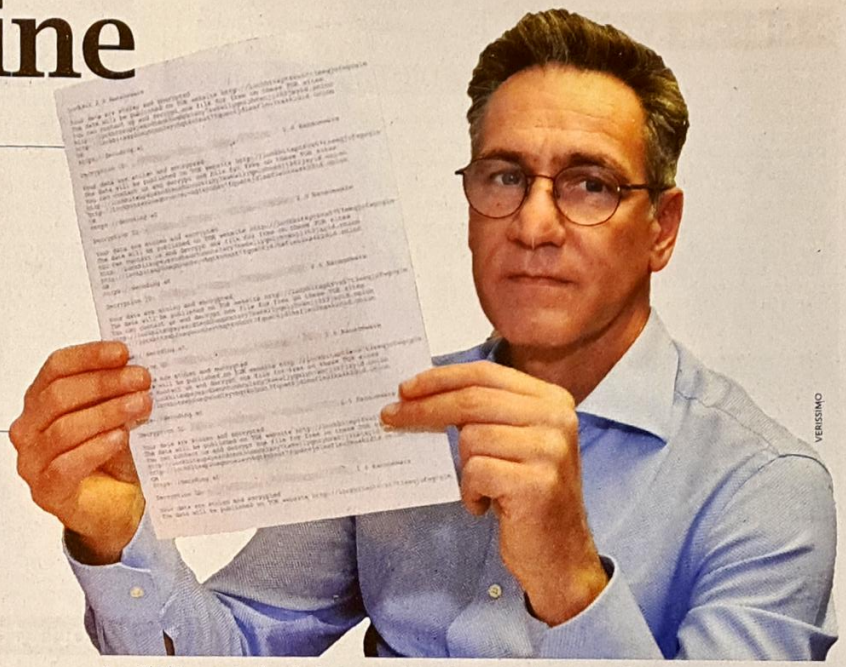
Des pirates attaquent les éditions Slatkine

- *L'entreprise valdo-genevoise a été hackée début novembre avec demande de rançon à la clé.*
- *Le patron de la maison d'édition, Ivan Slatkine a décidé de payer pour récupérer les précieuses données.*
- *Il accepte de témoigner pour prévenir que ça n'arrive pas qu'aux autres et que la menace est à prendre au sérieux. Récit.*

Marie Prieur



VERISSIMO

Ivan Slatkine montre l'un des 8000 exemplaires du message des pirates informatiques découverts dans les bureaux de la maison d'édition, le samedi 6 novembre.

Lockbit 2.0. Un nom de code synonyme de gros ennuis. Il y a un mois, les éditions Slatkine ont découvert que ce logiciel malveillant ou ransomware (*lire encadré*) avait été introduit dans leur système informatique. «On a été piraté, confirme le patron, Ivan Slatkine. Le samedi 6 novembre, un employé est venu au bureau. Il a découvert que toutes les imprimantes avaient craché le même message en anglais jusqu'à épuisement du papier. Il y avait environ 8000 exemplaires. Tout était *down*! Plus un ordinateur ne fonctionnait. Nos back-up de secours étaient eux aussi vérolés.» Sont touchées les cinq branches du groupe.

Pas d'impact en revanche sur son activité de président de la Fédération des entreprises romandes (FER). «Il n'y a pas de connexion possible», insiste Ivan Slatkine. Reste que le système informatique de l'entreprise est HS. «Les pirates préparaient leur coup depuis longtemps, précise-t-il. Ils ont frappé pile lors d'une fenêtre durant laquelle notre système était un peu plus vulnérable.»

Les ouvrages en sécurité

Par chance, les nombreux ouvrages parus aux éditions Slatkine sont en sécurité. «J'ai la chance d'avoir un secteur imprimerie détaché du reste de l'entreprise.» De plus, la base de données centrale n'est pas atteinte.

Les locaux de l'entreprise étant basés à Chavannes-de-Bogis (VD), le patron dépose une plainte pénale auprès de la police vaudoise. «Ils nous ont dit qu'il y avait une avalanche de cas en Suisse. Environ un par jour. Que notre pays était le paradis pour les hackeurs.» Afin de gérer cette situation de crise, les éditions Slatkine font appel à une boîte spécialisée. Ces experts entrent en contact avec les pirates.

Quatre jours plus tard, la demande de rançon atterrit sur le bureau du directeur général. «Par chance, la somme exigée n'était pas astronomique.» Combien? «Ce n'était ni des millions, ni des centaines de milliers de francs...», indique-t-il sobrement. «On a fait la balance entre le montant pour remonter de A à Z tout notre système informatique et le fait de payer... Puis, après négociations, on a réussi à faire baisser de moitié la rançon.» L'accord ficelé, les pirates laissent à Ivan Slatkine 48 heures pour payer en monnaie numérique. «Il a fallu créer dans l'urgence un compte pour acquérir des bitcoins et être en mesure de verser la rançon», se souvient le patron. Mais aussi croiser les doigts pour que les données soient effectivement rendues. Heureusement, le tout leur est restitué par l'intermédiaire d'une clé de décryptage envoyée sur le Darkweb.

«On pensait qu'on était protégé»

«Depuis trois semaines, on est en phase de reconstruction. On veut tout sécuriser avant de repartir.» Selon les statistiques qui ont été rapportés à Ivan Slatkine, il faut en général 70 jours pour remettre en état le système informatique. «Et 45% des entreprises hackées ferment boutique... On a de la chance dans notre malheur», souligne-t-il.

Et le patron de conclure: «On pensait qu'on était protégé. En réalité, n'importe qui peut se faire cyber-attaquer. Quelles que soient la taille de sa structure ou son activité. C'est une menace à prendre au sérieux.» ■

Ransomware en série: «C'est une pandémie»

MP • On les appelle Ransomware ou rançongiciel. Mais, késako? Les explications de Steven Meyer, cofondateur et directeur de Zendata, entreprise genevoise spécialisée dans la cybersécurité: «Il s'agit d'un logiciel malveillant qui, d'un côté, chiffre toutes les données afin d'empêcher les utilisateurs de travailler et, de l'autre côté, les exfiltre afin que les criminels puissent les lire et les publier. Lors de l'intrusion, les hackeurs détruisent aussi les sauvegardes afin d'empêcher une restauration du système.»

Puis, comme le nom Ransomware l'indique, vient la demande de rançon. «L'extorsion est double: si l'entreprise ne paie pas, elle n'a plus accès à ses données. Et, les données en question sont publiées sur le darkweb.» Quid du montant de la rançon? «Pour les PME, il varie entre 50'000 francs et un million, avant négociations», précise Steven Meyer.

Quant à savoir combien d'entreprises sont touchées... Selon cet expert: «C'est une véritable pandémie. Notre société reçoit à elle seule trois appels de victimes par semaine. Sans compter tous ceux qui se taisent, ne portent pas plainte et essaient d'étouffer l'affaire...» Dès lors, difficile d'obtenir une statistique: «Mais, un cas par jour, c'est un minimum...», déplore Steven Meyer.