RAPPORT D'ACTIVITÉ DES CSIRT TERRITORIAUX

2024

ÉDITO

VINCENT STRUBEL

DIRECTEUR GÉNÉRAL DE L'ANSSI

La menace cybercriminelle s'est largement amplifiée et cible désormais une variété d'acteurs de plus en plus étendue. Les TPE, PME, ETI, associations et collectivités territoriales sont aujourd'hui fréquemment victimes d'attaques opportunistes à des fins d'extorsion. La création de CSIRT ministériels, sectoriels et territoriaux est une des réponses à cette progression des cyberattaques, notamment via leur mission principale de réponse à incident. C'est pourquoi l'ANSSI encourage et soutient depuis 2021 leur émergence. Portés par les Régions, les CSIRT territoriaux participent à renforcer les actions de prévention et d'assistance dans les territoires. En 2024, a eu lieu le lancement opérationnel de nouveaux CSIRT territoriaux, situés dans les territoires ultramarins : le CSIRT ATLANTIC, le Centre cyber du Pacifique et le CSIRT La Réunion. La France compte désormais 15 CSIRT territoriaux, qui sont des interlocuteurs au plus près des enjeux et problématiques locaux.

Pour répondre à l'enjeu de massification de la menace, la révision de la directive européenne sur la sécurité des réseaux et des systèmes d'information, dite « NIS 2 », vise à faire monter en maturité cyber l'ensemble des chaînes de valeur de notre économie et de nos services publics en élargissant le nombre d'entités concernées par les exigences de cybersécurité à plusieurs milliers d'entités. Ce changement d'échelle ne pourra se faire qu'avec l'aide d'une communauté de relais (associations, fédérations professionnelles, CSIRT,

prestataires privés,...) capables de mener des actions de prévention et de sensibilisation auprès des entités concernées. Les CSIRT territoriaux, au plus proche des tissus économiques et administratifs dans les territoires, jouent déjà activement ce rôle. Ils s'appuient sur l'ensemble de l'écosystème des prestataires de cybersécurité pour investiguer, remédier, restaurer et renforcer les systèmes d'information. Cet écosystème est au cœur du fonctionnement de la politique publique de développement du numérique dans les territoires.

Afin de consolider les capacités des CSIRT en matière de réponse et de sensibilisation, le CERT-FR de l'ANSSI et les CSIRT territoriaux échangent régulièrement sur des problématiques de connaissance de la menace et de réponse aux incidents. Ces réunions opérationnelles fréquentes sont essentielles pour créer les conditions favorables au développement d'une communauté de CSIRT soudée et coordonnée. Cette coopération opérationnelle entre le CERT-FR et les CSIRT territoriaux a été renforcée en 2024 avec la mise en place des renvois d'appels téléphoniques entre la plupart des CSIRT territoriaux et le CERT-FR afin d'assurer une continuité dans la réponse à incident, y compris en heures non ouvrées, au bénéfice des victimes. Par ailleurs, dans le même objectif de renforcer l'assistance aux victimes, l'ANSSI soutient et finance l'intégration des CSIRT territoriaux à la plateforme 17Cyber portée par le groupement d'intérêt public ACYMA (Action contre la cybermalveillance) en partenariat avec la Police nationale et la Gendarmerie nationale. L'objectif de ces différentes actions est qu'une victime, quels que soient ses besoins, trouve toujours facilement le bon interlocuteur.

Les CSIRT territoriaux, comme le montre ce rapport d'activité, se positionnent progressivement comme des acteurs clés des écosystèmes cyber locaux. Ce rapport témoigne à ce titre de la pertinence de ce modèle de politique publique innovant, ce travail en réseau, qui inspire aujourd'hui d'autres Etats.

Les CSIRT territoriaux sont des partenaires privilégiés de l'ANSSI. Face à la menace, c'est en travaillant de concert que nous atteindrons notre ambition commune de résilience cyber.

INTRODUCTION

LANCÉ EN 2021, UN COLLECTIF DES CSIRT TERRITORIAUX QUI ARRIVE À MATURITÉ

Issus d'un projet du plan France Relance de 2021, les *Computer Security Incident Response Team* (ou CSIRT) territoriaux sont des centres de réponse aux incidents cyber implantés en région, au plus près des entités de leurs territoires. Ils traitent les demandes d'assistance des petites et moyennes entreprises, les entreprises de taille intermédiaire, les collectivités territoriales et les associations. Ils mettent en relation les entités victimes d'incidents de sécurité avec des partenaires de proximité : prestataires de réponse à incident et partenaires étatiques.

L'émergence de ces CSIRT a permis de fournir localement un service personnalisé de réponse à incident de premier niveau gratuit, complémentaire de celui proposé par les prestataires privés, la plateforme Cybermalveillance.gouv.fr au travers de son service 17Cyber et des services de l'autorité nationale du CERT-FR.

Ces CSIRT territoriaux opèrent également des missions de prévention, sensibilisation et d'accompagnement dans la montée en maturité des acteurs de leurs territoires associés à la dynamique de déploiement des campus cyber dans les régions.

Le dispositif est à ce jour constitué de 15 CSIRT territoriaux opérationnels.

4 CSIRT territoriaux ont déjà rejoint l'InterCERT France, la première communauté française de CERT. Il s'agit des CSIRT des régions Bourgogne Franche Comté, Bretagne, Ile-de-France et récemment Provence Alpes Côte d'Azur.

FRISE CHRONOLOGIQUE AVEC LES DATES D'OUVERTURE DES DIFFÉRENTS CSIRT TERRITORIAUX

** Carte et fiches d'identités des CSIRT territoriaux en annexe pages 40 et 41.*

16/05/2022

NORMANDIE

CSIRT NORMANDIE CYBER

03/10/2022

BOURGOGNE-FRANCHE-COMTÉ

CSIRT BOURGOGNE-FRANCHE-COMTÉ

14/02/2023

GRAND EST

GRAND EST CYBERSÉCURITÉ

01/04/2023

NOUVELLE-AQUITAINE

CENTRE DE RÉPONSE AUX INCIDENTS CYBER NOUVELLE-AQUITAINE

16/03/2023

HAUTS-DE-FRANCE

CSIRT HAUTS-DE-FRANCE

15/03/2023

OCCITANIE

CSIRT OCCITANIE

14/09/2023

PAYS DE LA LOIRE

PAYS DE LA LOIRE CYBERASSISTANCE

21/11/2023

BRETAGNE

BREIZH CYBER

04/12/2023

ÎLE-DE-FRANCE

URGENCE CYBER ILE-DE-FRANCE

17/04/2024

PROVENCE ALPES CÔTE D'AZUR

URGENCE CYBER RÉGION SUD

03/04/2024

CORSE

CYBER CORSICA

20/03/2024

CENTRE-VAL DE LOIRE

CYBERÉPONSE

30/07/2024

OCÉAN ATLANTIQUE

CSIRT ATLANTIC

24/10/2024

OCÉAN PACIFIQUE

CENTRE CYBER DU PACIFIQUE

04/11/2024

OCÉAN INDIEN

CSIRT RÉUNION

2024, UNE ANNÉE CHARNIÈRE POUR LES CSIRT TERRITORIAUX

En 2024, tous les CSIRT territoriaux ont débuté leurs opérations. Ainsi, 2024 marque la première année d'un dispositif pleinement fonctionnel, offrant une première évaluation concrète de l'impact des CSIRT territoriaux.

L'année 2024 a été marquée par un renforcement individuel et collectif des CSIRT régionaux. Grâce au déploiement de leurs capacités opérationnelles, à l'élaboration de bonnes pratiques et de procédures à l'état de l'art, ainsi qu'à la mutualisation de certaines actions, le collectif des CSIRT territoriaux a renforcé sa réactivité et optimisé la réponse aux cyberattaques, au service des acteurs locaux. De nombreuses initiatives spécifiques ont été lancées dans les différentes régions, contribuant à mettre en lumière les enjeux de la cybersécurité au plus près des territoires.

Par ailleurs, au cours de l'année 2024, les territoires ultra-marins ont développé des CSIRT dans les trois grands espaces géographiques où la France est présente : l'océan Atlantique, l'océan Indien et l'océan Pacifique.

Ces centres, adaptés aux réalités économiques, sociales, culturelles et géopolitiques de leurs régions respectives, assurent une présence locale déterminante. Ils renforcent la sécurité numérique et protègent ainsi les TPE, PME, ETI, collectivités et associations de leurs territoires.

Enfin, le développement des campus cyber territoriaux a également marqué cette année 2024. Ces campus territoriaux, déclinés du modèle du campus cyber basé à la Défense, s'implantent dans différentes régions françaises. Ils visent à fédérer et animer l'écosystème cybersécurité régional sur différents axes comme le développement de la filière cybersécurité, la diversification et des formations des professionnels dans un contexte de tension sur les effectifs dans le secteur, l'intégration et le transfert d'innovations dans les offres et la diffusion d'une culture cyber auprès de tous les publics. Cette dynamique des campus cyber territoriaux est vertueuse pour les CSIRT territoriaux par la dynamique créée et les opportunités que ces campus développent dans les territoires.

FRISE CHRONOLOGIQUE AVEC LES DATES D'OUVERTURE DES DIFFÉRENTS CAMPUS CYBER TERRITORIAUX

08/06/2022

HAUTS-DE-FRANCE

CAMPUS CYBER HAUTS-DE-FRANCE
LILLE MÉTROPOLE

06/04/2023

NOUVELLE-AQUITAINE

CAMPUS RÉGIONAL DE CYBERSÉCURITÉ ET DE CONFIANCE NUMÉRIQUE NOUVELLE-AQUITAINE

26/04/2024

BRETAGNE

BRETAGNE CYBER ALLIANCE

12/09/2024

NORMANDIE

CAMPUS CYBER NORMANDIE

22/10/2024

RÉGION SUD

CAMPUS CYBER RÉGION SUD

À VENIR OU EN PROJET

OCCITANIE

CAMPUS CYBER OCC'

GRAND EST

CAMPUS CYBER GRAND EST

CENTRE-VAL DE LOIRE

CAMPUS CYBER CENTRE-VAL DE LOIRE

AUVERGNE-RHÔNE-ALPES

CAMPUS RÉGION DU NUMÉRIQUE

I

MENACE OBSERVÉE PAR LES CSIRT TERRITORIAUX

A
INTRODUCTION

La menace cyber observée par les CSIRT territoriaux illustre les observations documentées dans le rapport de la cybermenace 2024 proposée par le CERT-FR. La menace se décompose en une menace systémique composée de groupes cybercriminels, d'hacktivistes opérant des actions de déstabilisation et d'une menace de niveau stratégique composée d'acteurs sponsorisés par des États.

Les cibles couvertes par les CSIRT territoriaux à savoir les entreprises de petite taille jusqu'au entreprises de taille intermédiaire, les collectivités territoriales et les associations sont essentiellement concernées par la menace criminelle et hacktiviste.

La menace stratégique s'intéresse à des acteurs spécifiques, grands groupes dans les secteurs d'activité critiques (ex. industrie pharmaceutique, industrie de défense, industrie aéronautique, etc.), acteurs publics sensibles qui sont soit couverts par le CERT-FR en tant que CERT gouvernemental ou CERT national pour des acteurs régulés. Il existe également des CERT sectoriels qui couvre des acteurs spécifiques d'un secteur comme le CERT-ED pour les entreprises de défense, le CERT-Aviation pour les acteurs du secteur aéronautique et aérien, le M-CERT pour les acteurs du secteur maritime et le CERT-Santé pour les établissements de soin.

Ce rapport couvre la menace qui concerne les bénéficiaires des CSIRT territoriaux et donc essentiellement la menace criminelle et hacktiviste.

La menace hacktiviste, notamment celle de groupes pro-russes touche les collectivités locales en particulier. Le groupe le plus actif en 2024 est le groupe pro-russe *NoName057(16)* impliqué dans le cadre de la guerre entre l'Ukraine et la Russie. Cette menace se matérialise par des attaques en déni de service d'impacts hétérogènes mais toujours de durée limitée (moins d'une heure à plusieurs heures au maximum en général). Cette menace engendre donc des impacts limités même si la médiatisation de ces actions, parfois par les entités victimes elles-mêmes, peut être importante.

À l'inverse, les groupes cybercriminels opérant des attaques par rançongiciel engendrent des impacts très lourds sur les entités victimes, entités publiques ou privées, parfois mettant en incapacité la victime à délivrer ses services critiques. Cela se traduit concrètement par un service public dégradé pour les entités publiques et des pertes d'exploitation très sérieuses pour les entités privées. Les effets de ces attaques par ailleurs perdurent dans le temps avec des impacts s'étalant sur plusieurs mois voire plusieurs années.

