PERSPECTIVES DU MARCHE

Pare-feu applicatif Web (WAF) côté client : la prochaine frontière en matière de sécurité

Christopher Rodriguez

SYNTHESE

FIGURE 1

Synthèse : menaces côté client et solutions émergentes

En 2018, les chercheurs en sécurité ont identifié une nouvelle forme de cybercriminalité, le vol de données de cartes bancaires en ligne, ou « web skimming ». Les attaques de Magecart ont exploité la tendance croissante consistant à déplacer les fonctionnalités des applications du serveur vers le client. Les cybercriminels sont parvenus à injecter du code malveillant dans des sources d'applications fiables, lequel s'exécutait dans les navigateurs des utilisateurs, sans la protection d'un WAF. Ces attaques ont représenté une violation des données de longue durée qui a révélé une vulnérabilité dans les pratiques de sécurité applicative Web d'entreprise.

Points à retenir

- Les scripts côté client constituent un outil précieux dans l'architecture des applications, car ils permettent d'améliorer l'expérience utilisateur, les performances des applications, l'analytique et la sécurité.
- Les scripts sont omniprésents. Les sites Web actuels utilisent des dizaines de scripts différents, dont les deux tiers sont des scripts tiers.
- Les scripts côté client représentent un écosystème de fonctionnalités fragile mais dynamique, avec un grand nombre de parties prenantes.
- Il y a des meilleures pratiques de base pour la sécurité côté client. Cependant, les complexités et les défis posés par la sécurité côté client feront augmenter la demande en solutions de sécurité d'entreprise pour ce vecteur de menace.

Actions recommandées

- Les solutions disponibles sur le marché varient considérablement selon les fonctionnalités. L'objectif principal des acheteurs est de sécuriser leur système opérationnel sans toutefois le perturber.
- Pour de nombreux fournisseurs, la visibilité et le contrôle côté client restent un domaine inconnu et complexe. Les nouveaux venus sur le marché devront envisager de construire leurs propres solutions ou bien d'acquérir des capacités existantes ou de s'y associer.
- De nombreuses entreprises du secteur informatique manquent d'informations concernant les scripts ou les environnements côté client. Peu d'entre elles comprennent véritablement les problèmes de sécurité. Pour cela, il est nécessaire d'étudier le marché en profondeur, à travers des démonstrations, des recherches, des démonstrations de faisabilité et des versions d'essai.

Source : IDC, 2021

Avril 2021, IDC N °US47623221

NOUVELLES EVOLUTIONS ET DYNAMIQUES DU MARCHE

Ces perspectives du marché d'IDC fournissent une analyse du vecteur de menace, des solutions émergentes et de l'avenir du marché du pare-feu applicatif Web (WAF, Web Application Firewall) côté client.

Akamai, Cymatic, PerimeterX et Tala Security ont ouvert une nouvelle voie en étendant la protection WAF aux réponses aux menaces côté client. Les scripts côté client représentent un vecteur de menace émergent et le marché de la sécurité évolue pour répondre à ce besoin.

Ces solutions de sécurité sont appelées *« WAF côté client », anti-script* ou *protection contre les scripts*, mais la terminologie peut prêter à confusion. Imaginez les options suivantes :

- Le terme de WAF évoque un ensemble spécifique de contrôles qui s'appliquent aux applications Web, bien que les scripts côté client constituent par nature un point de contrôle différent dans le modèle de sécurité des applications.
- Le terme « *WAF côté client* » est utile, dans le sens ou il établit un lien avec un contrôle de sécurité bien établi dans le WAF, tandis que « *protection contre les scripts* » est flou et porte à confusion en comparaison.
- Le terme « *anti-script* » généralise et laisse entendre que tous les scripts sont une technologie indésirable, imparfaite ou tout bonnement malveillante. En réalité, les scripts représentent un outil précieux et puissant dans l'architecture des applications.

Dans l'ensemble, IDC se réfère à ces solutions sous le terme de « WAF côté client », principalement en raison de la familiarité associée au WAF. En outre, ce terme permet d'étendre les types de menaces côté client au-delà des scripts.

