Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.31, NO.6, Dec. 2021 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2021.31.6.1267

효과적인 음성스팸 역공격 시스템

박 해 룡,[1†‡] 박 수 정,[2] 박 강 일,[2] 정 찬 우,[2] 김 종 표,[1] 최 근 모,[3] 모 용 헌[4]
[1,2]한국인터넷진흥원 (팀장, 연구원), [3,4]서울경찰청 (팀장, 수사관)

An Effective Counterattack System for the Voice Spam

Haeryong Park,[1†‡] Sujeong Park,[2] Kangil Park,[2] Chanwoo Jung,[2] Jongpyo KIM,[1]
Keun Mo Choi,[3] Yonghun Mo[4]
[1,2]Korea Internet & Security Agency (Manager, Researcher),
[3,4]Seoul Metropolitan Police Agency (Manager, Investigator)

요 약

보이스피싱 범죄 접근 단계에서 미끼로 활용되는 광고 문자 및 음성에 이용되는 전화번호가 대량 불법대출 스팸 발송에 이용되고 있어 이를 신속하게 차단하는 것이 필요하다. 이에, 본 고에서는 불법대출 스팸 및 보이스피싱을 자행하는 음성스팸 전화번호에 대해서 신속한 이용제한을 함과 동시에 해당 전화번호로 전화 통화 연결이 원활하지 않게 지속적인 콜을 보냄으로서 해당 전화번호를 이용하여 불법을 자행하지 못하게 하는 음성스팸 역공격 시스템을 제안한다. 제안하는 시스템은 불법스팸신고처리기관과 수사기관간 대표적인 협업 모델로서 각각 역할을 정립하여 본 시스템을 개발한 후 실제 적용해 본 결과, 불법대출 음성스팸과 문자스팸 신고건수가 각각 1/3 수준으로 감소하는 것을 확인하여 본 시스템의 효과성을 입증할 수 있었다.

ABSTRACT

The phone number used for advertising messages and voices used as bait in the voice phishing crime access stage is being used to send out a large amount of illegal loan spam, so we want to quickly block it. In this paper, our system is designed to block the usage of the phone number by rapidly restricting the use of the voice spam phone number that conducts illegal loan spam and voice phishing, and at the same time sends continuous calls to the phone number to prevent smooth phone call connection. The proposed system is a representative collaboration model between an illegal spam reporting agency and an investigation agency. As a result of developing the system and applying it in practice, the number of reports of illegal loaned voice spam and text spam decreased by 1/3, respectively. We can prove the effectiveness of this system by confirming that.

Keywords: Illegal Spam, Voice Phishing, Voice Spam Counterattack

I. 서 론

우리는 일상생활을 하면서 핸드폰이 필수품처럼 느껴지는 때가 많아졌다. 핸드폰으로 다양한 회사업무를 처리할 수도 있고 인터넷서핑, 게임 등 즐거움을 주는 도구로 사용할 때도 있다. 이렇게 핸드폰이 우리에게 이로운 점만 준다면 좋겠지만 우리에게 불편한 점을 주는 때도 간혹 있다. 시도 때도 없이 울려대는 불법스팸 전화 때문에 성가셨던 경험이 한번쯤은 있었을 것이다. 또한, 그런 전화가 너무 자주 수신하게 되어 힘들어 하는 사람도 있었을 것이다.

불법스팸[1]은 수신을 동의하지 않는 광고나 마케

Received(10. 14. 2021), Modified(11. 22. 2021), Accepted(11. 23. 2021)
† 주저자, hrpark@kisa.or.kr
‡ 교신저자, hrpark@kisa.or.kr(Corresponding author)

팅을 권유하는 전화, 문자, 이메일, FAX 등을 의미하며, 이로 인해 생활의 불편함을 야기하곤 한다. 이러한 불편함을 해결하고자 불법스팸을 신고처리해 주는 한국인터넷진흥원이 있으며, 불법스팸을 수신하게 되면 다양한 방법으로 불법스팸을 한국인터넷진흥원에 신고할 수 있다. 불법스팸을 신고하는 방법[2]은 핸드폰 기능 중 간편신고, 국번없이 118로 신고, (한국인터넷진흥원)불법스팸대응센터 홈페이지 신고 등이 있다.

한국인터넷진흥원[3-6]에 따르면, 불법스팸신고 건수는 2018년 3,216만건, 2019년 3,688만건, 2020년 4,250만건으로 매년 증가 추세에 있는 것으로 나타났다. 불법스팸이 우리를 성가시게 하는 것 뿐만아니라 불법대출 스팸 중에는 보이스피싱을 하는 악의적인 법죄와 연결되는 경우가 다수 발견되고 있는 실정이다.

최근 경찰청[7]에 따르면 보이스피싱 발생건수 및 피해금액이 증가하는 추세에 있다. 2018년에 발생건수는 34,132건으로 피해금액은 4,040억원이고 2019년에 발생건수는 37,667건으로 피해금액은 6,398억원이며, 2020년 발생건수는 31,681건으로 피해금액은 7,000억원으로 역대 최고 수준을 보이는 것으로 나타났다.

이에, 불법대출 및 보이스피싱으로부터 국민의 피해를 예방 및 최소화하고자 불법대출 및 보이스피싱을 자행하는 음성스팸 전화번호에 역공격을 실행하는 시스템을 제안하고 이를 실제 적용해 보고자 한다.

