WordPress et Drupal mal gérés à l’origine du piratage Panama Papers ?

WordPress et Drupal mal gérés à l’origine du piratage Panama Papers ?

C'est peut-être l'absence de prise en compte de patchs de sécurité pour un plug-in WordPress et pour le CMS Drupal qui aurait permis de récupérer chez Mossack Fonseca les fameux Panama Papers qui font trembler le monde de la finance.

La fuite massive des documents de Mossack Fonseca, le cabinet panaméen qui gère des compagnies offshores, n'a pas fini de faire parler d'elle. Les 11,5 millions de documents contenus dans les 2,6 To de données – les fameux Panama Papers – ont déjà ébranlé de nombreuses sociétés et les sphères politiques, poussant par exemple le Premier ministre de l'Islande à démissionner. Mais comment ces données ont-elles été obtenues ?

NÉGLIGENCE INFORMATIQUE

De nombreuses questions demeurent concernant l'origine de la fuite qui provient d'une source anonyme. Mais beaucoup s'accordent sur le fait que la sécurité informatique a été négligée par Mossack Fonseca, ce que le cabinet avoue à demi mots en portant plainte pour piratage informatique.

Dans un mail qu'il ne fallait pas prendre pour un poisson d'avril, le cabinet avait expliqué à ses clients dès le 1er avril qu'il avait été victime d'une « brèche non autorisée de [son] serveur mail », comme le montre une copie publiée par Wikileaks le 3 avril. Bien sûr, les réactions sur Twitter ne se font pas fait attendre, amusées par la date d'envoi du mail et par l'absence de chiffrement des courriers électroniques de la part d'une entreprise qui met en avant « ses prestigieux services en ligne », comprenant « un compte sécurisé qui vous permet d'accéder n'importe où aux informations de votre société ».

DE L'IMPORTANCE DE METTRE À JOUR DRUPAL ET WORDPRESS

De récentes informations corroborent la thèse du piratage, qui aurait pu être facilitée par des vulnérabilités au sein des CMS utilisés par Mossack Fonseca, à savoir les gestionnaires de contenus Drupal et WordPress.

Comme le rapporte Forbes, le portail client du cabinet fait tourner une vieille version de Drupal (7.23). Or cette version est antérieure à un patch de sécurité qui corrigeait une énorme faille à partir de la version 7.32. Dans une notice de sécurité, Drupal allait jusqu'à recommander une nouvelle installation aux utilisateurs n'ayant pas mis à jour immédiatement après la sortie du correctif.

Il se peut donc qu'un attaquant ait exploité cette faille durant les deux années pendant lesquelles le cabinet n'a pas mis à jour sa version du CMS. Mais d'autres experts en informatiques ont découvert une autre porte qui aurait pu permettre à un hacker d'entrer dans le système.

Si le portail client du cabinet est sous Drupal, le site principal est lui sous WordPress. L'entreprise Wordfence, spécialisée dans la sécurité de l'omniprésent gestionnaire de contenus, a remarqué que l'installation WordPress utilisait une ancienne version du plugin Revolution Slider, connue pour présenter une faille sérieuse.

La version 3.0.95 de Revolution Slider (et les versions antérieures) contiennent en effet une vulnérabilité qui permet à un assaillant d'envoyer un fichier sur le serveur web sans avoir à s'identifier. L'entreprise note qu'un attaquant aurait donc pu prendre le contrôle du serveur sur lequel se trouvait l'installation WordPress… Le même serveur qui hébergeait les très précieux e-mails du cabinet.

En l'occurrence, rien ne prouve que les failles au sein des installations WordPress et Drupal du cabinet aient facilité la fuite des données. Dans la mesure où les journalistes n'ont pas rendu publics les documents, il sera d'ailleurs difficile de déterminer d'où ils proviennent. De son côté, le cabinet affirme qu'il s'agirait d'une attaque effectuée depuis l'étranger, écartant par la même toutes idées de fuites internes.

… [Lire la suite]

Source : *Panama Papers : des WordPress et Drupal mal gérés à l'origine d'un piratage ? – Tech – Numerama*