한국컴퓨터정보학회 하계학술대회 논문집 제19권 제2호 (2011. 6)

Google Hacking을 통한 정보탈취와 포렌식 자료 생성

이재현°, 박대우*
°*호서대학교 벤처전문대학원 IT응용기술학과
e-mail: leejh9708@paran.com, prof1@paran.com

Hijacking and Forensic Data Generation through Google Hacking

Jae-Hyun Lee°, Dea-Woo Park*
°*Dept. of IT Application Technology, Hoseo Graduate School of Venture

● 요 약 ●

악의적 목적을 가진 Hacker는 Google의 검색 기능과 키워드 사용을 이용해 인터넷 상에 존재하는 개인정보를 탈취하거나 웹 페이지의 취약성, 해킹 대상에 대한 정보들을 수집할 수 있다. Google의 검색 결과 인터넷에서는 수많은 개인정보가 검색되고, 이중에는 타인에게 노출되지 않아야 하는 개인의 이력서, 기업의 기밀자료, 관리자의 ID, Password 등도 인터넷 상에서 보안되지 않은 상태로 존재하고 있다. 본 논문에서는 Google을 이용한 정보검색과 정보탈취에 대해 연구하고, 개인 탈취 정보를 이용한 침해사고와 포렌식 자료 생성에 관한 기술과 보안방안을 제안한다. 본 논문 연구를 통하여 인터넷 검색 결과에 대한 보안 취약성 보완의 기술 발전과 기초자료로 활용될 것이다.

키워드: 구글(Google), 해킹(Hacking), 포렌식(Forensic), 정보탈취(Hijacking)

I. 서론

Google은 최대 검색엔진으로 전 세계 70% 이상의 웹사이트 정보가 Google 데이터베이스에 저장되어 있어 Google의 간단한 검색 키워드와 검색 방법을 알고 있다면 원하는 정보를 빠르고 정확하게 찾을 수 있다. 하지만 악의적 목적을 가진 사람에게 Google의 검색 키워드와 검색 방법과 기능은 개인정보 탈취, 기업의 기밀자료, 관리자의 ID, Password, 해킹 대상에 대한 정보 등 정보들을 불법적으로 수집하는 스캐너 도구가 된다.

특히 Google의 검색엔진을 이용하여 사진, 음악, 영화, 문서, 등 다양한 정보 인터넷에서 획득을 할 수 있다. 이 정보 중에는 공개를 위한 정보도 존재하지만 공개되지 말아야 하는 개인의 이력서, 기업의 기밀자료 등 민감한 정보도 인터넷 상에 존재한다. 따라서 Google 검색엔진을 이용한 정보의 탈취 및 유출의 위협을 증가시킬 수 있다[1].

본 논문에서는 Google 검색엔진을 이용해 정보탈취에 대한 포렌식 증거자료를 생성하고 Google을 이용한 정보탈취 보안방안에 대해 기술한다.

II. 관련 연구

본 장에서는 Google Hacking과 해킹정보로 침해사고가 발생했을 시에 수사를 하기 위한 포렌식에 대해 연구한다.

2.1 Google Hacking

그림 1과 같이 Google은 검색 할 수 있는 범위와 검색 결과가 정확한 전 세계에서 가장 큰 검색엔진으로 알려져 있다. Hacker는 스캐너와 같은 강력한 Google 검색엔진을 이용하여 데이터베이스에 안에 저장된 민감한 정보를 수집하기 위하여 Google 알고리즘을 이용한다. 따라서 검색 시 사용되어지는 기본 검색 옵션 intitle, intext, inurl, link 등을 이용하여 중요 정보에 접근할 수 있다.

