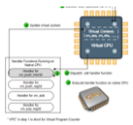
가상화 난독화 악성코드 분석 연구

에뮬레이션 기술 및 인공지능을 활용한 가상화 난독화 악성코드 복원 기법

적용분야·제품

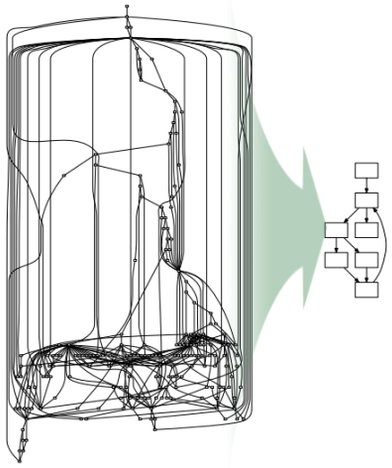
분석 방지기술 적용
악성코드 분석

난독화 적용
악성코드 분석



가상화 적용
악성코드 분석

기술개요



- 최근 가상화 난독화 기술을 적용한 악성코드의 경우, 원본 코드를 파악하는 것이 매우 어렵고 기존의 탐지 기술을 우회할 수 있는 문제점이 존재함
- 에뮬레이션 기술 및 인공지능 기반의 복원 기법을 통해 가상화 난독화 기술이 적용된 악성코드를 복원함으로써, 악성코드 탐지 성능을 높이고 미탐을 줄이는 것이 가능함

기술 경쟁력

기존기술 — 기술 차별성 — 대상기술

- 기존의 악성코드 탐지 시, 가상화 난독화가 적용되어 실제 코드를 파악하지 못하게 되고 탐지 성능을 높이지 못하는 문제가 존재

- 가상화 난독화 악성코드를 복원할 수 있는 에뮬레이션 기술 및 인공지능 기바의 가상화 난독화 악성코드 복원 기술 개발

기술적 한계

- 난독화(packing & obfuscation) 적용 시, 원본 코드에 대한 복원이 어려워지고 실제 악성 행위에 관련된 API를 파악하기 어려움
- 가상화(virtualization) 적용 시, 원본 코드가 가상 머신에서 에뮬레이션 되므로, 악성 행위을 파악하기 어려움

기술적 우위

- 에뮬레이션 기반의 난독화 악성코드 복원을 통해, 원본 파일을 복원하고 실제 악성 행위와 관련된 API를 복원 가능
- 인공지능 기반의 가상화 코드 복원을 통해, 원본 코드에 대한 파악 및 분석 가능