(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.
G06F 15/00 (2006.01)
G06F 17/00 (2006.01)

(45) 공고일자 2007년03월02일
(11) 등록번호 10-0688604
(24) 등록일자 2007년02월22일

(21) 출원번호 10-2004-0094614
(22) 출원일자 2004년11월18일
심사청구일자 2004년11월18일

(65) 공개번호 10-2006-0055147
(43) 공개일자 2006년05월23일

(73) 특허권자 고려대학교 산학협력단

(72) 발명자 한제헌
장현준
권극한
이희조

(74) 대리인 현종철

(56) 선행기술조사문헌
KR1020000010253 A
KR1020030042318 A
KR1020030061666 A
KR1020040056998 A
KR1020020062071 A
KR1020030048933 A
KR1020040048466 A
KR1020050107651 A
* 심사관에 의하여 인용된 문헌

심사관 : 한선경

전체 청구항 수 : 총 5 항

(54) 네트워크 악성실행코드 차단장치 및 방법

(57) 요약

본 발명은 네트워크 상에서 악성실행코드에 감염되기 이전에 데이터를 추출, 변경하여 상기 악성실행코드가 제거된 데이터만을 전송하기 위한 장치 및 방법을 제공하는 것으로서, 보다 상세하게 설명하면 스파이웨어 의심 데이터를 수집하여 악성실행코드를 분석하고 데이터를 추출하여 상기 악성실행코드를 감염시킨 후 내부적으로 어떠한 동작을 하는지 모든 이벤

트와 데이터를 분석하여 정보로 변경하고, 데이터베이스에 저장하여 상기 저장된 정보를 이용하여 악성실행코드 패턴을 분석하고 판별한 결과 악성실행코드일 경우 차단 패턴을 입력하여 주기적으로 새롭게 입력되는 차단 패턴을 이용한 악성실행코드의 필터링 및 정상적인 패킷이나 데이터를 전송하는 장치 및 방법을 제공하는 것이다.

대표도

도 1

특허청구의 범위

청구항 1.

네트워크를 통해 다운로드된 악성실행코드를 탐지하는 악성실행코드 차단 장치에 있어서,

인터넷을 검색하여 스파이웨어로 의심되는 데이터를 자동으로 다운로드 하는 악성실행코드 수집부;

상기 악성실행코드 수집부에 다운로드된 악성실행코드를 분석하고 데이터를 추출하여 상기 수집부에 의해 수집된 악성실행코드를 감염시킨 후 내부적으로 어떠한 동작을 하는지 모든 이벤트와 데이터를 분석하여 정보로 변경하는 악성실행코드 분석부;

상기 악성실행코드 분석부에서 변경된 정보를 관리하고, 데이터베이스에 저장하는 관리 서버;

상기 관리 서버로부터 저장된 정보를 호출하여 악성실행코드 패턴을 분석하고 판별한 결과 악성실행코드일 경우 차단 패턴을 입력하는 관리 풀;

상기 관리 풀에서 차단 패턴으로 입력된 악성실행코드를 관리 서버로 저장하고, 상기 관리 서버에 저장된 차단 패턴을 기존에 저장된 패턴과 비교하여 갱신하는 업데이트 서버;

상기 업데이터 서버에서 주기적으로 새롭게 입력되는 차단 패턴을 이용하여 악성실행코드를 필터링하여 정상적인 패킷이나 데이터로 전송하는 악성실행코드 차단부; 로 이루어진 네트워크 악성실행코드 차단 장치.

청구항 2.

제1항에 있어서,

상기 악성실행코드 수집부는 외부 장비나 소프트웨어에 의해 만들어진 URL 목록을 다운로드한 후 FTP를 이용하여 파일을 가지고 있는 서버에서 다운로드 하여 필터부가 인식할 수 있는 형태의 포맷으로 변환하는 URL 파일 다운로드 모듈(URL File Download Module);

상기 URL 파일 다운로드 모듈(URL File Download Module)을 통해 변환된 데이터를 룰셋(Rule Set)과 비교하여 데이터 추가나 삭제를 결정하고, 상기 룰셋(Rule Set)은 데이터베이스 모듈과 연동하여 데이터 무결성을 체크하는 필터부;

상기 필터부와 연동하여 무결성 체크를 거친 데이터를 화이트 리스트(White List)와 블랙 리스트(Black List)로 구분하여 관리하는 데이터베이스 모듈;

상기 필터부에 의해 추출된 URL의 스파이웨어 파일을 HTTP나 FTP 프로토콜을 사용하여 다운로드 하는 스파이웨어 파일 다운로드 모듈(Spyware File Download Module);

상기 필터부와 스파이웨어 파일 다운로드 모듈을 통해 받은 최종 데이터를 상기 악성실행코드 분석부에서 인식할 수 있는 포맷으로 변환하고 TCP를 이용하여 전송하는 출력 모듈(Output Module); 을 더 포함하여 이루어진 것을 특징으로 하는 네트워크 악성실행코드 차단 장치.

