Le DNS, ce protocole oublié qui n'aurait jamais dû l'être

Évidemment, le trafic web est vital, tant pour la sécurité (car c'est par là que commencent bon nombre d'incidents) que pour les performances (le ressenti des utilisateurs, internes comme externe, vis-à-vis des applications métiers ou de commerce électronique peut avoir un impact significatif sur l'activité ou la productivité).

Mais quel autre protocole permet au trafic web de fonctionner ? Le DNS, bien sûr ! Paradoxalement, il est pourtant l'un des protocoles les moins supervisés de tous. Bien souvent, tout ce qui compte c'est que la résolution de noms se fasse correctement, peu importe qui s'en charge (et parfois même, en combien de temps !).

Ainsi dans le grand public, rares sont les internautes qui sauraient dire qui assure leur résolution de noms (réponse : leur FAI par défaut, le plus souvent). Et plus rares encore sont ceux qui ont pris la peine de souscrire à un service DNSdédié. Et dans les entreprises ? C'est malheureusement souvent à peu près pareil…

Pourtant l'impact d'un trafic DNS mal maîtrisé et non supervisé peut se faire sentir aussi bien en termes de performances que de sécurité.

Améliorer les performances

Beaucoup d'entreprises internationales s'appuient sur un DNS central pour leur résolution de noms, plutôt que des DNS locaux. Cela facilite notamment la résolution des noms internes sans avoir à gérer une multitude de serveurs locaux. Malheureusement, cette configuration fait que lorsque les collaborateurs demandent des ressources servies par un réseau de distribution de contenu (un CDN, pour *Content Delivery Network*), ils seront dirigés vers le point de présence le plus proche du siège de leur entreprise, et pas forcément de là où ils se trouvent réellement. Cela peut conduire à une dégradation des performances, notamment en ce qui concerne la téléphonie sur IP ou la visioconférence (c'est d'ailleurs mentionné par Microsoft dans la documentation officielle de Skype).

Pour répondre à ces besoins, il est nécessaire de pouvoir réécrire la résolution de nom en fonction de la localisation géographique réelle de l'utilisateur – ce qui est beaucoup plus simple à faire dans le Cloud qu'avec une multitude de serveurs DNSlocaux à gérer.

… et la sécurité !

Le rôle absolument essentiel du DNS dans la sécurité de l'entreprise n'est plus à démontrer. C'est par le DNS que les collaborateurs sont dirigés vers les sites web qu'ils demandent, et donc pour un attaquant, contrôler le DNS, c'est pouvoir mener des attaques de type phishing parfaites et à

grande échelle, en usurpant aussi bien des destinations externes (sur le web) que des applications internes.

Pour s'en protéger, il peut être utile de déployer des technologies telles que DNSSEC (la signature des enregistrements DNS pour certifier les données servies) ou DNS-over-TLS (le chiffrement du trafic DNS afin de préserver la confidentialité des requêtes). Mais c'est rarement mis en œuvre, car ces approches introduisent un peu plus de complexité dans un système simple qui fonctionne tout seul depuis longtemps : on ne préfère donc pas y toucher…

Et puis il n'y a pas que la menace du phishing ! Le DNS peut être détourné de bien d'autres manières encore. Par exemple, de plus en plus de malwares utilisent leDNS pour exfiltrer des données (dans des champs TXT) en profitant du fait que ce protocole est rarement inspecté, et encore moins filtré.

D'ailleurs selon une étude menée par la société Efficient IP, en 2018 91 % des malwares s'appuyaient sur une résolution DNS pour contacter leur serveur de commandes & contrôle. Et pourtant, seulement 38 % des entreprises considèrent la protection de leur DNS comme une priorité.

Et pour ajouter encore à la confusion, certains antivirus eux-mêmes exploitent la technique de DNS tunneling pour assurer leurs mises à jour de base de signatures même s'ils sont bloqués par un pare-feu. Il peut devenir difficile, dans ces conditions, de faire la distinction entre le trafic légitime et celui initié par un code malveillant.

Il est donc urgent pour les entreprises de se pencher sur la sécurité de leurs serveurs DNS et de commencer à inspecter ces flux. Elles pourraient y découvrir des surprises ! Hélas, une telle inspection n'est pas triviale, et il peut être avantageux d'y appliquer des techniques d'apprentissage machine appuyée sur un gros volume de requêtes afin de détecter les anomalies qui pourraient passer sous le radar. Là aussi, le Cloud est un outil essentiel pour mener ce type d'analyses.

En fait, maintenant que les entreprises ont bien pris soin de leur trafic Web, il est temps de se faire la même chose pour leur DNS. Et pour cela, les atouts du Cloud qui ont fait son succès dans la protection du trafic web (centralisation, capacités d'analyse quasi infinie, abstraction de l'infrastructure locale) sont tout aussi applicables.