

Mobile Telephony Threats in Asia

Black Hat Asia 2017, Singapore

Dr. Marco Balduzzi

Dr. Payas Gupta

Lion Gu

Sr. Threat Researcher
Trend Micro

Data Scientist
Pindrop

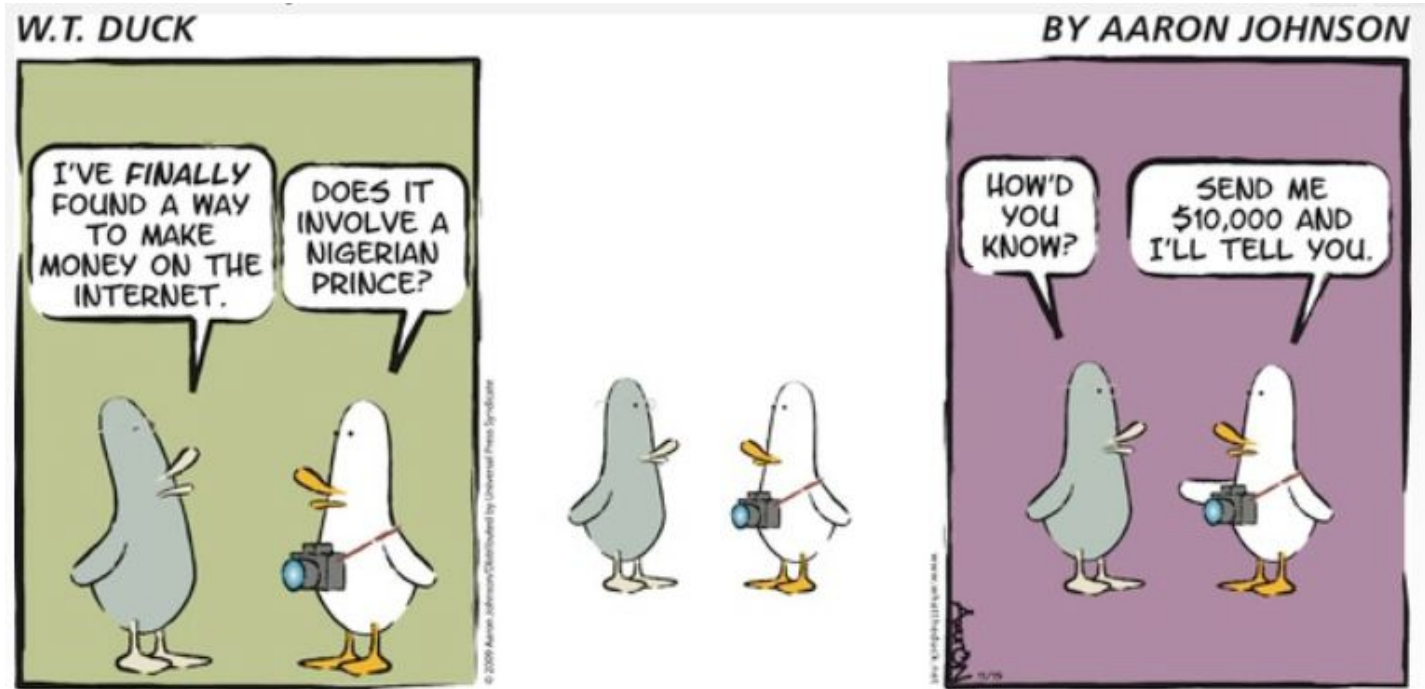
Sr. Threat Researcher
Trend Micro

Joint work with Prof. Debin Gao (SMU) and Prof. Mustaque Ahamad (GaTech)

Marco's 9th BH Anniversary :-)



Click to play recording [removed]



