산업융합연구 제21권 제9호 pp. 41-48, 2023
ISSN 2635-8875 / e-ISSN 2672-0124
DOI : https://doi.org/10.22678/JIC.2023.21.9.041

사전 탐지와 예방을 위한 랜섬웨어 특성 추출 및 분류

황윤철*
한남대학교 탈메이지 교양 · 융합대학 조교수

Extraction and Taxonomy of Ransomware Features for Proactive Detection and Prevention

Yoon-Cheol Hwang*
Assistant Professor, Department of Talmage Liberal Arts · Convergence College, Hannam University

요 약 최근 들어 개인, 기업, 국가 등 사회 전반에 랜섬웨어에 의한 피해가 급증하고 있으며 그 규모도 점차 커지고 있다. 랜섬웨어는 사용자 컴퓨터 시스템에 침입하여 사용자의 중요 파일들을 암호화하여 사용자가 해당 파일들을 사용하지 못하게 하고 그 댓가로 금품을 요구하는 악의적인 소프트웨어이다. 랜섬웨어는 기타 다른 악의적인 코드들에 비해 공격기법이 다양하고 정교하여 탐지가 어렵고 피해 규모가 크기 때문에 정확한 탐지와 해결 방법이 필요하다. 정확한 랜섬웨어를 탐지하기 위해서는 랜섬웨어의 특성들로 학습한 탐지 시스템의 추론엔진이 요구된다. 따라서 본 논문에서는 랜섬웨어의 정확한 탐지를 위해 랜섬웨어가 가지는 특성을 추출하여 분류하는 모델을 제안하고 추출된 특성들의 유사성을 계산하여 특성의 차원을 축소한 다음 축소된 특성들을 그룹화하여 랜섬웨어의 특성으로 공격 도구, 유입경로, 설치파일, command and control, 실행파일, 획득권한, 우회기법, 수집정보, 유출기법, 목표 시스템의 상태 변경으로 분류하였다. 분류된 특성을 기존 랜섬웨어에 적용하여 분류의 타당성을 증명하였고, 차후에 이 분류기법을 이용해 학습한 추론엔진을 탐지시스템에 장착하면 새롭게 등장하는 신종과 변종 랜섬웨어도 대부분 탐지할 수 있다.

키워드 : 랜섬웨어, 특성, 추출, 선택, 분류

Abstract Recently, there has been a sharp increase in the damages caused by ransomware across various sectors of society, including individuals, businesses, and nations. Ransomware is a malicious software that infiltrates user computer systems, encrypts important files, and demands a ransom in exchange for restoring access to the files. Due to its diverse and sophisticated attack techniques, ransomware is more challenging to detect than other types of malware, and its impact is significant. Therefore, there is a critical need for accurate detection and mitigation methods. To achieve precise ransomware detection, an inference engine of a detection system must possess knowledge of ransomware features. In this paper, we propose a model to extract and classify the characteristics of ransomware for accurate detection of ransomware, calculate the similarity of the extracted characteristics, reduce the dimension of the characteristics, group the reduced characteristics, and classify the characteristics of ransomware into attack tools, inflow paths, installation files, command and control, executable files, acquisition rights, circumvention techniques, collected information, leakage techniques, and state changes of the target system. The classified characteristics were applied to the existing ransomware to prove the validity of the classification, and later, if the inference engine learned using this classification technique is installed in the detection system, most of the newly emerging and variant ransomware can be detected.

Key Words : Ransomware, Feature, Extraction, Selection, Taxonomy

This work was supported by 2022 Hannam University Research Fund.
*Corresponding Author : Yoon-Cheol Hwang(dolpin2010@gmail.com)
Received July 14, 2023 Revised July 25, 2023
Accepted September 20, 2023 Published September 28, 2023

1. 서론

지난 몇 년 동안 정보통신 기술과 클라우드 컴퓨팅 기술이 발전함에 따라 클라우드 서비스를 이용하여 정보를 저장하는 양이 기하급수적으로 증가되고 있다. 이로 인해 디지털 콘텐츠를 대상으로 진행되는 악성 코드들이 컴퓨터 시스템을 감염시켜 사용자의 접근을 제한하고 가동성을 떨어뜨리는 행위도 증가하고 있는 실정이다. 그 중에서도 국가 기관, 기업, 개인 등 사회 전반에 거쳐 매우 큰 피해를 발생시키고 있는 악성 코드는 랜섬웨어(Ransomware)를 꼽을 수 있다[1].

현재 공격자들에게 랜섬웨어는 아주 매력적인 사업으로 자금을 현금화할 수 있는 수단으로 자리매김하였으며, 다른 악성 코드와 달리 감염 시스템을 폐기하여도 이미 암호화된 파일은 공격자의 도움 없이는 복구하기 어렵다. 따라서 기존의 기타 악성 코드들에 비해 공격 수법이 매우 지능적이고 교활하며, 피해 규모가 개인과 기업, 국가에게도 상당히 크기 때문에 현재 확실한 예방과 해결책이 요구되고 있다[2].

