최근 사이버위협 전망 및 분석

강순희*, 박용조**, 김은철***
한국전력거래소*, **, ***

Response plan for Recent cyber Threaten

Kang Sun-Hee*, Park Yong-Joe**, Kim Eun-Cheol***
KOREA POWER EXCHANGE*, **, ***

Abstract - 글로벌시대 '세계는 사이버 전쟁중이다'. 사이버냉전이 시작된 것이다. 해커들의 공격에 각국 정부 당국들이 전전긍긍하면서 대응책 마련에 부심하고 있다. 그런 가운데에서도 미 국방부와 국무부가 해커들에 뚫리는가 하면 영국, 독일, 프랑스의 정부 및 주요기간 전산망들을 해커들이 휘젓고 다니고 있어 보안에 빨간 불이 켜진 상태다. 더욱이 우리나라는 유럽 등으로부터 받는 공격도 적지 않지만 중국, 미국이 연습 상대나 놀이터쯤으로 여기고 있는 상대"라고 한다. 인터넷 보급률 세계 1위 명성에 걸 막게 네트워크 구성, 주요 전산망 연결이 얼마나 잘되어 있는가? 충분이 세계 해커들의 시험대상이 되기 충분하다. 이러한 상태에서 사이버 역기능에 대한 해결방안은 주기적 분석·대응 활동을 통해 보안대책을 신속히 추진하는 길만이 사이버안전을 지키는 일이다.

1. 서 론

최근 청와대 해킹사고, 국민건강관리공단 직원의 72만 개인정보 유출, 국내유명 인터넷 쇼핑사이트 1천만명에 달하는 회원정보 유출 등 피해가 잇따르고 있다. 이는 인터넷 의존도 증가함에 따라 이를 통한 국가기관·첨단기업 중요자료 절취, 개인정보 유출, 프라이버시 침해, 금전적 갈취 등의 정보화역기능이 지속적으로 확산되고 있는 상황이다. 특히, 중국 해커들의 침해행위가 일/일 5천여 건씩 출현 하는 등 해킹사고가 연일 발생하고 우리나라가 해커들의 놀이터가 된지 오래된 일이다. 또한, 이용자의 편익이 증가함에 따라 최근 IT환경은 웹 2.0도입과 UCC(User Created Contents) 대중화로 인하여 인터넷의 새로운 패러다임이 도래하였으며, 이에 대한 사회적인 역기능도 부각되고 있다. 이외에도 Windows Vista의 출현, 이동형 저장장치를 통한 악성코드의 전파, 인터넷 뱅킹에 대한 메모리 해킹, 디지털 포렌식 기술의 사회 이슈화, 기밀정보 유출사고에 대응하기 위한 내부자 보안의 중요성 재부각 등이 최근 주요 사이버 위협 이슈라고 할 수 있다.
향후에는 국가간의 사이버 스파이, 자동화 공격수법, DDoS 공격의 계속된 위협, UCC 및 Web 2.0 기반의 악성코드 증가, 홈페이지 해킹을 통한 악성코드 유포시도 지속, 지능화 된 3세대 피싱 출현 등이 이슈가 될 것으로 전망된다. 이에 본 논문에서는 최근 사이버위협 이슈들을 분석하고, 향후에 사이버위협 이슈가 될 사항들을 전망하고자 한다.

