Security & Online Gaming 2010

"Online gaming has become a massive industry over the last decade. With so many users and so much money involved, malware writers have the perfect opportunity to cash in on online games and virtual worlds."

- Albin Bodahl, malware analyst at Lavasoft Malware Labs

LAVASOFT

Security & Online Gaming 2010

In the past few months, the amount of threats targeted specifically at gamers increased by 600%, according to Lavasoft Malware Labs. Game accounts, log-in details, and passwords are getting stolen, new malware designed to gain unauthorized access to your system is developed at an alarming rate – and as the virtual world grows, cyber thieves will keep cashing in.

Table of Contents

---

*Just how big is the online gaming industry? One Massively Multiplayer Online Role-Playing Game alone, World of Warcraft, has over **11 million** active users. That's more users than the entire population of Sweden - the home of Lavasoft's headquarters.*

Security & Online Gaming

Online gaming, already a booming industry during the whole of the past decade, has lately been surging like never before. Take, for instance, these statistics from comScore, Inc.: in the U.S. alone, usage of online gaming sites has grown 27 percent during the past year to 86 million visitors in December 2008; the total time spent gaming online has spiked by 42 percent.[1]

For years now, consumers have been turning to their computers to be entertained by video games or escape from the routines of their daily lives by creating new personas in Massively Multiplayer Online Role-Playing Games (MMORPG's), enabling them to connect with thousands of people around the globe. Partially explaining the current boom in online gaming, experts say, is the need to find low and no cost entertainment solutions in the tight economic climate.

"It appears that online, ad-supported gaming is one of the activities that has benefited during this economic downturn," says Edward Hunter, comScore director of gaming solutions. "Not only have consumers turned to outlets such as gaming to take their minds off the economy, but as they curtail their discretionary gaming-related purchases they are turning to free alternatives."

But it's not all fun and games in these virtual worlds. Virtual worlds mimic everyday life in a variety of ways; unfortunately, fraud and theft is included. And that means that the games you, or friends and family members, play on your computer may be putting you in harm's way, according to security experts.

"Not all is well in these virtual worlds, where virtual evil can become greedy reality. Online games are played by real people, including thieves and con artists who make real money by stealing other people's virtual property," said Sergey Golovanov, in an analysis of online games and fraud at VirusList.com.[2]

It seems to be the same cycle of fraud that we so often see on the Web - popular sites and services that draw in high amounts of visitors and money, in turn, attract fraudsters looking to plunder a cut of the profits.

"Online gaming has become a massive industry over the last decade. Industry statistics tell us that in 2008, Western consumers, alone, spent over $1.4 billion on gaming subscriptions. With so many users and so much money involved, malware writers have the perfect opportunity to cash in on online games and virtual worlds," says Albin Bodahl, malware analyst at Lavasoft Malware Labs.

In fact, malware authors are capitalizing on the transfer of cash and virtual goods that takes place regularly in online games by developing Trojans aimed specifically at plundering passwords and harvesting log-in details from users of MMORPG's. The scammers are usually after the credit card and billing information for online game accounts, and even the virtual world loot, which they can auction off for real world money. Malware Labs at Lavasoft works to prevent this type of fraud and to keep users protected by constantly updating Ad-Aware's Detection Database with newly emerging threats; a high amount of unique files in the online games family of threats are added into detection with every update, according to Malware Labs.

"There's little doubt in my mind that the amount of malware targeting various MMORPG's will continue to increase in proportion to the amount of new game subscribers," Bodahl says.

[1] http://www.comscore.com/Press_Events/Press_Releases/2009/1/Online_Gaming_Grows

[2] http://www.viruslist.com/en/analysis?pubid=204791963

The Top Threats to Online Gamers

Fraud, thievery and malware are running rampant in online games and virtual worlds. Malware Labs at Lavasoft has compiled a list of the most common types of foul play that frequent gamers are bound to face. Keep reading, below, to prepare yourself for what you may encounter; giving you the information you need to avoid these hazards.

Rogue servers offering low or no cost games

Looking to cut corners by finding low or no cost versions of virtual worlds and online games? Not so fast! There are an abundance of rogue servers for Massively Multiplayer Online Role-Playing Games (MMORPG's) out there on the Web.

These rogue servers offer free versions of online games, and likewise are popular among those who cannot afford, or choose not to pay for, legitimate game servers. While rogue sites are widely available online, they pose a plethora of issues for users, from low game quality to support problems - and even a higher prevalence of theft and fraud.

