La préparation et l'anticipation, clés d'une sécurité réussie

Avec la pandémie, les cybercriminels sont de plus en plus présents et performants, profitant de failles dans les secteurs en première ligne de la crise comme la santé, la finance ou le retail. Les campagnes d'attaques malveillantes, qu'elles soient effectuées grâce à des ransomwares ou par Déni de Services (DDoS) ont fortement augmenté depuis le début de l'année et tirent profit du basculement en ligne de nombreuses activités.

Si la pandémie semble avoir ouvert de nouvelles portes aux cybercriminels, elle n'a rien de nouveau comme l'ont démontré des attaques de ransomwares perpétrées contre des organismes de santé aux quatre coins du monde ces dernières années. La visibilité sur les attaques induit également leur connaissance, et en cybersécurité, il est indispensable de connaître son ennemi.

Dans "L'Art de la Guerre", Sun Tzu pose le constat que "Qui connaît l'autre et se connaît lui-même, peut livrer cent batailles sans jamais être en péril. Qui ne connaît pas l'autre mais se connaît lui-même, pour chaque victoire, connaîtra une défaite. Qui ne connaît ni l'autre ni lui-même, perdra inéluctablement toutes les batailles. ? Des conflits tels que le philosophe a connu, à la pandémie actuelle en passant par la cyberguerre, il est indispensable de savoir contre quoi on se bat. Ainsi, force est de constater que bien que les cybercriminels utilisent différentes méthodes d'attaques dans leurs campagnes de ransomwares ou d'attaques DDoS, ces dernières possèdent des points communs - et une différence majeure.

Tout d'abord, les deux groupes sont motivés par l'appât du gain. En effet, le recours aux ransomwares vise à pousser les victimes à verser une rançon en échange de la clé de déchiffrement permettant de déverrouiller leurs fichiers. Dans le cas d'une attaque de déni de service, les pirates informatiques accompagnent leurs actions de demandes de paiement pour éviter une seconde vague qui détruirait le réseau de la victime. Si les tactiques sont différentes, elles visent pourtant le même but.

De plus, nous avons pu observer que la fréquence de ces attaques est en hausse, surtout depuis le début de la pandémie, et aurait augmenté de 25% pendant les mois du premier confinement, entre mars et juin. Pour les ransomwares, Checkpoint rapporte qu'ils sont 50% plus nombreux par jour en moyenne au troisième trimestre de 2020. Les deux méthodes ont également le même impact de disponibilité. D'un côté, les cybercriminels peuvent réaliser des attaques de déni de service afin de dégrader ou bloquer la disponibilité des services ou des ressources aux utilisateurs, lorsque dans le cas des ransomwares, la finalité d'interrompre les activités est la même et réalisable grâce au chiffrement des données, qui deviennent inutilisables.

Par ailleurs, afin de recourir au ransomware, il suffit simplement d'accéder à des programmes affiliés afin d'acheter de multiples versions, chacune avec un code source accessible. Des tutoriaux en ligne sont aussi disponibles, permettant aux plus novices de se prêter à l'exercice. Le DDoS possède la même facilité d'entrée puisque les services de lancement de ces attaques communément appelés "Booter" et "Stresser", sont disponibles à la demande et sont également simples d'accès et peu onéreux. De plus, les cybercriminels exploitent ainsi une gamme de vecteurs d'attaques toujours croissante.

Enfin, ils recherchent tous deux l'effet de surprise. Les victimes peu ou non préparées sont des cibles de choix, pour les attaques ransomwares comme DDoS, car les hackers abusent d'organisations qui manquent de sauvegardes de données de secours adéquates, de segmentation de réseau ou encore de programmes de récupération.

La principale différence entre ces deux types d'attaques réside dans la possibilité pour la victime de reprendre le contrôle. En effet, pour le ransomware, la seule solution pour espérer récupérer ses données est de payer. Tandis que pour le déni de service, les organisations disposant des ressources internes et externes adéquates, et qui utilisent des solutions de protection modernes, ont plus de chances de maîtriser la finalité de l'attaque. Or, dans un écosystème qui évolue rapidement et dans lequel la notion de contrôle est relative, il est important que les organisations connaissent les différents risques pour s'en prémunir et maintenir leurs activités.

La majorité des activités des entreprises se déroulant désormais en ligne, la question n'est pas de savoir si l'on va se faire attaquer, mais plutôt de savoir quand. Il est donc nécessaire pour les entreprises de se protéger au maximum contre les cyberattaques, lorsque c'est possible. Pour cela, la visibilité réseau est primordiale car elle permet d'anticiper et de se préparer aux risques et ainsi limiter leur impact sur le réseau et les données, maintenant donc l'activité. »