(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2010-0075043
(43) 공개일자 2010년07월02일

(51) Int. Cl.
H04L 12/22 (2006.01) *H04L 12/26* (2006.01)
(21) 출원번호 10-2008-0133644
(22) 출원일자 2008년12월24일
심사청구일자 2008년12월24일

(71) 출원인
한국인터넷진흥원
서울 송파구 가락동 78
(72) 발명자
정현철
서울특별시 송파구 오금동 55-24 멀티파크 B동 201호
임채태
서울특별시 송파구 잠실3동 27번지 주공아파트 528동 1107호
(뒷면에 계속)
(74) 대리인
특허법인다울

전체 청구항 수 : 총 13 항

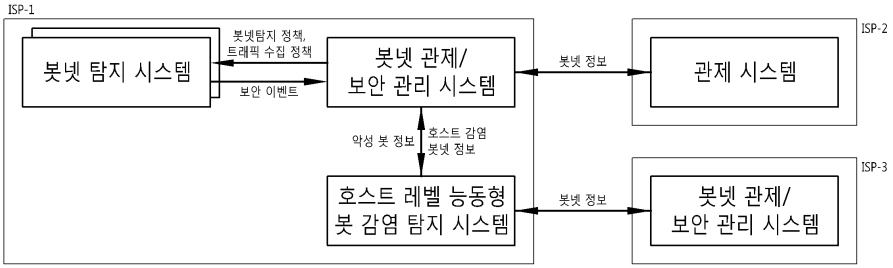
(54) IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템 및 그 방법

(57) 요 약

본 발명은 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템 및 방법에 관한 것으로서, 인터넷 서비스 제공자 망의 봇넷을 탐지하여 봇넷에 대한 정보를 데이터베이스에 저장하고 이에 대응하는 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템에 있어서, 상기 인터넷 서비스 제공자 망내의 봇넷 정보를 시각화하며 상기 봇넷에 대한 대응 정책을 설정하는 봇넷 관제 및 보안관리 시스템을 포함하는 것을 특징으로 하는 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템 및 방법에 관한 것이다.

이에 본 발명은 봇넷 관제 및 보안 관리 시스템을 이용하여 IRC와 HTTP 봇넷의 보안 관제를 효율적으로 관리할 수 있는 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템을 제공할 수 있으며, 봇넷 관제 및 보안 관리 시스템을 이용하여 IRC와 HTTP 봇넷을 효과적으로 방어할 수 있는 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템을 제공할 수 있다.

대 표 도 - 도1



(72) 발명자

지승구

경기도 용인시 수지구 죽전동 인현마을 현대홈타운 7차 2단지 204동 902호

노상균

광주광역시 북구 누문동 162-4

오주형

서울특별시 관악구 신림2동 96-55

이 발명을 지원한 국가연구개발사업

과제고유번호	2008-S-026-01
부처명	지식경제부
연구사업명	IT성장동력기술개발사업
연구과제명	신종 봇넷 능동형 탐지 및 대응 기술 개발
주관기관	한국정보보호진흥원
연구기간	2008.03.01~2009.02.28

특허청구의 범위

청구항 1

인터넷 서비스 제공자 망의 봇넷을 탐지하여 봇넷에 대한 정보를 데이터베이스에 저장하고 이에 대응하는 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템에 있어서,

상기 인터넷 서비스 제공자 망내의 봇넷 정보를 시각화하며 상기 봇넷에 대한 대응 정책을 설정하는 봇넷 관제 및 보안관리 시스템을 포함하는 것을 특징으로 하는 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템.

청구항 2

제 1 항에 있어서,

상기 다수의 인터넷 서비스 제공자 망에 분포되어 트래픽 정보를 상기 봇넷 탐지 시스템에 전달하는 트래픽 정보 수집 센서와,

상기 트래픽 정보 수집 센서와 봇넷 탐지 시스템의 설정 및 상태 정보를 관리하는 관리 시스템을 포함하는 것을 특징으로 하는 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템.

청구항 3

제 1 항에 있어서,

상기 봇넷 관제 및 보안 관리 시스템은,

상기 봇넷 탐지 시스템으로부터 보안 이벤트를 수신하여 처리하는 보안 이벤트 관리 모듈과,

상기 보안 이벤트에 대한 봇넷과의 유사도를 분석하는 예외 구성 로그 분석 모듈과,

상기 보안 이벤트 중 미분류 행위 로그를 전달받아 분류하는 미분류된 행동 로그 분석 모듈과,

상기 탐지된 봇넷에 대한 대응 정책을 수립하는 봇넷 대응 기술 모듈과,

상기 탐지된 봇넷 정보와 봇넷 악성행위 정보와 시스템 정보와 정책 정보 및 봇넷 대응 정책 정보를 관리하는 탐지 로그 감독 모듈과,

상기 봇넷 관제 및 보안 관리 시스템의 정책을 설정하는 정책 감독 모듈과,

상기 봇넷 관제 및 보안 관리 시스템에 봇넷 탐지 시스템과 트래픽 수집센서와 도메인 네임 시스템 싱크홀 서버와 BGP 라우터와 도메인 네임 시스템 서버 및 웹 방화벽을 등록하는 시스템 감독 모듈과,

상기 탐지된 봇넷 정보 및 악성행위 정보를 기초로 통계 데이터를 생성하는 정적인 리포팅 관리 모듈과,

상기 탐지된 봇넷 구조 및 악성행위를 모니터링하는 봇넷 모니터링 모듈을 포함하는 것을 특징으로 하는 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템.

청구항 4

제 3 항에 있어서,

상기 보안 이벤트 관리 모듈은,

상기 수집된 보안 이벤트를 분류하는 보안 이벤트 수집 분류 모듈과,

상기 정책 감독 모듈이 설정한 정책에 따라 봇넷의 차단을 위한 대응 정책 요청 메시지를 상기 봇넷 대응 기술 모듈부에 전송하는 대응정책 체크 모듈과,

상기 보안 이벤트에 대한 수집/분류/정책 생성관리 모듈과,

상기 수집된 보안 이벤트 중 비정상 구성로그를 저장하는 비정상 구성로그 버퍼를 포함하는 것을 특징으로 하는 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템.

청구항 5

제 3 항에 있어서,

상기 예외 구성 로그 분석 모듈은,

상기 보안 이벤트 중 비정상 구성 로그 버퍼를 주기적으로 리딩하여 동일 타임 슬롯내에서 발생된 구성로그를 구성별로 매트릭스에 기록하는 비정상 구성로그 검색 및 분류 모듈과,

현재 타임 슬롯내의 봇넷 C&C와 바로 이전의 타임 슬롯의 봇넷 C&C 정보를 비교하는 봇넷 C&C 비교 모듈과,

현재 타임 슬롯과 바로 이전 타임 슬롯에 존재하는 봇넷 C&C의 소스 IP들을 대상으로 악성 봇넷과의 유사도를 분석하는 C&C 분석 및 탐지 모듈과,

상기 C&C 분석 및 탐지 모듈에서 탐지된 봇넷 트래픽을 전송 받아 프로토콜별로 C&C를 추출하여 분석결과를 로그에 저장하는 C&C 추출 모듈과,

상기 봇넷 관제 및 보안관리 시스템에서 신규로 탐지된 봇넷 C&C에 대한 블랙리스트 생성 대응 정책 설정 요청 메시지를 생성하는 대응 정책 설정 모듈을 포함하는 것을 특징으로 하는 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템.

청구항 6

제 5 항에 있어서,

상기 봇넷 대응 기술 모듈은 블랙리스트 공유, 도메인 네임 시스템 싱크홀, HTTP 봇넷 C&C URL 접근 차단, BGP 피딩을 포함하는 봇넷 대응 정책을 설정하는 것을 특징으로 하는 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템.

청구항 7

제 3 항에 있어서,

상기 탐지 로그 감독 모듈은,

상기 데이터베이스와의 접속을 관리하는 커넥션 풀과,

상기 데이터베이스로의 조회와 삽입과 삭제 및 수정 요청을 담당하는 조회/삽입/삭제/수정 모듈과,

상기 탐리 로그 감독 모듈로의 요청 메시지를 분류하여 상기 조회/삽입/삭제/수정 모듈로 전달하는 쿼리 분류 모듈과,

상기 조회/삽입/삭제/수정 모듈에서 상기 데이터베이스로의 삽입 요청과 수정 요청에 대한 중복 여부를 체크하는 중복체크 모듈과,

상기 요청 메시지를 전달 받아 SQL문을 생성하여 전송하는 SQL문 생성/전송 모듈과,

상기 생성된 SQL문을 전송한 후 응답 받은 결과를 리턴하는 결과 전송 모듈을 포함하는 것을 특징으로 하는 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템.

청구항 8

제 3 항에 있어서,

상기 시스템 감독 모듈은 상기 인터넷 서비스 제공자 망내에서 봇넷 정보를 수집하는 다수의 트래픽 수집 센서 또는 다수의 트래픽 수집 센서에서 수집된 트래픽을 기초로 봇넷을 탐지하는 봇넷 탐지 시스템으로부터 전송된 상태 정보를 수신하여 처리하는 기능과,

사용자가 웹상에 디스플레이된 상기 봇넷 관제 및 보안관리 시스템을 조작할 수 있는 관리 콘솔 그래픽 유저 인터페이스로부터 상태 정보 조회 요청을 처리하는 기능을 수행하는 것을 특징으로 하는 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템.

청구항 9

인터넷 서비스 제공자 망의 봇넷을 탐지하여 봇넷에 대한 정보를 데이터베이스에 저장하고 이에 대응하는 IRC

및 HTTP 봇넷 보안 관제를 위한 방법에 있어서,

상기 인터넷 서비스 제공자 망에서 봇넷을 탐지하는 단계와,

상기 봇넷에 따른 대응 정책을 수립하는 단계를 포함하는 것을 특징으로 하는 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 방법.

청구항 10

제 9 항에 있어서,

상기 인터넷 서비스 제공자 망에서 봇넷을 탐지하는 단계는,

상기 인터넷 서비스 제공자 망에서 트래픽을 수집하는 단계와,

상기 수집된 트래픽을 기초로 로그를 분류하는 단계와,

상기 로그를 처리하는 단계를 포함하는 것을 특징으로 하는 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 방법.

청구항 11

제 10 항에 있어서,

상기 로그는 탐지로그와 분류 행위 로그와 비정상 구성 로그와 미분류 행위로그를 포함하는 것을 특징으로 하는 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 방법.

청구항 12

제 11 항에 있어서,

상기 로그를 처리하는 단계는,

상기 탐지로그를 처리하는 단계와,

상기 분류 행위로그를 처리하는 단계와,

상기 비정상 구성로그를 처리하는 단계와,

상기 미분류 행위로그를 처리하는 단계를 포함하는 것을 특징으로 하는 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 방법.

청구항 13

제 10 항에 있어서,

상기 봇넷 정보에 대한 통계 데이터를 작성하는 단계를 더 포함하는 것을 특징으로 하는 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 방법.

명 세 서

발명의 상세한 설명

기 술 분 야

[0001] 본 발명은 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템 및 방법에 관한 것으로서, 특히 봇넷 관제 및 보안 관리 시스템을 이용한 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템 및 방법에 대한 것이다.

배 경 기 술

[0002] 봇은 로봇(Robot)의 줄임말로서 악의적 의도를 가진 소프트웨어에 감염된 개인용 컴퓨터(Personal Computer, PC)를 의미한다. 이러한 봇넷은 봇넷이 사용하는 프로토콜에 따라 분류될 수 있다. 즉, 봇넷을 이루는 봇 클라이언트와 C&C(Command & Control) 서버간의 통신 프로토콜로 IRC 프로토콜일 경우에 IRC 봇넷으로 분류되며, HTTP 프로토콜일 경우에는 HTTP 봇넷으로 분류될 수 있다. 이때, 개인용 컴퓨터에 감염되어 수많은 봇이 네트워크로 연결되어 봇넷(Botnet)을 형성하게 된다. 이렇게 형성된 봇넷은 봇 마스터(Bot Master)에 의해 원격 조종

되어 디도스(DDoS) 공격, 개인정보 수집, 피싱, 악성코드 배포, 스팸메일 발송 등 다양한 악성행위에 이용되고 있다.

[0003] 이와 같이, 봇넷을 통한 공격이 지속적으로 증가하고, 점차 방법이 다양화되고 있으며, 또한 금전적 이득을 목표로 하는 범죄화 양상을 보이고 있다. 디도스(DDoS)를 통한 인터넷 서비스 장애를 유발하는 경우와 달리, 개인 시스템 장애를 유발하거나, 개인정보를 불법 취득하는 봇들이 있으며, 아이디/암호(ID/Password), 금융정보 등 사용자 정보의 불법 유출을 통하여 사이버 범죄에 악용하는 사례가 커지고 있다. 또한, 기존의 해킹 공격들이 해커 자신의 실력을 뽐내거나 커뮤니티를 통한 실력 경쟁과 같은 수준인데 반해 봇넷은 금전적인 이익을 목적으로 해커 집단이 이를 집중적으로 악용하고 협력하는 모습을 보이고 있다.

[0004] 하지만, 봇넷은 주기적 업데이트, 실행압축기술, 코드자가변경, 명령채널의 암호화 등의 첨단기술을 사용하여 탐지 및 회피가 어렵도록 더욱 교묘해지고 있다. 또한, 봇넷은 그 소스가 공개되어 있어 수천 종의 변종이 발생하고 있으며, 유저 인터페이스를 통해 쉽게 봇 코드를 생성하거나 제어할 수 있어 전문적인 지식이나 기술이 없는 사람들도 봇넷을 만들고 이용할 수 있어 그 문제점이 심각하다.

발명의 내용

해결 하고자하는 과제

[0005] 본 발명의 목적은 IRC와 HTTP 봇넷의 보안 관제를 효율적으로 할 수 있는 IRC와 HTTP 봇넷 보안 관제를 위한 관리 시스템 및 그 방법을 제공하는 것이다.

과제 해결수단

[0006] 상술한 목적을 달성하기 위해 본 발명은 인터넷 서비스 제공자 망의 봇넷을 탐지하여 봇넷에 대한 정보를 데이터베이스에 저장하고 이에 대응하는 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템에 있어서, 상기 인터넷 서비스 제공자 망내의 봇넷 정보를 시각화하며 상기 봇넷에 대한 대응 정책을 설정하는 봇넷 관제 및 보안관리 시스템을 포함하는 것을 특징으로 하는 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템을 제공한다.

[0007] 상기 다수의 인터넷 서비스 제공자 망에 분포되어 트래픽 정보를 상기 봇넷 탐지 시스템에 전달하는 트래픽 정보 수집 센서와, 상기 트래픽 정보 수집 센서와 봇넷 탐지 시스템의 설정 및 상태 정보를 관리하는 관리 시스템을 포함한다.

