스마트폰에서 Smishing 해킹 공격과 침해사고 보안 연구

박인우, 박대우*

호서대학교 벤처전문대학원

A Study of Intrusion Security Research and Smishing Hacking Attack on a Smartphone

In-Woo Park, Dea-Woo Park*

Hoseo Graduate School of Venture

E-mail : cowboyiw@daum.net, prof_pdw@naver.com

요 약

2013년도 들어 스마트폰을 이용한 스미싱(Smishing) 해킹 공격으로 인하여 피해가 급증하고 있다. 스미싱 해킹공격과 연계된 직접적인 금전적 피해와 개인정보 탈취가 야기되고 있다. 스마트폰에서 스미싱 해킹 공격과 연계되어 안전결제 시스템(ISP)과 인터넷 결제서비스로 이어지는 금전적인 피해가 발생하고 있다. 본 논문에서는 스미싱 해킹 공격과 침해사고를 실제 사례를 실험실에서 연구분석 한다. 스미싱 해킹 공격의 기술적인 원리와 실제적인 사례 분석을 하고, 스미싱을 이용한 안전결제 시스템의 피해를 예방하는 보안 방법을 강국한다. 본 연구를 통해 스마트폰을 통해 보다 안전하고 편리하게 온라인 결제를 할 수 있도록 하는 연구가 될 것이다.

ABSTRACT

Damage is increasing by (Smishing) hacking attack Smishing you use a smart phone after entering 2013. Takeover of personal information and direct financial damage in collaboration with graphics sewing machine hacking attack has occurred. Monetary damage that leads to Internet payment service (ISP) and secure payment system in conjunction with graphics sewing machine hacking attack on a smartphone has occurred. In this paper, I will study analysis in the laboratory examples of actual infringement vinegar sewing machine hacking attack. It is a major power security measures to prevent damage to the secure payment system that a case analysis and practical principle technical nest sewing machine hacking attack, using Smishing. In this paper, I will be to research to be able to through a smart phone, to the online payment safer and more convenient.

키워드

스미싱, 안전결제(ISP), 해킹 공격,

Key word

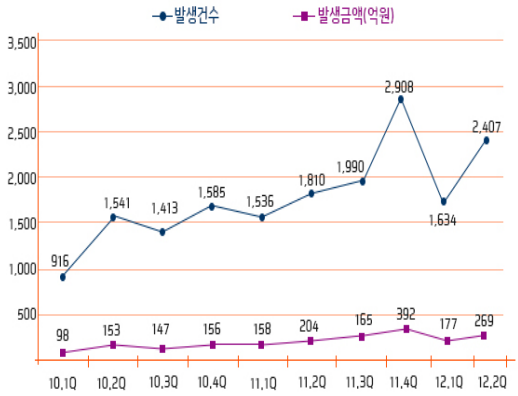
Smishing, Secure Payment(ISP), Hacking Attack,

Ⅰ. 서 론

스미싱(Smishing) 사고는 단문자서비스(Short Message Service)와 피싱(Phishing)의 합성어로, 2013년도부터 급속하게 사회문제화가 되기 시작하였다. 스마트폰을 이용하여 공격자는 피싱 사기를 유도하고, 스마트폰상으로 개인정보를 빼내거나, 본인도 모르게 소액결제를 하게하는 신종 휴대폰 사기 수법이다(출처 : 경찰청 사이버 테러대응센터). 휴대폰 또는 스마트폰에서 웹사이트 링크에 접속하려는 피해자는 바이러스 퇴치를 위한 애플리케이션을 무료로 다운받을 것을 권고 받게 되나, 이 파일에는 트로이 목마 바이러스가 포함되어, 다운로드 즉시 해커의 조종으로 개인정보가 유출되어 버린다.

2010년도부터 사회문제화 되기 시작한 피싱 공격은 표 1과 같이 국내에서 보이스 피싱으로 인한 피해가 급증하였다. (출처 : 금융감독원).

표 1. 보이스피싱 피해(2010. 6)
(출처 : 금융감독원)



이와 같이 스마트폰 사용자들이 금융거래가 급증하면서, 피싱 사고로 인한 피해가 급증하였고, 피싱 공격이 진화한 형태로 스미싱 해킹 공격을 통한 금융피해 피해사례가 늘어나고 있다.

