M3AAWG
MESSAGING MALWARE MOBILE

The Mobile Problem

Alex Bobotek
Co-Chairman, M3AAWG
October 2012
New Delhi, India

Desired Outcomes

M3AAWG
MESSAGING MALWARE MOBILE

1. Deploy “This is Spam” reporting

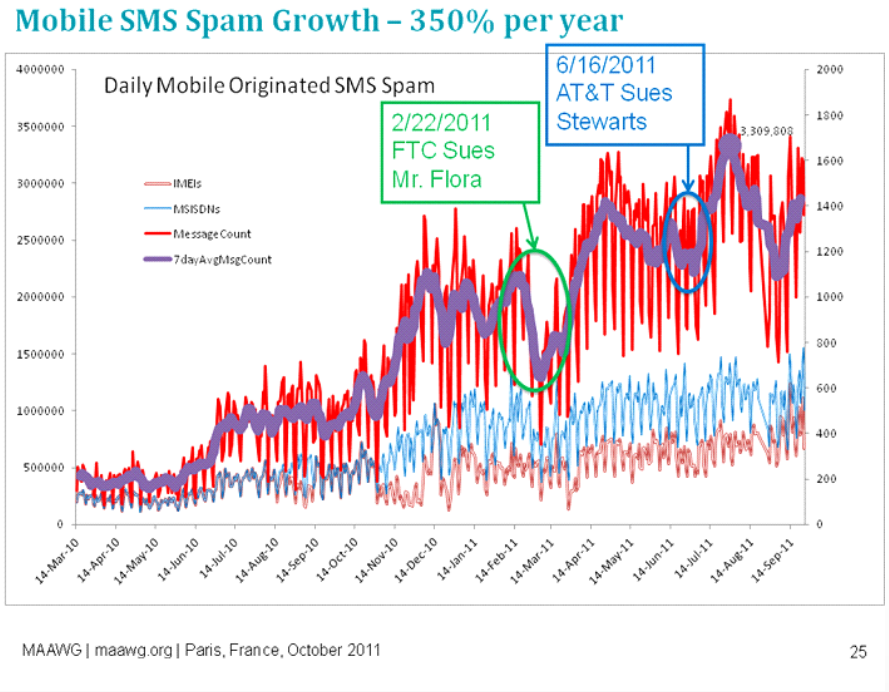
2. Deploy spam filters in SMS messaging

3. International collaboration
   - Enforcement
   - Abuse data exchange
   - Attend forums (M3AAWG, GSMA, …)

History: North American SMS Spam 2010

M3AAWG
MESSAGING MALWARE MOBILE

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



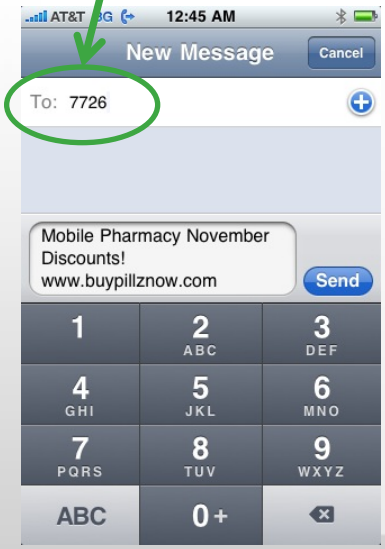
MAAWG | maawg.org | Paris, France, October 2011 25

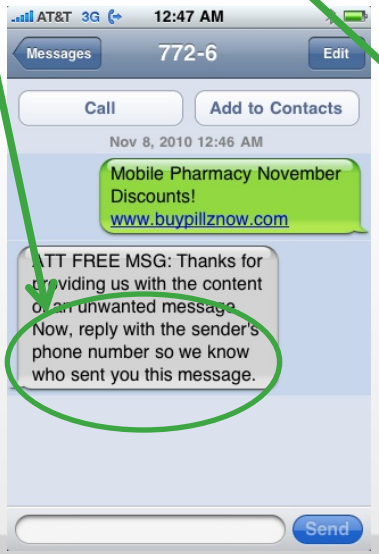
- **SIM Shutdown (late 2010)**
  - Detect by 7726 spam reporting
  - Shut down SIMs after 5-10 days
  - Attacker buys new SIMs
  - Spam continues
- **Lawsuits**
  - Spammer sued after many months
  - Spammer stops for weeks
  - Spam continues

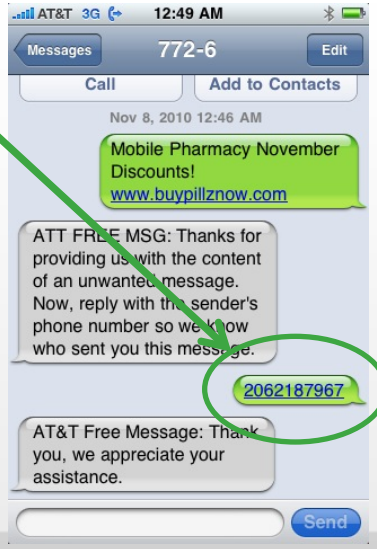
7726 Spam Reporting (North America)

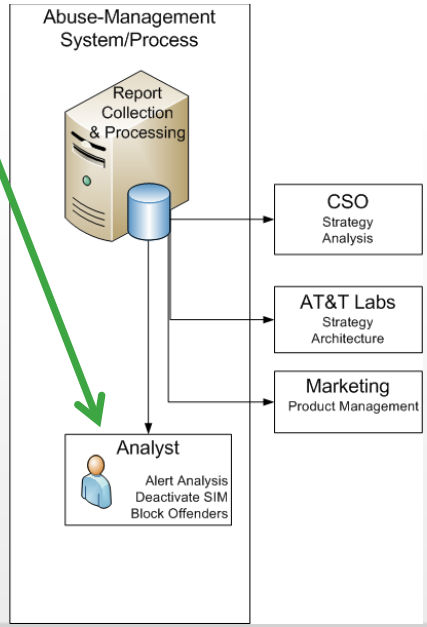
- Subscriber's abuse report (example)
  1. Subscriber forwards spam to 7726 ("SPAM")
  2. 7726 system asks subscriber "who sent it?"
  3. Subscriber supplies abuser's MSISDN

- Spam management process: deactivate/block







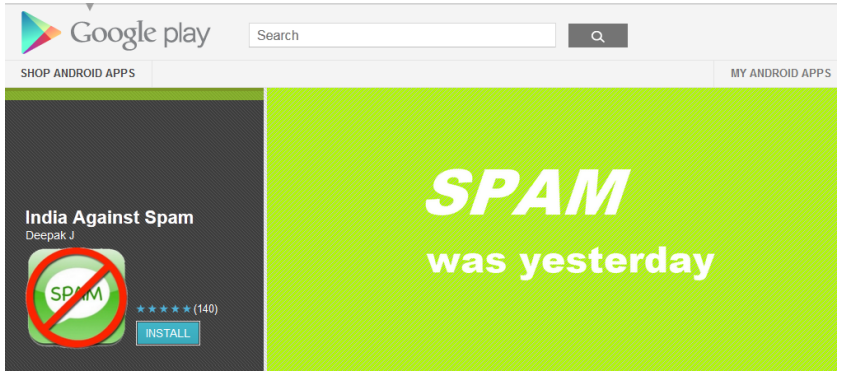


Spam Control (India)

- 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 XXXXXXXXXX;dd/mm/yy;Time in hh:mm; short description of Unsolicited Commercial Communication***
  - Carrier must respond

