사이버 블랙박스 및 통합보안상황 분석 기술

박 해룡 한국인터넷진흥원 보안기술팀 팀장

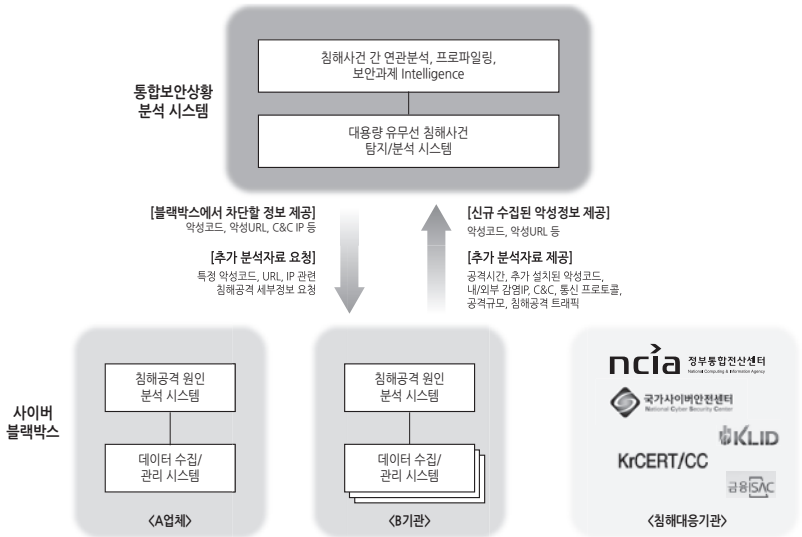
1. 머리말

최근 10년 간 PC 기반의 악성코드는 꾸준히 증가하고 있으며 2013년에는 약 1.9억 개의 악성코드가 유포되고 있는 현황이다[1]. 또한 과거 3.20, 6.25 사이버테러 등과 같이 사이버 침해의 대상이 특정 기업·기관 및 주요 시설을 겨냥하고 있어 그 피해 규모가 사회·국가적으로 확대되고 있다. 이에 다수의 전문 연구기관과 제품개발 업체에서 대응기술 개발의 연구가 활발히 이루어지고 있으나, 3.20 사이버테러 등 침해사고 발생 시 공격 원인에 대한 분석에 수개월이 소요되는 등 적절한 대응에 한계를 보이고 있다. 이에 고도화된 침해공격에 대한 증거보존, 신속한 원인 분석 및 공격자 추적을 가능하게 하는 사이버 블랙박스 및 다수의 사이버 블랙박스에서 수집된 정보를 기반으로 인텔리전스(Intelligence)한 분석정보를 제공할 수 있는 통합보안상황 분석 기술은 사이버 공격의 신속한 사후 조치 및 사전 탐지와 분석을 통해 피해를 최소화하는데 기여할 수 있다.

2. 침해공격 대응을 위한 요구사항

최근 침해사고는 조직의 취약점을 이용하여 장기적이고 지속적으로 정보를 수집하고, 이를 바탕으로 치밀한 공격을 감행할 정도로 지능화되고 있다. 이렇게 지능화 된 공격이 확산되는 가운데, 방어하는 조직의 입장에서는 침해사고 인지 및 원인 분석 수단 부재, 신속한 침해공격 정보공유 및 대응 미흡, 비효율적인 보안관제 등 다양한 문제에 부딪혀 대응이 쉽지 않은 상황이며 이를 위한 기술적인 대책이 요구되고 있다.

첫째, 침해사고의 원인 분석 및 공격 재현 기술이 필요하다. 조직은 장기적이고 지속적으로 공격하는 침해사고의 발생 여부조차 인지하기 쉽지 않으며, 주로 언론 또는 외부 대응기관을 통해 침해사고 피해



[그림 1] 개발기술 개념도

여부를 뒤늦게 확인하는 수준이다. 또한, 침해사고를 인지하더라도 사고의 증거를 보존하고 원인을 분석하는 여력조차 없는 것이 현실이다. 또한, 최근 신종 악성코드는 흔적을 남기지 않거나 증거를 삭제할 정도로 지능화되어 증거 보존도 쉽지 않다[2]. 따라서 침해사고 관련 정보의 무결성을 보존하면서 장기간 보존하고, 그 원인을 정확하게 분석할 수 있는 기술적 수단이 제공되어야 한다.

