Étude OSINT des compromissions de données en Nouvelle-Calédonie

Analyse des données exposées du territoire entre janvier 2024 et avril 2025

Laurent Rivaton

AdDo - Audit, Conseil et Formation en Cybersécurité

Document de restitution - Version publique

Mai 2025

AdDo

1. Synthèse

Cette étude s'appuie sur une analyse OSINT [1] pour identifier l'ampleur et la nature des compromissions de données en Nouvelle-Calédonie. En combinant une approche classique (analyse de fuites liées aux domaines en .nc) et une méthode plus ciblée (analyse de logs de stealers [2]), elle révèle l'ampleur d'une menace encore sous-estimée.

Plus de 1100 domaines en .nc et jusqu'à 900 postes individuels compromis ont été recensés de janvier 2024 à avril 2025. Un décompte hebdomadaire sur la même période confirme le caractère permanent des compromissions.

Afin d'endiguer ce phénomène, des recommandations pragmatiques sont proposées pour les entreprises et les organisations, mais aussi pour les particuliers et enfin pour les institutions locales.

2. Introduction

La cybersécurité est un enjeu de plus en plus pressant, y compris dans les territoires supposés isolés comme la Nouvelle-Calédonie. Depuis plusieurs années, des recherches OSINT [1] ont été menées pour tenter de quantifier les données compromises accessibles publiquement. L'étude présentée ici s'inscrit dans cette démarche, avec une approche plus ciblée en 2025.

L'objectif est double : dresser un état des lieux, et aider les actions de sensibilisation menées sur le Caillou en s'appuyant sur des données concrètes.

3. Méthodologie

3.1. Cadre général

L'étude repose sur une démarche OSINT [1] visant à identifier et analyser les données compromises accessibles publiquement sur l'ensemble de l'Internet (web, deep web [3], dark web [4]), en ciblant spécifiquement la Nouvelle-Calédonie.

Deux phases ont structuré cette recherche :

- une première, avec une approche globale, consistant à recenser les fuites d'identifiants associés aux domaines en .nc,
- une seconde, plus ciblée, orientée vers l'identification de machines locales compromises via des stealers [2].

3.2. Sources et outils

L'étude a mobilisé un ensemble de sources accessibles publiquement ou via des plateformes spécialisées, dans le respect des principes de l'OSINT [1]. L'objectif était de recouper des données fiables, représentatives, et pertinentes pour le périmètre géographique étudié.

Les principales sources qui ont été exploitées :

- Have I Been Pwned (HIBP) : pour les premières vérifications d'adresses liées à des fuites grand public,
- DeHashed : pour l'extraction de résultats plus détaillés à partir de noms de domaines ou d'adresses de courrier électronique,
- IntelligenceX : utilisé à la fois comme source principale pour accéder à des dumps [5] de données liées aux stealers [2], et comme moteur de recherche OSINT [1] pour repérer des fuites peu référencées.

Le traitement des données a été réalisé exclusivement à l'aide d'outils en ligne de commande (bash), sans recours à des langages de scripting comme Python. Cette approche minimaliste, choisie comme un défi personnel, a permis de réaliser l'ensemble des étapes d'analyse (tri, filtrage, structuration, dénombrement) à l'aide de commandes classiques comme grep, awk, sort, uniq, etc., en garantissant sobriété, reproductibilité et maîtrise du traitement.

3.3. Critères de localisation géographique

Les données ont été filtrées selon plusieurs indicateurs permettant d'identifier les cas en lien avec la Nouvelle-Calédonie :

- adresses IP localisées en NC,
- suffixes ou domaines de messagerie spécifiques (@canl.nc, @mls.nc, @lagoon.nc, @gouv.nc, etc.),
- métadonnées système (langue française, fuseau horaire UTC+11, etc.).

3.4. Contenu des données

Les jeux de données analysés contiennent, selon les cas :

- des identifiants (adresse de courrier électronique, compte) et mots de passe, généralement avec le site associé,
- des cookies [6] de session, des données de saisie automatique, des historiques de navigation,
- des documents bureautiques, des captures d'écran, des fichiers professionnels,
- des métadonnées système : nom d'ordinateur, OS, matériel, logiciels,
- des informations personnelles : nom, prénom, adresse, numéro de téléphone, numéro de passeport, informations de CB.

