

Software vulnerabilities the main target of cyber criminals in 2013

By [Jeremy Matthews](#)

21 Dec 2012

PandaLabs, Panda Security's malware laboratory, has compiled a list of the security trends that will predominate in 2013. Software vulnerability is undoubtedly the preferred method of infection for compromising systems transparently, used by both cyber criminals and intelligence agencies in countries around the world.

In 2012, we saw how Java, which is installed on hundreds of millions of devices, was repeatedly compromised and used actively to 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.

Companies 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 in which updating all computers must be co-ordinated. At the same time, it is essential to ensure that all the applications used in a company 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 September 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 world 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 cyberspace. 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 both 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 figures 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 the absence of borders on the Internet. A police force can only act within its jurisdiction, whereas a cyber crook can launch an attack from country A, steal data from citizens of country B, send the stolen data to a server situated in country C, and could be living in country D. This can be done with just a few clicks, whereas the co-ordinated 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 Mac susceptible

to malware attacks, but that there are also massive infections affecting hundreds of thousands of 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), means 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 only, but 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 of the type of device used are developed, we could see a specific development of malware for Windows 8 that could take attacks to a new level.

ABOUT THE AUTHOR

Jeremy Matthews is the country manager of Panda Security.

For more, visit: <https://www.bizcommunity.com>