Wangiri Fraud, Japan

Wangiri Telephone Fraud – One Ring to Scam Them All

BY [DAVID HARLEY](#) POSTED 10 FEB 2014 - 04:53AM

OPINION

1

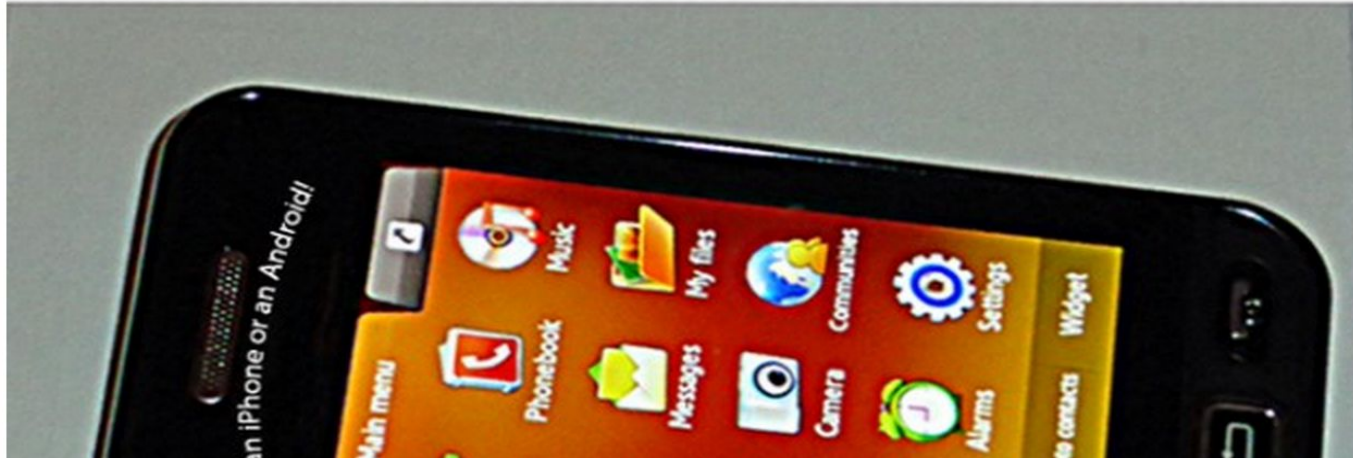
TAGS

BETTER BUSINESS BUREAU

FACECROOK

SNOPES

WANGIRI



Fake Officials Fraud, China

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

This is your Telco calling, UAE

Scammers 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

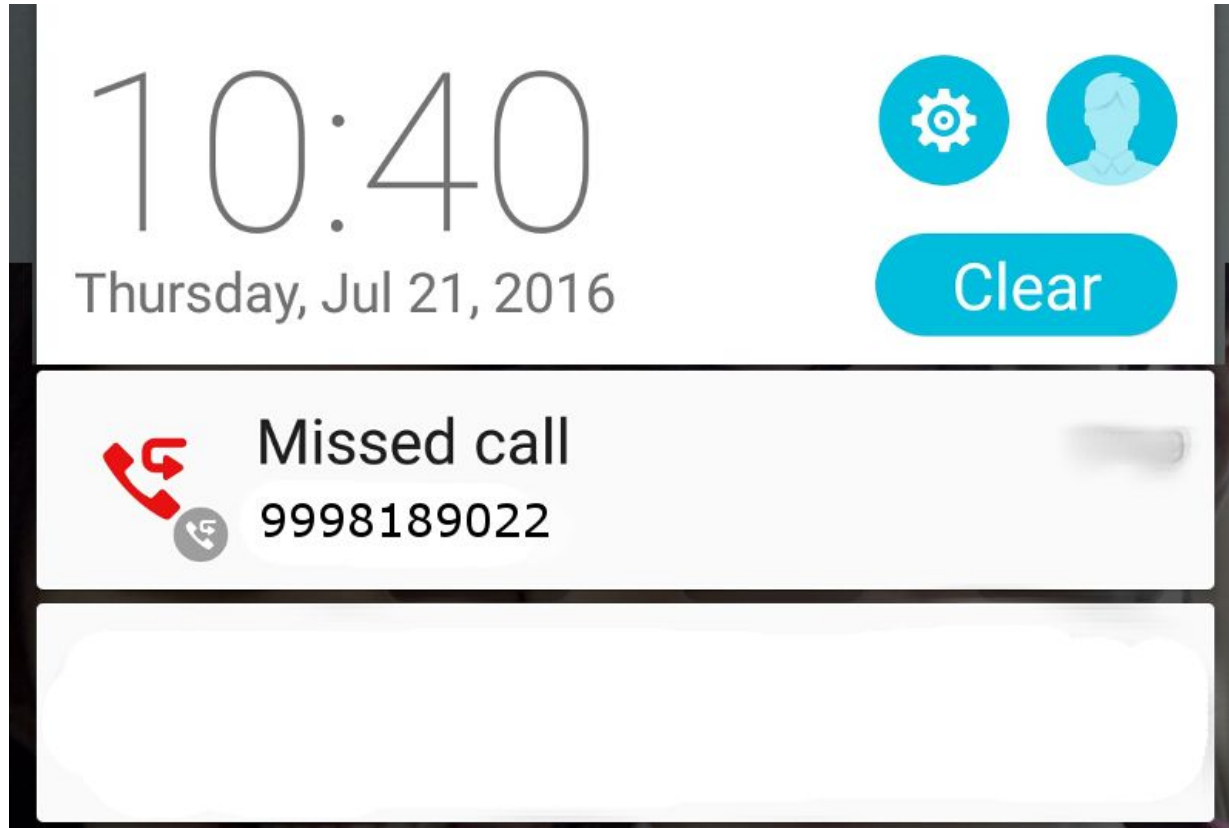
GULF NEWS 

Dubai: Even after over three years of scam warnings from etisalat, SIM card scammers 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".

Police Scam, Singapore



BringBackOurCash, Nigeria

PONZI SCHEME, PONZI SCHEME

Bringbackourcash Ponzi wants to scam scammed investors

Written by PageOne on February 19, 2017

More in Ponzi Scheme:



This is no joke. A Ponzi Scheme called Bringbackourcash has actually launched.

But never mind even if it is not a joke because it is a scam hoping to scam already scammed victims.

Why is Happening?

- Lack of users' awareness
- Users publicly disclose their mobile numbers
- Expose themselves and the organization they work for!

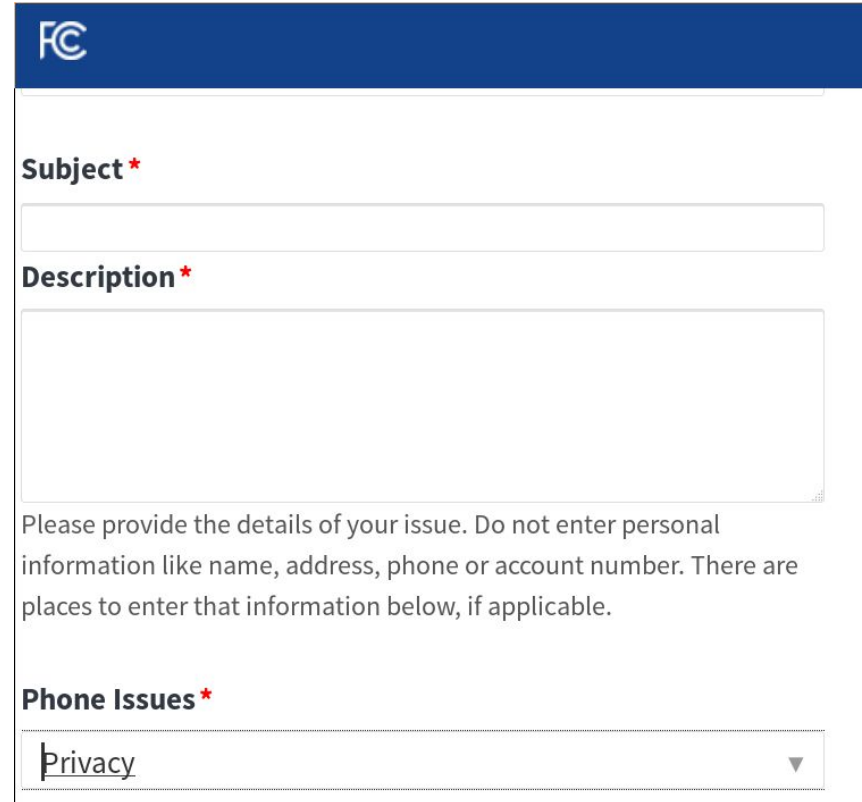
Salespeople, 10 Ways to Find Your Prospect's Phone Number

October 4, 2016 by Adam Honig 2



Current Defeat Strategies

- Telcos
- Crowd sourced
 - FTC, fraud complaints
 - 800notes open datasets
- Proprietary



The screenshot shows a complaint form from the FCC. At the top is a blue header with the FCC logo. Below the header, there are three main sections: 'Subject', 'Description', and 'Phone Issues'. Each section has a red asterisk indicating it is required. The 'Subject' field is a single-line text input. The 'Description' field is a large multi-line text area. Below the 'Description' field is a paragraph of text: 'Please provide the details of your issue. Do not enter personal information like name, address, phone or account number. There are places to enter that information below, if applicable.' The 'Phone Issues' field is a dropdown menu with 'Privacy' selected.

