메신저피싱 예방을 위한 Open API 활용 메신저 위험 인자 감지 시스템 설계

김도윤 [1], 박광영 [2]
[1] 숭실대학교 전자정보공학부
[2] 숭실대학교 소프트웨어학부

yun0368@soongsil.ac.kr, 1004pky@ssu.ac.kr

Design of Messenger RISK Detection System for Smishing Prevention Using Open API

Do-Yun Kim[1], Kwang-Young Park[2]
[1] Dept. of Electronic Engineering, Soong-Sil University
[2] Dept. of Software, Soong-Sil University

요 약

코로나 19 로 대면이 아닌 비대면이 일상이 되며 공공기관과 기업들이 사용자에게 보내는 메시지의 양이 증가하였다. 이에 따라 공공기관을 사칭하는 메신저피싱이 증가하였다. 본 논문에서는 OpenAPI 데이터를 활용한 메신저 위험 url 감지 시스템의 설계를 제시한다. 메신저피싱으로 인한 금전 피해 및 개인정보 탈취를 예방하기 위해 메시지의 포함된 피싱 url 과 기관, 기업의 사전 안전 인증을 통한 안전 url 을 구분한다. 이를 통해 사용자에게 안전하고 쾌적한 인터넷을 제공한다. 향후, 제안하는 시스템의 현실적인 검증과 성능 평가가 필요하다.

1. 서론

코로나 19 로 인해 메신저의 역할이 커지며 2019 년도부터 지금까지 메신저 피싱의 피해가 증가하였다. 모바일 메신저를 통해 이체 요구, 개인정보 탈취, 피싱 url 접속을 통한 원격조종 앱 설치를 유도한다.[1] 허위 결제 문자, 택배사 사칭 문자, 공공기관 사칭을 하기에 사용자는 의심 없이 url 에 접속하며, 기본 메신저에서는 경고메시지만 제공할 뿐 피싱 예방 시스템은 존재하지 않는다.

기존 백신 어플리케이션들은 의심 번호로부터 송신된 음성통화 및 메시지의 경고를 주거나, 악성앱이 설치되기 시작할 때 알림이 발생한다. 또한 악성 url 을 검증하는 다양한 사이트가 존재하지만. 이는 사용자가 직접 해당 사이트에 url 을 입력하는 과정이 필요하다. 그러나 메신저피싱은 사용자가 메신저로 전송받은 url 을 의심없이 누르며 시작된다. 안전한 url 과 위험한 url 을 일반 사용자가 구별해 내는 것은 쉽지 않은 일이다.

이에 본 논문에서는 메신저 프로그램의 백그라운드에서 동작하며 url 을 감지 시, 자동으로 url 을 추출하여 OpenAPI 기반 서버 데이터베이스에 전송하여 위험도를 판단하고 메신저피싱을 예방하는 시스템을 제안한다.

2. 메신저피싱

메신저피싱은 문자메시지나 메신저를 통해 이루어지는 피싱이다. 스미싱(Smishing)와 같은 의미로 불리며, Smishing 은 SMS 과 phishing 의 합성어로 문자 메시지를 통한 피싱을 뜻한다.

메신저피싱은 두 가지 형태의 프로세스가 있다. 허위 결제 문자, 공공기관 사칭을 하여 사용자의 개인정보(아이디, 패스워드, 계좌)를 유출하는 방식과 특정 사이트로 유도하여 해킹 앱, 스파이웨어, 랜섬웨어를 설치하는 방식이다. [2]

두 가지 방식 모두 피싱 url 을 기반으로 이루어진다. 해당 url 을 통해 접속하여 개인정보를 입력하거나 첨부파일이 설치되며 피싱이 시작된다. 하나의 피싱 url 이 제작되면 보이스 피싱과는 다르게 전파속도가 빠르고 다수의 피해자를 발생시킨다. 따라서, url 의 안전성을 검증하는 것이 메신저피싱 방지의 핵심이라 판단한다. 이에 본 논문은 메신저의 백그라운드에서

url 의 수신을 감지하면 이를 검증하는 시스템을 제안한다.

3. 메신저 위험 인자 감지 시스템

3-1 url 링크 신뢰성 사전 인증제

메신저 피싱 예방에서 피싱 url 을 감지하여 차단하는 것이 중요하다. 또한 사용자가 안전한 url 을 걱정 없이 접속하는 것도 중요하다. 이에 한국 인터넷 진흥원에서 제공하는 피싱사이트 url 모음(그림 1)을 활용한 url 링크 신뢰성 사전 인증제를 제안한다.

