PRIORITÉ À LA SÉCURITÉ DES APPLICATIONS

APRÈS LES SPAMS, LES ATTAQUES DDoS

3 STRATÉGIES POUR TRANSFORMER UNE CATASTROPHE EN SIMPLE DÉSAGRÉMENT

INTRODUCTION

À mesure que les attaques DDoS prennent de l'envergure et deviennent plus complexes et envahissantes, notre avenir s'annonce ardu avec d'inévitables interruptions de service et des périodes de stress.

Selon le dernier rapport *Threat Horizon* de l'Information Security Forum, les pannes causées par les attaques par déni de service distribué (attaques DDoS) représentent l'une des plus grandes menaces de sécurité auxquels sont confrontées les organisations d'aujourd'hui[1].

Il y a moins de 10 ans, nous devions gérer un tout autre problème : les courriers indésirables, ou spams. En 2009, près de 80 % des 200 milliards d'e-mails envoyés chaque jour contenaient des demandes d'aide provenant de princes nigérians, des offres de pilules miracles délivrées par des pharmacies en ligne et des combines pour se faire de l'argent sans sortir de chez soi. Près de la moitié des spams contournaient les filtres, encombrant les boîtes de réception du monde entier. Pendant une certaine période, il était même tentant de renoncer complètement aux e-mails.

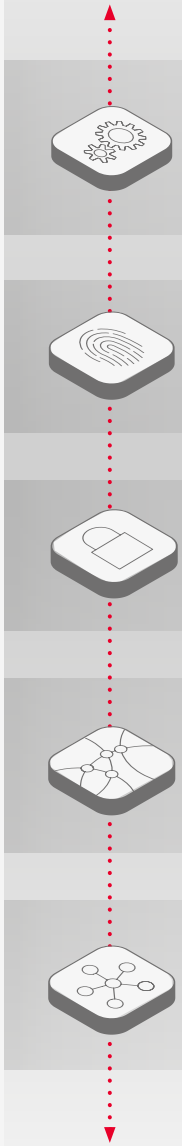
Aujourd'hui, les moyens de défense contre ces courriers indésirables se sont grandement améliorés. Les spams sont désormais envoyés directement dans un dossier dédié, et les quelques demandes provenant d'un prince héritier du Nigeria deviennent plus une source d'amusement qu'autre chose. Nous pouvons désormais nous moquer de ces arnaques. Le spam est à présent un désagrément, un « bruit de fond » que nous remarquons occasionnellement, mais qui ne risque pas vraiment de gâcher notre journée.

Toutefois, nous ne maîtrisons pas toujours le problème des attaques DDoS. Si nous recevons un e-mail similaire frisant l'absurde, mais menaçant de lancer une attaque DDoS, nous ne pouvons ni en rire, ni l'ignorer. Nous devons toujours le prendre au sérieux. L'année dernière, les hackers ont ciblé diverses organisations, tous secteurs confondus, en vue d'influencer des événements politiques, perturbant du même coup les transactions financières traditionnelles ainsi que celles en Bitcoin. Ils ont ainsi envoyé des demandes de rançons à de nombreuses entreprises. Ces dernières n'étaient en effet pas préparées à contrer les attaques volumétriques de masse, qui sont pourtant devenues partie intégrante des actions quotidiennes en ligne[2].

Il est clair que les attaques DDoS ne sont pas près de disparaître. En outre, puisque les attaques et les motivations évoluent, nous devons nous mettre au diapason si nous souhaitons préserver la disponibilité de nos services et la continuité de nos opérations.

