한국컴퓨터정보학회 하계학술대회 논문집 제21권 제2호 (2013. 7)

악성코드 탐지를 위한 실시간 통합관리 시스템에 관한 연구

김효남[O]
[O]청강문화산업대학교 게임전공
e-mail: hnkim@ck.ac.kr[O]

A Study on the Realtime Integrated Management System for the Detection Malware

Hyo-Nam Kim[O]
[O]Dept. of Computer Game, ChungKang College of Culture Industries

● 요 약 ●

최근에 발생한 3.20 사이버테러와 6.25 사이버테러와 같이 특정 방송사와 금융권 전산망을 마비시키고 임직원 시스템을 망가뜨려 못쓰게 만드는 피해 유형이 발생되고 있다. 이런 사이버 공격에 사용되는 악성코드에 대해서 탐지에서 분석 그리고 검증 단계를 통합적으로 모니터링하고 필터를 통해 악성코드를 추출하고 차단하는 시스템 개발이 필요하다. 본 논문에서는 실시간으로 악성코드를 탐지하는 엔진들의 분석 및 검증 현황을 확인하고 실시간 통계 모듈에서 수집한 자료들을 바탕으로 향후 보안 정책 방향 및 미래 예측을 계획할 수 있는 실시간 악성코드 분석 통합 관리 시스템을 제안한다.

키워드: 악성코드(Malware), 사이버 공격(cyber Attack), 통합관리 시스템(Integrated Management System)

I. 서 론

최근 인터넷 환경의 급속한 발전으로 인하여 도래한 정보사회는 다양하고 신속한 정보 수집을 통해 사회적 경제적 풍요로움을 가져왔다. 그러나 이런 풍요로움 이면에는 악의적인 목적으로 해킹 바이러스 유포 등을 이용한 사이버테러 공격이 사회적으로 큰 문제가 되고 있다. 최근에 발생한 3.20 사이버테러와 6.25 사이버테러와 같이 특정 방송사와 금융권 전산망을 마비시키고 임직원 PC을 망가뜨려 못쓰게 만드는 피해 유형이 발생되었다[1]. 그리고 매년 신규 악성코드의 증가량을 보면 그 증가세가 매년 증가하고 있다. 이와 같은 추세에 APT(Advanced Persistent Threat)공격을 목적으로 하는 악성코드와 같이 전파도가 낮고 은폐기능과 정보유출 및 파괴기능을 가진 이러한 악성코드들이 자주 등장하면서 이에 대해서 차단하고 탐지하는 백신들은 기존의 방식으로는 한계가 있다고 본다[2].

본 논문에서는 최근 악성코드를 빠르게 탐지, 차단하기 위하여 네트워크로 유입되는 실시간 패킷을 분석하여 파일 기반으로 패킷을 분석하고 해당 파일에 악성코드를 저장하여 상세 정보를 기록하고 이에 대한 통계 및 연관 정보를 저장하여 통합적으로 관리할 수 있는 기능을 제공하는 실시간 악성코드 분석 통합 관리 시스템을 제안한다.

II. 관련 연구

1. 악성코드 자동분석 시스템

현재 최근 악성코드를 빠르게 탐지, 차단하기 위하여 그림 1과 같이 샌드박스 기반의 악성코드 자동분석 시스템이 자주 도입되고 있다. 특히 이에 관련된 다양한 솔루션들이 개발되고 있으며 이에 대한 연구들이 지속적으로 이루어지고 있다. 이러한 솔루션들은 악성코드를 분석할 수 있는 가상화 PC내부에 다양한 모니터링 프로그램들이 유기적으로 정보를 수집할 수 있게 되어 있으며 이렇게 수집된 정보를 통하여 악성코드 동작 여부 및 내부 기능들에 대해서 바로 사용자에게 제공하고 있다[3].

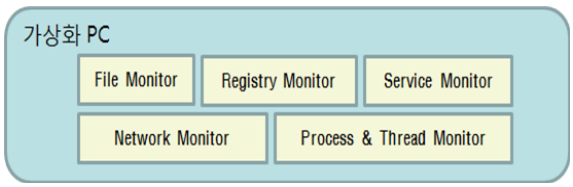

그림 1. 샌드박스 기반의 시스템 구성도
Fig 1. SandBox Based System Diagram

현재 이와 같은 악성코드 자동분석 솔루션은 여러 기업에서 다양한 형태로 제공되고 있다. 특히 사용자가 원할 경우 장비형태로 구입도 가능하고 직접 개발을 원할 경우 오픈 소스 형식으로도 도입이 가능하다.

