국민안전을 위한 스미싱 범죄수법분석★

최관* · 김민지**

요 약

이 연구는 신종범죄인 스미싱(smishing) 범죄의 수법(Modus Operandi)분석을 시도한 최초의 연구이다. 본 연구를 위한 자료수집방법으로 87건의 '스미싱 사건의견서분석' 과 '피해자 사례분석' 그리고 일선경찰서에서 스미싱 범죄담당 경찰공무원 10명을 대상으로 '면접조사'를 실시하였다. 연구조사결과, 스미싱 범죄는 범죄 실행 전 단계와 실행단계로 분류할 수 있으며, 스미싱 범죄 준비 단계에서는 크게 2가지(개인정보 수집, 문자메시지 스크립트 구성)의 수법패턴을 보이는 것으로 확인되었다. 범죄 실행 단계에서는 크게 7가지(스미싱 문자발송 및 악성App 설치, 개인정보유출, 서버를 통한 스미싱 범죄조직에 개인정보 전달, 게임사이트 등에서 개인정보를 이용한 결제시도, 인증번호 가로챔, 가로챈 인증번호로 결제완료, 피해자에게 결제금액 청구)의 수법패턴을 보이는 것으로 확인되었다. 이 연구에서는 이러한 두 단계로 이루어지는 스미싱 범죄의 MO를 범죄스크립트 분석을 통해 구체적으로 파악하였다.

A Study on the Modus Operandi of Smishing Crime for Public Safety

Choi Kwan* · Kim Minchi**

ABSTRACT

The purpose of this study is to analyse Modus Operandi of smishing. For the study, 87 cases of smishing crime reports and smishing experiences of victims were analysed and 10 police officers who investigates smishing crime were interviewed. The results indicated that smishing crime can be divided into the preparation stage and the implementation stage. In the preparation stage, two modus operandi patterns, collection of personal information and text message script composition, were identified. In the implementation stage, seven modus operandi patterns were identified: sending smishing text messages and installation of malicious mobile applications, leak personal information, sending personal information to smishing crime organization through online server, payment attempt using collected personal information, intercept authorization code, completion of payment using intercepted authorization code, and payment amount was delivered to victims. Further implications were discussed.

Key words : Smishing, Crime, Modus Operandi, Phishing, South Korea

접수일(2016년 4월 18일), 게재확정일(2016년 5월 27일)

★ 이 논문은 2015년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2015S1A5A8017000)

* 삼성교통안전문화연구소 책임연구원 (주저자)
** 숙명여자대학교 사회심리학과 교수 (교신저자)

1. 서 론

한국의 경우 스마트폰 사용자의 현황은 2014년 12월 기준으로 4000만명을 돌파하였지만 그 이면에는 신종금융사기범죄 역시 증가하고 있다[11]. 기술의 발전에 따라 범죄의 행태역시 점차 증가하여 피싱, 스미싱, 파밍, 메모리해킹 등으로 점차 발전하는 양상을 보이고 있다. 그 중에서도 스미싱 범죄가 한국에서 발현한지 수년 밖에 되지 않았지만 그 피해는 날로 심각해지고 있다. 스마트폰 사용자가 증가하면서 스마트폰 안에 개인정보 등을 저장하기 시작하면서 해당 피해가 늘어났으며 2013년에는 '정보보호 10대 이슈'로 선정되었다. 구체적인 피해로서, 한국인터넷진흥원(KISA)의 집계에 따르면, 2014년 4월, 5월 세월호 및 가정의 달 관련 메시지를 사칭하여 피해가 증가하기 시작하였으며 그리고 4월 한 달간 총 24만 5,378건으로 3월(15만 5,377건) 대비 약 60% 증가하였다[6]. 또한 경찰청의 공식통계를 확인해보면, 2012년에는 스미싱 범죄발생수가 2,182건이며 그 피해액은 5억 6천9백만원 정도였으나, 2013년 10월까지 경찰청에서 인지한 사건은 2만, 8,469건이며 그 피해액은 54억 5천만 원으로 1년 사이에 접수건수는 13배, 해당 피해액은 약10배 정도 증가한 것으로 확인 되었다[16]. 게다가 2014년 1월 KB국민, 농협, 롯데카드, 농협, KB국민에서 유출된 수천만의 해당 고객정보로 인해 개인정보유출 사건이 발표된 지난 1월 8일부터 21일까지 고객정보 유출과 관련한 내용의 스미싱 범죄가 약800건이나 발생한 것으로 확인되었다[6]. 이번 사건으로 인하여 앞으로 더욱 많은 스미싱 범죄가 발생할 것으로 예상된다. 이에 본 연구에서는 스미싱 범죄가 가지는 상황적 맥락과 수법을 정확히 분석하는 것에 중점을 두었다. 해당범죄를 이해하기 위해서 그 수법을 분석하고 파악하는 것의 중요성을 살펴보면 먼저, 스미싱 범죄의 거래수단으로 이용되고 있는 스마트폰을 활용한 금융거래에 대한 관련 대책을 수립하고 또한 해당기관들 사이의 업무협조 및 정보공유 방안부족 등의 문제해결을 위한 법률적 그리고 제도적 및 기술적 개선을 위해서 무엇보다도 해당 신종 범죄가 가지는 수법과 그 상황적 맥락에 대한 분석이 우선적으로 선행되어야 적절한 예방 및 대응방안 수립이 가능하기 때문이다[11].

