

Security 2.0



The revolution caused by the printing press was not lived as such back in the XV century. It was no more than a good invention. A huge number of people could not read, and back then, books were no more than objects for learned.

When the Internet started to be developed in the 70s of the last century, the situation was very similar: a system only for experts, for the privileged few who knew how to use a computer and had access to one. However, as with the printing press, the revolution took place: many people learned to read, and in the 90s, Internet started to reach many places, and from the year 2000, it even reached many homes.

Although nowadays, books are very common, the UNESCO calculates that in the year 2000, around 90 million people were illiterate. And, if the Internet reached 1,100 million users in 2006 (according to IDC), today, there are still many people who are technologically illiterate. That is not to speak of the functionally technologically illiterate, who use the Internet but have no idea of what they are doing or how it works.

And, more problematic than illiteracy is the despotism of the old concept of the Internet: the 'privileged' few make information available to the rest of the users. A kind of 'enlightened despotism', version Internet 1.0.

But, times are changing. Now, the Internet is true collaboration among users. The information no longer belongs to someone who is kind enough to offer it to the rest, and that's that. Before, a few people shared their information, and now, users do more than just share information: they share knowledge.

There are many clear examples of this new trend, and perhaps the clearest is Wikipedia. An encyclopedia in which users dump their knowledge about a concept, and the rest of the Internet community completes, corrects, or changes it. In this way, Internet users create free knowledge for all Internet users.

This system can be applied to an area of IT that until now continued to be based on these old concepts: antimalware security. Given the current malware situation, the huge amount of malicious codes in circulation cannot reach the research laboratories. Sharing all malicious codes is instrumental to effectively detecting them.

In the same way as an encyclopedia can be built by gathering the knowledge of all Internet users, by collecting information on all the malware installed on Internet users' computers, a collective intelligence system can be formed, which is capable of detecting many more threats than traditional signature-based systems. The security of each computer will dramatically increase, and could directly benefit the community.

This model of Web 2.0 needs real implementation, which is not easy. Firstly, the malware needs to be collected from the computers connected to the Internet, and to do this, malware needs to be clearly defined. In traditional antivirus systems, it was very clear: if the virus laboratory of an antivirus company had received a certain

Security 2.0



code and identified it as malicious, it was classified as malware and added to the famous virus signature file.

However, nowadays, there is so much malware circulating in the Internet that it is impossible for the laboratories to receive samples of all the malicious code around. Therefore, a system is needed that automatically identifies a malicious code without needing a specialized technician to analyze it. If this were the case, the laboratories would be made up of hundreds or thousands of technicians.

Technology is sufficiently developed for a malware detection system to exist that does not rely on previous knowledge of each specimen, just like the collective intelligence system developed by Panda. In this way, only certain characteristics of the code need to be detected to classify it as harmful. Few legitimate programs capture keystrokes and send them out through an open TCP port. Therefore, the probability of a program that does this being malware is extremely high. The same applies to many malicious actions that give away malicious software.

Once the program causing the problems (or that could cause them) has been detected, it is sent to be analyzed in-depth, cataloged and added to the virus database to be used by Internet users. Therefore, any other user with this same malware can take advantage of the fact that a computer connected to the Internet somewhere in the world has fallen victim to this code.

All of the computers in the world can now automatically share malware solutions and detections online at www.infectedornot.com. This website allows users worldwide to check their computers, and any unknown threats detected are sent to a database of new malware, which will be shared with the rest of the community.

Web 2.0 technology in its purest state, helping user security to attain previously unknown levels, making security another feature of the Internet community.

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