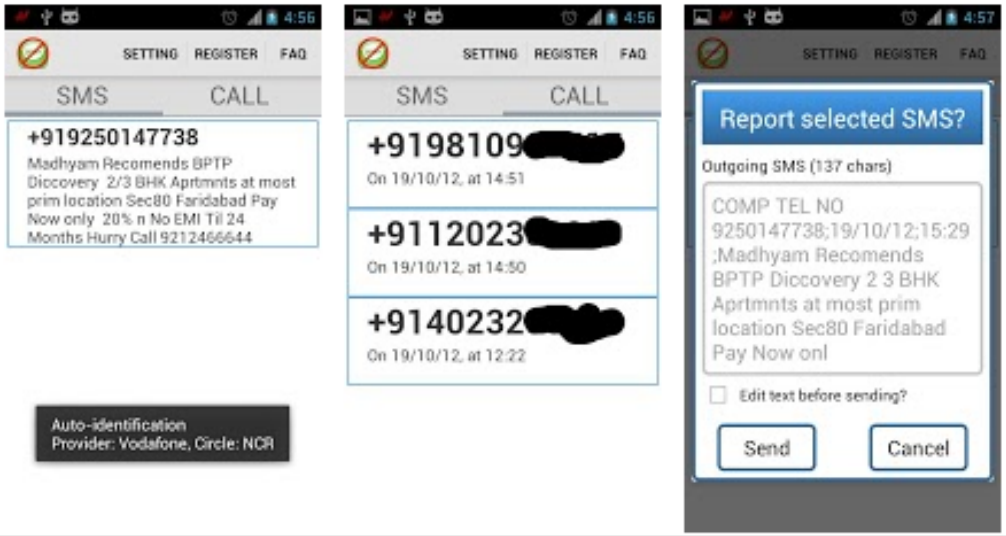
1909 Spam Reporting App

- Android app on Google play



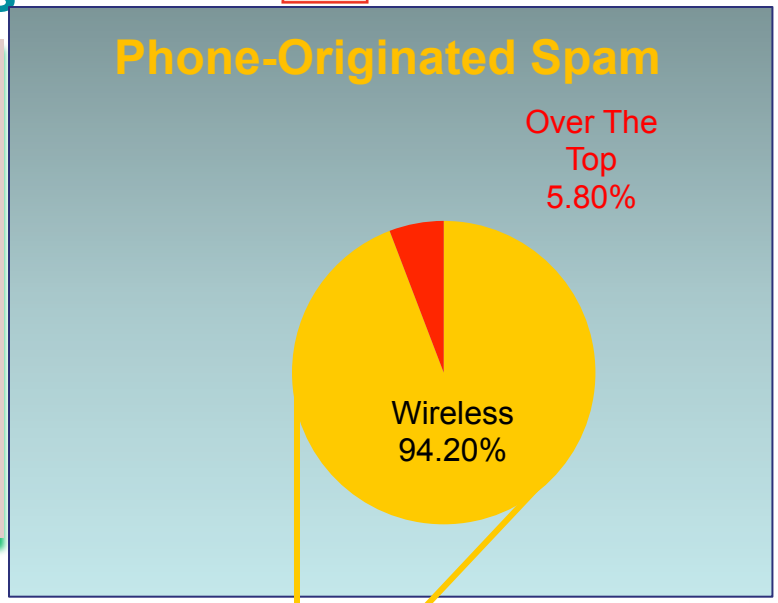
- Automates 1909 reporting

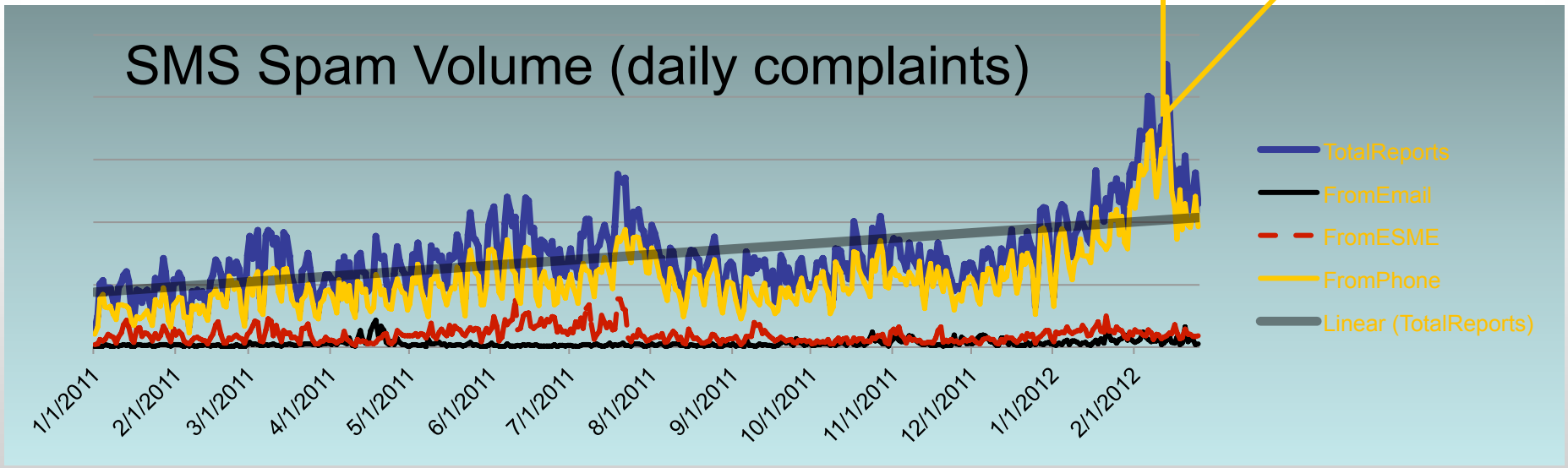
App Screenshots



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





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

M3AAWG
MESSAGING MALWARE MOBILE

New York Times Front Page 4/8/12

Spam Invades A Last Refuge, The Cellphone

By NICOLE PERLROTH

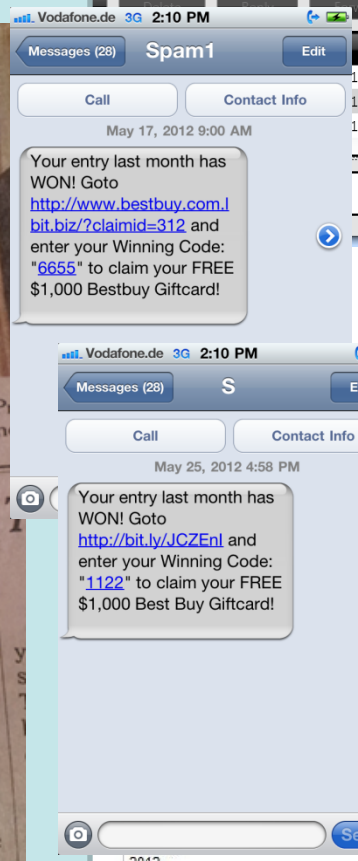
Text message spam has started waking Bob Dunnell in the middle of the night, promising cheap mortgages, credit cards and drugs. Some messages offer gift cards to, say, Walmart, if he clicks on a Web site and enters his Social Security number.

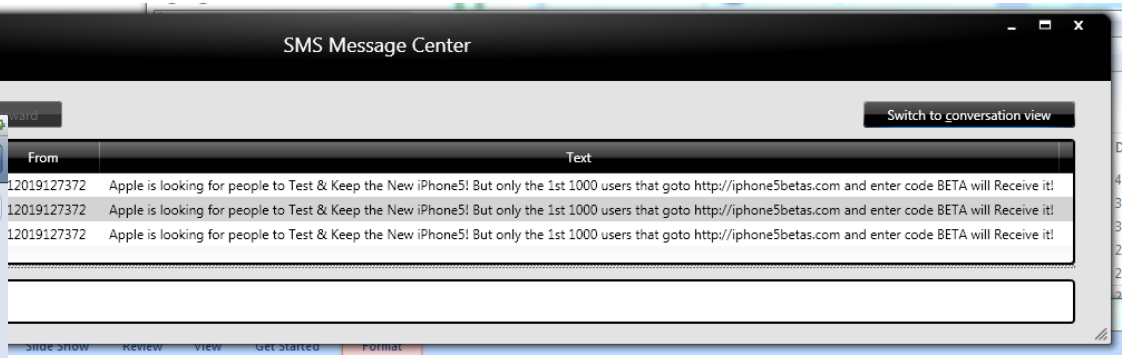
Once the scourge of e-mail providers and the Postal Service, spammers have infiltrated the last refuge of spam-free communication: cellphones. In the United States, consumers received roughly 4.5 billion spam texts last year, more than double the 2.2 billion received in 2009, according to Ferris Research,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

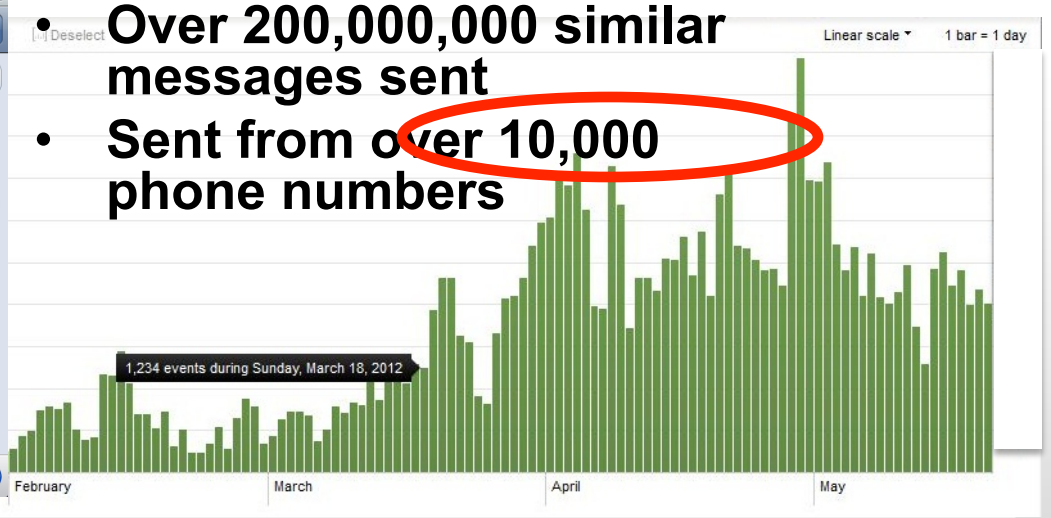
“Unsolicited text messaging is a pervasive problem,” said Christine Todaro, a lawyer with the Federal Trade Commission, the consumer watchdog agency, which is turning to the courts for

