Detecting and Characterizing SMS Spearphishing Attacks

Mingxuan Liu, Yiming Zhang, Baojun Liu,
Zhou Li, Haixin Duan, Donghong Sun

清華大學 Tsinghua University

UCI University of California, Irvine

奇安信 QI-ANXIN

What is SMS Spearphishing Attacks ?

What is SMS Spearphishing Attacks ?

Example of Spearphishing SMS

Spearphishing Short Messages:

(1) Contains victim's personal information

(2) Contains attacker's contact method

Spearphishing Attack: A Persistent Problem

Spearphishing attacks are widely spread via Email, social media and even telephone.

Billions of dollars have been lost due to spearphishing attacks in recent years!!

From: “Alice”<alice@company.com>
To: “Bob’<bob@victim.com>
Subject: Company

Hi, Bob
Here is the new contract in this link (which is a phishing link.)

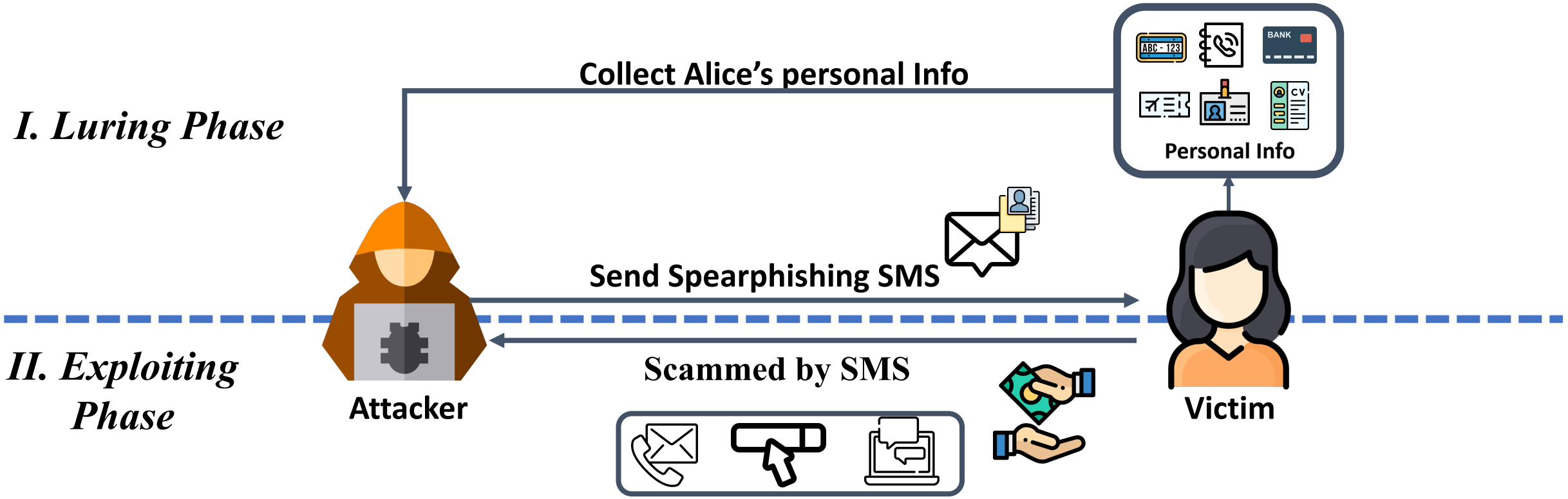
Regards,
Alice

Spearphishing Email

Spearphishing Telephony

However, SMS Spearphishing attack is very different from these attacks via other channels!!

Threat Model of SMS Spearphishing Attack



Dataset: A Real-World Dataset

- 31,956,437 detection logs of spam messages from Dec. 1 2019 to Mar. 25 2020 (three months).

