LANCEURS D'ALERTE

# WikiLeaks fête ses dix ans

**WikiLeaks a bouclé ses dix années d'existence. La plateforme non-gouvernementale qui publie des documents secrets, impliquant des Etats, des politiques et des grandes entreprises, est au cœur du débat sur la nécessité de défendre la neutralité de l'internet et sa transparence.**

Par Farid Farah

Julian Assange, le fondateur de la plateforme de publication en ligne WikiLeaks, est âgé de 45 ans. Malgré ses quatre années passées dans une chambre de l'ambassade équatorienne à Londres, loin des bienfaits du soleil, ce hacker activiste a saisi l'occasion du 10e anniversaire de la création de WikiLeaks pour s'adresser via une visioconférence à des dizaines de journalistes et photographes. Il n'a pas perdu son temps pour renouveler son combat pour les libertés numériques et tenter de convaincre l'opinion mondiale de l'utilité de l'internet dans la mise en place d'un système politique transparent. Internet est-il un danger pour la démocratie ou, au contraire, un espace numérique à travers lequel la transparence politique se renforce dans les processus électoraux ? L'homme qui a plongé les Etats-Unis dans une paranoïa IT, au lendemain de la mise en ligne des secrets de l'armée américaine, est en train de jouer un rôle très actif dans l'élection présidentielle américaine. Pour bien marquer le dixième anniversaire de son site, il a publié plus de 19 000 emails montrant que le Parti démocrate avait secrètement saboté la campagne électorale du sénateur Bernie Sanders pour faire gagner Hillary Clinton aux primaires. Suite à cette révélation, le président du parti Debbie Wasserman Schultz a démissionné de ses fonctions.

Historiquement, c'est sur l'idée d'entreprise journalistique qu'Assange a fondé WikiLeaks au début de l'année 2007. Il lui a choisi la personne de Daniel Ellsberg comme mascotte. Cet ancien analyste militaire qui a divulgué à l'opinion une collection de documents secrets sur la guerre des Etats-Unis au Viêtnam est connu par sa célèbre citation : «Nous étions jeunes, nous étions insensés, nous étions arrogants, mais nous avons eu raison.» C'est pourquoi, le site d'Assange s'ouvre avec une page blanche sur laquelle cette citation s'affiche. En 2008, WikiLeaks avait publié un manuel qui avait été distribué aux soldats américains à Gitmo (Camp de Guantánamo), des documents sur les pratiques religieuses de l'Eglise de scientologie et les emails privés de l'ancien gouverneur de l'Alaska, Sarah Palin. En 2010, Assange a mis en ligne deux vidéos et des centaines de milliers de documents confidentiels concernant la politique étrangère des Etats-Unis, la première puissance mondiale et surtout le pays «locomotive» du «train» de la vie numérique ! L'exploitation professionnelle des données «diplomatiques» exfiltrées ou volées a été confiée, pour des raisons d'éthique, à 150 journalistes de cinq journaux : *Le Monde*, *The New York Times*, *The Guardian*, *El Pais et Der Spiegel*. Une coopération inédite.

Photos : DR

### Panique au cœur du système

Face à cet acte de piratage le plus célèbre de la planète, la réaction du ministère de la Défense US ne s'est pas fait attendre. Le US Department of Defense a publié des recommandations, totalement similaires à celles qu'une banque destine à ses analystes et administrateurs réseaux. Ces derniers doivent veiller à désactiver la fonction «écriture» sur les supports amovibles (clés USB, disques durs externes) sur les machines classifiées, et limiter le nombre de systèmes autorisés à déplacer les données de systèmes classifiés vers des systèmes non classifiés. Aussi, désormais, deux personnes seront nécessaires pour déplacer des données de systèmes classifiés vers des systèmes non classifiés. Des groupes travaillant sur les menaces internes seront également créés pour réagir à l'incident WikiLeaks et empêcher qu'il ne se reproduise. Sur un autre volet, les douanes américaines ont désactivé plus de 80 sites Web suspectés d'activités illégales. La procédure est simple, l'ICE (US Immigration and Customs Enforcement) a sollicité cette désactivation auprès de la société Verisign, en charge de la gestion du domaine «.com» en collaboration avec le régulateur mondial de l'internet ICANN. Ce dernier a dépourvu WikiLeaks de son domaine «.org» l'obligeant à passer en «Wikileaks.ch». Le fournisseur de DNS de WikiLeaks, EveryDNS, a aussi désactivé les ponts avec le site, responsable selon lui de mettre en danger son infrastructure à cause du nombre important d'attaques de pirates par déni de service (DDOS) dont WikiLeaks était la cible.

Dans la série des actions en réaction aux révélations du site, le 1er décembre 2010, Amazon a retiré WikiLeaks de ses serveurs d'hébergement. Le lendemain, c'était au tour des organismes d'Etat comme la bibliothèque du Congrès, le département du Commerce ou l'armée américaine qui ont bloqué sur leurs réseaux l'accès au site de WikiLeaks. Mieux, des représentants de l'Etat américain ont demandé aux universités d'interdire à leurs étudiants l'utilisation des documents rendus publics par WikiLeaks dans leurs travaux de recherche. Selon l'ancien hacker et informaticien australien, des sénateurs américains l'ont qualifié de «terroriste technologique» et ont appelé à son élimination physique par l'intermédiaire d'un drone. Une équipe de 120 personnes appartenant au FBI, à la CIA et au Département d'Etat américain, a en effet été constituée sous le nom de WikiLeaks Task Force, ou WTF, pour mener des actions contre Wikileaks et son créateur.

