



The good, the bad and the malware 2.0

Opinion article
Fernando de la Cuadra

October 2007

A movie has recently been released in which a terrorist manages to take control of absolutely ALL computers in the United States thanks to a cyber-attack. The movie in itself is interesting, as it highlights our social dependence on IT systems.

Fortunately, it is nothing more than cyber-fiction, as the attacker even manages to cut off running water to houses. No doubt water management is heavily dependent on computer systems, but as yet it does not rely exclusively on the Internet. There must be some old pipes somewhere, I'm sure.

The attack, however, could come from another angle. The combined power of computers that are currently infected is enormous. Just remember that in January 2004, MyDoom managed to cause problems for Santa Cruz Operation, as the worm was designed to launch a denial of service attack against the website of this company.

We are talking about 2004. Now in 2007, the situation has advanced radically. Malware is more abundant than ever, and the number of infected computers is far greater than in 2004. And it's not just the number, although there are more computers than in 2004, the percentage of them with problems is also much higher. There are more computers, there is more malware, there is more danger.

Moreover, another factor has increased which is often ignored: bandwidth available for personal systems. There are now many providers offering upwards of a megabyte per second, a figure that some years ago was unthinkable. Is quite common for homes to have 4MB of bandwidth, and even in mid-sized companies this figure is quite small. What this means is that we are increasingly offering malware greater communication capacity.

Several sources indicate that there are currently more than 2 million zombie computers in Asia. If each of these has at least one megabyte per second of bandwidth... the communication capacity that can be used for malicious ends in Asia alone is frightening. In addition there are more than 20,000 new zombies every day, outstripping those that are detected or simply fail to operate.

With this sort of attack power, any service that depends on the Internet could be brought down. There would be no way to withstand such an avalanche of information, and Web services would fall one by one. Communications would grind to a halt as the Internet would be completely saturated.

But there is a fundamental error with this cyber-fiction. Why would a hacker want to leave an entire city without water? What is the point of suddenly bringing a nuclear power station to halt? Not even the most radical environmentalists want to do that. Just like an Agatha Christie novel, if you want to find the perpetrator look for the person who stands to gain most; leaving a city in the dark brings no benefits to a hacker.

Today's cyber criminals have no megalomaniacal ambitions of global destruction. Lex Luthor, the bad guy from Superman, might have done, but that was a comic. In the real world, it's not world domination, but money that crooks are after, operating as quickly and quietly as possible.

It's much more profitable to steal the account details of several users and drain these accounts bit by bit. For this, all that is needed are a few Trojans installed on systems and the ability to handle them correctly. And several accounts could become hundreds or thousands of bank accounts and credit cards, offering a considerable cash flow at someone else's expense.

And yet this is not cyber-fiction. Data on real infections is alarming, and worse still: most users don't even know they are infected. They still put their faith in antivirus solutions based on obsolete technologies that can detect a lot of code, but only if it is known.

When a new code appears and reaches a system without adequate protection capacity, the compromised computer will become just another addition to the list of zombies. Transforming a known malicious code into a new strain is a simple task. They can even be automated to create a

new one every few minutes. Are laboratories able to detect them and offer new solutions every 10 minutes? And even if they could, can they update users every 10 minutes? And if they did, can solutions rapidly process multi-megabyte signature files?

Evidently, the answer is 'no' to all of these questions. The solution to a new security panorama is not old technology. We need to take a step forward and realize that although this technology can help, we need something else. A single computer cannot analyze and process this quantity of data.

Some years ago, when the calculation power of systems was small, large calculation centers were often used, and in fact, today such 'supercomputers' are still employed in areas such as weather forecasting or the analysis of protein folding. These special centers have sufficient scale for macro-processing of calculations, where the number of operations per second is infinitely greater than normal systems.

This same calculation power can be used in the fight against malware. In the face of the kind of avalanche of malicious code that we are now witnessing, a simple PC does not have the power and processes necessary to detect more than 2 million malicious codes in a matter of milliseconds. However, specialized scanning and detection centers can do this.

Moreover, these centers have the advantage of having information online from millions of computers transmitting data on malicious code, so real-time information on the latest threat is available, even malware created just five minutes beforehand and that has only infected a couple of computers.

Therefore, given the reality of this malware avalanche, we need the power that these specialized centers can offer. They are already available, and thanks to them you can scan your computer and discover even the most recent malicious code without having to wait for tomorrow's update. In the current climate, tomorrow could be too late.

Fernando de la Cuadra

Community & Spokesperson Manager

Panda Security (<http://www.pandasecurity.com>)

E-mail: fernando.delacuadra@pandasecurity.com