Un nouveau ver se répand à travers MSN Messenger

Les messageries instantanées sont devenues en quelques mois, le vecteur privilégié d'attaques. Selon Postini, le trafic sur ces applications a augmenté de 138 % en mai. Mais dans le même temps, les attaques ont progressé de 500 %!

AOL Instant Messaenger (AIM) est de loin la principale victime de cette recrudescence, et regroupe à lui seul la majorité des nouvelles attaques détectées. Mais ses concurrents ne sont pas en reste. Ainsi l'éditeur PandaLabs alerte les 200 millions d'utilisateurs de MSN Messenger (Live Messenger) qui serait victime de la propagation d'une nouvelle variante du ver BlackAngel.B. Afin de se propager, le malware envoie des messages à toutes les personnes de la liste des contacts MSN de l'utilisateur et envoie une copie de lui-même, présentée comme étant une vidéo du nom de 'Fantasma' (fantôme). Si le destinataire ouvre le fichier, une image s'affiche à l'écran avec un texte en espagnol : ?En el 1er día te espantas, en el 2º te desesperas, en el 3º buscas ayuda y en el 4º mueres? (le 1er jour tu es effrayé, le 2ème jour désespéré, le 3ème jour tu cherches de l'aide et le 4ème tu meurs), explique l'éditeur dans un communiqué. Lorsque le fichier est exécuté, le code malveillant BlackAngel.B effectue plusieurs modifications dans le système. Il ferme notamment plusieurs programmes de sécurité (logiciels antivirus, firewalls, etc.) afin de ne pas être détecté. Il tente également de fermer certaines fenêtres (gestionnaire des tâches Windows, panneau de configuration, éditeur de base de registres, utilitaire de configuration système, outil de restauration du système) dans le but d'empêcher sa victime d'utiliser les outils de configuration du système d'exploitation. Enfin, pour se diffuser à tous les contacts enregistrés dans MSN Messenger, le ver bloque une fenêtre de l'application et empêche l'utilisateur d'y accéder. Depuis cette fenêtre, il entame une conversation avec les contacts, au cours de laquelle il envoie des messages tels que « jaja look a that » ou « mira este video » et donne une adresse web depuis laquelle le ver est téléchargé pour infecter l'ordinateur. Les attaques contre les messageries instantanées devraient continuer à progresser grâce au rapprochement des protocoles des messageries de Yahoo et MSN. A terme, les codes malveillants seront donc multiplates-formes, multipliant ainsi les dégâts.