차세대 사이버 보안 이슈와 위협 및 대처방안


김 경 신
청강문화산업대학교


강 문 식
강릉원주대학교

Ⅰ. 서 론

오늘날 현대인들은 인터넷으로 대표되는 컴퓨터 네트워크 기술의 눈부신 발전으로 과거 그 어느 시대에서도 경험할 수 없었던 새롭고 편리하며 경이로운 세계 속에서 생활하고 있다. 세계 어느 곳에서나 스마트폰이나 인터넷을 통해 교통·숙박 시설 및 항공권 등을 예약하는 것은 물론, 첨단의료 정보시스템을 이용한 원격진단 및 진료가 가능해졌고, 더욱 신속하고 정확한 기상예보와 재해예보, 첨단 디지털 영상문화 서비스, 주문형 비디오서비스(VOD)가 일상화되었다. 마치 물, 공기, 전기처럼, 인터넷은 우리생활과 불가분의 관계가 되었다. 그러나 이것과 함께 컴퓨터 바이러스에 의한 공격과 같은 사이버 보안 문제 또한 그 어느 때보다 심각하게 대두되고 있다. 컴퓨터 바이러스란 컴퓨터 프로그램이나 운영제제의 실행 가능한 부분을 변형하고 여기에 자기 자신 또는 그 무엇이가를 복사하여 정상적인 프로그램이나 다른 데이터 파일 등을 파괴하는 등 의 컴퓨터 작동에 피해를 주는 악성 프로그램을 말한다.

컴퓨터 바이러스의 정확한 유래를 찾기란 쉽지 않다. 다만, 1970년대 초부터 바이러스라는 개념이 사용되기 시작했고 '크리퍼 (The Creeper)' 바이러스가 최초로 보고된 것도 바로 이때였다. 이후 발견된 여러 바이러스 중 유명세를 탄 바이러스중 하나는 브레인 바이러스로, 이것은 1986년 파키스탄 출신의 앰자드 알비와 배시트 알비 형제가 불법 복제 사용자들에게 낭패를 안겨 주려는 목적으로 전세계적으로 전파시켰던 바이러스로 알려진다.

브레인 바이러스를 시작으로 이보다 더욱 악성적인 바이러스들이 줄지어 출현하기 시작했다. 예루살렘 바이러스,가 1986년에 발견되었고, LBC 바이러스, 체르노빌 바이러스와 슬래머 바이러스 등은

PC 사용자들을 공포에 빠뜨렸다. 일반 사용자들은 앞다투어 컴퓨터 백신 프로그램의 최신 경신(update) 발표를 기다렸다가 이것을 설치해야만 했다. 그러나 어느 시점에서부터 악의적 해커들은 일반 사용자의 개인용 PC보다는 은행, 언론, 정부의 컴퓨터(서버)를 노렸고 악성코드와 APT 그리고 디도스를 이용하여 그들이 가진 그 무엇인가를 빼어가거나 혹은 무력화시켰다. 아마도 그 이유는 개인용 PC보다 더 큰 이득을 얻을 수 있기 때문일 것이다. 일반 사용자의 PC가 해커들의 공격 대상에서 멀어졌다는 분위기에 따라 사용자들은 바이러스 백신의 경신에 관심이 소홀해진 듯하다. 그러나 올해 2014년부터는 상황이 달라질 것으로 예상된다. 악의적 해커들이 그들의 타깃을 공공기관의 대형 서버에서 일반인의 컴퓨터로로 눈을 돌리기 시작했기 때문이다. 바로 비트코인으로 알려진 인터넷 화폐의 등장이 결정적인 계기가 되었다. 또한 유비쿼터스시대의 새로운 대안으로 꼽히는 사물인터넷과 클라우드 시스템도 보다 많은 사이버 공격을 받을 것으로 예상된다.

비트코인은 거래의 익명성이 보장되고 별다른 규제가 적용되지 않아 자금 세탁, 탈세, 마약 및 무기 밀매 등 불법적인 거래에 활용될 수도

본고에서는 이러한 2014년의 주요 사이버 보안 이슈인 비트코인과 랜섬웨어의 위협 그리고 사물 인터넷, 모바일, 클라우드 등 첨단 컴퓨팅 기술을 대상으로 하는 차세대 사이버보안 이슈와 최신 기술의 동향 및 대안을 살펴보고자 한다.

Ⅱ. 비트코인과 랜섬웨어

1. 비트코인

비트코인이란, 단어 그대로 디지털 단위인 '비트(bit)'와 '동전(coin)'을 합친 가상 화폐를 말하는데, 2009년 사토시로 불리우는 익명의 프로그래머 혹은 단체가 기존 화폐 시스템의 대안으로 개발한 것으로 알려져 있다. 비트코인은 탄생 당시엔 그다지 주목을 받지 못했지만 1 BTC(비트코인)이가 14 달러 가치로 책정된 2013년 초부터 거래가 폭발적으로 늘기 시작하였다. 더욱이 키프로스 금융위기와 유럽연합의 통화위기까지 겹치면서 1 BTC의 가치는 200달러를 돌파했다. 이후 중국을 중심으로 수요가 폭증하게 된 11월 무렵엔 1,000달러를 넘어서기도 했다. 해커들의 주목을 끌만큼 충분한 가치를 지니게 된 것이다.

