Comment mieux protÃ©ger ses donnÃ©es ?
Internet
PostÃ© par : JulieM
PubliÃ©e le : 2/2/2022 13:00:00

Câ□□est une annÃ©e 2022 qui commence sur les chapeaux de roues en matiÃ¨re de cybermenaces. Des pirates de Lockbit 2.0 ont revendiquÃ© le vol de fichiers au ministÃ¨re de la Justice franÃ§ais. Les attaquants menacent de diffuser des informations confidentielles au grand jour dâ□□ici deux semaines, le 10 fÃ©vrier 2022, faute de ranÃ§on.

L'attaque confirmÃ©e par le ministÃ¨re de la Justice, nous apprend que les donnÃ©es obtenues par le biais du ransomware Lockbit contiennent des fichiers de toutes sortes (audio, excel, pdf, photos ect..) et seraient hautement confidentielles.

Cette menace est la preuve quâ□□il existe encore des lacunes majeures dans les systÃ¨mes de sÃ©curitÃ© et protection des donnÃ©es. Certes, les failles de sÃ©curitÃ© et autres cyberattaques font souvent la une des mÃ©dias, mais il ne sâ□□agit quâ□□une petite partie Ã©mergÃ©e de lâ□□iceberg.

Dâ□□aprÃ¨s Brian Spanswick, CISO chez Cohesity :

â□□Les ransomwares demeurent un type de cyberattaque puissant et potentiellement dÃ©vastateur en France et dans d'autres pays du monde. Les ransomwares as a Service (RaaS) en particulier ont connu une Ã©volution continue en 2021 et nous nous attendons malheureusement Ã voir une augmentation d'attaques au niveau mondial en 2022.

Les attaquants, qui tentent d'infiltrer les systÃ¨mes informatiques pour accÃ©der Ã des donnÃ©es sensibles, les supprimer et les exfiltrer et tenter d'extorquer de l'argent aux propriÃ©taires de ces donnÃ©es, font constamment Ã©voluer leur approche pour contrer les mesures prises pour les bloquer. InÃ©vitablement, cela signifie que les responsables de la protection des systÃ¨mes et des donnÃ©es informatiques doivent Ã©galement faire Ã©voluer leurs stratÃ©gies.

Ils doivent amÃ©liorer leur posture de sÃ©curitÃ© avec des capacitÃ©s de gestion des donnÃ©es modernes qui fournissent des instantanÃ©s de sauvegarde immuable, des algorithmes de chiffrement robustes, des contrÃ´les d'accÃ¨s stricts, et peuvent offrir une dÃ©tection et une analyse alimentÃ©es par l'IA qui peuvent aider Ã identifier les anomalies qui pourraient signaler une attaque en cours.

En 2022, l'appel Ã l'action pour les DSI et les RSSI est non seulement de s'assurer que leurs dÃ©fenses sont robustes et capables de faire face Ã l'Ã©volution des stratÃ©gies de ransomware, mais aussi de mettre en place un ensemble appropriÃ© de plans de restauration pour faire face aux problÃ¨mes lorsqu'ils surviennent, ce qui, pour certaines entreprises, se produira inÃ©vitablement."