Mobile Telephony Threats in Asia

Black Hat Asia 2017, Singapore

Dr. Marco Balduzzi
Sr. Threat Researcher
Trend Micro

Dr. Payas Gupta
Data Scientist
Pindrop

Lion Gu
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

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

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”.


Police Scam, Singapore

10:40
Thursday, Jul 21, 2016

Missed call
9998189022
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!
Current Defeat Strategies

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

Report a phone call from 909-693-3689:

Your Name *

Message *
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 vodafone.

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

<table>
<thead>
<tr>
<th>Rule</th>
<th>Destination no.</th>
<th>Destination IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incoming call</td>
<td>88800 - 88899</td>
<td>192.168.1.10</td>
</tr>
<tr>
<td></td>
<td>83345</td>
<td>192.168.1.11</td>
</tr>
<tr>
<td></td>
<td>83351</td>
<td>192.168.1.12</td>
</tr>
<tr>
<td></td>
<td>88346</td>
<td>192.168.1.13</td>
</tr>
</tbody>
</table>

Telephone Exchange

Call Manager table

SIP Trunk

Call Manager/ PBX

Switch

Phone

IP-192.168.1.11
Tel. ext - 83345

IP-192.168.1.12
Tel. ext - 83351

192.168.1.10
Tel. Range -
     to 88899

Honeypot
Using GSM/VoIP Gateways

Honeycards

GSM

Seeding
1. Mobile Malware
2. Social Networks
3. Public Abuse Lists

Gateway

VoIP

VoIP backend

Calls and sms records

DB

Analysis and reporting (threats)
## Mobile Telephony Honeypot

<table>
<thead>
<tr>
<th>Call Date</th>
<th>Recording</th>
<th>System</th>
<th>CallerIDD</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014-10-09 06:00:05</td>
<td></td>
<td>1412805605.22</td>
<td>&quot;15621192273 &lt;goip1_user&gt;&quot;</td>
</tr>
<tr>
<td>2014-10-08 03:16:04</td>
<td></td>
<td>1412709364.21</td>
<td>&quot;13932125820 &lt;13932125820&gt;&quot;</td>
</tr>
<tr>
<td>2014-10-07 23:05:03</td>
<td></td>
<td>1412694303.20</td>
<td>&quot;15361099194 &lt;15361099194&gt;&quot;</td>
</tr>
<tr>
<td>2014-10-06 12:41:34</td>
<td></td>
<td>1412570494.19</td>
<td>&quot;15921962935 &lt;goip1_user&gt;&quot;</td>
</tr>
<tr>
<td>2014-10-04 18:58:07</td>
<td></td>
<td>1412420287.18</td>
<td>&quot;10086 &lt;10086&gt;&quot;</td>
</tr>
<tr>
<td>2014-10-04 08:52:02</td>
<td></td>
<td>1412383922.17</td>
<td>&quot;02759375431 &lt;02759375431&gt;&quot;</td>
</tr>
<tr>
<td>2014-10-04 07:48:55</td>
<td></td>
<td>1412380135.16</td>
<td>&quot;15678278590 &lt;15678278590&gt;&quot;</td>
</tr>
<tr>
<td>2014-10-02 21:38:38</td>
<td></td>
<td>1412257118.15</td>
<td>&quot;13146397703 &lt;13146397703&gt;&quot;</td>
</tr>
<tr>
<td>2014-09-30 09:21:44</td>
<td></td>
<td>1412040104.14</td>
<td>&quot;13552070625 &lt;13552070625&gt;&quot;</td>
</tr>
<tr>
<td>2014-09-29 18:34:07</td>
<td></td>
<td>1411986847.13</td>
<td>&quot;13262374867 &lt;13262374867&gt;&quot;</td>
</tr>
<tr>
<td>2014-09-29 17:03:08</td>
<td></td>
<td>1411981388.12</td>
<td>&quot;15259205763 &lt;15259205763&gt;&quot;</td>
</tr>
<tr>
<td>2014-09-29 09:38:08</td>
<td></td>
<td>1411954688.11</td>
<td>&quot;13552188861 &lt;13552188861&gt;&quot;</td>
</tr>
<tr>
<td>2014-09-28 19:40:27</td>
<td></td>
<td>1411904427.10</td>
<td>&quot;13261803466 &lt;13261803466&gt;&quot;</td>
</tr>
</tbody>
</table>
Mobile Telephony Honeypot

<table>
<thead>
<tr>
<th>D</th>
<th>App</th>
<th>Destination</th>
<th>Disposition</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Playback</td>
<td>15621192273</td>
<td>ANSWERED</td>
<td>00:01</td>
</tr>
<tr>
<td></td>
<td>Playback</td>
<td>18757194227</td>
<td>ANSWERED</td>
<td>00:02</td>
</tr>
<tr>
<td></td>
<td>Playback</td>
<td>13860141274</td>
<td>ANSWERED</td>
<td>00:03</td>
</tr>
<tr>
<td></td>
<td>Playback</td>
<td>15921962935</td>
<td>ANSWERED</td>
<td>00:47</td>
</tr>
<tr>
<td></td>
<td>Playback</td>
<td>18757194227</td>
<td>ANSWERED</td>
<td>00:40</td>
</tr>
<tr>
<td></td>
<td>Hangup</td>
<td>hangup</td>
<td>ANSWERED</td>
<td>00:49</td>
</tr>
<tr>
<td></td>
<td>Wait</td>
<td>15602228631</td>
<td>ANSWERED</td>
<td>00:01</td>
</tr>
<tr>
<td></td>
<td>Playback</td>
<td>13477033614</td>
<td>ANSWERED</td>
<td>00:02</td>
</tr>
<tr>
<td></td>
<td>Playback</td>
<td>18701408339</td>
<td>ANSWERED</td>
<td>00:06</td>
</tr>
<tr>
<td></td>
<td>Playback</td>
<td>13477033614</td>
<td>ANSWERED</td>
<td>00:02</td>
</tr>
<tr>
<td></td>
<td>Playback</td>
<td>13860141274</td>
<td>ANSWERED</td>
<td>00:32</td>
</tr>
</tbody>
</table>
Example of Call Recording
例示短信录音

- 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?
General Results
Social Networks

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

[*] http://www.xhqm.cn/
Malicious Apps

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

[*] 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

1. Pretend to know the victim
2. Ask for IM contact
3. Confirm IM
4. Send payment instructions (paypal)
5. Confirm paypal
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