Detecting DNS Root Manipulation

Ben Jones[1(✉)], Nick Feamster[1], Vern Paxson[2,3], Nicholas Weaver[2], and Mark Allman[2]

[1] Princeton University, Princeton, USA
bj6@cs.princeton.edu
[2] International Computer Science Institute, Berkeley, USA
[3] University of California, Berkeley, USA

Abstract. We present techniques for detecting unauthorized DNS root servers in the Internet using primarily endpoint-based measurements from RIPE Atlas, supplemented with BGP routing announcements from RouteViews and RIPE RIS. The first approach analyzes the latency to the root server and the second approach looks for route hijacks. We demonstrate the importance and validity of these techniques by measuring the only root server ("B") not widely distributed using anycast. Our measurements establish the presence of several DNS proxies and a DNS root mirror.

1 Introduction

The integrity and availability of many forms of Internet communication rely on replies from the DNS root name servers. Entities operating unauthorized root servers can completely control the entire Internet name space for any systems within their sphere, including blocking access to sites by disrupting their name resolution, or arbitrarily interposing on communication by redirecting through man-in-the-middle proxies. In this paper, we present some techniques for assessing the prevalence of unauthorized root servers.

We develop techniques to detect several scenarios where clients cannot direct queries to the authorized DNS root servers. We call this phenomenon *DNS root manipulation*, regardless of whether correct DNS results are returned, because such servers can provide adversarial responses. Countries such as China [3], Pakistan [12,18], and Turkey [1] already manipulate DNS to impose censorship, sometimes incidentally affecting DNS resolution for other countries [2,8]. We are interested in similar cases where an attacker can control where DNS packets are sent, thereby preventing access to the root. Given the size of this threat, we focus on attackers who manipulate all DNS root-server replicas, rather than those who subvert only a subset of them.

As deployed today, the DNS root comprises 13 server addresses run by 12 organizations, designated `a.root-servers.net` ... `m.root-servers.net`. DNS resolvers have the IP addresses for these 13 logically distinct entities hardwired into their configurations, grounding DNS resolution. All but one

T. Karagiannis and X. Dimitropoulos (Eds.): PAM 2016, LNCS 9631, pp. 276–288, 2016.
DOI: 10.1007/978-3-319-30505-9_21

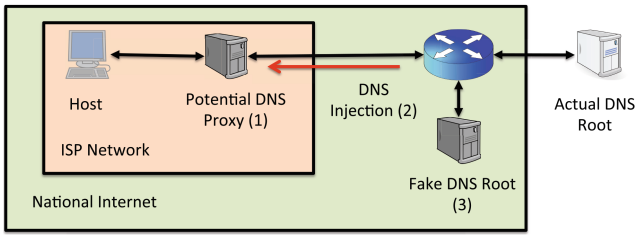

Fig. 1. Attackers can manipulate access to the DNS root with (1) an in-path DNS proxy, (2) DNS injection, or (3) changes to Internet routing to false DNS root servers.

of these servers uses anycast to route the corresponding IP address to multiple servers around the Internet. The number of topologically distinct replicas for each anycasted root server range from two (`h.root-servers.net`) to 150 (`l.root-servers.net`).

Threat Model. Figure 1 illustrates three ways that an attacker can implement DNS root manipulation. Although some malware has controlled DNS lookups directly on end-systems [10], that approach presumably presents difficult scaling issues to conduct in a widespread fashion. In this paper, we focus on network-based manipulation. The first method interposes a middlebox to intercept DNS traffic bound for root servers. For smaller networks, a transparent proxy achieves both control as well as potential performance improvements by caching queries. Transparent proxies are easy to implement because DNS operates over UDP, which is connectionless; thus, proxies do not need extensive state. Second, an attacker may observe DNS requests and inject responses before legitimate responses return. Finally, an attacker can compromise IP routing to redirect traffic for the DNS root servers to a false root replica—analogous to the anycast technology used for legitimate root replicas.