[0008] 상기 봇넷 관제 및 보안 관리 시스템은 상기 봇넷 탐지 시스템으로부터 보안 이벤트를 수신하여 처리하는 보안 이벤트 관리 모듈과, 상기 보안 이벤트에 대한 봇넷과의 유사도를 분석하는 예외 구성 로그 분석 모듈과, 상기 보안 이벤트 중 미분류 행위 로그를 전달받아 분류하는 미분류된 행동 로그 분석 모듈과, 상기 탐지된 봇넷에 대한 대응 정책을 수립하는 봇넷 대응 기술 모듈과, 상기 탐지된 봇넷 정보와 봇넷 악성행위 정보와 시스템 정보와 정책 정보 및 봇넷 대응 정책 정보를 관리하는 탐지 로그 감독 모듈과, 상기 봇넷 관제 및 보안 관리 시스템의 정책을 설정하는 정책 감독 모듈과, 상기 봇넷 관제 및 보안 관리 시스템에 봇넷 탐지 시스템과 트래픽 수집센서와 도메인 네임 시스템 싱크홀 서버와 BGP 라우터와 도메인 네임 시스템 서버 및 웹 방화벽을 등록하는 시스템 감독 모듈과, 상기 탐지된 봇넷 정보 및 악성행위 정보를 기초로 통계 데이터를 생성하는 정적인 리포팅 관리 모듈과, 상기 탐지된 봇넷 구조 및 악성행위를 모니터링하는 봇넷 모니터링 모듈을 포함한다.

[0009] 상기 보안 이벤트 관리 모듈은 상기 수집된 보안 이벤트를 분류하는 보안 이벤트 수집 분류 모듈과, 상기 정책 감독 모듈이 설정한 정책에 따라 봇넷의 차단을 위한 대응 정책 요청 메시지를 상기 봇넷 대응 기술 모듈부에 전송하는 대응정책 체크 모듈과, 상기 보안 이벤트에 대한 수집/분류/정책 생성관리 모듈과, 상기 수집된 보안 이벤트 중 비정상 구성로그를 저장하는 비정상 구성로그 버퍼를 포함한다.

[0010] 상기 예외 구성 로그 분석 모듈은 상기 보안 이벤트 중 비정상 구성 로그 버퍼를 주기적으로 리딩하여 동일 타임 슬롯내에서 발생된 구성로그를 구성별로 매트릭스에 기록하는 비정상 구성로그 검색 및 분류 모듈과, 현재 타임 슬롯내의 봇넷 C&C와 바로 이전의 타임 슬롯의 봇넷 C&C 정보를 비교하는 봇넷 C&C 비교 모듈과, 현재 타임 슬롯과 바로 이전 타임 슬롯에 존재하는 봇넷 C&C의 소스 IP들을 대상으로 악성 봇넷과의 유사도를 분석하는 C&C 분석 및 탐지 모듈과, 상기 C&C 분석 및 탐지 모듈에서 탐지된 봇넷 트래픽을 전송 받아 프로토콜별로 C&C를 추출하여 분석결과를 로그에 저장하는 C&C 추출 모듈과, 상기 봇넷 관제 및 보안관리 시스템에서 신규로 탐지된 봇넷 C&C에 대한 블랙리스트 생성 대응 정책 설정 요청 메시지를 생성하는 대응 정책 설정 모듈을 포함한다.

[0011] 상기 봇넷 대응 기술 모듈은 블랙리스트 공유, 도메인 네임 시스템 싱크홀, HTTP 봇넷 C&C URL 접근 차단, BGP 피딩을 포함하는 봇넷 대응 정책을 설정한다.

[0012] 상기 탐지 로그 감독 모듈은 상기 데이터베이스와의 접속을 관리하는 커넥션 풀과, 상기 데이터베이스로의 조회와 삽입과 삭제 및 수정 요청을 담당하는 조회/삽입/삭제/수정 모듈과, 상기 탐리 로그 감독 모듈로의 요청 메시지를 분류하여 상기 조회/삽입/삭제/수정 모듈로 전달하는 쿼리 분류 모듈과, 상기 조회/삽입/삭제/수정 모듈에서 상기 데이터베이스로의 삽입 요청과 수정 요청에 대한 중복 여부를 체크하는 중복체크 모듈과, 상기 요청 메시지를 전달 받아 SQL문을 생성하여 전송하는 SQL문 생성/전송 모듈과, 상기 생성된 SQL문을 전송한 후 응답 받은 결과를 리턴하는 결과 전송 모듈을 포함한다.

[0013] 상기 시스템 감독 모듈은 상기 인터넷 서비스 제공자 망내에서 봇넷 정보를 수집하는 다수의 트래픽 수집 센서 또는 다수의 트래픽 수집 센서에서 수집된 트래픽을 기초로 봇넷을 탐지하는 봇넷 탐지 시스템으로부터 전송된 상태 정보를 수신하여 처리하는 기능과, 사용자가 웹 상에 디스플레이된 상기 봇넷 관제 및 보안관리 시스템을 조작할 수 있는 관리 콘솔 그래픽 유저 인터페이스로부터 상태 정보 조회 요청을 처리하는 기능을 수행한다.

[0014] 또한, 본 발명은 인터넷 서비스 제공자 망의 봇넷을 탐지하여 봇넷에 대한 정보를 데이터베이스에 저장하고 이에 대응하는 IRC 및 HTTP 봇넷 보안 관제를 위한 방법에 있어서, 상기 인터넷 서비스 제공자 망에서 봇넷을 탐지하는 단계와, 상기 봇넷에 따른 대응 정책을 수립하는 단계를 포함하는 것을 특징으로 하는 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 방법을 제공한다.

[0015] 상기 인터넷 서비스 제공자 망에서 봇넷을 탐지하는 단계는 상기 인터넷 서비스 제공자 망에서 트래픽을 수집하는 단계와, 상기 수집된 트래픽을 기초로 로그를 분류하는 단계와, 상기 로그를 처리하는 단계를 포함한다. 이때, 상기 로그는 탐지로그와 분류 행위 로그와 비정상 구성 로그와 미분류 행위로그를 포함한다.

[0016] 상기 로그를 처리하는 단계는 상기 탐지로그를 처리하는 단계와, 상기 분류 행위로그를 처리하는 단계와, 상기 비정상 구성로그를 처리하는 단계와, 상기 미분류 행위로그를 처리하는 단계를 포함한다. 상기 봇넷 정보에 대한 통계 데이터를 작성하는 단계를 더 포함한다.

효 과

[0017] 본 발명은 봇넷 관제 및 보안 관리 시스템을 이용하여 IRC와 HTTP 봇넷의 보안 관제를 효율적으로 관리할 수 있는 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템을 제공할 수 있다.

[0018] 또한, 본 발명은 봇넷 관제 및 보안 관리 시스템을 이용하여 IRC와 HTTP 봇넷을 효과적으로 방어할 수 있는 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템을 제공할 수 있다.

발명의 실시를 위한 구체적인 내용

[0019] 도 1은 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 구성도이고, 도 2는 본 발명에 따른 IRC와 HTTP 봇넷 정보 공유 시스템의 봇넷 탐지 시스템의 구성도이다. 도 3은 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 스택이고, 도 4는 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 봇넷 관제 및 보안관리 시스템의 개념도이다. 도 5는 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 봇넷 관제 및 보안관리 시스템의 구성도이고, 도 6은 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 보안 이벤트 관리 모듈의 구성도이다. 도 7은 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 보안 이벤트 관리 모듈을 설명하기 위한 순서도이고, 도 8은 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 탐지/분류 행위로그 처리에 대한 SEC 시퀀스 다이어그램이다. 또한, 도 9는 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 비정상 구성로그 처리에 대한 SEC 시퀀스 다이어그램이고, 도 10은 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 AOA의 구성도이다. 도 11은 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 AOA를 설명하기 위한 순서도이고, 도 12는 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 BAT의 구성도이다. 도 13은 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 BAT를 설명하기 위한 순서도이고, 도 14는 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 BAT 시퀀스 다이어그램이다. 도 15는 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 봇넷 대응 정책 설정 요청 검증의 순서도이고, 도 16은 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 봇넷 대응 정책 설정 요청 검증의 구성도이다. 도 17은 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 봇넷 통계 시퀀스 다이어그램이고, 도 18은 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 봇넷 좀비 통계 시

퀀스 다이어그램이다. 도 19는 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 도메인 네임 시스템 싱크홀 트래픽 통계 시퀀스 다이어그램이고, 도 20은 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 통합 보고서 시퀀스 다이어그램이다. 도 21은 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 보고서 예약 시퀀스 다이어그램이고, 도 22는 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 초기화면 및 봇넷 C&C 클릭에 대한 시퀀스 다이어그램이다. 도 23은 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 BM 구성도이고, 도 24는 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 리프레쉬와 줌인/줌아웃 및 타이머 시퀀스 다이어그램이다. 도 25는 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 TOP N 통계 시퀀스 다이어그램이고, 도 26은 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 DLM 구성도이다. 도 27은 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 SM 구성도이다.

[0020] 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템은 도 1에 도시된 바와 같이, 인터넷 서비스 제공자 망에 각각 마련된 봇넷 탐지 시스템과, 봇넷 탐지 시스템의 정보를 취합하는 통합관제/보안관리 시스템을 포함한다. 이때, 인터넷 서비스 제공자(Internet Service Provider, ISP) 망은 각 개인이나 단체가 인터넷에 접속할 수 있는 회선 등을 포함하는 서비스 망을 의미하며, 본 실시예는 이러한 인터넷 서비스 제공자 망으로 세 개의 인터넷 서비스 제공자 망을 예시한다. 또한, 이에 따라, 인터넷 서비스 제공자 망은 제 1 내지 제 3 인터넷 서비스 제공자 망을 포함한다. 하지만 본 발명은 이에 한정되는 것은 아니며, 적어도 하나 이상의 인터넷 서비스 제공자 망을 포함하는 네트워크에 적용될 수 있다.

[0021] 봇넷 탐지 시스템은 인터넷 서비스 제공자 망에 마련되어 트래픽 수집 센서에서 수집된 트래픽 정보를 기초로 해당 인터넷 서비스 제공자 망에서 활동하는 봇넷을 탐지한다. 이러한 봇넷 탐지 시스템은 도 2에 도시된 바와 같이 트래픽 정보 수집 센서와, 트래픽 정보 수집 센서에서 수집된 트래픽 정보에 의해 봇넷을 탐지하는 봇넷 탐지 시스템과, 트래픽 정보 수집 센서와 봇넷 탐지 시스템의 설정 및 상태 정보를 관리하는 관리 시스템을 포함한다.

[0022] 트래픽 수집 센서는 봇넷 탐지를 위해 해당 인터넷 서비스 제공자 망의 트래픽을 수집한다. 이때, 트래픽 수집 센서는 해당 인터넷 서비스 제공자 망에 봇넷 탐지 시스템의 개수(m)×해당 봇넷 탐지 시스템에 구비된 트래픽 수집 센서의 개수(n)개 만큼 존재할 수 있다. 또한, 이러한 트래픽 수집 센서는 봇넷 관제 및 보안관리 시스템에서 설정한 수집 정책에 따라 도메인 네임 시스템(Domain Name System, DNS) 트래픽과 트래픽 정보 등을 수집한다. 이때, 수집된 트래픽 정보는 주기적으로 봇넷 탐지 시스템에 전송된다.

[0023] 봇넷 탐지 시스템은 트래픽 수집 센서에서 수집된 특정 트래픽을 기초로 봇넷을 탐지한다. 이러한 봇넷 탐지 시스템은 해당 인터넷 서비스 제공자 망에 m개 존재할 수 있다. 또한, 수집된 트래픽 정보를 이용하여 봇넷을 탐지하고 악성행위를 분석한다. 탐지된 봇넷 정보는 봇넷 관제 및 보안 관리시스템으로 전송된다. 한편, 상기 트래픽 수집 센서와 봇넷 탐지 시스템의 정책은 관리 시스템에서 설정될 수 있다.

[0024] 호스트레벨 능동형 봇 감염 탐지 시스템은 독립적으로 설치된 시스템으로서, 능동적으로 감염된 악성 봇을 분석하여 봇넷이 사용하는 봇 정보를 제공한다.

[0025] 봇넷 관제 및 보안관리 시스템(Botnet Management Security Management, BMSM)은 해당 인터넷 서비스 제공자 망의 봇넷 정보를 시각화하며 대응 정책을 설정할 수 있는 기능을 제공한다. 이때, 일반적으로 봇넷 관제 및 보안관리 시스템은 인터넷 서비스 제공자 망에 한 개가 존재한다. 이러한 봇넷 관제 및 보안관리 시스템(Botnet Management Security Management, BMSM)은 도 3에 도시된 바와 같이, 봇넷 대응, 봇넷 정보 통계 리포팅, 시스템 관리, 봇넷 구조/악성행위 시각화, 정책 관리를 위한 인터페이스는 HTTP를 사용하여 관리자가 웹 브라우저를 통해 운영 할 수 있다.

[0026] 또한, 봇넷 관제 및 보안관리 시스템은 도 4와 도 5에 도시된 바와 같이, 보안 이벤트 관리 모듈(Security Event Collector, SEC)과, 예외 구성 로그 분석 모듈(Anomaly Organization Log Analysis, AOA)과, 미분류된 행동 로그 분석 모듈(Unclassified Behavior Log Analysis, UBA)과, 봇넷 대응 기술 모듈(Botnet Against Technology, BAT)과, 정적인 리포팅 관리 모듈(Statics Reporting Management, SRM)과, 봇넷 모니터링 모듈(Botnet Monitoring, BM)과, 탐지 로그 감독 모듈(Detection Log Management, DLM)과, 정책 감독 모듈(Policy Management, PM)과, 시스템 감독 모듈(System Management, SM)을 포함한다.

[0027] 도 6을 참조하면, 보안 이벤트 관리 모듈(Security Event Collector, SEC)은 다수의 탐지시스템으로부터 탐지로그와, 분류 행위로그 및 비정상 구성로그로 이루어진 보안 이벤트를 수신한다. 이때, 탐지로그는 봇넷 탐지시스

템에서 봇넷 구성 분석 수행 결과 탐지된 봇넷의 정보이며, 분류 행위로그는 봇넷 탐지시스템에서 봇넷 행위 분석 수행결과 탐지된 봇넷의 행위 정보이다. 또한, 비정상 구성로그는 봇넷 탐지 시스템에서 봇넷 구성 분석 수행 결과 유사도 값이 최소 임계값 이상이며 신뢰 임계값 이하인 경우 봇넷 관제 및 보안관리 시스템(Botnet Management Security Management, BMSM)으로 전송하는 로그이다. 로그의 분류는 보안 이벤트 메시지 헤더의 클래스(Class) 정보를 참고하여 분류할 수 있다. 이러한 보안 이벤트 관리 모듈(Security Event Collector, SEC)은 수집/분류/정책생성관리 모듈과 보안 이벤트 수집 분류 모듈과 대응 정책 체크 모듈 및 버퍼를 포함한다. 이때, 버퍼는 비정상 구성로그 버퍼와 미분류 행위로그 버퍼를 포함한다.

[0028] 보안 이벤트 수집 분류 모듈은 수집한 보안 이벤트를 분류하여 탐지로그와 분류 행위로그는 대응 정책 체크 모듈로 전달하고, 비정상 구성로그는 비정상 구성로그 버퍼에 저장한다.

