Attaques récentes contre les noms de domaine, que se passe-t-il ?

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 25 février 2019

https://www.bortzmeyer.org/attaques-noms-domaine-explications.html

---

Le week-end des 23 et 24 février a vu beaucoup d'articles dans les médias à propos d'une campagne d'attaques Internet menées via les noms de domaine. Que s'est-il passé ?

Cet article se veut pédagogique et prévu pour des gens qui ne sont pas des experts en noms de domaine. (Les experts qui veulent plein de détails techniques devront lire un autre article <https://www.bortzmeyer.org/dnspionage.html>.)

Donc, commençons par un avertissement : la cybersécurité est un domaine compliqué, et qui n'est pas facile à résumer et à vulgariser. Je vais être obligé de simplifier (rappelez-vous que cet article n'est pas pour les experts) tout en restant rigoureux. Il n'est pas possible de résumer ce qu'on sait de ces attaques discutées récemment en un seul paragraphe. Et tout n'a pas encore été découvert, il est possible que des investigations ultérieures nuancent, voire annulent, ce que j'écris ici. D'autre part, un point important de la cybersécurité est que tout n'est pas public, loin de là. Il y a des tas de choses que je ne sais pas, et d'autres dont je ne peux pas forcément parler. Comme le dit l'adage, « ceux qui savent ne parlent pas, ceux qui parlent ne savent pas ». Donc, prudence.

Commençons par les certitudes : au dernier trimestre de l'année 2018, plusieurs attaques informatiques ont eu lieu, en utilisant des méthodes similaires, et visant notamment des objectifs gouvernementaux. On voit déjà qu'il ne s'agit pas du tout d'une attaque en cours, qui aurait commencé le 22 ou le 23 février, mais d'un problème déjà passé. Ces attaques avaient en commun le détournement des noms de domaine. Avant de continuer, il faut donc s'arrêter sur les noms de domaine et sur leur utilité.

Un nom de domaine est un identificateur pour un service ou une machine sur l'Internet. Il se présente sous la forme de chaînes de caractères séparées par des points. Par exemple, `www.bortzmeyer.org` est un nom de domaine, tout comme `brexit.gouv.fr` ou `réussir-en.fr`. Des informations techniques, utiles uniquement pour les machines, sont associées à ces noms. Ces informations sont cruciales pour faire en sorte que vous, utilisateur ordinaire de l'Internet, arriviez bien au bon endroit. Par exemple, si votre banque est accessible en ligne et que vous utilisez le nom de domaine `client.mabanque.example`,

votre ordinateur ou ordiphone va obtenir, en échange de ce nom, les informations dont il a besoin pour se connecter au site Web de la banque. (Il s'agit entre autres de l'adresse IP.) Si, par malheur, ces informations étaient incorrectes, vous n'arriveriez pas sur le site de votre banque mais sur un autre.

Et c'est précisement le cœur de l'attaque qui a fait tant de bruit depuis quelques jours : les pirates informatiques ont réussi à prendre le contrôle d'un certain nombre de noms de domaine, et à y associer d'autres informations techniques. Ainsi, les utilisateurs, croyant se connecter à tel ou tel service, allaient en fait sur un autre. Lorsque le service est un site Web, l'attaquant copiait le site Web original, faisait quelques modifications, et le plaçait sur le serveur qu'il contrôlait. Une telle attaque n'a pas d'équivalent dans le monde physique. Si vous voulez vous rendre à la Tour Eiffel et qu'on vous donne une mauvaise adresse pour ce monument, vous vous rendrez bien compte que vous n'êtes pas au bon endroit. (Des lecteurs érudits de ce blog me font remarquer qu'une attaque très similaire est pourtant montrée dans le film Ocean 11 ou dans la série "*The Blacklist*".) Mais, sur l'Internet, vous ne voyez pas la distance (vous ne savez pas facilement si vous vous connectez à un site Web situé au Maroc ou au Japon) et vous ne voyez pas du premier coup que le site a été copié.

Et il n'y a pas que le Web. Les attaquants avaient également détourné des serveurs de messagerie, ce qui est encore plus facile, car l'utilisateur ne « voit » pas le serveur de messagerie, connexion et échange de messages se font de manière automatique.

Avec le détournement de sites Web, l'attaquant peut capter des informations confidentielles, comme le mot de passe, qu'il pourra ensuite utiliser avec le vrai site Web. Avec le détournement d'un serveur de messagerie, l'attaquant pourra capter du courrier, possiblement confidentiel (rappelez-vous que les attaquants en question visaient surtout des noms de domaine de gouvernements).

Par exemple, l'un des noms de domaine détournés était `webmail.finance.gov.lb`. C'est l'interface Web du service de courrier électronique au ministère des finances libanais (`.lb` indique le Liban). Il est normalement connecté par l'opérateur libanais TerraNet. Le 6 novembre 2018 (et peut-être davantage), en essayant de se connecter via ce nom de domaine, on arrivait chez l'hébergeur ukrainien DeltaHost. L'utilisateur qui ne se méfiait pas entrait donc le mot de passe de son compte sur un serveur contrôlé par le pirate.

