01

초연결네트워크

웹 악성코드 탐지 기술

- **특 허 명 :** 다중 분석기반 웹 악성코드 탐지 기술
- **보유기관 :** 국가보안기술연구소
- **상태정보 :** 출원예정

특허원문보기

출원예정

기술개요

- 웹리소스 수집, 자바스크립트 분석, Yara 분석 등 여러 기술들을 종합적으로 활용하여 입력된 Workflow에 따라 분석을 수행하고 분석된 내용을 종합 판단하여 웹 악성코드를 탐지하는 기술
- 웹 악성코드 탐지 서비스를 제공하는 보안기업 또는 대응탐지가 필요한 기업(조직)

기존 문제점

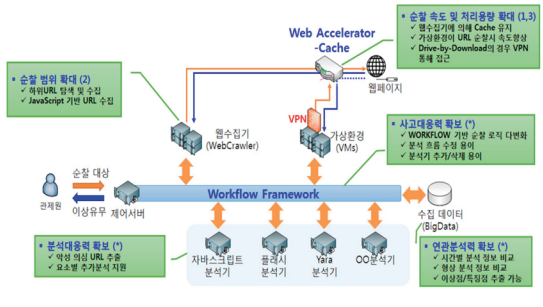
- 탐지 데이터의 지속적인 업데이트
- 탐지 범위의 한계 및 유포 스크립트의 난독화
- 동적 분석으로 인한 공격자 회피 및 분석 시스템 우회

기술 차별점

- 복합적인 분석기술 활용 및 로직 변경 용이
- 캐싱과 VPN 활용 성능과 시스템 은닉성 확보
- 범용 적용

세부내용

- 웹리소스 수집 속도, 분석 성능, 공격자에 대한 시스템 은닉성을 확보하기 위한 선택적 VPN 네트워크 라우팅 및 웹 리소스 캐싱 구조 적용
- 지속적으로 변화하는 웹 공격에 신속한 대응을 위하여 Workflow, 분석 연동기술 적용
- 웹 악성코드 탐지 및 웹 서비스 보안 유지를 필요로 하는 곳에 범용적으로 적용가능



기술이전 문의

- 국가보안기술연구소 주익수(042-870-4965, tech@nsr.re.kr)
- 공동마케팅사무국 이가영(042-862-6985, gylee@wips.co.kr)