

Voice over IP under threat?



There has recently been considerable alarm about the possibility of a malicious code spreading via Skype. Skype is a system that allows voice communication over established Internet connections, in an environment very similar to that of telephone calls. It even allows calls to be made to telephones from a computer, with lower tariffs than that of a normal call.

The real problem that a malicious code for Voice over IP (VoIP) would suppose is that it opens a whole new field for hackers to create new types of malware. Initially, one might think of malicious code that uses VoIP in order to propagate, as was the case with the Trojan mentioned at the beginning. In reality, this represents nothing more than finding a new communication channel. New? No! There are already many worms that spread using numerous instant messaging systems. So this Trojan has not really done anything that hasn't been going on for many years now.

The problem lies in using the full characteristics of VoIP in order to spread malicious code. Imagine a dataflow across an audio channel (perhaps at a frequency that is not audible to humans) that could crash the voice system, causing a denial of service. Or that this dataflow could be used to create a system status that would allow execution of malicious code. This would be something genuinely new with respect to propagation of code, unlike other hundreds of codes that use messaging systems simply to propagate. But this is nothing more than speculation.

Evidently, this would require a large degree of innovation, research and development on the part of the creators of malicious code, and I genuinely doubt that they would bother. The situation that we find ourselves in now is a long way from that kind of 'paradise' in which hackers were not such bad types, and were only after achieving personal notoriety. Now, practically all malicious codes created are designed specifically to generate profits for their authors, whether it be through scams, fraud, identity theft, stealing passwords...

The precautions that users should take in the face of this new panorama are not that different from those adopted until now by the majority of reliable antivirus developers: a good system for scanning files and a good database of virus identifiers, that's all. This is how things have worked until now, and the results have been more or less acceptable. Protection has been, well, adequate.

But virus creators are well aware of how antivirus applications operate and, needless to say, they create new strategies to evade detection. And as security providers are becoming much faster at detecting malicious code, so virus creators need to find a way to counter this speedy response.

Their method until now has been to send out massive amounts of malware (generally with the same techniques used for sending spam), and, on the other hand, continual renewal of the code. Where previously there could be dozens of versions of each example, recently there have been hundreds of variants of a single worm, many released on the same day.

Voice over IP under threat?



If this strategy were implemented in IP telephony systems, such as Skype, we could well see many highly dynamic malicious codes, so that the technologies used until now (based on virus signatures) would not be sufficient for protecting users. If it were necessary to update virus signatures quickly enough to outstrip the speed of 'flash threats', which additionally could change elements of their code in a single day, no antivirus laboratory could cope with the task. In order to prevent this new range of code that tries to exploit telephony systems, we cannot rely solely on virus signatures. This would simply be too slow to thwart the hackers.

Let's imagine a scenario that could become commonplace in the near future: A user has an IP telephony system on his computer (both at home and at work). In his address book on the computer there is an entry, under the name "Bank", with the number 123-45-67. Now, a hacker launches a mass-mailing attack on thousands or millions of email addresses using code that simply enters users' address books and modifies any entry under the name "Bank" to 987-65-43. The problem has now been created.

If any of these users receives a message saying that there is a problem in their account, and asking them to call their bank (a typical phishing strategy), they may not be suspicious, as they are not clicking on a link in an email (as they have been advised not to do to avoid this type of fraud) nor calling a number in the email (another typical ploy). If they use their VoIP system to call the 'bank', they will be calling the modified number, where a friendly automated system will record all their details.

Traditional antivirus systems might well not have sufficient time to react to a completely new code, as the attack can be carried out in just a couple of minutes. If it is a known code, there would be no problem, it would be in the database and it would be detected. In the case of completely new code, the protection system needs to be able to see what is happening on the computer, and when the malicious code tries to take any type of dangerous action (in this case changing entries in the address book), the code will automatically be blocked.

In this way users will be properly protected against any possible waves of attacks using voice over IP systems. For traditional problems (known malicious code), signature-based scanning; for new problems, new technologies (intelligent detection of unknown code).

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