LA CYBERSÉCURITÉ CENTRÉE
SUR LA CONNAISSANCE DE LA MENACE

OSSIR – 11.07.2023

Panorama de la cybermenace maritime 2022

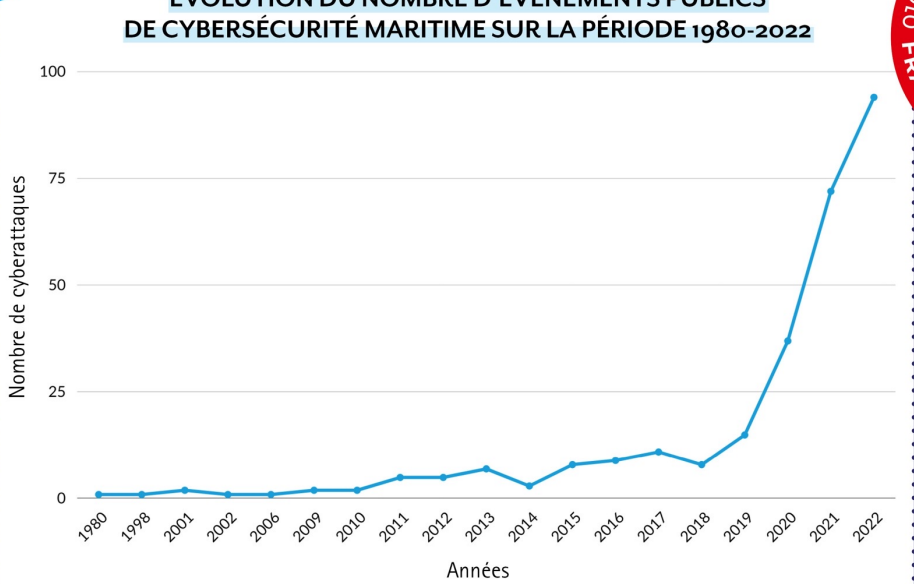
France Cyber Maritime & OWN

PRÉSENTATION DE FRANCE CYBER MARITIME & DU M-CERT
- Olivier Jacq, France Cyber Maritime

PRÉSENTATION DE OWN & DU CERT-OWN
- Marion Lachiver, Analyste CTI, OWN

PRÉSENTATION DU PANORAMA DE LA CYBERMENACE MARITIME 2022
- Olivier Jacq, France Cyber Maritime
- Marion Lachiver, Analyste CTI, OWN

