Les attaques DDoS ont augmenté de 151% au cours du premier semestre 2020

Neustar, Inc., société mondiale de services et de technologies de l'information, leader dans le domaine de la résolution d'identité, a publié aujourd'hui son dernier rapport sur les menaces et les tendances en matière de cybercriminalité, qui identifie des changements importants dans les modèles d'attaques par déni de service distribué (DDoS) au cours du premier semestre 2020. Le Centre des opérations de sécurité (SOC) de Neustar a constaté une augmentation de 151 % du nombre d'attaques par déni de service distribué par rapport à la même période en 2019. Parmi celles-ci, les attaques les plus importantes et les plus longues que Neustar ait jamais atténuées, avec 1,17 térabit par seconde (Tbps) et 5 jours et 18 heures respectivement. Ces chiffres sont représentatifs du nombre, du volume et de l'intensité croissants des cyberattaques de type réseau, à mesure que les organisations évoluent vers des opérations à distance et que la dépendance des travailleurs à l'égard d'Internet augmente.

Ce communiqué de presse contient des éléments multimédias. Voir le communiqué complet ici : https://www.businesswire.com/news/home/20200916005641/fr/

Figure 1: Percentage change in number of attacks by size category, 2020 vs. 2019 (Graphic: Business Wire)

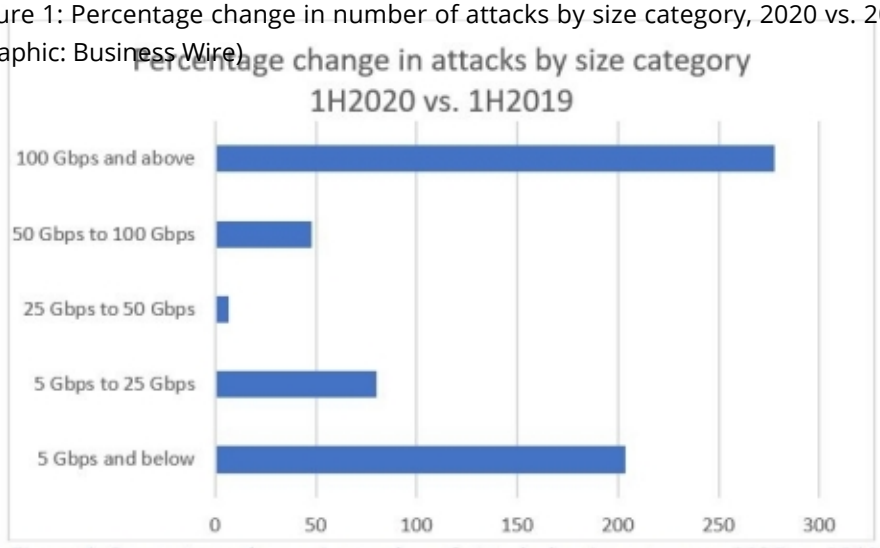

Figure 1: Percentage change in number of attacks by size category, 2020 vs. 2019

Le rôle de Neustar dans la navigation pour les requêtes Internet (via son réseau mondial UltraDNS) et dans la détection et l'atténuation des menaces (grâce à son service UltraDDoS Protect) a permis à l'entreprise d'être aux premières loges pour observer les tendances des macro-cyberattaques, comme le montre son rapport « CyberThreats and Trends Report: Jan-Jun 2020 ».

Les plus grandes comme les plus petites attaques DDoS deviennent de plus en plus intenses et sophistiquées

Les grandes attaques DDoS sont plus importantes, plus intenses et plus nombreuses que jamais. Les attaques de grande envergure ont connu un pic notable dans l'ensemble du secteur, notamment l'attaque de 2,3 Tbps visant un client d'Amazon Web Services en février – la plus grande attaque DDoS volumétrique jamais enregistrée.

Neustar a vu le nombre total d'attaques augmenter de plus de deux fois et demie entre janvier et

juin 2020 par rapport à la même période en 2019. L'augmentation a été ressentie dans toutes les catégories de taille, la plus forte croissance se produisant aux deux extrémités de l'échelle – le nombre d'attaques de 100 Gbps et plus a augmenté de 275% et le nombre d'attaques de très petite taille, de 5 Gbps et moins, a augmenté de plus de 200%. Dans l'ensemble, les petites attaques de 5 Gbps et moins ont représenté 70 % de toutes les attaques mitigées par Neustar entre janvier et juin 2020.

« Alors que les attaques volumétriques de grande envergure attirent l'attention et font les gros titres, les auteurs malveillants reconnaissent de plus en plus l'intérêt de frapper à un volume suffisamment faible pour contourner les seuils de trafic qui déclencheraient une atténuation pour dégrader les performances ou cibler avec précision les infrastructures vulnérables comme un VPN », a déclaré Michael Kaczmarek, vice-président des produits de sécurité chez Neustar. « Ces changements font courir à toute organisation ayant une présence sur Internet le risque d'une attaque DDoS – une menace particulièrement critique pour la main-d'œuvre mondiale qui dépend des VPN pour se connecter à distance. Les serveurs VPN sont souvent exposés, ce qui permet aux cybercriminels de mettre hors ligne toute une équipe en lançant une attaque DDoS ciblée ».

