ICANN

Internet Corporation for Assigned Names and Numbers

Toronto

August

20 thru 21

2009

Schedule

Thursday, August 20

9:00	**gTLD Registry Continuity Plan Workshop** – *Patrick Jones*
10:30	**Core Planning Team Meeting/Registry Data Escrow** – *Patrick Jones*
11:00	**Coffee**
11:30	**Welcome, Introductions & Key Messages** *Craig Schwartz & Tim Cole*
12:00	**ICANN Policy** – *Margie Milam*
13:00	**Lunch**
14:00	**Registry Presentations**
14:30	**Terminated Registrar Transition Process** – *Mike Zupke*
15:30	**Coffee**
16:00	**New gTLDs** – *Kurt Pritz*
17:30	**Networking / Free Time**
18:00	**Evening Event - Baseball Game** *Sponsored by* Afilias

gTLD Registry Continuity Workshop

Patrick Jones
ICANN Registry Liaison Manager

Workshop Agenda (45-min)

- Continuity Plan Implementation Update
- Continuity Communications
  - Scenario discussion, identify areas of information sharing
  - Coordinating media contacts
  - Communications protocol

Workshop Agenda (2nd 45-min)

- Escrow Testing Update
  - Current Process Test with escrow agents
  - Draft Spec Testing with registries
- New gTLD Applicant Guidebook Language
  - Applicant Evaluation Questions
  - Escrow Specification
  - Performance, Interoperability + Continuity Spec

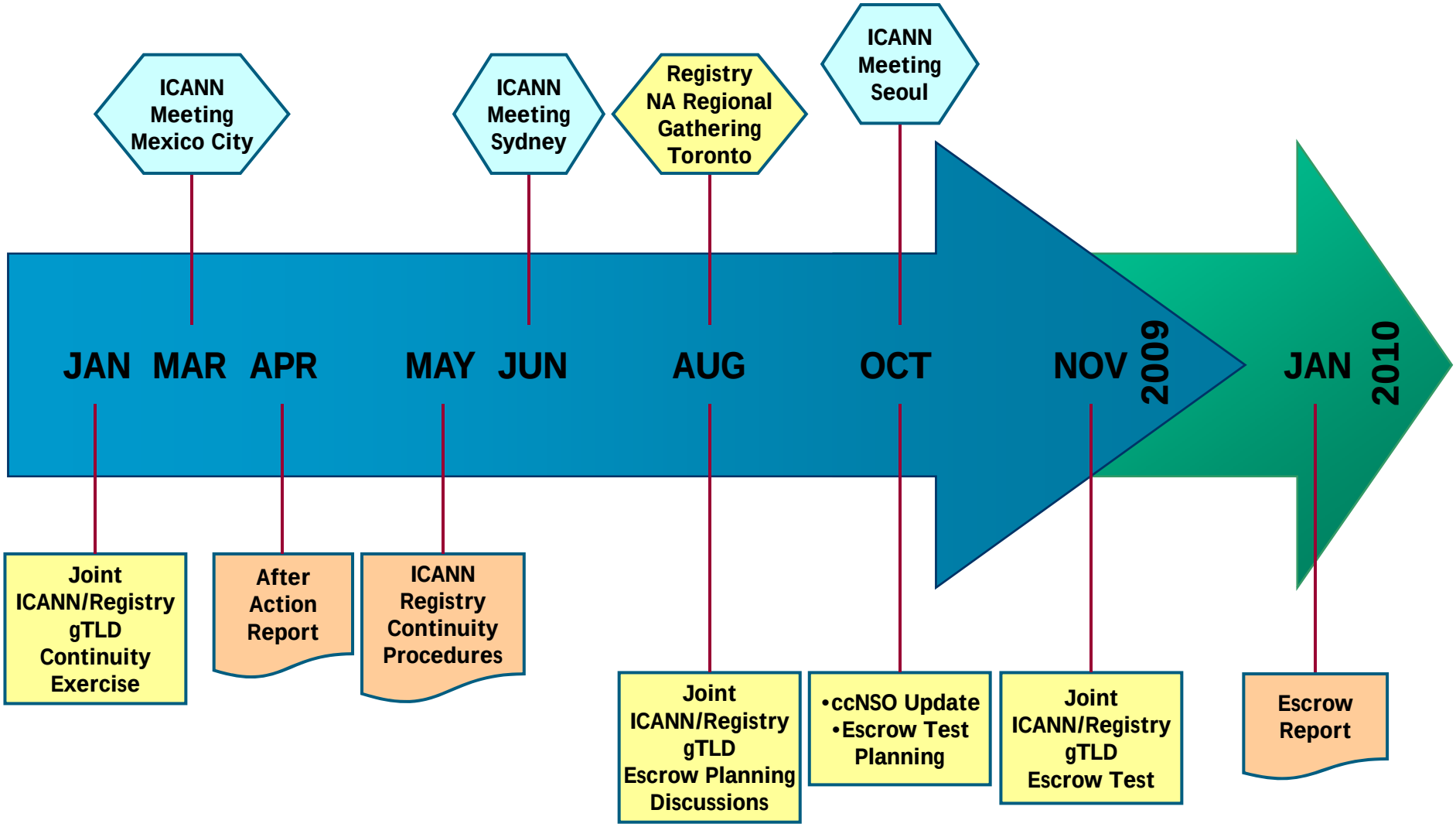
gTLD Registry Continuity Plan Covers

- Information Sharing + Communications
- Situation Handling & Event Management
- Crisis Response
- Business Continuity
- Data Escrow
- TLD Transition
- Registry Closure

gTLD Registry Continuity - Timeline

- Plan Development [Jul 2006-Apr 2008]
- Failover Plan Finalized [Jun-Aug 2008]
- Scenario-Based Table-Top Testing [Jan 2008, Jan 2009]
- Implementation Development [May 2009-Present]
- Data Escrow Technical Testing [Sep-Nov 2009]

gTLD Registry Continuity Plan Timeline 2009-2010



January 2009 Joint Continuity Exercise

- Scenario-based table-top exercise
- 65 participants among Afilias, Neustar, PIR, VeriSign and ICANN
- Designed to validate, test & enhance the ICANN gTLD Registry Continuity Plan
- Identified operational impacts & consequences of specific disruption scenarios

January 2009 Joint Continuity Exercise (cont'd)

- Suggestions for further collaboration:
  - ICANN & gTLD Registries should work further on crisis communications & information sharing;
  - develop criteria & a process for data collection, verification and monitoring to supplement Monthly Reports; and
  - develop procedures to assure resumption of failed registry's services (or closure if appropriate).

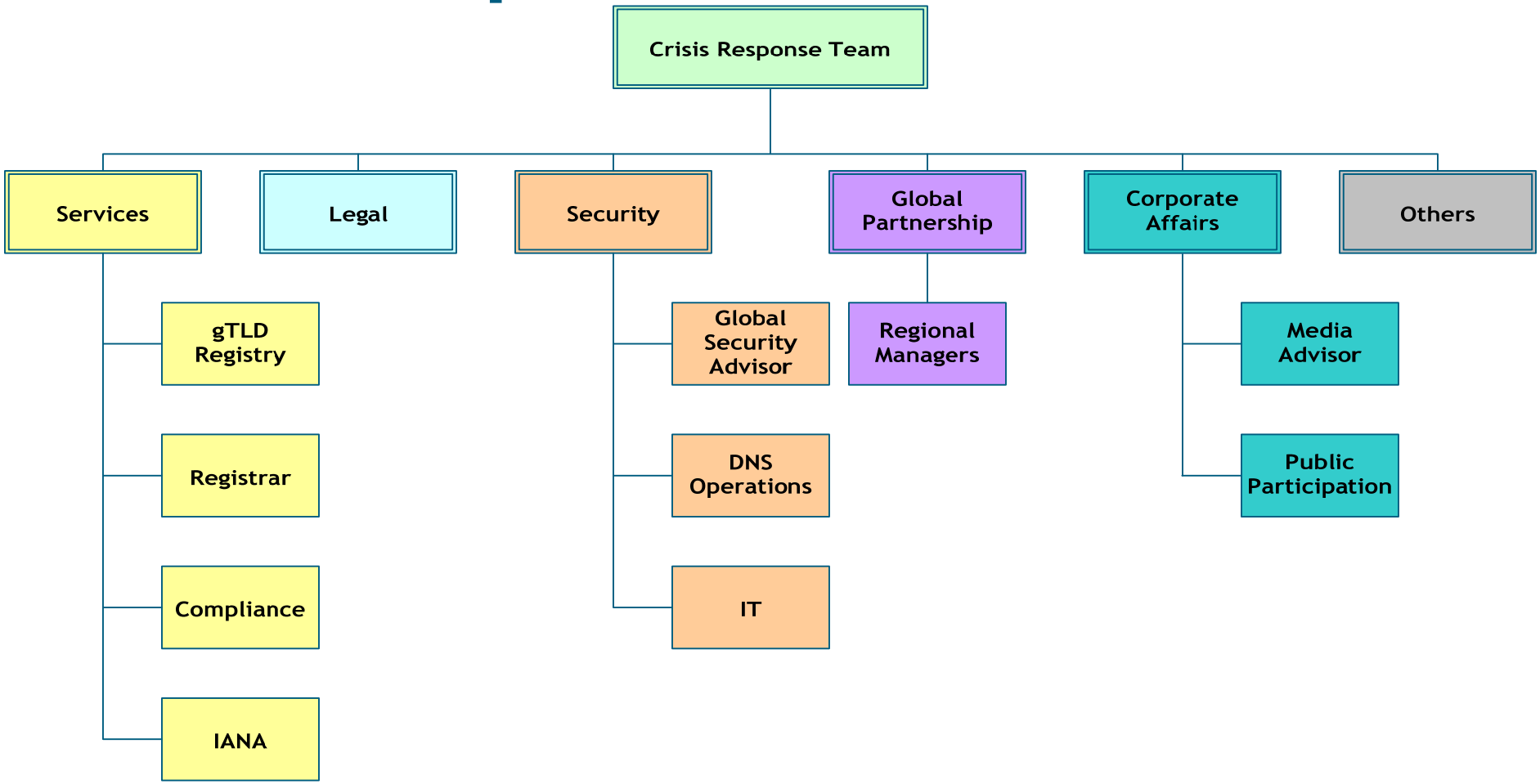
January 2009 Joint Continuity Exercise (cont'd)