MEMBRES DE FRANCE CYBER MARITIME



Source : ADMIRAL - https://gitlab.com/m-cert/admiral

NOS MISSIONS

1 Accroître la résilience du monde maritime et portuaire face à la menace cyber

2 Contribuer à la création d'une filière d'excellence française en cybersécurité maritime

REMINDER IN 2022

SEKOIA

SERVICES

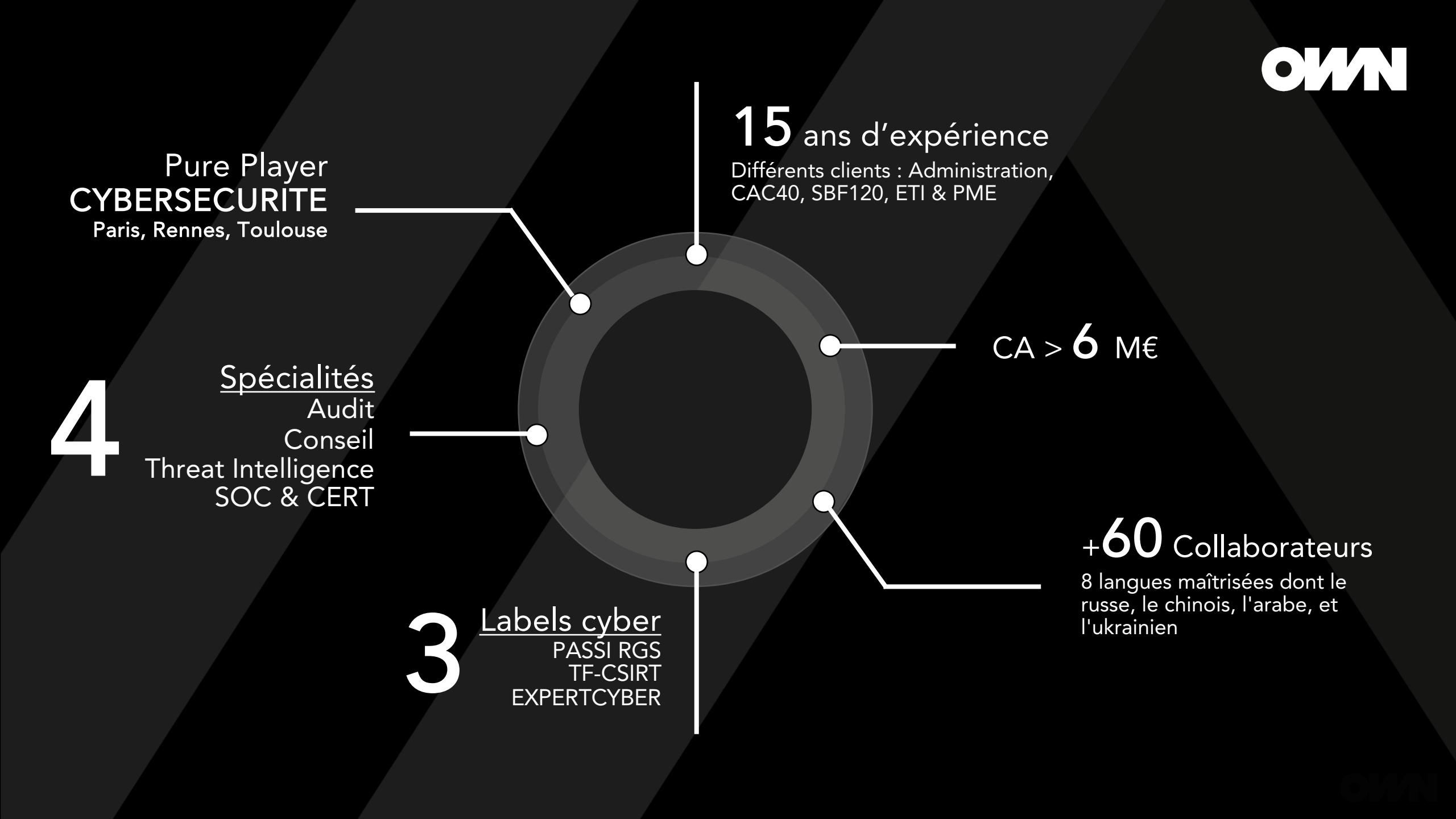
CONSULTING

SOFTWARE

OWN

SEKOIA.IO

2 DIFFERENTS COMPANIES


OWN
15 ans d'expérience
Différents clients : Administration, CAC40, SBF120, ETI & PME
Pure Player
CYBERSECURITE
Paris, Rennes, Toulouse
CA > 6 M€
4
Spécialités
Audit
Conseil
Threat Intelligence
SOC & CERT
+60 Collaborateurs
8 langues maîtrisées dont le russe, le chinois, l'arabe, et l'ukrainien
3
Labels cyber
PASSI RGS
TF-CSIRT
EXPERTCYBER

NOS EXPERTS

- FORENSICS
- FRAUD
- APTS
- GEOPOLITICS
- SOC ANALYST
- MALWARE ANALYSIS
- IE
- PURPLE TEAM
- DATA ANALYSIS
- DARKWEB INFILTRATION
- OSINT
- DEVOPS
- LAW INTELLIGENCE
- INCIDENT HANDLER
- YARA, SIGMA
- CYBERCRIME ANALYST
- CRISIS

Des profils aux expériences variées, issus des secteurs bancaire, énergie, télécommunication, défense, IT, services de renseignement, sociétés de conseil.

Une expertise CERT d'activités de réponse à incident, ancrant l'analyse des menaces dans l'observation de cas client, et de leur télémétrie, et mettant la CTI au service d'une meilleure réponse à incident.

Des formations multiples : géopolitique, sécurité économique, ingénierie informatique, cybersécurité, développement, juridique…

Une expertise confirmée avec des analystes senior de plus de 20 ans, 10 ans d'expérience dans l'analyse des menaces.

Des profils aguerris aux méthodes d'investigation, produisant des formations à l'attention d'analystes CTI junior.

