스미싱의 피해와 대응방안에 관한 연구

김 장 일* · 이 희 석* · 김 지 웅* · 정 용 규**

목 차

요약

모바일 기기의 발달은 삶의 여유를 가지도록 만들었지만 그 반대편에서는 이를 금융범죄의 대상으로 간주하고 공격하는 세력들이 나타나게 되었다. 스마트폰을 대상으로 하는 범죄 중에서 금융관련 범죄는 스미싱, 피싱, 파밍, 보이스 피싱 등이 있으며, 특히 모바일의 특성상 문자메시지를 이용한 스미싱이 많이 증가되고 있는 현상이다. 스미싱 공격으로부터 안전하게 개인과 기업 및 국가의 자산이 보호되기 위해서는 사후적인 대응보다는 사전적인 예진이 더욱 중요하다. 이를 위해서는 스미싱 공격을 사전에 감지하고 차단할 수 있는 프로그램을 개발하고 배포하는 것이 필요하다.

표제어: 모바일, 스미싱, 금융범죄, 차단앱, 문자메시지

접수일(2015년 2월 28일), 수정일(1차: 2015년 3월 15일), 게재확정일(2015년 3월 30일)
* 을지대학교 의료IT마케팅학과
** 교신저자, 을지대학교 의료IT마케팅학과 교수, ygjung@eulji.ac.kr

1. 서론

스마트폰의 대중적 보급과 사용의 확대 및 기능의 첨단화는 필연적으로 스마트폰을 범죄의 대상으로 하는 공격을 유발하게 되었다. 스마트폰을 대상으로 하는 범죄 중에서 금융관련 범죄는 스미싱, 피싱, 파밍, 보이스 피싱 등이 있다(신재헌, 김상운, 2014). 우리나라의 스마트폰 보급률은 2014년 12월 현재 80%로 추정되고 있으며(뉴스토마토, 2014, 12, 22). 2009년 최초의 스마트폰이 보급된 이후 5년만에 스마트폰 가입대수는 4,000만대를 넘어서 약 80%의 보급률을 보이고 있다(아이티투데이, 2014, 12, 28).

모바일 기기 특히 스마트폰을 이용한 금융거래가 가능해지면서 스마트폰 가입자의 대부분이 스마트폰을 기반으로 하는 금융거래를 하고 있다. 모바일 뱅킹 이용자는 2014년 9월 현재 4,559만 명이며, 일일평균 3,181만 건을 이용하고, 일일평균 거래금액은 1조 8,561억 원이며, 이중에서 스마트폰 뱅킹 이용자는 3,161만 건에 1조 8,232억 원의 금융거래를 하고 있다(아이트디포, 2014, 11, 19). 다음 표 1은 모바일뱅킹서비스 이용실적 현황이다.

모바일 기기의 발달은 삶의 여유를 가지도록 만들었지만 그 반대편에서는 이를 금융범죄의 대상으로 간주하고 공격하는 세력들이 나타나게 되었다.

스마트폰 기반 금융범죄의 현황을 간략하게 살펴보면, 금융감독원에 접수된 모바일 기기 기반 금융사기의 피해는 2012년 24,533건에 약 1,159억 원이었으며, 2013년에는 55,884건에 1,423억 원으로 증가하였으며, 2014년 상반기에는 17,891건에 약 889억 원의 금융피해가 발생하였다. 따라서 2014년 스마트폰 기반 금융사고의 피해를 추정하면, 총 피해건수는 감소하였지만, 피해액은 증가하는 것으로 예측할 수 있다. 스마트폰을 이용한 피싱이나 스미싱 금융범죄는 피해자가 그 피해를 인지하기 전에 발생하고 가해자가 알지 못하는 사람이거나 또는 외국에 서버를 두고 공격하기 때문에 더욱 방어와 구제에 어려움이 있다.

