특허 1: 악성 코드 수집 방법 및 시스템

웹 기반 공격에 사용되는 악성 코드를 자동으로 수집하고 분석하는 시스템에 관한 기술이다. 수 집된 도메인의 악성 확률을 기반으로 분석 순위를 정하고, 하위 페이지까지 크롤링하여 의심 콘 텐츠를 선별한다. 이들 콘텐츠는 먼저 악성 탐지 모델로 1 차 필터링되며, 이후 허니팟 에이전트를 통해 2 차 분석된다. 이 과정에서 정적 및 동적 피처를 추출하고, 이를 딥러닝 기반 알고리즘으로 분석하여 악성 여부를 판단한다. 면웹, 딥웹, 다크웹, 해커 사이트의 콘텐츠까지 수집 대상에 포함 되며, 자동화된 수집·분석을 통해 높은 정확도와 리소스 절감을 동시에 실현할 수 있다.