INTERCERT FRANCE

TF-CSIRT Trusted Introducer

Authorized to Use CERT™
CERT is a mark owned by Carnegie Mellon University

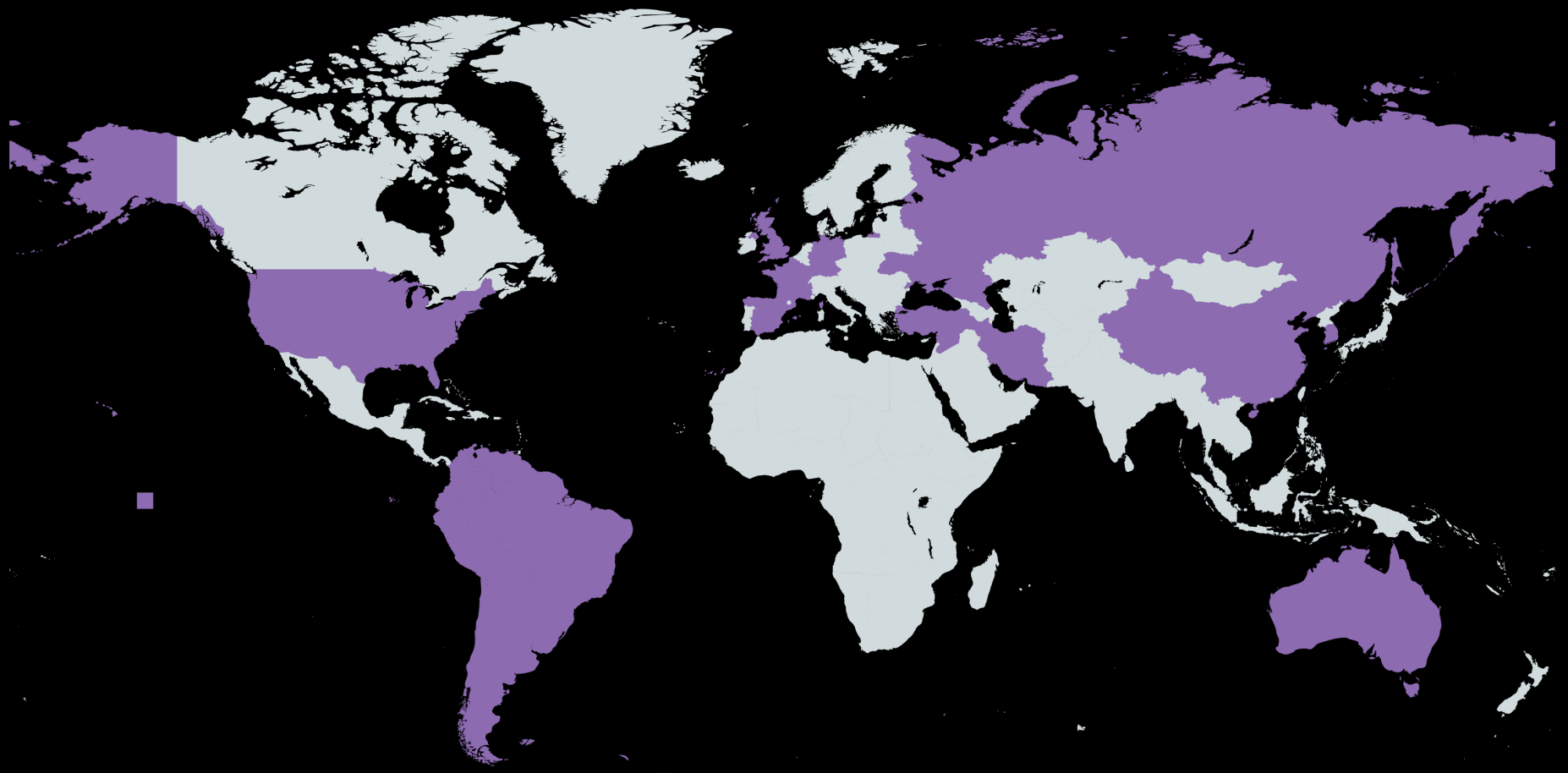
EXPERT CYBER

GCTI

GCFE

OWN

EXPERTISES PAYS ET PLURILINGUISTIQUE



Géopolitique & Ecosystèmes cybercriminels

De nombreux langages maîtrisés :
le russe, le chinois, l'arabe, l'ukrainien, l'allemand ou l'espagnol

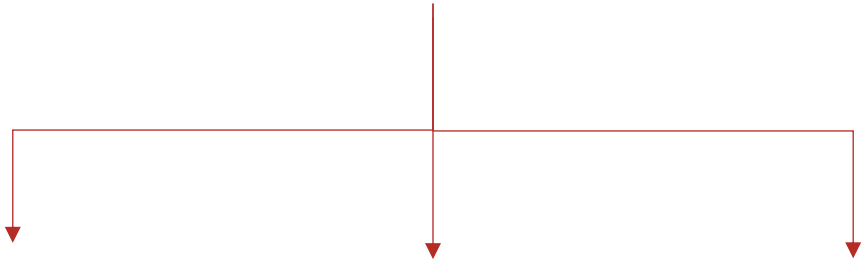
MÉTHODOLOGIE

LE SUIVI QUOTIDIEN

Sources privilégiées

Capteurs OSINT
Trackers techniques, Espaces d'échange cybercriminels

Presses et publications ouvertes



Campagnes de phishing et spear phishing

Suivi des groupes d'attaquants

Identification des malware et infrastructures

OBJECTIF
Identifier les campagnes ciblant ou usurpant des acteurs du secteur maritime

DÉMARCHE
Anticiper les opérations s'appuyant sur l'ingénierie sociale

UN BAROMÈTRE MENSUEL

TENDANCES OBSERVÉES

- Campagnes de phishing et spear phishing
- Principaux malware distribués
- Bases de données et accès vendus en ligne
- Ransomware

TRAVAUX D'ANALYSE

- Tactiques, techniques et procédures
- Evolutions des modes opératoires
- Analyse de malware
- Identification et clusterisation de campagnes
- Caractérisation de groupes d'acteurs

PRODUCTIONS

- Un baromètre mensuel avec des chiffres clés
- Des articles d'analyse approfondie
- Des indicateurs de compromission contextualisés
- Des recommandations (prévention, détection, hunting)

