DynamoRIO를 이용한 시간제약 악성코드 행위 수집 기법

장진석°, 조호묵, 김용민

° 카이스트 사이버보안연구센터, 전남대학교 전자상거래전공

° ejsjang@kaist.ac.kr, chmook@kaist.ac.kr, ymkim@chonnam.ac.kr

Behavior Collection Technique for Time Constraint Malware using DynamoRIO

Jin-Seok Jang°, Ho-Mook Cho, Yong-Min Kim

° KAIST Cyber Security Research Center, Dept. of Electronic Commerce. Chonnam Nat'l Univ.

요 약

최근 ICT 발전에 따라 악성코드를 통한 사이버 위협은 지속적으로 증가하고 있다. 이를 효과적으로 대응하기 위해 자동화 동적 분석 시스템이 다양하게 연구되고 있다. 하지만 최근 대부분의 악성코드는 난독화 및 가상머신 감지, 사용자 행위 개입 요구, 시간 제약 등 분석우회 기법이 적용되어 악성 판단을 위한 선행 조건인 악성코드의 완전한 구동 및 악성 행위 수집에 한계가 발생하였다. 따라서 본 논문에서는 분석우회 기법 중 시간제약 기술이 적용된 악성코드를 보다 완성도 높게 구동을 모의하여 의미 있는 악성 행위가 수집될 수 있도록 DynamoRIO를 이용한 행위 수집 기법을 제안한다.

1. 서론

최근 IT 환경에서의 악성코드 위협은 과거에 비하여 가파른 증가세가 보이고 있다. 이는 코드 난독화, 행위 감지, 시간 제약 등 분석 및 탐지를 어렵게 하는 분석우회 기법이 확대 적용되어 기존 정보보안 시스템의 탐지 한계와 더불어 신규 취약점을 기반으로 하는 악성코드가 폭발적으로 증가하였기 때문이다[1]. 이와 같이 증가하는 악성코드 위협에 대해 효과적이고 빠르게 대응하기 위한 자동화된 분석 및 탐지 시스템이 필요하며, 다양한 방법으로 연구되고 있다. 하지만 분석을 어렵게 하는 회피 기술 또한 지속적으로 고도화되고 있어 분석우회 악성코드에 대한 효과적이고 새로운 대응 기법이 필요하다[2].

따라서 본 논문에서는 분석우회 악성코드의 완성도 있는 구동을 모의하여 분석에 필요한 행위 정보를 효과적으로 수집할 수 있는 DynamoRIO 기반 악성코드 행위 수집 기법을 제안하고자 한다.

2. 관련연구

2.1 악성코드 분석 기법

전통적으로 악성코드를 분석하는 방법은 크게 정적 분석과 동적 분석으로 나눌 수 있다. 정적 분석은 악성코드를 실행 시키지 않고 구성 요소들의 연관성 및 호출 관계 등을 분석함으로써 악성코드의 구조와 삽입된 DLL 등을 빠르게 파악 할 수 있어 선행 분석에 많이 사용된다. 하지만 코드 암호화 해제, 은닉 기술이 적용되어 있는 경우 분석에 상당한 시간과 노력이 필요한 단점이 있다. 실제 악성코드를 실행시킨 다음 시스템 변화를 분석하여 악성 여부를 판단하는 동적 분석은 정적 분석에 비해 탐지 정확도가 높으나, 행위 감지, 분석 환경 감시 등의 분석우회 기법에 의해 효과적인 분석이 제한되는 단점이 있다[3]. 하지만 폭발적으로 증가하는 악성코드를 효과적으로 분석하기 위해 최근에는 자동화된 동적 분석 방안에 대한 연구가 대부분이다[4].

2.2 분석우회 기법

분석우회 기법은 크게 세 가지로 분류 할 수 있다. 첫 번째, 실행 파일, 참조 레지스트리, 네트워크의 MAC 주소 등 가상머신 및 에뮬레이터의 고유 환경 설정 값을 식별하여 우회 할 수 있다[1]. 이는 환경 설정 값을 변경하거나 리얼머신을 통해 대응이 가능하다. 두 번째, 사용자 행위 개입을 요구하는 형태의 마우스 클릭, 팝업 창 확인 등 사용자 행위 이벤트 트리거를 전제로 한 분석 우회 기법이 있으며 이는 클릭, 드래그 등 사용자 행위 개입을 자동화하여 대응이 가능하다. 세 번째, 시간을 지연하거나 특정 시간에 악성 행위를 수행하는 시간 제약 분석우회 기법이 있다. 이 분석우회 기법은 무한정 대기를 통해 대응할 수 있으나 상당한 리소스 및 시간 소모가 발생하여 현실적으로 사용이 불가능하다. 따라서 시간제약 기법에 효과적으로 대응하기 위해서 새로운 대응 방법이 필요하다.

2.3 기존 연구 및 한계점

악성코드를 자동 분석하기 위해 기존에 연구된 대표적인 동적 분석 시스템은 표 1과 같이 Anubis, CWSandbox, WiLDCAT, Joebox, CuckooSandbox가 있

표 1. 기존 동적 분석 시스템 기능 비교

구분	Anubis	CW Sandbox	WiL DCAT	Joebox	Cuckoo Sandbox
커널 구성 요소 수집	X	○	○	○	○
API 호출 수집	○	○	X	○	○
시스템 변화 수집	○	○	X	○	○
가상환경 감시 대응	X	X	X	X	X
사용자 행위 개입 대응	X	X	X	○	△
시간제약 대응	X	X	X	X	X

다[5]. 대부분의 시스템은 커널 구성 요소, File, Registry, Process 등 시스템 변화, API 호출 수집이 가능한 반면, 가상머신 또는 에뮬레이터를 기반 프레임으로 활용하기 때문에 가상환경 감시에 대응하지 못하는 한계가 발생한다. 또한 사용자 행위 개입 요구에 대한 대응은 대부분이 제한되며, 시간제약 기법에는 모두 대응하지 못하는 한계가 있다. 따라서 본 논문에서는 리얼머신을 통해 가상환경 감시 기법에 대응하고, 버튼 클릭과 같은 행위 개입을 자동화와 DynamoRIO 를 이용하여 시간제약 기법에 대응하는 행위 수집 기법을 제안하고자 한다.