스마트폰을 기반으로 하는 금융범죄 중에서 특히 스미싱은 이용자 즉, 피해자가 인식하기 전에 범죄

표 1. 모바일뱅킹 서비스 이용실적 현황
Tab. 1 Mobile Banking Service Achievement

	2013			2014		2014
	2/4	3/4	4/4	1/4	2/4	3/4
이용건수	20,565	22,304	24,462	27,597	29,412	31,805
	(8.6)	(8.5)	(9.7)	(12.8)	(6.6)	(8.1)
(스마트폰 기반)	20,316	22,235	23,910	27,369	29,368	31,610
	(8.7)	(9.4)	(7.5)	(14.5)	(7.3)	(7.6)
조회서비스	18,587	20,269	22,207	25,181	26,756	29,020
	(8.3)	(9.0)	(9.6)	(13.4)	(6.3)	(8.5)
	<90.4>	<90.9>	<90.8>	<91.2>	<91.0>	<91.2>
자금이체	1,977	2,034	2,255	2,416	2,656	2,785
	(11.8)	(2.9)	(10.9)	(7.1)	(10.0)	(4.8)
	<9.6>	<9.1>	<9.2>	<8.8>	<9.0>	<8.8>
이용금액	1,393.4	1,419.2	1,573.2	1,663.4	1,718.6	1,856.1
	(10.2)	(1.8)	(10.9)	(5.7)	(3.3)	(8.0)
(스마트폰 기반)	1,352.3	1,372.3	1,525.2	1,627.6	1,694.3	1,823.2
	(10.4)	(1.5)	(11.1)	(6.7)	(4.1)	(7.6)

가 발생하고, 이용자가 피해를 인식하였을 때는 상황을 돌이킬 수 없는 상태가 되어 버린 이후이다. 스미싱 메시지는 대부분 사용자가 신뢰할 수 있는 기관이나 지인, 친근한 형태의 광고 등을 사칭하고 있으며, 모바일 웹 브라우저를 이용해 전달된 URL에 쉽게 접속할 수 있기 때문에 사용자는 각별히 주의하지 않을 경우 매우 쉽게 스미싱 공격에 노출될 수 있다. 더군다나, 스마트폰은 PC에 비해 여러 제약이 있어 PC를 위한 피싱 공격 방지법이 그대로 적용될 수 없기 때문에 위험에 노출될 확률은 더욱 커진다. 상대적으로 작은 화면으로 인해 표시할 수 있는 정보의 양이 제한되어 있다는 점, 모바일 웹사이트를 비롯해 스마트폰의 사용자 인터페이스(user interface)가 PC에 비해 구조적으로 단순하다는 점 등이 대표적인 요인이 된다. 모바일 웹 브라우저 역시 상대적으로 PC용 웹 브라우저만큼 강력한 보안 기능을 지원하지 않기 때문에 스스로 악의적인 웹사이트를 탐지하고 접속을 차단하는 기능을 제공할 것을 기대하기 어렵다. 또한, 구조가 단순한 모바일 웹사이트는 공격자가 위조하기 쉽다는 문제점(한승환, 2014)도 있다.

2. 스미싱의 정의와 위험성

스미싱 공격은 'SMS'와 'Phishing' 두 단어를 조합한 것으로, 모바일 피싱 공격의 한 유형에 해당한다. 사용자를 유혹하는 단문 메시지(Short Message Service, 이하 'SMS')에 URL을 첨부하여 전송해 악의적인 가짜 웹사이트에 접속하도록 유도한 뒤 악성코드를 몰래 설치하거나 개인정보를 입력하도록 유도하여 가로챈 다음 금전적인 피해를 입히거나 2차 공격의 도구로 활용한다. 즉, 스마트폰을 이용하여 피싱 사기를 유도하고, 스마트폰 상으로 개인정보를 빼내거나, 본인도 모르게 소액결제를 하게하는 신종 휴대폰 사기 수법이다.

스미싱 공격은 감염시킬 스마트 폰에서 동작할 악성 앱을 반드시 설치해야 하는 문제점 때문에 공통적으로 문자메시지 안에 악성 앱 다운로드를 위한 URL 링크가 포함되어 있는 특징이 있다. 대부분 실제 URL이 아닌 단축 URL 서비스를 거친 사용자가 알아볼 수 없는 URL로 변환하여 문자 메시지를 발신한다(박상호, 이준형, 2013).