[1] https://www.cio.com/article/3185725/security/9-biggest-information-security-threats-through-2019.html
[2] https://securelist.com/ddos-attacks-in-q2-2017/79241/

LES ATTAQUES PAR DÉNI DE SERVICE TOUCHENT TOUTES LES COUCHES DES SUITES D'APPLICATIONS



SERVICES D'APPLICATIONS
- ATTAQUES LOURDES DES URL (RESSOURCES TRÈS SOLLICITÉES)
- ATTAQUES SLOWLORIS (DE TYPE « LOW & SLOW »)
- ATTAQUES PAR SATURATION GET
- ATTAQUES PAR SATURATION ET CONTOURNEMENT DE CACHE HTTP

ACCÈS/IDENTITÉ
- ATTAQUES DE SESSION FACTICES
- ATTAQUES PAR SATURATION ET VERROUILLAGE DE COMPTE
- ATTAQUES PAR PRISE DE CONTRÔLE D'UN COMPTE

TLS/SSL
- ATTAQUES PAR SATURATION SSL
- ATTAQUES PAR RENÉGOCIATION SSL
- DÉTOURNEMENT DU PROTOCOLE SSL

DNS
- ATTAQUE PAR AMPLIFICATION DNS
- ATTAQUE PAR RÉFLEXION DNS
- EMPOISONNEMENT DE CACHE DNS
- ATTAQUES NXDOMAIN DES DNS

RÉSEAU
- ATTAQUES PAR SATURATION SYN VIA TCP
- ATTAQUES PAR SATURATION ICMP ET UDP
- ATTAQUES PAR SATURATION FIN/RST
- ABUS DE PROTOCOLE RÉSEAU

NOUS AVONS TERRASSÉ LE SPAM,

ALORS QU'ATTENDONS-NOUS POUR MAÎTRISER LES ATTAQUES DDoS ?

Pour faire simple, les attaques DDoS sont compliquées à gérer, car il devient difficile de prédire et de distinguer les demandes légitimes de celles d'un trafic malveillant. Tous les réseaux possèdent plusieurs goulots d'étranglement et zones de vulnérabilité. C'est pourquoi les attaques multivectorielles actuelles sont de plus en plus sophistiquées et utilisent une panoplie de tactiques.

ATTAQUES VOLUMÉTRIQUES

Il s'agit des attaques dont nous entendons constamment parler. Elles saturent nos réseaux avec pour mission d'accaparer vos liens en amont sur Internet, empêchant votre base d'utilisateurs d'accéder à vos services.

ATTAQUES DE TYPE « LOW & SLOW »

Nos adversaires utilisent de plus en plus d'attaques de ce type sur les ressources de la couche applicative, tout en exploitant des faiblesses (requêtes de base de données gourmandes en ressources par exemple), pour rendre les services inutilisables. Ces attaques peuvent être difficiles à détecter et à contrer en utilisant les méthodes d'atténuation traditionnelles.

ATTAQUES PAR ÉTRANGLEMENT DES RESSOURCES

Avec plus de 50 % du trafic Internet chiffré à l'aide des protocoles SSL/TLS, les demandes des entreprises pour bénéficier d'une infrastructure de chiffrement (TLS ASIC par exemple) ont grimpé en flèche[3]. Les hackers peuvent submerger les fonctionnalités de déchiffrage de votre réseau. Vos services deviennent alors indisponibles sur les canaux sécurisés nécessaires.

ATTAQUES DE LOGIQUE MÉTIER

Toutes les attaques ne ciblent pas les vulnérabilités de votre réseau ou vos applications. Certains hackers utilisent des bots pour réaliser des opérations frauduleuses sur des sites de vente en ligne, afin d'augmenter les coûts de fonctionnement et d'empêcher des clients légitimes d'accéder à certains services.

COMBINAISON D'ATTAQUES

De nombreuses attaques combinent différents vecteurs qui s'exécutent simultanément, dans le but de trouver un maillon faible dans votre infrastructure, puis de l'exploiter.

[3] https://f5.com/Portals/1/PDF/labs/R065%20-%20REPORT%20-%20The%202016%20TLS%20Telemetry%20Report.pdf

Les attaques DDoS sont lancées avec diverses motivations, allant de l'activisme politique[4] à la revanche mesquine[5] en passant, évidemment, par l'aspect lucratif[6]. Les attaques DDoS sont également de plus en plus utilisées pour faire diversion et faciliter d'autres attaques – une stratégie communément appelée « écran de fumée ». Pendant que vous essayez de faire face au flot de trafic pour maintenir vos services en ligne, les hackers contournent vos défenses et subtilisent des données d'entreprise, des identifiants ou d'autres biens à forte valeur. Les attaques DDoS peuvent également être utilisées pour surcharger les contrôles de sécurité existants (système de détection d'intrusions, services de journalisation, etc.) qui devraient normalement détecter ces activités. D'autres parties de votre réseau se retrouvent alors vulnérables.

