RSAConference2015
Abu Dhabi | 4–5 November | Emirates Palace

SESSION ID: CCT-R04

Understanding Cyber Attacks That Leverage the Telephony Channel

Payas Gupta

Research Scientist
CRISSP-AD, New York University Abu Dhabi
payasgupta@nyu.edu

In collaboration with

Mustaque Ahamad

Professor at Georgia Institute of Technology
Global Professor at New York University Abu Dhabi
Former Director, Georgia Tech Information Security Center

Pindrop Security

Provides Solutions to protect enterprise call centers and phone users.

جامعة نيويورك ابوظبي
NYU | ABU DHABI

GLOBAL THREAT

Robocall Credit Card Interest Scam Continues to Plague Consumers

by HERB WEISBAUM

Has "Rachel from Card Services" called you?

Telephone fraudsters know that Americans are fed up with high interest rates on their credit card balances and have for years been trying to cash in on that frustration by tricking consumers into paying them as much as several thousand dollars for bogus rate reduction programs.

This con, often initiated by pre-recorded robocallers like "Rachel," has been going on for years. And despite numerous enforcement actions by the Federal Trade Commission (FTC), it just won't go away.

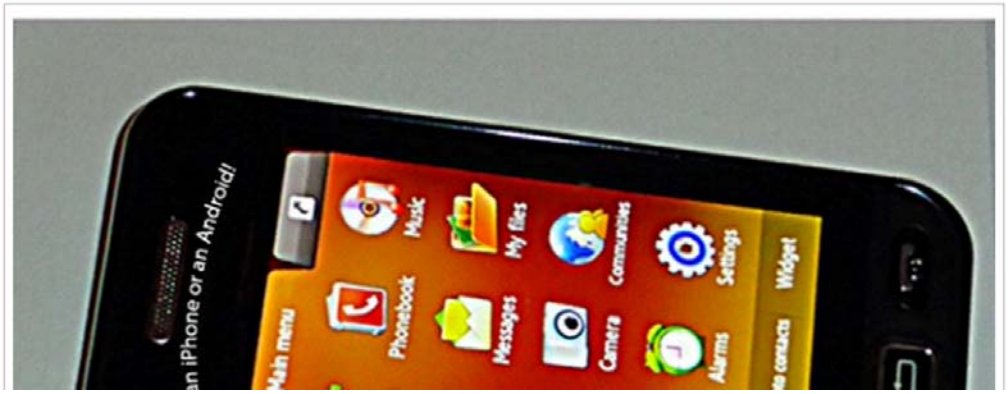
'It's disheartening'

Rachel Credit Card Calling, USA

Wangiri Telephone Fraud – One Ring to Scam Them All

BY DAVID HARLEY POSTED 10 FEB 2014 - 04:53AM

OPINION 1 TAGS BETTER BUSINESS BUREAU FACECROOK SNOPES WANGIRI



Wangiri Fraud, Japan

The unstoppable "tech support" scam

Advice | Sep 15, 2015

Like 212

Tech Support Scam, UK

Duped Hongkongers hand over HK$27m after scam phone calls by fake mainland Chinese officials

Professionals and businesspeople among those to hand over HK$27m to people posing as mainland officials in first six months of the year after just four similar cases last year

Samuel Chan
samuel.chan@scmp.com

PUBLISHED : Wednesday, 15 July, 2015, 3:14am
UPDATED : Wednesday, 15 July, 2015, 2:48pm

Fake Officials Fraud, China

Scamsters back with bait of etisalat prizes

Beware of callers detailing rewards process involving bank details or prepaid credit

By Shweta Jain, Deputy Business Editor
Published: 21:00 June 6, 2013

GULF NEWS

Dubai: Even after over three years of scam warnings from etisalat, SIM card scamsters are at it again.

In a conversation with a Gulf News employee on Wednesday, a caller claiming to be from etisalat's finance department and using an etisalat SIM number offered Dh200,000 in prize money following an apparent draw at the telecom operator's headquarters in Abu Dhabi.

The receiver of the call was asked to follow a process before receiving the prize money. This involved, first, to disconnect the phone call and call back the caller on his number. The person was then asked by the caller to note down what he described as a "lucky number: 89971" besides a "bank coupon number".

Etisalat scam, UAE

#RSAC

UNDERSTANDING TELEPHONY ABUSE

جامعة نيويورك ابوظبي
NYU | ABU DHABI

Current Data Sources

- Telcos
- Crowd sourced
  - FTC, CRTC fraudulent complaint datasets
  - 800notes open datasets
- Proprietary

ACT Principles

- Accuracy
- Completeness
- Timeliness

Accuracy

PROBLEMS WITH CURRENT DATA SOURCES

Details of Calls

909-693-3689

Did you get a call from 9096933689? Read the posts below to find out details about this number. Also report unwanted calls to help identify who is using this phone number.

909-693-3689
Country: USA
Location: California (Anaheim, Chino, Diamond Bar)

Annoyed Victim
1 h 27 min ago

0

I have received probably 30 calls to my cell phone from this number. Never leaves a message. It's truly annoying. I have no idea who or where this person is calling from and can only assume it's a scam!

Caller: No idea

Reply !

Report a phone call from 909-693-3689:

Your Name *

Your name as you would like it to appear in the title of your post.

Message *

Perception v/s Reality

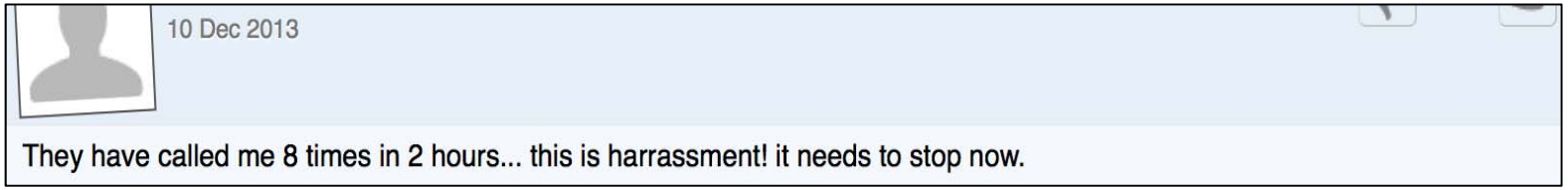
Also got this call on
nov 8
nov 9, and
nov 10. Extremely annoying. It cost me about 2 hrs on nov 8 to figure out who was calling me, cuz I was expecting a call from my friend who is traveling in US, and this call bothered me for 2 days until now!

Caller: Rogers
Call Type: Telemarketer

We keep getting calls, even several times a day, from 800 288 2020! And this is AT&T....the company we've done business with for years....why would they want to annoy their very bread and butter? Common sense says they would not or they will go down the toilet faster than a flush. What does this mean....SCAMS....which AT&T being a....err, "phone company" in part, better get on the ball and do something about this quickLY!! At least they should put a notice out to their customers that it is "not YOU who is acting so irresponsibly"...or are they?

Caller: AT&T

No Actual Timestamps



Been getting these calls for hours now. I tried to unsubscribe but the phone call drops three digits into my cell phone number. I only answered twice. It was the same lady 'Ashley' I hung up the first time. The second time I answered, I told them to stop calling me right now. She immeadiatley hung up. I haven't been called since, but it usually only happens once an hour so they may call back.

Caller: Academic Advisor.
Call Type: Survey

Spoofing

This number call me multiple times a day for the past 5 weeks!!!

I answered twice claiming they are Chase bank! I do not have a bank with Chase!!!

They ask me for private information even though I do not have a Chase account!!!

Wish they would leave me alone!!!!!!!!!

Caller: Scammers!

