# Après MongoDB, les instances Elasticsearch rançonnées

Le monde n'en a pas fini avec les prises d'otages des bases de données MongoDB qui se multiplient, qu'il faut déjà penser à une nouvelle menace visant les instances Elasticsearch. Ce dernier est un système Open Source d'indexation et un moteur de recherche distribué. Il est de plus en plus utilisé notamment dans le secteur bancaire et des assurances comme nous nous en étions fait l'écho avec l'expérience de Natixis Financement.

Tout comme les bases MongoDB, plusieurs instances Elasticsearch ont été victimes depuis quelques heures d'attaques visant à faire payer une rançon. La méthode est connue, les cybercriminels utilisent une mauvaise configuration de la solution Open Source pour d'abord récupérer les données, les effacer et réclamer de l'argent pour les récupérer. Une victime citée par *The Register* a reçu ce message : *« Send 0.2 bitcoins to this wallet: 1DAsGY4Kt1a4LCTPMH5vm5PqX32eZmot4r if you want recover (sic) your database! Send to this email your service IP after sending the bitcoins p14t0s@sigaint.org (sic). »* 0,2 bitcoin correspond à environ 160 euros.

Niall Merrigan, un développeur .net, qui comptabilise les bases de données MongoDB infectées, calcule maintenant les instances Elasticsearch touchées. A son compteur publié sur Twitter, il recense plus de 600 instances affectées. Les Etats-Unis sont les principales victimes avec 245 instances. Puis vient la Chine avec 59 instances et la France arrive en troisième position avec 52 instances dont 40 hébergées chez OVH.

## 35 000 instances Elasticsearch visibles sur le web

Et comme dans le cas de MongoDB, le phénomène risque de tourner au viral et de s'accélérer sous l'impulsion de cybercriminels organisés comme le groupe Kraken. John Matherly, fondateur de Shodan, évalue ce nombre à 35 000 dont une grande majorité est hébergée sur Amazon Web Services (cf graphique ci-dessous). On remarquera qu'OVH se situe en 6ème position pour héberger les instances Elasticsearch.


La firme américaine n'a pas tardé à réagir et s'est fendu d'un message sur son blog pour conseiller et rassurer. Elasticsearch pousse bien évidemment les clients à ne pas exposer leurs instances sur

le web. Si c'est le cas, les clients doivent s'assurer de disposer d'une sauvegarde de l'ensemble des donnés et de recréer un environnement Elasticsearch sur un réseau isolé. En cas d'incapacité d'appliquer ces règles, l'accès à l'instance doit se faire via une connexion sécurisée (firewall, VPN, reverse proxy). L'éditeur rappelle que la version Cloud de son offre n'est pas concernée par ce problème de sécurité, car elle est protégée par le X-Pack Security.

**A lire aussi :**

Epidémie pour MongoDB : 28 000 serveurs pris en otage

Des hackers combinent Elasticsearch et Cloud pour lancer des attaques DDoS