KIPS Trans. Comp. and Comm. Sys.
Vol.7, No.10 pp.251~258 pISSN: 2287-5891

https://doi.org/10.3745/KTCCS.2018.7.10.251

Real-Time Ransomware Infection Detection System Based on Social Big Data Mining

Mihui Kim† · Junhyeok Yun††

ABSTRACT

Ransomware, a malicious software that requires a ransom by encrypting a file, is becoming more threatening with its rapid propagation and intelligence. Rapid detection and risk analysis are required, but real-time analysis and reporting are lacking. In this paper, we propose a ransomware infection detection system using social big data mining technology to enable real-time analysis. The system analyzes the twitter stream in real time and crawls tweets with keywords related to ransomware. It also extracts keywords related to ransomware by crawling the news server through the news feed parser and extracts news or statistical data on the servers of the security company or search engine. The collected data is analyzed by data mining algorithms. By comparing the number of related tweets, google trends (statistical information), and articles related wannacry and locky ransomware infection spreading in 2017, we show that our system has the possibility of ransomware infection detection using tweets. Moreover, the performance of proposed system is shown through entropy and chi-square analysis.

Keywords : Ransomware, Infection Detection System, Social Big Data Mining, Entropy, Chi-Square

소셜 빅데이터 마이닝 기반 실시간 랜섬웨어 전파 감지 시스템

김 미 희† · 윤 준 혁††

요 약

파일을 암호화시켜 몸값을 요구하는 악성 소프트웨어인 랜섬웨어는 빠른 전파력과 지능화로 더욱 위협적이 되고 있다. 이에 빠른 탐지 및 위험 분석이 요구되고 있지만, 실시간 분석 및 보고가 미비한 상태이다. 본 논문에서는 실시간 분석이 가능하도록 소셜 빅데이터 마이닝 기술을 활용하여 랜섬웨어 전파 감지 시스템을 제안한다. 본 시스템에서는 트위터 스트림을 실시간 분석하여 랜섬웨어와 관련된 키워드를 가진 트윗을 크롤링한다. 또한 뉴스피드 분석기를 통해 뉴스서버를 크롤링하여 랜섬웨어 관련 키워드를 추출하고, 보안업체의 서버나 탐색 엔진을 통해 뉴스나 통계데이터를 추출한다. 수집된 데이터는 데이터 마이닝 알고리즘으로 랜섬웨어 감염 정도를 분석한다. 2017년 전파가 많이 되었던 워너크라이와 록키 랜섬웨어 감염전파 시 관련 트윗의 수와 구글 트렌드(통계 정보) 정보, 관련 기사를 비교하여 트윗을 이용한 본 시스템의 랜섬웨어 감염 탐지 가능성을 보이고, 엔트로피와 카이-스퀘어 분석을 통해 제안 시스템 성능을 보인다.

키워드 : 랜섬웨어, 전파 감지 시스템, 소셜 빅데이터 마이닝, 엔트로피, 카이-스퀘어

1. 서 론

랜섬웨어는 몸값(ransom)과 소프트웨어(software)의 합성어로 시스템을 잠그거나 데이터를 암호화해 사용할 수 없도록 만들고 이를 통해 금전을 요구하는 악성 프로그램이다[1]. 2017년 5월 12일 워너크라이(wannacry) 랜섬웨어는 유포 하루 만에 전세계 100여 개국 컴퓨터 12만대 이상 감염시키며 전세계를 공포로 몰아넣었다[2]. 이후 다양한 랜섬웨어가 등장하여 그 피해가 증가하고, 병원, 극장 등의 사회간접자본을 마비시키는 사례도 발생하였다[3]. 랜섬웨어 전파속도는 앞에 소개한 워너크라이의 경우에서도 알 수 있듯이 빠르게 진화하고 있고, 2016년 국내 랜섬웨어 감염된 피해자는 13만 명에 이르며, 피해액은 3000억 원에 달하는 것으로 보고되었다[4]. 전세계적으로는 2017년 랜섬웨어 피해만 2년 만에 15배 증가해 50억 달러를 기록할 것이라 보고되었다[1].

이러한 위협적인 악성 소프트웨어에 대한 대응을 위해 국내에서는 한국랜섬웨어침해대응센터가 생겼고, 각 보안업체

※ 이 논문은 2015년도 정부(교육부)의 재원으로 한국연구재단 기초연구사업의 지원을 받아 수행된 연구임(No. 2015R1D1A1A01057362).
† 종신회원 : 한경대학교 컴퓨터공학과(컴퓨터시스템연구소) 교수
†† 준 회 원 : 한경대학교 컴퓨터공학과 학부생
Manuscript Received : May 14, 2018
First Revision : June 27, 2018
Accepted : July 26, 2018
* Corresponding Author : Mihui Kim(mhkim@hknu.ac.kr)

에서도 관련 분석 기사를 내고 있다. 하지만 사후처리로 랜섬웨어 침해사고 신고 접수나 침해사고 통계 및 분석을 제공하고, 사전예방으로 주기적 데이터 백업, 최신 보안업데이트 적용, 익숙하지 않은 웹 사이트 방문 자제, 익숙하지 않은 의심 파일 실행 자제 등 일반적인 대응 방법만을 제공할 뿐이다. 랜섬웨어도 빠른 전파력이 위협적인 만큼 빠른 대응이 중요한데, 현재 랜섬웨어의 위험도나 전파 급증 등을 실시간으로 알려주는 언론 매체나 보안 사이트가 없다. 랜섬웨어는 점점 지능화되고 공격범위도 확장되고 있지만, 뒤늦은 경고나 보고, 대응으로 감염 피해가 증가하는 실정이다.

