La cartographie du Net de la NSA pirate les réseaux d'opérateurs allemands

Selon une nouvelle enquête du *Spiegel* basée sur des documents dérobés par Edward Snowden, l'Agence de sécurité nationale américaine (**NSA**) et son équivalent britannique, le **GCHQ** (Government Communications Headquarters), auraient obtenu, avec la complicité des services secrets locaux, **un accès clandestin aux réseaux et routeurs d'opérateurs allemands**, mais aussi aux terminaux de leurs abonnés.

« Treasure Maps », un « Google Earth du Net »

Outre l'opérateur historique allemand **Deutsche Telekom**, les entreprises **NetCologne, Stellar, CETel et IABG** seraient concernées par la surveillance à grande échelle pratiquée par la NSA et le GCHQ. Des identifiants auraient été piratés pour disposer d'un accès aux serveurs.

Les données ainsi collectées alimenteraient le programme *« **Treasure Maps** »* (*« carte au trésor »*) de la NSA, dont le *New York Times* s'est fait l'écho dès novembre 2013. À travers la collecte et l'analyse de données massives, la NSA et le GCHQ parviennent à cartographier les principaux noeuds du réseau, mais aussi les terminaux qui s'y connectent (PC, smartphones, tablettes, objets…), selon le *Spiegel*.

Cette *« **carte interactive de l'Internet mondial** »* ou *« Google Earth de l'Internet »*, selon les termes de l'hebdomadaire allemand, permettrait de localiser quasiment en temps réel *« n'importe quel appareil, à n'importe quel endroit et à n'importe quel moment »*. Les détails concernant les réseaux câblés et satellitaires – par exemple, l'obtention d'un accès à l'insu des exploitants – peuvent apparaître. Les réseaux *« observés »* (avec des points d'accès activés), dont ceux de Deutsche Telekom et NetCologne, feraient ainsi l'objet d'une marque rouge.

En Allemagne, les données de plus de 60 millions de clients sont exposées, et celles de millions d'autres individus et entreprises à l'international. D'autres agences de renseignement qui coopèrent avec la NSA américaine, du Royaume-Uni à la Nouvelle-Zélande, disposeraient de cette carte pour leurs propres opérations de veille, voire la préparation d'**attaques informatiques**.

Des pratiques contraires au droit allemand

Alerté par *Der Spiegel*, les opérateurs allemands ont réaffirmé que les cyberattaques sont contraires à la loi allemande. Berlin ne tolère pas non plus la surveillance du smartphone de sa chancelière, **Angela Merkel**. Des enquêtes internes sont en cours. *« L'accès de services de renseignement étrangers à nos réseaux serait tout à fait inacceptable »*, a commenté un porte-parole de Deutsche Telekom. La NSA et le GCHQ, de leur côté, ont assuré, en novembre dernier, louer des espaces serveurs dans différents datacenters dans le cadre d'opérations *« légales »*.

Le **soupçon de collusion** entre les services de renseignement et l'industrie IT est vivace. En France,

Orange, qui aurait été ciblé en 2013 par une opération de la NSA visant un câble sous-marin reliant la France à l'Afrique du Nord et l'Asie, entretient lui-même une relation étroite avec la DGSE (Direction générale de la sécurité extérieure).

Lire aussi

Scan de ports TCP : comment la NSA et le GCHQ préparent leurs attaques

NSA et GCHQ décodent les communications chiffrées sur Internet