RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

OTT, Virtual Carriers and the new wave of spam threats in the 4G/LTE World

SESSION ID: MBS-W04A

Simeon Coney

Senior Vice President: Security Practice
AdaptiveMobile Security

www.AdaptiveMobile.com

Big Statements

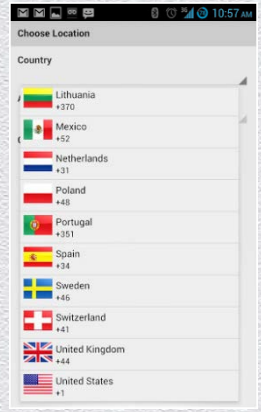
- Mobile Spam in North America – originating from “Main” operators is collapsing
  - Better defenses, technology & intelligence
  - Collaboration (Operators, Industry, Law Enforcement)

- Mobile Spammers are now switching to other routes to your handset
  - VoIP / Virtual Carriers now preferred
  - Other less well protected interfaces

Getting new accounts from Virtual Carriers is trivial

On Handset Apps

- Pick your country & city of choice for snow-shoe accounts
- No Physical SIM card / device required



Bulk Sending API's even easier

- API's commonly available

JSON | XML | **PHP** | Python | C# | Java | Ruby | Node.js

```
<?php
// Get the PHP helper library from *****.com/docs/php/install
require_once('/path/to/*****-php/Services/*****.php');
// Your Account Sid and Auth Token
$sid = "********************";
$token = "{{ auth_token }}";
$client = new Services_*****($sid, $token);
$client->account->messages->sendMessage($snowshoeaccountnumber,
$target_list , "Spam message goes here");
```

