스마트폰에서 Smishing 해킹 공격과 침해사고 보안 연구

박인우¹ · 박대우^{2*}

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

In-woo Park¹ · Dea-woo Park^{2*}

¹ Conversing Technology, Hoseo Graduate School of Venture, Seoul 137-867, Korea

² Conversing Technology, Hoseo Graduate School of Venture, Seoul 137-867, Korea

요 약

2013년도 들어 스마트폰을 이용한 스미싱(Smishing) 해킹 공격으로 인하여 피해가 급증하고 있다. 스미싱 해킹 공격과 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 강구한다. 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, 해킹, 해킹공격, 보안, 침해사고, 스마트폰

Key word : Smishing, Hacking, Hacking Attack, Security, Intrusion, Smartphone

접수일자 : 2013. 10. 01 심사완료일자 : 2013. 10. 25 게재확정일자 : 2013. 11. 06

* **Corresponding Author** Dea-woo Park(E-mail:prof_pdw@naver.com, Tel:+82-10-5274-3511)

Conversing Technology, Hoseo Graduate School of Venture 137-867, Korea

Open Access <http://dx.doi.org/10.6109/jkice.2013.17.11.2588>

print ISSN: 2234-4772 online ISSN: 2288-4165

©This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License(<http://creativecommons.org/licenses/by-nc/3.0/>) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.
Copyright © The Korea Institute of Information and Communication Engineering.

I. 서 론

작년인 2012년까지 해킹 피해가 해마다 증가하여 1억 8천만 원이었다. 스마트폰의 급격한 보급과 함께 컴퓨터 해킹뿐만 아니라, 스마트폰 해킹으로 인해 피해 사례가 점차 늘어나고 있다[1].

더불어 최근인 2013년 시장조사업체 IDC가 발표한 자료에 따르면 전세계 PC 출하량이 지난해보다 상당히 줄어들었다고 한다[2]. 이것은 스마트폰과 태블릿 보급이 확산되면서 사람들이 PC보다 스마트폰을 더 많이 사용하기 시작한다는 신호로 PC 전성시대가 가고 스마트폰 전성시대가 오고 있음을 의미한다.

이와 같이 급증하는 스마트폰 사용자들을 겨냥한 스미싱을 이용한 안전결제 해킹공격으로 인한 피해사례가 점점 늘어나고 있으며, 특히 개인정보보호법 시행에 따른 개인정보의 보호를 위해서 스미싱 공격에 대한 보안 대응 지침 연구가 필요하다[2].

본 논문에서는 보안강화를 위해 시행되고 있는 스미싱 공격에 대한 보안 대응 지침을 연구한다.

II. 본 론

2.1. 스미싱 정의

스미싱사고는 2013년도부터 급속하게 사회문제가 되기 시작하였고, 단문자서비스(Short Message Service)와 피싱(Phishing)의 합성어로, 스마트폰을 이용하여 피싱 사기를 유도하고, 스마트폰상으로 개인정보를 빼내거나, 본인도 모르게 소액결제를 하게하는 신종 휴대폰 사기 수법이다(출처 : 경찰청 사이버 테러대응센터)[3].

그림 1. '스미싱' 피해 단계
Fig. 1 'Smishing' Losses Step

휴대폰 또는 PC로 웹사이트에 접속한 피해자는 바이러스 퇴치를 위한 애플리케이션을 무료로 다운받을 것을 권고받게 되나, 그림 1과 같이 이 파일에는 트로이목마 바이러스가 포함되어, 다운로드 즉시 해커의 조종으로 개인정보가 유출되어 버린다[4].

2.2. 해킹공격 사례 및 해킹 침해사고의 원리

스마트폰사용이 늘어남에 따라 스마트폰 해킹의 위협 또한 갈수록 커지고 있다[5].

스미싱에 악용되는 해킹공격 사례는 다양하다. 대표적인 것이 그림 2와 같이 SMS로 호기심을 자극할만한 문구를 쓴 뒤 악성코드가 숨겨진 인터넷 URL을 함께 보내오는 경우이다.

그림 2. 호기심 자극하는 스미싱 해킹공격 사례
Fig. 2 Smishing hacking attack case

스미싱은 문자 메시지를 기반으로 이루어진다. 스미싱 공격의 피해 원리를 알아보면, 해커는 그림3처럼 SMS/MMS 등과 같이 메시지를 공격목표 사용자에게 보내고, 공격목표 사용자가 첨부된 링크를 클릭하게 되면, 악성코드가 포함된 애플리케이션을 다운로드 된다[6].

그때부터 해커는 그림 3처럼 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 정

보를 절취하게 된다. 절취된 사용자의 개인정보를 이용하여, 사용자를 가장한 금융결제를 통해 금전적 손실을 입히도록 하는 원리이다[7].

그림 3. 스미싱 공격의 피해 원리
Fig. 3 Principles of Damage on Smishing Attack

< 스미싱 공격을 이용한 금융사기 기법 흐름도 >

그림 4와 같은 원리로 해커는 스미싱을 이용해서 사용자들의 스마트폰을 해킹하고, 금융사기를 저지르게 된다[8].