28 May 2014

Got a call showing my own phone # on called ID, answered to find out what was going on, it was Rachel from card services....I guess now I need to get rid of my phone#

My daughter had the same thing happen on her phone the week before(she lives in a different town)

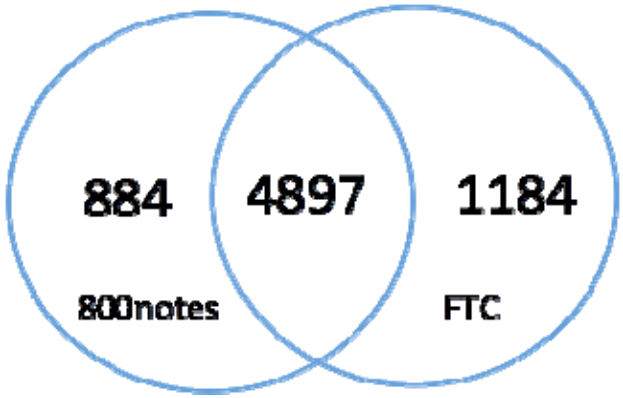
FED UP !!

Completeness

PROBLEMS WITH CURRENT DATA SOURCES

Not all fraudulent calls are reported

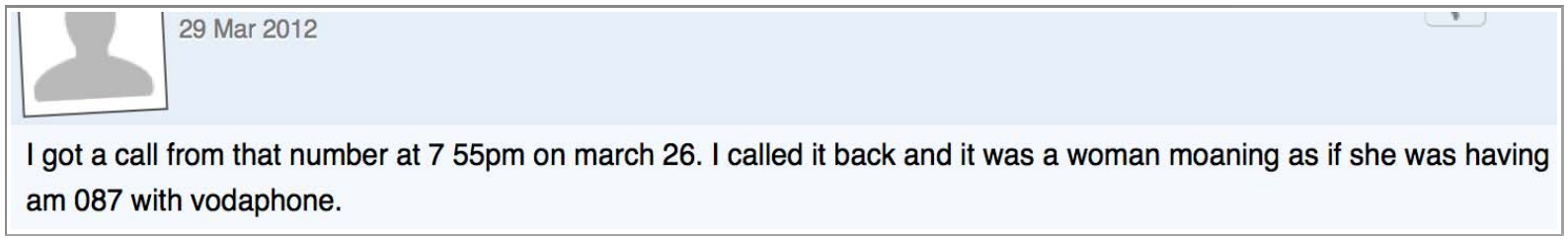
- Compared both FTC and 800notes against each other for a certain set of numbers



Timeliness

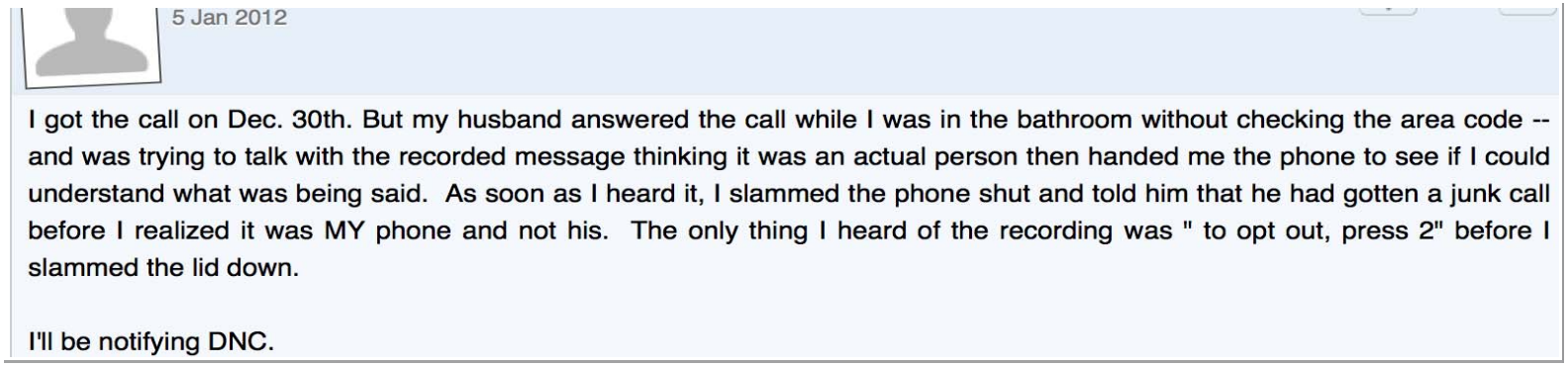
PROBLEMS WITH CURRENT DATA SOURCES

Delay in Reporting Fraudulent Calls



29 Mar 2012

I got a call from that number at 7 55pm on march 26. I called it back and it was a woman moaning as if she was having am 087 with vodaphone.



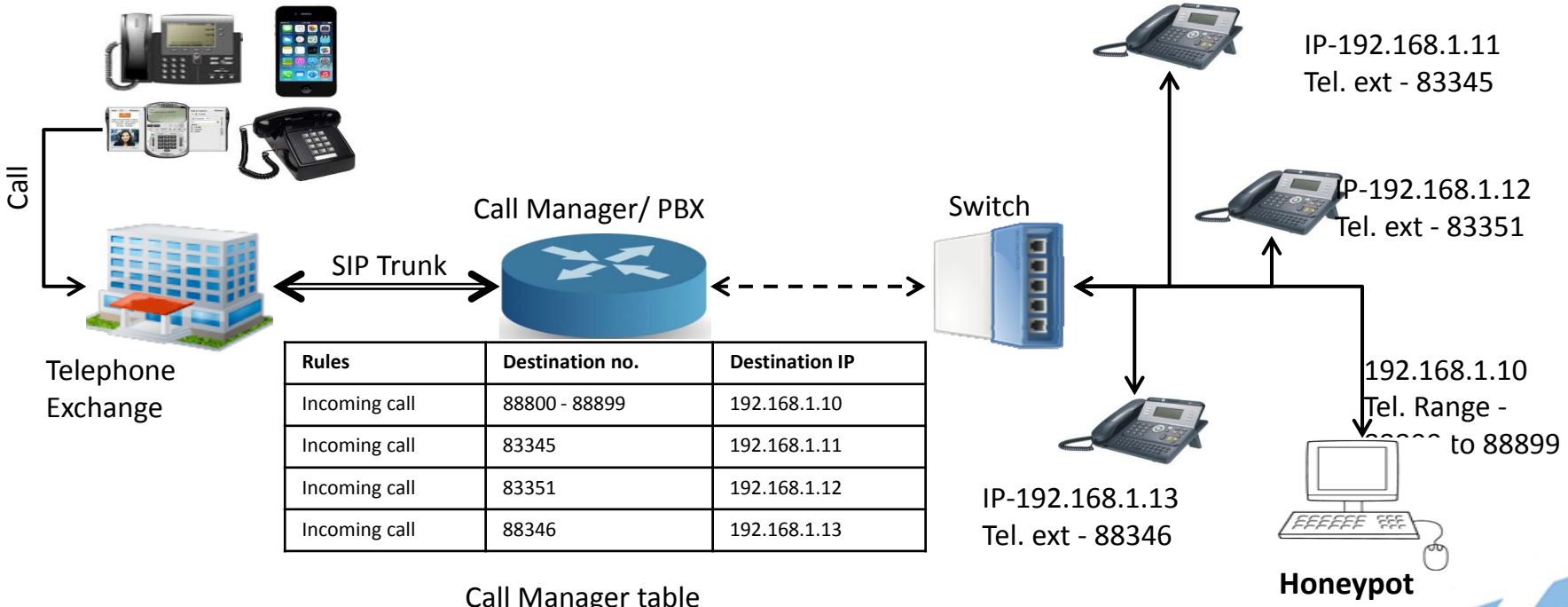
5 Jan 2012

I got the call on Dec. 30th. But my husband answered the call while I was in the bathroom without checking the area code -- and was trying to talk with the recorded message thinking it was an actual person then handed me the phone to see if I could understand what was being said. As soon as I heard it, I slammed the phone shut and told him that he had gotten a junk call before I realized it was MY phone and not his. The only thing I heard of the recording was " to opt out, press 2" before I slammed the lid down.

I'll be notifying DNC.

HOW TO SETUP ONE?