In all three cases, the attacker controls DNS responses, providing complete control over DNS. Due to the scale and complexity required to manipulate queries to the root servers, we assume that an entity seeking to subvert the DNS root servers would do so across all 13 logical servers to obtain unambiguous control. Additionally, our techniques assume that an in-path device does not selectively choose which DNS requests to manipulate.

Approach. As discussed in Sect. 3, our approach identifies some unauthorized root servers by examining side effects introduced by putting infrastructure in place to handle DNS root lookups. Specifically, we examine the latency and routing from various points around the Internet to the one non-anycasted root server, `b.root-servers.net`, which in the absence of unauthorized manipulation should reflect its singular location in Los Angeles, USA. We use the roughly 8,000-node RIPE Atlas [23] measurement platform for large-scale measurements. We complement our active probing with BGP routing table snapshots from RouteViews [26] and RIPE RIS [22].

We develop methods to cast a wide net and demonstrate their validity by finding several instances of DNS root manipulation. We find one ISP that redirects clients at the IP layer to an unauthorized root replica. Further, we find several ISPs prevent direct access to the authorized root servers by interposing on DNS lookup with proxies. Our methods give us confidence that we have detected most, if not all, DNS root mirrors from our vantage points, though we do not cover all ASes and we may underestimate DNS proxies. Section 2 sketches related work in examining the fidelity of DNS resolution. We then discuss our measurement approach in Sect. 3, and apply our approach in Sect. 4. We discuss future work in Sect. 5 and summarize in Sect. 6.

2 Related Work

Several previous efforts have explored DNS manipulation, measured DNS root servers, and looked for prefix hijacking.

DNS Manipulation. Dagon *et al.* found corrupt DNS resolvers by measuring open resolvers [10]. This effort focused on finding compromised hosts rather than DNS root manipulation and found that 2 % of resolvers provided incorrect queries and 0.4 % provided misleading answers. Closer to our work, Weaver *et al.* used the Netalyzr end-system network measurement platform to explore DNS manipulation [28] and characterize home network DNS resolution [13,27]. Between them, these two studies have characterized DNS manipulation from both the server and the client side but did not focus on root replicas.

DNS Root Measurement. Several studies of the DNS root infrastructure examine performance issues, particularly for anycast. Unfortunately, these works are often out of date (some over 10 years old) or measure from only a few vantage points [5,15,16,24,25]. Ballani *et al.* explored the DNS root anycast deployment using open resolver measurements, but made no attempt to find unauthorized roots [6]. Liang *et al.* also explored the DNS root, but focused on typical performance rather than exploring oddly low response times [14]. We also focus on using these measurements to find unauthorized roots, which Liang *et al.* mention but do not explore.

Prefix Hijacking. Several studies have explored prefix hijacking, theoretically and practically. Ballani *et al.* showed that ASes are theoretically capable of hijacking a large fraction of the IP space, especially if they are a tier-1 ISP [7]. Nordström *et al.* defined several potential attacks against BGP and suggested where new countermeasures were needed [19]. The past several years have also seen several studies of hijacking attacks in the wild, such as the Pakistani misconfiguration that prevented users around the world from accessing YouTube [20], and protecting important infrastructure, like the DNS root [9]. We use these methods to look for BGP attacks against the DNS root.

3 Measurement Method

To infer whether clients receive responses from an unauthorized root replica instead of the actual DNS root, we examine both *latency* (as evident from responses that return more quickly than they should, according to the distance to `B` root) and *server identity* (as evident from HOSTNAME.BIND replies, traceroutes, and BGP routes).

Table 1. Data sources used to investigate possible manipulation.

