Auroragold : la NSA surveille les trois quarts des réseaux mobiles de la planète

La NSA surveille les réseaux mobiles du monde entier depuis 2010 au moins. Ce sont les dernières révélations apportées par *The Intercept*, le média créé par le journaliste Glenn Greenwald qui avait révélé le programme Prism de surveillance mondiale d'Internet sur la base des documents fournis par le lanceur d'alerte Edward Snowden à l'été 2013. **La NSA a espionné des centaines d'opérateurs et organisations internationales**, y compris issues de pays alliés, pour exploiter les failles de leurs réseaux cellulaires à des fins de surveillance.

Exploiter les failles des réseaux

Baptisée **Auroragold**, cette opération visait à exploiter les vulnérabilités, voire en créer, des systèmes de communication pour mieux s'y introduire et contourner les politiques de sécurité… au risque d'**ouvrir également les réseaux aux pirates**. Si le *Washington Post* avait révélé que la NSA pouvait déchiffrer les communications mobiles encodées sous l'algorithme de cryptage A5/1, les techniques développées pour l'opération Auroragold sont visiblement à jour pour lire les données chiffrées sous A5/3, une version plus récente de l'algorithme d'encodage.

Plus de **1200 comptes emails** associés à l'activité de grands opérateurs mobiles et d'organisations de travail ont ainsi été espionnés depuis 2011, date de mise en œuvre de l'opération secrète de la National Security Agency. La GSMA, l'association regroupant les industriels du secteur des télécom, a ainsi été une cible de choix. Outre les équipementiers et opérateurs, on y retrouve des acteurs américains comme Cisco, Microsoft, Intel ou Facebook.

Plus de 700 réseaux infiltrés

Selon l'expert en sécurité de téléphonie mobile Karsten Nohl interrogé par *The Intercept*, tous les réseaux mobiles de la planète sont potentiellement accessibles aux oreilles expertes de la NSA. Selon les documents exfiltrés par Edward Snowden, la NSA a collecté des informations sur 701 réseaux cellulaires, soit quelque 70% des 985 infrastructures mobiles d'opérateurs estimées dans le monde. Pour le seul mois de mai 2012. **En France, 47% des réseaux nationaux étaient ainsi «couverts»**, selon un document datant de juin 2012.

Auroragold a été menée par deux unités de l'Agence : la Wireless Portfolio Management Office, chargée de définir la stratégie des surveillances des communications sans fil; et le Target Technology Trends Center, qui assure la veille sur les développements technologiques de l'industrie.

La NSA en contradiction avec le Nist

Par la voix de sa porte-parole Vanee Vines, la NSA rétorque que la loi américaine légalise ses

pratiques à des fins de sécurité du pays quels que soient les moyens employés. Le discours habituel, donc, mais contradictoire avec la politique du Nist (National Institute for Standards and Technology) qui, en septembre dernier, a dégagé un budget de 3 millions de dollars pour **soutenir des projets visant à renforcer la protection de la vie privée**, de la sécurité et la facilité de leurs usages. La GSMA figurait parmi les trois organismes bénéficiaires de la subvention (avec Confyrm et Morpho Trust USA) et à reçu à ce titre plus de 820□000 dollars. Les révélations du jour ne vont certainement pas apaiser les tensions vives entre le Nist et la NSA.

Par ailleurs, en décembre 2013, un groupe de travail réuni par Barack Obama autour des questions des technologies de l'information, suggérait qu'**en aucun cas, la NSA ne devrait *« subvertir, nuire, affaiblir ou rendre vulnérables des logiciels commerciaux généralement disponibles »*** et que l'Agence devrait prévenir les organismes concernés quand elle trouve des failles zero day, sauf dans les cas exceptionnels de *« collecte de renseignements hautement prioritaires »*. La surveillance des réseaux mobiles de la planète fait-elle partie de cette haute priorité□? La porte-parole de la NSA n'a, dans tous les cas, pas indiqué si l'opération Auroragold était toujours en service aujourd'hui.

Lire également

[La NSA injecte des backdoors dans les matériels IT à l'export]
[L'espionnage de la NSA pourrait « casser Internet » selon les géants du Web]
[L'espionnage de la NSA coûte plus cher que prévu à l'industrie US]