둘째, 신속한 침해사고 관련 정보의 공유 및 대응 체계가 필요하다. 침해사고 발생 시 조직은 대응 기술 및 인력, 관련 정보 부족으로 침해사고 대응에 많은 어려움을 겪고 있다. 특히 악성코드 샘플, 유입 경로, 차단패턴 등 침해사고 관련 정보의 조기 확보는 신속한 대응에 중요한 가치를 가지고 있다. 따라서 보안업체들이 자발적으로 정보를 공유하고 그 가치를 보상받을 수 있는 체계 및 공유 기술이 제공되어야 한다.

셋째, 보안 인텔리전스(Intelligence) 서비스가 필요하다. 현재 보안관제 요원은 당일 침해공격 탐지/차단 건수, 악성코드 건수 등 기계적이고 형식적으로 보고할 정도의 낮은 탐지 및 대응 능력을 보유하고 있다. 이러한 업무 수준은 보안 관제의 전문성을 저하시키고, 낮은 대우로 인한 보안 인력 채용에도 악영향을 미치고 있다. 따라서 현재 수동적인 단순 업무 환경에서 좀 더 능동적으로 분석하고 대응할 수 있는 업무 환경을 조성하기 위해서는 차세대 보안 관제 및 시각화 기술이 제공되어야 한다.

3. 사이버 블랙박스 및 통합보안상황 분석 기술

3.1 기술 개요

사이버 블랙박스 및 통합보안상황 분석 기술(이하 '사이버 블랙박스 기술')은 고도화된 사이버 침해 공격에 사전·사후 대응을 위하여 침해사고의 신속한 분석과 증거 보존을 목표로 한다. 사이버 블랙박스 기술은 [그림 1]과 같이 크게 사이버 블랙박스와 통합보안상황 분석시스템으로 구성된다. 사이버 블랙박스는 네트워크 트래픽의 휘발성, 비휘발성 정보의

장기간 보존과 무결성을 확보함으로써 침해사고의 신속한 원인 파악과 대응을 가능하게 해준다. 통합보안상황 분석시스템은 플랫폼별 위협 환경을 고려하여 PC와 모바일로 분류하여 처리하며, 기존 단순 탐지/분석 수준을 넘어 다양한 침해사고 정보를 기반으로 연관분석 및 프로파일링을 통한 공격자 추적 및 공격 예측을 가능하게 해 준다.

사이버 공격의 사전 사후 대응을 위한 사이버 블랙박스의 요구사항은 ① 성능 목표치에 준하는 트래픽 저장 및 무결성 확보, ② 공격 원인 분석 및 재현, ③ 분석 대상 정보 전송, ④ 공격 대응이다. '공격 원인 분석 및 재현'의 요구사항은 공격 관련 입력에 대한 원인 분석과 재현결과를 제공할 수 있다. 또한, '분석대상 정보 전송'의 요구사항은 탐지된 악성 의심 파일이나 URL, Outbound 등 의심 트래픽과 악성코드 시그니처 관련 트래픽을 포함하고 있다. 마지막으로 '공격 대응'의 요구사항은 분석된 결과를 바탕으로 차단패턴을 적용하고 차단결과를 전송하여 이루어질 것이다.

3.2 사이버 블랙박스

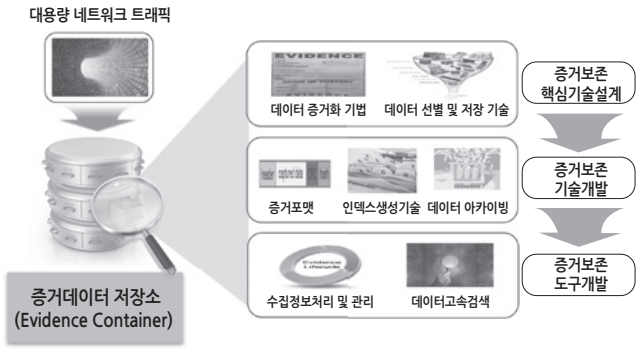
사이버 블랙박스는 사이버 침해사고 증거보존, 블랙박스 내 침해사고 원인 분석 기술을 포함하고 있다. '사이버 침해사고 증거보존' 기술은 네트워크 트래픽을 수집하여 악성행위를 탐지할 수 있게 한다. 특히, 사이버 블랙박스는 10G급 대용량 네트워크 트래픽 정보를 실시간 수집하고 분석할 수 있는 기능을 가지고 있다. 또한, 애플리케이션, IP 등 다중 소스별 대용량 데이터 수집 및 분산처리 시스템과의 연동 제공의 이점이 있다. 여기서 증거보존 핵심 요소 기술은 효율적인 네트워크 트래픽 저장·보관을 위한 증거 보존형 데이터 선별 및 대용량 데이터 아카이빙 기술 적용하며, 수집 데이터의 무결성/기밀성을 보장하는 증거화 데이터 구조 구현이 특징이다. [그림 2]는 네트워크 데이터 증거화 보존 도구의 로드맵을 나타낸다.

