# Mobile Security Threats: Apps

## Tales from the real (Mobile Network) World

OWASP
The Open Web Application Security Project

adaptivemobile™
trusted network protection

# About Me

- Cathal Mc Daid
  - Head of Data Intelligence & Analytics

- AdaptiveMobile
  - **World leader in Mobile Security**
  - **Unique, Complete, ‘Multi-bearer’ Solution**
  - **Scalable**
  - **Industry Leading Experience**
  - **Privately held**
  - **Global presence**

adaptivemobile™
trusted network protection

# Mobile Security

OWASP
The Open Web Application Security Project

## Many things to many people:

- **In the News**
  - Mobile Malware/Spyware
  - Mobile Network Security
  - Security of Banking transactions
  - Bring Your Own Device (BYOD)
  - Data Loss Protection (DLP)
  - Mobile Spam
  - Stolen devices
  - Privacy Concerns
  - Internet of Things
  - Etc,,,,

## However, in many it involves non-obvious threats

# Recent App threats you wouldn't have considered

OWASP
The Open Web Application Security Project

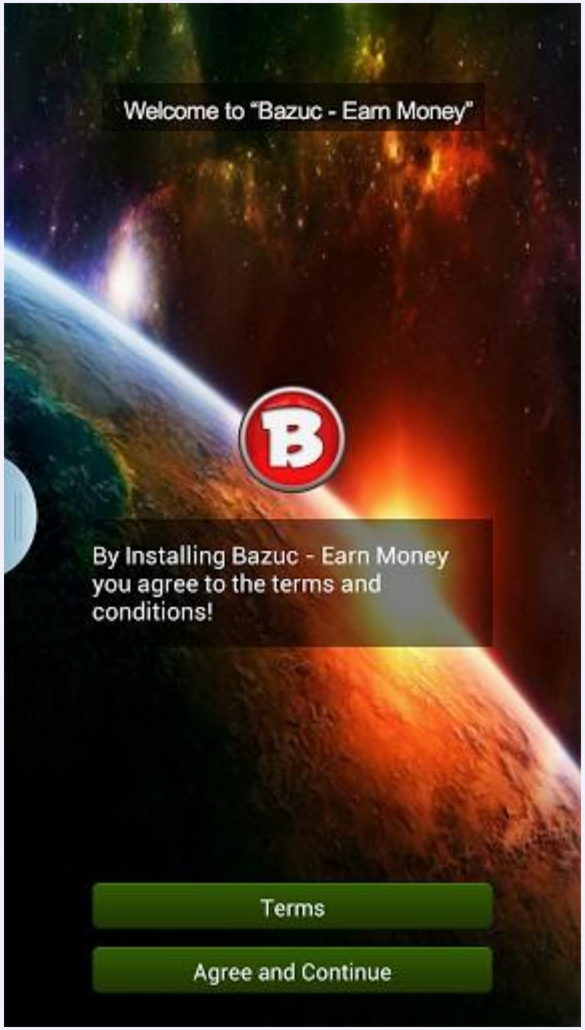
# Recent App threats you wouldn't have considered

## Broadening your Horizons

- 1) Why would you deliberately infect your mobile phone
  - How your App choices can affect the stock market

- 2) Misbehaving Billion Dollar Apps
  - Right & Wrong ways to get noticed

# Bazuc: Money for Nothing



Welcome to "Bazuc - Earn Money"

By Installing Bazuc - Earn Money you agree to the terms and conditions!

# What is Bazuc?

'A free Android app that will allow you to earn extra money every day by selling us your SMS / Text Message credits that come with your monthly phone plan.'

