

Safaricom lance un programme de stage pour des étudiants

Safaricom, la plus grande entreprise de télécommunications intégrée au Kenya, a annoncé l'ouverture des demandes pour son programme de stages en 2017. Le programme, connu sous le nom de la Safaricom Technology Academy, verra la sélection de 63 étudiants universitaires, avec au moins 40 femmes et quatre personnes handicapées. Les étudiants sélectionnés suivront des cours sur le réseautage IP, le développement d'applications, les compétences interpersonnelles, la préparation à l'emploi et les finances. A cela s'ajoute l'expérience pratique lors du stage. «Notre Académie de technologie reflète notre engagement à renforcer les capacités locales et à doter les Kényans des compétences nécessaires pour s'adapter aux changements rapides de la technologie. Nous avons soigneusement conçu la structure de l'Académie afin de s'assurer que les participants sont bien préparés à affronter le secteur technologique exigeant», a déclaré Thibaud Rerolle, Directeur - Technologie, Safaricom. Le programme de cette année cible particulièrement les personnes handicapées dans les domaines des sciences, de la technologie, de l'ingénierie et des mathématiques. Lancé en 2012, le programme de stages a été suivi par plus de 360 étudiants à ce jour. Il a contribué à combler le fossé entre les sexes au sein du personnel même de l'opérateur mobile qui compte maintenant 164 ingénieurs femmes contre 92 en 2013.

Sony lance Koov un jeu de programmation pour enfants

Sony Global Education, filiale de la société éponyme, a lancé le jeu Koov, un ensemble de pièces lego qui enseignent aux enfants les bases du codage et la construction de robots, selon Nikkei Tech. Ces blocs de lego sont reliés à un ordinateur ou une tablette (via une application) pour être animés comme des robots. Les pièces du jeu Koov contiennent des capteurs et des actionneurs qui se mettent en mouvement selon le codage utilisé par les enfants pour se déplacer et s'allumer. Sony semble vouloir se lancer dans l'apprentissage de la programmation ludique pour enfants, mais ce n'est pas une première puisque la société Hasbro a déjà créé des jouets pour enfants contrôlés par des applications, tandis que Fisher-Price a introduit l'année dernière des jouets «Code-a-Pillar» destinés à des enfants en âge de préscolaire. Les blocs de Koov, lancés en partenariat avec le fabricant de jouets Artec Co, devraient être vendus aux Etats-Unis et en Europe au courant de cette année pour environ 350 \$.

Comcast rachète Icontrol Networks

Comcast a complété son achat de Converge, filiale de la société Icontrol Networks spécialisée dans l'internet des objets (IoT), afin de renforcer son activité Xfinity Home des produits de sécurité et d'automatisation. Le directeur général de Comcast Xfinity Home, Daniel Herscovici, a écrit sur le blog de la société que l'achat de l'unité Converge donne à Comcast un «contrôle total sur notre feuille de recherche et de développement», ce qui permettra à l'entreprise d'investir plus stratégiquement à l'avenir. Il a ajouté qu'avec cette acquisition, Comcast développera un «centre d'excellence IoT» à Austin, Texas. «Ce sera un centre clé où nos ingénieurs et développeurs vont concevoir des innovations pour soutenir nos différentes entreprises IoT», a écrit Herscovici, ajoutant que les ingénieurs à Austin travailleront en étroite collaboration avec des équipes à Philadelphie, Silicon Valley et d'autres endroits. «Nous serons en mesure d'offrir des services de gros à de nouveaux clients, nationaux ou internationaux», a-t-il écrit.

Wikileaks démasque les activités de piratage et de dissémination de virus de la CIA

● Plus d'une agence de renseignement et de coups tordus, la CIA est aussi un nid de hacker et de diffusion de virus informatiques. Près de 9000 documents publiés le 7 mars dernier par Wikileaks le démontrent. L'organisation non-gouvernementale fondée par Julian Assange promet d'autres révélations encore plus fracassantes. C'est, sans doute, la plus importante divulgation de documents secrets après celle d'Edward Snowden sur les activités d'espionnage planétaire menées par la NSA. Affaire à suivre...

