ICANN and DNS Security, Stability and Resiliency Activities

Greg Rattray
Chief Internet Security Advisor
Internet Corporation for Assigned Names and Numbers (ICANN)
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
What is ICANN?

• International, public benefit, non-profit organization managing the Internet unique identifier systems, including the DNS
  – Includes a range of supporting organizations and advisory committees

• Ensuring “Security and Stability” of those systems is a core mission
ICANN/IANA (Internet Assigned Numbers Authority)

cCountry Top-Level Domain (ccTLD) registry

gGlobal Top-Level Domain (gTLD) registry

Root Zone w/ USG and VeriSign

.IP address

Registrar

I want 'example.net' to setup www.example.net

I need 1 IP address to setup www.example.net

www.example.net = 192.0.2.1
ICANN/IANA (Internet Assigned Numbers Authority)

ccTLD registry

Root Zone w/ USG and VeriSign

Root Zone

.gTLD registry

domain names

IP address

RIR

ARIN

AfriNIC

RIPE NCC

APNIC

LACNIC

NCC

JPNIC

CNNIC

KRNIC

ARIN

AfriNIC

RIPE NCC

APNIC

LACNIC

NCC

JPNIC

CNNIC

KRNIC

ISP

ISP

ISP

ISP

ISP

ISP

ISP

I want 'example.net' to setup www.example.net

I need 1 ip address to setup www.example.net

www.example.net = 192.0.2.1
ICANN Plan for Enhancing Internet Security, Stability and Resiliency

• Required by Strategic Plan
• Accomplished during last operating year
  – Approved by Board June 2009 (Sydney meeting)
• Plan intended as an initial foundation
  – Not tabling new initiatives; programs and activities already in ICANN strategic & operational plans
    • Details planned activities & resource commitments in FY 10

Next revision will serve as basis for AoC review

Plan can be found at www.icann.org/en/security
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
- **Enabler:** Work with broader Internet and security communities to combat systemic DNS abuse; assist operators to protect DNS registration and publication process
- **Contributor:** Identification of risks to security, stability and resiliency of the DNS as part of cybersecurity challenges
- **Not involved** in cyber war/espionage or content control
Key Initiative: Internet Assigned Numbers Authority (IANA) Operations

• Supporting the implementation of DNS Security Extensions (DNSSec)
  – Working with USG/VeriSign to sign root by mid-2010
• Initiate improving root zone management through automation
• Improve authentication of communication with TLD managers
Key Initiative: Working with TLD Registries and Registrars

- Establishing New gTLDs & IDNs: Ensure establishment of new gTLD & IDN applicants provide for stable operations & enhanced security controls
- gTLD Registries:
  - Mature the gTLD registry continuity plan and test the data escrow system
  - Establish expedited security request and response system
- ccTLD Registries:
  - Mature the joint Attack and Contingency Response Planning (ACRP) program that has been established with the regional TLD associations and establish technical training program with ISOC
  - Facilitate the ccTLD working group on incident response
- Registrars: Enhance registrar accreditation and data escrow requirements
New gTLD Malicious Conduct: Key Issues Identified

A. How do we ensure that bad actors do not run Registries?
B. How do we ensure integrity and utility of registry information?
C. How do we ensure more focused efforts on combating identified abuse?
D. How do we provide enhanced control framework for TLDs with intrinsic potential for abuse?
Proposed Solutions for Mitigating Malicious Conduct

1. Enhanced requirements and background checks
2. Requirement for DNSSEC deployment
3. No wildcarding/remove glue records
4. Requirement for thick WHOIS
5. Anti-abuse contact and documented policy
6. Expedited Registry Security Request process
7. Elective TLD security verification program
High Security Zones Designation Program

• Establish a common set of standards for gTLD security and operational controls
  – Designed for gTLDs with intrinsic potential for malicious abuse
  – Voluntary participation by gTLD registry and registrars
  – Focused on gTLD registry operator
  – Expects registry to require specific security measures by registrars

• Require registry and its registrars to comply with defined standards of security and operational controls
Key Initiative: ccTLD Security and Resiliency Capacity Building Initiative

**Attack and Contingency Response Planning (ACRP)**
- Understanding and Assessing Risks to TLD Operations
- Developing a Contingency Plan / Strategy

**Registry Operations Curriculum (ROC)**
- Three-tier, Hands-on Operations and Security Training
- Cyber Attack Detection, Monitoring, Analysis & Response
• Survey Course of Principles & Planning
• Innovative Use of Templates Simplify the Planning Process for Small Operations
• Instructs ccTLDs in Assessing Risks, Developing a Strategy, Executing the Strategy
Registry Operations Curriculum

Registry Operations Curriculum (ROC)
- Three-tier, Hands-on Operations and Security Training
- Technical Components & Concepts Needed Run a Registry
- Cyber Attack Detection, Monitoring, Analysis & Response