3.5. Limitations et éthique

- L'étude repose uniquement sur des données publiées (ou rendues publiques).
- Un seul type de malware [7] est analysé : les stealers [2].
- D'autres formes de compromission (ransomware, spyware, etc.) ne sont pas prises en compte.
- L'approche est volontairement non intrusive, avec un strict respect de l'anonymat des victimes.
- Aucun usage ou test des identifiants trouvés n'a été réalisé.

4. Résultats

4.1. Données liées aux domaines .nc

Une première phase de l'étude a consisté à analyser les fuites d'identifiants associées aux noms de domaine en .nc, en s'appuyant sur des bases de données accessibles publiquement.

- Plus de 1100 domaines en .nc ont été identifiés comme concernés.
- Environ 80 000 lignes de données compromises ont été recensées.
- Chaque ligne contenait généralement une adresse de courrier électronique, un compte d'accès et un mot de passe.

Ces données donnent une vision globale, bien que partielle, de la compromission du territoire, mais ne permettent pas d'identifier directement des postes ou des utilisateurs spécifiques.

4.2. Postes infectés par des stealers

La seconde phase a porté sur les machines présentes en Nouvelle-Calédonie et compromises par des logiciels malveillants de type stealer [2].

- Entre 500 et 900 postes distincts ont été identifiés comme compromis.
- Chaque log contenait des couples identifiant/mot de passe avec le site internet correspondant, ce qui rend l'exploitation beaucoup plus directe et ciblée.

Les services compromis couvrent un large spectre :

- des services personnels : réseaux sociaux, sites de vidéo à la demande, jeux en ligne, sites pour adultes, etc.,
- des services essentiels : banques, impôts, santé, énergie, télécommunications, commerce électronique, etc.,
- des services professionnels : cabinets médicaux, collectivités, fournisseurs, bureaux d'études, etc.

Les données associées incluent également :

- des métadonnées système : nom du poste, adresse IP, OS, configuration matérielle,
- des historiques de navigation, de téléchargements, des captures d'écran,
- des fichiers bureautiques et documents professionnels (ex. : AutoCAD, tableurs, traitements de texte),
- des données personnelles : nom, prénom, date de naissance, adresse, numéros sensibles.

4.3. Suivi hebdomadaire des compromissions (2024–2025)

- Un décompte hebdomadaire a été réalisé sur la période allant du 1er janvier 2024 au 30 avril 2025, recensant les alertes OSINT [1] liées à des compromissions par stealer [2].
- En général, quelques dizaines d'alertes par semaine sont relevées.
- Des pics allant jusqu'à 50 alertes en une seule semaine ont été observés.

La compromission la plus récente analysée date d'avril 2025, ce qui confirme une activité toujours en cours.

Ces données permettent de constater que la compromission est un phénomène continu et répété, affectant le territoire de manière diffuse, mais persistante.

