IP·Domain 기반의 알려지지 않은 악성 URL 탐지 기법 연구

서민재[1], 정윤성[2], 이동우[3], 박수성[4], 류현[5], 곽나영[6], 이경문[7]▪, 전상현[8]▪

[1]국립한밭대학교, [2]세종대학교, [3]한국기술교육대학교, [4]전남대학교, [5]청주대학교, [6]명지대학교,
*[7]이스타미디어, *[8]악성코드검거단㈜
{arulroo19654, j6sung, ehddn2083, suseong0401, hyen43204, hny12202423}@gmail.com,
▪gilgil1973@gmail.com, ▪seon.jeon@akdan.co.kr

A Study on Unknown Malicious URL Detection Technique Based on IP and Domain Analysis

Minjae Seo[1], Yunseong Jung[2], Dongwoo Lee[3], Suseong Park[4], Hyeon Ryu[5], Nayeong Kwag[6],
Gyeonmoon Lee[7]▪, Sanghyeon Jeon[8]▪

[1]Hanbat National University, [2]Sejong University, [3]Korea University of Technology and Education,
[4]Chonnam National University, [5]Cheongju University, [6]Myongji University,
*[7]Estarmedia Inc., *[8]AKDAN Inc.

요 약

피싱 사이트나 악성코드 배포지와 같은 악성 URL은 주요 공격 벡터로 활용되고 있으며, 그 수가 급격히 증가함에 따라 보안 생태계 전반에 심각한 위협을 초래하고 있다. 본 연구는 머신러닝에 의존하지 않고, IP 및 Domain 수준의 네트워크 특성을 활용하여 알려지지 않은 악성 URL을 효율적으로 탐지하는 경량 탐지 기법을 제안한다. 제안된 스캐너는 WHOIS, RDAP, DNS, IP 정보를 기반으로 각 요소를 가중치화하여 스코어링을 수행하며, URL을 악성·의심·안전으로 분류한다. 또한 제안된 기법을 실제 환경에서 구현하여 실시간 대응성과 탐지 효율성을 검증하였다.

Ⅰ. 서 론

최근 피싱 사이트나 악성코드 유포지와 같은 악성 URL의 수가 급격히 증가함에 따라, 개인정보 탈취나 소프트웨어 공급망 공격 등 보안 생태계 전반에 심각한 영향을 미치고 있다.[1] Palo Alto Networks의 Unit 42 위협 인텔리전스 보고서(2024)에 따르면, 랜섬웨어 전달 방식의 약 77%가 URL 또는 웹 브라우징을 통해 이루어지는 것으로 분석되었으며, APWG(Anti-Phishing Working Group)의 2025년 1분기 보고서에서도 피싱 공격 건수가 역대 최대치를 기록한 것으로 보고되었다. 실제로 2025년 9월 8일 피싱 링크를 통해 핵심 자바스크립트 패키지 18개가 악성코드에 감염되어 주간 26억 회 이상 다운로드된 사례는 악성 URL이 주요 공격 벡터로 활용되고 있음을 보여준다.

기존 블랙리스트 기반의 악성 URL 차단 방식은 제로데이 공격이나 변형된 URL을 탐지하기 어려운 한계가 존재한다. 이를 보완하기 위해 머신러닝 기반의 악성 URL 탐지 모델에 대한 연구가 이루어지고 있으나, 새롭게 생성되거나 난독화된 URL에 대해서는 탐지 성능이 급격히 저하되며, 데이터 불균형 문제와 실시간성 및 설명 가능성의 제약 또한 보고되고 있다.[2]

이에 본 연구에서는 IP 및 Domain 수준의 네트워크 특성을 활용하여 악성 URL의 특징을 분석하고, 이를 기반으로 URL을 악성·의심·안전으로 효율적으로 분류할 수 있는 경량 탐지 기법을 제안한다. 제안된 기법은 빠른 분석 속도와 실시간 대응성 측면에서 향상된 성능을 목표로 하며, 실제 환경에서 구현 및 실험적 검증을 수행하였다.

Ⅱ. IP/Domain 분석 및 실험 설계

ⅰ. 정의

본 연구에서는 URL을 목적과 기능 수행 관점에서 정상과 악성으로 구분하였다. 정상 URL은 사용자가 의도한 서비스 목적을 수행하는 경우로 정의한다. 따라서 콘텐츠가 성인물이나 도박 등 사회적으로 바람직하지 않더라도, 사용자가 인지하고 자발적으로 접속하여 의도된 기능을 수행하는 경우에는 정상으로 분류한다. 반면, 악성 URL은 사용자의 의도와 무관하게 추가적인 위협 행위를 수행하는 경우로 정의한다. 대표적으로 사용자 계정 및 개인정보 탈취를 목적으로 한 피싱(phishing) 사이트나 악성코드 및 불법 프로그램을 다운로드하도록 유도하는 사이트 등이 이에 해당한다.

