Akamai

LIVRE BLANC

Vecteurs d'attaque menaçant la confiance de vos clients

La sécurité et la confiance en la marque n'ont jamais été aussi interdépendantes. Avec les applications et les API qui déterminent la façon dont les marques se présentent au monde (et le nombre de cyberattaques qui monte en flèche à l'échelle mondiale), sécuriser les applications digitales sans nuire à l'expérience client est aujourd'hui une priorité pour les équipes de sécurité du monde entier.

Une solide expérience client renforce la confiance en la marque, ce qui a un impact mesurable sur les performances de l'entreprise. Des performances des sites Web à la protection des données, et tout ce qui se trouve entre les deux, les choix de sécurité des entreprises empirent trop souvent l'expérience client. Les lourds contrôles qui protègent l'entreprise peuvent créer des zones de friction pour le client, entraînant une perte de confiance et, en fin de compte, une perte de revenus.

Les choix en matière de sécurité influent également sur la croissance et l'innovation. Alors que les entreprises poursuivent leur expansion digitale et la migration de leurs données et applications dans le cloud, d'innombrables acteurs malveillants se concentrent sur les vecteurs d'attaque engendrés par ces mouvements. Les solutions de sécurité doivent désormais viser à évoluer en amont de leurs tactiques changeantes et d'attaques multivectorielles sophistiquées (différents types d'attaques en même temps ou se succédant rapidement) en optant pour des solutions qui fonctionnent conjointement, pour sécuriser votre entreprise et maintenir la confiance des clients en votre marque.

Quels vecteurs d'attaque devraient figurer en tête de liste ?

La nouvelle cible de choix : les API

Les applications pilotent presque tous les aspects de votre entreprise, et les interfaces de programmation d'applications (API), qui connectent les éléments logiciels et permettent la communication entre différentes applications, sont devenues la nouvelle cible privilégiée des acteurs malveillants. Pourquoi ? Trop souvent, les applications et les processus métier impliquant des API sont lancés et déployés à un rythme plus rapide que celui des évaluations des équipes de sécurité, ce qui entraîne des problèmes de configuration et des vulnérabilités. Les acteurs malveillants recherchent justement ces failles : en utilisant l'abus de logique métier, les attaques d'API réussies leur permettent d'accéder à votre environnement, où ils peuvent voler des données et même lancer des attaques supplémentaires. Les acteurs malveillants ne ciblent pas seulement les API qui traversent votre pare-feu d'application Web. Même lorsqu'elles sont authentifiées par votre WAF, les API peuvent toujours devenir vulnérables aux attaques. C'est le signe que les pirates effectuent désormais régulièrement des opérations de reconnaissance pour identifier les API à exploiter.

Il est important de se rappeler que n'importe quelle API peut potentiellement être ciblée. Dans des secteurs tels que la santé, l'interopérabilité des terminaux IoT, par exemple, a fait des API une cible de choix pour les criminels cherchant à voler des informations personnelles identifiables (PII) ou à lancer des attaques par ransomware. La sécurisation des API commence donc par une vue sur chaque API associée à votre organisation, également appelée parc d'API.

Akamai API Security vous aide à inventorier votre parc, puis vous offre une visibilité sur le comportement historique de chaque API, afin que vous puissiez découvrir quels sont les comportements normaux et abusifs des API. Grâce à ces connaissances, vous pouvez rechercher des menaces actives, afin de pouvoir arrêter rapidement les abus avant que les acteurs malveillants n'atteignent leurs objectifs.

Plus sophistiqués et plus faciles à déployer que jamais : les bots malveillants

les bots se déplacent sur votre site Web, tout le temps. De fait, tous vos efforts d'optimisation des moteurs de recherche ont pour but de gagner leurs faveurs. Au milieu des bons, on trouve des bots malveillants qui entreprennent une multitude de cyberattaques. Les bots malveillants sont peut-être le mieux connus pour monopoliser des stocks limités, en achetant des chaussures de sport en édition limitée ou d'énormes quantités de billets de concert ou de réservations d'hôtel par exemple, mais les bots utilisent à peu près la même méthode lorsqu'ils submergent votre entreprise avec un nombre excessif de requêtes dans une attaque par déni de service distribué, ou DDoS, conçue pour mettre votre entreprise hors ligne.

Ce que beaucoup de gens ne savent pas, c'est que les attaques DDoS sont devenues une forme d'attaque relativement facile et peu coûteuse utilisée par une nouvelle génération d'attaquants pour mettre hors service des entreprises valant plusieurs milliards de dollars et des infrastructures publiques critiques, notamment les écoles, les hôpitaux, les aéroports et les fournisseurs de services publics. Ces attaques créent des interruptions de service massives qui coûtent à leurs victimes d'énormes quantités de revenus par minute. Au contraire des attaquants traditionnels du passé, ces attaques sont presque toujours menées par des acteurs sophistiqués des États-nations, des hacktivistes politiques et des cybercriminels professionnels avec l'aide de botnets de grands réseaux d'appareils connectés (qui peuvent être des appareils utilisateurs ou de simples terminaux IoT) infectés et contrôlés par des bots.

