통일문제연구원
『통일문제연구』 제2권 제1호
2019. 12. pp.31-43

논문접수일 : 2019년 12월 15일
게재확정일 : 2019년 12월 23일

북한의 해킹 사례와 대응 방안

이재길
강릉원주대학교

<요약문>

북한은 지난 수십 년 동안의 경제적 어려움으로 인해 재래식 무기 분야에서는 남한과의 무기 경쟁에서 크게 뒤지게 되었다. 핵무기와 미사일 개발은 이에 대한 열세를 만회하기 위한 보완책으로 보인다. 이런 한계를 극복하기 위한 또 다른 대안으로 북한은 IT 기술에 투자해 왔으며, 초기 하드웨어 중심의 개발에서 현재 소프트웨어 중심의 개발로 바뀌고 있는 추세이며 특히 저렴한 비용으로 막대한 피해를 끼칠 수 있는 사이버 전쟁을 위한 다양한 소프트웨어 기술 개발에 집중하고 있다. 이처럼 최근 들어 사이버 테러와 사이버 전쟁 등에 대한 관심이 집중되고 있지만, 남한에서는 사이버 보안에 관한 경각심이 부족하여 이에 대한 이해와 대책이 절실한 실정이다. 이에 본 논문에서는 지금까지 알려진 다양한 해킹 기법들에 대해 소개하고, 이 중에서 북한에서 사용한 다양한 해킹 기법들과 피해 사례들을 소개한 후, 북한의 해킹에 대한 우리의 대응 전략을 소개하여 북한의 사이버 테러 또는 사이버 전쟁에 효과적으로 대응할 수 있는 방안을 제시하였다.

◆ 주제어 : 사이버 전쟁, 보안, 해킹, IT 기술

Ⅰ. 서 론

최근 들어 인터넷 기술이 발전함에 따라 인터넷을 활용한 다양한 혜택을 보고 있지만 이와 더불어 해킹으로 인한 피해 또한 심각하게 증가되는 추세이다. 올해 업비트 업체의 경우 암호화폐 거래소 해킹을 통해 580억 상당의 피해 금액이 발생했으며(「조선일보」, 2019/8/24), 악성코드 침투가 매일 수백만 건 정도로 급증하고 있다. 한국인터넷진흥원(KISA)에 따르면 2017년 국내에서 하루 동안 발생하는 악성코드 활동의 평균 횟수는 약 2만3883건, 디도스(DDoS)공격은 1.25건으로 파악됐다. 실제 피해로 이어지는 홈페이지 변조는 5건, 랜섬웨어 피해는 16건, 피싱·파밍 사이트 생성은 35건, 홈페이지 악성코드 유포는 37건으로 집계됐다. 1년에 약 7억 건에 달하는 악성코드 활동이 벌어지고 있는 셈이다(『Tech M』, 2018년 10월호).

이와 함께 북한의 사이버 공격과 해킹에 의한 피해가 나날이 증가하고 있고 이에 따른 대비책이 절실히 요구되고 있다. 전문가들은 북한 사이버 공격은 2004년경에 처음으로 인식되기 시작되었다고 본다. 그러나 사이버 범죄에 대한 본격적인 관심은 2009년 북한의 DDoS 공격을 계기로 증폭되었다. 2009년 DDoS 이전의 대부분의 사이버 공격은 기본적인 기술을 사용하는 전자 메일을 해킹하는 방법이 주종을 이루고 있었다. 2009년 DDoS 공격 후, 북한은 한국에 대한 사이버 공격이 더욱 빈번해졌고, 공격에 의한 피해는 더 심해지고 있는 실정이다. 전문가들은 북한 사이버 공격을 비대칭 전략의 구현으로 본다. 실제로 사이버 위협은 비대칭 위협과 동의어가 되었다. 북한은 수십 년 동안의 경제적 어려움으로 인해 재래식 무기 분야에서 한국과의 무기 경쟁을 포기하는 대신 핵무기 개발과 정교한 사이버 무기 개발로 열등성을 상쇄하려고 시도하고 있다. 북한은 1980 년대 중반부터 전문 해커를 훈련시켜 사이버 공격 능력을 향상시켰다. 뉴스 보도에 따르면 북한은 사이버 전사 교육을 목적으로 미림 대학, 모란봉 대학 및 기타 고등 교육 기관을 설립했다. 이 학교는 북한 인민군과 밀접한 관련이 있으며 매년 수백 명의 전문 해커를 교육하고 있다. 그들은 최고 수준의 해커로 추정되며 졸업 후 해킹 부대의 군사 공무원으로 임명하고 있는 실정이다.

이에 본 논문에서는 현재 지금까지 알려진 해킹 기법과 형태를 조사하고, 그 중에서 북한이 주로 사용하고 있는 해킹 기법과 공격 방법을 사례를 통해 연구하여 북한의 해킹 공격에 효과적으로 대비하는 방법을 소개하여 북한의 해킹에 의한 피해를 최소화할 수 있는 방안을 제시하였다.

Ⅱ. 잘 알려진 해킹 기술 현황

북한의 해킹 기법과 전략을 연구하기 전에 먼저 이 장에서는 현재까지 잘 알려진 다양한 해킹 기법 또는 인터넷을 통한 공격 기법들에 대해 설명한다. 현재까지 알려진 수 많은 해킹 기법과 기술들이 있지만 주로 사용되는 해킹 기법들은 다음과 같다.

