# Scanning Alexa's Top 1M for AXFR - Internetwache - A secure internet is our concern

By Internetwache.org

Published: 2015-03-29 · Archived: 2026-04-05 15:44:23 UTC

In this blogpost we will discuss a simple information disclosure problem called unauthorized AXFR. This can be used to leak DNS settings of a particular target, thus revealing internal / private considered DNS entries.

We've checked Alexa's Top 1M for this kind of issue and came to some interesting results.

## What is AXFR?

`Asynchronous Xfer Full Range` is a mechanism used by the DNS system to transfer zone information for a domain from a master (primary) DNS server to several slave (secondary) DNS servers. A slave sends an AXFR-request to the master which replies with all DNS information associated to a domain (zone).

## What could possibly go wrong?

If the master server does not validate the source of an AXFR request, anyone will be able to download the DNS zone file from this server. Usually only the secondary servers should be allowed to download the zone information from the master server.

One could argue that all the information in a zone file is publicly available, because you can request it "easily":

```
 > dig NS google.com
;; ANSWER SECTION:
google.com.               21599       IN       NS       ns3.google.com.
google.com.               21599       IN       NS       ns2.google.com.
google.com.               21599       IN       NS       ns1.google.com.
google.com.               21599       IN       NS       ns4.google.com.
```

We request information about the nameservers of `google.com` first. There are four nameservers which are answering DNS-requests for the domain.

```
 > dig A google.com @ns4.google.com
;; ANSWER SECTION:
google.com.               300       IN       A       173.194.32.196
google.com.               300       IN       A       173.194.32.201
google.com.               300       IN       A       173.194.32.198
google.com.               300       IN       A       173.194.32.199
google.com.               300       IN       A       173.194.32.194
google.com.               300       IN       A       173.194.32.193
google.com.               300       IN       A       173.194.32.200
google.com.               300       IN       A       173.194.32.206
google.com.               300       IN       A       173.194.32.195
google.com.               300       IN       A       173.194.32.192
google.com.               300       IN       A       173.194.32.197
```

Now, we asked the fourth nameserver ( `ns4.google.com` ) to list us all `A` (IPv4) entries for the domain `google.com` .

The same works for other request types (AAA/TXT/MX/CNAME/…), but you will need to know the DNS entry to ask for. It's not possible to ask something like "List me all subdomains for `google.com` in your zone". There are tools like Subbrute which brute-force the entries.

From a security perspective this information is the most valuable, because you are probably going to find some entries pointing to unprotected/vulnerable software.

For example an admin sets up a monitoring system at the subdomain `monitoring.internal.server1.domain.tld`. He thinks that it is hard for an attacker to guess this subdomain and that he does not need to set up additional layers of security to protect the system from unauthorized access.

If one of his nameservers is misconfigured, an attacker can send an AXFR request, download the zone and get access to the monitoring system.

## Scanning Alexa's top 1M

We wanted to see how many misconfigured nameservers can be found in Alexa's top 1M websites. We used a small python script to do the work. You can find it on GitHub.

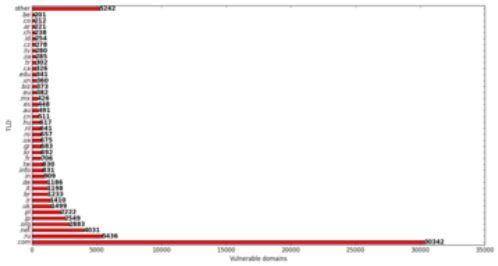
The results were a bit astonishing:

- 132854 AXFRs were made
- 72401 unique domains are affected
- 48448 unique nameservers are affected

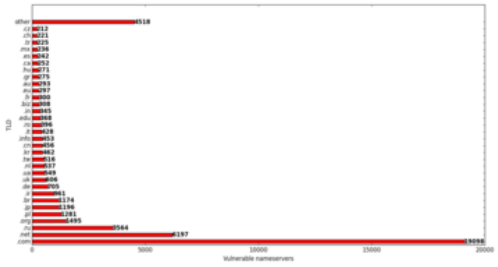
Some domains had multiple misconfigured nameservers, thus there have been more transfers than domains affected or the other way round that one nameserver served more than one zonefile.

**So on average every 20th website of the top Alexa 1M runs a misconfigured webserver.**

TLDs of the affected domains:



TLDs of the affected nameservers:



We were very disappointed to see some well and not so well known hosting companies running misconfigured nameservers. Grabbing some random samples from the data lead to the conclusion that information of the companies or it's customers could be accessed unauthenticated (similar to the scenario described above).

All other kind of websites could be found in our research results, too: Ranging from (huge) news portals over shopping sites to small personal websites.

## How to fix?

The easiest way to fix this issue is to re-check your dns server's configuration file. Make sure that the nameservers only allow AXFR to subsidiary nameservers and that these aren't allowed to answer AXFR requests.

If you want to check if your nameservers are misconfigured, you can use the following one-liner directly on your bash shell:

```
#!/bin/bash
# You need to have dnsutils installed
```

```
DOMAIN="YOURDOMAIN.TLD"
dig NS $DOMAIN +short | sed -e "s/\.$//g" | while read nameserver; do echo "Testing $DOMAIN @ $nameserver"; dig AXFR $DOMAIN "@$r
```

If you don't want to use the shell, you can use the following website: https://hackertarget.com/zone-transfer/

**We deeply recommend you to do so :)**

If you get the following output for all nameservers then you're safe.

```
; Transfer failed.
```

Otherwise you're probably running a misconfigured server. In case it's the popular `BIND` DNS-server you can use the following option to limit the IP addresses:

```
allow-transfer { 192.168.1.1; };
```

Where `192.168.1.1` is the IP address of the secondary DNS server.

## Conclusion

It's interesting to see that such 'easy' configuration mistakes, which had already been discussed around the 90's, are still happening.

The US CERT picked up on the topic and publised an alert about it.

Stay safe,

the team of internetwache.org

## Updates

- #1: 29/03/15: Changed URL for the AXFR testing website. Added configuration option for BIND.
- #2: 08/01/16: Added link to US CERT Alert.

---