[별첨 5]

호스트 행위기반 악성코드 탐지기술

김익균 (ikkim21@etri.re.kr)
네트워크보안연구실

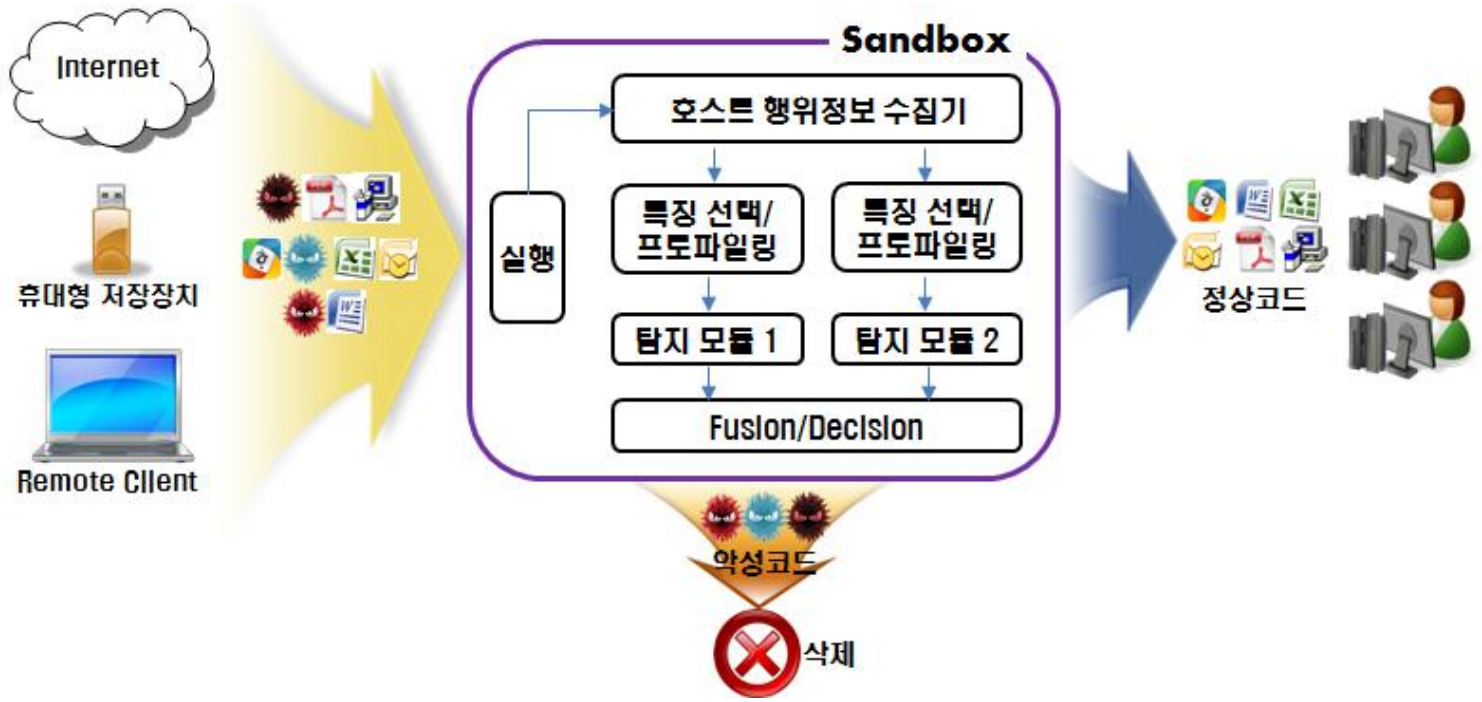
ETRI 한국전자통신연구원
www.etri.re.kr
SW콘텐츠연구소/사이버보안연구본부

