CYBERSECURITE MARITIME
CONTEXTE ET RISQUES

8 octobre 2020

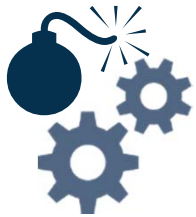
LES ATTAQUES DANS LE CYBERESPACE

ATTEINTE À L'IMAGE

CYBER CRIMINALITÉ

ESPIONNAGE

SABOTAGE

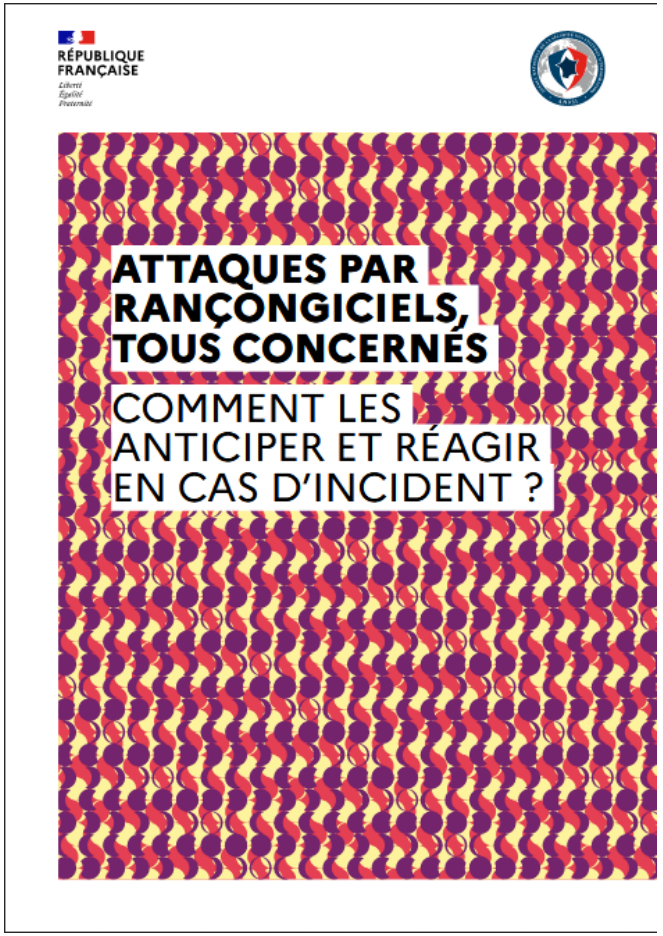


LES CONSTATS

- **Prolifération d'outils d'attaque informatique (Multitudes de techniques et d'outils malveillants réutilisables)**
- **Cybercriminalité : Recrudescence des rançongiciels en 2019 et 2020 (Menace qui impacte tous les secteurs d'activité)**
- **Augmentation de la surface d'attaque (Internet des objets, numérisation et interconnexion croissantes, intégration des technologies (IT) au cœur des réseaux industriels (OT) …)**
- **Supply chain attack ; principe : atteindre une cible sécurisée par la compromission d'un prestataire (rebond vers la cible via l'interconnexion des réseaux) ou de la mise à jour d'un logiciel ;**

RANÇONGICIELS : UNE MENACE QUI EXPLOSE

- Objectif : paiement d'une rançon
- Chiffrement des données par des mécanismes cryptographiques => consultation ou utilisation impossibles
- Souvent associé à la menace de publication de données sensibles (accroitre la pression sur les victimes)
- Importantes ressources financières et compétences techniques des attaquants
- Conséquences : arrêt de la production, chute du chiffre d'affaires, risques juridiques (notamment en cas de compromission de données personnelles), altération de la réputation, perte de confiance des clients, etc.



VERS UNE HAUSSE DE LA CYBERMENACE

- Exposition accrue de nos sociétés (de plus en plus numérisées et interconnectées) au risque de crises cyber majeures
- Cyberattaques croissantes en nombre, intensité et sophistication
- Cybercriminalité : Explosion des attaques due à la forte rentabilité des opérations lucratives.

Augmentation générale de la menace, en proportion de la numérisation

Le secteur du transport maritime n'échappe pas à cette tendance

Exemples d'attaques lucratives

- **Juin 2013, compromission du réseau informatique du Port belge d'Anvers**
- **Juillet 2018, Armateur chinois de porte-conteneurs Cosco, victime d'un rançongiciel sur son terminal portuaire de LongBeach aux USA**
- **Septembre 2018, ports de Barcelone (Espagne) et San Diego (US)**
- **Novembre 2018, Austal (Australie), spécialisée dans la construction navale**

- **Décembre 2019, plusieurs entités du secteur maritime américain, selon l'U.S. Coast Guard, victimes du rançongiciel *Ryuk***
- **2020, prestataires du secteur : DESMI (Danemark) ; TOLL GROUP (Australie) ; CLASQUIN (France, rançongiciel *Sodinokibi*)**

Exemples d'attaques par sabotage

- **Juin 2017, vague mondiale d'infection par le malware NotPetya (vecteur d'infection initiale : mise à jour piégée d'un logiciel ukrainien de comptabilité) : MAERSK**
- **Mai 2020, Port iranien Shahid Rajaee (ville côtière de Bandar Abbas, en Iran)**

NotPetya attack: Maersk reinstalled 45,000 PCs, 2,500 apps & 4,000 servers

LA RÈGLEMENTATION

Loi de programmation militaire – article 22

Loi Française qui concerne les Opérateurs d'Importance Vitale (OIV) des 12 secteurs d'activité d'importance vitale, dont celui des « transports » et son sous-secteur « transports maritime et fluvial »

Directive NIS (2016/1148 du 6 juillet 2016)

Directive européenne, transposée en droit national en 2018, qui concerne les Opérateurs de Services Essentiels (OSE), répartis par secteur / sous-secteur, dont celui du « transport par voie d'eau »

Règles de sécurité et délais d'application

OIV : 20 règles de sécurité [Arrêté sectoriel du 11 août 2016 applicable aux OIV du sous-secteur « Transports maritime et fluvial »

OSE : 23 règles de sécurité [Arrêté du 14 septembre 2018]

OIV et OSE soumis à des contrôles de leur niveau de sécurité et obligations de notification des incidents de sécurité

CONCLUSION

- Un secteur de plus en plus **numérisé** et **connecté**
- Une règlementation forte qui **responsabilise** les entreprises critiques du secteur maritime (OIV, OSE)…
- … mais des risques qui concernent **l'ensemble** des acteurs du secteur
- Le Conseil de Cybersécurité du Monde Maritime créé en novembre 2019 (par décision du CIMER de novembre 2018) :
  - structure de gouvernance nationale de la cybersécurité maritime
  - répond au besoin de coordonner l'action des organismes publics et des opérateurs privés
- Le projet de centre de coordination cyber du monde maritime

Contacts

Agence nationale de la sécurité des systèmes d'information

christian.cevaer@ssi.gouv.fr / Délégué à la sécurité numérique pour la région Bretagne
sylvie.andraud@ssi.gouv.fr / Coordination sectorielle secteur maritime