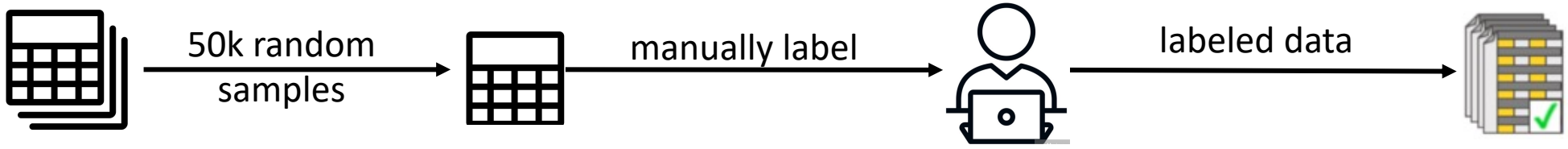
Example of a spam message log

Timestamp	Sender Phone Number	IMEI (hashed)	IMSI (hashed)	IP address of mobile client	Message content	
2020-02-01 15:34:01	400****3371	HASH_1	HASH_2	172.xxx.xxx.231	尊敬的Name，你的航班MU****，福州飞往南京，已经被取消。退订请联系东方航空，0371-65****19	Dear Name, your Flight MU****, from Fuzhou to Nanjing, has been cancelled. Please contact Eastern Airline 0371-65****19

- Discussion of **ethical** considerations (shown in our paper).

Detecting Spearphishing Messages

Collect Ground-truth Dataset



Origin Dataset (31.96 M)

Subset for Manually Inspect

2 Researchers Labeled Independently

Ground-Truth Dataset with **1,196** spearphishing messages

Key Observations

- "Luring": Personal information of victims.

  Name, Flight Info., Plate Nu., Bank Card Nu. and ID Card Nu.

- "Exploiting": Out-of-band contacts of attackers.

  URL, CellPhone, Hotline, Phone, QQ, WeChat

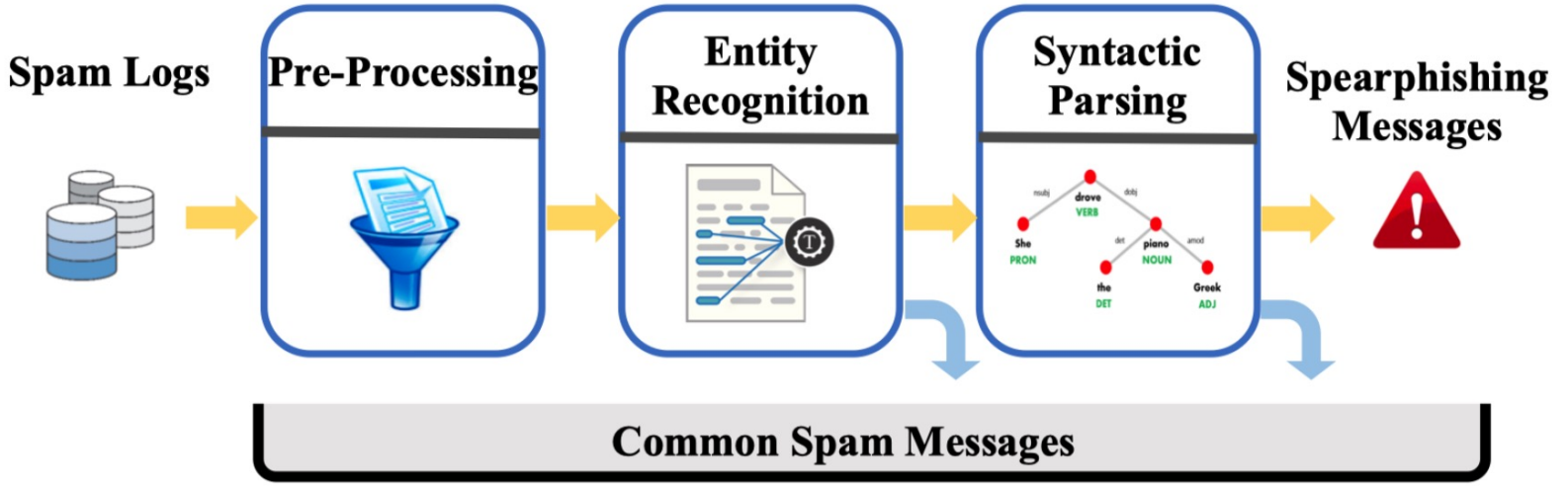
- "Syntactic": Syntactic relationship of personal pronouns.

  I am **NAME (Attacker)** from Lottery company.
  This is my phone number: 17***31.

Syntactic Relationship

Dear Alice: Your reservation for flight MU**** from Fuzhou to Nanjing on February 24 has been forced to be cancelled due to mechanical problems. Please contact China Eastern Airlines 0371-65****19 for refund or ticket change [Eastern Airline]

Detection System of SMS Spearphishing Attack



Step I: Data Pre-Processing

"Sanitize" the text content of fraudulent messages before forwarding them to the next module.

