

## Cybercrime: over 3 million PCs infected worldwide

Over 3 million PCs worldwide were attacked by cyber criminals through a botnet, dismantled by the Italian National Police with operation "Rubbly".

The botnet server, which was located in the Milan area, was seized by the police of the Italian National Cybercrime Center for the Protection of Critical Infrastructure (CNAIPIC) and will be made available to the European Cybercrime Center at Europol for further investigations.

The experts of the Italian Postal and Communications Police were able to ascertain that the malware, installed through links or spam e-mails or infected websites, enabled offenders to take control of PCs and steal banking information, e-mail passwords as well as credentials to access the most popular social networks.

The botnet malware, known as "Ramnit", was targeting Microsoft Windows operating systems and could also disable antivirus software.

The virus used an algorithm for the automatic generation of domain names (DGA) which were then registered and used to contact the Command and Control server (C&C) set up within the malware, which made them very hard to detect.

The cybercrime police operation, which led to dismantling the C&C servers used by the criminals, is the result of close cooperation between the Italian National Police and the European Cybercrime Centre (EC3) of Europol, in addition to the cybercrime units in Germany, the Netherlands and the United Kingdom.

Italian

26/02/2015