정 보 보 호 학 회 지
제28권 제2호, 2018. 4

KOSIGN:정보보호제품 관점의 사이버위협정보 공유 체계

임 원 식*, 윤 명 근*, 조 학 수**

요 약

맥아피 연구소의 2017년 12월 위협 보고서에 따르면 2017년 3분기에만 사상 최대인 5,760만개의 신규 악성코드가 수집되었다. 쏟아지는 악성코드와 신규위협에 대응하기 위해 각 기관의 위협대응센터에서 정보를 분석해 대응정책을 수립하고 보안제품을 운영하기에는 한계에 봉착했다. 위협대응 비용을 절감하고 사이버위협에 선제적으로 신속하게 대응하기 위해 사이버위협 정보 공유 체계 구축이 해법으로 제시되고 있다. 국내 보안산업계 또한 사이버위협정보 공유의 필요성이 증대되고 있으며 2017년부터 KOSIGN(Korea Open Security Intelligence Global Networks) 프로젝트를 통해 정보수집체계, 분석시스템, 정보 표현 포맷과 공유 프로토콜 정의 및 각 주체간의 정보공유를 위한 동기부여 방안에 대해 연구가 진행되고 있다. 본 논문에서는 해외 및 국내의 정보공유체계 동향에 대해 소개하고 KOSIGN 프로젝트에서 수행한 정보공유체계에 적용한 기술에 대해 소개하고자 한다.

Ⅰ. 서 론

맥아피 연구소의 2017년 12월 위협보고서에 따르면 2017년 3Q에 사상 최대인 5,760만개의 신규 악성코드를 수집했다[1]. 악성코드 증가 원인으로 전문가들은 악성코드 소스의 공개 및 자동제작도구의 등장으로 인한 손쉬운 악성코드 개발을 원인으로 꼽고 있다[2].

악성코드의 폭증과 은밀해지는 사이버 위협을 대응하기에는 “위협정보 공유만이 기술격차를 극복할 방안이다”[3]라고 언급할 정도로 사이버위협정보 공유의 중요성이 커지고 있다.

본 논문에서는 사이버위협정보 공유에 대한 국제 및 국내 동향과 정보공유 체계에 대한 소개와 2018년 현재 개발 중에 있는 국내 정보보호 산업계 중심의 사이버위협정보 공유시스템인 KOSIGN에 대한 소개와 사이버위협정보 공유의 문제점과 대응방안을 제시하고자 한다.

1.1. 해외 동향

1998년 정보공유분석센타(ISAC,Information Sharing & Analysis Center))이 최초 설립 당시에는 국가기반시설에 대한 취약점 정보 공유 및 대응이 목적이었다. 2013년 2월 미행정부는 주요 기반시설의 사이버보안 강화를 위한 행정명령을 발효하였으며, 사이버보안 정보공유시스템 구축과 민관 정보공유 강화가 포함되었다.

국토안보부(DHS,Department of Homeland Security)는 주요 기반시설 운영자간의 정보 공유 및 관리 프로세스와 매뉴얼 작성하여 정부와 민간부문간 정보 공유체계의 근거를 마련하였으며, 이로 인해 2014년 사이버 위협정보공유 협의체(CTA, Cyber Threat Alliance)가 설립되었다.

STIX(Structured Threat Information Expression) 및 TAXII(Trusted Automated eXchange of Indicator Information)는 정보공유시스템에 활용하기 위한 표준화된 언어와 통신프로토콜에 대한 요구에 맞추어 DHS

이 논문은 2018년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임(No. 2017-0-00513, Security Analytics 기반의 이기종 보안솔루션 위협 분석 및 대응 기술 개발)
* 국민대학교 소프트웨어융합대학 컴퓨터공학과 정보보호연구실(mkyoon@kookmin.ac.kr)
** ㈜윈스 연구개발본부(excel21c@wins21.co.kr, marius71@wins21.co.kr)

에서 표준화가 시작되었다.

2014년 북한이 연루된 것으로 추정하는 SONY Pictures의 해킹 사건을 계기로 미국 백악관에서는 2015년 2월 재차 행정명령을 내리는 등 사이버보안위협은 국가안보 문제로 격상되었다.