**$0.001** per SMS sent from user's device

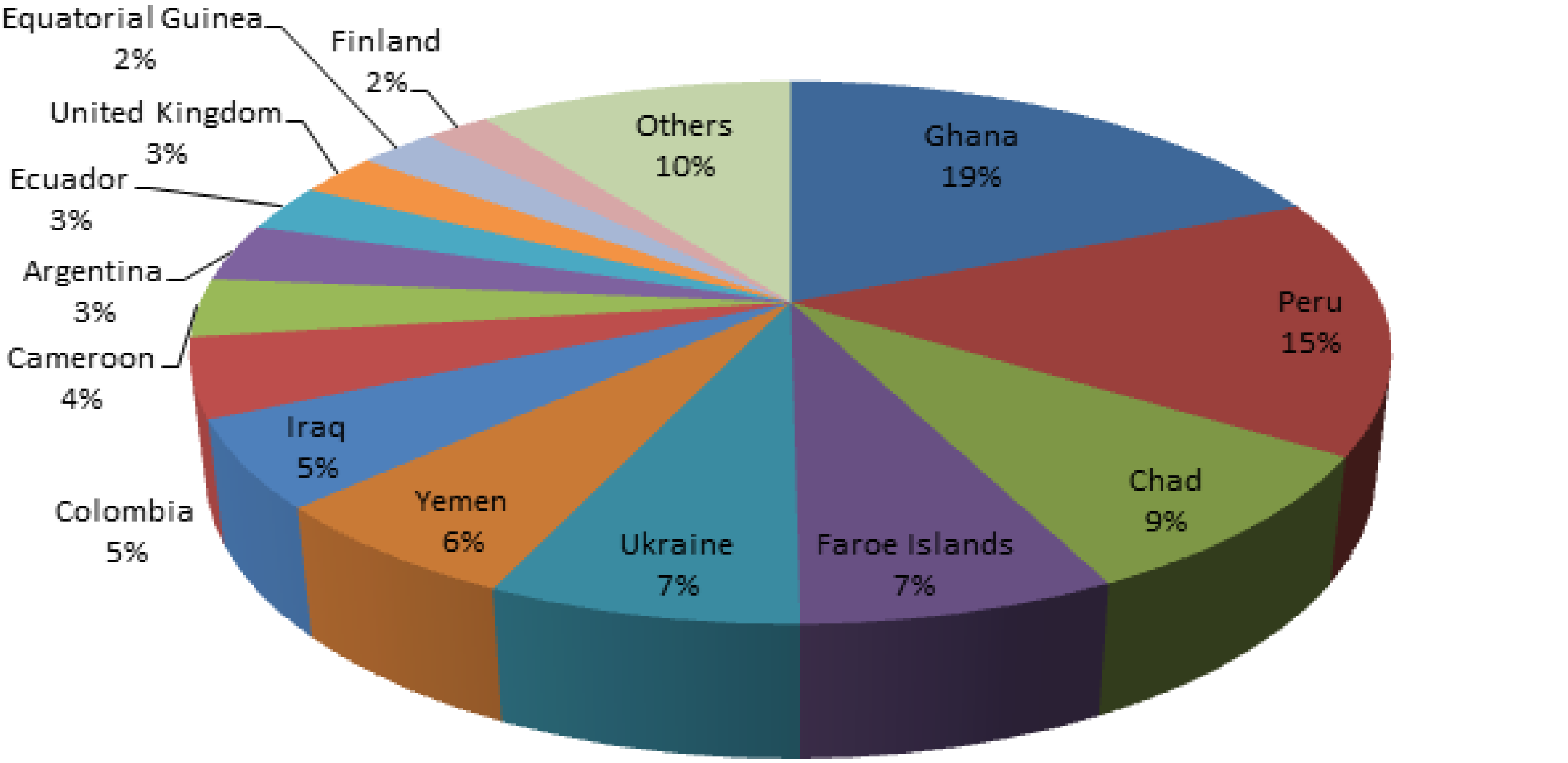
# How it works

- **User goes to App store & installs Bazuc**
  - ***2 versions***
- **User Configures account**
- **If phone switched on**
  - **Bazuc App connects to central server over IP**
  - **Central server sends text content and recipient mobile numbers to App**
  - **App sends text content (silently) from your mobile phone**
  - **You get paid $0.001 per message**
  - **Not a bad idea? : text-sharing of user’s messaging plan**

# How it works

- **What kind of texts?**
  - *App Verification codes:*
    - Your XXXXXX code is 2416. Enter your code or just tap this link: m.xxxxxx.com/c/2416
  - *Personal messages*
    - “Sereza,Spasibo tebe Bolscoe sa babuscku..Spasibo!!!!” [Sergey, thank you very much for grandma. Thank you!]
  - *Spam*
    - Dear gillian your loan application of  250 GBP has been accepted. Please call 0872563****.”
- **User never sees these texts,**

# Where do messages go?: International Version



Most popular SMS destinations

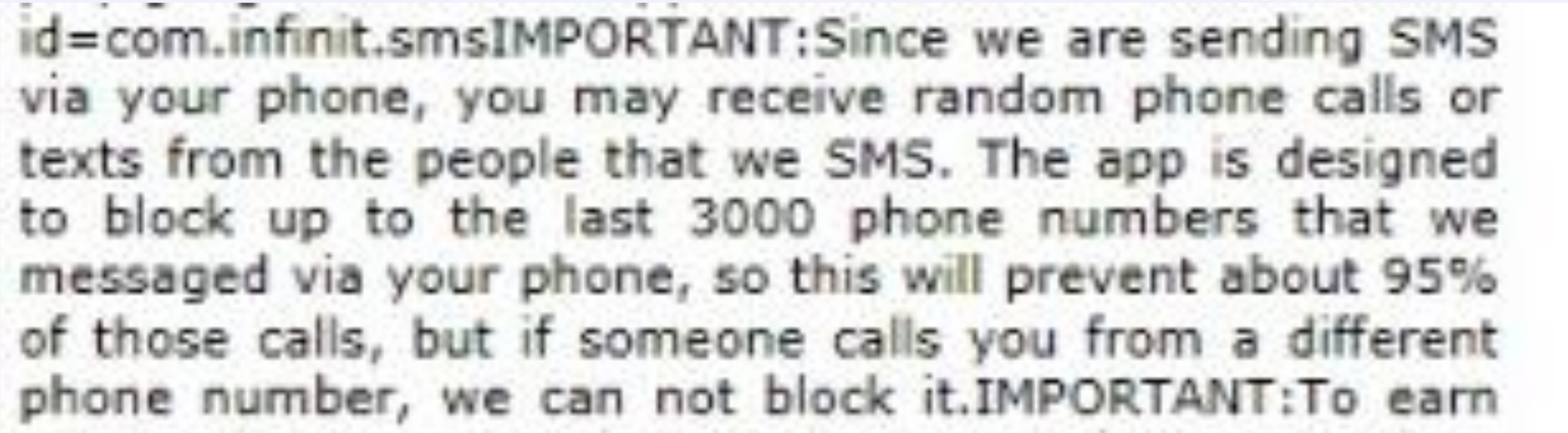
# Why are they doing this

OWASP
The Open Web Application Security Project

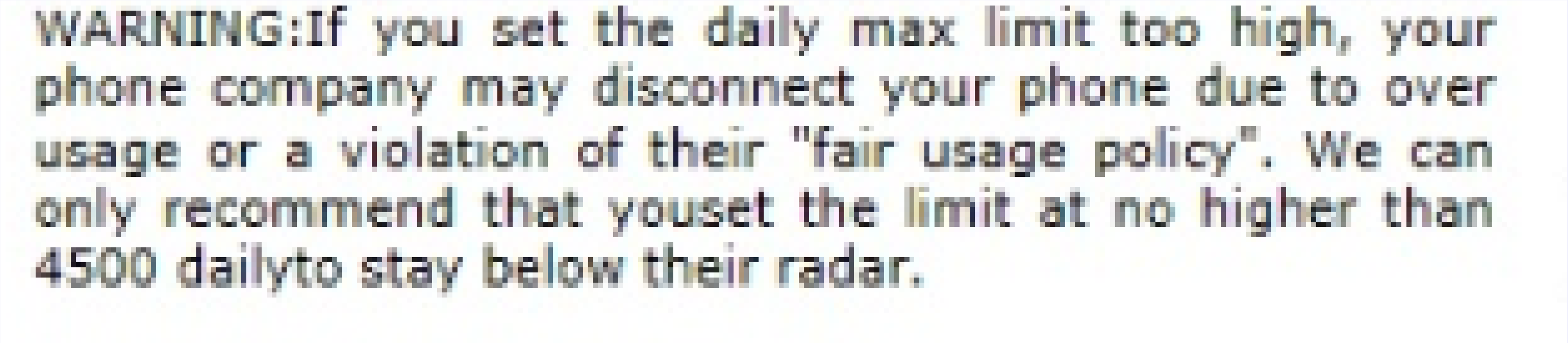
- Bazuc uses your phone to send text messages very cheaply
  - The Bazuc owners exploits **imbalances** in the costs of sending SMS

- Some problems:
  - If **international version** Bazuc could run up bills **of <u>tens of thousands of dollars/euro</u>** for those who think they have unlimited international messaging when they don't
  - Breaks operators terms and conditions (lead to disconnection)
  - Privacy concerns:
    - What are these messages being sent from my phone?
    - Start receiving phone calls & messages from strangers?

