

Une banque Suisse aurait cédé au chantage de hackers



Des établissements financiers helvétiques ont reçu des menaces d'un collectif de hackers. L'un au moins aurait payé une forte somme pour éviter une attaque, selon «20 Minuten».

Des cybercriminels s'attaquent à la place financière suisse. Au moins dix banques ont reçu en début de semaine des menaces de la part d'un collectif de hackers nommé Armada. Dans son message, le groupe affirme qu'il paralysera les serveurs des institutions si celles-ci ne s'acquittent pas d'une somme de 10'000 francs, à verser en 25 bitcoins (à l'heure actuelle, 1 bitcoin vaut 400 francs).

Les inconnus ont par ailleurs précisé qu'ils nuiront aux entreprises qui ne cèdent pas au chantage en lançant une attaque par déni de service (DDoS). Celle-ci consiste à rendre indisponible un service en submergeant ses serveurs de requêtes afin de les saturer. Si l'argent n'est pas versé dans les délais impartis, la somme revendiquée est doublée à 50 bitcoins. Chaque jour supplémentaire coûte 20 bitcoins en plus, peut-on lire dans le document que les entreprises ont reçu. «Ce n'est pas une blague. Nos attaques sont très puissantes», écrit le collectif.

Porte-monnaie virtuel crédité de 25 bitcoins

Ce n'est pas la première fois que ce groupe menace des institutions helvétiques. En novembre dernier, la Confédération avait même publié une mise en garde à l'encontre d'Armada sur son site.

Des recherches menées par nos collègues alémaniques de «20 Minuten» montrent que le porte-monnaie virtuel des maîtres-chanteurs a été crédité de 25 bitcoins. Ce qui laisse supposer qu'au moins une banque a accepté le marché des hackers. Mais comme on ignore si les pirates informatiques ont attribué un porte-monnaie virtuel différent à chaque banque menacée ou, si le même compte a été utilisé pour toutes les institutions victimes du chantage, il est impossible de savoir quelle firme a effectué le virement de 10'000 francs.

Ne jamais verser de l'argent aux inconnus

Contacté, Max Klaus, directeur adjoint de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (Melani), n'a aucune connaissance d'une banque ayant cédé au chantage. Il doute par ailleurs que le collectif Armada se cache réellement derrière ces menaces: «Normalement, le groupe Armada lance des attaques en guise de démonstration pour montrer de quoi il est capable. Mais aucune de ces démonstrations n'a été effectuée auprès des banques en question», note Max Klaus.

La Confédération déconseille de manière générale de céder au chantage et de verser de l'argent aux inconnus. «Il n'existe aucune garantie que les attaques cesseront une fois la somme payée. Les sommes versées ne font que renforcer les hackers, qui peuvent alors solidifier leur infrastructure et investir dans du matériel leur permettant de lancer des attaques de plus en plus puissantes», met en garde Max Klaus... [Lire la suite]



Réagissez à cet article

Source : *20 Minutes Online – Une société au moins cède au chantage de hackers – Suisse*