- 2009 After Action Report published at:
  - http://ta.gg/2r1
- Available at ICANN gTLD Registry Continuity page:
  - http://www.icann.org/en/registries/continuity/

gTLD Registry Continuity – Current Implementation

- Distribution of ICANN and Registry Contacts
- Situation Handling + Event Management Process in Place
- gTLD Registry Continuity Crisis Response Team Identified
- gTLD Registry Data Escrow Test Plan Developed

Crisis Response



gTLD Registry Continuity – What's Next

- ICANN Communications materials and process to be defined
- gTLD Crisis Response Team and connection to overall ICANN & IANA continuity efforts
- gTLD Registry Data Escrow testing to occur in Sept & Nov-Dec 2009
- Update continuity elements in AGv3 as necessary

Internet Corporation for Assigned Names and Numbers

Continuity Communications

Continuity Communications

- Communication and media coordination has previously been identified as a vital part of the gTLD Registry Continuity Plan
  - ICANN & gTLD registries should create a public information coordination working group,
  - with regular calls to develop a joint information plan based on realistic scenarios, &
  - Q & A's prepared for the media & community.

  (from January 2009 Joint Continuity Exercise AAR)

Continuity Communications (cont'd)

- Pre-identified media contacts at gTLD registries, with contacts shared with ICANN
- ICANN designating points of contact as part of its internal public information management process
- Method to coordinate and clear information for release (to media or community)
- Capability of communicating with stakeholders

Assumptions

- The time between an Event and media inquiry will be short
  - Initial media and/or public inquiries will likely precede an initial assessment of the Event
  - Communications around initial response should occur as quickly as possible
  - Multiple forms of messaging may be used

Assumptions (cont'd)

- Once decision is made to inform media
  - It will be important for media to feel they are receiving timely and accurate information about the Event & what is being done
  - ICANN and registries should have a coordinated message, or at least be in communication

Continuity Communications

- ICANN and registries working on improved information sharing – Conficker is an example
- This will help increase community confidence in the DNS and TLD operations
- Information sharing can occur for routine issues, situations and Events, and should occur in an environment of trust & confidentiality

If a Situation or Event Occurs

- ICANN will attempt to determine the nature and circumstances surrounding the Event
- Cause and severity
- Whether the Event is likely to be temporary or long term
- Whether the registry can continue the TLD's critical functions

If a Situation or Event Occurs

- ICANN will question what, if any, services will be unavailable or operated a reduced level of service
- Whether the registry has interim measures in place to protect the registry's critical functions
  - Note that a determination on whether a registry can continue its critical functions operations will be made in consultation with the registry

Scenarios

- Business/Financial Failure
- Technical Failure
  - Natural Disaster
  - Human Acts
  - Malicious Attack
  - Infrastructure or System Failure
- Other scenarios may include government or regulatory intervention

Scenario Discussion

- Business Failure may raise questions for non-affected TLD operators
- Disasters Occur
  - Earthquake Cable Cuts
  - Hurricanes/Cyclones
  - Blackout/Energy Failure

Scenario Discussion (cont'd)

- Malicious Attacks
  - Conficker
  - DDoS
  - Data Breach
- System Failure or Infrastructure Problems
- Name Server Failure

Pre-Media Advice for Discussion

- Not to communicate with media until group conference call
- If you have not been contacted by anyone else in the group, use contact numbers to contact them immediately
- Vital to follow agreed common messages in first 24-48 hrs, when speculation is greatest & most inaccurate

Internet Corporation for Assigned Names and Numbers

Escrow Testing

Escrow Testing

- Internal Testing September 2009
  - Authorized release of registry escrow deposit to ICANN; testing ICANN's process for receiving & verifying deposit
  - Testing ability to recreate a registry using escrow
  - Working with NCC Group and Iron Mountain, will report initial results in Seoul

Escrow Testing (cont'd)

- Registry Testing November-December 2009
  - Testing by registry operators of draft spec for new gTLD process
  - Sample data to be generated and used by group
  - Look at issues of flexibility, transmission size, IDNs, format
  - Interest so far from Afilias, Neustar, PIR, VeriSign, possibly others

New gTLD Applicant Guidebook - Continuity Areas

Continuity in AGv2

- Applicant Evaluation – Technical Criteria
- Applicant Evaluation – Financial Criteria
- Performance, InterOperability and Continuity Specification
- Data Escrow Specification

Anticipated Updates in AGv3

- Applicant Evaluation
  - Updated Technical Questions
  - Financial Instrument for Continuity
- Updated Escrow Specification

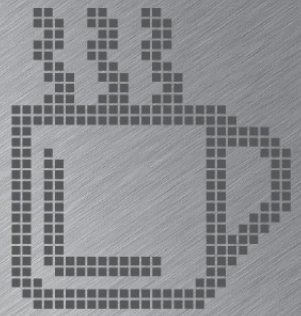
Thank You!

Patrick Jones
Registry Liaison Manager
ICANN Registry Department
patrick.jones@icann.org

ICANN

Internet Corporation for Assigned Names and Numbers

Coffee Break



Welcome, Introduction, & Key Messages

Tim Cole
ICANN Chief Registrar Liaison

Craig Schwartz
ICANN Chief gTLD Registry Liaison

Schedule

Thursday, August 20

9:00	**gTLD Registry Continuity Plan Workshop** – *Patrick Jones*
10:30	**Core Planning Team Meeting/Registry Data Escrow** – *Patrick Jones*
11:00	**Coffee**
11:30	**Welcome, Introductions & Key Messages** *Craig Schwartz & Tim Cole*
12:00	**ICANN Policy** – *Margie Milam*
13:00	**Lunch**
14:00	**Registry Presentations**
14:30	**Terminated Registrar Transition Process** – *Mike Zupke*
15:30	**Coffee**
16:00	**New gTLDs** – *Kurt Pritz*
17:30	**Networking / Free Time**
18:00	**Evening Event - Baseball Game** *Sponsored by* Afilias

Schedule

Friday, August 21

9:00	Contractual Compliance – *Stacy Burnette*
10:00	New RAA Implementation – *Tim Cole*
10:30	**Coffee**
11:00	Registry/Registrar Dialogue – *David Maher and Mason Cole*
12:30	Registry Presentations
13:00	**Lunch**
14:00	Registrar Constituency Update – *Mason Cole*
14:30	Security – *Yurie Ito*
15:30	**Coffee**
16:00	National Cyber Forensic Training Alliance (NCFTA)
17:00	**Networking / Free Time**

Internet Corporation for Assigned Names and Numbers

GNSO Policy Development

Margie Milam
ICANN Senior Policy Counselor

ICANN Policy Staff

- Denise Michel – Vice President, Policy Development (CA, USA)
- Liz Gasster – Senior Policy Counselor, GNSO (CA, USA)
- Margie Milam – Senior Policy Counselor, GNSO (CA, USA)
- Robert Hoggarth – Senior Policy Director (Washington, DC, USA)
- Marika Konings – Policy Director, GNSO (Brussels, Belgium)
- Glen de Saint Géry – Secretariat, GNSO (Cannes, France)
- Bart Boswinkel – Senior Policy Advisor, ccNSO (Netherlands)
- Gabriella Schittek – Secretariat, ccNSO (Warsaw, Poland)

ICANN Policy Staff

- Dave Piscitello – Senior Security Technologist, SSC (SC, USA)
- Julie Hedlund – Director, SSAC Support (Washington, DC, USA)
- Nick Ashton-Hart – Director for At-Large (Geneva, Switzerland)
- Heidi Ullrich – Manager At-Large Regional Affairs (CA, USA)
- Matthias Langenegger – Secretariat At-Large (Geneva, Switzerland)
- Scott Pinzon – Director Policy Communications/Information Services (CA, USA)
- Marilyn Vernon – Executive Assistant (CA, USA)

Future GNSO Council Structure: 2009

GNSO Council
[22 members — 20 votes]
(1 NCA)

ccNSO[2]

ALAC[1]

"Contract" Party House [6+1]
Voting NCA

- Registry Stakeholder Group [3]
  - –Registries
  - –Others
- Registrar Stakeholder Group [3]
  - –Registrars
  - –Others

"Non-Contract" Party House [12+1]
Voting NCA

- Commercial Stakeholder Group [6]
  - –Business
  - –Intellectual Property
  - –Internet Svc Prov.
  - –Others
- Non-Commercial Stakeholder Group [6]
  - –Non-Comm'l Users
  - –Others

Legend: [ ] Voting; ( ) Non-Voting

[1] Non-Voting Liaison – counted as a member
[2] Observer – not counted as a member

Restructring: Current Status

Recent Board Actions

- Stakeholder Group Charters Approved on 30 July
- Resolved Selection of Board Seats #13 and #14
  - Contracting Parties House selects #13
  - Non-Contracting Parties House selects #14
- Board scheduled to approve Bylaws Amendments at 27 August Meeting to enable new GNSO Council to be seated in Seoul
  - Public Comment Period open on Proposed Bylaws until 24 August
  - http://www.icann.org/en/announcements/announcement-03aug09-en.htm

