머신러닝기반의 지도학습과 분류 알고리즘을 적용한 웹쉘 탐지시스템(MWSDS)제안 연구

김기환[O], 이상도[*], 신용태(교신저자)[**]
[O]한국전자통신연구원,
[*]육군사관학교 컴퓨터과학과,
[**]숭실대학교 컴퓨터공학과
e-mail: itconsult@hanmail.net[O], znf42da@kma.ac.kr[*], shin@ssu.ac.kr[**]

Proposal and empirical study of web shell detection system (MWSDS) applying machine learning-based supervised learning and classification

Ki-hwan Kim[O], Sangdo Lee[*], Yongtae Shin(Corresponding Author)[**]
[O]ETRI,
[*]KMA,
[**]Dept. of Computer Science, Sungsil University

● 요 약 ●

본 논문에서는 웹쉘 악성코드를 정확하게 분류하고, 빠른시간안에 자동으로 웹쉘 분류 및 분석을 통하여 웹쉘을 탐지하기 위하여 인공지능 머신러닝 기반의 Supervised AI ML 및 Classification 알고리즘을 적용하여 빠른 시간안에 분류, 정확한 분석을 통하여 자동화된 탐지시스템인 MWSDS를 제안하고 웹쉘 실험 데이터를 통하여 실증하였다. 본제안의 경우 웹쉘악성코드 공격에 대한 대응뿐만아니라 관리적인 정보보호 체계수립을 통하여 보다 효과적이며, 지속적으로 대응할 수 있을 것으로 전망된다.

키워드: 웹쉘공격(WebShell attack), 머신러닝(Machine learning), 웹쉘수집및분석(WebShell collection and analysis), 방어시스템(Defense System), 자동화된웹쉘 탐지시스템(MWSDS), 인공지능(AI)

I. Introduction

최근 인터넷의 발달로 언제, 어디서든 컴퓨터, 스마트폰, 탭, 노트북 등을 통하여 인터넷검색, 모바일뱅킹, 원격 재택근무가 늘어나고 있으며, 이로 인해 인터넷을 기반으로 사용하는 기기는 기존 컴퓨터뿐만 아니라 스마트폰, 탭, IoT 기기 등 기하급수적으로 많아지고 있다. 인터넷에 언제든지 접속하여 다양한 서비스를 받고 있는 편리함과 더불어 많은 사이버공격으로 인하여 개인뿐만 아니라 기업, 국가기관에 까지 많은 피해가 발생하고 있다. 웹(WEB)으로 이루어져 있는 경우 웹쉘 악성코드를 이용한 사이버 공격이 많이 일어나고 있다. [그림 1]과 같이 2010년 약 2백만 대의 인터넷접속 디바이스가 2018년에는 약 10배에 달하는 2천만 대이며, 그중에서도 웹 기반 디바이스의 폭발적 증가로 웹쉘(WebShell) 악성코드 공격으로 인한 피해가 매년 꾸준히 발생하고 있다[1].

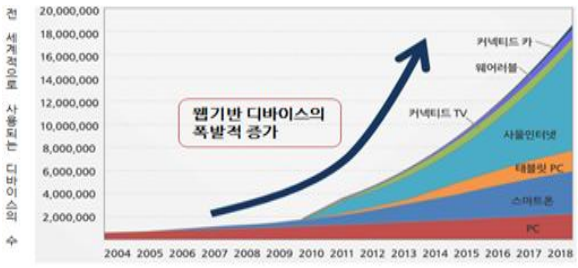

Fig. 1. 전 세계 인터넷 사용전망-디바이스 기준[1]

웹쉘이 각 시스템에 업로드 될 경우 시스템의 제어가 손쉽게 이루어질 수 있어서, 랜섬웨어, 개인정보유출 등 다양한 피해를 입히고 있다. 웹쉘 악성코드로 인한 피해가 많이 발생하면서 공공기관 및 기업에서는 방화벽, 침입통제시스템, 웹방화벽, 백신 등 다양한 보안

공격에 대비하고 있지만, 현재 설치되어있는 일반적인 보안소프트웨어 및 네트워크 보안장비에서는 웹쉘 패턴 및 특징을 알 수 없는 관계로 사전 탐지가 어려운 실정이다. 수백만건이 넘는 웹쉘을 수집하고, 수집된 웹쉘을 정확하게 분류하고, 빠른시간안에 자동으로 웹쉘 분류 및 분석을 통하여 웹쉘을 탐지하기 위한 연구가 필요한 것이다. 이에 기존 웹쉘 악성코드 뿐만아니라, 알려지지 않은 웹쉘을 사전에 탐지하기 위한 인공지능 머신러닝 기반의 Supervised AI ML 및 Classification 알고리즘을 적용하여 빠른 시간안에 분류, 정확한 분석을 통하여 자동화된 탐지시스템인MWSDS(Machine learning-based Web Shell Detection System)를 제안하였다.

