랜섬웨어 동적 분석을 위한 시그니처 추출 및 선정 방법

Method of Signature Extraction and Selection for Ransomware Dynamic Analysis

저자 (Authors)

이규빈, 옥정윤, 임을규

Gyu Bin Lee, Jeong Yun Oak, Eul Gyu Im

출처 (Source)

정보과학회 컴퓨팅의 실제 논문지 24(2), 2018.2, 99-104 (6 pages)

KIISE Transactions on Computing Practices 24(2), 2018.2, 99-104 (6 pages)

발행처 (Publisher)

한국정보과학회

KOREA INFORMATION SCIENCE SOCIETY

URL

http://www.dbpia.co.kr/Article/NODE07367759

APA Style

이규빈, 옥정윤, 임을규 (2018). 랜섬웨어 동적 분석을 위한 시그니처 추출 및 선정 방법. 정보과학회 컴퓨팅의 실제 논문지, 24(2), 99-104.

ISSN 2383-6318(Print) / ISSN 2383-6326(Online)
KIISE Transactions on Computing Practices, Vol. 24, No. 2, pp. 99-104, 2018. 2
https://doi.org/10.5626/KTCP.2018.24.2.99

랜섬웨어 동적 분석을 위한 시그니처 추출 및 선정 방법

(Method of Signature Extraction and Selection for Ransomware Dynamic Analysis)

이 규 빈 † 옥 정 윤 †† 임 을 규 †††
(Gyu Bin Lee) (Jeong Yun Oak) (Eul Gyu Im)

요 약 최근 랜섬웨어에 의한 피해가 전 세계적으로 급증하고 있으며, 국가 기관, 기업, 민간 등 사회 전반에 막대한 피해를 입히고 있다. 랜섬웨어는 컴퓨터 시스템을 감염시켜 사용자의 접근을 제한하고 일종의 몸값을 요구하는 악성 소프트웨어이다. 컴퓨터 시스템 자체를 잠그거나 하드 디스크에 존재하는 파일들을 암호화하여 사용자가 컴퓨터를 정상적으로 이용할 수 없게 만들고, 컴퓨터의 정상 복구를 위해 사용자들은 공격자로부터 몸값(Ransom) 지불을 요구받는다. 기존의 기타 악성코드들에 비해 공격수법이 매우 악랄하고 피해규모가 막대하므로 확실한 해결책이 필요하다. 악성코드 분석 방식은 크게 정적 분석, 동적 분석 두 가지로 나뉜다. 최신 악성코드들은 정교한 패킹 기술이 도입된 경우가 많아 정적분석은 분석에 한계가 있다. 따라서 본 논문에서는 랜섬웨어의 활동 모니터링 및 보다 정밀한 분석을 위해 동적 분석 방법을 제안한다. 정상파일, 랜섬웨어, 기타 악성코드의 시그니처를 추출하는 방법과 랜섬웨어 탐지에 가장 적절한 시그니처를 선정하는 방법을 제안한다.

키워드: 랜섬웨어, 랜섬웨어 탐지, 악성코드, 동적 분석, 시그니처, 유사도 분석

Abstract Recently, there are increasing damages by ransomware in the world. Ransomware is a malicious software that infects computer systems and restricts user's access to them by locking the system or encrypting user's files saved in the hard drive. Victims are forced to pay the 'ransom' to recover from the damage and regain access to their personal files. Strong countermeasure is needed due to the extremely vicious way of attack with enormous damage. Malware analysis method can be divided into two approaches: static analysis and dynamic analysis. Recent malwares are usually equipped with elaborate packing techniques which are main obstacles for static analysis of malware. Therefore, this paper suggests a dynamic analysis method to monitor activities of ransomware. The proposed method can analyze ransomwares more accurately. The suggested method is comprised of extracting signatures of benign program, malware, and ransomware, and selecting the most appropriate signatures for ransomware detection.

