



## Stopping Cyberspace Pollution – International Cooperation on Fighting Spam and Botnets (including readout from Monday M<sup>3</sup>AAWG workshop)

Michael O'Reirdan – M<sup>3</sup>AAWG Co-Chairman

Zhou Yonglin – Director, Internet Society of China

Alex Bobotek – M<sup>3</sup>AAWG Co-Chairman



# Objective and Agenda

- Introductions and Objectives for the Interest Seminar
- Update – “China-U.S. Fighting Spam to Build Trust” report, recommendations and best practices
- Summary of Monday M<sup>3</sup>AAWG Workshop
- Collaboration Next Steps for Workshop
- Discussion

## **“China-U.S. Fighting Spam to Build Trust” report, recommendations, and best practices**

- Zhou Yonglin – Director, Internet Society of China

# Summary of Monday M<sup>3</sup>AAWG Workshop



- Michael O'Reirdan – M<sup>3</sup>AAWG Co-Chairman
- Alex Bobotek – M<sup>3</sup>AAWG Co-Chairman

# The Spam Problem Threat Picture



Large scale blocking; negative reputation of Indian IPs

India “leads the world” in the number of virus infected IP addresses

Local bulk email and SMS spammers and marketers who don't follow best practice, even local street corner shops

Parts of the cybercrime ecosystem get outsourced to India

- Massive registration of criminal domains in the .in ccTLD
- Production of pills sold by illegal online pharmacies
- Tech support scams run by shady call centres
- Blackhat SEO (“googlespamming”), forum / blog comment spam
- Nigerian scams are localized to India

# The Spam Problem

## What can Indian ISPs do about messaging abuse?

### Best practice implementation and localization

- Spam and virus filtering of email and messaging services
- Network security and threat mitigation
- Acceptable Use / Anti Spam policy enforcement
- User education and secure access to ICT
- Local and international cooperation
  - Champions for M<sup>3</sup>AAWG India?
- Coordination and targeted information sharing

# The Spam Problem

## How Indian email marketers can help

- Adopt the M<sup>3</sup>AAWG Sender Best Communications Practices
- Vet your new customers and audit existing customer lists
- Work to ensure your colleagues in the industry don't spam
- Adopt a shared code of conduct?
- Industry associations you can consider joining M<sup>3</sup>AAWG, ESPC, and of course, IAMAI

# The Spam Problem Government & Law Enforcement – Suggestions

Mitigation of malicious domains, botnet C&C etc.

- Data sharing by additional trusted third parties with CERT-IN

Stepped up action against local criminals

- Vendors of email address databases, unsolicited bulk email and SMS products and services, other parts of the cybercrime ecosystem (illegal drug suppliers, fake call centres.)

Increased engagement with intergovernmental and public/private groups

- [The Budapest Convention on Cybercrime](#)
- [The London Action Plan against Spam](#)
- [FIRST](#) / [APCERT](#), [M<sup>3</sup>AAWG](#), [OECD WPISP](#) ...



# The Bot Problem

## Policy is key

- May sound like a list of roles but up to regulators and policy folks to work together to ensure everyone plays their position.
- Not just the role of the ISP
- ISPs core competency
  - Detection and notification, manages relationship between IP resource and subscriber
- Other players
  - Law Enforcement
  - OS Vendors
  - Tools vendors
  - Software vendors

# The Bot Problem

## Global efforts

- US
  - FCC Bot Code
    - [ABCs for ISPs](#)
  - Major programs at several ISPs
    - Century Link, ATT, [Comcast](#)
- Germany / Eire
  - [BotFrei.DE](#), Spreading to 14 European countries, EU funded
- Finland
- Australia
  - [iCode](#) since 2010
- Japan
  - [Cyber Clean Centre](#)

# The Bot Problem Monetization

- Need financial justifications
  - ROI may need to be sought
  - Reduced churn of subscribers
  - Reduced numbers of call centre contacts
  - Spam can consume expensive bandwidth resource
- Free versus paid
  - Important not to make this seem to be an upsell for additional services
  - Need a prominent “free” remediation path
  - Often too complex
- Do your own Geek Squad approach
  - Geek Squad, large scale consumer tech support organization, counters in computer stores and in home support
  - Some ISPs have set up fee-based remediation services

# The Bot Problem

## Technology / Resources

- DNS
  - Widely deployed
- DPI
  - Depends on country attitude to DPI
- NetFlow
  - Good for detecting botnets but not malware
- IETF Guide to bot remediation, [RFC 6561](#)
- IETF Guide to a possible notification system, [RFC 6108](#)
- Free data sources
  - [Team Cymru](#), [Shadow Server](#), Arbor Networks
- Free A/V and tools
  - Avira, AVG, Microsoft Security Essentials, Malwarebytes, Spybot, Adaware

# The Bot Problem

## Role of domain name registrars



- India based registrars have the strongest ability to respond and curtail bad registrations:
  - Directi is one of the largest Indian reseller-based registrars, with prior abuse experience
  - Net4India is the largest retail based registrars, with a well-developed validation method
  - Mitsu is one of the fast growing registrars, with some current abuse
- Largest abuse seems to come from automated, non-verified systems
- Domains are one of the raw materials for botnets

# The Bot Problem

## DNS Changer

- FBI Operation Ghost Click
- First discovered in 2007 by private researchers
- Rove Digital
- DNS servers in the US
- Initially thought to be 4 million users infected, turned out to be less but still substantial
- November 8<sup>th</sup> 2011, 7 arrests, servers and cash seized
- DNSs run by ISC from Nov 8<sup>th</sup> 2011 to June 9<sup>th</sup> 2012
- Need to remediate end users
- Interesting statistics
  - Do nothing ISP -40%
  - Active ISP -80%

## The Mobile Problem

- Alex Bobotek – M<sup>3</sup>AAWG Co-Chairman

# Desired Outcomes

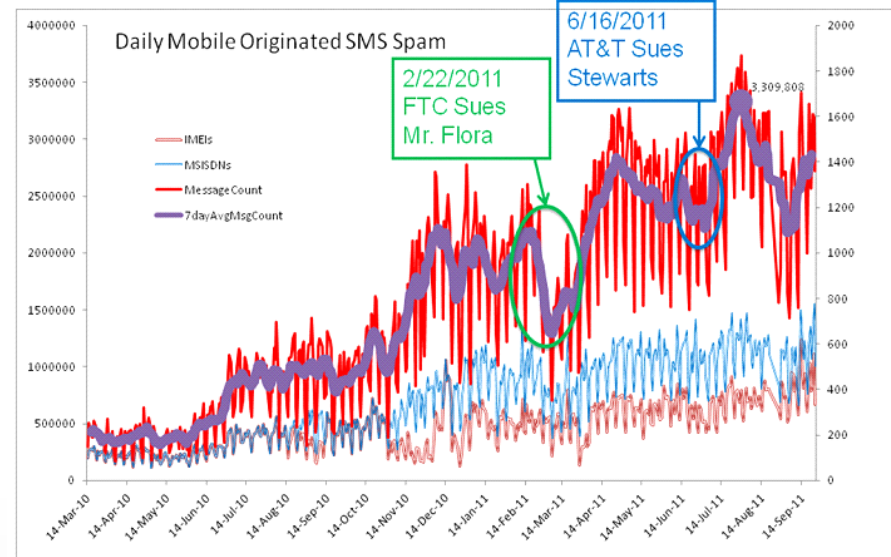
1. Deploy “This is Spam” reporting
2. Deploy spam filters in SMS messaging
3. International collaboration
  - Enforcement
  - Abuse data exchange
  - Attend forums (M<sup>3</sup>AAWG, GSMA, ...)