3. 시간제약 악성코드 행위 수집 방안

3.1 DynamoRIO 기반의 API 모니터

악성코드를 효과적으로 분석 및 탐지하기 위해 의미 있는 악성행위 정보 수집은 필수 사항이다. 완전한 구동을 통해 의미 있는 악성 행위 정보를 수집 할 수 있지만 시간 제약 악성코드는 시간 지연 함수를 이용하여 악성 행위를 회피한다. 이를 대응하기 위해 악성코드의 동작 흐름을 제어하여 완전한 실행이 될 수 있도록 모의 할 수 있는 방법이 필요하다. 동작 흐름 제어 방법으로 API 변조가 있다. DBI(Dynamic Binary instrumentation) Tool 은 실시간 명령 제어로 프로그램 코드 변환이 가능하고, 그 중 DynamoRIO 는 직접 명령을 삽입하여 API 변조와 흐름 제어의 효율성이 높다. 본 논문에서는 그림 1 처럼 분석 환경 프레임과 API 흐름 제어 기술로 시간 제약 악성코드의 행위 수집을 한다.

악성코드 행위 수집 환경은 리얼머신을 사용하여 가상 환경 감시 기법에 대응하고, 분석 우회 기술 중 하나인 사용자 행위 개입은 기존 연구에서 검증

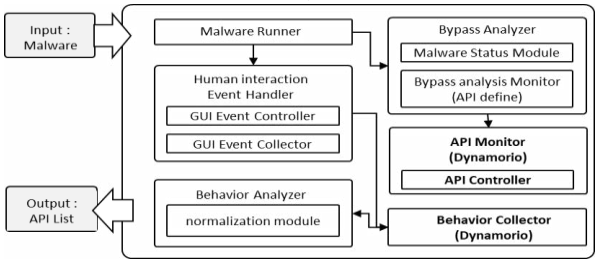

그림 1. DynamoRIO 기반 행위 수집 아키텍처

된 기술을 사용하여 분석 우회에 대응한다[1]. 시간 제약 동작 행위는 Sleep, SleepEx API 로 실행 시 커널레벨에서 호출되는 API 는 NtdelayExcution, NtWaitForSingleObject 이다. DynamoRIO 를 이용하여 악성코드 실행 및 API 호출을 추적하고, 시간 제약 API 가 호출 될 경우 흐름 제어 할 수 있는 BasicBlock 를 추가하여 시간 제약의 최종 호출 단계인 NtdelayExcution 의 파라미터를 변경하거나 호출을 우회하여 완전한 동작으로 의미 있는 악성 행위 수집을 극대화 한다.

3.2 실험 및 분석

악성코드가 동작 할 수 있는 동일한 윈도우 환경에서 임의의 악성코드 100 개에 대한 API 호출 리스트를 비교하였다. 시간 제약이 없는 악성코드 81 개는 동일한 API 호출 결과를 보였으며, 19 개의 악성코드에서 상이한 결과가 확인되었다.

흐름 제어를 하지 않은 경우 평균 181 개 API 가 호출되었고, 흐름 제어를 했을 경우 악성 행위와 관련된 NtReadFile, NtWriteVirtualMemory 등 추가 API 가 발생되어 평균 271 개가 호출되어 약 33%가 증가된 것을 확인 할 수 있었다.

4. 결론 및 향후 연구

악성코드를 효과적으로 분석하기 위해 선행적으로 완전한 구동이 선행되어야 한다. 본 논문에서는 시간제약 악성코드 구동의 완성도를 높이기 위해 분석 환경 프레임과 DynamoRIO 를 이용한 API 흐름 제어를 통한 악성행위 수집 기법을 제안하였고 API 수집 결과를 통해 시간제약의 분석우회 악성코드 수집 성능이 향상함을 보였다. 향후 특정 시간 및 시간 지연 분석우회 기법 외에 다양한 분석우회 기술에 사용하는 API 를 분석 및 정의하고, 동적 분석 시스템 설계와 고도화 연구를 진행할 계획이다.

5. 참고 문헌

[1] 조호묵외 3 인, “지능형 악성코드 분석을 위한 리얼머신 기반의 바이너리 자동실행 환경,” 정보과학회 컴퓨팅의 실제 논문지, 제 22 권, 제 3 호, pp. 139-144, 2016 년 3 월.

[2] 이경률외 2 인, “분석기법을 우회하는 악성코드를 분석하기 위한 프로세스 설계,” 정보화정책저널, 제 24 권, 제 4 호, pp. 68~78, 2017 년.

[3] 한경수외 2 인, “API 순차적 특징을 이용한 악성코드 변종 분류 기법,” 보안공학연구논문지, 제 8 월 제 2 호, 2011 년 4 월.

[4] 안랩, “안랩 트러스트와처, 메모리 분석 기반의 익스플로이트 탐지 기술 탑재,” 2014 년.

[5] Egele, Manuel, et al, “A survey on automated dynamic malware-analysis techniques and tools,” ACM computing surveys, Volume 44 Issue 2, Feb. 2012.