신뢰모형을 고려한 APT 악성 트래픽 탐지 기법

윤경미 · 조기환

전북대학교

An APT Malicious Traffic Detection Method with Considering of Trust Model

Kyung-mi Yun · Gi-hwan Cho

Chonbuk National University

E-mail : {kmyun, ghcho}@jbnu.ac.kr

요 약

최근 특정 대상을 목표로 하는 지능적이고 지속적인 공격(APT: Advanced Persistent Threat)이 급속히 증가하고 있다. APT는 악성코드 유입 시 완벽한 방어가 불가능하기 때문에 일반적인 탐지 기법으로 대응이 어려움이 있다. 따라서 본 논문에서는 악성코드 침투 이후의 콜백 단계를 차단하기 위하여 아웃바운드 트래픽을 분석하고 신뢰도를 기반으로 한 APT 공격 탐지기법에 대해 제안한다. 제안기법은 기존 탐지기법에 비해 탐지율을 크게 높이는 기반을 제공한다.

ABSTRACT

Recently, an intelligent APT(Advanced Persistent Threat) attack which aims to a special target is getting to be greatly increased. It is very hard to protect with existing intrusion detection methods because of the difficulties to protect the initial intrusion of malicious code. In this paper, we analyze out-bound traffics to prevent call-back step after malicious code intrusion, and propose an APT malicious traffic detection method with considering of trust. The proposed method is expected to provide a basement to improve the detection rate in comparing with that of existing detection methods.

키워드

Malicious Traffic, APT, Attack Detection, Trust

Ⅰ. 서 론

최근 특정 대상을 목표로 지능적이고 지속적으로 은밀히 공격을 하여 정보를 수집하고 유출하는 방법인 지능형 지속위협(APT, Advanced Persistent Threat)이 증가하고 있다. KISA의 통계에 따르면 2008년 ebay 해킹으로 1800만 건의 개인정보가 유출되었고, 2011년 농협의 전산망이 마비되었으며, 2013년 3.20 사이버 공격으로 주요 금융, 방송사의 전산이 마비, 2013년 6월 사이버 공격으로 정부, 공공기관 홈페이지에 피해를 입었다. 최근 이러한 공격으로 피해가 지속되고 있으며, 2013년 사이버 범죄에 따른 연간 피해 규모가 약 120조원에 달한다고 한다[1][2].

현재 APT 공격 탐지를 위한 다양한 보안솔루션이 존재하지만 제로데이 취약점과 같은 정교한 공격기법은 솔루션에서 탐지가 어렵다. 즉 기존의 패턴, 시그니처 기반의 탐지기법으로는 APT 공격에 대한 완벽한 방어가 불가능함을 전제할 수 있다. 이와 같은 지능적인 공격에 대응하기 위해서는 인바운드(in-bound)와 아웃바운드(out-bound) 트래픽을 고려한 추가적인 방어 기법이 필요하다.

본 논문에서는 악성코드 침투 이후의 콜백 단계를 차단하기 위하여 아웃바운드 트래픽을 분석하고 신뢰도 기법을 반영하여 APT 공격을 탐지할 수 있는 방안에 대해 제안한다.

Ⅱ. 관련 연구

2.1 APT 단계별 공격 절차

APT는 운영체제나 애플리케이션의 알려지지 않은 취약점이나 새로운 형태의 악성코드를 사용하여 공격목표에 접근하는 제로데이(zero-day)를 이용해 목표 시스템을 감염시키며, 감염된 시스템은 C&C(Command & Control) 서버로 접속(callback)된다. 이후 목표 시스템에 추가적인 악성코드를 은밀히 설치하여 정보를 수집하고, 시

스템을 통제함으로써 데이터를 유출한다[3]. 표 1은 APT 공격단계에 따른 절차를 간략하게 정리하여 나타낸다.

<표 1> APT 단계별 공격 절차

공격 단계	내용
침투	공격자가 목표에 침입하기 위한 환경구축 및 정보 수집
탐색	침투 후 장기간에 걸쳐 내부 시스템 분석, 정보를 수집
수집/공격	시스템 내 서버 침투, 데이터 수집 또는 시스템 공격 준비
유출/파괴	수집한 정보 유출, 공격대상 서버, PC 파괴

APT 공격탐지를 위한 기존의 연구들에서는 주로 침투 단계에서의 공격을 탐지하고 방어한다. 하지만 APT 특성 상 알려지지 않거나 정교한 공격기법을 사용할 경우 기존 방법으로는 정확한 탐지가 어렵기 때문에 악성코드 유입 후 트래픽 분석을 통한 새로운 탐지기법이 필요하다.

2.2 기존 탐지기법

침입탐지시스템(IDS : Intrusion Detection System)이란 컴퓨터 또는 네트워크에서 발생한 행위를 모니터링하고 침입 발생여부를 실시간으로 탐지하는 시스템으로, 네트워크로부터 정보를 수집한 뒤 침입과 오용의 정보를 분석한다.

