Polizia di Stato

Cybercrime: GameOver Zeus Botnet Disrupted

An international operation disrupted a crime ring that had infected hundreds of thousands of PCs around the world with the Zeus virus, which allowed cyber criminals to remotely control the victim's computer. This malicious software was designed specifically to steal sensitive information and to use the infected machines for other illicit purposes, unbeknownst to their rightful owners.

The "GameOver Zeus" investigation was carried out by the National Cybercrime Center for Critical Infrastructure Protection (CNAIPIC) of the Italian Postal Police, in collaboration with the Federal Bureau of Investigation in the U.S., and under the coordination of the European Cybercrime Centre (EC3) of Europol.

Besides Italy and the U.S., law enforcement from Ukraine, the United Kingdom, Germany, Japan, France, the Netherlands and Canada participated in the operation. In the latter two countries, in particular, some computer servers central to Cryptolocker and Zeus malware were seized. Cryptolocker is a type of "ransomware" that encrypts the files on victims' computers and demands a fee in return for decrypting them.

160 botnet nodes were identified in Italy, with at least 10,000 computers infected. The number rises between 500,000 and 1 million worldwide, resulting in more than €100m of losses globally.

Through this system, cyber criminals could harvest banking information, such as login credentials from a victim's computer, or engage in other malicious activities, such as participating in Distributed Denial-of-Service (DDoS) attacks, which are launched simultaneously from multiple points, in order to evade detection from law enforcement.

Italian

04/06/2014