Des données sensibles de comptes Box en vadrouille sur Google et Bing

Box a corrigé rapidement une faiblesse dans la façon de gérer les comptes et les dossiers partagés publiquement. Un chercheur a trouvé des documents confidentiels appartenant à des clients de la solution de stockage Cloud à travers une simple requête sur des moteurs de recherche comme Google ou Bing.

Du pain bénit pour les pirates

C'est Markus Neis, en charge de la gestion des menaces chez Swisscom qui a levé le lièvre. En faisant des recherches sur Internet, il a trouvé des invitations officielles pour compulser plus de 10 000 comptes publics de Box. La plupart ne renferme pas de fichiers importants, mais d'autres documents sont classés « confidentiels » en intégrant des données financières. Les sociétés concernées par ces fuites sont notamment Dell Technologies (documents sur ses partenaires distributeurs), Discovery Communications (projets vidéo) ou Illumina, une société de biotechnologie.

Pour le spécialiste, ces trouvailles sont du pain bénit pour les cybercriminels. « *En plus d'avoir accès à des informations sensibles, ces documents ouvrent la porte à des attaques d'ingénierie sociale* », précise Markus Neis. Et d'ajouter que les pirates ont une multitude de possibilités. « *Placer des logiciels malveillants dans un projet Box, identifier les cibles des collaborateurs à hameçonner via un email, héberger des malwares et partager des liens.* » Résultat des courses, « *le compte Box.com de votre entreprise peut avoir la réputation d'être un nid à malwares* ».

Une URL d'invitation indexée par les moteurs de recherche

Le cœur du problème vient pour l'expert dans la façon dont Box permet aux titulaires de comptes d'inviter des participants externes à accéder aux fichiers et dossiers partagés. Lors de cette invitation, une URL est générée. Mais, en plus, Box crée automatiquement une page de destination pour l'URL. Et dans certains cas, cette page est indexée par les moteurs de recherche comme Bing ou Google. Pire, ces liens ont été générés avec des privilèges d'éditeur donnant ainsi la capacité de visualiser, télécharger, modifier et renommer les fichiers.

Interpellé sur ce problème, Box a indiqué que les liens indexés par les moteurs de recherche avaient été explicitement partagés par les détenteurs de comptes Box. Mais, l'éditeur a quand même « *contacté Google pour supprimer les liens publics de leur index. Une procédure en phase d'aboutissement* ». Et d'ajouter que « *nous avons retravaillé l'ensemble de ces pages pour s'assurer que les liens d'invitation ne soient plus indexés par Google à l'avenir* ». Les sociétés citées dans cette affaire ont été sollicitées pour commentaires par nos confrères de *ThreatPost*. Dell Technologies a reconnu « *qu'un jeu limité d'informations a été par inadvertance et temporairement visible à plus de personnes qu'il*

n'aurait dû. C'est maintenant réparé ». Du côté de Discovery Communications et d'Illumina pas de commentaires, mais les documents sont depuis inaccessibles.

A lire aussi :

Stockage : Google Docs toujours plus intégré à Box

Box s'associe à Amazon et IBM pour conquérir l'Europe

Photo via VisualHunt