L'augmentation des petites attaques DDoS a été accompagnée d'une augmentation de la sophistication et de l'intensité des attaques. 52 % des menaces atténuées par Neustar ont utilisé trois vecteurs ou plus, le nombre d'attaques ne comportant qu'un seul vecteur étant pratiquement inexistant. Neustar a également suivi les nouvelles méthodes d'amplification et les attaques de plus grande intensité visant des éléments critiques de l'infrastructure web. Le précédent record de 500 millions de paquets par seconde (Mpps) a été dépassé cette année, avec une attaque de plus de 800 Mpps enregistrée.

« La dépendance et la croissance des communications en ligne depuis COVID-19 ont fondamentalement changé ce que les organisations doivent faire pour réussir », a déclaré Brian McCann, président de Neustar Security Solutions. « Il n'existe pas de solution unique pour la sécurité, mais le fait de disposer d'un service en nuage fiable qui assure la disponibilité et la sécurité de tous les services et utilisateurs s'est révélé être une différence essentielle entre le fait de survivre à peine ou de prospérer dans cet environnement en évolution rapide ».

Impact continu de la COVID-19 sur les cybermenaces et le trafic web de l'industrie

L'augmentation rapide des attaques DDoS reflète la croissance du trafic Internet observée pendant la pandémie. L'utilisation de l'internet a augmenté de 50 à 70 % et les médias en streaming de plus de 12 % au cours du premier trimestre 2020.Cela signifie que les agresseurs de tous types, qu'il s'agisse de cybercriminels sérieux ou d'adolescents ennuyés coincés à la maison, ont disposé de plus de temps d'écran pour perturber les activités.

Une étude sur l'un des plus grands sites de cybercriminalité réalisée par le Cambridge University's Cybercrime Centre a révélé que le nombre d'attaques lancées par le site web a fortement augmenté au début de la pandémie et du verrouillage qui en a découlé. Ils ont également constaté qu'au lieu que les cybercriminels existants organisent davantage d'attaques, ce sont les nouveaux attaquants qui sont à l'origine de l'augmentation des attaques DDoS.

Les attaques correspondantes, comme le trafic Internet, n'ont pas été réparties de manière égale

sur tous les sites web. Il est bien connu que les sites de commerce électronique et de jeux ont reçu beaucoup d'attention négative de la part des pirates, mais il y a d'autres secteurs qui ont été durement touchés par les cybercriminels au cours des six derniers mois. Les établissements de soins de santé contiennent des informations sensibles sur les patients et un nombre croissant de dispositifs IdO qui sont facilement exploitables. Conjugués à la pression supplémentaire de la pandémie, les hôpitaux sont devenus l'une des cibles les plus recherchées par les cybercriminels. Les industries qui ont connu une forte croissance pendant la pandémie, comme les jeux d'argent en ligne, sont également propices aux cybermenaces. La vidéo en ligne, notamment, a connu une augmentation incroyable de l'utilisation et des attaques DDoS. Omdia a rapporté 200 milliards d'heures supplémentaires de visionnage de Netflix ou d'appels vidéo Zoom par rapport aux prévisions initiales pour 2020.Là où le trafic augmente, les attaques augmentent aussi ; l'atténuation des attaques de Neustar pour ce secteur vertical a augmenté de 461 % au cours des six derniers mois.

« Alors que 2020 a apporté des changements radicaux dans le comportement des consommateurs et des criminels, il est naïf de supposer que les actions de l'un ou l'autre public reviendront complètement aux normes pré-pandémiques une fois la crise passée », a ajouté M. Kaczmarek. « L'atténuation de ces attaques DDoS de plus en plus sophistiquées continuera d'être un élément nécessaire pour faire des affaires en ligne. À une époque où de nombreuses organisations pourraient s'inquiéter moins, des services entièrement gérés peuvent alléger la pression et garantir la sécurité des biens numériques essentiels ».

Le rapport met en évidence plusieurs nouvelles tactiques d'attaque observées dans l'ensemble du secteur, notamment une augmentation des attaques DDoS par rafales et par impulsions, l'abus croissant des protocoles de réseau intégrés tels que ARMS, WS-DD, CoAP et Jenkins pour lancer des attaques par amplification DDoS qui peuvent être menées avec des ressources limitées et provoquer des perturbations importantes, les attaques NXNS visant les serveurs DNS, les attaques RangeAmp visant les réseaux de diffusion de contenu (CDN), et une résurgence de logiciels malveillants de type Marai capables de créer de vastes réseaux de zombies en exploitant des dispositifs IdO mal sécurisés.

Un exemplaire gratuit du rapport CyberThreats and Trends Report 1H 2020 de Neustar est disponible ici.

-FIN-

À propos de Neustar

Neustar est une entreprise de services et de technologies de l'information et un leader dans la résolution d'identité. Elle fournit les données et la technologie qui permettent d'établir des connexions de confiance entre les entreprises et les personnes au moment le plus important. Neustar propose des solutions de pointe dans les domaines du marketing, du risque, des communications et de la sécurité qui relient de manière responsable les données sur les personnes, les appareils et les lieux, corroborées en permanence par des milliards de transactions. Neustar compte plus de 8 000 clients dans le monde entier, dont 60 entreprises du Fortune 100. Découvrez ici comment votre entreprise peut bénéficier de la puissance des connexions de confiance : https://www.home.neustar.

# # #

Le texte du communiqué issu d’une traduction ne doit d’aucune manière être considéré comme officiel. La seule version du communiqué qui fasse foi est celle du communiqué dans sa langue d’origine. La traduction devra toujours être confrontée au texte source, qui fera jurisprudence.

Consultez la version source sur businesswire.com : https://www.businesswire.com/news/home/20200916005641/fr/