Continued on Page 4





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

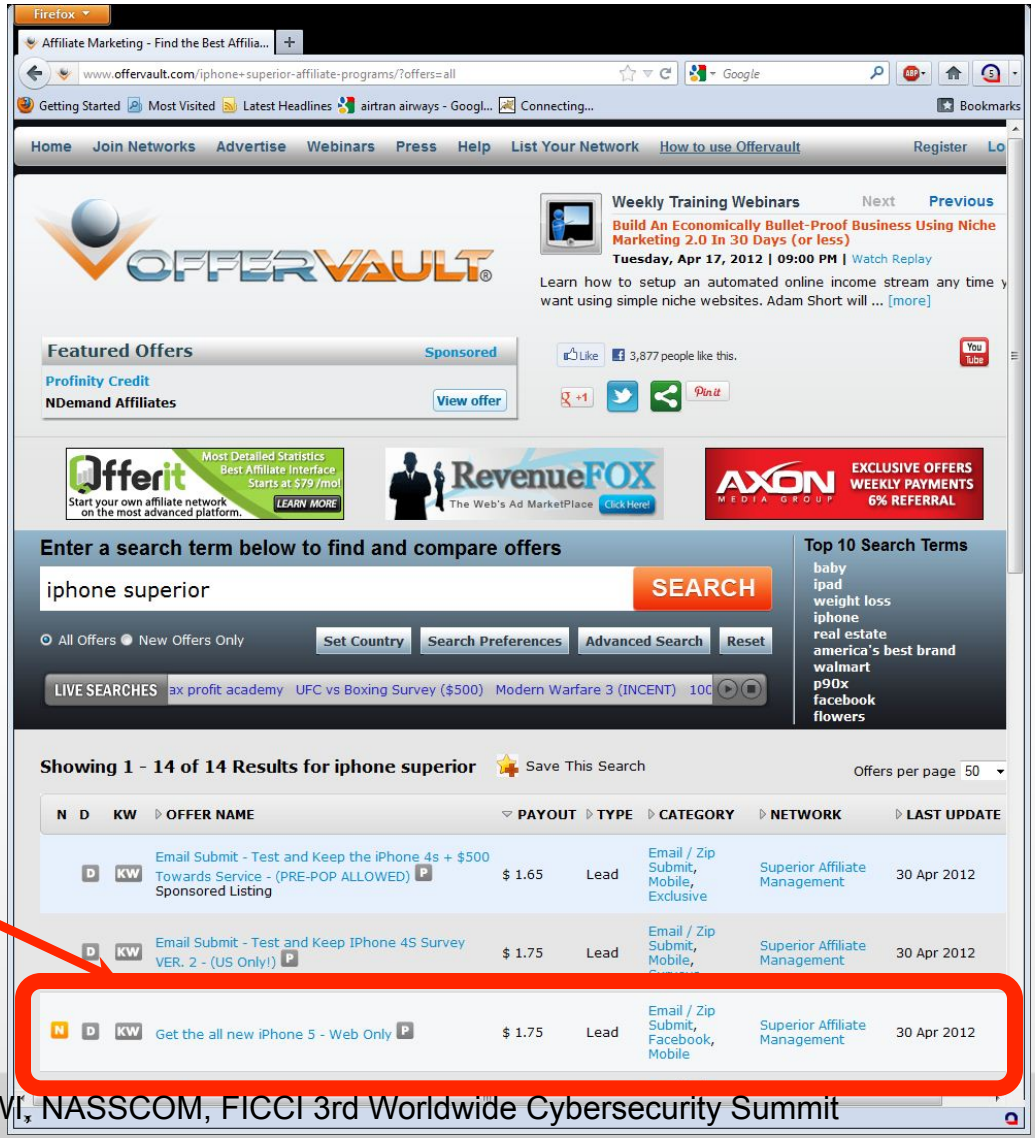


iPad/iPhone/GiftCard Scam Complaint rate

Affiliate Spam
Why SMS Spam Has Exploded

M³AAWG
MESSAGING MALWARE MOBILE

- 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

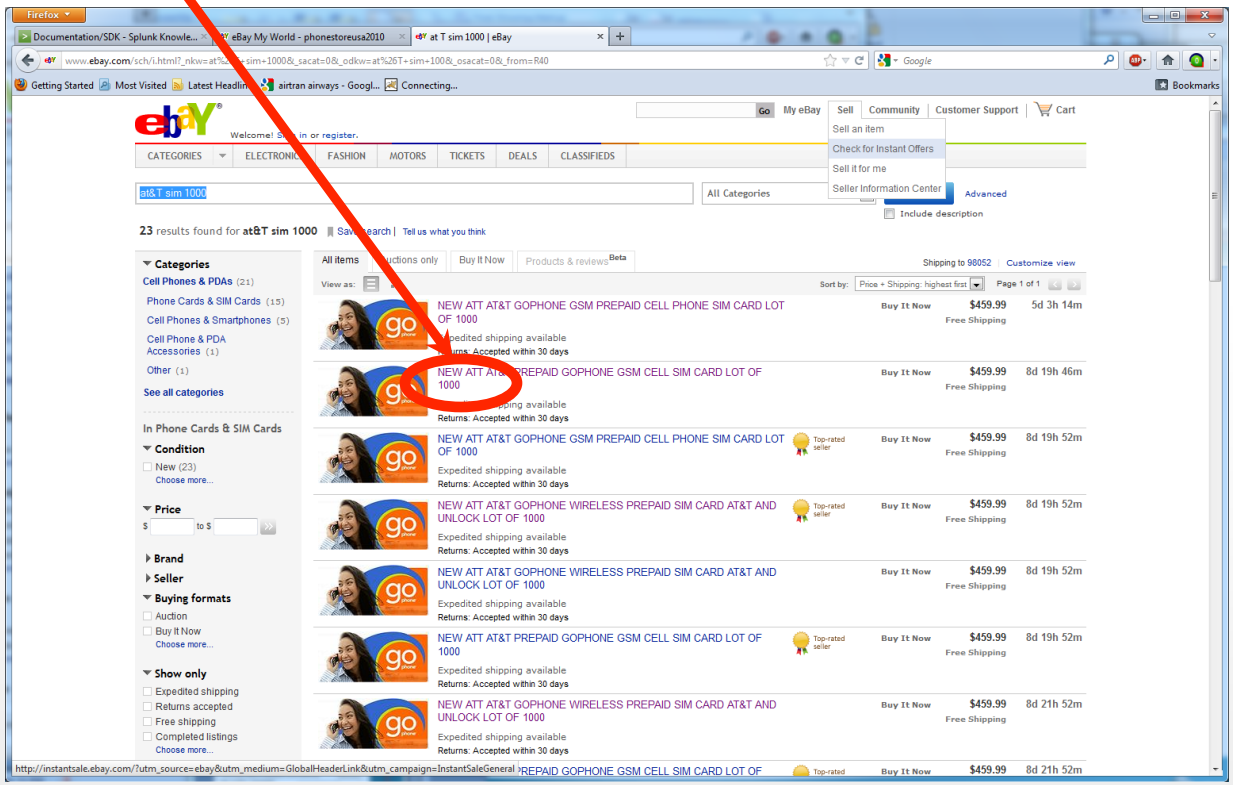


How Affiliates Make Mobile Spam

Boxes of of cheap anonymous SIMs

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

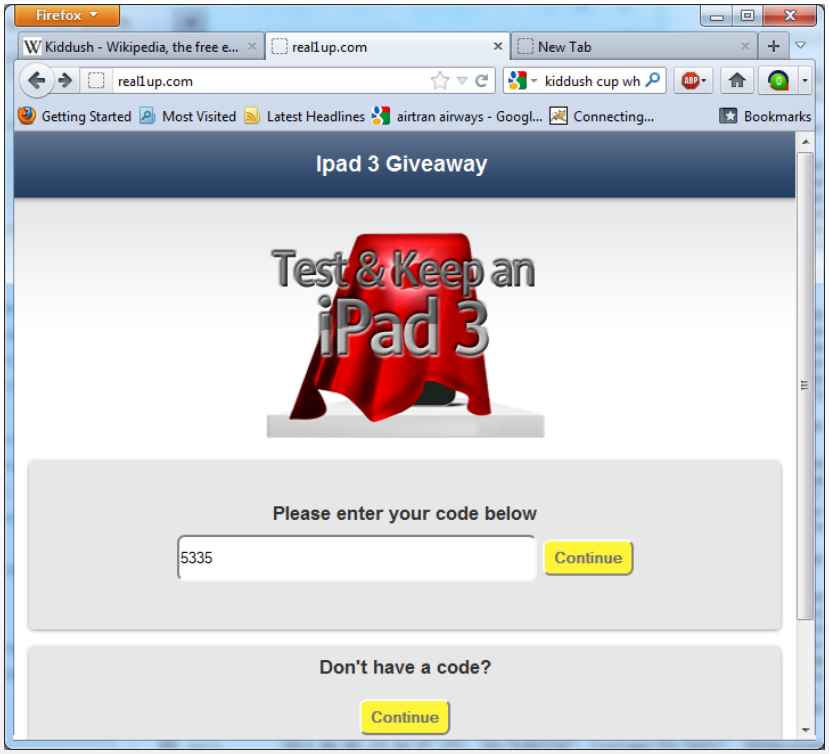
- Bulk SIMs - $0.46 each on eBay
- 10, 100, 1000, 10,000, name your lot size
- Overwhelms manual shutdown defense

