The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 16, No. 6, pp.287-294, Dec. 31, 2016. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2016.16.6.287
JIIBC 2016-6-36

빅데이터를 활용한 이상 징후 탐지 및 관리 모델 연구

A Study on Anomaly Signal Detection and Management Model using Big Data

권영백*, 김인석**

Young-baek Kwon*, In-seok Kim**

요 약 APT(Advanced Persistent Threat)공격은 기관, 기업의 정보통신 설비에 대한 중단 또는 핵심정보의 획득을 목적으로 장기간 IT인프라, 업무환경, 임직원 정보 등의 다양한 정보를 수집하고, 이를 바탕으로 제로데이 공격, 사회공학적기법 등을 이용하여 공격을 실행한다. 악성 시그니처 탐지 등의 단편적인 사이버 위협대응 방법으로는 APT 공격과 같이 고도화된 사이버 공격에 대응하기 어렵다. 본 논문에서는 APT 공격 대응 방안 중 하나로 이종 시스템 로그(Heterogeneous System Log)를 빅데이터로 활용하고, 패턴기반 탐지 방법과 이상 징후 탐지 방법을 병합하여 사이버 침해시도를 탐지하는 모델을 제시하고자 한다.

Abstract APT attack aimed at the interruption of information and communication facilities and important information leakage of companies. it performs an attack using zero-day vulnerabilities, social engineering base on collected information, such as IT infra, business environment, information of employee, for a long period of time. Fragmentary response to cyber threats such as malware signature detection methods can not respond to sophisticated cyber-attacks, such as APT attacks. In this paper, we propose a cyber intrusion detection model for countermeasure of APT attack by utilizing heterogeneous system log into big-data. And it also utilizes that merging pattern-based detection methods and abnormality detection method.

Key Words : Big Data, APT, Anomaly Signal Detection

Ⅰ. 서 론

정보통신 기술이 급속히 발달함에 따라 사용자들의 정보 접근에 대한 자유도가 높아졌다. 이러한 기술들은 사용자의 편의성만 유도한 것이 아니라 기업의 업무 효율성 증대도 동시에 가지고 왔다. 기업의 업무 수행 시각 종 정보조회 등의 활동을 통해 경쟁력을 확보하는 주요한 방법으로써 인터넷 서비스를 이용하고 있다. 그러나 이런 네트워크 환경으로 인해 주요 시스템 등이 직, 간접적으로 외부네트워크에 연결되는 상황이 발생하고, 악의적인 목적을 갖은 사용자에 의해 정보유출 등의 침해사고 발생 가능성이 존재하게 된다.

사이버 침해사고를 방지하기 위해 방화벽(Firewall), 침임탐지시스템((Instruction Detection System, IDS), 침입차단시스템(Intrusion Prevention System, IPS)과 같은 네트워크 보안장비와, 바이러스 백신(Anti-Virus), 내부

*정회원, 고려대학교 정보보호대학원 금융보안학과
**정회원, 고려대학교 사이버국방학과(교신저자)
접수일자: 2016년 10월 5일, 수정완료: 2016년 11월 5일
게재확정일자: 2016년 12월 9일

Received: 5 October, 2016 / Revised: 5 November, 2016
Accepted: 9 December, 2016
*Corresponding Author: iskim11@korea.ac.kr
Dept. of Information Security, Korea University, Korea

정보유출방지 기술(Data Loss Prevention, DLP) 등의 호스트 PC보안 기술들이 사이버 공격에 대응하기 위해 사용되고 있다. 이러한 기존 기술들은 대부분 알려진 공격에 대한 블랙리스트(blacklist)나 시그니쳐(signature)에 기반을 두고 있기 때문에 알려진 공격에 대해서는 효과적인 탐지 및 대응능력을 보여주고 있으나, 제로데이(Zero-day)취약점 및 신종/변종 악성코드를 지속적으로 이용하는 APT 공격을 대응하기에는 한계가 있다. [1][2][3][4][6]

본 연구는 각 보안솔루션들의 단편적인 탐지 결과를 관리하던 기존의 보안체계에서 벗어나 이종시스템 로그의 통합 관리 및 행위 분석을 통한 이상 징후 탐지를 통해 입체적이고 적극적인 사이버 위협 대응 모델을 제시하고자 한다.