# 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

# 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

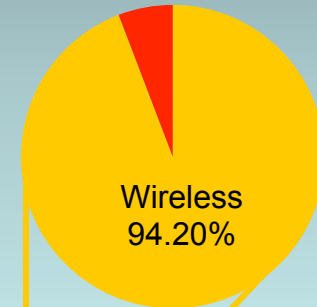
# History: 2011/2012

## North American Messaging Threats

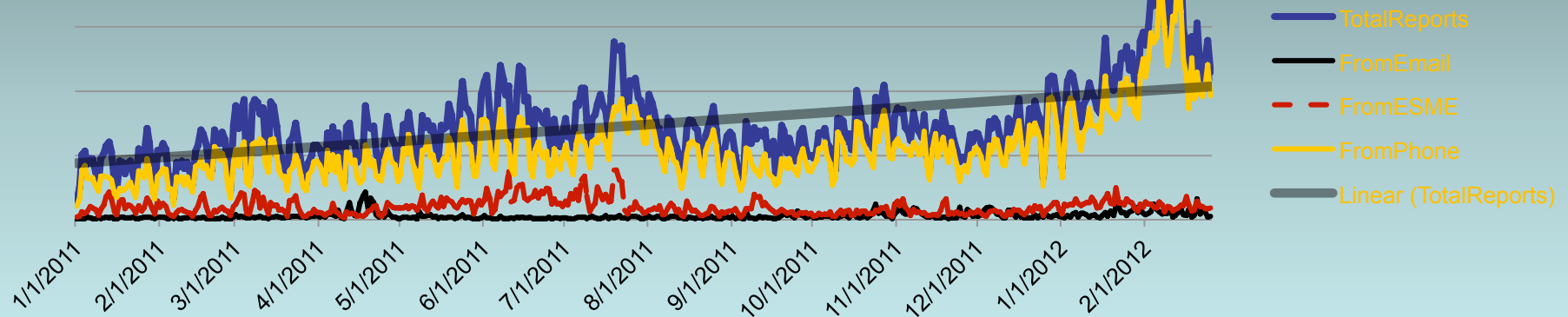
- SMS abuse growing <100%/year
- Sources
  - Mobile Phones: dominant today
  - Over The Top: significant and exploding
  - Mobile botnets/malware: significant threat
  - ESME & Email → SMS: small and controlled

### 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

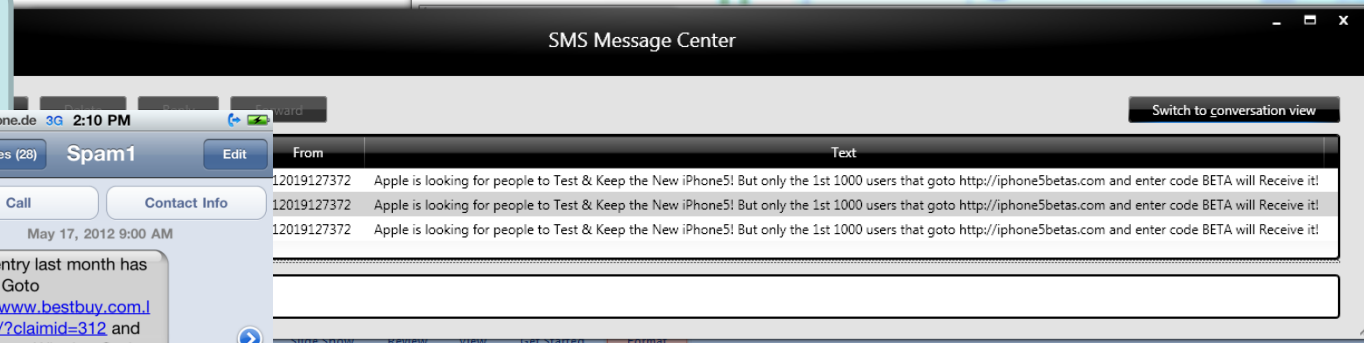
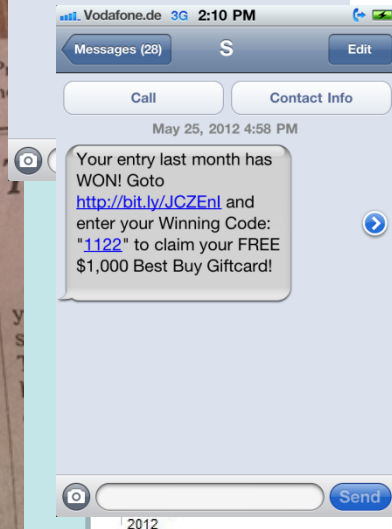
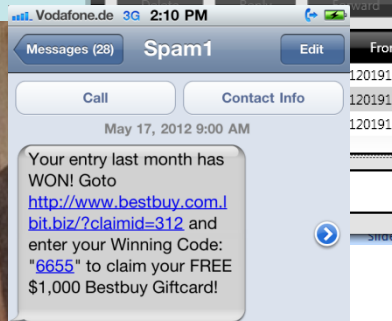
Text message spam has started waking Bob Dunnell in the middle of the night, promising cheap mortgages, credit cards and drugs. Some messages offer gift cards to, say, Walmart, if he clicks on a Web site and enters his Social Security number.

