Comment la CIA suit les PC à la trace à l'aide du Wifi

Wikileaks poursuit la publication des documents relatifs aux méthodes de surveillance de la CIA. Daté de septembre 2013, le projet ELSA décrit comment l'agence du renseignement américain suit à la trace des individus ciblés à l'aide des réseaux Wifi. *« ELSA est un logiciel qui géolocalise les ordinateurs dotés du Wifi*, explique la CIA. *ELSA fournit un modèle d'information de localisation en enregistrant les détails d'un point d'accès Wifi proche de la machine ciblée et en transmettant les métadonnées à une base de données tierces pour déterminer la latitude et longitude ainsi qu'une mesure de précision. »*

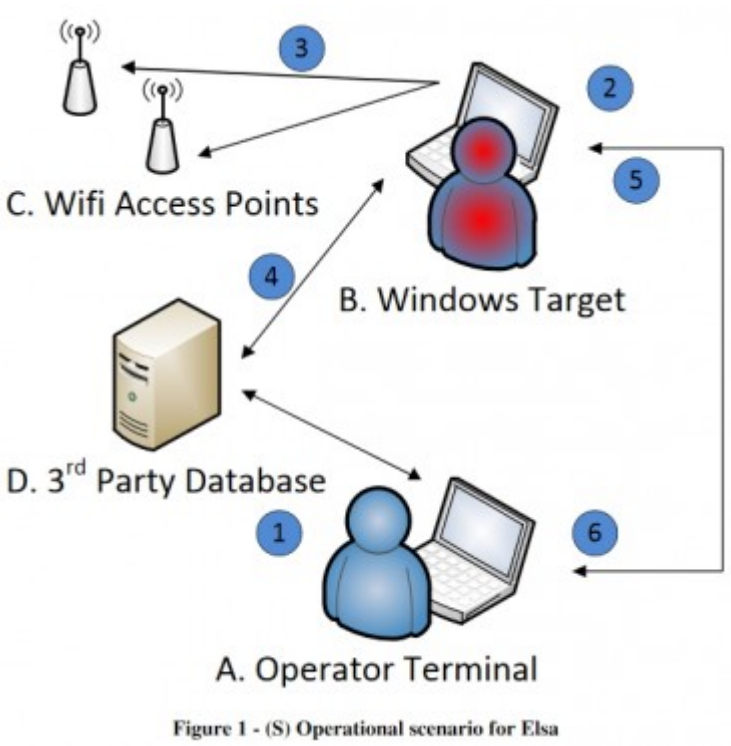

Figure 1 - (S) Operational scenario for Elsa

Cette surveillance rapprochée à distance (si l'on peut dire) se fait en deux étapes. Elle nécessite d'abord l'injection d'un malware dans le PC de la victime. Ce que l'agence opère probablement en exploitant une faille système. Une fois installé, le logiciel caché assure la détection des hotspot Wifi environnant par le PC infecté et commence l'enregistrement à des intervalles réguliers de l'identifiant ESS (Extended Service Set soit l'ensemble des points d'accès locaux), de l'adresse MAC de la carte réseau et de la force du signal, résume Wikileaks. Qui précise que *« pour effectuer la collecte des données, la machine cible ne doit pas nécessairement être en ligne ou connectée à un point d'accès mais peut fonctionner avec un périphérique WiFi activé »*. Autrement dit, l'utilisateur qui se croirait protégé en se déconnectant du réseau aurait tout faux.

Géolocalisation à l'aide de Google et Microsoft

Néanmoins, dès que le PC rejoint le réseau, le malware s'empresse de se connecter aux bases de données géographiques de Google et Microsoft pour déterminer la localisation de la cible de manière horodatée. ELSA utilise pour ce faire des connexions chiffrées (HTTPS) et sauvegarde ses données dans des fichiers chiffrés en 128 bits AES en attendant leur récupération par la CIA. Difficile, pour l'utilisateur un peu méfiant, de vérifier ce qu'ils contiennent, donc. D'autant que les fichiers en question ne sont pas envoyés automatiquement à un serveur de l'agence américaine mais récupérés manuellement par un de ses opérateurs à l'aide de backdoor et autre exploitation de vulnérabilité système.

A noter que, dans sa version 1.0 décrite dans le document, ELSA n'est compatible qu'avec

l'environnement Windows. Soit les PC antérieurs à Windows 8.x et 10. Mais il n'est pas déraisonnable de penser que la CIA a une version de ELSA pour chaque version de l'OS de Microsoft. Windows 10 pourrait donc ne pas être plus à l'abri de cette méthode de surveillance que ne l'était Windows 7 au moment de la mise au point du malware. Et la suppression manuelle de ce dernier et des différentes portes dérobées installées nécessite probablement des connaissances poussées en administration système. ELSA pourrait donc rebondir d'une mise à jour de Windows à l'autre tant que l'utilisateur conserve la même machine. Les révélations de Wikileaks vont-elles désormais pousser Microsoft à se pencher sur la question ?

Lire également

Brutal Kangaroo : quand la CIA cible les réseaux les plus sensibles
CherryBlossom, le programme de la CIA pour pirater les hotspots Wifi
Wikileaks : les outils de hacking de la CIA seront « désarmés » avant publication