III. 본 론

1. 실시간 악성코드 분석 통합관리 시스템

최근에 악성코드의 종류가 다양해진 만큼 다양한 동작과 방법으로 공격을 하고 피해를 주기 때문에 여러 단계의 필터를 통해 (탐지, 분석, 검증) 악성코드를 추출하여 차단해야 한다[2]. 이런 공격에 대한 차단 솔루션으로 실시간으로 악성코드를 분석하기 위해 통합관리 시스템이 필요하다. 그림 2는 본 논문에서 제안하고자 하는 통합관리 시스템의 실시간 패킷 탐지 화면을 보여주고 있다.

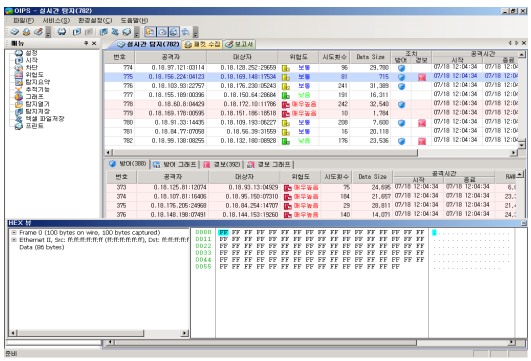

그림 2. 실시간 패킷 탐지 화면
Fig 2. Realtime Packet Detection View

네트워크로 유입되는 실시간 패킷을 분석하여 파일 기반으로 패킷을 분석하고 해당 파일에 악성코드를 저장하여 상세 정보를 기록하고 이에 대한 통계 및 연관 정보를 저장하여 통합적으로 관리할 수 있는 기능을 제공한다. 그리고 실시간 탐지 기법을 기반으로 패킷에 대한 악성코드 실시간 탐지 기능을 설계하는데 있어서 네트워크 패킷을 방화벽으로부터 복사하여 패킷을 수집하고 수집된 패킷 내부의 파일 정보를 추출한다. 표1에서와 같이 실시간으로 악성코드를 탐지하기 위해 모니터링 필터를 구성해야한다. 모니터링의 경우 필터를 분류하여 표1의 항목들에 대한 정보를 기반으로 분석 기능을 수행하며, 각 항목을 데이터베이스로 저장하는 과정을 실시간으로 처리한다.

표 1. 분석 항목
Table 1. Analysis Element

No	항목	장비에서 생성	용도
1	공격자 IP	O	공격하는 IP
2	대상자 IP	O	공격 받은 IP
3	공격자 Port	O	공격하는 Port 번호
4	대상자 Port	O	공격 받는 Port 번호
5	위험도	O	위험도 Level 4등급
6	시도횟수	0	공격 시도 횟수
7	Data Size	O	공격 데이터 크기
8	조치-방어	O	조치- 방어에 대한 정보
9	조치-경보	O	조치- 경보에 대한 정보
10	공격시간-시작	O	공격 시작 시간
11	공격시간-종료	O	공격 종료 시간
12	Raw Data	O	공격한 정보 데이터
13	공격명	O	공격시 공격한 공격명

IV. 결 론

정보통신 환경이 발달하는 만큼, 사이버 상에서 공격하려는 악의적인 시도들도 교묘해지고 다각화되고 있다. 사이버 공격으로 사용되는 악성코드의 종류가 다양해진 만큼 다양한 동작과 방법으로 공격을 하고 피해를 주기 때문에 탐지에서 분석 그리고 검증 단계를 통합적으로 모니터링하여 필터를 통해 악성코드를 추출하고 차단해야 한다.

본 연구는 실시간으로 악성코드 탐지 엔진들의 분석 및 검증 현황을 확하고 실시간 통계 모듈에서 수집한 자료들을 바탕으로 향후 보안 정책 방향 및 미래 예측을 계획할 수 있는 통합 관리 시스템 기술 개발을 제안하고자 한다.

참고문헌

[1] AhnLab, *http://www.ahnlab.com*

[2] Hyo Nam Kim, Jae Kyoung Park, Yoo Hun Won "A Study on the Malware Realtime Analysis System Using the Finite Automata." Journal of the Korean Society of Computer Information Conference. Vol. 18, No. 5, May 2013.

[3] KAIST CSRC, "Malware Trend Analysis Report," 2012.