Keywords: ransomware, ransomware detection, malware, dynamic analysis, signature, similarity analysis

· 이 논문은 2017년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.2017-0-00388, 랜섬웨어 대응 기술 개발)
· 이 논문은 2017 한국정보과학회 고신뢰컴퓨팅 하계워크샵에서 '랜섬웨어 동적분석을 위한 시그니처 추출 및 선정 방안 제안'의 제목으로 발표된 논문을 확장한 것임

† 비 회 원 : 한양대학교 컴퓨터소프트웨어학과
rbqlse1004@hanyang.ac.kr
†† 비 회 원 : 한양대학교 정보보안학과
oakhouse@hanyang.ac.kr
††† 종신회원 : 한양대학교 컴퓨터소프트웨어학부 교수(Hanyang Univ.)
imeg@hanyang.ac.kr
(Corresponding author임)

논문접수 : 2017년 10월 23일
(Received 23 October 2017)
논문수정 : 2017년 12월 13일
(Revised 13 December 2017)
심사완료 : 2017년 12월 14일
(Accepted 14 December 2017)

정보과학회 컴퓨팅의 실제 논문지 제24권 제2호(2018. 2)

1. 서 론

최근 랜섬웨어로 인한 피해가 지속적으로 증가하고 있다. 랜섬웨어는 랜섬(Ransom)과 소프트웨어(Software)의 합성어로 이메일 혹은 업데이트 등으로 위장하여 침입해 사용자의 디바이스 내 데이터를 암호화한 뒤, 암호를 푸는 대가로 금전 지불을 요구하는 악성 프로그램을 말한다. 랜섬웨어는 자동화된 익스플로잇 킷(Exploit Kit)을 기반으로 인터넷을 통해 널리 유포되고 있다.

랜섬웨어는 크게 두 가지 종류가 있다. 첫째, 라커-랜섬웨어(Locker-Ransomware)는 사용자의 컴퓨터를 잠그고 더 이상 사용할 수 없게 만들도록 고안된 랜섬웨어이다. 둘째, 최근 가장 흔하게 나타나는 랜섬웨어인 크립토-랜섬웨어(Crypto-Ransomware)는 사용자 개인의 파일을 암호화하여 더 이상 파일에 접근할 수 없게 만들도록 고안된 랜섬웨어이다. 2014년에 Symantec사의 조사에 따르면 68,000여 건의 랜섬웨어 감염 사례 중 2.9%에 달하는 피해자들이 돈을 지불했다고 한다. 공격자들은 주로 비트코인을 통해 지불을 요구하며, 이는 비트코인이 추적이 불가능한 자산이기 때문이다. 안티 바이러스 개발업체들이 정교한 악성코드 변종들 및 최신 랜섬웨어에 대응하려고 하지만, 기존의 시그니처 기반 정적분석은 패킹 기술 또는 새로운 악성코드 변종 출현 등에 의해 쉽게 무력화 될 수 있다. 이러한 문제점에 대한 해결책이 될 수 있는 분석 방법이 동적 분석이다. 동적 분석은 악성코드를 실제로 실행시키며 분석하는 방법으로, 파일이 패킹되어 있어도 분석이 가능하고 실제 행위 관찰을 통해 악성코드 변종에 또한 대응 가능하다는 장점이 있다. 본 논문에서는 랜섬웨어를 동적 분석하기 위해 시그니처를 추출하는 방법과 추출된 시그니처들로부터 랜섬웨어를 특징적으로 구분 짓는 가장 적절한 시그니처를 선정하는 방법을 제안한다. 제안할 방법의 기반 근거는 랜섬웨어는 기존의 악성코드 및 정상파일과 다른 특징적인 동적 정보가 있을 것이라는 가정이다. 이에 대한 자세한 설명은 3장에서 다룰 것이다.

2. 관련연구

B. J. Kang 외 3인은 동적 바이너리 명령어의 출현 빈도를 활용하여 악성코드를 분류했다[1]. 해당 연구에서는 동적 바이너리 명령어(Instruction)를 추출하기 위하여 Intel Pin을 활용한다. 유사도 계산 오버헤드를 감소시키기 위해 반복되는 명령어 블록을 제거하고 분석했다는 점에서 의의가 있으나, 랜섬웨어 시그니처 선정으로 이어지지 못한 한계가 있다.

