DNS STABILITY, SECURITY AND RESILIENCY

Meeting Report of the 4th Global Symposium

25 October 2012, Las Croabas, Puerto Rico

ICANN

Anti-Phishing Working Group APWG

The 4th Global DNS Stability, Security and Resiliency Symposium
25 October 2012, Las Croabas, Puerto Rico

Report

Editors:

Steve Sheng, *Internet Corporation for Assigned Names and Numbers*
Dave Piscitello, *Internet Corporation for Assigned Names and Numbers*

Contributors:

G.Aaron, R.Arends, J.Crain, J. Dunn, S.Powell. R. Rasmussen.

Sponsors:

Internet Corporation for Assigned Names and Numbers (ICANN)
The Anti-Phishing Working Group (APWG)

Table of Contents

Executive Summary

The 4th Global DNS Stability, Security and Resiliency Symposium, held in conjunction with the 2012 Anti-Phishing Working Group (APWG) Fall General Meeting and eCrime Researchers' Summit[1], focused on the *abuse or misuse* of the DNS and domain registration systems.

Participants from academia, security and DNS operations communities, and global DNS ecosystem stakeholder groups met to discuss operational and policy issues and challenges related to the DNS abuse or misuse.

Symposium participants brainstormed and identified 14 major threats they observe in their research, daily operations or anticrime (mitigation) activities, and then grouped these into (1) threats to the DNS infrastructure, and (2) misuses of resources.

Threats to the DNS Infrastructure	**Resource Abuse Issues**
Distributed Denial of Service (DDoS) Attacks Open misconfigured resolvers Broken DNS software Lack of adoption or incorrect implementation of DNSSEC DNS tunneling Spoofing Transparency /Accountability of Root server operators (lack of contracts of root operators and the contents delivered)	Malicious Registrations Domain Generation Algorithms (DGAs) Malicious use of URL shorteners Use of DNS as a persistent architecture for use in attacks Hijacking (DNS account, names) Binaries delivered via the DNS Malicious use of Dynamic DNS providers

Of the 14 issues listed above, symposium participant chose six threats and explored in detail the problem space and proposed potential mitigation options for the community's consideration.

[1] http://docs.apwg.org/events/2012_ecrime.html

Introduction

As a core element of the Internet infrastructure, the domain name system (DNS) has a direct and signficant impact on the performance and dependability of nearly all aspects of interactions on the Internet. The broad constituency that use or provide name resolution services, from DNS Registries through to individual Internet end-users, all have an interest in ensuring that the DNS operates in a secure, stable and resilient manner.

Since 2009, experts from the DNS community have met annually to initiate and discuss the security, stability and resilience of the DNS. This report summarizes the outcome of the fourth symposium.

The fourth symposium focuses on the *abuse or misuse* of the DNS and domain name registration services. Stakeholders from academia, government, technical and DNS operations communities considered and attempted to categorize the large and diverse set of malicious or criminal activities that abuse or misuse the DNS or domain name registration services, and discussed operational and policy issues and challenges related to the DNS abuse or misuse.

Symposium organization and method

The theme for this Fourth Symposium was *Interaction, Creativity, and Involvement*.

From its inception, the Symposium was designed to encourage free thinking and brainstorming. Volunteers selected by the Steering Committee moderate breakout sessions. Aside from an invited keynote speech and nominal opening remarks delivered by moderators, participants are not expected to prepare lectures or presentations in advance. Participants are invited to share their perspectives and to collaborate to lend clarity to or advance current thinking related to the DNS issues discussed in each session.

The symposium operates under the Chatham House Rule[2], which allows for the candid sharing of information without regard for or concern over attribution.

The organizers arranged two sessions for this symposium:

1. Morning session: The role of Domain Name System in electronic crime.

2. Afternoon session: Classification of abuse cases and framework for sharing data.

Dr. David Dagon, a renowned and respected member of the academic and security research communities, delivered a keynote presentation on the "off-label" use of

[2] *Chatham House Rule:* "When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed." http://www.chathamhouse.org

DNS to frame the discussion. Dr. Dagon's presentation stands on its own merit and no summary is included here.

