Mobile Smishing 해킹 공격 동향 분석 및 보안대책

박대우* 양성용**

*호서대학교 벤처대학원

Hacking Aattack Trends Analysis of Mobile Smishing and Security Measures

Dea-Woo Park*, Sung-Yong Yang**

* **Hoseo Graduate School of Venture

E-mail : prof_pdw@naver.com, ysyktg@naver.com

요 약

스마트폰, 태블릿 PC, 노트북 등 모바일 장치를 이용하여 인터넷뱅킹과 전자상거래는 물론 본인의 업무까지 처리하고 있다. 모바일 기기의 가용성과 편리성은 높아가고 있지만, SNS나 문자 이메일을 이용한 Smishing 금융사기사건과 개인정보유출 등 범죄사건도 많이 발생하고 있다. 스마트폰에서 Smishing 사고는 2013년부터 급격하게 증가되어 MERS 감염 사건, 지뢰도발 사건, 추석의 택배 등을 사회공학적 방법을 이용하여 교묘하게 발생하고 있다. 본 논문에서는 2014년 이후의 모바일 장치에서의 Smishing 해킹 공격에 대한 동향을 분석한다. 사회적 이슈와 관련하여, 모바일 사용자들에게 금융사기로 이어지는 Smishing 해킹 공격의 프로세스를 분석한다.

ABSTRACT

Smartphone, tablet PC, notebook, such as the Internet banking and electronic commerce using a mobile device, as well as process and to their work. While going to high availability and convenience of mobile devices castle, SNS, letters, using an email Smishing financial fraud and leakage of personal information such as crime has occurred many. Smishing smartphone accidents increased sharply from 2013, MERS infection cases, landmine provocative events, such as the delivery of Thanksgiving has occurred cleverly using social engineering techniques. In this paper, i analyze the trends in Smishing hacking attacks on mobile devices since 2014. With regard to social issues, it analyzes the process of hacking attacks Smishing leading to financial fraud to mobile users.

키워드

Hacking Attack, Smartphone crime, Smishing

Ⅰ. 서 론

스미싱 사고는 2013년도부터 급속하게 한국에서 사회문제화 되기 시작하였고, 단문자 서비스(Short Message Service)와 피싱(Phishing)의 합성어로,

①'무료쿠폰 제공'등의 문자메시지 내 인터넷주소를 클릭하면, ② 악성코드가 스마트폰에 설치되어 ③ 피해자가 모르는 사이에 소액결제 피해 발생 또는 개인.금융정보 탈취[1] 한다

최근 발견된 스미싱 문자는 스마트폰 보안강화, 예비군, 민방위 훈련, 유머를 활용하는 등 지인이나, 공공기관을 사칭하여 정치적, 사회적 이슈를 가장해 악성코드의 설치를 유도하는 '사회공학적 기법'이 주를 이루고 있다[2].

본 논문에서는 2014년 이후의 모바일 장치에서의 Smishing 해킹 공격에 대한 동향을 분석한다. 사회적 이슈와 관련하여, 모바일 사용자들에게 금융사기로 이어지는 Smishing 해킹 공격의 프로세스를 분석한다. 해킹 공격에 대한 분석 자료를 토대로 방어적인 보안대책과 적극적인 예방적 보안대책에 대해 연구한다.

Ⅱ. Smishing 해킹 공격에 대한 동향을 분석

2.1 2014년 Smishing 해킹 공격 동향 분석

예비군/민방위 훈련 문자는 2014년 2월에 가장 많이 유포된 스미싱 문자 유형으로 2월에 국방부가 주의를 발표한 이래, 3월 첫째 주에 발견된 스미싱 악성코드의 약 66%를 차지하였다. 또한, 봄철을 맞아

결혼과 건강에 화두를 두고, '웨딩'과 '건강 암 검진 대상' 스미싱도 등장 하고 있다. "[청첩장] 저희 두 사람 하나가 되기를 약속하려합니다. 청첩장보기 w*w.c**.do/Y**, "고객님은 2014년 암 검진 대상이오니, 꼭 암 검진 받으십시오. H**p://goo.**/M3a**u" 등의 시즌 별 문구가 발견되기도 했다.