Subject *

Description *

Please provide the details of your issue. Do not enter personal information like name, address, phone or account number. There are places to enter that information below, if applicable.

Phone Issues *

Privacy ▼

Missing Caller's Details


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

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 *

No Actual Timestamps



10 Dec 2013

They have called me 8 times in 2 hours... this is harrassment! it needs to stop now.

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

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

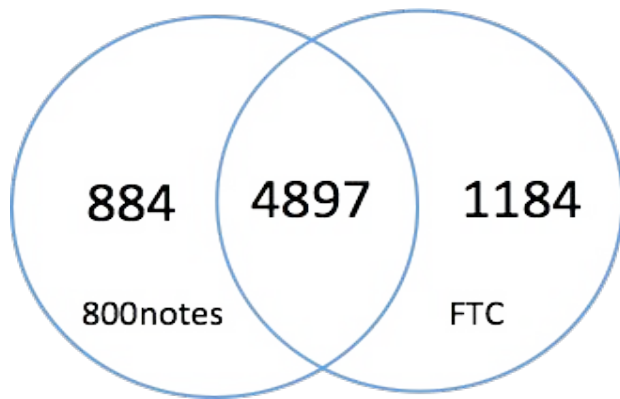
Call Type: Telemarketer

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

Not all Fraudulent Calls are Reported

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



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.

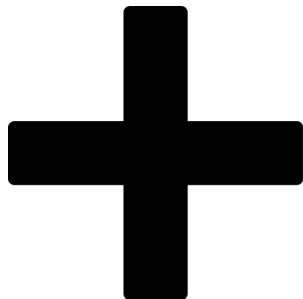


5 Jan 2012

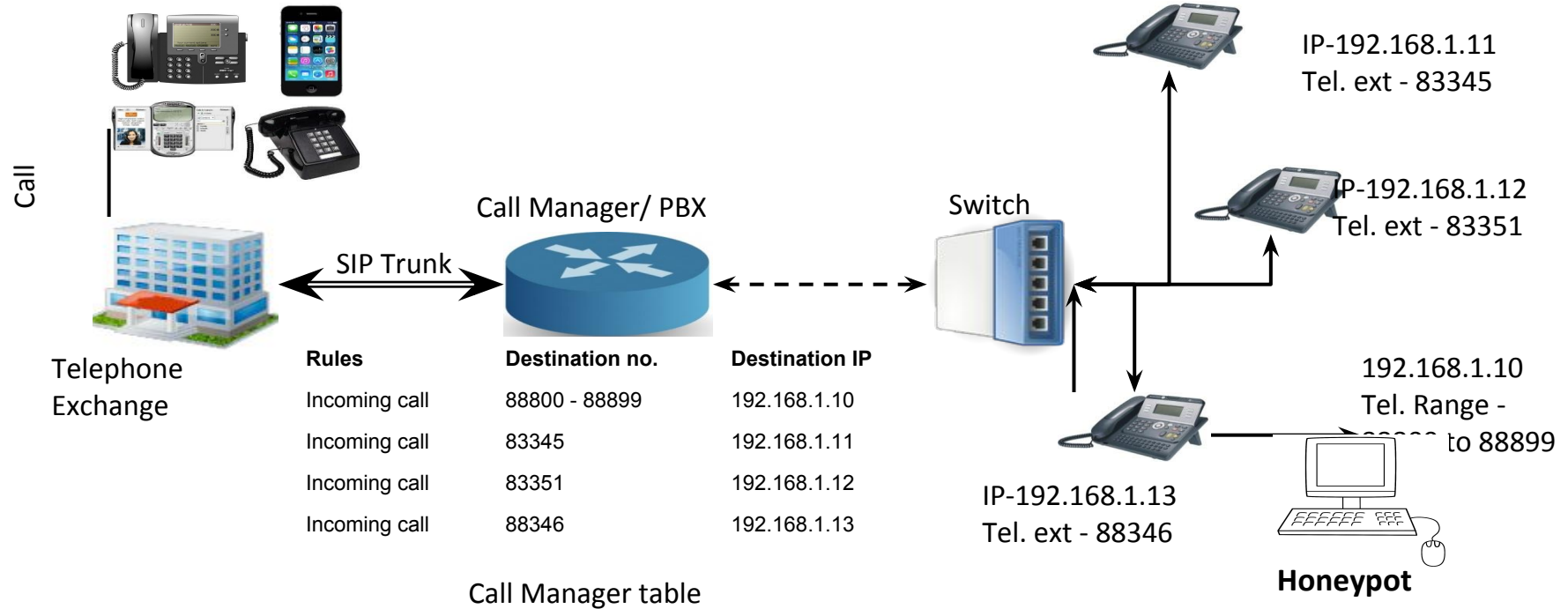
I got the call on **Dec. 30th.** But my husband answered the call while I was in the bathroom without checking the area code -- and was trying to talk with the recorded message thinking it was an actual person then handed me the phone to see if I could understand what was being said. As soon as I heard 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.