D. Sgandurra외 3인은 다수의 기계학습 알고리즘을 적용해 랜섬웨어의 다양한 시그니처를 학습시켜 쿠쿠 샌드박스(Cuckoo Sandbox) 환경에서 동적 분석 기반 랜섬웨어 탐지를 수행하였다[2]. 실험 결과에서 랜섬웨어 탐지에 가장 효과적인 시그니처는 레지스트리 키 관련 동작과 API 호출임을 밝혔고, 문자열, 파일 확장자 변경, 파일 시스템 관련 동작 등 기타 유용한 시그니처 또한 결과로 제시하였다.

Monika외 2인은 Windows 환경에서 쿠쿠 샌드박스를 통해 랜섬웨어 동적 분석을 수행하였다[3]. 해당 연구에서 랜섬웨어 시그니처로 분석하고 제시한 항목은 파일 시스템 활동, 암호화, 레지스트리 활동, 디바이스 통신, 네트워크 활동, 라킹(Locking) 메커니즘이었다. 해당 연구의 한계는 랜섬웨어의 동적 분석 정보 제시에 그치고, 시그니처 최적화 및 실제 랜섬웨어 탐지 실험 결과 제시로 이어지지 못했다는 점이다.

M. Zhang 외 3인은 시그니처 또는 기계학습 기반의 기존 악성코드 분류 방식이 바이트코드 수준 변형 공격에 취약하다는 점을 개선하기 위해, 가중치(Weight)가 부여된 API 의존성 그래프를 기반으로 악성코드와 정상파일을 분류하는 연구를 수행하였다[4].

Y. Park 외 3인은 시스템 콜을 기록하여 행동 그래프를 생성하고, 이를 이용하여 자동화된 행동 그래프 매칭 기법을 고안했다[5]. 해당 기법은 시스템 콜 인젝션 공격에 취약할 수 있으므로, 이에 대응할 방법을 고안해야 할 필요가 있다.

L. Nataraj 외 3인은 바이너리 이미지화를 통해 시각적 이미지 유사도 기반 악성코드 분류 방법을 제안하였다[6]. 해당 연구의 바이너리 이미지화 기법은 8bit 벡터 단위의 Gray Scale 이미지를 생성한다. 생성된 악성코드 이미지를 전처리하여 KNN 알고리즘에 적용, 악성코드 분류를 수행하였다.

J. Kinable 외 1인은 호출 그래프 클러스터링을 이용한 악성코드 분류 기법을 연구하였다[7]. 호출 그래프 간 구조적 유사성을 분석하고, 이를 기반으로 악성코드 분류 실험을 수행하였다[8].

3. 랜섬웨어 동적 분석 모델

본 논문에서는 Intel Pin을 이용하여 랜섬웨어의 특징 정보들을 추출하고, 이를 정상파일, 기타 악성코드 군에서 추출된 특징정보들 값과 비교하며 유효한 시그니처를 생성, 더 나아가 랜섬웨어 탐지에 최적화된 시그니처와 파라미터 값을 선정하는 방법을 제안한다. 전체 모델의 개요는 그림 1과 같다.

3.1 Intel Pin Tool

Pin은 Intel社에서 개발된 DBI를 수행할 수 있는 저수준 프로그램이다. DBI이란 실행파일을 실행시키는 도중에 명령어 코드를 삽입하여 원하는 정보를 얻어낼 수

