정 보 보 호 학 회 지
제24권 제1호, 2014. 2

미국 정부의 사이버 공격에 대한 보안 전략

이 동 범*, 곽 진**

요 약

정보기술이 발전함에 따라 편리성이 향상되고 있지만, 사이버 공간에서의 보안 위협은 증가하고 있다. 최근에는 국가 기반시설과 같은 주요 인프라와 기관 및 기업을 목표로 하여 사이버 공격을 시도하고 있고, 해당 공격 방법도 지능적으로 발전하고 있다. 따라서 사이버 공간의 보안 위협에 대응하기 위해 국가적 차원에서 전략을 마련하고 있다. 특히 사이버 보안과 관련하여 미국은 사이버 공격에 대응하기 위해 각 기관의 연계성 및 협력을 위한 전략을 타 국가보다 앞서 준비하고 실행을 하고 있다. 따라서 본 고에서는, 국내 사이버 공격에 대한 보안 전략 수립을 위해 최근 사이버 공격이 이루어지는 유형과 사례를 분석하고, 이에 대처하는 미국 각 기관의 전략과 역할에 대해 분석한다.

Ⅰ. 서 론

최근, 인터넷 서비스와 같은 정보 통신 기술의 발전으로 인해 다양한 정보를 쉽고 빠르게 접할 수 있게 되면서 실생활에서 많은 도움을 받고 있다. 그러나 정보화 사회의 실현은 순기능뿐만 아니라 사이버 공격으로 인한 사이버 공간에서의 보안 위협과 같은 역기능도 나타나게 되었다. 사이버 공격은 공격 근원지를 식별하고 추적하는 것이 어려우며 인터넷과 같은 네트워크를 통해서 악성코드들을 쉽게 전파시킬 수 있는 특징을 갖고 있다. 이러한 사이버 공격은 최초에는 개인과 기업을 대상으로 악성코드 유포 및 감염을 통한 개인정보 유출과 온라인 상업 거래의 핵심인 전자 상거래에 대한 위협, 디지털 저작권 침해행위 등을 일으켰으며, 현재에는 제로데이 공격과 APT(Advanced Persistent Treat) 공격과 같이 지속적으로 피해를 주고 탐지 및 차단이 어렵게 지능화된 형태의 사이버 공격으로 발전하고 있다. 더 나아가 사이버 공간에는 국가별 국경선이 명확하지 않다는 특징을 이용하여 공격 대상을 개인과 기업에서 국가범위로 확장해 나가고 있으며 이 때문에 전 세계적으로 사이버 보안 위협이 증가하고 있다. 이로 인해 개인과 기업뿐만 아니라 국가 차원의 사이버 보안 정책과 전략 등에 대한 관심이 높아지고 있다.

따라서 본 고에서는 이러한 상황을 고려하여 최근의 사이버 공격 상황, 공격 기법 및 미국 연방 정부의 사이버 공격에 대처하기 위한 각 기관의 전략과 역할에 대해서 분석하고자 한다.

Ⅱ. 사이버 공격

최근 주요 인프라, 정부기관, 민간기업을 불문하고 외부로부터의 해킹이나 공격에 의한 개인 정보 유출이 증가하고 있다. Verizon社가 발표한 2012년 Data Breach Investigations Report에 따르면 2012년에 발생한 미국의 데이터 유출 사건은 855건, 유출 데이터 레코드는 총 1.7억 개에 이르고 그중 81%가 외부 해킹에 의한 것이라고 발표 하였다[1].

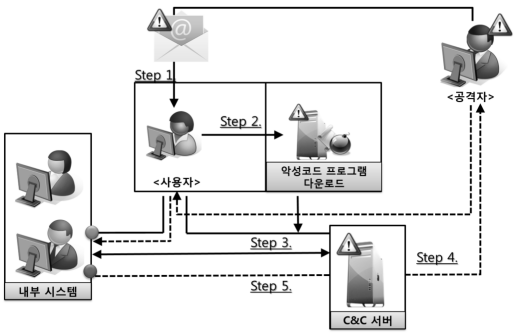
따라서 본 장에서는 주요 사이버 공격을 포함하여 APT 공격에 해당하는 대표적인 공격 방식을 분석한다. 최근 공격 방식을 살펴보면 사회 공학 및 일반적인 공격 방법에서 특화형 공격까지 다양한 공격 방법이 이용되고 있으며, APT 공격이 진화하고 있는 모습을 보이고 있다[2-3].

다음은 사이버 공격에서 주로 이용되는 APT 공격 방식이다.

