Security Spotlight articles discuss recent noteworthy threats that users may encounter and should be aware of while surfing the Web.

FROM VIRTUAL WORLDS TO REAL-WORLD THREATS

As a widely popular form of entertainment, online games have naturally become part of a lot of people's lives. This same popularity, unfortunately, has also made online games lucrative targets of attacks ranging from simple spamming to more complicated data stealing.

Online Games Take over the World

The past few years have turned the Web into a hub of online games that cater to a wide variety of consumers. These games ranged from simple card games to more complicated and exciting massively multiplayer online role-playing games (MMORPGs).

In an MMORPG, several online gamers from around the world meet in a virtual world to interact and play with one another. Online games have become such a hit among users that LCM Research reported that the total online gaming market revenue in 2009 reached US$15 billion. Even more impressive, however, is that this figure is expected to further increase to US$20 billion this year.

As a widely popular form of entertainment, online games have naturally become part of a lot of people's lives. This same popularity, unfortunately, has also made online games lucrative targets of attacks ranging from simple spamming to more complicated data stealing.

Interactive Entertainment—Online	2008 Revenue	2009 Revenue	2010 Revenue	2009–2010 Growth
China online	US$3.1B	US$4.5B	US$5.6B	25%
WoW	US$1.3B	US$1.5B	US$1.6B	5%
Brazil, Russia, India, and rest of Asia	US$0.3B	US$0.8B	US$1.5B	100%
Korea online	US$1.3B	US$1.3B	US$1.4B	5%
Virtual worlds/Casual MMORPGs	US$0.7B	US$1.0B	US$1.4B	35%
Online casual (e.g., EA games)	US$0.9B	US$1.2B	US$1.4B	20%
Social networking games	US$0.2B	US$0.7B	US$1.2B	92%
iPhone games/apps	US$0.1B	US$0.5B	US$1.0B	100%
Xbox Live!	US$0.6B	US$0.8B	US$1.0B	25%
EA Digital	US$0.4B	US$0.6B	US$0.8B	36%
Rest of the world and others	US$0.3B	US$0.5B	US$0.7B	40%
Sony PlayStation	US$0.1B	US$0.3B	US$0.5B	50%
Nintendo	US$0.1B	US$0.1B	US$0.1B	20%
Subtotal	US$9.3B	US$13.6B	US$18.1B	33%
PC downloads	US$0.6B	US$0.8B	US$1.0B	25%
In-game advertising	US$0.5B	US$0.6B	US$0.8B	33%
Total	US$10.4B	US$15.0B	US$19.9B	32%

Source: LCM Research

Table 1. *LCM online game forecast*

TREND MICRO

In China alone, the online gaming market revenue is expected to reach US$5 billion this year, as the number of online gamers in the country increases to 338 million. Online gaming is also a huge hit in Europe, as British, German, and French gamers have been reported to spend hundreds of millions just to play them. In a recent study, the Deutsche Bank estimated that the online gaming market penetration rate in the region will reach 9 percent by 2012.

Online Gamers Take on Web Threats

The explosive growth and reach of the online gaming market naturally made it an appealing cybercriminal target, as evidenced by the following reported cases:

- **Phishers target "World of Warcraft (WoW)."** Blizzard Entertainment's "WoW," one the world's most popular MMORPGs, has also become one of the most targeted online games to date. "WoW" players are most commonly victimized via the game's in-game chat/whisper system.

  In such an attack, a "WoW" player receives an in-game chat/whisper from an unknown person offering free gifts. To avail of these, however, the recipient must register on a site, which in reality, is a phishing site that collects *Battle.net* login credentials.

  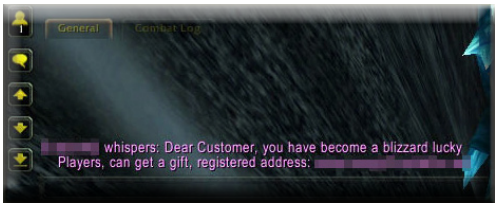

  Figure 1. *Sample malicious "WoW" in-game whisper*

  TrendLabs engineers recently saw a new approach to this scam. Cybercriminals sent out phishing URLs via "WoW's" in-game email service to players' mailboxes. The email message references other Blizzard Entertainment games such as "Starcraft II: Wings of Liberty." To make the message look credible, the embedded URL contains the string *worldofwarcraft* along with an abbreviation of *Cataclysm*. It is, however, worth noting that the site's domain is registered and hosted in China.

