Un réseau de cyber-espions visant plus de 30 pays mis au jour.

Moscou , La société spécialisée en sécurité informatique Kaspersky Lab a annoncé mardi avoir mis au jour un redoutable réseau de cyber-espions à l'origine d'attaques d'une complexité sans précédent infectant les disques durs de gouvernements, agences gouvernementales et sociétés stratégiques dans plus de 30 pays.

Baptisé Equation par Kaspersky, ce groupe a infecté à partir de 2001 des milliers, voire des dizaines de milliers de victimes dans plus de 30 pays dans le monde, écrit la société dans un rapport.

Kaspersky évoque un réseau qui surpasse tout ce qui est connu en termes de complexité et de sophistication des techniques et unique dans presque tous les aspects de ses activités.

Il utilise des outils très compliqués et coûteux à développer en vue d'infecter les victimes, accéder à leurs données et masquer son activité avec un professionnalisme remarquable, explique Kaspersky.

Concernant les auteurs de ces attaques, le laboratoire russe fait état de liens solides avec le fameux virus Stuxnet, à l'origine d'attaques contre le programme nucléaire iranien et utilisé selon Téhéran par les Etats-Unis et Israël.

Ainsi le virus Fanny, l'un de ceux utilisés par le groupe, porte des traces qui indiquent que les développeurs d'Equation et Stuxnet sont soit les mêmes, soit coopèrent étroitement.

Les pays les plus touchés sont l'Iran, la Russie, le Pakistan, l'Afghanistan, l'Inde, la Chine, la Syrie et le Mali. Les cibles, sélectionnées avec une précision chirurgicale, vont des gouvernements aux antennes diplomatiques, armées, médias, organisations islamiques ou les secteurs des télécoms, des hydrocarbures, du nucléaire, des nanotechnologies, de la finance.

Le mode opératoire faisait en sorte de ne pas viser certains pays comme la Jordanie, la Turquie et l'Egypte.

Agissant par le biais de virus connus sous le terme de cheval de Troie, les outils utilisés par le groupe Equation avaient la particularité d'infecter des disques durs et le programme informatique gérant leur fonctionnement. Ces disques durs étaient même reprogrammés afin que les virus deviennent quasi impossibles à éliminer.

Les données des ordinateurs des victimes pouvaient être récupérés via des clés USB ou des CD-ROM infectés. Ainsi, raconte Kaspersky, des scientifiques participant à une conférence au Texas ont reçu des CD-ROM consacrés à l'événement mais aussi porteurs de ces virus capables de transmettre leurs informations vers des serveurs du groupe Equation.

L'avocat russe de l'ex-consultant du renseignement américain Edward Snowden, Anatoli Koutcherena, a vu dans ce rapport la confirmation des avertissements de son client, réfugié en Russie après avoir révélé l'ampleur du système de surveillance du gouvernement des Etats-Unis.

Cela ne s'arrêtera pas là: bientôt nous verrons le contrôle total exercé sur les citoyens et les hommes politiques se renforcer encore par le biais des nouvelles technologies imaginées par les services secrets américains, a-t-il déclaré à l'agence publique russe Ria-Novosti.

Les services de renseignements intérieurs et extérieurs russes ont assuré ne pas avoir été victimes de ces attaques.

A bientôt.

Et grosse bise numérique.