A well-known expert from the anti-abuse community moderated the first session, while the second session was lead by an equally well-known expert from the DNS operations community. Scribes were assigned to each session and their notes form the bases of the reports of the proceedings, which follow.

Morning Session: Role of the Domain Name System in E Crime

Criminals and miscreants leverage or exploit the domain name resolution and name registration systems. The purpose of this session was to gather input from participants on the roles that domain names (and the DNS) play in electronic crime, catalog and categorize these, and to consider or formulate methods to mitigate e-crime facilitated by domain names and DNS.

Framework for Categorizing Issues

Symposium participants brainstormed and identified 14 major threats they observe in their research, daily operations or anticrime (mitigation) activities, with the intention to consider as many as possible in the time allocated. They then grouped the threats into two categories: (1) threats to the DNS infrastructure, and (2) misuses of resources. Table 1 illustrates this categorization. A check (√) indicates a topic was discussed.

Threats to the DNS Infrastructure	Resource Abuse Issues
√ Distributed Denial of Service (DDoS) Attacks	√ Malicious Registrations
√ Open misconfigured resolvers	Domain Generation Algorithms (DGAs)
√ Broken DNS software	Malicious use of URL shorteners
√ Lack of adoption, incorrect implementation of DNSSEC	Use of DNS as a persistent architecture for use in attacks
DNS tunneling	Hijacking (DNS account, names)
√ Spoofing	Binaries delivered via the DNS
Transparency/Accountability of root server operators	√ Malicious use of Dynamic DNS providers

Threats to the DNS Infrastructure

For each identified threats to the DNS infrastructure, the participants attempted to define the problem and enumerate existing (known) mitigations. Summaries from DNS infrastructure threat discussions follow.

DDoS attacks / Botnets / Open Misconfigured Resolvers

Problem Space

DDoS attacks against any element of the DNS are easy to execute because:

1) The DNS protocol is suitable for amplification, where a small query can instigate a large response,
2) Parts of the infrastructure can be less resilient as compared to attacks on Port 80 because organizations may invest more heavily in online (commercial) presence than in their name server infrastructure, and
3) Attackers are able to leverage the existence of many misconfigured open-resolvers in reflection attacks.

It should be noted that DNSSEC would not be able to solve this problem, and in certain cases, DNSSEC itself is exploited in attack scenarios. Specifically, because DNSSEC responses can be significantly larger compared to non-signed responses, they are useful in amplification attacks; in certain of these attack scenarios, e.g., where servers and clients are not DNSSEC-capable, DNSSEC resource records may be less readily detectable from other resource records (e.g., TEXT) that have been used in amplification attacks.

Potential Solutions

Black hats search the Internet for open recursive resolvers to exploit and employ in DDoS attacks. In response, white hats try to enumerate open recursive resolvers, and then attempt to contact the operators to encourage them to correctly configure (e.g., configure according to BCP 140[3]). Participants identified the following potential mitigations to this threat:

- (More) aggressively identify open resolvers and encourage operators to correctly configure the resolvers so they cannot be used as attack platforms.

- Promote awareness and use of BCP 140 and similar mitigation methods through publication and social media.

- Adopt a policy that "names and shames" or penalizes resolver operators who do not comply with best configuration guidelines.

- Mitigation IP spoofing. Many operators currently do not implement BCP38. Increasing pressure from regulatory or law enforcement agencies might change the risk calculation of these operators to implement BCP38.

- Encourage government procurement agencies to make BCP38 and BCP 140 requirements for government use of Internet access services and name service operations (DNS hosting).

[3] BCP 140, Preventing Use of Recursive Servers in Reflector Attacks, *tools.ietf.org/html/*bcp140

- Promote the use of DNS response rate limiting[4], blocking, null routing and other accepted countermeasures among (all levels of) DNS operators.

Broken DNS Software

Problem Space

Symposium participants noted that implementing DNS resolvers is difficult (and a separate issue from configuring open resolvers). Recursive DNS server software development has a long learning curve that demands considerable knowledge of DNS, familiarity with general-purpose or specialized operating systems, networking protocols, and sound (secure) programming skills. The challenge of developing interoperable, "correct" implementations is exacerbated due to ambiguities in DNS standards. These factors contribute to problems in many implementations of recursive DNS servers.

