«Nous avons décidé de ne pas prendre contact avec les pirates»

CYBERSÉCURITÉ Christophe Hubschmid, responsable du groupe immobilier dont fait notamment partie Domicim, raconte de l'intérieur le piratage informatique que son entreprise a subi il y a quinze jours. Plus de 2000 fichiers ont été mis en ligne sur le darknet

PROPOS RECUEILLIS PAR ANOUCH SEYDTAGHIA
@Anouch

Les pirates qui ont attaqué la société immobilière suisse DBS Group sont passés à l'action. Et ils ont publié leur butin sur le darknet, comme l'a constaté *Le Temps*. Le groupe, qui possède notamment l'enseigne Domicim, s'était fait voler de nombreux fichiers lors d'une cyberattaque intervenue début décembre. *Le Temps*, qui avait révélé cette cyberattaque lundi, a pu consulter les fichiers mis en ligne sur le darknet, grâce à l'aide de l'entreprise genevoise de cybersécurité ZenData. Celle-ci analyse en permanence ce qui est mis en ligne sur le darknet afin de vérifier si des informations volées concernant ses clients sont publiées.

Au total, DBS Group s'est semble-t-il fait voler un volume de données de 750 Mo, répartis entre 2145 fichiers. Parmi ces fichiers, on trouve environ 1370 images, principalement des photos de maisons et d'appartements, tant prises de l'extérieur que de l'intérieur. On voit aussi des centaines de contrats de bail, avec l'ensemble des données des clients qui sont lisibles.

Il y a également des factures avec des coordonnées bancaires et des informations sur des garanties de loyer. On y trouve aussi des plans précis d'appartements et de maisons, et cela peut être considéré comme des données sensibles, notamment s'agissant de bureaux d'entreprises d'assurances. Dans la masse de fichiers apparaissent aussi des e-mails de certains collaborateurs.

DBS Group possède 12 marques en Suisse, dont Domicim, Brolliet, Duc-Sarrasin, Guinnard Immobilier & Tourisme, Bruchez & Gaillard ou encore Batiline. L'ensemble du groupe compte plus de 700 collaborateurs en tout. L'entreprise rejoint la longue liste d'organismes suisses piratés, après notamment Comparis, Matisa (qui avait aussi vu ses données publiées sur le darknet) ou encore la commune de Rolle cet été. Les données de 5000 de ses habitants sont elles aussi sur le darknet.

Directeur de DBS Group, Christophe Hubschmid a répondu à nos questions mardi après-midi en visioconférence.

«Le fédéralisme montre ses limites face aux cyberattaques et un appui plus important du canton et de la Confédération, dans ce genre de crise, serait nécessaire»

INTERVIEW

Quand avez-vous vu que vous aviez été piratés? Nous avons décelé le problème il y a quinze jours, en constatant que certains fichiers étaient chiffrés. Immédiatement, nous avons activé notre plan en cas de cyberattaque: pour la Suisse romande uniquement, nous avons coupé tous les systèmes vers l'extérieur, mais aussi entre eux au sein de notre groupe, coupé les transactions bancaires (pour des sorties uniquement) et les accès à nos serveurs. Nous avons pu continuer à travailler, mais avec ces contraintes. Nos collaborateurs ont continué à recevoir des e-mails, mais y ont répondu depuis un autre système de messagerie pour les questions qui ont passé par nos sites web, par exemple. Nous avons a priori été infectés par une pièce jointe, contenue dans un e-mail, qui intégrait des lignes de code malveillant.

Quel était le montant de la rançon réclamée? Nous n'avons pas reçu de demande de rançon, mais un message nous invitant à prendre contact avec les pirates. Nous avons décidé, en accord avec notre assureur, avec la police et de par la politique de notre groupe, de ne pas y donner suite. Car nous savions que nous avions des sauvegardes de tous nos fichiers et que nous pourrons, à terme, récupérer toutes nos données. Nous avons construit ces dernières années nos systèmes avec plusieurs types de sauvegardes.

Que représentent, pour vous, les données volées? Nous possédons au total environ 15 teraoctets de données, ce n'est donc, a priori, qu'un extrait de nos données qui se trouve sur le darknet. D'après nos analyses, une fraction de nos données a été volée, même si je ne peux exclure de nouvelles découvertes ces prochains temps. Mais je suis optimiste. Nous avons fait appel à plusieurs sociétés de cybersécurité, dont une chargée de surveiller ce qui était publié sur le darknet. C'est ainsi que nous avons vu ces données publiées lundi. A priori, il ne s'agit pas de données jugées trop sensibles. Mais nous ne pouvons exclure que parmi les informations volées se trouvent des e-mails entre collaborateurs dans lesquels ils parlent de salaire, par exemple.

Avez-vous averti tous vos clients? Oui, nous avons, ces derniers jours, averti bien sûr tous nos collaborateurs, nos partenaires et nos clients. D'une façon ou d'une autre, nous avons pu assurer tous nos services. Il faudra un peu de temps pour un retour complet à la normale, nous devrons faire attention à redémarrer nos systèmes uniquement lorsque nous serons sûrs qu'ils ne présentent aucun risque.

Comment ont réagi vos collaborateurs? Bien sûr, des employés ont été désécurisés. Travailler en temps de pandémie n'était déjà pas facile pour eux avant cette attaque. Aujourd'hui, environ 400 de nos 700 collaborateurs travaillent en «mode dégradé», c'est-à-dire avec des outils alternatifs. Nous espérons un retour à la normale rapide, mais uniquement lorsque nous serons sûrs de la fiabilité absolue de nos systèmes.

Allez-vous déposer plainte? Oui, nous allons déposer plainte prochainement, sans doute auprès de la police vaudoise. Je suis un fervent défenseur du fédéralisme, mais sans doute qu'il montre ses limites face aux cyberattaques et qu'un appui plus important du canton et de la Confédération, dans ce genre de crise, serait nécessaire.

Vous ne semblez pas avoir subi des dégâts importants à la suite de cette attaque? C'est une expérience difficile. Mais grâce aux mesures que nous avons prises ces dernières années, grâce à la robustesse de nos systèmes, l'appui du groupe international Foncia auquel nous appartenons, grâce aux sauvegardes que nous avions mises en place, nous parvenons, je crois à limiter les dégâts. ▬