최근에는 SMS 뿐만 아니라 다양한 메신저 app을 이용해 URL이 포함된 메시지를 전달하는 경우도 등장하고 있다. 스마트폰에서는 URL이 포함된 SMS를 이용해 광고를 하거나 인터넷 상의 내용을 공유하는 경우가 많기 때문에 사용자의 의심을 피하기 쉬워 모바일 피싱 공격 유형의 다수를 스미싱 공격이 차지하고 있다. 수신된 URL에 접속할 때 사용되는 모바일 웹 브라우저는 앞서 언급한 바와 같이 PC용 웹 브라우저만큼 강력한 보안 성능을 갖추고 있지 않고 구성이 간단한 모바일 웹 페이지는 쉽게 위조될 수 있기 때문에 사용자가 스미싱 공격으로 피해를 입을 확률은 더 올라가게 된다.

악성 앱은 일반 앱이라면 가지고 있을 필요가 없는 권한들을 많이 가지고 있다. 메시지수신, 개인정보열람, 저장소 접근, 전화통화, 시스템 도구 권한 등은 일반적인 앱이라면 가지지 않아야 하는 높은 등급의 권한을 요구하고 있다. 물론 앱이 설치되기 전에 유심히 살펴보는 사람들이라면 이를 감지하고 사전에 설치를 차단할 수 있겠지만, 신빙성 있는 일반 앱으로 위장한 앱의 설치를 할 때는 텍스트로 나타나는 권한은 유심히 보지 않고 지나가는 경우가 많다. 일단 설치가 되고 난 다음에는 아이콘과 실행화면을 보고서는 악성 앱인지 판단하기 힘들다. 스미싱을 통해 악성 앱을 설치한 다음에는 악성 앱

의 감지가 어렵고 실제로 개인정보 유출이나 과금이 부과되는 과정도 사용자가 인지하기 어려운 형태로 백 그라운드 형태에서 눈에 보이지 않게 진행되다 보니 피해자는 자신이 피해자라고 인지도 하지 못한 체 피해자가 되는 일이 벌어지게 된다(김형휘, 2014).

3. 스미싱 공격에 대한 대응 방법

스미싱 공격의 방지를 위해 내용 기반 필터링(content-based filtering), 블랙리스트, 화이트리스트 기법들이 사용되는데, 기존에 사용되던 내용기반 필터링은 패턴이 다양하고 URL의 약어가 사용되는 등의 이유로 스마트폰에 그대로 적용되기 힘들다. 블랙리스트 기반의 스미싱 방지 기술은 알려진 악성 코드에 대한 방어는 뛰어나지만 새로 발견되는 악성 코드에 대한 대응이 느린 단점이 있다. 화이트리스트 기반의 기술은 가장 확실한 효과를 보일 수 있지만, 초기에 많은 데이터의 수집이 필요하고 사용자의 불편을 야기한다는 단점이 있다(장준혁 외, 2014).

현재까지 스미싱을 탐색 차단하는 방법은 일반적으로 다음의 세 가지를 기반으로 하고 있다(이시영, 강희수, 문종섭, 2014).

첫째, URL 및 문자열을 이용하여 탐지하는 방법은 사용자 기기에 수신된 문자메시지의 내용을 블랙리스트에 등록된 URL 및 문자열과 비교하여 탐지하는 방법이다.

둘째, 어플리케이션의 권한을 기반으로 안정성 검사를 하는 경우, 설치된 어플리케이션이 스미싱을 발생시키는데 필요한 특정 권한들을 가지고 있을 시, 사용자에게 경고 및 삭제를 요청하는 방식이다.

셋째, 일반적인 어플리케이션의 무 결성 검사 방법의 경우, 실행중인 어플리케이션의 APK 파일내용에 대한 해시 값을 계산하여 서버로 안전하게 전송한 후, 서버에서 보관중인 원본 APK 파일의 해시값과 비교하는 방식이다.

스미싱 공격에 대한 구체적인 대응방안(이시영, 강희수, 문종섭, 2014)을 제시하면 다음과 같다.