L'année 2024 a été marquée en France par la tenue des Jeux Olympiques et Paralympiques de Paris à l'été. Un dispositif avec des moyens très importants a été mis en place sous l'égide de l'ANSSI pour sécuriser l'ensemble des opérations associées à cet événement d'envergure mondiale. Dans ce dispositif, les CSIRT territoriaux ont été positionnés dans un rôle d'appui des acteurs du périmètre de leurs bénéficiaires naturels et impliqués dans l'accueil des épreuves olympiques par exemple des collectivités locales dans lesquelles se déroulaient certaines épreuves des Jeux Olympiques en dehors de la plaque parisienne.

B
LA MENACE RANÇONGICIEL

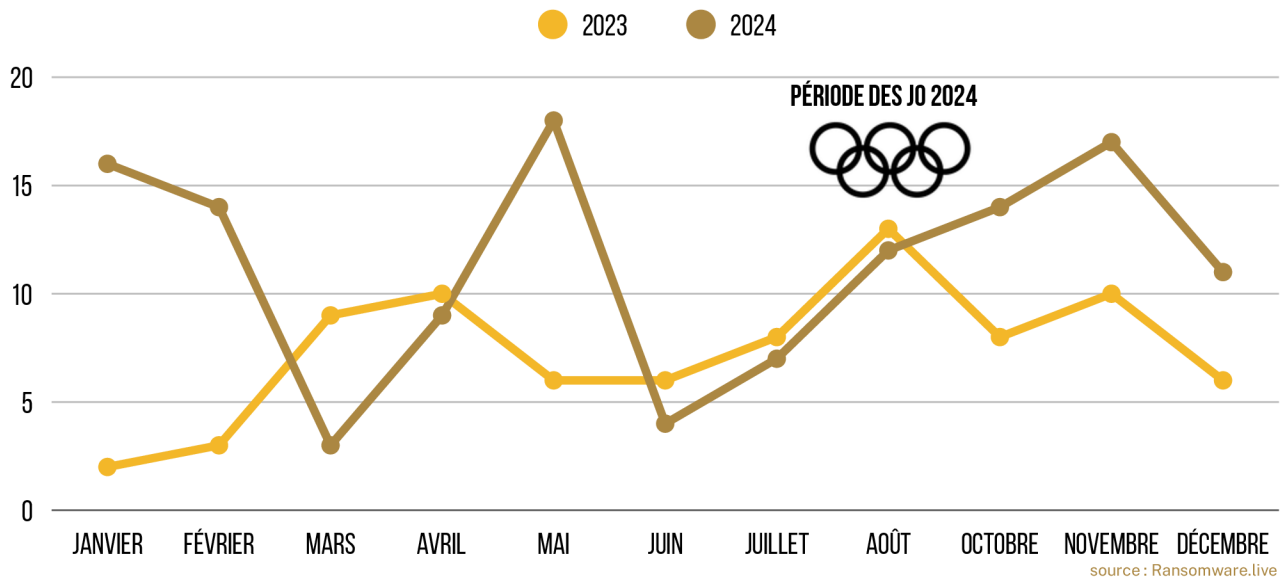
Sur la base des sites web spécialisés dans le suivi des activités des groupes criminels de haut niveau opérant des attaques par rançongiciel, il est possible de dégager les tendances marquantes de l'évolution de ces groupes ainsi que de donner un aperçu de cette activité cybercriminelle sur le territoire national. Les statistiques présentées sont issues du site *Ransomware.live*. Celles-ci ne comprennent par définition que les revendications publiques des attaquants.

Entre 2023 et 2024, les attaques revendiquées sur la France ont augmenté de 90 à 128 au total. Ces chiffres sont cohérents avec les données du panorama de la menace 2024 de l'ANSSI (144 en 2024 contre 143 en 2023) et suggèrent une menace plutôt stable. La tenue des Jeux Olympiques de Paris 2024 n'a pas entraîné d'augmentation significative des attaques par rançongiciel sur la période olympique. Les victimes françaises représentent 5,6% de l'ensemble des victimes des groupes criminels dans le monde et la France fait partie du top 10 des pays les plus visés. Les États-Unis représentent à eux seuls 42% des victimes.

Les groupes criminels les plus actifs en France ont évolué, suivant à la fois les réorganisations des groupes eux-mêmes et des actions judiciaires qui ont marqué l'année 2024. Les faits principaux sont le retrait très net du groupe LockBit 3.0 à compter du deuxième semestre suite à l'opération judiciaire internationale CRONOS en février 2024 et l'annonce de l'identification et les sanctions prises contre le leader du groupe criminel LockBit Dmitry Khoroshev, alias LockBitSupp en mai 2024.

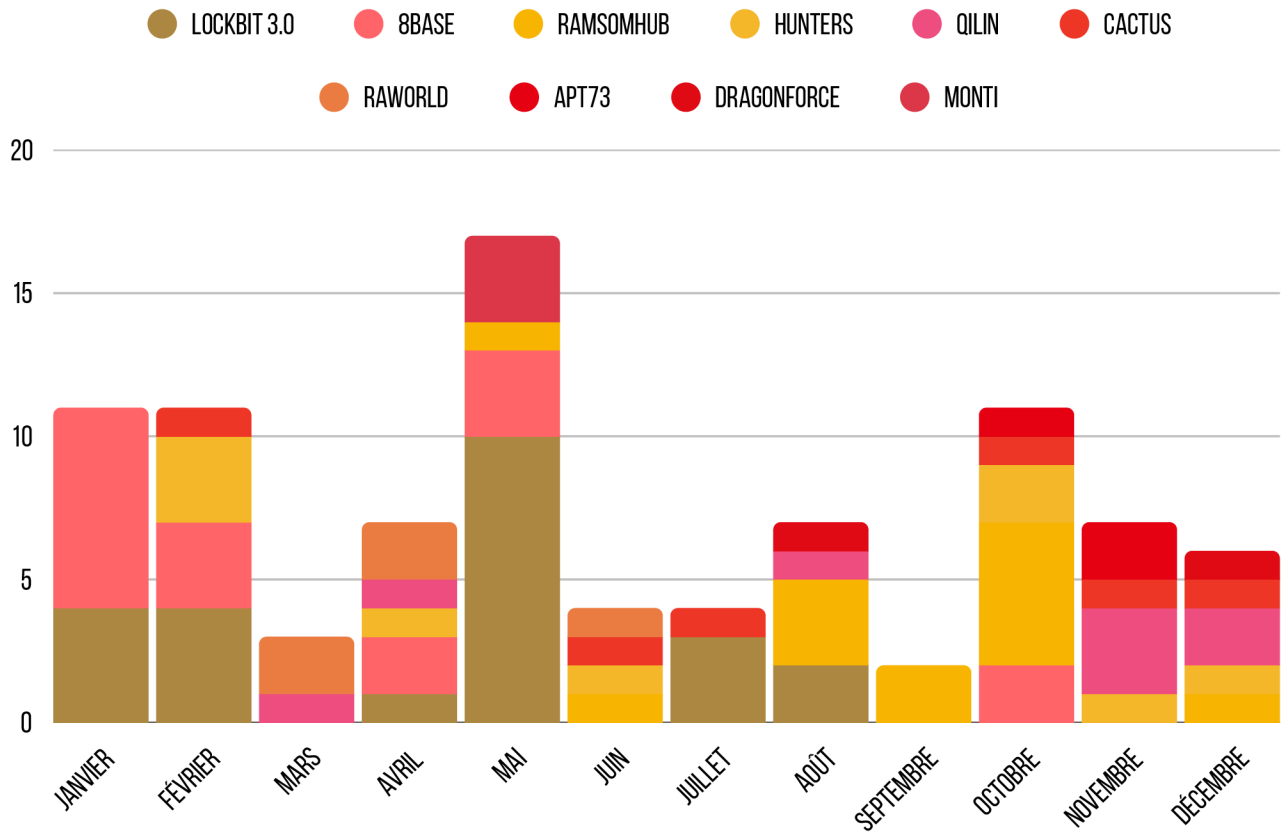
Ce groupe représentait à lui-seul quasiment le quart des attaques en 2023. L'autre fait notable est la montée en puissance du groupe RansomHub qui devient le groupe criminel le plus actif dans le monde et un des plus actifs en France.

NOMBRE DE VICTIMES FRANÇAISE PAR MOIS



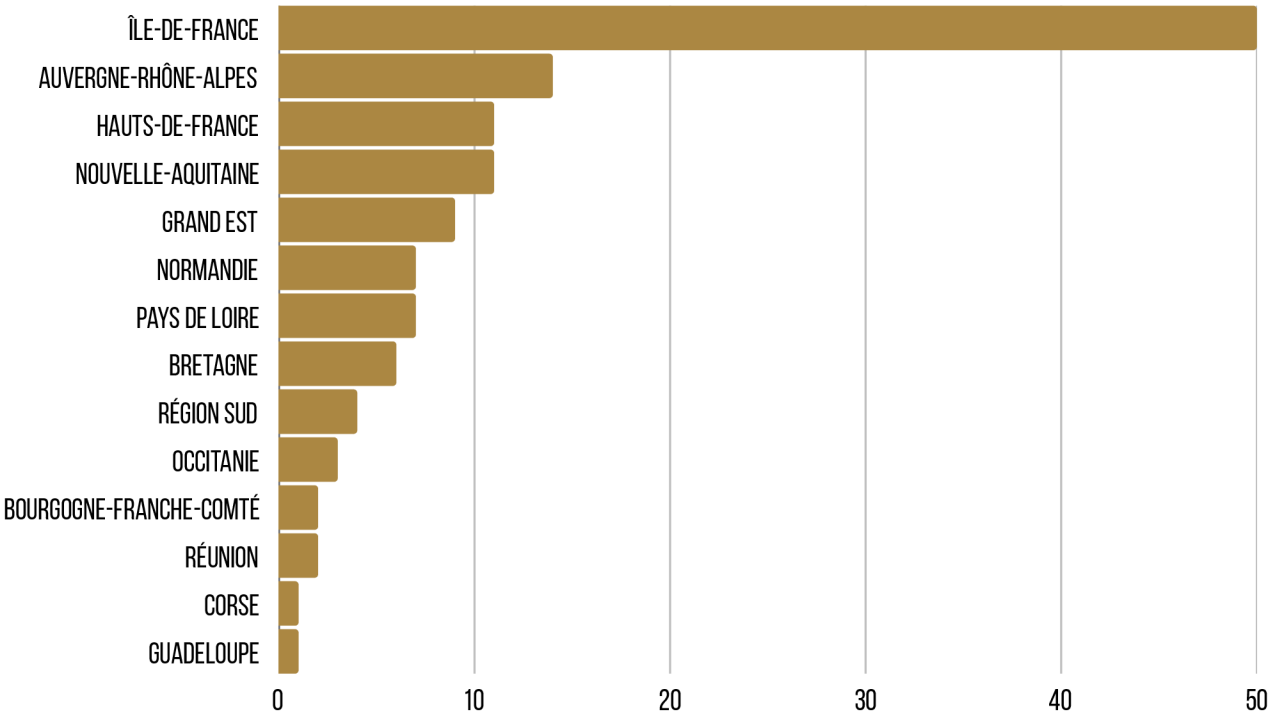
source : Ransomware.live

ACTIVITÉ MENSUELLE DES 10 GROUPES CRIMINELS LES PLUS ACTIFS EN FRANCE



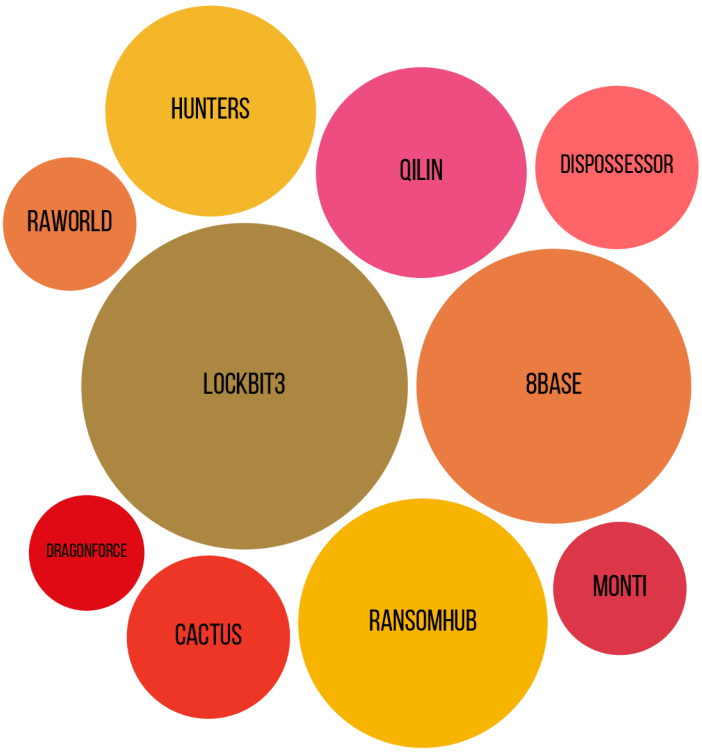
source : Ransomware.live

NNOMBRE DE VICTIMES PAR RÉGION EN FRANCE



source : Ransomware.live

NOMBRE D'ATTAQUES REVENDIQUÉES PAR LES GROUPES CRIMINELS EN FRANCE



LOCKBIT3	24
8BASE	17
RANSOMHUB	14
QILIN	10
HUNTERS	10
CACTUS	6
DISPOSSESSOR	6
MONTI	4
RAWORLD	4
DRAGONFORCE	3

source : Ransomware.live

La répartition des attaques par région montre que le nombre de victimes est de manière approximative corrélé au poids économique de chaque région. Cette observation montre bien que l'activité criminelle ne cible pas ses victimes mais fonctionne bien de manière aléatoire selon des opportunités offertes par des entités insuffisamment sécurisées ou via des identifiants récupérés par la criminalité des *Initial Access Brokers* de manière non discriminée.

