네트워크 전달 신종 악성파일 탐지 기술

Ⅰ. 제안기술 개요

-본 기술은 시그너쳐 기반 악성코드 탐지 기술의 한계를 극복하기 위해, 호스트에서 발생하는 다양한 행위 이벤트 정보를 수집하고, 수집된 행위정보를 데이터 마이닝 방법에 적용하여 악성코드를 탐지하는 기술에 관한 것임
-호스트에서 실행되는 프로세스들의 행위정보, 즉 API후킹을 통해 호출되는 API정보를 수집하며, 수집된 일련의 API 정보는 각 프로세스의 행위 프로파일을 표현할 수 있음
-행위 프로파일은 결정트리 등 데이터 마이닝 알고리즘을 통해 악성코드 여부를 판단할 수 있으며, 특히, Zero-day 악성코드와 같은 알려지지 않은 신종/변종 악성코드를 탐지할 수 있음

[해외동향]
-시그너쳐 기반 악성코드 탐지 방식 외에 샌드박스 방법과 함께 트래픽의 행위를 분석해 이상행위를 찾아내는 행위기반 분석기법, 기존 소프트웨어 평판을 기준으로 분석하는 평판기반 기법 등이 사용되고 있음. 행위정보를 이용하여 데이터 마이닝 기술에 의한 악성코드 탐지 기술개발 시도가 있으나, 상용화 수준은 아님

[국내동향]
-국내 역시 해외 현황과 매우 유사한 상태임

-다만, 행위정보를 이용한 데이터 마이닝 기술에 의한 악성코드 탐지 기술은 개발된 사례 없음

-바이러스 백신의 국내 시장은 국내 기업이 주도하고 있으나, 세계시장 점유율은 2% 이하임
-세계 컴퓨터 바이러스 백신의 선도 기업과 차별화된 기술력 확보를 통해 기술 경쟁력 확보 및 점유율 확대가 기대됨
-PC에서 발생하는 행위 데이터를 분석하기 위한 데이터 마이닝 기술의 확보는 보안로그 빅데이터를 분석하는 SIEM 시장으로 사업영역 확대가 기대됨
-컴퓨터바이러스 백신 : 제로데이 악성코드 탐지, 행위정보 수집, 비정상행위 탐지 모듈
-침입탐지 시스템 : 호스트 기반 침입탐지 모듈, 샌드박스 기반 탐지 모듈
-PC 보안 : 비정상 프로세스 탐지 모듈
-통합보안관제 : 호스트 기반 침입탐지 모듈
-SIEM : 호스트 기반 빅데이터 로그 분석 모듈

상용화단계	일반	①아이디어 ②연구단계 ③개발단계 ❹개발완료(시제품) ⑤제품화 단계
	의약바이오	①라이센싱 ②개발단계 ③제품화 단계
핵심키워드	한글	컴퓨터 바이러스 백신, 악성코드 탐지, 비정상 행위 탐지
	영문	Anti-Virus Engine, Malware Detection, Anomaly Detection

Ⅱ. 기술개발자 정보

기관명	한국전자통신연구원	**부 서**	네트워크보안연구실
성 명	문대성	**직 급**	선임연구원
전화/핸드폰	042-860-1083	**이메일**	daesung@etri.re.kr

Ⅲ. 수행과제정보

지원지관명		**연구사업명**	
연구과제명		**수행기간**	
주관기관	한국전자통신연구원	**공동연구기관**	-

Ⅳ. 특허정보

특허현황	**사업화대상기술 관련특허 총 3 건**				
상세현황	**구 분**	**상 태**	**출원(등록)일자**	**권리번호**	**특허명**
	대상기술	■출원□등록	2014.02.03	2014-0012280	수집된 이벤트 정보 기반 악성코드 탐지 장치 및 방법
	관련기술	■출원□등록	2015.01.22	14/603241	APPARATUS AND METHOD FOR DETECTING A MALICIOUS CODE BASED ON COLLECTING EVENT INFORMATION
	관련기술	■출원□등록	2015.02.11	2015-0020977	명령어 집합의 행위 패턴을 엔-그램 방식으로 모델링하는 방법, 그 방법으로 동작하는 컴퓨팅 장치, 및 그 방법을 컴퓨팅 장치에서 실행하도록 구성되는 기록 매체에 저장된 프로그램

1. 기술성 분석

1. 기술의 내용 및 특징

○ 본 기술은 호스트 PC에서 실행되는 프로세스의 API 호출 정보를 수집하는 행위 정보 수집 기술과, 수집된 대용량의 행위정보를 프로세스 별로 재구성하여 벡터형태로 표현하는 특성인자 명세화 기술, 마지막으로 악성행위 여부를 판별하는 악성행위 분석 기술로 구성됨

○ 본 기술과 관련하여 3건의 특허를 확보하고 있음. 대표특허로는 “수집된 이벤트 정보 기반 악성코드 탐지 장치 및 방법(특허 출원번호 : 2014-0012280)”가 있음

○ 대표특허는 악성행위 분석 기술은 수집된 데이터에 대해 각 특성인자의 발생빈도를 프로세스 ID 별로 재구성하여 실행파일이 호스트에서 실행되는 동안의 행위정보를 아래 그림과 같이 M-차원의 벡터로 표현하는 것을 포함하는 방법 및 장치임

900

		특성인자 명세화 ID										
프로세스 명	프로세스 ID	1	2	3	4	5	6	7	8	...	M-1	M
Explorer.exe	1664	1	5	0	0	0	0	0	1	0	0	0
iexplore.exe	3108	1	4	0	0	0	0	0	1	0	0	0
java.exe	3556	1	3	0	0	0	0	0	1	0	0	0
cmd.exe	3724	2	1	0	0	0	0	0	1	0	0	0
cmd.exe	3824	1	0	0	0	0	0	0	1	0	0	0
cscript.exe	3832	0	0	0	0	0	0	1	0	0	0	0

<특성인자 M-차원의 벡터>

○ 해당 프로세스의 행위 뿐만 아니라, 해당 프로세스의 자식 프로세스에서 발생하는 특성인자 이벤트의 발생빈도를 함께 표현하는 것을 포함하는 방법 및 장치임

○ 프로세스 별로 재구성된 M-차원의 벡터는 다양한 기계 학습(Machine Learning) 알고리즘의 입력으로 사용이 가능하여 악성행위 여부를 판단하는 것을 포함하는 방법 및 장치임

○ 호스트에서 실행되는 모든 프로세스를 아래 그림과 같이 트리형태로 표현 및 관리하는 것을 포함하는 방법 및 장치임

<특징벡터 트리 표현 모델>

○ 본 기술 관련 특허권의 청구범위는 다음과 같음

○ 본 기술과 관련된 보유특허 중에서 “수집된 이벤트 정보 기반 악성코드 탐지 장치 및 방법”의 대표 청구항 : “정의된 특성인자를 기반으로 컴퓨팅 장치에서 특성인자 이벤트의 정보를 수집하는 특성인자 수집 모듈과, 상기 수집된 특성인자 이벤트의 정보를 분석에서 사용 가능한 형태인 특성인자 명세화 데이터로 변환하는 특성인자 명세화 모듈과, 상기 명세화된 데이터를 이용하여 악성코드 여부를 분석하는 악성코드 판별 모듈을 포함하는 것을 특징으로 하는 악성코드 탐지 장치”

○ 수집부터 특징벡터 생성, 판별에 이르기 까지 모든 과정에 대하여 권리 범위에 포함됨. 특히, 프로세스 행위정보를 특징벡터의 형태로 표현하는 내용을 권리 범위에 광범위하게 포함하였음

○ 따라서, 수집기술과 악성코드 분류기술을 포함한 본 대상기술의 모든 구성요소를 보호할 수 있음

○ 본 기술과 관련된 보유 특허들은 대상기술의 핵심 구성요소인 프로세스 행위정보를 벡터형태로 표현하는 방법에 대해 권리를 주장하고 있어 유사기술로 회피할 수 없도록 구성하고 있음

2. 기술의 수준

○ 모방용이성(기술의 난이도)

- 본 기술은 경량화된 실시간 행위정보 수집 기술에서부터 이상행위 분석 기술까지 행위기반 악성코드 탐지를 위한 모든 과정을 포함하고 있어, 본 기술을 모방하여 유사 솔루션을 구현 및 제품화 하는 것은 어려운 상태임

- 학습과정에서 생성된 정상파일과 악성코드의 행위 모델은 수집된 데이터에 기반하기 때문에 리버스 엔지니어링 등의 방법으로 모방할 수 있는 것이 아님

○ 회피비용(회피설계비용)

- 프로세스의 행위 정보를 벡터형태로 표현하는 기술과 데이터 마이닝에 기반한 악성행위 판별 기술 등 핵심기술을 특허로 확보하고 있어, 유사기술을 이용한 상용화를 원천적으로 차단하고 있음

- 악성코드 분석, 데이터 마이닝, DB 등 다양한 분야 전문가들의 유기적인 협력이 필수적으로 요구되어 유사기술을 개발하는데 상당한 비용이 소요될 것으로 예상

- 유사기술의 설계뿐 만 아니라, 정상/악성 모델 생성을 위해 대용량의 정상/악성 행위정보를 수집해야 함. 행위 데이터 수집을 위해 소요되는 개발 기간의 비용이 요구됨

