된다. 예컨대, 침입차단시스템은 출발지IP와 포트, 목적지 IP와 포트가 저장된다. 침입탐지시스템은 출발지IP와 포트, 목적지 IP와 포트이외에 공격명이 저장된다. 가상사설망의 경우 출발지 IP, 포트와 목적지 IP와 포트가 저장되며 사용자 ID 등이 저장된다. 이 과정에서 Time Stamp는 당연히 저장된다. 그런데 만일 이러한 여러 로그들을 연결할 고리로는 사실상 IP 주소가 유일하다.

[0073] 공격자가 외부에서 내부로 공격을 하는 경우를 생각해보면, 대부분의 침입차단시스템은 내부망 주소를 숨기기 위해서 NAT를 사용한다. 그러므로 NAT로 변경된 공인 IP 주소와 변경 전의 사설 IP 주소가 같은 이벤트로 기록이 되어야 한다. 또한 침입차단시스템의 NAT 공인 IP와 침입탐지시스템에서 탐지된 공인 IP와의 연관성을 IP 주소의 고리로 찾아야 한다. 가장 큰 문제는 탐지된 사설 IP의 추적성을 확보하기가 매우 어렵다는 것이다. 이를 위해서는 해당 IP를 사용한 호스트 또는 서버를 찾아야 하며 이를 위해서는 IP 할당 기록을 찾아야 하는 것이다.

[0074] 이렇듯 하나의 해킹사고를 추적하기 위해서라도 다양한 로그가 수집되므로 이러한 정보를 상관 분석하는 시스템을 구축하는 것은 공격자의 위협에 대응하기 위해서라도 좋은 대비책이 될 것이다.

[0075] 또한, 수집 로그 상관 분석부(220)는 수집 로그 분석을 위해 로그별 탐지 규칙을 설정하는 것이 바람직하다. 본 발명의 바람직한 실시예에서는 프로토콜 단위로 수집하는 것을 기반으로 프로토콜 기반으로 탐지 규칙을 제안한다. 프로토콜 기반의 탐지규칙은 해당 프로토콜에서 발생하는 이상 징후를 판단하기에 용이하며, 프로토콜의 성격별로 공격자의 행위를 손쉽게 파악할 수 있는 장점이 존재한다.

[0076] 로그 분석은 두 가지로 분류하여 진행한다. 첫 번째는 단순히 통계 기반의 분석을 진행하는 것이다. 이것은 사용량이 많은 각종 보안 지표 예를 들어, 목적지 포트, 목적지 IP, 출발지 IP, 목적지 도메인 등을 기반으로 해당 내역에 대한 이상 징후를 판단하는 것이다. 두 번째로는 보안상 의심 행위를 분석하는 것이다. 이것은 행위 기반 보안 지표 예를 들어, 비정규 포트 통신, 비정규 프로토콜 통신, 지속적인 접속 실패, 파일 전송 성공 여부 등을 이용하여 분석을 수행하도록 한다.

[0077] 마지막으로, 통합 대시보드(230)는 분석된 정보를 보안 담당자에게 제공하여 보호대상 네트워크의 현재 상황을 직관적으로 볼 수 있도록 하는 일종의 상황판이다.

[0078] 대개 대시보드는 방대한 로그의 낮은 가독성을 개선하고자 특정 보안지표에 대해서 특징 값들을 추출하고 이를 차트와 같은 그림으로 도식화를 하는 것이 일반적이다. 하지만 과거 많은 제품들의 대시보드는 통계정보를 의미하는 Top 10 위주의 화면을 보여주고 있다. 하지만 이러한 통계는 보안에 그리 도움이 되지 않는다. 일례로 Top 10 사용포트에 대한 정보를 살펴보면, 해당 정보는 패킷의 포트번호를 기반으로 정보를 추출하게 되는데 만일 공격자가 포트번호를 비정규 포트 예를 들어, SSH를 5000/TCP로 변경하여 사용하는 경우 전혀 다른 내용이 대시보드에 나타나게 된다.