Introduction

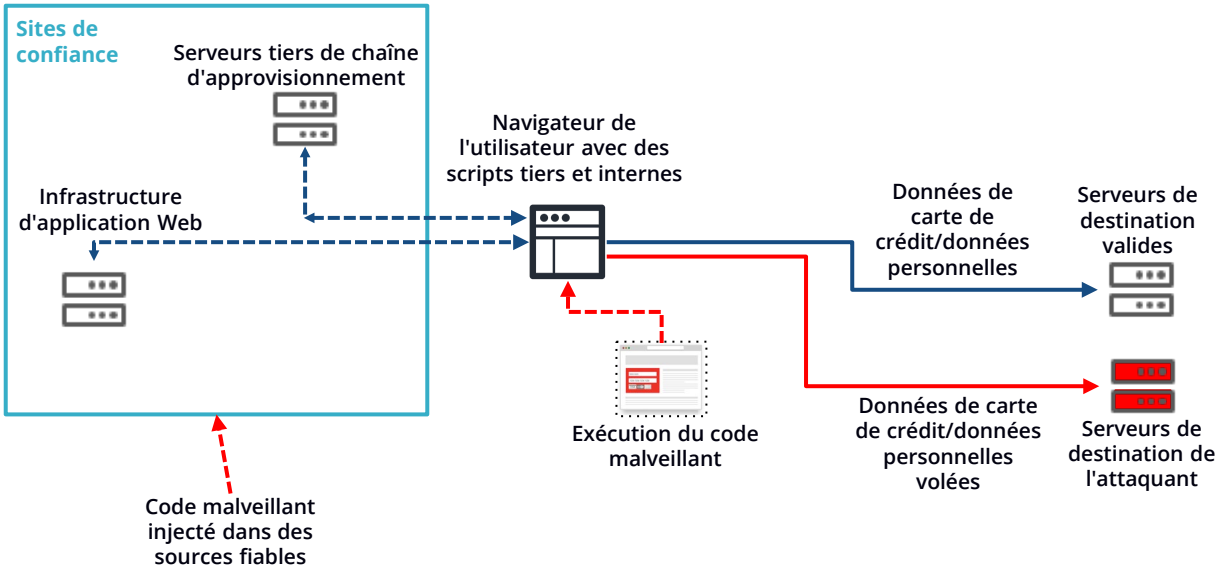
Une nouvelle technique de vol de données de carte de paiement a vu le jour en 2018 et a été attribuée au groupe de hackers Magecart. Les attaques de Magecart ont exploité un nouveau vecteur de menace : les scripts qui s'exécutent dans les navigateurs clients. Une fois la campagne d'attaque détectée, les enquêtes ont démontré que le groupe Magecart avait compromis pendant des mois les sites Web de grandes entreprises en ligne, telles que Ticketmaster, NewEgg et British Airways.

La campagne Magecart a utilisé des attaques côté client pour effectuer des vols de données en ligne, ou web skimming (également appelé vol de données de cartes bancaires ou détournement de formulaires). Le web skimming est l'un des types d'attaques les plus fréquemment observées de ce vecteur de menace, mais on rencontre également des attaques par point d'eau (watering hole) ou de cryptojacking (minage de cryptomonnaie malveillant). L'objectif de ces attaques contre la sécurité client peut varier, mais d'une manière générale, elles visent à engendrer des campagnes de vol de données, qui entraînent des violations de données massives et à long terme.

La figure 2 montre un aperçu du cycle de vie d'une attaque côté client. Notez que le code malveillant s'exécute dans le navigateur, loin des protections offertes par un WAF. En outre, un code malveillant peut être injecté à la fois dans des sources tierces et internes.

FIGURE 2

Anatomie d'une attaque de type web skimming (dans le navigateur)



Source : Akamai, 2021

Dynamique du marché

Le WAF côté client est un marché naissant, avec un fort potentiel de croissance. Cette technologie répond à un vecteur de menace émergent qui résulte d'un changement dans les pratiques de développement d'applications. Ces dernières années, les fonctionnalités des applications se sont déplacées des serveurs vers les clients et les tendances indiquent que cela devrait continuer. Le passage des fonctionnalités du serveur au client déleste le serveur des exigences de performances, ce qui permet aux utilisateurs finaux de bénéficier de meilleures performances et d'une expérience plus interactive. Résultat : les scripts sont des outils de plus en plus populaires pour améliorer les expériences interactives en ligne. Ils sont utilisés pour de nombreuses applications légitimes, telles que le suivi, l'analytique, l'expérience utilisateur et la sécurité. Ils sont omniprésents dans les sites Web d'aujourd'hui, qui contiennent environ une quinzaine de scripts différents voire plus, selon certaines estimations.

