Le problème du serveur whois du .mobi

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 12 septembre 2024

https://www.bortzmeyer.org/whois-mobi.html

Des chercheurs en sécurité ont publié un article <https://labs.watchtowr.com/we-spent-20-to-achieve-r> sur un problème causé par le serveur whois du TLD .mobi. Le problème est réel et le travail des chercheurs excellent, mais je souhaiterais ajouter quelques points.

D'abord, les faits : beaucoup de TLD (notamment la totalité de ceux qui sont sous contrat avec l'ICANN, au moins jusqu'en janvier 2025) ont un serveur whois, pour permettre d'obtenir des informations sur le titulaire et les contacts des noms de domaine. Ce protocole, whois, est normalisé dans le RFC 3912 [1]. C'est un protocole très simple, voire simpliste, qui présente de nombreuses limites (on reparlera plus loin de son ou ses successeurs). Notamment, il n'existe pas de mécanisme normalisé pour découvrir le serveur pertinent pour un nom de domaine donné. Chaque logiciel client whois développe donc ses propres heuristiques. Par exemple, GNU whois <https://github.com/rfc1036/whois>, qui est probablement celui que vous trouverez sur une machine Debian ou Fedora, utilise une liste de TLD et de leurs serveurs, qui est « en dur » dans le programme mais peut être surpassée par un fichier de configuration, /etc/whois.conf. D'autres clients whois utilisent d'autres méthodes pour récupérer une information analogue. Notons qu'il existe beaucoup de clients whois et, contrairement à ce qu'écrivent parfois les ignorants, ils ne sont pas forcément en ligne de commande. (Sinon, pour les TLD, la source faisant autorité est la base IANA des TLD <https://www.iana.org/domains/root/db>.) Vous voyez bien le problème : cette liste de TLD et de leurs serveurs évolue et le logiciel peut avoir une liste dépassée. Comme beaucoup d'utilisateurices et d'administrateurices système ne tiennent pas à jour leurs logiciels et les configurations, le risque d'avoir une vieille information sur les serveurs whois est non négligeable.

Et c'est justement ce qu'ont constaté Benjamin Harris et Aliz Hammond <https://labs.watchtowr.com/we-spent-20-to-achieve-rce-and-accidentally-became-the-admins-of-mobi/>, les chercheurs en sécurité dont je parlais. Constatant que le TLD .mobi (TLD qui est par ailleurs une mauvaise idée <https://www.w3.org/2004/07/dotmobi_diwg.html>, mais c'est une autre histoire) avait changé son serveur whois, de whois.dotmobiregistry.net à whois.nic.mobi, **et** que

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc3912.txt

le nom de domaine dotmobiregistry.net, non renouvelé, avait expiré et était donc libre, les chercheurs ont enregistré le nom dotmobiregistry.net, mis en place un serveur whois (je rappelle que le protocole est très simple et que n'importe quel·le étudiant·e peut programmer un serveur whois en un quart d'heure) et récolté d'innombrables requêtes provenant de clients whois qui n'avaient pas mis leur base à jour.

Les chercheurs ont ensuite creusé **qui** envoyait ces requêtes à un serveur qui normalement n'existait plus. Sans surprise, une bonne partie provenait de relais, de passerelles entre Web et whois. Comme certains utilisateurs de whois n'ont pas de client whois sur leur machine, ils passent par des passerelles dont rien ne garantit l'honnêteté, l'intégrité…ou la tenue à jour de leur liste. C'est ainsi que who.is ou whois.ru allaient visiter le serveur whois « pirate ». (Je découvre à cette occasion qu'il y a apparemment des gens qui sont dans la cybersécurité et qui, au lieu de contacter le serveur whois faisant autorité, se servent de whois.ru. Des gens qui sont dans la cybersécurité…) Donc, un rappel : on ne doit pas utiliser ces passerelles mais toujours interroger directement un serveur qui fait autorité <https://www.afnic.fr/observatoire-ressources/papier-expert/trouver-les-informations-sociales-asso
>.

Mieux (ou pire), parmi les clients qui contactaient le serveur « pirate » se trouvaient des AC ! Pour découvrir les adresses de courrier électronique des contacts, ces « Autorités » de « Certification » (la liste figure dans l'article) utilisaient une information plus à jour…Cela a de quoi faire réfléchir sur la valeur ajoutée de ces AC en sécurité.

Au passage, le fait d'enregistrer un domaine qui est libre, mais toujours référencé quelque part, pour capter du trafic, souvent à des fins malveillantes, est nommé une attaque flamant (l'oiseau, pas la région de la Belgique dont le nom des habitants se termine par un D, pas un T). C'est une catégorie d'attaques qu'on retrouve de temps en temps. Pour s'en prémunir, faites attention avant de supprimer un domaine <https://www.itforbusiness.fr/que-faire-dun-nom-de-domaine-dont-on-na-plus-besoin-868
dont vous croyez qu'il ne sert plus. (Vous êtes sûr·e ? Vous avez vérifié tous les endroits en dehors de vos machines où ce nom est cité ?)

L'article des chercheurs ne le mentionne pas mais, si on veut faire les choses proprement, on ne doit plus utiliser whois mais son successeur RDAP (RFC 9082 et RFC 9083) qui a notamment l'avantage d'avoir un mécanisme standard de découverte du serveur (spécifié dans le RFC 9224), qui évite ces listes codées en dur, trop susceptibles d'erreurs, comme l'a bien montré l'affaire du .mobi. Bref, la solution technique existe depuis de nombreuses années, mais on sait qu'il est difficile de faire abandonner une vieille technique mauvaise pour une moderne qui marche ; whois s'accroche.

(Pour les programmeureuses : un exemple de script Python pour trouver le serveur RDAP est disponible en ligne <https://gitlab.rd.nic.fr/afnic/code-samples/-/tree/main/RDAP/Python>. Il est documenté dans un article sur RDAP <https://www.afnic.fr/observatoire-ressources/papier-expert/rdap-obtenir-des-informations-sur-un-nom-de-domaine/>.)

Sinon, Ars Technica a fait un article résumant l'affaire <https://arstechnica.com/security/2024/09/rogue-whois-server-gives-researcher-superpowers-no-one-should-ever-have/>. L'article est bien mais reste purement factuel et ne met pas assez en perspective.