[0029] 대응 정책 체크 모듈은 탐지로그와 분류 행위로그를 봇넷 정보 데이터베이스(Botnet Information Database, BIDB) 또는 봇넷 행위 데이터베이스(Botnet Behavior Database, BBDB)에 저장한다. 또한, 정책 감독 모듈(Policy Management, PM)이 설정한 정책에 따라 자동 대응이 필요한 경우 봇넷 C&C 접근 차단 또는 봇넷 악성행위 차단을 위한 대응 정책 요청 메시지를 봇넷 대응 기술 모듈(Botnet Against Technology, BAT)로 전송한다. 이때, 정책 감독 모듈(Policy Management, PM)은 탐지 로그에 대해 자동 대응 여부를 설정할 수 있다.

[0030] 한편, 도 7을 참조하면, SEC의 메시지 처리는 탐지 로그/분류 행위로그 처리와 비정상 구성로그를 버퍼에 저장하는 것으로 구분되며, PM이 설정한 '탐지 정보에 대한 자동 대응 정책 생성'에 따라 대응 정책을 설정될 수 있다.

[0031] 도 8을 참조하면, 탐지로그 처리는 보안 이벤트로부터 분류한 탐지로그는 봇넷 정보 데이터베이스(BIDB) 또는 봇넷 행위 데이터베이스(BBDB)에 저장한다. 이때, 데이터베이스 저장 후 탐지 정보에 대한 '자동 대응 정책 설정'기능이 온(on)되어 있을 경우 봇넷 C&C 접근 차단 대응 정책이 존재하는지 검사한다. 봇넷 C&C 접근 차단 정책이 존재하지 않을 경우 봇넷 C&C 접근 차단 대응 정책 설정 요청 메시지를 생성하여 BAT로 전송한다. 이때, 봇넷 C&C 접근 차단 정책은 도메인 네임 시스템 싱크홀, 웹 방화벽을 이용한 C&C URL 접근 차단이 있다.

[0032] 분류 행위로그 처리는 보안 이벤트로부터 분류한 분류 행위로그는 봇넷 행위 데이터베이스(BBDB)에 저장한다. 또한, 이와 같이 데이터베이스를 저장한 후 분류 행위로그에 대한 '자동 대응 정책 설정'기능이 온(on)되어 있을 경우 봇넷 악성행위 대응 정책이 존재하는지 검사한다. 봇넷 악성행위에 대한 대응 정책이 존재하지 않을 경우 봇넷 악성행위 대응 정책 설정 요청 메시지를 생성하여 BAT로 전송한다.

[0033] 도 9를 참조하면, 비정상 구성로그 처리는 보안 이벤트로부터 분류한 비정상 구성로그는 비정상 구성로그 버퍼에 저장하며, 미분류 행위로그 처리는 보안 이벤트로부터 분류한 미분류 행위로그는 미분류 행위로그 버퍼에 저장한다.

[0034] 도 10을 참조하면, 예외 구성 로그 분석 모듈(Anomaly Organization Log Analysis, AOA)은 탐지시스템은 도메인 유사도와 IP/Port 유사도 및 URL(Uniform Resource Locator) 유사도의 분석 결과 유사도가 최소 임계치 이상이며 신뢰 임계치 미만인 비정상 로그를 봇넷 관제 및 보안관리 시스템(Botnet Management Security Management, BMSM)으로 전송한다. 이때, 봇넷 관제 및 보안관리 시스템(Botnet Management Security Management, BMSM)은 다수의 탐지 시스템으로부터 비정상 로그를 취합하여 분석한다. 이러한 예외 구성 로그 분석 모듈은 비정상 구성로그 검색/분류 모듈과 봇넷 C&C 비교 모듈과 C&C 분석 및 탐지 모듈과 C&C 추출 모듈과 대응 정책 설정 모듈을 포함한다.

[0035] 비정상 구성로그 검색/분류 모듈은 비정상 구성로그 버퍼를 주기적으로 읽어 동일 타임 슬롯내에서 발생된 구성로그를 Dst 도메인, Dst IP/Port 또는 Dst hash별로 소스 IP들을 매트릭스에 기록한다.

[0036] 봇넷 C&C 비교 모듈은 현대 타임 슬롯내의 봇넷 C&C와 바로 전 타임 슬롯의 봇넷 C&C 정보를 비교한다. 이때, 현재 타임 슬롯내에 발생된 로그들 중 바로 전 타임 슬롯에 존재하지 않는 봇넷 C&C는 삭제하는 것이 바람직하다.

[0037] C&C 분석 및 탐지 모듈은 현재 타임 슬롯과 바로 전 타임 슬롯에 존재하는 봇넷 C&C의 소스 IP들을 대상으로 유사도를 분석한다. 이때, 이러한 유사도 분석은 도메인 유사도 분석과 IP/Port 유사도 분석 및 URL 유사도 분석을 포함한다.

[0038] 도메인 유사도 분석은 도메인별로 쿼리를 한 소스 IP들을 매트릭스에 기록한 후 특정 시간이 지난 후 매트릭스를 분석하여 유사도를 측정한다. 또한, 이와 같이 유사도를 분석한 후 좀비 IP 리스트를 생성한다. 이때, 좀비

는 봇넷에 감염된 컴퓨터를 의미한다.

[0039] IP/Port 유사도 분석은 DST_IP/Port 정보를 읽어 각 IP/Port 조합과 매칭되는 패킷을 전송한 소스 IP들을 매트릭스에 기록한다. 또한, 특정 시간이 지난 후 매트릭스를 분석하여 유사도를 측정하며, 이에 따라 좀비 IP 리스트를 생성한다.

[0040] URL 유사도 분석은 DST_URL 정보를 읽어 각 URL별 쿼리를 한 소스 IP들을 매트릭스에 기록한다. 또한, 특정 시간이 지난 후 매트릭스를 분석하고 유사도를 측정하며, 이에 따라 좀비 IP 리스트를 생성한다.

[0041] C&C 추출 모듈은 C&C 분석 및 탐지 모듈에서 탐지된 봇넷 트래픽을 전송받아 프로토콜별 C&C를 추출하여 분석결과를 로그에 저장한다. 이때, 분석을 마친 트래픽은 다시 좀비 리스트 추출 모듈로 전송한다.

[0042] 대응 정책 설정 모듈은 봇넷 관제 및 보안관리 시스템(Botnet Management Security Management, BMSM)에서 신규 탐지된 봇넷 C&C에 대한 정보를 탐지시스템으로 전송하기 위해 '블랙리스트 생성 대응 정책' 설정 요청 메시지를 생성한다.

[0043] 한편, 도 11을 참조하면, 예외 구성 로그 분석 모듈(Anomaly Organization Log Analysis, AOA)에서의 비정상 구성로그 처리는 주기적으로 비정상 구성 로그 버퍼를 검색하여 구현할 수 있다. 이때, 검색한 비정상 구성 로그가 현재 타임 엔트리(Time Entry)에 해당되지 않는다면 해당 구성 로그를 버퍼에서 삭제하는 것이 바람직하다. 이 경우, 현재 타임 엔트리에 해당되는 구성로그를 C&C 정보를 기반으로 분류한다. 이때, 분류 후 IP 카운트(Count)값이 임계값보다 클 경우 봇넷으로 탐지하며, 탐지된 봇넷 정보는 '블랙 리스트 공유 요청' 메시지를 생성하여 PM으로 전송된다.

[0044] 미분류된 행동 로그 분석 모듈(Unclassified Behavior Log Analysis, UBA)은 미분류 행위로그를 전달받아 이를 분류하고 대응 정책을 설정한다. 또한, 이를 위해 탐지시스템은 미분류된 행위 로그를 봇넷 관제 및 보안관리 시스템(Botnet Management Security Management, BMSM)으로 전송하고, 봇넷 관제 및 보안관리 시스템(Botnet Management Security Management, BMSM)은 다수의 탐지시스템으로부터 미분류 행위로그를 전달받아 분류를 수행한다.

[0045] 도 12를 참조하면, 봇넷 대응 기술 모듈(Botnet Against Technology, BAT)은 탐지된 봇넷에 대한 대응 정책을 수립한다. 또한, 탐지된 봇넷을 기초로 작성된 블랙리스트의 공유와, 도메인 네임 시스템 싱크홀의 적용과, BGP 피딩(Border Gateway Protocol feeding), 웹 방화벽을 이용한 HTTP 봇넷 C&C 접근 URL차단 등의 대응 정책을 수립한다. 이러한 대응 정책의 생성은 SEC, MMBOA, MMBBA, BIS, 관리 콘솔 그래픽 유저 인터페이스로부터 '봇넷 대응 정책 설정 요청'을 수집하여 실시될 수 있다. 또한, 이와 같이 대응 정책을 생성한 후 도메인 네임 시스템 서버와 BGP 라우터와 탐지 시스템 및 웹 방화벽 등과 같이 등록된 시스템으로 전송하는 역할을 수행한다. 이때, 봇넷 대응 기술 모듈(Botnet Against Technology, BAT)을 이용하여 설정할 수 있는 봇넷 대응 정책은 블랙리스트 공유, 도메인 네임 시스템 싱크홀, HTTP 봇넷 C&C URL 접근 차단, BGP 피딩을 포함한다.

[0046] 블랙리스트 공유는 SEC, MMBOA, MMBBA, BIS로부터 생성되는 봇넷 대응 정책으로서, 특정 AS(탐지 시스템이 관리하는 영역)와 짧은 시간에 다수의 좀비가 새로운 C&C에 접근하는 것이 발견될 경우 C&C에 대한 정보를 다른 AS의 탐지 시스템에게 공유한다.

[0047] 도메인 네임 시스템 싱크홀은 SEC와 MMBOA, BIS로부터 생성되는 봇넷 대응 정책으로서, 주로 IRC 기반의 봇넷 C&C 접근 차단을 위해 사용되는 대응 정책이다. 이때, 신규로 발견된 IRC 봇넷에 대한 접근 차단을 위해 도메인 네임 시스템 자원 레코드(Domain Name System Resource Record, DNS RR)를 생성하여 도메인 네임 시스템 서버로 전송한다.

[0048] HTTP 봇넷 C&C URL 접근 차단은 SEC와 MMBOA 및 BIS로부터 생성되는 봇넷 대응 정책으로서, 주로 HTTP 기반의 봇넷 C&C 접근 차단을 위해 사용되는 대응 정책이다. 이러한 좀비의 HTTP 봇넷 C&C URL 접근 차단은 공개 웹 방화벽의 룰 설정을 통해 구현될 수 있다.

[0049] BGP 피딩은 SEC와 MMBBA 및 BIS로부터 생성되는 봇넷 대응 정책으로서, 디도스(DDoS) 등의 봇넷을 이용한 공격 행위 차단을 위해 사용되는 대응 정책이다. 이러한 BGP 피딩에 의한 대응 정책에 의해 공격 대상(Victim)으로 가는 디도스(DDoS) 트래픽 등을 널 라우팅(Null Routing)을 통해 차단할 수 있다.

[0050] 한편, 도 13 및 도 14를 참조하면, 봇넷 대응 기술 모듈(Botnet Against Technology, BAT)에 의한 메시지 처리는 관리 콘솔 그래픽 사용자 인터페이스로부터의 봇넷 대응 정책 설정 요청 처리와 나머지 요청 처리로 구분될 수 있다. 이때, 관리 콘솔 그래픽 사용자 인터페이스로부터 봇넷 대응 정책 설정 요청은 대응 정책 설정 요청

검증을 수행하고 대응 정책을 생성한 후 등록된 시스템으로 전송한다.

[0051] 한편, 도 15를 참조하면, 봇넷 대응 정책 설정 요청 검증 메시지 처리는 대응 정책 타입에 따라 도메인 네임 시스템 자원 레코드(DNS RR) 검증, BGP 라우팅 룰 검증, 공개 웹 방화벽 기반 HTTP C&C URL 접근 차단 룰 검증으로 구분될 수 있다.

[0052] 도메인 네임 시스템 자원 레코드를 이용한 도메인 네임 시스템 싱크홀 대응 정책 검증은 도메인 네임 시스템 자원 레코드에 포함된 도메인 네임 시스템이 봇넷 정보 데이터베이스(BIDB)에 존재하는지 검사한다. 또한, 도메인 네임 자원 레코드를 적용할 도메인 네임 시스템 서버가 시스템 정보 데이터베이스에 존재하는지 검사한다.

[0053] BGP 라우팅 정책을 이용한 BGP 피딩 정책 검증은 BGP 라우팅 정책의 목적지 주소가 봇넷 행위 데이터베이스(BBDB)에 존재하는지 검사한다. 또한, BGP 라우팅 룰을 적용할 BGP 라우터가 시스템 정보 데이터베이스에 존재하는지 검사한다.

[0054] 공개 웹 방화벽을 이용한 HTTP 봇넷 C&C 접근 차단 정책 검증은 차단룰의 URL이 봇넷 정보 데이터베이스(BIDB)에 존재하는지 검사한다. 또한, 차단룰을 적용한 공개 웹 방화벽이 시스템 정보 데이터베이스에 존재하는지 검사한다.

[0055] 한편, 도 16에 도시된 바와 같이, 봇넷 대응 정책 검증은 관리 콘솔 그래픽 사용자 인터페이스로부터 대응 정책 생성 요청일 경우 수행하는 대응 정책 검증 프로세스를 관리자가 수동으로 수행할 수 있다. 이때, 대응 정책에 포함된 봇넷 정보 또는 시스템 정보가 실제 시스템 정보 데이터베이스에 등록된 것인지 확인이 필요하다.

[0056] 도메인 네임 시스템 싱크홀 정책 검증은 도메인 네임 자원 레코드에 포함된 C&C 도메인 네임이 봇넷 정보 데이터베이스에 존재하는지 체크하고, 이를 적용하고자 하는 도메인 네임 시스템 서버가 존재하는지 검사한다. BGP 피딩 정책 검증은 라우팅 정책에 포함된 IP 주소를 공격 대상(Victim)으로 하는 악성 행위가 존재하는지 체크하고, 적용하고자 하는 BGP 라우터가 존재하는지 검사한다. HTTP C&C 접근 차단 룰 검증은 룰 파싱 후 해당 URL을 C&C로 가지는 HTTP 봇넷이 존재하는지 체크하고, 적용하고자 하는 보안 장비가 존재하는지 검사한다. 물론, 블랙리스트 공유는 관리자가 직접 생성할 수 없으므로 검증 과정이 필요하지 않다.

[0057] 정적인 리포팅 관리 모듈(Statics Reporting Management, SRM)은 봇넷 정보 및 악성행위 정보를 다양한 그래프와 테이블 등과 같은 통계 데이터 생성한다. 또한, 생성된 통계 데이터에 대해서 리포팅 기능 제공하며, 이러한 정적인 리포팅 관리부는 웹 기반 사용자 인터페이스(User Interface, UI)를 통해서 사용할 수 있다.

[0058] 도 17을 참조하면, 봇넷 통계 시퀀스는 우선, 사용자가 메뉴에서 봇넷 통계를 선택([1])한다. 이후, 기본 검색 조건을 기간'최근 일주일'로 하여 봇넷 정보 데이터베이스에 쿼리하고 결과를 수집([2])한다. 수집한 봇넷 통계(봇넷 타입, 봇넷 C&C 도메인 네임, IP 주소, 보유 좀비 수 등)를 추이 그래프로 표시하고 내림차순 정렬하여 화면에 표시([3])한다. 사용자는 통계 항목의 검색 조건(통계 영역, 봇넷 타입, C&C 도메인 네임, 도메인 IP, 포트 번호, 악성 행위 등)을 활용하여 해당 통계를 요청([4])한다. 사용자가 선택한 검색 조건을 봇넷 정보 데이터베이스와 악성행위 데이터베이스로 쿼리하여 정보를 수집([5])하고, 이에 대한 결과를 화면에 표시([6])한다.