Les bots sont également utilisés pour lancer des attaques par credential stuffing qui conduisent à des attaques de piratage de comptes. Le credential stuffing se produit lorsqu'un attaquant utilise une liste de noms d'utilisateur et de mots de passe obtenus lors d'une importante violation de données, puis soumet ces informations d'identification lors de tentatives massives de connexion à d'autres institutions. Des bots sont déployés pour entreprendre des millions de tentatives de prise de contrôle de compte, et comme beaucoup de monde a tendance à réutiliser les noms d'utilisateur et les mots de passe, une petite fraction fonctionnera. Une fois que l'attaquant accède à un compte, cela devient une attaque de piratage de contrôle de compte.

Le credential stuffing n'est qu'une des nombreuses méthodes utilisées par les acteurs malveillants pour prendre le contrôle de comptes légitimes. Une fois qu'ils contrôlent un compte, ils peuvent siphonner des points de fidélité et transférer des actifs digitaux, drainer les soldes des cartes-cadeaux et effectuer des achats frauduleux en utilisant les informations de carte de crédit stockées. Ils peuvent même vendre le compte tout entier à un autre acteur malveillant. Lorsque cela arrive à un client, la confiance est presque toujours irrévocablement brisée. Mais même les attaques de credential stuffing infructueuses peuvent être nuisibles à votre marque, car le trafic de bots qui inonde votre site pendant ces tentatives peut réduire considérablement la disponibilité des ressources et ralentir les temps de réponse, créant ainsi des expériences frustrantes pour vos clients et les visiteurs du site.

Enfin, les bots d'extraction sont utilisés à des fins à la fois bonnes et malveillantes, mais ce qui est moins évident, c'est que leur présence peut ralentir les performances du site et polluer les indicateurs dont les entreprises ont besoin pour prendre des décisions importantes, rendant leurs effets secondaires potentiellement pires pour votre marque que les données qu'ils extraient.

Akamai dispose d'une suite de solutions spécialement conçues pour atténuer les menaces introduites par les bots malveillants :

Akamai App & API Protector avec le module de protection contre les logiciels malveillants est la base de la protection contre le vol de vos données, informations personnelles identifiables et autres informations de compte, et pour bloquer les attaques DDoS dirigées par des bots, ainsi que les ransomwares, les logiciels malveillants, etc. Il permet à vos clients d'avoir un accès constant à vos propriétés Web et garantit que les performances du site ne soient pas ralenties lorsque vous subissez une attaque.

Akamai Bot Manager détecte tout le trafic de bots et atténue les bots malveillants en bordure de l'internet. Il utilise des modèles d'IA pour analyser le comportement des bots et déploie des algorithmes d'empreintes digitales du navigateur et d'apprentissage automatique pour rendre la détection de plus en plus précise, réduisant les frictions pour les utilisateurs tout en les protégeant des activités frauduleuses.

Akamai Content Protector empêche les extracteurs de voler votre contenu Web qui peut être utilisé à des fins malveillantes, tout en limitant la dégradation des performances du site. Avec la détection reposant sur l'apprentissage automatique, l'activité potentiellement malveillante du bot extracteur est classée par risque pour informer la réponse appropriée.

Une autre solution fondamentale pour protéger vos clients consiste à améliorer l'accès sécurisé aux comptes. Akamai Account Protector contrecarre les fraudes humaines souvent coordonnées par des bots, tout en permettant aux utilisateurs de confiance d'accéder à votre site de manière sécurisée et sans friction, ce qui les encourage à rester connectés plus longtemps et à revenir plus souvent.

Le coût des scripts malveillants : les menaces côté client

De la même façon que les bots, les scripts tiers font en grande partie de bonnes choses. Ils activent des fonctionnalités, des outils marketing, des analyses et bien plus encore pour améliorer votre expérience utilisateur globale. Mais ils transforment également le navigateur Web en une surface de menace critique côté client.

Les menaces côté client cherchent à inciter vos clients à accéder à du contenu malveillant. Elles tirent parti des faiblesses des applications qui s'exécutent sur l'ordinateur utilisé directement par l'utilisateur (généralement votre client), appelé ici le client. La sécurité côté client englobe donc les technologies et les stratégies utilisées pour protéger les clients contre les activités malveillantes survenant sur les pages Web.

Les attaques par script peuvent être à l'origine de dommages financiers importants aux entreprises et diminuer la confiance envers les clients, les partenaires et les processeurs de paiement. Sans surprise, la sécurité côté client est au cœur des nouvelles exigences de la norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS v4.0). Pour s'y conformer, toute entreprise traitant des cartes de paiement en ligne doit savoir quels scripts sont en cours d'exécution sur son site, quand ils changent et quand ils cessent de fonctionner.

