

Internet Security and Resiliency: A Collaborative Effort



Baher Esmat
Manager, Regional Relations
Middle East

MENOG 4
Manama, 9 April 2009

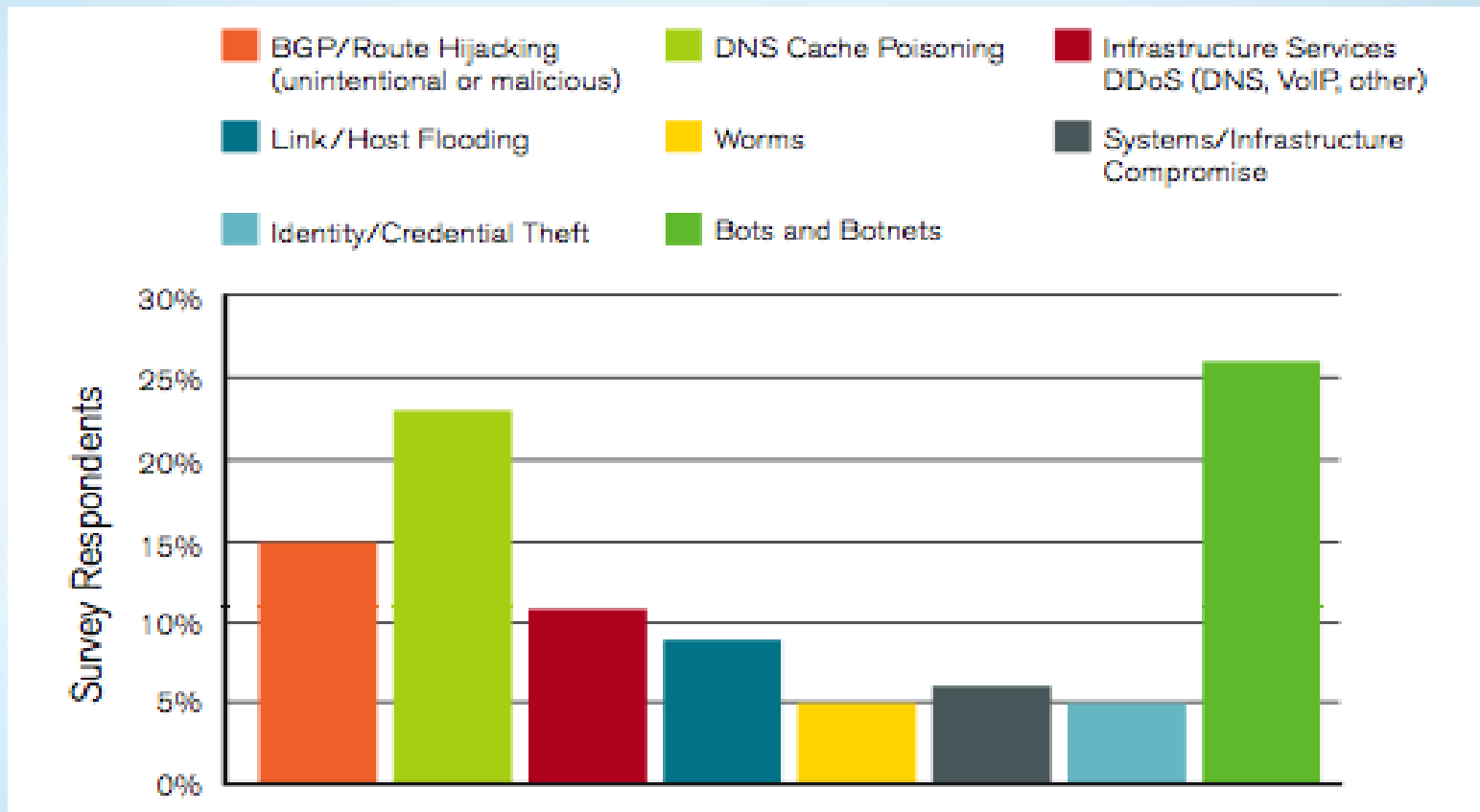
WHAT IS THIS PRESENTATION ABOUT?