본 고에서는 제안하는 시스템을 음성스팸 역공격 시스템으로 명명하고 세부적인 설명을 하고자 한다. 본 고의 2장에서는 관련 동향에 대해서 언급하고, 3장에서는 음성스팸 역공격 시스템을 제안하고, 4장에서는 음성스팸 역공격 시스템을 세부적으로 설명하고, 5장에서는 음성스팸 역공격 시스템 적용 효과에 대해서 기술하고, 6장에서는 결론을 맺고자 한다.

II. 관련 동향

국내 불법스팸신고처리기관으로는 한국인터넷진흥원이 있고, 보이스피싱 수사기관으로는 대검찰청(지방검찰청 포함), 경찰청(지방경찰청 포함) 등이 있다. 현재까지는 불법스팸신고처리기관과 보이스피싱 수사기관간 협력체계는 미비한 실정이었으며, 기관별 각자 본연의 역활만 충실히 수행하고 있었다. 이에, 이러한 상황을 반영하여 이 장에서는 불법스팸신고처리기관 동향과 보이스피싱 수사기관 동향에 대해서 각각 살펴보도록 하겠다.

2.1 불법스팸신고처리기관 동향

한국인터넷진흥원[2]은 불법스팸으로부터 국민의 피해를 예방 및 최소화하고자 10여개의 시스템을 운영 중에 있다. 운영 중인 시스템에 대해서 좀 더 자세히 살펴보도록 하겠다.

한국인터넷진흥원에서는 핸드폰에 수신된 불법스팸(음성, 문자)을 수집 혹은 차단하기 위해서 5가지 시스템을 운영하고 있다.

① 핸드폰(휴대전화) 간편신고 시스템 : 핸드폰 단말기에서 한번 클릭으로 간편하게 스팸 신고를 할 수 있는 시스템
② 핸드폰(휴대전화) 스팸트랩 시스템 : 무작위로 배포된 핸드폰 가상번호로 문자스팸 혹은 음성스팸이 수신되게 하여 수집하는 시스템
③ 문자스팸 실시간 차단시스템 : 문자스팸 전송번호(회신/원발신번호)를 정보통신서비스제공자에게 제공하여 실시간으로 차단하는 시스템
④ 음성스팸 실시간 차단시스템 : 음성스팸 전송번호(회신번호)를 정보통신서비스제공자에게 제공하여 실시간으로 차단하는 시스템
⑤ 이미지 스팸 실시간 차단시스템 : 스팸 이미지 해시코드를 정보통신서비스제공자에게 제공하여 실시간으로 차단하는 시스템

한국인터넷진흥원에서는 이메일로 수신된 불법스팸을 수집 혹은 차단하기 위해서 3가지 시스템을 운영하고 있다.

① 이메일 스팸 실시간 차단시스템 : IP기반의 이메일 스팸 실시간 차단 리스트를 생성하고 이를 이메일서비스업체에게 제공하여 차단하게 하는 시스템
② 도메인 신뢰도 평가 시스템 : 기업, 개인의 메일서버 및 도메인의 신뢰도를 사전에 평가하는 시스템
③ 이메일 스팸트랩 시스템 : 무작위로 배포된 도메인 가상이메일 계정으로 수신된 스팸메일을 수집하는 시스템

한국인터넷진흥원에서는 게시판에 게시된 불법스팸을 수집 혹은 차단하기 위해서 2가지 시스템을 운영하고 있다.

① 게시판 스팸트랩 시스템 : 무작위로 배포된 도메인 내 가상게시판을 통해 불법스팸 게시물을 수집하는 시스템
② 게시판 스팸 실시간 차단시스템 : 게시판 스팸을 차단할 수 있는 플러그인 및 오픈API를 제공하는 시스템

2.2 보이스피싱 수사기관 동향

보이스피싱 피해 예방 및 신고 처리를 효율적으로 하기 위해서 전국 모든 지방경찰청에 보이스피싱 전담수사팀 운영('15.2), 서울경찰청 금융범죄수사대 신설('21.1), 부산경찰청 사이버 경제 범죄수사팀 신설('21.1), 전국 모든 검찰청 보이스피싱 전담 검사 지정('21.7), 강원경찰청 보이스피싱 피해예방 홍보전담팀 신설('21.8) 등 수사기관에서 보이스피싱 피해 근절을 위해 관련 조직을 신설하고 인력을 증원하고 있는 실정이다.[8, 9, 10, 11, 12]

III. 제안하는 음성스팸 역공격 시스템

이 장에서는 음성스팸 전화번호 역공격 시스템의 전반적인 사항에 대해서 기술하기로 한다. 음성스팸 전화번호 역공격 시스템은 크게 두 단계로 이루어진다. 첫 번째는 음성스팸 전화번호 수집 단계, 두 번째는 음성스팸 전화번호 역공격 단계로 구분이 된다.

음성스팸 전화번호 수집 단계에서는 불법적으로 음성스팸을 발신하고 있는 전화번호를 수집하는 단계로 불법스팸신고처리기관에서 4가지의 음성스팸 전화번호를 수집하는 채널을 활용할 수 있으며 해당 내용은 다음과 같다.

