Detekt, l'anti-spyware gouvernemental d'Amnesty et l'EFF

Nom : **Detekt**. Nature : anti-spyware. Environnement d'exécution : Windows. Particularité : est promu par plusieurs groupes de défense des droits civiques et des libertés à l'ère numérique.

L'Electronic Frontier Foundation et Amnesty International soutiennent effectivement ce projet Open Source inscrit dans un contexte de lutte contre les opérations de cyber-surveillance visant les militants des droits de l'homme, les opposants à des régimes politiques, les minorités religieuses ou ethniques, les journalistes ou encore les chercheurs, selon nos confrères d'ITespresso.

A l'origine de ce logiciel disponible en six langues dont l'anglais, l'italien et l'espagnol (mais pas le français), le développeur Claudio Guarnieri enregistre aussi le soutien de l'association allemande Digitale Gesellschaft et de l'ONG britannique Privacy International. Ces dernières ont contribué à la mise en avant de Detekt via le site Web *resistsurveillance.org*.

Une première version perfectible

En version 1.2, le logiciel recèle encore de nombreux bugs, comme le reconnaît son créateur. Mais il est déjà capable de détecter de nombreux signes d'infection par des chevaux de Troie accessibles à distance (RAT, pour « Remote-Access Trojans »). DarkComet, BlackShades, Gh0st, ShadowTech… Autant de programmes utilisés notamment dans le cadre d'opérations de surveillance « à long terme » menées par des États.

Certains se trouvent tout simplement sur Internet, intégralement libres de droits. D'autres sont commercialisés par des sociétés privées à des agences de renseignement. Illustration avec FinSpy, ce cheval de Troie qui contrôle l'activité des machines qu'il infecte et récupère des informations confidentielles comme des mots de passe, des historiques de conversation sur Skype, des données de géolocalisation ou encore des coordonnées bancaires.

Il ne s'agit en fait que d'une composante de la solution de contrôle à distance FinFisher, que le groupe Gamma développe via sa filiale allemande basée à Munich. Mais il a déjà constitué le cœur d'action de nombreuses attaques ciblées aux motivations essentiellement politiques, par exemple au Bahreïn face à des activistes démocrates et dans le cadre des élections présidentielles en Malaisie, l'année dernière.

Attention aux faux positifs

Detekt ne fonctionne pas comme un antivirus : il ne supprime aucun fichier. Si des menaces sont détectées, l'utilisateur doit considérer que sa machine n'est plus suffisamment sûre, la déconnecter d'Internet et consulter un professionnel. Avant d'installer Detekt, il faut s'assurer d'avoir fermé tous les programmes en cours : certains sont faussement détectés comme des logiciels espions. Surtout… les antivirus. Autres vérifications à effectuer : disposer d'un OS compatible (de Windows XP à Windows 8 en 32 ou 64 bits ; uniquement en 32 bits pour Windows 8.1) et d'une version

suffisamment récente des librairies Python, Yara, Volatility et Winmpem.

A lire aussi :

Cybercriminalité : un rapport au gouvernement préconise une surveillance préventive

Espionnage : les Etats-Unis lancent des avions renifleurs de data mobile

Credit Photo : Carlos Amarillo-Shutterstock