이 보고서는 2012년도 국가정보화전략위원회 정책연구용역사업의 연구결과로서 보고서의 내용은 연구자의 견해이며, 국가정보화 전략위원회의 공식입장과 다를 수 있습니다.

제 출 문

국가정보화전략위원회 위원장 귀하

본 보고서를 “고도화된 사이버 위협에 효과적으로 대응하기 위한 국가 보안 Knowledge-Base 구축전략 연구”의 최종연구보고서로 제출합니다.

2011년 11월 30일

수 탁 기 관 : (사) 한국정보보호학회
수탁기관장 : 박 창 섭
연구책임자 : 박 동 규(순천향대학교 정보통신공학과 교수)
연구보조원 : 이 태 영(순천향대학교 정보통신공학과 학부생)

요 약

1. 제 목

고도화된 사이버 위협에 효과적으로 대응하기 위한 국가보안 Knowledge-Base 구축전략 연구

2. 연구의 필요성

- 우리 사회는 광대역 ICT 인프라의 확충과 스마트 디바이스, 클라우드 서비스 및 소셜 미디어 서비스의 활성화로 인해 언제 어디서나 다양한 지식의 공유/관리/제어/창조가 가능한 혼합현실 환경의 상시 연결사회로 진화하고 있고 이로 인해 사람들의 일상생활 패턴은 급격한 변화를 가져오고 있음.
- 이러한 편의성과 함께 증가하고 있는 사이버 위협은 조직적인 방법으로 진화하고 있고 특정 기업이나 국가를 노리고 장기간의 기획 침투 및 잠복, 정보의 유출 등 타겟공격(지능형지속가능위협: APT(Advanced Persistent Threats))의 성격을 나타내는 등 정치적인 성격의 공격이 증가하고 있고, 국가 간 사이버전의 양상을 보이기도 함
- 향후 사회는 물리 및 논리공간의 융합, 스마트 객체의 유기적 연결, 상시연결 사회의 보편화로 인하여 사이버 위협에 대한 효과적 대응을 하지 못하는 경우에 더욱 복잡하고 미묘한 문제를 야기할 수 있어 APT와 같은 고도화된 사이버 위협에 대한 새로운 접근방법과 대응체계에 대한 연구가 요구됨

3. 연구 내용

- 인터넷을 통한 물리공간의 융합과 스마트 디바이스에 의한 이동성이 극대화되는 환경변화에 따른 사이버 위협 및 공격단계 분석
- APT 공격대응을 위한 각 보안업체의 솔루션 동향 분석 및 APT 공격 대응전략 추진 현황 분석
- 특정 국가에 대한 테러의 수단으로 사이버공격 무기를 활용하고 있어 각국의 사이버전 대응전략을 분석하여 국가 사이버 위협 협업 대응을 위한 사이버공격 대응체계 연구
- 향후 다양한 미래서비스 환경 변화와 상시 연결사회의 보편화에 따른 새로운 유형의

사이버 위협에 능동적으로 대응하기 위한 기반으로써 국가 보안 Knowledge-Base 구축 전략 연구

4. 기대 효과

- 안전한 복지사회 인프라 제공을 위한 국가 종합 보안 프레임워크의 기초자료로 활용
- 국가 악성코드 전달경로 정보 지식 베이스 구축 전략으로 활용
- 국가 주요정보 유출 방지를 위한 종합적이고 체계적인 모니터링 수단을 위한 핵심기술개발 로드맵 기초자료로 활용

목 차

그 림 목 차

1. 서 론

우리 사회는 광대역 ITC 인프라의 확충과 스마트 디바이스 보급, N드라이브/유클라우드/다음클라우드 등의 클라우드 서비스 확대와 더불어 페이스북/카카오톡/유튜브와 같은 소셜 미디어 서비스의 활성화로 인해 언제 어디서나 다양한 지식의 공유/관리/제어/창조가 가능한 상시 연결사회로 진화하고 있다. 이로 인해 사람들의 일상생활 패턴은 시간과 공간의 제약을 벗어나게 되었으며, 사이버공간과 현실공간의 구분이 없는 서비스 제공으로 혁신적인 형태로 변화하고 있는 상황이다. 이러한 편의성과 함께 증가하고 있는 사이버 위협은 조직적인 방법으로 진화하고 있고 특정 기업이나 국가를 대상으로 장기간의 기획침투 및 잠복, 정보유출 등의 지능형지속가능위협(APT: Advanced Persistent Threats) 공격의 성격을 나타내는 등 정치적인 성격의 공격으로 발전하고 있다. 구글 해킹 사건, 오퍼레이션 오로라(Operation Aurora), 이란 원전을 마비시켰던 스턱스넷(Stuxnet), 글로벌 에너지 기업을 노렸던 나이트 드래건(Night Dragon), RSA사의 OTP 기술 유출 사고 등은 특정 지역, 특정 국가를 대상으로 한 고도화된 APT 공격의 대표적인 사례로 거론되고 있고 이로 인해 국가 간 사이버전에 대한 우려를 사고 있다.

따라서 이러한 사이버 위협에 효과적으로 대처하지 않으면 국가의 안보가 위태로운 지경에 이를 수 있어 이에 대한 체계적이고 능동적인 대응전략이 필요한 상황이다. 또한 향후 사회는 물리 및 논리공간의 융합, 스마트 객체의 유기적 연결, 상시연결 사회의 보편화로 인하여 사이버 위협에 대한 효과적 대응을 하지 못하는 경우에 더욱 복잡하고 미묘한 문제를 야기할 수 있어 사이버 위협에 대한 새로운 접근방법과 대응체계에 대한 연구가 요구된다.

본 연구를 통하여 인터넷을 통한 물리 및 논리공간의 융합과 스마트 디바이스에 의한 이동성이 극대화되는 환경변화에 따른 APT 사이버 위협 및 공격단계를 분석하고, 이를 기반으로 향후 다양한 미래서비스 환경 변화와 상시 연결사회의 보편화에 따른 새로운 유형의 사이버 위협에 능동적으로 대응하기 위한 기반으로 국가 보안 Knowledge-Base 구축전략을 수립함으로써 APT등 고도화된 사이버 위협에 효과적으로 대응할 수 있으리라 사료된다.

2. APT 등 고도화된 사이버 위협 분석

우리 사회가 광대역 ITC 인프라의 확충과 스마트 디바이스 보급 및 소셜 미디어 서비스의 활성화로 인하여 상시 연결사회로 진화하게 됨에 따라 이러한 편의성과 함께 사이버 위협도 같이 진화하여 특정 기업이나 국가를 대상으로 하는 지능형지속위협이 현재 전 세계적으로 중요한 사회문제로 대두되고 있다.

APT 공격은 최신 기술로서 기존의 공격이 불특정 다수를 대상으로 시도한 것과는 달리 명확한 표적을 정하여 공격자가 목적을 달성할 때까지 장기간 동안 지속적으로 정보를 수집하고, 이를 바탕으로 치밀한 공격을 감행한다는 점에서 보다 지능화된 기법이라고 볼 수 있으며, 공격의 방식도 시스템에 직접 침투하는 것뿐 아니라, 표적이 된 조직의 내부 직원들이 이용하는 다양한 단말기 등에 대한 우회 공격들을 사용한다는 점에서 보다 정밀한 공격 방식이라고 할 수 있다. 그러므로 APT와 같은 고도화된 위협에 대응하기 위해서는 기존의 방어보다 심도 있고 조직적인 대응이 필요하며 개별 보안 기술 및 솔루션 적용이 아닌 전사 및 통합 차원의 보안 체계 구성이 필요한 상황이다.

현재 APT 공격을 방어하기 위하여 전 세계의 모든 보안 관련 기업들과 보안 관련 기관에서 많은 연구를 진행하고 있는 중이다. 국외에서는 IBM, 델 시큐어웍스(DELL SecureWorks), 카스퍼스키(KASPERSKY), 시만텍(Symantec), CA 테크놀로지(CA technologies), 엣지 웨이브(EdgeWave), 웹센스(Websense)등 많은 기업 및 연구소에서 연구를 수행하고 있으며, 국내에서도 안랩(Ahn Lab.), 트랜드마이크로(Trendmicro)등의 기업과 한국인터넷진흥원(KISA), 한국전자통신연구원(ETRI)에서도 APT 공격에 대한 대응방안을 연구하고 있는 중이다. 각각의 연구에서는 APT의 피해 사례 분석을 통하여 APT 공격의 특성을 파악하고 APT 공격을 단계별로 분석하여 다 계층화된 데이터 중심의 깊이 있는 방어 대책을 수립하고 있는 중이다. 그러나 아직까지도 완전하다고 할 수 있는 해결 방안은 없으며, 특히 국가적인 대응체계에 대한 연구는 미진한 편이다.

APT 공격과 같은 고도화된 사이버 위협에 대처하기 위해선 위협 발생 전(사전 대응, 운영 대응)과 위협 발생 후(사후 대응)를 구분하여 지속적으로 관리, 감독할 수 있는 정부 차원에서의 대응체계가 필요하며, 이를 기반으로 민간 기업을 대상으로 APT 대응 보안정책 컨설팅, 내부자 교육, 망 분리 등의 기술 지원 등을 통해 기업 자체적인 보안 관리 체계 강화를 지원하는 것이 중요하다고 할 수 있다.

2.1 APT의미

‘APT’라는 단어 자체는 최근에 들어서 새롭게 정의된 단어와 의미는 아니고, 미국 공군사령부에서 사용하던 군사용어에서 유래된 용어로 군사 전술에서 ‘장기간에 걸쳐 지능적으로 공격하고 위협하는 전략’을 일컫는 말이었다. 최근 들어 스턱스넷이나 플레임 같은 사이버공격을 설명하는 과정에서 보안 전문가들이 APT란 용어를 사용하면서 보안업계에서도 통용되는 용어로 자리를 잡게 되었다.[1]

- Advanced

사전적인 의미는 ‘앞선’, ‘고급의’로 정의되고 있으나, APT에서 ‘Advanced’라는 단어의 의미는 APT 형태의 보안 위협을 생산하는 조직에서 사용하는 기술적인 범위와 수준을 지칭하는 것으로 APT 형태의 보안 위협을 생산하는 조직은 특정한 목적을 수행하기 위해 보안 위협 생산에 사용되는 기술들을 한 가지로만 제한시키는 것이 아니라 광범위하게 많은 기술들을 동시에 사용 한다. 간단한 예로 APT 형태의 보안 위협을 생산하기 위해 마이크로소프트(Microsoft)의 윈도우(Windows) 운영체제를 깊이 있게 분석하여 새로운 제로데이(Zero-Day) 취약점을 찾아내어 악용할 수도 있으며, 특정 조직의 내부 시스템을 장악하기 위한 목적으로 기존 보안 소프트웨어로 부터 탐지를 회피 할 수 있는 새로운 형태의 악성코드를 제작하는 것을 들 수가 있다. 즉 ‘특정 목적을 달성하기 위해 보안 위협을 생산하는 조직은 IT 인프라와 관련된 모든 기술들을 다양하게 사용 할 수도 있다.’라는 의미로 해석 할 수 있다.

- Persistent

APT의 두 번째 단어에 해당하는 ‘Persistent’는 사전적인 의미로 ‘영속하는’, ‘끊임없이 지속되는’으로 정의되어 있다. APT에 있어서 이 ‘Persistent’라는 단어의 의미는 보안 위협을 생산하는 조직이 가지고 있는 특정 목적을 대하는 자세 또는 공격 대상에 대한 태도로 해석 할 수 있다. 이는 보안 위협을 생산하는 조직이 원하는 특정 목적이 달성되기 전까지는 그 공격 대상에게 새로운 기술과 방식이 적용된 공격들을 끊임없이 지속적으로 수행하기 때문이다. 이러한 특징으로 인해 APT 형태의 보안 위협을 논하는 정보 보호 분야에서는 이 ‘Persistent’적인 특성으로 인해 APT 형태의 보안 위협의 목표가 되는 대상이 치명적인 손상을 입게 된다고 보고 있다.

- Threat

APT에서 의미하는 'Threat'은 사전적인 의미의 '위협'을 그대로 뜻한다. 그리고 여기서 이야기하는 위협의 구체적인 형태로는 악성코드, 취약점, 해킹 등으로 IT 기술에 의해 생산되는 형태가 될 수도 있으며, 사람에 의해 직접적으로 만들어지는 사회공학(Social Engineering) 기법적인 형태가 될 수도 있다.

이렇게 APT가 가지는 개별적인 단어들의 의미와 함께 현재 발생하는 보안 위협의 특성들이 합쳐져 2006년 미국 공군사령부에서 사용하던 APT 의미에서 변형된 다른 의미가 성립하게 되었다. 이렇게 성립된 APT가 가지는 의미를 요약하여 정의해본다면 APT는 '다양한 IT 기술과 방식들을 이용해 조직적으로 경제적이거나 정치적인 목적을 위해 다양한 보안 위협들을 생산해 지속적으로 특정 대상에게 가하는 일련의 행위'라고 할 수 있으며 공격상대를 연구한 뒤 지능적으로 접근하는 해킹방식으로 사회공학 기법이라고도 말할 수 있다.[1]

2.2 APT의 특징

APT 공격은 다음과 같은 특징을 갖는다.

- 지능적 (Advanced)

일반적인 공격과 더불어 APT는 제로데이(Zero-Day) 취약점, 루트 킷과 같은 고도의 지능적인 보안 위협을 동시에 이용하여 목표에 침투해 은밀히 정보를 빼돌리는 킬 체인(Kill Chain)을 생성한다.

- 지속적(Persistent)

APT 공격은 보안탐지를 회피하기 위하여 은밀하고, 천천히 움직여야 하기 때문에 일반적인 공격에 비해 몇 배가 되는 긴 시간동안 공격이 행해진다. 보통 다수의 표적공격이 순식간에 목표를 공격해 필요한 정보를 탈취해 간다면, APT는 목표 시스템에 활동 거점을 마련한 후 은밀히 활동, 새로운 기술과 방식이 적용된 보안 공격들을 지속적으로 공격해 정보 유출이나 삭제, 시스템에 대한 물리적인 피해 등 공격자들이 궁극적으로 원하는 목적을 이루기 위해 행해지는 공격이다.

- 공격의 동기(Motivated)

APT는 주로 국가 간 첩보 활동이나 기간 시설 파괴 등의 특정 목적을 달성하기 위해 행해지며, 대부분 배후에 후원하는 첩보 조직이나 단체가 연관되어 있는 경우가 많고, 이는 APT가 단순히 정보 유출만을 노리는 것이 아니라 공격자가 지속적으로 표적을 원격 조종하여 정보 유출을 포함한 시스템에 운영을 방해하거나 물리적인 타격까지도 유발하는 공격이다.

- 공격의 목적(Targeted)

지적 재산권이나 가치 있는 고객 정보를 가진 거의 모든 조직들이 표적공격의 대상이라면, APT는 주로 정부기관이나 기간 시설, 방위 산업체, 그리고 전 세계적으로 경쟁력 있는 제품, 기술을 보유한 주요 기업들과 이들의 협력업체 및 파트너 기업들을 대상으로 한다.[2]

- 공격의 맹점(Blind Spot)

APT는 USB, 외장하드 등 네트워크를 이용하지 않고 정상적인 트래픽 경로를 사용하는 경우가 대부분이기 때문에 방어가 매우 어렵고, 정상적인 메일이나 웹 사이트 등을 통해 악성코드 배포가 가능하기 때문에 이를 사용하여 표적에 가해지는 APT 공격을 완벽하게 차단하기는 매우 어렵다.[3]

2.3 주요 APT 해킹 피해 사례

- 국내 피해 사례

· 농협 전산망 해킹사건

2011년 4월 12일에 있었던 농협 전산망 해킹사건으로 농협 전산망에 있는 자료가 대부분 손상되어 수일에 걸쳐 전체 또는 일부 서비스 이용이 마비된 사건이 발생하였다. 당시 공격방법은 외주 업체 직원이 웹 하드 무료 쿠폰을 사용하여 서버 관리 업무용 노트북에 영화를 다운로드 받다가 악성코드에 감염됨으로써 발생하게 되었다. 공격자는 이 악성코드를 통해 노트북을 점령하고, 7개월 여간 노트북을 모니터링해서 최고위 관리자의 비밀번호 등, 전산망 관리를 위한 각종 정보를 탈취하여 공격 명령 파일을 설치하고, 원격으로 공격명령을 실행하였다. 이로 인해 1차 공격을 받은 서버들이 좀비 컴퓨터로 변해 다른 서버들을 공격하였으며, 600여대의 내부 서버 중 절반에 해당하는 서버가 디스크 손상피해를 입었고, 재해복구용 서버마저 파괴되면서 농협은 최소 80억 원에 해당하는 피해가 발생했던 사건이다.[4]

· 현대캐피탈 해킹 사건

2011년 4월 현대 캐피탈의 고객정보가 유출되는 사건이 발생하였다. 해커 그룹이 업무 관리자의 아이디와 비밀번호를 습득한 뒤, 보조 서버인 광고 메일 서버와 정비내역 조회 서버에 침입해 화면을 복사하거나 해킹 프로그램을 통해 다운로드하는 방법으로 175만 명의 고객정보를 해킹한 사건이다. 현대 캐피탈은 퇴직한 직원의 아이디와 비밀번호를 삭제하지 않아서, 이 퇴직한 직원이 사용하던 아이디와 비밀번호를 통해 해킹이 이루어지게 되었으며, 7회에 걸쳐서 무단 접속이 수행되었다.[4]

· 네이트/싸이월드 개인정보 유출 사건

2011년 7월, 공격자가 네이트 내부 개발자의 PC를 장기간 집중 공격하여 이를 통해 네이트의 데이터베이스에 저장된 가입자 3,500만 명의 ID, 비밀번호, 이름, 주민등록번호, 연락처 등 개인정보를 유출시킨 사건이 발생하였다. 이 사건은 공격자가 내부 개발자의 PC를 장기간 집중 공격하여 이를 통해 해킹에 성공한 것으로 국내에 대표적인 APT 피해 사례라고 추정할 수 있다.[4]

- 해외 피해 사례

· 달빛 미로 사건

1998년 3월부터 2000년까지 '달빛 미로'라고 명명된 사이버공격이 국방부의 컴퓨터, 미 항공 우주국 (NASA), 미국 에너지부, 연구 실험실 및 사립대학을 대상으로 실행되었다. 공격자는 성공적으로 수 만개의 파일에 액세스 할 수 있었다.[5]

· 미국 하원 사건

2006년 8월부터 2007년까지 두 의원의 사무실 컴퓨터 네트워크가 손상되었다는 사실이 보도되었다. 이 공격으로 인해 북경 정권의 중요한 반체제 인사에 대한 정보가 도난당한 것으로 추측된다.[5]

· 미국 국방부 사건

2008년 초에 미 국방부에 외국 정보기관이 USB 플래시 드라이브에 악성 소프트웨어를 배치한 이후에 모든 군사 컴퓨터 네트워크 시스템이 누출되는 사건이 발생하게 되었다. 감염 장치가 미국 군사 노트북을 감염시켜 악의적인 코드가 미국 네트워크를 통해 전파되는 사건이었다.[5]

· 교황 달라이 라마 사무실 사건

2008년 9월에 달라이 라마(OHHDL) 교황의 사무실로 전송되던 이메일이 중

간에 탈취되어 악성 콘텐츠가 포함 된 파일로 대체되는 사건이 발생하였다.

이 공격은 해커가 달라이 라마 컴퓨터 네트워크에 액세스하기 위해 사회공학적 기법을 사용한 것으로 추측되며, 해커가 침입을 통해 사용자 암호를 얻고 나중에 원격으로 달라이라마 메일 서버에 액세스하기 위해 사용자 암호를 사용한 것으로 보인다.[5]

· 영국 RBS 월드페이 해킹 사건

2008년 일명 "캐쉬어(Cashier)"로 알려진 러시아, 에스토니아, 몰도바 등 8명의 다양한 국적을 가진 해킹 그룹이 영국의 RBS 은행의 시스템에 침입 후, 신용카드 정보를 훔쳐 복제카드를 생성하고, 신용카드 한도를 올려서 12시간 동안 미국, 러시아, 우크라이나, 에스토니아, 이탈리아, 홍콩, 일본, 캐나다 등 49개 도시의 2100여개의 ATM기기에서 950만 달러를 인출한 사건이 발생하였다. 해커들은 네트워크에 접속하여 카드번호와 비밀번호를 알아내었고, 이 사실을 숨기기 위해 시스템 데이터를 파괴했다. 이 사건으로 월드페이 서버에서 150만 카드 이용자들의 개인정보와 금융정보, 110만 노동자들의 사회보장번호가 유출되었다.[4]

· 미국 오크리지 국립 연구소 해킹 사건

2011년 4월 미국 에너지부(DOE) 산하의 오크리지 국립 연구소(ORNL)에 대한 사이버공격이 발생하였다. 이 공격은 직원 복지와 관련된 이 메일을 연구소 인사부에서 발송하는 것처럼 만든 스피어 피싱(Spear Phising)메시지를 통해 연구소 시스템에 접근하였으며, 이 사건에서 이메일 수신자들이 링크를 클릭한 순간 악성코드가 시스템에 다운로드 되어 감염되었고, 그 중 2대의 컴퓨터가 악성코드에 감염되어 7일 간 정보를 수집하여 원격 서버에 데이터를 수집하여 전송한 것이다. 이 공격을 통해 1GB 정도의 기술 데이터가 유출되었다.[4]

· 이란 원자력 발전시설 해킹 사건(스턱스넷)

2010년 7월 이란 원자력 발전시설을 마비시켜, 이란 원자력 발전 시설의 원심분리기중 20%가 가동이 중단되는 사건이 발생하였다. 이 사건은 일명 스턱스넷이라고 불리는 악성코드에 의해 수행되었으며, 스턱스넷에 의한 공격은 독일 지멘스사의 SCADA 소프트웨어를 공격 대상으로 하였다. 이 사건에서 SCADA 내부 시스템에 접근할 수 있는 사용자의 단말이 인터넷에서 1차 감염되었고, USB 등의 외장 매체로 복제 전파되어 해당 매체가 SCADA 내부 시스템에 접속하게 되는 경우에 시스템을 감염시켜 침투하게 되었다. 스턱스넷은

SCADA 제어 시스템을 감염시켜 밸브, 펌프 등의 제어 기능을 방해하거나 시스템이 마비되도록 악성코드가 설계되었고, 해커들은 원자력 발전소 내부의 다른 시스템으로 유포시키기 위하여 윈도우 셸 바로가기 취약점(MS10-046), 작업 스케줄러 취약점(MS10-092), 서버 서비스 취약점(MS10-092), 프린트 스풀러 서비스 취약점(MS10-061), 커널 모드 드라이버 취약점(MS10-073)등 5개의 취약점을 사용하였다.[5]

· 다국적 석유회사 해킹 사건(일명 Night Dragon)

2011년에 쉘, 엑슨 모빌, BP, 마라톤오일, 코노코 필립스, 베이커 휴즈 등의 미국의 다국적 석유 및 가스회사 다섯 곳이 해킹을 당해 정보가 유출된 일명 “나이트 드래건(Night Dragon)”이라 불리는 사건이 발생하였다. 이 사건은 2009년부터 2년 동안에 걸쳐 해킹 공격을 받아 가스와 석유 분야의 생산 시스템 및 산업통제 시스템 관련 정보가 유출 된 사건이다. 이 사건은 해커들이 사회공학 기법, 윈도우 시스템 취약점, Active Directory, 원격 접근 도구(RATs)등의 기법을 통하여 공격을 시도하였다. 웹 서버의 SQL 인젝션 공격을 통해 악성코드를 유입하였고, 스피어 피싱(Spear Phising)을 통해 계정정보를 획득하여 악성코드 다운로드 및 감염을 시도하였다. 획득한 계정정보로 시스템에 대한 접속을 시도해 시스템 내부 사용자 계정정보를 추가 확보하고 침투 시스템을 경유하여 주요 정보 시스템 접근 및 주요 정보를 탈취한 사건이다.[4]

· RSA해킹사건

2011년 3월 암호 전문 보안기업인 미국 EMC RSA사가 해킹되어 데이터가 유출되는 사건이 발생하였다. 이 사건은 공격자가 악성코드를 이메일에 첨부하여 EMC RSA 직원에 송부하였고, EMC RSA 직원은 이메일에 첨부된 파일을 실행(파일명 : 2011 Recruitment plan.xls)함으로써 XLS(마이크로소프트 엑셀)파일에 포함된 공격 파일(Flash 취약점 이용 악성코드)이 실행되어, 즉시 시스템 제어 권한을 탈취 당하게 되었다. 이 사건으로 EMC RSA의 OTP 제품인 시큐어 ID의 기밀 정보가 유출되었으며, 현재까지 피해 사례는 보고되지 않고 있지만, RSA 기술을 사용하는 기업이나 기관의 위험이 높아지게 되었고 시큐어 ID 제품 4천만대가 리콜 조치되었다.[5]

· 모건 스탠리 해킹사고(일명 오로라 사건)

이 사건은 2009년 6월부터 6개월 동안 200개 이상의 회사를 상대로 해킹을 시도하여 첨단 정보통신사업체들이 가지고 있는 중요한 기업 정보를 탈취

하기 위하여 수행되었다. 이 사건에서 마이크로소프트사의 인터넷 익스플로러 제로데이 취약점인 MS10-002가 사회공학적으로 악용되었으며, 사이버 위협 대응 형태의 악성코드가 사용되었다.[5]

· GhostNet 사건

2009년 3월 29일에 해커가 주중한국대사관, 동남아 정부와 달라이라마에 속한 컴퓨터를 포함하여, 103개국에서 최소 1,295대의 컴퓨터를 감염시켜 장악한 뒤 원격 조정할 수 있는 사이버 스파이 네트워크(일명 'GhostNet')를 구축한 사건이다.[5]

· 프랑스 정부 사건

2010년 12월부터 2011년 3월까지 프랑스 정부가 사회공학적인 이메일 캠페인의 대상이 되어서 프랑스 경제 부처 및 프랑스 금융 중앙 서비스 부문의 150대의 컴퓨터가 손상되는 사건이 발생하였다. 해커는 원격으로 각 부처의 컴퓨터를 제어할 수 있었으며 세 달 동안 문서를 검색 할 수 있었다. 해커는 G20과 국제 경제와 관련된 프랑스 대통령에 관한 문서를 검색하고 있었다.[5]

· 캐나다 정부 사건

2011년 1월에 캐나다 정부 부처들이 부서 내의 선임 직원으로부터 전송된 것처럼 보이는 사회공학적 이메일(캐나다 정부 컴퓨터를 손상시키는 악성 첨부 파일을 포함)의 대상이 되어 캐나다 정부의 기밀 정보가 도용되는 사건이 발생하였다.[5]

· 호주 정부 사건

2011년 2월부터 3월까지 호주 의회 컴퓨터가 적어도 1 개월 이상의 기간에 걸쳐서 비합법적으로 접근되는 사건이 발생하였다. 이 기간 동안에 호주 총리, 외무 장관과 국방 장관의 일정을 포함한 수 천 개의 메일이 외부로 유출된 것으로 추측된다.[5]

· 록히드 마틴 사건

2011년 5월 21일에 록히드 마틴사에서 자사의 컴퓨터 네트워크에서 사이버 공격을 감지하는 사건이 발생하였다. 이 회사의 정보 보안 팀은 시스템을 보호하기 위해 공격적인 조치를 수행하였으며, 결과적으로 데이터의 유출이 발생하지 않은 것으로 알려져 왔다. EMC RSA는 같은 해 3월에 RSA 해킹에서 도난당한 정보가 록히드 마틴사의 공격 요소로 사용되었음을 공식적으로 발표하였다.[5]

· 국제 통화 기금 (IMF) 사건

2011년 5월부터 6월까지 IMF를 대상으로 특별히 작성된 것으로 보이는 악의적인 소프트웨어를 사용한 정교한 사이버공격으로 적어도 한 대 이상의 국제 통화 기금 (IMF) 컴퓨터가 손상되는 사건이 발생되었다. 감염된 컴퓨터는 내부 시스템 및 파일을 액세스하는 데 사용되었으며, 해커들은 그들에게 중요한 경제적, 정치적 정보를 도용한 것으로 추정된다.[5]

2.4 APT 공격 수법

- 공격 수법

APT공격의 전형적인 수법은 공격 대상 기업을 정한 후 해당 기업에 소속되어있는 특정 개인에게 협력업체의 제안서 등을 가장해 바이러스가 첨부된 표적형 메일을 송부한다. 메일 수신자가 아무 의심 없이 이 파일을 열어 백도어 프로그램 등이 설치되면 이를 통하여 사내 정보를 추가적으로 수집하고 사내 중요 데이터베이스 등에 침투하여 첩보 활동을 수행하여 수개월에 걸쳐서 표적이 되는 기업의 정보를 수집하는 행위가 대표적이다.

