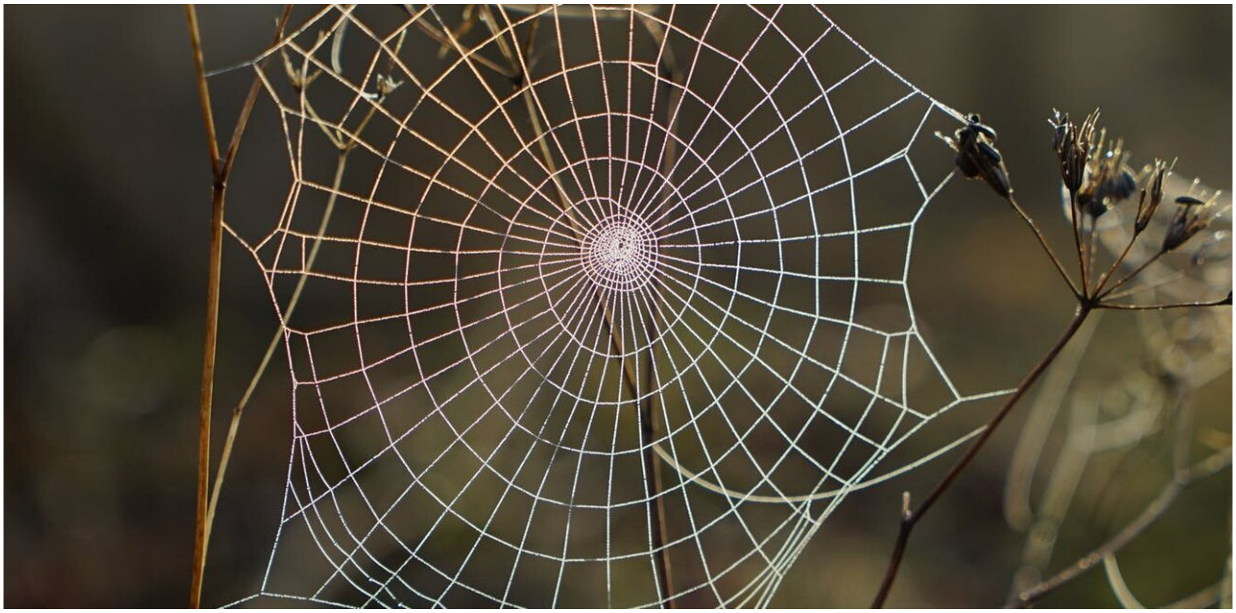
# Domain name fraud: is the global Internet in danger?

October 8 2019, by Hervé Debar



A spider's web is secure, and ours? Credit: Robert Anasch/Unsplash, CC BY

In late February 2019, the Internet Corporation for Assigned Names and Numbers (ICANN), the organization that manages the IP addresses and domain names used on the web, issued a warning on the risks of systemic Internet attacks. Here is what you need to know about what is at stake.

## What is the DNS?

The Domain Name Service (DNS) links a domain name (for example, the domain ameli.fr for French health insurance) to an IP (Internet Protocol) address, in this case "31.15.27.86"). This is now an essential service, since it makes it easy to memorize the identifiers of digital services without having their addresses. Yet, like many former types of protocol, it was designed to be robust, but not secure.

DNS defines the areas within which an authority will be free to create domain names and communicate them externally. The benefit of this mechanism is that the association between the IP address and the domain name is closely managed. The disadvantage is that several inquiries are sometimes required to resolve a name, in other words, associate it with an address.

Many organizations that offer Internet services have one or several domain names, which are registered with the suppliers of this registration service. These service providers are themselves registered, directly or indirectly with ICANN, an American organization in charge of organizing the Internet. In France, the reference organization is the AFNIC, which manages the ".fr" domain.

We often refer to a fully qualified domain name, or FQDN. In reality, the Internet is divided into top-level domains (TLD). The initial American domains made it possible to divide domains by type of organization (commercial, university, government, etc.). Then national domains like ".fr" quickly appeared. More recently, ICANN authorized the registration of a wide variety of top-level domains. The information related to these top-level domains is saved within a group of 13 servers distributed around the globe to ensure reliability and speed in the responses.

The DNS protocol establishes communication between the user's machine and a domain name server (DNS). This communication allows this name server to be queried to resolve a domain name, in other words, obtain the IP address associated with a domain name. The communication also allows other information to be obtained, such as finding a domain name associated with an address or finding the messaging server associated with a domain name in order to send an electronic message. For example, when we load a page in our browser, the browser performs a DNS resolution to find the correct address.

Due to the distributed nature of the database, often the first server contacted does not know the association between the domain name and the address. It will then contact other servers to obtain a response, through an iterative or recursive process, until it has queried one of the 13 root servers. These servers form the root level of the DNS system.

To prevent a proliferation of queries, each DNS server locally stores the responses received that associate a domain name and address for a few seconds. This cache makes it possible to respond more quickly if the same request is made within a brief interval.