ICANN's effort in enhancing security and resiliency of the Internet's unique identifiers

Internet's Threat Landscape

- Combine web, malware, botnets and spam (*Cisco 2008 Annual Security Report*)
- Botnets are becoming more sophisticated and more harmful
 - Almost 10% of computers on the Internet are infected by botnets (*Source: Emerging Cyber Threats Report 2008, Georgia Tech Information Security Center*)
 - From spam and DDOS, to financial fraud and espionage – and could also be “multi-tasking”
 - Techniques to hide (i.e. fast-flux)
- Growth in DDOS attack size – reached 40 Gbps in 2008 (*Source: Worldwide Infrastructure Security Report, October 2008, Arbor Networks*)
- Involvement of criminal organizations in malicious activities
 - 24-hour DDOS attack for \$35 (*Source: Global Threat Research Report: Russia, iDefense*)
 - Motives could be commercial or political
- Continuous DDOS attacks against core DNS operations; DNS vulnerabilities (i.e. cache poisoning)

Most Significant Threats



Risks to DNS

- Continued DDOS attacks against core DNS operations
 - Root servers
 - TLD operations
 - DNS service providers
- Cache poisoning
 - Kaminsky vulnerability
- Registry/Registrar failures
 - Technical
 - Business

CircleID

INTERNET INFRASTRUCTURE

Home | Blogs | News | Industry | Community | Topics

\$7.99 .mobi Domain - Save
Tell the mobile world who you are. #1 Best Overall - ICANN Accredited
GoDaddy.com

European domain names
Domains for Resellers and Providers Easy through Web- Mail- XML-API
www.realtimeregister.com

Home / News

Attack Seriously Slows Two Internet Root Servers

Feb 07, 2007 9:31 AM PDT | Comments: 9 | Views: 8,689

NETWORKWORLD News | Blogs & Columns | Subscriptions | Videos | Events | M

Security | LANs & WANs | VoIP | Infrastructure Mgmt | Wireless | Software | Data Center | SA

Anti-Malware | Compliance & Regulation | Desktop Firewall / Host IPS | Enterprise Firewall / UTM | IDS / IPS | NAC

Some UltraDNS customers knocked offline by attack

NeuStar confirms 'significant' denial of service attack on Tuesday morning

By Carolyn Duffy Marsan, Network World, 03/31/2009

Share/Email | Tweet This | 14 Comments | Print | Newsletter Sign-Up

NeuStar confirmed that some of its UltraDNS managed DNS service customers were knocked offline for several hours Tuesday morning by a distributed denial of service attack.

BBC Low graphics Help Search

NEWS

Watch ONE-MINUTE WORLD NEWS

Page last updated at 09:00 GMT, Thursday, 7 August 2008 10:00 UK

E-mail this to a friend | Printable version

Net address bug worse than feared

By Maggie Shiels
Technology reporter, BBC News, Silicon Valley

A recently found flaw in the internet's addressing system is worse than first feared, says the man who found it.

Dan Kaminsky made his comments when speaking publicly for the first time about his discovery at the Black Hat conference in Las Vegas.

He said fixes for the flaw in the



Attackers could use the loophole to redirect web users to fake sites

Why DNS Security Matters

- Significance of DNS
 - Essential to the effective operation of the Internet
- Managed as a distributed system with diffuse roles and responsibilities
 - User, ISP, Registry/Registrar, root server operator, ICANN
- Range of threats and risks
 - To user, to business, to the whole Internet

ICANN Roles and Responsibilities

- Mission: Coordinate, at the overall level, the global Internet's systems of unique identifiers, and ensure the stable and secure operation of such systems
- Core: Preserve and enhance the operational stability, reliability, security, and global interoperability of the Internet
- Contributor: Identifications of DNS abuse; challenges to Internet security
- Not involved in content control, spam, and areas related to cyber espionage and cyber war

What is ICANN Doing?

- Continued implementation of agreements
 - With Registries/Registrars on Data Escrow, WHOIS, other provisions
- Enhancing and exercising the gTLD registry continuity plan
- Working towards implementing DNSSEC at the root
- Participating in Anti-Phishing Working Groups and other forums to understand effective approaches to identify abuse
- Co-sponsored the first Global Symposium on DNS Security, Stability and Resiliency (<http://www.gtisc.gatech.edu/icann09>)
- ccTLD capacity building initiative in planning and response to disruptions
 - Partnered with ccTLD regional organizations to provide training/exercise events to develop capacity

A Collaborative Effort

- ICANN's efforts in this area ensure its partnership with other organizations and stakeholders
 - Root server operators; Registries and Registrars community
 - IETF and IAB
 - ISOC
 - RIRs
 - Regional TLD Associations
 - Regional NICs and NOGs
 - DNS Operations, Analysis and Response Center (OARC)
 - Forum of Incident Response and Security Teams (FIRST)
 - Anti-Phishing Working Group
- ICANN is engaging and will continue to collaborate with regional organizations and governments across the globe
- ICANN is also willing to pursue constructive collaboration with any relevant stakeholders to enable security, stability and resiliency activities