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 a weekly training webinar. 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 with 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

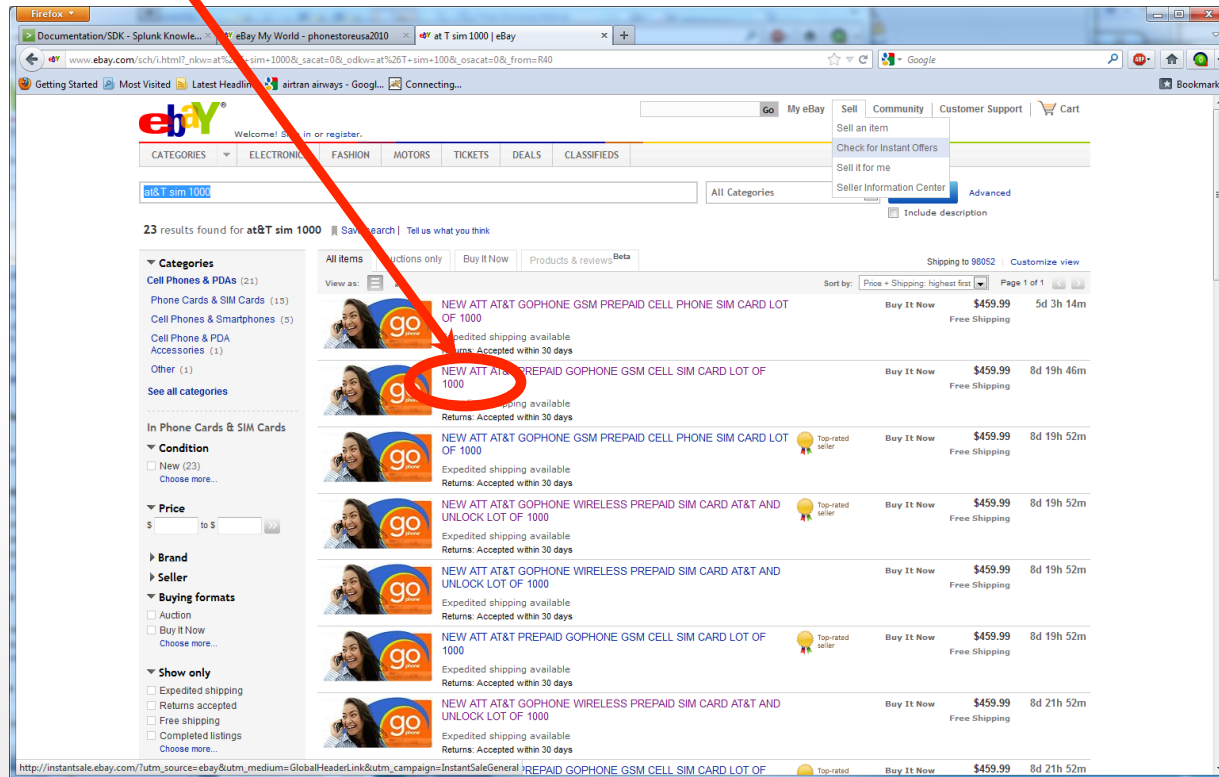


# How Affiliates Make Mobile Spam

## Boxes of of cheap anonymous SIMs

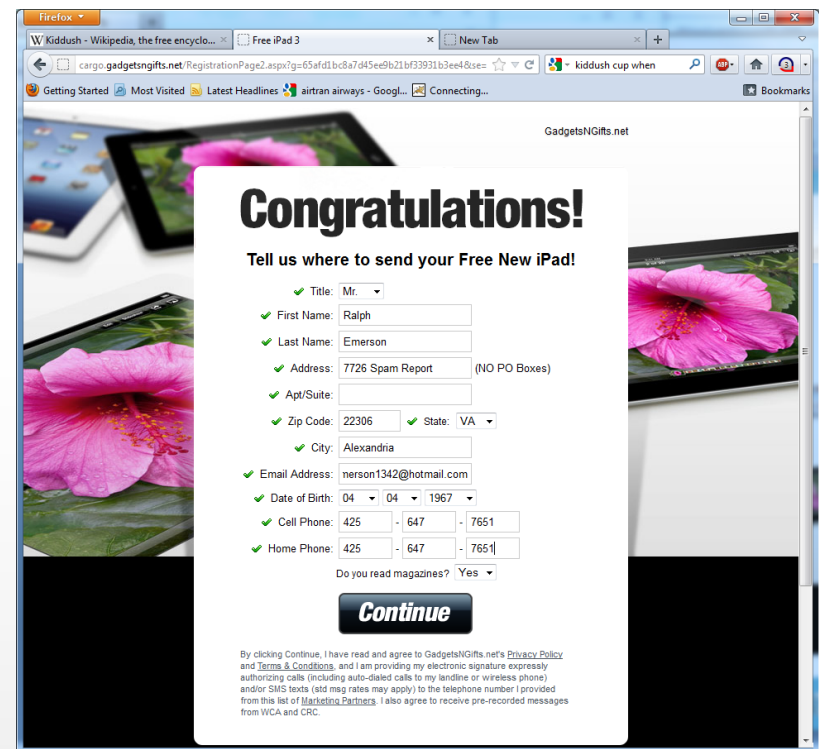
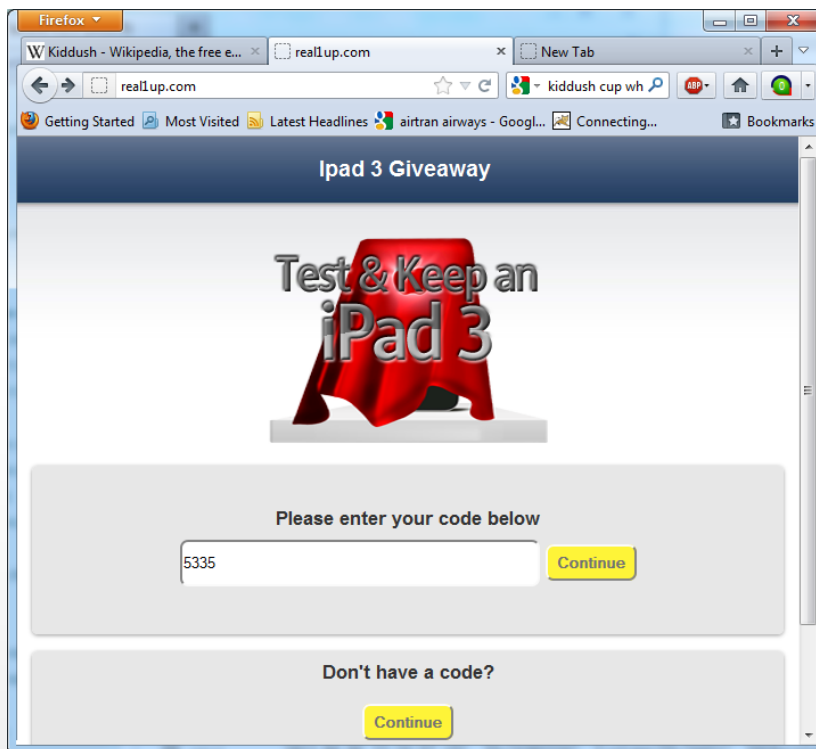
### Cheap anonymous rate plan: Prepaid unlimited SMS for \$2/day

