# SAC 032
# Preliminary Report on DNS Response Modification


An Advisory from the ICANN
Security and Stability
Advisory Committee
(SSAC)
June 2008

# Introduction

The Response code (RCODE) field of the DNS protocol[1] provides a means for a name server to signal and describe problems it encounters when attempting to respond to a query from a client (resolver). An authoritative name server will return an RCODE set to the value *Name Error* to indicate that the domain name in the query does not exist. Internet standards also use the terms a *non-existent domain* or *NXDomain response* to describe this error response[2].

The Name Error value is only meaningful in responses from an authoritative name server. In some cases, domain registrants entrust their authoritative name service to internal staff; in others, they entrust an external organization to manage their DNS. SSAC calls these entrusted name service agents or simply, Entrusted Agents. DNS clients customarily do not query authoritative name servers directly. Rather, the majority of DNS queries are resolved by intermediary systems known as *iterative resolvers*. Iterative resolvers may be operated privately by any organization. They are also operated publicly by service providers that host name services on behalf of customers or offers domain name resolution to subscribers. Whereas domain registrants commonly have a business and trust relationship with entrusted agents, they do not generally have such relationships with all operators of iterative resolvers. Thus, in this report, we use the term *third party* when we speak of this class of name service providers.

In this preliminary report, we describe the practice of DNS response modification by entrusted agents or third parties. In the first case, an entrusted agent receives a DNS query for a name. The entrusted agent determines that the name in the query does not exist in the zone file it hosts for the domain registrant, but rather than returning a DNS response indicating a *non-existent name*, the entrusted agent returns a response indicating the name exists and containing an IP address mapping for the queried name of the agent's choosing. In the second case, a third party operating an iterative resolver receives NXDomain responses generated by an authoritative name server and silently alters the contents, changing the *non-existent name* response to one that signals *name exists* and inserting an IP address mapping for the queried name of the third party's choosing.

This behavior is known by various labels: subdomain redirection, NXDomain redirection, NXDomain rewriting, NXDomain hijacking, subdomain hijacking, error resolution, and error marketing. These labels illustrate that the practice has commercial significance and is controversial.

The purpose of this report is to describe the effects of DNS response modification on domain name registrants, DNS operators and Internet users, and to explore possible exploitation of the practice by bad actors. This initial report focuses on explaining the effects of and unintended consequences to users, domain registrants, and those who rely on non-existent domain responses for error reporting and administrative purposes.

---

[1] See RFC 1035, Domain Name System Implementation and Specification, http://rfc.net/rfc1035.html and IANA registry http://www.iana.org/assignments/dns-parameters

[2] RFC 2308, NXDomain, http://rfc.net/rfc2308.html

# What is DNS response modification?

DNS response modification is a practice whereby a name server provider returns a DNS response message signaling *name exists* rather than a one that indicates a non-existent name when a name is queried but that name is not published in a domain registrant's zone information. In some cases, the domain registrant's entrusted agent uses the opportunity presented by the non-existence of a name within a domain (e.g., a typing error such as ww.example.com for www.example.com) to return a *synthesized response*, i.e., a IP address mapping for the queried name of its choice. The entrusted agent may use a common or default IP address mapping for all queried names that are not published in the zone file: this is called *wildcard synthesis.*

In other cases, an iterative resolver operated by a third party will examine DNS responses to queries it has attempted to resolve on behalf of its clients. When a DNS response is discovered to contain a response code set to the value *Name Error*, the third party configures the iterative resolver to silently alter[3] the contents of that DNS response before forwarding the message towards the client that originated the query. Specifically, the iterative resolver changes the response code from one that indicates the name does not exist to a response that signals the name exists. The provider further configures the resolver to modify the contents of response by inserting an IP address mapping for the queried name; in particular, this mapping is not published in the domain registrant's zone file but is a mapping of the third party's choosing.

## *Redirection at the Registry Level of the DNS*

SSAC and the Internet Architecture Board (IAB) have previously commented on redirection and DNS synthesis at the registry level of the DNS[4, 5, 6]. SSAC makes no further comments or recommendations in this report. However, for the sake of completeness, we illustrate the basic flow of a *synthesized response from a TLD operator* here:

1) A client submits a DNS query to resolve a domain name *example.tld* into an IP address to an iterative resolver *A*.
2) The iterative resolver A begins the resolution process by forwarding the query to a root name server.
3) The root name server returns a list of name servers that are able to resolve labels for *tld*.