# Some Bazuc Fine print



id=com.infinit.smsIMPORTANT:Since we are sending SMS via your phone, you may receive random phone calls or texts from the people that we SMS. The app is designed to block up to the last 3000 phone numbers that we messaged via your phone, so this will prevent about 95% of those calls, but if someone calls you from a different phone number, we can not block it.IMPORTANT:To earn



WARNING:If you set the daily max limit too high, your phone company may disconnect your phone due to over usage or a violation of their "fair usage policy". We can only recommend that youset the limit at no higher than 4500 dailyto stay below their radar.

# Different way of thinking about it

- Imagine someone asks you to:
  - – *Transport something using unused space*
  - – *Don’t worry what the space will be used for*
  - – *You will get some money for it*
  - – *Stay under the radar!*
- Sound familiar?
- Turns Mobile Phone Subscribers into **Spam-Mules**

# Indication of Spam-mule Volumes

OWASP
The Open Web Application Security Project

| Sender | Number of messages |
|---|---:|
| **Spam-Mule A** | ~3000 |
| **Spam-Mule B** | ~100 |
| **Spam-Mule C** | ~2300 |
| **Spam-Mule D** | ~50 |
| **Spam-Mule E** | ~120 |
| **Spam-Mule F** | ~50 |
| **Spam-Mule G** | ~10200 |
| **Spam-Mule H** | ~1800 |
| **Spam-Mule I** | ~4500 |
| **Spam-Mule J** | ~150 |
| **Spam-Mule K** | **~40000** |

# Other Dangers?

- **Most** messages sent by Bazuc apps are not spam, are relayed commercial/personal msgs
  - Spam causes the spam-mule to get detected/blocked quicker

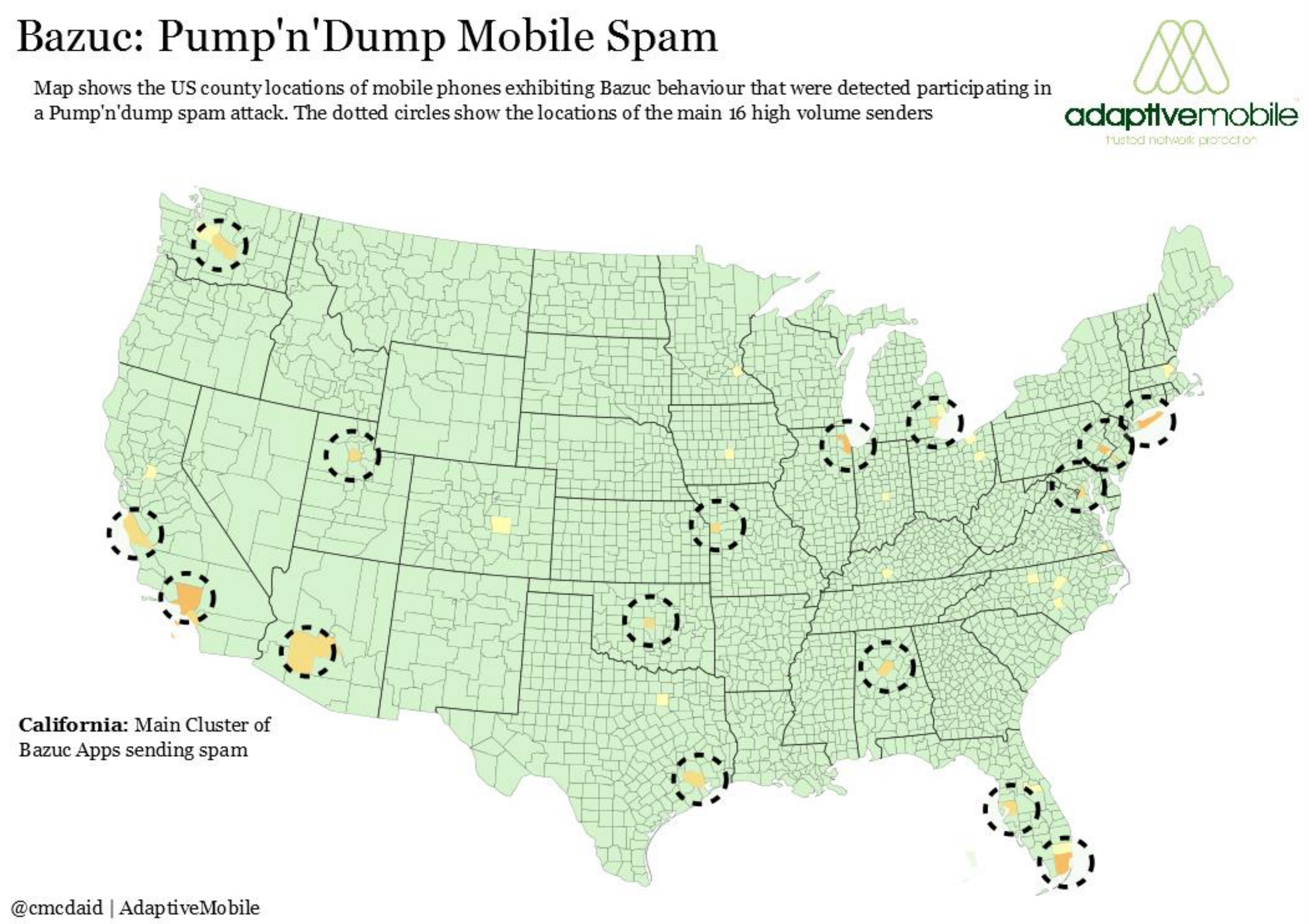
**However**

- Mobiles exhibiting Bazuc app behaviour took part in massive (~100k) **Penny Stock** spam attack in September/October in US

# Penny Stock

***Buy Signal Alert – [REDACTED] is hot. Get in now and look for potential 3000% gain. www.[REDACTED].com***

# Visual Impact (1) – Geographic Spread of Bazuc-infected phones



## Bazuc: Pump'n'Dump Mobile Spam

Map shows the US county locations of mobile phones exhibiting Bazuc behaviour that were detected participating in a Pump'n'dump spam attack. The dotted circles show the locations of the main 16 high volume senders

