

LE RANONGICIEL ou RANSOFTWARE

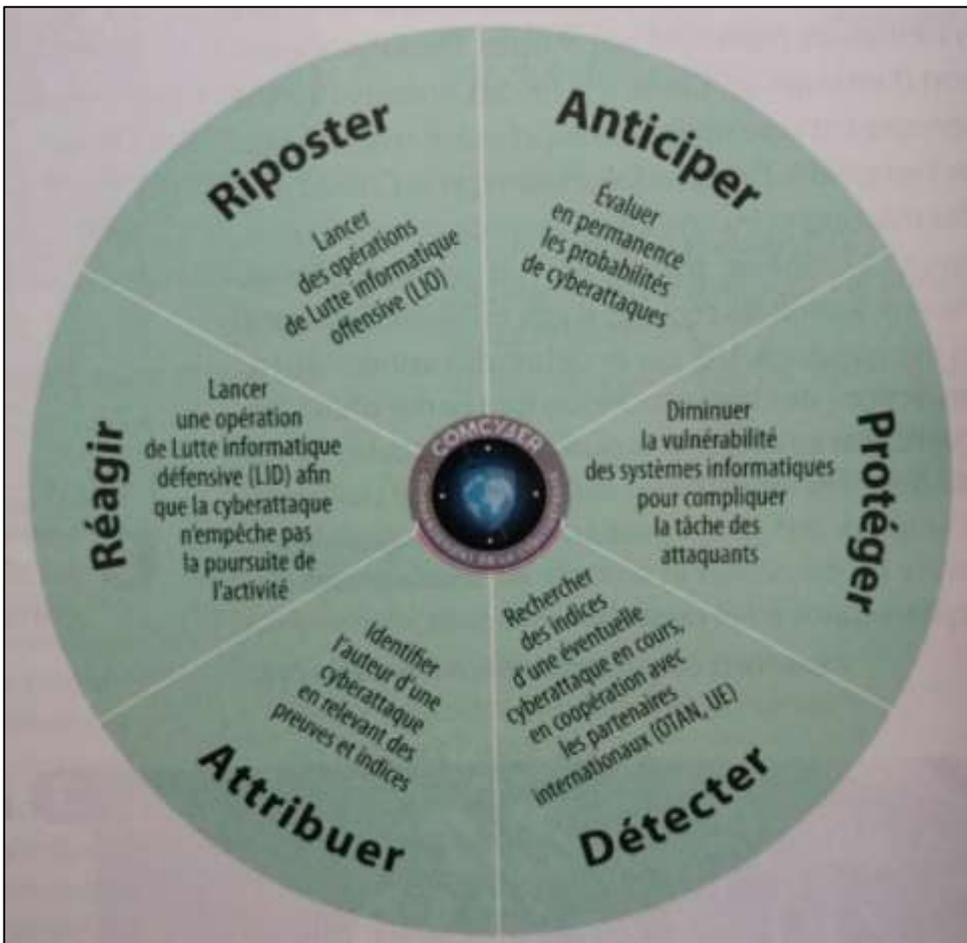
Doc1. La cyberattaque du rançongiciel Wannacry en mai 2017

Royaume-Uni, Russie, Espagne, Portugal, France, Mexique... Vendredi 12 mai, des dizaines de milliers d'ordinateurs, dans au moins 99 pays, ont été infectés par un logiciel malveillant bloquant leur utilisation. [...] Outre-Manche, c'est le système de santé qui a été largement perturbé par ce virus informatique. Examens médicaux annulés ou perturbés, communications téléphoniques affectées, accès aux données bloqués... Le service national de santé (NHS) britannique [...] a été largement déstabilisé vendredi après-midi par ce logiciel qui prend en otage les usagers des ordinateurs en bloquant l'accès à leurs fichiers. [...] Le NHS n'as pas été la seule cible touchée par les pirates. [...] Ainsi, Telefonica, le géant espagnol des télécommunications, et plusieurs autres entreprises du pays ont été victimes d'un virus similaire. [...] Des opérateurs téléphoniques portugais et l'entreprise américaine de livraison FedEx ont également été touchés, de même que le ministère de l'intérieur russe [...].

Les rançongiciels ont connu un développement exponentiel ces trois dernières années. Ils sont généralement conçus par des petits groupes criminels, et touchent le plus souvent les petites et moyennes entreprises, auxquelles ils extorquent des sommes variant entre quelques centaines d'euros par machine infectée – le paiement s'effectue en bitcoins, une monnaie virtuelle anonyme.