■ DDOS 공격

디도스(Ddos)란 'Distributed Denial of Service'의 약자로 많은 '좀비PC'를 만든 후 분산 배치하여 한꺼번에 동작시켜 어떠한 특정 사이트를 공격하는 해킹 방식이다. 사용자의 특정 인터넷 사이트가 소화할 수 없는 규모의 접속 통신량(트래픽)을 한꺼번에 일으켜 서비스 체계를 마비시키는 특징을 가진다. 좀비PC'란 공격자가 명령을 하달하기 위해 악성코드로 감염을 시킨 컴퓨터로, 공격자에 의해 제어가 가능한 PC를 의미한다.

■ MBR 파괴 공격

MBR은 Master Boot Record의 약어로 하드디스크의 특정 영역이다. 이 영역은 시작 부분에 위치하기 때문에 이 영역이 파괴되면 뒤에 순차적으로 실행될 명령들이 무시되고 데이터를 읽지 못하게 되어 pc의 부팅이 불가능해진다. MBR이 감염되면 메모리 검사 시 모드 0값으로 초기화되어 있는 것을 확인할 수 있다. 더 발전된 공격의 경우, 0으로 초기화 시킬 뿐만 아니라 MBR영역에 자신만의 코드를 삽입하여 부팅 시 마다 코드가 실행되게 할 수 있다.

■ 크로스 사이트 스크립팅(XSS) 공격

공격자는 XSS 취약점이 존재하는 웹사이트에 자신이 만든 악의적인 스크립트를 업로드하고, 이것을 일반 사용자의 컴퓨터에 전달하여 실행시킬 수 있다. 이러한 공격으로 사용자 쿠키를 훔쳐서 해당 사용자 권한으로 로그인하거나 브라우저를 제어한다. XSS 취약점은 다음과 같이 동적으로 웹페이지를 생성하는 사이트에 주로 존재한다.

- 입력한 검색어를 다시 보여주는 검색엔진
- 입력한 스트링을 함께 보여주는 에러 페이지
- 입력한 값을 사용자에게 다시 돌려주는 폼
- 사용자에게 메시지 포스팅이 허용된 웹보드

■ 이메일 위조

이는 'CEO 사칭' 등으로 일컬어지는 사이버공격 수법이다. 사이버범죄자들은 회사 대표의 이메일 주소를 위조해 의심하지 않을 법한 직원에게 그럴싸한 요청을 한다.

■ 랜섬웨어

랜섬웨어는 몸값(ransom)과 소프트웨어(software)의 합성어이다. 사용자 컴퓨터 시스템을 잠그거나 데이터를 암호화해서 사용할 수 없도록 만든 다음 사용하고 싶다면 돈을 내라고 요구하는 악성 프로그램이다. 랜섬웨어를 만들어 불법적인 경로로 돈을 벌려는 해커들의 근거지는 주로 해외에 있기 때문에 정체가 드러나지 않으며, 피해를 당했더라도 범인을 잡는 것이 사실상 불가능하다. 피해 사례를 보면 2017년 5월에는 전 세계가 워너크라이, 페트야 등의 랜섬웨어로 공포에 떨어야 했다. 전 세계에 있는 기업, 공공기관의 컴퓨터가 랜섬웨어 피해를 입었다. 국내의 한 영화관 운영 기업의 경우, 랜섬웨어 피해를 입어 한동안 자동 발권기를 사용하지 못하는가 하면, 영사기 시스템이 고장나 영화관 운영 자체가 불가능한 상황이 일어나기도 했다. 랜섬웨어의 일종으로 워너크라이[WannaCry]가 있다. 이는 사용자의 중요 파일을 암호화한 뒤 이를 푸는 대가로 금전을 요구하는 랜섬웨어의 일종이다. 워너크라이는 마이크로소프트(MS) 윈도 운영체제의 취약점을 파고들어 중요 파일을 암호화한 뒤 파일을 복구하는 조건으로 300~600달러(한화 34만~68만원)에 해당하는 비트코인(가상화폐)을 요구하고 있다.

피해사례를 보면 2017년 5월 12일부터 대규모 사이버 공격을 통해 널리 배포된지 하루 만에 전세계 100여 개 국에서 컴퓨터 12만대 이상을 감염시켰으며 15일까지 전세계 150개 국에서 30만대의 기기를 감염시켜 병원, 기업, 정부기관 등의 업무가 마비되거나 차질을 빚고 있는 등 사상최대 등 사상최대의 피해를 낳고 있다.

러시아에서는 내무부 컴퓨터 약 1천 대가 감염된 것으로 파악됐고 영국에서는 국민보건서비스(NHS·한국의 건강보험공단과 유사한 조직) 산하 40여 개 병원이 환자 기록 파일을 열지 못하는 등 진료에 차질을 빚거나 예약을 취소했으며 중국에서는 일부 중학교와 대학교가 공격을 당했다. 체코 보안회사인 아베스트(Avast)에 따르면 워너크라이 공격으로 가장 큰 피해를 입은 국가들은 러시아, 대만, 우크라이나, 인도다.

■ 디렉터리 탐색

디렉터리 탐색(Directory Traversal)은 웹브라우저에서 확인 가능한 경로의 상위로 올라가서 특정 시스템 파일을 다운로드하는 공격 방법이다. 자료실에 올라간 파일을 다운로드할 때 전용 다운로드 프로그램이 파일을 가져오는데, 이때 파일 이름을 필터링하지 않아서 생기는 취약점이다. 특정 파일을 다운로드할 때 공격자는 파일명(filename) 변수에 해당하는 값을 간단한 조작을 통해 상위 디렉터리로 거슬러 올라가 /etc/passwd 파일을 다운로드할 수 있다.