adaptivemobile
trusted network protection

Visualizing Spam Attacks from these sources

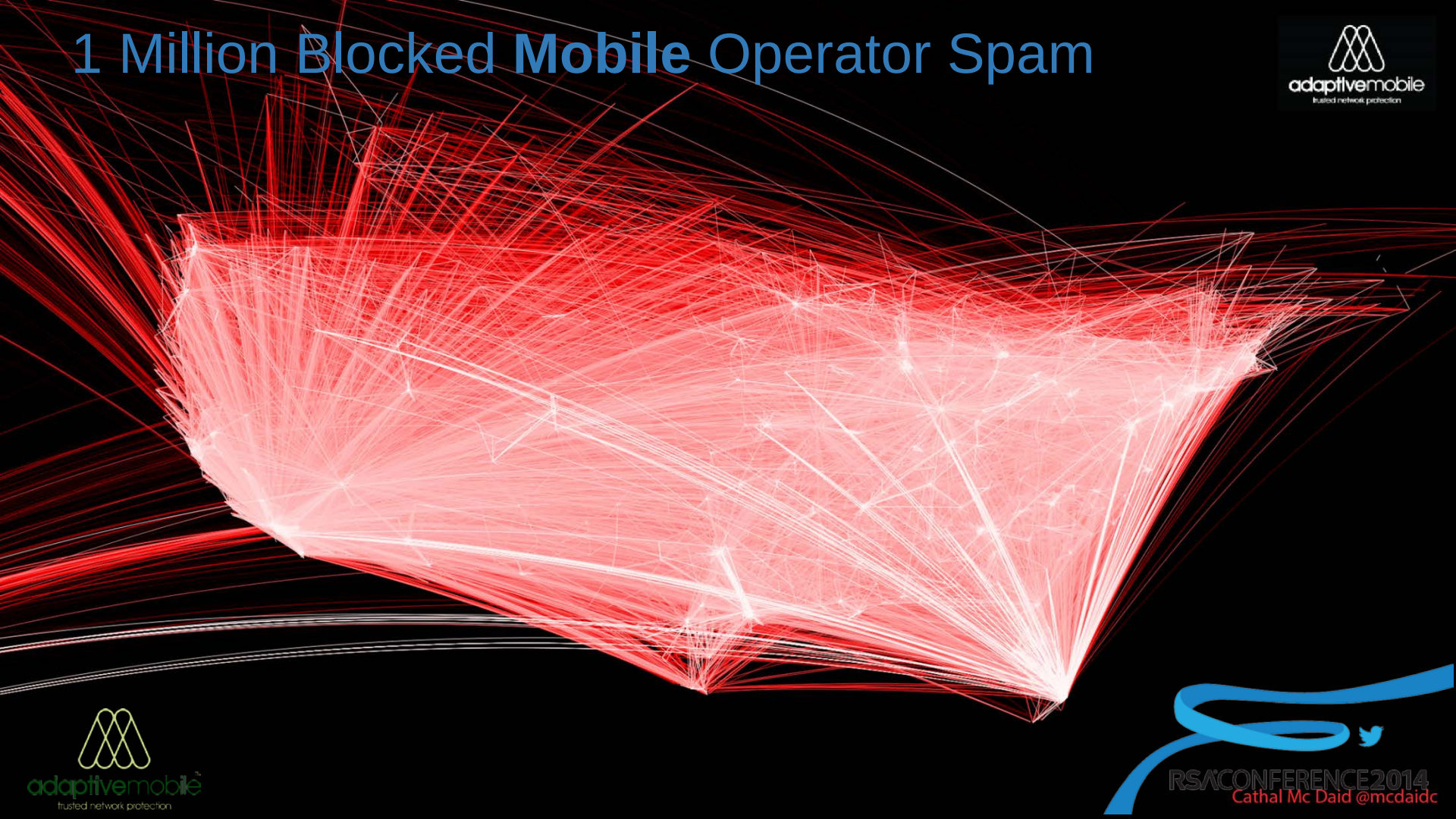
From “Main” Mobile Operators

- Messaging attacks should be concentrated / bursty
  - Physical presence (i.e. location) required