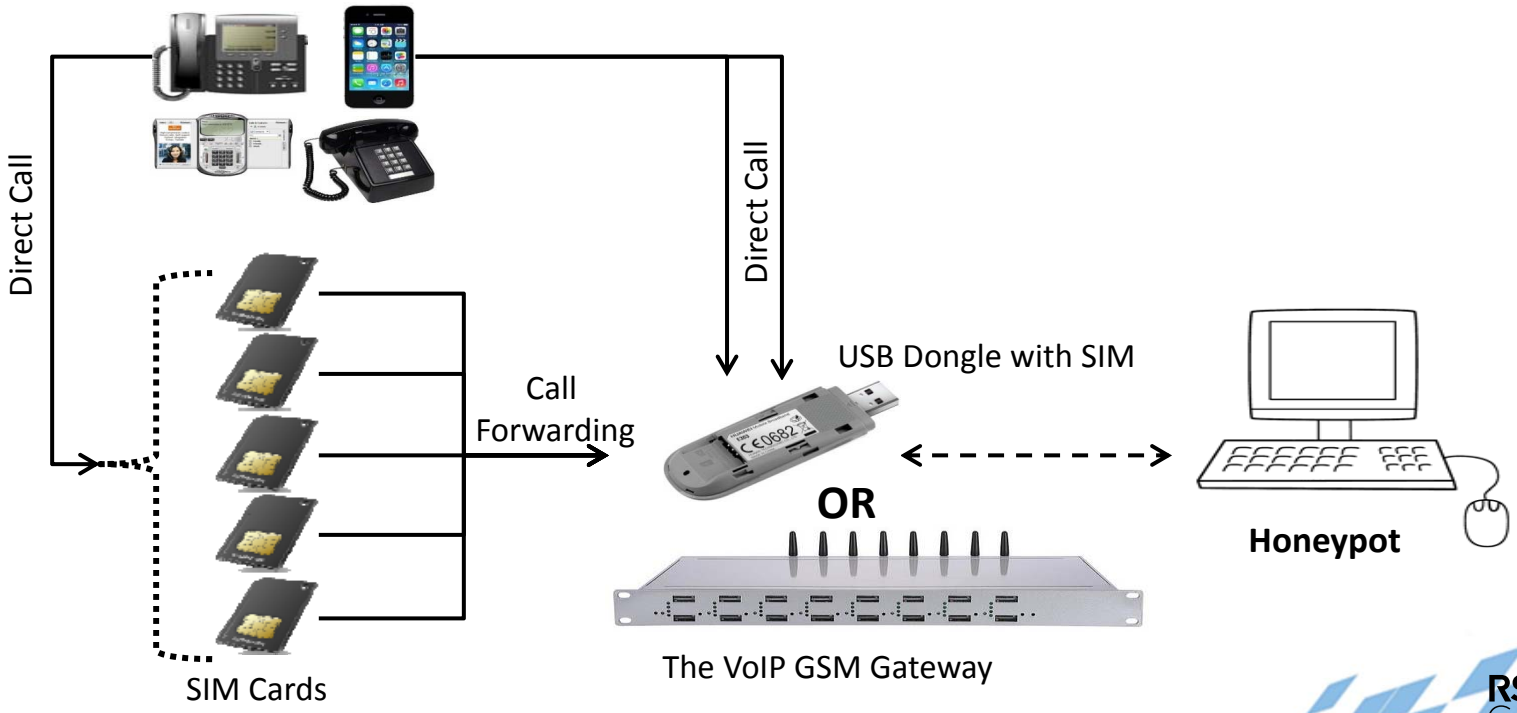
Using SIP Trunk



Rules	Destination no.	Destination IP
Incoming call	88800 - 88899	192.168.1.10
Incoming call	83345	192.168.1.11
Incoming call	83351	192.168.1.12
Incoming call	88346	192.168.1.13

Call Manager table

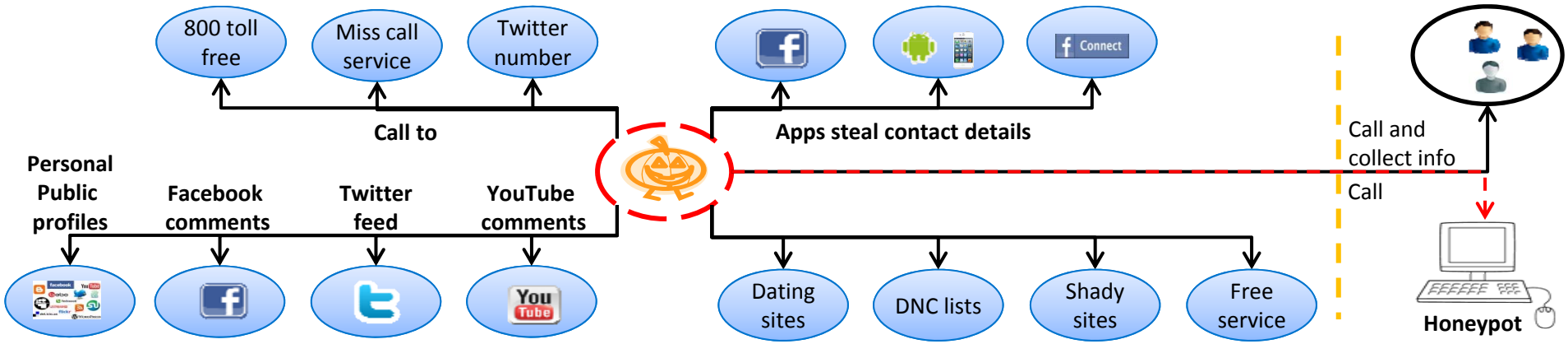
VOIP GSM Gateway



Phoneytokens

- Phoneytokens are digital piece of information (phone numbers + features in our case) whose value lies in the unauthorized use of these token.
- Features
  - Age
  - Profile
  - Sequential
  - Geography

