COMMUNIQUÉ DE PRESSE

17 JANVIER 2022

Ransomware : après une année 2021 record, la France sera exposée à 2 fois plus d'attaques en 2022

Rennes, le 17 janvier 2022 – ANOZR WAY, entreprise française spécialisée dans la lutte contre le piratage par ruse et l'analyse de données cyber, révèle les résultats de son second baromètre du ransomware (ou rançongiciel) en France. À l'occasion de cette publication, les dirigeants de la start-up rennaise alertent sur la viralité des ransomwares : pour 1 entreprise attaquée, 150 autres sont en danger à cause des fuites de données sensibles. L'étude révèle aussi que les données piratées viennent constituer de véritables bases d'informations personnelles des citoyens français. Au moins 680 000 français ont été directement concernés par l'exposition de leurs données personnelles, dont des dossiers médicaux et pièces d'identité.

2022 : une année qui s'annonce deux fois plus virulente

L'année écoulée a connu un nombre record d'entreprises victimes de ransomware, en particulier au second semestre : au niveau mondial, le nombre d'attaques revendiquées a bondi de **200% entre le mois de juillet et le mois de novembre 2021.** En France, le nombre d'entités impactées a également augmenté de manière exponentielle : en moyenne, une entreprise française est attaquée tous les deux jours. Il est important de préciser que l'état réel de la menace actuelle est largement sous-estimé puisque **65% des cas d'entreprises impactées par un ransomware ne sont pas médiatisés.**

L'observation des mécanismes à l'œuvre en 2021 a démontré que les données récupérées lors des attaques sont massivement utilisées par les groupes de hackers. **Plus de 13% des cas d'attaques par ransomware en France touchent des partenaires ou clients d'une première entreprise victime.** Ces attaques sont rendues possibles par les données sensibles volées et exploitées à la première entreprise. A titre d'illustration, en 2021 les données volées à une première entreprise, ont permis au groupe de hackers Everest de réaliser 100% de leurs autres attaques en France. **Pour une seule entreprise attaquée, en moyenne 150 autres sont en danger.**

Alban ONDREJECK, co-fondateur et CTO (Chief Technology Officer) d'ANOZR WAY : *« Ce phénomène d'attaques par rebond d'entreprises en entreprises est en train de s'intensifier. Nous avons la preuve que les pirates analysent finement les données exfiltrées afin d'y trouver de quoi mener de nouvelles attaques. C'est une véritable bombe à retardement.* ***La France peut s'attendre au moins à 2 fois plus de victimes par ransomware en 2022. »***

La France est le 1er pays ciblé dans l'Union Européenne en 2021

Cette première place a des conséquences directes sur l'économie et la stabilité du pays. Financièrement d'abord, cela représenterait **2,5 milliards d'euros de pertes de CA cumulées pour les entreprises victimes.** Ces attaques participent également à déstabiliser le tissu économique en ralentissant la productivité.

Stratégiquement enfin, ANOZR WAY rappelle que 59% des entités victimes en 2021 travaillent avec des grands groupes ou disposent d'informations sensibles pour la défense et l'indépendance de la nation. Des PME peuvent ainsi servir de passerelles pour atteindre des entités stratégiques.

L'intensification de la menace pèse particulièrement sur les PME, qui représentent 44% des entités touchées. Plus vulnérables et moins résilientes, ces petites et moyennes entreprises restent encore en 2021 moins bien protégées et alertées des répercussions d'une attaque. En moyenne, une entité perd 27% de son chiffre d'affaires annuel dans une attaque. Pour une petite entreprise, cela peut même l'obliger à mettre la clé sous la porte.

Il est aussi primordial de rappeler qu'une attaque par ransomware ne s'arrête pas avec la reprise de l'activité : les données volées restent exploitables et constituent des clés de voûte pour de nouvelles nuisances.

Les données personnelles des Français, véritable butin des attaques par ransomware ?

Au-delà d'impacter les entités touchées et leurs partenaires, **ces données volées viennent constituer de véritables bases d'informations personnelles des citoyens français.** Dans 87% des attaques, des informations personnelles soumises au Règlement Général sur la Protection des Données (RGPD) ont fuité et circulent dans le darkweb.

A partir d'un seul échantillon analysé par ANOZR WAY, **680 000 français ont été directement concernés en 2021 par l'exposition de leurs données personnelles,** du fait des vols de données des entreprises piratées par ransomware. En effet, chaque entité victime de ransomware expose en moyenne 5 500 personnes (collaborateurs, clients, patients). Ces données concernent des documents d'identité (carte d'identité, passeport, numéro de sécurité sociale) mais aussi des informations médicales et des données financières (RIB, prêts). Ces informations constituent une mine d'or pour les cybercriminels afin de mener des usurpations d'identité et arnaques financières.

À PROPOS D'ANOZR WAY

ANOZR WAY est une start-up rennaise spécialisée dans la lutte contre le piratage par ruse. Fondée 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 mis au point une solution alliant Intelligence Artificielle et analyse des données en Sources Ouvertes Internet. ANOZR WAY propose aux dirigeants d'entreprise et à leurs collaborateurs les moyens de se prémunir des risques cyber. Avec une première levée de 2M€, ANOZR WAY compte BPI, Breizh Up et BNPP Développement dans son capital.

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

Contacts presse ANOZR WAY

Lucas RENNESSON
lucas.rennesson@dentsuconsulting.fr
06 30 76 97 61

Benjamin MAITREHEU
benjamin.maitreheu@dentsuconsulting.fr
06 14 63 93 10