청구항 3.

제1항에 있어서,

상기 악성실행코드 분석부는 상기 악성실행코드 수집부로부터 네트워크를 통해 수신받는 모듈로 서버 역할을 하는 입력 모듈(Input Module);

상기 입력 모듈(Input Module)로부터 수신받은 스파이웨어 파일을 컴퓨터에서 실행하는 실행 모듈(Executive Module);

상기 실행 모듈(Executive Module)에서 스파이웨어 파일이 실행될 때 시스템에 어떠한 영향을 미치는지 모든 함수와 메시지 호출을 분석하여 출력하는 분석 모듈(Analysis Module);

상기 분석 모듈(Analysis Module)을 통해 출력된 데이터를 상기 관리 서버로 전송하는 출력 모듈(Output Module); 로 구성되는 것을 특징으로 하는 네트워크 악성실행코드 차단장치.

청구항 4.

제1항에 있어서,

상기 악성실행코드 차단부는 외부로부터 상기 악성실행코드 차단부를 통해 나가는 모든 패킷의 흐름을 내부의 필터링 모듈로 전송하는 패킷 제어부;

상기 패킷 제어부를 통해 전달된 패킷을 필터링하여 상기 데이터베이스 모듈에서 가져온 악성실행코드 패턴과 패킷 제어부로부터 전송된 패킷을 비교하여 패킷에 악성실행코드가 포함되었는지를 분석하여 상기 악성실행코드 정보, 전송 위치를 판별하는 필터링 모듈;

상기 필터링 모듈에서 필터링된 데이터를 패킷 그대로 원래 경로로 전송하는 패스, 악성실행코드가 포함된 패킷을 삭제하는 삭제, 패킷을 변조 후 원래 경로로 전송하는 데이터 처리부;

상기 필터링 모듈에서 사용할 수 있도록 데이터를 변환하고, 최신의 데이터를 상기 업데이트 서버를 통해 수신받아 저장하는 데이터베이스 모듈; 로 이루어지는 것을 특징으로 하는 네트워크 악성실행코드 차단장치.

청구항 5.

네트워크 상에서 악성실행코드에 감염되기 이전에 데이터를 추출, 변경하여 상기 악성실행코드가 제거된 데이터만을 전송하기 위한 방법에 있어서,

악성실행코드 수집부에서 인터넷을 통해 악성실행코드 의심 데이터를 수집하는 제1단계;

상기 제1단계에서 수집된 데이터를 분석하여 상기 악성실행코드를 판별한 후 감염시켜 발생하는 이벤트와 데이터를 분석하여 정보로 변환하는 제2단계;

상기 제2단계에서 변환된 정보를 관리 서버로 전송하는 제3단계;

상기 제3단계에서 관리 서버로 전송하여 데이터베이스에 데이터를 저장하는 제4단계;

상기 제4단계에서 상기 관리 서버로부터 저장된 데이터를 관리 풀로 호출하는 제5단계;

상기 제5단계에서 호출된 데이터를 분석하여 악성실행코드와 패턴을 관리 서버에 입력하는 제6단계;

상기 제6단계에서 입력된 관리 서버에서 데이터베이스로 데이터를 저장하는 제7단계;

상기 제7단계에서 데이터베이스로 데이터를 저장하고, 업데이트 서버에서는 데이터베이스에 새롭게 입력된 데이터를 주기적으로 악성실행코드 차단부에 입력하는 제8단계;

상기 제8단계에서 악성실행코드 차단부는 악성실행코드를 필터링하여 정상적인 패킷이나 데이터를 전송하는 제9단계로 이루어진 네트워크 악성실행코드 차단방법.