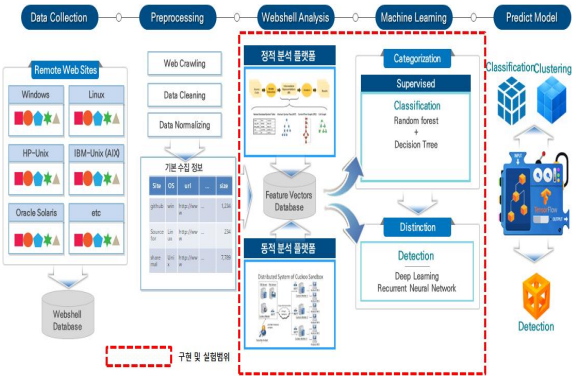

Fig. 2. MWSDS 전체 개념도

II. Preliminaries

1. Related works

1.1 웹쉘 및 머신러닝

웹쉘은 웹 파일 형태의 명령 실행 환경이자 웹 컨테이너의 원격관리 도구이다. 악성 웹쉘은 웹 서비스의 안전을 위협한다. 돌연변이 웹쉘을 효과적으로 탐지하는 것은 전 세계적으로 컴퓨터 보안에서 큰 어려움이 되었으며 PHP 웹쉘의 돌연변이 스크립트는 모든 종류의 돌연변이 웹쉘에서 가장 많고 복잡하며, 탐지하기 어렵다. 다양한 분류에서 웹쉘을 탐지하는 데 사용되는 머신러닝 기반의 혼합 시스템 모델을 제안했다. 많은 기능 엔지니어링 및 샘플 밸런싱 알고리즘을 사용하여 이 모델은 랜덤 포레스트(RF)와 컨볼루션 신경망(CNN)의 머신 러닝 알고리즘을 혼합한다. 97% 이상의 최적화된 정확도로 돌연변이 웹쉘 공격 탐지를 위한 실용적인 지능형 솔루션을 제안했다[2].

AI 기반 악성코드 분석 기술은 이러한 문제를 해결할 기술로 기대되고 있다. 알려진 악성코드 패턴들을 미리 학습하고 이를 판단하여 새로운 악성코드에도 대응할 수 있기 때문이다. 이러한 AI의 기본 분석 모델은 지도학습 모형(Supervised Learning Model)이 기본이 된다[3].

III. The Proposed Scheme

기존 웹쉘 탐지시스템의 탐지정확도 저하와 성능 문제로 인하여, 머신러닝 기법을 활용하여 [그림 2]와 같이 머신러닝 기반 웹쉘 탐지시스템(MWSDS)을 제안한다. 보안데이터 분석에 이용될 수 있는 머신러닝 기술중에 웹쉘악성코드 탐지시스템을 살펴본다. 머신러닝을 이용한 보안데이터 분석 과정은 데이터수집, 가공, 피처추출, 학습모델 구현 및 검증, 테스트과정으로 이루어진다. 웹쉘을 자동 분석하기 위하여 정적, 동적 분석 플랫폼 레이어별 컴포넌트 및 역할이 필요하다.

IV. Conclusions

웹쉘 자체는 악성코드가 아니므로 백신, 스파이웨어 등의 기본 보안솔루션에서 탐지가 잘 안 되는 상황이었다. 최근에는, 난독화된 웹쉘이 많아지고 있어서. 기존 네트워크 보안솔루션인 방화벽, IDS, IPS, WAF(웹 방화벽) 등에서도 탐지가 안 되고 있으며, 한번 침투하게 되면 인접 시스템으로 전파가 쉽다[4]. 이와같이, 웹쉘 악성코드가 갖는 잠재적인 위협과 막대한 피해 규모에도 불구하고 기본적인 웹 소스 중 하나이고, 인가된 프로세스에 의하여 침투하므로 웹쉘 탐지에 어려움이 많은 상황이다. 이러한 웹쉘 악성코드 사이버위협에 대한 방안으로는 기존의 웹쉘 악성코드 데이터에 대한 분석 뿐만 아니라, 신규 웹쉘 데이터를 수집하고, 특징을 자동으로 분류하고 분석하기 위하여 머신러닝을 통한 지속적인 학습이 필요하다. 그러하여, 기존 웹쉘 탐지솔루션의 탐지불가, 탐지성능저하 등의 문제점을 해결하기 위하여 머신러닝기반의 자동화된 MWSDS를 제안하였다. 현재 연구가 미진한 웹쉘과 같은 악성코드 탐지 자동화 부문에서도 다양한 연구 개발 과 기술 개발을 위하여, 국가에서도 정보보호지원 정책수립이 필요하다.

REFERENCES

[1] https://www.cisco.com

[2] LuJinping,TangZhi,MaoJian,Gu Zhiling,Zhang Jiemin," Mixed-Models Method Based on Machine Learning in Detecting WebShell Attack". CIPAE 2020S.G. Lee(2017-12-13), Global digital healthcare technology trends and challenges

[3] Jeong Woo-cheol. “Graph database-based malicious code multi-action pattern detection and tracking technique”. Soongsil University Graduate School. 2020

[4] KimKiHwan."Research on defense system through collection and analysis of web shell based on artificial intelligence machine learning",KSII,2019