침입탐지시스템은 탐지방법에 따라 지식기반 탐지(misuse detection)와 행위기반 탐지(anomaly detection)으로 구분할 수 있다. 지식기반 탐지 기법은 특정 침입에 대해 기존에 알려진 지식을 바탕으로 기존 패턴과 일치하는 경우 침입으로 간주한다. 행위기반 탐지 기법은 사용자의 행동 패턴을 분석해 입력된 패턴과 비교해 침입을 탐지한다. 지식기반의 시그니처 방식으로는 악성코드의 패턴이 변형된 경우나 알려지지 않은 침입에 대해서는 탐지가 어려우며, 행위기반 탐지 방식은 새로운 공격 유형을 탐지할 수는 있지만 과도한 오탐(False Positive)이 발생할 수 있으며, 실시간 시스템으로 작동하기에는 시스템의 부하를 가중시킬 수 있다. 행위 기반의 신뢰 모형을 고려한 악성 트래픽 탐지에서는 오탐을 줄여 에러율을 낮추는 것을 목적으로 한다.

Ⅲ. 네트워크 행위 분석 시스템

3.1 네트워크 행위 분석 시스템

네트워크 행위 분석(NBA: Network Behavior Analysis)은 네트워크 트래픽의 구조와 특성의 패턴을 사용하여 가능한 공격과 기술적인 문제를 식별하고 데이터의 정보 보호에 미치는 영향을 최소화 하는 침입 탐지 기술이다[4]. 즉 네트워크 행동 분석 시스템은 트래픽의 행동 분석을 통해 네트워크 인프라 구조와 호스트에 대한 공격을 판별하는 것을 목적으로 한다.

네트워크 트래픽은 NetFlow/IPFIX data를 통해 각 라우터에서 플로우 기반의 트래픽을 측정한다[5]. 각각의 흐름은 단 방향의 TCP 연결(또는 UDP/ICMP)에 해당하며, 소스 IP 주소, 소스 포트, 목적지 주소, 목적지 포트 및 프로토콜로 관찰되는 모든 패킷의 흐름으로 구성한다.

NBA 시스템에서의 성능을 높이기 위해서는 에이전트 기반(agent-based)의 신뢰 기법과 평판(reputation) 모델링 분야에서 개발된 기법을 사용한다[6]. 효율적인 에이전트 플랫폼의 배치는 멀티프로세서 코어를 통해 쉽게 배분되고 업무의 병렬화를 지원하여, 집단의 탐지 시스템에서의 에러율을 향상시킬 수 있다.

3.2 신뢰 모델

신뢰 모델은 주변 에이전트(Agent)의 신뢰성에 관한 정보를 유지하도록 설계된 지식 구조이다[7]. 에이전트 자신의 상호작용으로 취득하거나, 다른 에이전트의 상호작용으로부터 얻거나, 평판 기법에 의해 다른 에이전트로부터 수신된다.

에이전트들은 상황 정보를 추론하여 신뢰모델을 만든다. 특정 에이전트의 성능 보다는 상호간의 추론에 의해 목적을 달성한다.

3.3 프로세스

탐지 기능은 분류하는 성능을 향상시키기 위해 서로 협력하는 에이전트 사이에 분포되며, 각 에이전트는 신뢰 모델에서 특별한 이상탐지 메소드를 가진다.

구성하는 모든 에이전트는 네트워크의 동일한 데이터를 처리하며 처리 과정동안 모든 검출 에이전트는 네트워크 플로우 세트에서 동일한 데이터를 수신하고 수신한 데이터는 전용 알고리즘에 입력된다. 이 프로세싱은 그림 1과 같이 3단계로 수행되며 다음과 같이 요약할 수 있다.

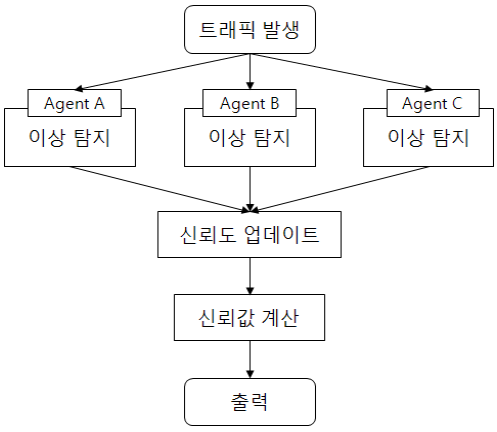

그림 1. 탐지 프로세스

- 이상탐지 : 개별 에이전트는 개별 메소드를 사용해 네트워크 플로우에서 이상을 탐지한다.
- 신뢰 모델 업데이트 : 각 에이전트는 자신의 신뢰 모델을 통해 플로우세트에서 이상 값을 통합할 수 있다. 모든 에이전트는 이상 값을 서로 공유하고, 각 플로우에 대해 동일한 이상 값을 가지며, 신뢰모델을 업데이트 한다.
- 공동의 신뢰도 평가에 의한 신뢰성 판단 : 모든 에이전트에서 업데이트 된 신뢰모델의 플로우를 집계하고, 각 플로우의 신뢰값의 평균을 구해 아웃풋을 구성한다.

