Apache Access log와 Yara Library를 활용한 웹쉘 탐지에 대한 연구

한 국 멀 티 미 디 어 학 회
2022년 11월 18일(금)

동명대학교 정보보호학과
강태화, 김민수, 권상헌, 권수빈

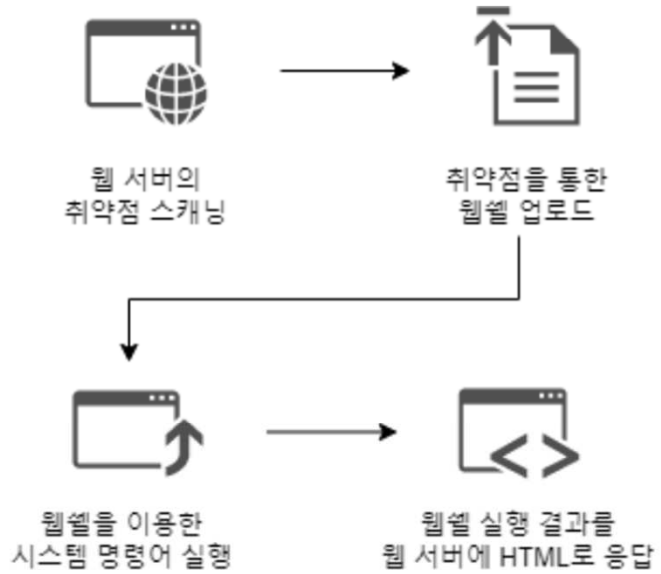
CONTENTS

1. 서론
2. 관련연구
   - WebShell, Yara Library
   - Apache Access log
3. 웹쉘 탐지 프로그램
   - 프로그램 구성
   - 탐지 시나리오
4. 결론

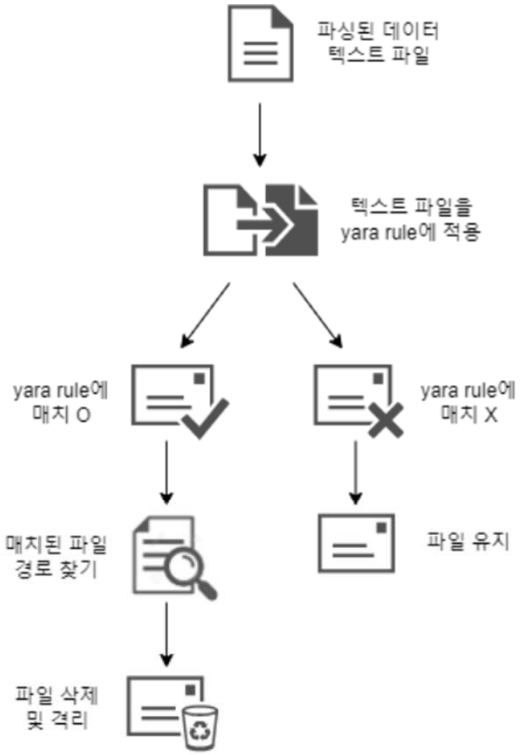
1. 서론

- 발생하고 있는 보안 위협에서 웹 기반 해킹 공격이 절반 이상의 높은 비중을 차지하며
  웹쉘을 통한 웹 서버 공격이 주를 이루고 있음
- 다양한 우회 기법이 적용된 웹쉘은 보안 장비를 갖추고도 웹 서버 안에 미리 숨겨진 웹쉘로 인해 사고가 발생함
- 네트워크 계층의 보안 장비를 우회하고 침투한 웹쉘은 어플리케이션 계층에서 동작하기 때문에 탐지하기가 어려움
- 이를 해결하기 위해 Apache Access log와 Yara Library를 활용한 웹쉘 탐지 방법을 제안함