[0079] 그러므로, 본 발명의 통합 대시보드(230)로는 Top 10 유형의 통계가 아닌 프로토콜별 유형의 세션정보를 기반으로 대시보드를 제작하는 기법을 제안한다. 이에, 그림 1을 참조하면, 그림 1은 통합 대시보드(230)에 각종 차트의 표현 방식을 나타낸 도면이다.

[0080] [그림 1]

[0081]

[0082] 앞서 언급하였듯이, 세션이란 통신 당사자인 출발지와 목적지간의 전송된 데이터의 집합을 의미한다. 많은 패킷을 주고받은 목적지 Top10이 아니라 많은 패킷을 전송한 출발지 Top10을 선정하고 이 출발지가 통신한 목적지를 동시에 연계하여 대시보드를 제작하는 것이다.

[0083] 또한, 방대한 양의 로그를 직관적이고 가독성 있는 대시보드 항목으로 제작하기 위하여 시각화 기법을 도입하여 구축하는 방법을 제안한다.

[0084] 대부분의 보안 관리 시스템은 저장된 로그에서 공격 여부를 판단하기 위해 공격 특정값(Attack Signature)을 기반으로 탐지를 수행한다. 그러나 이러한 공격 특정값은 알려진 공격만을 탐지할 수 있다는 문제점이 존재한다.

[0085] 그러므로, 본 발명의 통합 대시보드(230)로는 수집된 로그를 대상으로 보안에 특화된 값을 추출하는 시각화 방법을 제안하며, 특히 세션 기반의 정보를 시각화하는 방법 중에 가장 효과적인 방법인 링크형(Link)형 방식을 사용하여 대시보드 시각화를 구축하는 것을 제안한다.

[0086] 도 2는 통합 대시보드에 세션 기반의 정보를 시각화하는 방법 중 링크형 차트를 예시한 것으로서, 링크형 방식을 사용하여 시각화를 구축한 것을 나타내고 있다.

[0087] 링크형 차트는 다음과 같은 장점을 가지고 있다.

[0088] · 출발지와 목적지의 방향성을 판단할 수 있다.

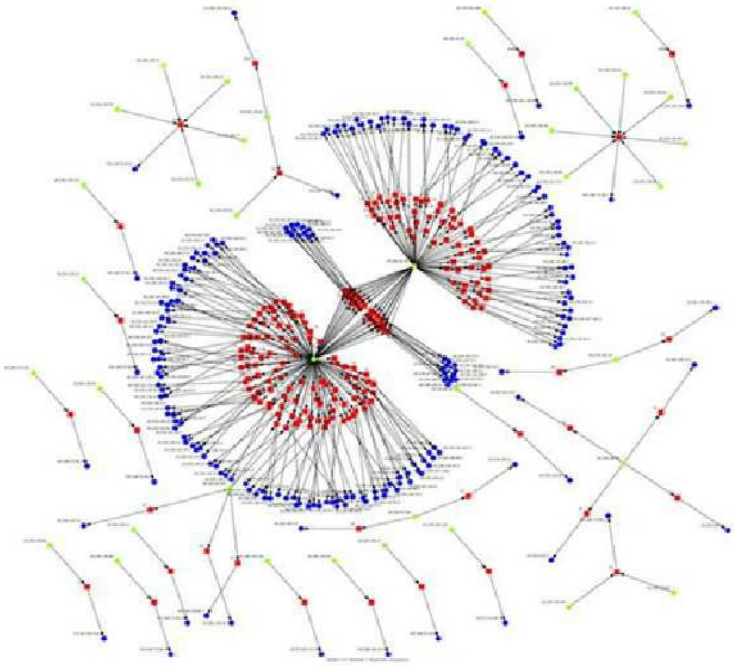
[0089] · 목적지 포트, 사용 프로토콜과 같은 부가 정보를 표현할 수 있다.

[0090] · N:1, 1:N의 접속 현황을 직관적으로 파악할 수 있다.

[0091] 링크형 방식의 도식화는 단순히 많고 적음을 표시하는 선이나 막대, 원이 아닌 링크 그래프를 사용하여 도식화를 진행한다. 링크 그래프 타입은 출발지와 목적지를 연결하여 방향성의 링크를 생성한다.