○ 대체기술 존재 여부

- 행위정보 수집 기술에서부터 이상행위 분석 기술까지 모든 과정을 포함하고 있는 행위기반 악성코드 탐지 기술은 없음

- 해외에서 행위정보를 기반으로 데이터 마이닝 기술에 의한 악성코드 탐지 기술개발이 시도가 있으나, 높은 오탐율로 상용화된 사례없음. 국내에서는 데이터 마이닝 기술에 의한 비정상 행위 탐지 기술 개발 사례 없음

- 본 대상 기술과 같이 상용화가 가능한 수준의 오탐율 성능을 보이는 기존 기술은 존재하지 않음

- n-gram 에 의한 행위정보 표현 기술이 논문 수준에서 일부 존재하고 있으나, 본 대상 기술과 같이 프로세스의 시작부터 종료 시점까지 발생되는 행위정보를 벡터형태로 표현하는 기술은 존재하지 않음

○ 경쟁자에게 미치는 영향

– 세계 바이러스 백신 시장은 AVAST, MS, ESET, Symantec 등 10개 미만 기업이 85%이상을 점유하고 있음

– 시장에서 절실히 요구되는 Zero-day 악성코드 탐지가 가능한 차별화된 기술을 제품에 적용하여 2% 이하인 국내 기업의 세계시장 점유율 향상이 기대됨

– 대체기술 및 유사기술 개발이 어려운 원천 기술을 확보하여, 세계 컴퓨터 바이러스 백신 분야의 기술적 우위를 확보할 수 있음

– 안티 바이러스 시장은 단말 위협 탐지/대응 기술로, 네트워크 보안 기술은 네트워크 기반 악성코드 샌드박스 분석 기술로, 보안관제 기술은 빅데이터 마이닝 기술을 이용해 차세대 SIEM 기술로 발전되며 사용자 행위 분석 기술까지 포괄하고 있기에 본 술은 사이버보안 전 분야에서 사용될 원천 기술로 활용이 가능함

○ 기술수명

– 개인정보 뿐만 아니라, 주요 정보시설을 겨냥한 사이버 공격이 심화되어 향후 이러한 공격의 지속적인 증가와 함께 더욱 큰 사회적 위험을 야기할 것으로 예상

– 주요 정보시설을 겨냥한 사이버 공격이 사이버 테러수준으로 심화되고 있고 불특정 대상 시스템을 이용하는 기존 공격과는 다르게 지능적이고 지속가능한 위협으로 전개되고 있음

<주요 사이버 사고 사례>

– 지능형 타겟 공격은 전 세계적으로 월 평균 80회 정도로 빈번히 발생하고 있고 단위사고의 피해규모로 볼 때 SONY사 개인정보 유출에 대한 피해액이 465억 달러로 천문학적인 침해비용이 발생됨

<지능형 타겟 공격의 증가와 피해규모>

- 향후 금융시스템(증권거래소), 산업시설 (화학, 원자력, 전략 발전소의 제어시스템) 등의 복합 시스템에 대한 공격이 예상되며 이러한 공격은 일시적인 혼란이 아닌 영구적 피해를 초래하고, 미국 9·11테러와 유사한 피해규모를 유발할 것으로 예상됨 (Gartner, Top predictions for IT Organizations and Users, 2011 and beyond : IT's growing transparency)

- 최근에 발생되는 사이버 공격은 기존의 개인적인 목표로 이루어진 공격들에 비하여 알려지지 않은 제로데이 공격을 적응적이고 지속적으로 진행하여 기존 방어기술로 대응하기에 한계가 있음

- 방화벽, 침임탐지 및 차단시스템과 같은 네트워크 경계 보안기술, 안티바이러스, 내부정보유출방지 기술, 이기종 보안 제품의 로그를 관리하는 통합 보안관리 분야의 기존의 기술로는 표적공격 방어가 불가능함

  ※ 기존의 알려진 탐지규칙을 이용하는 사이버 방어 기술과 보안제품으로는 표적공격에 대하여 20% 미만 정도의 수준으로 대응이 가능함 (NSS Lab, Fire eye)

- 기존의 보안 제품들이 활용하고 있는 패턴기반의 공격 제어 기법의 한계를 넘어서 내부 네트워크의 다양한 특성 인자들 (시스템 프로세스, 활동성, 네트워크 트랜잭션 등)의 관계성 분석을 통하여 알려지지 않은 새로운 공격을 탐지하는 기술 필요

- 불특정 취약 시스템을 이용하는 기존 공격과는 달리 주요정보 시스템을 겨냥한 사이버 표적공격은 장시간 수집된 다중 계층 데이터 분석을 통한 공격인지기술이 필요

항목	기존 보안 인프라	신규 요구되는 보안 인프라
위협유형	악성코드, DDoS, 알려진 취약점 침투	알려지지 않은 취약점을 이용한 장기적 계획의 표적공격
제어방법	시그니처 (규칙)기반 제어 (AV, Firewall, IPS)	누적 데이터 상관분석을 통한 활동 감시제어

- 기술이 발전함에 따라, 더욱 고도화된 사이버 공격 기술이 발생할 것으로 예상되기 때문에, 공격 대응 기술의 수요는 계속 증가할 뿐만 아니라 악성코드를 탐지하는 제품은 지속적으로 수익을 창출할 가능성이 높음

3. 기술의 필요성

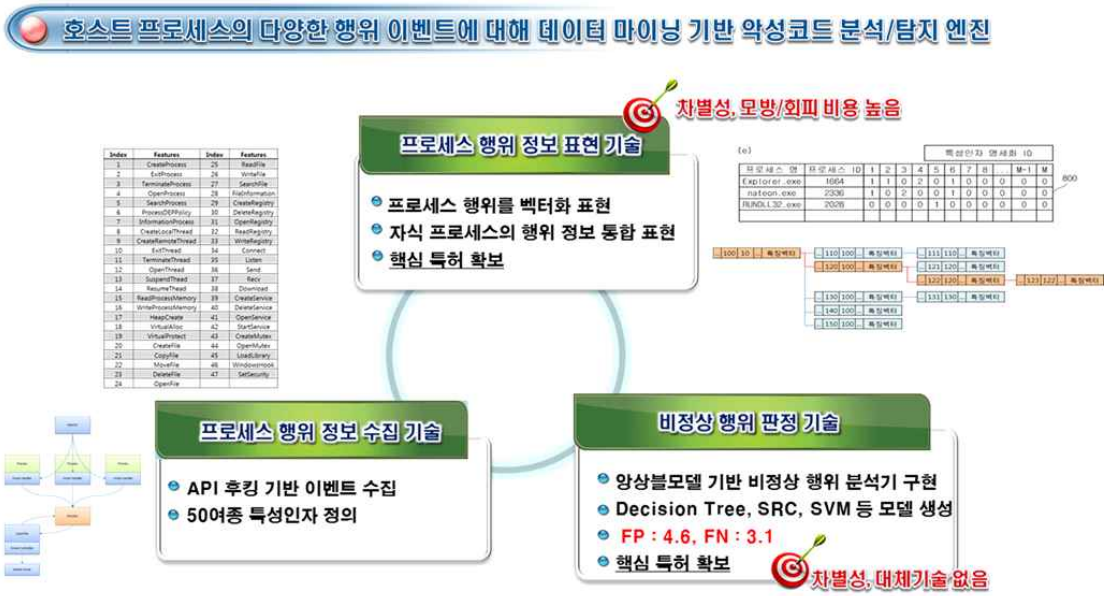
○ 혁신성

- 전통적으로 악성코드 탐지는 악성코드에서 특성 패턴을 데이터베이스화하여 비교하는 시그너처(Signature) 방식 탐지 기법이 주를 이루고 있음

- 이러한 시그너처 기반의 진단법은 악성 코드로 분류된 파일의 특정 부분 또는 고유한 부분을 검사의 대상으로 삼으므로 오탐(False Positive)과 미탐(False Negative)을 최소화하는 정확한 진단이 가능하다는 것과 파일 검사 시에 파일들의 특징적인 부분들만 비교함으로 빠른 스캐닝(Scanning)의 장점이 있음

- 그러나 이러한 시그너처 기반 진단법은 악성 코드의 파일 자체가 조금만 변경된 새로운 변형에 대해서는 대응을 할 수가 없고, 기존에 알려진 악성코드에 대해서만 대응을 할 수 있으므로 새로운 형태의 알려지지 않은 악성 코드에 대해서는 대응을 할 수 없다는 단점이 있음