① 트랩번호 기반 음성스팸 전화번호 수집 : 오토콜 등을 활용하여 핸드폰 번호를 수집한 후 수집한 핸드폰 번호로 불법적인 내용을 광고하는 음성스팸 전화번호를 알아내기 위해서 핸드폰 가상번호를 활용하여 음성스팸을 발신한 전화번호 수집
② 음성트랩 기반 음성스팸 전화번호 수집 : 무작위로 배포된 핸드폰 가상번호를 활용하여 해당 전화번호로 음성스팸 수신 시 발신한 음성스팸 전화번호 수집

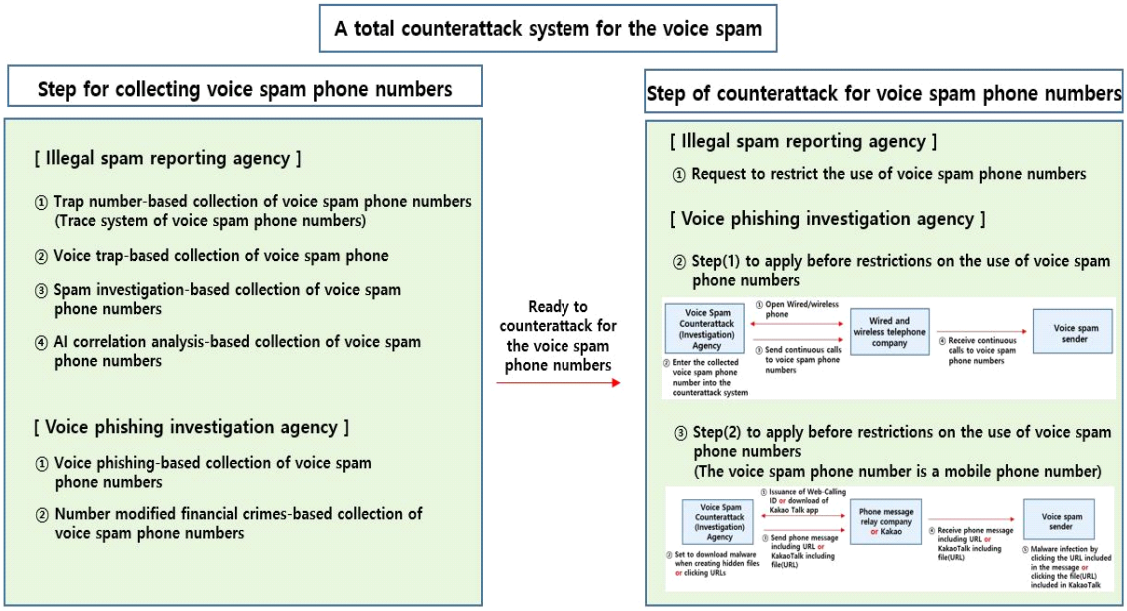


Fig. 1. A total counterattack system for the voice spam

③ 스팸사실조사 기반 음성스팸 전화번호 수집 : 불법스팸신고 처리 과정에서 음성스팸 전화번호 수집
④ AI 연관분석 기반 음성스팸 전화번호 수집 : 불법스팸신고 빅데이터에 대해 최적화된 AI를 활용하여 음성스팸 전화번호 수집

음성스팸 전화번호 수집 단계에서 불법적으로 음성스팸을 발신하고 있는 전화번호를 수집하는 단계로 수사기관에서 2가지의 음성스팸 전화번호를 수집하는 채널을 활용 할 수 있으며 해당 내용은 다음과 같다.

① 수사기관 제공 보이스피싱 관련 음성스팸 전화번호 수집 : 수사기관에서 보이스피싱 피해 신고 시 수집된 음성스팸 전화번호 수집
② 수사기관 제공 변호변작 금융범죄 관련 음성스팸 전화번호 수집 : 수사기관에서 번호를 변작하여 금융범죄에 활용한 음성스팸 전화번호 수집

음성스팸 전화번호 역공격 단계에서는 불법적으로 음성스팸을 발신하고 있는 전화번호에 대해서 역공격하는 단계로 불법스팸신고처리기관과 수사기관이 각각 역할을 분담하여 협업하는 단계이다. 불법스팸신고처리기관은 음성스팸 전화번호에 대해 정보통신서비스제공자(유무선통신사 등)에게 이용제한을 요청한다. 한편, 수사기관은 2가지의 음성스팸 전화번호 역공격 방법(음성스팸 전화번호 이용제한 이전 적용1·적용2)을 실행한다.

다만, 수사기관에서 음성스팸 전화번호 이용제한 이전 적용2를 실행하기 전에 악성코드 제작·감염 등과 관련하여 수사기관의 권한으로 가능한지 여부를 법률 검토한 후 수행해야 하며, 음성스팸 전화번호가 번호도용, 번호변작 등이 있었는지 확인 후 시행해야 한다.

구체적인 음성스팸 전화번호 역공격 단계는 다음과 같다.

① 음성스팸 전화번호 이용제한 요청 : 불법적으로 음성스팸을 발신한 전화번호에 대해서 정보통신서비스제공자에게 이용정지 혹은 계약해지를 요청
② 음성스팸 전화번호 이용제한 이전 적용1 : 불법적으로 음성스팸을 발신한 전화번호에 대해서 지속적으로 전화통화를 시도하여 해당 전화의 발신을 방해(전화 불통)
③ 음성스팸 전화번호 이용제한 이전 적용2 : 불법적으로 음성스팸을 발신한 전화번호(핸드폰 번호만 적용 가능)로 악성코드가 숨겨진 URL이나 파일이 포함된 문자나 SNS 메시지(카톡 메시지 등)를 발송하여 음성스팸 전송 기기가 악성코드에 감염하도록 유도

IV. 제안하는 음성스팸 역공격 시스템 세부 설계

이 장에서는 음성스팸 역공격 시스템의 세부 설계에 대해서 언급하기로 한다. 먼저 음성스팸 전화번호 역공격 단계에 대해서 세부적으로 살펴보도록 하겠다.

