Ransomwares : les 3 secteurs les plus ciblés

L'entreprise de cybersécurité Trellix (anciennement FireEye et McAfee Enterprise) a livré son rapport sur les menaces avancées de sécurité au troisième trimestre 2021.

REvil/Sodinokibi, BlackMatter, LockBit 2.0… « Au troisième trimestre de 2021, les groupes de ransomwares (rançongiciels) de haut niveau ont disparu, sont réapparus, se sont réinventés et ont même tenté de changer de nom, tout en restant pertinents et répandus en tant que menace diffuse et potentiellement dévastatrice contre un spectre croissant de secteurs », soulignent les auteurs du rapport Trellix.

Selon l'entreprise de cybersécurité, les services bancaires et financiers ont été la cible la plus courante, à l'échelle mondiale, des attaques de ransomwares au cours de la période de référence, représentant 22% des attaques détectées. Les services publics et le commerce de détail (retail) arrivent ensuite, agrégeant respectivement 20% et 16% des attaques.

Les assauts contre ces trois secteurs combinés ont ainsi représenté 58% de toutes les attaques de ransomwares détectées entre juillet et septembre 2021.

Les autres secteurs d'activité qui ont été particulièrement visés sur la période sont l'éducation (9% des attaques), les gouvernements centraux (8%) et l'industrie (4,3%).

Quels sont les autres enseignements à retenir de ce rapport ?

Forte hausse des attaques détectées en France

Les clients basés aux États-Unis ont été la cible de plus d'un tiers (34%) des ransomwares détectés par Trellix au T3 2021. Mais c'est la France qui a enregistré le plus forte hausse (+400% en un trimestre).

Selon d'autres sources, les exploitants de rançongiciels ont revendiqué quantité de victimes françaises durant l'été 2021, des sociétés de juristes aux prestataires IT.

De nombreuses cibles sont ainsi apparues sur les « sites vitrines » de ransomwares, dont celui d'Everest, visant tout particulièrement les cabinets d'avocats, parmi lesquels Rémy Le Bonnois et Alcya Conseil. Everest a également revendiqué des attaques réussies contre Confiance Immobilier, Alltech France (nutrition animale) et XEFI (services informatiques).

Un autre ransomware, Conti, a également livré une liste particulièrement fournie de victimes sur la période étudiée. L'intégrateur Solware, l'antenne Côtes-d'Armor du réseau d'expertise comptable Cerfrance, Voltalia, Inserm Transfert, Aris ou encore GTID.

(crédit photo © i3d – shutterstock)