GNSO Restructuring: Next Steps

- GNSO Council Operating Procedures [Aug-Sep]
- Finalize Restructure Implementation Plan [Sep]
- Constituency Charter Reconfirmations [Sep]
- GNSO Councilor Elections [Sep]
- Seat the New GNSO Council in Seoul [Oct]
- Elect GNSO Chair & Vice-Chairs [Oct-Seoul]

Current Issues being Discussed in GNSO

- Inter-Registrar Transfer Policy
- Post-Expiration Domain Name Recovery (PEDNR)
- Registration Abuse Policies (RAP)
- WHOIS Studies
- Possible changes to the Registrar Accreditation Agreement (RAA)
- Fast Flux Hosting
- Other – currently there are 13 WGs/WTs underway

Internet Corporation for Assigned Names and Numbers

Inter-Registrar Transfer Policy

IRTP Background

- Inter-Registrar Transfer Policy (IRTP) is a consensus policy adopted in 2004 – provides a straightforward way for domain name holders to transfer domain names between registrars
- As part of an overall review of this policy, a working group identified issues for improvement and clarification that were divided in to six IRTP-related PDPs
- Policy work on the first two PDPs is complete

IRTP Part B

- For efficiency, the GNSO Council decided in April 2009 to combine a number of issues related to undoing domain name transfers and related to registrar lock status into one IRTP Part B
- The Issues Report was submitted to the GNSO Council on 15 May, 2009

IRTP Part B (cont'd)

a) Whether a process for urgent return/resolution of a domain name is needed

b) Whether additional provisions for undoing inappropriate transfers are needed especially with regard to disputes between a Registrant and Admin Contact

c) Whether special provisions are needed for a change of registrant when it occurs near to the time of a change of registrar

IRTP Part B (cont'd)

d) Whether standards or best practices should be implemented regarding use of Registrar Lock status

e) Whether/how to clarify denial reason #7: When a domain name is in 'lock' status, as long as the Registrar provides a reasonable means for the Registrant to remove the lock status

Recent Developments & Next Steps

- ICANN staff recommended the initiation of a PDP
- GNSO Council decided to initiate a PDP at its meeting in Sydney on 24 June
- GNSO Council approved charter for IRTP Part B WG
- Call for volunteers and WG will start deliberations

Additional Information

- To join the IRTP Part B WG, please contact the GNSO Secretariat:
  - gnso.secretariat@gnso.icann.org
- IRTP Part A Final Report:
  - http://gnso.icann.org/issues/transfers/irtp-final-report-a-19mar09.pdf
- IRTP Part B Issues Report:
  - http://gnso.icann.org/issues/transfers/irtp-report-b-15may09.pdf
- Inter-Registrar Transfer Policy:
  - http://www.icann.org/en/transfers/policy-en.htm
- IRTP Part B Wiki:
  - https://st.icann.org/irtp-partb/index.cgi?irtp_part_b

Internet Corporation for Assigned Names and Numbers

Post-Expiration Domain Name Recovery

PEDNR Background

- The At-Large Advisory Committee (ALAC) requested an Issues Report in November 2008
- ALAC alleges that current measures 'have proven to be ineffective,' 'loss of domain name can cause significant financial hardship,' and previous attempts to instill predictability for post-expiration domain name recovery are 'not successful'
- GNSO Council initiated PDP in May 2009

The PEDNR PDP

The PDP will consider the following questions:

- Whether adequate opportunity exists for registrants to redeem their expired domain names;
- Whether Whether expiration-related provisions in typical registration agreements are clear and conspicuous enough;
- Whether adequate notice exists to alert registrants of upcoming expirations;

The PEDNR PDP (cont'd)

- Whether additional measures are needed to indicate that once a domain name enters the Auto-Renew Grace Period, it has expired (e.g. Hold status, a notice on the site with a link to information on how to renew, or other options to be determined);
- Whether to allow the transfer of a domain name during the RGP.

WG Charter was adopted by GNSO Council at meeting in Sydney on 24 June, 2009

PEDNR WG Charter

- The WG initially will:
  1. Consult with ICANN Compliance staff to understand how current RAA provisions and consensus policies regarding deletion, auto-renewal and recovery of domain names following expiration are enforced;
  2. Review the current domain name life cycle;
  3. Review current registrar practices regarding domain name expiration, renewal and post-expiration recovery.
- The WG will then consider the PDP questions outlined previously.

How to get involved?

- Join the PEDNR WG (contact the GNSO Secretariat: gnso.secretariat@gnso.icann.org)
- Monitor the PEDNR Wiki: https://st.icann.org/post-expiration-dn-recovery-wg/index.cgi

Additional Information

- Post-Expiration Domain Name Recovery Issues Report: http://gnso.icann.org/issues/post-expiration-recovery/report-05dec08.pdf
- Translations available at: http://gnso.icann.org/policies/

Internet Corporation for Assigned Names and Numbers

Registration Abuse Policies

Registration Abuse Background

- Registries and registrars lack uniform approaches to deal with domain name registration abuse, and questions persist as to what role ICANN should play in addressing registration abuse
- September 2008 Report found: no uniform approach by registries/registrars to address abuse, no clear definition of abuse, many registry agreements explicitly allow registries to take down or terminate names for abuse, some registries have no provision
- The Council launched a Pre-PDP WG in February 2009

Registration Abuse Background (cont'd)

- Issues Report recommends further research to determine how abuse policies are implemented and complied with, and how effective they are in addressing abuse
- WG will address such questions as: distinctions between registration abuse and domain name use abuse; the effectiveness of existing abuse policies; and which areas, if any, are suitable for GNSO policy development
- The GNSO Council will not decide whether to initiate a PDP on registration abuse policies until the RAP WG has presented its findings

Registration Abuse Status Update

- The RAP WG provided an update to the GNSO Council on 2 June
- Activities to-date include a workshop on registration abuse in Mexico City; SSAC participation and collaboration; and extensive discussion of the definition and scope of registration abuse. The WG is also defining certain types of abuse, such as cyber-squatting, and will be examining ways to curtail abuse (that are "in scope" for GNSO policy)
- WG will continue bi-weekly meetings and report back to the Council in due time

RAP Additional Information

- RAP WG Status Update:
  - http://gnso.icann.org/issues/registration-abuse/rap-wg-status-update-02jun09.pdf
- RAP WG Wiki:
  - https://st.icann.org/reg-abuse-wg/index.cgi?registration_abuse_policies_working_group
- Registration Abuse Policies Issues Report:
  - http://gnso.icann.org/issues/registration-abuse/gnso-issues-report-registration-abuse-policies-29oct08.pdf

ICANN

Internet Corporation for Assigned Names and Numbers

WHOIS

WHOIS Studies

- In March 2009, the GNSO Council indentified six WHOIS study areas that should be assessed for cost and feasibility.
  - Misuse of WHOIS data to generate spam or for other illegal or undesirable activities;
  - Whether registrants are misrepresenting who they are by providing inaccurate WHOIS data;
  - Who uses proxy/privacy services (individuals/businesses/other);
  - Extent to which proxy and privacy services are being used for abusive and/or illegal purposes, and complicate investigation into e-crimes;
  - Extent to which proxy and privacy services respond to information requests when presented with reasonable evidence of actionable harm; and
  - The growing presence of non-ASCII character sets in WHOIS records and whether this will detract from data accuracy and readability.

WHOIS – Additional Activities

- In May 2009, the GNSO Council asked staff to compile a comprehensive set of requirements for WHOIS service based on current requirements and a review of previous GNSO WHOIS policy work.
  - Staff will perform this work in consultation with the SSAC, ALAC, GAC, ccNSO and GNSO
- In June 2009, the Board asked the GNSO and SSAC to convene a WG to study the feasibility of introducing display specifications to deal with internationalized registration data.

Additional Information

- http://gnso.icann.org/issues/whois/
- http://gnso.icann.org/resolutions/#200903
- http://gnso.icann.org/meetings/minutes-gnso-07may09.shtml
- http://www.icann.org/en/minutes/resolutions-26jun09.htm#6

Internet Corporation for Assigned Names and Numbers

Registration Accreditation Agreement

RAA – Recent Amendments

- Board approved in May, changes include:
  1. New enforcement tools – audits, group liability for affiliated entities, changes to registrar fees, including assessing interest on late fees;
  2. Registrant protections – new data escrow requirements for proxy and privacy registrations or prominent notice, new contractual obligations for resellers;
  3. Enhancing the Registrar marketplace – ICANN accreditation mandatory registrar training and testing;
  4. Other changes – streamlines notice obligations to registrars of new consensus policies, clarifies data retention requirements.
- Implementation will occur over time, voluntarily or as existing agreements renew.

RAA – Pending Activities

- Drafting team of GNSO and ALAC representatives to develop a "Registrant's Rights and Responsibilities" charter
  - Policy staff prepared an initial inventory of registrants' rights and responsibilities reflected in the newly approved RAA
- GNSO drafting team will discuss further amendments to the RAA
- Deadline will be extended from initial GNSO target of 31 July–mid-September

RAA – Additional Information

- For more information on this RAA-related WG, please see:
  - http://www.icann.org/en/topics/raa/

Internet Corporation for Assigned Names and Numbers

Fast Flux Hosting

Fast Flux Background

- January 2008: SAC 025 — Fast Flux Hosting and DNS
  - Describes Fast Flux (FF) as an evasion technique that enables cybercriminals to extend the lifetime of compromised hosts employed in illegal activities
  - 'Encourages ICANN, registries, and registrars [...] to establish best practices to mitigate fast flux' and 'consider whether such practices should be addressed in future agreements'
- May 2008: GNSO initiates Policy Development Process
- June 2008: Fast Flux Hosting WG formed

Fast Flux Final Report

- Final Report (7 August, 2009), includes no new policy recommendations, but describes ideas for next steps:
  - Highlight recommendations addressable by policy development, best practices or industry solutions
  - Consider whether registration abuse policy provisions could empower registries/registrars to take down a domain name involved in malicious or illegal fast flux
  - Explore developing Fast Flux Data Reporting System
  - Explore ICANN's role as a best practices facilitator
  - Explore involving other stakeholders in the fast flux policy development process
- GNSO to review the Final Report and the decide on the next steps

Internet Corporation for Assigned Names and Numbers

Questions?

