Redirecting DNS for Ads and Profit

Nicholas Weaver
ICSI
nweaver@icir.org

Christian Kreibich
ICSI
christian@icir.org

Vern Paxson
ICSI & UC Berkeley
vern@cs.berkeley.edu

Abstract

Internet Service Providers (ISPs) increasingly try to grow their profit margins by employing "error traffic monetization," the practice of redirecting customers whose DNS lookups fail to advertisement-oriented Web servers. A small industry of companies provides the associated machinery for ISPs to engage in this monetization, with the companies often participating in operating the service as well. We conduct a technical analysis of DNS error traffic monetization evident in 66,000 *Netalyzr* sessions, including fingerprinting derived from patterns seen in the resulting ad landing pages. We identify major players in this industry, their ISP affiliations over time, and available user opt-out mechanisms. One monetization vendor, Paxfire, transgresses the error-based model and also reroutes all user search queries to Bing, Yahoo, and (sometimes) Google via proxy servers controlled or provided by Paxfire.

1 Introduction

Error traffic monetization solutions leverage the context provided by ISP customer traffic in order to rewrite protocol error messages to valid responses, redirecting users to Web servers—*ad servers*, in the following—that show advertisements or search results hopefully of interest to the user. Examples of such protocol errors include HTTP 404 status codes and, more commonly, DNS responses with return code 3 (Name Error), indicating that the looked-up name could not be resolved to an IP address. Rewriting of such DNS responses also goes by the name "NXDOMAIN wildcarding," and is the focus of this paper.

ISPs commonly deploy this controversial practice with the assistance of a *monetization provider*. These third parties supply the infrastructure needed to rewrite the name errors, and Web servers to redirect traffic to the ad servers. One provider claims that ISPs deploying their solution will see profits of 1–3 USD per customer per year [14].[1] ICANN has criticized this practice due to its potential to cause both security and stability problems, and called out the existence of third-party involvement [5]. Security researchers have exploited cross-site scripting vulnerabilities in two providers' ad servers to demonstrate fairly sophisticated phishing and cookie theft attacks [7].

In the *ICSI Netalyzr* [8], our widely used network debugging and diagnostic tool,[2] we have employed tests for various forms of NXDOMAIN wildcarding since we started offering the service in mid-2009. In this paper we illuminate the DNS error monetization market by combining Netalyzr's measurements with an analysis of the redirection pages collected between January 2010 and May 2011, the location and content of the ad servers, and the marketing material provided by the companies involved. We identify ISPs employing DNS error monetization, their choice of monetization provider (including shifts of provider and apparent in-house realization), potential redirection policy customizations, as well as availability of opt-out mechanisms.

We also observe a more aggressive form of DNS-driven traffic manipulation, *search-engine proxying*. One monetization provider, Paxfire [11], optionally supports blanket redirection of users' entire Web traffic for `www.bing.com`, `search.yahoo.com`, and sometimes `www.google.com`. Paxfire routes Bing and Yahoo through its own servers while treatment of Google depends on ISP policy, for which we observe three alternatives: Google's traffic remains unmolested; redirected through Paxfire's servers; or redirected through Paxfire proxies located within the ISP's network.

In § 2 we sketch the typical architecture used for error traffic monetization. In § 3 we describe our methodology, including DNS and HTTP data collection and redirection page categorization. Next, we briefly summarize the monetization providers and their modes of operation (§ 4), along with the corresponding ISP relationships and monetization policies (§ 5). We then discuss Paxfire's search-engine proxying and which ISPs employ this feature (§ 6) before we conclude the paper (§ 7).

2 DNS Error Monetization

DNS-based error monetization tries to convert DNS name errors into clicks on advertisements that are hopefully relevant in the context of the user's error-causing traffic. This conversion generally operates under the assumption that the error occurs in Web surfing, as the redirection of the otherwise failing traffic only succeeds for Web traffic. For other applications, say VoIP, email,

[1] We currently have no way of validating these profit claims. The same provider previously claimed 2–4 USD per customer per year.