본 논문은 다음과 같이 구성된다. 2장에서는 기존의 통합이벤트 관리시스템의 현황과 이상 징후 탐지 방법에 관한 연구 현황을 살펴보고 패턴기반탐지(rule-based detection)과 이상 징후 탐지(anomaly detection)의 장단점을 분석해 본다. 3장에서는 고도화된 이상 징후 탐지 모델을 구현하기 위한 데이터 수집 전략, 침해시도 탐지 처리 절차와 이상 징후 탐지, 대응 방법을 제시한다. 마지막으로 4장에서는 A사의 적용 사례를 바탕으로 이상 징후 탐지를 통해 등록된 시나리오 중 악성 e-mail 탐지 상세 결과를 확인하고, 전체 시나리오 등록현황 및 오탐률을 포함한 탐지결과와 악성코드, 악성사이트 탐지 현황을 확인하여 제시한 모델의 효과성을 확인하고 5장에서 결론을 맺는다.

II. 관련 연구

1. 통합이벤트 관리 체계(SIEM)에 관한 연구

단편적인 사이버 보안 기술에서 벗어나 입체적인 관점에서 보안 이벤트 정보를 관리하기 위해 SIEM(Security Infomation & Event Management)이 활용되고 있다. SIEM은 보안 관리 영역에서 실시간 모니터링, 이벤트의 상관관계, 알림 및 콘솔 뷰 기능으로 알려진 SIM(Security Information Management)와 분석 및 로그 데이터의 보고를 담당하는 SEM(Security Event Manager)으로 구성된다. 보안시스템 전반에 걸쳐 생성되는 이 기종 간의 로그와 이벤트를 통합 관리하여 외부 위험을 사전에 대응하기 위한 플렛폼이다. SIEM의 경우 패턴 탐지 기반의 분석기법을 기반으로 하고 있기 때문에 Zero-day Attack 등 신·변종 취약점을 이용한 공격 탐지에 취약하다. [8][11][12][16][17]

표 1. SIEM 주요 기능 명세
Table 1. Function list of SIEM

Function	Contents
Data aggregation	Log management aggregates data from network, security, server, database, application.
correlation	Looks for common attributes, and links events together into meaningful bundles.
Alerting	The automated analysis of correlated events and production of alerts, to notify recipients of immediate issues.
Dashboards	Tools can take event data and turn it into informational charts
Compliance	Applications can be employed to automate the gathering of compliance data, producing reports.
Retention	Employing long-term storage of historical data to facilitate correlation of data over time.

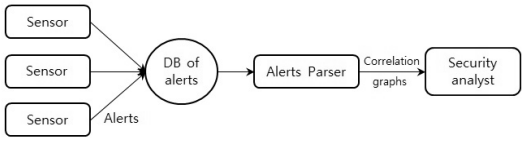

그림 1. SIEM(Security Information & Event Management) 구성
Fig. 1. SIEM architecture

2. 이상 징후 탐지 연구

보안이벤트로부터 알려져 있지 않은 신·변종 사이버 공격을 탐지하기 위해 k-means 클러스터링 기법을 이용한 통계치 기법이 제안되었다. 이 기법은 각각의 네트워크 패킷 버퍼로부터 신종 공격을 탐지하기 위해 8개 통신 항목의 통계치를 기반으로 새로운 특징 벡터를 생성한 후 확률기반 분류기(naive bayesian)를 이용하여 네트워크의 이상 유무를 판단한다. [10][15]

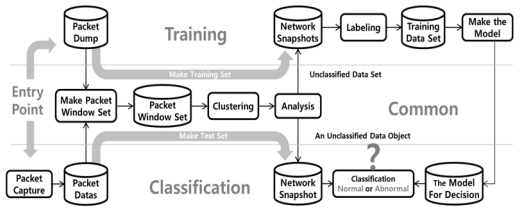

그림 2. 네트워크 이상 징후 탐지 알고리즘
Fig. 2. The algorithm for determining the anomaly network status

악성 e-mail 에 대한 탐지 방법론으로 사례기반추론 기법(CBR)을 이용한 악성메일 프로파일링 기법도 제안되었다. 이 기법은 기존의 사례를 바탕으로 유사도 측정을 통한 악성 e-mail을 탐지하는 기법이다. [13][14]

