인터넷 침해유형과 대응조직

우성희

한국교통대학교

Cyber Attack Type and CERT

Sung-hee Woo

Korea National University of Transportation

E-mail : shwoo@ut.ac.kr

요 약

인터넷이 우리의 생활의 기본 인프라로 자리 잡고 사이버 공간에서의 생활이 일상화되면서 부가적인 많은 문제점들이 생겨났다. 그 중 사이버 침해는 정보사회의 가장 심각한 문제 가운데 하나가 되었다. 해마다 증가하는 사이버공격, 지능화되고 진화하는 공격 유형 등으로 사이버 생태계가 더 복잡해지고 있다. 따라서 본 연구에서는 최근 인터넷 침해 사고 현황과 인터넷 침해 유형 및 해킹 방법을 분석하고 국내 대응 조직 및 국제 협의체 현황을 분석하였다.

ABSTRACT

The internet is established as the basic infrastructure of our life and we live in cyberspace on internet, and additionally many problems on cyberspace arise. One among them is the most serious cyber attack of the information society. The cyber attacks increase each year, attack type and the intelligence is evolving, and then the cyber ecosystem is getting more complicated. In this study, we analyze the Internet last incident status and type of Internet invasion and hacking methods, and analyze the corresponding national and international organizations and associations active status.

키워드

cyber attacks, hacking, cyberspace, invasion, CERT

Ⅰ. 서 론

우리나라는 지난 10년간 정보통신기술의 발달로 특히, 정보화와 인터넷 관련 기술의 발달로 생산성과 효율성이 향상되었고 선진국으로 도약할 수 있는 발판이 되었다. 이를 기반으로 모든 사회가 연결되어 네트워크화 되고 국가기관 및 민간기업 대부분의 활동이 인터넷 기반으로, 심지어는 개인의 활동 역시 인터넷 기반으로 이루어지고 있다. 그러나 이에 따른 침해사고 시 그 피해는 기하급수적으로 늘어나고 그 파장은 모든 영역을 한순간에 마비시키는 결과를 초래할 수 있다. 따라서 이러한 정보통신기술의 기능을 최대한 활용하고 역기능을 최소화하기 위해서는 인터넷 침해사고에 대한 분석과 대응방안에 많은 관심을 가져야 할 것이며 지능화 되고 진화하는 침해 방법들을 지속적으로 분석하여 대응방안을 만들어내는 일 또한 정보화 사회의 가장 중요한 일이라 할 수 있다.

최근 10여 년간 다양한 인터넷 침해사고[7]가 발생하고 그 시점에서는 언론이나 주요 전문가들에 의해서 이슈화가 되고 주목을 받지만 그 시기가 좀 지나면 그에 대한 관심도는 현저히 줄어든다. 따라서 네트워크화 된 사회에서 그 기능을 최대한 활용하기 위해서는 국가 차원의 보호 방향을 제시하여 국민들의 인식을 끌어올려 인터넷 사회가 나아가야 할 방향성을 제시하여야 할 것이다. 따라서 본 연구에서는 최근 인터넷 침해 사고 현황과 인터넷 침해 유형 및 해킹 방법을 분석하고 국내 대응 조직 및 국제 협체 현황을 분석하였다.

Ⅱ. 최근 인터넷 침해사고 및 현황

이전의 인터넷 침해가 바이러스나 웜과 같이 개인의 PC에 악성코드를 감염시키고 이를 통하여 발생하는 사고가 주를 이루었다면, 지금은 공격기법이 변화, 진화[3]하여 APT 공격 및 개인정보 유출, DDoS 공격 등으로 인한 사고가 그림1[1]과 같이 증가하는 추세이다. 실제 KISA가 분석한 해킹사고를 살펴보면 악성코드감염으로 인한 해킹사고가 줄어들고 점차 새로운 공격기법이나 특정한 목적으로 한 서버대상 해킹사고가 늘어난 것을 확인할 수 있다. 최근 주요 해킹 사례들[1]을 보면 다음과 같다.

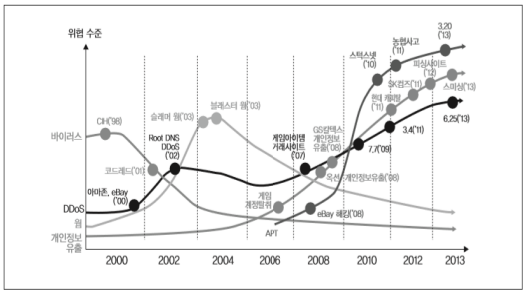

그림 1. 국내해킹사고 변화

1) 사례 1

최근 A게임 유럽지사의 00게임이 DDoS 공격의 대상이 되었다는 신고를 받아 KISA은 00게임의 과도한 트래픽을 전송한 국내 IP를 조사, 조사결과 NTP 서버 포트(123)가 열려 있고, 해당 NTP 서버에 인-바운드 아웃-바운드 트래픽의 변화가 많은 것으로 DDoS 공격을 한 것을 확인 할 수 있었다.

