# PANORAMA DE LA MENACE CYBER MARITIME 2022

M-CERT-2023-CTI-001

AVRIL 2023

**TLP:CLEAR**

**TLP:EX:NC**

# Sommaire

Sommaire 2
1 Introduction 4
1.1 Le secteur maritime et portuaire 4
1.2 Numérique et maritime : la marétique 6
2 Cybersécurité maritime : Bilan 2022 8
2.1 Contexte 8
2.2 Analyse de la menace 8
2.3 Bilan chiffré 9
3 Le secteur maritime face aux attaques cybercriminelles opportunistes 11
3.1 Le phishing principal vecteur d'intrusion initial 12
3.2 Les infostealers et le secteur maritime 18
3.3 Fuites et reventes de données du secteur maritime 27
3.4 Business Email Compromise (BEC) 30
3.5 Les rançongiciels 37
4 Les attaques ciblées contre le secteur maritime 42
4.1 Les clés USB, un vecteur d'infection initiale toujours d'actualité pour le secteur 43
4.2 L'écosystème maritime usurpé à des fins d'ingénierie sociale 43
4.3 Les menaces visant les systèmes « Supervisory Control And Data Acquisition » et « Industrial Control System » (ICS) 46
4.4 Les câbles sous-marins 49
4.5 Les télécommunications par satellite 49
4.6 Leurrage et brouillage GNSS (Géolocalisation et Navigation par Système de Satellites) 50
4.7 Leurrage et brouillage AIS (Automatic Identification System) 52
5 Les acteurs maritimes, victimes collatérales du cybercrime politique? 54
5.1 Les attaques en déni de service distribué 54
5.2 Les acteurs malveillants pratiquant les attaques DDoS 57
6 Cybersécurité maritime : Perspectives 2023 63
7 Glossaire 65
8 A propos de France Cyber Maritime et du M-CERT 68
9 A propos de OWN 69
10 Références 70

Chers membres et partenaires de France Cyber Maritime,

Chers acteurs du monde maritime, portuaire et de la cybersécurité.

Alors que France Cyber Maritime célèbre ses deux années d'existence, je suis heureux de partager avec vous son premier panorama annuel de la menace cyber maritime pour l'année 2022, réalisé en partenariat avec OWN.

L'année 2022 a vu une forte reprise de l'activité maritime mondiale, grâce au recul de la pandémie. Mais cette année a aussi été tragiquement marquée par une guerre aux frontières de l'Europe, qui a eu un impact important sur nos économies et sur le secteur maritime et portuaire. Ce conflit, combiné avec les tensions récurrentes en Asie, complexifie l'établissement d'une vision claire de nos horizons maritimes.

La pandémie nous a rappelé l'importance du secteur maritime et portuaire pour nos économies et le rôle vital des ports, des navires, des marins et de toutes les équipes de soutien et de logistique maritime et portuaire. La numérisation croissante de l'ensemble de l'écosystème maritime contribue fortement à sa performance, sa sûreté et sa sécurité. Mais elle apporte aussi de nouvelles vulnérabilités. De nombreux acteurs, en France et à l'étranger, font face quotidiennement à des enjeux et incidents de cybersécurité. Les cyberattaques perpétrées par des acteurs étatiques, des cybercriminels et des hacktivistes impactent le fonctionnement du secteur et peuvent avoir des conséquences financières et physiques graves. Il est essentiel d'accorder la plus haute priorité à notre résilience numérique.

Ce panorama de la menace a pour objectif de donner une vue globale des menaces cyber ayant touché le secteur maritime en 2022 et d'offrir quelques perspectives pour 2023, pour aider nos adhérents, nos partenaires et nos lecteurs à partager une vision commune. Travailler ensemble pour partager et mieux comprendre ce paysage évolutif de la menace est, plus que jamais, essentiel pour conduire nos activités maritimes en toute sécurité.

France Cyber Maritime a continué sa croissance en 2022, accueillant de nouveaux acteurs majeurs du secteur maritime et portuaire, de nouvelles entreprises de la cybersécurité et des administrations et services publics, en tant que nouveaux adhérents et partenaires. Nous les en remercions. Nous espérons avoir l'occasion de vous rencontrer en 2023, à notre Assemblée générale, aux *European Maritime Days*, à l'*European Cyber Week*, aux Assises de l'économie de la mer ou à *Battleship 2023*, notre évènement live de *Bug Bounty* !

Nous espérons que vous apprécierez autant la lecture de ce rapport que nous avons apprécié le co-écrire !

Xavier REBOUR, Directeur de France Cyber Maritime

# 1. Introduction

Disposer d'un panorama annuel et ouvert de la menace est une demande régulière de nos partenaires, mais également de nos adhérents et d'autres entités publiques et privées du secteur maritime et de la cybersécurité. La rédaction de ce type de rapport réclame soin et précaution, en raison de la sensibilité de l'information, du volume d'information à traiter et de la multiplicité des sources.

Bien entendu, ce rapport annuel n'a pas pour vocation de résumer ni évoquer tout le spectre des évènements partagés par le M-CERT avec ses adhérents et partenaires, mais nous avons essayé d'y synthétiser au mieux l'information pertinente.

Ce panorama de la menace porte le marquage **TLP:CLEAR**. Tel que défini par le FIRST[1], ce marquage indique que les lecteurs peuvent diffuser ces informations sans limitation particulière, tout en respectant les droits et devoirs liés aux droits d'auteurs.

Afin de respecter le **TLP:CLEAR**, les informations mentionnées dans ce bilan sont exclusivement issues d'informations publiques et disponibles en sources ouvertes sur Internet, couplées à des analyses menées par le M-CERT et/ou le OWN-CERT.

De par leur nature publique, ces chiffres ne représentent qu'une partie des attaques ayant visé le secteur au cours de l'année 2022. Ainsi, la détection de menaces étatiques et avancées (comme les *Advanced Persistent Threats - APT*) fait rarement l'objet de publicité ou n'est possible qu'avec un délai parfois important. Leur caractère partiel, couplé avec des analyses d'autres sources à la disposition du M-CERT et/ou de OWN permettent cependant de dégager des tendances intéressantes.

La base de données publique ADMIRAL[2], mise à disposition par le M-CERT, permet de disposer d'une bonne vision d'ensemble sur la majorité des attaques publiques recencées par le M-CERT, ayant touché le secteur.

## 1.1. Le secteur maritime et portuaire

Le secteur maritime et portuaire (Figure 1-1) est un secteur industriel mondial, complexe et imbriqué, impliquant de nombreux acteurs à terre et en mer, parmi lesquels on peut citer :

- Les ports : qu'ils soient de commerce, de pêche, multimodaux, d'importance locale, régionale, nationale ou internationale : avec leur *hinterland* [3], ils irriguent l'économie de matières premières, de biens et de services indispensables au fonctionnement des économies ;
- Les navires, dans toute leur diversité : navires à passagers, porte-conteneurs, méthaniers, pétroliers, navires de soutien, navires de recherche, navires câbliers ;

- Les armateurs ;
- Les installations offshore ;
- Les nombreuses entreprises du secteur maritime : sous-traitants, chantiers navals et réparation navale ;
- L'industrie navale ;
- La plaisance ;
- Le secteur de la pêche, de l'aquaculture et des produits de la mer ;
- Les acteurs du transport, de la logistique, de la manutention ;
- Les sociétés de classification, assurances ;
- Les services numériques maritimes partagés ;
- Les administrations publiques maritimes ;
- Les énergies marines renouvelables (EMR) ;
- Les écoles et centres de recherche maritimes ;
- Les infrastructures sous-marines : câbles sous-marins, infrastructures de distribution de pétrole et de gaz.


*Figure 1-1 : Représentation schématique d'une partie de l'écosystème maritime. © Cluster Maritime Français, reproduit avec leur aimable autorisation.*

Le Cluster Maritime Français estime que l'économie maritime française représentait, en 2021, 386000 emplois directs, et était à l'origine d'une valeur de production de 90,6 milliards d'euros[4]. Au niveau mondial, ce sont 80 % du volume mondial de marchandises qui empruntent la voie maritime. La libre circulation des biens et des personnes en mer, le bon fonctionnement des ports et, par conséquent, des systèmes numériques qui les composent revêtent donc un caractère particulièrement stratégique.

Le fonctionnement du secteur maritime reste parfois méconnu et peut être perçu comme complexe.

Cette appréciation peut avoir plusieurs origines :

- Caractère mondial du transport maritime, avec de nombreux acteurs mondiaux, nationaux, régionaux et locaux ;
- Réglementation riche et diverse, issue d'organismes internationaux, nationaux ou régionaux ;
- Impact de la géopolitique sur le secteur ;
- Variété des navires, des ports, et des installations industrielles et numériques associées.

Le secteur maritime civil se trouve aussi à l'intersection d'un certain nombre d'autres secteurs, avec lesquels il interagit ou est interconnecté :

- Le naval de défense, avec bien souvent des technologies duales ;
- Le commerce et la logistique ;
- L'énergie ;
- Les télécommunications.

## 1.2. Numérique et maritime : la marétique

En termes de numérique, un port et un navire sont des systèmes de systèmes complexes, associant systèmes d'information classiques (*Information Technology*, IT) avec des systèmes industriels, cyber-physiques ou métiers, que l'on regroupe souvent sous le terme d'OT (*Operational Technology*)[5].

La numérisation des navires et ports s'est largement développée au cours des dix dernières années, apportant plus de souplesse, de rapidité, de sécurité et de traçabilité tout au long de la chaîne logistique maritime. Cette transformation numérique continue se poursuit avec le développement des technologies de *smart shipping* (suivi et maintenance préventive et corrective à distance), de *green shipping* (intégration des enjeux environnementaux) et le développement des drones maritimes et navires autonomes.

Cette numérisation entraîne malheureusement un niveau d'interdépendance et d'exposition numérique des systèmes jamais atteint jusqu'alors. A ce constat, que l'on peut dresser dans d'autres secteurs industriels, s'ajoutent des particularités sectorielles parmi lesquelles on peut citer :

- Des contraintes de connectivité, pour les navires, qui restent tributaires du bon fonctionnement de leurs systèmes de télécommunication par satellite en mer ou des réseaux de téléphonie type 4G/5G à proximité des côtes. Même si les systèmes de télécommunication se sont fortement améliorés au cours des dernières années, ces caractéristiques de dépendance, de bande passante et de coût contraignent les opérations de maintenance, d'administration et de surveillance à distance ;
- Le contexte très concurrentiel du secteur apporte des contraintes importantes sur les opérations des navires, qui doivent optimiser leurs temps de parcours, leur présence dans les ports et leurs opérations de chargement et de déchargement : les temps de disponibilité et

donc d'intervention à quai sont donc limités ;
- L'absence quasi générale de ressource humaine cyber, voire même de spécialiste du numérique à bord de la plupart des navires civils, complexifie toute investigation ou intervention sur le systèmes numériques ;
- Les particularités des systèmes IT et OT des navires, aux technologies hétérogènes provenant de constructeurs et intégrateurs multiples, parfois peu sensibles aux questions de cybersécurité, entraînent des effets importants de « boîte noire » et de difficultés de maintien en conditions de sécurité par l'apparition rapide d'obsolescences.

Les atteintes potentielles en confidentialité, intégrité ou disponibilité sur les systèmes d'information maritimes et portuaires peuvent avoir des conséquences importantes pour le secteur. Si l'occurrence et les impacts potentiels dépendent fortement des systèmes concernés et de leur emploi, les conséquences peuvent être multiples :

- Perte de la continuité d'activité (opérations portuaires, par exemple) ;
- Sécurité ou sûreté du navire et de l'équipage compromises ;
- Dysfonctionnements suite au contournement de mesures et de procédures de sécurité.

Les enjeux financiers, réglementaires, humains, environnementaux, liés à l'image de marque de l'entreprise ou de l'organisation sont majeurs.

# 2. Cybersécurité maritime : Bilan 2022

## 2.1. Contexte

D'un point de vue géopolitique et économique, l'année 2022 a été marquée par deux évènements majeurs pour le secteur maritime :

- La nécessité de redémarrage très rapide du secteur, après deux années de pandémie qui avaient fortement freiné l'activité et complexifié l'organisation de la chaîne logistique ;
- L'invasion de l'Ukraine par la Russie à compter du 24 février 2022, qui a entraîné des conséquences majeures et historiques aux niveaux géopolitiques, militaires et économiques, qui n'avaient plus été vues depuis la seconde guerre mondiale. Cette invasion a conduit au renforcement de la bipolarité de certains acteurs de la cybercriminalité, voire à leur affiliation claire en soutien de certains pays ou zones d'influence. Dans un contexte mondialisé, cette invasion aura des conséquences durables pour l'ensemble des pays de la planète qui demeurent aujourd'hui incertaines, voire inconnues.

Le caractère stratégique du secteur maritime et portuaire, de la liberté de circulation en mer et de l'intégrité des infrastructures sous-marines (câbles sous-marins de télécommunication, pipelines, Énergies Marines Renouvelables (EMR)) a ainsi été régulièrement rappelé au cours de l'année 2022.

## 2.2. Analyse de la menace

Comme d'autres secteurs industriels, le secteur maritime et portuaire est confronté à trois types de menaces :

1. La menace étatique, agissant de manière frontale, ou sous couvert. Le caractère particulièrement stratégique du secteur peut en faire une « cible » aux yeux de certains pays compétiteurs. Les capacités de ces pays en termes techniques, humains et d'attaques hybrides, sont importantes et doivent être suivies et évaluées en permanence, que ce soit à des fins d'espionnage, de sabotage ou de pré-positionnement.
2. La menace cybercriminelle, qui peut prendre deux formes :
    - La première, purement opportuniste, visant à exploiter des vulnérabilités sur des systèmes d'information maritimes et portuaires exposés sur Internet (services non mis à jour ou mal sécurisés, etc.). C'est essentiellement le cas des attaques par rançongiciel et des tentatives d'extorsion lors de fuites de données. Dans le cas de certains groupes, le soutien étatique ne fait plus de doute.
    - La seconde, qui vise particulièrement le monde maritime et portuaire, en utilisant des techniques telles que le harponnage et le Business Email Compromise, à des fins de revente d'accès, d'arnaque (type faux ordres de virement). Ces attaques et tentatives, permanentes, utilisent bien souvent la création de noms de domaines proches et des courriels parfois correctement forgés pour tromper la victime. Au-delà de l'atteinte à

l'image, ce type d'attaque peut être un précurseur à des attaques plus avancées et destructrices.

3. Des menaces hacktivistes, dont la particularité au cours de l'année 2022 a été un renforcement clair de la bipolarisation. Ainsi, des attaques qui étaient devenues moins médiatisées qu'auparavant, comme les attaques en déni de service distribué (*Distributed Denial of Service, DDoS*) ont été à nouveau détectées en soutien d'actions d'influence politique, comme dans les cas des groupes « Killnet » ou « NoName057(16) ». Ces attaques, bien que souvent temporaires et de complexité relativement limitée, se coordonnent à présent en temps réel via des réseaux sociaux, avec une liste quasi quotidienne de cibles à viser. Les conséquences, bien que limitées, sont plutôt des atteintes à l'image de marque dans une perspective d'influence. Dans certains cas, l'affiliation, voire la coordination, avec certains États, ne fait guère de doute.

## 2.3. Bilan chiffré

### 2.3.1. Au niveau mondial

Avec les précautions d'usage relatives aux chiffres, ce sont près de 90 incidents de cybersécurité notables et publics qui ont été détectés en 2022 dans le secteur maritime et portuaire au niveau mondial, en augmentation de 21 % par rapport à 2021, et de 135 % par rapport à 2020. L'augmentation constatée au cours des dernières années et qui se poursuit est essentiellement attribuable au renforcement de l'activité cybercriminelle.

En proportion, les quatre sous-secteurs d'activité maritime et portuaire principalement touchés par des cyberattaques publiques en 2022 sont, par ordre croissant :

1. Les armateurs (15 %), stable par rapport à 2021 ;
2. Les ports (17 %), en augmentation de 70 % par rapport à 2021 ;
3. La logistique et les transports (18 %), en augmentation de 50 % par rapport à 2021 ;
4. L'industrie maritime et les fournisseurs (21 %), dont le nombre d'attaques a été multiplié par 6 par rapport à 2021.

Ces chiffres semblent apporter les éclairages suivants :

- Les armateurs continuent à être victimes d'attaques sérieuses, notamment par rançongiciels. Si la coordination et l'action des forces de l'ordre, conjuguées avec certaines mesures prises par les armateurs, semblent porter leurs premiers fruits, la situation demeure très hétérogène et fonction de la taille des armateurs, de leur niveau de maturité et, souvent, du dynamisme cyber de leur pays de rattachement et de leurs partenaires.
- Le nombre d'attaques impactant les ports poursuit une augmentation très significative, essentiellement en-dehors de l'Europe. Ces écosystèmes complexes aux acteurs multiples peinent encore, pour une part importante d'entre eux, à se sécuriser en profondeur.
- La logistique et les transports continuent à être les principales victimes. Les analyses que nous

avons pu réaliser montrent notamment leur forte exposition aux tentatives de *phishing* et de *spearphishing*, particulièrement réalistes et ciblant spécifiquement ce type d'acteurs. Agissant en lien numérique direct avec de nombreux autres acteurs du secteur (transitaires, ports, armateurs…), leur sécurisation dans les années à venir est un enjeu majeur.

- Les attaques réussies visant l'industrie maritime et, de manière générale, la *supply chain*, au-delà même de la logistique et des transports, sont particulièrement préoccupantes. En visant, de manière opportuniste ou délibérée, ces acteurs (fournisseurs de services numériques ou physiques, opérateurs de maintenance, équipementiers, etc.), les attaques peuvent impacter de manière globale un ensemble important de navires et d'armateurs, qui peuvent perdre un accès nécessaire à leur fonctionnement au quotidien (par exemple : service cloud ou infogéré).
- Les précurseurs, déjà notés en 2021, relatifs aux Énergies Marines Renouvelables (EMR) et au fluvial, perdurent en 2022.
- En termes de zones géographiques, l'Europe a été le continent proportionnellement le plus touché en 2022 (40 % des attaques ayant fait l'objet d'une publication, stable), suivi par l'Asie (34 %, en baisse) et l'Amérique du nord (21 %, en baisse). Le nombre d'attaques en Europe est plus important qu'en 2021, l'impact du conflit russo-ukrainien ayant entraîné un certain nombre d'attaques opportunistes sur des entités maritimes publiques ou privées occidentales. Les principaux évènements notables au niveau du continent européen sont présentés à la Figure 2-1.

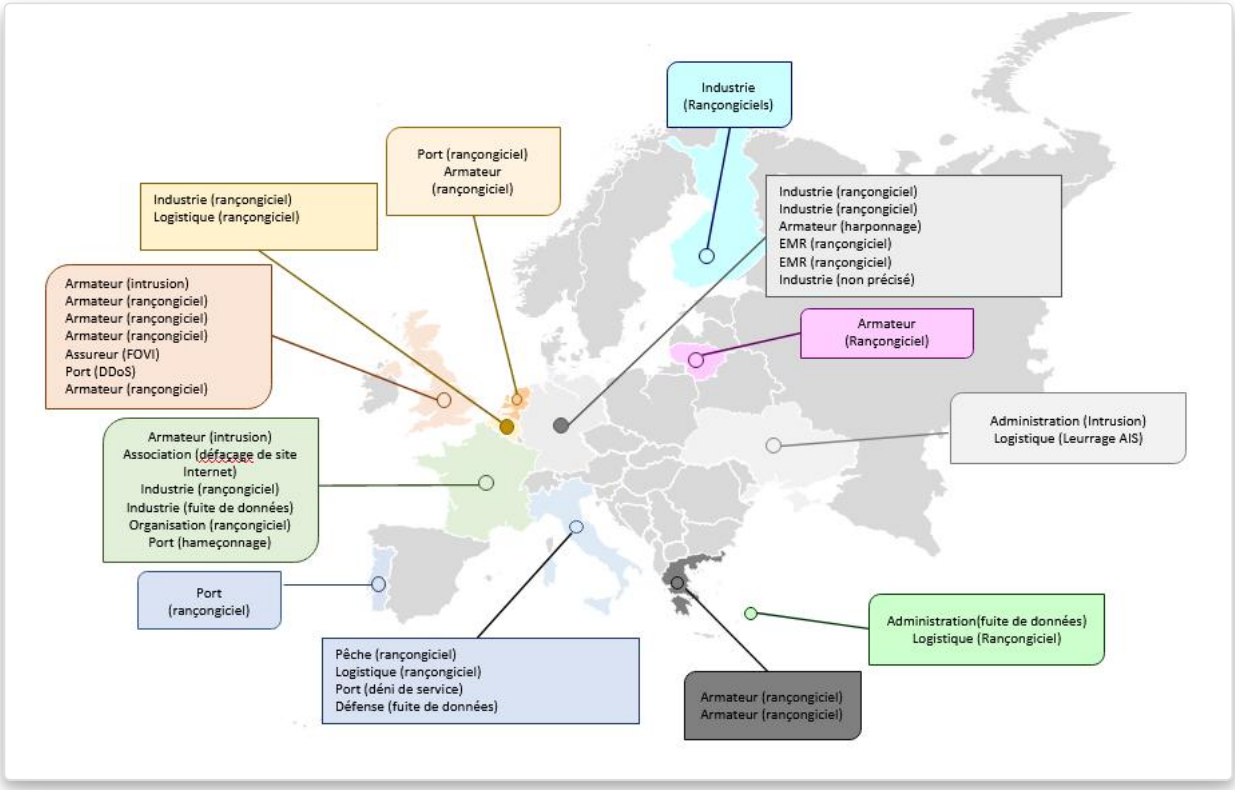



*Figure 2-1 : Répartition des principaux incidents de cybersécurité maritime au niveau européen. Source : M-CERT/ADMIRAL.*

## 3. Le secteur maritime face aux attaques cybercriminelles opportunistes

Les attaques cybercriminelles par opportunisme visent à exploiter une ou plusieurs vulnérabilités d'un service généralement exposé sur Internet pour compromettre une organisation dans un but lucratif. Même si aucun groupe cybercriminel ne se distingue par des activités qui viseraient spécifiquement le secteur maritime, le caractère stratégique et global du secteur, dont dépendent bon nombre de sous-secteurs d'activité, peut en faire une cible privilégiée pour les attaques à but lucratif.

L'enjeu clé est la collecte de données de connexion en vue de l'obtention d'accès initiaux. Pour cela, les attaquants s'appuient sur trois types d'opérations :

**L'exploitation de vulnérabilités** : les données d'accès initial peuvent être obtenues par l'exploitation de vulnérabilités sur des équipements exposés. Parmi les principaux types d'accès vendus, on retrouve les accès VPN, RDP, Pulse Secure, Fortinet et Citrix. Les vulnérabilités exploitées varient suivant les modes opératoires adverses, leur niveau technique et l'existence d'outils d'exploitation. Plusieurs vulnérabilités parues en 2021 et 2022 sont toujours activement exploitées par les attaquants. Les plus courantes en 2022 ont notamment été celles relatives à Fortinet, Zimbra, VMWare, Citrix et aux produits Microsoft (notamment Exchange[6]).

| Recommandation |
| --- |
| Une cartographie exhaustive du système d'information, ainsi qu'une politique de gestion des vulnérabilités sont essentielles pour identifier et corriger rapidement toute vulnérabilité dont l'exploitation permettrait la récupération d'identifiants critiques. |

**Les attaques par force brute** : l'attaquant utilise des outils « sur étagère », assortis de dictionnaires ou d'algorithmes pour tester, l'une après l'autre, chaque combinaison possible d'un mot de passe pour un identifiant donné, afin d'identifier des comptes privilégiés insuffisamment sécurisés ou dont les mots de passe par défaut n'ont pas été modifiés.

| Recommandation |
| --- |
| La recommandation la plus évidente est la mise en place du blocage de comptes à la suite d'un nombre défini d'échecs d'authentification ou l'utilisation d'une authentification multi-facteurs. Les outils permettant de détecter et de contrer les attaques par force brute sont assez communs, mais encore insuffisamment présents sur l'ensemble du périmètre des systèmes d'information du secteur maritime, notamment sur certains équipements propriétaires. Contractuellement, ils ne sont pas non plus nécessairement exigés vers les sous-traitants et hébergeurs. Là encore, le partage des informations relatives à ce type de détection vers le M-CERT permet une analyse globale au niveau du secteur et l'alerte de l'ensemble de la communauté maritime et portuaire. |

**Les attaques par hameçonnage ou *phishing*** : l'orchestration de campagnes de *phishing* est rendue aisée par l'existence de services dédiés (plateformes de type « *Phishing as a Service* ») et la

distribution de kits de *phishing*. Les adresses de courriel ciblées sont également faciles à lister par l'utilisation de bases d'adresses de courriers électroniques récupérées lors de fuites de données (*combo-list*), la collecte de manière automatisée des adresses exposées (*email web scraping*) ou l'identification de formats d'adresses par défaut et de technologies utilisées au sein d'une organisation, (combinaisons nom.prénom@entreprise.tld par exemple).

| Recommandation |
| --- |
| La protection contre le hameçonnage est encore insuffisamment présente dans de nombreuses entreprises. Il est en effet nécessaire de combiner des mesures organisationnelles, techniques et humaines. La lutte à un niveau central, afin de viser les infrastructures de *phishing* et les groupes d'attaquants reste insuffisante face au caractère évolutif de la menace. La remontée de renseignement technique et opérationnel lié au hameçonnage vers le M-CERT est ainsi essentielle pour que le M-CERT puisse analyser et contrer ce type de menace. Ces remontées et analyses contribuent directement au partage rapide et efficace de l'information au sein du secteur pour améliorer la protection de l'ensemble des acteurs. |

Tous les mois, OWN produit à destination du M-CERT du renseignement sectoriel s'appuyant sur la détection, l'investigation et l'analyse des campagnes d'attaque affectant le secteur maritime. Il ressort de ces travaux que le secteur maritime a, sur l'année 2022, été la cible de nombreuses campagnes de *phishing* délivrant des codes malveillants de type *infostealer*. Ces données sont généralement proposées à la revente, puis exploitées en vue de réaliser des actions de type *Business Email Compromise* ou par des opérateurs de rançongiciel.

## 3.1. Le *phishing* principal vecteur d'intrusion initial

Le *phishing* demeure le vecteur d'intrusion privilégié tous secteurs d'activité confondus, dans près de 70 % des cyberattaques[7]. Le maritime n'échappe pas aux campagnes génériques (citons l'exemple des invites de connexion à des plateformes cloud, en vue de récupérer des identifiants/mots de passe de connexion pour une revente ultérieure). Cependant, certains acteurs s'intéressent tout particulièrement au secteur et personnalisent leurs campagnes d'attaque pour maximiser leurs chances de réussite. Plusieurs opérations identifiées au cours de l'année 2022 exploitent ainsi des mots clés, images, formats de documents, signatures, ou pièces jointes ancrés dans la réalité du secteur.

Le OWN-CERT suit quotidiennement les campagnes d'hameçonnage usurpant les grands armateurs. Sur l'année 2022, une prédominance dans l'usurpation des armateurs Maersk et CMA-CGM a été constatée (Figure 3-1). Parmi ces campagnes, il est possible de distinguer les opérations de phishing visant spécifiquement les acteurs du secteur maritime de ceux usurpant l'écosystème maritime pour viser des entreprises d'autres secteurs, tels que la logistique (Figure 3-2).