- **Supposed figures of authority threaten online gamers.** Another "WoW" scam involved cybercriminals posing as Blizzard Entertainment employees. They used company names with strings similar to *Blizzard*.

  The fake employees threatened to suspend the recipients' accounts should they fail to register on a site whose link was embedded in a chat message. The link, of course, led to a phishing site that looked almost the same as the legitimate *WoW Armory* site.

  In response, Blizzard Entertainment intensified its information drive on *Battle.net's* security page. It also provided an accessible means for users to report similar threats.

- **Malicious links spread via *PlayOnline.*** In this attack, cybercriminals sent out phishing URLs via the *PlayOnline* gaming service platform instead of via usual means like email messages. This threat targeted the players of one of *PlayOnline's* most popular MMORPGs, "Final Fantasy XI."

  "Final Fantasy XI" players can chat with their fellow players using the in-game *Tell* command. Leveraging this feature, malicious users posed as game administrators and sent out messages written in Japanese to players.

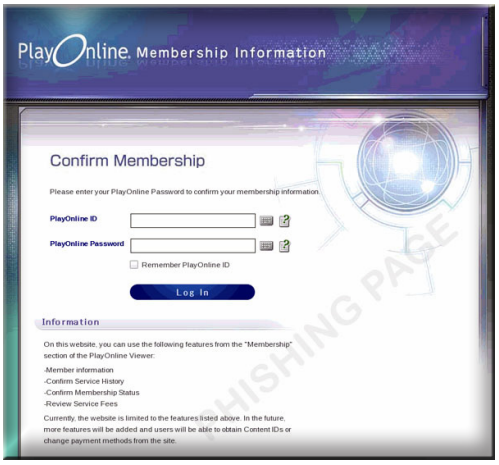

Figure 2. *Sample* PlayOnline *phishing page*

Trend Micro senior threat researcher Noriyaki Hayashi noticed that the messages were grammatically incorrect and so might not have come from a native Japanese speaker. Clicking the link embedded in the messages led users to a fake *PlayOnline* login page.

Hayashi further observed that although the overall appearance of the said login page looked identical to the legitimate site, its contents were written in English while those of the real *PlayOnline* page were in Japanese.

Inside the Enemy's Lair

In the research paper, "Dissecting the *XWM Trojan Kit:* A Peek at China's Growing Underground Online Gaming Economy," senior threat researcher Lion Gu unraveled a threat that targeted China's thriving online gaming industry in the form of the *XWM Trojan Kit.* The said kit has 21 Trojan generators and a back-end server component that serves as a site for storing stolen data.

In the paper, Gu described how cybercriminals configured the *XWM Trojan Kit's* generator to steal pertinent user information via Trojans in the form of malicious .EXE files. These Trojans usually performed several routines, including dropping a .CFG and a .DLL file that were then loaded onto an infected system's memory.

The .DLL file performed several functions, including terminating antivirus software processes, dropping a driver file, and stealing online gaming information and sending these to a back-end server.

To distribute the said Trojans, the cybercriminals behind the attack compromised legitimate sites by inserting download URLs into their pages or by exploiting vulnerabilities. At times, they also cut a deal with the administrators of small sites to distribute the malware along with or in the guise of free music, movie, and/or software files.

Perpetrators of such a scam certainly have profit in mind. The registration window that appeared and required a user to pay for a registration code was proof that this was indeed a money-making scheme. Apart from wheedling online gamers to part with their hard-earned cash, the creators of the kit also advertised and sold their creation for RMB 2,300 to their criminal peers. Each executable Trojan was also sold for RMB 250. To entice people to buy, they also offered free anti-detection services for six months and hosting services for the customers' back-end servers.

Playing the Game Right

The incidents featured in this article prove that everyone can become victims of cybercrime. Online gamers are just as susceptible to information theft and monetary loss as any enterprise, especially those who are into buying virtual items and memorabilia.

