Fernando de la Cuadra
International Technical Editor
Panda Software (http://www.pandasoftware.com)
E-mail: Fdelacuadra@pandasoftware.com

Console viruses?

This year has seen a succession of news stories about malicious code affecting numerous devices, going beyond the concept of the typical 'computer virus'. We have had the first viruses for cell phones, followed by malicious code for cars with Bluetooth technology, then along came a virus for the Sony PSP videogame console, and a week later, one for Nintendo DS.

There is nothing unusual about the appearance of these viruses, sooner or later they were bound to appear. Basically, in the IT security world, wherever there is a programmable system, malicious code can also be created. All the more so in the case of complex systems such as video game consoles, which don't just include a complete operating system, but also documentation for developers.

This situation should come as no surprise, and no doubt more threats of this type will emerge in the not too distant future. At least there is the consolation that it is unlikely they will be able to spread under their own steam.

In theory, videogame consoles are not open systems and new software cannot be entered into them in the same way as with a personal computer. PCs have been designed as general purpose tools, adapting functionality to the needs of the user by means of the installation of purpose-built programs. The same hardware can be used for, say, writing a letter as for cataloguing botanical species or for corporate accountancy; while a video game console has been designed for a sole purpose: playing games.

Similarly, unlike a game console, a personal computer also includes numerous devices through which information can be entered. It is true that latest generation consoles use common communication devices such as memory sticks or USB, IrDA and WiFi connections, but it is still not as simple as it seems to infiltrate these systems, and substantially more difficult than it is with a PC.

Software developed for videogame consoles (games) is designed to cause as few problems as possible. Under no circumstances will it try to exploit vulnerabilities, overwrite prohibited zones or multiply itself in the same way as malicious code.

For a user to become infected they would need to be the victim of some kind of deceit, i.e. being duped into installing software without knowing what it will really do. Although this in itself is easy enough to someone (who wouldn't enter a cartridge or memory stick lent by a friend to try out a new game or demo?), what's the point? The only thing it would serve to do is lose a friend.

Imagine another, perhaps more theoretical scenario: downloading software through the wireless link offered by the new consoles. Involuntarily downloading software through this connection could lead to infection. But in this case, the security situation is the same as in a normal computer, where downloading software could lead to the effects of malicious programs or unexpected errors.

Fortunately, the solution is simple: don't be taken in. All software you run on the console should be original and certified by the developer. Activision, Game Freak, Blade Interactive and SOE are among the many game developers that take extreme care in ensuring that their software is the best, the fastest, the most spectacular and, of course, causes the fewest problems possible.

In short, the console itself is not a game. Regardless of price or capacity, it is still a computer and you have to take care with the software you install. If you do it will surely last for many years to come, maybe even as many as my Atari.

Fernando de la Cuadra
International Technical Editor
Panda Software (http://www.pandasoftware.com)
E-mail: Fdelacuadra@pandasoftware.com