Subscribe to the month Policy Update:

http://www.icann.org/en/topics/policy/

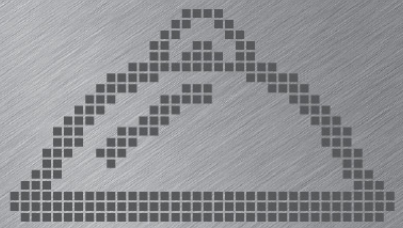
Thank You!

Margie Milam
Senior Policy Counselor
ICANN Policy Department
margie.milam@icann.org

ICANN

Internet Corporation for Assigned Names and Numbers

Lunch



Internet Corporation for Assigned Names and Numbers

Registry Presentations

Internet Corporation for Assigned Names and Numbers

Terminated Registrar Transition Process

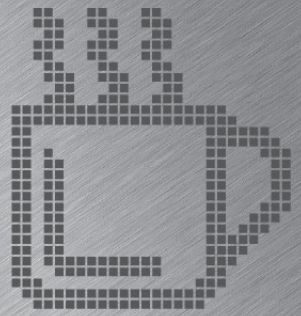
Mike Zupke

ICANN Registrar Liaison Manager

ICANN

Internet Corporation for Assigned Names and Numbers

Coffee Break

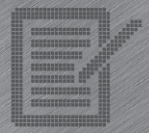


Internet Corporation for Assigned Names and Numbers

New gTLDs

Kurt Pritz
ICANN Senior Vice President – Services

Sponsor



Afilias SM

ICANN

Internet Corporation for Assigned Names and Numbers

Toronto

August

20 thru 21

2009

Schedule

Friday, August 21

9:00	Contractual Compliance – *Stacy Burnette*
10:00	New RAA Implementation – *Tim Cole*
10:30	**Coffee**
11:00	Registry/Registrar Dialogue – *David Maher and Mason Cole*
12:30	Registry Presentations
13:00	**Lunch**
14:00	Registrar Constituency Update – *Mason Cole*
14:30	Security – *Yurie Ito*
15:30	**Coffee**
16:00	National Cyber Forensic Training Alliance (NCFTA)
17:00	**Networking / Free Time**

Contractual Compliance Update

Stacy Burnette
ICANN Director, Contractual Compliance

Agenda

- FY2009-2010 Contractual Compliance Program Objectives
- Enforcement Statistics [Jan-Jun 2009]
- WHOIS Data Accuracy Study
- Planned Audit Activities
- Questions, Comments and Suggestions
- Closing Thoughts

FY2009-2010 Contractual Compliance Program Objectives

- Enforcement – Enhance enforcement by sending breach and termination notices for failure to comply with RAA requirements, enforce amended RAA
- Audits – Registrar contact info, RDE requirements, financial compliance, transfer policy, registry reporting requirements
- Research – Complete WHOIS data accuracy study

FY2009-2010 Contractual Compliance Program Objectives (cont'd)

- Budget – 28% increase over prior fiscal year's budget
- Staffing – Hire additional staff to carrying out program objectives (2 auditors)
- Risk Assessment – Identify contract compliance risks and develop appropriate strategies and controls to minimize risks

Contractual Compliance Program Enforcement Statistics

Quick Stats	
Registrars Under Contract	937
Registries Under Contract	16
Total Registrars Terminated by ICANN since 2003	33
Registrars Terminated in 2009 (Jan-Jun)	7
Total # of Consumer Complaints in 2009 (Jan-Jun)	6,338
Total # of Consumer Complaints in 2008	11,348

Common Registrar Termination and Non-Renewal Causes in 2009

- Registrars failed to comply with RDE deposit requirements
- Registrars failed to comply with UDRP requirements (implementation of panel decisions)
- Registrars failed to pay accreditation fees
- Registrars failed to comply with WHOIS data investigation requirements

WHOIS Data Accuracy Study Purpose

- Determine accuracy of WHOIS data for the total population of domain names registered in the gTLDs
- Deploy a name and address verification methodology to determine accuracy of WHOIS registrant data
- Estimate the percentage of domain names that are "accurate" with a ±5% margin of error at a 95% confidence level
- Share findings with the Internet Community for discussion and use

WHOIS Data Accuracy Study

- ICANN collaborated with the National Opinion Research Center (NORC) to conduct the study
- NORC will attempt to verify registrant names and addresses
- WHOIS Data Accuracy Study results are expected by December 2009
- For study design details, go to:
  - http://www.icann.org/en/compliance/norc-whois-accuracy-study-design-04jun09-en.pdf

Planned Registrar Audit Activities

Registrar Audit Schedule – FY2010		
July – October	**November – March**	**April – June**
Registrar Primary Contact Information Audit, Phase 1	Public Contact Information Audit, Phase 2	Registrar Non-Implementation of UDRP Arbitration Panel Decisions Audit, Phase 2
Registrar Transfer Policy Audit	Registrar Non-Implementation of UDRP Arbitration Panel Decisions Audit, Phase 1 (Development)	RDE Audit
RDE Audit	RDE Audit	

Planned Registry Audit Activities

Registry Audit Schedule – FY2010		
July – October	**November – March**	**April – June**
Data Escrow Agreement Requirement	Verification of WHOIS Availability and Data Output	

Community Questions, Comments and Suggestions

- What do you think ICANN should do to enhance its contractual compliance program?
- What suggestions do you have to assist ICANN in improving its contractual compliance audit processes or other compliance related processes?
- What do you think the ICANN community should do to address concerns about WHOIS data accuracy?

Closing Thoughts

- Participate in ICANN's bottom-up consensus building process to ensure the continual improvement of the Contractual Compliance Program
- Write ICANN if you have questions regarding contractual compliance matters

Thank You!

Stacy Burnette
Director, Contractual Compliance
ICANN Contractual Compliance
stacy.burnette@icann.org

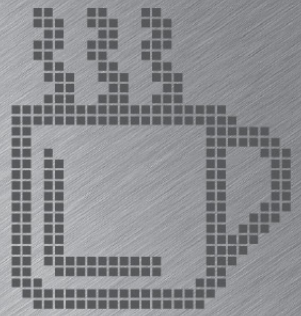
New RAA Implementation

Tim Cole
ICANN Chief Registrar Liaison

ICANN

Internet Corporation for Assigned Names and Numbers

Coffee Break



Internet Corporation for Assigned Names and Numbers

Registry/Registrar Dialogue

David Maher
Chair, Registry Constituency

Mason Cole
Chair, Registrar Constituency

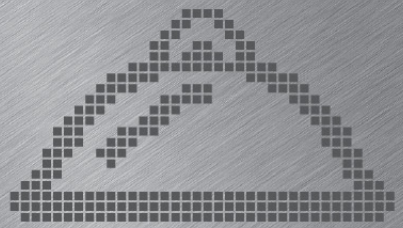
Internet Corporation for Assigned Names and Numbers

Registry Presentations

ICANN

Internet Corporation for Assigned Names and Numbers

Lunch



Internet Corporation for Assigned Names and Numbers

Registrar Constituency Update

Mason Cole
Chair, Registrar Constituency

Internet Corporation for Assigned Names and Numbers

Enhancing Collaborative Response to Security Challenges Involving the DNS

Yurie Ito

ICANN Director, Global Security Programs

The Internet as an Ecosystem

- Built as experiment; now part of everyday life
  - Assumed benign, cooperative users
- Now involves a wide variety of systems, stakeholders, opportunities & risks
  - Governments, corporations, civil society, criminals
- Malicious actors now use Internet
  - Growing centers of gravity – economically, socially, militarily
  - Anonymity & ability to leverage 3rd Parties for Bad Acts
  - Underground economy is developed

Underground Ecosystem

Business, Ecommerce, Online Banking...

Key Logger
Spyware
Botnets

Phishing
Trojan..

