Le ver Stuxnet au service du terrorisme?

Le ver Stuxnet, considéré comme très sophistiqué, passe du stade de l'espionnage industriel à la menace terroriste. Ainsi, la communauté des experts en sécurité IT émet une alerte à propos de ce *malware*, qui peut se propager depuis une simple clé USB.

Découvert en juin 2010, l'agent malveillant exploite une vulnérabilité dans Windows Shell et lui permettrait de détecter dans les ordinateurs infectés des applications industrielles du groupe Siemens (produits WinCC-PCS7), contrôlant des sites stratégiques comme les oléoducs ou les centrales électriques (systèmes SCADA).

Dans son édition de vendredi, le *Financial Times* illustrait la menace Stuxnet en prenant le cas d'une installation nucléaire iranienne susceptible d'être visée. L'article se veut alarmiste: on ne parle pas seulement de paralysie d'un système informatique mais de destruction physique des installations.

Selon Symantec, ce malware serait actif en Iran mais aussi en Indonésie, en Inde et au Pakistan. Une zone géostratégique considérée comme conflictuelle… De son côté, Siemens a reconnu qu'il a identifié 15 clients infectés. Mais *« il n'y a eu en aucun cas de conséquences sur leur production »* et un correctif a été diffusé, selon l'AFP.

Selon ESET Virus Lab, *« le ver Stuxnet ne pose pas plus de problèmes sur les ordinateurs des particuliers que les menaces traditionnelles rencontrées généralement sur les postes de travail »*. Le danger résiderait dans la vulnérabilité de la plate-forme Windows liée aux processus lancés par des fichiers .LNK, corrigée par Microsoft. Une faille sensible qui pourrait être exploitée par des malwares encore plus virulents.