情 報 保 護 學 會 誌
第 16 卷 第 1 號, 2006. 2

최근 주요 해킹 피해 동향과 대응 방안

성 재 모*, 노 봉 남*, 안 승 호*

요 약

최근의 홈페이지 해킹은 단순 홈페이지 변조뿐만 아니라 피싱에 악용하거나 해킹한 홈페이지를 이용하여 홈페이지 방문자의 게임 계정과 비밀번호 유출 및 개인금융정보를 유출하는 등 금전적 이득을 위한 범죄적인 성향으로 바뀌고 있다. 인터넷 상에서 고객의 개인정보를 지키고, 기관의 신뢰를 유지하기 위해서 기관을 대표하는 얼굴인 홈페이지 보안 관리에 관심을 가져야 할 것 같다. 본고에서는 최근 발생한 홈페이지 관련 해킹 피해 사례를 분석해 보고 피해 예방을 위한 대응 방안을 기술한다.

Ⅰ. 서 론

국내 월 평균 인터넷 사용자가 3,250만 명을 넘었으며 초고속인터넷 가입자수가 1,210만 명을 넘었고 인터넷 보급률은 71.9%로 전세계 최고 수준이다.[1] 국내의 인터넷 환경은 최근 OECD 보고서를 기준으로 하여도 언제 어디서나 사용 가능한 초고속인터넷 환경이 가장 좋은 국가 중의 하나이다.

하지만, 이러한 세계최고의 인터넷 환경은 정보보안에 대한 대비 및 준비를 하지 않은 경우는 세계에서 가장 인터넷 보안이 허술한 국가라는 오명을 쓰게 되고, 잘 발달된 국내 초고속통신망 인프라 및 보안이 취약한 서버와 PC는 전 세계 해커들의 해킹 대상이 되어 제3국에 위치한 다른 시스템을 공격하거나 해킹을 위한 중간 매개체로 악용이 된다.

초고속 인터넷의 이용이 보편화되고, 정보화가 성숙되어 감에 따라 인터넷상에서 개인, 기관 등의 홈페이지가 정보를 알리고 공유하는데 중요한 역할을 차지하기 시작하였고, 게임, 쇼핑몰, 인터넷뱅킹 등 인터넷을 통한 활동이 증가함에 따라 인터넷상의 취약점을 이용한 악성코드 유포 및 해킹 등 인터넷 침해 사고도 증가하고 있는 실정이다.

또한, 최근에는 웹서버를 해킹하여 악성코드를 삽입함으로서 게임 아이디와 비밀번호를 빼내어 게임 머니와 아이템을 훔쳐가는 사고가 급증하고, 금융기관 홈페이지를 사칭하여 개인 금융정보를 훔치는 피싱(Phishing) 사례가 국내에도 발생하였다.

과거의 해킹은 단순 실력 과시를 위한 목적을 행한 사례가 많았는데, 이제 국내에도 금적적인 이득을 목적으로 불특정 다수를 대상으로 한 해킹 피해 사례가 증가하고 있는 실정이다.

본고에서는 최근 발생한 주요 해킹 피해 사례 중 홈페이지와 관련된 사례에 대하여 살펴보고 대응 방안을 기술 한다.

Ⅱ. 홈페이지 관련 해킹 피해 사례

최근 홈페이지 해킹 사고 중 가장 이슈화 된 사고가 대규모 홈페이지 변조사고와 홈페이지 해킹 후 악성코드를 유포하는 사고이다.

본 장에서는 2005년 발생한 이 두 가지 사고 분석을 통하여 홈페이지 해킹 피해 동향 등을 기술한다.