Les attaques par rançongiciel se distinguent en attaques par simple extorsion (l'attaquant chiffre des données et demande une rançon pour la clé de déchiffrement) ou par double extorsion (l'attaquant chiffre et exfiltre des données, avec menace de publication ou de vente des données volées si la rançon n'est pas payée en plus de la rançon pour la clé de déchiffrement).

Les groupes criminels pratiquant les attaques par rançongiciel peuvent être classées en deux catégories.

Tout d'abord, des acteurs criminels affiliés à un (ou plusieurs) groupe(s) criminel(s) avec qui ils partagent les revenus souvent via le modèle du Ransomware-as-a-Service (RaaS). La plupart de ces acteurs pratiquent la double extorsion en publiant les données sur les sites des groupes criminels avec qui ils sont affiliés. C'est la menace la plus connue notamment au travers des revendications de ces groupes sur leurs sites vitrines, ce qui rend cette menace visible. Les CSIRT territoriaux observent toutefois que certains incidents menés par des affiliés de groupes criminels ne conduisent pas systématiquement à des publications sur les sites vitrines des groupes concernés y compris sans paiement de la rançon.

Mais il existe également des acteurs indépendants qui opèrent de manière autonome, et souvent réutilisent des outils développés par des groupes criminels de type RaaS « tombés » dans le domaine public. La plupart du temps ces acteurs pratiquent la simple extorsion.

Ces acteurs, moins visibles car ne disposant pas de site « vitrine » sur le dark web, ont souvent des capacités plus limitées et un niveau de technicité plus faible. Mais ils visent des cibles eux-mêmes avec un niveau de maturité plus faibles, comme des TPE et PME.

Par exemple, parmi ces acteurs, le groupe criminel *DiskStation Security* s'est spécialisé dans la compromission de serveurs de la marque Synology mal sécurisés exposés sur Internet. Ces équipements sont répandus dans les organisations de taille petite et moyenne. Les CSIRT territoriaux ont traité plusieurs incidents de ce groupe criminel utilisant ce mode opératoire.

LA MENACE RANÇONGICIEL SE DÉCOMPOSE EN DEUX SOUS-ENSEMBLES DES ACTEURS ORGANISÉS SELON LE MODÈLE DU RANSOMWARE-AS-A-SERVICE AVEC AFFILIATION ET LES ACTEURS INDÉPENDANTS QUI REPRÉSENTENT UNE MENACE MOINS VISIBLE MAIS TOUT AUSSI IMPACTANTE

C
AUTRES FAITS MARQUANTS

L'année 2024 a été ponctuée par des incidents spécifiques, en particulier des attaques par la chaîne d'approvisionnement logiciel. Un incident en particulier a retenu l'attention des CSIRT territoriaux, la compromission de l'entreprise Octave, éditeur de solution ERP en mode SaaS pour le secteur du commerce de détail. L'attaque survenue le 16 août 2024 sur leur infrastructure, a entraîné avec elle une grande partie des 80 à 90 clients d'Octave, entreprises de commerce de taille petite à moyenne. L'impact a été immédiat et souvent catastrophique pour les clients de l'éditeur, car une solution ERP est au cœur du fonctionnement d'une entreprise de commerce (prise de commandes, gestion des stocks, facturations, etc.). Les systèmes de l'éditeur ont globalement repris entre 2 et 3 mois après la survenue de l'incident. Octave a été placé en redressement judiciaire en novembre 2024 et a été finalement placé en liquidation judiciaire le 19 mars 2025.

Autre incident de même nature, en décembre 2023, la société Coaxis, hébergeur de solutions métier pour les experts comptables, a subi une attaque par rançongiciel par le groupe criminel LockBit 3.0. Le CSIRT de la Région Nouvelle Aquitaine et divers partenaires se sont ainsi rapidement mobilisés. L'incident a révélé une compromission majeure avec 2 500 machines virtuelles affectées. Les centres de données de l'entreprise ont été touchés, nécessitant un accompagnement minutieux des clients et des cabinets comptables. Le rétablissement des services a débuté le 17 décembre, avec une tolérance de l'URSSAF pour les déclarations retardées jusqu'en janvier 2024. Malgré ces efforts, certains cabinets peinaient encore à récupérer l'accès à leurs outils en début d'année, prolongeant les mesures de soutien.

Ces événements, impliquant un fournisseur logiciel en mode SaaS et de nombreux clients victimes mettent en lumière l'importance de la coordination de la réponse face aux cybermenaces. Dans le cas de ces attaques par la chaine d'approvisionnement logiciel, la réponse se fait au niveau de l'éditeur victime, sa capacité à remettre en service ses opérations et assurer une reprise d'activité pour ses clients étant la clé de la gestion de crise.

Enfin, de nombreux incidents relatifs à des exfiltrations de données de grande ampleur en dehors d'attaques par rançongiciel ont également été observés auprès d'enseignes de commerce en ligne notamment. Ces fuites de données massives soulignent une nouvelle tendance criminelle de vol et de revente de données commerciales ou techniques. Les cibles visées sont les entités qui regroupent une quantité très importante de données individuelles d'organisations publiques ou privées.

II

ÉVÉNEMENTS TRAITÉS PAR LES CSIRT TERRITORIAUX

A
SYNTHÈSE SUR LES ÉVÉNEMENTS TRAITÉS

En 2024, les CSIRT territoriaux ont traité 1387 événements de sécurité composés de 658 incidents et 729 signalements. Parmi ces incidents, les CSIRT territoriaux ont accompagné le traitement de 136 entités victimes de rançongiciels.

1387 ÉVÉNEMENTS DE SÉCURITÉ TRAITÉS PAR LES CSIRT TERRITORIAUX EN 2024

658 INCIDENTS TRAITÉS PAR LES CSIRT TERRITORIAUX EN 2024 DONT 136 ATTAQUES PAR RANÇONGICIEL

La taxonomie utilisée par les CSIRT territoriaux pour classer les événements de sécurité est disponible en annexe page 43. Elle précise la nature pour chaque type d'événement de sécurité c'est-à-dire si c'est un signalement ou un incident.

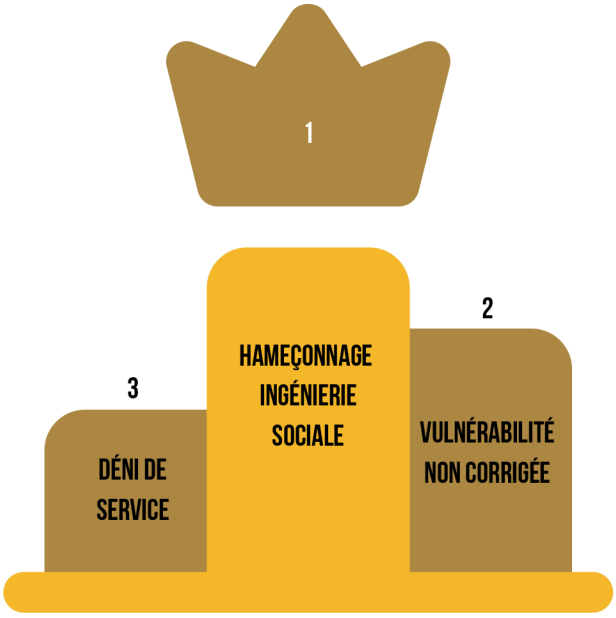
UN ÉVÉNEMENT DE SÉCURITÉ EST UN INCIDENT OU UN SIGNALEMENT PORTÉ À LA CONNAISSANCE DES CSIRT TERRITORIAUX ET QUI A DONNÉ LIEU À UN TRAITEMENT PAR LES ÉQUIPES OPÉRATIONNELLES.

UN SIGNALEMENT EST UN ÉVÉNEMENT DE SÉCURITÉ QUI CARACTÉRISE UN COMPORTEMENT ANORMAL OU INATTENDU D'UN SI POUVANT AVOIR UN CARACTÈRE MALVEILLANT OU OUVRIR LA VOIE À DES USAGES NÉFASTES À L'ENCONTRE D'UN SYSTÈME D'INFORMATION (EX. UN MESSAGE D'HAMEÇONNAGE, UNE VULNÉRABILITÉ NON CORRIGÉE SUR UN SYSTÈME EXPOSÉ SUR INTERNET, ETC.).

ENFIN, UN INCIDENT EST UN ÉVÉNEMENT DE SÉCURITÉ OÙ LES CSIRT TERRITORIAUX SONT EN MESURE DE CONFIRMER QU'UN ACTEUR MALVEILLANT A CONDUIT DES ACTIONS MALVEILLANTES AVEC SUCCÈS SUR UN SYSTÈME D'INFORMATION (EX. ATTAQUES PAR RANÇONGICIEL)

B
SIGNALEMENTS DE SÉCURITÉ

TOP 3 DES SIGNALEMENTS LES PLUS RENCONTRÉS

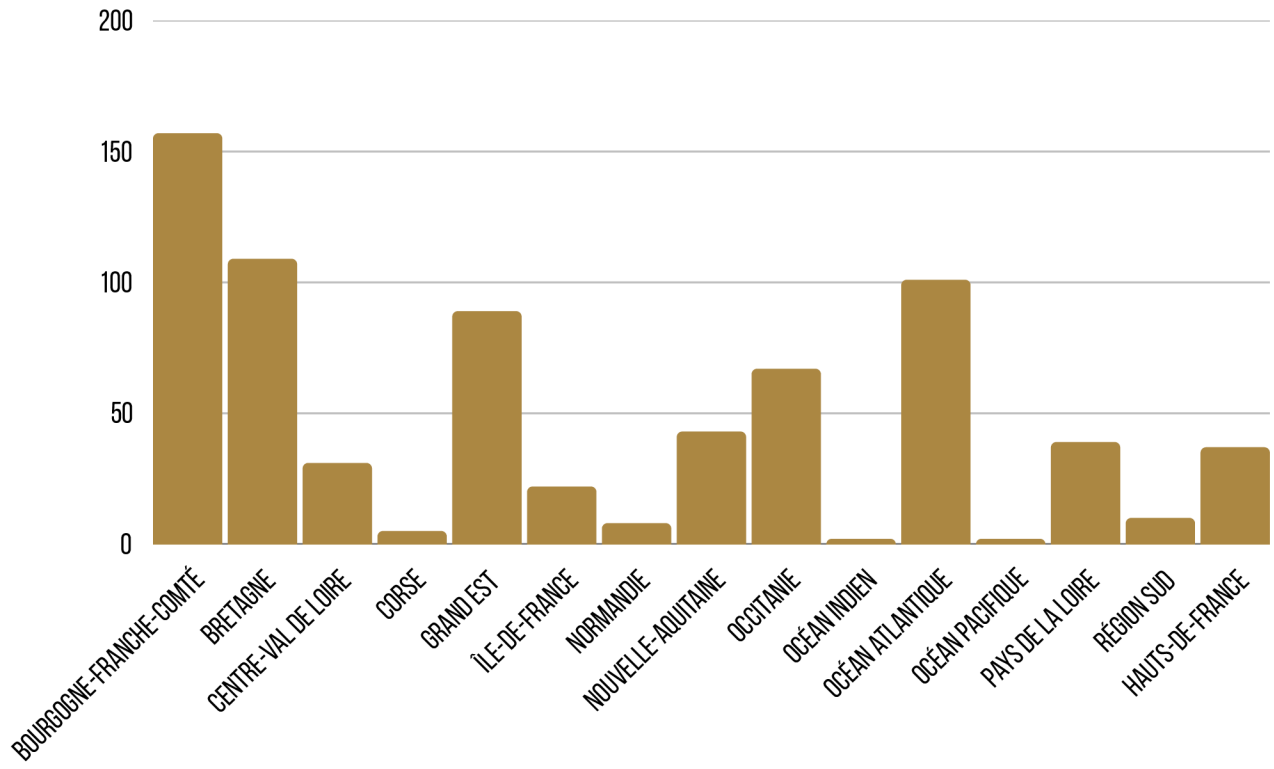


CES 3 TYPES DE SIGNALEMENTS REPRÉSENTENT PLUS DE 90% DES SIGNALEMENTS TRAITÉS PAR LES CSIRT TERRITORIAUX

Ces événements de sécurité pourraient être considérés comme moins importants. Ils sont toutefois potentiellement le germe d'incidents plus graves avec l'objectif en tant que défenseur d'arrêter un attaquant dans le déroulé de son action malveillante.