- 공격 기술

· 스피어 피싱

피싱(Phishing)이 불특정 다수를 대상으로 인터넷 사이트를 통해 공격을 하는 것에 비해 스피어 피싱(Spear Phishing)은 특정인을 대상으로 공격하는 것을 말한다. 스피어 피싱 방법으로는 신뢰할 수 있는 기관이나 기업, 사람, 직원 또는 부서를 사칭한 메일 발송이 대표적인 방법이며, 최근에는 SNS(Social Network Service)를 이용한 악성 링크 클릭 유도로도 이용되고 있다. 최근에는 스피어 피싱 대상이 APT 공격의 최종 목표 달성에 가까운 사람인 VIP인 경우 이를 훼일 피싱(Whale Phishing)이라 부르고 있다.[4]

· 난독화

난독화(Obfuscate)라는 단어의 사전적 의미는 '가리거나 불분명하게 만든다.' 는 뜻이며, 해킹에서는 최근 해커들이 상용 네트워크 보안 솔루션의 보안 기능을 우회하기 위해서 자바 스크립트 코드나 PDF를 난독화하여 공격에 활용하는 것이 중요한 특징이다. 난독화의 대표적인 예는 자바 스크립트 난독화이며, 자바 스크립트는 데이터를 코드처럼 실행하고, 조작하거나 암호화 할 수 있기 때문에 해커는 악성코드를 자바 스크립트내의 인코딩이 많이 된 데이터

가 밀집되어 있는 부분에 숨겨서 공격을 수행한다. 특히 자바 스크립트 코드는 단말에서는 브라우저와 문서 뷰어에 의해 쉽게 해석되지만 네트워크 단에서는 해석에 많은 비용이 소비되므로 난독화된 악성 자바 스크립트 코드에 대한 효과적인 대응에는 많은 어려움이 있다. 또한 난독화는 합법적인 웹 사이트에서 소스코드 유출을 방지하기 위해 사용하기 때문에 네트워크 보안 제품이 난독화된 모든 자바 스크립트를 차단하는 기법을 적용하는 것도 어려움이 있을 수 있다.[4]

· PDF공격

PDF 공격은 해커가 PDF 취약점을 이용하여 PDF 파일 내에 악성코드를 삽입하여 발송 또는 배포하는 것으로 최근 해커가 이용자들을 새로운 방법으로 속이려 함에 따라 활용이 지속적으로 증가하고 있다. 이 방법은 엔드 포인트(Endpoints)가 조직에서 일반적으로 가장 취약한 연결고리이기 때문에, 공격에 성공할 가능성이 높고, 특정 엔드 포인트에 중요한 정보가 없더라도 중요 정보가 있는 다른 엔드 포인트에 접근할 권한을 갖고 있을 수 있기 때문에 공격의 최종 목표를 달성하기 위한 방법으로 APT 공격에서 많이 이용되고 있는 방법이다. 더구나 브라우저 공격은 다양한 종류의 브라우저에 대해서 모두 공격 기법을 개발하여야하고, 그 중 취약점이 복잡한 브라우저가 있다면 APT 공격 대상이 제한적으로 이용될 수 있기 때문에 공격의 효과 및 범용성 측면에서 보다 효과적인 PDF 공격이 최근에 널리 이용되고 있다. 또한 PDF 문서는 규격이 복잡하기 때문에 해커가 PDF 문서의 한부분에 데이터를 숨긴 후 나중에 프로그램을 통해 해당 데이터를 회수하고 디코딩 알고리즘을 적용하여 악성 스크립트를 반환할 수 있다는 점에서 특정 브라우저를 대상으로 한 공격보다 유리하다고 할 수 있다.[4]

· 제로데이 악성코드

APT 공격에서 이용하는 악성코드는 대부분 안티 바이러스 제품에서 탐지되지 않는 제로데이 악성코드로서, 표적대상에 특화된 형태로 개발되어 이용되고 있어 탐지하는데 많은 어려움이 따르고 있다. 즉, 제로데이 악성코드는 악성파일이 저장되는 폴더 명이나 파일명이 랜덤하게 부여되고, 새롭게 감염될 때마다 실행파일을 약간 다르게 수정하는 등 보안 제품의 탐지를 우회하기 위한 다양한 기법을 사용하고 있다. 뿐만 아니라 상용 소프트웨어의 복사방지 기법을 이용하여 개발된 악성코드의 경우는 실행파일이 설치될 때 설치되는 단말기 및 환경 정보를 이용하기 때문에 외부 시스템으로 파일을 복사한 후에

는 실행되지 않으므로 악성코드에 대한 분석을 어렵게 하는 특징이 있다.[4]

- APT 공격단계

공격 단계는 각 연구마다 조금씩 차이가 있으며 대표적인 분석단계를 보면 다음 그림 1과 같다.

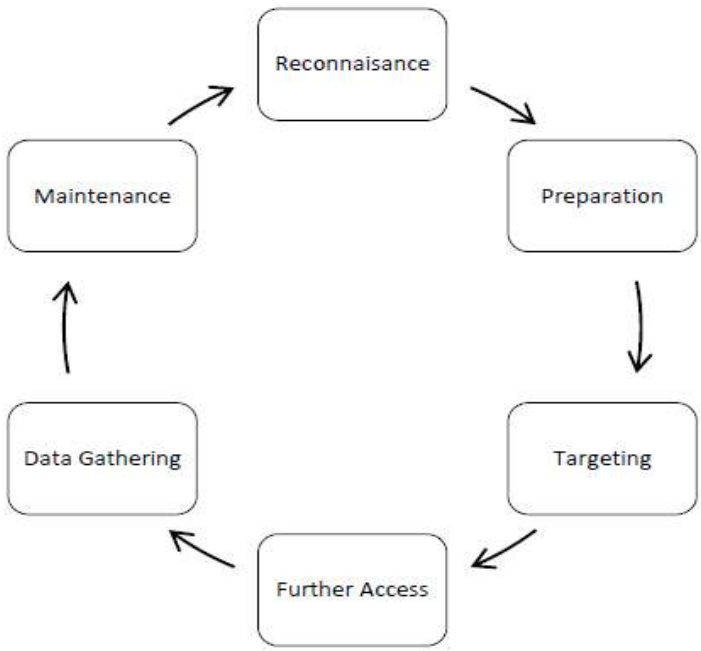

그림1. APT 공격 방법 분석

· 정찰 (Reconnaisance)

공격자는 수동적으로 최선의 표적 대상을 확인하기 위해 자신의 목표에 대한 정보를 수집한다. 이 정보에는 대상의 사무실의 위치, 그들의 컴퓨터의 위치, 회사에서 사용하는 기술, 그들이 통신하는 방법, 직원들, 직원의 연락처 세부 정보, 관심 분야 및 연락처가 포함 될 수 있다.

· 준비하기(Preparation)

공격자는 적극적으로 자신이 의도한 피해자를 공격하기 위한 적절한 도구와 기술을 개발하여 앞으로의 공격에 대해 준비하고 테스트를 한다. 이 작업에는 취약점을 결정하기 위한 스캔과 악성코드를 작성하거나 또는 코드의 인수, 사

회공학적 이메일의 초안 작성, 어떤 이메일 계정에서 사회공학적 이메일을 보낼 것인지에 대한 결정, 필요한 하드웨어(예 : USB 플래시 드라이브)의 인수, 공격을 시작하고 명령 및 제어 통신을 할 때 어떤 인프라가 사용되어야 하는지에 대한 결정, 필요한 계정(이메일 주소, 콜 백 도메인 등)에 등록하고 설정하는 작업 및 테스트 수행 등이 포함된다.

· 타겟팅(Targeting)

공격자는 공격을 수행하고 손상 또는 고장의 징후에 대한 모니터링을 실행한다. 공격자는 취약점을 악용하기 위해 서버에 원격으로 연결을 시도 할 수 있으며, 전략적으로 USB 플래시 드라이브를 배치하거나 공격 대상에게 하나를 제공할 수 있다. 그리고 사회공학적인 이메일을 보낼 수도 있으며, 바운스 백 알림을 확인할 수도 있고, 명령을 모니터링하고, 인프라를 제어하며, 잠재적으로 감염된 컴퓨터에 대한 인 바운드 연결을 시도하거나 내부자의 피드백을 기다릴 수도 있다.

· 접근 확장(Further Access)

공격자가 성공적으로 컴퓨터 네트워크에 대한 액세스 권한을 얻고 나면, 그들은 일반적으로 관심 있는 데이터에 대한 접근과 추가, 백도어를 설치하기 위해 기존 네트워크 및 이동이 가능한 네트워크를 식별 하게 된다. 이것은 보통 2 단계(준비)와 3 단계(타겟팅)로 돌아가는 것을 필요로 할 수 있으며, 도구 및 악성 소프트웨어의 업로드, 권한 상승, 네트워크 연결 및 백도어가 설치된 취약 호스트의 식별을 필요로 할 수 있다. 또한, 암호 해시를 얻기 위해 도메인 컨트롤러에 대한 액세스 권한을 얻는 것과 로그를 변경함으로써 추적을 막는 것, 그리고 데이터 수집을 위한 메일이나 파일 서버에 대한 액세스를 포함할 수 있다.

· 데이터 수집(Data Gathering)

공격자가 관심 정보를 확인하고 나면, 그들은 이 정보를 수집하고 유출을 시도한다. 그들은 감지되기 전에 원하는 데이터를 유출하려고 노력하고 이 작업을 수행 할 수 있다. 또한 그들은 오랜 기간 동안 소량의 데이터를 유출하기 위하여 ‘낮은 속도와 느린’ 접근 방식을 선택할 수 있다.

· 유지(Maintenance)

공격자가 정보 수집 목적으로 네트워크에 대한 접근을 얻은 후에, 그들은 일반적으로 그들의 접근을 유지하려고 노력한다. 그들은 탐지를 피하기 위하

여 네트워크에 대해 그들이 발생시키는 악의적인 행위를 최소화하고, 네트워크 내의 백도어가 그들이 원하는 대로 작동하는 지를 확인하기 위해 주기적으로 통신을 수행하며, 적절하게 변경을 하게 된다. 만약 자동화된 데이터 수집 도구가 사용된다면 탐색 용어 또는 유출 경로, 유출된 데이터의 양 또는 빈도수를 수정하는 것과 관련될 수도 있다. 또한 유지 단계에서는 백도어와 통신하기 위하여 사용되는 임의의 중간 하부구조와 콜백 도메인을 유지하는 것을 필요로 할 수도 있다. 접근이 소실되면, 공격자는 접근을 얻기 위하여 단계 1(정찰)또는 단계 2(준비)로 되돌아 갈 수도 있다.[5]

2.5 APT 공격 대상

APT 형태의 보안 위협에 있어 그 위협의 대상은 보안 위협을 만들어내는 조직이 가지고 있는 목적들과 밀접한 관련이 있으며, 그 목적에 따라 그 대상 역시 다양하다. 그림 2는 APT 형태의 보안 위협에 대상이 되는 조직들을 보여주고 있다. APT공격의 대상이 되는 조직들은 정부기관, 사회 기간 산업 시설, 정보 통신 기업, 제조 업종 기업과 금융 업종 기업들과 같은 기관과 기업들이 주요 대상이 되고 있다. 이러한 기관과 기업들이 APT 형태의 보안 위협에 주요 대상이 된다는 점은 결국 해당 보안 위협을 만들어 내는 조직들이 가지고 있는 목적 자체가 정치적인 목적이 상반되는 조직에 대한 정치적인 행동 또는 경제적으로 커다란 이익을 확보할 수 있는 데이터 탈취가 가능한 기업이 된다는 것을 알 수 있다.[1]

그림 2. APT 형태의 보안 위협에 대상이 되는 조직들

- 정치적인 목적

일반적으로 정부기관과 사회 기간산업 시설이 APT 형태의 보안 위협에 주요 공격 대상이 되고 있다. 정부기관을 대상으로 하는 경우에는 생산한 APT 형태의 보안 위협을 이용해 국가 정부기관에서 보관 중인 특정 기밀문서를 탈취하거나 특정 정부 정책과 관련된 정보들을 확보하기 위해서이다. 또한 사회 기간산업 시설을 대상으로 하는 경우에는 일종의 사이버 테러리즘 활동으로 볼 수도 있다. 발전소 및 댐과 같이 사회 운영의 근간이 되는 기간산업 시설에 대해 APT 형태의 보안 위협으로 공격을 가하는 것은 해당 산업 시설들의 정상적인 동작을 방해하여 해당 국가 사회 전반의 정상적인 활동이 이루어지지 않도록 하기 위해서라고 볼 수 있다.[1]

- 경제적인 목적

일반적인 기업들이 대상이 되고 있으며 그 중에서도 소프트웨어나 통신 장비 등을 생산하는 첨단 정보통신 기업들과 함께 자동차, 선박, 가전제품 등을 생산하는 제조 업종의 기업들도 대상이 되고 있다. 그리고 은행, 증권사 등 금융 업종에 포함되는 기업들도 역시 APT 형태의 보안 위협들의 대상이 되고 있다. 이러한 일반적인 기업들이 대상이 되는 경우에는 일반적으로 산업 보안(Industrial Security, Corporate Security) 분야에서 언급하고 있는 주된 위협인 산업 스파이(Corporate Espionage) 활동의 일종으로 주로 경쟁 기업 내부의 주요 소프트웨어 소스코드, 제품의 설계도 등을 탈취하여 경쟁 기업의 제품 생산과 판매에 치명적인 손상을 가해 반사적인 이익을 얻기 위한 경제적인 목적이 가장 크다고 할 수 있다. 금융 업종 기업의 경우에는 경쟁 기업의 내부 재무 관련 기밀이나 비공개 투자 계획 문서 등을 탈취하여 경쟁 기업의 비즈니스 활동 전반에 걸친 타격을 주기 위한 목적도 가지고 있다.[1]

2.6 APT 보안 위협에 대한 대응방안

APT 형태의 보안 위협에 대응하기 위해서는 보다 체계적이고 전략적인 접근이 필요하며, 이를 위해 다양한 접근 방식이 존재할 수 있다. 먼저 사고 예방차원과 실제 위협으로 인한 보안사고가 발생한 단계에서의 방안은 다음 그림 3과 같다.

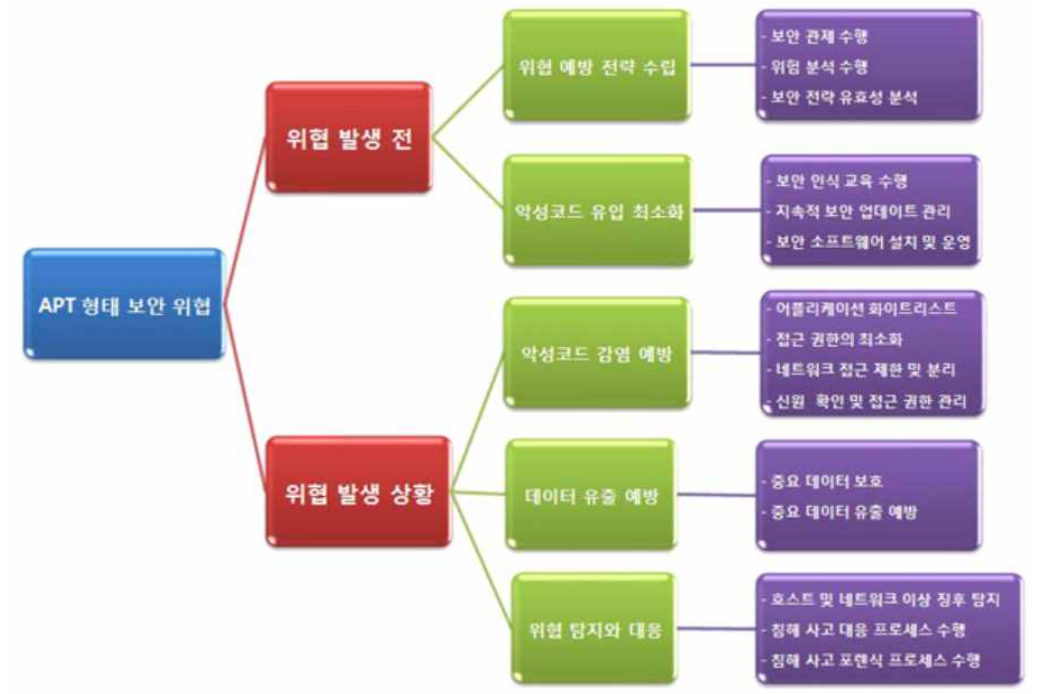

그림 3. APT 형태의 보안 위협에 대응하기 위한 방안

- 사고 예방 차원에서의 활동

APT 공격은 표적이 되는 대상의 보안 체계 분석을 바탕으로 여러 취약점을 분석하여 행해지기 때문에 이에 대한 대응을 위해서는 정기적인 보안 관제로 기업 내부 네트워크에서 침해사고로 간주 할 수 있는 이상 징후들이 발생하는지에 대한 주의 깊은 모니터링이 필요하다. 그리고 기업 내부에서 현재 사용하고 있는 보안정책들의 실효성에 대해 검토함과 동시에 조직의 종합적인 보안 위험을 분석하여 보안 체계를 재정비해야 한다. 보안 체계 정비를 위해서는 보안정책에서 보안 관리 및 운영에 대한 전체 사항을 세밀하게 체크하고, 조직의 위협을 분석하여 이에 대한 대응책을 수립하여야 한다. 보안 체계를 재정비한 후, 이 체계의 지속적인 운영을 위해서 보안 관리 조직을 중심으로 조직 전체적으로 보안 관리가 수행되도록 꾸준한 관리를 하는 것이 무엇보다 중요하다. 그리고 각각의 시스템들이 보관하고 있는 데이터들의 중요성과 기밀성에 따른 위험성 분석을 수행하여 보안사고가 발생하더라도 그 피해를 최소화 할 수 있는 방안을 수립하는 것이 중요하다고 할 수 있다.

APT 공격은 그 공격방법이 매우 다양하고 지속적이며, 치밀하기 때문에 이에 대응하기 위해 할 수 있는 가장 효과적인 방법 중 하나는 조직 구성원들의 적극적인 참여를 유도하는 것이다. 이를 위해서는 조직의 구성원 전체에 대한 효과적인 교육이 필요하며, 특히 보안 체계 분석 단계에서 APT 공격에 취약하다고 판단되는 임직원들을 구별하여 이들에게 APT 공격의 성격과 그 원리에 대해 교육한다면, 이들은 APT 공격에 대한 일차 방어선이 될 것이다.

APT 공격의 1차 목표는 엔드 포인트라고 할 수 있기 때문에, 엔드 포인트에 대한 보안은 APT 공격 대응에서 무엇보다도 중요하다. 엔드 포인트에서는 인터넷, 이메일, 메신저, P2P 등의 통신서비스뿐 아니라, USB 등의 매체를 통해서도 악성코드가 잠입할 수 있다. 최근에는 스마트워크 플랫폼이 확산됨에 따라 엔드 포인트에 대한 보안은 더욱 취약해지고 있다. 이러한 제약사항에도 불구하고 엔드 포인트 보안은 조직 내 모든 엔드 포인트에서 반드시 적용되어야 한다. 그 주요 내용으로는 운영체계 등에 대한 보안 업데이트, 보안 소프트웨어 설치 및 운용, 화이트리스트 기반 애플리케이션 제어 등을 들 수 있다.

대부분의 APT 공격들은 조직 내 취약 지점을 통해 시스템 접근 권한을 가진 계정정보를 취득하여 이루어진다. 따라서 조직에서 보호하고자 하는 중요 정보에 대한 접근 권한 관리는 APT 공격 대응을 위해서 매우 중요하다. 이를 위해서는 먼저 중요 정보에 접근하는 권한을 가진 사람을 최소화 하여야 하며, 정보의 중요도에 따라 접근 권한을 세분화하고, 중요도가 높은 정보의 경우에는 사람에 대한 인증뿐만 아니라 기기에 대한 인증을 추가하는 등의 권한 관리를 전략적으로 수행하여야 한다. 또한 퇴직자 또는 휴가자 등 권한의 영구 또는 일시 소멸되는 경우, 이 정보가 조직 내 보안 운영에 즉각적이고 지속적으로 반영되도록 하여야 한다.

APT 공격의 최후 목표는 중요 정보이기 때문에, 중요 정보에 대한 직접적인 보안은 APT 공격 대응의 중요한 요소 중 하나라고 할 수 있다. 따라서 조직 내 중요 정보는 기본적으로 암호화하여 저장함으로써 정보 유출이 발생하더라도 해커들이 이에 대한 해독을 불가능하게 또는 매우 어렵게 하는 것이 무엇보다도 중요하다. 특히 중요 정보의 저장 형태에 따라 정보의 유출은 여러 가지 형태로 변형되어 시도될 수 있으므로, 이를 위해서 DLP(Data Loss Prevention) 제품을 운영 하는 것도 하나의 안전장치가 될 것이다.[4]

APT 형태의 보안 위협들에서는 그 목적을 달성하기 위한 하나의 수단으로 악성코드가 제작되어 사용되므로, 모든 시스템들과 클라이언트들에는 보안 소

프트웨어들을 설치하여 운영하도록 하며 주기적으로 운영되고 있는 보안 소프트웨어와 보안 장비들의 업데이트 및 관리를 하는 것이 중요하다.

- 위협이 발생하였을 경우의 방안

위협 발생 전의 단계가 침해사고 예방적인 관점에서의 접근이었다면 실제 APT 형태의 위협이 발생한 것을 인지하였거나 유사한 형태의 보안사고가 발생한 것으로 간주 된다면 크게 세 가지 형태로 나누어서 접근 할 필요가 있다.

첫 번째로 기업 내부 네트워크의 시스템들에 악성코드가 감염되는 것을 막도록 한다. 이를 위해 기업 내부에서 검토하고 인증한 애플리케이션들을 대상으로 화이트리스트(White List)를 작성하여 해당 애플리케이션들 외에 임의로 다른 애플리케이션들을 설치 및 실행되지 않도록 차단한다. 그리고 중요 시스템들에서는 확인되지 않거나 인가되지 않은 계정들의 접근 권한을 최소화 및 차단하고 네트워크 역시 중요 시스템들이 있는 네트워크 대역과 일반 임직원들이 사용하는 네트워크 대역을 분리 및 차단하여 원천적인 접근을 제어하는 것도 방안이다.

두 번째로 APT 형태의 보안 위협들이 최종적으로 시도하는 형태는 데이터의 파괴나 탈취이기 때문에 실제 위협이 발생한 것으로 파악되는 상황이라면 기업 내부 기밀 데이터가 보관 중인 시스템과 데이터의 로그정보의 연관성 분석에 의해 비정상적인 접근이나 데이터 전송 유무 등으로 유출징후에 대한 파악을 수행한다. 만약 유출 징후가 확인되면 이를 차단하기 위해 침해사고 대응 프로세스를 따라 보안 대응 정책의 생성 및 전파를 통한 단계적 조치를 수행한다.

마지막으로 실제 보안 위협이 어떠한 경로로 기업 내부 네트워크로 침입을 하였으며 어떠한 시스템과 데이터에 대해 접근을 시도하여 어떤 정보를 유출하였는지 파악하는 과정이 필요하며 이를 위해 디지털 포렌식(Digital Forensic) 프로세스에 따라 자세한 분석을 진행한다.[1]

2.7 APT 공격 대응 단계 분류 사례

이러한 APT 공격에 대한 단계 분류 및 대응방안에 대한 국내외 주요 보안업체의 현황을 살펴보면 아래와 같다.

2.7.1 안랩(Ahn Lab.)

안랩에서는 APT 공격 프로세스를 분석하고 단계별 대응방안을 연구 중에 있다. 안랩에서 분석한 APT 공격 진행 프로세스는 다음 그림 4와 같다.[6]

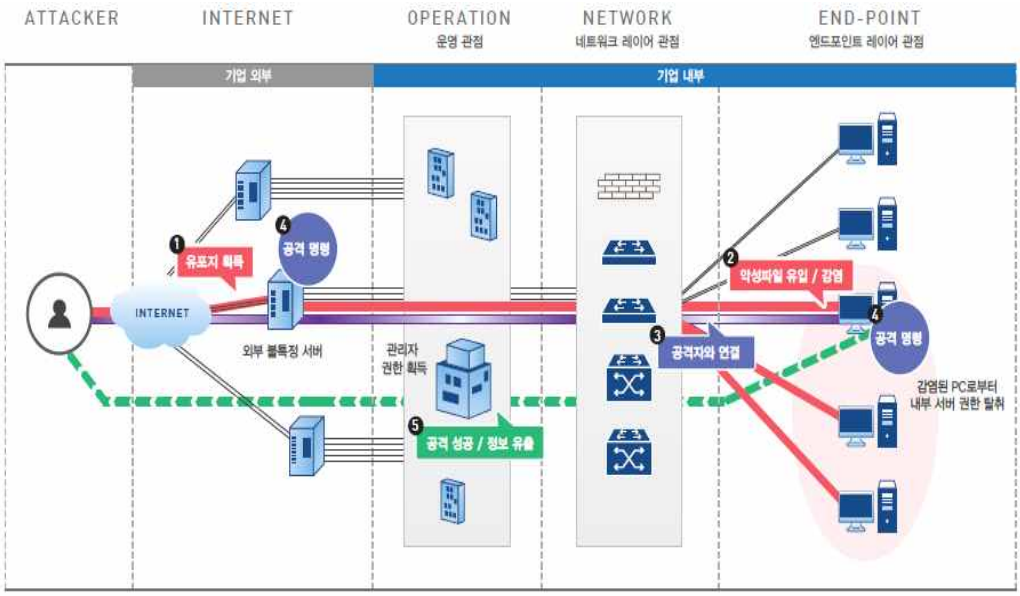

그림 4. 안랩 APT 공격 진행 프로세스

안랩에서는 APT 공격을 공격 준비 · 악성코드 유포 시도 · 악성코드 감염 및 공격자의 침입 · 보안사고 · 공격 종료 등 다섯 단계로 이루어진다고 분석하고 있다. 각 단계별 상세 내용은 다음과 같다.[6]

- 단계 1. 공격 준비 단계

공격자는 특정 또는 불특정 다수에게 악성코드를 배포하기 위하여 여러 형태의 공격을 준비한다. 최근 악성코드의 배포 동향을 살펴보면, 악성코드를 직접 전파하기보다는 일반 사용자에게 많이 알려진 사이트의 웹 서버를 통한 배포가 주류를 이루고 있다. 공격자들은 SQL 인젝션, 서버 권한 획득 등의 기법을 이용하여 웹 서버에 악성코드를 업로드 한다. 이렇게 공격에 이용된 웹에 일반 사용자가 접근했을 때 악성코드를 자동으로 다운로드하거나 혹은 메일

등을 이용하여 일반 사용자가 악성코드를 다운로드할 수 있도록 유도한다. 최신 보안 위협 사례를 살펴보면, 웹 또는 특정 서버에 악성코드를 다운로드하게 하는 것뿐만 아니라 특정 프로그램의 업데이트 서버를 이용하여 악성코드를 유포하는 방식도 이용되고 있다. 이는 최근의 PC용 프로그램들이 자동 업데이트 기능을 이용하여 인터넷상에서 해당 프로그램들이 자동으로 업데이트 파일을 다운로드하게 하는 것을 악용한 것이다. 즉 업데이트 서버를 해킹하여 자동 업데이트 시 사용자도 모르게 악성코드가 다운로드 되고, 자동으로 실행되어 PC가 악성코드에 감염되는 경우이다. 만약 이러한 방법을 이용해 특정 대상만 악성코드를 다운로드할 수 있게 제한을 걸어둔다면, 바로 ‘APT 공격’의 가장 기초적인 공격 준비 단계가 되는 것이다.