An example of how these factors conspire to complicate DNS software development serves to illustrate this problem space:

> *A DNS recursive server is supposed to wait 5,000 milliseconds (5 seconds) for a response from an authoritative, as defined in the RFC. However some recursive resolvers stop waiting for a response after 300 milliseconds. In a case where the authoritative is just out of range, the client will hop recursive servers and trigger a 'query storm' against both the recursive and the authoritative servers.*

With the introduction of new gTLDs, some new top-level domain operators wish to write their own DNS resolvers. Thus the problem space could expand (perhaps quickly).

Potential Solutions

Participants discussed the following potential solutions:

- Encourage or develop directly a tool that performs conformance testing to ensure standards are upheld and open resolvers work and interoperate as intended. FPDNS[5] is one example of a program to do tests that identify resolvers that generate non-compliant DNS messages.
- Encourage IETF to develop "resolver requirements" as it has done in the past with hosts[6] and routers[7,8].

[4] Vixie. P. *DNS Response Rate Limiting (DNS RRL)*. ISC Technical Note Series. Available at: http://ss.vix.com/~vixie/isc-tn-2012-1.txt

[5] https://www.dns-oarc.net/tools/fpdns

[6] http://*www.**ietf**.org/rfc/rfc1123.txt*

[7] http:// *www.ietf.org/**rfc**/**rfc**1812.txt*

[8] http://tools.ietf.org/html/rfc6204

Lack of adoption or incorrect implementation of DNSSEC

Problem Space

DNSSEC adoption for second and third level domains is low. For example, only 0.13% of .com domains is secured with DNSSEC[9]. Moreover, few resolvers validate signatures.

Participants cited several reasons for lack of adoption. From many organizations' IT managers' perspectives, the return of investment (ROI) on DNSSEC is not high compared to other projects such as managing IPv4 exhaustion, mobile devices, and implementing IPv6. Lack of registrar implementation (passing DS records) also inhibits adoption, although registrar offerings are also a reflection of market demand. Even if adoption were to increase, the utility of DNSSEC will remain limited until applications provide adequate user feedback or awareness at the client level.

Providers and DNS operators claim that the return of implementation is too low, in part due to low demand from users. They further contend that DNSSEC makes name resolution brittle: if DNSSEC is implemented improperly, or if key management is executed poorly, an organization's name service is disrupted in a manner that is different from any disruption they currently manage, and operators contend that protracted time to restore name service can hugely impact performance, profit-loss, or (customer perceived) stability of platforms or services.

Potential Solutions

The solution space is very broad and affects users, clients, resolvers, name servers, authorities and their zone data management.

Participants commented that registrars are beginning to accommodate registrants who choose to upload DS records directly. Some registrars provide DNSSEC signing services for customers that use the registrar's operated name servers (hosted DNS). Some registries use money as an incentive while others use regulation (e.g., the .gov registry requires all second level domains to implement DNSSEC and conform to NIST standards).

Participants also noted that some progress has been made in making applications DNSSEC-aware:

- *Windows 8* is performing DNSSEC validation at the recursive level, and the OS encrypts the traffic between recursive and stub resolver. This suggests that Microsoft will unlikely do validation at the stub resolver level.
- *Google Chrome* is checking DNSSEC if all other validation fails (SSL)
- *DNSSEC validating add-ons, extensions or plug-ins for browsers (e.g., Firefox) are available*

Participants next considered the question; "Should there be a killer application for DNSSEC?" Here, participants expressed different opinions. Proponents pointed to

[9] http://scoreboard.verisignlabs.com

the fact that having a killer application for DNSSEC changes the risk profile for enterprises and increases the incentive for further DNSSEC adoption. Opponents argued that DNSSEC is designed to be an error detection mechanism. Finding a killer application is finding a solution in search of a problem.