* 순천향대학교 정보보호학과 정보보호응용및보증연구실 박사과정 (dblee@sch.ac.kr)
** (교신저자) 순천향대학교 정보보호학과 교수 (jkwak@sch.ac.kr)

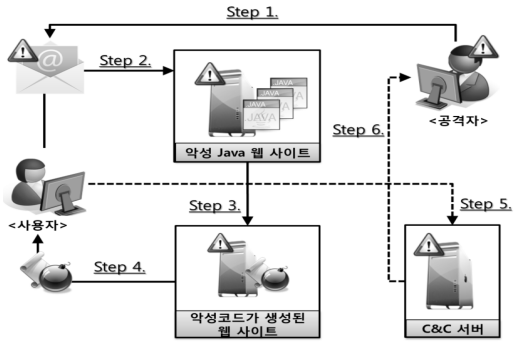
2.1 Operation Shady RAT

2006년부터 발견된 공격으로 정부기관, 언론 기관 등을 대상으로 기밀 정보를 획득하기 위해 무단 접속을 시도하는 공격이다[4].



〔그림 1〕 Operation Shady RAT 공격 방식

① 컴퓨터의 취약성을 이용한 악성코드가 포함된 피싱 메일이 대상 조직의 내부 시스템에 접근 권한을 가진 인원에게 전송
② 악성코드가 실행되면 악성 프로그램이 다운로드
③ 악성 프로그램이 실행되면 C&C(Command & Control) 서버로부터 공격 명령을 전송 받을 공격 경로를 확보하기 위해 백도어를 설치
④ 공격자가 악성 프로그램이 실행 중인 컴퓨터에 무단 침입
⑤ 감염된 컴퓨터를 이용하여 내부 시스템에 대한 접근 권한을 높이거나 다른 컴퓨터에 악성코드를 감염시켜 기밀 정보에 무단으로 접근 시도



〔그림 2〕 Operation Aurora 공격 방식

2.2 Operation Aurora

인터넷 익스플로러의 보안 취약점을 이용하여 특정 대기업의 내부 네트워크에 악성코드를 침투시켜 기밀 정보에 대한 무단 접속을 시도하는 공격이다. 피해 기업은 Google을 포함하여 30여 개에 이루고 있다[5-6].

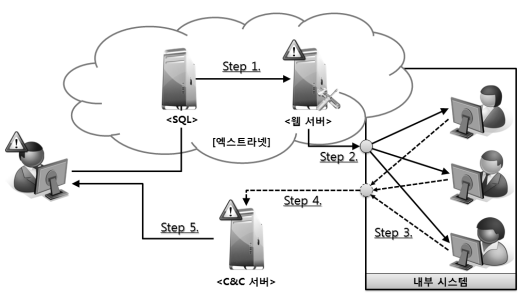
① 목표대상에 신뢰할 수 있는 대상으로 가장하여 전자 메일이나 인스턴트 메시지에 링크를 전송
② 목표 대상이 링크를 클릭하면 악성 JAVA 스크립트가 포함된 웹 사이트로 이동
③ 대상 브라우저에서 악의적인 JAVA 스크립트가 인터넷 익스플로러의 보안 취약점을 이용하여 실행
④ JAVA 스크립트가 웹 서버에서 이미지 파일로 위장한 악성코드를 다운로드
⑤ 악성코드를 실행하면 침입을 위한 백도어가 설치되고, C&C 서버와의 연결을 설정
⑥ C&C 서버를 통해 공격자가 내부 시스템에 침입하고, 내부 시스템의 소프트웨어 구성 등에 대한 정보에 무단으로 접근하여 침입 피해가 확대

2.3 Night Dragon

글로벌 규모의 석유 회사, 전력 회사, 제약 회사가 대상이 되어, 각 기업의 내부 네트워크에 악성코드가 전송되어 기밀 정보에 대한 무단 접속을 시도하는 공격이다[7-8].

Operation Aurora와 비슷한 수법이 사용되었으며 공격 방식은 다음과 같다.

① 엑스트라넷에 위치한 웹 서버를 SQL 인젝션 등을 이용하여 악성코드로 감염시키고, 원격 접근툴



〔그림 3〕 Night Dragon 공격 방식

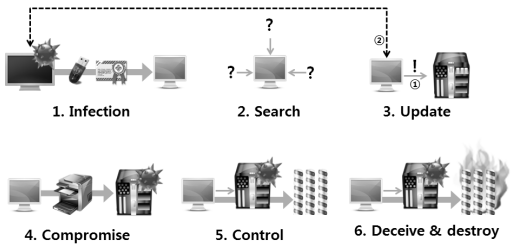
(RAT : Remote Access Tool)을 설치
② 악성코드에 감염된 서버를 거점으로 내부 시스템에 무단 접근
③ 모바일이나 VPN 등 내부 시스템에 접근하는 직원으로 표적을 좁혀 피싱을 통해 내부 시스템에 접근
④ 또한 다양한 공격툴을 이용하여 다른 내부 시스템에 접속하여 악성코드의 감염 대상 및 RAT 설치 대상을 수집
⑤ 조직 간부의 이메일과 파일에 접근하여 기밀 정보 등에 무단 접근

2.4 Stuxnet

미국 정부가 이란의 핵 관련 시설의 제어 시스템에 타격을 목적으로 한 사이버 공격이다. 미국 정부가 이스라엘 정부와 공동으로 Windows OS의 취약점을 이용하여「Stuxnet」이라는 악성코드를 개발하고, 이를 이란의 핵 개발 시설의 컴퓨터 시스템에 감염시킨 것이다[9].