- 단계 2. 악성코드 유포 시도 단계

공격자가 악성코드를 준비하는 단계가 끝나면, 그 다음 과정으로 공격자는 해당 PC가 악성코드를 다운로드하고, 실행할 수 있도록 끊임없이 유도한다. 가장 대표적인 예가 우리가 일상생활에서 가장 많이 접하는 메일을 이용한 악성코드 유포이다. 물론 단순히 메일에 악성코드를 첨부한다면 감염률은 그리 높지 않을 것이다. 하지만 공격자는 더 많은 감염을 유발하기 위하여 사회공학적 기법을 이용한다. 예를 들어 당시 가장 큰 사회적 반향을 일으키는 화제의 키워드를 이용해 메일이나 인터넷 검색을 통해 해당 페이지를 열어보도록 유도한다. 이때 해당 페이지를 방문한 사용자 PC에는 악성코드가 다운로드 되고 감염이 진행된다. 실제 국외에서 발생한 APT 공격 사례를 보면, ‘연봉 협상’과 관련한 내부 메일을 가장하여 메일을 발송한 후 내부 직원들이 그 메일을 열어보도록 유도한 일이 있었다.

- 단계 3. 악성코드 감염 및 공격자의 침입 단계

악성코드에 감염되면, 해당 악성코드는 공격자와의 연결을 시도한다. 이후 공격자는 감염된 PC를 마음대로 조종할 수 있게 된다. 이것이 소위 좀비(Zombie) PC라고 이야기하는 것이다. 공격자는 장악한 감염 PC를 조작할 수 있는 권한을 획득하였으므로, PC의 중요 자료나 개인정보를 마음대로 가져갈 수가 있다. 하지만 APT 공격의 경우 공격자가 목표로 하는 기관 또는 기업의 주요 정보를 획득할 때까지 장악한 PC를 점진적이고 지속적으로 이용하는 것이 가장 큰 특징이다.

예를 들어 만약 장악한 PC가 내부 일반 직원의 PC라면, 이 PC를 주요 자원

으로 접근할 수 있는 또 다른 PC를 장악하는 수단으로 활용할 수 있다. 이미 알려진 ARP 스푸핑(Spoofing)이나 패킷 스니핑(Sniffing)을 통하여 내부 네트워크상에 있는 다른 PC 정보를 획득하고, 이를 바탕으로 주요 정보/자산 관리자의 PC 정보를 획득하는 단계에 이르게 된다. 이후 관리자 PC를 획득하기 위하여 앞서 설명한 두 번째 단계인 악성코드 유포 시도를 수행할 수 있다.

이해를 돕기 위해 가상의 시나리오를 만들어보자. 공격자가 장악한 PC를 이용하여 내부 직원이 관리자에게 업무 요청 등의 메일을 보내는 형태로 침입을 시도하고, 이때 악성코드를 다운로드할 수 있도록 한다면 충분히 관리자 권한의 PC까지 감염시킬 수 있게 된다. 또한 이미 공격자의 손에 들어온 PC는 인터넷을 통하여 추가적인 악성코드를 다운로드할 수 있다. 예를 들어 공격자가 이미 감염을 유발한 악성코드가 2차 보안 사고를 일으키기에 기능이 부족하다고 판단하면, 공격자는 장악한 PC에 있는 프로그램을 추가 공격 기능이 포함된 악성코드로 업그레이드 할 수 있다.

특히, 앞선 예와 같이 추가적으로 다운로드한 악성코드 여러 개가 모여 비로소 실제적인 보안 사고를 일으킬 수 있는 형태가 되는 악성코드의 모듈화가 최신 트렌드이다. 이 경우 개별적인 악성코드를 보면 일반적인 악성 행위를 하는 것으로 판단되지만, 모듈이 모이게 되면 기존에 분석되었던 위험성보다도 훨씬 높은 위험성을 가지는 악성코드로 자체 진화하는 것이다. 그러므로 이러한 악성코드의 모듈화에 난독화 과정까지 추가하게 되면 기존의 보안 위협 대응체계를 무력화할 수 있는 가장 진화된 보안 위협이라고 이야기할 수 있다.

- 단계 4. 보안사고 단계

세 번째 단계를 통해 주요 정보 및 자산에 접근할 수 있는 권한이 획득되면, 이는 공격자가 목적한 것을 이룰 수 있는 단계에 진입한 것이다. 특히, 감염된 PC가 보안 관리자에게 노출되지 않도록 이미 장악한 PC는 악성코드의 활동을 중단시키는 형태로 은폐하는 것도 최근 APT 공격 양상의 특징이다. 4단계에 이르면 공격자는 내부 주요 정보가 저장되어 있는 데이터베이스를 파일로 백업한 후 외부로 전송할 수도 있고, 시스템 마비가 목적이라면 주요 정보 삭제 또는 시스템 장애 등을 유발할 수도 있다.

- 단계 5. 공격 종료 단계

마지막 단계인 공격 종료는 공격자의 특성에 따라 수행할 수도 있고, 수행하지 않을 수도 있다. 스파이와 같이 완전히 은밀한 형태의 공격을 원하는 공

격자의 경우에는 공격 종료 단계에서 자신의 흔적을 지울 수 있다. 반면에 협박 등 추가적인 행위를 위해서 자신의 침해사고 행위를 노출할 수도 있다. 이때에 이르러서야 기관이나 기업에서는 침해사고가 일어났다는 것을 비로소 인지하게 되는 것이다. 그러나 공격은 이미 종료되었으며, 대응하지 못하였다면 피해는 이미 발생한 것이다.[6]

2.7.2 델 시큐어웍스(DELL SecureWorks)

델 시큐어웍스에서도 APT 공격 프로세스를 분석하고 단계별 대응방안을 연구 중에 있다. 델 시큐어웍스에서 분석한 APT 침입의 일반적인 단계는 다음 그림 5와 같다. 공격자들은 병렬로 다중 공격을 수행할 수 있으며, 각 공격은 일련의 단계들로 나누어 질수 있다. 준비와 초기 진입점을 획득하는 단계들은 사전 요구사항들이다. 공격의 다른 부분들은 병렬로 처리될 수 있으며 효율성을 위하여 이용될 수 있는 몇 개의 동작들로 나누어 질 수 있다.[7]

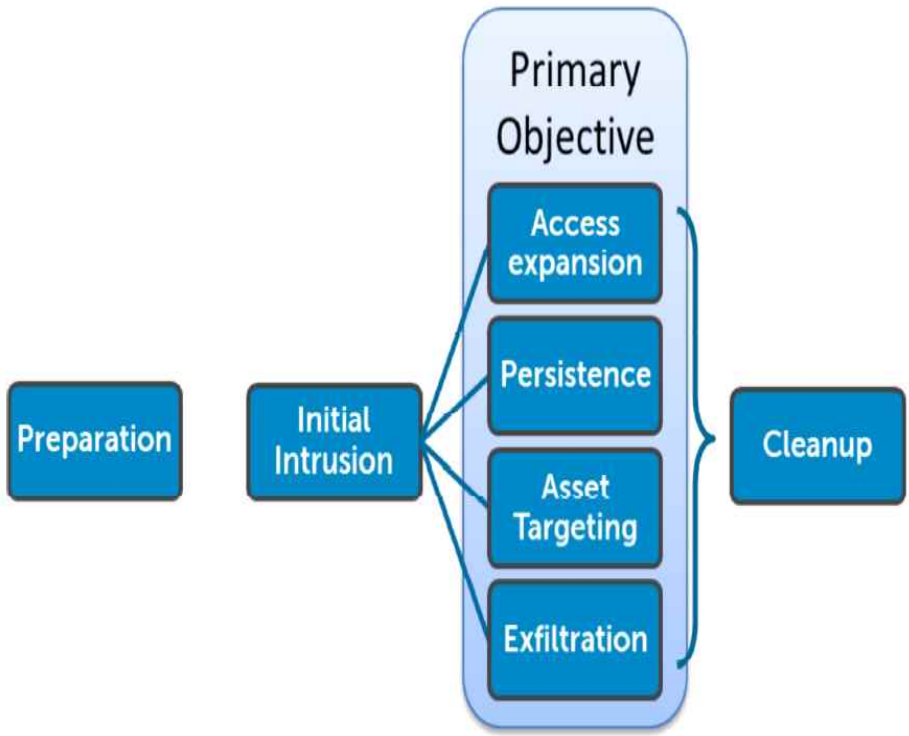

그림 5. 델 시큐어웍스사의 APT 침입 단계 분석

델 시큐어웍스사의 APT 침입 단계 분석에서 각 단계별 상세내용은 다음과 같다.

- 단계 1. 준비(Preparation)

APT 공격은 일반적으로 높은 수준의 준비와 관련이 되어 있다. 계획이 수행되기 전에 추가적인 자산과 데이터가 필요할 수 있으며, 매우 복잡한 과정들이 주요 목표에 대한 공격 계획 수행 이전에 필요하다. 준비 단계에서 공격자들은 자신의 계획을 수행하기 위해 필요한 구성요소들을 나열하고 해당 구성요소들을 수집하기 시작한다. 이 구성요소들에는 인프라구조, 도구, 데이터, 목표 환경에 대한 정보, 그 외 다른 필요한 자산들이 포함된다. 공격자들은 보안 제어와 침입을 수행하고 대응방안을 수립하기에 필요한 절차들에 관한 지식을 모으기도 한다.

- 단계 2. 초기 침입(Initial Intrusion)

공격자들이 준비를 마친 후에, 다음 단계로 목표 환경의 기본 진입점을 획득하기 위하여 시도를 수행한다. 매우 일반적인 침입 전략은 웹 링크 또는 부가 파일을 포함하고 있는 스피어 피싱 메일을 사용하는 것이다. 이메일 링크는 공격자가 사회공학적인 공격을 시도할 수 있는 장소를 연결하게 된다. 성공적으로 침입이 되고나면, 표적 컴퓨터에 초기 맬웨어(Malware)가 설치되게 된다.

- 단계 3. 확장(Access expansion)

어떤 경우에는 악용의 대상이 단일 시스템일 수 있으며, 이때에는 초기 침입 후에 목적에 대한 접근이 가능하기 때문에 더 이상 접근에 대한 확장이 필요 없게 된다. 그러나 많은 경우에 공격자의 목적을 완성하기 위하여 한 개의 시스템이나 데이터 저장소보다 많은 곳에 접근을 필요로 하게 된다. 이 경우에 초기 침입 후에 공격자들에 의해 수행되는 첫 번째 행위가 접근의 확장이다.

이 단계의 목적은 추가적인 시스템에 대한 접근과 차후의 시스템들에 대한 접근을 허용하게 해주는 인증정보에 대한 접근을 얻는 것이다. 영역 레벨 관리 권한을 얻기 위한 일반적인 형태는 먼저 초기 표적에 대한 관리권한을 얻고, 초기 표적에 로그인한 영역 관리자 계정에 대한 인증서를 획득한 다음 다른 시스템에 대한 접근권한을 얻기 위하여 획득한 인증서를 사용하는 것이다.

- 단계 4. 지속(Persistence)

표적의 방어를 극복하고 네트워크 내부의 진입점을 설치하는 것은 많은 노력을 필요로 할 수 있다. 그래서 공격자가 진입점을 설치한 시점부터 표적의 자산이나 데이터에 대한 활용이 더 이상 필요 없는 시점까지, 공격자는 접근을 유지하기 위하여 다양한 기법들을 사용한다. 공격자들은 대부분의 조직들이 자신의 환경에서 안티 바이러스 도구들을 사용한다는 것을 알고 있다. 이런 가정 하에 공격자들은 자신들의 도구가 탐지되지 않도록 하는 단계를 수행한다. 이것은 일반적으로 맬웨어를 생성하거나 일반적으로 사용되는 도구를 재작성하거나 재포장하는 것을 의미한다. 이렇게 최적화된 도구들은 공격자들이 탐지되는지 여부를 평가하기 위하여 최신의 안티 바이러스 도구와 다른 보안 도구들에 대하여 시험을 수행하게 된다. 도구들이 모든 검색을 통과할 때까지 계속 수정된다. 공격자들은 표적 시스템이 사용하는 것과 같은 보안 도구들을 사용할 수 있기 때문에, 이 과정은 매우 효과적이다.

- 단계 5. 탐색과 유출(Search & Exfiltration)

네트워크 악용의 궁극적인 목표는 일반적으로 미래 악용을 위해 사용될 수 있는 자원이나 침입자에게 가치가 있는 문서나 데이터들이다. 많은 경우에 공격자들은 공격을 시작하기 전에 특정한 문서나 데이터 형태를 염두에 두게 된다. 또 다른 경우로 공격자들은 표적의 네트워크나 시스템의 어느 곳에 가치 있는 데이터가 있다는 것을 알지만, 가치 있는 데이터가 저장된 장소는 확신하지 못할 수도 있다. 탐색과 유출에 대한 가장 선호하는 방식은 흥미 있는 네트워크로부터 모든 것을 가지고 오는 것이다. 이것은 모든 문서, 이메일, 네트워크에서 발견 가능한 다른 모든 형태의 데이터를 의미한다. 파일 확장자에 기초하여 문서들을 수집하는 것도 선호되는 방식이다. 또 다른 방식으로 공격자가 표적 환경에 대한 특정한 흥미로운 속성이나 응용 프로그램을 알고 있다면 그것이 표적이 될 수도 있다.

- 단계 6. 정화(Cleanup)

침입한 동안에 정화노력은 탐지를 회피하는 것과 침입 증거와 표적이 되었다는 증거를 삭제하는 것과, 이벤트 이후에 남게 되는 증거를 삭제하는 것에 중점을 두게 된다. 가끔 정화는 다른 방향으로의 유도를 목적으로 환경 내의 데이터를 조작하거나 주입하게 된다. 공격자가 자신의 흔적을 더 잘 숨길수록, 피해자는 침입의 영향을 평가하기가 더욱 어렵게 된다.[7]

2.7.3 웹센스(Websense)

웹센스 사에서도 APT 공격 프로세스를 분석하고 단계별 대응방안을 연구 중에 있다. 웹센스 사에서는 다음과 같이 3단계로 APT 공격을 분석하고 있다.[8]

- 단계 1. 정찰, 착수, 전염

공격자는 정찰을 수행하여 취약성을 식별하고, 공격을 시작하여 표적 호스트를 전염시킨다.

- 단계 2. 제어, 갱신, 발견, 지속

공격자는 전염된 호스트를 제어하고, 코드를 갱신하며, 다른 기계들로 확산시키고, 타겟 데이터를 발견하고 수집한다.

- 단계 3. 추출, 행위수행

공격자는 타겟 네트워크로부터 데이터를 추출하고 악성 행위를 수행한다.

웹센스 사에서는 APT 공격을 막기 위한 요구사항으로 내용 인식, 문맥 인식, 데이터 인식을 중시하고 있으며, APT 공격 방어를 위하여 Websense Advanced Classification Engine(ACE)를 제안하고 있다. ACE는 내용 보안 위협 탐지 엔진으로 웹 보안, 이메일 보안, DLP(Data loss prevention)를 제공하며, 이를 기반으로 내용 보안 및 문맥 보안을 수행할 수 있다고 제시하고 있으며, 각 단계별 대응방안으로 TRITON 아키텍처를 제시하고 있다. 다음 그림 6은 ACE 엔진이고 이 엔진의 각 기능을 함께 조합하여 이용함으로써 내용 보안 및 문맥 보안을 수행한다.

그림 6. 웹센스사의 Advanced Classification Engine(ACE)

다음 그림 7은 TRITON 아키텍처로 웹센스 사에서 APT 공격을 분석한 각 단계별로 대응방안을 제시하고 있다. 먼저 중요한 데이터 재산과 고용인들을 식별하고, 단계 1에서 전염을 방지하며, 단계2 에서는 서버 명령 제어를 식별하고, 단계 3에서는 데이터 추출을 방지한다. 그리고 전염된 호스트와 데이터 유출 시도를 식별하며, 이벤트의 영향을 측정하고, 공격에 대응하고 방어 대책을 수립한다.[8]

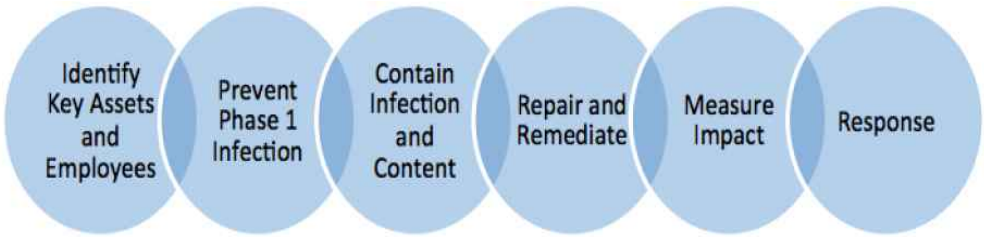

그림 7. 웹센스사의 TRITON 구조

2.7.4 트랜드마이크로(Trendmicro)

트랜드마이크로사는 다음과 같은 여섯 가지 단계로 APT 공격을 분석하고 이에 대한 대응방안을 제공하고 있다.[9]

- 단계 1. Intelligence Gathering

잘 알려진 소스(LinkedIn, Facebook, etc)를 통해 각각의 대상을 찾고 선정하며, 요구에 맞는 공격을 준비한다.

- 단계 2. Point of Entry

일반적으로 사회공학적 방법(email/IM or drive by download)을 이용하여 제로데이 맬웨어를 초기에 표적에 감염시킨다. 그 결과 백도어가 생성되게 되고 이에 네트워크 침투가 가능하게 된다. (또는 웹 사이트 취약점을 이용하거나 네트워크에 직접 해킹을 시도한다.)

- 단계 3. Command & Control (C&C)

해커는 침투한 호스트를 감시/제어할 수 있게 되고, 해당 맬웨어로 차후 목적까지 지속적인 이용이 가능하게 된다.

- 단계 4. Lateral Movement

해커는 같은 네트워크의 타 호스트들에 추가침투를 진행하고 기밀 정보를 탈취하며, 권한을 얻어 지속적 감시/제어를 수행한다.

- 단계 5. Asset/Data Discovery

몇몇 테크닉(ex. Port scanning)을 사용하여 주목할 만한 서버나 서비스를 확인 하고 관심 있는 데이터를 수집한다.

- 단계 6. Data Exfiltration

일단 중요 정보가 수집되면, 데이터는 내부 침투된 시스템으로 전송되고, 이후 압축 및 간혹 암호화 하여 외부로 전송한다.[8]

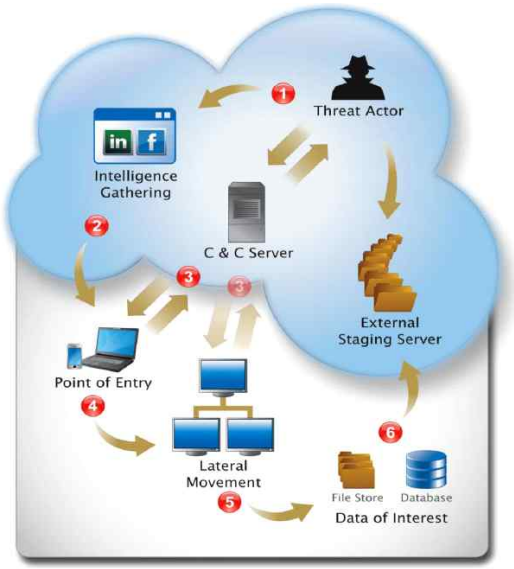

그림 8. 트랜드마이크로 APT 공격 단계 분석

트랜드마이크로사는 APT 공격 대응방안으로 좀비PC 탐지 및 치료 솔루션 '딥 디스커버리(Deep Discovery)'와 물리·가상·클라우드 서버 보안 솔루션 '딥 시큐리티(Deep Security)', 악성코드 관제 솔루션 'TIM'으로 포트폴리오를 제시했다. 트랜드마이크로 딥 시큐리티는 숨겨진 위협을 조기에 탐지하고 정밀 분석하여 정보유출을 시도하는 좀비PC를 자동으로 치료하는 원스톱 APT 보안 솔루션이다. 딥 시큐리티는 알려진 악성코드뿐만 아니라 네트워크 행위 기반으로 의심스러운 통신 및 알려지지 않은 악성코드를 탐지하여 은밀하게 침입해오는 예상할 수 없는 위협을 조기에 탐지한다. 전용 엔진과 샌드 박스(Sandbox)를 통한 정밀 분석으로 실질적인 위협을 검증하고 이를 바탕으로

감염된 PC를 자동으로 치료하여 좀비PC로 인한 정보유출 사고를 미연에 방지한다. 끊임없는 모니터링으로 잠재된 위협에 대해 조기에 대처하고 탐지, 분석, 치료와 보고를 한 번에 제공함으로써 사전에 방지가 가능한 종합적인 APT 대책이 가능하게 된다. 모든 네트워크 트래픽을 서비스에 영향 없이 미러 방식으로 감시하여 악성 컨텐츠 및 통신을 탐지하고 공격 행위 재현 확인 및 상관관계 분석을 통한 검증을 통하여 실시간 위험 분석을 수행한다. 다음 그림 9는 선제적 APT 공격 분석 및 대응방안 개념도이다.[9][10]

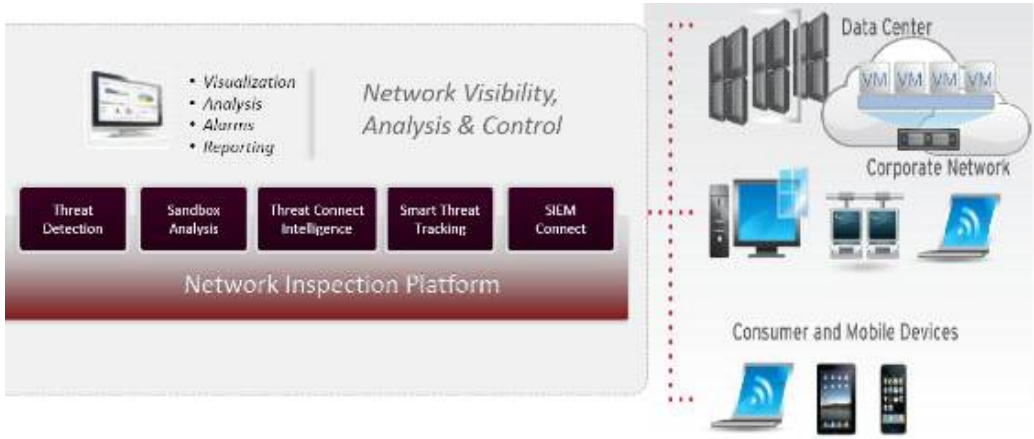

그림 9. 트랜드마이크로 선제적 APT 공격 분석 및 대응방안

2.7.5 IBM

IBM사는 APT등 고도화된 위협을 방지하기 위하여 다 계층 방어 개념을 사용하여 X-FORCE 보안 연구소의 끊임없는 연구 개발 노력으로 선제적 보안을 제공하고 있다. IBM사의 다 계층 방어의 핵심은 다 계층 방어 엔진 PAM (Protocol Analysis Module)으로, 이 엔진은 IBM 위협 완화 보안 솔루션의 핵심 엔진으로 네트워크 트래픽과 컨텐츠를 인지하고 분석하며, 업계 최대인 247개의 프로토콜 및 데이터 파일 포맷을 분석한다. 또한 이 엔진은 스무 가지 이상의 탐지 분석 기법을 사용하며 IP Frag, TCP Stream Frag, RPC Frag, URL 난독화 등과 같은 우회 공격에 대한 탁월한 대응을 수행한다. 그리고 이 엔진은 IBM X-FORCE 보안연구소에 의해 검증된 취약점 (Vulnerability) 분석기반의 위협 탐지 및 방어를 제공한다. 다음 그림 10은 IBM 다 계층 방어 엔진 개념도이다. IBM사는 보안정책에 따라 ActiveX

/Suspicious ActiveX, HTTP/Email_Executable/DLL, P2P, IM, Tunneling, TOR, 봇넷 활동, 특정 통신 Connection 등 네트워크 애플리케이션, 서비스 접근에 대한 허용/차단을 모니터링 한다. 그리고 IBM사의 Virtual Patch Technology는 소프트웨어 패치와 독립적으로 취약점을 노리는 공격을 선제적으로 방어하며, 긴급 보안패치가 발표된 경우, 서비스 중단 없이 해당 공격으로부터 보호를 수행한다. 또한 패치관리 프로세스에 유연성을 제공하고 정해진 유지보수 시간에 패치를 할 수 있도록 패치관리 프로세스에 일조한다. 그리고 One-Click으로 자산에 대해 패치효과를 구현한다. 또한 IBM사는 Client Side 애플리케이션 보호를 위하여 파일 포맷 취약점을 공격하는 Shellcode를 행위기반으로 인식하여 차단하는 Shellcode Heuristics (SCH)을 사용한다. 이 방식은 IBM X-FORCE 특허 기술로 2006년 3월 PAM 엔진에 탑재되었으며, 시그니처 갱신 없이 Microsoft Office 관련 신규 취약점의 80% 이상을 탐지한다. VML(MS06-055), XML(MS06-071)와 같은 여러 가지의 IE 취약점을 발견했으며, 2천 2백만 개의 미디어 파일에서 2개의 오탐율을 기록했다.[11]

그림10. IBM 다계층 방어 엔진

IBM사는 컴플라이언스 요구 사항과 진화하는 위협에 대응하고 Web Application, Web 2.0, 데이터베이스를 보호하기 위하여 웹 애플리케이션 방화벽(WAF) 기능을 제공하며, 행위기반의 인젝션 공격 방어 엔진인 ILE (Injection Logic Engine)를 탑재하여 다양한 공격으로 부터 보호를 수행한다. IBM사는 네트워크상의 데이터 흐름을 파악하고 잠재적 위험이 존재하는지 파악/결정하는데 도움을 주기 위하여 개인정보(PII) 및 기밀 정보를 인식하고 모니터링하며, 유연하고 커스터마이징 가능한 데이터 검색을 제공하여 기업의 데이터 보안 전략을 보완해 준다.[11]

2.7.6 EMC RSA

EMC RSA사는 다음 그림 11과 같은 여섯 가지 단계로 APT 공격을 분석하고 이에 대한 대응방안을 제공하고 있다. EMC RSA사는 NetWitness를 사용하여 APT와 같은 고도화된 공격에 대한 대응방안을 제공하고 있다. EMC RSA의 NetWitness의 주요 특징은 다음과 같다.[12]

- 알려지지 않은 악성코드 탐지 : 실행 파일의 특성, 유입 경로, 행위를 기반으로 알려지지 않은 신규/변종 악성코드를 탐지한다.
- 악성코드 / 좀비PC의 외부 접속 행위 탐지 : 네트워크 트래픽 분석을 통해 악성코드에 감염된 좀비PC가 외부의 해커에게 접속하는 행위를 탐지한다.
- 모든 네트워크 트래픽 저장 / 분석 : 모든 네트워크 트래픽을 저장하고 분석할 수 있는 기능을 제공하여 허용되지 않은 외부 접속 행위 탐지, 악성코드 유입경로를 추적한다.
- 최신 공격 정보 활용 : 최신 공격 패턴, 악성코드 배포지점, 좀비 PC 원격조정 지점 정보 등을 실시간으로 자동 업데이트하여 공격 탐지에 활용한다 .