Measurements	Dates	Manipulation
RIPE Atlas		
Ping	July 6–13, 2014	Root mirrors
HOSTNAME.BIND	July 22, 2014	Proxies & Root mirrors
Traceroutes	July 6, 2014	Proxies & Root mirrors
BGP		
RIPE RIS	July 6–13, 2014	Root mirrors
RouteViews	July 7, 2014	Root mirrors

We use two different approaches to observe potential DNS root manipulation: (1) direct end-system measurements using RIPE's Atlas infrastructure (about 8,000 nodes in 2,755 distinct ASes over 189 countries); and (2) control-plane analysis via BGP monitoring. For each platform, Table 1 shows what measurements were collected, when they were collected, and the types of manipulation that can be detected from each measurement. We analyzed a week of measurements from the RIPE Atlas platform, spanning July 6–13, 2014. We received one HOSTNAME.BIND measurement from each of 6,135 Atlas probes and about 2,500 ping measurements from each of 6,546 Atlas probes. For reasons we could not determine, the dataset does not include all Atlas probes listed as currently deployed, but we use data from the 5,929 Atlas probes providing both measurements.

3.1 Anomalous Response-Time Latency

To look for transparent DNS proxies, we draw upon the ongoing ICMP ping measurements that by default the RIPE Atlas nodes make to each of the DNS roots every 240 s (four minutes) [21], analyzing in particular the ping times to the singular `B` root. Additionally, we time HOSTNAME.BIND DNS queries sent to `B` root. In the absence of a DNS proxy, we expect these response times to be similar. In the presence of a DNS proxy, we expect the DNS response time to be much lower because the DNS query will not go all the way to the authoritative `B` root DNS server. The latency difference would be evident in DNS injection and difficult for an attacker to mask. A strong attacker who can intercept DNS traffic

could of course transform DNS replies instead of answering requests directly, and hence produce the expected latency from querying the corresponding authorized root servers.

3.2 Anomalous Server Identity

We next sketch three methods to establish the identity of the DNS root server and its position in the network.

HOSTNAME.BIND Queries. To identify anomalous server identities, we issue HOSTNAME.BIND queries from Atlas probes—special DNS queries that ask a DNS server to identify itself. HOSTNAME.BIND replies from the correct `B` root follow the pattern `b`x, where x ranges from 0 to 9. Invalid or null responses may indicate that the replies did not come from the actual root server. We also explored using the EDNS NSID extension [4], another DNS server identification protocol, but the extension does not provide additional information for our purposes, and is not supported by `B` root. It would be difficult for a DNS proxy to fake the HOSTNAME.BIND response because for responses to appear valid, they would need to be customized based on the root to which the original request was sent. This mode of operation would make the proxy more complex and is not supported by default software, making its use unlikely. A DNS root mirror might instead falsify the response of the singular `B`, but we did not observe such scenarios.

Traceroutes. We look for DNS root mirrors by analyzing the ongoing UDP traceroutes conducted from RIPE Atlas nodes to the `B` and `L` roots[1] every 1800 s (30 min) [21].[2] We use traceroutes to identify potential root mirrors by (1) checking the ASN on the penultimate hop before reaching `B` root and (2) comparing traceroutes from the Atlas probe to `B` and `L` roots. By checking the ASN on the penultimate hop, we can verify that the traffic left the Atlas probe's AS and that the probe's traffic took a valid route to `B` root. We assume that an attacker would have difficulty falsifying all of the traceroute hops to the root servers.

Similarly, we hypothesized that an attacker might use a single root mirror to serve multiple DNS roots to avoid replicating the same functionality. To detect root mirror reuse, we check how many hops match between traceroutes to `B` and `L` roots. (We again assume that an attacker would have difficulty falsifying all traceroute hops to the root servers.)

BGP Routing Tables and Updates. We also looked for evidence of manipulating routing to alter the topological location of the root servers. Private routes can occasionally leak to the public Internet, as when Pakistan censored YouTube [20]. Brown *et al.* found anecdotal evidence of DNS censorship in China affecting the DNS root for other countries [8].

[1] We `L` root selected solely for convenience.

[2] The UDP query packets are not DNS requests, nor do they use the DNS service port.

If a hijacked route propagates outside the targeted network, the announcement may appear in public BGP databases. To explore this possibility, we examine BGP data from University of Oregon's RouteViews project [26] and RIPE's Routing Information Service (RIS) [22] for the same time period as the RIPE Atlas data. Both RouteViews and RIS collect public peering data from exchange points around the world by pulling the data from route servers at regular intervals. We analyzed the data by checking RIBs for `B` root's prefix, and checking if the AS path or prefix differed from real announcements. We speculated that an AS might perform a hijacking attack (directed at either their internal BGP network or at other ASes) by interjecting themselves into the AS path or announcing a more specific prefix.