[0059] 도 18을 참조하면, 봇넷 좀비 통계 시퀀스는 우선, 사용자가 메뉴에서 봇넷 좀비 통계를 선택([1])한다. 이후, 기본 검색 조건을 기간'최근 일주일'로 하여 봇넷 정보 데이터베이스에 쿼리하고 결과를 수집([2])한다. 수집한 봇넷 통계(봇넷 타입, 봇넷 C&C 도메인 네임, IP 주소, 사용 봇 바이너리, 악성행위 등)를 추이 그래프로 표시하고 내림차순 정렬하여 화면에 표시([3])한다. 사용자는 통계 항목의 검색 조건(봇넷 타입, 봇넷 C&C 도메인 네임, 좀비 IP 주소, 사용 봇 바이너리, 악성행위 등)을 활용하여 해당 통계를 요청([4])한다. 사용자가 선택한 검색 조건을 봇넷 정보 데이터베이스와 악성행위 데이터베이스로 쿼리하여 정보를 수집([5])하고, 이에 대한 결과를 화면에 표시([6])한다.

[0060] 도 19를 참조하면, 도메인 네임 시스템 싱크홀 트래픽 통계 시퀀스는 우선, 사용자가 메뉴에서 도메인 네임 시스템 싱크홀 유입 트래픽 통계를 선택([1])한다. 이후, 기본 검색 조건을 기간'최근 일주일'로 하여 봇넷 정보 데이터베이스에 쿼리하고 결과를 수집([2])한다. 수집한 도메인 네임 시스템 싱크홀 서버 트래픽을 추이 그래프와 표 형태로 화면에 표시([3])한다. 사용자는 통계 항목의 검색 조건(소스 IP)을 활용하여 해당 통계를 요청([4])한다. 사용자가 선택한 검색 조건을 봇넷 정보 데이터베이스로 쿼리하여 정보를 수집([5])하고, 이에 대한 결과를 화면에 표시([6])한다.

[0061] 도 20을 참조하면, 통합 보고서 시퀀스는 우선, 사용자가 메뉴에서 통합 보고서를 선택([1])한다. 이는 통합 보

고서의 이름, 형식, 기간, 보고서 종류 등을 선택하여 보고서 생성을 클릭함으로써 수행할 수 있다. 사용자가 선택한 검색 조건에 따라 봇넷 정보 데이터베이스와 악성행위 정보 데이터베이스를 쿼리하여 결과를 수집([2])한다. 해당 보고서를 생성하여 보고서 테이블에 결과를 기록([3])하고 생성된 보고서를 사용자의 화면에 표시([4])한다.

[0062] 도 21을 참조하면, 보고서 예약 시퀀스는 우선, 사용자가 메뉴에서 보고서 예약을 선택([1])한다. 예약 보고서 리스트 데이터베이스를 쿼리하여 예약 보고서 리스트 결과를 읽고([2]), 이를 화면에 표시([3])한다. 이후, 사용자가 예약 등록을 선택([4])하면 예약등록 화면이 화면에 표시([5])된다. 예약 등록 화면에서 예약할 보고서의 종류를 선택하고, 보고서 이름과 보고서의 확장자 및 기간 등을 선택하고 보고서 예약 버튼을 선택([6])한다. 예약 보고서 리스트 데이터베이스에 해당 보고서 정보를 저장([7])하고 예약 보고서 리스트를 화면에 표시([8])한다. 예약된 시간이 되면 봇넷 정보 데이터베이스와 악성 행위 데이터베이스 등에 쿼리하여 정보를 수집하고 보고서 데이터베이스에 해당 보고서를 생성한 후 저장([9])한다.

[0063] 봇넷 모니터링 모듈(Botnet Monitoring, BM)은 봇넷 구조 및 악성행위를 쉽게 확인 할 수 있는 모니터링 기능을 제공한다. 또한, 생성된 통계 데이터에 대해서 리포팅 기능을 제공한다.

[0064] 이러한 봇넷 모니터링 모듈(Botnet Monitoring, BM)은 도 22 및 도 23에 도시된 바와 같이, 사용자가 시스템을 시작([1])하면 C&C 지도 화면과 C&C와 관련된 모든 정보인 C&C 리스트를 요청([2])한다. 또한, 봇넷 정보 데이터베이스에 C&C 정보를 쿼리([3])하며, 타 인터넷 서비스 제공자 망에 존재하는 C&C와 좀비 정보(OtherISPList)를 수신([4][5])한다. 이때, 봇넷 정보 데이터베이스는 데이터베이스에 존재하는 C&C 정보(CCList)와 현재 인터넷 서비스 제공자 망인지 타 인터넷 서비스 제공자 망인지를 파악하여 이에 대한 정보를 전송([6])한다. 이후, 그래픽 사용자 인터페이스에 C&C 맵과 C&C 리스트를 출력([7])하고, 사용자가 맵에서 특정 C&C를 클릭([8])한다. 또한, 정책 감독 모듈(Policy Management, PM)에 해당 C&C(CC)의 좀비 지도와 좀비 리스트 및 대표 공격 유형 시각화를 요청([9])한다. 이때, 정책 감독 모듈(Policy Management, PM)은 봇넷 정보 데이터베이스에 해당 C&C(CC)의 좀비 정보를 요청([10])하며, 이에 따라 봇넷 정보 데이터베이스는 정책 감독 모듈(Policy Management, PM)에 좀비 정보를 전송([11])한다. 이후 정책 감독 모듈(Policy Management, PM)은 악성 행위 데이터베이스에 해당 좀비들의 공격 유형을 요청([12])하며, 악성 행위 데이터베이스는 해당 좀비들에 대한 공격 유형을 전송([13])한다. 또한, 이에 따라 봇넷 정보 데이터베이스는 정책 감독 모듈(Policy Management, PM)은 좀비 리스트와 공격 유형을 분석하여 가장 많이 사용된 공격 유형(HighZom)을 찾는다([14]). 이후 정책 감독 모듈(Policy Management, PM)은 가장 많이 사용된 공격 유형(HighZOm)에 해당하는 시각화를 시각화 정책 데이터베이스에 요청([15])하며, 이에 따른 시각화 정보(AttackVisual)를 전송([16])받는다. 또한, 이에 따라 그래픽 사용자 인터페이스 지도에 좀비들의 위치와 공격 유형과 좀비 리스트 및 대표 공격 유형을 시각화하여 출력([17])한다.

[0065] 도 24를 참조하면, 리프레쉬(Refresh)와 줌인(Zoom in)/줌아웃(Zoom out) 및 타이머(Timer) 시퀀스는 우선 관리자가 리프레쉬를 요청([1])하면, 정책 감독 모듈(Policy Management, PM)은 C&C 지도 화면과 C&C와 관련된 모든 정보인 C&C 리스트를 요청([2])한다. 또한, 봇넷 정보 데이터베이스에 C&C 정보를 쿼리([3])하며, 타 인터넷 서비스 제공자 망에 존재하는 C&C와 좀비 정보(OtherISPList)를 수신([4][5])한다. 이때, 봇넷 정보 데이터베이스는 데이터베이스에 존재하는 C&C 정보(CCList)와 현재 인터넷 서비스 제공자 망인지 타 인터넷 서비스 제공자 망인지를 파악하여 이에 대한 정보를 전송([6])한다. 이후, 그래픽 사용자 인터페이스에 C&C 맵과 C&C 리스트를 출력([7])하면, 사용자가 줌인/줌아웃을 요청([8])한다. 줌인/줌아웃(InOut)에 따라 사용자는 정책 감독 모듈(Policy Management, PM)에 새로운 봇넷 지도와 리스트를 요청([9])한다. 또한, 정책 감독 모듈(Policy Management, PM)은 InOut에 따라 사용자의 봇넷 지도와 리스트 범위를 변경([10])한다. 그래픽 사용자 인터페이스에 새로운 봇넷 지도와 리스트를 출력([11])한다. 사용자가 타이머 시간을 지정해서 요청([12])하며, 이에 따라 정책 감독 모듈(Policy Management, PM)에 시간(Start~End)에 해당하는 봇넷 지도와 리스트를 요청([13])한다. 정책 감독 모듈(Policy Management, PM)은 봇넷 정보 데이터베이스에 해당 시간에 해당하는 C&C 정보를 요청([14])한다. 또한, 정책 감독 모듈(Policy Management, PM)은 타 인터넷 서비스 제공자 망에 존재하는 C&C와 좀비 정보(OtherISPList)를 요청하고 이를 수신([15][16])한다. 봇넷 정보 데이터베이스는 데이터베이스에 존재하는 C&C 정보(CCList)와 현재 인터넷 서비스 제공자 망인지 타 인터넷 서비스 제공자 망인지를 파악하여 이에 대한 정보를 전송([17])한다. 이후, 그래픽 사용자 인터페이스에 C&C 맵과 C&C 리스트를 출력([18])한다.

[0066] 도 25를 참조하면, 정적인 리포팅 관리 모듈(Statics Reporting Management, SRM)의 TOP N 통계 시퀀스는 우선, 사용자가 메뉴에서 TOP N 통계를 선택([1])한다. 이후 기본 검색 조건을 기간 '최근 일주일'로 하여 봇넷 정보 데이터베이스에 쿼리하고 결과를 수집([2])한다. 수집한 봇넷 통계(봇넷 타입, 봇넷 C&C 도메인 네임, 보

유 좀비 수 등)를 내림 차순 정렬로 화면에 표시([3])한다. 사용자는 통계 항목의 검색 조건을 활용하여 해당 통계를 요청([4])하고, 사용자가 선택한 검색 조건을 봇넷 정보 데이터베이스와 악성 행위 데이터베이스로 쿼리하여 정보를 수집([5])한다. 이후, 이에 따른 검색 결과를 화면에 표시([6])한다.

[0067] 도 26을 참조하면, 탐지 로그 감독 모듈(Detection Log Management, DLM)은 봇넷 정보, 봇넷 악성행위 정보, 시스템 정보, 정책 정보, 봇넷 대응 정책 정보 등을 관리하기 위한 프로세서이다. 또한, 탐지 로그 감독 모듈(Detection Log Management, DLM)은 SM, BAT, SRM, BM, PM으로부터 장비 정보 데이터베이스, 봇넷 대응 정보 데이터베이스, 봇넷 정보 데이터베이스, 악성행위 데이터베이스, 정책 데이터베이스 등으로의 로그 삽입/삭제/수정/검색 등의 요청을 받아 결과를 돌려주는 기능을 수행한다. 이러한 탐지 로그 감독부(Detection Log Management, DLM)는 데이터베이스와의 커넥션을 관리하는 커넥션 풀과 쿼리 분류와 조회/삽입/삭제/수정, 중복체크, SQL문 생성/전송 모듈로 구성된다.

[0068] 커넥션 풀(Connection Pool) 모듈은 DB와의 커넥션을 관리하고 있는 버퍼로써, 미리 데이터베이스 커넥션을 생성하여, 데이터베이스 접속(Connection) 요청 시 할당을 수행한다.

[0069] 쿼리 분류 모듈은 탐지 로그 감독부(Detection Log Management, DLM)로의 요청을 분류하여 조회, 삽입, 삭제,수정 모듈로 전달하는 기능을 수행한다. 또한, 조회/삽입/삭제/수정 모듈은 데이터베이스로의 조회/삽입/삭제/수정 요청을 담당한다.

[0070] 중복체크 모듈은 조회/삽입/삭제/수정 모듈에서 데이터베이스로의 삽입 요청과 수정 요청에 대한 중복 여부를 체크한다. 또한, SQL문 생성/전송 모듈은 요청 메시지를 전달 받아 SQL문을 생성하여, 전송하는 기능을 수행하며, 결과 전송 모듈은 생성된 SQL문을 전송 한 후, 응답 받은 결과를 리턴해 주는 기능을 수행한다.

[0071] 정책 감독 모듈(Policy Management, PM)은 봇넷 관제 및 보안관리 시스템(Botnet Management Security Management, BMSM) 내부에서 실행되고 있는 모듈에 대한 정책을 설정한다. 또한, 정책 감독부는 봇넷 관제 및 보안관리 시스템(Botnet Management Security Management, BMSM)에 등록된 탐지시스템의 탐지 정책을 설정한다. 또한, 등록된 탐지 시스템을 통한 트래픽 수집 센서 정책을 설정한다.

[0072] 도 27을 참조하면, 시스템 감독 모듈(System Management, SM)은 탐지시스템, 트래픽 수집센서, 도메인 네임 시스템 싱크홀 서버, BGP 라우터, 도메인 네임 시스템 서버, 웹 방화벽 등을 봇넷 관제 및 보안관리 시스템(Botnet Management Security Management, BMSM)에 등록하는 기능을 제공한다. 또한, 등록된 탐지 시스템, 트래픽 수집센서에 대한 모니터링 및 온/오프 기능을 제공한다. 이러한 시스템 감독 모듈(System Management, SM)은 관리자가 접근해서 사용하는 웹 사용자 인터페이스와 시스템 감독 프로세스로 구성된다. 또한, 시스템 감독 모듈(System Management, SM)은 웹 사용자 인터페이스를 통해 시스템의 등록, 수정, 삭제를 수행하고, 등록된 트래픽 수집 센서와 탐지 시스템에 대한 모니터링 및 환경설정을 수행한다. 시스템 감독 프로세서는 다수의 트래픽 수집 센서 또는 탐지 시스템으로부터 전송된 상태 정보(on/off, cpu usage 등)를 수신하여 처리 하는 상태 정보 처리 기능과 관리 콘솔 그래픽 사용자 인터페이스로부터 상태 정보 조회 요청을 처리한다.

[0073] 상태 정보 처리는 트래픽 수집 센서 또는 탐지 시스템은 상태 정보를 봇넷 관제 및 보안관리 시스템(Botnet Management Security Management, BMSM)로 주기적으로 전송한다. 이때, 시스템 감독 모듈(System Management, SM)은 IP 필터 기능을 사용하여 등록된 트래픽 수집 센서 및 탐지 시스템으로 부터의 정보만 수신한다. 또한, 수신된 상태 정보 메시지는 상태 메시지 수집/분류를 거친 후, 상태정보 저장 버퍼로 저장한다.

[0074] 관리 콘솔 그래픽 사용자 인터페이스로부터 상태 정보 조회 요청 처리는 관리 콘솔 그래픽 사용자 인터페이스는 관리자의 요청에 따라 등록된 트래픽 수집 센서 또는 탐지 시스템의 상태 정보 요청한다. 시스템 감독 모듈(System Management, SM)은 상태 정보 요청 메시지를 전달 받아 상태 정보 저장 버퍼에 저장된 상태 정보를 조회한다.

[0075] 상술한 바와 같이 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템은 봇넷 관제 및 보안 관리 시스템을 이용하여 IRC와 HTTP 봇넷의 보안 관제를 효율적으로 관리할 수 있다.

