https://www.reflectiz.com/blog/all-you-need-to-know-about-web-skimming-attacks/

Tout ce que vous devez savoir sur les attaques d'écrémage Web (Web skimming)

Magecart & Web-skimming

Avr 26, 2021 Temps de lecture: 7 minutes

L'écrémage Web, également connu sous le nom d'écrémage numérique, est une technique de piratage qui cible les entreprises numériques en manipulant des applications Web côté client non surveillées et compromises. Habituellement, ces attaques sont lancées en plaçant stratégiquement du code JavaScript malveillant (JS) sur les pages de paiement et de paiement du site Web où les utilisateurs sans méfiance remplissent leurs informations personnelles et financières. Bien que l'on trouve couramment sur les sites Web de commerce électronique, les services bancaires, financiers, les soins de santé, le tourisme et d'autres plates-formes de services électroniques sont également ciblés aujourd'hui.

Les attaques d'écrémage Web existent depuis un certain temps, mais elles ont occupé le devant de la scène après l'attaque Magecart de 2018 contre British Airways, qui a coûté à la société plus de 1 milliard de dollars en efforts d'atténuation, amendes pour violation du RGPD et autres coûts. Alors que les pirates continuent d'utiliser les scripts Magecart pour voler des informations de

carte de paiement, les nouvelles techniques utilisées par les cybercriminels ont transformé cette activité malveillante en un phénomène mondial.

Les cybercriminels ont maintenant commencé à placer des écumeurs Web et des scripts Magecart dans des images, des logos et des favicons pour les ajouter à des bibliothèques JavaScript populaires ou, dans certains cas, les cacher dans des widgets de sites Web tels que la fenêtre de chat en direct que vous pouvez trouver sur chaque site Web eService aujourd'hui. Les vecteurs d'attaque se multiplient, obligeant les RSSI et DSI à repenser leur stratégie de sécurité. Examinons de plus près cette tendance inquiétante.

Qu'est-ce que l'écrémage Web ?

Avant de nous plonger dans les détails de la lutte contre les menaces d'écrémage Web, il est important de savoir ce qu'elles sont réellement. Web Skimming est une technique de piratage où l'attaquant viole la page de paiement ou de paiement des sites Web en injectant un script malveillant ou un logiciel malveillant via les applications tierces utilisées par le site Web. Les informations de carte de crédit et les informations personnelles sont collectées, souvent sans être détectées.

Il existe de multiples variantes d'attaques d'écrémage Web qui exploitent la complexité du site Web moderne, mais il existe deux principaux points d'entrée utilisés aujourd'hui.

- **Attaques directes –** Ce point d'entrée implique l'implantation de code d'écrémage (malware) directement sur le site Web qui va être exploité. Les pirates peuvent ensuite exploiter les failles zero-day ou automatiser les identifiants de connexion (également connus sous le nom d'attaques par force brute) pour localiser les bons détails et informations d'identification de l'administrateur. Il faut dire que l'exécution de ces attaques n'est pas facile et nécessite beaucoup de planification préalable et de coordination.

- **Attaques de la chaîne d'approvisionnement des logiciels de site Web –** Ces attaques deviennent populaires en raison de l'utilisation intensive de tiers (plus de 60 en moyenne sur les sites de commerce électronique aujourd'hui). Bien que ces tiers améliorent rapidement les fonctionnalités, ils créent également de nouvelles dépendances. Les logiciels malveillants sont injectés dans le site d'hébergement tiers de confiance, après quoi la charge utile est exécutée via tous les sites Web utilisant l'application Web.

Les solutions et outils de sécurité des applications traditionnels ne sont pas entièrement efficaces contre ces attaques, car le logiciel malveillant est intégré au code tiers d'origine. En outre, les méthodes d'obscurcissement évoluent et rendent la vie plus difficile aux RSSI et aux équipes de sécurité. Le résultat final – « l'action » se déroule du côté du client, où les victimes sans méfiance ignorent totalement ce qui se passe jusqu'à ce qu'il soit trop tard et que la violation se soit produite.