Stuxnet의 공격 방식은 다음과 같다.

① USB 메모리 등을 통해 컴퓨터 시스템에 Stuxnet을 감염시켜 시스템의 모든 Windows 컴퓨터에 Stuxnet이 작동하도록 함
② Stuxnet은 감염 대상의 컴퓨터가 공격 대상인 Siemens社의 제어 시스템인지 여부를 확인
③ 공격 대상이 아닌 경우는 방치하고, 대상인 경우에는 인터넷을 통해 악성코드의 최신 업데이트를 다운로드
④ Windows의 보안 취약점을 이용하여 해당하는 제어 시스템에 침투
⑤ 제어 시스템의 가동을 확인한 후, 그 정보를 이용하여 작동에 악영향을 줌
⑥ 대상으로 한 제어 시스템이 다른 시스템과 오작동하도록 조작함으로써 시스템 가동을 타격



〔그림 4〕 Stuxnet 기법
(출처: IEEE Spectrum Magazine)

〔표 1〕 대표적인 APT 공격 방식

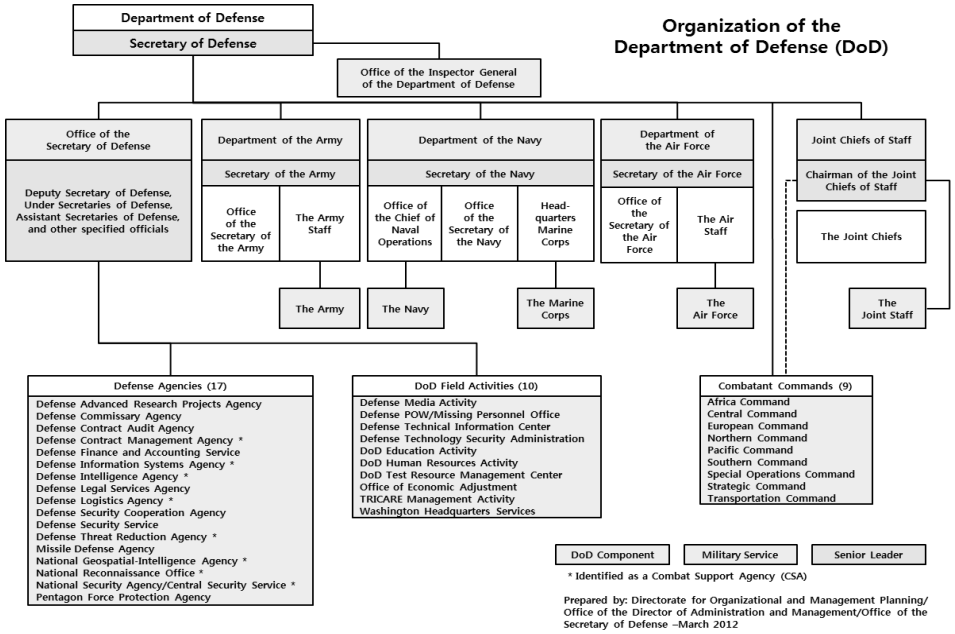
공격 유형	방법	목적
Operation Shady RAT	· 악성코드 이용 · 백도어를 통한 침입	· 기밀 정보 획득
Operation Aurora	· 악성 JAVA 스크립트 및 악성코드 이용 · 백도어를 통한 침입	· 기밀 정보 획득
Night Dragon	· SQL 인젝션 및 악성코드 이용 · 원격 접근 툴로 침입	· 기밀 정보 획득
Stuxnet	· 악성코드 이용 · OS 보안 취약점을 통한 침입	· 기반 시설 공격

Ⅲ. 사이버 공격 동향

본 장에서는 최근에 주요 정부기관, 민간 기업을 대상으로 발생한 사이버 공격 동향에 대해서 분석한다. 대규모 공격과 특정 조직을 겨냥한 APT 공격이 많이 발생하고 있고 Operation Shady RAT, Operation Aurora, Night Dragon 등과 같이 집중적이고 정교한 공격이 발생하고 있다[4],[7],[10-23].

