- Blog Magecart et Web-skimming

Nouvelle étude de cas : Cyberattaque cachée et récupération de Leeds United

Onn Nir

Gestionnaire de contenu

- 24 juin 2025
- 7 min de lecture

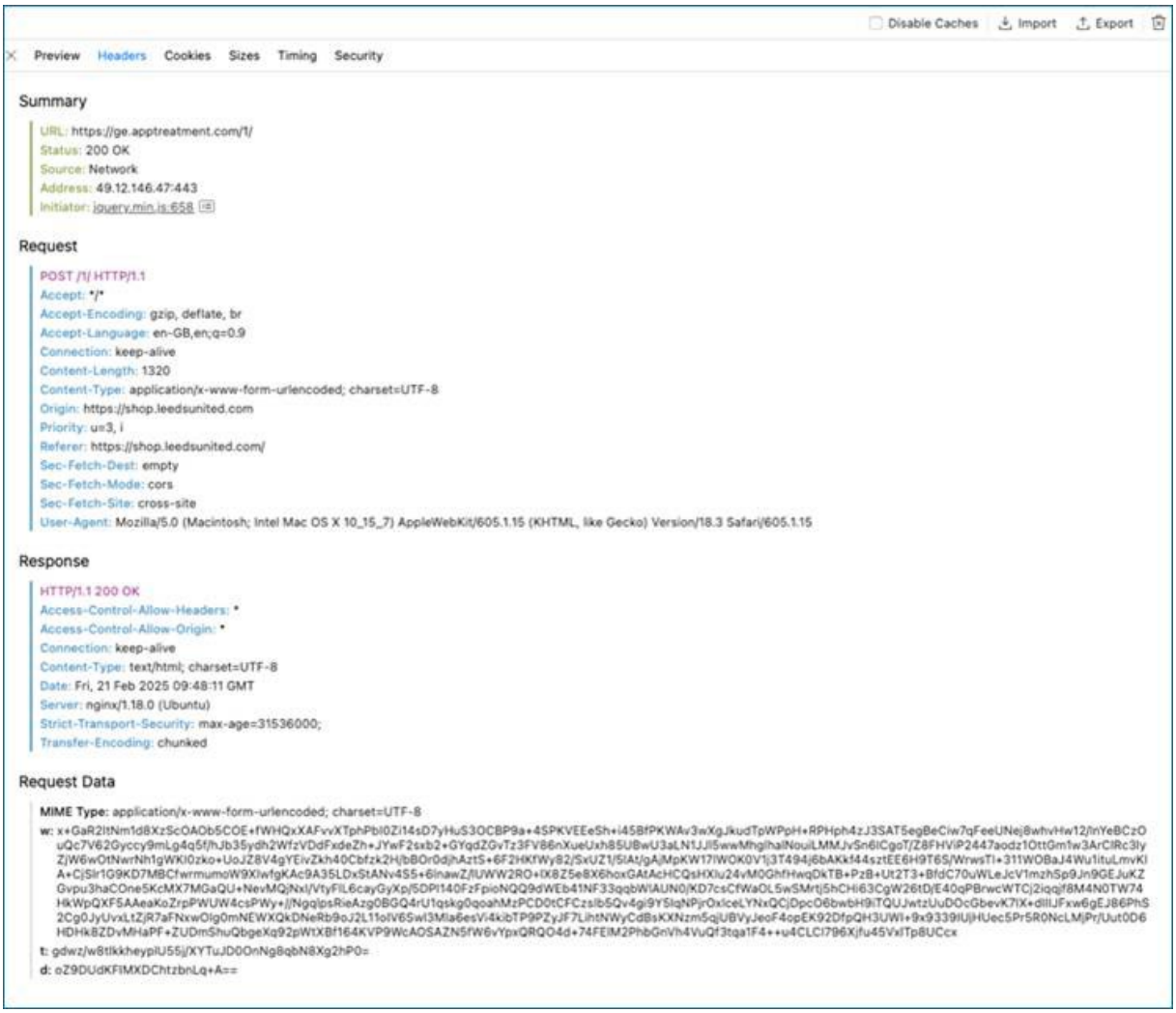
Découvrez comment un code malveillant a infiltré la boutique en ligne du club de football Leeds United par le biais de services tiers de confiance, mettant en évidence la menace universelle de Magecart et le risque de la chaîne d'approvisionnement dans l'écosystème Web moderne. Apprenez-en plus sur cet incident dans notre prochain Webinaire en direct avec Graham Peck, responsable informatique et sécurité.

L'attaque

À 10 heures du matin le 24 février, deux policiers locaux de la cybercriminalité sont arrivés à Elland Road, domicile de l'équipe de football de la Premier League anglaise, Leeds United. Ils étaient là pour informer Graham Peck, responsable informatique et sécurité, que le National Cyber Security Centre (NCSC) du Royaume-Uni avait remarqué quelque chose d'étrange. Alors qu'ils surveillaient les communications entre un serveur malveillant et une autre entreprise six jours auparavant, ils avaient observé que ce serveur recevait du trafic de la boutique en ligne de Leeds United.