4.1 음성스팸 전화번호 역공격 단계

4.1.1 음성스팸 전화번호 이용제한 요청

불법스팸신고처리기관은 음성스팸 전화번호 수집 단계에서 확보한 음성스팸 전화번호에 대해서 정보통신서비스제공자(유무선사업자 등)에게 해당 전화번호를 이용제한 요청하는 과정이다. 이용제한은 통상 가

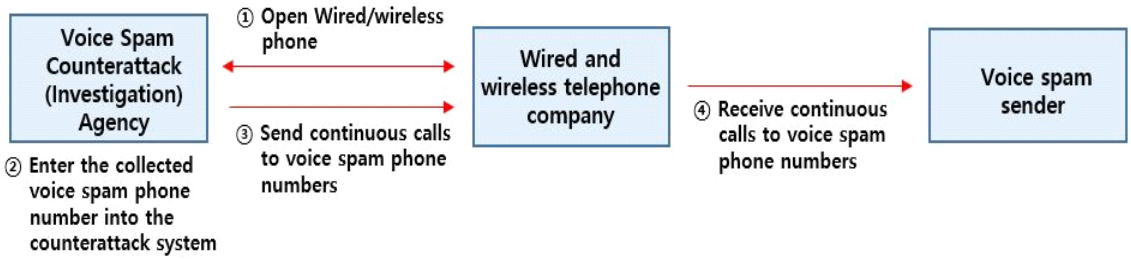


Fig. 2. Step(1) to apply before restrictions on the use of voice spam phone numbers

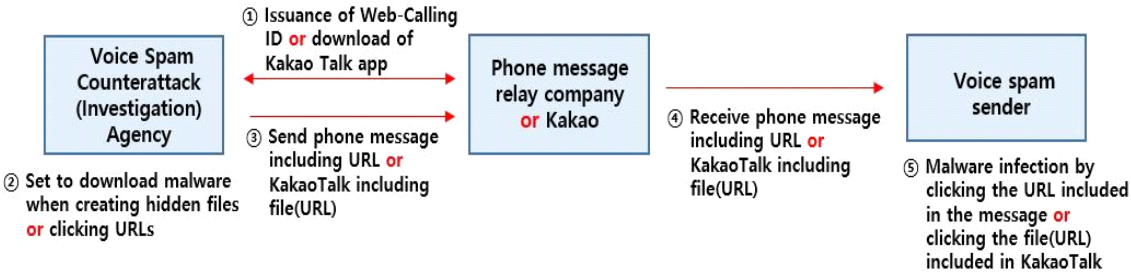


Fig. 3. Step(2) to apply before restrictions on the use of voice spam phone numbers

능한 빠른 시일 내로 처리하도록 불법스팸신고처리기관과 정보통신서비스제공자간에 협력 관계로 수행한다.

4.1.2 음성스팸 전화번호 이용제한 이전 적용1

수사기관은 음성스팸 전화번호 수집 단계에서 수집된 음성스팸 전화번호가 불법스팸신고처리기관에서 정보통신서비스제공자에게 음성스팸 전화번호를 이용제한 요청 후 이용제한 되기 전에 음성스팸 전화번호로 지속적인 콜을 수행하여 해당 음성스팸 전화번호를 무력화 시킨다. 이를 통해 음성스팸 전화번호로 확인된 즉시 해당 번호로 전화 발신을 할 수 없게 되어 피해를 예방할 수 있게 된다.

음성스팸 전화번호 이용제한 이전 적용1의 프로세스는 다음과 같다.

① 수사기관은 유무선통신사에게 유선·무선전화를 개설한다.
② 수사기관은 수집된 음성스팸 전화번호를 지속적인 콜을 발생시키는 시스템에 입력한다.
③ 수사기관은 음성스팸 전화번호로 지속적인 콜을 발생시킨다.
④ 유무선통신사를 통해 음성스팸 전송자는 음성스팸 전화번호로 지속적인 콜을 수신한다.

4.1.3 음성스팸 전화번호 이용제한 이전 적용2

이 시스템을 적용하기 위한 전제조건으로는 음성스팸 전화번호가 휴대폰 번호여야 한다. 수사기관은 음성스팸 전화번호 수집 단계에서 수집된 음성스팸 전화번호가 불법스팸신고처리기관에서 정보통신서비스제공자(유무선통신사 등)에게 음성스팸 전화번호를 이용제한 요청 후 이용제한 되기 전에 음성스팸 전화번호로 악성코드[1](랜섬웨어 등)가 숨겨진 URL을 포함한 문자를 전송하여 음성스팸 발송 기기(스마트폰, 태블릿PC 등)에서 수신된 문자에 포함된 URL을 클릭하도록 유도해서 악성코드 다운로드 및 감염시킬수 있다. 이를 통해 음성스팸 발송 기기를 일정기간 동안 무력화 할 수 있는 시스템이다. 또한, 수사기관이 음성스팸 전화번호로 카카오톡 대화하기를 신청해서 악성코드가 숨겨진 파일(URL)을 포함한 카톡을 전송하여 음성스팸 발송 기기(스마트폰, PC, 태블릿PC 등)에서 수신된 카톡에 포함된 파일(URL)을 클릭하도록 유도해서 악성코드 다운로드 및 감염[2]시킨다. 이를 통해 음성스팸 발송 기기를 일정기간 동안 무력화 할 수 있다.

음성스팸 전화번호 이용제한 이전 적용2의 프로세스는 다음과 같다.