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



Table-Top Exercise (TTX) Workshop

- Techniques for Designing and Running Table-Top Exercises
- Hands-on Planning and Execution of an Exercise

ACRP – Progress To Date



Kuala Lumpur, May 2008

- Prototype with APTLD
- ~ 25 participants

Cairo, October 2008

- ~ 40 participants, 25 ccTLDs
- 4 regions
 - APTLD, AfTLD, LACTLD, CENTR
- ICANN, ISC, and ISOC



Mexico City, February 2009

- ~ 25 participants, 11 ccTLDs
- 4 regions
 - APTLD, AfTLD, LACTLD, CENTR
- ICANN



Upcoming Events

- “Mini” ACRP & SROC, Arusha, Tanzania, 13 – 15 April 09
 - During AfTLD meeting, sponsored by AfTLD
- ACRP Workshop, Nadi, Fiji, 26 – 28 April 09
 - During PITA meeting
- ACRP Workshop, Amsterdam, 11 – 13 May 09
 - Follows RIPE meeting, sponsored by CENTR

Information Sharing

- Bridge the experience gap between ccTLDs
- Engage the ccTLD community to collaborate with each other
- Combined ICANN/OARC effort to create a trusted TLD portal
- Provides access to templates, best practices, lessons learned, forums, etc

Prototype Site:

<http://tld-portal.dns-oarc.net>



The screenshot shows the homepage of the Top Level Domain Portal. The header features the title "Top Level Domain Portal" in a large, bold font. To the right of the title is a search bar with the text "Search: OR" and a "GO!" button. Below the search bar is a "Advanced Search" link. In the top right corner, there is a login form with fields for "Username:" and "Password:", and a "Forgot Password Register" link.

The main content area is divided into several sections:

- NEWS:** A list of recent news items, including "1 Dec 08 - Los Angeles, CA ICANN & ISOC Announce Partnership for TLD Portal" and "24 Dec 08 - San Antonio, TX TLD Portal Takes Shape".
- Forums:** A section for discussion boards on topics like Q&A, troubleshooting, and collaborative efforts.
- Case Studies & Lessons Learned:** A section for specific examples on security, configuration, and day-to-day operations.
- Presentations / Documents / Templates:** A section for conference presentations, operating documents, and templates for contingency response and critical communications plans.
- Training & Course Support:** A section for online workshops, webinars, training materials, and wikis.
- How-To:** A section for step-by-step operator guides and checklists for incident response, technical implementation, and day-to-day operations.
- Calendar:** A section for listings and information for upcoming events of interest to the TLD community.

On the right side of the page, there is a "What's New on Your Portal:" section with a list of updates, including "12/24/08 - Site Design Updated" and "12/26/08 - ACRP Cairo Content Added". Below this is a "Calendar of Events:" section for January 2009, which includes a calendar grid and a list of events such as "01/01/09 - Happy New Year!", "02/18/09 - NSRC Network Management Course", and "02/21/09 - ICANN TTX Workshop".

A Recent Event: Conficker C

- Represents the third major revision of the Conficker malware family
 - Previous revisions (A and B) focused on a limited number of domain names
 - Conficker C seeks large number of domain names - 50,000 randomly generated names a day -116 zones of 110 top-level domains
- Collaboration among security, vendor and DNS communities to disseminate information about how the malicious code may seek to leverage the DNS system
 - Conficker Working Group (<http://www.confickerworkinggroup.org/wiki/>)
 - ICANN helped reach out to 110 TLD Registry
- Activation date: April 1st 2009
 - Nothing major was expected to happen
 - More than one million infected computers around the world (<http://www.networkworld.com/news/2009/040309-confickerc-controls-4-of-all.html?page=2>)
 - Cooperation will continue to stop the spread of the worm and block control of the infected computers
- Resources:
 - <http://mtc.sri.com/Conficker/addendumC/>
 - <http://www.f-secure.com/weblog/archives/00001647.html>
 - <http://confickerworkinggroup.org/wiki/>

Conclusions

- ICANN understands its role going forward must include plans and activities related to making the DNS a more secure, stable and resilient environment
- ICANN also recognizes the limits to its role and resources and its strategy in this area plans to rely heavily on partnerships and a wide ranging collaboration

ICANN's Security Team

A group of senior staff focusing on security issues that relate to ICANN and the Internet's Identifier Systems

Greg Rattray, Chief Internet Security Advisor

John Crain, Chief Technical Officer

Geoff Bickers, Director of Security Operations

Thanks!

baher.esmat@icann.org

