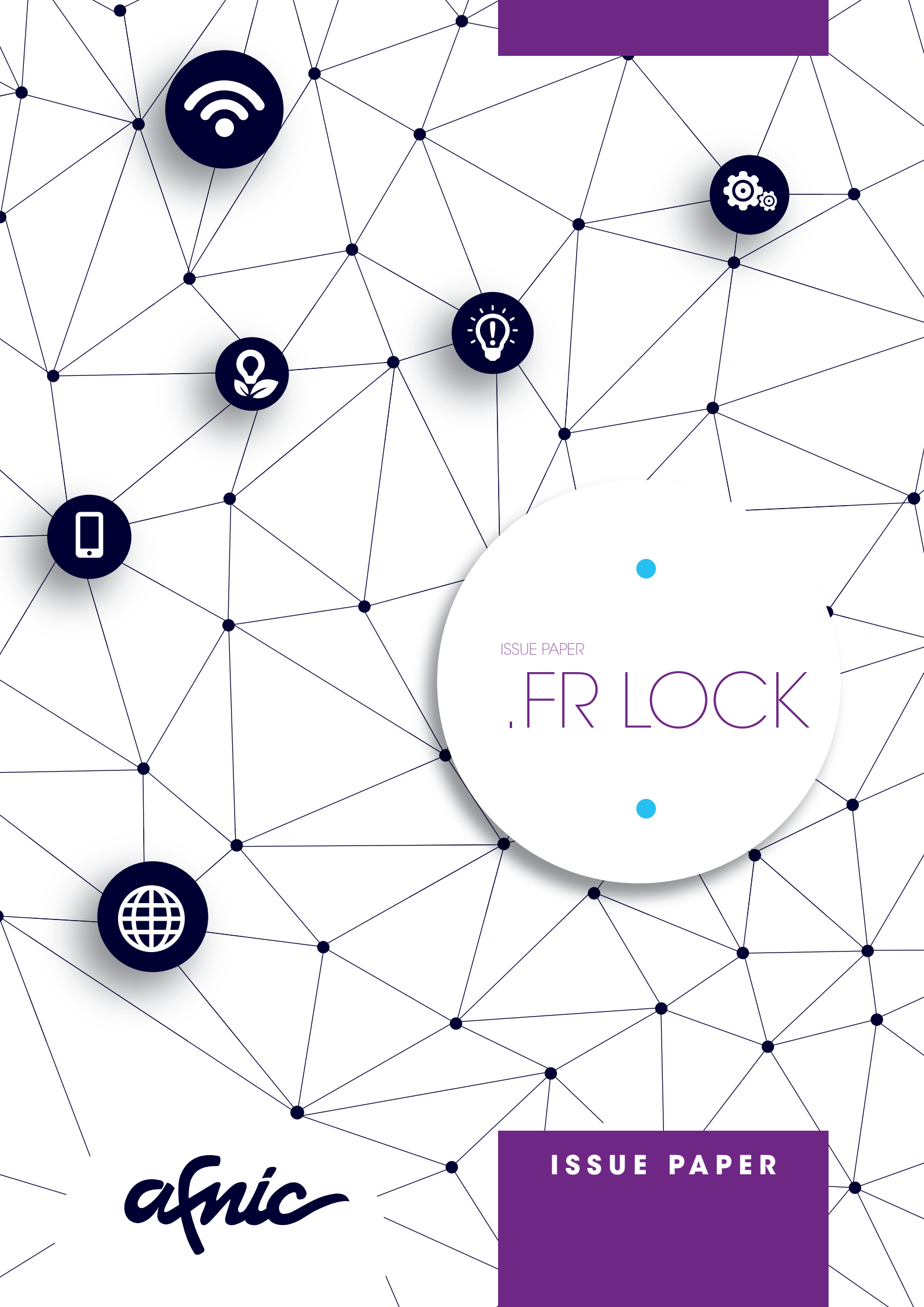


ISSUE PAPER

.FR LOCK

afnic

ISSUE PAPER

In 2015, Afnic launched .Fr Lock, a registry lock service designed to secure the most sensitive domain names against cyber-attacks linked to domain name hijacking. This issue paper provides an overview of this type of attack and an initial assessment after two years of commissioning.

/// OVERVIEW OF CYBER-ATTACKS RELATED TO DOMAIN NAME HIJACKING

Among the threats to domain names, the risk of hijacking is the reason for the existence of name locking services.