3.1 스미싱 탐지 어플리케이션

꾸준하게 발생하고 있는 스미싱을 방지하기 위하여 통신사와 보안회사에서는 여러 가지 해결책을 내놓고 있다. 첫째, URL 및 문자열을 이용하여 탐지하는 방법은 사용자 기기에 수신된 문자메시지의 내용을 블랙리스트에 등록된 URL 및 문자열과 비교하여 탐지하는 방법이다. 하지만, URL Shortener를 이용하여 주소를 압축하거나, SNS를 통한 스미싱 기법이 등장하면서 오탐율이 증가하고 있다. 둘째, 어플리케이션의 권한을 기반으로 안정성 검사를 하는 경우, 설치된 어플리케이션이 스미싱을 발생시키는데 필요한 특정 권한들을 가지고 있을 시, 사용자에게 경고 및 삭제를 요청하는 방식이다. 하지만 검사 후 어플리케이션을 삭제하기 이전에, 악성 어플리케이션의 공격이 수행 된다면 피해를 입을 수 있는 위험이 존재한다. 또한 권한 정보만으로는 어플리케이션이 어떤 행위를 하는지 정확히 판단할 수 없으므로, 정상 어플리케이션과 비정상 어플리케이션을 명확하게 구분할 수가 없다. 마지막으로 일반적인 어플리케이션의 무결성 검사 방법의 경우, 실행중인 어플리케이션의 APK 파일내용에 대한 해시값을 계산하여 서버로 안전하게 전송한 후, 서버에서 보관중인 원본 APK 파일의 해시값과 비교하는 방식이다. 하지만 APK 파일을 변조한 후, 실행중인 APK 파일의 경로를 얻어오는 자바 코드를 별도의 디렉토리에 보관된 원본 APK 파일의 경로로 반환되도록 수정하면, 무결성 검사가 우회되므로 취약점이 존재한다.

3.2 출처가 불분명한 어플리케이션 설치 차단

공식마켓 이외에 다른 출처에서 어플리케이션을 다운로드하여 설치하지 못하도록 '환경설정 → 보안 → 알 수 없는 출처'를 통해 기본적인 설정이 가능하다. 그러나 특정 통신사 마켓이나 금융 앱스토어에서 어플리케이션을 다운로드 받는 경우, 설정을 "허용"으로 변경해야만 설치가 가능하기 때문에, 이 상태에서 사용자의 기기는 악성 어플리케이션이 설치 될 가능성이 존재하게 된다.

3.3 소액결제 금액 차단 및 제한

악성코드가 포함된 어플리케이션이 설치된 경우 사용자가 인지하지 못하는 사이에 소액결제가 이루어지므로, 피해를 입지 않기 위해 통신사에서 소액결제를 차단하도록 설정하거나, 금액의 이용한도를 제한할 수 있다. 그러나 소액결제를 차단할 경우에는 작은 금액이라도 결제 시에 카드나 금융거래를 이용해야 하므로, 추가적으로 발생하는 과정으로 인해 불편을 초래 할 수 있다. 또한 금액의 한도를 제한하는 방법의 경우에도, 스미싱을 당하면 제한범위 내의 금액도 피해를 입을 수 있기 때문에 완벽하게 스미싱을 차단하는 방법이라 할 수 없다. 그리고 많은 사용자들이 소액결제 차단 및 제한 서비스의 존재를 모르고 있어, 제대로 기능을 사용하지 못하고 있는 상태이다.

4. 스미싱 공격 단계별 차단 방법

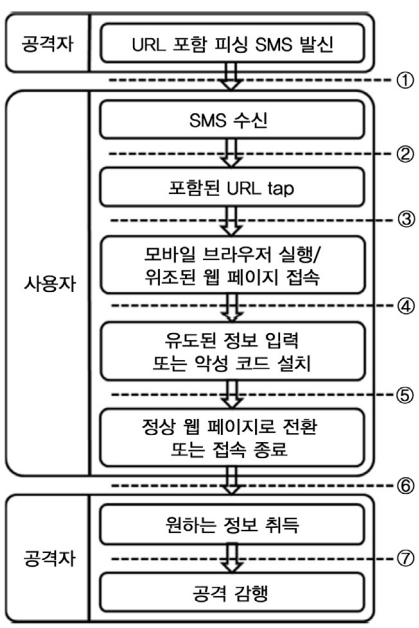

그림 1. 스미싱 공격 흐름의 각 단계별 가능한 차단방법
Fig. 1. Blocking Flow of SMS Phishing Attacks

스미싱 공격 흐름의 각 단계별 가능한 차단 방법을 간략하게 제시하면 그림 1과 같다(한승환, 2014).

