COMMUNIQUÉ DE PRESSE 30 avril 2013

ESET et Sucuri découvrent une faille sur les serveurs Apache

Le vers Linux/Cdorked.A: ouvre une porte dérobée affectant des milliers de sites Web

Les Pavillons-sous-Bois, le 30 avril 2013, les chercheurs d'ESET et leurs homologues de la société Sucuri, ont analysé une nouvelle menace pesant sur les serveurs Web Apache, le serveur web le plus connu et le plus utilisé dans le monde. La menace est une porte dérobée très complexe et furtive utilisée pour générer du trafic vers des sites malveillants hébergeant des packs d'exploits Blackhole. Les chercheurs ont nommé cette porte dérobée, Linux/Cdorked.A et considèrent qu'il s'agit de la backdoor Apache la plus sophistiqué repérée jusqu'alors.

À ce jour, les chercheurs d'ESET ont identifié des centaines de serveurs Web attaqués grâce au système de télésurveillance et d'analyse dans le Cloud ESET LiveGrid ®.

« *La porte dérobée Linux/Cdorked.A ne laisse pas de traces sur le disque dur autre que la modification d'un fichier "httpd", un processus démon utilisé par Apache. Toutes les informations relatives à cette backdoor sont stockées dans la mémoire partagée sur le serveur, ce qui rend difficile la détection et entrave son analyse*, » explique Pierre-Marc Bureau, expert en sécurité chez ESET.

En outre, le code Linux/Cdorked.A prend d'autres formes pour éviter la détection, à la fois sur le serveur Web compromis et sur les navigateurs des visiteurs. *« La configuration du backdoor est envoyée par l'attaquant en utilisant des requêtes HTTP qui ne sont pas seulement masquées, mais qui ne sont pas non plus enregistrées par Apache, ce qui réduit la probabilité de détection par les outils de surveillance conventionnels. La configuration est stockée dans la mémoire, ce qui signifie qu'aucune information de commande et de contrôle pour la backdoor n'est visible, ce qui rend complexe l'investigation,* » ajoute Righard Zwienenberg, chercheur principal chez ESET.

Très populaire et répandu, le kit d'exploit Blackhole utilise de nouvelles failles dites "Zéro day" qui permettent de prendre le contrôle d'un système lorsque l'internaute visite un site qui est infecté par le kit Blackhole. Lorsqu'une personne visite un serveur web compromis, il n'est pas simplement redirigé vers un site Web malveillant ; un cookie Web est installé dans le navigateur de sorte que le code backdoor ne l'y renvoie pas une seconde fois. Le cookie web n'est pas installé dans les pages de l'administrateur : le code malveillant vérifie l'origine du visiteur et, si ce dernier est redirigé vers la page Web à partir d'une adresse URL qui a certains mots clés, tels que "admin" ou "cPanel", aucun contenu malveillant n'est servi.

ESET invite les administrateurs système à contrôler dès que possible leurs serveurs et à vérifier qu'ils ne sont pas confrontés à cette menace. Un outil de détection gratuit comprenant des instructions détaillées sur la façon de vérifier la présence de cette backdoor et une analyse technique complète du code Linux/Cdorked.A sont disponibles sur le site WeLiveSecurity.com ; la nouvelle plate-forme d'ESET qui contient les dernières informations et des analyses sur les cyber-menaces et des conseils de sécurité utiles. (voir le lien : Linux/Cdorked blog post.)

D'autres informations sur le code Linux/Cdorked.A sont également disponibles à l'adresse de Sucuri blog

À propos d'ESET

Fondée en 1992, la société ESET est spécialisée dans la conception et le développement de logiciels de sécurité pour les entreprises et le grand public. Pionnier en matière de détection proactive des menaces véhiculées par l'Internet, ESET est aujourd'hui l'un des leaders dans ce domaine. En obtenant la 75ème récompense VB100 en septembre 2012, ESET NOD32 Antivirus détient le record mondial pour le nombre de récompenses Virus Bulletin (VB100), et n'a jamais manqué un seul ver ou virus «In-the-Wild" depuis le début des tests en 1998. . ESET a été reconnue comme l'une des entreprises les plus innovantes en Europe pour 2011 au titre des HSBC European Business Awards et a été primée maintes fois par les laboratoires AV-Comparatives, AVTest et bien d'autres encore.

ESET NOD32, ESET Smart Security et ESET Cybersecurity pour Mac sont reconnus et appréciés par des millions d'utilisateurs dans le monde.

ESET a son quartier général à Bratislava (Slovaquie), possède des filiales à San Diego (U.S.), Buenos Aires, et Singapour et des bureaux à Sao Paulo et Prague. Ses centres de recherche sont établis à Bratislava, San Diego, Buenos Aires, Singapour, Prague, Košice (Slovaquie), Cracovie (Pologne), Montréal et Moscou. ESET est également représenté dans plus de 180 pays à travers un réseau de partenaires.

À propos de Sucuri

Sucuri est une entreprise basée en Californie qui intervient dans tout le continent américain. La société a été fondée par deux membres très passionnés par la sécurité des systèmes d'information en mettant l'accent sur deux domaines très distincts : la prévention et la sensibilisation. Créée en 2007, Sucuri a été pensée dès 2004 pour s'attaquer au problème des logiciels malveillants sur le Web.

Pour en savoir plus, veuillez visiter le site Internet : www.sucuri.net

À propos d'Athena Global Services

Créée en 1997, ATHENA Global Services est une entreprise indépendante spécialisée dans la distribution de logiciels de sécurité informatique.

À travers un vaste réseau de distribution, constitué de VAR, revendeurs locaux professionnels et des plus importantes enseignes spécialisées dans la distribution de logiciels, Athena Global Services propose des logiciels et équipements de sécurité novateurs destinés aux particuliers et aux entreprises, pour protéger et gérer leur environnement informatique : antivirus, pare-feu, chiffrement, politique de sécurité, authentification, sauvegarde, migration des données, et contrôle du trafic Internet.

En outre, ATHENA Global Services propose une gamme de logiciels utilitaires également dédiés à la protection et à l'optimisation des parcs informatiques. Grâce à son savoir-faire, ATHENA Global Services entretient des relations privilégiées avec les éditeurs mondiaux qui lui confient la localisation et la distribution de leurs logiciels.

Pour en savoir plus, veuillez visiter le site Internet : www.athena-gs.com

Contact Presse

InterPresse - Norbert Spitéri - nspiteri@interpresse.fr – Tél : 01 45 87 80 54 / 06 60 91 97 49