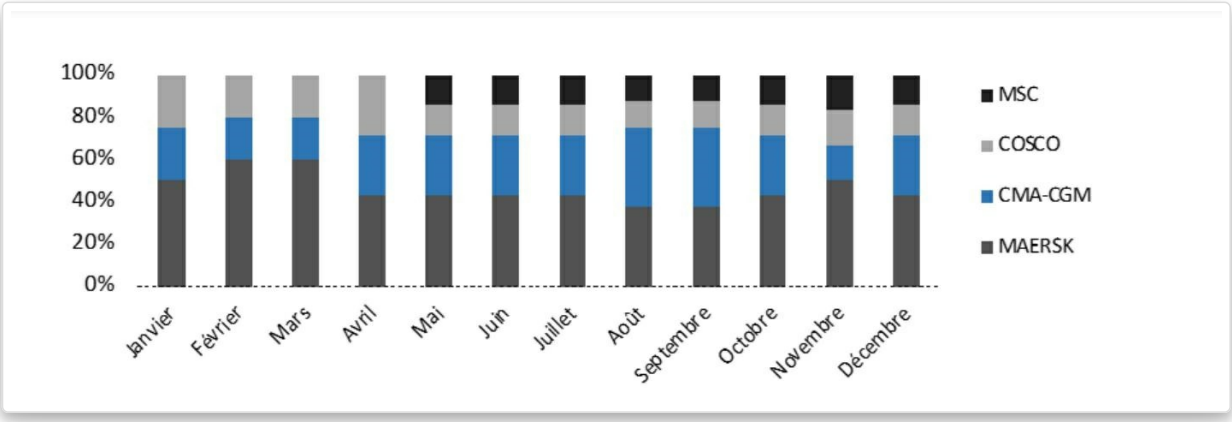



*Figure 3-1 : Répartition des grandes campagnes de phishing identifiées sur l'année 2022. Source : OWN-CERT.*

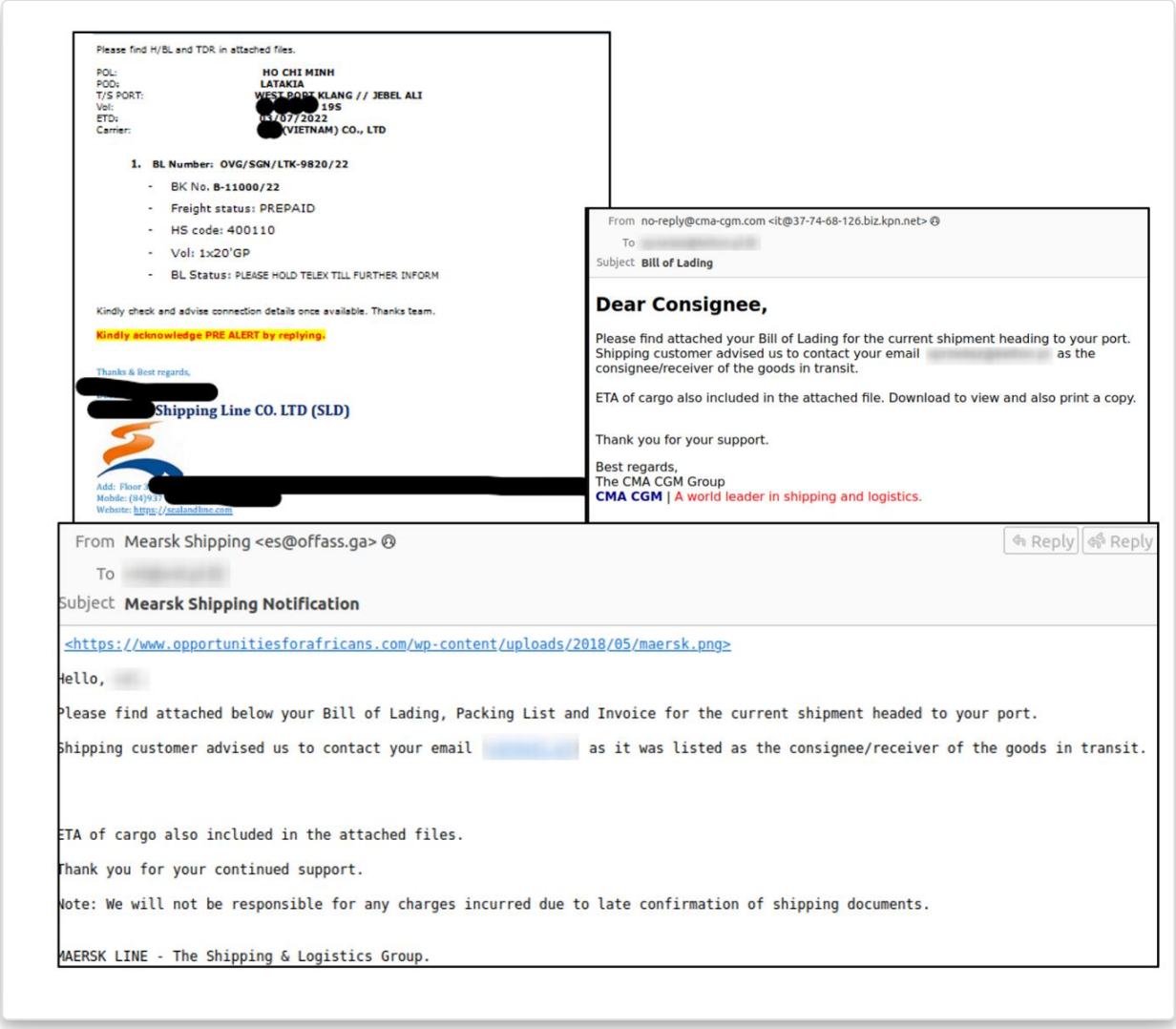



*Figure 3-2 : Courriels de phishing réalistes visant la chaîne logistique.*

Nous dissocions également les campagnes de *phishing* distribuant des liens menant à une page usurpant l'armateur (*typosquatting*), de celles distribuant directement des pièces-jointes malveillantes.

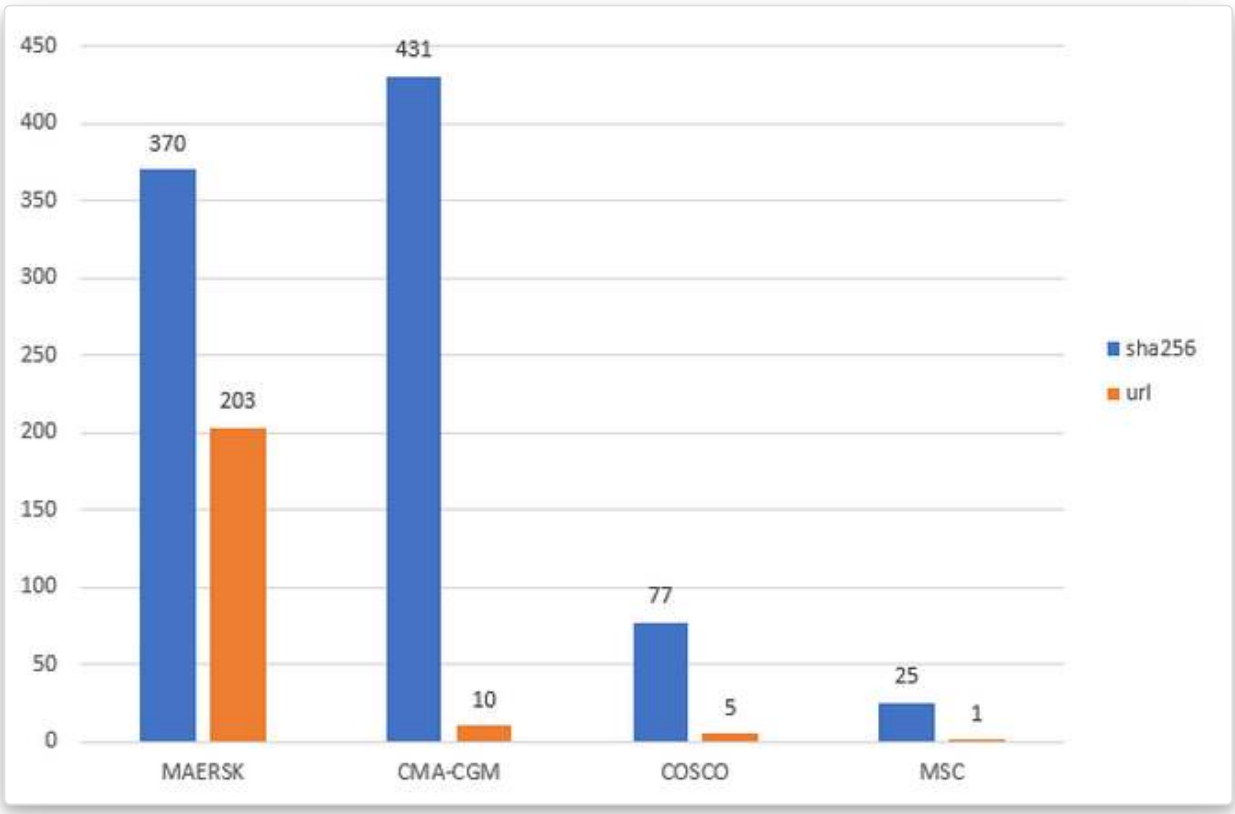



*Figure 3-3 : Répartition des grandes campagnes de phishing identifiées sur l'année 2022, par armateur usurpé, distinguant la technique employée : liens (URL) et pièces jointes (SHA256). Source : OWN-CERT.*

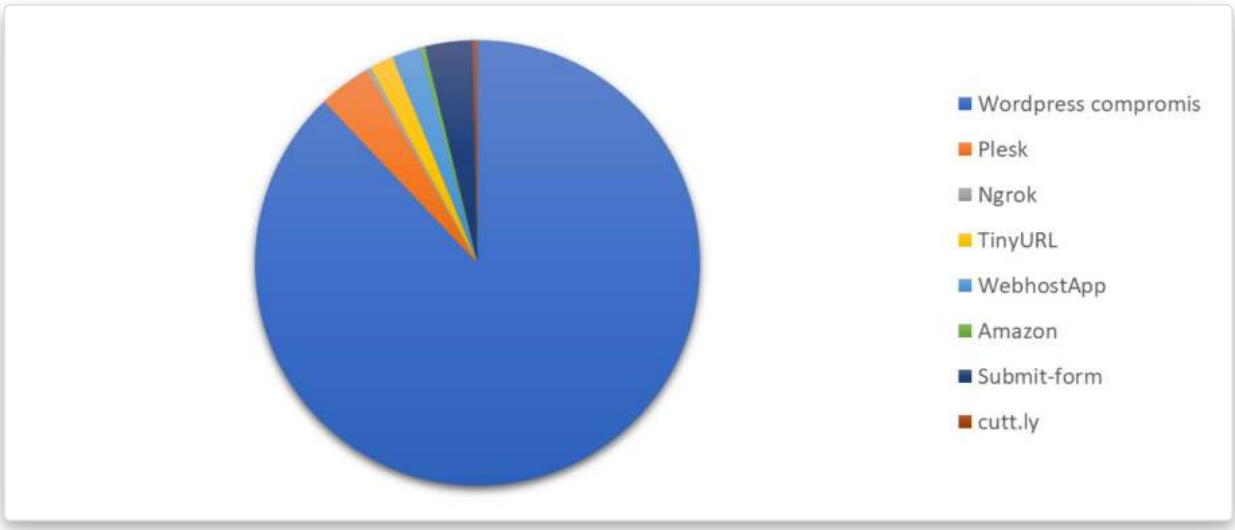



*Figure 3-4 : Principaux services utilisés pour héberger des pages de phishing. Source : OWN-CERT.*

La distinction des deux sous-techniques par MITRE ATT&CK[8] (*Spearphishing Link* (T1566.002) et *Spearphishing Attachment* (T1566.001)) permet d'analyser avec précision les infrastructures malveillantes correspondantes. Plus de 87 % des pages de *phishing* distribuées étaient hébergées sur des sites Wordpress compromis. S'en suivent les services Plesk, WebhostApp et Submit Form (Figure 3-4).

### 3.1.1. Spearphishing Link (T1566.002)

Les thèmes d'ingénierie sociale utilisés (Figure 3-5) reprennent le vocable propre au secteur maritime (*Bill of lading*, *Terminal departure report*, *shipping documents*...), associé à des noms d'acteurs du monde maritime ou de la logistique maritime et portuaire. Les plus régulièrement observés sont représentés Figure 3-6.

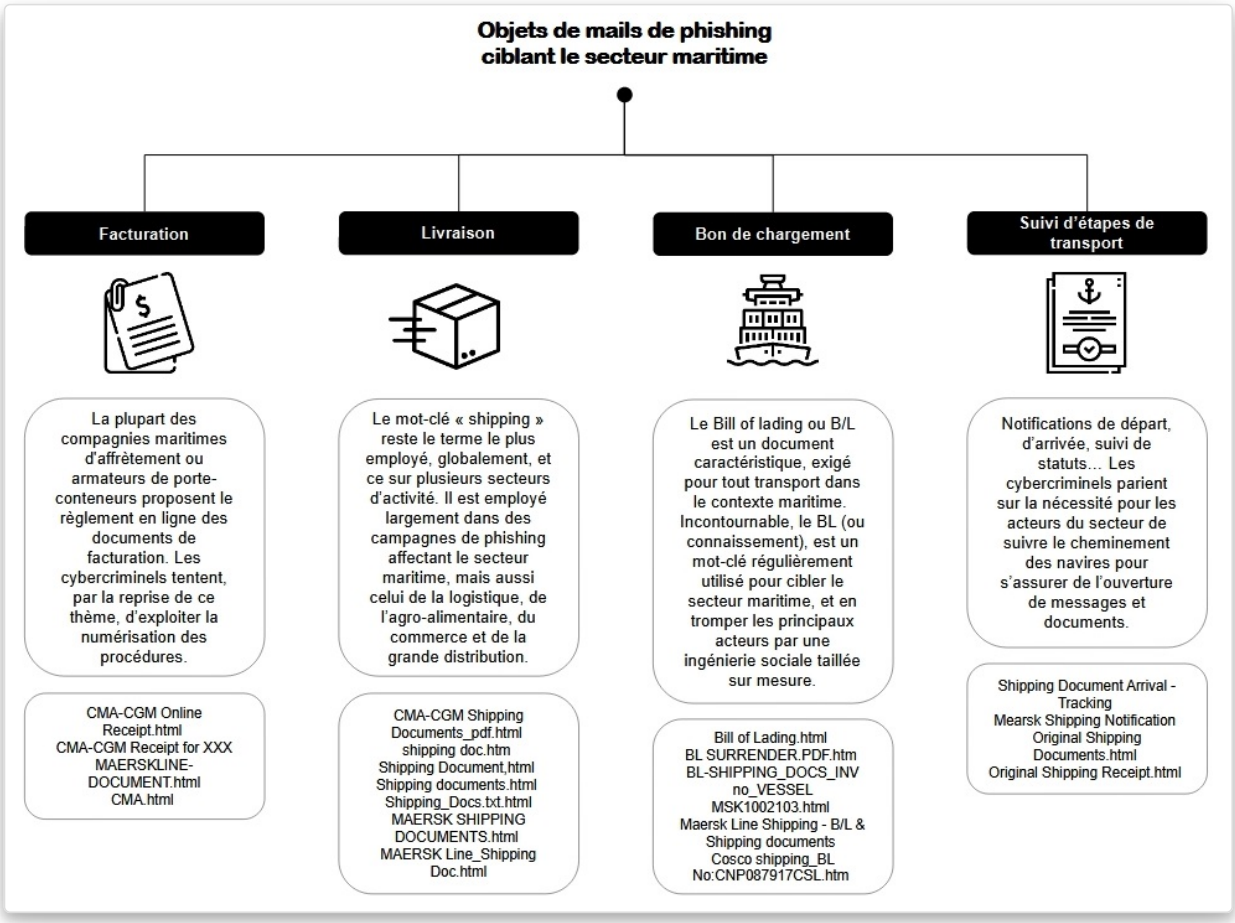



*Figure 3-5 : Objets de courriels de phishing ciblant le secteur maritime. Source : OWN-CERT.*


*Figure 3-6 : Nuage de mots de l'ensemble des thèmes d'ingénierie sociale utilisés lors de l'année 2022. Source : OWN-CERT.*

### 3.1.2. Spearphishing Attachement (T1566.001)

Pour être crédibles, les noms de fichiers malveillants joints aux campagnes de *phishing* adressées aux acteurs du secteur maritime reprennent les 5 thèmes suivants, parfois combinés: les noms de navires, les noms d'acteurs du secteur, les zones géographiques, les étapes logistiques et celui de la facturation.

Le nuage de mots Figure 3-7 montre les mots-clés qui apparaissent dans les fichiers exécutables envoyés aux victimes. Ici également, le champ lexical propre à la mer et au transport de marchandises est récurrent, avec la prédominance du terme « *Bill of Lading* » (Figure 3-8)

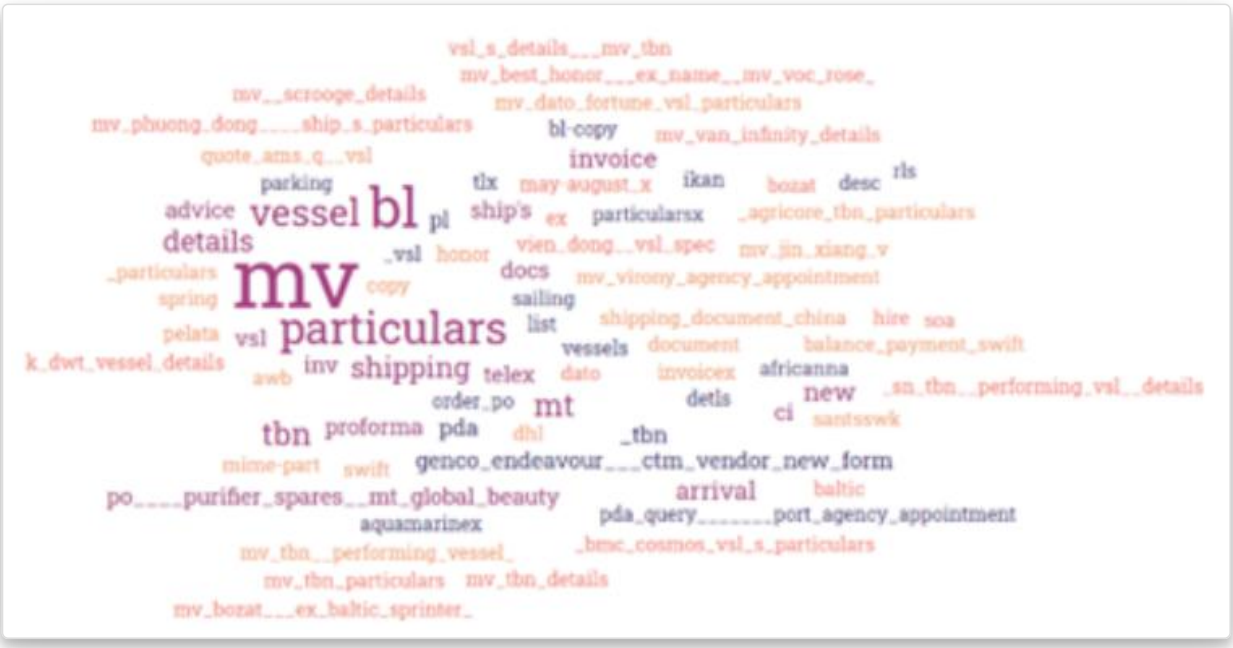



*Figure 3-7 : Nuage de mots-clés pour les noms de fichiers malveillants ciblant le secteur maritime. Source : OWN-CERT.*

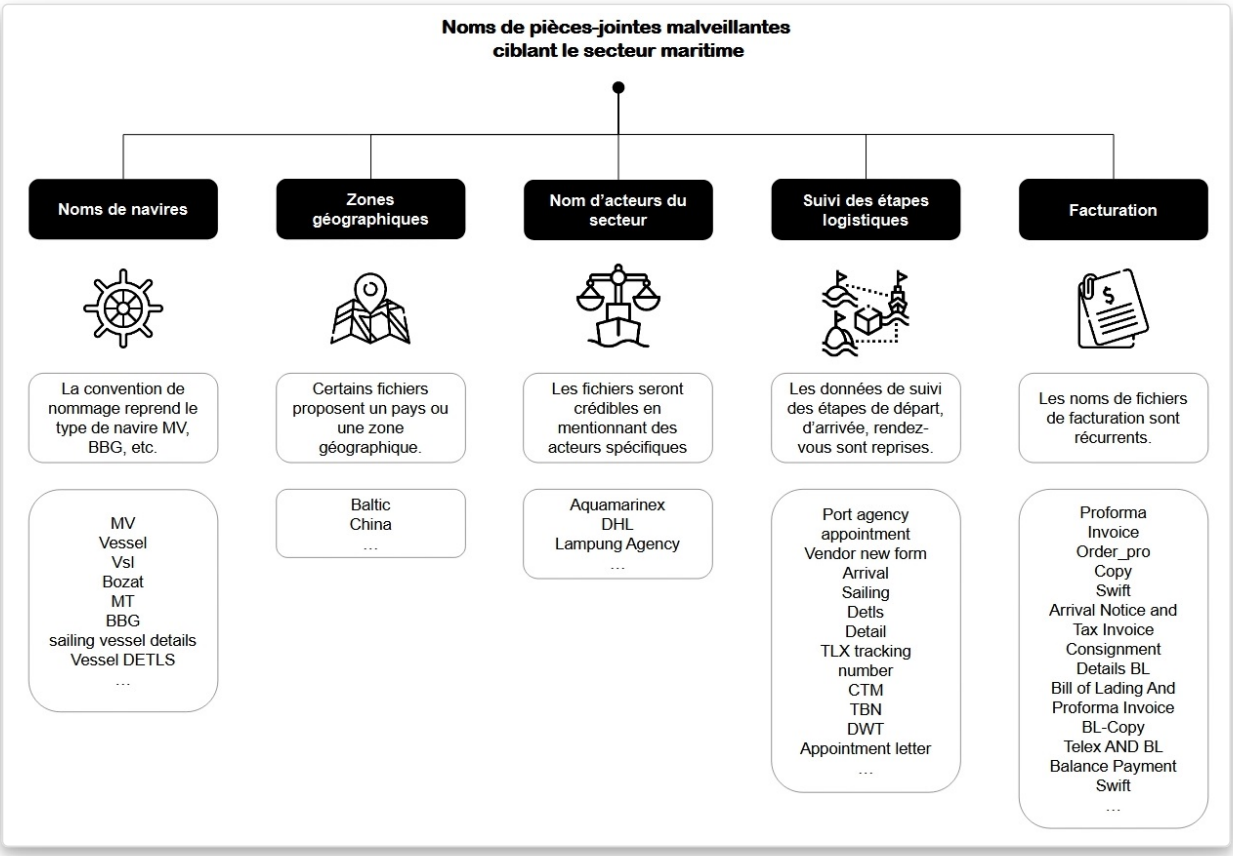



*Figure 3-8 : Noms de pièces jointes malveillantes ciblant le secteur maritime. Source : OWN-CERT.*

## 3.2. Les *infostealers* et le secteur maritime

Durant ses activités de suivi des menaces affectant le secteur maritime, OWN a collecté sur l'année 2022 plus de 2 200 binaires malveillants uniques, dont plus de 1 600 sont des *infostealers*. Ces chiffres confirment la tendance générale: OWN a pu identifier que la majorité des sujets relatifs aux codes malveillants sur les forums cybercriminels en 2022 concerne les *infostealers*. Ces codes malveillants sont vendus sur des canaux cybercriminels en tant que « *malware-as-a-service* ».

| Définition |
| --- |
| Un *infostealer* est un code malveillant conçu pour collecter des données sur un système d'information. Ces données concernent notamment les informations de connexion (bancaires ou des cookies de session) (Figure 3-9). |

Sur le plan méthodologique, l'ensemble des indicateurs collectés sur l'année 2022 a fait l'objet d'enrichissement afin d'identifier les codes malveillants distribués, les techniques employées, les infrastructures malveillantes et les modes opératoires adverses en activité.

24 familles *d'infostealers* affectant le maritime ont ainsi été détectées sur l'année, avec une nette majorité d'échantillons de **Formbook** (aussi appelé **Xloader**) , **Agent Tesla**, **Snake Keylogger** et **Lokibot** (Figure 3-10).

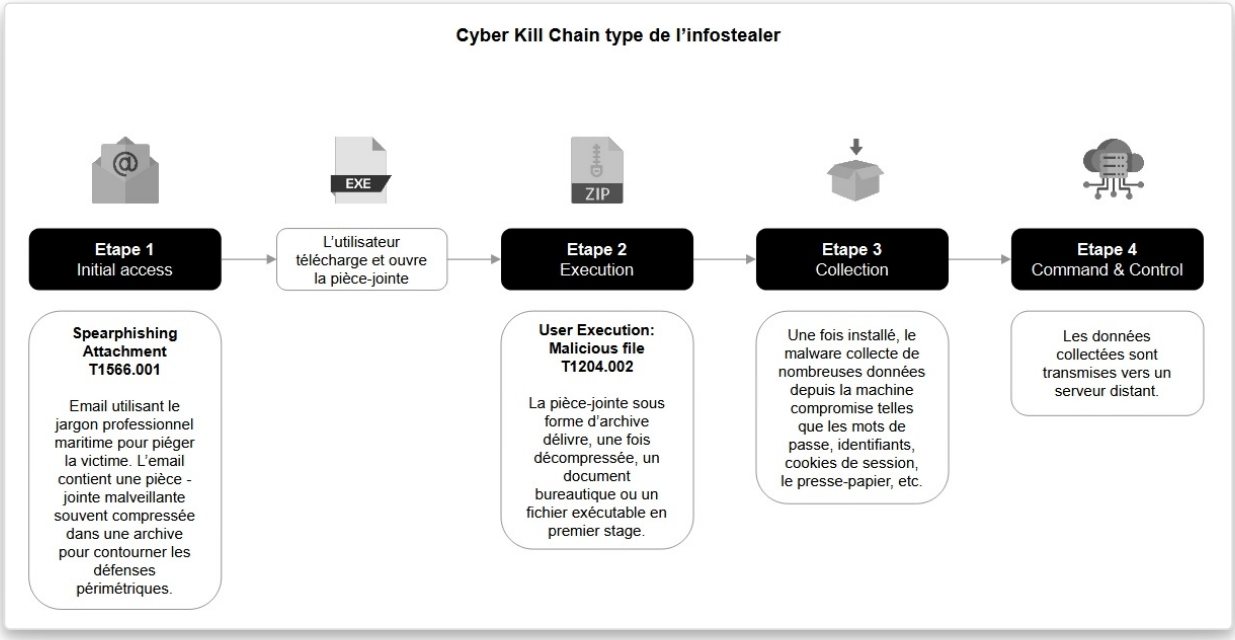



*Figure 3-9 : Cyber kill chain type de l'infostealer. Source : OWN-CERT.*

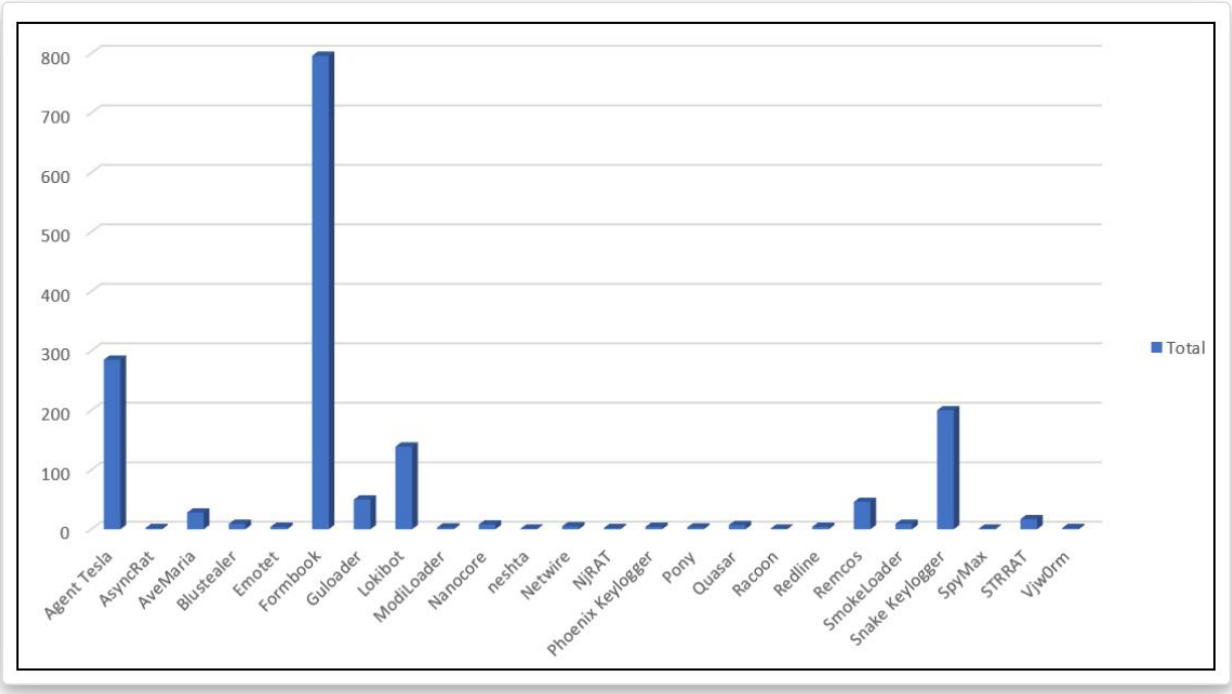



*Figure 3-10 : Nombre de fichiers par famille de code malveillant. Source : OWN-CERT.*

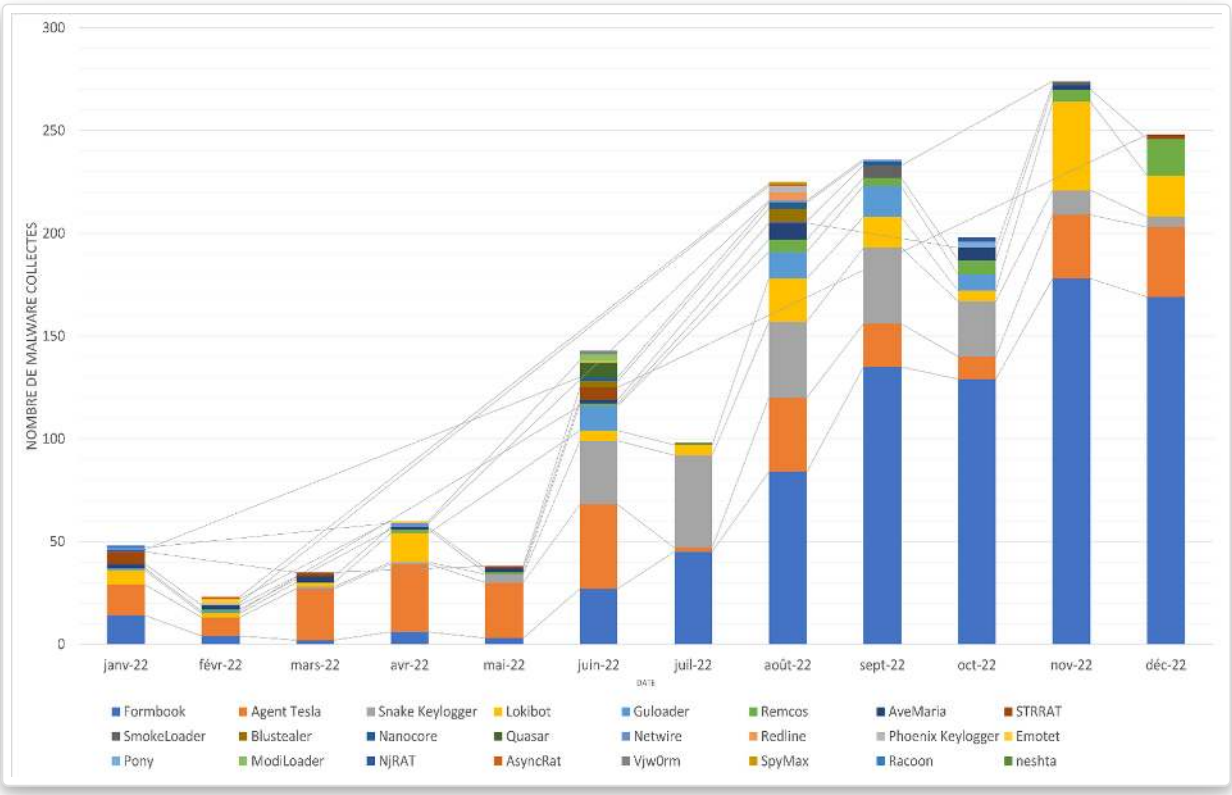



*Figure 3-11 : Evolution mensuelle du volume d'infostealers observés en 2022. Source : OWN:CERT.*

La Figure 3-11 montre l'évolution du nombre de fichiers collectés chaque mois par famille de code malveillant. Plusieurs constats peuvent être dressés :

- Une constante augmentation du nombre de fichiers malveillants ciblant le secteur maritime, avec un pic en fin d'année ;
- Une présence équilibrée tout au long de l'année des infostealers Formbook, Agent Tesla et Lokibot ;
- Une forte augmentation du nombre de fichiers liés à Snake Keylogger et Remcos dès l'été 2022.

