TLP:WHITE

N° 1
FÉVRIER
2025

SYNTHÈSE

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

CYBER RÉUNION

Ce document a été rédigé en collaboration avec

OWN

TLP:WHITE

La Réunion : un territoire stratégique sous pression cyber

Île française au cœur de l'océan Indien, La Réunion occupe une position stratégique dans cette région du monde, servant de point d'ancrage pour la France et l'Union européenne. Son dynamisme économique, en faisant l'un des territoires les plus prospères de la région, attire naturellement l'attention des cybercriminels, qui exploitent ses ressources numériques et ses infrastructures sensibles.

Avec des câbles sous-marins essentiels comme LION, METISS et SAFE, l'île assure une connectivité internationale de premier plan, reliant l'Afrique, l'Asie et l'Europe. Cependant, ces infrastructures critiques sont également vulnérables aux cyberattaques et aux actes de malveillance.

La Réunion : un territoire stratégique sous pression cyber

TLP:WHITE

Les cybermenaces pesant sur La Réunion sont multiples et polymorphes : attaques opportunistes (phishing, ransomwares, fuites de données), campagnes de hacktivisme ciblées, et tensions géostratégiques croissantes dans l'océan Indien impliquant des acteurs majeurs tels que la Chine, les États-Unis et l'Inde. L'île est ainsi directement exposée à des risques liés aux rivalités internationales.

Dans ce contexte, la présente synthèse, issue d'une collaboration entre CYBER RÉUNION et la société OWN, offre un aperçu des cybermenaces auxquelles La Réunion est confrontée. Elle met en lumière les tendances majeures observées et propose des recommandations clés pour renforcer la résilience des acteurs économiques et institutionnels du territoire.

Le rapport complet, détaillant l'ensemble des analyses et des modes opératoires des cyberattaquants, est accessible sur le site internet de CYBER RÉUNION, afin de permettre aux parties prenantes d'approfondir leur compréhension des risques et d'adopter des stratégies de protection adaptées.

TLP:WHITE

Chiffres clés et tendances

14 incidents
remontées par l'ANSSI en 2023 ciblant La Réunion, parmi lesquels les cyberattaques contre des entités du secteur du transport, de la logistique ou encore de la santé.

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.