또한, 해당 연구의 필요성으로서 먼저, 세계 최고 수준의 정보기술(IT) 인프라를 자랑하는 한국이 각종 첨단 피싱류(보이스피싱, 파밍, 스미싱, 메모리해킹) 사기의 진원지 역할을 하고 있기 때문이다. 글로벌 인사이트 컨설팅 회사인 TNS가 발표한 "모바일 라이프 2012: M-커머스"에 의하면, 한국의 경우 금융창구를 통한 입출금이나 자금이체 거래는 11.6%로, 나머지 88.4%는 모두 ATM거래 및 모바일 뱅킹과 같은 비대면거래 형태이기 때문에 이는 여러 다른 나라들보다 피싱류 관련 사기범죄 실행에 적합한 범죄환경을 조성해 주고 있어 범죄자들에게 매력적인 배경이 되고 있다고 하였다[17].

결국 이 연구의 목적은 스미싱 범죄와 관련된 사건의견서와 인터넷의 피해자 사례분석 그리고 일선 경찰공무원 면접조사를 통해 범죄자들이 스미싱 범죄를 저지르기 위해 어떠한 상황적 양태를 보였는지 범죄스크립트기법을 활용하여 살펴봄으로써 스미싱 범죄 과정에서 발생하는 수법을 살펴보는 것에 목적을 두었다.

Clarke와 Cornish(1985)는 해당 범죄를 근본적으로 이해하기 위해서, 무엇보다도 인간의 인지과학적 구조와 과정을 이해할 필요가 있다고 하였다. 이는 인간이 어떻게 상황이나 현상에 대해서 인식하고 또한 인지적 측면에서 구조화하는지를 이해할 때 인간행동 중 하나인 범죄현상도 설명이 가능 때문이다. 범죄스크립트기법은 주어진 범죄에 대한 각 과정별 행위패턴과 관련내용들을 정확히 분석적으로 제공한다는 특징이 있다. 그러므로 범죄라는 하나의 "사건"을 인지과학적 측면에서 각각의 단계로 분리하여 그 의도 및 행위패턴을 분석하는 스크립트분석과 이러한 상황적 맥락이해를 통해 범죄의 본질 및 특성을 이해하는 과정분석은 스미싱 범죄 연구에 매우 필요하다.

2. 이론적 배경

2.1 스미싱의 정의 및 발생원인

스미싱(Smishing)이란 보안 소프트 회사인 McAfee[1)]

에서 최초로 사용되기 시작한 용어로서 문자메시지(Short Message Service: SMS)와 피싱(Phishing)을 합성하여 탄생된 언어이다[6]. 일반적으로 스미싱 범죄는 문자메시지를 기반으로 하여 개인의 스마트폰 해킹기술을 활용해 Site Link가 포함된 문자메시지를 보내고 스마트폰 사용자가 해당 사이트링크를 클릭하게 되면 자동적으로 악성코드(트로이목마[2] 등)가 설치되어 범죄자가 피해자의 스마트폰을 통제 및 접근 가능한 상태로 만들게 되는 것이다. 결국, 스마트폰으로부터 금융정보를 포함한 개인정보를 허가 없이 취득하고 이를 활용하여 소액결제를 통한 결제피해를 청구하는 범죄를 지칭한다.

2016년 현재 한국에서 발생하고 있는 스미싱 범죄로 인한 피해 사례들을 기반으로 하여 스미싱 범죄의 양태를 구체적으로 살펴보면 나타나는 공통점이 문자메시지 내용은 다양하지만 URL(Uniform Resource Locator: 이하 URL)[3]이 포함되어 있는 문자 메시지를 피해자가 선택하면 즉시 악성코드가 설치된다는 점이다. 경찰청을 대표로 한 여러 기관에서 악성 URL을 Blacklist로 지정하고 관리하는 방안을 내놓고 있지만 스미싱 범죄관련 문자 메시지를 효과적으로 예방하는 데에는 한계가 있는 실정이다[1]. 효과적인 예방의 가장 큰 한계로서 첫째, 스미싱 범죄를 위한 문자 메시지에 포함된 URL이 수시로 변경되고 또한 단축 URL로 구성되어 있어 유해한 사이트인지 정확하게 식별하기가 매우 어려우며 또한 Blacklist를 우회하여 침투하는 경우도 배제할 수 없기 때문이다. 둘째, 통신3사(SKT, KT, LG 등)의 경우 스미싱 범죄 실행을 위한 악성 App[4]이 스마트폰에 설치되면 초기화기법을 활용하여 완전 삭제가 가능하지만 지속적으로 수법양태가 지능화하는 메시지 유형과 악성 App의 암호화 등으로 스미싱 범죄 예방에 어려움이 있다.

스미싱 범죄의 발생 원인들을 살펴보면 첫째, 한국 스마트폰 사용자들의 급격한 증가(2016년 1월 기준 4000만명)이다. 스마트폰 사용자가 증가 한만큼 스미싱 범죄로 인한 피해 역시 늘어날 수밖에 없다. 둘째, 출처확인이 불가능한 사이트에서 앱을 다운로드 하는 과정에서 악성 앱이 다운로드 되는 것을 들 수 있다. 셋째, 주민등록번호와 모바일폰 번호 그리고 통장계좌번호 등과 같은 개인정보의 유출로 인해 개인의 사생활 정보가 노출되면서 각종 맞춤식 문자들이 대량으로 수신되고 있다. 이로 인해 문자메시지에 포함된 URL를 클릭하게 되고 결국 악성코드가 다운로드 되는 것이다. 넷째, 게임사를 통한 환전목적으로 스미싱 범죄가 발생하는 경우이다.