Hijacking is a form of cyber-attack in which the hackers succeed in gaining control of a domain name, enabling them to place data of their choosing in it (for example the IP address of a website they control). This form of cyber-attack does not jeopardize the DNS protocol in any way, since it only makes use of the domain name registration system. But since the registration system involves several players, the attack can target any one of them. In most cases, the stakeholders involved are the registry, the registrar and the DNS host (which is often the registrar, but may also be the registrants themselves or a third party).

Here are a few examples of hijackings in recent years. Each has been the subject of a study, although not all of the information is publicly available.

Example of an attack AGAINST A REGISTRY

In December 2016, the .bd (Bangladesh) registry was hacked. The attackers modified the name servers of google.com.bd thus transferring the Bangladeshi users of Google to a website controlled by the hackers.
In a case such as this, the technical solutions implemented by the registry are not sufficient. The only protection is registry security.

Examples of attacks AGAINST A REGISTRAR

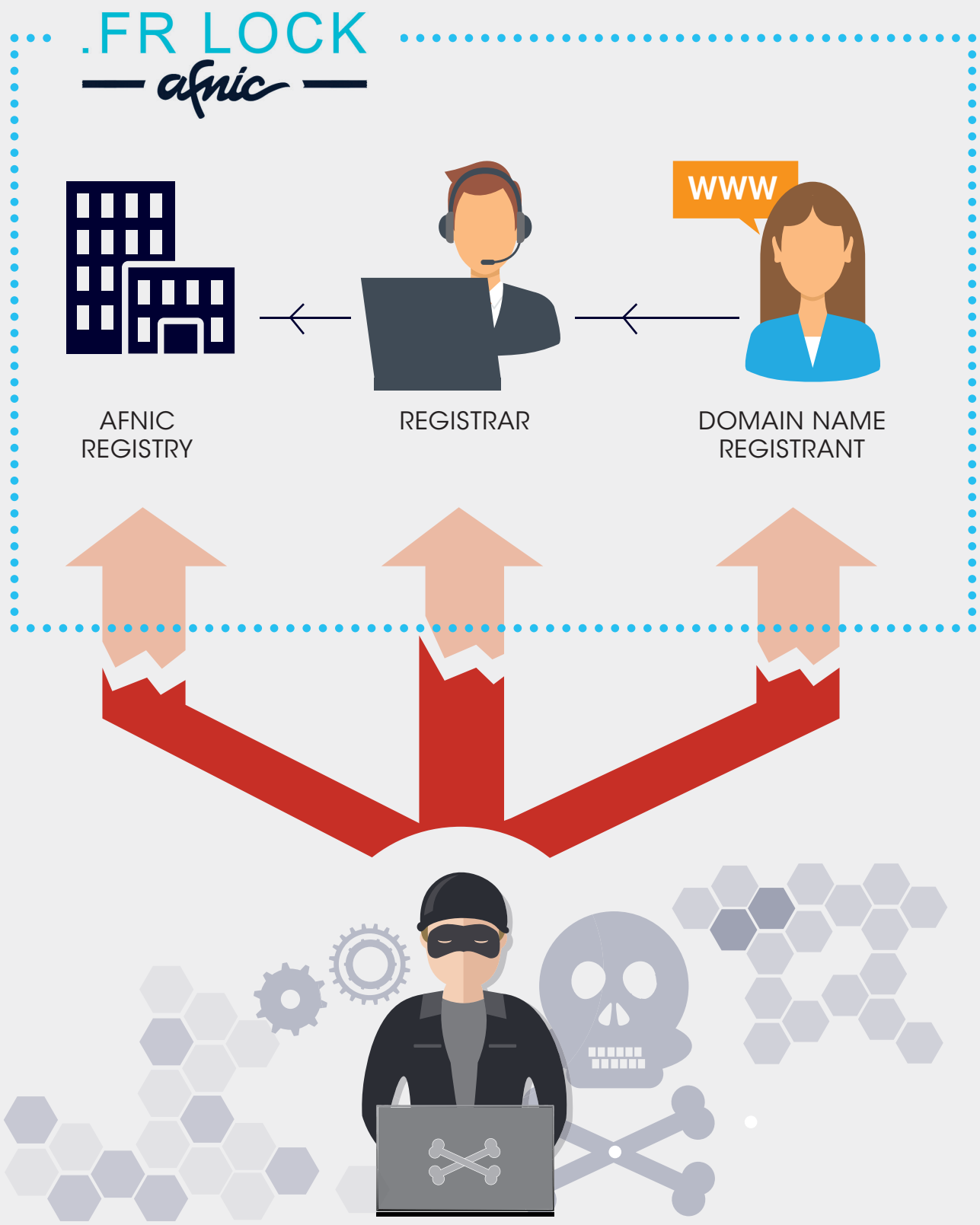
In April 2015, the eNom registrar was apparently hacked. The hackers were able to redirect a bank, stlouisfed.org, to a site that they controlled. The attack would not have been possible if the domain had been locked.
For example, in August 2013, when a political group hacked the MelbourneIT registrar, the domain nytimes.com, which was not locked, was hijacked, but because the domain twitter.com, equally as interesting and located on the same registrar, was locked, it could not be hijacked.
In another example, in February 2015, Lenovo had its domain lenovo.com hijacked after Superfish malware had been installed on the PCs of its customers. At least one other domain on the same registrar was hijacked by the same group, so we can deduce that the target of the attack was the registrar.

