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

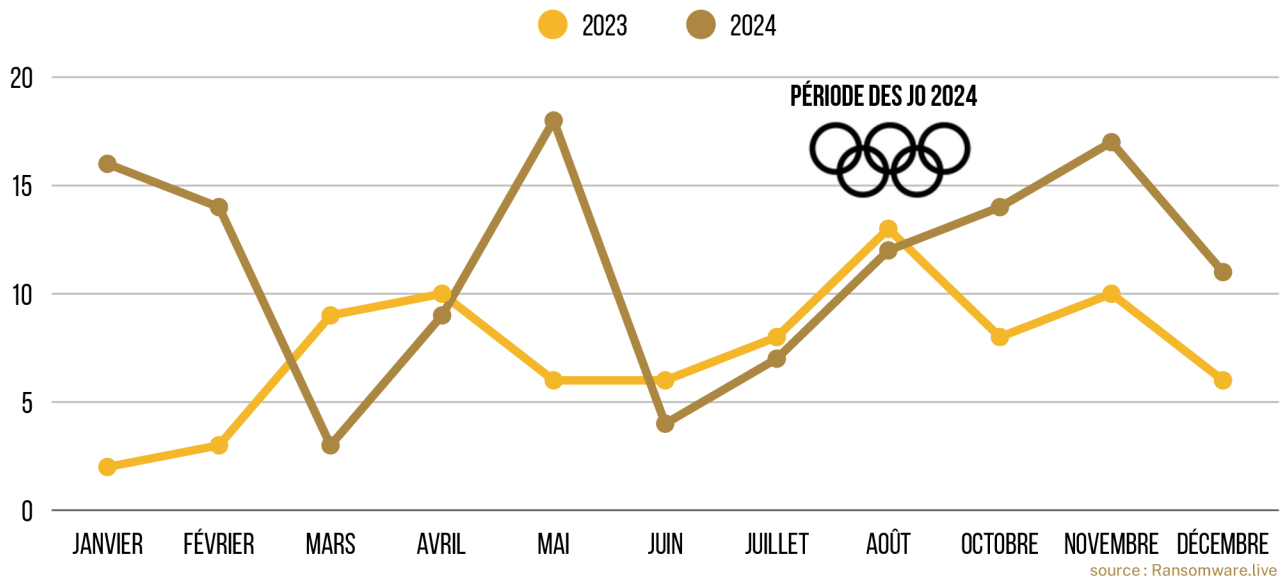
Sur la base des sites web spécialisés dans le suivi des activités des groupes criminels de haut niveau opérant des attaques par rançongiciel, il est possible de dégager les tendances marquantes de l'évolution de ces groupes ainsi que de donner un aperçu de cette activité cybercriminelle sur le territoire 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.

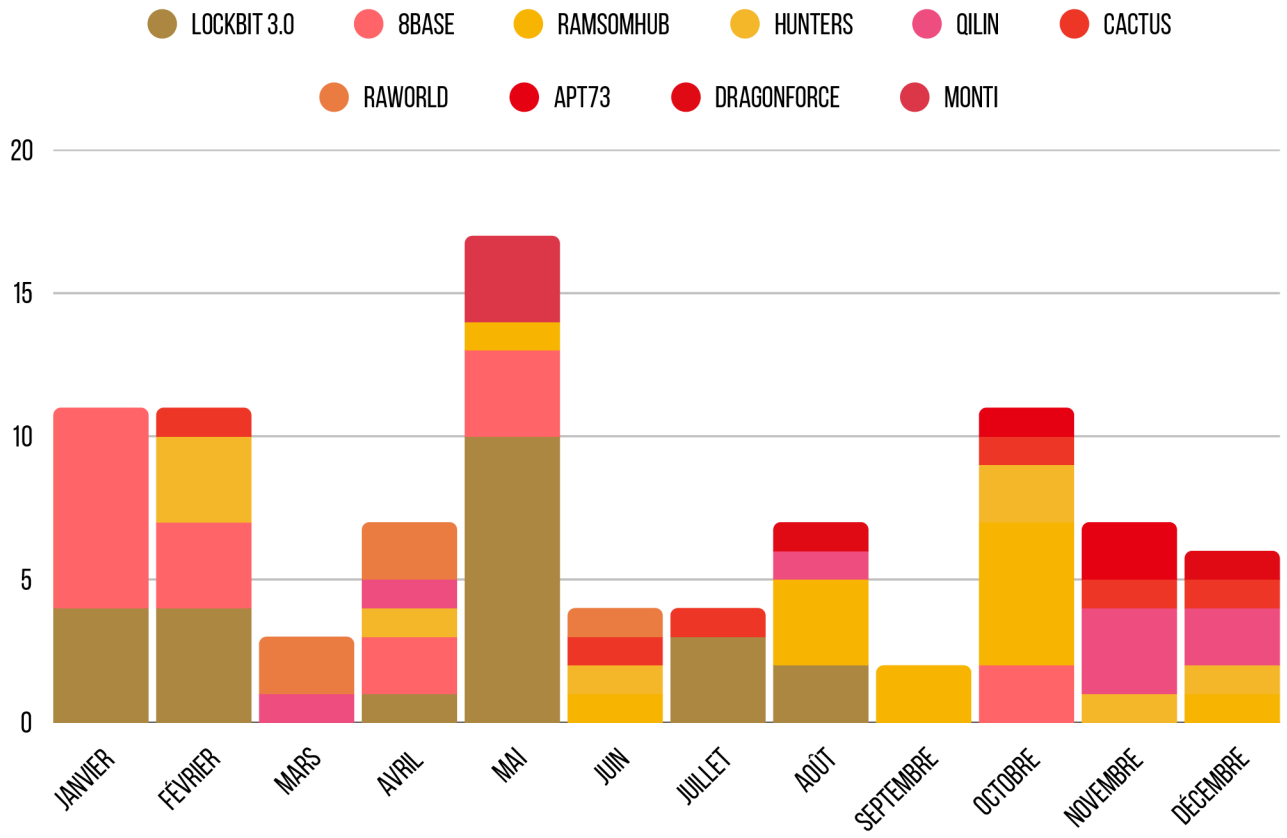
Ce groupe représentait à lui-seul quasiment le quart des attaques en 2023. L'autre fait notable est la montée en puissance du groupe RansomHub qui devient le groupe criminel le plus actif dans le monde et un des plus actifs en France.