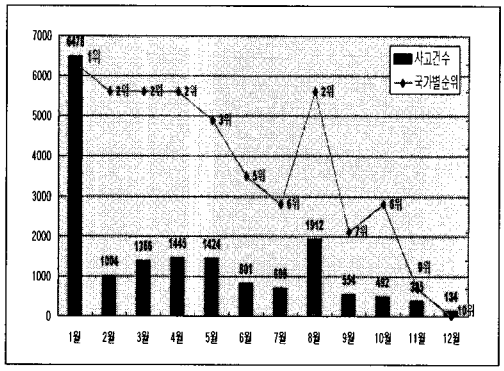
2.1 홈페이지 변조 사고

'05년은 국내 홈페이지 변조사고가 이슈가 되었던 한 해로서 '05년 1월 한 달 변조사고가 '04년 전체 사고 건보다도 많이 발생하는 등 급격히 증가하는 추세를 보였다.[2]

이러한 홈페이지 변조사고의 증가는 다수의 홈페이지가 운영 중인 웹 호스팅 서버 환경에서 많이 사용되

* 전남대학교 정보보호협동과정 (jmseung@kisa.or.kr, bongnam@chonnam.ac.kr, shahn@chonnam.ac.kr)
* 본 연구는 정보통신부 대학 IT연구센터 육성, 지원사업의 연구결과로 수행 되었습니다.

고 있는 공개 웹 S/W 취약점 공개가 주요 원인인 것으로 확인되었는데, 해당 취약점은 이미 국내 언더그라운드 해커 사이에서는 어느 정도 알려진 취약점이었지만, 국외의 보안사이트에 취약점이 공개된 이후 해당 취약점을 이용하는 국외 해커그룹이 늘어남에 따라 '05년 상반기(1월~7월)에만 13,214건의 변조사고가 발생하는 등 국내 홈페이지 변조사고는 심각한 상황에 이르고 있다.



〔그림 1〕 '05년 홈페이지 변조통계 및 국가별 순위

이런 홈페이지 변조사고는 제로보드 등의 공개 웹 S/W의 보안 취약점에 대한 패치를 하거나, PHP의 설정을 변경함으로써 막을 수 있는 문제이지만 웹 호스팅 업체와 홈페이지 운영자들의 보안인식 부재와 지식 부족으로 인해 홈페이지 변조사고가 지속적으로 발생하는 원인이 되었다.

'05년 국내 홈페이지를 대상으로 홈페이지 변조작업을 한 해커그룹은 130여개 그룹으로, 개인 홈페이지부터 대기업 홈페이지까지 다양한 홈페이지를 대상으로 변조작업을 하였다.

전체 대상 그룹 중, 국가가 확인된 해커그룹은 총 86개 그룹으로 그 중 28개 그룹의 소속이 터키로 확인되어 가장 많은 홈페이지 해커그룹이 있는 나라로 확인되었고, 브라질이 24개, 중동지역 국가 소속의 해커그룹은 6개로 확인되었다.

국내 홈페이지 변조에 이용된 주요 취약점은 Linux 계열 OS의 경우, 공개 S/W 게시판의 취약점이 가장 높은 비율을 차지하였고, Windows 계열 OS에서는 WebDAV 설정오류 취약점이 높은 비율을 차지하는 것으로 확인되었다.

'05년 6월부터 하향 추세를 보이던 홈페이지 변조사고는 8월 들어 전월 대비 174.7%가 증가한 1,912건이 발생하였는데, 확인결과 브라질의 특정 그룹에서 우리나라를 타겟으로 한 홈페이지 변조사고의 발생이 원인인 것으로 파악되었다.

〔표 1〕 해커그룹 소속국가 및 주요 변조취약점 Top 5

순위	그룹 소속국가	변조건수	순위	주요 변조취약점	취약점 건수
1	터키	28	1	WebDAV 설정오류 취약점	42
2	브라질	24	2	PHP Injection	25
3	중동(쿠웨이트 등)	5	3	PHPBB 취약점	11
4	멕시코	5	4	제로보드 취약점	5
5	이란	3	5	PHP Nuke 취약점	4

해당 그룹은 SPYKIDS라는 브라질 해커그룹으로, 8월 한 달 동안 1,217건의 사고를 일으킨 것으로 확인되었는데, 이는 8월 홈페이지 변조사고의 64%를 차지하는 수치로서 대부분 호스팅 서비스를 하고 있는 Linux 서버를 대상으로 변조작업을 한 것으로 확인되었다.