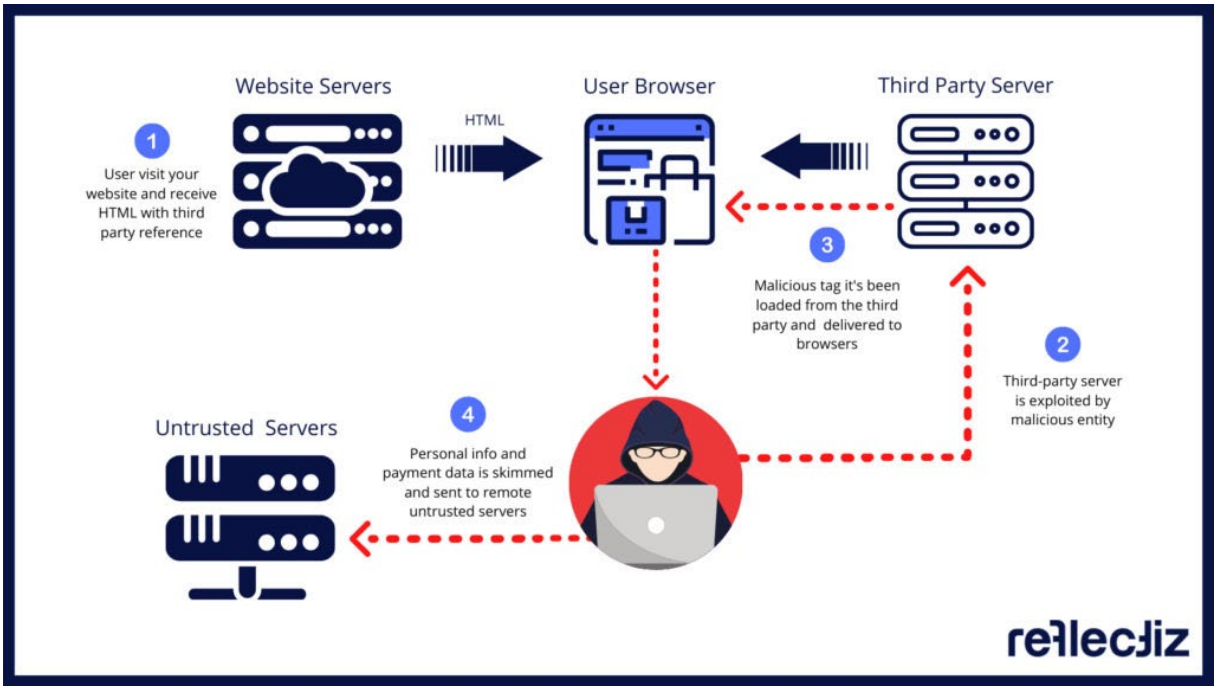
Comment l'écrémage Web est-il exécuté ?

Les attaques d'écrémage Web sont essentiellement des attaques de la chaîne d'approvisionnement logicielle qui peuvent atteindre des centaines ou des milliers de sites Web à l'aide de l'application Web tierce exploitée.

Apparenté: ***Rétrospectivement: l'attaque SolarWinds***

Étant donné que le code HTML / JavaScript tiers est livré au site Web à partir d'un référentiel complètement différent sur lequel le propriétaire du site Web n'a aucun contrôle (et ne peut pas surveiller directement), les pirates ciblent ces serveurs Web tiers. Cela permet à l'attaquant d'accéder sans autorisation à toutes les bibliothèques tierces. Il s'agit ensuite d'injecter le code d'écrémage dans l'un des fichiers JavaScript existants et de le cacher.

Désormais, lorsqu'un utilisateur / client du site Web ouvre le site Web dans un navigateur ou un appareil mobile, le code malveillant est téléchargé sur le navigateur de l'utilisateur avec le code tiers légitime. Étant donné que le code malveillant est téléchargé à partir des serveurs tiers, le propriétaire du site Web ne dispose d'aucun journal ou indication indiquant l'existence du code malveillant ou même quelque chose de suspect se produit.



Comment l'écrémage Web est-il exécuté ?

