

The Mobile Problem

Alex Bobotek

Co-Chairman, M³AAWG

October 2012

New Delhi, India



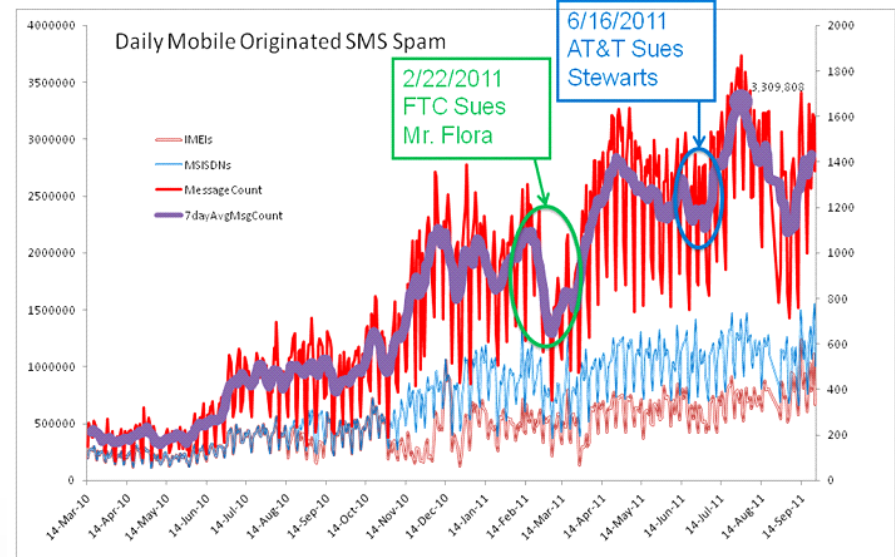
Desired Outcomes

1. Deploy “This is Spam” reporting
2. Deploy spam filters in SMS messaging
3. International collaboration
 - Enforcement
 - Abuse data exchange
 - Attend forums (M³AAWG, GSMA, ...)

History: North American SMS Spam 2010

Mobile spam and malware grew because then-current defenses couldn't break the attackers' business cases

Mobile SMS Spam Growth – 350% per year



MAAWG | maawg.org | Paris, France, October 2011

25

- **SIM Shutdown (late 2010)**

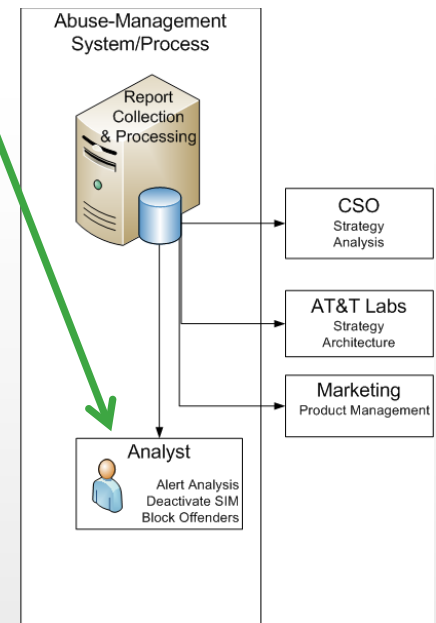
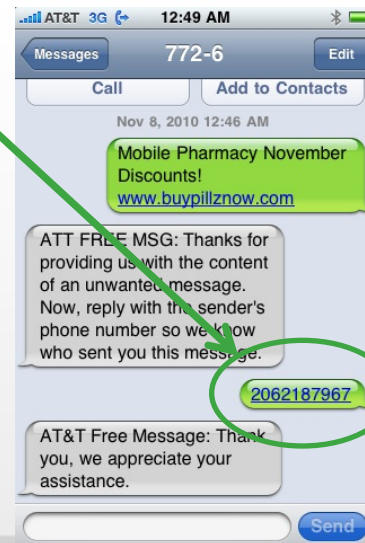
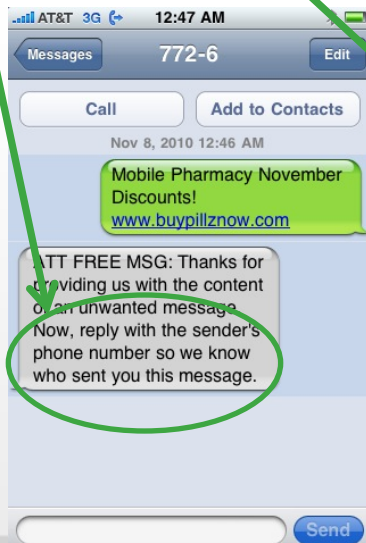
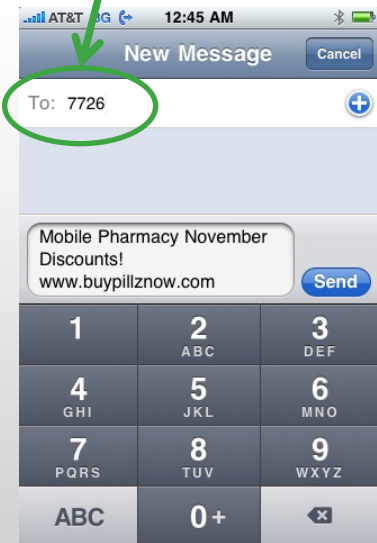
- Detect by 7726 spam reporting
- Shut down SIMs after 5-10 days
- Attacker buys new SIMs
- Spam continues

- **Lawsuits**

- Spammer sued after many months
- Spammer stops for weeks
- Spam continues

7726 Spam Reporting (North America)

- Subscriber's abuse report (example)
 1. Subscriber forwards spam to 7726 ("SPAM")
 2. 7726 system asks subscriber "who sent it?"
 3. Subscriber supplies abuser's MSISDN
- Spam management process: deactivate/block

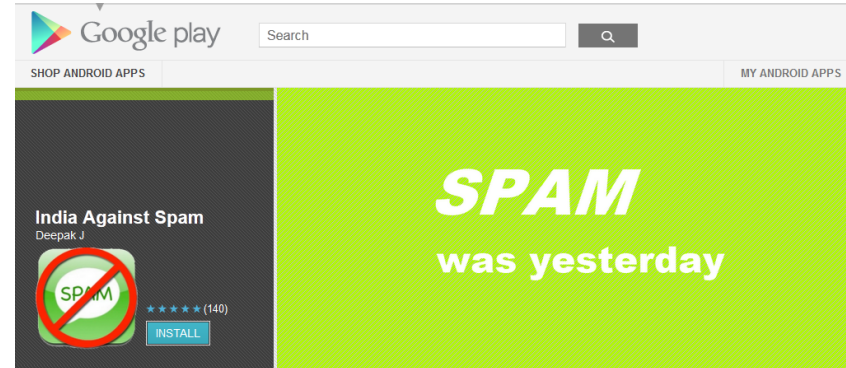


Spam Control (India)

- TRAI SMS Limits
 - 100 SMS/day (prepaid SIM)
 - 3000 SMS/month (postpaid SIM)
 - Higher if sender signs undertaking
- Opt out
 - Send “Start 0” to short code 1909
- Manual SMS spam reports to carrier
 - User sends to short code 1909
 - Format: *COMP TEL NO XXXXXXXXXXXX;dd/mm/yy;Time in hh:mm; short description of Unsolicited Commercial Communication*
 - Carrier must respond

