



CAPTURED

Name

APTs (Advanced Persistent Threats)

Date of Birth

1989

Origin

Moscú

Modus Operandi

This is a set of stealthy, complex and continuous computer hacking processes orchestrated by organized groups of cybercriminals, and generally targeting governments, large companies or institutions.

They are called advanced due to their coordination and their use of sophisticated techniques to penetrate into victims' IT systems, using vulnerabilities and backdoors in operating systems.

ATPs are characterized by their intention to stay hidden for as long a time as possible, in order to steal as much information as they can. They search for the companies' and organizations' most valuable asset: their most sensitive corporate information, and the data that will allow them to monetize the attack immediately.

Arrest

This threat has already been arrested and neutralized by Panda Security.

But if you are not a Panda Security client and you catch sight of it on the company network, contact us immediately to facilitate its capture.

Criminal Record

GhostNet

Large-scale attack discovered in March 2009. Its origin is most likely the People's Republic of China.

GhostNet infiltrated the computers of political, economic and media targets in more than 100 countries.

Operation Aurora

A series of cyberattacks launched in 2009 originating in China. It used a Zero-day exploit to install a Trojan designed to steal information.

In 2010, Google revealed these attacks, alleging that other companies had also been attacked.

Among these companies were leading banks, defense contractors, security providers, oil and gas companies, as well as other tech companies.

Stuxnet

Computer worm that affected computers running Windows, discovered in June 2010. It was the first worm known to spy on and reprogram industrial systems.

The target of this worm was Iran's nuclear infrastructures that used Siemens control systems. Some media outlets attributed it to the US and Israeli secret services.

Red October

In October 2012, a malware program was discovered that was designed to steal confidential information from governments and research organizations.

It is believed that it had been operating all over the world for at least five years before its discovery, stealing sensitive information from diplomatic, commercial, military, aerospace and research organizations in Russia, Iran, the USA and at least 36 other countries.

900 90 70 80

info@pandasecurity.com