따라서 본 논문에서는 많은 피해를 주고 있는 랜섬웨어(Ransomware)를 탐지하는 탐지시스템의 추론엔진에서 랜섬웨어를 효과적으로 사전 탐지하고 예방할 수 있는 학습 데이터를 제공하기 위해 대표적인 랜섬웨어를 대상으로 랜섬웨어의 특성을 추출하는 기법을 제안하고 각 랜섬웨어가 가지고 있는 공통적인 특성을 분류한다.

분류한 랜섬웨어 특성 정보들로 이루어진 데이터를 기반으로 학습한 랜섬웨어 탐지시스템의 추론엔진을 구축하면 기존에 발생 되었던 랜섬웨어뿐만 아니라 랜섬웨어의 변종이나 신종도 쉽게 탐지할 수 있어 랜섬웨어에 의한 경제적 피해 규모도 최소한도로 줄일 수 있다.

논문의 구성은 다음과 같다. 2장에서는 랜섬웨어의 개요와 동향, 그리고 주요 랜섬웨어 대한 내용을 살펴보고 3장에서는 랜섬웨어의 특성을 추출하는 모델을 제안하고 특성을 추출하는 과정을 기술한다. 4장에서는 제안한 랜섬웨어 추출 모델에서 생성된 특성 정보들을 기반으로 랜섬웨어의 특성들을 분류하고 기존의 랜섬웨어에 분류된 속성을 적용하여 특성 분류의 타당성을 검증한다. 5장에서는 연구의 당위성과 결과를 평가하고 향후 연구 내용을 제시하면서 결론을 맺는다.

2. 관련연구

랜섬웨어는 금전적인 요구, 즉 몸값(Ransome)을 요구하는 악성 프로그램이라고 정의할 수 있다. 초기 랜섬웨어는 피해자의 정보자산에 접근 후 암호화를 수행할 뿐, 피해자 정보를 직접 훔치지는 않았지만, 최근 랜섬웨어들은 기업 및 피해자와의 협상력을 높이기 위해 피해 대상의 개인정보나 중요 및 기밀정보를 유출하고 탈취한 정보를 볼모로 다크웹에 단계적으로 공개하는 등 더욱 악질적 협상 방법으로 진화하고 있다. 최근 랜섬웨어 동향을 살펴보면 공격자들은 큰 돈을 목적으로 대기업을 목표로 APT 공격 등 다양한 해킹 기술을 이용한 공격을 수행하고 있고, 트로이목마와 같은 해킹 툴과 같이 접목되어 기존의 ATP 공격과 유사한 경향을 보이고 있다. 실제로 내부 정찰 및 공격 확산을 통해 기업 대상의 대규모 피해를 이끌어내는 해킹 그룹 주도의 공격이 늘어나고 있으며, 이들 그룹 모두 내부 정찰 및 랜섬웨어 공격 확산을 위해 트로이목마, 크리덴셜스터핑, 보안 솔루션 회피기술, 악성코드 난독화 기술, 심층 정찰기술, 악성코드 업데이트 기술, 봇 네트워크 관리기술 등을 복합적으로 사용하고 있다. 랜섬웨어 공격 대상 OS 플랫폼은 Windows 플랫폼이 대부분이지만, 최근 랜섬웨어는 OS를 가리지 않고 대규모 침해사고를 유발하기 위해 MacOS, Androiod, iOS 및 Linux/Unix에 이르기까지 감염 범위를 넓혀가고 있는 상태다. 공격자들이 기업을 랜섬웨어에 감염시키기 위해 사용한 공격벡터를 살펴보면 RDP 공격, 이메일을 통한 악성코드 전파, 소프트웨어 취약점 공격 등이 가장 주된 공격벡터로 사용되고 있다[3,4].

랜섬웨어의 종류는 다양하지만 주요 랜섬웨어들은 Crypt와 Cerber 그리고 Locky 계열로 분류할 수 있다. 현재 가장 빈번하게 발생되고 있는 랜섬웨어는 Crypt 계열의 랜섬웨어로 CryptoWall이 대표적이다. 이 랜섬웨어는 2016년 4월 카스퍼스키에서 해독하는 툴을 만들면서 발생빈도가 감소했는데 최근 변종이 등장하면서 복구하기가 많이 힘들어진 상태이다. Cerber 계열 또한 피해가 급증하고 있는 랜섬웨어로 이 랜섬웨어에 감염되면, 인터넷이 강제 종료되는 현상을 시작으로 .txt, .mp3, .mp4 등의 확장자가 .cerber 확장자로 암호화되고, 암호화된 파일이 있는 폴더에는 “내 파일 복구하는 법”이라는 텍스트 파일과 암호화 되었다는 음성파일, 웹 링크 등이 추가된다. 이러한 문제를 복구 업체에 맡겨도 30% 정도의 낮