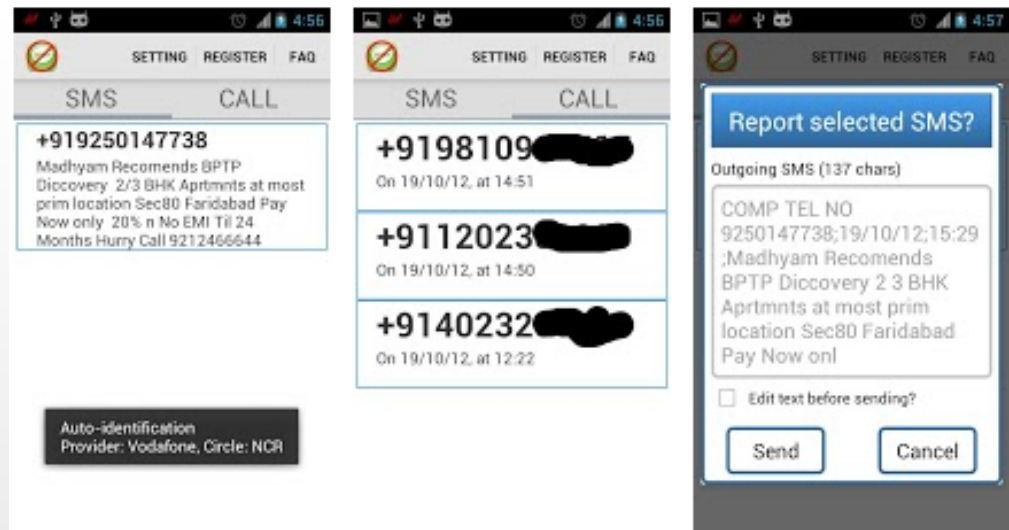
1909 Spam Reporting App

- Android app on Google play



- Automates 1909 reporting

App Screenshots



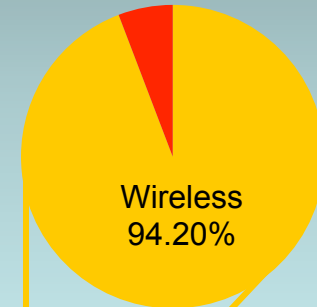
History: 2011/2012

North American Messaging Threats

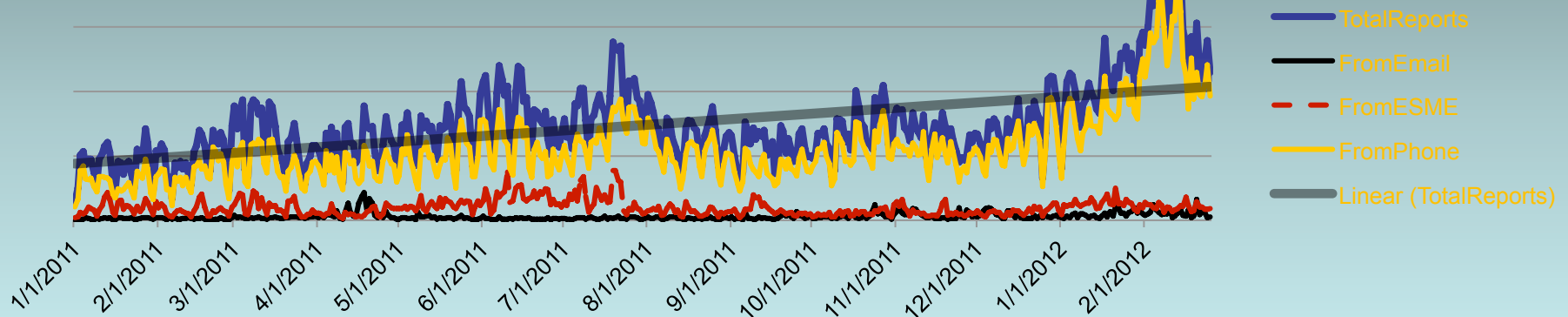
- SMS abuse growing <100%/year
- Sources
 - Mobile Phones: dominant today
 - Over The Top: significant and exploding
 - Mobile botnets/malware: significant threat
 - ESME & Email → SMS: small and controlled

Phone-Originated Spam

Over The Top
5.80%



SMS Spam Volume (daily complaints)



“Apple is looking for people to test & keep iPhone 5”

New York Times
Front Page 4/8/12

**Spam Invades
A Last Refuge,
The Cellphone**

By NICOLE PERLROTH

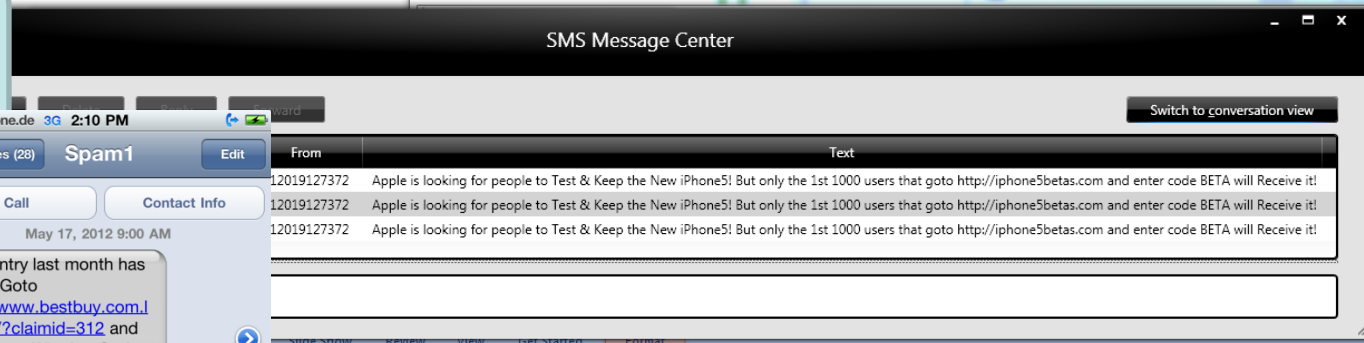
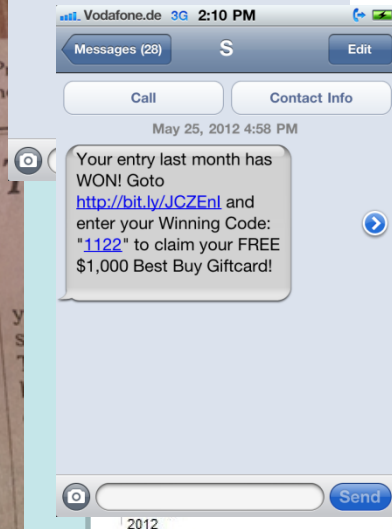
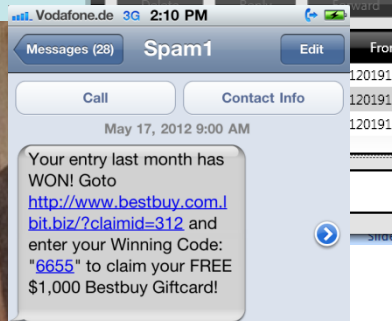
Text message spam has started waking Bob Dunnell in the middle of the night, promising cheap mortgages, credit cards and drugs. Some messages offer gift cards to, say, Walmart, if he clicks on a Web site and enters his Social Security number.

Once the scourge of e-mail providers and the Postal Service, spammers have infiltrated the last refuge of spam-free communication: cellphones. In the United States, consumers received roughly 4.5 billion spam texts last year, more than double the 2.2 billion received in 2009, according to Ferris Research, a market research firm that tracks spam.

Spread over 250 million text message-enabled phones, the problem is not as commonplace as e-mail spam. But it is a growing menace, with the potential for significant damage.

“Unsolicited text messaging is a pervasive problem,” said Christine Todaro, a lawyer with the Federal Trade Commission, the consumer watchdog agency, which is turning to the courts for

Continued on Page 4



- 300+ new SIMs/day
- Over 200,000,000 similar messages sent
- Sent from over 10,000 phone numbers



iPad/iPhone/GiftCard Scam Complaint rate

Affiliate Spam

Why SMS Spam Has Exploded

- Create an “Incredible Offer” website (often too good to be true)
 - “Free \$1000 gift card” if you sign up for these programs
 - And give us your credit card #zz
- “Affiliate” spammers advertise website and get \$1.75 for each subscriber that visits offer site

The screenshot shows the OfferVault website interface. At the top, there's a navigation bar with links like Home, Join Networks, Advertise, Webinars, Press, Help, List Your Network, and How to use OfferVault. Below this is the OfferVault logo and a featured offer for 'Weekly Training Webinars'. A search bar is prominently displayed with the text 'iphone superior' and a 'SEARCH' button. Below the search bar, there are filters for 'All Offers' and 'New Offers Only', and buttons for 'Set Country', 'Search Preferences', 'Advanced Search', and 'Reset'. A table of search results is shown below, with columns for 'N', 'D', 'KW', 'OFFER NAME', 'PAYOUT', 'TYPE', 'CATEGORY', 'NETWORK', and 'LAST UPDATE'. The table lists three offers, with the third offer, 'Get the all new iPhone 5 - Web Only', highlighted by a red box. A red arrow points from the text 'subscriber that visits offer site' in the list to this highlighted offer.