---

[3] We describe this behavior as a *silent alteration* because the iterative resolver does not provide any explicit protocol information to indicate that the contents have been altered to the client or the authoritative name.

[4] SAC 006 Redirection in the COM and NET Domains (9 July 2004) http://www.icann.org/committees/security/ssac-report-09jul04.pdf

[5] SAC 015 Why Top Level Domains Should Not Use Wildcard Resource Records (10 November 2006) http://www.icann.org/committees/security/sac015.htm

[6] SAC 013 SSAC Response to ICANN Letter re: Tralliance Proposed New Registry Service, http://www.icann.org/committees/security/sac013.htm

4) The iterative resolver *A* sends the query to resolve *example.tld* to one of *tld's* name servers identified by the root name server.
5) *tld's* name server determines that the label *example* does not match a specific label in *tld's* zone file. Instead of returning a DNS response message with a response code set to the value *Name Error*, *tld's* name server composes and returns a DNS response message that resolves *example.tld* to an IP address it chooses to iterative resolver A.
6) Iterative resolver A forwards the positive response message to the client that originated the request (and may optionally cache this response).

## *Synthesized DNS responses from Entrusted Agents*

In this example, we describe how an entrusted can synthesize a DNS response from the domain for *example.tld*:

1) A client submits a DNS query to resolve a domain name *service.example.tld* into an IP address to an iterative resolver *A*.
2) The iterative resolver A begins the resolution process by forwarding the query to a root name server.
3) The root name server returns a list of name servers that are able to resolve labels for *tld*.
4) The iterative resolver *A* sends the query to resolve *service.example.tld* to one of the *tld* name servers identified by the root name server.
5) *tld's* name server returns a list of name servers that are able to resolve labels for *example.tld*.
6) Iterative resolver *A* continues the resolution process by issuing a query to resolve *service.example.tld* to one of the *example.tld* name servers identified by *tld's* name server.
7) *example.tld's* name server determines that the label *service* does not specifically match a label in *example.tld's* zone file. *example.tld's* name server composes and returns a DNS response message that resolves *service.example.tld* to a default IP address defined in the zone file to iterative resolver A.
8) Iterative resolver A forwards the positive response message to the client that originated the request (and may optionally cache this response).

Figure 1 illustrates this form of DNS response modification:

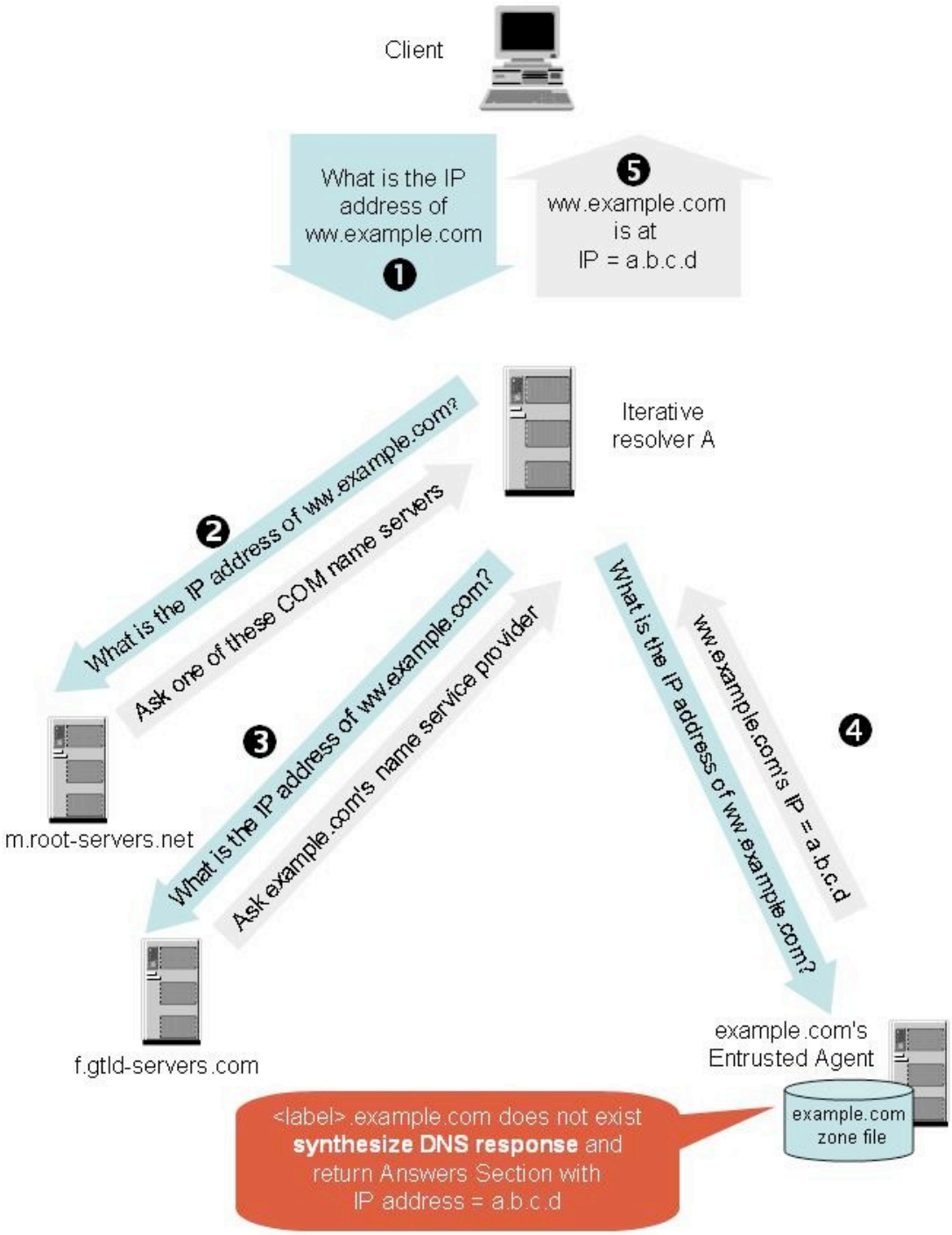


Figure 1. NXDomain response modified by entrusted agent

## *NXDomain response modification by third party NS providers*

Any third party name server operator at any iterative resolver that is involved in a given name resolution process can perform NXDomain response modification. For example:

1) A client submits a DNS query to resolve a domain name *service.example.tld* into an IP address to an iterative resolver *A*.
2) The iterative resolver A begins the resolution process by forwarding the query to a root name server.
3) The root name server returns a list of name servers that are able to resolve labels for *tld*.
4) The iterative resolver *A* sends the query to resolve *service.example.tld* to one of the *tld* name servers identified by the root name server.
5) *tld's* name server returns a list of name servers that are able to resolve labels for *example.tld*.
6) Iterative resolver *A* continues the resolution process by issuing a query to resolve *service.example.tld* to one of the *example.tld* name servers identified by *tld's* name server.
7) *Example.tld's* name server determines that the label *service* does not exist in *example.tld's* zone file and returns a DNS response message with a response code set to the value *Name Error* to iterative resolver *A*.
8) Iterative resolver *A* observes that *example.tld's* name server has returned a response message indicating non-existent name. Instead of delivering that response message to the client, iterative resolver *A* silently alters the RCODE in the DNS response message to an RCODE signaling *name found* and inserts an answer to the query that maps *service.example.tld* to an IP address the third party name server operator chooses before it forwards the response along to the client.

It is important to note that, in practice, any party involved in the resolution process can perform NXDOMAIN redirection for *every* name which it determines or is notified does not exist, regardless of whether or not an authoritative server gives an NXDOMAIN.