2-1. WebShell, Yara Library



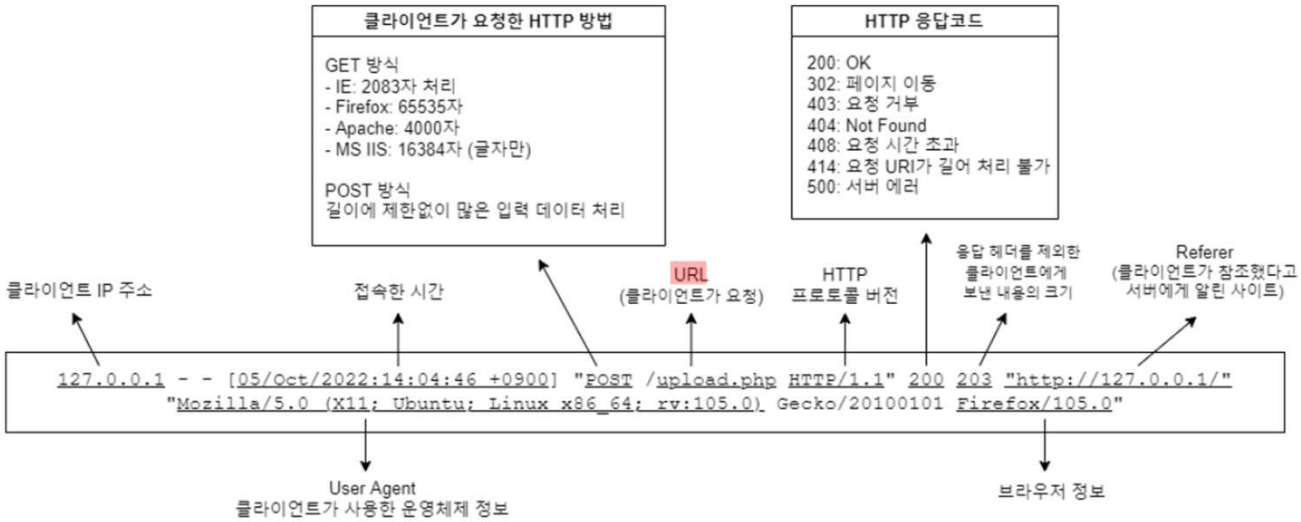
◑ 웹쉘은 악의적인 목적으로 웹 서버에 임의의 명령을 실행할 수 있도록 제작한 스크립트 파일



◑ Yara는 시그니처를 기반으로 악성코드를 분류하는 도구

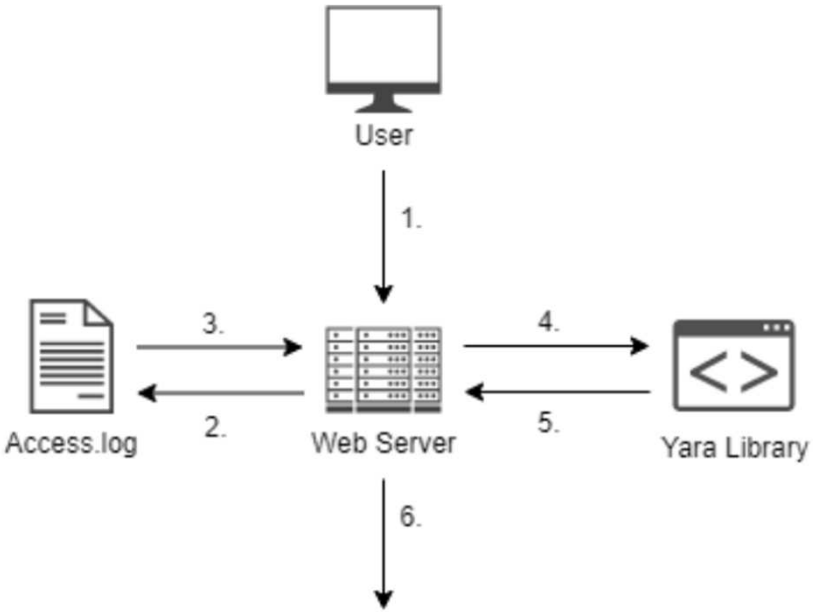
2-2. Apache Access log

- Apache Access log는 서버로부터 접속자 정보들을 보여주는 역할을 함
- 데이터의 구성은 "그림" 과 같음
- 본 논문에서는 Access log의 데이터 중 URL 데이터를 사용함