4 Results

We applied the techniques from Sect. 3 to look for evidence of DNS root manipulation. Analyzing anomalous latencies and HOSTNAME.BIND replies identified a modicum of DNS root manipulation; the routing and traceroute data did not yield any additional evidence of such manipulation.

4.1 In-Path DNS Proxies

We identified eleven HOSTNAME.BIND responses that did not match the expected `b`x pattern discussed in Sect. 3.2. One of these coincides with a DNS mirror in China, which we discuss in Sect. 4.2. We find that the other ten HOSTNAME.BIND responses from other root servers yielded identical results, suggesting that the Atlas probes reside behind a hidden DNS proxy. Only one ISP with such a DNS proxy hosted multiple Atlas probes, but three of the four Atlas probes on that network exhibited correct HOSTNAME.BIND responses, suggesting that the proxy may reflect user configuration rather than ISP deployment. For the other nine instances, the use of DNS proxies appears to reflect an intentional decision, because several HOSTNAME.BIND responses correspond to the name of the ISP. This manipulation may be used to improve performance. For example, an Atlas probe hosted by Wananchi, a Kenyan ISP, received a response purportedly from `B` root that identifies the server `dns3.wnanchi.com` in 14 ms—as opposed to 318 ms for ping measurements to `B` root.

Using the ping data, we looked for minimum ping times that were less than the minimum speed-of-light propagation delay from RIPE Atlas nodes to `B` root. These measurements should not be affected by any hidden DNS proxies because we base them on ICMP ping packets; they should also not reflect unrelated network failures (which can only increase latency, assuming we eventually receive a reply). To determine whether to deem a ping RTT as implausibly low, we geolocated each Atlas probe and restricted our analysis to low ping times from Atlas probes outside of North and South America. We compared Atlas's own geolocation information with MaxMind's [17] geolocation of the Atlas probe's externally visible IP address (as determined by Atlas's servers). This process

yields only one source of geolocation for 1,388 Atlas probes (22.6 %); we find inconsistent location information for another 106 Atlas probes (1.7 %), which we do not use for our analysis.

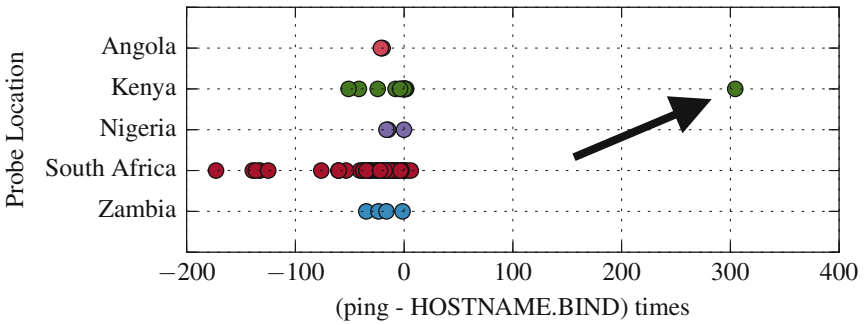

Fig. 2. Difference in response times between pings and HOSTNAME.BIND queries to `B` root. DNS response times significantly lower than ping times suggest the presence of a DNS proxy like the one the arrow points to.

These measurements detected the same ten DNS proxies as the HOSTNAME.BIND measurements we describe above by looking at the difference in response time between DNS queries and pings to `B` root. The fact that two independent techniques detected the same ten DNS proxies increases our confidence in the result.

Figure 2 shows the difference in response time between DNS queries and pings to `B` root for a representative sample of African countries. We observe a slightly smaller ping response time, except for the previously discussed DNS proxy in Kenya. These results are representative of the rest of our dataset; only eleven Atlas probes have DNS response times more than 50 ms faster than their ping and ten of these eleven Atlas probes are behind DNS proxies. The remaining Atlas device, which is not behind the root mirror, appears to reflect a network change between the ping and DNS measurements because both the ping and DNS query response time are over 350 ms. Our results are qualitatively consistent with those of Weaver *et al.* [27], which found that 1.4 % of Netalyzr clients resided behind hidden DNS proxies, although we observe one-tenth of that previously observed rate.