[0076] 다음은 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 방법에 대해 도면을 참조하여 간략히 설명하고자 한다. 후술할 내용 중 전술된 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 설명과 중복되는 내용은 생략하거나 간략히 설명하기로 한다. 이때, 후술할 내용의 각 단계에 대한 상세한 설명은 전술된 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템에서 기술되었으므로 생략하기로 한다.

[0077] 도 28은 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 방법을 설명하기 위한 순서도이다.

[0078] 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 방법은 도 28에 도시된 바와 같이, 봇넷을 탐지하는 단계(S_1)와, 대응 정책을 수립하는 단계(S_2)와, 통계 데이터를 작성하는 단계(S_3)를 포함한다.

[0079] 봇넷을 탐지하는 단계(S_1)는 다수의 인터넷 서비스 제공자 망 각각에서 봇넷을 탐지한다. 이러한 봇넷을 탐지하는 단계는 트래픽을 수집하는 단계(S_{1-1})와, 로그를 분류하는 단계(S_{1-2})와, 로그를 처리하는 단계(S_{1-3})를 포함한다.

[0080] 트래픽을 수집하는 단계(S_{1-1})는 다수의 인터넷 서비스 제공자 망 각각에서 트래픽을 수집한다. 이를 위해 다수의 인터넷 서비스 제공자 망에는 트래픽 수집 센서가 구비되며, 봇넷 관제 및 보안관리 시스템에서 설정한 트래픽 수집 정책에 따라 도메인 네임 시스템 트래픽과 트래픽 정보 등을 수집한다. 이때, 상기 트래픽 수집 정책은 예를 들어, 특정 서버에 집중적으로 접속하는 중앙집중형 접속 특성을 갖는 트래픽 등과 같이 특정한 특성을 보이는 트래픽일 수 있다.

[0081] 로그를 분류하는 단계(S_{1-2})는 수집된 트래픽의 보안 이벤트를 분류한다. 이때, 분류된 보안 이벤트는 탐지 로그와 분류 행위 로그와 비정상 구성 로그 및 미분류 행위 로그를 포함한다.

[0082] 로그를 처리하는 단계(S_{1-3})는 트래픽을 수집하는 단계에서 수집된 트래픽의 로그를 분석한다. 이러한 로그를 분석하는 단계는 탐지로그를 처리하는 단계(S_{1-3-1})와, 분류 행위 로그를 처리하는 단계(S_{1-3-2})와, 비정상 구성 로그를 처리하는 단계(S_{1-3-3})와, 미분류 행위로그를 처리하는 단계(S_{1-3-4})를 포함한다.

[0083] 탐지로그를 처리하는 단계(S_{1-3-1})는 보안 이벤트로부터 분류한 탐지 로그를 봇넷 정보 데이터베이스에 저장한다. 이후, 탐지 정보에 대한 '자동 대응 정책 설정'기능이 온되어 있을 경우 봇넷 C&C 접근 차단 대응 정책이 존재하는지 검사한다. 이때, 봇넷 C&C 접근 차단 정책이 존재하지 않을 경우 봇넷 C&C 접근 차단 대응 정책 설정 요청 메시지를 생성하여 봇넷 대응 기술 모듈로 전송한다.

[0084] 분류 행위 로그를 처리하는 단계(S_{1-3-2})는 보안 이벤트로부터 분류한 분류 행위 로그를 봇넷 행위 데이터베이스에 저장한다. 이후, 분류 행위 로그에 대한 '자동 대응 정책 설정'기능이 온되어 있을 경우 봇넷 악성행위 대응 정책이 존재하는지 검사한다. 이때, 봇넷 악성행위에 대한 대응 정책이 존재하지 않을 경우, 봇넷 악성행위 대응 정책 설정 요청 메시지를 생성하여 봇넷 대응 기술 모듈로 전송한다.

[0085] 비정상 구성 로그를 처리하는 단계(S_{1-3-3})는 보안 이벤트로부터 분류한 비정상 구성로그를 비정상 구성로그 버퍼에 저장한다. 또한, 예외 구성 로그 분석부는 주기적으로 비정상 구성 로그 버퍼를 검색하며, 검색한 비정상 구성 로그가 현재 타임 엔트리에 해당되지 않는다면 해당 구성 로그를 버퍼에서 삭제한다. 또한, 현재 타임 엔트리에 해당되는 구성로그를 C&C 정보를 기반으로 하여 분류한다. 이후, IP 카운트 값이 임계값보다 클 경우 봇넷으로 탐지하며, 탐지된 봇넷 정보는 '블랙 리스트 공유 요청'메시지를 생성하여 정책 감독 모듈에 전송한다.

[0086] 미분류 행위로그를 처리하는 단계(S_{1-3-4})는 보안 이벤트로부터 분류한 미분류 행위로그를 미분류 행위로그 버퍼에 저장한다.

[0087] 대응 정책을 수립하는 단계(S_3)는 타 인터넷 서비스 제공자 망의 봇넷 관제 및 보안관리 시스템에서 탐지된 봇넷 정보를 수신하고 이를 토대로 대응 정책을 수립한다. 상기 대응 정책은 봇넷 대응 기술 모듈에 의해 구현될 수 있다. 이때, 상기 대응 정책은 봇넷으로 판명된 블랙 리스트의 공유, 도메인 네임 시스템 싱크홀 적용, BGP 피딩, 웹방화벽을 이용한 HTTP 봇넷 C&C 접근 URL 차단 등을 포함할 수 있다.

[0088] 통계 데이터를 작성하는 단계(S_4)는 봇넷 정보 및 악성행위 정보를 다양한 그래프와 테이블 등과 같은 통계 데이터로 작성한다. 이때, 생성된 통계 데이터에 대해서 리포팅할 수 있으며, 이러한 통계 데이터의 작성 및 리포팅은 웹 기반 사용자 인터페이스를 통해 구현될 수 있다.

[0089] 이상에서는 도면 및 실시예를 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 하기의 특허청구범위에 기재된 본 발명의 기술적 사상으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

도면의 간단한 설명

[0090] 도 1은 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 구성도이다.

[0091] 도 2는 본 발명에 따른 IRC와 HTTP 봇넷 정보 공유 시스템의 봇넷 탐지 시스템의 구성도이다.

[0092] 도 3은 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 스택이다.

[0093] 도 4는 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 봇넷 관제 및 보안관리 시스템의 개념도이다.

[0094] 도 5는 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 봇넷 관제 및 보안관리 시스템의 구성도이다.

[0095] 도 6은 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 보안 이벤트 관리 모듈의 구성도이다.

[0096] 도 7은 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 보안 이벤트 관리 모듈을 설명하기 위한 순서도이다.

[0097] 도 8은 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 탐지/분류 행위로그 처리에 대한 SEC 시퀀스 다이어그램이다.

[0098] 도 9는 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 비정상 구성로그 처리에 대한 SEC 시퀀스 다이어그램이다.

[0099] 도 10은 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 AOA의 구성도이다.

[0100] 도 11은 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 AOA를 설명하기 위한 순서도이다.

[0101] 도 12는 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 BAT의 구성도이다.

[0102] 도 13은 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 BAT를 설명하기 위한 순서도이다.

[0103] 도 14는 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 BAT 시퀀스 다이어그램이다.

[0104] 도 15는 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 봇넷 대응 정책 설정 요청 검증의 순서도이다.

[0105] 도 16은 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 봇넷 대응 정책 설정 요청 검증의 구성도이다.

[0106] 도 17은 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 봇넷 통계 시퀀스 다이어그램이다.

[0107] 도 18은 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 봇넷 좀비 통계 시퀀스 다이어그램이다.

[0108] 도 19는 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 도메인 네임 시스템 싱크홀 트래픽 통계 시퀀스 다이어그램이다.

[0109] 도 20은 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 통합 보고서 시퀀스 다이어그램이다.

[0110] 도 21은 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 보고서 예약 시퀀스 다이어그램이다.

[0111] 도 22는 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 초기화면 및 봇넷 C&C 클릭에 대한 시퀀스 다이어그램이다.

[0112] 도 23은 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 BM의 구성도이다.

[0113] 도 24는 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 리프레쉬와 줌인/줌아웃 및 타이머 시퀀스 다이어그램이다.

[0114] 도 25는 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 TOP N 통계 시퀀스 다이어그램이다.

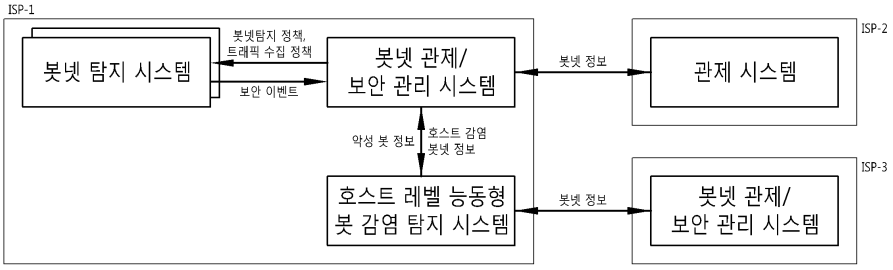
[0115] 도 26은 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 DLM의 구성도이다.

[0116] 도 27은 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 시스템의 SM의 구성도이다.

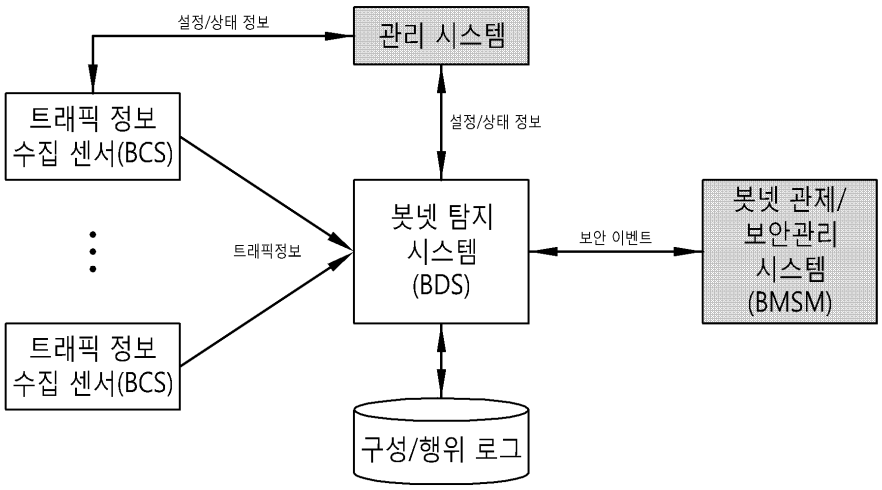
[0117] 도 28은 본 발명에 따른 IRC 및 HTTP 봇넷 보안 관제를 위한 관리 방법을 설명하기 위한 순서도이다.

도면

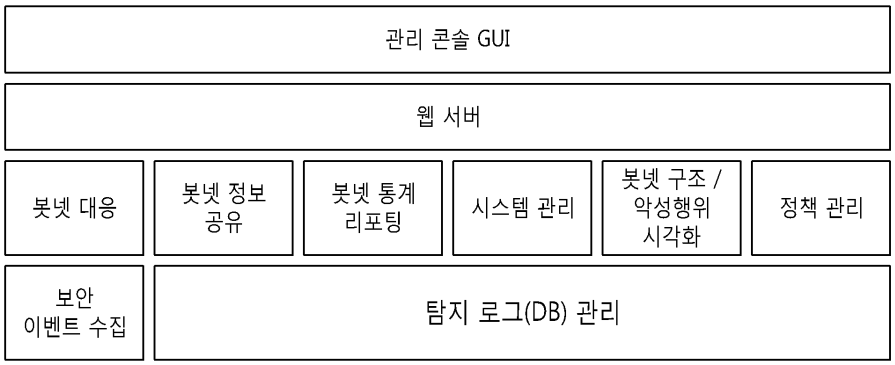
도면1



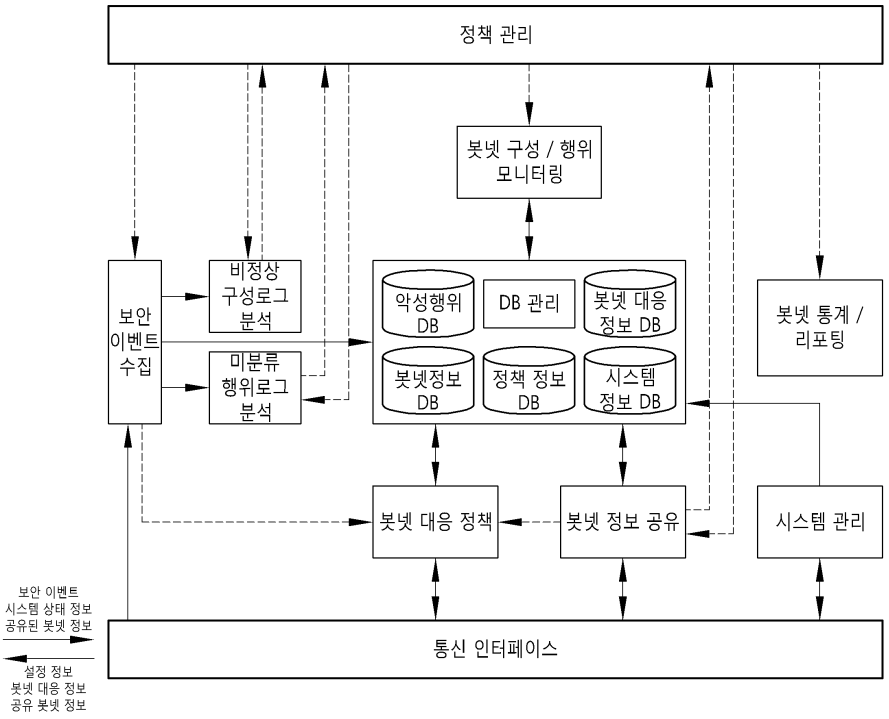
도면2



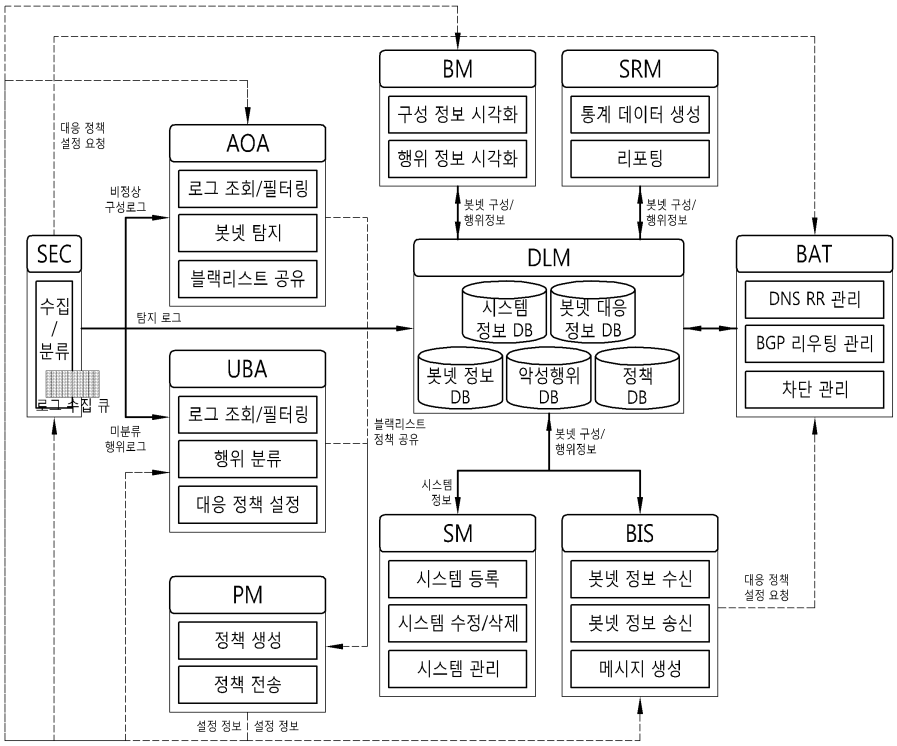
도면3


관리 콘솔 GUI
웹 서버
봇넷 대응
봇넷 정보 공유
봇넷 통계 리포팅
시스템 관리
봇넷 구조 / 악성행위 시각화
정책 관리
보안 이벤트 수집
탐지 로그(DB) 관리

