

ISSN 1738-9593 제 19권 제 2호



2018 추계 학술 발표대회

2018.11.2(금)~3(토)

서울디지털재단 새롭관

논문집

주최 사단법인 한국인터넷정보학회, 재단법인 서울디지털재단

후원 서울특별시, (주)아이티센, LGCNS(주), 한국과학기술정보연구원
(주)애드포스인사이트, (주)씨어스테크놀로지

B-2. 지능형시스템 2 (좌장 : 한희준 박사 / 한국과학기술정보연구원)

B-2-1. 최신 점진적 유틸리티 데이터 마이닝의 성능 평가 및 분석	51
남효주, 윤은일, 백윤지, 김종성, 김현호, 임현근(세종대)	
B-2-2. ☆ AR 기반 보행 균형 측정 콘텐츠	53
마준, 성낙준, 서귀빈, 홍민(순천향대)	
B-2-3. 직거래 유통플랫폼에서의 거래 주체 특성을 반영한 Node.js기반 페이지 라우팅 설계 및 구현	55
이송연, 백종호(서울여대)	
B-2-4. 도서 관리를 위한 클래스 설계 및 구현	57
임현근, 윤은일, 남효주, 백윤지, 김종성, 김현호(세종대)	
B-2-5. 가중화 이레이저블 패턴 마이닝 알고리즘의 분석	59
윤은일, 남효주, 백윤지, 김종성, 김현호, 임현근(세종대)	
B-2-6. 머신러닝을 이용한 지능형 컴플라이언스 적용 시스템 설계에 관한 연구	61
고영민, 곽진(아주대)	
B-2-7. 소셜 미디어 콘텐츠 기반 실시간 질병 감지 시스템을 위한 연구	63
양성민, 유소엽, 김대호, 정옥란(가천대)	

C. 인터넷보안 (좌장 : 백종호 교수 / 서울여대)

C-1. ☆ 분산형 데이터베이스 환경에서 개인정보보호를 위한 암호화방식	69
강형석, 박석천(가천대)	
C-2. 신·변종 보안위협에 대한 예측 및 탐지 방안에 관한 연구	71
최슬기, 곽진(아주대)	
C-3. 무선 센서 네트워크에서 ID 기반 키 교환 프로토콜 연구 동향	73
오정민, 정익래(고려대)	

신·변종 보안위협에 대한 예측 및 탐지 방안에 관한 연구

최슬기*, 곽진**

*아주대학교 컴퓨터공학과 정보보호응용및보증연구실

**아주대학교 사이버보안학과

e-mail : *skchoi.isaa@gmail.com, **security@ajou.ac.kr

A Study on the Prediction and Detection Method for New and Variant Security Threats

Seul-Ki Choi*, Jin Kwak**

*ISAA Lab., Department of Computer Engineering, Ajou University

**Department of Cyber Security, Ajou University

요약

빠르게 발전하는 IT 기술만큼 악성코드로 또한 IT 기술의 변화속도에 맞춰서 진화함으로써 신·변종의 보안위협들이 발생하고 있다. 이처럼 빠르게 발전하는 악성코드들을 차단하기 위하여 신·변종의 악성코드들을 탐지하고 분류하기 위한 다양한 연구들이 진행되고 있다. 특히 악성코드가 활동하기 적합한 컴퓨팅 능력과 네트워크 기능을 갖춘 모바일 환경은 여전히 높은 비율의 악성코드들이 발생하고 있다. 한편 악성코드 통계자료를 분석한 결과, 전체 악성코드 대비 신종 악성코드의 발생 비율은 최대 10% 정도로 대부분이 변종의 악성코드인 것을 확인할 수 있다. 즉 대부분의 악성코드들은 완전히 새로운 악성코드보다는 기존에 사용하였던 악성코드들을 재사용하고 있음을 유추할 수 있었다. 또한 악성코드에 악성 기능을 포함되어 있지만 실제로 동작하지 않았던 코드들에 대해서 보다 더 적합한 환경이 나타나면 다시 발생하는 등의 특징도 찾을 수 있었다. 따라서 본 논문에서는 IT 기술과 악성코드의 변화 및 발전 과정 분석을 통하여 향후에 발생 가능한 신종 및 변종의 보안위협을 예측 및 탐지할 수 있는 방안을 제안한다.

