Déception : on a testé Detekt, il ne s’est rien passé

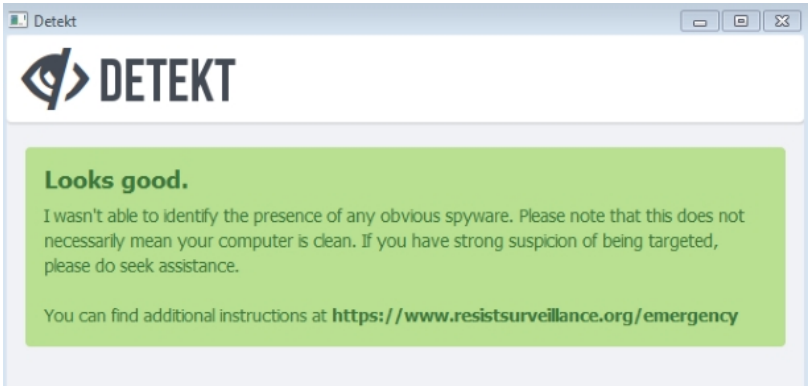
	Déception : on a testé Detekt, il ne s’est rien passé

La promesse était belle : Detekt scanne votre ordinateur à la recherche des logiciels espions qui ciblent les activistes de tout poil, les minorités religieuses, et les journalistes. Nous avons essayé. Ça semble marcher, mais on est un peu amer.

Développé pendant deux ans par Claudio Guarnieri (un informaticien basé à Berlin) en partenariat avec Amnesty International et l'EFF entre autres, Detekt est un logiciel gratuit dont la promesse est d'informer l'utilisateur sur les spyware qui se seraient potentiellement glissés dans sa machine.

« Les défenseurs des droits de l'homme, les journalistes, les ONG, les opposants politiques, les minorités religieuses ou ethniques » sont particulièrement ciblés par les agences de renseignement qui utilisent des outils numériques d'espionnage, avertit l'auteur du logiciel.

La rédaction s'est donc prêtée au jeu du test. Après tout, savoir être espionné par la NSA, la DGSE ou Kim Jong-un, ça crédibilise notre travail.



(Personne ne nous espionne)

Après un scan offline de la machine, le verdict tombe. Rien de suspect sur l'ordinateur utilisé pour rédiger cet article. D'où deux propositions qui nous chagrinent : nous n'entrons dans aucune des catégories espionnées sus-nommées, ou bien nous sommes totalement inoffensifs pour les dites agences de renseignement. Préférons dire que nous avons beaucoup de chance.

En cas de détection d'un danger, l'auteur de Detekt mentionne que le nettoyage reste à faire soi-même. Detekt avertit, mais ne soigne pas. Par ailleurs, s'il ne trouve rien, cela ne signifie pas nécessairement que l'ordinateur ne soit pas la cible d'un service espion, mentionne le site de Detekt (ndlr. ouf !).

Programmé en Python, Detekt recherche des chevaux de Troie de certaines familles, comme DarkComet RAT, XtremeRAT, BlackShades RAT, njRAT, FinFisher FinSpy, HackingTeam RCS, ShadowTech RAT et Gh0st RAT. L'acronyme RAT signifie ici Remote Access Trojans. Le fichier readme.md donne d'autres informations techniques.

Au delà de cette annonce, qui est assurons-le une initiative salutaire, se pose la question de la pérennité de ce type de solution. Tout comme les antivirus, les anti spyware ne sont efficaces que s'ils sont régulièrement mis à jour, pour intégrer les nouvelles menaces, et celles déjà recensées, mais qui évoluent.

Et vous ? Vous en pensez quoi ?

Cliquez et laissez-nous votre avis…

Source : http://www.zdnet.fr/actualites/deception-on-a-teste-detekt-il-ne-s-est-rien-passe-39809965.htm