Pire, il est facile de lancer une attaque DDoS pour une somme dérisoire. Pour environ 100 $, n'importe qui peut lancer une attaque à 125 Gbit/s pendant six minutes, ce qui est suffisant pour submerger les capacités en amont de la plupart des organisations[7]. Vu la somme, nous sommes donc tous théoriquement en danger : toute personne motivée ou ayant une rancune personnelle peut s'offrir une attaque DDoS.

[4] https://www.csoonline.com/article/3054652/security/political-statements-largely-behind-ddos-attacks.html
[5] https://www.csoonline.com/article/3180246/data-protection/hire-a-ddos-service-to-take-down-your-enemies.html
[6] http://www.zdnet.com/article/ransomware-ddos-now-top-threats-as-hackers-look-for-big-paydays/
[7] https://securelist.com/the-cost-of-launching-a-ddos-attack/77784/

LES ATTAQUES DDOS PEUVENT ÉGALEMENT ÊTRE UTILISÉES POUR SURCHARGER LES CONTRÔLES DE SÉCURITÉ EXISTANTS. D'AUTRES PARTIES DE VOTRE RÉSEAU SE RETROUVENT ALORS VULNÉRABLES.

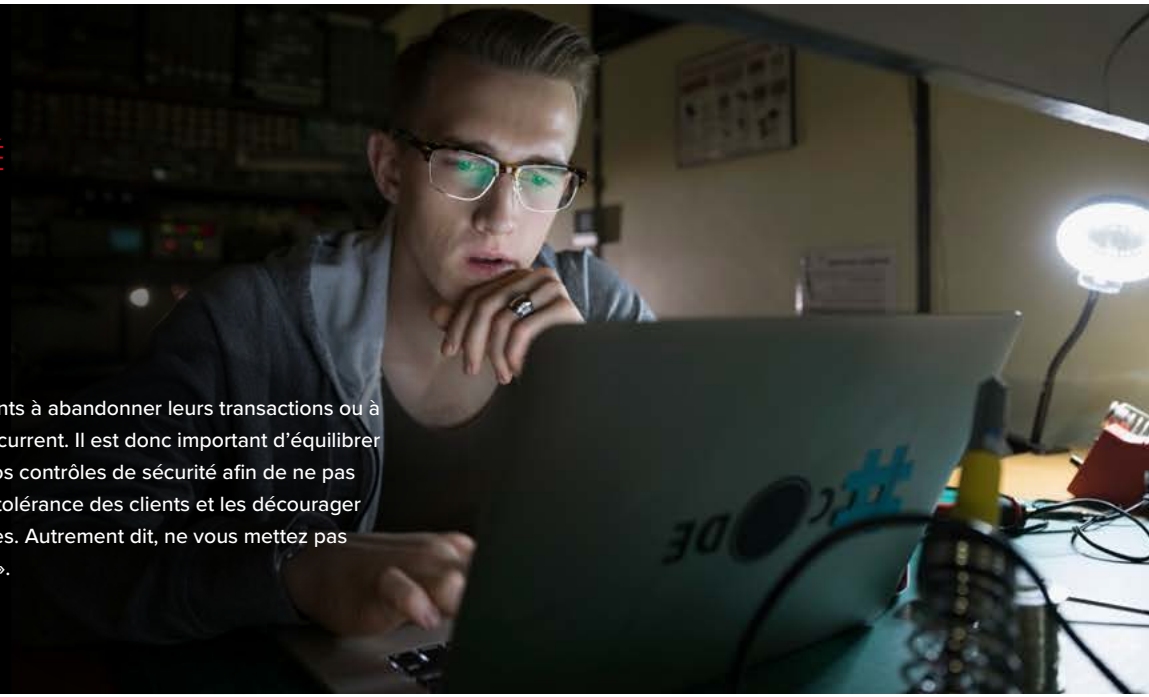
100 $

POUR ENVIRON 100 $, N'IMPORTE QUI PEUT LANCER UNE ATTAQUE À 125 GBIT/S PENDANT SIX MINUTES.