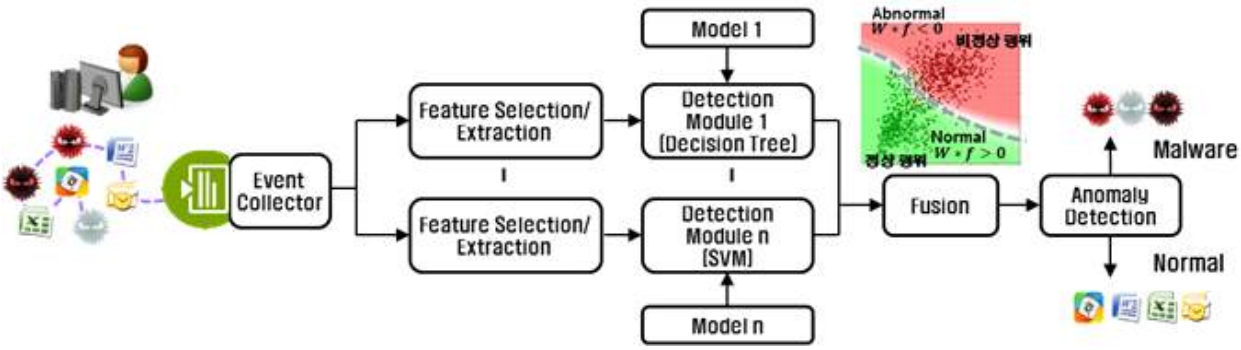
- 이러한 문제점을 해결하기 위해서, 최근 네트워크 트래픽, 호스트 로그정보 등 악성코드가 실행되는 동안에 발생되는 이벤트들을 종합적으로 분석해 악성코드를 탐지하는 비정상 행위 탐지(Anomaly Detection) 기술이 절실히 요구되고 있으나, 상용 제품에 적용되기 위한 필요조건인 높은 오탐율로 인하여 상용화 제품에 적용된 사례가 없음



<본 기술의 신종 악성코드 탐지기술 개념도>

- 네트워크 전달 신종 악성파일 탐지 기술(이하 SigFreeAV)은 기존 시그너쳐기반 악성코드 탐지 기술이 Zero-day 악성코드(신종/변종 악성코드)를 탐지하지 못하는 한계를 극복하기 위해, 호스트에서 발생하는 다양한 행위 이벤트 정보를 수집하고, 수집된 행위정보를 데이터 마이닝 방법에 적용하여 악성코드를 탐지하는 기술에 관한 것임

- 악성/정상 행위를 구분하기 위한 40종 이상의 호스트 행위정보를 정의하고 API 후킹을 통해 호스트에서 실행되는 프로세스의 행위정보를 실시간으로 수집함



<신종 악성코드 탐지기술 워크플로우>

- 수집된 프로세스 행위정보는 프로세스의 행위패턴을 표현할 수 있는 특징벡터로 재구성하고, 특징벡터를 데이터 마이닝 기술에 입력으로 사용하여 악성/정상 행위 분석모델 생성

– 실시간 행위 이벤트 수집 모듈과 비정상 행위 탐지 모듈이 통합된 호스트 이상행위 탐지 엔진 제공

– 악성코드 동적 분석을 위한 가상머신 환경에서 동작 가능한 비정상행위 탐지 엔진 제공

– 비정상 행위 탐지를 위해 빅데이터 처리, 데이터 마이닝 기술 등 다양한 분야 기술을 융합

– 본 기술은 기존 기술로 대응하기 힘든 알려지지 않은 악성코드를 탐지할 수 있는 차별성을 가지고 있으며, 특히 사업화에 초점을 맞추어 정상파일에 대한 오탐과 악성파일에 대한 미탐을 최소화하여 상용화제품에 적용될 수 있음

○ 파급성

– 본 기술은 컴퓨터 바이러스 백신과 같은 endpoint 보안 제품에서부터 SIEM 보안 로그분석 제품에 이르기까지 정보보안 모든 제품의 호스트 행위 분석 모듈로 적용될 수 있음

o 컴퓨터바이러스 백신 : 제로데이 악성코드 탐지, 행위정보 수집, 비정상행위 탐지 모듈

o 침입탐지 시스템 : 호스트 기반 침입탐지 모듈, 샌드박스 기반 탐지 모듈

o PC 보안 : 비정상 프로세스 탐지 모듈

o 통합보안관제 : 호스트 기반 침입탐지 모듈

o SIEM : 호스트 기반 빅데이터 로그 분석 모듈

– 대부분 외산 바이러스 탐지 엔진을 사용하여 기술의존도가 높은 국내 바이러스 백신 업체의 기술경쟁력 확보

○ 고객에게 미치는 영향

– 바이러스 백신의 국내 시장은 국내 기업이 주도하고 있으나, 국내 기업의 세계시장 점유율은 2% 이하임

– 기존 제품들의 문제점인 신종/변종 악성코드 탐지 기술의 확보를 통해 세계시장 점유율 향상이 기대됨

– 시그너처 기반 탐지 성능을 세계 최고 수준으로 높이기에는 한계가 있기 때문에, 세계 컴퓨터 바이러스 백신 기술의 한계점을 극복하여 기술력 향상 및 세계시장 점유율 확대 가능

- 안티 바이러스 시장은 비정상 행위 동적분석을 위한 단말 위협 탐지/대응 기술(ETDR : Endpoint threat Detection & Response)로 확대되고 있고, 네트워크 보안 기술은 네트워크 기반 악성코드 샌드박스 분석 기술 (Network-based malware sandbox)로 확대되며, 보안관제 기술은 빅데이터 마이닝 기술을 이용해 차세대 SIEM 기술로 발전되며 사용자 행위 분석 (UBA: User Behavior Analysis)까지 포괄하고 있기에 본 기술은 사이버보안 전 분야에서 사용될 원천 기술로 활용이 가능함

○ 연구개발 지원

- 2009년 공공부문 침해사고는 1만 659건으로 2008년 7,965건에 비해 25.3% 증가하였고 이 중 지방자치단체의 사이버 침해사고 발생건수는 4,398건으로 전체의 41%를 차지하여, 지속적인 지방자치단체의 침해사고 대응활동에도 불구하고, 공격 방법은 날로 발달되고 있음

<표 1> 공공분야 사이버 침해사고 발생현황 (단위: 건)

연도별	합계	국가기관	지방단체	산하기관	교육기관	기타
2008	7,965	1,187	3,067	1,490	1,867	354
2009	10,659	1,734	4,398	1,287	2,653	587

출처 : 국가 사이버안전센터 : 침해사고 현황 2010

- 최근 사이버 테러의 배후로 의심되는 북한은 3만여 명의 사이버공격 전문가를 보유하고 있으며 해킹과 사이버전 관련 교육이 집중적으로 이루어지고 있고 이를 통해 매년 100여명 정도의 최정예 사이버 공격 특수군이 양성되고 있고 현재 북한의 사이버 공격 수행능력은 미국 CIA 수준으로 평가됨

- 정부기관에 대한 사이버위협은 지능화·대형화되어 국가의 안전을 위협하고 있으며 이에 대한 대비책 마련이 지속적으로 제기됨에 따라, 범 정부차원에서 체계적·종합적 정책 추진을 통해 국가 전반의 정보보호 수준을 세계 선도국가 수준으로 향상시키고 새로운 공격 대응에 대한 기술개발이 국가적 위협에 대응할 수 있음

- 2011년 3·4 DDoS 공격 이후 국가적인 사이버위기에 대응하기 위해, 국가정보원, 행정안전부, 방송통신위원회, 경찰청, 금융결제원 등 유관기관이 합동으로 '국가 사이버안보 마스터플랜'(2011.8)을 마련하는 등 국가적인 대응이 필요한 사이버 공격에 대해 범정부적인 공조체제를 가동함으로써 제반 기술에 공헌

4. 기술의 차별성

○ 차별성

– 기존 기술에 대한 본 기술의 차별성은 다음과 같음

. 기존 시그니처 기반 악성코드 탐지 기술의 한계를 극복하여 Zero-day 악성코드 탐지가 가능함 (세계 5위권 Zero-day 악성코드 탐지 성능)

. 행위 기반 악성코드 탐지 기술의 문제점인 오탐율을 향상시켜 상용 서비스화 가능

. 특성인자 정의 및 API 후킹을 통한 대용량 행위 정보 수집 및 행위 모델 생성 기술

. 프로세스 행위 정보의 벡터화 및 앙상블 모델 기반 악성코드 분석 기술

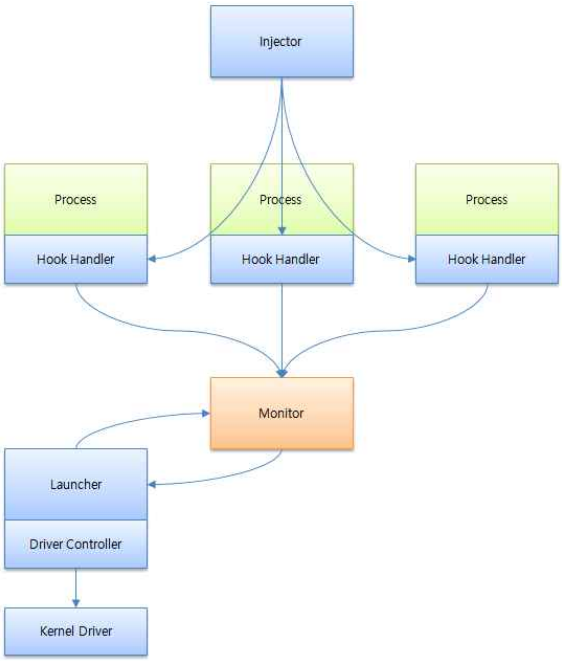
Index	Features	Index	Features
1	CreateProcess	25	ReadFile
2	ExitProcess	26	WriteFile
3	TerminateProcess	27	SearchFile
4	OpenProcess	28	FileInformation
5	SearchProcess	29	CreateRegistry
6	ProcessDEPPolicy	30	DeleteRegistry
7	InformationProcess	31	OpenRegistry
8	CreateLocalThread	32	ReadRegistry
9	CreateRemoteThread	33	WriteRegistry
10	ExitThread	34	Connect
11	TerminateThread	35	Listen
12	OpenThread	36	Send
13	SuspendThead	37	Recv
14	ResumeThead	38	Download
15	ReadProcessMemory	39	CreateService
16	WriteProcessMemory	40	DeleteService
17	HeapCreate	41	OpenService
18	VirtualAlloc	42	StartService
19	VirtualProtect	43	CreateMutex
20	CreateFile	44	OpenMutex
21	CopyFile	45	LoadLibrary
22	MoveFile	46	WindowsHook
23	DeleteFile	47	SetSecurity
24	OpenFile		