〔표 2〕 최근의 사이버 공격 동향

구분	대상	내용
2006년	국외	2011년 8월, 보안 소프트웨어 업체 McAfee社가 지난 5년 동안 “Operation Shady RAT”이라는 공격이 국외의 다양한 조직을 대상으로 시행되었다고 발표. 이 공격은 대상 조직의 네트워크에 침입하여 기밀 정보에 무단으로 접근하며, UN과 71개국의 조직이 공격을 받음
2008년	DOD	2010년, 미국 국방부(DOD : Department of Defense)는 펜타곤의 군사 기밀 정보를 취급하는 네트워크가 무단 접근 받은 것을 공표. 중동에서 노트북 PC에 바이러스가 감염된 USB 드라이브를 연결한 것이 요인
2009년	미국·한국의 정부 기관, 언론, 기업	웹 사이트용 서버에 침입하여 트래픽을 오버플로 시켜 실질적으로 사이트를 다운시키는 DDoS 공격 발생
2009년	미국 대기업	주요 브라우저 「인터넷 익스플로러」의 보안 취약성을 이용하여 「Operation Aurora」라는 악성코드를 이용하여 기업의 네트워크에 침입하는 공격이 빈발. 공격을 받은 기업은 Google, Adobe, RSA, Lockheed Martin 등 30여 개
2009년	석유, 전력, 제약 회사	글로벌 규모의 석유 회사, 전력 회사, 제약 회사를 대상으로 기밀 정보에 대한 무단 접근을 하는 「Night Dragon」이라는 악성코드를 이용하여 공격
2011년	대형 금융 기관	웹 사이트의 기능을 상실시키는 DoS(Denial of Service) 공격이 빈발. 이란에서 공격이 시작되어 Bank of America, JPMORGAN CHASE & CO, Citi Group 등이 피해를 봄
2012년	AT&T	운영하는 2개의 DNS 서버에 DDoS 공격이 시도된 것을 발표. 기업 사용자를 위한 관리 서비스 및 DNS 관련 서비스가 영향을 받아 많은 기업 사용자가 일시적으로 서비스를 이용할 수 없게 되는 사태가 발생
2012년	전력 회사의 발전 시설	2013년 1월, 국토안보부(DHS : Department of Homeland Security) 산하의 ICS-CERT(Industrial Control Systems Cyber Emergency Response Team)가 전력 회사의 발전 시설에서 악성코드에 의한 감염 사고가 2건 발생했음을 신고. 감염원은 제어 시스템의 설정을 미리 저장하기 위해 사용된 USB이며, 이에 따라 에너지 산업의 제어 시스템을 노린 사이버 공격의 위험이 부상
2013년	New York Times	2013년 1월, 지난 4개월 동안 중국 해커에 의해 컴퓨터 시스템에 무단 침입의 피해를 본 것을 발표. 2012년 10월에 당시 원자바오 총리의 일족이 27억 달러 이상을 부정 축재를 하고 있다고 보도한 것을 계기로 중국이 출처를 찾는 목적으로 공격을 가했다고 여겨지고 있음. 실제로 기자의 패스워드 등이 무단으로 취득됨
2013년	Wall Street Journal	Dow Jones&Co社가 중국 해커에 의해 지속적인 공격을 받고 있다고 발표. 중국에 불리한 기사를 집필한 기자에 대한 중국 내 정보원을 찾는 것이 목적이었던 것으로 알려졌음. 2월에는 모회사 News Corp의 CEO Rupert Murdoch가 해킹 공격이 지속되고 있다고 발표
2013년	Twitter	악성코드의 감염을 통해 사용자 25만 명의 이메일 주소, 사용자 이름, 암호화가 완료된 패스워드에 무단 접근이 있었음을 발표
2013년	Facebook	해커에 의한 사이버 공격에 있었음을 발표. 직원이 사용하는 개발자 사이트에 방문하면 악성코드에 감염됨
2013년	Apple	Twitter, Facebook에 대한 공격과 같은 것으로 보이는 공격원에서 사이버 공격을 받았다고 발표. Facebook의 경우와 같이 직원의 개발자용 사이트에 접속 했을 때 컴퓨터가 같은 악성코드에 감염됨
2013년	DOE	미국 에너지국(DOE : Department of Energy) 본부의 서버 14대, 워크스테이션 20대에 무단 접근을 시도하여 직원 수백 명의 개인 정보가 유출됨. 또한, 산하기관에 국가핵안보실(NNSA : National Nuclear Security Administration)이 있기 때문에 핵 관련 기밀 정보를 무단으로 사용할 목적으로 표적이 되고 있다고 판단
2013년	Federal Reserve Bank (연방 준비 은행)	긴급통신시스템(ECS : Emergency Communications System)이 침해당한 로그가 확인됐다고 발표. 공격 당시 시중 은행들의 감독당국과 담당자들의 비상연락망 등이 저장된 곳에 무단 접근했던 로그를 확인. 이 공격은 유명 해킹그룹인 「어나니머스(Anonymous)」의 소행인 것으로 전해졌고, 어나니머스와 연관된 트위터 계정인 “작전명 최후의 수단(Operation Last Resort)”을 통해 은행원 4,000여 명의 이름과 직책, e-메일 주소 등의 신상 정보가 유출



〔그림 5〕 DOD 조직 구성도

Ⅳ. 사이버 보안을 위한 미국 정부의 노력

위와 같이 지능적인 사이버 공격이 많이 발생하고 있는 가운데, 각 조직에는 이러한 사이버 공격에 대한 대책이나 방어 체제 구축이 요구되고 있다.

따라서 본 장에서는 미국 정부 기관이 사이버 보안 확보를 위해 설립한 주요 기관의 역할과 대응 방안에 대해서 분석한다.