비트코인은 P2P 네트워크상에서 암호화 알고리즘에 따라 채굴되며, 채굴자들을 포함한 다수의 네트워크 참가자들은 계좌 이체 방법으로 비트코인을 거래한다. 채굴이란 계좌이체 거래 기록들을 이용하여 일종의 수학 문제를 풀어내는 작업을 말하는데, 채굴 성공자에게는 시스템 운영에 기여한 대가로 일정한 비트코인이 새로 발행되어 주어지게 된다. 채굴에 성공하면 채굴과정에서 이용된 거래 기록들이 승인되며, 채굴 성공하기 전까지의 거래는 미확정 상태를 유지하게 된다. 거래 미확정 상태에서 수취자는 계좌이체로 받은 비트코인을 사용할 수 없다. 채굴자들의 성공보수 (현재 25 BTC)가 약 4년 마다 반으로 줄어들도록 설계되어 있어서 총 발행량은 2100만 BTC로 제한된다.

그렇다면 나름 건전하게 보이는 이 비트코인의 문제점은 무엇일까? 비트코인은 거래의 익명성이 보장되고 별다른 규제가 적용되지 않기 때문에 자금 세탁, 탈세, 마약 및 무기 밀매 등 불법적인 거래에 활용될 수 있다. 일례로 마약 및 무기 밀거래 사이트인 실크로드는 지급수단으로 비트코인 만을 허용하는 것으로 알려져 있다. 또한 비트코인이 환차익을 위한 투기수단으로 이용될 수 있다는 이유로 각국 정부는 규제를 하고 있는데, Q 머니라는 인터넷 화폐가 비교적 활성화되고 있

〈그림 1〉 비트코인

는 중국에서조차 비트코인의 투기성과 가격변동성이 높은 점을 들어 업무취급을 금지시키고 있다. 또한 각 개인이 보유한 비트코인을 목표로 하는 랜섬웨어의 등장을 촉발시킨 점도 유의해야 할 것이다. 또 다른 문제점은 비트코인을 담는 전자지갑에 있다. 전자지갑은 컴퓨터나 USB에 저장하여 사용하는데, 이 전자지갑 전체를 그대로 해킹 당할 수가 있기 때문이다. 비트코인 블록을 캘 때 마다 암호가 복잡해져 보안성이 높아지는 것과는 달리 막상 비트코인을 담아놓는 전자지갑은 상대적으로 보안이 취약하다. 이런 이유로 전자지갑을 훔치는 해커들에 의한 피해규모는 수백원에서 1000억원 정도에 이르고 있다. 그럼에도 아직 전자지갑을 오프라인 저장장치에 보관해야 한다는 캠페인 정도의 대책에서 그치고 있는 실정이다.

2. 랜섬웨어

비트코인을 얻는 방법은 몇 가지가 있는데, 가장 손쉬운 방법은 비트코인 환전소에서 다른 사람의 비트코인을 구매하는 것이다. 또 다른 방법은 광산에서 금을 캐듯 복잡한 수학문제를 풀어주는 프로그램을 사용하는 방법, 즉 마이닝(Mining) 과정을 사용하여, 암호화 계산 과정을 수행한 후 비트코인을 얻는 방식이다. 후자의 방식을 사용하면 누구나 자신의 컴퓨터를 이용하여 비트코인의 채굴이 가능해진다. 그러나 채굴 과정이 너무 복잡하여 개인용 컴퓨터를 사용하는 것은 현실적으로 어렵다는데 문제가 있다. 해커들은 불법적인 방법으로 다른 사용자의 고성능 컴퓨터를 몰래 사용하거나, 혹은 컴퓨터를 공격하여 비트코인을 탈취하려는 시도를 하게 되었고, 이 과정에 일본의 마운틴 곡스라는 세계 최대의 환전소가 털리는 사태까지 이르게 되었다. 또한 비트코인이 있는 컴퓨터를 고도의 암호화 프로그램으로 감염시킨 다음, 암호를 풀어주겠다고 제안하며 거액을 요구하는 신종 악성 공격들도 출현하였는데, 이것을 랜섬웨어 (RansomeWare)라 부른다. 이러한 공격은 이후로 더 기승을 부릴 것으로 예측된다. 특히 비트코인의 특징 중의 하나인 익명성으로 인해 비실명 거래가 가능하기 때문에 수사기관의 추적이 어렵기 때문에 랜섬웨어를 이용한 공격사례는 지속적으로 증가하고 있는 실정이다. 이미 미국 매사추세츠 주의 어느 기관에서는 랜섬웨어 공격을 받은 후 감염된 문서를 복구하기 위해 비트코인으로 750달러를 지불했다는 보도도 있었다.

