데이터 마이닝 기반 보안관제 시스템

김민준* · 김귀남**

요 약

최초 사회공학기법의 발달로 해킹, 악성코드가 고도화, 첨단화 되어 기업에 대한 표적 공격인 APT(Advanced Persistent Threat)공격이 급격히 증가하고 있다. APT공격의 가장 큰 특징 중 하나는 지속성이다. 공격자는 내외부에서 지속적으로 공격대상의 정보를 수집 및 활용한다. 보안관제 시스템(Enterprise Security Management)의 경우 이러한 지속적인 공격에 대하여 정상적인 접근 실패로 오인 공격을 받고 있음에도 별도의 경고를 할 수 없는 한계점이 있다. 이러한 오탐 데이터를 철저히 분석하기 위한 시스템 설계 및 연구가 필요하다. 본 논문에서는 데이터마이닝을 이용하여 지나칠 수 있는 오탐을 임계치 기준 분류하여, 산출된 비교 값을 기준으로 지속적으로 일어나는 공격에 대한 예측 및 공격에 대한 개선된 대응 방안을 제시한다. 제안 기법을 사용하여 장기적으로 시도되는 공격 데이터를 분류, 앞으로 일어날 수 있는 공격 징후 탐지가 가능하다.

A Study Of Mining ESM based on Data-Mining

Kim Min Jun*, Kim Kui Nam**

ABSTRACT

Advanced Persistent Threat (APT), aims a specific business or political targets, is rapidly growing due to fast technological advancement in hacking, malicious code, and social engineering techniques. One of the most important characteristics of APT is persistence. Attackers constantly collect information by remaining inside of the targets. Enterprise Security Management (EMS) system can misidentify APT as normal pattern of an access or an entry of a normal user as an attack. In order to analyze this misidentification, a new system development and a research are required. This study suggests the way of forecasting APT and the effective countermeasures against APT attacks by categorizing misidentified data in data-mining through threshold ratings. This proposed technique can improve the detection of future APT attacks by categorizing the data of long-term attack attempts.

Key words : Data-mining, ESM, APT

접수일(2011년 12월 2일), 수정일(1차: 2011년 12월 13일), 게재확정일(2011년 12월 19일)

* 경기대학교 산업보안학과
** 경기대학교 융합보안학과

1. 서 론

해킹 및 악성코드 기술발전 및 사회공학기법의 발달로 특정 그룹, 기관에 대한 표적 공격(APT)에 의한 위협이 급격히 증가하고 있다. 원자력 발전소와 같은 중요한 산업기반시설 뿐만 아니라, 구글, 야후와 같은 유명 인터넷 업체, EMC RSA같은 대표적인 보안업체, 영국 RBS 월드페이, 다국적 석유회사, 미국 국립 오크리지연구소, 모건 스탠리의 해킹사건 등 다수의 APT 공격 의심 사건이 발생하고 있다.

APT공격은 공격의 성공률을 높이기 위해 제로데이 취약점 및 루트 킷과 같은 고도의 공격 기술과 '드라이브 바이 다운로드(Drive-by-download)', SQL 인젝션, 악성코드, 스파이웨어, 피싱, 및 스팸 등을 복합적으로 사용하며, 공격자는 내외부에서 지속적으로 공격 대상의 정보를 수집 및 활용한다.

보안관제 시스템(ESM)의 경우 이러한 지속적인 공격에 대하여 정상적인 접근실패로 오인, APT 공격을 받고 있음에도 별도의 경고를 할 수 없는 한계점이 있다.

따라서, 이러한 오탐 데이터에 대한 보다 철저한 분석을 위한 시스템 설계 및 연구가 필요하다. 본 논문에서는 Data-Mining 을 이용하여 지나칠 수 있는 오탐을 임계치 기준 분류하여, 마이닝 값을 토대로 지속적으로 일어나는 공격에 대한 예측 및 APT 공격에 대한 개선된 대응 방안을 제시한다.

본 논문의 구성은 다음과 같다. 2장에서 관련 연구에 대하여 기술하고, 3장은 데이터마이닝 기법을 기반으로 한 개선된 마이닝 기반의 보안관제시스템(ESM) 운영 방법에 대하여 설명한다. 4장에서는 제안 모델에 국내외 공격 사례를 적용해 결과를 분석하고, 5장에서는 결론 및 향후 연구 방향에 대해 살펴본다.