4.2 Rogue DNS Root Mirrors

One HOSTNAME.BIND response did not match the expected format from `B` root but did not appear to be a DNS proxy. We identified this response as an unauthorized DNS root replica in China and confirmed its presence with pings and traceroutes.

We explored the minimum response time to `B` root by continent, highlighting four clear outliers, one of which is shown in Fig. 3. As mentioned, one outlier was

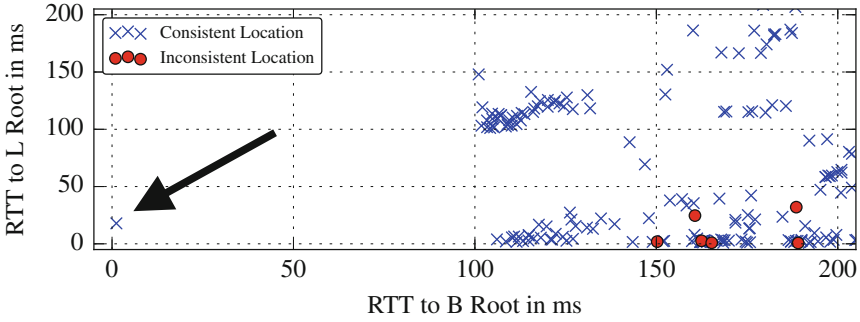

Fig. 3. Response times to `B` root (unicast from USA) and `L` root (150 anycast sites) from 184 RIPE Atlas probes geolocated to Asia. The arrow points to the DNS root mirror, a clear outlier.

a DNS root mirror, but the other three outliers were measurement errors. Despite these outliers, we are confident in our timing data because Fig. 3 demonstrates that the response times were generally consistent, even when geolocation was problematic (the plot also includes responses that were discarded for inaccurate geolocation). We continued exploring the outliers by validating our geolocation information with traceroutes. As a result of this validation, we discarded an Atlas probe in New York that erroneously geolocated to Switzerland. (The traceroute showed that the first hop was only a few milliseconds away and included "`us`" as part of the router name.)

When further analyzing the ping responses for the remaining outliers, we found that aside from the DNS root mirror itself, the other two outliers were measurement errors due to improper handling of ICMP error messages. For example, an Atlas probe in Belgium received many ping responses with a TTL of 255 and a response time around 5 ms followed by duplicate responses with a TTL of 44 and a response time around 168 ms. The TTL of 255 indicates that the first hop router sent an ICMP error message which the RIPE Atlas platform interpreted as an ICMP ECHO reply.

We determined that the fourth outlier was an unauthorized root mirror in the China Education and Research Network. The Atlas probe could ping `B` root in 1.2 ms and a HOSTNAME.BIND query produced an invalid response with a response time of 16 ms. The Atlas probe experienced infrequent network issues with 8 pings (0.11 %) over 100 ms, but Fig. 4 demonstrates that the pings were otherwise consistent. Both RIPE Atlas and MaxMind geolocated the Atlas device to China, and all hops on a traceroute to `B` root are in the same ASN. Additionally, the Atlas probe could directly communicate with a (non-root) authoritative DNS server under our control, so the Atlas probe does not appear to be behind a DNS proxy. The presence of so many measurements makes it more likely that this RIPE Atlas probe is behind a DNS root mirror.