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



# SMS Spam

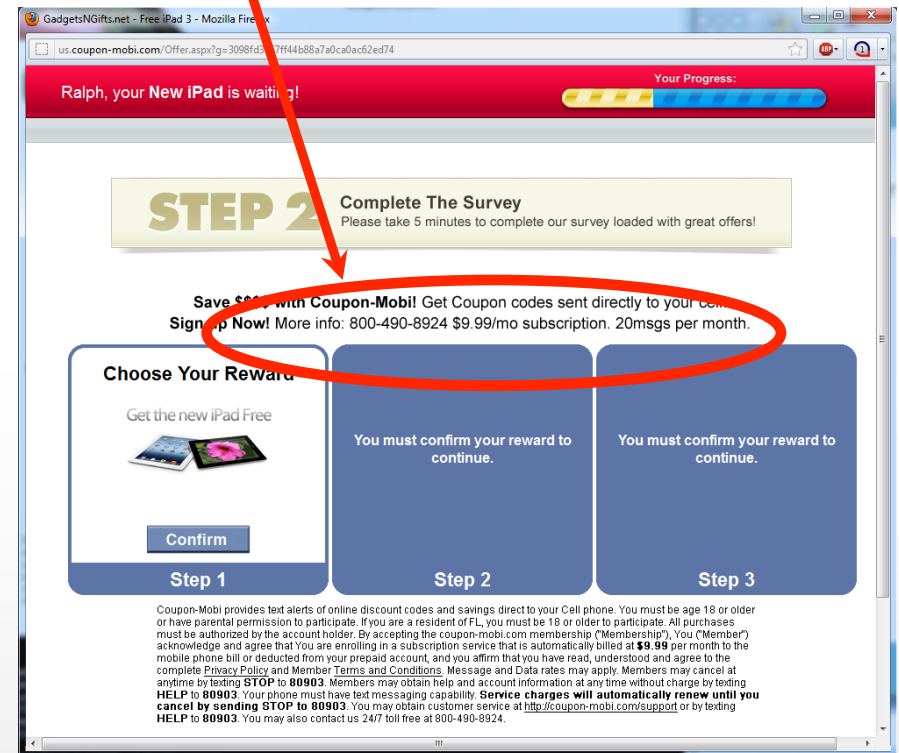
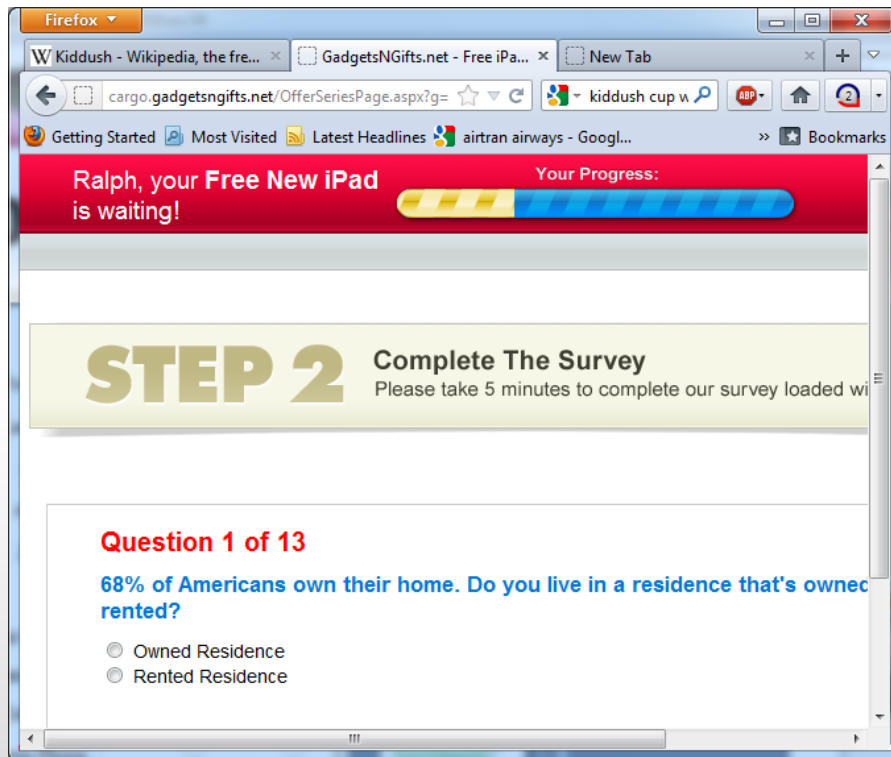
Visiting the spamvertized website ...



# Monetization

Take a “survey” ...

SMS monetization!





