Protecting Your Infrastructure from the Coming Scourge: DDoS, Hijacking, & Conficker

APTLD Meeting
August, 2009

Presented by:
John Kane
VP, Corporate Services
Afilias
Agenda

• Current security issues facing your DNS Infrastructure

• Why Diversity is the Key to Securing your TLD

• Options to Increasing your DNS Diversity
• DNS is the technology that underpins the development and functionality of the Internet
• Since DNS was developed, the use and effect of the Internet has fundamentally shifted
• The Internet is now mission critical to EVERYONE and ALL communications

Future looking:
DNS and DNS networks need to be based on:
1. a stable, reliable security model to thwart criminal attacks
2. a diverse, scalable network with no single points of failure
Today’s Security Threats

Largest Attack Size – 40 Gigabits Per Second

![Bar chart showing the largest attack size from 2001 to 2007.](image)

Most Concerning Threats

- BGP/Route Hijacking (unintentional or malicious)
- DNS Cache Poisoning
- Infrastructure Services DDoS (DNS, VoIP, etc.)
- Link/Host Flooding
- Worms
- Systems/Infrastructure Compromise
- Identity/Credential Theft
- Bots and Botnets

![Bar chart showing the most concerning threats.](image)

Figure 1: Largest Attack Size – 40 Gigabits Per Second
Source: Arbor Networks, Inc.

Figure 4: Most Concerning Threats
Source: Arbor Networks, Inc.
Today’s Security Threats: DDoS

• What is it?

• DDoS attacks are increasing in number and damages

Source: shadowserver.org
DDoS attacks are increasing in number and damages
  • Daily attacks targeting everyone, not just big brands
    • Used for extortion or reputation damage

  • Major reference events in the last week = Twitter/ Facebook / Live Journal and others targeted
    • Due to political motivations to silence one blogger

  • Mitigate your risk by adding diversity in your DNS
Implementing DNS Diversity

Diversity at all levels

- Multiple DNS providers
- Multiple types of DNS software (e.g. : Bind + NSD)
- Geographically diverse datacenters and NOCs
- Geographically diverse DNS node constellation on multiple continents
- Nodes configured with Anycast technology
- Multiple bandwidth providers w/ min. 1 gbps
- Multiple brands of hardware (e.g: both Cisco and Juniper Routers)
- No single OS or other software
- Diversity in Personnel and expertise
5 elements of DNS Diversity

1. Diversity of DNS software and providers
2. Geographic diversity in DNS node architecture
3. A diverse physical infrastructure relying on multiple brands and suppliers
4. Multiple connectivity providers for each DNS node
5. Diversity in personnel and expertise
Today’s Security Threats: DNS Hijacking

• DNS Hijacking, also known as man-in-the-middle attack or cache poisoning
  • Allows a malicious actor to get between a visitor and your Web site – WITHOUT YOU KNOWING!

• DNSSEC is the best solution
  • US government mandated .gov and .mil to be signed by end of 2009
  • 12 countries in total signed today
  • Afilias signed .ORG on behalf of PIR – June 2009
Today’s Security Threats: Conficker

- One of the top 10 most prolific Internet worms
  - What will it’s next incarnation be?

- Effects of Conficker
  - gTLD and ccTLDs with over 110 targeted
  - New policies required for blocking names
  - Increase DNS query volume and traffic spikes
  - TLD Reputation

- What are the solutions?
  - Need for stable and proven registry system and abuse prevention policies
  - Have the technical and policy resources available internally
  - Monitor for signs and contact global community

- Have an infrastructure that can handle high traffic volume and queries
Today’s Security Threats: Conficker

Conficker
Daily Population

Source: Conficker Working Group and ShadowServer.org
• No other Internet technology matters if users can not get to the Web site, or the e-mail can not be delivered.
• Treat your DNS like you do any other technology – Build your network with diversity
• Build it with redundancy, scalability and ensure *no single points of failure*

**To deploy diversity across your DNS your options include:**
1. Internal development
2. Adding an outsourced provider
• Outsourcing or adding a Secondary DNS provider adds a high level of diversity
• Afilias Managed DNS Provides Security based on Diversity
  – Anycasted
  – Geographically dispersed across 18 locations
  – Cisco and Juniper routers, multiple hardware providers
  – Multiple firewall and load balancer providers
  – 3 network monitoring tools
• Advanced Distributed Denial of Service (DDoS) protection and mitigation
• DNSSEC capable
• High capacity bandwidth (providers with >1 gbps)
• Afilias linked to international security experts: CERTs, ICANN’s SSAC, APWG
Afilias supports 15 TLDs

- Superior, proven registry services
- Diverse DNS Network handling BILLIONS of queries daily
  - We offer both Primary DNS services and Secondary DNS services
- Scale/Knowledge/Experience of ~15million registrations

Generic & Sponsored TLDs

- .info
- .org
- .mobi
- .Asia
- .aero

Country Code TLDs

- .bz
- .HN
- .Nic.Ar
- .Gl
- .in
- .VC
- .LC
- .MN
- .SC
- .Me
Thank you!

John Kane
jkane@afilias.info
www.afilias.info/dns