Devoir surveillé n° 7 : Le cyberespace, conflictualité et coopération entre les acteurs

Vous traiterez l'un des deux sujets au choix :

Sujet de dissertation : Le cyberespace, quelles réalités et quels défis ?

ou

Sujet d'étude critique de documents :

En analysant le document suivant et en vous appuyant sur vos connaissances, vous montrerez pourquoi et comment la sécurité du cyberespace est devenue un enjeu majeur des relations internationales.

Document :

Piratage informatique : une faille chez Microsoft touche 30 000 organisations américaines

Selon un spécialiste de la cybersécurité, l'Etat chinois serait derrière cette attaque sur la messagerie Exchange du géant de l'informatique.

Des dizaines de milliers d'entreprises, villes et institutions locales aux Etats-Unis ont subi des attaques d'un groupe de hackers soutenus par l'Etat chinois, selon un spécialiste de la cybersécurité, lequel a donné des détails, vendredi 5 mars, à propos d'un piratage de la messagerie de Microsoft.

« Au moins 30 000 organisations (…) ont été piratées au cours des derniers jours par une unité chinoise de cyberespionnage inhabituellement agressive, qui se concentre sur le vol d'e-mails, d'après des sources multiples », a indiqué Brian Krebs sur son blog KrebsonSecurity.

Microsoft a averti mardi que les hackers du groupe baptisé « Hafnium » exploitaient des failles de sécurité dans ses services de messagerie Exchange pour voler les données de ses utilisateurs professionnels. Cet *« acteur hautement qualifié et sophistiqué »*, selon le géant de l'informatique, a déjà ciblé des entreprises aux Etats-Unis par le passé, notamment dans le domaine de la recherche sur les maladies infectieuses, mais aussi des cabinets d'avocats, des universités, des entreprises de défense, des groupes de réflexion et des ONG.

« Le groupe d'espionnage exploite quatre nouvelles failles dans le logiciel Exchange et a semé des outils chez des centaines de milliers d'organisations dans le monde, qui donnent aux attaquants un contrôle à distance total sur les systèmes infectés », a détaillé Brian Krebs.

« La menace est active », a souligné Jen Psaki, la porte-parole de la Maison Blanche, lors d'un point presse vendredi. L'attaque *« pourrait avoir un impact très étendu »*, a-t-elle ajouté, avant d'appeler les collectivités *« qui utilisent ces serveurs à agir maintenant pour se protéger »*.

Pas de lien avec le piratage de SolarWinds[1]

Mardi le directeur de Microsoft, Tom Burt, avait déclaré que sa société avait publié des mises à jour pour corriger les failles, et exhorté les clients à les appliquer. *« Nous savons que de nombreux acteurs étatiques et des groupes criminels agiront rapidement pour tirer profit de tout système non corrigé »*, avait-il averti. *« Appliquer rapidement les correctifs est la meilleure protection contre cette attaque. »* Selon Microsoft, Hafnium est établi en Chine, mais opère par le biais de serveurs privés virtuels loués aux Etats-Unis.

L'année dernière, Pékin avait accusé Washington de diffamation à la suite d'allégations selon lesquelles des pirates informatiques chinois tentaient de voler des recherches sur le Covid-19.

En janvier, les autorités américaines avaient désigné la Russie comme le principal suspect du piratage informatique massif contre l'entreprise SolarWinds, contredisant ainsi l'ex-président Donald Trump, qui avait accusé la Chine d'être à l'origine de cette intrusion dans les logiciels du gouvernement américain et de milliers d'entreprises privées. Microsoft a déclaré mardi que les attaques Hafnium *« n'étaient en aucun cas liées aux attaques distinctes en rapport avec SolarWinds »*.

Le Monde, avec l'***AFP***, 6 mars 2021

[1] Solarwinds désigne une affaire de cyberespionnage qui a eu lieu en novembre et décembre 2020. Solarwinds est une entreprise informatique qui fournit des services et des logiciels de cybersécurité à l'État fédéral et aux grandes entreprises américaines. Des hackers ont infiltré dans l'une de leurs applications un logiciel espion qui leur a permis d'accéder à plus de 10 millions de données secrètes contenus dans les serveurs du gouvernement des EU et de plusieurs grandes entreprises.