랜섬웨어의 빠른 전파속도 및 점점 넓어지는 전파 범위로 사전대응과 함께, 랜섬웨어 전파 시 빠른 탐지가 가장 중요하다. 본 논문에서는 실시간 탐지를 위한 기본 빅데이터로서 소셜 네트워크 서비스(Social Network Service, SNS) 데이터를 사용하고자 한다. SNS는 사용자 간의 자유로운 의사소통과 정보 공유를 하는 등 사회적 관계를 생성하고 강화해 주는 온라인 플랫폼이다[5]. 대표적인 SNS인 페이스북(facebook)이나 트위터(twitter)의 이용자 수는 이미 2011년에 1천만 명을 돌파하여 사람들의 관심, 현재 이슈 등을 분석하는데 좋은 빅데이터 소스로서 주목 받고 있다. 이는 SNS 데이터를 활용하여 데이터 마이닝 기술을 접목하여 분석하는 '소셜 빅데이터 마이닝'이라는 이름으로 최신 유행, 최근 관심, 실시간 분석을 위해 다양한 분야(예, 학문 분야 및 융합 키워드 추천 서비스[6], 대학 인식 및 선호도 분석[7], 독감 유행의 예측을 위한 연구[8, 9], 관광행동 분석 또는 개인 맞춤형 장소 추천 시스템 개발[10] 등)에 사용되고 있다.

본 논문에서는 소셜 빅데이터 마이닝 기술을 활용하여 랜섬웨어 실시간 전파 감지 시스템을 제안하고자 한다. 해당 시스템은 크게 데이터 수집 모듈과 데이터 처리모듈로 구성되어 있다. 데이터 수집 모듈에서는 트위터 SNS 스트림을 실시간 분석하여 랜섬웨어와 관련된 키워드를 가진 트윗을 크롤링한다. 또한 뉴스피드 분석기를 통해 뉴스서버를 크롤링하여 랜섬웨어 관련 키워드를 추출한다. 이러한 스트림 데이터와 함께, 보안업체의 서버나 탐색엔진에서 뉴스나 통계데이터를 추출한다. 데이터 처리 모듈에서는 불필요한 정보가 함께 담긴 경우 필터링하여 데이터 마이닝 알고리즘으로 랜섬웨어 감염 정도를 분석한다.

본 논문은 선행연구[11]의 확장연구로서 랜섬웨어 전파 감지 시스템의 간단한 설계내용을 담고 있다. 본 논문에서는 [11]에서 제안한 모델을 상세 설계한 후, 이에 대해 프로토타입 시스템을 구현하고 실험 분석을 수행한다. 특정 랜섬웨어와 관련된 트윗을 추출하여 관련 기사와 구글 트렌드 통계값을 비교하여 트윗을 통한 랜섬웨어 위험성 분석의 가능성을 보여준다. 또한 관련 트윗에 대한 엔트로피, 카이-스퀘어 분석을 통해 랜섬웨어 감염 전파의 정도를 분석한다.

2장에서 랜섬웨어와 관련연구를 소개하고, 3장에서 제안하는 랜섬웨어 전파 감지 시스템을 설명한다. 4장에서 실험 및 분석내용을 설명하고, 5장에서 결론을 맺는다.

2. 관련 연구

2.1 랜섬웨어

신뢰할 수 없는 사이트나 스팸메일, 파일공유사이트 등을 통해 유포되는 랜섬웨어는 1989년 AIDS라는 이름으로 처음 등장하여 2015년 유명 커뮤니티사이트를 통한 대규모 감염 사태를 분수령으로 본격적인 존재감을 드러냈다[12]. 국내에는 2017년 윈도우즈의 SMB (server message block) 취약점으로 전파되는 워너크라이 랜섬웨어에 대거 감염되는 사태가 발생하며 그 피해와 함께 관심도가 높아지게 되었다.

이로 인해 빠른 탐지 및 감염전파 차단에 대한 중요성이 강조되고 있어 관련 연구로서 시그니처 기반의 탐지패턴 자동화 모델이 연구되었다[13]. 이 연구에서는 이미 공개된 랜섬웨어의 특정 패턴, 즉 시그니처 기반 탐지 방법은 변종 랜섬웨어가 나오는 경우 제한적일 수 있으므로 이를 극복하기 위해 탐지패턴 자동화 방법을 제안하였다. 그러나 제안된 자동화 과정의 한 부분인 감염신호분류 과정에서 기 정해진 감염신호 리스트로 분류하여 이에 벗어난 경우 탐지패턴을 만들 수 없다는 한계가 있고, 다양한 랜섬웨어에 대한 검증이 필요하다. 또한 크립토락커(cryptolocker)라는 특정 랜섬웨어의 공격 방법을 분석하여 이에 대한 대응방안을 연구하기도 하였다[14]. 그러나 이러한 대응방안은 해당 랜섬웨어에만 한정된다.

2016년에는 윈도우즈뿐만 아니라 MacOS에서도 랜섬웨어가 발생되었다. 이를 탐지하기 위해 랜섬웨어가 암호화한 파일의 확장자를 변경한다는 점을 이용하여 해당 경우가 발생되는 경우 랜섬웨어 감염을 탐지하는 방법이 제안되었다[15]. 그러나 이 방법에서는 확장자 변경이 이루어지지 않는 경우 탐지하지 못한다.

안드로이드 플랫폼에서도 랜섬웨어 방지 시스템을 설계하였다[16]. 기 알려진 랜섬웨어의 프로세스가 수행되는 경우 해당 프로세스를 중지시키는 시스템이다. 그러나 리스트에 없는 새로운 또는 변종 랜섬웨어에 대해서는 대응할 수 없다는 문제점이 있다.

이처럼 계속 변종으로 고도화되고 있는 랜섬웨어에 대해 실시간 탐지하여 위험도를 분석하고 보고하는 시스템이 필수적이다. 본 논문에서는 이러한 기능의 시스템에 대해 제안한다.