"Administrators at rogue servers don't have the time or resources to investigate theft and fraud. This makes it easier for criminals to hide their presence and avoid getting caught," says Albin Bodahl, a malware analyst at Lavasoft Malware Labs.

Social engineering scams and phishing to gain log-in details

In order to pilfer credit card information or log-in details from gaming accounts, scammers have been known to employ a variety of social engineering tactics to get victims to play right into their hands and give up their real or virtual world loot.

To pull off this devious tactic, criminals may login on forums or game servers and send messages to inexperienced users, offering their expertise in return for passwords or other personal information.

"They may use the information they gather to make use of the "Have you forgotten your password?" function on gaming sites. The thief will search for known answers to security questions, and then he or she will have the option to change the password and hijack the account," Bodahl explains.

Phishing, when online scammers attempt to entice users into disclosing personal or financial information by appearing to be a trustworthy or familiar source, is also employed by thieves to specifically target gamers. According to the analysts at Malware Labs at Lavasoft, phishers, guised as representatives of the game - such the gamer server's administrator - have been known to persuade victims to authenticate their account, threatening to suspend gaming activity if they fail to comply. Once perpetrators have access to a user's password, they are able to steal the victim's virtual property and sell it to others.

Malware specifically targeting online games

Malware writers are seizing the opportunity to cash in on the transfer of money and goods that takes place regularly in online games and virtual worlds. They do this by developing Trojans aimed at plundering passwords and harvesting log-in details from users of MMORPG's.

Lavasoft Malware Labs calls this specific family of threats, which are detected by Ad-Aware, Win32.TrojanPWS.OnlineGames. Malware Labs also has MMORPG malware related to certain games in detection, such as Win32.TrojanPWS.WOW, which sets its sights on World of Warcraft players. These types of specific threats are often constructed to harvest passwords on the most popular game sites, stealing them from users as they visit the targeted game-server and fill in their log-in data.

Malware Labs works to prevent this type of fraud by constantly updating Lavasoft's Detection Database with threats related to online games and virtual worlds.

Exploiting vulnerabilities in game servers and browsers

An exploit is a vulnerability or bug in software used to take advantage of a user's system to gain unauthorized access. To target gamers, cyber criminals exploit vulnerabilities in both web browsers and game servers.

Game servers are servers, run either remotely or locally, that online entertainment fans use to play multi-player games or video games. Just like any other software, game servers can contain vulnerabilities, which can be leveraged by cyber thieves in order to access databases and passwords.

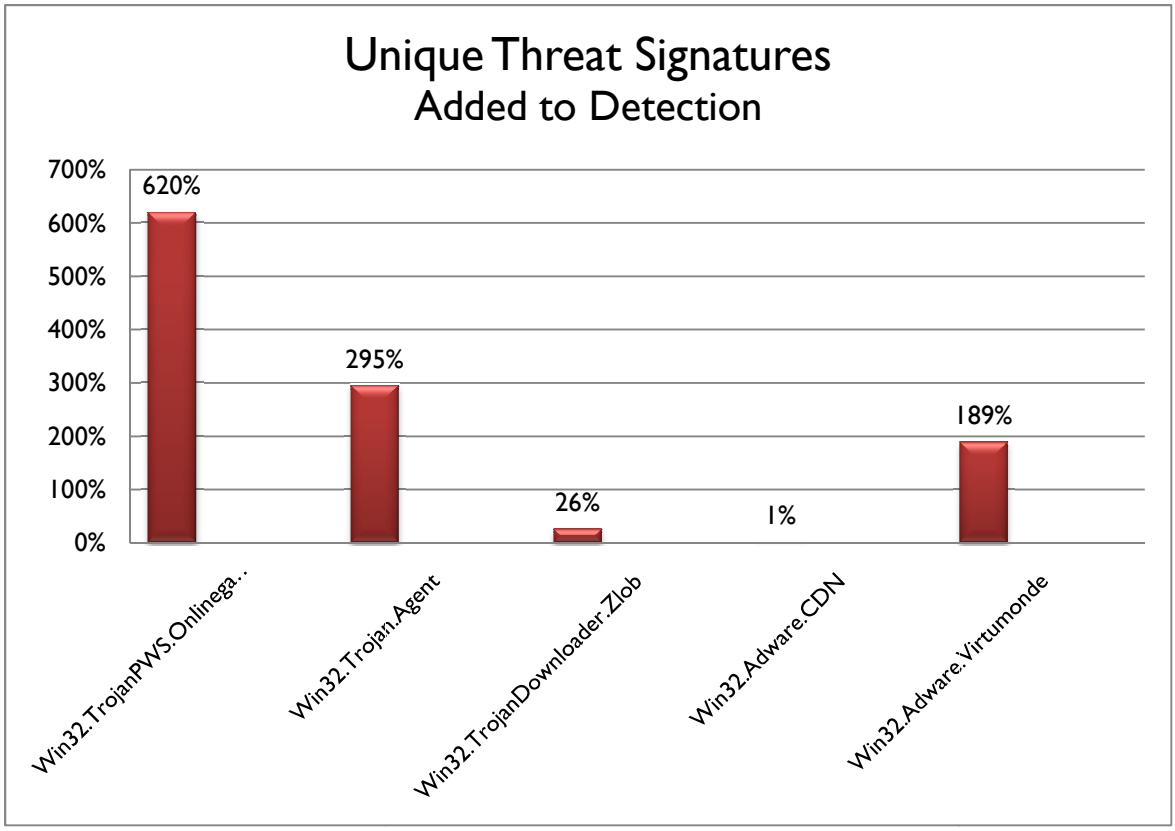
Browser exploits can be used to make the browser itself do something unexpected and unwanted, like propagating a virus or installing spyware. Browser vulnerabilities may be used by criminals on specific game sites and forums to download MMORPG malware, such as the Win32.TrojanPWS.Onlinegames family of threats.