[2] `http://netalyzr.icsi.berkeley.edu`

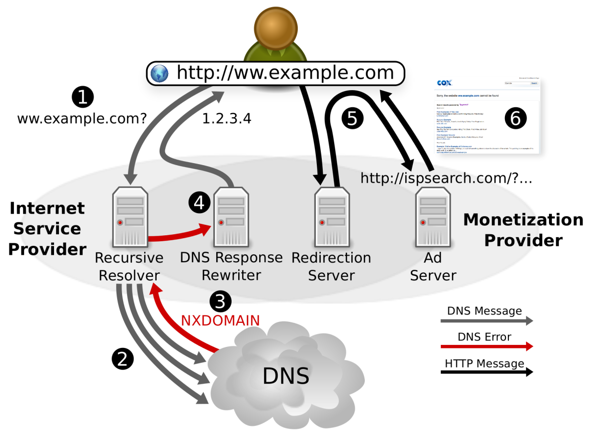
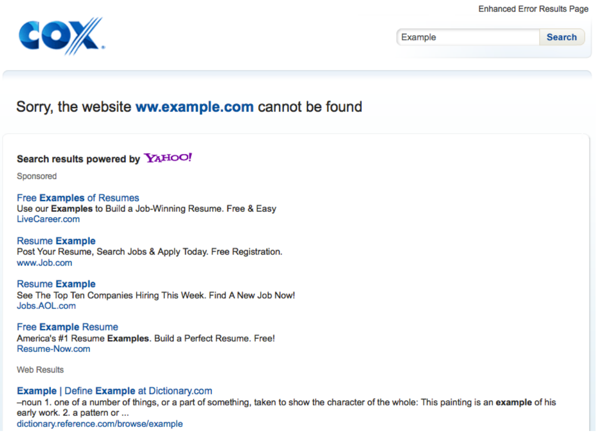


Figure 1: The typical architecture employed by ISPs in tandem with monetization providers to facilitate DNS error monetization.



Sorry, the website **ww.example.com** cannot be found

Search results powered by YAHOO!

Sponsored

Free **Examples** of Resumes
Use our **Examples** to Build a Job-Winning Resume. Free & Easy
LiveCareer.com

Resume **Example**
Post Your Resume, Search Jobs & Apply Today. Free Registration.
www.Job.com

Resume **Example**
See The Top Ten Companies Hiring This Week. Find A New Job Now!
Jobs.AOL.com

Free **Example** Resume
America's #1 Resume **Examples**. Build a Perfect Resume. Free!
Resume-Now.com

Web Results

Example | Define **Example** at Dictionary.com
–noun 1. one of a number of things, or a part of something, taken to show the character of the whole: This painting is an **example** of his early work. 2. a pattern or ...
dictionary.reference.com/browse/example

Figure 2: A typical search results page resulting from DNS wildcarding.

or FTP, the advertisement context does not exist and redirection would imply serious privacy implications.

ISPs and monetization providers most commonly implement the redirection procedure using four components, shown in Figure 1: a recursive DNS resolver, a DNS response rewriter, a redirection Web server, and the ad server itself. Whether ISP or monetization provider owns, controls, or operates these components varies. The ISP usually provides the recursive DNS resolver. When a user enters a URL into the browser or clicks on a link (❶), the browser sends a DNS request to this DNS resolver, which performs the actual DNS queries on behalf of the customers and acts as a cache for DNS replies (❷). When the name lookup fails, it forwards the resulting NXDOMAIN error (❸) to the response rewriter, which consists of a software module on the existing resolver [9] or an in-path device placed between the recursive resolver and the user [11]. The rewriter inspects incoming DNS responses and depending on its rule-set rewrites responses indicating name error responses to regular A-record responses containing the IP address of a redirection server (❹). The rule-set's coverage varies, and may trigger on all name errors, only on those for names beginning with a `www` subdomain, or exclude name errors only affecting the given subdomain. When triggering, the redirection server redirects the client to the ad server (❺), which provides the advertisements and search results to the client (❻).

Typically, the monetization provider operates the redirection server, a simple web server whose only task is to examine the `Host` headers and URLs the Web browsers request, and to generate an HTTP-level redirection response with a suitable URL pointing the browser at the ad server. According to our dataset, monetization providers typically assign a different redirection server IP address to each ISP, allowing the redirection sever to know which ISP sourced the traffic. On occasion monetization providers also locate redirection servers within the ISPs' networks.