### 3.2.1. Formbook (Xloader)

Au cours de l'année 2022, OWN a identifié 796 échantillons délivrant Formbook à des cibles du secteur maritime. Ce « *malware as a service* » est vendu sur plusieurs forums cybercriminels. Il est souvent distribué via courrier électronique assorti d'ingénierie sociale incitant la victime à l'exécuter sur son poste.

| Définition |
| --- |
| Formbook, également appelé Xloader, est un *infostealer* dédié au vol de données, de formulaires et de mots de passe. Le code malveillant s'injecte dans divers processus et installe des fonctions lui permettant d'enregistrer les frappes au clavier (*keylogger*), récupérer les contenus de presse-papiers, prendre des captures d'écran ou extraire des données de sessions http. Il peut aussi exécuter des commandes à partir d'un serveur de commande et contrôle (C2). Plus de 92 applications ont été identifiées comme étant la cible du code malveillant, parmi lesquelles « firefox.exe », « chrome.exe », « microsoftedgecp.exe », « opera.exe », « safari.exe » ou encore « WhatsApp.exe »[9]. |

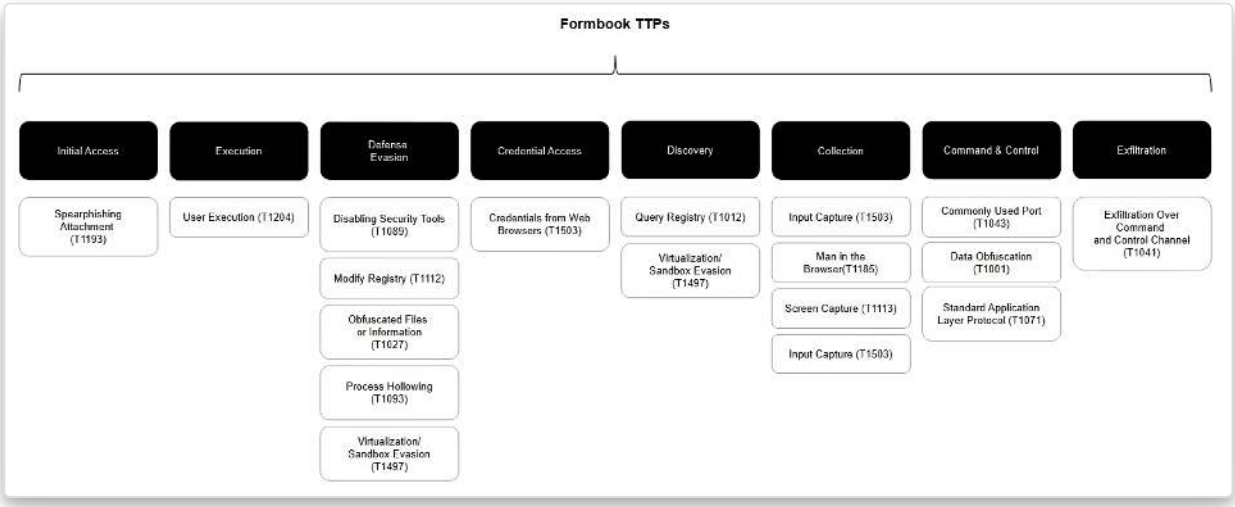



*Figure 3-12 : Tactiques, techniques et procédures de Formbook. Source : MITRE ATT&CK.*

Une fois décompressé le fichier[10] au format d'archive .rar dépose un exécutable *Formbook* sur le poste compromis[11]. L'exécutable reprend le vocabulaire sectoriel en utilisant le format de

dénomination de navires existant « MV[12] nom du navire » . Au cours de différentes campagnes, il arborera plusieurs noms de navires (Figure 3-13).

En analysant les entêtes du courrier électronique, OWN a pu observer l'usurpation d'une entreprise de frêt de marchandises basée à Singapour : PLATINA BULK CARRIERS. Le corps du courrier électronique confirme que l'attaquant est bien informé du jargon professionnel sectoriel et l'emploie afin de récolter des informations sur le port ciblé et inciter la victime à exécuter la pièce jointe. En pivotant sur l'adresse IPv4 du serveur d'envoi, OWN a été en mesure d'identifier de nombreux autres courriers électroniques ciblant expressément le secteur maritime sur la même période. Tous délivrent une pièce jointe malveillante (Figure 3-14).

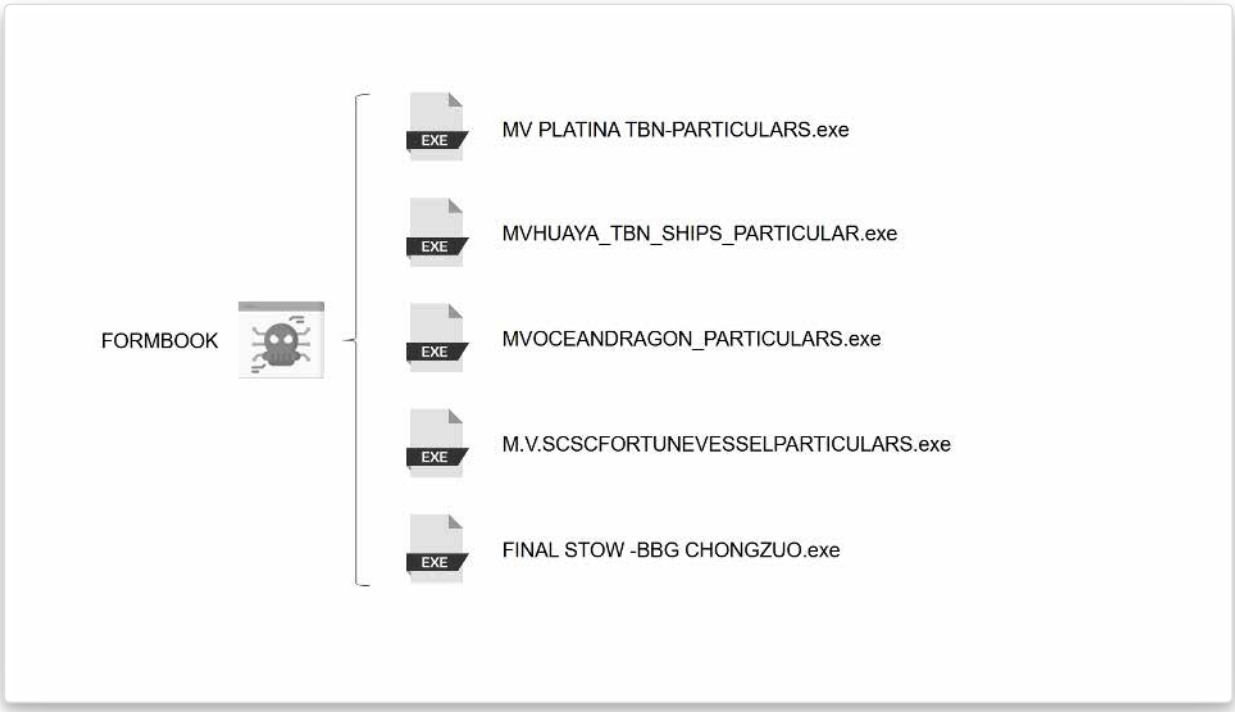



*Figure 3-13 : Noms de navires utilisés durant les campagnes.*

Au cours de l'investigation sur ce cluster spécifique, OWN a pu identifier plus de 600 autres fichiers malveillants liés à Formbook partageant notamment des serveurs de commande et contrôle. Tous ces fichiers indiquent une campagne visant spécifiquement le secteur maritime et son écosystème.

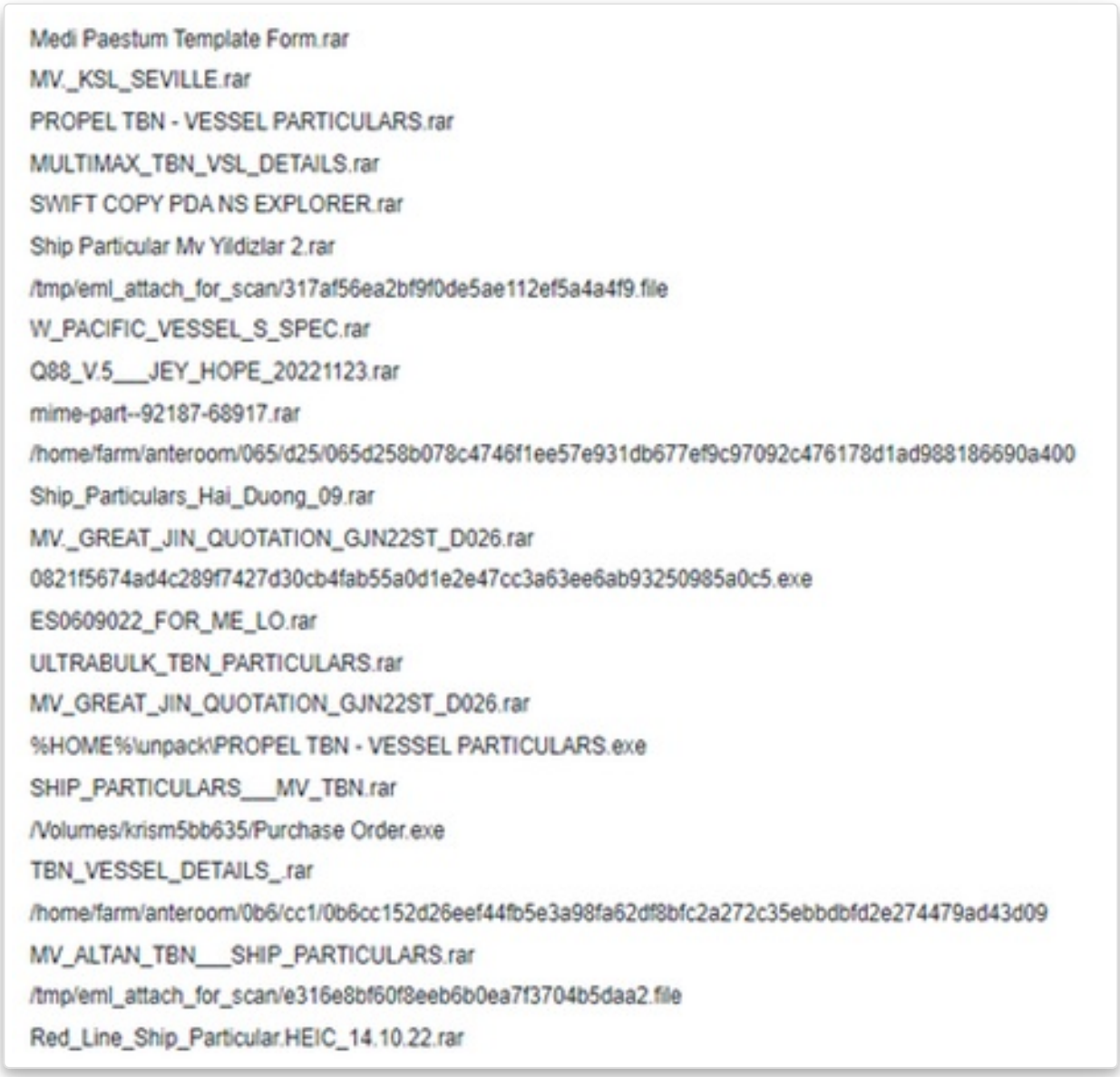



*Figure 3-14 : Exemples de noms de fichiers délivrant Formbook.*

### 3.2.2. Agent Tesla

| Définition |
| --- |
| Découvert fin 2014, Agent Tesla est un enregistreur de frappe au clavier ( *keylogger*) possédant de nombreuses fonctionnalités telles que l'enregistrement du presse-papiers, la capture d'écran, l'extraction de mots de passe stockés à partir de nombreux navigateurs. Il prend en charge toutes les versions du système d'exploitation Windows et il est écrit en .NET. |

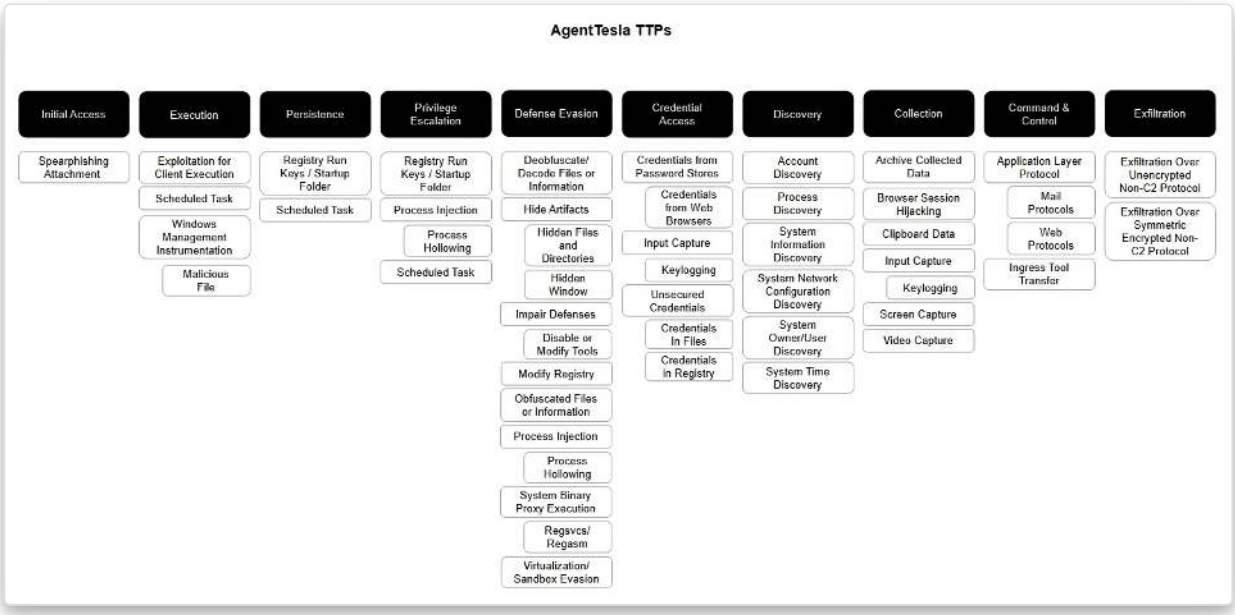



*Figure 3-15 : Tactiques, techniques et procédures d'AgentTesla. Source : MITRE ATT&CK.*

Agent Tesla a été omniprésent au cours de l'année 2022. Dans plusieurs courriers électroniques collectés, l'attaquant usurpe l'identité et les infrastructures d'armateurs (Figure 3-16). L'archive jointe au courrier électronique est décompressée et exécute un échantillon d'Agent Tesla[13]. Ce dernier récupère les identifiants de courrier électronique, ainsi que des données stockées par les navigateurs. Les informations collectées sont exfiltrées vers un *bot* Telegram.

```
Received: from unknown by localhost (amavisd-new, unix socket) id 89ldNodfiRbV
        for <brotaru@electroputere.ro>; Tue, 11 Oct 2022 10:48:34 +0300 (EEST)
Received: from maersk.com (unknown [45.137.22.249])
        by spin.electroputere.ro (amavisd-milter) with ESMTP id 29B7mRnp021289;
        Tue, 11 Oct 2022 10:48:27 +0300
        (envelope-from <info@maersk.com>)
From: "services" <info@maersk.com>
To: brotaru@electroputere.ro
Subject: TOP URGENT//RE:SHIPMENT SCHEDULE/MAERSK SHIPPING LINE.
```

*Figure 3-16 : Exemple d'entête d'un courriel délivrant AgentTesla, et usurpant Maersk.*

### 3.2.3. Lokibot

| Définition |
| --- |
| Lokibot est un logiciel malveillant vendu sur des forums cybercriminels. Il est conçu pour subtiliser des données sur les machines infectées, puis soumettre ces informations à un hôte de commande et de contrôle via HTTP POST. Ces données sont principalement des mots de passe stockés, des informations d'identification des navigateurs web ainsi que des portefeuilles de cryptoactifs. |

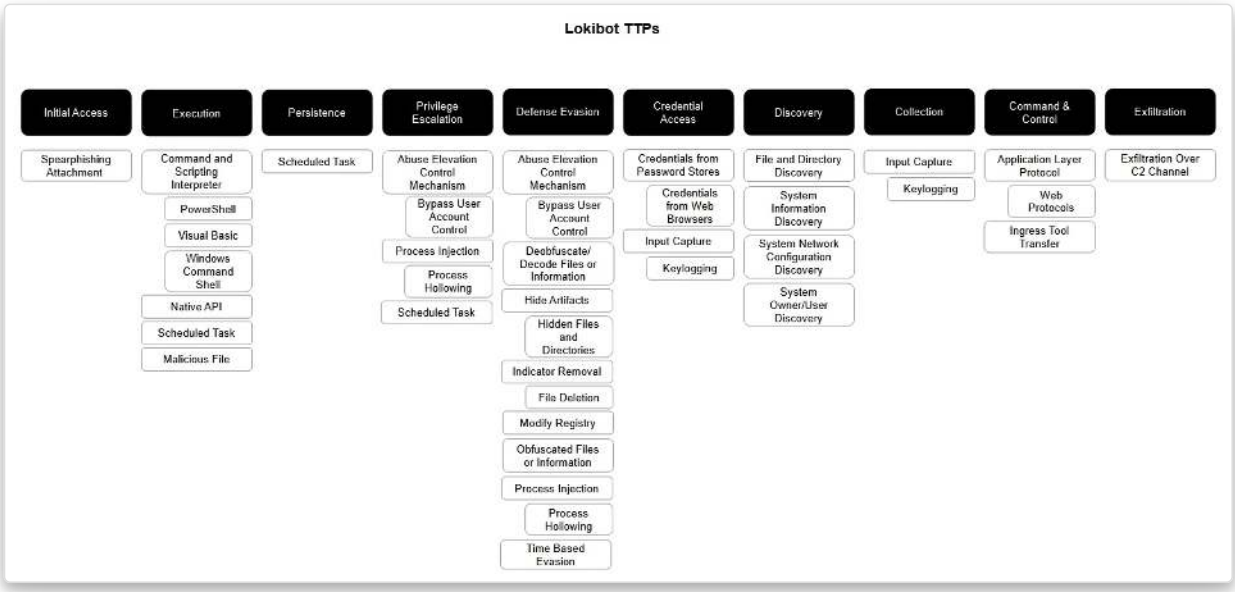



*Figure 3-17 : Tactiques, techniques et procédures de Lokibot. Source : MITRE ATT&CK.*

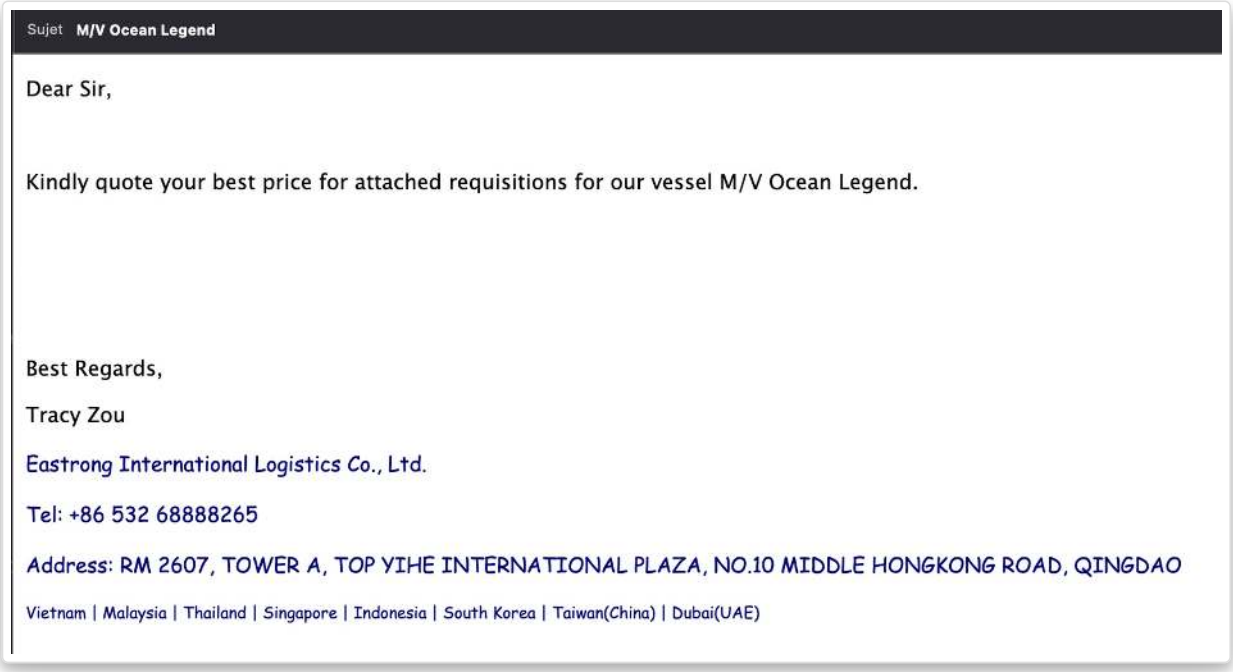



*Figure 3-18 : Courriel malveillant distribuant Lokibot dans une campagne ciblant le secteur maritime.*

Un des échantillons[14] distribués lors de campagnes d'attaques visant le secteur maritime, et récoltés par OWN, délivre le code malveillant Lokibot via un fichier Excel transmis en pièce jointe d'un courriel de *phishing* (Figure 3-18). Le fichier Excel[15] suit la nomenclature « MV_NOM_NAVIRE » et, cette fois, reprend le nom du navire « *Ocean Legend* ». Une fois le document ouvert, une fausse notification Office apparaît et demande à l'utilisateur d'activer la modification du document (Figure 3-19).

Cette activation va permettre l'exploitation de la vulnérabilité CVE-2017-11882 (*Microsoft Office Memory Corruption Vulnerability*) qui touche un composant de MS Office appelé « *Equation Editor* » et conduit à l'exécution de code à distance sur la machine infectée. Pour Lokibot, cette faille est utilisée pour se connecter au serveur de commande et contrôle et récupérer la dernière étape de son exécution.

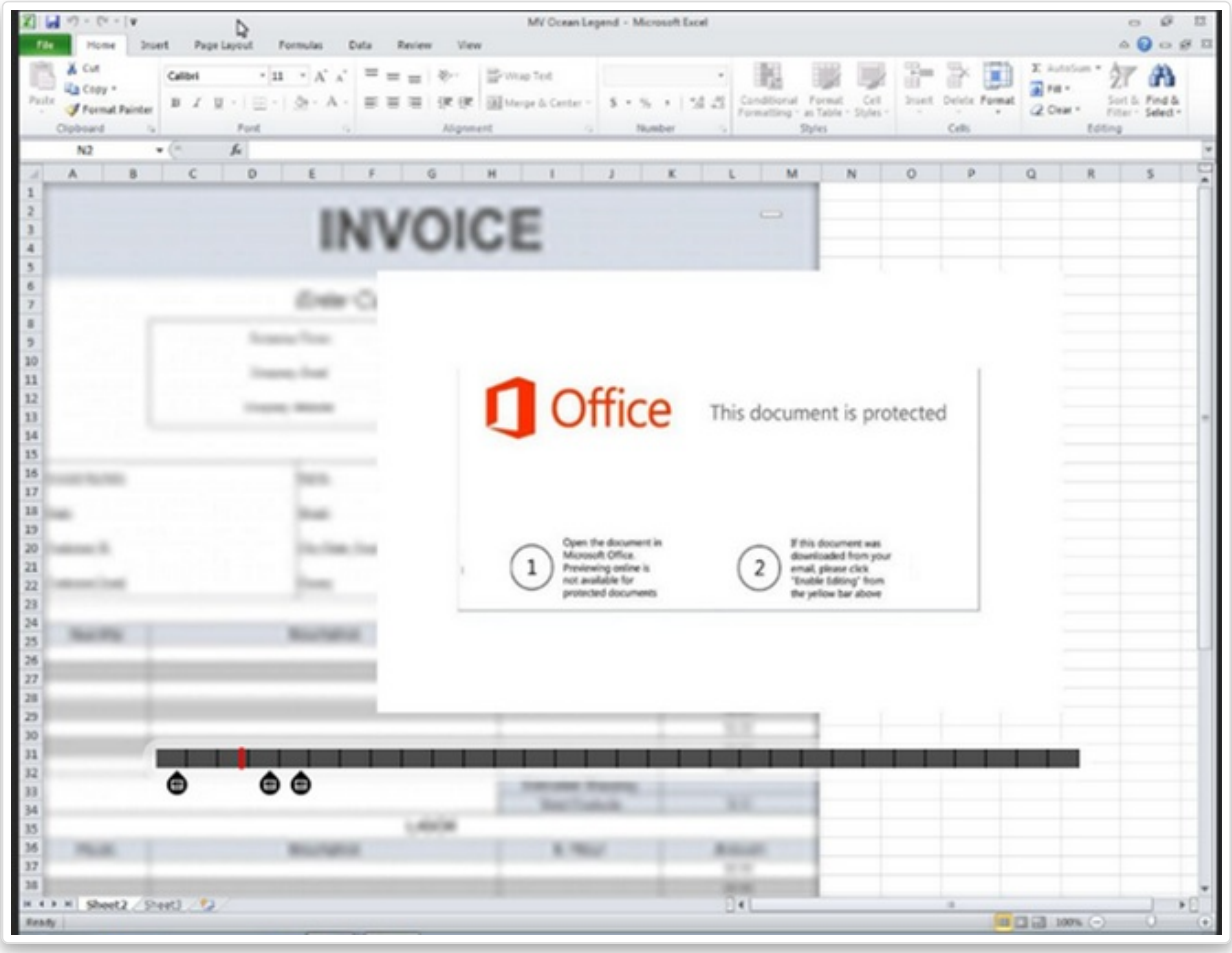



*Figure 3-19 : Fichier Microsoft Excel malveillant.*

### 3.2.4. Vector Stealer

En février 2023, une récente souche d'infostealer a été remontée par les règles de détection du OWN-CERT comme pouvant viser le secteur maritime : Vector Stealer. Bien que ces campagnes aient été initiées en 2023 (Figure 3-20), Vector Stealer est en vente sur les canaux cybercriminels depuis 2022.