1. 서론

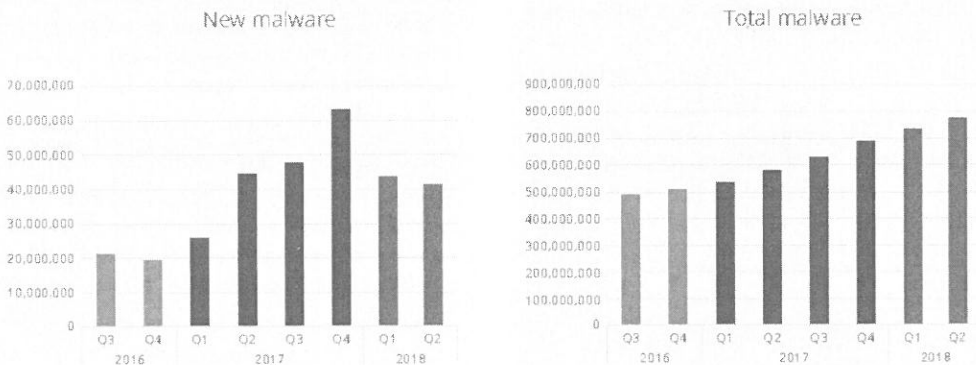
최근 IoT 기술의 힘을 입어 스마트 홈, 스마트 팩토리, 스마트시티 등 우리의 주거 생활환경에 IT 기술이 밀접하게 녹아들어 함께 공존하고 있다[1][2]. 이처럼 IT 기술은 우리의 삶을 단순하게 편리하게 해주는 수단을 넘어서서 우리 삶의 환경까지 바뀌음을 만큼 발달하고 있다. 또한 최근에는 차세대 지능형 교통시스템이라 불리는 C-ITS(Cooperative-Intelligent Transport System)로 인해 교통수단까지 IT 기술 스며들고 있는 실정이다[3].

한편, IT 기술이 발전하는 만큼 IT 기술을 역이용하는 악성코드 또한 빠르게 진화하고 있다. IT 기술의 발전으로 인해

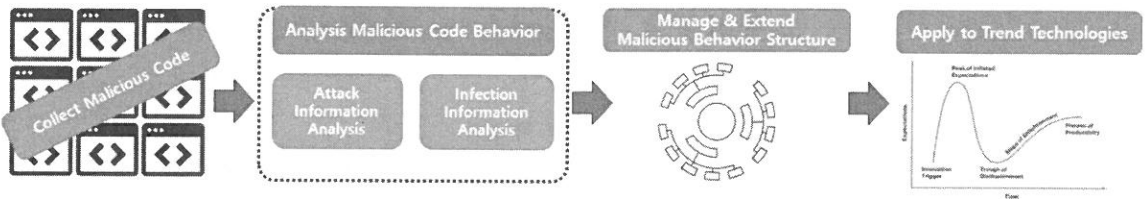
다양한 IT 환경을 맞이함으로써 보안 분야에서는 새로운 환경에서 발생할 수 있는 신·변종의 보안위협을 예측하고 탐지하기 위하여 많은 연구들이 진행되고 있다. 우리는 끊임없이 발전하고 진화하는 IT기술과 악성코드의 관계를 고려하여 지속적으로 활용 및 확장 가능한 프레임워크를 제안한다.

2. 악성코드 통계 자료

2018년 09월에 McAfee Lab에서 “McAfee Labs Threats Report September 2018” 보고서를 공식 홈페이지를 통해 공개하였다. 해당 보고서에는 2018년 2분기부터 약 2년 동안에 발생하였던 악성코드들의 발생 통계자료가 포함되어있다. 아



(그림 1) 신종 악성코드 및 전체 악성코드 발생 건수



(그림 2) 신·변종 보안위협 예측 및 탐지 방안

래 그림 1은 해당 보고서에 수록되어있는 신종 악성코드(New malware)와 전체 악성코드(Total malware)의 발생 건수를 나타내고 있다[4].

위 통계자료를 살펴보면 전체 악성코드 중에 신종 악성코드의 발생 비율은 신종 악성코드가 가장 많이 발생하였던 2017년 4분기를 기준으로 계산해보아도 10%가 되지 않는 것을 확인할 수 있다. 즉 대부분의 악성코드들은 완전히 새로운 형태의 악성코드를 사용하기보다는 기존의 사용하였던 악성코드들을 재사용하고 있는 것을 확인할 수 있다.

3. 신·변종의 보안위협 예측 및 탐지 방안

본 논문에서는 IT 환경의 변화로 인해 발생할 수 있는 새로운 형태의 보안위협이나 변형된 형태의 보안위협을 예측하고 탐지하기 위하여 악성코드 샘플이라 부를 수 있는 바이너리에 포함된 정보만을 활용하지 않고 악성코드의 감염 과정과 공격 과정에서 얻을 수 있는 모든 정보들을 기반으로 악성코드의 악성행위를 구체화한다. 이러한 정보를 악성행위 구조정보를 지속적으로 관리하고 정보들의 항목을 확장함으로써 지금까지 발생한 악성코드 감염 경로와 실행 방법 및 공격 대상과 공격 행위 등을 구체화한다.