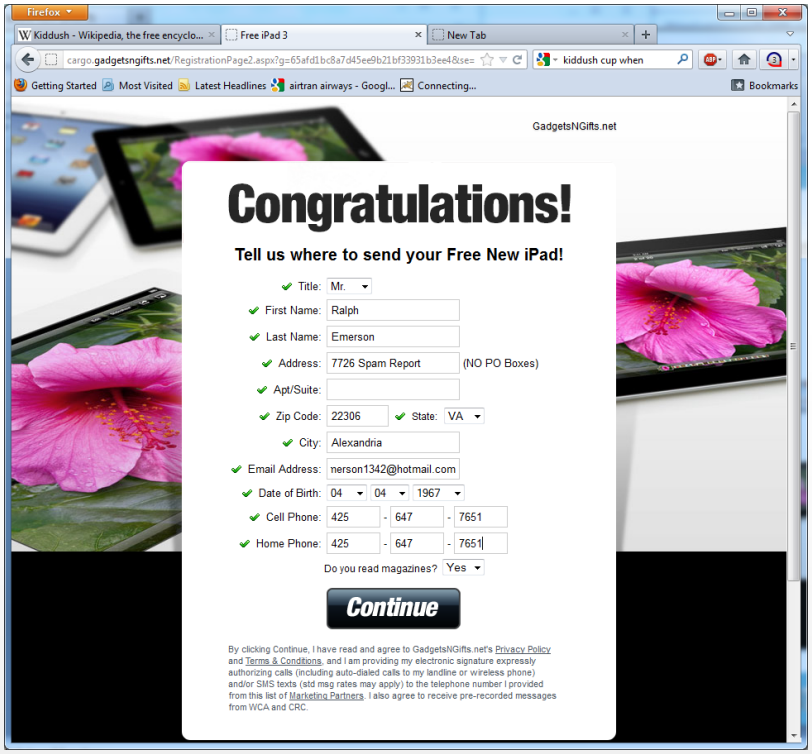


SMS Spam

M3AAWG
MESSAGING MALWARE MOBILE

Visiting the spamvertized website …



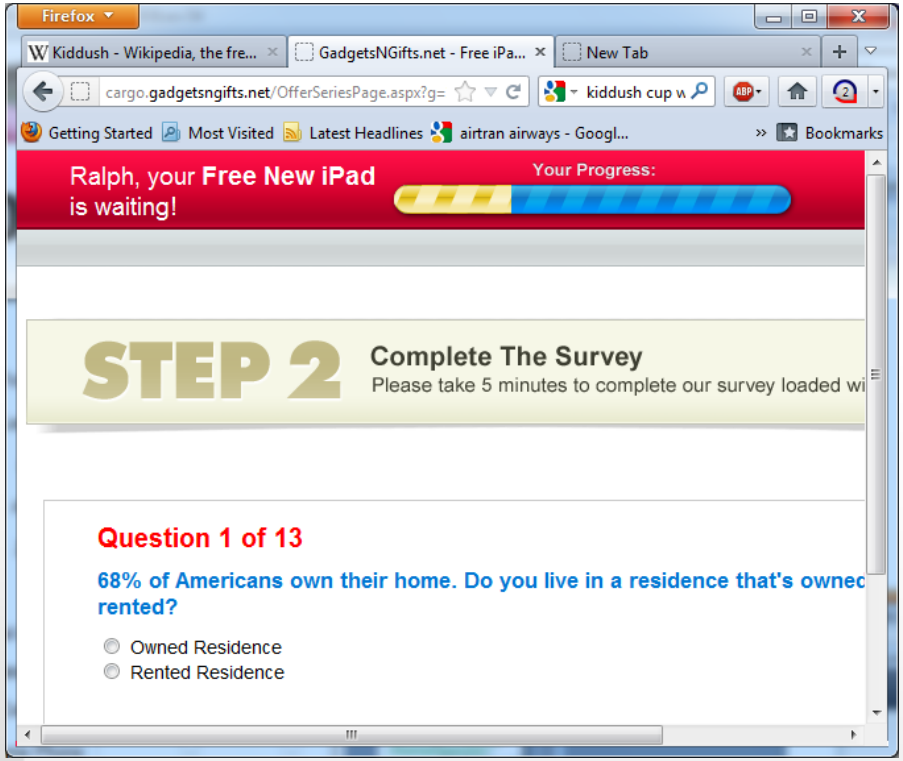


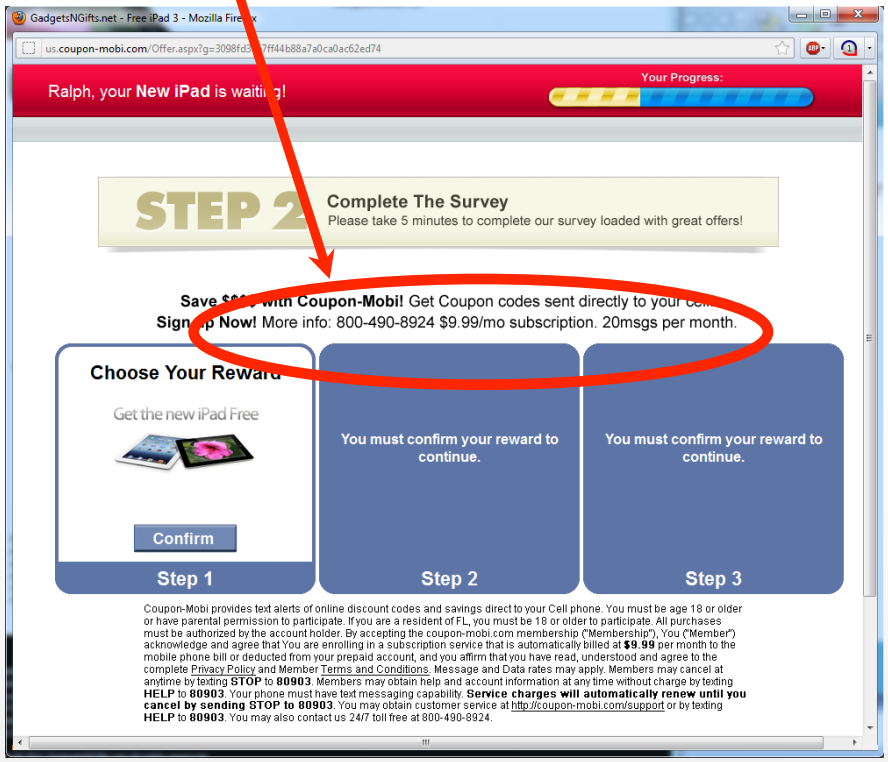
Monetization

M3AAWG
MESSAGING MALWARE MOBILE

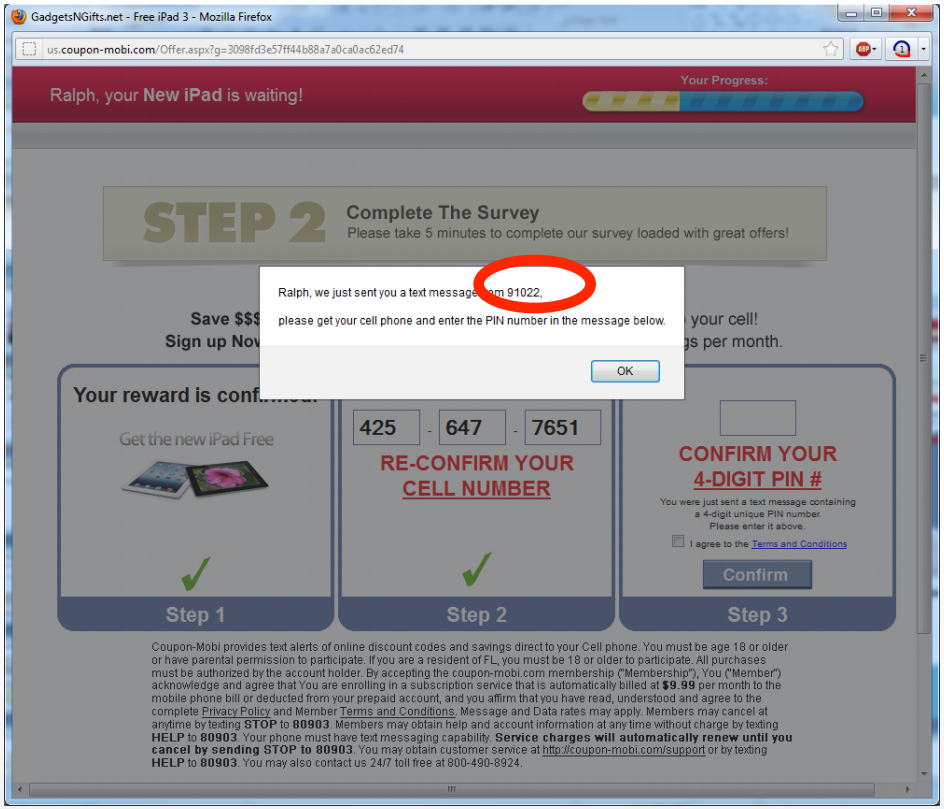
Take a “survey” …

SMS monetization!