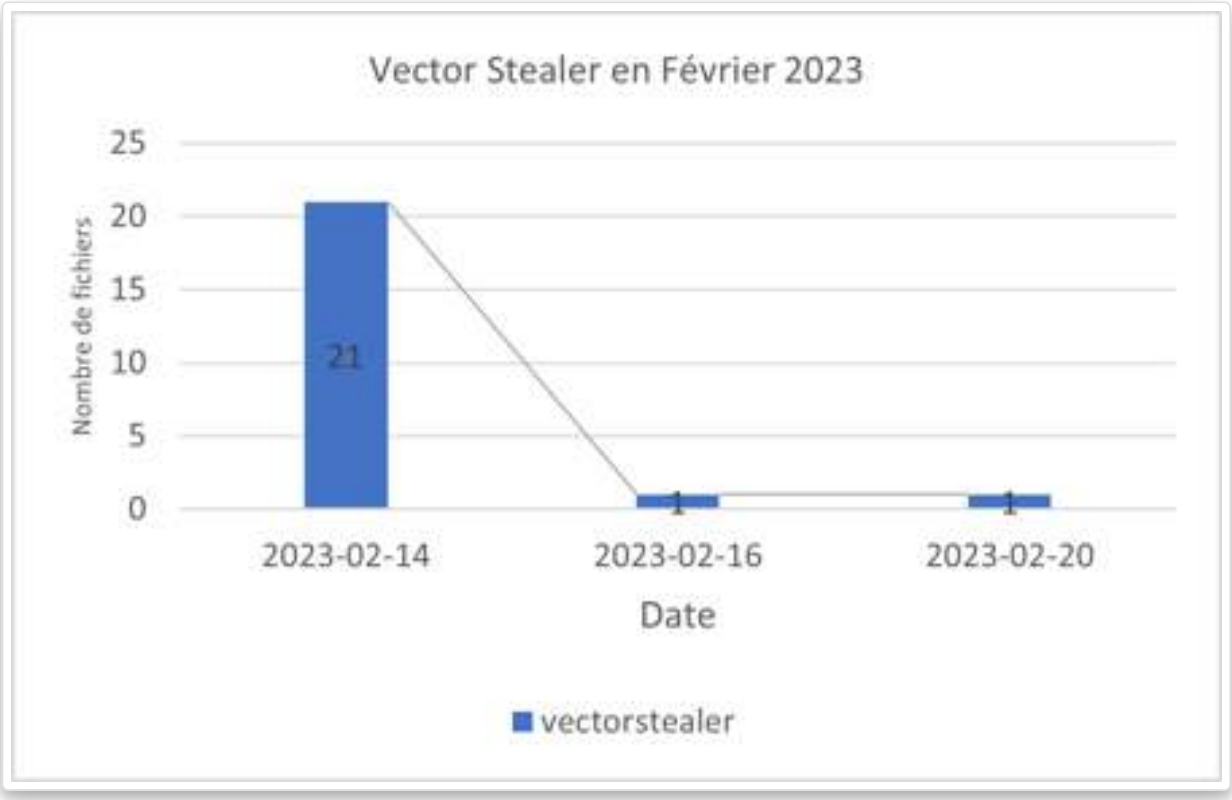



*Figure 3-20 : 23 vagues de distribution de Vector Stealer ont été identifiées.*

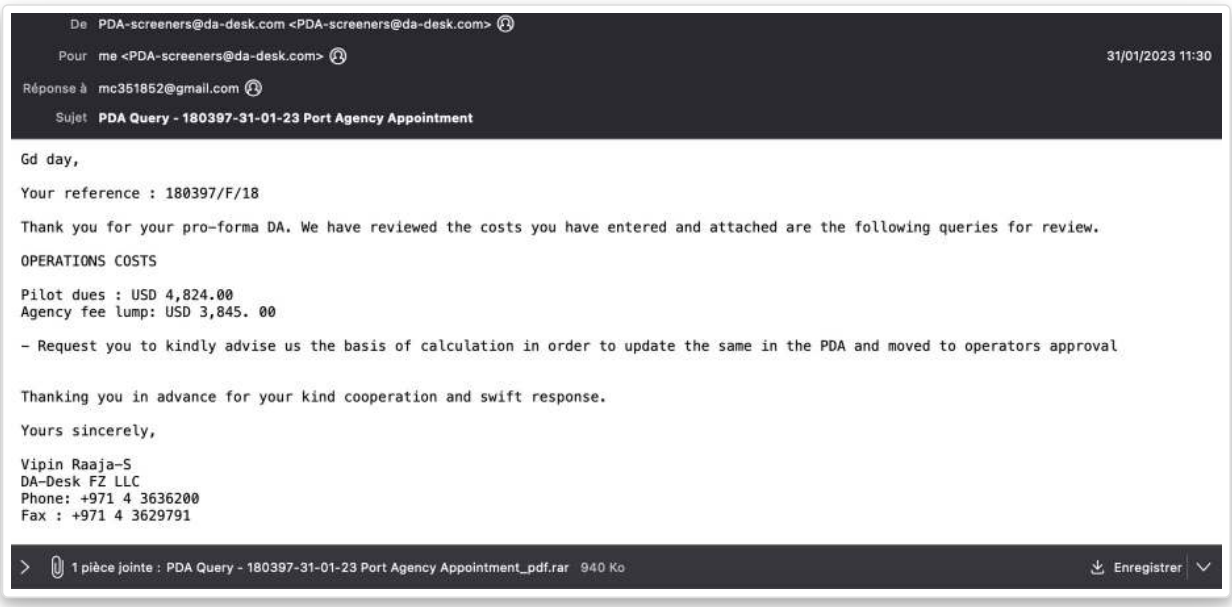



*Figure 3-21 : Courrier électronique distribuant Vector Stealer au secteur maritime.*

Le code malveillant se propage via courrier électronique, sous forme de pièce jointe, comme les précédents *infostealers* documentés. Dans l'exemple choisi, le courrier électronique comporte une

archive .rar prétendant être une facture d'escale d'un navire nommée « PDA Query – 180397-31-01-23 Port Agency Appointment_pdf.exe ». L'archive délivre un exécutable de *Vector Stealer* nommé « KOREA SHIPPING – KLCSM)_pdf.exe » [16](Figure 3-21).

Une fois exécuté, le code malveillant délivre un exécutable nommé de façon aléatoire. Le fichier collecte des données issues des clients de messagerie tels qu'Outlook et Foxmail. Vector Stealer a également la particularité de cibler les fichiers liés au protocole RDP pour garder un accès sur la machine ciblée. Il crée un dossier d'exfiltration dans le répertoire «AppData» afin d'y stocker les données volées. Ces données seront exfiltrées vers un bot Telegram (Figure 3-22).

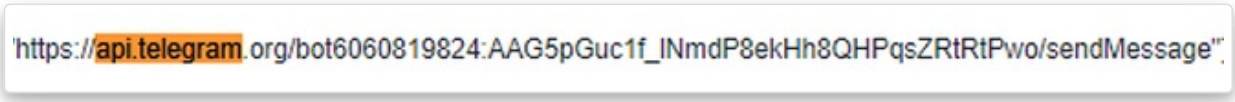



*Figure 3-22 : Exfiltration des données vers Telegram.*

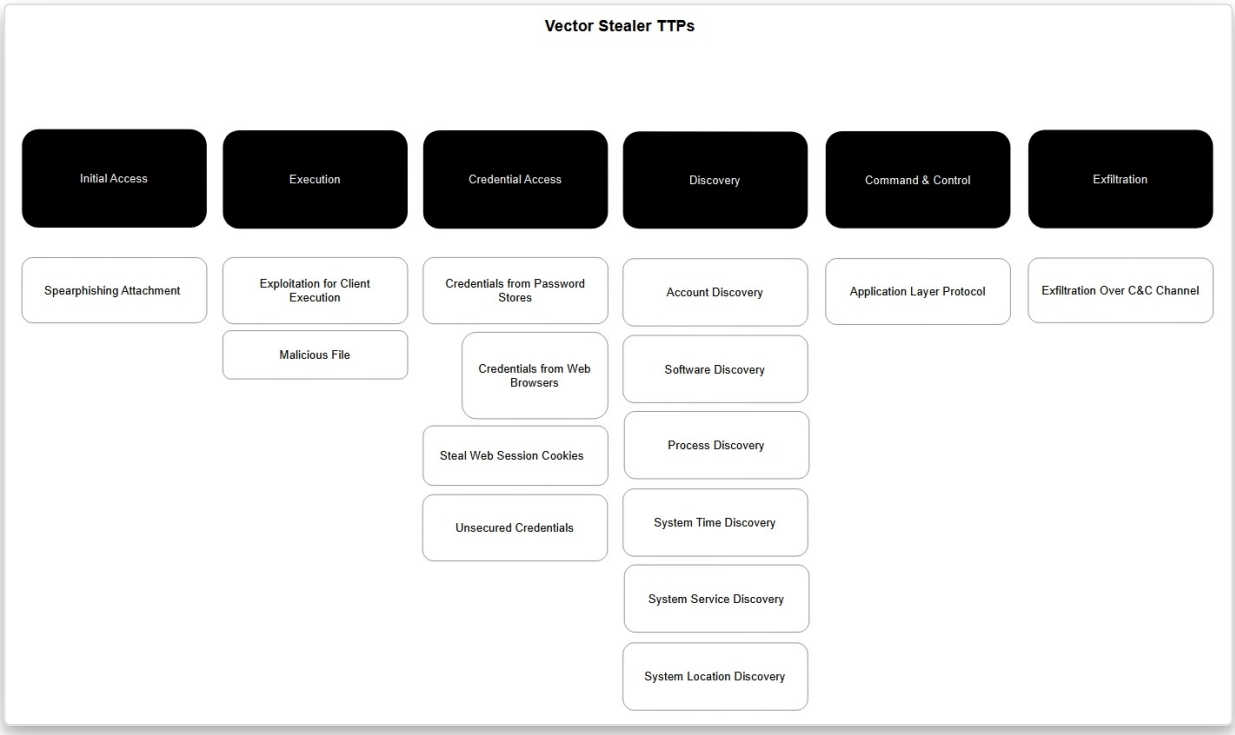



*Figure 3-23 : Tactiques, techniques et procédures de Vector Stealer. Source : OWN.*

## 3.3. Fuites et reventes de données du secteur maritime

Les plateformes de vente d'identifiants d'accès initial (*Initial Access Brokers, IAB*) sont devenues des carrefours incontournables de l'écosystème cybercriminel, essentielles notamment au fonctionnement des « *Ransomware as a Service* ». De la même manière que l'outillage de certains rançongiciels est vendu à des affiliés, la recherche des points d'entrée sur les systèmes d'information des victimes (*initial access*) peut également être sous-traitée. OWN mène une surveillance accrue des canaux

cybercriminels à la recherche de potentielles fuites ou ventes de données concernant le secteur maritime. Bien qu'isolés, certains cas de vente ou de fuite ont été identifiés sur l'année 2022.

Les canaux cybercriminels (marchés, forums, chaînes Telegram…) permettent la mise en vente d'outils nécessaires à l'exécution d'attaques, tels que des codes malveillants, des identifiants ou encore des informations bancaires (numéros de carte bancaire, codes de vérification, etc.). Aucun secteur n'est spécifiquement visé car, dans cet écosystème, les acteurs agissent de manière opportuniste : ils vendent des bases de données de n'importe quelle entreprise, tant que cela peut leur être profitable. Quelques exemples de fuites de données sont détaillés ci-après.

Actif depuis le 18 mars 2022, l'utilisateur Kelvinsecurity est spécialisé dans les fuites de données (*leaks*). Il a publié deux jeux de données relatifs à deux entités du secteur maritime (une entreprise fournissant de l'électronique de marine et une agence ministérielle maritime). Les fuites annoncées concerneraient des clés privées de systèmes Very Small Aperture Terminal (VSAT) de yachts privés et de navires militaires (Figure 3-24) ou encore des données telles que noms, prénoms, courriers électroniques, adresses, téléphones, etc. (Figure 3-25).


*Figure 3-24 : Annonce d'une fuite de données par l'utilisateur Kelvinsecurity. Source : OWN-CERT.*

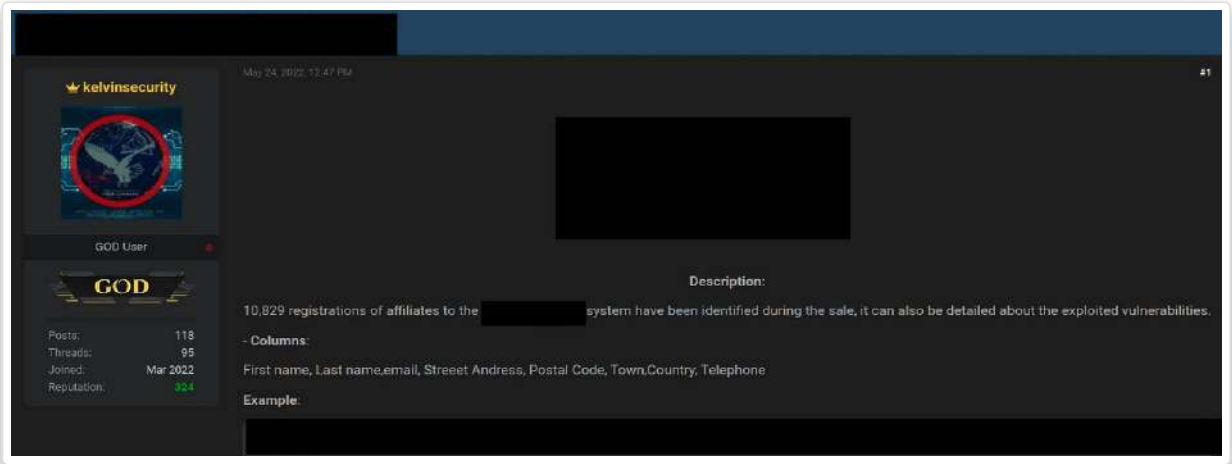



*Figure 3-25 : Annonce d'une fuite de données par l'utilisateur Kelvinsecurity. Source : OWN-CERT.*

Autre utilisateur d'intérêt, YourAnonWolf, actif depuis mars 2022, est connu pour être le leader de SiegedSec, un groupe cybercriminel apparu en février 2022 et spécialisé dans la vente de données issues de fuites et de défacement de sites Internet. Les modes opératoires types des membres du groupe peuvent s'orienter vers l'injection SQL, l'exploitation de failles XSS, de vulnérabilités dans des plateformes de création de site, voire les attaques par force brute.

La victime présumée de YourAnonWolf serait une académie maritime (Figure 3-26). Les données mises en vente seraient issues de fichiers présents sur des serveurs FTP, de courriers électroniques ou encore de services cloud utilisés par l'école.


*Figure 3-26 : Annonce d'une fuite de données par l'utilisateur YourAnonWolf. Source : OWN-CERT.*

Les groupes cybercriminels migrent massivement vers des messageries chiffrées, notamment Telegram, pour éviter la surveillance ou profiter d'une plateforme de publication non censurée (les comptes Twitter des groupes d'attaquants étant régulièrement suspendus). La décentralisation de Telegram constitue une couche de dissimulation supplémentaire ainsi qu'un canal de communication redondant. Ainsi, les chaînes Telegram recoupent partiellement les forums et les marchés noirs. C'est ce qu'a fait notamment YourAnonWolf en publiant son annonce de manière conjointe à la fois sur un forum de revente de données et sur le compte Telegram de SiegedSec.

Plusieurs autres exemples peuvent être cités : Le 11 septembre 2022, un membre d'un forum de fuites de données prétend détenir des données sur la Marine d'un pays (Figure 3-27).

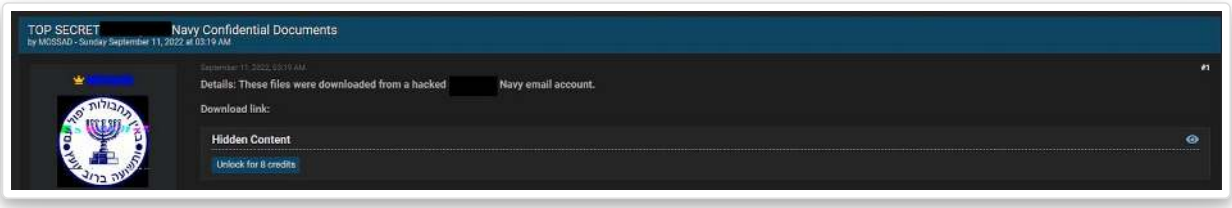



*Figure 3-27 : Annonce d'une fuite de données concernant la Marine d'un pays sur un forum spécialisé. Source : OWN-CERT.*

Le 14 septembre 2022, 17.5 Go de données appartenant à une entreprise de construction navale ont été mis en vente sur un forum de fuite de données (Figure 3-28).

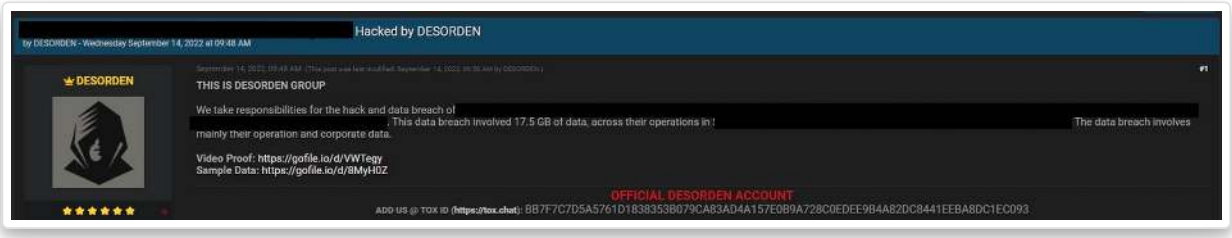



*Figure 3-28 : Annonce d'une fuite de données concernant un chantier naval sur un forum spécialisé. Source : OWN-CERT.*

| Recommandations |
| --- |
| En cas d'annonce de publication d'informations volées, il est nécessaire d'évaluer l'importance de la fuite potentielle et son origine. Les données peuvent avoir été volées au moyen de l'exploitation d'un actif vulnérable accessible publiquement sur Internet, d'une compromission par code malveillant ou par un accès légitime utilisant des identifiants volés. Une mauvaise configuration d'un serveur ou d'une application peut également être la cause de la fuite. Une analyse complète des actifs exposés, mais aussi de la source de la menace et des fichiers qu'elle publie permettront de prioriser ces recherches. |

Seule une investigation complète du système d'information permettra d'évaluer la véracité de la fuite et son impact sur le système d'information.
Une sensibilisation à ce type de risque des dirigeants, des équipes de supervision du SI, ainsi que des responsables de la communication, voire du département légal, peut permettre à l'organisation de mieux faire face lors de la survenue d'une fuite de données.

Les *Initial Access Brokers* peuvent travailler pour leur propre compte : dans ce cas, une fois l'accès initial obtenu, ils revendent directement les données dérobées au plus offrant sans poursuivre l'attaque. Ils peuvent également participer à la chaîne d'exécution d'une opération globale (*Business Email Compromise* ou rançongiciel), où l'accès initial leur est sous-traité.

## 3.4. *Business Email Compromise (BEC)*

L e *Business Email Compromise (BEC)*, ou arnaque au Faux Ordre de Virement (FOVI), est une technique par laquelle l'attaquant utilise le courrier électronique pour inciter un employé à effectuer des virements de fonds ou à divulguer des informations confidentielles sur son entreprise.

L'acteur malveillant se fait passer pour une figure de confiance (autorité hiérarchique, direction financière, administration, client habituel, partenaire, banque…) et demande le paiement d'une fausse facture ou la transmission de données sensibles. Les comptes de messagerie d'entreprise sont préalablement usurpés ou compromis pour initier les discussions et effectuer des transferts frauduleux.

En 2022, des cas plus nombreux d'utilisation de messageries instantanées (comme Whatsapp) pour tenter de mener ce type d'attaque ont été reportés au M-CERT. Si le principe se rapproche de celui du

phishing, ces attaques plus ciblées s'appuient sur un sentiment de confiance plus fort, par l'utilisation de techniques d'ingénierie sociale bien plus sophistiquées que pour un simple courrier électronique. Elles sont ainsi souvent plus difficiles à reconnaître et s'avèrent parfois plus coûteuses dans leurs conséquences que d'autres attaques moins ciblées.

En mai 2022, le FBI Internet Crime Complaint Center a publié un rapport qui mettait en évidence la croissance continue des attaques *Business Email Compromise (BEC)[17]. Les pertes mondiales dues aux BEC entre juillet 2019 et décembre 2021 ont augmenté de 65 % par rapport à l'année précédente et représentaient 35 % de l'ensemble des pertes imputables à la cybercriminalité.

En 2022, on peut notamment citer le cas d'une organisation du secteur maritime qui a été victime de ce type d'arnaque au mois d'avril[18].

### 3.4.1. Retour sur le mode opératoire SILVER TERRIER

En janvier 2022, Interpol a arrêté plusieurs personnes impliquées dans des opérations de BEC au Nigéria, suite à une coopération avec Palo Alto[19]. Leur mode opératoire était le suivant :

1. Envoi de courriels malveillants génériques (factures, confirmation de paiement SWIFT, bons de commandes, etc.) destinés à tromper la victime afin d'installer à son insu un code malveillant ou pour l'inciter à se rendre sur un site de *phishing* dont l'objectif est de dérober les identifiants de connexion à sa boîte de courrier électronique ;
2. Connexion à la boîte de courrier électronique de la victime et mise en place de règles de transfert automatique selon certains mots-clés ou surveillance manuelle des courriers électroniques ;
3. Lorsqu'une discussion sur un paiement est entamée entre la victime et l'un de ses prestataires ou fournisseurs, les fraudeurs déposent un nom de domaine proche du partenaire concerné (*typosquatting* : par exemple marrinsa[.]com pour usurper marinsa.com) et utilisent ce nom de domaine afin de s'insérer dans la conversation en reprenant toute la chaîne de messages. Le fraudeur demande alors de procéder au paiement sur un autre compte bancaire en prétextant, par exemple, une indisponibilité de la banque ou une erreur de compte.

Si les parties concernées ne remarquent pas le changement de nom de domaine dans les courriers électroniques, ou en l'absence de protocole de vérification de ce type de changement, le risque de réaliser le paiement vers ce nouveau compte bancaire (détenu par les fraudeurs) est très élevé.

Parmi les personnes arrêtées, l'une d'elles ciblait plus particulièrement les sociétés de logistique, en créant de nombreux domaines afin de tromper les utilisateurs, par exemple :

- atlanticexpresslogistics[. ]com
- clarionsshipping[. ]com
- dpdexpressuk[. ]com

- dynamicparceldelivery[. ]com
- shipatlanticlogistics.co[. ]uk.

Selon PaloAlto, cette personne aurait enregistré plus de 250 noms de domaines et ces domaines seraient liés à l'utilisation de différentes familles de codes malveillants (chevaux de Troie ou infostealers) dont Formbook, Agent Telsa, PredatorPain, Nanocore, DarkComet, etc. Cette personne utilisait souvent les pseudos « Fyzee » et « Encryption Code » sur différents forums cybercriminels, ainsi que sur les réseaux sociaux tels que Facebook. Son activité sur ces espaces est alors le reflet de son activité criminelle : il acquiert des logiciels pour copier des sites, créer des fichiers Word infectés ou décliner des chevaux de Troie, notamment Nanocore ou Betabot. Le suivi de l'activité de cet individu par le OWN-CERT confirme son mode opératoire : création de sites à des fins d'escroquerie, puis infection des utilisateurs afin de récupérer leurs données.

Bien que ces techniques soient relativement simples, elles sont éprouvées depuis plusieurs années et terriblement efficaces : près de 20 000 victimes sont recensées chaque année aux États-Unis, pour des montants de fraude compris entre 1 et 2 milliards de dollars. Le risque de ce type d'attaque est avant tout financier, car ces acteurs cherchent à détourner des flux d'argent, et apparaît donc minimal pour l'aspect opérationnel du secteur maritime.

Il est occasionnellement possible de remonter à l'identité du fraudeur, car ceux-ci sont souvent assez peu regardants sur leur sécurité opérationnelle, ce qui facilite leur arrestation. Néanmoins, le fait que des individus ayant déjà été arrêtés par Interpol en 2020 soient arrêtés à nouveau fin 2021 reflète les difficultés à endiguer de façon pérenne ce type de criminalité. L'impact de ces arrestations sera très certainement indolore au regard des volumes d'attaque observés. En effet, des dizaines de milliers de noms de domaines sont déposés chaque année pour réaliser ce type de fraude, ce qui implique une logistique et une automatisation importante de la part de ces acteurs. En témoignent les investigations menées par le OWN-CERT qui ont permis, sur l'année 2022, de caractériser plusieurs modes opératoires similaires ciblant notamment le secteur maritime, dont POSEIDON-IS_001.

### 3.4.2. Focus sur le mode opératoire POSEIDON-IS_001

Un acteur de la menace ciblant le secteur maritime a été identifié par les équipes du OWN-CERT. Surnommé POSEIDON-IS_001, il opère depuis 2019 et est encore aujourd'hui en activité. Son mode opératoire se caractérise par l'usage de techniques d'hameçonnage et l'utilisation de *l'infostealer* Lokibot. Ont également été identifiées de sa part des campagnes d'hameçonnage usurpant l'identité de DHL, Excel, Outlook ou encore Yahoo.

Un faisceau d'indices permet de rattacher POSEIDON-IS_001 au cluster SilverTerrier. Le OWN-CERT estime en effet avec un niveau de confiance élevé que l'objectif final de POSEIDON-IS_001 est probablement le vol de données et leur réutilisation dans le cadre d'attaques BEC. Dans un premier exemple de campagne surnommée « Aldo Group », POSEIDON-IS_001 envoie ses courriers électroniques d'hameçonnage à partir du domaine aldoqroup[. ]com, usurpant la raison sociale de

l'entreprise Aldo group (Retail), ainsi que le nom d'un véritable employé de l'entreprise (Figure 3-29).

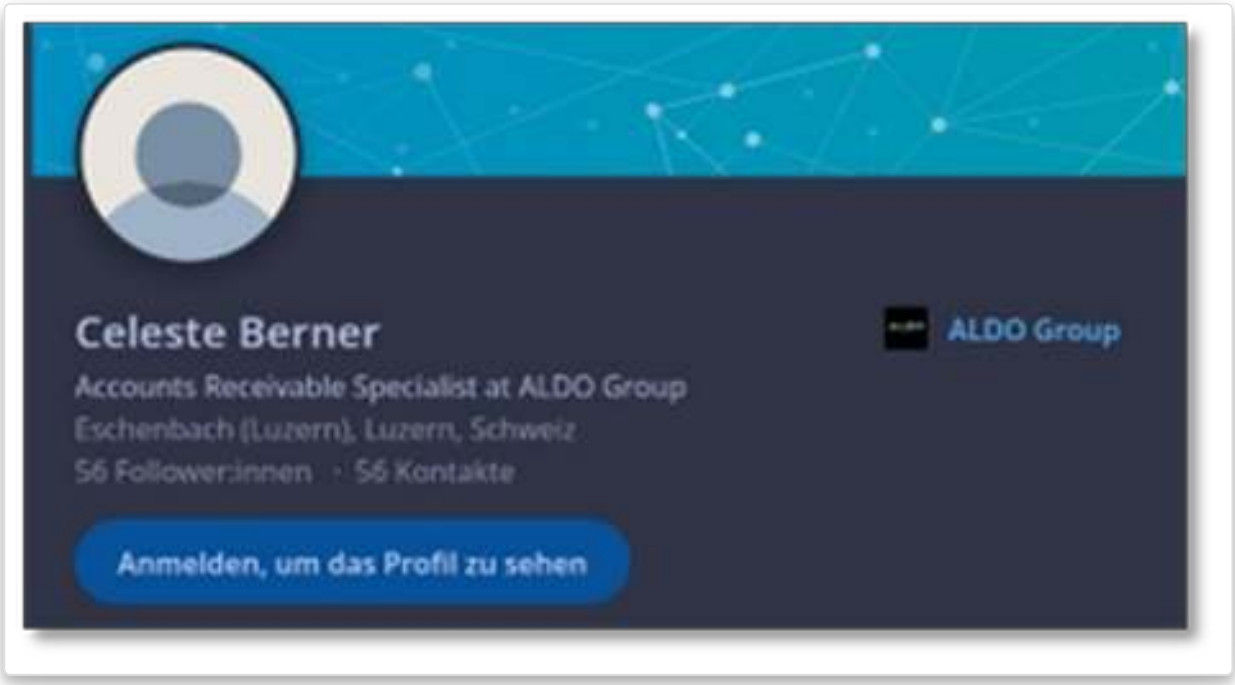



*Figure 3-29 : Compte d'employé légitime usurpé par POSEIDON-IS_001. Source : LinkedIn, OWN-CERT.*

Le courrier électronique envoyé à la victime (Figure 3-30) contient une pièce jointe nommée « 44 R.I MI2KT.rar. » Cette archive renferme un exécutable Lokibot (nommé : « EYQشSڤ0بچء.exe »[20]). Le domaine d'exfiltration de cet exécutable est un autre domaine possédé par POSEIDON-IS_001 : allamaldives[. ]com.

Dans une seconde campagne, POSEIDON-IS_001 envoie un courrier électronique malveillant à sa cible (dont l'activité consiste au développement de systèmes embarqués) en usurpant l'identité de « PetroSeis Asia » (dont l'activité consiste en des relevés hydrographiques pour des autorités portuaires). L'archive en pièce jointe contient ici aussi un exécutable Lokibot. Le sujet et le contenu du courrier électronique contiennent des termes relatifs au secteur du maritime (Figure 3-31).