그림 4. 스미싱 공격을 이용한 금융사기 기법 흐름도
Fig. 4 Financial trick techniques using the Smishing Attack

III. 스미싱 이용한 안전결제 해킹공격 분석

3.1. 스미싱 이용한 안전결제 해킹공격 분석

스미싱 공격은 문자 메시지 내 인터넷 주소를 클릭하여 악성코드를 자동 설치하고, 해커에게 소액 결제 인증번호를 전송함으로써 해커가 게임 아이템 및 사이버머니를 결제할 수 있다. 그로 인해 소액 결제 대금이 청구되는 것이다. 그림 5는 androapkinf.py를 이용하여 smishing.apk의 API권한을 살펴본 모습이다[9].

```
#./androapkinf.py -i /root/Desktop/smartbilling.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 5. Smishing.apk의 API권한의 소스
Fig. 5 The API permission source of Smishing.apk

androapkinf.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 API권한이 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 권한이다.

3.2. 스미싱 공격 피해 분석

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

그림 6. SMS를 통한 악성 애플리케이션(음악) 설치 후 실행 화면
Fig. 6 The running screen of an application (music) installed through a smishing scheme SMS

해당 악성 애플리케이션을 설치를 하게 되면 그림 7과 같이 빨간색 표시된 URL로 스마트폰 사용자의 전화번호를 해커의 서버로 전달을 한다.

그림 7. 해커에게 정보가 전달되는 모습
Fig. 7 Delivery of the user's information to the Hacker

또한 그림 8과 같이 와이어샤크를 통하여 해커의 서버로 스마트폰 사용자의 전화번호를 전송하는 것을 확인할 수 있다.

그림 8. 해커의 서버로 스마트폰 사용자의 시리얼 번호가 전송되는 모습
Fig. 8 Transmission of the serial number of the smartphone user to the hacker's server

IV. 스미싱 공격에 대한 보안대책

4.1. 통신사 측 보안대책

해커에게 스미싱 공격을 당했더라도 각 통신사 고객센터 또는 통신사 인터넷 홈페이지를 이용하여 휴대폰 소액결제를 원천적으로 차단을 하면 방지할 수 있다. 표 1은 3사 통신사들의 스미싱 차단 방안을 나타낸다.

표 1. 3사 통신사의 스미싱 차단 방안
Table. 1 Smishing Countermeasures of 3 agency

통신사	KT	SKT	LGU+
고객센터 통한 소액 결제 차단 방법	[1] 114을 눌러 '5'번, 그리고 '1'번을 순차적으로 눌러 KT 모바일 고객센터로 연결 → [2] 상담원과 통화하여 오프라인 결제 · 무선결제 · 청구대행 · 본인인증차단 등을 선택적으로 신청하여 소액결제 차단 → 완료.	[1] 자신의 스마트폰으로 114로 통화버튼을 눌러 SKT 고객센터로 연결 → [2] '3'번을 눌러 상담원과 연결 → [3] 소액결제 모두 차단 → 완료.	[1] 자신의 스마트폰으로 114를 눌러 전화하면 LGU+고객센터로 연결 → [2] '0'번을 눌러 상담원과 연결 → [3] 자동결제 · 인증결제 모두 차단 → 완료.

- 스미싱 피해 발생시 인터넷 결제 대행사는 콘텐츠 공급자와 협의해 결제를 취소한다.
- 게임 아이템 회사들과 협력해 1회 결제 한도나 월간 결제 한도를 축소한다.
- 게임 아이디당 결제 가능 회선(이동통신 번호)을 2회 선으로 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)를 이용하도록 결제시스템 개선한다.
- 스마트폰 신규 가입 시 발송하는 SMS에 소액결제 이

용한도 포함하여 고지(적용 예정)한다.

- 스미싱 피해자가 경찰로부터 ‘사건사고 사실 확인원’을 발급받아 제출하면 결계청구를 보류·취소한다.

4.2. 정부 측 보안방안

1) 법제도 개선 대책

- 명시적 동의자에게만 통신과금서비스 제공
- 운영규정 마련을 통한 이용자 보호 수준 제고
- 통신과금 이용 세부사항 명시에 관한 약관 개선

2) 자율규제 및 모니터링 강화

- 통신과금서비스 제공자의 자율 안전조치 강화
- 스팸 모니터링과 연계하여 악성코드 배포 방지
- 통신과금 위해요소 공동대응 체계 구축
- 통신과금서비스에 대한 이용자 이해 증진

3) 공동 대응 체계 구축 및 홍보 강화

- 통신과금 위해요소 공동대응 체계 구축
- 통신과금서비스에 대한 이용자 이해 증진

이번 보안대책의 시행을 통해, 통신과금서비스 시장의 건전한 성장기반을 구축하고 이용자 보호 수준을 한층 높일 수 있을 것이라 본다[8].

< 방송통신위원회 >

- 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 대응센터 운영.
- 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 소액 결제 대책을 마련한다.
- 제조사와 협조하여 해킹 피해 축소 및 개인정보보호를 위한 대책 마련한다.

4.3. 스마트폰 사용자 측 보안대책

< Android 사용자 측면 >

