ANOZR WAY
PEOPLE-CENTRIC CYBER PROTECTION

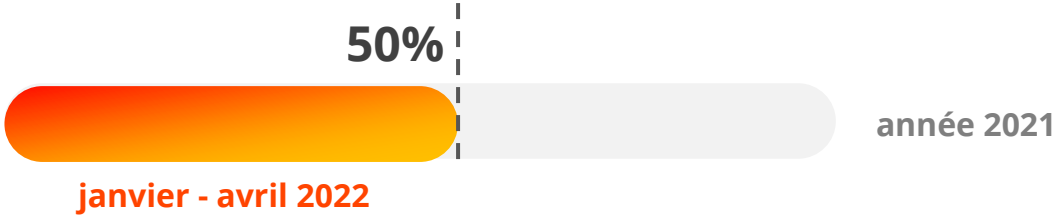
BAROMÈTRE ANOZR WAY DU RANSOMWARE

Évolution de la menace de janvier à avril 2022

Edition du 16 mai 2022

SOMMAIRE

Ransomware burn rate
2022 vs 2021



En 2022 en 4 mois seulement, le nombre d'organisations victimes de ransomware dans le monde est déjà égal à 50% de celui de 2021

53%

des attaques en UE impactent trois pays : 1) l'Allemagne, 2) l'Italie et 3) la France de janvier à avril 2022

660 millions €

de perte de CA cumulé estimée pour les entreprises françaises victimes de janvier à avril 2022

au moins

168 300 Français

aux données personnelles divulguées dans le darkweb suite aux ransomwares

Alban ONDREJECK
CTO & Co-fondateur
ANOZR WAY

Expert en cyberdéfense*,
Alban ONDREJECK a été officier dans les services de renseignement français et Directeur cybersécurité au sein d'Orange Business Services.

** La cyberdéfense regroupe l'ensemble des moyens physiques et virtuels mis en place par un État dans le cadre de la guerre informatique menée dans le cyberespace.*

Après l'accalmie toute relative des mois de décembre 2021 et janvier 2022, le volume d'organisations victimes de ransomware est rapidement revenu à un niveau élevé. **En 4 mois seulement, le nombre d'organisations victimes de ransomware est déjà égal à 50% de celui de 2021. L'état de la menace ransomware reste toujours aussi élevé avec 35 à 40 groupes actifs.**

Durant ces premiers mois de 2022, le conflit Ukraine-Russie a évidemment marqué la sphère cyber. Malgré quelques tentatives rapidement avortées de s'allier à la Russie, les groupes de ransomware ont continué leur ligne « business as usual ». **Lockbit 2.0 est en bonne voie d'être le leader mondial du marché du ransomware en étant à l'origine de 39% des attaques mondiales.**

Autres faits marquant de la période, le secteur de l'énergie est particulièrement ciblé dans le monde depuis ce début d'année 2022. **En quatre mois seulement, on constate déjà +138% d'entreprises de l'énergie victimes de ransomware par rapport à l'ensemble de l'année 2021.** Le contexte du conflit Ukraine-Russie peut expliquer le choix de ces cibles stratégiques, l'énergie étant au cœur des débats européens et des sanctions économiques imposées à la Russie.

En France on assiste à une sur-représentativité du secteur public victime de ransomware, en comparaison aux autres pays européens. Le contexte électoral peut jouer un rôle dans le choix de ces cibles par les attaquants. L'intérêt pour les hackers de s'en prendre à ces organismes publics est multiple : déstabiliser la nation, perturber voire interrompre les services publics, et mettre la main sur les données personnelles des citoyens.
Sur ces premiers mois de 2022, au moins 168 300 Français sont directement concernés par le vol de leurs données personnelles. La menace ransomware nous concerne tous, organisations privées, publics et particuliers.

COMPRENDRE LE RANSOMWARE

Historiquement, le ransomware ou “rançongiciel” en français est une technique d’attaque cybercriminelle qui consiste à infiltrer l’appareil de la victime et à y installer un logiciel malveillant qui perturbe le fonctionnement du système informatique et en chiffre les données. Seul le paiement d’une rançon par la victime à l'attaquant permettrait d’obtenir la clé de déchiffrement.

L'utilisation de ce type d'attaque s'est organisée autour de groupes diffusant des kits de logiciels malveillants sur abonnement appelés Ransomware as a Service (RaaS) et de nouvelles stratégies en pratiquant la double voire la triple extorsion. La majorité de ces groupes sont des cybers mafieux n'ayant qu'un but principalement financier.

Le conflit en Ukraine a brouillé l'image du ransomware avec l'apparition de groupes utilisant les RaaS à des fins hacktivistes, politiques ou de déstabilisation qui ne sont pas à proprement parler des groupes de ransomware.

Pendant la guerre en Ukraine, de nombreux hacktivistes ont utilisé le ransomware comme technique d'attaque. C'est notamment le cas de NB65 qui a utilisé le code fuité de Conti pour attaquer plusieurs entreprises russes.

Enfin, après une utilisation massive de blogs sur le darkweb pour communiquer et revendiquer leurs attaques, les groupes de ransomware ont également évolué dans leurs canaux de communication en utilisant plus largement les messageries Telegram et Discord ou encore Twitter qui a ouvert son service en mars sur TOR, le plus connu des réseaux du Darkweb.

COMPRENDRE LE RANSOMWARE

Simple extorsion

Infiltration
Chiffrement des données
Demande de rançon en échange de la clé de déchiffrement

La simple extorsion est utilisée par des hackers isolés qui n'appartiennent pas à des groupes organisés.

Comme ces attaques ne sont jamais revendiquées, elles sont difficilement quantifiables.

Double extorsion

Simple extorsion
+
Menace de publication ou de vente des données exfiltrées si refus de paiement.

La double extorsion est utilisée par la majorité des groupes de ransomware aujourd'hui actifs. Elle concerne 84% des attaques par ransomware.

Le chantage s'effectue directement sur leur blog en ligne ou via des réseaux sociaux comme Telegram.

Triple extorsion

Double extorsion
+
Attaque DDoS

La triple extorsion est apparue pour la première fois au milieu de l'année 2021 et s'est depuis démocratisée.