Malware in Online Games

Detection Statistics from Lavasoft Malware Labs

The amount of unique signatures in the Win32.TrojanPWS.Online games family of threats – made up of malware aimed specifically at plundering passwords and harvesting log-in details from online gamers – increased by over 600 percent.

The chart below shows the percent increase in unique threat signatures added to five prevalent threat families in Ad-Aware's Detection Database from November 2008 through August 2009.



Top Security Tips for Online Gamers

Fraud, thievery, and malware are targeting online gamers at rising rates. Be smart as you play in order to avoid the game thieves and crooks looking to take advantage of you. Brush up on these security essentials – Lavasoft's list of the top 9 things you need to know to stay safe in online games and virtual worlds.

1. **Use real-time anti-malware protection**. Ad-Aware Game Edition, which provides real-time anti-virus and anti-spyware protection, is designed specifically with gamers in mind.
2. **Play only on legitimate and trustworthy game servers.** Cutting corners by using free games provided by rogue servers can result in low game quality, support problems, and a higher prevalence of theft and fraud.
3. **Use complicated, "non-dictionary" passwords.** Compose passwords that are at least 10 characters long, and are made up of a mix of letters, numbers and symbols.
4. **Use common sense when you're approached for information or given a suspect call to action.** Exercise caution with e-mail and in-game messages, and never give out your account information.
5. **Update the definitions file of all security software constantly.** This will ensure the threat database is up-to-date and that the program is prepared to catch the latest threats as they are placed into detection.
6. **Use Hosts file protection** to help avoid redirections to malicious servers.
7. **Keep your operating system updated with the latest security patches,** along with any other potentially high-target third party software, like Adobe Acrobat Reader.
8. **Install and run applications that support rootkit protection.** Many computer users like to run a variety of different scanners to help find infections. Still, use caution when choosing new programs in order to make sure to use reliable, respected security software
9. **Keep your main web browser updated with the latest patches.** Browser vulnerabilities may be used by criminals on specific gaming sites and forums to download MMORPG malware.

About Lavasoft

Founded in 1999, Lavasoft is "the original anti-spyware company", with over 400 million downloads worldwide for the flagship Ad-Aware product. A private company headquartered in Gothenburg, Sweden, Lavasoft provides security solutions for individual consumers and enterprise clients alike, including anti-spyware, anti-virus, registry optimization, firewall, digital shredding, and encryption.

For additional articles, white papers, blogs, and more, please visit www.lavasoft.com

Address

Lavasoft AB
Odinsgatan 10
411 03 Gothenburg
Sweden

+46-(0)31-777 77 50
Fax: +46-(0)31-15 69 10

press@lavasoft.com