2.2 소셜 빅데이터 마이닝을 이용한 실시간 분석 활용 예

SNS는 즉시성, 공유성, 실시간성, 상호작용성, 집단지성의 특징을 가지고 있다[17]. 특히, 실시간성, 집단지성은 SNS의 특성상 양방향성을 활용해 정보나 의견을 교환하고 이를 통해 콘텐츠 제작, 수정 등 일반적인 활동이 누구나 가능하게 되며, 이러한 정보는 커뮤니티를 통해 개방적이고 지속적으로 축적 발전됨으로써 거대한 지성이 만들어진다는 특징이다. 이러한 두 특징을 이용하여 해당 SNS 데이터를 분석하면 현재 사람들의 관심사, 문제점 등을 알 수 있고, 미래를 예측할 수 있는 빅데이터로 활용 가능하다. 특히 SNS 서비스 사용율이 계속 증가하고 있어 빅데이터의 분석은 유의미한 정보를 추출하는데 유용한 데이터 셋으로 사용할 수 있다.

이러한 SNS 빅데이터를 기반으로 데이터마이닝 기술이 접목되어 '소셜 빅데이터 마이닝'이라는 이름으로 여러 분야에 활용되고 있다. 연구 [6]에서는 학문 분야 및 융합 키워드 추천 서비스를 위해서 SNS와 연관관계 분석을 수행하고 빈번하게 출현하는 키워드 쌍을 추천한다. 이를 근거로 전체 키워드 간 네트워크를 구축하여 학술 분야별 중심 키워드 및 분야 간 융합을 위한 연계 키워드 추천 서비스를 제공하였다. 연구 [7]에서는 트위터 데이터를 활용하여 국내 대학에 대한 평판을 분석하였다. 대학 이름과 동의어, 대학과 연관된 키워드를 사용하여 6개월간의 데이터를 수집하고 하둡(hadoop) 기반 하이브(hive)에 탑재한 후, 다차원분석을 수행하여 RHive를 통해 통계분석 및 시각화를 제공하고 국내 대학에 관한 인지도와 감성분석을 평가하였다.

또한 랜섬웨어 감염 및 전파처럼 독감 유행의 예측을 위한 연구를 위해서도 트워터 SNS 데이터가 활용되었다[8, 9]. 연구[10]에서는 마펑워(mafengwo.cn)의 서울 관광 후기 데이터를 분석하여 중국 관광객의 주요 관광지와 행위 매개체로서의 관광지에 대한 역동적인 관계를 분석하였다. 지금까지의 이러한 연구는 SNS의 실시간성과 집단지성을 이용하여 최근 관심, 유행, 평판을 분석하고 예측하는 내용이다.

3. 제안하는 랜섬웨어 전파 감지 시스템

3.1 시스템 구조도

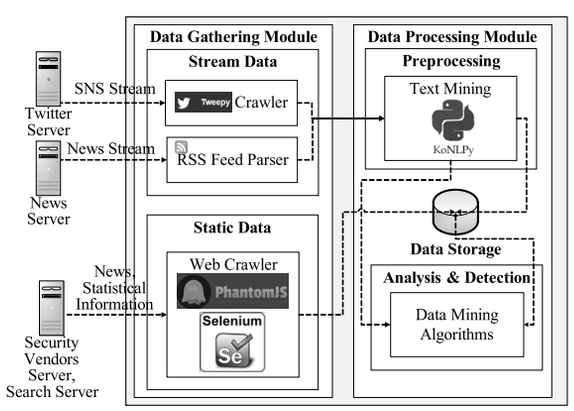


Fig. 1. Proposed System Structure

본 논문에서 제안하는 시스템은 Fig. 1과 같이 데이터 수집 모듈(Data Gathering Module)과 데이터 처리 모듈(Data Processing Module)로 구성되어 있다.

데이터 수집 모듈은 스트림 데이터와 정적 데이터를 수집한다. 스트림 데이터는 트위터 SNS 데이터와 뉴스피드를 통해 수집하여 실시간 처리를 위해 사용되고, 정적 데이터는 보안업체 웹서버 또는 탐색엔진을 통해 수집하여 추후 데이터 마이닝을 위해 사용된다.

수집된 데이터는 데이터 처리 모듈로 입력되어 불필요한 노이즈를 제거하는 등의 전처리(Preprocessing) 과정을 통해 저장되거나 분석 및 탐지(Analysis & Detection)를 위해 입력되어 사용된다.

3.2 데이터 수집 모듈

1) 스트림 데이터

스트림 데이터를 수집하기 위해 SNS 중 트위터(twitter.com)를 사용한다. 트위터는 140자 미만의 텍스트 위주의 개인 블로그이다. 트위터는 현재 많은 사용자에 의해 사용되는 SNS 하나로서 실시간 마이닝의 표본 데이터로서 충분한 가치가 있고 분석이 상대적으로 용이하다. 트위터에서 제공하는 퍼블릭 스트림에 대해서 특정 키워드로 필터링을 하고 그 결과를 마이닝한다. 이 때 트윗을 수집하는데 사용하는 라이브러리는 Tweepy로 이는 트위터를 액세스하기 위한 파이썬(python) 라이브러리이다[18]. 트위터에서 제공하는 스트림 데이터에는 트윗이 생성된 시간, 트윗을 게시한 사용자 아이디, 트윗 내용, 트윗에 포함된 이미지 소스 등이 포함된다. Tweepy를 이용해 랜섬웨어 키워드를 포함하는 트윗을 크롤링해 텍스트 파일로 저장하는 작업을 할 때, 스트림 데이터에서 제공하는 트윗 생성 시각에서 부터 작업 완료 시각까지 1초미만의 시간이 걸렸다. 따라서 Tweepy를 이용해 수집한 데이터는 실시간 데이터로서 충분한 의미를 가진다.