■ 인증 우회

인증 우회란 관리자 페이지나 인증이 필요한 페이지의 인증을 처리하지 않고 인증을 우회하여 접속할 수 있는 취약점을 이용한다. 이 취약점에 노출되면 일반 사용자나 로그인하지 않은 사용자가 관리자 페이지에 접근하여 관리자 권한을 획득한 뒤에 모든 기능을 자신이 원하는 대로 악용할 수 있게 된다.

■ 디렉터리 리스팅

디렉터리 리스팅(Directory Listing)은 웹브라우저에서 웹서버의 특정 디렉터리를 열면 그 디렉터리에 있는 모든 파일과 디렉터리 목록이 나열되는 것을 말한다. 이것이 디렉터리 리스팅의 취약점이다. 물론 관리자가 어떤 목적을 위해서 웹서버의 특정 디렉터리를 리스팅할 수 있도록 설정하기도 하지만, 어쨌든 공격자는 디렉터리 리스팅 취약점을 이용하여 웹서버에 어떤 파일이 있는지 확인할 수 있고, 추가적인 공격 취약점을 찾을 수 있게 된다.

■ 사전 공격

암호화되어 저장된 비밀번호를 알아내기 위한 공격방법 중 하나이다. 보통 널리 사용되는 단어나 날짜, 전화번호 등의 패턴들을 사전형태로 만들고 이들을 조합하는 방식으로 공격하는데, 의외로 적중할 확률일 높다고 한다! 사람들이 자신의 생일이나 전화번호, 이름 이니셜 등의 특정한 패턴을 사용하는 경향이 있기 때문이다.

■ SQL 인젝션 공격

웹 애플리케이션에서 사용자에게서 SQL문을 입력받는 부분, 즉 데이터베이스와 연동되는 부분은 크게 로그인, 검색, 게시판으로 나눌 수 있다. 어느 사이트에서든 로그인을 하려면 아이디와 비밀번호를 넣어야 한다. 그리고 웹 애플리케이션 개발자는 정상적인 아이디와 비밀번호를 넣을 것을 기대하고 프로그래밍 한다. 그러나 모든 공격은 언제나 예상치 않은 곳에서

일어난다. 공격자는 아이디와 비밀번호를 정상적인 문자가 아닌 특정 SQL문을 넣어 공격한다. 이렇게 아이디나 비밀번호 부분에 엉뚱한 SQL문이 삽입되면 그것이 그대로 데이터베이스에 전송되어 공격자가 원하는 일이 일어나게 된다.

■ 파일 업로드

파일 업로드(File Upload) 공격은 공격자가 공격 프로그램을 해당 시스템에 업로드하여 공격하는 방법을 말한다. 파일 업로드는 공격이 쉬우면서도 영향력이나 파급 효과는 큰 공격 방법이다. 공격 방식은 공격자가 시스템 내부 명령을 실행할 수 있는 웹 프로그램(ASP, JSP, PHP)을 제작하여 자료실과 같이 파일을 업로드할 수 있는 곳에 공격용 프로그램을 업로드하는 것이다. 그리고 웹브라우저를 이용해 공격용 프로그램에 접근하면 시스템 내부명령을 실행시킬 수 있게 되는데, 이를 이용해 공격자는 리버스 텔넷(Reverse Telnet)과 같은 기법으로 자신의 컴퓨터로 피해 대상 시스템의 명령창을 띄워 편하게 작업할 수도 있다. 쉽게 말해 원격지에서 공격한 컴퓨터의 전권을 가지게 되는 것이다.

■ USB 충전기를 이용한 해킹

최근 스페인에서 지하철역 등 공곡장소에 있는 무료 휴대전화 충전기를 이용하여 해킹하는 사례가 발생하였다. 해커들은 충전기능 뿐만 아니라 데이터 전송 기능도 가지고 있는 USB 케이블을 이용하여 휴대전화에 저장되어 있는 정보에 접근한다고 한다.

■ 무선 칩을 이용한 해킹

기밀 유지가 중요한 공공·금융 기관은 망분리가 의무화돼 있다. 국가정보원의 '국가정보보안기본지침', 금융감독원의 '전자금융감독규정시행세칙'이 외부망(업무망)과 내부망 분리를 규정하고 있다. 하지만 보안 강화를 위해 내부 업무망과 외부망으로 네트워크를 분리해서 운용해도 반드시 안전한 것은 아니라는 인식이 점차 고조되고 있다.

무선 신호 탐지 기술을 보유한 보안 기업 지슨은 이런 망분리 체제를 우회할 수 있는 해킹 유형에 대처해야 한다고 주장한다. 외부와의 연결이 단절돼 있는 업무망 PC 속 정보도 무선 통신 방식으로 탈취하는 사이버공격이 나타날 수 있다는 것이다. 이런 공공·금융 인프라에 대해 무선 해킹이 이뤄지면 그만큼 민감한 정보가 탈취될 가능성이 있다.