Le NCSC a essayé de déterminer le type de données transmises, mais celles-ci étaient cryptées et donc illisibles. Cependant, ils ont localisé le script sur le site Web de Leeds United responsable de son

envoi. Pour comprendre sa fonction, ils ont déployé un paquet de test non crypté, qui a révélé que le script récupérait les données de carte de crédit – un signe clair d'une violation de données.



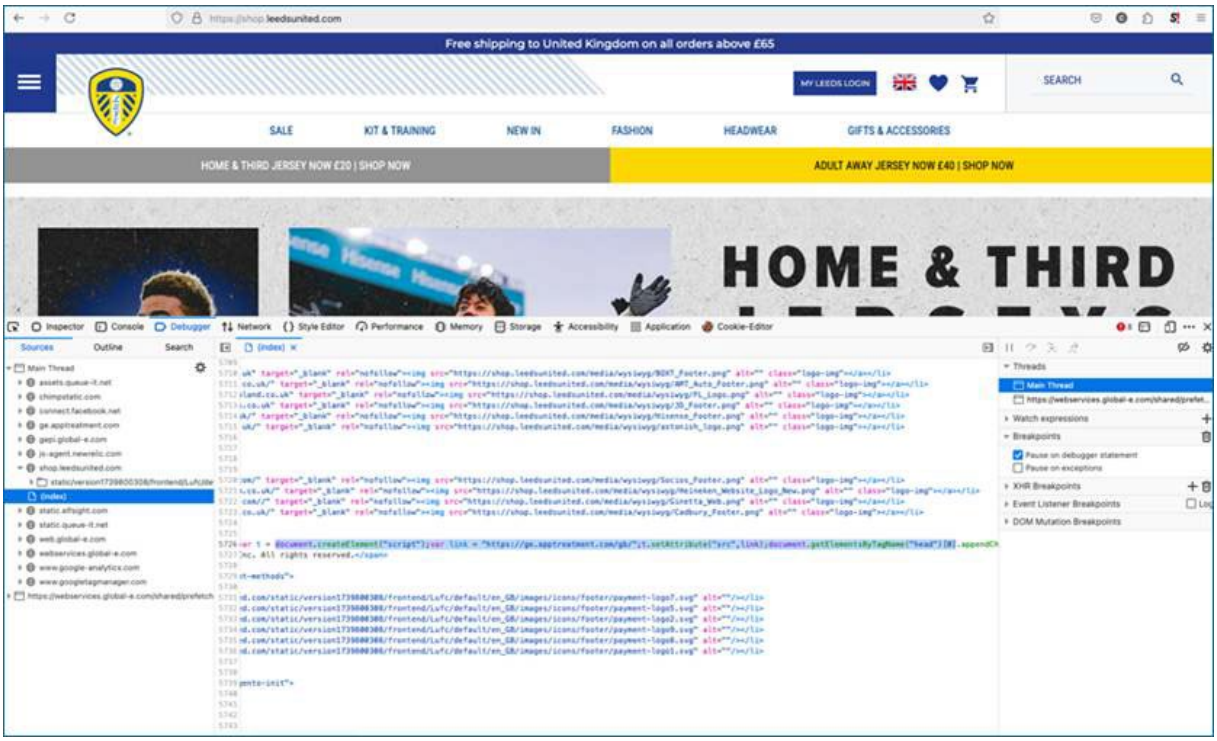
Les mystérieux attaquants avaient déployé un skimmer JavaScript malveillant intégré à la page de paiement de la boutique en ligne du club. Les principaux éléments techniques de l'attaque sont les suivants :

- **Exploitation de scripts par des tiers :** Ils ont compromis un composant de service tiers (peut-être un widget de chat, un outil d'analyse ou un module publicitaire) chargé sur le site Web, ce qui leur a donné accès à la fonctionnalité de paiement.
- **Exécution côté client :** Le code malveillant s'est exécuté dans les navigateurs des utilisateurs, contournant efficacement les mesures de sécurité traditionnelles côté serveur qui étaient impuissantes à identifier la violation.
- **Vol immédiat de données :** Les détails de paiement des clients ont été transmis en temps réel via des canaux cachés à des serveurs contrôlés par les attaquants.