La force de ce type d'attaques particulier est son caractère **indirect**. Au lieu de pirater le site Web, ou le serveur de messagerie, probablement bien défendus, l'attaquant pirate les informations qui indiquent comment s'y rendre. La gestion des noms de domaine est souvent le **maillon faible** de la cybersécurité. Les attaquants appartenant à ce groupe de pirates particulier n'ont pourtant pas innové. Ils n'ont trouvé aucune faille de sécurité nouvelle, ils n'ont pas réalisé une percée technologique. Ils n'ont même pas été les premiers à comprendre l'intérêt des attaques indirectes, via le nom de domaine. Un exemple fameux d'une telle attaque avait été le détournement du nom de domaine du New York Times <`https://www.bortzmeyer.org/attaques-sea.html`> en 2013. Mais ces attaquants de 2018 ont attaqué un grand nombre de noms de domaine.

Bon, mais si c'est si facile, pourquoi est-ce que tout le monde ne le fait pas ? Pourquoi est-ce que je ne détourne pas le nom de domaine du RN pour pointer vers un site Web servant un contenu antiraciste ? Bon, d'abord, c'est parce que je suis un citoyen respectueux des lois. Mais il n'y a pas que ça. Pour comprendre, voyons comment fonctionne la gestion de noms de domaine, vue, par exemple, du webmestre. Je vais reprendre un exemple utilisé dans mon livre <`https://cyberstructure.fr/`> : « suivons M. Michu, pizzaiolo, qui habite à Soissons et gère un restaurant nommé "Au soleil de Soissons". Il n'a pas de compétence spéciale en informatique mais voudrait un site Web pour sa pizzeria. Il va alors contacter une entreprise locale, mettons "Aisne Web", qui réalise des sites Web. Aisne Web réserve le nom de domaine `au-soleil-de-soissons.fr` auprès d'un bureau d'enregistrement, qui sert également d'hébergeur des serveurs de noms de domaine. Aisne Web indiquera, via une interface

---

`https://www.bortzmeyer.org/attaques-noms-domaine-explications.html`

Web, l'adresse IP du serveur Web hébergeant le site et réalisera le contenu qui apparaitra sous forme de pages Web. Dès qu'Aisne Web aura terminé ce site Web, les visiteurs pourront alors se connecter à `au-soleil-de-soissons.fr`. »

Mais supposons qu'Aisne Web ne soit pas une entreprise très attentive en matière de sécurité. Pour s'authentifier auprès du bureau d'enregistrement de noms de domaine, ils ont choisi le mot de passe « toto12345 ». Un tel mot de passe est facile à deviner, surtout pour un logiciel qui peut faire de nombreux essais sans s'en fatiguer. Même avec un mot de passe plus difficile, peut-être qu'un employé d'Aisne Web est crédule et que, quand quelqu'un prétendant être « un technicien de Microsoft » (ou d'Apple, ou d'Orange…) appelera, l'employé acceptera de communiquer le mot de passe. (C'est ce qu'on nomme l'ingénierie sociale et c'est beaucoup plus efficace qu'on ne le croit.)

Une fois le mot de passe connu, le pirate peut alors se connecter à l'interface Web du bureau d'enregistrement, **en se faisant ainsi passer pour l'utilisateur légitime**. Il va alors modifier les informations techniques, par exemple l'adresse IP du site Web. Et voilà, en croyant se connecter à la pizzeria, les visiteurs iront sur le site du pirate. Bien sûr, pour une pizzeria, ce n'est pas forcément très grave. Mais des noms de domaine bien plus sensibles peuvent être détournés ainsi. Et ces attaques forment un véritable bruit de fond sur l'Internet. Les attaques comme celles perpétrées dans l'affaire qui fait du bruit en ce moment ne sont ni les premières, ni les seules.

Comme souvent en sécurité, il n'y a pas de solution magique unique et simple à ce problème, et à ces vulnérabilités. Ce n'est pas spécifique à la cybersécurité. Pour d'autres questions de sécurité, on voudrait aussi une solution immédiate et qui résolve tout, et les politiciens sont particulièrement rapides à passer à la télé, après un fait divers, pour réclamer de telles solutions magiques. Mais la sécurité ne marche pas comme cela. Elle nécessite des efforts sur le long terme, faits avec sérieux et constance. Par exemple, un tout premier élément serait de choisir des mots de passe forts (difficiles à deviner) et de ne pas les communiquer à quelqu'un à la voix chaleureuse et qui inspire confiance. Ces mesures simples et peu spectaculaires, l'**hygiène numérique**, empêcheraient déjà un certain nombre d'attaques.

Comme dit plus haut, on ne sait pas tout sur cette campagne d'attaques. Il y a beaucoup d'incertitudes. Par exemple, quand les détournements ont-ils commencé ? En octobre 2018 ou avant ? Les attaquants ont-ils renoncé après la publication, de novembre 2018 à février 2019, de plusieurs articles détaillant leurs opérations ? Nous ne le savons pas.

Et il y a bien sûr la question de l'**attribution**. Qui a effectué ces attaques ? Beaucoup des objectifs étaient au Moyen-Orient, ce qui fait qu'on peut spéculer que l'attaquant était impliqué dans un conflit du Moyen-Orient (je ne dis pas **le** conflit du Moyen-Orient, car il y en a plusieurs, parfois entremêlés). Mais ça fait beaucoup de suspects. La lecture de la BD « Cyberfatale » <`https://www.bortzmeyer.org/cyberfatale.html`> vous donnera une idée de la difficulté de l'attribution des cyberattaques…

Enfin, si vous vous intéressez aux questions de la cybersécurité, je vous encourage à lire le livre « La face cachée d'Internet » <`https://www.bortzmeyer.org/face-cachee-internet.html`>.

`https://www.bortzmeyer.org/attaques-noms-domaine-explications.html`