뉴욕타임스는 지난 2014년 미국 국가안보국(NSA)이 무선 통신이 가능한 스파이 칩을 세계 PC 10만대에 심었다고 폭로했다. 폭로한 자료에 따르면 이 스파이 칩은 소형 USB의 형태로, 최장 13km 거리 내에서 내부 정보를 유출할 수 있었다. 인터넷 연결 없이도 무선 전파를 통해 통신이 가능했으며, 스파이 칩이 연결된 컴퓨터에 NSA가 악성코드를 심는 등의 사이버공격도 가능했다. 무선 해킹이 현실적인 사이버 위협으로 다가왔지만, 이를 탐지하기 위한 시스템을 갖추고 있는 곳이 많지 않다. 이에 주파수 기반 통신 탐지 체계가 해답이 될 수 있다는 게 지슨 측의 주장이다.

■ 파밍

파밍(Pharming)이란 악성 코드 프로그램들이 컴퓨터 내부에서 작동해 올바른 도메인 주소를 입력해도 자동적으로 특정한 IP주소로 바뀌어 해커가 만들어 둔 가짜 사이트로만 접속이 되도록 유도하는 방법이다.

컴퓨터에 대한 일정 수준 이상의 지식이 없는 일반인들은 당하고도 파밍 수법에 걸려든 사

실 자체를 모르는 경우가 매우 많다.

■ 제로 데이 공격

아직까지 공표되지 않았거나 공표되었지만 아직까지 패치되지 않은 특정 소프트웨어의 취약점을 이용한 해킹을 말한다. 풀어 말하자면 'Zero-day'는 해당 취약점이 공표 혹은 발견된 날을 뜻하므로, 개발사는 공격이 행해진 시점에서 이 취약점을 해결할 시간을 하루도 채 가지지 못했음을 의미한다.

■ APT 기법

최근 지능형 지속공격(Advanced Persistent Threat, 이하 APT)이라는 개념이 등장하면서 악성코드 공격이 더욱 끈질기고 집요하게 변화했다. APT는 조직 내부 직원이나 일반인 사용자 PC와 스마트폰에 악성코드를 심고, 3~5년 이상 잠복기간을 거쳐 정보를 획득한다. 중앙서버만 공격하는 것이 아니라 홈페이지와 투자자 스마트폰, 사물인터넷(IoT)기기까지 무차별적으로 공격한다는 점에서 기존 해킹 수법과 다르다(김태환, 2018).

지난 2월 평창올림픽 조직위원회와 주요 파트너사에 대한 사이버 테러 역시 APT를 활용한 공격으로 알려졌다. 이로 인해 총 300여대가 영향을 받았으며, 메인프레스센터에 설치된 IPTV가 꺼지고 조직위 홈페이지에 접속 장애가 나타났다. 뿐만 아니라 암호화폐거래소 해킹에도 APT 기법이 동원됐다. 지난 1월 발생한 코인체크 해킹사태는 크래커가 APT를 통해 내부 네트워크에 침투해 송금암호를 취득하고 5700억 원을 탈취했다(김태환, 2018).

■ 사회공학적 해킹(Social engineering hacking) 기법

시스템이 아닌 사람의 심리를 이용하여 원하는 정보를 얻는 해킹 기법으로, 해커가 기술적인 방법이 아닌 사람 사이의 신뢰를 기반으로 사람을 속여 비밀 정보나 돈 등을 갈취하는 기만행위를 말한다.

■ 머신러닝을 이용한 해킹 기법

최근에는 AI 기술이 발전함에 따라 머신러닝을 통해 AI가 자동으로 악성코드를 생성하고 유포하는 기법이 등장했다. AI 기법 중 적대 신경망 구축(Generative Adversarial Network, 이하 GAN) 기술은 상반되는 두 모듈이 대결함으로써 솔루션 생성을 학습하는 구조이다. GAN을 해킹에 활용하면 침투를 막는 탐지 시스템과 이를 피하려는 악성코드 샘플 알고리즘을 대결시켜 가장 이상적인 악성코드를 만들 수 있다. 실제 지난해 데프콘(DEFCON) 콘퍼런스에서 보안업체 엔드게임(Endgame)은 일론머스크의 오픈AI 프레임워크를 사용해 보안 엔진이 탐지하지 못하는 '맞춤형 악성코드'를 제작해 시연하기도 했다(김태환, 2018).

작년 미국에서 열린 '블랙햇 2017(Black Hat 2017)'에 참석한 사이버 보안전문가 중 62%가 올해 해커들이 AI를 활용해 공격할 것이라고 답했다. 이제 AI를 활용해 해킹과 보안 기술이 맞서고 있다. AI 해킹시대 우리의 선택이 중요한 이유다.

Ⅲ. 북한의 해킹 사례

■ 2010년 DDoS 공격

2010년 7월 7일 북한은 한국 정부와 민간 부문 웹 사이트에 대한 DDoS 공격을 시도했다. 그들은 P2P 사이트, 대화방, 웹 하드 및 무료 백신 프로그램 사이트를 통해 멀웨어를 유포했으며 이 맬웨어는 PC를 감염시켜 좀비 PC로 만들었다. 북한 해커들은 전 세계 수천만 대의 좀비 PC 자원을 통제했다. 사이버 공격을 시작하기로 결정했을 때, 이 좀비 PC는 엄청난 양의 데이터 패킷을 지정된 웹 사이트와 웹 사이트 서버의 용량을 초과하여 전송했다. 때때로 DDoS 공격은 사회에 심각한 피해를 입힌다. 이러한 종류의 사이버 공격은 웹 사이트의 마비와 웹 사이트 손상 등을 초래하게 된다.

■ 2011년 DDoS 공격

2011년 3월 4일 북한 해커는 더욱 강화된 사이버 공격을 시연했다. 북한은 주한 미군을 포함한 40개의 한국의 공기업, 정부, 군사 및 개인 웹 사이트에 대한 DDoS 공격을 시작했다.