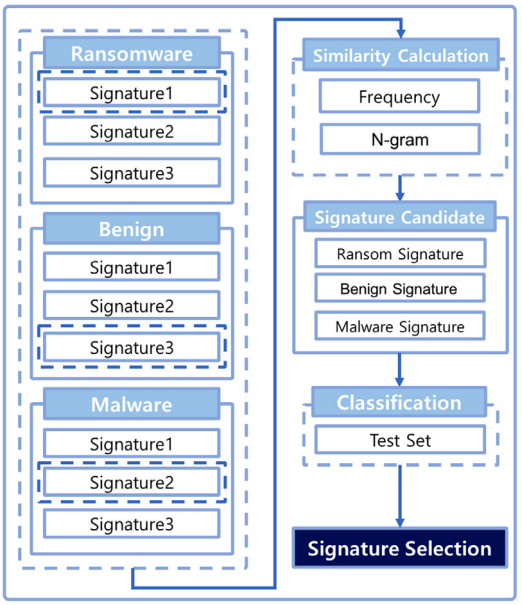

그림 1 랜섬웨어 동적 분석 모델 개요

Fig. 1 Abstract of ransomware dynamic analysis model

있는 기술이다. Pin은 JIT(Just-In-Time) 컴파일 기법을 이용하여 해당 코드의 실행 직전에 기계어로 컴파일하기 때문에, 명령어 코드 삽입 시 코드 전체에 대한 재컴파일이 필요 없다. Pin은 Windows, Linux, OSX, Android 운영체제 환경이 지원되며, CPU 버전에 의존적이다. 컴파일러 버전에 따라 Pin 버전이 다르게 제공되며, 정확한 환경설정이 필수적이다. Pin에서 예제 코드로 기본 제공되는 기능들 중엔 명령어의 총 개수 계산, 명령어의 호출 순서 기록, API 호출 기록 등이 있다. 프로그래머가 추가적으로 원하는 기능이 있다면 Pin API를 이용해 소스코드를 구현하여 Pin을 통해 DBI를 수행함으로써 얻어낼 수 있다.

3.2 랜섬웨어 특징정보

랜섬웨어의 특징정보로 추출할 수 있는 항목들은 아래와 같다. 아래 특징정보들을 기반으로 각 파일군에 대해 유사도 분석을 진행하여 시그니처를 추출한다.

3.2.1 N-Gram API 시퀀스

Pin Tool을 이용해 랜섬웨어 실행 시 호출되는 API 리스트를 추출한다. 추출된 API 리스트에서 N-Gram 시퀀스를 적용하여 유사도 계산에 활용한다. 이는 악성행위가 한 개의 API 단위보다는, 2개 이상의 단위로 이루어지는 경우가 많기 때문이다. 즉, 개별 API의 호출 빈도뿐 아니라, API들의 상호간 호출 순서 또한 매우 중요하다.

3.2.2 N-Gram 명령어 시퀀스

Pin Tool을 이용해 랜섬웨어 동적 분석 시 실행되는 명령어 리스트를 추출한다. 추출된 명령어 리스트에서 N-Gram 시퀀스를 적용하여 유사도 계산에 활용한다. N-Gram을 적용하는 이유는 3.2.1에서와 같다.

3.2.3 명령어 출현 빈도

3.2.2에서 추출된 명령어 리스트에서 각 명령어의 빈도를 기록한다. 한 명령어가 항상 똑같은 기능을 하지 않는다. 그러나 프로그램의 기능 및 특성에 따라 특정 명령어가 많아지게 되는 경향성이 존재한다. 따라서 각 명령어의 빈도수를 시그니처로 유사도 계산에 활용한다.

3.2.4 파일 확장자 변경 관련 API

대부분의 랜섬웨어는 파일을 암호화하면서 확장자를 임의로 변경한다. 사용자 PC내 파일들을 암호화하는 기능이 랜섬웨어의 가장 큰 특징이라 할 수 있으며, 짧은 시간 동안 대량의 파일 확장자 변경이 일어날 가능성이 높다. 이를 시그니처로 확보할 수 있다면 높은 정확도의 분석 결과가 예상된다. 명령어는 프로세스에서 CPU가 처리하는 가장 작은 실행 단위이기 때문에 명령어 단위로 확장자 변경 등의 포괄적 기능을 파악하기 어렵다. 반면, Windows API는 운영체제 상에서 기본 기능을 제어할 수 있도록 제공되는 인터페이스이므로, 파일 확장자를 변경하기 위해 사용되는 API들이 존재한다. 파일 확장자를 변경하는 프로그램의 호출 API들을 분석해 파일 확장자 변경 관련 API들로 그룹화 할 수 있다. 해당 API들의 출현 빈도를 유사도 계산에 활용한다.

3.2.5 파일 시스템 활동

대부분의 랜섬웨어는 암호화 시간, 비용 등을 고려하여 사용자의 PC 내에 전체 파일이 아닌 특정 확장자(.hwp, .pdf, .doc, .png 등) 파일을 중심으로 암호화를 진행한다. 암호화를 목표로 하는 확장자의 파일을 찾는 과정에서 디렉토리와 파일을 검색하고 생성하고 제거하는 등 파일 시스템에서 읽고 쓰는 동작(Read and Write)을 반복적으로 수행한다. 따라서 파일 시스템 관련 읽기, 쓰기 동작의 발생 빈도를 유사도 계산에 활용할 수 있다.