Une fois la charge utile exécutée, le script commence à collecter les numéros de carte de paiement et les informations personnelles de toutes les données utilisateur saisies et les envoie aux cybercriminels, qui sont ensuite vendus sur le Web sombre. Les cibles les plus courantes – les pages de paiement et de paiement sur les sites Web. Pour aggraver les choses, les exploits d'écrémage Web continuent souvent de persister pendant de longues périodes avant d'être découverts par le propriétaire du site Web.

Voici quelques techniques d'écrémage Web « effrayantes » utilisées récemment:

- **La campagne Gocgle** – Chercheurs en sécurité ont exposé la campagne Gocgle en 2020, qui a été essentiellement actif à partir de la fin de 2019, tout comme la pandémie de COVID-19. Cette campagne malveillante a été adaptée autour de produits Google tels que G-Analytics et utilise la similitude de dénomination troublante pour tromper les utilisateurs et les équipes de sécurité. Cet écumeur est probablement encore actif sur des centaines de sites Web.

Exploits Gocgle – Imitant la suite G-Analytics

- **Pipka** – Nous ne pouvons pas continuer sans mentionner le Pipka exploit, probablement le skimmer JavaScript le plus notoire de mémoire récente, qui a été exposé par l'équipe Visa Payment Fraud Disruption (PFD) à la fin de 2019. Pourquoi est-ce si dangereux? Cet écumeur furtif a la capacité dangereuse de se retirer du code HTML une fois l'exécution terminée. Un véritable cauchemar de RSSI.

L'écrémage Web : un phénomène grandissant

Le risque d'attaques d'écrémage Web continue de sévir dans toutes les entreprises en ligne aujourd'hui. Par conséquent, toute entreprise numérique qui traite des informations personnelles et des données de carte de paiement ne peut plus ignorer ces menaces qui se multiplient. C'est avant de mentionner les réglementations de confidentialité telles que GDPR, CCPA et 23 NYCRR 500, qui mettent maintenant beaucoup l'accent sur l'optimisation des normes de sécurité des applications tierces.

Magecart (un sous-ensemble de l'écrémage Web) est extrêmement bien connu dans les cercles de sécurité et est devenu une cyber-pandémie mondiale aujourd'hui. Il existe plus d'une douzaine de groupes Magecart (que nous connaissons officiellement) qui utilisent les outils Magecart illicites disponibles sur le dark web et coexistent sous le même nom de groupe. Il y a même des groupes financés politiquement qui ont été retracés jusqu'à Le régime dictatorial de la Corée du Nord dirigé par Kim Jong-un.

Le saviez-vous?
Selon un récent Symantec Les attaques d'écrémage Web sont détectées après 46 jours en moyenne, de nombreux sites Web restant infectés pendant plus d'un an.

Voici quelques-uns des plus grands cas d'écrémage Web de ces dernières années:

1. **Violation de Ticketmaster UK** En juin 2018, Ticketmaster a annoncé qu'il avait été victime d'une violation de carte de paiement qui, après une inspection plus approfondie, s'est avérée être une campagne massive

d'écrémage Web. Les attaquants ont compromis Inbenta, un fournisseur d'applications Web tiers, qui a été exploité pour placer des écumeurs sur d'autres sites Web tiers. Pour aggraver les choses, les outils de sécurité traditionnels n'ont pas réussi à détecter le problème en temps réel. L'enquête qui a suivi l'atteinte à Inbenta a également révélé des éléments de preuve indiquant que le groupe Magecart se concentrait sur la compromission d'autres fournisseurs tiers pour voler davantage de données de cartes de paiement et de renseignements personnels. En juillet 2018, les enquêtes de la campagne Magecart ont révélé une compromission de plus de 800 sites Web de commerce électronique et de services électroniques du monde entier provenant de multiples secteurs.