Lastly, participants considered the question; "How can DNSSEC adoption be accelerated?" Suggestions included:

1. Simplify managing DNSSEC (generating keys, signing, management): for consumer, mass market, reducing management of DNSSEC to a single action (click and done) may make DNSSEC attractive.
2. Use DNSSEC to secure additional records: e.g., DNAME with validation performed at or by the end client.
3. Move validation closer to end client: e.g. validation at stub resolver level.
4. Have registries sign DNSSEC for domains: Registries may provide a service for the registrant to defer the signing and escrow of their domains, likely for a small fee, to enable DNSSEC per-domain, without the registrar (or reseller) needing the infrastructure itself.

Resource Abuse Issues

For each identified resource abuse issue, the participants attempted to define the problem and enumerate existing (known) mitigations. Summaries from each resource abuse discussion follow.

Domain Name Registration Abuse

Problem Space

Various domain name blacklists exist and several of these collectively identify approximately 3.5 million malicious domains during the course of a year. One participant's back-of-the-envelope calculation shows that nearly 5% of the total gTLD and ccTLD domains registered every day appear on these black lists at some point during their first year of registration, and they are in nature malicious in one way or another, either by their association with spam (e.g., advertised via spam, often sent via botnets), malware and phishing,, or botnet command-and-control mechanisms[10]. Participants agreed that this is a large number and that reducing or discouraging registration abuse is an important objective to pursue.

Potential Solutions

Participants discussed the following potential solutions:

- **Registrant verification.** Some participants suggest that verifying the email address, phone number, contact information and organization affiliation would enhance accountability, and would prove more helpful for identification in the case of malicious use or abuse.

[10] http://toronto45.icann.org/meetings/toronto2012/presentation-detecting-abuse-tld-aaron-young-15oct12-en.pdf

- **Reputation systems** for email accounts, source IP, account registrant, browser finger printing, nameservers assign reputation (often in the form of scores) to each of these identifiers based on its abuse history. Participants posited that reputation systems would enable policy for blocking used by various intermediaries such as routers, email gateways, firewalls, etc.
- **Class-action lawsuits against a registry or registrar that does not suspend domains.** This drastic action stimulated a discussion that centered around questions that would need to be addressed for any class action, including: 1) Who would be parties to the class action (e.g. users, phishing targets?); 2) Is the action directed only at registry operators, or could include other parties such as registrars, 3) What would be the nature of or grounds for the complaint?
- **Block all names registered by a malicious registrar** or reseller (one that is unresponsive to abuse reports, or is allegedly complicit): A proposed solution to such registrars is to block all lookups at-will on recursive servers to prevent any resolutions for names coming from that registrar or domains under its control. This can be achieved through IP/nameserver reputation or Whois lookup. This action has numerous implications for registrars whose portfolios are not 100% malicious, and for their law-abiding registrants.
- **Identify an abuse metric and deny (or regulate) the ability to add domains (register new domains) to registrars who exceed the metric.** For example, use the APWG Global Phishing report metric but apply it to registrars. Registrars that exceed the mean cannot register new domains. This would affect how spammers in particular might register domains.
- **Publication of abuse statistics so that end users can make an informed decisions regarding when selecting a registrar.** Publications of statistical information on registrars may help inform users and implementers of systems, aiding them to avoid using them for registrations and perhaps in systems like web browsers and email clients. Browsers could, for example, color address bars differently based on registrar reputation data.

Participants discussed the major challenges that security responders and interveners face when attempting to mitigate threats associated with malicious registrations:

- Many registries and registrars will not suspend a domain without a court order. What solutions to this problem provide for expedited intervention and due process?
- Many ccTLD registrars are not ICANN-accredited and thus pose a different set of problem related to policy enforcement. Their registrations are governed on a ccTLD-by-ccTD basis, according to each TLD's terms of service.
- What liabilities (e.g., litigation) inhibit publication of abuse statistics?

- Attackers take heavy advantage of the nature of the DNS, which is a decentralized system, and it is easy for an attacker to pack up and move from one registrar (or registry) to another without much difficulty.