  - Account take down motivated by Operators to maintain reputation

From Virtual Operators

- Messaging attacks from VoIP operators should be distributed
  - Lots of accounts possible (to spread attack profile)
  - Multiple sources

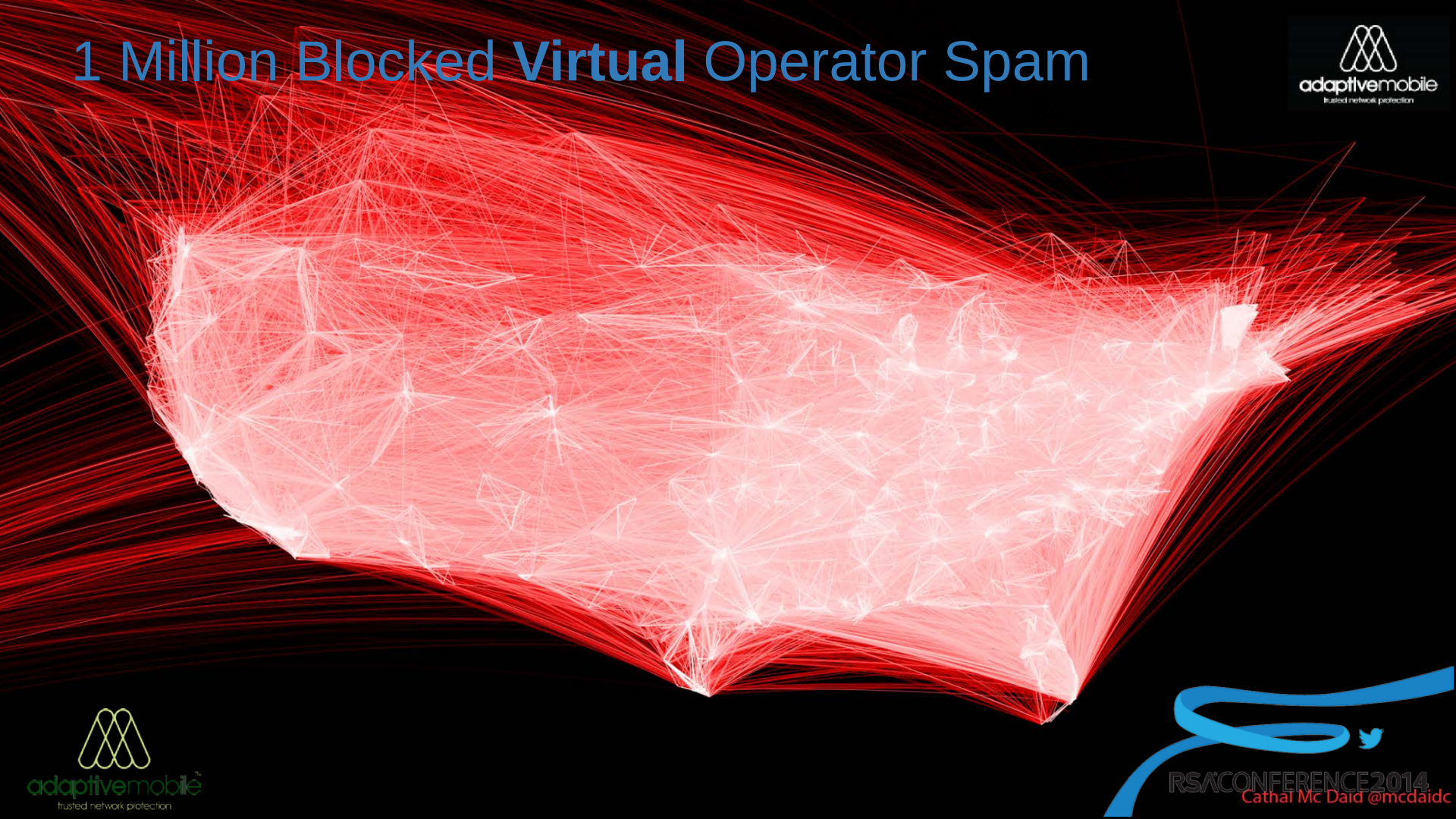
1 Million Blocked **Mobile** Operator Spam