PANORAMA DE LA CYBERMENACE MARITIME 2022

LE SECTEUR MARITIME

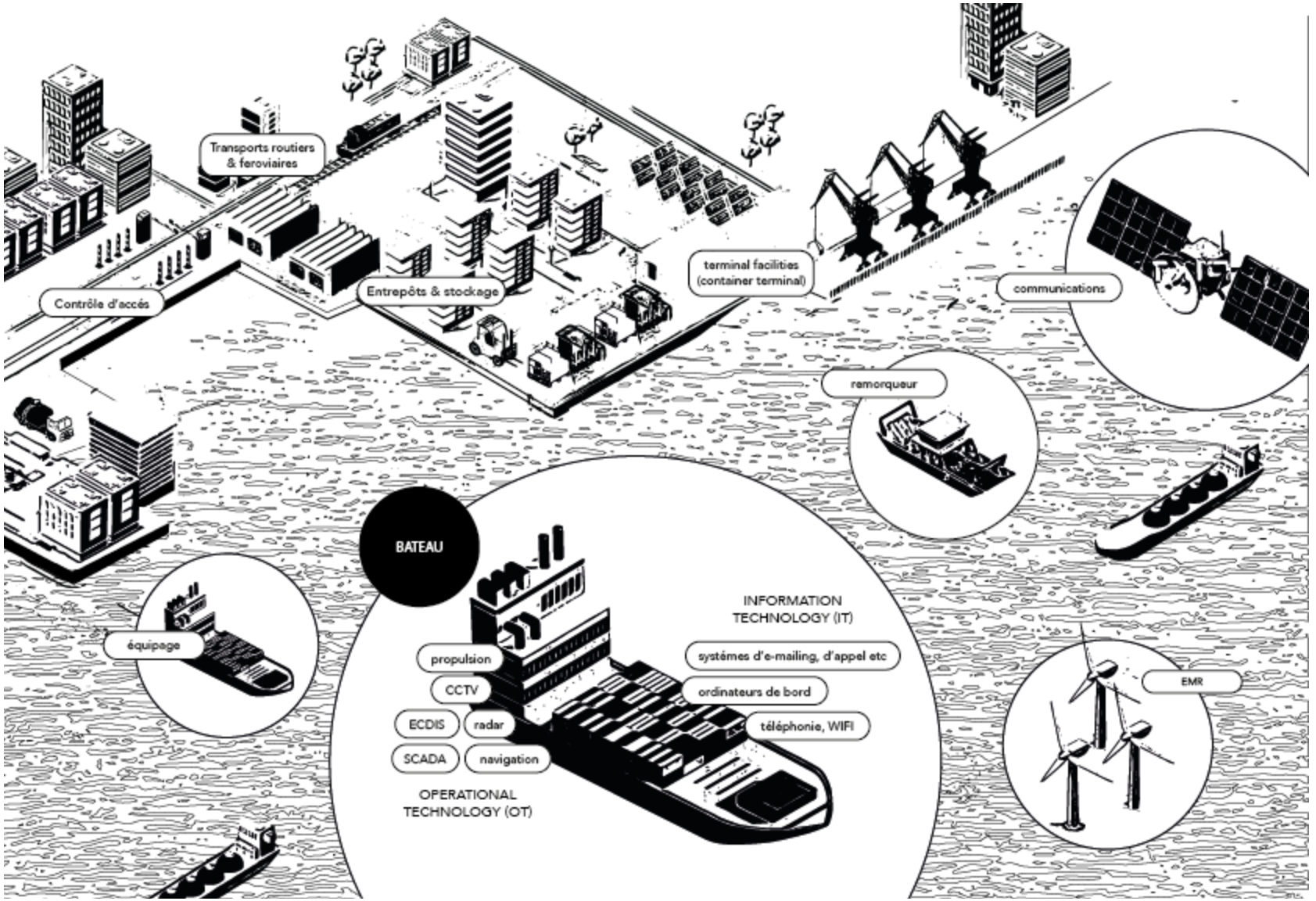
386 000 emplois
91 Mds – 80 %

• Les **ports** : qu'ils soient de commerce, de pêche, multimodaux, d'importance locale, régionale, nationale ou internationale : avec leurhinterland [zone d'influence et d'attraction économique du port s'étendant dans les terres], ils irriguent l'économie de matières premières, de biens et de services indispensables au fonctionnement des économies ;

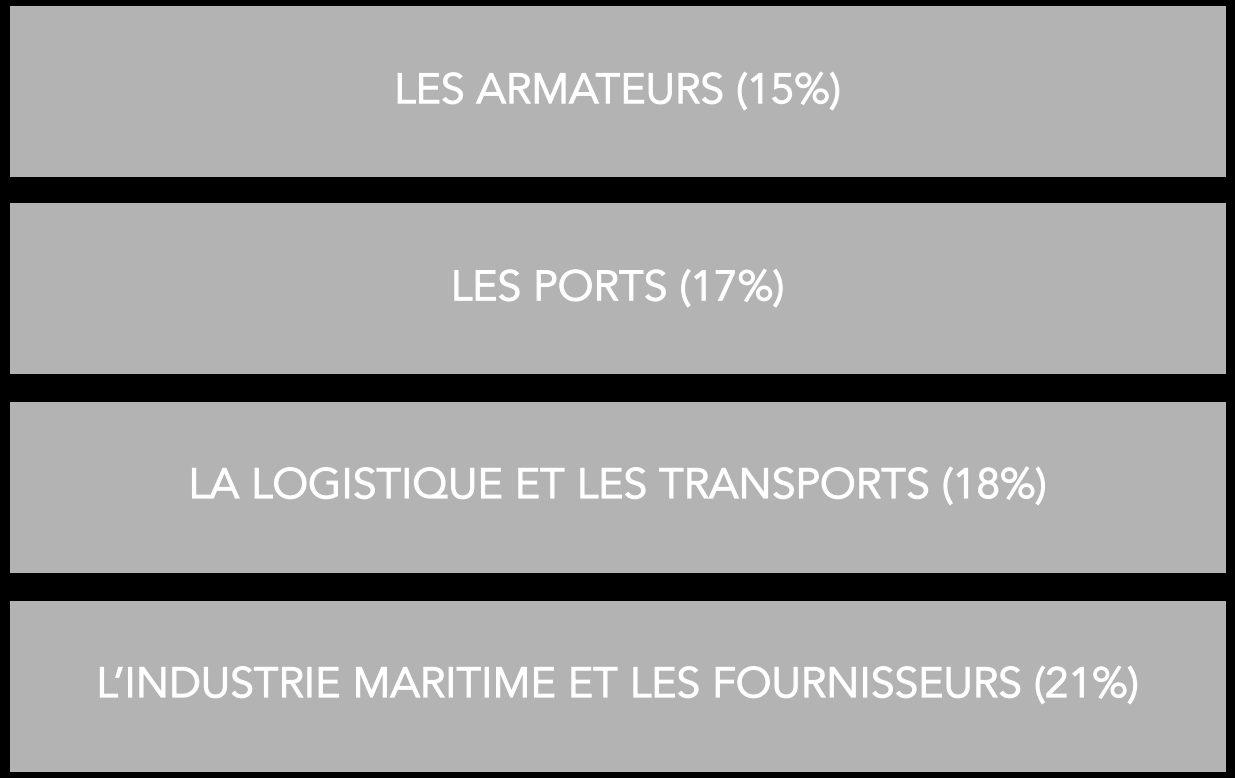
• Les **navires**, dans toute leur diversité :
navires à passagers, porte-conteneurs, méthaniers, pétroliers, navires de soutien, navires de recherche, navires câbliers

• 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 ;
• 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.



