스미싱 공격 동향 분석 및 Mobile Forensic

노정호* · 박대우*

*호서대학교 벤처전문대학원

Analysis on Smishing Attack Trends and Mobile Forensic

Jung-Ho Noh* · Dea-Woo Park**

*Hoseo Graduate School of Venture

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

요 약

우리나라 국민의 대부분이 스마트폰을 소유하고, 스마트폰으로 인터넷뱅킹, 전자상거래 및 본인의 업무까지도 처리하고 있다. 스마트폰의 사용성과 편리성은 높아가고 있지만, 역기능인 스마트폰을 통한 사기사건과 범죄사건도 높아가고 있다. 스마트폰에서의 스미싱 사고는 2013년부터 급격하게 증가되어 세월호 사건, 추석 명절 등의 사회적인 이슈와 연계되어 교묘하게 발생하고 있다. 본 논문에서는 2014년 이후의 스마트폰에서의 스미싱 공격에 대한 동향을 분석한다. 사회 이슈와 연관된 스마트폰에서 스미싱 공격에 대한 공격 기술 및 내부적인 금융사기로 이어지는 공격의 프로세스를 분석한다. 이를 법적인 증거자료로 사용하기 위해 스마트폰 포렌식을 분석한다. 스마트폰에서의 스미싱 공격의 기술적 공격 원리와 연계된 금융 사기의 연계 고리를 밝혀, 안전한 국민생활을 위한 사회적 기술적 기초자료가 되고자 한다.

ABSTRACT

Most of Koreans have smartphone. By using smartphone, they have done internet-banking, e-commerce and private scheduling. However, convenience of smart phone has been made side effect such as tool of fraud and crime. Especially, Smishing on smartphone has been increased rapidly since 2013. Smishing have utilized social-engineering technique with social issue such as Korean near-sea cruse ship, ‘Sewol-Ho’, Sinking and traditional thanks-giving holiday, ’ Chu-Seok’, etc. This paper proposed the oncoming trend of smishing on smartphone after 2014. This paper also analyzed the process and technique of smishing on internal financial fraud. It also covered smartphone forensic for using legal evidence. By discovering the connectivity of smishing and financial fraud, this paper could be reference for social security on smartphone.

키워드

Attack, Forensic, MobilePhone, MobilePhone crime, Smishing

Ⅰ. 서 론

우리나라에 국민당 1명씩은 스마트폰을 이용할 정도로 없어서 안되는 필요한 존재이다.

하지만 이러한 스마트폰을 가지고 해커들은 피싱공격, 스미싱 공격, 파밍 공격을 하고 있으며 이러한 스마트폰 공격은 날이 갈수록 지능화 되어 스마트폰 이용자들이 피해는 해가 지날수록 피해 건수와 피해 금액이 점차 커지고 있다.

본 논문에서는 이러한 스마트폰 공격에 대해 파악하며 모바일 포렌식을 통해 공격 피해 과정에 대해 분석한다.

Ⅱ. 관련 연구

2.1 스마트폰 기능

스마트폰은 휴대폰과 개인휴대단말기(personal digital assistant; PDA)의 장점을 결합한 것으로, 휴대폰 기능에 일정관리, 팩스 송·수신 및 인터

넷 접속 등의 데이터 통신기능을 통합시킨 것이다. 가장 큰 특징은 완제품으로 출시되어 주어진 기능만 사용하던 기존의 휴대폰과는 달리 수백여 종의 다양한 애플리케이션(응용프로그램)을 사용자가 원하는 대로 설치하고 추가 또는 삭제할 수 있다는 점이다.

무선인터넷을 이용하여 인터넷에 직접 접속할 수 있을 뿐 아니라 여러 가지 브라우징 프로그램을 이용하여 다양한 방법으로 접속할 수 있는 점, 사용자가 원하는 애플리케이션을 직접 제작할 수도 있는 점, 다양한 애플리케이션을 통하여 자신에게 알맞은 인터페이스를 구현할 수 있는 점 그리고 같은 운영체제(OS)를 가진 스마트폰 간에 애플리케이션을 공유할 수 있는 점 등도 기존 휴대폰이 갖지 못한 장점으로 꼽힌다[1].

또한 스마트폰의 주요 기능으로 SMS/MMS 문자 서비스가 있으며 국내로 문자 메시지를 보낼 때는 전화번호만 입력하고 방문 국가나 제3국으로 메시지를 보낼 때는 국가번호와 전화번호를 함께 입력해서 보낼 수 있다.

문자 메시지를 이용할 때 중요한 점은 데이터 사용료이다. 데이터 사용료는 단문 메시지인 SMS와 장문 및 데이터를 첨부할 수 있는 MMS로 나눌 수 있는데, SMS 전송비는 국내 통신 비용과 같으나 80byte를 초과되거나 데이터를 첨부하면 MMS로 바뀌게 되어 데이터로밍 요금이 부과되어 요금이 많이 나올 수 있다.

