bizcommunity

Vulnerabilities - main target for cybercriminals in 2013

It's reckoned that vulnerabilities in social networks and mobile devices will be the major targets cyber-criminals in 2013 and vulnerabilities in Java and Adobe will be widely used as a point of entry to infect computers.

Software vulnerabilities will be the main target of cyber-criminals next year. This is according to a list, compiled by PandaLabs, Panda Security's malware laboratory, of the security trends that will predominate 2013.

According to Jeremy Matthews, Panda Security' country manager, "It is undoubtedly the preferred method infection for compromising systems transparently, used by both cyber-criminals and intelligence agencies countries around the world.

"In 2012, we saw how Java, which is installed on hundreds of millions of devices, was repeatedly compromised and used to actively infect millions of users. In second place is Adobe, which, given the popularity of its applications (Acrobat Reader, Flash, etc.) and its multiple security flaws, is one of the favourite tools for massively infecting users as well as for targeted attacks," warns Matthews.

Companies also at risk

"Although we may think that home users are exposed to the highest risk, remember that updating applications, which is essential for protection against such attacks, is a complex process, particularly in companies where updating all computers must be coordinated," explains Luis Corrons, technical director PandaLabs, who adds: "At the same time, it is essential to ensure that all the applications used in a compa work correctly. This makes the update processes slow, which opens a window that is exploited to steal information in general and launch targeted attacks in search of confidential data."

Other areas expected to feature significantly in 2013 in terms of security issues are:
• **Social networks:** The second most widely used technique is social engineering. Tricking users into collaborating to infect their computers and steal their data is an easy task, as there are no security applications to protect users from themselves. In this context, use of social networks (Facebook, Twitter, etc.), places where hundreds of millions of users exchange information (very often personal data), makes them the preferred hunting ground for susceptible users.
Particular attention should be paid to Skype, which after replacing Messenger, could become a target for cyber-criminals.

• **Malware for mobile devices:** Android has become the dominant mobile operating system. In Septemb 2012, Google announced that it had reached the incredible figure of 700 million Android activations. Although it is mainly used on smartphones and tablets, its flexibility and the fact that it doesn't require a licence for use will result in new devices opting to use Google's operating system. Its use is going to become increasingly widespread, from televisions to all types of home appliances, which opens up a worl of possible attacks as yet unknown.

• **Cyber-warfare/Cyber-espionage:** Throughout 2012, different types of attacks have been launched against nations. The Middle East is worth mentioning, where the conflict is also present in cyber-space. In fact, many of these attacks are not even carried out by national governments but by citizens, who feel that they should defend their nation by attacking their neighbours using any means available.

Furthermore, the governments of the world's leading nations are creating cyber commandos to prepare bo defence and attack and therefore, the cyber-arms race will escalate.

• **Growth of malware:** For two decades, the amount of malware has been growing dramatically. The figur are stratospheric, with tens of thousands of new malware strains appearing every day and, therefore, this sustained growth seems very far from coming to an end.

Despite security forces being better prepared to combat this type of crime, they are still handicapped by tl absence of borders on the internet. A police force can act only within its jurisdiction, whereas a cyber-croo can launch an attack from Country A, steal data from citizens of Country B, send the stolen data to a serve situated in Country C and could be living in Country D. This can be done with just a few clicks, whereas coordinated action of security forces across various countries could take months. For this reason, cyber-criminals are still living their own golden era.

• **Malware for Mac:** Cases like Flashback, which occurred in 2012, have demonstrated that not only is Ma susceptible to malware attacks but that there are also massive infections affecting hundreds of thousands users. Although the number of malware strains for Mac is still relatively low compared to malware for PCs, we expect it to continue rising. A growing number of users added to security flaws and lack of user awareness (due to over-confidence), mean that the attraction of this platform for cyber-crooks will continue to increase next year.

• **Windows 8:** Last but not least, Windows 8. Microsoft's latest operating system, along with all of its predecessors, will also suffer attacks. Cyber-criminals are not going to focus on this operating system onl but they will also make sure that their creations work equally well on Windows XP to Windows 8, through Windows 7.

One of the attractions of Microsoft's new operating system is that it runs on PCs, as well as on tablets and smartphones. For this reason, if functional malware strains that allow information to be stolen regardless o the type of device used are developed, we could see a specific development of malware for Windows 8 t could take attacks to a new level.

About Panda Security

Panda Security is one of the world's leading providers of cloud-based security solutions, and claims to be the first IT security company to harness the power of cloud computing with its Collective Intelligence technology. Automatically analysing and classifying thousands of new malware samples every day. This is claimed to guarantee corporate customers and home users the most effective protection against Internet threats with minimum impact on system performance. In 2006, Jeremy Matthews founded Panda's local subsidiary in Cape Town, opening the international vendor's first presence on the African continent.

For more information, visit http://www.pandasecurity.co.za/.