Origin Format	Sanitized Format
d1git	digit
hell0	hello
微信	微信 (Wechat)

Step II: Entity Recognition

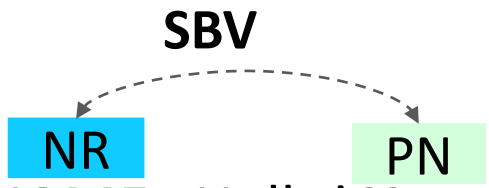
Entity Type	Identify Method
Name	Name Entity Recognition
Flight, License Plate, License Plate, License Plate	Regular Matching
URL, CellPhone, Hotline, Phone, QQ, Wechat	Regular Matching

Detection System of SMS Spearphishing Attack

Step III: Syntactic Parsing

Spearphishing

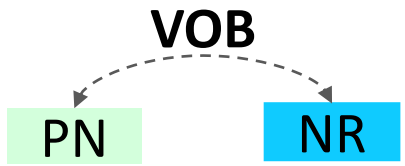
SBV: Subject-Verb



NAME, Hello! **Your** payment is overdue. Please contact 61***97. [Bank of China]

Promotion

VOB: Verb-Object



I am **NAME** from Lottery company. This is my phone number: 17***31.

* NR: Name. PN: Pronoun.

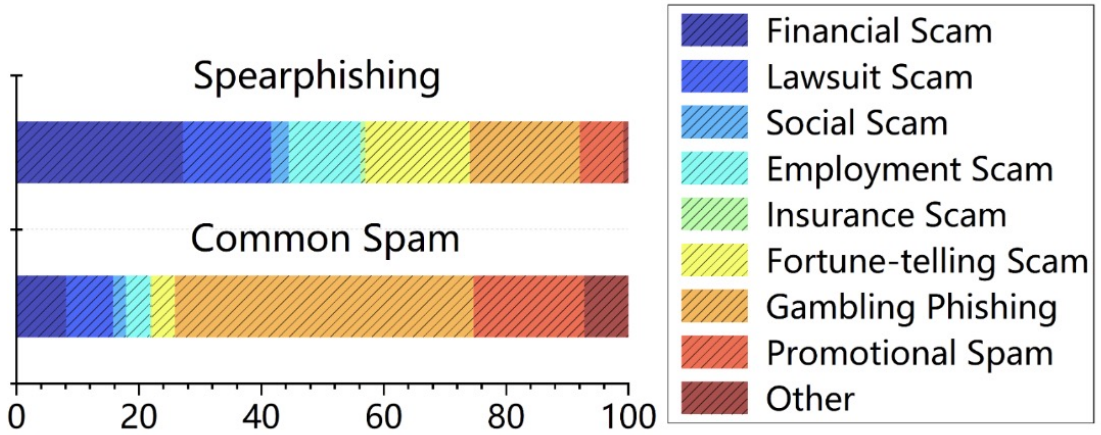
Our detection system reports 90,801 spearphishing messages, with 96.16% precision and 75.33% recall in ground-truth dataset.

Measurement of SMS Spearphishing

Categories of Spearphishing SMS

Examples of each categories

Category	Example of message content
Financial Scam	Dear Mr/Mrs. **NAME**, your BOC credit card has been suspended due to an overdue payment. Please contact 86137****765.
Lawsuit Scam	[CMB] **NAME**, your credit card has been deemed to be seriously overdue. We will formally prosecute you after 24 hours! Please contact: 86239****7834
Social Scam	**NAME**, how are you recently? I changed WeChat. Please add my new WECHAT 266****491.
Employment Scam	**NAME**, hello! Your resume in 5*.com investment has been accepted. Please contact the QQ: 33****471.
Insurance Scam	[China Life Insurance] Dear **NAME**, our company has issued a commercial insurance policy for your car, **PLATE**. Visit http://***.cc/bX8Vg for details
Fortune-telling Scam	[Lingji Culture] **NAME**. Full analysis of fortune in next ten years is coming! See the future and prevent bad luck: https://s.k****a.cn/dbgc8
Gambling Phishing	Hi, **NAME**. Yabo Sports join hands with Wuhan, register on f**8.cn and you can get recharge and get masks, come on, Wu Han!
Promotional Spam	[Tantan application] **NAME**, someone loves you, do you want to accept? It is only 3 Km away from you! Click tan****pp.com.
Other	Mr. **NAME**, do you want to purchase brand products at a discount? Please contact QQ: 324 *** 558.