Attack Tools
Methods

Social Engineering

Attack against
Vulnerability

Actors (could be internal, external)

technology

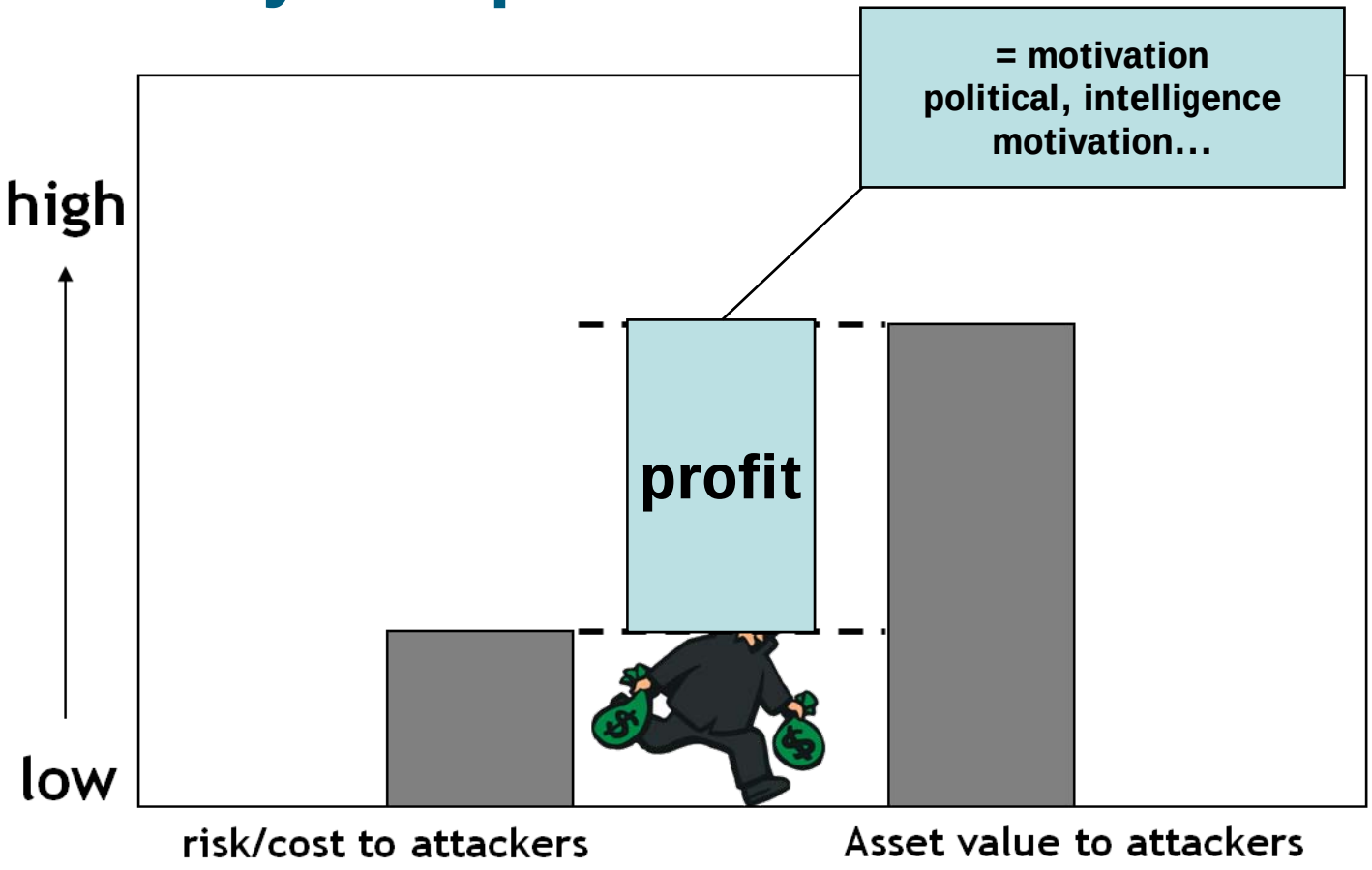
Assets (Information, System, Resources, IP...)

Monetary Stolen Assets

Money, Threat...

Criminal Organizations, Terrorists, Industry Spy, etc.

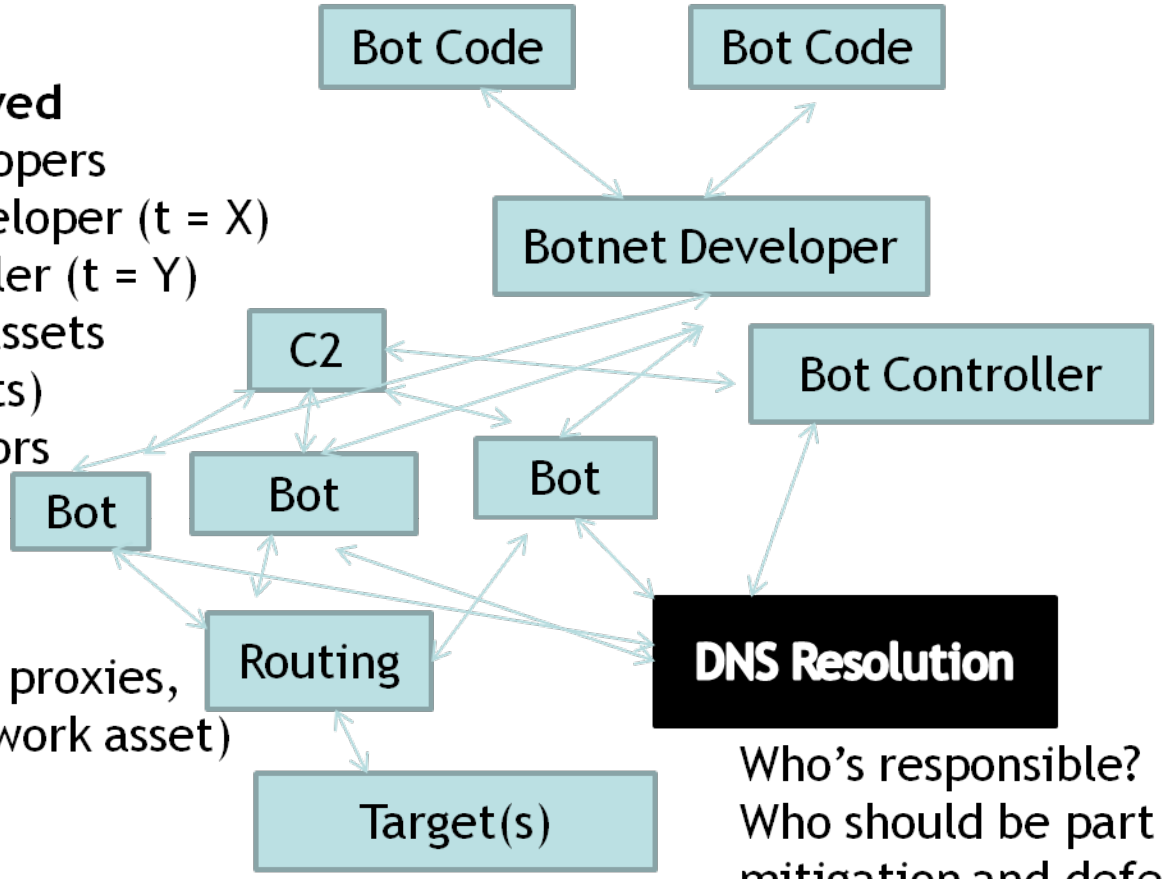
Risk and Cost to the Attackers vs. Asset Value in Cyber Space



Bot Nets and Complexity of Attacks

Actors Involved
- Code Developers
- Botnet Developer (t = X)
- Bot Controller (t = Y)
- Owners of assets (C2 and bots)
- DNS operators
- ISPs
- Target(s)

(to include firewall, IDS, proxies, targeted network asset)



Multiple purposes; Possibly no digital connection

Who's responsible?
Who should be part of a cooperative mitigation and defense?
Who should be in a investigation/legal enforcement?

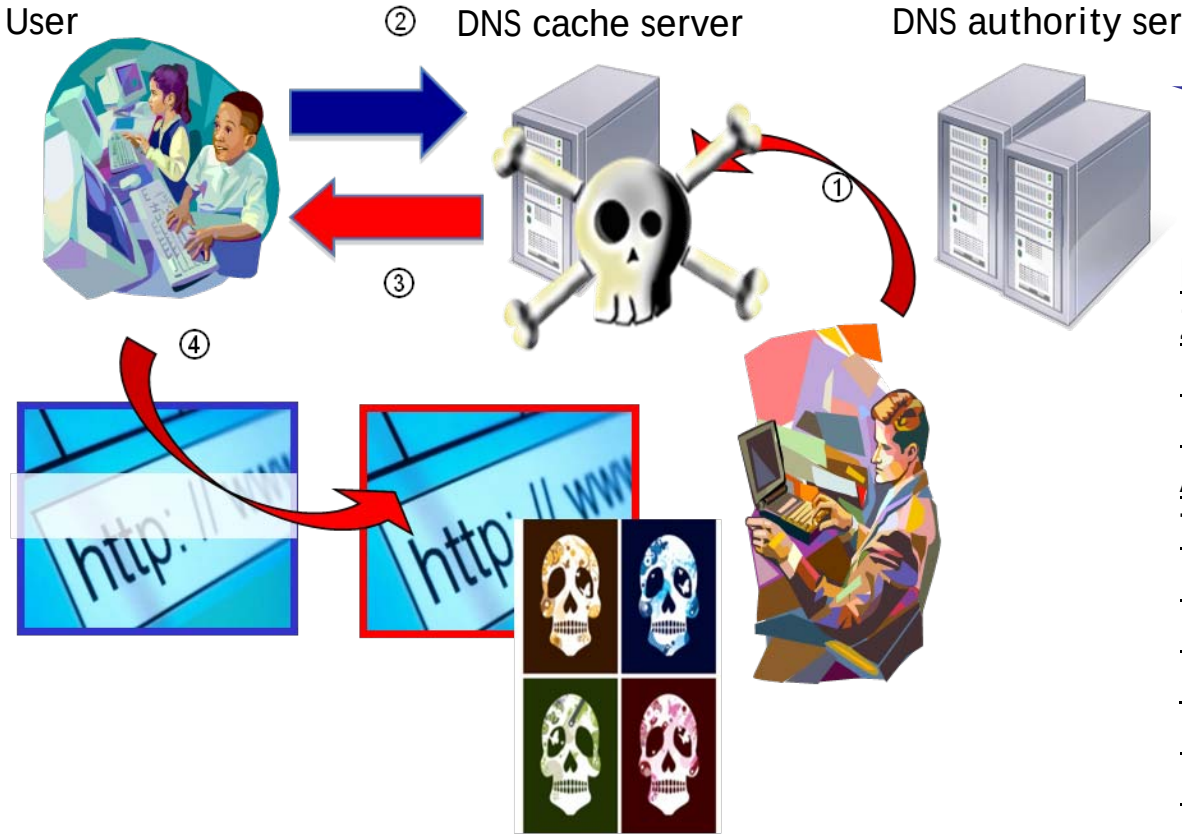
Attack the swamps, not the fever

What is ICANN?