2) 사례 2

국가기관 친목단체인 F사는 최근 한 언론사에서 해킹을 당해 개인정보가 유출되었다는 제보로 실제 정보가 유출되었는지 확인할 수가 없었기 때문에 기술지원 요청을 하였고 KISA에서는 서버분석을 진행하였다. 결과로 해당 서버는 외부에서 웹 페이지를 크롤링한 흔적을 확인, SQL injection 작업을 수행하여 대규모 개인정보를 탈취한 증거를 확보하였다.

3) 사례 3

2013년 말 H 쇼핑몰은 공격자가 홈페이지 내 악성 스크립트를 삽입하여, 악성코드 경유지로 활용되었다. KISA 탐지시스템에서는 H 쇼핑몰이 악성코드 경유지로 악용되는 것을 탐지하고 업체에 이를 알렸으며, H 쇼핑몰은 이에 KISA에 해킹원인을 확인해 달라는 기술지원 요청을 하였다.

4) 기타 사례들

지난해 발생한 2013년 3.20 및 6.25 사이버 공격이외에도 2011년도 디도스 대란, SK컴즈 개인정보 유출사고, 2008년 옥션 해킹사고, 2006년 리니지게임 명의도용 사고, 2003년 1.25 인터넷 침해사고 등 많은 인터넷 침해사고[6][7]들이 있었다.

Ⅲ. 인터넷 해킹사고 유형 및 해킹기법

인터넷 세계는 유무선으로 연결된 인터넷 서비스 장비와 소프트웨어들 그리고 이용자들이 복잡하게 연결된 하나의 거대한 생태계 구조를 갖는다. 이 생태계는 복잡하고 때로는 사이버공격이 발생되어 정보유출 등의 피해를 볼 수 있다. 새로운 형태의 기기가 다양하게, 대량으로 인터넷에 연결 되면서 사이버 생태계는 더욱 복잡해지고, 빠른 변화 속도를 가져왔다. 언제 어디서나 편리하고 쉬운 인터넷 환경으로 바뀌어가기 때문에, 사이버공격 수법도 빠르게 변화하고 있다. 공격자 또한 사이버 공격수법을 계속적으로 개발하고 있다. 국내에서 빈번하게 발생하고 있는 종래의 홈페이지 악성코드 유포, 홈페이지 변조, 디도스 등의 해킹 사고 유형과 최근에 국내에서 자주 발생하는 피싱, 파밍, 스미싱 등의 유형[2]은 다음과 같다.

표 1. 침해유형

사고유형	개 요
홈페이지 악성코드	이용자가 많은 홈페이지 서버에 악성코드 혹은 악성스크립트를 은닉하여 홈페이지 접속자에게 악성코드를 유포하는 사이버공격 유형
홈페이지 변조	홈페이지 서버를 공격하여 홈페이지 화면을 공격자의 이미지로 변조
디도스	공격자가 감염시킨 좀비 PC를 이용해 다량의 패킷을 웹서버나 DNS 서버등의 특정 시스템으로 송신하여 서비스를 마비시키는 분산 서비스 공격
피싱	피싱은 지인 또는 유명기업을 사칭한 메시지를 이메일, 메신저, 문자 등 다양한 서비스를 통하여 공격대상자에게 전송, 메시지 수신자는 가짜사이트에 접속하여 이용자가 자신의 금융정보를 직접 입력하도록 유도
파밍	홈페이지의 주소를 정확히 입력하더라도 공격자가 만든 가짜 사이트로 접속하게 되는 사이버공격
스미싱	안드로이드 스마트폰 이용자를 대상으로 문자메시지 전송을 이용한 공격

다음은 시스템 관리 차원의 시스템 해킹 방법들이다. 하드웨어 취약점 악용, OS 또는 웹어플리케이션과 같은 서비스단의 취약점 악용, 사회공학적 기법을 이용한 악성코드 감염과 계정 유출 등 공격자들은 다양한 수준과 방법의 공격기법을 선택할 수 있다. 공격자는 공격대상 시스템이 어떠한 취약점을 가지고 있는가에 따라 공격기법을 결정하게 된다. 해킹된 시스템 분석을 통해 주로 확인되는 해킹기법[1][5]은 다음 표 2 와 같다.