2. 본 론

2.1 취약점에 의한 해킹 및 악성코드 전파 증가

청와대 관계자는 부인하지만 중국·북한 해커에 의해 국가기관의 심장인 청와대가 속수무책으로 뚫렸다. 청와대 전산망이 해킹 당했다는 사실, 현재까지도 잃어버린 자료의 규모와 내용을 모른다는 사실은 충격을 넘어 국가안보 차원의 심각한 우려를 낳고 있다. 이러한 언론보도를 접하면서 해외발 해킹(Hacking) 및 악성코드(malicious code)에 의한 공격은 매일 5천여 건씩 출현하는 것으로 파악되고 있다. 특히 중국은 1990년대 중반부터 시스템 및 네트워크에 대한 연구를 통하여 중국 특유의 언더그라운드 해커 문화를 형성하였다. 1990년대 후반 중국 해커들의 기술은 외국에서 개발된 프로그램을 이용하는 수준이었지만 차차 해커들 스스로 트로이목마 프로그램이나 해킹 프로그램을 제작하기 시작하였으며, 최근에는 국내 국가·공공기관의 시스템을 해킹하여 주요 자료를 빼내가거나 웹서버 해킹을 통하여 우리나라 국민의 개인정보를 빼내가는 수준에 이르고 있다. 중국발 해킹은 우리나라 뿐만 아니라 미국 등도 목표가 되고 있어 최근 미 육군에서는 주요 PC를 매킨토시로 교체하는 작업까지 수행하고 있는 상황이다. 그만큼 중국발 해킹은 전 세계적으로 큰 위협으로 자리 잡고 있다. 중국발 해킹에서 개인정보를 유출해가는 절차를 보면, 우선 접속자가 많은 유명 사이트의 웹서버를 해킹하고, 자신이 만들거나 인터넷으로 다운받은 해킹 프로그램으로 악성코드를 이식한 뒤, 보안패치나 백신이 없는 일반접속자의 PC로 악성코드를 번식시키고, 접속자 PC에 상주하여 주민등록번호, 각종 사이트 아이디 및 비밀번호를 추출함으로써 마지막으로 추출된 개인정보 해커 컴퓨터로 이동시키는 방법을 이용하고 있다.
한국정보보호진흥원에 따르면 외국의 국내 사이트 해킹 시도 중 중국의 비중이 2007년 8월 69.6%, 9월 65.9%, 10월 42.9%에 해당하여 국가단위로는 1등이라고 발표하였다. 심지어는 중국 내에서 한국의 웹서버를 해킹하는 방법이나 한국인의 개인정보를 취득하는 해킹기법에 대한 자세한 설명과 도구가 담겨져 있는 잡지가 시중에 유통되고 있는 상황이다.
세계적으로 취약점에 의한 해킹 및 악성코드 전파가 중국의 의해 65% 이상을 주도되고 있어 중국발 해킹 및 악성코드 예를 들었던 것이다.

2.1.1 USB메모리 감염 악성코드 폭증

최근 USB메모리를 비롯한 이동식디스크를 대상으로 하는 악성코드가 증가하고 있다. 심지어 PC를 지키기 위한 보안 USB도 감염이 가능한 것으로 드러났다. 특히 지난 6월 이후 USB를 이용하는 악성코드가 많이 출현하고 있다.

<표 1> 2007년도 USB를 이용한 악성코드 발견 건수 (출처:뉴테크웨이브)

월	1월	2월	3월	4월	5월	6월	7월	8월	9월	10월	11월
건수	5	3	14	30	64	276	290	276	235	188	168

이들 악성코드는 평상시에는 정상적인 윈도우즈 운영체제 구성파일(autorun.inf)인 것처럼 숨겨져 있다가 이동식디스크가 연결되는 순간 자동으로 실행된다. 따라서 USB 메모리 안에 autorun.inf 파일이나 휴지통이 생성되어 있다면 악성코드에 감염되었을 가능성이 높다. 이 악성코드는 autorun.inf 파일을 이용해 해당 드라이브를 열려고 시도하면 연결된 악성파일이 자동 실행돼 이동식 디스크를 포함한 모든 디스크 드라이브를 감염시키는 행위를 수행한다.
따라서 사용자들은 USB메모리를 PC에 연결할 때 반드시 해당 드라이브를 백신 프로그램을 이용하여 검사하여야 한다. 또한, 사이버안전센터 홈페이지를 통해 배포중인 'usbguard'를 PC에 내려받아 수행하면, 이후부터는 autorun.inf 파일의 자동실행 차단으로 USB메모리 바이러스도 실행이 차단된다. 앞으로도 이와 같은 USB를 통한 악성코드는 다양하게 출현할 것으로 예상된다.