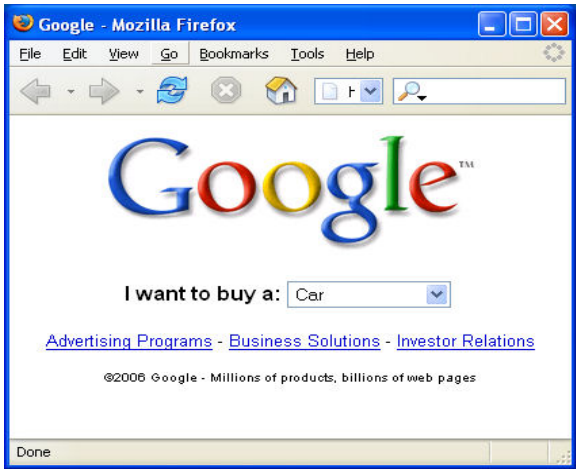

그림 1. Google
Fig. 1. Google

2.2 디지털 포렌식

디지털 포렌식(Digital Forensics)은 법정 제출용 디지털 증거를 수집하여 분석하는 기술을 말하며 인권을 보장하기 위한 수사 방법이다. 일반적으로 디지털 증거는 불가시성, 취급상의 취약성, 대량성이라는 특징이 있는데 이러한 디지털 증거의 증거 수집 단계에서는 현장의 사진을 촬영하고, 압수수색 영장이 허용하는 범위에서 하드웨어, 소프트웨어 등을 압수하여 증거자료를 수집하여 법정에 제출할 수 있다[2].

디지털 포렌식의 절차와 기술은 현장에서부터 연구되어져, 학문적으로 명확한 구분을 하기는 어렵지만 일반적으로 사용 장치와 단말에 따라서 디스크 포렌식, 데이터베이스 포렌식, 네트워크 포렌식, 모바일 포렌식 등으로 구분할 수 있다. 또한 디지털 자료의 추출하는 기법에 따라 휘발성 자료의 추출 기법과 비휘발성 자료를 추출하는 기법으로 구분 할 수 있다[3].

디스크 포렌식은 보통의 컴퓨터에 저장된 자료를 추출하고 분석하는 기법으로 메모리, 하드디스크 드라이브(HDD), USB, CD-ROM 등에 저장된 정보를 추출하는 것이며, 데이터베이스 포렌식은 기업의 전산화가 대형화되고 글로벌 화됨에 따라 기업 중요 기술 DB서버, 회계서버, 메일서버 등에 저장된 정보를 추출하고 분석한다.

네트워크 포렌식은 유선 LAN 등과 무선 WiBro(Wireless Broadband), CDMA(Code Division Multiple Access), GSM(Global System for Mobile communications) 등 유무선 인터넷과 연결된 네트워크에서 발생하는 범죄에 대한 증거를 추출하고 분석하는 것으로 로그분석, 패킷분석, 헤더분석, 접속기록(log), 전송기록 및 전송내용 등에 대한 정보를 추출하게 된다[4][5].

III. Google Hacking을 통한 정보검색과 정보탈취

3.1 Google Hacking을 이용한 정보 검색

Google Hacking은 Google 검색엔진을 이용하여 공격자인 Hacker가 찾고자하는 파일이나, 내용의 결과물을 출력하여 정보를 이용하는 방법이다. 즉 Google에서 제공하는 검색 상세옵션을 이용해서 해당 정보를 검색한다. 검색 옵션은 소문자이며 검색문자열 사이에 빈 공간이 없어야 한다.

본 장에서는 Google을 이용한 정보탈취 과정을 나타낸다. 실험은 intext, intitle, inurl 기본 검색 옵션을 사용하여 정보 탈취 과정을 진행한다.

- intext : 웹페이지 내용 안에 포함되어 있는 글들을 검색할 때 사용
- intitle : 웹 페이지 제목표시줄에 포함되어 있는 글들을 검색할 때 사용
- inurl : 웹페이지에 포함되어 있는 url주소를 검색할 때 사용

그림 2. 이력서 획득
Fig. 2. CV obtained

그림 2는 Google 검색엔진을 이용해 intitle, intext 옵션을 사용하여 이력서를 개인 신상정보인 이력서의 정보를 나타나는 것을 알 수 있다.

그림 3. intitle, inurl 검색어구를 이용한 정보검색
Fig. 3. intitle, inurl search information using search terms

그림 3은 Google 검색엔진을 이용해 intitle:index of/home 이라는 명령어를 사용하여 웹페이지에 저장해 놓은 파일정보를 확인할 수 있다.