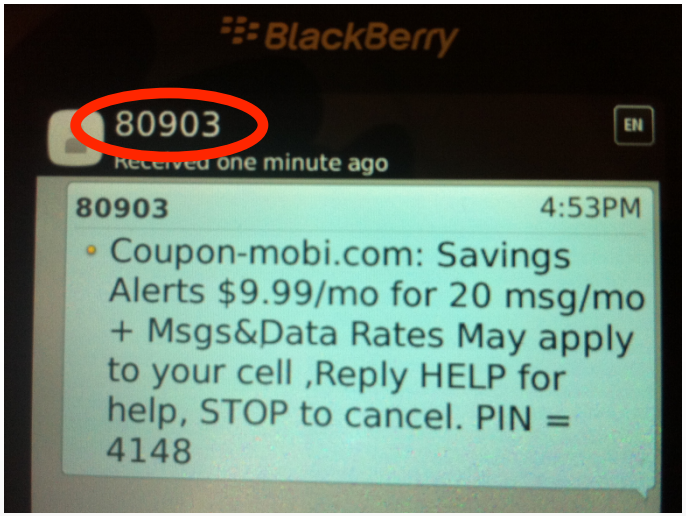




SMS Monetization



Instantly received on my Blackberry …



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

Other Monetization

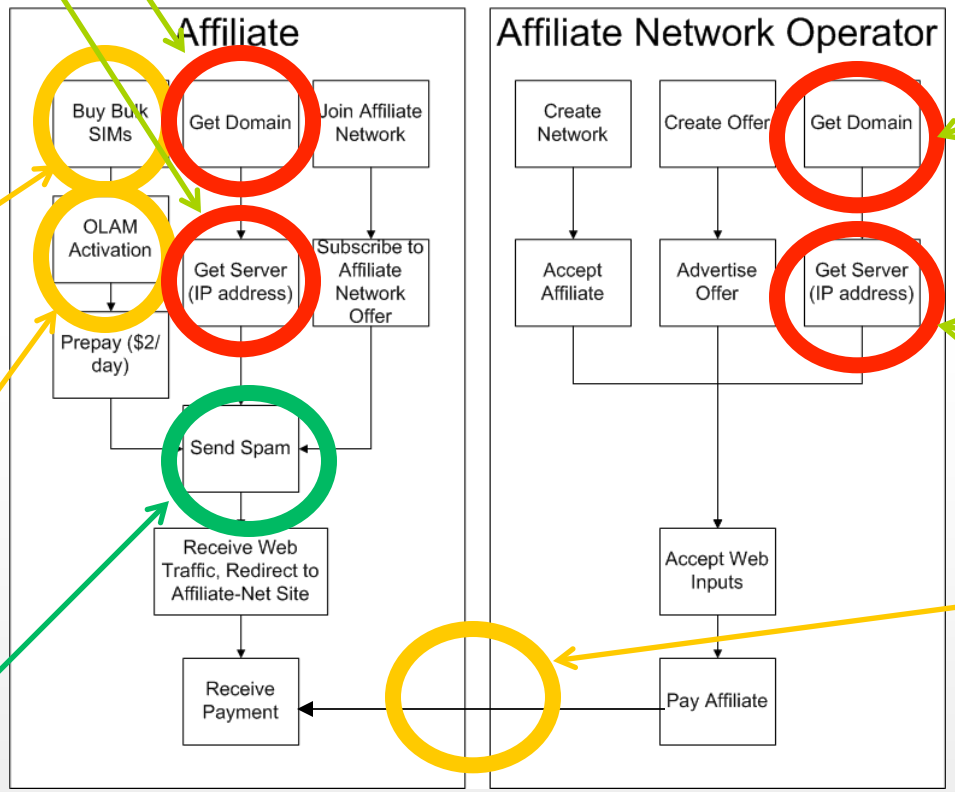
M3AAWG
MESSAGING MALWARE MOBILE

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

Develop a Strategy

M3AAWG
MESSAGING MALWARE MOBILE

Shutdown domain
Shutdown server



Control bulk purchases

Detect bulk activation

Shutdown or block

Shutdown Domain

Shutdown Server

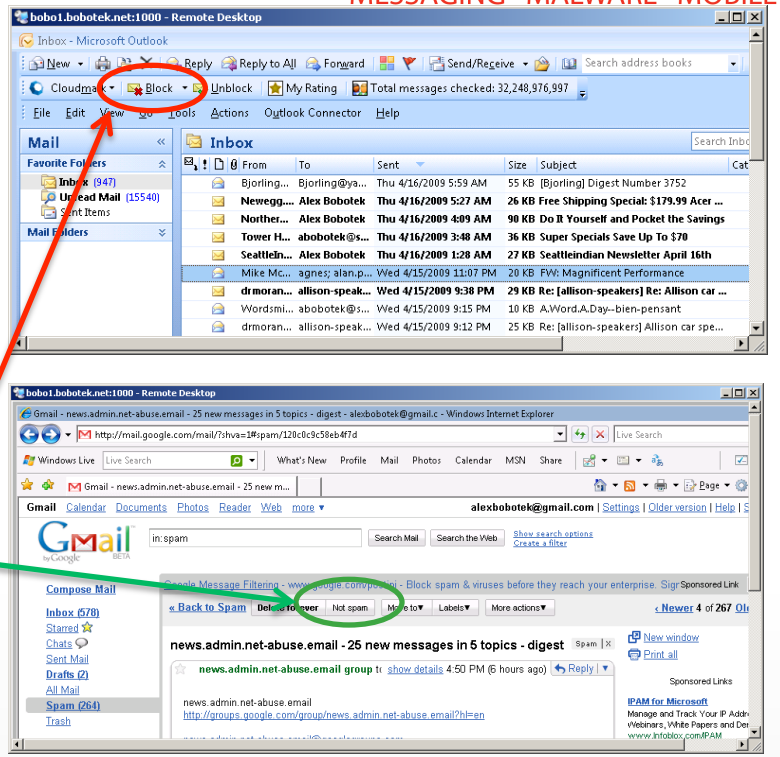
Legal Intervention

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**

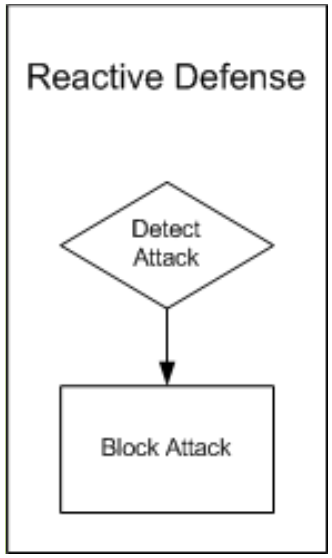
- Typical email user agents have “This is Spam” and “Not Spam” buttons

- **A standard ‘Report Spam’ button**
  - **Use OMA Standard “SpamRep”**
  - SpamRep standard completed

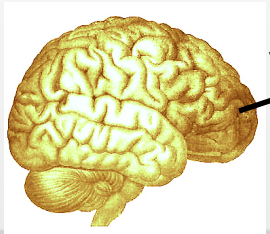


Filter Defense (takes time/resource)

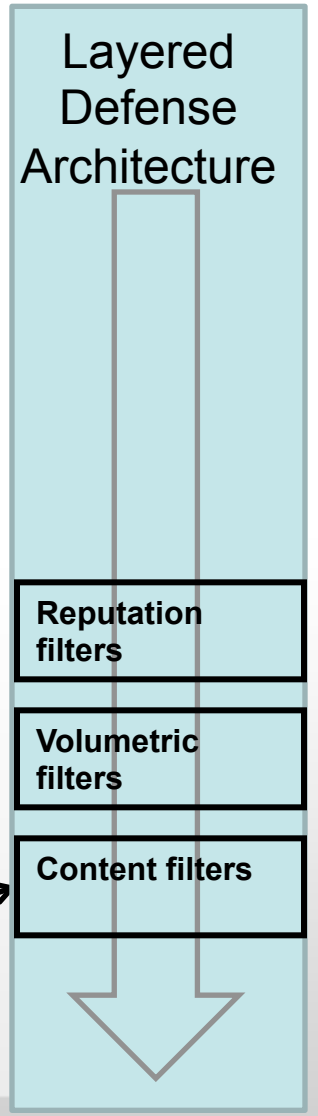
- Deploy spam/virus filters
- Build better spam reporting
  - "This is Spam" button in UA



- **Abuse detection - the human brain**
  - Ideally nimble, adaptable abuse detector
  - Stochastic - error rate of ~ 1%
  - Often off-duty
  - Occasionally malign



