Bots : ces robots sociables qui ne nous veulent pas que du bien

Énervants et surtout dangereux, les robots informatiques malveillants, plus souvent appelés bots, font partie du quotidien de chaque internaute. Convertis aux réseaux sociaux, comme une bonne partie de la population mondiale au cours des années 2000, ils s'y épanouissent aujourd'hui, guettant au détour de chaque page Facebook

Prêts à surgir au moindre clic, ils attendent l'utilisateur malheureux qui viendra se prendre les pieds dans leur toile. Les bots, ces « robots informatiques », ne ressemblent pas plus à WALL-E, l'opiniâtre robot nettoyeur du film éponyme, qu'au Terminator, montagne de muscles et de ferraille, icône populaire incarnée par un futur ex-gouverneur de Californie. Moins évocateurs mais beaucoup plus collants, les bots, logiciels automatiques programmés pour effectuer des tâches répétitives à une très grande échelle, s'adonnent plus volontiers au spam publicitaire et au phishing (vol de données personnelles, ndlr). Dans ce second cas, les cybercriminels à l'origine de ces bots vont jusqu'à créer *« de fausses demandes de paiement pour des factures EDF ou autres, dans le but de voler des données confidentielles à la victime pour les réutiliser dans des opérations de fraude bancaire et d'usurpation d'identité »*, explique Marion Couturier, consultante en Sécurité & Risk Management chez Solucom depuis 2007. Et si ces messages pirates présentent bon nombre d'incohérences et se révèlent la plupart du temps peu crédibles, il se trouve toujours des utilisateurs pour *« tomber dans le panneau »*, note la jeune femme, dont les clients sont souvent confrontés à ce genre de risques sécuritaires, notamment sur les réseaux sociaux, nouvelles cibles privilégiées des pirates informatiques.

« Socialbots »

Véritables mines d'informations privées, les réseaux sociaux n'ont en effet pas tardé à attirer les bots. Et à en croire une étude menée par quatre chercheurs de l'University of British Columbia de Vancouver, les programmeurs de ces logiciels malveillants peuvent dormir sur leurs deux oreilles. Après avoir crée 102 « socialbots », faux profils entièrement automatisés, les scientifiques de l'université canadienne les ont lâchés sur Facebook. Huit semaines de bons et loyaux services plus tard, les fidèles robots sont rentrés au bercail. Pas les mains vides, non, avec 250Go de données privées, récoltées auprès des utilisateurs qui les ont acceptés dans leur groupe d'amis. Fait alarmant : seuls 20% de ces « socialbots » ont été rattrapés par la patrouille, généralement parce qu'ils *« avaient été désignés comme spam par des utilisateurs »*, est-il précisé dans l'étude. *« En réalité, nous n'avons constaté de réactions du FIS (Facebook Immune System, l'infrastructure de sécurité du réseau* social, ndlr) que lorsqu'il avait été alerté par des utilisateurs », s'inquiètent les chercheurs, qualifiant d'efficace *« l'infiltration d'un réseau* social comme Facebook par des bots imitant de vrais utilisateurs ».

http://mcetv.fr/mon-mag/0412-bots-ces-robots-sociables-qui-ne-nous-veulent-pas-que-du-bien

Love this joliprint PDF? Add it to **your Reading List**! ⇢ joliprint.com/mag

Bots : ces robots sociables qui ne nous veulent pas que du bien

« Maintenant, je fais gaffe »

Équipés de profils Facebook censés étayer leur vraie fausse existence, les bots nouvelle génération seraient-ils plus convaincants que leurs aînés ? A en croire Hugo, 20 ans, étudiant à Paris, ce n'est pas vraiment le cas, « la faute à des méthodes d'appât encore trop voyantes ». Il se rappelle pourtant avoir succombé à l'un de ces robots du Net : *« J'ai accepté parmi mes amis Facebook une fille que je ne connaissais pas, simplement en voyant sa photo. Une créature de rêve, à la plastique parfaite. J'aurais dû me douter que quelque chose ne tournait pas rond »*. Un rapide coup d'œil au profil de sa nouvelle amie suffit à chasser ses doutes : en dehors des informations essentielles (nom, photo, date de naissance, ville de résidence), la page ne contient que des liens publicitaires vers une boutique de vêtements en ligne. *« J'ai été fixé quelques minutes plus tard lorsqu'un autre membre m'a demandé de devenir son ami. Même physique de top-model, mêmes* informations personnelles ou presque, et, surtout, les mêmes liens renvoyant vers la même page internet ». Jurant qu'on ne l'y reprendrait plus, Hugo garde de cette rencontre doublement virtuelle un souvenir amusé et une leçon édifiante pour ses futures pérégrinations sur la Toile. *« Maintenant, je fais gaffe »*, prévient-il.

Prévenir et sensibiliser

« Faire attention, être prudent, c'est encore le meilleur moyen de se prémunir contre ce type d'attaques informatiques », conseille Marion Couturier, pour qui la prévention et la sensibilisation à ces nuisances virtuelles sont primordiales. Même son de cloche chez Nicolas Caproni, expert en sécurité informatique chez BSSI Conseil & Audit et animateur du blog Cyber-sécurité.fr. *« Les bots ont toujours fait partie intégrante d'Internet, depuis les premiers forums de discussion jusqu'aux Facebook et Twitter que tout le monde connaît. Les « socialbots » n'ont pas vraiment changé la donne. La prudence reste le mot d'ordre »*, assure-t-il, avant d'ajouter que le véritable combat ne se mène pas sur un quelconque réseau social mais bien sur le terrain, *« en étroite collaboration avec les services de police, pour démanteler les réseaux de cybercriminels »*.

Arthur Bernard

http://mcetv.fr/mon-mag/0412-bots-ces-robots-sociables-qui-ne-nous-veulent-pas-que-du-bien

Love this joliprint PDF? Add it to **your Reading List**! ⇢ joliprint.com/mag