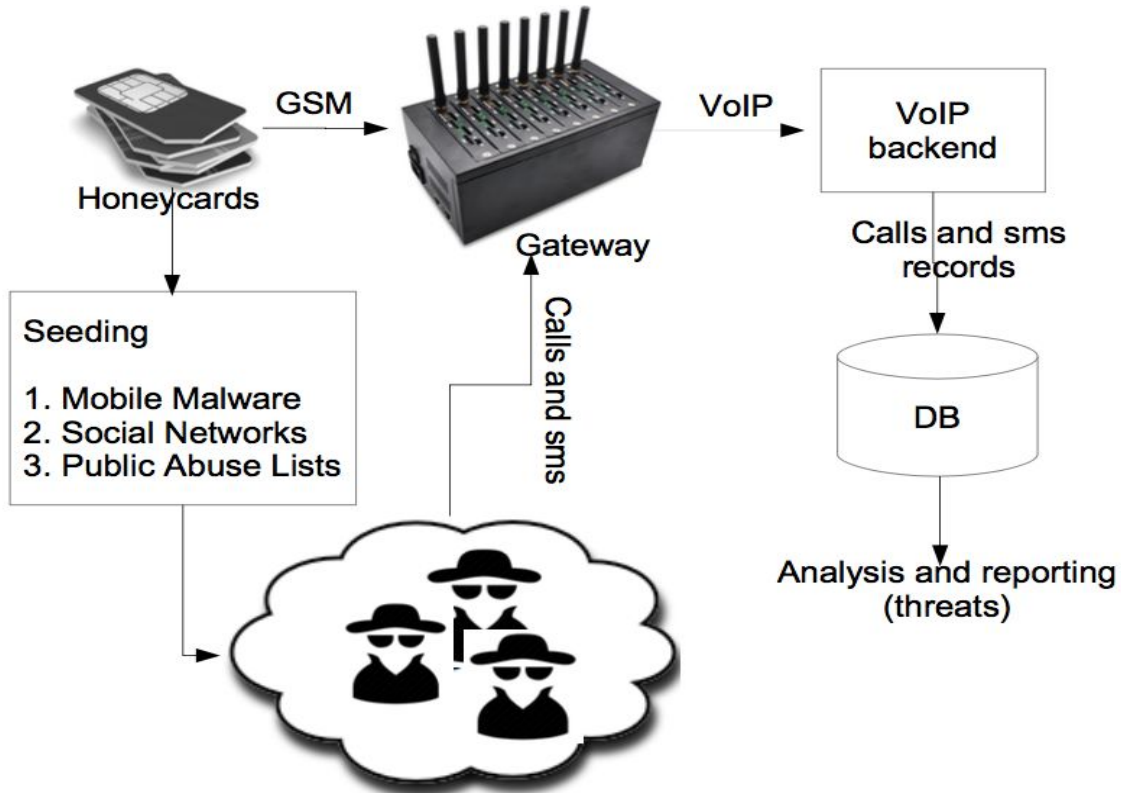
Any Solution?
















Using SIP Trunks



Using GSM/VoIP Gateways



Mobile Telephony Honeypot

Call Date	Recording	System	CallerID
2014-10-09 06:00:05		1412805605.22	"15621192273 "<goip1_user>
2014-10-08 03:16:04		1412709364.21	"13932125820 "<13932125820>
2014-10-07 23:05:03		1412694303.20	"15361099194 "<15361099194>
2014-10-06 12:41:34		1412570494.19	"15921962935 "<goip1_user>
2014-10-04 18:58:07		1412420287.18	"10086 "<10086>
2014-10-04 08:52:02		1412383922.17	"02759375431 "<02759375431>
2014-10-04 07:48:55		1412380135.16	"15678278590 "<15678278590>
2014-10-02 21:38:38		1412257118.15	"13146397703 "<13146397703>
2014-09-30 09:21:44		1412040104.14	"13552070625 "<13552070625>
2014-09-29 18:34:07		1411986847.13	"13262374867 "<13262374867>
2014-09-29 17:03:08		1411981388.12	"15259205763 "<15259205763>
2014-09-29 09:38:08		1411954688.11	"13552188861 "<13552188861>
2014-09-28 19:40:27		1411904427.10	"13261803466 "<13261803466>

Mobile Telephony Honeypot

D	App	Destination	Disposition	Duration
	Playback	15621192273	ANSWERED	00:01
	Playback	18757194227	ANSWERED	00:02
	Playback	13860141274	ANSWERED	00:03
	Playback	15921962935	ANSWERED	00:47
	Playback	18757194227	ANSWERED	00:40
	Hangup	hangup	ANSWERED	00:49
	Wait	15602228631	ANSWERED	00:01
	Playback	13477033614	ANSWERED	00:02
	Playback	18701408339	ANSWERED	00:06
	Playback	13477033614	ANSWERED	00:02
	Playback	13860141274	ANSWERED	00:32

Example of Call Recording

Example of SMS Recording

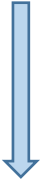
- 确认了哈, 位置还留起的 之前在等qq消息, 我刚才电话问了, 给我转款吧。建 行四川分行第五支行5240 9438 1020 0709, 户名:王玲。

(I have confirmed. Reservation is still valid. I am waiting QQ message, and I contact you by phone call. Please transfer money to me. *China Construction Bank Sichuan Provincial Branch Fifth Sub-branch, account number: 5240 9438 1020 0709, account name: Wang Ling*)



How to make honeypot
numbers “appealing” to
fraudsters?

Seeding



Social network



Mobile malware



Abuse list

Simulating Social-Network Leaks

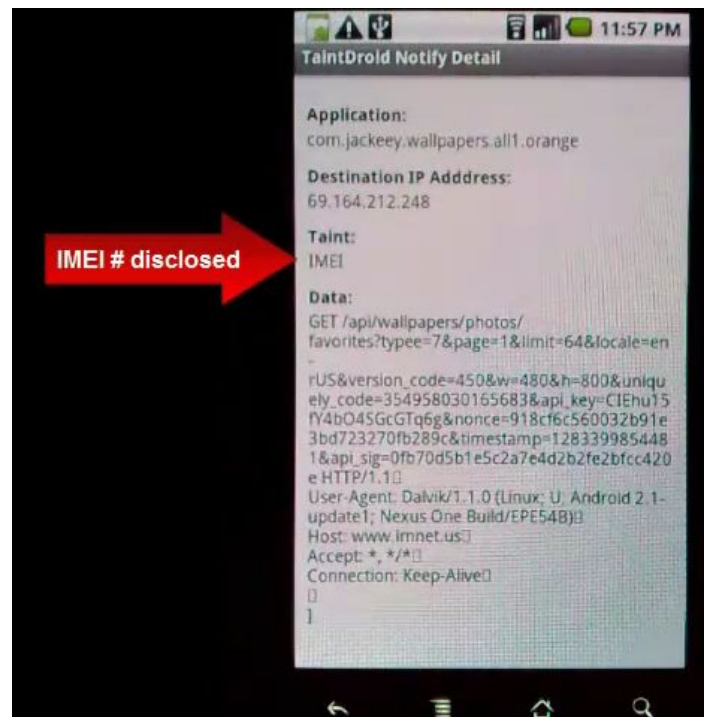


Mandela, the first anniversary of the death of # # my cell phone is lost, replaced with a new phone number: 18757194227

Fig. 2: Social networking seeding via Weibo

Mobile Malware Leak

- Honeypot numbers in contact list
- ~400 samples of 60 families
- Track 140 C&C leakages
 - Taint Droid
 - Network traffic



Active Engagement with Fraudsters

- 2000+ reported (*abuse*) numbers
- Engaged with SMS and one-ring call
 - *I am fine with our discussion. How do we want to proceed?*

