Sécurité des blogs et des sites PHP : Protéger Wordpress et les sites similaires contre les pirates

Par Christian Funk, Senior Virus Analyst chez Kaspersky Lab

Rueil-Malmaison – 13 août 2013

Il serait aujourd'hui impossible d'imaginer Internet sans blogs ni contenus dynamiques. Grâce aux systèmes de gestion de contenu dynamique (CMS) et de blogs clés en main, quiconque souhaite publier quoi que ce soit sur le Web peut mettre en place l'infrastructure nécessaire en y consacrant un minimum de temps et de travail.
L'un des systèmes les plus connus est WordPress, qui a récemment fêté son dixième anniversaire. Sans ce logiciel, la blogosphère actuelle n'aurait probablement jamais connu un tel succès. WordPress et les autres systèmes de blogs sont faciles à installer et, grâce à des modules d'extension (« plug-ins »), peuvent être enrichis de nouvelles fonctions et de différents thèmes. Le problème est que de nombreux utilisateurs en oublient qu'il ne s'agit pas d'un simple site Web, mais d'un système élaboré de gestion de contenu offrant aux auteurs d'attaques une multitude d'opportunités d'infecter et de détourner les blogs.

Comme tout autre logiciel, un système CMS présente des points faibles. C'est ainsi que, depuis 2004, plus de 200 vulnérabilités ont été détectées dans WordPress, dont 47 ont permis à des pirates d'exécuter leur propre code sur le système. Selon le site CVE Details[1], il existe au moins 43 malwares connus exploitant des failles de WordPress[2]. La situation est comparable pour les autres systèmes. Le site Drupal[3], par exemple, recense plus de 100 vulnérabilités connues, tandis que Typo3[4] en cite pas moins de 150. Il est cependant à noter que les versions plus récentes de ces logiciels savent se protéger contre les attaques exploitant de telles vulnérabilités répertoriées. Le livre blanc prend l'exemple de WordPress car la plupart des conseils et procédures qui y figurent peuvent facilement s'appliquer aux autres systèmes.

Attaques massives

En raison de son succès, WordPress est la cible de multiples attaques massives automatisées. En avril 2013, celles-ci ont atteint leur paroxysme lorsque des pirates ont utilisé un botnet comprenant plus de 90 000 ordinateurs afin de percer les mots de passe des administrateurs d'installations WordPress.

Une autre tactique consiste à exploiter des vulnérabilités connues[2], lesquelles deviennent notoires lorsque, par exemple, des développeurs de systèmes de blogs publient des mises à jour et documentent les modifications apportées. Les auteurs d'attaques créent alors des programmes qui explorent le Web à la recherche d'installations vulnérables. A l'instar des robots des moteurs de recherche, ceux-ci progressent de lien en lien jusqu'à ce qu'ils aboutissent à un site Web présentant une vulnérabilité connue. Lorsque c'est le cas, le malware lance son attaque pour accéder au blog, puis il se met en quête d'autres installations vulnérables, et ainsi de suite. Quand, par exemple, vous

lisez des gros titres tels que « 100 000 installations de XX piratées », il est probablement question d'une attaque automatisée.

Une fois qu'un pirate a réussi à s'infiltrer dans un blog, il dispose des mêmes droits d'accès que tout autre administrateur et les exploitent pleinement. Les attaques massives visent généralement à créer un réseau de serveurs destinés, soit à stocker des données pour des malwares, soit à infecter leurs visiteurs. C'est ce qui motive les auteurs d'attaques à prendre le contrôle d'un aussi grand nombre de sites Web et de blogs que possible. Qu'il s'agisse de blogs d'entreprise, de blogs de voyage ou même privés, tous ces sites recèlent des ressources sur lesquelles ces criminels ont des visées, à savoir des visiteurs, du trafic et de la bande passante. Les pirates mettant en œuvre ces stratégies opèrent généralement de la même manière que les créateurs de botnets : leur objectif est de faire en sorte que les exploitants légitimes des sites ne remarquent pas leurs actions et laissent donc ceux-ci accessibles aux attaques le plus longtemps possible.

Le cas particulier du défacement

Ce n'est toutefois pas le cas des attaques de « défacement », qui consistent à accéder à un site Web pour en manipuler ou effacer le contenu original et le remplacer par un autre. Ce contenu de substitution se compose en général de messages politiques dénonçant ce que des militants considèrent comme des injustices flagrantes. Les auteurs de ces attaques tendent à être des apprentis programmeurs ou pirates, se servant de boîtes à outils prêtes à l'emploi pour infliger un vandalisme numérique maximum.

Pour les exploitants de sites, les attaques de ce type sont souvent plus graves que les autres, du fait qu'elles ont pour objectif de susciter le plus de médiatisation (ou de dégâts) possible. Souvent, leurs auteurs effacent ou remplacent tous les contenus qu'ils trouvent sur le serveur.