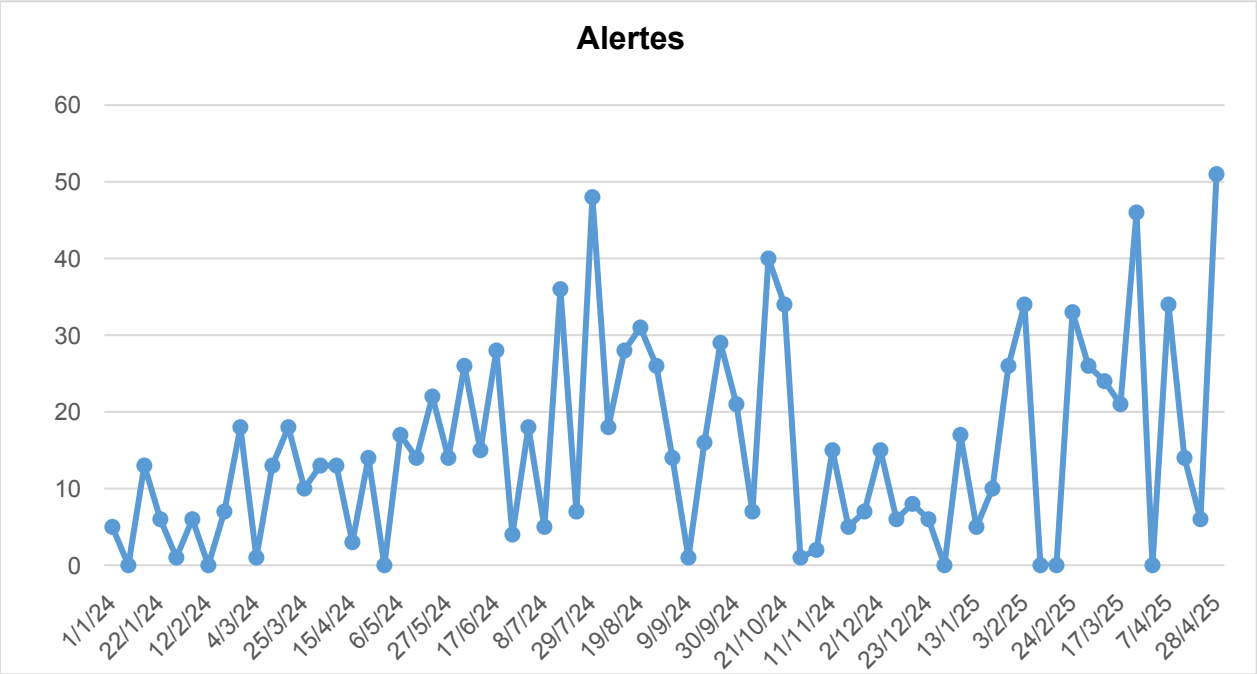

Figure 1 : Suivi hebdomadaire des alertes de stealers de janvier 2024 à avril 2025

4.4. Enrichissement comparatif

Pour donner un point de repère, le nombre d'alertes OSINT [1] sur la dernière semaine de mars 2025 a été comparé entre trois territoires :

- Nouvelle-Calédonie : environ 40 alertes, pour une population estimée à 270 000 habitants,
- France hexagonale : environ 8 000 alertes, pour environ 68 millions d'habitants,
- Australie : environ 4 000 alertes, pour environ 26 millions d'habitants.

Rapporté à la population, cela correspond à :

- 1 alerte pour 6 750 habitants en Nouvelle-Calédonie,
- 1 alerte pour 8 500 habitants en France hexagonale,
- 1 alerte pour 6 500 habitants en Australie.

Bien que ces chiffres soient trop partiels pour permettre une analyse pertinente (données limitées à une seule semaine et à un seul type de malware), ils donnent un aperçu de la cohérence entre la Nouvelle-Calédonie et d'autres territoires plus vastes et auxquels on voudrait pouvoir se comparer.

5. Analyse et interprétation

5.1. Une compromission silencieuse, massive et continue

L'analyse des résultats montre que la compromission de données par stealer [2] est un phénomène régulier et durable. Les dizaines d'alertes hebdomadaires recensées depuis janvier 2024 témoignent d'une activité constante, dont l'impact reste souvent invisible pour les victimes. La récurrence des infections suggère une vulnérabilité persistante et structurelle du territoire. Cette compromission s'opère de manière silencieuse, sans alerte pour l'utilisateur, et sans détection systématique par les outils de sécurité traditionnels.

5.2. Un changement d'échelle dans la perception du risque

Alors que les études antérieures portaient sur des fuites de données liées à des services distants (réseaux sociaux, commerce en ligne, services divers), cette étude permet d'identifier des postes physiquement présents sur le territoire, infectés par des malwares actifs. Cela change la perception du risque : on passe de l'impression diffuse d'un piratage lointain à la réalité tangible d'une compromission personnelle et locale. Ce changement de point de vue est crucial pour favoriser la prise de conscience, car il montre que les risques cyber ne concernent pas uniquement les grandes entreprises ou les plateformes internationales, mais aussi les citoyens, les TPE, les collectivités locales.