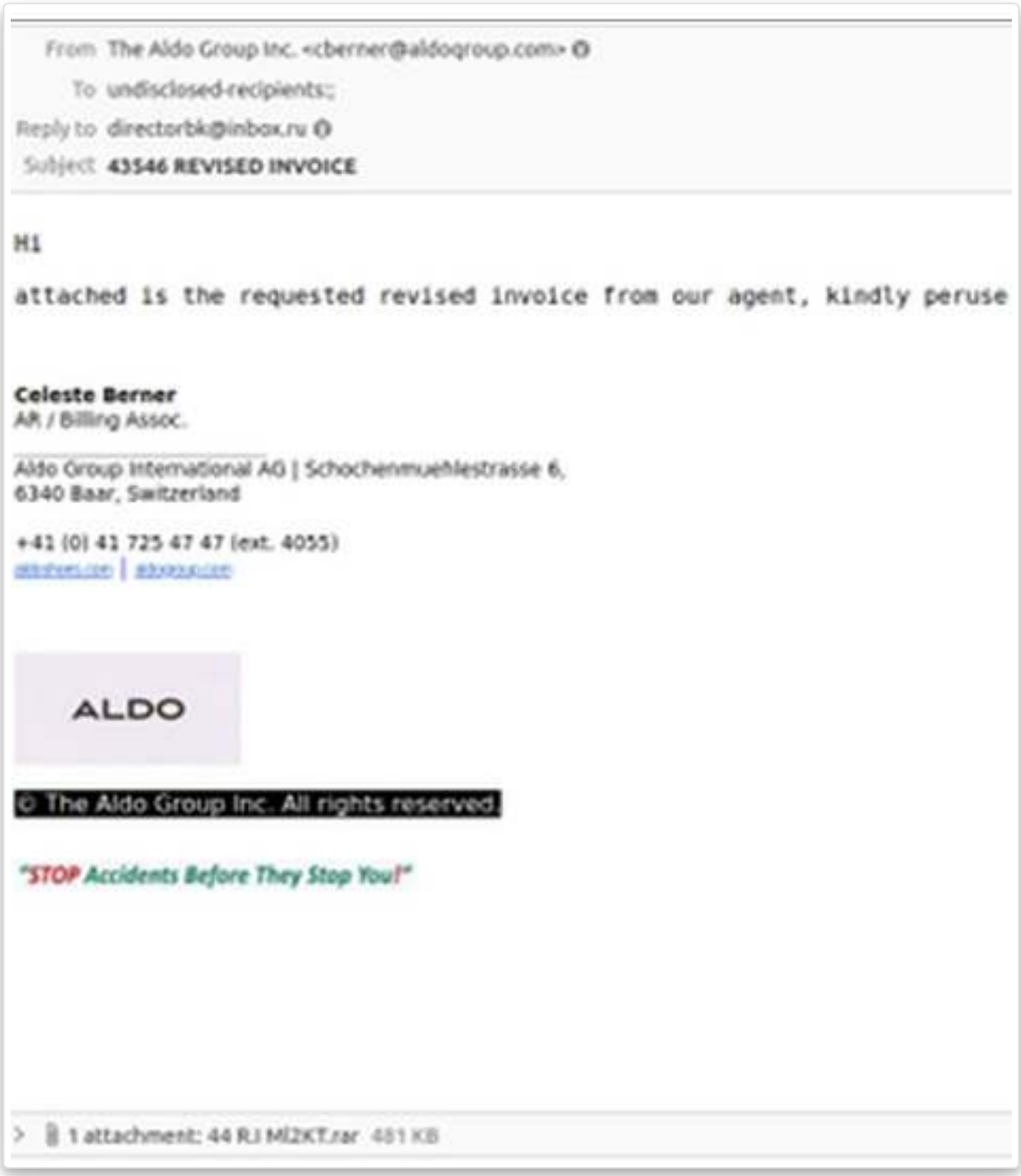



*Figure 3-30 : Courrier électronique malveillant envoyé par POSEIDON-IS_001. Source : OWN-CERT.*


*Figure 3-31 : Courrier électronique malveillant envoyé par POSEIDON-IS_001. Source : OWN-CERT.*

Il est très probable que POSEIDON-IS_001 utilise également ces données volées pour s'introduire dans le réseau des entreprises cibles dans le cadre d'attaques BEC. Le OWN-CERT a en effet relevé des similitudes dans les modes opératoires avec le groupe menaces SilverTerrier :

- l'utilisation de Lokibot avec des courriels provenant de domaines typosquattés
- une victimologie similaire (entreprises des secteurs « Technology » et « Manufacturing »)
- l'identification d'un numéro de téléphone nigérian enregistré parPOSEIDON-IS_001et directement lié à son adresse de courrier électronique

Le mode opératoire adverse POSEIDON-IS_001 est resté très actif sur l'année 2022, comme en témoigne son rythme d'enregistrement de nouveaux noms de domaines (Figure 3-32).

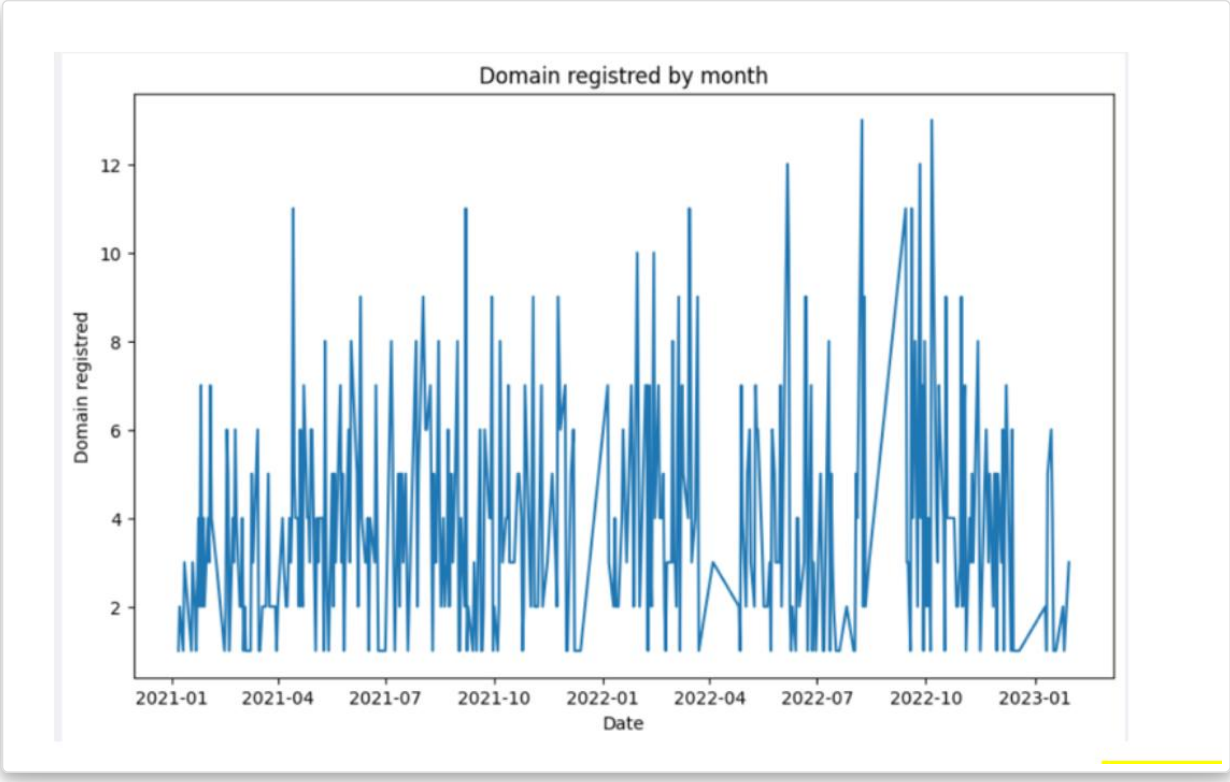



*Figure 3-32 : Domaines enregistrés par POSEIDON-IS_001 sur les derniers mois. Source : OWN-CERT.*

| Recommandations |
| --- |
| - Sensibiliser tous les employés à détecter les tentatives de phishing.<br>- Sensibiliser et former les employés responsables des paiements à détecter les fraudes aux faux ordres de virement.<br>- Créer des procédures de vérification des changements de comptes bancaires en interne et avec les partenaires (contrôles, détection d'irrégularité et lutte contre la fraude).<br>- Mettre en quarantaine tous les fichiers exécutables envoyés par courriels (même sans l'extension .exe ou contenus dans des archives).<br>- Mettre en place une authentification multiple (MFA) sur les comptes. Les clés physiques ou FIDO2 permettent une résilience au phishing.<br>- S'appuyer sur des individus désignés et utilisant du MFA pour les transferts d'argent.<br>- Vérifier l'authenticité des informations comprises dans les correspondances.<br>- Surveiller les accès aux comptes de courrier électronique et vérifier les règles concernant les courriers électroniques non autorisés et les paramètres de transfert.<br>- Avoir une haute vigilance lors de la réception de courriers électroniques ou de liens n'appartenant pas à l'organisation. |

## 3.5. Les rançongiciels

Avec 56 attaques recensées à l'encontre du secteur en 2022, contre 51 en 2021, la pression exercée par les sources de menaces exploitant les rançongiciels (*ransomware*) s'est accentuée. Aucun groupe de rançongiciel n'est, à ce jour, spécialisé dans l'attaque d'entreprises du secteur maritime. Dans la grande majorité des cas, les attaques sont réalisées de manière opportuniste. La lutte contre ces groupes s'est également intensifiée, avec plusieurs arrestations et démantèlements.

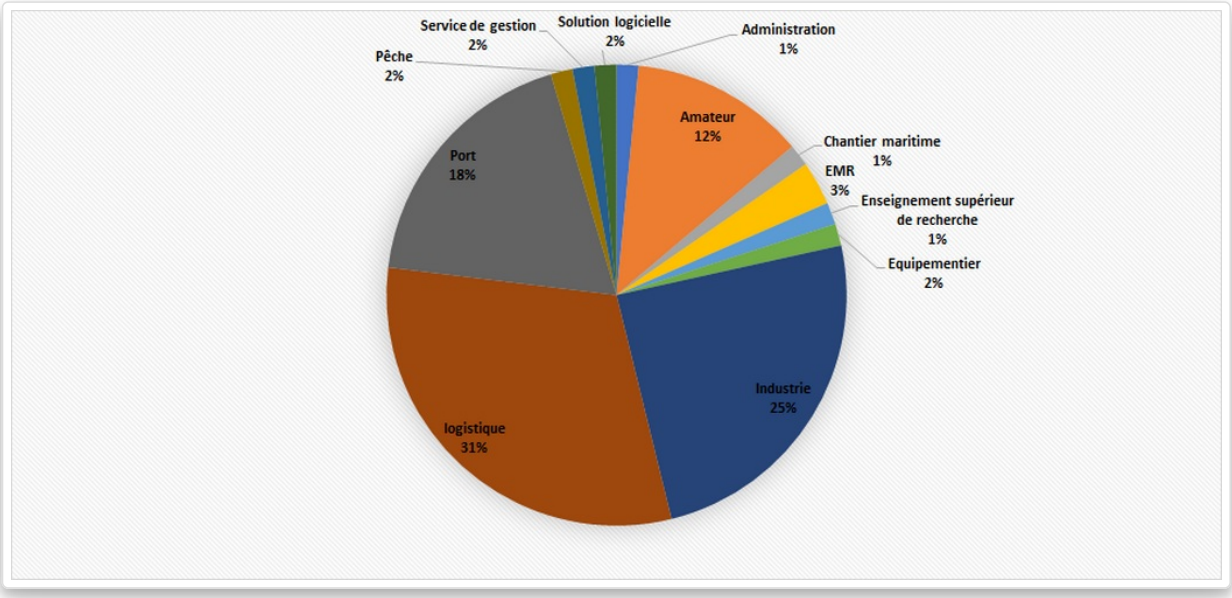



*Figure 3-33 : Nombre d'attaques de rançongiciels par secteur d'activité lié au maritime en 2022. Source : OWN-CERT.*


*Figure 3-34 : Répartition géographique des attaques de rançongiciels en 2022. Source : OWN-CERT.*

Durant l'année 2022, les groupes rançongiciels ayant le plus visé le secteur maritime sont Lockbit, Conti et Play. Sans surprise, il s'agit des principaux rançongiciels ayant sévi durant cette même année sur les autres secteurs (Figures 3-31, 3-32).

Parmi les techniques privilégiées par les opérateurs de rançongiciel, on retrouve :

| 1 | 2 | 3 |
|---|---|---|
| **L'infection préalable par un code malveillant**<br>Emotet, Dridex, Trickbot, BazarLoader, Qbot, IcedID, SquirrelWaffle… | **La compromission d'actifs exposés à Internet (RDP, VPN, passerelles…) par l'exploitation de vulnérabilités**<br>Les vulnérabilités PulseSecure (CVE 2019-11510) et Citrix (CVE-2019-19781) sont connues pour être fréquemment utilisées par les groupes de rançongiciel.<br>ProxyShell (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207), PrintNighmare (CVE-2021-34527) ainsi que la vulnérabilité Log4Shell (CVE-2021-44228) sont des vulnérabilités régulièrement utilisées par les opérateurs de rançongiciels LockFile, Magniber et Vice Society. | **L'achat d'identifiants et d'accès à des tiers sur les epsaces d'échanges cybercriminels.** |

L'objectif final de l'utilisation du rançongiciel évolue également. En janvier 2022, les « Partisans Cyber biélorusses », un groupe d'hacktivistes, ont lancé une attaque par rançongiciel sur les infrastructures ferroviaires de la Biélorussie[21]. Au lieu de demander une rançon pour récupérer les données des serveurs chiffrés, le groupe a fourni une série de conditions politiques en échange des clés de déchiffrement : retrait des troupes russes présentes sur le territoire, libération de prisonniers politiques (Figure 3-38). Lancer une attaque par rançongiciel ne répond pas ici à un intérêt financier, mais à une volonté de faire passer un message politique.

Le seul impact visible de cette attaque aurait été l'impossibilité pour les employés d'accéder aux bases de données de l'entreprise de transport, et pour les clients, d'utiliser le système de réservation en ligne. Néanmoins, le réseau ferroviaire étant un élément stratégique de soutien logistique militaire, l'attaque aurait également pu affecter un exercice militaire conjoint russo-biélorusse et représente ainsi une cible symbolique.

L'attaque des infrastructures de transport n'est ici pas une finalité en soi, mais un moyen de s'imposer dans les rapports de force en touchant à un secteur stratégique. C'est la première fois qu'un

groupe d'hacktivistes utilisait le vecteur du rançongiciel comme moyen de contestation. L'année 2022 a démontré, en lien avec la guerre en Ukraine, que le secteur maritime pouvait être touché par ce genre d'hacktivisme.


*Figure 3-35 : Revendication de l'attaque. Source : Twitter.*

| | Scénario prospectif : quel impact pour un rançongiciel dans l'écosystème maritime ? |
|---|---|
| Août 2022 | En utilisant un outil permettant de recenser les sites Internet vulnérables, un attaquant a repéré un système de gestion de contenu (*Content Management System, CMS*) vulnérable chez un armateur.<br>Le CMS, mis en place il y a quelques années par un prestataire, n'a pas été mis à jour depuis 2018. De nombreuses vulnérabilités ont pourtant été publiées, mais la contractualisation avec un nouveau prestataire tarde, ralentie par le COVID, la surcharge de travail de certains acteurs-clés et le manque d'intérêt (le site Internet fonctionnant correctement). |
| Étape 1 – Découverte et compromission initiale | En exploitant une vulnérabilité touchant ce CMS, l'attaquant parvient à obtenir la liste et les adresses de courriels de 37 collaborateurs ayant accès au CMS, également utilisé pour permettre la diffusion de documents vers le personnel et les partenaires de l'armateur (intranet et extranet). L'attaquant ne parvient cependant pas à récupérer les mots de passe associés aux comptes. Cette attaque passe inaperçue, personne – ni aucune technologie - n'assurant la surveillance de l'outil. |

| Scénario prospectif : quel impact pour un rançongiciel dans l'écosystème maritime ? | |
|---|---|
| Étape 2 - *Phishing* | L'attaquant mène ensuite une opération de *phishing* à l'encontre de l'organisation, en visant les comptes qu'il a récupérés. Cette attaque invite les utilisateurs à se connecter sur Office365 pour consulter un document récemment transmis à l'armateur pour une relecture indiquée comme urgente.<br>La connexion au cloud nécessite que l'utilisateur s'identifie et s'authentifie, ce que font 2 des 37 collaborateurs. Pour les autres, le courriel apparaît suspect et ils ne cliquent pas sur le lien. Cependant, par manque de communication interne, aucune alerte générale n'est transmise et les deux personnes ayant diffusé leurs identifiants/mots de passe pensent à un problème temporaire et passent à autre chose. |
| Étape 3 - Revente | L'attaquant vend ensuite les deux identifiants / mots de passe récupérés sur la plate-forme d'un Initial Access Broker. 48 heures plus tard, les comptes sont achetés par un opérateur de rançongiciel. |
| Étape 4 - Compromission | En utilisant les comptes obtenus, dont l'un est un compte à privilège, l'opérateur de rançongiciel accède à la messagerie interne de l'entreprise. Il usurpe une adresse interne pour émettre un courriel avec une pièce jointe contenant un logiciel malveillant. Ce logiciel a deux fonctions : d'une part, permettre l'exfiltration de données sensibles de l'entreprise (les comptes et mots de passe, l'architecture logique du réseau) et, d'autre part, assurer à l'attaquant un accès complet au système d'information de l'armateur. |
| Étape 5 - Installation | Plusieurs salariés de l'armateur ouvrent cette pièce jointe : l'attaquant mène alors les deux dernières phases de l'attaque : il commence par exfiltrer l'ensemble des données présentes sur les postes clients qui ont été infectés et sur les lecteurs réseaux auxquels ils ont accès. Puis, en utilisant le compte à privilège qu'il possède et en exploitant une vulnérabilité présente sur le serveur *Active Directory* de l'armateur, il parvient à exfiltrer de nouvelles données et, enfin, active le chiffrement de l'ensemble du parc informatique de l'armateur. |
| Impacts sur le SI interne | Progressivement, l'ensemble des 120 postes de l'armateur est injoignable : le serveur *Active Directory* est chiffré, de même que le serveur de sauvegarde qui n'assure pas de sauvegarde hors ligne, privant l'organisation de toute capacité de communication interne, d'accès à ses fichiers et de messagerie.<br>Le réseau téléphonique, qui avait récemment été migré à la demande d'un prestataire pour être raccordé à l'*Active Directory* est également hors service. |

| | Scénario prospectif : quel impact pour un rançongiciel dans l'écosystème maritime ? |
|---|---|
| Impacts sur l'écosystème | Cette organisation assurant les fonctions d'armateur côtier, le système de gestion de la sécurité, les fichiers et la communication électronique avec les navires sont perdus. Depuis deux ans, un poste client du réseau de l'entreprise avait été installé à bord de chaque navire, avec une connexion 4G/5G vers le réseau de l'armateur.<br>Fort heureusement, ce poste est isolé des autres postes et des systèmes d'information métier du navire. Les conséquences opérationnelles sont donc minimes pour les navires. |
| Impacts sur le SI interne | Pour l'armateur, les conséquences sont importantes : la reconstruction de son système d'information va prendre trois semaines. L'ensemble du travail mené au cours des trois derniers mois est perdu définitivement. Heureusement, un archivage hors ligne réalisé quelques mois auparavant pour libérer de la place sur les serveurs permettra de récupérer des données essentielles. L'ensemble des postes et des serveurs devra être réinstallé et sécurisé. |
| Bilan | Le directeur mandate, tardivement, une équipe d'investigation pour analyser l'évènement : cette équipe lui recommande de déposer plainte, ce qui est fait une fois les postes réinstallés, limitant les capacités d'investigation des enquêteurs. Cependant, leur analyse permettra d'identifier le CMS comme vecteur initial d'intrusion, alors que cela n'avait pas été du tout identifié en interne. Le CMS est placé en mode « maintenance » pendant plusieurs jours, le temps de trouver un prestataire en urgence pour le mettre à jour. |
| Impact financier | Pour l'armateur, le coup est rude : il identifie également que son assurance ne prend pas en charge ce type de sinistre. Le coût total de l'attaque, de l'investigation, de la reconstruction, de la perte de données et du renforcement en urgence des systèmes d'information sera chiffré plus tard à plus de 180 000 €, un coût particulièrement important pour ce petit armateur qui connaissait déjà quelques difficultés financières.<br>Si d'autres armateurs comme lui ont été victimes de ce type d'attaque dans le monde, la perte de certains clients craignant pour la sécurité de leurs données nécessitera de sa part un travail à long terme pour regagner leur confiance. |

## 4. Les attaques ciblées contre le secteur maritime

De longue date, des acteurs étatiques ont montré un intérêt marqué pour le secteur maritime et portuaire en raison de son caractère hautement stratégique. Les objectifs sont triples :

- Se prépositionner, afin de pouvoir mener des actions de sabotage contre des systèmes d'information critiques, à terre ou à bord.
- Mener des campagnes d'espionnage, afin de récupérer une avance stratégique ou économique, notamment sur des chantiers navals ou des entreprises du naval de défense.
- Être actif dans l'espace informationnel en y menant des campagnes de désinformation ou d'influence.

Si certaines de ces actions sont souvent difficiles à détecter, ou le sont a posteriori, parfois avec plusieurs mois ou années de retard, d'autres peuvent être détectées de manière plus rapide, mais restent confidentielles. Enfin, d'autres actions sont menées plus ouvertement, notamment lorsqu'il s'agit de lutte informatique d'influence.

De nombreuses craintes avaient été formulées en début d'année 2022 sur le déclenchement d'un conflit cyber en parallèle de l'action offensive russe sur l'Ukraine. Malgré l'existence effective de certaines actions devant être soulignées, la menace pour les systèmes d'information occidentaux ne s'est, dans bien des cas, et de l'avis de nombreux acteurs, pas ou peu concrétisée.

En revanche, une bipolarisation de plusieurs groupes de cybercriminels s'est confirmée, entraînant des tensions au sein de certaines franchises (Conti). Enfin, cette bipolarisation a également déclenché un regain d'attaques qui avaient tendance à se faire plus discrètes au cours des dernières années, comme les attaques en déni de service distribué (Distributed Denial of Service, DDoS). En se coordonnant via les réseaux sociaux (liste de cibles à viser, mise à disposition d'outil, communication de procédures, revendication et, parfois, paiement), ces groupes contribuent à la lutte d'influence des états qu'ils soutiennent.

| Définition |
| --- |
| APT, pour *Advanced Persistent Threat*, désigne une typologie d'attaque mise en œuvre par des acteurs disposant de moyens importants et souhaitant se prépositionner de manière stratégique, discrète et sur une période longue afin d'atteindre leurs objectifs (espionnage, sabotage…). L'exécution d'une APT nécessite souvent plus de ressources qu'une attaque cybercriminelle opportuniste. Les auteurs sont généralement des équipes expérimentées disposant d'un soutien financier substantiel, comme des financements étatiques, afin de répondre notamment à certains enjeux nationaux.<br>Face à ce type d'attaques, il est souvent difficile de disposer d'une vision complète de la menace. Cependant, celles ayant été rendues publiques permettent d'analyser les techniques utilisées par ces acteurs. Certains éléments en sources ouvertes, ainsi que l'exploitation de sources propres au OWN-CERT, ont permis d'identifier les tendances pour le domaine maritime durant l'année 2022. |

## 4.1. Les clés USB, un vecteur d'infection initiale toujours d'actualité pour le secteur

Les supports USB restent des vecteurs potentiels de propagation de codes malveillants au sein du secteur maritime. En effet, de nombreux systèmes d'information de navires ou de ports, notamment des systèmes de contrôle industriels, de vidéosurveillance ou de sûreté restent déconnectés d'Internet et des infrastructures IT « classiques ». Pour autant, les opérations de maintenance préventive ou corrective dont ils font l'objet (mise à jour de programmes, de micrologiciels, etc) ont recours aux supports USB. Ces supports USB ne sont cependant que trop rarement propriété de l'armateur ou des navires, et peuvent être apportés par des opérateurs de maintenance qui les exploitent au profit de plusieurs armateurs, sans décontamination préalable : le risque d'infection « par rebond » d'un ou plusieurs systèmes d'information est donc un scénario vraisemblable.

Parmi les codes malveillants dont la propagation est réalisée par ce type de méthode, on retrouve le code malveillant PlugX. PlugX est principalement utilisé par des groupes étatiques réputés chinois. L'utilisation des clés USB a été identifiée comme étant un des vecteurs d'infection de ces attaquants. En effet, lorsque PlugX compromet une machine, le code malveillant infecte également les appareils USB qui y sont connectés ou qui se connectent par la suite. La technique utilisée permet à PlugX d'être presque indétectable sur ce type de support (Figure 4-1)[22].

Le OWN-CERT a ainsi eu connaissance de l'infection d'au moins sept navires par le code malveillant PlugX durant l'année 2022. Du fait de l'utilisation accrue des clés USB pour les installations et mises à jour de logiciels au sein du secteur, et en particulier les navires, ce vecteur constitue donc un moyen d'infection initiale qui pourrait être privilégié par les acteurs étatiques pour viser le secteur maritime.

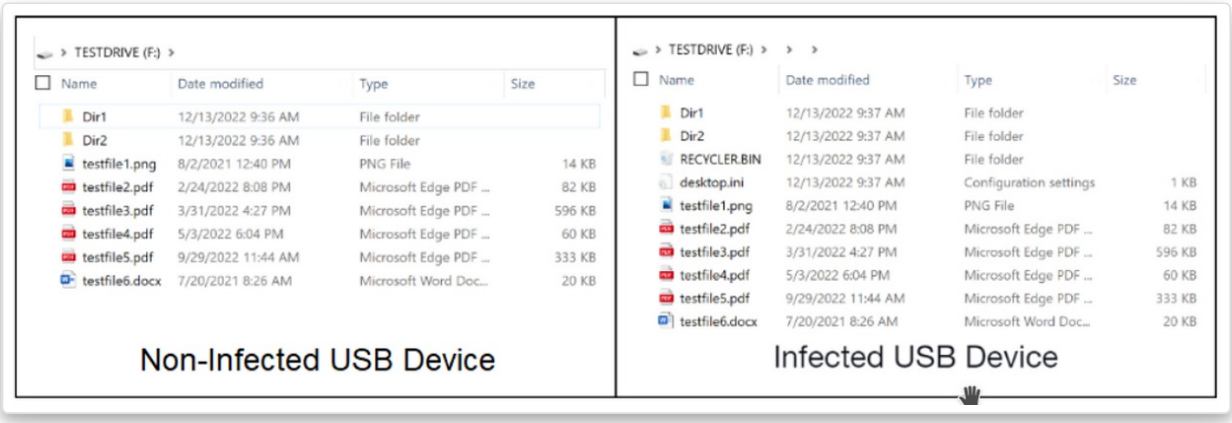



*Figure 4-1 : Comparaison des répertoires racines d'un périphérique USB non infecté et d'un périphérique USB infecté. Source : Unit42.*

## 4.2. L'écosystème maritime usurpé à des fins d'ingénierie sociale

A l'image des campagnes de *Business Email Compromise* qui usurpent, via des courriels frauduleux, des pratiques officielles utilisées par les administrations sur des navires, les attaquants utilisent

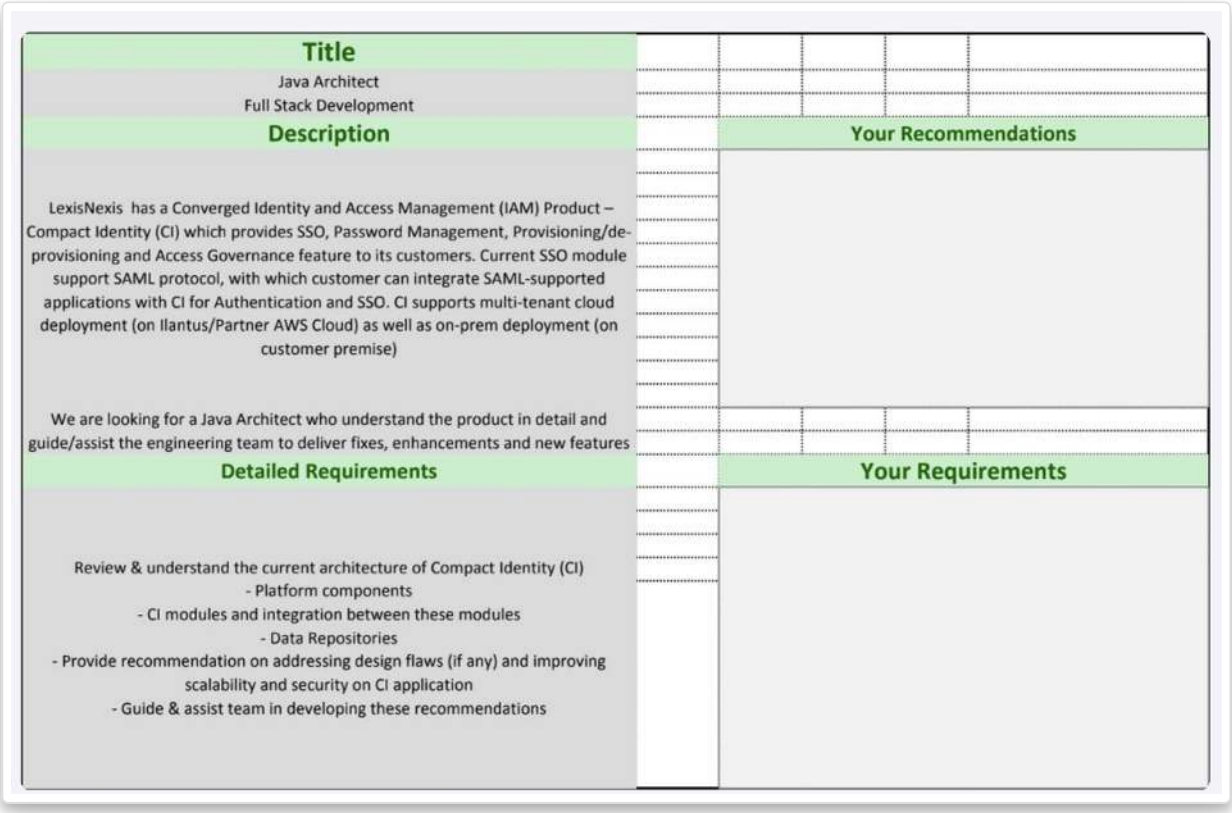
également ces pratiques, mais vont souvent plus loin dans la compréhension de l'écosystème de leurs victimes.

