

Alerte 'malware': Spamta propage une double attaque combinée

Selon PandaLabs, cette attaque combinée représente déjà 80% des malwares détectés par l'éditeur. L'offensive est donc massive.

Comment s'effectue l'attaque ? Lorsque le ver **Spamta.VK** infecte un ordinateur, il se connecte à plusieurs serveurs afin d'envoyer des emails en masse. Ces emails contiennent une copie du cheval de Troie **SpamtaLoad.DT**, généralement dans un fichier exécutable. Quand il infecte un ordinateur, SpamtaLoad.DT télécharge à son tour une copie du ver Spamta.VK, recommençant ainsi le cycle d'infection. Un véritable cercle vertueux du piratage ! Le cheval de Troie SpamtaLoad.DT affiche une icône semblable à celle d'un fichier texte. Lorsqu'il est exécuté, SpamtaLoad.DT affiche un message d'erreur et crée une entrée dans la base de registre Windows afin de s'assurer de toujours être lancé à chaque démarrage de l'ordinateur.

« Il s'agit d'un exemple typique d'attaque combinée. Les capacités de propagation du ver sont utilisées pour distribuer le cheval de Troie qui, à son tour, assure la prolifération du ver en infectant chaque nouvel ordinateur avec une copie de ce dernier. Cette stratégie explique le grand nombre d'infections détectées par PandaLabs. », indique Luis Corrons, le directeur technique de PandaLabs.

L'offensive de Spamta n'est pas prête de s'arrêter, PandaLabs estime probable l'apparition de nouvelles variantes au cours des prochaines heures.