Elle est notamment utilisée par Avaddon et Darkside afin d'accentuer la pression sur les victimes.

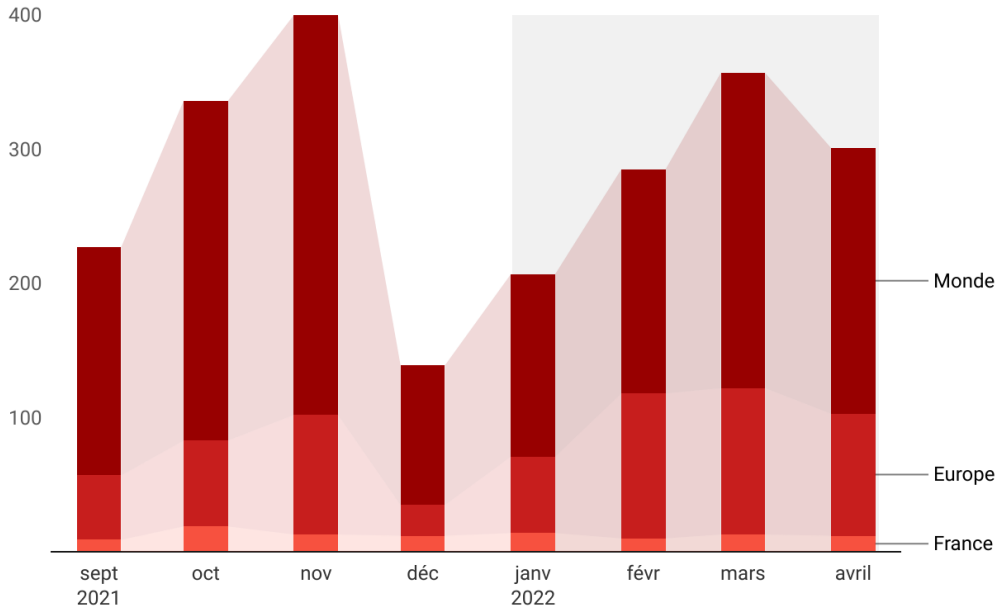
Ces modes opératoires sont en constante évolution. Les groupes de ransomware cherchent à innover pour augmenter leur productivité et rester sous le radar. C'est particulièrement le cas de Conti qui, à travers des partis tiers, se diversifie. Son groupe Karakurt, arrivé en juin 2021 utilise le modèle "Out of the Land" qui consiste à privilégier le vol de données sensibles sans systématiquement déployer de ransomware. Cette attaque est moins coûteuse, plus rapide et surtout plus discrète car aucune charge n'a besoin d'être installée sur le système d'information de la victime.

ÉVOLUTION DE LA MENACE

janvier – avril 2022

Après l'accalmie toute relative des mois de décembre 2021 et janvier 2022, le volume d'organisations victimes de ransomware est rapidement revenu à un niveau élevé en ces premiers mois de 2022.

Le mois de mars 2022 se solde par un volume à mi-chemin de ceux d'octobre et novembre 2021, démontrant le retour à **une haute intensité de la menace ransomware et confirme ainsi l'accélération du phénomène constatée dès l'automne 2021.**



Évolution du nombre d'organisations victimes de ransomware dans le monde, en Europe et en France de septembre 2021 à avril 2022

IMPACT ÉCONOMIQUE

janvier – avril 2022

660 millions €

de perte de CA cumulé estimée pour les entreprises françaises victimes de janvier à avril 2022

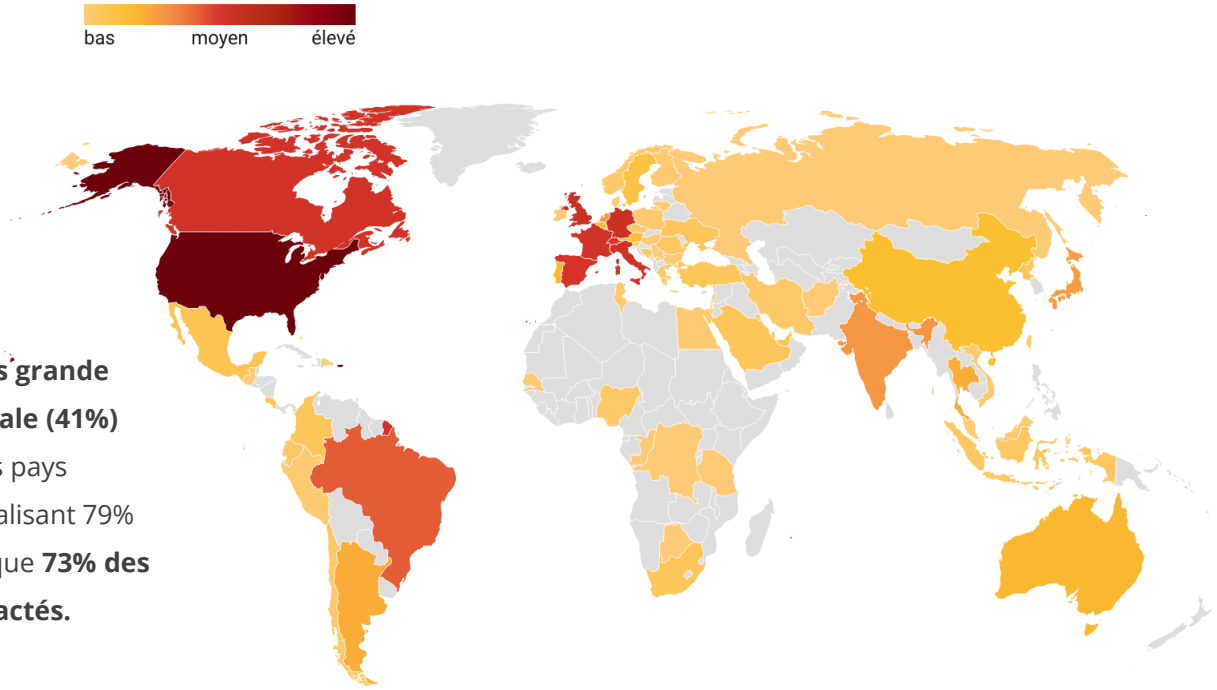
La perte de CA annuel par entreprise est estimée en moyenne à 27% [1], hors paiement éventuel d'une rançon qui peut s'élever jusqu'à 128 000€ en moyenne par entreprise.