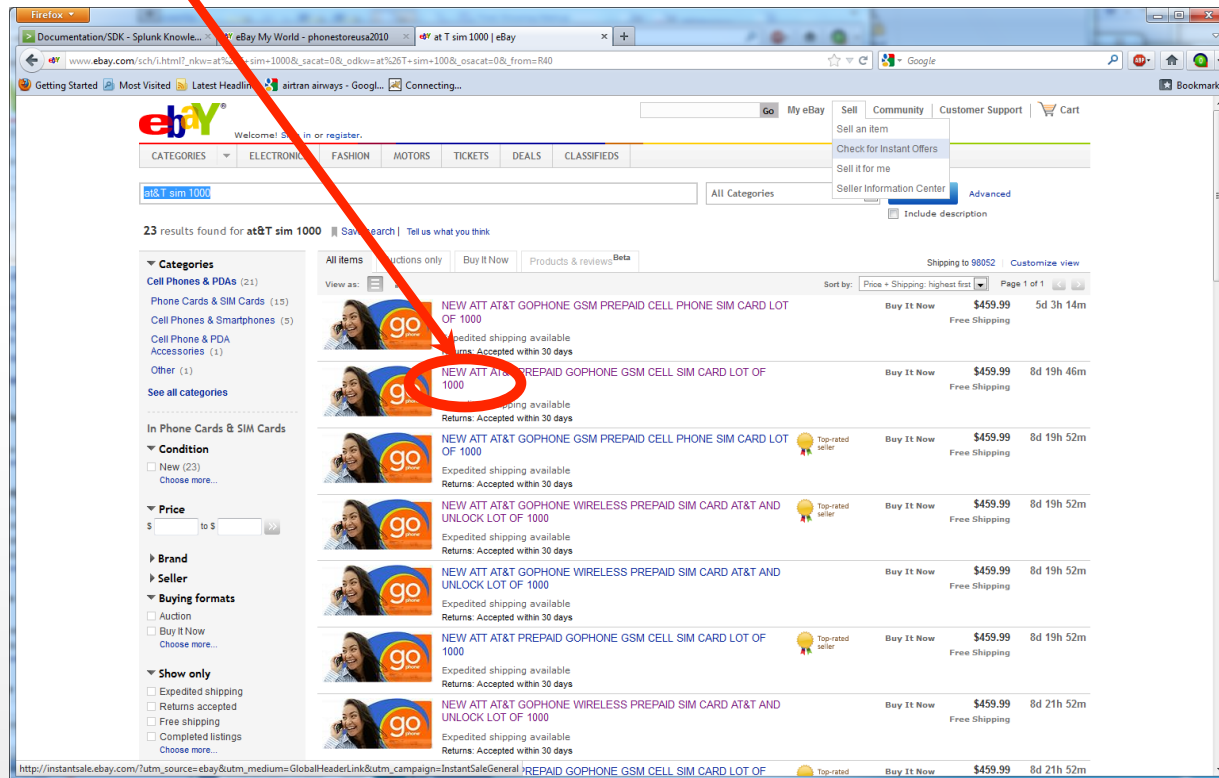
N	D	KW	OFFER NAME	PAYOUT	TYPE	CATEGORY	NETWORK	LAST UPDATE
	D	KW	Email Submit - Test and Keep the iPhone 4s + \$500 Towards Service - (PRE-POP ALLOWED) Sponsored Listing	\$ 1.65	Lead	Email / Zip Submit, Mobile, Exclusive	Superior Affiliate Management	30 Apr 2012
	D	KW	Email Submit - Test and Keep iPhone 4S Survey VER. 2 - (US Only!)	\$ 1.75	Lead	Email / Zip Submit, Mobile, Exclusive	Superior Affiliate Management	30 Apr 2012
N	D	KW	Get the all new iPhone 5 - Web Only	\$ 1.75	Lead	Email / Zip Submit, Facebook, Mobile	Superior Affiliate Management	30 Apr 2012

How Affiliates Make Mobile Spam

Boxes of cheap anonymous SIMs

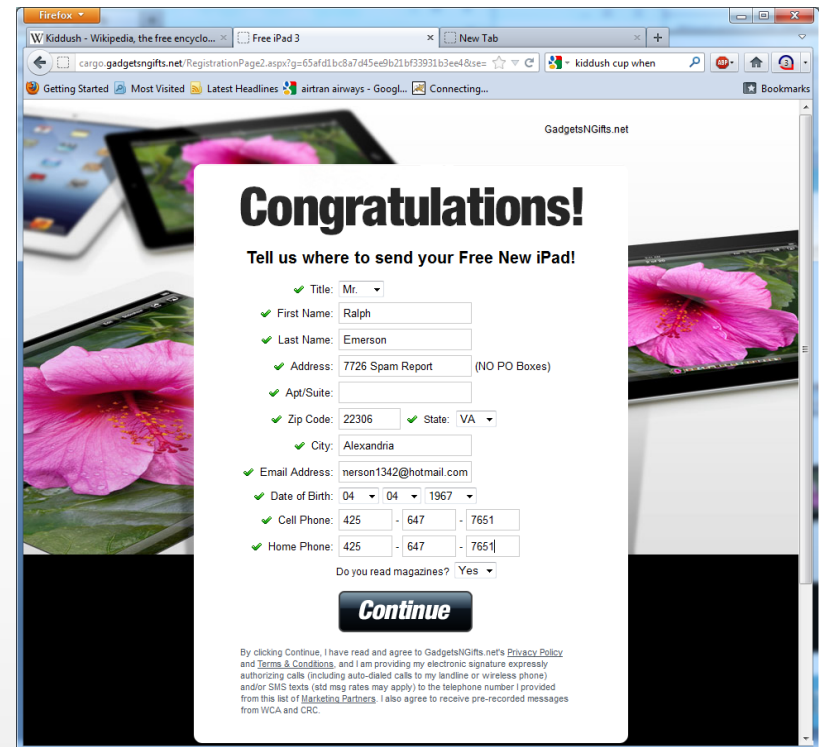
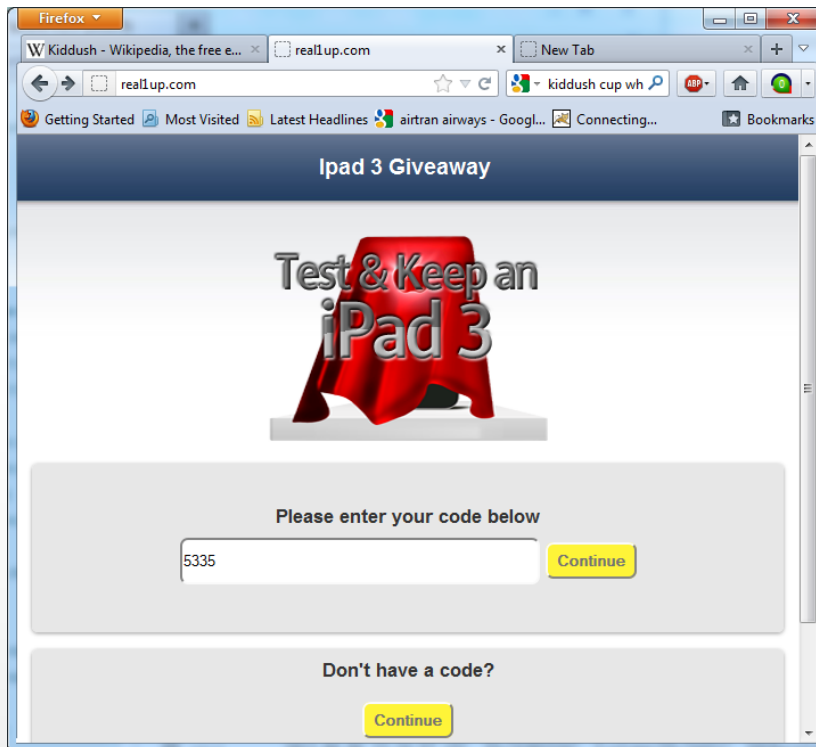
Cheap anonymous rate plan: Prepaid unlimited SMS for **\$2/day**

- Bulk SIMs - \$0.46 each on eBay
- 10, 100, 1000, 10,000, name your lot size
- Overwhelms manual shutdown defense