ⅱ. Domain 기반 특징 및 분석

PhishTank, OpenPhish 등에서 수집한 악성 URL 10,497개와 tranco-list 등에서 수집한 정상 URL 약 8,972개를 기반으로 분석을 수행하였다. 분석 결과, 악성 URL의 상당수는 도메인이 생성된 지 얼마 되지 않았거나, 만료일이 임박한 경우가 많았다. 이는 공격자가 탐지를 회피하기 위해 짧은 기간만 도메인을 운영한 뒤 폐기하는 전략으로, MITRE ATT&CK의 T1583.001(Acquire Infrastructure: Domains) 및 T1568(Dynamic Resolution) 전술에 해당한다. 이러한 특성으로 인해 악성 행위에 사용된 도메인은 단기 등록된 후 갱신 없이 폐기되는 사례가 다수 확인되었다.

반면 일부 악성 URL은 등록 후 1년 이상 지난 기존 도메인을 재활용하거나

탈취하여 사용하는 경우도 확인되었다. WHOIS 응답 내에서 도메인 상태코드가 serverHold, clientHold와 같은 제한 상태가 설정된 도메인은 정상 서비스에서는 거의 존재하지 않았으며, 해당 코드가 포함된 도메인은 악성 비율이 높게 나타났다. 반면 정상 URL의 경우 'client transfer prohibited', 'client update prohibited'와 같이 도메인 이전 또는 변경을 제한하기 위한 보호 코드가 적용된 사례를 다수 확인하였다.

네임서버(NS) 관점에서도 차이가 확인되는데, WHOIS로 확인한 NS 정보와 dig로 조회한 권한 NS가 불일치하는 현상은 악성 URL에서 상대적으로 높은 빈도로 관찰되었다. 또한 NS의 TTL(Time to Live) 값이 비정상적으로 짧거나, 과도하게 긴 경우에도 악성 URL에서 자주 나타났다.

한편, framer.app, vercel.app 등 웹 빌더 기반 도메인에서 악성 URL도 다수 확인하였다. 이러한 도메인은 상위 루트 도메인이 정상 서비스에 속하므로, 도메인 특성만으로는 악성 판별하기 어려워 '의심' 범주로 분류하였다.

iii. IP 기반 특징 및 분석

정상 URL과 악성 URL 모두 Cloudflare, AWS, Akamai 등과 같은 공용 CDN(Content Delivery Network) 또는 IaaS(Infrastructure as a Service) 인프라를 다수 사용하였다. 이러한 구조적 특성으로 인해 IP는 도메인보다 변동 주기가 짧고, 다수의 서비스 간 공유되는 경우가 많아 단독 지표로는 악성 여부를 판별하기 어렵다. 그래서 IP의 소유 기관, ASN, 등록 국가, 운영 주체 간 일관성을 중심으로 분석하였다.

분석 결과 eTLD+1 기준의 조직 단위 도메인이 정상적으로 운영되더라도, 그 하위 FQDN(Fully Qualified Domain Name) 단위에서 악성 URL이 호스팅 되는 사례가 다수 확인되었다. 특히 eTLD+1 도메인과 해당 FQDN이 서로 다른 ASN에 속하거나, 상이한 네트워크 사업자 인프라를 사용하는 경우 악성 행위와의 상관성이 높게 나타났다.

또한 다중 IP로 운영되는 경우에, 각 IP의 도메인 등록국가, IP 대역 등록국가, IP 관리 기관의 실제 운영 국가가 서로 상이한 경우, 악성 가능성이 높게 관찰되었다. 이는 공격자가 지리적 분산 및 관할 회피를 목적으로, 서로 다른 지역의 호스팅 업체를 조합하여 사용하는 전략과 관련이 있다. 반면, 단일 IP로만 운영되는 경우에도 해당 IP가 공용 CDN 또는 IaaS 호스팅 자원에서 제공되는 경우 악성 비율이 높게 나타났다.

