https://doi.org/10.33778/kcsa.2023.23.5.101

분류 알고리즘 기반 URL 이상 탐지 모델 연구 제안★

김 현 우*, 김 홍 기**, 이 동 휘***

요 약

최근 사이버 공격은 지능적이고 지속적인 피싱사이트와 악성코드를 활용한 해킹 기법을 활용하는 사회공학적 공격이 증가하고 있다. 개인 보안이 중요해지는 만큼 웹 어플리케이션을 이용해 악성 URL 여부를 판별하는 방법과 솔루션이 요구되고 있다. 본 논문은 악성 URL를 탐지하는 정확도가 높은 기법들을 비교하여 각각의 특징과 한계를 알아가고자 한다. 웹 평판 DB 등 기반 URL 탐지 사이트와 특징을 활용한 분류알고리즘 모델과 비교하여 효율적인 URL 이상탐지 기법을 제안하고자 한다.

A Study proposal for URL anomaly detection model based on classification algorithm

Hyeon Wuu Kim*, Hong-Ki Kim**, DongHwi Lee***

ABSTRACT

Recently, cyberattacks are increasing in social engineering attacks using intelligent and continuous phishing sites and h acking techniques using malicious code. As personal security becomes important, there is a need for a method and a soluti on for determining whether a malicious URL exists using a web application. In this paper, we would like to find out each feature and limitation by comparing highly accurate techniques for detecting malicious URLs. Compared to classification al gorithm models using features such as web flat panel DB and based URL detection sites, we propose an efficient URL an omaly detection technique.

Key words : Classification Algorithm, Malicious URL, Data set

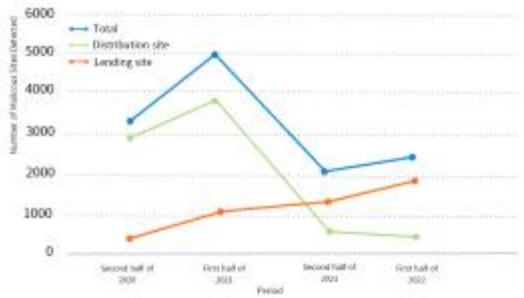
접수일(2023년 12월 22일), 게재확정일(2023년 12월 28일)

★ 본 과제(결과물)는 2023년도 교육부의 재원으로 한국연구재단의 지원을 받아 수행된 지자체-대학 협력기반 지역혁신 사업의 결과입니다.(2021RIS-002)

* 동신대학교/정보보안학과(주저자)
** 동신대학교/정보보안학과
*** 동신대학교/정보보안학과(교신저자)

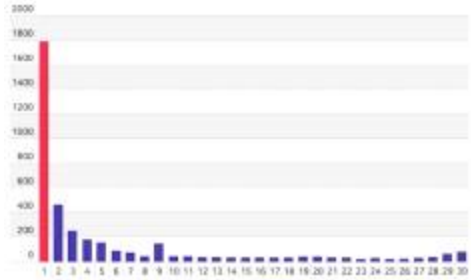
1. 서 론

현대 사회에서 웹 사용은 우리의 일상생활에 더 많은 편의성을 제공하지만, 온라인 보안 위협은 더욱 심각해지고 있다. Fig. 1은 악성코드 자체나 유포 URL이 은닉된 국내 사이트의 탐지율을 나타낸 그래프이다[1]. 스크립트가 삽입된 경유지가 증가하는 추세를 보이며 악성 URL은 매년 높은 탐지 건수를 보이고 있다. 매년 평균적으로 악성 URL이 꾸준히 보이고 있다. 이러한 악성코드를 사용자의 PC에 감염시킬 수 있는 사이트를 악성코드 은닉사이트 또는 악성 URL(Uniform Resource Locator)이라고 한다. 악성 URL을 통한 공격은 사용자가 웹 사이트에 방문하거나, 이메일을 확인하거나 스미싱 및 스팸문자를 확인할 때 발생한다. 소프트웨어 버그를 악용하여 악성코드를 실행하고, 데이터를 가로채고 공격자의 의도대로 사용자의 브라우저를 조종한다. 이와 같은 지능적이고 지속적인 공격에서 악성 URL은 악성코드를 배포하기 위한 중재자 역할을 하며 피싱사이트를 통해 사용자에게 피해를 주기도 한다.

