Libroscope, plus que des logiciels libres, des hommes libres !

-- Actualité --

Actualité

Verisign sur le point de perdre son autorisation à enregistrer des noms de domaines.

Quand votre valeur est basée sur la confiance, faites attention à votre réputation !

Julien Tayon
lundi 9 septembre 2002

En juin 2002, *Verisign* était en procès pour avoir utilisé des techniques déloyales afin de débaucher des clients faisant appel à une autre société qu'elle pour gérer leurs noms de domaines [1].

Aujourd'hui, elle est -pour une raison non liée- menacée de se voir retirer son autorité à délivrer des noms de domaines. Voici la suite de l'histoire, qui illustre notre série sur la *valeur de la confiance*.

L'article n'a pas pour but de paraphraser ce qui a été écrit ailleurs, mais de vous apporter des éléments nécessaires à la compréhension de la situation et de ses enjeux. J'ai essayé de m'exprimer dans un langage le moins technique possible et je répondrai volontiers à toute demande d'éclaircissements.

Historique

Nous vous décrivions dans nos colonnes le procès qui a eu lieu en juin aux États-Unis, le règlement à l'amiable qui avait suivi, et enfin notre analyse de la situation.

l'article précédent

La situation actuelle

Article dans les colonnes de CNET La nouvelles sur ZDNET L'analyse de Homo Numericus

Les enjeux

Cette fois-ci, l'autorité régulatrice en question n'est pas un tribunal mais l'ICANN, une autorité de régulation informelle mondiale pour l'attribution des noms de domaines. Le différend porte sur le non-remplissage de la base **whois** [2] [3].

La base whois

La base **whois** permet d'accéder aux informations sur les personnes responsables du domaine notamment :
- l'adresse,
- le numéro de téléphone,
- et l'e-mail.

Ces informations sont importantes : elles permettent de connaitre l'identité des responsables *réels* d'un domaine sur Internet. En effet, TCP/IP (la couche réseau d'Internet) est conçue dans l'optique d'une utilisation loyale par tous les utilisateurs des ressources informatiques, et de partage de l'information. TCP/IP n'as pas été conçue dans une optique de traçage systématique des connexions ; elle est basée sur l'idée que la meilleure façon de régler et d'éviter les problèmes est de dialoguer. En un mot elle permet de dialoguer.

La sécurité, le réglement de différent dû à l'utilisation abusive de ressource se base sur la responsabilité des détenteurs d'un nom de domaine. La responsabilité est déléguée de sous-domaine en sous-domaine, afin que tout détenteur d'un domaine de machines visibles sur

Internet puisse être averti que :
- son domaine est piraté,
- un de ses serveurs est mal configuré,
- il est tenu responsable d'acte délibéré de piraterie.
- il existe une violation de la propriété intellectuelle sur du contenu d'un de ses serveurs,
- il a un trou de sécurité qui compromet son domaine.

Ceci peut aussi être utile pour retrouver un administreur indélicat dans le cas du cybersquattage [4].

Internet est il virtuel ?

Contrairement à la croyance, Internet n'est pas un espace virtuel, mais il le devient à force d'être considéré et utilisé comme tel. Quand vous téléphonez, la personne n'est pas plus présente auprès de vous qu'un interlocuteur à qui vous envoyez un e-mail. Pourtant, vous êtes sûrement plus rassuré(e) à l'idée de faire une transaction avec votre banquier par téléphone que de le faire par e-mail. La grande différence avec les télécommunications est la confiance que vous avez dans les sociétés qui constituent l'ensemble du réseau téléphonique. Vous avez confiance dans le fait que l'appel est bien dirigé vers la bonne personne [5], et qu'il n'y a pas de possibilité de manipulation. Pourtant, ce sont des ordinateurs qui effectuent automatiquement les tâches de connexion sur Internet comme dans le réseau téléphonique. Dans les deux cas ils sont supervisés par des hommes aussi faillibles dans les deux cas.

La valeur de la confiance

La différence entre es deux réseaux tient à une chose : comme dans le cadre des banques, vous avez confiance dans les sociétés qui gèrent les domaines (France Telecom, Cegetel et Bouygues Telecom en France, Sprint et ATT&T Bellsouth aux États-Unis, par exemple). Vous les pensez loyales et responsables juridiquement de leurs éventuels mauvais comportements. Sur Internet, on peut comparer chaque domaine à autant de compagnies téléphoniques. Mais certaines sont injoignales, car les informations d'enregistrement ne sont pas toujours remplies correctement (pour vous en convaincre regardez les enregistrements relatifs au domaine sexisfun.com). Il est ainsi difficile d'engager la responsabilité des personnes ou de les contacter pour régler les différends.