'블랙박스 내 침해사고 원인분석' 기술은 내부 유입 실행파일의 재구성과 메타정보의 추출을 통해 악성패턴이 고성능의 수준에서 분류된다. 또한, 내외부에서 수집된 악성패턴 기반의 네트워크 악성행위/악성URL을 탐지하고 차단하는 수집된 악성패턴 기반의 네트워크 기술을 포함한다. 블랙박스 내 침해사고 원인분석의 결과는 악성행위 증거 재현에 이용될 수 있으며, 블랙박스 기반 공격 시나리오를 추출하고 재현하는 공격 정보 분석 기술을 상용화시킬 수도 있다[그림 3].

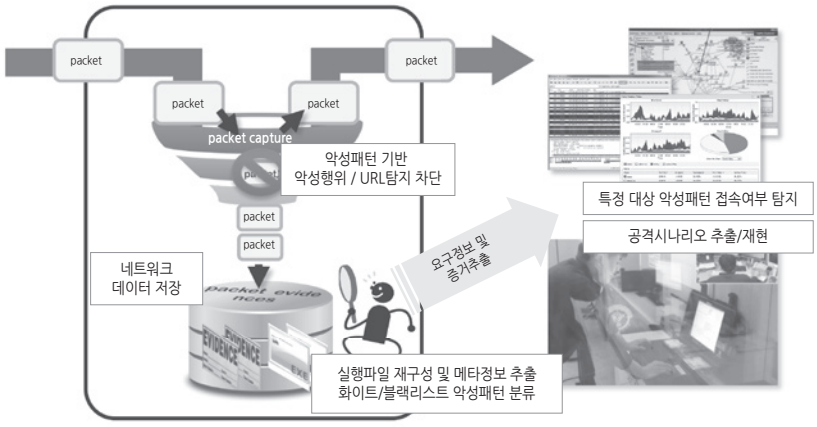
3.3 통합보안상황 분석시스템

통합보안상황 분석시스템은 클라우드 기반 대규모 악성코드 분석, 모바일 침해사고 분석 및 대응, 침해사고 프로파일링 및 공격 예측, 침해사고 정보 공유 기술을 포함하고 있다. '클라우드 기반 대규모 악성코드 분석' 기술은 클라우드 기반의 대용량 악성코드 분석환경을 제공하여 악성코드 분석시간을 단축시키고, 악성코드의 코드블록, 커널행위, API를 기반으로 유사도 분석을 통한 변종 악성코드를 탐지할 수 있는 기능을 가지고 있다. 또한, 가상머신 Hiding, 키보드/마우스 행위 발생, 리얼머신 운용 등 분석회피형 악성코드를 분석할 수 있는 기술을 포함하고 있다[그림 4].

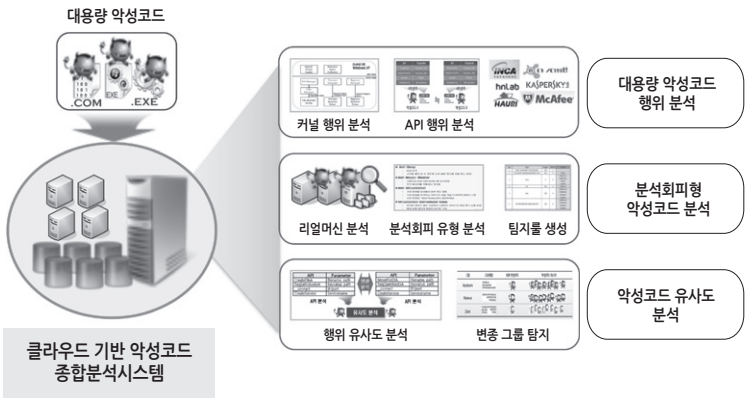
'모바일 침해사고 분석 및 대응' 기술은 Drive-by-Download 형태의 네이티브(Native) 악성코드와 E-mail, SMS와 연동을 통한 악성앱을 수집하여 정적/동적 분석을 할 수 있는 기능을 제공한다. 이를 기반으로 모바일 악성코드 유사도 분석을 통한 변종 탐지 및 프로파일링 기능도 포함하고 있다. 또한,