Finally, the ad server may operate in-house at the ISP or at the monetization provider. It serves pages branded to the ISP and commonly containing a combination of "sponsored" search results (i.e., advertisements), actual search results derived from the attempted domain name and any keywords it can extract from the original URL, and a link to opt-out instructions for the customer. Figure 2 shows an example search page Cox Communications presents to its users.

Monetization providers explicitly sell this service to ISPs as a method to increase revenue, while ISPs advertise it to their users as a navigational aid presenting search results and sometimes also providing a link correcting common spelling mistakes (e.g. a link on the page for `yahoo.cmo` pointing to `yahoo.com`).

Name error rewriting causes significant collateral damage. Web browsers commonly rely on these errors to present browser-specific assistance, such as falling back to a web search. Wildcarding names that do not begin with `www` assumes that a Web browser generated the lookup. This may break non-HTTP protocols, disrupt local services that rely on name suffixes in the local DNS search path, and expose the user to cross-site scripting vulnerabilities [7]. Therefore it is critical the ISPs provide effective opt-out mechanisms [2].

3 Wildcard Detection and Redirection Fingerprinting

Since mid-2009 we have provided the ICSI Netalyzr service, a popular network diagnostic, measurement, and debugging applet. Users around the world run it from their browsers in order to debug or clarify their network connectivity. To date, we have collected 259,000 sessions from 193,000 distinct IP addresses located in virtually every country of the world. For more details, we refer the reader to our main paper on the service [8].

Netalyzr includes tests to detect NXDOMAIN wildcarding. We employ random string nonces to compose nonexistent names in the following ways. Netalyzr first uses the system's DNS library to check if a name of the form `www.`*nonce*`.com` is wildcarded. If so, it explores variations to determine the policy for non-Web names (*nonce*`.com`), alternative TLDs (*nonce*`.org`), common typos (`www.yahoo.cmo`), subdomains (*nonce*`.example.com`), and DNS server failures. In January 2010 we added code to the applet to capture the web page content when it detects the presence of NXDOMAIN wildcarding. In those cases, the applet sends an HTTP `GET` to the redirection Web server and uploads any returned content to the Netalyzr servers. The code neither follows redirects nor interprets the contents in any way.

Our data set comprises 45,020 web pages captured in this manner. We manually classified them by identifying distinct content features, for which we defined regular expressions. We used content features including the structure of the redirection target URLs (such as redirects containing `/dnserror?url=`) if the response was an HTTP redirect, unique JavaScript snippets, HTTP response headers, and redirection techniques. A set of 81 rules allowed us to categorize 96% of the uploaded web pages. The twenty most common rules match 94% of pages. No page matches more than one rule. We used neither the addresses of the redirection servers nor their hostnames for classification.

A related Netalyzr DNS check verifies DNS lookup integrity. The applet looks up the IP addresses for each of approximately 80 DNS names, including search properties, advertisement sites, banks, financial institutions, IM clients, and other domains of interest. It uploads the resulting set of IP addresses to the Netalyzr servers, which validate the correctness of the addresses via reverse lookups and inspection of the resulting host names.

We note that our measurements are skewed by Netalyzr's user base: the nature of the service biases it toward technophile users. In particular, we observe a large number of OpenDNS and Comcast users, mainly because a major technology news site featured Netalyzr in context of coverage of Comcast's DNS policy. Our data collection is generally prone to such "flash crowds," resulting from exposure the tool receives on technical blogs and news sites.

4 Error Monetization Providers

All ISPs for which Netalyzr has recorded over a hundred distinct redirection pages either use one of 6 monetization providers or implement an ISP-specific solution. While other competitors may exist, the major ISPs in the Netalyzr dataset do not employ them.