4.1 미국 국방부(DOD)

DOD는 국가 방위 및 안전 보장이라는 관점에서 연방 기관 및 군대의 사이버 공간에서 보안을 강화하기 위해서 설립된 기관으로 2010년 5월에 사이버 공간에서 작전 능력의 강화를 목적으로 사이버 사령부(US Cyber Command)를 개설하였다[24].

사이버 사령부는 육군, 해군, 공군, 해병대 등 군 조직이 개별적으로 운영하며, 사이버 부대를 통합하고 미군의 IT 인프라에 대한 사이버 공격에 포괄적으로 대응하기 위해 개설되었다. 미군과 국방부의 IT 인프라와 사이버 공간 운영의 안전을 지키는 것뿐만 아니라 사이버 공간의 보안 강화를 통해 미국 시민의 권리와 프라이버시 보호 등 다양한 분야에서 다른 부처와 민간과의 연계 등도 적극적으로 추진하고 있다.

또한, DOD는 사이버 사령부를 통해 구체적인 사이버 보안 작업을 수행하는 것 외에 2011년 7월에 국방부 사이버 공간 전략(Department of Defense Strategy for Operating in Cyberspace)을 발표하였다[25].

이 전략은 사이버 공격 및 범죄가 급증함에 따라 기존의 군사 전략 수행범위에 육해공 사이버 공간을 추가하는 등의 전략 계획을 보여준 것이며 DOD로서 첫 사이버 보안에 대한 전략 문서이다.

구체적인 전략은 다음과 같이 5개의 개념으로 명시되어 있다.

- □ DOD의 국가 안보를 향한 대처 영역으로 공공 및 민간에 상관없이 사이버 공간 전체를 포함
- □ DOD의 IT 인프라를 보호하기 위한 새로운 전략 수립
- □ 국가 전체의 사이버 보안 전략 개발을 위해 다른 정부 기관이나 민간과 연계
- □ 연계된 사이버 보안을 실현하기 위해 동맹국 및 국제 파트너와의 협업 강화를 도모
- □ 사이버 인재를 양성하여 급속한 사이버 기술의 혁신에 대응

2013년 1월에 사이버 사령부는 DOD를 포함하여 미국의 주요 시스템의 방어뿐만 아니라 국외에서의 사이버 공격에 대한 대응 능력의 향상을 위해 인원을 900명에서 4,900명으로 증강한다는 계획을 밝혔었다[26].

인원 증강 후에는 조직 체제를 다음과 같은 3개의 부대로 편성하여 방어뿐만 아니라 공격까지 고려한 조직으로 변화하고 있다.

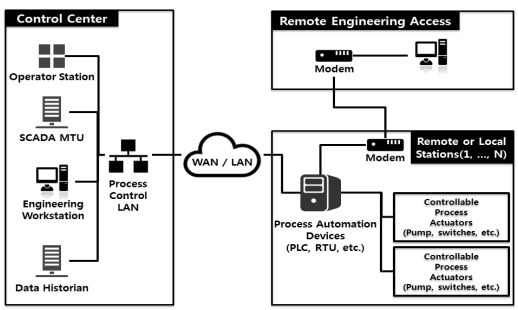
- □ 발전소와 송전망 등 주요 국가 인프라를 방어하는 부대
- □ 해외에서의 군사 작전을 지원하는 부대
- □ 국방부 인프라 방어에 특화된 부대

이 외에도 DOD는 DC3(Department of Defense Cyber Crime Center)라는 조직을 운영하고 있다. DC3는 DOD의 사이버 보안 활동을 지원하는 목적하에 사이버 공간에서 부정행위나 범죄에 대한 증거의 처리, 분석, 검사 및 복원 등에 관한 표준과 기준을 수립하는 조직이다[27].

4.2 국가안보국(NSA)

NSA(National Security Agency)는 DOD에 있는 정보 활동 조직으로서 국방 정보 및 기밀 정보의 유기적인 연계를 중요한 책무로 수행하며, 국방과 관련하여 사이버 공간에서 정보 수집 및 분석과 보안 등을 중심으로 활동한다[28].

DOD 산하에 있지만, DOD의 활동 지원뿐만 아니라 다른 정부 기관, 민간 기업, 동맹국 등의 지원도 수행하며, 국방 정보 및 기밀 정보의 유기적인 연계를 목표로 진행하고 있다.



〔그림 6〕 Perfect Citizen 인프라 구조

정보 활동 조직이기 때문에 구체적인 활동의 전체 범위는 밝혀지고 있지 않지만, 미국 내 주요 인프라의 취약성을 보호하기 위해 「Perfect Citizen」이라는 목표를 추진하고 있다[29]. 이는 전력망 제어 시스템, 가스 제어 시스템 등과 같은 국가 주요 인프라를 대상으로 시스템의 취약점을 분석하는 중요한 테스트를 실시한다.

또한, NSA는 사이버 공격이 증가함에 따라 사이버 보안을 선도하는 능력을 갖춘 인재 양성 및 확보에 주력하고 있다.

NSA의 사이버 보안 인력 양성을 위한 활동은 다음과 같다[30].

