Piratage de l'Elysée en 2012 : le coup venait bien de la NSA

Dans une conférence donnée à l'école Centrale de Paris, repérée par *Le Monde*, Bernard Barbier, l'ancien directeur technique de la DGSE, a confirmé que Paris était bien persuadé de la responsabilité des Etats-Unis dans le piratage de l'Elysée, en mai 2012. Entre les deux tours de l'élection présidentielle, des ordinateurs des collaborateurs du chef de l'Etat Nicolas Sarkozy avaient été écoutés.

Selon l'ex-directeur technique des services de renseignement extérieurs de la France, l'analyse de cette attaque, à laquelle il a participé à la demande du RSSI de l'Elysée, un ancien de la DGSE, a révélé la présence d'un malware dont la signature était déjà présente sur une attaque contre la Commission européenne en 2010. « *Mon équipe de reverse engineering avait à l'époque compris comment ce malware très compliqué fonctionnait. On avait conclu que seuls les Américains ou les Russes avaient pu fabriquer ce malware »,* a expliqué Bernard Barbier, dans cette conférence tenue en juin dernier. Le mécanisme de l'infection est complexe : une connexion à Facebook depuis l'Elysée entraîne la fabrication de faux paquets IP. Cette technique sera ensuite décrite dans les documents exfiltrés par Edward Snowden sous le nom de « Quantum attack ». La méthode est jugée comme *« révolutionnaire »* et *«redoutable »* par Bernard Barbier.

« On est allé les engueuler »

Après l'attaque de l'Elysée, grâce aux métadonnées que conserve la DGSE, les services de Bernard Barbier retracent une partie de la vie de cette souche infectieuse. « *J'en suis venu à la conclusion que cela ne pouvait être que les Etats-Unis »,* ajoute-t-il.

« On a reçu l'ordre de tout nettoyer et d'aller voir mes amis américains pour les engueuler », ajoute l'ex-directeur technique de la DGSE. *« Les Américains se doutaient qu'on venait les voir à ce sujet, raison pour laquelle ils ont écrit une note pour préparer cette réunion (note qui a ensuite fuité dans Le Monde après avoir été dérobée par Edward Snowden, NDLR). Après la réunion, Alexander (le patron de la NSA à l'époque) n'était pas content. Dans le bus, il m'a expliqué que la NSA pensait que jamais on ne détecterait l'attaque. »*

Babar était bien français

Lors de cette même conférence (disponible sur YouTube), Bernard Barbier a également confirmé l'origine française d'un malware appelé Babar, mis en évidence dans une note dévoilée par Edward Snowden. Dans cette dernière, publiée par *Le Monde* en 2013, on apprend que les services secrets canadiens ont isolé un malware et qu'ils suspectent Paris. *« Les Canadiens ont fait du reverse engineering sur ce malware et ils ont vu que le programmeur avait mis des commentaires dans lesquels apparaissait le mot Babar. Et ce programmeur a signé Titi ! Ils se sont dit que ça, c'était un Français. Et, effectivement, c'était un Français. »*

Rappelons que, fin 2013, après sept années à la direction technique de la DGSE, Bernard Barbier a

rejoint Sogeti en tant que conseiller pour la cybersécurité et la cyberdéfense.

Mise à jour le 6/09 à 9h30 : le premier lien YouTube étant inopérant (la vidéo a été supprimée par l'utilisateur), nous vous indiquons un second lien permettant de visionner la conférence de Bernard Barbier.

A lire aussi :

Projet Sauron : anatomie d'une plateforme de cyberespionnage avancée

Pour Snowden, c'est la Russie qui a piraté la NSA

Espionnage de Hollande, Sarkozy, Chirac : la NSA dit merci à Gemalto ?