2.1.2 Windows Vista 보안취약점 본격 출현

2007년 초에 MS社는 새로운 개념의 운영체제로 Windows Vista를 출시하였다. Windows Vista의 모든 사용자는 관리자 그룹에 속해 있더라도 일반 사용자의 권한으로만 프로세서를 생성할 수 있으며, 관리업무가 필요할 때에는 반드시 사용자 및 관리자의 허가를 득하도록 제제를 가하고 있다. 또한 과거 해커들의 주공격 대상이 되어 왔던 서비스와 커널 모듈에 대한 보호 정책을 통해 인증되지 않은 사용자 프로세스는 높은 권한의 프로세스 및 파일에 접근이 불가능하도록 되어 있다. 이렇듯 Windows Vista 보안기능은 기본은 "대부분 사용자는 관리자 권한으로 모든 프로그램을 구동 및 개발할 필요가 없다"이다.
2007년도부터 Windows Vista가 본격 사용됨에 따라 아래[표1]과 같이 보안취약점들이 많이 발견되었다. Windows XP에 비해서는 발견 건수가 적지만 계속적으로 보안취약점이 발견되고 있으므로 계속적인 주의가 필요하다.

〈표 2〉 2007년도 Windows 운영체제 보안취약점 발견 건수

순 위	Windows XP	Windows Vista
극도로 심각한 취약점 발견 건수	3	1
심각한 취약점 발견 건수	19	12
중간수준의 취약점 발견 건수	2	1
심각도가 낮은 취약점 발견 건수	3	1
취약점 발견 전체 건수	34	20

(출처:ZDNet.co.uk)

위 [표 2]는 ZDNet.co.uk의 발표자료를 참조한 것이며, http://www.microsoft.com/technet/security/current.aspx 사이트를 통하여 확인한 결과, 발표된 Windows Vista 보안 취약점은 22개로 확인할 수 있다.

2007년도에 Windows Vista의 출현으로 갑작스럽게 강화된 보안 기능들로 인해 Windows XP/2000 등의 기존 운영체제 개발자가 빠른 적응을 보이지 못해 어려웠던 점도 있었으며, 오히려 이러한 호환성 컴포넌트가 새로운 보안 위협 요소로 작용할 가능성도 배제할 수 없다는 분석이다. 현재까지는 Windows Vista 사용자가 급격히 증가하지 못한 상황이다. Windows Vista는 대부분 주요 보안 관련 결정을 사용자에게 전가시키고 있다는 분석도 있지만, 보안성을 향상시키는 효과는 가지고 있다고 본다. 향후에는 Windows Vista 사용자가 증가하면서 관련 보안취약성 및 보안사고가 더욱 이슈가 될 것으로 전망된다.

2.1.3 공격·방어기술 자동화 적용 심화

최근에 발견되고 있는 악성코드들은 자동으로 다운로드되고 업데이트되는 방식으로 유포되고 있어 이에 대처할 수 있는 자동화 기법이 향후 정보보호 시장의 키워드가 될 것으로 전망되고 있다. 기존의 안티바이러스 솔루션들도 시그니처 기반의 탐지에서 점차 다기능 다계층 보호를 제공하는 방향으로 발전되고 있다. 특히, 자동화된 데이터베이스 업데이트, 휴리스틱기법 등을 이용한 사전행동분석 및 실시간 행동분석 기법 등이 이러한 노력에 해당된다. 또한 최근 한국전자통신연구원 정보보호연구단에서 발표한 ZASMIN 프로젝트의 경우에도 제로데이 공격에 대응하기 위하여 하드웨어 기반의 고성능 시그니처 자동생성 기법을 연구 및 개발하고 있다.

이와 같이 향후에는 새롭게 변화하는 악성코드에 실시간적으로 대응하기 위하여 침입탐지시스템 및 백신프로그램과 같은 보안제품에 자동으로 패턴을 추가하는 기술에 대해 계속적인 연구개발이 이루어지게 될 것이다. 또한 더 나아가서 공격이 탐지되었을 때 해당 공격에 대한 대응을 위하여 라우터 및 침입차단시스템에 자동으로 정책을 설정해주는 기술도 필요하게 될 것이다.