우선 공공기관과 기업에서 url 이 첨부된 메시지를 전송하는 경우, 미리 url 도메인을 시스템에 등록하여 신뢰성 검사를 받고 인증 데이터베이스에 등록한다. 한국 인터넷 진흥원의 피싱사이트 모음은 피싱 데이터베이스의 등록한다. 이후 감지 시스템이 메신저의 백그라운드에서 작동하며 url 이 포함된 메시지의 경우 url 의 안전 인증 유무와 피싱 url 인지를 감지한다. 미등록 url 송, 수신 시에는 'url 안전 인증을 받지 못한 링크입니다. 메신저 피싱의 유의바랍니다.'와 같은 알림을 발생시켜 피해를 방지한다. 웹과 앱을 이용하여 시스템에 접속하여 url 입력 시, 안전 인증의 유무와 피싱 url 을 감지하여 사용자에게 전달한다.

1975	11월 29일	http://hrc.wtbj.hair
1976	11월 29일	http://yfgd3.ponm3.hair
1977	11월 29일	http://jhrx5.oiwx.hair
1978	11월 29일	http://bit.ly/3Pjutql
1979	11월 29일	http://han.gl/GHMzb
1980	11월 30일	http://7ydb.wunrx.quest
1981	11월 30일	http://m14.j0xt.black
1982	11월 30일	http://fdssg3.svyw.hair
1983	11월 30일	https://nanourl.org/GfJ
1984	11월 30일	http://tuc.bit7.ink
1985	11월 30일	http://hrc.wtbj.hair
1986	11월 30일	http://kut31.xvys.hair

한국인터넷진흥원_피싱사이트 URL_20221130

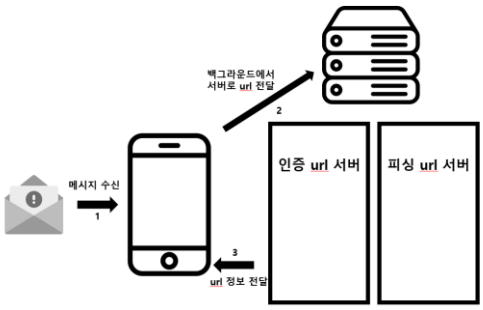
(그림 1) 한국인터넷진흥원 피싱사이트 데이터셋

3-2 피싱활용 유의어 감지

메신저 피싱의 기반이 되는 메시지는 문자로 이루어져 있다. 보이스피싱과는 다르게 쉽게 위험 단어를 추출해 낼 수 있다. url 링크 신뢰성 사전 인증에 실패한 무인증 url 이 첨부된 메시지에 추가 확인을 진행한다. 검토된 메시지의 계좌 이체, 개인정보 관련 등 문자가 검색될 시, 경고 알림을 나타낸다.

3-3 시스템 구조

그림 2 와 그림 3 은 본 논문에서 제안하는 시스템의 구조와 사용자 인터페이스이다. 본 시스템은 메신저를 통해 url 을 수신 시, 백그라운드에서 서버로 url 을 전달한다. 이를 데이터베이스 서버에 url 과 비교하여 안전 인증 url, 피싱 url, 무인증 url 을 확인하여 사용자에게 전달한다. 또한 무인증 url 에 경우, 메시지에서 피싱에 활용되는 유의어를 추가로 감지한다. 이를 통해 사용자는 메신저피싱을 예방한다.



(그림 2) 시스템 구조

(그림 3) 사용자 인터페이스

4. 결론

본 논문에서는 OpenAPI 데이터와 신뢰성 사전 인증제로 피싱 url 을 구분해 내는 메신저 피싱을 감지해 내는 시스템을 제안한다. 제안하는 시스템은 의심번호 방지와 악성 앱 설치 방지 같은 방식이 아닌 Open API 의 피싱 데이터와 인증된 공공기관과 기업의 url 을 활용하여 메신저 피싱의 1 차 예방을 목표로 한다. 피싱 url 자체를 사전에 방지함으로써 금전 피해, 개인정보 유출을 막을 수 있으며, 이를 통해 사용자들에게 안전하고 쾌적한 인터넷 생활을 제공한다. 향후 개발에서는 GPT4 기반 감지 모델을 적용하고자 한다. 또한 제안하는 시스템의 현실적인 검증과 성능 평가가 필요하다.

ACKNOWLEDGMENT

"본 연구는 과학기술정보통신부 및 정보통신기획평가원의 지역지능화혁신인재양성사업의 연구결과로 수행되었음" (IITP-2023-RS-2022-00156360)

참고문헌

[1] 금융감독원. "21 년 보이스피싱 피해현황 분석". KDI 경제정보센터. 2022

[2] Yeboah-Voateng, E.O. "Phishing, SMiShing & Vishing: An assessment of threats against mobile devices". Journal of Emerging Trends in Computing and Information Sciences. 5. 297-307. 2014