Phoneytokens

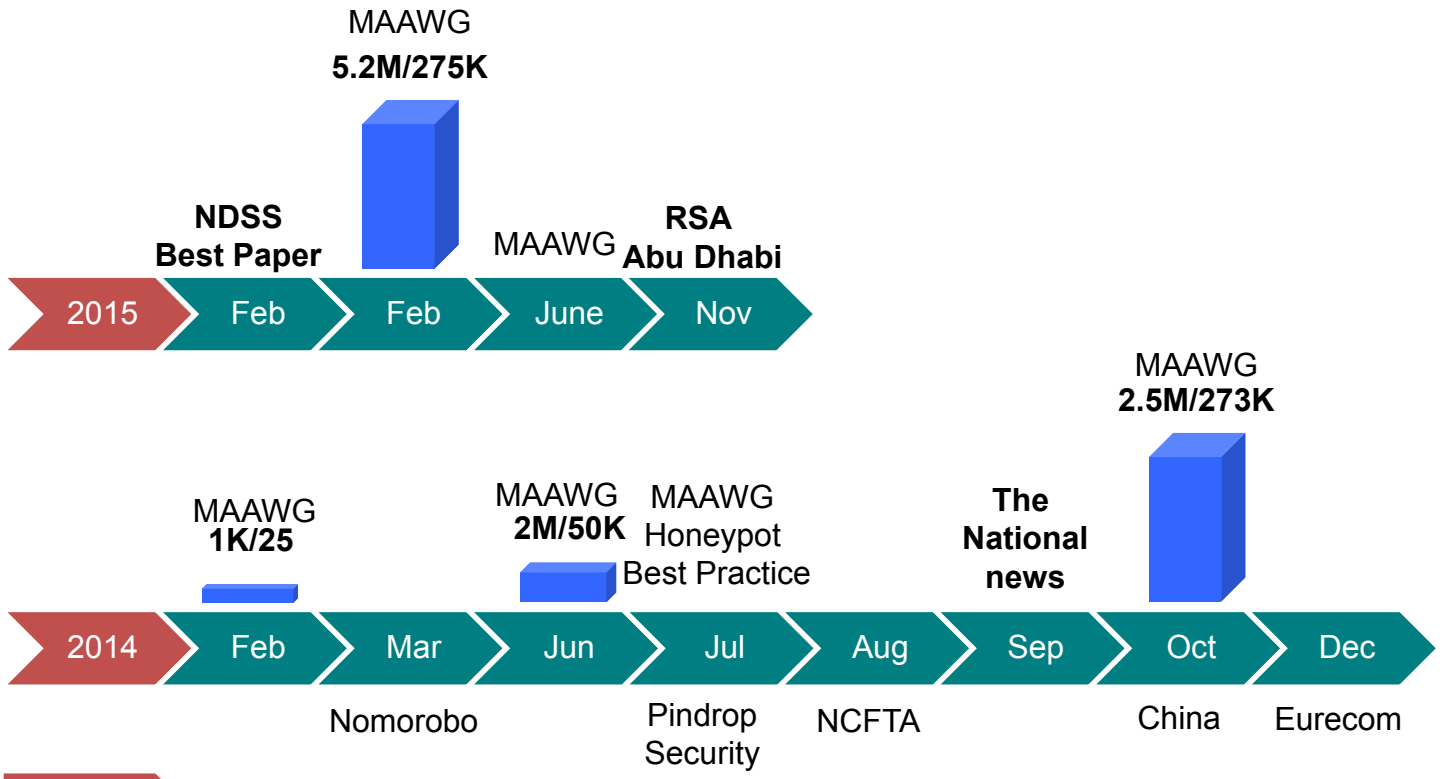


Challenges

- Anonymously pushing phoneytokens
- Ability to engage callers
- Automation
- Legal: Telephone conversation recording laws
- Dealing with false positives
- Cost
- Ethics

Progressing in Combating Phone Abuse

SUCCESS SO FAR



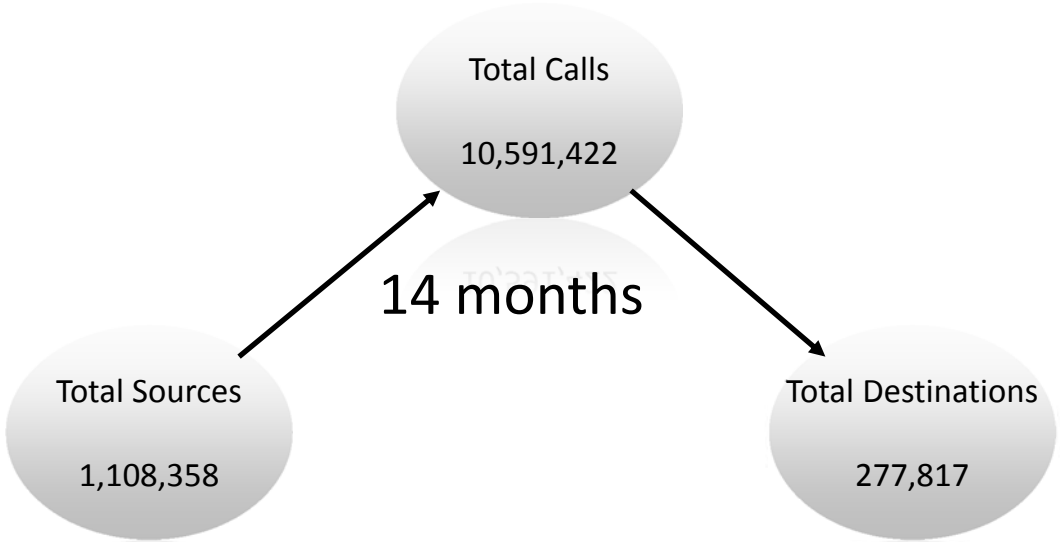
NYUAD, Gatech, Pindrop Security

ANALYSIS

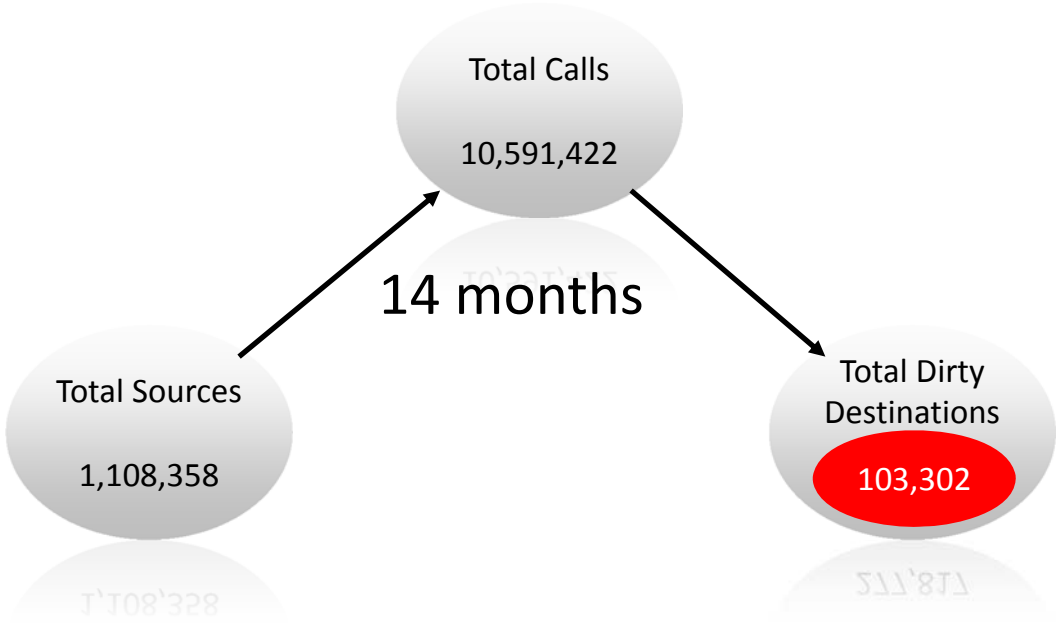
Case Study on Pindrop's Telephone Honeypot

- 10 million calls in first 14 months on 277K honeypot numbers
- What we have seen
  - Telephony Denial of Service
  - Automated Callers
  - Telemarketing
  - Debt Collector
  - Spoofing
  - CNAM Fraud
  - Geo-targeted Attacks