adaptivemobile
trusted network protection

RSACONFERENCE2014
Cathal Mc Daid @mcdaidc

1 Million Blocked **Virtual** Operator Spam



adaptivemobile
trusted network protection

RSACONFERENCE2014

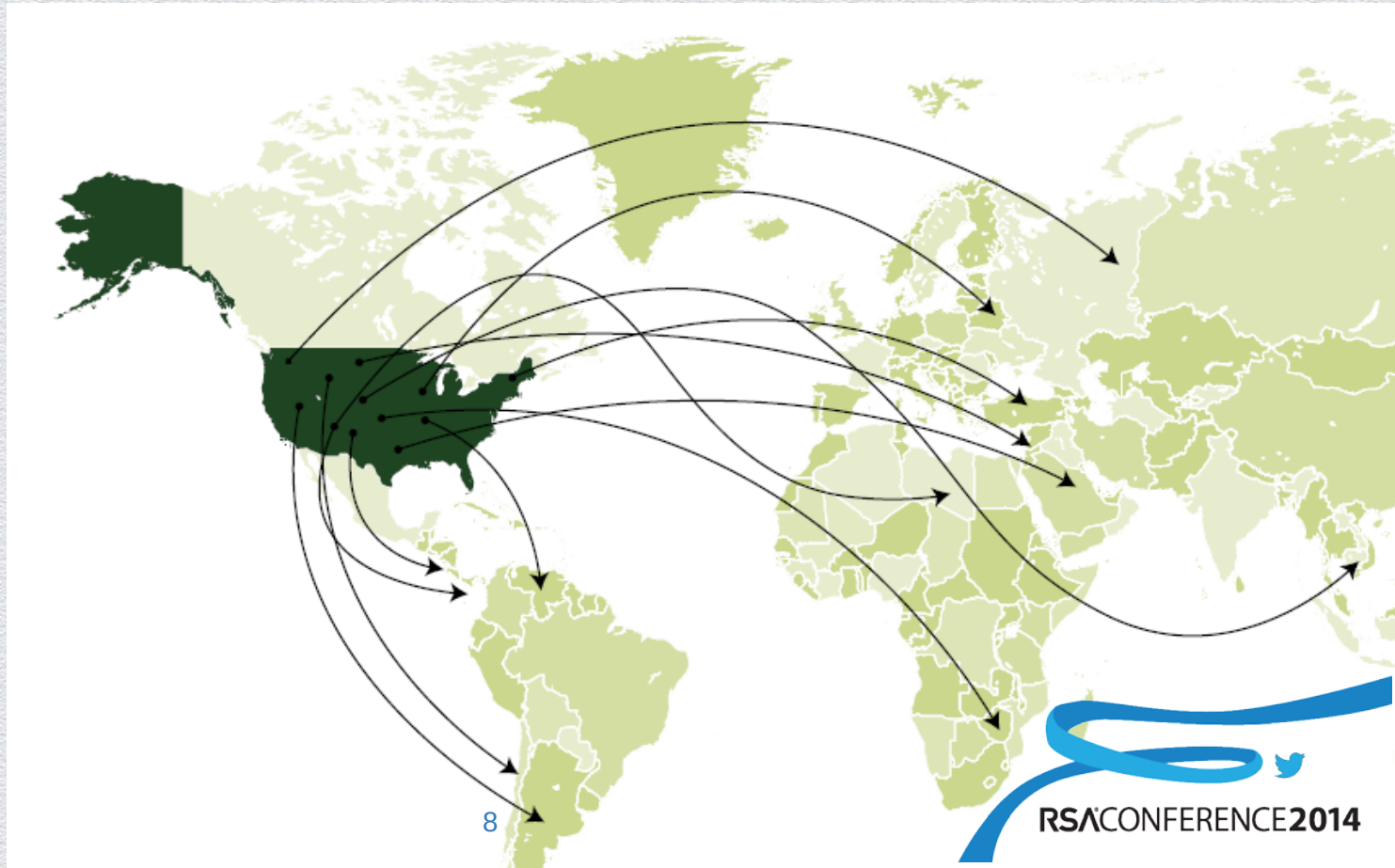
Cathal Mc Daid @mcdaidc

An example of a Local Target Campaign

- High value bank scams
- Using both national & local banks
- Local brands used in focused attacks

Cross border abuse is becoming the norm

Attacks now going to international destinations



adaptivemobile
trusted network protection

RSACONFERENCE2014

Examples of long range campaigns

Mobile Attacks linked with Hacks

- Highly organized & cross group co-operation
- Profile changes rapidly
  - From new websites
  - To hacked legitimate websites (in conjunction with PC virus)
  - To heavy Redirector usage (Short URLs)
  - To Content Delivery Networks
- From months to years in attack evolution
- Now seeing days in attack type evolution

Compromised Legitimate Sites

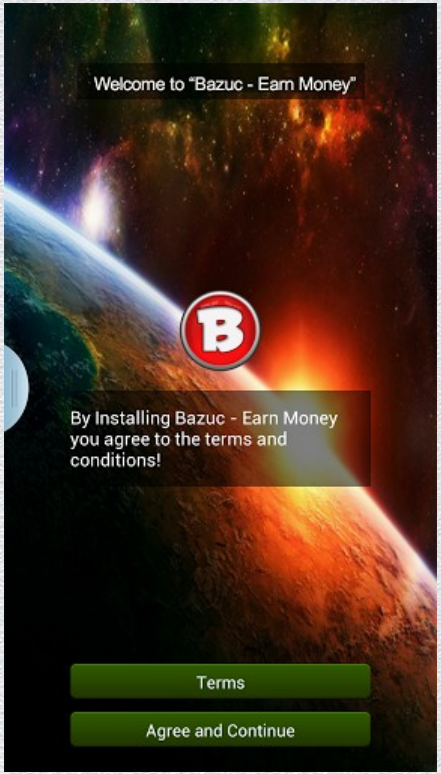
Hosted Redirect Sites

Content Delivery Networks

adaptivemobile
trusted network protection

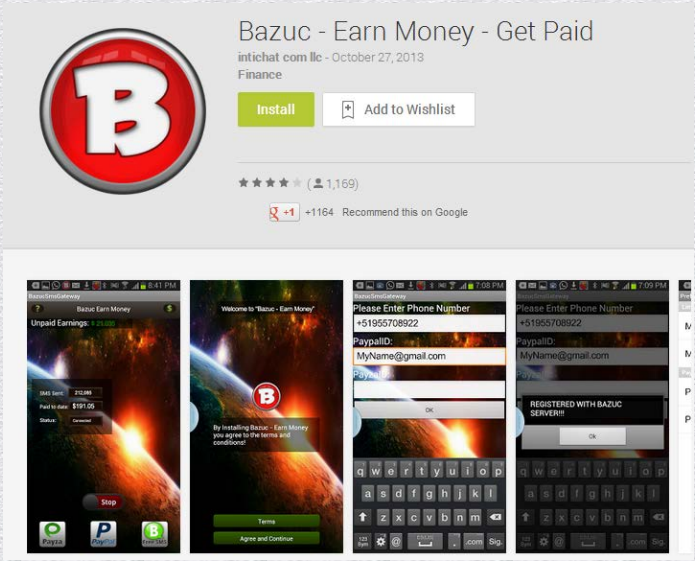
#RSAC
RSACONFERENCE2014

When App Choices affect the Stock Market



Free Android app that **earns you money** by selling your unused SMS credits that come with your monthly phone plan.