The differences between monetization providers lie mostly in the rule determining the set of names whose resulting name errors they rewrite, the implementation of the redirection, and the opt-out mechanism. The rewriting rule in practice either matches all name errors or only those whose names begin in `www`, and thus reflects different levels of collateral damage. The redirection mechanism is also important, as the methods vary in reliability. The HTTP specification provides for clean redirections using status code 302, which any HTTP client understands. Unfortunately, several vendors return pages containing either just JavaScript, or JavaScript in combination with an HTML Meta refresh tag. Finally, opt-outs are up to the ISP (via maintenance of IP address whitelists), the monetization provider (via HTTP cookies on the ad server), or the customer (via selection of an alternate DNS provider).

Barefruit's products provide error monetization for DNS and HTTP traffic [1]. In the DNS space, they offer patches for the BIND, PowerDNS, and djbdns DNS servers that add wildcarding functionality and include a whitelist based on IP addresses. Barefruit's redirected URLs include the string `main?InterceptSource=0`, presumably to distinguish between DNS and HTTP redirections. Barefruit has provided Cox, Earthlink, and Qwest with in-ISP redirection servers; for others they reside in three of Barefruit's address blocks. Their website contains a public FAQ section on opting out, simply encouraging users to search the Web for alternative DNS resolvers.

FAST Search & Transfer, owned by Microsoft, is a software and services company specializing in enterprise-level search. We could locate no advertising material indicating they offer this service, so we base this vendor assignment only on IP address allocations.

Two ISPs use a total of five redirection servers in three address ranges belonging to FAST Search & Transfer. Comcast's redirection servers construct URLs of the form `?cat=dnsr&con=ds&url=`*domain*, while Time Warner's uses `?q=`*domain*`&con=nxd`, a construction that appears related but not identical. This is the only case we have observed in which a vendor uses a different URL pattern with different customers, necessitating two separate signatures.

Infospace primarily build a "meta" search engine but they also provide multiple business products, including DNS Error Assist Service [6], which integrates with their search engine. A path component starting with `dnsassist/main/`, for their "DNS Error Assist" service, provides the redirection URL's distinct signature. Infospace hosts the redirection servers on nine IP addresses within two Infospace-owned subnets.

Nominum primarily constructs large-scale DNS systems. Many major ISPs employ their caching nameservers. For their Vantio nameservers, Nominum offers NXR [9], a module that forwards NXDOMAINs to their NavAssist service. Nominum's redirection URLs begin with either `subscribers/assist?` or `assist.php?`, which matches the NavAssist name. Nominum switched from the former to the latter form in the summer of 2010. Nominum owns the two address ranges this service uses.

Paxfire exclusively provides DNS error monetization services [11]. They offer three ways in which ISPs may implement the redirection: (*i*) an in-path hardware device that rewrites DNS replies, (*ii*) a software module for various DNS resolvers, and (*iii*) a hosted DNS service. Their service operates on a revenue-sharing basis.

Paxfire, for unknown reasons, employs an obfuscated JavaScript-only redirection. The obfuscation uses concatenation of static strings to produce a redirection target URL that it places into `document.location`. Most strings never change, which allows us to easily recognize the Paxfire redirector.

They provide a local redirection server for Versatel and place others in seven different subnets. These subnets are in address ranges with no identifying WHOIS or reverse DNS information. We confirmed the redirection page signature by querying the demonstration servers we discovered during our investigation of search-engine proxying (§ 6).

Paxfire offers two opt-outs for ISPs. The first uses a standard whitelist of IP addresses. The second employs an HTTP cookie on the ad server's domain. This cookie opt-out is *fictional*: the rewriter continues to mask the customer's name errors, but the ad server now returns HTML content matching the default error page of the user's browser.

Xerocole [14] previously realized Sandvine's DNS wildcarding product [13] and specializes entirely in DNS error monetization. It spun off from Sandvine in the summer of 2010. Xerocole provides a DNS server proxy that exists between the resolver and the customers.

Their initial redirection used Apache servers using HTTP-level 302 redirects. In the fall of 2010 they switched redirection servers to Nginx. These servers return a compressed page with an in-page meta refresh and JavaScript. They deploy redirection servers in Time Warner's network but all other servers are in five subnets, three of which are registered to Sandvine or Xerocole.

