24 janvier 2014
Snowdenovitch

Il n'y a pas que la NSA, les Russes aussi nous espionnent sur les réseaux sociaux

Deux chercheurs de l'université de Karlstad (Suède) affirment qu'en Russie, des oreilles indiscrètes exploitent le réseau anonyme Tor pour espionner les internautes, notamment sur Facebook.

Avec Atlantico.fr

Quelque part en Russie, des oreilles indiscrètes exploitent un nœud d'écoute à la périphérie de Tor, un réseau capable d'anonymiser les transferts d'information sur Internet. Et ces oreilles s'intéressent tout particulièrement à ce qui se passe sur Facebook. C'est la conclusion de deux chercheurs qui ont publié une étude sur le sujet lundi, au terme de quatre mois de recherches,rapporte le site Wired.

Philipp Winter et Stefan Lindskog, de l'université de Karlstad (Suède), ont identifié 25 nœuds Tor capables d'altérer le trafic Web, de censurer certains sites, voire d'émettre de faux certificats de sécurité, garant du chiffrement des communications. Certains nœuds au comportement étrange relèvent probablement d'erreurs de configuration ou de problèmes venant des FAI. Mais 19 d'entre eux ont, a priori, été créés volontairement pour espionner les internautes.

Parfois, ces nœuds ont été programmés pour intercepter uniquement le trafic vers des sites particuliers (comme le réseau social Facebook), peut-être pour réduire les chances d'être détectés. "Ce sont ceux-là que nous avons trouvés", explique Philipp Winter. "Mais il pourrait bien y en avoir d'autres."

Tor (The Onion Router) est un réseau décentralisé qui fait transiter les connexions des internautes par des serveurs mis en place par des volontaires répartis dans le monde, dans le but de les anonymiser. "Il existe ainsi environ 3 400 nœuds TOR répertoriés", identifiables et potentiellement blocables, détaille au Monde un bénévole qui maintient un nœud. Il existe aussi environ un millier de nœuds non-répertoriés, dont les adresses ne sont pas connues publiquement.

Problème : le nœud de sortie ("exit node") est le seul maillon de la chaîne à avoir toutes les cartes en main pour lire les données de l'internaute. Il est donc extrêmement vulnérable à l'espionnage. Comme les nœuds de Tor sont gérés par des bénévoles, la moitié du temps anonymes, le trafic Web peut parfois tomber entre les mains d'un opérateur de nœud de sortie corrompu.

Philipp Winter et Stefan Lindskog ont découvert plusieurs nœuds de sortie en Russie mettant en scène une attaque*man-in-the-middle attack* (MITM) permettant d'usurper le certificat de sécurité, garant du chiffrement des communications.

La signature numérique des nœuds russes était la suivante : "Main Authority" ("Autorité principale"). Et contrairement aux autres nœuds de sortie anormaux, ceux qui étaient signés "Main Authority" et qui étaient blacklistés sur Tor réapparaissaient systématiquement en un rien de temps. En quatre mois, Philipp Winter et Stefan Lindskog ont trouvé 19 nœuds de sortie signés "Main

Authority". Dix-huit venaient de Russie et un des Etats-Unis.

Les deux chercheurs ne savent pas précisément qui se cache derrière cette "Autorité principale". Selon eux, il s'agirait davantage d'un hacker ayant la mauvaise manie de fouiner et d'espionner les autres que d'une agence gouvernementale.