Le cap des 10 millions d'attaques DDoS franchi en 2020

Pour la première fois, les attaques DDoS franchissent le seuil annuel de 10 millions en 2020, soit près de 1,6 million d'attaques de plus qu'en 2019.

« Tous les records du monde ne méritent pas d'être célébrés - il suffit de regarder les chiffres des attaques par déni de service (DDoS) pour 2020. Pour la première fois de l'histoire, le nombre d'attaques DDoS enregistrées sur une année a franchi le seuil des 10 millions. ATLAS Security Engineering and Response Team (ASERT) de NETSCOUT a recensé 10 089 687 attaques au cours de l'année dont 3,71 millions en région EMEA. Cela représente près de 1,6 million d'attaques de plus qu'en 2019 (8,5 millions) au niveau mondial. Au niveau régional 598 000 attaques (contre 389 000 en 2019) concernaient le Royaume-Uni, 445 000 ont touché l'Allemagne (contre 162 000) et 178 000 (contre 137 000 en 2019) ont visé la France.

Il est vrai que les attaques DDoS ne progressent que dans un sens : à la hausse. Il est toutefois important de tenir compte du contexte lorsque l'on examine les statistiques sur les attaques DDoS en 2020. De mars à la fin de l'année, les auteurs d'attaques DDoS ont opéré en pleine pandémie de COVID-19. Tandis que la majeure partie du monde traversait une crise sanitaire mondiale sans précédent, les acteurs malveillants ont vu de nouvelles vulnérabilités et de nouvelles opportunités. Il est rare que l'activité annuelle soit aussi profondément affectée par un même événement, mais tel est pourtant le cas de l'activité et des tendances des attaques DDoS en 2020. Le fait que ce nombre important d'attaques mondiales soit atteint à un moment où les entreprises dépendent largement des services en ligne pour survivre n'est pas une coïncidence.

Le début du confinement lié à la pandémie a instauré une "nouvelle norme" dans notre façon de vivre et de travailler, provoquant un bouleversement majeur dans l'utilisation de l'internet, puisque les individus se sont de plus en plus tournés vers le monde en ligne. Lorsque les employés du monde entier se sont convertis au télétravail, les appareils et les dispositifs qui se trouvaient auparavant derrière les pares-feux et les environnements sécurisés des entreprises se sont retrouvés à la maison, derrière les routeurs et les dispositifs de réseau classiques des consommateurs. Les attaques ont rapidement exploité cette situation en multipliant par plus de deux le nombre d'échantillons de logiciels malveillants spécifiques à l'IoT circulant dans la nature, contribuant ainsi à la hausse des attaques DDoS en 2020.

Le nombre d'attaques DDoS, la largeur de bande et le débit ont tous fortement augmenté depuis le début de la pandémie de COVID-19.

Ainsi, la fréquence des attaques a progressé de 20 % en un an, mais ce chiffre englobe les mois précédant la crise sanitaire, à savoir janvier, février et la majeure partie de mars. Au cours du second semestre 2020, qui a été entièrement placé sous le signe de la pandémie, les attaques ont augmenté de 22 % par rapport à l'année précédente.

À mesure que les cybercriminels exploitaient rapidement les possibilités offertes par la pandémie, nous avons vu émerger un autre type de "nouvelle normalité". À partir de mars, les attaques DDoS mensuelles ont régulièrement dépassé les 800 000, alors que le confinement induit par la situation sanitaire entrait en vigueur. En effet, comme indiqué dans le rapport "Threat Intelligence Report" de

NETSCOUT pour le premier semestre 2020, les cybercriminels ont lancé 929 000 attaques DDoS en mai, soit le nombre d'attaques mensuelles le plus élevé jamais enregistré. Si les fournisseurs de services à large bande câblés et sans fil ont été les plus touchés par les attaques, les secteurs vitaux dans le contexte de la pandémie, tels que le commerce électronique, l'apprentissage en ligne et les soins de santé, ont tous fait l'objet d'une attention accrue de la part des acteurs malveillants. L'ASERT a ainsi réalisé un examen semestriel des réseaux d'éducation mondiaux pour analyser l'activité DDoS et a constaté une augmentation de 25 % des attaques par rapport à l'année précédente.

Campagne de cyber-extorsion DDoS

L'autre activité DDoS marquante de 2020 a débuté à la mi-août, lorsqu'un cybercriminel relativement prolifique a lancé la campagne mondiale d'attaques d'extorsion DDoS "Lazarus Bear Armada" (LBA), une campagne qui reste active puisque les pirates ont commencé à recibler les victimes initiales. Les attaquants justifient leurs nouvelles attaques par le fait que la victime n'a pas payé la demande d'extorsion initiale.

Ici aussi, les exigences imposées par la pandémie ont probablement influencé les choix de cibles des attaquants. Si la campagne LBA était initialement axée sur les services financiers, les acteurs de la campagne ont rapidement élargi leur champ d'action pour inclure les grandes entreprises du secteur des soins de santé, notamment les assureurs, les sociétés de dépistage médical et les sociétés pharmaceutiques mondiales. Certaines de ces entreprises étaient associées aux efforts de dépistage de la COVID-19 et au développement de vaccins. Bien qu'il soit peu probable que les attaquants aient cherché expressément à perturber leurs travaux, ces entreprises étaient des cibles privilégiées, car elles avaient à la fois des moyens financiers importants et étaient soumises à des délais urgents.

Les fournisseurs de services de communication, les FSI, les grandes entreprises technologiques et les fabricants ont également fait l'objet d'attaques intensives.

En outre, les attaquants ont ciblé les infrastructures parallèlement aux attaques plus classiques axées sur les services en ligne. Ici aussi, les mesures d'adaptation à la pandémie telles que le travail à distance ont joué un rôle déterminant, dans la mesure où les cybercriminels se sont employés à perturber les opérations courantes au sein d'une entreprise, comme l'utilisation entrante/sortante des VPN et des outils fondés sur le cloud par les collaborateurs travaillant à domicile.

Alors que la pandémie de COVID-19 se poursuit en 2021, nous pouvons logiquement nous attendre à ce que les acteurs de la menace ciblent les vulnérabilités exposées par la crise mondiale et à ce qu'ils découvrent et utilisent de nouveaux vecteurs d'attaque destinés à exploiter les points faibles de notre nouvelle normalité. En effet, ces chiffres ne font qu'effleurer le problème, et nous nous attendons à mettre au jour de nouveaux éléments au fur et à mesure que nous poursuivrons nos recherches dans le cadre du prochain rapport "Threat Intelligence Report" de NETSCOUT. Il est impératif que les défenseurs et les professionnels de la sécurité se montrent vigilants afin de protéger les infrastructures critiques qui connectent le monde moderne et lui permettent de fonctionner. »