IP Address Registration Abuse Issues

Problem Space

Participants discussed the question, "Why aren't RIRs involved in assisting in migitating abuse?" One major spam blacklist provider has 6.7 million IP addresses on its blocked list. Participants identified a few possible reasons:

- **Lax policy**. The self-governing RIRs have not shown interest in anti-abuse policies for the numbers space (unlike ICANN, domain registries, and domains registrars have on the naming side). Participants reported that in certain instances, large address blocks appear to be allocated with little identity assertion or verification. Invalid and out-of-date WHOIS records for at the RIRs is a known problem.
- **Complex problem space**. There are some abuses types native to IP space: route injection (advertisement), IP or ASN block hijacking, registration hijacking. However, much of the problem is ownership of IP allocations by criminals, using those blocks for spamming, bulletproof hosting, and other abusive uses.
- **Resources.** RIRs usually do not have dedicated staff to handle abuse.
- **Coordination.** There is little coordination among RIRs and domain name registry/registrar operators to correlate domain name and address space abuse. ARIN has an effort to verify IPv4 allocations – in some cases attackers have registered expired or parked domains because these domains are used in POC information for IPv4 allocations and the criminals can gain ownership – but this effort is not adopted universally across RIRs.

Malicious Use of Dynamic DNS Providers

Problem Space

Dynamic DNS services provide support for dynamic IP addresses and the capability to issue propagated IP updates as soon as a change is made. These services enable individuals and small systems that do not have static IP address to use the domain name system. However, this feature can also be abused to allow attacker to constantly switch IP addresses within a botnet. One participant estimated that at any given time, 50% of dynamic DNS are botnet.

Dynamic DNS providers are often small operations that do not have the staff or infrastructure to properly enforce policy on their own systems. Many do not have any policies at all, and let their users free-roam. Verification of users in DDNS systems is increasingly more difficult, as much of the time the third+ level domains are free.

Potential solutions

Participants discussed the following potential solutions:

- In general, the dymanic DNS provider space is responsive to anti-abuse community requests. So the best path forward is for the anti-abuse community to work with dynamic DNS providers and **develop best practices** to identify and mitigate abuse.
- Given there is no authority over the dynamic DNS providers, a **reputational system** is also a good approach to dealing with providers that do not have a functioning abuse protocol or are in general malicious themselves.

Summary of Issues and Proposed Ideas

The table below summarizes the proposed mitigation ideas for some of the threats discussed in the morning session of the symposium.

Issue	**Mitigation Ideas**
DDoS / Botnet / open misconfigured resolvers / Spoofing	Identify open misconfigured resolvers; encourage BCP 38 & BCP 140 implementation; DNS response rate limiting
Broken DNS Software	DNS implementation conformance test suite; BCPs or Internet standard for resolver requirements
Lack of adoption or incorrect implementation of DNSSEC	Regulatory requirement; incentives; simplified management, DNSSEC aware applications
Domain Name or IP Registration Abuse	Registrant verification; reputation system; class action lawsuits; registry-registrar selection contracts; block lists; abuse statistics; coordination among RIRs and domain registry/registrar operators
Misuse of Dynamic DNS Providers	Block list more subdomains; reach out to dynamic DNS community leaders; reputational system.

Afternoon session: classification of abuse names and sharing data

Many organizations produce lists of domain names (or hyperlinks) that they have investigated and determined to be malicious or "abusive" or used in association with criminal activities. This session examines:

- What are the current mechanisms for classifying and distributing such data?
- Are conventions or practices for normalizing these data worthwhile?
- Can these facilitate accessibility and utility?

Practical challenges for mitigating abuse include:

- **Complexity:** There are over two hundred domain registries of different sizes and capabilities for handling abuse. Each registry has its own protocols and policies defined as per capacity and needs to be treated appropriately. This means peer-to-peer communication from the anti-abuse community to the domain registry does not scale very well.

- **Resource issue:** Even if most of the large registries started sharing data between all others, some registries still do not have the resources to act on such data.

- **Diversity of laws:** Some from the community has been calling for uniform Terms of Service that would apply to every domain registry. This concept is limited due to the diversity of laws across countries. Registrants can be in one country, registrars can be in another, and registries can be in yet another country. Which laws are followed?

Solutions that could improve abuse mitigation include:

- Collaboration between the APWG and Registries to deploy a trusted accelerated abuse process.

- Publish contact information for abuse-related reporting to registry and registrar operators, possibly coordinated by or proxied through APWG.