- International public benefit, non-profit organization managing the Internet unique identifier systems, including the DNS
  - Authority over name spaces is distributed to generic and country-specific registries
  - Includes a range of supporting organizations and advisory committees
- Ensuring "Security and Stability" of those systems is a core mission

DNS Risks and Threats

DNS vulnerabilities — DNS cache poisoning



Cache poisoning attack

- Routing hijack
- Zone transfer
- Non-authoritative spoofing
- Distributed Denial of Service
- Asymmetric Denial of Service
- TXID prediction
- Botnet
- Key management in DNSSEC
- Bad caching policies
- DNS rebinding
- Lame delegation….

ICANN Roles and Responsibility Related to Security, Stability and Resiliency

- ByLaws: To coordinate, overall, the global Internet's system of unique identifiers, and to ensure stable and secure operation of the Internet's unique identifier systems
- Core: Ensure DNS system stability and resiliency; enable operator to protect DNS registration and publication process
- Enabler: Work the broader Internet and security communities to combat systemic abuse of the unique identifier systems that enable malicious activity
- Contributor: Identification of risks to security, stability and resiliency of the DNS and other identifier systems
- Not involved in content control

Board approved ICANN Plan for Enhancing Internet Security, Stability and Resiliency SSR Plan: http://www.icann.org/en/announcements/announcement-2-21may09-en.htm

ICANN Security Staff

- Greg Rattray: Chief Internet Security Advisor
- John Crain: Chief Technical Officer
- Geoff Bickers: Director of Security Operations
- Dave Piscitello: Senior Security Technologist
- Yurie Ito: Director, Global Security Programs

Internet Assigned Numbers Authority (IANA) Operations

- Supporting the implementation of DNS Security Extensions (DNSSec)
  - Agreement with USG/VeriSign to sign root by end of year
- Initiate improving root zone management through automation
- Improve authentication of communication with TLD managers

DNS Root Server Operations

- Continuing to seek mutual recognition of roles and responsibilities and initiate a voluntary effort to conduct contingency planning and exercises
- Secure, resilient L-root operation

ICANN Relationships with TLD Registries and Registrars

- New gTLDs:
  - Ensure applicant evaluation of new gTLD and IDN applicants continues to provide for secure operations
- gTLD Registries:
  - Mature the gTLD registry continuity plan and test the data escrow system
  - Conduct RSEP (Registry Services Evaluation Process)/RSTEP (Registry Services Technical Evaluation Panel) processes on registry services proposals
- ccTLD Registries:
  - Enhance collaboration on maturing the joint Attack and Contingency Response Planning (ACRP) program that has been established in conjunction with the ccNSO and the regional TLD associations
- Registrars:
  - Continue policy development to enhance registrar accreditation and data escrow requirements through improvements to the RAA (Registrar Accreditation Agreement)

ICANN Relationships with TLD Registries and Registrars (cont'd)

- Contractual Compliance:
  - Continue to enhance the scope of contractual enforcement activities involving gTLDs
  - Initiating audits of contracted parties as part of implementing the March 2009 amendments to Registrar Accreditation Agreement (RAA)
  - Identify potential involvement of contracted parties in malicious activity for compliance action

ICANN Relationships with TLD Registries and Registrars (cont'd)

- TLD Security, Stability and Resiliency Collaboration:
  - Mature Attack and Contingency Response Program
  - Establish Joint ISOC/ICANN Tech Training Program
  - Establish TLD Exercise Planning Workshops
  - Establish Program Metrics

Ensure Global Engagement and Cooperation

- Enhance partnerships to include the Internet Engineering Task Force (IETF), Internet Society (ISOC), regional internet registries and network operators groups, the DNS Operations, Analysis and Response Center (DNS-OARC), and global incident response community such as Forum of Incident Response Security Teams (FIRST)
- Engage in global dialogues to foster understanding of the security, stability, and resiliency challenges that face the Internet ecosystem and how to address these challenges with multi-stakeholder approaches

ccTLD Security and Resiliency Capacity Building Initiative

- Partnered with ccTLD regional organizations to provide training/exercise events to develop capacity
  - Managerial-level Attack and Contingency Response Planning course – process & best practice
  - Technical-level, hands-on defense techniques in simulated threat environment
  - Workshop to establish exercise programs
- Multiple events planned through mid-year 2009
  - Exercise Training Workshops in Jordan, Seoul
  - Technical Training with LACTLD Association in Santiago [Sep]

Looking to leverage lessons and partners

1st Global DNS SSR Symposium

- Co-hosted with Georgia Tech, George Mason University, DNS-OARC: Over 90 participants – technologists, academia, operators, security experts, vendors
- Major Themes:
  - Combating malicious abuse of the DNS
  - Enterprise DNS risk and remediation
  - DNS security in resource constrained environments

Initial Findings from 1st Global DNS SSR Symposium

- Need for improved collaborative response
- Need for training across all sectors of the industry to raise both skills and awareness
- Other findings are available in the symposium report at:
  - http://www.gtisc.gatech.edu/icann09

Collaborative Response to Malicious Abuse of Domain Name System

- ICANN will build on its collaborative efforts related to defeating malicious conduct enabled by the use of the DNS and facilitate information sharing to enable effective response involve with:
  - DNS registries and registrars
  - Security research community
  - Security response community
  - Software and security/anti-virus vendors
  - Law enforcement as appropriate

What is Conficker?

- An Internet worm
  - Self-replicating malicious code
  - Uses a network for distribution
- Uses various methods to spread the infection (network file shares, map drives, removable media)
- Conficker code is *injected* into Windows Server Service
  - Variants disable security measures
  - Provides the attacker with remote control, execution privileges, and ability to download more malware
- Enlists the infected computer into a botnet
  - Conficker bots query rendezvous points for additional malware or instructions for already present malware

Fighting Conficker: Chronology of Events

- November 2008 – 1 January, 2009
  - Security community identify Conficker.A
  - Researchers preemptively register domains to contain botnet
- 2 January – 3 February, 2009
  - Conficker.B name algorithm uses more names, more TLDs
  - Security community asks DNS community for help in containing Conficker
  - DNS community joins ad hoc partnership, blocks Conficker domains at registry
- 12 February, 2009
  - Public announcement of collaborative operational response
  - Microsoft offers $250,000 reward

Fighting Conficker: Chronology of Events (cont'd)

- 19 February – 31 March, 2009
  - Conficker.C/D identified, more aggressive in domain registrations, begins using P2P
  - DNS community continues to block domains, Security community releases Conficker scanners
- 1 April, 2009
  - Conficker.E variant activated on previously infected hosts
- 3 May, 2009 – present
  - Conficker.E variant removes itself but leaves DLL and P2P network in place
  - Security community continues to monitor activities and collaborate on keeping blocks in place

Affected Country Code TLDs – Conficker C

Positive Lessons Learned

- Security and DNS communities can work effectively together, at an operational level, to contain global security threats
  - Trust was a critical element in ad hoc partnership
- Communications channels are essential in coordinating operational response
  - ICANN's role in enabling communications and staff participation in ad hoc partnership was appreciated
- Security and DNS communities need each other
  - Leverage competencies rather than duplicate them
  - Collective, global expertise is essential for effective response

Problems Not Yet Solved

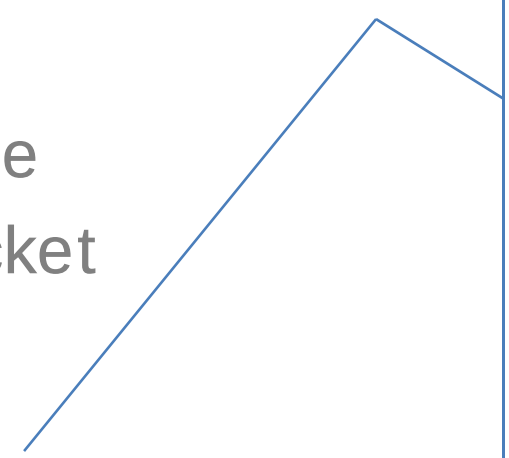
- Collaborative response forced botnet operators out of comfort zone but not out of business
- Botnet writers are agile and elusive
  - Cannot put them out of business without adopting a similarly agile model for response
- Collaborative can be difficult to sustain
  - Numerous and complex, harder to build and maintain, more fragile than botnets
- The risk-reward equation favors worm creators

Way Forward on DNS Collaborative Response

- Efforts to effectively block Conficker use of the DNS should be sustained
  - Must address challenges of long-term engagement
- Broader collaborative efforts within both the security and DNS communities should be considered
  - Security community dialogue about future collaboration models ongoing
- In the DNS community, key players have continued to discuss how to organize effectively
  - Country code DNS TLD operators established working group
  - ICANN plans for active participation in these efforts

Exploitation or Misuse Against Domain Registration Services

- Attacks against domain registration accounts
  - ICANN
  - Comcast
  - CheckFree
  - Photobucket
  - RedTube
  - DomainZ
  - some ccTLD operators



Also victimized:
- Coca-Cola
- Fanta
- F-secure
- HSBC
- Microsoft
- Sony
- Xerox

What Do These Incidents Reveal? (from SAC040 Study)

- All an attacker needs to gain control of an entire domain name portfolio is a user account and password
  - Guess, phish, or socially engineer a single point of contact
  - Attackers also scan registrar account login portals for web application vulnerabilities
  - Attacker can change contact and DNS information of **ALL** domains in the account
- Email may be only method registrar employs to notify a registrant of account activity
  - Attackers know this and block delivery to registrant by altering DNS configuration
- Recovery from DNS configuration abuse is slow

Findings (from SAC040 Study)

- Attackers exploit password-based authentication to gain access registration accounts
  - Compromise exposes all domains in account to attack
  - DNS configurations are favorite targets
- Attackers often alter DNS configurations to prevent email delivery of registrar notifications to registrants
- Security measures vary among registrars
  - Customers need more information to make informed decisions when choosing a registrar
- Domain name account access should be as secure as an e-banking or e-merchant transaction

Recommendations (from SAC040 Study)

- Registrars: offer more protection against registration exploitation or misuse
  - Complement existing measures to protect domain accounts with security measures identified in the SSAC report
- Registrars: make information describing measures to protect domain accounts more accessible to customers
- Registrars: consider a voluntary, independent security audit as a component of self-imposed security due diligence
- ICANN: consider whether a trusted security mark programs would improve registration services security

- How can community work more collaboratively to respond to threats and risk against DNS?
- What more should we do?

