ccTLD security issues, attacks, conficker

John Crain
Senior Director, SSR

Sept 8, 2009

Bled, Slovania

The Internet as an Ecosystem

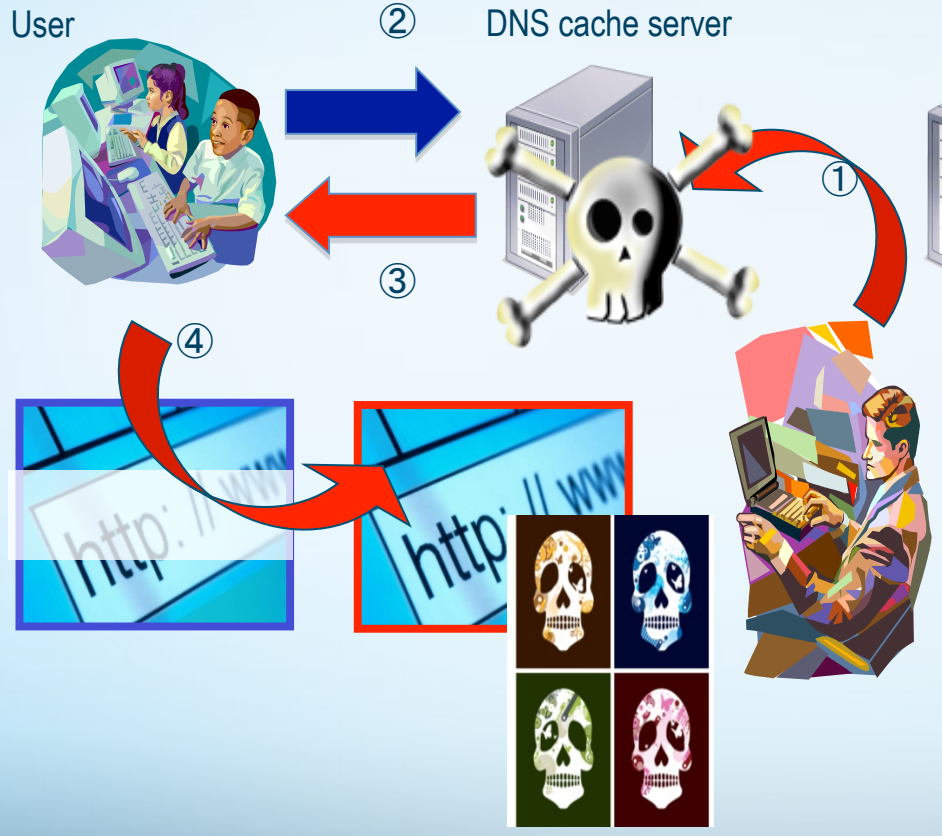
- Built as experiment; now part of everyday life
  - *Assumed benign, sophisticated and cooperative users*
- Now involves a wide variety of systems, stakeholders, opportunities & risks
  - Governments, corporations, civil society, criminals
- Malicious actors now use Internet
  - Growing centers of gravity – 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
  - 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



- 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 Team

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

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
- 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)

ccTLD
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 2009
  - Contingency Response Planning and Exercise Training Workshops Jordan and Seoul 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 2009 – 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 together, at an operational level.
  - 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

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

- There is an interest from the registrant community, especially “Big Business”, to see a more secure DNS registration environment.

- Will we see technologies that are used in the e-commerce and banking sectors, such as multi-factor authentication, become more prevalent in the DNS industry?

John Crain
Senior Director,
Security, Stability and Resiliency Programs
ICANN

john.crain@icann.org