Se défendre contre ces attaques n'est pas facile. Les scripts tiers sont nombreux et changent continuellement, ce qui les rend extrêmement difficiles à surveiller. Les attaques de script elles-mêmes prennent également diverses formes, telles que le web skimming et le détournement de formulaires. Des syndicats criminels entiers (le plus connu d'entre eux étant Magecart) se sont organisés autour de ce genre de techniques pour voler des données de carte de paiement et des informations personnelles identifiables.

Dans notre monde de paiements digitaux et d'achats et de recherches en ligne, la sécurité côté client est plus essentielle que jamais, en particulier sur les pages de paiement où des données personnelles et financières sont collectées. Vous devez avoir une visibilité sur tous les scripts exécutés sur votre site, la capacité de détecter les comportements suspects et des mesures d'atténuation en place pour vous défendre contre les attaques. Akamai propose une solution spécifique pour faire face aux menaces suivantes :

Client-Side Protection & Compliance maintient la confidentialité et la confiance des clients dans le navigateur en protégeant tous vos utilisateurs contre les attaques côté client telles que le web skimming, le détournement de formulaire et Magecart.

Protégez votre infrastructure pour protéger l'expérience client

Au cœur de l'expérience client se trouve l'infrastructure digitale sous-jacente qui alimente tout ce qui concerne votre marque. La sécurité, la fiabilité et les performances DNS sont ce qui garantit que vos clients puissent accéder à vos services quand ils en ont besoin. Les systèmes DNS équivalent essentiellement à votre présence en ligne. Lorsqu'ils tombent en panne, toute votre présence digitale le fait également. C'est pourquoi les acteurs malveillants attaquent constamment les systèmes DNS de leurs cibles avec des attaques DDoS. Compte tenu du terrain de jeu extrêmement concurrentiel auquel tous les secteurs sont confrontés, vous n'avez besoin que d'une disponibilité DNS continue et d'un temps de disponibilité de 100 % pour garantir aux clients et aux clients potentiels le meilleur que votre marque a à offrir.

Akamai propose un éventail de solutions de référence pour protéger votre infrastructure digitale contre diverses attaques DDoS :

Pour la défense la plus puissante contre les attaques DDoS, Akamai Prolexic propose plusieurs options de protection, notamment des centres de nettoyage répartis dans plus de 32 sites dans le monde et une capacité de défense dédiée de 20 Tbit/s.

Akamai Edge DNS offre une solution DNS complète, spécialisée et faisant autorité, qui exploite l'évolutivité, la sécurité et la capacité d'Akamai Connected Cloud pour gérer vos zones DNS.

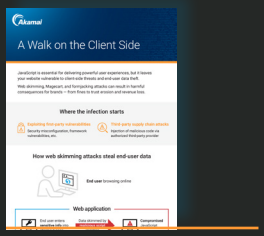
Akamai Shield NS53, une solution proxy DNS bidirectionnelle avec application dynamique des règles de sécurité, peut être utilisée pour protéger les composants clés de votre infrastructure DNS d'origine, que ce soit sur site, dans le cloud ou en hybride, contre les attaques par épuisement des ressources.

Nous sommes votre partenaire pour assurer la confiance de vos clients

Chez Akamai, nous nous concentrons sur la façon dont les marques se présentent depuis plus de 25 ans. En tant que pionnier des réseaux de diffusion de contenu, nous avons résolu les problèmes de vitesse des toutes premières vitrines digitales. Au cours des dix dernières années, nous avons utilisé la visibilité sur le trafic offerte par notre réseau de diffusion de contenu (l'un des plus importants au monde) pour surveiller et analyser les menaces au quotidien, des recherches qui nous permettent de faire évoluer nos solutions de sécurité de manière organique à mesure que les vecteurs d'attaque continuent de croître et d'évoluer. En tant que partenaire de sécurité clé pour nos clients, nous partageons un engagement commun à maintenir leurs activités opérationnelles et à protéger leur expérience client, tout en leur donnant la confiance nécessaire pour expérimenter les nouvelles expériences digitales qui dominent leurs industries.

Étapes suivantes

Voici quelques ressources pour vous aider à envisager la prochaine étape à suivre pour protéger votre marque :



Renforcez l'intégrité de vos pages Web avec une protection côté client.

Obtenez une sécurité tout-en-un et sans compromis pour les sites Web, les applications et les API.

Découvrez les principales considérations nécessaires à une stratégie de gestion des bot.

Akamai protège votre expérience client, votre personnel, vos systèmes et vos données en vous aidant à intégrer la sécurité dans tout ce que vous créez, dans toutes vos conceptions et diffusions. La visibilité de notre plateforme sur les menaces mondiales nous aide à adapter et à faire évoluer votre stratégie de sécurité (activer le Zero Trust, bloquer les ransomwares, sécuriser les applications et les API, ou lutter contre les attaques DDoS), vous donnant ainsi la confiance nécessaire pour innover, prospérer et ouvrir le champ des possibles. Pour en savoir plus sur les solutions de Cloud Computing, de sécurité et de diffusion de contenu, rendez-vous sur akamai.com et akamai.com/blog, ou abonnez-vous à Akamai Technologies sur X (anciennement Twitter) et LinkedIn.
Publication : 06/24.