Le site du gouvernement hollandais victime d’une attaque DDoS

	Le site du gouvernement hollandais victime d’une attaque DDoS

Suite à une attaque DDoS, le site du gouvernement néerlandais n'était plus accessible pendant 10 heures. L'attaque, qui a utilisé différents vecteurs, a également mis d'autres sites hors ligne.

Mardi dernier, une attaque sophistiquée par déni de service distribué (DDoS) a bloqué pendant plus de 10 heures le site du gouvernement néerlandais et d'autres sites commerciaux.
Le ministère des Affaires générales, le Centre National de la cybersécurité (NCSC), l'hébergeur Prolocation et le fournisseur de services Centric passent au crible les techniques utilisées pour mener cette attaque et tentent d'identifier ses auteurs.

« L'attaque DDoS, qui a débuté à 9 h 45 heure locale, a été difficile à contrer parce que les modalités utilisées ont changé régulièrement », a déclaré le directeur de Prolocation, Raymond Dijkxhoorn. « La stratégie était différente des attaques DDoS habituelles auxquelles nous sommes confrontés quasi quotidiennement et contre lesquelles nous arrivons plus facilement à nous défendre », a-t-il ajouté. « C'est même la première fois que nous n'arrivons pas à la contenir », a encore déclaré le directeur de Prolocation. « L'attaque visait directement les sites du gouvernement fédéral, mais elle a aussi eu pour conséquence la mise hors ligne de sites hébergés sur le même réseau », a-t-il expliqué. C'est le cas notamment du site de blogging Geenstijl.nl et de celui de l'opérateur de téléphonie Telfort, également bloqués par l'attaque. « Certains sites du même réseau ont utilisé les services de détournement anti-DDoS de fournisseurs comme Cloudflare », a aussi déclaré Raymond Dijkxhoorn. « Mais si les clients d'un même réseau ne parviennent pas tous à détourner l'attaque DDoS, il y a un de fortes chances que les autres sites soient affectés », a-t-il ajouté. Par exemple GeenStijl a utilisé Cloudflare. En général, le service arrive à maintenir le trafic jusqu'au serveur du site, même si celui-ci est visé par une attaque DDoS. « Mais le serveur de GeenStijl peut lui-même ne plus être accessible si l'attaque DDoS vise d'autres sites sur le réseau qui n'utilisent pas de service de détournement », a encore expliqué le directeur de Prolocation. Et, comme il l'a précisé, « le gouvernement néerlandais n'a pas utilisé des services de protection DDoS externes ». Selon Raymond Dijkxhoorn, l'attaque DDoS a mis en oeuvre plusieurs techniques en alternance. « Et même si Prolocation a beaucoup d'expérience en matière d'attaques DDoS, c'est la première fois que le fournisseur a du faire face à ce type de stratégie », a-t-il déclaré. À la demande du NCSC, Raymond Dijkxhoorn a refusé de donner plus de détails sur les attaques tant que l'enquête ne serait pas terminée.
Le Centre National de la cybersécurité (NCSC) et le fournisseur de services hollandais Centric ont tous deux refusé de commenter les détails de l'attaque tant que l'enquête était en cours. Mais Prolocation a évoqué l'incident avec les ingénieurs de Prolexic et d'Akamai, qui ont déjà vu des attaques DDoS basées sur des méthodes similaires ailleurs dans le monde. « Les sites hébergés sous le même bloc IP peuvent être mis hors ligne, même si un seul des sites est ciblé spécifiquement par l'attaque », a confirmé Hans Nipshagen, le directeur d'Akamai pour la Belgique, les Pays-Bas et le Luxembourg. « Si les sites du gouvernement avaient utilisé des services de filtrage DDoS externes, le réseau aurait pu tenir », a-t-il aussi ajouté. « Même s'il est difficile de savoir de l'extérieur quelles méthodes ont été utilisées contre les sites du gouvernement néerlandais, il semble que l'attaque DDoS était une attaque à grande échelle, et qu'elle a mobilisé une grosse quantité de trafic », a encore déclaré Hans Nipshagen. Selon Akamai, « certaines attaques DDoS de grande envergure utilisent de multiples vecteurs pour saturer la bande passante avec de grandes quantités de paquets à une vitesse extrêmement élevée, bloquant les sites ciblés ». Le nombre d'incidents de ce type ne cesse d'augmenter : « D'abord, les outils d'attaque sont de plus en plus faciles à utiliser. Il existe aussi une industrie criminelle florissante qui vend des services d'attaque DDoS pour le compte d'autrui », a déclaré Akamai. Après la Hollande, la France…

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.lemondeinformatique.fr/actualites/lire-le-site-du-gouvernement-hollandais-victime-d-une-attaque-ddos-60227.html