보안 에이전트 기반의 악성프로세스 검출 시스템 모델

최성묵* · 조희훈**· 김종배***

*,**,***숭실대학교

E-mail : kjb123@ssu.ac.kr

요 약

최근 인터넷 사용이 급증함에 따라 통신망을 통한 악성코드의 감염 경로가 다양해지고 있다. 특히, 봇(Bot)에 의한 공격은 주로 C&C(command-and-control)서버에서 이루어지는데, C&C서버가 IP 형태로 운영되므로 IP를 차단하는 방식을 통해 보안을 유지할 수밖에 없었다. 그러나 공격자들 역시 이러한 서버 차단을 회피하기 위해 우회적인 방법으로 접속을 시도하는 등 차츰 지능화되고 있다. 이러한 악성코드는 사용자의 시스템에 침입하면, 실행이 되는 동안 일반적인 검출방법으로는 검출해내기가 쉽지 않다. 따라서 본 논문에서는 악성코드 감염에 의한 피해 확산을 방지하기 위해 보안에이전트 기반의 악성프로세스 검출시스템 모델을 제시하고자 한다.

Ⅰ. 서 론

오늘날 통신망의 확산으로 인해 인터넷의 보급이 증가하였고, 인터넷을 통하여 악의적인 의도를 가진 소프트웨어가 유포되고 그 감염 경로 또한 다양해지고 있다. 악의적인 소프트웨어들은 악성 소프트웨어, 악성코드로 불리며 이른바 봇(Bot)으로도 불린다. 봇이란 로봇(Robot)의 줄임 말로서, 봇에 감염된 시스템을 조종하는 악성프로그램을 말하며 이는 다양한 형태의 공격을 행한다. 이러한 악성코드는 봇넷(Botnet)이라는 네트워크를 형성하여 공격자, 즉 봇 마스터(Bot master)의 명령에 의해 정보 수집, 스팸 메일 발송, 피싱, 악성코드 배포, DDos(Distributed Denial of Service) 공격을 비롯하여 다양한 형태의 공격을 수행한다. 봇넷은 인터넷 사용자뿐만 아니라, 라우터, DNS(Domain Name System) 서버 등의 네트워크 인프라에도 악영향을 끼치게 된다. 먼저 봇 마스터는 많은 사람들이 사용하는 프로그램의 업데이트 서버나 웹 사이트를 해킹하여 악성코드를 심어 놓는다. 그 후, 사용자가 해당 웹사이트에 접속하거나 프로그램을 실행하면서 업데이트를 수행하면, 사용자의 시스템에 악성코드가 설치된다. 이후 사용자의 시스템에 설치된 봇 에이전트(Bot agent)가 봇 마스터의 C&C서버에 접속하면, 봇 마스터는 시스템에 대한 제어권을 획득하게 된다. 따라서 봇 마스터는 제어권을 획득한 시스템에 대한 명령 수행을 통해 취약점 공격 등 각종 악성 행위를 수행할 수 있다.따라서 이러한 악성코드 감염에 의한 피해 확산을 방지하기 위해서는 C&C서버로의 접속을 차단하여 이후 발생 할 수 있는 악의적인 행위를 막기 위한 기술이 요구된다.

Ⅱ. 관련 연구

봇 탐지에 관한 연구로는 DHCP를 이용한 악성 봇 치료 기법 연구가 있다[3]. 이 연구에서는 악성 봇 치료 백신을 설치하지 않는 컴퓨터에게 DHCP 서버가 IP 주소를 제한적으로 공급하는 기법을 제안하였다. 또한 행동 패턴 모델을 이용한 게임 봇 검출 방법이 있다[4]. 게임 서버측면에서 사람과 게임 봇의 행동을 비교하여 게임 봇 사용자들이 조작이나 회피가 힘든 게임 봇 검출 방법을 제안한다. 제안방법으로는 게임 봇과 사람의 행동 패턴 차이 모델을 정의하고 나이브 베이지안 분류기를 사용하여 게임 봇을 검출한다.

악성 프로세스 제어에 관한 연구로는 악성 프로세스 제어 시스템의 성능 향상을 위한 보안 프레임워크가 있다[5]. 제안된 보안 프레임워크에서는 가상머신을 이용하여 제어서버 구축비용을 줄이며, 사용되지 않는 여분의 IP 주소를 동적으로 인터넷 웜 공격 탐지에 이용함으로써 부분적 공격유형의 인터넷 웜 공격 탐지 확률을 증가시킬 수 있다. 또한 인터넷 웜 공격으로부터 서버를 보호하기 위한 악성 프로세스 제어 시스템이 있다[6]. 제안 시스템은 보호대상서버와 동일한 서비스 프로그램을 구동하면서 인터넷 웜에 의한 멀티캐스팅 공격을 탐지하는 제어서버와 제어서버의 지시에 따라 보호대상서버에 생성된 악성 프로세스와 악성 실행파일을 제거하는 에이전로 구성된다. 제안 시스템은 탐지룰을 사용하지 않기 때문에 신종 인터넷 웜에 효과적으로 대응할 수 있으며, 기존의 보안 시스템들과 통합될 경우 보안을 더욱 강화 할 수 있다.

