

**Le nombre de serveurs MongoDB infectés augmente chaque jour...**



**Le  
nombre  
de  
serveurs  
MongoDB  
infectés  
augmente  
chaque  
jour...**

**L'irruption d'un groupe de cybercriminels spécialisé dans le ransomware a encore dopé le nombre de piratages des bases MongoDB. Une quinzaine d'acteurs malveillants exploitent désormais le filon.**

Déjà en nette expansion la semaine dernière, l'infection touchant les bases de données MongoDB laissées librement accessibles sur Internet tourne à l'épidémie. Alors que les deux chercheurs suivant cette attaque, Victor Gevers et Niall Merrigan, recensaient un peu plus de 10 000 serveurs pris en otage vendredi, le total dépasse désormais les 28 300. Cette soudaine inflation est en grande partie due à l'entrée d'une scène d'un groupe de cybercriminels spécialistes des ransomwares, Kraken. Ce dernier, responsable à lui seul de 16 000 infections, serait entré en lice vendredi dernier, après avoir probablement pris conscience de la simplicité d'exploitation de ce nouveau filon. Selon les éléments recensés par Victor Gevers et Niall Merrigan dans un tableau récapitulant les données relatives à la quinzaine de groupes impliqués dans des attaques de ce type, Kraken aurait déjà convaincu 67 organisations de lui verser une rançon de 0,1 Bitcoin (86 euros environ) ou, dans certains cas, de 1 Bitcoin.

Rappelons que l'attaque ne consiste pas à déployer un ransomware, mais exploite la (très discutable) configuration par défaut des bases MongoDB, au sein duquel l'accès n'est pas protégé par une authentification. Lorsque que ces bases sont librement accessibles sur Internet, les pirates se contentent d'exporter le contenu des bases non sécurisées, d'effacer les données du réceptacle originel et d'y déposer un fichier comportant les informations poussant à la victime à payer une rançon (entre 0,1 et 1 Bitcoin) afin de retrouver ses données. Notons que MongoDB a publié un billet de blog expliquant comment paramétrer sa solution pour éviter ce type de mésaventure.

## Un défaut connu de longue date

Victor Gevers et Niall Merrigan signalent que certains groupes de cybercriminels se contentent d'effacer les données, sans les télécharger au préalable, rendant toute récupération de l'information illusoire pour les victimes. Selon Victor Gevers, 12 organisations ayant versé une rançon à Kraken n'ont pour l'instant obtenu aucune réponse du groupe de cybercriminels. Les deux chercheurs notent également que certains acteurs malveillants en concurrence sur ce segment n'hésitent pas à remplacer les fichiers de demande de rançon d'autres groupes de hackers. La conséquence ? Les victimes peuvent se retrouver à verser des bitcoins à des individus qui, de toute façon, ne détiennent pas leurs données...[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 DRETEF 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](#)



Régissez à cet article

Original de l'article mis en page : Epidémie pour MongoDB : 28 000 serveurs pris en otage