Campaign Analysis

Clustering Campaigns

Messages embedded with the **same contact** or from the **same content template** are belonging to the same campaign.

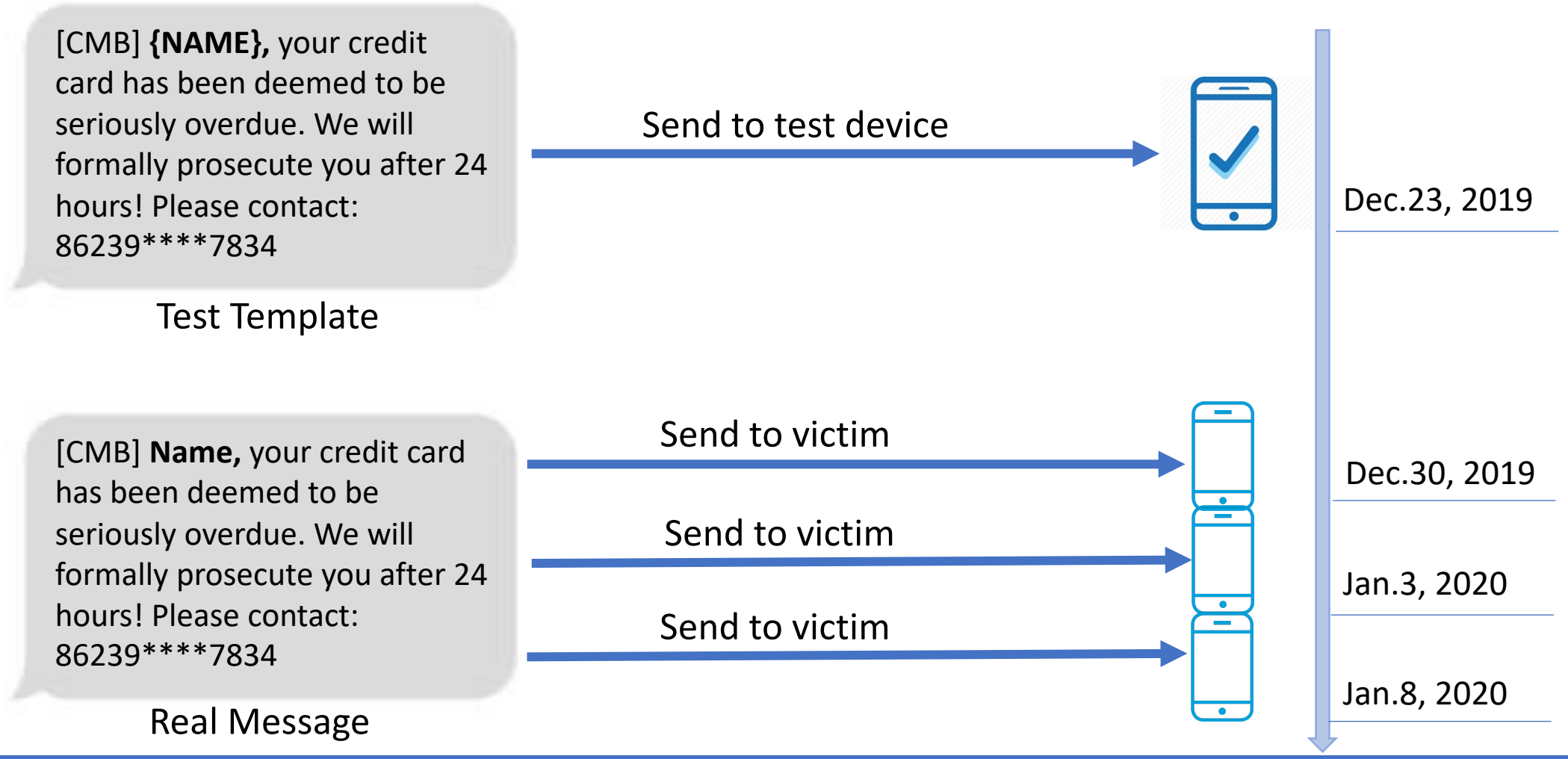
- A total of **11,475** campaigns were reported.