De plus, la multiplication des grands domaines (contenant 65535 adresses par exemple) gérés par une seule entité est plus problématique, comme les FAI [6], par exemple, qui sous-louent des plages à des particuliers. Il est facile d'avoir une idée de ce qui est fait dans un lieu unique (une université ou une entreprise), mais il est beaucoup plus difficile de connaître les abus commis par un client parmi des milliers.

Je ne suis pas un numéro, je suis un Homme libre - Le prisonnier

Il existe un doute sur l'identité de votre interlocuteur tant que tout responsable de domaine n'est pas identifiable et ne peut donc apporter son crédit à la réalité physique de l'interlocuteur. Quand identifier et contacter les personnes responsables d'un domaine d'où viennent des abus répétés de ressources Internet n'est pas possible, nous assistons à l'émergence d'une solution malheureuse et perverse : les listes noires (*black lists*). Perverse, car ces listes noires n'ont pas toujours comme seul objectif d'aider les internautes :
- elles peuvent aussi servir des intérêts politiques (Google est interdit d'accès depuis la Chine),
- ou économiques (empêcher un petit fournisseur d'accès à Internet d'échanger des données avec

les abonnés d'un gros réseau sous prétexte de sécurité est assez efficace pour le contrer).

On peut parler de **balkanisation** car les listes noires diminuent la connectivité entre les personnes sur Internet, et lui fait perdre son intérêt : partager l'information.

Le maillon faible

En conclusion, l'ICANN reproche à Verisign d'être une société à laquelle on ne peut faire confiance. Dans la RFC 1591, nous trouvons ce qui est attendu de sociétés comme *Verisign* :

"These designated authorities are trustees for the delegated domain, and have a duty to serve the community." *Les autorités désignées sont des tiers de confiance pour les domaines délégués et ont un devoir de servir la communauté*.

La sécurité sur Internet est basée sur la confiance :
- la certitude de pouvoir trouver des personnes responsables et aptes à remplir leurs fonctions,
- autant que sur la possibilité de dialoguer avec eux.

La confiance est une chaîne dans laquelle aucun maillon faible ne peut être toléré. La défense de *Vérisign* est de dire que 17 incidents en 18 mois pour 30000 domaines gérés est marginal. Le problème est que :
- 17 erreurs sont intolérables surtout quand la société sus-nommée refuse de les corriger,
- et il est certain que ce chiffre ne représente que les incidents ayant été rapportés à l'ICANN, et est très largement en dessous de la réalité des faits [7].

Ironiquement, le slogan de Verisign est *la valeur de la confiance*. Et ils ont raison, la confiance est une denrée trop précieuse pour être confiée à n'importe qui.

Il est à noter que la faillite du système de délégation de confiance permet de justifier les logiques de rétention des traces de connexion des utilisateurs, ainsi que le filtrage des données dans la lutte contre la cybercriminalité. Pour connaître les dérives sécuritaires, lire :

Rapport sur l'évolution de la vie privée dans le monde par l'EPIC

Légitimité et légalité

Le côté intéressant de l'histoire est qu'une autorité **supranationale informelle** réussit à menacer une société commerciale de manière crédible. Comment est-ce possible ?

Au départ, le logiciel libre est un peu le coeur d'Internet [8]

Je vous conseille, pour mieux comprendre la relation Internet/logiciel libre, de lire cet ouvrage en ligne :

http://www.oreilly.fr/divers/tribun...

Sur Internet, la régulation et les acteurs sont, comme dans le logiciel libre, issus d'autorités informelles qui tiennent leur pouvoir de la légitimité. Il est intéressant de s'apercevoir que les entreprises habituées à ne traiter qu'avec des interlocuteurs légaux se sentent à même de traiter et menacées par une autorité auto-déclarée comme gouvernement d'Internet dont l'existence légale et le domaine de compétence sont a priori enterrinés par aucune loi. La confiance accordée à cette communauté n'est liée :
- ni à sa territorialité,
- ni à ses garanties juridiques ou financières puisqu'elle est informelle.

En revanche elle est liée a son inscription dans un anneau de réputation [9]. Dans cette communauté, les personnes sont identifiables et connues, ce qui assure que les gens vont respecter le contrat dans leur intérêt à conserver leur réputation : c'est leur richesse à titre personnel. Il est donc faiblement envisageable que la personne trahisse un jour [10].