3. 탐지 방식별 장·단점

사이버 공격을 탐지하기 위한 방법은 비정상 공격 행위에 대한 패턴을 이용하는 패턴 기반 탐지 방법(Rule-based Detection)과 정상 행위에 대한 베이스라인(Baseline)을 기준으로 유의미한 공격 행위를 찾는 이상 징후 탐지 방법(Anomaly Detection)으로 분류할 수 있다. 패턴기반 사이버 위협 대응 체계는 공격자로부터의 공격을 미리 정의된 규칙으로 시스템과 네트워크를 감시함으로서 침입탐지 대응에 효율적이고 신속하다. 그러나 신·변종 취약점을 이용한 공격과 같은 새로운 공격방식에 대처가 불가능하며, 침입대응 시간에서 많은 문제을 가지고 있다. 이와 반대로 신·변종 취약점에 대응하기 위해 고안된 이상 징후 탐지 방법의 경우 정·오탐의 축소가 효율성 확대가 해결해야할 문제이다. 두 방법의 장단점은 표 2 와 같이 나타낼 수 있다. [5][9]

표 2. 패턴 기반 탐지와 이상 징후 탐지 방법의 비교
Table 2. Comparison of rule-based detection and anomaly detection

구분	Rule-based Detection	Anomaly Detection
장점	◆ 알려진 공격 패턴, 방법 식별 용이 ◆ 탐지 방법과 정책 구현 용이	◆ 비정상적 상태 확인에 용이 ◆ 새로운 공격 방법 탐지 가능
단점	◆ 기 확인되지 않은 공격 기법 대응에 부적합	◆ 오탐 축소에 자원 소요 ◆ 비정형 환경에서 사용 부적합

Ⅲ. 고도화된 이상 징후 탐지 모델

진화하는 사이버 침입 시도에 대응하기 위해 기존의 패턴기반 탐지 기법과 이상 징후 탐지 기법을 조합한 이상 징후 탐지 모델을 제시한다. 본 모델에서는 탐지 방법의 개선뿐만 아니라 보안 담당자가 주 관리자가 되어있는 현재의 관점에서 벗어나 침해시도와 관련된 서비스 담당자 및 사용자가 보안 관리 역할을 수행할 수 있도록 사용자 소명절차(User Verification Process)를 도입하였다.

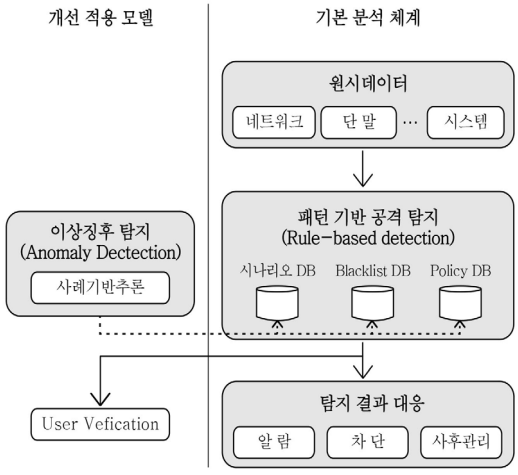

그림 3. 고도화된 이상 징후 탐지 프로세스
Fig. 3. Sophisticated detection process

1. 원시데이터 수집

사이버 위협에 대한 방어 전략은 다음과 같이 구분할 수 있다. [8]

- 퍼리미터(Perimeter) 방어: 내부 네트워크와 신뢰되지 않은 외부 네트워크의 인터페이스 지점으로 인터넷, 비즈니스 파트너, 가상사설망, 전화선 등의 네트워크 퍼리미터가 포함됨. 라우터, 방화벽, 네트워크 침입탐지시스템, 프록시 서버, 원격접근서버 등을 설치하여 방어
- 네트워크(Network) 방어: 내부 네트워크를 보호하기 위해 무선랜 보안, IPSec, 네트워크 세그먼트 기술을 사용하여 보안성, 가용성, 확장성, 관리성, 신뢰성 등의 서비스를 제공
- 호스트(Host) 방어: 서버보안, 개인방화벽, 패치관리시스템, 안티바이러스, 감사로깅 등의 보안 솔루션을 설