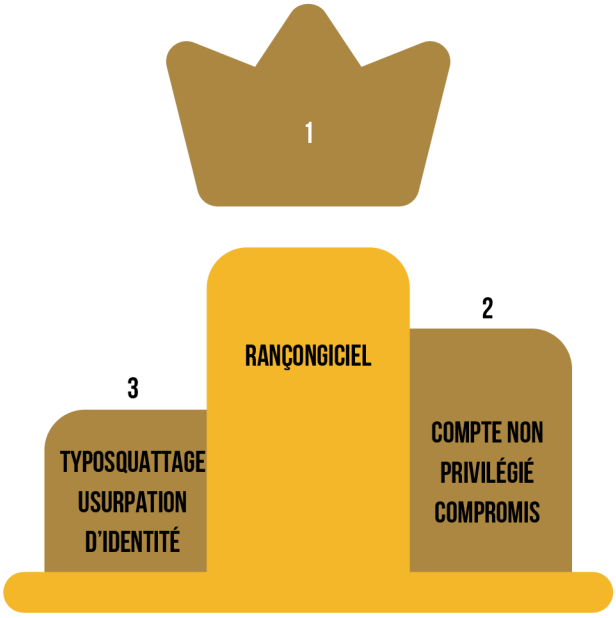
Par exemple, un compte de messagerie compromis à la suite d'un hameçonnage ou une vulnérabilité critique non corrigée sur un serveur exposé sont des vecteurs d'incidents pouvant être très graves. Leur résolution préventive diminue drastiquement les risques.

NOMBRE DE SIGNALEMENTS TRAITÉS PAR LES CSIRT TERRITORIAUX EN 2024



C
INCIDENTS DE SÉCURITÉ

TOP 3 DES INCIDENTS LES PLUS RENCONTRÉS

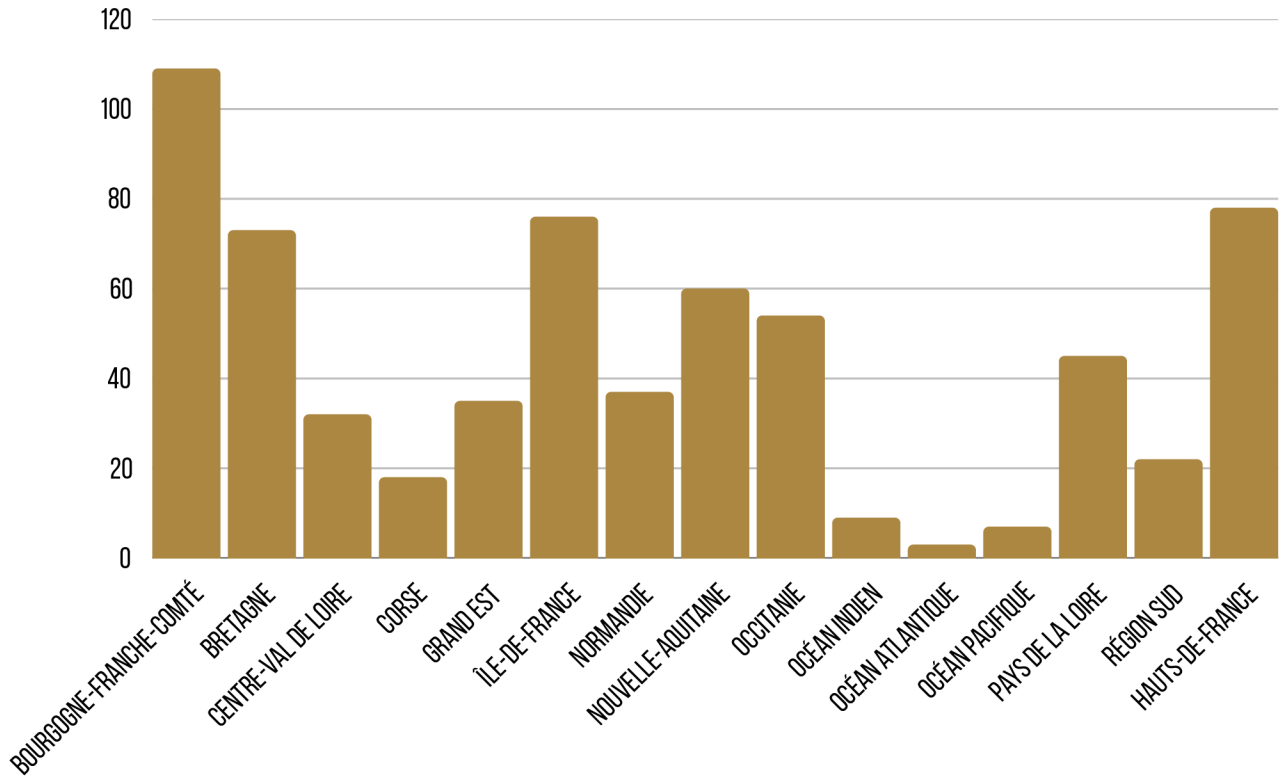


CES 3 TYPES D'INCIDENTS REPRÉSENTENT PLUS DE 50% DES INCIDENTS TRAITÉS PAR LES CSIRT TERRITORIAUX

Ces événements de sécurité matérialisent des incidents conduisant à des compromissions avérées de systèmes d'information. Il s'agit du cœur de métier des CSIRT territoriaux.

Parmi ces incidents, on distingue les incidents qui affectent très fortement le fonctionnement des SI comme les attaques par rançongiciel et des incidents de moindre envergure mais tout aussi importants à traiter.

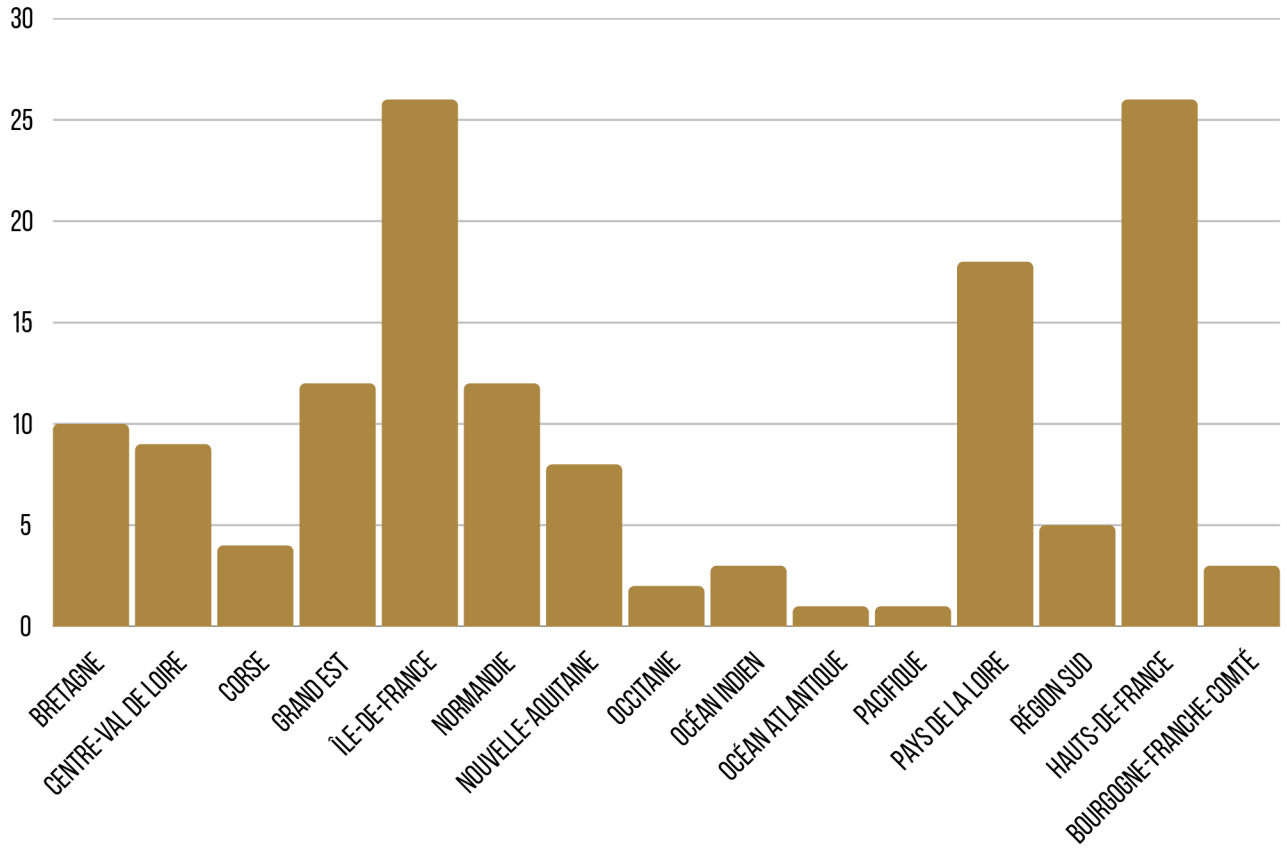
NOMBRE D'INCIDENTS TRAITÉS PAR LES CSIRT TERRITORIAUX EN 2024



D
ATTAQUES RANÇONGICIEL

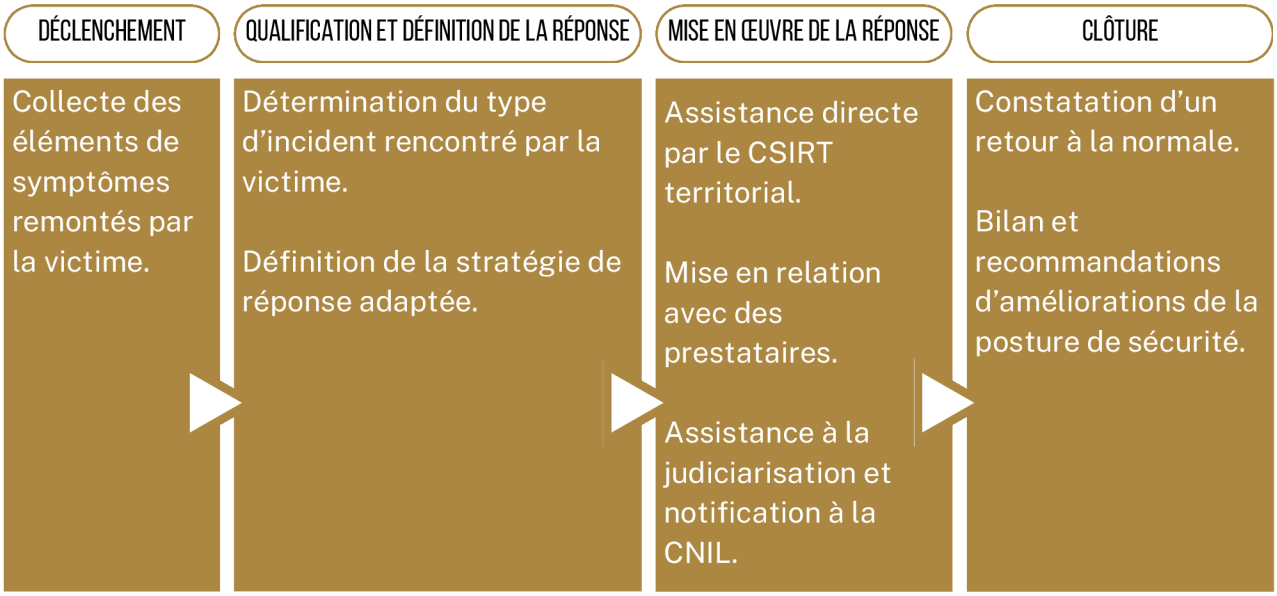
Les CSIRT territoriaux ont accompagné 136 entités victimes de rançongiciels en 2024 avec une répartition comme suit :

NOMBRE D'ATTAQUES RANÇONGICIEL TRAITÉS PAR TERRRITOIRE EN 2024



E
PROCESSUS DE TRAITEMENT DES INCIDENTS

Une assistance par un CSIRT territorial pour un incident se déroule comme suit :



Il s'agit d'un accompagnement de bout en bout de l'appel initial jusqu'à la résolution finale de l'incident. La durée de traitement ou de résolution d'un incident dépend du type d'incident rencontré. Pour les incidents les plus simples, le traitement est très rapide en 2 ou 3 jours ouvrés. Pour les incidents les plus graves, comme les rançongiciels, la durée de traitement d'un incident se compte en semaines voire en mois.