홈페이지 변조에 이용된 취약점은 '05년 초부터 지속적으로 문제가 되어온 공개 게시판 프로그램인 제로보드의 취약점으로서, 이미 제로보드에 대한 보안패치가 발표되었고, 보안대책도 공지 되었지만 실제 시스템을 운영하는 관리자와 홈페이지 운영자의 보안에 대한 관심 없이는 피해사고를 예방할 수 없다는 것을 보여준 단적인 예라고 할 수 있다.

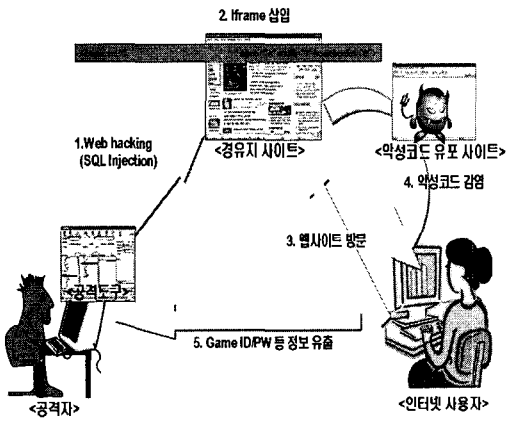
〔표 2〕 '05년 8월 홈페이지 변조사고 현황

해커그룹	변조건수	웹서버 종류	국가	주요 대상OS
SPYKIDS	1,217	Apache	브라질	Linux 계열
nET^DeViL	120	Apache	중동	Linux 계열
eno7	50	IIS	터키	Windows 계열
hackbsd Crew	28	IIS	-	Linux, Windows
기타	497	-	-	-
합계	1.917	-	-	-

2.2 홈페이지 해킹 후 악성코드 유포 사고

최근 대형 포털 사이트, 뉴스 사이트 등 유명 웹 사이트들이 연이어 해킹당해 악성코드가 삽입되는 사고가 지속적으로 발생되고 있다. 이러한 공격은 주로 중국에 할당된 IP 블록으로부터 발생되는 경우가 많은데 온라인 게임 아이템이 현금으로 거래되고 있어 게임 아이템을 불법적으로 획득하기 위한 목적으로 해킹을 하는 것으로 보인다. [3]

이러한 공격은 일반적으로 다음의 과정을 통해 이루어진다. [4]



① 공격자는 홈페이지에 존재하는 SQL Injection 취약점을 주로 이용하여 해킹을 수행
② 해킹한 국내 웹사이트들의 초기 화면에 특정 iframe을 삽입, 해당 iframe은 사용자 PC를 감염시킬 수 있는 특정 사이트(악성코드 유포 사이트)로 접속을 유도함
③ 인터넷 사용자가 해킹당한 웹사이트에 방문
④ 인터넷 사용자의 PC가 보안패치 되지 않았을 경우 악성코드 유포 사이트로부터 트로이목마 프로그램 등에 감염
⑤ 감염된 인터넷 사용자의 게임 ID와 패스워드 등 정보를 특정 주소로 유출

악성코드 경유지 사이트로 이용되는 국내 유명 웹 사이트들은 주로 웹 게시판의 URL 인자값의 입력값 검증을 하지 않음으로 해서 발생되고 있으며, 이를 공격할 수 있는 자동화된 도구들이 인터넷을 통해 공개되어 있다. 또한 악성코드 유포사이트는 중국 등 해외나 국내 웹사이트가 역시 해킹당해 유포사이트로 악용되고 있다.

Ⅲ. 홈페이지 침해사고 대응 방안

3.1 사용자 입력값 검증(SQL Injection 취약점 제거)

악성코드 경유지 사이트로 악용된 사이트들은 다양한 경로를 통한 사용자 입력값이나 URL의 인자값에 대한 검증을 하지 않았다. 따라서, SQL Injection 공격을 방어하기 위해 사용자 입력값이나 URL 인자값에 대한 검증이 우선시 되어야 한다. [5]

- 데이터베이스와 연동을 하는 스크립트의 모든 파라미터들을 점검하여 사용자의 입력 값이 SQL injection을 발생시키지 않도록 수정한다.
- 사용자 입력이 SQL injection을 발생시키지 않도록 사용자 입력 시 특수문자(' " / \ ; : Space -- +등)와 SQL 구문(union, select, insert 등)이 포함되어 있는지 검사하여 허용되지 않은 문자열이나 문자가 포함된 경우에는 에러로 처리한다.
- SQL 서버의 에러 메시지를 사용자에게 보여주지 않도록 설정한다. 공격자는 리턴 되는 에러 메시지에 대한 분석을 통하여 공격에 성공할 수 있는 SQL Injection 스트링을 알아낼 수 있다. 따라서 SQL 서버의 에러 메시지를 외부에 제공하지 않도록 한다.

