Nom de domaine, attention danger

Au cœur de l'organisation et de l'identité de la marque, les noms de domaine font l'objet de cyber-attaques. Les protéger est un impératif, comme le souligne le rapport de MarkMonitor, leader mondial de la protection de marque.

Entretien avec Stéphane Berlot*

Votre dernier rapport[1] souligne que près d'un quart des marques ont vu leur nom de domaine ciblé par des cybercriminels. Cette proportion a-t-elle augmenté sur la longue durée ?

Stéphane Berlot : Oui, parce que les menaces sont de plus en plus fortes et que les marques représentent plus que jamais une importante valeur immatérielle dans le compte de résultat des entreprises. L'étude révèle également que 62 % des marques ont déclaré que les cyber-crimes ont eu des répercussions sur leur entreprise l'année dernière. Près de la moitié de l'échantillon (48 %) pense que les violations de marque ont augmenté au cours de l'année précédente. 46 % déclare que les cyber-menaces et le *cybersquatting* des noms de domaine ont influencé leur stratégie de développement de nom de domaine. Le rapport souligne également que la responsabilité de la gestion et de la sécurité des noms de domaine est cloisonnée et que les départements suivants sont souvent seuls responsables de leur gestion : informatique ou sécurité informatique (46 %), juridique (16 %), marketing (13 %). Seulement 13 % des marques ont adopté une approche combinée, pourtant la meilleure pratique de l'industrie quant à l'atténuation de risque. 56 % des entreprises identifient la sécurité comme leur principale faille.

** Responsable des ventes de la filiale France et Benelux de MarkMonitor*
1 - markmonitor.com/protectionlifecycle.

> Hier, on pouvait connaître les fraudeurs. Aujourd'hui, avec le RGDP, leur impunité est totale. Il est interdit de donner des informations sur le propriétaire d'un nom de domaine.

Auprès de quel échantillon avez-vous réalisé votre étude ?

S. B. : L'étude commandée par MarkMonitor a été conduite par la société de sondage Vitreous World auprès d'un échantillon le plus large possible de 700 décideurs dans les noms de domaine du marketing, de l'informatique et du droit, en France, au Royaume-Uni, aux États-Unis, en Allemagne et en Italie. Ceci afin de comprendre les attitudes et les pratiques en matière de gestion des noms de domaine, de sécurité et de protection globale des marques en ligne. Les entretiens ont été réalisés en ligne en avril 2019.

Depuis quand les noms de domaine sont-ils ciblés et pour quelles raisons ?

S. B. : Depuis qu'ils existent ! Grâce à leur nom de domaine, les marques peuvent communiquer sur Internet, promouvoir leur image. Aujourd'hui, toutes les marques sont convoitées par les fraudeurs, qui peuvent ainsi détourner à leur profit des trafics de clients, bien sûr à leur insu. Ils utilisent la notoriété des marques et usurpent leur identité. Ils utilisent le *phishing* pour récupérer des informations comme des coordonnées bancaires, abusant ainsi les clients. D'autres fraudeurs peuvent selon la méthode du *cybersquatting* créer des noms de domaine proches de ceux des marques. L'internaute va vite, ne fait pas attention et se fait prendre au piège...

Quelles sont les marques et secteurs les plus touchés ?

S. B. : On ne peut pas dire qu'il y ait une marque plus touchée que les autres, même si une entreprise peu connue sera nécessairement moins ciblée qu'une entreprise réputée : c'est la rançon du succès qui est la cause des cyber-attaques. 32 % des entreprises de notre échantillon ont été victimes d'usurpation d'identité et d'abus de marque. Mentionnons cependant que les premières marques à avoir été attaquées œuvrent dans les domaines pharmaceutique – car à l'exception de la France, les produits sont chers et mal remboursés –, et du luxe – en raison de la notoriété des marques –, rendant ce trafic très lucratif. Aujourd'hui, n'importe qui peut enregistrer un nom de domaine faisant mention d'un nom de marque connu. Les fraudeurs – qui font du parasitisme de marque – enregistrent ainsi de nombreux noms de domaine, ce qui peut les amener à engranger des profits conséquents grâce aux liens publicitaires des domaines parking ou au détournement de trafic...