4월 12일 북한은 농협 인터넷 뱅킹 시스템을 마비시켰다. 은행의 서버가 중단되고 데이터가 지워졌다. 전문가들은 이 공격을 면밀히 평가한 후 북한 해커가 인터넷 뱅킹 시스템의 유지 관리 기술자에 대해 APT를 사용한 것으로 보인다. 북한 해커들은 유지 보수 기술자를 식별하고 그 기술자의 PC에 악성 코드를 주입하기 위해 많은 시간과 에너지를 소비 한 것으로 보였다. 이를 알지 못한 채 기술자는 자신의 PC를 농협인터넷 뱅킹 시스템에 연결하여 정기 점검을 수행했으며 이때 맬웨어가 시스템에 주입되었던 것이다.

■ 2013년 MBR 와이퍼 공격

3월 20일, MBR(Master Boot Record) 와이퍼 공격으로 농협, 신한은행, 제주은행 등을 포함하는 은행과 YTN, KBS, and MBC 등을 포함하는 미디어 대행사 등 32,000 대의 컴퓨터의 하드디스크가 파괴되고 차단되었다. 이로 인해 공격을 받은 방송사들은 방송에 차질을 빚었으며 금융기관들의 거래가 한동안 중단됐다. 이 사건은 2013년 3.20 사이버 테러로 명명되었다. 보안업체들의 자체 조사 결과 악성코드가 백신 프로그램의 구성 파일로 위장해 기업 내부 백신 업데이트 서버를 통해 곳곳에 퍼졌다는 사실이 드러났다. 정부·민간 합동 대응팀은 북한이 적어도 8개월 전부터 공격을 준비했다고 분석했다. 이 사건으로 한국의 시민들은 사이버공격이 얼마나 가공할 만한 위력을 가질 수 있는지를 확인했다.

3.20 사이버 테러 5일 후, 북한 사이버 전사들은 DailyNK, Free North Radio 및 NKnet을 공격했다. 이 기관들은 탈북한 북한 지식인이 운영하는 공공 언론 기관으로서 북한 정권의 잘못된 내용을 전파하는 언론 기관이다.

■ 2013년 DDoS 공격

6월 25일 16개의 정부 및 미디어 대행사 웹 사이트에 대한 DDoS 공격이 있었다. 또한 북한 해커들은 그 웹 사이트의 DNS 서버를 목표로 삼았다.

■ 2014년 MBR 와이퍼 공격

11월 북한이 소니 픽쳐스를 해킹한 사건이 발생했다. 이는 북한 김정은 노동당 위원장을 희화화한 영화 '인터뷰'를 제작한 소니 픽쳐스가 해킹을 당해 회사 내부 자료가 유출되는 사건이 있었다. 이로 인하여 소니에서 제작한 미개봉 영화가 유출되었고 임직원들의 연봉 자료까지 공개됐다. 2015년 1월, 제임스 코미 당시 FBI 국장은 북한이 소니 픽쳐스 해킹에 연관됐다는 결정적인 증거를 확인했다고 말했다. 해커들이 가끔씩 접속한 지역의 IP 주소를 숨기지 못한 경우가 있었는데 이렇게 드러난 IP 주소는 북한만 쓰는 것이란 주장이다. 해킹 방법으로는 MBR 와이퍼 공격 방법을 통해 시도하였다.

12월, 한국 원자력 발전소 기업인 한국 수력 및 원자력 정보 시스템에 대한 사이버 공격 시도가 있었으며 '원전반대그룹'의 대외비 문서 유출 사건이 발생했다. 그들은 데이터 절도 및 MBR 와이퍼 공격을 시도했다. 이는 한국수력원자력(한수원)의 직원 이메일을 통해 악성코드를 유포하려고 시도하였으며 이후 '원전반대그룹'을 자칭하는 해커가 블로그와 트위터를 통해 한수원의 내부 자료를 유출했다. 원전반대그룹은 국내 원자력발전소의 설계도를 비롯하여 청와대, 국방부, 국정원 문서라고 주장하는 자료까지 공개했다. 당시 공개된 문서 중 하나에는 중국이 북한 지역을 미국, 러시아, 중국, 한국의 4개국이 분할 통제하는 방안을 제안했다는 내용이 담겨 있어 한국에서 적잖은 파장을 몰고 왔다. 검찰은 해커로 추정되는 인물이 북한 정찰총국 해커가 활동하고 있는 곳으로 알려진 중국 선양(瀋陽)시를 비롯한 특정 지역에서 접속했다고 발표했다. 당시 접속 지역으로 확인된 중국 요녕성의 IP로 2016년 1월에도 청와대를 사칭하는 이메일이 정부기관과 국책연구기관 등에 대량으로 발송된 일이 있었다. 이 사건은 북한이 사이버 공격을 통해 실제적이고 물리적인 피해를 입힐 수 있는 것으로 보였기 때문에 심각한 사건으로 여겨졌다(백승구, 2015).

■ 2016년 전산망 해킹

북한 사이버 위협이 다시 문제가 되었다. Jetco Technology의 김민호에 따르면 북한은 2016년 상반기 동안 최소 10건의 사이버 공격을 시작했다고 한다. 북한은 4차 핵 실험 이후 사이버 공격을 증가시켰다.