① 수사기관은 문자중계사업자(혹은 카카오)를 통해 웹발신ID를 발급 받는다.(카카오톡 앱을 다운로드 한다.)
② 수사기관은 악성코드가 숨겨진 파일을 제작하거나 URL을 클릭 시 악성코드가 다운로드 될 수 있도록 설정한다.
③ 수사기관은 설정된 URL을 포함한 문자를 발송하거나 설정된 파일(URL)을 포함한 카톡을 발송한다.
④ 문자중계사업자(혹은 카카오)를 통해 음성스팸 전송자는 설정된 URL을 포함한 문자를 수신

1) 정보탈취형 악성코드를 활용할 경우 수사기관은 음성스팸 발송 기기에 저장된 정보를 수집할 수 있게 된다. 또한, 정보무력화형 악성코드(랜섬웨어 등)를 활용할 경우 음성스팸 발송 기기에 저장된 정보를 암호화하여 일정기간 동안 기기에 저장된 내부정보를 이용 불가능한 상태로 만들 수 있다.
2) 악성코드가 숨겨진 파일명을 "은행_계좌번호_비밀번호.jpg"로 제작·배포한다면, 음성스팸 전송자가 클릭할 가능성이 높아질 수 있다.

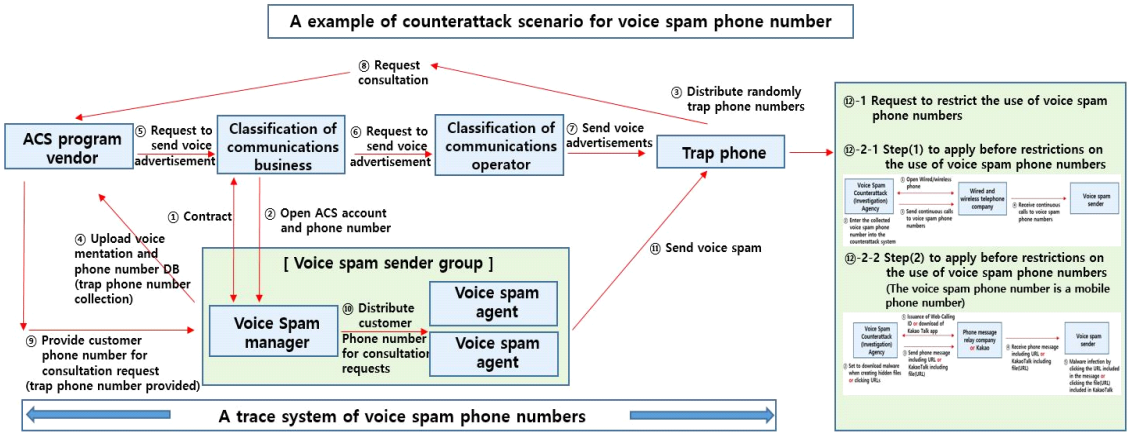


Fig. 4. A counterattack system scenario for the voice spam

하거나 설정된 파일(URL)을 포함한 카톡을 수신한다.

⑤ 음성스팸 전송자는 문자에 포함된 URL을 클릭하거나 카톡에 포함된 파일(URL)을 클릭하여 악성코드에 감염된다.

음성스팸 전화번호 이용제한 이전 적용1·적용2는 음성스팸 전화번호 이용제한하는 것 보다 더 효과적일 수 있기 때문에 상황에 따라서는 음성스팸 전화번호를 이용제한 요청 후에 실행할 수도 있고 이용제한을 요청하지 않은 상태에서 실행할 수도 있다.

4.2 음성스팸 전화번호 수집 단계

앞에서 살펴본 음성스팸 전화번호 이용제한 이전 적용1·적용2를 포함한 음성스팸 전화번호 수집 단계를 세부적으로 살펴보도록 하겠다.

4.2.1 트랩번호 기반 음성스팸 전화번호 수집 및 역공격

(수신용)핸드폰 가상번호인 트랩전화번호를 미리 이통사를 통해서 가입하고 이를 사용해서 음성스팸 전화번호를 수집하는 역할을 한다. 음성스팸 전화는 먼저 ACS(Auto Call System) 프로그램을 활용한 ARS 전화로 발신하는데 해당 전화번호는 대부분 (송신용)전화번호이기 때문에 해당 전화번호를 수집하더라도 해당 전화번호로 전화통화를 할 수 없는 경우가 발생할 수 있다. 이에, 숨겨진 음성스팸 전화의 (송수신용)전화번호를 알아내는 것이 중요하게 되는데 해당 전화번호를 알아내는 과정 및 해당 전화번호를 습득 후 음성스팸 역공격을 하는 시스템을 제시하고자 한다.

트랩번호 기반 음성스팸 전화번호 수집 및 역공격의 프로세스는 다음과 같다.

① 음성스팸 전송자 그룹[3]은 별정통신사를 통해 ACS 계약을 한다.

② 별정통신사는 음성스팸 전송자 그룹에게 ACS 계정 및 (수신용)전화번호를 부여한다.

③ 불법스팸신고처리기관은 트랩전화번호를 웹사이트, SNS 등의 채널을 통해 무작위로 배포한다.

④ 음성스팸 관리자는 웹사이트, SNS 등에서 수집한 전화번호 DB(트랩전화번호 포함)를 불법스팸 음성멘트와 함께 계약된 ACS 프로그램 업체에 제공하여 ARS 음성스팸 발송을 요청한다.

⑤ ACS 프로그램 업체는 전달받은 전화번호 DB에 있는 전화번호로 ARS 음성스팸을 발송하기 위해 별정통신사의 ACS계정을 활용하여 발송한다.

⑥ 별정통신사는 ACS계정에 입력된 사항(ARS 음성스팸 포함)을 기간통신사에게 발송한다.