- Registry Technical & Security Training
  - Provide Operational Training to ccTLDs
  - Create Foundation to Build Resiliency in ccTLDs
  - Addresses Gaps Identified by the Community
Key Initiatives: Ensure Global Engagement and Cooperation

• Enhance and establish partnerships to include the Internet Engineering Task Force (IETF), Internet Society (ISOC), Regional Internet Registries (RIRs) and Network Operators Groups (NOGs), the DNS Operations, Analysis and Response Center (DNS-OARC), and global incident response community such as Forum of Incident Response Security Teams (FIRST).
  – Develop scalable capacity to raise awareness and develop appropriate collaborative response to DNS threats, vulnerabilities and risks
  – Engage in global dialogues to foster understanding of the security, stability, and resiliency challenges
Global Cyber Security Community

Policy
- APEC-TEL, ASEAN
- EU, EC, ENISA
- ISOC
- CCDCOE
- OECD
- OAS
- IGF
- Atlantic Council
- ITU

Operational/Response
- CERTs community: FIRST, APCERT, TF-CSIRT, GCC, OIC, EGC, IWWN...
- NOG community: AfNOG, NANO, PACNOG, MENOG, ccNOG
- CIP Domain ISACs
- Meridian: CIIP Directory
- TLD community: AFTLD, AP-TLD, CENTRE, LAC-TLD, RISG
- DNS-OARC
- Vulnerability Handling Community: CERTs, ICASI
- Malicious code analysis community
- IETF, IEEE

Law Enforcement
- G8 Lyon group
- Subgroup on High-Tech Crime
- Operators Security community: NSP-Trust, Ops-Trust, Etc..
- Abuse Response community: MAAwG, COUSE, Etc.
- DCC(BTF), Underground economy conference, Etc.
Key Initiative - Collaborative Response to Malicious Abuse of Domain Name System

• Events that threaten systemic security, stability and resiliency of the DNS
• ICANN will collaborate to mitigate malicious conduct enabled by the use of the DNS with:
  – DNS registries and registrars
  – Security research community
  – Security response community
  – Software and security/anti-virus vendors
  – Law Enforcement as appropriate

Security team contact point – security-ops@icann.org
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
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
• Collaboration can be difficult to sustain
  – Numerous and complex, harder to build and maintain, more fragile than botnets
• The risk-reward equation favors worm creators

Must have public – private collaboration & standing response capability
Lessons Learned

• Exploitation or misuse against domain registration services
• Major Hacking Attacks against domain registration accounts around April
  – Domain Hijacked
  – 5 ccTLD operators

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

• Used old protocol vulnerability (2008)
  – Response slow
  – Predicated on ability to find “key people”

• A coordination center would have improved situational awareness

Diagram of cache poisoning attack
Lessons learned

• Avalanche botnet
  – Targets financial sector
  – Exploits a limited number of names/registrars

• Complex coordination requires dedicated team
  – Security analysis
  – Domain Name Registries/Registrars
  – Information Sharing

Avalanche attacks in 2009
Source: Rod Rasmussen, October 2009
Situational Awareness Information Sharing

- ICANN security team sent out situation awareness bulletins to DNS registration community

- Potential attack against ccTLD Registration Systems (Published 13 July 2009)

- High volume criminal phishing attack known as Avalanche the delivery method for the Zeus botnet infector (Published 6 October 2009)
Collaboration with FIRST

• Raise awareness and knowledge in CSIRT community
  – Outreach effort began FIRST Kyoto July 2009
• DNS Security training for CISRTs under development
  – Joint effort planned for Nairobi in March 2010
  – Joint workshop at FIRST Miami 2010
Moving Forward: Affirmation of Commitments & Security, Stability and Resiliency

• "Preserving security, stability and resiliency" one of four major joint commitments
• Section 9.2 details specific responsibilities
  – Have a DNS SSR plan and update regularly
  – Community review every 3 years; first one in Oct 2010
  – Focus areas:
    • security, stability and resiliency matters relating to DNS
    • ensuring appropriate contingency planning
Global DNS CERT

Business case for collaboration in security

Pre-Decisional Version
Not for Further Dissemination
Mission of DNS CERT

“Ensure DNS operators and supporting organizations have a security coordination center with sufficient expertise and resources to enable timely and efficient response to threats to the security, stability and resiliency of the DNS”
Goals

• Gain DNS situational awareness and share information
• Improve response coordination within the DNS operational community
• Improve response coordination with the broader cyber security community
• Standing, accountable organizations serving broad range of stakeholders impacted by security, stability and resiliency of the DNS
Stakeholders by role
Stakeholders by interaction
Participation and feedback

• DNS CERT must respond to stakeholders
  – Serve the less advantaged operators and users
• Participation by key experts/organizations
  – Adds capability to CERT
  – Extends its geographic reach
  – Helps keep focus on constituency needs
Questions?

• Contacts:
  – Greg Rattray, Chief Internet Security Advisor
    greg.rattray@icann.org
  
  – Yurie Ito, Director Global Security Programs
    yurie.ito@icann.org