



UN NOUVEAU VIRUS INFORMATIQUE CIBLANT L'IRAN EST CAPABLE D'IMMOBILISER DES OLÉODUCS, DES CENTRALES ÉLECTRIQUES ET DES CENTRALES NUCLÉAIRES

Un nouveau virus informatique, appelé Stuxnet, s'immisce dans les infrastructures de contrôle d'usines et de centrales nucléaires. Si son origine et sa façon de se propager restent encore très floues, sa cible est clairement définie : l'Iran, et plus particulièrement les infrastructures du pays. Stuxnet peut immobiliser des oléoducs, des centrales électriques et d'autres installations contrôlées par ces automates et provoquer une catastrophe en commandant des valves ou en faussant l'affichage des capteurs de pression et de température.

Selon Symantec, sur les 10.000 ordinateurs infectés, près de 60% ont en effet été détectés en Iran. Sur le même sujet, le PDG de Kaspersky, un logiciel anti-virus, explique « qu'une attaque de ce type ne peut être conduite qu'avec le soutien et le financement d'un Etat ». De là à soupçonner l'état hébreu, il n'y a qu'un pas. Israël a-t-il lancé le premier cyber-missile de l'histoire ?

Reuter en septembre dernier avait annoncé qu'Israël était en train de développer des capacités de cyber-guerre qui pourraient s'attaquer aux systèmes de contrôle militaires et industriels du pays », ce qui est justement le cas... Plus récemment, le 23 septembre, le Guardian franchit ce pas en expliquant quelques raisons qui pourraient laisser penser qu'Israël est derrière ce virus informatique, en particulier que cela lui ferait regagner en dissuasion, parce que c'est une véritable arme contre l'Iran, mais enfin parce qu'il est beaucoup plus facile de se protéger des cyber attaques lorsque l'on est un petit pays que lorsqu'on est un grand pays. [Pour retrouver cet article](#)

Un article du Figaro explique le fonctionnement du virus : dans le détail, Stuxnet s'attaque

d'abord à des postes fonctionnant sous Windows en se déployant depuis des clés USB grâce à des failles «zero day», qui n'ont pas encore été identifiées. Il parcourt ensuite le réseau local à la recherche d'un logiciel très précis, conçu par Siemens. Une fois installé, il reprogramme un composant – l'automate de programme industriel – et envoie de nouvelles instructions aux machines. Il sait ensuite échapper à la vigilance des administrateurs et se mettre à jour grâce à un module «peer-to-peer», qui vient télécharger les fichiers sur les machines disposant de la toute dernière version. israelvalley