La NSA mène la chasse aux administrateurs systèmes

De nouvelles révélations sur les écoutes massives américaines témoignent de l'intérêt prononcé de l'Agence nationale de sécurité américaine (NSA) pour une population en particulier : **les administrateurs systèmes**. D'après un document dérobé à la NSA par son ex-consultant **Edward Snowden,** et obtenu par *The Intercept*, site co-fondé par le journaliste **Glenn Greenwald**, l'agence américaine **traque les courriels privés et les comptes Facebook des sys admin**. Et ce avant de pirater leurs ordinateurs pour obtenir un accès aux réseaux contrôlés par leurs soins.

« Je chasse les sys admin »

Le document daté de 2012 inclut plusieurs notes issues d'un forum de discussion interne à la NSA. L'un des billets est intitulé *« je chasse les sys admin »* (sic). Un agent de la NSA explique que pirater les ordinateurs d'administrateurs systèmes travaillant pour des **opérateurs télécoms et FAI étrangers** peut offrir un accès étendu aux communications échangées sur leurs réseaux (lire : *NSA : les 5 enseignements des dernières révélations de Snowden*).

Outre la collecte de données de systèmes infiltrés (CNE – Computer Network Exploitation), l'agent évoque la création d'une **base de données d'administrateurs systèmes** internationaux à cibler. Bien que les *« sys admin »* ne soient pas suspectés d'activité criminelle, ils sont visés parce qu'ils contrôlent l'accès aux réseaux d'organisations que la NSA veut infiltrer au nom de la lutte antiterroriste. *« Quelle meilleure cible que la personne ayant déjà les 'clés du royaume' ? »*, résume la NSA.

Le mappage réseau

La NSA ne s'arrête pas aux identifiants, mots de passe et noms d'utilisateurs. La note interne inclut une liste d'autres données à glaner une fois compromis les ordinateurs d'administrateurs systèmes. Parmi lesquelles : le mappage réseau et les **listes d'accès IP.**

Impliqué dans les travaux de la NSA visant à accéder aux routeurs et réseaux étrangers, l'auteur de ces notes serait membre de l'unité de renseignement électromagnétique de l'agence. Ce même spécialiste réseau serait lié au programme controversé visant à identifier les personnes utilisant **le réseau d'anonymisation Tor** (lire : *Prism : Le réseau Tor résiste aux attaques de la NSA*).

L'étendue des attaques de type CNE est difficile à déterminer. Outre les cibles étrangères, des citoyens américains pourraient en être victimes. Or, il est illégal pour la NSA de les surveiller sans autorisation judiciaire. L'agence n'a pas commenté ces révélations. Elle s'est également abstenue d'expliquer comment ses services s'assurent que des Américains ne sont pas ciblés.

Qualifiant le sys admin de *« **moyen pour parvenir à ses fins** »*, l'agent de la NSA souligne : *« les administrateurs systèmes ne sont généralement pas mon objectif final. Ma cible ultime est l'extrémiste/terroriste ou les officiels de gouvernements qui utilisent le réseau dont s'occupe tel ou tel admin »*.

Le lanceur d’alertes **Snowden, lui-même administrateur système**, peut en témoigner.

crédit photo © Sam72 – Shutterstock

En complément :

Tout sur l’arsenal secret des espions de la NSA
