Stopping Cyberspace Pollution – International Cooperation on Fighting Spam and Botnets (including readout from Monday M³AAWG workshop)

Michael O'Reirdan – M³AAWG Co-Chairman
Zhou Yonglin – Director, Internet Society of China
Alex Bobotek – M³AAWG Co-Chairman

Objective and Agenda

M3AAWG
MESSAGING MALWARE MOBILE

- Introductions and Objectives for the Interest Seminar
- Update – "China-U.S. Fighting Spam to Build Trust" report, recommendations and best practices
- Summary of Monday M3AAWG Workshop
- Collaboration Next Steps for Workshop
- Discussion

China – U.S. Progress Update

M3AAWG
MESSAGING MALWARE MOBILE

"China-U.S. Fighting Spam to Build Trust" report, recommendations, and best practices

- Zhou Yonglin – Director, Internet Society of China

Summary of Monday M³AAWG Workshop

- Michael O'Reirdan – M³AAWG Co-Chairman
- Alex Bobotek – M³AAWG Co-Chairman

The Spam Problem
Threat Picture

M3AAWG
MESSAGING MALWARE MOBILE

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?

M3AAWG
MESSAGING MALWARE MOBILE

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^{3}AAWG India?
- Coordination and targeted information sharing

The Spam Problem
How Indian email marketers can help

- Adopt the M³AAWG 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
  M³AAWG, ESPC, and of course, IAMAI

The Spam Problem
Government & Law Enforcement – Suggestions

M3AAWG
MESSAGING MALWARE MOBILE

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, M3AAWG, OECD WPISP …

The Bot Problem
Policy is key

M3AAWG
MESSAGING MALWARE MOBILE

- 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

M3AAWG
MESSAGING MALWARE MOBILE

- 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

M3AAWG
MESSAGING MALWARE MOBILE

- 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

M3AAWG
MESSAGING MALWARE MOBILE

- 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

M3AAWG
MESSAGING MALWARE MOBILE

- 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

M3AAWG
MESSAGING MALWARE MOBILE

- 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 8th 2011, 7 arrests, servers and cash seized
- DNSs run by ISC from Nov 8th 2011 to June 9th 2012
- Need to remediate end users
- Interesting statistics
  - Do nothing ISP -40%
  - Active ISP -80%

M3AAWG
MESSAGING MALWARE MOBILE

The Mobile Problem

- Alex Bobotek – M3AAWG Co-Chairman

Desired Outcomes

M3AAWG
MESSAGING MALWARE MOBILE

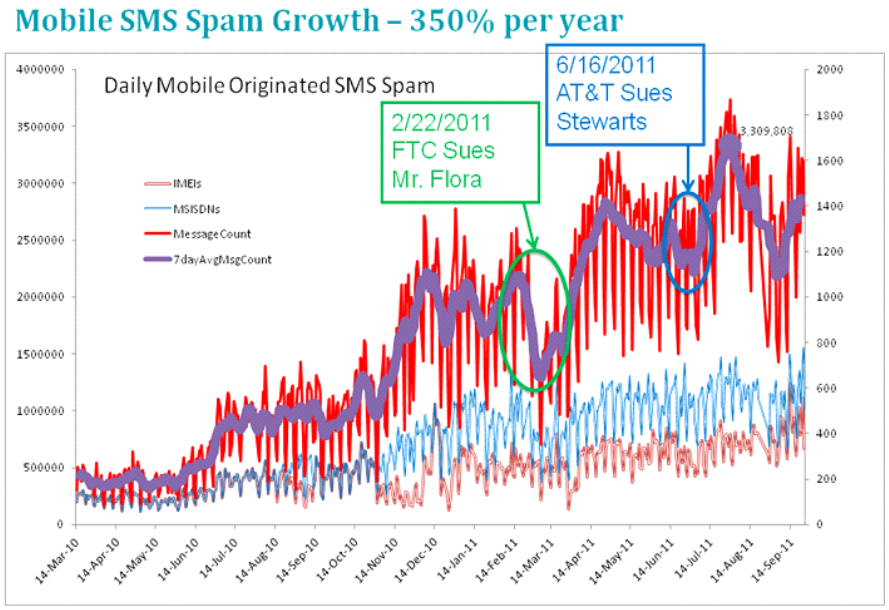
1. Deploy “This is Spam” reporting

2. Deploy spam filters in SMS messaging

3. International collaboration
   - Enforcement
   - Abuse data exchange
   - Attend forums (M^{3}AAWG, GSMA, …)

History: North American SMS Spam 2010

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



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

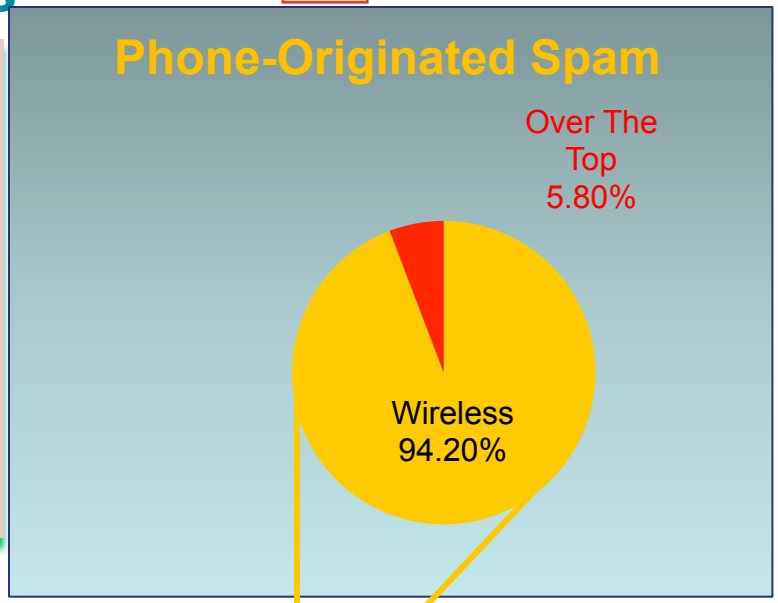
- **SIM Shutdown (late 2010)**
  - Detect by 7726 spam reporting
  - Shut down SIMs after 5-10 days
  - Attacker buys new SIMs
  - Spam continues
- **Lawsuits**
  - Spammer sued after many months
  - Spammer stops for weeks
  - Spam continues

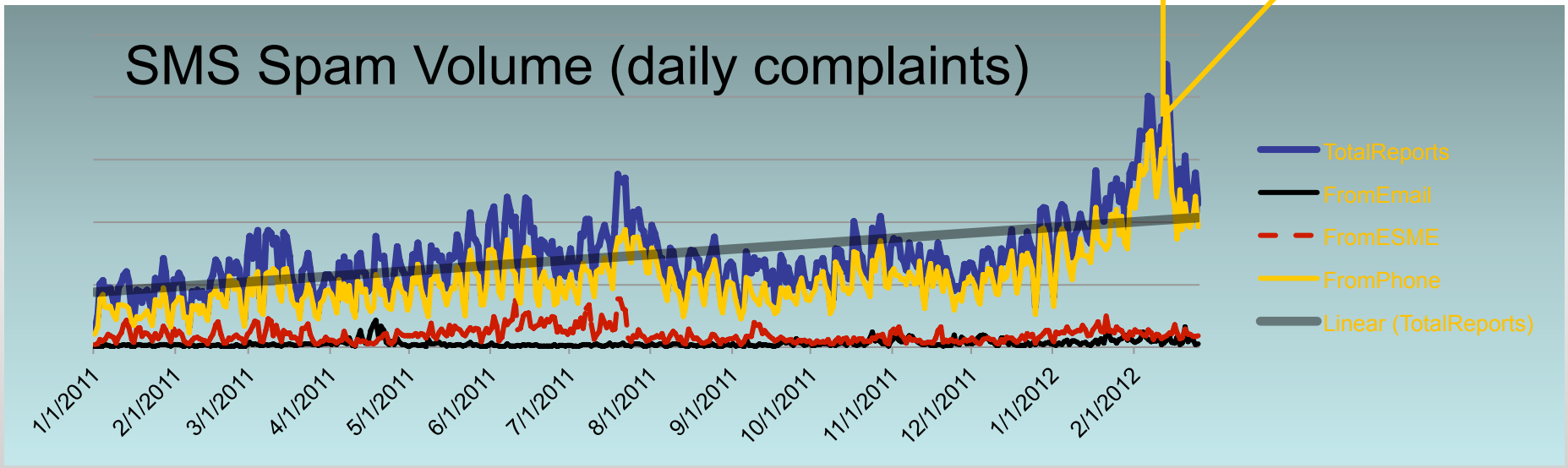
Spam Control (India)

