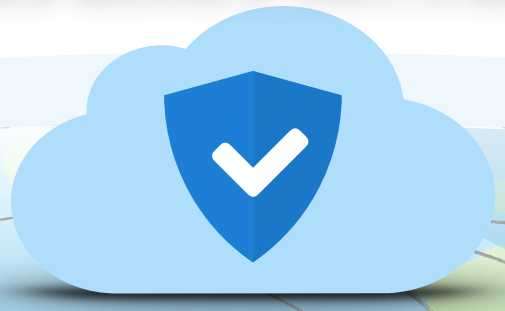
GROUPEMENT DE GENDARMERIE DES ALPES-MARITIMES

BULLETIN D'ALERTE…CYBERATTAQUE

INDUSTRIES, ENTREPRISES SÉCURISER VOS DONNÉES



Une nouvelle forme de cyberattaque d'ampleur appelée «Meow» entraîne la <u>suppression des bases de données stockées sur des cloud publics non sécurisés</u> auprès de fournisseurs de service et d'entreprises

Le Pôle national de lutte contre les cybermenaces communique[1]:

- Cette cyber attaque consiste à remplacer les bases de données stockées sur les clouds non sécurisés par une série de chiffres et le mot « **Meow[2]** ». Les pirates se contentent d'effacer ces données sans demander de rançon en échange.
- Une fois connectés à la base de données en tant qu'administrateur, le ou les attaquants procèdent à sa **suppression et laissent un message railleur «Meow »** en tant que signature.
- Les cibles et le mode opératoire utilisés suggèrent que ces attaques sont menées pour faire prendre conscience aux responsables de bases de données qu'elles sont vulnérables à la visualisation et à la suppression par des entités tierces.
- S'il est avéré que les attaquants n'abusent pas des données avant de les supprimer, **cette attaque pourrait aussi bien servir à protéger les données des utilisateurs autant qu'à nuire aux entreprises.**
- **Cette cyberattaque est une véritable alarme pour les industries et les entreprises qui ne respectent pas les règles d'hygiène numérique[3]. Cette opération de suppression de données non sécurisées est toujours en cours.**

Quelles perspectives pour lutter contre le vol, l'utilisation et la suppression de données stockées sur le Cloud public ?

- En lançant des recherches dans Shodan[4], il est possible de voir tous les dispositifs et services non sécurisés existants et disponibles en ligne,
- En sensibilisant les entreprises à une meilleure hygiènes informatique,
- En valorisant l'utilisation des Cloud privés plutôt que des Cloud publics,
- En optant pour un meilleur chiffrement des données disponibles en ligne et par le biais d'audits de sécurité à l'aide de « bug bounty[5] » ou en faisant appel à des hackers éthiques

Votre contact sur le département des Alpes-Maritimes

covid19-conseils-entreprises-06@gendarmerie.interieur.gouv.fr

1 https://twitter.com/cybergend
2 « Miaou » en français
3 https://www.ssi.gouv.fr/actualite/le-nouveau-guide-dhygiene-informatique-renforcer-la-securite-de-son-systeme-dinformation-en-42-mesures/
4 **Shodan** est un moteur de recherche qui référence le résultat de balayages de ports massifs effectués sur le réseau Internet.
5 Un bug bounty (chasse aux bugs) est une méthode proposée par de nombreux sites web et développeurs de logiciel qui permet à des personnes de recevoir reconnaissance et compensation après avoir reporté des bugs, surtout ceux concernant des exploits et des vulnérabilités