[1]Ce coût comprend les pertes directes et indirectes de l'entreprise. ***Les pertes directes*** *prennent en compte notamment les coûts de réponse à incident et de gestion de crise, la sécurisation des données post-incident, la remise à niveau de la cybersécurité ainsi que les éventuels amendes et frais de justice liés à la perte des données.*
Les coûts indirects *concernent la perturbation ou l'interruption des activités, la perte de confiance des clients et des prestataires, l'augmentation des assurances ou encore la dépréciation de la valeur de l'entreprise.*

PAR ZONE GÉOGRAPHIQUE

janvier – avril 2022

1. **Amérique du Nord 41%**
2. **Europe 38%**
3. Asie 9%
4. Amérique latine 7%
5. Moyen-Orient 3%
6. Afrique 2%
7. Océanie 1%



Intensité du nombre d'organisations victimes de ransomware par zone géographique de janvier à avril 2022

L'Amérique du Nord concentre toujours la plus grande proportion d'attaques par ransomware mondiale (41%) suivi de près par le continent européen (38%). Les pays occidentaux restent ainsi les plus impactés en totalisant 79% des victimes mondiales. Il est également à noter que **73% des pays membres et associés de l'OTAN sont impactés.**

Le nombre d'organisations victimes en Amérique latine fait un bond spectaculaire sur ces premiers mois de 2022 en comptabilisant déjà l'équivalent de 60% du total de victimes dénombrées en 2021.

Cette intensification pourrait s'expliquer en partie par les récentes prises de position pro-ukrainiennes de ces pays. Une étude sur le plus long terme donnera peut-être plus d'indices Leurs institutions publiques sont particulièrement impactées.

PAR PAYS

janvier – avril 2022

Les États-Unis d'Amérique restent le pays au monde le plus impacté par la menace ransomware (37%).

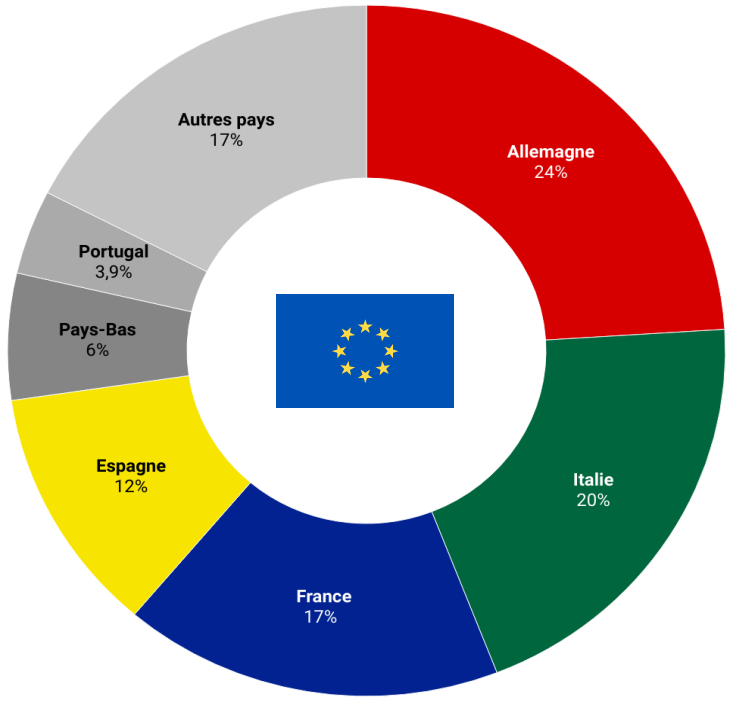
Les 3 pays de l'Union européenne les plus touchés sont l'Allemagne, l'Italie et la France. Ils concentrent plus de la moitié (53%) des victimes de ransomware de l'Union européenne. L'écart est faible entre ces trois Etats.

La France, auparavant 1er pays de l'UE en 2021 dénombrant le plus de victimes passe maintenant à la 3ème position. Cela malgré un nombre de victimes supplémentaires par rapport à l'année passée sur la même période de janvier à avril.

L'Espagne est en 4ème position puis les Pays-Bas en 5ème.

1. Etats-Unis d'Amérique 37%
2. Royaume-Uni 7%
3. Allemagne 6%
4. Italie 5%
5. France 5%

Classement mondial des pays comptabilisant le plus grand % d'organisations victimes de ransomware de janvier à avril 2022



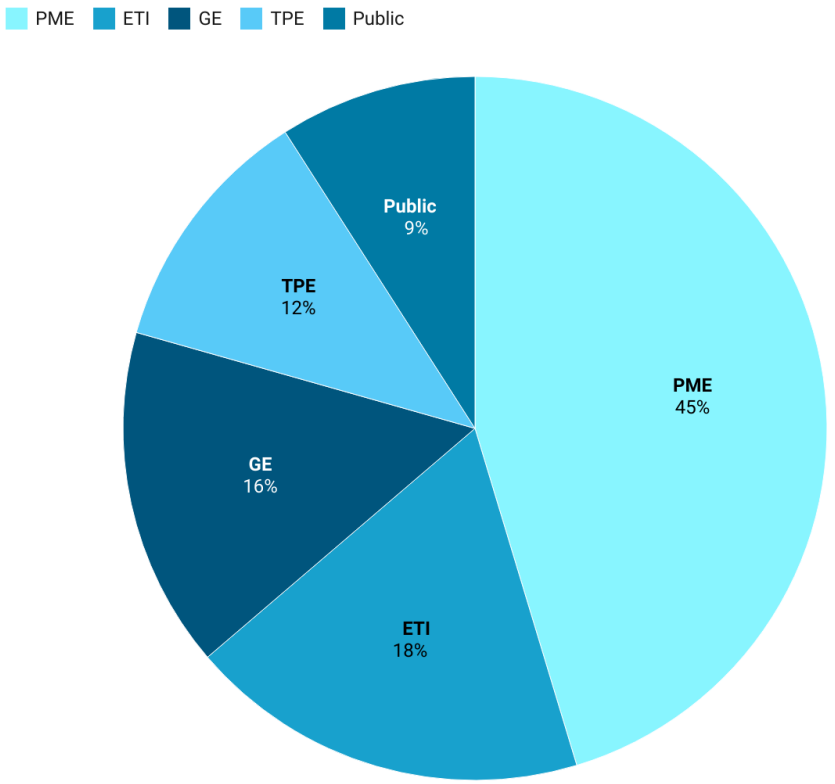
Répartition des pays de l'UE par % d'organisations victimes de ransomware de janvier à avril 2022

PAR CATÉGORIE D'ENTREPRISE

janvier – avril 2022

En France comme en Europe, une entreprise sur deux victimes de ransomware est une TPE-PME. Il s'agit des types d'entreprises les moins préparées et armées face à cette menace.

