Télégrammes : Amazon renforce Alexa ; Ethereum braqué ; Force brute contre Office365, Fusion Broadcom-Brocade compromise

Amazon rachète Graphiq pour renforcer Alexa. Selon le *Los Angeles Times*, Amazon.com a racheté en mai dernier une start-up spécialisée dans l'analyse de données et les moteurs de recherche : Graphiq. Cette société comptant plus de 100 personnes, et installée à Santa Barbara, a été fondée en 2009 sous un premier nom (FindTheBest). Elle entendait alors collecter et organiser des données pour faciliter l'accès à l'information sur les produits, les lieux ou les individus. Ce rachat vise à renforcer Alexa, la technologie d'IA d'Amazon, selon le *Los Angeles Times*, qui analyse notamment les dernières annonces de recrutement de Graphiq pour parvenir à cette conclusion. Le quotidien californien estime que ce rachat, que les deux entreprises ont refusé de commenter, a coûté plusieurs dizaines de millions de dollars au géant du e-commerce.

Braquage contre Ethereum : un butin de 30 M€. Trois projets sur la Blockchain, Edgeless, Swarm City et æternity, viennent d'être victimes d'un hold-up massif, l'équivalent de 30 millions d'euros ayant été dérobés dans ces trois porte-feuilles. Le point commun de ces trois projets ? Ils s'étaient lancés dans une ICO (levée de fonds en cryptomonnaies)… et se sont fait voler tout ou partie des sommes récoltées dans ce cadre. Soit au total 153 000 ethers qui se sont volatilisés. Le braquage a été rendu possible par un bug dans le client Ethereum de Parity Technologies. Cette entreprise établie à Londres a réagi mercredi dernier, évoquant une « faille critique » dans son logiciel, à partir de la version 1.5, dite « Nativity ». Cette dernière, sortie en début d'année, avait notamment introduit la prise en charge des portefeuilles dits « multisignatures » ; en d'autres termes, exigeant des approbations multiples indépendantes pour valider des transactions. C'est l'implémentation de cette fonction qui pose problème, plusieurs fonctions d'initialisation de portefeuille n'étant pas suffisamment protégées. Parity affirme avoir désormais éliminé la faille. En l'état, sur les 596 portefeuilles vulnérables recensés par ses soins, seuls trois paraissent avoir été touchés : ceux d'Edgeless, Swarm City et æternity.

L'acquisition de Brocade par Broadcom en danger. Le rachat de Brocade par Broadcom, annoncé en novembre 2016 pour 5,9 milliards de dollars, pourrait être remise en cause. Alors que l'opération a reçu le feu vert des autorités US, Brocade a fait savoir à la SEC, le gendarme américain de la bourse, qu'un dossier de réexamen du rapprochement avait été déposé suite aux discussions menées avec le CFIUS (le comité américain sur les investissements étrangers). Le CFIUS est chargé de vérifier les risques de basculement du contrôle d'une entreprise américaine vers l'étranger. Si Brocade est côté au Nasdaq, la société possède également un siège à Singapour. Un délais de 30 jours est à prévoir et pourrait être prolongé de 45 jours supplémentaires. Dans un communiqué commun, Broadcom et Brocade indiquent qu'il *« n'y a aucune garantie que le CFIUS accepte que les parties mènent l'acquisition en cours à son terme »*. La fusion doit être finalisée avant le 1er novembre prochain. Si ce n'est pas le cas, Broadcom pourrait y mettre un terme définitif.

La force brute pour casser Office365 ? Selon le spécialiste de la gestion des accès dans le Cloud Skyhigh Networks, un assaillant non identifié s'est lancé, depuis le début 2017, dans une campagne d'accès frauduleux au service Office365 de Microsoft. L'opération cible des entreprises et vise à tenter de prendre possession des accès d'employés de haut niveau, pour récupérer des informations sensibles. Skyhigh affirme avoir identifié plus de 100 000 tentatives (échecs d'authentification), émanant de 67 IP et dirigées contre 48 organisations utilisant le service Saas. La société explique, dans un billet de blog, qu'il s'agit là d'une attaque assez sophistiquée, les assaillants ciblant seulement certains profils, conservant un rythme de tentatives suffisamment discret pour ne pas générer d'alerte sur le service de Microsoft et lançant leurs attaques depuis d'autres services Cloud publics. Classiquement, les assaillants misent sur la réutilisation des mots de passe sur divers services pour forcer le verrou de l'authentification (à partir de listes de login / mots de passe récupérées ou achetées sur le Darknet) et essayent différentes constructions pour 'deviner' l'adresse mail de chaque cible. Skyhigh indique toutefois n'avoir à ce jour aucune preuve d'une compromission de compte ou d'un éventuel vol de données.