Source : Philippe Bernard, Damien Leloup et Nathalie Guibert, « Une cyberattaque massive bloque des ordinateurs dans des dizaines de pays », *Le Monde*, 13 mai 2017

Doc2. Les six missions de commandement de la cyberdéfense française



Source : Ministère des Armées, 2020.

Doc3. Un exercice international unique de cybersécurité : le locked shields



L'équipe française composée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et le ministère des Armées est arrivée à la première place de l'édition 2019 du plus grand exercice international de cybersécurité en situation réelle, Locked Shields, organisé [depuis 2010] par le NATO Cooperative Cyber Defence Centre of Excellence de Tallinn. La République tchèque et la Suède complètent le podium.

A l'issue d'une compétition qui s'est déroulée du 7 au 12 avril 2019, ce sont plus de 1200 experts en cybersécurité de 23 nations qui ont dû faire face à plus de 2 500 cyberattaques. La France a mobilisé 60 spécialistes (civils, militaires et réservistes) [...] qui ont œuvré ensemble à déjouer ces cyberattaques.

Source : d'après <https://www.defense.gouv.fr/operations/actualites2/la-france-remporte-l-exercice-international-de-cyberdefense-locked-shield-2019>, article mis à jour le 18 avril 2019

Doc4. Spécialiste cybersécurité de la Défense nationale

Mission : Votre spécialité consiste à participer, au sein d'une équipe, à la sécurisation des moyens de télécommunication et du matériel informatique. A l'aide de moyens spécifiques, vous proposez des solutions techniques pour améliorer le niveau de sécurité. Vous partez régulièrement en opérations extérieures.

Avantages et rémunération : 9 semaines soit 45 jours/an de permission, -75% toute l'année avec la SNCF, logement et repas inclus.

Affectation : sous-officier, 1384€ net/mois dès votre affectation, pour un célibataire, sans enfant à charge, hors prime, la rémunération en opération extérieure peut être multipliée jusqu'à 2,5.

Profil : homme ou femme de 18 à 29 ans, nationalité française, aptitude militaire, diplômé du baccalauréat, vos qualités : très méthodique, goût prononcé pour la technologie, réactif.

Source : <https://www.sengager.fr/emplois/informatique-telecoms/specialiste-cybersecurite>

CONSIGNES :

Vous devez constituer un ensemble de 5 cartes sur le thème du rançongiciel :

- une carte définition,
- une carte situation,
- une carte mission,
- une carte action,
- une carte formation.

Compétences mobilisées :

- * Raisonner, justifier une démarche et les choix effectués
- * Analyser et comprendre un document pour en extraire des informations
- * Pratiquer différents langages
- * Coopérer et mutualiser

Guide sur le contenu des différentes cartes :

- Carte définition : Doc1, proposez une définition du rançongiciel.
- Carte situation : Doc1, résumez brièvement un cas concret de situation de rançongiciel.
- Carte mission : Doc2, identifiez parmi les six missions de commandement de la cyberdéfense française, celle qui vous semble être la plus efficace pour contrer le rançongiciel.
- Carte action : Doc3, résumez la stratégie qui peut être appliquée à l'échelle européenne pour contrer le rançongiciel.
- Carte formation : Doc4, présentez un métier de la cyberdéfense.

Pour compléter et affiner vos réponses vous pouvez utiliser d'autres outils : manuel, dictionnaire, ordinateur. Une fois les 5 cartes réalisées, un élève ou plusieurs élèves rapporteurs présenteront à l'oral le travail de leur groupe à l'ensemble de la classe.

Toutes vos réponses doivent être rédigées sur les patrons de cartes ci-dessous.

LE RANÇONGICIEL

① Carte définition

Source : Philippe Bernard, Damien Leloup et Nathalie Guibert, « Une cyberattaque massive bloque des ordinateurs dans des dizaines de pays », *Le Monde*, 13 mai 2017.

LE RANÇONGICIEL

② Carte situation

Source : Philippe Bernard, Damien Leloup et Nathalie Guibert, « Une cyberattaque massive bloque des ordinateurs dans des dizaines de pays », *Le Monde*, 13 mai 2017.

LE RANÇONGICIEL

③ Carte mission

Source : Ministère des Armées, 2020.

LE RANÇONGICIEL

④ Carte action

Source : <https://www.defense.gouv.fr/operations/actualites2/la-france-remporte-l-exercice-international-de-cyberdefense-locked-shield-2019>,
article mis à jour le 18 avril 2019.

LE RANÇONGICIEL

⑤ Carte formation

Source : <https://www.sengager.fr/emplois/informatique-telecoms/specialiste-cybersecurite>