L'accompagnement des CSIRT territoriaux sur les cas de rançongiciels permet aux victimes de s'appuyer sur des tiers de confiance en capacité de les conseiller sur de nombreux aspects d'une gestion de crise cyber. Sur un aspect juridique, l'accompagnement permet aux victimes d'être informé sur leurs obligations face à un incident de sécurité. Cet aspect peut être crucial car par exemple les assurances cyber imposent le respect scrupuleux des délais légaux de 72h pour la notification auprès de la CNIL et du dépôt de plainte pour bénéficier de l'assurance.

Le niveau d'accompagnement des CSIRT territoriaux auprès des bénéficiaires est variable suivant l'origine de la sollicitation d'une part s'il s'agit d'une demande d'assistance par la victime elle-même ou s'il s'agit d'une action proactive des CSIRT territoriaux et d'autre part la maturité en cybersécurité de la victime.

Lorsqu'une entité est mentionnée dans les revendications de groupes criminels ou signalée par un partenaire, les CSIRT territoriaux peuvent être amenés à la contacter directement.

Les CSIRT territoriaux peuvent parfois faire face à des défis pour établir une relation de confiance avec les victimes lors d'un incident, notamment lorsqu'ils prennent l'initiative d'une action proactive.

L'ACCOMPAGNEMENT PAR UN CSIRT TERRITORIAL PERMET DE STRUCTURER LES ACTIONS POUR RÉPONDRE EFFICACEMENT À UN INCIDENT

Le risque le plus important face à un incident de sécurité est de réaliser une remédiation incomplète sans compréhension du mode opératoire utilisé par l'attaquant lui laissant le champ de réitérer ses actions malveillantes. Les opérations d'investigations numériques sont ainsi cruciales car elles permettent de reconstituer la chronologie de l'attaque c'est-à-dire les actions réalisées par l'attaquant sur le système d'information et le vecteur d'intrusion initial. Les actions de remédiation peuvent ainsi prendre en compte les vulnérabilités par lesquelles l'attaquant a pu s'introduire dans le système d'information en les corrigeant, assurant une protection durable de la victime.

Dans les situations où les victimes n'ont plus aucune sauvegarde, leur serveur de sauvegarde ayant lui aussi été chiffré, il existe une solution de la dernière chance encore trop souvent méconnue de la part des victimes de cyberattaques : la récupération de données par des laboratoires spécialisés. Les CSIRT territoriaux peuvent ainsi mettre en relation des victimes de cyberattaques avec ces laboratoires pour recouvrer leurs données de manière éthique sans le paiement de la rançon. Les chances de succès ne sont pas totalement garanties mais dans de nombreux cas, ces opérations de récupération fonctionnent.

Parmi les incidents largement rencontrés, l'arnaque au changement de RIB est une escroquerie courante où un fraudeur se fait passer pour un créancier légitime pour inciter la victime à effectuer un virement sur un compte bancaire frauduleux. Cette arnaque peut avoir des conséquences financières graves, car les recours auprès des banques sont souvent inefficaces si ils ne sont pas menés très rapidement au moment de la survenue de l'incident. Cette fraude est le plus souvent permise suite à la compromission d'un compte de messagerie d'un utilisateur de l'organisation. Ce type d'incident souligne l'importance de la protection des comptes de messagerie.

LORS D'UNE ATTAQUE PAR RANÇONGICIEL, LES CRIMINELS NE CHIFFRENT EN RÉALITÉ QU'UNE PETITE PARTIE DES DONNÉES, EN CIBLANT DES SECTIONS SPÉCIFIQUES DES FICHIERS. CETTE MÉTHODE LEUR PERMET DE GAGNER DU TEMPS TOUT EN RENDANT LES FICHIERS INACCESSIBLES, MÊME SI LA MAJORITÉ DES DONNÉES SONT EN RÉALITÉ INTACTES.

DES LABORATOIRES EXPERTS EN RÉCUPÉRATION DE DONNÉES PEUVENT AINSI SOUVENT RESTAURER CES FICHIERS EN SE CONCENTRANT SUR LES PARTIES NON CHIFFRÉES. CETTE APPROCHE PERMET AUX VICTIMES DE RÉCUPÉRER LEURS INFORMATIONS SANS PAYER DE RANÇON, OFFRANT AINSI UNE SOLUTION ÉTHIQUE QUI ÉVITE DE FINANCER DES ACTIVITÉS CRIMINELLES.

RANSOMWARE.LIVE

F
IMPACT DE L'ACCOMPAGNEMENT DES CSIRT TERRITORIAUX

Les coûts directs liés aux cyberattaques pour des collectivités locales de taille moyenne sont de l'ordre de 50 k€ à 60 k€ en coûts directs (prestations d'investigations et de remédiation) d'après les retours d'expériences suite à des incidents avérés. Les coûts indirects de dégradation de la qualité des services publics sont difficiles à évaluer mais bien réels (ex. interruption de la délivrance des titres d'identité, impacts sur les services de périscolaire ou de gestion des EHPAD communaux etc.) sans compter l'impact psychologique et les conséquences à plus long terme sur les équipes des collectivités locales concernées. De nombreux témoignages confirment des conséquences encore visibles d'une cyberattaque plus de 12 mois après la survenue de l'incident.

COÛT MOYEN D'UNE CYBERATTAQUE POUR UNE COLLECTIVITÉ DE TAILLE MOYENNE 50 K€ À 60 K€ EN COÛTS DIRECTS

Concernant les entreprises, les coûts sont souvent répartis souvent comme suit : environ 20% pour les coûts directs (prestations d'investigations et de remédiation) et environ 80% pour les pertes d'exploitation associées au sinistre. D'après les assureurs, le coût moyen d'une cyberattaque pour les PME / ETI est de l'ordre de 150 k€ (Source : étude LUCY, édition 2024, collection AMRAE) pouvant largement fragiliser la santé financière de ces entités. Un assureur spécialisé en cybersécurité indique que la perte moyenne pour les cas de fraude est de 55 k€ et pour les cas de rançongiciel, le coût moyen monte à plusieurs centaines de milliers d'euros.

COÛT MOYEN D'UNE CYBERATTAQUE POUR UNE PME – ETI 150 K€ COMPOSÉ DE 20% DE COÛTS DIRECTS ET DE 80% DE PERTES D'EXPLOITATION

L'intervention des CSIRT territoriaux dans l'accompagnement sur la réponse à incidents permet de limiter les impacts d'une attaque en cours pour les incidents les moins graves et les signalements, et évite qu'ils ne dégénèrent en incident plus graves (ex. compromission de compte, hameçonnage, fraude ou tentative de fraude, etc.).

Pour les incidents les plus graves, et les cas de rançongiciel en particulier, l'accompagnement apporté permet aux victimes de répondre de manière efficace et rapide à un incident limitant sérieusement les pertes d'exploitation qui constituent le coût principal des attaques.

L'action des CSIRT territoriaux a donc un impact significatif. On peut prendre par exemple le cas d'une entreprise bretonne de 300 salariés au moment de la survenue de la cyberattaque dont l'accompagnement par le CSIRT régional breton a permis de relancer ses activités 15 jours après la survenue du sinistre en partant d'une situation initiale dramatique pour la victime, avec le chiffrement complet des données et serveurs applicatifs de l'entreprise et en l'absence de sauvegarde saine.

G
COLLABORATION ET PARTAGE D'INFORMATIONS SUR LE TRAITEMENT D'INCIDENTS

Les CSIRT territoriaux collaborent au quotidien sur les signalements et incidents dont ils ont connaissance. Les échanges se déroulent sur un canal dédié de la messagerie gouvernementale Tchap. Des réunions sont également organisées de manière bi-hebdomadaire sur le pilotage des activités des CSIRT territoriaux avec le CERT-FR.

3 CSIRT territoriaux ont rejoint l'InterCERT France au cours de l'année 2024. L'InterCERT France a pour mission d'incarner la voix commune des CERT français, de promouvoir et d'accompagner leur développement, de développer les échanges opérationnels et d'animer la communauté de confiance des CERT. Une des forces de la communauté de l'InterCERT France est la collaboration opérationnelle au travers d'une plateforme d'échanges sécurisées.

JULIEN MOUSQUETON A DÉVELOPPÉ UN SITE NOMMÉ RANSOMWARE.LIVE QUI COLLECTE ET RECENSE LES REVENDICATIONS DES ATTAQUES DES GROUPES CRIMINELS DE RANÇONGICIELS SUR LEUR SITE WEB. LE CSIRT BRETON A DÉVELOPPÉ UN OUTIL D'ALERTE GRÂCE À L'API OFFERTE PAR LE SITE RANSOMWARE.LIVE CONSISTANT CONCRÈTEMENT À ENVOYER DES MAILS EN TEMPS RÉEL POUR CHAQUE PUBLICATION DES GROUPES CRIMINELS AFFECTANT UNE ENTITÉ FRANÇAISE. CES ALERTES SONT PARTAGÉES À LA COMMUNAUTÉ DE TOUS LES CSIRT TERRITORIAUX.

Ils collaborent sur des incidents de manière bilatérale ou multilatérale. Par exemple, le CSIRT Bretagne et le CSIRT Hauts de France ont collaboré en mai 2024 sur une attaque rançongiciel d'une victime prétendument bretonne revendiquée par le groupe criminel 8Base. Après qualification de l'incident, le CSIRT breton a pu identifier que la victime réelle de l'attaque était située dans les Hauts de France. Les CSIRT breton et des Hauts de France ont ensuite collaboré sur le traitement de cet incident avec les éléments recueillis initialement par le CSIRT breton au profit de la victime réelle située dans les Hauts de France.

Sur les incidents d'attaque par chaine d'approvisionnement ou les attaques en déni de service impliquant de nombreuses victimes réparties sur tout le territoire dans un temps donné, les CSIRT territoriaux se partagent en temps réel les informations. Des actions coordonnées sur un incident peuvent être montées le cas échéant.

L'ANSSI a proposé d'intégrer les CSIRT territoriaux lors de la refonte de sa plateforme téléphonique opérationnelle avec la mise en œuvre du numéro court 32 18. Un serveur vocal interactif a notamment été déployé au printemps 2024 en amont de la cérémonie d'ouverture des Jeux Olympiques de Paris 2024.

Les CSIRT territoriaux métropolitains ont été intégrés à ce déploiement, d'une part en heures ouvrables où les appelants au 32 18 peuvent être redirigés vers les CSIRT territoriaux, et d'autre part en heures non ouvrées des CSIRT territoriaux avec une redirection vers la permanence opérationnelle du CERT-FR ouvert 24 heures sur 24.

Ainsi, du 1er juillet au 31 décembre 2024, 52 appels ont été transférés en heures ouvrables du CERT-FR vers les CSIRT territoriaux métropolitains actuellement déployés sur ce service.

III

ENSEIGNEMENTS DES INCIDENTS ET ACTIONS DE PRÉVENTION

A
ENSEIGNEMENTS TIRÉS DES INCIDENTS

Nous pouvons tirer de nombreux enseignements des incidents traités par les CSIRT territoriaux. Le principal enseignement est que la majorité des attaques opérées par les acteurs criminels et observées par les CSIRT territoriaux peuvent être évitées avec l'adoption de mesures d'hygiène de cybersécurité adaptées.

LA PLUPART DES CYBERATTAQUES PEUVENT ÊTRE ÉVITÉES AVEC L'ADOPTION DE MESURES D'HYGIÈNE DE CYBERSÉCURITÉ ADAPTÉES

Ce constat est une bonne nouvelle car il montre que les cyberattaques ne sont pas une fatalité et que ce risque peut être géré. Il souligne néanmoins en creux le déficit de maturité notamment des entités de taille petite et moyenne en cybersécurité, constat connu et partagé par la communauté des experts en cybersécurité.