① 단계: 스팸 SMS의 발신/수신 차단. 스미싱 공격의 주요 수단이 되는 가짜 웹사이트의 URL을 포함한 SMS의 발신을 차단하거나 사용자에게 수신되지 않도록 하면 스미싱 공격을 비교적 원천적으로 방지할 수 있다.

② 단계: URL 선택 차단. 스미싱 SMS가 수신되었어도 사용자가 포함된 URL을 선택하지 못하게 차단하면 공격을 방지할 수 있다. 이 때 중요한 것은 사용자가 정상 URL과 위험 URL을 확실히 구분 지을 수 있도록 도와주는 것이다.

③ 단계: URL 접속 차단. 사용자가 스미싱 SMS의 URL을 선택해도 선택된 URL에 대한 접속을 자동으로 차단할 수 있다면 공격을 방지할 수 있다. 피싱 URL을 사전에 판별해 내는 능력이 매우 중요하다.

④ 단계: 피싱 웹 페이지 분석 및 차단. URL에 접속한 경우에도 접속한 웹 페이지를 분석해 피싱 위험이 있으면 사용자의 정보 입력을 차단하거나 악성코드가 자동으로 설치되는 것을 차단하면 공격을 방지하고 사용자를 보호할 수 있다. 다양한 형태의 피싱 웹 페이지를 자동으로 분석해낼 수 있는 기법이 중요하다.

⑤ 단계: 접속 전환 차단. 사용자가 이미 중요 정보를 입력한 후에도 웹 페이지 전환을 차단하고 이후 단계의 진행을 차단하면 유출된 정보를 보호하고 공격을 방지할 수 있다. 하지만, 기술적 관점으로는 사실상 방지가 어려운 단계에 해당한다.

⑥ 단계: 적용 가능한 방지법 없음. 피싱 웹사이트를 벗어나게 되면 유출된 정보가 이미 공격자에게 전달되었다고 볼 수밖에 없다. 따라서, 스미싱 공격은 더 이상 방지할 수 없다. 다만, 이론적으로는 웹 페이지 전환 내역을 분석하여

피싱 웹사이트에 접속했던 사실을 탐지할 수 있으면, 사용자에게 가능한 한 빨리 이 사실을 경고하고 유출된 정보를 변경하여 공격자가 취득한 정보가 무의미 하게 되면 피해를 예방할 수 있다.

⑦ 단계: 사실상 적용 가능한 방지법이 없는 단계에 해당한다.

5. 결론

스미싱 공격으로부터 안전하게 개인과 기업 및 국가의 자산이 보호되기 위해서는 사후적인 대응보다는 사전적인 예진이 더욱 중요하다. 이를 위해서는 스미싱 공격을 사전에 감지하고 차단할 수 있는 프로그램을 개발하고 배포하는 것이 필요하다. 또한 현재 전 세계 악성코드 유형은 해마다 증가하고 있는데, 이들 중 대부분은 안드로이드 플랫폼 기반 악성코드이다. 안드로이드 플랫폼 기반 악성 코드가 많은 것은 다른 모바일운영체제보다 높은 시장점유율과 악성 APP제작 및 유포가 용이하기 때문이다. 또한 각각의 APP이 APK(Android Application Package) 파일 형태로 되어 있어서, 이 APK 파일을 다운로드를 통하여 모바일 기기에 저장하여 실행하기만 하면 쉽게 해당 Application이 설치가 되며, 많은 앱스토어에서 강력한 검증절차 없이 등록 가능하도록 되어 있다(공간 POC, 2013). 즉, 이용자들이 편리하고 무료로 사용할 수 있도록 제공된 서비스가 악성 금융범죄의 표적이 된 것이다.

