Un autre programme secret de la NSA cible les réseaux GSM mondiaux

	Un autre programme secret de la NSA cible les réseaux GSM mondiaux

Des documents livrés par Edward Snowden évoquent un programme d'espionnage secret de la NSA. Appelé Auroragold, il cible les membres du GSMA pour recueillir des informations confidentielles sur les failles et les systèmes de cryptage, exploitées ensuite pour s'infiltrer dans les réseaux mobiles.

Selon des informations contenues dans des documents livrés par l'ex-consultant Edward Snowden, la NSA a lancé une campagne secrète pour intercepter les communications internes d'opérateurs et d'acteurs du secteur de la téléphonie mobile dans le but d'infiltrer leurs réseaux partout dans le monde. Dans un article publié samedi par le site The Intercept, qui a également mis en ligne les documents concernés, l'Agence nationale de sécurité américaine a mené, dans le cadre d'un programme appelé Auroragold, des opérations encore jamais rendues publiques.
Deux unités – Wireless Portfolio Management Office et Target Technology Trends Center – mises sur pied par la NSA, ont été chargées de surveiller de près les membres de la GSM Association, espionnant plus de 1200 adresses emails. L'objectif était d'intercepter dans les entreprises visées des messages internes et de recueillir des informations sur les failles de sécurité des réseaux et le cryptage des communications.
Les derniers documents indiquent qu'en mai 2012, sur les 985 réseaux de téléphonie mobile mondiaux, la NSA avait récolté des informations techniques sur 70 % d'entre eux. Mis à part les pays de quelques opérateurs ciblés – Libye, Chine et Iran – le document fourni par l'ancien consultant de l'agence américaine, toujours réfugié en Russie, ne contient aucun nom d'entreprises. Ces opérations d'espionnage ont permis à la NSA de récupérer des documents IR.21 utilisés par les membres de la GSMA pour signaler des failles de sécurité dans leurs réseaux. Les IR21 contiennent également des détails sur les solutions de cryptage utilisées par les opérateurs mobiles. D'après les documents d'Edward Snowden, la NSA, qui n'a pas répondu à une demande de commentaire, s'est servie de ces informations pour contourner le cryptage des communications.

Espionnage tous azimuts
Depuis juin 2013, de nombreux rapports et articles basés sur les documents fournis par Edward Snowden montrent l'étendu des opérations d'espionnage menées par la NSA sur Internet et les réseaux télécoms à travers le monde. Ils ont aussi permis de savoir que la NSA avait piraté les courriels de dirigeants de pays alliés des États-Unis et de découvrir qu'elle avait infiltré les réseaux et les systèmes d'entreprises étrangères, comme c'est le cas du constructeur chinois Huawei. L'an dernier, divers articles parus dans ProPublica, The Guardian et The New York Times, ont révélé que, pendant plusieurs années, la NSA s'était employée à affaiblir les normes de sécurité pour faciliter les opérations d'espionnage à grande échelle du gouvernement américain. Par exemple, des articles publiés en septembre 2013 par le Guardian et le NYT indiquent, sur la base des documents de Snowden, que la NSA a créé sa propre version du standard Dual_EC_DRBG (Dual Elliptic Curve Deterministic Random Bit Generator), un générateur de nombres aléatoires utilisé en cryptographie. Cette norme, approuvée pour un usage mondial en 2006, contiendrait une porte dérobée permettant à la NSA de s'introduire dans les systèmes de communications. Dès 2007, certains spécialistes et l'éditeur lui-même, RSA Security, recommandaient de désactiver par défaut le Dual_EC_DRBG. Des documents divulgués par Edward Snowden l'an dernier ont également apporté la preuve que la NSA pouvait espionner le trafic GSM chiffré avec l'algorithme A5/1.

Fin novembre, Symantec et Kaspersky Labs ont révélé l'existence d'un malware baptisé Regin, probablement développé par les États-Unis. Actif depuis au moins six ans, Regin cible les réseaux cellulaires GSM pour espionner les gouvernements, les infrastructures des opérateurs de téléphonie mobile, des instituts de recherche, des entreprises et des particuliers. En plus de ces opérations secrètes, la NSA espionne collectivement les conversations téléphoniques des citoyens américains. Le mois dernier, le directeur de la NSA, Michael Rogers a déclaré que l'agence ne prévoyait pas de réviser son programme de collecte : un projet de loi déposé devant le Sénat pour encadrer cette collecte n'a pas abouti.
Glenn Greenwald et Laura Poitras, les deux éditeurs et fondateurs du site The Intercept, ont déjà aidé Edward Snowden à diffuser ses documents par le biais de différents médias.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.lemondeinformatique.fr/actualites/lire-un-autre-programme-secret-de-la-nsa-cible-les-reseaux-gsm-mondiaux-59530.html
Par Jean Elyan / IDG News Service