그림 11. EMC RSA APT 공격 단계 분석

EMC RSA사의 NetWitness NextGen은 Decoder, Concentrator 그리고 Broker 등 세 가지 핵심 구성 요소를 통해 네트워크 상황을 정확하게 파악하여, 그에 대한 정확한 대책을 강구하고 상황을 인식하며, 지속적인 모니터링 능력을 확보할 수 있는 단일 코어 보안 플랫폼이다. 네트워크 토폴로지와 필요한 성능에 따라 NextGen의 구성 요소 전체 혹은 일부를 이용하여 인프라를 유연하게 구축할 수 있으며, NextGen 인프라는 NextGen AppSuite 제품인 Investigator, Informer, Visualize, Live 및 SIEMLink와 직접 호환되도록 설계되어 있다. 사용자는 NetWitness의 개방형 API/SDK를 활용함으로써 운영 요건과 비즈니스 요건을 충족하는 맞춤형 애플리케이션을 직접 생성하여 NextGen 플랫폼과 원활하게 통합하고 기존 보안 투자를 보호할 수 있다. 고객은 모든 정보에 즉시 접근할 수 있으므로 신종 위협에 대응하고 비즈니스 프로세스에서 발생한 문제를 파악하는 한편, 의도적인 데이터 유출을 막을 수 있게 된다. 전사적 네트워크의 데이터 기록 및 분석 인프라의 토대이자 핵심 요소인 Decoder는 다양한 사용자 설정을 지원하는 네트워크 어플라이언스로서 모든 네트워크 데이터를 실시간으로 수집, 분류 및 분석할 수 있도록 해준다. 기존 여타 패킷 수집 제품이나 네트워크 모니터링 제품과 달리 Decoder는 전체 세션을 실시간으로 분석할 수 있도록 OSI 모델의 모든 계층에서 네트워크 트래픽을 완전하게 재구성하여 전체적으로 표준화한다. 모든 네트워크 계층과 사용자 애플리케이션에서 검색 가능한 메타데이터로 구성된 완벽한 체계를 탄력적으로 생성하는 네트워크 모니터링 특허 기술이 적용된 Decoder는 분석에 필요한 메타데이터를 Decoder에서 실시간으로 수집하는 Concentrator 및 네트워크 전체에 대한 포괄적인 실시간 모니터링 능력을 제공하는 Broker와 연동되도록 설계되어 있다. Concentrator는 메타데이터를 계층적으로 수집하여 기업 전용 네트워크 토폴로지 및 물리적 장소에서 확장성과 유연성을 확보할 수 있도록 설계되어 있다. 필요한 계층에 구성할 수 있으므로 다수의 Decoder 수집 장소에 대한 가시성과 고가용성이 보장된다는 특징이 있다. Broker는 NextGen 인프라의 최상위 계층에서 가동된다. Broker는 다수의 Concentrator가 사용되는 전사적 구성 환경에서 원활하게 쿼리를 처리하고 모든 NextGen 메타데이터에 대한 단일 접속점(single point of access)을 제공하며 네트워크 지연 시간, 처리 속도 및 데이터 볼륨에 구애 받지 않고 모든 네트워크 환경에서 운용 및 확장할 수 있도록 설계되어 있다.

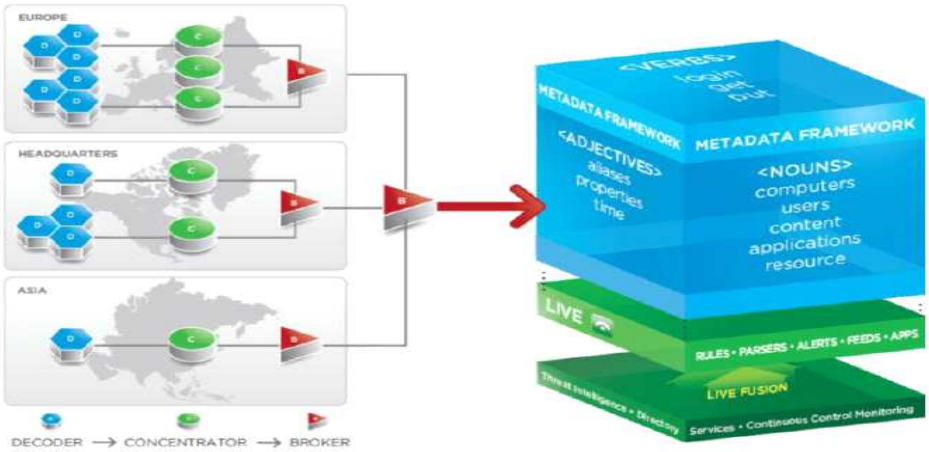

그림 12. NetWitness NextGen Platform

NetWitness AppSuite의 구성 요소 중 하나인 Informer는 전사적 시각화, 경보, 보고 및 실시간 상황 분석용 애플리케이션으로, 모든 세션, 통신, 서비스, 애플리케이션 및 사용자의 활동을 분석할 수 있어서 적용 분야가 넓다. Informer의 규칙 기반 접근법과 대시보드를 이용하면 제로데이 악성코드, 봇넷, 정책 회피 전술, 의도적인 데이터 유출, 변칙적인 통신, 규정 허점 및 네트워크의 기타 동향을 쉽게 파악할 수 있으며, 양방향 웹 기반 사용자 인터페이스(UI)를 지원하여 경보 기록 보기, 도표 작성 및 타일 방식 보기가 가능하다. Informer의 사용자 인터페이스를 이용할 경우 사용자의 기술 수준에 관계없이 자신만의 맞춤형 경보, 조회, 보고 및 규칙을 쉽게 구축할 수 있다. Informer는 기존의 보안 작업 프로세스와 통합되며 이전과 다른 수준의 실시간 상황 인식 기능을 제공하도록 설계되어 있다.[12]

NextGen AppSuite 제품 중의 하나인 Visualize는 마우스나 손가락(멀티-터치 모니터가 설치된 경우)으로 사용자(예: 분석가, 사고 대응 담당자, 조사관)가 수집한 트래픽을 확대/축소하고 시간별로 발생한 사건을 정확히 분석 및 확인할 수 있는 분석 솔루션이다. Visualize를 이용할 경우 또한 Informer에서 구축한 모든 규칙, 키워드 검색 및 기타 필터를 활용해 확보한 정보를 처리 할 수 있다. 이런 이유로 보안 관리의 효율성과 정확도가 크게 개선된다.

RSA NetWitness Investigator는 NetWitness NextGen 인프라에 수집된 대량의 정보를 다양한 방식으로 분석할 수 있다. 179개국 5만 명 이상의 보안 전

문가들이 NetWitness Investigator를 이용하고 있다. Investigator는 NextGen Metadata Framework를 이용하여, 데이터 수집 시점에 세션을 재구축하면서 NextGen이 분석한 실제 애플리케이션 계층의 내용과 상황에 대한 지표 역할을 한다. Investigator는 맞춤형 사용자 인터페이스와 뛰어난 분석 능력으로 사용자가 범위 제약 없이 네트워크 트래픽을 분석할 수 있으며, 복잡한 보안 문제에 대한 양방향 분석을 자동으로 수행할 수 있다. Investigator는 클릭 한 번으로 NetWitness 분석기능에 직접 접근할 수 있는 유틸리티 애플리케이션인 NetWitness의 SIEMLink를 이용함으로써 기존의 IDS 또는 SIEM 콘솔에서 시작된 이벤트를 취소하거나 포렌식 확인 작업을 수행할 수 있다. NetWitness Live와 함께 사용할 경우 오늘날 비즈니스 환경이 필요로 하는 문제를 철저하게 조사할 수 있다.

RSA NetWitness Spectrum은 기업 네트워크를 노리는 악성코드 기반의 공격을 파악 및 분석하고 취해야 할 조치의 우선순위를 결정하는 분석 플랫폼으로, 분석 전문가들이 이벤트를 조사하고 취해야 할 조치의 우선순위를 결정하는데 사용하는 네 가지의 개별적인 조사 기법을 활용하여 각종 공격을 감지하고 네트워크에 존재하는 모든 데이터를 분석할 수 있다. Spectrum은 네트워크를 통과하는 모든 실행 파일을 자동으로 분석하며 네트워크 환경에서 이뤄지는 모든 파일의 활동을 파악할 수 있다. Spectrum은 NetWitness 네트워크 보안 플랫폼을 기반으로 구현되며 모든 네트워크 트래픽을 기록 및 분석하여 위협에 보다 철저히 대비할 수 있다. Spectrum은 모든 네트워크 데이터 및 활동을 분석하여 전체적인 공격 배경 정보를 제공하며, 시그니처나 알려진 악성코드 정보가 없어도 차단솔루션에서 탐지하지 못하는 공격을 인지할 수 있다. 또한 샌드 박스 커뮤니티 정보, 파일 컨텐츠 및 네트워크 활동 분석과 같은 각기 다른 네 가지의 조사 기법을 동원하여 가장 광범위한 위험도를 기준으로 분석 결과를 보여주며, 공격자의 의도, 잠재적 공격 대상, 해당 공격의 위협 수준을 보다 철저히 파악할 수 있도록 수 천 가지의 질문을 기준으로 모든 실행 파일과 관련 네트워크 활동을 분석한다. Spectrum은 작업 시간을 절약하고 가장 중요한 이벤트에 관심을 기울일 수 있도록 분석가들의 워크플로우를 자동화한다.

RSA NetWitness Live는 문제 발생 시에 식별, 평가 및 사건에 응답하는데 걸리는 시간을 최소화해 보안운영 센터의 수준을 한 단계 높여주는 위협 정보 전달 시스템이다. 단일 소스 인텔리전스에 초점을 둔 여타서비스와 달리

RSA NetWitness Live는 사용자들이 자신의 독특한 환경과 위협 프로파일에 따라 적절한 인텔리전스를 구축할 수 있도록 해준다. NetWitness는 가장 강력하면서도 포괄적인 위협 인텔리전스 서비스를 제공한다.[12]

RSA NetWitness 기대효과는 다음과 같다.

- Inbound/Outbound 트래픽 상세 모니터링 분석 체계 확보
  - 네트워크를 통해 송수신되는 모든 패킷을 저장하고 세션 단위로 분석
  - 프로토콜 분석 및 트래픽 Payload 분석을 통해 실제 송수신 내역에 대한 면밀한 분석 가능

- 주요 위협 탐지 / 대응방안 제시
  - 알려지지 않은 신규 공격 행위 파악 및 대응
  - 탐지를 회피하는 정교한 공격 탐지 / 제거
  - 위협이 되는 사이트 접근 행위 탐지 및 통제

- 내부 직원의 행동 유형 분석
  - 조직에 위협이 될 수 있는 업무 관행 파악 및 개선
  - 트래픽 통제 시에 기존 업무 영향도 분석

2.7.7 인텔-맥아피(Intel-McAfee)

인텔-맥아피 두 회사는 합병 후 반도체(CPU)가 곧 보안솔루션이 되는 개념을 제시하고 있다. 양사는 '딥 세이프(Deep Safe)'라는 핵심기술을 개발해 올해 초 '딥 디펜더(Deep Defender)'라는 제품을 출시했다. 이 방식은 PC, 노트북, 스마트폰, 태블릿 등 각각의 스마트 디바이스마다 보안 소프트웨어를 적용하지 않고 여기에 사용되는 CPU에 보안솔루션을 올리는 작업을 진행한 것이다. 최근 들어 특정한 목표물을 대상으로 이뤄지는 APT 공격이 늘어나고 있는데, 이 APT 공격 유형은 대부분이 운영체제(OS)가 실행되기 전에 임시 메모리 영역에서 악성코드를 실행하는 추세이다. 따라서 사전에 공격을 차단하기 위해서는 OS 이전 영역까지 감시하는 것이 필요하며, 이를 위해 CPU 자체에 임시메모리까지 감시하는 보안솔루션을 탑재한 딥 디펜더를 개발하게 되었다. 이 기술은 가상환경에서 구동되는 v프로 기능을 지원하는 인텔 코어 i 시

리즈에서는 모두 적용이 가능하다.[13]

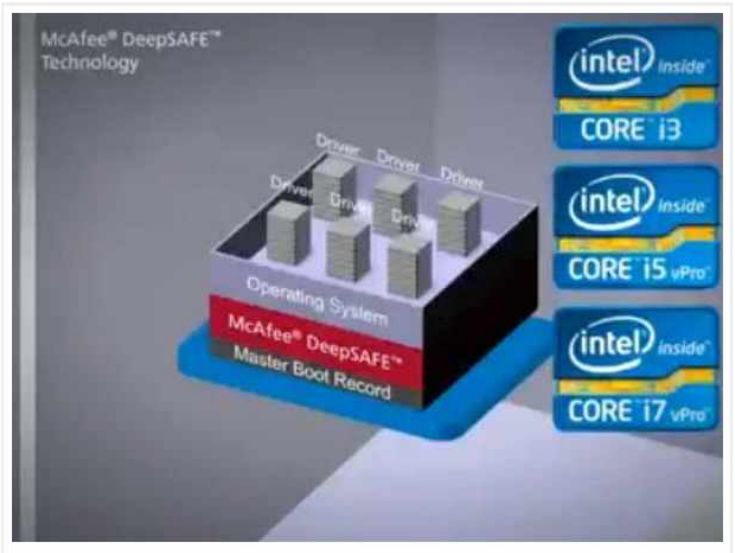

그림 13. 맥아피 딥 세이프 기술의 개념.

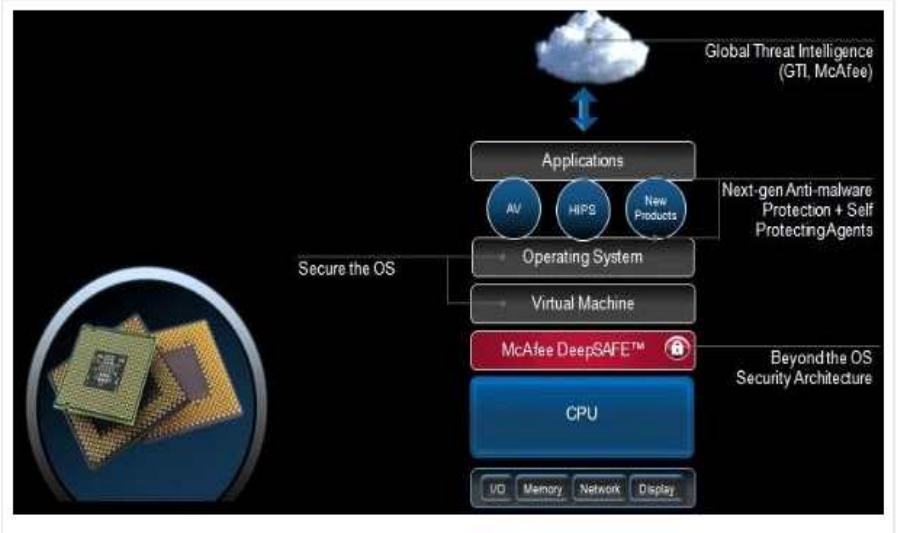

그림 14. 딥 디펜더 개념도

딥 디펜더는 OS가 실행되기 전에 CPU 단에서 발생하는 루트 킷과 같은 악성 공격을 막는다.

3. 국가 사이버공격 대응 기술 현황

3.1 국내 사이버공격 대응 기술 현황

국내에서도 사이버공격 대응을 위한 연구를 수행해 오고 있었다. 한국인터넷진흥원(KISA)에서는 봇 넷 연구를 수행하였으며, 한국전자통신연구원(ETRI)에서도 자스민(ZASMIN) 프로젝트를 수행하여 사이버공격에 대한 공격 시그니처를 실시간으로 생성 관리하는 방법을 개발하였다.

한국전자통신연구원에서 개발한 악성코드 탐지시스템은 알려지지 않은 공격들에 대한 공격특징을 탐지하고, 이를 기반으로 해당 공격을 네트워크상에서 탐지할 수 있는 공격 시그니처를 실시간으로 생성 및 관리 하는 시스템이다. 자스민은 개발 초기부처 상용화를 고려하여 설계가 되었으며, H/W 기반 이상 트래픽 탐지 및 시그니처 추출 기술을 적용하여 고속 네트워크에서 실시간 적용이 가능하다. 그리고 생성된 시그니처 검증을 위한 공격 연관성 기능을 제공하여 시그니처의 신뢰도를 향상시켰으며, 그 시그니처를 기존의 IDS/IPS로 실시간으로 적용할 수 있어 공격 차단의 효율성이 뛰어나다. 이를 통해 신종 공격에 대해서도 기존 보안 장비들의 재사용성이 증가되고, 비정상 행위 탐지의 높은 오탐율과 탐지 후 불명확한 대응 기능을 보완 할 수 있으며, 자동 시그니처 생성 및 이에 대한 정보 제공으로 CERT 팀의 업무 지원을 도울 수가 있다. 자스민 프로젝트는 국내 대표적인 보안 업체들이 파트너로 참여하고 있으며, 정보통신부와 지식경제부의 지원을 받아서 2006년 3월부터 2009년 2월 까지 3년간 진행되었다. 자스민 프로젝트 운영환경은 다음 그림 15와 같다.[14]

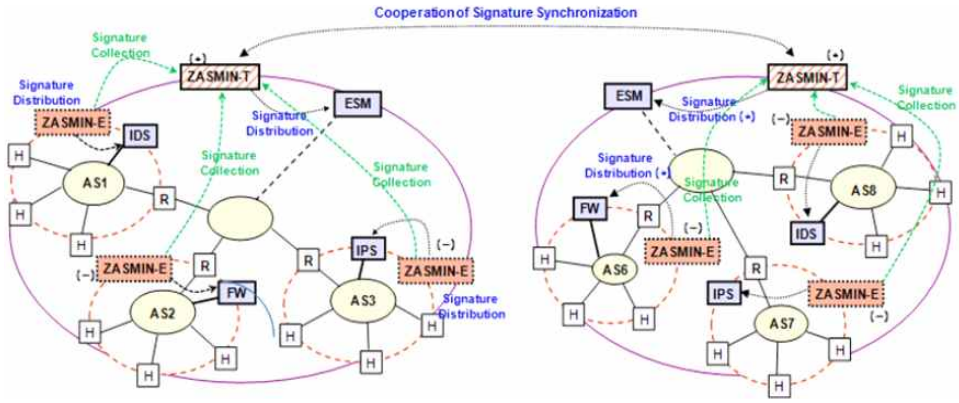

그림 15. 자스민 프로젝트 운영환경

자스민은 ZASMIN-T와 ZASMIN-E가 있다. ZASMIN-E는 하나의 AS 레벨에서 발생하는 공격을 탐지하고 이에 대한 시그니처를 생성한다. 이 시그니처는 ZASMIN-T로 전송이 되며, ZASMIN-T는 다른 ZASMIN-E로 부터도 생성된 시그니처를 전송받아 생성된 시그니처들 간의 연관성 분석을 수행한다. 그 후 최종적으로 분배하기로 판단된 시그니처들이 ESM이나 다른 ZASMIN-E로 전송된 후 해당 AS의 IDS나 IPS로 분배되고, 해당 보안 시스템들은 이 시그니처를 사용하여 현재 공격을 탐지하거나 차단하게 된다. 자스민의 논리적 구성도는 다음 그림 16과 같다. 이와 같은 과정들은 수 분 내로 실시간으로 이루어지기 때문에, 하나의 AS에서 공격이 발생한다면, 이미 그 시그니처들은 공격이 퍼져나기기 전에 다른 AS 들에 적용되어 공격을 하는 역할을 수행하게 된다. ZASMIN-T에서 생성된 시그니처들 간의 연관성 분석을 하는 이유는 최종 시그니처의 신뢰도를 더욱 높이기 위한 작업이며, 유사 시그니처들을 제거하는 작업도 병행하게 된다.

ZASMIN-E는 하나의 AS 레벨에서 탐지 활동을 수행하며, 크게 CES, FES, SMS 세 가지의 가능으로 구성되어 있다. CES(내용기반 시그니처 추출 서브시스템)는 취약성을 가진 호스트들로 빠르게 퍼져나가는 익스플로잇 코드나 웜 파일을 탐지하여 이를 차단하기 위한 시그니처를 생성하는 역할을 한다.

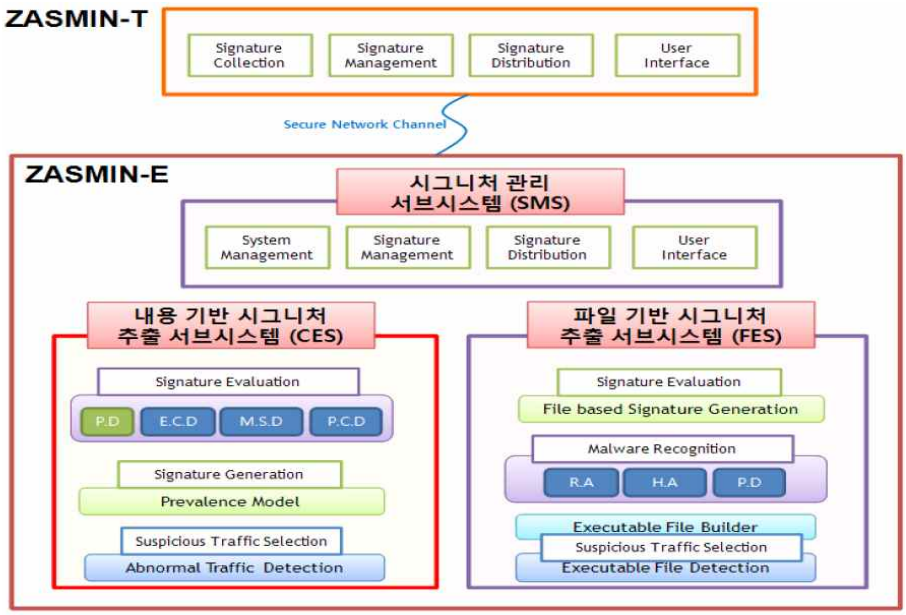

그림 16. 자스민의 논리적 구성도

또한, ZASMIN-E는 기가급 트래픽을 실시간으로 처리하기 위한 보안 카드가 장착되어 있으며, 이 보안카드에서 주기적으로 주소 확산 정도, 세션 성공률 등이 측정되어 이상 탐지 분석 기능으로 보내진다. 이상 탐지 분석 기능이 몇 주기 동안의 측정 정보를 분석하여 공격이 확신된다고 의심되는 3-Tuple을 선정하고, 패킷들의 캡쳐를 위해 이를 보안 카드에 재 적용한다. 3-tuple로 캡쳐된 패킷들 속에 반복된 페이로드 패턴이 들어있는지가 분석되며, 이 반복된 페이로드 패턴으로부터 시그니처를 생성하게 된다. 실제 네트워크 환경에서는 여러 가지 이유로 공격이 아니지만 위와 같은 이상 트래픽 현상이 자주 일어나기도 한다. 따라서 생성된 시그니처가 공격이 포함된 트래픽으로부터 생성되었는지에 대한 검증을 할 필요가 있다. 이와 같은 역할을 수행하는 것이 시그니처 평가기능이다. 여기에는 실행 코드가 포함되어 있는지의 여부, NOP 이나 반복된 리턴 주소 같은 악성코드의 포함여부, 폴리몰픽 코드 포함여부, '/bin/sh'와 같은 악성 스트링이 포함되어 있는지의 여부를 판단하여, 생성된 시그니처의 신뢰도를 판단하게 되고, 신뢰도가 낮을 경우는 최종 시그니처로 활용하지 않게 된다. 다음 그림17은 CES의 구성도를 나타낸다.

FES (파일 기반 시그니처 추출 서브시스템)는 익스플로잇 코드에 의해 정복된 호스트로 전송되는 실행 파일(웜이나 바이러스 같은 실행 파일)혹은 사용자가 오프라인으로 가지고 와서 AS 내부에서 돌아다니는 악성 파일 등을 탐지하여 이를 차단하기 위한 시그니처를 생성하는 역할을 한다. 다음 그림18은 FES의 구성도를 보여준다.

ZASMIN-E는 기가급 트래픽에서 실행 파일 헤더(PE헤더, ELF 헤더 등)를 탐지하는 보안 카드가 장착되어 있으며, 이 보안 카드에서 실행 파일 헤더가 탐지 되면 해당 세션의 모든 패킷들이 실행 파일 재조합 기능으로 보내진다. 해당 기능에서는 실행 파일의 여부와 재조합 가능성 여부를 판단을 하게 된다. 이렇게 재조합된 실행파일은 악성 파일 유무를 판단하는 기능에서 파일 패킹 여부, 파일 헤더 이상 유무 등을 판단하여 최종적으로 악성 파일 여부가 결정된다.[14]

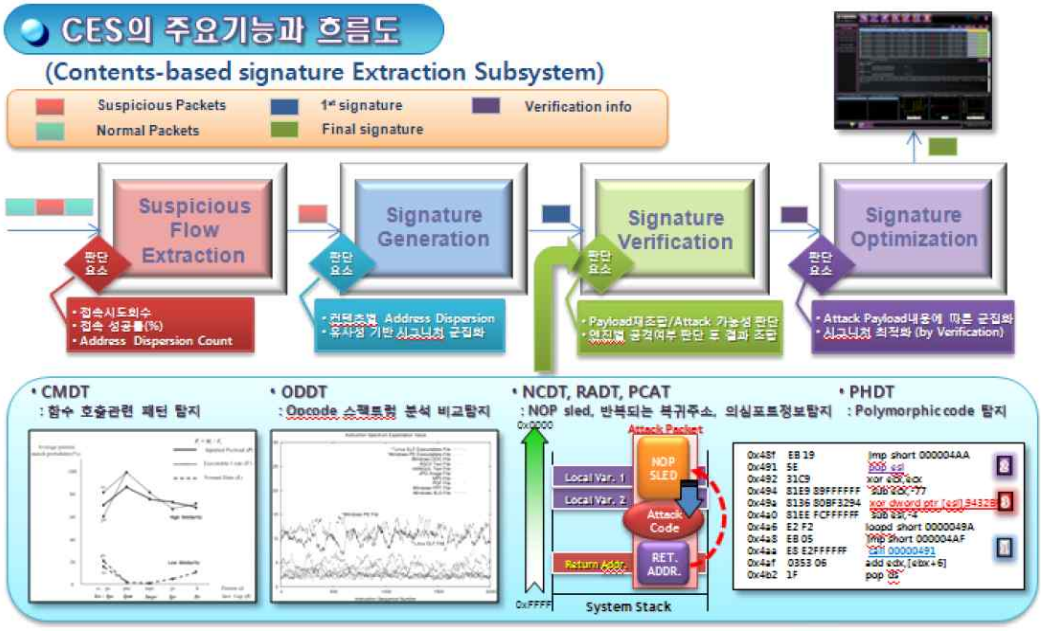

그림 17. CES 구성도

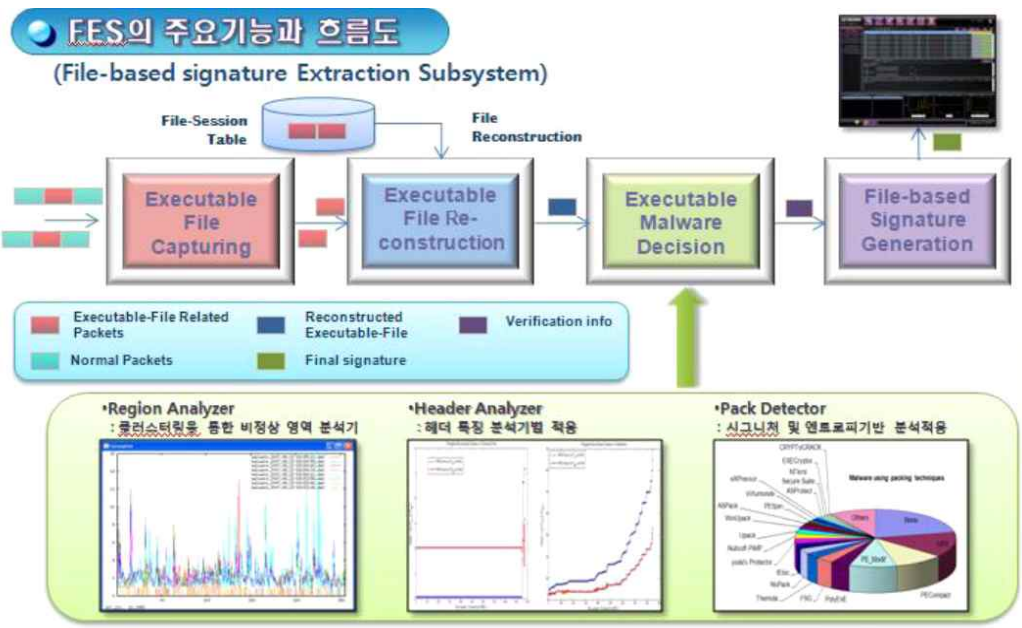

그림 18. FES 구성도

한국인터넷진흥원(KISA)에서는 봇 넷 연구를 수행하였으며 안전한 인터넷 서비스 제공을 위한 신종 봇 넷 능동형 탐지 및 대응 기술을 개발하였다. 개발한 기술은 다음과 같다.[15]

- 호스트 기반의 악성 봇 능동형 탐지 및 대응 기술
- 네트워크 기반의 신종 봇 넷 탐지 기술
- 실시간 봇 넷 통합 관제 및 보안 관리 기술

호스트 기반의 악성 봇 능동형 탐지 및 대응 기술은 호스트 레벨 능동형 봇 감염 탐지 기술, 위장 봇 기반 봇 넷 실시간 행동 모니터링 기술, 악성 봇 감염 통보/치료유도 시스템으로 구성되어 있으며, 네트워크 기반의 신종 봇 넷 탐지 기술은 중앙 집중형 IRC/HTTP/CS 봇 넷에 대한 그룹행위 기반 탐지 기술, 분산형 P2P 봇 넷에 대한 그룹행위 기반 탐지 기술, 네트워크 기반 봇 넷 그룹행위 탐지 센서, IRC/HTTP/P2P/CS 통합 봇 넷 탐지 시스템으로 구성되어 있다. 그리고 실시간 봇 넷 통합 관제 및 보안 관리 기술은 봇 넷에 대한 통합(IRC/HTTP/P2P/CS) 관제 및 보안 관리 기술, 네트워크/호스트/위장 봇 기반 탐지정보 통합 분석 기술, 봇 넷 구성/분포/행동 시각화 및 통계/리포트 기술, 정책기반 통합 봇 넷 탐지/대응 관리 시스템으로 구성되어 있다. 다음 그림 19는 연구 결과를 나타내는 봇 넷 대응 기술 구성도이다.