Ⅳ. 침해사고 대응조직 및 국제 협의체

인터넷으로 연결된 우리의 환경에 사이버 공격이 발생하면 그 피해는 한순간에 지구 전체로 퍼져 나갈 수 있다. 따라서 이런 사이버 사고나 해킹으로부터 우리의 사이버 생태계와 개인정보를 지키고 공격에 대응하기 위해서는 정부 뿐 아니라 전 세계적인 협의체제[4]와 대응체제가 마련되어야 한다. 최근 몇 년간 수차례 발생한 대규모의 네트워크 공격, 카드사 고객 정보 유출 등이 바로 그 예이며 빅데이터의 등장으로 개인정보가 악용될 소지도 높아지고 있다. 따라서 보안은 사람들의 삶에도 많은 영향을 끼칠 것으로 예상되며 인터넷 자체가 보호되어야만 하는 중요 인프라가 되었다. 이러한 중요 인프라를 보호하고자 국내에서는 한국인터넷진흥원(舊 한국정보보호진흥원)의 CERTCC-KR(現 KrCERT/CC)을 중심으로 CERT 활동이 시작되었으며, 1990년대 말부터 국제사회에서도 한국의 정보보호 활동이 본격적으로 주목받게 된다.

1) CERT

1988년 최초의 웜인 모리스(Morris)가 인터넷을 통해 급속히 전파되자 미국 방위고등연구계획국(Defence Advanced Research Projects Agency,

DARPA)은 카네기멜론대학교 소프트웨어공학연구소(Software Engineering Institute,SEI) 내에 침해사고대응팀 조정센터(Computer Emergency Response Team Coordination Center, 이하 CERT/CC)를 설립하였다. 이것은 세계 최초의 CERT이며, CSIRT (Computer Security Incident Response Team)로 불리기도 하는 인터넷상 침해사고에 대응하는 조직이다. 국가의 핵심 자원과 주요 인프라를 보호하고 CERT 간 커뮤니티를 구축하기 위해 다양한 국가 및 지역적 역할이 강조되고 침해사고 대응 활동을 조정하기 위한 국가 차원의 중심지 설정이 필요하고, 이를 통해 광범위한 사이버 침해사고 정보를 공유하고 다수의 영역에서 동시다발적으로 발생하고 있는 위협 등을 종합하여 분석정보를 병합하는 것이 가능하게 되었다. 이것이 바로 한 국가의 사이버보안 조정 역할을 수행하는 국가 CERT (CERT with National Responsibility)이며 통상 국가대표 CERT(National CERT)로 부르고 있다. 다음 표 3 은 국가대표 CERT의 몇 가지 예이다.

표 2. 해킹유형

해킹유형	개요
NTP 증폭을 사용한 DDoS 공격	공격자가 자신의 IP를 위조해서 monlist[1]를 NTP (Network Time Protocol) 서버에 요청, 위조된 IP로 NTP 서버에 접속한 리스트 전송
SQL injection을 통한 계정정보 탈취	가장 널리 악용되고, 오래된 전통적인 해킹 기법 중 하나이며 해커들이 많이 사용하는 필수 공격 기법
파일업로드 취약점을 악용한 웹셸 업로드	웹사이트 방문자가 게시물(파일)을 업로드 할 수 있는 기능이 존재할 경우 악용
게임 스킨 등을 통한 악성코드	일반 사용자들을 대상으로 한 공격으로 컴퓨터를 악성코드에 감염시키는 방법, 사용자에게 무료로 배포, 이를 이용하여 사용자 PC에 악성코드를 감염시킴
시큐어셸(SSH) 백도어	공격자는 지속적으로 시스템에 쉽게 접속하기 위해 백도어를 설치해두고 이 백도어를 통해 시스템에 접속하는 공격자는 관리자 권한을 획득
동기화 프로그램 악용	웹 서비스를 위해 여러대의 서버를 동시에 운영하는 경우 웹서버간의 동기화 프로그램 이용, 공격자는 동기화 프로그램을 통해 공격대상 서버의 파일을 다운로드하거나 공격대상 서버에 악성코드를 업로드 함
관리용 PC 해킹	관리용 PC가 해킹될 경우 공격자는 관리자가 관리하는 다수의 시스템에 대한 계정을 쉽게탈취
가상사설망(VPN) 서비스 악용	공격자가 자신을 숨기기 위해 주로 사용하는 방법이 해킹 경유지를 사용, 해킹 경유지를 확보하기 위해 사용하는 방법이 OS에서 제공하는 VPN 서비스를 악용하는 방법
윈도우 고정키(Sticky Key) 백도어	Sticky Key 백도어는 윈도우의 고정키 기능을 악용하는 해킹 기법다. 윈도우에서 고정키와 관련된 실행파일은 sethc.exe 연속으로 shift키를 5번 클릭하게 되면 실행, 악용, 및 해킹수행

