Hacking Team, un spécialiste de cyber-armes massivement piraté

Un ou des hackers se sont fait remarquer en dérobant plus de **400 Go de données** de Hacking Team. Cette société italienne est connue pour proposer **des outils de surveillance et d'intrusion** (via des failles zero day) pour les gouvernements et les autorités policières et judiciaires. Elle est inscrite sur la liste noire des associations de défense des droits de l'Homme (elle est classée comme « **ennemi de l'Internet** » par Reporter Sans Frontières au même titre que Blue Coat ou Amesys) pour fournir des cyber-armes aux gouvernements afin de réprimer violemment les opposants politiques. Hacking Team s'est toujours défendu de cela en mettant en avant un hacking éthique.

Les données subtilisées ont été publiées en fichier Torrent (puis sur Pastebin) et comprennent des enregistrements audios, des emails ou du code source. L'analyse de ces documents (notamment par @SynAckPwn) montre les rapports étroits avec les gouvernements oppressifs. La société italienne a ainsi vendu son logiciel de contrôle d'accès à distance (RCS Remote Control System) Da Vinci à l'Egypte, le Soudan, le Liban et l'Ethiopie.

Le contrat avec le Soudan est particulièrement mis en avant, car Hacking Team avait affirmé n'avoir jamais passé de contrat avec ce pays. De plus, le Soudan est soumis à un embargo sur les armes décrété par les Nations Unies, qui est couvert par le droit européen. Or dans les documents piratés, on retrouve une facture de **480 000 euros** en date du 2 juillet 2012 avec le Soudan avec la mention « not officialy supported » (pas officiellement supporté).

Une communication difficile

Le package de documents subtilisés comprend d'autres factures qui visent les autorités policières italiennes, Oman, la Corée du Sud, les Emirats Arabes Unis, le Kazakhstan, la Mongolie, le Liban, l'Allemagne, l'Arabie Saoudite, le Mexique, le Brésil, Singapour, l'Egypte et le Vietnam. Le total des prestations est évalué à **4,324 millions d'euros**.

Parmi les autres documents publiés, on retrouve certaines méthodes de piratage, comme l'infection d'application Android ou le moyen d'intercepter le trafic Tor en passant par la surveillance des discussions et des échanges de photos sur WhatsApp.

La société italienne a mis du temps pour réagir, en raison du piratage de son compte Twitter. Christian Pozzi, un des responsables de la sécurité de Hacking Team a indiqué plusieurs heures après le piratage que « *la firme était sur le pont. Les responsables seront arrêtés et nous travaillons actuellement avec la police* ». Avant d'ajouter sur son compte Twitter qu'*« une grande partie de ce que les pirates affirment concernant notre entreprise est faux. Merci de ne pas répandre de fausses informations sur les services que nous offrons »*. Une demande qui a sonné le glas de son compte Twitter piraté très rapidement.

A lire aussi :

Reporters sans frontières s’attaque aux éditeurs d’outils de filtrage

Crédit Photo : Creativa Image-Shutterstock