- 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

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

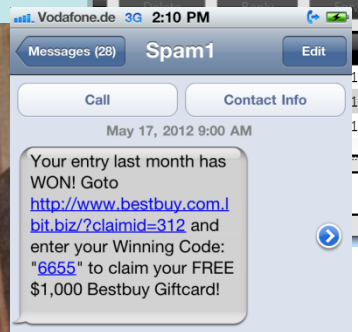
Text message spam has started waking Bob Dunnell in the middle of the night, promising cheap mortgages, credit cards and drugs. Some messages offer gift cards to, say, Walmart, if he clicks on a Web site and enters his Social Security number.

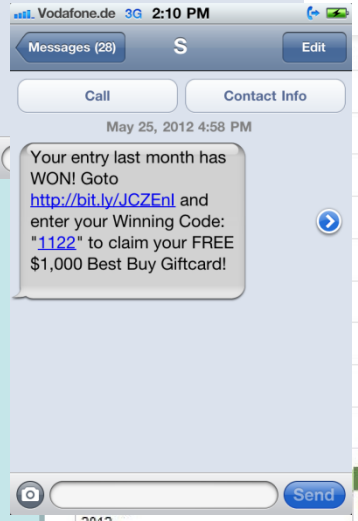
Once the scourge of e-mail providers and the Postal Service, spammers have infiltrated the last refuge of spam-free communication: cellphones. In the United States, consumers received roughly 4.5 billion spam texts last year, more than double the 2.2 billion received in 2009, according to Ferris Research,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

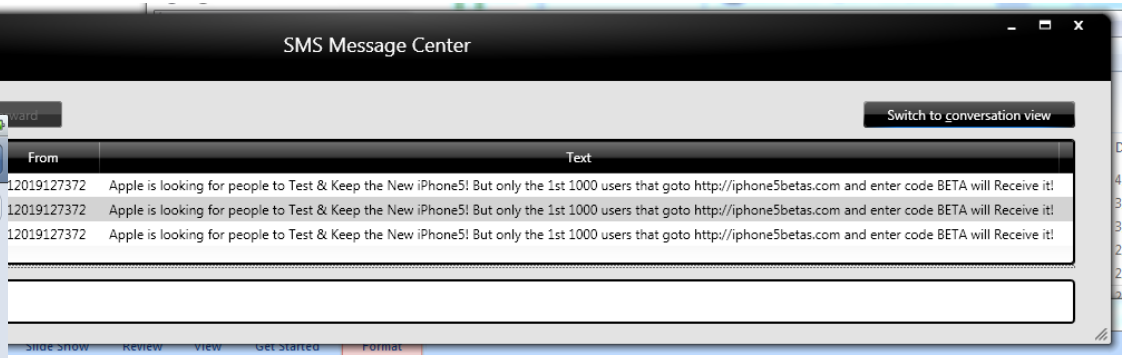
Spread over 250 million text message-enabled phones, the problem is not as commonplace as e-mail spam. But it is a growing menace, with the potential for significant damage.

