100 000 ordinateurs trafiqués par la NSA… Le soupçon grandit à Bruxelles

Nouvelles révélations concernant les multiples programmes d'écoute mis au point par la NSA. Selon le *New York Times (NYT)*, l'agence de renseignement a implanté un **système espion dans près de 100 000 ordinateurs** répartis dans le monde. Cette faille intrinsèque permet à la NSA d'**écouter ces machines** et lui fournit également un **vecteur d'attaque** quand elle veut pénétrer sur les réseaux des organisations où ont été placées ces machines vérolées.

Selon le quotidien américain, qui s'appuie sur des documents de la NSA, des témoignages d'experts et d'officiels américains, l'agence utilise cette technique depuis 2008. Cette dernière repose sur des transmissions par ondes radio, assurées par un **circuit dédié implanté dans un connecteur USB.** Le *NYT* parle également de petits circuits parfois insérés dans l'ordinateur lui-même. Cette technique d'espionnage fonctionne donc y compris avec des ordinateurs non reliés à Internet. Les informations transmises par radio sont recueillies par une station placée par la NSA à quelques kilomètres de la cible.

Dans la plupart des cas, ces mouchards sont installés **par un espion** (rappelons que des documents dévoilés par Edward Snowden montrent que l'agence intercepte des colis renfermant des équipements IT lors de leur livraison, afin de les piéger), **par le constructeur lui-même** ou **par un utilisateur complice**, explique le quotidien new-yorkais.

L'affaire Belgacom a laissé des traces

Si le quotidien ne précise aucun nom d'industriel impliqué, ces nouvelles révélations **renforcent les soupçons pesant sur l'industrie IT américaine**. Pour l'instant, seul RSA a été pris les doigts dans le pot de confiture. La filiale sécurité de EMC a intégré comme algorithme par défaut un standard de cryptage volontairement affaibli par les espions américains, ignorant les doutes pesant sur la fiabilité de ce logiciel du fait de l'implication de la NSA dans la définition de cette norme. Le tout alors que RSA était lié à l'agence de renseignement par un contrat de 10 millions de dollars.

Parmi les cibles de ce programme d'infection d'ordinateurs, **programme baptisé Quantum**, figurerait l'armée chinoise, régulièrement accusée par les Etats-Unis de mener des cyber-attaques contre les intérêts américains, mais aussi des réseaux militaires russes, la police et les cartels de la drogue au Mexique, des partenaires des Etats-Unis comme l'Inde, l'Arabie Saoudite ou le Pakistan. Surtout, cette liste comporte également des **institutions chargées du commerce au sein de l'Union européenne**. Rappelons que l'Europe mène en ce moment des négociations avec les Etats-Unis portant sur un approfondissement des accords de libre-échange.

Une nouvelle anicroche dans le partenariat transatlantique qui ne va pas améliorer la cote de la NSA à Bruxelles. L'affaire Belgacom, le piratage de l'opérateur belge qui est également **le prestataire de la Commission européenne, du Conseil de l'Europe et du Parlement européen**, a mis les institutions du Vieux Continent en émoi. Rappelons que la NSA, avec la complicité du GCHQ britannique, est parvenue à s'introduire sur le réseau de l'opérateur en trompant certains de

ses employés avec de fausses pages LinkedIn. Belgacom a indiqué que le malware utilisé par la suite était extrêmement complexe et avait requis des ressources financières et humaines qui ne sont pas à la portée d'organisations privées ou de hackers isolés.

NSA : « Pas d'espionnage économique »

Les premières versions du **rapport d'enquête de la Commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen** montrent le degré d'inquiétude à Bruxelles et Strasbourg. Ce rapport préconise en effet une action déterminée de l'UE, notamment une révision des traités transatlantiques portant sur l'échange de données (comme une suspension de Safe Harbour ou de l'accord Swift), un **soutien au développement d'une industrie IT européenne indépendante** des Etats-Unis (via le levier de la commande publique) ou encore le renforcement des exigences de sécurité des données imposées aux opérateurs télécoms et aux services Cloud. Sans oublier, évidemment, un audit de la sécurité IT des institutions européennes. Le rapport ne manque pas d'égratigner au passage l'attitude de certains pays membres, la Grande-Bretagne bien sûr, mais aussi l'Allemagne et la France, pour la proximité de leurs services avec la NSA américaine. Précisons que **les directeurs de la DGSE et de la DCRI**, respectivement les services extérieurs et intérieurs français, ont **refusé de témoigner** devant la commission d'enquête du Parlement européen.

Dans ce même rapport, les rapporteurs livrent le fond de leur pensée. Et écrivent « *qu'il est plus que douteux qu'une collecte de données de cette ampleur (celle mise en œuvre par la NSA, NDLR) soit seulement dictée par la lutte contre le terrorisme* ». Et de pointer « *l'existence possible d'autres motivations comme l'espionnage politique et économique* ».

Dans l'article du *New York Times*, un porte-parole de la NSA nie toute volonté de ce type : « *Nous n'utilisons pas nos capacités d'espionnage à l'étranger pour voler des secrets à des entreprises étrangères pour le compte de compagnies américaines afin d'améliorer leur compétitivité à l'international ou améliorer leurs profits. Pas plus que nous ne leur transmettons des informations que nous collectons.* »

Selon une carte publiée par un journal néerlandais, document transmis par Edward Snowden, la NSA avait, **en 2008, pénétré plus de 50 000 réseaux** dans le monde, avec des malwares du type de celui utilisé pour l'espionnage de Belgacom. Selon un officiel américain interrogé par le *NYT*, ce chiffre serait désormais plus proche de 100 000. Une source interrogée par le quotidien explique que ces mouchards servent à détecter des cyber-attaques ciblant les Etats-Unis.

Voir aussi

Silicon.fr étend son site dédié à l'emploi IT
Silicon.fr en direct sur les smartphones et tablettes