Panda Security predicts main security threats in 2016

Panda Security has predicted that the coming year will be filled with threats that could affect private users and small businesses, as well as large corporations. The creation and spreading of new malware samples, aimed at infecting users, will continue growing at an exponential rate, just as we have seen in 2015 where the number of new samples registered daily reached 230,000.

©lithian via 123RF

During 2016, there is a predicted increase in infections via JavaScript and a growth in the number of cybercriminals using Powershell, a tool included in Windows 10 that allows scripts with all types of functionalities to be executed.

Large scale and mobile-based attacks

Cybercriminals are looking for ways to attack the greatest number of users and businesses while achieving the greatest possible profit. For this reason, they will continue to use tools such as Exploit Kits, as many current solutions aren't capable of combatting this type of attack effectively, which means its rate of infection is very high. For the same reason, malware on mobiles will also increase, especially for Android, as it is the most popular operating system on the market.

"Although Android attacks have been commonplace in recent years, the difference in 2016 is the manner in which mobiles will be infected. We will see more threats that root the device, which makes eliminating them a serious challenge for an antivirus, with the exception of those that come installed from the factory", says Jeremy Matthews, Country Manager Panda Security Africa.

There will also be an increase in direct attacks through rootkit techniques, which allow hackers to hide from the operating system and security solutions.

Internet of Things and mobile payment

2016 will be the year in which the Internet of Things flourishes, with more devices than ever connected to the Internet, a feature that enables cybercriminals to access and take control of such devices. With this in mind, cybercriminals are predicted to carry out attacks on devices, such as those seen in 2015 on cars with software that is connected to the internet.

Payment platforms on mobile devices will be under scrutiny as cybercriminals look to take advantage of them, as an easy way for criminals to steal money directly.

"When a platform gets popular it becomes more of a target for attackers who then begin searching for weaknesses in the system", continued Matthews.

Main challenges for security

In the face of the current environment, where the number of threats is growing exponentially and attacks are becoming more sophisticated, users and businesses will have to adopt extra security measures to remain protected against the dangers of the internet in 2016. What's more, for businesses there are also threats that could seriously damage both their reputation and finances. Cybercriminals will make it their goal to steal confidential information relating to the company and even information belonging to their customers. Once they have it, they will try to blackmail the company into paying a ransom to get the information back, a method known as Ransomware.

To face the complexity of these attacks, and those that await us in 2016, it will be necessary for users and businesses to have security tools and solutions that analyze and classify the behavior of all executables, and that also offer advanced protection to prevent and act against security threats.