L'ingénierie sociale via des courriels de harponnage (*spearphishing*) reste le premier vecteur d'intrusion de ces attaquants, notamment pour les campagnes d'espionnage. Durant l'année 2022, plusieurs campagnes de *phishing* visant de près ou de loin le secteur maritime ont ainsi été identifiées.

Selon une analyse de Proofpoint[23], TA423[24], groupe actif depuis dix ans et considéré comme proche du gouvernement chinois, serait à l'origine de campagnes de *phishing* distribuant un lien qui redirige les victimes vers un site malveillant se faisant passer pour un média australien (Figure 4-2) et délivrant le code malveillant ScanBox. Les cibles sont essentiellement des pays ou des entités opérant en Mer de Chine méridionale, dont des opérateurs d'éoliennes ainsi qu'un fabricant européen fournissant des équipements pour le parc éolien *offshore* Yunlin dans le détroit de Taïwan. Les courriels frauduleux usurpent des sujets tels que « *Sick Leave* », « *User Research* » ou encore « *Request Cooperation* ».


*Figure 4-2 : Capture d'écran issue de l'article de Fortinet comparant l'article d'australianmorningnews[. ]com, qui se présente comme « le plus grand site d'information d'Australie », avec un article similaire de la BBC. Source : Fortinet.*

Selon Mandiant[25], le cluster UNC3890 réputé lié à l'Iran aurait visé des entités israéliennes, dont des compagnies de transport maritime, par le biais de fausses offres d'emplois, dans le cadre d'une campagne de phishing ou de point d'eau (watering hole), avec un fichier .xls leurre, conçu comme une fausse offre d'emploi (Figure 4-3). L'ouverture de ce fichier aurait ensuite permis l'installation du code malveillant SUGARDUMP, un outil de collecte d'informations d'identification.



| Title | |
|---|---|
| Java Architect<br>Full Stack Development | |
| **Description** | **Your Recommendations** |
| LexisNexis has a Converged Identity and Access Management (IAM) Product – Compact Identity (CI) which provides SSO, Password Management, Provisioning/de-provisioning and Access Governance feature to its customers. Current SSO module support SAML protocol, with which customer can integrate SAML-supported applications with CI for Authentication and SSO. CI supports multi-tenant cloud deployment (on Ilantus/Partner AWS Cloud) as well as on-prem deployment (on customer premise)<br><br>We are looking for a Java Architect who understand the product in detail and guide/assist the engineering team to deliver fixes, enhancements and new features | |
| **Detailed Requirements** | **Your Requirements** |
| Review & understand the current architecture of Compact Identity (CI)<br>- Platform components<br>- CI modules and integration between these modules<br>- Data Repositories<br>- Provide recommendation on addressing design flaws (if any) and improving scalability and security on CI application<br>- Guide & assist team in developing these recommendations | |

*Figure 4-3 : Fausse offre d'emploi de LexisNexis délivrant le code malveillant Sugardump. Source : Mandiant.*

Les équipes de Symantec[26] ont également identifié l'acteur Hydrochasma comme à l'origine d'attaques de *phishing* à l'encontre de compagnies maritimes et de laboratoires médicaux en Asie. Le groupe utilise l'envoi d'un document avec un nom de fichier adapté à la langue maternelle de l'organisation visée comme « *Product Specification-Freight-Company Qualification Information wps-pdf Export.pdf.exe* ». Certains éléments techniques permettent d'émettre une hypothèse sur l'origine d'Hydrochasma : Les domaines utilisés par Hydrochasma utilisent le TLD « .cn », relatif à la Chine. Ces domaines sont hébergés sur des adresses Internet (IP) localisées en Chine. De plus, ces domaines sont relatifs à des entreprises chinoises. L'ensemble de ces éléments pourrait indiquer un ciblage de la Chine, rappelant la campagne attribuée à APT32 — un groupe étatique réputé rattaché au Vietnam — au début de l'année 2020[27]. De plus, la plupart des indicateurs partagés par Symantec[28] sont des logiciels libres utilisés lors de tests d'intrusion, ou des outils génériques d'intrusion, comme Cobalt Strike. Aucun de ces outils n'est attribuable à un acteur spécifique, ce qui suggère que Hydrochasma souhaite rester discret.

Certains évènements organisés par le milieu maritime ont également été utilisés pour cibler des victimes. C'est le cas de la *Pakistan International Maritime Expo & Conference (PIMEC-2023)*, dont l'objectif est de développer l'écosystème maritime du pays. Les équipes de BlackBerry ont découvert une campagne de *phishing* attribué à un acteur nommé « NewsPenguin »[29]. L'attaquant a eu recours

à un document de hameçonnage diffusé numériquement sous la forme d'un « manuel de l'exposant », en ciblant les visiteurs de l'événement (Figure 4-4). La charge utile est un outil d'espionnage avancé chiffré, avec une clé de chiffrement « penguin ».

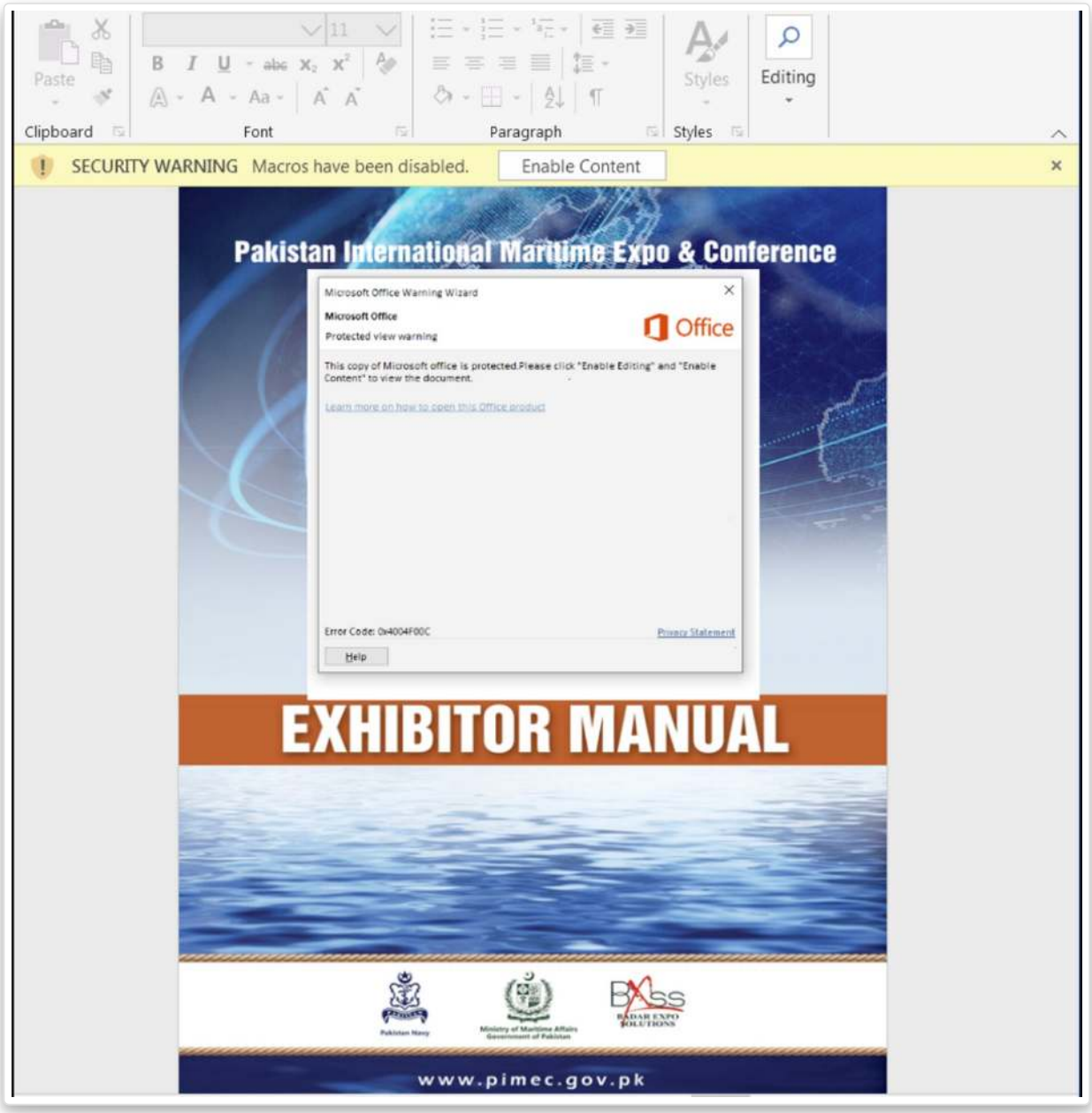



*Figure 4-4 : Document malveillant utilisé pour cibler les exposants de la PIMEC-23. Source : Blackberry.*

## 4.3. Les menaces visant les systèmes « *Supervisory Control And Data Acquisition* » et « *Industrial Control System* » (ICS)

Les ports et les navires dépendent de systèmes complexes, associant systèmes d'information

classiques (*Information Technology*, IT) avec des systèmes industriels, cyber-physiques ou métiers, que l'on regroupe souvent sous le terme d'OT (*Operational Technology*). Si historiquement, les systèmes informatiques associés à la bureautique demeurent les principales cibles, les systèmes de contrôle industriel (*Industrial Control Systems*, ICS) sont progressivement devenus des cibles stratégiques. Ces systèmes sont basés sur le numérique pour gérer des opérations industrielles. Dans un navire par exemple, il s'agira de la propulsion, de la navigation, de l'alimentation électrique…

D'après un rapport de Dragos[30], les vulnérabilités impactant les systèmes industriels ont augmenté de 27 % en 2022. Le fait que les attaques sur les systèmes industriels soient complexes et nécessitent des ressources importantes, explique qu'elles soient habituellement attribuées à des attaquants liés à des États. Toutefois, ce même rapport indique que les attaques par rançongiciel visant des entreprises relevant du domaine industriel ont augmenté de 87 %, notamment à cause du conflit Russo/Ukrainien et de l'écosystème de « *Ransomware as a Service* ».

Si la menace est bien réelle, il est difficile d'avoir une vision globale des attaques ayant eu lieu et une connaissance précise des attaquants. De par leur technicité, ces attaques ne sont réalisées que par des groupes spécialisés. C'est le cas d'un groupe apparu récemment, Bentonite, qui a visé le domaine du pétrole et du gaz maritime. D'après Dragos, ce groupe mènerait ce type d'attaque à des fins d'espionnage et de perturbation, en exploitant principalement les accès à distance ou les ressources exposées sur Internet.

Durant l'année 2022, un rapport de Forescout[31] a fait état de 56 vulnérabilités critiques regroupées sous le nom de « IceFall », et concernant plus de neuf fournisseurs de systèmes OT (Honeywell, Motorola, Omron, Siemens, Emerson, JTEKT, Bentley Nevada, Phoenix Contact, Code). Les vulnérabilités identifiées pourraient entraîner la compromission d'identifiants, la manipulation de micrologiciel (*firmware*), l'exécution de code arbitraire à distance ou encore le contournement de mécanismes d'authentification.

Des attaquants proches du gouvernement chinois auraient également exploité une vulnérabilité dans Microsoft Exchange (CVE-2021-26855) à l'encontre de systèmes industriels d'entreprises localisées au Pakistan, en Afghanistan et en Malaisie, dont une entreprise de transport maritime[32]. Cette exploitation aurait notamment permis l'installation de la porte dérobée « ShadowPad » (Figure 4-5). Connue depuis quelques années, cette porte dérobée, qui vise particulièrement le domaine de la logistique, permet aux attaquants de télécharger d'autres modules malveillants ou encore de voler des données.

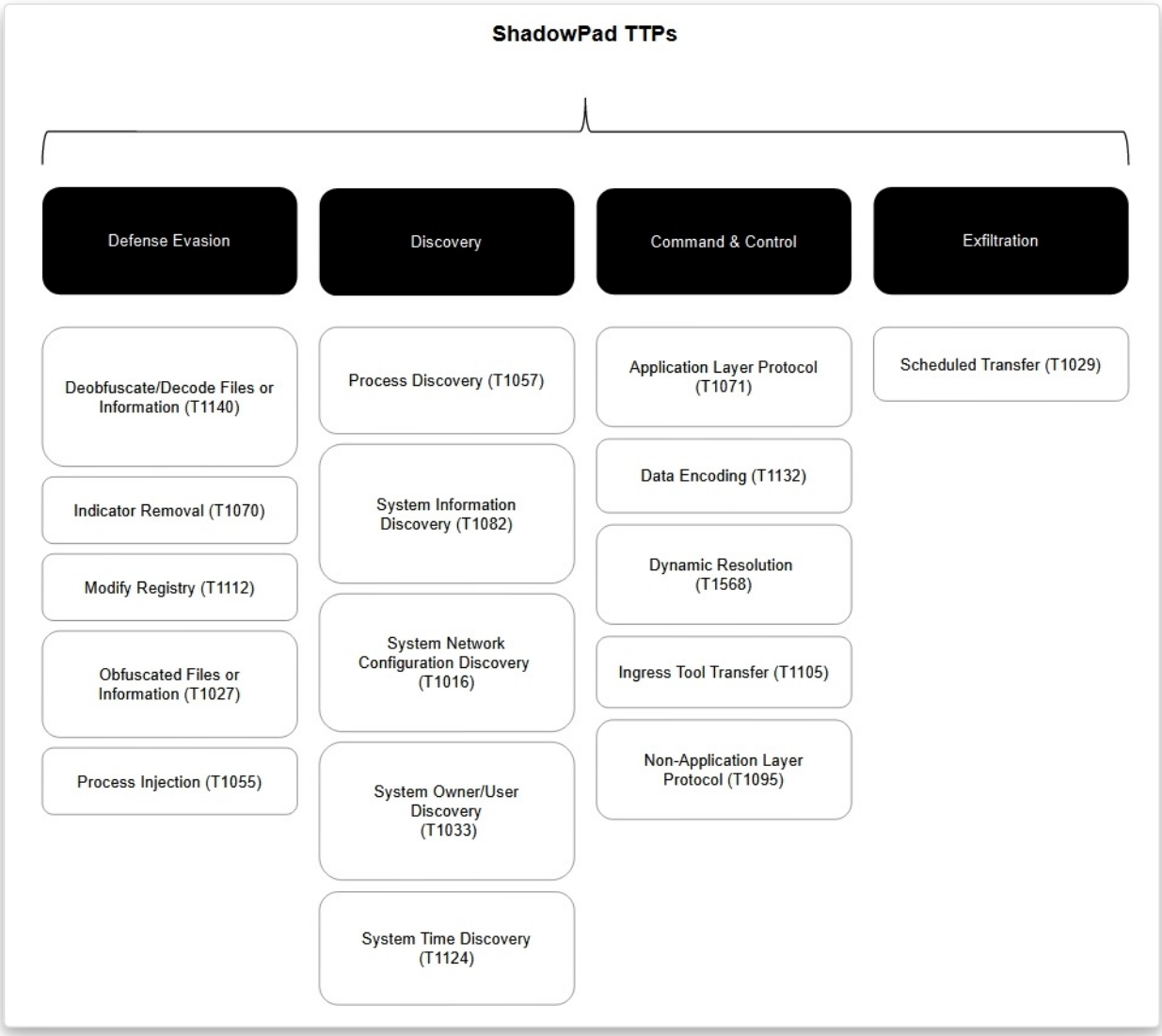



*Figure 4-5 : Tactiques, Techniques et Procédurees de ShadowPad. Source : MITRE ATT&CK.*

Un autre code malveillant a été conçu pour viser spécifiquement les systèmes industriels. Il s'agit du code malveillant *« Incontroller »* (Pipedream)[33]. Ce code malveillant, apparu en 2022 dans le cadre de la guerre en Ukraine, a été spécialement développé pour interagir avec des équipements industriels intégrés dans différentes machines qui sont utilisés dans plusieurs secteurs. Cet outil permet ainsi aux attaquants d'obtenir un accès système complet à plusieurs dispositifs ICS et de contrôle de supervision et d'acquisition de données (*Supervisory Control And Data Acquisition, SCADA*), une fois un accès initial au réseau industriel établi (Figure 4-6). La société Dragos estime que les cibles les plus probables de ce code malveillant sont les équipements de Gaz Naturel Liquéfié (GNL) et les réseaux électriques.

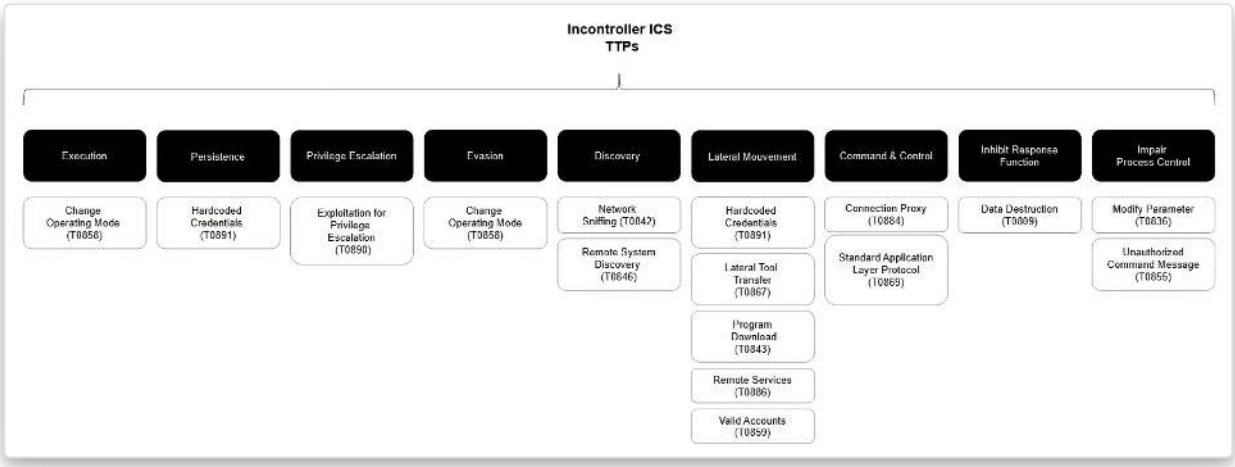



*Figure 4-6 : Tactiques, Techniques et Procédures d'Incontroller. Source : MITRE ATT&CK ICS.*

Ces quelques exemples démontrent la capacité des attaquants à se spécialiser sur l'écosystème OT et à développer des codes malveillants de plus en plus sophistiqués qui s'adaptent à leur environnement.

## 4.4. Les câbles sous-marins

Infrastructures essentielles aux télécommunications électroniques mondiales, les câbles sous-marins ont été à de nombreuses reprises évoqués comme étant des cibles potentielles dans le cadre du conflit entre la Russie et l'Ukraine, ou encore lors des tensions entre Chine et États-Unis[34].

Ces craintes font suite, d'une part, au sabotage des gazoducs Nordstream 1 et 2 fin septembre 2022 et, d'autre part, à l'intérêt supposé de nombreux navires militaires ou de « recherche » vis-à-vis des trajets de câbles sous-marins intercontinentaux, régionaux, voire locaux.

En 2022, en-dehors d'incidents de croche (parfois présumés comme attaques physiques lorsque des bâtiments militaires évoluaient à proximité), une cyberattaque sur une infrastructure de câble sous-marin a été publiquement reconnue[35].

## 4.5. Les télécommunications par satellite

Dans un contexte où les données sont centrales et indispensables au secteur pour assurer ses fonctions opérationnelles, un intérêt marqué continue à être porté sur les équipements et infrastructures de télécommunication par satellite. Cet intérêt s'explique par deux raisons essentielles :

- D'une part, il est fréquent que des vulnérabilités soient identifiées sur les différents segments de ces installations, tels que les modems et installations embarquées, mais aussi sur les équipements de télécommunications et les infrastructures à terre, employées notamment au profit du secteur maritime. Ces vulnérabilités s'expliquent généralement par un défaut

d'intégration de la cybersécurité par conception en l'absence, soit de demande contractuelle, soit de mise en œuvre de bonnes pratiques, soit d'évaluation et, enfin, par absence de configuration sécurisée et de maintien en conditions de sécurité permettant d'assurer un bon niveau de cybersécurité dans le temps.

- D'autre part, si certains armateurs et compagnies offshore ont bien pris en compte les enjeux de chiffrement sur ces liaisons, il est encore trop fréquent que ces liaisons ne fassent pas l'objet d'un chiffrement. Leur interception demeure donc, dans de nombreux cas, une possibilité pour des attaquants avec des moyens relativement peu sophistiqués.

Le fait que, dans une grande majorité des cas, les mots de passe par défaut de ces équipements ne soient pas modifiés pour en faciliter la maintenance à distance ultérieure, notamment par des tiers maintenanciers, présente également un risque majeur de compromission.

Dans un contexte de forte numérisation des navires et de migration progressive vers des technologies connectées dites « smart shipping » et « green shipping », les connexions à distance entre la terre et les navires vont être amenées à se multiplier, de même que les solutions de type « passerelle connectée », afin notamment de faciliter la mise à jour des cartes de navigation.

Enfin, il est à noter plusieurs évènements ayant impacté ce secteur au cours des derniers mois, notamment :

- L'attaque sur le segment sol de KA-SAT au début du conflit russo-ukrainien. Cette attaque destructrice, qui a fait l'objet de plusieurs analyses détaillées, dont une de SEKOIA[36] a pu impacter une faible partie du secteur maritime utilisant ce type d'équipement, essentiellement dans le secteur de la pêche. En revanche, le secteur des EMR a été fortement impacté[37].
- La compromission de certains équipementiers du secteur a pu également engendrer des fuites d'information sensibles sur des installations de télécommunication par satellite.

## 4.6. Leurrage et brouillage GNSS (Géolocalisation et Navigation par Système de Satellites)

Les systèmes de Positionnement, de Navigation et de Temps (PNT) comme le GNSS sont importants pour le secteur maritime et portuaire. L'interdiction d'accès aux informations obtenues ou calculées à partir d'une de ces sources peut entraîner des conséquences non négligeables et devant être anticipées :

- Dans le cas d'un brouillage, la perte de références géographiques a un impact immédiat en passerelle, où la perte du GPS par brouillage génère normalement des alarmes. Il est indispensable que le personnel soit entraîné à réagir efficacement dans ce cas et que des procédures de réaction efficaces soient formalisées. La perte du GNSS a un impact immédiat, par propagation, sur d'autres systèmes : Voyage Data Recorder (VDR), Automatic Identification System (AIS), ainsi que sur les systèmes de télécommunication par satellite, qui utilisent les

informations issues du GPS pour positionner correctement leurs antennes paraboliques.
- Dans le cas d'un leurrage, cibler un navire en particulier pour le faire dévier de sa trajectoire est une attaque compliquée à réaliser, qui nécessite souvent d'être à proximité voire sur le navire. Les cas plus fréquemment étudiés montrent des leurrages de zone, où une multitude de navires se retrouvent décalés de leur position de plusieurs centaines de mètres, voire de kilomètres.

Dans les deux cas, la perte potentielle de la référence horaire peut causer des troubles à certains systèmes d'information qui utilisent les systèmes GNSS comme référence horaire, soit directement, soit pour alimenter un service NTP à bord. Les impacts peuvent alors différer suivant la configuration des équipements concernés.

Souvent oubliés, les ports ont également parfois recours aux systèmes de positionnement par satellite, pour le positionnement de leurs grues, notamment, ainsi que, dans certains cas, pour la synchronisation horaire.

| Recommandations |
| --- |
| Les solutions de contournement existent, en fonction du type de navire ou de sa zone de navigation, par exemple : utilisation d'antennes protégées contre le brouillage (*Controlled Reception Pattern Antennas, CRPA*), utilisation de récepteur bi ou tri-constellations, détection d'anomalies, utilisation de moyens tiers de positionnement : centrale inertielle, autres systèmes satellitaires.<br>France Cyber Maritime a organisé fin 2022 un webinaire spécifique sur ce sujet au profit de ses adhérents. |

De manière générale, certaines zones sont confrontées à un brouillage permanent d'origine étatique. D'autres zones plus éphémères peuvent être détectées, notamment en marge de déploiements militaires. Le contexte du conflit russo-ukrainien a entraîné l'apparition de nouvelles zones d'Anti Access/Area Denial (AA/AD) (Figure 4-7).

- Zone Mer de Barents, Mer Baltique et mer du Nord
  - Des perturbations permanentes et sensibles sont notées dans la zone proche de Mourmansk depuis au moins le mois d'août 2022.
  - En complément d'une petite zone déjà implantée au fond du Golfe de Finlande, une nouvelle zone de perturbations est apparue au large de l'enclave de Kaliningrad à la mi-décembre 2022, qui semble s'étendre jusqu'au à une centaine de nautiques au large de la Lituanie, de la Pologne et de la Lettonie.
- Zone Méditerranée
  - Une zone présente depuis plusieurs années au large de la Libye s'est atténuée au cours du second semestre 2022 et ne semble plus aujourd'hui représenter de menace permanente.
  - Une importante zone présente depuis plusieurs années entre Port Saïd, Chypre, le Sud-est de la Turquie, la Syrie, le Liban, et Israël demeure particulièrement active et perturbe, par moments, jusqu'au Sinaï et aux zones de mouillage à proximité de Port Saïd et d'entrée/sortie du Canal de Suez.
- Zone Mer Noire

- Une zone importante de brouillage GPS impacte la mer de Marmara, le détroit du Bosphore, et toute la zone sud-ouest de la mer Noire, jusqu'aux côtes Roumaines, de Burgas à Constanta, l'est de la mer Noire étant également fréquemment impacté, jusqu'à Sochi notamment. En l'absence de capteurs plus au nord, les opérations militaires qui se déroulent dans le nord de la zone rendent l'AA/AD sur les fréquences utilisées par les systèmes GNSS permanents[38].

- Zone Golfe Persique
  - Si aucune zone permanente et importante de brouillage GNSS n'est détectée, certains exercices ou opérations militaires peuvent entraîner des pertes ponctuelles de référence GNSS.
- Zone Asie
  - Présence ponctuelle de brouilleurs, probablement non étatiques, dans certaines grandes villes portuaires, pouvant entraîner des dénis d'accès lors d'escales de navires ;
  - Certains cas de brouillages ont également été recensés en marge d'exercices militaires.


*Figure 4-7 : Zones à risques de brouillage GNSS. Source : M-CERT.*

## 4.7. Leurrage et brouillage AIS (*Automatic Identification System*)

Si les cas de brouillage AIS sont peu documentés, en revanche un intérêt continu est porté sur le leurrage AIS. Celui-ci peut prendre essentiellement deux formes :

- Injection de fausses informations directement sur l'API de plateformes de fusion de l'information. Cette technique privilégiée permet facilement de compromettre une information. Si certaines falsifications sont faciles à détecter (Figure 4-8), ce n'est pas le cas pour toutes. Certains cas de leurrage au niveau des API des grandes plateformes de fusion d'information AIS peuvent également concerner des dizaines, voire des centaines de navires « fantômes ».
- Les cas de leurrage utilisant exclusivement le support radiofréquence existent aussi : ils ont souvent pour vocation première de masquer les intentions, ou le type du navire, voire sa position réelle, dans des cas d'opérations militaires, de contrebande, de pêche illégale, etc. Ils peuvent avoir lieu en pleine mer ou à proximité des côtes.