⑦ 기간통신사는 트랩전화로 ARS 음성스팸을 발송한다.

⑧ 불법스팸신고처리기관은 트랩전화로 ARS 음

3) 음성스팸 전송자 그룹은 음성스팸 관리자와 음성스팸 상담원으로 구성되어 있다.

성스팸[4])이 수신되면 상담요청을 한다.

⑨ ACS 프로그램 업체는 상담요청 한 전화번호를 DB(트랩전화번호 포함)로 저장하고 이후 음성스팸 관리자에게 해당 DB를 제공한다.

⑩ 음성스팸 관리자는 상담요청을 한 전화번호 DB(트랩전화번호 포함)에 저장된 전화번호를 음성스팸 상담원에게 분배하여 전화를 하게 한다.

⑪ 음성스팸 상담원은 트랩전화번호로 전화를 해서 상담을 수행한다. 이때 트랩전화로 전화한 숨겨져 있던 (송수신용)음성스팸 전화번호를 저장한다.

⑫ 불법스팸신고처리기관은 저장된 (송수신용)음성스팸 전화번호에 대해 정보통신서비스제공자에게 이용제한을 요청한다. 또한, 수사기관은 해당 전화번호가 이용제한 되기 전에는 음성스팸 전화번호로 지속적인 콜을 하던지 음성스팸 전화번호가 핸드폰 번호인 경우 악성코드를 다운로드 하도록 유도해서 해당 음성스팸 전화번호를 무력화 한다.

4.2.2 음성트랩 기반 음성스팸 전화번호 수집 및 역공격

(수신용)핸드폰 가상번호인 음성트랩번호를 미리 이통사를 통해서 가입하고 이를 사용해서 음성스팸 전화번호를 수집하는 역할을 한다. 음성스팸을 전송한 (송수신용)전화번호를 알아내고 수집된 음성스팸 전화번호로 역공격하는 과정에 대한 설명은 다음과 같다.

① 불법스팸신고처리기관은 음성트랩번호를 웹사이트, SNS 등의 채널을 통해 무작위로 배포한다.

② 음성스팸 관리자는 웹사이트, SNS 등에서 수집한 전화번호를 DB(음성트랩번호 포함)로 저장한다. 다만, 여기서는 음성스팸 관리자는 ACS에 ARS전화를 활용하지 않는다.

③ 음성스팸 관리자는 전화번호 DB(음성트랩 전화번호 포함)에 저장된 전화번호를 음성스팸 상당원에게 분배하여 전화를 하게 한다.

④ 음성스팸 상담원은 음성트랩전화번호로 전화를 해서 상담을 수행한다. 이때 음성트랩전화로 전화한 (송수신용)음성스팸 전화번호를 저장한다.

⑤ 트랩번호 기반 음성스팸 전화번호 수집 및 역공격의 ⑫번 단계를 수행한다.

4.2.3 스팸사실조사 기반 음성스팸 전화번호 수집 및 역공격

불법스팸신고처리기관은 불법스팸으로 신고된 내용에 대해서 사실조사를 수행하고 사실조사 과정에서 확인된 음성스팸 전화번호를 수집·저장한 후 트랩번호 기반 음성스팸 전화번호 수집 및 역공격의 ⑫번 단계를 수행한다.

4.2.4 AI 연관분석 기반 음성스팸 전화번호 수집 및 역공격

불법스팸신고처리기관은 불법스팸으로 신고된 내용에 대해서 AI 시스템을 활용하여 음성스팸간 연관분석을 수행하고 이를 통해 확보한 음성스팸 발송 그룹별 음성스팸 전화번호를 수집·저장한 후 트랩번호 기반 음성스팸 전화번호 수집 및 역공격의 ⑫번 단계를 수행한다.

4.2.5 수사기관 제공 보이스피싱 관련 음성스팸 전화번호 수집 및 역공격

수사기관에 접수된 보이스피싱 피해신고 정보에서 음성스팸 전화번호를 추출하여 저장한 후 트랩번호 기반 음성스팸 전화번호 수집 및 역공격의 ⑫번 단계를 수행한다.

4.2.6 수사기관 제공 번호변작 금융범죄 관련 음성스팸 전화번호 수집 및 역공격

수사기관에 금융범죄 수사과정에서 번호변작과 관련하여 수집된 음성스팸 전화번호를 수집·저장한 후 트랩번호 기반 음성스팸 전화번호 수집 및 역공격의 ⑫번 단계를 수행한다.

V. 제안하는 음성스팸 역공격 시스템 적용 효과

불법스팸신고처리기관에서 제공하는 불법대출 스

4) ARS 음성스팸은 대부분이 상담을 요청할 경우 1번 버튼을 누르라는 멘트를 활용하고 있다.

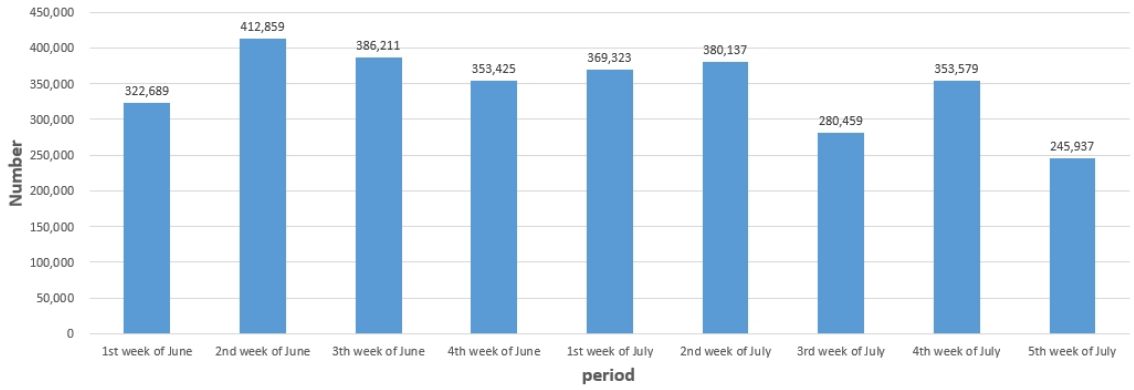


Fig. 5. Numbers graph of illegal loan voice spam by week in June - July 2021.

