가상 분석환경 회피기술이 적용된 지능형 악성코드 탐지를 위한 리얼머신 기반 분석방법

홍길동*

*한국대학교 정보보호학과

I.서론

정보보호 R&D 데이터 챌린지 데이터셋 가운데 가상 분석환경 회피기술(Anti-VM)이 적용된 악성코드를 추출하여 동적 분석환경의 완성도를 높이기 위한 새로운 접근 방법을 제시하고자 한다. KISA-CISC2017-Intelligent-Mal 데이터셋 중 가상 분석환경 회피기술이 적용된 악성코드는 총 10개로 레스트리 정보 확인, 파일 또는 폴더 정보 확인, 프로세스 및 서비스 정보 확인 등을 통해 가상 분석환경을 회피하고 있는 것을 확인하였다. [데이터셋 분석결과 요약] [알고리즘 요약]

II. 방법론

Anti-VM기술이 적용된 악성코드의 특징을 분석, 단점을 보완하여 탐지환경을 구성하였다. 기존의 Anti-VM악성코드 탐지를 위해 활용하였던 동적 분석 환경의 특성을 문헌분석하여, 이를 보완하는 환경을 구축하였다.

우선, API후킹 기술을 이용하여 실시간 추출하여 악성행위정보를 파악한다. 그리고 능동적 사용자 행위 개입 기법구현을 위해 사용자 행위를 분류하였다.

2.1 데이터셋 분석결과

2.2 알고리즘 설명

2.3 pseudo code

III. 프로그램 설명

IV. 실험

Anti-VM기술이 적용된 악성코드 15개를 대상으로 활동성 비율을 실험하였다. 논문에서 제안하는 바이너리 자동실행 시스템을 이용하여 악성코드를 구동시킨 후 악성

행위와 관련하여 호출된 API를 추출하였다. [실험환경] [실험방법]

V.평가

실험결과, 15개 악성코드 중 20%에 해당하는 3개 악성코드는 기존의 기술을 회피하기 위한 기법이 적용되어 행위정보 수집에 한계를 보였다. [실험결과]

VI.결론

알려진 가상머신을 이용한 동적 분석 기술은 악성코드 특성을 추출하는데 한계가 있으므로, 리얼 머신기반의 분석기술이 필요함을 확인하였다. [결론]

[참고문헌]

[1] D.S.Milojicic, V.Kalogeraki, R.Lukose,K.Nagaraja, J.Pruyne, B.Richard, S.Rollins and Z.Xu, Peer to Peer Computing, HP Laboratories Palo Alto HPL-2002-57, March, 2002.

[2] 조호묵 외,“지능형 악성코드 분석을 위한 리얼머신 기반의 바이너리 자동실행 환경”, 정보과학회, 22(3) 2016.3, 139-144.