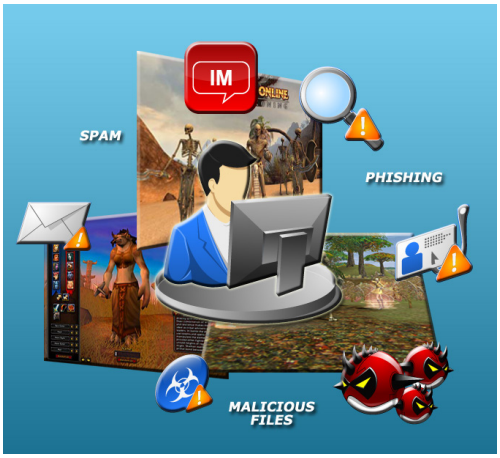

Figure 3. *Threats online gamers face*

This problem, however, is not without a solution. As in the "WoW" and *PlayOnline* incidents, online gamers must refrain from entertaining in-game messages with embedded links from unknown senders. They must especially be wary of clicking the said dubious-looking links. It will also help if they know the specific URLs of the legitimate sites related to their favorite games so they will not be easily tricked into clicking fake URLs.

As an added precaution, using unique login credentials and email addresses to register on gaming sites is a must. They should ensure that the user names, passwords, and email addresses they use for gaming sites differ from those for social networking and for conducting online transactions.

Since it is common for online gamers to hide behind pseudonyms and take the guise of virtual characters, they must exercise caution when dealing with their peers at all times. If at all possible, they should never share personal account information with others, gamer or not. They should keep in mind that there is always that possibility that the people they are dealing with may be an agent of online threats.

To proactively address online threats, gaming sites such as that of Blizzard Entertainment have made it a practice to post security advisories on their pages to help customers protect themselves.

Online gamers should also be careful when downloading tools or add-ons to improve their gaming experience, as these may be malicious in nature. For added measure, they should make sure that their OSs, Web browsers, and software are always up-to-date.

Installing a security solution that works by blocking access to all kinds of online gaming threat vectors—spammed messages and malicious URLs and files—is also advisable.

References:

- Adobe Incorporated. (2010). *Adobe Acrobat 9 Standard*. "Security Alerts." http://help.adobe.com/en_US/Acrobat/9.0/Standard/WS981E9B4B-F8E4-4511-ADE4-2D7380472979.html (Retrieved October 2010).
- Chad Catacchio. (October 9, 2010). *TNW*. "Report: China Online Gaming Market to Reach $5B This Year, 338M Gamers." http://thenextweb.com/asia/2010/10/09/report-china-online-gaming-market-to-reach-5b-this-year-338m-gamers/ (Retrieved October 2010).
- Menard Oseña. (September 28, 2010). *TrendLabs Malware Blog*. "World of Warcraft Scams: Free Gifts and Fake Account Suspension Threats." http://blog.trendmicro.com/world-of-warcraft-scams-free-gifts-and-fake-suspend-account-threats/ (Retrieved October 2010).
- Nicholas Lovell. (June 22, 2010). *GAMESbrief: The Business of Games*. "The Online Games Market Was Worth $15 Billion in 2009, and Will Grow to $20 Billion in 2010." http://www.gamesbrief.com/2010/06/the-online-games-market-was-worth-15-billion-in-2009-and-will-grow-to-20-billion-in-2010/ (Retrieved October 2010).
- Noriaki Hayashi. (August 11, 2010). *TrendLabs Malware Blog*. "Phishing Attacks Target Japanese Gamers." http://blog.trendmicro.com/phishing-attacks-target-japanese-gamers/ (Retrieved October 2010).
- Richard Law. (June 23, 2010). *Reuters*. "Online Gaming Market on the Verge of an Explosion." http://blogs.reuters.com/great-debate-uk/2010/06/23/online-gaming-market-on-the-verge-of-an-explosion/ (Retrieved October 2010).
- Trend Micro Incorporated. (October 2008). *TrendWatch*. "Threat Management: Virtual Worlds." http://us.trendmicro.com/imperia/md/content/us/pdf/threats/securitylibrary/virtual_worlds_white_paper_10_31_08.pdf (Retrieved October 2010).
- Wikimedia Foundation Inc. (October 21, 2010). *Wikipedia*. "Massively Multiplayer Online Role-Playing Game." http://en.wikipedia.org/wiki/Massively_multiplayer_online_role-playing_game (Retrieved October 2010).