LES CHIFFRES



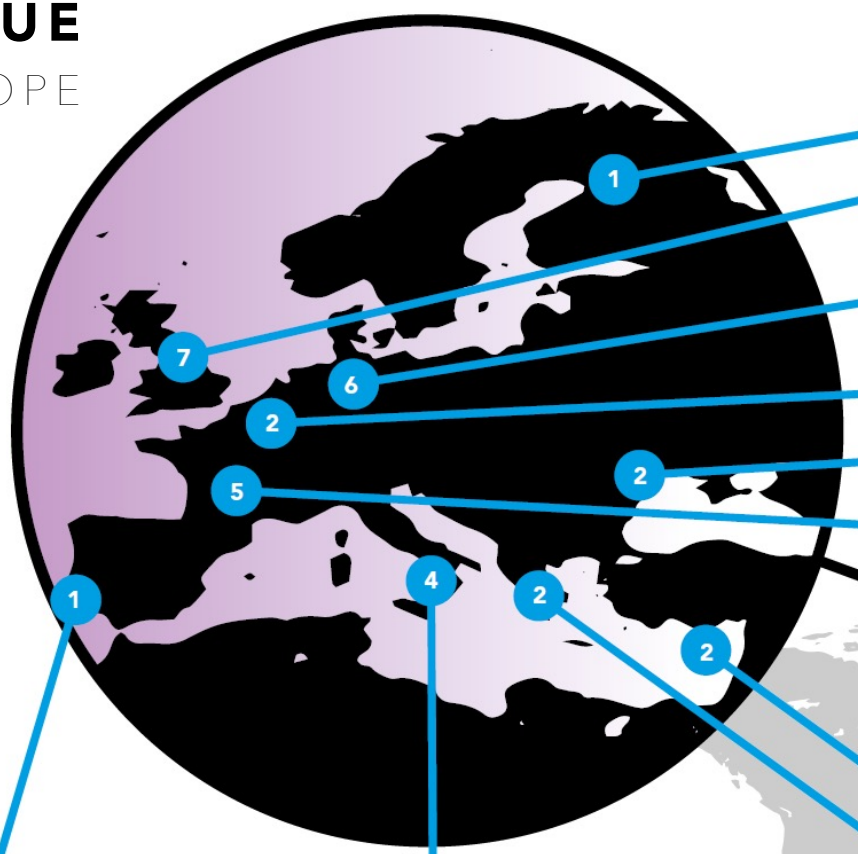
+21 % (2021), +235 % (2020)

90 INCIDENTS EN 2022

- Les armateurs continuent à être victimes d'attaques sérieuses, notamment par rançongiciels.
- Forte exposition aux tentatives de phishing et de spearphishing.

RÉPARTITION GÉOGRAPHIQUE

FOCUS EUROPE



Finlande : 1 évènement : Industrie (rançongiciel, juillet 2022)

Grande Bretagne : 7 évènements : Armateur (intrusion, février 2022), Armateur (rançongiciel, février 2022), Armateur (rançongiciel, mars 2022), Armateur (rançongiciel, avril 2022), Assureur (FOVI, avril 2022), Port (DDoS, mai 2022), Armateur (rançongiciel, juillet 2022)

Allemagne : 6 évènements : Industrie (rançongiciel, janvier 2022), Industrie (rançongiciel, février 2022), Armateur (harponnage, mars 2022), EMR (rançongiciel, mars 2022), EMR (rançongiciel, avril 2022), Industrie (non précisé, décembre 2022)

Belgique : 2 évènements : Industrie (rançongiciel, janvier 2022), logistique (rançongiciel, août 2022)

Ukraine : 2 évènements : Administration (intrusion, janvier 2022), navire (leurrage AIS, février 2022) : je compte l'Ukraine comme faisant partie du continent européen.

France : 5 évènements : Armateur (intrusion, janvier 2022), Association (défaçage de site Internet, juillet 2022), Industrie (rançongiciel, juillet 2022), industrie (fuite de données, août 2022), organisation (rançongiciel, octobre 2022), port (hameçonnage, novembre 2022)

Portugal :
1 évènement : port (décembre 2022)

Italie :
4 évènements :
pêche (rançongiciel, janvier 2022),
logistique (rançongiciel, janvier 2022),
port (déni de service, juin 2022),
défense (fuite de données, août 2022)

Chypre : 2 évènements : Administration (fuite de données, mai 2022), Logistique (Rançongiciel, juin 2022)

Grèce : 2 évènements : Armateur (rançongiciel, avril 2022), armateur (rançongiciel, avril 2022)

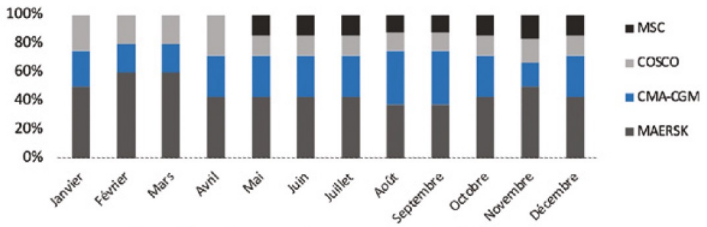
ETATIQUES • CYBERCRIMINELLES • HACKTIVISTES