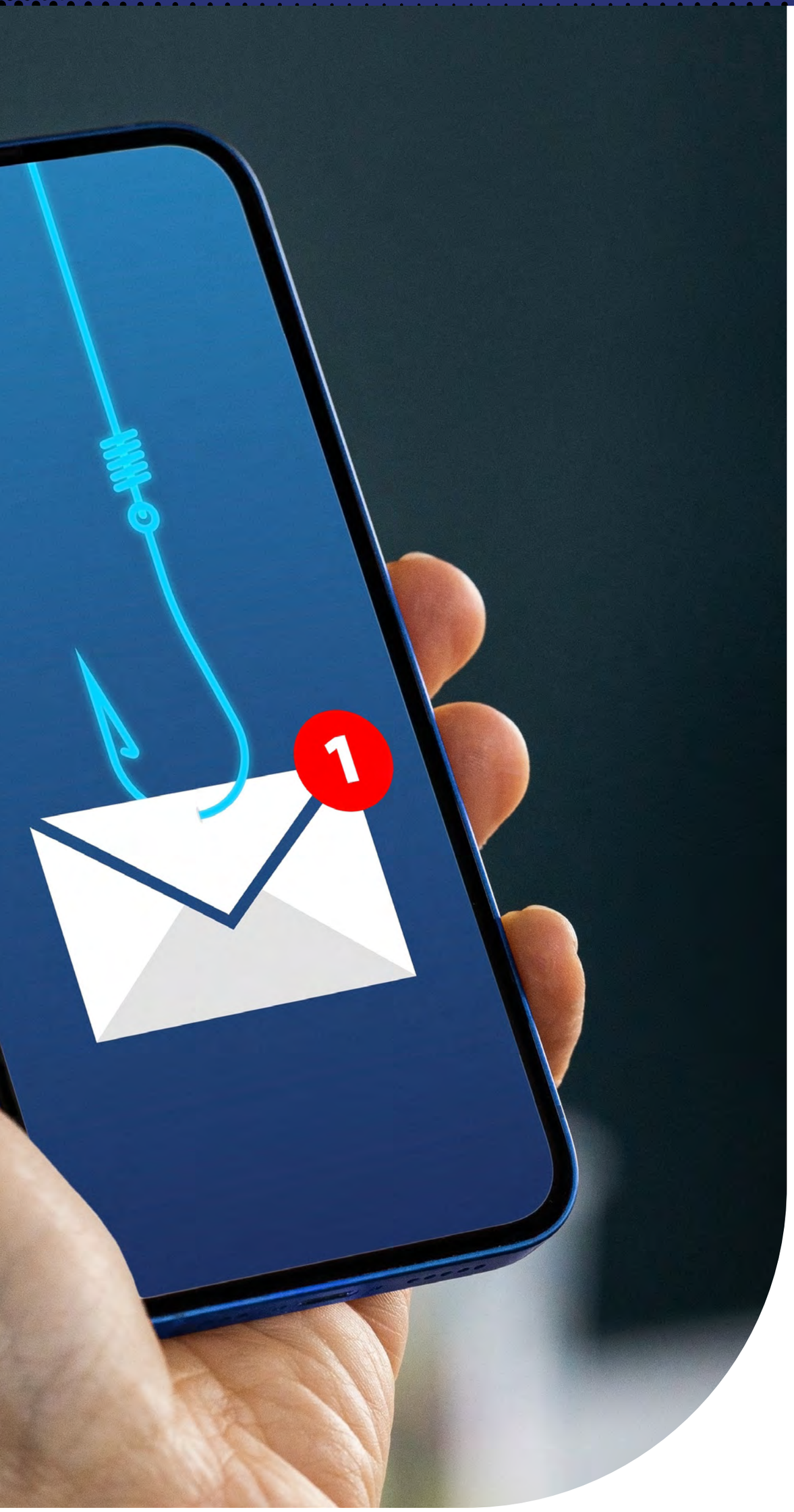
LES DYNAMIQUES DE LA MENACE CYBER À LA RÉUNION EN 2024

Une menace cybercriminelle opportuniste et en expansion

La cybercriminalité opportuniste, principalement générique, demeure la menace prédominante à La Réunion. En 2024, les attaques à des fins d'extorsion ont maintenu un niveau élevé, reflétant une évolution constante de l'écosystème cybercriminel. La diffusion en source ouverte de codes de rançongiciels et la prolifération d'outils exploitables par des acteurs peu qualifiés contribuent à une accessibilité accrue aux techniques d'attaque, amplifiant ainsi les risques pour les entreprises et les institutions locales.

Un territoire peu ciblé par des opérations étatiques, mais exposé à des menaces régionales

Aucune activité d'espionnage ou de sabotage directement dirigée contre La Réunion n'a été détectée par le OWN-CERT. Toutefois, la zone Asie-Pacifique, dont l'île fait partie, reste un terrain d'action pour plusieurs groupes d'attaquants sophistiqués. Certains, affiliés à la Chine comme **Volt Typhoon** et **Earth Baxia**, déploient des modes opératoires avancés visant notamment les infrastructures critiques et les télécommunications dans la région, ce qui pourrait, à terme, avoir des répercussions sur le territoire réunionnais.



Les techniques d'intrusion les plus courantes

L'analyse des Tactiques, Techniques et Procédures (TTPs) met en évidence deux vecteurs d'attaque majeurs :

- **Le phishing (T1566)** reste le principal moyen d'intrusion, utilisé aussi bien par des acteurs cybercriminels opportunistes que par des groupes plus sophistiqués.
- **L'exploitation de vulnérabilités (T1190)** constitue un levier d'attaque privilégié, non seulement contre les entreprises locales mais aussi à travers l'ensemble de la chaîne d'approvisionnement, augmentant ainsi l'exposition des organisations aux compromissions de grande ampleur.

