

Today's malware technology



Fifteen years ago, nobody could have imagined how far malicious code would get into our day-to-day work. When a new virus emerged, weeks or even months could go by before it could spread: a floppy disk is not the fastest means of propagation!

The technologies applied to protecting against these pre-historic viruses were extremely simple, but so were the viruses. Therefore, a couple of basic techniques were adequate to combat these threats and computers had a very satisfactory level of security.

However, viruses started getting more complex. Hackers conquered new territories: first, email; then, viruses that could spread without the user needing to open a message; viruses that could infect computers simply because they connected to the Internet...

Each of these steps taken by hackers represented, at the time, a new technology to develop. If email was a threat, permanent antivirus scans should also protect POP3 traffic, in other words, new technology for new viruses.

What's happening in 2006? Are we witnessing a new revolution in the technology used by the authors of malicious code? Not at all, it could even be considered a step back in innovation. The techniques used to drop codes on users' computers are coarser. There is no longer an ingenious idea of how to get into computers, such as using Entry Point Obscuring (EPO) or infecting Windows PE files. The most advanced technique uses a rootkit, commercial or not, but almost never developed by the virus author.

It is complicated to innovate; it requires effort, imagination and work, a lot of hard work. And these three concepts don't seem to characterize virus authors. Security companies have been researching and developing more powerful and effective technologies to combat hackers and at the moment, security seems to have won that battle.

The new dynamic started by hackers has left the technological aspect to one side to focus on the criminal variant. A few years ago, virus authors boasted to the rest about how far their virus had spread, but now, they boast about the amount of money they have stolen through Internet fraud scams.

To achieve this, they don't need to analyze complex APIs nor experiment with new infection systems. A classic trick, an old scam, is enough to get the user's money. In the 30s in the United States, a sales man announced that he sold the definitive solution to the potato beetle at a

Today's malware technology



modest price. Many potato growers replied to the letter they had received with this offer to exterminate the bug.

After paying the fee, these trusting farmers received two small blocks of wood, each about the size of a cigarette packet. In order to kill the beetle, all they had to do was catch one and place it on one of the blocks and then hit it with the other to kill it. Just as the trickster had advertised; rapid, safe and simple. What is the difference between a scam in 1930 and one in 2006? Simply the means.

After winning the technology battle, security technologies are starting the second battle; the fight against malicious codes that are not in the least bit innovative, but take advantage of users who fall into the traps set out by hackers. There is no weaker spot in IT security than an inexperienced or over-trusting user, and therefore, technologies should help to avoid problems.

As hacker technology is stuck where it is and is now known to all, new systems for protecting against malicious code are going to be able to block hacker threats. And if they are not so new, what's the danger? Your money. Think about it and choose how to protect yourself.

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