Overall Analysis of Campaigns

- Long-Tail Distribution: a few campaigns hold the majority of the market share.

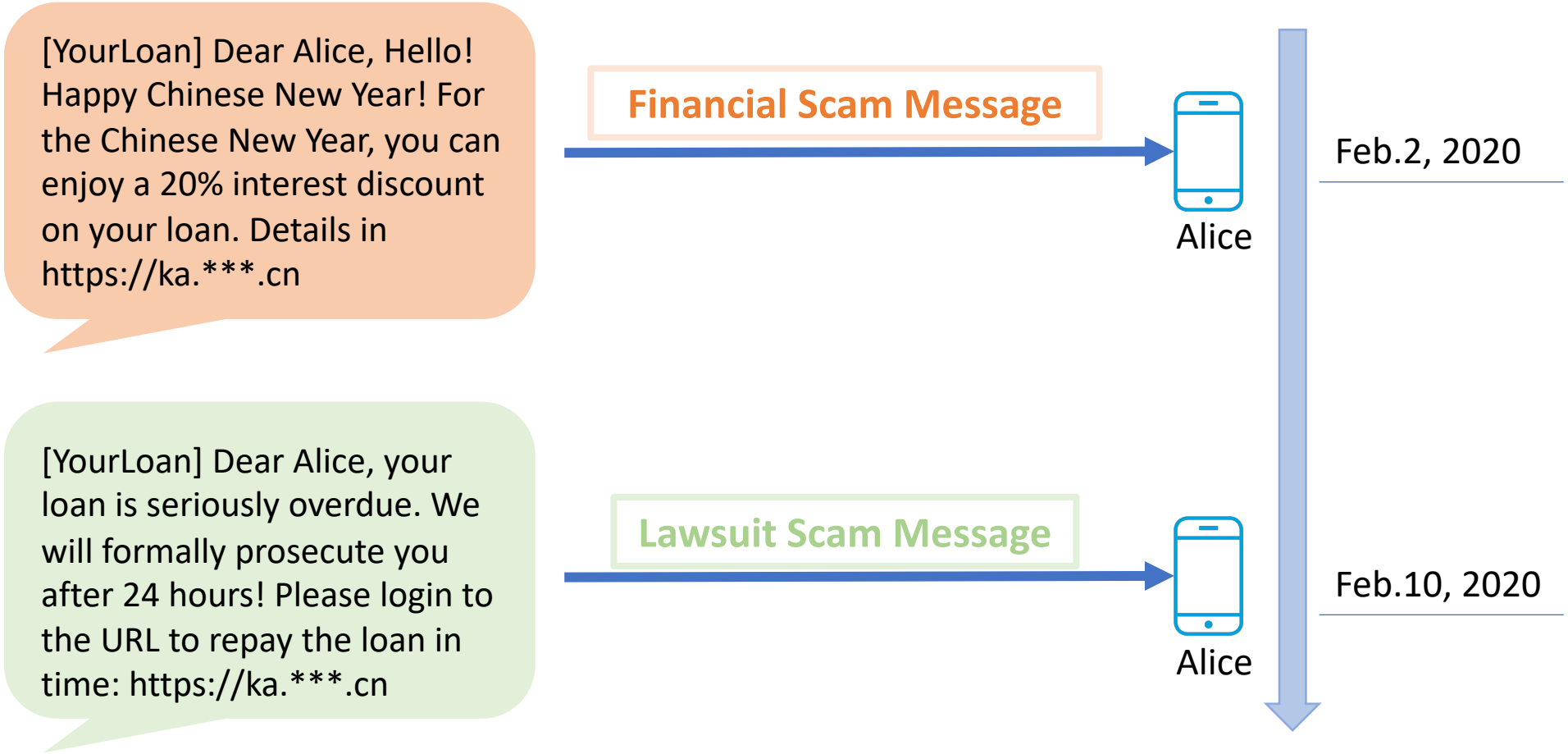
- Interesting Strategies.

Strategies of Spearphishing: Test-Sending



4 Campaigns employ "test-sending" strategy, which totally sent **539** test messages and **9,062** formal spearphishing messages and affected **2,275** victims.

