Ransomware : un tiers des entreprises sont impactées

C'est l'un des enseignements d'une enquête* internationale menée par la société d'études IDC en juillet 2021 auprès de 791 décideurs informatiques de moyennes et grandes entreprises. 37% des organisations ont été la cible d'une ou plusieurs attaques de ransomware ces 12 derniers mois.

« Les ransomwares ont évolué. Ils sont plus sophistiqués, se déplacent latéralement, élevent les privilèges, échappent activement à la détection, exfiltrent les données et tirent parti de l'extorsion multiforme », a déclaré Frank Dickson, VP de programme produits de cybersécurité chez IDC.

Les entreprises actives dans les secteurs de la production manufacturière et de la finance ont enregistré les taux d'incident les plus élevés sur la période étudiée.

Selon une autre analyse (celle d'ESET), entre janvier 2020 et juin 2021, les systèmes du fournisseur de solutions de cybersécurité ont détecté plus de 71 milliards d'attaques contre le protocole RDP (Remote Desktop Protocol) couramment utilisé pour l'accés à distance à des postes de travail. Il est aussi le vecteur initial d'attaque de ransomware le plus courant et ce depuis plusieurs années.

Face à la multiplication d'attaques de ransomware, dont celles contre Accenture et Kayesa dernièrement, et des centaines de millions d'attaques par force brute au quotidien, « rester sans défense n'est plus une option », a souligné Ondrej Kubovič, security evangelist chez ESET.

250 000 dollars de rançon en moyenne

IDC, de son côté, a relevé que seules 13% des organisations qui ont subi une attaque ayant bloqué l'accès à leurs systèmes ou données disent « ne pas avoir payé » une rançon.

Pour d'autres qui indiquent avoir payé dans l'espoir de reprendre le contrôle de leurs actifs, le montant moyen versé a atteint 250 000 dollars par demande de rançon. Mais cette moyenne est faussée par quelques requêtes qui dépassent allégrement le million de dollars.

Dans l'attaque cyber contre la société de conseil Accenture, un groupe d'attaquants a demandé 50 millions de dollars en échange de 6 To de données. Dans l'attaque contre l'éditeur américain de logiciels Kaseya, 70 millions de dollars ont été demandés en contrepartie du déchiffrement de fichiers. Mais Kaseya a dit avoir obtenu l'outil de décryptage, sans paiement de rançon.

*source : « IDC's 2021 Ransomware Study: Where You Are Matters! »