보안업체 Trend Micro에 따르면 최근 3개월간 세계적으로 비트코인 악성코드에 감염된 PC가 12,213개에 이르며, 일본과 미국이 가장 높은 비율을 차지하고 있다고 한다. 이제 비트코인의 보유와 상관없이 해커들은 개인용 컴퓨터를 대상으로 랜섬웨어 공격을 실시할 것으로 예상된다. 감염시킨 PC를 볼모로 하여 익명성을 지닌 인터넷 화폐를 요구할 것으로 보인다.

대표적인 랜섬웨어로 크립토로커(Crypto Locker)와 프리즌로커(Prison Locker)를 들 수 있다. 맥아피 연구소는 크립토로커같은 매우 널리 퍼진 툴을 사용한 랜섬웨어 공격이 급증할 것으로 보고 있으며, 기업체들을 상대로 핵심 데이터를 암호화하려는 새로운 형태의 랜섬웨어 공격도 예고하고 있다. 크립토로커 공격자들은 피해자에게 비트코인을 통해 돈을 지불하면(일반적으로 300달러 정도) 데이터 암호를 풀 수 있는 키를 주겠다고 제안한다.

랜섬웨어 피해 사례와 그 대응방법을 알아보자. 2013년 11월 애리조나 주 챈들러에 소재한 W.C. 머신 & 툴에서 누군가가 크립토로커가 첨부된 이메일을 열었다. 그 결과 크립토로커가 맹렬한 기세로 확산되어 윈도우 기반 컴퓨터들을 감염시키고, 가능한 모든 폴더의 파일을 암호화했다. W.C. 머신 & 툴은 즉시 관련 업체에 연락했고, 확인결과 수만 개의 파일이 암호화되어 접근할 수 없다는 것이 판명되었다. 이 무렵 암호화 키를 대가로 돈을 요구하는 메시지가 수신되었지만 아무도 그 요구에 응하지 않았다. 왜냐하면 이 회사는 클라우드 제공업체를 통해 매일 백업을 하고 있었기 때문이었다. 회사는 바로 이 백업을 이용하여 데이터를 복구하는데 성공했다. 크립토로커는 AES 256비트 암호화를 사용해서 공격 대상의 데이터를 변형시키기 때문에 수작업으로 이러한 암호를 풀기란 거의 불가능하다. 이 회사의 경우처럼 데이터를 복구하기 위한 유일한 방법은 백업데이터를 사용하는 것이다.

Ⅲ. 차세대 사이버 공격과 보안 위협

1. 사물인터넷에서의 보안위협

최근 IT분야 융합의 급격한 발전은 다양한 디바이스와 기계간의 연결을 통한 무선네트워크 기술의 발달에 힘입어 유비쿼터스 환경으로 빠르게 진화되고 있다. 이것과 관련하여 사물 인터넷 IoT(Internet of Things) 기술이 매우 새롭고 유망한 분야라고 자주 사람들의 입에 오르내리고 있다. IoT는 사용되는 분야의 다양한 시각이 많기 때문에 명확하고 표준화된 정의를 내리는 것이 쉽지 않다. 유비쿼터스 환경에 대한 연구는 IT분야를 기반으로 한 융합분야의 발전과 함께 많은 새로운 분야의 연구가 이루어지는 계기가 되었다. 특정 산업 분야에서 제한적으로 이용되던 M2M 통신 서비스가 사물인터넷 중심으로 자리매김하고 있으며, 특히 이동통신 사업자들의 새로운 비즈니스 모델로 대두되고 있다. M2M이란 Machine to Machine 또는 Mobile to Machine 또한 Machine to Mobile 통신을 모두 의미한다. 그러므로 M2M (Machine-to-Machine)은 사람과 기기 또는 기기와 기기 간의 통신을 의미하고, 광의적으로는 통신과 IT 기술을 결합해 원격지의 사물, 시스템, 차량, 사람의 상태, 위치정보 등을 확인하고 제어할 수 있는 솔루션으로, 우리의 일상생활 속에 널리 퍼져있는 컴퓨터/기기/장비간의 네트워킹에 관한 개념이라고 볼 수 있다. 현재 M2M 통신 개념은 GSM/CDMA망을 넘어 Wi-Fi/UHF등 다양한 유무선 네트워크를 활용하는 개념으로 확장되어가고 있다. 이를 활용하면 사람과 사물 사이의 상호작용을 통해 위치, 건강, 온도, 습도 등 다양한 데이터를 얻을 수 있게 된다.