IL EST DONC IMPORTANT D'ÉQUILIBRER MÉTICULEUSEMENT VOS CONTRÔLES DE SÉCURITÉ AFIN DE NE PAS EXCÉDER LE SEUIL DE TOLÉRANCE DES CLIENTS.

NE VOUS METTEZ PAS VOS CLIENTS À « DoS ».

Lorsque les gens parlent de déni de service distribué (DDoS), ils font souvent allusion aux énormes attaques volumétriques générées par des botnets. Toutefois, n'oubliez pas que les hackers n'ont pas besoin de surcharger complètement vos systèmes pour les rendre pénibles pour vos clients. Des pannes ou des niveaux de service médiocres sont suffisants pour inciter vos clients à abandonner leurs transactions ou à aller sur un site concurrent. Il est donc important d'équilibrer méticuleusement vos contrôles de sécurité afin de ne pas excéder le seuil de tolérance des clients et les décourager d'utiliser vos services. Autrement dit, ne vous mettez pas vos clients à « DoS ».

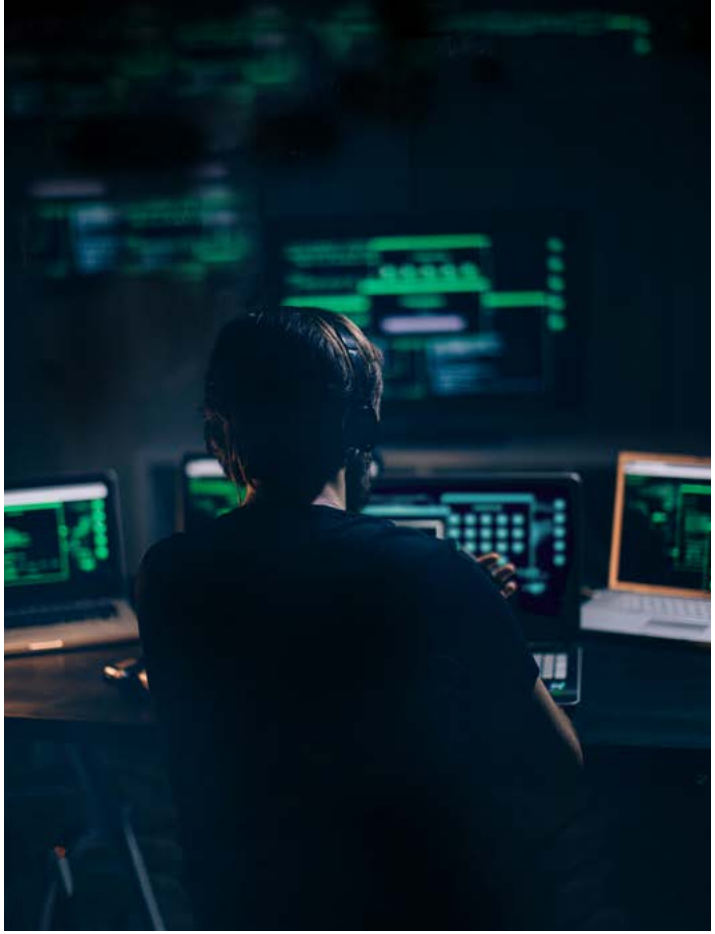


3 STRATÉGIES POUR
CONTRER LES ATTAQUES DDoS

Les attaques DDoS sont en constante évolution, et donc difficiles à contrer. Comment pouvez-vous équilibrer les coûts et vous développer pour répondre aux pics de demande et du trafic, tout en continuant de fournir des niveaux de service satisfaisants à vos clients ? Ou, à l'inverse, comment pouvez-vous repasser à un niveau inférieur de manière souple afin de minimiser les coûts ? Ces problématiques se posent dans chaque organisation à un moment donné. Certaines entreprises avant-gardistes ont testé la résilience de leur infrastructure en lançant des attaques simulées en interne, fréquemment, et n'importe quand[8]. Sous la contrainte, on sait être ingénieux : passer du temps à gérer les attaques DDoS peut avoir des avantages. Tous les acteurs doivent alors redoubler d'efforts, et développer des réseaux et architectures d'applications plus résilients.