2.1.4 DDoS 공격의 위험성 상존

DDoS(Distributed Denial of Service) 공격은 네트워크 내에 수많은 시스템들을 해킹하여 마스터 프로그램 및 에이전트 프로그램을 설치하여 공격자가 목표 시스템으로 공격시에 활용하는 공격 기법이다. 이 공격은 일반적인 해킹과 달리 목표 시스템의 관리자 권한을 획득하는 등 고도의 기술이나 전문지식이 필요하지 않다. 단순히 해당 시스템에 무수히 많은 접속을 시도하는 간단한 방법으로 시스템을 마비시킬 수 있어 공격자 입장에서는 너무나도 매력적인 공격 기법이다. DDoS공격은 규모와 피해면에서 더욱 커지면서 이를 탐지하고 완화하는 것도 더욱 어려워지고 있는 실정이며, 그 대상이 데이터베이스 서버, 어플리케이션 서버, 웹 서버, DNS(Domain Name System) 서버, 메일 서버, 라우터 및 침입차단시스템 등으로 다양하다.

또한 최근에 발생한 게임 아이템 중개사이트에 대한 DDoS 공격의 경우, 과거에 비해 그 강도가 전례를 찾아볼 수 없을 정도의 규모로 수십G에 해당되는 공격이었다고 한다. 이 정도 용량의 공격은 ISP 및 금융관련 사이트도 일순간에 마비시킬 수 있는 규모에 해당된다. 이렇듯 DDoS 공격은 데이터나 정보를 훔치는 다른 공격과는 달리 몇 일 또는 몇 주 동안 비즈니스를 중단시키는 결과를 초래할 수 있는 주요 위협으로 향후에도 발생 가능하다.

문제는 이러한 DDoS 공격이 국가 간의 분쟁 시 이용이 가능하다는 점이며, 최근에 발견되고 있는 봇넷들이 DDoS 공격의 중간 마스터 및 에이전트 시스템으로 활용이 가능하다는 점이다. 따라서 개인 사용자들은 최신 윈도우즈 보안패치를 설치하고, 백신프로그램을 이용하여 자신의 시스템을 주기적으로 점검 및 치료하는 노력을 기울여야 할 것이다.

2.1.5 UCC를 이용하는 악성코드의 증가

UCC는 일반 사용자들이 컨텐츠를 만들고 공유할 수 있다는 점을 이용해 누구나 흥미를 가질만한 내용의 컨텐츠를 작성하고 해당 컨텐츠에 보안 취약점을 이용하여 애드웨어나 스파이웨어 또는 바이러스를 설치하는 코드를 삽입해 이를 보는 사용자를 공격하는 방법으로 사용될 가능성이 매우 높다. 실제로 얼마전 국내 애드웨어 제작사의 경우 보안 취약점(MS06-014)을 이용해 자사의 애드웨어를 배포하는 사례가 발견되었다.

따라서 수익을 극대화하기 위한 애드웨어 제작사와 배포자가 이를 이용할 가능성이 높아졌다. 특히 보안패치가 발표되기 이전에 해당 취약점을 이용하는 제로데이 공격이 성행하고 있는 요즘 그 위험성은 더욱 높아지고 있다. UCC를 이용하는 공격은 대부분 윈도우즈 운영체제나 응용 프로그램의 취약점을 이용하게 되는데 사용자의 보안패치 설치 미숙이나 새로운 취약점을 이용하는 제로데이 공격에 대해서는 속수무책일 수밖에 없는 실정이다. 얼마전 MySpace에서 동영상 제생을 위해 사용하고 있는 Apple社의 Quick Time 도영상에 악성 자바 스크립트를 삽입해 동영상을 플레이하면 피싱 사이트로 변경되어 사용자의 계정정보를 유출하려는 시도가 있었다. 이러한 사고는 해당 서비스를 제공하는 회사에서 사용자가 이용하거나 업로드 하는 컨텐츠 데이터의 이상 유무를 확인해 문제가 될 수 있는 부분을 사전에 필터링해야 하는 부분을 처리하지 않는 등 보안의 중요한 요소를 간과하고 있기 때문에 발생한 것이라고 볼 수 있다.

이렇듯 이러한 사고는 서비스 제공 회사에서 지속적인 모니터링과 관리가 있어야 예방이 가능한 부분이라고 생각된다. 향후에도 이러한 UCC를 이용하여 악성코드를 전파하려는 시도가 증가할 것이며, 사용자가 직접 만들어서 배포하는 소프트웨어인 UCS(User Created Software) 또한 UCC와 같이 새로운 악성코드 전파의 방법으로 증가할 것으로 예상된다.