IoT 플랫폼 상에서의 보안은 인터넷 상에서의 보안기술 및 모델과 큰 연관성을 갖는다. 전통적인 인터넷 환경과는 달리 IoT 환경에서는 동일한 실행 환경 제공이 쉽지 않으며, 통합된 형태의 보안 플랫폼을 제공하는 것이 어렵게 된다. 이와 더불어 다수의 노드들 간 통신과 노드 클러스터링 문제 또한 IoT 환경에서의 보안 고려 사항으로, 물리적 보안, 정보 획득 보안, 정보 전송 보안, 정보 처리 보안 등을 포함한다. 먼저 물리적 보안의 경우, 악의적인 사용자가 환경 속에 설치된 저가의 태그와 센서에 접근하여 데이터 정보를 파악하거나 불법적인 인가작업을 할 수 없도록 안전한 암호화와 프로토콜이 사용되어야 한다. 정보 접근 및 획득에 대한 보안에서는 이기종의 기기들 간의 다중 미디어 스위칭 기술과 위치관리 기술로 인해 발생하는 다중 정보 접근에 대한 보안 취약성을 제거하여야 한다. 또한, 무선통신에서 사용되는 무선 인터페이스의 공개성으로 인해 전송되는 메시지가 캡처되어 변조될 위험성도 있다. 이러한 문제점은 일반적인 무선 네트워크 환경에서 발생하는 문제와 동일하며, IoT와 같은 많은 수의 노드들이 통신하는 경우에는 DoS공격을 통해 네트워크를 마비시킬 수 있으므로 이에 대한 보안 요구사항이 구비되어야 한다. 특히 IoT의 응용 계층에서는 다양한 앱과 플랫폼간의 정보처리과정에서 발생할 수 있는 정보의 손실이나 해킹에 관한 대비가 필요하다.

> **스마트폰 사용자들을 겨냥한 앱으로 위장한 악성 멜웨어의 증가와 스미싱을 이용한 안전결제 해킹공격으로 인한 피해사례가 점점 증가**

2. 모바일을 대상으로 한 사이버 공격

스마트폰의 급격한 보급과 함께 컴퓨터 해킹뿐만 아니라, 스마트폰 해킹으로 인한 피해 사례가 점차 늘어나고 있다. 2013년 시장조사업체 IDC가 발표한 자료에 따르면 전 세계 PC 출하량이 지난해보다 눈에 띌 정도로 줄어들었다고 한다. 이것은 스마트폰과 태블릿 보급이 확산되면서 일반 사용자들이 PC보다 스마트폰을 더 많이 사용하기 시작했다는 것을 알려주는 신호로, PC 전성시대를 지나 스마트폰 전성시대가 오고 있음을 암시한다. 이와 같이 급증하는 스마트폰 사용자들을 겨냥한 앱으로 위장한 악성 멜웨어의 증가와 스미싱을 이용한 안전결제 해킹공격으로 인한 피해사례가 점점 증가하고 있다. 미국의 모바일 시장조사 그룹인 Trend Micro Trend Lab의 위협보고서에 따르면

2013년 1분기 50만여 건이었던 고 위험군의 악성 안드로이드 앱의 수가 2분기에는 71만건으로 증가하였다고 한다. 이런 앱의 증가 속도를 살펴보면, 종전에는 35만건에 도달하기까지 약 3년이 소요되었지만 최근에는 단 6개월로 단축되었다. 멀웨어의 대부분은 인기 앱의 트로이목마 버전 혹은 모방 버전으로 포장되어 있다. 특히 모바일 멀웨어의 절반 정도는 사용자 자신도 모르는 사이에 고가의 서비스에 가입하도록 설계되어 있으며, 더욱이 안드로이드 기기가 사이버 공격에 취약한 것으로 알려짐에 따라 우려가 점점 커지고 있다. 안드로이드 마스터 키가 갖는 취약점은 사용자의 동의 없이 기기에 설치된 앱을 변경할 수 있도록 허용하기 때문에 안드로이드 에코시스템의 단편화 문제와 함께 기기 보호를 위해 전적으로 검사 앱에 의존하는 현 방식에 대한 우려가 증폭되고 있는 실정이다.

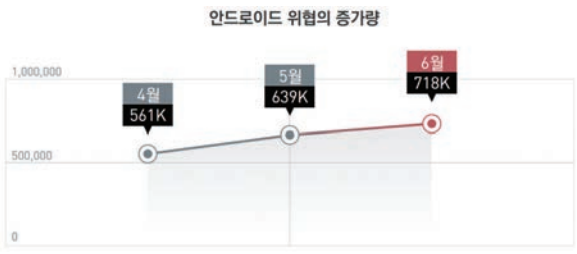
스미싱은 단문자서비스 (Short Message Service)와 피싱(Phishing)의 합성어로, 스마트폰을 이용하여 피싱 사기를 유도하고 개인정보를 빼내거나, 사용자 몰래소액 결제를 유도하는 신종 휴대폰 사기 수법이다. 스미싱 악성코드는 2013년에 들어서 급속하게 사회 문제로 등장하였으며, 2014년 올해에는 모바일 악성코드를 활용해 특정 대상을 감시하거나 정보를 유출하는 소규모 모바일 악성코드가 출현할 가능성이 농후하다. 스미싱 악성코드는 대량 유포를 목적으로 했기 때문에 비교적 발견을 신속하게 할 수 있었다. 하지만 만일 악성코드 제작자가 코드를 불특정 다수에 유포하지 않고, 특정 기업의 내부 기밀 유출이나 감시를 목적으로 하여 소량만 유포한다면 그 발견이 결코 녹녹한 일이 아니다. 이런 취약점을 노린 '다품종 소량' 스파이 앱이 등장할 가능성 또한 크다고 하겠다.