랜섬웨어의 피해사례를 조사해 보면, 국내와 해외에서 이용된 랜섬웨어의 종류는 상이하다[19]. 따라서 국내 실정에 맞는 시스템이 필요하다. 이를 위해서 RSS피드(Rich Site Summary Feed)를 사용하였는데, RSS는 뉴스나 블로그 사이트에서 주로 사용하는 콘텐츠 표현 방식이다[2]. 본 시스템에서 사용하는 RSS피드는 안랩에서 제공하는 보안 뉴스 제목을 제공해 주는 피드이다[20]. RSS FeedParser 라이브러리를 사용해 피드를 주기적으로 수집하고 랜섬웨어 관련 키워드를 추출하여 사용한다.

2) 정적 데이터

정적 데이터는 보안업체 또는 탐색엔진(예, 구글 트렌드)을 통해 수집되며 데이터 마이닝을 위해 사용된다. 해당 데이터를 수집하기 위해 Selenium 라이브러리와 PhantomJS 드라이버를 이용하여 웹페이지를 크롤링한다[21, 22]. 그 후 수집된 자료를 BeautifulSoup4 라이브러리를 이용해 스크래이핑한다[23]. 스크래이핑된 자료는 MySQL Connector를 이용하여 미리 만들어 놓은 데이터베이스 테이블에 저장한다. 크롤링은 각 페이지마다 그리고 크롤링이 실시되는 시점에 따라 다른 크롤링 방법을 요구하기도 한다. 따라서 여러 보안관련 페이지(예, Rancert[24] 보안뉴스 페이지, Rancert 랜섬웨어 피해사례 페이지 등)에서 수행되며, RSS피드와 마찬가지로 국내 실정에 맞는 시스템 개발을 위해 이용자가 충분히 많은 국내 사이트에서 랜섬웨어 관련 키워드를 주기적으로 수집한다.

3.3 데이터 처리 모듈

데이터 수집 모듈에서 수집된 데이터는 적절한 전처리가 필요한 경우 전처리 과정을 통해 노이즈 제거 등 불필요한

부분을 삭제하고 중요 정보만을 추출하고, 이를 이용해 분석 및 탐지할 수 있도록 한다. 실제 측정 결과로 퍼블릭 스트림을 통해서 일일 7천개 이상의 트윗이 만들어진다. 트윗 중에 스팸성인 데이터와 너무 짧아서 분석하기 어려운 경우가 많아 이를 제외하는 과정이 필수적이다.

1) 전처리 과정

모든 데이터는 자연어 형식으로 구성되어 있으며 표준어 형식을 지키지 않은 데이터가 많다. 이 때의 노이즈를 최소화하기 위해 KoNLPy 라이브러리를 사용하여 비표준어 데이터를 정규화하고, 형태소를 분리하여 명사를 추출하는 과정을 수행한다[25].

2) 분석 및 탐지

데이터 분석 및 랜섬웨어의 탐지를 위해서는 데이터의 종류(예, 실시간 데이터, 과거 통계 데이터 등)에 따라 여러 데이터 마이닝 알고리즘이 적용가능하다. 본 논문에서는 트윗 정보를 사용하여 통계 분석을 위해 엔트로피 및 카이-스퀘어 분석하고자 한다. 두 통계역학적 함수는 분포도 분석을 위해 많이 사용되어 데이터마이닝 기법의 대표적 메소드로서 공격 탐지 등에 사용되었다[26].

엔트로피 분석은 Equation (1)을 이용한다. p_i는 n개의 그룹 i (b_i)에 해당하는 빈도수에 대한 확률값으로 랜섬웨어와 관련된 키워드를 담고 있는 트윗 수(x_j)를 이용한다. 특정 j번째 유닛시간 동안 관련 트윗 수를 x_j라고 했을 때, 지금까지의 x_j 최대값을 참고해 그 값을 n개의 그룹으로 나눈다. 예를 들어, x_j의 최대값이 30이고, n이 3이라면 b_1그룹은 x_j가 0이상 10미만, b_2그룹은 x_j가 10이상 20미만, b_3그룹은 x_j가 20이상으로 한다. 특정 윈도우 시간(=j개의 유닛시간) 내 각 유닛시간의 x_j값을 고려하여 b_i의 유닛시간 개수를 세어 확률 p_i를 구한다. 예를 들어, 윈도우 시간을 24시간으로 하고 유닛시간을 1시간으로 한다면(j=24), 지난 24시간동안 매 시간의 x_j값을 카운팅한다. 예를 들어, b_1내 포함된 유닛시간 개수가 20, b_2 그룹에 포함된 유닛시간 개수가 3, b_3 그룹에 포함된 유닛시간 개수가 1이라면 H값은 약 0.78524가 된다(Fig. 2 참조, $H=-(\frac{20}{24}log_2\frac{20}{24}+\frac{3}{24}log_2\frac{3}{24}+\frac{1}{24}log_2\frac{1}{24})$).

$$H = -\sum_{i=1}^{n} p_i \log_2 p_i \quad (1)$$

피어슨 카이-스퀘어(Pearson's chi-square) 분석은 이산 수(discrete values)로 이루어진 분포도에 대한 비교를 위해 사용할 수 있으며 Equation (2)를 이용한다. 엔트로피 분석에서처럼 n은 그룹 수이고, N_i는 해당 그룹에 속한 유닛개수이고, n_i는 i 그룹의 기대값이다. N_i는 윈도우 내의 해당 그룹에 속한 유닛 수로 계산할 수 있다. Fig. 2의 예를 통해 설명하면, 24시간을 윈도우, 1시간을 유닛시간일 때, N_1은 20, N_2는 3, N_3는 1이 되고, 각 그룹의 기댓값은 윈도우보다 더 넓은 구간을 통해 구할 수수 있다. 예를 들어 한달동안 각 날짜에 구한 N_i값들을 그룹별 평균 내어 기댓값 n_i로 사용할 수 있다. Table 1은 Equation (1), (2)에 사용된 파라미터를 설명하였다.