목 차

▣호스트 프로세스 행위정보 수집 및 악성코드 탐지 기술

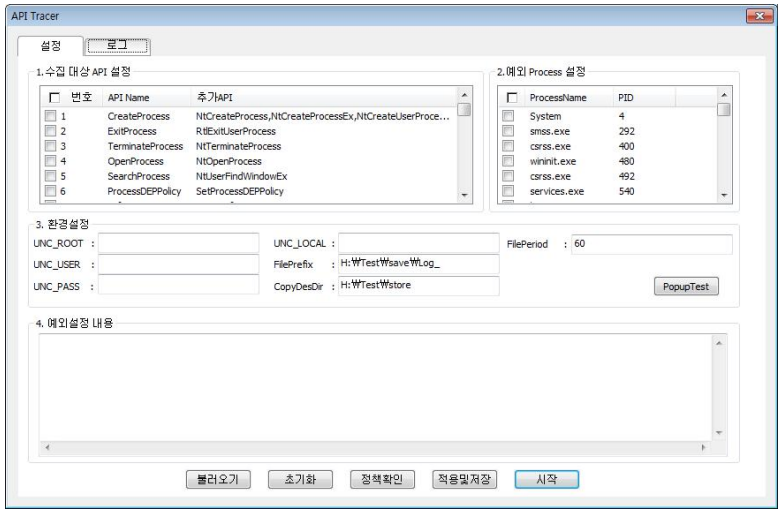
❖ Signature 기반 악성코드 탐지 기술의 한계를 극복하기 위해,

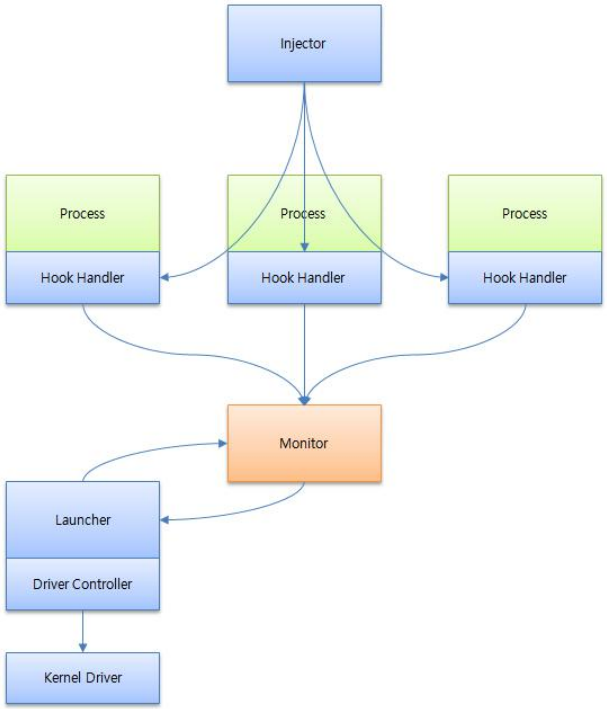
- 호스트에서 발생하는 다양한 행위 이벤트 정보를 수집하고
- 수집된 행위정보를 기계학습 및 데이터 마이닝 기술을 활용하여 신종 악성코드를 탐지하는 기술



▣ 호스트 프로세스 행위정보 수집 기술

- ❖ 호스트의 모든 프로세스의 행위정보를 API 후킹에 의해 실시간 수집
- ❖ 8개의 카테고리, 40종 이상의 특성인자 수집
- ❖ 예외 프로세스 처리 및 예외 수집 특성인자 선택적 수집 기능