2.1.6 홈페이지 해킹을 통한 악성코드 유포시도 지속

홈페이지를 대상으로 하는 해킹은 웹 프로그램 개발 단계에서 보안에 대한 고려가 없이 개발을 하였거나, 웹서버에 대한 원격관리를 위한 서비스를 오픈하여 이용하는 부분에서 취약점이 이용되는 경우가 많다. 아직까지도 SQL Injection 등 많이 알려져 있는 취약점이 존재하여 해킹 공격을 당하는 보안사고가 많이 발생되고 있다.

이와 같이 국내 웹사이트를 해킹한 뒤 트로이목마를 유포시키는 경유지로 악용하는 사고는 향우에도 계속적으로 발생될 것으로 전망된다. 특히 공격 대상 사이트로 국내 인터넷 사용자들의 접속이 많은 국내 웹사이트들이 주로 이용될 것이며, SQL Injection 등의 취약점이 계속적으로 많이 이용될 것으로 전망된다. 따라서 각 기관에서는 웹 프로그램 개발 시 취약점이 될 수 있는 코드들이 삽입되지 않도록 주의하여야 하며, 시스템 운영시 보안 관리에 만전을 기해야 한다.

2.1.7 지능화된 3세대 피싱 출현

피싱(Phishing)은 개인정보(Private Data)와 낚시(Fishing)의 합성어로서, 낚시 수법으로 일반인의 개인정보를 빼내간다는 의미의 합성어다. 은행과 같은 유명기관을 사칭해서 개인에게 이메일을 보낸 뒤 사람들이 이메일을 통해 위장 홈페이지에 접속하면, 개인정보를 입력하도록 유도하여 개인정보를 몰래 빼내가는 것이 일반적인 방법이다. 올해 초에만 해도 국내 유명 은행의 인터넷뱅킹 사이트를 모방한 가짜 홈페이지에 접속한 이용자 5,000여 명이 개인정보와 보안카드 비밀번호를 의심 없이 입력하여 이들의 공인인증서가 유출되는 해킹사고가 발생하였다.

피싱의 초기 형태는 사회공학적 방법을 이용한 사용자의 ID와 패스워드를 탈취하는 것이었으나 시간이 지날수록 계정정보까지도 도용하여 금융정보에 불법적으로 접근하거나 피싱 사이트를 이용하여 인터넷 이용자를 유인하는 기법으로 진화하고 있다. 최근에는 악성코드를 활용하여 이용자 컴퓨터를 공격하는 수법이 등장하였다. 트로이 목마를 통한 정보수집, 웜이나 바이러스를 이용하여 호스트파일을 변경하고 전송 경로를 재설정하여 사이트 접속시 피싱사이트로 접속되도록 유도하는 방법, 키로거 등의 스파이웨어를 통하여 ID와 패스워드를 수집하는 방법 등으로 발전하고 있다. 향후에도 기존의 사회공학적기법과 악성코드를 이용하는 침투기법이 합세한 3세대 피싱 공격이 새롭게 출현할 것으로 전망된다.

3. 결 론

본 논문에는 최근 이슈가 되었던 사이버위협들을 분석하고, 향후의 사이버위협 전망에 대하여 기술하였다. 물론 본 논문에서 언급하지 못한 최근 사이버위협 이슈들도 존재하며, 향후 전망에서 언급하지 못한 사항도 있을 수 있다. 이러한 최근 사이버위협 현황을 분석하고, 향후를 전망하는 것만으로도 전력IT의 사이버위협 예측 및 대응활동에 도움이 될 것으로 사료된다. 또한 사이버위협에 대한 트랜드를 살펴볼 수 있는 기회가 본 논문을 통해 제시함으로서 향후 전력IT 개발·적용·활용 등 있어 보안성 확보에 기여했으면 한다. 따라서 국가기관을 주축으로 하는 국가·공공기관의 정보보호 활동이 더욱 중요시될 것으로 전망되며, 빠르게 고도화·지능화되는 사이버위협에 적절히 대응할 수 있도록 정보보호기술에 대한 연구개발에도 박차를 가해야 할 것이다.

[참 고 문 헌]

[1] 서울신문
[2] 국가사이버안전센터 사이버시규리티
[3] 월별 사이버침해동향 정보보호대응반, 한국정보보호진흥원(KISA)