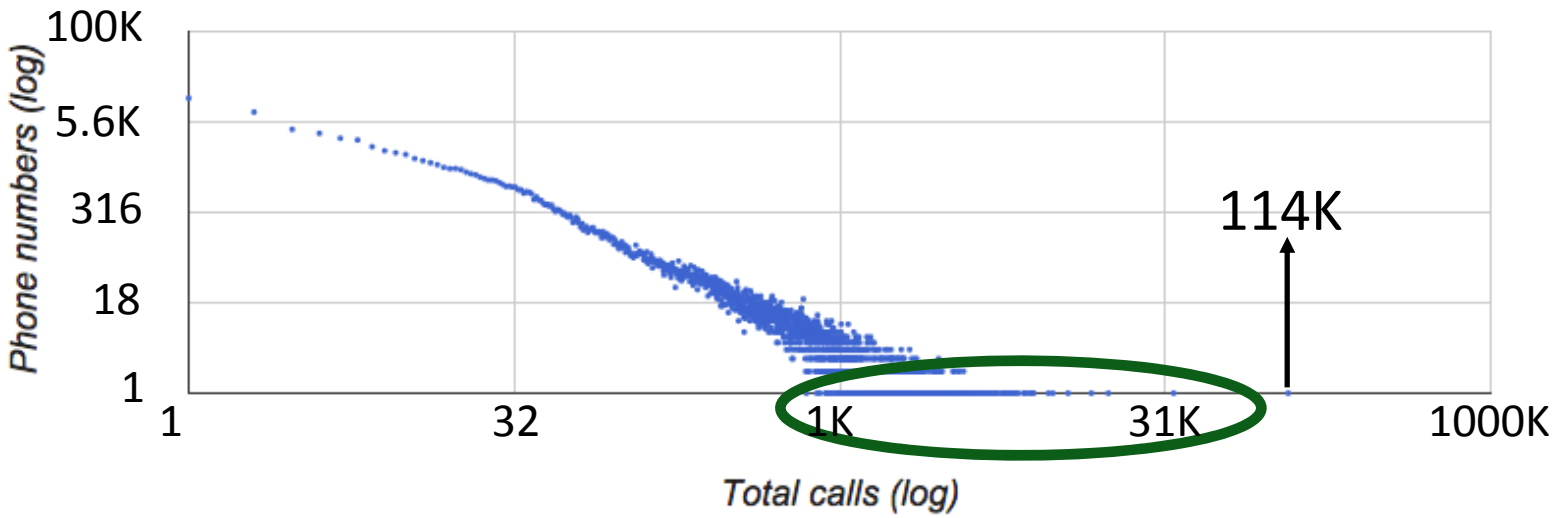
Initial Results



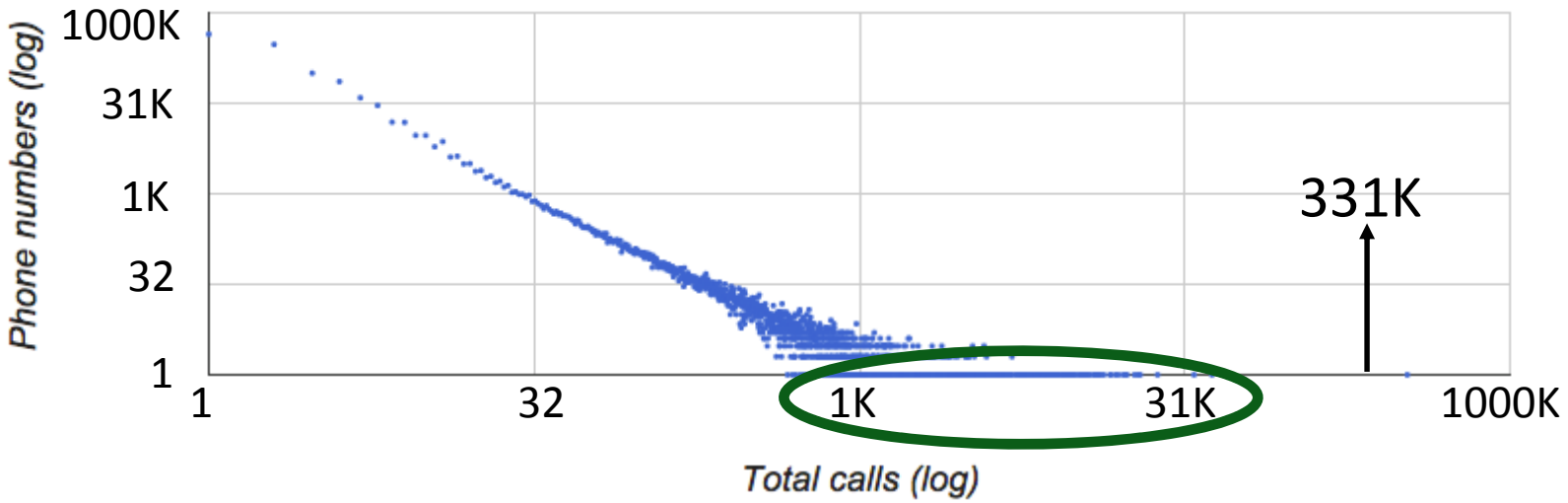
Initial Results



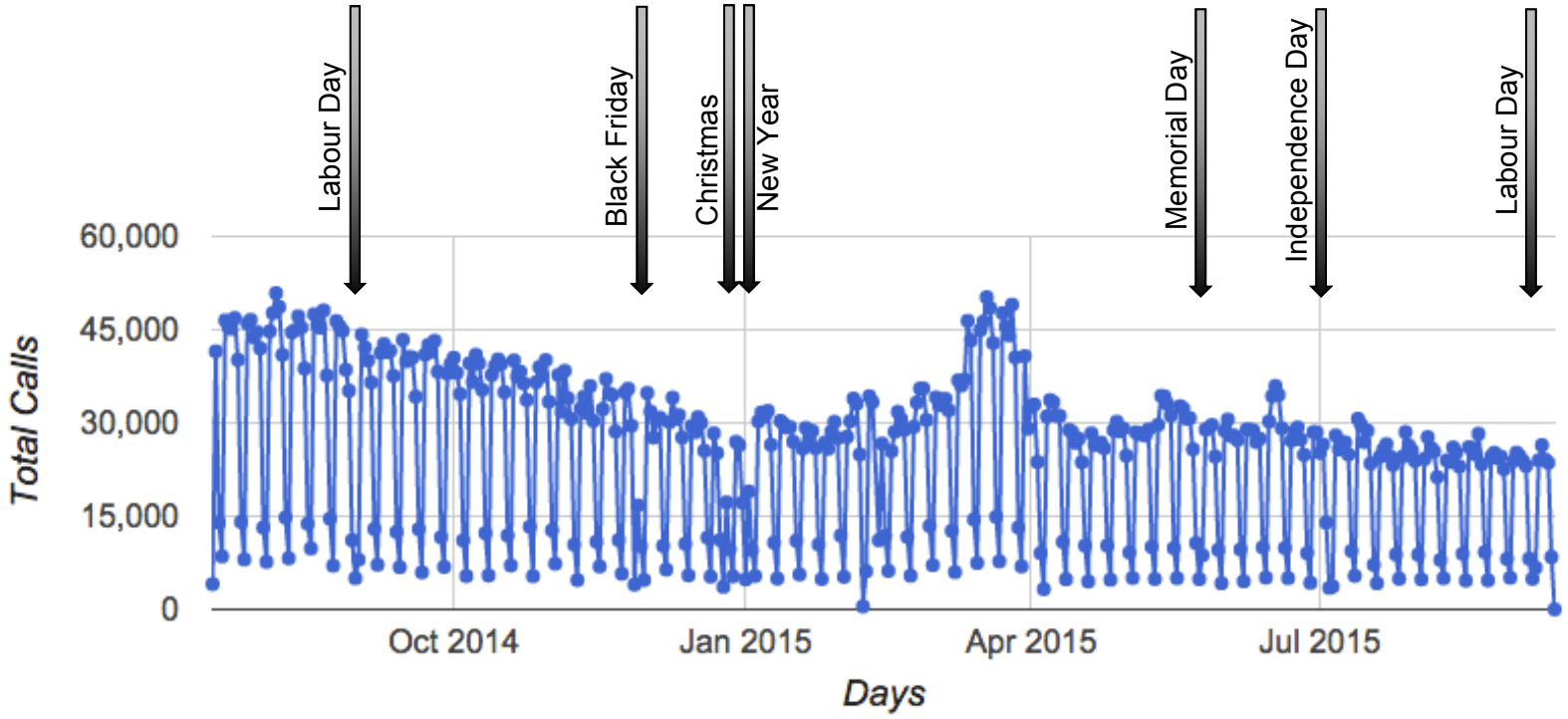
Destination Numbers Distribution



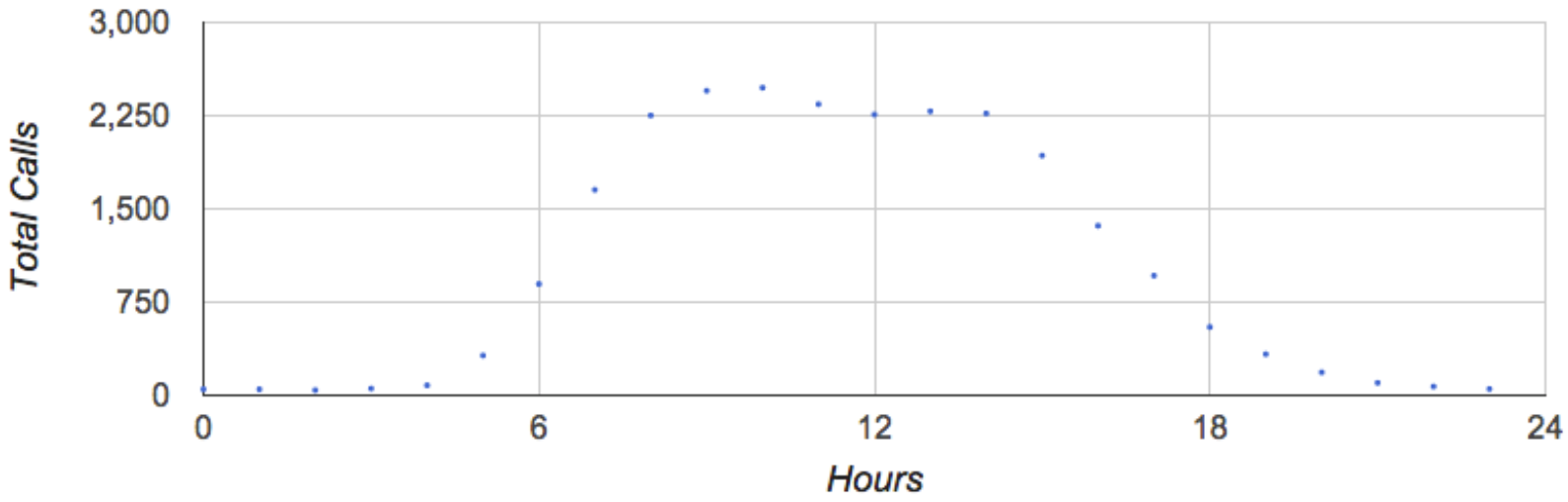
