Cybercriminals target online gamers

Kaspersky Lab experts recorded 7000 attempts to infect gamers around the world every day in 2012. The attacks are launched in an attempt to gain access to personal user data, such as passwords to online games and online banking systems. Where games are concerned, malicious users attempt to steal avatars and in-game items subsequently to sell these virtual goods for real money. In the case of online banking, cybercriminals aim to steal money directly from real bank accounts.

As Kaspersky Lab experts discovered, in order to do this, malicious users send an average of 10 emails with malicious links and attachments to gamers every day, in addition to making roughly 500 attempts to infect gamers via browser-based attacks. What's more, the company's "collection" of malicious programs targeting online games is increasing at a rate of 5000 new programs a day.

Phishing

One of a malicious user's most favoured tactics in the world of online games is, of course, social engineering - phishing in particular. For example, cybercriminals invoke the names of well-known gaming worlds and desperately try to lure gamers to their fake websites in order to harvest passwords from registered gaming accounts. In 2012, Kaspersky Lab experts recorded 15 million attempted visits to phishing websites designed to look like the pages of one of the largest developers of online games. As it turns out, there were up to 50 000 attempted redirects to phishing sites each day. Fortunately, all of these trusting users were saved by the professional anti-phishing system built into Kaspersky Internet Security, which promptly detected the threat.

Threats targeting gamers are found all over the world, but are, of course, not found in equal concentrations everywhere as their numbers are in direct correlation to the number of active players found in different countries. In 2012, the top-three unlucky targeted countries turned out to be Russia, China, and India. These are the countries where gamers face the highest risk of infection and subsequent theft of avatars and in-game valuables. We also hasten to note that this list of "leaders" has remained more or less unchanged over several years and there is, unfortunately, no reason to expect malicious users to lessen their interest in this area.

Don't just click on the link

Nevertheless, it is entirely possible to protect yourself and your in-game alter ego against attacks from cybercriminals. At first glance, expert recommendations appear to be obvious, although in practice they have proven to be effective time and again. Kaspersky Lab's malware expert Sergey Golovanov suggests that gamers adhere to the following simple code of Internet conduct:

"First and foremost, one needs to be alert when receiving emails featuring, for example, a request from an online game's admin server for personal information about your account or an authorisation offer under some pretext. Don't just click on the link right away - it could be a phishing site.

"Next, don't download unofficial patches from dubious sources - you could easily end up downloading a 'bonus' in the form of a Trojan that would then infiltrate your system and start stealing all of your passwords. And I don't mean just for online games, but also for bank cards, if your bank offers online services. With this in mind, gamers might consider keeping an up-to-date virtual debit card that lets them limit their spending to an amount they choose - with no risk of someone else cleaning out their account."

All the same, malicious users are just that, and some of them can outsmart even the most cautious user. That is why experts strongly recommend using professional security solutions. For example, Kaspersky Internet Security 2013 contains the most up-to-date technologies available today for detecting and blocking malicious programs - particularly anti-phishing, automatic security against exploits, a virtual keyboard for entering usernames and passwords, and many other functions. Furthermore, it includes a special gaming mode that will run with minimal interference or burden on your system resources and will turn off notifications as soon as the game is launched.