

Security myths



The IT world is full of myths and legends circulated via email or simply spread by word of mouth. These legends are not the infamous hoaxes or chain letters, but assume that certain things are true, when they usually aren't. However, they are so difficult to prove that they are accepted as true without any evidence whatsoever.

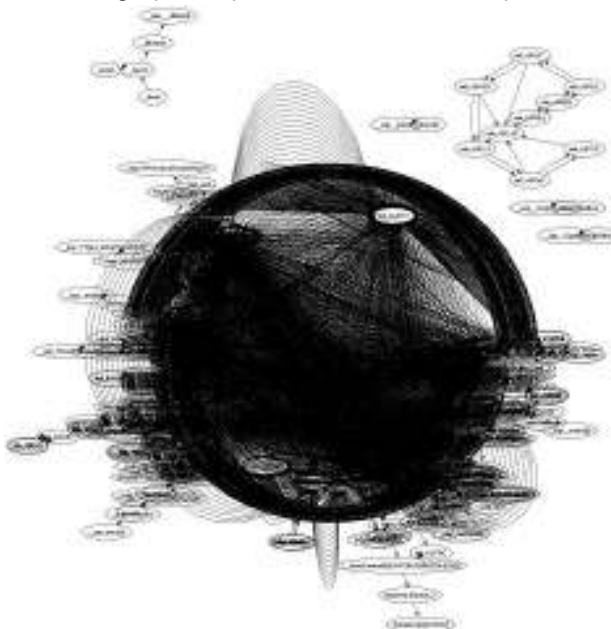
And these strange myths also exist in the IT security world. One of them, based on an accepted fact, is being increasingly refuted: creators of malicious code are good programmers. Some time ago, when viruses were in their prehistoric era, this was true.

For a program to multiply automatically, without users realizing or prehistoric security programs detecting it, it must have been created by a good programmer. Programmers needed a wide knowledge of systems, the options they offered and a huge capacity to innovate.

However, nowadays, these programmers are no longer the "stars" of IT coding. Malicious codes are becoming coarser, less innovative, and sloppier.

The Gaobot.AAF case

The statement that creators of malicious code are poor programmers (or at least, not as good as we think) is not unfounded, as there are methods for scanning programs to see how they were built. One of them, which is widely used for its visual results, offers graphic representation of the components of a program.



These graphs are lines that relate each sub-routine of the code, so that a simple and well-built program would return a simple and clear graph. However, a program without any internal organization and without adequate systemization would offer an extremely complex and disorganized graph.

What's more, two similar programs would offer similar graphs. PandaLabs, Panda Software's malware detection laboratory, has used them to establish the similarities between different variants of a malicious code. They have done this because calls to the same function in different programs are shown graphically.

Security myths



When PandaLabs analyzed a bot (Gaobot.AAF), they were surprised with the result: not only because it was spectacular (they called it “Death Star” due to its resemblance with the space station from Star Wars) but for its strange complexity.

Why is this strange drawing returned? Simply because the original source code of the Gaobot bot family was released to malicious code writers and each one created a new variant. But these variants were not optimized, and therefore, each variant was more complex.

Instead of demonstrating that they were good programmers, all the creators of the Gaobot variants did was prove that their in-depth knowledge was a myth and that they are simple apprentice thieves who copy others' code.

The “undetectable” viruses

Another widespread myth, which is fed by many false email messages is that there are viruses (worms, or Trojans, etc.) that no security solution can detect. And unfortunately, even though this is not true, this myth is sometimes rumored.

A recent news article reported that a student had created a Trojan that recorded the images of his classmates' webcams and then blackmailed them with the recordings. It was said that the Trojan was “undetectable.”

The statement that a Trojan is undetectable contradicts this information, as the authorities created a system to detect and eliminate this code. So, is it undetectable or not?

The problem lies in the difficulty to detect a certain Trojan. The majority of manufacturers of antivirus solutions depend on samples of malicious code to develop a detection and disinfection routine. For this to happen, two circumstances must arise:

1. The malicious code arouses suspicion from a user. If a message is not displayed or if it does not carry out any special action on the computer that makes the user realize that something strange is happening, the system will remain infected, as a sample will not be sent to the laboratories for analysis.
2. The malicious code must have a certain rate of propagation. This increases the probability of affected users notifying the laboratories of the appearance of the code.

In the case of this Trojan, neither of the two circumstances arose. Like most Trojans, it did not show any messages or leave any clues that could give it away. What's more, as it was distributed to very few computers (only the hacker's classmates), it did not arouse any suspicion.

This is an example of the malware situation today: reduced and well-hidden examples. Therefore, antivirus companies will not detect it, as the report says.

Security myths



However, this statement is not complete: it will not be detected until it has been discovered.

In spite of this, this problem only arises with old malicious code detection systems. These systems rely exclusively on data stored about malicious programs and do not incorporate any other detection systems. Therefore, anything that is not stored in its program signature database will be considered valid.

More modern technology for combating malicious code prevents these problems, as instead of clinging to previous knowledge of malicious codes, it seeks them out by analyzing their behavior. Therefore, a program that tries to carry out a malicious action on a computer will be blocked, not because it can be identified, but because of the action it was going to perform.

While users continue to trust in partial and outdated solutions to detect viruses and other malicious programs, they cannot adequately protect their computers, as “undetectable malicious codes” will continue to exist for them, instead of simply “dangerous programs unidentified up until now”.

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