따라서 개인정보 유출에 의한 개인정보보호법의 준수와 스미싱을 이용한 급격한 금융피해가 발생함에 따라 스미싱 공격과 안전결제 피해를 가져오는 스미싱 해킹공격을 분석하고 연구하여, 안전한 스마트폰 사용을 위한 보안대책을 제시할 필요가 있다.

본 논문에서는 스미싱을 이용한 해킹공격에 대한 금융결제 피해를 연구하고, 스미싱 사고에 대한 보안강화를 위한 대책을 연구한다.

Ⅱ. 스미싱 사고와 해킹 공격 사례

2.1 스미싱 사고와 해킹 공격

스미싱은 SMS와 Phishing의 결합어로 문자메시지를 이용 피싱하는 방법을 말한다. 이 기법을 사용하는 해커는 스마트폰과 같은 (이동)통신단말기 사용자에게 웹사이트 링크를 포함한 문자메시지를 보내고, 스마트폰 사용자가 웹사이트에 접속하면, 트로이목마 등 공격 툴을 사용자 모르게 주입하여 인터넷 사용이 가능한 스마트폰을 통제할 수 있게 된다. 불특정 다수에게 지인으로 가장하여 스마트폰에서 문자메시지를 이용, 사용자의 단말기에 애플리케이션으로 위장한 트로이목마를 설치하는 해킹 기법이다[3].

스미싱 공격 기법을 사용하는 공격자 해커는 그림 1과 같이 사용자에게 웹사이트 링크를 포함한 문자메시지를 보낸다. 해커는 휴대폰이나 스마트폰 사용자가 웹사이트에 접속하면 트로이목마를 사용자 스마트폰에 설치해 인터넷 사용이 가능한 휴대폰이나 스마트폰을 통제할 수 있게 된다.

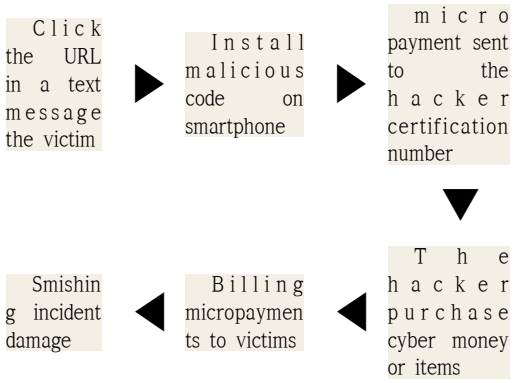


그림 1. '스미싱' 피해 단계*

2.2 스미싱 해킹 공격 사례

스마트폰사용이 늘어남에 따라 스마트폰 해킹의 위협 또한 갈수록 커지고 있다[4].

스미싱을 이용하는 해킹공격 사례는 그림 2와 같이 SMS로 호기심을 자극할만한 문구를 쓴 뒤 악성코드가 숨겨진 인터넷 URL을 함께 보내오는 경우이다.

2013년 9월 2일 스미싱 공격자가 스마트폰 사용자에게 지인으로 가장하고 보낸 공격기법은 모바일 돌잔치 초대장을 링크한 경우로 문자링크를 선택(누르는)하는 순간, 사용자의 금융계좌에서 소액결제와 연계된 금액이 해커의 대포통장으로 인출된다. 또한 그림 2와 같이 2013년 9월 10일 [법원]에서 등기가 발송되었으나 사용자가 부재하여 전달을 못하였으니, 조회해 보라는 내용으로, 사용자가 선택(누르는)하는 순간, 사용자의 금융계좌에서 소액결제와 연계된 금액이 해커의 대포통장으로 인출된다.

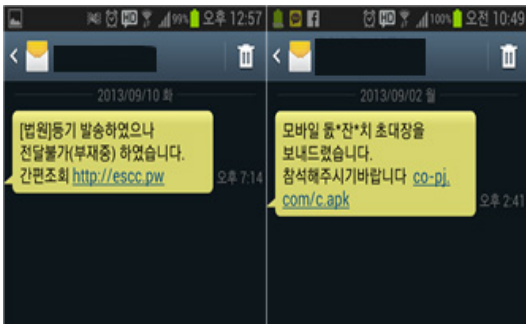


그림 2. 스미싱 해킹 공격 사례

Ⅲ. 스미싱 해킹 공격 분석

3.1 스미싱 해킹 공격 분석

해커가 스미싱 공격을 위해 사용자에게 보낸 SMS를 통하여 설치한 악성 애플리케이션을 실행시키면 그림 3과 같이 “점검시간입니다. 불편을 드려서 죄송합니다” 라는 문구로 가장하여 사용자를 안심시키고 실제로는 악성코드가 설치되어 SMS 탈취 서비스가 동작하고 있다[6].

