TLP:AMBER

N° 1
FÉVRIER
2025

RAPPORT SUR L'ÉTAT DE LA MENACE CYBER DANS L'OCÉAN INDIEN

CYBER RÉUNION

Ce document a été rédigé en collaboration avec

OVN

TLP:AMBER

Sommaire

1

Rapport sur l'état de la menace cyber
dans l'Océan Indien

Introduction

1.1 AVANT-PROPOS

La Réunion, territoire stratégique au cœur de l'Océan Indien, se situe à un carrefour essentiel de nombreux enjeux mondiaux. En tant que l'une des rares représentations de la France dans cette région, l'île occupe une position unique, tant sur le plan géopolitique que sur le plan économique. Cependant, cette position privilégiée l'expose également à des menaces cybernétiques croissantes.

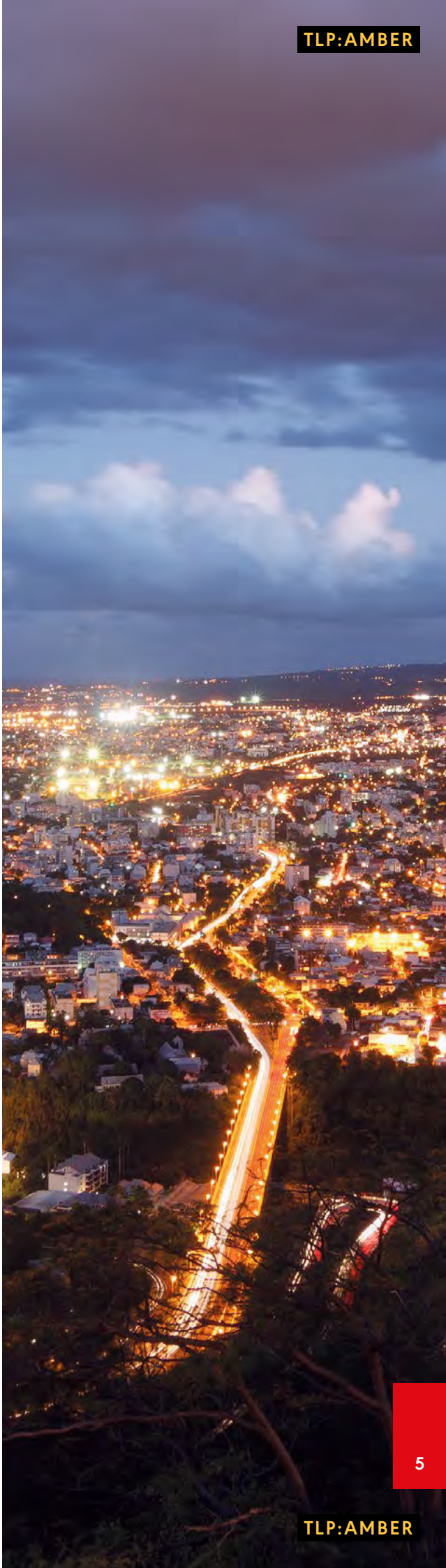
Dans ce contexte, le présent rapport zonal, fruit d'une collaboration entre CYBER RÉUNION et la société OWN, vise à fournir une analyse approfondie des cybermenaces auxquelles l'île est confrontée. Nous visons à accompagner les entreprises réunionnaises et les acteurs publics de notre territoire en leur fournissant, grâce à ce rapport zonal, des informations précises, concrètes et directement exploitables pour renforcer leur résilience face à des attaques cyber de plus en plus sophistiquées.
L'accent est mis sur la nature polymorphe des menaces, allant des campagnes de phishing aux usurpations d'identité, en passant par les fuites de données sur le deep et dark web.

Ainsi, plusieurs niveaux d'analyse ont été menés afin d'obtenir une vision globale et cohérente. Le concept de rapport zonal a été abordé sous différents angles :

- D'une part en recherchant les menaces visant le territoire réunionnais, les îles françaises et francophones gravitant autour de La Réunion et l'Océan Indien. Ce dernier espace étant particulièrement étendu et soulevant de nombreux enjeux, des choix ont été réalisés afin d'identifier les seules menaces pouvant hypothétiquement viser les entités de La Réunion.
- D'autre part, l'île étant un département d'Outre-mer français, les menaces visant la France et les autres îles françaises ont également été prises en compte.

Ce rapport offre ainsi un éclairage sur l'écosystème cybercriminel et étatique qui cible spécifiquement La Réunion, mais aussi de manière plus large les territoires qui l'entourent, dans le but de permettre aux entreprises et aux institutions d'adopter des stratégies de protection adaptées au territoire.

À terme, CYBER RÉUNION ambitionne d'enrichir ce type de rapport grâce aux informations partagées par l'écosystème des offreurs de solutions et de prestations de cybersécurité. En déployant des outils dédiés pour faciliter la collecte et le partage d'indicateurs de compromission, CYBER RÉUNION vise à affiner les connaissances sur la menace et à produire des rapports toujours plus proches des réalités des entités réunionnaises, contribuant ainsi à une défense collective plus efficace face aux cyberattaques.



1.2 LA RÉUNION ET SON ÉCOSYSTÈME

PIB EN 2023

La Réunion : 21,7 milliards d'euros

Mayotte : ≃ 3,1 milliards d'euros

Maurice : ≃ 13,4 milliards d'euros

Madagascar : ≃ 15,6 milliards d'euros

La Réunion se distingue comme le territoire le plus riche de la région, ce qui accroît son attractivité pour les cybercriminels cherchant à exploiter ses ressources économiques et à cibler ses infrastructures numériques vulnérables.

La Réunion, île française au cœur de l'océan Indien, se distingue par son statut particulier de département et région d'outre-mer (DROM), qui lui confère un rôle stratégique dans cette région du monde. Elle fait partie d'un écosystème régional complexe, composé d'États insulaires comme les Comores, Maurice, les Seychelles, Madagascar, et de territoires voisins tels que Mayotte. Ce positionnement, à la croisée des routes commerciales, politiques et numériques, en fait un point d'ancrage essentiel pour la France et l'Union européenne dans l'océan Indien. En tant que territoire ultramarin, La Réunion partage de nombreuses similitudes avec les autres DROM-COM, que ce soit en termes de dépendance technologique ou de vulnérabilités face aux cybermenaces. Cependant, l'île se distingue par son niveau de connectivité avancé, avec des infrastructures numériques cruciales, comme des câbles sous-marins reliant l'Afrique, l'Asie et l'Europe.

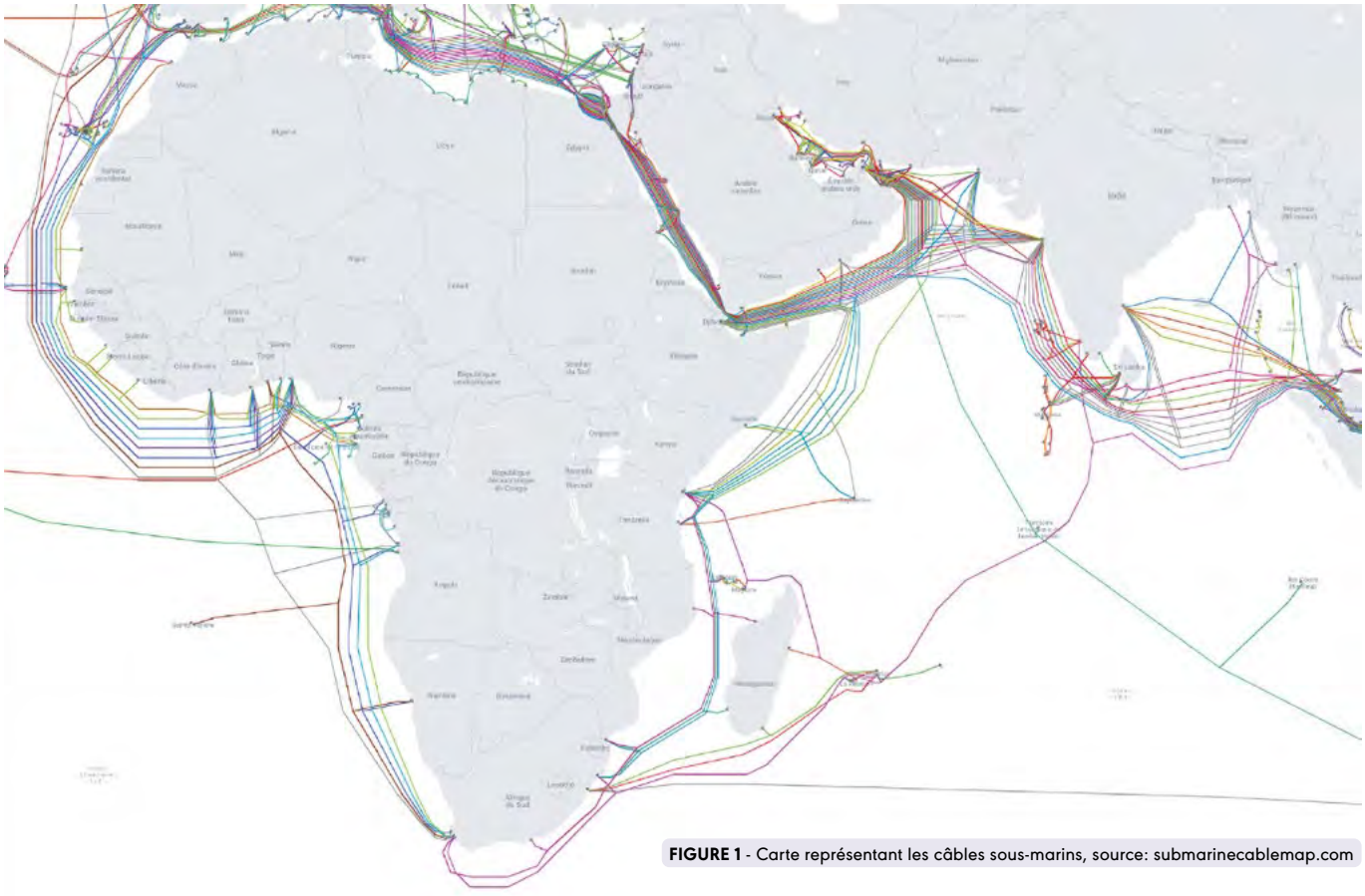
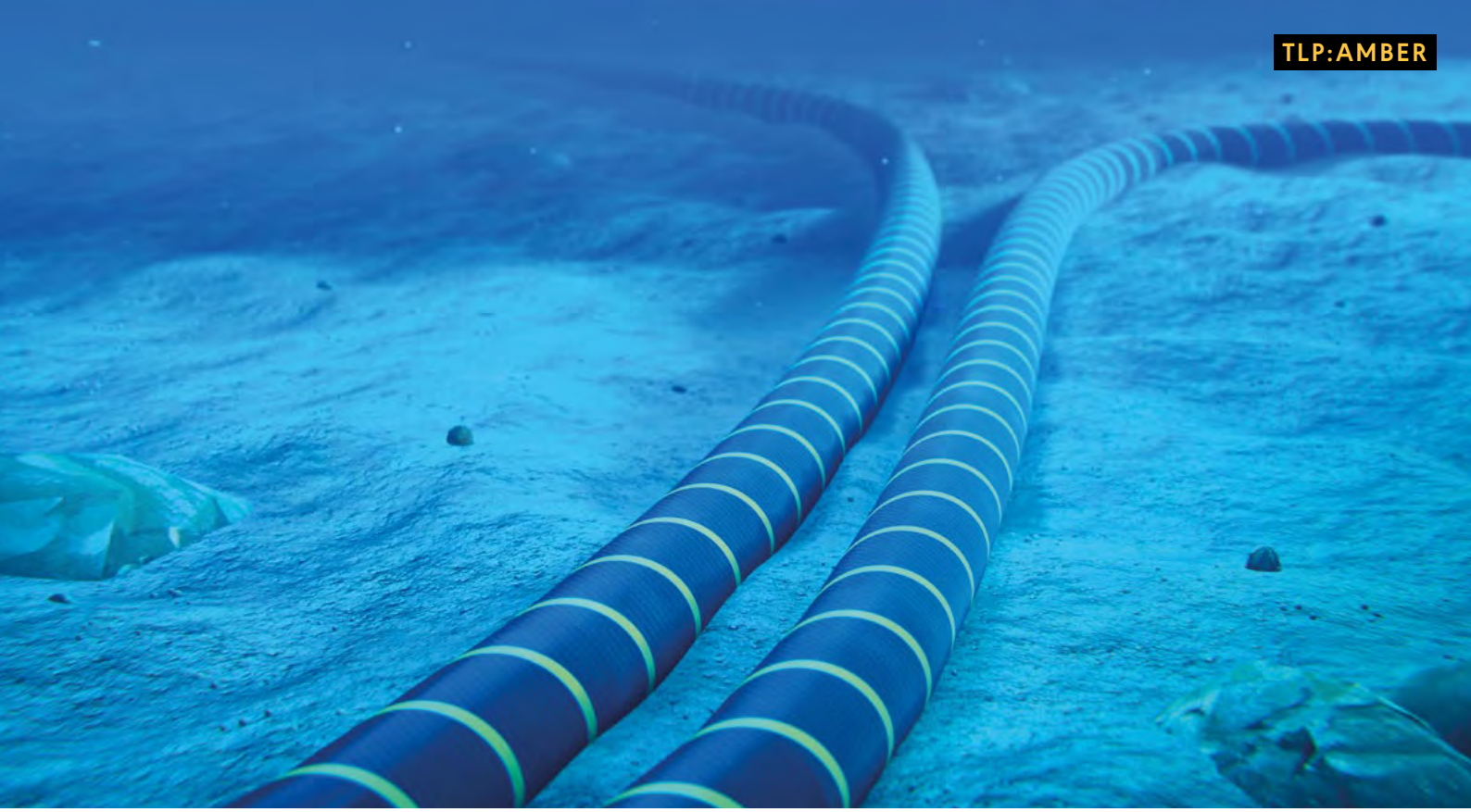