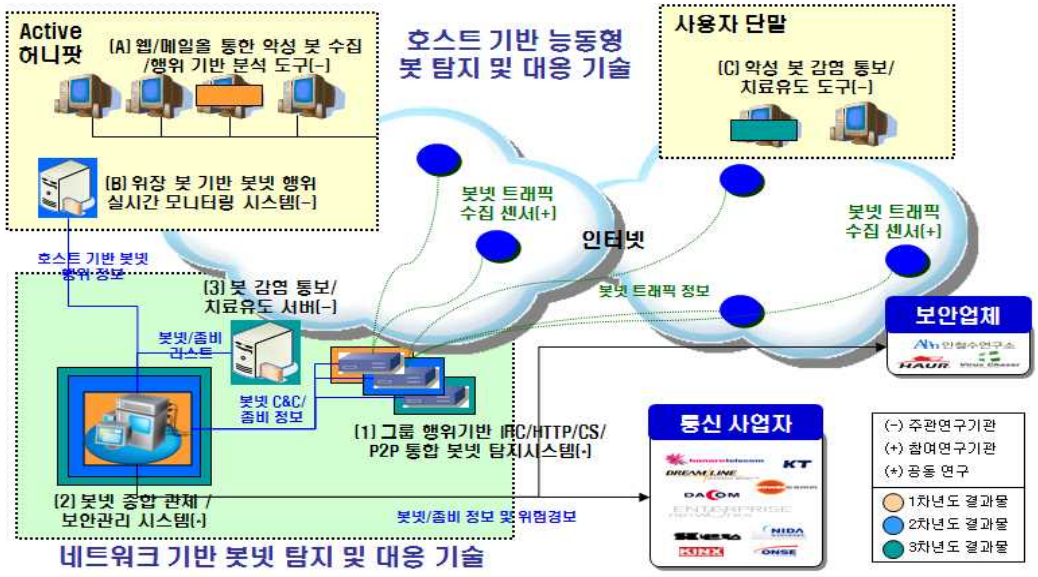

그림 19. 봇 넷 능동형 탐지 및 대응 기술 구성도

다음 그림 20은 호스트 기반 능동형 봇 악성·탐지 및 대응 시스템 구성도이고, 그림 21은 네트워크 기반 봇 넷 탐지 시스템 구성도이며, 그림 22는 봇 넷 관제 및 보안 관리 시스템 구성도이다.

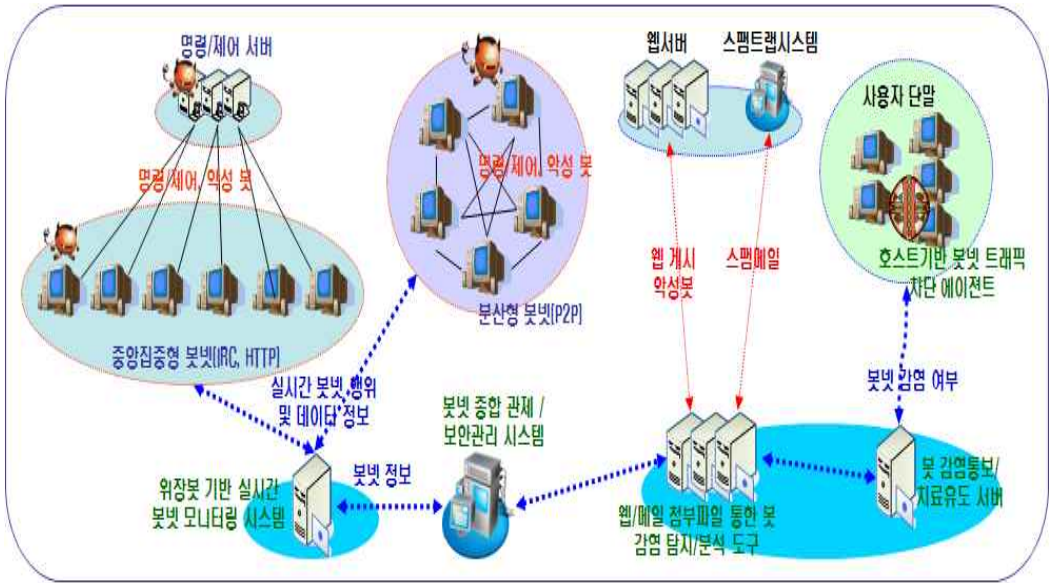

그림 20. 호스트 기반 능동형 봇 악성 봇 탐지 및 대응 시스템 구성도

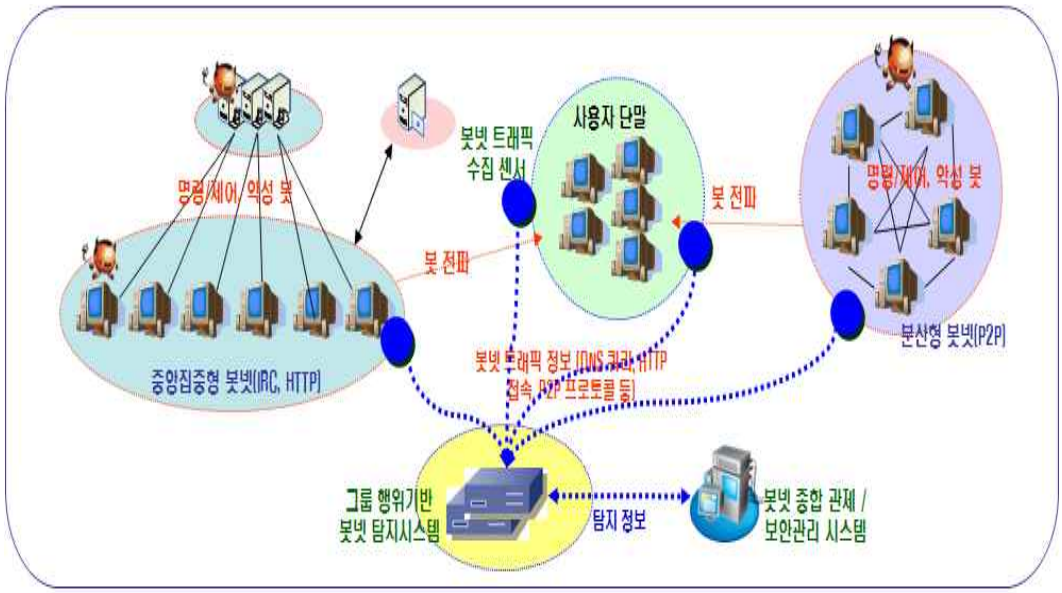

그림 21. 네트워크 기반 봇 넷 탐지 시스템 구성도

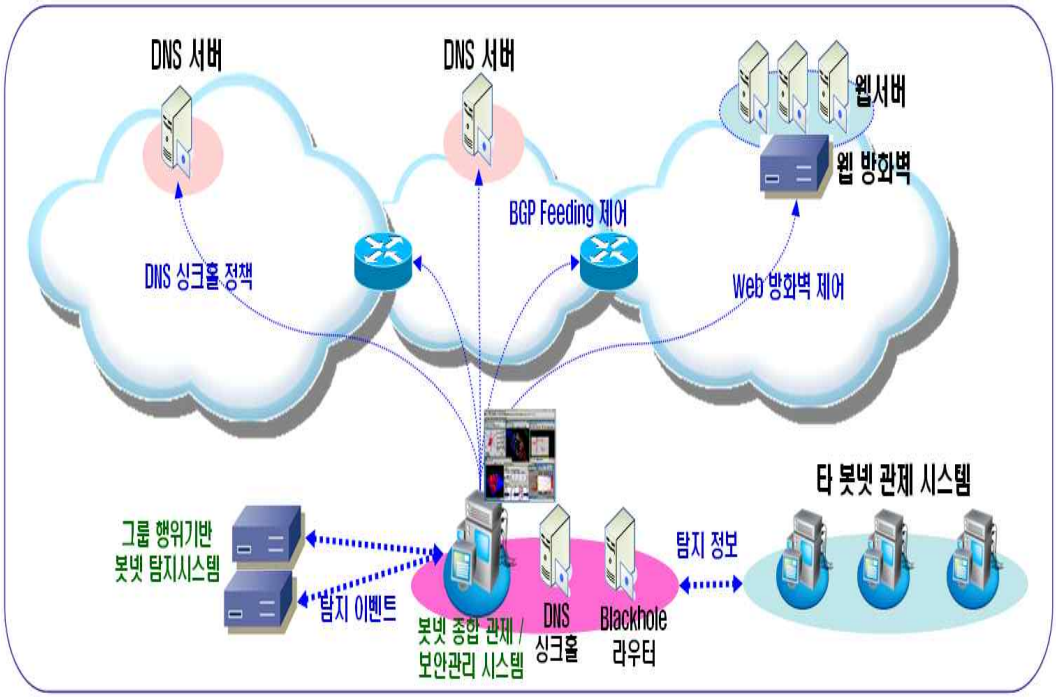

그림 22. 봇 넷 관제 및 보안 관리 시스템 구성도

한국인터넷진흥원에서 개발한 봇 넷 능동형 탐지 및 대응 기술은 봇 넷 고유의 그룹행위를 기반으로 다양한 유형의 봇 넷을 탐지/분석 할 수 있으며, 악성 봇의 형태 및 특성에 상관없이 네트워크 트래픽 분석을 통한 행위 기반으로 봇을 탐지/분석할 수 있다. 또한 능동형 악성 봇 탐지 기술을 통해 다양한 악성 봇의 감염 경로를 차단할 수 있으며, 악성 봇의 감염 통보 및 치료 유도가 가능하다.[15][16]

그러나 국내에서 수행된 사이버공격 대응 연구는 고도화된 공격에 대응하기에는 다음과 같이 부족한 점이 존재한다. 한국인터넷진흥원에서 수행된 봇 넷 능동형 탐지 및 대응 기술은 서버의 봇 감염 여부는 알 수 있으나 서버를 통해 감염된 호스트의 정보는 알 수 없는 단점이 있다. 그리고 한국전자통신연구원에서 개발한 자스민 시스템도 사이버공격에 대한 공격 시그니처를 실시간으로 생성하고 관리할 수 있지만 비정상행위 분석 시 분석을 통한 결과가 악성코드 데이터베이스하고 매칭이 안 되는 단점을 가지고 있다. 그리고 두 시스템 다 악성코드별 분포 현황, 악성코드 전달 경로 현황, 좀비 연계도 현황 등 고도화된 사이버공격에 사전 대응을 하기 위한 정보 구축이 불가능한 상황이다.

3.2 국외 사이버공격 대응 기술 현황

국외에서도 사이버공격 대응을 위한 연구를 수행해 오고 있었다. 그 중 대표적인 프로젝트로 자동화된 정보 수집과 전달 시스템을 갖춘 에셜론 프로젝트(ECHELON Project)와 연방 망을 통과하는 인터넷 트래픽을 실시간 모니터링 하여 사이버공격의 가능성이 있는 비정상적인 상태를 탐지하는 아인슈타인 프로그램을 들 수 있으며, 또한 허니팟 기술을 사용하여 공격 정보와 공격 차단 시그니처를 생성하는 노아(NoAH) 프로젝트를 예로 들 수 있다.

3.2.1 에셜론 프로젝트 (ECHELON Project)

에셜론 프로젝트는 5개 국가 - 미국, 영국, 캐나다, 호주, 뉴질랜드 - 의 첩보기관에 의해 운영되고 있는 전 세계에 걸친 자동화된 정보 수집과 전달 시스템을 지칭하는 암호로, 미국 NSA의 주도하에, 호주 Defense Signals Directorate(DSD)를 비롯한 다른 국가 기관들과 함께 운영되고 있다. 또한 영국의 Government Communications Headquarters(GCHQ)와 각종 조약에 따른 미국의 여타 동맹 기관들도 이에 가담하고 있다.[17] 이러한 국가들은 1947년의 UKUSA 협정에 따라, 그들의 활동을 조정하기 시작하였고, 최초의 에셜론은 1971년까지 소급된다. 그리고 이러한 형성 이후, 에셜론의 능력과 우위성은 급속도로 확대되었다. 보고서에 따르면, 여러 종류의 통신을 가로채고 처리하는 능력은 전 세계에 걸쳐있다고 한다. 사실상, 에셜론은 전화, 이메일, 인터넷 다운로드, 위성송신 등을 포함하여 매일 30억 통신을 가로챌 수 있다고 알려졌다. 에셜론 시스템은 모든 전파 송신들을 무차별적으로 수집하여, 인공 첩보 프로그램을 통해 가장 핵심적인 정보만을 추출할 수 있다고 한다. 몇몇 정보에 따르면, 에셜론은 인터넷에 흘러 다니는 통화량 중에서 약 90%를 걸러낼 수 있다고 한다. 그러나 에셜론의 정확한 능력과 목적은 아직 불분명하다. 예를 들어, 에셜론이 실제 어떤 통신을 목표로 삼고 있는가에 대해서는 아직 알려지지 않고 있으며, 광통신과 같은, 어떤 특정 종류의 송신을 가로채는 능력이 있는지는 아직 밝혀지지 않고 있다. [18]

에셜론은 여러 방법으로 정보를 수집한다. 보고서에 따르면, 에셜론은 위성송신을 가로챌 수 있는 라디오 안테나에 근거한 광범위한 기반을 가지고 있으며, 몇몇 지역에서는 육상 통화를 도청하는 역할을 하고 있는 것으로 알려졌

다. 이러한 안테나들은 미국, 이탈리아, 영국, 터키, 뉴질랜드, 캐나다, 호주, 그리고 다른 여타 장소에 설치되어 있다고 한다. 유사한 방법으로 에셜론은 도시들 간 통신으로부터 많은 자료들을 수집하기 위해 수많은 위성을 사용하고 있으며, 위성들은 지상에 있는 처리 센터에 이러한 정보들을 송신하는 것으로 알려졌다. 미국(Denver 주변), 영국(Menwith Hill), 호주, 독일에 처리 본부가 있으며, 에셜론은 정기적으로 인터넷 통신을 가로채는 활동을 수행하고 있다. 이 조직은 수많은 "탐지기(sniffer)" 장치를 구축하고 있는데, 이 탐지기들은 인터넷을 통과하는 자료 패킷으로부터 필요한 정보만을 수집한다. 또한 이것은 흥미로운 웹 사이트를 조사하기 위해 탐색 소프트웨어도 사용한다. 게다가 에셜론은 바다를 가로지르는 전화 케이블을 도청할 수 있는 특수 수중 장치를 사용하고 있다고 알려졌다. 에셜론은 가공되지 않은 무수히 많은 정보를 포착한 후에, 탐색 프로그램을 사용하여 사용자들이 원하는 특정 주제에 초점을 맞출 수 있도록 하고 있다. 에셜론에 대한 최초의 보고서는 1988년에 발간되었으며. 에셜론은 극도로 비밀에 부쳐진 운영체계로서, 국가의 의회나 법원의 감시를 거의 받지 않고 운영되어져 왔다. 대부분 에셜론에 대해 알려진 것은 밀고자나 기밀문서로부터 유출된 것이며, 에셜론이 어떠한 용도에 사용되었는가를 정확히 알아내는 방도가 없는 상황이다.[18]

3.2.2 아인슈타인 프로그램

미국의 국토안보부(DHS)는 군사용 네트워크를 감시하는 국방부의 프로그램을 이용해 2003년에 처음 아인슈타인 프로그램을 개발했다. 이 프로그램은 교통부와 같은 연방정부 기구 인터넷으로 들어오고 나가는 정보의 흐름을 추적하여 사이버공격일지 모르는 비정상적인 흐름을 찾아내는 것으로 2007년까지는 불과 16개 정부기구가 이 프로그램을 채택했었다. 부시 행정부가 추가로 자금을 지원하여 '아인슈타인 2'로 명명된 새 버전의 연구가 시작되었으며, 이 프로그램은 알려져 있는 사이버공격유형을 찾아내 사이버보안센터에 즉각 경보를 발생시킬 수 있다. 그러나 이 프로그램도 아인슈타인 1과 마찬가지로 알려져 있지 않은 정교한 공격을 막거나 찾아내지 못하는 문제가 존재했었다. 2009년까지 이 프로그램을 사용하는 정부부처는 국토안보부가 유일했지만 그 이후에 다른 정부부처와 기관들도 국토안보부가 운영하는 아인슈타인 2를 이용하였다.[19] 아인슈타인은 미국 정부 및 공공 기관의 사이버보안을 강화하

기 위해 구축한 보안 프로그램으로 1, 2, 3 세 가지 버전으로 나누어진다. 아인슈타인 1, 2는 침입 탐지에 중점을 두고 있으며, 아인슈타인 3은 미리 예방하는데 주력하고 있다. 세 가지 버전의 특징은 다음과 같다.

- 아인슈타인 1 : 연방 망을 통과하는 인터넷 트래픽을 실시간 모니터링 하여 사이버공격일수 있는 비정상적인 상태를 탐지한다. 그러나 사이버공격 자체는 차단하지 못한다.

- 아인슈타인 2 : 비정상적인 상태의 탐지 외에 바이러스와 기존에 알려진 침해 사고에 대한 정보에 기초한 공격의 징후를 탐지하여 즉각적으로 경고를 발생시킨다. 그러나 사이버공격 자체는 차단하지 못한다.

- 아인슈타인 3 : 현개 개발 중인 프로그램으로 Tutelage라고 명명된 국가보안원(NSA) 프로그램의 기술에 기초하여, 보안 침해 요소를 탐지한다. 아인슈타인 3의 필터링 기술은 이 메일이나 기타 통신의 콘텐츠까지 읽을 수 있다.[20]

부시 정부 때 구상되어 현재 개발 중인 '아인슈타인3' 은 개인 사생활과 시민의 자유를 보호하는 문제로 인하여 당초 예상보다 지연될 것으로 예측되고 있다. '아인슈타인 3' 에 사용된 필터링 기술은 사이버공격을 검사할 때 정부 시스템을 통해 전송된 이메일과 다른 메시지의 내용을 읽을 수 있는 능력을 갖추고 있어 사생활 보호 문제에 직면하고 있다. 그러나 미국 국토안보부는 2012년 내에 아인슈타인 3(실시간 네트워크 침입 탐지 및 방지 시스템)을 도입할 예정이다.

3.2.3 NoAH 프로젝트

유럽에서는 허니팟 기술에 기초하여 사이버공격 시그니처를 생성하는 노아 프로젝트를 수행하였다. 노아 프로젝트는 허니팟 기술에 기초하여 보안 모니터링을 위한 인프라의 개발을 위해 필요한 기술적인 작업들을 수행하고 설계하는데 그 목적이 있었다. 허니팟 그자체로는 공격 차단을 위해 직접적으로 생성하는 것들이 없지만, 대신에 망 자체를 의도적으로 취약하게 구성하여 유

인된 공격들을 분석할 수 있으므로 공격 차단을 위한 좋은 자료들을 제공한다. 노아는 초기 경보 시스템으로서 지리적으로 분포된 허니팟들을 사용하고, 공격 정보와 공격 차단 시그니처를 생성하는데 허니팟들에서 수집된 정보를 이용하게 된다.

노아가 지향하는 것은 사이버공격 발생시 NERO(National Research Network Organization)과 ISPs(Internet Service Providers)의 피해를 최소화하고, 정보 보안 관련 조직들이 해당 위협에 더욱 능동적으로 대처하도록 하며, 연구자들에게 탐지 기술 향상을 위한 좋은 자료를 제공하는 것이다. 노아 프로젝트는 학계, 연구소, 산업체 등의 8개의 파트너들이 참여하고 있으며, 유럽 연합의 연구 인프라 프로그램(The Research Infrastructure of the European Union)에서 지원하고 있다. 이 프로젝트는 2005년 4월에 시작하여 2008년 3월에 끝나는 3년간의 프로젝트이다.

허니팟은 사이버공격을 유도하기 위해 특별히 설계된 호스트들로, 이들은 현재 사용하지 않는 IP 대역들을 이용하기 때문에, 허니팟으로 유입되는 모든 트래픽들은 대부분 악의적인 것들이라고 할 수 있다.

노아 프로젝트는 두 가지 형태의 허니팟을 포함하고 있다. 하나는 로우 인터랙션(Low-Interaction:LI) 허니팟으로 실제 애플리케이션을 흉내 내는 것처럼 에뮬레이션 한다. 단지 에뮬레이션 혹은 시뮬레이션만을 수행하기 때문에 공격에 감염되어도 안전하다. 그러나 대부분의 경우에 에뮬레이션만으로는 알려지지 않은 취약점을 대상으로 하는 새로운 공격을 탐지하는 것이 어렵다. 하이-인터랙션(Hi-Interaction :HI) 허니팟은 이런 단점을 극복하기 위해 에뮬레이션을 하는 것이 아니라 실제 애플리케이션을 동작시키게 된다. 노아는 사용되지 않은 IP 주소들을 액세스 하거나 악성 트래픽과 상호 작용하는 허니팟으로부터 관련 자료들을 얻게 된다.

노아 코어(NoAH Core)는 허니팟들의 위치와는 별개로 제로데이 공격의 자동화된 시그니처를 생성하기 위한 서비스들을 말한다. 노아 코어에서 LI는 트래픽 필터의 역할을 수행하며, 포트 스캐닝과 같은 현상들을 효과적으로 탐지하게 된다. LI에 의해 처리될 수 없는 트래픽들은 HI로 넘어가게 되며, HI의 감염으로 인한 피해를 막기 위해 관련 서비스들은 VMware, Xen 혹은 노아 프로젝트에서 제작된 Argos와 같은 버츄얼 머신 상에서 동작하게 된다.[14]

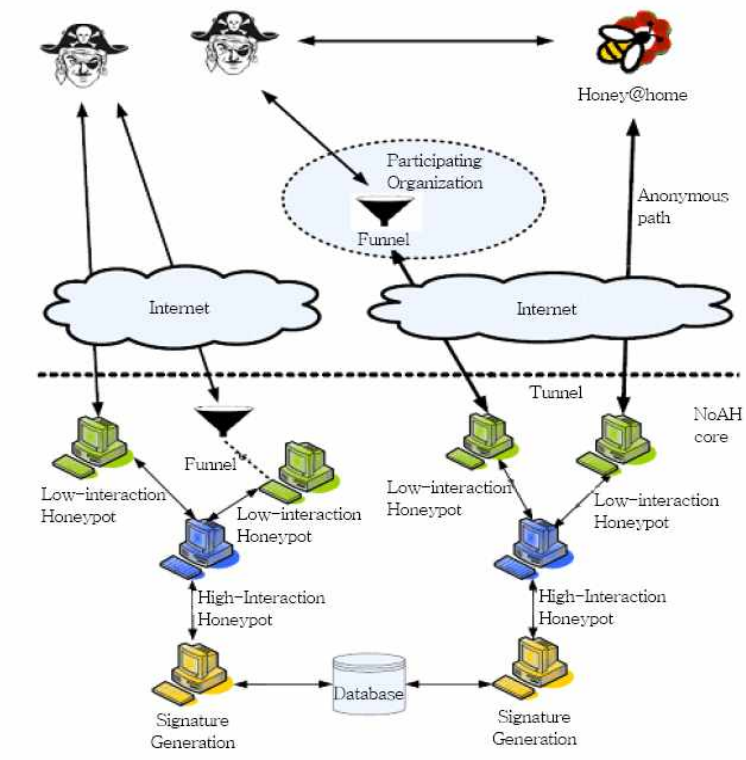

그림 23. 노아 프로젝트 운영환경

노아가 처리하는 IP 주소 공간은 확장이 용이하며, 플러그인 모듈을 통해 캠퍼스 망, 기업 망 등의 사용되지 않는 IP로 유입되는 트래픽들을 터널링을 통해 수집할 수도 있다. 또한 이와 같은 방식으로 사용되지 않은 IP를 노아 와 공유할 수 있는 일반 홈 유저나 작은 기업들에도 적용하기 용이하다. 결국 노아는 허니팟들의 유연성을 위해 다양한 네트워크와 호스트들과의 유기적인 관계를 맺을 수 있다.

시그니처를 생성하는 노아 코어는 HI 허니팟에 Argos라는 의심 트래픽 통제 환경으로 구축되어 있다. 1) 허니팟으로 유도된 네트워크 데이터가 Argos에 도착되며, 해당 정보가 기록되고 Argos 에뮬레이터로 보내진다. 2) 에뮬레이터는 입력된 트래픽을 표시하고, 3) guest OS에서 해당 트래픽을 프로그램의 실제 입력으로 사용한 결과를 포렌직한다. 4) 보안정책을 위반하는 동작이 발생되면 해당 트래픽과 관련된 정보를 모두 dump하여, 5) 시그니처를 생성하는 곳(Signature generator Component:SGC)으로 전송한다.

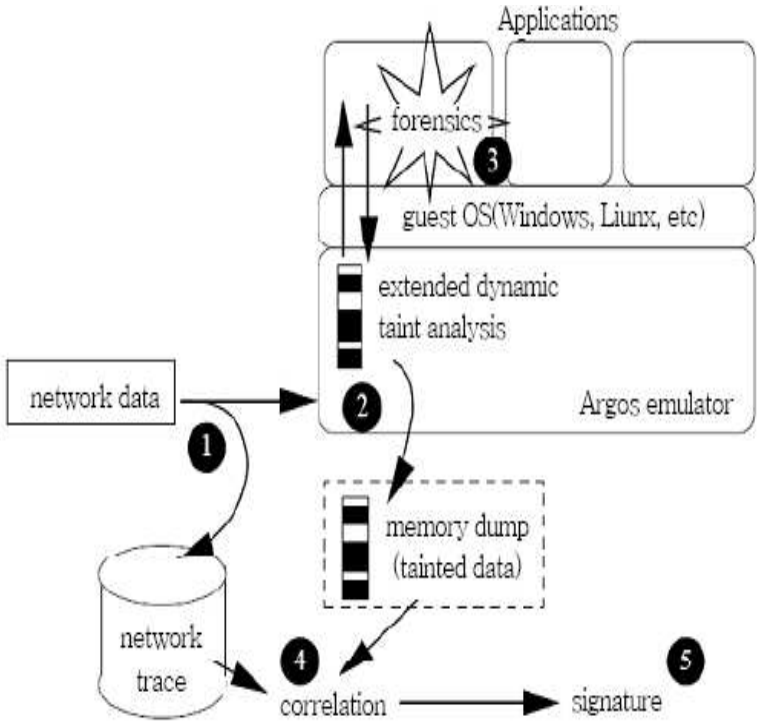

그림 24. Argos의 의심 트래픽 통제 환경

시그니처 생성을 담당하는 SGC는 각종 트래픽의 상태를 기록하는 상태 추적기와 Argos로부터 이용 가능한 정보를 수집하여 시그니처를 생성하게 된다. Argos에 의해 경고가 발생한 트래픽의 바이트 정보들은 각종 탐지 메커니즘에 의해 세부적으로 분석이 되고 바이트 길이 분포와 바이트 빈도 분포를 종합하여 결과적으로 특정 패턴 형태를 가진 바이트들은 패턴 기반 시그니처로 제작할 수 있다. 이때 탐지 메커니즘으로 이용할 수 있는 방법들은 기존의 방법들을 포함하여 다양하게 이용될 수 있다. 이렇게 최종적으로 생성된 시그니처들은 기존의 IDS/IPS로 전송되어, 공격 탐지 및 차단에 이용되어 진다.[14]

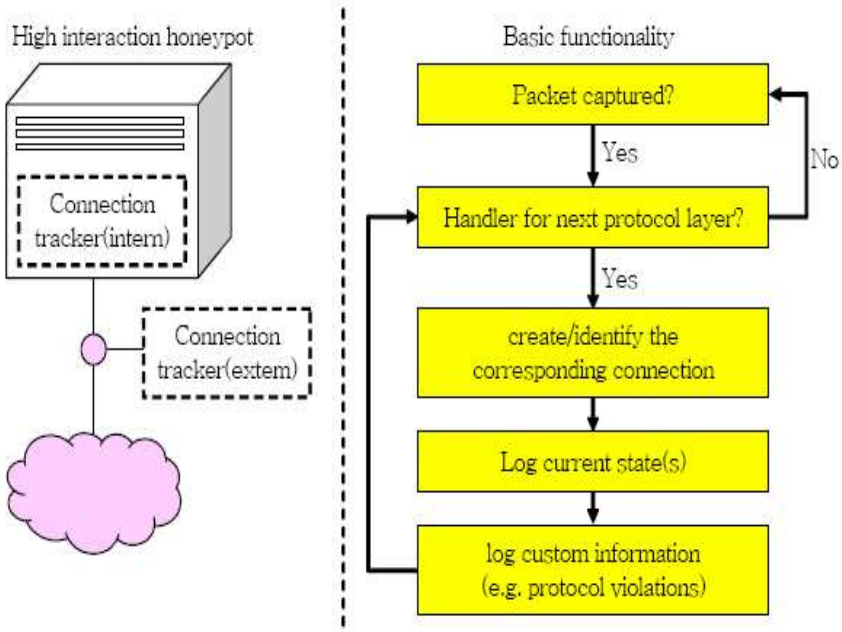

그림 25. 상태 추적기 동작 흐름

국외에서도 위와 같이 사이버공격 대응을 위한 연구를 수행해 오고 있지만, 국외에서 수행된 사이버공격 대응 연구도 고도화된 공격에 대응하기에는 다음과 같이 부족한 점이 존재한다. 에셜론 프로젝트(ECHELON Project)는 자동화된 정보 수집과 전달 시스템은 갖추었으나 실행코드를 탐지할 수 없으며, 아인슈타인 프로그램도 트래픽의 실시간 모니터링으로 비정상적인 상태를 탐지할 수는 있지만 여전히 실행코드를 탐지할 수 없는 문제를 가지고 있다. 또한 노아 프로젝트도 공격 차단 시그니처를 생성할 수는 있지만 여전히 고도화된 사이버공격에 사전 대응을 하기 위한 정보 구축이 불가능한 상황이다.