**California:** Main Cluster of Bazuc Apps sending spam

@cmcdaid | AdaptiveMobile

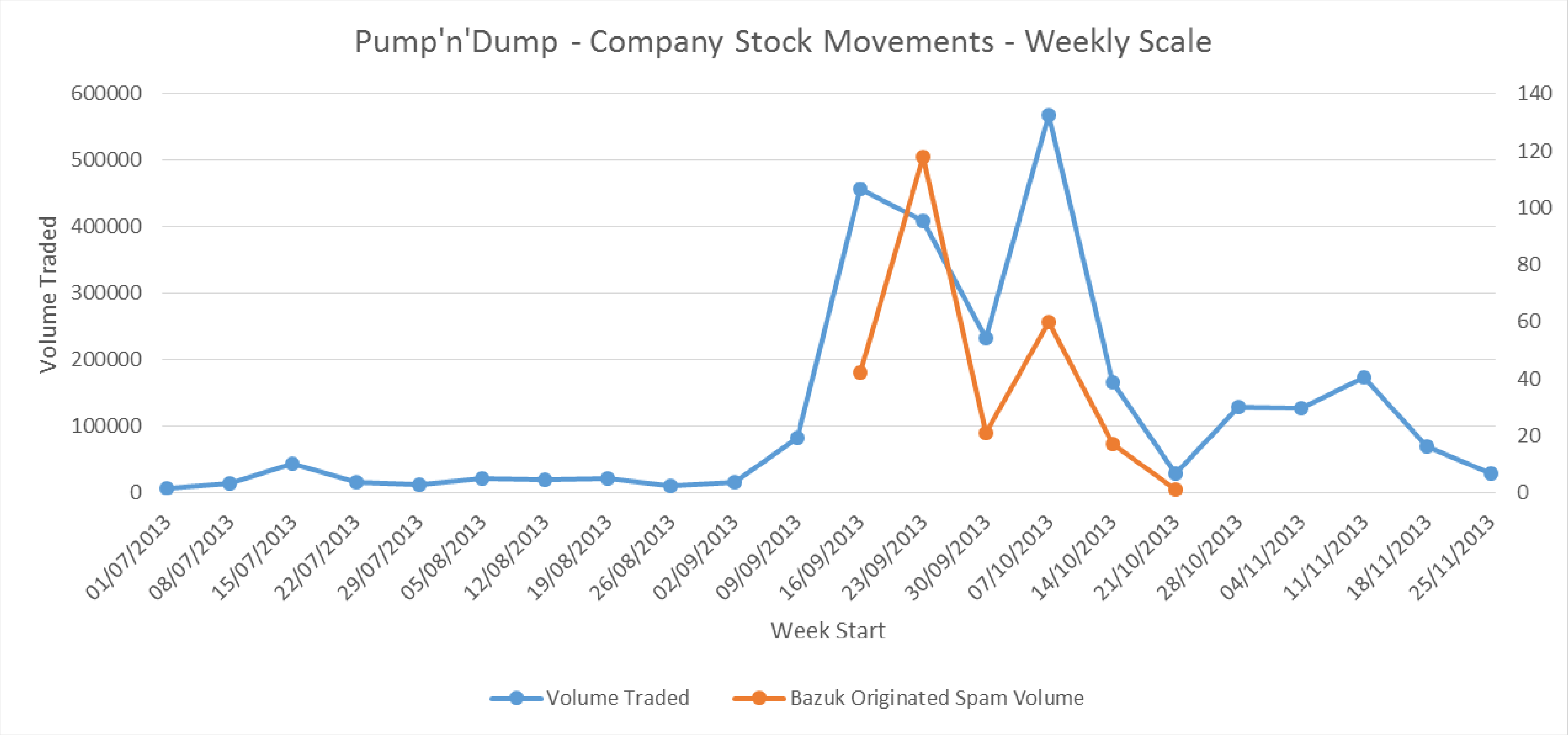
# Visual Impact (2) – Geographic Spread of spam attack

adaptivemobile
rusted network protection

Cathal Mc Daid @mcdaidc

# Stock Impact?

OWASP
The Open Web Application Security Project



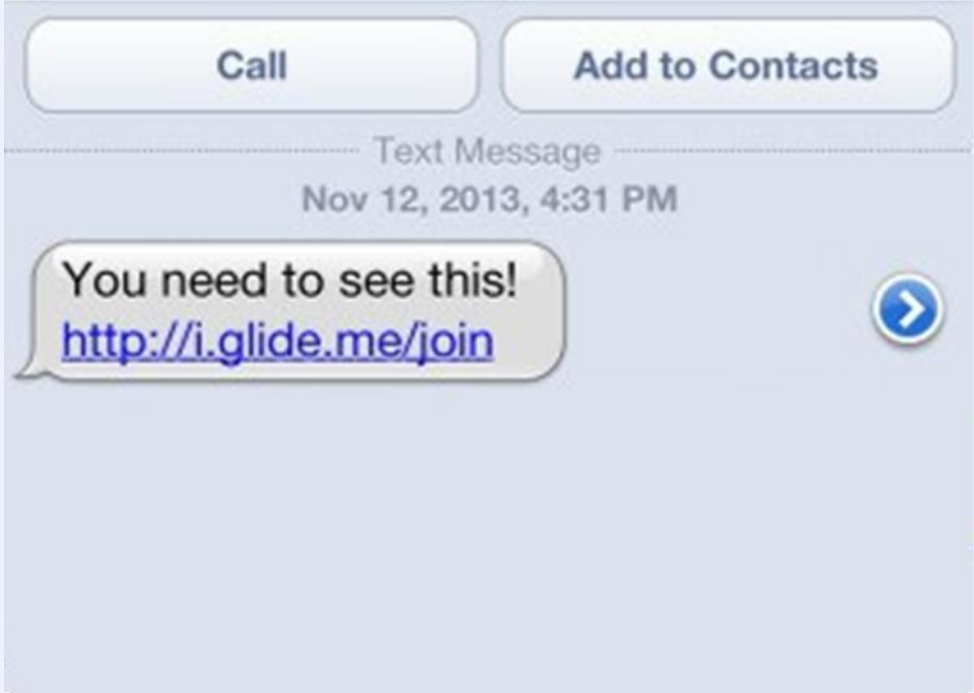
Total Stock traded during July/Aug period: **$31k**

Total Stock traded during Sep/Oct period: **$682k**

# Conclusion

- **Bazuc was removed from Google play and some other App stores. For more info:**
  - **Initial AdaptiveMobile blog: http://www.adaptivemobile.com/blog/money-nothing-sms-free**
  - **Follow up Lookout blog : https://blog.lookout.com/blog/2013/12/19/shoot-the-bulk-messenger/**
- **Attempting to Exploit imbalances via Mobile Subscribers,**
  - **left them holding the risk**
  - **Broke Operators term & conditions**
- **If too good to be true, it normally isn't**

# Part 2: What's a Friendly (Social) App to do



Nov 12, 2013, 4:31 PM

You need to see this!
http://i.glide.me/join

# What’s the problem?

- Growth hacking: aggressive, viral app promotion via mass SMS
- Causes lots of traffic, and lots of subscriber complaints

