



[SEARCH](#) [ANALYSIS](#) [ARCHIVE](#) | [PR](#)

KPMG ANALYSIS

Hackers, Cheaters Threaten Online Games' Business Model

March 3, 2005

By Dave Pelland, Managing Editor, Technology Insider

Operators of online multiplayer games are battling cheaters, hackers, and other miscreants who chase away legitimate players and increase support costs.

"When multiple players are competing in an online environment, many avenues exist to hack the game to the unfair advantage of the hacker," says Tony Ray, president of security software provider Even Balance Inc.

While piracy and hacking have long been problems for game and software publishers, multiplayer online games exacerbate the challenge. The most elaborate game services, such as Microsoft's Xbox Live or Sony's Everquest, can host thousands of players at once. Most require subscription fees that range between \$6 to about \$15 a month.

According to research firm Yankee Group, the global market for online games is expected to reach \$1.1 billion by 2008, a three-fold increase from 2004.

In addition to generating additional revenue, Steven Davis, chief executive of security firm IT Global Secure, says an online component to a game can increase its sales between 10 and 40 percent and extend its shelf life.

But game services are falling under attack from hackers and cheaters trying to avoid subscription costs, cheat, or harass and taunt fellow players in what is known as "griefing."

Graham Cluley, senior technology consultant for antivirus firm Sophos Inc., says hackers are stealing keys and registration information to either "stay alive" longer or give themselves more attributes within the game.

In late January, for instance, Sophos said a Trojan horse variant, LegMir-Y, was launched to steal user names and passwords from the multiplayer online game "Lineage."

So far, most of the gaming-related exploits haven't included stealing other types of personal information.

"A lot of these attacks are accomplished by capturing keystrokes of people visiting

MORE...

[Tech Firms Competing Models](#)

MARCH 9 The recording hoping that electronic sut services and music on ce take off.

[S-O Compliance Playin: Next M&A Wave](#)

FEBRUARY 23 Audit con finding out that Sarbanes given them yet another n responsibility -- more due mergers and acquisitions

[Compliance Promoting Management Growth](#)

FEBRUARY 16 Corporat regulations are driving sa enterprise content mana software.

[Food Companies Turn Tracking](#)

FEBRUARY 9 As food co to comply with laws fight terrorism, they've had to tracking operations.

[Data Center Heat Prom Solutions](#)

FEBRUARY 3 High temp blade servers have force to change room-cooling s

[Selected Technology C Earnings](#)

JANUARY 27 Mixed resu characterized the fourth c technology companies, w reporting flat or declining

['Ease-of-Use' Becomes Industry's Rallying Cry](#)

JANUARY 19 Instead of i cool but unwanted featur companies are trying to r products simpler to use.

gaming sites," Cluley says. "As far as online banking sites, we haven't that kind of cross-over yet, but [the effort in] doing so would be relatively trivial."

Also in January, Microsoft said "thousands" of players were expelled from the Xbox Live service for unsavory behavior including cheating and making offensive comments to other players.

Such behavior dilutes the community aspect that the games depend on for growth, Davis says. Not only are irritated customers more likely to cancel their subscriptions, they probably won't recommend a game to friends.

"Who wants to play a game that's frustrating and unfair because people are cheating?" Davis says. "Cheating and griefing can have a really negative impact on product sales."

In addition, Davis says, griefing can increase a game's technical support costs up to 25 percent as customers complain about apparent defects in the game caused by hackers and cheaters.

Davis says another popular cheating technique is "speed hacks" that allow players to send commands faster than competitors or to slow down a game to give them extra time to react to other players' movements.

In response to the griefing challenge, game developers are turning to numerous security technologies. For instance, EvenBalance's PunkBuster software acts like antivirus protection, scanning the memory of players connected to servers to search for patterns of known cheats.

In addition, Ray says, PunkBuster allows game administrators to search for customized exploits by grabbing screenshots from suspected cheaters or to verify that players are using authentic game components instead of files that have been modified to exploit the game. Depending on the specific game's policies, accounts can be closed for severe or persistent violations.

IT GlobalSecure has created software named SecurePlay that allows developers to embed cryptographic security algorithms into their game code to ensure, among other things, that game events are random and players aren't altering the game's timing. The company also validates the legitimacy of software to help reduce piracy.

"These are building blocks developers can use to improve game security," Davis says. "We're not going to solve every problem, but we can solve a lot of them."

Sophos' Cluley suggests the problem could be reduced if game publishers did more to inform users about security, including firewalls and patches. But Ray says security remains a distant afterthought for most computer users.

"People hear about cool new programs from their friends and use them without even thinking about the security implications," Ray says. "I don't think that is going to change,

no matter how educated the gaming public becomes with regard to security issues."

Cluley says most of the attacks so far have been aimed at PC-based games using the Windows operating system, in part because hackers are familiar with it.

"Most of these [hackers] realize lots of people are running Windows computers and often they're poorly protected," Cluley says "They don't need to go after more obscure operating systems where they have to put in more effort to learn how to attack them."

But EvenBalance's Ray says this distinction is likely to be short-lived as online gaming becomes more popular among console game players.

"A console is just a computer that doesn't really look much like a typical computer," Ray says. "I'm pretty sure the lines will continue to blur in the near future."

To print this article or share it with a colleague, click an option below.

Print this Article

E-Mail this Article

PLEASE RATE THIS ANALYSIS

Quality of Analysis

1  2  3  4  5 
POOR EXCELLENT

Comments or Questions

e-Mail Address (optional to enable Insiders to reply)

Submit

© 2005 KPMG LLP, the U.S. member firm of KPMG International, a Swiss cooperative. All rights reserved.

[KPMG Online Privacy Statement and Disclaimer](#)