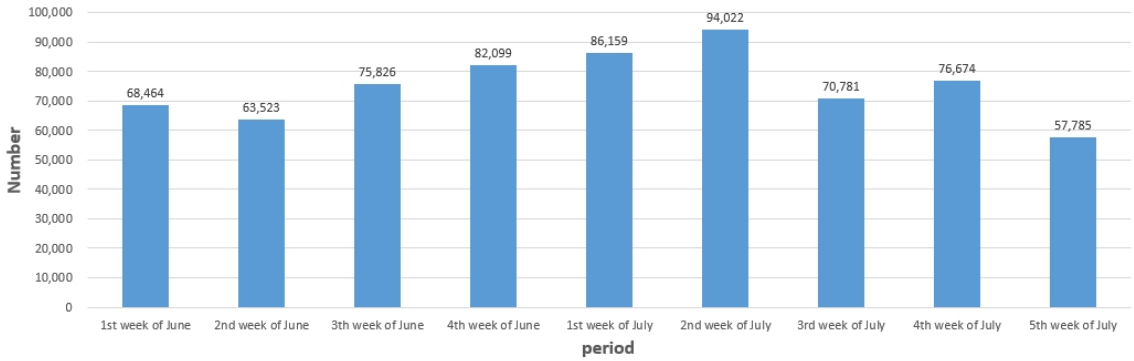


Fig. 6. Numbers graph of illegal loan message spam by week in June - July 2021.

팸 정보와 수사기관에서 제공하는 보이스피싱 신고 정보를 비교 분석하여 실제로 제안한 음성스팸 전화번호 역공격 시스템을 개발하여 적용해 보았다. 본고에서 제안한 내용 중 음성스팸 전화번호 수집단계에서는 음성트랩 기반 음성스팸 전화번호 수집, 스팸 사실조사 기반 음성스팸 전화번호 수집 및 수사기관 제공 보이스피싱 관련 음성스팸 전화번호 수집 과정을 통합(모두 적용)하여 실제 적용했다.

또한, 음성스팸 전화번호 역공격 단계에서는 불법스팸신고처리기관이 정보통신서비스제공자(유무선통신사 등)에게 수집된 음성스팸 전화번호를 이용제한(이용정지 혹은 계약해지) 요청하는 것과 수사기관이 해당 전화번호가 이용제한 되기 전에는 음성스팸 전화번호로 지속적인 콜을 발송하는 음성스팸 전화번호 이용제한 이전 적용1을 실제 적용했다. 여기서 이용제한을 요청하지 않은 음성스팸 전화번호도 다수 포함하여 음성스팸 역공격 시스템을 실행해 보았다.

개발한 음성스팸 역공격 시스템을 '21년 7월부터 적용해 본 결과, 불법스팸신고처리기관에서 음성스팸 전화번호 이용제한을 7월에 185건을 수행했고, 수사기관은 확보한 보이스피싱 피해 정보와 불법스팸신고처리기관에서 수집한 불법대출 스팸 정보로부터 추출한 1,000여건의 음성스팸 전화번호에 대해 약 2주간(21.7.19~28) 60회선의 (송신용)유무선전화를 활용하여 단기간에 약 500여건의 전화번호가 이용정지 혹은 해지된 상태로 전환되는 것을 확인했으며 이는 약 50% 성공률을 보이는 효과를 보였다. 이렇게 효과성이 뛰어남이 확인됨에 따라 제안한 시스템을 좀 더 적극적으로 적용해 보고자 향후에는 (송신용)유무선전화회선을 900회선으로 확대해서 제안한 시스템을 동일하게 적용해 볼 계획이다.

또한, 〔Fig.5〕를 살펴보면, 불법대출 음성스팸 신고건수는 '21년 1월부터 계속 증가추세에 있다가 '21년 7월1주에 369,323건을 기록했지만, 제안한 음성스팸 역공격 시스템을 적용 후 7월3주에는 280,459건, 7월5주에는 245,937건으로 7월1주 대비 불법대

출 음성스팸 신고건수가 약 34% 줄어든 것으로 나타났다. 이와 더불어 음성스팸 전화번호를 전송하는데 사용될 수 있는 불법대출 문자스팸 신고건수도 〔Fig.6〕에서 보는 바와 같이 불법대출 음성스팸 건수 추이와 비슷하게 줄어드는 것으로 나타났다. 불법대출 문자스팸 신고건수는 '21년 7월1주에 86,159건을 기록했지만, 7월3주에는 70,781건, 7월5주에는 57,785건으로 불법대출 문자스팸 신고건수가 약 33% 줄어드는 것으로 나타났다.

앞에서 열거한 본 시스템의 적용 결과를 통해 본고에서 제안한 음성스팸 역공격 시스템이 효과적인 시스템임을 입증하였다.