3.2.6 네트워크 통신 활동

랜섬웨어는 감염된 PC에서 C&C서버(Command and Control server)와의 통신을 구축해 암호화키와 감염 PC내의 데이터를 암호화하는데 필요한 정보를 받는다. 따라서 지속적인 네트워크 통신 활동이 발생한다. 네트워크 통신 관련 API들을 모니터링 그룹으로 정하고, 해당 그룹의 API 출현빈도를 유사도 계산에 활용해 볼 수 있다.

3.2.7 레지스트리 활동

Windows 레지스트리는 하드웨어, 소프트웨어 및 사용자 PC의 설정(Preferences)에 대한 정보가 포함되어 있다. 랜섬웨어는 컴퓨터 재부팅 후에 자신의 악성 프로

표 1 Windows 레지스트리 관련 API
Table 1 Windows Registry-related API

Registry API	
RegCloseKey	RegSetValue
RegCreateKey	RegNotifyChangeKeyValue
RegDeleteKey	RegConnectRegistry
RegEnumKey	RegCreateKeyEx
RegEnumValue	RegDeleteValue
RegGetKeySecurity	RegEnumKeyEx
RegOpenKey	RegFlushKey
RegQueryInfoKey	RegLoadKey
RegQueryValue	RegUnLoadKey
RegReplaceKey	RegOpenKeyEx
RegSaveKey	RegQueryMultipleValues
RegQueryValueEx	RegSetKeySecurity
RegRestoreKey	RegSetValueEx

세스 종료를 방지하기 위해, 레지스트리 키를 업데이트 한다. 이는 재부팅 후에도 랜섬웨어의 지속적인 활동을 가능케 한다. 레지스트리 값을 변경하려면 Windows API를 이용해야한다. 레지스트리 관련 API의 예는 표1과 같다. 랜섬웨어의 동작과정에서 레지스트리 관련 API의 호출이 빈번하게 일어날 것이므로, 레지스트리 관련 API의 출현빈도를 정상파일, 기타 악성코드의 출현빈도와 비교하여 유사도 계산에 활용한다.

4. 실험 방법 및 실험 결과

랜섬웨어군 샘플 504개, 악성코드군 샘플 3120개, 정상파일군 샘플 5000개를 대상으로 시그니처 API 출현빈도 기반 분류 실험을 진행한다.

4.1 시그니처 기반 유사도 측정 방식

본 논문에서 제안하는 동적 분석 모델의 유사도 측정은 정상파일군, 악성코드군, 랜섬웨어군 총 3개 군에 대해 수행한다. 랜섬웨어 외 악성코드군을 유사도 측정에 포함하는 이유는 랜섬웨어와 기타 악성코드군들 사이의 차이점을 분석하기 위함이다. 3.2.1~7에서 제시한 랜섬웨어 특징정보를 바탕으로 각 군의 파일들을 대상으로 시그니처별 N-Gram 시퀀스 또는 출현 빈도를 산출한다. 각 군의 파일들을 대상으로 산출한 값을 기반으로 아웃라이어(Outlier) 값을 제거한 뒤, 평균값을 계산하고 이를 해당 군의 유사도 벡터로 정한다. 해당 과정은 시그니처별로 각 군에 대해 시행한다.

4.2 유사도 비교 분류 실험

4.1에서 산출한 각 파일군별 유사도 벡터를 바탕으로 랜섬웨어 탐지 및 파일군 분류 실험을 진행한다. 테스트 샘플을 대상으로 각 파일군과 유사도 비교실험을 수행한다. 테스트 파일의 시그니처(N-Gram 시퀀스 or 출현빈도)와 각 파일군별 시그니처를 비교하여 가장 높은 유사도를 보이는 파일군에 테스트 파일이 속하는 것으로 판정한다. 랜섬웨어 탐지 정확도와 정상파일 및 기타 악성코드군 분류 정확도 평가를 위해 식 (1)을 이용한다.

