

Quand les attaques DDoS servent à leurrer les équipes IT

L'entreprise de cybersécurité Kaspersky Lab et la société d'études B2B Internationale ont publié leur [enquête 2015](#) sur les attaques par déni de service distribué (DDoS). Elle a été réalisée auprès de **5 500 entreprises dans 26 pays**. Selon le rapport, les attaques DDoS ne sont ni la première cause des fuites de données, ni la menace externe qui pèse le plus lourdement sur les réseaux et systèmes d'entreprise. Les malwares et les intrusions l'emportent dans ces domaines. Mais le DDoS est de plus en plus utilisé pour détourner l'attention de la DSI tandis que d'autres attaques se préparent.

Le DDoS, un bel écran de fumée

74% des attaques DDoS ayant entraîné une interruption de service notable ont été accompagnées d'autres incidents, comme l'exécution d'un **malware** (dans 45 % des cas) ou une **intrusion** dans le réseau de l'entreprise cible (32 %). Résultat des courses : 26 % des entreprises victimes d'attaques DDoS ont déclaré une perte de données sensibles.

Les infrastructures les plus ciblées par ces attaques par déni de services sont : les sites web publics (47 %), les portails clients et les espaces d'authentification (38 %), suivis des services de communication (27 %).

Une interruption totale dans 1 cas sur 4

20 % des entreprises de 50 salariés et plus déclarent déjà avoir été victimes d'au moins une attaque DDoS (une proportion stable par rapport à 2014). Les **télécoms** (24 %), les **services financiers** (22 %) et **l'IT** (21 %) sont les secteurs les plus touchés. 50 % des attaques déclarées ont entraîné une interruption notable de service (un chargement très lent des pages Web dans 53 % des cas). Et 24 % des attaques ont entraîné une interruption totale de service (contre 13 % l'an dernier). Globalement, 35 % des attaques DDoS ont duré plusieurs heures, 21 % entre 10 minutes et 1 heure et 14 % toute une journée. Une minorité (7 %) s'est tout de même prolongée durant plusieurs semaines.

Un coût élevé pour les entreprises

48 % des organisations victimes d'attaques DDoS déclarent connaître l'identité de leurs auteurs. Une majorité cite des cybercriminels externes à l'entreprise. Et 12 % des responsables IT interrogés pointent un concurrent... Quels que soient leurs initiateurs, ces attaques ont un coût. Selon le rapport, une entreprise de 1 500 salariés et plus dépense en moyenne **417 000 dollars** pour se remettre d'une attaque par déni de service (coûts directs et indirects inclus). Une PME, qui ne dispose pas toujours des moyens pour se prémunir, débourse 53 000 dollars en moyenne.

Lire aussi :

[Les protocoles Internet de plus en plus exploités par les attaques DDoS](#)
[En 10 ans, les attaques DDoS se sont fortement amplifiées](#)

crédit photo © stockhits / shutterstock.com