

Victime de Ransomware ? Payer ou ne pas payer ?



Selon une étude d'IBM, près de 70% des entreprises victimes d'un ransomware acceptent de payer les cybercriminels pour récupérer leurs données. 50% de celles-ci ont versé plus de 10.000 dollars. Pourquoi payer ? Pour récupérer l'accès à leurs données critiques.



« On ne paie pas, ce n'est pas une solution raisonnable » jugeait en début d'année le patron de l'agence de sécurité de l'Etat (Anssi). Pour Guillaume Poupard, verser des rançons aux auteurs de ransomware n'est pas la solution.

Pourquoi ? Car, entre autres, « cela contribue uniquement à soutenir financièrement les développeurs du malware » justifie Catalin Cosoi, responsable de la stratégie sécurité de BitDefender. Mais voilà, faute de sauvegarde et compte tenu de l'importance des données, des entreprises se résignent à payer.

Ransomware : des attaques à large spectre

C'est ce qu'observe IBM Security dans une étude. D'après Big Blue, les entreprises sont de plus en plus victimes de ransomware. Mais d'abord par opportunisme. Ces attaques sont désormais bien moins ciblées et affectent des victimes plus que des cibles.

L'attaque fin novembre contre le système de transport de San Francisco en est une illustration. Les pirates expliquaient ainsi automatiser l'infection par un ransomware après détection de vulnérabilités. La municipalité avait cependant refusé de payer la rançon de 100 bitcoins (alors plus de 70.000 dollars).

Selon IBM, la rentabilité du ransomware encourage à la multiplication des attaques. Près de 40% des emails de spam contiendraient désormais un tel programme malveillant. Cela se traduit mécaniquement par une hausse du nombre de victimes.

Et les entreprises victimes auraient donc majoritairement tendance, à près de 70%, à payer la rançon pour récupérer leurs données, chiffrées par les cybercriminels et donc inexploitable. Le préjudice financier dépasserait les 10.000 dollars pour 50% de ces sociétés.

Payer ou renoncer à ses données critiques

Les 20% restants auraient versé plus de 40.000 dollars, estime IBM. Au total, Big Blue évalue à 1 milliard de dollars, le montant ainsi extorqué aux entreprises grâce à un ransomware...[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRIEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)



Réagissez à cet article

Original de l'article mis en page : Ransomware – Payer ou ne pas payer ? Une large majorité d'entreprises a choisi – ZDNet