

Sécurité : le 'trojan' Pushdo mène la danse

Le trojan Pushdo.EV se hisse à la première place du « Top Ten ». Ce « canasson » malveillant s'est hissé en tête du classement en envoyant des cartes postales animées laissant espérer à leurs victimes qu'un simple clic leur permettrait de consulter des photos pornographiques.

« L'activité du mois dernier montre l'efficacité du réseau botnet de Pushdo : un signe évident que les techniques d'ingénierie sociale reposant sur l'envoi en masse de cartes postales électroniques ont encore la cote », déclare Guillaume Lovet, responsable de l'équipe anti-menaces chez Fortinet.

« Les internautes doivent être conscients du fait que les cartes postales électroniques légitimes ne sont généralement pas envoyées sous forme de pièces jointes, mais plutôt accessibles sous forme de lien renvoyant sur un site Web les hébergeant. En règle générale, il faut toujours éviter d'ouvrir des pièces jointes provenant de courriels non sollicités. »

Les équipes de recherche de Fortinet, ont ainsi observé un pic d'activité quatre dimanches de suite (ndlr : de fin février à fin mars), propulsant ainsi les différentes variantes de Pushdo dans le top 10 des menaces les plus répandues.

Il représente à lui seul **13,5%** du volume d'activités malveillantes du mois de mars. Conséquence de cette prolifération, il permet à la famille des chevaux de Troie de totaliser presque un tiers (32,2%) du nombre total de menaces observées.

La famille Netsky maintient son leadership face aux autres familles de malwares avec 14.5%. Mais, « la concurrence est rude », notamment face aux variantes de Pushdo qui représentent désormais un volume inférieur d'à peine un point (13.7%) à celui de la famille Netsky.

Enfin, les familles MyTob et MyDoom maintiennent un niveau d'activité constant, avec 4 variantes parmi les 10 menaces les plus répandues sur Internet.