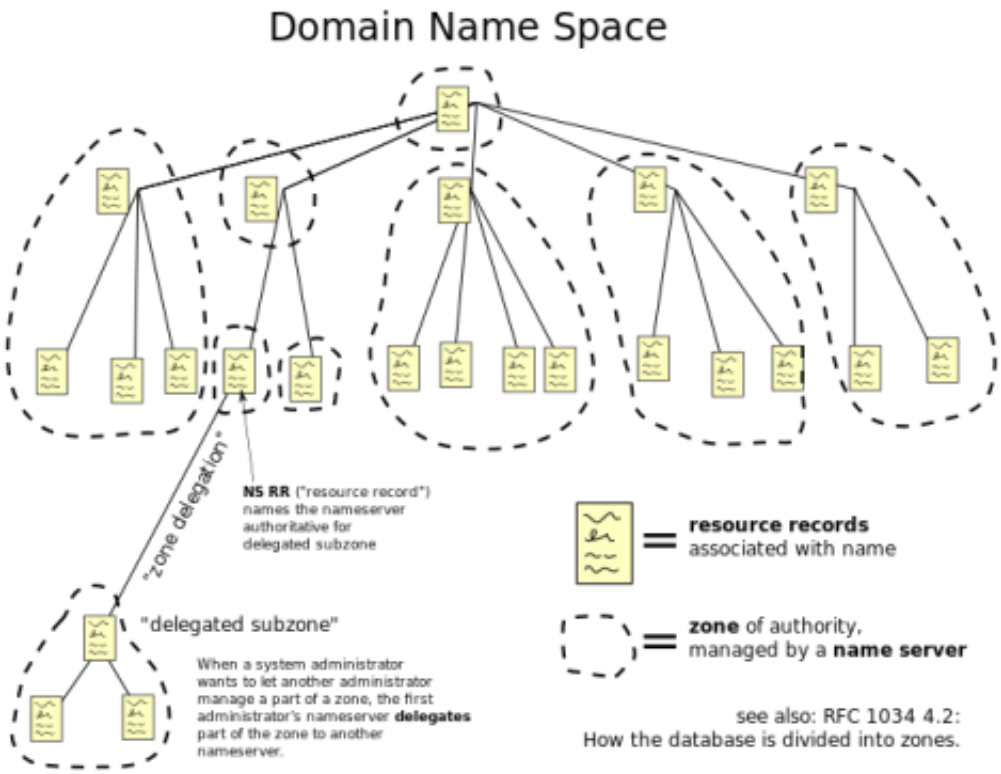
The router in your home might be intercepting some of your Internet traffic—but it may be for your own good

December 15 2021



The hierarchical Domain Name System, organized into zones, each served by a name server. Credit: Public Domain

The router in your home might be intercepting some of your Internet

traffic and sending it to a different destination. Specifically, the router can intercept the Domain Name System traffic—the communications used to translate human-readable domain names (for example www.google.com) into the numeric Internet Protocol (IP) addresses that the Internet relies on. That's the finding from a team of computer scientists at the University of California San Diego, which they presented at the Internet Measurement Conference on Nov. 3, 2021.

Why does this matter?

"The primary concern is privacy," said Audrey Randall, a Ph.D. student in computer science at the University of California San Diego and first author of a paper on this subject. "When you visit a web site, you first have to do a DNS lookup for that site. So whoever gets your DNS traffic gets to see all the sites that you're visiting. In principle, you get to choose who performs your DNS lookups and you might pick a company that you trust not to sell your data or a company that uses robust security to protect their logs. But if your DNS traffic is being silently intercepted and routed elsewhere, then someone else gets to see all that information."

Many cases of DNS interception are not malicious, Randall pointed out. Often, interception is used by Internet Service Providers (ISPs) to protect users from malware that contacts particular Domain Name System (DNS) resolvers, which are essentially the Internet's phone books. These resolvers transform the website URL users enter into a browser into an IP address for the servers that store the website's content. In this case, interception can be helpful, by preventing malware from harming a user's computer.

Researchers even found one instance of interception that was neither malicious nor benign: it was a simple bug. The UC San Diego team disclosed this bug to two Internet service providers. Both said they would

work to fix issues. However, DNS queries also provide valuable data about users' behavior that can be sold to advertisers, which might provide a less altruistic motive for some companies to intercept them.

The phenomenon of DNS interception has been studied in recent years, but little was known about where in the network interception takes place—until now. It turns out that in a surprising number of cases, users' own home routers are the culprit.

These routers don't send DNS queries to the target DNS resolver that the user specified. Instead, the software reroutes them to an alternate resolver. The query response is then modified so that it appears to come from the original target resolver. This modification makes the interception "transparent" to the user, and therefore very difficult to detect.

Determining where transparent interception takes place is difficult. But researchers were able to do this by devising an innovative and clever methodology. They first made use of special DNS queries that were invented as debugging tools, but they found that no single query could give enough information to pinpoint an interceptor's location. The key turned out to be to compare the responses from *two* special queries: the responses were identical if the interceptor was the home router, but different if the interceptor was elsewhere in the network.

Even though DNS interception is often used to foil malware, the fact remains that users have no idea that their traffic is being redirected, or where it's redirected to. "If you are concerned enough about who sees your data and who sells your data to advertisers, you want to make sure that the company handling it is actually who they say they are," said Randall. "When this type of transparent interception is used, you think you have control over your traffic, but you don't."

Researchers caution that their study has some limitations. For example, the platform they used to conduct their study is not representative of all interception cases, because it over-represents certain Internet service providers, countries, or demographics.

The research was published in *Proceedings of the 21st ACM Internet Measurement Conference*.

More information: Audrey Randall et al, Home is where the hijacking is, *Proceedings of the 21st ACM Internet Measurement Conference* (2021). DOI: 10.1145/3487552.3487817

Provided by University of California - San Diego