명세서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 네트워크 상에서 악성실행코드에 감염되기 이전에 데이터를 추출, 변경하여 상기 악성실행코드가 제거된 데이터만을 전송하기 위한 장치 및 방법을 제공하는 것으로서, 보다 상세하게 설명하면 스파이웨어 의심 데이터를 수집하여 악성실행코드를 분석하고 상기 악성실행코드의 패턴을 저장하여 그 판별 결과를 가지고 악성실행코드일 경우 차단 패턴을 주기적으로 새롭게 입력시켜 상기 차단 패턴을 이용한 악성실행코드의 필터링 및 정상적인 패킷이나 데이터를 전송하는 장치 및 방법을 제공하는 것이다.

종래의 웹 사용 환경은 일반 텍스트 전송과 같이 정적이며 단순한 형태를 가지고 있었으며, 실행 프로그램들도 하나의 컴퓨터에서만 실행되었다. 따라서 다른 컴퓨터 시스템에서 프로그램을 실행시키고자 할 경우에 이동식 저장장치를 이용해서 프로그램을 이동시켜 실행시키거나 공유하여 사용하는 방법을 기본으로 하였다. 그러나 인터넷의 등장을 통해 다양한 형태의 정보가 다양한 경로를 통해 이동되고 실행될 수 있는 환경이 구축되었다. 이러한 다양한 정보를 접근하는데 있어서 보다 향상된 편의성 및 기능을 제공하기 위해 실행코드 기술들이 개발되었다.

그러나 상기 실행코드 기술들은 자체 보안 기능을 가지고 있는 등 보안 요구 사항을 충족시키기 위한 여러 가지 방안들을 제시하고 있으나, 각 실행코드별 취약점을 이용하여 비밀성, 무결성, 가용성 침해공격과 사용자 불편 및 불쾌감 유발 등 다양한 피해가 발생하고 있다. 그리고 사용자 편의를 위해 실행코드를 사용할수록 상기의 문제점들은 보다 많이 발생하게 되었다.

발명이 이루고자 하는 기술적 과제

본 발명의 목적은 종래 악성실행코드의 차단에 대한 이해가 부족한 사용자로 하여금 개인용 컴퓨터에 설치되어 악영향을 미치거나 상업적 목적으로 광고를 게재하는 등 악성실행코드를 통해 발생되는 문제점을 해소시키고, 운영체제에서 제공되는 삭제방법으로도 제거되지 않는 악성실행코드를 원천적으로 제거함으로써 기존의 사용자가 보유하고 있는 데이터가 유출되거나 유실되는 위험을 방지하고자 하는 것이다.

발명의 구성

본 발명은 상기와 같은 문제점을 해결하기 위해 안출한 것으로, 네트워크 상에서 악성실행코드에 감염되기 이전에 데이터를 추출 및 변경하여 상기 악성실행코드가 제거된 데이터만을 전송하기 위한 장치에 있어서,

도 1을 참조하여 상세히 설명하면, 네트워크를 통해 다운로드된 악성실행코드를 탐지하는 악성실행코드 차단 장치는

인터넷을 검색하여 스파이웨어로 의심되는 데이터를 자동으로 다운로드 하는 악성실행코드 수집부;

상기 악성실행코드 수집부에 다운로드된 악성실행코드를 분석하고 데이터를 추출하여 상기 수집부에 의해 수집된 악성실행코드를 감염시킨 후 내부적으로 어떠한 동작을 하는지 모든 이벤트와 데이터를 분석하여 정보로 변경하는 악성실행코드 분석부;

상기 악성실행코드 분석부에서 변경된 정보를 관리하고, 데이터베이스에 저장하는 관리 서버;

상기 관리 서버로부터 저장된 정보를 호출하여 악성실행코드 패턴을 분석하고 판별한 결과 악성실행코드일 경우 차단 패턴을 입력하는 관리 풀;

상기 관리 풀에서 차단 패턴으로 입력된 악성실행코드를 관리 서버로 저장하고, 상기 관리 서버에 저장된 차단 패턴을 기존에 저장된 패턴과 비교하여 갱신하는 업데이트 서버;

상기 업데이터 서버에서 주기적으로 새롭게 입력되는 차단 패턴을 이용하여 악성실행코드를 필터링하여 정상적인 패킷이나 데이터로 전송하는 악성실행코드 차단부; 로 이루어진다.

상기와 같이 구성된 네트워크 악성실행코드 차단장치를 이하, 첨부된 도면을 참조하여 더욱 상세히 살펴보면 도 2는 본 발명의 바람직한 실시예에 의한 네트워크 악성실행코드 차단장치 중 악성실행코드 수집부를 나타낸 도면이다.