3.2 불필요한 확장 저장 프로시져 제거

MS-SQL 서버에서 제공하고 있는 확장 저장 프로시져 중 사용하지 않는 프로시져들을 제거하도록 한다. xp_cmdshell, xp_regread, xp_dirtree와 같은 프로시져들은 공격자에 의해 이용될 수 있으므로 가능한 제거하는 것이 바람직하다.

3.3 업로드 취약점 제거

파일 업로드 취약점은 이미 오래전에 알려진 홈페이지 취약점이지만 악성코드 유포지 사이트 분석 사례에서도 알 수 있듯이 아직 공격에 많이 이용되고 있다. 업로드 취약점을 제거하기 위해서는 다음과 같은 대책이 필요하다.

- 첨부파일의 확장자 필터링 처리
  사용자가 첨부파일의 업로드 시도 시, 업로드되는 파일의 확장자를 검토하여 적합한 파일인지를 검사하는 루틴을 삽입하여, 적합한 파일의 확

장자 이외의 파일에 대해서는 업로드 되지 않도록 함

- 업로드 파일을 위한 디렉토리의 실행설정 제거
  업로드 파일을 위한 전용 디렉토리를 별도 생성하여 웹 서버 설정파일에서 실행 설정을 제거함으로써, Server Side Script가 업로드되더라도 웹 엔진이 실행하지 않게 환경을 설정함

업로드 된 디렉토리에서 실행 권한을 제거하는 방법은 임시적이기는 하지만 소스 코드의 수정 없이 간단히 수행 될 수 있다. IIS 웹서버에서는 다음의 절차를 통해 설정할 수 있다.

〔설정〕→〔제어판〕→〔관리도구〕→〔인터넷 서비스 관리자〕 선택

해당 업로드 폴더에 오른쪽 버튼을 클릭을 하고 등록정보→디렉토리→실행권한을 "없음"으로 설정한다

Ⅳ. 결 론

기존의 시스템이나 네트워크 취약점을 이용한 공격에서 최근 어플리케이션의 취약점을 이용한 공격이 크게 증가하고 있는데, 특히 인터넷을 통해 공개 서비스되고 있는 웹 어플리케이션이 주요한 공격 대상이 되고 있다. 또한, 홈페이지는 공개 서버의 특성으로 인하여 기존 방화벽으로부터 보호받지 못하고 있으며, 다양한 웹 공격 형태로 기존의 IDS에서도 공격 탐지가 쉽지 않다.

한 번 해킹당한 홈페이지가 재 해킹 당하는 경우를 자주 볼 수 있는데, 이는 자신이 관리하고 있는 홈페이지의 보안 취약점을 알고 있지만 취약점 제거를 위해서는 프로그램 소스코드 수정이 필요하여 속수무책으로 해킹을 당하고 있다. 이처럼 홈페이지 보안은 실제 너무나 다양한 공격 형태가 존재하여 지엽적인 보안 대책만으로는 충분하지 못하다.

홈페이지 운영 중에 발생되는 보안 문제점에 대한 수시조치 보다는 홈페이지를 최초 설계·개발하는 단계에서부터 보안이 고려되어야 한다. 따라서 한국정보보호진흥원에서 작성·배포하고 있는 「홈페이지 개발 보안 가이드」[6]를 참고하여 홈페이지 개발 과정에서부터 공격 가능성이 있는 다양한 취약점에 대해 보안조치를 할 필요가 있다.