[0092] 또한, 출발지와 목적지에 대한 링크를 표시할 때에는 프로토콜별로 링크를 표시하여 해당 프로토콜의 접속 현황에 대해서 확인하도록 할 수 있다. 이는, 프로토콜별로 접속하는 경우 출발지와 목적지의 통신 내역에 대한 직관적인 파악이 가능하며, 해당 응용 프로토콜의 표준 포트 사용 등이 지켜지지 않는 경우 이상 징후를 즉시 파악할 수 있기 때문이다.

[0093] [그림 2]

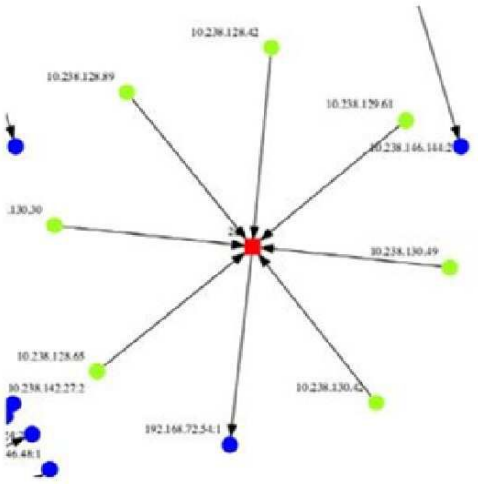


[0094]

[0095] 그림 2는 시험용으로 구축한 시스템에서 추출한 로그를 방향성을 기반으로 도식화한 그림이다. 이 그림에서 분석가는 화살표 방향을 기반으로 출발지와 목적지의 방향성을 파악할 수 있다. 가운데 사각형은 목적지로 접속할 때 사용한 포트를 의미한다. 본 시각화 그림은 약 10,000 줄의 SSH 텍스트 로그를 시각화한 것으로서, 본 그림에서 관리자는 1개의 출발지에서 많은 목적지로의 접속 실패에 대하여 매우 손쉽게 이상 징후를 판단할 수 있다. 1:N의 실패를 명확하게 보여주는 본 시각화 그림에서 숙련된 관리자라면 네트워크 스캐닝이라는 것을 확인할 수 있기 때문이다.

[0096] 이와는 반대의 개념인 N:1의 접속도 그림 3에서 확인할 수 있다. 그림 3 역시 시험을 위한 구축 시스템에서 추출한 SSH 접속 실패 로그를 도식화한 것이다. 이 그림은 다양한 출발지에서 1개의 목적지로 접속을 실패하는 것을 보여준다.

[0097] [그림 3]



[0098]

[0099] 이러한 N:1의 접속인 경우 해당 PC의 계정이 도용되었는지도 확인해 보아야 한다. N:1의 접속 실패가 정상 행위는 아니기 때문이다.

[0100] 이렇듯 로그의 시각화는 방대한 로그의 양을 분석하는 시각을 획기적으로 단축시켜주며, 시각화 이미지가 주는

의미에 대한 해석이 매우 용이하다고 할 수 있다.

[0101] 침해 사고 관리부(300)는 악성 코드 감염 PC 현황 분석부(310), 침해 사고 대응 현황 관리부(320)를 포함한다.

[0102] 악성 코드 감염 PC 현황 분석부(310)는 기업 보안 담당자가 관리하는 내부망에서 악성 코드 감염 현황을 파악하는 것이다. 이는 후술하는 침해 사고 대응 현황 관리부(320)와 연결되어 내부망 대상 공격을 보안 관리자들이 어떻게 대응하고 있는지에 대한 침해 사고 대응 및 진행 현황과 연동함으로써 현재 기업 내부망의 보안 상태를 파악할 수 있게 해준다.

[0103] 다음으로, 침해 사고 대응 현황 관리부(320)는 현재 기업이 대응하고 있는 침해 사고를 체계적으로 시작부터 종료까지를 일관적으로 관리하는 것이다. 이는 기업 내에서 활동하는 침해 사고 대응팀(CERT; Computer Emergency Response Team)에서 사용하는 가장 기본적인 업무 체계로서 대응에 대한 전반적인 현황을 관리하는 워크플로우 시스템이라고 할 수 있다.