치하여 클라이언트 및 서버를 방어

- 응용프로그램(Application) 방어: 웹서버, DB서버, e-mail서버 등을 보호하기 위해 웹 방화벽, DB보안, 메일서버 보안 등의 솔루션을 설치하거나, 소프트웨어 개발 보안 등을 통해 중요자료에 접근 가능한 응용프로그램을 방어
- 데이터(Data) 방어: 접근 통제, 무결성 검증, 암호화, 백업 등을 통해 시스템에 저장되어 있는 중요 자료를 방어

방어 전략에 해당되는 내부시스템을 확인하고 관련 로그 수집을 통해 원시데이터로 확보할 수 있다. 이상 징후 탐지는 이상 패턴, 내부 정책에 의해서 구분되는 경우 정상인 것으로 판단이 되나 특정 기준에 의해서 이상 여부를 확인하는 방법이다. 선정된 기준에 따라 적절한 결과를 확인할 수 있도록 데이터를 수집해야 하는 대상을 상황에 따라 확장할 수 있도록 유연한 연동 구조를 취해야한다. 그러나 현실적으로 모든 시스템의 로그를 관리하는 것은 물리적, 자본적, 기술적인 제약사항이 존재할 뿐만 아니라 정확한 결과를 도출하기 위한 과정에도 도움이 되지 않는다.

본 논문의 제안 모델은 2013년도 금융기관 및 방송사를 대상으로 APT 공격을 수행한 과거 사례를 기반으로 표 3 과 같은 연동 대상을 선정하였다.

표 3. 원천 데이터 선정 대상
Table 3. Source data list

분 류		대상 로그
보안 시스템	공통	감사로그
	방화벽	접근로그, 차단로그
	IPS	침입탐지 로그
	유해차단	외부 사이트 접근 로그
	APT	APT 탐지로그
	DLP	데이터 암호화 적용 로그, 데이터 입출력 관리 로그
	Anti-Virus	악성 프로그램 탐지 로그
	NAC	네트워크 비정상 접속 로그
	DB보안	쿼리 수행 로그
	USB통제	USB 매체 사용 로그
	PMS	파일 배포 로그
	SA	서버 접속 로그, 수행 명령어 로그
	출입관리	출입 관련 로그
서버	공통	시스템로그, 프로세스 로그
	WEB	응용로그
	MAIL	메일 로그
	DB	감사로그
	감사	시스템 로그인, 수행 명령 로그

2. 침해시도 탐지

침해시도 탐지 프로세스는 그림 4 와 같은 형태로 진행이 된다.

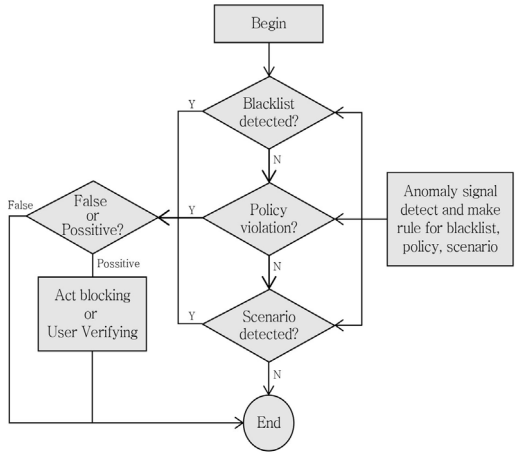

그림 4. 침해시도 탐지 프로세스
Fig. 4. Infringement attempt detection process

효율적인 침해시도 탐지를 위해 패턴기반탐지 방법의 요소인 blacklist, 정책, 시나리오를 점검 수행한다. 탐지 결과는 정오탐 확인 후 관련 계층 장비를 통해 대응하고, 사용자 소명 절차를 통해 오탐률 축소를 기도한다.