3-1. 프로그램 구성

- Apache Access log는 서버에 접근하는 사용자 기록을 수집함
- 서버는 수집한 Access.log 파일에 정규표현식을 적용하여 .txt 형식의 파싱 데이터를 생성함
- Yara Library는 파일의 시그니처를 탐색, 악성코드의 종류를 식별하고 텍스트 문자열을 탐지하기 위한 Yara Rule을 정립함



3-2. 탐지 시나리오

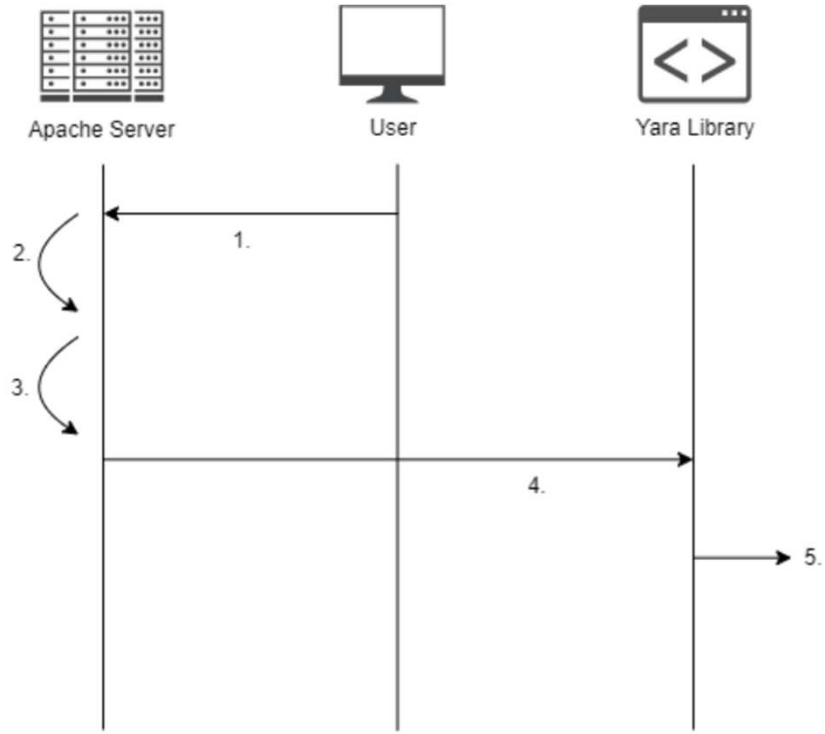
① 탐지 프로그램은 Yara Rule에 파싱된 데이터를 적용하여
탐지 과정을 수행함

② 웹 서버에 웹쉘을 업로드한 후 Access log 파일에 생성된
데이터 중 URL 데이터만 정규표현식을 이용하여 파싱함

③ 파싱을 진행한 데이터는 텍스트 파일로 저장하여 Yara Rule에 적용함

④ 이후 도출된 결과를 바탕으로 정상 탐지의 경우
파싱된 데이터를 바탕으로 탐지된 파일을 삭제 및 격리함

⑤ 탐지가 되지 않았다면 정상 파일로 판단하고 유지함



4. 결론

- 웹 기술이 고도화된 시점에서 웹 보안도 중요시 되고 있음
- 그 중 웹 기반 해킹 공격 중 하나인 웹쉘 공격으로 인한 피해가 증가하는 추세임
- 탐지를 우회하는 웹쉘은 제작이 쉽고 이 과정을 통해 침투한 웹쉘은 탐지하기 어려움
- 본 논문은 Apache Access log와 Yara Library를 활용한 탐지 프로그램을 제안함
- 제안 모델은 탐지를 우회하여 침투한 웹쉘을 탐지하여 서버 내에서 내포된 위험도를 한층 낮출 수 있음
- 점점 고도화되는 웹쉘의 기술에 대응하기위해 향후 연구로 다양한 행위기반 탐지 기법에 대한 연구가 필요함