<호스트 행위 특성인자>

– 악성코드 탐지를 위한 기존의 악성코드 행위정보 수집기술은 호스트 시스템에 기록되는 로그 정보를 활용하는 것이 대부분이었음

– 본 기술은 호스트 PC에서 실행되는 프로세스의 API 호출 정보를 수집하는 행위정보 수집 기술과, 수집된 대용량의 행위정보를 프로세스 별로 재구성하여 악성행위 여부를 판별하는 악성행위 분석 기술로 구성됨

– 행위 정보 수집기술은 위 그림의 호스트 행위 특성인자와 같이 47종 이상의 행위를 특성인자로 정의한 후, 호스트 PC에서 실행되는 모든 프로세스의 행위정보를 아래 그림과 같이 API 후킹에 의해 실시간 수집



<호스트 행위 정보 API 후킹>

- 행위 정보 수집기술은 특성인자에 해당되는 API의 호출여부 뿐만 아니라, API 호출 시 전달되는 파라미터 정보를 함께 수집하여 악성코드 여부를 판단할 때 활용할 수 있음. 아래 그림의 호스트 행위 API 후킹 정보 사례는 수집된 API 호출 정보의 예를 보여줌

```
ID:9    DATE:2015-08-01 00:09:38
        EN:10 PPID:3352 PID:400 TID:2816
         UserID:SYSTEM ProcName:SearchProtocolHost.exe
         PathName:C:₩Windows₩system32₩SearchProtocolHost.exe
         EventName:ExitThread API:RtlExitUserThread
         Arg0 Name:ExitCode Type:0x1010 RawValue:0x0000000000000000 DataSize:0

ID:10   DATE:2015-08-01 00:09:38
        EN:51 PPID:3352 PID:400 TID:2816
         UserID:SYSTEM ProcName:SearchProtocolHost.exe
         PathName:C:₩Windows₩system32₩SearchProtocolHost.exe
         EventName:Unhook₩indowsHook API:Unhook₩indowsHookEx
         Arg0 Name:HookHandle Type:0x1010 RawValue:0x0000000000020088 DataSize:0
         Ext0 Name:Return Type:0x2010 RawValue:0x0000000000000001 DataSize:0

ID:11   DATE:2015-08-01 00:09:38
        EN:11 PPID:3352 PID:400 TID:2816
         UserID:SYSTEM ProcName:SearchProtocolHost.exe
         PathName:C:₩Windows₩system32₩SearchProtocolHost.exe
         EventName:TerminateThread API:NtTerminateThread
         Arg0 Name:ThreadHandle Type:0x1010 RawValue:0x0000000000000000 DataSize:0
         Arg1 Name:ExitStatus Type:0x1010 RawValue:0x0000000000000000 DataSize:0

ID:12   DATE:2015-08-01 00:09:38
        EN:62 PPID:3352 PID:400 TID:2060
         UserID:SYSTEM ProcName:SearchProtocolHost.exe
         PathName:C:₩Windows₩system32₩SearchProtocolHost.exe
         EventName:RegCloseKey API:RegCloseKey
         Arg0 Name:RegKey Type:0x1010 RawValue:0x0000000000000278 DataSize:0
         Ext0 Name:Return Type:0x2010 RawValue:0x0000000000000000 DataSize:0
```

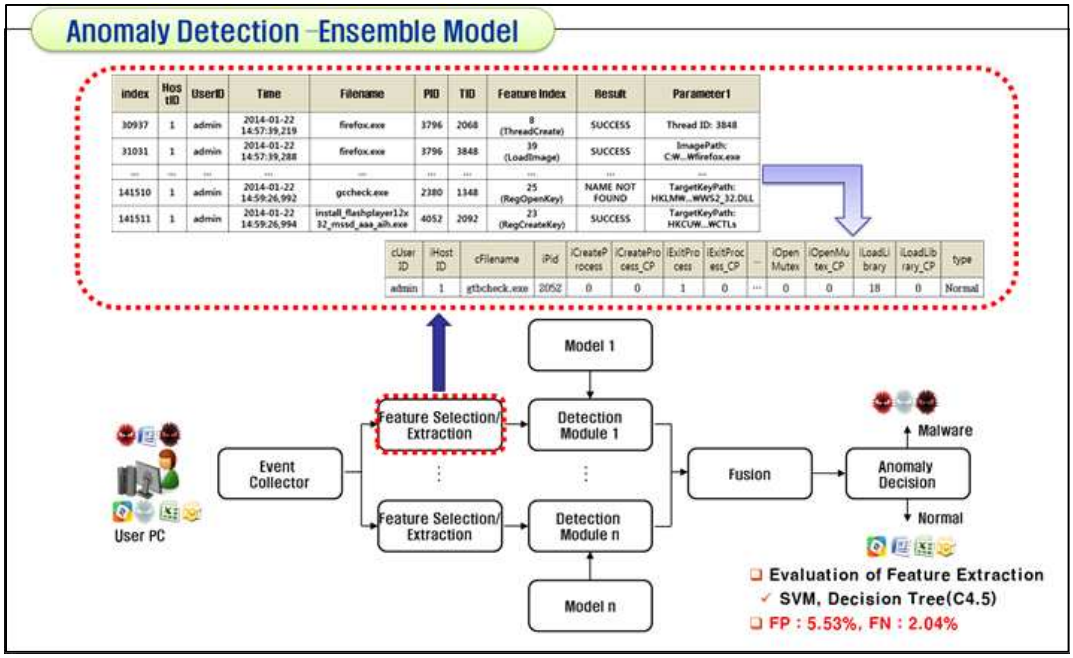
<호스트 행위 API 후킹 정보 사례>

- White 리스트를 설정하여 행위 정보를 수집하지 않는 예외 프로세스 처리 및 수집하지 않는 행위 정보 설정 가능

- 악성행위 분석 기술은 수집된 데이터에 대해 각 특성인자의 발생빈도를 프로세스 ID 별로 재구성하여 실행파일이 호스트에서 실행되는 동안의 행위정보를 94차원의 벡터로 표현

- 특히, 자식 프로세스에서 발생하는 특성인자 이벤트의 발생빈도를 포함함으로써 보다 정확한 행위정보의 표현이 가능

- 악성행위 분석 기술은 프로세스 별로 재구성된 94차원의 벡터는 다양한 기계 학습(Machine Learning)알고리즘의 입력으로 사용이 가능하며, 본 기술에서는 SVM, 결정트리, Sparse Coding 알고리즘을 분류기로 사용하는 앙상블 모델 기반 악성코드 탐지 기술임



<어노멀리 탐지의 앙상블 모델>

- 본 기술에 의한 악성코드 탐지 성능은 1차 시험결과 3.1%의 미탐율과 4.6%의 오탐율의 성능을 보이고 있고 기존 행위기반 악성코드 탐지의 문제점인 높은 오탐율 극복함
- 악성코드(3419개)와 정상파일(3194개)을 호스트 PC에서 실행시켜 수집된 행위 정보를 기반으로 악성코드 탐지 성능 시험

<탐지성능 서험 결과>

	개수	# of TP	# of FP	TP Rate	FP Rate	Precision	Recall
정상 파일	3194	3046	106	95.4 %	3.1 % (미탐율)	96.6 %	95.4 %
악성 코드	3419	3313	148	96.9 % (탐지율)	4.6 % (오탐율)	95.7 %	96.9 %

- 83개의 Zero-day 악성코드를 수집하여 VirusTotal(www.virustotal.com)을 통해 기존 컴퓨터 바이러스 백신 엔진의 성능 측정

- VirusTotal에서 제공하는 전체 54개의 컴퓨터 바이러스 백신 엔진의 평균 탐지율은 18.83%임

- 대표 12개 컴퓨터 바이러스 백신 엔진의 평균 진단율은 35.24%임. 특히, 국내 컴퓨터 바이러스 백신 엔진의 탐지율은 아주 낮음 (국외 제품 8개사 평균 : 46.84%, 국내 제품 4개사 평균 : 12.05%)

- 동일한 83개의 신규 악성코드에 대한 본 기술의 탐지 성능은 51.81%로 국내 기술보다 훨등히 높은 성능을 보였으며, 세계 5위의 탐지 성능을 보임

< Zero-day 악성코드 수집 및 탐지 실험 모델 >

< Zero-day 악성코드 수집 및 탐지 실험 모델 >

	국외 백신								국내 백신				SINBAPT-SigFree
탐지 개수	61	61	45	45	33	26	21	19	8	4	16	12	43
탐지율(%)	73.49	73.49	54.22	54.22	39.76	31.33	25.30	22.89	9.64	4.82	19.28	14.46	51.81