“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

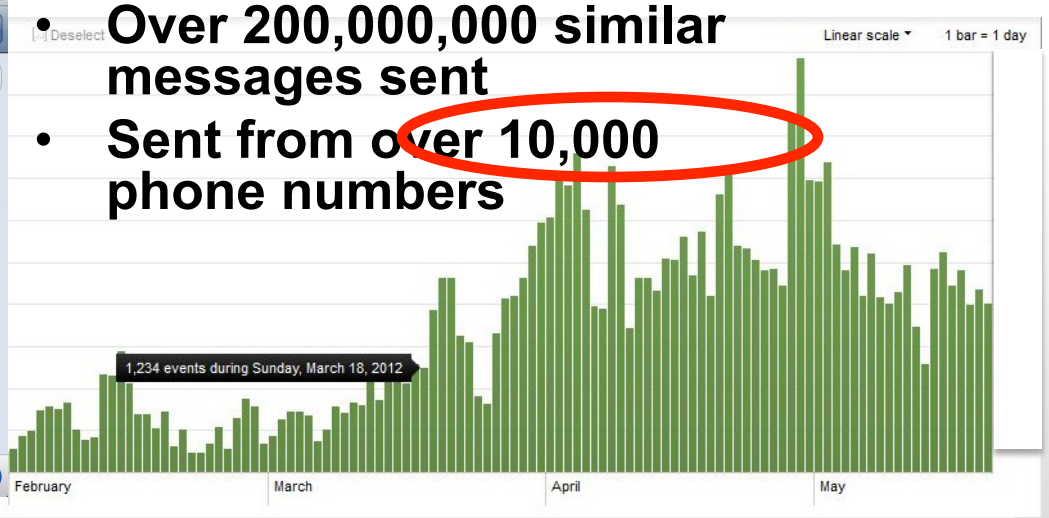
Continued on Page 4







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

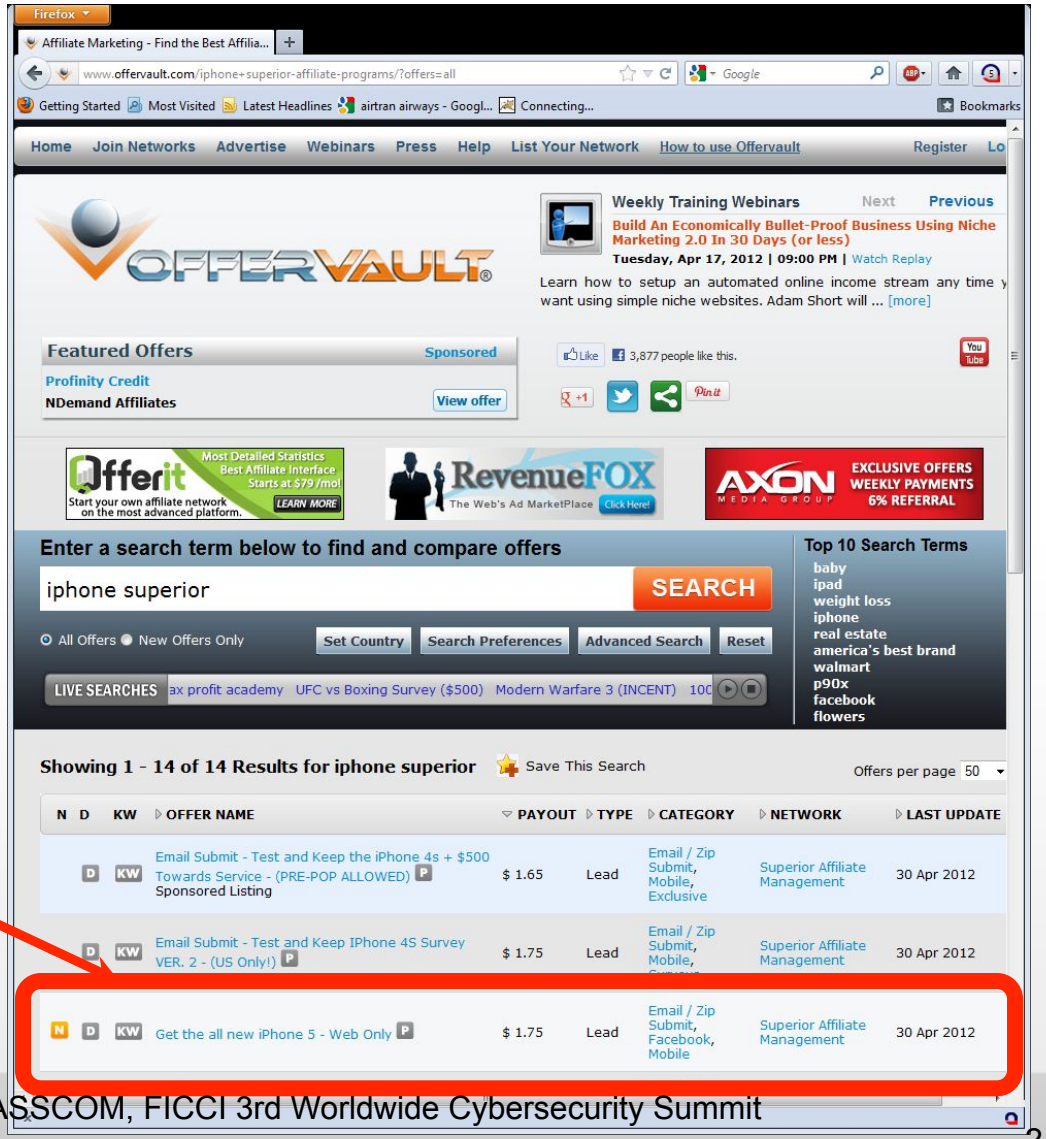


iPad/iPhone/GiftCard Scam Complaint rate

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

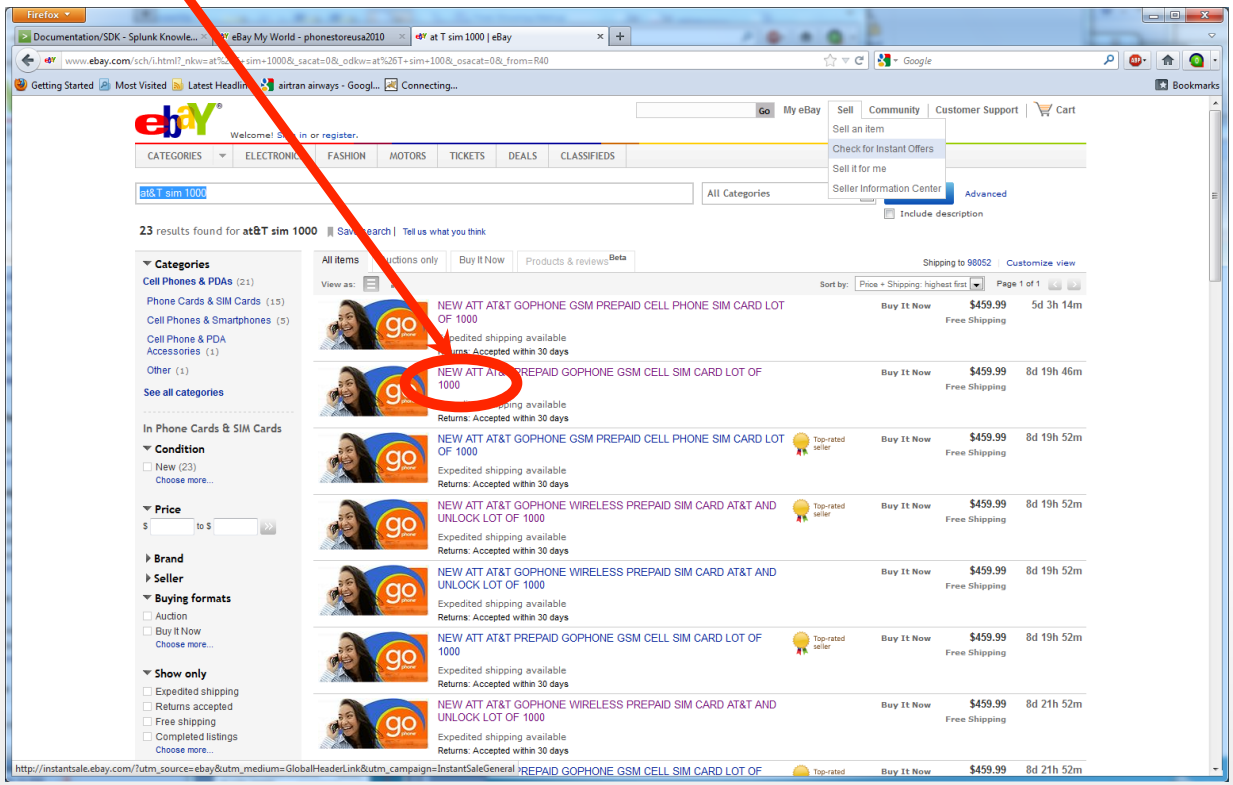


How Affiliates Make Mobile Spam

Boxes of of cheap anonymous SIMs

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

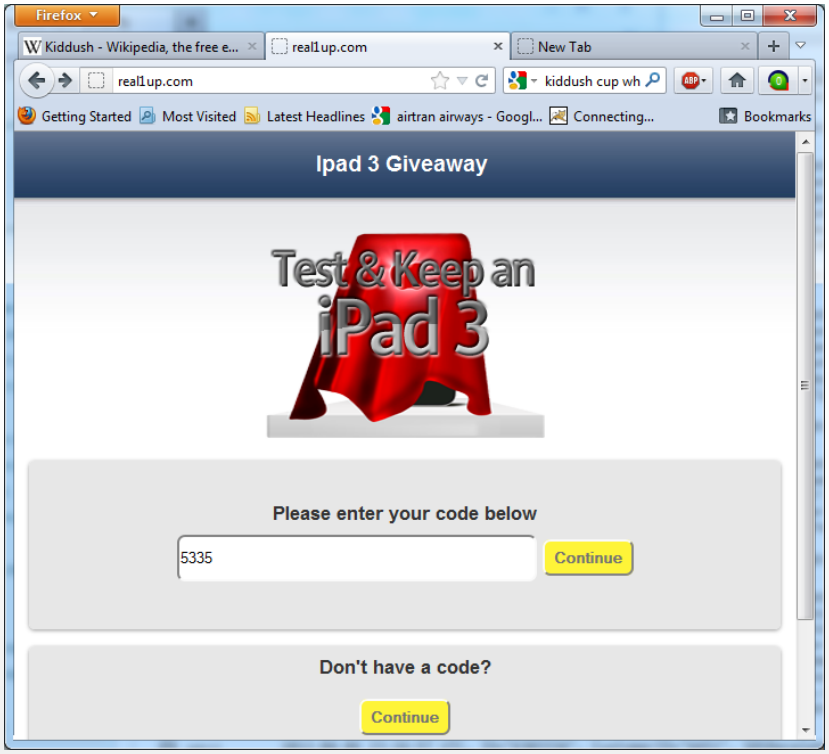
- Bulk SIMs - $0.46 each on eBay
- 10, 100, 1000, 10,000, name your lot size
- Overwhelms manual shutdown defense