[8] https://medium.com/netflix-techblog/tagged/simian-army

IL EST FORT UTILE D'AVOIR UNE GRANDE VISIBILITÉ SUR VOTRE RÉSEAU ET LES ATTAQUES POTENTIELLES AU MOMENT OÙ VOUS DEVEZ OPTIMISER VOS CONTRÔLES POUR MIEUX GÉRER CES ATTAQUES.



1 L'ANALYSE DU COMPORTEMENT ET L'APPRENTISSAGE AUTOMATIQUE PEUVENT VOUS AIDER À LIMITER LES ATTAQUES DDoS

Et si nos systèmes étaient capables d'apprendre de manière autonome à analyser le comportement du trafic, à reconnaître les attaques DDoS et à les arrêter automatiquement ? Ce serait fantastique, non ? Bonne nouvelle : c'est précisément ce que font les solutions intelligentes. En surveillant l'intégrité des services et les tendances du trafic en continu, les technologies avancées de défense peuvent exploiter les données analytiques du comportement et apprendre automatiquement à comprendre le contexte et à reconnaître le trafic normal de référence à partir d'un grand nombre de données. Il est donc de plus en plus facile d'identifier les transactions ou processus anormaux, de prendre des mesures pour minimiser les actions des clients suspects et d'affiner les données afin d'améliorer le processus au fil du temps. Seul bémol : même si les données analytiques du comportement sont pertinentes pour arrêter les attaques DDoS de la couche 7, elles ne permettent pas vraiment de se défendre contre les attaques volumétriques par saturation à grande échelle. Le trafic indésirable parviendra tout simplement à noyer toutes les demandes légitimes.

Il est donc fort utile d'avoir une grande visibilité sur votre réseau et les attaques potentielles, au moment où vous devez optimiser vos contrôles pour mieux gérer ces attaques. Par exemple, si 90 % de votre clientèle est située en France et que vous détectez un grand nombre d'attaques provenant d'adresses IP en dehors de l'hexagone, il peut alors s'avérer nécessaire de bloquer tout le trafic venant de l'étranger pendant la durée de l'attaque, afin de maintenir la disponibilité du service pour la grande majorité des clients. Dès que l'attaque par saturation est terminée, vous pouvez alors réduire les contrôles et restaurer la disponibilité à l'échelle mondiale.

Si vous constatez des demandes répétées au niveau de la couche applicative provenant de certaines adresses IP ou de souches de logiciels malveillants, vous pouvez aussi simplement bloquer le trafic provenant de ces clients au niveau de la couche réseau et ne pas le traiter du tout. Vous pouvez également mettre en œuvre des règles de qualité de service (QoS) pour réduire l'impact de leurs demandes.

33 %

EN 2017, 33 % DE TOUTES LES ORGANISATIONS ONT ÉTÉ CONFRONTÉES À AU MOINS UNE ATTAQUE DDoS[9].

Des solutions intelligentes vous permettront d'identifier votre trafic de référence, de définir les paramètres pour gérer ce trafic et d'intensifier automatiquement les contrôles en fonction de conditions prédéfinies. Les données analytiques du comportement et le « relevé de traces numériques » peuvent vous donner un aperçu plus nuancé des intentions de n'importe quel point de terminaison distant (trafic inoffensif ou malveillant, provenant d'une personne réelle ou d'un bot). Vous êtes alors à même de classifier votre trafic de manière appropriée.