2. 특허성 분석

1. 국내외 특허 동향

○ 국내 동향

- 네트워크 전달 신종 악성파일 탐지 기술과 관련해서, (컴퓨터 and 바이러스 and 백신) or (악성코드 and 탐지) or (비정상 and 행위 and 탐지) 등의 키워드 검색식으로 검색한 결과를 살펴보면,
- 국내에서는, 한국인터넷진흥원이 65건, 한국전자통신연구원이 51건, 주식회사 안철수연구소가 15건, 주식회사 비즈모델라인이 9건, 한국정보보호진흥원이 8건, 주식회사 잉카인터넷이 8건 등의 순으로 많은 관련 특허출원을 한 것을 확인함
- 그 외 삼성전자주식회사 등 대기업의 특허출원도 확인함

○ 국외 동향

- 네트워크 전달 신종 악성파일 탐지 기술과 관련해서, ((Anti-Virus and Engine) or (Malware and Detection) or (Anomaly and Detection))등의 키워드 검색식으로 검색한 결과를 살펴보면,
- 국외에서는, International Business Machines Corporation이 237건, Microsoft Corporation이 205건, Symantec Corporation이 155건, Mcafee, Inc.가 108건, Kaspersky Lab ZAO가 50건, Raytheon Company가 49건 등의 순으로 많은 관련 특허출원을 한 것을 확인함
- 관련 분야를 양분하는 Symantec Corporation 및 Mcafee, Inc. 특허가 다수 존재하는 것을 확인했음
- 한편, 최근 모바일 환경에서의 네트워크 전달 신종 악종파일 탐지 기술과 관련해서는, MS 등의 출원이 다수 존재하는 것은 시장의 상황을 그대로 반영한 것으로 판단됨

2. 선행특허분석

특허번호	KR 10-2013-0068424	KR 10-2014-0011518	KR 10-2013-0030086	KR 10-2013-0005609
특 허 명	악성코드 경유-유포 주소지 탐지 시스템 및 그 방법	악성코드를 차단하기 위한 방법 및 시스템	비정상 세션 연결 종료 행위를 통한 분산 서비스 거부 공격 방어 방법 및 장치	모바일 악성코드 자동 수집 및 분석 시스템
출 원 인	한국인터넷진흥원	주식회사 시큐아이	한국전자통신연구원	(주) 세인트 시큐리티

기술요약	시스템 부하를 감소시킬 수 있는 악성코드 경유-유포 주소지 탐지 방법이 제공됨. 악성코드 경유-유포 주소지 탐지 방법은, 다수의 탐지 대상 주소지 정보(location address) 중 유효(valid) 주소지 정보를 추출하고, 유효 주소지 정보 중 무결성(integrity)이 변경된 주소지 정보를 추출하고, 무결성이 변경된 주소지 정보 중 인입 집중도가 K(여기서, K는 실수) 이상인 타겟 주소지 정보(target location address)를 추출하고, 타겟 주소지 정보를 대상으로 시그니쳐 탐지를 수행하는 것을 포함함	본원발명은 외부 네트워크로부터 내부 네트워크로 유입되는 파일에 관한 정보를 적어도 하나의 보안 장비를 활용하여 신속하게 수집할 수 있으며, 하나의 악성코드 관리 장비가 이와 같이 수집된 정보를 분석한 후, 그 결과를 시스템 내의 모든 보안 장비에 전송함으로써, 신속하게 악성코드를 탐지하고, 상기 탐지된 악성코드를 시스템 내의 모든 보안 장비에서 차단되게 하는 신속하고 일체화된 보안 서비스를 제공함	비정상 세션 연결 종료 행위를 통한 분산 서비스 거부 공격 방어 방법 및 장치가 개시됨. 분산 서비스 거부 공격 방어 장치는 수집한 패킷을 파싱하여 헤더 정보를 추출하고, 추출된 헤더 정보에 기초하여 미리 정의된 유형의 비정상 세션 연결 종료를 추적한 후, 비정상 세션 연결 종료 개수를 측정하는 세션 추적부 및 측정된 비정상 세션 연결 종료 개수를 미리 설정된 임계값과 비교하여 분산 서비스 거부(DDoS) 공격 여부를 판단하는 공격 탐지부를 포함하여, 분산 서비스 거부 공격에 대한 오탐율 및 탐지를 위한 연산량을 획기적으로 감소시킴	본 발명은 모바일 악성코드 자동 수집 및 분석 시스템에 관한 것임. 모바일 단말에 탑재되어 모바일 악성코드를 자동으로 탐지하는 모바일 악성코드 자동 수집 및 분석 시스템에 있어서, 네트워크 트래픽 분석을 통해 모바일 악성 의심코드를 수집하는 수집 모듈; 수집 모듈에 의해 수집된 모바일 악성 의심코드로부터 코드 정보 및 행위 정보를 추출하는 분석 모듈; 및 분석 모듈에 의해 추출된 코드 정보 및 행위 정보로부터 모바일 악성 의심코드가 악성코드인지 여부를 판단하여 모바일 악성코드를 탐지하는 탐지 모듈을 포함하여 구성됨
관련도 분석	A	A	A	A
	* 관련도 : X - 관련높음, Y - 관련있음, A - 관련은 없으나 참고할 자료 * X, Y - 주요참증에 해당, A - 참고참증에 해당			
조사결과	본 기술은 현재 특허출원된 3건으로 특허청의 심사를 대기하는 상태임. 관련 분야의 선행조사를 한 결과, 관련된 기술 분야의 특허들이 일부 검색됨. 하지만, 본 발명은 시그너쳐 기반 악성코드 탐지 기술의 한계를 극복하기 위해, 호스트에서 발생하는 다양한 행위 이벤트 정보를 수집하고, 수집된 행위정보를 데이터 마이닝 방법에 적용하여 악성코드를 탐지하는 기술에 관한 것으로, 구체적으로, 호스트에서 실행되는 프로세스들의 행위정보, 즉 API후킹을 통해 호출되는 API정보를 수집하며, 수집된 일련의 API 정보는 각 프로세스의 행위 프로파일을 표현할 수 있으며, 행위 프로파일은 결정트리 등 데이터 마이닝 알고리즘을 통해 악성코드 여부를 판단할 수 있으며, 특히, Zero-day 악성코드와 같은 알려지지 않은 신종/변종 악성코드를 탐지할 수 있는 기술이며, 이와 관련해서는, 유사한 특허문헌이 검색되지 않았음			

3. 사업성 및 시장성 분석

1. 사업화 제품화

○ 네트워크 전달 신종 악성파일 탐지 기술을 바탕으로 선도적이고 경쟁력 있는 제품 사업화 가능

○ 제품 경쟁성

- Smart Security(ESET), Endpoint Security(카스퍼스키랩), 엔드포인트 프로텍션 12(시만텍) 등의 외국 선도기업 제품들은 signature, 평판, 화이트리스트 등의 기술에 기반하고 있음

- 국외 주요 기업의 제품 및 서비스 현황

. 카스퍼스키랩의 제품은 악성 코드 차단 기능과 함께 PC의 모든 파일 활동을 모니터링하고, 방대한 화이트리스트 DB를 활용한 애플리케이션 제어 기능을 통합하여 '제로-데이' 공격에 대응

. 카스퍼스키랩 제품의 주요 기능으로는 각종 악성 코드 차단뿐만 아니라, △클라우드 기반 방역 △암호화 △애플리케이션 시작 제어 및 권한 제어 △매체 제어 △특정 웹사이트에 대한 접근 제한 △PC 취약점 체크 등이 있음

. 시만텍은 네트워크 접근제어, 애플리케이션 제어, 안티바이러스, 안티스파이웨어, 데스크톱 방화벽, 디바이스 제어와 같은 다양한 보안 기술들을 하나로 통합한 보안 솔루션 제공

. 시만텍의 평판 보안 기술인 '인사이트(Insight)' 및 행위기반 기술과 평판 보안 탐지 기술을 결합한 3세대 보안 엔진 '소나(SONAR)' 기술을 기반으로 물리 및 가상 환경에서 각종 최신 보안 위협을 탐지해 고객들의 소중한 정보와 인프라를 보호함

. AV-TEST에서도 멀웨어 차단 측면에서 업계 최고의 정확도를 기록했으며, 톨리 그룹(Tolly Group) 테스트에서도 99%의 멀웨어 위협을 오·탐지 없이 차단 또는 무력화하는 것으로 나타나는 등 뛰어난 보호 기능을 제공

. ESET 제품군은 루트킷 탐지에 특화된 안티스텔스, 평판 기반 분석 클라우드 시스템인 ESET Live Grid 기능 등 강력한 성능을 제공. 또한, 안티피싱, 방화벽, 안티스팸, 익스플로잇 블로커, 향상된 메모리 스캐너, 네트워크 취약점 보호, 장치 제어 등 다양한 보안 기능 제공