모바일 악성코드를 활용해 특정 대상을 감시하거나 정보를 유출하는 소규모 모바일 악성코드가 출현할 가능성이 농후

3. 클라우드를 대상으로 한 사이버 공격

클라우드 서비스는 2010년 상반기를 기점으로 한 스마트폰 열풍과 더불어 웹하드 방식의 클라우드 서비스가 일반 대중들에게 소개되면서 널리 알려지기 시작하였다. 사실 웹 하드 형식의 자료를 저장하는 기능만 제공하는 서비스는 클라우드 서비스의 일부분에 지나지 않는다. 클라우드 서비스 구조에 대해 먼저 살펴보고, 각 클라우드 서비스별 보안 요구사항을 알아본다. 클라우드 서비스(Cloud Service)를 사용하면 흔히 사용하는 개인용 컴퓨터처럼 하드디스크에 소프트웨어를 설치하여 구동하지 않고도 모든 IT 서비스를 제공이 가능해진다. 즉 우리들의 실생활에서 전기, 물, 가스 등을 우리가 필요로 할 때 사용하는 것처럼 클라우드 서비스는 모든 IT 서비스를 가상공간에 저장해 놓고 필요할 때 가져다 쓰는 형태가 된다.

클라우드 서비스는 신속성, 사용의 편리성, 그리고 관리비용의 감소 등과 같은 속성이 있다. 마치 경영방식에서의 아웃소싱과 같은 속성으로 이해할 수도 있다. 대표적인 클라우드 서비스에는 IaaS, PaaS, SaaS 등이 있는데, 이중 IaaS (Infrastructure as a Service) 서비스 방식은 인프라 부분을 클라우드 서비스 사업자가 제공하는 서비스로, 하드웨어, 네트워크 서버, 저장



〈그림 2〉 안드로이드 위협의 증가량

〈그림 3〉 클라우드 서비스

공간 등을 제공받을 수 있는 방식이다. PaaS (Platform as a Service)는 인프라를 갖추고 O/S 등 표준화된 플랫폼까지 서비스로 제공하는 방식이며, SaaS (Software as a Service)는 사용자는 제공자로부터 서비스를 제공 받고 소비하는 형태의 소프트웨어 서비스를 이용하는 방식이다. 기존 정보시스템과 달리 클라우드 서비스는 서비스 제공자와 사용자간의 물리적인 관리대상이 구분되어 있다. 이는 서비스 사용자의 직접적인 관리권 또한 제약이 있으며, 사용자가 서비스 제공자와 계약 간에 자신의 관리권을 양도한다는 사전적인 약속이 있어야 한다는 것을 의미한다. 만일 사용자가 개인의 정보를 IaaS 서비스를 이용하여 개인정보를 저장하게 된다면, 서비스 제공자는 개인정보에 대한 보안성을 고려해야 한다. 또한 서비스 접근 간 변조(spoofing) 공격을 이용하여 서비스 이용 접근을 방해하고, 악의적인 제 3자가 sniffing기법을 사용하여 서비스 사용자의 서비스 이용 계정정보를 절취하여 이용할 경우 프라이버시 보호에 심각한 문제 가 생긴다. 따라서 서비스 제공자는 DoS공격 등 서비스 거부에 대한 대책은 물론, 인증방법에 대한 대책 등 네트워크에 대한 보안이 필요하게 된다.

클라우드 기반의 애플리케이션은 수많은 유용한 기능과 경제적 잇점을 가지고 있는 반면, 공격자들에게는 새로운 표적으로 주목

클라우드 기반의 어플리케이션은 분명히 수많은 유용한 기능과 경제적 잇점을 가지고 있는 반면, 공격자들에게는 새로운 표적으로 주목 받게 된다. 특히 자원공유, 서비스의 집중화, 가상화 기술의 취약성, 보안 책임 소재의 불명확성 등 취약성 해결이 쉽지 않기 때문이다. 특히 2014년도에는 클라우드 PaaS 서비스를 이용한 비트코인 채굴이 증가하면서 이에 대한 악성코드 공격과 특히 랜섬웨어 공격이 크게 증가할 것이다. 이것을 입증이라도 하듯이 최근 멀웨어 배포의 16%가 아마존 클라우드를 대상으로 삼고 있으며, 14%가 미국의 GoDaddy를 대상으로 했다는 보고가 있다.