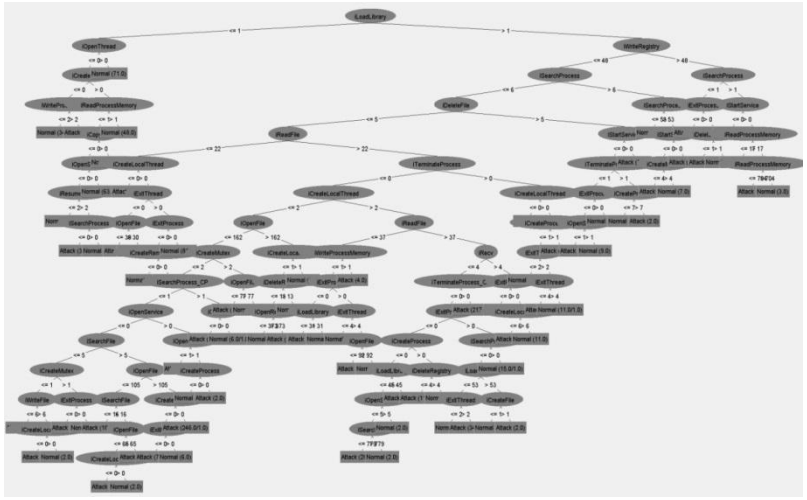


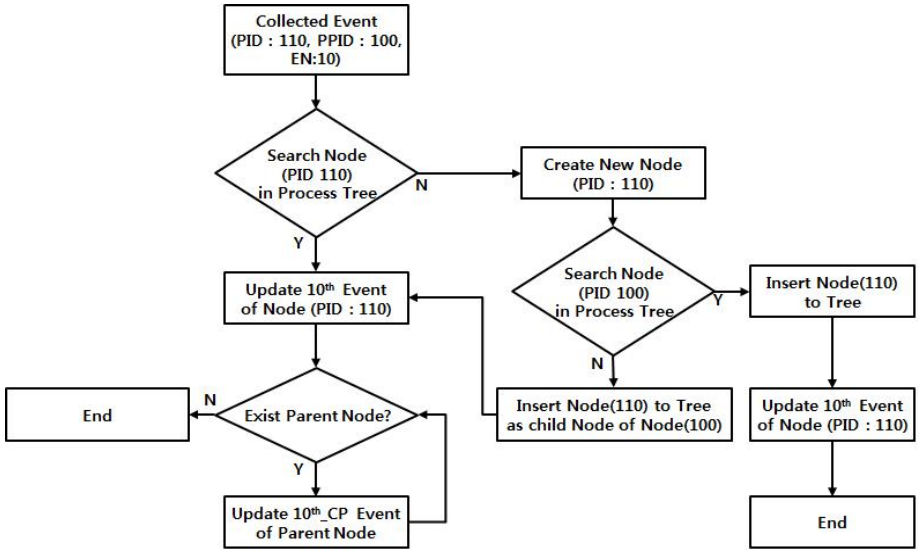


<수집기 구조>

▣ 호스트 행위기반 악성코드 분석 기술

- ❖ 프로세스 행위정보를 표현하는 특징벡터 생성
- ❖ 자식 프로세스의 행위정보 표현 기술
- ❖ 특징벡터를 이용한 결정트리 기반 악성코드 탐지 기술





▣ 기술이전 내용 및 범위

- 기술이전 내용
  - 호스트 프로세스 행위정보 수집 기술
  - 호스트 행위기반 악성코드 분석 기술

- 기술이전 범위
  - 소스코드: 호스트 프로세스 행위정보 수집 프로그램, 데이터 마이닝 기반 악성코드 탐지 프로그램
  - 문서: 시스템 설계서, 개발문서, 기술문서
  - 관련 특허

▣ 기술 개발 현황

❖ **기술성숙도**(TRL : Technology Readiness Level) **단계 : (5)단계**

구 분	단계	정 의	세 부 설 명
기초 연구 단계	1	기초 이론/실험	▫기초이론 정립 단계
	2	실용 목적의 아이디어 특허 등 개념정립	▫기술개발 개념 정립 및 아이디어에 대한 특허 출원 단계
실험 단계	3	실험실 규모의 기본성능 검증	▫실험실 환경에서 실험 또는 전산 시뮬레이션을 통해 기본성능이 검증될 수 있는 단계 ▫개발하려는 부품/시스템의 기본 설계도면을 확보하는 단계
	4	실험실 규모의 소재/부품/시스템 핵심성능 평가	▫시험샘플을 제작하여 핵심성능에 대한 평가가 완료된 단계 ▫3단계에서 도출된 다양한 결과 중에서 최적의 결과를 선택하려는 단계 ▫컴퓨터 모사가 가능한 경우 최적화를 완료하는 단계
시작품 단계	5	확정된 소재/부품/시스템 시작품 제작 및 성능 평가	▫확정된 소재/부품/시스템의 실험실 시작품 제작 및 성능 평가가 완료된 단계 ▫개발 대상의 생산을 고려하여 설계하나 실제 제작한 시작품 샘플은 1~수개 미만인 단계 ▫경제성을 고려하지 않고 기술의 핵심성능으로만 볼 때, 실제로 판매가 될 수 있는 정도로 목표 성능을 달성한 단계
	6	파일롯 규모 시작품 제작 및 성능 평가	▫파일롯 규모(복수 개~양산규모의 1/10정도)의 시작품 제작 및 평가가 완료된 단계 ▫파일롯 규모 생산품에 대해 생산량, 생산용량, 불량률 등 제시 ▫파일롯 생산을 위한 대규모 투자가 동반되는 단계 ▫생산기업이 수요기업 적용환경에 유사하게 자체 현장테스트를 실시하여 목표 성능을 만족시킨 단계 ▫성능 평가 결과에 대해 가능하면 공인인증 기관의 성적서 확보
실용화 단계	7	신뢰성평가 및 수요기업 평가	▫실제 환경에서 성능 검증이 이루어지는 단계 ▫부품 및 소재개발의 경우 수요업체에서 직접 파일롯 시작품을 현장 평가(성능 및 신뢰성 평가) ▫가능하면 인증기관의 신뢰성 평가 결과 제출
	8	시제품 인증 및 표준화	▫표준화 및 인허가 취득 단계
사업화	9	사업화	▫본격적인 양산 및 사업화 단계 ▫6-시그마 등 품질관리가 중요한 단계

▣ 호스트 프로세스 행위정보 수집 기술

- ❖ 악성코드 탐지를 위한 기존의 악성코드 행위정보 수집기술은 호스트 시스템에 기록되는 로그 정보를 활용하는 것이 대부분이었음
- ❖ 본 기술에서는 40종 이상의 특성인자를 정의하고, 호스트 프로세스가 실행되는 동안 호출하는 API를 후킹하여 수집함
- ❖ 본 기술은 호출되는 API의 발생여부 뿐만 아니라, API 호출 시 전달되는 파라미터 정보를 함께 수집하여 악성코드 여부를 판단할 때 활용할 수 있음

