Commercial Anti-Smishing Tools and Their Comparative Effectiveness Against Modern Threats

Daniel Timko, Muhammad Lutfor Rahman
California State University San Marcos
San Marcos, CA, USA
timko002@csusm.edu, mirahman@csusm.edu

Abstract

Smishing, also known as SMS phishing, is a type of fraudulent communication in which an attacker disguises SMS communications to deceive a target into providing their sensitive data. Smishing attacks use a variety of tactics; however, they have a similar goal of stealing money or personally identifying information (PII) from a victim. In response to these attacks, a wide variety of anti-smishing tools have been developed to block or filter these communications. Despite this, the number of phishing attacks continue to rise. In this paper, we developed a test bed for measuring the effectiveness of popular anti-smishing tools against fresh smishing attacks. To collect fresh smishing data, we introduce Smishtank.com, a collaborative online resource for reporting and collecting smishing data sets. The SMS messages were validated by a security expert and an in-depth qualitative analysis was performed on the collected messages to provide further insights. To compare tool effectiveness, we experimented with 20 smishing and benign messages across 3 key segments of the SMS messaging delivery ecosystem. Our results revealed significant room for improvement in all 3 areas against our smishing set. Most anti-phishing apps and bulk messaging services didn't filter smishing messages beyond the carrier blocking. The 2 apps that blocked the most smish also blocked 85-100% of benign messages. Finally, while carriers did not block any benign messages, they were only able to reach a 25-35\% blocking rate for smishing messages. Our work provides insights into the performance of anti-smishing tools and the roles they play in the message blocking process. This paper would enable the research community and industry to be better informed on the current state of anti-smishing technology on the SMS platform.

BIBLIOGRAPHIC REFERENCE

Introduction

Motivation
To counter the threat of smishing, anti-smishing tools and regulations have been developed to help combat smishing.
- SMS filtering can be applied at several phases of the messaging process.
- Each tool implements their own techniques to stop malicious SMS.
- SMS messages are regulated through the Telephone Consumer Protection Act (TCPA).

Despite these efforts, smishing continues to increase.
- Within first six months of 2021, smishing increased by 700%. [1]
- SMS messages are regulated through the Telephone Consumer Protection Act (TCPA).

Contributions
Define the role that our tested SMS filters play on the messaging process.
- We explore 5 bulk messaging services, 5 carriers, and 10 anti-smishing apps.
- Smishtank – A collaborative resource for Smishing datasets.
- We provide a live SMS feed of unfiltered smishing messages.
- We analyze our collected phishing SMS across several categories.
- We provide a public repository called smishtank.com for future researchers.

Methodology

SMS Collection
- To collect "fresh" smishing messages, we created smishtank.com.
- 75 messages submitted.
- 55 verified through a security professional.
- 20 selected for delivery.

Testing Process
Benign
- From the UCI Machine learning repository.

Virus and Domain Info

Data Characterization

Tool Performance

4. Results

VirusTotal Scores

Domain History

[30/46] created within 1-3 months of us receiving the message.

[36/46] if last updated is considered.

[3/46] could not be confirmed.

[5/46] used authentic domains (e.g., social media smishing).

5. Discussion

Recommendations

Opt-In and Opt-Out

- Opt-In compliance was loosely enforced.
- Easy to find services that don’t require Opt-Out dialogue.

Message Blocking

- Similar messages blocked across carriers on the same network implies shared filtering.
- Most of the tested Anti-Smishing Apps and bulk messaging services blocked no additional messages over what the carrier already blocked.

6. Conclusion and Future Work

- We provide a public repository called smishtank.com for future researchers.
- We scanned messages through VirusTotal and characterized the dataset.
- Some bulk messaging services, carriers and anti-smishing apps performed significantly different than one another on our smishing sets.
- In future, we will investigate the role of Machine Learning in commercial anti-smishing technology.