Saint Valentin : avec les Love Bots, la croisière ne s'amuse pas toujours !

PC Tools met en garde les internautes contre les « Flirt Bot », ces robots qui rôdent sur certaines messageries instantanées à la recherche des âmes esseulées

Paris, le 10 février 2010 - Pas de répit pour la Saint Valentin et ceux qui cherchent le grand amour sur Internet : le fournisseur de logiciel de sécurité PC Tools (www.pctools.com) met en garde les internautes contre un nouveau robot en ligne de type « botnet ». Ce robot « Flirt Bot » s'attaque aux personnes qui flirtent via les messageries instantanées.

PC Tools a obtenu une copie d'une conversation MSN d'une victime baptisée "Marie" (la victime ne veut pas révéler son identité) où le « Flirt Bot » s'est mis en relation avec elle sur son compte MSN privé. Ces « Flirt Bots », identifiés par PC Tools dès 2007 comme faille logicielle, sont désormais une réalité. Ils présentent un risque réel pour les internautes car ils sont conçus pour piéger les utilisateurs en les faisant cliquer sur des sites Web infectés ou pour voler leur identité et leurs coordonnées bancaires.

Voici la façon dont les Flirt Bots procèdent:

- Le Flirt Bot s'introduit dans une « chatroom » et entame une conversation avec un utilisateur.

- Les bots utilisent une série de scénarios et de dialogues facilement adaptables avec des questions et de sujets de discussion préprogrammés pour établir un rapport précis sur chaque personne qu'ils rencontrent.

  Exemple: ernestineholom553@hotmail.com dit: "Salut ça va?"

- Les victimes sont alors invitées à se rendre sur un site Web qui pourrait être utilisé pour différents types d'activités malveillantes

  Exemple: ernestineholom553@hotmail.com dit: «Clique sur http://twurl.nl/meec1n et accepte l'invitation sur la page, chéri!"

- Dans ce cas, la victime est envoyée sur un site web "mywebcamcrush.com" et doit fournir des informations personnelles comme ses coordonnées bancaires afin d'afficher la « webcam »

- Le site peut être utilisé pour beaucoup de choses : héberger des malwares, des téléchargements à risque, ou essayer de vendre de faux anti-virus (Fake AV).

  Par exemple, les cybercriminels créent souvent une base de données remplies d'informations personnelles et la vendent au plus offrant.