5.3. Des profils de victimes variés

Les types de services compromis révèlent une grande diversité des profils concernés : particuliers, employés, agents publics, professions libérales, etc. Le phénomène ne se limite ni à un secteur d'activité, ni à une catégorie d'âge ou de compétence numérique. La porosité entre sphère personnelle et professionnelle accentue les risques, notamment lorsque les usages numériques personnels et professionnels cohabitent sur un même équipement. Des accès à des outils métiers, à des plateformes administratives ou à des services critiques peuvent ainsi être compromis via des postes personnels mal protégés.

5.4. Une menace sous-estimée

Les résultats obtenus reposent sur l'analyse d'un seul type de malware [7] (stealer [2]) et sur des données publiquement accessibles. Il est donc probable que la réalité soit bien plus sévère. De nombreuses compromissions ne sont pas rendues publiques, soit parce que leurs butins sont en vente, soit parce qu'elles sont encore exploitées de manière discrète. Par ailleurs, d'autres types de logiciels malveillants (keylogger, backdoor, ransomware, etc.) échappent totalement au

champ de cette étude. Il faut donc considérer les chiffres comme des ordres de grandeur minimaux.

5.5. Un enjeu local aux conséquences collectives

Dans un territoire insulaire comme la Nouvelle-Calédonie, la compromission d'un poste peut avoir des conséquences en chaîne : exposition d'un réseau professionnel, rebond vers des partenaires, atteinte à la réputation, voire coercition ou chantage. Dans un contexte où les acteurs sont étroitement liés, une compromission peut se propager bien au-delà du poste initialement touché. De plus, les services publics, les structures de santé ou les entreprises locales peuvent se retrouver impactés de manière disproportionnée. La cybersécurité devient ici une responsabilité partagée, où l'action individuelle peut avoir un impact collectif. Construire une culture commune du risque numérique est un impératif de souveraineté locale.

6. Recommandations

Les résultats de cette étude montrent une compromission significative, persistante et probablement sous-estimée en Nouvelle-Calédonie. Pour y faire face, plusieurs niveaux d'action sont nécessaires, impliquant à la fois les entreprises, les particuliers, les institutions et les acteurs publics. Ces recommandations visent à amorcer une dynamique de prévention durable, adaptée au contexte local.

6.1. Recommandations pour les entreprises et les organisations

Les structures professionnelles doivent structurer leur approche cybersécurité afin de limiter les surfaces d'attaque, d'assurer la continuité d'activité, et de protéger les données de leurs clients, utilisateurs ou partenaires.

- Former et sensibiliser régulièrement les collaborateurs avec des formations courtes, interactives ou des rappels mensuels de bonnes pratiques.
- Mettre en place des outils de protection avancée : antivirus professionnels, filtrage DNS, EDR [8], IDS/IPS [9], etc.
- Mettre à jour les équipements de manière centralisée ou systématique, à l'aide d'outils adaptés.
- Cartographier les équipements et les flux critiques : identifier ce qui est réellement exposé ou vulnérable.
- Appliquer le principe du moindre privilège : les utilisateurs se voient attribuer les accès strictement nécessaires à leur mission et uniquement pendant la durée de celle-ci.
- Établir un plan de réponse à incident : savoir quoi faire, qui appeler, et comment communiquer en cas de compromission.

Même les TPE/PME peuvent mettre en œuvre ces mesures à leur échelle, avec des solutions simples et peu coûteuses. En cybersécurité, le pragmatisme est de rigueur et il faut gérer son risque en tenant compte de ses moyens et ressources.

6.2. Recommandations pour les particuliers

Les particuliers représentent une part importante des victimes identifiées. Il est donc essentiel de renforcer l'hygiène numérique individuelle, souvent négligée par manque de formation ou de moyens. Parmi les gestes à adopter :

- Utiliser un gestionnaire de mots de passe (Bitwarden, KeePass, Proton Pass, etc.) pour générer des identifiants uniques, complexes et non réutilisés.

