Les dessous de la société d’espionnage Hacking Team… | Le Net Expert Informatique

Les dessous de la société d’espionnage Hacking Team…

La firme, qui s'est fait voler plus de 400 gigaoctets de données confidentielles, avait présenté ses technologies aux services de renseignements français. La société Hacking Team, soupçonnée d'avoir livré des logiciels d'espionnage à des régimes autoritaires, assure n'avoir rien commis d'illégal.

On soupçonnait Hacking Team de rouler sa bosse pour des dictatures. Et voilà que le journal Le Monde nous apprend que la sulfureuse entreprise d'espionnage a également eu des contacts avec les services d'espionnage français… Lundi 6 juillet, la société italienne a été victime d'un piratage de grande ampleur de ses données confidentielles et des comptes Twitter de plusieurs de ses responsables. Des centaines de gigaoctets de données se sont déversées sur le Web et ont été immédiatement téléchargées et consultées par ceux qui l'accusaient de faire bénéficier de ses technologies des régimes autoritaires.
L'entreprise est en effet spécialisée dans le développement et la commercialisation de logiciels de surveillance ou de piratage très performants, principalement destinés à des États. Logiciels de blocage de pages internet, systèmes de mise sous surveillance de boîtes mails jugées suspectes… Hacking Team a développé une impressionnante gamme de services. Leur produit phare, dénommé RCS (pour Remote Control Systems), est un packaging incluant des logiciels tels que DaVinci et Galileo, qui permettent de visualiser les frappes effectuées sur le clavier de l'ordinateur visé, d'en collecter les informations sensibles telles que les adresses mails, les documents enregistrés ou les mots de passe, ou encore de récupérer les historiques de navigation.

Ennemie d'Internet
La facilité avec laquelle ces outils peuvent être utilisés à des fins d'espionnage de masse avait conduit certaines ONG à dénoncer les pratiques de cette société. Cette dernière avait même fini par être classée parmi les ennemis d'Internet par Reporters sans frontières en 2013, en raison des rapports commerciaux qu'elle entretenait alors avec le Maroc et les Émirats arabes unis. Des traces de ses logiciels avaient ainsi été retrouvées sur les ordinateurs du site d'information marocain Mamfakinch, quelques jours après que ce média a reçu le Breaking Borders Award 2012 remis par Global Voices et Google.
Autre soupçon : « Un expert en sécurité, Morgan Marquis-Boire, a examiné des pièces jointes attachées à un e-mail envoyé à Ahmed Mansoor, un blogueur émirati. Elles étaient contaminées. Il y a trouvé de fortes indications suggérant que la source du cheval de Troie provenait de Hacking Team », écrit également RSF.
L'entreprise jouit dans le milieu d'une réputation douteuse, et est soupçonnée de collaborer avec des pays peu recommandables. Jusqu'à présent, la société clamait son innocence et aucune preuve de son implication dans la mise en place des systèmes de surveillance électronique de ces pays n'avait été découverte. « Nous faisons extrêmement attention à qui nous vendons nos produits. Nos investisseurs ont mis en place un comité légal qui nous conseille continuellement sur le statut de chaque pays avec lequel nous entrons en contact », assurait le PDG de Hacking Team, David Vincenzetti, dans une interview accordée en 2011 au journaliste Ryan Gallagher.

Des régimes autoritaires en clients
Kazakhstan, Arabie saoudite, Azerbaïdjan… De nombreux États – dont les dirigeants ne font pas toujours des libertés individuelles une priorité de leur règne… – font partie de la liste des clients. Parmi ces pays, certains sont connus pour une répression dure de leur population et leurs violations répétées des droits de l'homme. On peut ainsi noter l'exemple du Soudan, avec lequel Hacking Team a toujours nié avoir collaboré. Cependant, les documents publiés révèlent l'existence d'un contrat de 480 000 euros avec le gouvernement actuellement en place. La Russie fait également partie des heureux bénéficiaires des services de Hacking Team. La firme prend même la peine d'indiquer sur ses documents internes que ces deux pays ne sont « officiellement pas clients » (« oficially not supported ») de l'entreprise.
Interrogé au sujet de la série de contrats signés avec le Soudan, le porte-parole de l'entreprise, Éric Rabe, a quant à lui maintenu que le document cité remontait à avant les sanctions décidées par les Nations unies contre le pays.

La France, elle aussi intéressée par les services de l'entreprise
D'après certains documents, la France et Hacking Team seraient entrés en contact plusieurs fois ces dernières années. La prise de contact entre le ministère de la Défense et l'entreprise a eu lieu en 2013, alors qu'une réunion de présentation s'est tenue fin 2014 dans un hôtel près de l'aéroport Charles-de-Gaulle à Paris. Étaient représentés à cette réunion la DGSI et le Groupement interministériel de contrôle (GIC) chargé quant à lui des écoutes administratives (c'est-à-dire menées sans mandat judiciaire), et dirigé par le Premier ministre.
Si la DGSI affirme n'avoir donné aucune suite à cette réunion, ce n'est pas le cas du GIC qui a poursuivi ses échanges avec Hacking Team. Comme le révèle un échange de courriels entre le GIC et Hacking Team, Philippe Vinci, l'un des responsables de l'entreprise, s'est rendu au siège du GIC le vendredi 3 avril 2015. Cette information est confirmée par un échange de courriels entre la société et le groupement interministériel datant du mardi 7 avril. On y apprend également que le GIC serait intéressé par une démonstration de la part d'Hacking Team. L'entreprise aurait alors proposé aux représentants du GIC de venir assister à une telle démonstration en Italie courant mai. Aucune information concernant la suite à donner à ces rendez-vous n'a pour le moment fuité.

« Nous n'avons rien à cacher »
Après deux jours sans réaction, l'entreprise a finalement commenté ce vol de données dans une interview accordée au site IBTimes : « Nous n'avons rien à cacher sur nos activités et nous pensons qu'il n'y a aucune preuve dans ces 400 gigabits de données que nous avons violé une quelconque loi », a ainsi affirmé le porte-parole de l'entreprise, Éric Rabe.
Pour le moment, et en attendant de connaître exactement le contenu des données qui ont été piratées, la société italienne a demandé à ses clients de cesser d'utiliser ses logiciels. Les auteurs du piratage ne se sont pas encore manifestés.

Source : http://www.lepoint.fr/high-tech-internet/les-curieux-clients-de-la-societe-d-espionnage-hacking-team-08-07-2015-1943190_47.php
Par Ian BEAURAIN