Cyber-représailles à Op CharlieHebdo : 20 000 sites français attaqués

La guerre contre le terrorisme se décline sur le terrain cybernétique depuis quelques jours après les attentats contre Charlie Hebdo et l'Hyper Casher de la Porte de Vincennes. Certains **Anonymous** ont mené une campagne baptisée **#OpCharlie** avec comme cibles des suppressions de comptes Twitter de personnes présumées en lien avec le terrorisme. Mais en menant cette bataille, ils ont activé les représailles de la part de pirates informatiques, qui se nomment Meca (Middle East Cyber), ArmyAnonGhost, Cyber Califat, Cyber Djihad, Fallag Anonyme, Virus3000, Votr3x, Prodigy TN, Makers Hacker Team, etc.

L'ensemble de ces pirates travaillent sous la bannière **#OpFrance** et ont mené depuis quelques jours une multitude d'attaques contre différents sites. En l'espace de 4 jours, des milliers de sites ont été touchés allant des administrations (mairie, centres hospitaliers, établissements scolaires, université), aux banques, des entreprises et même comble de l'ironie, une mosquée. Arnaud Coustillère, contre-amiral, officier général cyberdéfense, a indiqué à l'Associated Press que « *ce qui est nouveau et important, c'est que 19 000 sites ont été touchés, du jamais vu auparavant* ». La plupart du temps, il s'agit de simple **défaçage**, c'est-à-dire remplacer le contenu de la page d'accueil, ou des **attaques par saturation** qui rendent inaccessibles le site. Les attaquants ont utilisé des faiblesses ou des absences de mises à jour dans les systèmes de gestion de contenus (CMS) et les outils de créations de site comme **Drupal ou Joomla**, rappelle nos confrères de *Zataz*.

L'ANSSI en mode recommandation

Devant le tir croisé de la campagne #OPFrance, l'ANSSI (Agence Nationale de Sécurité des Systèmes d'Information) est montée au créneau hier pour publier ses recommandations. Elles se déclinent en une fiche à l'intention des internautes qui comprend notamment des règles de base comme choisir des mots de passe robustes, éviter l'utilisation des réseaux WiFi, des connexions en HTTPS, des navigateurs et OS mis à jour, etc. Une autre fiche s'adresse aux administrateurs de sites avec plusieurs éléments liés à la protection des sites contre la défiguration ou les dénis de services, les procédures judiciaires et techniques, etc. L'ANSSI n'est pas la seule à délivrer ses conseils. Les experts en sécurité ont pris position pour apporter des réponses à ces différentes attaques qui montrent que la cybersécurité est encore loin d'être prise en considération par les entreprises et les administrations.

Un 15 janvier sous haute surveillance

L'ANSSI a réagi devant l'annonce faite par le groupe #OPFrance de mener une attaque d'envergure le 15 janvier. Si plusieurs sites comme les universités de Toulouse et Montpellier ont été touchées, ainsi que des petites entreprises, il n'y a pas eu de violente charge contre des sites institutionnels. On notera simplement la fermeture pour cause de « *maintenance technique* » du site Internet-signalement.fr qui a pour objet de signaler les contenus illicites sur Internet. C'est à travers ce canal que les internautes peuvent avertir les autorités d'une photo, d'une vidéo ou d'un texte illicites. Ce

site est très sollicité depuis les attentats de la semaine dernière.

Parmi les autres faits d'arme, AnonGhost a revendiqué **le vol d'une ancienne base de données de fonctionnaires** du ministère des Finances et de l'Intérieur (environ 10 000 noms), selon nos confrères du *Monde*. Un tweet de Mauritania666 ce matin évoquait **le piratage visant la téléphonie mobile en France**, mais il n'y a pas eu d'échos de la part des opérateurs. Sur le fil Twitter de #OPFrance, le groupe Meca revendique le vol de **320 000 adresses emails d'un jeu**. Il faudra attendre demain pour dresser un bilan de cette cyber-guerre qui tourne de plus en plus à une bataille de communication.

A lire aussi :

Les Anonymous prennent fait et cause pour Charlie

Anonymous : OpCharlieHebdo déclenche une guerre cybernétique