. ESET 제품군의 특징은 이러한 모든 기능이 동작하면서도 낮은 시스템 리소스 점유율로 시스템 성능 저하를 최소화

< 국외 관련 제품 및 서비스 동향 >

업체명	제품명	제품 특징
ESET	Smart Security	평판 기반 분석 클라우드 시스템
카스퍼스키랩	Endpoint Security	암호화, 클라우드 기반, 화이트리스트
시만텍	엔드포인트 프로텍션 12	행위기반 기술과 평판 보안 탐지 기술

< 국내 관련 제품 및 서비스 동향 >

제품 현황 / 주요 특징	V3	바이로봇
동작 형태	클라우드, PC 기반	PC 기반
판매 형태	무료/상용	무료/상용
분석 가능 파일 포맷	EXE, Javascript, 문서	EXE, 문서
부가 기능	악성 의심 웹사이트 차단	악성 봇 탐지, 데이터 유출 방지

- 국내 주요 기업의 제품 및 서비스 현황

. 국내에서는 Endpoint 보안제품, 특히 악성코드 탐지관련 제품은 안랩, 이스트소프트, 잉카인터넷, 하우리, SGA가 있음. 세인트 시큐리티가 SIMBA-HV라는 제품에서 파일 재구성 기능을 제공하는 것으로 발표

. 안랩만이 독자 기술을 보유하고 있으며, 나머지 업체에서는 세계적으로 유명한 비트디펜더 엔진을 활용하고 있음

. 안랩의 V3는 글로벌 백신 테스트인 VB100 이외에도 AV-TEST, AV-Comparatives, Checkmark, ICSA 등 해외 주요인증을 획득했으며, 테스트 및 인증을 외산 엔진이 아닌 순수 자체 기술로 통과함으로써 기술력 종속 없는 안정적인 서비스와 대응이 가능

. 이스트소프트의 알약은 비트디펜더, 소포스 엔진과 알약 자체개발 엔진인 테라까지 얹은 '트리플 엔진'을 적용하여, 탐지력을 높음

. 잉카인터넷의 nProtect Anti-Virus/Spyware는 독자적인 타키온 엔진과 비트디펜더 엔진의 강력한 듀얼 엔진 매커니즘을 적용하여 신속하고 정확한 멀웨어 탐지 기술을 구현

. SGA의 바이러스 체이서는 악성코드가 특정 목적을 수행하는 과정 중, PC 내에서 발생하는 여러 악성 행위의 특징을 분류 기준으로 악성코드를 탐지하고 차단하기 때문에 신·변종 악성코드를 통한 보안위협을 차단하는데 효과적임

- 이상에서와 같이, 국내외 선도 기업들에서는 signature, 평판, 화이트리스트 등의 기술에 기반한 제품을 출시하고 있으며, 행위 기반 악성코드 탐지는 일부 제품에서 도입하고 있으나, 행위 룰 수준 임

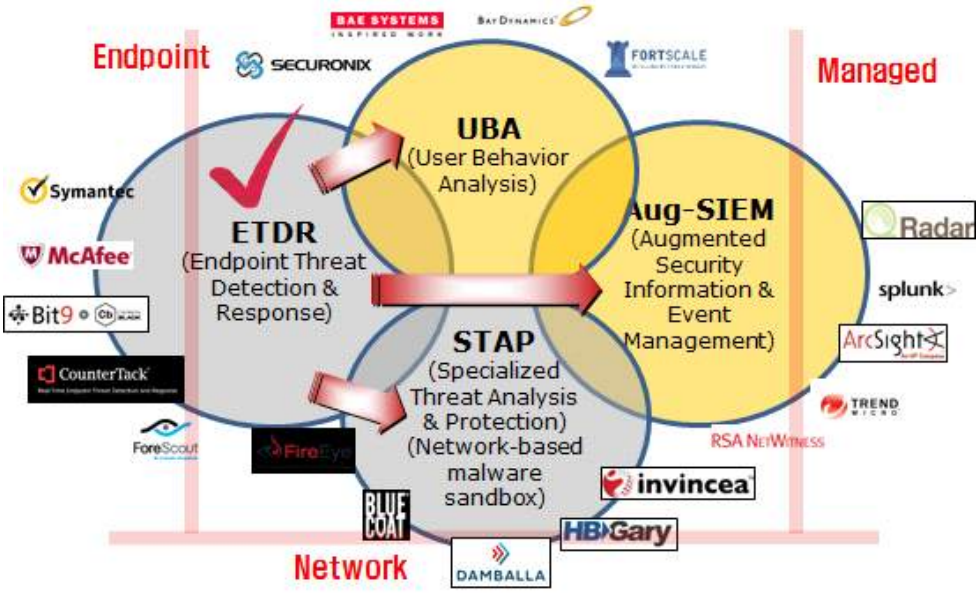
- 아래의 그림과 같이 기존 Signature, 평판 등의 기술에 본 대상기술인 행위기반 비정상행위 탐지 기술을 접목한다면, 기술 경쟁력이 확보되어 차별화된 제품 및 서비스를 제공할 수 있을 것으로 기대됨. 나아가 컴퓨터 바이러스 백신 시장의 점유율이 확대될 것임

< 경쟁력 강화 제품 출시 >

2. 사업화 방법 및 성공요인

○ 사업화 실현 가능성

- 본 대상기술이 기술이전되어 사업화가 가능한 제품 및 서비스는 다음과 같음
  . 컴퓨터바이러스 백신, 침입탐지 시스템(IDS, IPS, Firewall), PC 및 서버 보안, 통합보안관제, SIEM 제품 등



< 사업화 가능성 및 추진 방향, 출처: Gartner and IDC 2014 >

- 국내 컴퓨터 바이러스 백신 업체가 본 대상기술은 활용하여 기존 제품과 차별화된 제품 및 서비스를 출시한다면 단말 위협 탐지/대응 분야의 경쟁력있는 제품을 출시 할 수 있음

- 이와 더불어 네트워크 보안 분야에서도 네트워크 기반 샌드박스와 같은 기술을 접목하여 기존의 IPS나 FW과 차별화된 시장 공략이 가능함

- 특히, 보안관제 기술은 단순 로그관리 외에도 통합모니터링/접속 관리 등 다양한 범위로 확장되어 보안/운용/어플리케이션분석을 제공하는 보안플랫폼으로서 발전하고 있어 예상되는 관련 시장은 급속도로 증가될 것으로 예상되고, 차세대 SIEM 시장으로 발전하기에 사용자 행위 분석에 주요 핵심기술로 활용이 가능

- 또한, 사용자 행위 분석 (UBA) 분야는 정보보호 제품을 넘어 FDS (Fraud Detection System)으로 대표되는 금융 이상거래 탐지 분야의 새로운 요구사항을 만족시킬 수 있음

3. 국내외 시장전망

1) 국내외 시장 규모 및 동향

○ 시장규모

- 관련 산업 및 소비자 엔드포인트 수가 증가하면서 시장에서 엔드포인트 보안 솔루션 및 서비스가 빠른 속도로 도입되고 있음

- 또한 사이버 공격, 데이터 절도, 멀웨어와 스팸웨어에 의한 공격 등 각종 위협이 엔드포인트 보안 시장 활성화를 촉진하고 있음

- IDC 보고서 “Worldwide Endpoint Security 2014-2018 Forecast and 2013 Vendor Shares”에 따르면, 세계 엔드포인트 보안 시장은 2013년 8,783.50백만 달러(약 10조 2천억원)에서 5.1%의 연평균 복합 성장률(CAGR)로 성장해 2018년에는 11,286.3백만 달러에 이를 것으로 전망

- 기업용 엔드포인트 보안 솔루션의 세계시장은 상위 5개 기업들의 점유율 총합이 60%로 하위 기업들의 규모도 상당한 수준이지만, 개인용 엔드포인트 보안 시장에서는 상위 5위 기업의 점유율이 약 80%로 압도적인 시장 장악력을 보유

< 세계 엔드포인트 보안 시장 규모 및 추정치, 2010-2018 ($M) >

	2012	2013	2014	2015	2016	2017	2018	2013 - 2018 CAGR (%)
Corporate	3,797.2	3,980.0	4,215.5	4,483.3	4,768.9	5,071.2	5,399.3	6.3
Consumer	4,691.9	4,803.6	4,982.3	5,197.9	5,427.6	5,655.9	5,887.0	4.2
Total	8,489.0	8,783.5	9,197.8	9,681.2	10,196.4	10,727.0	11,286.3	5.1

< 2013년도 개인용 엔드포인트 보안시장 규모, 상위 10개, 2013 >

	Revenue ($M)	Share (%)
Symantec	2,034.20	42.3
McAfee (an Intel company)	692.6	14.4
Kaspersky Lab	422.1	8.8
Trend Micro	403.2	8.4
AVG Technologies	237.8	5
ESET	165.5	3.4
Panda Security	95.8	2
Webroot	91.9	1.9
Avast Software	65.9	1.4
F-Secure	63.1	1.3
Other	531.4	11.1
Total	4,803.60	100

< 2013년도 기업용 엔드포인트 보안시장 규모, 상위 10개, 2013 >

	Revenue ($M)	Share (%)
Symantec	732.6	18.4
McAfee (an Intel company)	676.9	17
Trend Micro	452.7	11.4
Sophos	311.1	7.8
Kaspersky Lab	244.9	6.2
ESET	226.6	5.7
IBM	189.8	4.8
F-Secure	110.4	2.8
Microsoft	76.5	1.9
Check Point	73.1	1.8
Other	885.2	22.3
Total	3,980.00	100