De plus, en raison de la simplicité de JavaScript , des personnes qui ne sont pas des professionnels de l'informatique se sont également mises à créer des scripts. Les scripts permettent aux unités commerciales extérieures au service informatique de créer et d'insérer du code dans les ressources Web à différentes fins. Les scripts facilitent également l'intégration et l'insertion de services tiers. Toutefois, leur sécurité reste largement négligée, en particulier parmi les entreprises qui continuent de se concentrer sur des outils essentiels comme le WAF.

Dans l'ensemble, la menace n'est pas bien comprise. Les violations les plus répandues dans cette catégorie sont axées sur les scripts tiers. La campagne de Magecart fournit un exemple pertinent. Dans ce cas, les pirates informatiques de Magecart avaient accès au code d'un fournisseur partenaire de l'entreprise ciblée et ont pu insérer du code malveillant dans des scripts considérés comme étant de confiance. Certaines entreprises semblent considérer qu'il suffit de déplacer les zones vulnérables pour faire face à ce vecteur de menace. La sécurisation d'un site Web contre les nombreuses et diverses menaces auxquelles sont confrontées les grandes entreprises en ligne est déjà compliquée, et il peut sembler injuste de devoir également prendre en compte les vulnérabilités des systèmes partenaires. Les scripts tiers sont les plus problématiques, car les services informatiques manquent de visibilité ou de contrôle sur le code, les mises à jour ou les modifications de leurs partenaires.

Malheureusement, le web skimming n'est qu'une partie du problème, car les scripts tiers ne représentent qu'une partie des scripts présents sur la plupart des pages Web. Pour référence, les chercheurs d'Akamai ont estimé qu'environ 67 % des scripts proviennent de tiers. En fin de compte, la plupart des pages Web constituent un écosystème de scripts de parties prenantes internes et de tiers. Ces systèmes internes peuvent également faciliter la tâche du code malveillant si les serveurs sont piratés.

Il existe certaines meilleures pratiques susceptibles de réduire les risques. Un contrôle plus strict des scripts tiers est un bon début. La mise en place d'examens réguliers du code et de tests d'application est également une pratique judicieuse. En outre, les entreprises du secteur informatique peuvent exploiter des technologies comme Subresource Integrity (SRI) pour hacher et détecter les modifications apportées aux scripts. Bien que ces options fournissent une base de protection nécessaire, l'histoire a montré que les auteurs de menaces sophistiquées utilisent constamment des tactiques complexes et intelligentes pour éviter la détection. Le recours à la technologie SRI et à d'autres pratiques constitue ainsi un point de départ utile mais limité contre les attaques avancées.

Par ailleurs, il est peu probable que les acteurs malveillants interrompent leurs efforts sans y être contraints. Depuis les méfaits très médiatisés de Magecart, les pirates informatiques ont apporté de nombreuses modifications à leurs attaques. Ils peuvent par exemple cibler les réseaux publicitaires de manière à d'injecter du code malveillant via des bannières publicitaires. D'autres tactiques incluent le ciblage de référentiels de code comme GitHub. Ces référentiels incluent des bibliothèques Open Source et des extraits de code qui sont généralement réutilisés et approuvés par de nombreuses entreprises pour être utilisées dans leurs applications Web. Ces sources de confiance représentent alors un moyen potentiel d'injecter des scripts malveillants dans des sites Web autrement sûrs.

Chaque fournisseur aborde le problème de façon légèrement différente. Les solutions sur le marché sont en grande partie déployées via des balises JavaScript, ce qui permet d'insérer la fonction de sécurité avant l'exécution des scripts. À partir de cette étape, les solutions divergent radicalement. Les fonctionnalités de base comprennent généralement la visibilité et le mappage des scripts et des communications (par ex : source et destination). Des fonctionnalités supplémentaires incluent la gestion des failles de sécurité, l'application des règles, ainsi que la détection des activités malveillantes et des événements suspects. Des fonctionnalités plus avancées sont possibles, comme le chiffrement des clés et des données intégrées, le brouillage de code, les environnements de test et d'autres mesures défensives. Pour l'instant, l'approche semble être de fournir une visibilité et une automatisation suffisantes des fonctionnalités de sécurité principales. Si des mesures de détection plus sophistiquées peuvent être bienvenues au fil du temps, l'accent continue d'être mis sur la fourniture d'une sécurité suffisante, sans perturber l'expérience de l'utilisateur final ni « endommager » les fonctionnalités du site Web.

