Markus Spiske

Des entreprises françaises ont été la cible d’une cyberattaque majeure

L'attaque a été menée entre 2017 et 2020 par l'intermédiaire du logiciel français Centreon, qui compte parmi ses clients de grandes entreprises et institutions, dont le ministère de la Justice, selon l'Agence nationale de la sécurité des systèmes d'information (Anssi).

L’Agence nationale de la sécurité des systèmes d’information (Anssi) a alerté lundi 15 février 2021 sur la découverte d’une intrusion informatique *« touchant plusieurs entités françaises »* via le logiciel français Centreon, qui compte parmi ses clients de grandes entreprises ainsi que le ministère de la Justice. *« Les premières compromissions identifiées datent de fin 2017 et se sont poursuivies jusqu’en 2020 »* , écrit l’Anssi dans un rapport présentant les informations techniques liées à cette campagne d’attaque.

La marque du renseignement russe

L’Anssi a établi que l’attaque présentait *« de nombreuses similarités avec des campagnes antérieures du mode opératoire Sandworm »* , généralement attribué au renseignement militaire russe. Mais elle n’accuse toutefois pas explicitement la Russie, conformément à sa pratique de se limiter à l’expertise technique des attaques. L’attribution est une décision politique, qui ne peut se faire uniquement sur des critères techniques qui peuvent être

trompeurs.

La cyberattaque *« rappelle les méthodes qui ont déjà été utilisées par le groupe lié au renseignement russe Sandworm, mais ça ne garantit pas que ce soit lui »* , a indiqué à l'AFP le spécialiste en cybersécurité du cabinet de conseil Wavestone Gérome Billois. La durée de l'attaque avant d'être découverte laisse entrevoir des attaquants *« extrêmement discrets, plutôt connus pour être dans des logiques de vol de données et de renseignements »* , a-t-il ajouté.

« Centreon a pris connaissance des informations publiées par l'Anssi ce soir, au moment de la publication du rapport, qui concernerait des faits initiés en 2017, voire en 2015, a réagi auprès de l'AFP la société Centreon. *Nous mettons tout en œuvre pour prendre la mesure exacte des informations techniques présentes dans cette publication. »*

À lire aussi

Covid-19 : Comment CybelAngel a neutralisé une escroquerie visant un fabricant de vaccins

Un précédent existe aux États-Unis

Utilisé par de nombreuses entreprises (Airbus, Air France, Bolloré, EDF, Orange ou encore Total) et par le ministère de la Justice, le logiciel Centreon permet de superviser des applications et des réseaux informatiques. *« Cette campagne a principalement touché des prestataires de services informatiques, notamment d'hébergement web »* , a indiqué l'Anssi. Mais elle pourrait aussi avoir touché de grands groupes et institutions. *« Il est possible que des clients de ces prestataires aient été touchés par rebond »* , a souligné Loïc Guezo, le secrétaire général du Clusif, une association de spécialistes français de la cybersécurité. D'une manière générale, il est *« exceptionnel »* que l'Anssi publie une telle note, a-t-il souligné.

Selon lui, la note est manifestement issue d'un long travail d'enquête dans des sociétés françaises compromises et de rapprochements avec des affaires antérieures publiquement révélées il y a plusieurs années. L'affaire rappelle notamment la vaste cyberattaque ayant visé les États-Unis en 2020 et attribuée à la Russie, les pirates profitant d'une mise à jour d'un logiciel de

surveillance développé par une entreprise texane, SolarWinds, et utilisé par des dizaines de milliers d'entreprises et d'administrations dans le monde.

« Les outils de supervision qu'on met dans son système d'information sont souvent des cibles pour les cybercriminels car ils permettent d'accéder à beaucoup de données, a expliqué Gérome Billois. *Ils sont connus pour être des outils d'amplification d'attaque. »* Aux États-Unis, la cyberattaque via SolarWinds a notamment touché les département d'État, du Trésor, de la Sécurité intérieure et les Instituts nationaux de la Santé. Contactés, le ministère français de la Justice et les entreprises concernées n'ont pas fait de commentaire à cette heure.

Article écrit par MADDYNESS, AVEC AFP