Ⅳ. 제안기법

시스템의 네트워크 상의 동일한 트래픽일지라도 어떠한 목적을 가진 시스템인지에 따라 에이전트의 특성에 따라 중요도를 다르게 설정하면 더욱 효율적인 평가모델을 구성할 수 있다는 전제로, 본 논문에서는 각 에이전트의 신뢰모델에서 작성하여 제시한 신뢰도에 추가적인 가중치를 부여하는 방법을 제안한다.

제안 방법은 트래픽 발생 후 시스템의 목적에 알맞은 에이전트를 평가 모델로 선정한 다음, 주 에이전트와 보조 에이전트를 설정한다. 에이전트에는 각각의 가중치를 두어, 주 에이전트의 신뢰도를 나타내는 직접 신뢰도(DT: Direct Trust)와 보조 에이전트 들이 평가한 간접 신뢰도 (IDT: InDirect Trust)로 구분하여 평가리스트를 작성한다. 주 에이전트 A와 보조 에이전트 B, C에 대한 신뢰도 T_{total}는 다음 식 1과 같다.

$$T_{total} = W_1 \times DT + W_2 \times IDT_1 + W_3 IDT_2 \quad (1)$$

전체 신뢰도를 나타내는 T_{total}은 N개의 병렬 에이전트로 이루어져 있으며 확장이 가능하다. T_{total} 식은 다음과 같이 나타낼 수 있다.

$$T_{total} = W_1 DT + \sum_{i=2}^{N} W_i IDT_i \quad (2)$$

W_1는 주 에이전트에서 제시하는 신뢰도 정보인 DT의 가중치이고, W_2와 W_3은 보조 에이전트에서 제시하는 간접신뢰도 IDT_1, IDT_2의 가중치이다. 이때 모든 가중치들의 합은 1이며, W_1은 모든 간접신뢰도의 가중치보다 크다는 조건을 가진다.

아웃바운드 트래픽 발생 단계에서 신뢰모델을 반영한 시스템을 통해, 신뢰도가 높은 트래픽은 통과, 신뢰하지 않는 트래픽은 제한 또는 차단하여 2차 공격의 피해를 줄일 수 있으며 불필요한 작업을 줄임으로서 시스템의 성능을 향상시킬 수 있다. 그림 2는 제안기법을 간략한 그림으로 도식하여 나타낸다.

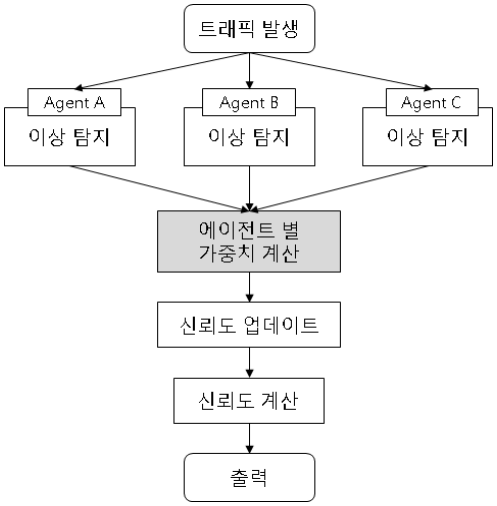

그림 2. 제안하는 탐지 프로세스

Ⅴ. 결 론

본 논문에서는 특정 타겟을 정하여 공격하는 APT 공격을 탐지하기 위해 네트워크의 트래픽의 흐름을 이용한 행위 분석 시스템에서, 이상 탐지를 위하여 동시에 작동하는 각 에이전트에도 신뢰도를 반영하는 기법을 제안하였다. 이는 보안 시스템의 과도한 비용을 줄임으로서 한정된 리소스를 가진 시스템의 부하를 줄여 더욱 효율적인 시스템을 구성할 수 있을 것이라 기대한다. 향후 연구에서는 제안기법에 대한 시험 분석을 통하여 더욱 신뢰할 수 있는 시스템을 구성하는 방안을 연구할 계획이다.

참고문헌

[1] 한국인터넷진흥원, “2013년 주요 침해사고 사례와 대응,” Dec, 2013
[2] Symantec “2013 Norton Report: Cost per Cybercrime Victim Up 50%,” Oct, 2013
[3] 심재화, 정준권, 김현주, 김익균, 정태명, “최근 APT 대응 솔루션 동향 연구,” 한국통신학회, 2013
[4] M. Rehák, M. Pěchouček, M. Grill, J. Stiborek, K. Bartos. P. Čeleda, “Adaptive Multiagent System for Network Traffic Monitoring,“ IEEE Intelligent Systems, pp.16-25, May, 2009
[5] Cisco Systems: Cisco IOS NetFlow (2007), http://www.cisco.com/go/netflow
[6] M. Rehák, M. Pěchouček, M. Grill and K. Bartos, “Trust-Based Classifier Combination for Network Anomaly Detection,” CIA2008, Sep, 2008
[7] Sabater, J., Sierra, C.: Review on computational trust and reputation models. Artif. Intell. Rev. 24, 33-.60(2005)