개인정보 유출과 스마트폰 뱅킹 보안에 대한 관심이 사회적 이슈가 되고 있어서, 스마트폰 사용자들은 무심코 URL을 클릭하기 쉽다. 스미싱 문자 내 URL 클릭 시 금융정보와 같은 민감한 개인정보 유출이나 소액결제, SMS[문자메시지]와 주소록 유출 및 전화 송수신 감시 등 피해가 발생할 수 있다.

그림 1처럼 성탄절 시즌을 악용한 Smishing 공격과 연말연시 분위기를 악용한 Smishing 공격이 있었다.

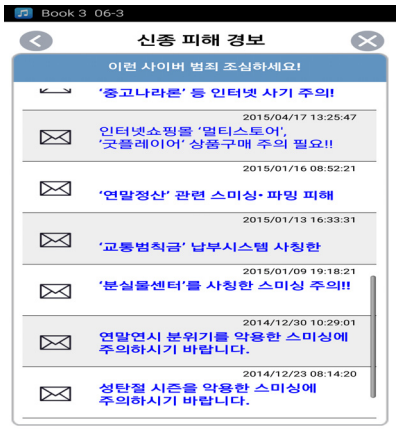

그림 1. 2014년 성탄절, 연말연시 Smishing 공격

2.2 2015년 Smishing 해킹 공격 동향 분석

2015년 연초의 휴일과 연말에서 연초로 이어지는 이동 중에 분실물 관련하여 Smishing 해킹 공격이 발생하였으며, 2015년 1월 역시 국민들에게 화두가 되었던, 연말정산 관련하여 Smishing 해킹 공격이 발생하여 많은 피해를 입었다.

2015년 6월 국가적인 메르스(MERS-coV) 감염으로 국민과 국가 경제에 큰 영향을 미치고, 국내 분만 아니라, 외국인의 방문객의 감소로 인한 경제적 타격을 입었다. 이를 이용한 메르스 Smishing 해킹 공격이 발생하여 많은 피해를 입었다.

2015년 9월 추석을 즈음하여 급격히 증가한 택배서비스를 이용한 사회공학적 Smishing 해킹 공격이 발생하였다. 그림 2처럼 추석을 전후해서 '택배 반송처리 주소지 재확인' 문구를 사용해 유명 택배업체를 사칭한 스미싱이 다량 발견되고 있다.

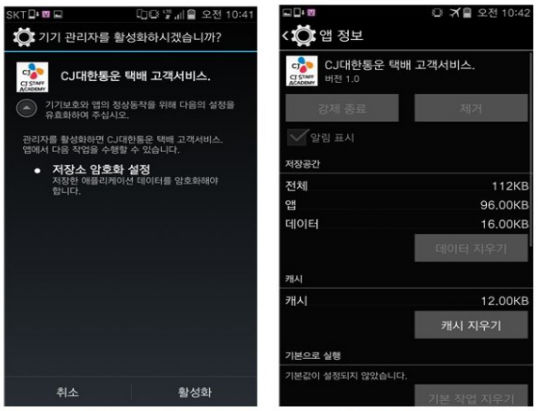

그림 2. 2015년 추석 택배서비스 Smishing 공격

Ⅲ. 결론

본 논문에선 2014년 발생한 예비군/민방위 훈련 관련 문자로 출발하여, 봄철에는 '웨딩'과 '건강 암 검진 대상' 스미싱 공격, 청첩장보기, 스마트폰 뱅킹 보안 관련, 성탄절, 연말연시 분위기를 악용한 Smishing 공격을 조사 분석 하였다. 2015년에 발생한 Smishing 공격분실물 관련, 연말정산 관련, 메르스(MERS-coV) 감염 관련, 추석 택배서비스 관련한 Smishing 해킹 공격의 동향을 분석하였다.

참고문헌

[1] 전기통신금융사기 (피싱, 파밍, 스미싱, 메모리 해킹 등), 사이버범죄신고/상담 정보통신망 이용 범죄, http://cyberbureau.police.go.kr 2015. 9.

[2] 박대우, Smishing 사고에 대한 Mobile Forensic 분석, 한국정보통신학회논문지, 18권 12호, pp2878-2883, 2014. 12.