Xerocole's appliance offers two options for handling DNSSEC. The first suppresses NXDOMAIN wildcarding if the query requested DNSSEC information and the sender signed the response. The second simply returns a rewritten NXDOMAIN without a signature and assumes that clients will not actually validate DNSSEC.

VENDOR	REWRITING RULE	REDIRECTION MECHANISM
Barefruit	all	Meta & JavaScript
FAST Search	`www`	302 redirect
Infospace	`www`	302 redirect
Nominum	`www`	302 redirect
Paxfire	all	JavaScript
Xerocole	`www`	Meta & JavaScript

Table 1: Monetization providers, their default rewriting policies, and their employed redirection mechanisms.

Non ISP-related providers. We observed two classes of monetization not related to ISPs.

First, voluntary third-party DNS providers such as OpenDNS [10] use DNS error monetization as their primary revenue stream. OpenDNS's redirection servers issue an HTTP 302 redirect. The wildcarding covers not just NXDOMAIN errors but also SERVFAIL. It will even create IPv4 address to their redirection server for valid names lacking an IPv4 address, causing substantial problems to IPv6-only services, as most clients will query for both IPv4 and IPv6 records simultaneously.

Second, D-Link home gateways include DNS error monetization in their "Advanced DNS Service" [3]. This service sets the user's DNS resolver address to D-Link-branded OpenDNS servers and suffers from the same overly aggressive wildcarding. We do not know whether D-Link enables this service by default.

Table 1 summarizes the providers' default choices for name rewriting and redirection mechanism.

5 ISP Usage of Error Monetization

World-wide prevalence. We examined the adoption of NXDOMAIN wildcarding in all countries for which our Netalyzr dataset contains over 1,000 sessions from users relying on ISP-provided resolvers. Most monetization occurs in Italy (40%), the US (33%), Brazil (33%), Argentina (27%), Germany (25%), and Austria (20%). The UK (18%), Canada (15%), and Spain (12%) occupy the medium range. ISPs in Australia, Belgium, Finland, France, Israel, Lithuania, New Zealand, Norway, Poland, Russia, Sweden, and Switzerland do not commonly use DNS error monetization: these countries have wildcarding adoption rates below 10%.

Major ISPs. For each of the 15 ISPs most prevalent in our Netalyzr dataset and for which Netalyzr's tests detected wildcarding, we examined the ISPs' redirection policy, choice of monetization provider over time, opt-out mechanism, and the fraction of Netalyzr users who have opted out of the redirection. For four ISPs we could not observe the search results page on the ad server as it is only available to these ISPs' customers. We consider users opted-out if their sessions show no evidence of wildcarding but do employ an ISP-operated resolver.

			MONETIZATION	REWRITING	— USER OPT-OUT —	
ISP	# SESSIONS	COUNTRY	PROVIDER	RULE	MECHANISM	% RATE
Alice DSL	3,761	DE	✘(AOL?)	www	Account Setting	25
Brazil Telecom	569	BR	✘	www	?	2
Charter	2,241	US	Paxfire → Xerocole	www	Account Setting	34
Comcast	17,362	US	FAST	www	Account Setting	27
Cox	2,633	US	Barefruit	all	Account Setting	18
Deutsche Telekom	12,671	DE	✘	all	Account Setting	30
Optimum Online	1,210	US	Infospace	www	Account Setting	15
Oi	657	BR	Barefruit	all	Cookie	25
Qwest	1,542	US	Barefruit	all	Account Setting	33
Rogers Cablesystems	1,197	CA	Paxfire	all	Cookie	4
Telecom Italia	1,429	IT	✘	all	?	33
Time Warner	7,287	US	Xerocole → FAST	www	Account Setting	20
UPC	964	NL	Infospace → Nominum	www	?	5
Verizon	4,751	US	Paxfire	www	Resolver Change	9
Virgin Media	1,890	UK	Nominum	www	?	28

Table 2: The 15 DNS-monetizing ISPs most prevalent in our Netalyzr dataset, their monetization providers, and monetization details. "→" indicates a provider switch, "✘" ISP-internal realization of the monetization service.

Table 2 summarizes our findings.