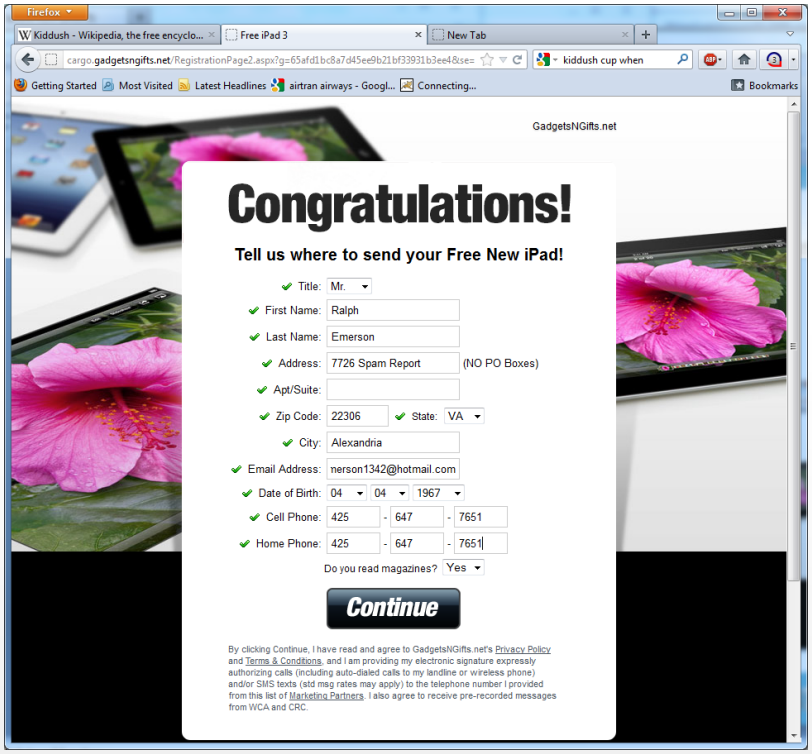


SMS Spam

MESSAGING MALWARE MOBILE

Visiting the spamvertized website …

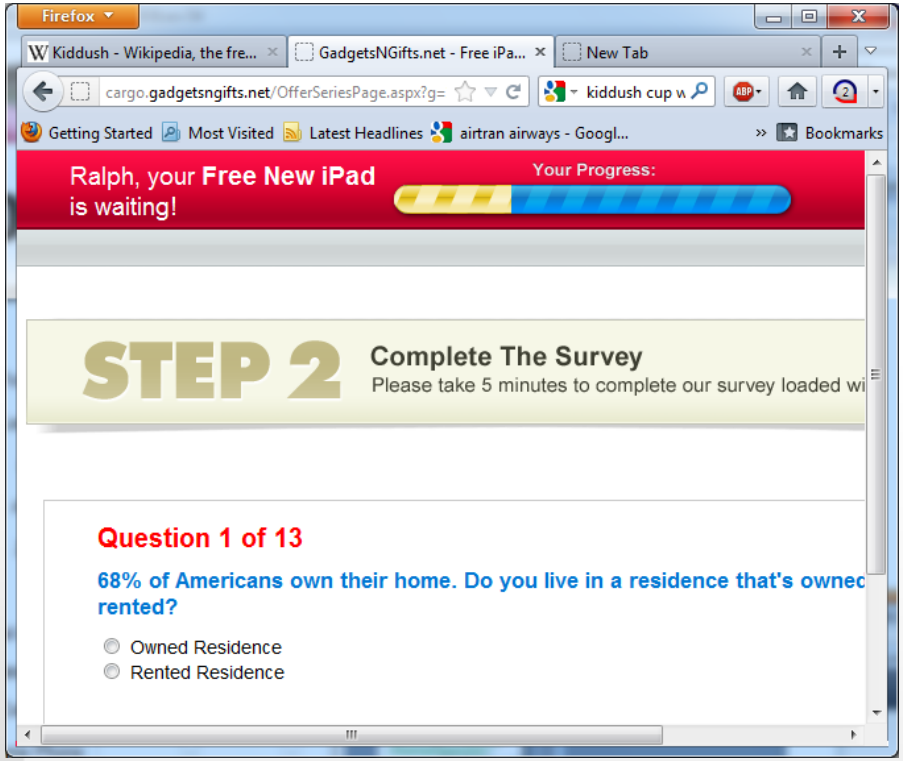


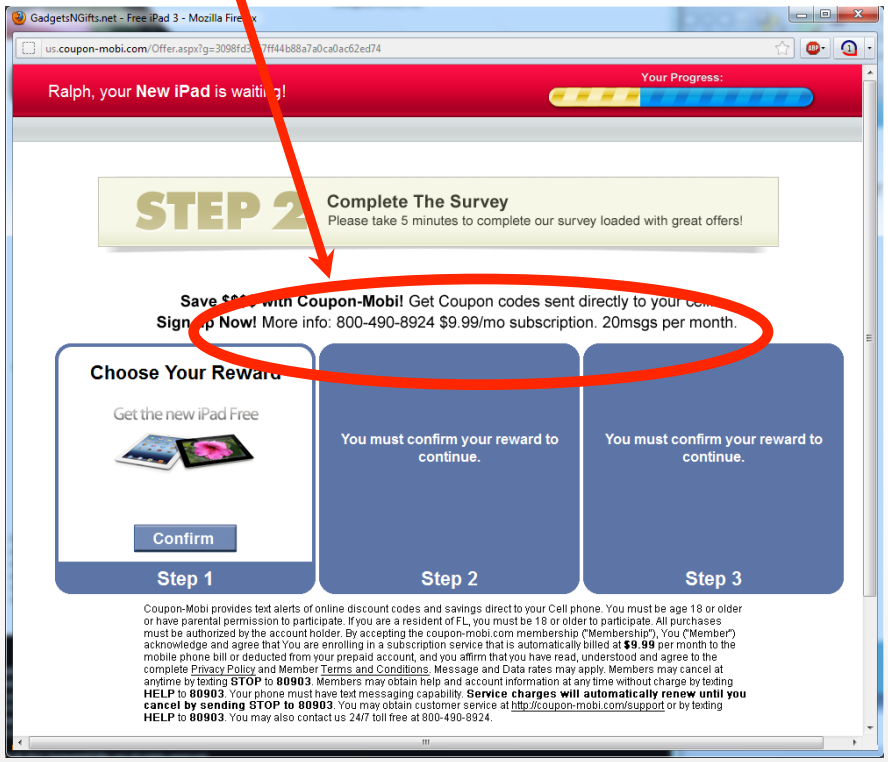


Monetization

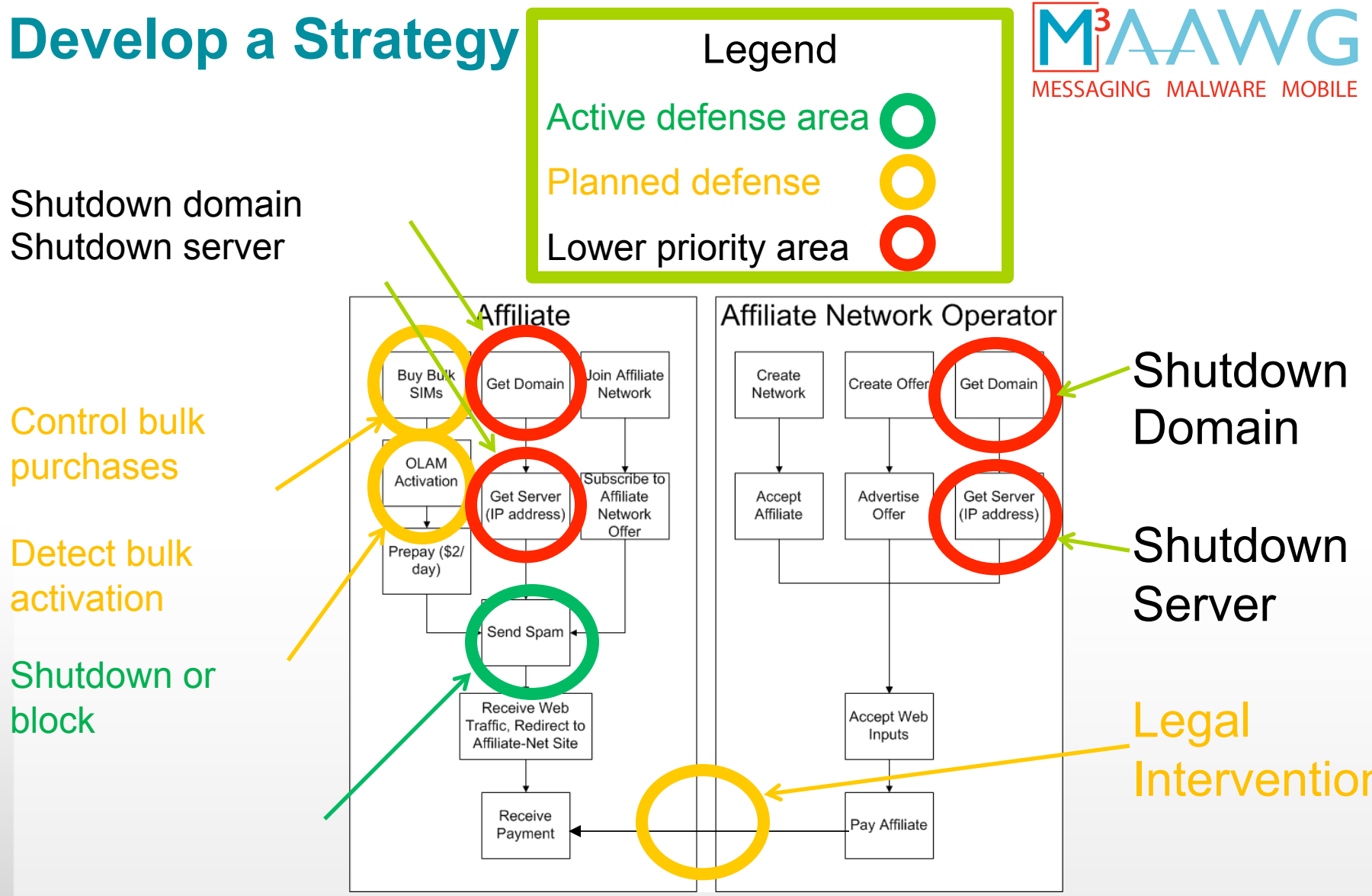
Take a “survey” …