1.2. 국내 동향

국내 사이버위협대응체계는 1995년 정보화촉진기본법 14조2항(정보보호 등)에 근거를 둔 한국정보보호센터가 설립하고, 이후 2001년7월 한국정보보호진흥원(현 한국인터넷진흥원)이 시초라 할 수 있다.

정보공유체계 측면에서는 2001년 7월 시행된 정보통신기반보호법의 16조(정보공유•분석센터)에 근거하여 2002년 설립된 금융 정보공유분석센터(ISAC) 및 증권, 통신, 전력 분야 ISAC으로부터 시작되었다고 볼 수 있다.

한국인터넷진흥원은 2014년 8월 사이버위협정보 수집분석공유를 위한 C-TAS 서비스를 시작하였다.

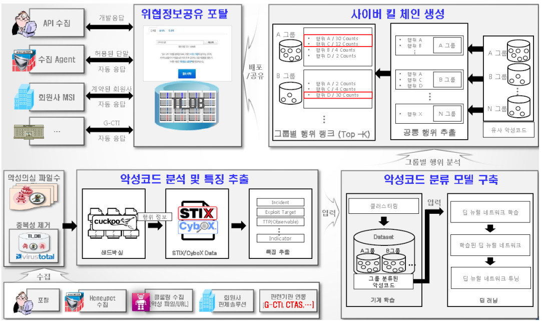
민간의 자발적 위협정보공유 체계는 1996년 정보통신망 침해사고 대응팀 간 정보 및 기술공유를 위해 발족한 한국 침해사고 대응팀 협의회(CONCERT, Consortium of CERT)가 있으며 보안산업계를 중심으로 정보공유 협의체는 별도로 구성되어 있지 않다.

Ⅱ. KOSIGN 정보 공유 서비스

본 연구에서는 보안 산업계를 중심으로한 사이버위협정보 공유체계의 구축과 운영에 필요한 요건을 분석하고 사이버 위협 정보공유시스템으로서 KOSIGN의 구현 내용을 소개하고자 한다.

KOSIGN은 보안산업계의 보안제품에서 활용 가능한 사이버위협정보를 정의하고 그 정보를 시스템 내에서 수집,생산,가공하여 표준화된 정보로 공유하기 위한 일련의 프로세스를 처리하는 시스템이다([그림 1] 참고).

NIST SP 800-150은 사이버위협정보 공유체계를 설계함에 있어 좋은 출발점이다. NIST에서 사이버위협정보는 조직이 위협으로부터 자신을 보호하거나 탐지하는 활동에 도움이 되는 정보로 정의하고 있다. 구체적으로는 지시자(Indicators), 전략기술절차(TTP), 보안경보



〔그림 1〕 KOSIGN 시스템 개요

(Security Alerts), 위협 첩보 보고서(Threat Intelligence reports), 도구 설정(Tool configurations)을 예로 들고 있다[4].

2.1. KOSIGN의 위협정보

KOSIGN에서 공유하는 정보는 정보공유체계를 거쳐 최종적으로 방화벽,침입방지시스템,백신,라우터 등 각 보안제품에서 보안정책으로 활용 가능한 정책을 공유하는 것을 목표로 한다. 보안제품에서 사용 가능한 정보와 정책을 기술하기 위해 STIX 표준을 사용하여지시자(Indicator)를 중심으로 한 위협정보를 생산한다.

한국인터넷진흥원에서 운영 중인 C-TAS(Cyber Threat Analysis System)의 공유 위협정보는 위협도메인, 사이버 사기 도메인, 악성파일, 취약점, 보고서등 총 5개 그룹, 36종의 정보를 외부기관에 공유하고 있으며 XML 형식의 자체 표준양식인 CTEX(Cyber Threat EXpression) 문법으로 작성된 문서를 자체 API를 통해

〔표 1〕 KOSIGN의 위협정보

분류	평판정보	공유정보 내역
지시자	악성파일	유포지, C&C, 해시, API, 유사 악성코드 그룹, 시스템 내 증적, Network 패킷정보, 악성 코드 유사도
지시자	도메인 IP	공격명, 패턴, 공격지, raw packet, 위험도
지시자	정상파일	제조사, 제품명, 해시,API, 유사 정상코드 그룹, 정상코드 유사도
지시자	탐지문자열	공격명, 공격패턴, 탐지정책 형식(SNORT, YARA), CVE 코드, 위험도

공유하고 있다. 사이버보안 관련 기업, 백신업체, 인터넷 서비스 제공업체 등 112개 회원기업을 보유하고 있으며 2억1백만건(2016.6.22. 기준)의 위협정보를 공유하고 있다[5].