2.2 스미싱 범죄 양태 유형 및 선행연구 검토

스미싱 범죄의 양태를 파악하기 위해 문자메시지 형태와 악성코드 형태를 기준으로 살펴보면, 먼저 문자메시지의 경우, 주로 할인 및 무료쿠폰, 지인사칭, 모바일청첩장, 결제, 기타 국가기관 사칭, 세월호 등과 같은 정치적 그리고 사회적 이슈 등의 내용들이 주된 내용으로 일반시민들의 심리를 활용한 사회공학적 기법을 사용하는 것으로 나타났다. 구체적으로 살펴보면, 평상시에는 보험관련(건강보험, 화재보험, 교육보험, 연금보험 관련 등)내용들과 커피와 영화 무료쿠폰이 많으며, 연말(11, 12월)이나 명절(설날, 추석 등) 그리고 학기시작(2월,3월, 9월 등)에는 할인 쿠폰과 무료쿠폰 형태의 메시지들이 급증하며, 정치적 이슈시기(세월호, 테러, 국회의원, 보궐선거 등)때 역시 관련 내용들의 메시지들이 급증하는 것으로 나타났다[11].

둘째, 스미싱 범죄에 사용되는 악성코드형태를 살펴보면, 크게 6가지 형태로 이루어지고 있다[7]. 먼저,

1) 보안 소프트웨어 업체이며, 2010년 8월 19일 인텔에 인수되었다.
2) 타인에게서 빌린 프로그램이 트로이 목마와 같은 역할을 하여 빌린 사람이 파일을 훔치거나 변경함으로써 프로그램에 결함을 가져오는 형태를 말함. 운영 체계에 대한 일반적인 침투 유형으로, 계속적 불법 침투를 위해 시스템 내 부호를 설치하여 영구적으로 시스템 내에 상주하는 형태와 원래의 목적달성 후 자취를 모두 지워버리는 형태로 구분된다[18].
3) 인터넷상의 정보 모임인 사이트에는 주소가 반드시 존재하는데, 그 주소에 데이터 전송 순서명을 붙인 것이다.
4) 넓은 의미에서는 운영 체제에서 실행되는 모든 소프트웨어를 뜻하며, 워드프로세서, 스프레드시트, 웹브라우저들뿐만 아니라 컴파일러나 링커 등도 포함된다. 또는 좁은 의미에서는 OS 위에서 사용자가 직접 사용하게 되는 소프트웨어들을 뜻한다. 이런 경우 컴파일러나 링커 등 시스템소프트웨어를 제외한 워드프로세서 등의 소프트웨어들만을 주로 뜻하고 간단히 애플리케이션이라 하며 앱(App)이라고도 한다.

“문자탈취형태”로서 수신SMS 인증문자를 탈취하여 소액결제피해를 발생시키는 것이다. 또한 “존비폰”으로서 다른 스마트폰을 감염시켜서 악성코드의 숙주역할을 하도록 만드는 형태이다. 또한 “보안프로그램 삭제”하는 방식으로서 백그라운드에서 실행중인 보안프로그램을 무단으로 삭제하는 형태이다. “문자임의 전송”형태로서 피해자의 스마트폰에 저장되어 있는 지인들의 주소에 단체로 스미싱 범죄문자를 자동으로 발송하여 대량 문제전용 요금을 발생시키는 방법이다. 또한, “금융정보 탈취”형태로서 저장된 보안카드나 공인인증서 등을 무단으로 탈취하여 이를 해커에게 전송하면 금융 뱅킹App을 사칭하는 가짜 App설치를 통해 개인정보 탈취 후 자동으로 이체시키는 수법이다. 마지막으로, “개인정보 탈취”로서 스마트폰에 저장된 주소록 리스트 및 사진파일, 메시지내용 등의 개인정보를 탈취 및 해커에게 전송하여 전화 수신 및 발신 그리고 문자메시지 내용들을 유출하는 것이다.

스미싱 범죄관련 국내외 선행연구들을 살펴보면, 2010년 이후에 소개된 스미싱 범죄의 특성으로 인해 기존의 선행연구들이 많지 않을 뿐만 아니라 그 선행연구들 대부분 정보보호 및 정보통신학 측면에서 어떻게 스미싱 범죄를 탐지하고 방지할 것인가 하는 것에 초점이 되어왔다. 구체적으로, 먼저 2014년 이재훈은 바이트코드분석을 통해 안드로이드를 기본 플랫폼으로 하는 스마트폰의 경우 어떻게 스미싱 범죄를 방지를 할까하는 것을 연구하였으며[3], 2014년 이아영은 컴퓨터 클라우드 환경에서 어떻게 실시간으로 스미싱 관련 문자들을 탐지할 것인지를 연구하였고[2], 2014년 이숙영은 스미싱 범죄 추적지원시스템으로서 스미싱 문자를 자동으로 추출해주는 스미싱 악성코드 분석기에 대한 연구를 진행하였다[1]. 2015년에 차용범은 단축 URL의 행위분석[7], 2014년에 조지호는 TaintDroid[5], 2015년에 주춘경은 개인식별화된 SMS 등을 활용해 스미싱 탐지에 관한 연구를 진행하였다[4]. 국내 인문사회계열에서도 스미싱 범죄 예방을 위한 다각적인 연구가 진행되고는 있으나 대부분의 연구가 정보보호차원의 시스템 구축 혹은 관련된 단속법규 또는 법적 보호 등에 치중해왔다.