Hacker는 자신이 방문한 브라우저의 방문기록이나 검색 기록의 흔적을 나타나지 않게 하기 위해 그림 4처럼 Google Chrome에서 제공하는 시크릿 창을 이용한다. 따라서 자신의 컴퓨터에 검색 기록을 남기지 않음으로서 자신을 보호할 수 있다.

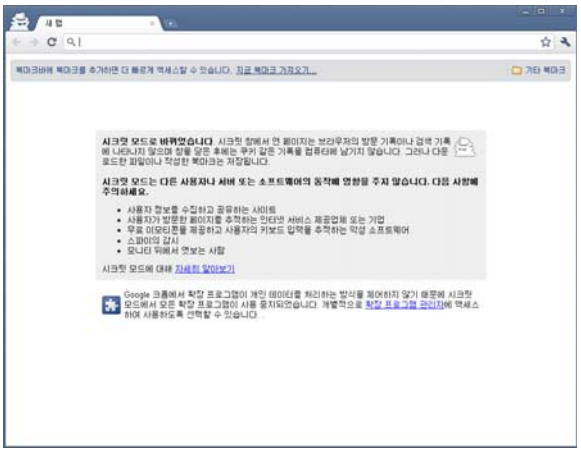

그림 4. Google Chrome 시크릿 창
Fig. 4. Google Chrome Secret Window

본 장에서는 Google을 이용하여 정보탈취 과정을 분석한다. Hacker는 자신이 방문한 브라우저의 방문기록이나 검색 기록의 흔적을 나타나지 않게 하기 위해 Google Chrome에서 제공하는 시크릿 창을 이용한다. 따라서 자신의 컴퓨터에 검색 기록을 남기지 않음으로서 자신을 보호할 수 있다.

3.2 Google Hacking으로 정보 탈취

Hacker는 Google 검색엔진의 검색옵션을 이용해 관리자의 권한을 획득할 수 있는 취약점이 발견되었다.

그림 5. 관리자 정보탈취
Fig. 5. Manager hijacks

그림 5는 inurl:admin을 이용하여 주소에 admin이 포함된 웹사이트를 검색한다. 또한 site 상세옵션을 추가하여 co.kr에 해당하는 페이지를 검색한다.

그림 6. 관리자 권한 획득
Fig. 6. Obtained administrator privileges

검색결과 그림 6과 같이 Password가 저장되어 있어 관리자 권한으로 접속이 가능한 페이지를 검색하게 되었다.

3.3 개인정보 탈취

또한 Google intitle 검색 옵션을 이용해 웹 사이트에 저장되어 있는 ID, 패스워드, 주민번호, 이력서, 전화번호, 메일 등 자료들을 검색 할 수 있다. 그림 7은 웹 사이트 상에 저장되어 있는 자료이다.

그림 7. 개인자료 탈취
Fig. 7. Seize personal data

Ⅳ. 탈취된 개인정보를 이용한 침해사고와 포렌식 자료 생성

탈취된 개인의 정보를 이용하여, 침해사고가 발생하였을 때 증거확보를 위해 포렌식 자료를 생성하여 법적인 책임과 사고에 대응하여야 한다.

4.1 탈취된 개인정보를 이용한 침해사고

Hacker는 개인 탈취 정보를 이용해 관리자 ID, Password를 변경 한다던가 홈페이지의 내용을 변경 할 수도 있다. 또한 금융 정보 취득으로 금전적인 피해를 입을 수도 있다.

다음은 Google Hacking을 통해 웹 페이지의 관리자 권한을 획득한 침해사고에 대한 실험이다.