2.2. 정보 수집 및 공유 방안

사이버위협정보 공유 서비스를 시작할 때 공유할 정보가 없는 상태에서 서비스를 시작하는 딜레마에 직면한다. 이를 해결하기 위해 서비스 시작 전에 일정 규모의 정보 수집을 위한 투자가 필요하며 이후에 지속 운영을 위한 비용이 수반된다.

이러한 정보의 수집 • 제공 측면의 비용을 포함한 가입조건 및 운영방식에 따라 다음 3종류의 공유협의체로 분류할 수 있다.

- ISAC 협의체 : CERT(Computer emergency response team)와 CSIRT(Computer Security Incident Respose Team) 같이 유사 영역에서 사이버 보안 업무를 수행하는 주체간의 동등한 위협정보 공유 함. 추천또는 자격심사에 따라 가입하는 폐쇄형으로 운영됨.
- 기관주도 협의체 : DHS의 AIS(Automated Indicator Sharing), KISA의 C-TAS와 같이 특정 기관이 주도하여 정보를 수집, 분석 공유.
- 기타 자율 협의체 : Google의 VirusTotal, KOSIGN, 세인트시큐리티의 malwares.com과 같이 민간이 운영하며 가입조건 및 공유정보 활용조건이 협의체에 따라 또는 가입 이후에도 변경된다[4].

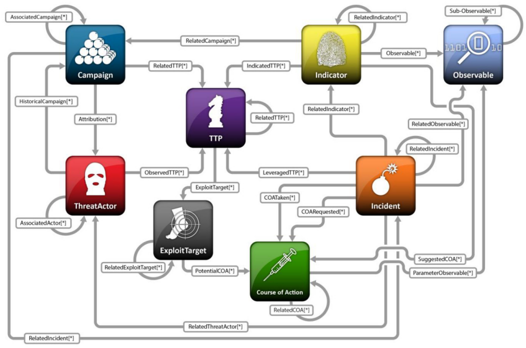
2.3. 정보공유 표준화

사이버위협정보를 공유하기 위해서 각 기관 간에 위협정보를 기술하는 언어와 그 언어로 표현된 문서를 전송하는 방식을 상호 표준화 하여야 한다. 다수 기업 간의 위협데이터 공유 표준화를 위해 미국토안보부는 MITRE와 함께 2013년 사이버 보안위협 정보공유 표현 표준 STIX와 전송 표준 TAXII를 발표하였다.

KOSIGN 서비스는 2017년에 STIX v1.2와 TAXII 1.1로 시범 개발하였으며 2.0으로 변경 진행 중이다.

2.3.1. STIX

STIX는 사이버 위협정보의 개념을 총 8개의 구성요소로 구조화하여 표준화 하였다. [그림2]는 STIX v1.1 8개 구성요소의 구성도이다. 그리고 기술하는 언어는 XML을 활용하였다. 이후 1.2에서 Report 객체가 추가되었다. 2017년 STIX v2.0에서는 총 12개의 STIX 도메인 객체(SDO:STIX Domain Objects)와 2개의 STIX 관계 객체(SRO:STIX Relationship Objects)로 정의하였다. 그 구현은 기존의 XML에서 JSON으로 간결하게 변경하였다.



〔그림 2〕 STIX v1.1 구성도

2.3.2. TAXII

TAXI는 또한 HTTP와 XML을 활용하여 전송프로토콜로 사용하고 있으며 PUSH, PULL, DISCOVERY, FEED MANAGEMENT 총 4종류의 서비스로 구성되어 있다. 하지만 암호화 통신에 대해 구체적인 정의가 없으며, 연동 주체간의 상호 인증에 대한 방법도 정의하지 않았다. 또한 XML을 사용하고 메시지의 크기가 너무 크다는 단점이 있다. 이에 TAXI v2.0에서는 JSON으로 변경되었고, 암호화를 위해 모든 통신에 HTTPS(HTTP over TLS)로 변경하였다. 또한 인증은 HTTP 기본 인증규격인 RFC7617을 채용하였다.