FIGURE 1 - Carte représentant les câbles sous-marins, source: submarinecablemap.com



Le territoire se situe à l'intersection des câbles LION (Lower Indian Ocean Network), METISS (MEltingpoT Indianoceanic Submarine System) et SAFE (South Africa Far East), qui permettent de relier notamment Madagascar, Maurice, l'Afrique du Sud, l'Inde et la Malaisie, renforçant ainsi les connexions régionales et internationales. Cependant, ces infrastructures sont vulnérables aux accidents, cyberattaques et tentatives d'espionnage. À titre d'exemple, plusieurs incidents observés en août 2023 et en janvier 2024 ont affecté les câbles sous-marins SAFE et LION, reliant La Réunion à d'autres territoires. Ces pannes ont notamment perturbé significativement les services Internet fixe et mobile d'opérateurs réunionnais, surtout dans les zones de Saint-Denis, Saint-Paul, Le Port et La Possession. Bien que ces incidents ne soient pas forcément malveillants, ils démontrent toutefois une certaine vulnérabilité du territoire face à d'éventuelles attaques ciblant ces infrastructures numériques.

En parallèle, le territoire peut être exposé à l'écoute des câbles, comme cela a pu être constaté à Maurice, par exemple. En 2022, le Premier ministre de l'île Maurice avait été mis en cause dans une affaire d'espionnage supposé sur les câbles reliant l'île à Internet, impliquant trois techniciens indiens.

Ce cas de « sniffing » n'est pas isolé. Récemment, dans le contexte des élections générales qui se sont tenues le 10 novembre 2024, la diffusion d'enregistrements téléphoniques privés sur les réseaux sociaux a de nouveau mis en lumière des accusations d'écoutes impliquant des personnalités politiques et judiciaires de l'île Maurice[1].

Dans la continuité des enjeux liés à la sécurité des câbles sous-marins, il est essentiel de comprendre l'importance stratégique du projet Umoji[2], annoncé par Google en mai 2024. Ce câble sous-marin reliera pour la première fois l'Afrique et l'Australie, consacrant encore plus l'océan Indien comme un pivot des échanges mondiaux de données. À l'image des anciennes routes de la soie, qui structuraient les échanges commerciaux et culturels entre continents, ces nouvelles routes numériques deviennent des artères vitales de l'économie mondiale, déterminant l'accès à l'information, au commerce digital et à la souveraineté technologique. Ce corridor stratégique illustre l'ambition de Google de sécuriser et contrôler des routes numériques critiques, tout en renforçant la connectivité et la résilience des infrastructures globales.

Ces interconnexions placent La Réunion au centre des enjeux cyber dans une zone où la sécurité numérique devient un enjeu majeur pour les gouvernements, les entreprises et les citoyens, d'autant plus dans un contexte géopolitique parfois instable.

1- https://www.zinfos974.com/enregistrements-telephoniques-divulgues-a-maurice-un-scandale-a-quelques-semaines-des-elections/

2- https://www.submarinenetworks.com/en/systems/africa-australia/umoja/google-to-build-umoja-subsea-cable-connecting-africa-with-australia

1.3 LES ENJEUX ET IMPACTS POTENTIELS

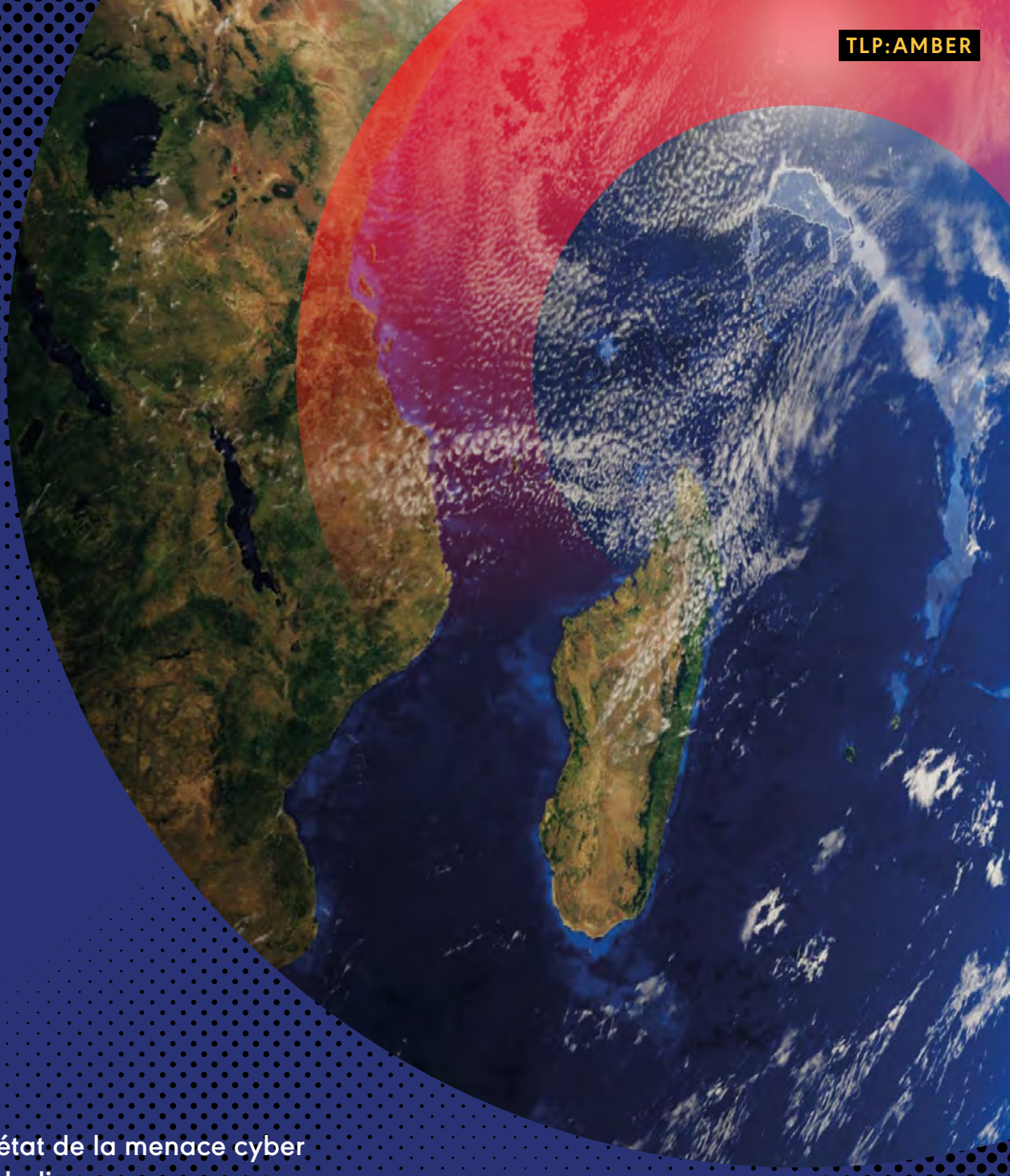
La Réunion fait face à des cybermenaces opportunistes croissantes, telles que le phishing, les ransomwares et d'autres attaques génériques. Ces menaces visent aussi bien les entreprises locales que les institutions publiques, souvent pour des gains financiers rapides. Le phishing et les ransomwares, par exemple, peuvent paralyser les systèmes, perturber les services essentiels et affecter gravement l'économie de l'île. En raison de sa connectivité internationale, La Réunion est exposée aux mêmes menaces que n'importe quel autre territoire connecté.

En parallèle, l'île a également été touchée par des actions de hacktivisme, comme lors de la campagne #FreeDurov, où des attaques ont visé des infrastructures locales pour protester contre l'arrestation de Pavel Durov, fondateur de Telegram, en France. Ces attaques, souvent idéologiques, créent des perturbations temporaires, notamment dans les services publics. La Réunion, en tant que territoire français, reste vulnérable à ces campagnes à portée mondiale, qui peuvent avoir des impacts locaux significatifs.

Enfin, sa position géostratégique dans l'océan Indien, combinée à son rôle de hub de communication numérique, soulève des enjeux cruciaux.

L'océan Indien, troisième plus grand espace maritime mondial après le Pacifique et l'Atlantique, constitue une plaque tournante essentielle entre l'Asie et l'Afrique, traversée par des points névralgiques tels que le détroit de Bab al-Mandeb. C'est un espace convoité non seulement pour la pêche intensive et la richesse de ses fonds marins en pétrole et gaz, mais aussi pour son intense trafic maritime, reliant les grandes économies mondiales via des routes commerciales stratégiques.

Dans ce contexte, La Réunion représente une extension de la présence française dans une région où les grandes puissances mondiales, notamment la Chine, l'Inde et les États-Unis, rivalisent pour étendre leur influence. Ces pays exercent un contrôle croissant sur cet espace maritime, matérialisé par des bases navales et militaires et des projets d'infrastructures majeurs comme les Routes de la Soie maritimes, financées par la Chine. Face à cette expansion chinoise, les États-Unis ont également renforcé leur présence militaire dans la région, tout comme la France via ses territoires ultramarins de La Réunion et Mayotte. Ces confrontations se traduisent également dans le cyberespace, où des acteurs étatiques mènent des opérations d'espionnage, de vol de données stratégiques et, parfois, de sabotage.



2

Rapport sur l'état de la menace cyber
dans l'Océan Indien

Chiffres clés et tendances

14 incidents
remontés par l'ANSSI en 2023 ciblant La Réunion, parmi lesquels les cyberattaques contre Colipays, Leal Reunion ou encore le Centre Hospitalier Universitaire (CHU).

2 activités hacktivistes
(NoName057 et Radnet64) ciblant spécifiquement La Réunion en 2024.

2 campagnes de phishing
identifiées ciblant spécifiquement La Réunion en 2024.

0 activité étatique ciblant spécifiquement La Réunion observée en 2024.

- **La menace cybercriminelle opportuniste – principalement générique – reste largement prédominante à La Réunion.** En 2024, les attaques informatiques à des fins d'extorsion se sont maintenues à un niveau élevé. L'écosystème cybercriminel ne cesse de se diversifier, notamment avec la diffusion de codes source de rançongiciels en open source et la multiplication d'outils accessibles à des acteurs disposant de compétences techniques limitées.

- **Peu ciblée par des opérations étatiques...** Aucune activité étatique liée à l'espionnage ou au sabotage n'a été détectée par le OWN-CERT.

Toutefois, plusieurs modes opératoires d'attaques sont actifs dans la zone Asie-Pacifique, à laquelle appartient La Réunion. C'est le cas de groupes affiliés à la Chine, tels que Volt Typhoon ou Earth Baxi.

- **Les techniques d'intrusion des attaquants...** Parmi les Tactiques, Techniques et Procédures (TTPs) les plus observées, le phishing (T1566) demeure le principal vecteur d'attaques, utilisé par tous types d'attaquants, qu'ils soient sophistiqués ou non. L'exploitation de vulnérabilités (T1190) constitue également un moyen d'intrusion initial couramment employé, non seulement contre les entreprises, mais aussi à travers l'ensemble de la chaîne d'approvisionnement.

L'île de La Réunion est visée en raison de...

...sa nationalité française

...son activité et de ses liens avec d'autres entités (plus importantes, en tant que fournisseurs...)

