Télégrammes : Arrestation dans l'affaire Sage, Locky reprend le chemin de l'hôpital, Nokia et BT ensemble sur la 5G, Wikileaks truffé de malwares

- **Fuite chez Sage : un employé arrêté à Heathrow.** Nos confrères de *TechweekEurope* révèlent qu'une employée de Sage, âgée de 32 ans, a été arrêtée le 17 août à l'aéroport d'Heathrow (Londres). Quelques jours plus tôt, l'éditeur britannique avait reconnu un « accès non autorisé » à des données confidentielles de 280 entreprises britanniques clientes de ses solutions. On suppose qu'y figuraient notamment des informations bancaires sur les salariés de ces organisations ainsi que leur niveau de rémunération. L'accès non autorisé à ces informations aurait été effectué par quelqu'un utilisant un login interne.
- **Le ransomware Locky reprend sa tournée des hôpitaux.** Une alerte de FireEye avertit les utilisateurs d'une recrudescence du ransomware Locky, qui a fait de nombreuses victimes en France au printemps dernier. L'éditeur américain relève que de nouvelles campagnes de diffusion du ransomware sont apparues, exploitant des macros logées dans des fichiers de Microsoft Office envoyés en pièces jointes. Les pirates ciblent avant tout le secteur de la santé. Rappelons que Locky s'était déjà fait connaître via l'infection de plusieurs hôpitaux américains, dont celle très médiatisée du Hollywood Presbyterian Medical Center. Un établissement qui a versé 17 000 dollars aux pirates pour se débarrasser du malware. Les Etats-Unis, la Corée du Sud et le Japon sont les pays les plus touchés par cette nouvelle vague ; la France semblant pour l'heure relativement épargnée. « Ces dernières campagnes constituent un rappel pour les utilisateurs, qui doivent se montrer prudents quand ils ouvrent des pièces jointes à des e-mails car ils prennent alors le risque d'être infectés et même de perturber les opérations de leur entreprise », écrit FireEye.
- **Nokia et BT font route vers la 5G.** L'opérateur britannique BT et l'équipementier télécom Nokia ont signé un accord de co-développement commun dans la 5G. L'objet du partenariat vise à créer des prototypes (proof of concept) de solutions technologiques 5G applicables sur un réseau commercial (rappelons que BT, opérateur fixe par essence, exploite le réseau mobile d'EE après son rachat auprès d'Orange et Deutsche Telekom en 2014). Les deux partenaires vont travailler sur les technologies d'ondes millimétriques (autour des 30 GHz), la convergence fixe-mobile ainsi que des services commerciaux comme l'ultra haut débit, les services critiques et l'Internet des objets (IoT). Cet accord s'inscrit dans le prolongement de la collaboration des deux entreprises sur la mise au point d'équipement 5G radio au laboratoire de BT à Adstral Park (Suffolk). Un système radio qui s'appuie sur l'offre AirScale de Nokia, présentée en février dernier à Barcelone.
- **Wikileaks truffé de malwares.** Selon le chercheur en sécurité Vesselin Bontchev, qui a notamment créé le National Laboratory of Computer Virology en Bulgarie, pas moins de

234 instances de malwares se promèneraient parmi les e-mails mis en cache sur Wikileaks, la plate-forme de l'organisation créée par Julian Assange et ouverte aux lanceurs d'alertes. Lesquels ne sont visiblement pas les seuls à se servir de ce site qui entend dénoncer scandales politiques, corruptions et autres violations des droits de l'Homme. Les cybercriminels y déposent aussi des e-mails infectieux en espérant probablement profiter de la notoriété du site pour propager leurs malwares. Et encore ne s'agit-il là que d'une analyse partielle. *« La liste est loin d'être exhaustive ; je commence tout juste l'analyse »*, prévient le chercheur qui a publié de premiers résultats. Un chercheur qui affirme n'avoir *« aucun doute »* sur la présence effective de malwares sur la plate-forme. A moins d'être assez stupide ou étourdi pour ouvrir la pièce jointe de ces courriels, un utilisateur de Wikileaks a toutefois peu de chance d'être infecté. Mais la présence des virus tend à démontrer que Wikileaks ne dispose pas de filtre contre les e-mails malveillants alors que les souches virales mises en évidence par Vesselin Bontchev sont largement détectées par VirusTotal, le service d'analyse des fichiers et URL suspects.