Par Abdelkader Zahar

Sous le nom de code «Vault 7», Wikileaks a mis en ligne récemment la «plus importante publication de documents confidentiels sur la CIA». La première partie de cette publication, appelée «Zero Day», contient 8 761 documents et fichiers contenus dans un réseau isolé d'internet et ultra-sécurisé basé au siège de la CIA, dénommé «Center for Cyber Intelligence» (CCI - Centre de Cyber Renseignement) qui permet à l'Agence de renseignement américaine de pirater et d'inoculer toutes sortes de terminaux et d'ordinateurs par des virus et autres cyber-armes. Les documents montrent une activité de hacking (piratage) d'un très large éventail de terminaux mobiles de toutes marques et de tous les systèmes d'exploitation, mais également des téléviseurs intelligents transformés en microphones pour espionner le propriétaire. La CIA a même une méthode pour pirater une version Windows 10 au lieu de l'acheter. La «division piratage» de la CIA, qui comptait plus de 5 000 hackers à fin 2016 (dont des contractants externes), «a produit plus d'un millier de systèmes de piratages, virus, chevaux de Troie, et autres «armes» de logiciels malveillants», indique Wikileaks. La source qui a permis à Wikileaks de disposer de ces informations est interne et affirme avoir travaillé sur des opérations de hacking. Cette source, qui souhaite un débat public aux Etats-Unis, sur les activités «hors mandat» de la CIA, en particulier les activités liées au hacking, met en garde contre la dissémination, aux risques incalculables, des outils de piratage et des virus produits

par la CCI, et qualifiés de véritables «cyber-armes».

Terminaux mobiles, voitures connectées...

Outre l'espionnage des ordinateurs et leur hacking, la CIA a développé de puissants outils pour casser la sécurité des terminaux mobiles, des voitures connectées et des smart TV (télévisions intelligentes). Selon Wikileaks, l'EDG (Engineering Development Group), le groupe de développement de logiciels relevant du CCI, a développé tous les «backdoors» (un outil inséré dans un ordinateur pour donner à un pirate l'accès à un ordinateur), les «exploits» (logiciels malveillants d'exploiter une faille), les chevaux de Troie, virus et tout autre type de malware «utilisés par la CIA dans ses opérations secrètes dans le monde entier». Pour hacker les terminaux mobiles (iPhone et autres smartphones Android et Windows), la CIA dispose d'une unité spéciale appelée «Mobile Devices Branch (MDB)». Pour cette tâche, l'Agence collabore étroitement avec d'autres services de renseignements britanniques, comme le MI5 et le GCHQ (service de renseignements électroniques), mais également des entités américaines comme la NSA et le FBI. Wikileaks révèle, par exemple, que le hacking de la smart TV de Samsung qui permet «d'enregistrer des conversations et de les envoyer via internet à un serveur de la CIA» a été réalisé grâce à une coopération avec le MI5. Avec la NSA, le FBI et le GCHQ, la CIA a développé des outils de hacking pour l'iPhone et l'iPad d'Apple, mais également pour les

terminaux Android de Google, pour exploiter la «vulnérabilité Zero day» dans ces terminaux. Pour les ordinateurs de bureau ou ordinateurs portables, la CIA a également développé des outils informatiques visant à infecter et pirater l'ensemble des systèmes d'exploitation, comme OSX d'Apple, Windows de Microsoft et Linux. Même les routeurs de Cisco n'ont pas échappé aux activités de piratage de la CIA, révèle Wikileaks.