은 복구율을 보이고 있을 정도로 복구가 힘든 유형이다. Locky라는 랜섬웨어는 주로 스팸메일을 통하여 유포되며, 가끔씩 자신에게 쓴 메일인 척 위장하는 경우도 있다. 자바 스크립트 파일이 들어있는 압축 파일들을 첨부하여 이를 실행 시에 랜섬웨어를 다운로드 및 감염이 시작된다. 감염이 되면 파일들이 암호화되고, 확장자가 .locky로 변하며, 바탕화면과 텍스트 파일로 복구 관련 메시지를 출력한다[5-9].

IBM 시큐리티(IBM Security)의 2022년 연례 보고서인 엑스포스 위협 인텔리전스 인덱스 보고서(X-Force Threat Intelligence Index)에 따르면 2021년 발생한 랜섬웨어 공격의 37%는 레빌(REvil)이 사용됐고, 류크(Ryuk)가 13%, 록빗 2.0(Lockbit 2.0)이 7%로 뒤를 이었다. 이외에 2021년 사이버 공격에 사용된 대표적인 랜섬웨어는 다크사이드(DarkSide),크리스탈(Crystal),블랙매터(BlackMatter),라그나로커(RagnarLocker),비트록커(BitLocker),메두사(Medusa),E킹(Eking),엑소리스트(Xorist)가 있다[10].

랜섬웨어의 주요 행위와 목적을 살펴보면, 대부분의 랜섬웨어는 침입 대상 컴퓨터에 C&C 서버에 암호화된 시스템 정보를 보내면서 네트워크 트래픽 발생시키고 파일 암호화에 방해가 될 만한 각종 하드 코딩 프로세스나 데이터베이스, 보안 애플리케이션, 백업 서비스 등과 같은 서비스를 종료시키는 행위를 주로 한다. 그리고, 침입 대상 컴퓨터의 볼륨 새도를 삭제하고 빈 공간과 이벤트 로그를 지우고 시스템 복원 기능을 비활성화하여 운영체제가 실행하는 시스템 복원 기능을 차단시킨다. 더불어 목표 시스템 사용자에게 파일 복원을 위한 값을 지불하게끔 하기 위해 사용자가 흔히 생성하고 사용하는 파일들을 암호화 대상으로 선택하여 암호화하고 사용자에게 몸값을 요구하는 메시지를 화면에 띄우는 작업을 수행한다[11, 12].

3. 랜섬웨어 특성 추출 모델

3.1 랜섬웨어 특성 추출 모델

랜섬웨어의 특성을 추출하고 분류하기 위해서 사용되는 특성 추출 모델은 정적 특성과 동적 특성을 추출하는 단계와 특성을 선택하는 단계, 그리고 특성을 통합하는 단계로 구성되어 있다. 제안하는 특성 추출 모델을 도식화하면 Fig. 1과 같다. Fig. 1에서 정적 동적 특성 정보 단계에서는 PEFeatureExtractor라는 도구를 사용하여 PE 파일 포맷에서 다양한 정적과 동적 특성을 추출한다. 그리고 특성 선택 과정에서는 추출된 특성 중에서 랜섬웨어를 판별하는데 유용한 특성들을 선택하고, 선택된 특성들 중에서 유사한 특성들을 그룹화하여 특성 정보를 축소하는 것은 특성 통합 과정에서 이루어진다.

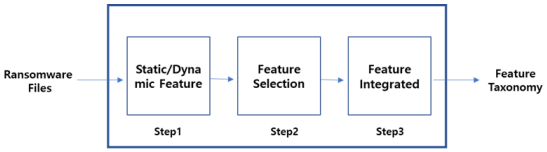

Fig. 1. Feature extraction model

3.2 랜섬웨어 특성 추출 기법

Fig. 2에서는 특성을 추출하고 분류하는 과정을 보여준다. Fig. 2에서 첫 번째 단계는 PEFeature- Extractor를 사용하여 대상 파일을 PE 파일 형식으로 로딩하고 PE 파일에서 정적과 동적 특성을 추출한다. 두 번째 단계에서는 대상 파일에서 추출한 정적과 동적 정보에서 값이 없는 항목은 제거하고 문자열과 DLL, API 정보 및 이벤트 특성을 기반으로 출현 빈도를 계산하여 특성을 선별하는 과정을 진행한다. 마지막 단계에서는 인접한 유사도를 가진 특성들을 하나의 카테고리로 통합하여 차원을 축소하고, 최종 얻은 차원 정보에 대해 이름을 명명하여 특성을 분류한다.