举报垃圾电话 - 轻松举报从此开始! 垃圾号码提交

请输入电话或手机 查询电话 我要举报

知: 13812345678, 010-87654321

首页 所有号码 诈骗资讯 号码吉凶 提交号码 邮编查询 归属地查询 星座命理 联系我们

安全提示: 因为存在用电话诈骗、短信陷阱、引诱回拨国际长途、引诱回拨收费声讯台等陷阱, 遇到陌生来电请谨慎接听、小心回电, 如果您使用的是接听免费的电话/手机则可以放心接听并问明对方电话来源, 如果需要回电, 在不知道对方底细的情况下, 最好使用公用电话。不要轻信中奖、冒充熟人、冒充银行等骗术, 未完全查明身份前, 千万不要给陌生人汇款、转账, 不要透露银行帐号、密码

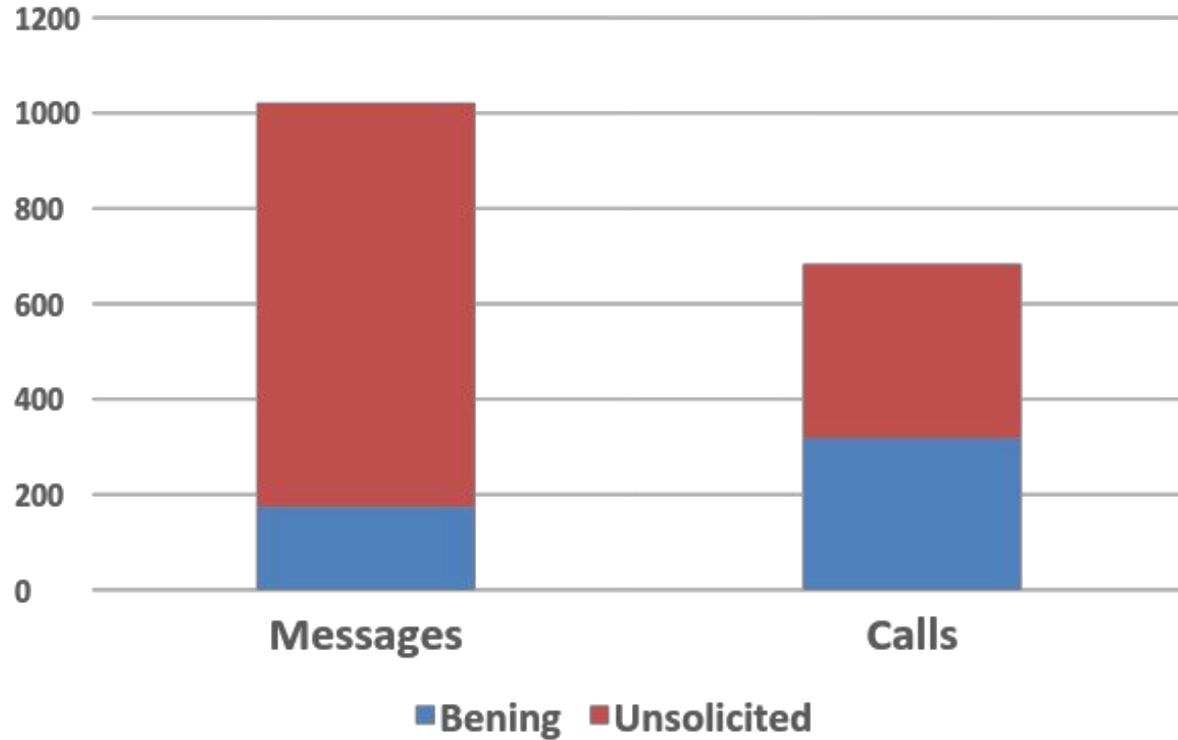
全部: 香港(00852) 北京(010) 广州(020) 深圳(0755) 上海(021) 天津(022) 重庆(023) 南京(025) 成都(028)

类型: 骗电话 骚扰电话 垃圾短信 诈骗信息 中介 问卷/市场调查 来电无声, 回拨不通 提高警觉 (不良销售手法)

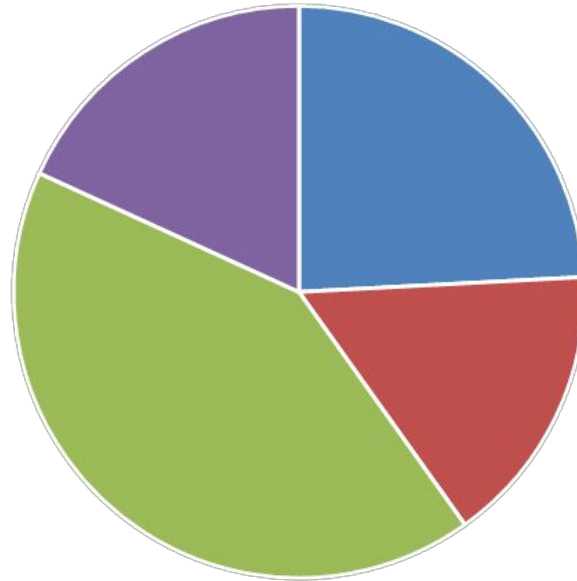
热门号码: 010 0755 020 número+oculto 0755- 110 -2 62 1391 1359 1392 1341 1340 81132300-020 1342 بلیب

最新举报电话	一周热门号码
076028174580 [广东 中山] 举报来源: 安徽省合肥市 移动	-1 (骗电话) 29条评论 2016-05-09 11:16:22
2016-05-16 10:45:45 (垃圾短信) 已有评论: 0条 120.210.191.** 【安徽省合肥市 移动】	-2 (骗电话) 17条评论 2016-05-09 15:11:48
076938941603 [广东 东莞] 举报来源: 安徽省合肥市 移动	13196316719 (骗电话) 13条评论 2016-05-09 11:52:44
2016-05-16 10:45:28 (垃圾短信) 已有评论: 0条 120.210.191.** 【安徽省合肥市 移动】	13103738120 (骗电话) 10条评论 2016-05-13 12:57:04
076028142037 [广东 中山] 举报来源: 安徽省合肥市 移动	+85266716495 9条评论 (骗电话)
2016-05-16 10:45:16 (垃圾短信) 已有评论: 0条 120.210.191.** 【安徽省合肥市 移动】	