SMS Spam

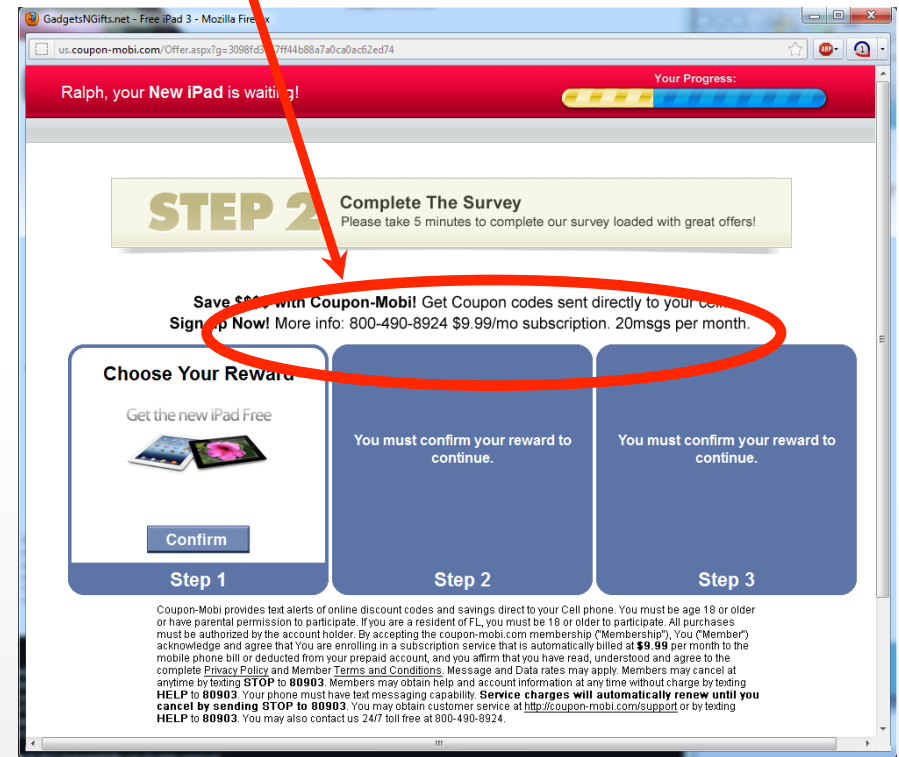
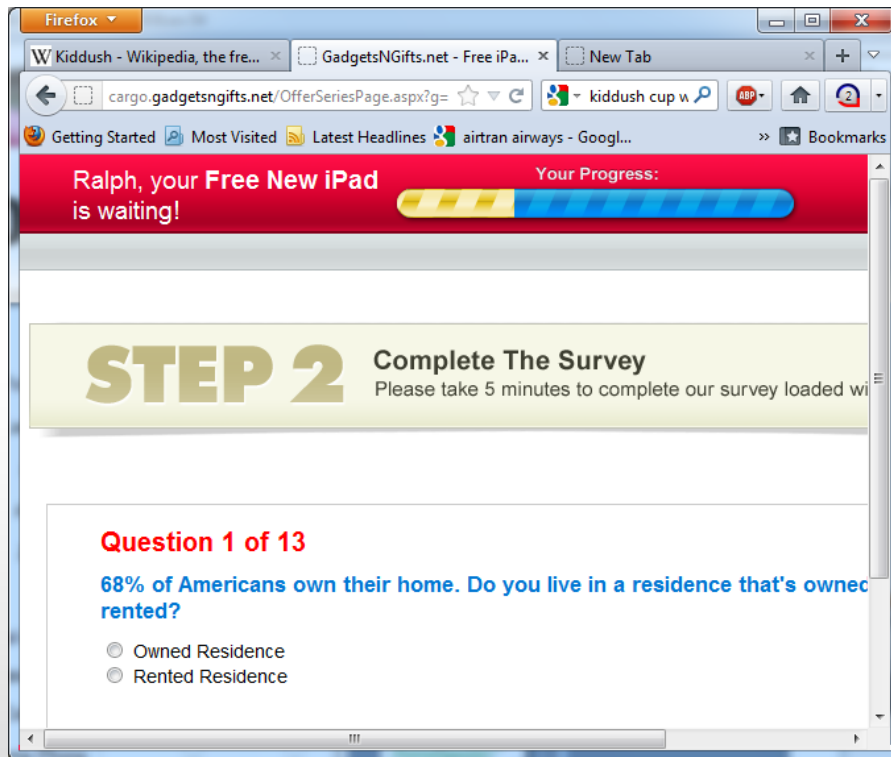
Visiting the spamvertized website ...



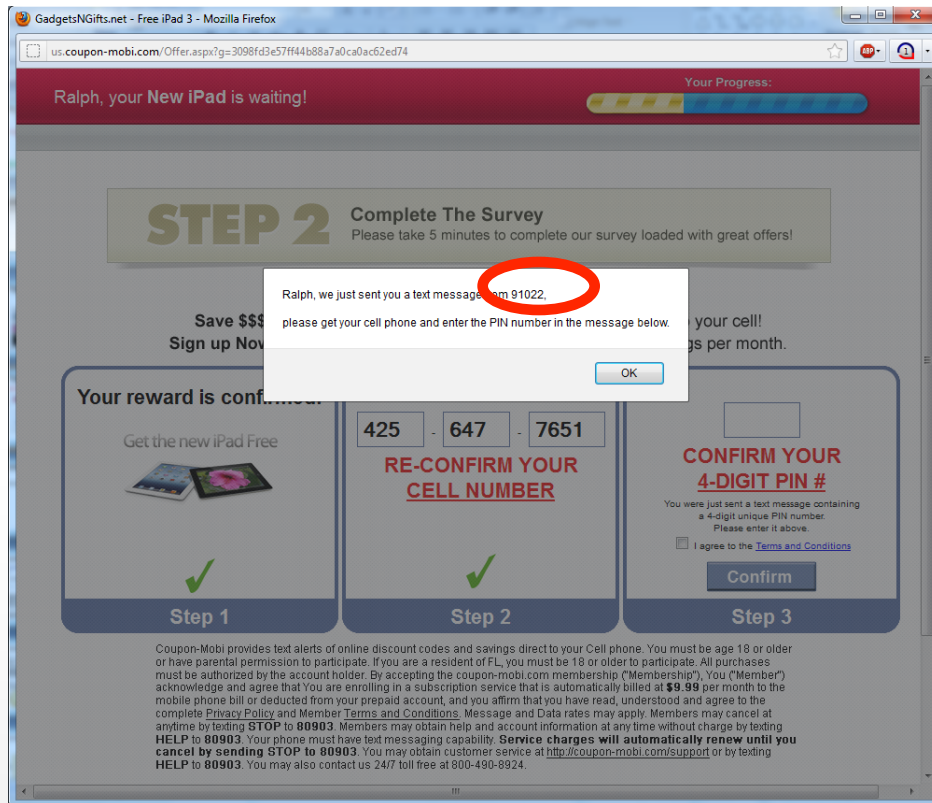
Monetization

Take a “survey” ...

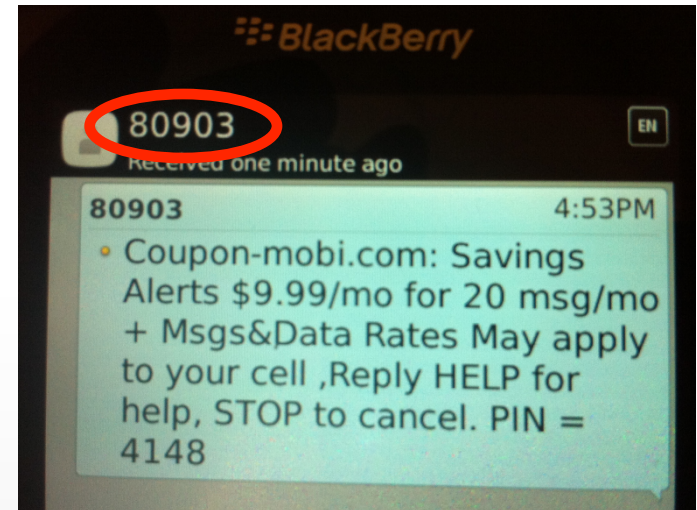
SMS monetization!



SMS Monetization



Instantly received on my Blackberry ...



Note that the short codes do not match. Was 91022 shut down?

