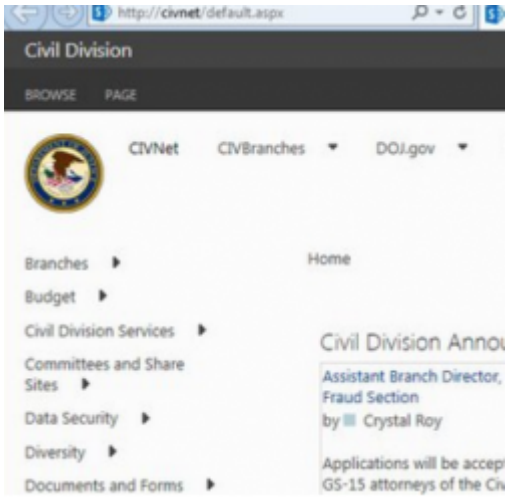
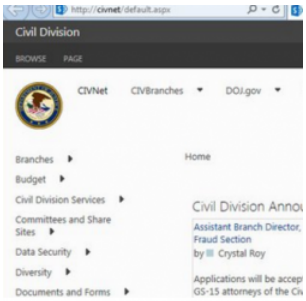
Hack au FBI : Les données privées de 22 175 employés du FBI piratées



Hack au FBI : Les données privées de 22 175 employés du FBI piratées

Un hacker est parvenu à s'introduire sur l'intranet du ministère américain de la Justice et à télécharger 200 Go de fichiers incluant des noms, numéros de téléphones et mails de 22 175 employés du FBI mais également des données personnelles relatives à 9 372 personnes travaillant pour le ministère de la Sûreté Intérieure des Etats-Unis.



Hack au FBI. Ce n'est malheureusement pas le nom d'une nouvelle série, mais bel et bien d'un second incident de sécurité majeur qui a permis de divulguer plusieurs dizaines de milliers de données personnelles d'employés du FBI mais également du ministère de la Sûreté Intérieure (Departement of Homeland Security). Si dans le précédent épisode du Hack of FBI en novembre dernier 3 000 coordonnées de policiers et de militaires américains s'étaient retrouvés dans la nature, le volume est donc cette fois-ci beaucoup plus important. Ainsi, le hacker, opérant sous le pseudonyme DotGovs sur Twitter, a publié une liste de 22 175 employés travaillant au FBI – parmi lesquels des agents spéciaux, analystes et officiers – incluant leurs noms, prénoms, fonctions mais également numéros de téléphone ainsi que leurs adresses mails. D'après Motherboard, qui s'est entretenu avec le hacker, ce dernier a également en sa possession des données personnelles appartenant à 9 372 employés de la Sûreté Intérieure américaine. Des données qui ont été également mises en ligne en tout début de semaine.

Alors que pour le précédent hack de données personnelles des employés du FBI, le groupe de hackers Crackas With Attitude s'en était pris au compte mail AOL du patron de l'agence, Mark Giuliano, le vol de données opéré par le mystérieux DotGovs a été effectué d'une toute autre manière. Ainsi, ce dernier a réalisé son méfait en piratant un compte mail d'un employé du département américain de la Justice. Le hacker a ensuite contacté le support du ministère en indiquant ne pas pouvoir se connecter au portail web. « Alors je les ai appelés et leur ai dit que j'étais nouveau et leur ai demandé comment accéder au portail », a expliqué le hacker à Motherboard. « Ils m'ont demandé si j'avais un code token, j'ai dit non, ils m'ont dit que ça allait et d'utiliser le leur. » Une fois connecté, le hacker raconte alors avoir cliqué sur un lien l'ayant amené sur une machine virtuelle en ligne et entré les identifiants du compte mail déjà hacké. « J'ai cliqué dessus et ai eu un accès total à l'ordinateur », a expliqué le pirate.

Un détournement classique

« Ces comptes détournés peuvent uniquement être détectés grâce à la capacité d'observer et de détecter les changements dans le comportement de l'utilisateur, par exemple la connexion de l'utilisateur à son compte à un horaire inhabituel ou d'un endroit inhabituel, la vitesse de frappe sur son clavier ou d'execution des commandes, etc. C'est ce que l'on appelle, l'analyse comportementale des utilisateurs. Cette technologie permet de fournir un profil réel de chaque utilisateur, basé sur des caractéristiques personnelles – en quelque sorte sorte une empreinte digitale – et ainsi de détecter tout comportement anormal du compte utilisateur et d'en référer instantanément à l'équipe de sécurité voire même de bloquer en temps réel l'activité de l'utilisateur jusqu'à nouvel ordre », a par ailleurs précisé dans un communiqué Zoltán Györkő, PDG de l'éditeur en sécurité Balabit.
En tout, ce sont près de 200 Go de données confidentielles qui ont été téléchargées, alors que le hacker indique avoir eu accès à 1 To de données. « J'ai eu accès à ces données mais n'ai pas pu tout prendre », fait savoir DotGovs. Parmi les contenus qui sont passés entre ses mains ou ses yeux, on trouverait aussi des mails de militaires ainsi que des numéros de cartes bancaires. Suite à la parution de ces listes hackées de plus de 30 000 employés, le DHS a réagi par le biais de son porte-parole S.Y. Lee : « Nous recherchons les articles relatant les informations de contacts des employés du département de la sûreté intérieure qui ont été divulgués. Nous prenons très au sérieux ces articles, cependant rien ne permet d'indiquer à ce jour qu'il y ait eu violation d'informations sensibles ou personnelles. » … [Lire la suite]

Réagissez à cet article

Source : *Les données privées de 22 175 employés du FBI piratées – Le Monde Informatique*