- Identification of resellers and their abuse contact information.

Classification of Abuse Domains

Participants discussed whether having an agreed-upon abuse classification system for handling abuses would be beneficial. Operational decisions are often made depending on the classification of abuses. Participants devoted much of the afternoon session to developing a straw man classification for the community to consider, agree upon, and adopt for abuse reporting and handling.

The participants began by compiling a list of types of abuse. During the preparation of this Report, the editors and contributors reviewed the list and included the definitions that were formally defined in documents or resources provided by the NCFTA, Internet Identity, or the GNSO RAPWG. The following list emerged from this process:

- **Cybersquatting:** the act of deliberate and bad-faith registration and use of a name that is a registered brand or mark of an unrelated entity, often for the purpose of profiting.

- **Front-running:** a party obtains some form of insider information regarding an Internet user's preference for registering a domain name and uses this opportunity to preemptively register that domain name.

- **Fake renewal notices:** misleading correspondence sent to registrants from an individual or organization claiming to be or to represent the current registrar.

- **False affiliation:** Web site that is falsely purporting to be an affiliate of a brand owner.

- **Cross- TLD Registration Scam:** a deceptive sales practice where an existing registrant is sent a notice that another party is interested in or is attempting to register the registrant's domain string in another TLD.

- **Domain tasting:** Abuse of the Add Grace Period through continual registration, deletion, and re-registration of the same names in order to avoid paying the registration fees.

- **Phishing:** Web site fraudulently presenting itself as a trusted site (often a bank) in order to deceive Internet users into divulging sensitive information.

- **Spam:** Bulk unsolicited e-mail often sent using illegitimate means (e.g., obscuring the sender's identity, via botnets, or snowshoe spam) or advertising some other abuse (e.g., 419 scams, malware, illegal pharma, etc.).

- **Malware:** a piece of software (a malicious executable) used for criminal activity.

- **Botnet:** a collection of computers used without authorization by an attacker to perpetrate many kinds of malicious activity, including distributed denial-of-service attacks (DDoS), spam, and fast-flux hosting of phishing sites.

- **Stolen Credentials:** the act of using stolen identity, access, or financial credentials to register domain names for malicious purposes.

- **Parasite:** A website which collects user credentials while claiming to provide a value-adding service that is potentially malicious and contains target brand(s).

- **Mule Recruitment:** A job posting used to recruit unwitting participants into a money laundering scam. The mule can be in URL or email form.

- **419:** Advance-fee fraud in which the scammer solicits upfront payments promising large sums of money.

- **Lottery Scam:** Fraud that informs the victim they've won a prize, usually monetary, and requests victim's sensitive information in order to process transfer of winnings.

- **Fake Escrow:** Fraud that requests the victim to provide funds to a 3rd party (escrow) service in order to process a transaction.

- **Evil DNS Server:** Server providing Domain Name Services solely for domains used for criminal activity.

- **Credential Gathering:** Unauthorized collection of credentials by a 3rd party for a value add service, or an unbranded clone or copy.

- **Unauthorized Distribution:** Distributing products in a manner or format that was not authorized by the content owners, or an authorized representative.

- **Rogue (Illegal) Pharma:** An online retailer that sells or distributes controlled prescription drugs without FDA registration, or an online retailer sells or distributes pharmaceutical products without a valid prescription including the sale of counterfeit versions of over the counter medications.

- **Financial Fraud:** Branded Sites that promote the "Get Rich Quick" products and similar schemes (Pyramid, Ponzi).

- **Fake Gift Cards:** Selling or distributing of gift cards of a major retailer that either has no money value or buyer will never receive.

- **Credential Distribution:** Online facility (forum, chat room, etc) that promotes exchange of user credentials.

- **Hacker Dialog:** Online website that provides information to or from hackers

- **Spam Bot:** Mail server used with intent to send high volumes of emails related to fraudulent activity.

- **Malicious IP:** An IP address determined to be setup for the sole purpose of conducting fraudulent activity.

- **Malvertising:** An advertisement on a website or ad network, setup to infect viewers with malware either every time it is seen or at various intervals based on time or number of hits.