상기 도 2에서 도시한 바와 같이 악성실행코드 수집부는 외부 장비나 소프트웨어에 의해 만들어진 URL 목록을 다운로드 한 후 FTP를 이용하여 파일을 가지고 있는 서버에서 다운로드 하여 필터부가 인식할 수 있는 형태의 포맷으로 변환하는 URL 파일 다운로드 모듈(URL File Download Module);

상기 URL 파일 다운로드 모듈(URL File Download Module)을 통해 변환된 데이터를 룰셋(Rule Set)과 비교하여 데이터 추가나 삭제를 결정하고, 상기 룰셋(Rule Set)은 데이터베이스 모듈과 연동하여 데이터 무결성을 체크하는 필터부;

상기 필터부와 연동하여 무결성 체크를 거친 데이터를 화이트 리스트(White List)와 블랙 리스트(Black List)로 구분하여 관리하는 데이터베이스 모듈;

상기 필터부에 의해 추출된 URL의 스파이웨어 파일을 HTTP나 FTP 프로토콜을 사용하여 다운로드 하는 스파이웨어 파일 다운로드 모듈(Spyware File Download Module);

상기 필터부와 스파이웨어 파일 다운로드 모듈을 통해 받은 최종 데이터를 상기 악성실행코드 분석부에서 인식할 수 있는 포맷으로 변환하고 TCP를 이용하여 전송하는 출력 모듈(Output Module); 을 포함하는 것을 특징으로 한다.

또한 도 3을 참조하면, 상기 악성실행코드 분석부는 도 2에서 설명한 상기 악성실행코드 수집부로부터 네트워크를 통해 수신받는 모듈로 서버 역할을 하는 입력 모듈(Input Module);

상기 입력 모듈(Input Module)로부터 수신받은 스파이웨어 파일을 컴퓨터에서 실행하는 실행 모듈(Executive Module);

상기 실행 모듈(Executive Module)에서 스파이웨어 파일이 실행될 때 시스템에 어떠한 영향을 미치는지 모든 함수와 메시지 호출을 분석하여 출력하는 분석 모듈(Analysis Module);

상기 분석 모듈(Analysis Module)을 통해 출력된 데이터를 상기 관리 서버로 전송하는 출력 모듈(Output Module); 을 통해 악성실행코드를 판별할 수 있는 것이다.

도 4는 본 발명의 바람직한 실시예에 의한 악성실행코드 차단부를 설명하기 위한 블록도이다. 도 4에서 보는 바와 같이 상기 악성실행코드 차단부는 외부로부터 상기 악성실행코드 차단부를 통해 나가는 모든 패킷의 흐름을 내부의 필터링 모듈로 전송하는 패킷 제어부;

상기 패킷 제어부를 통해 전달된 패킷을 필터링하여 상기 데이터베이스 모듈에서 가져온 악성실행코드 패턴과 패킷 제어부로부터 전송된 패킷을 비교하여 패킷에 악성실행코드가 포함되었는지를 분석하여 상기 악성실행코드 정보, 전송 위치를 판별하는 필터링 모듈;

상기 필터링 모듈에서 필터링된 데이터를 패킷 그대로 원래 경로로 전송하는 패스, 악성실행코드가 포함된 패킷을 삭제하는 삭제, 패킷을 변조 후 원래 경로로 전송하는 데이터 처리부;

상기 필터링 모듈에서 사용할 수 있도록 데이터를 변환하고, 최신의 데이터를 상기 업데이트 서버를 통해 수신받아 저장하는 데이터베이스 모듈; 을 이용하여 악성실행코드가 포함되어 있는 패킷을 분류하여 패스, 삭제, 변조의 과정을 거쳐 상기 악성실행코드를 제거하여 전송하는 것을 특징으로 한다.

