Internet : G-Data, Poker en ligne DÃ©jouer les piÃ¨ges
Internet
PostÃ© par : JPilo
PubliÃ©e le : 9/8/2010 0:00:00

Le poker en ligne est un jeu trÃ¨s Ã la mode. En dix ans, le poker est passÃ© du loisir privÃ© rÃ©servÃ© Ã quelques passionnÃ©s Ã un phÃ©nomÃ¨ne de masse pouvant gÃ©nÃ©rer des concours de grandes envergures, relayÃ©s par de vÃ©ritables shows tÃ©lÃ©visÃ©s. Une popularitÃ© qui dÃ©passe les frontiÃ¨res des pays. Ainsi, dans le monde entier le poker en ligne alimente une industrie qui gÃ©nÃ¨re des milliards. Pas Ã©tonnant que ce jeu attire l'attention des cybercriminelsâ¦

Pour contrer les risques, les grands sites de poker en ligne ont adoptÃ© des mesures de sÃ©curitÃ©s efficaces afin de garantir Ã leurs utilisateurs une plate-forme de jeu sÃ©curisÃ©e. Malheureusement, cette garantie est loin dâ□□Ãªtre rÃ©unie lorsquâ□□il sâ□□agit des ordinateurs de la plupart des utilisateurs. Ceux-ci forment le point faible dans cette chaÃ®ne sÃ©curitaire et peuvent Ãªtre la cible des cybercriminels.



Les scÃ©narios dâ□□attaques possibles

1. Une des mÃ©thodes les plus communes employÃ©es par des cybercriminels est lâ□□envoi dâ□□un courrier Ã©lectronique offrant un crÃ©dit important (souvent des centaines dâ□□euros) Ã dÃ©penser sur un casino en ligne. Lâ□□utilisateur est alors invitÃ© Ã visiter un faux site de jeu en ligne et Ã y laisser ses coordonnÃ©es bancaires pour recevoir cette dotation.

2. Une autre mÃ©thode basÃ©e sur le spam consiste Ã alerter lâ□□internaute dâ□□un problÃ¨me sur son compte de jeu en ligne. Il est alors invitÃ© Ã visiter une page Internet falsifiÃ©e et a y entrer ses donnÃ©es personnelles pour validation. Le cybercriminel en possession de ces codes peut transfÃ©rer lâ□□argent contenu sur le compte.

3. Les cybercriminels emploient Ã©galement les spywares et les chevaux de Troie pour obtenir les mots de passe des utilisateurs dâ□□ordinateurs infectÃ©s. Le programme nuisible est capable de se rÃ©veiller seulement lorsque lâ□□utilisateur se connecte sur un site de jeu en ligne. Certains sont aussi capables de rechercher ces donnÃ©es de connexion dans les

fichiers de lâ□□ordinateur.

4. Une autre mÃ©thode basÃ©e sur lâ□□arnaque est aussi utilisÃ©e . Sur Internet, il est

possible de trouver des propositions de logiciels spÃ©ciaux qui, par exemple, permettent Ã un joueur de voir les cartes de leurs adversaires. Ces faux logiciels peuvent avoir plusieurs buts. Lâ□□internaute achÃ¨te un faux logiciel avec de l'argent bien rÃ©el. Ou la carte de crÃ©dit est utilisÃ©e pour des transactions frauduleuses. Ou encore le logiciel achetÃ© contient des programmes nuisibles.

Faire face aux dangers

Pour se protÃ©ger de cette sÃ©rie de dangers, il est conseillÃ© dâ□□appliquer **quelques mesures de sÃ©curitÃ© et de bon se**ns :

- Installer une suite de sÃ©curitÃ© et la maintenir Ã jour.

- Maintenir Ã jour son systÃ¨me, son navigateur et ses applications.

- Effacer tout courrier contenant des offres d'argent ou des propositions de logiciels spÃ©ciaux et illÃ©gaux pour les casinos en ligne.

- Maintenir le pare-feu actif pendant les phases de jeux en ligne afin d'Ã©viter toute intrusion sur le PC et toute sortie de donnÃ©es non autorisÃ©e.

- Jouer en ligne, exclusivement sur des sites Internent ayant reÃ§u **lâ□□agrÃ©ment de l'ARJEL**, lâ□□autoritÃ© de rÃ©gulation des jeux en ligne.