At least 8 of the 15 ISPs implement opt-out via a user account setting. As we are not customers, we cannot universally verify their reliability. Oi and Rogers appear to employ HTTP cookies, and Verizon requires its users to change their resolver configuration manually. We note that distinguishing opted-out users from partial wildcarding deployment within an ISP is difficult. Thus our opt-out numbers may be an upper bound.

We observe monetization provider switches in Charter (October 2010), Time Warner (March 2010), and UPC (October 2010), suggesting low barriers to switching. The switch-overs may be gradual, over a month or two. Indeed, Netalyzr captured 30 sessions by Charter customers indicating Charter used Xerocole to wildcard `www`-prefixed domains, and Paxfire for all others. This suggests that either different resolvers used different monetization providers, or that Charter placed the Xerocole rewriter before Paxfire's existing one.

ISPs sometimes override monetization provider defaults. Verizon seeks to reduce collateral damage by applying Paxfire only to `www` names, while two smaller ISPs (Kcom, using Infospace, and Maxonline, a Xerocole customer) override the defaults to wildcarding of all failing names.

Several non-US ISPs appear to employ their own systems, showing distinct redirection server content. Alice DSL may have developed theirs in conjunction with AOL. Alice uses a distinct redirection page and most redirection servers reside in their address range. We discovered a single landing page served from outside of AliceDSL's network. Its server resides in AOL space and redirects to an unbranded AOL search page. The other servers redirect to Alice-branded AOL search pages.

6 Paxfire's Search-Engine Proxying

We previously reported [8] that some ISPs redirect *all* Web search traffic of parts of their customer base through proxy servers of unknown purpose and ownership, significantly transgressing the common error-based redirection model. Zhang et al. [15] independently observed the same effects. We can now provide more insight into the phenomenon.

The affected ISPs redirect all web searches that affected customers send to `www.bing.com`, `www.google.com`, and `search.yahoo.com` via unrelated HTTP proxies that seemingly do not alter the content. These proxies redirect HTTPS connections to *any* of the three search sites to `https://www.google.com`.[3]By sending HTTP requests directly to the proxies, we identified them as Squid proxies. Deliberately invalid HTTP requests yield HTML content mentioning `phishing-warning-site.com`, an anonymously registered domain parked at GoDaddy. Instances in which the proxies have erroneously returned this response to legitimate requests have triggered ISP customer discussions in online forums, whose puzzled participants posted reports à la "Google is down" and wondered about the domain's involvement [12].

At least 12 ISPs support in this search-engine proxying: Cavalier, Cogent, DirecPC, Frontier, Fuse, IBBS,[4] Insight Broadband, Megapath, Paetec, RCN, Wide Open West and XO Communications. The subset of customers

[3] The HTTPS protocol performs the key exchange before the Host field is revealed, forcing the proxy to statically decide where to route encrypted traffic. The proxies can safely proxy the encrypted traffic as only Google uses HTTPS-based services on the search domain.

[4] IBBS provides DNS and other support services to small ISPs. It is unclear whether these ISPs are aware of the redirection.

affected varies from temporal localized deployments to almost the entire customer base. Charter used the service in the past but appears to discontinue this practice as they switch NXDOMAIN vendors, while Iowa Telecom used it until Windstream acquired them.

The redirectors always send `search.yahoo.com` and `www.bing.com` to ISP-specific IP addresses in two address ranges.[5] `www.google.com`'s treatment varies among redirection through Paxfire proxies (e.g. Fuse), redirection via in-house proxies (e.g. DirecPC, Frontier, and Wide Open West), and no redirection (e.g. Charter and Cogent).

After WHOIS, traceroute, and passive DNS analyses proved inconclusive, we scanned the proxies' IP address neighborhoods for HTTP proxies and discovered that they contain several NXDOMAIN redirection servers, including Paxfire's demonstration servers and another Squid proxy we did not observe in our Netalyzr sessions.[6] We also began working with the EFF during this process. They were able to provide independent confirmation that Paxfire was responsible for this behavior.