Les pratiques en matière de gestion des noms de domaine varient-elles selon les pays étudiés dans votre rapport ?

S. B. : Elles sont identiques dans la mesure où les sociétés touchées sont toutes internationales.

Quelle stratégie de protection recommandez-vous qui dépasse la simple gestion des noms de domaine ?

S. B : Les entreprises ne peuvent pas tout prévoir, tout imaginer. Il leur est recommandé de déposer des noms de domaine dans tous les pays où elles exercent. Cependant, l'enregistrement coûte cher, ce qui limite le nombre de dépôts. Il leur faut trouver un juste équilibre entre l'enregistrement de certains noms de domaine indispensables et la surveillance des noms de domaine enregistrés par des cyber-squatteurs. Il faut donc disposer de solutions de surveillance des noms de domaine et des sites Web. Les fraudeurs ont de plus en plus d'imagination et nous sommes en présence d'un puits sans fond.

Les marques sont-elles plus ou moins vigilantes quant au renouvellement de leur nom de domaine ?

S. B. : Bien que l'importance des noms de domaine soit largement reconnue – 43 % de notre échantillon en convient : ils jouent un rôle essentiel dans la construction et le maintien de la confiance des clients envers la marque –, de nombreuses entreprises n'anticipent pas suffisamment leur gestion et leur sécurisation. C'est particulièrement vrai en ce qui concerne le processus de renouvellement : 26 % des marques s'appuient uniquement sur les avis de renouvellement, 21 % sur une seule personne pour gérer le processus, tandis que 25 % ont un plan qui implique une collaboration interdépartementale. Les systèmes d'auto-renouvellement mis en place par les bureaux d'enregistrement évitent le risque d'oubli.

Le fait de posséder beaucoup de noms de domaine inactifs est-il pertinent ? Quelles raisons donner à cette boulimie ?

S. B. : 56 % des répondants possèdent jusqu'à 100 noms de domaine, mais seulement 18 % disent que plus des trois quarts d'entre eux sont actifs. De fait, cette boulimie n'est gère pertinente. Pour gagner en pertinence, l'entreprise

doit se poser trois questions : que faut-il enregistrer ? jusqu'où aller ? dans quelle limite budgétaire ? Cette profusion de noms de domaine inactifs a souvent un but défensif : les fraudeurs déposant des noms de domaine inimaginables, d'où la nécessité de se défendre. Il est néanmoins utile de faire une revue des noms de domaine utiles ou non au moins une fois par an, pour éviter un accroissement superflu de son portefeuille.

En quoi le RGPD affecte-t-il la stratégie de nom de domaine ?

S. B. : Hier, on pouvait connaître les fraudeurs. Aujourd'hui, avec le RGPD, leur impunité est totale. Avant, quand on enregistrait un nom de domaine, on recevait la carte d'identité du nom de domaine, le « *who is?* », à savoir le nom du bureau d'enregistrement, le registrant, la marque... Avec le RGPD et la protection des données, le « *who is?* » a disparu. Il est interdit de donner des informations sur le propriétaire d'un nom de domaine. N'importe qui peut enregistrer un nom de domaine en toute impunité, personne ne saura qui est derrière et on ne pourra plus attaquer si c'est un fraudeur. Ce sera en tout cas long et compliqué de le débusquer. Près de la moitié des répondants (46 %) ont déclaré que le RGPD affectait leur stratégie de nom de domaine et 18 % ont déclaré qu'il leur était plus difficile de faire respecter la loi en cas de violation.

> On ne peut pas dire qu'il y ait une marque plus touchée que les autres, même si une entreprise peu connue sera nécessairement moins ciblée qu'une entreprise réputée.

Quels sont les défis de demain ?

S. B. : Aujourd'hui, les défis les plus cités dans la gestion des noms de domaine incluent la sécurité (56 %), les coûts (40 %), le suivi des noms de domaine (34 %), la connaissance des noms de domaine à enregistrer (22 %), l'optimisation des portefeuilles de noms de domaine (21 %). Demain, il faudra convaincre l'ICANN (Internet Corporation for Assigned Names and Numbers) de lever l'anonymat du fraudeur pour pouvoir se défendre. ■