참 고 문 헌

〔국내 문헌〕

[1] 공간POC (2013), 안드로이드 악성코드 분석 현황, 주간정보분석.

[2] 김형휘 (2014), 안드로이드 악성 애플리케이션 차단 서비스, 고려대학교 공학대학원 석사학위논문.

[3] 뉴스토마토 (2014), http://www.newstomato.com/.

[4] 박상호, 이준형 (2013), “인증 및 사전검증을 통한 스미싱 방지 시스템 제안”, 정보보호학회지, 23(6), 5-12.

[5] 아이티디포 (2014. 11. 19), 2014년 3/4분기 국내 인터넷뱅킹서비스 이용현황: http://itdepot.co.kr/220186136792.

[6] 아이티투데이 (2014),http://www.ittoday.co.kr/.

[7] 이시영, 강희수, 문종섭(2014), “안드로이드 플랫폼 환경에서의 스미싱 차단에 관한 연구”, 정보보호학회논문지, 24(5), 975-985.

[8] 장준혁, 한승환, 조유근, 최우진, 홍지만 (2014), “안드로이드 환경의 보안 위협과 보호 기법 연구 동향”, 보안공학연구논문지, 11(1), 1-12.

[9] 한승환 (2014), 허위 사용자 정보를 이용한 피싱 웹사이트의 공통 동작 기반 스미싱 공격 방지 기법, 서울대학교 대학원 전기, 컴퓨터 공학부 석사학위논문.

김 장 일 (Jang Il Kim)

순천대학교에서 학사를 취득하였고 을지대학교 의료IT마케팅학과 대학원에서 석사를 수료하였다. 현재는 ㈜디플렛폼 연구소장으로 IT관련 컨설팅을 하고 있다. 또한 KISA 피싱센터 자문 컨설턴트로 활동 중이며, 보안 및 의료정보 관련 분야에 관심이 많다.

이 희 석 (Heui Seok Lee)

을지대학교에서 의료IT마케팅학으로 학사학위를 취득하였고, 현재 을지대학교 대학원에서 석사로 재학 중이다. 또한 ㈜디플렛폼 연구소에서 연구원으로 재직 중이며, 네트워크보안 및 가상화 관련 분야에 관심이 많다.

김 지 웅 (Ji Ung Kim)

을지대학교에서 학사를 취득하였고 현재 ㈜디플렛폼 연구소 연구원으로 재직 중이며, 네트워크 및 가상화 분야에 관심이 많아 System Architecture에 관심이 많다.

정 용 규 (Yong-Gyu Jung)

서울대학교, 연세대학교, 경기대학교에서 각각 학사, 석사, 박사학위를 취득하였고, 현재 을지대학교 의료IT마케팅학과 교수로 재직 중이다. ISO, UN의 전자거래분야 한국대표위원으로 활동하였으며, 의료정보, 전자무역, 물류유통 등에 Semantic Web, Process Modelling, ebXML 등의 표준기술의 적용에 관심이 많다.

A Study on Damage and Countermeasures of SMS Phishing

Jang Il Kim* · Heui Seok Lee* · Ji Ung Kim* · Yong-Gyu Jung**

ABSTRACT

Created, but the development of mobile devices to have a margin of life have appeared in the opposite forces that are considered to be the target of financial crime and attacks them. Financial crime among crimes that target the smartphone SMS phishing, phishing, pharming, phishing, etc. voice and, in particular, a phenomenon that is growing a lot of SMS phishing is by nature a text message to your mobile. Ye Jin proactive rather than post responses in order to be safe from the SMS phishing attack individuals and businesses, and asset protection is even more important in the country. For this, the SMS phishing attack detected in advance and that can block the development program, it is necessary to deploy.

Keywords: Mobile, SMS Phishing, Financial Crimes, Blocking Apps, Texting

* Department of Medical IT Marketing, Eulji University
** Corresponding Author, Department of Medical IT Marketing, Eulji University, ygjung@eulji.ac.kr