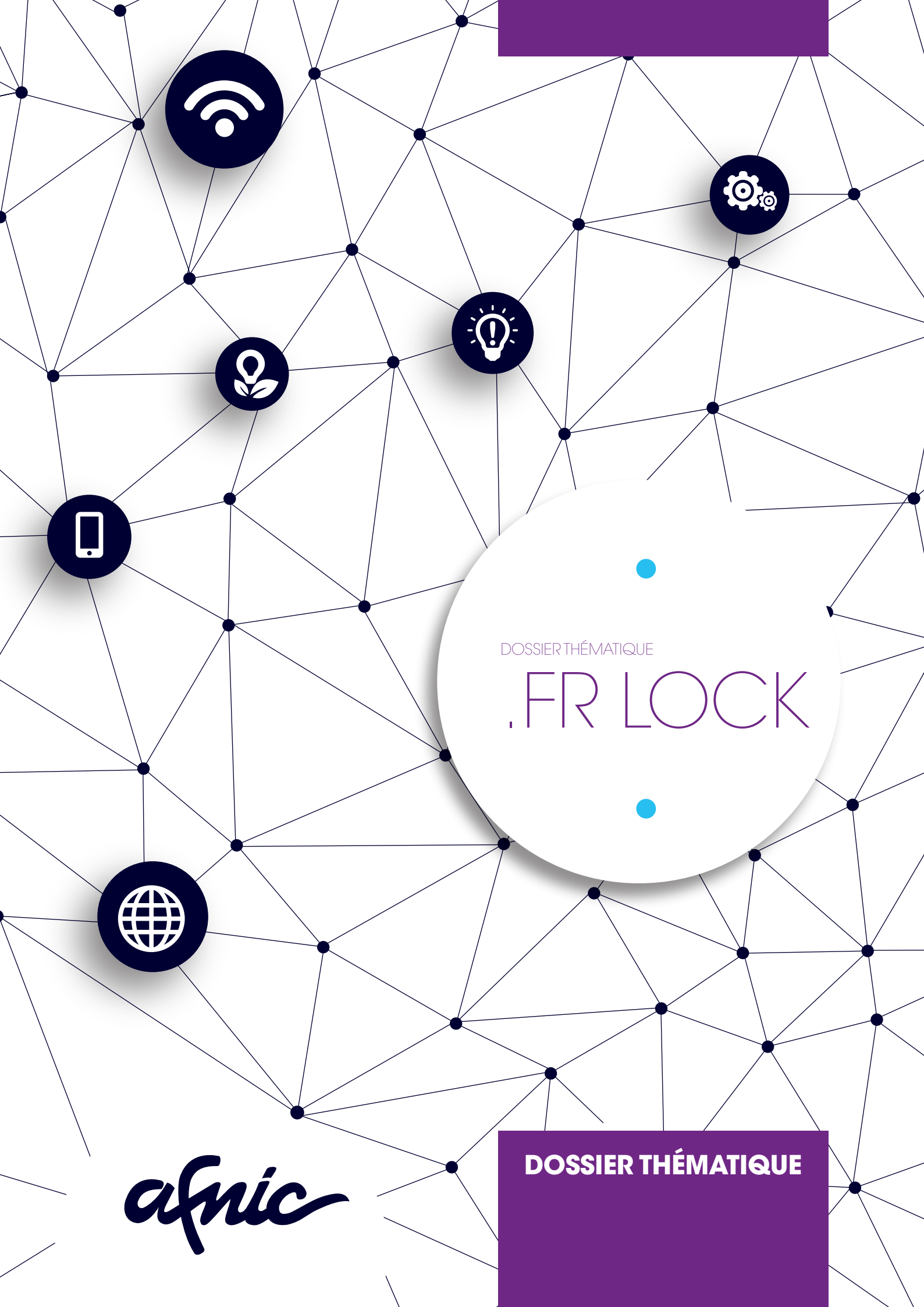


DOSSIER THÉMATIQUE

.FR LOCK

afnic

DOSSIER THÉMATIQUE

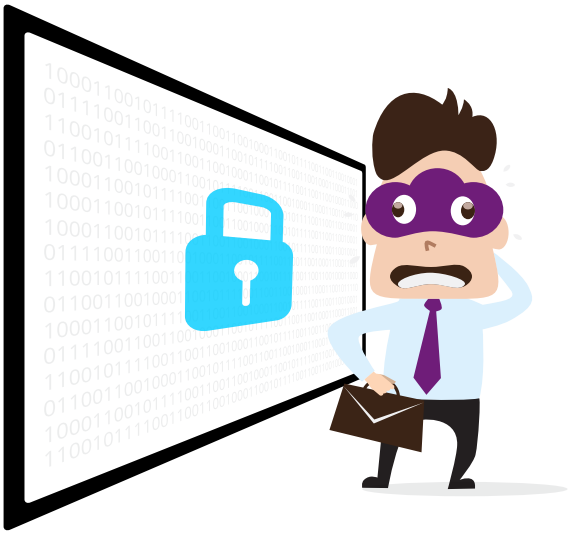
En 2015, l'Afnic lançait .Fr Lock, un service de verrouillage (registry lock) destiné à sécuriser les noms de domaine les plus sensibles contre les cyberattaques liées à des détournements de noms de domaine. Ce dossier thématique dresse un panorama de ce type d'attaque et fait un 1er bilan après deux ans de mise en service.

/// PANORAMA DES CYBERATTAQUES LIÉES À DES DÉTOURNEMENTS DE NOMS DE DOMAINE

Parmi les menaces qui pèsent sur les noms de domaine, le risque de détournement est celui qui a motivé l'existence de services de verrouillage des noms.

Un détournement (« hijacking ») est une attaque où l'assaillant parvient à prendre le contrôle du nom de domaine, lui permettant d'y mettre les données de son choix (par exemple l'adresse IP d'un site internet qu'il contrôle).

Cette attaque ne met pas du tout en jeu le protocole DNS, elle se fait uniquement via le système d'enregistrement des noms. Ce système d'enregistrement étant composé de plusieurs acteurs, l'attaque peut viser l'un de ces acteurs. Dans le cas le plus fréquent, il y a le registre, le bureau d'enregistrement et l'hébergeur DNS (qui est souvent le bureau d'enregistrement, mais qui peut aussi être le titulaire lui-même, ou bien un tiers).
Voici quelques exemples de détournements faits ces dernières années. Chacun d'eux a fait l'objet d'une étude bien que toutes les informations ne soient pas disponibles publiquement.



Exemple d'attaque CONTRE UN REGISTRE

En décembre 2016, le registre du .bd (Bangladesh) a été piraté. L'attaquant a modifié les serveurs de nom de google.com.bd renvoyant ainsi les utilisateurs bangladais de Google vers un site internet qu'il contrôlait.
Dans un tel cas, les solutions techniques mises en œuvre par le registre ne suffisent pas. La seule protection est la sécurité du registre.