Other Monetization

And I was soon called from . . . about diabetes, one of the Survey's question topics that I replied "yes" to

Develop a Strategy



Shutdown domain
 Shutdown server

Control bulk purchases

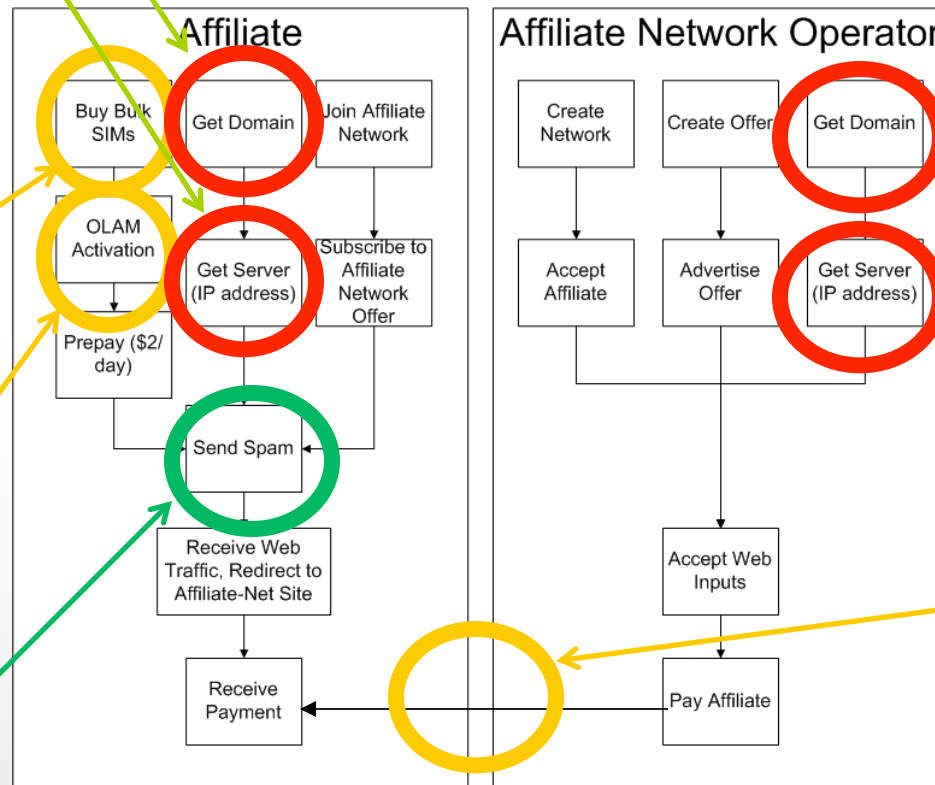
Detect bulk activation

Shutdown or block

Shutdown Domain

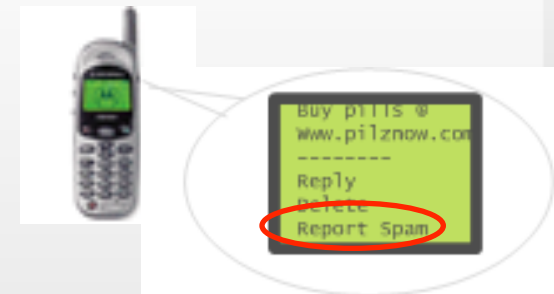
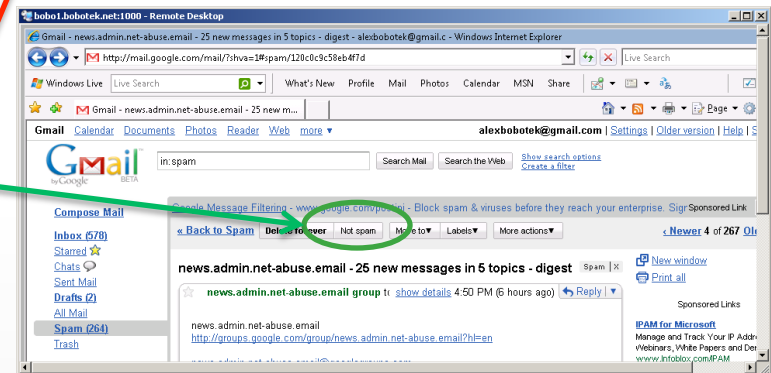
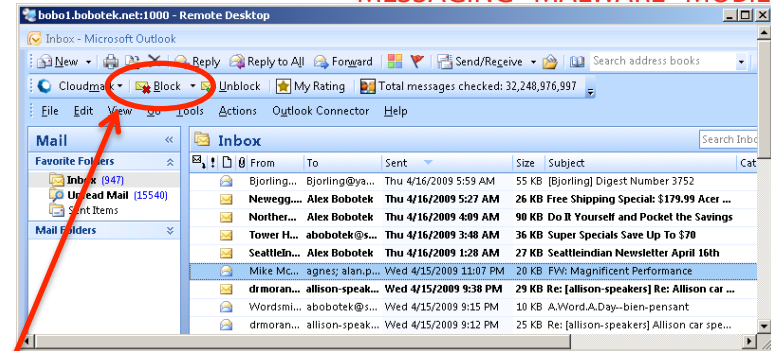
Shutdown Server

Legal Intervention



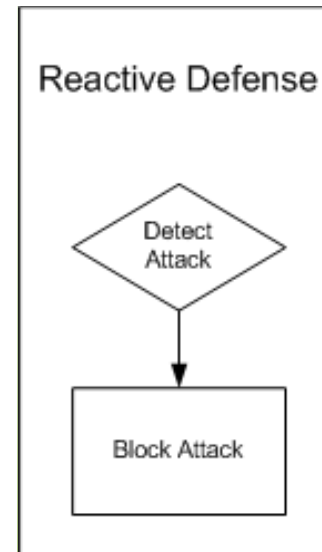
Add a “This is Spam” Button

- **7726 limitations**
 - **Without publicity, 7726 won't work**
 - If users don't know what to do, they will do nothing
 - **Body-only reporting loses envelope**
 - Timestamps lost
 - Source and routing information lost
- Typical email user agents have “This is Spam” and “Not Spam” buttons
- A standard ‘Report Spam’ button
 - Use OMA Standard “SpamRep”
 - SpamRep standard completed



Filter Defense (takes time/resource)

- Deploy spam/virus filters
- Build better spam reporting
 - “This is Spam” button in UA
- **Abuse detection - the human brain**
 - Ideally nimble, adaptable abuse detector
 - Stochastic - error rate of ~ 1%
 - Often off-duty
 - Occasionally malign

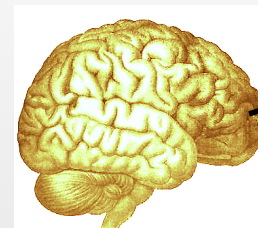


Layered Defense Architecture

Reputation filters

Volumetric filters

Content filters



This is spam

Account-Level Defense: Detect and Block

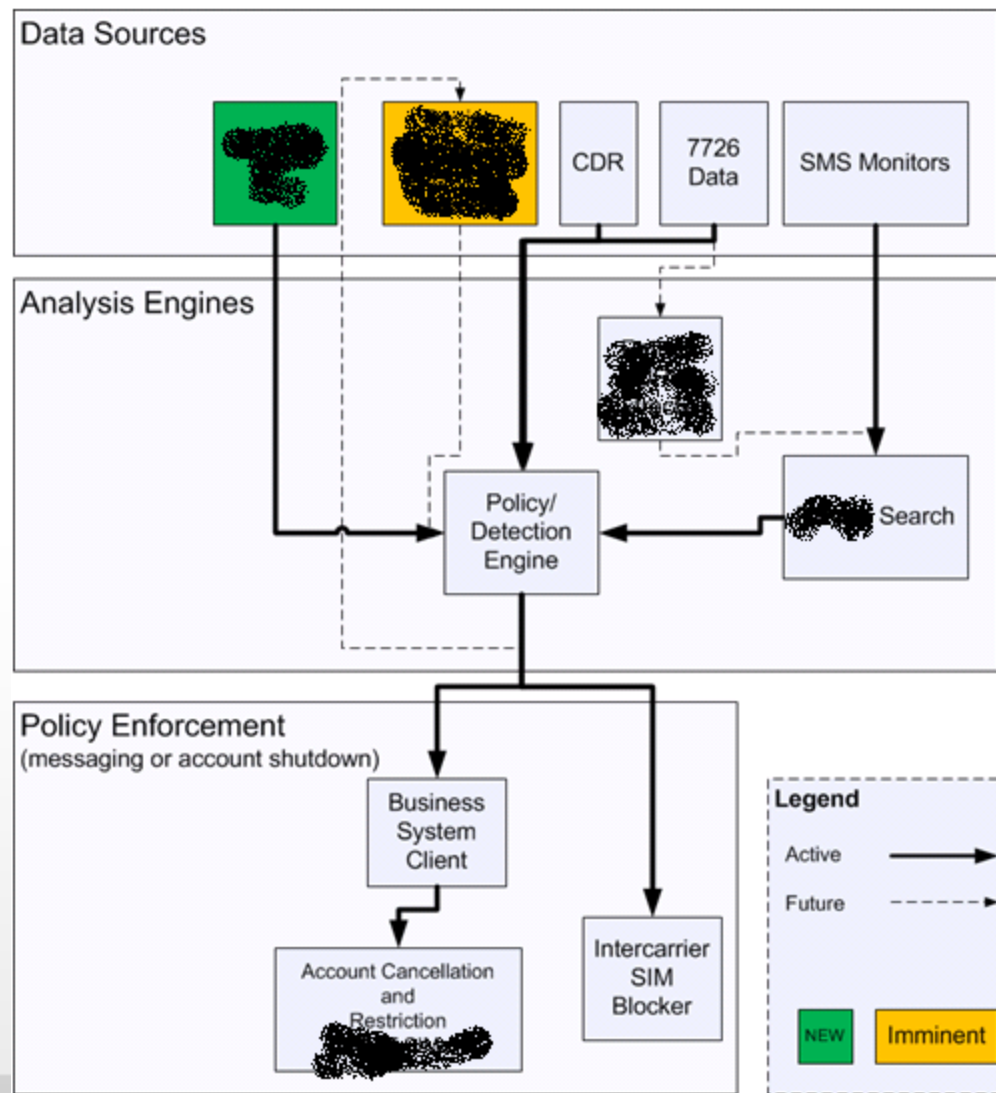
- Goal: minimize attackers' cost (msg/\$)