# Develop a Strategy



Shutdown domain  
Shutdown server

Control bulk purchases

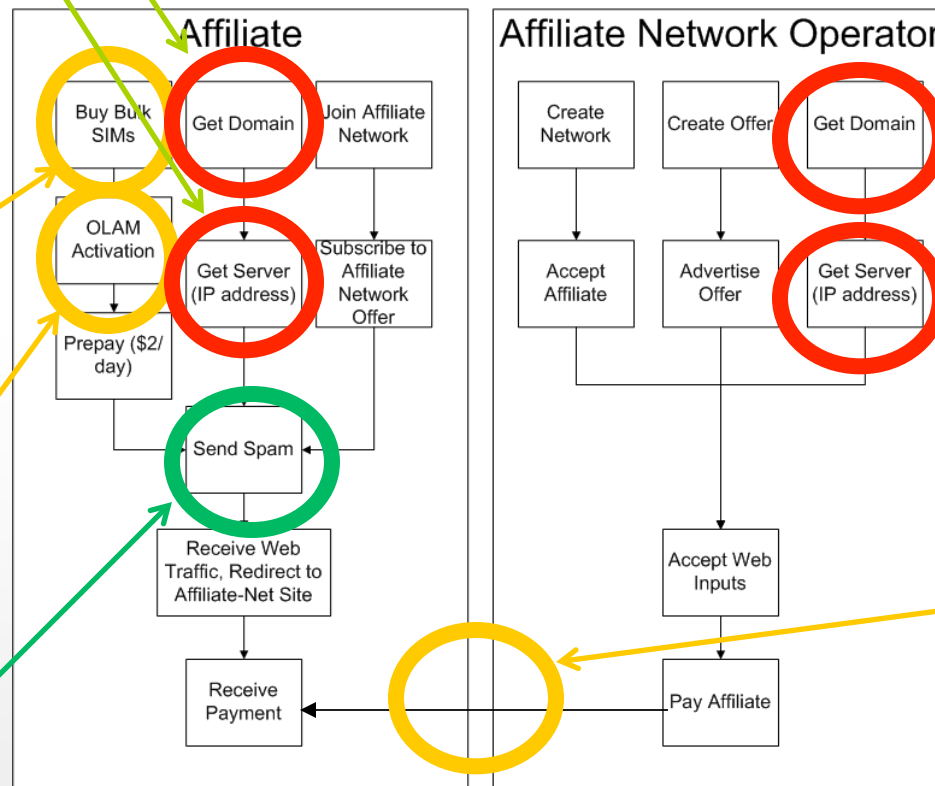
Detect bulk activation

Shutdown or block

Shutdown Domain

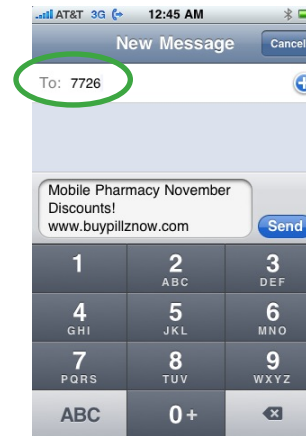
Shutdown Server

Legal Intervention

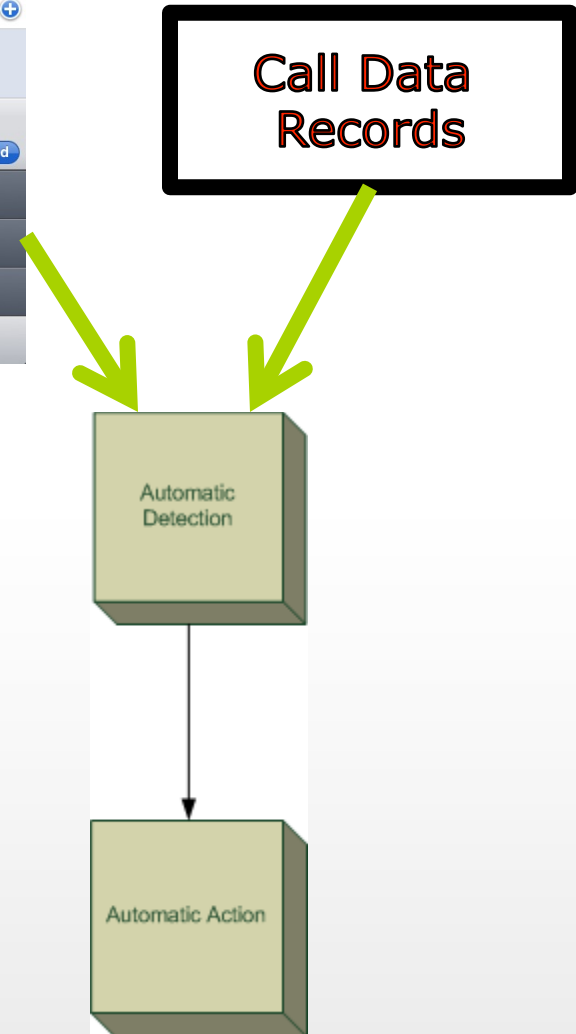


# Short Term Defense

- 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



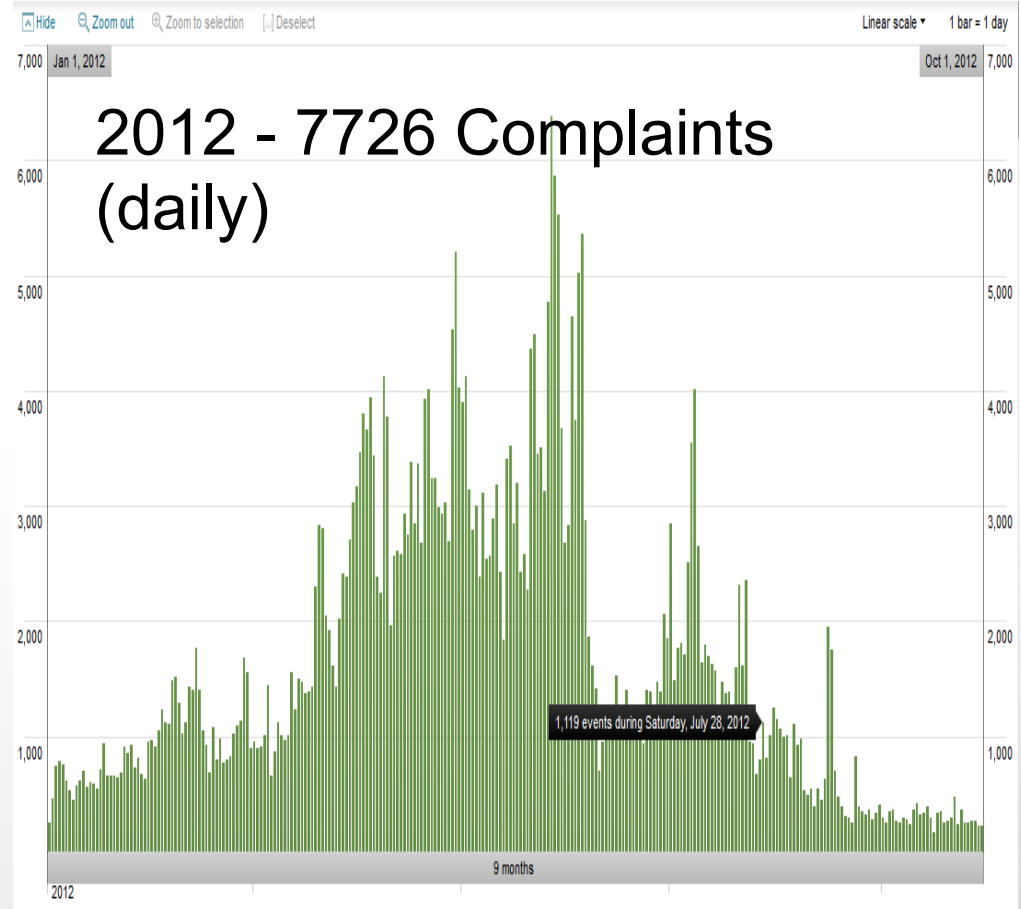
**Call Data  
Records**



# US Domestic Spam Status

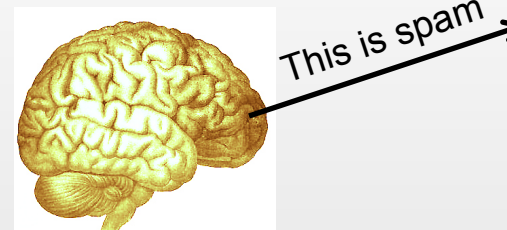
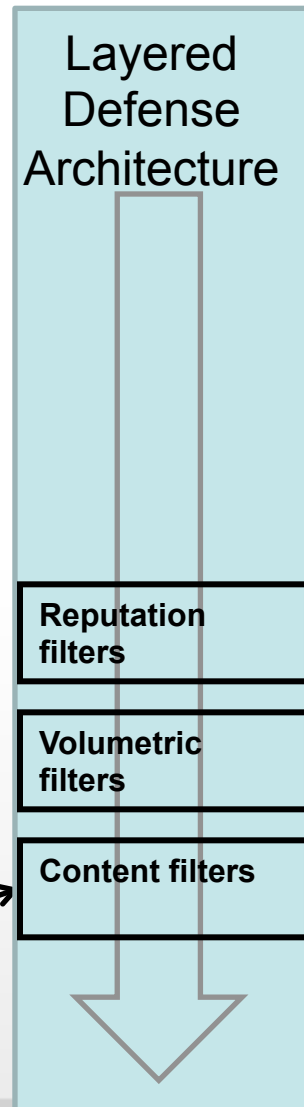
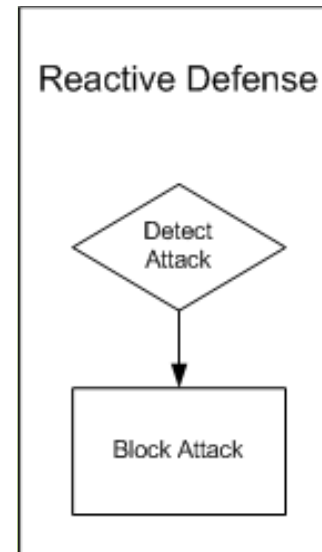
## Now Under Control: iPhone/iPad/Gift Card Spam

- 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



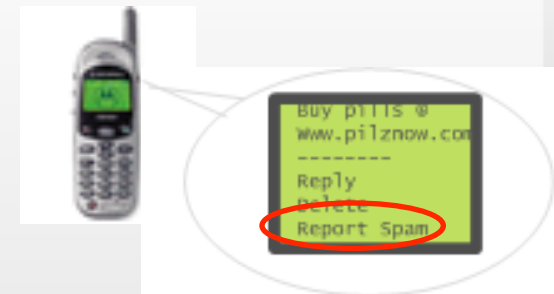
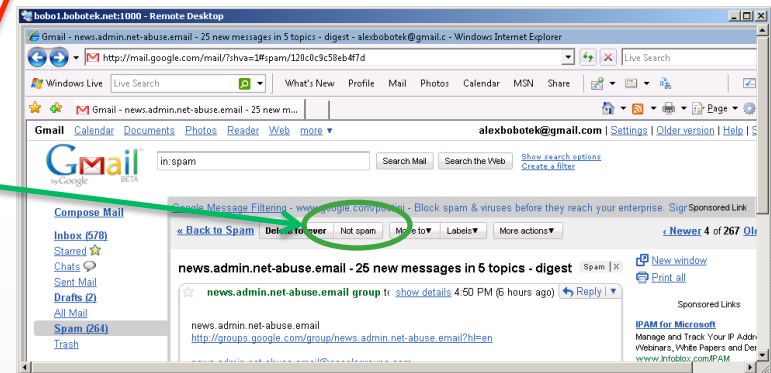
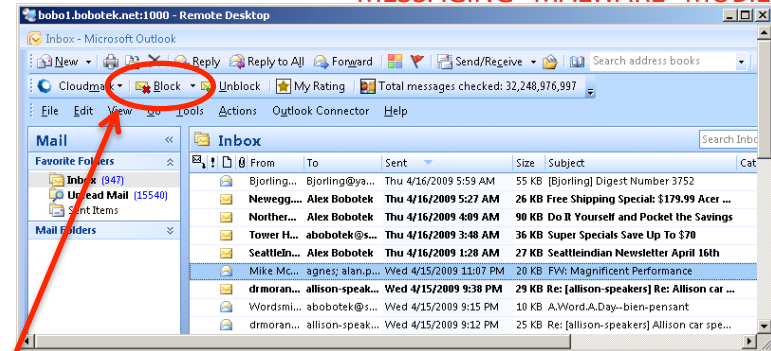
# Filter Defense (takes time/resource)

- 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



# 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



# 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 the address bar showing `bestbuy.thetopoffers4u.com/?t_id=QvCEUX8AAAEAFnWDOIAAAAR&spid=260055&sub=2548`. The browser's developer tools are open, showing the Network tab with a list of requests. The selected request is a GET request to `http://j.mp.realtraq.net/aff_r?offer_id=3854&aff_id=2548&redirect_%2Faffiliate.abltrk.com%2Frd%2F.php%3Faid%3D20%26pub%31%3D%26c3%3D1022d594d34ee6367a5dc65825246`. The page content below the logs features a Best Buy advertisement for a free \$1000 gift card, with a form to enter an email address and a 'Continue' button. A small 'Inspect Network Request' window is overlaid on the page, showing the details of the selected request.

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://j.mp.realtraq.net/aff\_c?offer\_id=3854&aff\_id=2548 [HTTP/1.1 302 Found 217ms]  
00:23:52.766 GET http://j.mp.realtraq.net/aff\_r?offer\_id=3854&aff\_id=2548&redirect\_%26c3%3D1022d594d34ee6367a5dc65825246 [HTTP/1.1 200 OK 42ms]  
00:23:52.906 GET http://j.mp.realtraq.net/aff\_r?offer\_id=3854&aff\_id=2548&redirect\_%26c3%3D1022d594d34ee6367a5dc65825246 [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=1022d594d34ee6367a5dc65825246 [HTTP/1.1 302 Found 305ms]  
00:23:53.318 GET http://hp.squareclk.com/183/sr?\_qse=ahRfcD0xN...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]

bestbuy.thetopoffers4u.com

**BEST BUY**

GET A FREE \$1000 BEST BUY GIFT CARD

Participation Required, [Click for Details](#)

Please complete the following steps:

1. Enter Your E-mail Address:

[Continue >](#)