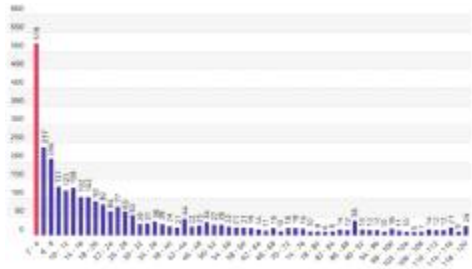


(그림 1) Statistics of Malicious Code Hidden Site Detection

.피싱 사이트는 정상 사이트와 거의 비슷하여 구분하기 어렵고 피싱 URL의 짧은 생명주기로 인하여 탐지의 어려움이 존재한다. Fig. 2를 확인해보면 피싱 URL은 24시간 안에 사라지지만 Fig.3을 보면 대부분은 단 몇 시간 안에 사라진다. 피싱 사이트의 약 84%는 24시간 미만 동안 존재하며, 평균 수명 주기는 15시간 미만으로 조사된다[2].



(그림 2) 30-day graph for disappearing phishing URLs (출처: https://www.dailysecu.com/form/html/ais/image/2023/AIS2023-6.pdf)



(그림 3) Missing Phishing URL Graphs per Hour (출처: https://www.dailysecu.com/form/html/ais/image/2023/AIS2023-6.pdf)

본 눈문 구성은 다음과 같다. 2장에서는 평판 DB 기반 URL 이상 탐지 사이트에 대해 특징과 제한을 나누고 3장에서는 VirusTotal과 AskURL 두 사이트들의 검사 결과를 비교 분석한다. 4장에서는 평판 DB 기반 URL 이상탐지 기법과 분류 알고리즘을 활용한 악성 URL 탐지 기법 두 가지를 비교하여 효율적인 기법이 무엇인지 평가하고 5장에서 특징을 추출한 분류 알고리즘 모델을 제안한다.

2. 평판DB 기반 URL 탐지 사이트

악성 URL을 탐지하려는 시도는 인터넷이 본격적으로 활성화 되며 지속 되어 왔다. 기존 악성 URL 분석 방식인 블랙리스트와 특징을 추출하는 방식은 개인 보안 및 소규모 네트워크에서 확인하기에는 잘 알려진 VirusTotal, Phishnet 등을 이용해 웹사이트 악성 여부를 검사하는 방법이 있다. 본 장에서는 기존 악성 URL 분 석 방식인 웹사이트 평판 등의 탐지와 분류 알고리즘 모델을 이용하는 방식에 대한 연구를 분석하고 한계점을 제시한다.

PhishNet은 알고 있는 데이터를 악성 목록에 추가하는 블랙리스트 기반 방식으로 악성 URL을 차단한다 [3]. 다양한 URL로부터 특징을 추출하여 블랙리스트의 목록과 비슷한 요소끼리 분류하고, 사용자가 접속한 URL에서 특징이 발견되면 즉시 차단하며 분석할 URL을 줄이면서 웹페이지 검색 공간을 확대하는 탐지 방법이다. PhishNet은 다른 탐지 모델에 함께 사용이 필요하다. 신규 및 변종 악성 URL 공격에 대응하기 어렵다. 블랙리스트 URL들을 수동적으로 새로운 규칙을 추가해야하며 이로 인해 새로운 악성 URL에 대한 식별과 차딘이 지연될 수 있다[4].

AsKURL은 문자 메시지나 이메일 내에서 URL, 이메일 주소, 단축 URL을 추출해 해당 주소들을 신속하게 분석하여 피싱 사이트인지 아닌지를 판단해 줍니다. 의심스러운 사이트를 접속하지 않고도 스크린샷을 통해 사이트를 확인하는 기능이 있어 사용자들에게 더욱 정확하고 신뢰할 수 있는 판단을 가능하게 해주는 유용한 기능을 가지고 있다[5].

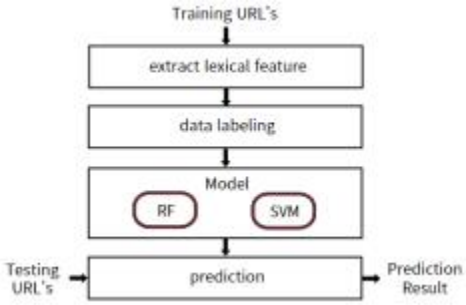
웹 사이트 평판 등의 자료기반 탐지에는 대표적으로 VirusTotal 등이 있다. VirusTotal은 많은 사용자들이 파일이나 URL이 악성 여부를 확인하기 위해 구축된 플랫폼이다. 다양한 보안 엔진을 통해 멀웨어 패턴을 탐지하고, 다양한 악성코드 및 패턴을 식별할 수 있다. 다른 사용자의 경험 정보를 공유하여 악성 URL에 대한 신뢰성을 확인 할 수 있다. VirusTotal은 특징을 명확이 가지고 있지만 한계도 존재한다[6]. 첫째, 무료 API 사용 제한으로 분당 4개의 URL을 처리한다. 대규모 처리나 대규모 트래픽에 제한이 있으며 웹 사이트 평판 등의 기반으로 많은 데이터셋을 처리하는데 제한이 있다.정상적으로 많은 URL들을 검사하기 위해서는 유료결제 및 허용된 계정 외에는 어려움이 있다. 두 번째, 엔진 업데이트가 주기적으로 필요하다. VirusTotal 사이트가 이용하는 검색엔진들은 악성파일 및 URL 검사 사이트의 엔진을 함께 이용하므로 검색 결과가 정확하지 않거나 관리적 측면에서 어려움이 존재한다.