3. 이상 징후 탐지

이상 징후 탐지 절차는 사전에 등록된 패턴으로 탐지되지 않아 정상적인 이용으로 분류되는 행위 이벤트들을 분석하여 이상 징후를 탐지하고 정오탐 분석 후 시나리오화 한다. 이상 징후 분석은 사례기반추론기법(CBR)을 활용한다. 표 4 와 같이 기존의 사고사례, 침입시도에서 4W/1H 원칙(who, when, where, what, how) 기준으로 공격 벡터(Vector)를 산출하고 공격 벡터를 기준으로 그림 5 와 같이 작성된 탐지트리(Tree)를 통해 이상 징후 여부를 결정한다. 트리의 Level 은 기존의 사례에서 유사한 공격 형태에 대한 질의를 수행하는 절차이다. 공격에 대한 질의를 트리 형태로 연속적으로 수행함으로써 기존 사례와 유사한 형태의 공격을 탐지할 수 있게 된다. 각 level 은 표 5 와 같이 작성할 수 있으며, 질의 항목이 추가되는 경우 탐지 트리 하위 level 로 유연하게 확장할 수 있다.

표 4. 공격 벡터 작성 예시 (e-mail)
Table 4. Example of Attack Vector for e-mail

4W/1H	구분	내용	vector no
who	발신자 IP 주소	실제 해킹메일 발송 PC 정보 확 인을 통한 공격자 정보 유추 가능	v1
	발신 계정	해킹한 계정을 통해 공격자 성향 유추 가능	v2
	발신 이름	발신 이름 통해 공격하려는 목표의 정 보를 유추 가능	v3
when	발신 일자	동일 날짜에 발송된 해킹메일은 동일 집단의 소행으로 유추 가능	v4
where	도메인	도메인 정보를 통해 해킹메일 특징 유추 가능	v5
	언어	공격자 지역정보 유추 가능	v6
what (whom)	수신 계정	공격 목표정보 및 의도 유추 가능	v7
how	제목	공격 의도와 공격 성향 유추 가능	v8
	첨부일명	공격 목표 연관 정보 수집 가능	v9

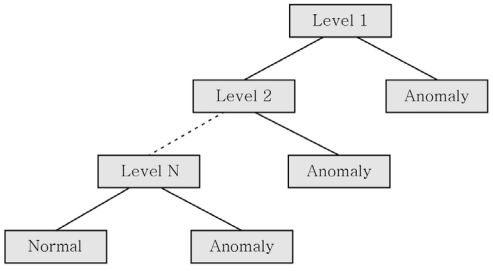

그림 5. 탐지 트리 구조
Fig. 5. Detection Tree structure

표 5. 사례(case)분석을 통한 Level 작성 방법 예시
Table 5. Example of Level writing by case analysis

case	동일 날짜에 동일 제목으로 발신된 메일이나 발신자명, 발신자IP 가 다수인 경우
character	발신일-당일, 제목-동일제목, 발신자IP-다수, 발신자계정-다수
case vector	v1~v9
level vector	v1`~v9`
level i	v4`=v4` and v8=v8` then v2`->N or v1`->N

4. 탐지 결과 대응

이상 징후 탐지 결과는 정형화된 패턴 또는 시나리오로 관리하여 효율성을 높이도록 활용한다. 특히 악성코드 및 악성 사이트 url 등의 정보는 blacklist DB로 관리하고 사용자의 기존 접속 또는 감염이 있었는지 확인하는 절차를 통해 탐지 이전의 타임라인에서의 최초, 최근의 악성 활동 시점을 확인할 수 있다.

Attack	IP	URL	malicious code	victim IP	nasty mail
방화벽	O				
IPS			O		
유해차단		O	O		
APT		O	O		O
DLP				O	
Anti-Virus			O		
NAC				O	
DB보안				O	
SA				O	
MAIL Fitter					O

그림 6. Blacklist 연계 대응 체계
Fig. 6. Blacklist response chain system

그림 6 과 같이 탐지된 blacklist, 패턴 등은 항목별 관련 시스템의 연계 대응 시스템과 같이 차단 등의 대응 설정과 과거 로그 조회를 통한 최초 유입 시기를 확인할 수 있다. [7]

이상 징후 및 침해시도 탐지결과는 보안 관리자 외 유관 시스템 관리자 또는 사용자로 탐지결과를 전달하고 결과 수령자는 소명 작업을 수행함으로써 오탐지률을 축소할 수 있다.

Ⅳ. 적용 사례

1. 이상 징후 탐지 결과

사용자들의 e-mail 사용에 관한 이상징후 탐지 결과 아래와 같이 시나리오를 정규화 하였다.