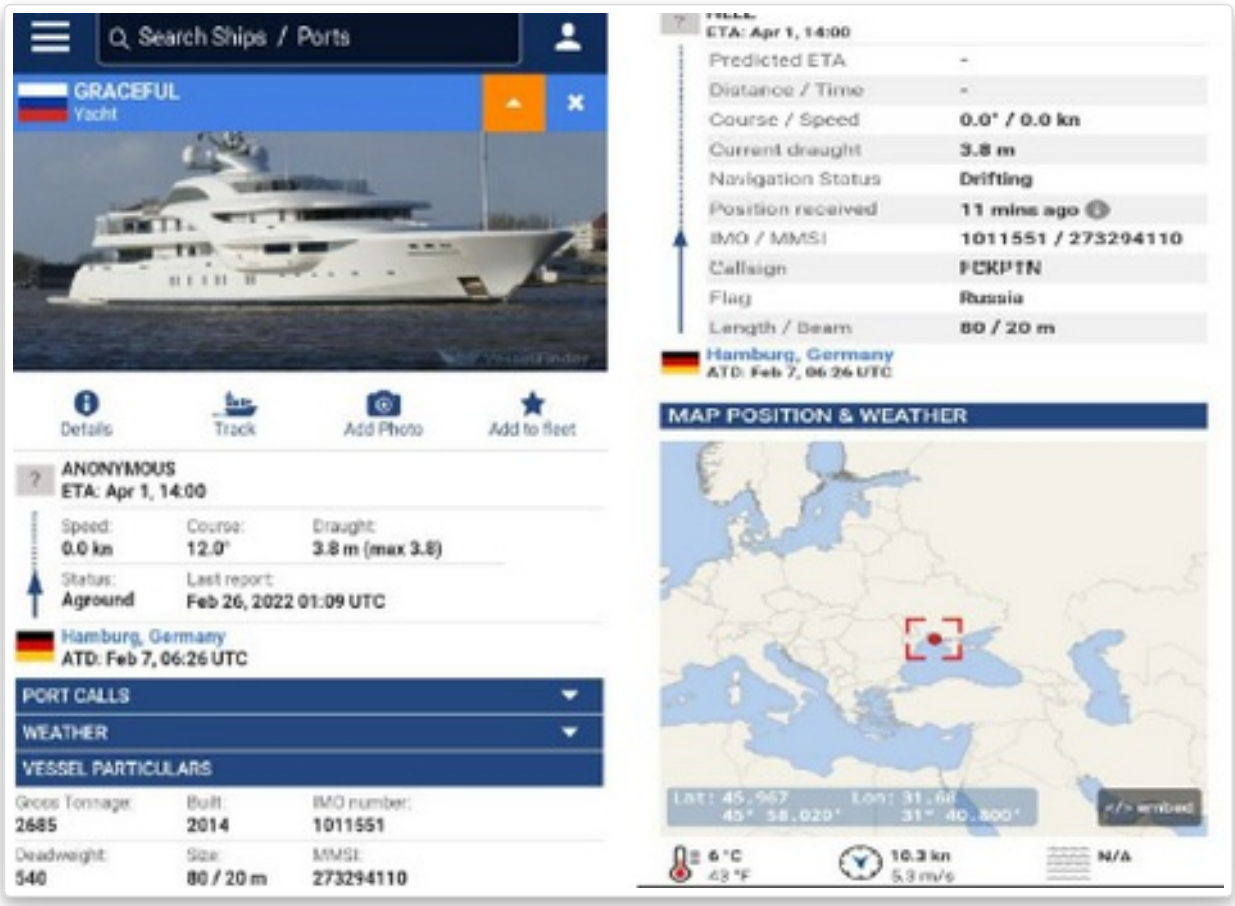



*Figure 4-8 : Exemple de compromission sur le positionnement et les informations de navigation d'un navire, en marge du conflit russo-ukrainien. Action revendiquée par « Anonymous ». Source : Marine Traffic.*

# 5. Les acteurs maritimes, victimes collatérales du cybercrime politique?

## 5.1. Les attaques en déni de service distribué

Sur l'année 2022, plusieurs attaques en déni de service distribué (*DDoS, Distributed Denial of Service*) affectant tant des sites Internet « vitrines » que des serveurs métiers exposés sur Internet. Avec l'invasion russe de l'Ukraine en 2022, le DDoS a pris une nouvelle dimension. En effet, les attaques DDoS sont de plus en plus souvent conduites par des cybercriminels animés de motifs politiques.

Le conflit russo-ukrainien a entraîné un regain de nationalisme à l'origine de l'émergence de groupes cybercriminels politiques (hacktivistes), leurs actions visant principalement à attaquer les institutions ukrainiennes ou des pays leur apportant leur soutien, sous quelque forme que ce soit.

Les attaques menées par ces acteurs sont majoritairement des attaques par DDoS ou des attaques par défacement. Si aucun secteur n'est spécifiquement visé par ces attaquants dont le but est de déstabiliser un pays, des entreprises du secteur maritime ont été ciblées symboliquement, parce que considérées comme des organismes essentiels aux états réellement dans le viseur des cybercriminels.

En effet, outre des entités connues tels que les *Anonymous*, de nouveaux groupes d'hacktivistes partisans de l'Ukraine ou de la Russie sont apparus et ciblent, entres autres, les infrastructures critiques ennemies. Les principaux d'entre eux sont notamment le groupe pro-russe *Killnet* et le groupe pro-ukrainien *UA IT Army*. Les attaques DDoS menées en 2022 sur les infrastructures critiques et les entreprises multinationales géopolitiquement exposées démontrent que le danger est bien réel pour le secteur maritime, dont le rôle-clé dans l'approvisionnement et le fonctionnement des pays occidentaux n'est pas à démontrer.

| Cible | Origine / Motivation |
|---|---|
| Port of London Authority[39] | Killnet/Altahrea Team/politique |
| Port de Klaipeda[40] | NoName057(16)/politique |
| Port de Ventspils | NoName057(16)/politique |
| Port de Tallin | NoName057(16)/politique |
| Bulgarian ports infrastructure company | Killnet/politique |
| Port de Nagoya | Killnet/politique |
| LTM Livorno Terminal | Killnet/politique |
| Port de Venise | Killnet/politique |
| Ports & Maritime Organization of Iran | Army of Thieves/politique |

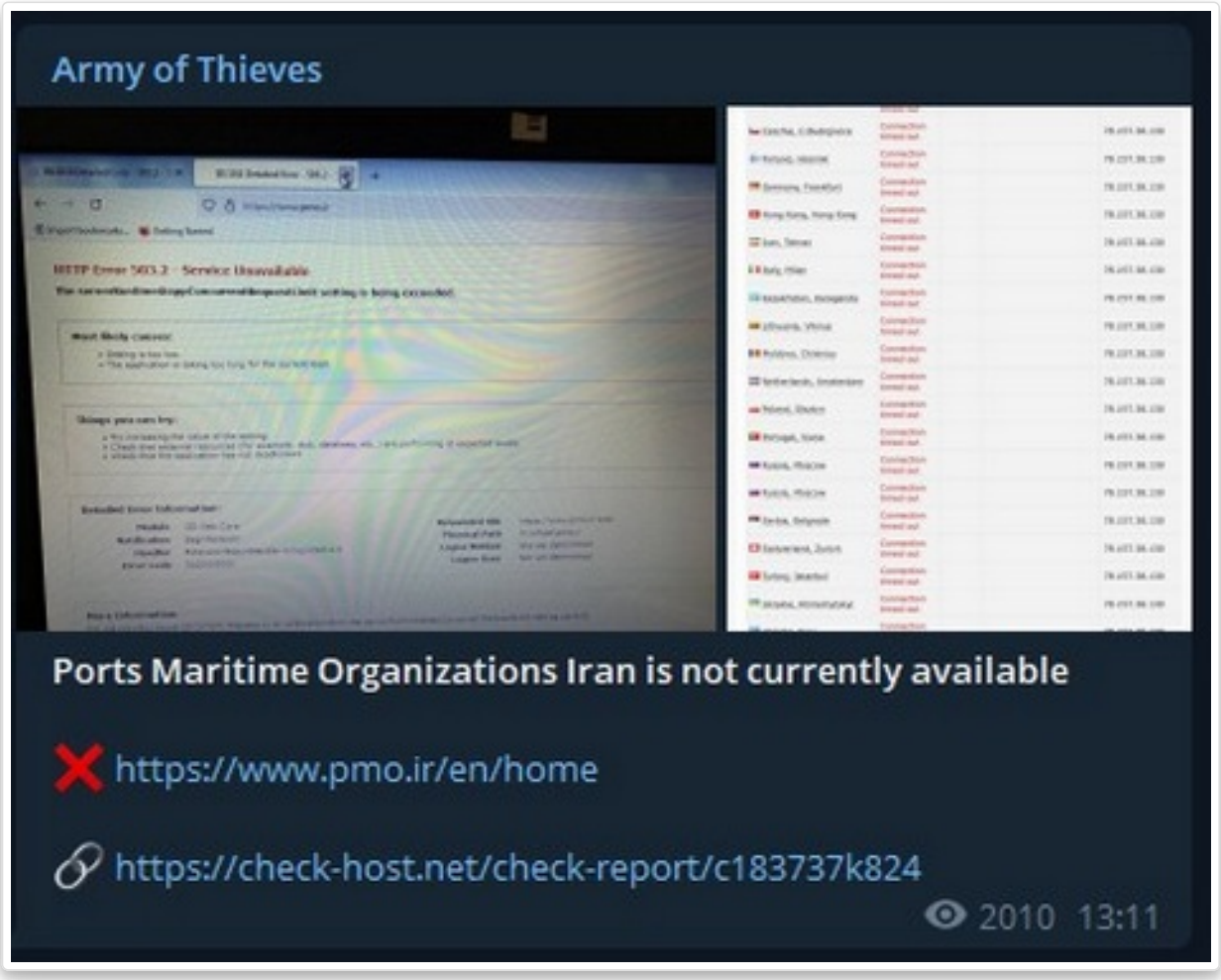



*Figure 5-1 : Le 31 août 2022, le site Internet de la Ports & Maritime Organization of Iran est ciblée par une attaque. Source : t[. ]me/ArmyThieves/125*

| Telegram |
| --- |
| Les chaînes Telegram – de même que les forums et marchés – sont à la fois en fin et en début de la chaîne d'attaque. Elles sont le débouché d'attaques réussies et permettent à d'autres attaquants de planifier leurs attaques. |

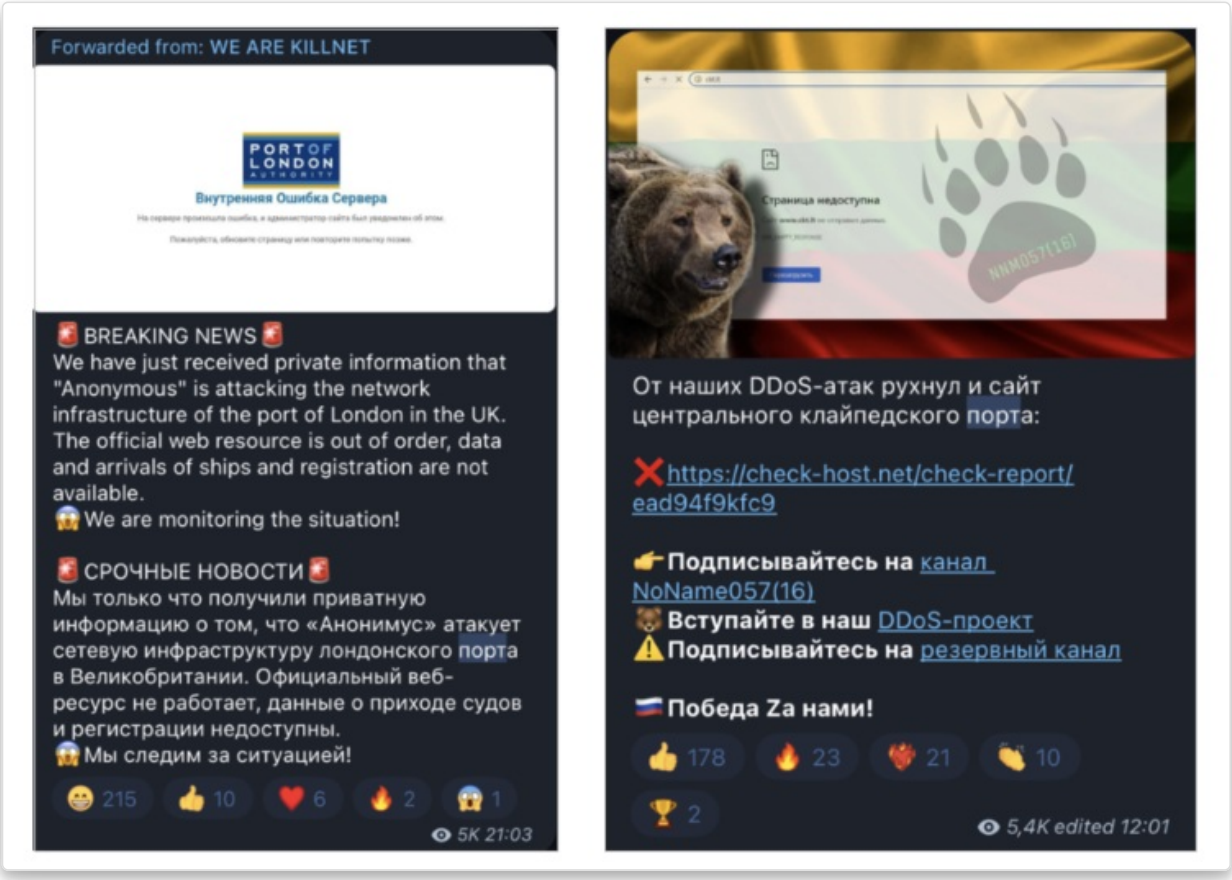



*Figure 5-2 : Annonces par Killnet et NoName057(16) de l'attaque DDoS sur Port of London et le Port de Klaipeda.*

| Les attaques DDoS |
| --- |
| Ces attaques sont fréquentes car relativement simples à mener et donc accessibles aux acteurs malveillants de tous niveaux. Leur finalité est de rendre indisponible un ou plusieurs services ciblés en exploitant des vulnérabilités matérielles ou logicielles. Le déni d'accès implique l'intervention d'un réseau de machines - souvent compromises - afin d'interrompre le ou les services visés. Que ce soit un site web ou un autre serveur applicatif, une fois paralysé par l'attaque, le service sera indisponible et inutilisable, ce qui peut conduire à des pertes financières et réputationnelles.<br>L'impact financier que peut engendrer un déni d'accès n'est pas à négliger, car il peut se chiffrer en millions d'euros. Ainsi, la société Bandwidth Inc aurait constaté un manque à gagner entre 9 et 12 millions de dollars du fait d'une attaque DDoS menée en 2021[41]. Selon une étude de la société Imperva, réalisée grâce à une enquête sur 270 entreprises, une attaque par déni d'accès coûte en moyenne 40 000 dollars par heure, soit environ 500 000 dollars en moyenne[42]. |

| Les attaques DDoS |
| --- |
| Le niveau d'expertise et de moyens des acteurs malveillants à l'origine de ces attaques varient de manière cardinale. OWN-CERT a observé des hacktivistes débutants qui se joignaient à une attaque organisée par un groupe comme *Killnet*, simplement en téléchargement un script et en se procurant un VPN. Des versions de ces scripts pour smartphones sont également proposées. A contrario, les cybercriminels les mieux organisés et spécialisés dans le « *DDoS as a Service* » mènent leurs attaques souvent à l'aide d'un réseau de machines compromises appelées *« botnet »*. |

## 5.2. Les acteurs malveillants pratiquant les attaques DDoS

Quatre types d'acteurs malveillants pratiquant les attaques DDoS sont généralement identifiables : les **acteurs étatiques**, les **acteurs financièrement motivés**, les **hacktivistes** et enfin plus marginalement les individus utilisant ces attaques par diversion.

Dans le cas d'acteurs employés et contrôlés par un État, les attaques DDoS ont généralement un objectif politique, celui de mettre hors service les cibles désignées comme importantes. Un des groupes étatiques connu pour sa spécialisation dans les attaques DDoS et au recours aux logiciels malveillants de type *wiper* [43] est l'entité «Unit 74455 [44]», que les services de renseignement américains rattachent à la Russie, et plus précisément au *Main Center for Special Technologies* du GRU[45]. Ce groupe opérerait depuis au moins 2009 et aurait ciblé spécifiquement les infrastructures critiques, dont notamment les systèmes de transport d'États membres de l'OTAN.

Certains acteurs malveillants utilisent les attaques DDoS afin d'en tirer un bénéfice financier. Plusieurs moyens de monétisation d'attaques DDoS existent.

### 5.2.1. Méthodes et organisation des acteurs

Des acteurs malveillants observés par le CERT OWN proposent le DDoS comme un service commercial (Figure 5-3). Un des objectifs peut être de nuire à un concurrent en rendant son site web inaccessible.

Un autre moyen de monétisation consiste à obliger la victime d'attaques à payer un abonnement pour se prémunir d'attaques futures. Dans ce cas, les cybercriminels garantissent également habituellement une protection contre les attaques DDoS effectuées par d'autres groupes cybercriminels.

Enfin, un dernier exemple de moyen de monétisation consiste à demander une rançon à la cible de l'attaque. Ce dernier cas peut être couplé à d'autres attaques, comme un chiffrement par rançongiciel. En effet, le groupe de rançongiciel LockBit a déclaré en août 2022 qu'il souhaitait coupler ses demandes de rançons avec des attaques DDoS, afin d'accroître la pression sur ses victimes et les contraindre à payer.

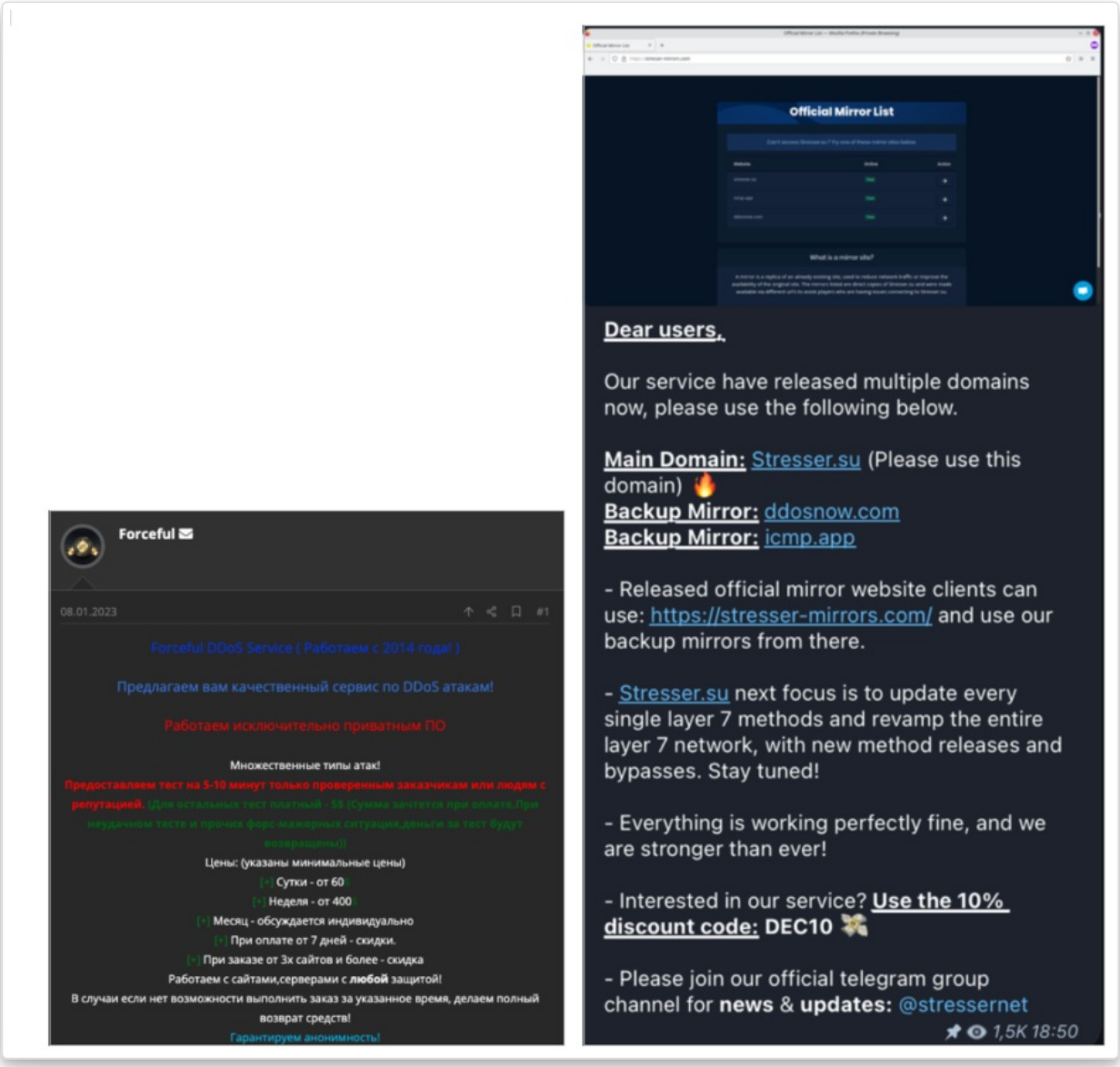



*Figure 5-3 : A gauche, vente d'un service de DdoS sur un forum cybercriminel russophone. A droite, vente d'un service de DdoS sur une chaîne Telegram anglophone et sinophone. Source : OWN-CERT.*

Les attaques DDoS menées par des hacktivistes ont particulièrement attiré l'attention médiatique du fait du contexte géopolitique avec l'invasion russe de l'Ukraine. Des dizaines de groupes comme Killnet, NoName057 et son projet «DDoSia», ou encore Infocentr, et Anonymous Russia sont connus pour leur engagement en faveur de la Russie et pour leurs attaques contre les sociétés et institutions occidentales (Figure 5-4).

Moins nombreux, des groupes bien organisés pro-ukrainiens existent également. Les plus importants d'entre eux sont notamment l'« IT Army of Ukraine », ou encore le «Comité étudiant de la cybersécurité et de la défense de l'Ukraine ».

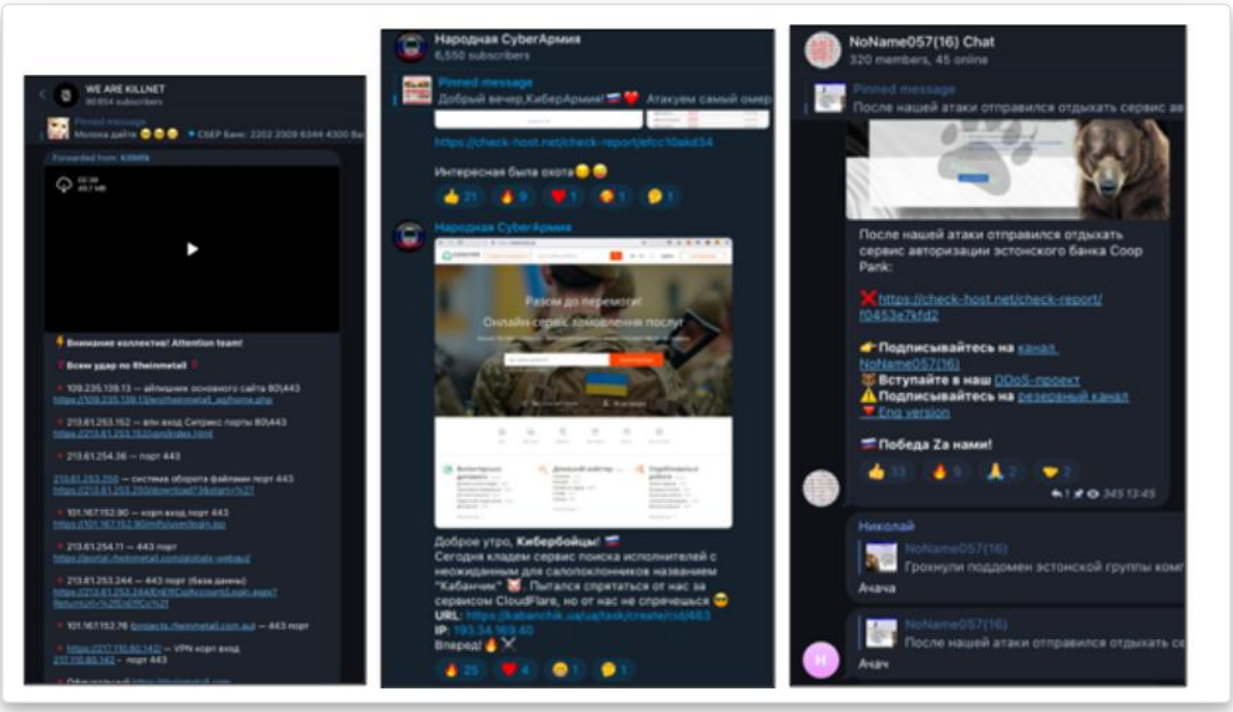



*Figure 5-4 : Exemples de chaînes Telegram appartenant à des groupes d'hacktivistes pro-russes se spécialisant sur les attaques DDoS. Source : OWN-CERT.*

L'IT Army of Ukraine possède son propre site web, où il est possible d'obtenir les outils et informations nécessaires afin de conduire des attaques contre les cibles nommées par l'entité. De plus, le site présente un classement des meilleurs acteurs ayant conduit le plus d'attaques contre les infrastructures ennemies (Figure 5-5).

Les exemples précédents illustrent le fait qu'actuellement, les attaques DDoS sont extrêmement courantes avec un accès relativement facile aux outils de DDoS. Les forums cybercriminels proposent des sections dédiées à cette thématique, avec des tutoriels et manuels permettant de se former (Figure 5-6).

Une alternative pour les cybercriminels ne souhaitant pas mener eux-mêmes les attaques consiste à payer un service de DDoS. Le « *DDoS as a Service* » est facilement accessible à toute personne cherchant des informations sur les forums cybercriminels, des chaînes Telegram ou tout simplement sur le web. En effet, des sites faisant la publicité des services d'« *IP Stressers* » et proposant des comparatifs en fonctions des types d'attaques et du prix sont facilement identifiables via une simple recherche sur Internet (Figure 5-7). Les prix peuvent varier de quelques dizaines d'euros pour des attaques de faible niveau, à plusieurs dizaines de milliers d'euros pour les plus sophistiquées et durables.

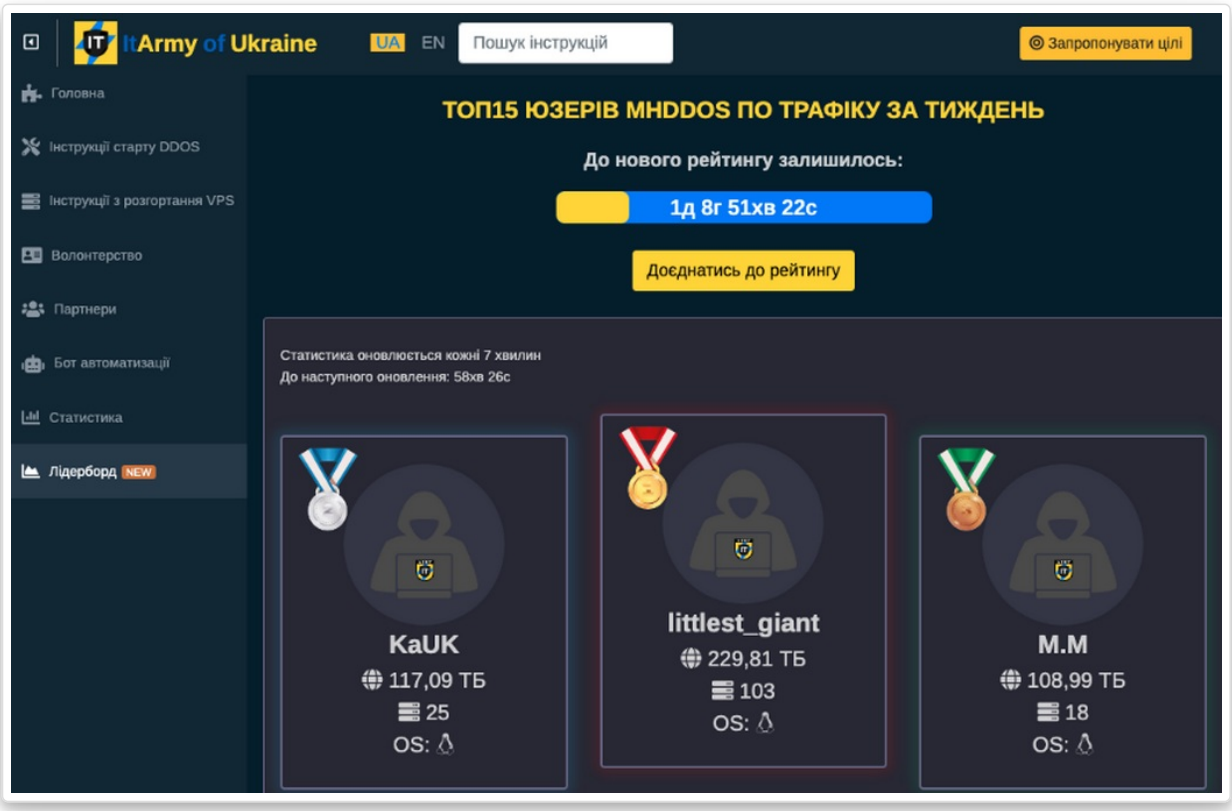



*Figure 5-5 : Site web officiel de l'IT Army of Ukraine. Classement des « meilleurs » DDoSeurs. Source : OWN-CERT.*

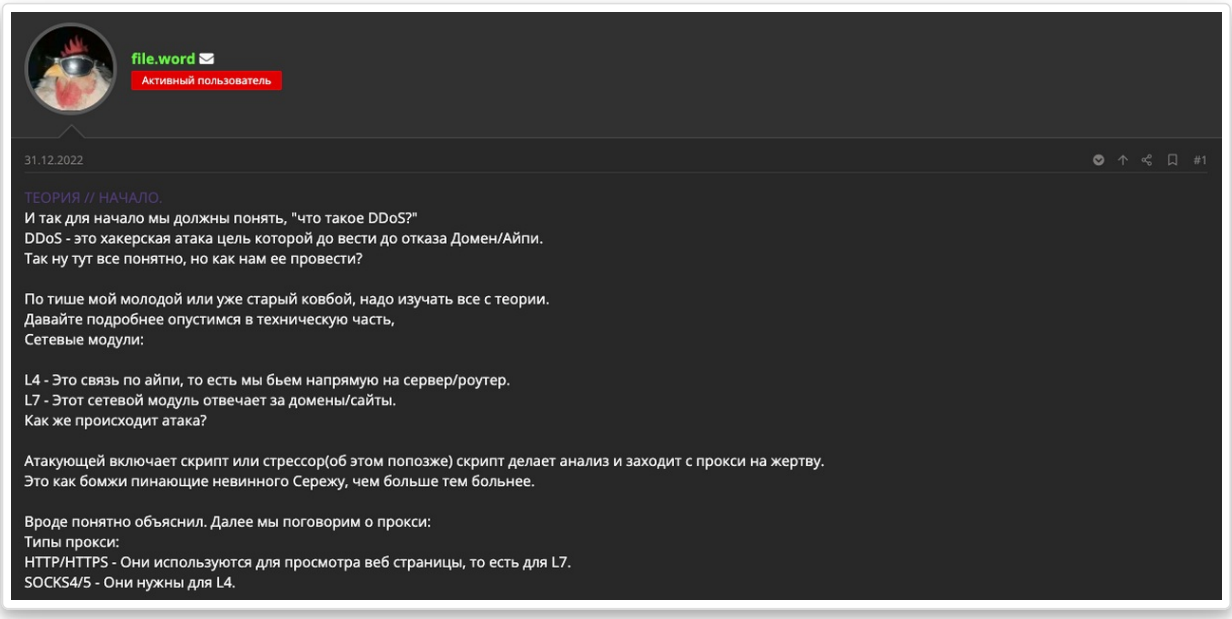



*Figure 5-6 : Un acteur malveillant donne des explications basiques sur le DDoS pour les débutants. Source : OWN-CERT.*

Des services proposant de tester la solidité et la fiabilité d'un réseau ou par exemple d'un site Internet existent aussi bien de façon légale qu'illégale. En effet, des services de *stresser* et de *booter* IP sont

proposés de façon tout à fait légitime aux administrateurs réseaux souhaitant évaluer la stabilité de leur système. Un *stresser* est un outil conçu pour tester la robustesse d'un réseau ou d'un serveur. Il permet notamment à l'administrateur d'évaluer si les ressources existantes - comme la bande passante ou les capacités de calcul - sont suffisantes pour gérer une charge supplémentaire. Le stresser IP peut cependant être détourné et utilisé afin de bloquer l'accès au service ciblé.