2. 관련연구

2.1 패턴기반 침입탐지

패턴기반 침입탐지는 오용 탐지(Misuse Detection)로 불리며, 이미 발견되고 정립된 공격을 미리 입력해 두고, 정책에 해당하는 패턴을 탐지하게 되었을 때 알려주는 기법이다. 방법론의 종류로는 서명 분석(Signature Analysis), 전문가 시스템(Expert System), 상태전이 분석(state transition analysis), 페트리 넷(petri-nets) 과 같은 방법이 있다. 패턴 기반 침입탐지의 경우 미리 정해진 패턴 외 침입 행위에 대한 탐지가 불가능하다.[1][2][3]

2.2 행위기반 침입탐지

행위기반 침입탐지 시스템은 사용자의 사용 패턴을 정적 또는 동적 분석을 통하여 인식하며, 이를 벗어난 것을 침입으로 간주하는 탐지 방식으로 알려지지 않은 침입 유형도 탐지 가능하다. 하지만 공격의 다양성을 이용한 정상 행위 위장 또는 불규칙한 사용자의 행위로 구현이 어려우며, 높은 시스템 자원을 요구한다. 따라서 정상 행위에 대한 오탐율이 높다. APT 공격과 같은 정상적인 접근 행위를 가장한 유형의 경우 탐지가 매우 어렵다.[4][5][6]

2.3 보안관제시스템(ESM)

보안관제시스템은 방화벽(firewall), 침입탐지 시스템(IDS), 스팸메일 차단 시스템(Anti-Spam)등의 보안 이벤트를 하나로 통합하여 관리할 수 있게 해주는 시스템을 말한다. 주요 기능은 네트워크 침입차단, 시스템/네트워크 침입탐지 등의 보안 이벤트를 수집하여 통합 보고서 제공이다.

현재 사용되는 보안관제시스템은 보안 담당자에게 수집한 보안 이벤트를 위험등급 구분 방법론(Risk Classification Methodology), 정규화/규칙 기반 이벤트 수집(Normalization/Rule base Event Collection), 비정상 감지 및 대응(Abnormal Detection/Reaction), 통합정책 관리(Intergrated Policy Management)와 같은 기술을 활용하여 매 순간 발생한 사이버 위협의 즉시적 대응을 가능하게 해준다.

하지만, 연동된 보안장비에서 탐지된 것만 수집, 전시하기 때문에 보안관제시스템(ESM)의 탐지 정보는 기존 장비에 종속된다는 특징을 가지고 있다.

또한 실시간으로 누적되는 대량의 보안 이벤트로 인하여, 전문가가 관제를 하고 있음에도 불구하고 매건마다 공격 진위 여부 분석을 위한 시간이 부족하며,

한번 잘못된 탐지로 판별할 시 장시간에 걸친 공격의 연관성을 분석하기 어렵다.

보안관제시스템(ESM)은 개방형, Multi Vendor 기반의 전사적 통합보안관리 플랫폼으로 F/W, IDS, Web F/W 등 보안 장비를 연동하여, 각 장비에서 보안 이벤트를 수집하며, 미리 정해진 패턴에 의해 위협 정보를 보여준다.

3. 개선된 마이닝 기반의 보안관제시스템(ESM)

보안관제시스템(ESM)의 대표적인 연동 장비로는 방화벽(Firewall), 침입탐지시스템(Intrusion Detection System), 웹 방화벽(Web Firewall), Anti-virus, Anti Spam 등이 있다. 각 장비에서 로그 데이터를 수집하여, 미리 정해진 패턴에 의해 위협 정보를 보여준다. 보안관제시스템의 경우 진단 방식이 선례를 보고 규칙을 생성하여 판단하는 방식이기 때문에, 오탐 진단이 내려지더라도 APT 공격의 경우에는 실제 공격의 전초 일 수 있다.

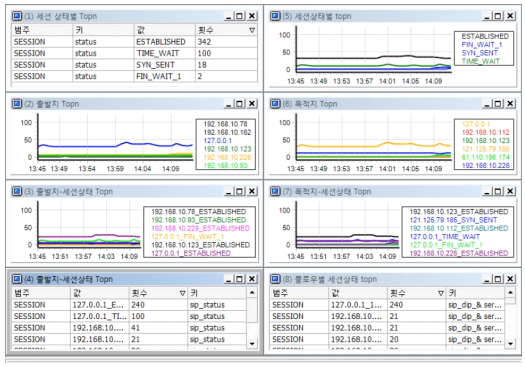
(그림 1)은 E社 통합보안관제 시스템에서 수집하는 데이터 베이스이다. 모든 이벤트 로그를 집계하여 보여주는 영역과, 방화벽에서 가져온 Syslog에서의 출발지, 목적지 IP정보의 집계 영역 각 세션의 상태를 표기해준다. 이외에도 IDS에서 받아온 값을 보여주는 영역, 안티바이러스에서 받아온 값을 보여주는 영역, Anti-Spam 에서 받아온 값을 보여주는 영역을 추가하여 보여줄 수 있다.