- Activer l'authentification à deux facteurs (2FA) sur les services importants (messagerie, banque, réseaux sociaux, etc.).
- Mettre à jour régulièrement ses logiciels et équipements, en incluant les smartphones et les navigateurs.
- Éviter les logiciels piratés ou les cracks [10], souvent associés à des stealers [2] dans les forums ou les sites de téléchargement.
- Faire régulièrement un "ménage numérique" : suppression des comptes inutilisés, des cookies [6], des historiques et des fichiers sensibles.
- Effectuer des analyses de sécurité régulières, même avec des solutions gratuites, pour repérer les comportements anormaux.

Il est important de rappeler que même des profils "non techniques" peuvent être ciblés, notamment via des techniques simples comme le phishing [11].

6.3. Recommandations pour les acteurs publics et territoriaux

Les collectivités, les établissements publics et les institutions locales ont un rôle fondamental à jouer dans la coordination et la montée en maturité cybersécurité du territoire :

- Organiser des campagnes locales de formation et de sensibilisation, dans les communes, les établissements scolaires, les centres de formation ou les espaces publics numériques.
- Soutenir les dispositifs d'initiation gratuite ou de découverte, comme les Tremplins du numérique ou les évènements comme le HacKagou organisés par OPEN NC, en favorisant la multiplication des ateliers orientés cybersécurité.
- Créer ou renforcer une cellule régionale de veille, d'analyse et d'alerte, sous forme d'un CERT/CSIRT [12] local ou d'une structure mutualisée, en lien avec les acteurs nationaux et régionaux.
- Appuyer le développement de la filière cybersécurité en Nouvelle-Calédonie, en facilitant l'émergence d'un tissu professionnel structuré et compétent.
- Favoriser les synergies entre acteurs publics, économiques, académiques et associatifs, via des dispositifs d'appui aux clusters, de financement de formations, de soutien à la recherche appliquée et à la professionnalisation.
- Encourager et faciliter la coopération régionale en matière de cybersécurité, notamment avec la Polynésie française, Wallis-et-Futuna, l'Australie et les pays du Pacifique.
- Intégrer des exigences de cybersécurité dans les marchés publics, notamment pour l'hébergement, la conception de sites web ou les prestations de maintenance.

Ce niveau d'action est essentiel pour structurer un écosystème cyber local robuste, durable et adapté aux spécificités du territoire.

6.4. Un levier transversal : la formation

La formation est le fil conducteur de toutes les recommandations précédentes. Elle constitue le seul levier réellement efficace pour changer durablement les comportements et réduire les vulnérabilités humaines, qui restent le maillon faible.

Il ne s'agit pas seulement de sensibiliser ponctuellement, mais de bâtir une culture du risque numérique accessible, continue et adaptée aux réalités du territoire. À l'image de l'exemple évoqué lors de la restitution du 14 mars (le "permis de conduire numérique"), il devient urgent de considérer que tout utilisateur du numérique devrait bénéficier d'une formation minimale avant d'accéder à certains outils critiques.

Cette formation doit aussi promouvoir les bases d’une véritable hygiène de vie numérique, c'est-à-dire l'adoption de gestes et comportements simples (mots de passe robustes, mises à jour, vigilance face aux messages suspects, protection des données personnelles, etc.) permettant de limiter efficacement les risques au quotidien.

Cette formation doit pouvoir se décliner à différents niveaux (initiation, perfectionnement, métiers spécifiques) et toucher tous les publics : scolaires, particuliers, salariés, décideurs.

7. Conclusion

Cette étude OSINT [1], consacrée aux compromissions par stealers [2] en Nouvelle-Calédonie, met en lumière une situation préoccupante et souvent invisible : des centaines de postes compromis, des dizaines d'alertes hebdomadaires, et des données personnelles, professionnelles et administratives régulièrement exfiltrées, sans que les victimes n'en aient conscience.