This is spam



Account-Level Defense: Detect and Block

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

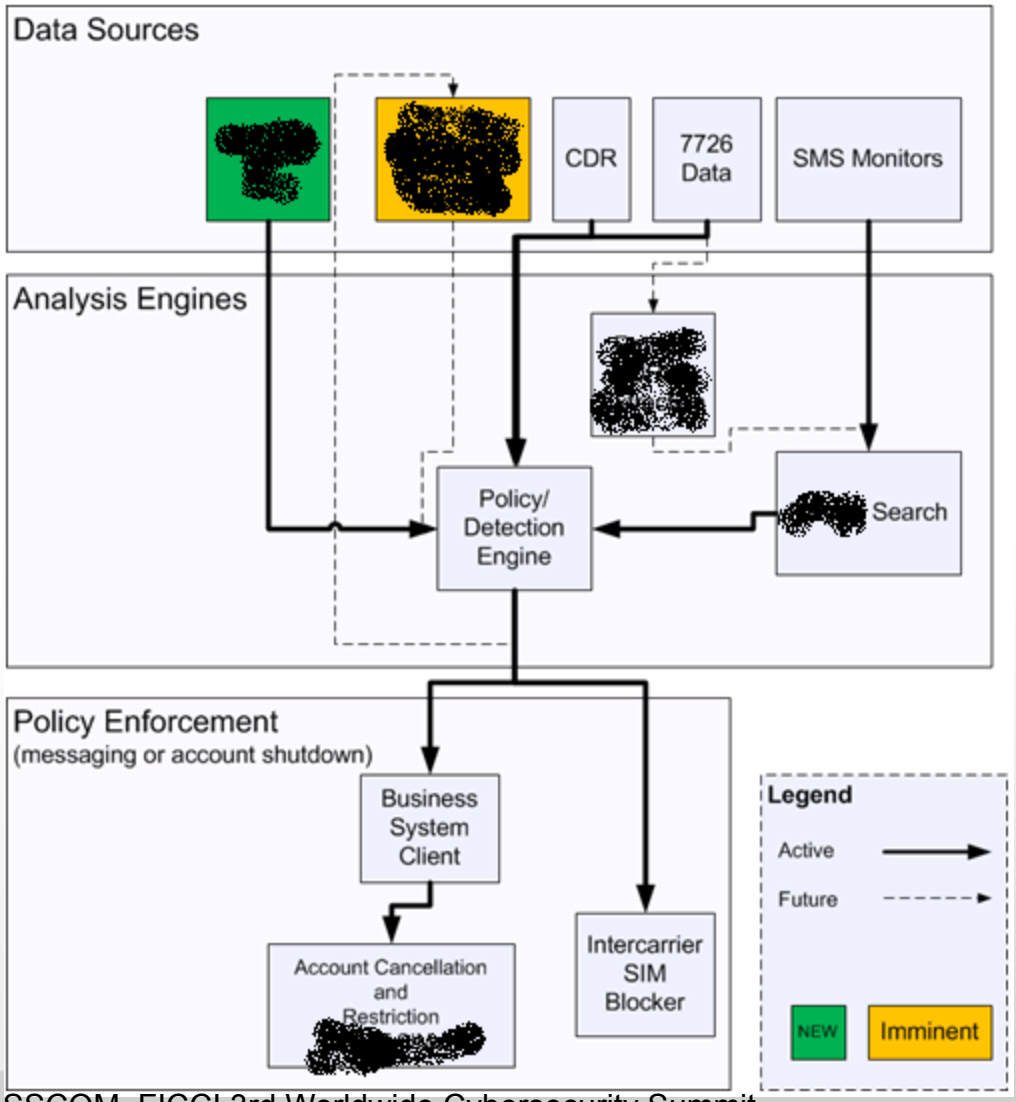
Detection

- By subscriber reports
- By message rate/volume
- By message content

- Exchange reports with other MNOs

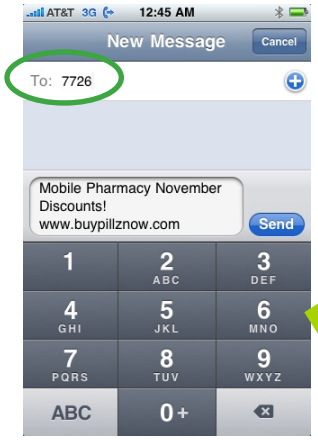
Whack SIMs

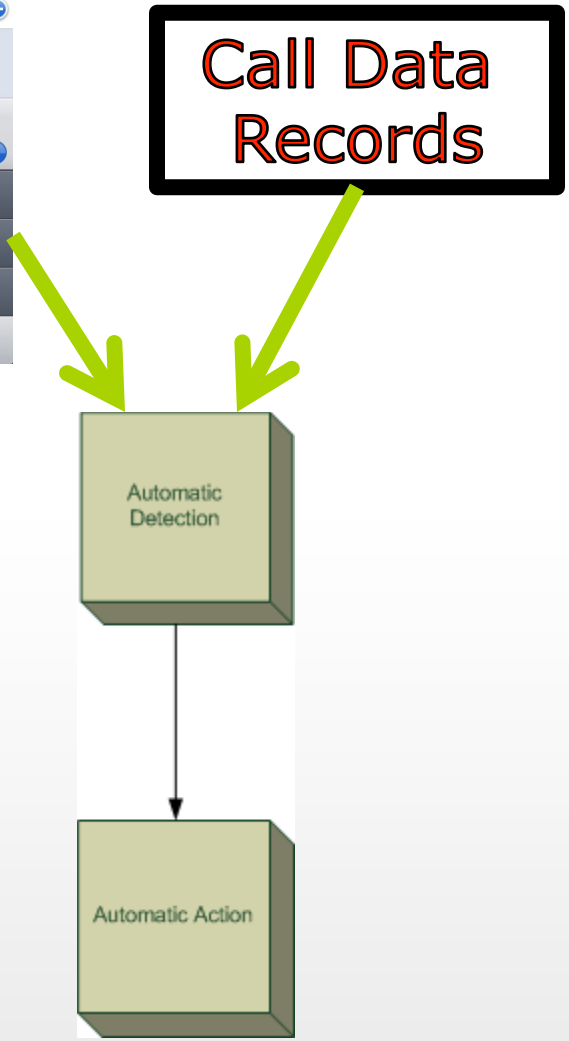
- Automated shutdown



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





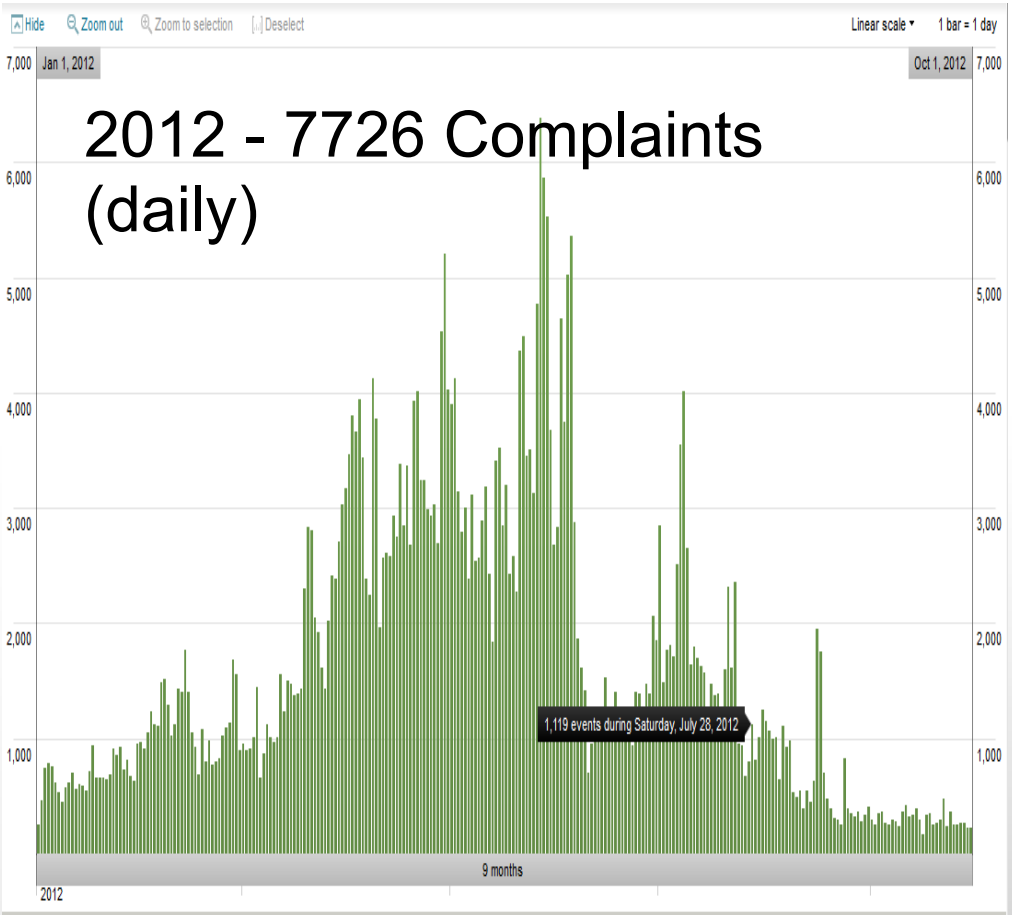
US Domestic Spam Status

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**

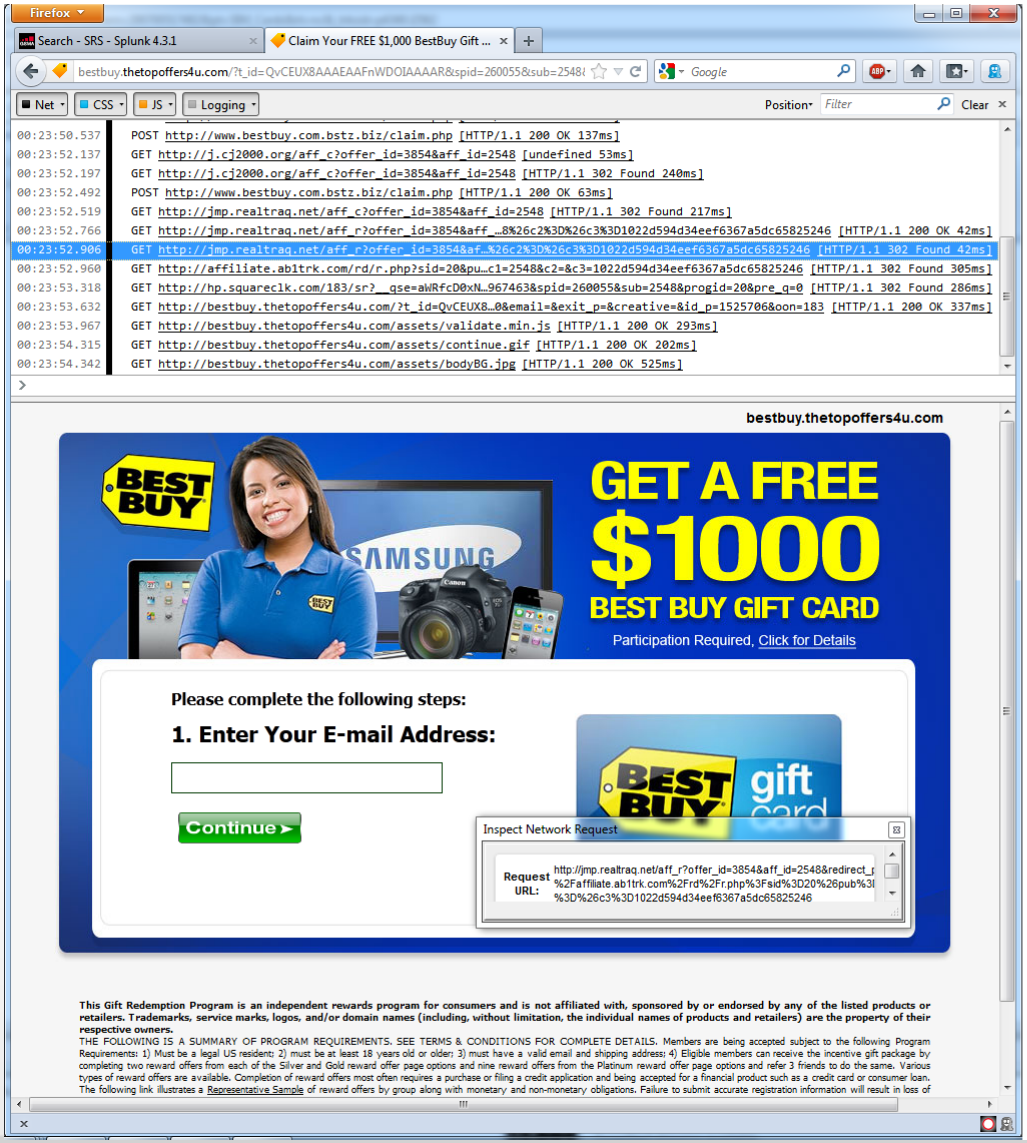


Problems

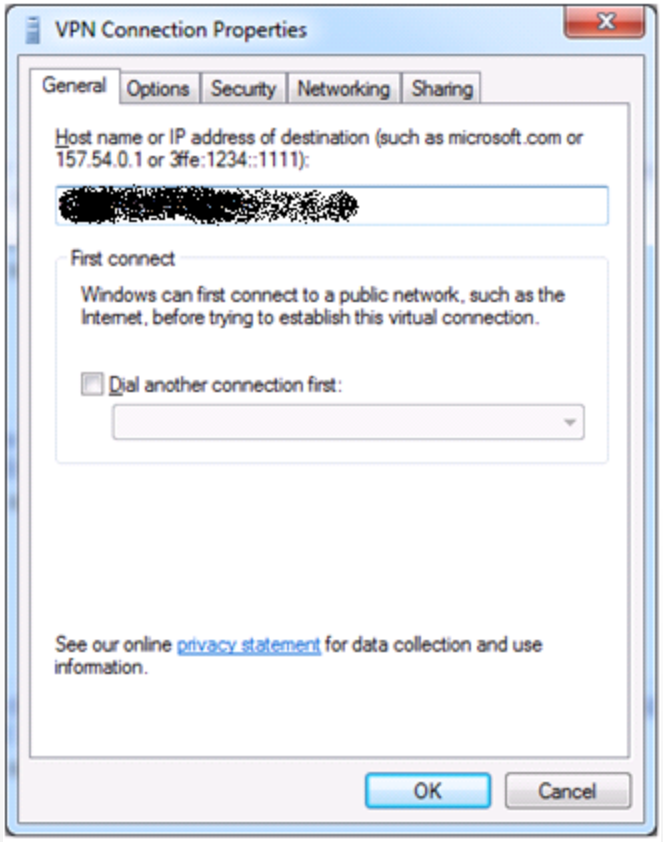
- Growing abuse
  - Spam
  - Malware
  - Fraud
  - Harassment
  - Network disruption
- Growing internationalization of abuse and global homogenization of abuse technologies
  - Toolkits
  - Criminal economy
  - Intra-carrier sensors (e.g., SRS) are effective against attacks which include intra-carrier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

