통신사 홈페이지 해킹을 통한 개인정보유출 사고 포렌식 연구

노정호* · 박대우**

*호서대학교 벤처전문대학원

A Study on Website Operators Privacy Breaches through Hacking Forensic Research

Jung-Ho Noh* · Dea-Woo Park**

*Hoseo Graduate School of Venture

E-mail : network87@daum.net · prof_pdw@naver.com

요 약

디지털 포렌식은 사고 발생 시 시스템 파일을 복원 하여 증거 자료를 찾는 유일한 수단이며 지금 일어나고 있는 KT 홈페이지 해킹, 카드사 3사 개인정보 유출 및 최근 일어난 스킨푸드 홈페이지 가입 고객 정보 유출 등 이러한 범죄를 저지른 해커를 찾기 위한 유일한 수단이기도 하다. 본 연구에서는 KT 홈페이지 해킹 공격에 시도한 우회 프로그램 및 자동화 프로그램을 활용하여 해킹을 시도했을 경우 어떤 정보가 유출 되었는가에 대한 실험과 이렇게 홈페이지 공격을 당 했을 경우 어떻게 포렌식을 해서 해커에 대한 증거 자료를 찾은 후 보고서를 만들 수 있는지에 대해 기술한다.

ABSTRACT

Digital Forensics in the event of an accident, the system restore files and the only way to find evidence KT Website hacking happening now, credit card companies, and leakage of personal information by three recent spills occurred, such as Skin Food Home Up Customer Information hackers to find these crimes only means as well.

This study attempted to bypass the KT website hacking attacks utilizing automated programs hacking programs, and if you try to experiment on whether any information has been disclosed and if so what home attacked forensics evidence for hackers to locate the can make a report is described

키워드

KT 고객정보 유출, 홈페이지 해킹, 개인정보 유출, 해킹공격, 취약점, 포렌식

Key word

KT Client Personal Information Leak, Homepage Hacking, Personal Information Leak, Hacking Attack Vulnerability, Forensic.

Ⅰ. 서 론

2013년도 6월 25일 청와대 홈페이지에 대한 DDoS 공격이 있었다[1].

홈페이지에 대한 해킹 공격은 계속되고 있다. 그 중에 KT 홈페이지 해킹공격을 통하여 2013년 2월부터 2014년 2월까지 KT 고객정보 1,200만 건을 유출하여 휴대전화 영업에 활용한 협의로 해커 김씨가 구속 되었다.

KT 고객정보 1,200만 건 유출사고는 해커 김모씨의 자동화 프로그램과 KT 홈페이지 취약성으로 인한 것이며 그 결과 해킹 공격에 의한 홈페이지 취약점 분석은 물론, 법적 손해 배상과 책임을 위해 포렌식 연구가 필요하다. 따라서 KT 해킹공격 사건을 분석하고 법적 책임에 대한 증거자료로서 포렌식 연구가 필요하다. 본 논문에서는 KT 홈페이지 해킹공격 패턴을 분석 후 실제 다른 홈페이지 에서 메시지 변조 및 메시지를 가로챈 후

ID/Password가 유출 되어 해킹 피해를 입는 과정에 대해 알아보도록 한다.

II. 관련연구

2.1 홈페이지 해킹공격 기술

홈페이지 구성을 변경하여 로그인 세션이 없는 경우에는 외부의 다른 서버로 트래픽을 유도하여 정상적인 웹페이지 호출 구분하는 방법을 DDoS 공격 유형에 따라 제시한다. 정상적인 웹페이지 호출인 것으로 가장하여 웹서버에 연결된 DB서버의 Overhead 증가시키는 공격도 존재한다.

침해사고는 시스템 해킹, 바이러스 및 웜, 홈페이지 변조[2], 자료 유출 등 그 유형이 다양하고, 단순한 바이러스나 웜 등의 유포가 아닌 개인정보 및 기업기밀 정보를 취득하거나 금전적 이득을 취하기 위한 목적으로, 공격자가 사용하는 공격 기법이 고의적인 데이터의 삭제나 변경 등 고도의 은닉 기법을 활용하여 흔적을 남기지 않기 때문에, 정확한 자료를 수집하기가 쉽지 않다. 침해사고 초기 대응 시 초동 대응자는 신속한 조사를 수행해야할 필요가 있는 침해위협 또는 범죄와 관련 현장 정보를 취급한다, 이때 체계적인 증거 수집을 위하여 침해사고의 식별에 적합한 디지털 포렌식 프로세스 방법론의 적용이 요구된다.

