Djezzy accélère la cadence de recrutement

Après la journée de recrutement pour certains profils des diplômés de l'Ecole supérieure algérienne des affaires (ESSA) du 25 janvier dernier, le département Talent Attraction, en collaboration avec le département Talent Development, a renouvelé l'initiative le 12 mars courant pour des entretiens avec des jeunes diplômés de l'ESSA. Les profils recherchés concernent essentiellement les secteurs de la finance, le commercial et les ressources humaines. Cette journée a permis de distinguer quelques profils intéressants, qui pourront prochainement intégrer l'entreprise et accompagner le programme de la transformation qui doit faire de Djezzy l'opérateur numérique de référence en Algérie. Pour rappel, à l'occasion de l'inauguration d'une nouvelle boutique à Oran, Matthieu Galvani, directeur général de Djezzy, avait annoncé le recrutement de 700 nouveaux postes ainsi que la création des nouveaux métiers du digital. Djezzy a lancé une véritable campagne de recrutement à travers les médias en ciblant plusieurs métiers du numérique dont des «Data Analysts», «Data Mining Scientists», «Social Media Experts», «Smartphone Experts», «Shop Managers», «Customer Coaching Leaders» et «Encoding and Programmers experts».

Des hôpitaux africains adoptent l'intelligence artificielle pour le diagnostic

Sophia Genetics, une société de technologie de la santé, a dévoilé, lors de la réunion annuelle 2017 du Collège américain de génétique médicale et de génomique (ACMG) à Phoenix, la liste des hôpitaux africains qui ont commencé à intégrer Sophia Artificial Intelligence dans leur flux de travail pour analyser les données génomiques pour identifier les mutations causant des maladies dans les profils génomiques des patients et décider des soins les plus efficaces. Selon la société, 260 hôpitaux dans 46 pays africains partagent des connaissances cliniques sur les patients et les populations de patients, ce qui alimente une base de connaissances des résultats biomédicaux pour accélérer les diagnostics et les soins. Pour Jurgi Camblong, P-dg et co-fondateur de Sophia Genetics, la solution Sophia «sera un partenaire clé pour les hôpitaux africains en oncologie». «Le cancer du sein, par exemple, a été décrit comme un «tueur en série» sur le continent car le manque de diagnostics pertinents et de soins personnalisés signifie que 60% des femmes atteintes du cancer du sein en Afrique meurent contre 20% aux États-Unis et en UE.» Le professeur Hicham Mansour, généticien à l'Université Mohamed-1er, département génétique - Centre d'oncologie Al Azhar au Maroc, affirme que «l'utilisation de Sophia nous permet d'analyser rapidement et avec une grande confiance les données génomiques afin de mieux diagnostiquer et suivre nos patients».

Google durcit ses conditions d'utilisation en matière de publicité

En réaction à la polémique déclenchée récemment par la diffusion de publicités accolées à des vidéos au contenu extrémiste, Google affirme avoir engagé un examen «en profondeur» de ses conditions d'utilisation relatives à la publicité. «Nous avons également durci nos conditions d'utilisation en matière de publicité afin de protéger les marques de nos annonceurs», affirme un porte-parole du géant de l'internet. Des grands groupes, allant des supermarchés aux banques en passant par des compagnies de télécoms, comme AT&T et Verizon, ont retiré récemment leurs publicités de YouTube, après avoir constaté qu'elles apparaissaient aux côtés de contenus extrémistes. Le nombre d'entreprises qui boycottent les réseaux publicitaires de Google a atteint environ 250 entreprises. Les entreprises ont rejoint le boycott qui a commencé au Royaume-Uni avec des organisations telles que la BBC, *The Guardian* et le gouvernement britannique. Google a promis de mieux contrôler ses sites web en renforçant ses effectifs et en amendant ses conditions d'utilisation. Les analystes pensent toutefois que les éditeurs de médias traditionnels tels que les journaux et les radios pourraient tirer profit de cette nouvelle polémique en mettant en avant leurs services comme étant fiables et plus sécurisés. En une semaine, Google a perdu plusieurs millions de dollars après le retrait des publicités des principaux grands annonceurs.

WIKILEAKS

«Dark Matter», ou comment la CIA a infecté des firmwares d'Apple

● Dans sa deuxième livraison des révélations «Vault 7» sur les activités de piratage informatique de la CIA, Wikileaks a publié, le 23 mars, «Dark Matter» révélant une douzaine de nouveaux documents sur des projets de l'agence centrale de renseignement américaine d'infecter des firmwares des MacBook et de l'iPhone d'Apple.