Exemples d'attaques CONTRE UN BUREAU D'ENREGISTREMENT

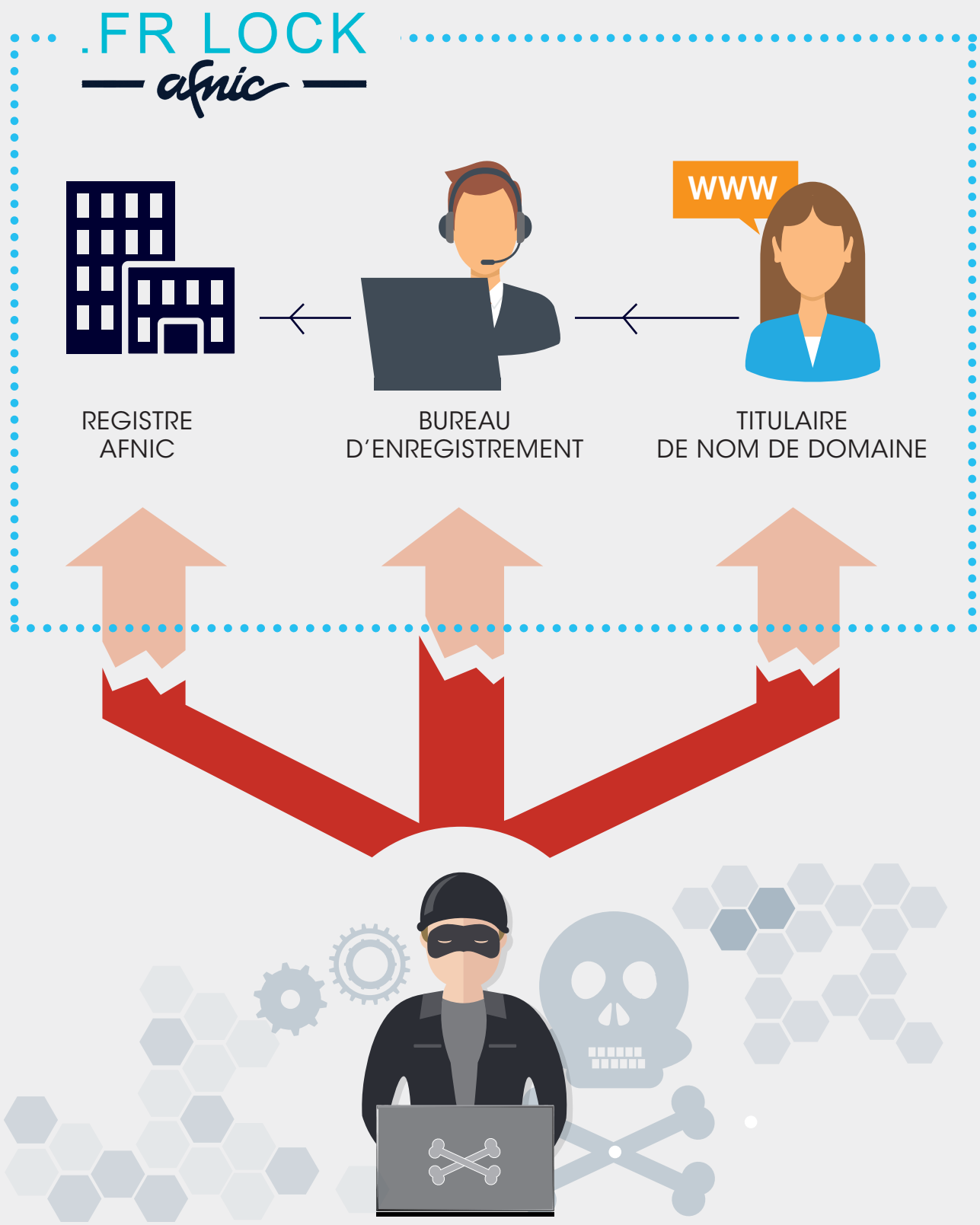
En avril 2015, le bureau d'enregistrement eNom est apparemment piraté. L'attaquant peut rediriger une banque, stlouisfed.org, vers un site qu'il contrôle. Cette attaque n'aurait pas été possible si le domaine avait été verrouillé.
Ainsi, en août 2013, lors du piratage du bureau d'enregistrement MelbourneIT par un groupe politique, le domaine nytimes.com, non verrouillé, avait été détourné, alors que le domaine twitter.com tout aussi intéressant et situé sur le même bureau d'enregistrement, mais étant verrouillé, n'avait pas pu être détourné.
Autre exemple, en février 2015, l'entreprise Lenovo (suite à l'installation du logiciel malveillant Superfish sur les PC de ses clients) a vu son domaine lenovo.com détourné. Au moins un autre domaine sur le même bureau d'enregistrement ayant été détourné par le même groupe, on peut en déduire que l'attaque portait sur le bureau d'enregistrement.

Exemple d'attaque CONTRE L'HÉBERGEMENT DNS

En décembre 2014, l'opérateur de télécommunications émirati Etisalat a vu son domaine détourné. En termes techniques, les serveurs de noms (« enregistrements NS ») n'ont pas changé mais l'adresse IP annoncée a été modifiée. Apparemment, l'hébergeur n'avait pas été piraté mais le compte d'Etisalat auprès de cet hébergeur l'était. Notez qu'il est difficile de distinguer un piratage du bureau d'enregistrement d'un piratage du seul compte d'un client. Ici, seul ce domaine avait été détourné, faisant plutôt penser au piratage d'un compte unique.

Conclusion

Le détournement de noms de domaine existe, et ces quelques exemples ne représentent que la partie émergée de l'iceberg : en l'absence d'un système de surveillance public des changements des noms de domaine, il ne fait pas de doute que bien des détournements passent relativement inaperçus. Il est donc crucial de prendre des précautions pour éviter les détournements. Les personnes qui, dans une organisation, gèrent les noms de domaine, doivent être compétentes en sécurité informatique et sensibilisés à ses enjeux.
D'autre part, il faut aussi se prémunir contre des problèmes de sécurité survenant chez des prestataires. C'est pour ces raisons que le verrouillage de registre de noms de domaine (registry lock) est utile.