Apple, Microsoft, et Samsung réagissent

Parmi les compagnies high-tech citées dans les documents de la CIA publiés par Wikileaks, la première à réagir est Apple. La firme de Cupertino a annoncé que «plusieurs parmi les vulnérabilités» citées dans les documents «ont été déjà patchées dans la dernière version de l'iOS (10.2.1)», et affirme «continuer à travailler rapidement à résoudre toutes les vulnérabilités identifiées», invitant les usagers de l'iPhone et de l'iPad à installer constamment les nouvelles versions de l'iOS. Google a également réagit en expliquant, comme Apple, que la plupart des vulnérabilités citées dans les révélations de Wikileaks ont été corrigées. «Nous sommes conscients du rapport et nous l'examinons», s'est contenté de déclarer un

porte-parole de Microsoft cité par le site de la BBC. Samsung affirme de son côté que «la protection de la vie privée des consommateurs et la sécurité» de ses appareils est sa «priorité absolue». «Nous sommes au courant du rapport en question et examinons d'urgence la question», a ajouté le constructeur sud-coréen.

L'aveu implicite de la CIA

Au lendemain de la publication de «Zero Day», la première partie de l'opération «Vault 7», la CIA a réagi dans un bref communiqué dans lequel elle s'abstient de tout commentaire sur l'authenticité des documents mis en ligne par Wikileaks. Néanmoins, l'Agence affirme implicitement que les informations livrées à Wikileaks par des informateurs internes, sont authentiques. En effet, tout en mettant en garde contre le «public américain» contre «toute divulgation de Wikileaks» pour «endommager la capacité de la Communauté du renseignement de protéger l'Amérique contre les terroristes et autres adversaires», la déclaration de la CIA considère clairement que «de telles divulgations compromettent non seulement le personnel et les opérations des Etats-Unis, mais aussi équipent nos adversaires d'outils et d'informations pour nous nuire».

A. Z.

La Californie ouvre la voie aux tests de voitures sans conducteurs

La Californie, le plus grand marché automobile des États-Unis, prévoit d'autoriser les essais sur les routes publiques de véhicules autonomes (sans chauffeurs) d'ici la fin de l'année. Le département des véhicules automobiles de l'Etat de Californie cherche à obtenir des commentaires du public sur les règlements proposés pour les essais sans conducteur et l'utilisation publique de véhicules autonomes qui ne seront plus tenus d'avoir des commandes manuelles conventionnelles comme les volants et les pédales. La réglementation actuelle exige que ces véhicules aient des commandes, ainsi qu'un pilote de secours. Le changement proposé offre la possibilité de la vente et de déploiement de véhicules autonomes. L'État a autorisé 27 compagnies à tester des véhicules sans conducteur sur la voie publique, y compris les constructeurs automobiles BMW et Tesla Inc. L'autorisation concerne également des fournisseurs comme Delphi Automotive Plc et Nvidia Corp; des sociétés technologiques telles que Waymo, Alphabet Inc et Baidu Inc, ainsi que des startups de véhicules autonomes tels que Zoox, Drive.ai, AutoX et PlusAI. Les véhicules sans conducteur doivent avoir un opérateur à distance capable de surveiller leur fonctionnement et de communiquer avec tous les passagers. Le public a jusqu'au 25 avril pour donner son avis sur cette réglementation.

CNN Digital lance une unité VR pour des vidéos 360 degrés

CNN Digital a annoncé la semaine dernière le lancement de CNNVR, une nouvelle «unité de journalisme immersif» et une plate-forme de réalité virtuelle qui couvrira les grands événements d'actualité au format 360 degrés. CNN a indiqué que cette nouvelle unité intégrera les équipes autour du globe, y compris New York, Atlanta, Londres, Hong Kong, San Francisco, Dubaï, Johannesburg, Tokyo et Pékin. Dès le début, le contenu de CNNVR sera offert via les applications mobiles iOS et Android, pour les navigateurs sur cnn.com/vr et sur les casques de réalité virtuelle y compris le Samsung GearVR, Oculus Rift et Google Daydream. CNN estime avoir produit plus de 50 reportages en VR/360 au cours de la dernière année.