Cet indicateur conforte encore la nécessité absolue pour les plus petites entreprises d'adopter une stratégie de défense préventive efficace face au ransomware.



Répartition en % des organisations victimes par catégorie d'entreprise de janvier à avril 2022 pour les pays européens

PAR SECTEUR D'ACTIVITÉ

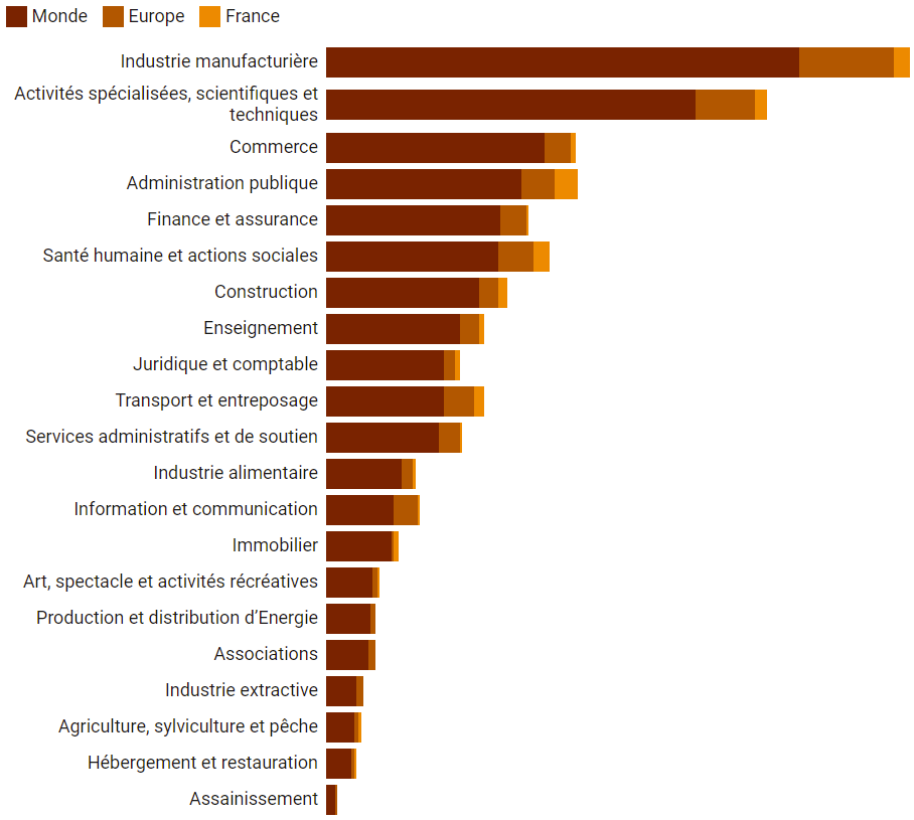
janvier – avril 2022

Comme en 2021, l'industrie manufacturière reste le secteur d'activité le plus impacté à l'échelle mondiale et européenne.

En plus d'être un secteur vaste et hétérogène, les entreprises qui le composent se sont souvent développées avant la mise en place de la cybersécurité. Les systèmes informatiques, peu adaptés et souvent obsolètes, peuvent être plus vulnérables aux cyberattaques.

Le secteur de l'énergie est particulièrement ciblé depuis ce début d'année 2022. **En quatre mois seulement, on constate déjà +138% d'entreprises de l'énergie victimes de ransomware par rapport à l'ensemble de l'année 2021.** L'ensemble de la chaine de production est impacté : industries extractives, transport, entreposage, distribution.

Dans le transport, ce sont les entreprises de l'aérien qui sont les plus touchées : **13 entreprises aéroportuaires et compagnies aériennes ont été victimes de ransomware entre janvier et avril 2022**. Cela peut s'expliquer par la reprise d'activité post-COVID et par la sensibilité des informations qu'elles détiennent.



Répartition en % des victimes de ransomware par secteur d'activité de janvier à avril 2022 dans le monde, incluant l'Europe et la France