VI. 결 론

불법대출 및 보이스피싱으로부터 국민의 피해를 예방 및 최소화하고자 불법대출 및 보이스피싱을 자행하는 음성스팸 전화번호에 대해서 전화 통화 연결이 되지 않게 지속적으로 해당 전화번호에 콜을 보냄으로서 해당 전화번호로 불법을 자행하지 못하게 하는 음성스팸 역공격 시스템을 제안하였다.

또한, 해당 시스템 개발하여 실제 적용해서 불법대출 음성스팸 신고건수가 약 34% 줄어들었고 불법대출 문자스팸 신고건수도 약 33% 줄어드는 효과를 확인했다.

제안하는 시스템 적용 시 (송신용)유무선전화회선을 60회선만 사용했지만 향후에는 900회선으로 확대해서 제안한 시스템을 동일하게 적용해 볼 계획이다. 또한, AI 연관분석 기반 음성스팸 전화번호 수집 시스템과 트랩번호 기반 음성스팸 전화번호 수집 시스템도 개발하고 있으며, 제안하는 시스템의 수집 단계 해당 2개 시스템을 추가적으로 사용한다면 음성스팸 전화번호 수집에 기여하는 바가 클 것으로 예상되며 이를 통해 본 시스템의 효과가 극대화 될 것으로 기대된다.

References

〔1〕 Ministry of Government Legislation, "Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.", June 2021.

〔2〕 Korea Information & Security Agency - Illegal Spam Response Center, https://spam.kisa.or.kr/, Sep. 2021.

〔3〕 Korea Communications Commission, "Report on Spam Distribution in the Second Half of 2019", Mar. 2020.

〔4〕 Korea Communications Commission, "Report on Spam Distribution in the First Half of 2020", Sep. 2020.

〔5〕 Korea Communications Commission, "Report on Spam Distribution in the Second Half of 2020", Mar. 2021.

〔6〕 Korea Communications Commission, "Report on Spam Distribution in the First Half of 2021", Sep. 2021.

〔7〕 Edaily, "Voice phishing investigation", https://www.edaily.co.kr/news/read?newsId=02236966629116160&mediaCodeNo=257&OutLnkChk=Y, Sep. 2021.

〔8〕 Moneytoday, "Voice phishing investigation", https://news.mt.co.kr/mtview.php?no=2015022412374200746&outlink=1&ref=https%3A%2F%2Fsearch.naver.com, Sep. 2021.

〔9〕 Mbc, "Voice phishing investigation", https://imnews.imbc.com/news/2021/society/article/6047664_34873.html, Sep. 2021.

〔10〕 News1, "Voice phishing investigation", https://www.news1.kr/articles/?4177076, Sep. 2021.

〔11〕 Hankookilbo, "Voice phishing investigation", https://www.hankookilbo.com/News/Read/A2021070815310005561?did=NA, Sep. 2021.

〔12〕 News1, "Voice phishing investigation", https://www.news1.kr/articles/?4396935, Sep. 2021.

〔13〕 Narucnc, "Auto Waring Call System", https://narucnc.co.kr/, Sep. 2021.

〈저 자 소 개〉

박 해 룡 (Haeryong Park) 종신회원
1999년 2월: 전남대학교 수학과 졸업
2001년 2월: 서울대학교 수리과학부 (암호학) 석사
2006년 8월: 전남대학교 정보보호 (암호학) 박사
2000년 12월~현재: 한국인터넷진흥원 팀장
〈관심분야〉 암호 설계 및 분석, 사용자 인증, 정보보호 R&D, 스팸 정책 및 조사, 개인정보보호

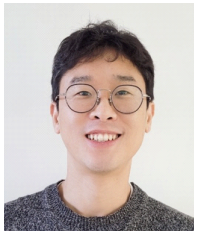
박 수 정 (Sujeong Park) 정회원
2014년 2월: 한림대학교 사회복지학과 졸업
2015년 11월~현재: 한국인터넷진흥원 선임연구원
〈관심분야〉 스팸 정책 및 조사, 개인정보보호

박 강 일 (Kangil Park) 정회원
2009년 2월: 한국방송통신대학교 컴퓨터과학 졸업
2015년 2월: 남서울대학교 산업보안 석사
2005년 9월~현재: 한국인터넷진흥원 수석연구원
〈관심분야〉 산업보안, 보안산업 해외진출, 스팸정책 및 조사, 개인정보보호, 정보보안지수

정 찬 우 (Chanwoo Jung) 정회원
2017년 2월: 전남대학교 전자컴퓨터공학부(컴퓨터공학과) 졸업
2018년 3월~현재: 한국인터넷진흥원 주임연구원
〈관심분야〉 정보보안 시스템 운영 및 개발, 스팸 정책 및 조사, 개인정보보호

김 종 표 (Jongpyo Kim) 정회원
2003년 8월: 경희대학교 정보통신전문대학원 정보통신망관리공학과 석사
2005년 3월~현재: 한국인터넷진흥원 팀장
〈관심분야〉 보이스피싱 대응 정책, 스팸대응 정책, 개인정보보호

최 근 모 (Keun Mo Choi) 정회원
2019년 7월: 한양대학교 행정학과 재학 중
2014년 6월~현재: 서울특별시경찰청 수사부 지능범죄수사대/금융범죄수사대 팀장
〈전문 분야〉 기업범죄 전문 수사관, 보이스 피싱 관련 전문 수사팀



모 용 헌 (Yonghun Mo) 정회원
2011년 7월: 국민대학교 영어영문학과 졸업
2015년 3월~현재: 서울특별시경찰청 수사과 금융범죄수사대 수사관
〈관심분야〉 스팸 정책 및 조사, 개인정보보호, 금융범죄수사