NOMBRE DE VICTIMES FRANÇAISE PAR MOIS



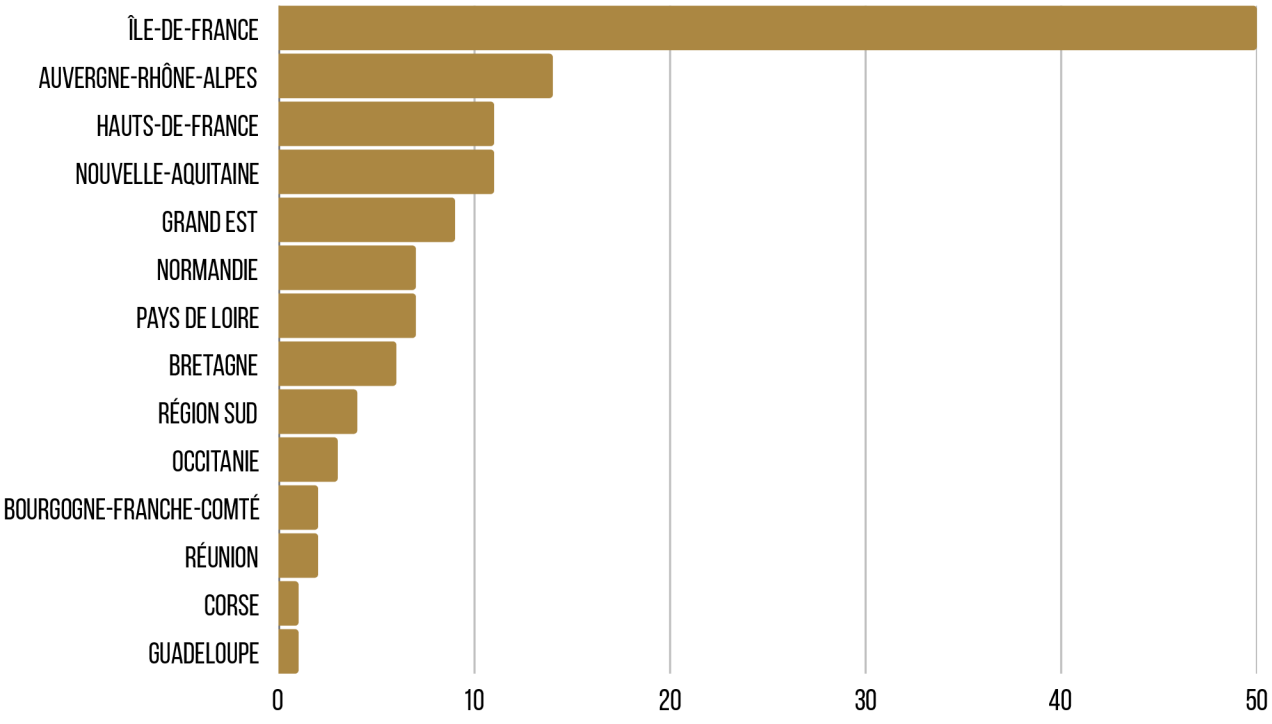
source : Ransomware.live

ACTIVITÉ MENSUELLE DES 10 GROUPES CRIMINELS LES PLUS ACTIFS EN FRANCE



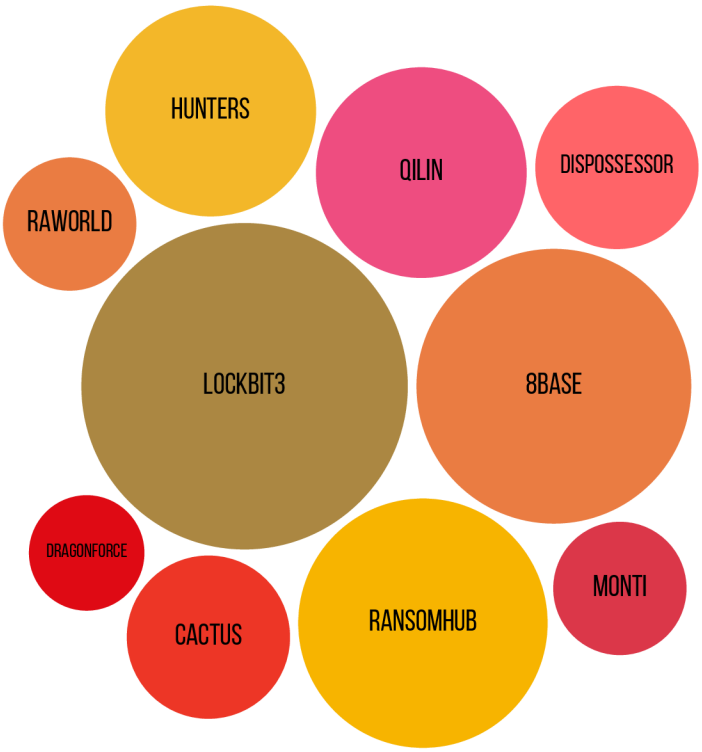
source : Ransomware.live

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.