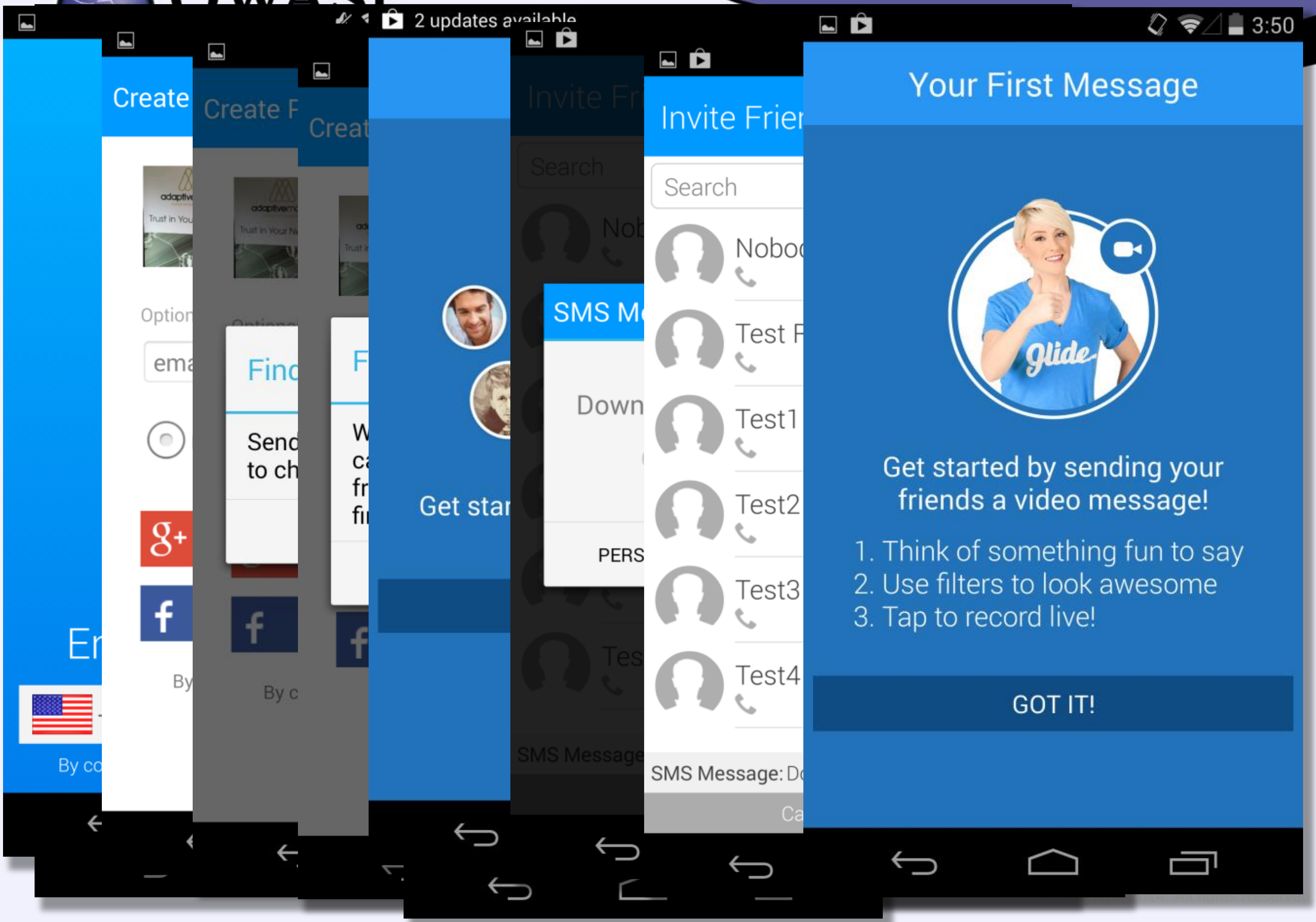
**Can cause app to be blocked completely**

# Growth Hacking Process

1. Install the app
2. Sign up
3. Invite your contacts

- Your contacts get spammed with “Install this great app! <LINK>”
- The messages are (nearly always) originated from your own phone
- It can be hard to avoid sending the invites, depending on UI…

# UI Case Study: Glide



## Your First Message

Get started by sending your friends a video message!

1. Think of something fun to say
2. Use filters to look awesome
3. Tap to record live!

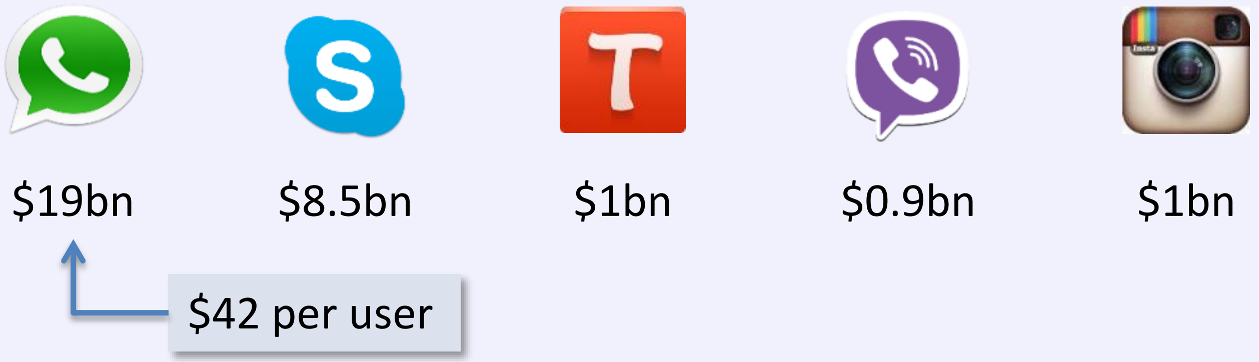
GOT IT!