Cette dynamique souligne la nécessité d'un renforcement des mesures de cybersécurité, notamment en matière de détection proactive, de sensibilisation des utilisateurs et de gestion des vulnérabilités pour limiter les opportunités d'intrusion.

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

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

...sa nationalité française

...sa situation géographique

...ciblée de manière opportuniste (exploitation de données qui ont fuité ou mauvaise exposition)

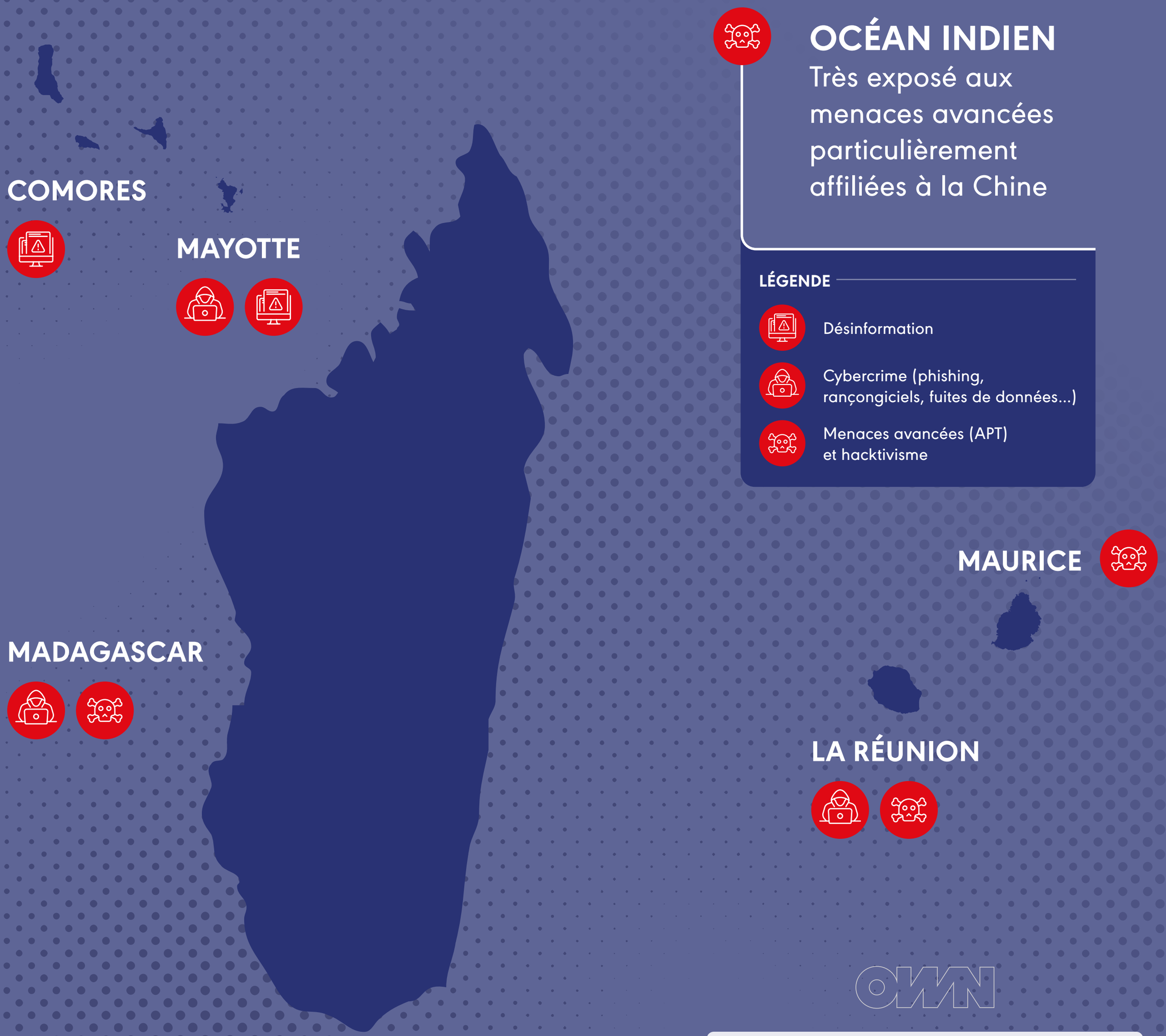


FIGURE 2 - Carte récapitulative des menaces observées dans le rapport, source: OWN-CERT

TLP:WHITE

Évaluation des risques cyber pour La Réunion

L’évaluation des risques cyber repose sur l’analyse des menaces susceptibles d’affecter les entités implantées sur l’île de La Réunion. Chaque menace est évaluée selon deux critères : son impact potentiel et sa probabilité d’occurrence, permettant ainsi d’attribuer un niveau de risque spécifique en fonction de sa gravité.