2012년에 들어와서 사이버전을 대비한 새로운 계획을 미국에서 추진하고 있는 중이다. 올해 들어서 미국 국방부는 실전투입용 사이버무기 개발을 위한 대규모 프로젝트 '플랜 X'를 추진하고 있다. '플랜X'는 국방부 산하 방위 고등 연구 계획국(DARPA)이 주도할 예정으로, 민간기업과 대학, 게임업체들도 대거 참여한다. 미 국방부가 플랜X에 돌입하게 된 것은 미국 군부의 심장부라 불리는 록히드 마틴이 해킹 공격을 받아 당시 군사기밀을 대량 유출하여 자국 국방 기밀에 대한 위협이 있다는 판단 때문이며, 사이버 공간의 적들이 갈수록 공격 능력을 향상시키고 있는 상황에서, 미국도 더 이상 소극적인 방어에만 치중할 수 없다는 판단에 의해서다. 미국 국립 과학 아카데미의 허

버트 린 박사(Herbert S. Lin)는 “만약 이 프로젝트가 성공한다면 엄청난 일이 될 것”이라고 하면서 “이는 이른바 ‘디지털 전투장’을 지배하게 된다는 의미”라고 언급하고 있다. ‘플랜X’는 적국의 방공망과 지휘통신체계를 무력화시키는데 초점을 두어, 미국 사이버 전략의 방향 전환을 시사하고 있다. 지금까지는 주로 자체 컴퓨터 시스템 보호와 정보 수집 등을 위해 사이버 전력을 활용해 왔다면 이번 계획은 직접 전투에 활용하는 것에 초점을 두고 있으며, 기존 사이버보안정책이 방어적으로 시스템을 보호하는 것이 목적이었던 것과 달리, ‘플랜X’는 적군의 컴퓨터를 교란해 재래식 전투력을 지원하는 것이 목적이다. 예를 들어 전투기가 출격해 폭격을 할 때 적군의 통신과 레이더망을 방해함으로써 효과를 극대화하는 사이버작전 등에 투입이 가능하다. 펜타곤의 사이버전 초점이 외부 침입으로부터 국방부 시스템을 지키는 것이었다면, 앞으로는 적의 시스템을 교란·파괴하는 것이 된다는 의미에서 ‘플랜X’는 미국 사이버 전략의 전환을 시사한다. ‘플랜X’는 적군의 통신망 레이더를 무력화시키는 것은 물론 전 세계 수백억대 PC위치를 담은 사이버 전자지도 작성 계획도 포함되어 있다. 전 세계 모든 컴퓨터의 도메인을 담은 사이버 지도를 작성하고 견고한 운영체계를 개발하여 사이버전 발생 시 적군의 PC를 한 번에 무력화시키겠다는 의지를 포함하고 있다. 사이버 지도를 지속적으로 업데이트함으로써 사이버전에 대비하도록 하는 동시에 이를 운용할 수 있는 첨단 시스템도 개발한다. 사이버 지도는 미국을 사이버 공격하는 컴퓨터를 즉각 파악하고 이에 대해 반격할 수 있는 경로를 시각화해 지휘부로 하여금 신속하고 적절한 결정을 내릴 수 있도록 지원한다. 적국의 컴퓨터를 붉은 색 점으로 미국의 컴퓨터는 파란 색 점으로 표시하고, 적국의 컴퓨터가 업그레이드 될 경우 노란 색으로 자동 표시되도록 하는 방식을 채택할 예정이다. 이 지도를 통해 미국의 사이버전 사령부는 표적을 공격하기 위한 루트가 공격을 받을 때 반격 루트를 효과적으로 파악할 수 있게 될 것으로 기대한다. 이번 프로젝트는 DARPA의 대규모 사이버 전력 증강 계획의 일환으로, 2017년까지 총 15억 4천만 달러의 예산을 투입할 예정이다. 미국 정부는 오는 2013년부터 2017년까지 사이버 전쟁 예산으로 15억 4천만 달러를 배정해 놓고 있으며, 플랜X에는 1억 1천만 달러 예산을 책정하였다. 사이버전 전문가 마틴 리비키(Martin Libicki)는 “DARPA의 구상 가운데 90%가 실패하더라도 10%의 성공 가능성만 있으면 투자 가치는 충분하다”고 언급하였다. 미 국방부는 실전에 투입할 수 있는 사이버무기 개발에 속도를 낼 수 있도록 관련 규정을 간소화하는 이른바 ‘신속처리 방식(fast track)’을 올 초 연방 의회에 요청하였다. ‘신속처리방식’은 사이버무기 개발은 재래식 무기 개발에 필요한 통상적인 절

차를 그대로 적용해서는 안 된다는 미국 국방부의 입장을 표명한 것이다. 민간 혹은 정부 차원에서 이미 개발을 마쳤거나 마무리 단계에 있는 하드웨어나 소프트웨어를 즉각 이용할 수 있도록 하는 동시에 관련 자금조달 절차도 간소화하는 것이 주요 골자이다. 위험도가 높은 사이버 무기는 최소 9개월 이상의 개발 기간을 두도록 명시했으나, 통상 재래식 무기를 개발할 때 몇 년이 소요된다는 점을 감안하면 개발 소요기간이 대폭 단축됨을 의미한다.[21] 플랜 X와 같은 최근의 추세를 볼 때 국가적으로 고도화된 사이버공격에 대응하기 위한 체계적인 방안에 대한 수립이 필수적이라고 할 수 있다.

4. 국가 사이버공격 대응체계 현황

4.1 국내 사이버공격 대응체계 현황

우리나라의 국가사이버 안전 체계는 ‘국가 사이버 안전 관리 규정’에 의해 정부가 국가안보차원의 사이버 위협에 대한 대응을 보다 강화하여 국가 인터넷망의 전자적 침해사고 조기탐지 및 피해확산 방지를 위해 구축한 범국가적 체계이다. 한국인터넷진흥원의 ‘인터넷 침해 대응 센터’가 민간분야를 담당하고, 국가안전보장회의(NSC) 사무처 주관 하에 범정부적 차원에서 출범한 국가정보원 소속의 ‘국가사이버 안전센터 (NCSC :National Cyber Security Center)’가 공공분야를 담당하며, 국방정보본부 산하의 ‘사이버사령부’가 군 분야를 담당하는 민 · 관 · 군 종합 대응체계이다.

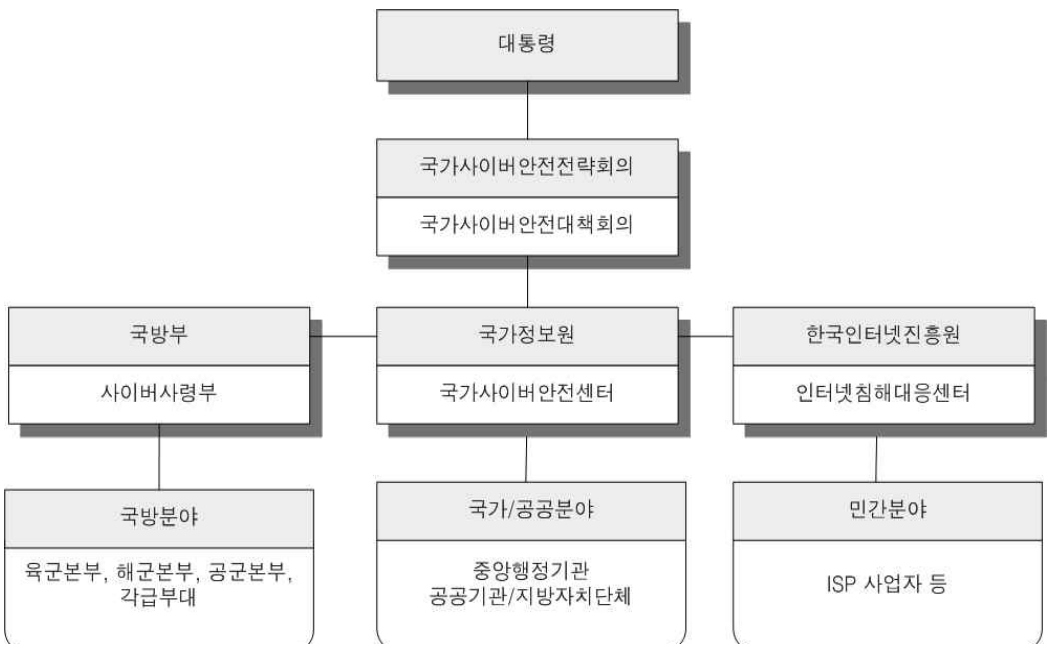

그림 26. 국가 사이버 안전 관리 체계

민간분야의 사이버 안전 활동은 정보통신망 법에 따라 방송통신위원회가 정보보호 지침을 정하여 고시하고 정보보호안전진단 수행기관을 관리 감독하며,

정보보호 관리 체계 인증업무를 수행한다. 이에 따라 한국인터넷진흥원 소속의 ‘인터넷침해대응센터’를 통하여 민간분야 정보통신망 침해사고에 관한 정보의 수집, 전파, 침해사고의 예보, 경보, 침해사고에 대한 긴급조치 등 각종 대응 업무를 수행한다. 한편, ISP 등 주요 정보통신 사업자와 집적 정보통신시설사업자는 침해사고가 발생하면 방송통신위원회나 한국인터넷진흥원에 신고하여야 한다. 공공분야는 ‘국가사이버 안전센터’에서 국가 사이버 안전 관리 규정에 따라 사이버 위협정보 수집, 분석을 위하여 보안관제시스템을 운용하고 국가전산망에 대한 사이버 침해에 대응, 복구지원 활동, 사이버 안전 정책결정 등 범정부 차원에서 국가사이버 안전 업무에 대한 총괄 조정 역할을 수행한다. 국방 분야의 사이버 안전 업무는 국방부가 국가 사이버 안전 관리 규정에 근거하여 수행 한다. 예전에 정보본부 산하 ‘사이버사령부’를 통하여 독자적으로 수행하며, 각 급 부대 정보통신망에 대한 안전성 확인, 경보발령, 사고조사 및 관련 정보 통보 등이 별도로 이루어졌다. 하지만 국방부는, 최근 국방정보화 기반조성 및 국방정보자원관리에 관한 법률 제정을 통해 국방사이버 안전 전담기구를 설치 국방정보침해 대응 기술 개발, 정보보호협력체계 구축 등을 마련하였다. 이 국방사이버 안전 전담기관은 국방 통합 보안관제 및 위협정보를 수집, 분석하고 사이버 위기 대응 전문기관 등과 협력할 수 있도록 했다. 사이버사령부는 2010년 1월 국방부 정보본부 산하에 창설되었으며, 육·해·공군별로 운영 중인 CERT(침해사고 대응 팀)간의 정보 공유 및 주의사항 종합분석, 진단 등의 임무를 수행하고 있다. 이에 따라 사이버사령부가 상당 부분 사이버 안전 전담기관과 역할이 유사하기 때문에 새롭게 신설되기보다는 업무를 지정하는 방식으로 진행된다고 볼 수 있다.

최근 사이버 위협은 단순한 웜·바이러스 유포에서 탈피, 각종 악성코드를 결합한 웹 해킹, 대규모 네트워크를 이용한 DDoS 공격, 무선인터넷 해킹 등 다양한 형태로 고도화 되고 발전하고 있다. 따라서 사이버피해를 최소화하기 위해서는 국가전산망에 대한 이러한 침입시도를 미연에 탐지하는 활동이 중요하다. 현재까지 사이버 위기 대응과 관련된 업무는 소관부처별로 이루어졌으며, 각 부처의 업무범위는 정보자산과 기반시설에 대한 침해사고 대응 및 복구에 한정되고 있다. 따라서 제어시스템이나 주요 정보통신기반시설로 지정되지 않은 시스템은 현행 법체계로는 보호할 수 없어 사이버공격에 무방비로 노출되어 있다. 또한 이에 대한 종합적이고 체계적인 대응이 이루어지고 있지 않아

새로운 국가 안보 위협으로 떠오르고 있는 것이다. 특히 현대의 APT 공격과 같이 고도화된 공격에 의한 사건들을 통해 이미 사이버공격이 국가·사회적으로 파급력이 막대하여 새로운 국가 안보의 위협 요인으로 대두되고 있다는 것을 잘 보여 주고 있다. 현대의 사이버 위기는 바로 국가적인 위기인 것이다. 이미 사이버공격은 국가안보의 새로운 위협요인으로 대두되었으나 민·관 분야별 구분대처로 인하여 한계성에 직면하고 있으며, 특히 APT와 같은 고도화된 공격을 방지하기 위하여 국가 차원의 일원화된 체계적인 사이버공격 대응 조직이 필요한 상황이다.[22]

4.2 국외 사이버공격 대응체계 현황

세계 각국은 사이버전 전담부대를 창설하는 등 사이버공격 대응능력을 국가 및 국방 핵심전략으로 추진하고 있는 상황이다. 이 장에서는 사이버침해를 효과적으로 대응하기 위하여 주요국의 사이버공격 대응체계에 대해 살펴보기로 한다.[22]

1. 미국의 사이버공격 대응체계

미국은 1970년대부터 이미 사이버공격의 심각성을 인식하고 대책을 세우고 법적장치를 마련하기 시작하였으나, 사이버 테러리즘에 대한 구체적인 대응책이 나타나게 된 것은 1991년 걸프전 당시 미 국방부의 사이트가 사이버테러리스트에 의해 해킹당한 사실이 상원 청문회를 통해 밝혀진 이후로 알려진다. 미국은 2003년 2월 14일에 확정된 사이버안보 국가 전략에서 사이버안보를 국가의 주요기반시설의 보호에 한정하지 않고 기존의 개념을 확장한 국가안보차원에서의 사이버안보의 중요성을 재확인하고 주요기반시설 및 핵심자산에 대한 물리적 보호전략과 양축을 이루게 되었다. 사이버안보 국가전략에서 미국은 사이버안보는 국민의 참여 없이 연방정부만으로 수행할 수 없는 매우 어려운 과제이므로 사이버안보에 대한 인식제고와 교육훈련, 기술개발과 취약성 해결 등으로 시장의 활성화, 정보의 공유와 운영계획의 수립 등 민간부문과 공공부문 간의 긴밀한 체계구축을 최우선 원칙으로 제시하고 있다. 또한 사이버 위협의 동적 특성을 고려하여 사이버 위협에 유연하게 대응하고 책임과 의

무를 명확히 하며 지속적인 정책의 필요성을 제시하고, 국가 간의 정보공유, 취약성 감소노력, 사이버 테러리즘 대응을 위한 국제적인 협력체계 구축의 필요성을 강조하고 있다. 2008년 1월에는 부시 대통령이 "NSPD-54/ HSPD-23"을 승인함으로서 이를 바탕으로 한 '국가 사이버보안 종합 전략' (CNCI : Comprehensive National Cyber Security Initiative)이 수립되었다. 이는 신 사이버보안을 위해 결정한 비밀정책으로, 지금까지는 각각의 침입사고에 대한 사후 대응에 비중이 높았다면, 이제 사전 대응체계 구축으로 사이버안보를 달성하겠다는 의지를 나타내고 있다.

오바마 행정부가 수립된 이후에도 역시 사이버보안은 중대한 정책이슈로 주목받게 되었으며, 이는 오바마 대통령이 취임 후 60일 이내에 기존 연방 사이버보안정책에 대한 검토와 향후 전략 수립을 위한 보고서 제출을 국가안보이사회(NSC) 등 관련기관에 요청한데서도 이 같은 의지를 짐작할 수 있다. 이에 따라 최근 2009년 5월 말에는 ① 백악관, 연방차원 등 최상위 리더십에 따른 정책 추진, ② 보안교육, 전문 인력 양성 등 디지털 국가를 위한 역량 제고, ③ 민 · 관 협력을 위한 파트너십 구축 등 사이버보안 책임 분배, ④ 효율적인 정보 공유 및 대응 능력 강화, ⑤ 보안 강화를 위한 혁신 촉진 등을 내용으로 하는 '사이버공간 정책 리뷰 (Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure)'를 발표하였다. 동 보고서에서는 단기 실행 계획(10개) 및 중기 실행 계획(13개)을 제시하고 있으며, 특히 단기실행계획 첫 번째로 국가 사이버보안정책 추진을 총괄할 사이버보안책임관을 임명할 것을 제안하고 있다. 이에 따라 오바마 대통령은 선거 공약에서부터 우선과제로 강조해 온 사이버보안에 대한 실질적인 정책 실현을 위한 범부처간 조정자로서 이른바 사이버 차르(Cyber Czar)로 불렸던 사이버보안조정관을 2009년 12월 22일 임명하였다. 사이버보안조정관은 미국 국가안전보장회의(NSC)에 상주하면서 대통령과 NSC에 정기적으로 보고하며, 미군과 민간기관의 연방정부 사이버보안정책 마련을 위한 자문관으로 역할을 수행하고 있다. 특히, 최근 2010년 5월 27일 오바마 정부는 출범 후 처음으로 국가안보의 현황과 지향점을 공개 발표한 국가안보전략(NSS : National Security Strategy)에서 사이버보안의 의미와 향후 정책 방향을 중요한 전략으로 다루고 있다. 즉, 국가안보와 공공안전 및 국가경제에 위협을 주는 사이버공간에서의 불법행위와 테러, 해킹 등을 안보 이슈로 인식하여 디지털 인프

라를 국가의 주요 자산으로 관리하겠다는 의지를 천명하였다. 이를 위해 관련 인력과 기술부문의 투자를 과감하게 늘리고, 공공 · 민간 · 학계 등 관련 부문 파트너십을 강화하는 방향으로 사이버보안 강화정책을 펼칠 것임을 밝혔다. 이처럼 미국은 사이버보안과 관련한 정책을 추진하는데 있어 가장 의욕적이고 강력하게 추진하고 있는 대표적인 나라로 평가되고 있다.

2. 영국의 사이버공격 대응체계

영국은 기술적인 측면에서 미국과 함께 사이버안보 분야를 선도하고 있는 국가 중 하나이다. 영국 정부의 정보보호에 대한 노력은 법률에 의한 행위규제 보다 일반 국민에게 정보침해에 대한 의식을 제고하고 사전적 대처 방안계획과 실행 역할에 중점을 두고 있다. 조사권한규제법(RIPA), 컴퓨터부정사용법, 대테러 범죄 및 안전 보장법 등으로 해커와 바이러스 유포자를 처벌하고 있으며, 스팸 관련규제는 프라이버시법리와 전기통신지침 등으로 이루어지고 있다.

영국은 정보통신 환경 변화와 이에 따른 정보보안 환경 변화에 적극적으로 대처하고 있으며, 이에 따라 정보보안과 관련한 입법 활동도 비교적 활발한 국가 중 하나이다. 영국은 EU의 기본적 정보보안 및 개인정보보호 방침을 자국 법으로 수용하는데 적극적이며 미국·EU 등 타 국가들이 주도적으로 추진하는 정보보안정책들을 받아들이고 있다. 정보보안과 관련해서 영국은 사이버범죄를 처벌할 수 있는 법률을 중심으로 상당히 적극적으로 관련 법률과 제도를 발전시켜왔으며, 특히 EU의 각종 지침을 자국 법으로 현실화시켜 국제적으로도 정보보안을 선도하고 있다.

영국의 사이버 안전체계를 보면, 네트워크 및 정보보호 정책은 내각부 산하의 정보 보증 중앙지원국(CSIA : Central Sponsor for Information Assurance)에서 정보보호 관련 활동에 대해 정부전체를 조정하며, 통상산업부(DTI : Department of Trade and Industry), 외무부 산하 정부통신총국(GCHQ : Government Communications Head Quarters)·통신전자보안단(CESG : Communications Electronics Security Group) 및 내무부 보안정보부(M15) 산하 국가기반보호센터(CPNI : Center for the Protection of National Infrastructure) 등이 국가전반에 걸친 정보보호 기관으로서 역할을 수행하고 있다. 정보보증중앙지원국(CSIA)에서는 2007년 국가정보보안정책(A National Information Assurance Strategy)을 발표하여, 기관의 효율적인 위협정보 관리를 위해 임원급

의 책임과 의무를 강조하는 한편, 전문 기술인력 양성 및 홍보 정책을 추진하고 있다. 내각부는 정부기관의 보안정책을 확산시키기 위한 '정보보호 기본정책' (HMG Security Policy Framework, 2008년 12월) 등 정보보호 관련 정책을 발표한 바 있다.

3. 독일의 사이버공격 대응체계

일반적으로 독일에서 IT 의존적 중요기반시설의 안전 및 보안개선의 필요성 인식과 필요조치 실행 의지는 서서히 지속적으로 높아가고 있다. 특히 미국의 9·11 사건 이후 막연한 절박감을 가지게 되어 국제적 협력에 관심을 기울이고 있다. 독일의 사이버 안전체계는 '연방정보기술안전청설치법' (BSIG : BSI-Erri-chtungsgesetz)에 의해 설립된 연방정보기술안전청(BSI : Bundesamt für Sicherheit in der Information stechnik) 및 연방통신망청법상의 연방 통신망청(BNetzA)이 주로 담당하고 있다. 1991년에 설립된 내무부 산하 '연방 정보 기술 안전청' 은 실질적인 국가 사이버 안전업무를 총괄하는 기관으로서 정보기술을 적용했을 때 야기되는 보안위험을 연구하고 보안조치, 정보기술보안을 위한 기술적 방법과 장치는 물론, 정보기술 시스템 및 그 구성요소에 대한 검사·평가를 위한 기준·방법 및 도구를 개발하여 정보기술 시스템 및 그 구성요소의 보안을 검사·평가하여 보안 인증서를 부여하고 있다.

한편, 경찰 및 형사소추기관의 법적 임무를 지원하며, 테러활동 감시 등 정보활동을 통하여 수집한 첩보를 활용, 평가하는 작업을 지원함과 동시에 정보기술보안 문제 발생 시 생산자와 유통자 및 사용자에게 자문 등의 임무를 수행하기도 한다. 독일은 정보 보안을 통해 정보통신기술의 신뢰를 조성하고 정보사회의 기회를 최대한 이용하기 위해 독일 자체의 정보보안 가이드라인(IT-Grundschutz-die Basis für ITSicher-heit)을 제정하여 시행하고 있다. 독일은 미래사회에서의 정보보호 및 정보보안에 대한 중요성을 깨닫고 1991년에 BSI를 창설하여 상당한 예산 및 인력투자를 해 왔다. 독일의 경우 정보보안을 위해 국가적 차원에서 상당한 지원을 하고 있고 사경제 분야에 있는 기업도 점차 정보 보안과 관련한 책임의 중대성을 인식하고 대비책을 마련하는 과정에 있다.

4. 프랑스의 사이버공격 대응체계

프랑스는 선진적으로 정보화가 진행된 서유럽의 다른 국가와 비교할 때 상대적으로 정보화가 늦은 나라였다. 1990년대 중반까지만 해도 프랑스는 이웃 선진유럽국가에 비하여 행정의 정보화뿐만 아니라 사회 전체의 정보화가 뒤져 있었다고 평가된다. 그러나 1998년 이후 매우 의욕적이고 계획적으로 정보화를 추진하고 있는 것으로 알려진다. 프랑스는 중앙 정보 시스템 보안국(DCSSI) 내에 프랑스 정부 CERT인 CERTA를 구축 운영하고 있으며 사이버보안 운영센터를 구축하여 각급기관에 대한 사이버 위협정보를 제공하고 있다. 아울러 프랑스 정부는 사이버보안 위기관리 체계를 수립하여 경계 수준을 5단계로 분류하고 DCSSI로 하여금 각 경계단계에 따른 일련의 사이버보안 기능적 조치를 수행하도록 하고 각 정부부처로 하여금 사이버보안 조치를 실행하도록 하고 있다.

이렇듯 프랑스는 사이버보안을 국가 안보의 문제로 인식하여 총리실 직속의 국방 사무국(General Secretariat of National Defense : SGDN)으로 하여금 사이버보안을 담당하도록 하고 있다. 즉 1996년 1월 29일에 발표된 프랑스 법령 96-67은 국방사무국으로 하여금 정보 시스템 보안(Information Systems Security)에 대한 책임을 부담하도록 명확하게 규정하고 있다. 또한 2001년 7월 31일에 발표된 프랑스 법령 2001-693은 국방사무국내에 중앙 정보 시스템 보안국(Central Directorate for Security of Information Systems : DCSSI)을 설립하여 사이버 공간과 프랑스 정보 시스템에 대한 보안을 수행하고 신뢰할 수 있는 정보화 사회를 조성하도록 하고 있다.

5. 일본의 사이버공격 대응체계

일본은 이미 과학 · 기술 선진국으로서 첨단 정보통신기술 능력을 갖추었지만 사이버공격 대비 능력은 막강한 경제력과 첨단기술력에 비추어 다소 뒤떨어져 있는 것으로 알려지고 있다. 이제 일본은 사이버공격에 대응하기 위한 다양한 대책을 마련해 나가고 있다. 일본에서는 아직까지 심각한 사이버 테러리즘은 발생하지 않고 있으나, 최근 들어 해킹 사례와 컴퓨터범죄가 급증하고 있다. 이에 대한 대책과 사이버 테러리즘을 미연에 방지하기 위해 통상 산업

성 주관으로 국민생활과 직결된 전력, 석유 산업 등의 컴퓨터 네트워크 현황을 분석하고 사이버 테러리즘 가이드라인을 작성하는 등 적극적인 대응에 나서기 시작했다. 2001년 1월, 일본 정부의 웹 사이트들과 민간 웹 사이트들이 외부의 무차별 공격에 순식간에 다운당할 정도로 일본의 사이버공격에 대한 취약성은 잘 알려져 있다. 또한 사이버공간 상에서 일본의 난징대학살을 비난하는 중국인들의 시위의 일환으로 일본정부의 웹 사이트가 무차별 공격을 받자 일본 정부는 방위청을 선두로 본격적으로 사이버공격 대응체계 구축을 시작하였다.

