BitDefender : La messagerie instantanÃ©e en danger
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 5/5/2010 0:00:00

Un ver extrÃªmement agressif assaille les messageries instantanÃ©es. Une nouvelle variante du ver Palevo attaque les systÃ¨mes non protÃ©gÃ©s avec de faux liens vers des galeries de photos.

Le dernier-nÃ© de la famille Palevo se diffuse ces jours-ci sous la forme dâ□□une vague massive de spam de messagerie instantanÃ©e, gÃ©nÃ©rÃ©e de faÃ§on automatique. Le message non sollicitÃ© incite les destinataires Ã cliquer sur un lien accompagnÃ© dâ□□un smiley souriant, censÃ© les diriger vers une image ou une galerie de photos.

Le message de spam reÃ§u via messagerie instantanÃ©e diffusant Palevo

Au lieu dâ□□ouvrir ce qui est censÃ© Ãªtre une galerie dâ□□images, les utilisateurs sont invitÃ©s Ã enregistrer un faux fichier JPG, qui est en fait un exÃ©cutable contenant la charge utile malveillante Worm.P2P.Palevo.DP.

Le faux fichier .JPG est en fait un fichier .EXE diffusant le ver

Palevo.DP est synonyme de ravage pour les systÃ¨mes non protÃ©gÃ©s qui sont infectÃ©s. Il commence par crÃ©er plusieurs fichiers cachÃ©s dans le dossier Windows : mds.sys, mdt.sys, winbrd.jpg, infocard.exe et modifie certaines clÃ©s de registre pour quâ□□elles pointent vers ces fichiers afin de neutraliser le pare-feu du systÃ¨me dâ□□exploitation.

Comme les autres membres de sa famille, Palevo.DP dispose dâ□□un composant de type backdoor qui permet aux attaquants de prendre Ã distance le contrÃ´le total de lâ□□ordinateur compromis pour y installer dâ□□autres malwares, voler des fichiers, lancer des campagnes de spam et des attaques de malwares sur dâ□□autres systÃ¨mes.

La famille Palevo est Ã©galement capable dâ□□intercepter des mots de passe et dâ□□autres donnÃ©es sensibles saisies dans les navigateurs web MozillaÂ® FirefoxÂ® et MicrosoftÂ® Internet ExplorerÂ®, ce qui la rend extrÃªmement dangereuse pour les internautes utilisant des services bancaires en ligne ou faisant des achats sur Internet.

Le mÃ©canisme de diffusion comprend Ã©galement lâ□□infection de partages rÃ©seau et de supports de stockage amovibles comme les clÃ©s USB, dans lesquels il crÃ©e des fichiers autorun.inf pointant vers sa copie. Lorsquâ□□un disque amovible ou une carte mÃ©moire sont insÃ©rÃ©s dans des ordinateurs dont la fonction dâ□□exÃ©cution automatique (autorun) est activÃ©e ou qui ne sont pas protÃ©gÃ©s par une solution de sÃ©curitÃ© avec analyse Ã lâ□□accÃ¨s, le systÃ¨me est automatiquement infectÃ©.

Les vers Palevo affectent Ã©galement les utilisateurs de plateformes de partage P2P telles quâ□□Ares, BearShare, iMesh, Shareza, Kazaa, DC++, eMule et LimeWire, en ajoutant leur code aux fichiers partagÃ©s.

Â« *Nous recommandons aux utilisateurs dâ□□Ãªtre extrÃªmement prudents et de ne cliquer sur aucun lien reÃ§u via des clients de messagerie instantanÃ©e sans avoir vÃ©rifiÃ© auprÃ¨s de lâ□□expÃ©diteur la validitÃ© des sites Web vers lesquels ces liens pointent. Cette offensive du ver Palevo est extrÃªmement agressive et nous avons assistÃ© au dÃ©but de cette attaque Ã des taux dâ□□infection dÃ©passant largement les 500% par heure pour des pays comme la Roumanie, la Mongolie ou lâ□□IndonÃ©sie* Â». dÃ©clare **Catalin Cosoi**, Chercheur des Laboratoires BitDefender.

Pour plus dâ□□informations concernant les produits BitDefender.