4. 딥웹 (Deep Web)

딥웹은 흔히 쓰는 포털 사이트 들과 기본 검색엔진에

〈그림 4〉 토르 브라우저

서 검색되어지는 인터넷의 표면보다 더 깊은 곳에 있는 웹 이라는 뜻이다. 일반 검색엔진으로는 검색이 불가능하고 해당 URL을 입력해도 일반 브라우저로는 접근이 되지 않는다. 따라서 실수로 이 웹 서버에 접속한다기보다는, 호기심 및 특정 정보를 얻기 위해 접속되는 경우가 대부분이다. 당연하겠지만 일반 검색엔진으로 검색되지 않는 문서나 파일, 즉 기밀문서와 마약자료, 성인물 등 특히 불법적 영상물이나 자료가 주로 대상이 된다. 일반 검색엔진으로 검색되는 양의 몇 백배의 자료 검색이 가능하다. 딥웹에 접속하기 위해서는 특별한 브라우저를 설치해야한다. 한 예로 토르 브라우저 (Tor Browser)라는 것이 있다. 이는 파이어폭스를 기반으로 하여 만들어졌고 연구목적과 해킹 목적이 결합된 복합적인 브라우저라고 생각하면 이해가 쉽다. IP추적이나 흔적을 제거하는 기능이 뛰어나고 익

〈그림 5〉 히든 위키 사이트

명을 보장하는 브라우저로 알려지고 있는데 이것도 매우 위험한 위협이라고 볼 수 있다. 토르 브라우저는 접속자의 IP를 철저히 보호하는 것으로 잘 알려져 있어서, 해커들이 나쁜 목적으로 변형시켜 유포하면 이를 사용하는 사용자의 개인정보나 이용 형태 등을 고스란히 빼앗길 위험이 많기 때문이다.

딥웹은 하나의 사이트가 아니라 감추어진 별도의 서버군을 형성하고 있기 때문에 일반적인 검색엔진으로는 찾을 수 없게 되어있다. 딥웹에도 naver.com과 daum.net 등의 URL이 있으며, 일반 사용자들이 딥웹에 들어갈 때 최초로 접속하는 페이지를 홈 또는 히든 위키라고 부른다. 히든 위키는 위키피디아와 유사하지만 숨겨져 있다는 의미를 가지고 있다. '7jguhsfwru-viatqe.onion' 사이트를 크롬이나 익스플로러 브라우저를 사용하여 접속해 보면, 들어갈 수 없는 곳이라는 메시지가 나온다. 그러나 토르 브라우저로 들어간다면 〈그림 5〉처럼 접속된다.

이러한 딥웹의 위험성은 그 내포된 불법성에 있다. 딥웹에는 청부업자 사이트와 해커 사이트, 그리고 마약 판매 사이트가 넘쳐난다. 그만큼 컴퓨터에 대한 전문성을 갖고 있으면서도 불법행위를 하는 사람들이 많다는 의미일 것이다. 또한 영어 등의 외국어로 사이트가 구성되므로 잘못 접근하면 해킹 위협이 커진다. 이때문에 보안 감찰을 하는 요원도 다수 존재하며, 경우에 따라서는 회사의 기밀문서를 저장하는데 딥웹을 사용하는 경우도 있을 수 있다.

5. 제로데이 공격

취약점이 발표되고 이에 대한 패치가 나오기 전까지 발생하는 모든 공격을 제로데이(Zero Day) 공격이라 한다. 이러한 공격의 경우 아직 패치가 적용되지 않은 상태의 수많은 시스템들이 공격의 대상이 되므로 막대한 피해가 예상되며, 해당 공격을 탐지하기 위한 징후도 있지 않아 더욱 위험한 공격이다. 일반적으로 공격 코드는 실행 가능한 코드가 대부분이므로, Zero Day 공격을 탐지하기 위한 악성코드 탐지 기술개발이 절실한 실정이다. 특히 윈도우 XP처럼 지원이 중단된 운영체제를 사용하는 것은 매우 위험한 상황에 처할 수 있다.

올해 4월 8일 마이크로소프트가 윈도우 XP에 대한 서비스 지원을 중단함으로서 국내뿐만 아니라 전 세계에서 지원 중단 이후의 상황에 대한 수많은 경고 메시지가 쏟아지고 있다. 윈도우 XP는 마이크로소프트사에서 판매 실적이 가장 우수했던 윈도우 시리즈에 속한다.

시장조사업체 넷 마켓쉐어 (NetMarketShare)에 따르면 2013년 말 기준으로 전 세계 PC의 31.42%가 윈도우 XP를 운영체제로 이용하고 있다. 특히 전 세계 은행 금전출입기 (ATM)의 40% 이상이 윈도우즈 XP를 사용하고 있다는 보고가 있을 정도이다. 아울러 경신 지원 중단 시점을 기준으로 윈도우 XP의 알려지지 않은 보안 취약점을 공격할 수 있는 멀웨어 보유 해커들의 활동이 개시될 것으로 예상된다. 이들은 사이버 공격을 원하는 사용자들에게 해당 멀웨어 공급을 시작할 것으로 보이며, 이와 같은 멀웨어는 상당한 고가에 판매될 것으로 보인다. 따라서 대량 감염 보다는 부가가치가 높은 기업 정보나 특정 개인 공격을 목적으로 사용될 것이라고 예상된다.

