Spamta, le ver qui se multiplie, se multiplie?

Rarement une menace ne se sera démultipliée à un rythme aussi soutenu? Ce sont à ce jour plus d'une centaine de versions du ver Spamta qui ont été découvertes par les chercheurs de Panda, au sein de leurs « laboratoires » de solutions antivirus Panda Software.

Deux approches mafieuses s'affrontent aujourd'hui : si la tendance est de cibler les menaces afin d'optimiser les résultats ? mieux vaut un 'client' bien ciselé qu'une multitude de cibles aléatoires ! ?, certains auteurs de menaces virales continuent de jouer la carte du volume afin de décupler la probabilité d'infecter un ordinateur.

Avec un rythme exponentiel de lancement de nouvelles variantes – 67 découvertes par les PandaLabs en 7 jours ! – les auteurs de Spamta ont choisi cette seconde approche, l'**attaque en masse**.

Les variantes de Spamta en circulation sont très similaires. Les seules différences se situent au niveau de la taille du ver, du message utilisé comme appât, du format de compression contenant le ver ou encore des fichiers qui y sont copiés.

La variante CY, par exemple, ouvre Notepad, qui affiche une série de caractères difformes, tandis que la variante FQ ouvre une boîte de dialogue annonçant que la mise à jour d'un programme a été effectuée avec succès…

En revanche, les experts de Panda s'interrogent sur les motivations de l'auteur (ou des auteurs) de Spamta, peu évidentes car ces codes malicieux semblent être typiquement des vers prévus pour se propager d'eux-mêmes vers le plus d'adresses possible.

?*Ces nouvelles variantes ne suivent apparemment pas la nouvelle dynamique des malwares, dont le but pour les créateurs des menaces est de générer de l'argent facile. Nous pensons que ce sont des tests menés dans le but de trouver un code malicieux qui puisse se propager le plus vite possible vers de très nombreuses adresses pour ensuite le modifier en y intégrant de nouvelles fonctionnalités, lui permettant de mener d'autres actions beaucoup plus dangereuses*?, explique Luis Corrons, directeur de PandaLabs.

On devrait sonc encore entendre parler de Spamta, ou d'une autre menace plus sérieuse encore qui prendra sa place en exploitant son code le plus pertinent pour attirer l'attention de l'internaute naif.