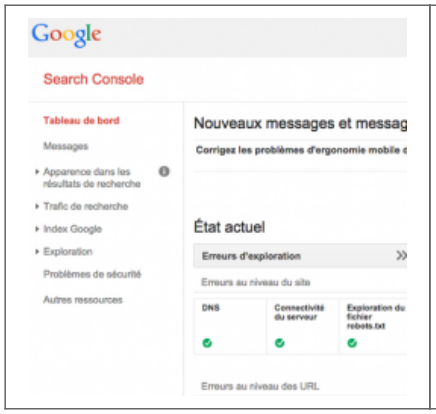
Les pirates du SEO s’attaquent à Google Search Console | Le Net Expert Informatique



Les pirates du SEO s’attaquent à Google Search ConsoleInformatique

Le spécialiste en sécurité Sucuri alerte sur la recrudescence d'attaquants qui se font passer pour les véritables propriétaires de sites web sur le service Google Search Console afin de détourner le trafic vers des pages et des sites infectés. Ces pirates vont jusqu'à supprimer les webmasters légitimes de la liste des propriétaires identifiés des sites.

Il arrive de plus en plus souvent que des pirates ayant compromis des sites web s'identifient eux-mêmes comme l'un des propriétaires de ces sites dans la Search Console de Google, constatent les chercheurs de la société Sucuri, spécialisée dans la sécurité sur Internet. Dans certaines circonstances, cela permet à ces attaquants d'agir plus longtemps sans être détectés. Précédemment connu sous le nom de Webmaster Tool, le service Search Console permet aux administrateurs de sites web de voir et comprendre où se situent leurs sites dans les résultats du moteur de recherche. Au-delà de ce type d'analyses, il permet aux webmasters de proposer de nouveaux contenus à indexer et de recevoir des alertes lorsque Google détecte des malwares ou des problèmes de spam sur leurs pages web (des mots-clés répétés abusivement). C'est particulièrement important car les infections entraînent des pertes de trafic et de réputation. Les utilisateurs qui cliquent sur des liens de résultats de recherche conduisant vers des sites hébergeant des malwares ou du contenu spammé reçoivent des avertissements inquiétants jusqu'à ce que ces sites soient nettoyés par leurs propriétaires.
Sur les comptes utilisateurs de la Search Console, Google permet en fait à plusieurs personnes de se dire propriétaires d'un site. Cela n'a rien d'inhabituel puisqu'il y a généralement plusieurs intervenants. Les spécialistes des outils de recherche, notamment, sont souvent distincts des administrateurs de sites et tous utilisent les données de la Search Console dans leurs rôles respectifs. Il y a plusieurs façons de se faire identifier comme propriétaire, mais la plus simple consiste à charger un fichier HTML avec un code unique pour chacun dans le dossier racine du site. Or, de nombreuses failles qui permettent aux attaquants d'injecter du code malveillant sur les pages web leur ouvrent aussi des portes pour créer des fichiers sur les serveurs web sous-jacents. Ces pirates peuvent notamment exploiter des vulnérabilités pour s'identifier comme l'un des propriétaires du site dans Search Console en créant les fichiers HTML requis.

Les attaquants exploitent des techniques de BHSEO

De tels abus deviennent de plus en plus courants. Sucuri cite pour preuve les multiples posts publiés à ce sujet sur les forums par les propriétaires de sites. Dans l'un des cas signalés, un webmaster a trouvé plus de 100 « utilisateurs vérifiés » dans sa console, note l'expert en sécurité Denis Sinegubko dans un billet. De nombreux pirates utilisent des sites compromis pour créer de fausses pages, tromper le classement des résultats de recherche et diriger le trafic vers d'autres pages à contenu dupliqué, ce qui permet aux attaquants d'exploiter des techniques d'optimisation de type BHSEO (black hat search engine optimization).

