

Comment un pirate a fait pour pirater Le FBI ?



Comment
un
pirate
a fait
pour
pirater
le FBI
?!

Il y a quelques jours un pirate a pris contact avec le site Motherboard pour se vanter d'avoir récupéré des données sur un ordinateur du département de la Justice américain. Aujourd'hui un autre site, The Telegraph, indique que, selon un porte-parole du service, les données ne seraient pas à caractère sensible mais que des investigations sont en cours.

Sur le site qui a dévoilé l'affaire en premier il est intéressant de suivre le récit de l'attaquant qui a réussi à pirater le système.

Tout a commencé lorsqu'il a réussi à avoir accès à un compte email appartenant à sa victime, un employé du département de la justice. Il n'explique pas comment il a pu obtenir cet accès mais a pu utiliser le compte puisqu'il est rentré en contact avec le journaliste par ce biais.

Le département de la justice a fourni le code

A partir du compte le hacker a tenté de se connecter, sans succès dans un premier temps, au portail intranet du département de la Justice. Devant cet échec, il a ensuite directement pris contact avec le support du service prétextant être nouveau et n'arrivant pas à accéder au portail. Son correspondant l'a simplement questionné pour savoir s'il était en possession du code de sécurité et, constatant que ce n'était pas le cas, lui en a fourni un sans difficulté.

Une fois connecté au service, le pirate a ensuite pu prendre la main à distance sur l'ordinateur personnel de sa victime. C'est ce qui lui a permis de récupérer les données, dont les noms et informations de contacts de 22000 employés du FBI. Sur 1 To de fichiers, seuls 200 Go seraient passés entre les mains du pirate qui dit détenir des documents incluant des informations de contact de militaires et des numéros de cartes de crédit.

Un compte email est relativement simple à pirater puisqu'il s'agit la plupart du temps de deviner ou dérober le mot de passe grâce à des méthodes d'ingénierie sociale. Des protections supplémentaires existent pourtant, la plupart des services proposent notamment un système de double authentification qui nécessite la saisie d'un code reçu par SMS en plus du mot de passe... [Lire la suite]



Réagissez à cet article

Source : *Piratage du FBI : le hacker a simplement demandé le code d'autorisation – CNET France*