[0104] 침해 사고 대응 현황 관리부(320)에는 최대한 많은 정보 예를 들어, 사고 대응 관리 번호, 현재 대응 현황, 담당 분석가, 침해 사고 생성일, 침해 사고 대응 시작일, 침해 사고 최종 수정일, 해당 사고의 심각도, 사고 유형 등을 저장하고 상세 내역을 남겨서 사고 대응에 도움이 되도록 한다. 이렇게 저장된 정보는 침해 사고 대응의 지식 베이스로 축적되어 동일한 사고를 처리하는 경우 투입되는 시간을 단축시킬 수 있다. 그리고 이러한 침해 사고 대응 현황 관리부(320)는 대응 내역에 대한 개인별 처리 현황, 이력 관리도 파악할 수 있어 업무 배치 등의 관리적 차원에서도 좋은 도구가 될 수 있다.

[0105] 이상에서 몇 가지 실시예를 들어 본 발명을 더욱 상세하게 설명하였으나, 본 발명은 반드시 이러한 실시예로 국한되는 것이 아니고 본 발명의 기술사상을 벗어나지 않는 범위 내에서 다양하게 변형실시될 수 있다.

부호의 설명

[0106] 100 : 정보 수집부 110 : 트래픽 정보 수집 센서

120 : RAW 패킷 수집 센서 130 : 실행파일 분석기

200 : 정보 분석부 210 : 로그 수집부

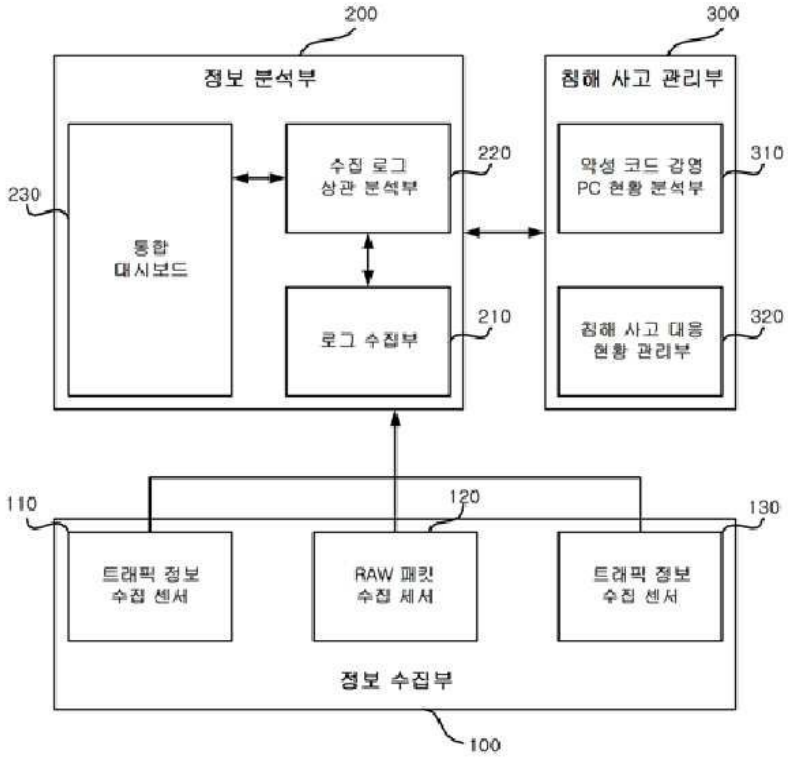
220 : 수집 로그 상관 분석부 230 : 통합 대시보드

300 : 침해 사고 관리부 310 : 악성 코드 감염 PC 현황 분석부

320 : 침해 사고 대응 현황 관리부

도면

도면1


200
300
정보 분석부
침해 사고 관리부
수집 로그
상관 분석부
220
악성 코드 감염
PC 현황 분석부
310
230
통합
대시보드
로그 수집부
210
침해 사고 대응
현황 관리부
320
110
120
130
트래픽 정보
수집 센서
RAW 패킷
수집 센서
트래픽 정보
수집 센서
정보 수집부
100

도면2