EXAMPLE OF AN ATTACK AGAINST DNS HOSTING

In December 2014, the Emirates telecommunications operator Etisalat had its domain hijacked. In technical terms, the name servers («NS records») were not changed, but the IP address advertised was changed. Apparently, the host was not hacked, but Etisalat's account with the host was hijacked. Note that it is difficult to distinguish the hacking of registrar from the hacking of a customer's account alone. In this case, only the domain name was hijacked, suggesting the purpose was to hack a single account.

Conclusion

Hijacking domain names is a real threat, and these few examples are just the tip of the iceberg. Without a public monitoring system for domain name changes, no doubt many occurrences of hijacking go relatively unnoticed. It is therefore crucial to take precautions to avoid hijacking. The individuals in an organization who manage domain names must be knowledgeable about computer security and aware of the issues involved. On the other hand, it is also necessary to guard against security problems involving providers' systems. It is for these reasons that a registry lock is useful.


.FR LOCK
afnic
WWW
AFNIC
REGISTRY
REGISTRAR
DOMAIN NAME
REGISTRANT

/// .FR LOCK IS AN EFFECTIVE COUNTER AGAINST THIS TYPE OF ATTACK, BUT IS STILL TOO LITTLE KNOWN

These attacks have numerous and costly repercussions in the short and long term:

- Loss of business income during service interrupts;
- Loss of data, in particular personal data;
- Impacts in terms of image on the company or organization and the security of its services;
- Loss of user confidence.

To date, registry lock services such as .Fr Lock are highly effective tools in countering this type of risk. Indeed, by locking the domain at the registry level, they prevent any operation or update that may affect the resolution of a domain without the knowledge of its owner, such as registrar or holder changes, or updates of name servers.

In the case of .Fr Lock, to modify the data of a domain name, the registrar must make a request to Afnic to unlock it.The unlock request is validated after an authentication and verification process carried out by Afnic. The process may also involve the holders if they have agreed to this with the registrar.

In its Best Practices Guide for the Acquisition and Use of Domain Names, the French National Agency for the Security of Information Systems (ANSSI) recommends **«selecting a register offering a registry-level lock service and obtaining contractual assurances or commitments on the level of service guaranteed for the feature».**

We launched the .Fr Lock product at the beginning of 2015 and nearly two and a half years after commissioning it, we have found that although the examples of attacks of this type are growing and the risks are numerous, the .Fr Lock system is still too little used.

Here are some statistics on the adoption and use of the service.

REGISTRARS OFFERING THE SERVICE

Of the more than 400 accredited Afnic registrars, 20 registrars have signed the service-specific contract in order to offer it to their customers.

DOMAIN NAMES LOCKED

Less than a hundred domain names are now locked by .Fr Lock. Most of them correspond to the websites of large companies, e-commerce platforms, information sites or institutional sites.

What are the obstacles?

/ *At the level of domain name holders*

Holders have a low perception of the risks

The risks are mainly perceived as being Denial of Service attacks, DDOS, which often make the headlines in the press. To date, attacks related to domain name hijacking, which are more technical, are less well known. However, if a domain name is hijacked, the consequences are just as dramatic.

A balance to be found between resilience and agility

Among some ISDs, locking systems can be perceived as not offering sufficient flexibility and agility. Their main fear is being incapable of performing an update operation quickly in case of a problem, since the ISDs must first contact their registrar and ask them to temporarily unlock the domain.