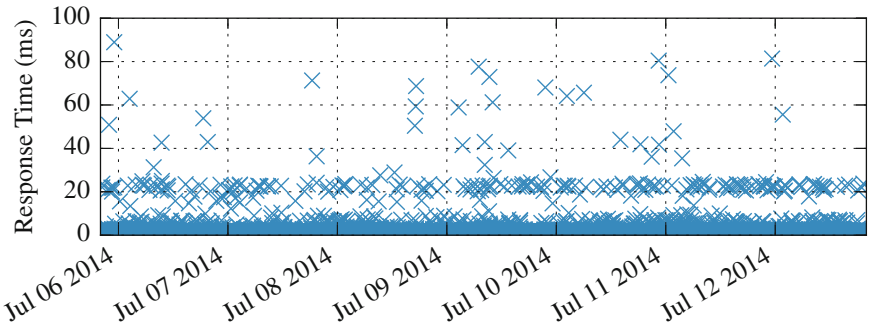

Fig. 4. 2,519 pings to B root from a Chinese Atlas probe are consistently, impossibly low, indicating a root mirror.

4.3 Traceroutes

We analyzed traceroutes to B and L roots and did not find any evidence of DNS root mirrors. We analyzed these traceroutes by noting the penultimate hop on the path to B root and comparing the traceroutes between B and L roots.

Validating Paths to B Root. To understand the penultimate router in the path to B root, we explored 4,333 traceroutes from 1,948 Atlas probes to B root. These totals do not include traceroutes that did not successfully complete or that contained any errors or packet drops. We found that the penultimate router for B root was in AS 226 (Los Nettos) for 1,647 Atlas probes (3,488 traceroutes), in AS 2153/2152 (California State University) for 295 Atlas probes (814 traceroutes), in AS 4 (ISI) for two Atlas probes (22 traceroutes), in AS 8121 (Layer 42) for 1 Atlas probe (5 traceroutes), in AS 34168 (Rostelecom) for one Atlas probe (2 traceroutes), and in AS 2914 (NTT Communication) for one Atlas probe (1 traceroute). The dataset included traceroutes from five Atlas probes identified as behind DNS proxies above, and in each case the Atlas probe transited through Los Nettos.

Los Nettos and California State University were the most prevalent routes and easily verified as legitimate given that Los Nettos is an advertised BGP neighbor of ISI (B root administrators) and ISI is located at the University of Southern California. The Layer 42 and NTT Communications cases can also be validated because they are different ASes than the ASes hosting the probes. Finally, the Atlas probe for Rostelecom is also hosted in Rostelecom, but the traceroute has 230 ms of latency, which suggests the Atlas probe is talking to the real root.

Comparing Paths Between B and L Roots. We hypothesized that if an attacker manipulated the DNS roots, they would likely redirect multiple roots to a single instance to avoid duplication. To evaluate this hypothesis, we analyzed 4,342 traceroute pairs to B and L roots from 1,292 Atlas probes. We removed all traceroutes that did not complete successfully or that contained an error

or drop, then matched B and L root traceroutes that originated from the same Atlas probe within 30 min.

We compared traceroutes by iterating over each hop in the L root traceroutes, then checking if any IP at the hop appeared at any hop in the L root traceroute. If the L root traceroute IP appeared in the B root traceroute, we marked the hop as matching. After performing the measurements, computed the fraction of matching hops by dividing by the number of hops in the L root traceroute.

These methods revealed no evidence of root manipulation. The closest traceroute pair had a matching hop fraction of 0.85 (12/14 hops matched). If manipulation were taking place, we would have expected the traceroutes to match exactly. The dataset also included 5 Atlas probes previously marked as DNS proxies, and their highest matching hop fraction was 0.8 (12/15 matching hops). These results are consistent with the absence of DNS root mirrors.

4.4 BGP Routing Table Manipulation

We analyzed BGP routing table snapshots for B root and found no evidence of hijacked routes. We analyzed BGP data from 13 RIPE RIS route servers Internet exchange points (IXPs) as geographically diverse as London and Japan. We supplemented this with data from the University of Oregon's RouteView's route servers in an additional nine IXPs around the world. We did not observe any prefix hijacking of B root. Our analysis is consistent with the general expectation that unauthorized root replicas are quite rare, even though we are not guaranteed to see a prefix hijack of B root.

5 Future Work

We have enumerated a few methods for measuring DNS root manipulation, but future work could expand these measurements, as follows.