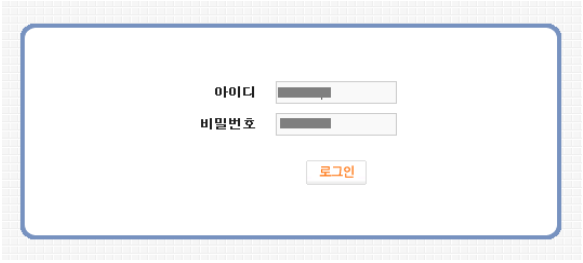

그림 8. 압수수색 포렌식 절차
Fig. 8. Confiscated search the forensic procedure

검색을 통해 그림 8과 같이 관리자 ID, Password를 그대로 들어난 페이지를 검색하였다.

그림 9. 압수수색 포렌식 절차
Fig. 9. Confiscated search the forensic procedure

관리자 권한으로 접속된 화면이다. 따라서 그림 9가입자 정보, 웹사이트 게시물 정보, 금융정도 등 많은 정보를 얻게 되며 또한 변경도 가능하게 되었다.

4.2 압수수색을 통한 포렌식 자료 생성

Google Hacking에 대한 침해사고가 일어났을 경우에 압수수색 절차를 통해 증거자료 확보를 해야 한다.

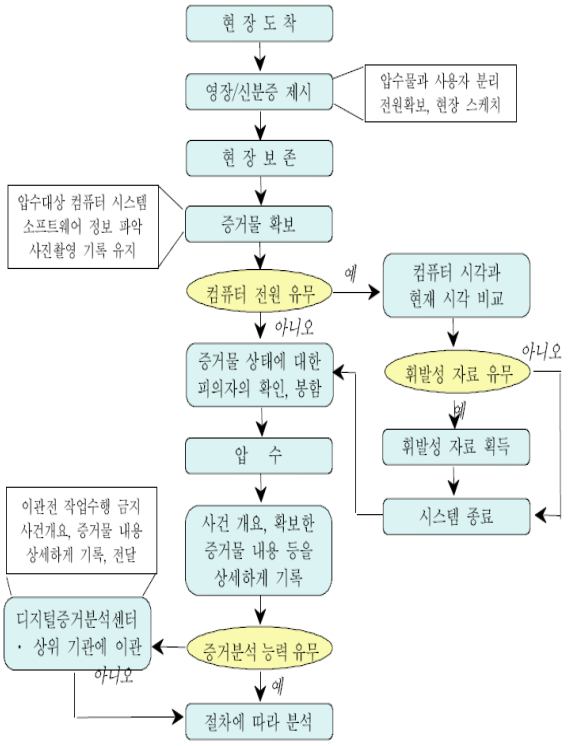

그림 10. 압수수색 포렌식 절차
Fig. 10. Confiscated search the forensic procedure

따라서 그림 10과 같이 현장에 도착 시 현장 보존하여 증거물 확보를 위해 사진 촬영을 하여 수사 기록을 남긴다. 증거물의 상태를 확인하고 압수를 진행하며 증거물의 내용 등을 상세히 기록한다. 증거분석 능력의 유무에 따라 증거분석센터에 이관하기도 한다.

4.2.1 압수수색 영장발부

검찰에서 개인정보 및 기업의 기밀자료 유출에 대한 단서를 포착, 범죄 혐의가 충분한 것으로 보고, 법원에서 압수수색영장을 발부 받기 위해 사건의 중점이 될 자료를 조사 한다. 영장의 내용은 은행거래 내역, 관련자의 침해 웹사이트 기록, 탈취한 기업의 자료, 우편물, 서류철들과, 컴퓨터와 서버 등의 전산 장비 자료를 포함한 압수수색 영장을 청구하여 법원으로부터 압수수색 영장을 발부받는다[6].

4.2.2 압수수색 기획

검찰은 압수수색 날짜 및 인원 편성을 목표인 해당 기업의 본사에 맞춰 편성, 기밀유지에 각별한 주의를 기울이고, 주 압수수색 대상을 본사의 회계 부서 내부와 우편물, 회계 관련 서류들, 컴퓨터 및 전자정보들과 회계 담당자들의 통화 기록, 은행 거래내역 으로 잡고, 원본의 위/변조가 불가능 하도록 전량 압수조치 한다.

