

Ransomware : en 4 mois seulement, le nombre d'organisations victimes dans le monde déjà égal à 50% de celui de 2021

Rennes, le 30 mai 2022 – ANOZR WAY, startup française spécialisée dans la protection des personnes face aux risques cyber, révèle les résultats de son troisième Baromètre du ransomware (ou rançongiciel) en France et dans le monde. Dans cette publication, les dirigeants de la start-up soulignent la proportion élevée d'attaques par rapport à l'année précédente et alertent sur les conséquences pour le secteur privé, public et les citoyens. L'impact économique pour les entreprises françaises victimes est estimé à 660 millions d'euros de perte de chiffre d'affaires cumulé. Chaque entité victime de ransomware peut exposer jusqu'à 20 000 personnes au vol et à la diffusion de leurs données personnelles dans le darkweb, engendrant à leur tour des usurpations d'identité et arnaques financières. En France, les attaques par ransomware sont à 87% revendiquées sous la bannière LockBit 2.0, qui est en bonne voie pour devenir leader mondial du marché du ransomware.

C'est un constat sans appel : après une apparente accalmie au début d'année, la menace ransomware s'aggrave. En 2022, en seulement 4 mois, le nombre d'organisations victimes de ransomwares dans le monde est déjà égal à 50% de celui de 2021.

Durant cette période, l'Amérique du Nord concentre toujours la plus grande proportion mondiale d'attaques par ransomware (41%) suivi de près par le continent européen (38%). **L'Allemagne, l'Italie et la France, en 3^{ème} place, concentrent la moitié (53%) des organisations victimes de ransomware de l'Union européenne.**

Les attaques en Europe suivent les tendances mondiales avec un impact fort sur l'industrie manufacturière et le secteur tertiaire. L'impact économique pour les entreprises françaises victimes est conséquent, puisqu'entre janvier et avril 2022 on estime à **660 millions d'euros les pertes de chiffre d'affaires cumulées.**

Depuis le début de l'année, on recense **+138% d'entreprises du secteur de l'énergie victimes de ransomware par rapport à l'année 2021 entière.** Le contexte du conflit entre la Russie et l'Ukraine, qui place l'énergie au cœur des débats européens, confère aux entreprises de ce secteur un statut de cible stratégique.

En France, le secteur public comptabilise le plus grand nombre d'assauts : services administratifs dont les collectivités territoriales et le secteur hospitalier notamment. Au moins 31 établissements de soin ont déjà été impactés entre janvier et avril 2022. Cette sur-représentation du secteur public, en comparaison aux autres pays européens, intervient alors que la France est en pleine période électorale.

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

Alban ONDREJECK, co-fondateur et CTO (Chief Technology Officer) d'ANOZR WAY : « *Après une accalmie toute relative fin 2021 et début 2022, le volume d'organisations victimes de ransomware est rapidement revenu à un haut niveau. L'état*

de la menace **est élevé avec 35 à 40 groupes de ransomware simultanément 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 pour certains, ces cybercriminels 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**. ».

Les trois franchises de ransomware les plus actives représentent à elles seules près de **6 attaques revendiquées sur 10 dans le monde** (LockBit 2.0, Conti et AlphVM / BlackCat). En **France**, les attaques par ransomware sont à **87%** revendiquées sous la bannière **LockBit 2.0**.

Ces groupes sont à considérer comme de véritables organisations criminelles motivées par l'appât du gain. Le cyberconflit lié à la situation en Ukraine a encore plus dévoilé les intentions capitalistiques de ces groupes. La poursuite de leurs activités lucratives a en effet été privilégié par rapport à l'hacktivisme politique.

Les Français largement impactés par le vol de leurs données personnelles

Depuis le début de l'année 2022, plus de **300 000 documents sensibles d'entités publiques et privées françaises** ont été publiés par les groupes de ransomwares sur le darkweb. 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.

En 2022, en quatre mois, au moins **168 300 Français** ont été directement concernés par le **vol et la diffusion de leurs données personnelles dans le darkweb**. Certaines attaques peuvent exposer les données personnelles de plus de **20 000 personnes pour une seule et même entité victime**.

En attaquant les hôpitaux et organismes de santé et les services d'état civil des collectivités, ce sont les données **médicales et d'identité des citoyens** qui sont volées - comptes-rendus médicaux, carte vitale, justificatif de domicile, permis de conduire etc. Dès qu'un serveur d'entreprise RH ou commercial est impacté par un ransomware, les données **financières et personnelles des collaborateurs et clients** sont exposées - bulletin de paie, RIB, identifiants de connexion de comptes en ligne etc.

De cette manière les **citoyens sont exposés à l'usurpation de leur identité pour ouverture de compte et prêt bancaire, création de faux passeport, fraude au remboursement des frais de maladie et autres arnaques financières**. Ce phénomène nous révèle que la menace ransomware impacte non seulement les organisations privées et publiques mais aussi leurs usagers, patients, clients, collaborateurs.

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](https://www.linkedin.com/company/anozrway) Twitter : twitter.com/anozrway

Contacts presse ANOZR WAY

Lucas RENNESSON

lucas.rennesson@mascaret.eu

06 30 76 97 61

Benjamin MAITREHEU

benjamin.maitreheu@mascaret.eu

06 14 63 93 10