L'Iran reconnaît avoir été ciblé par un virus à tête chercheuse

- Informatique - Sécurité Informatique -

Date de mise en ligne : lundi 27 septembre 2010

Spyworld Actu

Les autorités iraniennes ont reconnu que 30 000 ordinateurs avaient été infectés par le virus Stuxnet. Un aveu confortant l'avis de ceux qui affirment que ce virus cible en priorité les installations sensibles iraniennes.

Le nouvel ennemi de Téhéran s'appelle Stuxnet. Les autorités iraniennes ont reconnu avoir un gros problème avec ce virus informatique. Mahmoud Liayi, responsable des technologies de l'information au ministère de l'Industrie, a précisé que 30 000 ordinateurs sur le sol iranien ont été infectés. Il a précisé, cependant, qu'"aucun dégât sérieux" n'avait été constaté et que la centrale nucléaire de Bouchehr, l'une des plus connues en Iran, aurait été epargnée.

Reste que c'est la première fois que les autorités iraniennes confirment la menace Stuxnet sur leurs installations industrielles. Jusqu'à présent, seuls des experts occidentaux affirmaient que ce virus visait particulièrement l'Iran. Tous s'accordent, en tout cas, sur son potentiel particulièrement destructeur et qu'il soit "l'un des virus les plus élaborés" jamais observés.

Bombe informatique

Contrairement à l'immense majorité des logiciels malveillants, ce virus cible spécifiquement les installations informatiques de complexes industriels et peut permettre de les neutraliser. Stuxnet exploite plusieurs failles informatiques pour s'infiltrer dans des ordinateurs équipés de logiciels développés par Siemens. Les programmes du groupe allemand sont intégrés dans plusieurs installations "sensibles" en Iran.

Ce virus avait une première fois effrayé les experts en informatique lors de sa découverte en juin dernier. C'est la petite boîte de sécurité biélorusse VirusBlokAda qui, la première, a décelé l'existence de Stuxnet. La complexité de cette bombe informatique et la parfaite connaissance des programmes que le virus cherche à infecter (il connait notamment le mot de passe du logiciel Siemens visé) exclut, selon les chercheurs qui l'ont analysé, l'hypothèse d'un hacker du dimanche.

Selon la société américaine de sécurité Symantec, l'origine du virus serait davantage à chercher du côté de groupes aux "motivations politiques, nationalistes ou religieuses" ou alors à de "l'espionnage d'État". Bref, ce logiciel malveillant a nécessité toute une équipe d'experts pour voir le jour. Des experts qui chercheraient à ralentir ou réduire à néant le programme nucléaire iranien ?

Natanz plutôt que Bouchehr ?

Des officiels iraniens ont évoqué, dans la presse, "une guerre électronique" menée contre leur pays. Mais, lors des premières semaines d'activité, Stuxnet a essentiellement frappé en Inde et en Indonésie avec près de 60 000 ordinateurs touchés. L'Iran n'arrivait alors qu'en troisième position. Il semblerait, aujourd'hui, que l'Inde et l'Indonésie ne sont que des victimes collatérales de l'attaque.

Un chercheur allemand, Frank Rieger a même suggéré que ce virus n'avait en fait qu'une seule réelle cible : la site nucléaire de Natanz. Il estime que la centrale de Bouchehr, dont Siemens a contribué à la construction avant la révolution islamique, n'était qu'une passerelle. "La centrale de Bouchehr ne sert qu'au nucléaire civil alors que celle de Natanz peut avoir des applications militaires", raconte-t-il au site spécialisé dans les nouvelles technologies Wired . Il rajoute que Natanz pourrait être infectée à partir de la centrale de Bouchehr.

Une hypothèse pour l'instant impossible à vérifier, puisque les autorités iraniennes n'ont évoqué que le cas de Bouchehr. Cependant en juillet dernier, alors que Stuxnet était déjà en activité, la presse iranienne et la BBC ont rapporté que le chef de l'Organisation atomique iranienne avait démissionné tandis que WikiLeaks expliquait qu'un "incident majeur" avait eu lieu sur ce site.

Post-scriptum :

http://www.france24.com/fr/20100927...