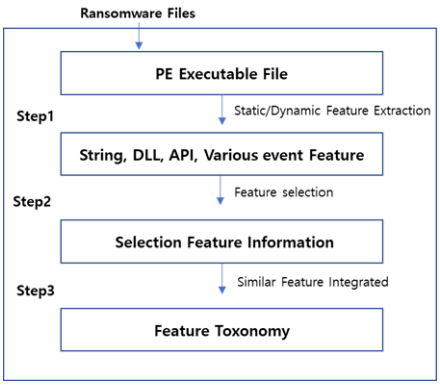

Fig. 2. Feature extraction process

3.2.1 정적 특성과 동적 특성 추출

특정한 PE 파일의 특성을 추출하는 PEFeature-Extractor라는 도구를 사용하여 PE 파일 포맷에서 PE 파

일의 크기, 시그니처와 섹션 수와 같은 파일 헤더 정보, 섹션 이름과 가상 크기와 같은 섹션 정보, PE 파일이 참조하는 DLL 파일 목록, URL과 이메일 주소 같은 특정 문자열 등과 같은 정적 특성과 파일이 처음 시작된 시간 정보, 인터넷을 통해 수행되는 네트워크 활동 정보, 파일 시스템에서 수행하는 활동 목록, 운영체제에 대해 수행하는 시스템 호출 목록, 레지스트리 수정과 파일 삭제와 같은 시스템에 가하는 변경 사항, PE 파일이 생성한 프로세스와 쓰레드 목록, 메모리 할당과 실행 가능한 코드 주소와 같은 프로세스 메모리에서 수행하는 활동 등과 같은 동적 특성들을 추출할 수 있다. 특성을 추출하는 과정은 다음과 같다.

PEFeatureExtractor를 사용하여 대상 파일을 PE 파일 형식으로 로딩하고 PE 파일에서 문자열을 추출한다. 이는 파일 내에 포함된 텍스트 데이터를 분석하여 중요한 정보를 찾는 과정입니다. 추출된 문자열은 후속 분석을 위해 저장된다. 그런다음 PE 파일에서 사용된 DLL 및 API 정보를 추출한다. 이를 통해 파일이 어떤 DLL을 사용하고 어떤 API를 호출하는지 파악할 수 있다. PE 파일의 Import Address Table (IAT)를 분석하거나 PE 헤더의 섹션 데이터를 확인하여 DLL과 API 정보를 추출합니다. 추출한 API 정보를 기반으로 API 호출을 분석하여 이벤트를 식별한다. 예를 들어, 파일 생성, 파일 삭제, 레지스트리 수정 등과 관련된 API 호출을 확인합니다. 이러한 API 호출을 기반으로 생성되는 이벤트를 식별한다.

랜섬웨어의 특성을 정상 파일과 구별하여 분류하기 위해서 특성 추출 과정을 기존의 발생하여 랜섬웨어로 판별되었던 파일과 정상 파일에 대해 각각 실행하여 추출한 특성들은 별도의 리스트로 관리한다. 랜섬웨어 파일에서 PEFeatureExtractor로 추출할 수 있는 주요 특성들을 정리해 보면 Table 1과 같다.

Table 1. PEFeatureExtractor extract feature

Feature	Extract Feature
Static info	file size, file header info, section info, DLL file list, file attribute, string, directory info, signature info, specific features info used by the file
Dynamic info	execution start time, API call pattern, file system activity, process and thread list, registry activity, system call list, network activity, External connection information, encryption info, memory activity

3.2.2 특성 선택

PEFeatureExtractor를 사용하여 대상 파일에서 추출한 많은 항목 중 값이 없는 항목은 제거하고 랜섬웨어를 판별할 수 있는 정보들중 문자열과 DLL, API 정보 및 이벤트 특성을 기반으로 출현 빈도를 계산하여 특성을 선별하는 과정을 수행한다[13][14]. 출현 빈도는 각 항목이 파일 내에서 등장한 횟수를 의미하고, 랜섬웨어와 정상 파일 간에 출현 횟수가 차이가 있는 특정 항목들을 선별하면 랜섬웨어의 특성으로 간주할 수 있다. 출현 빈도수와 출현 횟수의 차이를 계산하여 랜섬웨어와 정상 파일을 구분할 수 있다. 계산식은 아래 식 (1)과 같다.