2월 스위프트 전산망 해킹사건이 발생했다. 이 사건은 현재까지 국가 차원에서 사이버공격으로 은행털이를 한 최초의 사례로 알려져 있다. 이는 방글라데시 중앙은행이 뉴욕 연방준비은행에 예치하고 있던 1억100만 달러(한화 약 1167억 원)가 해킹으로 인해 도둑맞은 사건이다. 해커들은 방글라데시 중앙은행의 서버에 악성코드를 심어 놓고 스위프트(SWIFT) 시스템 접속 정보를 훔쳐냈다. 스위프트 시스템은 전세계 은행 공동의 전산망으로 해외 송금에 주로 사용된다. 여기에 방글라데스 중앙은행 명의로 접속하는 데 성공한 해커는 뉴욕 연방준비은행에 필리핀과 스리랑카의 은행으로 자금 이체를 요청하는 메시지를 보냈다. 해커는 이체시킨 1억100만 달러 중 8100만 달러를 빼돌리는 데 성공했다. 이후 보안업체의 조사 결과 소니 픽쳐스 해킹을 주도한 라자러스(Lazarus) 그룹의 흔적이 발견됐다. FBI는 소니 픽쳐스 해킹이 북한의 소행이라고 발표한 바 있다. 2016년 6월 말 현재 한국은 평양 류경동에 16대의 공격 서버를 식별했다. 사이버 공격에서 북한 해커가 사용한 것으로 알려진 33개의 악성 코드를 분석하였다. 그 결과 북한의 사이버 공격은 다음과 같은 관심을 끄는 몇 가지 특징을 찾을 수 있다.

첫째, 기존의 보안 위협과 비전통적 위협을 혼합하는 것이 일반적인 공격 패턴이 되었다.

북한 해킹 조직의 엘리트들은 제4차 핵 실험과 같은 다른 군사적 도발과 사이버 공격을 통합하라는 명령을 받은 것으로 보인다. 북한의 의도는 한국인의 마음을 분산시키는 것이며,이 목표를 달성하기 위해 해커는 잘못된 정보와 선전 등을 유포했다. 예를 들어, 북한 해커들은 현재 북한의 핵 문제에 대한 정부의 접근 방식을 비판하는 대량의 이메일을 보냈다. 영향력 있는 학자나 방송사(예: MBC, SBS)의 도난당한 계정에서 전자 메일을 보내어 전자 메일을 보다 안정적으로 만들려고 시도했다.

둘째, 북한 사이버 전사들은 북한이 여러 정치인과 고위 군인들의 스마트 폰을 해킹한 사건과 같이 모바일 영역으로 사업 영역을 확장했다. 그들은 문자 메시지를 가로 채고, 전화 대화를 녹음하고, 연락처 정보를 얻었다.

셋째, 북한이 대규모 혼돈으로 이어질 대중 교통 관리 시스템 등을 혼란시키려고 의도하였다.

실제로 서울 지하철 시스템인 서울 메트로에 대한 해킹 시도가 있었다.

사이버로 인한 교통 사고를 예고하게 하여 한국의 대중들을 불안하게 하였다.

■ 2016 방위 관련 기업에 대한 해킹

F-16의 유지 보수 매뉴얼, 한국 드론 부품 사진 및 기타 민감한 문서를 훔쳤다. 당국은 42,600 개의 문서가 도난 당했다고 추정했다. 이는 새로운 현상이며 북한 해커가 군사적 목적에 더 가깝다는 인상을 준다.

■ 2016년 군 인트라넷 해킹

원래 국방부 PC는 해킹 방지의 목적으로 인트라넷과 일반 인터넷 회선이 분리가 되어 있다. 그런데 국방부 내 한 PC에서 임의의 랜카드를 추가해서 사용하였고 그 랜카드가 결국 일반 인터넷망과 연결되면서 해킹이 시작되어 국방부 내 PC 약 3200대가 해킹되었다. 이 해킹은 북한의 소행이라고 추측하였지만 군사기밀은 이미 유출된 뒤였고 한·미 연합군 대응계획인 '작전계획 5027' 까지 유출되지 않았나 하는 의혹까지 있었다. 작전계획 5027은 북한의 선제공격과 우발적 도발 등에 대응한 미군의 전시 증원 계획이 담긴 핵심 작전계획으로, 작계 5027이 북한에 유출됐다면 남침 대비 방어 계획이 고스란히 적에게 넘어가게 된다(「KBS 뉴스」, 2017).

Ⅳ. 북한의 해킹에 대한 대비책

■ DDOS 공격에 대한 대비

DDOS 공격을 예방하기 위해서는 다음과 같은 방법들을 통해 자신의 PC가 좀비 PC가 되지 않도록 주의하여야 한다.『네이버 지식백과』

① 윈도우 운영체제 보안패치가 나오면 즉시 업데이트를 해준다.(자동 업데이트 설정)

② 백신 프로그램을 설치하고 주기적으로 악성코드 검사도 해준다.

③ 방화벽을 설정한다.

④ 신뢰할 수 있는 웹사이트에서 제공하는 프로그램만 설치한다.

⑤ 웹하드, P2P 등 인터넷에서 다운로드한 파일은 실행 전에 반드시 악성코드를 검사한다.
⑥ 출처가 불분명한 메일은 클릭하지 않는다.
⑦ 메신저, SNS 사용 시 첨부된 링크와 파일 클릭에 주의한다.