<표 1> Previous Research on Web site Detection

Previous Research	Feature	Limitation
PhishNet	· Categorized into elements similar to blacklist entries · If see that feature in the URL, block It immediatel	· Unable to respond to attacks on new and variant malicious URLs · Decreased accuracy
Virustotal	· Detect different malware patterns through many security engines · Share information about other people's experiences	· Public APIs are limited to a maximum of four requests per minute frame · Requires regular engine updates
AskURL	· Check through screenshot without connecting suspect URL · Separate URL only and conduct inspection	· Error detection for patterned sites similar to malicious sites

3. 분류 알고리즘 기반 탐지 모델 연구

본 장에서는 제안하는 분류 알고리즘 기반을 이용한 악성 URL 탐지 기법 설명한다. Fig. 7은 데이터셋을 이용한 분류 알고리즘 기반의 악성 URL탐지 구조이다. 분류 알고리즘으로는 Random Forest(RF), Support vector machine(SVM)을 이용한 모델이다.

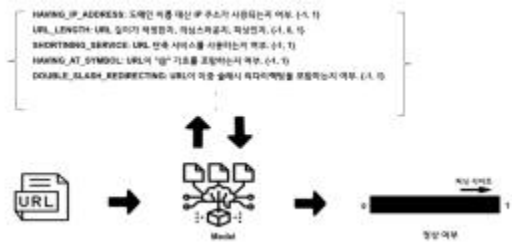


(그림 7) Malicious URL Detection Structure Based on Classification Algorithm

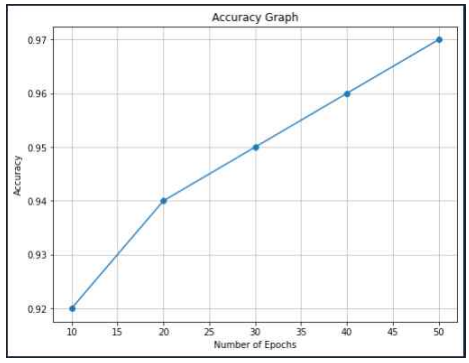
제안되는 시스템은 URL의 특징을 추출하는 모듈, 추출한 데이터를 라벨링하는 모듈, 모델을 생성하는 모듈, 악성 URL을 예측하는 모듈로 구성된다. Training Set과 성능 측정을 위한 Testing Set을 구성한 모델을 통해 여러 기반으로 분류된 어휘적 특징을 볼 수 있다. Training Set은 악성 URL의 어휘적 특징을 추출하고 Random Forest (RF), Support vector machine(SVM) 모델을 통해 학습하게 된다. 학습이 끝난 모델에 Test Set도 어휘적 특징을 라벨링하여 분류 알고리즘 모델 결과를 예측하게 된다.

모델의 훈련 단계는 다음과 같다. 데이터를 수집하여 라벨링화를 위해 데이터 전처리를 진행한다. 특징을 추출하여 해당 모델에 적용하고 그 값에 대해 성능평가를 통해 결과를 출력하는 방식이다.

URL의 특징을 추출하여 특징에 따른 모델을 구현하였으며 URL 주소 링크 내에 특징과 자바스크립트 불필요 태그 및 속성 값에 대한 특징들로 나눠 모델링을 한다. Fig 8은 각 특징들에 대해 {-1, 0, 1}로 표현해 데이터셋에 대한 평가를 통해 정상여부를 나눈다. 예측하는 결과 값을 0~1 사이의 숫자로 표기하여 1에 가까울수록 정상사이트로 구분하였다.



(그림 8) Implementing a Normal Detection Model



(그림 9) URL Detection Model Accuracy

특징을 추출하여 만든 데이터 셋은 모델링을 통해 각 URL이 특징에 따라 위험도를 판단하고 악성률을 나타낸다. 모델을 Training Set과 Test Set을 통해 모델을 학습 시키고 에포크가 늘어날수록 데이터는 점점 1의 수렴한다. Fig 9에서의 에포크는 x축이 50개로 숫자가 늘어날수록 y축 1에 가깝게 수렴하며 x축 50 이후에는 곡선형태가 아닌 직선 형태에 가까운 그래프로 예측이 된다.

