Decode FBI spyware

In a new set of declassified files, the US Federal Bureau of Investigation (FBI) has admitted that they have used a spyware for many years to 'grab' cybercrime.

In a new set of decrypted files, the US Federal Bureau of Investigation (FBI) has admitted it has been using a spyware for many years to "grab" cyber criminals .

FBI spyware (CIPAV) is called CIPAV (short for Computer and Internet Protocol Address Verifier - Computer and Internet address verification tool).

CIPAV was known for the first time after the arrest of Josh Glazebrook, a 15-year-old student who threatened to bomb Timberline High School, near Olympia (Washington state) in May 2007. Glazebrook used controlled computers to carry out the "terrorist" mental attacks.

Tracing the origin of these threats to the FBI is not difficult, but after routine investigation, the results only lead to a computer at the Italian National Nuclear Physics Institute. The FBI decided to use CIPAV and they succeeded. In fact, computers at the Italian National Nuclear Physics Institute were taken over by this hacker.

In the FBI's new decrypted file, there is a text that instructs FBI staff how to sneak CIPAV through a link on the secret chat rooms of MySpace.com.

A sworn affidavit of FBI agent Norman Sanders said at the time that CIPAV was able to send information about

MAC addresses, IPs, environment variables and registry information, the closest website to which the machine was. that has just been accessed, the license code of the operating system .

Normally, the FBI will sneak the CIPAV installation on the suspects' computers with a 'secret service' to localize the object when they are contacting the police or victims via email. If the 'secret service' does not work, the FBI will forge an email from the Internet service provider and it is almost certain that the suspect will be trapped.

A document from March 2007 said that the FBI initially used a simple procedure called "Web bug" written by the US Department of Justice's computer and intellectual property department. ' *Some investigators have started using a trick related to' Internet Address Identification Tool - IPAV 'or' Web bug ' ,*' this document writes. continue to develop this trick to become a complete software called Magic Lantern - Magic Lantern (actually a Trojan Horse.) Over a few more developments, this software has become CIPAV.

The first public sign shows the operation of CIPAV appeared in March 2006 when the electronic data analysis unit and password were asked to trace the culprit who was controlling the owner of a Hotmail mailbox. and forced the victim to give him $ 10,000 to redeem. CIPAV has been mobilized and the culprit has not expected him to be caught so quickly.

The FBI file also recounted another victory of CIPAV in August 2005. A hacker broke into a company's system, erased the data on it and asked the victim to pay him a large sum of money to recover the data.

However, like all other spyware, CIPAV can still be detected by antivirus programs before it is installed on the suspect's computer.

However, some people are also concerned that the FBI will use similar tools to detect information from government computer systems of countries around the world.