General Results



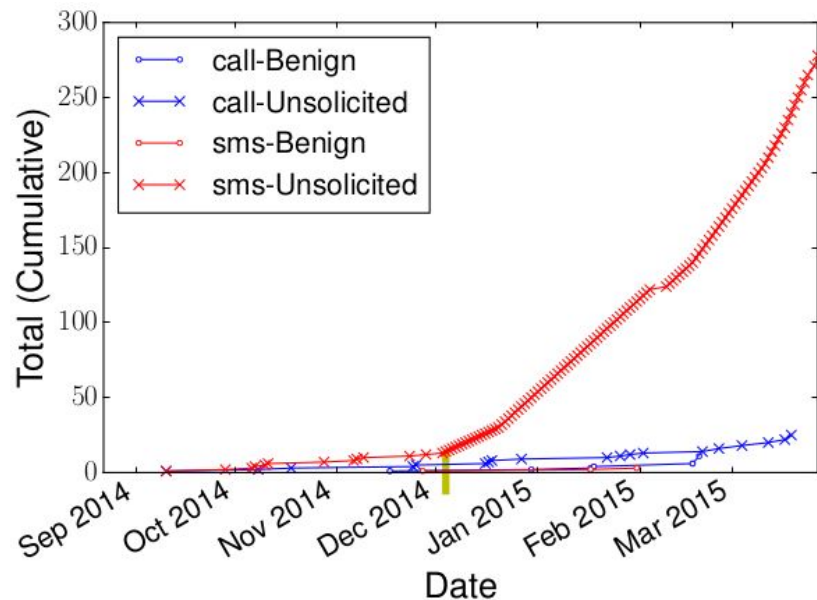
Effect of Seeding



- Social Networks
- Mobile Malware
- Active Engagement
- Not Seeded

Social Networks

- Very effective
- Picked up by Xinhua
Quanmei [*]
- Daily news in the form
of spam -> 221
messages

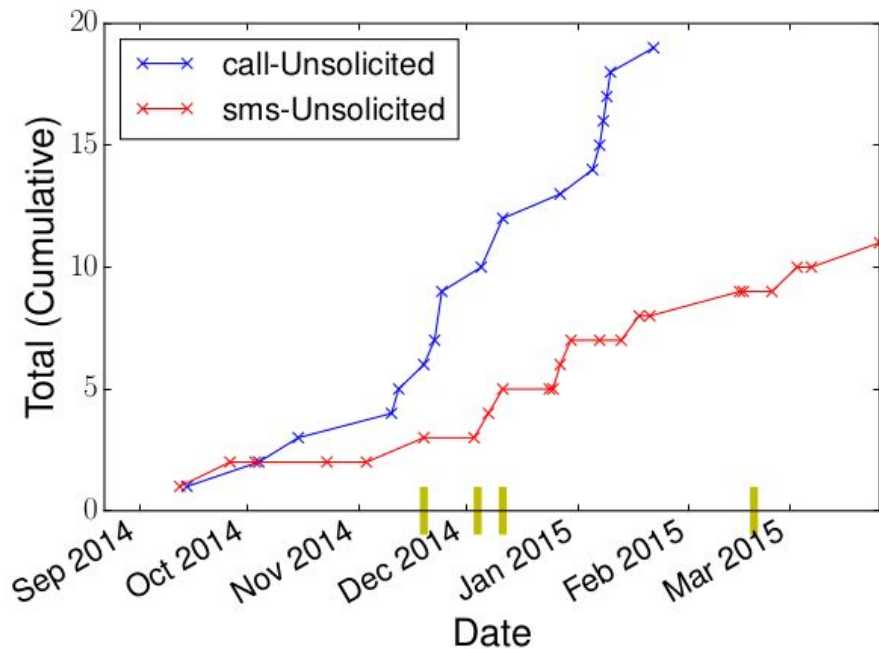


(a) Volume - soc1

[*] <http://www.xhqm.cn/>

Malicious Apps

- 79 ADs from 106588302
- Self-promoting app [*]
 - 0690123590110 (mal1)
 - 1065502004955590110 (mal2) are spoofed

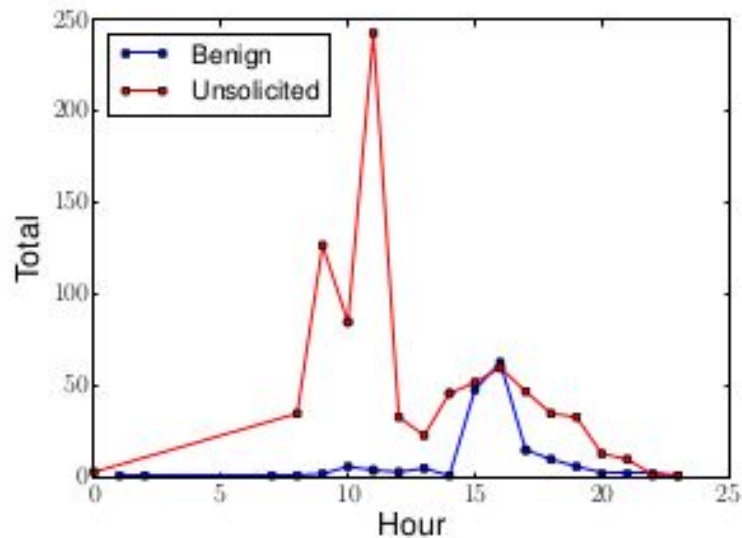


(k) Sources - mal2

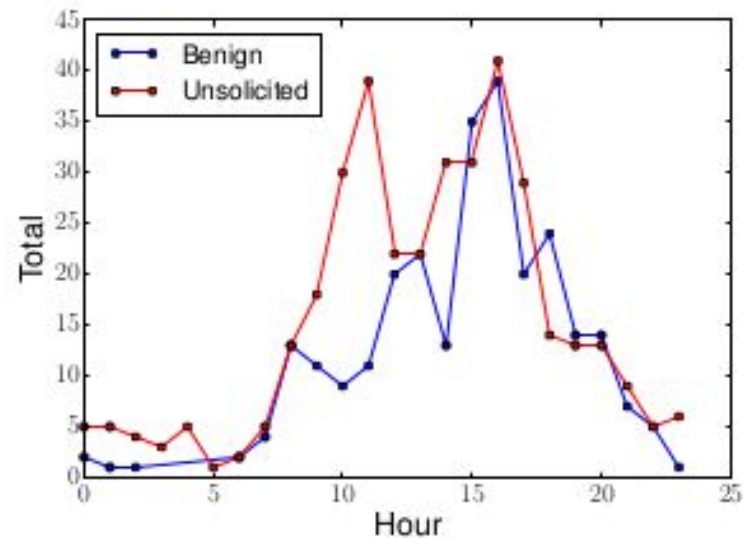
[*] <http://wap.guanxi.me>

Fraudsters' Strategies

Blended Malicious Traffic



(c) Hourly Volume (SMS)