Attaques ciblées

Contrairement aux infections massives, les attaques ciblées ne visent généralement qu'un ou deux sites Web. Elles ont pour but de causer un préjudice à une entreprise ou de préparer d'autres attaques en vue de prendre le contrôle d'un blog ou d'un site. A l'image des attaques de phishing, leurs auteurs identifient souvent leurs cibles de manière exhaustive et longtemps à l'avance, se préparant à frapper dès lors qu'une opportunité se présente.

Que faire en cas d'attaque

Si vous avez été la cible d'une attaque, gardez votre sang-froid et évitez de surréagir. La première chose à faire est d'arrêter le serveur touché et de remplacer le site Web par une simple page HTML statique. Si vous comptez engager des poursuites, vous devrez faire appel à un expert légal qui rassemblera des preuves exploitables par la justice.

Tous les utilisateurs touchés doivent en premier lieu analyser leurs systèmes locaux à l'aide d'un scanner de virus[5]. C'est en effet le seul moyen de vérifier leur intégrité. Contactez ensuite un expert technique, par exemple chez l'hébergeur de votre site Web, pour vous aider à « nettoyer » votre blog car il est souvent extrêmement difficile de repérer et de supprimer tous les éléments infectés. Les pages de support de votre hébergeur constituent un bon point de départ. WordPress, par exemple, propose un FAQ complet sur le sujet[6]. L'étape suivante consiste à changer tous les mots de passe[7], ce qui protègera l'accès à l'interface Web ainsi qu'aux serveurs FTP et aux bases de données.

Les utilisateurs disposant de sauvegardes récentes verront leur tâche relativement facilitée puisqu'il leur suffira d'effacer purement et simplement le contenu de leur site Web et de leur base de données. Après quoi, il faudra recréer le blog à partir de zéro puis réinstaller la dernière sauvegarde en date. La marche à suivre est notamment expliquée par WordPress [8].

Pour les utilisateurs dépourvus de sauvegardes, cela sera plus difficile. Tout d'abord, il convient d'enregistrer la totalité des données sur un système local.
Si l'attaque est de type « défacement », les données les plus importantes sont peut-être encore en place. En recherchant sur le Web le message affiché par le pirate ou le nom de ce dernier, accompagné de mots-clés tels que « contre-mesures », « nettoyer » ou « aide», vous pourrez trouver des conseils utiles, notamment des instructions indiquant comment (au moins) restaurer votre site Web.

Protection et prévention

Mieux vaut prévenir que guérir. Quelques règles simples peuvent considérablement réduire la surface d'exposition de la cible et prévenir efficacement les attaques massives ou de défacement.
La règle la plus important est d'appliquer les mises à jour. Toute nouvelle version d'un système de blog, d'un plug-in ou d'un thème doit être installée dès sa publication. Une fois qu'une vulnérabilité corrigée a été documentée, les pirates vont l'ajouter à leur arsenal. Cependant, des criminels peuvent en effet être au courant de certaines failles avant même que les détails n'en soient rendus publics.

L'étape suivante consiste à renforcer l'application Web. Il s'agit, au moyen de méthodes éprouvées, de réduire encore la vulnérabilité. WordPress a compilé une documentation complète[9] sur le sujet, et des instructions similaires sont disponibles pour les autres systèmes. En cas de doute, effectuez une recherche sur le nom de votre système, accompagné de mots-clés tels que « le nom du système + renforcer ».

Les conseils suivants restent valables pour la plupart des systèmes :

- Masquez le numéro de version. Les auteurs d'attaques auront ainsi nettement moins de possibilités de déterminer, à l'aide de scripts automatiques, si le système n'est pas à jour.
- Ne vous servez pas d'un compte administrateur standard. Celui-ci est généralement très bien documenté, des criminels peuvent facilement le pirater. Mieux vaut donc le mettre en sommeil ou le désactiver une fois votre site Web installé et créer un nouveau compte spécial à cette fin.
- Mettez à profit les différents niveaux d'utilisateur disponibles. Chaque utilisateur n'a pas besoin d'un accès complet. Même si vous gérez seul votre blog, servez-vous d'un compte bénéficiant d'autorisations minimales pour effectuer les opérations quotidiennes. Un accès total n'est nécessaire que pour la mise à jour du système.
- Faites attention aux autorisations d'accès. Dans de nombreux cas, tous les administrateurs n'ont pas besoin d'un accès en lecture-écriture aux données du serveur Web. Concentrez-vous sur les autorisations nécessaires et adaptez-les à votre installation.
- Installez le moins de plug-ins possibles. Chacune de ces d'extensions risque en effet d'ouvrir une nouvelle porte donnant accès à votre système. Désactivez (ou mieux, supprimez) les modules superflus.
- Installez les mises à jour dès qu'elles sont disponibles. Assurez-vous également que tous les plug-ins et thèmes installés font l'objet d'un suivi actif par leur développeur : rien n'est pire que de se reposer sur un logiciel périmé.
- Utilisez des plug-ins de sécurité, qui constituent la seule exception à la règle « installez le moins d'extensions possible ». Ceux-ci peuvent souvent appliquer automatiquement nombre de meilleures pratiques et protéger votre blog contre les attaques.
- Effectuez des sauvegardes régulières au moyen des fonctions offertes par le système. Vous pourrez ainsi restaurer celui-ci plus rapidement après une attaque.