Inspect Network Request

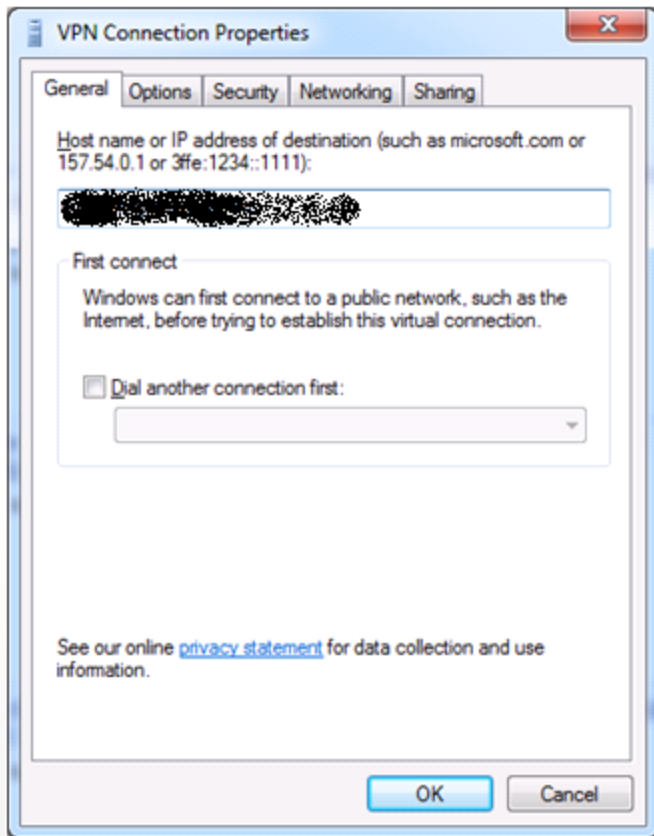
Request URL: http://j.mp.realtraq.net/aff\_r?offer\_id=3854&aff\_id=2548&redirect\_%2Faffiliate.abltrk.com%2Frd%2F.php%3Faid%3D20%26pub%31%3D%26c3%3D1022d594d34ee6367a5dc65825246

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 ad asks the user to answer a question: "Wie is de nieuwe CEO van Apple?" with two options: "Hitaka Mishamo" and "Tim Cook". Below the ad, there 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 errors and successful GET requests. 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.

```
Firefox
Search - SRS - Splunk 4.3.1
Test de QI - Testez votre QI et compa...
www.funfone.me/1p/2472/?af=868&uc=14050800249_e632d1_3fa_73_4fa8d078
Net CSS JS Logging
Declaration dropped.
00:50:06.701 ▲ Expected end of value but found '5'. Error in parsing value for 'font-family'. data
Declaration dropped.
00:50:06.706 ▲ Expected end of value but found '('. Error in parsing value for 'font-family'. data
Declaration dropped.
00:50:07.131 POST http://clients.bluecava.com/data/Complete.aspx [HTTP/1.1 200 OK 1201ms]
00:50:08.260 GET http://bcpd.x7y24x365.com/dot.gif?d=5039_-8Addr1-8Addr2-8city-8region-8email-8z= [HTTP/1.1 200 OK 949ms]
00:50:54.022 GET http://carquestionswebsite.com/go/1445-41a1g=6348og-822&id=0&m=0&p=1&c=@ [HTTP/1.1 302 Found 625ms]
00:50:54.702 GET http://aff.mobileimp.com/geo/preset/2037_tpp_id_da3060c0610c3405c4db99cf9d35e5ef [HTTP/1.1 200 OK 984ms]
00:50:55.810 GET http://cdnw.mobileimp.com/background_loader/getJS/exittraffic.js [HTTP/1.1 200 OK 946ms]
00:51:16.032 GET http://www.trafficimp.com/geo/preset/4204/49 [HTTP/1.1 200 OK 871ms]
00:51:17.154 GET http://aff.adimps.com/conversion/visit?xx=3_49_e632d1_3fa_73_4fa8d078_1f061bab_0_0_0_2 [undefined 782ms]
00:51:17.915 GET http://www.fr.funfone.me/1p/2472/?af=868_4fa8d078_1f061bab_0_0_0_2&af_e=25d9652c [HTTP/1.1 200 OK 902ms]
00:51:18.760 GET http://www.fr.funfone.me/javascripts/jquery.js?1336391266 [HTTP/1.1 200 OK 618ms]
00:51:18.797 GET http://www.fr.funfone.me/javascripts/check/208.js?1336391266 [HTTP/1.1 200 OK 360ms]
00:51:18.843 GET http://www.fr.funfone.me/javascripts/main.js?1336391266 [HTTP/1.1 200 OK 374ms]
00:51:18.890 GET http://www.fr.funfone.me/1p/2472/img/question1.gif [HTTP/1.1 200 OK 566ms]
00:51:18.974 GET http://www.fr.funfone.me/1p/2472/img/208/continue.gif [HTTP/1.1 200 OK 679ms]
00:51:19.000 GET http://www.fr.funfone.me/1p/2472/img/question3.jpg [HTTP/1.1 200 OK 1234ms]
00:51:19.057 GET http://www.fr.funfone.me/1p/2472/img/flag1.jpg [HTTP/1.1 200 OK 514ms]
00:51:19.095 GET http://www.fr.funfone.me/1p/2472/img/flag2.jpg [HTTP/1.1 200 OK 514ms]
00:51:19.141 GET http://www.fr.funfone.me/1p/2472/img/flag3.jpg [HTTP/1.1 200 OK 1012ms]
00:51:19.166 GET http://www.fr.funfone.me/1p/2472/img/flag4.jpg [HTTP/1.1 200 OK 580ms]
00:51:19.212 GET http://www.fr.funfone.me/1p/2472/img/question7.jpg [HTTP/1.1 200 OK 1076ms]
00:51:19.247 GET http://www.fr.funfone.me/images/smspluslogo.jpg [HTTP/1.1 200 OK 773ms]
00:51:19.289 GET http://www.fr.funfone.me/1p/2472/img/steps/step1.gif [HTTP/1.1 200 OK 865ms]
00:51:19.466 GET http://www.fr.funfone.me/1p/2472/img/208/index.jpg [HTTP/1.1 200 OK 1540ms]
00:51:31.066 GET http://www.fr.funfone.me/1p/2472/img/steps/step2.gif [HTTP/1.1 200 OK 361ms]

Entraînez votre cerveau grâce à nos jeux cérébraux/de QI sur votre
Testez votre QI
Quel est votre niveau d'intelligence?

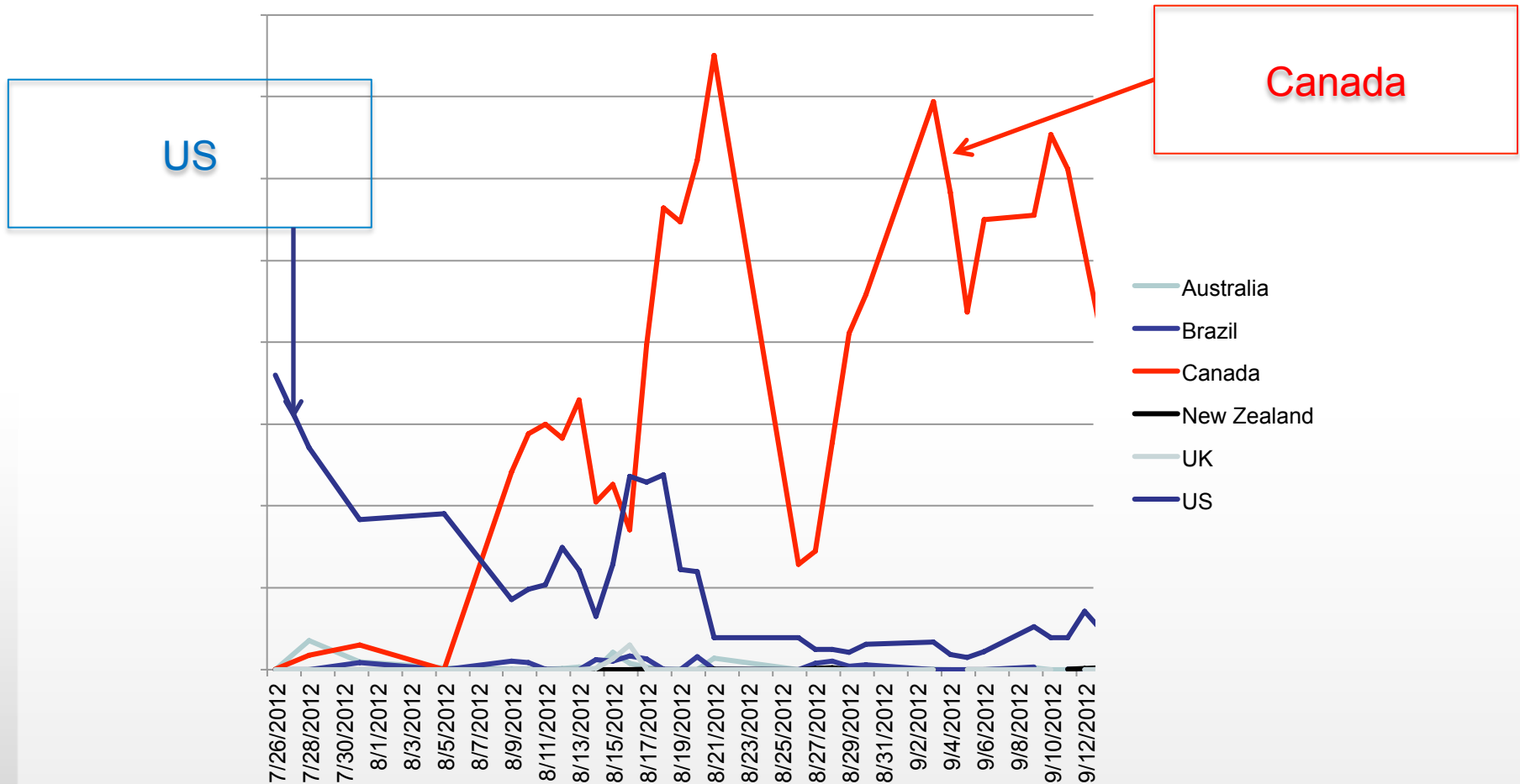
Génie = 140 ou plus
Très intelligent = 120 - 139
Intelligence moyenne = 80 - 119
Idiot = 79 ou moins

2. Quel est le chiffre qui doit suivre dans cette série ? 3, 5, 8, 13, 21,.....
 4
 21
 34

Le qi moyen est considéré comme l'« intelligence normale ».
A quel point vous croyez-vous intelligent?

Continuer >>>
```

