

World Cup and virus



Safeguarding your security

The world of security is extremely concerned about Zero Day Exploits, those techniques or programs that take advantage of a new specific vulnerability in a system for various aims, such as the introduction of malware, the theft of personal data, etc.

Software companies always try to provide the quickest possible solution to vulnerabilities, but where a code has been published that takes advantage of a specific vulnerability, the urgency factor is heightened, and it is normally corrected more quickly.

However, the problem of these zero day exploits is that, although the solution to the problem is readily available, (even simultaneously to the exploit itself), those users affected by the problem will take more time in patching a system than in receiving, via whatever route, the malware developed for this security hole, which thus represents an extremely high risk.

Furthermore, this risk is even higher in cases where the hackers try to take advantage of certain events as a decoy, in order to fool users with engineering techniques. These techniques are extensive and direct, and when they take advantage of a moment when users are particularly exposed, there can be total catastrophe in their systems (or, even worse, in their current accounts).

Phishing is a particularly severe case: this is nothing more than a deceit that repeats over and over again, without ever seeming to diminish. As phishers keep acting it is obvious that their techniques are working, as there will always be some user who bites and gives their bank details to false websites.

In June we are going to be faced with an event that will give numerous fraudsters the perfect excuse to deceive many unwarned users: the FIFA Soccer World Cup. On other occasions events are local and attacks are focused on a specific country or culture – now, this is the ideal time to launch a mass-scale attack. Let's say that a supposedly lower-rated team beats one of the favorites. A hacker could send a file with proof of a referee bribe, the perfect environment for a new virus.

In fact, the FIFA World Cup has already been used on two previous occasions to attack users. In May 2005 the Sober.V worm used the possibility to obtain free tickets for matches as a decoy, leading users to open an email attachment that contained the malicious code.

Likewise, less harmful (in IT terms) but just as annoying, was a hoax that was distributed recently, perhaps originating from the Sober.V worm,

World Cup and virus



Safeguarding your security

which referred to the appearance of a reportedly harmful virus relating to the World Cup. As in all cases where hoaxes are concerned, this supposed malicious code is harmful, as it deletes all the data stored on a disk with no possibility of recovery, with no antivirus company being able to solve it.

It's not surprising to hear that an event of this size can, once again, give rise to both malicious code and hoaxes. The huge collection of email addresses managed by spammers (now sold at ridiculous prices) is the ideal way for hackers to distribute a new worm or bot, or to carry out massive user fraud.

In this case, the mere installation of an antivirus will not be enough. The technology used in almost all anti-malware solutions does not have the sufficient capacity to tackle viruses that have not been previously detected and had a classic "vaccine" created for them. Time is required to develop the solution and, although this period is quite short, it is long enough for the hacker to do what he is hoping to do: infect computers, steal passwords, create armies of zombie computers...

When faced with a zero day exploit, (i.e. a vulnerability or factor that takes advantage through social engineering techniques), there are just two solutions: firstly, to be permanently alert to any possible change in the state of security of a computer or entire network, which has been seen over the years as something that is practically impossible; or secondly, to have a package of solutions that are truly capable of detecting unknown threats.

Hackers are already prepared so that, when the first opportunity arises, they can use their malicious code against computers that are protected with obsolete technology. Right from the first kick of the ball in Germany, how many examples of malware will already have been distributed? It's impossible to know, but you'd better make sure that your security solution (whether private or corporate) is able to detect it, or you will fall into the mafia-like networks used by today's hackers.

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