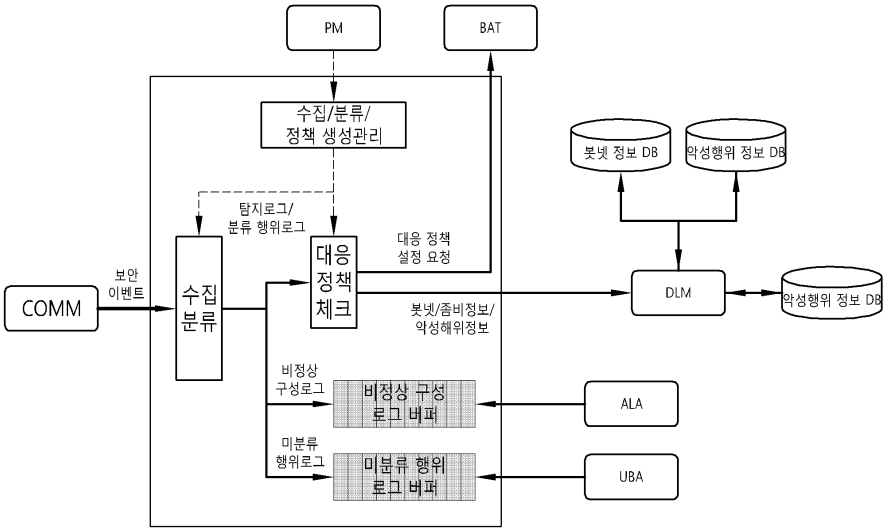
도면4


정책 관리
봇넷 구성 / 행위 모니터링
보안 이벤트 수집
비정상 구성로그 분석
미분류 행위로그 분석
악성행위 DB
DB 관리
봇넷 대응 정보 DB
봇넷정보 DB
정책 정보 DB
시스템 정보 DB
봇넷 통계 / 리포팅
봇넷 대응 정책
봇넷 정보 공유
시스템 관리
통신 인터페이스
보안 이벤트
시스템 상태 정보
공유된 봇넷 정보
설정 정보
봇넷 대응 정보
공유 봇넷 정보

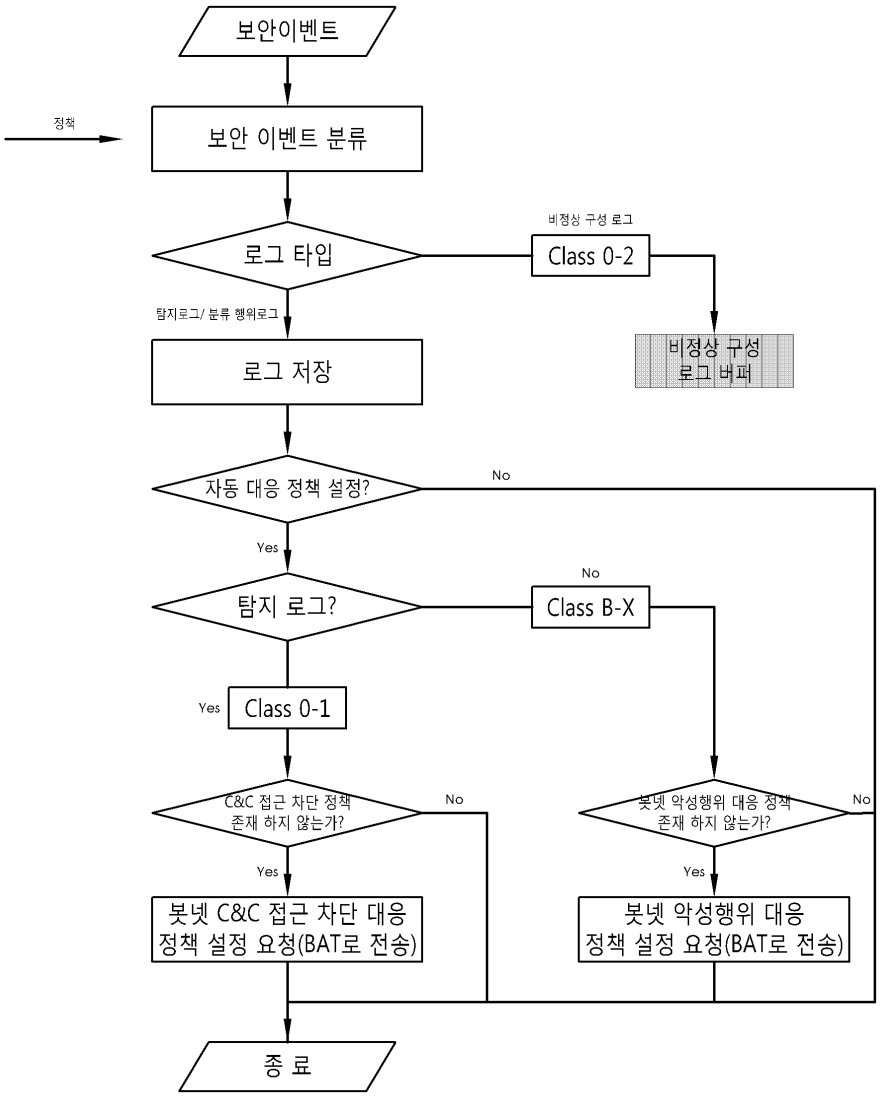
도면5


BM
구성 정보 시각화
행위 정보 시각화
SRM
통계 데이터 생성
리포팅
대응 정책 설정 요청
AOA
로그 조회/필터링
봇넷 탐지
블랙리스트 공유
비정상 구성로그
봇넷 구성/행위정보
봇넷 구성/행위정보
SEC
수집 / 분류
로그 수집 큐
탐지 로그
DLM
시스템 정보 DB
봇넷 대응 정보 DB
봇넷 정보 DB
악성행위 DB
정책 DB
BAT
DNS RR 관리
BGP 리우팅 관리
차단 관리
UBA
로그 조회/필터링
행위 분류
대응 정책 설정
미분류 행위로그
블랙리스트 정책 공유
봇넷 구성/행위정보
시스템 정보
SM
시스템 등록
시스템 수정/삭제
시스템 관리
BIS
봇넷 정보 수신
봇넷 정보 송신
메시지 생성
대응 정책 설정 요청
PM
정책 생성
정책 전송
설정 정보
설정 정보

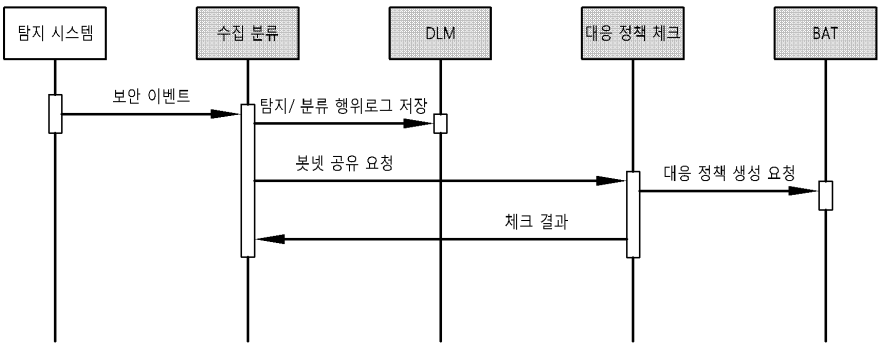
도면6


PM
BAT
수집/분류/ 정책 생성관리
봇넷 정보 DB
악성행위 정보 DB
탐지로그/ 분류 행위로그
대응 정책 설정 요청
보안 이벤트
COMM
수집 분류
대응 정책 체크
DLM
악성행위 정보 DB
봇넷/좀비정보/ 악성해위정보
비정상 구성로그
비정상 구성 로그 버퍼
ALA
미분류 행위로그
미분류 행위 로그 버퍼
UBA

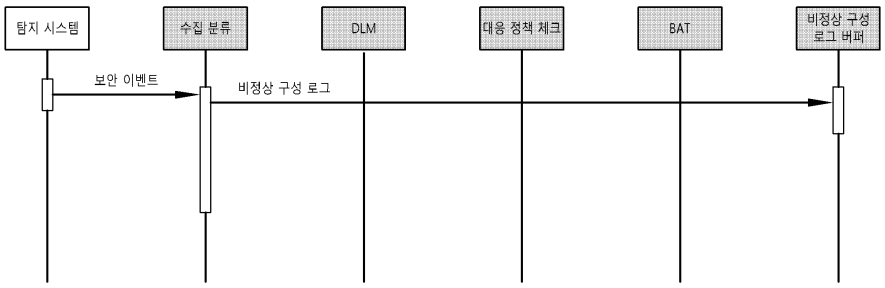
도면7


보안이벤트
정책
보안 이벤트 분류
로그 타입
비정상 구성 로그
Class 0-2
비정상 구성
로그 버퍼
탐지로그/ 분류 행위로그
로그 저장
자동 대응 정책 설정?
No
Yes
탐지 로그?
No
Class B-X
Yes
Class 0-1
C&C 접근 차단 정책
존재 하지 않는가?
No
Yes
봇넷 C&C 접근 차단 대응
정책 설정 요청(BAT로 전송)
봇넷 악성행위 대응 정책
존재 하지 않는가?
No
Yes
봇넷 악성행위 대응
정책 설정 요청(BAT로 전송)
종 료

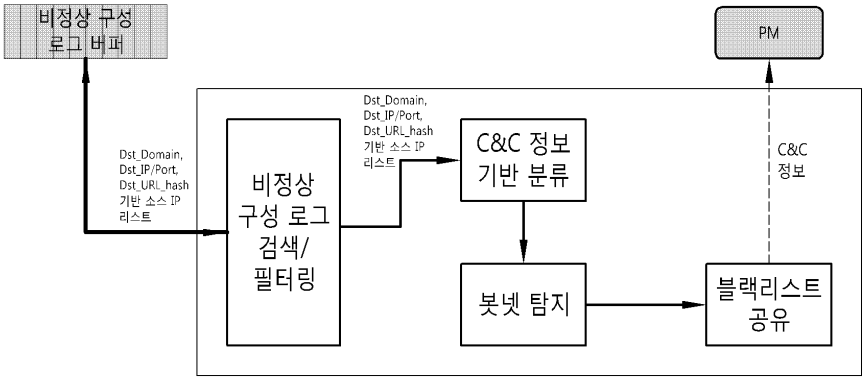
도면8


탐지 시스템
수집 분류
DLM
대응 정책 체크
BAT
보안 이벤트
탐지/ 분류 행위로그 저장
봇넷 공유 요청
대응 정책 생성 요청
체크 결과

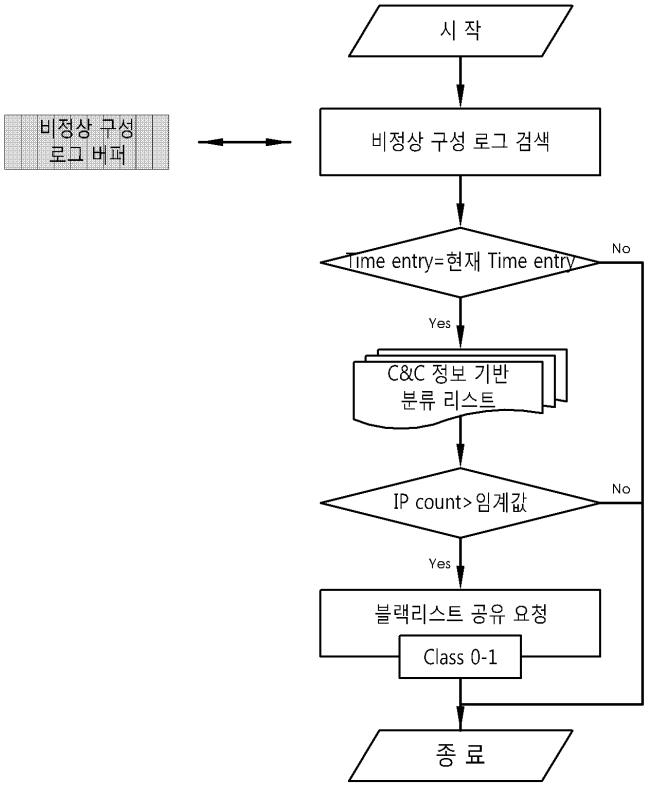
도면9


탐지 시스템
수집 분류
DLM
대응 정책 체크
BAT
비정상 구성 로그 버퍼
보안 이벤트
비정상 구성 로그

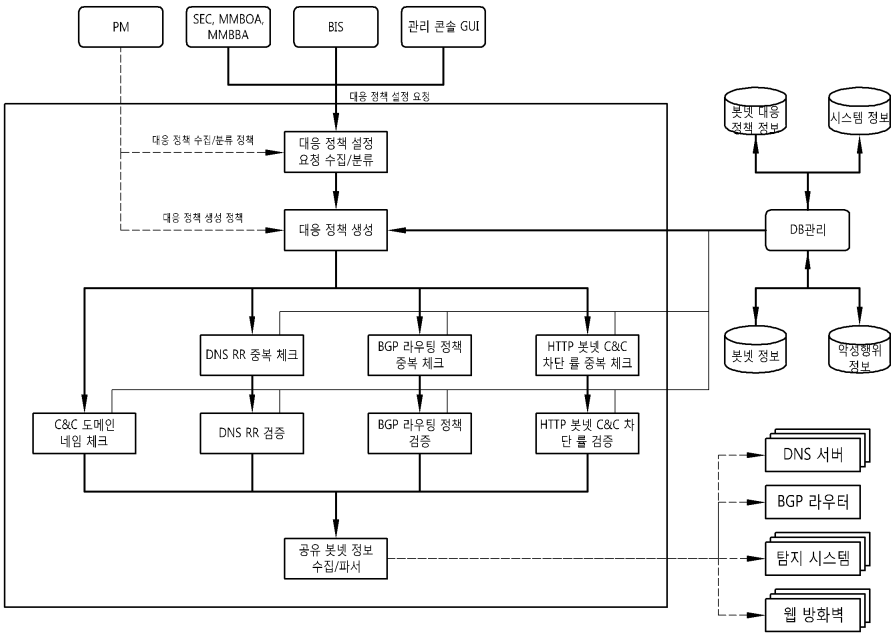
도면10


비정상 구성 로그 버퍼
PM
Dst_Domain, Dst_IP/Port, Dst_URL_hash 기반 소스 IP 리스트
비정상 구성 로그 검색/ 필터링
Dst_Domain, Dst_IP/Port, Dst_URL_hash 기반 소스 IP 리스트
C&C 정보 기반 분류
C&C 정보
봇넷 탐지
블랙리스트 공유