- □ 사이버 보안 인재 양성 및 확보를 목표로 하는 프로그램인 NICE(National Initiative for Cybersecurity Education)을 지원하려는 방법으로 「National Centers of Academic Excellence(CAE) in Cyber Operations」라는 인재 육성 프로그램 개설
- □ 카네기멜론대학과 협력하여 사이버 보안 인재를 육성하기 위해 초등학교 6학년부터 고등학교 3학년을 대상으로 하는 해킹 및 방어를 하는 콘테스트 「Toaster Wars」를 개최

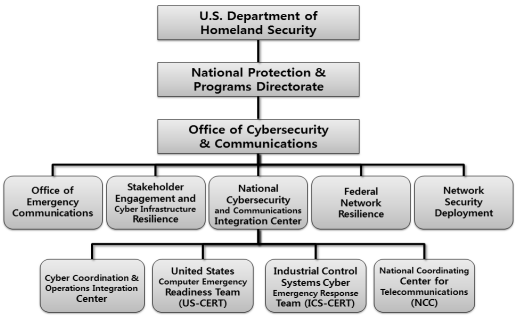
4.3 국토안보부(DHS)

DHS는 9·11 테러가 발생한 계기로 국가안보법(Homeland Security Act of 2002)에 의거하여 설립된 기관으로 국가 안보와 관련된 핵심 임무는 다음과 같다.

- □ 테러 방지 및 보안 강화
- □ 국경의 안전성 확보 및 관리
- □ 이민법 시도 및 운영
- □ 사이버 공간의 보호 및 안전성 확보
- □ 재해에 대한 복구 정의, 확보 및 보증

DHS의 임무는 사이버 보안 분야에 특화하고 있는 것은 아니지만, 다양하게 국토 안보 실현의 관점에서 민간 부문을 포함하고 있으며, DHS에서 사이버 보안도 중요한 임무가 되고 있다[31].

DHS에서 사이버 보안 관련 부서는 주요 인프라 및 IT 시스템의 사이버 보안을 담당하는 NPPD(National Protection and Programs Directorate)가 있으며, NPPD



〔그림 7〕 DHS 조직 구성도

부서 산하의 CS&C(Office of Cyber Security and Communications)는 사이버 보안 전문 조직으로, 사이버 보안 업무를 주도하고 있다[32].

CS&C에는 OEC(Office of Emergency Communications), SECIR(Stakeholder Engagement and Cyber Infrastructure Resilience), NCCIC(National Cybersecurity and Communications Integration Center), FNR(Federal Network Resilience), NSD(Network Security Deployment)와 같은 5개의 조직이 있다.

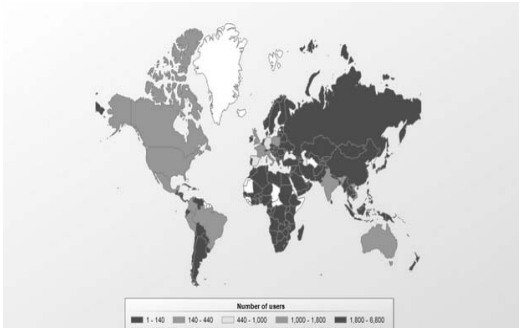
NPPD 산하의 CS&C 중 특히 주요 인프라를 중심으로 한 사이버 정보 집계 기관으로서 중요한 역할을 담당하는 기관이 NCCIC이다. NCCIC는 「사이버 보안 사안에 대한 대응 능력 강화 및 민관 협력 강화」를 실현하기 위해 전미 규모의 사이버 공격 시, 국가로서 대응 계획인 국가사이버사고대응계획(NCIRP : National Cyber Incident Response Plan)에 따라 설립된 기관이다[33].

또한, NCCIC에는 미국 사이버 위협 정보 통합 및 경계 정보나 주의 환기 정보를 발신하는 US-CERT(United States Computer Emergency Readiness Team), 제어 시스템에 대한 사이버 보안을 담당하는 ICS-CERT(Industrial Control Systems Cyber Emergency Response Team)와 더불어 24시간 사이버 공간을 모니터링하는 C3OIC(Cyber&Communications Coordination&Operations Integration Center), DHS 소관의 주요 인프라 중 IT 분야의 정부 측 조정 기관인 NCCT (National Coordinating Center for Telecommunications)와 같은 4가지 종류의 업무를 담당한다.

4.4 연방수사국(FBI)

연방수사국은 법 집행 기관으로서 수사 목적의 정보 활동도 적극적으로 진행하고 있다. 해당 수사 및 정보 활동의 대상에는 사이버 공간도 포함되어 사이버 범죄의 단속과 공격에 대한 조사 등은 FBI의 「Cyber Crime」 부서가 담당하는 임무 중 하나이다[34].

FBI는 2011년 11월 「Operation Ghost Click」이라는 전략을 통해 2007년부터 지속된 “DNSChanger”라는 악성코드에 기반을 둔 봇 인터넷 기반의 사이버 공격에 대응하고 폐쇄시키는 것을 성공하였다.