그림 3. 스미싱의 SMS를 통한
애플리케이션(음악) 설치 후 실행 화면(

스미싱 공격의 피해 원리는 해커는 SMS/MMS 등과 같이 메시지를 공격목표 사용자에게 보내고, 공격목표 사용자가 첨부된 링크를 클릭하게 되면, 악성코드가 포함된 애플리케이션을 다운로드 된다.

해커는 그때부터 사용자가 눈치 채지 못하게, 스마트폰에 트로이목마와 같은 악성코드를 배포하여, 악성코드나 악성애플리케이션을 통해 사용자 스마트폰의 문자, 수신알람, 카메라, 전화번호, 금융정보, 개인정보 등과 같은 스마트폰의 기능을 제어하면서 정보를 절취하게 된다. 절취된 사용자의 개인정보를 이용하여, 사용자를 가장한 금융결제를 통해 금전적 손실을 입히도록 하는 원리이다.

3.2 스미싱 해킹 공격 Process 분석

그림 4는 androapkinfo.py 툴을 이용하여 smishing.apk의 API권한을 살펴본 모습이다.

```
#./androapkinfo.py -f /root/Desktop/smarbilling.apk

생략..

PERMISSIONS:
        android.permission.RECEIVE_BOOT_COMPLETED ['normal', 'automatically start at boot', 'Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.']
        android.permission.READ_PHONE_STATE ['dangerous', 'read phone state and identity', 'Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.']
        android.permission.ACCESS_NETWORK_STATE ['normal', 'view network status', 'Allows an application to view the status of all networks.']
        android.permission.RECEIVE_MMS ['dangerous', 'receive MMS', 'Allows application to receive and process MMS messages. Malicious applications may monitor your messages or delete them without showing them to you.']
        android.permission.WAKE_LOCK ['normal', 'prevent phone from sleeping', 'Allows an application to prevent the phone from going to sleep.']
        android.permission.RECEIVE_SMS ['dangerous', 'receive SMS', 'Allows application to receive and process SMS messages. Malicious applications may monitor your messages or delete them without showing them to you.']
        android.permission.INTERNET ['dangerous', 'full Internet access', 'Allows an application to create network sockets.']
        android.permission.WRITE_EXTERNAL_STORAGE ['dangerous', 'modify/delete SD card contents', 'Allows an application to write to the SD card.']

생략..
```

그림 4. Smishing.apk의 API권한의 소스

androapkinfo.py에서 확인한 API권한 정보를 보면 알 수 있듯이, android.permission.INTERNET, android.permission.Receive_MMS, android.permission.RECEIVE_SMS, android.permission.READ_PHONE_STATE, android.permission.WRITE_EXTERNAL_STORAGE API 권한이 악의적으로 사용될 수 있는 API이다. 즉 APP이 SMS/MMS를 조작할 수 있는 권한, APP이 인터넷에 액세스할 수 있는 권한, APP이 개인 정보에 액세스할 수 있는 권한인 것이다[5].

해당 악성 애플리케이션을 사용자의 스마트폰에 설치하게 되면 그림 5와 같이 빨간색 표시된 해커의 URL로 스마트폰 사용자의 중요정보가 해커의 서버로 전달되게 된다.

```
public int a(String paramString1, String paramString2)
{
  a("------------PostMsm 1");
  if (this.b.a("CMD_GETTIME"))
  {
    b("register->register request is exist!");
    return -1;
  }
  HashMap localHashMap = new HashMap();
  localHashMap.put("sn", paramString1);
  localHashMap.put("sbody", paramString2);
  this.c = 1;
  return this.b.a("CMD_GETTIME", "http://210.209.72.103/u_news.asp", localHashMap);
}
```

그림 5. 해커에게 사용자의 정보의 전달

그림 6은 패킷 분석 툴 Wireshark을 통하여 패킷을 분석한 결과, 해커의 서버로 스마트폰 사용자의 시리얼 번호가 전송되는 것을 확인할 수 있다.