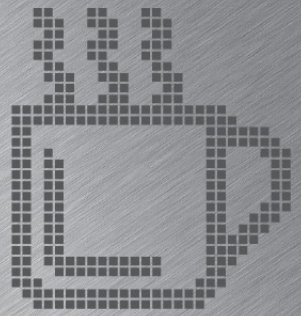
Thank You!

Yurie Ito
Director, Global Security Programs
ICANN Security Team
yurie.ito@icann.org

ICANN

Internet Corporation for Assigned Names and Numbers

Coffee Break



Internet Corporation for Assigned Names and Numbers

National Cyber Forensic Training Alliance (NCFTA)

Derek Brown

Mike McKeown

NCFTA Overview

August 2009

National Cyber Forensics and Training Alliance

The National Cyber-Forensics and Training Alliance provides a neutral collaborative venue where critical confidential information about cyber incidents can be shared discreetly, and where resources can be shared among industry, academia, and law enforcement.

History

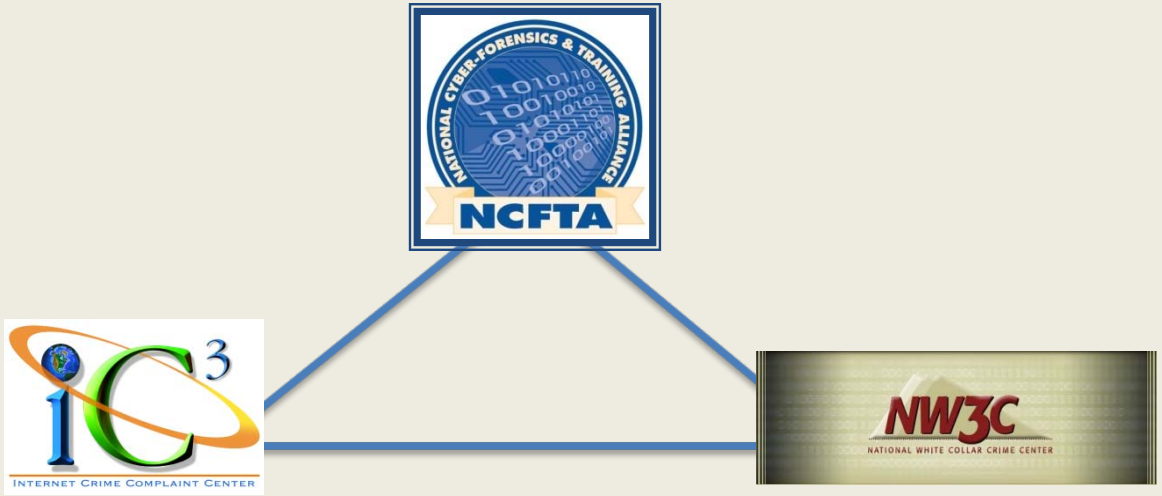
- Initial conceived by the Pittsburgh High Technology Task Force
- Recognized
  - the need for Industry, Academia, and L/E to collaborate and share information about cyber incidents
  - the value subject matter experts from industry and academia
  - the need for a neutral venue to facilitate the sharing of information
- Goal to identify and mitigate threats
- 2002 non-profit is established in Pittsburgh PA

NCFTA

- Mission
  - to facilitate collaboration and information sharing between private industry, law enforcement/intelligence community, and academia in order to efficiently research computer crimes and improve network security
- Staffing
  - NCFTA
  - FBI (CIRFU)
  - USPIS
  - Industry

Partnerships

- Initial LE Partnerships
  - PGH HTTF
  - FBI Cyber Division (CIRFU)
  - Internet Crime and Compliant Center (IC3)
  - National White Collar Crime Center (NW3C)*



Partnerships

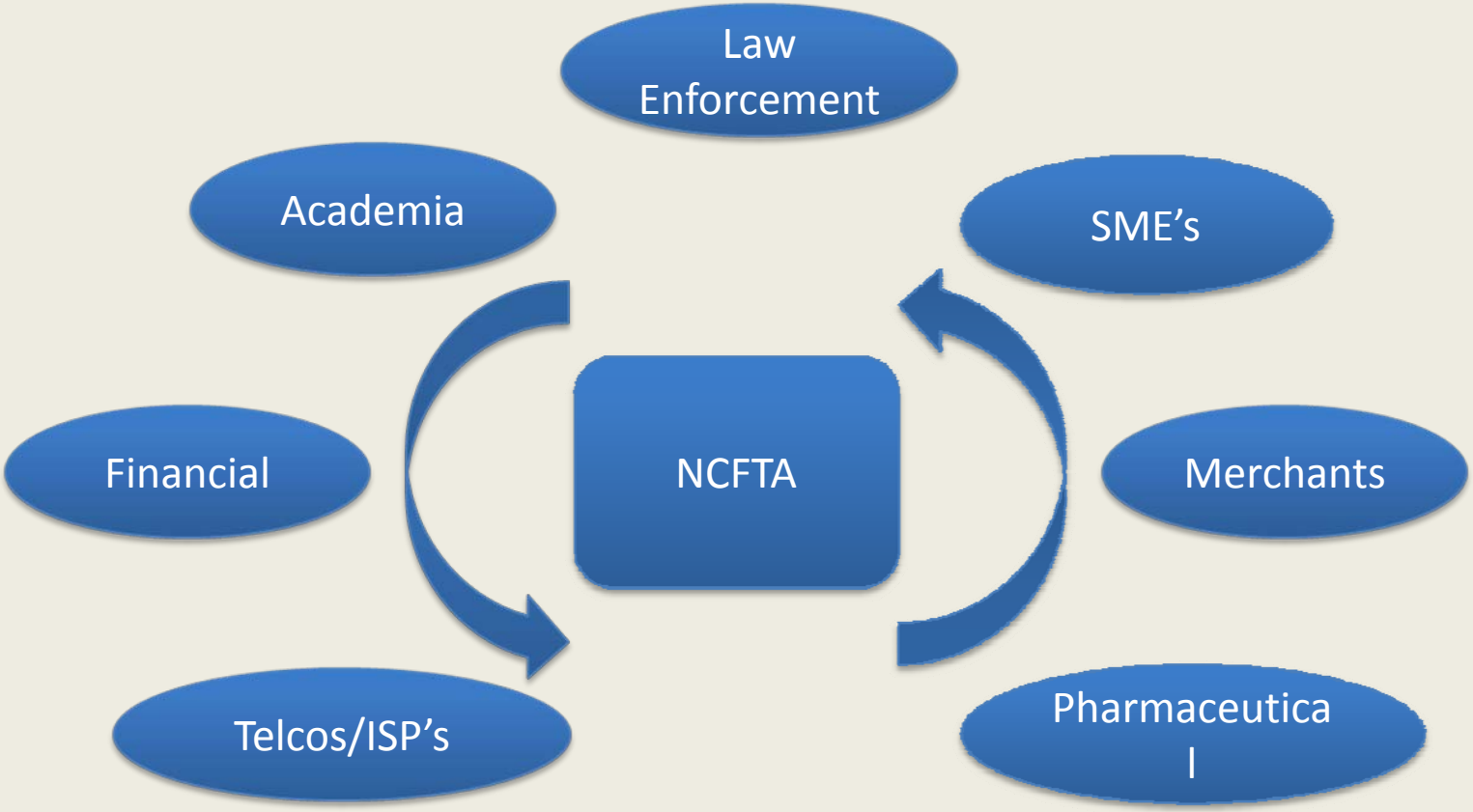
- Initial Industry Partners
  - Fidelity Investments
  - Target Corporation
  - Microsoft Corporation
- Initial Academic Partners
  - Carnegie Mellon University
  - University of Pittsburgh
  - University of West Virginia
  - Duquesne University