En adoptant une double approche, avec une analyse classique des fuites associées aux domaines en .nc, et une identification directe de machines locales compromises, cette enquête apporte un éclairage inédit sur la réalité du risque cyber dans un territoire insulaire. Elle montre que les compromissions ne concernent pas seulement les grandes structures ou les pays fortement industrialisés et peuplés, mais aussi des communautés plus restreintes, où les effets peuvent être amplifiés par la proximité sociale, l'interconnexion professionnelle, et l'insuffisance de structures spécialisées en cybersécurité.

Cette étude révèle également que la menace est persistante, actuelle et sous-estimée. Les données collectées ne représentent qu'une fraction visible d'un phénomène probablement bien plus large : un seul type de malware [7], une seule famille de fuites (publiques), et une méthodologie volontairement non intrusive. Le nombre réel de victimes est donc certainement bien supérieur à ce qui est documenté ici.

Malgré ce constat, des leviers d'action existent. Les recommandations proposées soulignent l'importance d'une réponse globale, collective, adaptée à chaque niveau : utilisateurs, entreprises, institutions. La formation, la coopération locale et régionale, et la mise en œuvre de pratiques simples mais structurées doivent être au cœur de la réponse.

Enfin, cette étude ne se veut pas exhaustive ni définitive. Elle constitue un point de départ, un socle factuel sur lequel il est possible de construire une meilleure résilience numérique pour la Nouvelle-Calédonie. Ce travail devra être prolongé, peut-être élargi à d'autres menaces, mais assurément inscrit dans une dynamique continue d'observation, de pédagogie et d'anticipation.

8. Annexes

Annexe 1 - Exemples de services compromis en NC

Les domaines suivants ont été identifiés dans les logs analysés. Ils sont regroupés par catégorie, sans indication d'identifiants spécifiques. Ils reflètent une diversité d'usages, tant personnels que professionnels, sur le territoire calédonien.

Remarque importante : La liste ci-dessous n'est pas exhaustive, de plus, la présence d'un domaine dans les résultats ne signifie pas que le service en lui-même a été compromis. Cette présence indique seulement qu'un utilisateur a saisi ses identifiants sur un site de ce domaine depuis un poste compromis.

- Services publics et collectivités : connect.gouv.nc, province-sud.nc, province-nord.nc, isee.nc
- Éducation et enseignement supérieur : ac-noumea.nc, univ-nc.nc, unc.nc
- Santé et protection sociale : cafat.nc, mdf.nc, caledobio.nc
- Banques et finances : bci.nc, bnc.nc, societegenerale.nc
- Télécoms et fournisseurs d'accès : opt.nc, lagoon.nc, canl.nc, mls.nc
- Énergie et services aux usagers : enercal.nc, eec.nc, cde.nc
- Transport et logistique : aircalin.nc, airfrance.nc, taneo.nc
- Entreprises et services professionnels : cci.nc, sln.nc
- Loisirs, sports et médias : oceanefm.nc, legratuit.nc, lnc.nc

Annexe 2 - Exemple de contenu d'un log typique (anonymisé)

Élément	Valeur
IP publique	202.22.xxx.xxx
Nom d'hôte	PC-BUREAU-ALICE
OS	Windows 11 Pro
Langue / fuseau horaire	Français / UTC+11
Date du log	23/04/2025 20:32:10
Navigateur	Chrome 126
Sites identifiés	Amazon, Facebook, Banque X, Tiktok, etc.
Nombre d'identifiants récupérés	283
Cookies de session	52
Fichiers sensibles	.docx, .xlsx, .dwg (AutoCAD), wallet.txt
Données personnelles détectées	Nom, prénom, date de naissance, CB

Tableau 1 : Contenu d'un log de stealer

Annexe 3 - Suivi hebdomadaire des compromissions (janvier 2024 - avril 2025)

Un graphique chronologique figure dans le rapport principal (page 8, figure 1). En voici un aperçu synthétique :

- Moyenne hebdomadaire : environ 15 alertes,
- Pics observés : 40 à 50 alertes sur certaines semaines,
- Tendance : variabilité potentiellement élevée d'une semaine à l'autre, pas de tendance à la baisse notée.