SMS monetization!



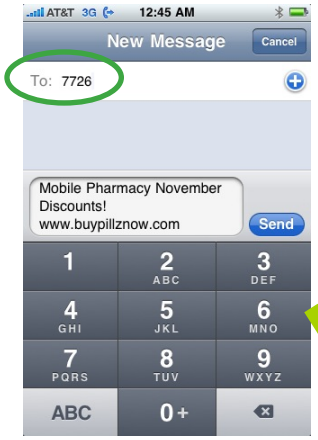


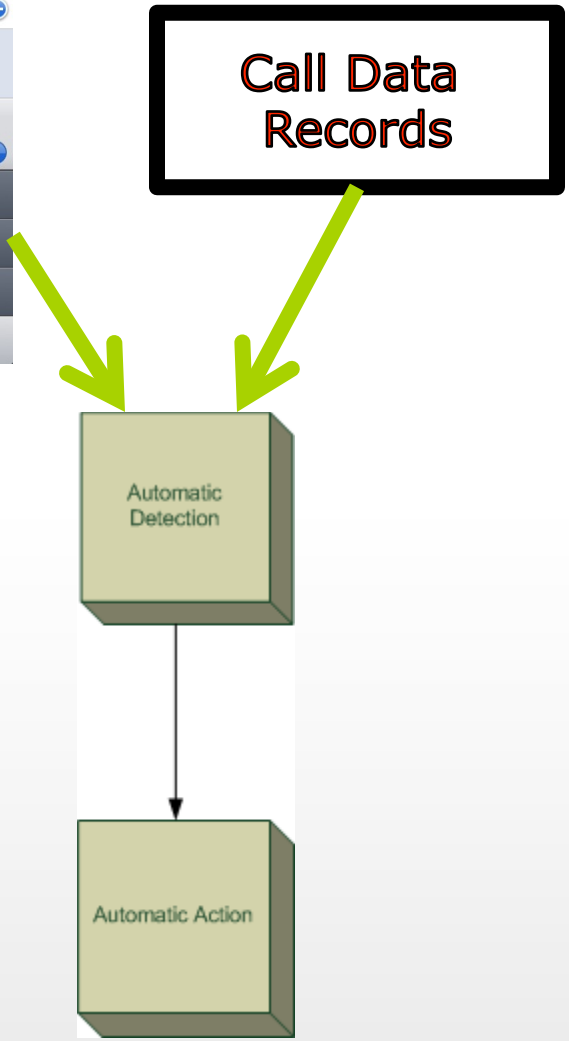
Develop a Strategy



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

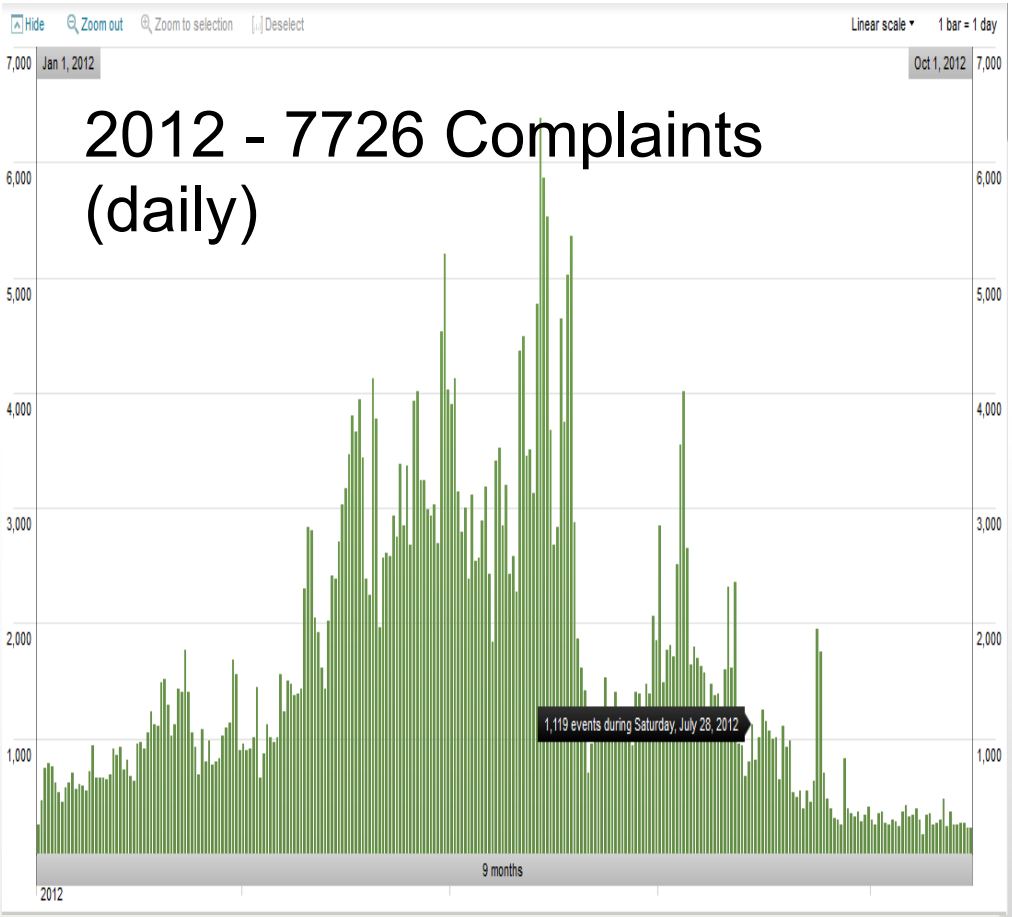
Now Under Control: iPhone/iPad/Gift Card Spam