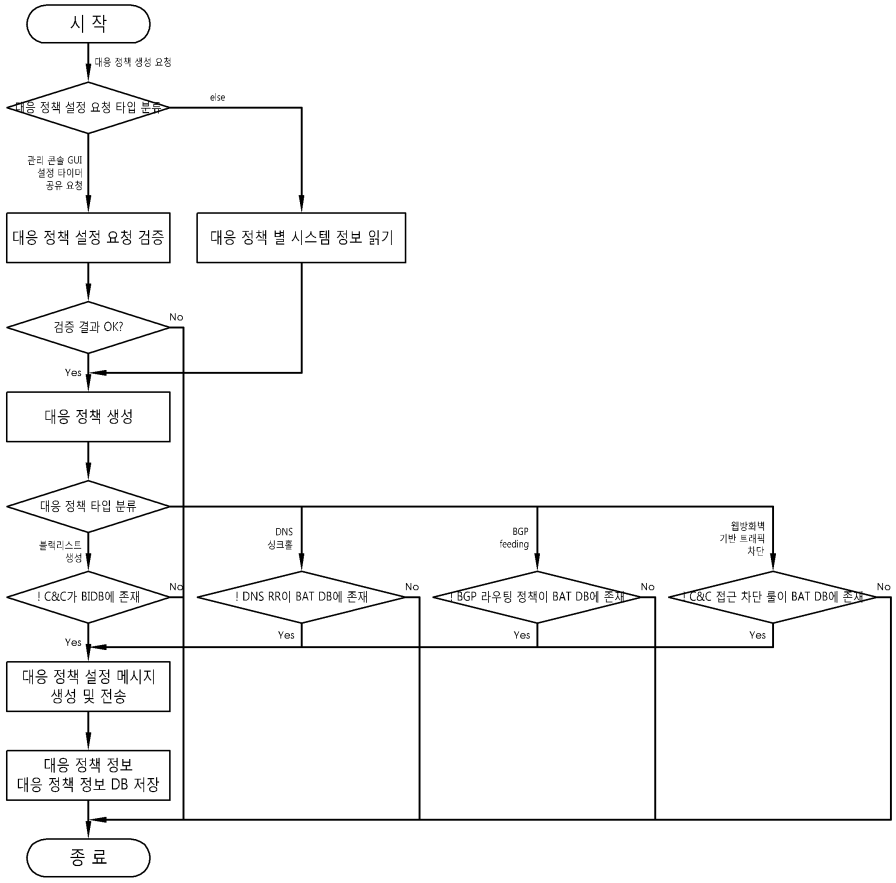
도면11


시 작
비정상 구성
로그 버퍼
비정상 구성 로그 검색
Time entry=현재 Time entry
No
Yes
C&C 정보 기반
분류 리스트
IP count>임계값
No
Yes
블랙리스트 공유 요청
Class 0-1
종 료

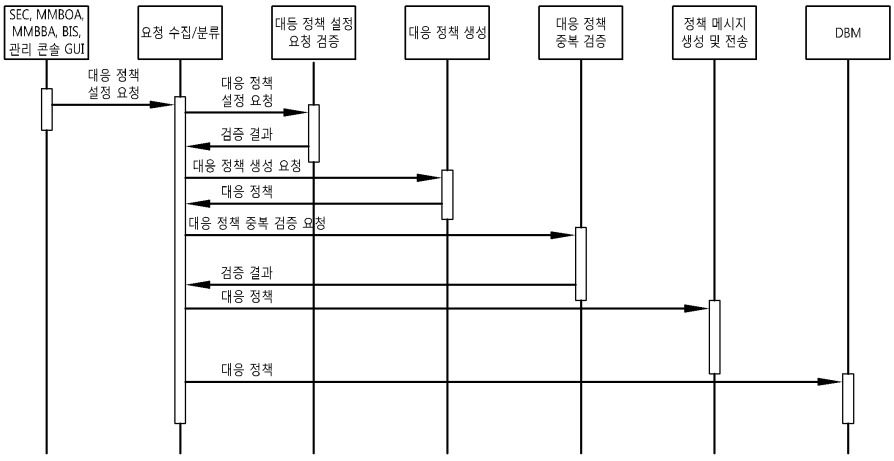
도면12


PM
SEC, MMBOA, MMBBA
BIS
관리 콘솔 GUI
대응 정책 설정 요청
대응 정책 수집/분류 정책
대응 정책 설정 요청 수집/분류
대응 정책 생성 정책
대응 정책 생성
봇넷 대응 정책 정보
시스템 정보
DB관리
DNS RR 중복 체크
BGP 라우팅 정책 중복 체크
HTTP 봇넷 C&C 차단 룰 중복 체크
봇넷 정보
악성행위 정보
C&C 도메인 네임 체크
DNS RR 검증
BGP 라우팅 정책 검증
HTTP 봇넷 C&C 차단 룰 검증
DNS 서버
BGP 라우터
탐지 시스템
웹 방화벽
공유 봇넷 정보 수집/파서

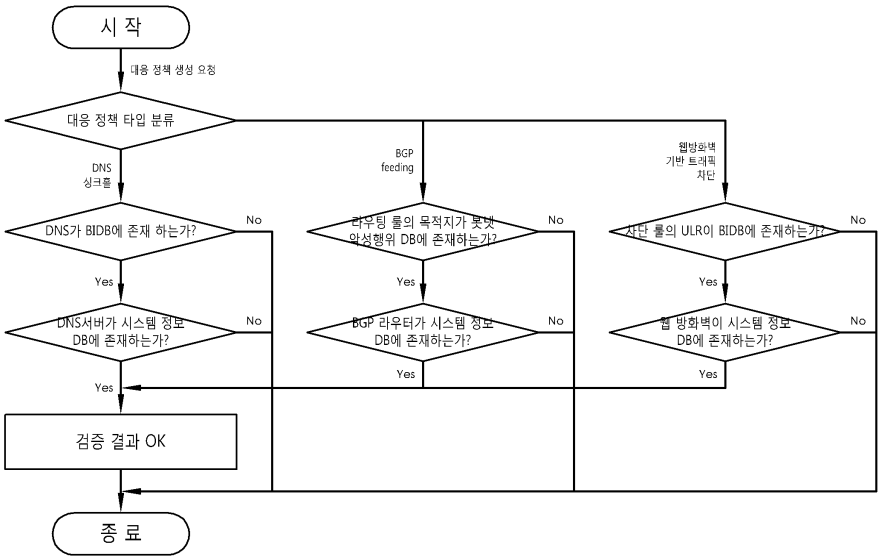
도면13


시 작
대응 정책 생성 요청
대응 정책 설정 요청 타입 분류
else
관리 콘솔 GUI
설정 다이미
공유 요청
대응 정책 설정 요청 검증
대응 정책 별 시스템 정보 읽기
검증 결과 OK?
No
Yes
대응 정책 생성
대응 정책 타입 분류
블랙리스트
생성
! C&C가 BIDB에 존재
No
Yes
DNS
싱크홀
! DNS RR이 BAT DB에 존재
No
Yes
BGP
feeding
! BGP 라우팅 정책이 BAT DB에 존재
No
Yes
웹방화벽
기반 트래픽
차단
! C&C 접근 차단 룰이 BAT DB에 존재
No
Yes
대응 정책 설정 메시지
생성 및 전송
대응 정책 정보
대응 정책 정보 DB 저장
종 료

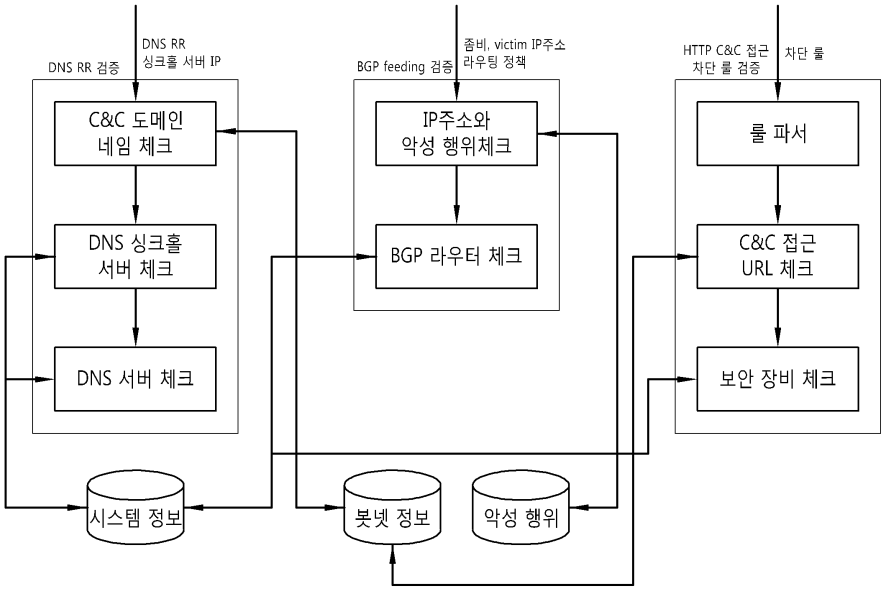
도면14


SEC, MMBOA,
MMBBA, BIS,
관리 콘솔 GUI
요청 수집/분류
대응 정책 설정
요청 검증
대응 정책 생성
대응 정책
중복 검증
정책 메시지
생성 및 전송
DBM
대응 정책
설정 요청
대응 정책
설정 요청
검증 결과
대응 정책 생성 요청
대응 정책
대응 정책 중복 검증 요청
검증 결과
대응 정책
대응 정책

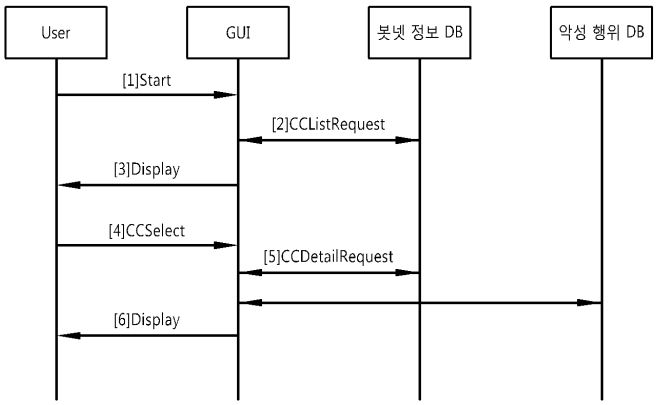
도면15


시 작
대응 정책 생성 요청
대응 정책 타입 분류
DNS 싱크홀
BGP feeding
웹방화벽 기반 트래픽 차단
DNS가 BIDB에 존재 하는가?
No
Yes
라우팅 룰의 목적지가 봇넷 악성행위 DB에 존재하는가?
No
Yes
차단 룰의 ULR이 BIDB에 존재하는가?
No
Yes
DNS서버가 시스템 정보 DB에 존재하는가?
No
Yes
BGP 라우터가 시스템 정보 DB에 존재하는가?
No
Yes
웹 방화벽이 시스템 정보 DB에 존재하는가?
No
Yes
검증 결과 OK
종 료

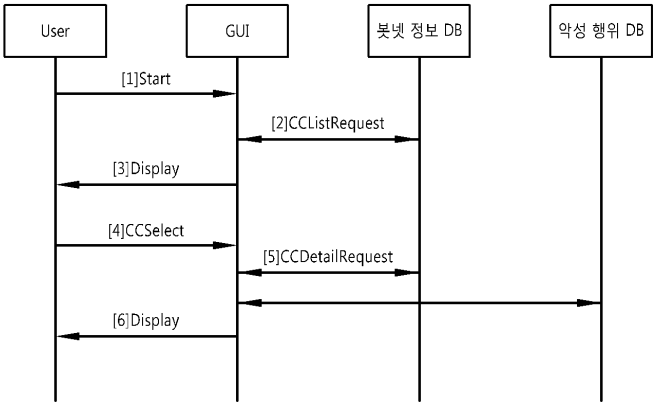
도면16


DNS RR 검증
DNS RR 싱크홀 서버 IP
BGP feeding 검증
좀비, victim IP주소 라우팅 정책
HTTP C&C 접근 차단 룰 검증
차단 룰
C&C 도메인 네임 체크
DNS 싱크홀 서버 체크
DNS 서버 체크
IP주소와 악성 행위체크
BGP 라우터 체크
룰 파서
C&C 접근 URL 체크
보안 장비 체크
시스템 정보
봇넷 정보
악성 행위