Detection

- By subscriber reports
- By message rate/volume
- By message content
- Exchange reports with other MNOs

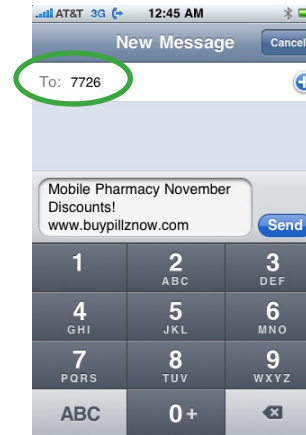
Whack SIMs

- Automated shutdown

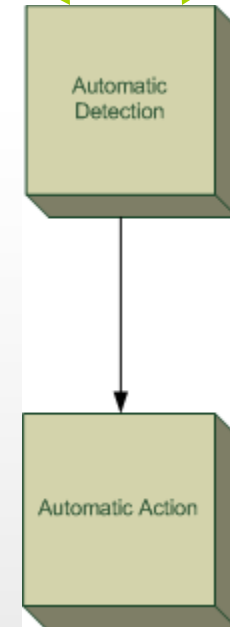


Short Term Defense

- Legal action
- Block mass SIM purchases
- Buy SIMs
- Collaborate with other MNOs
- Automated shutdown
 - Detect abusing SIMs via
 - 7726 spam complaints
 - Call data records
 - Sale fingerprint (e.g., name/address/seller on account)
 - Activation fingerprint (e.g., IP address, other forensics)
 - Shutdown
 - Disable SMS/MMS origination in HLR
 - Deprovision SIMs
 - Block intercarrier senders in intercarrier gateway



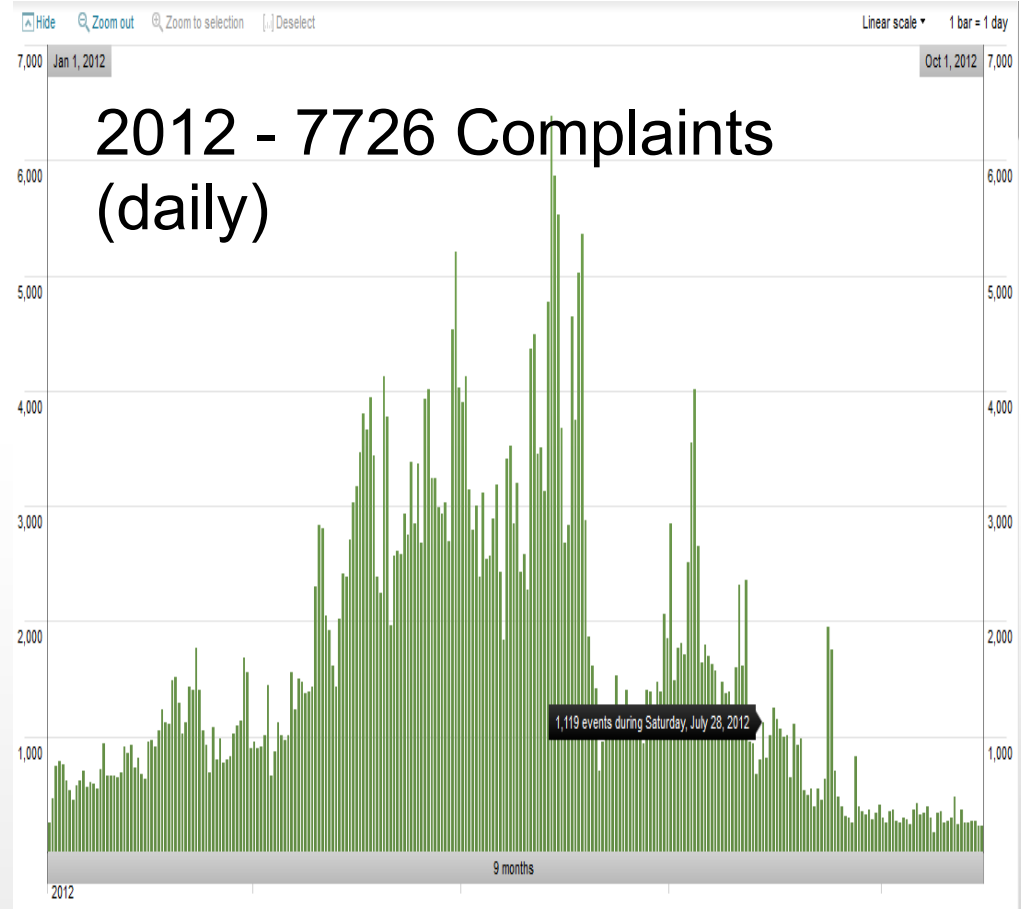
Call Data Records



US Domestic Spam Status

Now Under Control: iPhone/iPad/Gift Card Spam

- Spam termination below pre-storm levels
- Improved defense is responsible
 - Automatic detection & shutdown
 - Improved 7726 reporting
 - Bulk SIM availability/cost
 - Reseller control
 - Manual backup (Fraud)
- 7726 Reporting ratio improvement
1 complaint per X spam messages (9/20)
Y x September 2011 rate
- Cautions:
 - **Spammers will return with new methods**
 - **Spoofing**
 - **Malware (Bots)**
 - » China has active mobile botnet of > 100k phones
 - » GGtracker malware infected > 250k US phones



Problems

- Growing abuse
 - Spam
 - Malware
 - Fraud
 - Harassment
 - Network disruption
- Growing internationalization of abuse and global homogenization of abuse technologies
 - Toolkits
 - Criminal economy
 - Intra-carrier sensors (e.g., SRS) are effective against attacks which include intra-carrier targets
 - Oceans do not separate PC malware-based technology (e.g., kits that focus on specific exploits)

We're fighting a growing and increasingly similar and mobile spam problem across continents and oceans