상기와 같이 구성된 네트워크 악성실행코드 차단장치를 이용하여 악성실행코드에 감염되기 이전에 데이터를 추출, 변경하여 상기 악성실행코드가 제거된 데이터만을 전송하기 위한 방법을 도 5의 흐름도를 통해 설명하면,

악성실행코드 수집부에서 인터넷을 통해 악성실행코드 의심 데이터를 수집하는 제1단계;

상기 제1단계에서 수집된 데이터를 분석하여 상기 악성실행코드를 판별한 후 감염시켜 발생하는 이벤트와 데이터를 분석하여 정보로 변환하는 제2단계;

상기 제2단계에서 변환된 정보를 관리 서버로 전송하는 제3단계;

상기 제3단계에서 관리 서버로 전송하여 데이터베이스에 데이터를 저장하는 제4단계;

상기 제4단계에서 상기 관리 서버로부터 저장된 데이터를 관리 풀로 호출하는 제5단계;

상기 제5단계에서 호출된 데이터를 분석하여 악성실행코드와 패턴을 관리 서버에 입력하는 제6단계;

상기 제6단계에서 입력된 관리 서버에서 데이터베이스로 데이터를 저장하는 제7단계;

상기 제7단계에서 데이터베이스로 데이터를 저장하고, 업데이트 서버에서는 데이터베이스에 새롭게 입력된 데이터를 주기적으로 악성실행코드 차단부에 입력하는 제8단계;

상기 제8단계에서 악성실행코드 차단부는 악성실행코드를 필터링하여 정상적인 패킷이나 데이터를 전송하는 제9단계를 통해 상기 악성실행코드를 네트워크 상에서 차단할 수 있는 것이다.

상술한 바와 같이 본 발명에 따른 바람직한 실시예를 설명하였지만, 본 발명은 상기한 실시예에 한정되지 않고, 이하의 특허청구의 범위에서 청구하는 본 발명의 요지를 벗어남이 없이 당해 발명이 속하는 분야에서 통상의 지식을 가진 자라면 누구든지 다양한 변경 실시가 가능한 범위까지 본 발명의 기술적 정신이 있다고 할 것이다.

발명의 효과

상술한 바와 같이 본 발명에서는 컴퓨터를 사용하는 대부분의 사용자가 스파이웨어와 같은 악성실행코드나 바이러스의 검색, 치료방법을 알지 못하고 심지어는 그 존재조차를 인식하지 못하는 경우가 많아 네트워크 상에서 사용자로 하여금 악성실행코드의 감염경로로부터 원천적으로 차단시키고, 상기 악성실행코드로 의심되는 데이터를 추출하여 정상적인 패킷이나 데이터로 변경한 후 안전한 데이터만을 전송하게 되어 악성실행코드 치료를 위한 솔루션을 다루지 못하는 사용자에게 편의성을 제공할 수 있다.

도면의 간단한 설명

도 1은 본 발명에 따른 네트워크 악성실행코드 차단장치를 나타낸 블록도.

도 2는 본 발명에 따른 네트워크 악성실행코드 차단장치 중 악성실행코드 수집부를 나타낸 도면.

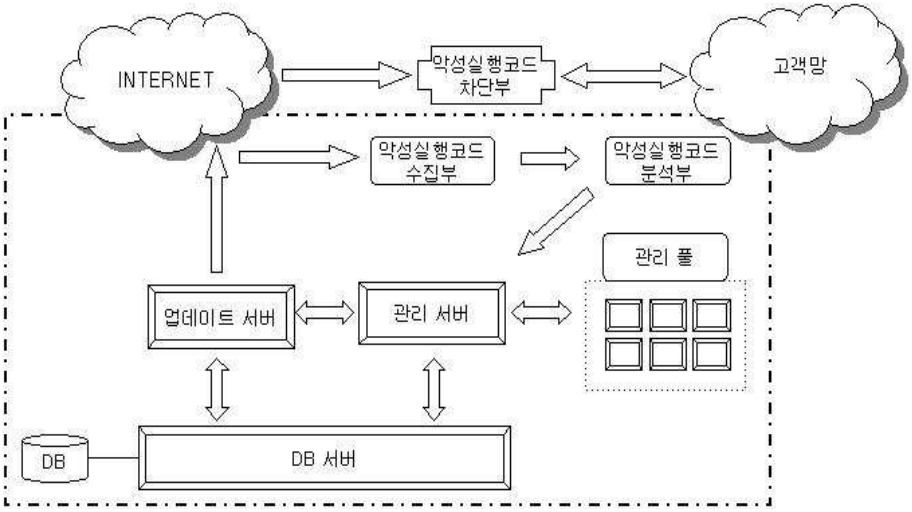
도 3은 본 발명에 따른 네트워크 악성실행코드 차단장치 중 악성실행코드 분석부를 나타낸 도면.

도 4는 본 발명에 따른 네트워크 악성실행코드 차단장치 중 악성실행코드 차단부를 나타낸 도면.