2.2 포렌식 기술

GM대우차와 쌍용차에 관한 기술 유출 사고에서의 국가 경제적인 피해로 인하여 포렌식 e-Discovery 제도가 필요하다. e-Discovery가 도입되면 포렌식 자료를 확보하기 위한 보안관제시스템에서 증거 자료의 확보가 가능하다[3].

인터넷 이용자의 74%가 UCC를 이용하고 있고, You Tube를 이용한 총기범죄가 발생하였다. 인터넷 UCC속에 나타난 인터넷 범죄의 양태를 분석하고 추적하는 네트워크 Forensic 방법과 기법에 대한 기술이 필요하다[4].

DDoS 공격과 APT 공격은 좀비 컴퓨터들로 정해진 시간에 동시에 공격을 가하여 사회적 혼란을 유발하였다. 이러한 공격에는 공격자의 명령을 수행하는 많은 좀비 컴퓨터들이 필요하며 좀비 컴퓨터에는 안티바이러스 제품의 탐지를 우회하는 알려지지 않은 악성코드가 실행되어야한다. 그동안 시그니처로 탐지하던 안티바이러스 제품을 벗어나 알려지지 않은 악성코드 탐지에 많은 방법들이 제안되어 왔다. 본 논문은 디지털 포렌식 기법을 활용하여 알려지지 않은 악성코드 탐지 방법을 제시하고 정상 파일과 악성코드의 다양한 샘플들을 대상으로 수행한 실험 결과에 대하여 기술한다[5].

휴대폰에서 포렌식 증거 자료를 추출하는 방법은 SYN, JTAG, Revolving 3가지 방법[6]이 있다. 하지만 휴대폰과 스마트폰의 기술과 사용방법의 차이로 인하여, 포렌식 증거 자료를 추출하는 방법도 달라야 한다. 따라서 본 논문에서는 압수 수색된 스마트폰에서의 포렌식 증거 자료의 추출 방법을 연구하고자 한다. 압수 수색된 스마트폰에서 많이 사용되는 구글 안드로이드와 윈도우모바일 스마트폰의 분석을 위하여 스마트폰의 사양과 운영체제, 백업 분석, 증거 자료를 분석 한다. 또한 구글 안드로이드와 윈도우모바일 스마트폰의 전화번호부, SMS, 사진, 동영상에 관한 포렌식 증거 자료를 추출하여 법적인 증거자료와 포렌식 보고서를 생성한다.

III. KT 홈페이지 해킹공격 분석

3.1 KT 홈페이지 해킹 공격 사고 배경

해커는 Paros Program이라는 신종 프로그램을 개발하여 2013년 2월부터 KT 홈페이지를 로그인하여 다수의 고객 정보를 빼내었다. 이 과정에서 해커는 하루에 평균 20만건 정도 개인정보를 탈취 하였으며 이들은 각 고객들의 이름, 주민번호, 집전화, 집주소, 계좌번호 등을 이용하여 KT 직원으로 가장하여 핸드폰(?)을 판매와 더불어 약1,200만건의 개인정보는 다른 지점에 팔아서, 부당 이익을 챙긴점으로 구속되었다.

범죄에 공모한 해커 2명은 구속된 상태이며, 조사 결과 115억 이상의 부당이익을 챙긴 것으로 조사된다.

KT 정보유출 확인, 아직 확인 안 돼..피해자 '답답'

OSEN= 정지량 기자 I 2014.03.10 08:55

KT 정보유출 확인이 화제다.

지난 6일 KT의 홈페이지가 해킹 돼 1200만 명의 개인정보가 유출된 사실이 경찰조사 결과 드러났다. KT는 사과문을 통해 "6일 경찰에서 발표한 고객정보 유출 사고와 관련 고객 피해 최소화를 위해 노력하겠다"며 "KT는 정보 유출경위에 대해 경찰조사에 적극 협조하여 사실관계를 확인할 계획"이라고 밝혔다.

하지만 경찰수사 결과 이용대금 명세서의 고유번호 9자리로도 고객 정보를 확인 할 수 있는 등 KT의 보안시스템이 허술한 것으로 드러나 KT를 향한 국민들의 공분이 쉽게 가라앉을 것으로 보이지는 않는다. 경찰은 KT 보안담당자의 고객정보 관리 소홀 여부에 관해 추가 수사를 진행할 계획이다.

