SecurityTrails | Wrong Bind Configuration Exposes the Complete List of Russian TLD's to the Internet

domains government security

SecurityTrails Blog · Mar 14 · SecurityTrails team

DNS is one of the most important services of the net — it's the heart and soul of the Internet as we know it. And when DNS servers are not well configured, they can easily be exploited to gain important information about their DNS zones and records.

One of the most common misconfigurations that can be found on DNS servers is to have DNS zone transfers enabled.

By running an AXFR DNS query, you can run a full DNS transaction, that will eventually allow you to get and replicate DNS zones across servers.

Apparently, thanks to a bad DNS server configuration on Bind, the global zone transfers were enabled by default on a few Russian DNS nameservers.

Around June 6, 2017, due to a DNS misconfiguration some DNS servers were allowed to transfer zones without restrictions (AXFR). This lead to the full list of Russian TLD zones like .ru, .su, .tatar, and .рф to be exposed.

At that time, the AXFR request could be made using the following DNS servers:

- a.dns.ripn.net
- b.dns.ripn.net
- d.dns.ripn.net

The folks at the TLDR project noticed this fast enough to capture the complete list of all domains registered under Russian TLD space.

At that time, in order to get the full list of domain names you just only had to run this command:

```
dig axfr su. @a.dns.ripn.net
```

On June 19, 2017, the AXFR was disabled for these DNS servers, and since then it's no longer working:

```
[webtech@localhost ~]$ **dig axfr su. @a.dns.ripn.net**; <<>> DiG 9.11.2-P1-RedHat-9.11.2-1.P1.fc26 <<>> axfr s
```

But this misconfiguration was live long enough for some people to get the full domain names information and spread it over the network, exposing 5.1% of all domain names on the internet.

@mandatoryprogrammer, for example, managed to get this full list of **5,788,031 domain names**, which was later uploaded to GitHub. These are the stats he got from this leak:

Summary of Domain Names Leaked

- .ru (Russia ccTLD): **5,214,868 domains**
- .su (Soviet Union ccTLD): **104,591 domains**
- .tatar (gTLD): **861 domains**
- .рф (IDN ccTLD): **466,890 domains**
- .дети (gTLD): **821 domains**

Links to the leaked domain lists:

- .ru: Zone data: Download here
- .su: Zone data: Download here
- .tatar: Zone data: Download here
- .рф: Zone data: Download here
- .дети: Zone data: Download here

Just as with the Russia DNS leak, having the right DNS toolkit in your hands can enable you to audit possible security holes on 3rd party networks, defend against bad guys on your own servers, or apply for a cool data bounty program like the one we have at SecurityTrails.

It doesn't matter the type of agency or company you work for, whether it is private or public, when you need to investigate domain names, DNS servers, as well as IP addresses, you can always count on the powerful and reliable SecurityTrails API.

Open a free account today, start using SecurityTrails, or have a look at our public free service SecurityTrails.