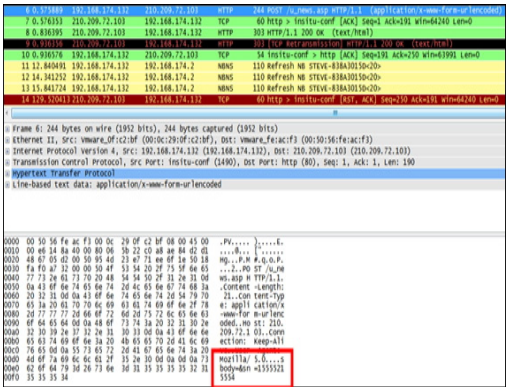


그림 6. 해커의 서버로 스마트폰 사용자의 시리얼 번호 전송

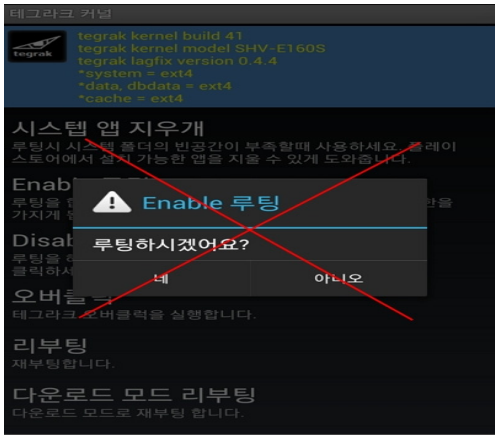


그림 7. 사용자 스마트폰 루팅 금지

Ⅳ. 스미싱 공격에 대한 보안대책

공격자인 해커로 부터 스미싱 공격이, 스마트폰 사용자들에게 금융피해를 야기시키는 문제가 사회적 이슈가 되고 있어, 스미싱 공격에 대한 보안대책을 강구해야 한다.

본 논문에서는 소극적인 보안대책으로 스마트폰 사용자에 대한 보안대책과, 적극적인 보안대책으로 통신사와 정부측에 대한 보안대책을 연구한다.

4.1 스마트폰 사용자 측 보안대책

- 발신처가 명확하지 않은 곳으로부터 전달되는 문자메시지의 단축URL은 클릭하지 않음. 클릭을 하였더라도 애플리케이션을 설치하라고 하는 경우에는 설치하지 않는다.
- 신뢰할 수 있는 보안업체에서 제공하는 모바일 백신을 설치하고 실시간 감시 기능을 활성화 한다.
- 평소에 스마트폰을 통한 소액결제를 자주 이용하지 않는다면, 자신이 사용하는 통신사 고객센터나 공식 홈페이지를 통해 “휴대폰 소액결제 서비스를 미리 차단 해두거나 통신사 홈페이지에서 소액결제 한도를 0원으로 변경한다.
- 그림 7과 같은 안드로이드에서 루팅이나 아이폰에서 탈옥을 사용하여 관리자 권한을 변경하지 않아야 상대적으로 보안성이 강화된다. 탈옥이나 루팅을 하면 일반 사용자보다 여러 기능을 사용할 수는 있지만, 스마트폰을 안전하게 지켜주는 관리권한을 외부로 노출시키게 되어 그만큼 해킹 위험도 증가한다.
- 마지막으로 스마트폰 사용자들은 ① 환경설정 -> ② 보안 -> ③ 디바이스 관리 ->④ 알 수 없는 출처에 체크가 되어 있을 경우 해제를 하여 스마트폰의 보안설정을 강화할 수 있다.

이와 같은 보안대책을 사용자의 스마트폰에 적용하여, 스미싱 해킹공격으로부터 금융피해를 예방할 수 있다.

4.2 통신사 측 보안대책

해커에게 스미싱 공격을 당했더라도 그림 8과 같이 각 통신사 고객센터 또는 통신사 인터넷 홈페이지를 이용하여 휴대폰 소액결제를 원천적으로 차단을 하면 방지할 수 있다[7].

한국에서 안전결제를 이용한 스미싱 해킹 공격으로부터의 3사 통신사들의 보안대책은 다음과 같다.