LA KILL CHAIN

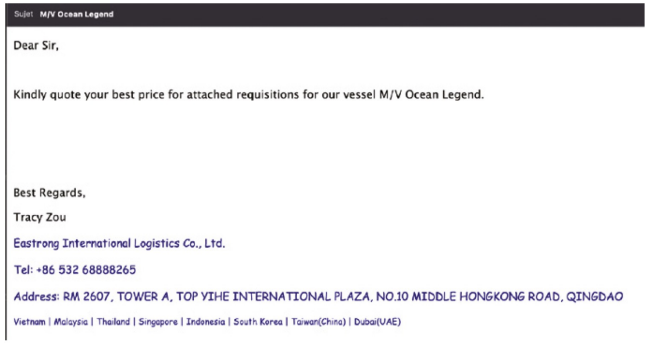
LES VECTEURS D'INTRUSION INITIALE → LES MALWARES DÉLIVRÉS → LES OBJECTIFS DES ATTAQUANTS

LES VECTEURS D'INTRUSION INITIALE

DES CAMPAGNES DE PHISHING TAILLÉES SUR MESURE



Répartition des grandes campagnes de phishing identifiées sur l'année 2022 par armateur usurpé. Source : OWN-CERT



Sujet: M/V Ocean Legend

Dear Sir,

Kindly quote your best price for attached requisitions for our vessel M/V Ocean Legend.

Best Regards,

Tracy Zou

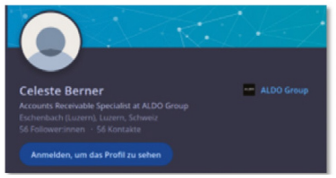
Eastrong International Logistics Co., Ltd.

Tel: +86 532 68888265

Address: RM 2607, TOWER A, TOP YIHE INTERNATIONAL PLAZA, NO.10 MIDDLE HONGKONG ROAD, QINGDAO

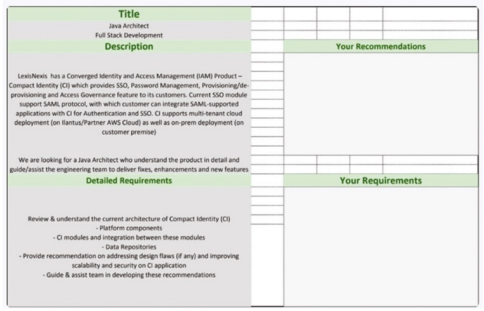
Vietnam | Malaysia | Thailand | Singapore | Indonesia | South Korea | Taiwan(China) | Dubai(UAE)

Courriel malveillant distribuant Lokibot dans une campagne ciblant le secteur maritime (SHA256 : 4797d55178aa25fa8e5938b65162d71dc4da21bc8bc51d3138bfb09a805190bd)

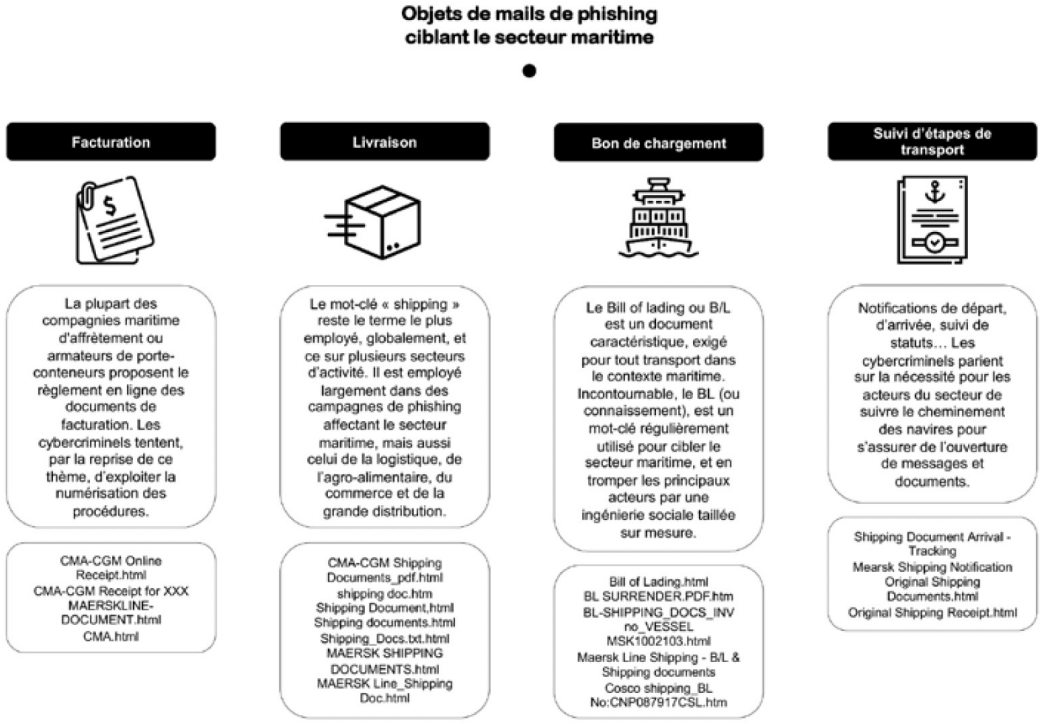


Employé d'une entreprise usurpée par l'attaquant POSEIDON-IS

Usurpation de la Pakistan International Maritime Expo & Conference (PIMEC-2023) – manuel d'exposant ciblant les visiteurs potentiels (NewsPenguin)