Android 스마트폰 사용자들은 기본 설치되어 있는 모바일 백신 애플리케이션은 정기적으로 업데이트는 필수적으로 해야 하고 발신처가 명확하지 않은 곳으로부터 전달되는 SMS의 인터넷 주소는 되도록 클릭하지 않는다, 그림 9와 같이 구글 플레이나 이동통신사 애플리케이션 장터에서 스미싱 해킹 무료방지라는 S-GUARD라는 애플리케이션을 다운받아 예방하는 것이 좋다.

그림 9. S-GUARD 애플리케이션 화면
Fig. 9 Screen of S-GUARD application

이 애플리케이션 같은 경우는 실시간으로 스미싱 해킹용 주소를 실시간 수집을 하여 클라우드 기반의 엔진으로 별도의 업데이트 필요 없이 자동으로 예방해준다. 또 다른 방법으로는, 그림 10과 같이 확인되지 않은 앱이 스마트폰에 설치되지 않도록 스마트폰의 보안설정을 강화하는 방법이다.

그림 10. 스마트폰의 보안 설정 강화 화면
Fig. 10 Security Settings update screen on Smartphone

① 환경설정 → ② 보안 → ③ 디바이스 관리 → ④ 알 수 없는 출처에 체크가 되어 있을 경우 해제를 하면 된다. 이와 같은 방법으로 스마트폰 사용자들은 스미싱 해킹공격으로부터 예방할 수 있다.

또한 그림 10과 같은 안드로이드에서 루팅이나 아이폰에서 탈옥을 사용하여 관리자 권한을 변경하지 않아야 상대적으로 보안성이 강화된다. 탈옥이나 루팅을 하면 일반 사용자보다 여러 기능을 사용할 수 는 있지만, 스마트폰을 안전하게 지켜주는 관리 권한을 외부로 노출시키게 되어 그만큼 해킹 위험도 증가한다.

V. 결 론

스미싱으로 인한 해킹공격에 대한 스마트폰 사용자들의 피해사례가 점점 늘어나고 있고, 해킹사고가 직접적인 금전적인 피해와 개인정보의 탈취를 야기하고 있는 걸 본 논문에서 알 수 있었다. 또한, 이에 대비하기 위해 스미싱 공격에 대한 보안 대응 지침을 연구, 분석하였다.

향후 연구에서는 스마트폰에서 스미싱 및 URL 탐지 기능이 강화 되는 연구와 해킹가능성이 크고 보안성이 약한 QR코드를 악용하여 이루어질 수 있는 해킹공격 연구를 하여야 할 것이다.

감사의 글

본 연구는 2013년도 교육부 한국연구재단(과제 번호 : 2013R1A1A2010118)의 지원에 의하여 이루어진 연구로서, 관계부처에 감사드립니다.

REFERENCES

- [1] Dea-Woo Park, Jeong-Man Seo, "A Study of Information Leakage Prevention through Certified Authentication in Phishing, Vishing, SMiShing Attacks", The Korean Society of Computer And Information, vol. 12, no. 2, pp. 171-180, 2007.
- [2] Security newsletter, April, 2009.
- [3] Cyber Terror Response Center, "Coping with smishing", Available: <http://www.netan.go.kr/>, the National Police Agency, 2013.
- [4] Kisa, "Monthly analysis and trend of Internet incidents : March", Korea Internet & Security Agency, Korea, March, 2013.
- [5] Kisa, "Monthly analysis and trend of Internet incidents : May", Korea Internet & Security Agency, Korea, May, 2013.
- [6] Kisa, "Monthly analysis and trend of Internet incidents : June", Korea Internet & Security Agency, Korea, June, 2013.
- [7] The Korea Economic Daily, "Safe approval hacking 'scare', damage of 180 million won ...steal information from game sites", Available: <http://www.hankyung.com/news>, 2013.
- [8] TickTalk, "Analysis of smartbiling.apk used in smishing", 2013.
- [9] Popp, Andreas, „Phishing, Pharming” und das Strafrecht, MMR, S. 84ff, 2006.

박인우(In-Woo Park)

2012년 2월 : 호서대학교 정보보호학과 졸업 (공학사)

2012년 9월 : 호서대학교 벤처전문대학원 융합공학과 (정보보호전공)

2012년 9월 ~ 현재 : 호서대학교 벤처전문대학원 융합공학과 석사과정

※ 관심분야 : 정보보호, 추적기법, Hacking, Forensic, 스마트폰 및 이동단말 보안

박대우(Dea-Woo Park)

1998년 : 송실대학교 컴퓨터학과 (공학석사)

2004년 : 송실대학교 컴퓨터학과 (공학박사)

2004년 : 송실대학교 겸임교수

2006년 : 정보보호진흥원(KISA) 선임연구원

2007년 ~ 현재 : 호서대학교 벤처전문대학원 부교수

※ 관심분야 : Hacking, CERT/CC, 침해사고대응, e-Discovery, Forensic, 사이버안보, 정보보호, 유비쿼터스 네트워크 보안, WiBro 보안, VoIP보안, 스마트폰 및 이동단말 보안