Strategies of Spearphishing: Progressive Deception



The strategy indicates that spearphishing attackers would track victims for a continuous period, which is more costly than one-time scams by also bringing high profits.

Strategies of Spearphishing

Multi-Semantic Evasion

Semantic 1: Financial

[Guangfa Bank] Dear Alice: Bob remitted 2.88 RMB to your account with the message: Tiancai Gambling service in tc***.com will send bonus to new users.

Semantic 2: Gambling

Global Affair Integration

Hi, NAME. Yabo Sports join hands with Wuhan, register on f**8.cn and you can get recharge and get masks, come on, Wu Han!

Profound Real-World Impact of SMS Spearphishing

Victim Coverage

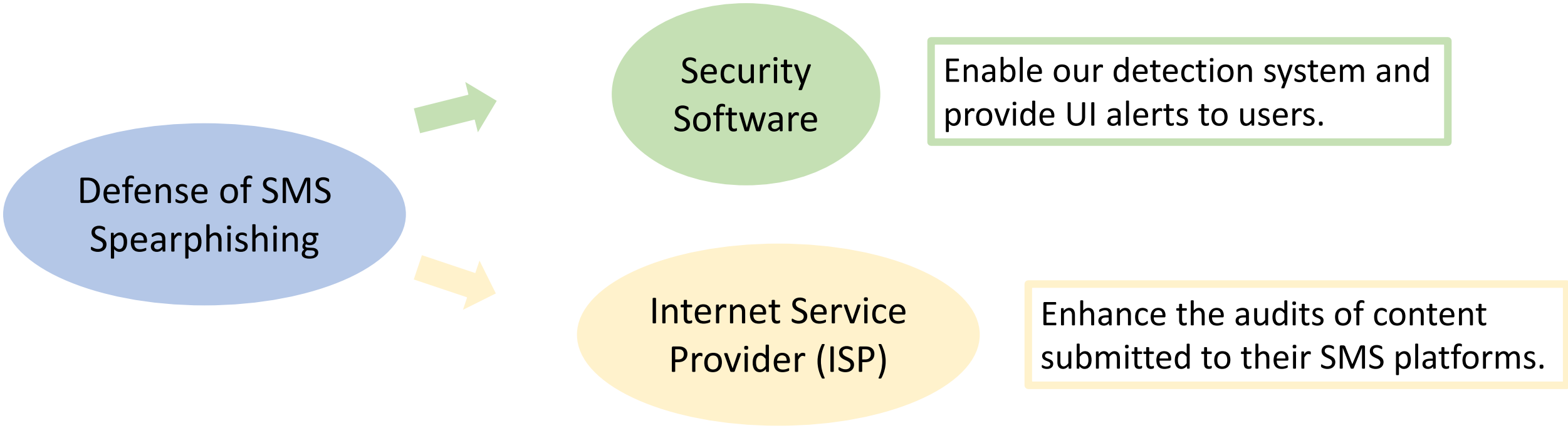
Around **24k victims** were endangered by spearphishing spam SMS from Dec. 2019 to Mar. 2020, covering all the provinces in China.

Follow-Up Domain Visits

[China Life Property and Casualty Insurance] Dear insured Name, our company has issued a commercial insurance policy for your car Yue MP***3, policy number is 805****612, the insurance period is 2020-03-19-2021-03-18, the premium amount is 1305.55 RMB. For more information, please see http://9**.cc/b***g

1,392 (94.50%) domains are marked as malicious, of which 105 are phishing-related.

Mitigation Recommendation



Attacking strategies we found would assist multiple parties in designing new detection methods of spearphishing SMS.

Summary

- **A first systematical measurement study on SMS Spearphishing ecosystem**

  From a country-level dataset, with 31.96M real-world data

  Design a NLP-based detection system

- **Understand the strategy and behavior of spammers**

  From Macro-Level and Micro-Level

  Still growing, with new categories emerging and various evasion strategies

- **Recommendation for mitigation SMS Spearphishing attacks**

  Attacking strategies can assist in designing new detection methods

清華大學
Tsinghua University

UCI University of California, Irvine

奇安信
QI-ANXIN

Detecting and Characterizing SMS Spearphishing Attacks

Mingxuan Liu, Yiming Zhang, Baojun Liu,
Zhou Li, Haixin Duan, Donghong Sun

Email: liumx18@mails.tsinghua.edu.cn