〔그림 8〕 국가별 DNS Changer 감염 수 (출처: Kaspersky)

FBI 사이버 보안 분야의 구체적인 전략적 조직 및 활동을 정리하면 다음과 같다[35-38].

- □ National Cyber Investigative Joint Task Force
  : 사이버 공간에서 범죄나 부정행위에 대한 수사를 횡단 조직적으로 수행할 수 있도록 관련 부처 간 조정, 통합 및 정보 공유
- □ Cyber Task Force
  : 모든 수준에서 활동을 보완 및 지원하기 위해 현지 수준의 사이버 범죄 수사 등에 종사하는 조직으로서 전미 56개소에 있는 FBI 사무실을 거점으로 사이버 공간에서의 공격, 범죄, 부정행위를 수사하고 단속하는 등의 활동을 수행
- □ InfraGard
  : DHS의 주요 인프라 보호활동을 지원하기 위한 FBI의 프로그램으로서 민간 IT 사업과 교육기관과의 연계를 목표로 사이버 보안 강화에 연결되는 사이버 공간에서 테러, 첩보, 범죄, 보안 등에 관한 정보를 공유

□ Strategic Alliance Cyber Crime Working Group
: 사이버 공간에서 범죄 단속 및 수사를 수행하기 위하여 5개국의 법 집행 기관으로 설립된 조직으로서 미국, 호주, 캐나다, 뉴질랜드, 영국의 법 집행 기관으로 구성

□ Cyber Action Teams
: 사이버 범죄 수사를 전문으로 하는 조직으로서 수사관, 분석관, 컴퓨터 감식 및 과학 수사관, 악성코드 전문가 등으로 구성

□ Internet Crime Complaint Center
: 인터넷상의 범죄 행위에 대한 불만 또는 정보를 받고 대응을 위해 적합한 기관에 전달해 주는 중개 조직으로서 주·지방 법 집행 기관의 사이버 수사 능력 향상을 목적으로 하는 비영리 단체인 전미 화이트 칼라 범죄 센터(National White Collar Crime Center)와 공동으로 설립

Ⅴ. 결 론

오늘날 모든 국가의 주요 인프라와 기관, 기업의 중요 자산을 목표로 사이버 공격이 이루어지고 있다. 또한, 사이버 공격의 다양한 방법과 이를 이용한 사이버 공격 동향을 통해서 전 세계적으로 사이버 보안 위협이 심각한 상황임을 인지할 수 있다.

따라서 본 고에서는 미국의 인프라 및 기관을 대상으로 이루어진 사이버 공격 중 APT 공격 유형과 이를 통한 사이버 공격 사례를 분석하였다. 이와 같이 다수의 사이버 공격이 시도됨에 따라 미국 정부도 사이버 보안에 대해 국가 차원의 정책 및 전략에 관심이 높아졌다.

이에 따라, 미국 정부는 사이버 공간에서 행해지는 보안 위협을 특정한 하나의 기관만 담당하는 것이 아니라 미국 국방부, 국가안보국, 국토안보부, 연방수사국 등 다양한 분야의 기관에서 사이버 보안을 위한 전략을 논의하고 임무를 수행한다. 이처럼 미국은 사이버 공격에 대해 조직적인 체계로 대응하고 있으며 장기적으로 고려하여 사이버 보안을 수행하기 위한 기술적인 측면과 더불어 인재 양성을 위한 활동도 다양하게 진행되고 있다.

앞으로 사이버 공격에 대한 방법은 더욱 지능적으로 이루어질 것이다. 따라서 본 고에서 분석한 사이버 공격에 대한 미국 정부 내 각 기관의 전략과 역할을 통해 기관별 연계성과 전략적인 대응을 마련하면서 도움이 될 것으로 기대된다.

참고문헌

[1] http://www.verizonenterprise.com/resources/reports/es_data-breach-investigations-report-2012_en_xg.pdf

[2] Tankard, Colin. "Advanced Persistent threats and how to monitor and deter them" Network security 2011.8 pp.16-19, 2011.

[3] de Vries, J. A., et al. "An analysis framework to aid in designing advanced persistent threat detection systems" 2012.

[4] http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf

[5] http://www.mcafee.com/us/resources/white-papers/wp-protecting-critical-assets.pdf

[6] Koch, R., Golling, M., Dreo, G., "Attracting Sophisticated Attacks to Secure Systems:A new Honeypot Architecture", Communications and Network Security (CNS), 2013 IEEE Conference on, pp. 409 - 410, 14-16 Oct. 2013.

[7] http://blogs.mcafee.com/archive/global-energy-industry-hit-in-night-dragon-attacks

[8] Bill M., Dale R., "A survey SCADA of and critical infrastructure incidents", RIIT '12 Proceedings of the 1st Annual conference on Research in information technology, pp. 51-56, 2012.