Anomalous Response Times. We could extend our anomalous response time measurements using open resolvers as our edge network vantage points, as well as accurate geolocation information to extend these techniques beyond B root. We could determine the likely closest anycast instance for each DNS root replica using the provided geolocation information [11] (accurate to the city level), but we would also need to accurately locate open resolvers. We could then force each open resolver to contact the root by querying a non-existent top level domain (TLD) and measuring the response time. If the client receives a response in less time than the speed-of-light propagation delay to the closest root instance, then we know that a root mirror or DNS proxy is in use. Unfortunately, we have already demonstrated that collecting such geolocation data is difficult and would be the primary challenge to extending our work.

Anomalous Server Identity. We could also extend techniques to identify anomalous server identities with server-side analysis. We could better identify DNS proxies by sending queries for a DNS zone we control and ensuring that

(1) the authoritative server receives the query and (2) the client receives the correct response. We could ensure that the queries always hit our server and are never cached by including a nonce and always returning the same value (*e.g.*, an A record for `1.1.1.1` or a SERVFAIL). We would also ideally also collect data from the vantage point of the roots and query for randomly generated, non-existent TLDs from Atlas probes and open resolvers. Such a configuration would reveal whether our measurement machines reached the root, providing strong conclusions about DNS root manipulation.

6 Summary

We extended earlier findings on hidden DNS proxies [27] and potential root-server manipulation [8] to develop a method for detecting DNS root manipulation. To do so, we used two measurement techniques. First, we use RIPE Atlas probes to conduct pings, HOSTNAME.BIND queries, and traceroute measurements. Second, we examine BGP routing table snapshots for evidence of route hijacks.

We cast a wide net to validate our methods—2,755 access networks in 189 countries and 22 IXPs—but we found only a modicum of tampering with access to `B` root. Our measurements located ten hidden DNS proxies, most likely deployed for performance purposes and self-identifying to an associated ISP, and one root replica in China. Even the latter is not widely deployed: only one out of the 24 RIPE Atlas probes in China encountered it. Although DNS root manipulation is rare, it is clearly important to detect it when it does occur. We have demonstrated that our methods can detect such manipulation. Given China's willingness to tamper with the DNS root [8], we expect that these methods will continue to be useful for detecting root manipulation.

Acknowledgments. This research was supported in part by NSF awards CNS-1540066, CNS-1602399, CNS-1223717, CNS-1237265, and CNS-1518918. Ben Jones is also partially supported by a senior research fellowship from the Open Technology Fund. Any opinions, findings, and conclusions or recommendations are those of the authors and do not necessarily reflect the views of the sponsors.

References

1. Anderson, C., Winter, P., Roya.: Global network interference detection over the RIPE atlas network. In: 4th USENIX Workshop on Free and Open Communications on the Internet (FOCI 2014). USENIX Association, San Diego, August 2014
2. Anonymous.: The Collateral Damage of Internet Censorship by DNS Injection. SIGCOMM Comput. Commun. Rev., 42(3), 21–27 (2012)
3. Anonymous.: Towards a comprehensive picture of the great firewall's DNS censorship. In: 4th USENIX Workshop on Free and Open Communications on the Internet (FOCI 2014). USENIX Association, San Diego, August 2014
4. Austein, R.: DNS Name Server Identifier (NSID) Option, August 2007. https://tools.ietf.org/html/rfc5001

