17.07.2023

Qu’est-ce qu’une attaque par déni de service ?

Vous aurez certainement entendu parler, au cours de ces dernières semaines, d’entreprises ou d’institutions publiques dont les services ont été compromis par des attaques informatiques, généralement des attaques DDos.

Les cybercriminels arrivent toujours à paralyser des entreprises ou des administrations entières. Souvent, ils y parviennent à l’aide de ransomwares (rançongiciels) ou crypto-malwares. Mais il existe également une autre méthode, relativement prisée ces derniers temps, à savoir l’attaque par déni de service distribué.

Une attaque DDoS (ou par déni de service distribuée) est une attaque portée contre le site web ou le serveur d'une entreprise. De nombreux dispositifs (appartenant généralement tous à un botnet) se mettent alors à bombarder leur cible de requêtes. Objectif : saturer le site ou le serveur pour le perturber ou le rendre indisponible. Les attaques DDoS portées contre les entreprises sont souvent des tentatives de chantage. Si l'entreprise ne paie pas, les cybercriminels menacent de répéter leur attaque.

Or, il n’existe malheureusement pas de protection sûre à 100% contre les attaques par déni de service. Par contre, les entreprises peuvent utiliser des services de contrôle pour détecter et bloquer les attaques DDoS. Toutefois, étant donné leur structure distribuée, ces attaques ne sont possibles qu’à un certain point. Une réduction de la surface d’attaque contribue néanmoins à minimiser les conséquences d’une attaque. Pour en savoir plus, consultez notre article « Les attaques par déni de service (https://www.ebas.ch/fr/les-attaques-par-deni-de-service/) » et notre section « Conseils pour les PME (https://www.ebas.ch/kmu) ».