La réponse

La réponse initiale a été rapide, comme l'a expliqué Graham. « Nous avons fermé le site Web afin de pouvoir enquêter et localiser le code responsable. Dès que nous l'avons trouvé, nous l'avons retiré. De plus, les acteurs malveillants externes avaient laissé derrière eux leurs adresses IP, ce qui nous a

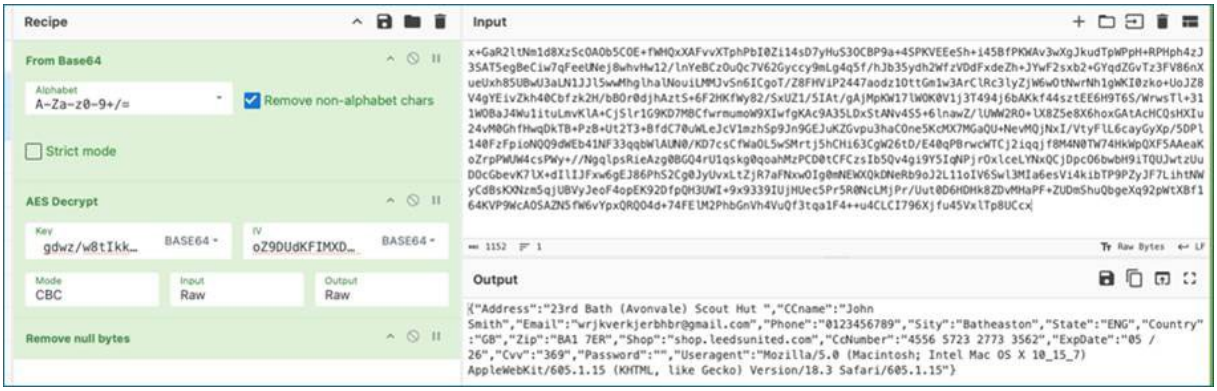
permis de mettre en place des bloqueurs sur Cloudflare et plusieurs autres plateformes pour bloquer l'accès à partir d'un serveur spécifique qui était actuellement lié au site Web.



L'enquête

Après avoir trouvé un code problématique sur le site Web, Graham a fait appel à une société de sécurité pour effectuer une analyse numérique, en passant au peigne fin les journaux d'enregistrement pour comprendre précisément ce qui s'était passé. Ils ont établi que l'atteinte avait commencé à 20 h le 18 février et s'était terminée à 11 h le 24 février. Un petit nombre de transactions ont été effectuées sur le site Web au cours de cette période, ce qui soulève des questions sur le nombre de transactions compromises.

De plus, Graham a reconnu la nécessité d'une solution proactive pour surveiller plus efficacement les composants tiers. Reflectiz, une solution spécialisée dans la gestion de l'exposition sur le Web, était déjà à l'horizon en tant qu'outil potentiel pour aider Leeds United à prévenir de telles attaques à l'avenir. Alors que l'équipe s'efforçait de contenir la brèche, l'outil allait bientôt révéler des failles de sécurité plus profondes.



À ce stade, il convient d'apprécier la chance qui a tourné en faveur de Leeds lors de cet incident :

- Ils ont eu de la chance que le NCSC ait repéré la transmission de données exfiltrées de sa boutique en ligne.
- Ils ont eu de la chance que le script malveillant n'ait été conçu que pour cibler les détails de la carte de crédit, de sorte que les clients utilisant Apple Pay et PayPal n'ont pas été affectés.
- Ensuite, il y a la fenêtre de six jours entre le moment où la violation se produit et la possibilité pour l'entreprise de la fermer. La plupart des entreprises n'ont pas cette chance. Selon le rapport 2024 d'IBM sur le coût d'une violation de données, le temps moyen nécessaire pour identifier une violation de données dans tous les secteurs est de 194 jours, le confinement prenant 64 jours supplémentaires, un cycle de vie de 258 jours au cours duquel les attaquants sont libres d'infliger toutes sortes de dégâts.

Une menace universelle dans tous les secteurs

Bien que cette attaque ait ciblé la plateforme de commerce électronique d'un club de football de Premier League, la technique utilisée – l'injection de code malveillant par le biais de services tiers – constitue une menace pour les organisations de tous les pays et de tous les secteurs. Qu'ils soient dans le commerce de détail, la santé, la finance, l'éducation ou le gouvernement :

- L'écrémage électronique peut compromettre toute application Web qui traite des données sensibles des clients ou des informations de paiement.
- Les vulnérabilités de la chaîne d'approvisionnement, y compris les dépendances de tiers, créent des failles de sécurité critiques dans les écosystèmes Web.

Graham Peck, responsable de l'informatique de Leeds United, explique : « La National Crime Agency nous a dit qu'il y avait une poussée concertée des acteurs de la menace dans les industries du divertissement. Les États hostiles font tout ce qu'ils peuvent pour semer la discorde et perturber les activités de leurs ennemis, en particulier les entreprises ayant une grande valeur commerciale et une chaîne d'approvisionnement étendue, comme Marks & Spencer. Nous avons récemment entendu parler d'une attaque où un gang de ransomware espionnait les communications internes d'une victime. Un membre du personnel a innocemment mentionné qu'ils avaient une couverture d'assurance cyber d'une valeur de 5 millions de livres sterling, c'est donc ce que le gang a exigé.