USA IP Address

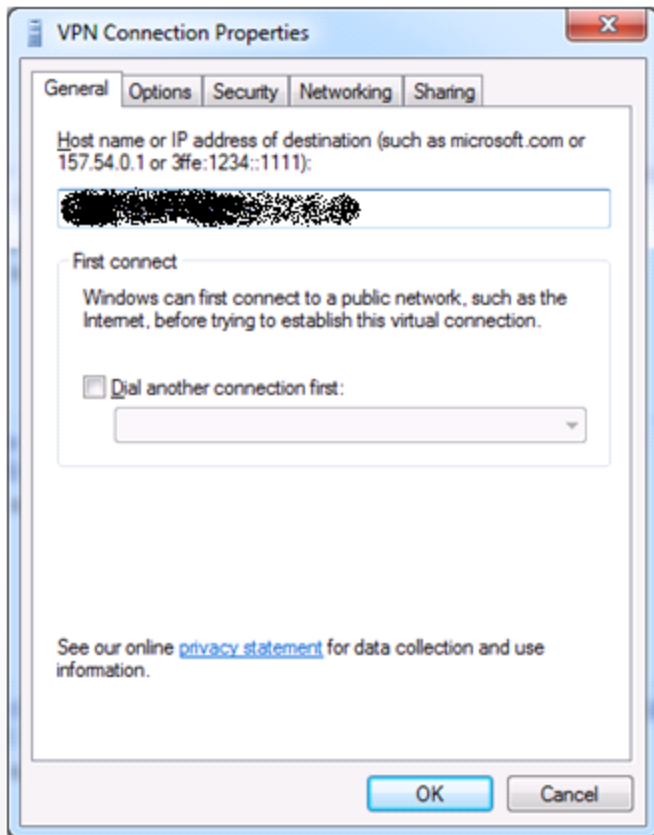
The screenshot displays a Firefox browser window with a network log at the top and a Best Buy promotional page below. The network log shows the following requests:

- 00:23:50.537 POST http://www.bestbuy.com.bstz.biz/claim.php [HTTP/1.1 200 OK 137ms]
- 00:23:52.137 GET http://i.cj2000.org/aff_c?offer_id=3854&aff_id=2548 [undefined 53ms]
- 00:23:52.197 GET http://i.cj2000.org/aff_c?offer_id=3854&aff_id=2548 [HTTP/1.1 302 Found 240ms]
- 00:23:52.492 POST http://www.bestbuy.com.bstz.biz/claim.php [HTTP/1.1 200 OK 63ms]
- 00:23:52.519 GET http://jmp.realtraq.net/aff_c?offer_id=3854&aff_id=2548 [HTTP/1.1 302 Found 217ms]
- 00:23:52.766 GET http://jmp.realtraq.net/aff_r?offer_id=3854&aff_id=2548&826c2%3D%26c3%3D1022d594d34eeef6367a5dc65825246 [HTTP/1.1 200 OK 42ms]
- 00:23:52.906 GET http://jmp.realtraq.net/aff_r?offer_id=3854&aff_id=2548&826c2%3D%26c3%3D1022d594d34eeef6367a5dc65825246 [HTTP/1.1 302 Found 42ms]
- 00:23:52.960 GET http://affiliate.abltrk.com/rd/r.php?sid=20&pu...c1=2548&c2=8c3=1022d594d34eeef6367a5dc65825246 [HTTP/1.1 302 Found 305ms]
- 00:23:53.318 GET http://hp.squareclk.com/183/sr?_qse=awRfCD0xN.9674638&spid=260055&sub=2548&progid=20&pre_q=0 [HTTP/1.1 302 Found 286ms]
- 00:23:53.632 GET http://bestbuy.thetopoffers4u.com/?t_id=QvCEUX8.0&email=&exit_p=&creative=&id_p=1525706&oon=183 [HTTP/1.1 200 OK 337ms]
- 00:23:53.967 GET http://bestbuy.thetopoffers4u.com/assets/validate.min.js [HTTP/1.1 200 OK 293ms]
- 00:23:54.315 GET http://bestbuy.thetopoffers4u.com/assets/continue.gif [HTTP/1.1 200 OK 202ms]
- 00:23:54.342 GET http://bestbuy.thetopoffers4u.com/assets/bodyBG.jpg [HTTP/1.1 200 OK 525ms]

The main content of the page is a promotional banner for a Best Buy gift card. It features a woman in a Best Buy uniform, a Samsung monitor, a camera, and a smartphone. The text reads: "GET A FREE \$1000 BEST BUY GIFT CARD" and "Participation Required, Click for Details". Below the banner is a form with the heading "Please complete the following steps:" and "1. Enter Your E-mail Address:". There is an input field for the email address and a green "Continue" button. An "Inspect Network Request" window is open over the URL: "http://jmp.realtraq.net/aff_r?offer_id=3854&aff_id=2548&redirect...%2Faffiliate.abltrk.com%2Frd%2Fr.php%3Fsid%3D20%26pub%3I...%3D%26c3%3D1022d594d34eeef6367a5dc65825246".

This Gift Redemption Program is an independent rewards program for consumers and is not affiliated with, sponsored by or endorsed by any of the listed products or retailers. Trademarks, service marks, logos, and/or domain names (including, without limitation, the individual names of products and retailers) are the property of their respective owners.
THE FOLLOWING IS A SUMMARY OF PROGRAM REQUIREMENTS. SEE TERMS & CONDITIONS FOR COMPLETE DETAILS. Members are being accepted subject to the following Program Requirements: 1) Must be a legal US resident; 2) must be at least 18 years old or older; 3) must have a valid email and shipping address; 4) Eligible members can receive the incentive gift package by completing two reward offers from each of the Silver and Gold reward offer page options and nine reward offers from the Platinum reward offer page options and refer 3 friends to do the same. Various types of reward offers are available. Completion of reward offers most often requires a purchase or filing a credit application and being accepted for a financial product such as a credit card or consumer loan. The following link illustrates a Representative Sample of reward offers by group along with monetary and non-monetary obligations. Failure to submit accurate registration information will result in loss of

Internationalization – Netherlands IP



The image shows a Firefox browser window with a network log and an advertisement. The network log displays various HTTP requests and responses, including GET requests for CSS files, JavaScript files, and images, as well as POST requests to a claim.php endpoint. The advertisement is titled "Neem een abonnement op onderstaande games en" and features a "WIN de nieuwe iPad!" promotion. The promotion asks the user to answer the question "Wie is de nieuwe CEO van Apple?" with two options: "Hitaka Mishamo" and "Tim Cook". Below the promotion is a grid of game covers, including "vampire lover", "RALLY 3D", and "T20".

Internationalization – Paris IP Address

The screenshot displays a Firefox browser window with a network log and a webpage. The network log shows various HTTP requests and responses, including GET requests for images and scripts. The webpage content includes a quiz question: "2. Quel est le chiffre qui doit suivre dans cette série ? 3, 5, 8, 13, 21,....." with radio button options 4, 21, and 34. A "Continuer >>>" button is visible at the bottom.