4.2.3 증거자료 확보를 위한 압수수색

영장을 제시 한 후 증거자료 확보를 위해 수색한다. 정보 탈취를 담당하는 컴퓨터와 정보 탈취를 위해 작성한 관련 서류 또한 압수 가능하다. 따라서 압수한 자료에 대해 분석하고 전자 정보를

담고 있는 컴퓨터와 드라이브를 수색한다.

4.2.4 증거자료 수집

압수한 컴퓨터와 하드 드라이브 들을 탐색하여 정보 침해 행위를 이루어 졌는지를 확인한다. 또한 포렌식 툴을 이용하여 삭제된 자료가 있는지 확인하고 증거자료가 가능한 정보를 수집한다[7].

4.3 포렌식 증거자료 생성

그림 11. 압수수색을 통한 증거자료 확보
Fig. 11. Confiscated search through securing evidence

그림 11과 같이 압수한 Hacker의 컴퓨터의 상태와 증거물의 무결성을 검증하기 위해 사진촬영을 한다[8].

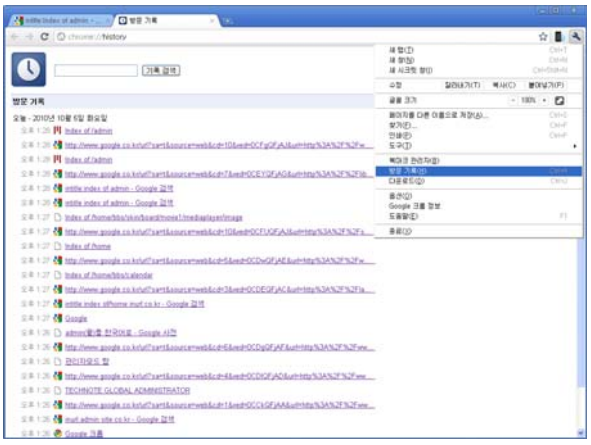

그림 12. 압수수색 포렌식 절차
Fig. 12. Confiscated search the forensic procedure

서버 컴퓨터와 컴퓨터 하드 드라이브 들을 탐색한 결과, 컴퓨터 하드 드라이브들은 정보 탈취 자료가 존재하는지 Google을 이용해 어떠한 웹 사이트에 접근하였는지 방문 기록 로그를 통해 증거자료를 확보한다.

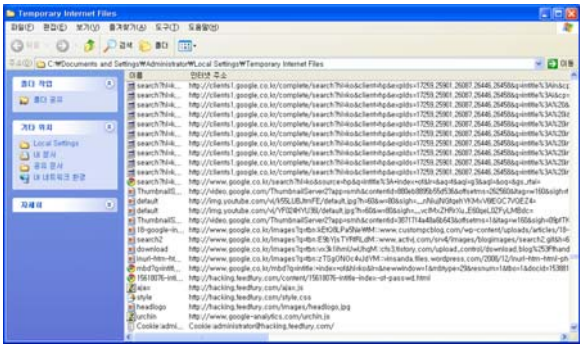

그림 13. 압수수색 포렌식 절차
Fig. 13. Confiscated search forensic procedures

또한 그림 13과 같이 인터넷 파일보기를 통해 사용자의 접근 경로를 알 수 있으며 어떠한 정보를 수집하려고 했는지를 알 수 있다. 만약 사용자가 사전에 방문기록을 삭제하였다면 삭제된 자료를 복구 할 필요가 있는지 결정한 후, 복구할 필요가 있을 경우, 포렌식 도구를 이용하여 자료를 추출함으로써 증거자료의 생성이 가능하다.