결론적으로, 2016년 현재까지 한국에서 진행된 스미싱 범죄 관련 연구들은 대부분 정보보호 및 정보통신학에 기반을 둔 연구들이며, 스미싱 범죄가 가지는 수법과 그 상황적 맥락에 대한 분석을 범죄학적 더 나아가 행동과학적 측면에 기반을 둔 연구는 전무한 실정이다. 국외에서도 스미싱 범죄 예방을 위해 스미싱 범죄가 발생하는 상황적 맥락을 실증적인 방법에 기초한 범죄학적 그리고 행동과학적 측면에서 연구한 경우는 거의 전무한 상황이며, 특히, 스미싱 범죄를 유발하는 범죄자를 실증적으로 연구한 사례는 국외에서도 전무한 것으로 확인되었다.

3. 연구방법

본 연구를 위해 채택한 연구방법은 스크립트 기법이다. 기존선행연구들은 자료수집을 위해 면담조사방법만을 사용해왔다. 그 이유는 스미싱 범죄와 관련하여 가장 중요한 특징은 양적자료인 정확한 공식통계가 존재하지 않는다는 점이다. 한국의 경우를 예로 들면, 2014년 경찰청소속 치안정책연구소에서 발간하는 “치안전망 2014”에서 비로소 스미싱 범죄 발생현황에 대한 공식통계가 제시되기 시작하였다.

하지만 본 연구와 관련된 자료수집의 정확도를 높이기 위해서 ‘다각화’를 시도하였는데, 과학적인 연구수행과 결과해석의 타당성을 높이기위해서 복수의 자료를 활용하는 것을 ‘다각화’라고 한다. 2003년 Yin과 2011년 Tompson과 Chainey은 과학적 연구를 위하여 두 가지 이상의 자료나 근거를 연구에 활용하는 방식의 중요성을 제시하였는데, 그 이유로 모든 연구방법은 그 자체로서의 한계점을 가지고 있기에 다각화가 각 연구방법의 한계점을 보완하는 역할을 한다고 하였다[15][14].

이에 이 연구에서는 경찰서에 보관되어 있는 ‘사건의견서 분석’, 5대 포털 사이트(네이버: naver, 다음: daum, 네이트: nate, 야후: yahoo, 구글: google 등)에 올라와 있는 스미싱 피해자 사례분석, 일선 경찰관 심층면접조사를 활용한 연구방법의 다각화를 시도하였다. 즉, 반 주관적 지표인 ‘사건의견서 분석과 5대 포털사이트의 피해자 사례분석’ 및 ‘주관적 지표인 일선 경찰관 심층면접조사’ 병행을 통한 스미싱 범죄의 수법을 살펴보고 이를 통해 최종적으로 스크립트를 작

성하였다.

3.1 사건의견서 분석

스미싱 범죄 피의자들의 범행을 분석하기 위해 기소된 피의자들의 구체적인 범죄행동을 기록하는 '사건의견서'를 기반으로 분석하였다. 조사 대상은 2015년 01월부터 2015년 12월까지 12개월 동안 서울지방경찰청 소속의 7개 경찰서에서 다룬 사건들 중에서 사전에 해당 경찰서의 동의협조를 구해 최종적으로 87건의 사건의견서 자료를 열람 및 조사하는 방식으로 진행되었다.

사건의견서 분석내용들에 대한 범주화는 2000년에 Clandinin과 Connelly이 제시한 3가지 차원의 공간접근, 즉 상호작용(개인적, 사회적), 연속성(과거, 현재, 미래), 상황(물리적 공간 등)방법에 의해 범주화할 계획이다[8]. 범주화과정이 가지는 장점은 특정한 일련의 과정 속에서 객관적인 경험과 정보를 찾아내고 분석하는데 도움이 되기 때문이다.

3.2 포털에서의 피해자 사례분석

범죄행위는 범죄자와 피해자 상호작용으로 발생한다. 그래서 범죄행위를 정확히 파악하려면 무엇보다도 가해자와 피해자 측면을 모두 이해할 필요가 있다. 그래서 피해자 사례분석이 중요한 것이다. 2011년에 Maxfield & Babbie는 Targeted Victim Surveys의 중요성을 언급하면서[12], 피해자조사는 일반적인 범죄자 조사에서 밝혀지지 않는 혹은 쉽게 묻히기 쉬운 정보들의 발견을 통해 범죄연구 뿐만 아니라 올바른 범죄예방 및 통제에 중요한 역할을 한다고 하였다.

이를 위해 이 연구에서는 국내 5대 포털 사이트(네이버: naver, 다음: daum, 네이트: nate, 야후: yahoo, 구글: google 등)들의 검색을 통해 스미싱 피해경험 사례들을 수집하였다. 스미싱 범죄의 경우 다른 범죄들과 비교하여 범행직후 피해사실을 알기 어렵고 또한 피해자들 대부분이 자신의 어리석음에서 범죄피해의 원인을 찾는 경향이 있다. 게다가 암수범죄율이 높기 때문에 관할경찰서에서 피해경험사례에 대한 접근이 거의 불가능하기에 국내 5대 포털 사이트에서 피해경험사례들을 수집하기로 하였다. 피해경험 사례에 대한 수집은 2015년 9월 1일부터 12월 31일까지 4개월 동안 피해사례들을 수집하고 관련 동향별로 범주화하고 주요 사례들을 스크립트기법을 활용하여 분석하였다.