iv. 아키텍처 설계 및 구현

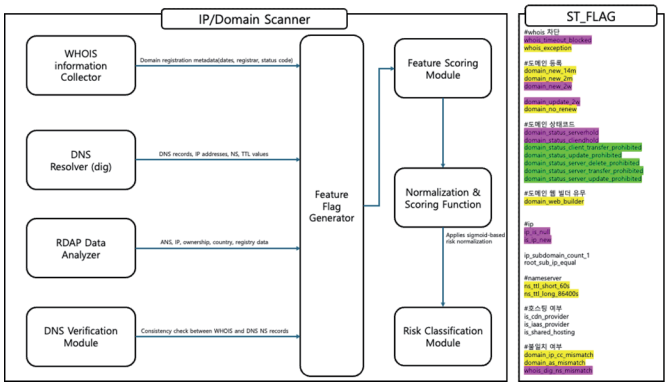

그림 1 IP/Domain 스캐너 아키텍처

그림 1은 IP/Domain 기반의 알려지지 않은 악성 URL을 분석하기 위한 IP/Domain 스캐너 아키텍처를 나타낸다. 입력된 URL에 대해 WHOIS, RDAP, dig, nslookup을 이용해 Domain 및 IP 정보를 수집하고, 수집된 각 항목이 사전 정의된 플래그(ST_FLAG)에 해당하는지를 판별한다. 판별된 플래그는 가중치 기반 스코어링 모듈에 의해 점수화되며, 이후 시그모이드(Sigmoid) 활성 함수를 적용한 정규화 과정을 거쳐 최종 위험도를 산출한다. 최종 위험도는 '악성', '의심', '안전'으로 임계값에 따라 분류된다. 또한 본 실험에서는 도메인 자체는 정상으로 보이나 경로(path) 또는 파일이 RCE(Remote Code Execution) 취약점 등으로 인해 악용된 사례는 평가 편향을 방지하기 위해 실험 대상에서 제외하였다.

Ⅲ. 성능 평가

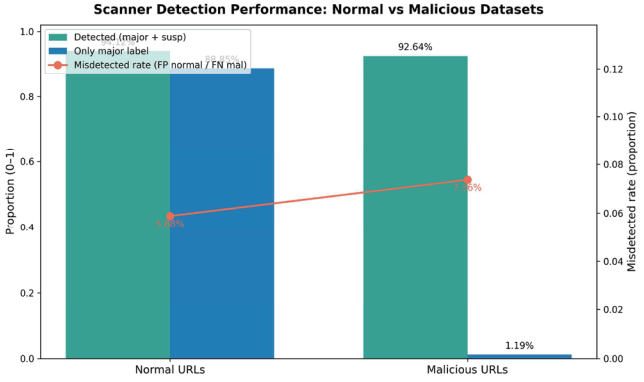

그림 2 IP/Domain 스캐너 실험 결과

그림 2는 제안된 IP/Domain 스캐너를 이용하여 정상 URL 8,972건과 악성 URL 10,497건을 대상으로 수행한 실험 결과를 시각화한 것이다. 실험 결과, 정상 URL에 대한 탐지 정확도는 94.12%, 악성 URL에 대한 탐지율(Recall)은 92.64%로 측정되었으며, 전체 평균 정확도는 약 93.3%로 확인되었다. 오탐률(False Positive Rate)은 5.88%, 미탐률(False Negative Rate)은 7.36%로 나타났다. 처리 속도 측면에서는 총 19,170개의 URL을 대상으로한 평균 처리 시간은 1.49초, 중앙값은 0.77초, 표준편차는 2.06초로 빠르게 측정되었다.

한편, 악성 URL 중 약 90% 이상이 vercel.app, start.page 등 웹 빌더 또는 공용 호스팅 인프라를 통해 배포된 사례로 확인되었다. 이러한 구조에서는 IP/Domain 기반 특성만으로는 명확히 악성 여부를 판별하기 어려워 대부분 '의심'으로 분류되었다. 반면, 정상 URL의 경우 WHOIS 도메인 나이나 상태 코드 등의 정보가 제한된 일부 예외를 제외하면 안정적으로 '정상'으로 탐지되었다.

Ⅳ. 결론

본 논문에서는 머신러닝에 의존하지 않고, IP 및 도메인 수준의 네트워크 속성에 기반한 악성 URL 탐지 스캐너 아키텍처를 설계하고 이를 구현하여 실험을 수행하였다. 실험 결과, 제안된 방식은 1차 필터링 단계에서 실시간으로 신속히 악성 URL을 선별할 수 있는 실용적 가능성을 보여주었다. 향후에는 다양한 계층의 데이터와 통합하여 스캐너의 탐지 성능을 고도화할 예정이다.

참 고 문 헌

[1] Tian, Y., Yu, Y., Sun, J., & Wang, Y. (2025). A Survey of Malicious URL Detection Techniques, Datasets, and Open-Source Implementations. Computer Networks (Elsevier).

[2] S.H. Ahammad, S. A. Mamum, M. A. H. Akhand, and M. A. Kiber, "Phishing URL detection using machine leraning methods", Advances in Engineering Software, vol. 173, p.103262, 2022

[3] S. Almomani, M. Alauthman, M. ALkhasawneh, and A. Mehmood, "A comprehensive survey of AI-enabled phishing attacks detection," Computers & Security, vol. 102, pp. 1-23, 2020(PMC7581503)