- 지식정보보안산업협회(KISIA)에서 발표한 “2013 국내 정보보호산업 실태조사” 국내 정보보안 시장은 네트워크보안(477,818백만원), 콘텐츠/정보유출 방지보안(280,369백만원) 분야의 매출 비중이 높으며, 교육/훈련 서비스(53.4%), 유지 보수 서비스(7.7%), 보안관제 서비스(7.3%) 분야의 성장률이 높은 것으로 조사됨

구분		2012년	2013년(E)	성장률(%)
정보보안 제품	네트워크 보안	466,979	477,818	2.3
	시스템 보안	168,381	170,139	1.0
	콘텐츠/정보유출 방지보안	275,817	280,369	1.7
	암호/인증	112,584	113,604	0.9
	보안관리	117,941	119,653	1.5
	기타 제품	109,012	109,716	0.6
	소계	**1,250,714**	**1,271,299**	**1.6**
정보보안 서비스	보안컨설팅	78,053	80,351	2.9
	유지보수	71,400	76,891	7.7
	보안관제	132,424	142,105	7.3
	교육/훈련	277	425	53.4
	인증 서비스	44,720	45,690	2.2
	소계	**326,873**	**345,462**	**5.7**
합계		**1,577,587**	**1,616,761**	**2.5**

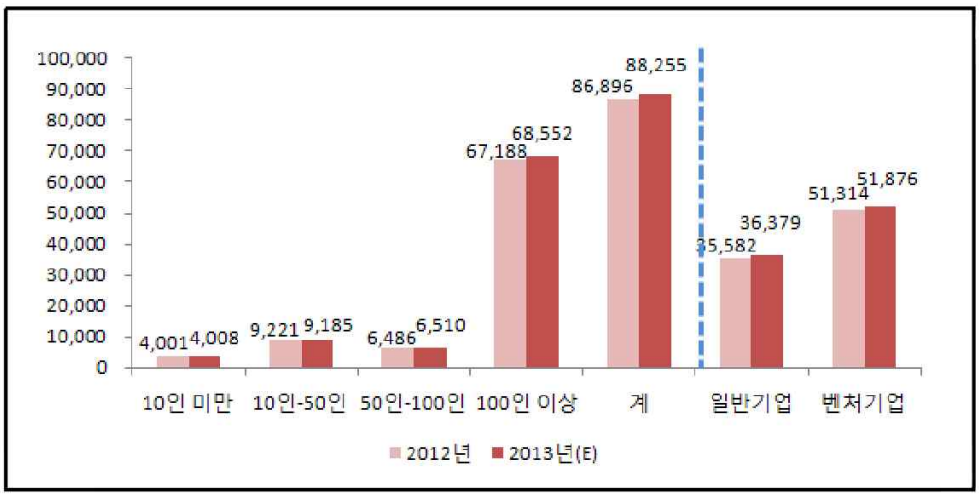
< 정보보안산업 전분야 매출 현황 (단위 : 백만원) >
출처 : 2013 국내 정보보호산업 실태조사, KISIA

분류		세부항목매출	2012년	2013년(E)	증감률(%)
정보보안 제품	네트워크 보안	웹 방화벽	48,244	49,139	1.9
		네트워크(시스템) 방화벽	77,595	77,728	0.2
		침입방지시스템(IPS)	84,939	85,237	0.4
		DDoS차단시스템	35,199	35,261	0.2
		통합보안시스템(UTM)	75,048	75,318	0.4
		가상사설망(VPN)	53,397	55,808	4.5
		네트워크접근제어(NAC)	42,964	43,678	1.7
		무선네트워크보안	22,248	24,661	10.8
		모바일 보안	16,782	19,582	16.7
		가상화(망분리)	10,564	11,406	8.0
		소계	**466,979**	**477,818**	**2.3**
	시스템 보안	PC방화벽	11,443	11,022	-3.7
		Virus백신	86,896	88,255	1.6
		Anti스파이웨어	18,164	18,414	1.4
		Anti피싱	3,819	4,119	7.9
		스팸차단S/W	16,278	14,860	-8.7
		보안운영체제	31,782	33,469	5.3
		소계	**168,381**	**170,139**	**1.0**

< 네트워크 및 시스템 보안 매출 현황 (단위 : 백만원)>
출처 : 2013 국내 정보보호산업 실태조사, KISIA

- 본 대상기술은 정보보안 제품중에서 네트워크보안과 시스템보안 시장 등 정보보안 산업의 핵심분야에 적용이 가능한 기술임

- 국내 엔드포인트 시장 중에서 Virus 백신의 시장 규모는 2013년에 882억원이었으며, 2018년에는 955억원(연평균 성장률 1.6%)이 예상됨. Virus 백신은 종사자가 10인 이상 50인 미만인 기업의 매출이 9,185백만원이며, 100인 이상인 기업의 매출이 68,552백만원으로 Virus 백신은 종사자가 100인 이상인 기업에서 주로 판매되는 것으로 나타남



< Virus 백신 매출 현황 (단위 : 백만원) >
출처 : 2013 국내 정보보호산업 실태조사, KISIA

< 국내 Anit-Virus 시장 규모 및 추정치, 2012-2018 (억원) >

	2012	2013	2014	2015	2016	2017	2018	2012 - 2013 CAGR (%)
국내 Anti-Virus 시장 규모 및 전망	868.9	882.5	896.6	911.0	925.5	940.4	955.4	1.6

* 국내 관련 시장규모 : Anti-Virus 매출 규모 기준, 2013 국내 정보보호산업 실태조사 (2012-2013 CAGR로 추정)

○ 시장수요

- 2014년도 IDC 보고서에 따르면, 사이버 공격이 더욱 고도화, 지능화됨에 따라 방어 시스템 또한 성능향상이 필요하고 언급하고 있음. 특히, 중요 정보 및 자산을 보유하고 있는 기관(금융 산업, 중요 인프라, 소매, 정부)들은 자신의 자산을 보호하기 위해 엔드포인트 보안 제품과 같은 정보보호 분야에 더 많은 지출을 권고하고 있음

- 정보보안산업의 2012년도 업종별(수요처별) 총 매출 현황을 살펴보면, 전체 제품 및 서비스에 대해 서비스/교육/통신업종이 28.1%의 가장 많은 매출 비중을 차지하고 있다. 다음으로, 제조업종 24.9%, 금융업종 24.5%, 공공부문 22.5%의 매출 비중을 차지하는 것으로 조사됨

- 정보보안 제품 분야의 업종별 매출비중은 서비스/교육/통신업종을 대상으로 27.9%의 가장 높은 매출 비중을 보였고, 다음으로 금융업종 25.3%, 제조업종 25.1%, 공공부문 21.7% 순으로 나타났음. 정보보안 서비스의 업종별 매출비중에서는 서비스/교육/통신업종을 대상으로 가장 많은 28.7%의 매출 비중을 보였으며, 공공부문 25.7%, 제조업종 24.2%, 금융업종 21.4%로 각각 조사됨

< 정보보안산업 업종별(수요처별) 매출 현황 (단위 : %) >

구분	업종(수요처)				
	공공	금융	제조	서비스	합계
정보보안 제품	21.7	25.3	25.1	27.9	100.0
정보보안 서비스	25.7	21.4	24.2	28.7	100.0

< Virus 백신 업종별 매출 비중 (단위 : %) >

구분	공공	금융	제조	서비스	합계
비중	16.0	18.2	20.5	45.3	100.0

- Virus 백신은 서비스업종 매출이 45.3%, 제조업종 매출이 20.5%로 주로 서비스 업종의 수요가 높은 제품으로 나타남

- 정보보안 제품 및 서비스의 수요는 금융 산업 뿐 아니라, 국방, 전력 등의 공공 분야의 수요가 더욱 확대될 것으로 예상됨

○ 산업특성

- 신규 보안 위협 및 악성코드 증가에 따른 보안 위협 대중화로 정보보안 인프라 구축 및 관리, 기업 및 개인 데이터 보호, 보안 전문가 양성 등이 핵심 과제로 부상하고 있음

- 소프트웨어정책연구소에서 발표한 “2015년 SW산업 10대 이슈 전망“ 보고서에 따르면 2015년 SW산업 10대 이슈 중에서 보안위협 증가에 따른 보안 수요 확대를 최고 이슈로 선정하는 등 정보보안 시장이 확대될 것으로 예상

- 미래창조과학부에서 2015년에 발표한 K-ICT 전략에 따르면, 정보보안 산업이 9대 전략산업으로 선정되어, 정보보호 서비스 제값받기, 사이버안전 대진단, IoT 보안 등 보안 신시장 창출을 위해 노력하고 있음

- 모든 사물과 사람이 인터넷과 네트워크로 연결됨에 따라 개인을 대상으로 하는 해킹은 홈·가전기기 해킹을 통한 개인정보 탈취에서부터, 스마트카 악성코드 감염으로 인한 오동작 유발 등 개인정보 탈취 뿐만 아니라 안전을 위협하는 수준으로 진화