Exemples de fournisseurs

Il existe actuellement quelques offres commerciales de WAF côté client, de portée et de capacité différentes. Un petit nombre de spécialistes sont présents sur le marché, notamment Digital.ai (anciennement Arxan), Source Defense, Cymatic, Tala Security et ChameleonX (racheté par Akamai en 2019). D'autres entreprises proposent de vastes gammes de solutions de sécurité applicative Web. Par exemple, Akamai a lancé Page Integrity Manager en 2020, dans le cadre de son approche visant à fournir une protection contre les attaques multivecteur via une gamme global de solutions de sécurité des applications Web et des API. De même, PerimeterX a lancé son offre en 2019 en complément de sa solution de gestion des bots d'entreprise. Un nouveau venu sur le marché est Cloudflare, qui a introduit sa nouvelle solution en mars 2021. IDC note que ces entreprises ont de l'expérience dans la gestion des bots, ce qui les aide peut-être à mieux comprendre les signaux de sécurité côté client. Il est difficile de bien gérer les bots et les meilleures solutions exploitent généralement plusieurs techniques (y compris JavaScript) pour détecter et classer les comportements des bots.

Les attaques côté client peuvent être difficiles à détecter. Cependant, une fois détectées, ces menaces sont très claires en termes de coûts financiers pour les entreprises touchées et leurs clients. Par exemple, ces types de violations de données peuvent souvent être mesurés en fonction du nombre de dossiers clients volés. Les concurrents existants ont démontré un haut degré d'efficacité dans la détection et l'atténuation des menaces basées sur des scripts. Les cybercriminels sont donc forcés de reconcentrer leurs efforts sur d'autres domaines, ce qui se traduit par un jeu du chat et de la souris dans l'industrie. L'objectif des pirates est de trouver des sites Web non sécurisés ou présentant des failles de sécurité qu'ils pourraient attaquer. Malgré la médiatisation des attaques de Magecart, la prise en compte de ce vecteur de menace sur le marché reste faible, ce qui permet aux acteurs malveillants de trouver de nouvelles cibles. Il est fort probable que le grand public prenne de plus en plus conscience de ce vecteur de menace, ce qui stimulera la demande et attirera de nouvelles entreprises sur le marché dans les années à venir.

Stratégies de marché

Les menaces côté client seront un défi pour les grandes entreprises en ligne tant que les cybercriminels considèreront ce vecteur d'attaque comme rentable. Cependant, ce type d'attaque est plus ciblé que celles de diffusion de masse, telles que les attaques par logiciel rançonneur. Cela prendra un certain temps pour la plupart des entreprises ciblées de détecter et d'atténuer les attaques basées sur des scripts. Sensibiliser davantage le marché à ces problèmes peut également prendre du temps et nécessiter des efforts. Les fournisseurs doivent relever le défi de sensibiliser le public par le biais de l'éducation continue, de démonstrations et de tests de démonstration de faisabilité.

De plus en plus d'entreprises lanceront probablement leurs propres produits et fonctionnalités. Akamai a lancé Page Integrity Manager il y a un an pour traiter la surface d'attaque grandissante créée par les scripts chargés dans les navigateurs, où les informations d'identification personnelle (PII) sont soumises et accessibles. Les menaces côté client se sont également multipliées en 2020 au niveau des navigateurs, à mesure que l'utilisation d'Internet pour les transactions s'est accélérée dans le contexte de la COVID-19.

Cloudflare est le dernier fournisseur arrivé sur le marché, introduisant une nouvelle solution appelée Cloudflare Page Shield. Avant cela, Cloudflare traitait ce vecteur de menace par le biais d'un partenariat technologique avec Tala Security.