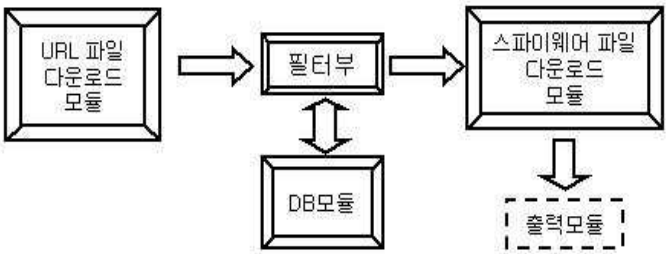
도 5는 본 발명에 따른 네트워크 악성실행코드 차단방법을 나타낸 흐름도.

도면

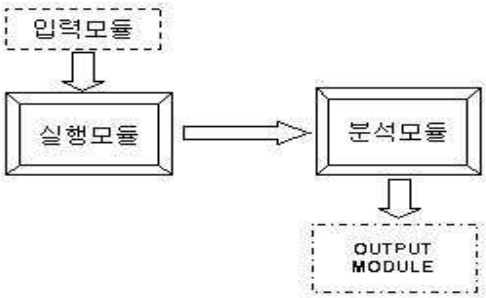
도면1



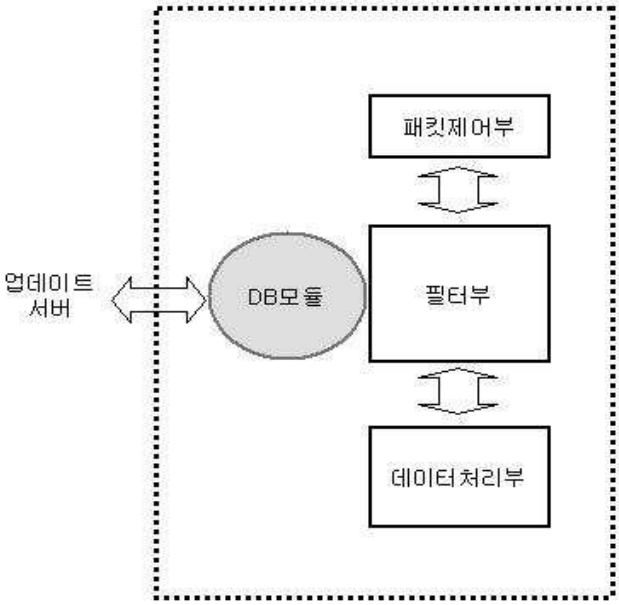
도면2



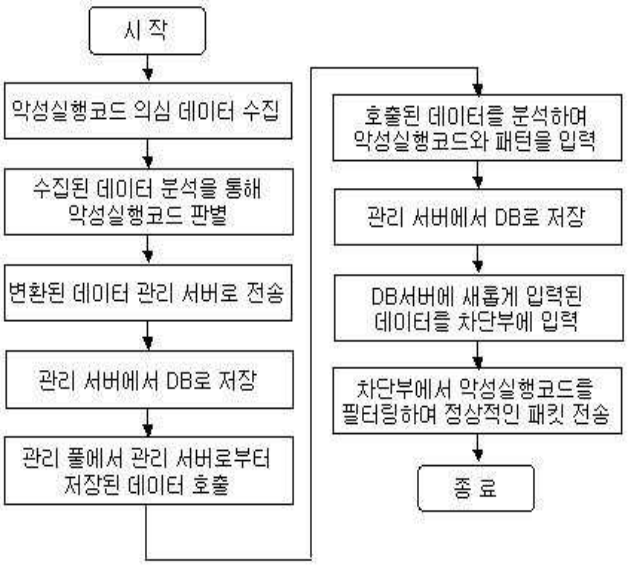
도면3



도면4


패킷제어부
업데이트 서버
DB모듈
필터부
데이터처리부

도면5


시 작
악성실행코드 의심 데이터 수집
수집된 데이터 분석을 통해 악성실행코드 판별
변환된 데이터 관리 서버로 전송
관리 서버에서 DB로 저장
관리 풀에서 관리 서버로부터 저장된 데이터 호출
호출된 데이터를 분석하여 악성실행코드와 패턴을 입력
관리 서버에서 DB로 저장
DB서버에 새롭게 입력된 데이터를 차단부에 입력
차단부에서 악성실행코드를 필터링하여 정상적인 패킷 전송
종 료