ÎLE DE LA RÉUNION

...fuites de données exploitées de manière opportuniste, issues d'incidents antérieurs où des informations sensibles ont été divulguées sur des forums ou des places de marché du dark web

...Sa situation géographique

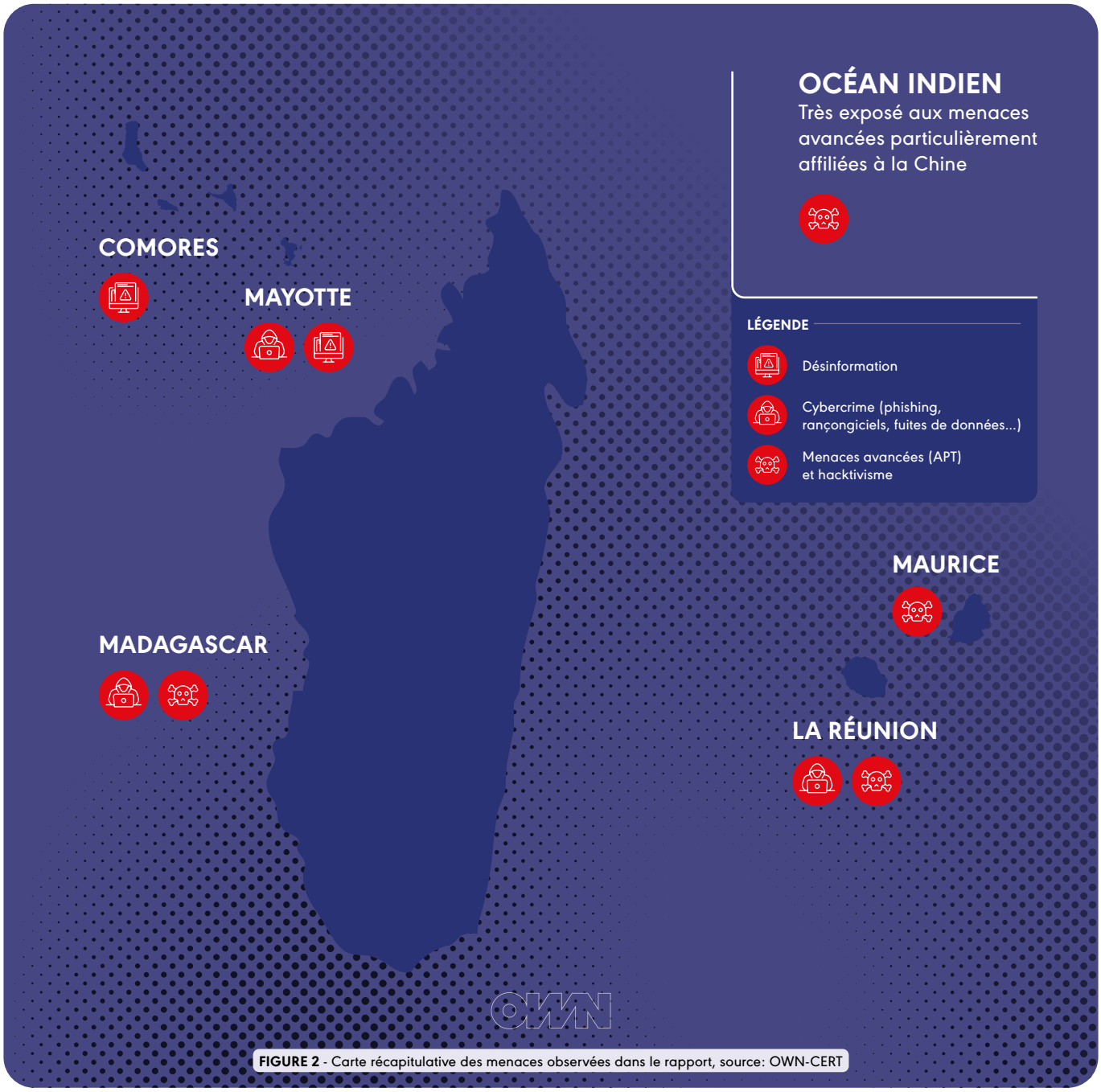


FIGURE 2 - Carte récapitulative des menaces observées dans le rapport, source: OWN-CERT

3

Rapport sur l'état de la menace cyber
dans l'Océan Indien

Évaluation des risques cyber à La Réunion

Une évaluation des risques est réalisée en fonction des menaces susceptibles d'impacter les entités implantées sur l'île de La Réunion. Le niveau d'impact et la probabilité sont ainsi évalués pour attribuer un score de risque en fonction du type de menace.

Cette première matrice se concentre sur une menace zonale identifiée à partir de sources ouvertes.

Elle a pour objectif d'aider les entreprises de La Réunion à se positionner face aux menaces susceptibles d'impacter leur activité. Cette matrice a vocation à être précisée et affinée au fil des rapports, grâce au partage d'observations sur les incidents cyber auxquels les entités de l'île sont confrontées.

FIGURE 3 - Matrice d'évaluation des risques, source : OWN-CERT

Cybercrime

La menace cybercriminelle a été évaluée comme un **risque critique** pour La Réunion, car les entreprises sont exposées non seulement aux fuites de données via des courtiers d'accès initial (Initial Access Brokers - IAB), mais également aux campagnes de phishing et aux attaques par rançongiciels.

Hacktivisme

L'hacktivisme a été évalué comme un **risque sérieux** pour La Réunion, plusieurs attaques ayant ciblé le territoire en réaction aux positions prises par la France. Outre le contexte géopolitique tendu entre la Russie et l'Ukraine, ainsi qu'entre Israël et le Hamas, l'arrestation du fondateur de Telegram, Pavel Durov, survenue en France le 24 août 2024, a été largement exploitée par différents groupes hacktivistes pour justifier certaines de leurs attaques.

Activités étatiques

La menace d'origine étatique a été évaluée comme un risque mineur pour La Réunion. Bien que le territoire occupe une place stratégique, celle-ci doit être relativisée par rapport à d'autres territoires de la zone Asie-Pacifique, qui se trouvent davantage au cœur des tensions.

Désinformation

Aucune campagne de manipulation de l'information visant spécifiquement La Réunion n'a, pour le moment, été identifiée par le OWN-CERT. Toutefois, les événements en cours dans différents territoires ultramarins, tels que Mayotte ou la Martinique, ainsi que les récentes manifestations sur les prix, ont été récupérés et amplifiés, notamment par des groupes affiliés à l'Azerbaïdjan.

4

Rapport sur l'état de la menace cyber
dans l'Océan Indien

Recommandations

Les recommandations suivantes sont formulées en tenant compte des menaces identifiées dans ce rapport. Des priorités ont été établies afin d'aider les organisations à hiérarchiser les actions à mettre en œuvre.

1 Établissement et maintien d'une veille proactive sur les vulnérabilités

P1 Établissement et maintien d'une veille proactive sur les vulnérabilités affectant les équipements utilisés au sein de l'organisation, afin de déployer les correctifs nécessaires en temps opportun, avant qu'elles ne soient exploitées par des acteurs malveillants.

2 Veille sur les menaces

P1 Mise en place d'une veille minimale sur les menaces spécifiques ciblant le secteur d'activité de l'organisation.

3 Surveillance du trafic réseau

P1 En s'appuyant sur la veille des menaces, surveiller ou bloquer les nouvelles connexions vers des infrastructures identifiées comme malveillantes ou suspectes (associées à des campagnes d'hameçonnage, etc.) ciblant le secteur d'activité de l'organisation.

4 Surveillance des journaux d'application

P1 Surveiller les journaux, messages et artefacts des applications nécessitant une intervention utilisateur pour leur exécution.

5 Mise à jour des solutions et outils

P1 Recenser les solutions logicielles utilisées et activer l'application automatique des correctifs de sécurité, notamment les mises à jour Microsoft publiées lors du «Patch Tuesday» mensuel.

6 Protection contre les attaques DDoS

P2 Déployer des pare-feux applicatifs et des répartiteurs de charge, utiliser des CDN (Content Delivery Networks) pour distribuer les ressources et améliorer la résilience face aux attaques DDoS en répartissant le trafic entre plusieurs serveurs, et garantir que les fournisseurs de services disposent des capacités nécessaires pour gérer ces attaques.

7 Hameçonnage exploitant des événements

P2 Sensibiliser vos utilisateurs aux techniques d'ingénierie sociale basées sur des événements, telles que les fausses offres commerciales ou les courriels frauduleux invitant à s'inscrire ou participer à un événement.

5

Rapport sur l'état de la menace cyber
dans l'Océan Indien

Rapport détaillé

5.1 MENACES CYBERCRIMINELLES OPPORTUNISTES

Les attaques informatiques à des fins d'extorsion demeurent les principales menaces à surveiller pour un territoire comme La Réunion. Elles s'appuient sur l'exploitation de vulnérabilités courantes, le phishing, l'utilisation d'infostealers et le déploiement de rançongiciels. Cette tendance est renforcée par la publication en source ouverte de codes de rançongiciels ainsi que par la démocratisation d'outils accessibles à des acteurs disposant de compétences techniques limitées.

5.1.1 INFOSTEALERS ET RAT

Les infostealers sont des logiciels malveillants conçus pour voler des données de connexion sur des machines infectées. Inspirés des fonctionnalités classiques des enregistreurs de frappe clavier (keyloggers) utilisés par des malwares bancaires tels que ZeuS ou SpyEye, initialement ciblant les identifiants des sites de banque en ligne, ces logiciels élargissent désormais leur champ d'action.

Les infostealers actuels capturent tous types d'identifiants présents sur une machine compromise :

- **Identifiants locaux** comme le nom d'utilisateur et le mot de passe du compte Windows des utilisateurs.
- **Identifiants de connexion à des services Internet** comme les webmail, les réseaux sociaux, les sites de commerce en ligne, les autres services numériques nécessitant une identification.
- **Identifiants présents dans la mémoire vive** de la machine.
- **Cookies, jetons de connexion** des navigateurs Internet.

Dans ce dernier cas (vol de cookies ou de token), la donnée volée peut permettre à un attaquant de contourner une authentification forte si la durée de validité de cette donnée est trop longue.

Une fois détectées par le malware, ces données sont collectées et exfiltrées vers un serveur de commande et de contrôle (C2) sous le contrôle de l'opérateur du malware. Elles peuvent ensuite être directement exploitées par ce dernier ou, plus fréquemment, mises en vente sur des places de marché cybercriminelles, comme en témoignent les annonces suivantes :

FIGURE 4 - Exemple d'offre de vente de données de connexion volées

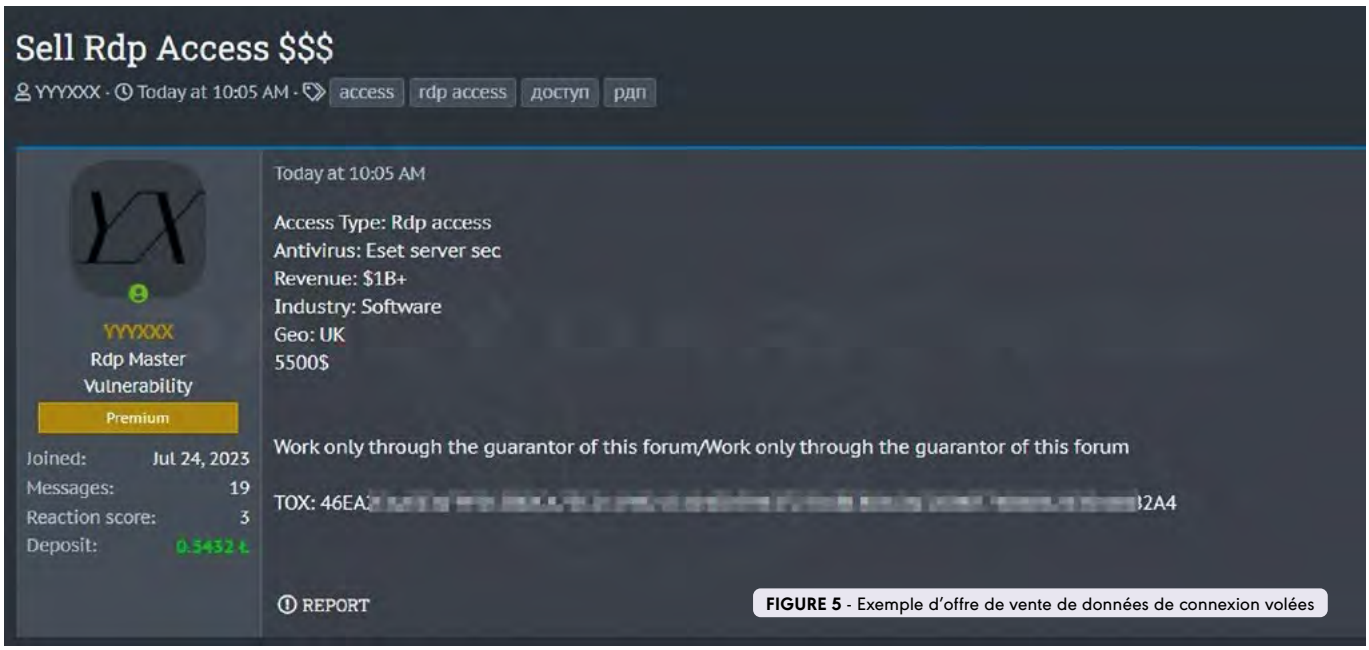


FIGURE 5 - Exemple d'offre de vente de données de connexion volées

Les infostealers, comme d'autres types de malwares, se propagent principalement via des pièces jointes dans des courriels, des liens malveillants, des téléchargements depuis des sites web compromis ou des logiciels piratés.