Si Cloudflare a décidé de développer ses propres fonctionnalités de sécurité côté client, IDC note que cette approche n'est peut-être pas aussi facile à suivre pour d'autres. Pour la plupart des fournisseurs du marché, le développement de capacités de WAF côté client a été précédé par des techniques de détection des bots qui exploitent les clients JavaScript. Les anciennes solutions WAF ne possèdent pas ces capacités, ni aucune autre expérience avec le code côté client.

Pour les fournisseurs qui renforcent leurs gammes de produits de sécurité des applications Web et des API, l'acquisition de solutions spécialisées peut être la meilleure manière de se mettre sur un pied d'égalité avec la concurrence. L'acquisition par Akamai de ChameleonX est un exemple des avantages potentiels que représente l'association de technologies dédiées et de l'évolutivité fournie par le cloud. Page Integrity Manager protège désormais plus de 3,7 milliards de pages consultées chaque mois, en analysant 6,4 milliards d'exécutions de scripts chaque jour. Environ 40 millions d'interactions suspectes et malveillantes avec les utilisateurs finaux sont observées chaque semaine, ce qui permet à Akamai de fournir des notifications en temps réel, une analyse des causes profondes, des mesures d'atténuation immédiates, ainsi que la création de règles d'automatisation.

LE POINT DE VUE D'IDC

Les attaques côté client constitueront une faille de sécurité croissante tant que les cybercriminels percevront le vecteur d'attaque comme rentable, ce qui pourrait être le cas pendant de nombreuses années. Une raison importante à cela est le fait que le vecteur de menace côté client n'est pas bien compris. Traditionnellement, les solutions WAF fonctionnent en analysant le trafic des applications Web ciblant le serveur Web. À mesure que JavaScript a gagné en popularité au fil des années, de nombreuses fonctionnalités ont migré vers le navigateur client. Pourtant, beaucoup d'entreprises négligent ces faits ou n'ont pas mené d'évaluation appropriée des risques et des implications en matière de sécurité de cette migration des fonctionnalités Web vers le navigateur client.

Le fait que ce type d'attaques soit plus ciblé que les attaques diffusées à grande échelle, comme les attaques par logiciel rançonneur, contribue encore davantage à la confusion qui règne sur le marché.
Par exemple, la plupart des entreprises connaissent bien les types d'attaques traitées par les solutions WAF et de protection contre les attaques DDoS. Le risque de sécurité présenté par les bots indésirables ou malveillants gagne également en notoriété. Toutefois, des domaines plus récents, comme la sécurité des API et la sécurité côté client, représentent des zones de risque émergentes qui ne sont tout simplement pas visibles et présentent donc un risque important, comme la moitié immergée d'un iceberg (voir Figure 3).

FIGURE 3

L'iceberg de la sécurité des applications Web et des API

Source : IDC, 2021

Une fois qu'une entreprise comprend le vecteur de menace potentiel, le processus de catalogage et de compréhension des scripts exécutés dans un environnement informatique complexe avec plusieurs domaines, pages et applications Web peut être une tâche herculéenne. Au moment des attaques de Magecart, le processus de détection des scripts malveillants injectés se résumait à un examen manuel de chaque ligne du code pour détecter les modifications. Le processus est désormais rationalisé, car les chercheurs comprennent les enjeux sous-jacents et les meilleures pratiques. Toutefois, la plupart des entreprises ciblées prendront du temps pour détecter et atténuer les attaques basées sur des scripts, car comprendre le vecteur de menace est chronophage, sans compter le temps nécessaire à l'identification des failles de sécurité ou des failles d'exploitation existantes. En outre, le vecteur de menace est une cible mobile, car 75 % des scripts sont modifiés chaque trimestre. Chaque nouvelle modification représente une opportunité d'introduire de nouvelles vulnérabilités et de nouveaux codes malveillants.

Malgré tout, il est crucial d'agir rapidement. Les violations connues dues aux attaques côté client ont eu une longue durée de vie, fournissant aux attaquants une avance de plusieurs mois. Au moment des attaques, un nombre incalculable de numéros de cartes de crédit ainsi que d'autres données personnelles ont été volés. Une fois qu'une attaque est détectée, les attaquants sont libres de fermer boutique et de tout recommencer avec leur prochaine victime. En résumé, les attaques côté client ont un délai de détection considérable, et ce déséquilibre représente un avantage énorme pour les

cybercriminels,
lequel doit absolument être réduit.