Source Numbers Distribution



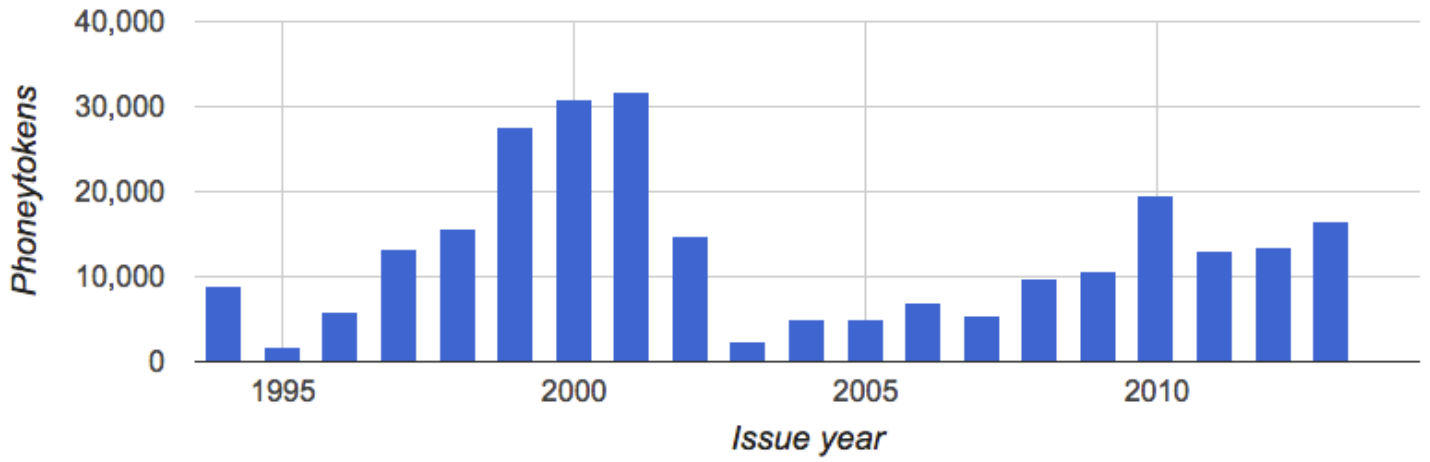
Daily Call Volume



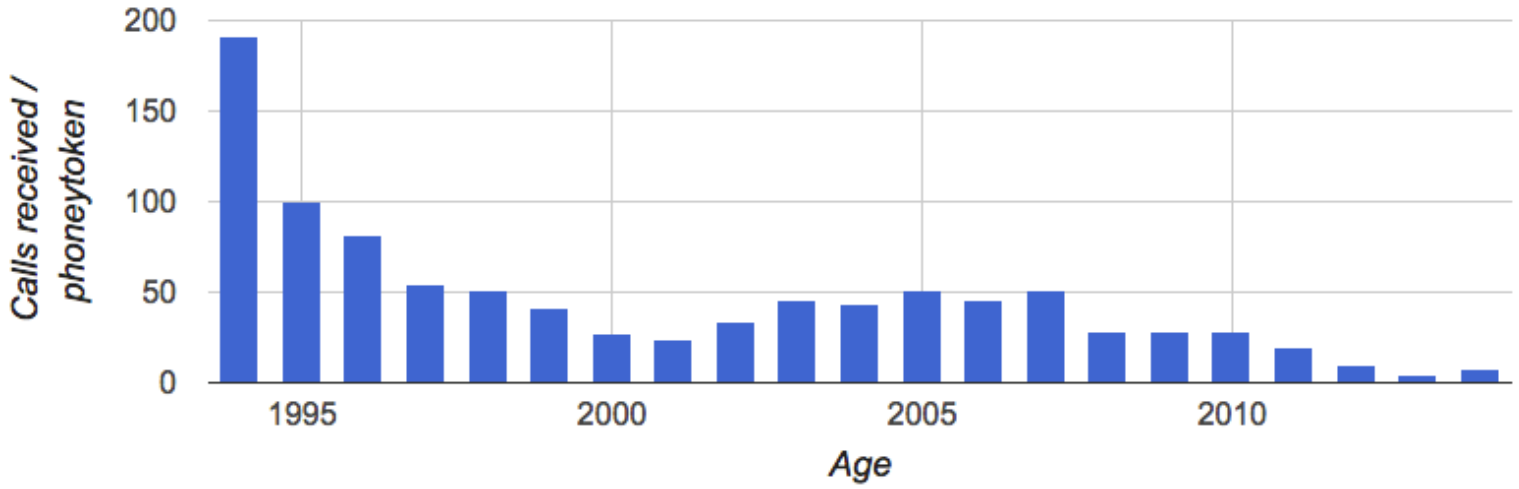
Hourly Call Volume



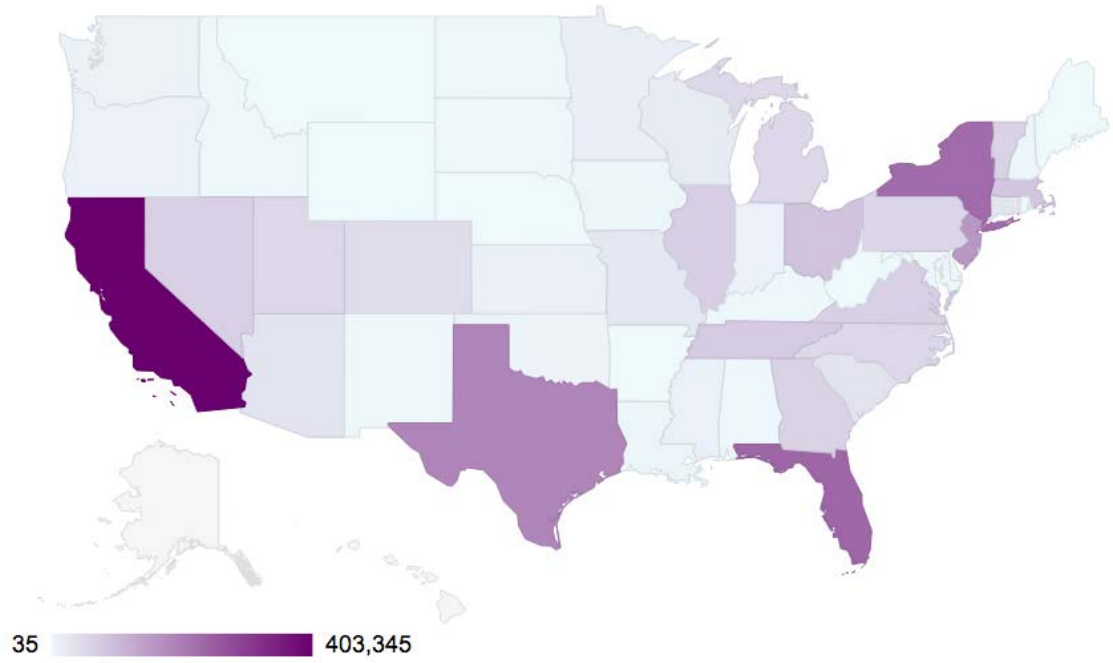
Age of destination numbers