2.3.3. MAEC

MITRE에서 맬웨어의 속성(attributes)과 행위(behaviors) 정보를 기술하기 위해 개발된 구조적 언어이다. 이전에는 악성코드 분석가들이 악성코드 분석보

고서를 작성하고 그 정보를 공유하는데 속성을 표현하기에 모호하게 기술되어 잘못된 정보로 공유되거나 중복으로 분석하는 문제가 발생하였으나 MAEC (Malware attribute enumeration and characterization)을 사용하므로 악성파일의 정보공유 문제가 해결되었다. MAEC 5.0에서는 기존의 XML에서 JSON (JavaScript Object Notation)으로 적용 가능하게 확장되었다.

2.3.4. CybOX

CybOX(Cyber Observable eXpression)는 MITRE에서 MAEC을 개발하던 팀이 2010년에 맬웨어의 행위를 포함한 전반적인 증적(Cyber Observable)을 기술하기 위해 개발된 표준 언어로서 2012년에 1.0이 완성되었다.

“Cyber Observable”이라함은 사이버 영역에서 상태 속성을 가지고 있거나 측정 가능한 이벤트를 의미한다. 즉 위협의 평가기준/속성, 각종 로그 기록, 사이버 상황 인지, 사고 대응, 디지털 증적, 사이버 위협정보 공유 등 다양한 영역을 포함한다.

이러한 특성으로 STIX v2.0에서는 아예 인해 CybOX를 포함하였다.

Ⅲ. 위협정보 분석 자동화

사이버위협정보의 생산은 기관의 업무 성격에 따라 다르다. CERT 업무를 담당하는 조직은 취약점 리포트를 수집하여 조직 내 침해사고에 대한 조사 및 분석활동과 그 리포트를 결과물로 생산한다. KISA의 C-TAS는 각 기관으로부터 접수한 위협도메인, 사기도메인, 악성파일, 취약점, 사고보고서의 방대한 정보를 생산한다.

맥아피의 2017년12월 보고서에 따르면 3분기에 수집된 악성코드의 수가 5,760만개에 달한다. 하루에 60만개 이상을 분석하여 사이버위협정보로 공유해야 하는 것을 의미한다.

악성코드 자동 분석은 악성파일의 실행 여부에 따라서 행위를 분석하는 동적 분석과 실행하지 않고 악성파일 자체 또는 역어셈블 결과를 이용하여 분석하는 정적 분석으로 나뉜다.

3.1. 정적분석

악성파일을 실행하지 않고 문자열, byte- sequence n-gram과 라이브러리 호출, 제어 흐름 그래프(control flow graph)와 opcode(operation code) 분포를 분석하거나, “IDA Pro”와 “OllyDbg”와 같은 역어셈블러나 디버거를 이용하여 어셈블리 명령어로 변환하여 분석하거나 “LordPE”와 “OllyDump”와 같은 메모리덤프 프로그램을 활용하기도 한다. 하지만 압축하거나 리버스 엔지니어링을 활용하지 못하도록 패킹 또는 난독화 하는 기법을 활용한 경우는 정적 분석의 한계가 존재한다 [6].

3.2. 동적분석

악성파일을 통제된 환경에서 실행하면서 시스템과 상호작용을 분석하는 방법을 동적 분석이라 부른다. 행위를 추출하기 위해서는 모니터링 도구와 “Capture BAT”과 같은 시스템 레지스트리 모니터링 도구와 프로세스 모니터링 도구, “Wireshark”과 같은 트래픽 모니터링 도구, “Regshot”과 같은 시스템 변형 탐지 도구를 활용한다.

동적분석은 정적분석보다 분석능력에 있어 월등 하지만 시간과 시스템 자원을 많이 소비하는 문제가 있다. 또한 특정시간에만 동작하도록 하는 시한폭탄(time bomb)과 특정 조건이 일치하면 행위를 시작하는 논리폭탄(logic bomb) 기능을 가지고 있는 경우 분석에 한계가 있다. 또한 주로 가상환경을 활용하는데 이러한 가상환경을 인식하여 행위를 조절하는 경우 분석에 한계가 있다.

