Stuxnet, le virus lancé contre le nucléaire iranien en 2010, refait surface

- Informatique - Sécurité Informatique -

Date de mise en ligne : mardi 25 octobre 2011

Spyworld Actu

La société de sécurité informatique Symantec assure avoir découvert un logiciel malveillant développé par la même équipe qui était à l'origine de Stuxnet, un virus qui avait perturbé les centrales nucléaires iraniennes en 2010.

Il est de retour... en quelque sorte. Stuxnet, le virus qui avait contribué à ralentir le programme nucléaire iranien à l'été 2010, fait de nouveau parler de lui. Duqu, un logiciel malveillant découvert la semaine dernière par la société de sécurité informatique Symantec, servirait en effet de poisson-pilote à de probables futurs Stuxnet.

Duqu fonctionne comme un logiciel espion qui se double d'un voleur numérique. "Son but est de dérober des informations sur les ordinateurs de sociétés très spécifiques, comme celles fournissant des systèmes de contrôle industriel", peut-on lire dans l'analyse détaillée mise en ligne le 14 octobre par les experts de Symantec.

Des données bien précises

Il a été conçu pour capturer, entre autres, des informations sur le design industriel présentes sur les ordinateurs d'entreprises bien définies. Il s'agit d'un type de données très précis et crucial pour les attaques informatiques de type Stuxnet. Pour rappel, ce virus utilisait le design du système de contrôle - mis au point par l'allemand Siemens - des centrales iraniennes afin d'en perturber le fonctionnement.

"Il s'agit de cyber-espionnage en vue de cyber-sabotage", confirme à France 24 Laurent Heslault, spécialiste en sécurité de l'information chez Symantec. Duqu a été repéré dans les systèmes informatiques d'une poignée d'entreprises - dont les identités n'ont pas été révélées - sans qu'il soit encore possible d'expliquer comment leurs ordinateurs ont été infectés. Clé USB vérolée ? Mail piégé ? "Il est encore trop tôt pour le dire, car l'analyse de Duqu n'est pas encore complète. Nous avons une équipe qui travaille jour et nuit dessus", affirme Laurent Heslault.

Stuxnet - Duqu, même combat ?

Un point dont Symantec semble, en revanche, convaincu : derrière Duqu, se cachent les mêmes personnes qui ont mis au point Stuxnet. "Les deux codes [la conception du logiciel, NDLR] sont identiques à au moins 50%", assure Laurent Heslault. L'équipe qui s'en était pris au programme nucléaire iranien aurait donc repris du service. A l'époque, un haut gradé de l'armée israélienne s'était vanté de la participation de Tsahal à l'élaboration du virus.

Pour d'autres, si ces similitudes sont bien un indice, elles n'en constituent pas pour autant une preuve. Des cybercriminels auraient pu se procurer le code sur Internet "où il circule depuis quelque temps", nuance Marco Gercke, directeur de l'Institut de recherche en cybercriminalité de Hanovre. Qui estime aussi qu'il est trop tôt pour conclure à la préparation d'un "Stuxnet, acte II".

"Le monde de la cybercriminalité est devenu beaucoup plus professionnel, ces dernières années. Les opérations très ciblées comme celles menées grâce à Duqu sont plus fréquentes", conclut-il, laissant entendre que les attaques comme celle de Stuxnet ne sont pas les seules à atteindre un tel degré de sophistication.

Post-scriptum :

http://www.france24.com/fr/20111019...