홈페이지 설계·개발 단계에서부터 보안을 고려하여 웹서버를 구축하는 것이 비용-효과적인 측면에서도 사후 재 수정하는 것에 비해 유리하지만, 현실적으로 많은 기업에서는 보안을 고려하지 않은 채 웹서버를 이미 운영하고 있는 경우가 많다.

이 경우, 운영 중인 웹서버의 보안성을 강화하기 위한 보안 솔루션의 도움을 받는 것도 하나의 방법이라 할 수 있다. 기존의 전통적인 보안 솔루션인 방화벽이나 IDS는 다양한 웹 공격을 탐지하여 차단하기에는 한계가 있으므로 웹 전용 보안 솔루션의 도입이 웹 보안 강화에 도움이 될 수 있다. 대표적인 웹 보안 솔루션으로는 웹 방화벽과 웹 취약점 스캐너가 있는데 웹 방화벽은 어플리케이션 레벨에서 웹 트래픽을 감시·분석하고 공격 트래픽을 차단하는 기능을 가지고 있으며, 웹 취약점 스캐너는 홈페이지에 존재하는 공격 가능한 취약점을 사전에 찾아주는 기능을 가지고 있다.

최근의 홈페이지 해킹은 단순 홈페이지 변조 수준이 아니라 해킹한 홈페이지를 이용하여 고객의 게임 비밀번호 유출, 금융정보 유출 등 범죄적인 성향으로 바뀌고 있다. 공격 방법도 공개 웹 게시판의 취약점 이용, 웹서버 설정 오류, SQL Injection 등 개발 오류 등 다양한 취약점들에 대해 공격하고 있으므로 기업 및 대학의 전반적인 웹 보안 현황을 점검하여 보완할 필요가 있을 것이다.

참 고 문 헌

〔1〕 "주요 인터넷 통계 지표", http://isis.nida.or.kr/index.html

〔2〕 "12월 해킹바이러스 분석 및 통계 월보", http://www.krcert.or.kr/statistics

〔3〕 "웹 해킹을 통한 악성코드 유포사이트 사고 사례", http://www.krcert.or.kr/report

〔4〕 "업로드 취약점을 이용한 악성코드 유포사례", http://www.krcert.or.kr/report

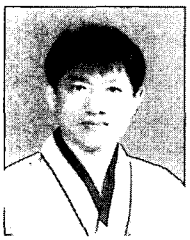
〔5〕 "SQL Injection 취약점을 이용한 윈도우즈 웹서버 사고 사례", http://www.krcert.or.kr/report

〔6〕 "홈페이지 개발 보안 가이드", http://www.krcert.or.kr/

〈著 者 紹 介〉

성 재 모 (Jaemo Seung)

1990년 2월 : 동국대학교 전자계산학과 (학사)
1993년 5월 : 스트븐스공과대학 전산학과 (석사)
1993년 8월 ~ 2003년 8월 : 데이콤 정보보호기술팀 팀장
2003년 8월 ~ 현재 : KISA 인터넷침해사고대응지원센터 해킹대응팀 팀장
2004년 ~ 전남대학교 정보보호협동과정 박사과정
관심분야 : MIS, 시스템 & 네트워크 보안 관리, 디지털포렌식 분야



노 봉 남 (Bong-Nam Noh)

1978년 2월 : 전남대학교 수학교육과 (학사)
1982년 2월 : KAIST 대학원 전산학과 (석사)
1994년 2월 : 전북대학교 대학원 전산과 (박사)
1983년 ~ 현재 전남대학교 전자컴퓨터정보통신공학부 교수
2000년 ~ 리눅스 보안 연구센터 소장
관심분야 : 컴퓨터와 네트워크 보안, 정보보호시스템, 전자상거래 보안, 사이버사회와 윤리

안 승 호 (Seungho Ahn)

1977년 2월 : 전남대학교 사범대학 수학교육과 (이학사)
1981년 8월 : 전남대학교 대학원 수학과(이학석사)
1985년 2월 : 전북대학교 대학원 수학과(이학박사)
1987년 12월 ~ 1989년 12월 : 미국 미시간 대학 수학과 방문교수
1983년 5월 ~ 현재 : 전남대학교 수학과 교수
관심분야 : 암호학 분야