Figure 2 illustrates this form of DNS response modification:

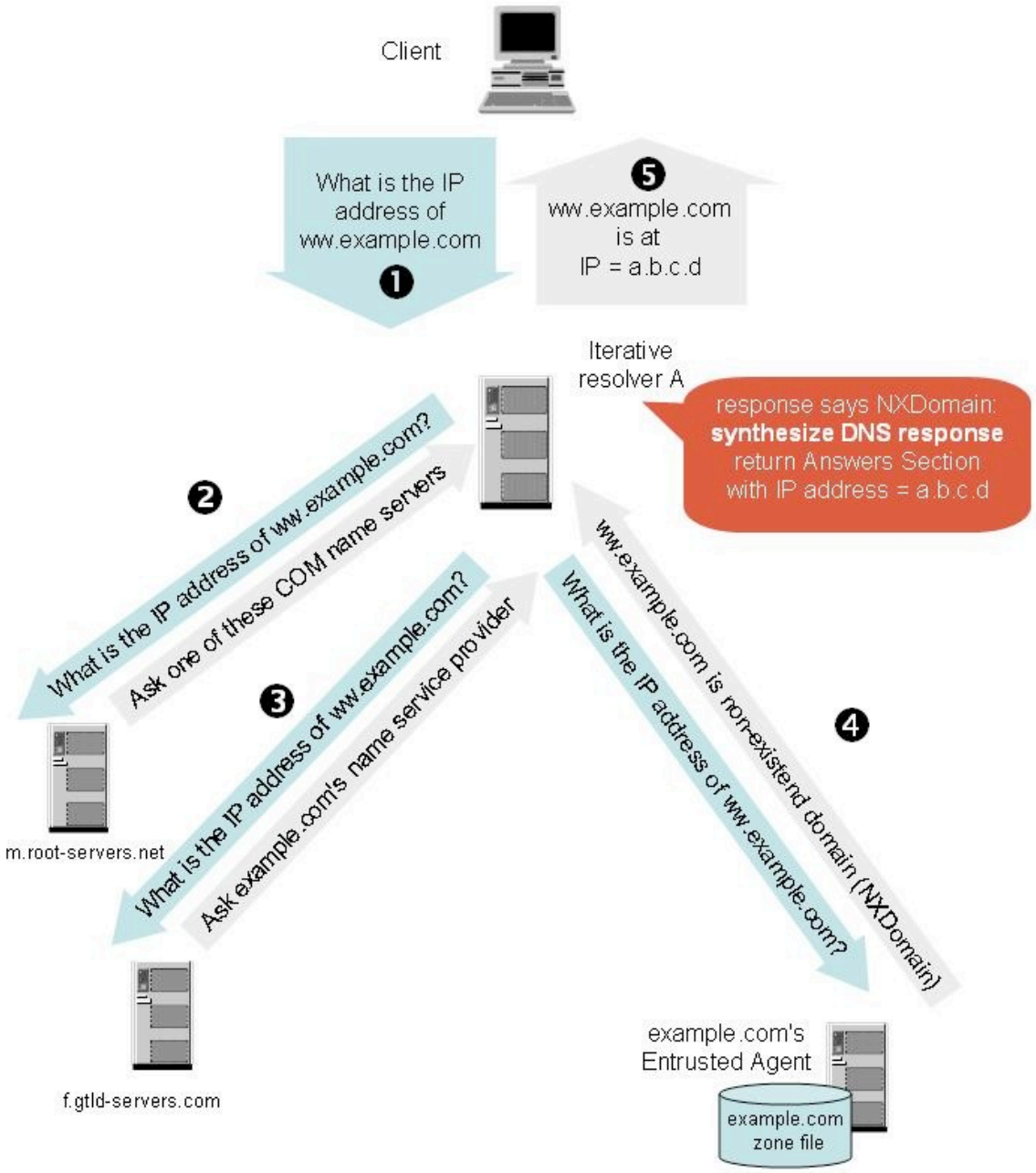


Figure 1. NXDomain response modified by entrusted agent

## Who can modify DNS response messages?

The examples in the previous section identify some of the parties who are able to redirect NXDomain response messages. The list includes entrusted agents and third parties.

**Entrusted Agents**. The domain registrant's internal staff may serve as the entrusted party and manage the registrant's zone information. The sponsoring registrar for the domain name, an Internet Service Provider, or outsourced DNS providers (companies that host an organization's DNS for fee) for an) may also act as the entrusted party and host the registrant's zone information.