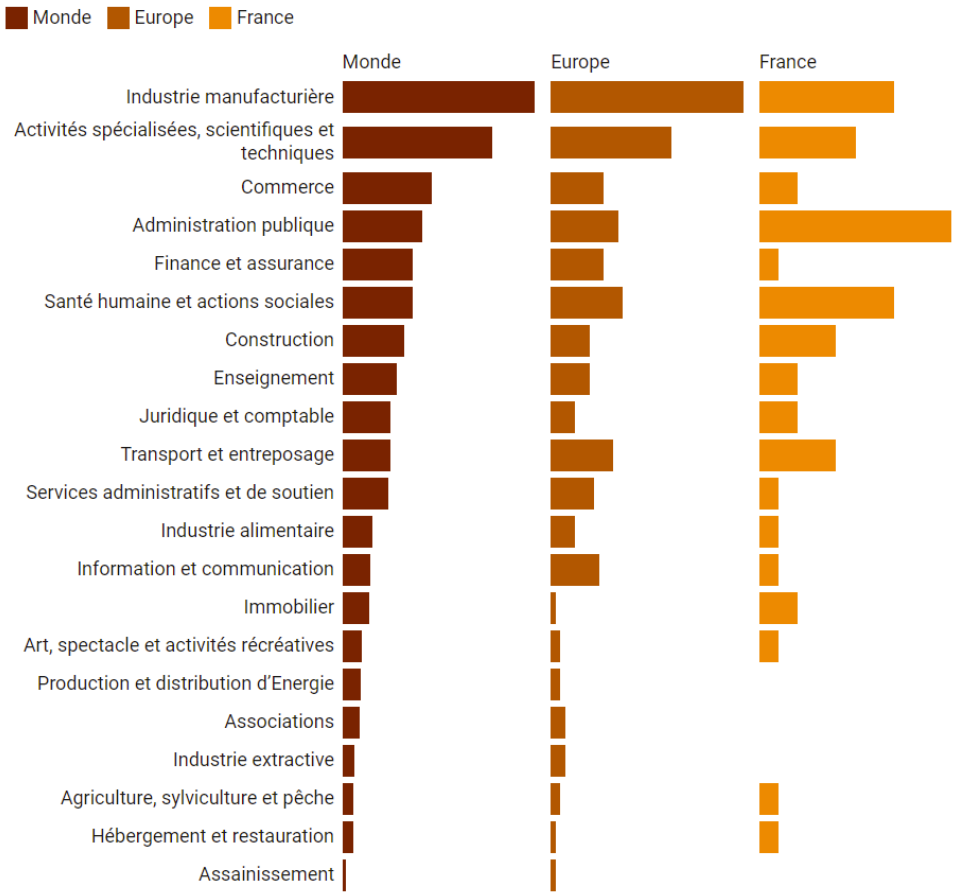
PAR SECTEUR D'ACTIVITÉ

janvier – avril 2022

Les attaques en Europe suivent les tendances mondiales avec un impact fort sur l'industrie manufacturière et le secteur tertiaire.

Plus généralement, les attaques continuent de cibler les intérêts occidentaux, tant leurs structures privées que leurs organisations publiques. La tendance haussière de ces derniers mois s'inscrit dans la continuité des constatations effectuées tout au long de l'année 2021.

En France, c'est davantage le secteur public qui essuie le plus grand nombre d'assauts : services administratifs (dont les collectivités territoriales) et secteur hospitalier notamment avec **au moins 31 établissements de soin déjà impactés entre janvier et avril 2022 en France.**



Répartition en % des victimes de ransomware par secteur d'activité de janvier à avril 2022 par zone géographique

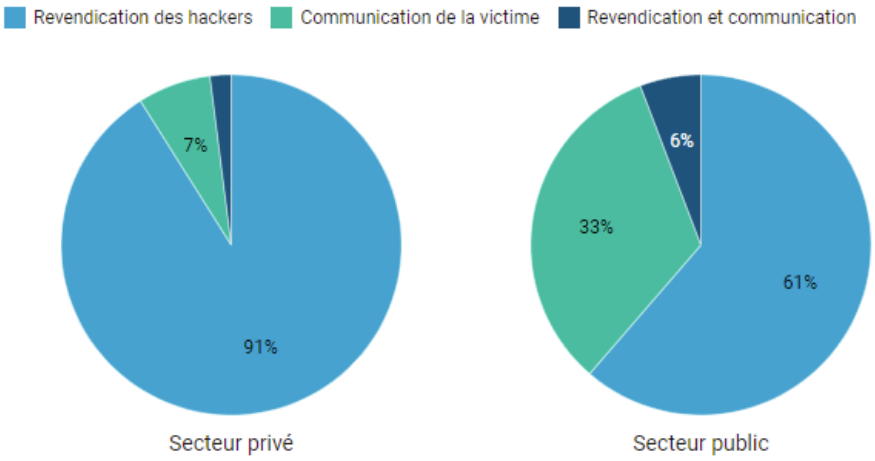
MÉDIATISATION

janvier – avril 2022

Les attaques par ransomware sur les entités publiques semblent moins souvent revendiquées. En effet, les groupes de hackers n'affichent pas ces attaques sur leur site et ne publient pas forcément les données sous le principe de la double-extorsion. **33% des attaques médiatisées par les entités publiques elles-mêmes n'ont en effet pas été revendiquées par les hackers.**

A l'inverse dans le secteur privé, seules 7% des attaques sont médiatisées par les victimes.

Cette constatation doit cependant être nuancée. Les services étatiques exercent des activités grand public et ont une visibilité importante. Ils ont un devoir de transparence et de responsabilité à l'égard des citoyens. En cas de dysfonctionnement ou d'interruption de service, ils vont donc davantage communiquer à leurs usagers que des entreprises privées qui vont favoriser une communication en interne, plus discrète.



Comparatif entre secteur privé et public de la médiatisation des cas d'attaques par ransomware réussis

