Ransomware : l'essor de la cybercriminalité en tant que service

La 4e édition du rapport franco-allemand sur la menace cyber (« common situational picture ») vient d'être publiée. L'Agence nationale de la sécurité des systèmes d'information (ANSSI) et le Bundesamt für Sicherheit in der Informationstechnik (BSI) font le constat d'une intensification des attaques par rançongiciels. Ainsi, entre 2019 et 2020, en France, leur nombre a augmenté de 255%.

Les collectvités territoriales, les secteurs de la santé et les fournisseurs de services numériques ont été parmi les plus ciblés par les ransomwares sur la période.

« Initialement, les ransomwares étaient le plus souvent utilisés contre des utilisateurs individuels et les demandes de rançon étaient relativement faibles », soulignent les auteurs du rapport. Depuis, la cybercriminalité en tant que service (CCaaS ou Cybercrime-as-a-Service) monte en puissance à travers, notamment, le Ransomware-as-a-Service (RaaS) et le recours à des courtiers d'accès.

Par ailleurs, davantage de groupes cybercriminels aux ressources et aux compétences techniques élevées ciblent les réseaux de grandes entreprises et institutions afin d'exiger d'elles des rançons significatives, voire de saboter leurs objectifs. Ces attaques dites de « chasse au gros gibier » (« Big Game Hunting », BGH) visent des organisations aux activités critiques.

« Ne payez pas la rançon »

Ryuk, DoppelPaymer, Egregor, REvil… Les ransomwares évoluent. Ils se déplacent latéralement, élevent les privilèges, échappent activement à la détection, exfiltrent les données et tirent parti de l'extorsion multiforme, comme l'a récemment relevé le cabinet d'études IDC.

L'hameçonnage (phishing), les site web compromis, un accès RDP (Remote Desktop Protocol) mal sécurisé, des vulnérabilités exploitées et des attaques de la chaîne d'approvisionnement constituent les principaux vecteurs d'attaques par rançongiciels.

L'ANSSI et le BSI rappellent dans leur rapport que le paiement d'une rançon ne garantit ni l'obtention d'un moyen de déchiffrement, ni la récupération des données exfiltrées. En revanche, les fichiers modifiés lors de l'attaque peuvent être corrompus et l'entité ciblée pourrait l'être à nouveau. Aussi, payer entretient ce système frauduleux. C'est pourquoi, l'ANSSI recommande de « ne pas payer la rançon ».

La situation varie dans la pratique. Une enquête internationale a été menée par IDC cet été auprès de 791 décideurs informatiques de moyennes et grandes entreprises à ce sujet.

Seules 13% des organisations ciblées par une attaque ayant bloqué l'accès à leurs systèmes ou données n'ont pas payé de rançon. Pour celles qui ont payé, le montant moyen versé a atteint 250 000 dollars par demande de rançon. Quelques requêtes dépassant allégrement le million de dollars.

(crédit photo © Shutterstock)