Fausse offre d'emploi (UNC3890 réputé lié à l'Iran) ciblant des compagnies de transport maritime



Sujets d'ingénierie sociale

DES CAMPAGNES DE PHISHING TAILLÉES SUR MESURE

Noms de pièces-jointes malveillantes ciblant le secteur maritime

Noms de navires	Zones géographiques	Nom d'acteurs du secteur	Suivi des étapes logistiques	Facturation
La convention de nommage reprend le type de navire MV, BBG, etc.	Certains fichiers proposent un pays ou une zone géographique.	Les fichiers seront crédibles en mentionnant des acteurs spécifiques	Les données de suivi des étapes de départ, d'arrivée, rendez-vous sont reprises.	Les noms de fichiers de facturation sont récurrents.
MV Vessel Vsl Bozat MT BBG sailing vessel details Vessel DETLS ...	Baltic China ...	Aquamarinex DHL Lampung Agency ...	Port agency appointment Vendor new form Arrival Sailing Detls Detail TLX tracking number CTM TBN DWT Appointment letter ...	Proforma Invoice Order_pro Copy Swift Arrival Notice and Tax Invoice Consignment Details BL Bill of Lading And Proforma Invoice BL-Copy Telex AND BL Balance Payment Swift ...

Le Bill Of Lading, BL, Bon de Chargement ou Connaissement est un document utilisé dans le commerce international pour accuser réception, faciliter l'envoi et assurer la sécurité de l'envoi de marchandises. Il cadre la propriété des marchandises transportées et les droits en découlant.

Extrait de document de phishing subtilisant des identifiants de la cible

Modèle de Bill of Lading présentant une typographie « Landing », largement partagé sur Internet et repris par les acteurs malveillants

Modèle de Bill of Lading

L'ACHAT D'ACCÈS EN LIGNE

LE CAS DES INITIAL ACCESS BROKERS

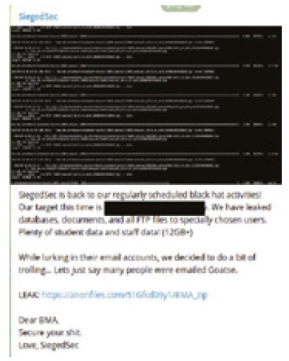
Des opérations opportunistes

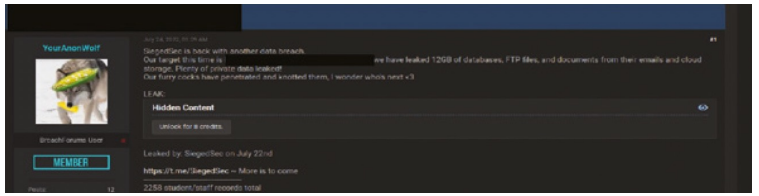
QUELQUES VICTIMES :

- Entreprise fournissant de l'électronique de marine
- Agence ministérielle maritime
- Académie maritime
- Chantier naval
- Marines nationales

EXEMPLES DE DONNÉES VENDUES :

- Clés privées de systèmes VSAT de yachts privés et de navires militaires
- Noms, prénoms, emails, adresses, téléphones, etc.
- Couples identifiant/mot de passe
- Fichiers présents sur des serveurs FTP
- Courriers électroniques
- Accès à des services cloud





LE CAS DES CLÉS USB

LES SUPPORTS USB RESTENT DES VECTEURS POTENTIELS DE PROPAGATION DE CODES MALVEILLANTS AU SEIN DU SECTEUR MARITIME.

Un SI déconnecté
De nombreux systèmes d'information de navires ou de ports, notamment des systèmes de contrôle industriels, de vidéosurveillance ou de sûreté sont déconnectés d'Internet et des infrastructures IT "classiques".

Risque supply chain
Pour autant, les opérations de maintenance préventive ou corrective dont ils font l'objet (mise à jour de programmes, de micrologiciels) ont recours aux supports USB apportés par des opérateurs de maintenance qui les exploitent au profit de plusieurs armateurs, sans décontamination préalable.