M3AAWG
MESSAGING MALWARE MOBILE

- **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

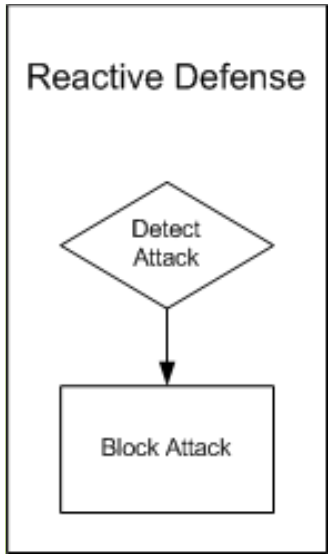
- **Cautions:**
  - **Spammers will return with new methods**
    - **Spoofing**
    - **Malware (Bots)**
      - » **China has active mobile botnet of > 100k phones**
      - » **GGtracker malware infected > 250k US phones**



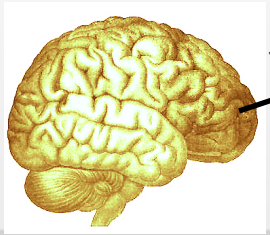
Cooperation on Fighting Spam and Bots | EWI, NASSCOM, FICCI 3rd Worldwide Cybersecurity Summit
New Delhi, India, October 2012

Filter Defense (takes time/resource)

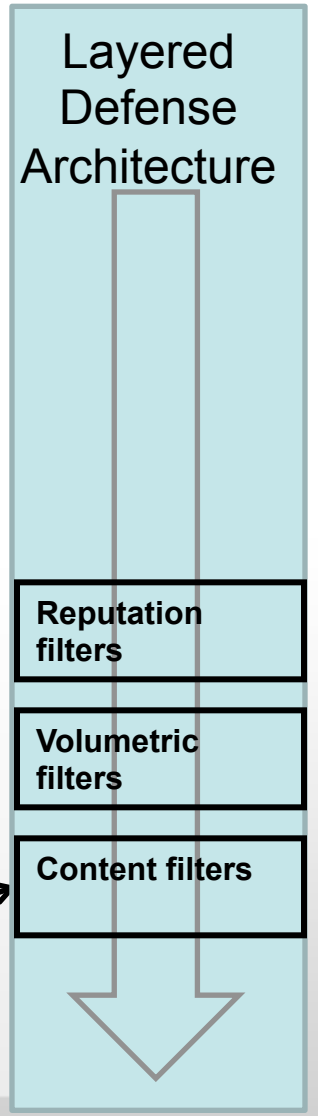
- Deploy spam/virus filters
- Build better spam reporting
  - "This is Spam" button in UA