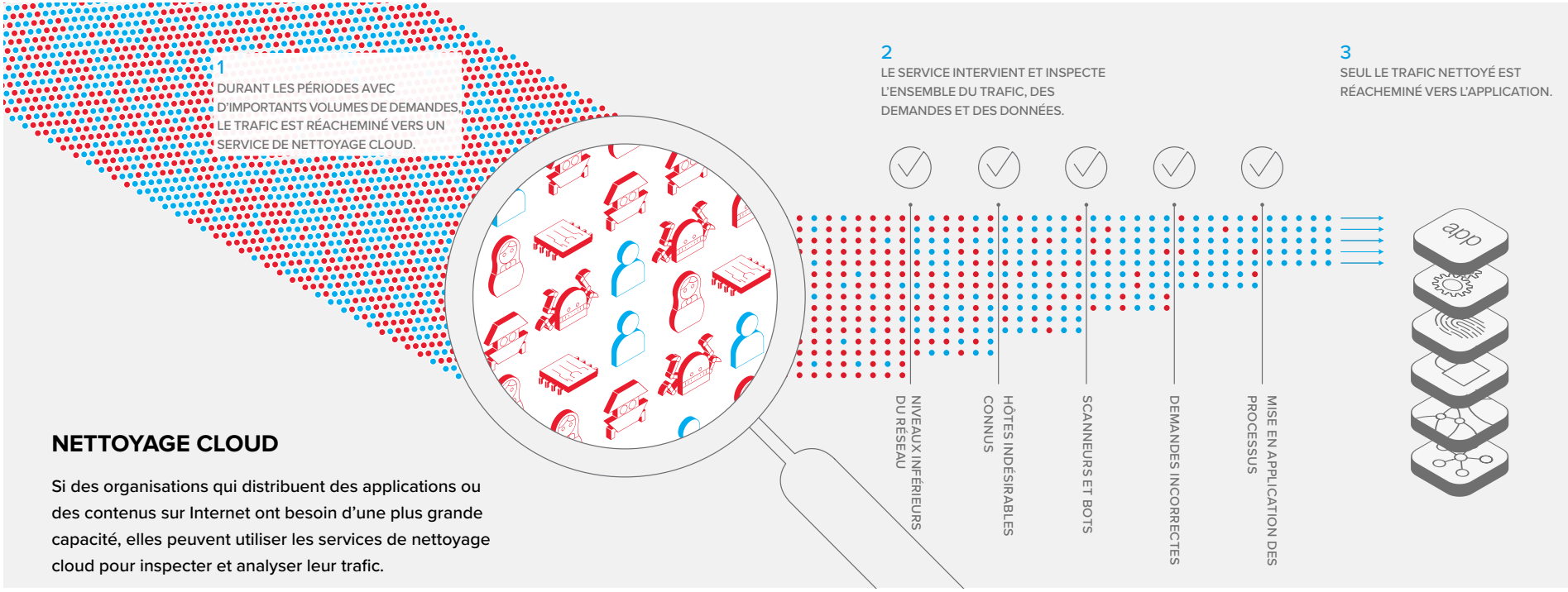
[9] https://www.techrepublic.com/article/33-of-businesses-hit-by-ddos-attack-in-2017-double-that-of-2016/

2 LE NETTOYAGE CLOUD MAINTIENT VOS ACTIVITÉS EN LIGNE AU COURS D'UNE ATTAQUE

Alors que les attaques par saturation partielle, basées sur l'authentification et situées au niveau des applications, peuvent généralement être contrées grâce à une solution sur site ou une plate-forme cloud toujours activée, les attaques volumétriques de masse parviennent facilement à dépasser les défenses les plus robustes. Vous devez donc élaborer un plan permettant d'exploiter une plus grande capacité que vos adversaires. C'est là qu'intervient le nettoyage cloud.

Toutes les organisations distribuant du contenu ou des applications sur Internet peuvent utiliser un service de nettoyage cloud pour maintenir leurs activités en ligne au cours d'une attaque, tout en minimisant l'impact sur les utilisateurs. Le nettoyage consiste à inspecter et à analyser le trafic, les demandes, les données d'entrée, etc., aussi bien pour jauger leur utilité que pour les valider. Lorsque le trafic traverse le centre de nettoyage hors site, il est continuellement analysé pour s'assurer que les demandes malveillantes sont filtrées. À la fin du processus, le trafic « nettoyé » vous est renvoyé pour que vous puissiez répondre aux demandes légitimes et continuer à opérer normalement.