Partnerships

Partnerships

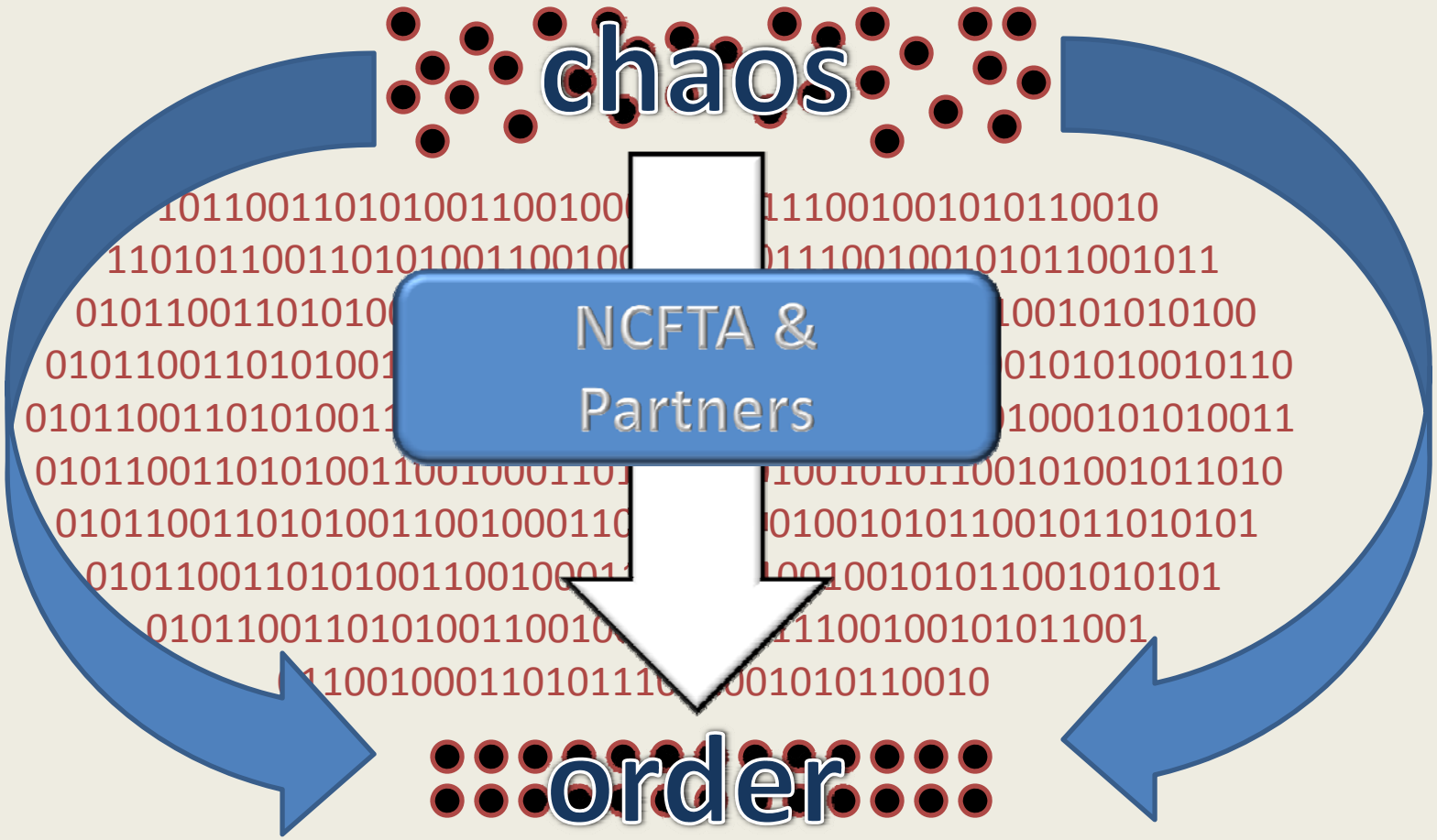
- Support from International Law Enforcement
  - U.K.
  - Germany
  - Romania
  - India
  - Turkey

Collaboration



Collaboration

Collaboration



Initiatives

- Stock Fraud
  - Stock manipulation through compromised trading accounts
- Credit Card Fraud
  - Compromised consumer credentials and card information, high profile carders, re-shippers
- Pharmaceutical Fraud
  - Pharmaceutical SPAM, counterfeiters, diverted shipments, re-shipping, compromised credentials

Initiatives

- Retail Fraud
  - Compromised credentials used for purchases, re-shipping, brand abuse
- Shipment Fraud
  - Re-shipping, Money Mules
- Grey Markets
  - Stolen telecommunication circuit cards

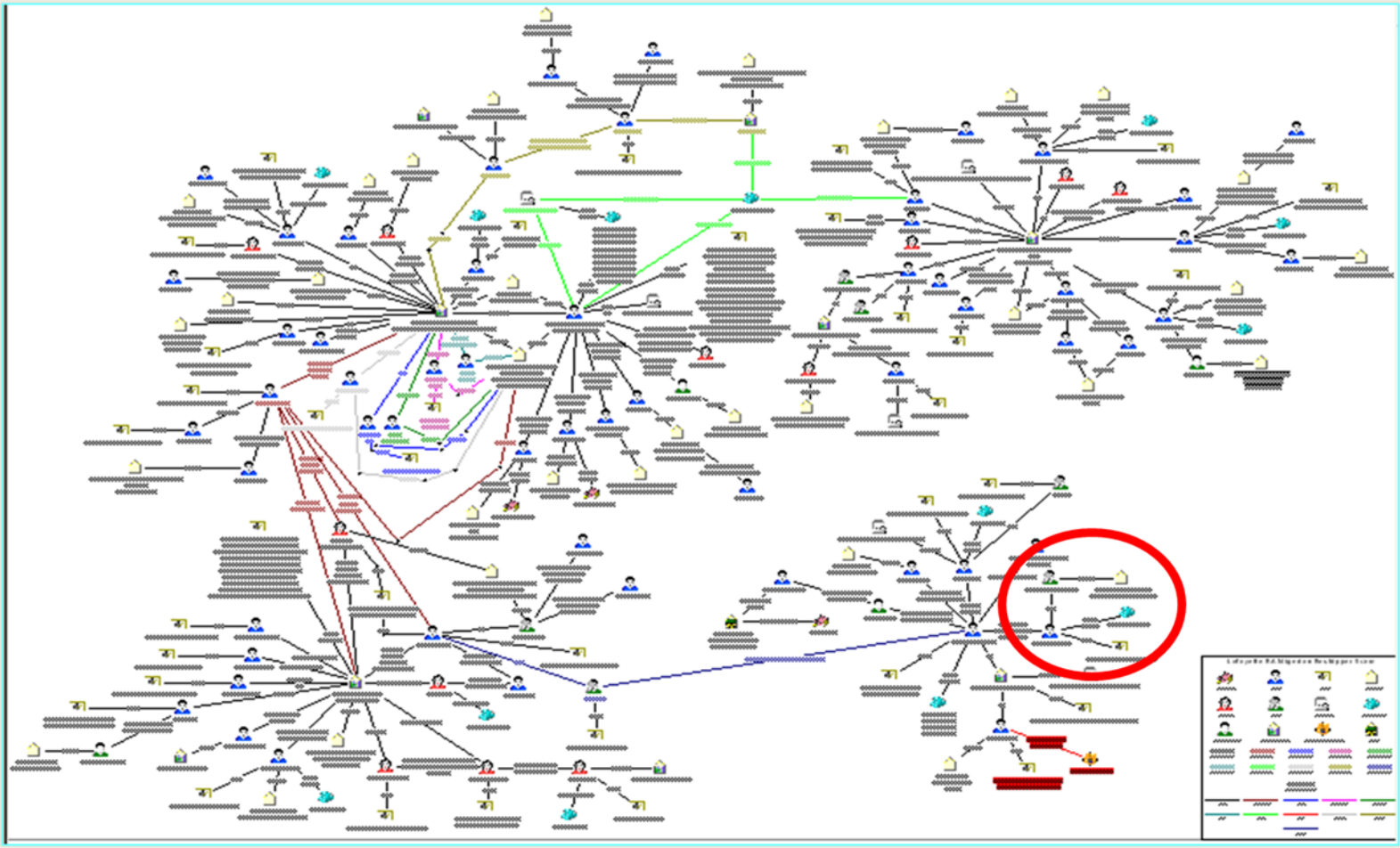
The Goal

- Our Goal is to
  - facilitates advanced research and intelligence sharing
  - promote security awareness to reduce cyber-vulnerability
  - conduct forensic and predictive analysis
- Assist Industry
  - fraud prevention, risk mitigation
  - infrastructure protection
- Assist Law Enforcement
  - enhance case work through research
  - provide subject matter expertise

Key Elements in Analysis

- Open Source Information
- Network Intelligence
  - Network Addresses
  - Domain Information
  - Hosting Providers (Bulletproof hosting)
- Threat Analysis
  - SPAM
  - Malware/Botnets
  - Phishing

Outcome



Outcome

- PELP – Potential Economic Loss Prevention
  - Calculation used to estimate the loss prevented by finding and distributing compromised credentials into the appropriate hands to prevent additional loss. – Calculated at $500 per credential.
  - Calculated at $500 per credential.
- 2008 PELP = $66,324,500.00
  - Q3-Q4 2008 - $29,225,000 (58,450)
- 2009 PELP (Jan to mid-Feb) = $1,435,500.00

Outcome

- Additional Outcomes
  - Expanded Intelligence
  - Enhanced Analytical Capability via SME's
  - Rapid Case/Intelligence Development
  - Enhanced Cyber-Forensic Ability
  - Human Capital Development

Outcome

- Romanian Arrests
  - Through a coordinated effort, the Romanian Police and the FBI arrested an organized crime ring of approximately 24 people
- Turkish Arrests
  - Turkish hacker who specialized in ATM "Skimmer" devices and PIN code pads, was arrested along with twenty eight co-conspirators as part of “DarkMarket”
- Digital PhishNet
  - The Digital Phishnet leverages subject matter experts from over 100 companies who report data regarding phishing attacks. NCFTA has received intelligence on 850,000 phishing attacks to date which has led to more than $220 million in potential economic loss prevented through this initiative alone

Questions

National Cyber-Forensics and Training Alliance
2000 Technology Drive, Suite 450
Pittsburgh, Pennsylvania
(412) 802-8000
www.ncfta.net