소프트웨어 측면에서의 위험성도 많다. 마이크로소프트(MS)의 웹브라우저인 인터넷 익스플로러(IE)가 보안에 취약하다는 점이 알려지면서 우리 정부도 다른 웹브라우저 이용을 권고하고 나섰다. 19일 한국인터넷진흥원(KISA)은 인터넷침해 대응센터 홈페이지에 "MS IE에서 원격코드 실행이 가능한 신규 취약점이 발견됐다"며, "해당 취약점에 대한 보안 업데이트는 아직 발표되지 않았지만, 취약점을 악용한 공격 시도가 (해외에서) 확인되어, (IE) 사용자의 주의가 특히 요구된다"고 공지했다. 이번 취약점에 영향을 받는 소프트웨어는 IE11을 제외한 IE6, IE7, IE8, IE9, IE10 등 현재 사용하고 있는 거의 모든 IE 버전에 해당한다. 공격자들은 이번 IE 보안 취약점을 이용해 악성코드를 제작해서 이에 감염된 PC를 원격으로 마음대로 조정하려 한다.

웹 브라우저 통계기관인 미국의 StatCounter의 2013년 7월 자료에 의하면 전 세계 웹 브라우저 사용 1위는 크롬(43.12%), 2위는 인터넷 익스플로러(24.53%), 3위는 20.09%의 파이어 폭스라고 한다.

2013년 7월과 2011년 9월의 점유율을 비교한 것으로, 불과 1년여 만에 크롬이 웹 브라우저 점유율 1위에 올라섰음을 보여준다. 그러나 국내의 웹 브라우저 사용률은 여전히 인터넷 익스플로러(68.57%)가 1위이며, 2위인 크롬(21.59%)과 큰 격차를 보이고 있다. 그러나 2011년 9월에 90%를 넘던 점유율에 비하면 인터넷 익스플로러의 점유율이 큰 폭으로 떨어진 것이다.

Ⅳ. 결론 및 향후 전망

2014년도 보안관련 이슈중 하나가 BYOD의 금지에 관련된 사항이다. BYOD (Bring Your Own Device)는 개인용 노트북이나 스마트폰과 같은 단말기를 지참하여 가정과 직장에서 동시에 사용하는 것을 말한다. 업무적으로도 높은 성능을 보이고 있어서 기업이나 기관의 비율이 매우 높은 상태이고, 이는 세계적인 추세로 보인다 . 그러나 2011년 4월 농협 사태에서 보듯이 개인이 외부에서 사용하던 단말기를 업무에 활용하는 것은 매우 치명적인 위험성을 내포하고 있다. BYOD가 보안에 있어서 중요한 이유는 개인 단말기의 보안수준이 기업이나 기관에서 요구되는 업무용 보안수준에 미치지 못할 가능성이 높기 때문이다. 따라서 2014년 올해에는 BYOD를 엄격히 금하는 업체가 증가할 것으로 예상되며, 특히 전산 인프라와 보안 관련 업무 종사자는 가장 먼저 적용될 것으로 보인다.

또 다른 이슈는 각종 인증방법의 다양화이다. 사용자를 인증하는 가장 일반적이면서 흔히 사용하는 방식은 비밀번호(password) 방식일 것이다. 그 이외에도 지문, 홍채, 그리고 정맥패턴, 음성 등의 다양한 방식이 이용되고 있지만 향후에는 심전도 인증방식도 등장할 것으로 보인다. 팔찌 형태로 되어 있는 심전도 인증방식 보안장비는 지문처럼 사람마다 심장의 박동패턴이 구분된다는 점에서 출발했다. 즉, 각 개개인의 심장 박동이 다르기에 그 심전도를 분석해서 차이를 명확히 구분할 수 있다면, 심장 박동을 비밀번호처럼 사용할 수 있게 된다. 심전도 인증방식 도입으로 주 전산소의 출입인증이나 시스템 관리가 간편하게 이루어 질 수 있을 것으로 조심스럽게 예상해 본다.

지금까지 몇 가지 주요 보안위협과 최신 보안 이슈에 관하여 살펴보았다. 먼저 2014년 최신 보안기술 동향으로 비트코인과 랜섬웨어에 관하여 알아보았다. IT계의 핫이슈인 인터넷 화폐의 등장과 그것으로 인해 다시 블랙 해커들의 목표가 개인용 PC로 회귀하고 있다는 점, 그리고 이러한 불법 공격의 방법으로 사용자의 데이터를 볼모로 한 공격방식, 즉 랜섬웨어의 출현이 예상된다. 향후 치열한 경쟁이 예상되는 사물인터넷(IoT)과 클라우드(Cloud) 그리고 모바일 기기를 대상으로 하는 보안위협이 날로 증가할 것이다. 사물인터넷을 이용한 데이터 통신이 늘어나고, PaaS와 같은 가상화 컴퓨터를 사용하는 호스트의 이용과, 주요 통신수단으로 스마프폰을 사용하는 현대인의 생활패턴을 파고 드는 보안위협이 확대될 것이다.