■ MBR 파괴 공격에 대한 대비

MBR은 공격은 사용자가 거의 대응 할 수 없으며 탐지가 어렵다. 안철수연구소는 개인 PC 안전을 위해 안전모드 부팅을 권장하고 전문 백신 프로그램을 통해 지속적인 PC 점검을 당부하고 있다. 한국정보보호진흥원을 통해 실제 감염된 좀비 PC가 어떻게 명령을 수행하는지를 알아본 결과 사용자가 접속을 수행치 않았음에도 순간적으로 대량의 트래픽이 좀비PC 내부에서 유발되는 것을 확인할 수 있었다고 한다(「경향비즈」, 2009/7/10).

■ 크로스 사이트 스크립팅(XSS) 공격에 대한 대비

XSS 취약점은 대부분 웹 애플리케이션 개발자가 사용자 입력을 받아들이는 부분에서 사용자 입력에 대해 어떠한 검증도 하지 않았기 때문에 일어난다. 따라서 다음과 같은 방법으로 예방할 수 있다.

• 사용자를 식별하기 위해서 쿠키에 비밀번호와 같은 민감한 정보는 담지 않는다.

• 스크립트 코드에 사용되는 특수문자를 이해하고 정확한 필터링을 해야 한다. 가장 효과적인 방법은 사용자가 입력 가능한 문자(예를 들면 알파벳, 숫자, 몇몇의 특수문자)만을 정해 놓고 그 문자열이 아니면 모두 필터링한다. 이 방법은 추가적인 XSS 취약점에 사용되는 특수문자를 사전에 예방하는 장점이 있다.

■ 이메일 위조에 대한 대비

이 수법은 상대적으로 높은 기술력이 필요하지 않으며 전통적인 해킹보다는 속임수에 더 의존하는 편이다. 따라서 주의를 기울이고 관찰하고 의심이 가면 직접 확인하는 습관을 가지기를 권장한다.

■ 랜섬웨어 공격에 대한 대비

랜섬웨어는 주로 이메일 첨부파일이나 웹페이지 접속을 통해 들어오기도 하고, 확인되지 않은 프로그램이나 파일을 내려받기 하는 과정에서 들어오기도 한다. 따라서 랜섬웨어의 피해를 입지 않기 위해서는 예방이 무엇보다도 중요하다. 확인되지 않은 주소의 이메일이나 스팸 메일은 열어보지 않는 것이 좋으며, 파일을 내려 받기 할 때에도 도메인이 정확히 확인된 공식 사이트에서만 내려 받는 것이 안전하다. 또한, 운영체제의 업데이트를 주기적으로 실시하는 것도 중요하다. 운영체제 업데이트를 최신 버전으로 유지하고 있으면 랜섬웨어를 어느 정도 차단할 수 있는 것으로 알려져 있다.

■ 디렉터리 탐색 공격에 대한 대비

전용 파일 다운로드 프로그램을 이용할 때는 '.. ', '/' 문자열에 대한 필터링이 없을 경우, 공격자는 상위로 올라가 특정 파일을 열어볼 수 있기 때문에 '.. '와 '/' 문자를 필터링해야 한다. 파일 업로드와 마찬가지로 자바 스크립트와 같은 클라이언트 스크립트 언어로 필터링하면 공격자가 우회할 수 있기 때문에 반드시 jsp나 asp 등 서버 쪽 스크립트 언어에 필터링을 추가해야 한다.

■ 인증 우회 공격에 대한 대비

웹 개발자가 자주 범하는 실수를 이용한 해킹 기법이다. 일반적으로 관리자로 로그인한 뒤 관리자가 이용하는 웹페이지에 접속해야 하는데, 로그인하지 않고 직접 관리자만이 이용할 수 있는 웹페이지에서 특정 작업을 수행하게 되므로 그 피해가 매우 크다.

이러한 공격의 피해를 막기 위해서는 관리자 페이지나 인증이 필요한 페이지에 대해 반드시 관리자 로그인 세션에 대한 검사를 수행하는 과정을 넣어야 한다. 이런 약점을 노출시키지 않으려면 관리자는 자신이 좀 불편하더라도 안전한 방법을 이용해 사이트나 파일을 관리해야 한다.

■ 디렉터리 리스팅 공격에 대한 대비

대부분의 웹서버는 해당 디렉터리 리스팅에 대한 여부를 가능 혹은 불가능하게 하는 옵션이 따로 준비되어 있으므로 해당 설정 내용을 적절하게 변경하기만 하면 디렉터리 리스팅을 이용한 공격은 통하지 않을 수 있다.

■ 사전 공격에 대한 대비

보통 널리 사용되는 단어나 날짜, 전화번호 등의 패턴들을 사전형태로 만들고 이들을 조합하는 방식으로 공격하기 때문에 자신의 생일이나 전화번호, 이름 이니셜 등의 특정한 패턴을 사용하지 않는 것은 좋은 대비책이 될 수 있다.

■ SQL 인젝션 공격에 대한 대비

- 사용자 입력이 SQL 인젝션을 발생시키지 않도록 사용자 입력을 필터링한다.
- SQL 서버의 에러 메시지를 사용자에게 보여주지 않도록 설정한다.
- 웹 애플리케이션이 사용하는 데이터베이스 사용자의 권한을 제한한다.
- 데이터베이스 서버에 대한 보안 설정을 수행한다.