Cette première matrice de risques se concentre sur les menaces identifiées à partir de sources ouvertes et apporte un éclairage sur les risques zonaux. Elle vise à aider les entreprises et institutions réunionnaises à mieux comprendre et anticiper les menaces susceptibles de perturber leurs activités.

Cette évaluation est évolutive : elle sera affinée au fil des publications grâce à l’intégration des retours d’expérience et des observations recueillies sur les incidents cyber touchant les acteurs du territoire. L’objectif est d’adapter en continu l’analyse des risques pour offrir une vision toujours plus précise et exploitable par les décideurs locaux.

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

Hacktivisme : un risque réel pour La Réunion

L'hacktivisme constitue **une menace significative** pour La Réunion, en raison de plusieurs attaques revendiquées contre le territoire en réaction aux positions françaises sur la scène internationale. Au-delà du contexte géopolitique marqué par les tensions entre la Russie et l'Ukraine ainsi que par le conflit au Proche-Orient, l'arrestation en France du fondateur de Telegram, Pavel Durov, a été largement instrumentalisée par divers groupes hacktivistes pour justifier des actions ciblées contre des infrastructures locales.

Cybercriminalité : une menace critique et omniprésente

La menace cybercriminelle reste particulièrement élevée à La Réunion, impactant fortement les entreprises locales. Les attaquants exploitent les fuites de données via des courtiers d'accès initial (Initial Access Brokers - IAB), à l'image de l'acteur mont4na, ainsi que des campagnes de phishing et de rançongiciels.

Depuis le 1er janvier 2024, le OWN-CERT a recensé des attaques visant principalement les secteurs suivants :

- **Manufacturing (25%)**
- **Construction (16%)**
- **Éducation (10%)**
- **Retail (10%)**
- **Santé (7%)**

Les groupes cybercriminels les plus actifs sur cette période incluent Lockbit3, 8base et Ransomhub. En parallèle, l'émergence d'un nouvel acteur, Termite, suscite une attention particulière, notamment après son attaque revendiquée contre une collectivité territoriale de premier plan en novembre 2024.

Menace étatique : un risque mineur mais une vigilance nécessaire

Bien que La Réunion occupe une position stratégique dans l'océan Indien, la menace étatique y est évaluée comme faible par rapport à d'autres territoires de la zone Asie-Pacifique, où les tensions géopolitiques sont plus marquées

Néanmoins, des activités malveillantes récentes, attribuées à des groupes affiliés à la Chine, ont été observées, ciblant notamment des entités gouvernementales à Maurice. Ces opérations soulignent l'importance d'un suivi attentif des dynamiques cyber dans la région, en raison des risques potentiels liés à l'espionnage et aux intrusions dans les infrastructures stratégiques.

Désinformation : une amplification des tensions ultramarines

À ce jour, aucune campagne de manipulation de l'information spécifiquement dirigée contre La Réunion n'a été identifiée par le OWN-CERT. Toutefois, certains événements récents dans les territoires ultramarins, ainsi que les tensions sociales liées à la hausse des prix, ont fait l'objet d'une récupération et d'une amplification sur les réseaux sociaux.

Ces narratifs ont été relayés par des groupes probablement affiliés à l'Azerbaïdjan, exploitant ces tensions pour alimenter des discours de contestation et influencer l'opinion publique. Ce phénomène s'inscrit dans une dynamique plus large où des acteurs extérieurs cherchent à fragiliser la cohésion des territoires français d'outre-mer à travers des campagnes informationnelles ciblées.

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