Les services de nettoyage cloud fonctionnent généralement selon l'un des deux modèles suivants : à la demande et toujours activé. Le modèle à la demande consiste à acheminer le trafic à travers le centre de nettoyage uniquement lorsqu'il dépasse votre capacité, qu'il s'agisse de demandes exigeantes en ressources, difficiles à traiter ou lancées en très grand volume. Le modèle toujours activé gère cette même opération à votre place en permanence et peut réduire ou éliminer le temps passé à réparer les dégâts. Il peut également décourager les hackers potentiels de vous attaquer lorsqu'ils recherchent des victimes, tout comme un chien dans un jardin peut dissuader des cambrioleurs de cibler une maison.



NETTOYAGE CLOUD

Si des organisations qui distribuent des applications ou des contenus sur Internet ont besoin d'une plus grande capacité, elles peuvent utiliser les services de nettoyage cloud pour inspecter et analyser leur trafic.

3 LA SIGNALISATION ET LA PROTECTION HYBRIDE À LA DEMANDE POURRAIENT ÊTRE L'AVENIR DE LA PROTECTION CONTRE LES ATTAQUES DDoS

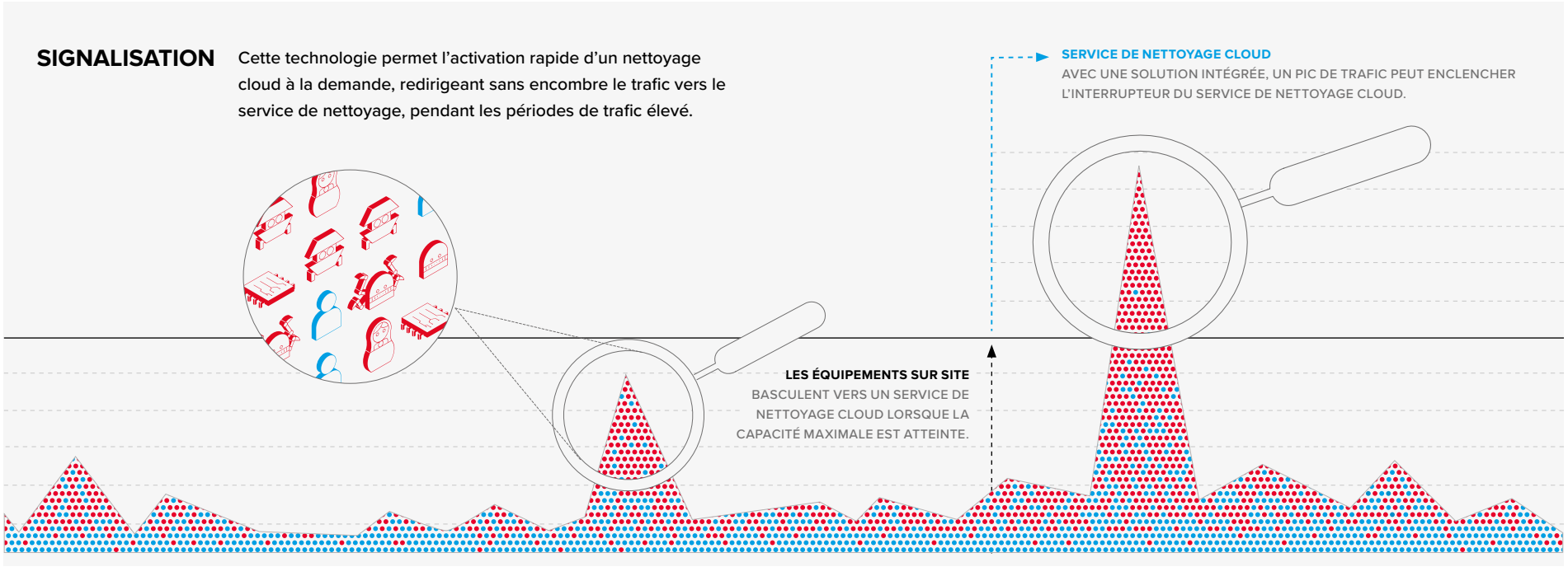
Tant que les attaques DDoS resteront efficaces et rentables, les vecteurs et tactiques des attaques continueront d'évoluer. Une solution robuste doit englober des fonctionnalités d'atténuation pour toutes sortes d'attaques, qu'il s'agisse d'attaques par saturation faibles et lentes (Low & Slow) ou volumétriques. Mais comment pouvez-vous optimiser vos systèmes pour qu'ils fonctionnent efficacement et vous permettent de rester en ligne lors d'une attaque ?