Leur sophistication a considérablement augmenté ces derniers mois, avec l'adoption de techniques d'évasion pour contourner les logiciels de sécurité et un recours accru à l'ingénierie sociale pour tromper les utilisateurs et les inciter à divulguer des informations sensibles.

Parallèlement, le nombre de familles d'infostealers distinctes a également grimpé, reflétant leur popularité et leur rentabilité au sein de la communauté cybercriminelle. Parmi les infostealers les plus actifs à ce jour, tous secteurs confondus, figurent notamment **Redline**, **Lumma** et **Raccoon**, qui jouent un rôle central dans le paysage des menaces liées à ces malwares.

DISTRIBUTION DE L'INFOSTEALER REDLINE

RedLine est un infostealer diffusé sous forme de jeux, d'applications ou de services piratés. Ce logiciel malveillant vole des informations sensibles issues de navigateurs web, de portefeuilles de crypto-monnaies et d'applications telles que FileZilla, Discord, Steam, Telegram ou encore des clients VPN. Il collecte également des données système sur la machine infectée, notamment les processus en cours, les logiciels antivirus installés, la version du système d'exploitation et l'architecture du processeur. Les données extraites sont converties en format XML et exfiltrées vers un serveur de commande et de contrôle (C2) à l'aide de messages SOAP.

FIGURE 6 - Capture d'écran du logo du stealer Redline, source : OWN-CERT

RedLine est commercialisé pour un prix compris entre 100 et 150 dollars américains ou proposé en mode SaaS pour 100 dollars par mois.
Une recherche sur la plateforme VirusTotal révèle que plus de 3 200 échantillons distincts de cette famille ont été soumis pour la première fois par des adresses IP françaises, dont 11 par des IP situées à La Réunion, depuis le 1er janvier 2023. Ces chiffres illustrent la large diffusion de ce malware.

5.1.2 INITIAL ACCESS BROKERS ET FUITES DE DONNÉES

Les acteurs de la menace ont besoin d'un accès à distance aux réseaux compromis pour réaliser leurs attaques, telles que le déploiement de logiciels malveillants, l'exfiltration de données ou les campagnes d'espionnage.

Ces accès compromis, souvent mis en vente sur le dark web ou divers forums cybercriminels, sont fournis par les Initial Access Brokers (IABs), qui jouent un rôle de plus en plus central dans l'écosystème cybercriminel. Leurs services sont majoritairement vendus à d'autres cybercriminels, qui exploitent ces accès ultérieurement pour compromettre les réseaux des victimes à des fins lucratives.

FIGURE 7 - Courtiers d'accès initiaux les plus observés sur la période 2024, source : OWN-CERT

En 2024, les acteurs les plus actifs dans la vente d'accès non autorisés à des entreprises françaises opèrent sous des pseudonymes tels que « mont4na », « TR4PSTAR », « IntelBroker » ou encore « Katy West ». Des recherches approfondies menées par le OWN-CERT révèlent qu'une partie importante des activités de « mont4na » se concentre sur Breach Forums, où il est actuellement connu sous le pseudonyme « threatbear ».

Il a également été identifié comme opérant sous le pseudonyme « al1ne3737 » et faisant partie d'un groupe baptisé « Pryzraky ».

À ce stade, aucun lien supplémentaire n'a pu être établi par nos équipes. Cependant, le nombre élevé de pseudonymes utilisés par « mont4na » suggère qu'il pourrait s'agir d'un groupe d'individus plutôt que d'un acteur isolé.

Forums	Pseudos utilisés	Origine de l'acteur
XSS Forum	**Forb1dden** –Telegram	Probablement brésilien
Breached	**mr** – Telegram	
BreachForums	**mont4na** –Breached, Raid	
RaidForums	Forums	
Telegram	**pumpedkicks** – Raid Forums	
Twitter	XSS	
Github	**threatbear** – BreachForums (currently active **0x3a0** – XSS **al1ne3737** - Github	

FIGURE 8 - Tableau d'informations relatives à l'acteur Mont4na, source : OWN-CERT

Les sources internes du OWN-CERT ont révélé qu'un acteur malveillant utilisant les pseudonymes « fooble », « Arken66612 », « John », « Johny », « Johnwick133 » et « Rezdy » a mis aux enchères 115 identifiants d'accès compromis à des réseaux d'entreprises le 29 septembre 2021. Parmi ces accès figuraient notamment des identifiants permettant d'accéder au réseau d'un établissement de santé public de La Réunion.

Il est probable que ces accès aient été réutilisés dans l'attaque qui a visé cet établissement en février 2023[3].

Pour rappel, cette cyberattaque avait été détectée à temps, ce qui avait permis à cet hôpital de prendre des mesures appropriées pour protéger la continuité des opérations, les données et les systèmes informatiques.

Par ailleurs, plusieurs fuites de données concernant des entreprises réunionnaises ont été signalées sur des forums comme Breach Forums ou LeakBase. Le 29 janvier 2023, les bases de données des entreprises réunionnaises de revente de produits informatiques et de téléphonie mobile d'occasion ont été publiées en ligne. Ces bases contenaient des informations sensibles, notamment les prénoms et noms de famille des utilisateurs, leurs adresses e-mail, mots de passe, dates de naissance et clés de sécurité.

```
[redacted]@prestashop.com,6456bd69c58dbf58db35b99c609c64de,1970-01-
15,66e3fbabe976709a3f4b102007fcf0b8,
[redacted]@yahoo.com,fe3ca5ca772662f7ccffe4e7cf01a11b,0000-00-
00,f35f09e37c4d55b9fb8515c9d4b78911,
[redacted]@hotmail.com,3fbbb08d9cf355f23ddfe74da989818f,0000-00-
00,2bbdb8c1b8fdc18fd15e2ef7d3838232,
[redacted]@gmail.com,a41fc45d2e03bd430ece6c95e9cda263,1996-05-
14,169b71aa4ef730ff28ae9e411ebf6ea1,
[redacted]@hotmail.com,df67eea39c6464b3c6971d90b4308bb6,1969-01-
17,d86fe6e00875192598c0db1e8da38a27,
[redacted]@gmail.com,c96f2c5462354fde64e88d884a574166,0000-00-
00,f61a30a4066a840320ec18d44315c2b1,
```

FIGURE 9 - Tableau d'informations relatives à l'acteur Mont4na, source : OWN-CERT

3- https://cert.europa.eu/publications/threat-intelligence/cb23-03/

5.1.3 RANÇONGICIELS

Depuis le 1er janvier 2024, le OWN-CERT a recensé 79 attaques par rançongiciel ciblant le territoire français, touchant principalement les secteurs du manufacturing (25 %), de la construction (16 %), de l'éducation (10 %), du commerce de détail (10 %) et de la santé (7 %).

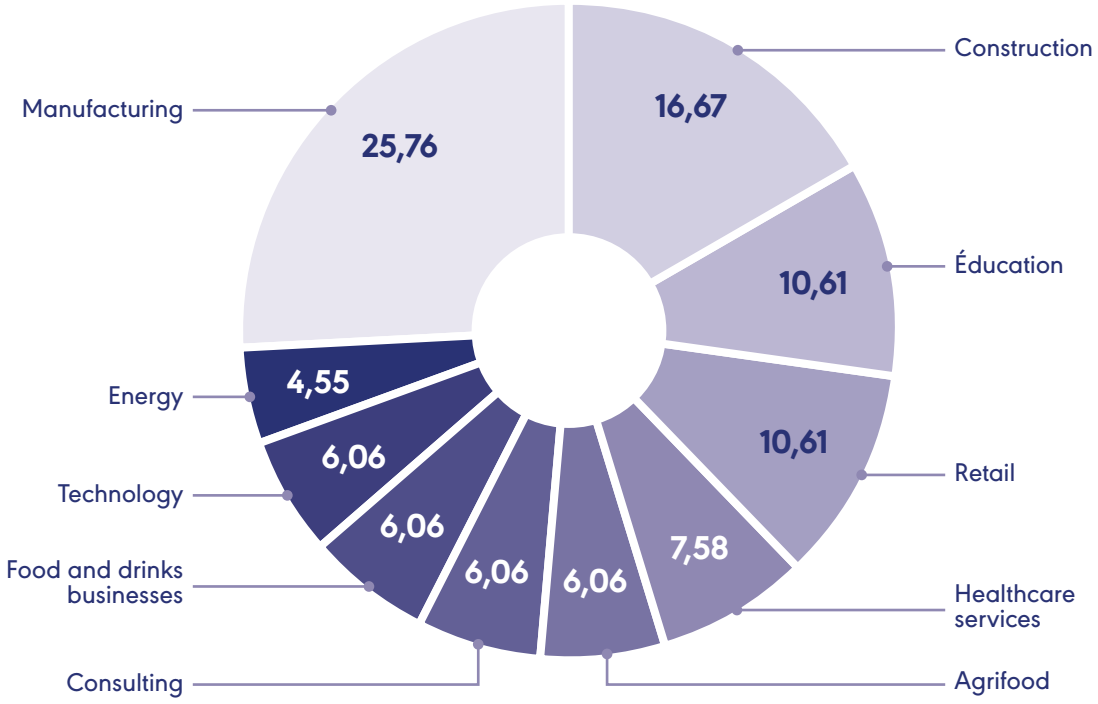


FIGURE 10 - Répartition des attaques par secteur, source : OWN-CERT

En 2024, Lockbit3 s'est imposé comme l'opérateur de rançongiciels ayant le plus ciblé la France, suivi des groupes 8base et Ransomhub. La prédominance de Lockbit3 n'est pas surprenante, étant l'un des acteurs les plus actifs dans le domaine des rançongiciels depuis plusieurs années. À titre d'exemple, le 26 juillet 2022, ce groupe avait revendiqué la compromission d'une collectivité territoriale à laquelle les 17 communes de Mayotte ont délégué leurs compétences eau et assainissement.

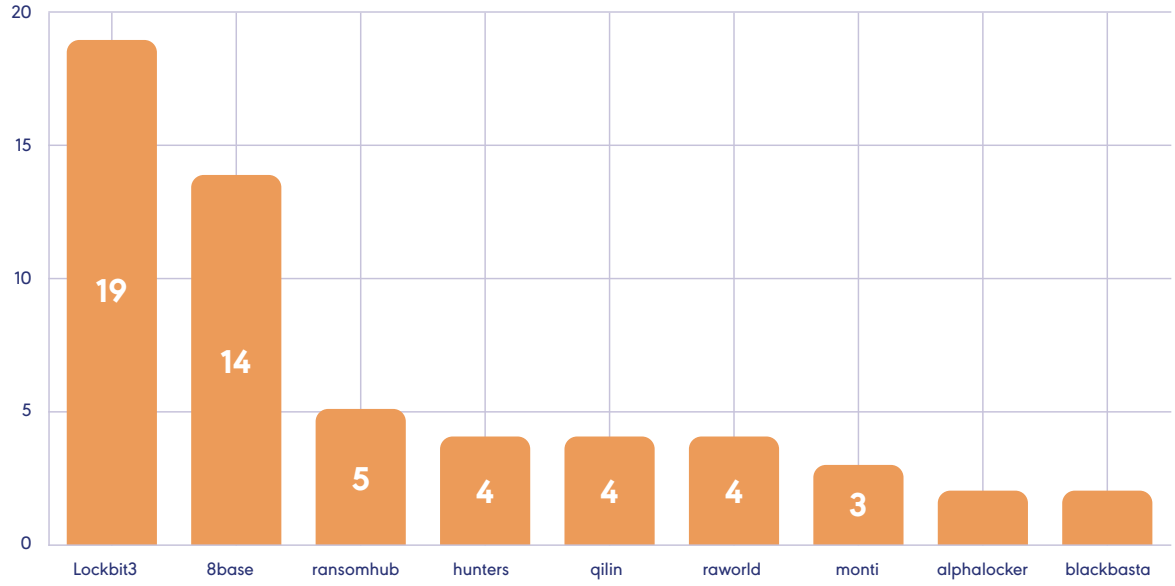


FIGURE 11 - Classement des opérateurs de rançongiciels les plus actifs, source : OWN-CERT

En 2024, plusieurs attaques par rançongiciels ont ciblé des départements d'Outre-mer. Par exemple, le 21 août 2024[4], des attaques par rançongiciels ont frappé une chaîne de télévision réunionnaise et plusieurs radios privées de l'île.

Ces cyberattaques ont paralysé les systèmes de diffusion de cette chaîne de télévision et de stations radios locales.

Les radios ont été incapables d'émettre en début de matinée, et des perturbations significatives ont également été constatées sur cette chaîne de télévision.

DONNÉES FUITÉES APPARTENANT À ANTENNE RÉUNION

Le OWN-CERT a identifié une fuite de données massive concernant Antenne Réunion Radio, impliquant une archive de 146 Go contenant des informations sensibles. Parmi les données compromises figurent des copies de cartes d'identité, des documents de facturation et des fichiers relatifs à la taxe d'habitation.