## Vulnerable protocol

DNS is a general-purpose protocol, especially within company networks. It can therefore allow an attacker to bypass their protection mechanisms to communicate with compromised machines. This could, for example, allow the attacker to control the networks of robots (botnets). The defence response relies on the more specific filtering of communications, for example requiring the systematic use of a DNS relay controlled by the victim organization. The analysis of the domain names contained in the DNS queries, which are associated with black or white lists, is used to identify and block abnormal queries.

The DNS protocol also makes denial of service attacks possible. In fact, anyone can issue a DNS query to a service by taking over an IP address.

The DNS server will respond naturally to the false address. The address is in fact the victim of the attack, because it has received unwanted traffic. The DNS protocol also makes it possible to carry out amplification attacks, which means the volume of traffic sent from the DNS server to the victim is much greater than the traffic sent from the attacker to the DNS server. It therefore becomes easier to saturate the victim's network link.

The DNS service itself can also become the victim of a denial of service attack, as was the case for DynDNS in 2016. This triggered cascading failures, since certain services rely on the availability of DNS in order to function.

Protection against denial of service attacks can take several forms. The most commonly used today is the filtering of network traffic to eliminate excess traffic. Anycast is also a growing solution for replicating the attacked services if needed.

## Cache poisoning

A third vulnerability that was widely used in the past is to attack the link between the domain name and IP address. This allows an attacker to steal a server's address and to attract the traffic itself. It can therefore "clone" a legitimate service and obtain the misled users' sensitive information: Usernames, passwords, credit card information etc. This process is relatively difficult to detect.

As mentioned, the DNS servers have the capacity to store the responses to the queries they have issued for a few minutes and to use this information to respond to the subsequent queries directly. The so-called cache poisoning attack allows an attacker to falsify the association within the cache of a legitimate server. For example, an attacker can flood the intermediate DNS server with queries and the server will accept the first response corresponding to its request.

The consequences only last a little while, the queries made to the compromised server are diverted to an address controlled by the attacker. Since the initial protocol does not include any means for verifying the domain-address association, the customers cannot protect themselves against the attack.

This often results in Internet fragments, with customers communicating with the compromised DNS server being diverted to a malicious site, while customers communicating with other DNS servers are sent to the original site. For the original site, this attack is virtually impossible to detect, except for a decrease in traffic flows. This decrease in traffic can have significant financial consequences for the compromised system.

## Security certificates

The purpose of the secure DNS (Domain Name System Security Extensions, DNSSEC) is to prevent this type of attack by allowing the user or intermediate server to verify the association between the domain name and the address. It is based on the use of certificates, such as those used to verify the validity of a website (the little padlock that appears in a browser web bar). In theory, a verification of the certificate is all that is needed to detect an attack.

However, this protection is not perfect. The verification process for the "domain-IP address" associations remains incomplete. This is partly because a number of registers have not implemented the necessary infrastructure. Although the standard itself was published nearly fifteen years ago, we are still waiting for the deployment of the necessary technology and structures. The emergence of services like Let's Encrypt has helped to spread the use of certificates, which are necessary for secure navigation and DNS protection. However, the use of these technologies by registers and service providers remains uneven; some countries are more advanced than others.

Although residual vulnerabilities do exist (such as direct attacks on registers to obtain domains and valid certificates), DNSSEC offers a solution for the type of attacks recently denounced by ICANN. These attacks rely on DNS fraud. To be more precise, they rely on the falsification of DNS records in the register databases, which means either these registers are compromised, or they are permeable to the injection of false information. This modification of a register's database can be accompanied by the injection of a certificate, if the attacker has planned this. This makes it possible to circumvent DNSSEC, in the worst-case scenario.

This modification of DNS data implies a fluctuation in the domain-IP address association data. This fluctuation can be observed and possibly trigger alerts. It is therefore difficult for an attacker to remain completely unnoticed. But since these fluctuations can occur on a regular basis, for example when a customer changes their provider, the supervisor must remain extremely vigilant in order to make the right diagnosis.

## Institutions targeted

In the case of the attacks denounced by ICANN, there were two significant characteristics. First of all, they were active for a period of several months, which implies that the strategic attacker was determined and well-equipped. Secondly, they effectively targeted institutional sites, which indicates that the attacker had a strong motivation. It is therefore important to take a close look at these attacks and understand the mechanisms the attackers implemented in order to rectify the vulnerabilities, probably by reinforcing good practices.

ICANN's promotion of the DNSSEC protocol raises questions. It clearly must become more widespread. However, there is no guarantee that these attacks would have been blocked by DNSSEC, nor even that they would have been more difficult to implement. Additional analysis will be required to update the status of the security threat for the protocol and the DNS database.

This article is republished from The Conversation under a Creative Commons license. Read the original article.

Provided by The Conversation

Citation: Domain name fraud: is the global Internet in danger? (2019, October 8) retrieved 9 April 2024 from https://techxplore.com/news/2019-10-domain-fraud-global-internet-danger.html