**Third parties.** Any DNS operator of an iterative resolver that participates in the resolution process for a given DNS query is in a position to process DNS response messages from the authoritative name server to the query initiator, including:

- Public DNS service providers, who derive revenue by
    - harvesting and selling DNS traffic analyses or
    - selling advertising opportunities on pages hosted at the addresses they insert in DNS responses they alter,
- ISPs or an ISP's agents (companies that run DNS for ISPs for fee) that provide name resolution to subscribers or generally, to any party that makes use of the ISP's name service.
- Service providers, who offer name resolution in conjunction with web proxy services.

**Attackers** may also modify DNS responses to support malicious or criminal activities.

This list also illustrates that there are many motives to modify DNS responses. We consider these in the following section.

## Why modify NXDomain response messages?

Several reasons why parties would choose to modify DNS responses have been described to and identified by SSAC. For example, instead of delivering the NXDomain response the authoritative name server issued, a third party can intercept and silently alter the contents of the DNS response so that it contains the IP address of a web page intended to:

- **Generate revenue.** The landing page hosts advertising or other revenue-producing content at a domain and subdomains of registered domains.
- **Enhance the user's web experience**. The landing page notifies the user (a prospective customer) that the domain name he queried is not available and provides the user with a way to resolve an error result, for example, the user may be able to recover from the error by using a (sponsored) search form accessed via the landing page.
- **Enforce a policy**. The landing page notifies a user that the content on pages in the domain he attempted to access violates an acceptable use policy. The landing page may identify the specific content type or may provide a copy of the AUP for the user to review.
- **Provide remedial education**. The landing page informs the user that he has attempted to access a domain that has been identified as a phishing domain and that the site was suspended. The user is given an opportunity to learn from this "close call" by reviewing anti-phishing educational material published at the landing page.
- **Abet unauthorized or criminal activities**. The landing page hosts malicious downloadable content at a name that is in the domain but is not instantiated by the registrant to facilitate criminal activities (phishing, identity theft, fraud, etc.)

### *Is DNS response modification a security and stability issue?*

Several characteristics of DNS response modification merit attention. SSAC observes the following from the behaviors exhibited by entrusted agents and third parties who engage in DNS response modification.

1) Entrusted agents are presumed to operate on behalf of the domain registrant. From an operational perspective, alterations the entrusted agent makes are permitted within the DNS data model. Whether the entrusted agent is permitted to generate a synthesized response is a matter that can be resolved between the agent and the registrant. The registrant can choose to have its zone hosted by a different agent if an entrusted agent is determined to be not trustworthy.
2) By the very nature of the DNS, any third party who provides an iterative resolver that participates in the resolution process is a potential man in the middle and has the ability to modify messages it receives from an authoritative name server before forwarding these to a client. Modification of NXDomain responses by third parties somewhere along the resolution path may be outside any business relationship that involves the registrant.

3) Third parties that alter the semantics and content of a DNS response can do so for their own benefit, without notice and consent of the domain registrant or the user that initiated the query.
4) Third parties that modify NXDomain response messages provide information about a domain that is different from the information the domain registrant intends to distribute in several meaningful ways. The response asserts that a label (subdomain) has been instantiated within a domain and is mapped to a specific IP address. From the domain registrant's perspective, this name does not exist in its zone. Such a response is incorrect and misrepresents the registrant's intentions.
5) Third parties influence the subsequent actions of the user who formulated the query by implying an association with the domain registrant. If the intent of the third party is to benefit from an implied relationship between the third party and the domain registrant then this is arguably an act of fraud, deception or unauthorized use of a brand name or trademark.
6) DNS response modifications can affect applications other than web and in particular can disrupt email, Internet telephony, and other Internet services.
7) DNS response modifications can create unpredictable responses (nominally a stability issue, but in the worst case possibly resulting in a denial of service attack).

We next explore how these security and stability concerns affect domain registrants.

## *How does DNS response modification affect domain registrants?*

In circumstances where NXDomain responses are modified without the express knowledge and consent of the domain registrant, the response message does not accurately reflect the domain registrant's intended operational state of the domain:

1) The non-existence of a name in a zone file should be reported to the querying client. Specifically, a response containing the response code *Name Error* should be returned by the entrusted agent or by the third party that silently alters the message to the client, but is not.