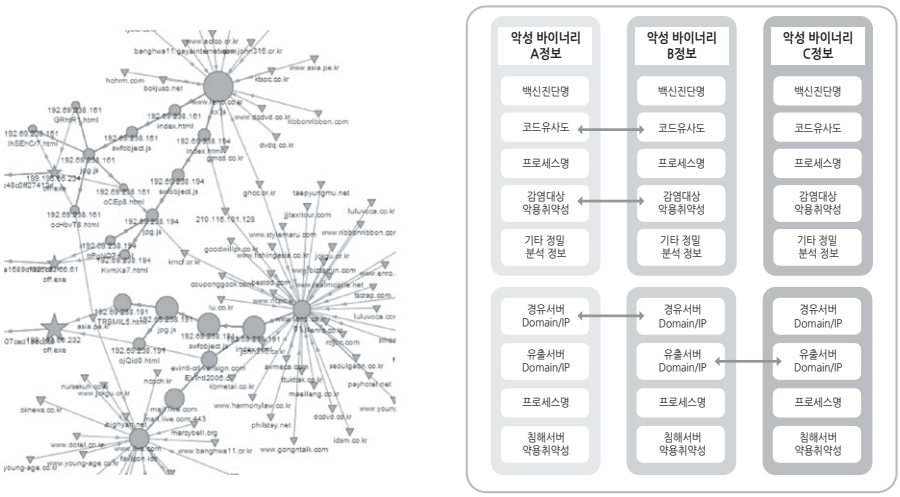
[그림 2] 네트워크 데이터 증거화 보존 도구 개발 로드맵



[그림 3] 블랙박스 내 침해사고 원인 분석 과정



[그림 4] 클라우드 기반 악성코드 종합분석시스템 개발 로드맵

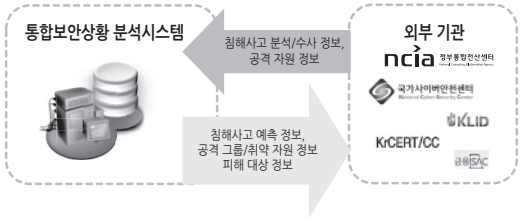


[그림 5] 악성코드 공격 경로 프로파일링 및 악성코드 프로파일링 예시

신속한 모바일 침해사고 대응을 위해 PC 수준의 침해사고 대응체제를 확립하고자, 정보 유출 등 2차 피해 방지를 위한 정보 공유 등을 제안할 예정이다.

'침해사고 프로파일링 및 공격 예측' 기술은 악성코드 분석정보와 침해사고 공격자원(IP, 서버, 도메인 등)을 기반으로 모든 침해사고를 프로파일링하고, 침해사고 간 유사도 분석을 통해 동일 공격자를 추정하는 기능을 포함하고 있다. 또한, 침해사고 프로파일링 정보를 시계열로 분석하여 침해사고 단계별 향후 공격을 예측하는 기능도 제공한다. 이러한 프로파일링 및 공격 예측을 통한 정보는 향후 침해사고 발생 시 선제적 대응에 중요한 역할을 할 수 있을 것으로 본다[그림 5].

마지막으로 '침해사고 정보 공유' 기술은 상이한 정보 공유 포맷 단일화와 국내외 표준 추진을 통해 정보 공유 체계를 강화할 수 있으며, 이를 통해 정보 공유 회원제 및 정보 제공에 대한 과금 기반을 마련할 수 있다. 또한 통합보안상황 분석시스템을 중심으로 침해사고별 악용서버, IP, 악성코드 등 정보를



[그림 6] 침해사고 정보 공유 기술 로드맵

통합 관리하고, 일반 기업을 대상으로 차단 정보 및 공격 예측 정보를 공유함으로써 보안을 강화시키는 특징을 가진다[그림 6].