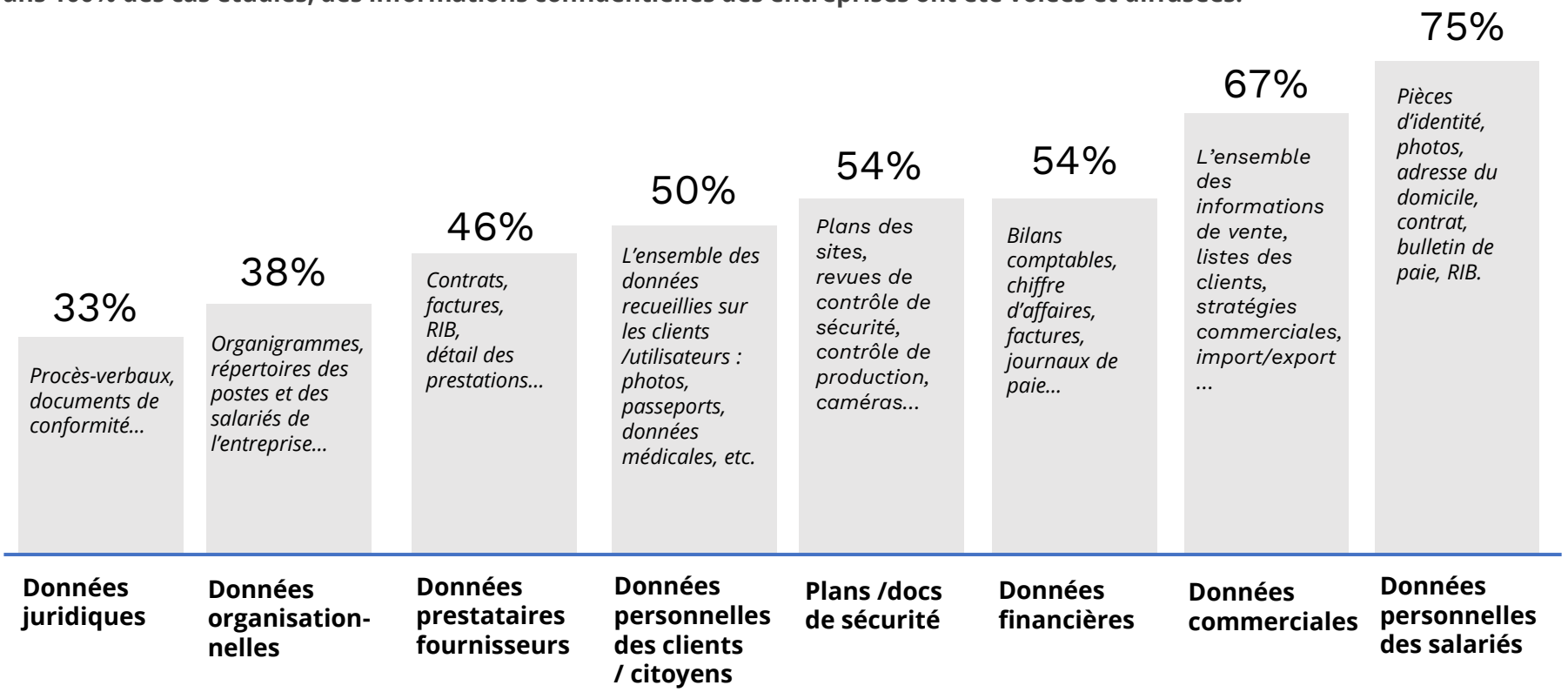
Secteur privé : ensemble des entreprises et organismes privés.
Secteur public : ensemble des entités majoritairement ou intégralement financées par l'Etat (centres hospitaliers, administrations publiques, universités).

DONNÉES VOLÉES ET DIFFUSÉES SUR LE DARKWEB

janvier – avril 2022

Les données personnelles des salariés et clients/usagers sont toujours les plus volées et diffusées par les hackers.

Dans 100% des cas étudiés, des informations confidentielles des entreprises ont été volées et diffusées.



Fréquence en % et type de données volées aux entreprises et diffusées sur le darkweb par les hackers en France de janvier à avril 2022

L'œil de l'expert

Depuis le début de l'année 2022, plus de 300 000 documents d'entités françaises ont été publiés par les groupes de ransomwares sur le darkweb. Parmi eux, plus de 213 000 l'ont été uniquement par les hackers de LockBit 2.0.

Le nombre de documents fuités varie beaucoup d'une attaque à une autre, allant de 1 320 documents à 46 340 pour une seule et même entreprise. Cela dépend à la fois du temps pris par le hacker pour récupérer les données avant le chiffrement et de la capacité de ses serveurs à les stocker.

Les données volées par les ransomwares proviennent principalement des organismes de santé avec des données médicales volées, mais aussi des collectivités et services RH avec des données d'identité et enfin à des services clients et commerciaux avec des données financières et d'authentification.

Ce sont les trois cibles privilégiées par les groupes de ransomwares et les données qu'ils peuvent le **plus revendre pour les exploiter à des fins de déstabilisation d'image, d'usurpation d'identité, de fraude fiscale et financière**. Cela leur permet aussi d'alimenter les jeux de données pour augmenter d'autres attaques ciblées, par phishing notamment et **accroître l'efficacité et le nombre de victimes.**

Les groupes de ransomwares améliorent l'efficacité de leurs outils pour l'aspiration des données car ils savent à quel point ces données sont utiles à des fins de revente. Cela alimente ce cercle infernal d'attaques compromettant encore plus **les intérêts économiques et stratégiques de l'entreprise concernée tout en exposant ses clients et collaborateurs**

IMPACT SUR LES PERSONNES

janvier – avril 2022

Français

aux données personnelles

volées et diffusées dans le darkweb

En moyenne depuis le début de l'année 2022, chaque attaque par ransomware engendre la violation de données de plus de 3 300 personnes.

Certaines attaques peuvent exposer les données personnelles de plus de **20 000 personnes pour une seule entreprise.**

IMPACT SUR LES PERSONNES

janvier – avril 2022

Le phénomène du ransomware impacte non seulement les entreprises mais atteint également leurs usagers, patients, clients, collaborateurs. Grâce aux données volées et exposées de nombreuses autres attaques, dont des arnaques financières, sont réalisables contre ces personnes.

TYPE D'ORGANISATION VICTIME DE RANSOMWARE	TYPE DE DONNÉES VOLÉES ET EXPOSÉES	EXEMPLE D'ATTAQUES RÉALISABLES
 **Hôpitaux et organismes de santé**	• Comptes-rendus médicaux • Carte vitale Mutuelle • Coordonnées (e-mail, téléphone, adresse)	↗ Fraude au remboursement des frais de maladie ↗ Atteinte à l'image par divulgation de la maladie
 **Service d'état civil des collectivités** **Serveurs RH d'entreprises**	• Bulletin de salaire, contrat de travail • Carte d'identité, passeport • Avis d'imposition • Justificatif de domicile • Permis de conduire, carte grise • Arrêt de travail	↗ Usurpation d'identité de type faux permis ↗ Usurpation d'identité pour ouverture de compte et prêt bancaires ↗ Usurpation d'identité pour création de faux passeport ↗ Réalisation d'acte malveillant sous fausse identité ↗ Fraude à l'aide sociale
 **Serveurs clients et commerciaux**	• RIB • Carte bancaire • E-mail • Adresses • Mots de passe utilisateurs	↗ Fraude bancaire ↗ Phishing ciblé ↗ Intrusion sur compte en ligne personnel