특히 미국과 캐나다 일부 지역, 일본 등의 국가에서는 SMS 서비스를 지원하지 않아 MMS로만 전송될 수 있음을 사용시 유의하도록 한다. 최근에는 SMS 뿐만 아니라(자동로밍 시 무료가 많다) MMS 메시지 수신도 무료로 제공하기도 하므로 자신이 사용하는 이동통신업체의 로밍 서비스를 확인한다[2].

2.2. 스마트폰에 대한 해킹공격

공격자는 희생자에게 악성 앱을 다운로드 받을 수 있는 URL을 첨부한 SMS를 발송한다. 공격자는 희생자가 스마트폰에 전달된 SMS의 URL을 클릭하여 악성 앱을 다운 및 설치하도록 유도한다.

이렇게 설치된 악성 앱은 감염된 스마트폰의 여러 정보 및 SMS의 수신내용을 공격자에게 전달하며, 특정 SMS를 희생자가 보지 못하도록 차단하며 공격자는 수집된 해당 스마트폰의 정보로 소액결제를 진행한다.

소액결제 업체는 결제요청을 받아 해당 스마트폰에 소액결제 인증문자를 발송하며 악성 앱은 이를 피해자가 보지 못하도록 차단하고 공격자에게만 인증메시지를 전달한다[3].

III. 스미싱 공격 동향 분석

3.1. 스마트폰에서 스미싱 공격 발생

2014년 하반기 스미싱 범죄가 또 다시 증가하고 있으며 스미싱 관련 국정감사 자료에 따르면 1년간 14배 증가 했으며 건수로는 2012년 2182건에 비해 2만9761건으로 늘어났다. 금전적인 피해도 2012년 5억6900만원에 비해 57억7000만원으로 늘었다.

표1. 2012년 이후 스미싱범죄 발생 현황

연도별	발생건수	검거건수	피해금액
2012년	2,182	-	569
2013년	29,761	-	5,770
2014년 1~7월	3,753	407	-

스미싱 범죄가 늘어나고 있는 만큼 스미싱 예방 교육을 통해 피해를 최소화해야 한다[4].

3.2. 스미싱 유형별 공격 동향 분석

스미싱 공격 유형으로 이벤트성 게임 광고메일로 위장하여 스마트폰 이용자에게 보내며 URL을 클랙하면 악성코드 감염이 되면 대금결제 인증번호가 사용자가 아닌 해커에 손으로 넘어가게 되어 금전적을 피해를 보게 되는 원리이다. 여기서 더 큰 문제는 해커들의 기술이 고도화 되어 보안 프로그램을 우회하여 감염시키는 경우가 있어서 사용자가 알지도 못하고 피해를 당하는 경우가 많다.

게임을 이용한 대금 결제뿐만 아니라 스마트폰 소액결제, 인터넷 쇼핑몰 대금결제 등도 그림1과 같은 원리를 통해 금전적 피해를 입는다.

그림 1. 스미싱 공격의 피해 원리

3.3. 스미싱 이슈별 공격 동향 분석

스미싱 공격은 주로 특별한 행사나 사회적 이슈가 있을 때 발생하며 유형으로는 그림2와 같이 추석 택배 및 안부 문자를 이용한 공격이 있으며

그림3과 같이 경찰 출석 요구를 위장한 경찰청 사칭 스미싱 문자가 있다.

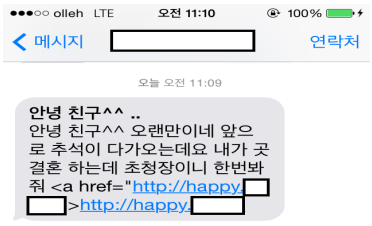


그림 2. 추석 스미싱 문자

그림 3. 경찰청 사칭 스미싱 문자
(출처 : 서울신문)

문제는 이러한 스미싱 예방 방법에 대해 모르는 이용자들이 많아 피해가 커지고 있는 실정이다.

Ⅳ. Mobile Forensic

4.1. 스마트폰에서 스미싱 공격 내용 분석

해커의 의해 스마트폰 탈취 과정은 자바 디 컴파일러 프로그램을 사용하여 그림 4. 안드로이드

```
public void onReceive(Context paramContext, Intent paramIntent)
{
  if (paramIntent.getAction().equals("android.provider.Telephony.SMS_RECEIVED"))
  {
    if (!new MetUtil().isServiceRunning(paramContext, "com.google.beasefirst"))
    {
      Intent localIntent = new Intent("activity");
      localIntent.setClass(paramContext, Mainservices.class);
      paramContext.startService(localIntent);
    }
    this.m_NotificationManager = ((NotificationManager)paramContext.getSystemService("notification"));
    this.m_Notification = new Notification();
    this.m_Notification.tickerText = "새로운 업데이트가 있습니다";
    this.m_Notification.defaults = 1;
    if (isAvilible(paramContext, "com.ATsolution.KBbank"))
    {
      this.m_Intent = new Intent(paramContext, one.class);
      this.m_PendingIntent = PendingIntent.getActivity(paramContext, 0, this.m_Intent, 0);
      this.m_Notification.setLatestEventInfo(paramContext, "KB스타뱅킹", "새로운 업데이트가 있습니다", this.m_PendingIntent);
      this.m_Notification.icon = 2130837508;
      this.m_NotificationManager.notify(0, this.m_Notification);
    }
    if (isAvilible(paramContext, "com.shinhan.sbanking"))
    {
```