# Growth Hacking: Why? Need to get message out

# The attraction of growth hacking

OWASP
The Open Web Application Security Project

Valuation = App functionality x User base



$19bn

$8.5bn

$1bn

$0.9bn

$1bn

$42 per user

- Land-grab for active users
- Value of being the “big player”
- Growth hacking is cheap
- Uses the strength of word-of-mouth endorsement

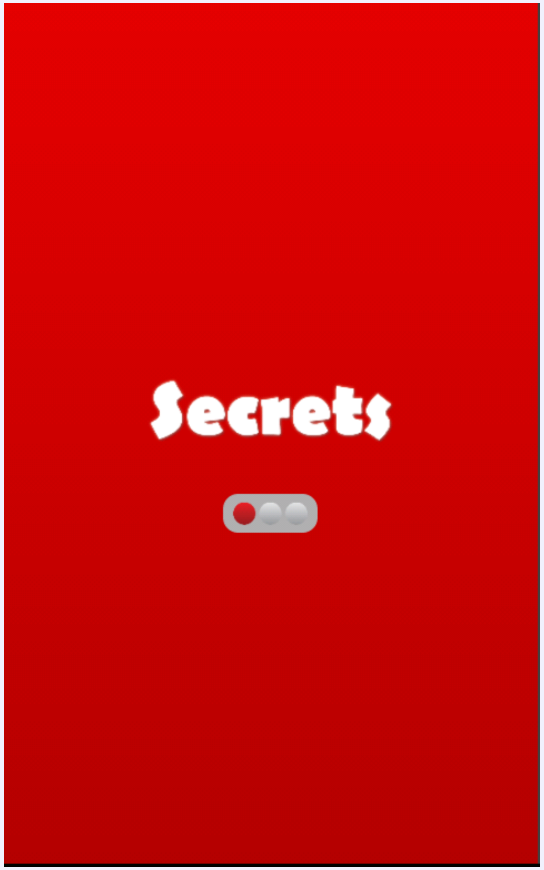
# Why we investigated growth hacking

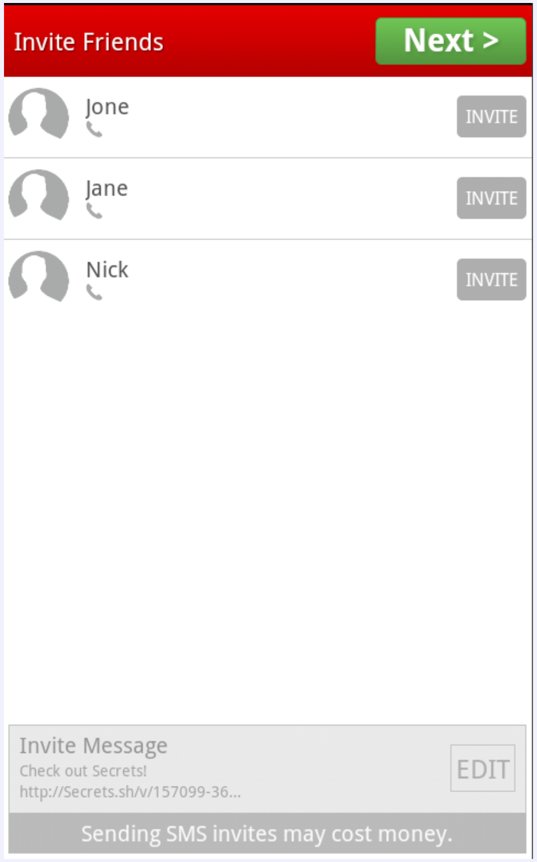
- People **complain** about it, it’s **unsolicited**, it’s in **bulk**, you **can’t unsubscribe**. It’s clearly spam
- Apps are generating a significant proportion of spam complaints
  - Especially in countries with active anti-spam programs
- Financial cost to users if SMS are out of bundle
  - Or if recipients are charged
- It’s commercial messaging, so it violates operator T&Cs
- In bad design cases “Viral” nature of propagation causes network congestion
  - Estimate 5.3 to 6.8 million sent in US per day

# Bad Design Case in point: Secrets

- Two problems:
  - Very Aggressive “Invite All” UI design
  - Incorrect Messaging Client Design

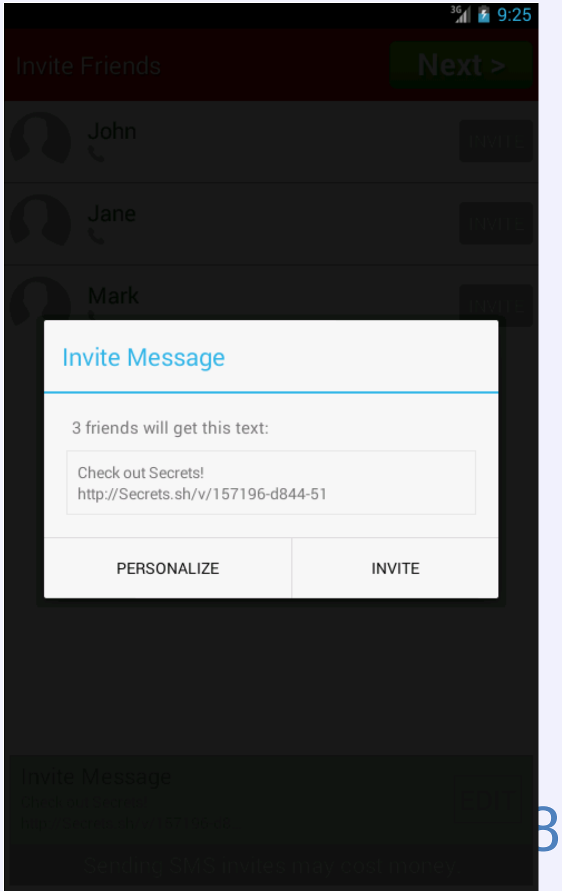
450k SMS sent in 2 days
One sender sent 30k





Invite Message
Check out Secrets!
http://Secrets.sh/v/157099-36...

Sending SMS invites may cost money.



Invite Message

3 friends will get this text:

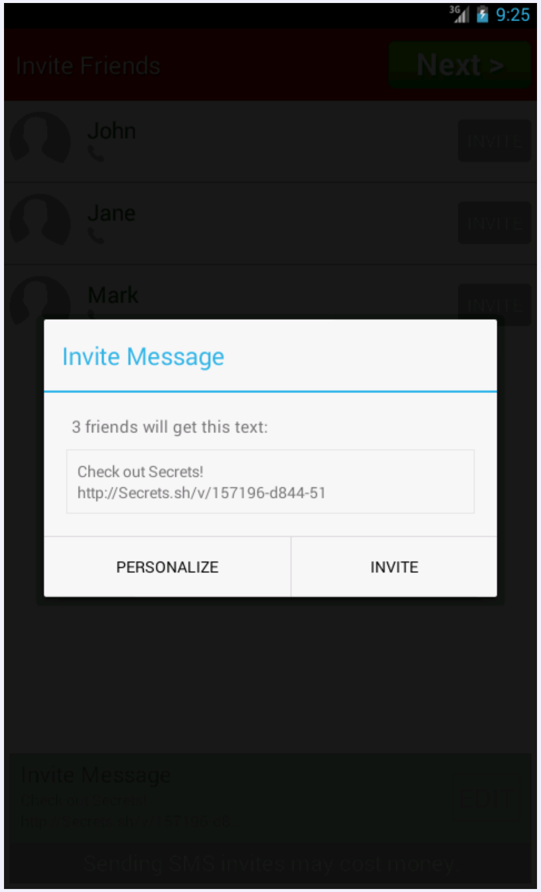
Check out Secrets!
http://Secrets.sh/v/157196-d844-51

# How we sized the problem

- We asked ourselves:
  - What are the traffic patterns?
  - What is the impact?
  - Which apps are the big offenders?
  - Which apps are "playing nice"?