[9] http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

[10] http://www.reuters.com/article/2011/08/03//us-cyberattacks-idUSTRE7720HU20110803

[11] http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain

[12] http://news.bbc.co.uk/2/hi/asia-pacific/8142282.stm

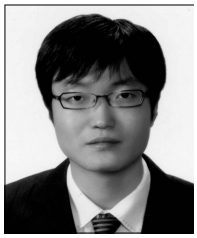
[13] http://www.reuters.com/article/2012/02/09/21/us-iran-cyberattacks-idUSBRE88K12H20120921

[14] http://www.fiercetelecom.com/story/att-reports-ddos-attack-its-dns-servers/2012-08-16?utm_medium=nl&utm_source=internal

[15] http://www.zdnet.com/u-s-power-plants-com-

bat-usb-malware-infections-7000009871/
[16] http://online.wsj.com/article/SB10001424127887323926104578276202952260718.html?mod=WSJASIA_hpp_LEFTTopWhatNews
[17] http://news.cnet.com/8301-1009_3-57567831-83/chinese-still-hacking-us-says-wall-street-journal-owner/
[18] http://bits.blogs.nytimes.com/2013/02/01/twitter-hacked-data-for-250000-users-stolen/
[19] http://bits.blogs.nytimes.com/2013/02/15/facebook-admits-it-was-hacked/
[20] http://bits.blogs.nytimes.com/2013/02/19/apple-computers-hit-by-sophisticated-cyberattack/
[21] http://www.networkworld.com/news/2013/020613-us-federal-reserve-admits-to-266472.html?source=nww_rss
[22] http://us.gizmodo.com/5981998/the-federal-reserve-said-it-was-hacked
[23] http://www.computerworld.com/s/article/9235721/MIT_to_probe_its_role_in_Aaron_Swartz_suicide
[24] http://www.defense.gov/home/features/2010/0410_cybersec/docs/USCC_Trifold-v13.pdf
[25] http://www.defense.gov/news/d20110714cyber.pdf
[26] http://www.washingtonpost.com/world/national-security/pentagon-to-boost-cybersecurity-force/2013/01/19/d87d9dc2-5fec-11e2-b05a-605528f6b712_story.html
[27] http://www.dc3.mil/
[28] http://www.nsa.gov/
[29] http://news.cnet.com/8301-1023_3-57560644-93/revealed-nsa-targeting-domestic-computer-systems-insecret-test
[30] http://www.nsa.gov/academia/nat_cae_cyber_ops/
[31] http://www.dhs.gov/our-mission
[32] http://www.dhs.gov/office-cybersecurity-and-communications
[33] https://www.dhs.gov/about-national-cybersecurity-communications-integration-center
[34] http://www.fbi.gov/about-us/investigate/
[35] http://www.fbi.gov/about-us/investigate/cyber/ncijtf
[36] http://www.fbi.gov/about-us/investigate/cyber/cyber-task-forces-building-alliances-to-improve-the-nations-cybersecurity-1
[37] http://www.fbi.gov/news/stories/2008/march/cybergroup_031708
[38] http://www.fbi.gov/news/stories/2006/march/cats030606

〈저자소개〉



이 동 범 (Dongbum Lee)
학생회원

2008년 2월 : 순천향대학교 정보보호학과 학사
2010년 2월 : 순천향대학교 정보보호학과 석사
2010년 3월~현재 : 순천향대학교 정보보호학과 박사과정
<관심분야> 정보보호, 정보보호 제품평가, 개인정보보호

곽 진 (Jin Kwak)
종신회원

2000년 8월 : 성균관대학교 학사
2003년 2월 : 성균관대학교 석사
2006년 2월 : 성균관대학교 박사
2006년 4월~2006년 11월 : 일본 큐슈대학교 방문연구원
2006년 4월~2006년 11월 : 일본 큐슈시스템정보기술연구소 특별연구원
2006년~2007년 2월 : 정보통신부 정보보호기획단 개인정보보호팀 통신사무관
2007년 3월~현재 : 순천향대학교 정보보호학과 교수
2010년 1월~2012년 12월 : 순천향대학교 SCH BIT 창업보육센터장
2011년 2월~2012년 12월 : 순천향대학교 중소기업산학협력센터 센터장
2008년 1월~현재 : 한국정보보호학회 이사
2008년 12월~현재 : 정보통신산업진흥원 기술평가위원
2010년 3월~현재 : 조달청 기술평가위원
2010년 5월~2010년 7월 : 교육과학기술부 국가기술수준평가 위원
2011년 1월~현재 : 한국정보처리학회 이사
2011년 1월~현재 : JIPS 논문지 편집위원
2011년 1월~현재 : 지식경제부 지식경제기술혁신평가단 위원
2012년 ~현재 : 한국암호포럼 운영위원
2012년 ~현재 : 한국방송통신전파진흥원 평가위원
2013년 ~현재 : 교육부 정책자문위원
2013년 ~현재 : 금융보안연구원 보안기술 자문위원
2013년 ~현재 : 금융감독원 인증방법평가위원
<관심분야> 자동차 보안, 암호프로토콜, 응용시스템보안, 개인정보보호, 정보보호제품평가, 클라우드 컴퓨팅 보안