L'un des facteurs aggravants lors de la survenue de cyberattaques est l'absence de données de sauvegardes saines, le plus souvent par l'absence de sauvegardes hors ligne. Cela engendre une perte souvent quasi nette du patrimoine informationnel de l'organisation victime qui la met gravement en péril.

Nous constatons également souvent l'absence ou l'insuffisance de solutions de sécurité déployées pour détecter et répondre à une menace. A cette fin, le déploiement d'une solution technologique de type *Endpoint Detection & Response* constitue une réponse abordable et efficace qui permet de détecter au plus tôt les menaces et en particulier les acteurs de rançongiciel. En cas d'incident avéré, elle offre également une capacité à répondre plus efficacement à l'échelle d'un parc informatique complet.

Enfin, dans de nombreux incidents, le vecteur d'intrusion a été l'exploitation de vulnérabilités de logiciels ou d'équipements de bordure de réseau exposés sur internet. Un simple processus de gestion des vulnérabilités aurait pu éviter un grand nombre de ces incidents.

B
BONNES PRATIQUES POUR SE PRÉMUNIR DES INCIDENTS LES PLUS COURANTS

Face à la multiplication des attaques, l'ANSSI a identifié 5 mesures clés pour protéger efficacement un système d'information et limiter l'impact des cyberattaques lorsqu'elles surviennent. Ces actions constituent les mesures d'hygiène de cybersécurité adaptées pour la plupart des organisations.

L'expérience des CSIRT territoriaux montre qu'avec l'adoption de ces mesures, et en y incluant un processus de gestion des vulnérabilités et de la surface d'attaque, une très grande proportion de ces attaques pourrait être arrêtée.

- RENFORCER LA SÉCURITÉ DE L'AUTHENTIFICATION VIA DES MÉCANISMES D'AUTHENTIFICATION MULTI-FACTEUR
- METTRE EN ŒUVRE UN SYSTÈME DE DÉTECTION MANAGÉ TEL LES SOLUTIONS EDR (ENDPOINT DETECTION & RESPONSE)
- SAUVEGARDER VOS DONNÉES ET APPLICATIONS CRITIQUES AVEC AU MOINS UNE COPIE HORS-LIGNE
- ÉTABLIR UNE LISTE PRIORISÉE DES SERVICES NUMÉRIQUES CRITIQUES ET PRÉPARER UN DISPOSITIF DE GESTION DE CRISE ADAPTÉ À UNE CYBERATTAQUE

C
INITIATIVES NOTABLES DE PRÉVENTION

Les CSIRT territoriaux ont réalisé des initiatives uniques ou spécifiques à leur territoire. Quelques exemples sont présentés ici.

Un exercice de gestion de crise cyber dans les Hauts-de-France en amont des Jeux Olympiques de Paris 2024

En mars 2024, un exercice de gestion de crise cyber a été organisé dans le cadre des Jeux Olympiques de Paris 2024, la métropole lilloise pouvant donc être une cible potentielle en accueillant des épreuves. Le CSIRT Hauts-de-France a ainsi réussi à mobiliser une trentaine de participants, incluant des acteurs clés tels que les acteurs étatiques sur le territoire dont la préfecture du Nord, les parties prenantes des Jeux Olympiques et les acteurs cyber locaux. Cet exercice visait à éprouver la mise en place d'une organisation de gestion de crise, tester des mesures stratégiques et opérationnelles, et évaluer la gestion du stress ainsi que la réactivité et la résilience des acteurs impliqués. L'exercice a été une réussite et cet événement a été salué par le préfet délégué pour la défense et la sécurité qui était présent lors de l'exercice. Cette simulation a permis de renforcer la préparation et la coordination entre les différents acteurs, essentielle pour assurer la sécurité des Jeux Olympiques.

Campagne de détection de vulnérabilités au profit des collectivités locales françaises

À l'initiative du CSIRT de la Région Bretagne, les CSIRT territoriaux français se sont unis pour mener une campagne de recherche en vulnérabilité au profit des collectivités locales. Cette campagne d'envergure a eu lieu en avril 2024, sur l'ensemble du territoire français. La campagne de recherche en vulnérabilités a été réalisée grâce à l'exploitation de bases de données publiques de l'administration. Ce ne sont pas moins de 25 000 noms de domaines d'entités publiques parmi les communes, intercommunalités, conseils départementaux, centres de gestion territoriaux et conseils régionaux qui ont été analysés. 186 entités publiques ont ainsi été identifiées comme présentant des équipements vulnérables à 311 failles critiques, parmi les 25 000 analysés, soit un taux de 0,73% du total. A la date du 26 juin, 25% des vulnérabilités identifiées en avril avaient été corrigées grâce à l'action coordonnée des CSIRT territoriaux.

Déploiement d'un service gratuit de scan de vulnérabilité en Grand Est

En complément du service gratuit d'assistance aux victimes de cyberattaques, le CSIRT de la région Grand Est a adopté un outil de scan de vulnérabilité, intégralement financé par la Région Grand Est, gratuit pour les bénéficiaires. Il peut être mis en œuvre, sur sollicitation du CSIRT, au profit de chaque organisation localisée sur le territoire. Il permet de déceler au plus tôt les défauts de sécurité et les vulnérabilités critiques visibles à partir de l'empreinte internet de chaque bénéficiaire. Ce service est pleinement opérationnel depuis juillet 2024. Une cinquantaine de scans ont été exécutés en 2024. Il permet de recueillir un premier indicateur pertinent concernant le niveau de cybersécurité d'un système d'information. Un rapport est délivré au bénéficiaire qui comprend un plan de remédiation avec des recommandations et des actions à conduire pour corriger les failles détectées.

Star-Hack, un défi avec des étudiants en Nouvelle-Aquitaine

Lancé en octobre 2024, le programme Star-Hack a débuté par un Capture The Flag (CTF) impliquant 15 écoles de Nouvelle-Aquitaine, où 70 étudiants ont obtenu le titre de Cadet Cyber du Campus. En novembre, ces cadets et leurs professeurs référents ont suivi des formations et entraînements intensifs. En décembre, les cadets ont été mis en relation avec des experts parrains, membres du campus. Le programme se poursuivra en 2025. À ce jour, 22 applications ont été testées, révélant 32 failles.

Les matinées de sensibilisation du CSIRT CyberCorsica

Le CSIRT CyberCorsica a initié des matinées de sensibilisation afin d'aller au plus près des territoires, notamment les plus isolés. L'objectif de cette initiative est d'apporter un service de proximité permettant de sensibiliser ses bénéficiaires aux risques numériques, aux enjeux et à la nécessité de tendre vers une maturité numérique. Aucune entité n'est à l'abri d'une cyber attaque peu importe sa taille et le lieu où celle-ci est implantée.

Un cycle d'événements dédiés à la cybersécurité, « L'appel du Cyber Juin » en Normandie

Le CSIRT normand, Normandie Cyber a coorganisé un cycle d'événements dédiés à la cybersécurité, « l'appel du Cyber Juin », initié par le délégué régional de l'ANSSI. Il organise également en lien avec les collectivités locales (EPCI) des demi-journées de sensibilisation incluant une partie de mise en relation directe avec des prestataires cyber régionaux au format B2B.

E
RÉALISATION DE DIAGNOSTICS *MON AIDE CYBER*

Les CSIRT territoriaux, en plus de leur action principale dans le champ de la réponse à incidents, sont également très actifs dans la prévention au travers notamment du dispositif déployé par l'ANSSI *Mon Aide Cyber*.

Les CSIRT territoriaux sont également engagés dans des opérations de sensibilisation déployées dans les territoires notamment à l'occasion du mois de la cybersécurité en octobre mais également tout au long de l'année.

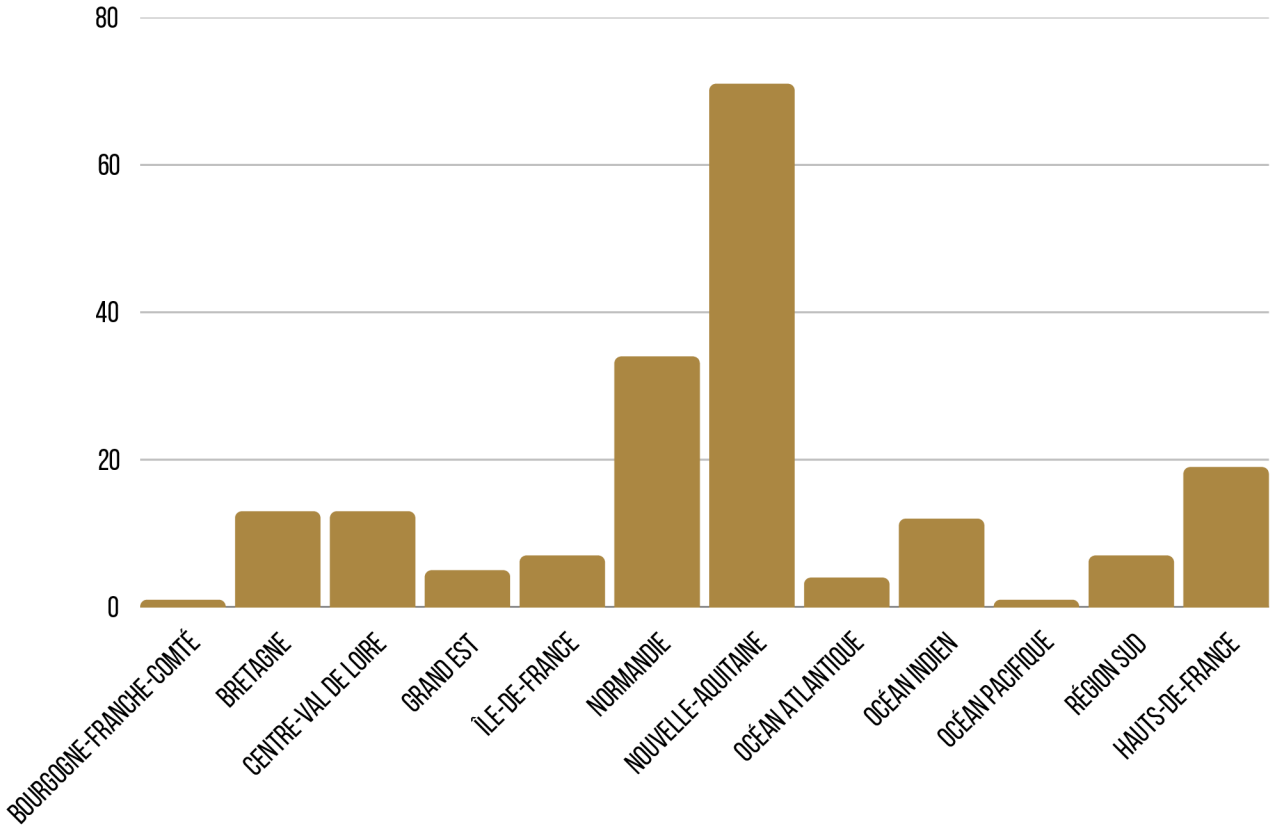
31 salariés des CSIRT territoriaux sont référencés comme aidants dans le dispositif. Ces aidants ont réalisé 189 diagnostics en 2024.

MONAIDECYBER EST UN DISPOSITIF QUI A POUR OBJECTIF D'ACCOMPAGNER LES ENTITÉS PUBLIQUES, LES ASSOCIATIONS ET LES ENTREPRISES SOUHAITANT MENER UNE PREMIÈRE DÉMARCHE DE SÉCURISATION INFORMATIQUE. CE DISPOSITIF EST BASÉ SUR DES AIDANTS.

LES AIDANT DES CSIRT TERRITORIAUX ONT RÉALISÉS 189 DIAGNOSTICS MON AIDE CYBER, REPRÉSENTANT 7% DE L'ENSEMBLE DES DIAGNOSTICS RÉALISÉS.

MonAide Cyber
INNOVATION ANSSI

NOMBRE DE DIAGNOSTICS MONAIDECYBER RÉALISÉS PAR LES CSIRT TERRITORIAUX EN 2024



IV

COOPÉRATIONS AU SEIN DE L'ÉCOSYSTÈME

A
COOPÉRATION AVEC LES PRESTATAIRES LOCAUX

Les CSIRT territoriaux ont parmi leurs premières actions réalisé une action de cartographie des prestataires de cybersécurité sur leurs territoires respectifs. Ces cartographies visent notamment à être en mesure d'identifier les prestataires locaux en capacité d'assister les victimes de cyberattaques en proximité dans les territoires. Elles sont également utilisées pour valoriser la filière cybersécurité du territoire.