$$FO = TOF / TSF$$
$$DO = (ONFR / NR) - (ONFN / NN) \quad (1)$$

FO: frequency of Occurrence, TSF: Total Size of Files

TOF: Total number of Occurrences of Feature

DO: Difference in number of Occurrences

ONFR: Occurrences Number of Feature in Ransomware files

NR: Number of Ransomware files, NN: Number of normal files

ONFN: Occurrences Number of Feature in Normal files

Table 2. Selection feature

Feature	Main Feature Factor
String	Your files are encrypted,Contact us,Payment instructions, Your personal files,Warning,Data encryption, Encryption key etc
API	CreateFile,ReadFile,WriteFile,DeleteFile,FindFirstFile, RegOpenKey,RegSetValue,InternetOpenUrl,CryptEncrypt HttpSendReques,CreateProcess,LoadLibrary etc
DLL	kernel32.dll,advapi32.dll,crypt32.dll,shell32.dll,urlmon.dll, ntdll.dll,ole32.dll,rpcrt4.dll,wininet.dll etc
Event	OpenFile,WriteFile,EncryptFile,RegistryWrite, CreateProcess,NetworkConnection,FileEnumeration, CodeInjection,MutexManipulation, ProcessEnumeration etc

출현 빈도수를 계산할 때는 특성의 총 출현 횟수뿐만 아니라 파일의 총 크기도 고려해야 한다. 특정 문자열이 정상 파일에서 100회 출현했지만, 파일의 크기가 매우 크다면 해당 문자열의 출현 빈도수는 낮아질 수 있기 때문이다. 그리고, 식(1)에서 랜섬웨어 파일의 특성 출현 횟수는 랜섬웨어 파일 전체에서 해당 특성이 등장한 총횟수이고, 정상 파일의 특성 출현 횟수는 정상 파일 전체에서 해당 특성이 등장한 총횟수이다. 또한, 랜섬웨어 파일 수는 랜섬웨어 파일의 총개수를, 정상 파일 수는 정상 파일의

총개수를 나타낸다. 식 (1)를 사용하여 각 특성의 출현 횟수 차이를 계산하고, 이를 통해 랜섬웨어와 정상 파일을 구분하는데 유용한 특성들을 선별한다.

선별된 특성들은 다음 단계에 사용할 입력 데이터로 사용되며, 선별된 특성 중에서 랜섬웨어 해당하는 주요 특성과 특성 인자들을 정리하면 Table 2와 같다.

3.2.3 특성 통합

선택된 특성들을 그룹화하기 위해 선별된 특성들의 유사도를 측정하여 인접한 유사도를 가진 특성들을 하나의 카테고리로 통합한다. 특성을 그룹화하기 위해 유사한 특성들을 하나의 그룹으로 묶는 군집화(Clustering) 알고리즘을 사용하여 특성의 수를 축소한다[15,16]. 이 연구에서는 파이썬에서 제공하는 Scikit-learn의 머신러닝 라이브러리인 sklearn.cluster. AgglomerativeClustering 클래스를 사용하여 계층적 군집화를 수행한다. 알고리즘으로 표현해 보면 Fig. 3과 같다.

```
from sklearn.cluster import AgglomerativeClustering

# Data preparation: matrix(row:point,column:feature of a point)
X = [[x1, x2], [y1, y2], [z1, z2], ...]

# Create and train a hierarchical clustering model
model = AgglomerativeClustering(n_clusters=10)

model.fit(X)

# Obtain cluster assignment results for each data point
labels = model.labels_
```

Fig. 3. Hierarchical clustering algorithm

Fig. 3의 계층적 군집화는 데이터 준비, 군집화 모델 생성 및 학습, 군집 할당 결과 얻기 3단계로 이루어진다. 데이터 준비에서는 군집화를 수행할 데이터를 준비한다. 데이터는 특성 행렬 X로 표현되고 각 행은 데이터 포인터(특성)을 나타내며, 각 열은 해당 포인트의 특성(특성인자)를 나타낸다. 그런 다음, AgglomerativeClustering 클래스의 인스턴스를 생성하여 군집화 모델 생성 및 학습 단계를 진행한다. AgglomerativeClustering 클래스는 거리 기반 계층적 군집화를 수행하는 클래스로, Agglomerative Clustering 클래스는 n_clusters 매개변수를 사용하여 군집의 수를 지정할 수 있다. AgglomerativeClustering 클래스는 linkage 매개변수를 사용하여 군집을 병합하는 방법을 지정할 수 있는데 여기에서는 분산을 최소화하는 방법 'ward'를 사용한다. 이 과정에서 매개변수로 군집의 개수(n_clusters), 거리 측정 방법(linkage), 연결 방식(affinity), 병합 전략(linkage) 등을 설정한다.. 그리고 fit 메서드를 호출하여 모델을 데이터에 학습시킨다. 학습이 종료된 후에는 학습된 모델을 통해 각 데이터 포인트에 대한 군집 할당 결과를 얻는다. 군집 할당 결과를 얻기 위해 labels_ 속성을 사용한다. labels는 각 데이터 포인트에 할당된 군집의 인덱스를 나타내는 1차원 배열이다.