그림 1. KT 개인정보 유출 기사

3.2 KT 홈페이지 취약점을 이용한 공격분석

해커 김모씨가 해킹공격을 위하여 사용한 Paros Program은 웹 페이지를 변조 할 수 있는 기능이 있다. 우회한 웹 페이지에 응답 메시지를 해커가 변조를 하면 웹 페이지에 내용을 변경 할 수 있는데 이러한 행위들은 Client에서 동작하기 때문에 사용자들이 보는 변조된 웹 화면은 일반인들이 구분하기가 어렵다.

그림 2와3은 파로스 프로그램으로 변조해도 아

무런 영향이 없다는 증명하기 위한 화면이다.

```
lass="search_link">
pan class="blind">질문형 검색어</span></h3>
"qu_txt">
cript">var qst_idx=0; var qst_size=1;</script>
search.naver.com/search.naver?sm=top_txt&amp;where=nexearch&amp;ie=utf8&amp;query='
', '', event, 1);" title="호서벤처대학원 융합공학과">'호서벤처대학원 융합공학과</a></span>
ref="http://news.naver.com/main/hotissue/sectionList.nhn?mid=hot&amp;sid1=102&amp;gid=
```

그림2. 파로스 프로그램을 이용한 메시지 변조

그림 3. 메시지 변조 후 네이버 실시간 화면

3.3 KT 홈페이지 개인 정보 유출 과정

해커 김모씨는 KT 홈페이지의 취약성을 이용하여 특정 파라미터를 변조하여 공격 방법 기법을 이용 하였으며 이 공격을 이용한 접근 방법은 Paros Program을 사용하여 우회 접속하고 김씨가 개발한 랜덤생성 프로그램을 만들어 취약한 홈페이지에 이용대금 9자리 고유번호를 유추하는 형식을 반복하여 개인정보의 이름/주민번호/집주소/전화번호/계좌 등 취득 하였다.

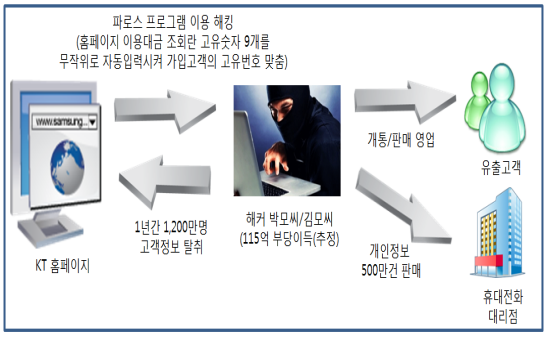

그림 4. KT홈페이지 해킹 개인정보 유출 흐름도

Ⅳ. 홈페이지 해킹공격 포렌식

4.1 홈페이지 취약점 포렌식

이번 취약점 실험을 위해 호서대학원 융합공학과 홈페이지를 타켓으로 실험 하였으며 아래 그림은 파로스 프로그램을 이용하여 Login 정보 메시지를 가로챈 화면이다.

```
<td width="80"><input type=text name='mb_id' size=20 maxlength=20 minlength=2 required itemname='아이디' class=input></td>
</tr>
<tr>
<td width="55"><img src="../skin/member/default/img/ico_pass.gif"></td>
<td><input type=password name='mb_password' size=20 maxlength=20 required itemname='비밀번호' class=input></td>
</tr>
<tr><td></td><td><input type="checkbox" name="auto_login" value="1" onclick="if (this.checked) { if (confirm('자동로그인을 사용하시면 다음
부터 로그인 하실 필요가 없습니다.\n공공장소에서는 개인정보가 유출될 수 있으니 사용을 자제하여 주십시오.\n\n자동로그인을 사용하시겠습니까?')) { this.checked = true; } else { this.checked = false; } }">자동로그인</td></tr>
```

그림 5 . 홈페이지 로그인 취약 소스코드 탈취

4.2 홈페이지 해킹공격 포렌식

아래 그림은 Paros로 융합공학과 홈페이지 접근 후 Response(응답)패킷을 가로채면 아래 그림6 같이 사용자 로그인 정보가 있는 Post.mb_login를 볼 수 있다.