.FR LOCK
afnic
WWW
REGISTRE
AFNIC
BUREAU
D'ENREGISTREMENT
TITULAIRE
DE NOM DE DOMAINE

/// .FR LOCK, UN REMPART EFFICACE MAIS ENCORE TROP PEU CONNU CONTRE CE TYPE D'ATTAQUES

Ces attaques ont des répercussions nombreuses et coûteuses à court et long terme :

- Perte de revenus d'activité pendant l'interruption de service ;
- Perte de données, notamment de données personnelles ;
- Impacts d'image sur l'entreprise ou l'organisme et la sécurité de ses services ;
- Perte de confiance des utilisateurs.

À ce jour, les services de registry lock comme .Fr Lock sont des outils très efficaces pour se prémunir contre ce type de risques. En effet, en verrouillant le domaine au niveau du registre, ils empêchent toutes les opérations et les mises à jour pouvant affecter la résolution d'un domaine à l'insu de son propriétaire, comme les changements de bureau d'enregistrement et de titulaire ou la mise à jour des serveurs de noms.

Pour modifier les données d'un nom de domaine, le bureau d'enregistrement doit faire une demande de déverrouillage auprès de l'Afnic. Cette demande est validée après un processus d'authentification et de vérification manuel effectué par l'Afnic. Ce processus peut également faire intervenir le titulaire s'il s'est mis d'accord avec son bureau d'enregistrement.

Dans son Guide des bonnes pratiques pour l'acquisition et l'exploitation de noms de domaine, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) recommande d'ailleurs de **« choisir un registre offrant un service de verrou de niveau registre et obtenir des assurances ou des engagements contractuels sur le niveau de service garanti pour cette fonctionnalité ».**

Nous avons lancé le produit .Fr Lock début 2015 et, après presque 2 ans et demi de mise en service, nous constatons que si les exemples d'attaques de ce type s'accumulent et que les risques sont nombreux, les verrous .Fr Lock sont encore trop peu utilisés.

Voici quelques statistiques d'adoption et d'utilisation du service.

BUREAUX D'ENREGISTREMENT PROPOSANT LE SERVICE

Sur les plus de 400 bureaux d'enregistrement accrédités Afnic, 20 bureaux d'enregistrement ont signé le contrat spécifique au service pour le proposer à leurs clients.

NOMS DE DOMAINE VERROUILLÉS

Moins d'une centaine de noms sont aujourd'hui verrouillés par le .Fr Lock. Il s'agit pour la plupart de sites de grandes entreprises, de plateformes de e-commerce, de sites d'information ou de sites institutionnels.

Quels sont les freins identifiés ?

/ *Au niveau des titulaires de noms de domaine*

Une faible perception des risques par les titulaires

La perception du risque est surtout concentrée sur les attaques par déni de service, DDOS, qui font souvent les unes de la presse. À ce jour, les attaques liées à des détournements de noms de domaine, plus techniques, sont moins connues. Pourtant, en cas de détournement d'un nom de domaine, les conséquences sont tout aussi dramatiques.

Un équilibre à trouver entre résilience et agilité

Dans certaines DSI, ce type de mécanisme peut être perçu comme n'offrant pas assez de souplesse et d'agilité. La crainte principale est de ne pouvoir effectuer une opération de mise à jour rapidement en cas de problème, le DSI devant d'abord contacter son bureau d'enregistrement pour lui demander de déverrouiller temporairement le domaine.

Bureaux d'enregistrement Afnic ayant signé le contrat .Fr Lock pour proposer le service à leurs clients

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

/ *Au niveau des bureaux d'enregistrement*

Un cycle de vente long

Les bureaux d'enregistrement qui proposent ce service à leurs clients doivent en premier lieu le mettre en place chez eux, ce qui suppose l'élaboration de procédures spécifiques à deux niveaux. La première est à mettre en place entre le registre et le bureau d'enregistrement. Dans le cas du .Fr Lock par exemple, il faut désigner des contacts de référence et les former à la procédure type avec le registre. Il faut ensuite décliner cette procédure entre le bureau d'enregistrement et le titulaire du nom de domaine, tout en s'assurant de répondre aux attentes des clients, notamment sur les aspects de disponibilité et réactivité pour les raisons évoquées ci-dessus.