# + impact of App UI characteristics

- UI design influences growth hacking impact
- We checked each app’s UI for:
  - Can contacts be invited?
  - Can all contacts be invited?
  - Is the user asked to invite contacts?
  - Is the user asked to invite all contacts?
  - Are all contacts preselected for invitation?
  - Is it easy to abort the invitation process?
  - Can the invitation be edited?



Invite Message

3 friends will get this text:

Check out Secrets!
http://Secrets.sh/v/157196-d844-51

Invite Message
Check out Secrets!
http://Secrets.sh/v/157196-d8

Sending SMS invites may cost money

# Results:  App characteristics

OWASP
The Open Web Application Security Project

| App | Can invite friends | Can invite all | Asks to invite friend | Asks to invite all | All pre-selected | Not easy to abort | Can't edit invite |
|---|---|---|---|---|---|---|---|
| Glide | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ |
| Secrets | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ |
| Video Kik | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ |
| Skout | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ |
| Pixer | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ |
| Hangtime | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ |
| Meow | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ | ✓ |
| Tango | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ | ✓ |
| Voxer | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ |
| Dice with Buddies | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |

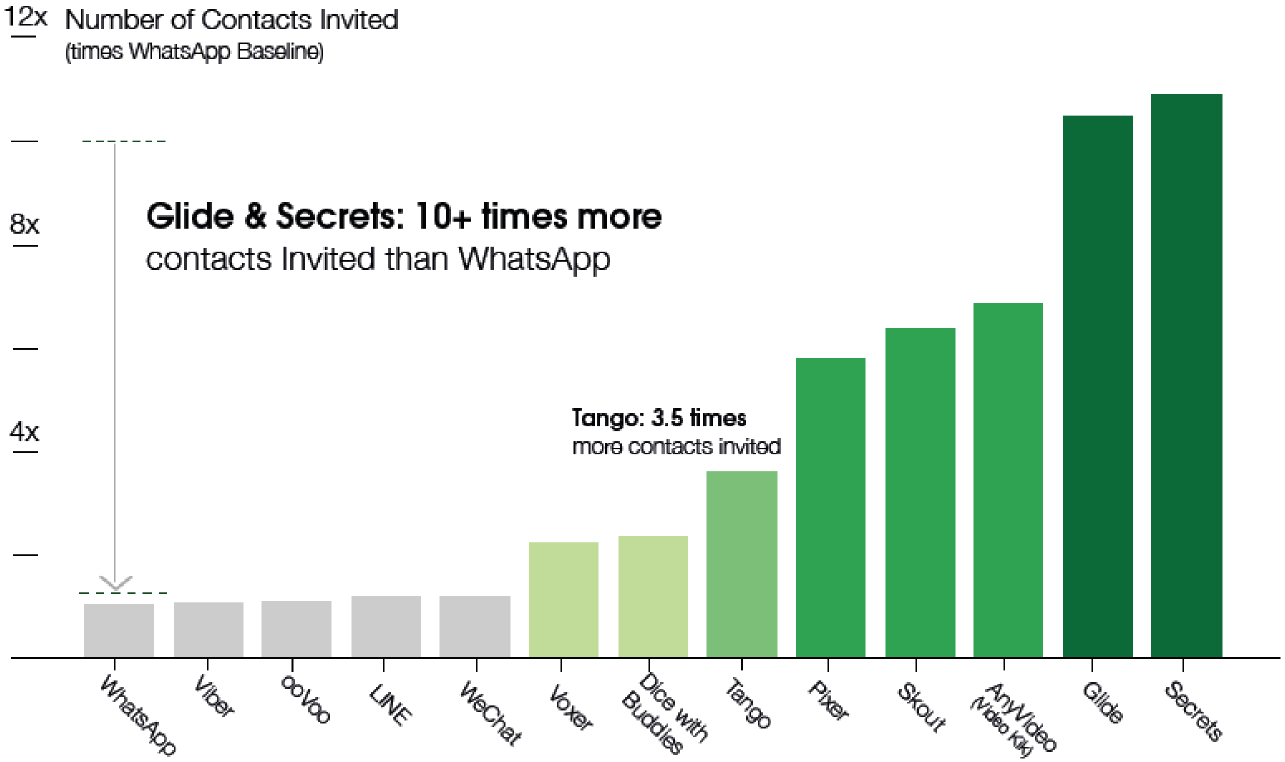
# Results: App characteristics

| App | Can invite friends | Can invite all | Asks to invite friend | Asks to invite all | All pre-selected | Not easy to abort | Can't edit invite |
|---|---|---|---|---|---|---|---|
| LINE | ✓ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| ooVoo | ✓ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| WhatsApp | ✓ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ |
| Viber | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| WeChat | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |

# Number of Invites sent per App

## How Many of your Contacts get Appspam from you?

Breakdown, in North America, of average number of Contacts sent an Invite once a Growth Hacking App is installed on a mobile device.