3.3. KOSIGN의 악성파일 자동분석

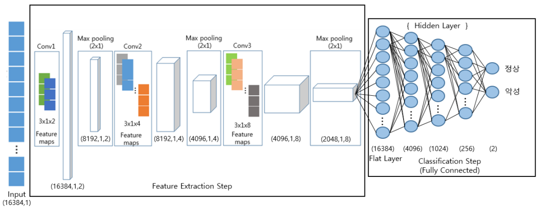
KOSIGN 시스템에서는 악성파일의 대량 분석을 위해 CNN(Convolutional Neural Network)을 활용한 정적 분석을 통해 악성파일을 분류하는 지도학습을 적용하였다. 지도학습 방식을 적용하는 경우 “학습데이터의 레이블을 어떻게 정의할 것인가”라는 문제에 봉착한다. 전문가가 분석하여 레이블을 정의하기에는 학습데이터가 너무 방대한 것이 문제이다. 본 연구에서는 카스퍼스키(Kaspersky) 백신의 탐지 레이블을 활용하였다.

KOSIGN에서는 2017년 7월27일부터 9월30일까지 총 66일간 수집한 윈도우 실행 악성코드 파일 3,494,747건을 사용하여 CNN을 활용하여 분석하였다. 66일중 초기 35일을 학습용 데이터로 활용하고 이후 31일을 테스트 데이터로 사용하여 시계열에 따른 지속적 학습•검증 모델로 활용할 수 있도록 시험을 설계하였다[7].

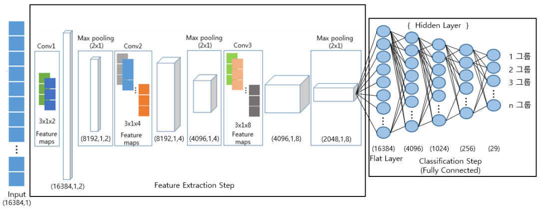
문제는 CNN에 악성파일을 입력하기 위해서는 고정 사이즈로 데이터를 변환하여야 한다. KOSIGN에서는 4,096 바이트의 고정 크기를 사용하였으며 바이너리를 “Objdump”를 활용하여 디스어셈블하고 정적분석을 진행하였다.

그 결과 악성과 정상만을 구분하는 이진 분류 시 98%의 정확도를 악성에 대해 29개의 세부 그룹까지 분류하는 다중분류의 경우 83%의 정확도를 기록하였다[8]([그림3] 이진 분류기,[그림4] 다중 분류기)

악성파일의 다중분류 결과가 이진분류대비 정확도가 낮은 점에 대해서는 Aziz의 연구에 따르면 학습데이터로 활용되는 악성코드의 레이블의 정확도에 의해 학습 및 시험결과의 정확도에 영향이 있다는 점이다[9]. 따라서 다중 분류의 정확성 향상을 위해서는 학습데이터의 레이블의 정확도를 향상하는 연구가 필요하다.



〔그림 3〕 CNN모델 이진 분류기



〔그림 4〕 CNN모델 다중 분류기

Ⅳ. 사이버위협정보 공유 문제점

사이버위협정보를 공유하기 위하여 조직간 공유 프로토콜을 표준화하고 시스템을 구축하고 사이버위협정보를 수집 공유하기 위해 투자 및 구축을 진행하게 되면 공격 대응시간 및 대응 비용에 있어 효과가 있다는 사실은 명확하다. 보안 산업계 또한 협업을 통한 정보공유로 사이버위협에 대응비용을 절감하고 사이버위협정보를 신속히 생산 공유하므로 인해 산업경쟁력 강화 효과를 기대할 수 있다. 하지만 보안 산업계의 특성상 각 기업 간 정보 공유 협업에 다음과 같은 문제점이 존재한다[4].

◦ 공유자 간 신뢰 부족
◦ 공유자 간 경쟁 관계로 인한 약한 공동목표
◦ 공유로 인한 정보유출 문제 법규, 계약 위반

4.1. 공유 정보 품질과 무임승차 문제

ISAC형태의 공유협의체를 운영하거나 기타 자율 협의체를 운영할 경우 위협정보를 지속적으로 생산하는 상임운영기관이 존재하지 않으면 공유자간의 무임승차와 같이 정보의 과실은 취하되 정보공유에 기여하지 않는 문제로 인해 공유체계의 정보품질이 약화되며 결과적으로 공유협의체를 지속하지 못하는 문제가 발생한다. 정보공유체계에서 무임승차문제는 P2P 시절부터 많은 연구가 이루어졌다[10].