L'attaque a été revendiquée sur le blog du groupe de rançongiciels Sarcoma, qui serait affilié à l'acteur connu sous les pseudonymes « Katy West » ou « Mont4na », déjà documenté précédemment (p.17).

Le 24 octobre 2024, les données fuitées étaient encore accessibles sur le dark web sur le site du groupe de rançongiciel Sarcoma.

4- https://www.linfo.re/la-reunion/faits-divers/antenne-reunion-les-cyber-hackers-reclament-une-rancon?utm_medium=Social&utm_source=Facebook

Le 13 novembre 2024, une collectivité territoriale majeure du territoire a subi une cyberattaque qui a perturbé ses services informatiques. L'attaque a été revendiquée par le groupe Termite.

LE RANÇONGICIEL TERMITE

Apparu en novembre 2024, Termite est un opérateur de rançongiciels spécialisé dans la double extorsion.

Après avoir chiffré les fichiers de ses victimes, il menace de divulguer les données volées via un site dédié sur le dark web, où il mène également ses négociations. Le rançongiciel utilise un chiffrement robuste basé sur l'algorithme Curve25519 et applique l'extension « .termite » aux fichiers chiffrés.

En complément du chiffrement, Termite laisse une note de rançon, généralement intitulée « How To Restore Your Files.txt », sur les systèmes compromis. Cette note contient un lien vers un site sécurisé de fuite de données, des adresses e-mail ProtonMail pour la communication, ainsi qu'un token unique permettant à la victime de négocier et d'effectuer le paiement.

Le OWN-CERT a relevé des similitudes dans le code source de Termite et de Babuk, suggérant que Termite pourrait utiliser ou adapter des éléments du code de Babuk pour ses opérations.

Contrairement à de nombreux autres rançongiciels, Termite semble fonctionner de manière autonome et n'adopte pas le modèle Ransomware-as-a-Service (RaaS). Il n'y a aucune preuve de collaboration avec d'autres groupes ou cybercriminels, et aucune campagne de recrutement explicite n'a été observée sur les forums du dark web. Cela indique que le groupe agit de manière indépendante et opère avec une discrétion remarquable dans la gestion de ses activités.

Depuis son apparition, Termite a mené des attaques dans plusieurs pays, dont la France, l'Allemagne, Oman et les États-Unis.

Son activité se caractérise par une répartition géographique variée, ciblant principalement les secteurs de l'éducation, de l'énergie, des administrations publiques, de la santé et de l'industrie.

5.1.4 TENTATIVES DE FRAUDE ET PHISHING

Depuis plusieurs années, des fraudeurs ciblent les particuliers avec des e-mails et SMS frauduleux visant à voler leurs données personnelles et bancaires, avant de les entraîner dans des escroqueries téléphoniques. Ces arnaques incitent les victimes à effectuer des virements vers des comptes bancaires contrôlés par les malfaiteurs. Chaque année, des milliers de noms de domaines et sites web sont créés pour alimenter un nombre limité de scénarios d'ingénierie sociale, bien rodés, tels que :

- Paiement d'une amende pour infraction routière ;
- Mise à jour d'une carte vitale proche de l'expiration ;
- Réception d'un colis avec paiement de frais de douane ;
- Régularisation liée à la vignette Crit'Air ;
- Achat de cartes de transport à prix réduit ;
- Paiement de factures pour des services essentiels (électricité, internet, etc).

Le OWN-CERT a également constaté que certains des noms de domaines créés pour ces fraudes incluent des références à des territoires ultramarins tels que La Réunion et la Guyane, bien que cela représente une faible proportion.

Par exemple :

- **la-poste-suivi-reunion.info**
- **douane-reunion-colis.info**
- **dedouanement-colis-reunion.com**
- **acheminement-colis-reunion.com**
- **reunion-antai-gouv.info**
- **antai-amende-reunion.info**
- **actualisation-la-reunion-ameli.info**
- **service-renouvellement-ameli-reunion.com**
- **ameli-gouv-reunion.com**
- **service-regularisation-la-reunion.info**
- **impot-reunion-gouv.com**
- **chronopost-fr-re.cfd**
- **dossierantai-enligne-re.com**
- **impost-fr-re.com**
- **guyane-douaneinfo.com**
- **guyane-douaneinfo.com**
- **suivichronopost-gf.com**
- **laposte-suivi-gf.com**

Bien que les données ne permettent pas de produire des statistiques scientifiquement valides, l'analyse d'un échantillon de 2 271 noms de domaines frauduleux liés à des thèmes classiques (ameli, antai, colis postal) a permis d'identifier 75 domaines mentionnant La Réunion et 4 domaines faisant référence à la Guyane, représentant respectivement 3,3 % et 0,2 % de l'échantillon.

Cependant, pour évaluer précisément la proportion d'attaques visant réellement l'île de La Réunion, il serait nécessaire d'analyser les noms de domaines associés à des messages envoyés vers des numéros de téléphone comportant l'indicatif local (+262).

Les dates de création de ces noms de domaines révèlent une vague continue d'attaques ciblant les particuliers réunionnais depuis décembre 2023.

Ciblage ultramarin des noms de domaines frauduleux en %

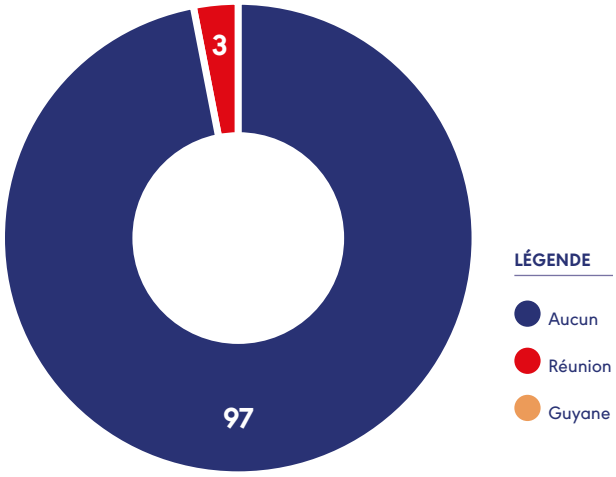


FIGURE 12 - Ciblage ultramarin des noms de domaines frauduleux, source : OWN-CERT

Enregistrement de domaines frauduleux ciblant La Réunion

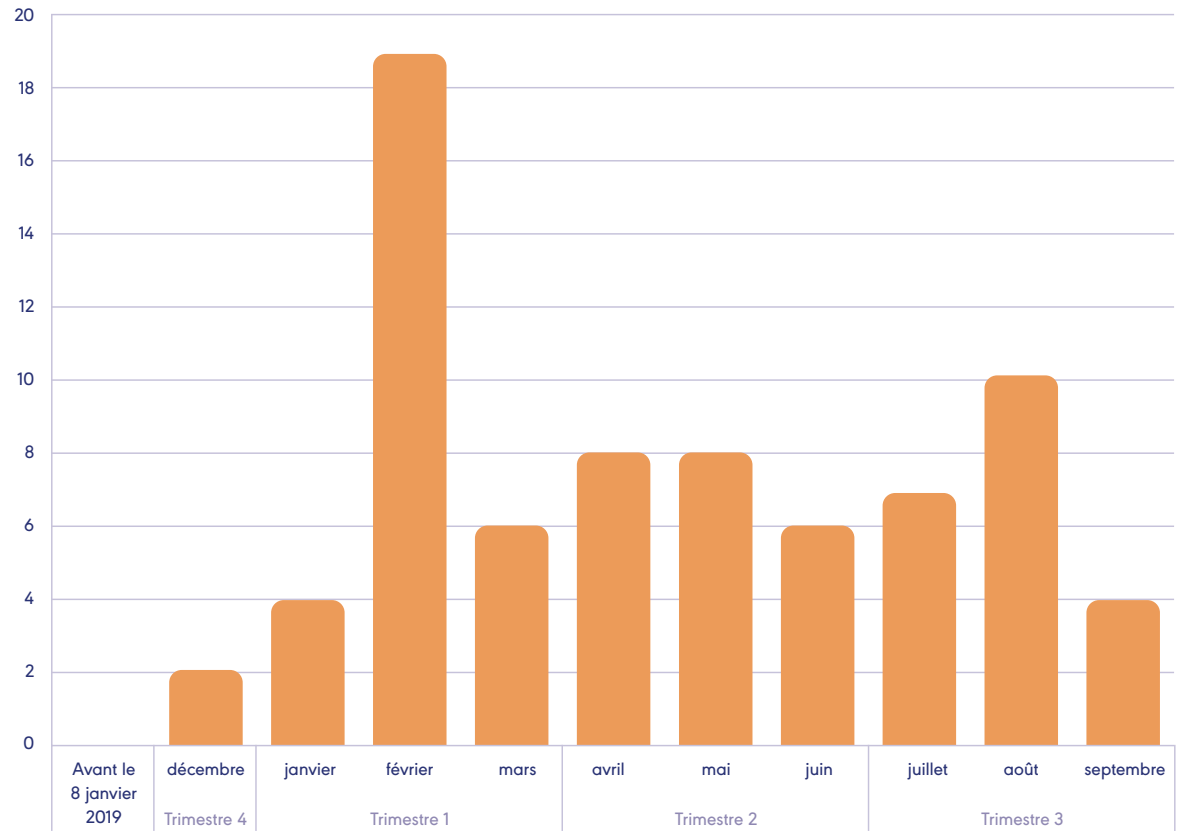


FIGURE 13 - Statistiques sur l'enregistrement de domaines frauduleux ciblant La Réunion, source : OWN-CERT

La majorité de ces noms de domaines (59 %) sont associés à des adresses IP relevant de l'AS 399979, un système autonome largement utilisé pour ce type de fraude à l'échelle internationale.

Phishing bancaire ciblant les territoires ultramarins

Nous avons également identifié une série d'attaques de phishing bancaires visant spécifiquement les clients réunionnais, antillais et guyanais d'une grande banque française. Ces attaques, survenues entre août 2022 et février 2023, s'appuyaient sur des noms de domaines créés à l'aide de services légitimes en cloud destinés aux développeurs :

- reunion-authentificat-domtom.firebaseapp.com
- reunion-la-departementale.firebaseapp.com
- xxxxx-reunion-2023.firebaseapp.com
- group-antilles-reunion.firebaseapp.com
- https-ile-reunion-dps2.firebaseapp.com
- antilles-guyanexxxxx.firebaseapp.com
- xxxxx-antilles-guyane.repl.co

FIGURE 14 - Capture d'écran de reunion-authentificat-domtom.firebaseapp.com, source : OWN-CERT

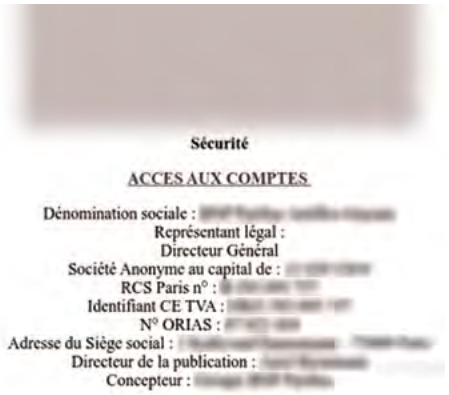


FIGURE 15 - Capture d'écran de antilles-guyanexxxxx.firebaseapp.com, source : OWN-CERT

Phishing ciblant les instances gouvernementales de La Réunion

Nous avons également identifié une tentative de vol d'identifiants d'authentification, probablement ciblant un service institutionnel d'une chambre consulaire à La Réunion, survenue en 2021.
Le nom de domaine xxxxx-revoir.com a été enregistré le 18 mai 2021. Une capture d'écran du site à cette date révélait une fausse page d'authentification imitant un compte Microsoft.

L'île de La Réunion n'est pas épargnée par les tentatives de fraude qui touchent également la France métropolitaine. Les cybercriminels déploient des moyens spécifiques pour cibler les particuliers réunionnais. Si ces attaques semblaient sporadiques par le passé, une vague continue de fraudes est observée depuis la fin de l'année 2023.