$0.001 per SMS sent from user's device



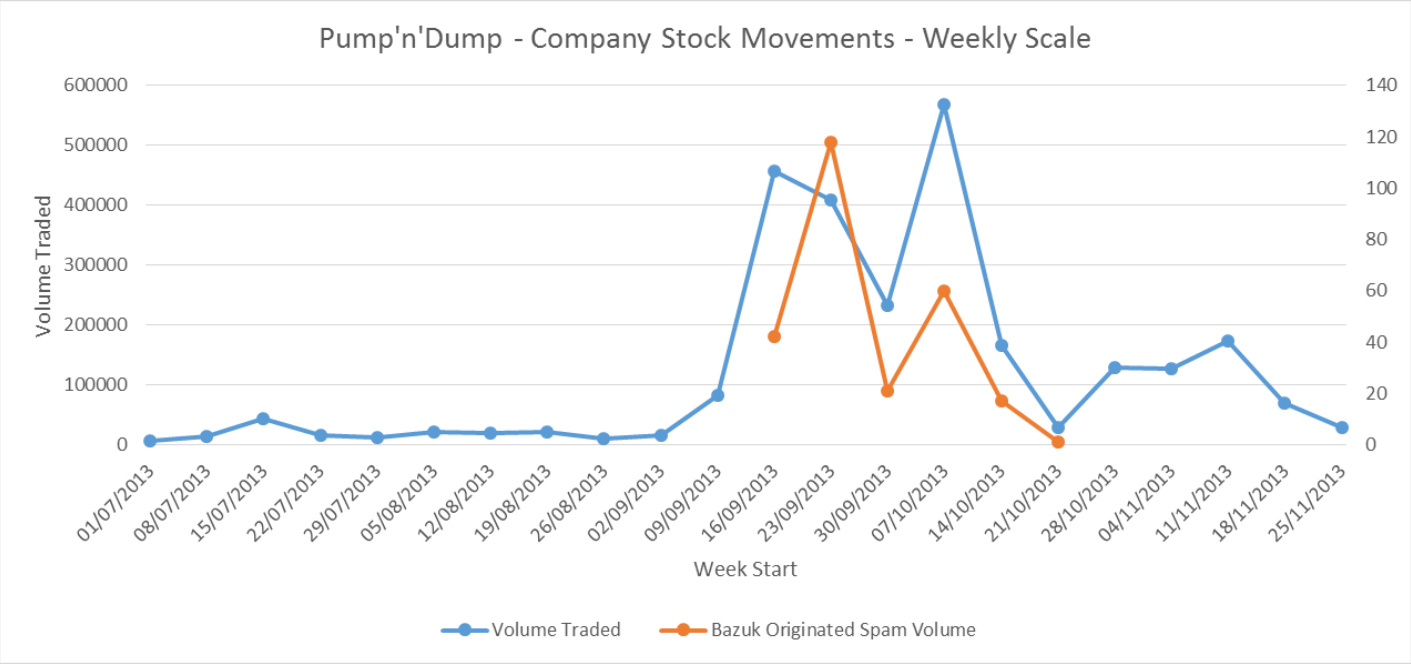
Penny Stock

Mobiles with Bazuc app installed took part in massive (~100k) **Penny Stock** spam in US

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

Geographic Spread of Bazuc-infected phones

Stock Impact



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

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

This attack has re-emerged this month

LTE Defense

- Spam & Abuse is beatable in mobile networks
- Lessons for the future for RCS/IM Messaging
- However as previous ‘safe havens’ are eliminated,
  Spammers will evolve (by accident or deliberately) to use less well defended inputs
  - **VoIP Carriers**
  - **Shortcodes**
  - **RCS**
- Think of all input points! Spammers will flow through weakest points

Thank You

SConey@AdaptiveMobile.com