Age based Distribution



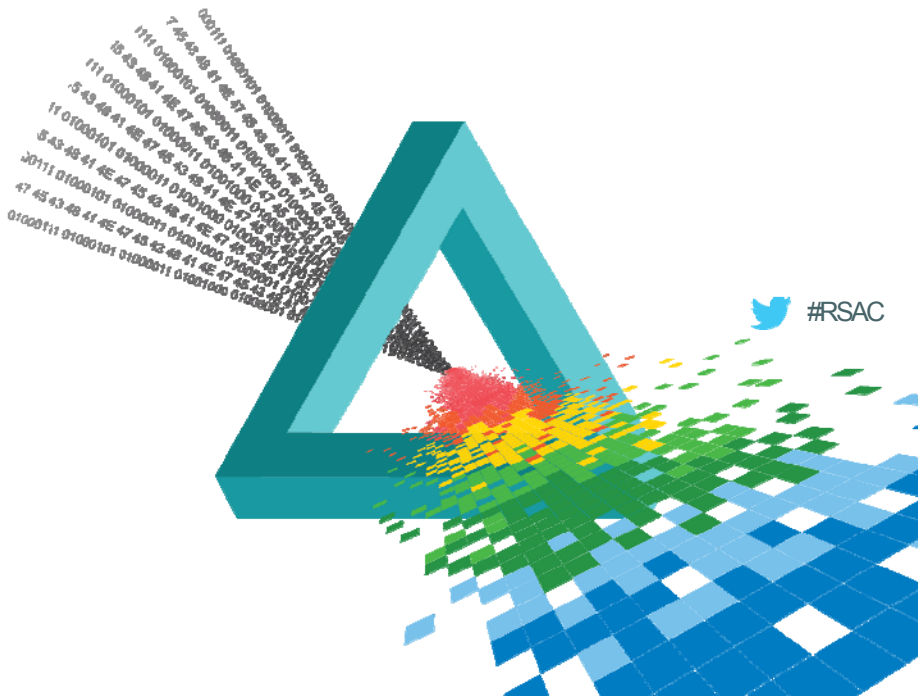
Geographical Call Distribution



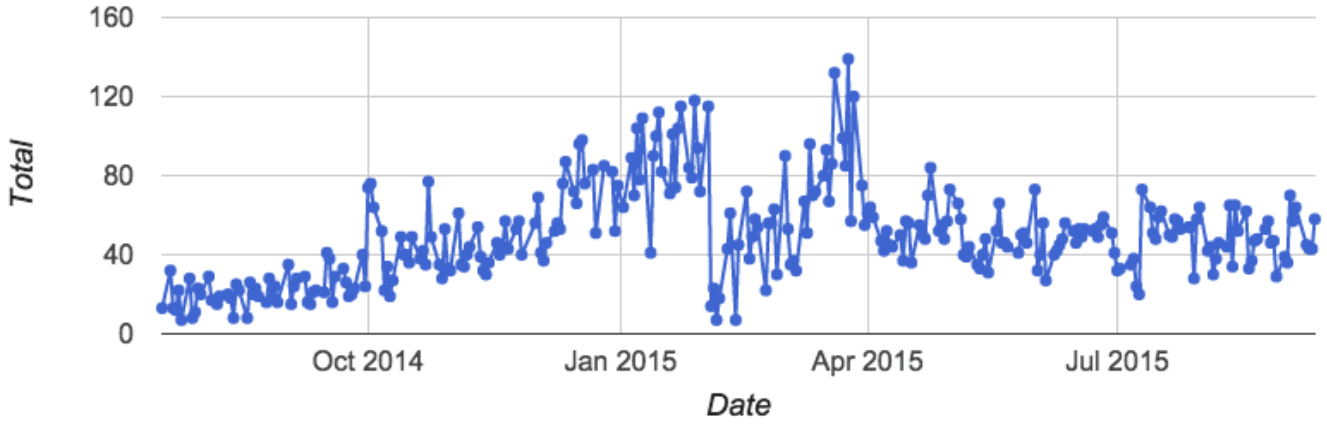
RSAConference2015

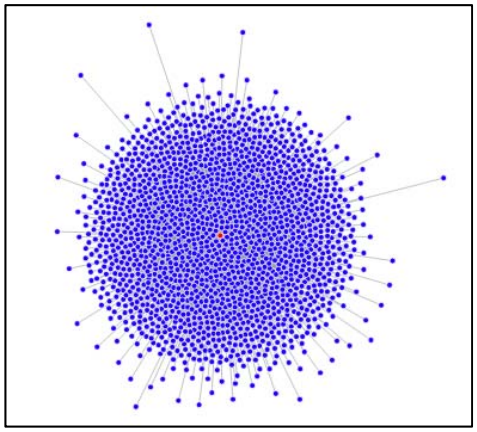
Abu Dhabi | 4–5 November | Emirates Palace