- 제목 : Signed copy 키워드 포함
- 첨부파일 : 첨부 파일이 있는 경우
- 특징 : 제목은 동일하나 발신자 정보 상이
  해당 사나리오를 통해 추출된 메일을 확인한 결과 난독화 되어 있는 악성파일을 확인할 수 있었다.
- 첨부파일명 : project_document_yfseo.zip
- 압축해제 : signed doc 6235.js
- 유도된 악성코드 유포지
  - hxxp://ding-a-ling-tel.com/b289dg
  - hxxp://blcbp.org/d9rk30u

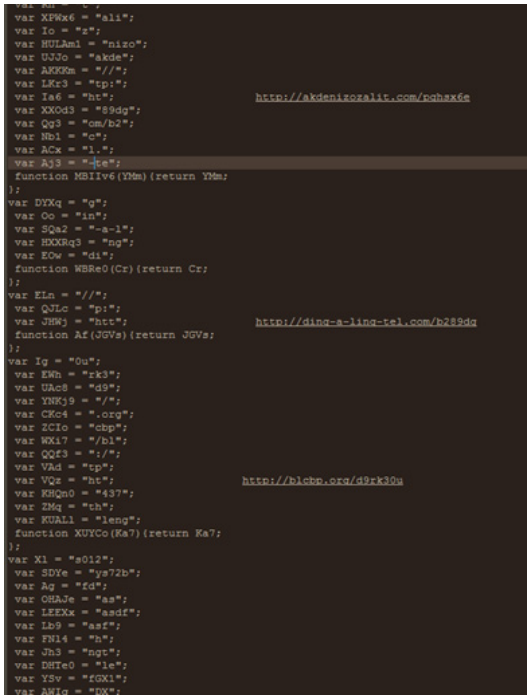

그림 7. 탐지된 악성파일 코드
Fig. 7. Malicious file code detected by scenario

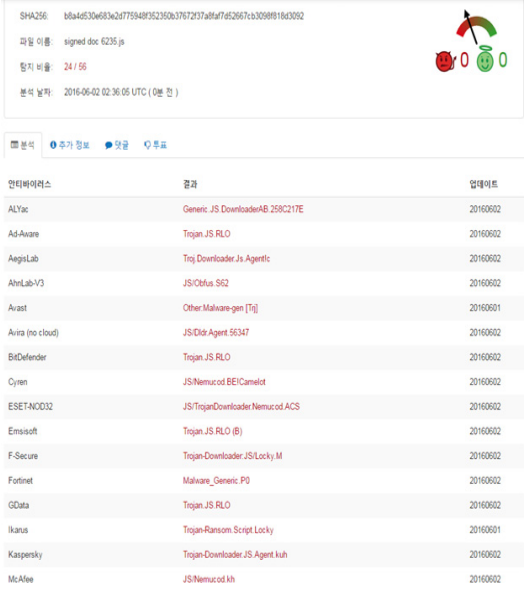

그림 8. 악성코드 분석 사이트 탐지 결과
Fig. 8. Detection result on malicious code analysis site

그림 7, 그림 8 은 시나리오에 탐지된 악성 e-mail 내 첨부파일의 악성코드 여부를 확인한 화면이다. 악성코드로 안티바이러스 제품에 등록하고, 관련 정보를 조회할 수 있는 인터넷 사이트에서 확인한 화면이다.

2. 시나리오 등록 및 탐지 결과

이상 징후 분석에 따른 시나리오 등록 현황과 탐지 결과, 오탐률은 표 6 과 같다. 평균 오탐률이 19%로 등록된 시나리오가 효과가 있음을 알 수 있다.