2) A Type A resource record is written into the Answers Section of the response message. The name-to-address mapping described by this resource record does not exist in the domain registrant's published zone file.

When examined closely, this is not merely an alternative method of handling an error condition but an alteration of content. When an entrusted agent for a domain registrant creates a DNS response message, whatever the response, the agent and registrant should have every reason to expect that intermediaries will attempt to deliver the content without alteration. If this assumption proves to be incorrect, the domain registrant may be affected in any of several ways:

**The response no longer conveys the intended information**. Any application or management activity that relies on NXDomain responses for correct operation or intervention will no longer work for all labels within the domain that are redirected.

**The response subverts the conventional domain trust model**. Typically, organizations make security decisions based on an implied trust model: a domain parent will trust subdomains within the domain. This implicit trust derives from the assumption that hosts named within an organization's domain are administered by the domain's IT staff or its designated and trusted agents. A modified NXDomain response directs users to services operating on a host that operates outside the administrative control and security domain of the domain registrant.

**The response adversely affects compliance testing and auditing**. An organization that conducts security audits, especially one that is required to do so to demonstrate regulatory compliance, must take into consideration that a third party may arbitrarily add a host that will appear to be named in its domain but that host will not fall within its administrative control and the name will not be published in its zone.

**The response may cause DNS operational instabilities**. Name resolution performed directly to the authoritative name server of a domain or through an iterative resolver that does not alter NXDomain responses will return the response the registrant intends, but the same query may return different responses depending on whether it is processed by a third party that modifies NXDomain responses or through any iterative or stub resolver that caches the modified response. This same situation may arise if a domain registrant

used two entrusted agents to host its zone file. One entrusted agent may publish the registrant's zone file with a wildcard entry while the other may publish the authentic (unaltered) zone file.

**The potential for conflicting address mappings is significant**. A domain registrant may add a type A resource record for a name (ww.example.com) to its zone file only to discover that a third party (or perhaps several) has already mapped an IP address to that name. [Note: this would be true in general for any record type a client requests.]

**Hosts in the domain are exposed to any vulnerability that can be exploited from or via the redirection host**. Even in circumstances where the host identified in the modified NXDomain response is operated by a legitimate business (for advertising or service promotions, for example), that host may be vulnerable to web server and web application attacks, cross site scripting, or operating system exploits; in particular, attackers can inject content into one of the domain registrant's systems via the host identified in the modified NXDomain response. Such attacks are not theoretical. Security researchers have publicly demonstrated that it is possible to inject scripts into the parent domain through hosts identified in modified NXDomain responses (ad injection servers)[7] , [8].

**The response adds hosts to the domain and the domain registrant's administrator cannot exercise content control over these sites**. Hosts identified in the NXDomain responses modified by a third party benefit from the domain registrant's brand, reputation, site and link popularity, and sponsored link agreements with search engines. The registrant does not accrue any benefit from this activity and in certain circumstances, may be harmed or suffer from this activity. For example,

- A third party may publish advertising at a host it identified in a modified NXDomain response. The ads could promote services or merchandise of the domain name registrant's competitors.
- Companies whose advertisements are published at host identified by a third party in a modified NXDomain response benefit from sponsored links associated with the domain name and keywords search engines associate with the registrant's business.
- The registrant may have its own advertising relationships, and ad services published at a host identified by a third party in a modified NXDomain response may undermine or compete with advertising the domain registrant publishes at its own web hosts. This affects the domain registrant, whose affiliation with a partner ad service is jeopardized, and the ad partner, whose revenue opportunities are hijacked.
- A host identified by a third party in a modified NXDomain response may publish negative ad campaigns or publish inaccurate or misleading information aimed at causing reputational harm to the registrant.