Par Abdelkader Zahar

Les activités de piratage informatique de la CIA dépassent de loin le développement et la dissémination de logiciels malveillants pour espionner des ordinateurs et des terminaux mobiles de toutes plateformes. Selon les dernières révélations de l'organisation Wikileaks, la CIA a mené des projets d'infection des firmwares (logiciels internes) des ordinateurs portables MacBook et de l'iPhone d'Apple. Un communiqué de Wikileaks explique que l'infection du firmware, «développée par la Direction du développement intégré (Embedded Development Branch - EDB)» de la CIA, signifie que «l'infection persiste même si le système d'exploitation est réinstallé». Les douze documents, publiés par l'organisation de Julian Assange, expliquent les «techniques utilisées par la CIA» pour avoir accès à des périphériques d'Apple, et démontrent «l'utilisation de logiciels EFI/UEFI (Unified Extensible Firmware Interface) et de microprogrammes (firmwares) malveillants». Le document appelé projet «Sonic Screwdriver» (2012) est un «mécanisme permettant d'exécuter du code sur des périphériques pendant qu'un ordinateur portable Mac ou un ordinateur de bureau démarre» même lorsque un mot de passe est exigé par le firmware d'Apple, explique la CIA dans ce document. «Normalement, un mot de passe du firmware d'Apple empêche les modifications du chemin d'amorçage. Le mécanisme «SonicScrewdriver» pour exécuter le code permettra à un utilisateur de démarrer via une clé USB, un DVD/CD ou un disque dur externe, même si un mot de passe du microprogramme est activé», ajoute le «Guide d'utilisateur» élaboré en 2012 par la CIA. Dans ce «guide», l'agence explique le code de «SonicScrewdriver» «est stocké sur le firmware d'un adaptateur Thunderbolt-to-Ethernet» d'Apple. «Le code de l'implant va scanner tous les périphériques internes et externes avec un nom de volume spécifique. Cela comprend les clés USB, les CD/DVD et les disques durs. Si le nom de volume spécifique est trouvé, il exécutera un démarrage UEFI de ce périphérique», ajoute le document de la centrale de renseignement américaine. Selon Wikileaks, «DarkSeaSkies» (2009) est un implant qui persiste dans le firmware EFI d'un ordinateur MacBook Air, et se compose des implants «DarkMatter», «SeaPea» et «NightSkies», respectivement EFI, kernel-space et user-space».

La Supply Chain de l'iPhone court-circuitée ?

Le «Guide d'utilisateur» élaboré par la CIA pour le programme «SonicScrewdriver» note que tous les ordinateurs Apple disposant d'un port Thunderbolt (une technologie pour connecter des périphériques développée par Intel en collaboration avec Apple), sont des «ordinateurs cibles». Il est également précisé que l'infection du firmware a été testée sur des «MacBook Air (11 et 13 pouces) construits entre 2011 et 2012», des MacBook Pro Retina éditions 2012 (13 et 15 pouces), et des MacBook Pro (13 et 15 pouces) produits en 2011. Le document donne tous les détails et les étapes de la procédure d'infection des firmwares de ces ordinateurs d'Apple. Quant au guide d'utilisation sur les logiciels malveillants «Triton» pour Mac OS X, son infuseur «Dark Mallet» et sa version persistante EFI «DerStarke», la CIA affirme cibler les versions 10.7 (Lion) et 10.8 (Mountain Lion) du système d'exploitation d'Apple. Si le document DerStarke1.4 a été publié en 2013, «d'autres documents Vault 7 montrent que jusqu'en 2016, la CIA continuait de s'appuyer sur ces systèmes et de les mettre à jour et travaille à la production de DerStarke2.0», rappelle Wikileaks. Quant à «NightSkies 1.2» de la CIA (élaboré en 2008), il s'agit d'un «outil de balise/chargeur/implantation pour l'iPhone 3G v2.1 d'Apple», explique le document de la CIA. «L'outil fonctionne en arrière-plan fournissant des capacités de téléchargement, d'upload et d'exécution sur le périphérique. Il est installé via un accès physique à l'appareil et attendra l'activité de l'utilisateur avant le balisage. Lorsque l'activité de l'utilisateur est détectée, il tentera d'interroger un LP (Listening Post – Poste d'écoute) préconfiguré pour récupérer les tâches, exécuter les instructions et réagir avec les réponses en une seule session», explique encore le document de la CIA. Le communiqué de Wikileaks, révélant les documents relatifs aux actions de la CIA pour espionner et infecter les produits d'Apple, note que le projet «NightSkies» lancé en 2008 «est expressément conçu pour être physiquement installé sur les iPhones sortis d'usine. C'est-à-dire que la CIA a infecté la chaîne d'approvisionnement de l'iPhone depuis au moins 2008». Réagissant à la publication des récents documents par Wikileaks, Apple affirme, via le site Tech Crunch, avoir résolu les vulnérabilités «depuis plusieurs années». La firme de Cupertino précise que les vulnérabilités de l'iPhone «n'ont affecté que l'iPhone 3G et ont été corrigées en 2009 lorsque l'iPhone 3GS a été publié». Quant aux vulnérabilités des ordinateurs Mac, elles ont été «corrigées dans tous les Mac lancés après 2013», affirme encore Apple.

A. Z.

Amazon va racheter le site Souq.com, basé à Dubaï

Amazon.com veut racheter le site Souq.com. Selon Reuters, citant des «sources proches du dossier», un «accord de principe» a été conclu entre le géant américain du commerce électronique et les actionnaires du site basé à Dubaï pour «racheter la totalité» de Souq.com qui vend une large gamme de produits électroniques, articles de mode et ménagers. Citant des «informations de presse», Reuters affirme que «la dernière levée de fonds, intervenue l'an dernier, a valorisé le site à un milliard de dollars (924 millions d'euros)», faisant état également d'une baisse de la «valorisation» du site depuis cette date. La même source indique que «cet accord permettra à Amazon d'être présent dans la région sans avoir à obtenir notamment l'autorisation des régulateurs de chaque pays, tout en disposant d'un réseau de vendeurs et de fournisseurs, a ajouté une des sources».