La résolution

Même si la violation a été rapidement isolée et que les clients concernés ont été informés, c'était loin d'être la fin du parcours de sécurité de Leeds United ; Ce n'était que le début. L'attaque de survol du Web a mis en évidence un énorme angle mort qui nécessitait une attention urgente. Cela a conduit le club à mettre immédiatement en œuvre Reflectiz dans l'ensemble de son infrastructure Web.

Dans la foulée, Reflectiz a révélé de graves lacunes dans la sécurité préalable du site de vente au détail. Graham a expliqué que Leeds United avait externalisé la gestion de son site Web de vente au détail, une pratique courante qui ne fonctionne qu'avec un tiers vraiment digne de confiance et professionnel – ce qui n'était pas leur expérience. La société précédente était responsable de tous les mécanismes de sécurité, mais n'offrait aucune visibilité ou contrôle, laissant Graham « voler à l'aveuglette » avec un actif de plusieurs millions de livres sterling destiné au public.

Avantages post-Reflectiz

Visibilité et preuves immédiates

Après avoir déployé Reflectiz, Graham a pu mieux comprendre les failles de sécurité du site Web de Leeds United. Cela lui a permis de présenter des preuves claires aux parties prenantes. « Il y avait beaucoup de tiers qui avaient trop d'informations, et il n'y avait pas d'en-têtes de sécurité. Tous les éléments de base que l'on aurait pu s'attendre à voir en place dans le cadre d'un site Web de vente au détail n'étaient pas là. Avec cet outil, j'ai pu leur montrer. Je pouvais leur envoyer des preuves que je n'avais pas auparavant, même si je ne suis pas développeur. Je n'ai pas besoin de passer d'un programme à l'autre. Je peux simplement exporter des informations sur ce que je vois et leur dire ce qu'il faut corriger pour réduire mon niveau de risque.

Opérations rationalisées et alertes intelligentes

Reflectiz a contribué à rationaliser le processus de surveillance de la sécurité, en réduisant les tâches manuelles tout en fournissant des alertes opportunes et exploitables. « Dans un test d'intrusion typique, vous devriez passer du temps à créer des comptes clients, mais c'était beaucoup plus facile. Il a été opérationnel très rapidement et surveillé en permanence », a expliqué Graham. Contrairement à certains outils de sécurité qui inondent les équipes de faux positifs, cette solution a permis à Leeds United de se concentrer sur les menaces importantes. « De nombreux systèmes disent qu'il s'agit de très bons produits de sécurité. Mais dans la plupart des cas, ce qu'ils font, c'est qu'ils créent tellement de bruit à partir d'alertes que vous finissez par courir le risque de ne pas être en mesure de voir quand vous avez un problème, ou comme nous l'avons dit, « Vous ne pouvez pas voir les bois pour les arbres ». Grâce à cet outil, nous pouvons repérer rapidement les problèmes et y réagir, ce qui réduit considérablement le temps et les efforts consacrés aux fausses alertes.

Un analyste de la sécurité toujours disponible

L'outil a fourni une surveillance continue et automatisée, ce qui a été particulièrement précieux pour la petite équipe de sécurité de Leeds United. « C'est presque comme si vous aviez un analyste de sécurité supplémentaire sur place. J'ai maintenant l'esprit tranquille qu'il existe un système qui surveille constamment tout ce qui est anormal sur le site Web tiers. Cette solution s'est facilement connectée à ma configuration de sécurité existante et était prête à l'emploi. Cela a également révélé des risques cachés de la chaîne d'approvisionnement dont j'ignorais l'existence.

Principaux points à retenir

- Les services tiers et les vulnérabilités de la chaîne d'approvisionnement constituent un risque majeur en matière de cybersécurité dans l'écosystème numérique actuel.
- Les attaques d'e-skimming (comme Magecart) peuvent compromettre les informations sensibles des clients si des composants tiers sont exploités.
- Une détection précoce et une action rapide peuvent réduire considérablement l'ampleur et les dommages d'une violation de données.
- La mise en œuvre d'outils de gestion de l'exposition Web peut fournir une visibilité continue sur l'état des applications Web et prévenir de futures attaques.
- Les entreprises doivent régulièrement évaluer leur posture de sécurité, en particulier lorsqu'elles externalisent la gestion de sites Web critiques à des tiers.

Demandez un replay de notre webinaire exclusif et regardez Graham Peck discuter de cet incident en détail et partager les principaux points à retenir pour d'autres organisations en adressant une email à contact@amcsoft.fr

Reflectiz est distribué en France par AMC SOFT
https://amcsoft.fr
Email : contact@amcsoft.fr
Tel : +33680741316