방화벽에서 받아오는 데이터 로그는 시간, 사용자(Source IP), 서버(Destination IP) 등이 있으며, 방화벽에서 받아온 IP를 주요 객체로 사용한다. 사용자 IP(Source IP)의 경우 인증된 외부 공간, 주사용 공간, 특정 사용 공간, 임시 사용 공간, 해외로 나뉠 수 있다.

공격자가 특정 ID로 로그인을 시도하는 경우 방화벽에서 차단된다.

해외 접속의 경우 정책에 의해 기본적으로 차단으로 분류되며, 국내의 경우는 허용하게 된다. 이는 행위 기반 차단 정책으로 예를 들어, 특정 ID 사용자가 출장의 경우 허용 되는 정상 트래픽이 될 수 있으므로 행위 기반으로 진위 여부를 판별하기 어렵다.

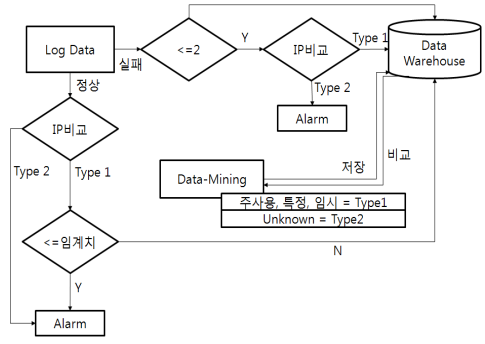
공격자의 IP 대역이 유해 IP로 등록되어 있는 경우 혹은 공격 지역으로 판단된 경우 패턴 기반 차단 기법을 통해 차단될 수 있지만, Spoofing 된 IP의 경우 비정상 차단으로 인식된다.



(그림 1) E 社 보안관제시스템

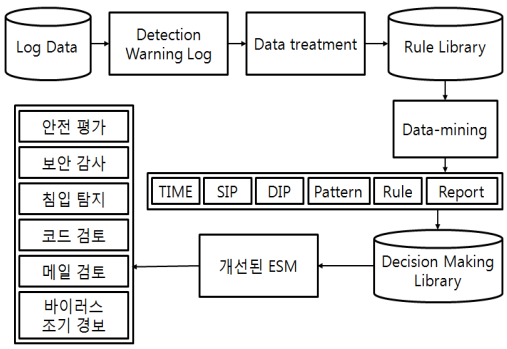
한 예로, 공격자가 국내 IP를 이용한 APT 공격으로 인증 정보를 획득하기 위한 가정을 세워보도록 한다. 보안관제시스템(ESM)은 로그인 시도의 경우48시간 동안 3~4번의 실패로그가 발생하면 사용자의 실수로 판단하고 공격으로 인정하지 않는다고 정책을 세웠다. 하지만 1시간 동안 3회 실패 시 계정 잠금 이라는 임계 치를 줄 수 있지만 이 또한, 공격을 식별했다고 볼 수 없다.

본 논문에서는, 실패 로그를 데이터 마이닝 비교값으로 사용한다. 해당 임계치 초과 값의 IP대역을 기준으로 주사용 구간, 특정 구간, 임시 구간으로 분류한다.



(그림 2) 개선된 보안관제시스템 알고리즘의 예

(그림2)는 APT 공격 시 제안하는 개선된 보안관제 시스템의 공격 판단 및 알람에 관한 알고리즘의 예이다. 1회 실패 시 IP 기준 비교를 통해 데이터베이스 웨어하우스에 저장된다. 그 후 정상 접속 로그가 나타나면 실패 시 IP 로그와 비교한다. 이는 임시장소와 , 정상 사용 장소, 공격성공으로 분류될 수 있다. 하지만, 실제로 공격 성공이라고 단정 지을 수 없기 때문에 일정 수준이상의 비슷한 패턴이 반복되면 위협으로 적용한다. 또한 이후에, 1회 실패 로그가 생성 되었을 경우 최초 실패 로그의 장소와 실패 로그 장소가 다르다면 공격의 전초로 보고 위협으로 적용한다.



