FICHE PRODUIT AKAMAI

Content Protector

Protégez vos revenus contre les attaques d'extracteurs de plus en plus sophistiquées

Grâce à l'extraction de votre contenu, il y a de l'argent à gagner (pour les attaquants) et à perdre (pour vous). Partager du contenu publiquement est un choix stratégique, mais il est essentiel de faire la différence entre l'engagement des utilisateurs et les activités d'extraction nuisibles. Vos concurrents et les attaquants peuvent exploiter les données extraites, et ainsi compromettre votre stratégie de tarification et nuire à vos clients. Akamai Content Protector identifie et arrête rapidement les extracteurs, grâce à des détections adaptées aux outils et techniques uniques des attaques d'extraction. Protégez votre activité et vos revenus sans compromettre la vitesse ou les performances.

Les attaques d'extraction représentent un défi permanent pour les entreprises en ligne. Contrairement aux cybermenaces classiques qui ont des points de départ et de fin évidents, les extracteurs peuvent accéder de manière persistante à votre site, ce qui entraîne des répercussions importantes si elles ne sont pas traitées. En voici quelques exemples :

- **Impact sur les performances du site Web :** les activités d'extraction persistantes peuvent ralentir votre site, entraînant une frustration des utilisateurs et une réduction des taux de conversion.
- **Inconvénients concurrentiels :** vos concurrents peuvent utiliser l'extraction pour surveiller vos tarifs et proposer des prix inférieurs, affectant ainsi vos revenus.
- **Risques pour la réputation de la marque :** des contrefacteurs pourraient utiliser le contenu extrait de manière abusive, et vendre de faux produits sous le nom de votre marque.

Bien évidemment, les extracteurs existent depuis de nombreuses années. Pourquoi sont-ils plus dangereux maintenant ? L'urgence à lutter contre les extracteurs s'est intensifiée récemment. Les événements de 2020, y compris la pandémie et les perturbations de la chaîne d'approvisionnement qui ont suivi, ont augmenté les motivations financières liées à l'extraction. Les articles à forte demande, que ce soient des articles essentiels du quotidien, des produits de luxe ou des services de voyage, sont devenus des cibles privilégiées pour les opérations d'extraction sophistiquées.

Avec plus d'argent potentiel à gagner, les opérateurs de bots ont commencé à innover activement, se spécialisant dans des éléments d'outils (comme la télémétrie), puis en les enchaînant avec des éléments conçus par d'autres opérateurs de bots pour créer des bots hautement spécialisés propres aux attaques d'extraction. Cela permet aux extracteurs d'être plus dangereux et aussi plus difficiles à détecter. Pis encore, l'extraction peut également se produire en utilisant d'autres méthodes comme les plug-ins ; il vous faut donc plus que la gestion des bots pour arrêter les extracteurs.

Mais vous ne pouvez pas simplement bloquer tous les extracteurs : les bots de recherche recherchent le nouveau contenu que vous souhaitez afficher dans les recherches publiques, certains bots d'achat grand public peuvent mettre en valeur vos produits sur des sites de comparaison et les partenaires peuvent collecter efficacement les dernières informations produits pour les partager avec leurs clients.

AVANTAGES POUR VOTRE ENTREPRISE

Augmentez les taux de conversion
Supprimez les bots qui ralentissent votre site et vos applications pour conserver vos clients sur votre site et améliorer les ventes

Réduisez les coûts
Ne payez pas pour servir le trafic de bots

Contrecarrez les extracteurs
Empêchez les extracteurs d'interroger votre site pour savoir quand vos stocks sont accessibles, réduisant ainsi la capacité des opérateurs de bots à passer à l'étape suivante dans une chaîne d'attaque d'accaparement de stocks

Contrariez vos concurrents
Arrêtez l'extraction automatisée qui permet à vos concurrents de proposer des prix inférieurs aux vôtres et de réduire vos ventes