# New Spam Plan: Spam Canada Instead



# 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



# 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

# Global Solutions – Overview

- Botnets (and other online threats) are **criminal problems** that require a multidisciplinary approach to solve. No one part of the Internet ecosystem can adequately address botnet and malware threats.
- The most interesting solutions may come at the intersection of different sectors and of social, economic and political concerns. **Require careful balancing**
- **Operational Validity:** A result (report, technology, capability, practice, policy, or process) is operationally valid when it delivers in practice the measurable properties it was intended to deliver.
- Service Providers are capable of **evaluating the tradeoff between business agility and security** and use this data to inform decisions to implement solution.
- Metrics programs help **demonstrate activity and progress** as well as provide crucial data to industry to better understand the size, scope and effectiveness of the problem and potential solutions.

# Public Policy – M<sup>3</sup>AAWG Objectives



Providing organizations/agencies/governing bodies with technical expertise including operational best practices inputs.

Recent Example: The newly published [Best Practices to Address Online and Mobile Threats](#) was developed by M<sup>3</sup>AAWG and the London Action Plan to encourage governments to implement the proven strategies, the best practices report was presented to the 34-member countries of the [OECD](#) (Organisation for Economic Co-Development) for review by M<sup>3</sup>AAWG members on Oct. 15 with Industry Canada.

Providing Industry support for proposals/initiatives that help the anti-abuse industry efforts regardless of the organization/agency/governing body including technical or operational rationale for the support.

Recent Example: The policy proposals we supported to improve the Abuse Contact Information in the WHOIS Database found consensus at APNIC, <http://www.apnic.net/policy/proposals/prop-079>, AfrinIC <http://afrinic.net/en/library/policies/current/698-abuse-contact-information-in-the-afrinic-service-region>, and last month at RIPE <http://www.ripe.net/ripe/docs/current-ripe-documents/ripe-563>

# Collaboration Next Steps for Workshop



- Michael O'Reirdan – M<sup>3</sup>AAWG Co-Chairman
- Alex Bobotek – M<sup>3</sup>AAWG Co-Chairman



# Collaboration Next Steps – Group 1

- Information sharing framework
- Security framework
- Best practices
- User education
- Working with government and regulators
- Overall theme is building trust – Potential first steps
  - Leverage existing info sharing body
  - Find list of “challenges” in local environment
    - Start by tackling “low hanging fruit” project
  - Determine primary focus areas
  - Utilize a knowledge management system

# Collaboration Next Steps – Group 2



- Create M<sup>3</sup>AAWG India chapter
  - Collaboration of industry partners
    - ISPs
    - Mobile service providers
    - Email service providers
  - Guidelines on data sharing to deal with:
    - Phishing
    - Spam
    - Scams
    - Malicious URLs
    - Known bad IP addresses
- Training required
  - DMARC.org
  - Outbound spam mitigation

# Discussion and Conclusions



## Discussion and Conclusions

# Closing

**More Information and Complete  
Monday Workshop Presentations at  
[www.M3AAWG.org/India/](http://www.M3AAWG.org/India/)**

**Contact: [Jerry.Upton@m3aawg.org](mailto:Jerry.Upton@m3aawg.org)**

**Thank You**