En ce qui concerne Verisign, cela reste l'exemple d'une entreprise qui a basé sa valeur sur la confiance comme un slogan et non comme une stratégie. À ce titre, si vous avez un certificat de sécurité hébergé chez eux, posez-vous les questions suivantes :
- puis-je leur faire confiance ?
- ont-ils vérifié de manière stricte mon identité *réelle* (envoi de courrier non électronique, demande d'extraîts officiels, coup de téléphone) ?
- s'ils ne l'ont pas fait pour moi, auraient-ils pu émettre un certificat de sécurité à mon nom qui pourrait être utilisé à mon insu pour faire du commerce électronique ?

NB ne faites pas confiance non plus à votre fureteur :

trou de sécurité dans IE concernant les certificats de sécurité

Annexes

Normes concernant le sujet

Les normes qui ont cours sur Internet, appelées RFC, sont disponibles sur le site suivant , elles sont éditées par l'IETF.

Numéro Description 2352 Légitimité et légalité dans le domaine de de l'attribution de noms de doamine (cybersquattage) 2345 Convention sur la gestion de nom de domaine pour améliorer l'efficacité de la gestion des informations sur les entreprises 1834 Description des contenus obligatoires et optionnels d'une base whois 1591 Administration et déléguation de la gestion de noms de domaines 1034 Nom de domaine : historique et définitions

L'ICANN lieu de gouvernance utopique ?

L'ICANN n'a rien d'une utopie d'une part, et d'autre part est agité régulièrement de problèmes liés à son fonctionement peu démocratique. En effet, lors des dernières élections, le mandat du candidat allemand [11] élu a été annulé. Les États-Unis sont soupçonnés de vouloir faire main-basse sur cet organisme pour récupérer le pouvoir de réguler Internet. La réalité est peut-être différente : n'oubliez pas de voter pour les prochaines élections de l'ICANN. L'information circulera sur Internet, notamment sur notre site.

Du rififi à l'ICANN L'ICANN, un nouveau mode de gouvernance intelligent ou une manipulation ? Un rapport de prospective sur la démocratie et l'ICANN Interview du candidat Allemand dont l'élection a été annulée sur *La Vie du Net*

Merci à Raphael Rousseau pour ses corrections, et sa relecture.

[1] Les noms de domaines sont intialement gérés par l'ICANN http://www.icann.org/general/abouti.... Cette association a pour co-président Vinton G. Cerf http://www.icann.org/biog/cerf.htm, l'un des hommes à l'origine de la création d'Internet. La mission de l'ICANN est de gérer les noms de domaines. Ceux-ci sont découpés en zones (*.fr*, *.com*, *.net*, *.eu* ...) dont la gestion est conjointement ou exclusivement déléguée à des organisations tierces. L'AFNIC http://www.nic.fr/ est par exemple la seule organisation autorisée à délivrer des noms de domaines en *.fr*. La gestion des noms de domaines est décrite par la RFC 1034

[2] Contenu attendu d'une base whois voir http://www.ietf.org/rfc/rfc1834

[3] Sur Unix la commande *whois* vous permet d'accéder à la base du même nom. La commande pour connaître le détenteur d'un nom de domaine est ainsi *whois example.com*.

Vous pouvez également trouver les mêmes informations via des interfaces comme celle du registrar GANDI : http://www.gandi.net/whois ?l=FR&dom...

[4] Utilisation non légitime d'un nom de domaine

[5] ...et aussi que vous ne recevrez pas de coup de téléphone intempestif si vous le désirez. Cela s'appelle la *liste rouge* pour le téléphone. Pour les e-mails, malheureusement, nous devons faire face aux courriers commerciaux non sollicités (spam) qui coûteraient plusieurs milliards de dollars en coûts de connexion aux internautes par an, mais cela ppourrait faire l'objet d'un autre article

[6] Fournisseurs d'Accès à Internet

[7] Il s'agit certainement de la partie émergée de l'iceberg.

[8] Quelques données à l'appui :
- Deux tiers des serveurs de pages web du monde tournent sur des serveurs Apache,
- la quasi-totalité des serveurs de noms de domaine de haut niveau (tels que *.fr*, *.com*, *.edu* ...) utilisent le logiciel Bind
- la moitié des courriers électroniques sont transférés à l'aide du serveur Sendmail.

En fait, la plupart des infrastructures (invisibles à l'utilisateur) qui soutiennent Internet sont basées sur des solutions logicielles

libres. Ce n'est pas vraiment un hasard, vu que qu'Internet a été développé dans un environnement universitaire dans lequel le partage de l'information et des logiciels est assez naturel.

[9] Un anneau de confiance a pour finalité de pouvoir certifier l'identité réelle de ses participants, et non de s'assurer de la confiance que l'on peut accorder à une personne.

[10] Voir David Kreps in *Perspectives on Positive Political Economy, chapter Corporate Culture and Economic Theory.* Cambridge University Press, 1990.

[11] Ancien membre du CCC