- 또한, 산업계에서는 기업의 주요 기술의 유출을 방지하기 위해 총력을 기울이고 있어, 정보보호 예산이 폭발적으로 확대되고 있음

- 최근 사이버위협은 지능화·은밀화되고 있으며 막대한 경제적 피해와 국가·사회적인 혼란을 유발하는 등 국민생명과 국가안보에 직결되고 있음

- 정부·공공기관 및 중요 인프라를 대상으로 표적공격이 이뤄지는 등 사이버보안이 국가 위기관리의 가장 중요한 과제로 부각됨

- 따라서, 본 기술과 관련된 정보보안 분야의 산업은 높은 성장세를 보일 것으로 전망될 뿐만 아니라 공공 안전을 담보하는 사회 복지의 특성이 있음

○ 산업성장성

- 에너지관련 기업과 같이 공공인프라 산업에서부터, RSA와 같은 세계적인 보안회사에 이르기까지 기업의 주요 정보 유출 심각

· 2011년 쉘, 엑슨모빌, BP, 마라톤오일, 코노코필립스, 베이커 휴즈 등 미국의 글로벌 에너지기업 5곳 공격으로 가스와 석유분야의 생산시스템, 석유탐사 관련 제정문서, 산업 통제시스템의 정보유출 (Night Dragon)

· 2011년 암호전문 보안기업인 미국 RSA의 정보보안 사업부 공격으로 RSA의 OTP제품인 시큐어 ID의 기밀정보 유출

· 방위산업 업체인 록히드 마틴(Lockheed Martin)을 공격한 사건을 분석 중에 국내 통신업체를 포함한 총 760여개의 세계적으로 유명한 기업들을 대상으로 공격이 진행됨을 확인

· 2011년 7월 네이트의 DB에 저장된 3,500만명의 개인정보 유출. 해킹 그룹이 내부 개발자의 PC를 장기간 집중 공격한 내부자 활용 공격 사례

– 지능화되는 사이버 공격으로부터 산업계 뿐 만 아니라 개인 및 공공 인프라의 주요정보를 보호하는 기술적인 대응책 마련이 절실히 요구되고 있기 때문에, 엔드포인트 시장을 포함하는 정보보안 시장을 폭발적인 성장이 예상됨

– 엔드포인트 시장에 관한 2014년도 IDC 보고서에 따르면 엔드포인트 보안 시장의 연평균 복합 성장률(CAGR)은 5.1%를 보여 지속적인 시장 확대가 전망됨

– 엔드포인트 보안 시장은 엔드 유저의 SW 설치를 통해 제공되는 가장 기본적인 솔루션으로서, 최근 멀웨어(malware: 악성 소프트웨어) 위협의 증가와 부분유료화(freemium) 모델의 등장, 모바일 보안 필요성 등에 힘입어 여전히 꾸준한 성장세를 보임

– 2013년도에 발표된 국내 정보보호산업 실태조사에 따르면, Anti-Virus 매출 규모 기준으로 국내 컴퓨터 바이러스 백신 시장의 평균 시장성장률은 1.6%임

○ 경기변동의 특성

– 정보보안 시장의 경우, 정보유출 및 공격을 받을 경우 해당 기업의 이미지 하락으로 인한 경제적 손실이 막대하여, 경기에 민감하지 않음

2) 시장의 구조, 경쟁강도 및 진입장벽

○ 시장구조

– 세계 엔드포인트 시장에서 여전히 Symantec과 McAfee가 양두 체제를 구축하고 있으며, 그 뒤를 Trend Micro, Sophos, Kaspersky Lab, ESET 등이 잇고 있음. 특히, ESET와 AVG Technologies의 경우 2013년도 매출이 전년도 대비 20%이상의 높은 성장률을 보임

- 엔드포인트 보안시장에서 매출기준으로 유일하게 20위권에 랭크되어 있는 안랩의 경우 2013년 매출액이 23.4 M$로 전년도 보다 19.4%의 성장을 보였으나, 세계시장 점유율이 0.3%로 아주 미미한 수준임

- 비정상 행위 탐지 기술 확보 및 기존 기술보다 뛰어난 시그너쳐 기반 기술 확보 없이는 경쟁자 출연 가능성이 낮음

- 엔드포인트 보안시장 중에서 컴퓨터 바이러스 백신 시장의 경우로 한정할 경우에도 여전히 Symantec이 가장 높은 점유율을 가지고 있으며, ESET, Trend Micro와 같은 백신 전문 기업의 점유율이 높음

< 세계 엔드포인트 보안 시장 규모, 2012-2013 ($M) >

	2012	2013	2013 Share (%)	2012 - 2013 Growth (%)
Symantec	2,784.00	2,766.80	31.5	-0.6
McAfee (an Intel company)	1,287.30	1,369.60	15.6	6.4
Trend Micro	826.2	855.9	9.7	3.6
Kaspersky Lab	628.6	667	7.6	6.1
ESET	320.1	392.1	4.5	22.5
Sophos	310.5	311.1	3.5	0.2
AVG Technologies	196.6	250.6	2.9	27.5
IBM	179.7	189.8	2.2	5.6
F-Secure	171.2	173.5	2	1.3
Panda Security	144	146.6	1.7	1.8
Webroot	123	124.6	1.4	1.3
Check Point	89.3	88.6	1	-0.8
Bit Defender	98.6	88.5	1	-10.3
Avast	73.5	83.9	1	14.1
Microsoft	70.5	76.5	0.9	8.5
Lumension Security	66.1	71.4	0.8	8
Bit9	25.3	42.3	0.5	67.3
LANDESK	28.3	28.3	0.3	-0.1
Dr. Web	32.4	27.2	0.3	-15.9
Hitachi	28.6	25.5	0.3	-10.9
AhnLab Inc.	19.6	23.4	0.3	19.4
Other	985.5	980.1	11.2	-0.6
Total	8,489.00	8,783.50	100	3.5

출처 : IDC 보고서 “Worldwide Endpoint Security 2014-2018 Forecast and 2013 Vendor Shares”

○ 기업간 경쟁강도

- 기업용 엔드포인트 보안 솔루션의 세계시장은 상위 5개 기업들의 점유율 총합이 60%로 하위 기업들의 규모도 상당한 수준이지만, 개인용 엔드포인트 보안 시장에서는 상위 5위 기업의 점유율이 약 80%로 압도적인 시장 장악력을 보유

- 이는 전반적으로 엔드포인트 보안 시장의 경쟁 구도가 상당 부분 안정화되어 있음을 의미하고 있어, 시장에서 필요로하는 혁신적인 기술을 확보하지 않고서는 점유율 확대가 어려움

- 국내 컴퓨터 바이러스 백신업체는 안랩, 이스트소프트, 잉카인터넷, 하우리, SGA 등 5개 기업이 대부분의 시장을 점유하고 있음

- 국내 컴퓨터 바이러스 백신 업체 중에서 안랩만이 독자기술을 보유하고 있으며, 나머지 기업들은 외산 기술(Bitdepender)을 기반으로 각 기업의 노하우를 접목한 제품을 출시하고 있기 때문에, 외산기술에 대한 의존도가 상당히 높음

- 보안 관제시스템의 경우, 대용량 로그 데이터 분석을 통한 사이버 공격 대응 시스템인 SIEM 시장으로 진화하고 있고 빅데이터 마이닝 기술을 이용해 차세대 SIEM 기술로 발전되며 사용자 행위 분석 기술까지 포함될 전망으로 인공지능 기술의 핵심 기술인 기계학습 원천 기술의 도입이 필요

4. 사업화 성공 가이드

1) 사업화 후보기업 요건

- ○ 국내 컴퓨터 바이러스 백신 업체
- ○ 네트워크 보안 분야 또는 통합 보안 관제 업체
- ○ 기업용 엔드포인트 보안 솔루션 분야의 기업

2) 사업화 투자비용

- ○ 대상 기술을 이전하여 성공적인 사업화를 위해서는 다음과 같은 추가적인 개발/테스트 내용이 필요함

. 다양한 플랫폼 적용 : SigFreeAV 엔진을 가상머신이나 다양한 OS 등에서 안정적으로 동작하는 과정이 필요

. 통합 시스템 구현 : SigFree AV엔진만을 이용한 독자적인 컴퓨터 바이러스 탐지 제품 출시 뿐만 아니라, 기존 제품에 통합되어 성능이 향상된 제품을 출시하기 위해서는 시스템 통합 과정이 필요

. 레퍼런스 사이트 검증 : SigFreeAV 엔진을 이용한 컴퓨터 바이러스 백신 제품이 안정적이고 우수한 성능으로 동작하는지 여부를 실제 사이트에 적용하여 검증하는 과정이 필요

. 상용제품 실증 서비스 : 베타버젼을 출시하여 실 사용자들의 추가적인 요구사항을 반영할 필요가 있음

– 따라서, 본 기술을 이용하여 성공적인 사업화를 위해서는 2년의 기간 동안 2억/년의 비용이 필요할 것으로 예상함

< 사업화를 위한 추가 요구사항 및 예상 제품 분야 >

3) 법적 검토사항

○ 기술이전 및 실시권 계약 범위 / 라이센싱 및 공동연구 범위 협의

○ 수익성 배분 협의 등

4) 희망 파트너쉽

① 기술이전 (○) ② 라이센싱 (○) ③ 공동연구 ( )

④ 기술출자 ( ) ⑤ 기타 ( )