Protection des sites PHP

Toutes les entreprises n'ont pas besoin d'un système complet de gestion de contenu. Certaines optent plutôt pour un système PHP pour l'exploitation de leur site Web ou la fourniture de services. Ce type de système présente l'avantage de protéger les utilisateurs contre les attaques ciblant des vulnérabilités dans les plug-ins de blog. PHP est toutefois loin d'être une forteresse imprenable, c'est même tout le contraire. Depuis 2000, CVE Details[10] a recensé 340 vulnérabilités détectées et au moins 41 exploitées.
Les attaques sur PHP sont donc tout aussi courantes que sur les systèmes de blog. Dans la mesure où PHP constitue la base de pages et de systèmes interactifs, les attaques réussies procurent à leurs auteurs des autorisations complètes sur le système cible, où ils ont alors accès à un grand nombre de sites Web et de services.

Les applications PHP doivent donc elles aussi être protégées contre les visiteurs malveillants. La règle numéro un, en l'occurrence, est de veiller à ce que les composants soient à jour. Qu'ils se servent de PHP ou de programmes auxiliaires, par exemple ImageMagick, les administrateurs doivent installer les nouvelles versions dès que celles-ci sont disponibles. Cela permettra de colmater les failles connues et de réduire la vulnérabilité du système au minimum.

La deuxième étape consiste à renforcer l'installation PHP. Comme pour WordPress, il existe une mine d'informations et de ressources disponibles en la matière. La documentation officielle[11] fournit un point de départ et de multiples ressources en ligne peuvent s'obtenir grâce une simple recherche.

Conclusion

La protection des applications Web, qu'il s'agisse de blogs WordPress, de forums ou d'applications PHP personnalisées, doit être intégrée dans leur conception dès le départ. La sécurité informatique n'est pas une fonctionnalité qui peut venir se greffer a posteriori : elle ne saurait être véritablement efficace que si elle est d'emblée ancrée au plus profond du système.

Les utilisateurs qui ne se jugent pas capables d'accomplir toutes ces tâches ou qui tout simplement n'en ont pas le temps ne doivent pas pour autant renoncer à leur blog. Il leur faut cependant choisir avec soin leur hébergeur. Initialement, un prestataire offrant ce type de service, tel Wordpress.com, peut être suffisant. Il existe également des hébergeurs spécialisés dans l'exploitation sécurisée de ce type de site. Ceux-ci proposent souvent des installations en marque blanche, permettant d'intégrer votre blog en toute transparence dans le site Web de votre entreprise.

Sources :

[1] http://www.cvedetails.com/vendor/2337/Wordpress.html
[2] http://www.viruslist.com/de/analysis?pubid=200883806
[3] http://www.cvedetails.com/product/2387/Drupal-Drupal.html?vendor_id=1367
[4] http://www.cvedetails.com/vendor/3887/Typo3.html
[5] http://www.kaspersky.com/de/home_user
[6] http://codex.wordpress.org/FAQ_My_site_was_hacked
[7] http://www.kaspersky.com/de/news?id=207566607
[8] http://codex.wordpress.org/Restoring_Your_Database_From_Backup
[9] http://codex.wordpress.org/Hardening_WordPress
[10] http://www.cvedetails.com/product/128/PHP-PHP.html?vendor_id=74
[11] http://www.php.net/manual/de/security.php

À propos de Kaspersky Lab

Kaspersky Lab est le plus grand fournisseur privé de solutions de sécurité informatique dans le monde. La société est classée parmi les 4 premiers fournisseurs de solutions de sécurité informatique pour les particuliers à l'échelle mondiale. Tout au long de ces 15 années d'existence, Kaspersky Lab n'a cessé d'innover et propose aujourd'hui des solutions de sécurité de pointe à destination des* grands comptes, PME/TPE et *des particuliers*. Le groupe Kaspersky Lab est présent *dans près de 200 pays et territoires, offrant une protection à plus de 300 millions d'utilisateurs à travers le monde*. Site Web : http://www.kaspersky.com/fr/

** La société a été classée quatrième dans le classement IDC Worldwide Endpoint Security Revenue by Vendor, 2011. Ce classement a été publié dans le rapport IDC « Worldwide Endpoint Security 2012-2016 Forecast & Vendor Shares 2011 » (IDC #235930, juillet 2012). Le rapport classe les éditeurs de logiciels selon les revenus des ventes de solutions de sécurité en 2011.*

Pour en savoir plus : www.kaspersky.com/fr/
Pour plus d'informations sur l'actualité virale : http://www.securelist.com
Salle de presse virtuelle Kaspersky Lab : http://newsroom.kaspersky.eu/fr/

Contacts presse :
Agence onechocolate
Edouard Fleuriau Chateau / Morgane Rybka
edouardfc@onechocolatecomms.fr
morganer@onechocolatecomms.fr
Tél. +33 1 41 3 75 16/06