4. 랜섬웨어 특성 분류 및 검증

4.1 랜섬웨어 특성 분류

랜섬웨어의 신종 및 변종은 기존의 랜섬웨어와 유사성을 기반으로 생성되며, 변종 랜섬웨어의 경우 행위가 유사한 기존 랜섬웨어와 행위 자체는 다를 수 있지만 논리적 구조의 주요 구성은 동일하고, 유사한 시스템 호출을 수행하기 때문에 공통 특성으로 학습된 탐지 추론엔진에서는 신종이나 변종을 쉽게 탐지할 수 있다. 본 연구에서 제안한 특성 추출 모델을 기반으로 랜섬웨어의 특성을 Fig. 4와 같이 10개의 특성으로 분류한다.

4.1.1 공격 도구

랜섬웨어는 시간이 지남에 따라 계속 발전하고 있으며 새로운 공격 도구가 나타나고 있다. 따라서, 랜섬웨어를 식별할 때 가장 좋은 특성은 목표 시스템에 대해 사용되는 랜섬웨어 공격 도구가 가지고 있는 특성들을 파악하는 것이다. 랜섬웨어에서 가장 보편적인 공격 도구로는 Exploit Kit과 Botnet, Phishing, 링크(리다이렉션), 매크로(Macro), SMB(Server Message Block), RDP(Remote Desktop Protocol), PsExec를 들 수 있다. 이런 도구들이 가지는 특성들은 랜섬웨어를 식별하는데 유용하다.

4.1.2 유입 경로

랜섬웨어는 다양한 방법으로 시스템에 침투할 수 있으며, 랜섬웨어가 사용하는 주요 유입 경로에는 Phishing 이메일, 소프트웨어의 취약점, 다운로드, PsExec 도구, 광고(Advertisement), PsExec 도구를 악용하여 침입 경로로 사용한다.

4.1.3 설치 파일

랜섬웨어 공격에서 공격자들은 다양한 실행 파일 형식

을 사용하여 악성 코드를 시스템에 설치한다. 이러한 실행 파일은 보통 .exe, .bat, .cmd, .scr 등의 확장자를 가지며, 사용자가 실행하면 랜섬웨어가 설치되고 실행된다. 랜섬웨어가 사용하는 대표적인 실행 파일은 악성 DLL 파일, mssecsvc.exe를 모방한 파일, taskhsvc.exe 있다. 이 파일들을 사용자가 실행하면 랜섬웨어가 시스템에 설치되고 실행되며, 파일들의 암호화 작업을 수행한다.

4.1.4 command and control

랜섬웨어가 타겟 시스템을 제어하기 위해 여러 프로토콜과 네트워크를 사용한다. 그 대표적인 것으로 DNS와 HTTP/HTTPS, P2P(Peer-to-Peer) 네트워크, SMB(Server Message Block) 프로토콜, Tor(Tor Onion Router) 네트워크, IRC(Internet Relay Chat) 프로토콜을 사용한다. 이러한 프로토콜은 랜섬웨어 공격자들이 제어 서버와 통신하고 명령을 전달하는 데 사용된다.

4.1.5 실행 파일

랜섬웨어들은 목표 시스템에 랜섬웨어를 설치하고 필요한 정보를 수집하여 유출하기 위해 다양한 파일들을 설치한다. 랜섬웨어가 목표시스템에 설치하는 대표적인 파일은 rundll32.exe, svchost.exe, explorer.exe cryptolocker.exe, cryptowall.exe를 들 수 있다.

4.1.6 획득 권한

랜섬웨어는 사용자 시스템에 침입하기 위해 사용자 시스템의 관리자나 사용자 권한을 획득하기 위한 일련의 작업을 수행한다. 이런 작업들은 랜섬웨어를 식별하는데 유용하다. 가장 중요한 획득 권한에는 관리자 권한이 있으며 랜섬웨어는 사용자의 무지 또는 부주의, 위장, 파일 시스템 취약점, 악의적인 프로그램 설치와 같은 다양한 방법으로 관리자 권한을 획득할 수 있다. 랜섬웨어의 목표는 관리자 권한과 파일 시스템 액세스를 획득하여 사용자의 파일을 암호화하고 시스템을 제어하는 것이다.

4.1.7 우회 기법

랜섬웨어는 원활한 침입을 위해 사용자 시스템에 작동하고 있는 보안 시스템을 우회하는 기법을 사용한다. 랜섬웨어가 사용하는 우회 기법은 암호화된 트래픽 위장기법과 시스템 취약점을 악용(Exploit vulnerabilities)한 기법, 키보드 훅(keyboard hook)을 사용한다. 이러한 우회 기법은 랜섬웨어 공격자들이 탐지와 분석을 피하고, 시스템에 침투하고 랜섬웨어를 실행하는 데 사용되는 주요 방법이다.