[7] h0h0h0h0 by Dan Kaminsky, at http://www.doxpara.com/DMK_Neut_toor.ppt

[8] Hacking ISP Error Pages, Bruce Schneier, at http://www.schneier.com/blog/archives/2008/04/hacking_isp_err.html

**Modified NXDomain responses are not limited to A resource records.** A third party is not limited to modifying NXDomain responses that would resolve what are assumed to be hostnames for use in HTTP connections, because an NXDomain response can pertain to a request for any resource record from any application—all the DNS resolver sees is a name and a record type in a request. A third party can in theory modify NXDomain responses for generally any query (MX, SRV, NAPTR); for example, DNS queries used to look up an IP telephony number (e.g. requests that return a NAPTR resource record) can in theory be redirected to a call server of the third party's choosing.

**The response creates opportunities for abuse and attacks**. Attacks that can be performed using counterfeit responses include:

- **Phishing via false site injection at spoofed subdomains**. Attackers may be able to exploit scripts they find on the host identified in modified NXDomain responses and attack the domain registrant's systems through these scripts. For example, an attacker may find a script that accepts input but fails to validate input to certain parameters of that script. By injecting his own executable code in that exploitable parameter, the attacker can trick visitors to the site into executing a fake version of a payment or login form on that site[9]. Attackers can apply similar techniques to post banner ads that invite users to download malicious software, or popup windows that invite users to update application or OS software but these updates are malicious rather legitimate copies.
- **Data extraction**. The redirection host can monitor traffic and collect web statistics of redirected visitors in much the same manner as an ad tracking company might.
- **Aribitrary cookie retrieval**. The redirection host can intercept and copy cookies that the domain registrant's web server intended to send to the client. This may result in the disclosure of personal information, credit card or account credentials.
- **Attacks against brand**. Many domain name registrants protect brands and trademarks by defensively registering names under TLDs that are offensive, defamatory, deceptively similar or typographically similar. The same labels can be instantiated as subdomains by an attacker that uses wildcard injection. Instead of all such name queries returning non-existent domain, these can be directed to a defacement or protest web page.

In addition to these operational and security impacts, SSAC notes that subdomain redirection may raise Intellectual Property and trademark issues. These, while outside SSAC's expertise, may merit consideration by qualified parties as this subject is studied further.

[9] *Anatomy of an XSS Attack: Exploit, Impact and Response*, Russ McRee, ISSA Journal, June 2008 pp 12-14.

## *Dueling Rewrites*

DNS response modification is itself subject to modification. This phenomenon has been described as *dueling rewrites* and can be summarized as follows:

1) A user, Fred, registers the domain *example.tld* via a registrar *X*.
2) The registrant of *example.tld* uses a DNS service offered by registrar *X* to host *example.tld's* zone file.
3) Fred's PC uses *NS1.mylocalisp.tld* as its default name server.
4) Fred opens a browser window from PC1 and attempts to connect to *ww.example.tld*. He's made a typographical error for *www.example.tld,* which is the hostname the registrant has used for the address used to contact his web server with the HTTP protocol.
5) *NS1.mylocalisp.tld* performs a resolution process to resolve *ww.example.tld*, first querying a root name server for *tld,* then querying *tld's* name server for *example.tld*, and finally querying registrar X's name server for *ww.example.tld*
6) Registrar X's name server returns a positive DNS response instead of a NXDomain response for *ww.example.tld.* This response contains an A record in the answer section mapping *ww.example.tld* to *a.b.c.d.*
7) *NS1.mylocalisp.tld* intercepts registrar *X's* DNS responses, recognizes the redirect address *a.b.c.d* as an advertising page from prior DNS traffic analysis.
8) *NS1.mylocalisp.tld* substitutes its own redirection information and returns a positive DNS response containing an A record in the answer section mapping *ww.example.tld* to *a.x.y.z.*
9) Fred opens a browser window from PC1 and attempts to connect to *ww.example.tld at a.x.y.z.*

## Preliminary Findings

SSAC offers the following preliminary findings and observations regarding the practice of DNS response modification.