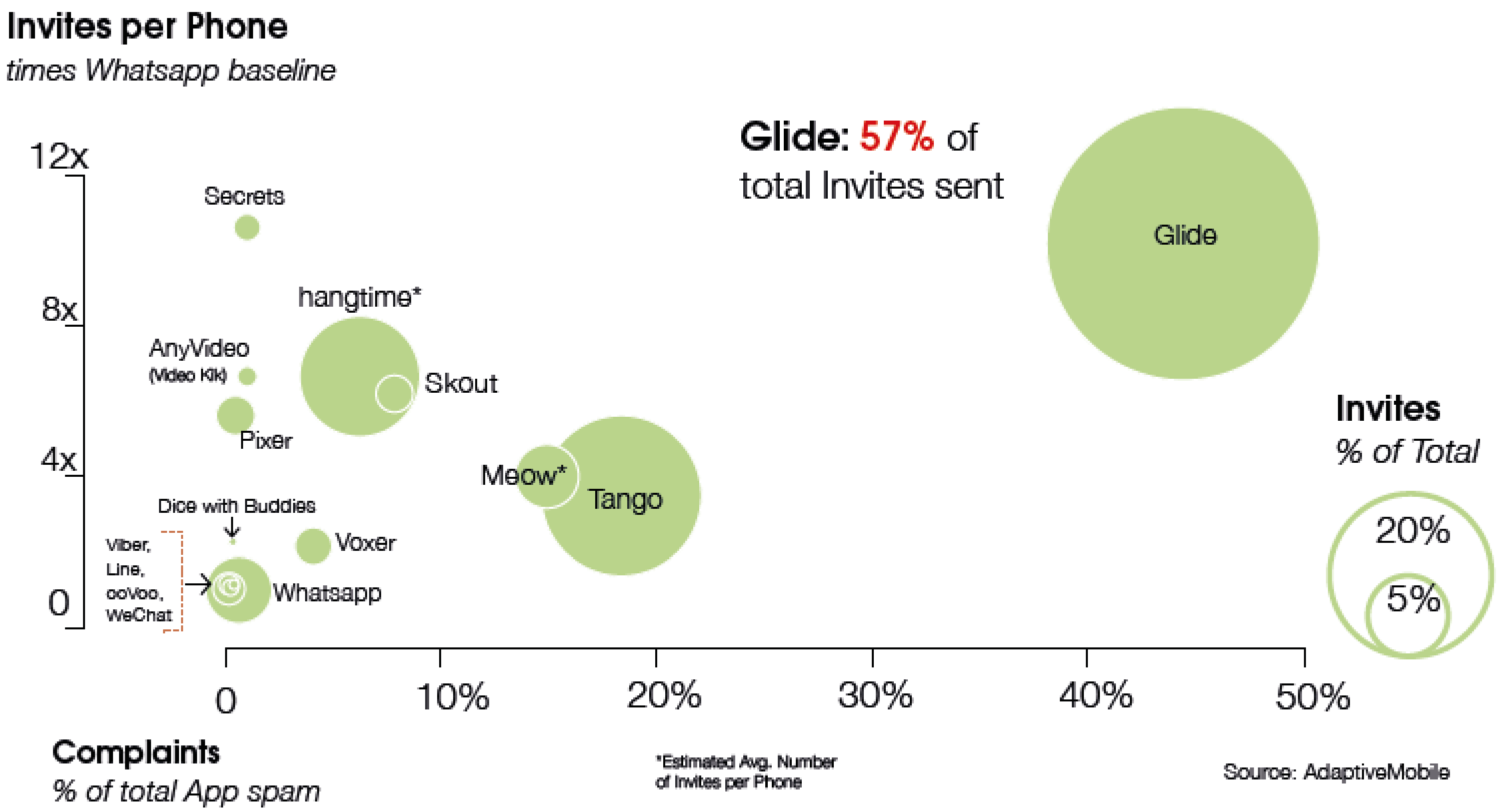
***HangTime & Meow** : No data shown as Invites are not generated from device

Sources: AdaptiveMobile

# Which apps generate complaints?

## The Biggest App Spammers

**Glide** & **Tango** account for **76.9%** of all high volume Growth Hacking Messages sent in North America.

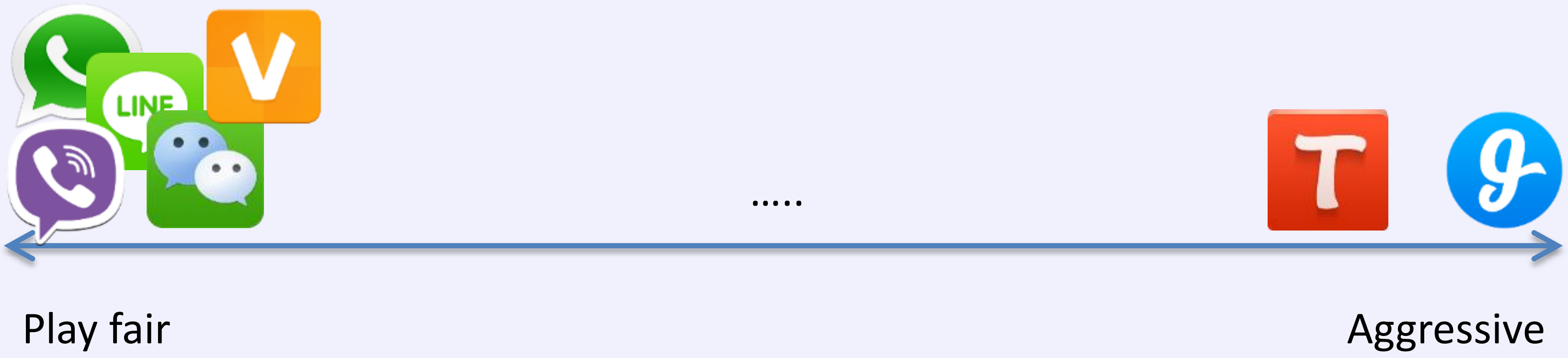


*Estimated Avg. Number of Invites per Phone

Source: AdaptiveMobile

# Results summary

- App UI characteristics correlate with growth hacking volumes and user complaints
  - The more aggressive UI characteristics an app has,
  - the more complaints it generates,
  - and the more growth hacking traffic it causes



# Our recommendations

OWASP
The Open Web Application Security Project

- Apps which use growth hacking "ethically" should:
  - Make it easy for a user not to invite all contacts
  - Not ask on start up or activity to invite all contacts
  - Not give an "invite all" option
  - Not pre-select all contacts to be invited in an invite screen
  - Allow the user to edit the invite text
  - Not make inviting others via SMS Invites, part of an incentive system

- Guidelines are derived from the well-behaved apps
  - They generate minimal complaints
  - Despite their large user bases

## Summary

- Aggressive Growth hacking is
  - Causing customer complaints: Both App users and those who receive them
  - Costing money
  - Violating network T&Cs
  - Causing unwanted network load
- But it’s not all bad: Many apps use growth hacking responsibly
- After a number of months of monitoring, our publications and Play Store changes, some apps are changing their behaviour
- Apps that exhibit aggressive behaviours put themselves at risk of being blocked and taken down

# Overall Conclusion

OWASP
The Open Web Application Security Project

- Mobile Security
  - Often thought of to mean Mobile Malware type attacks
- But many other areas:
  - Network (SS7) Security, Messaging Security,  Privacy Security etc
- Regards Apps: whole spectrum of activity, from
  - Innovative bad (Bazuc) to badly executed good (aggressive Growth Hacking)
  - In the end it always comes down to money