4. 기대 효과 및 전망

4.1 기대효과

사이버 블랙박스의 고도화된 사이버 침해공격에 대한 사전·사후 대응 기술은 침해사고의 신속한 분석을 통해 침해공격을 조기 탐지/대응하고, 증거 보존 및 신속한 원인 분석의 기술적 기반을 마련할 것으로 예상한다. 특히 과거 침해사고의 프로파일링을 기반으로 공격 예측 분야의 원천기술을 확보

하게 됨으로써, 지능형 신종 공격 대응에 적합하고 신속한 기술적 방안을 마련할 수 있다. 이는 기존 APT 공격과 같은 복합적이고 장기적인 공격에 대응하는 데 유리한 이점이 있을 것으로 기대된다. 또한, 침해사고 증거보존 모듈을 통해 지능화된 사이버 범죄에 대한 신속한 디지털 증거 확보 및 분석은 사이버 수사 관련 기술의 경쟁력을 강화와 이에 대한 시너지 효과를 기대할 수 있다. 이는 기존 장시간이 소요되었던 PC 기반의 디지털 포렌식 기술의 한계를 보완하여 침해사고 분석시간 단축, 유력 디지털 증거 선별 및 효율적인 관리를 통해 신속한 사이버 수사 프로세스 확립에 기여할 수 있을 것이다. 사이버 블랙박스를 통해 침해공격의 증거를 수집하고, 이를 분석하는 것은 기술적 측면뿐만 아니라 침해사고 과실 여부 등의 책임 소재 파악과 법적 증거자료 수집과 같은 사회적 측면에서의 기대효과도 발생한다. 또한 능동적 사이버 보안 대응기술의 확보는 사이버 범죄로 인한 피해를 최소화할 수 있고, 대국민 정서의 안정화와 신뢰도를 제공하여 본 기술적용 기업 및 조직의 신뢰도 향상에 기여할 수 있을 것으로 예상한다.

4.2 전망

본 사이버 블랙박스 기술 개발은 높은 경제적·산업적 이익 창출의 가능성을 가지고 있다. 과거 3.20, 6.25 사이버테러 등 침해사고가 빈번히 발생했던 일례는 증거 보존이 지속적으로 가능하고 신속한 분석을 위한 '사이버 블랙박스' 신규 시장의 수요를 증가하게 할 것이다. 2012년 KISA 지식정보보안산업 실태 조사에 따르면, 보안관리 제품 시장은 2012년 1,430억 대비 2015년 1,911억 원으로, 약 10.1% 증가를 전망한다[3]. 또한, 최근 스마트폰 보급의 증가와 함께 스미싱, 보이스피싱 등 사이버 사기 범죄의 피해가 함께 증가하고 있어 이에 대한 피해를 최소화하기 위한 '모바일 악성코드 대응' 기술 시장의 수요가 증가할 것으로 전망된다. 2013년 경찰청은 2013년(1~10월) 스미싱 피해 건수는 28,469건, 피해액은 54.5억 원이 측정된 결과를 조사하였다[4]. 이러한 추세를 볼 때, 2012년 대비 향후 피해 건수 및 피해액은 모두 10배 이상 증가할 것으로 예상하며 이에 대응하기 위한 사이버 블랙박스의 높은 수요를 전망해 볼 수 있다. 마지막으로 국외 지능형 사이버 보안 시장은 현재 형성 초기 단계로, 본 기술의 개발을 통해 원천기술을 확보할 수 있고 솔루션 제품 출시를 통해 글로벌 시장 선점이 가능하다.

5. 맺음말

본 고에서는 사이버 블랙박스의 개발을 통해 침해사고의 증거수집 및 보존, 분석을 통해 네트워크 보안 및 침해사고에 대하여 높은 기술적·경제적·사회적 파급효과를 가질 것을 기술하였다. 디지털 증거보존과 신속한 사후 분석처리를 통해 복합적이고 장기적인 공격에 대응에 유리한 이점은 최근 빈번하게 발생되고 있는 환경에서 이에 대한 수요를 증가하게 할 것이다. 또한, 인텔리전스 기법 기반의 악성코드 분석 기술적용이 타 기술과 차별화를 보이는 공격 예측 분야의 원천기술 확보에 높은 산업적 가치를 부여해 줄 것으로 예상된다.

[참고문헌]

[1] McAfee, 'AV-TEST Report', 2014

[2] Sophos, 'Sophos Security Threat Report', 2014. 1

[3] KISA, '지식정보보안산업 실태조사', 2012. 6

[4] 경찰청, '스미싱 실태 보도자료: 스미싱의 다양한 수법진화, 이것만은 기억하세요', 2013. 11

[5] ABI research, 'Enterprise Incident Response Market Booms to $14bn as Attacks and Threats Multiply', 2012. 12