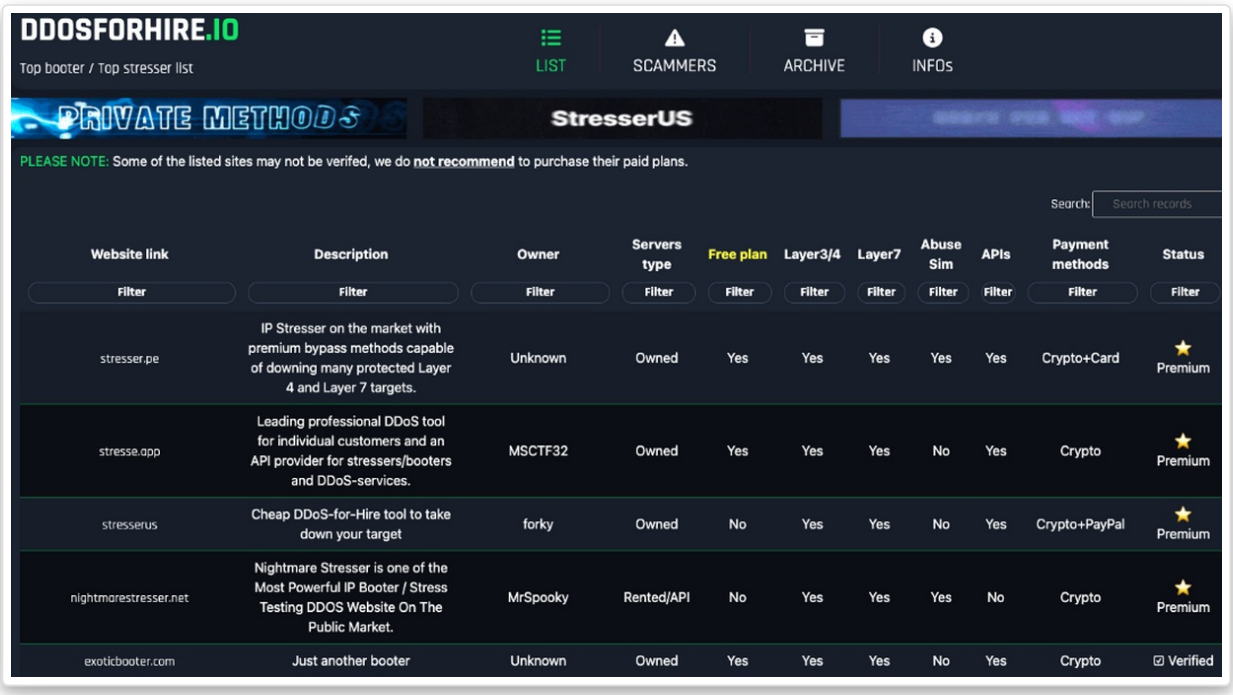



*Figure 5-7 : Un site proposant un comparatif des services de DDoS Existants. Source : OWN-CERT.*

Les *booters*, également connus sous le nom de *service booter*, sont des services d'attaque DDoS à la demande, proposés par certains criminels dans le but de neutraliser des sites Internet et des réseaux. En d'autres termes, les booters englobent l'usage détourné des stressers IP[46].

Ces deux outils sont fréquemment présentés sous couvert de services SaaS (logiciel en tant que service). Leurs prix varient entre quelques dizaines de dollars par mois à plusieurs milliers de dollars pour les services les plus complets (Figure 5-8).

Enfin, les acteurs malveillants souhaitant se lancer dans cette activité par eux-mêmes peuvent le faire, sans pratiquement rien débourser. Les scripts sont, par exemple, disponibles gratuitement sur GitHub (Figure 5-9) et sont largement exploités par les cybercriminels comme Killnet. Ces scripts, initialement dédiés à l'audit et aux test d'intrusion, finissent par être détournés et utilisés à des fins malveillantes. Ainsi, le CERT-UA a découvert que le JavaScript BrownFlood, utilisé pour attaquer des sites ukrainiens, a été publié sur GitHub un mois avant l'attaque[47].

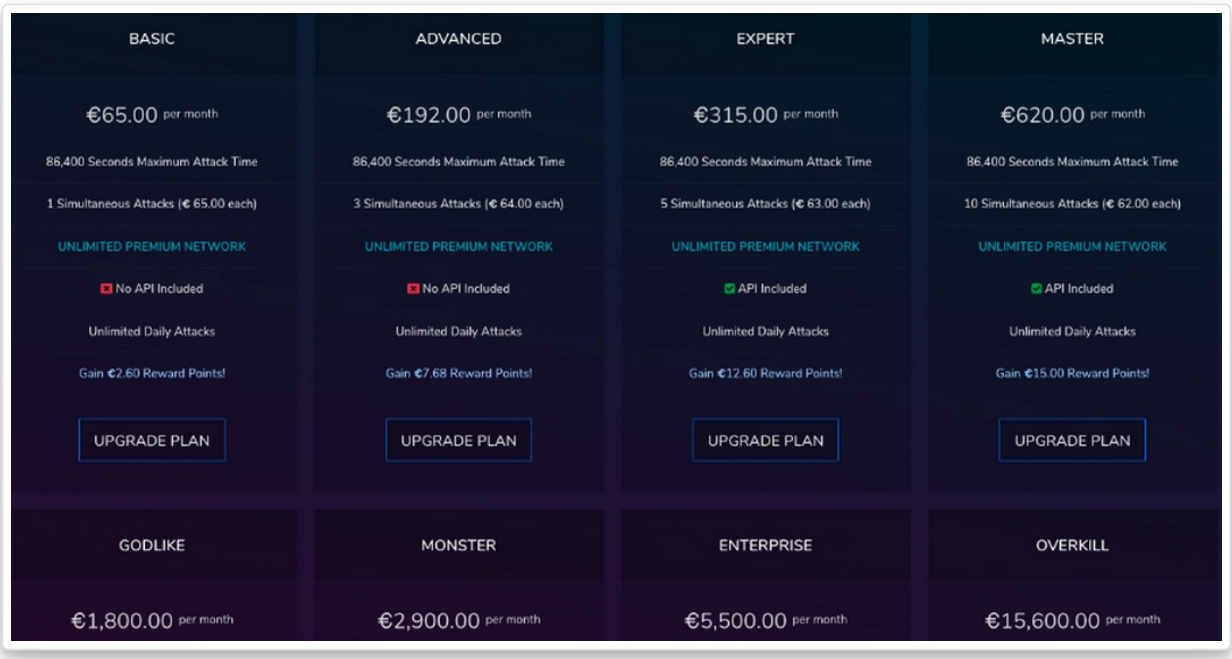



*Figure 5-8 : Exemple de services de stresser et prix associés. Source : OWN-CERT.*


*Figure 5-9 : Exemple d'un script DDoS proposant jusqu'à 56 méthodes d'attaques. Source : OWN-CERT.*

## 6. Cybersécurité maritime : Perspectives 2023

Le chapitre des perspectives est toujours un exercice difficile en cybersécurité : anticiper reste un défi, étant donné le caractère protéiforme et changeant de la menace et la complexité du secteur maritime. Cependant, les tendances longues identifiées en 2022 permettent de dresser quelques perspectives :

- Tout d'abord, sans aucun doute, **l'activité cyber pour 2023 restera plus que jamais intimement liée au contexte géopolitique**. A l'heure de la rédaction de ce document, il existe peu de doutes quant à la poursuite dans les mois qui viennent du conflit russo-ukrainien : les différents évènements identifiés en 2022 en lien avec ce conflit (tentatives de sabotage, lutte d'influence informationnelle, criminalisation d'activités type DDoS) devraient se poursuivre, visant notamment le secteur du naval de défense, les administrations et plus largement toutes les entités maritimes, navales, portuaires et industrielles considérées comme jouant un rôle en soutien du conflit[48].
- Une attention toute particulière devra être portée sur le renforcement de la bipolarisation à une échelle plus globale, avec des tensions géopolitiques qui pourraient se renforcer et avoir des conséquences dans le spectre cyber, en préalable ou en accompagnement d'actions militaires : l'entrée en lice de nouveaux acteurs cyber apporterait de nouvelles techniques, tactiques et procédures, de nouvelles plateformes, de nouvelles cibles.
- La multiplication des campagnes sur les systèmes industriels démontre l'adaptation des acteurs dans ce domaine, certains se spécialisant même dans ce type d'attaque. Le secteur maritime, par ses spécificités, constitue une cible directe ou indirecte : les ports et les navires dépendent de systèmes complexes, longtemps restés déconnectés du reste, ce cloisonnement étant aujourd'hui beaucoup moins tranché face à l'hyperconnectivité croissante. Dans le contexte géopolitique que nous connaissons, il n'est pas à exclure que des attaquants proches d'États aient recours à des codes malveillants spécialisés sur les systèmes industriels.
- La menace cybercriminelle, politisée ou non, ne doit pas non plus être écartée, puisque des attaques par rançongiciel ont déjà visé ce type d'installations. Particulièrement révélée durant l'année 2022, ce type d'attaque se poursuit en 2023 et, sans être un outil de destruction, il peut avoir des impacts sur les entreprises, qu'ils soient réputationnels ou financiers.
- L'emploi *d'infostealers* divers tel que Vector Stealer, initié fin 2022, se poursuit en 2023.
- **Le secteur maritime ne fait pas exception au déploiement de nouvelles techniques d'intrusion initiale.** Ainsi, en tant que cible principale, d'opportunité ou de victime collatérale, le secteur maritime devra composer et s'ajuster en permanence aux innovations des acteurs malveillants. Le OWN-CERT identifie déjà, par exemple, sur le début de l'année 2023, l'usage généralisé de pièces jointes au format OneNote, tous secteurs confondus. Pour rendre leurs méthodes d'ingénierie sociale toujours plus crédibles, les acteurs de la menace s'appliqueront encore et toujours à personnaliser leurs contenus (courriels, fichiers…) à l'aide du vocabulaire professionnel ou de référence à des évènements sectoriels. S'ils s'appuient déjà sur les documents-types échangés par l'IT maritime (*Bill of lading*, *Notice of readiness*…), **il est**

**possible que certains acteurs aux capacités avancées élargissent leur scope au jargon de l'OT** (thématiques SCADA, automatismes, contrôle de cargaison ou de propulsion).

- **L'utilisation potentielle de moyens alternatifs au *phishing*** par courriel afin d'obtenir des informations (par exemple : réseaux sociaux professionnels ou privés, appels téléphoniques, *smishing*…) devrait se renforcer.
- L'hétérogénéité des systèmes d'information, connectés ou déconnectés, à terre, offshore ou sur les navires renforce la nécessité d'**être vigilant quant aux méthodes de propagation sur les périphériques physiques.**
- La poursuite de la découverte de**vulnérabilités** dans des librairies de développement largement employées qui, **dans un contexte renforcé d'infogérance**, sont parfois difficiles à identifier en absence de cartographie partagée entre tous les acteurs, devrait rester d'actualité.
- Devant une lutte plus acharnée contre les rançongiciels,**les fuites de données devraient rester un point de pression important**.
- Si certains doutaient de l'intérêt de l'intelligence artificielle (IA) en préparation d'une attaque cyber, les démonstrations par certains chercheurs d'outils comme ChatGPT doit alerter la communauté sur l'existence et la performance de certains outils mis à disposition du public. Le renforcement de la concurrence dans ce secteur, avec l'arrivée de nouveaux acteurs, accentuera le nombre d'outils à disposition, leurs capacités, leur actualité et leur précision. Au-delà de la préparation des attaques, il n'existe guère de doute que le développement d'outils automatisés d'attaque à base d'IA se poursuivra, tant par des officines étatiques ou pseudo-étatiques que cybercriminelles.
- **Les attaques visant délibérément ou de manière opportuniste les acteurs de la chaîne logistique maritime et portuaire, au sens large, devraient être amenées à se poursuivre**, pour plusieurs raisons : le nombre et la maturité technologique et organisationnelle parfois faible de certains acteurs en termes de cybersécurité, la transformation numérique forte du secteur avec un recours important à la sous-traitance et au cloud. Dans un contexte de forte interdépendance, une attaque sur un acteur de la *supply chain* comme les infogérants ou MSP (*Managed Service Provider*) a des conséquences considérables : par exemple, une multitude de navires d'armateurs différents peuvent se retrouver impactés par la perte d'un système d'information commun opéré par un acteur de la *supply chain*.

En lien direct avec les secteurs de l'approvisionnement logistique, des systèmes de supervision industrielle, de l'agro-alimentaire, de la grande distribution, des télécommunications, de la défense ou encore de l'énergie, le secteur maritime se doit d'élargir son modèle de menace et de risques vers une approche contiguë et globale du renseignement.

Dans ce contexte où la transformation numérique du secteur se poursuit, on peut reconnaître la montée en maturité progressive de certains acteurs, se regroupant au sein d'associations comme France Cyber Maritime pour favoriser le partage d'informations cyber, qui reste un moyen particulièrement efficace pour la prévention des attaques, en France mais aussi à l'international et sans oublier les outremers : les efforts en ce sens méritent être poursuivis et soutenus.

# 7. Glossaire

Ce glossaire précise la signification de certains acronymes ou expressions, parfois anglophones utilisés dans ce bulletin. En effet, l'expérience maritime et portuaire des personnes destinataires de ces bulletins peut différer et un langage commun est nécessaire à la bonne compréhension des notions abordées.

**A2/AD**

*Anti Access/Area Denial* : tactique visant à interdire le recours à une zone et, par extension, à tout moyen pouvant permettre de mener des opérations dans cette zone.

**ADMIRAL**

*Advanced Database of Maritime cyber Incidents Released for Litterature*

**AIS**

*Automatic Identification System* : il s'agit d'un système radioélectrique communautaire de partage d'informations nautiques (position, type de navire, nom) créé afin d'améliorer la connaissance de la sécurité nautique et, notamment, de prévenir les abordages en mer.

**APT**

*Advanced Persistent Threat* : ces sources de menaces dites « avancées » et « longue durée » sont reconnues comme étant souvent conduites par des acteurs chargés d'accomplir des actions offensives de niveau étatique. Ayant parfois recours à des menaces non encore connues (appelées « zero day »), leurs objectifs visent généralement des pays ou des secteurs particuliers, en vue de sabotage, d'espionnage ou de création de « dossiers d'objectifs ».

**BEC**

*Business Email Compromise*

**CERT**

*Computer Emergency Response Team* : le CERT est un centre expert en charge de l'analyse et du partage d'information cyber. Ses missions peuvent varier suivant les centres, leurs objectifs, leur niveau de maturité et leurs moyens. En France, le M-CERT est le CERT sectoriel des secteurs maritimes et portuaires. Travaillant en lien avec les autorités et acteurs du secteur public, il veille à maintenir et à partager une connaissance de la menace visant le secteur. Il travaille en coordination avec d'autres CERT, en France et à l'international.

**CMS**

*Content Management System*

**CRPA**

*Controlled Radiation Pattern Antenna*

**CTI**

*Cyber Threat Intelligence* : il s'agit du processus permettant de d'orienter, de générer, d'analyser et de diffuser du renseignement d'intérêt cyber.

**DDoS**

*Distributed Denial of Service*

**EMR**

Énergies Marines Renouvelables

**FOVI**

Faux Ordre de VIrement

**GNL**

Gaz Naturel Liquéfié

**GNSS**

*Global Navigation Satellite System* : système de référence de positionnement, de navigation et de temps utilisant des constellations de satellites.

**GPS**

*Global Positioning System*

**IAB**

*Initial Access Broker*

**IoC**

*Indicator of Compromise* : un indicateur de compromission est une information technique (par exemple : adresse IP, Uniform Resource Locator, nom de domaine, adresse de courriel, etc.) attribué à une menace. Il est généré à partir de capteurs, de sources ouvertes ou fermées, ou de partenaires. Sa durée de vie est normalement éphémère, de quelques semaines à quelques mois. L'intégration des IoCs dans des outils de détection d'intrusion (type sonde) ou de pare-feux contribue à la protection des systèmes. Un IoC est un élément de renseignement : sa diffusion doit respecter les TLP. Il ne faut pas tenter de consulter ou d'interagir avec l'IoC, afin de ne pas compromettre d'action en cours.

**IT**

*Information Technology* : il s'agit, de manière générale, des systèmes d'information présentant des caractéristiques non industrielles (en termes de temps-réel ou d'impact sur le monde physique). Exemples : systèmes de messagerie électronique, sites Internet…

**M-CERT**

*Maritime Computer Emergency Response Team*

**OSINT**

*Open Source Intelligence* : le renseignement d'origine source ouverte correspond à la recherche et à l'analyse d'informations ouvertes et publiques.

**OT**

*Operational Technology* : il s'agit, de manière générale, des systèmes d'information présentant des caractéristiques industrielles (en termes de temps-réel ou d'impact sur le monde physique). Exemples : systèmes à automates, vidéo-protection…

**PNT**

Position, Navigation, Temps

**RAT**

*Remote Administration Tool*

**RDP**

*Remote Desktop Protocol*

**SSH**

*Secure SHell*

**SQL**

*Structured Query Language*

**TLP**

*Traffic Light Protocol* : il s'agit d'un protocole mis en place dans la diffusion du renseignement d'intérêt cyber, afin de contrôler la diffusion de l'information associée pour en assurer la protection.

**TTP**

Techniques, tactiques, procedures : il s'agit d'éléments relatifs aux modes opératoires des attaquants pouvant permettre de les identifier ou de mieux s'en protéger.

**USB**

*Universal Serial Bus*

**VDR**

*Voyage Data Recorder*

**VPN**

*Virtual Private Network*

**VSAT**

*Very Small Aperture Terminal*

**XSS**

*Cross Site Scripting*

# 8. A propos de France Cyber Maritime et du M-CERT

France Cyber Maritime est une association Loi 1901 créée en novembre 2020 et soutenue par l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) et par le Secrétaire Général de la Mer (SGMer).

Les objectifs principaux de France Cyber Maritime sont :

- de développer un réseau d'expertise en cybersécurité maritime en stimulant la création de services à haute valeur ajoutée et adaptés aux besoins de l'industrie
- d'améliorer la résilience des opérations maritimes et portuaires face aux menaces cyber en développant et opérant le M-CERT (Maritime Computer Emergency Response Team), qui fournit assistance et information à tous les opérateurs.

L'activité du M-CERT a démarré en mars 2021. Le M-CERT produit des bulletins d'analyse réguliers aux adhérents de l'association. En complément des services de Cyber Threat Intelligence, le M-CERT est également engagé dans la prévention des risques et la coordination de la réponse à incident, en relation avec les autorités de l'État et les organisations de cybersécurité.

Début 2023, France Cyber Maritime regroupe 70 membres, de l'écosystème maritime au sens large, et bénéficie de partenariats nationaux et internationaux.

Pour nous contacter :

| | France Cyber Maritime | M-CERT |
|---|---|---|
| Site Internet | https://www.france-cyber-maritime.eu | https://www.m-cert.fr |
| Courriel | contact@france-cyber-maritime.eu | contact@m-cert.fr |
| Twitter | @FrCyberMaritime | @M_CERT_FR |
| LinkedIn | https://www.linkedin.com/company/france-cyber-maritime | |

## 9. A propos de OWN


*Figure 9-1 : Logo de OWN*

Créé en 2008, OWN est un Pure Player de la cybersécurité qui s'empare de la cybersécurité avec une vision lucide et perspicace des enjeux de ses clients, au travers d'un portefeuille d'activités riche se déclinant en 5 compétences : Audit, Conseil, Threat Intelligence, CERT et SOC.

OWN accompagne au quotidien des petites, moyennes et grandes organisations pour leur permettre d'exercer leur métier dans les meilleures conditions en proposant une amélioration en continue de leur cybersécurité et une assistance pour mieux anticiper, détecter et réagir à une menace cyber. La cybersécurité d'OWN, c'est une approche centrée sur la menace et les risques dans ses dimensions techniques, organisationnelles et géopolitiques, qui constitue son ADN dont le séquençage repose sur : Operate, Warn, Neutralize. Trois actions qui symbolisent pleinement le rôle de ses experts au quotidien : conseiller et prendre part à des actions de cyberdéfense, informer et alerter lorsque le risque est imminent et enfin contribuer à la remédiation pour neutraliser la menace.

Site Internet : https://ww.own.security

Contact : contact@own.security

## 10. Références


1. https://www.first.org/tlp/↩
2. https://gitlab.com/m-cert/admiral↩
3. Zone d'influence et d'attraction économique du port s'étendant dans les terres.↩
4. https://www.cluster-maritime.fr/la-filiere-maritime/leconomie-maritime/↩
5. https://csrc.nist.gov/publications/detail/sp/800-82/rev-3/draft↩
6. Voir https://www.cert.ssi.gouv.fr/alerte/CERTFR-2022-ALE-009/ (Fortinet), https://www.cert.ssi.gouv.fr/alerte/CERTFR-2022-ALE-009/ (Zimbra), https://www.cert.ssi.gouv.fr/alerte/CERTFR-2022-ALE-002/ (VMWare), https://www.cert.ssi.gouv.fr/alerte/CERTFR-2022-ALE-013/ (Citrix) et https://www.cert.ssi.gouv.fr/alerte/CERTFR-2022-ALE-007/ (Microsoft), dont Exchange : https://www.cert.ssi.gouv.fr/alerte/CERTFR-2022-ALE-008/↩
7. https://thedfirreport.com/2023/03/06/2022-year-in-review/↩
8. MITRE ATT&CK est une base de connaissances ouverte sur les acteurs de la menaces, leurs outils, leurs tactiques, techniques et procédures d'attaques. MITRE ATT&CK propose sa propre kill chain dans laquelle sont répertoriées des techniques d'attaque. cf https://attack.mitre.org.↩
9. https://www.fortinet.com/blog/threat-research/deep-analysis-formbook-new-variant-delivered-phishing-campaign-part-ii↩
10. SHA256 : edf47cd187c4b8d92f09152b5e1285366c03afa1a4be4815f853ded3b1240ce6↩
11. SHA256 : bc3a22bf48c38ec75a45f8d70f04af9fee4f58b190dada24c2f65fe73184b596↩
12. MV : Motor Vessel↩
13. SHA256 : 5b312f6c8aaea04ae089007f9429a8e651bb73fa2069fb9418d0fa85f04f7c17↩
14. SHA256 : 4797d55178aa25fa8e5938b65162d71dc4da21bc8bc51d3138bfb09a805190bd↩
15. SHA256 : 63c6132898aa1688e9cbc165713df00213d9aee29127aa710d138e0d55eb5145↩
16. SHA256 : 11f59f304cbb0d10023ff8e405f28bc52e02fcefa963ff35e79e66020770703b↩
17. https://www.fbi.gov/file-repository/fy-2022-fbi-congressional-report-business-email-compromise-and-real-estate-wire-fraud-111422.pdf↩
18. https://britanniapandi.com/2022/04/cyber-fraud-incident/↩
19. https://unit42.paloaltonetworks.com/operation-falcon-ii-silverterrier-nigerian-bec/↩
20. SHA256 : 46b006db8260be2e32171038ee3fe8cc52552d460efef4ab8cf2c549a778dc86↩
21. https://www.wired.com/story/belarus-railways-ransomware-hack-cyber-partisans/↩
22. https://unit42.paloaltonetworks.com/plugx-variants-in-usbs/↩
23. https://www.proofpoint.com/us/blog/threat-insight/chasing-currents-espionage-south-china-sea↩
24. aussi connu sous les noms de Léviathan ou APT40.↩
25. https://www.mandiant.com/resources/blog/suspected-iranian-actor-targeting-israeli-shipping↩

26. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/hydrochasma-asia-medical-shipping-intelligence-gathering↩

27. https://www.mandiant.com/resources/blog/apt32-targeting-chinese-government-in-covid-19-related-espionage↩

28. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/hydrochasma-asia-medical-shipping-intelligence-gathering↩

29. https://blogs.blackberry.com/en/2023/02/newspenguin-a-previously-unknown-threat-actor-targets-pakistan-with-advanced-espionage-tool↩

30. https://www.dragos.com/year-in-review/↩

31. https://www.forescout.com/blog/ot-icefall-56-vulnerabilities-caused-by-insecure-by-design-practices-in-ot/↩

32. https://ics-cert.kaspersky.com/publications/reports/2022/06/27/attacks-on-industrial-control-systems-using-shadowpad/↩

33. https://www.mandiant.com/resources/blog/incontroller-state-sponsored-ics-tool↩

34. https://www.ege.fr/infoguerre/les-cables-sous-marins-nouvel-echiquier-du-conflit-americano-chinois↩

35. https://www.hawaiinewsnow.com/2022/04/13/hsi-agents-honolulu-disrupted-cyberattack-undersea-cable-critical-telecommunications/↩

36. https://share.sekoia.fr/s/B6s8EtRLp2G8EnT↩

37. https://securityintelligence.com/news/acidrain-malware-modems-ukraine-germany/↩

38. https://shipping.nato.int/nsc/page10303037↩

39. Claudia Glover, « Port of London Authority Hit by "politically Motivated" Cyberattack », Tech Monitor (blog), 24 mai 2022, https://techmonitor.ai/technology/cybersecurity/port-of-london-authority-cyberattack↩

40. Ylabs, « Analysis of the Russian-Speaking Threat Actor NoName 057(16) », YLabs, 13 octobre 2022, https://labs.yarix.com/2022/10/analysis-of-the-russian-speaking-threat-actor-noname-05716/↩

41. https://www.sec.gov/Archives/edgar/data/1514416/000151441621000280/q32021exh991-preliminaryth.htm↩

42. https://www.imperva.com/blog/ddos-impact-cost-of-ddos-attack/↩

43. "Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure | CISA", Cybersecurity and Infrastructure Security Agency CISA, 9 mai 2022, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a↩

44. https://intelnews.org/tag/gru-unit-74455/↩

45. https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and↩

46. https://www.imperva.com/learn/ddos/booters-stressers-ddosers/↩

47. https://www.malwarebytes.com/blog/news/2022/04/ukraine-government-and-pro-ukrainian-sites-hit-by-ddos-attacks↩

48. "jouant un rôle" étant du ressort de l'attaquant, il continuera à être particulièrement subjectif.↩