What is it?

Amongst the most serious and dangerous threats we cannot miss to mention the Trojan Horse. It is represented by an executable file in the Windows OS with various specific characteristics.

From all types of attacks, the Trojan horse is the most popular and widely used form of attack on computers. The name suggests that it has the ability to deceive the user into thinking that the used computer program is running a user authorized action when, in fact, it is meant to manipulate the system.

As mentioned above, the Trojan Horse is an executable file, therefore it cannot run without the initial permission from the user of the system. In order for a permission to be given, it must seem to the victim as a legitimate software. Once the user runs the executable, the hacker gains remote access to the system.

Depending on the damaging action, Trojan Horses can be classified in five categories:

1. Remote access Trojan: provides the attacker with unlimited access to the system allowing him to access, modify, destroy and steal private data, personally identifiable information as well as intellectual property.
2. Data sending Trojan: is designed to send sensitive data such as financial information, specific account credentials, bank account details and many more to the hacker.
3. Destructive Trojan: is created with the intention for it to destroy specific files from the system and is also not detectable by anti-virus applications.
4. Security software disabler Trojan: has the purpose to make the system vulnerable by disabling all security services such as firewalls and antiviruses on the attacked system.
5. Denial-of-Service attack Trojan: is meant to keep the system busy so that no user requests can be performed.

How can I detect it?

The most common way to detect a malicious software is by using anti-virus applications, however those have proven themselves inefficient when it comes to detecting Trojan Horses due to the polymorphism property.

Since those files are made to deceive, it is difficult to differentiate between malicious and legitimate files. Also, collecting the signature of all Trojan Horses and keeping them up-to-date in a directory, is not only unmanageable but due to the fact that new ones are being scripted every day, it is widely impossible.

It is important to notice that those harmful executable files possess certain properties which makes it possible for us to distinguish them from the legitimate ones.

Rather than using signatures, a more efficient way of detecting infected files is to isolate suspicious processes and programs based on its properties and behavior.

Programs such as Wireshark can be used to monitor the activities and processes in the system and have us notified whenever a foreign activity/process takes place.