Le ver Storm se trouve un remplaçant, Nugache

Nugache, un ver qui vient d'apparaître, va vraisemblablement être encore plus nuisible que Storm. Il a en effet la capacité, de rendre inefficaces tous les systèmes de sécurité qui reposent sur des bases de signatures.

Ce code malveillant s'appuie sur le chiffrement d'échanges choisis au hasard pour contourner les défenses basées sur des signatures. Il utilise les échanges en Peer-to-Peer ou P2P, sans avoir recours à un quelconque serveur de contrôle de commande (C&C).

Une fonction qui lui permet de rester dans l'ombre et de devenir indétectable. Cette fonctionnalité rend invisibles les échanges entre les « bots » individuels et leur serveur de contrôle de commande tout en fournissant un nouveau niveau de résilience pour le réseau de « bots ».

Nugache exploite les carences des systèmes de protection actuels suivantes : l'absence de scan anti-malware, l'utilisation des catégories de filtres URL d'ancienne génération…

Mais aussi le système de connexion par défaut des utilisateurs, qui aboutit à des connexions à Internet non vérifiées, le manque de contrôle granulaire des applications.

Il exploite également l'utilisation des signatures dans un modèle de sécurité « négatif », qui ne bloque que le trafic s'appuyant sur des signatures identifiées comme nocives

En 2007, Storm a fait figure de l'une des menaces les plus dangereuses sur Internet. En ce début 2008, Nugache émerge en s'appuyant sur des fonctionnalités techniques similaires qui ont permis à Storm de se répandre très rapidement, et ce, en contournant les systèmes de défense courants.

Pour Secure Computing à l'origine de cette découverte, *« en adoptant ces mêmes caractéristiques techniques, Nugache pourrait très vite devenir une menace aussi sérieuse, voire plus dangereuse. »*