표 6. 이상 징후 탐지 결과에 따른 시나리오 등록 현황
Table 6. Scenario state applied by anomaly detection

구분	항목	시나리오 수	탐지 건 수	오탐률
보안 통제	해킹시도	8	706	44%
	비인가 S/W	2	31	48%
	단말보안정책	16	275	14%
	서버/DB 접근	12	180	11%
	악성코드유입	21	808	18%
	업무서비스 이용	12	115	2%
	계정/권한	27	231	53%
정보 보호	과다조회	5	1,139	-
	과다보유	8	180	8%
	유출징후	34	1,525	5%
	유출사고	2	193	2%
	DATA 오남용	7	54	6%
물리적 보안	출입	2	52	37%
	반출/분실	1	-	-
합계(평균)		157(-)	5,489	(19%)

표 7 은 보안통제 시나리오를 통해서 탐지된 악성사이트, IP, 악성코드 탐지 결과다. 표 7 에서 보이는 것과 같이 2016년도 4월부터 9월간 탐지되는 악성사이트 수가 사이버침해대응 관련 기관의 탐지 정보와 비교했을 때 상대적으로 많은 악성사이트 정보를 수집했다. 제안한 개선 모델이 효율적임을 나타낸다.

표 7. 악성사이트 탐지 현황 (2016.4.~2016.9.)
Table 7. Detection state of malicious site

출처	악성사이트IP or URL	백분율
A 사	4,343	82%
KISA	620	12%
금융보안원	362	7%
합 계	5,325	100%

표 8. 이상 징후 탐지에 의한 Anti-Virus solution 패턴 등록 현황 (Zero-day 악성코드)

Table 8. Pattern state applied to Anti-Virus solution by anomaly detection (Zero-day malicious code)

구분	4월	5월	6월	7월	8월	9월	합계
악성	8	22	12	48	33	49	172
오탐	-	3	-	-	-	1	4
총	8	25	12	48	33	50	176
정탐율	100%	88%	100%	100%	100%	98%	98%

표 8은 악성코드 탐지 결과 및 안티바이러스 제품에 악성코드 탐지 규칙 등록 현황을 나타낸다. 98%의 정탐율로 zero-day 악성코드 탐지에도 효과가 있음을 보인다.

V. 결론 및 향후 연구 방향

최근의 침해시도는 고도화된 공격기법으로 침입의 사실을 인지하기 어렵다. 본 연구에서는 정상 행위 이벤트 분석을 통한 이상 징후 탐지 모델 제시를 통해 최근의 침해시도 대응 방법을 제시하였다. 패턴 기반의 이상 징후의 효율적인 분석 능력과 결합하여, 적용 실 사례와 같이 그 효과를 입증하였다. 또한 보안관리자 중심으로 수행되어진 기존의 보안관리, 침해사고 대응 태세를 사용자 및 관련 관리자의 방향으로 무게 중심을 이동하여 전체 사용자의 보안 의식을 항상 시키고자 하였다.

제안한 이상 징후 탐지, 관리 모델은 탐지 기법과 탐지 결과를 공유함으로써 그 효과를 향상시킬 수 있다. 또한 관리자가 관여해야하는 절차를 자동화하여 더욱 관리자의 역량에 의지하지 않고 보편적인 침해시도 탐지 수준을 향상시킬 수 있다.

앞서 거론한 것과 같이 시장에서 탐지 기법, 시나리오, Blacklist 등을 공유할 수 있도록 법적인 요소와 기술적인 요소를 추가적으로 연구할 필요가 있다. 또한 탐지 기법의 자동화, 표준화를 위해 머신러닝 등의 기술 적용 방안에 대해서도 연구를 진행할 예정이다.

References

[1] Daesung Moon, Hansung Lee, Ikkyun Kim, “Host based Feature Description Method for Detecting APT Attack”, Journal of The Korea Institute of Information Security & Cryptology VOL.24, NO.5, Oct. 2014
DOI: https://doi.org/10.13089/jkiisc.2014.24.5.839

[2] MoonGoo, Lee, Chunsock Bae, “A Study for the Principle Cases of Advanced Persistent Threat Attacks”, THE INSTITUTE OF ELECTRONICS ENGINEERS OF KOREA pp.939-942, Nov. 2013

[3] Sul-Hwa Im, Jong-Soo Kim, Jun-Keun Yang, Chae-ho Lim, “Present situation of APT and Response Strategies of new malware”, Korea Institute Of Information Security And Cryptology VOL.24, NO.2, April. 2014

[4] Sung-Baek HAN, Sung-Kwon Hong, “Countermeasures in APT attack for the financial sector”, Korea Institute Of Information Security And Cryptology VOL.23, NO.1, Feb. 2013