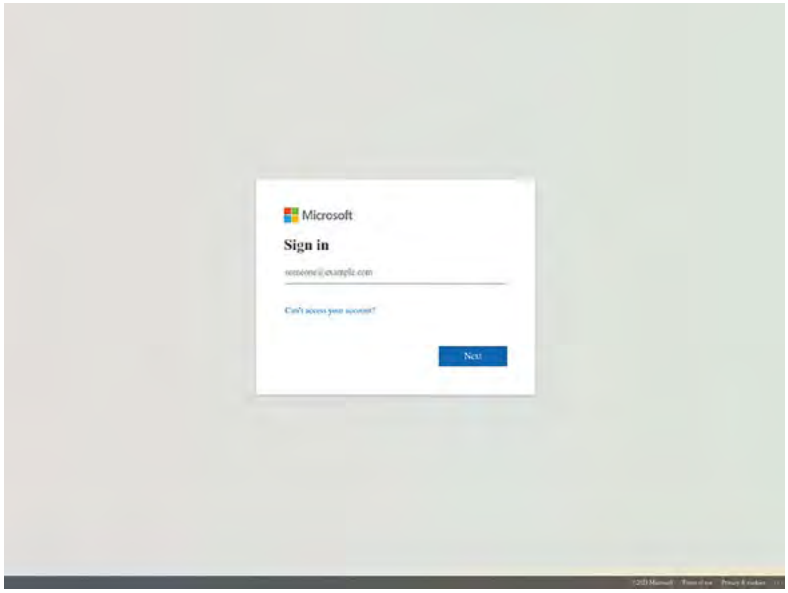


FIGURE 16 - Capture d'écran de antilles-guyanexxxxx.firebaseapp.com, source : OWN-CERT

5.2 MENACES HACKTIVISTES ET ÉTATIQUES

Cette section du rapport se focalise sur les menaces présentant des liens, directs ou indirects, avec des États. Contrairement aux cybercriminels, dont les objectifs sont principalement financiers, les menaces étatiques visent essentiellement l'espionnage et la déstabilisation. Parmi les acteurs les plus connus figurent les groupes utilisant des modes opératoires avancés (MOA) pour mener des opérations cyber répondant à des intérêts étatiques.

À ces menaces s'ajoutent les actions des hacktivistes et les tentatives de manipulation de l'information. Bien que les liens avec les États ne soient pas toujours clairement établis, ces acteurs opèrent souvent dans l'intérêt de leur pays d'origine, se positionnant comme des défenseurs de leurs valeurs.

5.2.1 HACKTIVISME

Dans un contexte géopolitique tendu, la France, incluant ses régions, collectivités et territoires d'Outre-mer, constitue une cible privilégiée pour des acteurs cherchant à renforcer l'impact de leurs positionnements politiques ou idéologiques.

Ces opérations de déstabilisation se manifestent généralement par des attaques DDoS, des défigurations de sites web, des divulgations de données ou des actes de sabotage.

Au cours des derniers mois, une recrudescence des attaques hacktivistes a été observée, notamment en lien avec les conflits russo-ukrainien et israélo-palestinien. Par exemple, le 2 septembre 2024, le groupe NoName057(16) a revendiqué sur son canal Telegram[5] - supprimé depuis - plusieurs attaques contre la France. Celles-ci faisaient suite à une réunion à la Maison Blanche impliquant des représentants français, allemands, anglais et ukrainiens, ainsi que le conseiller à la sécurité nationale du président américain, pour discuter du soutien à apporter à Kiev.

Dans cette vague d'attaques, une cible notable était le site « Reunion Traffic Information », qui fournit des informations en temps réel sur les conditions de circulation à La Réunion (trafic, incidents, fermetures de routes, etc.).

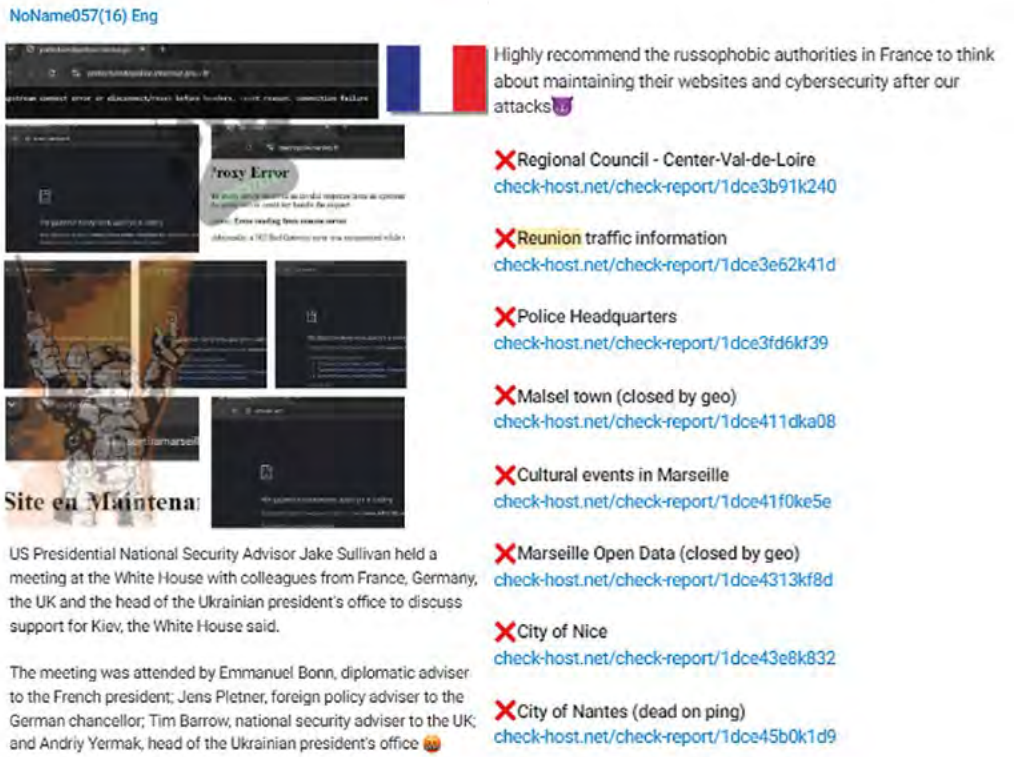


FIGURE 17 - Capture d'écran des messages de NoName057(16) revendiquant l'attaque sur un site de suivi du trafic routier à La Réunion le 02/09/2024, source : Telegram

5- @noname05716eng

Le groupe pro-russe avait déjà ciblé le site d'une collectivité territoriale majeure de Guadeloupe à trois reprises, les 4 février, 21 février et 11 mars 2024, en s'appuyant sur le même narratif «anti-Ukraine». De manière similaire, le 6 septembre 2024, le groupe a renouvelé ses attaques, cette fois contre les sites des services publics de Nouvelle-Calédonie, de Polynésie française et de Wallis-et-Futuna

FIGURE 18 - Capture d'écran des messages revendiquant des attaques sur plusieurs départements français d'outre-mer le 6/09/2024, source : Telegram

L'arrestation de Pavel Durov, fondateur et PDG de la plateforme Telegram, survenue le 24 août en France, a déclenché une vague de protestations parmi les groupes hacktivistes.

Cette mobilisation a donné naissance à une campagne intitulée #FreeDurov.

Rejointe par plusieurs groupes, dont CyberArmyRussia, CyberDragon, Cyberia, EvilWeb, RipperSec, SERVER KILLERS, UserSec et High Society, cette campagne vise à cibler des entités françaises en représailles à l'arrestation de Pavel Durov.

Initialement concentrées sur les institutions et entités gouvernementales, les cibles ont progressivement inclus d'autres secteurs tels que les transports, la logistique et la santé. Ainsi, le 27 août 2024 à 16h11, le groupe Radnet64 (pro-Palestine a annoncé sur son canal[6] avoir attaqué le site internet du principal aéroport de La Réunion. Selon les preuves fournies par le groupe, le site serait resté inaccessible pendant près de 40 minutes, et l'attaque aurait été réalisée en collaboration avec RipperSec dans le cadre de la campagne #FreeDurov.

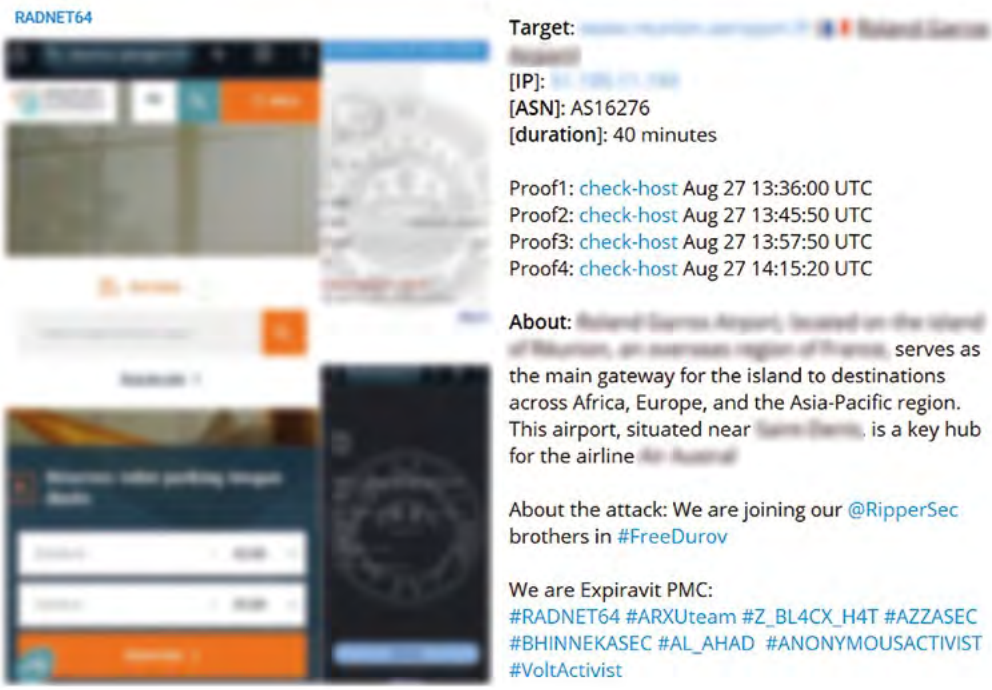


FIGURE 19 - Capture d'écran des messages du groupe RADNET64 revendiquant une attaque sur le principal aéroport réunionnais le 27/08/2024, source : Telegram

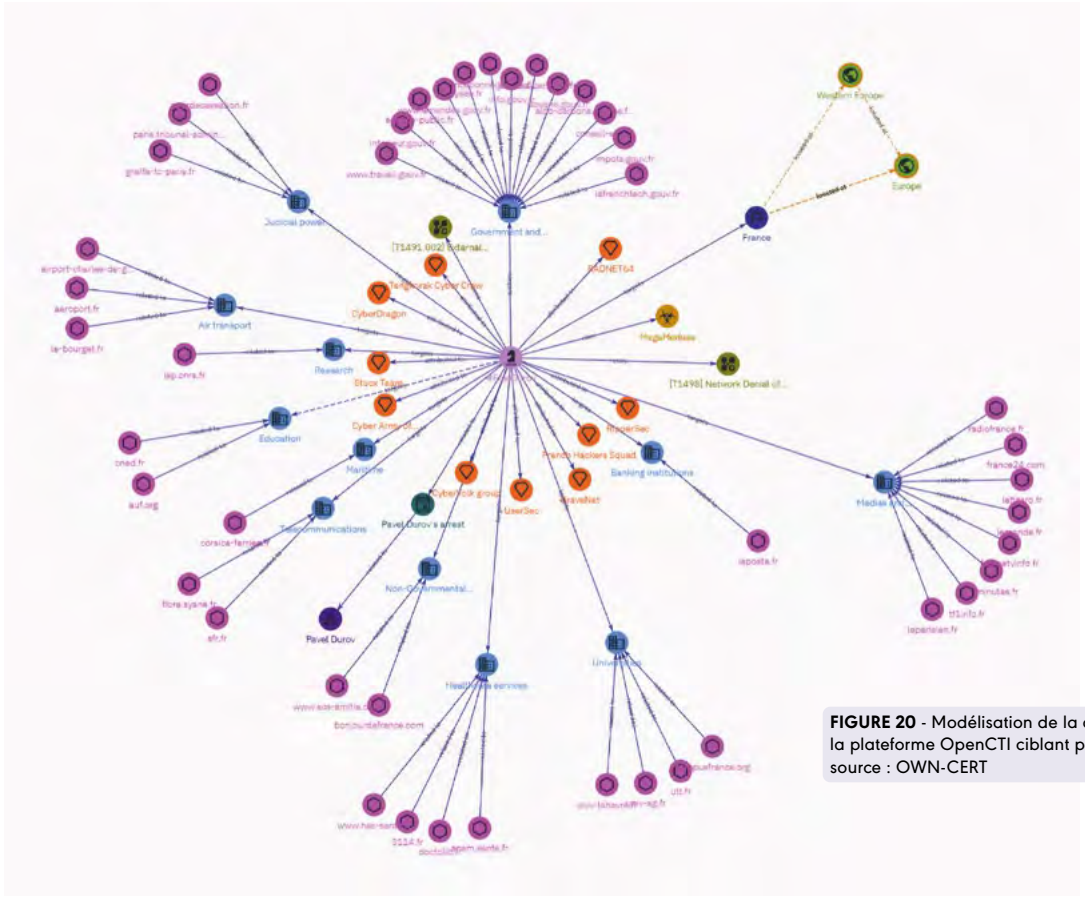


FIGURE 20 - Modélisation de la campagne #FreeDurov sur la plateforme OpenCTI ciblant plusieurs entités françaises, source : OWN-CERT

6- https://t.me/radnetbak

5.2.2 MENACES PERSISTANTES AVANCÉES

Aucune attaque spécifiquement dirigée contre des entités réunionnaises n'a été identifiée. Cependant, certaines attaques visant d'autres territoires français d'Outre-mer ont été documentées. Par exemple, en 2023, la Polynésie française aurait été ciblée par l'acteur Gallium[7][8], présumé lié à la Chine et réputé pour compromettre des fournisseurs de télécommunications. Gallium aurait exploité des vulnérabilités présentes sur des serveurs Microsoft Exchange et IIS, déployant le malware mim221, un malware de vol d'identifiants basé sur Mimikatz.