4.1.8 유출 기법

랜섬웨어가 가지는 특성중 하나로 유출기법을 들 수 있다. 랜섬웨어는 감염된 시스템에서 중요한 정보를 수집하고 이를 자신의 시스템으로 전송하는 기능을 수행하기도 한다. 여기에 포함되는 기능으로는 데이터 압축 및 암호화, C&C 서버로의 통신, 암호화된 파일 전송, 명령 및 제어 등을 들 수 있다. 랜섬웨어는 악의적인 목적을 달성하기 위해 대부분 암호화된 형태로 목표 시스템의 정보를 C&C 서버로 유출한다.

Fig. 4. Ransomware feature taxonomy

4.1.9 수집 정보

랜섬웨어는 목표 시스템에서 가치가 있는 정보들을 수집한다. 수집하는 정보에는 사용자 파일, 시스템 로그, 인증 정보, 브라우저 기록, 이메일 데이터 등과 같은 로컬 데이터들과 특정 파일 형식을 대상으로 파일 암호화 작업을 수행하는 데 사용하는 사용자 파일의 확장자를 수집한다. 그리고 랜섬웨어는 특정 사용자를 대상으로 한 피싱 이메일을 보내거나 사회 공학 기법을 사용하기 위해 이메일 주소, 연락처, 수신함 구성, 보낸 사람 정보 등을 수집하여 피해자의 이메일 환경을 파악한다.

4.1.10 목표 시스템 상태 변경

랜섬웨어의 최종 목적인 금전적 이득을 얻기 위해 랜섬웨어는 목표 시스템의 상태를 변경한다. 따라서 목표 시스템의 상태를 정상적인 상태가 아닌 비정상적으로 만드는 기능은 랜섬웨어를 식별하는 특성으로 볼 수 있다. 랜섬웨어가 목표 시스템의 상태를 변경하기 위해 사용되는 방법에는 디스크 구조 삭제와 암호화 기법, 복구 도구나 백업 파일 삭제나 손상, 시스템의 중요한 서비스나 프로세스 중단이 있다. 그리고 램섬웨어는 최종적으로는 사용자에게 금전적 보상을 요구하는 메시지를 표시하고, 해독 키 또는 복구 도구를 제공하기 위해 금전을 요구한다.

4.2 검증

제안한 랜섬웨어 특성 분류를 Windows 운영체제를 대상으로 하는 랜섬웨어인 Santana에 적용해서 그 타당성을 검증한다.

Satana는 피싱 이메일이나 악성 웹사이트를 통해 유입 되며, Santana가 감염되면 시스템의 모든 파일을 암호화하고 피해자에게 금전을 요구하는 랜섬웨어이다. Santana가 목표 시스템을 침입하는 데 사용하는 도구와 침입 경로는 피싱 이메일과 악성 웹사이트, USB 드라이브 등 이고, Santana가 목표 시스템에 설치하는 파일들은 ransomware.exe, config.txt이다. Santana가 목표 시스템을 제어하는 방법은 C&C 서버와 통신하는 방식을 사용하고 백도어를 생성한다.

Santana는 목표 시스템에 ransomware.exe, regsvr32.exe, cmd.exe와 같은 파일을 실행하고 관리자 권한을 획득한다. 그리고 암호화된 파일을 탐지하는 방어 기재를 무력화하고, 백도어를 생성하여 공격자가 시스템에 원격으로 접근할 수 있도록 하여 목표 시스템에 설치되어 있는 보안 시스템을 우회한다. Santana는 로컬 데이터인 사용자 이름, 암호, 이메일 주소, 신용 카드 정보와 같은 정보를 목표 시스템에서 수집하고 C&C 서버나 이메일, 암호화된 파일을 통해 수집된 정보를 유출한다. 그런 다음 목표 시스템의 상태를 모든 파일을 암호화하고, 사용자에게 금전을 요구하며 시스템을 사용할 수 없게 만든다.

5. 결론

본 논문에서는 현재 사회에 큰 피해를 입히고 있는 랜섬웨어를 효과적으로 탐지하기 위한 선결 조건으로 랜섬웨어의 특성들을 분류하는 기법을 제안하고 제안된 분류 기법에 의해 생성된 특성들을 그룹화하여 랜섬웨어 특성을 분류하였다. 랜섬웨어의 특성을 분류하기 위해 랜섬웨어 파일과 정상 파일을 대상으로 PEFeatureExtractor를 사용하여 PE 파일의 포맷에서 문자열과 DLL, API와 API를 통해 발생하는 다양한 이벤트 정보를 추출하고 출현 횟수와 빈도를 기준으로 추출된 정보들을 기반으로 랜섬웨어를 분석하는데 필요한 특성 정보들만 선택하였다. 그런 다음 계층적 군집화를 통해 유사한 특성을 가진 항목들을 그룹화하여 특성의 차원을 축소하여 최종 특성들을 선정하였다. 그리고 선정된 특성들을 기반으로 랜섬웨어의 특성을 공격 도구, 유입 경로, 설치 파일, command and control, 실행 파일, 획득 권한, 우회 기법, 수집 정보, 유출 기법, 목표 시스템의 상태 변경으로 분류하였다. 그리고 기존의 랜섬웨어인 santana를 대상으로 제안한 분류를 적용해서 분류의 타당성을 증명하였다. 제안된 분류를 사용한 데이터를 최신의 기술인 인공지능을 이용하여 추론엔진을 제작한 다음 랜섬웨어 탐지시스템에 탑재하면 지금보다 랜섬웨어를 탐지하는 성능이 향상될 것이다. 그리고 제안한 분류 특성를 좀 더 확대하여 랜섬웨어를 탐지하는 시스템의 성능을 높이는 연구와 정확한 랜섬웨어 탐지를 위한 추론엔진의 제작 연구가 꾸준히 진행되어야 한다.