III. 악성 프로세스 검출

본 연구에서의 악성 프로세스 검출과정은 [그림 1]과 같이 이루어진다. 프로세스의 감시를 통해 악의적인 행위를 하는 실행파일의 검출과 전송, 그리고 관련 정보 업데이트를 수행하는 단말장치와 검출된 프로세스의 실행 파일을 분석하여 차단기준을 판단하는 보안 관리 서버를 통해 [그림 2]와 같이 정보가 전송된다.

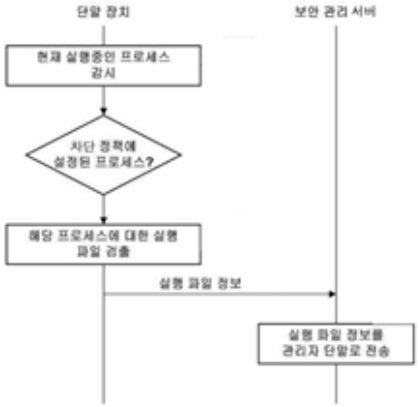

그림 1. <악성프로세스 검출 과정>

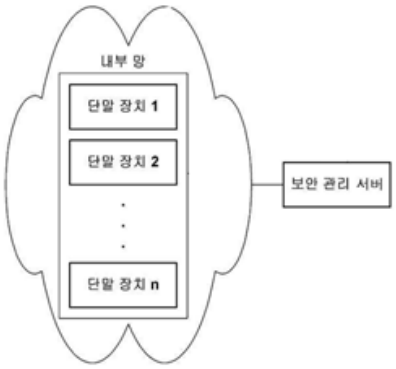

그림 2. <단말장치와 보안관리서버 구조>

IV. 악성 프로세스 검출

단말장치 내부는 통신, 입력, 출력, 저장, 보안 에이전트 5가지 컴포넌트로 구성되며 보안관리서버는 차단 정책 데이터베이스, 차단 정책 생성 컴포넌트, 모니터링 컴포넌트로 구성되어 있다. 관리자 단말장치의 실행 화면에는 프로세스, 프로토콜, 로컬 주소, 원격주소, 연결상태 등이 표시 된다. 이때 프로세스는 현재 실행중인 프로세스이고, 프로토콜은 TCP, UDP와 같이 현재 사용중인 프로토콜, 로컬 주소는 로컬 단말장치의 IP주소 또는 호스트 이름과 포트번호를 의미한다. 원격주소는 원격 단말장치의 IP주소 또는 호스트 이름과 포트번호가 표시된다. 연결상태 표시는 연결상태 종료 대기 상태, 연결종료상태, 연결중인 상태, 연결 요청 수신 상태, 연결요청 발신상태, 소켓과 연결이 종료중인 상태, 원격지로 인한 연결 종료 발신 대기 상태, 포트를 열고 원격지로부터 연결 발신 대기 상태, 연결 종료 후 최종확인 대기 상태 연결 종료 후 원격지의 수신 보장을 위한 대기 상태, 연결 목록 색인(초록색: 정상연결, 빨간색: 연결이 끊기거나 종료, 노란색: 연결이 바뀜)이 나타난다.

V. 결 론

본 논문에서는 보안에이전트를 설치하여 악성코드의 감염을 방지할 뿐만 아니라 시스템내부의 프로세스 상의 악성코드를 감지하여 차단하는 시스템 모델을 제시하였다. 제시된 시스템 모델은 단말장치와 보안관리서버로 구성된다. 단말장치를 통해 프로세스에 관한 정보를 보안관리서버로 전송하게 된다. 보안관리서버로 전송된 정보는 내부 정책에 의해 악성코드 판별 여부를 거치게 된다. 이를 통해 시스템 내부에 침투하여 악의적인 행위를 하는 프로세스를 판별하여 차단하게 된다. 위 시스템 모델은 악성코드의 침입을 차단하는 기존 방식과는 달리 침투한 악성 코드에 대하여 검출을 시도하는 것으로 보안을 유지하게 된다.

참고문헌

[1] Botnet Detection Technique using Traffic Profiling Method
[2] BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic
[3] Hong-Yoon Kim, A Malicious Bot Curing Technique Using DHCP
[4] Behavior Pattern Modeling based Game Bot detection.: Sang-hyun Park, Hye-Wuk Jung, Taebok Yoon and Jee-Hyong Lee
[5] Security Framework for Improving the Performance of the Malicious Process Control System.: Ik-su Kim, Jong-myung Choi
[6] A Malicious Process Control System for Protecting Serves from Internet Worm Attacks,: Ik-su Kim