IMPACT PAR REBOND

janvier – avril 2022

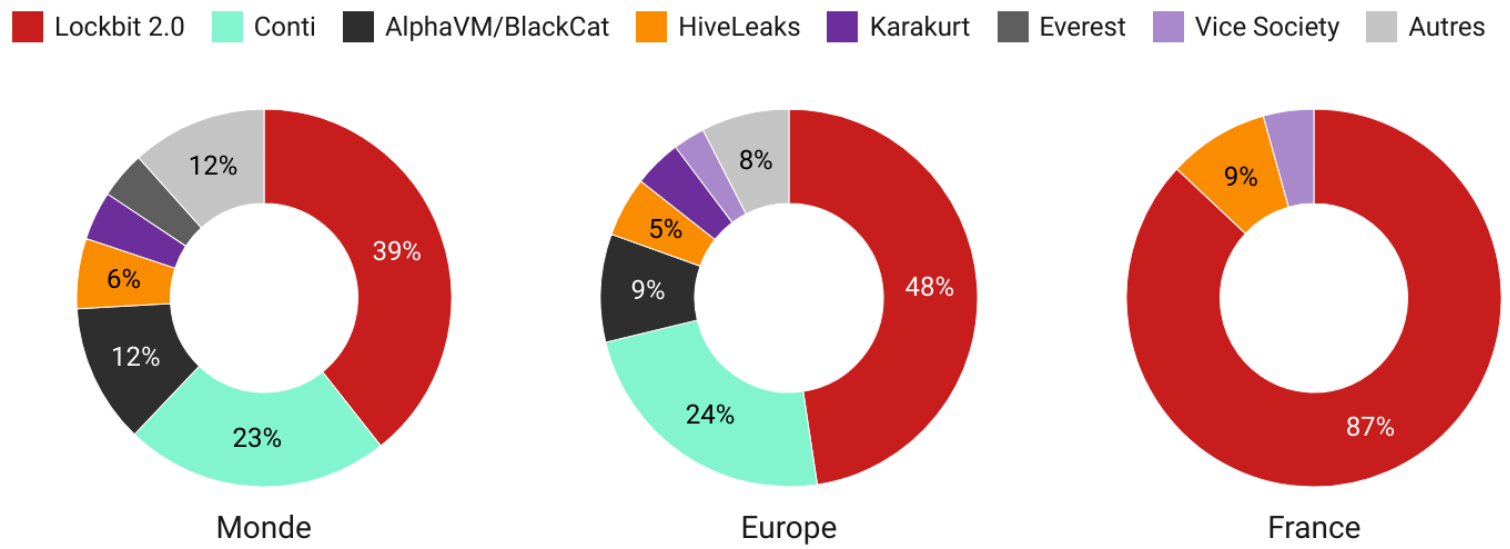
7 050

entreprises françaises exposées aux attaques par rebond
à la suite d'attaques réussies de janvier à avril 2022

L'observation des mécanismes à l'œuvre en 2021 avait déjà démontré que les données récupérées lors des attaques sont massivement utilisées par les groupes de hackers.
Ces attaques sont rendues possibles par les données sensibles volées et exploitées lors d'attaques précédentes. **Pour une seule entreprise attaquée, en moyenne 150 autres sont en danger.**
Les impacts juridiques sur l'image et sur les relations commerciales liés à ces rebonds sont considérables et ne doivent pas être écartés.

PAR FRANCHISES DE RANSOMWARE

janvier – avril 2022



Sans grande surprise, les franchises LockBit 2.0 et Conti poursuivent leurs activités en 2022 en tenant la tête du classement des groupes les plus actifs au niveau mondial. Ils sont désormais suivis du groupe AlphVM / BlackCat.

Les trois franchises de ransomware les plus actives représentent à elles seules près de 6 attaques revendiquées sur 10 dans le monde. L'organisation cybercriminelle Lockbit 2.0 domine le marché du RaaS en comptabilisant le plus grand nombre de victimes sous sa bannière.

En ce qui concerne Conti, les annonces relatives à un piratage de l'intérieur ne semblent pas avoir eu d'influence sur ses activités jusqu'à fin avril puisque celui avait redoublé d'intensité depuis le mois de février 2022. Cette franchise doit être particulièrement surveillée : mi-mai, le groupe a annoncé la fin de son activité après 15 jours sans nouvelle attaque revendiquée. Il est hautement probable que le groupe reprenne son activité sous un autre nom ou qu'il réapparaisse dans quelques semaines ou quelques mois.

Les franchises de ransomware n’ont jamais été aussi nombreuses

Le milieu du ransomware est en constante mutation. Hormis les 2 groupes les plus actifs, LockBit 2.0 et Conti, présents depuis plus d'un an, toutes les autres franchises ne jouissent que d'une durée d'activité limitée, allant de quelques semaines à quelques mois. On assiste à un ballet incessant de créations, arrêts et restructurations de groupes de ransomware. Néanmoins, **le nombre de groupes actifs simultanément reste élevé depuis 2021 : autour de 35 à 40 organisations toujours dénombrées en avril 2022.**
Depuis le début de l'année 2022, certaines enseignes ne semblent plus être en activité. C'est notamment le cas des groupes Pysa et Spook, inactifs depuis décembre 2021. Des groupes comme Rook et Sabbath semblent également avoir mis en pause leurs activités : leur site n'est actuellement plus disponible.

Cette période a également vu l’émergence de nouvelles franchises. S'il est parfois difficile de confirmer rapidement qu'il s'agit effectivement de ransomware, certaines sont déjà très actives comme BlackShadow, LeakTheAnalyst, Pandora, Stormous et très récemment Black Basta (26 avril) et Onyx dont le site a été mis en ligne le 27 avril.
Le groupe Lapsus$, en proie à des démêlés judiciaires au Royaume-Uni, poursuit son activité et allonge la liste de ses victimes : Globant, Microsof, Okta, LG, Samsung, Nvidia.

Le groupe AlphVM / BlackCat est apparu fin décembre 2021. Très probablement créé par des anciens membres et affiliés de REvil et de BlackMatter, il convoite une position de leader auprès de Conti et de LockBit 2.0. S'il ne semble pas pour le moment revendiquer autant d'attaques que ces derniers, il s’est hissé au 3ème rang mondial en peu de temps, démontrant ainsi l’élévation de ses capacités.
Ce même groupe semble bénéficier de l'appui du groupe de type furtif dit *Advanced Persistent Threat* (APT) russe dénommé FIN7, actif depuis 2014. Ce dernier cible habituellement ses victimes par la mise en œuvre de techniques de piratages de points de vente ou encore de phishing. Il serait désormais actif dans le domaine du ransomware : en conduisant ses propres attaques mais également en fournissant des codes malveillants à d'autres groupes actifs.