$$Classfication\ Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (1)$$
$$(TP: True Positive,\ TN: True Negative,$$
$$FP: False Positive,\ FN: False Negative)$$

4.3 랜섬웨어 시그니처 자동화 추출 방법

Pin Tool 기반 시그니처 자동화 추출 모듈을 구현하여 랜섬웨어 샘플 504개, 악성코드 샘플 3120개, 정상파일 샘플 5000개를 대상으로 API, 명령어 시퀀스를 추출한다. 동적 분석의 특성상 랜섬웨어와 악성코드는 호스트와 분리된 가상 머신에서 추출해야 한다. 실험에 사용한 가상머신은 VMware Workstation 10이다. 가상 머신 환경에서샘플 파일별 일련의 시그니처 추출 과정들은 시간 소모가 상당하므로 자동화 모듈 구현이 필수적이다. 해당 모듈은 VMware社에서 기본으로 제공하는 vmrun 유틸리티를 활용하여 게스트 PC에 vmrun 명령어를 전달하여 조작하는 방식으로 동작한다. 호스트 PC에서 게스트 PC에 vmrun 명령어를 전달하는 서브프로세스(subprocess)를 생성하고, 해당 서브프로세스는 일련의 동작들을 반복하면서 랜섬웨어 시그니처 자동화 추출을 수행한다. 상술한 일련의 동작들은 게스트 PC에서 랜섬웨어 실행, 시그니처(API 또는 명령어) 추출, 로그 파일 호스트로 복사, 게스트 PC 스냅샷 복구 순으로 구성된다. 시그니처 자동화 추출 모듈의 동작원리 전체 개요는 그림 2와 같다.

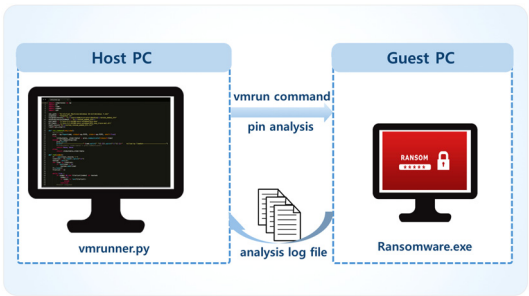

그림 2 랜섬웨어 시그니처 자동화 추출 모듈 작동 원리
Fig. 2 Automated ransomware signature extraction module

4.4 실험 방법

10겹 교차검증 방식으로 분류 실험을 진행하며, 각 군별 시그니처 리스트를 생성할 때 사용되는 임계값(threshold)은 트레이닝 셋으로부터 학습시킨 트레이닝 결과 파일에서 빈도 수 기준 상위 N%를 의미하는 값이다. 각 트레이닝 단계에서 다수의 임계값을 기준으로 시그니처 리스트를 생성 후, 각 리스트에서 API별 출현

비율에 따라 스코어를 부여하고 기록한다. 스코어가 반영된 시그니처 리스트를 기반으로 테스트 셋 대상 임계값 별 교차 분류를 수행한다. 즉, 악성코드군의 시그니처 리스트 생성 기준 임계값 개수가 n개 이고, 랜섬웨어군의 임계값 개수가 m개라면 총 n*m번의 교차 분류를 수행하는 것이다. 이는 시그니처 리스트 기반 유사도 비교 시 임계값에 따른 분류 정확도 차이 양상을 확인하기 위함이다. 군별 유사도를 측정하는 방법은 다음과 같다.

1) 테스트 파일의 API 리스트를 저장한다. 2) 각 API의 군별 시그니처 리스트에 산출된 호출 빈도 기반 스코어를 합산한다. 3) 최대 스코어가 산출되는 군에 테스트 파일이 속하는 것으로 분류한다.

4.5 실험 결과

정상파일군, 악성코드군, 랜섬웨어군에 대한 분류 실험 정확도는 표 2와 같다. 표 2의 실험에서 시그니처 생성 임계값은 정상파일, 악성코드, 랜섬웨어군 각각 8%, 5%, 7%이다.

