

IT Backbones - Dedicated To IT Security Issues, Featuring News, Press Releases, IT Directory & Links



Finjan gives you protection that signature-based products **cannot even see**

Dedicated To IT Security Issues, Featuring News, Press Releases, IT Directory & Links

- [Home](#)
- [About](#)
- [Submit News](#)
- [Search News](#)
- [IT Events](#)
- [Time & Money](#)
- [European Media](#)

Trojan Steals Usernames And Passwords From Online Gamers

Published 13th November 2007

Online gamers, be on guard! A new Trojan named 'Win32.OnLineGames.dr' can rob your username and password of the game account, warn Security Experts at the AntiVirus, AntiSpam and Content Security provider MicroWorld Technologies...

'OnlineGames.dr' comes into computers via offers and help notes posted by crooks in game forums or by exploiting browser vulnerabilities. Written in Delphi language, 'OnlineGames.dr' injects its DLL component into running processes and places an 'autorun.inf' file in the root of each drive to ensure that it gets activated every time a drive is opened.

Once active, it snoops on user activity, steals confidential account information from unwitting victims and sends it to a remote attacker. In a few cases, the Trojan also posts this stolen information to certain malicious websites. With the username and password of a virtual game player in his hand, the Trojan writer can directly log on to the victim's account and sell off the characters and other goods for real world money.

This Trojan targets 'Massively Multiplayer Online Role-playing Games' (MMORPG), particularly the ones like Gamania and Wowtaiwan, meant for the Taiwanese audience. MMORPG is a genre of online computer role-playing games where a huge number of players interact with each other in a fantasy world. Every participant plays the role of a

fantasy character and buys and sells fictional goods online, while they also barter stuff among each other. On many websites you can buy goods and characters using actual currency and do vice versa.

“The magnitude of the online gaming economy is much bigger than what meets the eye,” points out Govind Rammurthy, CEO of MicroWorld Technologies. “The total amount of real world money connected to all gaming sites is close to half a billion dollars, and there you can see why malware writers are training their guns on virtual game players. Trojans are known for their direct or indirect financial motives and this breed is no different”.

Password stealing Trojan variants lurking in the web are many and their targets varied. While most of them eye credit card and banking information, some of them go after eBay or Paypal accounts. A good number of Trojans send the stolen information to its creator via email where as others connect to the attacker through ports.

“Malware targeting online game accounts has been in existence for a long time, but the stakes were never as high as they are now. To combat this menace, gaming companies need to come up with more sophisticated authentication procedures while users should deploy competent protection for their computers. Because when you are pitted against a cyber criminal, neither does he play by the rules of the game nor does he give you a second chance,” says Govind Rammurthy.

[Links](#) | [About Us](#) | [Privacy Policy](#) | © 2004-2007 IT Backbones Limited

Site developed and hosted by [Design Solution](#) Ltd.