3.3 경찰공무원 심층면접조사

스미싱 범죄 피의자에 대한 사건의견서와 포털에서의 피해자 사례분석을 살펴봄과 동시에 경찰조사과정에서 확인된 피의자들의 수법 및 심리에 대한 정보들을 살펴보는 것 역시 중요하다. 일반적으로 경찰사건의견서와 피해자 사례분석에서는 범인들의 범행과정에서 나타난 행동 및 심리에 대한 구체적인 정보들이 포함되어 있지 않다. 이를 보완하기 위해 일선 경찰서에서 스미싱 범죄를 담당하는 경찰공무원들에 대한 면접조사를 계획하였다. 즉, 사건의견서를 통해 얻을 수 없었던 정보들은 해당사건의 전문가인 경찰공무원 면접조사를 통해 얻는 것이 스미싱 범죄 연구의 목적달성을 위해 타당하다고 판단하였다. 해당경찰공무원 면접조사 시에는 범죄 실행 과정에서의 범죄자 유형 및 행동 특성 그리고 심리를 중점적으로 살펴보았다.

심층면접조사의 조사대상은 경찰서 지능범죄수사팀소속 경찰공무원 10명이며, 반구조화된 설문(Semi-Unstructured Interview)[5]형식에 기초하여 동일한 조건에서 이루어졌다. 면담조사 진행을 위해 2015년 12월부터 2016년 1월까지 2개월 동안 1회 평균 50분간 진행되었다. 면접조사대상이 10명인 이유는 심층면접조사에서 수집된 자료를 정리하는 과정에서 8명을 초과하면서 수집된 자료의 중복성이 높아져 심층면접의 추가적인 필요성이 줄어들어 최종 10명으로 하였다.

질적 분석의 기준은 2007년 Beauregard와 그의 동료들이 성범죄자가 피해자를 찾는 과정에 대한 스크립트분석연구과정에서 사용한 2단계(① Pre-Crime Phase: Offense Planning; ② Criminal Event Phase: Offense Strategies)로 구분하여 연구의 목적을 설명하기 위해 적합하다고 하였다[8]. 이에 대한 장점으로 범죄행위가 발생하는 전 과정을 범죄 전, 범죄 실행

5) 정해 놓은 최소한의 질문들을 중심으로 면접을 진행하되, 상황에 맞게 면접자 취향대로 자유롭게 질문하는 형태를 말한다.

단계로 구분해 봄으로써 각 단계별 차이를 파악할 수 있다는 것이다. 그러므로 본 연구에서는 Beauregard와 그의 동료들의 접근방법에 따라 면접조사 단계별 설문내용을 '범행 준비 단계', '범행 실행 단계'의 2단계로 나누어 분석하였다.

4. 분석결과

자료 분석 결과, 한국에서 발생하는 스미싱 범죄를 발생시키는 조직은 크게 국내와 해외조직으로 구성되어 있으며 국내조직의 경우 외국(중국 혹은 대만 등)의 스미싱 범죄조직원이 한국에 점조직을 두고 총책을 담당하거나, 자신의 신분을 드러내지 않기 위해 다른 총책을 두는 방식으로 운영되는 것으로 나타났다. 대부분의 업무연락은 SMS를 통해 이루어지는 것으로 조사되었다. 해외조직은 대부분 헤커업무를 담당하며, 한국조직원들의 업무는 주로 "스미싱 문자발송", "해외서버 관리", "게임계정 생성", "설치된 스미싱을 통해 설치되는 악성 애플리케이션(App)이 잘 작동하는지 테스트하는 업무", "유출한 개인정보를 바탕으로 신용카드 도용결제" 등으로 분석결과 확인되었다.

4.1 범죄 준비 단계

스미싱 범죄 준비 단계에서는 크게 2가지(개인정보 수집, 문자메시지 스크립트 구성)의 수법패턴을 보이는 것으로 확인되었다. 첫째, 개인정보 수집의 경우 사건의견서의 87건 중에서 78건(약 90%)이 중국의 포털사이트(바이두, 소후 등) 혹은 국내 개인(개인정보 판매상 등) 및 업체(대리운전업체 등) 등을 통해 개인정보 한 건당 1원도 안 되는 헐값에 개인정보를 수집하는 것으로 나타났다. 구체적으로, 한 사례의 경우, 범죄피의자들은 3500만 건의 개인정보를 100-200만원으로 불법적으로 취득하였다. 또 다른 사례에서는 600만 명에 대한 3500만 건에 의 개인정보를 300만원에 사들인 것으로 나타났다.

둘째, 문자 메시지 시나리오 작성이다. 문자메시지 시나리오는 여러 가지 상황들을 고려하여 50가지 이상을 제공하고 있었으며, 스미싱 범죄성공율을 높이는데 가장 중요한 부분이기도 하며, 시나리오별 사칭기관에 따라 내용 역시 여러 가지 형태로 작성되는 것으로 나타났다. 스미싱 범죄 특성에 따라 크게 불특정다수와 특정인을 대상으로 한 유형으로 분류가능하다. 대부분의 스미싱 범죄는 불특정다수를 대상으로 한다. 이 유형의 경우 '보호형'과 '사회정의형' 그리고 '보상제공형'이 있다. 첫째, 보호형의 경우 주로 경찰 및 검찰 그리고 법원 등과 같은 사법기관 문자 메시지 시나리오, 금융기관(은행, 생명보험회사, 화재보험회사 등) 및 금융감독원 등의 금융관련 기관 문자 메시지 시나리오, 우체국 및 지역민원센터 그리고 구청 등을 위한 공공기관 문자 메시지 시나리오 등이 존재하고 있었다. 둘째, 사회정의형의 경우 현 사회 및 시국이슈(세월호, 지방선거, 공직자 부정 문제 등)에 대한 고발 및 정보제공을 목적으로 한 문자 메시지 시나리오들이 존재하였다. 셋째, 보상제공형의 경우 건강보험공단, 국민연금공단, 국세청, 이동통신회사, 여러 특정회사 등이 있으며 보상제공을 미끼로 첨부된 단축 URL 주소를 클릭하도록 유도하는 수법을 사용하였다.

