Lumen analyse et donne les grandes tendances des attaques DDoS de début 2021

Au travers de son nouveau rapport, Lumen met en lumière les méthodes d'attaque DDoS notamment utilisées lors des récentes cyberattaques menées contre le réseau du gouvernement belge.

DENVER – le 19 mai 2021 – Les attaques DDoS sont de plus en plus complexes, fréquentes et étendues. Spécialiste dans l'identification et la lutte contre ce type de menaces (incluant les botnets Gafgyt et Mirai), **Lumen Technologies** (NYSE : LUMN) publie ce jour son tout dernier rapport trimestriel DDoS 2021. Ce rapport, qui met en perspective l'environnement DDoS, soulignent les grandes tendances de ce type de menaces.

Le rapport repose sur les recherches et analyses réalisées conjointement par le **Black Lotus Labs[1]** et les équipes de sécurité Lumen. Grâce aux contre-mesures directement intégrées au sein de son réseau mondial, **Lumen DDoS Mitigation Service** a également permis à l'entreprise de déceler des tendances d'attaque du premier trimestre 2021.

« Alors que les entreprises dépendent de plus en plus des applications pour générer des revenus, beaucoup réalisent qu'elles ne peuvent plus prendre le risque de renoncer à des défenses DDoS devenues essentielles. Notre rapport vient confirmer cet état de fait », a déclaré Mike Benjamin, Lumen Vice President of Security and Black Lotus Labs. « Alors que les botnets DDoS visant les dispositifs IoT continuent d'évoluer, Lumen souhaite tirer avantage de sa visibilité pour identifier et déstabiliser les infrastructures malveillantes. »

Vous pourrez trouver ci-dessous les principaux enseignements du rapport Lumen :

Les attaques mentionnées ci-dessous sont les attaques les plus importantes contrées par les infrastructures internationales anti-DDoS de Lumen et non pas celles ayant seulement transité sur le réseau.

Botnets IoT :

- Les botnets IoT bien connus comme Gafgyt et Mirai restent des menaces DDoS sérieuses, avec 700 serveurs de commande et de contrôle (C2) actifs ayant fait 28 000 victimes uniques au total.
- Lumen a recensé près de 3 000 attaques DDoS (C2) dans le monde au cours du premier trimestre 2021. Les plus nombreuses étant en provenance de Serbie (1 260), des États-Unis (380) et enfin de la Chine (373).

- Parmi les C2 mondiaux les plus actifs observés par Lumen et en train d'émettre des commandes d'attaque, figuraient les États-Unis (163), suivis des Pays-Bas (73) et de l'Allemagne (70).
- Lumen a suivi plus de 160 000 hôtes de botnets DDoS dans le monde. La plupart se trouvaient aux États-Unis avec 42 000 hôtes recensés.

Tendances des attaques DDoS

- L’attaque la plus importante détectée par Lumen a atteint 268 Gbps de bande passante. En matière de débit, le nombre de paquets a culminé à 26 Mpps pour l’attaque la plus importante.
- La plus longue période d'attaque DDoS contrée par Lumen pour un client a duré presque deux semaines.
- Les atténuations multi-vecteurs ont représenté 41% de l’ensemble des atténuations de DDoS, la plus courante utilisant un flood de requêtes DNS combinée à un flood TCP SYN.
- Les trois principaux secteurs visés par les 500 attaques les plus importantes du premier trimestre 2021 sont la finance, l’IT et les softwares et enfin les institutions gouvernementales.

Suivi des réflecteurs UDP (User Diagram Protocol)

- L'un des principaux outils qu’utilisent les cybercriminels qui cherchent à augmenter la bande passante de leurs attaques est la réflexion basée sur le protocole UDP qui exploite des services tels que Memcached, CLDAP et DNS.
- Grâce à ce processus, un attaquant usurpe une IP source, puis utilise un serveur intermédiaire - un réflecteur - pour envoyer des paquets de réponses massifs à l'IP de la victime plutôt que de les renvoyer à l'attaquant.
- Black Lotus Labs exploite la visibilité de son vaste réseau à l’international pour identifier les services susceptibles d'être utilisés pour lancer ce type d'attaques.
- Sur la base des données du 1er trimestre 2021, Black Lotus Labs constate que les services Memcached, CLDAP et DNS sont particulièrement exploités à ce jour.

Ressources supplémentaires :

- Lire l'intégralité du **rapport DDoS du premier trimestre 2021**
- Consultez **l’infographie/résumé** du rapport DDoS
- Apprenez-en plus sur les **réflecteurs UPD**
- Pour en savoir plus sur le service **DDoS Mitigation Service** de Lumen
- Découvrez comment les organisations actuellement attaquées peuvent mettre en place une atténuation des DDoS en quelques minutes grâce à **Lumen DDoS Hyper**.

À propos de Lumen Technologies

Lumen est guidé par la conviction que l'humanité atteint son apogée lorsque la technologie fait progresser notre façon de vivre et de travailler. Avec un réseau de près de 450 000 km de fibre optique, des clients présents dans plus de 60 pays, Lumen dispose de la plateforme la plus rapide et la plus sécurisée pour gérer les applications et les données afin d'aider les entreprises, les gouvernements et les communautés à offrir les meilleures expériences clients possibles.

Pour en savoir plus sur les services Lumen (Réseau, Cloud, Edge Computing, Cybersécurité et Outils Collaboratifs) et son engagement à promouvoir le progrès humain par le biais de la technologie, vous pouvez consulter : **news.lumen.com**, LinkedIn : /lumentechnologies, Twitter : @lumentechco, Facebook : /lumentechnologies, Instagram : @lumentechnologies et YouTube : /lumentechnologies.

---

[1] Branche de recherche sur les menaces Lumen

For further information: Contacts presse: Suzanne K. Dawe Lumen Public Relations Connected Security | Black Lotus Labs 720.217.5476 suzanne.dawe@lumen.com

---

https://news.lumen.com/2021-05-28-Lumen-analyse-et-donne-les-grandes-tendances-des-attaques-DDoS-de-debut-2021