이와 같이 지속적으로 관리된 악성행위 구조정보를 IT 환경의 변화를 일으킬 것으로 예상되는 최신 트렌드 기술과 비교하여 최신 트렌드 기술을 포함할 수 있는 항목들을 분석한다. 이를 기반으로 과거에 활동하였던 악성코드들이 새로운 IT 환경에서 활동할 악성 행위를 예측하고 대비하여 탐지할 수 있다.

간단한 예시로 스마트폰의 보급화가 이루어지고 있던 시점에 스미싱(Smishing)이라는 이름으로 널리 전파되었던 악성 앱에 시간이 지날수록 악성 앱 내부에 다양한 악성 기능들이 추가되어 배포되곤 하였다. 특히, 스마트폰을 이용한 DDoS 공격 기능이 포함되어있는 경우도 종종 발견하였지만, 실제로 스마트폰을 이용한 DDoS 공격은 크게 성공하지 못하였다. 하지만 스마트폰과 컴퓨팅 성능과 네트워크 기능은 비슷하면서 스마트폰과 비교할 수 없을 정도로 많은 수로 이용되었던 IoT 디바이스를 이용한 강력한 DDoS 공격이 발생하였다[5].

이 외에도 사용자 PC에 저장된 파일을 암호화하여 금전을 요구하는 랜섬웨어 또한 최근에는 스마트폰 환경에서 전면 화면을 잠그는 형태로 변형되어 활동하고 있다[4]. 이처럼 기존에 활동하였던 악성코드들의 악성행위에 대한 정보를 구체화하고 관리하고 새로운 IT 환경에 대한 특징 조사와 악성행위 구조정보를 비교·분석하여 향후 발생할 수 있는 보안위협의 종류를 예측할 수 있으며, 미리 대비하여 그 징후를 탐지할 수 있을 것으로 판단한다.

4. 결 론

본 논문에서는 기존의 악성코드들에 대하여 악성코드 샘플과 같은 바이너리 정보만을 분석하는 것이 아닌, 감염 과정과 공격 과정을 분석하면서 획득할 수 있는 악성 행위 정보를 지속적으로 수집 및 관리하고 확장함으로써 지속적으로 변화하는 IT 환경과 끊임없이 진화하는 악성코드에 적응하고, 새로운 환경에서 발생할 수 있는 보안위협을 기존의 악성코드들의 악성 행위 사례를 통하여 예측하고 탐지할 수 있는 방안을 제안하였다.

하지만 본 논문에서 제시하는 방법을 실제로 지속적으로 관리하고 운영한 실제적인 데이터가 없기 때문에 현실적으로 적용 가능한지, 얼마나 효과적으로 보안위협을 탐지하는지 그에 따르는 문제들이 무엇이 있는지 분석 및 검증은 수행하지 못하였다. 따라서 향후에는 해당 방안을 지속적으로 운영 및 관리하여 실제적인 보안 위협을 예측함으로써 그 효율성을 입증하는 연구를 진행할 예정이다.

참 고 문 헌

- [1] Vu-Anh-Quang Nguyen, "Study on realtime control system in IoT based smart factory: Interference awareness, architectural elements, and its application", Information Science and Technology (ICIST), 2017 Seventh International Conference on, April 16-19, 2017.
- [2] H. Arasteh, V. Hosseini-zhad, V. Loia, A. Tommasetti, O. Troisi, M. Shafie-khah and P. Siano, "IoT-based Smart Cities: a Survey", Environment and Electrical Engineering (EEEEIC), 2016 IEEE 16th International Conference on, June 7-10, 2016.
- [3] Jorge Alfonso, Nuria Sánchez, José Manuel Menéndez and Emilio Cacheiro, "Cooperative ITS communications architecture: the FOTsis project approach and beyond", IET Intelligent Transport System, vol. 9, issue. 6, pp.591 - 598, August 06, 2015.
- [4] McAfee Labs, "McAfee Labs Threats Report September 2018", September, 2018
- [5] James A. Jerkins, "Motivating a market or regulatory solution to IoT insecurity with the Mirai botnet code", Computing and Communication Workshop and Conference (CCWC), 2017 IEEE 7th Annual, January 09-11, 2017.