표 2에서 볼 수 있듯이 정상파일의 분류 정확도는 악성코드, 랜섬웨어군에 비해 확연히 높다. 이는 정상파일 시그니처에 비해 악성코드와 랜섬웨어의 시그니처 유사도가 상대적으로 높다는 의미로 해석할 수 있다. 악성코드와 랜섬웨어간 분류 정확도를 높이기 위해 공통 시그니처를 필터링하고 시그니처 리스트 내 API 스코어를 정규화하여 악성코드와 랜섬웨어군 대상으로 분류 실험을 진행한 결과는 그림 3과 같다. 그림 3의 결과에서 이전 실험 정확도와 비교해볼 때, 악성코드와 랜섬웨어의 분류 정확도가 각각 약 11%, 5% 정도 향상된 것을 확인할 수 있다. 이는 분류 정확도에 시그니처 리스트가 적지 않은 영향을 미침을 나타낸다. 이에 대하여 임계값 최적화와 시그니처 리스트 필터링 및 정규화로 분류 정확도를 향상시킬 수 있음을 보였다[9].

표 2 정상파일, 악성코드, 랜섬웨어 분류 정확도
Table 2 Classification accuracy among benign program, malware, and ransomware

# of folds	Benign	Malware	Ransomware
1	81.72%	81.70%	81.81%
2	94.06%	97.56%	78.18%
3	88.96%	70.12%	77.27%
4	94.16%	72.21%	90.90%
5	95.86%	94.51%	88.88%
6	93.78%	76.89%	100.00%
7	91.24%	77.56%	81.81%
8	93.42%	32.92%	95.45%
9	94.56%	62.80%	90.90%
10	97.84%	90.85%	86.36%
Average	92.50%	75.71%	87.16%

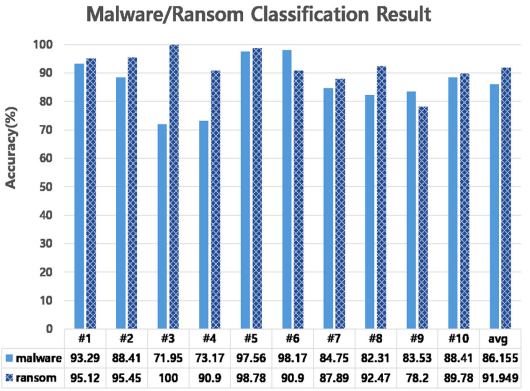

그림 3 랜섬웨어/악성코드 분류 실험 정확도
Fig. 3 Classification experiment result of ransomware and malware

5. 결론 및 향후연구

본 논문에서는 랜섬웨어 동적 분석 시 이용 가능한 특징정보를 조사하였고, 특징정보 추출 및 시그니처 선정 방법을 포함하는 랜섬웨어 동적 분석 모델을 제안하고 해당 모델을 통한 실험 방법 및 결과를 제시하였다.

랜섬웨어 동적 분석 모델의 한계점은 랜섬웨어를 동적 분석 시에 악성행위가 바로 일어나지 않고 일정 시간 잠복기를 거칠 수 있다는 점이다. 이는 랜섬웨어 개발자가 시한폭탄(Time-Bomb)과 같은 기법을 적용한 것으로 랜섬웨어의 탐지 및 분석을 더욱 어렵게 하는 요소 중 하나이다. 또한 기타 악성코드와 랜섬웨어 간의 분류 오류(False Positive)가 높게 발생할 수 있다는 점이다. 이는 악성코드 군별 시그니처와 랜섬웨어의 시그니처의 유사도 비교 과정을 더욱 정교하게 수행하여 랜섬웨어군과 기타 악성코드군 분류를 위한 최적화된 시그니처를 정하고 유사도 값을 개량하여 산출해야 할 것이다.

API 출현빈도 기반으로 수행한 분류 실험 결과에서 랜섬웨어의 탐지 정확도가 평균 92%, 악성코드와 랜섬웨어 간의 분류 정확도는 평균 88%로 산출되었다. 이에 반해 정상파일과 악성코드, 정상파일과 랜섬웨어의 분류 정확도는 평균 97% 이상으로 확연히 높게 산출된다. 이는 랜섬웨어 또한 악성코드의 한 종류로써, 기타 악성코드 군과 뚜렷하게 분류할 수 있는 시그니처를 추출하여 분류하는 것이 쉽지 않음을 나타낸다. 시그니처 기반 분류 정확도를 높이기 위해서, 시그니처 생성 임계값 조정, 시그니처 최적화, 시그니처의 각 요소별 스코어에 가중치를 적용하는 방식을 고려해 볼 수 있다. 또한 샘플 데이터 전처리 과정과 특이 결과 샘플 분리 및 분석 과정을 전체 실험에 포함시켜야 할 것이다.

