Protégez votre organisation contre les attaques par déni de service

Un article écrit par les experts de TELUS

Une attaque par déni de service est sans contredit un des types de cyberattaques les plus visibles auxquels votre organisation peut être confrontée. Ces attaques peuvent toucher directement votre présence sur le Web, puisqu'elles compromettent l'accès de vos clients à vos sites Web et à vos applications mobiles. Même si la plupart des organisations ne diffusent pas d'information sur les attaques qu'elles ont subies, il existe tout de même plusieurs cas bien documentés.

Ce mois-ci, une vaste attaque par déni de service a touché de nombreux services en ligne. Dyn, un important service d'hébergement DNS, a fait l'objet d'une attaque qui a eu une incidence importante sur de nombreuses organisations qui utilisent ses services.

Un déluge de trafic malveillant

Pour illustrer ce qu'est une attaque par déni de service, imaginons une ville frappée par un gros orage. Normalement, le système d'évacuation des eaux peut prendre en charge le volume d'eau qui s'écoule lorsque les citoyens arrosent leur pelouse, lavent leur voiture et rincent leur terrasse. Des collecteurs d'eaux pluviales sont installés un peu partout pour recueillir cette eau et l'acheminer vers la mer. Lorsqu'un orage frappe, l'accumulation d'eau forte et soudaine dépasse la capacité des collecteurs d'eau, causant ainsi des inondations.

C'est un peu la même chose sur Internet. Lorsqu'un grand nombre d'appareils reliés à Internet génèrent un flot de trafic malveillant dirigé vers une organisation, la passerelle vers les services Internet ou les applications Web de celle-ci est submergée, entraînant des pannes de service et perturbant ses activités. C'est ce qu'on appelle une attaque par déni de service.

Incidence des attaques par déni de service sur votre organisation

La protection des organisations contre les menaces à la cybersécurité est un problème de plus en plus complexe parce que la variété et le type de menaces évoluent constamment. Une attaque par déni de service vise le canal qui relie votre organisation au monde extérieur. Ainsi, l'idéal est de contrer ces attaques à l'extérieur de votre réseau, avant qu'elles n'atteignent votre pare-feu ou votre système de détection des intrusions.

Ces attaques se produisent régulièrement et peuvent frapper votre organisation sans prévenir. Pour voir en temps réel de telles attaques se produisant en ce moment même dans le monde, consultez la carte Digital Attack Map de Google Ideas et Arbor Networks (en anglais).

Les attaques par déni de service touchent spécifiquement la présence d'une organisation sur le Web. Ce sont la capacité à effectuer des opérations en ligne et la réputation de celle-ci qui sont le plus souvent compromises. Les motifs les plus courants de ces attaques sont les suivants :

Extorsion : Certains groupes exigent des rançons des organisations en les menaçant de mener contre elles, si elles ne collaborent pas, des attaques par déni de service susceptibles de nuire à leur marque. Ces attaques sont souvent lancées durant des périodes critiques, comme le lancement d'un produit. Plus tôt cette année, First Securities a été victime d'une attaque par déni de service pour laquelle une rançon a été demandée (en anglais).

Politique : Des groupes comme Anonymous diffusent des messages politiques au moyen d'attaques par déni de service. Récemment, Anonymous a ciblé le gouvernement brésilien (en anglais) pour protester contre les Jeux olympiques de Rio.

Distraction : Il est de plus en plus courant de voir des attaques par déni de service s'inscrire dans le cadre d'une attaque plus vaste et plus élaborée. Pendant que le service de la sécurité informatique s'occupe d'une attaque aux répercussions graves et immédiates, une attaque est menée en parallèle contre un autre actif de grande valeur, par exemple, les données de l'entreprise.

Protéger votre organisation contre les attaques par déni de service

TELUS vous offre divers moyens de contrer les attaques par déni de service. Les ingénieurs de l'équipe Assurance du réseau veillent à la protection des organisations contre les points de vulnérabilité connus en exerçant une surveillance constante du réseau de TELUS et en y apportant les améliorations nécessaires. D'ailleurs, TELUS a lancé récemment un service visant à aider ses clients des services Internet d'affaires à contrer ce type d'attaque grâce à des centres de filtrage au sein du réseau TELUS. La protection contre les attaques par déni de service offerte à la clientèle d'affaires de TELUS est fondée sur les mêmes technologies, expertise et expérience que celles utilisées par TELUS pour protéger son propre réseau interne.