[5] Si-Jang Park, Jong-Hoon Park, “Current Status and Analysis of Domestic Security Monitoring Systems”, The Korea Institute of Electronic Communication Sciences VOL.9, NO.2, pp.261-266, Feb. 2014
DOI: https://doi.org/10.13067/jkiecs.2014.9.2.261

[6] Jaeho Lee, Sangjin Lee, “A Study on Unknown Malware Detection using Digital Forensic Techniques”, Journal of The Korea Institute of Information Security & Cryptology VOL.24, NO.1, Feb. 2014
DOI: https://doi.org/10.13089/jkiisc.2014.24.1.107

[7] Hojin Park, Sangjin Lee, “Build a Digital Evidence Map considered Log-Chain”, Journal of The Korea Institute of Information Security & Cryptology VOL.24, NO.3, Jun. 2014
DOI: https://doi.org/10.13089/jkiisc.2014.24.3.523

[8] Jae-Hwa Sim, Sung-Hwan Kim, Tai-Myoung Chung, “A Survey of Solutions using Security Information Event Management”, Proceedings of Symposium of the Korean Institute of communications and Information Sciences, pp.390-391, Jan. 2014

[9] Hyu Keun Shin, Kichul Kim, “Security Monitering Technology trends survey and A Study on the

next generation of security monitering framework", Journal of The Korea Institute of Information Security & Cryptology VOL.23, NO.6, Dec. 2014

[10] Kyu-il Kim, Hark-soo Park, Ji-yeon Choi, Sang-jun Ko, Jung-suk Song, "An Auto-Verification Method of Security Events Based on Empirical Analysis for Advanced Security Monitoring and Response", Journal of The Korea Institute of Information Security & Cryptology VOL.24, NO.3, Jun. 2014
DOI: https://doi.org/10.13089/jkiisc.2014.24.3.507

[11] Dae-Soo Choi, Yong-Min Kim, "BigData and Integrated security 2.0", COMMUNICATIONS OF THE KOREA INFORMATION SCIENCE SOCIETY VOL.30, NO.6, pp.65-72, Jun. 2012

[12] DeokJo Jeon, Dong-Gue Park, "Analysis Model for Prediction of Cyber Threats by Utilizing Big Data Technology", Journal of Korean Institute Of Information Technology. Vol. 12, No. 5, pp. 81-100, May. 2014
DOI: https://doi.org/10.14801/kiitr.2014.12.5.81

[13] Mee Lan Han, Deok Jin Kim, Huy Kang Kim, "Applying CBR algorithm for cyber infringement profiling system", Journal of The Korea Institute of Information Security & Cryptology VOL.23, NO.6, Dec. 2013
DOI: https://doi.org/10.13089/jkiisc.2013.23.6.1069

[14] Hyong-su Park, Huy-kang Kim, Eun-jin Kim, "Hacking Mail Profiling by Applying Case Based Reasoning", Journal of The Korea Institute of Information Security & Cryptology VOL.25, NO.1, Feb. 2015
DOI: https://doi.org/10.13089/jkiisc.2015.25.1.107

[15] Ho-sub Lee, Eung-ki Park, Jung-taek Seo, "A New Method to Detect Anomalous State of Network using Information of Clusters", Journal of the Korea Institute of Information Security and Cryptology VOL.22, NO.3, pp.545-552, Jun. 2012

[16] Ki-Soon Yu, Sul-Hwa Im, Hak-Beom KIM, "Technology Trends of SIEM and direction of improvement", Journal of The Korea Institute of Information Security & Cryptology VOL.23, NO.6, Dec. 2014

[17] Kyung-Shin Kim, "Security Analysis and Improvement of Integrated Security Management System", Journal of Institute of Internet, Broadcasting and Communication VOL.15, No.1, pp.15-23, Feb. 2015
DOI: https://doi.org/10.7236/jiibc.2015.15.1.15

저자 소개

권 영 백(정회원)

- 2015년 3월~현재 : 고려대학교 정보보호대학원 금융보안학과 석사과정

김 인 석(정회원)

- 2008년 : 고려대학교 정보경영공학과 (박사)
- 2009년~현재 : 고려대학교 정보보호대학원 교수
- 現 FDS산업포럼 회장, 한국사이버정보전학회 운영위원 등