**F. F.**

TAGS WikiLeaks, Julian Assange, FBI, CIA, Etats-Unis, Clinton, Internet, Amazon, ICANN

«NOKIA SECURITY CENTER»

# Les infections mobiles sont de plus en plus sophistiquées

**Le rapport «Nokia Threat Intelligence» pour le premier semestre 2016 est un appel à la vigilance. Les infections de smartphones s'accélèrent et deviennent de plus en plus sophistiquées.**

Par Abdelkader Zahar

La technologie a son revers de la médaille. Maintenant qu'on emporte avec soi sa connexion, grâce à la 3G et la 4G, on emmène aussi les dangers de l'internet. La révolution créée par les terminaux mobiles et la hausse des usages et de la consommation data s'est accompagnée par une hausse des menaces. Le rapport «Nokia Threat Intelligence» (NTI) pour le 1er semestre 2016 (NTI–H1 2016), réalisé par Nokia Security Center, avertit sur la multiplication des menaces d'infections des terminaux mobiles et met en exergue la sophistication des attaques. Rendu public récemment, le rapport «NTI-H1 2016» commente les statistiques des infections par des logiciels malveillants (malwares).

Les données ont été regroupées depuis les réseaux où la solution «Nokia NetGuard Endpoint Security» a été déployée. Ils attestent de l'importance grandissante des infections des smartphones dont le taux a atteint 0,49% au 1er semestre 2016. Ce taux, qui peut paraître infime, représente une «hausse de 96% par rapport à 0,25% enregistré à la même période de 2015». En avril 2016, 0,82% des smartphones présentaient une certaine forme de logiciels malveillants. «Cela représente 78% du total des infections observées pour ce mois», soit «1 smartphone sur 120 observés a été infecté par un malware au cours du mois d'avril 2016», affirme le rapport. Les infections de smartphones représentent 78% des infections détectées dans les réseaux mobiles. Parmi les infections enregistrées par Nokia en 2016, «74% étaient des appareils Android, 22% Windows/PC et 4% iPhone et autres», précise l'étude à ce sujet. Les échantillons de logiciels malveillants Android poursuivent leur croissance en 2016, explique l'étude. «Un indicateur de la croissance des malwares Android est l'augmentation du nombre d'échantillons dans notre base de données de logiciels malveillants (…) qui a augmenté de 75% au premier semestre 2016», note le document. L'étude constate que le nombre de malwares est passé d'environ 4 millions à fin 2015 à près de 9 millions en juillet 2016. Sur une liste de «Top 20 logiciels malveillants» pour smartphones détectés dans la première moitié de l'année 2016 dans les réseaux où les solutions Nokia NetGuard Endpoint Security sont déployées, «10 sont nouveaux», «19 ont ciblé des terminaux Android de Google» et «un seul concerne l'environnement iOS d'Apple». En terme de degré de risque, «18 des 20 malwares sont une «menace de haut niveau», et deux «modérés».

### Hausse des échantillons de malware Android

Les plus virulents de ces malwares touchant Android sont «UaPush», «Kasandra» et «Smstracker». «Dans la première moitié de 2016, nous avons remarqué une augmentation significative de leur activité, qui est responsable du saut d'infections enregistré en avril». L'activité du malware «XcodeGhost» touchant l'iPhone a diminué en 2016, «mais il est encore dans le Top 10». Les logiciels malveillants mobiles «sont certainement de plus en plus sophistiqués, en particulier dans l'espace Android», affirme le rapport de Nokia. De nombreux exemples ont été rencontrés où le malware est enraciné dans le dispositif afin de se rendre difficile à détecter et à désinstaller.


Les trois principales menaces mobiles Android observées dans Netguard Endpoint Security sont de classe «Spyware» (logiciel espion), «Cybercrime» et «Identity Theft» (voleur d'identité). «Uapush.A» est un adware Trojan (cheval de Troie) Android avec un niveau de «menace modérée». Il envoie des SMS et vole des informations personnelles à partir du smartphone compromis. «Ce malware a son site web C&C (command and control) situé en Chine». «Kasandra.B» est un trojan Android de niveau de menace élevée. Il est conditionné de façon à «ressembler à une application mobile de sécurité de Kaspersky».

Il donne à l'attaquant un accès illimité aux informations sensibles telles que les SMS, la liste de contacts, les journaux d'appels, l'historique du navigateur, et les données de localisation GPS. Il stocke ces données dans un fichier pour les télécharger via une commande C&C située sur un serveur basé aux USA. «Smstracker» est une application Android Spyphone qui permet à l'attaquant de suivre à distance et surveiller tous les SMS, MMS, appels vocaux, emplacements GPS et l'historique du navigateur. Le serveur C&C de ce malware est basé aux USA. La sophistication des malwares Android atteint des niveaux jamais vus, explique le rapport de Nokia. Parmi les nouveautés des attaques, c'est la tentative de prise de contrôle total du smartphone et d'établir une «présence permanente sur le dispositif». Dans cette catégorie, le rapport cite «Viking Horde» une famille de malwares qui tire son nom du jeu Viking Jump et qui a également infecté d'autres applications mobiles Android comme Wifi Plus, Memory Booster, et Parrot Copter. Enfin, ceux qui ont téléchargé le jeu «Pokémon GO» en dehors de la plateforme Google Play peuvent aussi considérer qu'ils ont été infectés par un puissant trojan répondant au nom de «DroidJack». Le malware s'identifie comme étant «Pokémon GO» et demande dès le premier lancement toutes les permissions d'accès à vos données, y compris prendre des photos et des vidéos, envoyer des messages et enregistrer de l'audio.

**A. Z.**

TAGS Malware, Trojan, Android, iOS, Infections, Pokémon GO, Nokia Threat Intelligence, Smartphone, Mobile