일본은 정부기관인 관방성 주도하에 사회기반 및 생산설비에 대한 사이버 테러리즘 대책을 수립 · 시행하였다. 1997년 8월, 정부 주도하에 정보보안대책실을 설치하고 국가적 정보보안대책을 추진하여 대규모 공장설비 네트워크의 보안대책위원회를 구성하여 네트워크 보호기술 및 운영체제의 표준화를 추구하고 보안수준을 향상시키기 위해 필요한 대책을 제안하였다. 1999년 9월 관방성·경찰청·방위청·금융 감독청 등 13개 기관의 국장급으로 정보 보안 관계부처 회의체인 정보 보안 관련 성청 국장 회의를 구성하고, 2003년을 목표로 해커 대책 등 기반 정비 행동 계획을 수립 발표하였다. 2000년 12월 '중요 인프라의 사이버 테러 대책에 관한 특별 행동 계획'을 발표하고 정부의 내각관방을 중심으로 관·민의 긴밀한 협력 하에 이 계획을 실시하기로 하였으며 민간의 주요 인프라 사업자 등도 이 계획을 토대로 자율적인 대책을 강구하도록 하였다. 미국의 9·11 사고 이후에는 사이버 테러리즘 대책 강화 등을 중점 추진사항으로 하여 사이버테러 특별행동계획과 그 후속조치를 마련하는 등 진일보한 대책을 서둘러, 2002년 4월 e-Government 사이버공격에 대한 정보공유와 사이버 테러리즘에의 긴급 대응을 임무로 하는 NIRT(National Incident Response Team)를 설치하였고, 경찰청 산하에 전문 기술가들로 Cyber Force를 구성하였다. 2003년 10월 국가 정보 보안 종합 전략을 수립·발표하고 내각관방의 사이버 테러리즘 대응 조직과 역할을 강화하였으며 민·관 공동 감시체제인 정보 방위 센터 설치를 추진하고 있다. 2006년 2월 내각관방에서는 국가 전반의 정보보호 요구에 대응하기 위해 '제1차 정보보호 기본계획'을 수립하여 추진하였다. 정부 · 지방공공단체, 주요 인프라, 민간(개인 및 기업)을 대상으로 '정보보호 기본계획'의 주요 대책을 2006년에서 2008년까지 3년간 추진하였으며, 정부 · 지방공공단체, 주요 기반, 기업, 개인 영역으로 구분하여

‘Secure Japan 200X’ 를 수립하고 실행성과를 평가하고 있다. 또한, 총무성에서는 u-Japan 정책을 통해 정보화 역기능에 관한 100대 과제를 정리한 ‘ICT 안심·안전 21 전략’ 을 추진 중에 있다. 경제 산업성에서는 정보보호 위협에 대한 국제적 대응, 국제경쟁력 강화 기반 마련, 국내외 다양화된 환경변화 대응을 위한 글로벌 정보 보호 전략을 추진 중에 있는 바, 이처럼 일본은 정보통신강국답게 국가기관협의체를 구성하여 사이버 테러리즘에 대치하고 미래의 사이버전에 대비하기 위하여 체계적인 정보보안대책을 마련하고 있는 것으로 평가된다. 최근 2009년 2월에는 ‘2차 정보보호 기본계획’ 을 마련하였다. 제2차 계획은 2009년도부터 2011년도까지 3년간을 대상으로 일본 전체 정보보안 문제에 대한 대책을 추진하기 위한 계획이며, ‘고품질, 고신뢰성, 안전 안심’ 을 추구하는 일본모델을 구현하고 “새로운 민관 협력 모델” 의 구축을 목표로 함을 명시하였다. 최근 2010년 7월 일본정부의 ‘정보 보안정책 회의’ 는 각부 부처가 실시하는 보안 대책을 정리한 계획 ‘정보 시큐리티 2010’ 을 결정했다. ‘정보 시큐리티 2010’ 은 2010년에서 2013년도에 이르는 4개년 계획으로 수립되었다. ‘국민을 지키기 정보 보안 전략’ 에서는 2014년까지 정보 보안에 대한 국민의 불안을 해소, 2020 년까지 세계 최첨단의 ‘정보 보안 선진국’ 을 실현하는 것을 목표로 각 기관이 2010 ~ 2011년도에 실시하는 196개의 시책을 제시하고 있다. ‘정보 시큐리티 2010’ 시책의 내역은 대규모 사이버공격에 대한 대처, 정보 보안정책의 강화 시책으로 구성되어 있다. 대규모 사이버공격에 대한 대처 시책으로는 적절한 초동 대처를 위해 내각 관방에 태세를 정비하고 훈련을 실시하거나, 방위성에 사이버 기획 조정관 (가칭)을 배치하는 것과 정보 수집 공유 체제 구축 강화 등이 있다. 구체적인 시책으로 각 행정 기관의 최고 정보 보안 책임자(CISO)에 의한 ‘정보 보안 대책 추진회의’ 를 설치하거나 범정부 정보 수집 분석 시스템의 충실 강화, 핵심 인프라 기반 강화, 클라우드화에 대응하는 정보 보안 확보 정책의 검토, (가칭) 정보 보안 안심 창구 검토, 사이버 범죄에 적절히 대처하는 법 정비의 추진 등을 들 수 있다.[22]

5. 국가 보안지식베이스(Knowledge-Base) 구축 방안

우리나라의 사이버공격 위기관리 체계에서 각 부분별로 서로 다른 조직에 속한 IT 보안 관리자들은 많은 같은 위협들에 직면하고 유사한 해결 방안을 사용하며, 같은 지식을 수집하고 적용 한다. 그러나 그들은 대부분 그들 자신에 의존하여 일을 수행하고 있으며, 이것은 매우 비합리적인 방식이라고 할 수 있다. APT 공격과 같은 고도화된 사이버 위협에 효과적으로 대응하기 위해서 이와 관련된 국가적인 공통의 지식 베이스 체계를 구축함으로써 범국가적으로 다양한 공공기관 및 민간 기업 그리고 군의 보안 관리자들에게 효율적인 서비스를 제공 할 수 있으리라 생각된다.

또한 미래사회는 물리공간과 논리공간이 융합되고 가상공간의 활용이 증대되어 다양한 스마트객체의 유기적인 연결을 통한 상시 연결사회가 보편화될 것으로 예상된다. 따라서 이러한 환경을 이용한 공격도 다변화되고 복합화 될 것으로 예상되며 다양한 정보의 유기적 관계분석을 통한 보안지식 빅 데이터 수집/저장과 장기간의 트래픽 행위분석을 통하여 APT 공격 또는 전문가 공격을 효과적으로 분석/파악하지 못한다면 이러한 위협을 대처하기 어려울 것이다.

더군다나 각국이 사이버전에 대한 필요성을 강조하고 있는 시점에 이와 관련한 부분은 더욱 중요하게 될 것이므로 향후 다양한 미래서비스 환경변화와 상시 연결사회의 보편화에 따른 새로운 유형의 사이버 위협에 능동적으로 대응하기 위한 기반으로써의 국가 차원의 보안지식베이스 구축전략에 대한 연구는 매우 필요하다고 할 수 있다.

지식 베이스체계를 구축하기 위해서는 공통의 보안지식베이스를 생성하기 위한 전략이 첫 번째 단계이고 두 번째로 국가 정보통신서비스 인프라의 안전을 도모하기 위한 선제적 공격대응이 가능한 국가 보안지식 관리 모델 개발이 필요하며, 신뢰를 통한 지식 공유방안 및 공유된 지식을 서비스하기위한 전략이 수립되어야한다. 다음 그림 27은 보안지식베이스 구축을 위한 보안지식베이스의 데이터 생성 예이다.

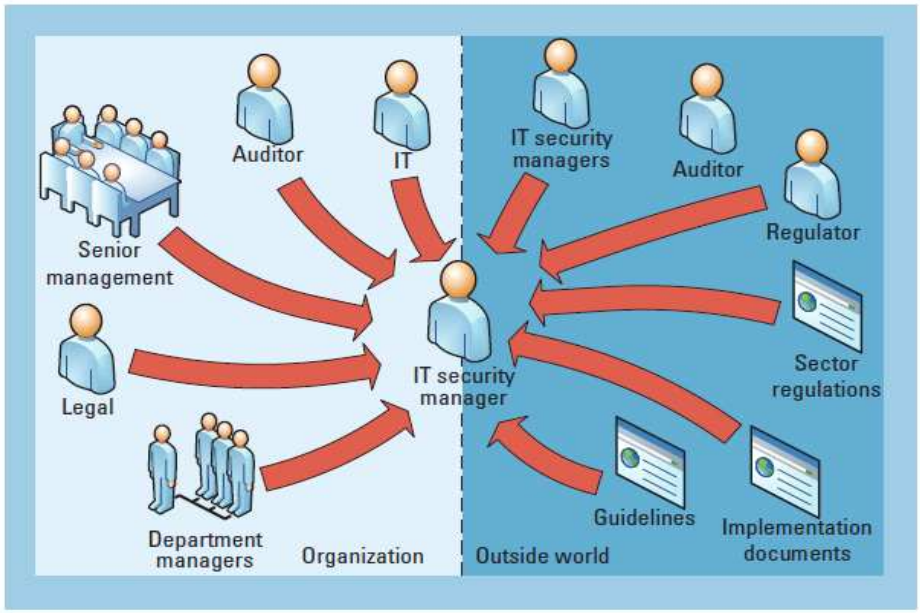

그림 27. 보안지식베이스 구축을 위한 보안지식베이스의 데이터 생성 예

5.1 현황 분석

기존에 국내에서 수행된 사이버공격 대응 연구는 한국인터넷진흥원에서 수행된 봇 넷 능동형 탐지 및 대응 기술과 한국전자통신연구원에서 개발한 자스민 시스템이 대표적이라고 할 수 있다. 그러나 이 두 가지 연구 다 APT 공격과 같은 고도화된 공격에 대응하기에는 부족한 점이 존재한다. 한국인터넷진흥원에서 수행된 봇 넷 능동형 탐지 및 대응 기술은 서버의 봇 감염 여부는 알 수 있으나 서버를 통해 감염된 호스트의 정보는 알 수 없는 단점이 있으며, 한국전자통신연구원에서 개발한 자스민 시스템도 사이버공격에 대한 공격 시그니처를 실시간으로 생성하고 관리할 수 있지만 비정상행위 분석 시 분석을 통한 결과가 악성코드 데이터베이스하고 매칭이 안 되는 단점을 가지고 있다. 그리고 두 시스템 다 악성코드별 분포 현황, 악성코드 전달 경로 현황, 좀비 연계도 현황 등 고도화된 사이버공격에 사전 대응을 하기 위한 정보 구축이 불가능한 상황이다.

현재 국내에서도 APT공격과 같은 고도화된 공격에 대하여 안랩, 트랜드마이크로 등의 기업과 한국인터넷진흥원에서도 대응방안을 연구하고 있는 중이

다. 각각의 연구에서는 APT의 피해 사례 분석을 통하여 APT 공격의 특성을 파악하고 APT 공격을 단계 별로 분석하여 다 계층화된 데이터 중심의 깊이 있는 방어 대책을 수립하고 있는 중이다. 그러나 아직까지도 완전하다고 할 수 있는 해결 방안은 없으며 특히 국가적인 대응체계에 대한 연구는 미진한 편이다. 그리고 현재 우리나라의 사이버 위기 대응기관으로는 국가정보원의 국가 사이버 안전센터, 국방부의 사이버사령부, 방송통신위원회(산하 한국인터넷진흥원)의 인터넷 침해사고 대응 지원 센터를 주축으로 대검찰청 인터넷 범죄 수사 센터, 경찰청 사이버 테러 대응 센터, 국가 보안 기술 연구소, 정보공유 분석 센터(ISAC)등이 다양하게 존재하고 있으나 이들 간의 협력체계를 뒷받침할 법체계가 미비하고 사이버침해 발생 시 신속하고 강력하게 이를 대응할 체계가 미흡한 실정으로 개선이 필요함을 알 수 있다. 따라서 APT 공격과 같은 새로운 유형의 사이버 위협에 능동적으로 대응하기 위하여 국가 차원의 보안지식베이스 구축 전략 및 이를 기반으로 한 사이버 위협 대응체계에 대한 연구가 필수적으로 수행되어야 한다.

일반적으로 악성코드를 탐지하는 방법은 misuse 기법이나 비정상행위 분석 기법에 의한 탐지 기법을 사용한다. 안랩 등의 백신의 경우 misuse 기반 탐지 방법을 사용하므로 이미 알고 있는 악성코드에 대한 정확한 탐지는 가능하지만 새로운 악성코드에 대한 탐지가 불가능하다. 따라서 새로운 악성코드를 탐지하기 위해서는 비정상 행위 기반의 탐지 또는 행위 분석을 통한 탐지가 가능하다. 네트워크를 통해 많은 정상적인 실행 코드와 백신 등에서 탐지가 가능한 악성코드들이 전달되고 있다. 이러한 정상 실행 코드나 알려진 악성코드를 네트워크에서 실시간으로 확인할 수 있는 지식데이터베이스가 구축되고, 이를 실시간으로 확인할 기술이 개발된다면, 데이터베이스에 존재하지 않는 실행코드를 집중 분석하여 새로운 악성코드를 찾을 수 있는 기회가 만들어 질 수 있다. 하지만 현재 이러한 데이터베이스가 존재 하지 않을 뿐만 아니라, 알려진 악성코드가 호스트로 유입되어도 전체 네트워크에서 이를 알 수 있는 시스템이 없어 국가적으로 악성코드의 유포나 감염 정도를 실시간 모니터링 할 수 없는 상황이다.

모든 실행 가능한 코드가 국가 네트워크에서 어떻게 유포되고 있으며, 국가 데이터베이스에 존재하지 않는 새로운 코드가 유포되고 있는지 실시간으로 모니터링 할 수 있는 국가 보안지식 데이터베이스 구축 및 실시간 검색 기술을 개발함으로써 국가의 보안을 한 단계 업그레이드 할 필요가 절실한 상황이다.

5.2 추진 체계

국가 보안지식베이스란 국내에서 사용되는 모든 실행 가능한 코드에 대한 국가 데이터베이스를 지칭하는 것으로, 이러한 데이터베이스는 정상 파일들과 국내에서 유통되는 모든 종류의 백신에서 탐지되는 악성코드에 대한 데이터베이스를 구축하고 네트워크를 통해 전달되거나 호스트에 새로 유입된 실행 코드를 확인하여 실행 코드의 유통을 검색 제어할 수 있는 국가 정보 시스템을 말한다. 국가 보안지식베이스 구축을 위하여 본 연구는 “안전하고 신뢰할 수 있는 스마트 정보 사회 구현”의 비전을 가지고, “고도화된 사이버 위협에 대응하기 위한 국가 보안지식베이스 구축”을 목표로 한다. 이 목표를 이루기 위하여 다음과 같은 추진전략을 수립한다.

- 고도화된 사이버 위협에 대응하기 위한 정부주도의 국가 보안지식베이스 구축 환경 조성
- 국가 차원의 보안지식베이스의 단계별 추진을 위한 중장기 계획 수립

위의 추진 전략을 기반으로 다음과 같은 추진 과제를 선정하여 수행한다.

- 보안지식베이스 구축 및 활용 프로세스 수립
- 보안지식베이스 시스템 운영 및 서비스
- 보안지식베이스 업무 전담조직 신설
- 위기 대응체계 구축 및 인력양성
- 법제도 개선

국가 보안지식베이스 구축을 위한 전략은 다음 그림 28과 같다.

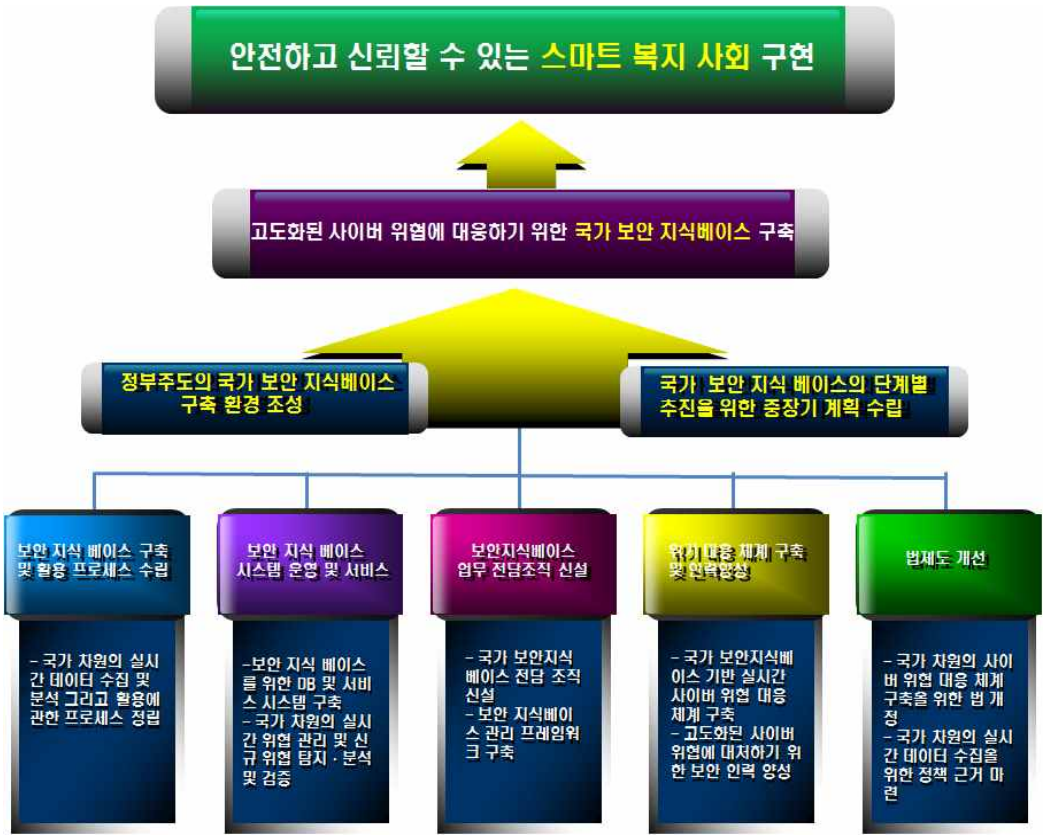

그림 28. 국가 보안지식베이스 구축을 위한 추진 체계

5.2.1 추진 전략

1. 고도화된 사이버 위협에 대응하기 위한 정부주도의 국가 보안지식베이스 구축 환경 조성

범 국가 차원의 실시간 보안지식베이스의 구축 및 관리 그리고 이를 기반으로 하는 사이버 위협대응체계 구축은 오직 정부만이 추진할 수 있다. 정부의 주도하에 조성할 수 있는 보안지식베이스의 구축 및 환경에 관한 내용은 다음과 같다.

- 실시간 보안지식베이스 구축을 위하여 국가 차원의 대규모 데이터 실시간 수집 기술 및 분석 기술 개발을 위한 재원 확보

- 신뢰할 수 있는 보안지식베이스 구축 환경조성을 위하여 기본 트래픽 데이터 정보 및 활용 데이터베이스 정보에 대한 검증 및 부실 요소 제거

- 최신의 화이트리스트 및 블랙리스트 데이터베이스의 구축을 위하여 유관기관의 연계 프로세스 수립 및 관련 사업 지원

- 보안지식베이스를 기반으로 범 국가 차원의 위기 대응체계를 구축하기 위하여 유관기관 과의 업무 협조 체제 구축

- 최신의 보안지식베이스 구축을 위하여 관계 법령 개정을 통한 실시간 데이터 수집을 위한 근거 마련

- 보안지식베이스가 적극적으로 활용될 수 있도록 대응기관, 학계, 산업계 등에 객관성이 부여된 양질의 정보 제공

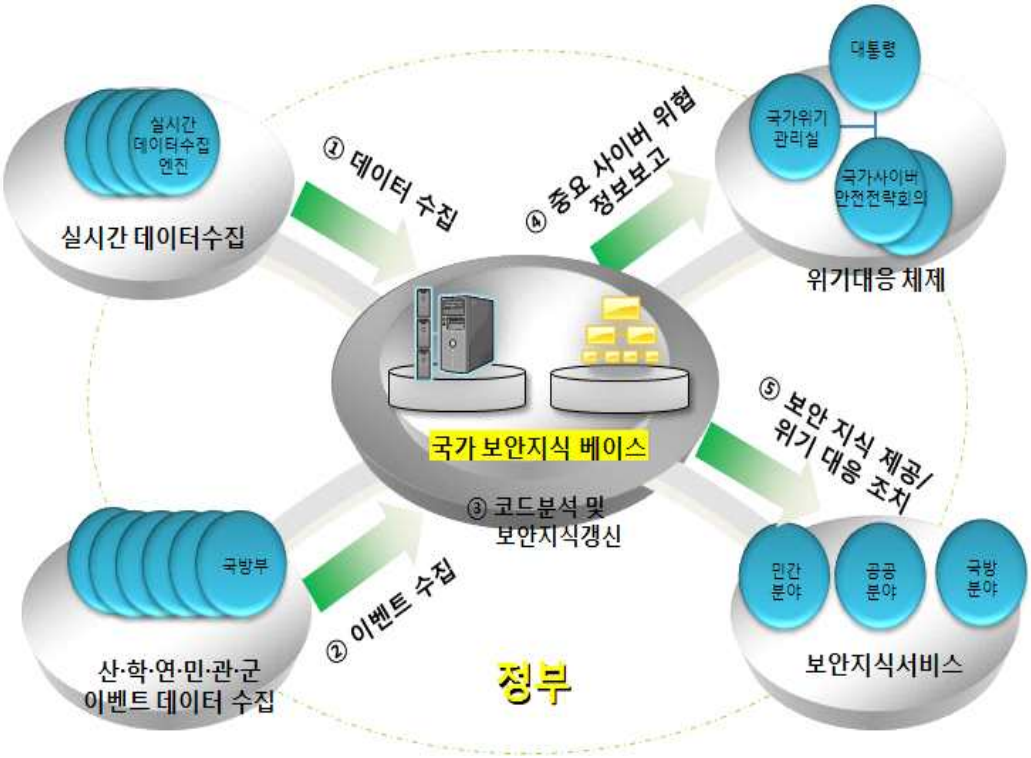

그림 29. 국가 보안지식베이스 구축 환경 조성 개념

2. 국가 차원의 보안지식베이스의 단계별 추진을 위한 중장기 계획 수립

국가 차원의 보안지식베이스의 단계별 추진을 위한 중장기 계획은 다음과 같다. 1단계(1차년도)는 보안지식베이스 구축 마스터플랜 도출을 통하여 중장기 계획을 체계적으로 마련하는 단계로 그 내용은 다음과 같다.

- 보안지식베이스 구축 프로세스의 확립 및 관련 제도를 제·개정하기 위한 준비

- 보안지식베이스 전담 조직을 신설하는 등 성공적인 정보공유 체계 구축을 위한 중장기 종합 계획 수립 단계

2단계(2차년도~3차년도)는 수립된 계획의 추진단계로 국가 차원의 보안지식베이스 시스템을 구축하며, 그 내용은 다음과 같다.

- 국가 차원의 실시간 데이터 수집 및 분석 프로세스 구축

- 보안지식베이스 구축프로세스를 도입하고, 실시간 트래픽 수집 및 데이터 분석을 통합관리하기 위한 데이터베이스 및 관리 시스템 구축

- 보안지식베이스 시스템 이용을 위한 사용자 인터페이스 개발

- 국가 보안지식베이스를 기반으로 한 위기 대응 체제 구축

- 국가 차원의 보안지식베이스 체계 구축 및 위기 대응 체제 구축을 위한 법·제도의 제·개정 추진

3단계(4차년도 이후)는 국가 차원의 보안지식베이스 체계 정착 및 고도화 단계로 정보주도로 시스템을 운영하여 국가 위기 대응체계를 갖추고 산·학·연·민·관·군이 함께 활용하는 단계로 그 내용은 다음과 같다.

- 실시간 위기 대응체계의 고도화를 위하여 실시간 데이터 수집 및 분석 프로세스의 양적·질적 향상을 도모

- 고도화된 사이버 위협에 대응하기 위하여 실행코드 블랙리스트 및 화이트리스트 데이터베이스의 고도화

- 실행 코드 데이터베이스의 공유 채널을 미국이나 일본 등 국외로 확대

- 국가 보안지식베이스를 기반으로 한 위기 대응 체제의 고도화

그림 30. 국가 보안지식베이스 추진을 위한 중장기 계획

5.2.2 추진과제

국가 보안지식베이스를 구축하기 위한 추진 과제는 다음과 같다.

1. 보안지식베이스 구축 및 활용 프로세스 수립

국가 차원의 실시간 데이터 수집 및 분석 그리고 위기 대응체계에 관한 프로세스를 정립하고, 보안지식베이스 전담 기관의 데이터 수집 및 타 기관에서 수집된 정보의 지식 베이스 화 및 보안지식베이스의 활용 프로세스를 수립한다.

국가 보안지식베이스 구축을 위하여 다음과 같은 단계를 수행하도록 한다.

(1) 정상 파일에 대한 데이터베이스 구축을 위해 국내외에서 개발된 정상 파일에 대한 시그니처와 해시 값 등을 화이트리스트로 구성한다.
(2) 국내외에서 유통되는 백신들을 설치한 시스템을 클라우드로 구성하고 네트워크에서 수집된 모든 실행 파일을 검사하여 탐지되는 경우 자동으로 시그니처 및 해시 값 등을 추출하여 블랙리스트를 구성한다.
(3) 이외 현재까지 개발된 비정상행위 탐지 기법 및 실행 기반 악성 유무 탐지를 위한 시스템을 클라우드로 구성하고 1, 2에서 확인되지 않는 모든 파일을 검사하여 화이트리스트, 블랙리스트, undefined 등의 데이터베이스를 자동 구축한다. 또한 새로운 탐지 기법이 되면 이를 수용하기 위한 open API를 개발한다.
(4) 이들 데이터베이스를 구성하고 네트워크에서 전달되는 모든 파일에 대해 실시간 모니터링 할 수 있는 GUI를 구성하여 국가 네트워크에서 전달되는 모든 실행코드의 악성유무를 파악하고, 데이터베이스의 블랙리스트에 매칭된 코드는 자동 행위 추적 또는 자동 차단하는 기능을 수행하여 새로운 공격에 대응 한다.

보안지식베이스 활용을 위한 시나리오는 다음과 같다.

- (시나리오 1) 사이버 위협에 대응하기 위하여 보안지식베이스 전담 기관에서 직접 데이터를 수집 및 분석 후 조치하는 경우의 보안 지식 활용 프로세스

① 실시간 데이터 수집 및 분석 또는 유관 조직에서 제공한 정보 제공을 통해 보안 지식이 될 수 있는 정보 수집

② 보안지식베이스 전담 기관은 수집된 데이터의 분석 및 보안지식베이스화를 수행하고 유관 기관과의 협력을 통하여 필요하다면 패치 제작과 패치 검증을 수행하고 위기관리 대응체계에 따라서 민간, 국가·공공, 국방 분야 등 국가적인 사이버 위협 대응을 수행하도록 한다.