특정인을 대상으로 한 유형의 경우, '협박형'과 '지인사칭형' 그리고 '의무부과형' 등이 있었다. 첫째, 협박형의 경우 최근에는 "도로교통법" 위반과 같은 고지서 발급내용들이 많은 것으로 나타났다. 이는 사회공학적 접근에 기초한 내용들이 많이 발생하는 것으로 나타났다. 예를 들어, 2016년 기준 한국의 자동차 보급율은 2000만대 이상으로서 평균 1가구당 1대 이상의 자동차를 소지하고 있다. 이러한 이유로 도로교통법 위반에 근거한 스미싱 문자의 경우 대다수의 시민들이 스미싱 범죄로 치부하고 무시하기는 사회공학적 측면에서 쉽지 않다. 둘째, 지인사칭형의 경우 가족, 친지, 지인 형태 문자 메시지 시나리오가 존재했고, 의무부과형은 동창회 및 각종 모임형태의 문자 메시지 시나리오 등이 존재하는 것으로 나타났다. 결론적으로, 7개 경찰서에 입건된 87개의 스미싱 범죄사건 의견서들을 분석 및 해당 유형들을 범주화하면 아래 <표 1>과 같다.

<표 1> 스미싱 범죄 메시지 유형

구 분		빈도	사칭기관
불특정다수대상	보호형	10	경찰, 검찰, 법원
			은행, 생명보험회사, 화재보험회사, 금융감독원
			우체국, 지역민원센터, 구청
	사회정의형	15	시국이슈(세월호), 지방선거, 공직자 부정 문제
	보상제공형	20	건강보험공단, 연금공단, 국세청
			이동통신회사, 기타회사
특정인대상	협박형	10	도로교통법 위반
	지인사칭형	27	가족, 친지, 지인, 직장동료 등
	의무부과형	5	동창회, 각종모임, 대학교 등
총계		87	
구 분		빈도	수법
불특정다수대상	보호형	10	- 범죄 사건 연루조사, 개인정보 유출 등
			- 카드대금, 금융거래정보 유출
			- 우편물, 택배, 가트반송 등
	사회정의형	15	- 정의실현을 위한 정보제공
	보상제공형	20	- 연금, 보험료, 세금환급 등
			- 전화요금 환급 및 커피쿠폰제공
특정인대상	협박형	10	- 과태료 청구 등
	지인사칭형	27	- 생일, 아이돌잔치 등
	의무부과형	5	- 기념일, 모임 장소 공지 등
총계		87	

4.2 범죄 실행 단계

스미싱 범죄 실행 단계에서는 크게 7가지(스미싱 문자발송 및 악성App 설치, 개인정보유출, 서버를 통한 스미싱 범죄조직에 개인정보 전달, 게임사이트 같은 곳에서 개인정보를 이용한 결제시도, 인증번호 가로챔, 가로챈 인증번호로 결제완료, 피해자에게 결제금액 청구)의 수법패턴을 보이는 것으로 확인되었다. 범죄준비단계에서 개인정보 수집과 문자메시지 스크립트 구성이 완료되면, 먼저, 불특정다수와 특정인들을 대상으로 스미싱 문자를 발송한다. 이 경우 가급적 성공적으로 악성App을 설치하기 위해, 월별 및 사회적 이슈 그리고 가장 일반적인 내용들의 스미싱 문자를 발송하는 것으로 나타났다. 예를 들어, 월별 이슈로 항상 보내는 문자내용은 “설날”, “추석”, “어린이날”, “어버이날”, “스승의날”, “광복절”, “크리스마스이브”, “성탄절” 등이 있는 것으로 나타났다. 사회 및 시국이슈로는 “세월호”, “대선”, “북한관계악화로 인한 예비군 소집”, “재난관련 문자내용” 등이, 일반적인 내용으로는 “도로교통법 위반에 따른 범칙금 및 과태료 청구” 등이 존재하였으며, 이를 통해 피해자들이 문자메시지에 첨부된 단축 URL주소를 클릭하도록 유도하고 이를 통해 악성App을 성공적으로 설치하는 것으로 나타났다. 또한, 스마트폰에 구글 등 정상적인 App을 가장한 악성App을 유포함으로서 피해자들이 악성코드 설치 사실을 인식하지 못하도록 하였다.

둘째, 악성App이 성공적으로 설치되면 그 다음, 개인정보를 유출하고 유출된 개인정보는 스미싱 범죄조직에 전달되는 것으로 나타났다. 개인정보의 유형으로는 일반적으로 전화번호, 개인신상정보, 주민등록번호, 각종카드번호 등이 주 대상으로 나타났다. 이렇게 유출된 정보들은 대부분 해외조직으로 보내지는 것으로 나타났으나, 범죄조직별 상황에 따라 국내조직에서 유출된 개인정보를 확보하기도 하는 것으로 조사되었다.