Lockbit 2.0 en bonne voie d'être le leader mondial du marché du ransomware

Le groupe LockBit2.0 continue sa croissance. Il recrute de plus en plus d'affiliés et améliore la qualité de son RaaS, plus rapide et plus facile d'utilisation. **Le groupe se définit lui-même comme un "business shark" dont l'objectif est le même que les entreprises qu'il attaque : accroitre sa productivité, sa compétitivité et son profit. Ces groupes sont à considérer comme de véritables organisations criminelles motivées par l'appât du gain.**
Une interview d'un membre d'AlphVM en février 2022 vient confirmer cette théorie. Le pirate explique comment ses développeurs améliorent constamment leur business model pour le rendre plus rentable.

La communication est également un aspect essentiel pour les groupes de ransomware. Ils créent et alimentent des sites vitrines hébergés sur le DarkNet. Cela leur permet d'asseoir durablement leur réputation et d'appuyer leur capacité de nuisance. Black Basta et Onyx, derniers arrivés dans la sphère, disposent déjà de leur propre site hébergé sur le DarkNet.

En 2020, un cartel de ransomwares avait été créé avant de disparaitre quelques mois plus tard. Le MAZE CARTEL consistait en un partenariat entre Conti, LockBit2.0, Ragnar Locker et Maze ransomware. Si aucune attaque concertée ne semble en avoir découlé, ce style de partenariat commercial pourrait à l'avenir se généraliser.

Le conflit en Ukraine a encore plus dévoilé les intentions capitalistiques de ces groupes. Ils ne se sont pas directement impliqués dans le conflit, privilégiant leur activité lucrative classique à l'hacktivisme politique.

Les groupes de ransomware sont-ils au service d'Etats ?

Dans une logique capitalistique, les groupes de ransomware peuvent choisir de travailler temporairement pour un Etat ou même en être un affilié direct. Les fortes nuisances provoquées par l'impact d'un ransomware couplées au vol de données sensibles sont autant de clés qui peuvent être utilisées par les Etats pour mener leur guerre hybride.

Cette théorie peut être justifiée par le nombre de victimes stratégiques ou touchant à la sécurité de la nation. L'exemple le plus probant est certainement les attaques en masse des médias portugais par le groupe Lapsus$ en janvier et février 2022. Si les groupes médiatiques ont bien confirmé le vol de données particulièrement sensibles, celles-ci n'ont jamais été publiées ou mises à la vente depuis. **Cela pourrait se justifier par la récupération de ces informations par des services de renseignement, moyennant une rémunération conséquente du groupe.** A noter cependant la spécificité de Lapsus$, qui ne semble pas toujours déployer de ransomware lors de ses attaques.

Pour certains groupes, cet accord avec des Etats peut permettre une meilleure reconnaissance avec des moyens supérieurs mis à leur disposition et des revenus moins aléatoires. Il est cependant difficile d'imaginer que les grands groupes de RaaS puissent abondamment utiliser cette stratégie : leur volonté d'expansion n'est que très peu compatible avec des partenariats étatiques évidents. Cela s'est notamment vérifié avec la débâcle de Conti lors de sa prise de position pour le gouvernement russe au début du conflit en Ukraine. Très rapidement, certains affiliés se sont retournés contre le groupe en guise de protestation de leur parti pris. Conti a été obligé de faire marche arrière pour ne pas perdre d'affidés et ainsi de gains financiers.

MÉTHODOLOGIE DE L'ÉTUDE

Le baromètre repose sur une étude inédite des attaques par ransomware revendiquées par les cybercriminels et des données volées divulguées dans le darkweb.
Cette étude se concentre sur les cas d'entreprises et organisations victimes de ransomware avérés, qu'ils soient revendiqués par les groupes de hackers ou médiatisés. L'étude recense 1 142 attaques, représentant 80 pays impactés par 42 groupes de ransomware entre janvier et avril 2022.
Ce baromètre n'a pas pour visée d'être exhaustif mais de mesurer et décrypter les évolutions et tendances du phénomène ransomware.

Cette étude est réalisée par :
Alban Ondrejeck : expert en cyberdéfense et intelligence économique, ex-officier des services de renseignement français
Julie Clauss : experte en géopolitique et influence cyber, ex-analyste du ministère des Armées
Fabrice Litaize : ex-gendarme expert en lutte contre la cybercriminalité et contre le blanchiment d'argent

Champ d'étude : les cas d'entreprises victimes d'attaques par ransomware (ou rançongiciel) réussies, revendiquées sur le darknet par les groupes de hackers opérateurs de ransomware et/ou médiatisées.
Période : janvier à avril 2022
Périmètres géographiques : France, Europe, Monde
Sources : données publiées issues du darkweb et analysées par le Lab ANOZR WAY, et communications des organisations victimes

À PROPOS D'ANOZR WAY

ANOZR WAY est une startup française spécialisée dans l'analyse des données exposées sur le web, darkweb, et la protection des personnes face aux risques cyber. Fondée à Rennes en 2019 par Alban ONDREJECK, ancien officier des services de renseignement français, et Philippe LUC, ancien dirigeant dans le secteur de l'assurance, ANOZR WAY a développé une technologie propriétaire innovante multi-récompensée à base d'Intelligence Artificielle et « Data Science ».

Les solutions logicielles ANOZR WAY permettent aux dirigeants d'entreprises et à leurs collaborateurs de maîtriser leur empreinte numérique pour se protéger face à des menaces d'ingénierie sociale, d'usurpation d'identité, d'espionnage, de ransomware, de vol de données etc.

Avec une première levée de 2M€ en 2021, BPI, Breizh Up et BNP Développement sont au capital, ANOZR WAY est en phase d'accélération avec une croissance de +271% et compte 30 collaborateurs.

Site web : www.anozrway.com
LinkedIn : linkedin.com/company/anozrway
Twitter : twitter.com/anozrway