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



This is spam

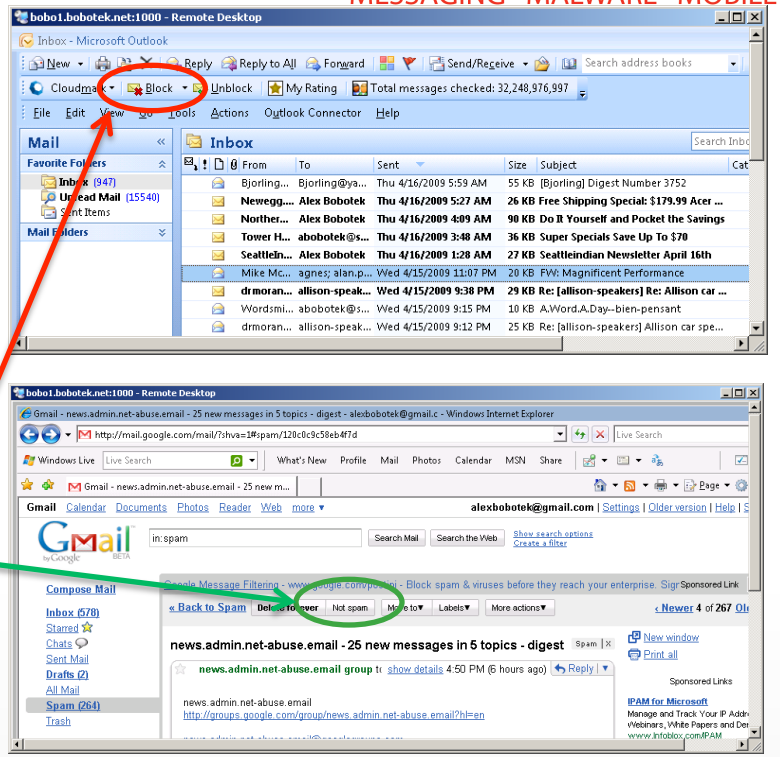


Add a “This is Spam” Button

- **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

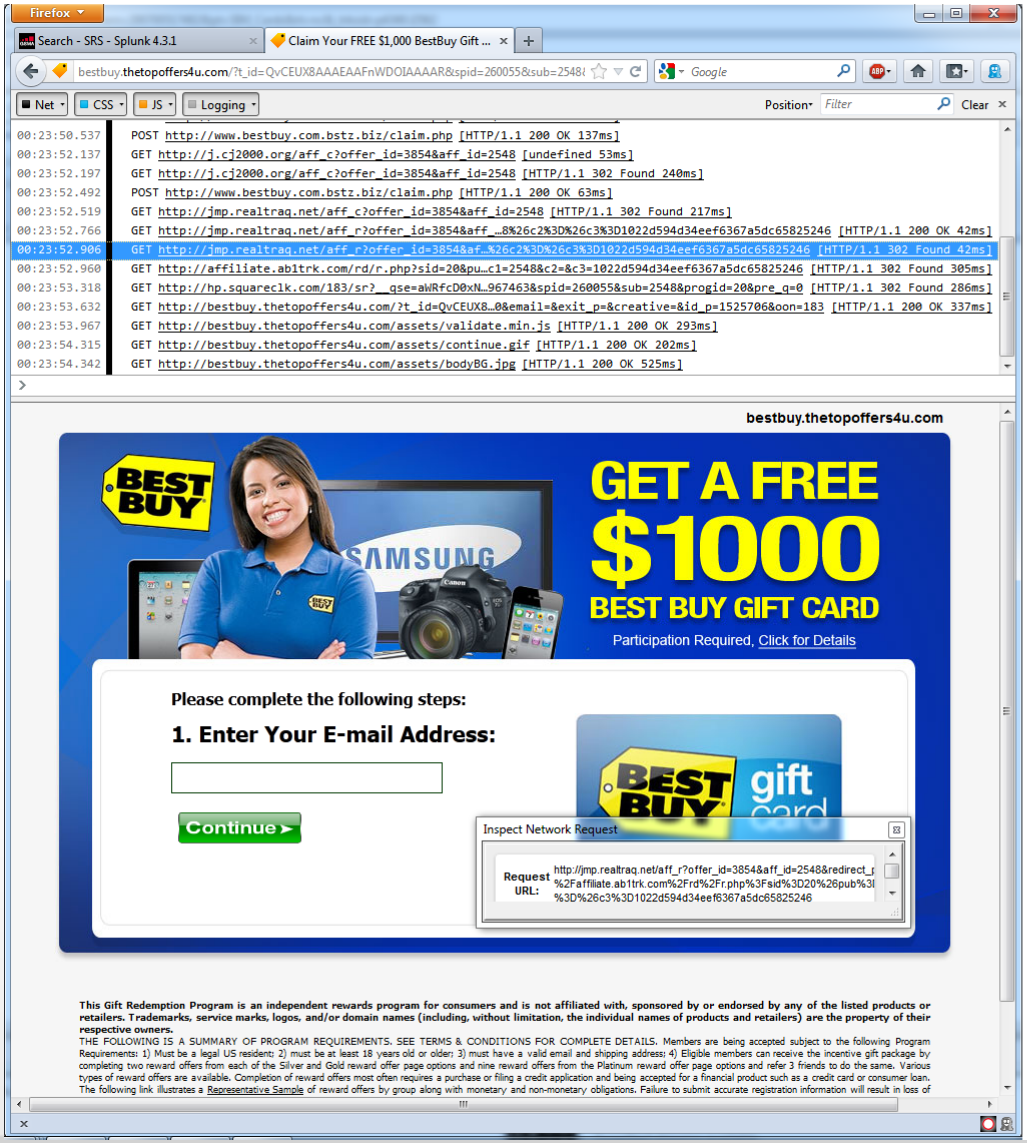


Problems

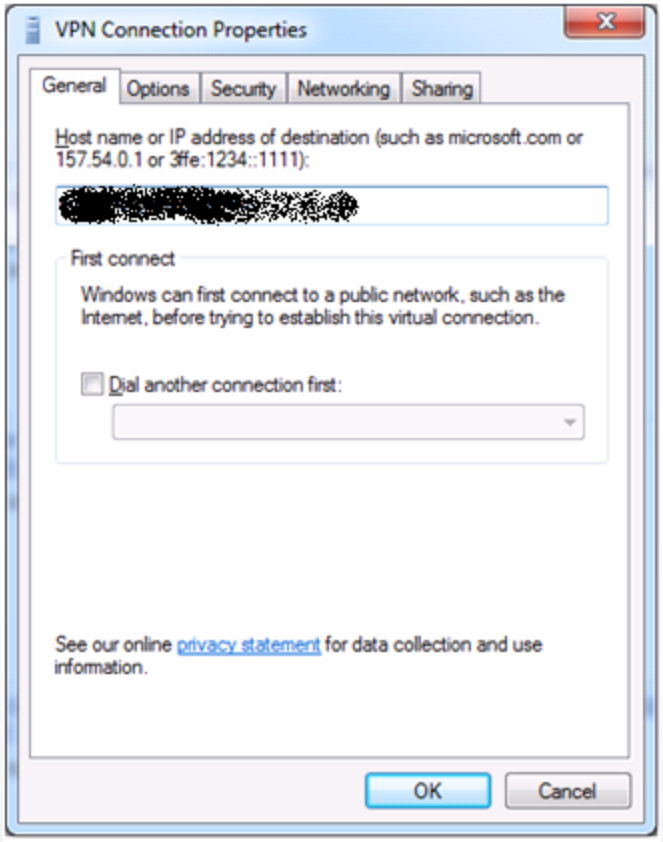
- Growing abuse
  - Spam
  - Malware
  - Fraud
  - Harassment
  - Network disruption
- Growing internationalization of abuse and global homogenization of abuse technologies
  - Toolkits
  - Criminal economy
  - Intra-carrier sensors (e.g., SRS) are effective against attacks which include intra-carrier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

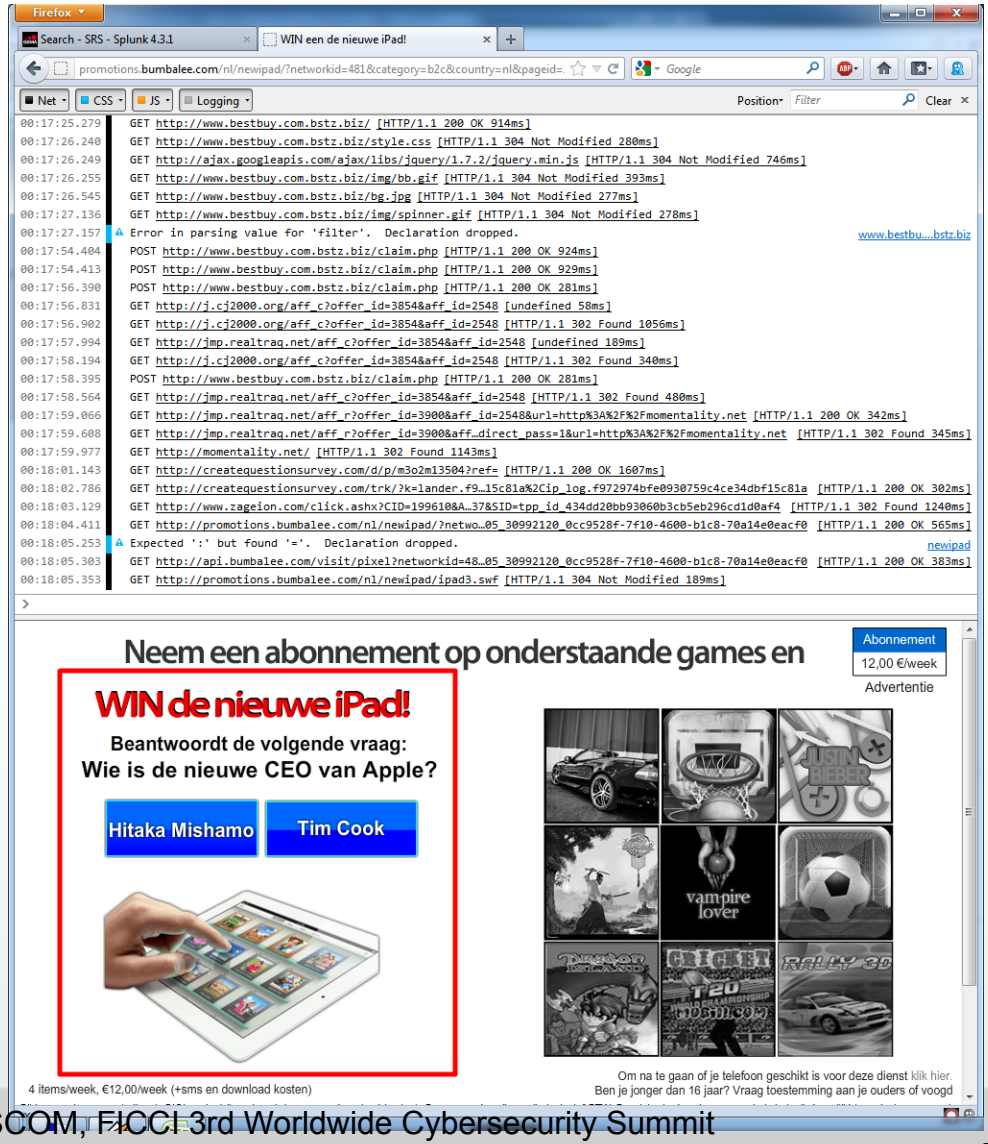
We're fighting a growing and increasingly similar and mobile spam problem across continents and oceans