REFERENCES

[1] Y. C. Hwang. (2022). Extraction and classification of malicious code feature information for intelligent detection model. Industrial Convergence Research (formerly Journal of the Korean Society of Industrial Management), 20(5), 61-68.

DOI : 10.22678/JIC.2022.20.5.061

[2] Y. C. Hwang, & H. J. Mun. (2022). Design of Intelligent Intrusion Context-aware Inference System for Active Detection and Response Journal of Convergence for Information Technology, 12(4), 126-132.
DOI : 10.22156/CS4SMB.2022.12.04.126

[3] H. S. Kim, & S. J. Lee. (2023). Comparative analysis of effective feature extraction techniques for machine learning-based ransomware attack detection. Journal of Convergence Security, 23(1), 117-123.

[4] K. B. Lee, J. Y. Ok, & K. Lim. (2018). Signature extraction and selection method for ransomware dynamic analysis. The actual journal of computing of the Society for Information Science, 24(2), 99-104.
DOI : 10.5626/KTCP.2018.24.2.99

[5] K. W. Moon, J. H. Lee. (2022). Recent Ransomware Trends and Development Direction. Journal of Information Security Society, 32(3), 33-39.

[6] K.W. Moon, J. H. Lee (2018). Analysis of latest ransomware features. Journal of the Korean Society of Communications and Communications, 43(4), 715-722.
DOI : 10.7840/kics.2018.43.4.715

[7] H. S. Kim, I. S. Kim. (2019). Malicious code distribution site characteristics analysis and countermeasures study. Journal of the Information Security Society, 29(1), 93-103.

[8] D. J. Jeon, & D. G. Park. (2018). Real-time malicious file detection technique using machine learning technique. Journal of the Korean Society of Information Technology, 16(3), 101-113.

[9] Y. S. Lee, J. W. Lee, N. Y. Rae, S. J. Jung, K Seong, & W. Y So. (2018, June). Malicious code detection method trend analysis using deep learning. In Proceedings of KIIT Conference (pp. 166-169).

[10] IBM Security X-Force Threat Intelligence Index (accessed January 6, 2023), https://www.ibm.com/reports/threat-intelligence

[11] H. M. Nam, J. S. Jang, & Y. H. Jeon. (2016). Research on analysis of ransomware attack techniques and countermeasures. Proceedings of the Korea Internet Information Society Conference, 17(1), 283-284.

[12] H. Choi, & Y. Cho (2017). Research on Minimizing the Damage from Ransomware Attack by Case Study. Journal of Korea Society of Digital Industry and Information Management, 13(1), 103-111.
DOI : 10.17662/KSDIM.2017.13.1.103

[13] Chandrashekar, G., & Sahin, F. (2014). A survey on feature selection methods. Computers & Electrical Engineering, 40(1), 16-28.

[14] K. H. Lee, M. C. Hwang, Y. I. Koo, D. Y. Hyun, & Y. Y. Yoo. (2022). A study on a ransomware detection model using opcode and API clustering and similarity analysis. Korean Information Processing Society Conference Proceedings, 29(1), 179-182.

[15] J. Y. Byeon, D. H. Kim, H. C. Kim, & S. Y. Choi, (2021). RFA: Recursive Feature Addition Algorithm for Machine Learning-Based Malware Classification. Journal of the Korea Society of Computer and Information, 26(2), 61-68.
DOI : 10.9708/JKSCI.2021.26.02.061

[16] Murtagh, F., & Contreras, P. (2017). Algorithms for hierarchical clustering: an overview, II. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 7(6), e1219.

황 윤 철(Yoon-cheol Hwang) [정회원]

- 2008년 2월 : 충북대학교 전자계산학과(이학박사)
- 2019년 3월~2021년 2월 : 가천대학교 소프트웨어 중심대학 사업단 소프트웨어교육센터 초빙교수
- 2021년 3월~현재 : 한남대학교 탈메이지 교양・융합대학 조교수
- 관심분야 : 네트워크 및 웹 보안, IDS, ITS, Fusion IT Technology(AI)
- E-Mail : dolpin98@nate.com