B
COOPÉRATION AVEC LES FORCES DE SÉCURITÉ INTÉRIEURES

En lien étroit avec les forces de sécurité intérieures, les CSIRT territoriaux jouent un rôle clef dans la lutte contre la cybercriminalité en accompagnement les victimes dans le processus de judiciarisation au travers des dépôts de plainte et dans le recueil et le partage des informations concernant les tactiques, les techniques et les procédures (TTP) utilisées par les cyberattaquants.

Les informations recueillies lors des opérations d'investigations numériques conduites par les forces de sécurité permettent, d'une part, d'instruire les dossiers à charge contre les cybercriminels et constituent des éléments de preuve qui contribuent à la modélisation, à la traçabilité et, dans le cas le plus favorable, au démantèlement d'un groupe cybercriminel.

D'autre part, la connaissance de ces TTP permet d'améliorer, de façon continue, les processus et les outils de cyberprotection en les enrichissant des bases de données nécessaires pour prévenir et contrer des cyberattaques déjà identifiées et modélisées.

Des actions combinées d'information et de sensibilisation sont conduites dans toutes les régions avec la gendarmerie et la police nationale pour faciliter le processus de judiciarisation et les dépôts de plainte. Il s'agit chaque fois que possible de permettre une intervention rapide et efficace des enquêteurs cyber.

En région Grand Est, cette démarche est formalisée au travers d'une convention tripartite signée en mars 2023. Cette convention formalise le processus de dépôt de plainte avec notamment un accompagnement préparatoire et une prise de rendez-vous auprès de la brigade ou du commissariat de rattachement. Ainsi des échanges réguliers sont organisées avec les experts de la gendarmerie et de la police en région Grand Est afin de partager l'information sur la menace et améliorer la connaissance mutuelle des outils et des procédures de chacun.

Dans la région des Hauts-de-France, le CSIRT régional a sensibilisé tous les commissariats de la métropole de Lille et accompagne 56 % des victimes ayant déposé plainte. Cette approche vise à faciliter la relation avec les services compétents. Une collaboration quotidienne est également mise en place avec les services de gendarmerie, de police, ainsi qu'avec la DRSD pour protéger le patrimoine économique régional.

C
COOPÉRATIONS AVEC LES EDIH RÉGIONAUX

Les *European Digital Innovation Hubs* (EDIH) sont des dispositifs régionaux financés par l'Union européenne pour soutenir la transformation numérique des entreprises et des acteurs publics. Implantés à travers toute la France métropolitaine et à la Réunion, ces hubs reflètent les stratégies et écosystèmes régionaux, avec des spécialisations variées telles que la maturité digitale, l'intelligence artificielle (IA), la cybersécurité, ou encore le calcul haute performance (HPC).

Leur mission est d'accompagner les secteurs privé et public en proposant des services d'expertise pour définir des stratégies numériques, des expérimentations technologiques avant déploiement, des formations pour monter en compétences, et un soutien pour accéder à des financements régionaux, nationaux et européens.

Dans les régions où coexistent un EDIH spécialisé en cybersécurité et un CSIRT territorial, une collaboration étroite se met en place. Par exemple, à La Réunion, l'EDIH et le CSIRT, tous deux pilotés par le pôle Cybersécurité de Réunion THD, travaillent de concert pour informer sur les risques cyber, sécuriser les organisations et répondre aux incidents.

Cette synergie permet aux CSIRT de rediriger, après la gestion d'un incident, les entités affectées vers l'EDIH pour un accompagnement renforcé, incluant des diagnostics, des formations et un soutien financier visant à améliorer leur maturité en cybersécurité. Par ailleurs, les bénéficiaires du programme EDIH sont systématiquement sensibilisés à l'existence et à la mission des CSIRT, assurant ainsi une réactivité accrue et un meilleur niveau de protection en cas d'incident cyber.

Les EDIH régionaux répondent précisément aux enjeux et besoins des territoires, notamment en garantissant une présence locale forte, essentielle pour délivrer efficacement des services de cybersécurité jusqu'au dernier kilomètre.

D
COOPÉRATIONS AVEC LES CAMPUS CYBER TERRITORIAUX

Les campus territoriaux et les CSIRT régionaux ont des missions complémentaires. Les CSIRT jouent leur rôle d'accompagnement et de réponse à incident, avec des missions bien définies et encadrées. Les campus cyber fédèrent la filière cybersécurité et permettent de tisser des liens avec les filières à sécuriser. Ils agissent comme des « hub », des plateformes aux ressources variées, dépendantes des maturités des territoires.

Les CSIRT et les campus contribuent à l'animation de la filière et la mise en lumière des enjeux de cybersécurité, mais là où les CSIRT délivrent des services normés, les campus se voient confier des missions variées, relatives à la structuration de l'écosystème.

Leur co-existence contribue à couvrir la chaine de valeur : identifier, protéger, détecter, répondre et récupérer. Cette coopération se traduit différemment en fonction des territoires et des modes de gouvernance choisis par les régions : entités juridiques séparées pour certaines régions, service du CSIRT intégré dans le campus pour d'autres.

Les modèles seront confrontés à la réalité opérationnelle et à l'évolution des menaces et de leur prise en compte. Mais la coopération, quelle qu'en soit la forme, sera le meilleur moyen d'œuvrer collectivement au service de la sécurisation des acteurs.

E
AUTRES COOPÉRATIONS

Certains CSIRT territoriaux ont signé des conventions de coopération avec les CSIRT sectoriels. Des conventions ont notamment été signées avec le M-CERT et le CERT Aviation France. Des échanges sont en cours pour des signatures de convention avec le CERT Santé notamment. Enfin, des échanges réguliers ont eu lieu entre les CSIRT territoriaux et le CERT-ED porté par la DRSD et qui contribue à la prévention des incidents de sécurité, pour le secteur des entreprises de défense et à la coordination de la réponse aux incidents ciblant ce secteur.

Les CSIRT territoriaux coopèrent également avec Cybermalveillance. Premièrement, les CSIRT territoriaux participent aux actions de sensibilisation du mois européen de la cybersécurité, tous les mois d'octobre. En France, c'est Cybermalveillance qui porte l'animation de cet événement européen. Les CSIRT territoriaux sont pleinement intégrés dans cette dynamique. Par ailleurs, au cours de l'année 2024, des travaux ont débuté pour intégrer les CSIRT territoriaux aux parcours du 17Cyber. Par ailleurs, certains CSIRT assurent la promotion du label Expert Cyber auprès des prestataires privés de leur territoire.

F
ÉVÉNEMENTS ET CONFÉRENCES

En moyenne chaque CSIRT territorial a participé à une quarantaine d'événements, conférences, tables-rondes, webinaires autour de la cybersécurité en 2024. Les actions de communication sont réalisées le plus souvent en partenariat avec les CCI, les fédérations professionnelles telles l'UIMM ou le CNAMS mais également les fédérations patronales comme le MEDEF, les clubs des ETI ou la CPME.

EN MOYENNE, UN CSIRT PARTICIPE À UNE QUARANTAINE D'ÉVÉNEMENTS PAR AN TOTALISANT PLUS DE 500 ÉVÉNEMENTS COUVERTS PAR LES CSIRT TERRITORIAUX EN 2024

Parmi les événements marquants dans les régions, les événements SECNUMECO organisés par l'ANSSI et le SISSE sont des temps forts. En 2024, le programme des SECNUMECO a rassemblé 14 événements sur tout le territoire, de Saint-Brieuc à Bastia en passant par Dôle et Le Mans.

De nombreux salons professionnels de la cybersécurité d'envergure nationale se déroulent en région dont le Forum InCyber à Lille début avril, l'European Cyber Week à Rennes et le Cybersecurity Business Convention à Toulouse organisés quant à eux en novembre. Normandie Cyber a participé au Cyber Show de Paris, avec un stand dédié et accompagné de 8 prestataires régionaux.

Des événements locaux sont organisés avec une participation active des CSIRT territoriaux comme la deuxième édition des Assises Régionales de la Cybersécurité en Centre Val de Loire organisée le 20 mars 2024 à Chartres. Le BreizhCTF, la plus grande compétition de cybersécurité en présentiel organisée en France a eu lieu en 2024 les 17 et 18 mai à Rennes et suivi les 22 et 23 mai par les journées *E Ghjurnate Smart Isula* à Ajaccio, organisé par la Collectivité de Corse qui ont permis une immersion au cœur des révolutions en cours dans les domaines de la cybersécurité, des données et de l'intelligence artificielle. Enfin, les assises régionales de cybersécurité & Hack-it-N 2024 ont eu lieu à Bordeaux le 18 décembre 2024.

En région Hauts-de-France, une *task force* a été constituée pour sensibiliser les collectivités locales et être au plus près des territoires. Cette équipe d'intervention, composée de la gendarmerie, de la police, de l'ANSSI, des centres de gestion, du CITC/EDIH GreenPowerIT et du CSIRT Hauts-de-France, permet d'agir ensemble de manière coordonnée face aux enjeux de cybersécurité. Tout au long de l'année 2024, un tour régulier des territoires a été organisé pour renforcer la coopération et accompagner efficacement les acteurs locaux : 14 territoires, 5 départements, 25 sessions ont été organisées.

SYNTHÈSE ET PERSPECTIVES

Les CSIRT territoriaux de par leur action se sont imposés en 2024 comme un maillon essentiel du dispositif national de réponse aux incidents de sécurité. Ils ont traité plus d'un millier d'événements de sécurité collectivement au cours de l'année écoulée dont plus d'une centaine d'attaques rançongiciels.

Dans le domaine de la prévention, ils auront conduit pas loin de 700 actions (évènements, webinaires, conférences, tables rondes, diagnostics Mon Aide Cyber…) au profit de tous les bénéficiaires.

Ils sont donc une remarquable illustration de ce que peut produire de mieux un partenariat entre l'Etat et les Régions.

Les CSIRT territoriaux sont les maillons de proximité qui assurent « le dernier kilomètre » du dispositif national de réponse aux incidents de sécurité. Une proximité qui leur confère une parfaite connaissance de leur territoire, des acteurs locaux de la cybersécurité, avec une capacité d'écoute, de dialogue et d'adaptation permanente au service des victimes d'un incident cyber.

Dans le texte de loi de transposition de la directive NIS 2 actuellement en débat dans les deux chambres parlementaires, les CSIRT territoriaux sont identifiés comme des futurs CSIRT relais. Du fait de la massification des acteurs régulés portée par cette loi, les CSIRT territoriaux auront un rôle à jouer dans l'accompagnement des futures entités régulées aussi bien dans le rappel dans leurs obligations de notification au CERT-FR en cas d'incident que dans l'accompagnement dans la montée en maturité de ces acteurs.

