



DAILY NEWS
OF THE
COMPUTER
GAME
INDUSTRY

HOME

[Home](#) [Reviews](#) [Interviews](#) [Editorials](#) [Subscription](#) [Contact Us](#) [Advertise](#) [GiNdex](#)



BEWARE: TROJAN STEALING ONLINE GAME ACCOUNTS

Posted: 11/13/2007

By: William Jackson

Special to GiN

Hackers, apparently hoping to tap into the growing real-world economy growing up around massively multiplayer online role-playing games, are distributing a Trojan that sniffs gamers' user names and passwords.

The antivirus company MicroWorld Technologies has identified a Trojan named Win32.OnLineGames.dr that is being disseminated through game forums and browser exploits. It places a file named autorun.inf in the root of each drive on the infected machine so that it will be activated when the drive is opened. It appears to gather game account information and send it to the attacker. The company reported that in some cases account information has been posted to malicious Web sites.

With log-on information an unauthorized user can access the victim's account and sell off characters and other assets. This is a variation on the more common practice of stealing bank and other financial account data, and games could be an increasingly attractive target as the real-world market place for digital goods grows, said MicroWorld CEO Govind Rammurthy.

"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," Rammurthy said.

The current Trojan appears to be targeting the games particularly the ones like Gamania and Wowtaiwan, meant for the Taiwanese audience.

As online games and virtual worlds grow in popularity and sophistication, so do the threats against them. Oliver Friedrichs, director of emerging technologies for Symantec Security Response, identified fraud in online worlds as one of the cyber threats to look out for in 2008.

In addition to outright theft of account information and assets, the market for digital goods also could provide a medium for laundering money, Friedrichs said. As the market matures and with no effective tracking of money exchanged in online accounts used by gamers, organized criminals participating in games could buy and exchange digital assets that could be sold for cash to hide the source of the money.

Rammurthy advised gaming companies to provide better authentication and access controls, and gamers to use antivirus protection, and keep it updated.

www.gameindustry.com

Copyright © 2007 Noble Order Press Enterprises Inc.

No part of this site may be used without the express written permission of the publisher.