정보공유 딜레마를 방지하기 위한 방법으로는 공유되는 정보의 품질(QoI,Quality of Indicators)을 계량화한다. 이를 위해 다음 4종류의 측도를 활용한다. 정확성(correctness) 즉 제공된 정보의 주석이나 분류가 의미있고 올바른지에 대한 측도와 제공된 정보가 회원들에게 필요한 정보인지(relevance), 제공된 정보가 사용성(utility)이 좋은지, 즉 회원들이 즉시 사이버위협 방어를 위해 주어진 정보를 활용할 가치가 존재하는지, 제공된 정보가 이미 다른 회원에 의해 제공된 정보와 유사하지 않는지(uniqueness)를 바탕으로 공유된 정보의 품질을 측정한다. QoI의 네 측도를 평가자 또는 공유정보를 활용하는 회원들이 매번 평가하는 것은 비용과 정확도에 문제가 발생한다. 이를 위해 일정 규모의 학습데이터를 구축하여 이를 학습한 이후에 회원이 제공한 공유데이터에 LDA를 이용하여 추정하는 방법론을 활용하였다[11].

4.2. 민감정보 공유

사이버위협정보를 공유할 때 개인정보 또는 관리되지 않은 민감 정보가 포함되어 공유 될 가능성이 존재한다. 보안회사에서 사이버위협정보 공유를 위해 정보를 제공할 때 의도치 않은 민감 정보의 공개로 인해 공유자는 법적,재정적 손실이 발생할 수 있다. 특히 국내의 경우 정보통신망법과 개인정보보호법으로 인해 직접적으로 법적 처벌을 받게 된다. 따라서 기관,기업의 사이버 위협정보의 자발적 정보공유는 더욱 어려운 환경이다.

Deepak은 정보공유체에 가입하려는 기관입장에서 정보 공유를 통한 인센티브와 가입비용 그리고 가입 후에 위협정보 공유로 인한 이익 관점에서 게임이론을 활용하여 기관이 정보공유 협의체에 자발적으로 참여할 수 있는 최적화 전략을 제시하였다[12].

KOSIGN 또한 그 운영에 있어 정보를 자발적으로 공유하는 기관과 법적 이유로 인해 자발적 정보 공유가 불가하고 단지 정보 활용만 가능한 기관이 존재한다. 차별화된 가입비와 인센티브 전략을 도입함으로써 지속가능한 정보공유체제 운영이 가능하다.

4.3. 사이버위협 정보의 변화

사이버위협정보는 한 조직에 공격이 유입된 정보를 자발적 신고에 의해서 위협정보공유체계에 수집하고 분석하여 회원사에 그 공격이 유입되어 침해사고가 발생하기 전에 공유 및 보안정책의 적용이 완료되어야 위협정보의 공유 목표가 달성되었다고 할 수 있다.

신속한 정보공유를 위해서 수집-분석-공유-정책적용의 네 단계가 자동화된 시스템에 의해 연동되어야한다. 실제로 구현된 사이버위협정보 공유체계는 점진적으로 자동화 되고 있다.

하지만 사이버위협은 지속적으로 변화되므로 인해 공유해야할 위협정보의 구조가 시간이 흐름에 따라 변경된다. 자동화된 공유체계의 각 구성요소가 변화된 환경에 맞게 수정되기 위해서는 막대한 비용이 소요될 수 있다. 이를 방지하기 위해서는 위협정보의 구조 변화에 유연하게 변경가능 하도록 정보공유체계를 설계하여야 한다.

V. 결 론

사이버 공격이 고도화됨에 따라 위협 대응 비용을 낮추고 신속하게 대응하기 위해 사이버위협정보 공유체계를 구축함에 있어 정보의 수집-분석-공유-적용 단계별 자동화가 필요하다. 수집된 정보에 대해 신속하고 정확한 분석을 위해 기계학습을 적용한 자동 분석시스템을 적용한다. 자동화된 공유체계를 유지하기 위해 STIX와 TAXII의 정보시스템 공유 표준을 공유시스템과 보안장비에 적용하여 공유 비용과 배포시간을 단축시킬 수 있다.