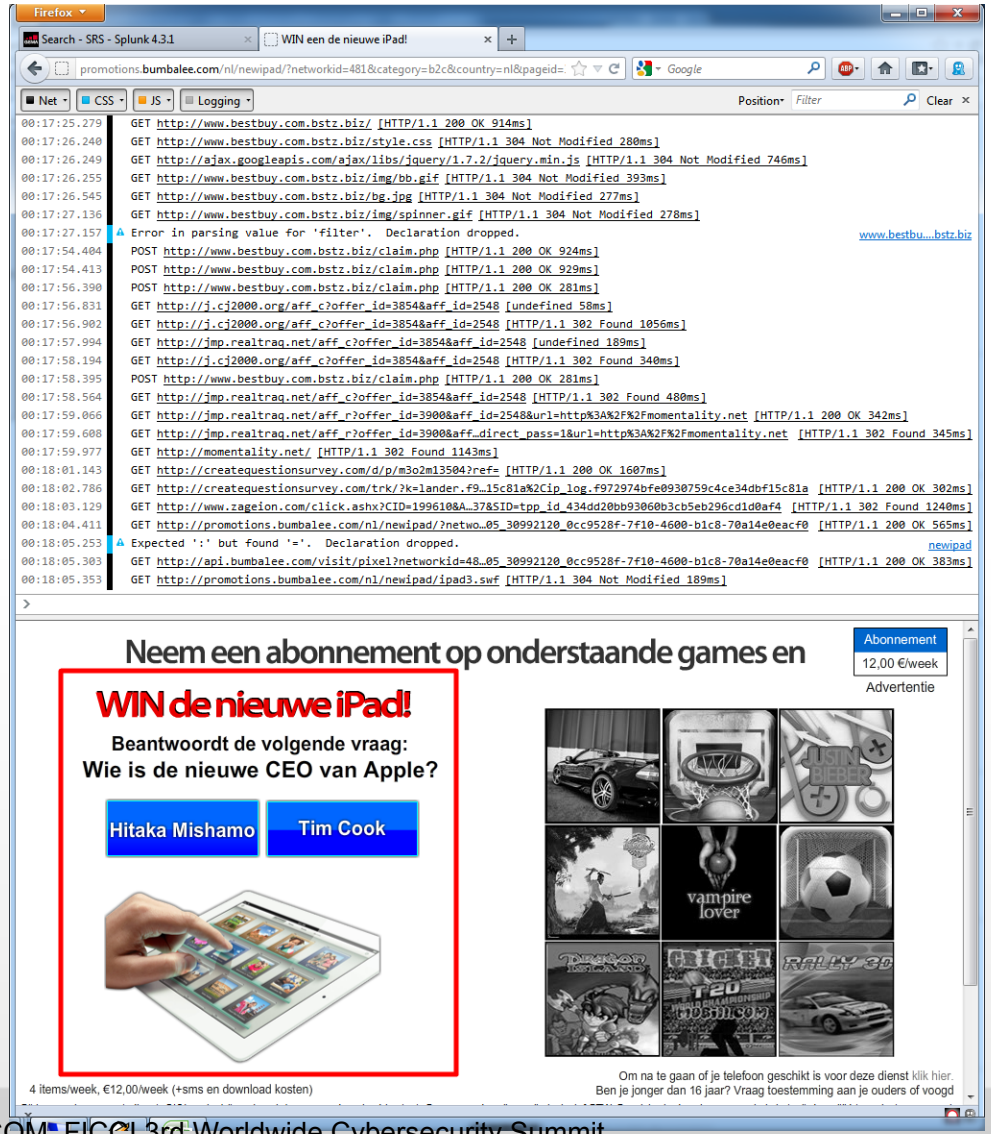
We're fighting a growing and increasingly similar and mobile spam problem across continents and oceans