À partir de novembre 2023, le groupe Sharp Panda, également présumé lié à la Chine, a mené des attaques contre des organisations gouvernementales dans les Caraïbes[9]. Ce ciblage marque un changement significatif dans la stratégie de Sharp Panda, dont les attaques étaient jusqu'alors limitées à l'Asie du Sud. Toutefois, ce n'est pas une première pour des groupes affiliés à la Chine, comme en témoigne le groupe Ke3chang, qui avait déjà ciblé la région des Caraïbes[10].

L'intensification des attaques, souvent motivées par des objectifs d'espionnage, semble étroitement liée à l'essor des échanges commerciaux entre la Chine et les Caraïbes.

En 2023, le commerce entre la Chine et cette région aurait atteint 11,8 milliards USD, soit une multiplication par dix par rapport à 2003.

À la lumière des récentes rencontres politiques, notamment le Forum de la coopération sino-africaine tenu le 2 septembre à Pékin, il est probable que des activités similaires à celles observées dans les Caraïbes se développent également autour de La Réunion. Lors de ce forum, la Chine a réaffirmé son soutien aux Comores, notamment dans leurs revendications sur Mayotte.
Le président Xi Jinping a souligné son engagement à défendre les principes d'intégrité territoriale pour les deux pays, consolidant un partenariat mutuel : la Chine considère que Mayotte appartient aux Comores, tandis que les Comores reconnaissent Taïwan comme une partie intégrante de la Chine.

En outre, le président chinois s'est engagé à investir plus de 45 milliards d'euros sur trois ans pour soutenir le continent africain, dont 25 millions d'euros spécifiquement destinés à Madagascar[11].

De la même manière, plusieurs MOA tels que Volt Typhoon ou encore Earth Baxia ont été observés comme étant actif dans la zone Asie-Pacifique.

7- https://web-assets.esetstatic.com/wls/en/papers/threat-reports/eset-apt-activity-report-q2-2023-q3-2023.pdf
8- https://www.sentinelone.com/labs/operation-tainted-love-chinese-apts-target-telcos-in-new-attacks/
9- https://research.checkpoint.com/2024/sharp-dragon-expands-towards-africa-and-the-caribbean/
10- https://attack.mitre.org/groups/G0004/
11- https://la1ere.francetvinfo.fr/mayotte/madagascar-comores-tanzanie-la-chine-annonce-plus-de-45-milliards-d-euros-d-aide-pour-l-afrique-1520282.html

Le 19 septembre, Trend Micro a publié un rapport sur Earth Baxia[12], un acteur de menace probablement basé en Chine. Ce groupe a ciblé des organisations gouvernementales à Taïwan ainsi que dans d'autres pays de la région Asie-Pacifique (APAC), exploitant la vulnérabilité GeoServer CVE-2024-36401. Leur campagne s'appuyait sur des services cloud publics pour héberger des fichiers malveillants, visant spécifiquement les secteurs gouvernementaux, des télécommunications et de l'énergie dans la région APAC.

Le OWN-CERT a identifié 27 serveurs potentiellement vulnérables à l'île Maurice, notamment des infrastructures associées à des opérateurs télécom Mauriciens.

Dans un article publié le 16 octobre 2024, les chercheurs de « nao_sec » ont analysé les activités d'un nouveau groupe, nommé « IcePeony ». Ce groupe aurait ciblé des entités gouvernementales, des institutions académiques et des organisations politiques en Inde, au Vietnam et à Maurice[13]. Ce ciblage semble viser la collecte de renseignements stratégiques, probablement exploités dans le cadre de la stratégie maritime de la Chine.

L'acteur « IcePeony », actif depuis au moins 2023, aurait probablement ciblé Maurice en raison de son rapprochement stratégique avec l'Inde. En février 2024, le Premier ministre indien, Shri Narendra Modi, et son homologue mauricien, Pravind Kumar Jugnauth, ont inauguré plusieurs infrastructures clés, dont une nouvelle piste d'atterrissage, la jetée de Saint James, ainsi que six projets de développement communautaire sur l'île d'Agalega. Ces initiatives de coopération renforcée pourraient refléter une méfiance croissante de l'Inde face à l'expansion chinoise dans l'océan Indien.

Dans cette campagne, analysée par « nao_sec », le groupe utilise des attaques par injection SQL ciblant des serveurs web publics. Lorsqu'une vulnérabilité est identifiée, ils déploient un webshell ou un malware, tel que « IceCache » ou « IceEvent », pour voler des identifiants de connexion et recueillir des informations stratégiques.

Actualités susceptibles de représenter un intérêt pour des APT

Des analyses techniques et des fuites d'information ont révélé qu'en décembre 2021, l'État malgache a acquis une licence d'utilisation du logiciel d'espionnage Predator pour une durée de trois ans. Cette technologie n'aurait pas été achetée par les services de renseignement ou de police, mais directement par les services de la présidence.

FIGURE 21 - Serveurs exposés à la vulnérabilité CVE-2024-36401, source : OWN-CERT

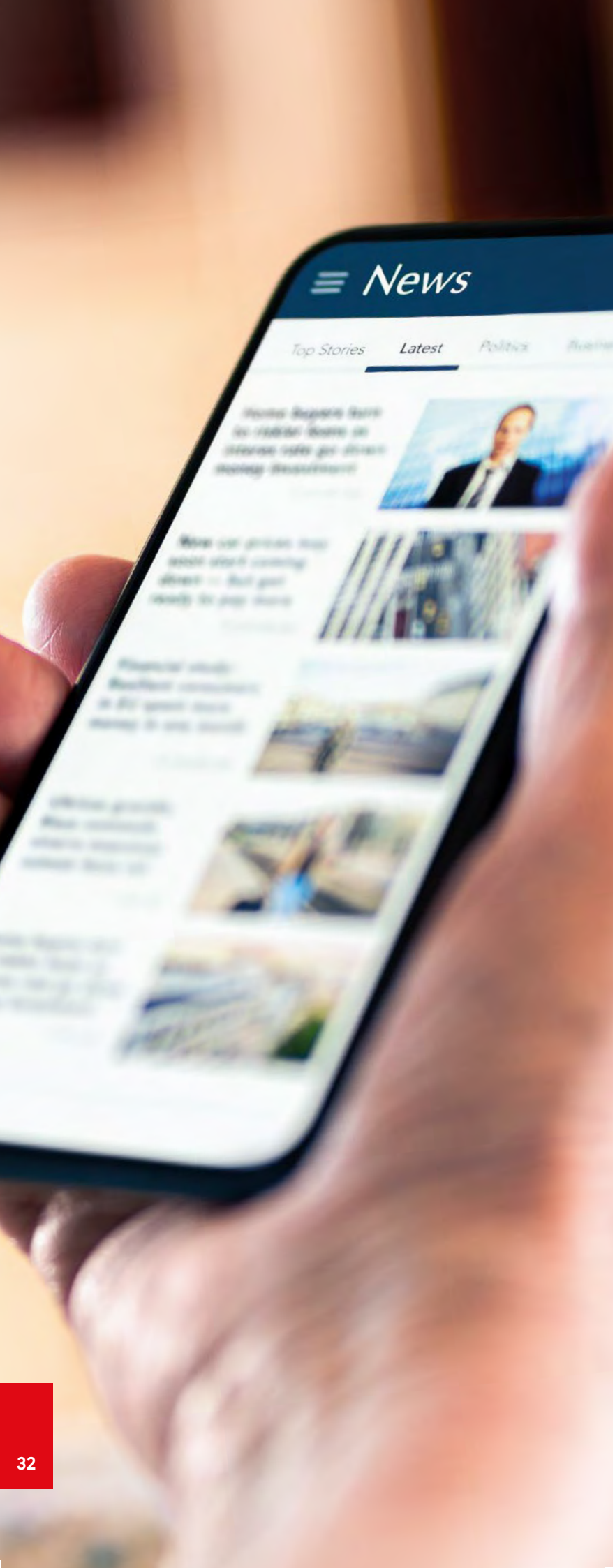
Predator, un logiciel développé par la société Intellexa, est conçu pour espionner et prendre le contrôle de smartphones. Il peut être déployé sur un appareil cible grâce à une infection dite « zero-clic », ne nécessitant aucune interaction de la part de la victime. Selon les révélations de Mediapart, un IMSI catcher serait requis pour effectuer cette infection zero-clic. D'autres méthodes existent également, comme la redirection du trafic web d'un téléphone cible vers une page contenant un code exploitant une chaîne de vulnérabilités 0-day4.

Selon Mediapart, le gouvernement malgache a utilisé Predator pour cibler, lors d'une démonstration, Lola Rasoamaharo, directeur et propriétaire de La Gazette de la Grande Île, un critique du président Rajoelina, ainsi que six ressortissants malgaches et un Français accusés de comploter contre le président. Par ailleurs, des analyses techniques menées par sekoia.io ont révélé une infrastructure associée à Predator à Madagascar, avec des serveurs résolus par des noms de domaines soutenant le président Rajoelina, candidat à sa réélection en 2023. Toutefois, aucun code d'exploitation de vulnérabilité n'a été trouvé sur ces serveurs.

Il semble que le gouvernement malgache ait acquis cette capacité principalement pour se protéger des opposants internes et se maintenir au pouvoir. Cependant, il est également plausible qu'il utilise cet outil contre toute menace extérieure perçue, ou pour collecter des renseignements susceptibles de favoriser Madagascar dans des négociations politiques ou économiques.

12- https://www.trendmicro.com/en_us/research/24/i/earth-baxia-spear-phishing-and-geoserver-exploit.html

13- https://nao-sec.org/



5.2.3 DÉSINFORMATION ET MANIPULATION DE L'INFORMATION

Les opérations de manipulation de l'information visent à diffuser des informations falsifiées, déformées ou erronées, souvent associées à des faits réels pour les rendre crédibles, ou sorties de leur contexte. Les réseaux sociaux sont l'un des principaux vecteurs utilisés par les acteurs de ces opérations. Parmi eux, on trouve des personnalités influentes, des médias, des associations ou des think tanks ayant des affinités, réelles ou supposées, avec des pays étrangers critiquant ou remettant en question les «valeurs occidentales».

Ces campagnes cherchent à fragiliser l'opinion publique ou à amplifier des discours et des oppositions. Dans ce contexte, les DROM-COM français sont ciblés par des campagnes de manipulation de l'information, souvent liées à des conflits sociétaux actuels, comme les aspirations à l'indépendance de certains territoires.

Premières observations sur X pour le périmètre des DROM-COM

Sur le réseau social X, l'analyse des termes « Colonisation », « Décolonisation », « colon », « coloniale », « politique coloniale » (sous le topic « Décolonisation ») associés à des îles françaises comme « Nouvelle-Calédonie », « Martinique », « Mayotte », « La Réunion », « Guadeloupe » (sous le topic « Îles ») a généré plus de 1 million de messages en septembre. Bien que le sujet de la décolonisation soit particulièrement sensible et source de confrontations, les réseaux sociaux comme X permettent de mesurer l'impact et la reprise de ces débats.

L'implication du Baku initiative group

Les intérêts français sont ciblés par des opérations de manipulation de l'information.

Un acteur particulièrement actif dans ce domaine est le Baku Initiative Group, un organisme azerbaïdjanais se présentant comme une ONG dédiée à la lutte contre le colonialisme.

Cependant, il devient rapidement évident que ses actions se concentrent exclusivement sur les territoires français, notamment contre ce qu'il qualifie de néo-colonialisme français.

Parmi les actions récentes du groupe, il joue un rôle actif dans les tensions en Nouvelle-Calédonie liées aux revendications d'indépendance. L'été 2024 a également vu se tenir à Baku le Congrès des Colonies Françaises, auquel ont participé des représentants de plusieurs territoires.

FIGURE 22 - https://x.com/bakuinitiative/status/1820364270942515426/photo/1

Premières conclusions sur les risques informationnels pour le périmètre des DROM-COM

Aucune campagne de manipulation de l'information spécifiquement ciblant La Réunion n'a été identifiée à ce jour. Cependant, les événements récents dans d'autres territoires ultramarins, tels que Mayotte avec la revendication du territoire par les Comores, ou la Martinique avec les manifestations contre la hausse des prix, ont été amplifiés par ce même groupe azerbaïdjanais. Les manœuvres s'organisent autour de plusieurs méthodes de diffusion, telles que la création de visuels, l'amplification via l'utilisation de hashtags (#FrenchColonies, etc.), et la reprise de contenus provenant d'autres médias.

