Événement
La cyberguerre des nerfs des hackers

Amaelle Guiton
767 mots
16 janvier 2015
Libération
LBRT
7
Français

Des groupes opposés aux caricatures du Prophète ont mené nombre d'attaques informatiques.

Jeudi soir, les «grosses grosses surprises» promises par le compte Twitter de la Middle East Cyber Army (Meca), l'un des groupes de pirates informatiques «anti-Charlie Hebdo» se revendiquant de la défense de l'islam, n'avaient pas véritablement eu lieu. Certes, la journée a connu son lot de cyberattaques, avec une accélération à partir de 17 heures. Au nombre des victimes, l'Institut de mathématiques de Toulouse, la paroisse Saint-François des Coteaux (dans le diocèse de Nantes), la commune de Wallers-en-Fagne dans le Nord, le label régional «durable» UrbAquitaine ou encore le très évocateur Plancul-strasbourg.fr.

La Meca a également publié, peu avant 18 heures, une liste de 320 000 adresses mails provenant du site de jeu Thé ou Chocolat. Mais aucun des «opérateurs d'importance vitale» (services de l'Etat, services de santé, banques, industries…) ne semblait avoir été touché.

Pour spectaculaire que soit le phénomène, il ne relève pas, en effet, d'une grande technicité. «La très grande majorité de ces attaques sont des défigurations de sites Internet [par remplacement de leur page d'accueil] ou des dénis de service [DDoS, qui consistent à rendre inaccessibles un serveur en le saturant de requêtes] qui exploitent les failles de sécurité de sites vulnérables», explique l'Agence nationale de sécurité des systèmes d'information (Anssi). «Les attaquants profitent de failles dans les systèmes de gestion de contenu [CMS, des logiciels destinés à la conception et à la mise à jour de sites web, comme WordPress] et il est alors très simple de "scanner" automatiquement les sites pour remplacer leur page d'accueil, précise Jean-Marc Bourguignon, consultant en sécurité informatique. Il y a énormément de CMS qui ne sont pas mis à jour. L'effet est d'autant plus impressionnant.»

Bercy visé. Le site spécialisé Zataz recensait, au 14 janvier, déjà plus de 20 000 sites attaqués et identifiait au moins 27 groupes différents. Meca, AnonGhost, APoca-DZ, Fallaga Team… autant de labels aux contours flous, aux origines diverses (Algérie, Tunisie, Mauritanie, etc.) et aux motivations pas toujours cohérentes, si ce n'est l'opposition aux caricatures de Mahomet, mais également à Anonymous, contre lequel cette nébuleuse a clairement engagé l'offensive (1). Quant aux cibles visées, les pirates font manifestement feu de tout bois. «Ce qui compte, c'est de toucher le maximum de gens, de diffuser l'esprit de crainte, indique **Nicolas Arpagian**, directeur scientifique à l'Institut des hautes études et de la justice. C'est la faille qui détermine la cible. On arrive ainsi à une grande disparité à la fois en termes d'entités touchées, de taille et de géographie.»

Pour faire face à ces attaques, regroupées sous le label #OpFrance (pour «Opération France»), l'Anssi a publié mercredi deux fiches d'information, l'une à destination des administrateurs de sites web, les invitant à mettre leurs infrastructures à jour, l'autre rappelant les «bonnes pratiques» en matière de cybersécurité. Pas de quoi, donc, paniquer à ce stade. Pour **Nicolas Arpagian**, on est essentiellement dans une opération «d'agit-prop», avec pour objectif de frapper l'opinion publique.

La publication jeudi matin, par un compte Twitter se revendiquant d'AnonGhost, d'une liste de noms, prénoms, adresses mail et numéros de téléphone d'une dizaine de salariés des ministères de l'Intérieur et des Finances, relève de la même logique. Contacté par LeMonde.fr, le pirate (dont le compte a été suspendu dans la soirée) affirmait être en possession d'une base comportant au total «plus de 10 000 entrées personnelles». Sauf que les données publiées, comme l'indiquait le site du quotidien, sont périmées. Contacté par Libération, Bercy confirme qu'elles sont antérieures à 2010, et «proviendraient du site web

personnel d'un ancien stagiaire de la préfecture de police». Selon l'Anssi, il s'agirait de données déjà volées en 2010 ou 2011 et opportunément republiées.

«Moins visibles». Plus que de cyberguerre, il faudrait plutôt parler, à ce stade, de guerre des nerfs. L'ampleur des dégâts constatés démontre que nombre de sites souffrent d'un déficit de sécurité. «Jusqu'ici, ce sont des attaques de basse intensité, conclut **Nicolas Arpagian**. Cela ne doit pas empêcher d'être vigilant : cette agitation peut être une manière de détourner l'attention d'opérations moins visibles, mais plus profondes.» D'autant que l'#OpFrance n'est pas finie.

(1) Lire l'article «Anonymous et islamistes s'affrontent à coup de piratages» sur Libération.fr

5077F5A20CB0E40893D50C120206D5CF01D1A66EF1CA51297CE2900

Document LBRT000020150116eb1g0002t