Paxfire's search-engine proxying is not mandatory, since Verizon uses Paxfire but exhibits only NXDOMAIN wildcarding. We rule out performance reasons for the redirection: not only are search results poorly cacheable, the small number of proxies also introduces a failure point that cannot come near the uptime of the actual search engines' servers. We suspect that Paxfire harvests user search behavior for commercial purposes yielding revenue they share with participating ISPs.

7 Final Thoughts

A potential revenue increase of 1–3 USD per customer per year [14] has resulted in a far-reaching change to the workings of one of the Internet's core protocols. Our analysis of the way major ISPs involve the 6 top error traffic monetization providers in central parts of their technical infrastructure demonstrates that ISPs are clearly willing to experiment in this space, sometimes even rerouting substantial volumes of error-unrelated traffic through these providers. DNS likely will not be the end of it: Barefruit claims to offer services to monetize HTTP 404 errors by rewriting them to ad server redirection. Xerocole also implies that it offers these tools in their discussion of DNSSEC. We have also observed public complaints about ISPs deploying resolver-independent *in-path* NXDOMAIN rewriting, which prevents customers from avoiding interference by using a third-party resolver.

We have recently augmented Netalyzr's test suite to detect such manipulations. Preliminary results show at least one ISP (Mediacom, in cooperation with Infospace) and some Linksys NATs performing 404 rewriting. We have not yet observed any significant in-path NXDOMAIN rewriting, but we have observed NATs redirecting all DNS requests through their configured recursive resolver, which creates the appearance of in-path NXDOMAIN rewriting [4].

8 Acknowledgments

As always, we are deeply grateful to our Netalyzr users for enabling this study. We are particularly grateful to Peter Eckersley at the EFF. We thank Amazon for supporting our EC2 deployment and acknowledge support by the National Science Foundation under grants NSF CNS-0722035, NSF-0433702, and CNS-0905631, with additional support from Google and Comcast.

References

[1] Barefruit. The Barefruit Solution. http://www.barefruit.com/.

[2] Creighton, T., Griffiths, C., Livingood, J., and Weber, R. DNS Redirect Use by Service Providers. Internet Draft draft-livingood-dns-redirect-03.

[3] D-Link. Advanced DNS. http://www.dlink.com/support/faqDetail/?prod_id=3383&print=1.

[4] Public DNS Discuss: Listen on 5353 too? http://groups.google.com/group/public-dns-discuss/browse_thread/thread/31fa7260772ace32?hl=en.

[5] ICANN Security and Stability Advisory Committee. SAC 032: Preliminary Report on DNS Response Modification.

[6] Infospace. DNS Error Assist Service. http://www.infospaceinc.com/business/hp_dnserrorassistservice.aspx.

[7] IOActive. Entire Web at Risk: Earthlink and Verizon Advertising Security Revealed. http://www.ioactive.com/news-events/KaminskyEarthlinkPR.html.

[8] Kreibich, C., Weaver, N., Nechaev, B., and Paxson, V. Netalyzr: Illuminating the edge network. In *Proc. ACM IMC* (Melbourne, Australia, Nov. 2010).

[9] Nominum. Vantio NXR. http://www.nominum.com/what-we-do/software-systems/vantio-nxr.

[10] OpenDNS. DNS Based Web Security. http://www.opendns.com/.

[11] Paxfire. Generating New Revenue for Network Operators. http://www.paxfire.com/.

[12] purezero. Google Support: Can't Resolve Google Through my ISP. http://www.google.com/support/forum/p/Web+Search/thread?tid=5c10868a8217917d&hl=en.

[13] Sandvine. Search Guide. http://www.sandvine.com/downloads/documents/sandvine_search_guide.pdf.

[14] Xerocole. Solutions. http://www.xerocole.com/solutions/.

[15] Zhang, C., Huang, C., Ross, K., Maltz, D., and Li, J. In-flight Modifications of Content: Who are the Culprits? In *Workshop of Large-Scale Exploits and Emerging Threats (LEET'11)* (2011).

[5] `8.15.228.128/25`, part of a large Level3 block, and `69.25.212.0/25`, registered to Almar Networks LLC, a Nevada shell company.

[6] Demonstration servers: `8.15.228.241-248`, additional proxy: `8.15.228.249`.