- 스미싱 피해 발생시 인터넷 결제 대행사는 컨텐츠 공급자와 협의해 결제를 취소한다.
- 게임 아이템 회사들과 협력해 1회 결제 한도나 월간 결제 한도를 축소한다.
- 게임 아이디당 결제 가능 회선(이동통신 번호)을 2회선으로 제한한다.
- 동일 IP에서 복수 소액 결제 발생시 인터넷 결제 대행사가 해당 IP 결제를 차단한다.
- 고객센터에서 URL을 신고 받아 스팸 필터링시스템에서 접속을 차단한다.
- 요금 고지서나 온라인 고객센터를 통해 악성코드 위험과 관련한 고객에게 고지한다.
- 소액결제 시 비밀번호(Carrier Pin)을 이용하도록 결제시스템 개선한다.
- 스마트폰 신규가입시 발송하는 SMS에 소액결제 이용한도 포함하여 고지(적용 예정)한다.
- 스미싱 피해자가 경찰로부터 ‘사건사고 사실확인

원’ 을 발급받아 제출하면 결제청구를 보류·취소 한다.

- 이미 사기 금액을 지불한 경우, 이동통신사 접수 후 2주 이내에 청구서가 발급되지 않았을 경우, 월말 청구서 발급 시까지의 피해를 구제 한다.

.

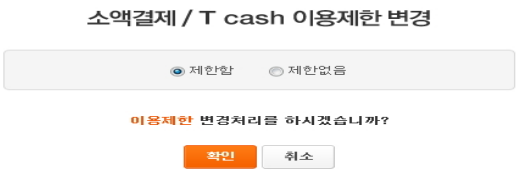


그림 8. 소액결제 이용제한 변경

4.3 정부 측 보안대책

- 2013년 하반기부터 국내에서 신규 출시되는 모든 스마트폰에 백신을 기본적으로 자동실행 상태로 출고하도록 한다.
- 현재 국내 스마트폰 제조사들이 자사 단말기에 백신을 기본으로 탑재하고 있으나 이용자의 선택권 제한, 내장 배터리 소모 가능성 등의 사유로 비활성화 상태로 출고한다.
- 한국인터넷진흥원과 함께 피싱 대응센터를 운영하여 대국민 금융피해를 줄이기위한 노력을 한다.
- 검찰, 경찰, 우체국, 은행, 보험 등 1,135개 주요기관 57만여개 전화번호 수집 후 데이터베이스(DB)화 하여 통신사에 제공한다.
- 통신사, 전기통신망의 전화교환기나 SMS서버 등에서 공공기관 전화번호를 사칭하는 경우를 판별할 수 있도록 하는 시설에 투자한다.
- 스마트폰 해킹공격으로 인한 개인정보 유출 및 소액결제 대책을 마련한다.
- 제조사와 협조하여 해킹 피해 축소 및 개인정보보호를 위한 대책 마련한다[8].

Ⅴ. 결 론

2013년 스미싱 해킹공격으로 인한 스마트폰 사용자들의 피해사례가 급증하고 있고, 소액결제 등을 이용한 직접적인 금전적 피해와 개인정보 탈취를 야기하고 있다. 이에 대비하기 위해 스미싱 해킹 공격의 사례와 Process을 분석하고, 사용자 보안대책, 통신사 보안대책, 정부측 보안대책을 연구 분석 하였다.

향후 연구에서는 해킹 가능성이 많은 QR코드를 이용한 사고 분석과 금융 피해가 발생하는 사례에 대한 연구가 필요하다.

참고문헌

[1] 한국경제, “안전결제 해킹 ’충격’, 피해액 1억 8천…게임사이트 정보 도용“, http://www.hankyung.com/news/app/newsview.php?aid=201212042411x&ltype=&nid=&sid=010610&page=1&rss=r, 2013년.

[2] TATTER&MEDIA, “급증하는 스미싱 피해, 올바른 대처 방법은? “ http://logfile.tistory.com/1340?_best_tistory=trackback_bestpost, 2013년.

[3] 경찰청 사이버 테러대응센터, “스미싱의 대처방법”, http://www.netan.go.kr/, 2013년.

[4] 박대우, 서정만, ’Phishing, Vishing, SMiShing 공격에서 공인인증을 통한 정보침해 방지 연구’, Vol 12, No 2, pp. 171-180, 2007년.

[5] TickTalk, ’아웃백 소액 결제 사기(스미싱)에 사용된 smartbiling.apk 분석’, http://darksoulstory.tistory.com/210, 2013년

[6] ’4월호 보안 뉴스레터’, 2013년.

[7] KISA, ’인터넷 침해사고 동향 및 분석월보’, 2013년, 6월.