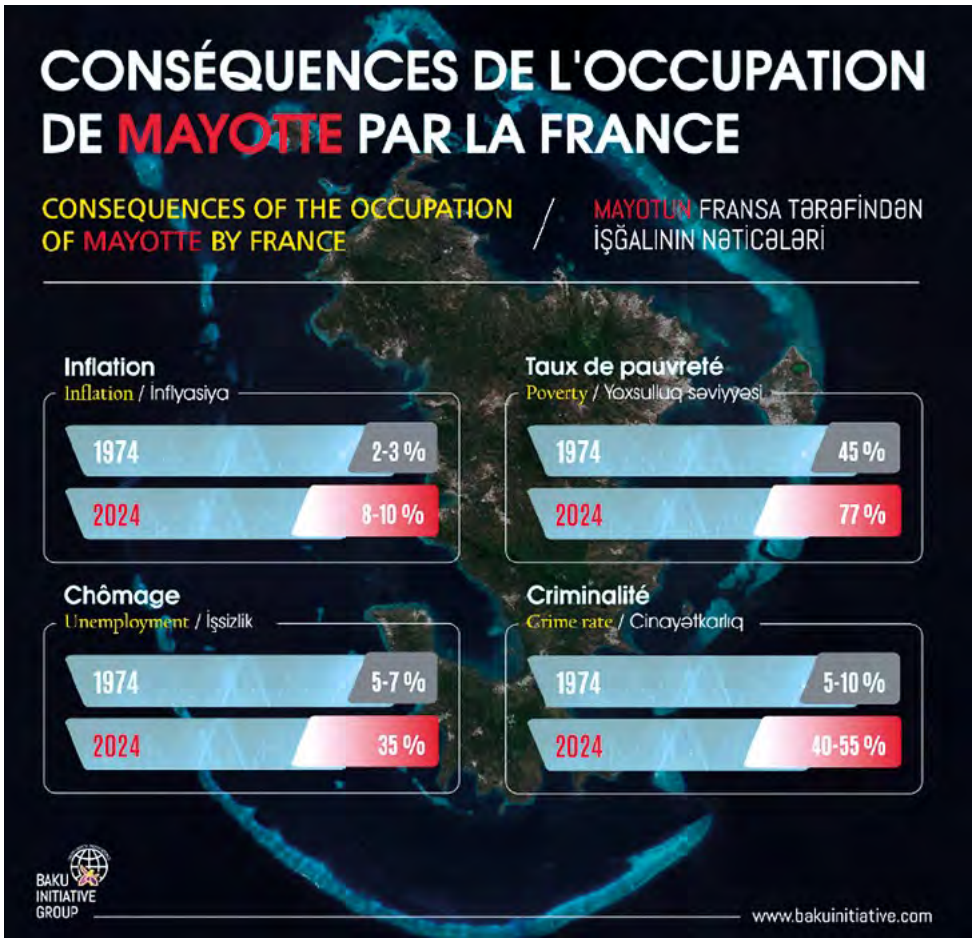


FIGURE 23 - https://x.com/bakuinitiative/status/1835955999435280415/photo/1

Les actions menées par l'Azerbaïdjan semblent être des mesures de rétorsion contre des politiques françaises jugées trop favorables aux intérêts arméniens. Elles font suite à une politique dite du « caviar », consistant à offrir des avantages à des représentants français pour influencer des décisions favorables à l'Azerbaïdjan.

Le mode opératoire du groupe se limite pour l'instant à établir des liens avec des politiciens indépendants de ces territoires, organiser des rencontres et partager des contenus soutenant leur discours. De plus, le groupe ne semble pas disposer d'une large audience (environ 2500 abonnés) sur X, son principal réseau social. Par conséquent, les conséquences réelles de ces tentatives de déstabilisation restent actuellement limitées.

Le groupe dispose également de profils sur Facebook, LinkedIn, YouTube, TikTok et Instagram, où sont publiés des contenus critiques envers la France, ainsi que des partages de médias, comme le média panafricain For You Média Africa, qui semble relayer des narratifs pro-russes.

Toutefois, des recherches supplémentaires sont nécessaires pour analyser et caractériser précisément ce média en ligne.

FIGURE 24 - Exemple de vidéo TikTok critique à l'égard de la France, source : TikTok

FIGURE 25 - Publication Instagram de promotion du média "For You Media Africa", source : Instagram

6

Rapport sur l'état de la menace cyber
dans l'Océan Indien

Analyses des modes opératoires des attaquants

6.1 TACTIQUES, TECHNIQUES ET PROCÉDURES (TTPS)

Les menaces identifiées permettent d'établir un tableau des tactiques, techniques et procédures selon le framework MITRE ATT&CK.

Cette compréhension des modes opératoires des attaquants aide les entités à anticiper les attaques et à vérifier la présence d'attaquants dans leur propre système d'information.

6.1.1 TTPS UTILISÉES PAR LES ACTEURS CYBERCRIMINELS

Les TTPs présentées ci-dessous correspondent à celles observées lors des différentes campagnes analysées dans ce rapport. Les autres tactiques et techniques ont volontairement été écartées pour faciliter la lecture du tableau.

Reconnaissance	Resource Development	Initial Access	Persistence	Privilege Escalation	Credential Access	Collection	Command and Control	Exfiltration	Impact
T1595 Active Scanning	T1650 Acquire Access	T1190 Exploit Public-Facing Application	T1078 Valid Accounts	T1078 Valid Accounts	T1056 Input Capture	T1185 Browser Session Hijacking	T1071 Application Layer Protocol	T1041 Exfiltration Over C2 Channel	T1485 Data Destruction
T1592 Gather Victim Host Information	T1583 Acquire Infrastructure	T1566 Phishing				T1114 Email Collection			T1486 Data Encrypted for Impact
T1597 Search Closed Sources	T1586 Compromise Accounts	T1078 Valid Accounts				T1056 Input Capture			T1561 Disk Wipe
	T1584 Compromise Infrastructure					T1113 Screen Capture			T1657 Financial Theft
	T1587 Develop Capabilities					T1125 Video Capture			
	T1585 Establish Accounts								
	T1588 Obtain Capabilities								
	T1608 Stage Capabilities								

FIGURE 26 - Matrice MITRE de la menace cybercriminelle opportuniste et lucrative, source : OWN-CERT

6.1.2 TTPS UTILISÉES PAR LES ACTEURS ÉTATIQUES ET HACKTIVISTES

Les TTPs présentées ci-dessous correspondent à celles observées lors des différentes campagnes analysées dans ce rapport. Les autres tactiques et techniques ont volontairement été écartées pour faciliter la lecture du tableau.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Discovery	Lateral Movement	Command and Control	Exfiltration	Impact
T1190 Exploit Public-Facing Application	T1106 Native API	T1574 Hijack Execution Flow	T1574 Hijack Execution Flow	T1574 Hijack Execution Flow	T1083 File and Directory Discovery	T1091 Replication Through Removable Media	T1573 Encrypted Channel	T1041 Exfiltration Over C2 Channel	T1565 Data Manipulation
T1091 Replication Through Removable Media	T1129 Shared Modules		T1055 Process Injection	T1202 Indirect Command Execution	T1120 Peripheral Device Discovery		T1008 Fallback Channels		T1491 Defacement
				T1036 Masquerading	T1018 Remote System Discovery		T1105 Ingress Tool Transfer		T1499 Endpoint Denial of Service
				T1055 Process Injection	T1497 Virtualization /Sandbox Evasion				
				T1497 Virtualization/ Sandbox Evasion					

FIGURE 27 - Matrice MITRE de la menace étatique et hacktiviste, source : OWN-CERT

6.2 TECHNIQUES UTILISÉES PAR LES ACTEURS DERRIÈRE LES ACTIONS DE MANIPULATIONS DE L'INFORMATION

Les actions de manipulation de l'information sont analysées et répertoriées dans un Framework appelé DISARM. Dans le cadre de l'analyse des tentatives d'ingérence du groupe du Baku Initiative Group, les principales techniques utilisées par le groupe ont été regroupées dans le tableau ci-dessous.

Les TTPs présentées ci-dessous correspondent à celles observées lors des différentes campagnes analysées dans ce rapport. Les autres tactiques et techniques ont volontairement été écartées pour faciliter la lecture du tableau.

Plan		Prepare		Execute		
TA01 Plan Strategy	TA02 Plan Objectives	TA06 Develop Content	TA16 Establish Legitimacy	TA07 Select Channels and Affordances	TA17 Maximize Exposure	TA10 Drive Offline Activity
T0073 Determine Target Audiences	T0075 Dismiss	T0015: Create hastags and search artifacts	T0100.003 Co-opt Influencers	T0104 Social Networks	T0049.003 Bots Amplify via Automated Forwarding and Reposting	T0057 Organize Events
T0074 Determine Strategic Ends	T0076 Distort	T0023: Distort facts		T0104.001 Mainstream Social Networks	T0118 Amplify Existing Narrative	
	T0077 Distract	T0084.001 Use Copypasta		T0104.002 Dating Apps		
	T0079 Divide			T0104.005 Use hashtags		
				T0104.006 Create dedicated hashtag		
				T0105.001 Photo Sharing		
				T0105.002 Video Sharing		

FIGURE 28 - Techniques issues de la matrice DISARM, source : OWN-CERT

7

Rapport sur l'état de la menace cyber
dans l'Océan Indien

Référentiels

7.1 TLP (Traffic Light Protocol)

Le Traffic Light Protocol (TLP), initié par le FIRST (Forum of Incident Response and Security Teams), est une convention largement adoptée par les acteurs de la réponse à incidents.

Avec ses quatre niveaux associés à des couleurs, le TLP définit les règles de partage des informations en fonction de leur sensibilité.

Échelle	Interprétation opérationnelle des différents niveaux de TLP (source : ANSSI, FIRST)
TLP:RED	Pour les yeux et les oreilles des destinataires individuels uniquement, aucune autre divulgation. Les sources peuvent utiliser l'appellation TLP:RED lorsque les informations ne peuvent pas être traitées efficacement sans risque significatif pour la vie privée, la réputation ou les opérations des organisations concernées. Les destinataires ne peuvent donc pas partager les informations avec l'appellation TLP:RED avec qui que ce soit. Dans le contexte d'une réunion, par exemple, les informations mentionnées avec le label TLP:RED sont limitées aux personnes présentes à La Réunion.
TLP:AMBER	Diffusion limitée à quelques entités identifiées, liées par un engagement (ex : une communauté fermée). Les destinataires ne peuvent diffuser ces informations que sur la base du besoin d'en connaître au sein de leur organisation, de leurs clients, etc.
TLP:AMBER + STRICT	Restriction du partage à l'organisation uniquement. Exclut le partage aux autres acteurs liées par un engagement.
TLP:GREEN	Diffusion libre au sein d'une communauté (ouverte ou fermée) bien identifiée, repartage libre au sein de ces communautés (prestataires inclus).
TLP:CLEAR	Diffusion publique, sans restriction, partage libre entre les différentes communautés, y compris sur Internet.

→ **Pour en savoir plus :** https://www.cert.ssi.gouv.fr/csirt/politique-partage/
https://www.first.org/tlp/

7.2 PAP (Permissible Action Protocol)

Introduit en 2016 dans les taxonomies de la plateforme MISP (Malware Information Sharing Platform) maintenue par le CIRCL (Computer Incident Response Center Luxembourg), le Permissible Action Protocol (PAP) définit les limites d'exposition, d'exploitation et de réutilisation d'une information à des fins d'investigation, de pivot en sources ouvertes, ou de détection sur un système d'information.

Échelle	Interprétation opérationnelle des différents niveaux de PAP (source : ANSSI)
TLP:RED	Utilisation limitée aux investigations numériques ou à la détection, sur des infrastructures dédiées : • seules les personnes ayant le besoin d'en connaître ont accès à ces infrastructures ; • ces infrastructures sont protégées des réseaux publics (ex.: Internet) et des infrastructures communes du système d'information (ci-après « SI ») de l'entité ; • afin de ne rien révéler des capacités de détection, seules des actions non visibles par un potentiel attaquant sont autorisées, telles que par exemple des recherches hors production sur des éléments collectés préalablement ; • les interactions directes ou indirectes, ainsi que les requêtes sur des services tiers, ne sont pas autorisées.
TLP:AMBER	Utilisation limitée à une exploitation passive de la donnée, c'est-à-dire aux seules actions non directement visibles des sources malveillantes. Les interactions, même indirectes, avec le système ou l'infrastructure de l'attaquant sont interdites.
TLP:GREEN	Utilisation encadrée autorisant les interactions non intrusives avec des sources malveillantes.
TLP:CLEAR	Utilisation libre dans le respect des licences et de la loi, pas de contrainte relative à l'exploitation ou à la manipulation de l'information.

→ **Pour en savoir plus :** https://www.cert.ssi.gouv.fr/csirt/politique-partage/

CYBER RÉUNION

Élever les niveaux de cybersécurité
et de cyber résilience du territoire

CYBER-REUNION.FR

CYBER RÉUNION

Porté par Réunion THD
établissement public de la Région Réunion

Soutenu par
RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Region Reunion
www.regionreunion.com