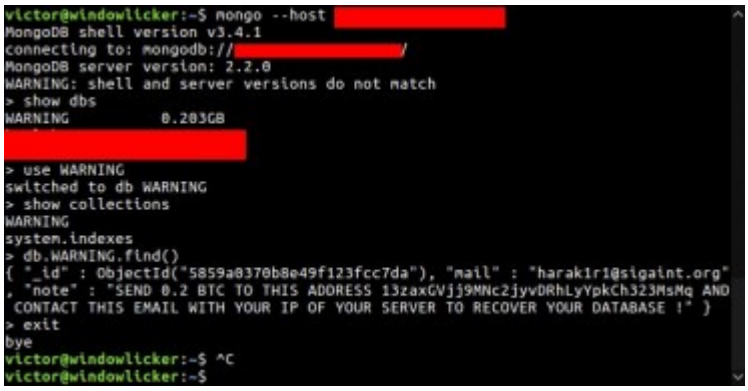
Après les ransomwares, les bases de données MongoDB prises en otage

Après les fichiers bureautiques pris en otage, les bases de données ? Un cybercriminel ou un groupe de cybercriminels connu sous le pseudonyme Harak1r1 s'attaque aux bases MongoDB non protégées, remplace les données qu'elles renferment et demande une rançon en bitcoin pour restituer l'information. Selon Bleeping Computer, cette attaque dure depuis au moins une semaine et cible des serveurs dans le monde entier.



Cette nouvelle forme d'extorsion de fonds a été isolée par le chercheur en sécurité Victor Gevers. Le 27 décembre, ce dernier repère, dans le cadre de ses activités au sein de la GDI Foundation (une organisation à but non lucratif défendant un Internet ouvert et sûr), une base MongoDB dont l'accès est ouvert (pas de mot de passe sur le compte admin). Sauf que cette dernière ne renferme qu'une seule table (appelée Warning), au sein de laquelle Harak1r1 livre ses instructions pour récupérer les données qu'il a exfiltrées au préalable. Un scénario confirmé par les logs de la base de données. Dans le cas présent, selon Victor Gevers, l'entreprise victime a pu restaurer ses données sans payer de rançon, une sauvegarde ayant été effectuée juste avant les manipulations du ou des cybercriminels.

Plus basique qu'un ransomware

Si le procédé s'apparente à celui rendu célèbre par les ransomwares – une prise en otage des données associée à une demande rançon -, l'attaque de Harak1r1 ne fait pas appel à un malware de ce type. En réalité, elle est bien plus basique et se contente d'exploiter une faille de sécurité grossière de MongoDB, mais malheureusement encore très répandue. « *Ce n'est pas un ransomware. La base de données n'est pas chiffrée, mais simplement remplacée. Nous avons affaire à quelqu'un qui effectue cette opération manuellement ou via un simple script Python* », explique Victor Gevers.

Selon les statistiques de Blockchain.info, au moins 16 organisations ou individus ont déjà payé le ou les pirates (à chaque fois 0,2 bitcoin). Un total encore faible au regard du potentiel de nuisance de cette attaque : selon un tweet de John Matherly, le fondateur de Shodan (un moteur de recherche de machines connectées), quelque 2 000 instances MongoDB seraient déjà infectées. Parmi les victimes, selon un chercheur de MacKeeper, Bob Diachenko, une organisation dans le domaine de la santé aux Etats-Unis, qui a perdu l'accès à 200 000 enregistrements.

MongoDB : des alertes dès 2014

« *Les bases de données MongoDB les plus ouvertes et les plus vulnérables se trouvent sur AWS parce qu'il s'agit de la plateforme préférée des organisations voulant travailler en mode Devops. Environ 78 % de ces hôtes font tourner des versions vulnérables* », détaille Victor Gevers. Dans le cas présent, les pirates recherchent d'anciennes versions de la base NoSQL où la configuration par défaut laisse la solution accessible à des connexions externes. Un bug évidemment corrigé depuis par l'éditeur de MongoDB, mais de nombreuses moutures défaillantes continuent à tourner sur le Cloud.

Le problème de l'insécurité des bases MongoDB est d'ailleurs connu de longue date. Dès 2014, un chercheur en sécurité identifiait plus de 33 500 instances MongoDB comportant un port d'administration ouvert, parmi lesquelles près de 19 000 ne demandaient aucune authentification. En 2015, dans un billet de blog, John Matherly avertissait des dangers des bases de données MongoDB non protégées, concluant que près de 600 To de données étaient ainsi exposées. Lors de ses dernières recherches, suite à la découverte des activités de Harak1r1, Victor Gevers est ainsi tombé sur une instance MongoDB non sécurisée, renfermant plus de 850 millions d'enregistrements d'appels de téléphones mobiles.

A lire aussi :

Après les ransomwares, la prochaine menace est le ransomworm

Comment le ransomware est devenu le gagne-pain des cybercriminels

Un hacker tombe par hasard sur des bases MongoDB non protégées

crédit photo © Imilian / Shutterstock.com