SÃ©curitÃ© : W32.Stuxnet a dÃ©jÃ infestÃ© plus de 14 000 IP
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 28/7/2010 0:00:00

Lâ□□Ã©quipe **Security Response chez Symantec** a dÃ©couvert que **W32.Stuxnet** a dÃ©jÃ infestÃ© plus de 14 000 adresses IP en seulement 72 heures, dont la plupart en Iran, pour accÃ©der Ã des informations sensibles et notamment aux systÃ¨mes SCADA, qui pilotent les technologies industrielles dans des domaines tels que lâ□□eau, lâ□□Ã©lectricitÃ©, le pÃ©trole ou encore les substances chimiques.

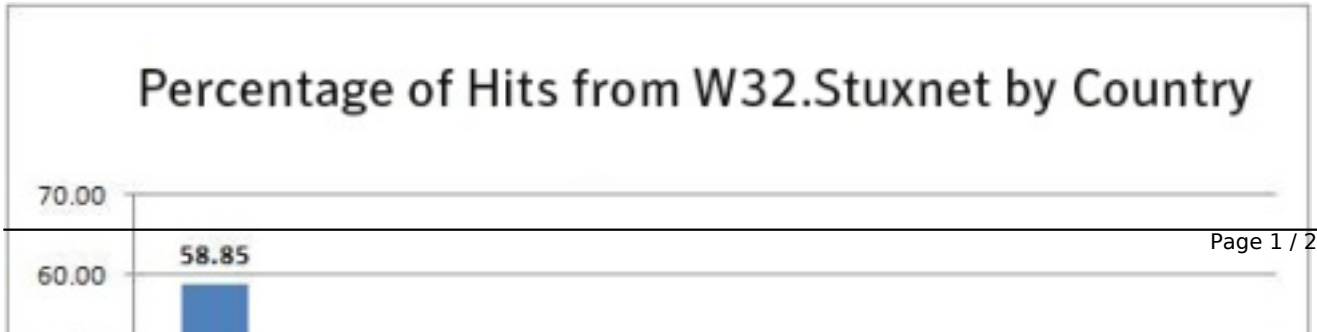
Suite Ã la dÃ©tection de la menace **W32.Stuxnet** la semaine derniÃ¨re, **Symantec** continue Ã lâ□□analyser afin dâ□□identifier la faÃ§on dont elle exploite les vulnÃ©rabilitÃ©s, sa cible, ainsi que son objectif.

Elle est particuliÃ¨rement dangereuse puisquâ□□elle peut dissimuler sa prÃ©sence grÃ¢ce Ã un systÃ¨me rootkit ainsi quâ□□en exploitant une vulnÃ©rabilitÃ© zero-day qui concerne toutes les versions Windows. Elle cible des logiciels utilisÃ©s pour contrÃ´ler des processus industriels SCADA, et dÃ©montre une profonde connaissance de ces outils.

Cette menace rÃ©agit Ã deux niveaux :

De faÃ§on automatique, comme la plupart des virus, mais Ã©galement commandÃ© Ã distance.

Le virus a Ã©tÃ© dÃ©tectÃ© sur un serveur en Malaisie, mais la localisation dâ□□une machine ne donne aucune information sur lâ□□origine de lâ□□attaque ni de lâ□□attaquant. Symantec a pu rapidement prendre le contrÃ´le en dÃ©routant et bloquant le trafic vers ce serveur afin dâ□□empÃªcher de contrÃ´ler les machines infectÃ©es et rÃ©cupÃ©rer les informations.



Comme souligne **Laurent Heslault**, Directeur des Technologies de SÃ©curitÃ© chez Symantec, sur son blog:

â¢ - Symantec ne connaÃ®t pas la/les personnes derriÃ¨re cette attaque..

â¢ - Si lâarchitecture de lâattaque se dessine (technologies, cibles, gÃ©ographieâ¦), la motivation reste trÃ¨s floue.

â¢ - Il est clair quâils sont loin dâÃªtre des amateurs.

Pour plus dâinformations concernant sur W32.Temphid