Devenus propriétaires vérifiés sur des sites compromis, les pirates peuvent alors suivre tranquillement les performances de leurs campagnes BHSEO sur le moteur de recherche de Google. Ils peuvent aussi soumettre de nouvelles pages de spams à indexer plus rapidement plutôt que de devoir attendre que ces pages soient naturellement découvertes par les robots de recherche. Ils peuvent aussi recevoir des alertes de Google si les sites sont identifiés comme étant compromis et, pire encore, ils peuvent éjecter les propriétaires légitimes des sites du service Search Console.

Des notifications qui passent entre les mailles

Lorsqu'un utilisateur est dit « vérifié » pour un site, les propriétaires de ce site vont recevoir une notification par email de Google. Cependant, ces messages peuvent facilement passer à travers les mailles du filet. Par exemple, s'ils sont envoyés vers une adresse mail qui n'est pas utilisée très souvent, ou bien s'ils sont noyés au milieu d'autres notifications reçues lors d'une journée très chargée en messages, ou encore s'ils arrivent pendant une période de congés. Dans ces cas-là, si les propriétaires légitimes n'ont pas consulté ces notifications et pris immédiatement des mesures, les attaquants peuvent alors les enlever de la liste de vérification du service Search Console en supprimant purement et simplement les fichiers de vérification HTML du serveur. Cela ne déclenchera aucune notification vers les véritables détenteurs du site, souligne Denis Sinegubko, de Sucuri.

Par la suite, si Google détecte un site web compromis et alerte automatiquement ses propriétaires identifiés comme tels, seuls les attaquants recevront cette notification. Ils pourront alors enlever temporairement du site les portes dirigeant vers leurs faux sites avant d'adresser à l'équipe antispam de Google une requête pour faire débloquer le site dans les résultats de recherche. Après quoi, ils pourront tranquillement remettre leur doorways vers différentes adresses URL, explique le chercheur de Sucuri.

Utiliser les méthodes alternatives de Google pour s'identifier

Si les véritables propriétaires ne sont plus identifiés comme tels, cela leur prendra un certain temps pour se rendre compte de ce qui s'est produit. Il est même possible qu'ils ne s'en aperçoivent pas. Pendant ce temps, les pirates continuent à exploiter leurs sites à leurs propres bénéfices. Et même si les administrateurs légitimes repèrent les faux propriétaires, il n'est pas toujours simple de s'en débarrasser. Les chercheurs de Sucuri ont vu de quelle façon les attaquants procédaient quelquefois en s'appuyant sur des règles de réécriture des URL dans le fichier de configuration htaccess et en générant dynamiquement des pages. Dans ces cas-là, les robots de vérification de Google détectent les fichiers HTML requis même si ceux-ci n'existent pas sur le serveur et si les vrais administrateurs ne peuvent pas les trouver.

Pour se préparer à de telles attaques, les webmasters peuvent prendre diverses mesures, indique Denis Sinegubko dans son billet. En premier lieu, ils doivent s'assurer qu'ils sont bien « vérifiés » comme propriétaires sur tous leurs sites web (en incluant les sous-domaines) dans la Search Console, même s'ils n'utilisent pas souvent ce service. Il existe trois méthodes alternatives de vérification acceptées par Google : à travers un fournisseur de noms de domaine, via un code de suivi Google Analytics ou, encore, avec une portion de code JavaScript à coller dans les pages. Cela évitera que des pirates suppriment leurs propres « vérifications » simplement en détruisant les fichiers correspondants sur le serveur. Enfin, à chaque fois qu'ils reçoivent des notifications de « new owners » de la part de Google, les webmasters doivent impérativement les contrôler en détail. « Dans la plupart des cas, cela signifie qu'ils ont un accès complet à votre site », avertit Denis Sinegubko. « Il faut alors intervenir sur toutes les failles de sécurité et supprimer tous les contenus malveillants que les attaquants auraient pu créer sur votre site », pointe le chercheur de Sucuri.

Source :
http://www.lemondeinformatique.fr/actualites/lire-les-pirates-du-seo-s-attaquent-a-google-search-console-62333.html?utm_source=mail&utm_medium=email&utm_campaign=Newsletter