Télégrammes : le codage au collège en 2017; 140 vulnérabilités au Pentagon; un botnet de 3 millions de comptes Twitter; Cedexis ajoute les alertes à son Radar

- **Brevet des collèges : une épreuve de codage dès 2017.** Dès l'année prochaine, les collégiens de 3e devront affronter, lors du brevet, «□au moins un exercice d'algorithmique ou de programmation□». Intégré à l'épreuve de mathématiques, physique-chimie, sciences de la vie et de la Terre et technologies (d'une durée totale de 3 heures), cet exercice s'inscrit dans le cadre de la réforme du collège, qui prévoit de familiariser les élèves avec «□les principes de base de l'algorithmique et de la conception de programmes informatiques□».
- **Hack The Pentagon en chiffres.** Après le lancement du son premier Bug Bounty, appelé Hack The Pentagon, le département de la Défense américain publie les chiffres de cette opération. Menée entre le 18 avril et le 12 mai, la campagne a permis de mettre au jour 138 vulnérabilités inconnues sur les sites de l'organisation. Les 117 hackers à l'origine de ces trouvailles ont touché des primes allant de 100 à 15□000 dollars. Au total, plus de 1□400 hackers se sont enregistrés à cette chasse aux bugs et 252 d'entre eux ont soumis au moins un résultat, soit un total de 1□189 rapports de vulnérabilités reçus par le ministère de la Défense. Après examen, ce dernier a confirmé l'existence de près de 140 vulnérabilités effectives et jusqu'alors passées inaperçues.
- **3 millions de faux comptes Twitter très actifs.** Spécialisée dans la détection d'anomalies dans les campagnes en ligne et réseaux sociaux, la firme SadBotTrue (on appréciera le jeu de mot) a probablement mis la main sur un botnet de 3 millions de faux comptes Twitter. Qui plus est indétectables. Ces comptes sont identifiables par leur nom qui s'incrémente entre @sfa_2000000000 et @sfa_2002999999 (à l'exception de 13 comptes). Le premier d'entre eux indique 3 millions de *followers*, ce qui le placerait parmi les principaux twittos du site de micro blogging. Pas mal pour un compte indétectable qui n'affiche aucune description de son profil. Bref, si le doute sur l'absence de personnalité humaine derrière chacun de ces comptes qui ont tous été créés le 17 avril 2014 ne fait aucun doute, il reste à savoir à quoi ils servent au-delà d'avoir envoyé 2,6 milliards de tweets en un peu plus de 2 ans□? La question reste entière alors que SadBotTrue a constaté que ces 3 millions de faux twitteurs faisaient partie d'un lot de 168 millions d'identifiants numériques réservés le 22 octobre 2013. Celui qui a réservé ces millions d'ID *« ne devait pas seulement être juste « admin » mais « super admin » »*. Un droit dévolu au seul directeur technique ou à la DSI de la plate-forme, selon la firme d'investigation. Sauf s'il y a une faille dans le système d'information de Twitter.
- **Cedexis enrichit son Radar d'un outil d'alertes.** Cedexis annonce une nouvelle version de Radar, sa solution de mesure de performance et d'optimisation des liaisons Internet pour sites Web et applications mobiles. Radar s'enrichit notamment «□Resource Timing□»,

un outil d'alertes de performance personnalisables qui offre une granularité approfondie des données. L'idée étant de permettre aux équipes DevOps de *« collecter des mesures sur chaque objet d'une page chargée et corréler la performance de ces objets à celle des serveurs, clouds et CDN, à l'origine de la diffusion »*, explique le fondateur Julien Coulon. Au bout, les développeurs obtiennent une mesure du chargement de la page qu'ils peuvent filtrer par type d'appareil (navigateur, CDN, Cloud, datacenter). Une vision de bout-en-bout permettant de résoudre les problèmes propres au site dès leur prise de connaissance.