셋째, 확보된 개인정보를 바탕으로 주로 게임 사이트 등에서 개인정보(전화번호, 이동통신사, 주민번호 등)를 활용하여 결제를 시도하고, 인증번호를 가로챈 후, 이를 통해 결제를 완료하고 결국 스미싱 범죄 피해자에게 결제금액을 청구하는 것으로 나타났다. 게임 사이트의 경우 게임 아이템을 구매한 후, 게임 계정 자체를 되팔아서 수익을 올리는 방법이 주로 사용되는 것으로 나타났다. 또한 신용카드의 경우 한도액까지 횟수 제한 없이 소액결제가 가능하다는 점 역시, 스미싱 범죄를 증가를 야기하는 것으로 조사되었다.

넷째, 인증번호 가로챔과 소액결재 완료이다. 대부분의 사건의견서 분석 결과, 스미싱 범죄조직들은 피해자의 스마트폰에 악성App을 설치하면서 수신문자를 스마트폰 화면에 표시하지 않고 가로채는 지능형 악성App 역시 활용하여 피해자들이 결제 확인 통보 문자를 받지 못하도록 하는 방법을 주로 활용하는 것으로 분석되었다. 마지막으로 결제가 완료되면 스미싱 범죄피해자에게 결제금액이 청구됨으로써 스미싱 범죄로 인한 소액결제가 발생하는 것으로 분석되었다.

5. 결 론

상기의 분석내용들을 종합해보면, 스미싱 범죄는 크게 8가지 단계로 이루어지는 것으로 나타났으며, 구

체적인 내용은 아래 (그림 1)과 같다

구분	내 용
1	개인정보 수집
2	문자메시지 시나리오 작성
3	스미싱 문자발송 및 악성App 설치
4	개인정보유출 - 전화번호, 신상정보, 주민번호, 카드번호 등
5	서버 통해 범죄조직에게 개인정보 전달
6	게임 사이트에서 개인정보 이용 결제시도 - (전화번호, 이동통신사, 주민번호 입력 후 인증번호 요청)
7	인증번호 가로챔
8	가로챈 인증번호로 결제완료
9	스미싱 범죄 피해자에게 결제금액 청구

(그림 1) 스미싱 범죄 수법 스크립트

상기의 스크립트를 통해 한국 발생하고 있는 스미싱 범죄에서 나타나는 몇 가지 특성들을 확인할 수 있다. 첫째, 국제성 범죄라는 것이다. 본 연구에서 소개된 대부분의 스미싱 범죄조직들은 해외조직과 국내조직으로 구분되어 있었으며, 또한 스미싱 범죄를 실행하는 사람은 조선족, 중국인 유학생, 한국인 등으로 다양하게 구성되어 있었다.

둘째, 스미싱 범죄조직이 점조직형태로 이루어지고 유지된다는 점이다. 스미싱 범죄조직의 구성원들은 수사기관(경찰, 검찰 등)의 추적과 검거를 피하기 위해 추적이 어려운 노트북을 활용하여 범죄를 저지르는 것으로 밝혀졌다. 그리고 범죄조직은 점조직 형태로 구성되어 문자발송, 개임계정 생성, 악성App 테스트 등으로 철저하게 분업화되어 있고 또한 조직구성원들이 검거되더라도 상부 조직에 대한 정보를 갖고 있지 않기 때문에 계속해서 수사기관의 추적을 피할 수 있다는 점이 발생하게 된다. 또한 업무지시 역시 SMS로만 이루어져 이름이나 주거소재지 정보조차 서로 모르는 것으로 연구결과 확인되었다.

셋째, 스미싱 범죄수법이 다양하게 진화하고 있다는 것이다. 경찰과 검찰과 같은 특정 기관들을 일정기간 동안 사칭하다가 사람들에게 많이 알려져 있다고 판단되면 새로운 기관으로 변경하여 사칭하고 있으며, 피해자들의 스마트폰에 악성App을 설치하면서 수신문자를 스마트폰 화면에 표시하지 않고 가로채는 지능형 악성App 역시 활용하여 피해자들이 결제 확인 통보 문자를 받지 못하도록 하는 방법 등을 통해 피해자들이 자신이 속았다는 사실을 바로 알지 못하도록 함으로써 범죄피해에 대한 효과적인 대응을 무력화 시키는 것으로 조사되었다.

넷째, 대부분의 스미싱 범죄에 가담하는 피의자들은 죄의식이 결여되어 있는 것으로 나타났다. 본 연구결과 스미싱 범죄는 국내의 불특정 다수의 피해자들에게 문자메시지를 통해 이루어지기 때문에 비대면성, 익명성이 보장되며 또한, 검거 가능성이 매우 낮아 범죄인들의 죄의식이 다른 사기사건에 비해 낮은 편이었다.

'문자메시지를 통해 개인정보를 낚아 올린다'는 의미를 지닌 스미싱은 한국에서 2012년에 처음 경찰에 접수되었고, 최근 몇 년 동안 한국사회에 엄청난 피해를 불러왔다. 또한, 신종범죄이기 때문에 공식통계 뿐만 아니라 선행연구 역시 부족한 현실이다. 이에 이 연구에서는 스미싱 범죄의 수법과 상황적 맥락을 파악하기 위해 범죄스크립트기법를 활용하여 분석하였다.

