Sites d’info bloqués: La thèse de la cyberattaque écartée

	Sites d’info bloqués: La thèse de la cyberattaque écartée

Ce n’est sans doute pas la grosse attaque promise par les hackers islamistes qui s’en prennent depuis une semaine au Web français, mais le timing interroge. De nombreux sites d’information, dont 20minutes.fr, ont été bloqués une heure et demie ce vendredi matin en raison d’un incident technique chez leur hébergeur Oxalide d’une ampleur a priori inédite.

France Inter, Le Parisien, Slate… et Sushi Shop

Les sites de 20 Minutes, L’Express, Mediapart, France Info, France Inter, Le Parisien, Slate, ZDNet ou encore Marianne, tous hébergés par Oxalide, sont devenus inaccessibles vers 10h. Des sites d’e-commerce, comme Sushi Shop, ont eux aussi été perturbés. Vers 11h30 certains sont redevenus accessibles. «Le niveau actuel d’information ne permet ni d’affirmer que la responsabilité d’Oxalide soit engagée, ni qu’il s’agisse d’un acte malveillant lié à l’actualité», affirmait l’hébergeur un peu avant 13h. Un peu plus tard, il tweetait: «Les premiers éléments en notre possession nous permettent d’écarter l’hypothèse d’une attaque externe de type DDoS.»

Même s’il semble dès lors écarté, le scénario d’une cyberattaque était considéré comme plausible en fin de matinée par les experts en sécurité informatique. «Toutes les caractéristiques techniques d’une attaque par déni de service (DDoS, lorsqu’un site est noyé sous les requêtes de connexion)» étaient réunies, selon Thierry Karsenti, directeur technique Europe de l’entreprise de sécurité informatique Checkpoint. «Il s’agit probablement d’une attaque DDoS», estimait auprès de 20 Minutes Olivier Hassid, directeur général du Club des directeurs de sécurité des entreprises. «Vu les cibles, on peut penser à une attaque virtuelle venant d’islamistes», renchérissait Eric Filiol, expert à l’École supérieure d’informatique, électronique, automatique.

Mercenaires en ligne

Pour Gérôme Billois, expert du cabinet Solucom, «si une attaque par déni de service menée dans le but de nuire à la liberté d’expression était confirmée, on ne serait plus sur du menu fretin.» Car jusqu’ici, les très nombreuses cibles touchées par les hackers tendance islamistes souffraient de failles faciles à identifier souvent causées par un simple défaut de mise à jour logicielle. S’en prendre à l’hébergeur de nombreux sites de presse dénoterait une montée en puissance, peut-être rendue possible grâce à l’achat des services de cybercriminels dotés de véritables moyens.

Car comme le rappellent Gérôme Billois et Eric Filiol, la cybercriminalité est un business en pleine expansion et les hackers s’achètent comme des mercenaires. «Il existe une grille tarifaire», explique Gérôme Billois. «Pour 200 dollars, des sites hébergés en Europe centrale proposent de louer à l’heure 1.000 machines infestées permettant de lancer une attaque DDoS», illustre Eric Filiol. Qu’elle ait lieu aujourd’hui ou plus tard, une attaque contre la presse française serait peut-être moins la preuve d’une montée en puissance des «cyberdjihadistes» que de leur volonté de mettre la main au portefeuille.

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

Source : http://www.20minutes.fr/high-tech/1518695-20150116-sites-info-bloques-incident-technique-attaque-informatique
Par Nicolas Bégasse et Romain Lescurieux