USA IP Address

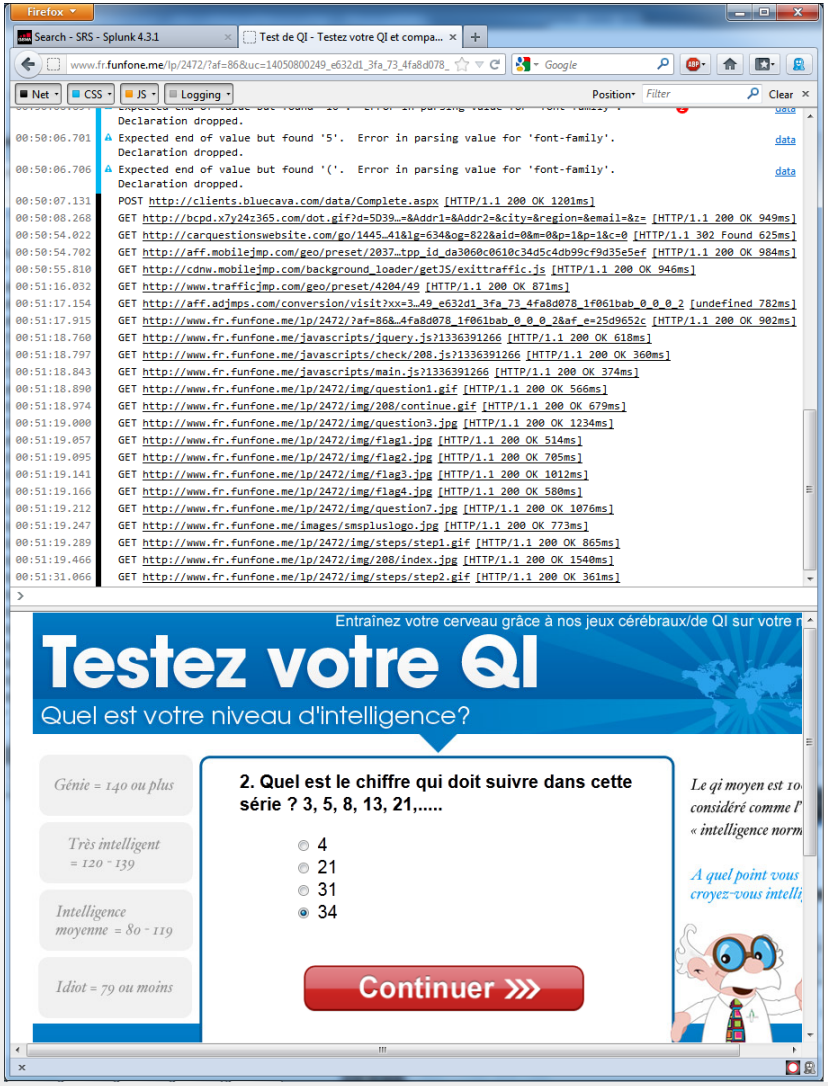


Internationalization – Netherlands IP

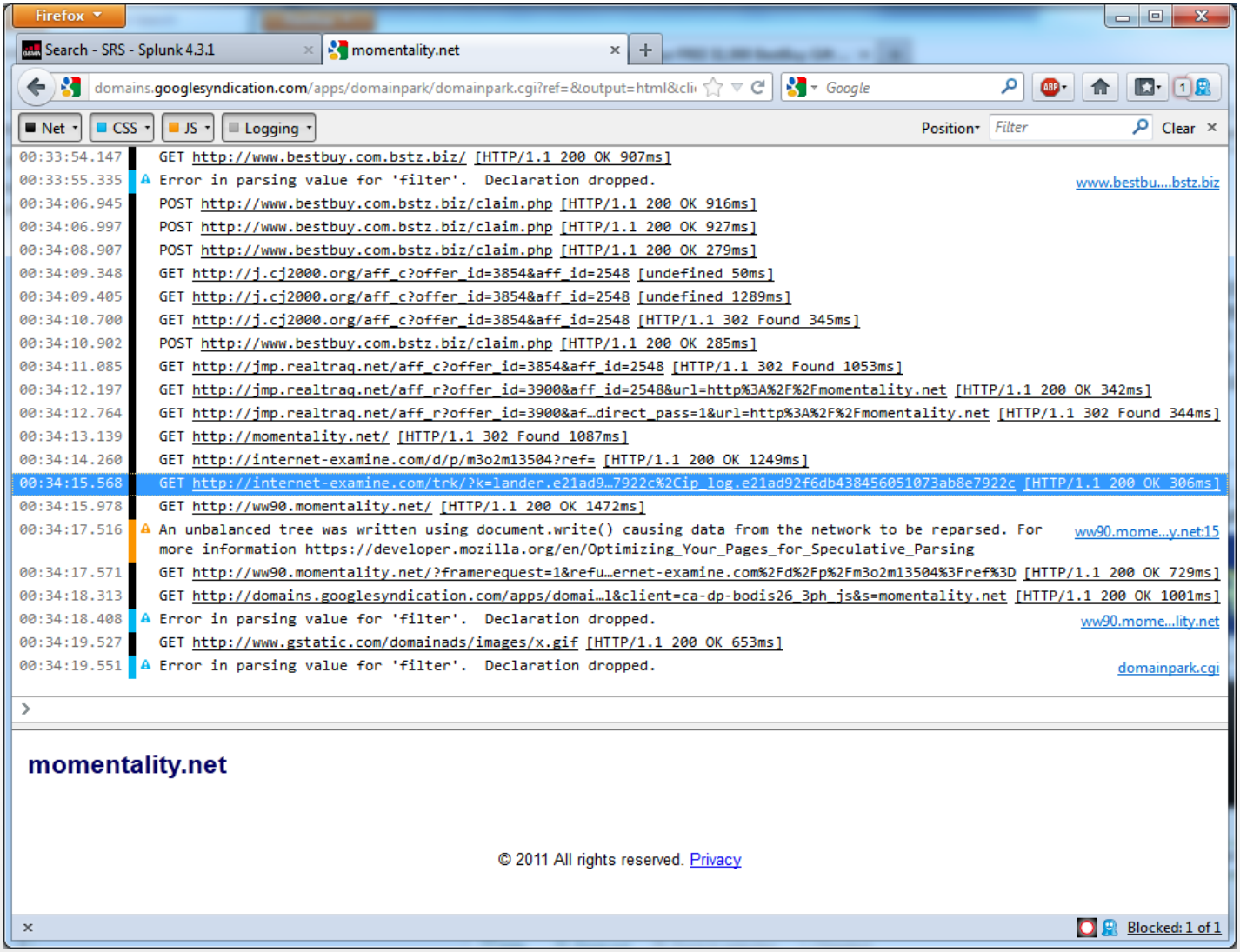




Internationalization – Paris IP Address

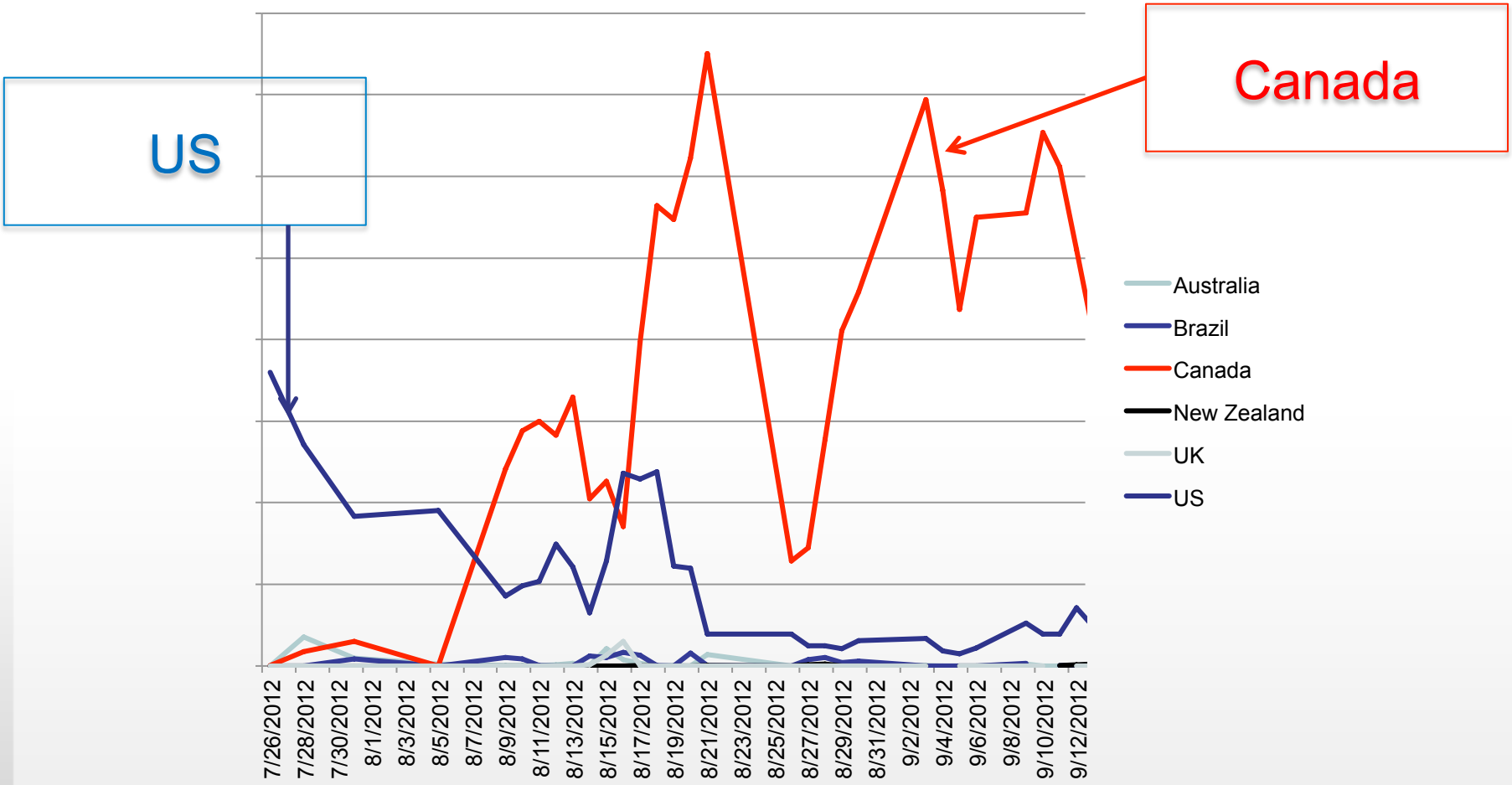


Internationalization - Germany



New Spam Plan: Spam Canada Instead

M3AAWG
MESSAGING MALWARE MOBILE



A Framework for Abuse Data Exchange

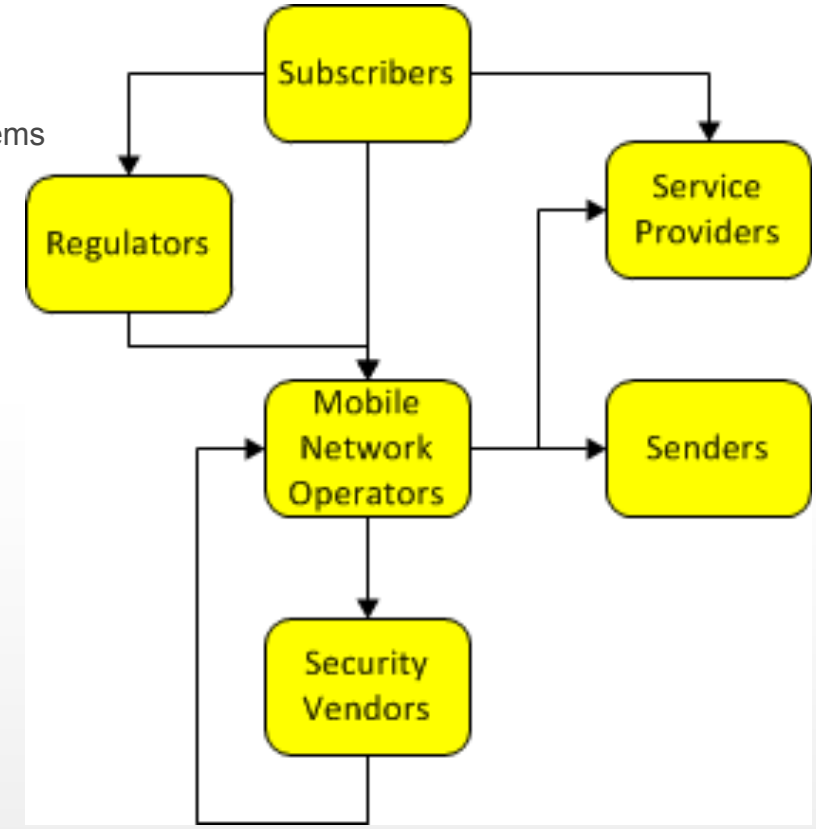
M3AAWG
MESSAGING MALWARE MOBILE

- 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

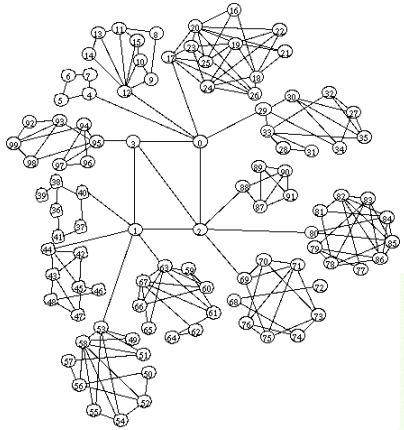
- Typical semantics
  - "I got spammed"
  - "High rate"
  - Botnet C&C traffic report
  - Passive DNS
  - "<MSISDN> is a spammer" assertions

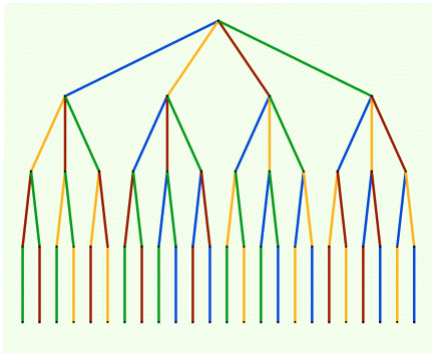


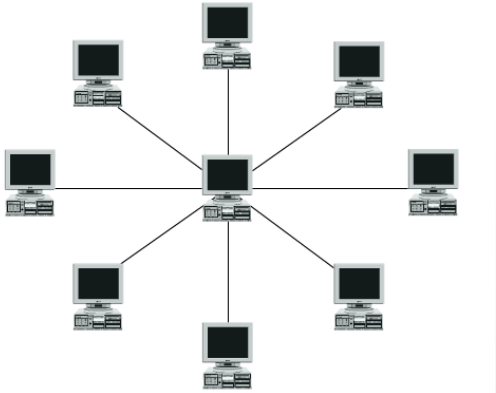
Data Flow Topology

M3AAWG
MESSAGING MALWARE MOBILE

- 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