V. Google Hacking에 대한 보안 방법

- 관리자는 자신이 관리하는 웹서버에 개인 신상정보 또는 관리자 ID, Password 등의 중요 데이터를 저장해 두지 않는다. 중요 데이터를 저장을 해야 한다면 암호화를 통해 Hacker가 정보를 열람할 수 없도록 한다.
- 개체 인증 이외에 시스템으로 접근하는 모든 device에 인증서를 통하여 접근 하도록 하여 인가된 사용자만이 접근할 수 있도록 한다.
- 사용자, 관리자는 자신에 웹사이트가 Google 검색엔진을 이용하여 검색하였을 때 중요 정보가 얼마나 노출되어지는가에 대한 사전 점검을 통해 보안해야 할 점을 확인하고 정기적인 로그 모니터링을 한다. 또한 중요정보가 검색되었을 때 검색결과의 삭제를 요청한다.
- 사용자 접근 로그를 주기적으로 확인하고 저장하여 침해사고 발생 시 역추적에 대한 포렌식 자료를 생성 하여 증거자료로 제출할 수 있도록 해야 한다.
- 인터넷 상에 정보를 수집하는 검색로봇에 검색을 차단할 수 있도록 명령어를 사용하여 인터넷 상에 정보들이 검색되지 않도록 한다.
- 사용자 접근 로그를 주기적으로 확인하고 저장하여 침해사고 발생 시 역추적에 대한 포렌식 자료를 생성 하여 증거자료로 제출할 수 있도록 해야 한다.
- 개인 사용자는 회원 가입 시 최소한의 정보만을 기입하여 개인정보가 탈취되었을 때 불이익이 발생하지 않도록 해야 한다.

Ⅵ. 결론

타인의 정보를 빼앗으려는 Hacker로부터 정보를 지켜내기 위해서는 보안시스템의 보안성과 정책의 지원도 중요하지만 개개인의 정보보호에 적절한 관리와 지침으로 데이터의 기밀성 및 안정성을 유지하는 것이 중요하다. 인터넷상의 네트워크 시스템들 간의 정보의 공유가 일반화 되고, 사용자에게 편리함을 제공하는 반면, 개개인 혹은 조직의 중요한 기밀 정보들에 대한 접근이 용이하여 정보의 탈취에 대한 보안이 필요하다. 따라서 Google 검색엔진을 이용한 침해사고에 맞는 사전 대책과 사후 대응방안에 대해 연구하였다.

본 논문에서는 Google 검색엔진을 이용한 해킹을 통해 정보가 탈취되는 과정을 분석하여 포렌식 절차에 맞게 법적 증거자료로 제출하기 위한 자료를 생성하고 이에 대한 보안방안을 제시하였다. 따라서 증거자료를 통해 정보 탈취에 대한 법적 처벌이 이루어져야 한다.

향후 연구로는 정보 탈취에 대한 침해를 당했을 때 실시간 역추적을 대한 기술과 포렌식 방법론에 대한 연구에 기여할 것이다.

참고문헌

[1] 이광열, 최윤성, 최해랑, 김승주, 원동호, “현행 증거법에 적합한 디지털 포렌식 절차,” 정보보호학회지, 18(3), 81-91쪽, 2008. 6.

[2] 이창훈, 백승조, 김태완, 임종인, “E-Discovery를 위한 디지털 증거 전송시스템에 대한 연구,” 정보보호학회논문지, 18(5), 171-180쪽, 2008. 10.

[3] 이상복, “디지털 포렌식 업무의 법ㆍ제도적인 개선방향,” 서강법학, 10(2), 139-178쪽, 2008. 12.

[4] 디지털 타임즈, “[알아봅시다] 디지털포렌식(Digital forensic),” http://www.dt.co.kr/contents.html?article_no=2007091702011832718002, 2007. 9.

[5] 김혁준, 이상진, “분석 사례를 통해 본 네트워크 포렌식의 동향과 기술,” 정보보호학회지, 18(1), 41-48쪽, 2008. 2.

[6] 이규안, 박대우, 신용태, “포렌식 자료의 무결성 확보를 위한 수사현장의 연계관리 방법 연구,” 한국컴퓨터정보학회논문지, 11(6), 175-184쪽, 2006. 12.

[7] 서계원, “정보 프라이버시와 개인정보의 보호 -개인정보보호 기본법안을 중심으로-,” 국제헌법학회, 11, 195-232쪽, 2005.

[8] 이월영, 황철, “멀티미디어 정보보호 : 컴퓨터 포렌식을 위한 디지털 저작권 보호시스템 개발,” 한국멀티미디어학회, 10(3), 365-372쪽, 2007.