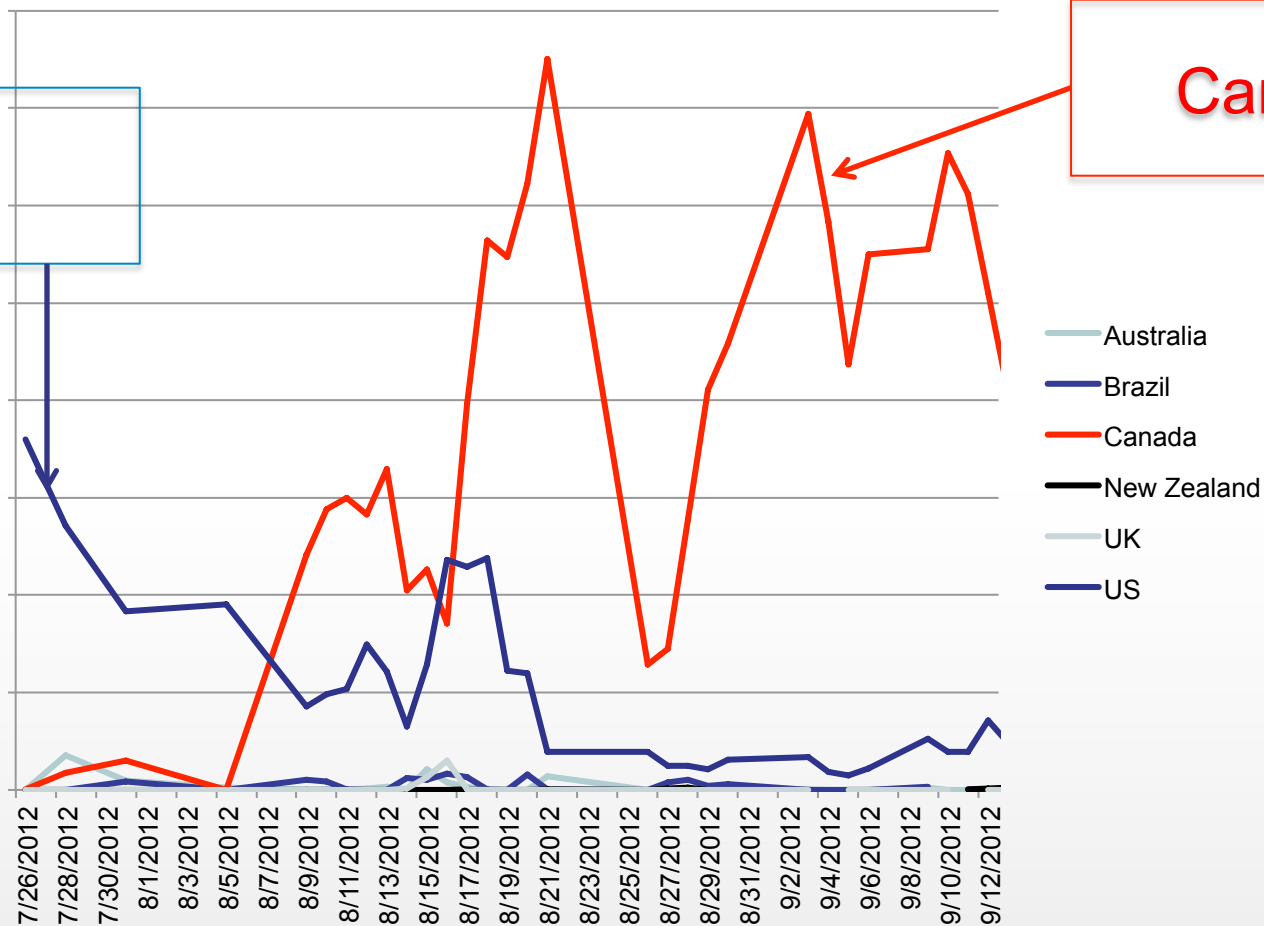
Internationalization - Germany

The screenshot shows a Firefox browser window with two tabs: 'Search - SRS - Splunk 4.3.1' and 'momentality.net'. The address bar shows the URL 'domains.google syndication.com/apps/domainpark/domainpark.cgi?ref=&output=html&cli'. The network log displays various HTTP requests and responses, including GET and POST requests to various domains like bestbuy.com, jmp.realtraq.net, and internet-examine.com. A warning message is visible: 'An unbalanced tree was written using document.write() causing data from the network to be reparsed. For more information https://developer.mozilla.org/en/Optimizing_Your_Pages_for_Speculative_Parsing'. The main content area shows the 'momentality.net' logo and a copyright notice: '© 2011 All rights reserved. Privacy'. The status bar at the bottom indicates 'Blocked: 1 of 1'.

New Spam Plan: Spam Canada Instead

US

Canada



A Framework for Abuse Data Exchange

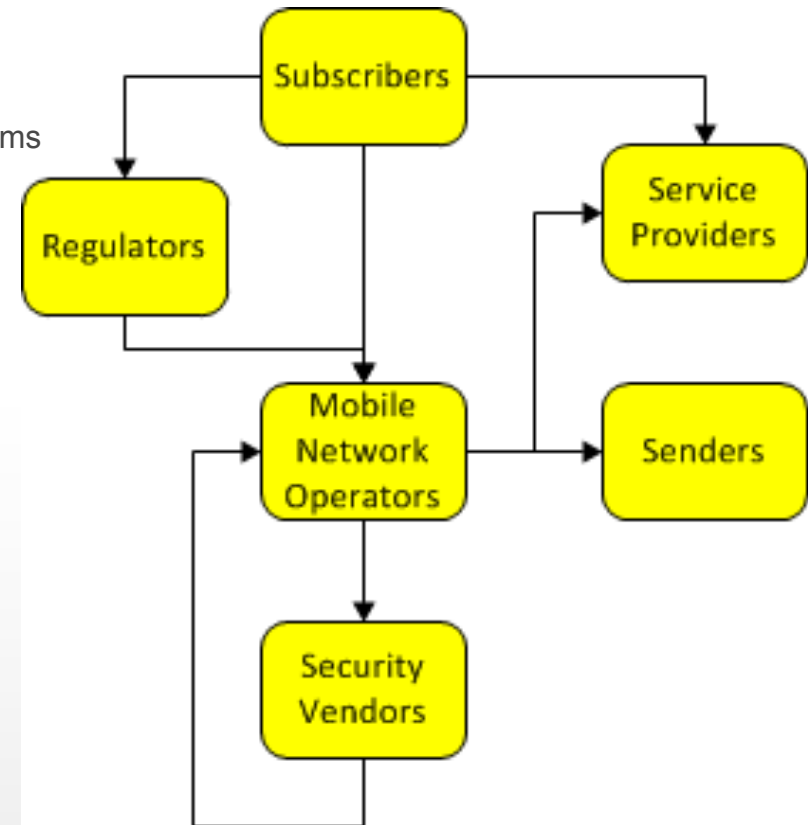
- Political boundaries are exploited by attackers
 - IF **OUR** SUBSCRIBERS DON'T COMPLAIN, CAN WE STOP IT?
- Defense requires coordination
 - Sensing abuse
 - Tracing to source
 - Acting at source
- Technical Framework
- Policy/Legal Framework
 - Privacy and access constraints
 - Must support multiple nations' laws
- Business framework
 - Getting parties to contribute data
 - Who pays?
 - Collaboration forums



Abuse Data and Data Flows

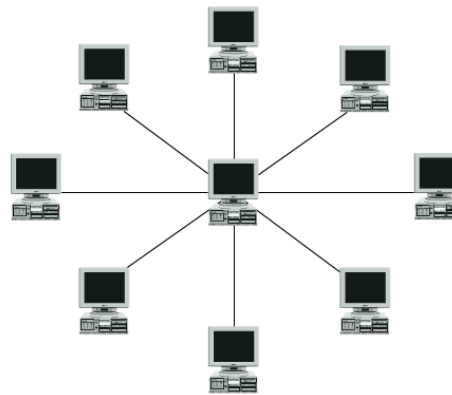
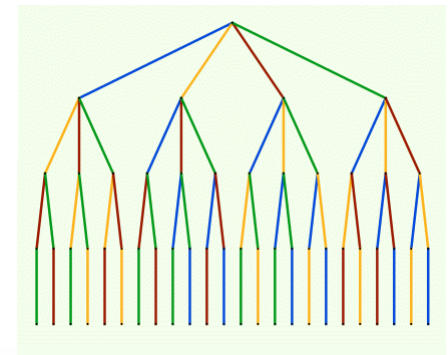
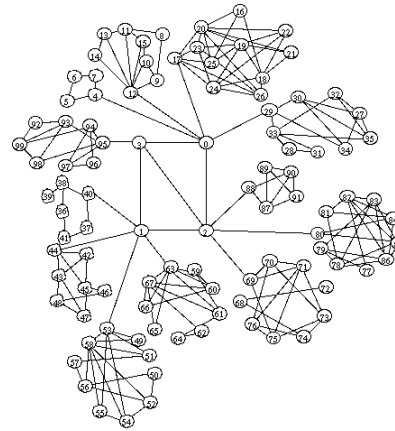
- Some typical abuse ecosystem endpoints/ flows
 - Subscriber → MNO (manual spam reports)
 - MNO “A” → MNO “B”
 - MNO → Vendor
 - Vendor → MNO
 - Messaging Network Element → Business (provisioning) Systems
 - → Researcher
 - → Regulator
 - Regulator → MNO

- Typical semantics
 - “I got spammed”
 - “High rate”
 - Botnet C&C traffic report
 - Passive DNS
 - “<MSISDN> is a spammer” assertions



Data Flow Topology

- 600+ MNOs on planet Earth
- Hundreds of government agencies
- Vendors
- Senders
- Service providers



Do we want $\frac{n*(n-1)}{2}$ bilateral data sharing agreements?

Needed: A Framework for Abuse Data Exchange

- **Technical Framework elements include:**

- Data format specifications
- Data transport protocol specifications
- Software libraries
- Software tools
- Host systems
- Information repositories
- Data access controls

- M³AAWG and GSMA can make this happen
- Your participation is needed

- **Legal Framework**

- Privacy and access constraints
- Must support multiple nations' laws and data-contributors' constraints

- **Business framework**

- Getting parties to participate by contributing data
- Solve important problems
- Provide good ROI: low costs/high value
- Who pays?
- Data access policies
- Collaboration forums

Mitigating Abuse: The Solution is Multifaceted



- Automated technical defense
 - “This is Spam” SpamRep standard reporting
 - Network Spam filters
- Attend forums: Collaboration/education in defense
- Abuse (spam) data exchange