$$\chi^2 = \sum_{i=1}^{n} \frac{(N_i - n_i)^2}{n_i} \quad (2)$$

Table 1. Parameters in Eqs.(1) and (2)

Eq.	Parameters	Comments
(1)	n	The number of groups
	x_j	The number of tweets with Ransomware-related keywords
	b_n	n groups that is divided as x_j (e.g., 1st group: 0-9, 2nd group: 10-19, 3rd group: 20 above)
	p_i	The probability of being occupied in i^{th} group
(2)	n	The number of groups
	N_i	The number of units in i^{th} group
	n_i	The expected value of units in i^{th} group

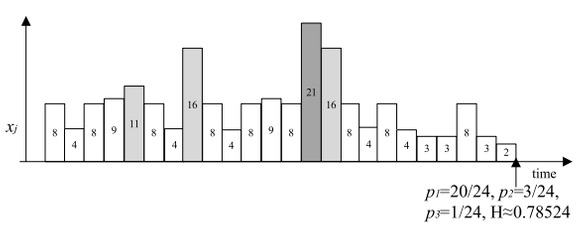


Fig. 2. Entropy Values Based on Tweet Count

4. 분석 및 탐지 실험

본 논문에서는 2017년 전파가 많이 되었던 랜섬웨어 중에 워너크라이와 록키(locky) 랜섬웨어 감염전파 시기(각 2017년 5월, 2017년 8~9월)의 트윗 수와 검색엔진 검색통계(google trend) 정보를 비교해 보고자 한다. 제안된 랜섬웨어 전파 감지에 기반 되는 데이터로서 소셜 데이터를 사용하는데 이에 대한 정당성을 입증하기 위해서는 실제 랜섬웨어 감염에 대한 시간별 통계정보가 필요하다. 그러나 실제 통계 정보를 제공하는 곳이 없어 이를 대신하여 구글 트렌드[27] 값을 이용한다. 구글 트렌드는 구글이 수집하는 다양한 데이터를 계량화하여 보여주는 도구로서 요새 핫한 이슈가 무엇인지, 주제어와 연관 검색어는 무엇인지, 시간에 따라 해당 주제가 어떻게 변하는지 그 트렌드를 알 수 있는 도구이다.

또한 이러한 트윗 수 분포에 대한 분석을 위해 엔트로피와 카이-스퀘어 분석을 한다. 이를 통해 감염 전파 증가에 대한 위험 분석의 가능성을 보이고자 한다.

4.1 트윗 수와 구글 트렌드

Fig. 3은 2017년 5월 한 달 간의 전세계 트윗을 분석하여, 2017년 5월 12일 전세계적으로 감염 전파된 워너크라이 랜섬웨어에 대한 트윗 수(Tweets#, 실선)와 동일한 키워드 'wannacry'에 대한 구글 트렌트 정보(Trend, 점선)를 그래프로 나타낸 자료이다. 두 자료를 보면 비슷한 증감을 보이고 있으나 트윗 수의 변화가 조금 앞선 경향을 보인다. 예를 들어, 해당 랜섬웨어가 전파된 12일부터 트윗의 급증 현상을 보여주고 있으나 구글 트렌드 통계값은 다음날인 13일부터 급증하고 있다.

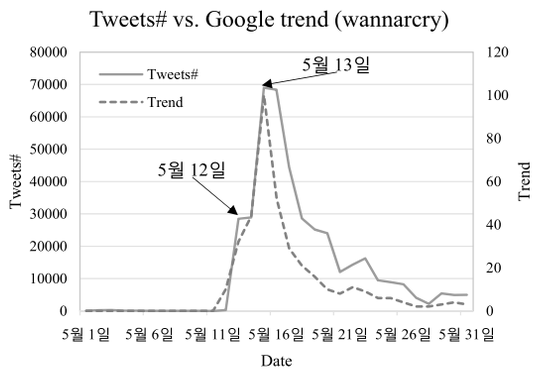


Fig. 3. Tweets# vs. Google Trend (Wannacry)

이와 비슷하게 Fig. 4는 2017년 8월 1일부터 9월 30일까지 전세계 지역에서 생성된 트윗을 분석하여, 'locky ransomware' 키워드가 포함된 트윗 수(Tweets#, 실선)와 동일한 키워드에 대한 구글 트렌트 정보(Trend, 점선)를 그래프로 나타낸 자료이다. 마찬가지로 두 값은 비슷한 증감을 보이고 있으나 트윗 수의 증감이 조금 앞선 경향을 보이고 있다. 예를 들어 처음 증가하는 날이 8월 17일로 동일하나, 더 급증하는 날짜는 트윗은 9월 1일 트렌드 값은 9월 3일로 조금 늦어지는 경향이다. 이러한 이유는 사람들이 해당 랜섬웨어에 감염이 되고 바로 트윗을 하지만, 구글 트렌드 값은 이미 기사화 되어 해당 자료를 자세히 알아보거나 감염이 되어 알아볼 때 사용할 것으로 추정되어 구글 트렌드 변화가 조금 늦은 것으로 추정된다.