USA IP Address

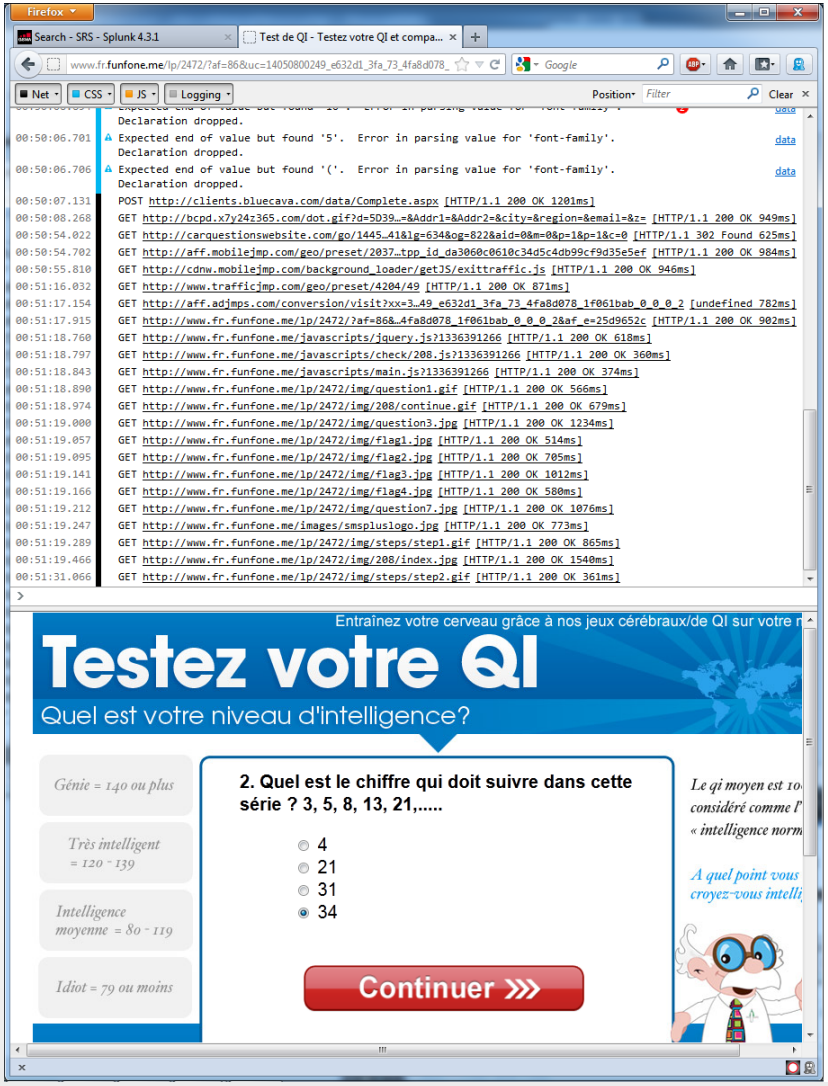


Internationalization – Netherlands IP

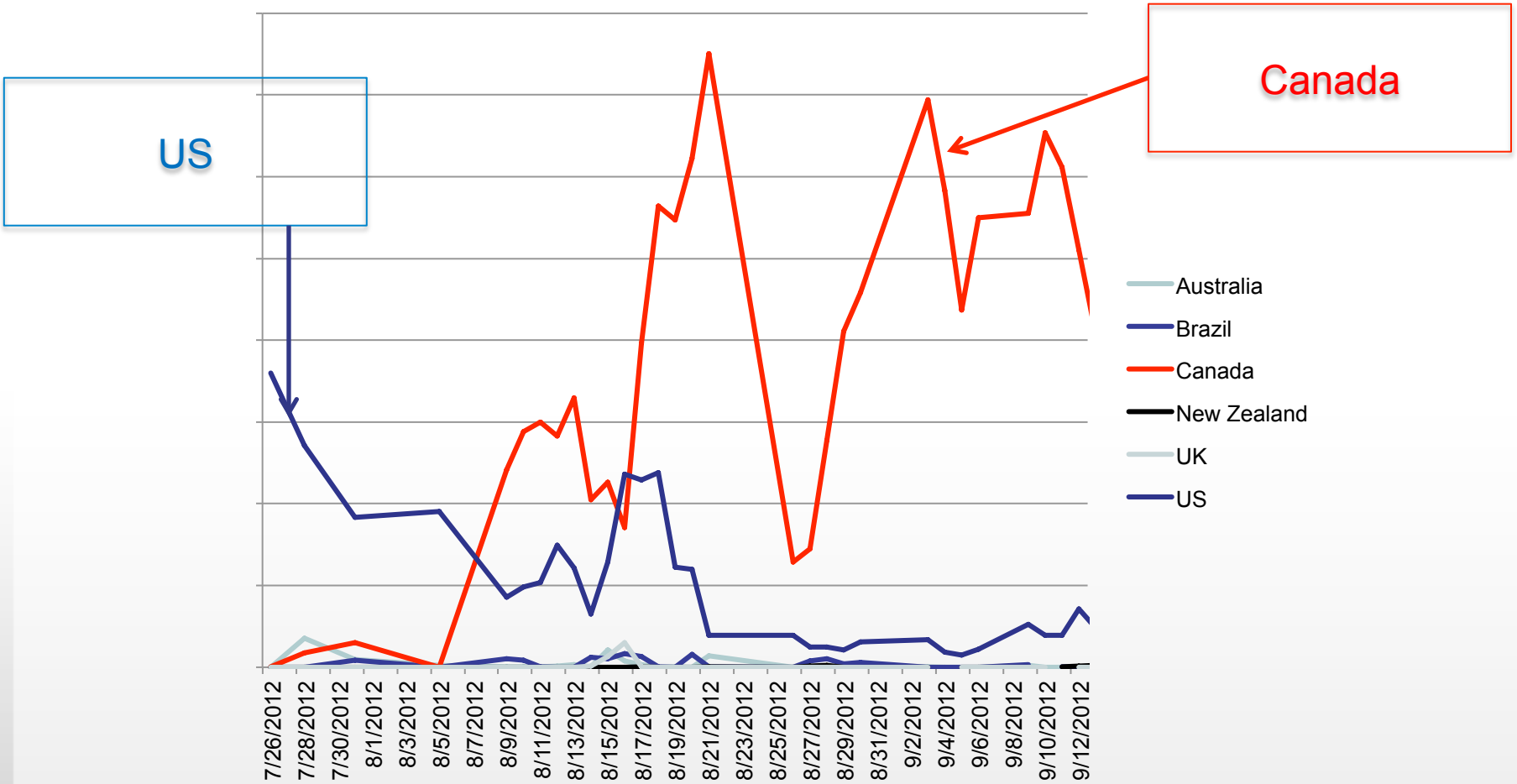




Internationalization – Paris IP Address



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

Cooperation on Fighting Spam and Bots | EWI, NASSCOM, FICCI 3rd Worldwide Cybersecurity Summit
New Delhi, India, October 2012

Needed:
A Framework for Abuse Data Exchange

M3AAWG
MESSAGING MALWARE MOBILE

- **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

M3AAWG
MESSAGING MALWARE MOBILE

- 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

M3AAWG
MESSAGING MALWARE MOBILE

- 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 – M³AAWG 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 M³AAWG 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 M³AAWG 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

M3AAWG
MESSAGING MALWARE MOBILE

- Michael O'Reirdan – M3AAWG Co-Chairman
- Alex Bobotek – M3AAWG 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 M³AAWG 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

M3AAWG
MESSAGING MALWARE MOBILE

Discussion and Conclusions

Closing

M3AAWG
MESSAGING MALWARE MOBILE

More Information and Complete Monday Workshop Presentations at

www.M3AAWG.org/India/

Contact: Jerry.Upton@m3aawg.org

Thank You