▣ 호스트 행위기반 악성코드 탐지 기술

- ❖ 기존의 악성파일 탐지기술은 시그니처 기반의 탐지 기술로 알려지지 않은 악성파일 탐지가 어려웠음
- ❖ 행위기반 악성코드 탐지기술 개발이 시도되었으나 탐지율이 저조하여 적용하기 어려운 상황임
- ❖ 본 기술은 악성코드가 실행되는 동안 발생하는 행위정보를 기반으로 데이터 마이닝 기술을 적용하여 악성여부를 판단함으로써 기존 이상탐지 방식에 비해 탐지 성능이 우수함
- ❖ 또한, 본 기술은 가상머신 환경에서 동작 가능하여, 악성코드의 감염을 사전에 방지할 수 있음

▣ 예상 응용제품 및 서비스

예상 제품/서비스	예상 수요자(층)
호스트 프로세스 행위정보 수집기	컴퓨터바이러스 백신 업체, 침입탐지 시스템 개발 업체, 네트워크 보안업체, SIEM 업체
호스트 행위기반 악성코드 동적 분석기	컴퓨터바이러스 백신 업체, 침입탐지 시스템 개발 업체, 네트워크 보안업체, SIEM 업체

▣ 기술이전 업체 조건

- ❖ **해당사항 없음**

▣ 사업화시 제약조건

- ❖ **해당사항 없음**

▣ 사업성

예상 제품 /서비스	예상단가 (천원)	이전기술의 비중(%)	잠재적/현재적 경쟁자와 가격,시장 등에서 경쟁상 유리한 점	판매 가능시기
호스트 행위기반 악성코드 탐지 솔루션	500 / 분석기	30%	a. 가격경쟁력면: 기존 외산제품에 비해 저렴하며 기능 요구사항에 따라 변동 가능 b. 시장환경면: 행위기반 악성코드 탐지 필요성 증대로 시장의 급속한 팽창 및 구매력 증가 c. 기타: 기능면에서 경쟁력 있음 (기존 시그너쳐 방식의 한계를 극복함)	2015

❖가격 경쟁력: 상용제품의 기능 요구사항에 따라 변동가능
❖상용화를 위한 생산설비 등 추가비용: S/W 이므로 생산 설비 등 추가비용 없음
❖상용화를 위한 추가적인 기술개발 내용: 해당 없음

▣ 국내외 시장 동향

- 사이버 공격, 데이터 절도, 멀웨어와 스팸웨어에 의한 공격 등 각종 위협이 엔드포인트 보안 시장 활성화를 촉진하고 있으며, 세계 엔드포인트 보안 시장은 2014년 5,030백만 달러에서 9.2%의 연평균 복합 성장률(CAGR)로 성장해 2019년에는 7,705백만 달러에 이를 전망
- Symantec이 엔드포인트 보안 시장에서 가장 큰 점유율을 차지한 가운데, McAfee(Intel), Trend Micro, Sophos, Kaspersky Lab 등이 주요 사업자로 자리해 있음
- 기업 시장은 상위 5위 사업자들의 점유율 총합이 65%로 하위 사업자들의 규모도 상당한 수준이지만, 개인 시장에서는 상위 5위 사업자의 점유율이 85%를 넘어설 정도로 압도적인 시장 장악력을 보유
- 국내외 시장규모

관련 제품 /서비스	시장	1차년도 (2015)	2차년도 (2016)	3차년도 (2017)	4차년도 (2018)	5차년도 (2019)	합계
호스트 행위기반 악성코드 탐지 솔루션	해외 (백만불)	5,495.5	5,979.0	6,473.4	7062.4	7705.1	32,715.5
	국내 (억원)	911	925.6	940.4	955.5	970.77	4,703.27

- 해외시장 규모 : IDC 보고서 "Worldwide Security and Vulnerability Management 2013–2017 Forecast and 2012 Vendor Shares"를 기반으로 관련 CAGR을 적용하여 2018~2019년도 시장규모를 추정함
- 국내 관련 시장규모 : Anti-Virus 매출 규모 기준, 2013 국내 정보보호산업 실태조사 (2013년도 국내 AV 관련 벤더 매출 규모 기준 보수적으로 시장규모 산정)

감사합니다.

www.etri.re.kr

♣ 연락처 : SW콘텐츠연구소/네트워크보안연구실 김익균 책·연 (042-860-5442, ikkyun21@etri.re.kr)