(d) Hourly Volume (Call)

Concealed Caller Numbers

- 51% fraudsters: Use of SMS gateways and VoIP services to hide identity
- Use of foreign sim-cards (mainly Thailand)
- Use of split-paid services to reduce cost on international calls

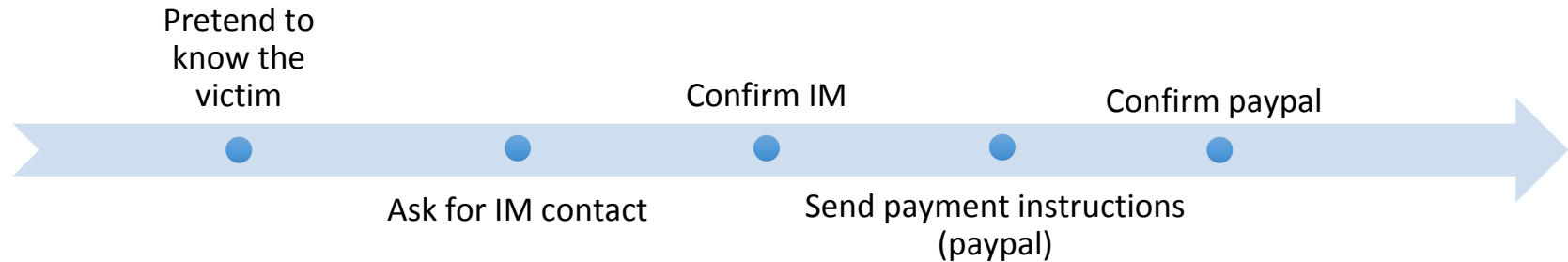
Social Engineering

- Human = weakest point in chain
- Multi-hop attack, similar to BEC
- Lateral movements