Une approche « multi-lock »

De nombreux bureaux d'enregistrement souhaiteraient proposer à leurs clients un service multi-lock, c'est-à-dire la possibilité de verrouiller un nom de domaine dans plusieurs extensions pour offrir une protection optimale de leur portefeuille. La mise en place d'un tel service est d'autant plus longue que les procédures des registres ne sont pas uniformisées.

Pour lever ces barrières, nous nous tenons à disposition des bureaux d'enregistrement afin de les accompagner au mieux dans la mise en place d'un tel service et les aider à sensibiliser leurs clients. Nous récoltons également leurs retours régulièrement pour faire évoluer le service et le rendre plus facile d'utilisation tout en conservant son niveau de sécurité. Objectif, avoir équipé le top 100 des sites en .fr les plus populaires d'ici 2018 !

/// INTERVIEW DE **NAMESHIELD**, BUREAU D'ENREGISTREMENT AFNIC QUI PROPOSE LE SERVICE .FR LOCK À SES CLIENTS.

Afnic : Vos clients sont-ils informés des risques de détournement de noms de domaine ?

— *Nameshield* : Jusqu'à présent nos différents contacts au sein des entreprises, qu'il s'agisse de PME ou de grands comptes, ne considéraient pas le nom de domaine comme un élément majeur à protéger.

Il a fallu que plusieurs entreprises, d'envergure nationale voire internationale, soient les victimes d'attaques diverses affectant la résolution du domaine, et que ces incidents majeurs soient relayés par les médias, pour que notre sensibilisation trouve une meilleure écoute. Les entreprises se préoccupent davantage des problèmes liés à l'hébergement de sites que du nom de domaine et du DNS.

Il y a cependant une lente évolution sur ce sujet. Certains interlocuteurs ne font pas nécessairement le lien entre les DNS, les serveurs d'hébergement des sites web et les serveurs de messagerie.

Afnic : Comment les sensibilisez-vous sur le sujet ?

— *Nameshield* : Nous faisons beaucoup d'évangélisation en nous appuyant sur les évolutions de l'usage d'internet, sur le côté stratégique de leurs actifs numériques que sont les noms de domaine et des conséquences financières en cas de défaillance du système en place. Nous sommes contraints de reprendre systématiquement des présentations détaillées et d'illustrer par des schémas, l'action réelle du DNS et les échanges entre internautes, registrar, registre etc...

Afnic : Y-a-t-il un profil type de client .Fr Lock : secteur d'activité, taille, etc. ?

— *Nameshield* : Non, il n'y a pas de profil type, c'est vraiment la sensibilité de l'individu face aux conséquences que peut avoir un détournement des ressources techniques qui fait agir. Les propriétaires de noms de domaine pensent que c'est de la responsabilité du bureau d'enregistrement ou du registre que d'en assurer le bon fonctionnement. Le nom de domaine reste le parent pauvre de l'internet alors qu'il est la porte d'entrée vers une multitude de services.

Afnic : Quels seraient selon vous les leviers pour développer l'adoption de tels verrous par des entreprises, institutions, etc. ?

— *Nameshield* : Une communication de la part des autorités d'État à plus grande échelle pour sensibiliser et présenter des cas pratiques. Il faudrait conditionner la résolution DNS au niveau du registre par la mise en place du registry lock. Un lobbying auprès des autorités de tutelle des grandes entreprises, de type l'AMF pour les marchés financiers, serait nécessaire afin qu'elles exigent la mise en place de DNSSEC ou du registry lock.

Lors de la création d'un nom de domaine, l'Afnic pourrait, par exemple, transmettre à chaque propriétaire un e-mail pour le sensibiliser. Si cette action est faite au niveau du bureau d'enregistrement, elle sera considérée comme commerciale.

RENSEIGNEMENTS UTILES

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

À propos de l'Afnic :

L'**Afnic** - Association Française pour le Nommage Internet en Coopération - est composée d'acteurs publics et privés : représentants des pouvoirs publics, utilisateurs et prestataires de services Internet (bureaux d'enregistrement). Elle est à but non lucratif.

L'**Afnic** est le registre des noms de domaine .fr (France), .re (Île de la Réunion), .yt (Mayotte), .wf (Wallis et Futuna), .tf (Terres Australes et Antarctiques), .pm (Saint-Pierre et Miquelon).

L'**Afnic** se positionne également comme fournisseurs de solutions techniques et de services de registre.