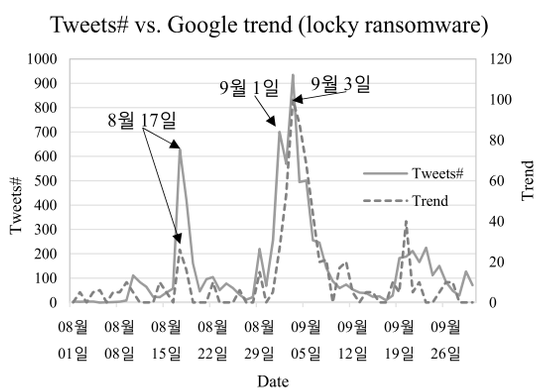


Fig. 4. Tweets# vs. Google Trend (Locky Ransomware)

이 기간 동안 보안업체를 통해 제공된 기사를 살펴보면, (주)하우리에서 9월 20일 '변종 Locky 랜섬웨어(.ykcol) 감염 주의'라는 제목으로 해당 랜섬웨어의 유포과정, 이에 대한 대응방법(해당 업체 소프트웨어 업데이트)을 소개하고 있다[28]. 또한 10월 5일 'Locky 랜섬웨어 변종 발견돼…스팸메일 주의'라는 제목의 데일리시큐(www.dayilsecu.com)에서 기사를 제공하고 있다[29]. 결과적으로 업체에서 제공하는 기사들은 트윗이나 구글 트렌드 값보다 훨씬 뒤늦은 20일 이상 지난 9월 20일 이후에 해당 랜섬웨어의 유포 과정과 대응방법을 제공하고 있어 그 실효성 및 실시간성이 떨어짐을 알 수 있다.

두 경우를 종합적으로 보면, 트위터가 탐색엔진 검색통계나 기사보다 빠르게 반응하는 경향을 보이고 있어 트위터를 통해 랜섬웨어 감염 전파 증가를 빠르게 판단하는 것이 가능성 높아 보인다.

4.2 엔트로피 vs 카이-스퀘어

본 절에서는 트윗 수의 분포도 분석을 통해 랜섬웨어 감염 전파 정도를 분석한다. 이때 3.3절에서 설명한 엔트로피와 카이-스퀘어 분석을 이용한다. Fig. 5는 'wannacry'에 대한 키워드를 포함한 트윗 수에 대해 5월 한 달간 엔트로피 값을 함께 나타낸 그래프이다. 트윗 수는 5월 12일 23시에 191로 증가하기 시작하여(이전 최고값 55), 188, 257, (5월 13일 03시) 777로 급증한다. 이러한 변화는 엔트로피 변화에도 영향을 주어 5월 13일 02시에 0.25로 증가하기 시작한다. 이러한 변화를 통해 감염 증가의 탐지 및 위험 정도를 판별해 낼 수 있다. Fig. 6은 Fig. 5의 일부 구간인 6일(5월12일~17일) 동안의 값 변화를 보여주고 있다.

Fig. 7, 8은 같은 기간의 wannacry 트윗 수에 대해 카이-스퀘어 값을 함께 나타내었다. 카이-스퀘어 값은 5월 13일 02시부터 급감하는 변화를 보이고 있다. 엔트로피, 카이-스퀘어 값의 변화를 보면, 두 수치 모두 트윗 수 변화를 빠르게 나타내는 것을 볼 수 있다.

Fig. 9는 'locky ransomware'에 대한 키워드를 포함한 트윗 수에 대해 엔트로피 분석한 그래프이다. 8월 12일 04시 트윗

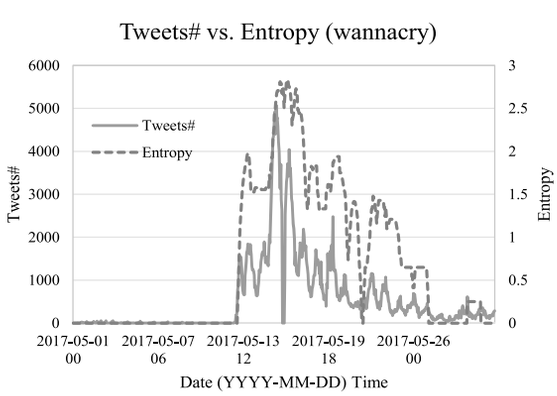


Fig. 5. Tweets# vs. Entropy (Wannacry, 1 Month)

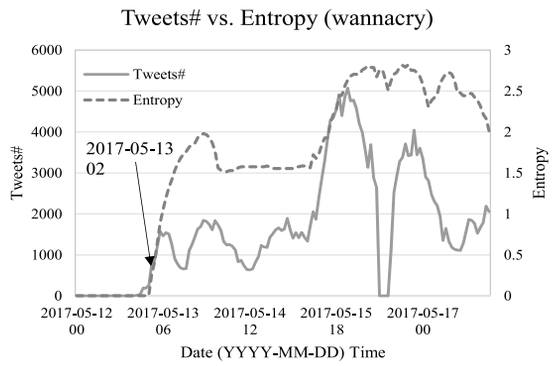


Fig. 6. Tweets# vs. Entropy (Wannacry, 6 Days)

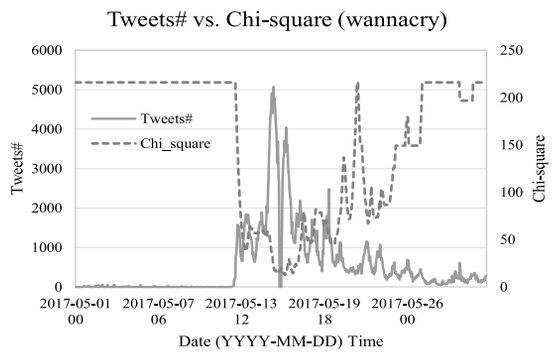


Fig. 7. Tweets# vs. Chi-Square (Wannacry, 1 Month)

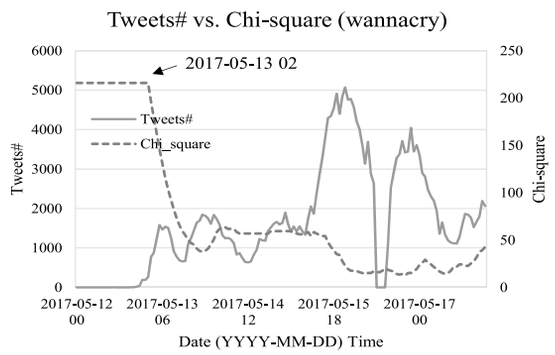


Fig. 8. Tweets# vs. Chi-Square (Wannacry, 6 Days)