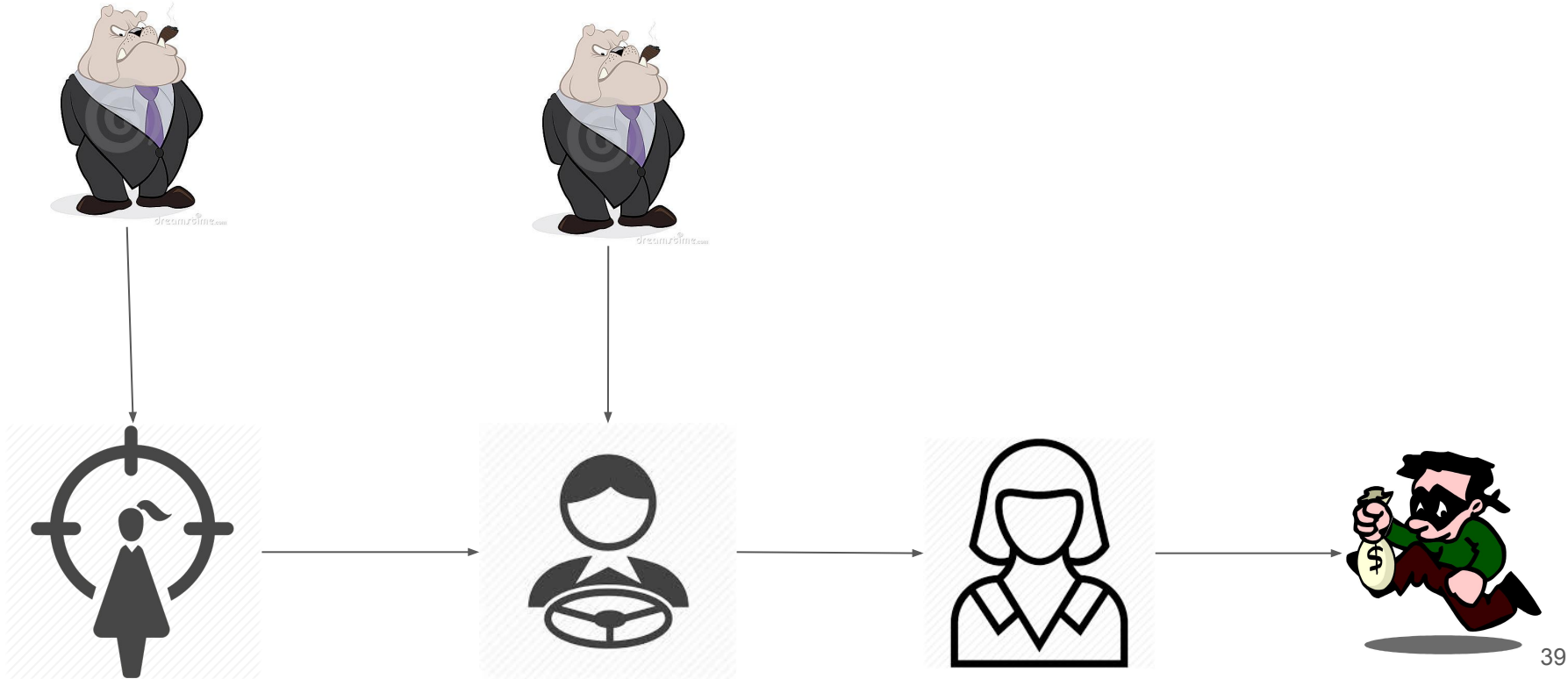


Multi-step Attack

- Repeated over time
- Combination of Calls and SMS

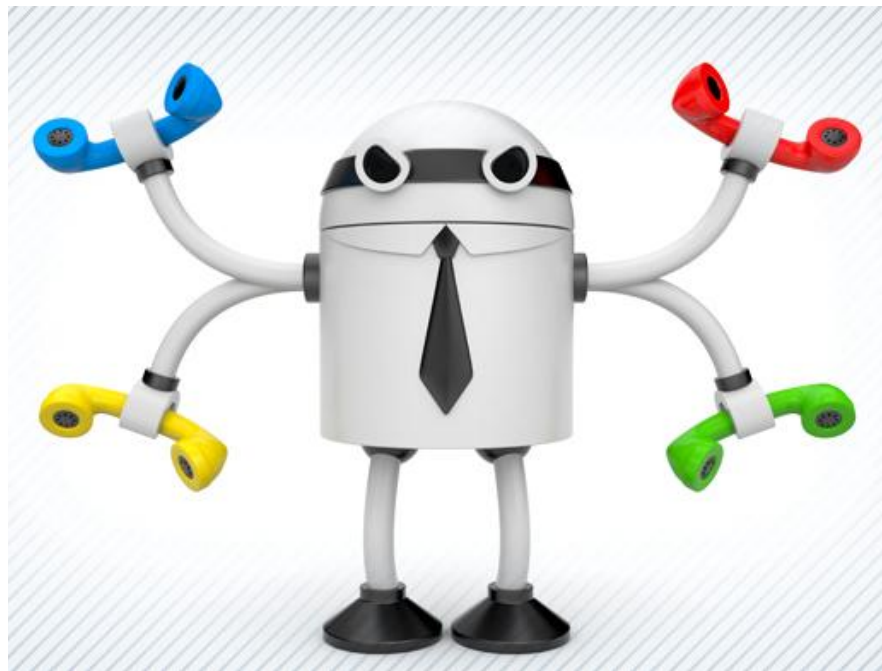


The “Big Boss” Example



Google Business Listing

- List your business online on Google
- Click here for recording [removed].



Can you hear me?

- Subscribe you to services when you say 'YES'
- Click here for recording.
[removed]

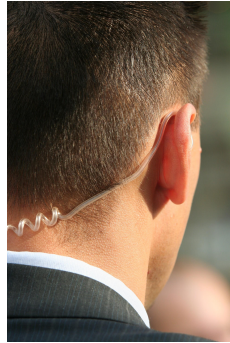


Tax Collection Agency

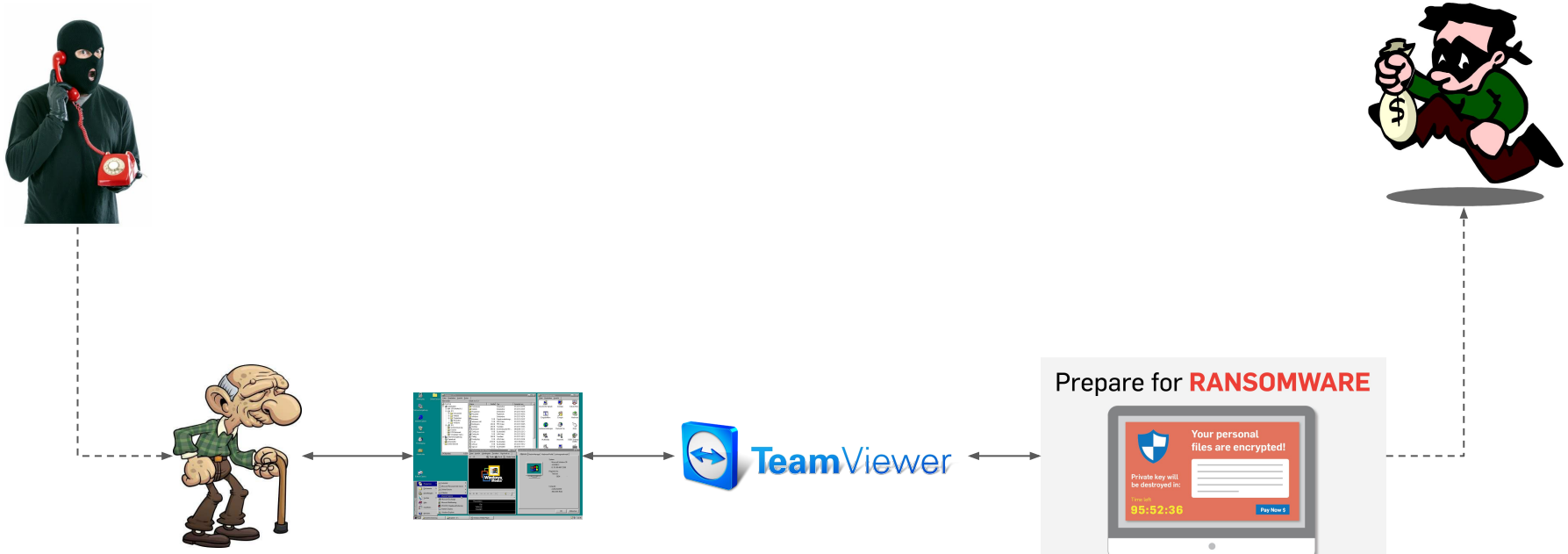
Find you and call
you

Intimidation

Pay using tax
vouchers



Technical Support Scam



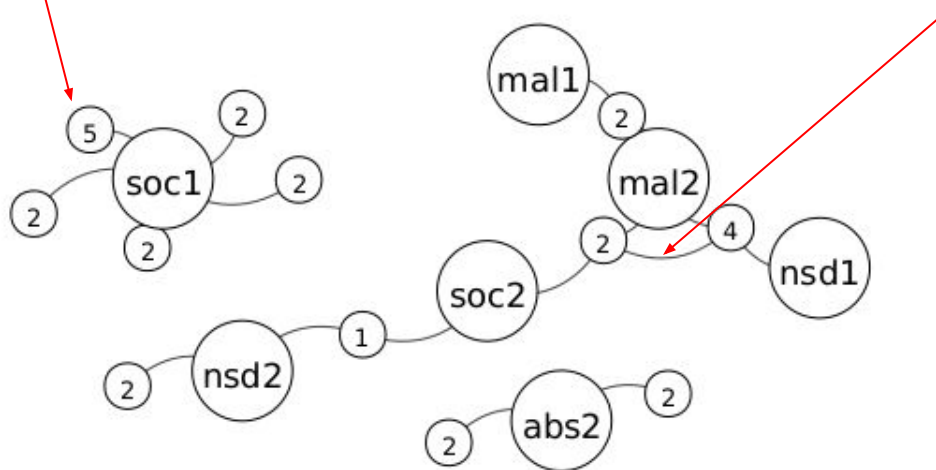
Use of intimidation

- Postal service
 - Fee requested for a package in customs hold
- Telephony provider
 - Contract suspended because bill not paid



How campaigns operate?

- Use of multiple calling numbers to avoid easy detection
- Common sources
 - Multiple campaigns ran by the same gang



Authentication Bypass

[Tencent] Verification code 658339. Use it to change the password of the QQ number 64*****5. Leaking the verification code has a risk. The QQ Security Center.

- Reuse of previously-terminated numbers
- Circumvent 2-factor auth!

Defensive Strategies

- 1) Adopt reputation-based solutions
- 2) Protect your number
- 3) Don't get social engineered
- 4) Look after your 2 auth



Thanks!

Questions?

[@embyte](#)