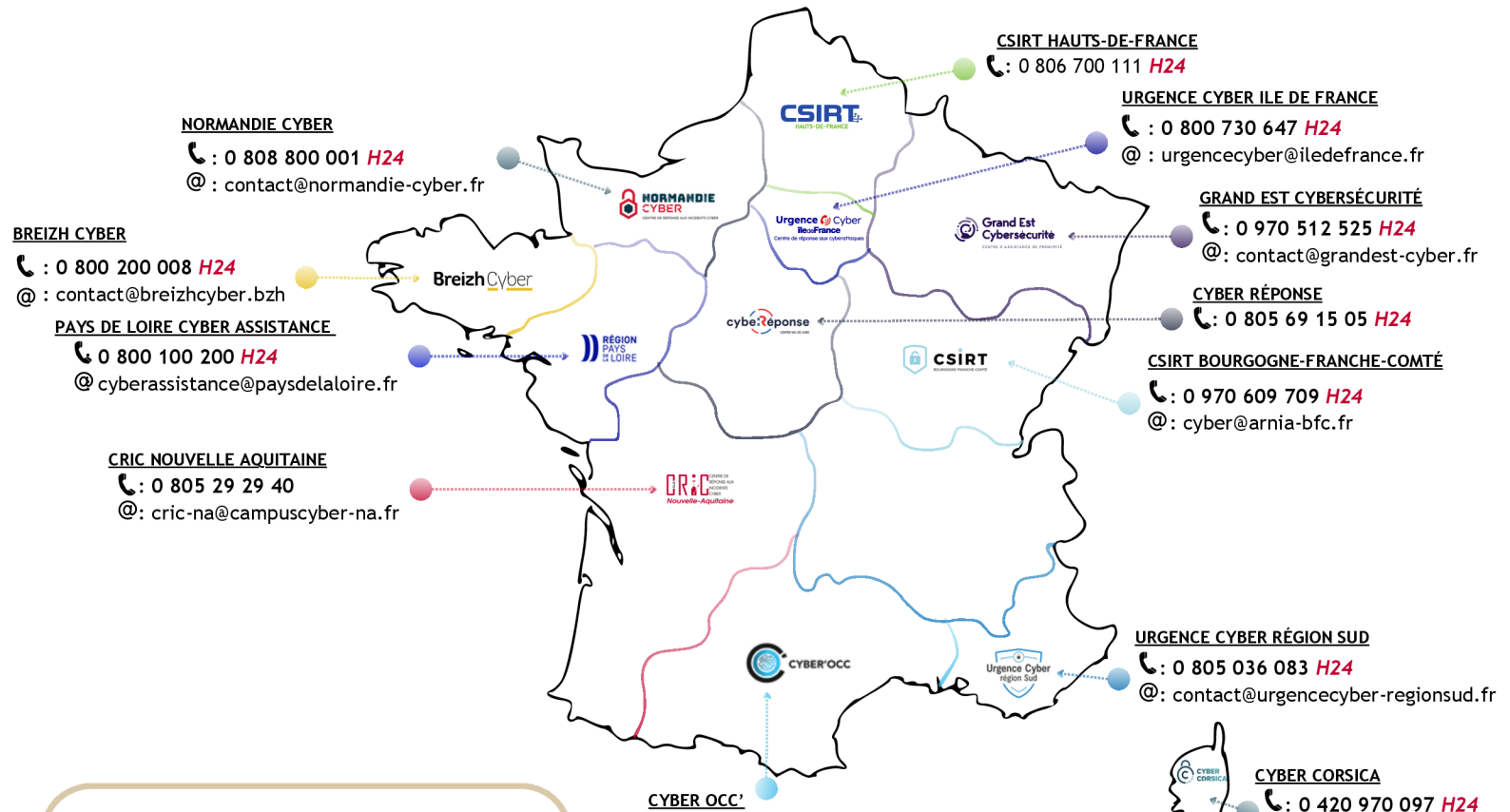
1387 ÉVÉNEMENTS DE SÉCURITÉ TRAITÉS DONT 729 SIGNALEMENTS DE SÉCURITÉ TRAITÉS ET 658 INCIDENTS DE SÉCURITÉ DONT 136 ATTAQUES RANÇONGICIEL TRAITÉS

PARTICIPATION CUMULÉE À 500 ÉVÉNEMENTS

189 DIAGNOSTICS MON AIDE CYBER RÉALISÉS PAR 31 SALARIÉS DES CSIRT TERRITORIAUX

ANNEXES

CARTOGRAPHIE DES CSIRT TERRITORIAUX



CSIRT LA RÉUNION *(OCÉAN INDIEN)*
: 0 262 974 999
@: csirt@cyber-reunion.fr

CSIRT ATLANTIC *(OCÉAN ATLANTIQUE)*
: 0 970 260 801
@: csirt-atlantic@accyb.org

CENTRE CYBER DU PACIFIQUE *(OCÉAN PACIFIQUE)*
: 505 300
@: contact@centrecyberpacifique.nc

ANSSI

: 7/7 - 24h/24
: 32 18 (09 70 83 32 18)
@ : cert-fr@ssi.gouv.fr

FICHE D'IDENTITÉ DES CSIRT TERRITORIAUX

NOM DU CSIRT	LOGO DU CSIRT	ENTITÉ PORTEUSE DU CSIRT	STATUT
NORMANDIE CYBER	NORMANDIE CYBER	ADNORMANDIE	EPL
BREIZH CYBER	Breizh Cyber	CONSEIL RÉGIONAL DE BRETAGNE	COLLECTIVITÉ TERRITORIALE
PAYS DE LOIRE CYBER ASSISTANCE	RÉGION PAYS DE LA LOIRE	GIGALIS	GIP
CRIC NOUVELLE AQUITAINE	CRIC Nouvelle-Aquitaine	CAMPUS RÉGIONAL DE CYBERSÉCURITÉ ET DE CONFIANCE NUMÉRIQUE DE NOUVELLE AQUITAINE	ASSOCIATION
CYBER OCC'	CYBER'OCC	CYBER'OCC	ASSOCIATION
CSIRT HAUTS-DE-FRANCE	CSIRT HAUTS-DE-FRANCE	CONSEIL RÉGIONAL HAUTS-DE-FRANCE	COLLECTIVITÉ TERRITORIALE
URGENCE CYBER ILE DE FRANCE	Urgence Cyber îledeFrance	CONSEIL RÉGIONAL D'ILE-DE-FRANCE	COLLECTIVITÉ TERRITORIALE
GRAND EST CYBERSÉCURITÉ	Grand Est Cybersécurité	GRAND EST DÉVELOPPEMENT	ASSOCIATION
CYBER RÉPONSE	cyberRéponse	RECIA	GIP
CSIRT BOURGOGNE-FRANCHE-COMTÉ	CSIRT	AGENCE RÉGIONALE DU NUMÉRIQUE ET DE L'INTELLIGENCE ARTIFICIELLE	GIP
URGENCE CYBER RÉGION SUD	Urgence Cyber région Sud	URGENCE CYBER RÉGION SUD	ASSOCIATION
CYBER CORSICA	CSIRT CYBER CORSICA	COLLECTIVITÉ DE CORSE	COLLECTIVITÉ TERRITORIALE
CSIRT LA RÉUNION (OCÉAN INDIEN)	CSIRT LA RÉUNION	RÉUNION THD	RÉGIE PUBLIQUE À CARACTÈRE INDUSTRIEL ET COMMERCIAL
CSIRT ATLANTIC (OCÉAN ATLANTIQUE)	ACCYB	AGENCE CARIBÉENNE POUR LA CYBERSÉCURITÉ	ASSOCIATION
CENTRE CYBER DU PACIFIQUE (OCÉAN PACIFIQUE)	CENTRE CYBER DU PACIFIQUE	CENTRE CYBER DU PACIFIQUE	ASSOCIATION

TAXONOMIE DES ÉVÉNEMENTS DE SÉCURITÉ

TAXONOMIE	TYPOLOGIE D'ÉVÉNEMENT
COMMUNICATIONS SUSPECTES / TENTATIVES DE CONNEXION	Signalement
COMPORTEMENT SUSPECT D'UN MATÉRIEL	Signalement
DÉNI DE SERVICE	Signalement
HAMEÇONNAGE / INGÉNIERIE SOCIALE	Signalement
INDISPONIBILITÉ ACCIDENTELLE / FAUX POSITIF	Signalement
PERTE ET VOL DE MATÉRIEL	Signalement
VULNÉRABILITÉ NON CORRIGÉE	Signalement
ATTAQUE PAR CHAINE D'APPROVISIONNEMENT	Incident
AUTRES	Incident
COMPROMISSION D'UN ACTIF / INTRUSION AVÉRÉE / EXPLOITATION D'UNE VULNÉRABILITÉ	Incident
COMPTE PRIVILÉGIÉ OU NON PRIVILÉGIÉ COMPROMIS	Incident
DÉFIGURATION	Incident
FRAUDE OU TENTATIVE DE FRAUDE	Incident
MALICIEL - HORS RANÇONGICIEL	Incident
RANÇONGICIEL	Incident
TYPOSQUATTAGE / USURPATION D'IDENTITÉ	Incident
VIOLATION DE DONNÉES (EXPOSITION OU EXFILTRATION DE DONNÉES)	Incident

Les sollicitations diverses reçues par les CSIRT territoriaux concernant des demandes de renseignement, des conseils, etc. ne sont pas comptabilisées dans ces statistiques.

GLOSSAIRE DES TERMES TECHNIQUES ET ACRONYMES

TERME	DÉFINITION OU SIGNIFICATION
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CERT-FR	Le CERT-FR (Computer Emergency Response Team France) est l'équipe nationale française de réponse aux incidents de sécurité informatique. Les bénéficiaires du CERT-FR sont prioritairement les entités publiques ministérielles et les opérateurs régulés.
CSIRT	Computer Security Incident Response – Equipe de réponse à incidents
DIRECTIVE NIS 2	La directive NIS 2 (Network and Information Security) est une réglementation de l'Union européenne visant à renforcer la cybersécurité au sein des États membres publiée en décembre 2022. Elle remplace la directive NIS 1 et élargit son champ d'application pour inclure davantage de secteurs et d'entités.
INITIAL ACCESS BROKERS	Les *Initial Access Brokers* (IABs) sont des acteurs de la cybercriminalité spécialisés dans l'obtention d'accès non autorisé à des réseaux ou systèmes informatiques, qu'ils revendent ensuite à d'autres cybercriminels.
CAPTURE THE FLAG (CTF)	Compétition de cybersécurité où les participants doivent résoudre des challenges techniques pour capturer des drapeaux (flags), qui sont des informations cachées. Ces compétitions sont utilisées pour tester et développer les compétences en cybersécurité des participants.
INTERCERT-FRANCE	Association professionnelle créée en 2021 qui rassemble les organisations françaises impliquées dans la détection et la réponse aux incidents de cybersécurité
ÉVÉNEMENT	Événement de sécurité porté à la connaissance des CSIRT territoriaux et qui a donné lieu à un traitement. Les événements regroupent les incidents et les signalements.
SIGNALEMENT	Événement de sécurité qui caractérise un comportement anormal ou inattendu d'un SI pouvant avoir un caractère malveillant ou ouvrir la voie à des usages néfastes à l'encontre d'un système d'information

TERME	DÉFINITION OU SIGNIFICATION
INCIDENT	Événement de sécurité où les CSIRT territoriaux sont en mesure de confirmer qu'un acteur malveillant a conduit des actions malveillantes avec succès sur un système d'information (ex. attaques par rançongiciel)
RANSOMWARE AS A SERVICE	Forme de cybercriminalité où les développeurs de rançongiciels (ransomware) créent et louent leur logiciel malveillant à des affiliés. Ces affiliés paient pour utiliser le ransomware et lancer des attaques sans avoir besoin de compétences techniques avancées
RANÇONGICIEL	Logiciel malveillant qui chiffre les données d'un système d'information, rendant ces données inaccessibles. Les cybercriminels à l'origine de l'attaque exigent ensuite une rançon en échange de la clé de déchiffrement qui permet à la victime de récupérer l'accès à ses données.
SIMPLE EXTORSION	Mode opératoire d'une attaque rançongiciel où l'attaquant chiffre des données d'un système d'information et demande une rançon pour fournir la clé de déchiffrement à la victime
DOUBLE EXTORSION	Mode opératoire d'une attaque rançongiciel où l'attaquant exfiltre puis chiffre des données d'un système d'information, puis menace de publier les données exfiltrées pour la clé de déchiffrement).

RÉFÉRENCES ET SOURCES D'INFORMATION

SOURCE	CONTENU OU DOCUMENT	ANNÉE
BREIZH CYBER	Statistiques d'incidentologie	2024
CENTRE CYBER DU PACIFIQUE	Statistiques d'incidentologie	2024
CRIC NOUVELLE AQUITAINE	Statistiques d'incidentologie	2024
CSIRT ATLANTIC	Statistiques d'incidentologie	2024
CSIRT BFC	Statistiques d'incidentologie	2024
CSIRT HAUT-DE-FRANCE	Statistiques d'incidentologie	2024
CYBER CORSICA	Statistiques d'incidentologie	2024
CYBER RÉUNION	Statistiques d'incidentologie	2024
CYBER'OCC	Statistiques d'incidentologie	2024
CYBERÉPONSE	Statistiques d'incidentologie	2024
GRAND EST CYBERSÉCURITÉ	Statistiques d'incidentologie	2024
NORMANDIE CYBER	Statistiques d'incidentologie	2024
PAYS DE LOIRE CYBER ASSISTANCE	Statistiques d'incidentologie	2024
URGENCE CYBER ILE-DE-FRANCE	Statistiques d'incidentologie	2024
URGENCE CYBER RÉGION SUD	Statistiques d'incidentologie	2024
JULIEN MOUSQUETON	Ransomware.live	2023/2024
AMRAE	LUCY – Light Upon Cyber Insurance	2024
ANSSI	Panorama de la cybermenace	2024
ANSSI	Statistiques d'appels au 32 18	2024

SOURCE	CONTENU OU DOCUMENT	ANNÉE
ANSSI	Statistiques de réalisation des diagnostics Mon Aide Cyber	2024
ANSSI	Les Mesures Cyber Préventives Prioritaires	2023

RAPPORT D'ACTIVITÉ DES CSIRT TERRITORIAUX 2024

Édité par Breizh Cyber en partenariat avec
l'ensemble des CSIRT territoriaux

Direction artistique : Manon Laurier

Mars 2025