OBJET: La cyberattaque « Meow »

Ce qu'il faut retenir:
- Cette cyberattaque consiste à remplacer les bases de données stockées sur des clouds non sécurisés par une série de chiffres et le mot « Meow ». Les pirates se contentent d'effacer ces données sans demander de rançon en échange (I).
- Il semble possible de détecter en amont les contenus qui peuvent être sensibles à ce type d'attaque à l'aide d'une veille sur le moteur de recherche « Shodan ». Enfin, une meilleure hygiène numérique, le recours aux cloud privées et des audits de sécurité devraient prémunir les entreprises de la suppression de leurs bases de données (II).

I. Une nouvelle forme de cyberattaque

Depuis la mi-juillet 2020, une nouvelle cyberattaque d'ampleur appelée « Meow », découverte par le chercheur Bob Diachenko, a entraîné la suppression de plus de 4000 bases de données de fournisseurs de services et d'entreprises, stockées sur des Cloud publics non sécurisés. Ainsi, plus de 5 millions de contacts étudiants à Oxford, Nirma, IIM, Hobsons, Griffdom auraient été détruits ainsi qu'une plateforme de paiement au Zimbabwe. Le ou les auteurs recherchent des bases de données non sécurisées et accessibles depuis internet grâce à l'outil Shodan.

Une fois connectés à la base de donnée en tant qu'administrateur, le ou les attaquants procèdent à sa suppression et laissent un message railleur « Meow » en tant que signature.

Contrairement aux rançongiciels, le ou les attaquants ne demandent pas de rançons aux entreprises ou aux utilisateurs dont les données sont compromises, ne les revendent pas sur le dark web, mais remplacent les données par des suites de chiffres.

Actuellement, les entreprises touchées sont UFO VPN, ElasticSearch (moteur de recherche), MongoDB, Cassandra, CouchDB, Redis (systèmes de gestion de bases de données) Hadoop (framework de création d'applications distribuées), Jenkins (outil open source d'intégration continue), ainsi que des périphériques de stockage connectés au réseau.

Les cibles et le mode opératoire utilisé 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 servir à protéger les données des utilisateurs ou bien 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. Cette opération de suppression de données non sécurisées est toujours en cours.

II. Quelles perspectives

En lançant des recherches dans Shodan, il est possible de voir tous les dispositifs et services non sécurisées existants et disponibles en ligne.

Depuis la découverte des attaques « Meow », plusieurs chercheurs ont identifié les bases de données à risques pour en notifier les responsables, afin qu'ils les sécurisent. La mise en place d'une veille pour détecter les contenus non sécurisés via Shodan, par des services de sécurité de l'État pourrait lutter en amont contre ce phénomène.

La sensibilisation des grandes entreprises à une meilleure hygiène numérique, la valorisation de l'utilisation des cloud privés plutôt que des cloud publics, un meilleur chiffrement des données disponibles en ligne et des audits de sécurité à l'aide de « bug bounty » ou en faisant appel à des hackers éthiques, sont des mesures qui, à terme, devraient lutter contre le vol, l'utilisation et la suppression de données stockées sur le cloud public.

Direction générale de la gendarmerie nationale
Direction des opérations et de l'emploi
Sous-direction de la police judiciaire
Pôle national de lutte contre les cybermenaces