Le temps est donc le plus gros obstacle pour le secteur de la sécurité quant à l'éducation et à l'amélioration de la sensibilisation des acheteurs à ce problème. Les fournisseurs doivent relever le défi de sensibiliser le public par le biais de l'éducation continue, de démonstrations et de tests de démonstration de faisabilité. Par exemple, Akamai propose une version d'essai gratuite de son offre Page Integrity Manager. La solution fournit une vue d'ensemble de l'écosystème des scripts des pages Web ciblées, ainsi qu'une analyse des différents scripts, vulnérabilités et facteurs de risque. D'autres fournisseurs proposent également des versions d'essai, des démonstrations et des ressources éducatives.

IDC a salué ces approches. Rien ne traduit mieux l'urgence d'une situation ou la valeur et l'efficacité d'une solution de sécurité qu'une démonstration de faisabilité. Pour les fournisseurs, l'avantage que représente une éventuelle conversion à des services payants est clair. Les acheteurs en bénéficient également considérablement, en obtenant une visibilité accrue sur un vecteur de menace qui constitue traditionnellement un angle mort pour la plupart des entreprises.

À plus long terme, IDC surveillera le marché du WAF côté client afin de comprendre son impact sur les marchés établis tels que le WAF, l'atténuation des attaques DDoS, la gestion des bots et la prévention des fraudes en ligne. Une fois l'angle mort de la sécurité côté client résolu, des discussions plus approfondies seront nécessaires sur l'impact de la visibilité et des capacités de mise en œuvre du côté client, telles qu'un point de contrôle de la sécurité.

EN SAVOIR PLUS

Recherches associées

- *IDC FutureScape: Worldwide Future of Trust 2021 Predictions* (IDC N° US46912920, octobre 2020)
- *Pervasive Application Edge Defense: An application-based Framework for Trust* (IDC N° US46810219, septembre 2020)
- *IDC Market Glance: Software-defined Secure Access, 2Q20* (IDC N° US46291520, mai 2020)
- *Worldwide Internet Defense Forecast, 2020-2023: Infrastructure and Application Security Drive Business Value* (IDC N° US46022619, février 2020)
- *Security Convergence at the Edge: Emerging Pervasive Data Defense and Response Platforms* (IDC N° US46075520, février 2020)

Synopsis

Ces perspectives du marché d'IDC fournissent une analyse du vecteur de menace, des solutions émergentes et de l'avenir du marché du WAF côté client. Peu d'entreprises du secteur informatique disposent d'une compréhension complète des menaces ciblant les scripts côté client qui s'exécutent dans leurs environnements Web. Les cybercriminels utilisent les scripts côté client comme un moyen d'exécuter du code malveillant subrepticement pour engranger d'énormes sommes d'argent, sans risquer de se faire prendre. Dans les années à venir, à mesure que ce vecteur de menace sera de plus en plus répandu, la demande de solutions WAF côté client pour entreprise devrait augmenter de manière constante.

« Le script côté client est la prochaine frontière en matière de sécurité. Les cybercriminels ne cessent de rechercher des failles de sécurité lucratives et ils ont trouvé une nouvelle vulnérabilité dans les systèmes de sécurité numérique des entreprises », déclare Christopher Rodriguez, directeur de recherche, Produits et stratégies de sécurité réseau, IDC.

À propos d'IDC

International Data Corporation (IDC) est le premier fournisseur mondial d'informations commerciales, de services de conseils et d'événements pour les marchés des technologies de l'information, des télécommunications et des technologies grand public. IDC aide les professionnels de l'informatique, les dirigeants d'entreprise et la communauté des investisseurs à prendre des décisions d'achats de technologies et de stratégie d'entreprise basées sur des faits. Plus de 1 100 analystes d'IDC fournissent une expertise mondiale, régionale et locale sur les opportunités et tendances technologiques et sectorielles dans plus de 110 pays à travers le monde. Depuis 50 ans, IDC fournit des informations stratégiques pour aider nos clients à atteindre leurs objectifs commerciaux clés. IDC est une filiale d'IDG, leader mondial dans le secteur des médias, de la recherche et des événements technologiques.

Siège social mondial

5 Speen Street
Framingham, MA 01701
États-Unis
508 872 8200
Twitter : @IDC
idc-community.com
www.idc.com