1) NXDomain responses may be modified by third party providers at any iterative resolver along the path between a client and the authoritative name server for a domain. Entrusted agents may include wildcard entries in a registrant's zone file and return this address mapping instead of a *Name Error*.
2) Third party NXDomain response modification redirection creates operational and stability issues for domain registrants that cannot be easily solved even by hosting one's own name service.
3) NXDomain response modification and synthesized responses can create security issues for domain registrants. In particular, trust relationships between a parent domain and its subdomains cannot be assured. The erosion of trust relationships may have an adverse effect on security auditing and compliance testing.
4) NXDomain response modification and synthesized responses can create opportunities for malicious attacks against the domain registrant as well as opportunities for attackers to exploit the domain registrant's domain assets for malicious or criminal purposes.
5) NXDomain response modification and synthesized responses are subject to modification by third parties that modify NXDomain responses they receive.
6) Entrusted agents that synthesize responses and third parties that modify NXDomain are known and identifiable, not speculative. Certain third parties practice NXDomain response modification directly or through *error resolution partners*[10].
7) Entrusted agents and third parties may not disclose the fact that they practice DNS response modification in a clear and unambiguous way, and in cases where they do disclose the practice, they may not divulge the possible adverse effects this practice could have on a domain registrant's interests. Certain providers give notice that they will exercise the right to perform error resolution or redirection as a condition of a service agreement and offer no opportunity for the registrant to opt out other than to choose a different provider.
8) NXDomain responses do not merely signal an error condition from the domain registrant, but convey content regarding the entries in a zone file. This content should be treated no differently from any other application content.
9) The effects of response modification extend beyond web applications. In particular, substitution and injection in electronic mail and voice over internet services are green fields for similar exploitation.
10) DNS response modification may raise Intellectual Property and trademark issues.

[10] Certain participants in this activity identify an annual worldwide error market in excess of $1B http://barefruit.com/services.htm

## Preliminary recommendations

SSAC makes the following preliminary recommendations.

1) SSAC has previously and repeatedly recommended against synthesizing DNS responses at the TLD level. Similar actions at subdomain levels should not be practiced.
2) Registrants can control how an entrusted agent answers a query for a name that does not exist in its zone file, via a trust and business relationship. Specifically, the registrant should dictate whether its authoritative name servers return Name Errors or synthesized responses.
3) Registrants should inquire how their entrusted agents treat their unregistered subdomains. SSAC concurs with the IAB and recommends that entrusted agents should not use DNS wildcards in a zone without informing the domain registrant of the risks identified in this Report and elsewhere, that entrusted agents should not generate wildcards and synthesized responses without the informed consent of the registrant, and that entrusted agents should provide opt-out mechanisms that allows clients to receive the original DNS answers to their queries.
4) Third parties should disclose that they practice NXDomain response modification and provide opportunities for customers to opt out.
5) Organizations that rely on accurate NXDomain reporting for operational stability should choose an entrusted agent that asserts it will not modify DNS responses in its terms of service.
6) Registrants should study ways to provide end-to-end authenticated proof of non-existence of subdomains, e.g., DNSSEC security extensions[11, 12, 13, 14]. Organizations should further seek to reduce the level of exposure to NXDomain response modification by selecting trusted parties to provide iterative resolvers so that queries from the organization's clients are not routed through arbitrary name resolution providers who may practice subdomain redirection

.

[11] RFC 4033 DNS Security Introduction and Requirements, http://rfc.net/rfc4033.html
[12] RFC 4034 Resource Records for DNS Security Extensions, http://rfc.net/rfc4034.html
[13] RFC 4035 Protocol Modifications for DNS Security Extensions, http://rfc.net/rfc4035.html
[14] RFC 5155 DNS Security (DNSSEC) Hashed Authenticated Denial of Existence, http://rfc.net/rfc5155.html

## Future Work

The business, economic, security and operational impacts of subdomain redirection merit additional attention. To our knowledge, DNS response modification appears to be largely confined to web-based applications, and the issue of how it may affect other IP-based services merits further study. SSAC encourages the community to consider the broad implications of turning negative responses into revenue opportunities without consideration of the operational consequences and without consideration for the wishes of either registrants or clients of DNS data. Fundamentally, error resolution and the "error markets" such practices enable set worrisome precedents by introducing ambiguity and variability into traditional error management and trust models. It is unclear whether such practices might be extended to email, voice and collaboration services, or even to addressing, routing, and other core Internet operations and equally unclear how severely these might impact IP-based communications.