BitDefender met en garde les amoureux pour la Saint-Valentin
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 11/2/2009 15:00:00

La flÃ¨che de Cupidon pourrait envoyer des e-menaces
Ã l'approche de la Saint-Valentin, BitDefenderÂ® met en garde les utilisateurs d'Internet : la flÃ¨che de Cupidon pourrait apporter plus que de tendres sentiments dans vos boÃ®tes de rÃ©ception. Elle pourrait en effet apporter diffÃ©rentes formes d'e-menaces capables d'infecter votre ordinateur, ou pire encore.

Les Laboratoires BitDefender conseillent aux internautes de se montrer particuliÃ¨rement mÃ©fiants envers les messages ayant pour thÃ¨me la Saint-Valentin et de ne pas ouvrir les e-mails suspects provenant d'expÃ©diteurs inconnus.

Â

Les crÃ©ateurs de virus sont connus pour lancer des attaques autour de fÃªtes populaires comme NoÃ«l, le Nouvel An et la Saint-Valentin. Le tristement cÃ©lÃ¨bre Â« **Storm Worm** Â» a infectÃ© les systÃ¨mes de millions d'internautes en fÃ©vrier 2008 en leur promettant un cadeau de la

Saint-Valentin. L'e-mail contenait un lien qui dirigeait les utilisateurs vers un site Internet oÃ¹ ils devaient en thÃ©orie tÃ©lÃ©charger une carte de Saint-Valentin.

Au lieu de recevoir une carte d'une personne chÃ¨re, leur systÃ¨me Ã©tait infectÃ© par Storm Worm et leurs informations personnelles Ã©taient volÃ©es.

Afin d'Ã©viter une infection similaire pour la Saint-Valentin 2009, il est recommandÃ© que les utilisateurs Ã©vitent d'ouvrir des e-mails ayant pour sujet des cadeaux de la Saint-Valentin, comme des pilules augmentant le plaisir, des copies de bijoux, des sacs et des montres de crÃ©ateurs. Ces e-mails sont susceptibles de contenir des piÃ¨ces jointes ou des liens vers d'autres sites pouvant infecter les ordinateurs des utilisateurs.

BitDefender met en garde les internautes contre le danger d'ouvrir des e-mails ayant pour sujet Â« **I Love Being in Love With You** Â». Cet e-mail contient un lien malicieux : si l'utilisateur clique dessus, son ordinateur sera infectÃ© via le botnet Waledac qui fonctionne d'une maniÃ¨re similaire Ã Storm Worm. Il infecte les utilisateurs via de fausses cartes de vÅux.

D'autres vagues de spam sur le sujet de la Saint Valentin ont Ã©tÃ© dÃ©tectÃ©es par les Laboratoires BitDefender, ils comprennent des messages non sollicitÃ©s provenant de pharmacies en ligne, de sites Internet et boutiques pour adultes, ainsi que de casinos en ligne.

Â

Vlad Valceanu, Directeur de la recherche anti-spam de BitDefender, explique que :

Â« ***la Saint-Valentin est un moment idÃ©al pour les crÃ©ateurs de malware qui trompent les utilisateurs peu mÃ©fiants en leur faisant ouvrir des piÃ¨ces jointes ou en les faisant cliquer sur des liens dans des e-mails romantiques. Â» Â« Les utilisateurs doivent Ãªtre prudents lorsqu'ils cliquent sur des URL pendant les pÃ©riodes de fÃªtes, car, ils ne tarderont pas Ã s'en rendre compte, leurs boÃ®tes de rÃ©ception sont inondÃ©es de spam ciblÃ© Ã ce moment-lÃ*** Â».

Quelques conseils supplÃ©mentaires permettent d'assurer la sÃ©curitÃ© de vos donnÃ©es personnelles, quelle que soit la pÃ©riode de l'annÃ©e :

- N'ouvrez pas les e-mails provenant de sources inconnues ou non fiables. De nombreux virus se diffusent par e-mail, mieux vaut donc demander une confirmation de la part de l'expÃ©diteur en cas de doute.
- N'ouvrez pas les piÃ¨ces jointes de messages contenant des sujets suspects ou inattendus. Si vous souhaitez les ouvrir, commencez par les copier sur votre disque dur et analysez-les avec un programme antivirus Ã jour.
- Supprimez tous les e-mails de chaÃ®nes et les messages non dÃ©sirÃ©s. Ne les transfÃ©rez pas et ne rÃ©pondez pas Ã leurs expÃ©diteurs. Ces types de messages sont considÃ©rÃ©s comme du spam parce qu'ils sont non sollicitÃ©s et surchargent le trafic Internet.
- Mettez Ã jour votre systÃ¨me et vos applications aussi souvent que possible. Certains systÃ¨mes d'exploitation et certaines applications peuvent Ãªtre mis Ã jour automatiquement. Profitez de cette possibilitÃ©. Ne pas installer les correctifs disponibles pour votre systÃ¨me peut le rendre vulnÃ©rable Ã des menaces pour lesquelles il existe dÃ©jÃ des solutions.
- Ne copiez aucun fichier si vous ne connaissez pas sa source ou considÃ©rez qu'elle n'est pas digne de confiance. VÃ©rifiez la source des fichiers que vous tÃ©lÃ©chargez et assurez-vous qu'un programme antivirus a analysÃ© les fichiers Ã leur source.

BitDefender recommande Ã©galement (en plus du fait de ne pas cliquer sur des liens douteux) d'utiliser une solution de sÃ©curitÃ© intÃ©grÃ©e comprenant un antivirus, un antispam et un pare-feu mais Ã©galement des fonctionnalitÃ©s avancÃ©es telles que le filtrage des sites web et la

protection d'identitÃ©.
Â

Visitez le site de BitDefender