향후 연구에서는 API N-Gram 시퀀스 기반 유사도

분석을 수행하여 랜섬웨어/악성코드 분류 실험을 수행할 계획이다. API 시퀀스는 API들의 호출 관계에 대한 패턴을 드러내므로, 출현 빈도 기반 분류보다 상대적으로 더 높은 분류 정확도를 보일 것으로 기대된다. 또한 명령어에 대해서도 동일한 방식으로 분류 실험을 진행하고, 최종 단계에는 API와 명령어 데이터를 가공해 기계학습에 적용하여 시그니처 기반 분류 방식과 정확도를 비교할 계획이다.

References

[1] B. J. Kang, K. S. Han, B. H. Kang, and E. G. Im, "Malware Categorization Using Dynamic Mnemonic Frequency Analysis with Redundancy Filtering," *Digital Investigation*, Vol. 11, No. 4, pp. 323-335, Dec. 2014.

[2] D. Sgandurra (2016, Sep 10). Automated Dynamic Analysis of Ransomware: Benefits, Limitations and Use for Detection [Online]. Available: https://arxiv.org (downloaded 2017, July. 12)

[3] Monika, P. Zavarsky, and D. Lindskog, "Experimental Analysis of Ransomware on Windows and Android Platforms: Evolution and Characterization," *Procedia Computer Science*, Vol. 94, No. 1, pp. 465-472, Aug. 2016.

[4] M. Zhang, Y. Duan, H. Yin, and Z. Zhao, "Semantics-Aware Android Malware Classification Using Weighted Contextual API Dependency Graphs," *Proc. of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1105-1116, 2014.

[5] Y. Park, D. Reeves, V. Mulukulta, and B. Sundaravel, "Fast Malware Classification by Automated Behavioral Graph Matching," *Proc. of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research*, pp. 1-4, 2010.

[6] L. Nataraj, S. Karthikeyan, G. Jacob, and B. S. Manjunath, "Malware Images: Visualization and Automatic Classification," *Proc. of the 8th International Symposium on Visualization for Cyber Security*, pp. 1-7, 2011.

[7] J. Kinable, and O. Kostakis, "Malware classification based on call graph clustering," *Journal in Computer Virology*, Vol. 7, No. 4, pp. 233-245, Nov. 2011.

[8] B. J. Kang, T. G. Kim, H. J. Kwon, Y. S. Choi, and E. G. Im, "Malware classification method via binary content comparison," *Proc. of the 2012 ACM Research in Applied Computation Symposium*, pp. 316-321, 2012.

[9] P. O'Kane, S. Sezer, K. McLaughlin, and E. G. Im, "SVM Training Phase Reduction Using Dataset Feature Filtering for Malware Detection," *IEEE Transactions on Information Forensics and Security*, Vol. 8, No. 3, pp. 500-509, Mar. 2013.

이 규 빈

2017년 2월 한양대학교 컴퓨터전공 학사
2017년 3월~현재 한양대학교 컴퓨터소프트웨어학과 석사과정. 관심분야는 악성코드 분석, 소프트웨어 보안, 리버싱

옥 정 윤

2017년 2월 경희대학교 컴퓨터공학과 학사
2017년 3월~현재 한양대학교 정보보안학과 석사과정. 관심분야는 개인정보보호, 악성코드 분석, 소프트웨어 보안

임 을 규

1992년 2월 서울대학교 컴퓨터공학과 학사
1994년 2월 서울대학교 컴퓨터공학과 석사
2002년 2월 University of Southern California, 컴퓨터공학과 박사
2005년 3월~현재 한양대학교 컴퓨터소프트웨어학부 교수. 관심분야는 악성코드 분석, 소프트웨어 보안, 펌웨어 보안, 클라우드 보안