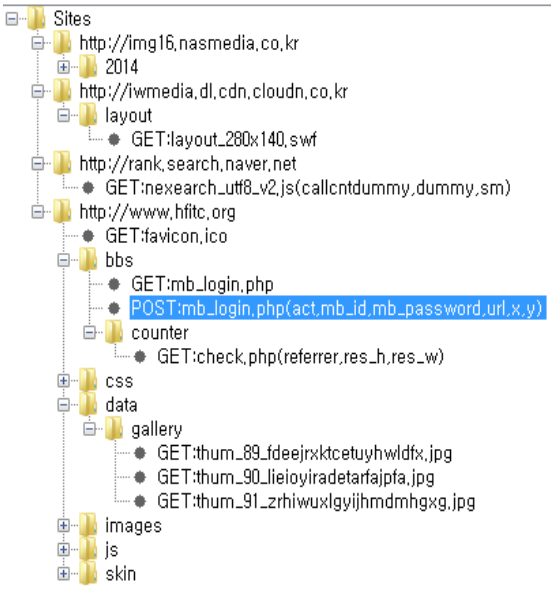

그림 6 . Post Mb_Login 메시지 화면

4.3 홈페이지 개인정보유출 포렌식

그림5와 같이 홈페이지 취약점이 있는 융합공학과 홈페이지를 타켓으로 그림6의 Post:mb_login의 패킷들을 분석하다 보면 아래 그림7처럼 ID와 Password가 그대로 노출 된 것을 볼 수 있다.

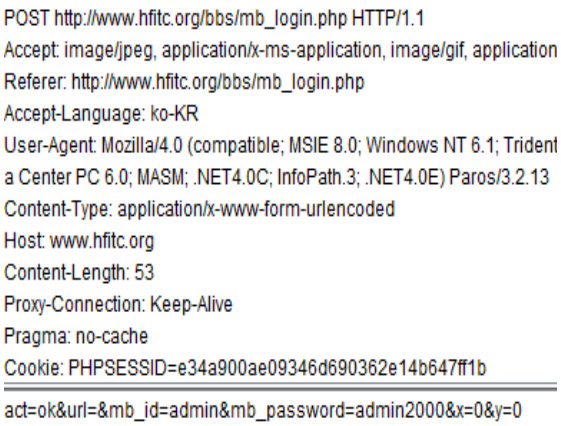

그림 7. 홈페이지 ID/Password 노출 화면

Ⅴ. 결 론

본 실험처럼 KT 개인정보 유출과 같이 호서대학학원 융합공과학과 홈페이지의 취약성을 밝혀냈으며 이 실험을 통해 유추 할 수 있는 상황으로 다른 사이트들도 웹 페이지 만들었을 시 암호화로 적용을 안 한 사이트일 시 파로스 프로그램을 이용하여 누구나 해킹이 가능 할 것으로 판단되며 이러한 피해를 줄이기 위해서 정부에서 주도하여 이런 취약 사이트를 점검 후 취약 웹 사이트에 암호화를 적용해야 개인 사이버 자산을 보호 할 수 있다고 판단 된다.

향후 연구로는 이런 악의적인 프로그램 사용에 대한 로그분석을 통해 찾는 과정 및 악성 행위에 대한 포렌식 보고서를 작성하는 방법을 연구 할 것이다.

참고문헌

[1] Hong-Il Kim, “A defense method of Distributed Denial of Service attack in restrictive traffic environments” Korea, Entertainment Industry Association, Vol.4, No.1, pp.19-24, 2010.

[2] SeungWon Lee, YoungSup Noh, Changwoo Han, “A Study on the Design and Implementation of an Digital Evidence Collection Application on Windows base computer” Journal of The Korea Institte of Information Security and Crytology, Vol.23, No.1, pp.57-69, 2013.

[3] Woo Sung Chun, Dea-Woo Park, “A Study of Authentication and encryption for e-Discovery Forensic Data” The Korea Society of Computer and Information, Vol.19, No.2, pp.185-189, June, 30, 2011.

[4] Kyu Ahn Lee, Dea-Woo Park, Yong Tae Sin, “A Study of Network Forensics related to Internet Criminal at UCC”, Journal of the Korea society of computer and information, Vol.13, No.2, pp.143-151, 2008.

[5] Jaeho Lee, Sangjin Lee, “A Study on Unknown Malware Detection using Digital Forensic Techniques”, Journal of The Korea Institute of Information Security and Cryptology, Vol.24, No.1, pp.107-122, 2014.

[6] Kyung-Bae Yoon, Woo-Sung Chun, Dea-Woo Park, “Forensic Evidence of Search and Seized Android and Windows Mobile Smart Phone”, Journal of the Korea Institute of Information and Communication Engineering, Vol.17, No.2, pp.323-331, 2013.