정보공유체계를 운영함에 있어 민감 정보의 의도하지 않은 노출을 방지하고자 정보의 자동 필터링 및 민감 정보 모니터링 체계가 필요하다. 또한 공유 회원의 자발적 정보 공유에 대한 동기부여를 위해 게임이론에 근거한 인센티브를 제공한다면 공유 체계의 부작용을 최소화 하면서 지속가능한 시스템 운영이 가능하다.

참 고 문 헌

[1] McAfee Labs, “McAfee Labs Threat Report”, McAfee, Dec. 2017.

[2] 강홍구, 김경한, 유대훈, 최보민, 박준형, “악성코드 행위기반 유사도 측정 기법 연구”, 한국통신학회 학술대회논문집, pp. 697-698, 2017.

[3] A. John, R. Peter, “Electric Communi- cation Development,” *Communications of the ACM*, 40, pp. 71-79, May 1997.

[4] NIST SP 800-150, Guide to Cyber Threat Information Sharing

[5] 보안뉴스, 국내 진출 글로벌 보안기업-KISA, 사이버위협 대응 ‘힘 모아’, 22. Jun. 2016

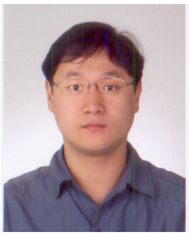
[6] Gandotra, Ekta, Divya Bansaland and Sanjeev Sofat. "Malware analysis and classification: A survey." Journal of Information Security vol. 5, no. 02, pp. 56, 2014

[7] Xin Hu, Sandeep Bhatkar, Kent Griffin, and Kang G. Shin, “MutantX-S: Scalable Malware Clustering Based on Static Features”, USENIX ATC, 2013

[8] 정지만, 홍성현, 김영재, 명준우, 정선민, 이진우, 김준호, 윤명근, “4차 산업혁명을 대비한 딥러닝

기술의 금융보안 적용 연구”, 금융정보보호공모전 최우수논문상 2017.
[9] Aziz Mohaisen, Omar Alrawi, Mannar Mohaisen, “High-fidelity, behavior-based automated malware analysis and classification”, computers & security, vol. 52, pp. 251-266, 2015
[10] Tomas Locher, Patrick Moor, Stefan Schmid, Roger Wattenhofer, “Free riding in BitTorrent is cheap”. in Proc. Workshop on Hot Topics in Networks (HotNets), pp. 85-90, 2006.
[11] Omar Al-Ibrahim, Aziz Mohaisen, Charles Kamhoua, “Beyond Free Riding: Quality of Indicators for Assessing Participation in Information Sharing for Threat Intelligence”, arXiv preprint arXiv:1702.00552, 2017.
[12] Deepak Tosh, Shamik Sengupta, Charles Kamhoua, Kevin Kwiat, Andrew Martin, “An evolutionary game-theoretic framework for cyber-threat information sharing”, In Communications(ICC), IEEE, pp. 7341-7346 2015

〈저자소개〉



임 원 식 (Lim Wonsick)
정회원
1998년 2월 : 수원대학교 전기공학과 졸업
2016년 8월 : 고려대학교 정보통신대학원 빅데이터융합학과 석사과정
2004년 3월~현재 : (주)윈스 연구개발본부 수석연구원/팀장
관심분야 : 통합보안솔루션, 기계학습, SIEM

윤 명 근(Yoon, MyungKeun)
정회원
1996년 2월 : 연세대학교 컴퓨터 과학과 학사
1998년 2월 : 연세대학교 컴퓨터 공학과 석사
2008년 12월 : University of Florida, 컴퓨터공학 박사
1998년 1월~2010년 2월 : 금융결제원 과장
2010년 3월~현재 : 국민대학교 컴퓨터공학과 부교수
관심분야 : 컴퓨터&네트워크 보안, Randomized Algorithm, 지능형 보안, 금융 보안

조 학 수 (Harksu Cho)
정회원
1997년 2월 : 서울대학교 계산통계학과 전산과학전공 졸업
1999년 2월 : 서울대학교 전산과학과 석사 졸업
2016년 3월 ~ 현재 : 고려대학교 컴퓨터 • 전파통신공학과 박사과정
2001년 12월 ~ 현재 : (주)윈스 연구개발본부장/전무이사
관심분야 : 사이버보안, 네트워크보안, 인공지능