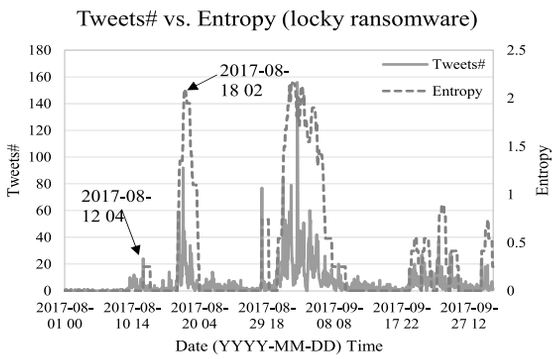


Fig. 9. Tweets# vs. Entropy (Locky, 2 Month)

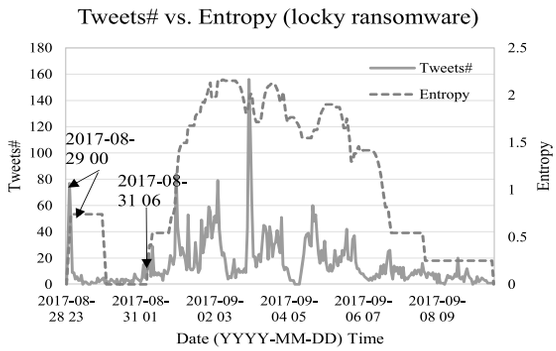


Fig. 10. Tweets# vs. Entropy (Locky, 12 Days)

수 증가로 엔트로피 값에도 바로 영향을 주어 같은 시간에 0.25로 증가한다(이전 0). 마찬가지로 8월 17일 01시 18개로 트윗 수가 증가하면서 감소를 보이다가 이러한 증가가 지속되어 8월 18일 02시 2.10의 값 증가를 보여주고 있다. 이러한 변화는 Fig. 10의 12일간의 확대 그래프에서 더 잘 보이고 있다.

Fig. 11, 12는 'locky ransomware'에 대한 트윗 수에 대해 카이-스퀘어 분석한 그래프이다. 엔트로피와 마찬가지로 8월 12일 04시 트윗 수 증가로 카이-스퀘어 값에도 영향을 주어 같은 시간에 196.83으로 감소한다(이전 216). 또한 8월 17일 01시 18개로 트윗 수가 증가하면서 감소를 보이다가 이러한 증가가 지속되어 8월 18일 02시 37.77의 작은 값을 나타내었다.

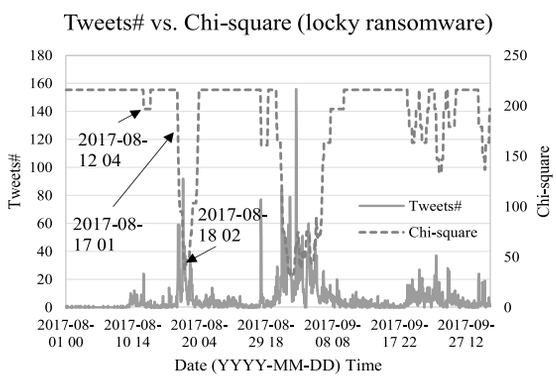


Fig. 11. Tweets# vs. Chi-Square (Locky, 2 Month)

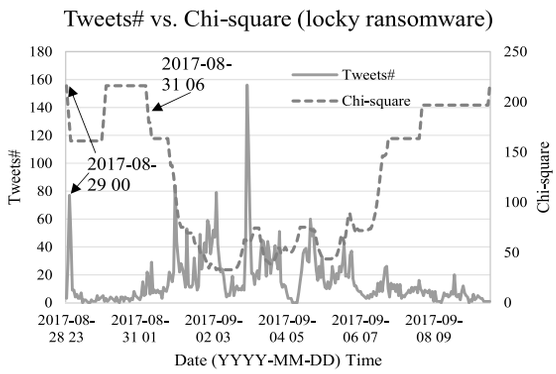


Fig. 12. Tweets# vs. Chi-Square (Locky, 12 Days)

결과적으로, 트윗 수의 변화는 엔트로피, 카이-스퀘어에 바로 잘 적용되고 있다. 엔트로피, 카이-스퀘어 값의 변화가 평소에 비해 비정상적으로 높은 변동을 보이는 경우를 감지하면 실시간으로 랜섬웨어 전파를 감지할 수 있다.

5. 결 론

본 논문에서는 랜섬웨어의 실시간 전파 감지를 위해 트위터 SNS 데이터를 가지고 마이닝하는 시스템을 제안하였다. 제안한 시스템은 2017년 전파가 많이 되었던 워너크라이와 록키 랜섬웨어 감염전파 시기의 트윗 수와 검색엔진 검색통계, 기사를 비교해 랜섬웨어 탐지를 위해 트윗 정보 사용의 가능성을 보여주었다. 또한 엔트로피, 카이-스퀘어 분석을 통해 랜섬웨어 전파 감지 시스템의 성능을 보였다.

References

[1] S. Morgan, Ransomware damage in 2017, 15-fold increase in two years to $ 5 billion [Internet], http://www.itworld.co.kr/tags/60228/랜섬웨어/104915.

[2] RSS Wikipedia [Internet], https://ko.wikipedia.org/wiki/RSS.

[3] Digital News Reporter, World's Largest Ransomware Attack ... 100 Countries Hit [Internet], http://news.mk.co.kr/newsRead.php?no=320427&year=2017.