종합해보면, 스미싱 범죄는 Clarke가 주장한 합리적 선택에 기초한 범죄이며[10], 그렇기 때문에 수사기관의 검거를 피하기 위해 점조직 형태로 존재하며 SMS로만 상호작용을 하므로 결국, 수사기관의 수사 및 법집행을 어렵게 만들게 된다. Clarke에 의해 이론화된 상황적 범죄예방(Situational Crime Prevention)은 범죄자나 피해자보다는 이를 둘러싼 환경과 상황에 초점을 두는 범죄예방기술인데, Clarke가 주장한 8가지[6] 전략들 중에서 '범죄수단의 차단(Controlling Facilitators)' 등은 스미싱 범죄예방에 효과를 발휘하고 있다.

6) Target Hardening; Controlling Facilitators; Entry/exit Screening; Formal Surveillance; Surveillance by Employees; Natural Surveillance; Target Removal; Rule Setting

이 연구의 결과를 통한 정책적 대안들을 제시한다면, 스미싱 범죄는 합리적 선택에 기초하여 발생하기 때문에 '범죄수단의 차단' 측면에서 스미싱이 문자메시지를 매개체로 이루어진다는 점에 착안하여 "스미싱 차단 어플"을 개발 및 설치하여 스미싱 범죄에 대응하여야 한다. 그리고 2016년 현재 스미싱 범죄와 관련된 신종범죄들이 증가추세이므로 스미싱 범죄에 대한 분석 및 후속 연구를 통해 신종사기범죄 예방을 위한 지속적인 노력이 요구된다. 또한, 스미싱 범죄는 그 수법이 날로 진화하고 있으며, 나아가 피싱사이트로 유인해 보안카드번호 등을 빼내 예치되어 있는 예금을 몰래 가로채는 파밍, 가짜 팝업창을 띄워 보안카드 비밀번호 앞뒤 2자리를 빼내는 메모리해킹수준까지 진화하고 있는 실정이다. 그러므로 범죄스크립트기법을 활용하여 변종 피싱 그리고 파밍 같은 신종범죄들에 대한 추가적인 후속 연구가 활발히 이루어져야 한다.

참고문헌

[1] 이숙영, '스미싱범죄 추적 지원시스템에 대한 연구', 동국대학교 대학원 석사학위논문, 2014.

[2] 이아영, '클라우드 환경에서 실시간 스미싱 탐지 기법에 대한 연구', 숭실대학교 정보과학대학원 석사학위논문, 2014.

[3] 이재훈, '바이트코드분석을 통한 안드로이드 플랫폼 스미싱 방지기법', 숭실대학교 정보과학대학원 석사학위논문, 2014.

[4] 주춘경, '개인식별화된 SMS 발송을 통한 스팸식별 및 스미싱 예방: 금융권중심', 고려대학교 정보보호대학원 석사학위논문, 2015.

[5] 조지호, 'TaintDroid를 이용한 스미싱 탐지 기법에 대한 연구', 한남대학교 대학원 석사학위논문, 2014.

[6] 치안정책연구소, '치안전망 2015', 서울: 치안정책연구소, 2015.

[7] 차용범, '단축 URL의 행위 분석을 통한 스미싱 범죄에 대한 선제적 대응방안 연구', 고려대학교 정보보호대학원 석사학위논문, 2015.

[8] Beauregard, E. & Leclerc, B., "An application of the rational choice approach to the offending process of sex offenders: A closer look at the decision-making", Sex Abuse, Vol 19, pp. 115-133, 2007.

[9] Canter, D. & Young, D., 'Investigative psychology: Offender profiling and the analysis of criminal action'. John Wiley & Sons, 2009.

[10] Clarke, R. V. & Cornish, D. B., Modeling Offenders' Decisions: A Framework for Policy and Research. In M. Tonry. & Morris, N. (Eds.) Crime and Justice: An Annual Review of Research. Vol 16. Chicago, IL: University of Chicago Press. pp. 79-91. 1985.

[11] Choi, K., Lee, J. K. & Chun, Y. T., "Voice Phishing Fraud and Its Modus Operandi", Security Journal. Online Version: pp. 1-13, 2015.

[12] Maxfield, M. G. & Babbie, E. R., 'Research methods for criminal justice and criminology', Belmont, CA: Wadsworth Cengage learning, 2011.

[13] Nykodym, N., Taylor, R. & Julia V., "Criminal profiling and insider cyber crime." Computer Law & Security Review, Vol 21(5), pp. 408-414, 2005.

[14] Tompson, L. & Chainey, S., "Profiling illegal waste activity: Using crime scripts as a data collection and analytical strategy", European Journal of Criminal Policy Research, Vol 17, pp. 179-201, 2011.

[15] Yin, R. K., Case Study Research: Design and Method, 3rd edition, London: Sage Publications, 2003.

[16] http://www.opengirok.or.kr/3665. (2016. 01. 03 검색).

[17] http://www.munhwa.com/news/view.html?no=2013090401031224219002O. (2016. 01. 03 검색).

[18] http://terms.tta.or.kr/dictionary/searchList.do (2016년 4월 3일 검색).

[저 자 소 개]

최 관 (Kwan Choi)

호주 모나쉬대학교
범죄학·형사사법학 박사
한세대 인문사회학부 교수
現) 삼성교통안전문화연구소
책임연구원

email : schgosi@daum.net

김 민 지 (Minchi Kim)

미국 뉴욕시립대학교
법심리학 박사
한국형사정책연구원
부연구위원
現) 숙명여대 사회심리학과 교수

email : mkim76@sm.ac.kr