그림 4. 안드로이드 코딩으로 스미싱 유도 화면

코딩과 같이 SMS 문자를 통해 전송하며 문자를 받는 사용자에게는 tickerText = " 새로운 업데이트가 있습니다. 라는 메시지로 스마트폰 이용자들에게 전송 되며 만약 이 새로운 업데이트를 유도하는 사이트를 클릭 할 경우 스마트폰에 악성코드가 감염 되어 정보들이 유출하게 된다.

4.2. Mobile Forensic 내용 분석

본 실험을 위해 Oxygen Forensic Suite 프로그램으로 사용하여 분석하였으며 그림 5는 삼성 갤럭시2로 실험 진행 후

그림 5. Oxygen Forensic Tool 준비과정

내용을 분석한 결과 그림 6과 같은 내용이 분석 되었다.

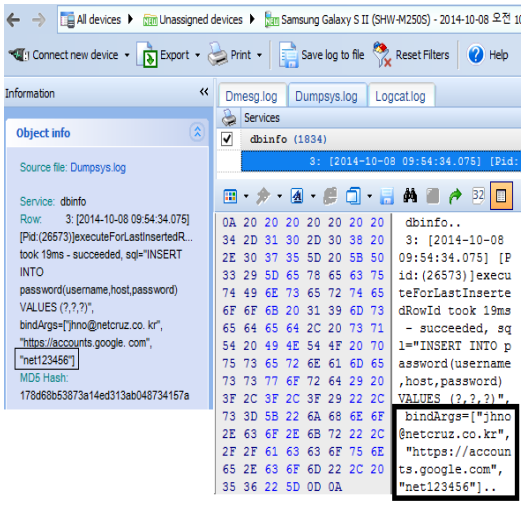


그림 6. Oxygen을 이용한 삼성 갤럭시2 정밀 분석

문제는 사용자가 삼성 갤럭시2를 정보를 이용하게 되며 이러한 정보들은 내장 메모리에 쌓이게 된다.

만약 운영하는 사이트 자체에서 웹페이지 암호화가 안 되어 있거나 또는 무선 공유기 암호화가 안 되어 있는 공공장소에서 암호를 입력 했을 경우 그림 6에 net123456라는 비밀번호도 그대로 정보에 저장 되며 툴로 분석 시 그대로 노출 된다.

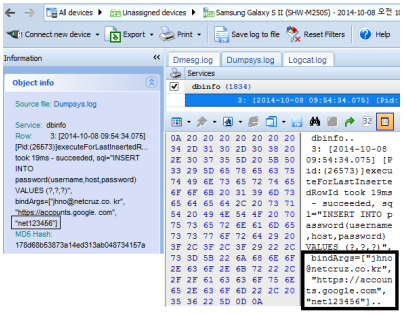
4.3. Mobile Forensic 보고서 작성

Oxygen Software Tool을 이용 후 결과에 대해 Forensic 보고서를 만들어 증거자료로 제출 한다.

표 2. Mobile Forensic 보고서

(양식 제 1 호)

Forensic 보고서

분석내용	 삼성 갤럭시2 추출 데이터
상세설명	삼성 갤럭시2 데이터 분석결과 jhno란 유저가 구글 드라이브 사이트를 이용 패스워드는 net123456으로 분석 되어 패스워드 암호화에 대한 취약점이 발견 되었다.

호서대학교 벤처전문대학원
HOSEO GRADUATE SCHOOL OF VENTURE

V. 결 론

본 실험을 통해 스마트폰 분석 툴인 Oxygen Software를 사용하여 삼성 갤럭시2 스마트폰 정보들을 분석 하였으며 스마트폰 정보에 대해 암호화 안 될 경우 패스워드가 그대로 노출 되었다.

향후 연구로는 해커들이 삼성 갤럭시2의 APK 취약점을 이용하여 정보를 탈취 하는데 이러한 취약점을 분석에 대해 연구가 필요하다.

참고문헌

[1] dooppedia 두산백과, “스마트폰 기능”, http://www.doopedia.co.kr

[2] 네이버캐스트, “스마트폰 해외에서 이용하는 법”, http://navercast.naver.com, 2012.9.

[3] 양준근, 하기웅, 김학범, “스마트폰 신종 Phishing의 피해사례 및 대응방안 분석”, 정보보호학회지, Vol.23, No.4, pp.73-81, 2013.8.

[4] 안전행정위원회, “1년 만에 14배 증가한 스미싱 범죄 감소하는 보이스피싱 범죄의 대체수단으로 악용되고 있어 “, http://yesokkh.blog.me/, 2014.8.19