Quand la CIA installait des spywares pour surveiller le FBI et la NSA

Quand la CIA s'amusait à espionner ses partenaires à coup d'utilitaires biométriques. C'est la dernière révélation de Wikileaks extirpée des documents dits «Vault 7» sur les outils de cybersurveillance de l'agence américaine du renseignement. En 2009, la Central Intelligence Agency lançait « ExpressLane », un projet visant à équiper en systèmes biométriques des services de liaisons dans le monde entier à travers le FBI, la NSA ou encore le DHS, le ministère de la sécurité intérieure.

Officiellement, ExpressLane servait à partager des données biométriques récupérées auprès des différentes agences américaines. *« Mais ce « partage volontaire » ne fonctionne évidemment pas ou est considéré comme insuffisant par la CIA*, avance le site créé par Julian Assange, *car ExpressLane est un outil de collecte d'informations cachées, utilisé par la CIA pour exfiltrer secrètement les collections de données provenant de ces systèmes fournis aux services de liaison. »* Autrement dit, un nid d'espions au milieu des espions qui témoigne du manque de confiance qui régnait entre les différents services américains.

Installation et exfiltration sur clé USB

Les documents rendus publics par Wikileaks nous apprennent comment la CIA profitait du déploiement et mises à jour des systèmes biométriques pour installer ses spywares. Ce sont les agents de l'OTS (Office of Technical Services), une branche de l'agence du renseignement, qui se chargeait des opérations. Ils pouvaient installer les programmes de récupération des données à partir d'une clé USB et télécharger ces dernières sur cette même clé, dans une partition cachée. Et cela de manière transparente puisqu'un écran classique d'installation d'une application Windows s'affichait lors de l'opération d'exfiltration des données. Un dispositif permettait également de couper la liaison avec le système au cas où le site «partenaire» n'aurait plus fourni d'accès à la CIA. La confiance régnait plus que jamais.

Les systèmes biométriques étaient, eux, fournis par CrossMatch, une entreprise américaine spécialisée dans la gestion des identités. Elle avait indirectement fait parler d'elle en 2011 avec l'assassinat d'Oussama Ben Laden au Pakistan alors que l'armée américaine avait utilisé ses systèmes d'identification pour authentifier l'ex chef d'Al-Qaïda.

Difficile de savoir si la CIA exploite toujours ExpressLane. On peut en douter alors que les documents récupérés par Wikileaks datent de bientôt 10 ans et se rapportent à des technologies propres à Windows XP. Si néanmoins c'était toujours le cas, nul doute que la surveillance des surveillants ne devrait plus perdurer sous cette forme très longtemps suite aux révélations du lanceur d'alertes.

Lire également
Vault 7 : Wikileaks dévoile les rapports cachés entre la société de sécurité Raytheon et la CIA

OutlawCountry : la CIA détourne le trafic des PC et serveurs Linux
Comment la CIA suit les PC à la trace à l'aide du Wifi