La « signalisation » combine des équipements sur site avec des services de nettoyage cloud, ce qui leur permet de communiquer entre eux lors d'une attaque. Cette technologie permet l'activation rapide d'un nettoyage cloud à la demande, redirigeant sans encombre le trafic provenant des attaques vers le service de nettoyage. Vous empêchez ainsi les attaques volumétriques de toute taille de saturer vos connexions en amont. Le Groupe de travail de génie Internet (IETF) possède une équipe chargée d'élaborer une approche fondée sur des normes de signalisation en temps réel entre les solutions sur site, les services de nettoyage et d'autres éléments et services du réseau[10]. À mesure que la technologie évolue, la signalisation gagne encore en efficacité. Il s'agit peut-être de votre meilleure ligne de défense au sein d'une stratégie globale de protection contre les attaques DDoS.

En fonction des solutions que vous possédez actuellement, vous avez peut-être la possibilité d'utiliser la signalisation pour protéger votre réseau et vos applications. Vous pouvez déclencher un « interrupteur » pour votre service de nettoyage cloud ou configurer votre système pour l'activer automatiquement via des règles et des seuils prédéfinis. Même si la méthode automatique nécessite une bonne préparation et des tests (en particulier pour les plans d'atténuation de la couche 7 nécessitant le déchargement SSL), elle peut vous faire gagner du temps et vous épargner bien des efforts lorsque vous devenez une cible active.

Comme pour toutes les stratégies de protection contre les attaques DDoS, il vous faudra planifier et vous préparer avant que le pire scénario ne se matérialise. Vous devrez certainement passer un peu de temps avec votre fournisseur de nettoyage pour déterminer le meilleur moyen de transférer sans encombre le trafic à destination et en provenance du service de nettoyage. Cependant, vos efforts seront récompensés quand vous en aurez le plus besoin.

[10] https://datatracker.ietf.org/wg/dots/about/



ATTAQUE DDoS : UN DÉSAGRÉMENT, PAS UNE CATASTROPHE

À mesure que la signalisation et la technologie de nettoyage évolueront (et que vos solutions deviendront de plus en plus adaptables), les attaques DDoS seront de moins en moins efficaces et attrayantes pour vos ennemis potentiels. Nous entrerons bientôt dans une ère où une attaque de 1 To provenant d'un botnet visant les objets connectés sera perçue comme un simple désagrément à peine visible, et non plus comme un événement catastrophique.

Alors, comment pouvez-vous y arriver plus rapidement ? Planifiez en amont en concevant une stratégie de défense en profondeur contre les attaques DDoS et collaborez avec un fournisseur de sécurité fiable pour faire face aux grandes attaques. Toute préparation préalable sera récompensée lorsque la menace des attaques DDoS ne vous empêchera plus de dormir.

Pour en savoir plus sur les menaces qui pèsent sur votre entreprise et les solutions pour vous défendre, rendez-vous sur f5.com/security.

TOUTE PRÉPARATION PRÉALABLE SERA RÉCOMPENSÉE LORSQUE LA MENACE DES ATTAQUES DDoS NE VOUS EMPÊCHERA PLUS DE DORMIR.

PRIORITÉ À LA SÉCURITÉ DES APPLICATIONS

Les applications toujours activées et toujours connectées peuvent dynamiser et transformer votre entreprise. Cependant, elles peuvent également servir de portes d'entrée vers vos données malgré les protections de vos pare-feu. Puisque la plupart des attaques surviennent au niveau des applications, la protection des fonctionnalités qui dynamisent votre entreprise implique forcément la protection des applications qui leur permettent d'exister.

Siège social aux États-Unis : 401 Elliott Ave W, Seattle, WA 98119 | 888-882-4447 // Amérique : info@f5.com // Asie-Pacifique : apacinfo@f5.com // Europe/Moyen-Orient/Afrique : emeainfo@f5.com // Japon : f5j-info@f5.com