La NSA écoute nos disques durs ?

	La NSA écoute nos disques durs ?

Kaspersky Lab a découvert une plate-forme de cyber-espionnage dont l'une des composantes, très certainement exploitée par la NSA, permet de surveiller des disques durs.

Iran, Russie, Pakistan, Afghanistan, Chine, Mali, Syrie, Yémen, Algérie… Les gouvernements, organes militaires, sociétés télécoms, banques, médias, chercheurs et activistes d'une trentaine de pays auraient été exposés à des logiciels espions cachés dans des disques durs.
Les équipes de Kaspersky Lab en sont arrivées à cette conclusion après plusieurs années d'enquête sur ce qu'elles considèrent aujourd'hui comme le dispositif de surveillance électronique « le plus complexe et le plus sophistiqué » découvert à date*.
Encore activement exploitée, cette plate-forme serait opérationnelle depuis au moins 2001, voire 1996, si on se fie à la date d'enregistrement de certains serveurs utilisés pour contrôler les malware.
Elle hébergerait notamment un ver très proche de Stuxnet. Ce virus complexe et polymorphe dont la conception est attribuée à l'Agence américaine de sécurité nationale (NSA) avec la collaboration de l'unité 8200 de l'armée israélienne (cyberdéfense) avait mis à mal un site d'enrichissement d'uranium implanté en Iran, endommageant un millier de centrifugeuses.
Mais c'est bien le module de piratage des disques durs qui retient l'attention de Kaspersky. Dans son rapport publié lundi (document PDF sur http://25zbkz3k00wn2tp5092n6di7b5k.wpengine.netdna-cdn.com/files/2015/02/Equation_group_questions_and_answers.pdf, 44 pages), l'éditeur russe note que la quasi-totalité des produits du marché sont affectés : Seagate, Western Digital, Toshiba, IBM, Micron, Samsung…
Il est d'autant plus difficile de détecter l'infection qu'elle se loge dans le firmware des disques durs. Ce qui lui permet aussi de s'activer presque instantanément au démarrage (la seule étape qui précède dans la séquence d'amorçage est l'initialisation du BIOS) et d'ouvrir discrètement des portes dérobées permettant de récupérer des données à foison.
Pour Kaspersky Lab, réussir à implanter un logiciel malveillant dans le firmware d'un disque dur est une prouesse. A moins que les pirates aient eu accès au code dudit firmware. Du côté de Western Digital, on assure ne pas avoir communiqué ce genre de données. Chez Seagate, on estime avoir intégré des couches de sécurité pour éviter les modifications non sollicitées du micrologiciel, ainsi que son étude par reverse engineering.

A qui la faute ?
Le problème remonte peut-être à 2009. Dans le cadre d'une vague de cyber-attaques contre des sociétés high-tech américaines, les pirates avaient eu accès à du code source qualifié de « très précieux » car hébergé sur les serveurs de multinationales et d'organes gouvernementaux.

Dans ce butin figuraient probablement des copies du firmware des différentes marques de disques durs. Et pour cause : lorsqu'elles acquièrent un équipement informatique, les agences classées « sensibles » peuvent demander, pour le compte du gouvernement américain, un audit de sécurité des produits pour s'assurer de l'intégrité du code source… lequel est certainement sauvegardé au passage.

Kaspersky Lab n'affirme pas que la NSA est à l'origine de ce « mouchard à disques durs ». Ses chercheurs disposent toutefois de nombreux indices, comme ce mot-clé GROK trouvé dans le code d'un enregistreur de frappe et déjà présent dans un outil d'espionnage dévoilé en 2013 par Edward Snowden.

Les multiples révélations du lanceur d'alertes pèsent sur l'activité des sociétés high-tech américaines : les ventes de solutions – aussi bien matérielles que logicielles – chutent. A tel point que Peter Swire, membre du groupe de réflexion «Renseignement et Nouvelles technologies» monté par Barack Obama, reconnaît qu'il est «plus que jamais indispensable, pour les Etats-Unis, de mesurer l'impact que chaque décision d'exploiter une faille de sécurité pourrait avoir sur les relations commerciales […] et diplomatiques».

* Malgré sa puissance, il semble que la plate-forme ne soit exploitée que contre un nombre restreint de «cibles d'intérêt» localisées hors des Etats-Unis.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.itespresso.fr/cyber-espionnage-nsa-ecoute-disques-durs-88684.html
Par Clément Bohic