표 3. 국가대표 CERT의 예

국가	CERT 명	소속기관 (예산지원기관)	형태
한국	KrCERT/CC	미래창조과학부(한국인터넷진흥원)	산하공공기관
중국	CNCERT/CC	공업정보화부	산하공공기관
일본	JPCERT	경제산업성	비영리기관
호주	CERT Australia	법무부	정부
미국	US-CERT	국토안보부	정부

2) 국가 협의체

전 세계를 하나의 네트워크로 연결해 주면서 한 국가에서 발생된 사이버 침해사고가 전 세계로 빠르게 전파될 수 있는 기반이 구축되고 최신 침해사고 정보의 공유 및 국가 보안문제에 영향을 미칠 수 있는 사안에 관하여 타 국가대표 CERT와 정보를 교류해야 할 필요성이 있다. 따라서 전 세계적으로 CERT간 신뢰할 수 있는 의사소통 채널을 활성화하고 예방 및 대응 조치의 조정(Coordination)을 신속하게 촉진하는 인프라와 메커니즘 개발 등이 필요하다. 따라서 CERT간 글로벌 협력체가 등장하게 되었으며 전 세계가 소통할 수 있는 다음과 같은 공식적인 장[4]이 마련되었다.

표 4. 국제협의회

협의회	개요
국제침해사고대응팀협의회	1990년 전 세계 최초로 CERT간 협력체인 FIRST가 창설, 64개국 289개의 팀으로 구성
아태침해사고대응팀협의회	2003년 설립, 아시아 태평양 지역 내 CERT 간 상호 협력을 강화목적
국가대표침해사고대응팀연례회의	2006년 CERT/CC 주관으로 최초 개최된 국가대표 침해사고대응팀 연례회의(이하 국가대표 CERT회의)
이슬람국가연합 침해사고 대응팀 협의회	2005년 6월 이슬람 개발은행(IDB, Islamic Development Bank) 연례회의에서 OIC 국가간 CERT 말레이시아, 튀니지, 나이지리아, 파키스탄, 사우디아라비아, 아랍에미레이트 등 6개국의 6개 기관을 창립멤버로 결성, 2009년 5월 시리아에서 개최된 이슬람협력기구의 소속기관으로 승인되어 국제기구로 변경

Ⅴ. 결 론

인터넷이 우리 생활의 기본 인프라로 자리 잡고 사이버 공간에서의 생활이 일상화 되면서 생겨나는 문제점 즉, 지능화 되고 진화하는 사이버 공격으로 사이버 생태계가 더 복잡해지고 개인정보 누출로 인한 많은 피해가 증가하고 있다. 오늘날 모든 분야에서의 정보보안은 기본 필수조건이다. 따라서 이것을 충족시키기 위해서는 인터네 침해유형을 분석하고 이에 대응방안을 마련해야 할 것이다. 따라서 본 연구에서는 최근 인터넷 침해 사고 현황과 인터넷 침해 유형 및 해킹 방법을 분석하고 국내 대응 조직 및 국제 협의체 현황을 분석하였다.

참고문헌

[1] 이재춘, “최근 주요 해킹사고 사례와 대응전략”, INTERNET & SECURITY FOCUS, 2014. 4.
[2] 유학용, 유동영, “사이버공격 대응 기본 매트릭스”, INTERNET & SECURITY FOCUS, 2014.
[3] 송지훤, 류소준, “진화하는 악성코드피싱・큐싱 결합해 PC・스마트폰 동시 공격”, INTERNET & SECURITY FOCUS, 2014.7.
[4] 정홍순, 박종원, “침해사고대응조직과 국제협력, INTERNET & SECURITY FOCUS, 2014.2.
[5] 이재광, “해킹기법과 대응 전략”, INTERNET & SECURITY FOCUS, 2013.4.
[6] 신종환, “국내 주요 인터넷 사고 경험을 통해 본 침해사고 현황”, INTERNET & SECURITY FOCUS, 2014.7.
[7] “2014년 6대 정보보안 위협요인”, 한국방송통신전파진흥원, KCA, 2014.2.
[8] “Inernet & security biweekly”, 한국인터넷진흥원, 2014.2.