Les espions anglais utilisent de faux profils LinkedIn et Slashdot

L'agence de renseignement britannique **GCHQ (Government Communications Headquarters)** aurait utilisé des versions piratées de sites Internet, dont LinkedIn et Slashdot, pour **compromettre les ordinateurs d'ingénieurs et accéder aux réseaux internes d'opérateurs en Europe**, rapporte *Der Spiegel*.

L'hebdomadaire allemand, qui fait à nouveau référence à des documents révélés par le lanceur d'alertes **Edward Snowden**, avait signalé dès septembre l'espionnage de l'opérateur belge Belgacom par le GCHQ. Le magazine a précisé lundi 11 novembre que des équipes spéciales du GCHQ auraient identifié des employés travaillant à la maintenance et à la sécurité des réseaux de Belgacom. Le GCHQ aurait déterminé lesquels utilisent le réseau social professionnel **LinkedIn** et le site d'information IT **Slashdot.org**, avant d'établir de faux profils et d'y associer un programme malveillant transformant les ordinateurs infectés en plateformes d'espionnage.

Quantum Insert : Belgacom et l'OPEP ciblés

Les ordinateurs ciblés ont été infectés en utilisant la technologie d'infiltration de l'agence de renseignement nommée *« Quantum Insert »*, qui a permis à une équipe de hackers du GCHQ (MyNoc – My Network Operations Centre) de s'infiltrer dans le réseau interne de Belgacom et celui de BICS (Belgacom International Carrier Services), filiale de l'opérateur belge en charge du transport international de communications. Les routeurs GRX, utilisés par Belgacom lorsque des utilisateurs passent des appels ou se connectent à l'étranger via leur téléphone mobile, feraient partie des cibles prioritaires du GCHQ. L'agence s'intéresserait à d'autres spécialistes de l'itinérance internationale, dont le suisse **Comfone** et la multinationale **Mach** (scindée depuis en deux : Starhome Mach et Syniverse).

Les administrateurs réseaux et autres professionnels IT seraient les premiers ciblés par le GCHQ, leurs ordinateurs permettant d'obtenir un accès étendu aux infrastructures des entreprises à surveiller. Le GCHQ utiliserait des **serveurs haute performance situés sur des points de commutation clés de l'Internet**. Quand une cible cherche à se connecter à un site web spécifique, comme LinkedIn, ces serveurs sont activés et **une copie exacte du site est proposée aux utilisateurs**. Le code malveillant associé permettant de pirater les ordinateurs ciblés.

Quantum aurait été développé à l'origine par l'homologue américain du GCHQ, la **NSA (National Security Agency)**, et aurait aussi été utilisé pour infiltrer le réseau informatique du **siège de l'OPEP à Vienne**, en Autriche.

LinkedIn condamne l'utilisation de faux profils

Le directeur du GCHQ, **Iain Lobban**, s'est présenté la semaine dernière devant le parlement britannique et a tenté de convaincre son auditoire du bien fondé des méthodes utilisées par

l'agence britannique. Iain Lobban a souligné à cette occasion que seuls les individus et organisations dont les activités constituent une menace pour la sécurité nationale ou l'économie du Royaume-Uni peuvent faire l'objet d'une surveillance par ses services. Mais, il ne s'est pas exprimé sur l'utilisation de techniques illégales telles que le détournement de sites officiels et l'utilisation de faux profils complétés de malwares…

LinkedIn, de son côté, a déclaré à *Der Spiegel* prendre la vie privée de ses membres *« très au sérieux »* et ne pas approuver *« la création ou l'utilisation de faux profils LinkedIn ou l'exploitation de sa plateforme »* à des fins illicites. Starhome Mach a indiqué mener un audit interne pour s'assurer que son infrastructure informatique soit bien sécurisée. Enfin, Syniverse et Comfone ont expliqué ne pas avoir eu connaissance d'une infiltration de leurs systèmes par les services de renseignement britanniques ou toute autre agence gouvernementale. Belgacom ne s'est pas encore prononcé sur ce dossier.

Quant au GCHQ, il n'a pas commenté ces dernières révélations, mais déclarait en 2011 vouloir atteindre si nécessaire *« tout terminal mobile, n'importe où, n'important quand »*.

Voir aussi
Rétrospective : la saga PRISM

crédit photo © Claireliot – Fotolia.com