

Online poker targeted by cyber criminals

May 16 2006

An online poker game is being targeted by identity-theft criminals, a Finnish computer-security company warned Tuesday.

Helsinki-based F-Secure said that rootkits -- software used by those who want to hide malicious software -- have been used on a gaming site called checkraised.com.

The back door, which is a method for securing illegal remote access to a computer, was created by silently dropping four executable files into the user's computer and using a rootkit driver to conceal the operation. With this in place, the tool's author could access login information from the user's computer for various online poker Web sites including Partypoker, Empirepoker, Eurobetpoker and Pokernow. Having gained access, the hacker could then play poker against himself, losing on purpose and reaping the rewards, F-Secure warned.

"Following the exponential rise of interest in online poker, it is inevitable that malware authors would follow suit with programs to separate players from their money. What is significant is the fact that this particular scam was hosted, albeit unwittingly on a legitimate site and used rootkit technology to cloak itself. Without our unique Blacklight technology to detect it, many online gamblers could have become victims of this exploit," Kimmo Kasslin, a researcher at F-Secure's data security laboratory, said in a news release.

Copyright 2006 by United Press International

Citation: Online poker targeted by cyber criminals (2006, May 16) retrieved 26 April 2024 from <https://phys.org/news/2006-05-online-poker-cyber-criminals.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.