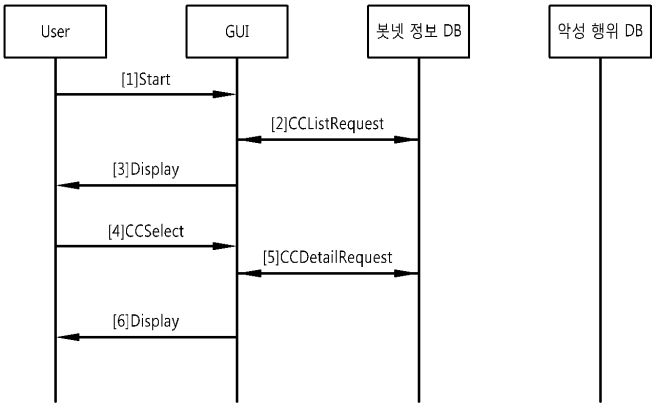
도면17



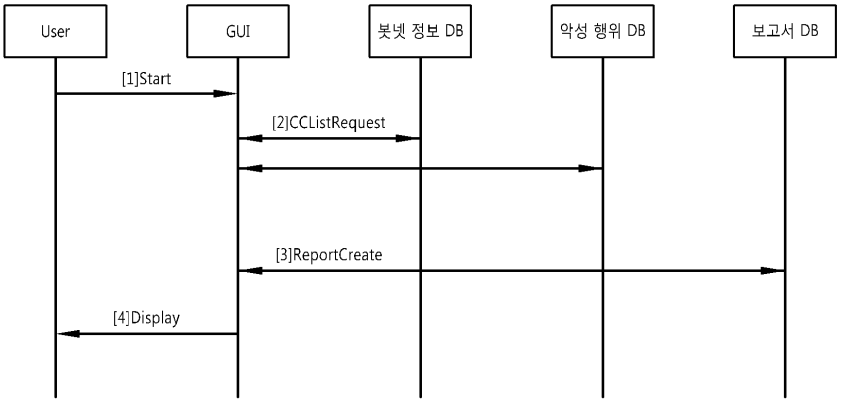
도면18



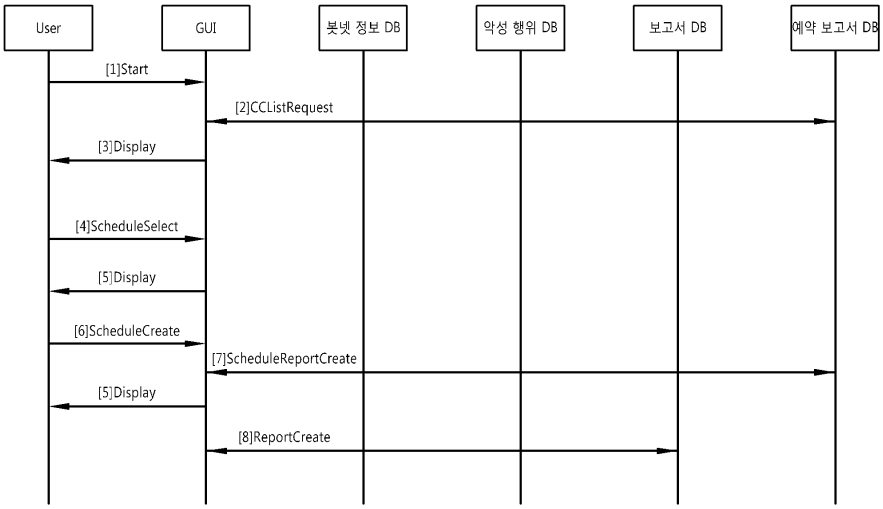
도면19



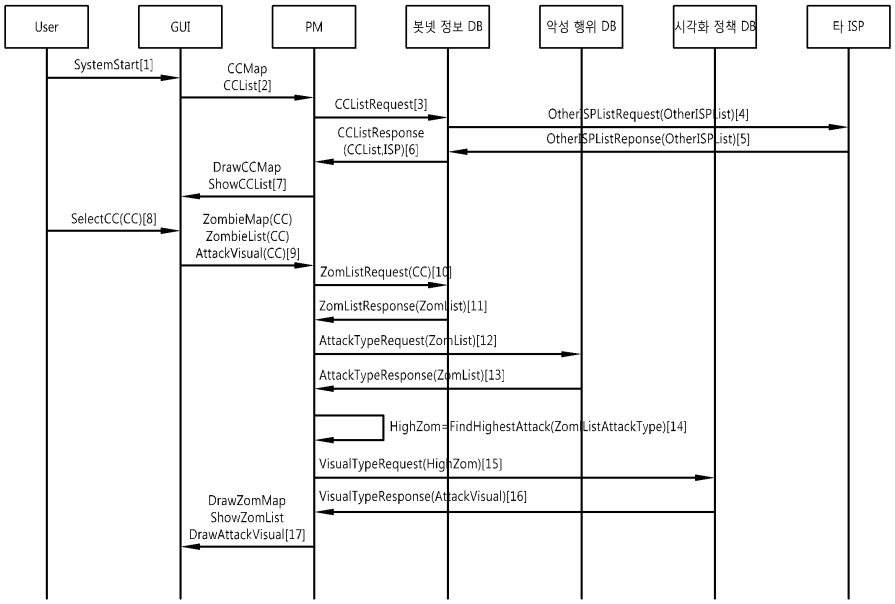
도면20


User
GUI
봇넷 정보 DB
악성 행위 DB
보고서 DB
[1]Start
[2]CCListRequest
[3]ReportCreate
[4]Display

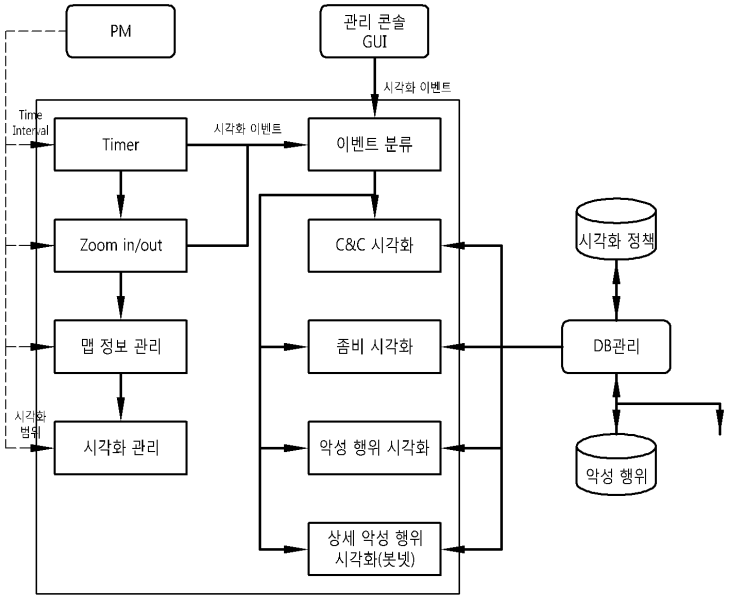
도면21


User
GUI
봇넷 정보 DB
악성 행위 DB
보고서 DB
예약 보고서 DB
[1]Start
[2]CCListRequest
[3]Display
[4]ScheduleSelect
[5]Display
[6]ScheduleCreate
[7]ScheduleReportCreate
[5]Display
[8]ReportCreate

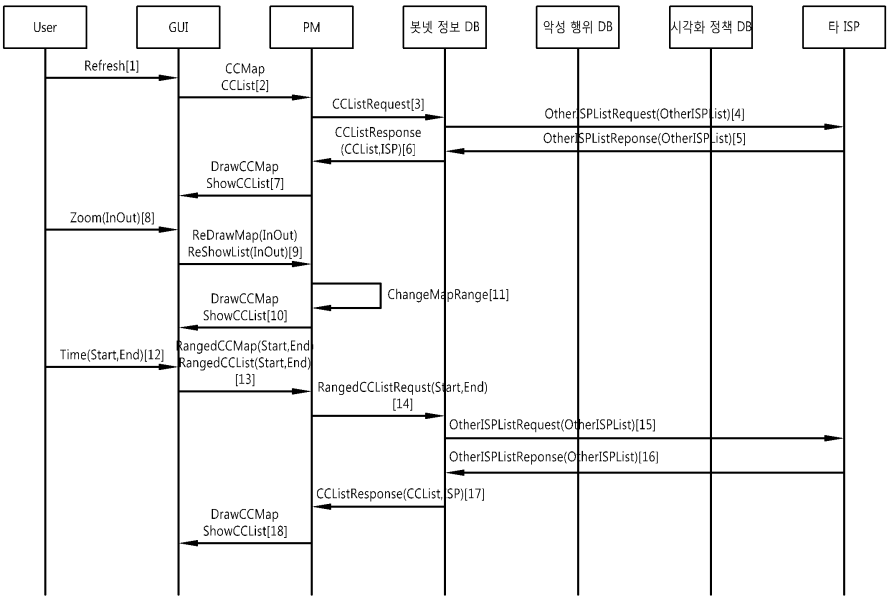
도면22


User
GUI
PM
봇넷 정보 DB
악성 행위 DB
시각화 정책 DB
타 ISP
SystemStart[1]
CCMap
CCList[2]
CCListRequest[3]
OtherISPListRequest(OtherISPList)[4]
CCListResponse
(CCList,ISP)[6]
OtherISPListReponse(OtherISPList)[5]
DrawCCMap
ShowCCList[7]
SelectCC(CC)[8]
ZombieMap(CC)
ZombieList(CC)
AttackVisual(CC)[9]
ZomListRequest(CC)[10]
ZomListResponse(ZomList)[11]
AttackTypeRequest(ZomList)[12]
AttackTypeResponse(ZomList)[13]
HighZom=FindHighestAttack(ZomListAttackType)[14]
VisualTypeRequest(HighZom)[15]
VisualTypeResponse(AttackVisual)[16]
DrawZomMap
ShowZomList
DrawAttackVisual[17]

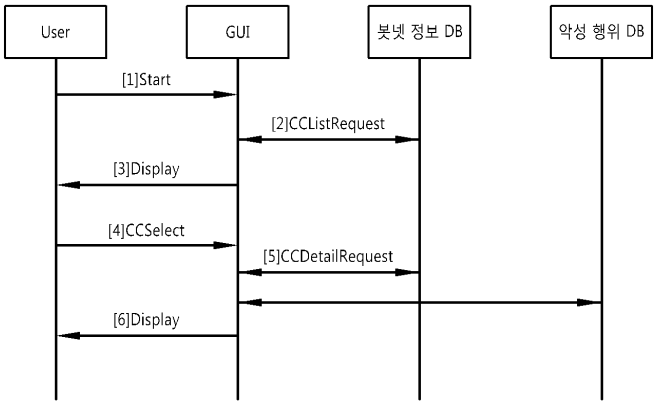
도면23


PM
관리 콘솔
GUI
시각화 이벤트
Time
Interval
Timer
시각화 이벤트
이벤트 분류
Zoom in/out
C&C 시각화
시각화 정책
맵 정보 관리
좀비 시각화
DB관리
시각화
범위
시각화 관리
악성 행위 시각화
악성 행위
상세 악성 행위
시각화(봇넷)

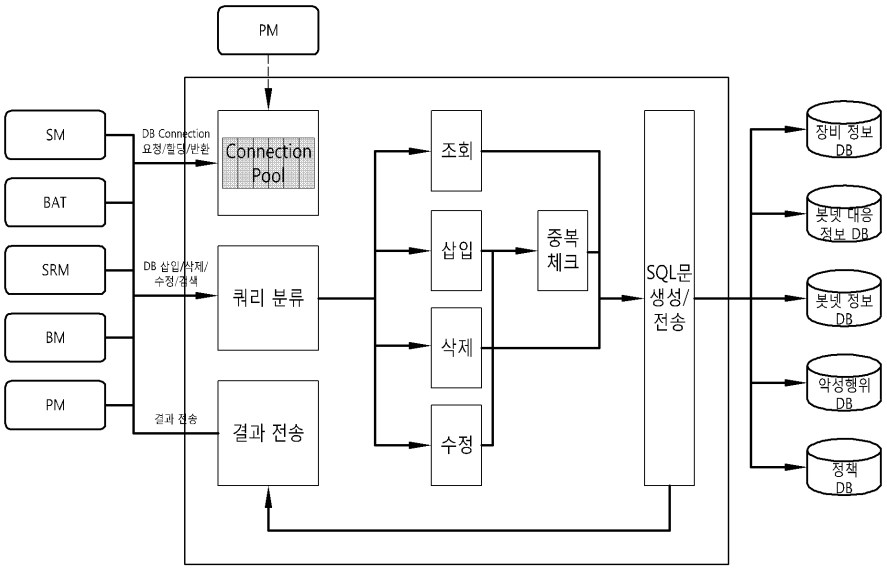
도면24


User
GUI
PM
봇넷 정보 DB
악성 행위 DB
시각화 정책 DB
타 ISP
Refresh[1]
CCMap
CCList[2]
CCListRequest[3]
OtherISPListRequest(OtherISPList)[4]
CCListResponse
(CCList,ISP)[6]
OtherISPListReponse(OtherISPList)[5]
DrawCCMap
ShowCCList[7]
Zoom(InOut)[8]
ReDrawMap(InOut)
ReShowList(InOut)[9]
ChangeMapRange[11]
DrawCCMap
ShowCCList[10]
Time(Start,End)[12]
RangedCCMap(Start,End)
RangedCCList(Start,End)
[13]
RangedCCListRequst(Start,End)
[14]
OtherISPListRequest(OtherISPList)[15]
OtherISPListReponse(OtherISPList)[16]
CCListResponse(CCList,ISP)[17]
DrawCCMap
ShowCCList[18]

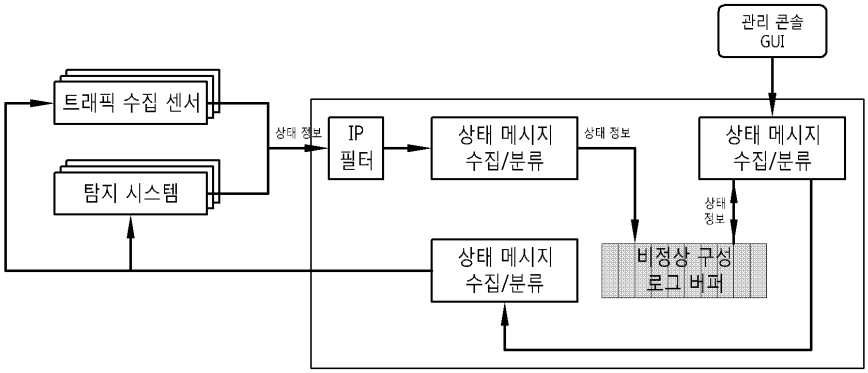
도면25


User
GUI
봇넷 정보 DB
악성 행위 DB
[1]Start
[2]CCListRequest
[3]Display
[4]CCSelect
[5]CCDetailRequest
[6]Display

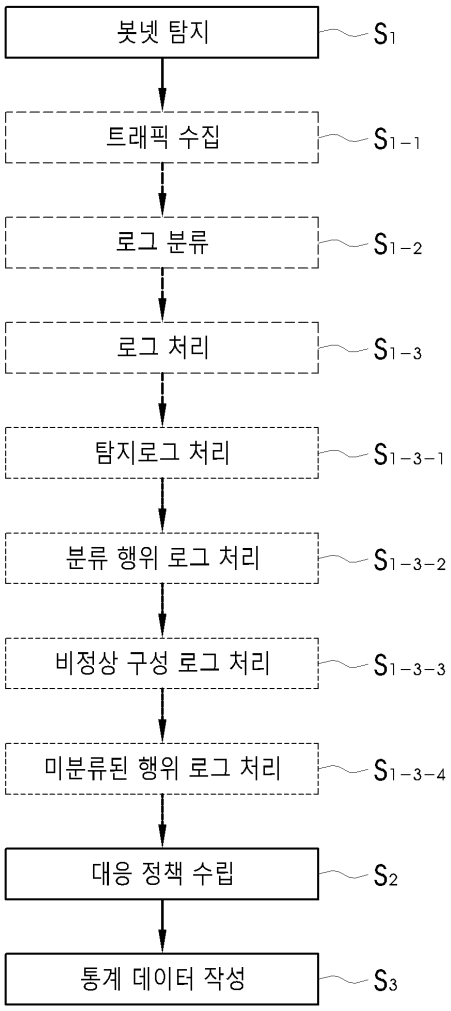
도면26


PM
SM
BAT
SRM
BM
PM
DB Connection 요청/할당/반환
DB 삽입/삭제/수정/검색
결과 전송
Connection Pool
쿼리 분류
결과 전송
조회
삽입
삭제
수정
중복 체크
SQL문 생성/전송
장비 정보 DB
봇넷 대응 정보 DB
봇넷 정보 DB
악성행위 DB
정책 DB

도면27


관리 콘솔 GUI
트래픽 수집 센서
탐지 시스템
상태 정보
IP 필터
상태 메시지 수집/분류
상태 정보
상태 메시지 수집/분류
상태 정보
상태 메시지 수집/분류
비정상 구성 로그 버퍼

도면28


봇넷 탐지
S1
트래픽 수집
S1-1
로그 분류
S1-2
로그 처리
S1-3
탐지로그 처리
S1-3-1
분류 행위 로그 처리
S1-3-2
비정상 구성 로그 처리
S1-3-3
미분류된 행위 로그 처리
S1-3-4
대응 정책 수립
S2
통계 데이터 작성
S3