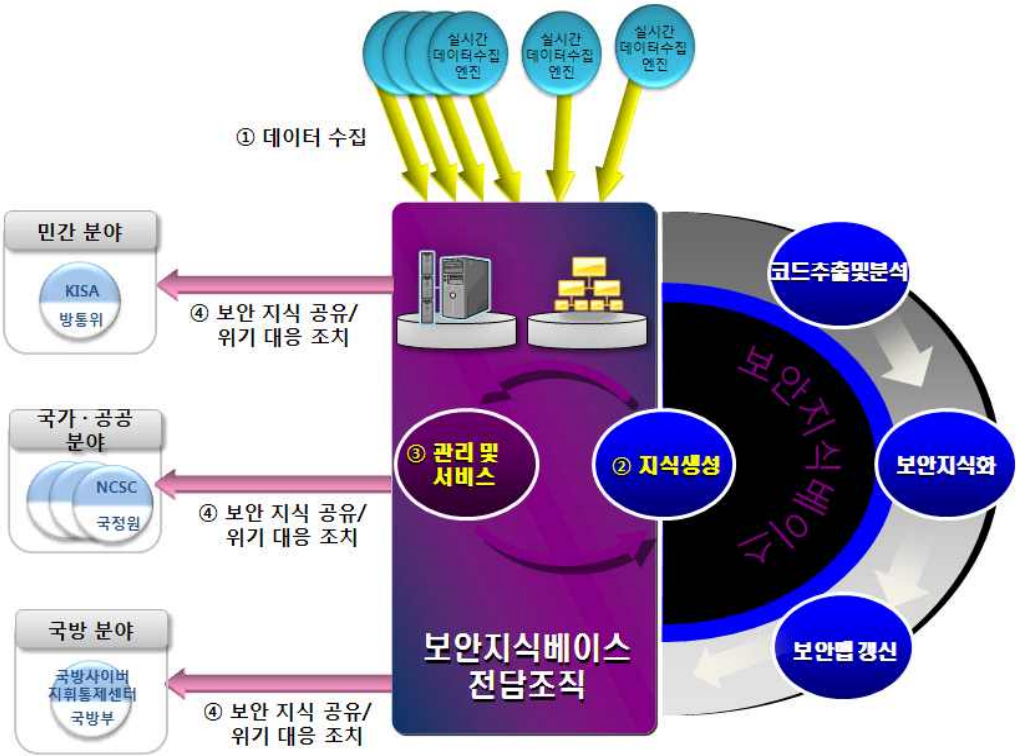

그림 31. 국가 보안지식베이스 활용 시나리오 1

- (시나리오 2) 기존 관련 분야 즉 민간, 국가·공공, 국방 분야의 정보보호 업무를 담당하는 기관에서 악성코드 관련 정보 등을 수집한 경우의 보안지식베이스 정보 구축 및 활용 프로세스

① 기존 악성코드 수집 시스템 및 신고접수로 악성코드 관련 정보가 각 관련 부처별(KISA, NCSC, NETAN 등)로 수집되는 경우 보안지식베이스 전담 조직으로 전달되어 분석 및 검증을 거쳐 보안지식베이스화를 수행한다.

② 보안지식베이스 전담 기관은 타 기관에서 수집된 정보를 기반으로 악성코드 전달 이력 보안 맵을 갱신하고, 위기관리 대응체계에 따라서 민간, 국가·공공, 국방 분야 등 범국가적인 사이버 위협 대응을 수행하도록 한다.

그림 32. 국가 보안지식베이스 활용 시나리오 2

- (시나리오 3) 국가적 차원의 축적된 보안지식베이스를 이용하여 실시간 좀비 현황, 악성코드 전달 경로, 지능화 및 고도화된 사이버 위협 정보, 특정 IP의 과거 이력 정보 등을 실시간으로 조회하는 프로세스

① 국가적인 보안지식베이스 정보 구축을 통하여 고도화된 사이버 위협과 관련된 신뢰할 수 있는 정보를 제공받을 수 있게 된다.

② 해당 권한을 가진 사용자는 IP나 도메인과 같은 식별 정보를 이용하여 보안지식베이스 전담 조직에서 관리하고 있는 사이버 위협 관련 정보를 검색한다.

③ 보안지식베이스 전담 조직은 요청된 정보를 사용자에게 제공하여 고도화된 사이버 위협에 대응할 수 있도록 한다.

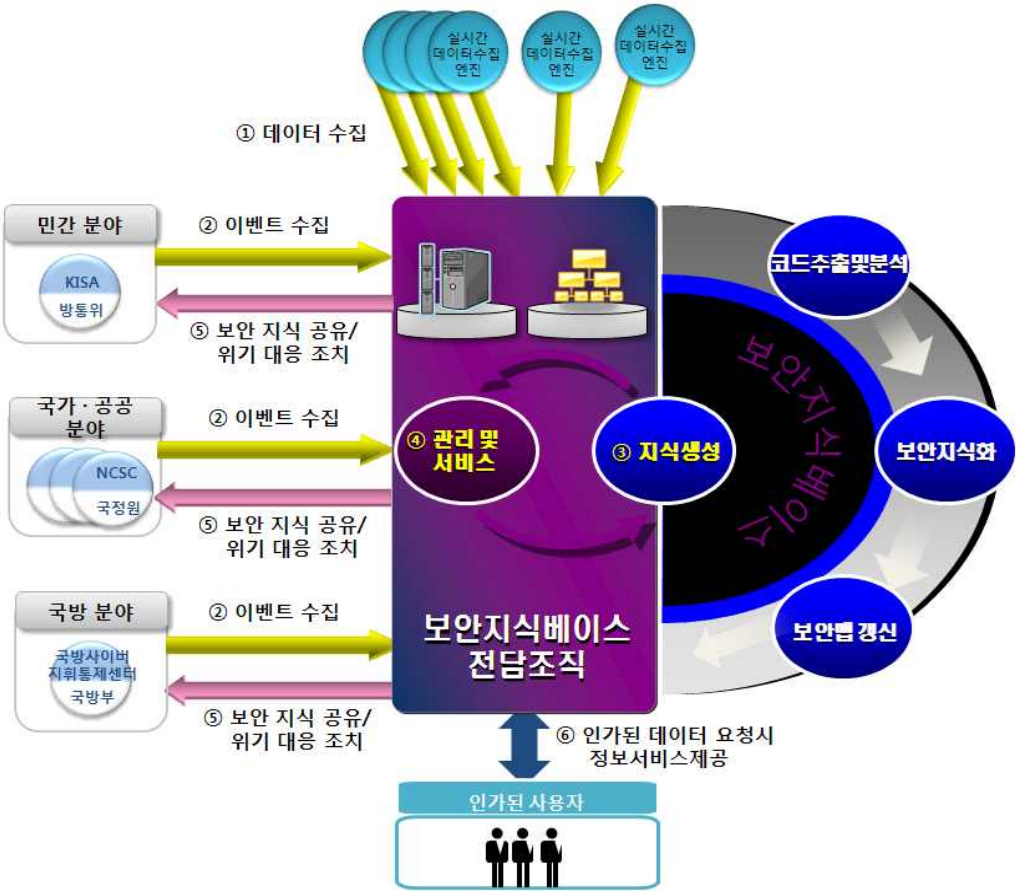

그림 33. 국가 보안지식베이스 활용 시나리오 3

그리고 사이버 위협의 위험도 및 시급성에 따른 위협 대응 프로세스를 수립한다.

- 사이버 위협 정보마다 다수의 이해관계자가 존재함에 따라 정보마다 이해관계자별 역할을 구분하고 이해관계자별 필요한 정보를 제공한다.

- 사이버 위협 정보의 위험도, 시급성 등에 따라 위협 대응체계의 프로세스를 결정하며, 위험도가 큰 경우에 정부 및 산·학·연 전문가로 구성된 심의위원회를 통해 대응방안을 결정한다.

2. 보안지식베이스 시스템 운영 및 서비스

국가 차원의 보안지식베이스 시스템 구축 운영을 위해 다음과 같은 사항이 수행되어야 한다.

- 악성코드 등 위협 관련 이벤트 정보의 실시간 수집, 분석 및 지식베이스화를 자동화 할 수 있는 보안지식베이스 시스템을 구축한다.

- 정부, 산업계, 학계, 연구소 등에서 권한을 가진 사용자가 접근하여 보안지식베이스 정보를 이용할 수 있는 인터페이스를 개발한다.

- 화이트리스트, 블랙리스트, 악성코드 이동 경로 보안 맵 등 보안지식베이스를 위한 데이터베이스를 구축한다.

- 수집된 악성코드 등 위협 관련 이벤트 정보를 분석 및 검증하고 관리하기 위한 통합관리 시스템을 구축한다.

그리고 실행코드의 분석을 위하여 악성코드의 블랙리스트 및 실행코드의 화이트리스트 정보를 수집하여 데이터베이스화해야 하며, 사이버 침해 정보 수집을 확대하고 관리해야 한다. 이를 위해 다음과 같은 사항을 추진해야 한다.

- 양질의 풍부한 사이버 위협 정보 수집을 위한 국내외 수집채널을 확대한다.

- 정부, 산업계, 학계, 연구소 등에서 화이트리스트 실행 코드, 악성코드 및 사이버 침해 관련 정보 수집 채널 및 체계를 확립한다.

- NIST, US-Cert 등 국외 침해사고 대응기관 및 연구기관에서 탐지·분석한 정보 수집 채널 및 체계를 확립한다.

- 모든 사이버 위협 관련 정보를 보안지식베이스 전담 조직으로 수집하고 수집된 정보는 분석, 검증, 지식정보화 과정을 거쳐 실시간으로 보안지식베이스를 갱신하고, 유관기관과의 연계 체제를 통한 보안 관련 데이터베이스를 확대하여 민, 관, 군 등에서 위기 대응을 위하여 활용될 수 있도록 한다.

또한 실시간 트래픽 검사를 통해 갱신된 입체적인 보안지식베이스를 활용하여 국가 차원의 실시간 위협 관리를 수행하고 신규 위협 탐지를 분석하며, 그 사항을 검증해야 한다. 이를 위해 다음과 같은 사항을 추진한다.

- 알려지지 않은 신규 위협 탐지 및 분석과 취약점이 존재하는 실행코드의 실시간 분포 정도, 실시간 좀비 현황 정도 등의 입체적인 정보를 활용할 수 있으며, 관련 정보를 유관기관과 공유하여 위협에 대응·조치하도록 유도한다.

3. 보안지식베이스 업무 전담조직 신설

국가 차원에서 실시간 데이터 수집 및 유관기관을 통한 사이버 침해 정보를 수집·분석 및 지식 베이스화하고 이를 기반으로 국가 적인 위기 대응 업무를 수행하기 위하여 국가 보안지식베이스 전담 조직 신설이 필요하게 된다. 이 전담조직에서는 다음과 같은 업무를 수행하게 된다.

- 실시간 사이버 위협 분석을 통한 유사 침해사고 재발 방지 및 신규 사이버 위협 정보를 탐지·분석하여 사전 예방 능력을 강화한다.
- 국내·외 유관 기관 간의 사이버 위협 정보 협력을 통한 신속한 위기 대응 업무를 추진 및 수행한다.

국가 보안지식베이스 전담 조직은 다음과 같은 팀으로 구성될 수 있다.

- 실시간 데이터 수집 및 분석 팀 : 실시간 데이터 수집 등 위협 정보 수집 및 분석한다.

- 보안지식베이스 통합관리팀 : 보안지식베이스 갱신, 유지 관리 및 서비스 제공 등 보안지식베이스 시스템 운영

- 국내외 총괄협력팀 : 국내·외 유관기관 및 산·학·연 등 타 기관과의 협력체계 구축 및 위기 대응 업무 수행

국가 보안지식베이스 전담조직에서는 정부 부처별로 산재하여 수집되고 공유되는 사이버 위협 정보의 신속한 통합 수집을 위하여 유기적인 공조체계를 구축하고, 수집된 정보의 분석·검증 및 지식베이스화를 통하여 통합 관리를 수행 할 수 있는 프레임워크를 구축하도록 한다.

4. 위협 대응체계 구축 및 인력양성

국가·공공, 민간, 국방 분야 정보보호 기관 및 산업체, 학계, 연구소등과 유기적인 공조 채널을 구축하여 사이버 위협 관련 이벤트 데이터를 수집하고 국가 보안지식베이스를 갱신한 이를 기반으로 국가 차원의 실시간 사이버 위협 대응체계를 완성한다. 이를 위하여 다음과 같은 사항을 수행한다.

- 사이버 위협 정보 수집 및 공조채널을 다변화하여 침해사고와 연계된 위협 정보를 보안지식베이스화하여 신속 정확하게 입체적으로 관리한다.

- 사이버 위협 대응 관련 정책을 제정 및 활성화 하여 국가 위기관리 체계를 강화하고 공조체계를 활성화한다.

- 해외 유관기관 및 산업계와의 협력 채널을 확보하고 공조 체계를 구성하여 국가 위기 상황에 대한 실시간 사이버 위협 대응 프로세스 구축

그리고 사이버 위협대응 정책, 기술, 표준화 연구를 위한 산업계, 학계, 연구소, 정부기관, 군 등으로 구성된 협의체를 구성 및 운영한다. 이 협의체를 통하여 국가 사이버 위협대응을 위한 보안지식베이스 전담 조직의 중요 정보 및 사이버 위협의 위험도에 따른 대응방안 및 연계된 종합 대책을 함께 협의할 수 있는 기회를 제공한다.

또한 고도화된 사이버 위협에 대처하고 보안지식베이스 전담 조직을 운영하기 위하여 보안 지식을 갖춘 고급 인력을 양성해야 한다. 산업계, 학계, 정부기관, 군의 보안 교육을 위한 활동을 지원하고 모의 해킹 등 실무를 통하여 위협에 대응 능력을 갖춘 실무 인력을 양성하고 사이버 위협 데이터 탐지 분석 및 보안지식 화 등 특화된 연구 활동 지원을 통하여 고급 인력을 양성 한다 또한 화이트해커의 양성화 활동 및 양성을 위하여 다음과 같은 내용을 수행한다.

- 해킹방어대회, 사이버공격 시나리오 공모전과 같은 활동을 통하여 국내 화이트 해커의 양성화 활동을 활성화하고, 학계 및 민간 부분 연구 지원을 통하여 화이트해커의 연구 참여를 지원한다.

- 화이트 해커들과의 교류를 활성화하고, 화이트 해커들과의 연합 모임을 구성하여 다양한 보안 정보 수집 및 전문가로써 활동할 수 있는 기회를 제공한다.

5. 법제도 개선

사이버 위협 대응을 위한 보안지식베이스 전담 조직 신설을 위하여 법 제정이 필요하며, 이를 위하여 다음과 같은 내용을 수행한다.

- 보안지식베이스 전담 조직 신설을 위한 법률 제정 및 침해사고 위기 대응 체계 통합 구축·운영을 위한 법률을 개정한다.

- 신설 조직의 법률적 근거를 위해 조직의 구성 및 운영에 관련된 '국가 보안지식베이스 센터 규정' (가칭) 또는 법률을 제정한다.

그리고 국가 차원의 실시간 데이터 수집 체계와 사이버 위협 대응체계 구축을 위한 제도 마련 및 법률 제·개정을 위하여 다음 내용을 수행한다.

- 고도화된 사이버 위협에 대응하기 위하여 실시간 데이터 수집과 관련된 정책을 마련한다.

- 공조 체계에 있는 유관기관에서 사이버 위협관련 정보 확보 시 즉각적인 신고 의무화 정책을 마련한다.

- 국가 차원의 사이버 위협대응 프로세스 이행 의무화 및 이해관계자별 역할을 규정한다.

- 사이버 안전 관리 규정 및 정보통신기반 보호법 등 위기 대응 관련 기존 법제 통합을 개정한다.

또한 사이버 위협 대응방안을 위한 인식제고 프로그램을 수행하여 사이버 위협에 대한 인식을 높이고 이를 기반으로 사이버 위협 관련 데이터의 수집과 위기 대응 조치를 수행하도록 한다. 이를 위해 다음 사항을 수행한다.

- 사이버 위협 대상별, 수준별 대응방안에 대한 교육·훈련을 추진한다.

- 위협 대응체계 구축을 통한 사이버 위협 대응 및 예방 사례에 대한 교육 및 대국민 홍보 활동을 수행한다.

- 대국민을 대상으로 사고정보 및 위협정보의 등록을 유도한다.

5.3 추진방안

상기 추진 체계를 실행하기 위한 추진방안은 다음과 같다.

1. 국가보안지식베이스 구축 프로세스 수립방안

범부처 및 산업체, 학계, 연구소 전문가들로 구성된 전담반을 구성하여 국가보안지식베이스 구축 프로세스를 수립한다. 구축 프로세스 내용은 다음과 같다.

- 산·학·연·민·관·군 등 범 부처를 포괄하는 국가 보안지식베이스 구축 프로세스 수립

- 실시간 데이터 수집을 위한 데이터 수집 프로세스 개발

- 타 기관에서 수집된 정보의 검증을 위한 검증 프로세스 개발

- 화이트리스트 및 블랙리스트 수집과 리스트 데이터베이스 갱신 프로세스 개발

- 실시간 실행코드 분석을 위한 빅 데이터 분석 프로세스 개발

- 실시간 보안지식베이스 갱신 프로세스 개발

2. 사이버 위협대응 협의체 및 국가 보안지식베이스 시스템 구축

국가 보안지식베이스 구축 및 사이버 위협대응 정책, 기술, 표준화 연구를 위한 산업계, 학계, 연구소, 정부기관, 군 등으로 구성된 협의체를 구성 및 운영한다. 그리고 국가 차원의 대규모 데이터의 실시간 수집, 수집된 빅 데이터의 실시간 분석, 분석된 정보의 지식 베이스 화, 보안 지식의 활용방법 등 고도화된 사이버 위협에 대응하기 위한 신기술 연구를 추진한다. 또한 고도화된 사이버 위협에 대응하기 위한 국가 차원의 사이버 위협 정보를 실시간으로 수집. 분석, 지식 베이스 화하는 독립적인 국가 보안지식베이스 시스템을 구축하고, 구축된 보안 지식을 사용하여 사이버 위협 정보의 위험도, 시급한 정도 등에 따라 위협 대응을 수행하는 사이버 위협 대응체계를 수립한다.

APT와 같이 고도화된 사이버공격에 대응하기 위한 지식 베이스를 구축하기 위해서 먼저 실시간 데이터 패킷의 전수 검사를 통하여 필요한 이벤트들을 수집할 수 있어야 하며, 수집된 정보를 사용하여 실행코드관련 정보 검색 및 실행코드 추출이 필요하며, 실행코드를 악성코드 데이터베이스와 화이트리스트 데이터베이스와의 비교 분석을 통하여 알려진 악성코드는 추적을 수행하고, 알려지지 않은 실행코드는 연관성 분석을 통하여 악성코드 분석을 수행하고, 악성코드일 경우 지식 베이스 화하여 실행코드 전달 이력 추적을 위한 보안 맵을 갱신한다. 다음 그림 34는 국가 보안지식베이스 생성 과정을 나타낸다. 이 과정을 통하여 생성된 실행코드 전달 이력 보안 맵은 고도화된 공격에 대하여 대응전략 수립 및 조기 공격 대응방안 확립이 가능하게 된다. 또한 국가보안지식베이스를 사용하여 다음과 같은 서비스가 가능하리라 기대된다.

- Inbound/Outbound 트래픽 상세 모니터링 분석 체계 확보
- 고급화된 또는 숨겨진 위협 탐지 / 대응방안 제시
- 위협이 되는 사이트 접근 행위 탐지 및 통제
- 공격의 Lifecycle을 제공
- 악성코드 유입 경로 분석
- 감염된 시스템 트래픽 분석

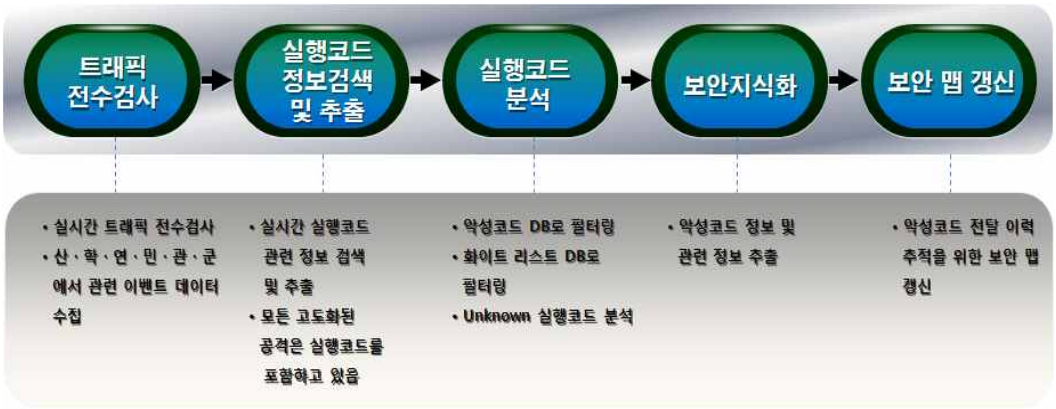

그림 34. 국가 보안지식베이스 생성 과정

3. 국가보안지식베이스 전담조직 운영 방안

고도화된 사이버 위협으로 인한 위기 상황이 발생하는 경우에 신속하게 국가적인 차원에서 대응하기 위하여 일관성 있는 정책 수립 및 운영이 필요하며 이를 위해 정부 주도의 독립적인 전담 조직으로 운영하고 기존의 위기관리체제와 연계하여 수행한다. 국가보안지식베이스 전담조직은 다음과 같이 세 개의 팀으로 구성하여 운영한다.

- 실시간 데이터 수집 및 분석 팀 : 실시간 데이터 수집 등 위협 정보를 수집 및 분석한다.

- 보안지식베이스 통합관리팀 : 보안지식베이스 갱신, 유지 관리 및 서비스 제공 등 보안지식베이스 시스템을 운영한다.

- 국내외 총괄협력팀 : 국내·외 유관기관 및 산·학·연 등 타 기관과의 협력체계 구축 및 위기 대응 업무를 수행한다.

국가보안지식베이스 전담조직은 현재의 국가 위기 대응체제와 유기적으로 연관된 독립적인 조직으로 구성되며, 산·학·연 단체와 민·관·군 사이버 위협대응체제와 연계하여 정책 및 종합대책을 수립하여 운영한다. 국가보안지식베이스 전담조직의 운영 예는 다음과 같다.

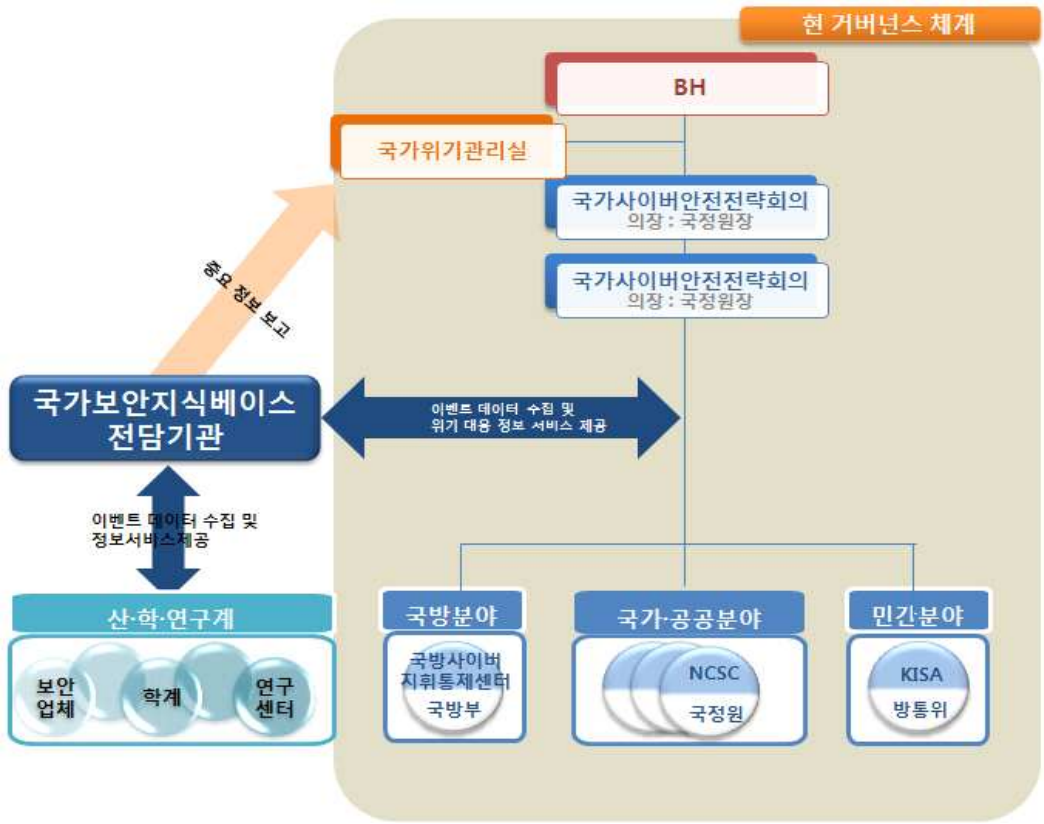

그림 35. 국가 보안지식베이스 전담조직의 운영 예

실행코드 전달 이력 보안 맵을 작성하기 위하여 실행코드 실시간 추적기술과 분석기술이 필요하다. 또한 기존에 알려진 악성코드와 관련된 데이터베이스가 필요하며, 이것을 실시간으로 검색할 수 있는 기술이 필요하다. APT등과 같이 고도화된 공격도 실제 공격 진행 과정 중에 반드시 네트워크를 통한 실행코드 전달이 포함되어 있으며, 실행코드 전달시 기 구축된 국가 지식 보안 지식베이스인 실행코드 전달 이력 보안 맵을 이용하여 실시간 추적 및 분석이 가능하게 된다. 그리고 민간과 공공 기관 및 군을 포함한 국가 차원의 체계적인 이벤트 수집 및 보안지식베이스의 구축 및 관리, 서비스를 제공하기 위하여 일원화된 조직이 구축되어야 한다.

안전하고 신뢰할 수 있는 스마트 복지사회 구현을 위해 국가 사이버 안전관리 체계 강화수단으로써 국가 보안지식베이스 구축이 필요하다. 국가 보안지

식베이스 구축을 통하여 다음 그림과 같이 미래의 위협에 대비한 국가 위기 상황 사전인지 및 효율적 대응전략 적용이 가능하리라 기대된다.

그림 36. 국가 보안지식베이스 기대 효과

6. 결 론

본 연구에서는 인터넷을 통한 물리 및 논리공간의 융합과 스마트 디바이스에 의한 이동성이 극대화되는 환경변화 상황에서의 APT 사이버 위협 및 공격단계를 분석하고, 각 단계별로 국내외 기업들의 대응방안을 분석하였다. 또한 국내외 사이버공격 대응 기술 현황 및 사이버공격 대응체계 현황을 조사 분석하였다. 그리고 이를 기반으로 새로운 유형의 고도화된 사이버 위협에 능동적으로 대응하기 위한 기반으로써 국가 보안지식베이스 구축 전략을 수립 하였다. 본 연구의 결과를 활용하여 APT등 고도화된 사이버 위협에 국가 차원의 효과적인 위기 대응이 가능 하리라 사료된다.

7. 참 고 문 헌

[1] http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=2&seq=16854

[2] http://yjlee.delighit.net/i/entry/75

[3] http://blog.daum.net/saschajin/12603

[4] 남기효, 김윤홍, 권환우, “최신 정보보호기술 동향: APT 및 그 대응”, 정보통신산업진흥원, 2011.9

[5] http://www.isssource.com/wp-content/uploads/2012/04/040412C5_APT_ADecadeInReview.pdf

[6] http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?curPage=1&menu_dist=2&seq=18487&dir_group_dist=0

[7] http://docs.media.bitpipe.com/io_10x/io_105022/item_550605/Lifecycle_of_the_Advanced_Persistent_Threat%5B1%5D.pdf

[8] http://www.웹센스.com/assets/white-papers/whitepaper-웹센스-advanced-persistent-threats-and-other-advanced-attacks-en.pdf

[9] http://www.trendmicro.com/us/enterprise/challenges/advance-targeted-attacks/index.html#understand-an-attack

[10] http://www.trendmicro.com/cloud-content/us/pdfs/business/datasheets/ds_deep-discovery.pdf

[11] 김형욱, “0-Day 공격 방어를 위한 IBM의 다계층 선제 대응방안”, IBM Security Summit, 2011.

[12] http://www.it-win.co.kr/EMC_RSA_NetWitness.pdf

[13] http://www.zdnet.co.kr/news/news_view.asp?artice_id=20120918220326&type=det

[14] http://image.itstv.net/upload_files/infocenter/file32599-137302.pdf

[15] http://www.eurosouthkorea-ict.org/documents/forum2_ppt/mijoo_kim.pdf

[16] “2010 해킹바이러스 현황 및 대응”, KISA 최종연구보고서, KISA-RP-2010-0051

[17] http://epc.neograph.co.kr/kor/info/kor_info_dic_list.html?sval=&mode=h8&page=3#

[18] http://blog.daum.net/damulkan/7563870

[19] http://blog.hitoos.com/radiohankook/44961

[20] 이창범, 강이석, “인터넷 법제 동향 제 22호”, 한국인터넷진흥원, 인터넷 법제 동향 제2009-07호
[21] http://netsquare.kisa.or.kr/report/securityTrend/[6월 3주] “미국, 사이버보안 강화 위한 ‘플랜 X’ 전략 추진” 2012-06-21
[22] 김일수, 강석구, 윤회상 외 5명, “사이버 안전체계 구축에 관한 연구”, 한국 형사 정책 연구원, 2010