[4] Last year, domestic Ransomware suffered 300 billion won [Internet], http://www.ddaily.co.kr/news/article.html?no=152419.

[5] Social Network Service Wikipedia [Internet], https://ko.wikipedia.org/wiki/소셜_네트워크_서비스.

[6] I. D. Cho and N. G. Kim, "Recommending Core and Connecting Keywords of Research Area Using Social Network and Data Mining Techniques," *Journal of Korea Intelligent Information Systems Society*, Vol.17, Issue.1, pp.127-138, 2011.

[7] Y. H. Yang, I. S. Jung, Y. T. Kim, and W. S. Cho, "An Awareness Identification and Preference Analysis for Domestic University Using SNS Data," *Journal of The Korea Big Data Service Society*, Vol.1, No.1, pp.1-13, 2014.

[8] B. Lee, J. Yoon, S. Kim, and B. Hwang, "Detecting social signals of flu symptoms," in *Proceedings of Collaborative Computing: Networking, Applications and Work-sharing*, 2012.

[9] S. Verma, Y. Park, and M. Kim, "Predicting Flu-Rate Using Big Data Analytics Based on Social Data and Weather Conditions," *Adv. Sci. Lett.* Vol.23, pp.12775-12779, 2017.

[10] S. W. Lee and H. Y. Lee, "A Data Mining and Social Network Analysis to Understand Multi-Destination Tour Behavior of Inbound Free Independent Tourists in Seoul," in *Proceedings of the Korean Academic Association of Business Administration*, pp.321-334, 2017.

[11] J. Na and M. Kim, "Design of a Real-time Risk Analysis System for Ransomware Using Mining based on Social Network Service," in *Proceedings of the Fall Conference of the KIPS*, 2017.

[12] Latest Ransomware Trend Analysis Report: Detailed analysis and forecast of major Ransomware in 2016, ASEC Response Team, 2017.

[13] H. Lee, J. Sung, Y. Kim, J. Kim, and K. Kim, "The Automation Model of Ransomware Analysis and Detection Pattern," *Journal of the Korea Institute of Information and Communication Engineering*, Vol.21, No.8, pp.1581-1588, 2017.

[14] Y. Kim, D. Ham, Y. Joo, and K. H. Lee, "Analysis and Countermeasures for the Ransomware Cryptolocker," in *Proceedings of Korea Information Processing Society*, Vol.23, No.1, 2016.

[15] J. M. Youn, and J. C. Ryu, "How to Detect and Block Ransomware with File Extension Management in MacOS," *Journal of the Korea Institute of Information Security & Cryptology*, Vol.27, No.2, pp.251-258, 2017.

[16] B. Kim, W. Kim, J. Lee, S. Yim, S. Song, and S. Lee, "Design and Implementation of a Ransomware Prevention System using Process Monitoring on Android Platform," *in Proceedings of the Korean Institute of Information Scientists and Engineers*, pp.852-853, 2015.

[17] S. Kim and Y. Lee, "Application of New Agenda Setting Model by Internet," in *Proceedings of The Korean Society for Journalism & Communication Studies*, pp. 529-551, 2006.

[18] Twitter Developer Documentation [Internet], https://dev.twitter.com/docs.

[19] Report of Ransomware Invasion Analysis in 2017 [Internet], https://www.rancert.com/bbs/bbs.php?bbs_id=notice&mode=view&id=52.

[20] AhnLab RSSfeed [Internet], http://www.ahnlab.com/kr/site/etc/rss.do.

[21] Selenium [Internet], http://www.seleniumhq.org/docs/.

[22] PhantomJS [Internet], http://phantomjs.org/documentation/.

[23] BeautifulSoup4 [Internet], https://www.crummy.com/software/BeautifulSoup/bs4/doc.

[24] Ransomware Computer Emergency Response Team Coordination Center(RanCERT) [Internet], https://www.rancert.com/.

[25] KoNLPy [Internet], http://konlpy-ko.readthedocs.io/ko/v0.4.4/#.

[26] L. Feinstein, D. Schnackenberg, R. Balupari and D. Kindred, "Statistical approaches to DDoS attack detection and response," in *Proceedings DARPA Information Survivability Conference and Exposition*, Vol. 1, pp.303-314, 2003.

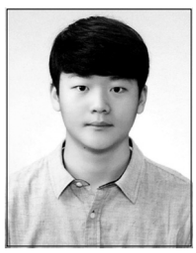
[27] Google trend [Internet], https://trends.google.com/trends/

[28] Variant Locky Ransomware (.ykcol) Infection Attention , Hauri Co. [Internet], https://www.hauri.co.kr/ransomware/viewer.php?idx=69.

[29] M. Gill, Locky Ransomware variant found ... Spam Mail Attention [Internet], http://www.dailysecu.com/?mod=news&act=articleView&idxno=24525.

김 미 희

https://orcid.org/0000-0002-4896-7400
e-mail : mhkim@hknu.ac.kr
1997년 이화여자대학교 전자계산학과 (공학사)
1999년 이화여자대학교 컴퓨터학과 (공학석사)
1999년~2003년 한국전자통신연구원 연구원
2007년 이화여자대학교 컴퓨터학과(공학박사)
2007년~2009년 이화여자대학교 컴퓨터학과 전임강사
2009년~2010년 노스캐롤라이나주립대학교 연구원
2011년~현 재 한경대학교 컴퓨터공학과(컴퓨터시스템연구소) 교수
관심분야 : 네트워크 성능 분석 및 보안, 무선네트워크 보안, 침입대응



윤 준 혁

https://orcid.org/0000-0001-6240-4455
e-mail : junhyeok.dev@gmail.com
2016년~현 재 한경대학교 컴퓨터공학과 학부생
관심분야 : 크라우드센싱, 블록체인, 기계학습