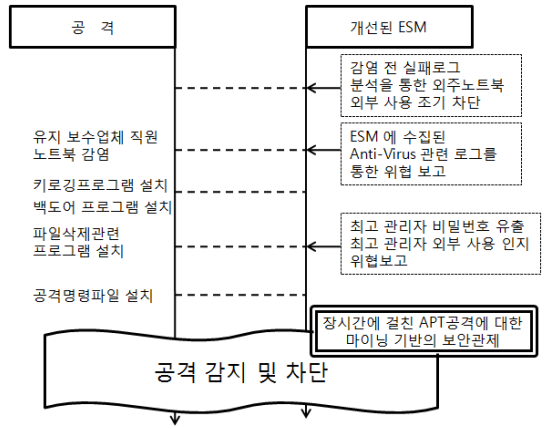
(그림 3) 개선된 보안관제시스템 모델

(그림 3)은 개선된 보안관제시스템(ESM)을 모델링한 결과이다. 최초 로그 데이터에서 위험으로 감지된 로그를 뽑아(Detection Warning Log)내어, 정규화 과정(Data treatment)을 거쳐 Rule Library에 저장된다. 이 값들은 데이터마이닝을 거쳐 새로운 모듈로 사용자 인터페이스에 맞추어 보여준다. 해당 모듈에서는 사건이 일어난 시간과, 출발지 IP, 목적지 IP, 해당 사건의 분류사항, 마이닝 룰에 따른 결과 그리고 보고사항으로 분류된다. 결과 데이터는 의사 결정 라이브러리에 저장되며 개선된 ESM 을 통해서 평가 및 검토한다.[7]

4. 개선된 보안관제시스템(ESM) 모델의 사례 분석

4.1 A 은행 해킹 사건

2011년 A 은행 전산망에 있는 자료가 대규모 손상되어 서비스가 마비되는 사건이 발생했다. 서버 관리 업무에 사용되는 노트북을 점령하여 7개월 동안 악성코드를 심고, 최고 관리자 비밀번호 등 전산망 관리를 위한 각종 정보들을 탈취, 공격명령 파일을 설치 후 원격으로 공격, 서버 운영시스템의 절반을 파괴한 사건이다.



(그림 4) 개선된 보안관제시스템(ESM)모델을 이용한 A은행 사례분석

(그림 4)은 개선된 모델을 A은행 사례에 적용한 시나리오이다. 7개월의 APT공격에 의해 시스템 마비가 일어났으며, 대표적인 공격 사례로 볼 수 있다.

이 경우 (그림 2)의 알고리즘에서 Type2 인 Unknown 장소에서의 접속 로그를 통해서 외부에서의 접속 여부를 확인 할 수 있다. 실패로그가 확인되지 않더라도 2차로 수집된 Anti-Virus 로그를 통해 위협을 인지할 수 있으며, 관리자 PC의 경우 임계 치를 최소로 두어 알람을 통해 공격 가능성을 미연에 방지할 수 있다. APT공격의 특성상 일반적인 실패로그로 보여도 데이터 마이닝을 이용한 탐지 룰 에 의하여 지나칠 수 있는 위협 정보를 보고 받아 조치할 수 있다.

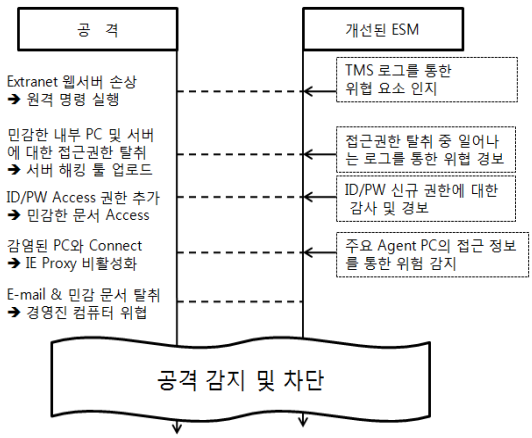
4.2 B 기업 해킹 사건

B 기업 해킹 사건은 외부 웹 서버 SQL Injection공격을 통해 C&C 서버로 사용, 대상 기업의 임직원 노

트북 또는 시스템을 이용해 기업 내부 네트워크로 접속을 시도하여 해킹 툴을 이용 중요 시스템의 사용자 계정 및 비밀번호를 취득, 공격을 성공한 사례이다.