Afnic registrars having signed the .Fr Lock contract in order to offer the service to their customers

COM LAUDE / CSC / DOMAINE.FR / DOMAINOO / GANDI / HOGAN LOVELLS / LEXSYNERGY LIMITED / MARKMONITOR / MEYER & PARTENAIRES / NAMEBAY / NAMESHIELD / NORDNET / ONLINE / ORANGE / ORDIPAT / OXYD / PHPNET / PORTS GROUP / SAFEBRANDS / SFR

/ *At the level of Registrars*

A long sale cycle

Registrars who offer this service to their customers must first set it up in their own system, which implies the development of specific procedures at two levels. The first procedure has to be set up between the registry and the registrar. In the case of .Fr Lock, for example, reference contacts must be designated and trained in the standard procedure with the registry. The procedure must then be applied between the registrar and the domain name holder, while ensuring that the customer's expectations are met, with particular respect to availability and reactivity issues for the reasons mentioned above.

A "multi-lock" approach

Many registrars would like to offer their customers a multi-lock service, i.e. the ability to lock a domain name with multiple suffixes in order to provide optimal protection for their portfolio. Setting up such a service is all the lengthier in that registry procedures are not standardized.

In order to overcome these obstacles, we are at every registrar's disposal in order to assist them in setting up such a service and help them raise their customers' awareness. We also regularly collect their feedback in order to upgrade the service and make it easier to use while maintaining its level of security. Our objective is to equip the top 100 of the most popular sites under the .fr TLD by 2018!

/// INTERVIEW WITH **NAMESHIELD**, AN AFNIC REGISTRAR WHICH OFFERS THE .FR LOCK SERVICE TO ITS CUSTOMERS.

Afnic: Are your customers aware of the risks of domain name hijacking?

— *Nameshield:* Up until now, our various contacts within companies, whether they are SMEs or large accounts, don't consider a domain name as a major factor requiring protection. It was only when several companies of national and even international scale had been the victims of various types of attacks affecting the resolution of the domain, and when these major incidents had been relayed by the media, that our customers started paying greater attention to our attempts to raise their awareness. Businesses are more concerned about site hosting issues than domain names and the DNS. A change is slowly taking place on the subject however. Some of our contacts do not necessarily make the connection between the DNS, web hosting servers, and mail servers.

Afnic: How do you raise their awareness about the issue?

— *Nameshield*: A lot of our work involves familiarizing customers about the subject, based on changes in Internet uses, the strategic value of their digital assets such as domain names and the financial consequences in the event of failure of the system in place. We systematically repeat the use of detailed presentations and illustrated with diagrams, the real work of the DNS and exchanges between Internet users, registrars, registries, etc.

Afnic: Is there a typical profile for an .Fr Lock customer, such as the sector of activity, size of the company, etc.?

— *Nameshield*: No, there is no typical profile; it really depends on the awareness of the individual about the consequences that hijacking of technical resources can cause. Owners of domain names believe it is the responsibility of the registrar or the registry to ensure that they work properly. Domain names continue to be the Cinderella of the Internet when they are the gateway to a multitude of services.

Afnic: In your opinion, what levers could be used to promote the adoption of locking systems by companies, institutions, etc.?

— *Nameshield*: Communication by the State authorities on a larger scale could be used to raise awareness based on practical case studies. At the registry level, DNS resolution needs to be conditioned by the installation of the registry lock. Lobbying with the supervisory authorities of large companies, such as the French Financial Markets Regulator (AMF), is needed so that companies are required to use DNSSEC or the registry lock.

When creating a domain name, Afnic could also send each owner an e-mail to raise their awareness about the need to use locking systems. If the registrar does that, customers would see it as part of a commercial operation on the registrar's behalf

USEFUL INFORMATION

To contact Afnic

Afnic
Immeuble Le Stephenson
1, rue Stephenson
78180 Montigny-Le-Bretonneux
France
www.afnic.fr

Tél. : +33(0)1 39 30 83 00

@AFNIC

support@afnic.fr

mastodon.social/@afnic

afnic.fr

About Afnic

Afnic (the French Network Information Centre) comprises public and private stakeholders, including government authorities, users, and Internet service providers (Registrars). It is a non-profit organisation.

Afnic is the French Registry for the .fr (France), .re (Reunion Island), .yt (Mayotte), .wf (Wallis and Futuna), .tf (French Southern Territories), .pm (Saint-Pierre and Miquelon).

Afnic is also positioned as a provider of technical solutions and services for registries and registrars.