■ 파일 업로드 공격에 대한 대비

파일 업로드 공격에 대응하는 가장 간단하고 효과적인 방법은 업로드할 때 파일 확장자 이름을 확인하는 것이다. asp나 jsp 같이 업로드되는 확장자를 소문자만 체크하지 않도록 주의해야 한다. 시스템은 aSp나 jSp 같은 대소문자 혼합도 인식하기 때문에 모든 가능한 조합을 필터링해야 한다. 반대로 특정 확장자 이름을 가진 파일만 업로드 되도록 하는 것도 좋은 방법이다. 이때 또 한 가지 주의할 점은 필터링을 위해 자바 스크립트 같은 클라이언트 스크립트 언어를 사용하지 말아야 한다는 것이다. 어느 정도 숙달된 해커라면 클라이언트 스크립트 언어쯤은 얼마든지 수정할 수 있기 때문에 asp나 jsp 같은 서버 쪽 스크립트 언어에서 필터링해야 한다. 필터링 이외에 파일이 업로드되는 디렉터리의 실행 권한을 없애는 방법이 있다. 이 경우에는 파일이 업로드되더라도 실행되지 않기 때문에 브라우저에 그대로 나타나거나 파일을 다운로드하게 된다.

■ USB 충전기를 이용한 해킹에 대한 대비

공공장소의 충전기를 이용하는 대신 보조 배터리를 사용하거나 피치 못하게 충전기를 사용해야 하는 경우 휴대전화의 전원을 아예 끄고 충전하거나 데이터 전송이 불가능한 충전 전용 USB 케이블을 이용할 것을 권장한다(「RedFriday」, 2019/11/26).

■ 무선 칩을 이용한 해킹에 대한 대비

무선 해킹이 현실적인 사이버 위협으로 다가왔지만, 이를 탐지하기 위한 시스템을 갖추고 있는 곳이 많지 않다. 이런 무선 해킹에 대한 대비책의 일환으로 주파수 기반 통신 탐지 체계를 갖출 필요가 있다는 것이 지슨측의 주장이다.

■ APT 해킹 기법에 대한 대비

기존의 보안 기술만으로는 절대로 막을 수 없는 것이며, 그저 초기 보이스 피싱 때처럼 구성원 개개인이 조심하고 스스로 보호하는 수 밖에 없다. 일반적인 대비책으로는 이메일로 들어오는 것은 일단 의심하는 습관을 가질 필요가 있다. 예를 들어 거래처의 이메일이라도 평소와 다른 어투를 쓰거나 메일주소나 이름 철자가 좀 다르거나, 갑자기 미국에서 오던 아이피 주소가 나이지리아, 인도에서 발신된 것으로 오거나, DHL이나 알리바바, 아마존을 사칭하며 보낸 적도 없는 물건의 도착여부를 확인하라고 요구한다던지 은행계좌가 블랙리스트니 여기 클릭해서 풀라고 한다든지, 급하니 기존에 잘 쓰던 송금 계좌를 바꾸자고 하는 경우 등 이메일 속의 사소하거나 큰 변화들을 눈치채고 의심하는 것이 필요하다.

특히 중요한 것은 절대 이메일 내 첨부파일과 링크를 함부로 열지 않는 것이 중요하다. 보내주기로 약속한 자료인지 확인하고, 이후 반드시 바이러스 유무를 재확인하고 백신의 샌드박스에서 돌려본 후에도 100% 안심하지 않는다. APT 기반은 기존의 유명 백신이 탐지하지 못하는 최신 바이러스를 첨부파일에 넣는 경우도 있다. 그래서 최신의 APT 백신들 중에는 아예 이메일 내용 자체를 전부 PDF 등으로 만들어 실행 자체가 불가능하게 하고 보여주거나, 기존의 이메일과 차이점이 있는 부분을 클로즈업하는 기능을 넣는 경우들도 있다.

Ⅴ. 결론

본 논문에서는 현재 주로 사용되고 있는 해킹 기술들을 조사하였으며, 북한이 주로 사용하고 있는 해킹 기술과 공격 방법을 연구하였다. 또한 이를 바탕으로 북한의 해킹 공격에 효과적으로 대비하는 방법과 북한의 해킹에 의한 피해를 최소화할 수 있는 방안을 제시하였다. 우리는 언제나 어느 장소에서나 항상 해킹의 위험에 노출되어 있다는 것을 인식하고 지금까지 소개된 다양한 해킹 방법들과 대응 방법을 잘 숙지하여 북한의 해킹 공격에 노출되지 않게 대비하는 자세가 필요하다.

참고문헌

김태환. (2018). "AI 머신러닝 활용한 최첨단 해킹 시대.“『Tech M』, (2018년 10월호).

백승구. (2015). “進化하는 북한 사이버테러 김정은 등장 이후 사이버테러 급증, 공격기술 高度化.”「월간조선」, (2015년 9월호).

안우정. (2019). “공항에서 USB로 핸드폰 충전하면 절대 안되는 이유는?”「RedFriday」, (11월 26일).

손재철. (2009). “좀비PC, 이젠 하드디스크까지 손상 일으킨다.”「경향비즈」, (7월 10일).

「국민일보」. (2019). "암호화폐 거래소 또 뚫렸다…업비트, 이더리움 580억원 유출.“ (11월 27일).

「뉴스투데이」. (2019). "사이버보안 강화하는 북한…새로운 악성코드 차단하는 '참빗 4.0' 공개.“ (11월 22일).

「KBS 뉴스」. (2017) “작전계획 5027 유출.” (4월 3일).

Boo, Hyeong-wook. (2014). “Crisis Pattern Change and Its Implication for National Crisis Management System.”『Journal of Defense Policy Studies』, Vol.30 No.1.