제안된 시스템 이용 시, 기업의 내부 시스템이 중요 시스템의 사용자 계정 및 비밀번호를 획득하고자 시도 할 경우, 생기는 로그 기록을 토대로 설정된 임계치 내에서 위협 정보로 통보를 내릴 수 있다. 이는 수년간 걸친 공격을 시도하는 APT 공격의 특성상을 이용, 공격 징후 탐지가 가능함을 보여준다.

(그림 5)는 개선된 모델을 이용한 B기업 해킹 사건 분석 시나리오이다. 원격 명령을 실행하는 일반적인 위협 패킷 정보는 경우에 따라 정상적인 로그로서 인지 할 수 있으며, 이는 마이닝 룰에 의해 저장된다. 이후 손상된 웹서버에서 일어나는 접근 권한 탈취 중 발생한 실패 정보와 함께 마이닝 룰에 적용 된 위협 패킷과 취합되어 위협 경보를 보내게 된다. 충분한 데이터의 부족으로 공격 여부를 판별하지 못하더라도, 후에 ID/PW 신규 권한에 대한 감사를 통해 위협을 조기에 탐지 할 수 있다. 그밖에, 민감한 주요 PC의 경우 ESM Agent를 이용하여 위험 감지가 가능하다.



(그림 5) 개선된 보안관제시스템(ESM)모델을 이용한 B기업 사례분석

5. 결 론

본 논문에서는, 데이터 마이닝을 기반으로 하는 보안관제시스템을 모델링 하고, 알고리즘을 통한 분석을 통해 APT공격 시도 시, 미리 방지할 수 있도록 하는 개선안을 제시하였다. 공격자의 로그인 시도 시, 계정 차단 및 정상사용 여부에 대한 임계 치를 두고 데이터마이닝을 거쳐 위협 가능성에 대한 알람 기능을 추가하였다. 이는 장기적으로 시도되는 공격에 대하여 데이터를 분류, 앞으로 일어날 수 있는 공격 징후 탐지 가능 여부를 개선 가능하다.

제안하는 방법에서는 공격 징후 로그에 대한 분석을 통해 탐지를 개선할 수 있었지만, 특정 실패로그가 접수되지 않으면, 확인이 불가능하며, 보안관제시스템(ESM)은 로그를 기반으로 위험을 평가하기 때문에, 해당 관제시스템에 접수되지 않은 위협에 대해서는 탐지가 불가능하다. 향후 연구에서는 다양한 공격 방식 분석과 함께 다각도에서 일어나는 공격 시도의 대응 방안에 관한 연구 및 구현이 이루어 져야 할 것이다.

참고문헌

[1] Lianying Zhou, Fengyu Liu, "Research on Computer Network Security Based on Pattern Recognition", 2003

[2] Li Peng, Teng Wen-Da, Zheng Wei, Zhang Kai-Hui "Formalized Answer Extraction Technology Based on Pattern Learning" IFOST 2010 Proceedings 2010

[3] Shreeranga P.R., Akshat Vig, Dr. V.S.Ananth Narayana "An Efficient Classification Algorithm based on Pattern Range Tree Prototypes", 10th International Conference on Information Technology 2007

[4] Matthias Scheutz, Virgil Andronache "Archiectural Mechanisms for Dynamic Changes of Behavior Selection Strategies in Behavior-Based Systems", Transactions on systems, man, and cybernetics-Part B:Cybernetics, Vol.34, No.6, December 2004

[5] Adrian P.Lauf, Richard A.Peters, William H.Robi

nson "Embadded Intelligent Intrusion Detection: A Behavior-Based Approach", 21st International Conference on Advanced Information Networking and Applications Workshops(AINAW'07)

[6] Nam-Yeol Park, Yong-Min Kim, Bong-Nam Noh"A Behavior based Detection for Malicious Code Using Obfuscation Technique", 2006.6

[7] Wenguang Chai "Analyzes and Solves Top Enterprise Network Data Security Issues with the Web Data Mining Technology" 2009 First International Workshop on Database Technology and Applications

[저 자 소 개]

김 민 준 (Min-jun Kim)
2010년 2월 안양대학교
전기전자공학과 학사
2011년 현재 경기대학교
산업보안 석사 과정

email : secuma66@gmail.com

김 귀 남 (Kui-nam Kim)
1989 Univ. of Kansas 수학과 학사
1993 Colorado State Univ
통계학과 석사
1994 Colorado State Univ
산업공학과 박사

email : harap123@hanmail.net