Annexe 4 - Glossaire OSINT et cybersécurité

[1] : OSINT. Open Source Intelligence. Collecte d'informations accessibles publiquement.

[2] : Stealer. Logiciel malveillant conçu pour voler des données (identifiants, cookies, fichiers, ...).

[3] : Deep web. Partie d'Internet non indexée par les moteurs de recherche classiques (ex. : intranets, bases privées).

[4] : Dark web. Sous-ensemble du deep web accessible par des réseaux anonymes comme Tor, souvent utilisé pour des activités illégales.

[5] : Dump de données. Fichier contenant des données volées, souvent diffusé ou vendu après un piratage.

[6] : Cookie de session. Fichier qui maintient la connexion à un site web après authentification.

[7] : Malware. Abréviation de malicious software (logiciel malveillant). Logiciel malveillant destiné à perturber, à espionner ou à compromettre un système.

[8] : EDR, Endpoint Detection and Response. Outil de détection comportementale.

[9] : IDS/IPS. Systèmes de détection/prévention d'intrusion, analysant le trafic réseau pour identifier et bloquer les menaces.

[10] : Crack. Logiciel ou méthode permettant de contourner la protection d'un programme (ex. : activation sans licence).

[11] : Phishing. Hameçonnage en français. Technique de fraude visant à tromper l'utilisateur pour obtenir ses informations sensibles (mots de passe, CB, etc.).

[12] : CERT/CSIRT. Équipe spécialisée dans la gestion des incidents de sécurité informatique au sein d'un État ou d'une organisation.

9. Bibliographie commentée

Sources de données OSINT

- Have I Been Pwned (HIBP) : base publique d'adresses de courrier électronique compromises, utile pour les premières vérifications.
- DeHashed.com : moteur de recherche d'identifiants compromis plus détaillé, avec capacités de requêtes par domaine.
- IntelligenceX.com : plateforme de recherche avancée utilisée pour interroger des dumps [5] liés aux stealers [2].
- Telegram (canaux publics spécialisés) : surveillance passive de canaux diffusant des logs volés.

Références institutionnelles et techniques

Les références ci-dessous n'ont pas nécessairement été mobilisées directement dans cette étude, mais elles constituent des ressources fiables et complémentaires pour mieux comprendre les enjeux abordés et mettre en œuvre les recommandations proposées :

- ANSSI, Guide d'hygiène informatique : bonnes pratiques essentielles pour les organisations et les particuliers.

  https://cyber.gouv.fr/publications/guide-dhygiene-informatique
- CNIL, Guide de la sécurité des données personnelles : cadre de référence pour la gestion des données personnelles.

  https://www.cnil.fr/fr/guide-de-la-securite-des-donnees-personnelles-nouvelle-edition-2024
- NIST, Framework for Improving Critical Infrastructure Cybersecurity : un cadre reconnu internationalement pour structurer les actions de cybersécurité.

  https://csrc.nist.gov/pubs/cswp/6/cybersecurity-framework-v11/final
- MITRE ATT&CK : base de connaissances sur les techniques des acteurs malveillants, incluant les stealers [2]. https://attack.mitre.org
- (ISC)², Cybersecurity Workforce Study : rapport annuel sur les tendances, besoins et lacunes en compétences dans le domaine de la cybersécurité.

  https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study

10. À propos de l'auteur

Laurent Rivaton est consultant en cybersécurité, fondateur de **AdDo**, société de cybersécurité spécialisée dans l'audit, le conseil et la formation.

Il intervient régulièrement auprès des entreprises et organisations publiques et privées et mène depuis plusieurs années des travaux de recherche appliquée sur les compromissions de données et la sensibilisation à la sécurité numérique.

Il est certifié CISSP, CCISO, CEH, OSCP, OSCE, ..., et s'implique activement dans le développement de la culture cyber du Caillou, en particulier à titre bénévole au sein du **Cluster OPEN NC** et du **Centre Cyber du Pacifique**, deux structures engagées dans la diffusion d'une culture numérique responsable en Nouvelle-Calédonie et dans sa région.