Apparenté: ***L'ICO inflige une amende de 1,25 million de livres sterling à Ticketmaster UK***

---

2. **British Airways (BA)**L'assaut s'est poursuivi. En septembre 2018, BA a reconnu qu'environ 380 000 informations de carte de paiement, y compris les noms, adresses, détails de carte bancaire et codes CVV de 500 000 clients, avaient été compromises. Cette violation, qui s'est produite entre août et septembre 2018, a de nouveau été attribuée au tristement célèbre groupe Magecart, qui a ajouté un logiciel malveillant à la page d'information sur la récupération des bagages sur le site Web de BA. Le porte-parole de British Airways a également confirmé que l'écumeur Web utilisé sur le site Web était également utilisé pour exploiter le navigateur de l'application mobile. La violation de la vie privée des clients par British Airways s'est avérée être un désastre du RGPD. Les régulateurs du RGPD de l'Union européenne ont imposé une amende de 230 millions de dollars et l'ont attribuée aux mauvaises mesures de sécurité sur le site Web de British Airways. L'imposition d'amendes sévères rend les organisations commerciales responsables de toute violation de données causée par les fournisseurs de services tiers sur leur site Web.
3. **Newegg**L'écrémage Web a également été attribué à la compromission du détaillant en ligne populaire – Newegg. Newegg est un site marchand en ligne populaire qui compte des millions d'utilisateurs enregistrés. Le site Web vend de l'électronique grand public, du divertissement, des appareils ménagers intelligents et des produits de jeu. L'écumeur de cartes de paiement lié à Magecart s'est avéré actif entre le 14 août 2018 et le 18 septembre 2018.Bien que le nombre exact de victimes et de dossiers volés soit encore inconnu, le fait que l'écumeur ait été actif pendant près d'un mois nous permet de supposer que l'attaque a fait un grand nombre de victimes. Les experts en sécurité ont souligné que les utilisateurs

d'applications de bureau et mobiles ont été affectés par l'attaque, qui n'a pas non plus été détectée par la boîte à outils AppSec traditionnelle que la société mettait en œuvre à l'époque.

Apparenté: ***Réaliser le CCPA avec la sécurité des applications tierces***

Sécurité des applications tierces : rendre l'activité numérique à nouveau sûre

Les technologies de sécurité traditionnelles telles que les pare-feu d'applications Web (WAF), les systèmes de prévention des intrusions (IPS) et la politique de sécurité du contenu (CSP) ne parviennent pas à détecter les problèmes tiers. Un autre fait troublant est que de nombreux fournisseurs tiers intègrent leurs propres applications tierces (quatrièmes parties) pour utiliser des fonctions critiques. Cela ajoute encore plus de dépendances et de vulnérabilités dans le mélange.

Les tiers et les quatrièmes parties aident les sites Web à obtenir des fonctionnalités prêtes à l'emploi à de nombreux niveaux - analyse, marketing, ventes, développement et productivité. Mais il faut noter que ces applications externes créent également de sérieux angles morts en matière de sécurité car elles changent et modifient constamment la dynamique de dépendance sous le capot, ce que les solutions traditionnelles de sécurité des applications ne peuvent pas surveiller en raison de leur nature statique.

La surveillance continue des applications tierces avec des informations en temps réel devient la méthode la plus efficace pour obtenir une visibilité totale et prendre le contrôle de votre site Web. C'est le seul moyen d'empêcher l'écrémage Web et les attaquants Magecart d'exploiter les codes JavaScript et iFrame intégrés à votre site Web. Il n'y a pas de meilleur moyen d'appliquer la sécurité des applications tierces pour une expérience en ligne plus sûre.

Apparenté: ***Effets des quatrièmes parties sur la cybersécurité sur les sites Web***

Conclusion

Alors que les entreprises en ligne continuent de se développer à un rythme rapide, avec de plus en plus de services numérisés, il est devenu important de rester sécurisé et conforme (RGPD, CCPA, HIPAA, etc.) en tout temps. La sécurité des données va désormais bien au-delà du simple chiffrement des communications et du partage de données en toute sécurité. Les sites Web de commerce électronique et les fournisseurs de services électroniques doivent s'assurer que leur écosystème tiers est régi et géré correctement.

Les entreprises doivent se rendre compte que la responsabilité de la mise en œuvre sécurisée par des tiers incombe à l'organisation et non aux fournisseurs tiers. Les outils AppSec traditionnels et les solutions de gestion des risques sont toujours bons à avoir, mais seuls la surveillance et le suivi continus des applications Web tierces vous aideront à maintenir une posture de sécurité et de conformité solide contre l'écrémage Web, Magecart et les attaques de la chaîne d'approvisionnement logicielle.