실시간 악성파일 탐지 프로세스

BoB 8th 강성민

설계

1. Linux 시스템

기본적으로 사용하는 서비스 목록 확인

수집하는 정보: 웹로그, 네트워크 정보, 프로세스 정보, 유저별 history, Who, SetUID 설정 파일 정보, wtmp, btmp, lastlog, xferlog, cron, secure, httpd/access\_log, httpd/error\_log

기본적으로 처음 실행 이후 새로 발생한 사항만을 기록해 탐지 및 분석에 들어가는 cost를 줄일 예정

서버로 쓰이는 만큼 유저가 아닌 공격자의 행위저장에 대한 추적이 중요함

백도어 탐지는 프로세스 리스트, 네트워크 리스트, wtmp, secure, lastlog, history기록, SetUID 파일 검사 및 로그 분석을 통해 진행할 예정

SetUID는 사용자가 파일을 실행하는 동안 파일 소유자의 권한을 획득하는 것을 말함  
리눅스에서 백도어는 주로 SetUID 권한을 가지는 프로그램 중 잘 사용하지 않는 파일에 코드 내용을 추가해 사용

Wtmp 로그: 사용자들의 로그인·아웃 정보, 시스템 관련 정보를 기록(last 명령어)  
시간순으로 이벤트를 확인할 수 있음, 로그인한 IP와 시간, 리부팅한 날짜 확인 가능

Btmp 로그: 실패한 로그인 정보 확인 가능

Lastlog: 사용자의 마지막 로그인 시간, 호스트명, 포트 등 확인 가능

Xferlog: ftp 등을 통해 파일이 전송된 기록이 저장된 로그 파일

Cron: cron에 예약한 작업이 정상적으로 실행되었는지에 관한 로그를 기록한 파일

Secure: telnet, ssh 접속에 대한 유저 로그인 인증 기록

Crontab 저장 위치(공격자가 지속성을 위해 crontab 설정할 가능성이 있음) 확인 필요

1. 윈도우

레지스트리 감사 활성화(새로운 프로세스 실행 감지 설정)

프로세스 실행 탐지

실행 프로세스 PE 여부 확인(pyhon pe module) 및 디지털 서명 확인 (sigcheck)

IAT 테이블 확인

String 추출, YARA Rule

Virustotal\_api

의심 프로세스 발견시

다운로드 경로 확인 (웹 아티팩트, 이메일 아티팩트 등)

프리패치 수집

파일 시스템 아티팩트 수집(forecopy.exe)

레지스트리 (regripper.exe)

악성코드 선호 경로 확인(시스템 폴더, 사용자 기본 폴더, 사용자 데이터 폴더, 휴지통 폴더, 시스템 볼륨 정보 폴더, 임시 폴더 등…)

백도어 탐지를 위한 실행 프로세스, 네트워크 정보 확인 필요, 계정 점검, 스케쥴러 확인 필요