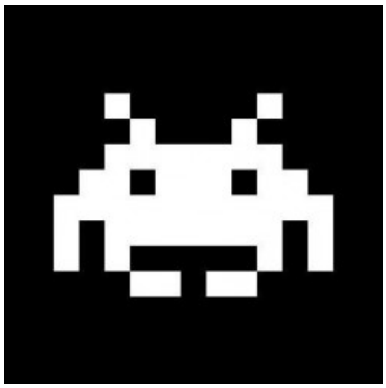
CryptoPHP – Plus de 23 000 serveurs web infectés



CryptoPHP – Plus de 23 000 serveurs web infectés

La propagation du backdoor CryptoPHP se fait par les plug-ins et les thèmes piratés pour les CMS WordPress, Joomla et Drupal.

Plus de 23 000 serveurs web ont été infectés par un backdoor baptisé CryptoPHP qui est arrivé avec les thèmes et les plug-ins piratés pour des systèmes de gestion de contenu très populaires, à savoir WordPress, Joomla et Drupal. CryptoPHP est un script malveillant qui permet des attaques à distance avec la possibilité d'exécuter du code délictueux sur des serveurs web et d'injecter du contenu inapproprié sur des sites web.

Selon le cabinet de sécurité néerlandais Fox-IT, qui a publié un rapport sur cette menace la semaine dernière, la porte dérobée est principalement utilisée pour l'optimisation de BHSEO (Black hat search engine optimization), une opération qui consiste à injecter des mots-clés et des pages indélicates sur les sites compromis afin de détourner les recherches effectuées par les moteurs traditionnels et pousser du contenu malveillant le plus haut possible dans les résultats de recherche.

Un backdoor profitant de la culture pirate des webmasters

Contrairement à la plupart des backdoors s'attaquant aux sites web, CryptoPHP ne s'installe pas en exploitant les vulnérabilités. Les hackers distribuent simplement des versions piratées des plug-ins et thèmes commerciaux pour Joomla, WordPress et Drupal et attendent simplement que les webmasters les téléchargent et les installent sur leurs propres sites web. Ces plug-ins et thèmes piratés intègrent le backdoor CryptoPHP. Les serveurs web infectés par CryptoPHP agissent comme un réseau de zombies. Ils se connectent à des serveurs de commande et de contrôle exploités par les hackers en utilisant un canal de communication chiffré et attendent les instructions.

Avec l'aide du Centre national de la cybersécurité du gouvernement néerlandais et d'organisations de lutte contre la cybercriminalité (Fondation Shadowserver, Abuse.ch et Spamhaus), Fox-IT a pris le contrôle des domaines de commande et de contrôle de CryptoPHP envoyant des instructions aux serveurs infectés pour recueillir des statistiques. Une opération connue sous le terme « sinkholing ».

Plus de 1000 sites web infectés en France

« Au total, 23 693 adresses IP uniques étaient reliés aux centres de contrôle », ont indiqué dans un billet de blog les chercheurs de Fox-IT. Cependant, le nombre de sites concernés est probablement plus élevé, parce que certaines de ces adresses IP correspondent à des serveurs d'hébergement web partagé qui ont plus d'un site infecté. Les cinq premiers pays infectés par CryptoPHP étaient les États-Unis (8657 adresses IP), l'Allemagne (2877 adresses IP), la France (1 231 adresses IP), les Pays-Bas (1008 adresses IP) et la Turquie (749 adresses IP).

Depuis la publication du rapport de Fox-IT sur CryptoPHP la semaine dernière, les hackers ont fermé les sites qui ont poussé les plug-ins et thèmes piratés pour en créer de nouveaux. Ils ont également introduit une nouvelle version de leur backdoor, peut-être dans une tentative d'échapper à la détection.

Les chercheurs Fox-IT ont publié deux scripts Python sur GitHub que les webmasters peuvent utiliser pour scanner leurs serveurs et leurs sites web à la recherche de CryptoPHP. Ils ont également fourni des instructions pour le supprimer sur leur blog, tout en notant que finalement il est préférable de complètement réinstaller son CMS afin de repartir sur une base saine.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.lemondeinformatique.fr/actualites/lire-plus-de-23-000-serveurs-web-infectes-par-cryptophp-59420.html?utm_source=mail&utm_medium=email&utm_campaign=Newsletter
Le rapport : https://foxitsecurity.files.wordpress.com/2014/11/cryptophp-whitepaper-foxsrt-v4.pdf
Article de Peter Sayer, IDG NS (adaptation Serge Leblal)