4. 탐지 모델 비교

본 장에서는 평판 DB 기반 이상탐지 기법과 분류 알고리즘 URL 검사를 비교한다. 평판 DB URL검사는 악성 URL 블랙리스트를 확인하고 악

성 URL 패턴을 확인한다. 반면에 분류 알고리즘 URL 검사는 머신러닝을 활용하여 URL을 분석하고 판별한다. 두 기술의 접근성, 피드백 루프, 대규모 처리, 정확도에 대한 각각의 장단점을 비교하여, 웹 보안 분야에서 어떠한 역할을 하는지 밝히고 더 나은 모델은 제안한다.

<표 5> Abnormal Detection System Feature Comparison

Feature	DB-based(A)	Classification Algorithm(B)
accessibility	O	X
Feedback Loop	X	O
Multi-data processing	X	O
accuracy	X	O

O: A 보다 B or B 보다 A가 높다
X: A 보다 B or B 보다 A가 낮다

DB-based는 웹 기반 도구로 쉽게 접근 할 수 있으며, 개인 및 소규모 조직에게 쉽게 이용 가능하다. 하지만 웹 사이트보다 분류 알고리즘 기반 이상탐지 기법이 Feedback loop, 다중 데이터 처리에서 우수하며 정확도 면에서는 상대적으로 높은 정확성을 보인다.

5. 결론

최근 피싱 메일이나 악성 URL을 악용한 악성코드 유포, 개인정보 탈취 등 사이버 위협이 지속적으로 발생하고 있다. 이러한 개인 보안을 위해 사용자들에게 접근성이 높은 정보보안 시스템이 요구된다. 본 논문에서는 평판 DB 기반 URL 검사 사이트와 분류 알고리즘 모델의 장단점을 비교하였다.

웹 사이트 및 분류 알고리즘을 결합한 URL 검사 모델을 제안한다. 이 모델은 다중 보안 엔진 검사 및 머신러닝 기반 URL 분석의 이점을 통합하여 보다 효과적인 악성 URL 탐지를 목표로 한다. 이러한 종합적인 웹 보안 접근 방식은 웹 사용자 및 조직에 대한 온라인 위협으로부터 보다 강력한 보안를 제공하며 악성 URL로부터 사용자를 더 효과적으로 보호하는데 기여할 것으로 기대된다.

참고문헌

[1] Korea Internet & Security Agency, “Report on the detection trend of malicious code hidden sites in the second half of 2021”, “https://www.kisa.or.kr/20205/form?postSeq=1018&page=1”, accessed Oct. 23, 2023, 2022.

[2] 사준호, 이상진, “피싱사이트 실시간 탐지 기법”. 정보보호학회논문지, 22(4), pp.819-825, 2012.

[3] Chae-rim Han, Su-hyun Yun, Myeong-jin Han, Il-Gu Lee, “Machine Learning-Based Malicious URL Detection Techniqu,” Journal of The Korea Institute of Information Security & Cryptology, VOL.32, NO.3, Jun, pp.555-564, 2022.

[4] P. Prakash, M. Kumar, R. R.Kompella and M. Gupta, "PhishNet:Predictive Blacklisting to DetectPhishing Attacks," 2010 Proceedings IEEE INFOCOM, pp. 1-5, Mar. 2010.

[5] Kei Choi, “빅데이터 기반의 AI 기술을 이용한 악성URL/APK 탐지 및 분석 기술“, AIS, 2023.

[6] ALEIELDIN SALEM, SEBASTIAN BANESCU, ALEXANDER PRETSCHNER, “Automatically Analyzing VirusTotal for Accurate Labeling and Effective Malware Dection,” arXiv: 2007.00510v1 [cs.CR] 1 Jul 2020.

〔저자소개〕

김 현 우(unun4972@naver.com〉
2023년 동신대학교 정보보안학과 재학

email : unun4972@naver.com

김 홍 기 (Hong-Ki Kim)
1996년 2월 전남대학교 전산통계학과 (이학박사)
현 재 동신대학교 정보보안학과 교수

email : hkkim@dsu.ac.kr

이 동 휘 (DongHwi Lee)
2007년 경기대학교 정보보호학 박사
2011년~2012년 University of Colorado Denver, Dept. of Computer Science
2015~현 재 동신대학교 정보보안학과 교수
email : dhclub@dsu.ac.kr