Risque : infection par rebond d'un ou plusieurs systèmes d'information

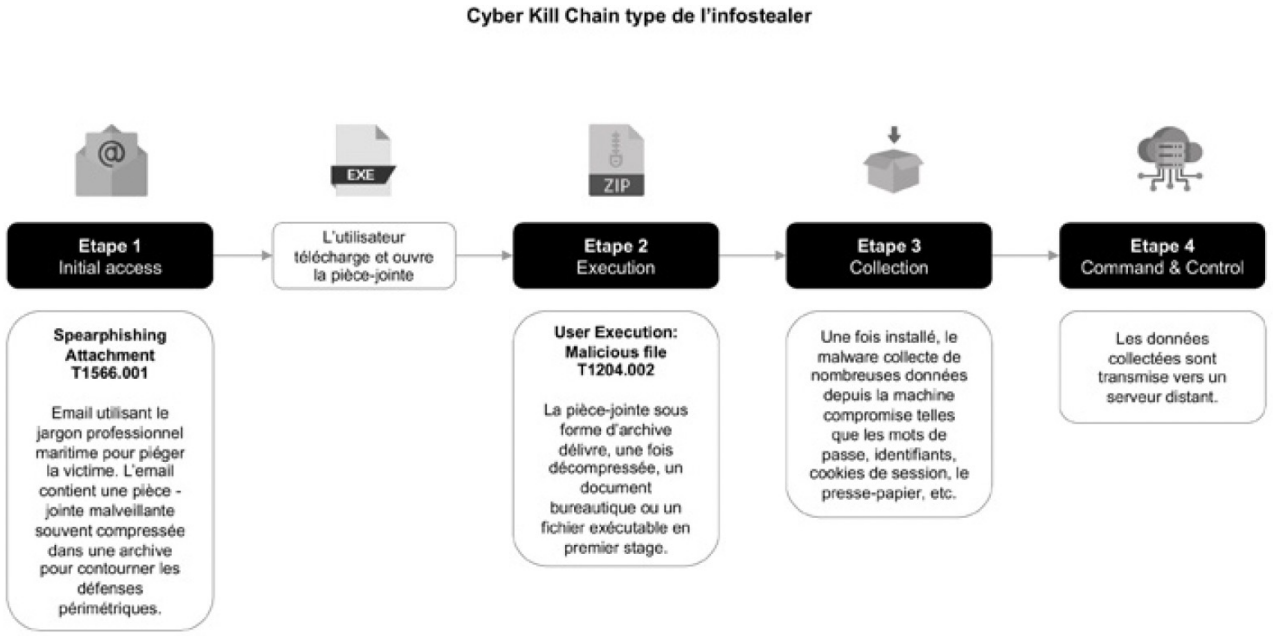
LES MALWARE DÉLIVRÉS

LA PRÉDOMINANCE DES INFOSTEALERS

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.

- 24 familles d'infostealers identifiées.
- Constante augmentation du nombre de fichiers malveillants ciblant le secteur maritime, avec un pic en fin d'année.
- Présence équilibrée tout au long de l'année des infostealers Formbook, Agent Tesla et Lokibot ; Apparition de Vector stealer.
- Forte augmentation du nombre de fichiers liés à Snake Keylogger et Remcos dès l'été 2022.



LE RAT PLUGX

OBJECTIFS DES APTS ÉTATIQUES

- 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.

PlugX est un Remote Access Tool (RAT), installant une porte dérobée sur les systèmes compromis. Les attaquants exploitent ce type de malware afin de se pré-positionner en vue de mener des exécutions de code malveillant à distance sans être détecté.

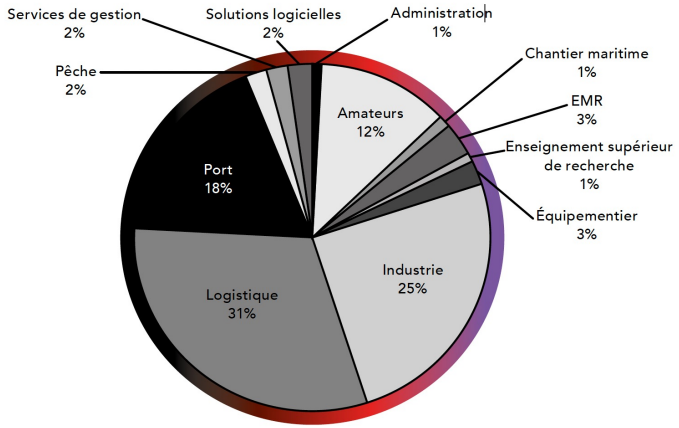
En 2022, 7 navires ont été compromis par PlugX.

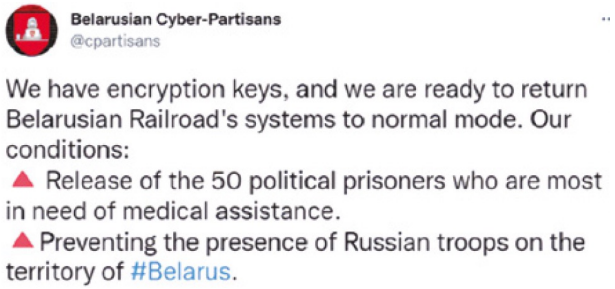
LES OBJECTIFS DES ATTAQUANTS

Revente de données, espionnage, brouillage GNSS, sabotage, Business Email Compromise, rançonnage, perturbation politique

RANÇONNAGE

- 56 attaques recensées sur l'année 2022.
- Aucun groupe de rançongiciel spécialisé dans l'attaque d'entreprises du secteur maritime.
- Prédominance des ransomware Lockbit, Conti et Play.
- Des attaques majoritairement opportunistes.
- Des exception avec des utilisations politiques.





En janvier 2022, les "Partisans Cyber biélorusses", un groupe d'hacktivistes, ont lancé une attaque par rançongiciel sur les infrastructures ferroviaires de la Biélorussie15. 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.

BUSINESS EMAIL COMPROMISE

QU'EST-CE QUE LE BEC ?

Business Email Compromise (BEC), ou arnaque au Faux Ordre de Virement (FOVI).

OBJECTIF

- Inciter un employé à effectuer des virements de fonds ou à divulguer des informations confidentielles sur son entreprise.
- Usurpation d'une figure de confiance (autorité hiérarchique, direction financière, administration, client habituel, partenaire, banque...).
- Utilisation de comptes de messagerie d'entreprise compromis pour initier les discussions et effectuer des transferts frauduleux.

FOCUS

POSEIDON-IS-001

- En activité depuis 2019 et est encore actif aujourd'hui
- **TTPs**
  phishing, distribution de l'infostealer Lokibot, utilisation de domaines typosquattés
- Overlap
  liens avec SilverTerrier, une attribution à des acteurs nigérians

PARIS - RENNES - TOULOUSE
-
Téléphone
+33 (0) 805 -690-234
-
contact@own.security

WWW.OWN.SECURITY