Atténuez la contrefaçon
Arrêtez l'extraction incessante que les contrefacteurs utilisent pour saisir votre contenu, puis se faire passer pour vous

Améliorez votre commercialisation
Supprimez le trafic de bots de vos analyses de site pour vous assurer que vos optimisations favorisent bien les vrais utilisateurs

Akamai

Akamai Content Protector dispose de fonctionnalités de détection spécialement conçues pour détecter les extracteurs et les arrêter. Et ce, tout en tirant parti de la visibilité du réseau Akamai, de notre position de leader en matière de gestion des bots et du développement continu de détections de pointe. Grâce à la mise à jour de votre protection au fur et à mesure que les menaces évoluent, nous intégrons automatiquement les informations de nos chercheurs en matière de renseignements sur les menaces et de nos spécialistes des données, de sorte que Content Protector continue de jouer un rôle de leader dans les détections personnalisées d'extracteurs.

Après avoir arrêté les extracteurs, vous pouvez vous concentrer sur l'optimisation de votre présence digitale, par exemple en améliorant les performances de votre site et les taux de conversion, et en réduisant l'impact des concurrents.

Principales fonctionnalités

- **Détections :** ensemble de méthodes de détections optimisées par l'apprentissage automatique (ML) qui évalue les données collectées côté client et côté serveur.
  - » **Évaluation au niveau du protocole :** l'analyse de l'empreinte protocolaire permet d'évaluer la façon dont le client établit la connexion avec le serveur au niveau des différentes couches du modèle OSI : TCP, TLS et HTTP, en vérifiant que les paramètres négociés correspondent à ceux attendus des navigateurs Web et des applications pour mobile les plus courants.
  - » **Évaluation au niveau de l'application :** elle consiste à évaluer si le client peut exécuter une logique métier rédigée en JavaScript. Lorsque le client exécute JavaScript, les caractéristiques du terminal et du navigateur ainsi que les préférences de l'utilisateur (empreinte) sont collectées par Content Protector. Ces différents points de données seront comparés et recoupés avec les données au niveau du protocole pour vérifier la cohérence.
  - » **Interaction avec l'utilisateur :** les indicateurs de comportement permettent d'analyser l'interaction humaine avec le client via des périphériques standard tels qu'un écran tactile, un clavier ou une souris. Le manque d'interaction ou une interaction anormale est généralement associé au trafic des bots.
  - » **Comportement de l'utilisateur :** il consiste à analyser le parcours de l'utilisateur sur le site Web. Les botnets s'attaquent généralement à un contenu spécifique, ce qui entraîne un comportement significativement différent du trafic légitime.
  - » **Détection de navigateurs sans interface :** un JavaScript personnalisé s'exécutant côté client recherche les indicateurs laissés par les navigateurs sans interface même en mode furtif.
- **Classification des risques :** elle consiste à fournir une classification déterministe et exploitable du trafic à faible, moyen ou haut risque, selon les anomalies détectées lors de l'évaluation.
- **Mesures de riposte :** ensemble de stratégies de réponse, y compris l'action simple de surveillance et d'exclusion, et de stratégies plus avancées telles que le système de répulsion (« tarpit »), qui simule un blocage de serveur ou divers types d'actions de défi. Les défis cryptographiques sont généralement plus simples à utiliser que les défis CAPTCHA pour traiter les faux positifs éventuels.

Les bases de Content Protector : l'environnement Akamai

Akamai offre des performances Internet rapides, intelligentes et sécurisées. Nos solutions complètes se basent sur l'Akamai Connected Cloud mondialement distribué, géré via le Control Center unifié et personnalisable d'Akamai, qui en assure la visibilité et le contrôle, et comprennent l'assistance d'experts en services professionnels qui vous aident à mettre en place votre service, à assurer son bon fonctionnement et à innover en fonction de l'évolution de vos stratégies.

Inscrivez-vous à une démo ou contactez l'équipe commerciale d'Akamai.