향후 치열한 경쟁이 예상되는 사물인터넷(IoT)과 클라우드(Cloud) 그리고 모바일 기기를 대상으로 하는 보안위협이 더욱 증가할 것

또 다른 보안위협으로 딥웹과 제로데이 공격이 있다. 일반적인 검색엔진은 사용할 수 없고, 반드시 특정 브라우저를 이용하여 검색해야 하는 딥웹은 그 폐쇄성과 불법적 정보로 접근성으로 인해 그 위험성이 날로 증가하고 있다. 특히 시스템 공격용 멜웨어는 마약과 같은 반사회적 요소를 포함하고 있기 때문에 각별한 주의를 필요로 한다. 그리고 BYOD의 위험성으로 인한 컴퓨터 단말기의 회사내 사용제한 예측과 보다 더 간편하고 정확한 심장박동 패턴을 이용한 심전도 인증시스템의 등장 등도 주목할 내용이다. 오늘날 정보화 사회는 컴퓨터와 인터넷에 의존적인 비중이 더욱 가속화 되고 있다. 각종 보안 위협으로부터 안전하게 대처하기 위해 서 보다 적극적인 방어 방식에 대한 분명한 인식과 함께 차세대 보안 기술에 대한 연구개발과 이에 대한 적극적인 관심이 그 어느 때보다 절실하게 필요한 시점이다.

참 고 문 헌

[1] 최영준, 허경미, 김진화, 수학동아, pp. 42-49, 동아사이언스, 2013. 12.

[2] 김원호, Bit Coin 디지털 화폐혁명, 한국마케팅연구원, 2014. 01.

[3] 이동규, 비트코인의 현황 및 시사점, 한국은행, 2013.

[4] 이근호, M2M기술 및 보안동향, 인터넷 정보학회지 13(1) pp. 21-29, 한국인터넷정보학회, 2012. 03.

[5] 김락철, 공정현, 김건, 이형효, 클라우드 서비스 보안 요구사항, 한국정보기술학회 논문집 pp. 430-434, 한국정보기술학회, 2012. 05.

[6] 서화정, 이동건, 최종석, 김호원, IoT 보안 기술 동향, 전자파기술 24(4) pp. 27-35, 한국전자파학회, 2013. 07.

[7] 박인우, 박대우, 스마트폰에서 Smishing 해킹공격과 침해사고 보안연구, 정보통신학회논문지 17(11) pp. 2588-2594, 한국정보통신학회, 2013. 11.

[8] http://chdlseoghk2.blog.me/40170094384. Parallel World, 2013. (Deep Web 기술자료)

[9] 이대영, 서비스지원중단을 앞둔 윈도우 XP에 대한 점 검과 대책, http://www.itworld.co.kr/news/86623, IT World, IDG.

[10] 김경신, New인터넷 이해와 활용, 한빛미디어, 2014. 01.

[11] 오진태, 장종수, 류재철, 제로데이 어택 방지를 위한 실시간 대응기술, 인터넷 정보학회지 9(3), pp. 25-31, 한국인터넷정보학회, 2008. 09.

[12] 라디오키즈, 키즈@IT/Online/HW 이슈&리뷰, 2013. 09.

김 경 신

1986년 2월 금오공과대학교 졸업(공학사)
1993년 2월 연세대학교 대학원 졸업(공학석사)
2007년 8월 경희대학교 대학원 졸업(공학박사)
1986년 3월~1991년 2월 중앙경리단전산소 프로그래머, DBA
1993년 3월~1997년 1월 육군전산소 프로그래머, 제도분석관
1999년 1월~2000년 2월 창원 종합정비창 전산과장
2000년 3월~현재 청강문화산업대학교 모바일 보안 전공 교수

〈관심분야〉
정보보호, 사이버보안, 서버기술, 인터네트워킹, 센서네트워크, IoT(m2m)

강 문 식

1985년 2월 연세대학교 전자공학과(공학사)
1988년 2월 연세대학교대학원 전자공학과(공학석사)
1993년 2월 연세대학교대학원 전자공학과(Ph.D)
1996년~1997년 Post-Doc at Dept of EE, University of Pennsylvania
2003년~2004년 Research Associate at IIT, Dept. of ECE,
2007년~2008년 정보통신부 정보통신국가표준 전문위원
2008년~2012년 국방과학연구소 민군겸용기술사업 총괄분과위원
2011년 1월~현재 대한전자공학회 이사
1993년 3월~현재 강릉원주대학교 전자공학과 교수

〈관심분야〉
초고속융합네트워크 구조 및 최적화, 무선네트워크에서의 QoS 트래픽 제어기법, 이동멀티미디어 트래픽 모델링 및 응용