Attack Patterns

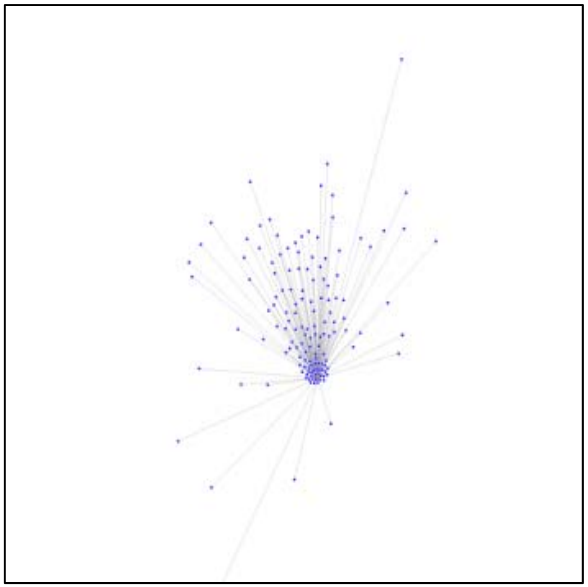


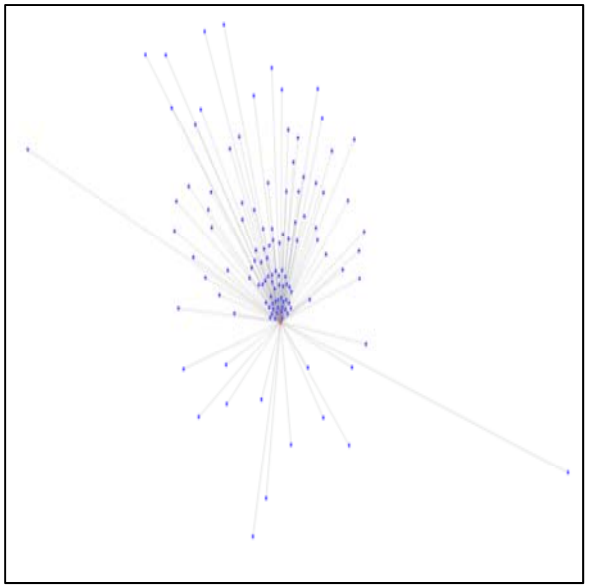
Telemarketer



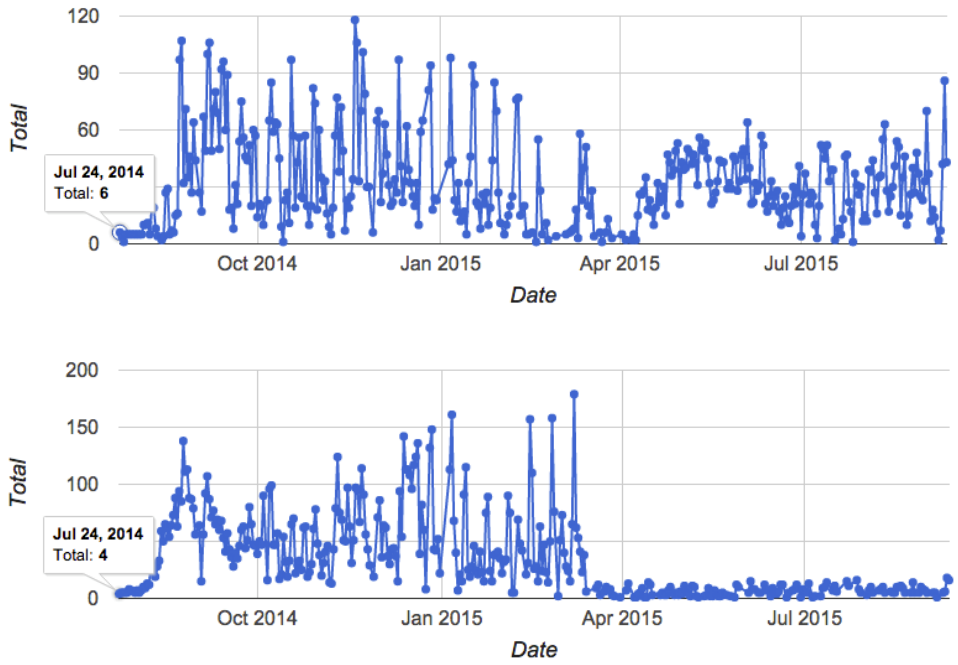


Penn Credit Debt Collector

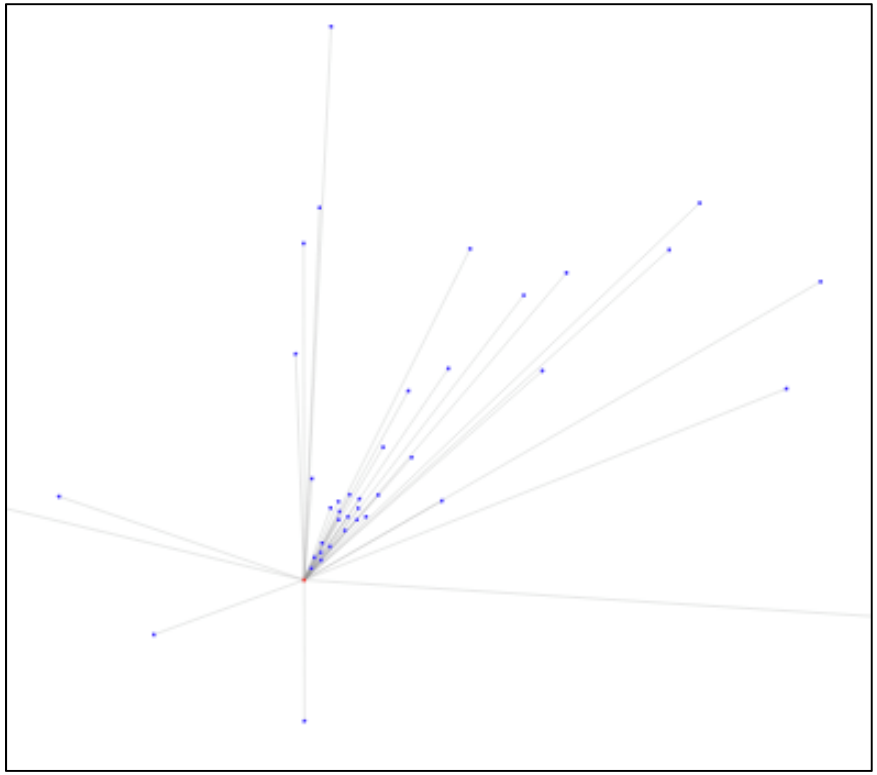




Penn Credit Debt Collector



Allied Interstate Debt Collector



Allied Interstate Debt Collector

FDCPA - Fair Debt Collection Practices

Florida Lawyer Fighting Debt Collection Abuse, Harassment, Calls, & Debt Collector Lies

CATEGORIES

Attorney General (2)
Bankruptcy (5)
Banks (7)
Collection Agencies (123)
Collection Calls (9)
Collection Lawsuits (13)
Collection Lawyer (4)
Collection Methods (4)

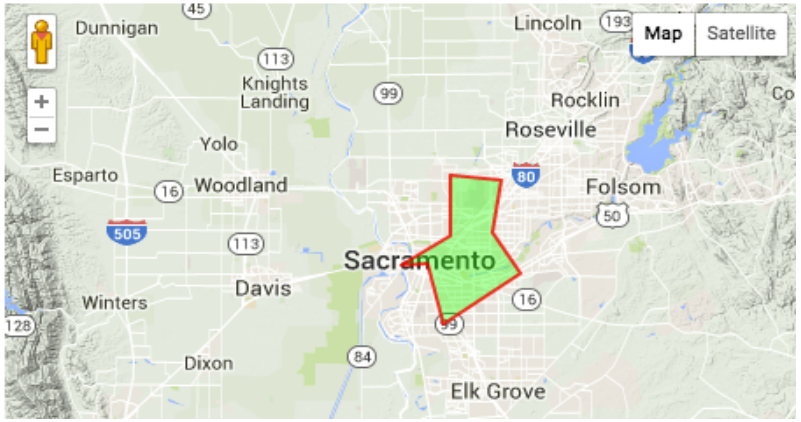
Allied Interstate Settles — Agrees to Pay $ 1.75 Million Fine

by DONALD PETERSEN on DECEMBER 11, 2010

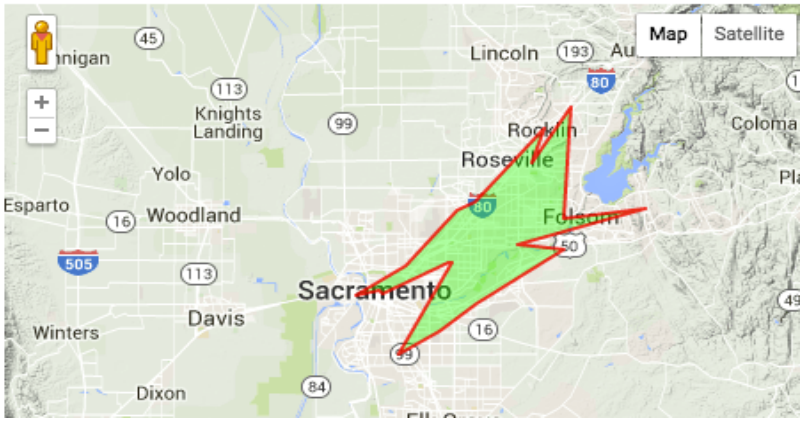
On October 22, 2010, Allied Interstate agreed to pay a fine totaling $ 1,750,000 to settle the FTC's allegations that Allied violated the FDCPA while attempting to collect accounts from consumers during 2006 through 2008. The $ 1,750,000 fine is the second largest that a debt collector has agreed to pay the FTC.

Geo-Targets

Source:12028005649, Date:2015-05-22



Source:15106757013, Date:2015-05-19



Geo-Targets

Source:13475410256, Date:2015-05-17

Source:13072782551, Date:2015-05-22

Summary

- Can be used to collect better intelligence about telephony attacks
- Accurate, complete and timely information can be obtained using telephone honeypots
- Noticeable calling patterns like telemarketer, debt collectors, spoofing etc. can be observed from the datasets.

Open Challenges and Questions

- How many numbers do we need for completeness?
- Understanding how numbers are chosen/qualified?
  - Sources
  - Destination
- Threat understanding should enable defense

APPLY

جامعة نيويورك ابوظبي
NYU | ABU DHABI

Going Forward

- Option 1
  - Get sufficient set of phone numbers
  - Set a phoneypot at your end
  - Help you to distribute phoneytokens
  - Share the data with us
  - Perform analysis and share the intelligence with you

- Option 2
  - Get some numbers
  - Forward the calls to those numbers to one of our phoneypots
  - Will share the raw data and intelligence with you