Ransomwares : à quoi ressemble la cible-type ?

À quel point existe-t-il un « code moral » dans le milieu des *ransomwares* ? Des indicateurs avaient émergé, en particulier, après l'épisode Colonial Pipeline. Certains offreurs avaient en l'occurrence modifié leurs règles de fonctionnement. Entre autres, en interdisant à leurs « clients » de s'en prendre au secteur public, à la santé, à l'éducation ou aux organisations à but non lucratif.

Des signaux, il y en a aussi dans la cinquantaine de fils de discussion que KELA a examinés cet été. Leur sujet commun : l'achat-vente d'accès à des systèmes compromis. Le fournisseur israélien de solutions de cybersécurité en a notamment tiré un « profil-type » des cibles de *ransomwares*.

Le cadre de négociation de plus en plus standardisé favorise l'élaboration d'un tel portrait-robot. Trois attributs se dégagent : emplacement géographique, revenus et secteur d'activité. Ils s'influencent parfois les uns les autres. KELA donne l'exemple d'un acheteur qui fixe le revenu minimal de ses cibles à 5 millions de dollars aux États-Unis, 20 millions en Europe et 40 millions dans le « tiers-monde ».

Les États-Unis sont le pays le plus souvent mentionné (47,37 % des fils de discussion). Suivent le Canada et l'Australie (36,84 % chacun). On relève des références à des pays d'Europe dans environ un tiers des cas (31,58 %).

« Avez-vous du VMware et du Citrix ? »

Qu'en est-il des revenus ? En moyenne, le montant minimum souhaité s'élève à 100 M$. Concernant les failles visées, les accès RDP et VPN semblent constituer le « minimum acceptable ». Ressortent souvent les solutions Citrix, Palo Alto Networks (essentiellement le VPN GlobalProtect), VMware (ESXi), Fortinet et Cisco. Les accès avec droits d'admin au niveau d'un domaine impliquent un net surcoût, mais n'apparaissent pas comme une priorité chez les acheteurs.

Reflet dudit « code moral », les listes noires sont fréquentes dans les fils de discussion créés par des acteurs de l'écosystème *ransomware*. Les principales exceptions concernent l'éducation (47,37 % de ces *threads*) et la santé (même pourcentage). Suivent les gouvernements (36,84 %) et les organisations à but non lucratif (26,32 %).

En moyenne, un acheteur est prêt à débourser jusqu'à 56 250 $. Environ un tiers se montrent prêts à verser une part de leur butin ultérieur.

Photo d'illustration © Pixels Hunter – Adobe Stock