5. Ballani, H., Francis, P.: Towards a global IP anycast service. In: Proceedings of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, SIGCOMM 2005, pp. 301–312. ACM, New York (2005)
6. Ballani, H., Francis, P., Ratnasamy, S.: A measurement-based deployment proposal for IP anycast. In: Proceedings of the 6th ACM SIGCOMM Conference on Internet Measurement, IMC 2006, pp. 231–244. ACM, New York (2006)
7. Ballani, H., Francis, P., Zhang, X.: A study of prefix hijacking and interception in the internet. In: Proceedings of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, SIGCOMM 2007, pp. 265–276. ACM, New York (2007)
8. Brown, M.A., Madory, D., Popescu, A., Zmijewski, E.: November 2010. http://research.dyn.com/wp-content/uploads/2014/07/DNS-Tampering-and-Root-Servers.pdf
9. Bush, R., Mankin, A., Massey, D., Pei, D., Wang, L., Wu, F., Zhang, L., Zhao, X.: Protecting the BGP routes to top level DNS servers, June 2002. https://www.nanog.org/meetings/nanog25/presentations/massey.ppt
10. Dagon, D., Lee, C., Lee, W., Provos, N.: Corrupted DNS resolution paths: the rise of a malicious resolution authority. In: Proceedings of 15th Network and Distributed System Security Symposium (NDSS), San Diego, CA (2008)
11. DNS Root Servers. root-servers.org (2015). http://root-servers.org/
12. Khattak, S., Javed, M., Khayam, S.A., Uzmi, Z.A., Paxson, V.: A look at the consequences of internet censorship through an ISP lens. In: Proceedings of the Conference on Internet Measurement Conference, IMC 2014, pp. 271–284. ACM, New York (2014)
13. Kreibich, C., Weaver, N., Nechaev, B., Paxson, V.: Netalyzr: illuminating the edge network. In: Proceedings of the 10th ACM SIGCOMM Conference on Internet Measurement, IMC 2010, pp. 246–259. ACM, New York (2010)
14. Liang, J., Jiang, J., Duan, H., Li, K., Wu, J.: Measuring query latency of top level DNS servers. In: Roughan, M., Chang, R. (eds.) PAM 2013. LNCS, vol. 7799, pp. 145–154. Springer, Heidelberg (2013)
15. Liston, R., Srinivasan, S., Zegura, E.: Diversity in DNS performance measures. In: Proceedings of the 2nd ACM SIGCOMM Workshop on Internet Measurment, IMW 2002, pp. 19–31. ACM, New York (2002)
16. Liu, Z., Huffaker, B., Fomenkov, M., Brownlee, N., Claffy, K.C.: Two days in the life of the DNS anycast root servers. In: Uhlig, S., Papagiannaki, K., Bonaventure, O. (eds.) PAM 2007. LNCS, vol. 4427, pp. 125–134. Springer, Heidelberg (2007)
17. MaxMind, Inc. GeoIP2 Country (2015). https://www.maxmind.com/en/geoip2-country-database
18. Nabi, Z.: The anatomy of web censorship in Pakistan. In: Presented as part of the 3rd USENIX Workshop on Free and Open Communications on the Internet. USENIX, Berkeley (2013)
19. Nordström, O., Dovrolis, C.: Beware of BGP attacks. SIGCOMM Comput. Commun. Rev. **34**(2), 1–8 (2004)
20. RIPE. YouTube Hijacking: A RIPE NCC RIS case study (2008). https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study
21. RIPE. Built-In Measurements (2015). https://atlas.ripe.net/docs/built-in/
22. RIPE. Routing Information Service (RIS) (2015). https://www.ripe.net/data-tools/stats/ris
23. RIPE. What is RIPE Atlas? (2015). https://atlas.ripe.net/about/

24. Sarat, S., Pappas, V., Terzis, A.: On the use of anycast in DNS. In: Proceedings of 15th International Conference on Computer Communications and Networks, 2006, ICCCN 2006, pp. 71–78, October 2006
25. Sekiya, Y., Cho, K., Kato, A., Somegawa, R., Jinmei, T., Murai, J.: Root and ccTLD DNS server observation from worldwide locations. In: Proceedings of Passive and Active Measurement 2003, April 2003
26. University of Oregon. RouteViews Project (2015). http://www.routeviews.org/
27. Weaver, N., Kreibich, C., Nechaev, B., Paxson, V.: Implications of Netalyzrs DNS measurements. In: Proceedings of the First Workshop on Securing and Trusting Internet Names (SATIN), Teddington, United Kingdom (2011)
28. Weaver, N., Kreibich, C., Paxson, V.: Redirecting DNS for ads and profit. In: Presented as part of the 1st USENIX Workshop on Free and Open Communications on the Internet. USENIX (2011)